The Cyber/Physical Security Framework

To ensure trustworthiness of a new type of supply chain in “Society5.0”,
so-called “value creation process”

Version 1.0

Cyber Security Division

Commerce and Information Policy Bureau

Ministry of Economy, Trade and Industry

Apr. 18, 2019

Table of contents

Executive Summary

- The Government of Japan is proposing creation of a next-generation smart social infrastructure program named *Society5.0*. The proposed program will provide a variety of products and services for the emerging needs of citizens. It also will provide both economic development and solutions for social challenges by integrating cyberspace and physical space. To support "Society5.0", the Ministry of Economy, Trade, and Industry (METI), proposed a program called *Connected Industries* which will create value by building connections between a wide variety of disparate industrial data.

- In the industrial society of "Society5.0", networking between companies and industries has produced "Connected Industries", in which the connections themselves create new data opportunities, for commerce. It is now possible to construct a more flexible and dynamic supply chain that includes new entities, and as cyberspace and physical space interact with each other, it is a new process that encompasses both spaces. The supply chain itself will create new added value.

- Cybersecurity is critical to the Connected Industries program. An attacker has many more possible targets in the new, interconnected supply chain, so cyber defenses must be drastically increased.

- In addition, the interconnection of cyberspace and physical space means that cyberattacks have an increasing impact on physical infrastructure. The physical consequences of a cyberattack could be enormous.

- The initiatives proposed for Society5.0 integrating cyberspace and physical space create great value for citizens and companies, but the risks and consequences of cyberattacks greatly increase as well. The Cyber/Physical Security Framework will guide the implementation of the Connected Industries program to reduce the risk of cyberattack.

- Because many varied entities participate in highly networked supply chains, measures adopted at a single enterprise cannot assure security across the supply chain or even within its own enterprise. Therefore, each supply chain participant must adopt "security by design" techniques in which security is one

of the primary requirements of a new system. In addition, all participants must ensure security of any shared data. Finally, the entire supply chain must build resilience into supply chain systems to minimize impact of both potential security breaches and system failures for other reasons.

- In the Framework, security measures are shown which are commonly required for all industries for the next-generation supply chain in "Society5.0" an industrial society in which cyber space and physical space are highly integrated. In order to ensure supply chain trustworthiness, security measure are shown from three viewpoints ("Connections between organizations", "Mutual connections between cyberspace and physical space" and "Connections in cyberspace").

- Companies and industries have widely varying tolerance for cybersecurity risks. The Framework is designed with this in mind and should be used as a reference document as enterprises consider their special cybersecurity approaches and needs.

- Finally new threats will emerge with advances in AI technology in the unified cyberspace and physical space. The Framework will evolve to manage new threats, and will be reviewed appropriately.

Introduction

1. Society realized by "Society5.0" and "Connected Industries"

Practical uses of networking and IoT (Internet of Things) are advancing now worldwide, and public and private sectors are beginning cooperation on highly advanced IT in the field of manufacturing to lead the revolutionary changes of "The Fourth Industrial Revolution" such as the "Industry 4.0" program in Germany. In Japan, "The 5th Science and Technology Basic Plan", approved in a Cabinet meeting on January 22, 2016, the Government of Japan proposed a next-generation smart society named "Society5.0" to produce products and services that satisfy a variety of needs, and which also provides both economic development and solutions for social challenges, by closely integrating cyberspace and physical space. Furthermore, we the Ministry of Economy, Trade and Industry (METI) need to develop a new industrial structure to realize "Connected Industries", which creates new added value for "Society5.0", focusing on increased and varied connections.

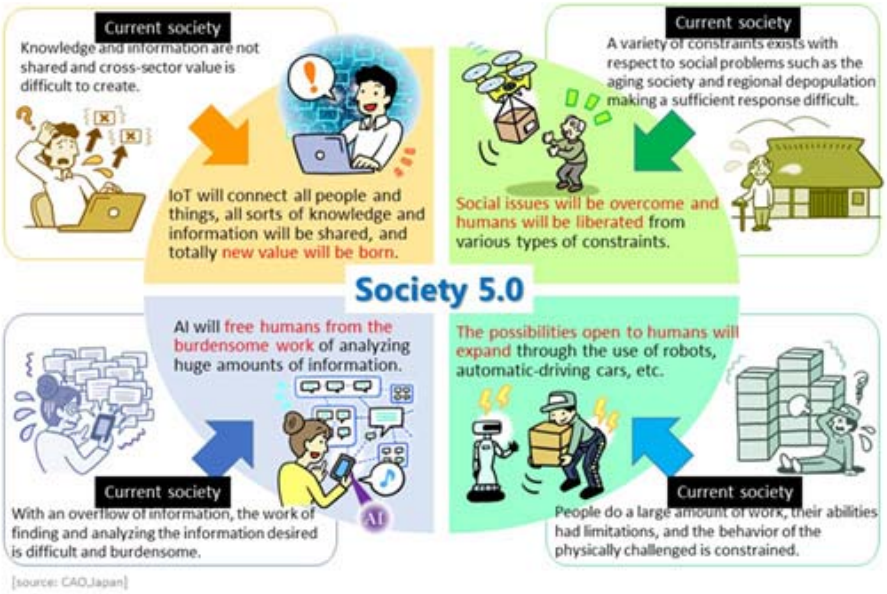


Figure i-1 Illustration of the society realized in "Society5.0"[1]

"Society5.0" is the latest in a series of social structures. It is the next in the series of the hunting society (Society1.0), agricultural society (Society2.0), industrial society (Society3.0), and information society (Society4.0).

[1] The illustration is quoted from the introduction of "Society5.0" by the Cabinet Office.

In the information society (Society4.0), sharing necessary knowledge and information was not enough. It was difficult to create new value, and it was also difficult and burdensome to find and analyze information in the huge amounts of data created.

In "Society5.0", all people and things are connected by IoT, a wide variety of knowledge and information are shared, and new value is created. Moreover, "Society5.0" relieves humans from the burdensome work of analyzing huge amounts of data through the use using Artificial Intelligence (AI). Furthermore, "Society5.0" is not a society where economic and organizational systems are prioritized, but is instead a human-centered society in which AI, robots, etc. will support work formerly done by humans, and provide people with the goods and services they need, when needed, and as much as needed.

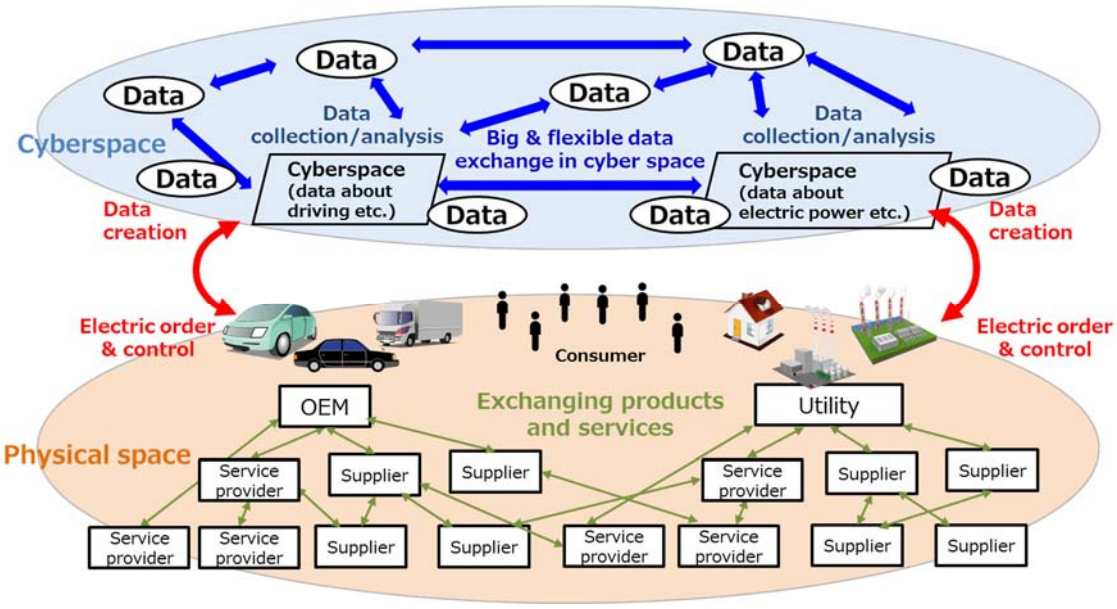


Figure i-2 Illustration of connections between components and data, etc. in Society5.0

■ Change in the supply chain structure

In "Society5.0", the supply chain, which is a series of activities by companies to create added value, will also change its form. The existing supply chain was a rigid, linear structure of strict planning, including design, procuring necessary parts and services based on the design, assembling and processing, and delivering final products and services. It was deployed in a fixed and unchanging manner. In "Society5.0," however, where cyberspace and physical space are highly integrated, needed goods and services are provided to the

people who need them when they need them. The starting point of a series of activities to create added value is not fixed. In the past, suppliers planned and designed the added value; from now on, there will be an increasing number of cases where consumers will become the starting point of creating added value. These activities may change during the process due to the changes made in the requirements specified when starting the creation of added value. If more effective data are obtained, the elements will be incorporated into the new activities.

Supply chains straddle both cyber and physical spaces, and will change into the creation of added value through various dynamically connected items and data. In contrast with conventional standard and linear supply chain, these changed supply chains need to be viewed as the "Society5.0" supply chain, and existing systems and procedures are to be "value creation process" so that it is distinguished from the conventional type.

2. Increase of threats by cyberattacks

In an industrial society of "Society5.0" where cyberspace and physical space are highly integrated, cyberspace expands drastically and points of cyberattack expand; the two spaces interacting with each other increase the impact of the damages on physical space. For this reason, threats to the value creation process (a new supply chain connecting across cyberspace and physical space) are different and more complex compared to what the standard and linear supply chain faced, and will cause a wider range of damage.

It is necessary to understand that major change in the environment will expand the points of cyberattacks. This means that the entire value creation process may become exposed to threats of cyberattacks. For this reason, measures to ensure security in all the elements relevant to the value creation process need to be examined, and trustworthiness of the process needs to be ensured through comprehensive measures, not partial ones.

In addition, new processes that occur with the advanced integration of cyber space and physical space, such as digitization of information obtained from IoT, and the exchange of a large amount of created data, are emerging as new targets for cyber attacks. This needs to be recognized, and ensuring security of the digitalization of information, and security measures to support the accuracy, distribution, and coordination of a large amount of data will become

important issues.

Table I-1 Features of Society5.0 and corresponding security concerns

A large quantity of data exchange	→	- Appropriate management suited for the characteristic of the data is becoming increasingly important
Integration of physical space and cyberspace	→	- Cyberattacks reach to physical space - Assume intrusion from physical space and attack on cyberspace - Intervention in information conversion between physical space and cyberspace
Supply chains connected complicatedly	→	- Range affected by cyberattacks expands

Threats to the supply chain are already arising as a real-life problem. In fact, a case was reported in which equipment of a European company was infected with ransomware. It infiltrated domestic enterprises in Japan via the supply chain, expanded the infection, and stopped some operations as a result.
Given the situation, the necessity to protect IoT and Industrial Control Systems (ICS) by supply chain management is becoming widely recognized in other countries. In the United States, the framework (Cybersecurity Framework), which provides the perspective of cybersecurity measures especially for the critical infrastructure developed by NIST[2] in February 2014, was revised in April 2018. In these documents, they added a description on supply chain risk management and requested to implement preventive measures to the entire supply chain and to conduct audits as needed.

3. Intention of developing the Framework and its scope of application

In the process of achieving "Society5.0" and "Connected Industries," the industrial and social environments are changing considerably. Along with these changes, there are more threats of cyberattacks, and new threats are emerging. Now is the time to begin preparing ourselves for these new and

[2] National Institute of Standards and Technology

increasing threats.
Under such problem awareness, METI has decided to formulate the "Cyber/Physical Security Framework," build a model that appropriately identifies the risks faced in creating added value in the new industrial society, identify the risk sources, organize the overview of the required security measures, and summarize examples of measures which the industrial community can utilize as their security measures.
The Framework covers the entire model of the new industrial society and targets all entities that are working to create added value in it.
In the contents of identifying risk sources and security measures, the following are included;

(1) those applicable to conventional supply chains,

(2) those that need new measures in the new industrial society model,

Security measures can be customized to each enterprise.
In addition, even if a system is not connected to the Internet or other outside networks, increased integration, convenience, and seamless interoperation between the components of the system increase the possibility that a small incident can spread system-wide. The reason is that most systems are designed for general purpose operation and are not customized for the increased security required. Therefore, you should recognize that the electronic equipment and the systems you own can be within the scope of the Framework, and you should take the necessary security measures for each of them.
The reader should make use of the Framework and implement necessary security measures according to the actual requirements of the enterprise etc. to which the reader belongs.

4. Intended readers of the Framework

The Framework should be referenced when working on a value creation process in the new industrial society, Society 5.0. The stakeholders should all be aware of and involved with security measures necessary for that activity. Stakeholders include the following.

- CISO(Chief Information Security Officer)
- Strategists and planners for supply chain creation and management teams (mostly Part I)

- Person in charge of security of the enterprises and groups involved in the value creation process
- Person in charge of development/quality assurance/design/construction of information systems and control systems
- Person in charge of data management
- Person in charge of standardization of security guideline for industrial associations

5. Overall structure of the Framework

In order to accurately identify the risk sources in terms of cybersecurity in the value creation process and show the measures for the risks, we METI decided that the three parts composed the entire framework as follows.

(1) Part I explains the Concept of the Framework , the followings are specified:
   - the model (the three-layer and the six elements) to identify the risk sources in terms of cybersecurity in the value creation process
   - an outline of the risks and risk sources
   - approaching the risks to ensure trustworthiness.

(2) Part II uses the model shown in Part I to identify the risk sources and presents measure requirements for these risk sources. This part clarifies measure requirements (Policy) that each company or organization should take.

(3) Part III organizes measure requirements shown in Part II according to a kind of measure. In addition, examples of the security measures classified based on the relative strength of security are presented in Appendix C. This part shows the specific Methods that each company or organization should acutually take.

The above three part structure is also suitable for timely and appropriate review of necessary revisions. In other words, Part II will be updated in order to take more new risk sources on the progress of integration between cyberspace and physical space. Part III will be updated in order to take up more valid measure instance by the progress of the security measure

technology.
In this way, by using the three part structure, the Framework can be updated with any changes continuously and flexibly.

6. Expected effects and features of the Framework

The Framework was designed with expectations on the following effects and characteristics.

(1) Expected effects in each enterprise utilizing the Framework

- Ensuring trustworthiness in the value creation process by implementing security measures
- Strengthening of competitiveness by enhancing the security quality of products and services into differentiation factors (value)

(2) Features of the Framework

i. It can be used to create and operate security measures for each enterprise

- The Framework shall allow enterprises to confirm the policy and have an actual implementation of the security measures (Part II and Part III), in addition to defining goals for security measures in the industrial society (Part I).

ii. It presents the necessity of security measures, and examples of measures that are appropriate for costs and risks

- It will identify the relation between the expected risk sources and countermeasures, and allow understanding of the costs so that the enterprises (including small- and medium-sized enterprises) which are building a value creation process can actually implement the measures.
- It allows us to devise ways to reduce cost while maintaining an appropriate level of security by deriving security measures from the risk source (risk-based thinking), and allowing enterprises to select the right measures for their circumstances.

iii. **Contribute to international harmonization**

- In order to ensure that the security measures in Japan for products and services are accepted by other countries in the global supply chains, Japanese policymakers and companies should understand trends in foreign nations and include contents that will ensure consistency with major standards in the United States and Europe, including international standards (e.g., ISO/IEC 27001) and the NIST Cybersecurity Framework, and promote mutual recognition with the certification systems of each country based on these standards.
- In the Framework, there are correspondence tables between the Framework and other standards. An enterprise which uses the correspondence tables can make sure that it satisfies security requirements of the other standards. A foreign enterprise can show its sufficient security treatment based on the other standards through the tables.

7. How to use the Framework

The Framework is intended to be referred to when an entity, who is working on creating added value in the new industrial society, "Society5.0," takes security measures necessary for that activity.

On the other hand, in each respective industry allowable risks are different, depending on industrial structure or business practice. The material assets which should be protected are influenced by industry, enterprise, human/financial resources, and allowable risks. Security requirements should be based on on the characteristics of each industrial sector.

(1) Identifying the risk sources [Part II, Appendix A, Appendix B]

By referring to the three-layer approach shown in the Framework, a model can be developed for the creation of added value for each enterprise based on trustworthiness. Necessary characteristics and functions are noted in each layer of the three-layer approach. Specific examples of equipment are presented in Part II. Appendix A shows a typical case of use in each industry. In addition, the risk source of each enterprise can be identified by referencing the security incidents, threats, and vulnerabilities translated into the six elements, which are organized in Part II and Appendix B.

Through these materials, it is expected that new risk sources will be identified regarding the following points by comparing with the conventional perspective of risk assessment.

i. **Relation of multi-stakeholders who surround each organization involved in the value creation process**
ii. **Integration of cyberspace and physical space through IoT devices**
iii. **Cross-organizational data exchange**
iv. **Securing the basis of trustworthiness of each layer**

(2) **Formulating security policy and implementing measures in each enterprise [Part III, Appendix C]**

Security policy for the organization can be formulated, and security measures can be implemented with reference to security requirements and examples of measures shown in Part III and Appendix C. Part III presents security measures organized in consideration of the concept of NIST cybersecurity frameworks. Appendix C gives examples of security measures that would satisfy each of the security requirements.
It is expected that these materials will help each of the enterprise's efforts, especially on the following points.

i. **Implementation of measures that take into account the level of measures to be implemented and costs in each organization**
ii. **Comparisons with relevant international standards**

(3) **Building a trustworthy chain among each enterprise and industry**

Trustworthiness of each value cration process can be ensured by identifying the risk and implementing security measures based on the Framework. Building up such efforts will build a trustworthy chain. To be specific, these efforts are expected to result in the following.

i. **Creating a list for trustworthiness (detailed definition is described in Part I: 4.(2).**
ii. **Authenticating organizations and equipment**

Part I (Concept): Industrial cybersecurity for connected cyber and physical systems

1. Efforts for "value creation process," a "Society5.0" supply chain in an industrial society where cyberspace and physical space are highly integrated

In the "Society5.0" and "Connected Industries" programs, the increased connectivity, data creation by IoT devices, and data analysis using AI, will result in very different supply chain and value creation models from today's practices.

In the Framework, a Society5.0 supply chain is defined as a "value creation process" to distinguish it from the conventional supply chain. The Framework provides a guide for security measures required by Society5.0 and Connected Industries extended supply chain models.

In conventional supply chain models, security measures are based on the idea that security of the entire process is ensured by business dealings with entities who used proper security—in other words, the conventional idea that trustworthiness of the supply chain is ensured if the organizational governance and management of the participating entities is secure and reliable. When a company entrusts its information processing work to other company, security measures such as obtaining ISMS certification were important. The basis for ensuring security was based on the trustworthiness of the organization's management.

However, in the value creation process, where cyberspace and physical space are highly integrated, trustworthiness of the process cannot be assured simply by the trustworthiness of the participating organizations' management.

For example, in an integrated cyberspace and physical space, various information such as environmental information (e.g., temperature, humidity) and biological information (e.g., body temperature, heart rate) that once would have been kept in physical space can be digitized and stored in large quantities in cyberspace. Also unlike the conventional supply chain, trusted entities are not the only ones involved with this process. To ensure trustworthiness of the entire process, there is a limit to the approach of ensuring trustworthiness of the participants.

In order to promote security and ensure trustworthiness in the value creation

process, a different approach is required, one which adopts alternate points of view to ensure security across all the supply chain participants.

Part I shows a model with the points of the value creation process that need security assurance, and describes policies to deal with risk sources in each of its elements.

2. Model for establishing the basis for trustworthiness to ensure security in the value creation process: The three-layer and the six elements

The security of physical data produced by IoT devices – and its digitization, transport, storage, and analysis – is very different from interactions between two trusted entities in a conventional supply chain. Often this IoT data is used to generate new data through automated analysis. Data is also used to create physical products and services in physical space by controlling physical IoT devices. All these interactions and more must be secured and controlled by value creation process participants.

In order to accurately identify the sources of security risks in activities that extend the conventional supply chain, the value creation process is organized into three layers, as follows:

The first layer – Connections between organizations
The second layer – Mutual connections between cyberspace and physical space
The third layer – Connections in cyberspace

Also, in order to implement measures against such risk sources at the operational level, it is necessary to identify elements with risk sources, and it is necessary to extract vulnerabilities and risk sources from this three-layer model.

On the other hand, because the value creation process would be built dynamically and flexibly, essential protection measures could be missed by simply addressing risks on business assets. Elements of the value creation should be abstracted to a certain extent, so security measures can respond to changing threats dynamically.

In the Framework, these elements are organized into the following categories:

each detailed definitions are described in 2.2.

- Organization[3]
- People
- Components
- Data
- Procedure
- System

The basic structure of the Framework is to identify the risk source of the value creation process based on the three layers, present security measures for each risk source based on the six elements, and present specific examples of the measures.

[3] In order to distinguish it from "organization" of general usage, when using the term "organization" as a unique meaning in this paper, " " is attached.

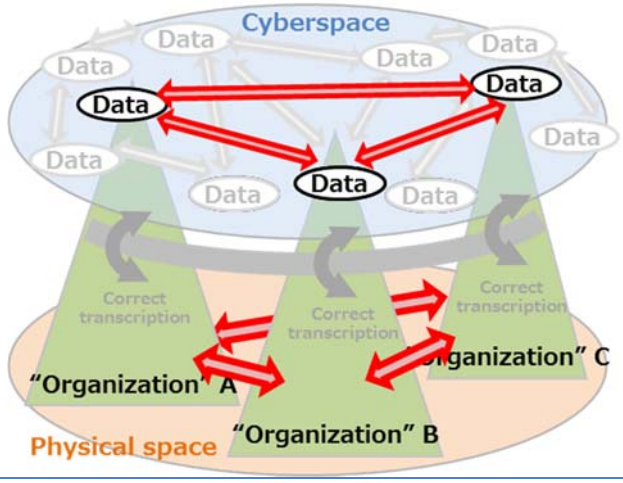
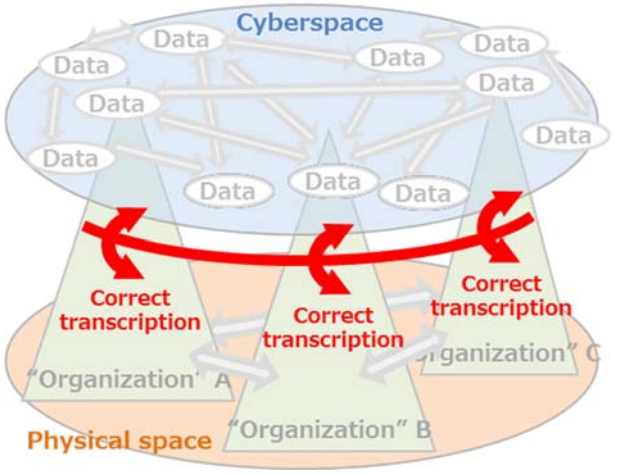
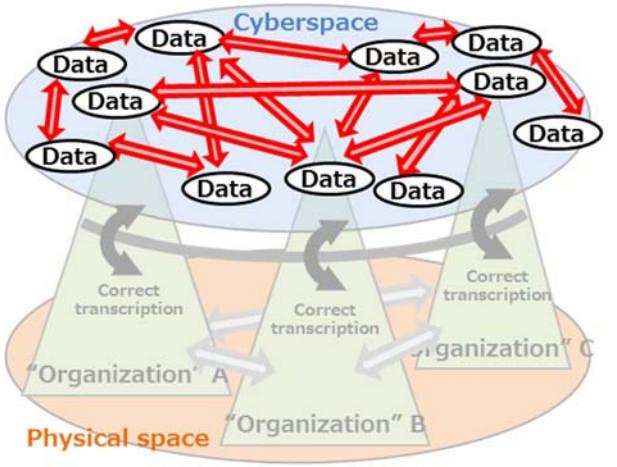
Three-layers	Conceptual diagram
The First Layer **(Connections between organizations)**	
The Second Layer **(Mutual connections between cyberspace and physical space)**	
The Third Layer **(Connections in cyberspace)**	

Figure 1.2-1 Three layers of the industrial society where value creation processes unwind

2.1. Significance of the three-layer approach

As already mentioned, it is no longer sufficient to ensure trust of the value creation process by ensuring trustworthiness of an organization's management. In order to deal with new risks in the value creation process, it is necessary to introduce additional requirements for trustworthiness. The three-layer approach described in this section is the Framework approach of ensuring trustworthiness. Trustworthiness to be verified in each layer is explained below.

The First Layer — Connections between organizations

The first layer aims for a level that ensures trustworthiness in the organization's management.
This idea has been adopted to achieve security in the supply chain. It is based on the idea that by confirming the trustworthiness of the enterprise's management and allowing only participants whose trustworthiness is established, security can be ensured.
Certification programs such as ISMS (based on ISO/IEC 27001) center on ensuring trustworthiness in the company's management, division management, and headquarters' management, and provide a mechanism that leads to connections between companies with confirmed trustworthiness to ensure security in the supply chain. Using this approach, security policies are shared, and the trustworthiness of management is confirmed and certified.
In summary, the first layer aims for a level that organizational management with shared security policy is certified as a basis for ensuring trust.
However, in an industrial society where cyberspace and physical space are integrated, it is impossible to ensure trust in the entire value creation process by only confirming the trustworthiness of the organization's management. In the second layer and the third layer of the model, there are introduction of further types of trustworthiness to ensure trustworthiness of the whole value creation process.

The Second Layer — Mutual connections between cyberspace and physical space

In an industrial society where cyberspace and physical space are highly

integrated, physical data can be digitized, delivered to cyberspace, processed and edited, analyzed, and returned to physical space. IoT seeks to connect everything to the network, and create borders between cyberspace and physical space. Connections between cyber and physical space are found in many industrial and social activities.

On the other hand, unreliable interactions between cyberspace and physical space could cause uncertainty in the entire industrial society. The value creation process expands over the border of cyberspace and physical space. Its trustworthiness cannot be ensured if accuracy of transcripted information over the border cannot also be ensured.

The value creation process goes beyond the border between of the cyberspace and the physical space. The interaction between the cyberspace and the physical space, that is, the data exchange between both spaces, is required to have high accuracy. In other words, the trustworthiness of the value creation process is not ensured unless the accuracy of transcription and translation is confirmed.

The second layer is based on the accuracy and trustworthiness of data transcription and transfer (including accurate translation) between cyberspace and physical space.

The actual border of cyberspace and physical space is established by the so-called IoT system, which is made up of elements such as sensors that transfers physical events (e.g., temperature, humidity and distance) to data, actuators and controllers. The security of the systems that transfer data on the border of cyberspace and physical space cannot be ensured by confirming the trustworthiness of the organization's management.

To ensure trustworthiness in transcription, in accordance with ISO/IEC 27036, all the elements of the system lifecycle, including construction and maintenance, must also be trustworthy.

Another point to be understood is that existing systems will be incorporated into the new frontier between cyberspace and physical space. It is important to reevaluate the systems' security and take measures to ensure security of transcription functions.

The Third Layer — Connections in cyberspace

As the quantity of data drastically increases in industrial society, the creation

of new value in cyberspace through exchange, analysis, and editing has become commonplace.

Trustworthiness of the data transcribed from physical space to cyberspace is guaranteed by ensuring trustworthiness of the transcription function in the second layer. However, it should be noted that data is created, edited, processed, and freely exchanged in cyberspace outside the second layer process as well, and not only by organizations with confirmed trustworthiness. Many entities may use and modify a data set, but the original data is the foundation for creation of value in cyberspace.

In cyberspace, to ensure trustworthiness in the value creation process and to create value as intended, the data itself must be trusted. Therefore, in the third layer, data integrity is the basis of trustworthiness. Data falsification and data breach during the distribution and storage of data will cause loss of trust for the entire value creation process. For that reason, security measures need to be implemented in the third layer for data distribution and storage, as well as for appropriate editing and processing.

In the value creation process in an industrial society where cyberspace and physical space are highly integrated, security measures from all three layers are required. Risk sources will be identified from the three-layer model and measures can be presented for each layer of the value creation process that create the foundations of trust.

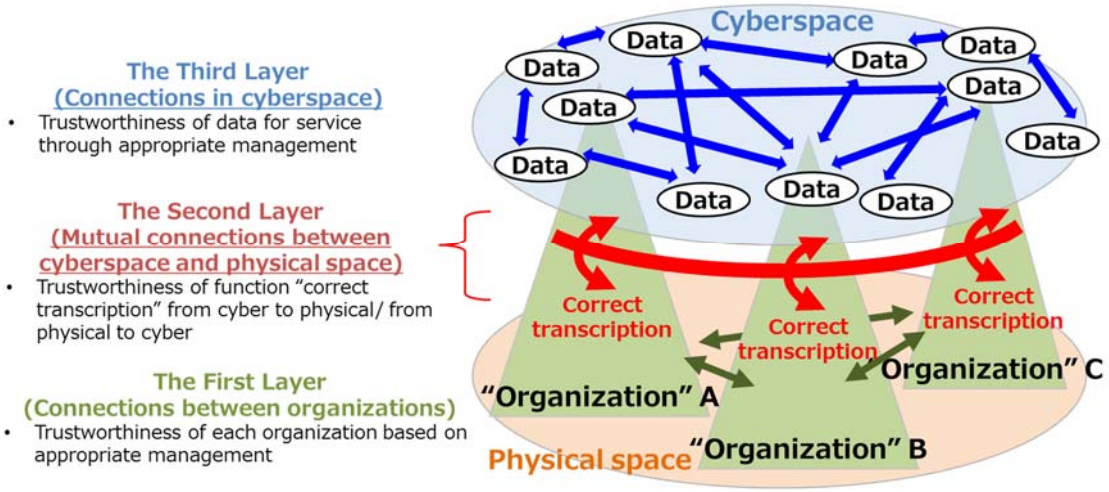


Figure 1.2-2 Significance of the three-layer model

2.2. The six elements

Through the three-layer model, it is necessary to identify the impact of the threat on the elements that make up the value creation process, and to identify the risk sources. The elements which make up the value creation process must be organized to establish a policy for security measures and to build specific measures.

In this point, it is necessary to understand that elements of the value creation process should be abstracted because the value creation process is organized dynamically and flexibly and it is difficult to grasp business assets fixedly.

Table 1.2-1 Six elements involved in the value creation process

Element	Definition
“Organization”	Companies, groups and organizations that compose value creation processes
People	People belonging to organizations. People directly participating into value creation process
Components	Hardware, software and parts including operating devices
Data	Information collected in physical space. Edited information through sharing, analyzing and simulating above information
Procedure	Sequences of activities to achieve defined purpose
System	Mechanisms or infrastructures configured with components for defined purpose

The six elements are established to extract factors from the value creation process and components of organizations based on the idea of quality control “4M (Man, Machine, Material and Method)”. As Figure 1.2-3 shows, organizations provide added values and outputs, as well as waste, through inputs (material, information, and so on) from other entities. Also, there are people, physical machines, IT/OT systems, and procedures like standards included in the value creation process. Each element is produced from outputs of other organizations as well. The six elements are related to each other in complex ways. For example, an IT system is an output from a value creation process composed of computer suppliers, system integrators, etc.

In an example of a value creation process of the manufacturing industry, the relationship of six elements and three layers is shown in Figure 1.2-4. The company "organization" on the left inputs "components", processes them, and

outputs “components". The company "organization" on the right inputs "components" output by the company "organization" on the left, adds processing, and outputs "components" of its own. Within each company "organization", there are "components" such as processing machines, sensors and actuators, “systems” such as systems to exchange data with other organizations, “people” such as people who monitor and control the systems, "procedures" such as procedures to establish each system activity, and “data” such as various types of data flowing between the systems.

These are the elements which each organization manages and they make up the first layer for each of companies. Within the elements of the first layer, sensors and actuators transcribing between cyber space and physical space, systems controlling them, and related procedures and data are organized as the elements of the second layer. Between two organizations, the data exchanged via the Internet and the related systems, procedures, and data are organized as the elements of the third layer that connects in cyberspace.

These six elements do not have an exclusive relationship to each other. For example, “organization” is formed of other elements such as "people", "system", "procedure", but "organization" also has the meaning of the original element in the value creation process. “People” is not only an element contained in "organization", but also the element participating in a value creation process directly. The trustworthiness of the value creation process is secured by taking a security measure for the risk sources of six elements in the value creation process, and in that way the trustworthiness of created hardware, software, and services is ultimately secured.

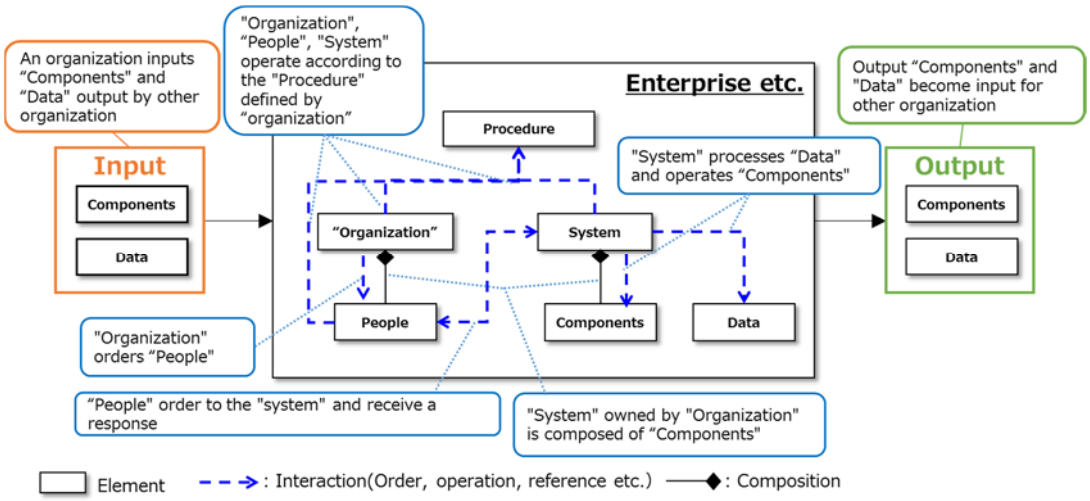


Figure 1.2-3 Relationship of six elements

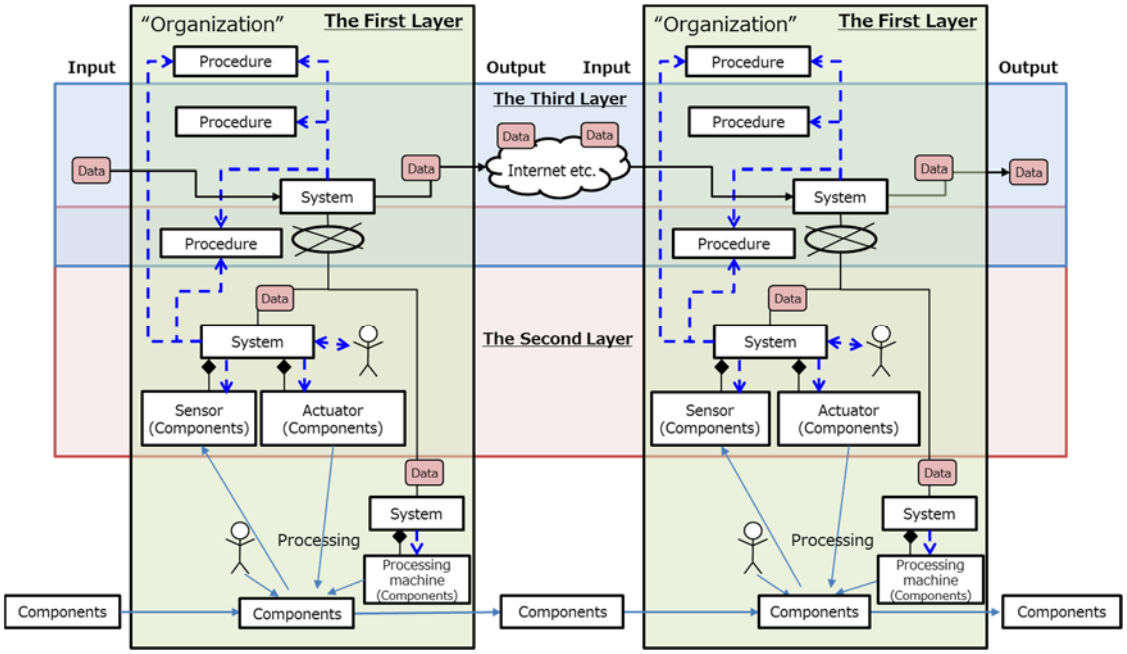


Figure 1.2-4 Relationship of six elements in the three-layer model

3. Identifying the risk sources in the value creation process and its policy

The risk sources in the value creation process will be identified and associated policies will be developed in Part II based on the three-layer model and the six elements. Part I especially shows that new risk sources appeared in the value creation process, which are different from conventional supply chains.

In the first layer, management by the enterprise is the basis of trustworthiness, and security measures are implemented based on the management of each enterprise. However, as already mentioned, security measures need to be taken in the second layer and the third layer for the value creation process that spans both cyber and physical spaces.

The important point in security measures for the second layer is to ensure correct transcription on the border of cyberspace and physical space. To ensure trustworthiness of the transcription, any organization which is directly or indirectly involved in the value creation process must cooperate.

This means that even organizations not directly involved in the value creation process are required to participate in implementing security measures. A multi-stakeholder approach is required.

For example, when an enterprise indirectly involved in a value creation process provides secured products and services to a directly involved

enterprise, the trustworthiness of the transcription, which is the basis of trustworthiness in the second layer, is ensured.

In addition, in the third layer, organizations participating in the value creation process will use various data in cyberspace. Security of the process is built on the premises that the data is handled appropriately and trustworthiness is ensured.

Here also, although not directly involved in the value creation process, an entity indirectly involved in distributing or handling the data is required to play a vital role in ensuring security. Efforts on security measures using a multi-stakeholder approach are necessary.

As an example, for a given data set, the same security measures must be taken by all participants who handle the data. Security measures for the data set from the first layer and the second layer will be based on the specific measure in the third layer which ensures data trustworthiness.

The risk sources are viewed differently in each layer, and the policy for managing risks also differs.

Taking these into account, the Framework will define and organize areas to be protected and risk sources in each layer, as well as measures that will be taken based on individual policies as shown in Figure 1.3-1.

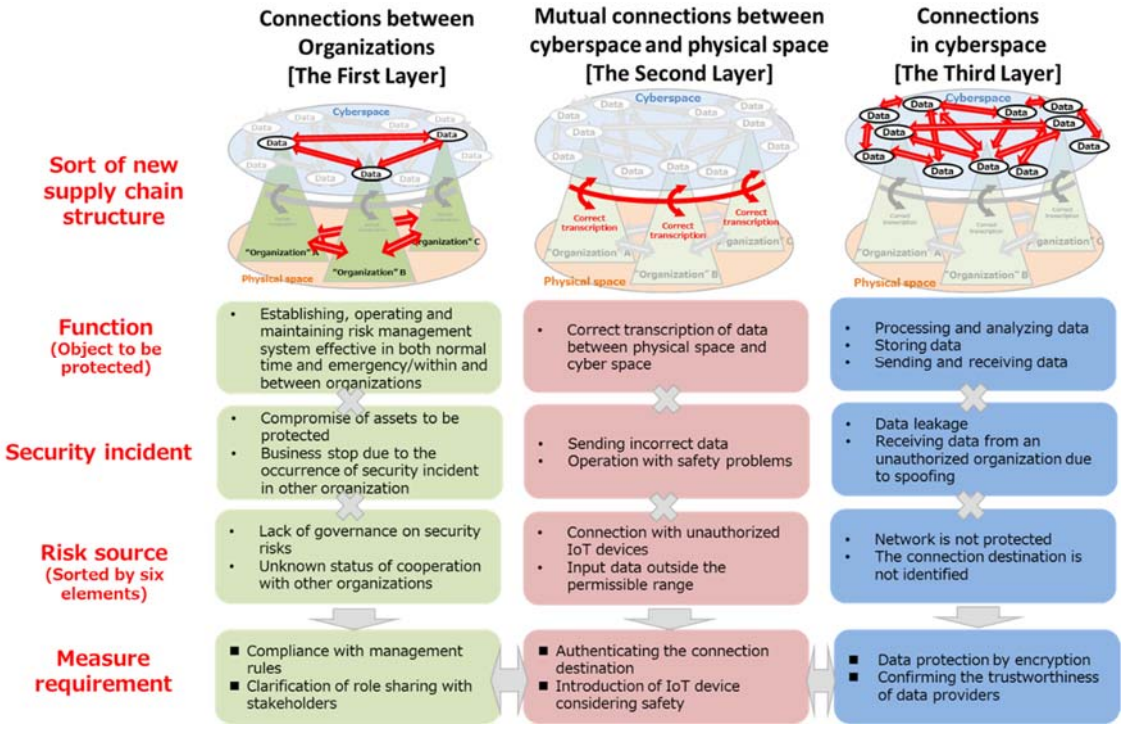


Figure 1.3-1 Overview of the measures in each layer

4. Concepts of securing trustworthiness based on the Framework

The security of the entire value creation process is ensured by each entity securing the security of each element that are the basis of trustworthiness based on the three layers. In order to do so, it is necessary to confirm each element's security requirements satisfied (creation of trust), be inquired by other subject except the subject of confirmation (proof of trust), structure and maintain a chain of trustworthiness relationships (trustworthy chain) built up in a chain by repeating creation and proof of trust (see Figure 1.4-2). Examples of matters that are required to achieve creation of trust, proof of trust and structuring and maintaining of trustworthy chain, are shown below.

(1) Creation of Trust

Examples)

- To create components/data that satisfy the security requirements.
- To preserve the above records.
- Self-confirmation of those components/data being created with security requirements satisfied.
- Third party certification of those components/data having been created with requirements satisfied.

(2) Proof of Trust

Examples)

- To create and manage a list (the list for trustworthiness) that can be inquired by the third parties other than the production subject that the target components/data are properly created in a form that satisfy security requirements; The list structure does not matter whether it is an integrated ledger or a distributed ledger (such as blockchain, etc).
- To confirm trustworthiness of the target components/data by inquiring to the list for trustworthiness.

(3) Structuring and Maintaining of Trustworthy chain

Examples)

- Structuring of trustworthy chain through repeated creation and certification for trustworthiness (each chain element's trustworthiness being confirmed between other elements, and thereby securing traceability).

- Detection of/protection against external attacks to the trustworthy chain.
- Improvement of resilience against attacks.

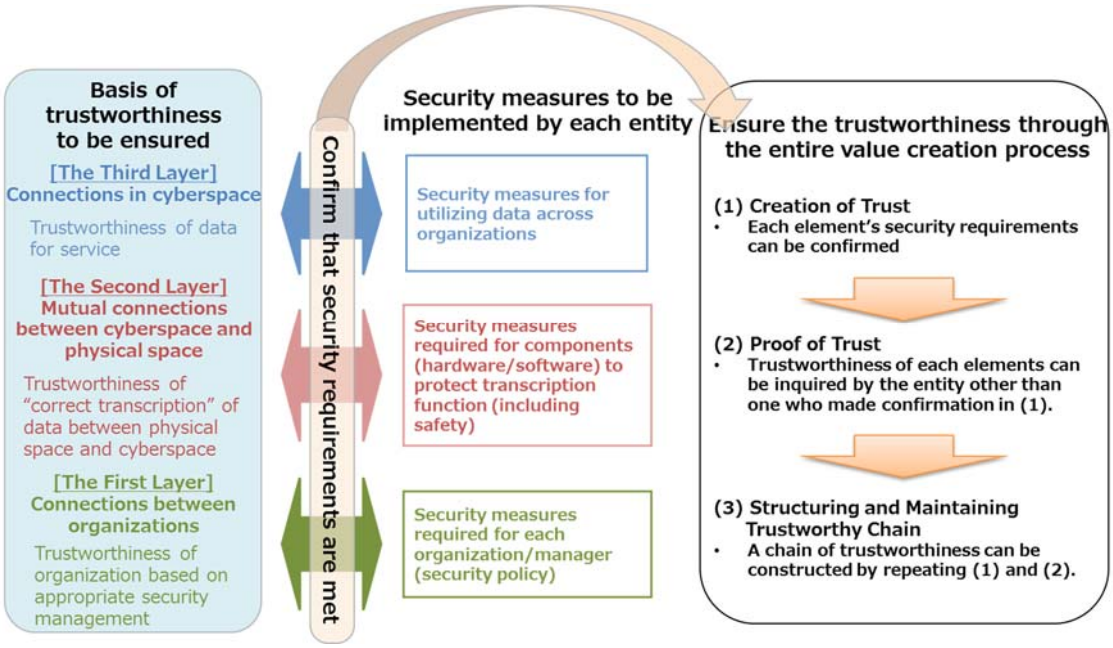


Figure 1.4-1 Concept of basis of trustworthiness

The value creation process is dynamic and flexible. An approach that will ensure security in a multilayered manner is required, such that it will ensure trustworthiness through the entire value creation process by structuring a trustworthy chain that can be traced and confirmed to its relationship, not just verifying trustworthiness of each element.

However, building a value creation chain requires many technical and system-related tasks, and requires the ongoing cooperation of public and private sectors. The technical and system-related preparations must include cybersecurity requirements, and they are described in Part II. Part II should be improved in the case that new technologies and/or rules would be introduced.

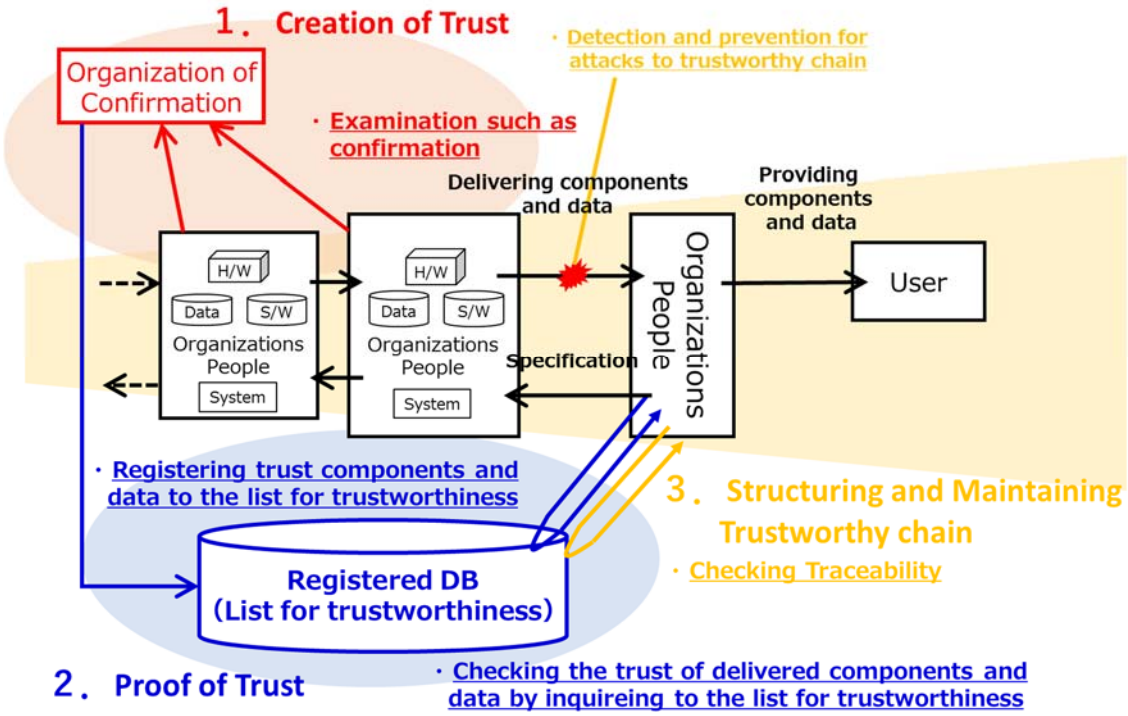


Figure. 1.4-2 Illustration of the relationship among Creation of Trust, Proof of Trust and Structuring and Maintaining of Trustworthy chain

5. Conclusion

The Framework presents security measures common among all industries of the value creation process in a proposed industrial society, "Society5.0," where cyberspace and physical space are highly integrated. However, there are wide difference of practices and variations of allowable risks between industries, and even between companies within an industry. Security measures must take these variations into account.

Therefore, in each industry and each enterprise, please use the Framework in order to adopt appropriate security measures internally.

Moreover, please use the Framework to identify gaps between existing security measures and best practices.

Part II (Policy): Identification of risk sources and measure requirements

In Part II, the risk sources for the Society 5.0 value creation process will be presented. Risks are organized based on the three-layer model that forms the basis of trustworthiness. Security measure requirements are also presented.

1. How to proceed with risk management that considers three-layer model and six elements

Entities involved in the value creation process can utilize the Framework by using the standard risk management process adopted in ISO 31000:2018 and ISO/IEC 27001:2013. The contents of Part II can be utilized in the risk management process, especially when scope, context, criteria, assessing risks, and treating the risks.

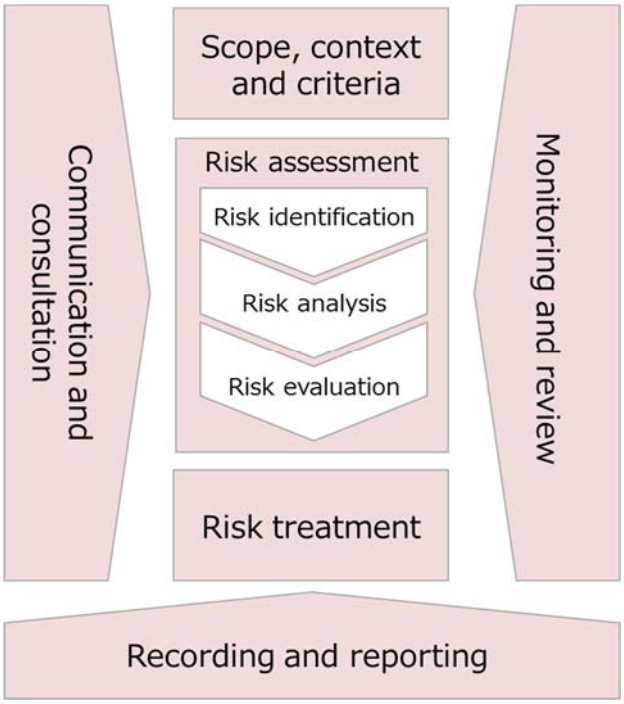


Figure 2.1-1 Typical risk management process[4]

The followings steps are followed when scope, context, criteria, establishing the contexts, assessing risks, and treating the risks.

[4] Created based on ISO 31000:2018 Risk management—Principles and guidelines

■ **Scope, context and criteria**

i. **Specifying the target of analysis (1.1)**

The value creation process targeted for analysis is specified based on the three-layer model, and elements in each layer are identified by implementing this step.

ii. Defining assumed security incident and business damage level **(1.2)**

Security incidents which have high impact on the organization's business are identified, and the business damage level is defined

■ **Risk assessment [Risk identification/Risk analysis/Risk evaluation]**

iii. **Analyzing risks (1.3)**

Potential attack scenarios for the security incidents defined in ii. will be studied, and risks are analyzed in terms of threats and vulnerabilities.

■ **Risk treatment**

iv. **Managing risks (1.4)**

Risks are addressed based on the risk analysis results.

Figure 2.1-2 Flow of risk management[5]

[5] Created with reference to "Security Risk Assessment Guide for Industrial Control Systems 2nd Edition" published by IPA

When implementing security risk management, it is necessary to understand the concept of security risks shown in Figure 2.1-3. Here, risk is defined as "the effect of uncertainty on objectives", and security risk means the effect of uncertainty regarding security on objectives. A security incident occurs due to risk sources such as threats and vulnerabilities, and then security risks become apparent. Therefore, in order to reduce security risks appropriately and efficiently, it is necessary to appropriately analyze and treat security incidents to be avoided and risk sources (for example, threats and vulnerabilities) that may lead to security incidents.

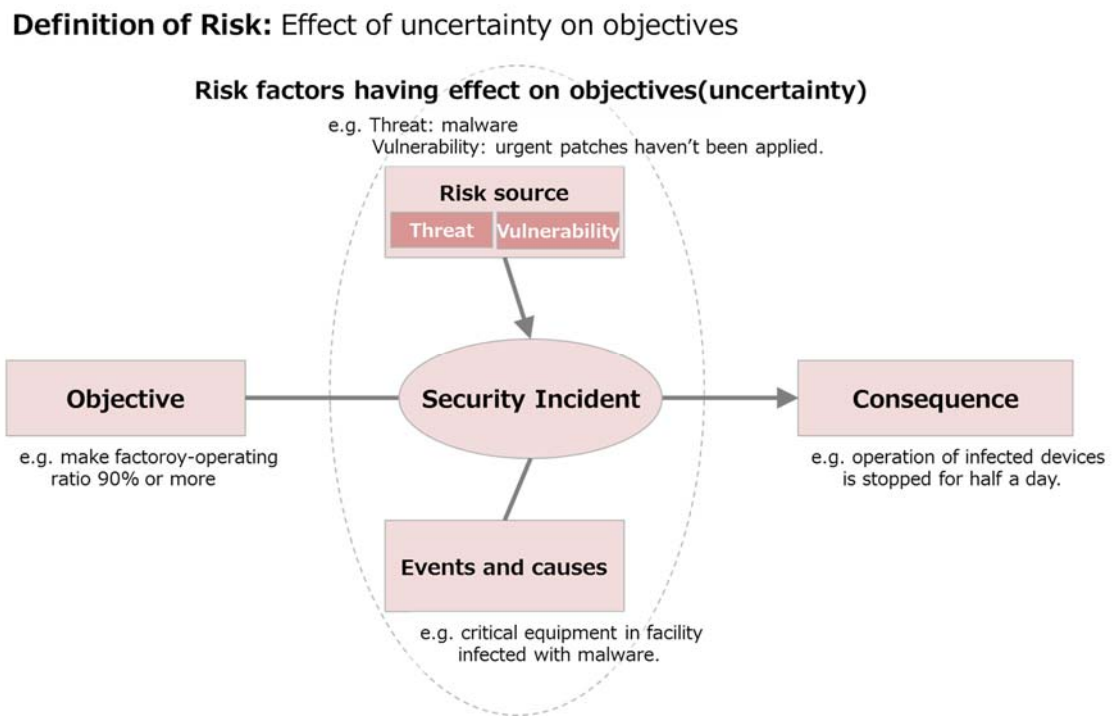


Figure 2.1-3 Concept of security risk

In particular, in order to properly assess the security risks in "Society5.0" and implement effective treatment, the following four points should be taken into consideration through the process shown in this part. These points will be described in detail in 1.1.(2).

i. Relation of multi-stakeholders who surround each organization involved in the value creation process
ii. Integration of cyberspace and physical space through IoT devices

iii. Cross-organizational data exchange
iv. Securing the basis of trustworthiness of each layer

In the following, the implementation of the security risk management will be explained in order, in consideration of the above view points.

1.1. Specifying the target of analysis (applying to the three-layer model)

The identification of the target of analysis for risk assessment will be described in the following, in the order of (1) implementation process and (2) points to note on the implementation.

(1) Process for identifying the target of analysis based on the three-layer model

The target of analysis must first be identified when assessing risks. "Security Risk Assessment Guide for Industrial Control Systems 2nd Edition" (published by IPA[6]) prescribes the following for the identification of the target of analysis.

- Deciding the scope of analysis and identifying the assets
- Identifying the system configuration
- Identifying the data flow

In an industrial society where cyberspace and physical space are integrated outside the organization, identifying the assets and the scope of analysis is expected to become more difficult. In order to implement the three items above, it is important to identify the stakeholders of the value creation process in which the enterprise is involved, and to grasp the flows of the items and data in both the cyberspace and physical space. The Framework provides guidance to identify the target of analysis based on the three-layer model presented in Part I. The enterprise can determine the scope of analysis by utilizing the method in this section and then identifying the system configuration and the data flow within the scope previously defined so that understanding for the object of the risk management can be

[6] Information-Technology Promotion Agency, Japan

detailed[7].

In order to identify the target of analysis for assessing risks, characteristics, and functions/roles of each layer should be understood. (See Tables 2.1-1, 2.1-2, 2.1-3) The scope of analysis and assets will be organized based on the approach of accounting for these these functions/roles, and focusing on the functions performed by each system.

All components to be managed in the enterprise etc. are included in the first layer. Among them, those having functions of the second layer or/and the third layer are analyzed as components related to the second layer or/and the third layer. Note that some components have functions of both the second layer and the third layer depending on the characteristics of the system. At the same time, in implementing the risk assessment, it is appropriate to pay attention to the "zone" where components and systems are set, and instances where people are required to follow certain procedures.

When using a cloud service, the resources provided by the service provider via the network are located in the third layer, but in risk analysis you also need to consider them as assets in the first layer if necessary, keeping in mind the service usage form (e.g., SaaS / PaaS / IaaS).

[7] When carrying out "identifying the system configuration" and "identifying the data flow", it is desirable to refer Section 3.2, 3.3 in "Security Risk Assessment Guide for Industrial Control Systems 2nd Edition" published by IPA.

Table 2.1-1 Characteristics, functions/roles, targets of analysis and concrete image of analysis targets in the first layer

Characteristics	Functions/roles	Targets of analysis	Concrete image of analysis targets
The First Layer (Connections between organizations)			
Maintain trustworthiness through appropriate governance and management of individual organizations Individual organizations maintain trustworthiness through appropriate business collaboration	• Establishing the organizational risk management system effective in normal times and appropriately operating it • Continuing the business of the organization appropriately even when a security incident occurs • Products or services in physical space are received or shipped with desired quality **[Security requirement]** **Defining and maintaining the security policy of the organization** **[Basis of trustworthiness]** **Organizational risk management**	• "Organization", people, components, data, procedure, system managed by organization etc • Zone where the above elements are managed • Data exchange within the organization	• Employees • Corporate IT assets • Corporate security policy • Contract between companies

Table 2.1-2 Characteristics, functions/roles, targets of analysis and concrete image of analysis targets in the second layer

Characteristics	Functions/roles	Targets of analysis	Concrete image of analysis targets
The Second Layer (Mutual connections between cyberspace and physical space)			
Connection between physical space and cyberspace is strengthened through IoT devices Longer lifecycle devices connected to the network will increase (Located in a remote place etc.) Devices connected to the network and difficult to manage will increase Devices connected to the network are separated into various places (critical infrastructure to home) The number of devices that perform work in physical space based on the input from cyberspace increases	• Reading events in physical space and translating them into digital data and sending the data to cyberspace in accordance with certain rules • Controlling components and displaying visualized data based on data received from cyberspace in accordance with certain rules **[Security requirement]** **Ensuring security in transcription between cyberspace and physical space** **[Basis of trustworthiness]** **Trustworthiness in the function to transcribe cyberspace and physical space correctly according to rules**	• "Organization", people related to transcription function • Components, system with the function of correctly transcripting cyberspace and physical space according to rules • Data related to transcription • Procedure related to transcription	• Actuator, sensor, controller, medical equipment, ECU, 3D printer, surveillance camera, personal computer (as input device), smart meter (as meter reading device) • Components related to the transcription that configures these devices etc.

Table 2.1-3 Characteristics, functions/roles, targets of analysis and concrete image of analysis targets in the third layer

Characteristics	Functions/roles	Targets of analysis	Concrete image of analysis targets
The Third Layer (Connections in cyber space)			
Collecting, storing, processing, and analyzing various and large amount of data across organizations in addition to the organization's data Data is collected from various end points across organizations and industries Various data including streaming data and confidential data etc. are collected Data collected from multiple data sources are processed for integrated analysis The organization's stored data including open data and confidential data etc. may be accessed from various end points across organizations and industries High-speed and technically advanced data processing is performed by using AI etc. in data processing / analysis The composition of the supply chain of data in cyberspace changes dynamically.	• Securely processing and analyzing data • Securely storing data • Securely sending and receiving data **[Security requirement]** **Ensuring security in data sending and receiving etc. in cyber space** **[Basis of trustworthiness]** **Data**	• "Organization", people dealing with data exchanging across organizations • Components, system sending and receiving, processing, analyzing, and storing data • Data to be exchanged across organizations • Common procedures for protecting data across organizations	• Server, router, smart meter (as a communication device for meter reading data) • Hardware and software (OS, middleware, applications, etc.) that configure systems, etc. • Open data • Data for Limited Provision • Data management policy etc.

For example, although a personal computer or a smart meter can be thought of as a component having both the function of the second layer and the third layer, it is desirable to assign the components to the second layer, the third layer or both layers considering the role of the device in the system to be analyzed.

It is desirable to create a document for the scope of analysis and assets identified based on the three-layer model and to be able to respond quickly when changes are made in the structure.

As a model simplifying the above arrangement, Figure 2.1-4 shows relationship of the target of analysis and assets in the first layer. In the first layer, these are organized regardless of the value creation process, and consider only the management of the organization that shares/implements its security policies.

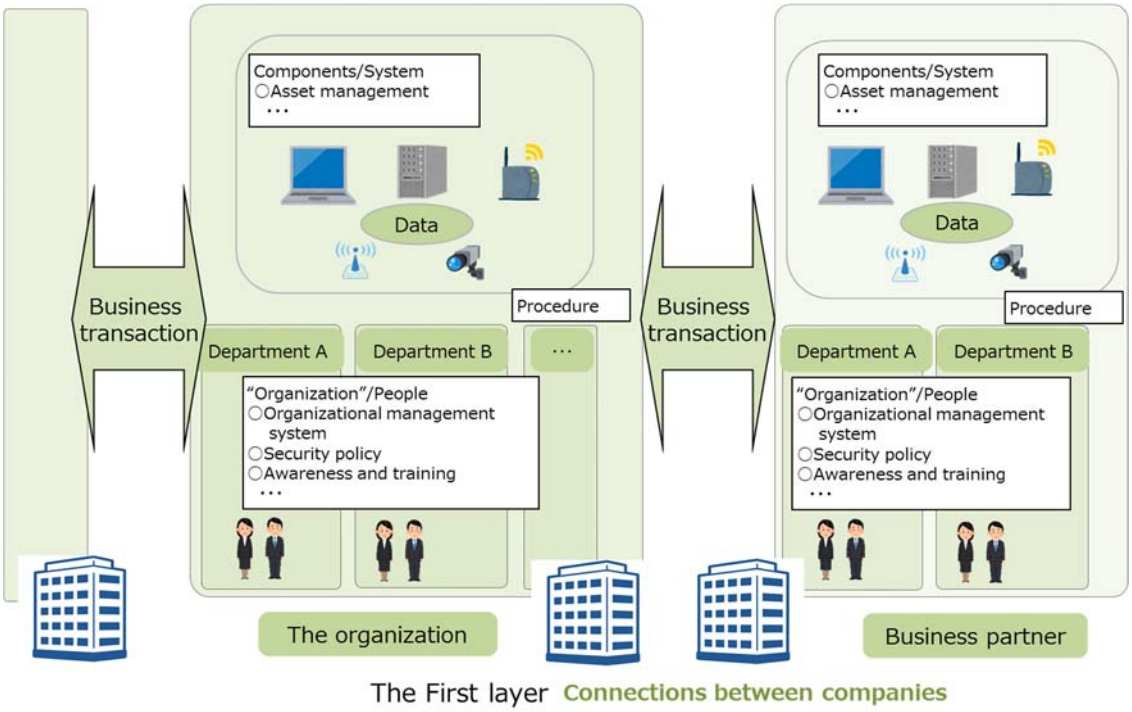


Figure 2.1-4 Targets of analysis and concrete image of analysis targets in the first layer

Next, Figure 2.1-5 shows the functions/roles and concrete image of analysis targets in the second layer and the third layer, and Figure 2.1-6 shows a concrete image of the analysis targets of the value creation process in which the analysis targets of the first layer are associated with the functions of the second layer and the third layer.

The organization's assets are positioned in the first layer. However, when the value creation process develops, not only the security policy of a single organization but the security of the functions of the second layer (transcription) and the third layer (data exchange etc.) as shown in Figure 2.1-5 should be ensured so that the trustworthiness is ensured.

It becomes possible to identify the elements related to the second layer and the third layer in one organization by associating the components arranged in the first layer with the functions of the second layer and the third layer. By using this method it is possible to set the basis of trustworthiness of each layer, and define what security measures should be taken with respect to each component.

Appendix A gives examples of use case of applying the model shown in Figure 2.1-6 in typical industrial fields. It is advisable for each organization to refer to them if necessary when identifying the target of analysis.

Regarding the specification of the detailed system configuration and data flow, the target of analysis is assumed to differ depending on industries and enterprises, and it is necessary that each implementing entity should identify the target of analysis.

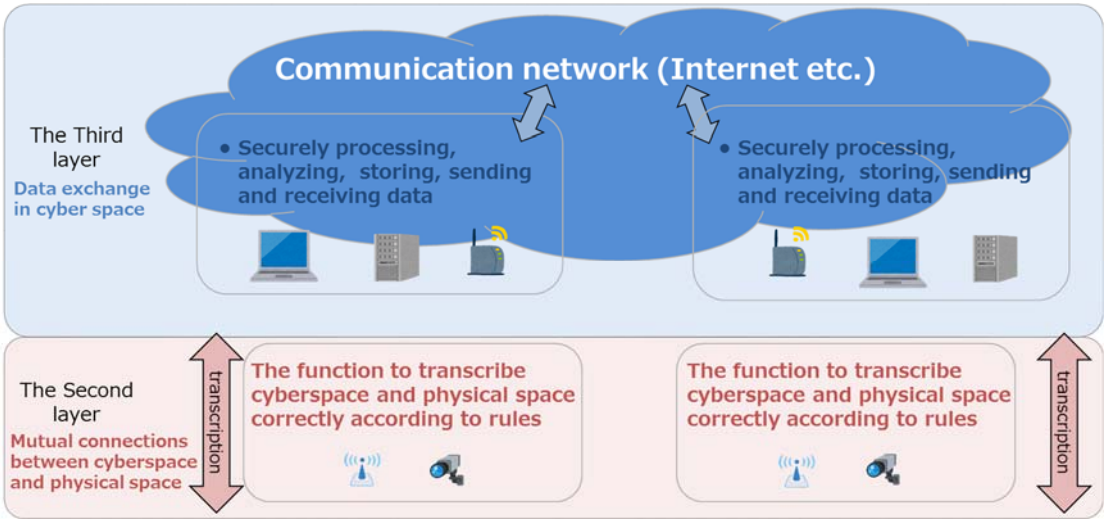


Figure 2.1-5 Functions/roles and concrete image of analysis targets in the second layer and the third layer

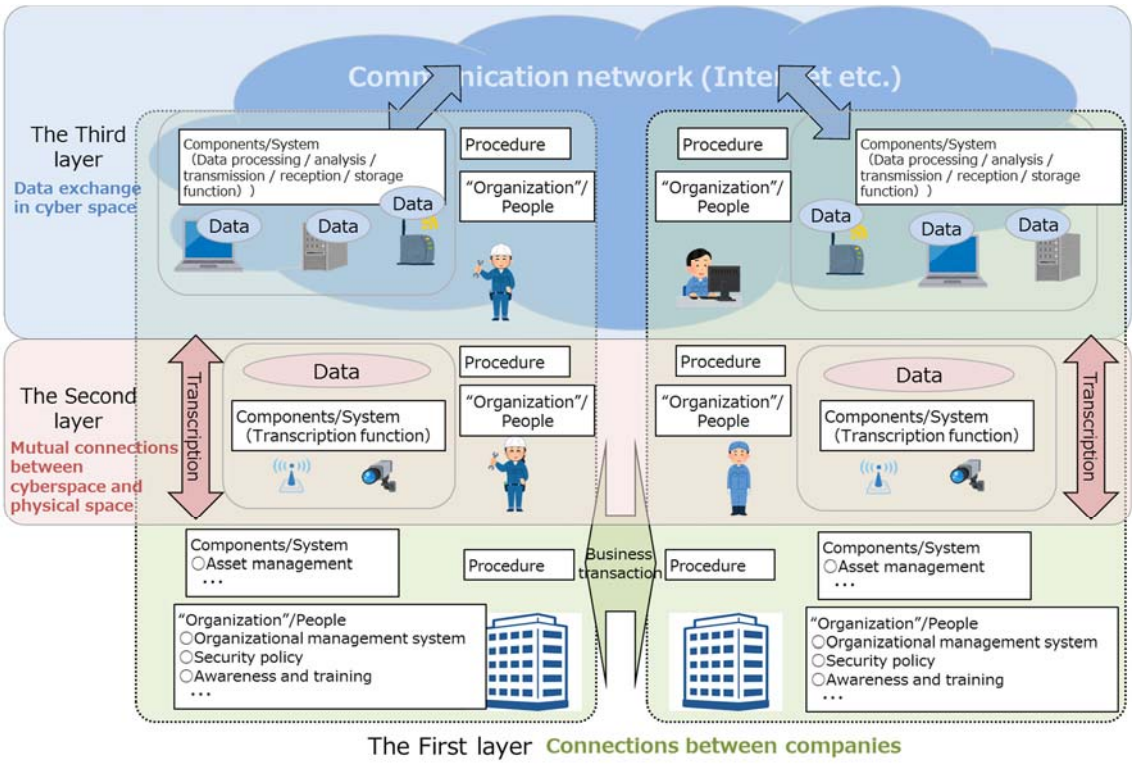


Figure 2.1-6 Concrete image of analysis targets based on the three-layer model and the six elements

(2) Points to note when identifying the target of analysis

When identifying the target of analysis based on the three-layer model, the entity implementing risk management needs to proceed with the operation while noting the following points for the purpose of ensuring the security of the entire value creation process.

i. Relation of multi-stakeholders who surround each organization involved in the value creation process

- As mentioned in Part I, in the second layer and the third layer, organizations not directly involved in the value creation process are required to participate in the security measures as an essential entity in implementing appropriate security measures. Efforts of multi-stakeholder approach are necessary.
- Therefore, using the three-layer approach, stakeholders involved in the value creation process need to be identified, and their role and importance in the organization's business need to be identified.

➢ "Organizations" related to the actions of the organization is identified in each of the three-layers. When doing so, service

providers who store, edit, and analyze the data in the third layer, IoT device venders, and suppliers of parts of products and services need to be identified. In addition, important business partners, including contractors and subcontractors, should also be identified.

ii. Integration of cyberspace and physical space through IoT devices

- On the border where cyberspace and physical space integrates, data in the physical space needs to be transcribed to data in cyberspace correctly. In such a case where the data in the physical space and the data in the physical space are not properly transcribed and the wrong data are provided to the cyberspace, trust of the data collected for analysis and that of the operation using such data will be lost.
- Therefore, it is necessary to identify properly the equipment (e.g., sensor) that measure the dynamics of the physical space and transmit data to cyberspace, and classify the equipment by the level of importance in the organization's operation.
- Opposite from the example above, on the border where cyberspace and physical space integrate, components in the physical space may be controlled based on the result of data analysis in the cyberspace. As a result, as shown in Figure 2.1-7 and 2.1-8, due to malfunction of components, security threats may lead to problems in safety such as physical harm to employees and damage to equipment.
- Therefore, when specifying the target of risk analysis, it is important to specify applicable equipment and items that may trigger incidents that could lead to safety issues as mentioned above using the results of risk analysis regarding safety and make them available for reference when implementing the risk analysis.

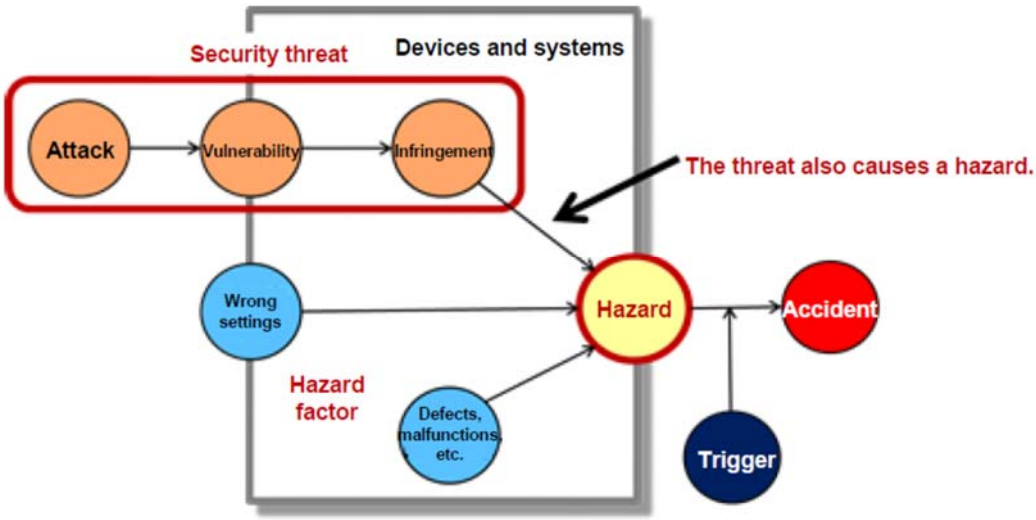


Figure 2.1-7 Model of security problems affecting safety[8]

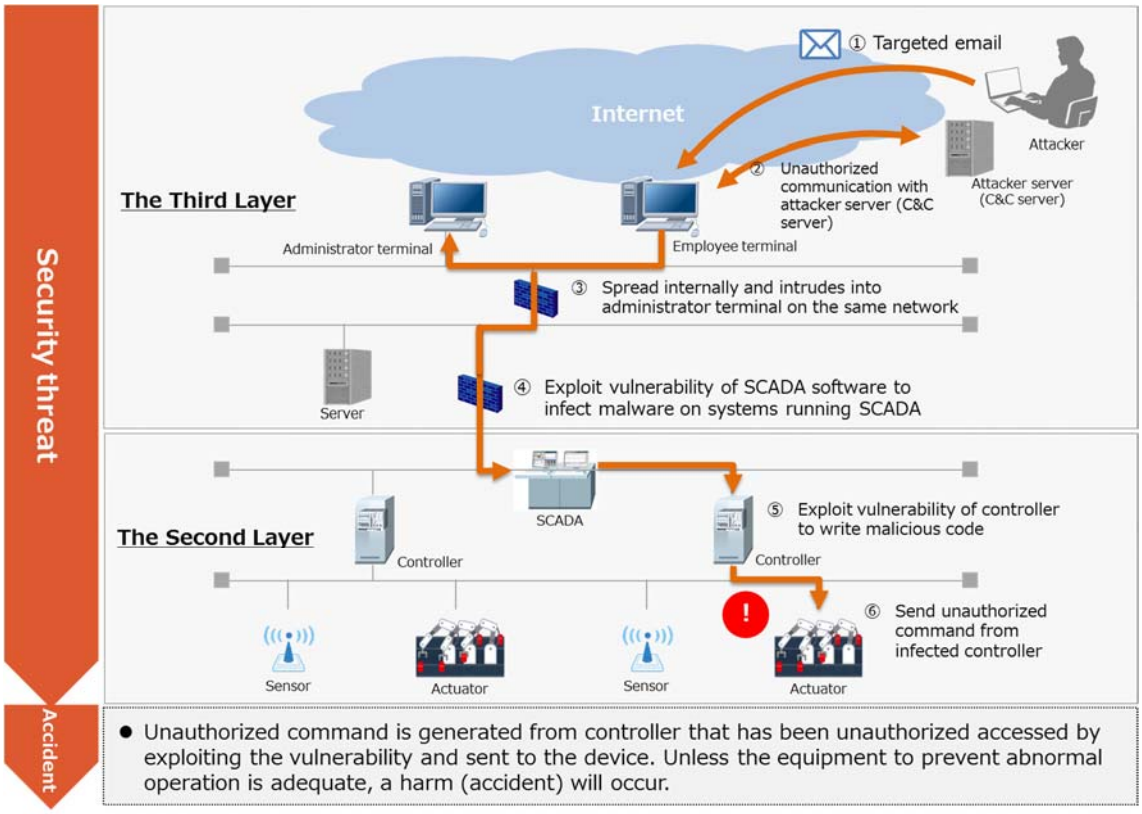


Figure 2.1-8 Example of security problems affecting safety

[8] Cited from IoT Acceleration Consortium, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry "IoT Security Guidelines Ver.1.0"

iii. **Cross-organizational data exchange**

- When exchange of data across organizations becomes active, it is assumed that there is a greater possibility that inappropriate data is provided to the organization from an unexpected element ("organization", person, component, etc.).
- In addition, it is assumed that there is a higher chance that data is provided to or by a third party beyond the organization and within a limited range.
- Therefore, it is necessary to list elements ("organization", person or component not belonging to "organization") that are the source of data assumed to be used by the organization and classify the list based on the level such as importance which is determined by the organization itself.

iv. **Securing the basis of trustworthiness of each layer**

- As mentioned in Part I, in "Society5.0", in order to produce the targeted value, it is important to take measures considering not only the viewpoint of the trustworthiness of the organizational management that has conventionally been taken in to consideration, but the plural viewpoints such as the accuracy of the transcription function through IoT devices in the second layer, and the trust of the data itself pertaining to the value creation process in the third layer.
- Therefore, in identifying the target of analysis, it is important to identify the factors that are connected with the basis of trustworthiness. In the above implementation, the measures described in i. to iii. in this section are effective.

1.2. Anticipating security incidents and their impact

Possible security incidents that may significantly impact business activities must be anticipated and organized. It is necessary to consider high-level incidents that could affect the functions of each layer at first, and then to identify potential cybersecurity breaches that could cause the incidents.

Corresponding to the functions of each layer described in Table 2.1-1 to 2.1-3, Table 2.1-4 lists high-level incidents that could threaten them (i.e. assumed adverse effect on the functions). Enterprises should define specific possible incidents in consideration of each item described in the column "Adverse

effect on functions" in Table 2.1-4.

Table 2.1-4 Image of adverse effect on functions in each layer

Layer	Functions in each layer (Object to be protected)	Adverse effect on functions
The First Layer	• Establishing the organizational risk management system and operating it properly • Continuing business operations appropriately even when a security incident occurs • Products or services in physical space are received or shipped with desired quality	• **Noncompliance with regulations etc.** • **Occurrence of a security incident** : Compromise of assets to be protected (leakage/tampering/destruction/unintended stop) • **Expansion of the impact of security incidents:** adverse impacts to business due to the expansion of damage (deactivation, mistaken output, employee's health and safety, negative impact on the environment etc.)
The Second Layer	• Reading events in physical space, translating them into digital data, and sending the data to the third layer in accordance with established rules • Controlling components and displaying visualized data based on data received from cyberspace in accordance with established rules	• **Device function stop**: operation of IoT device stops • **Low trustworthiness operation**: IoT device does not operate as intended ✓ Operation with safety, environmental and hygiene issues ✓ False measurement
The Third Layer	• Securely processing and analyzing data • Securely storing data • Securely sending and receiving data	• **Noncompliance with data protection regulations etc.** • **Non-secure operation**: compromise of assets due to security incidents in cyberspace (leakage/tampering/destruction/unintended stop) • **Operation with low trustworthiness**: Data-related services do not operate as

		intended (malfunction, unintended stop, etc.)

It is also important to consider each of the four points listed in 1 of this part. If any of them are not considered sufficiently when identifying risks and, as a result, protection measures are inadequate, there is a greater possibility of disruption to the value creation process. The examples shown in Table 2.1-5 illustrate the impact on the organization and other relevant organizations.

Table 2.1-5 Risk when viewpoints that should be considered are unnoticed when identifying the risk sources

Aspects not adequately considered	Security incidents that may occur	Security incidents[9] relevant in [Appendix B]
Understanding the relationships of stakeholders inside and outside the organization	Business is not continued appropriately when security incidents occur at a certain point in the value creation process	L1_3_b, L1_3_c
Understanding new security incidents that may arise from the integration of cyberspace and physical space	Incidents that may affect safety occur at the point of contact (IoT device) between cyberspace and physical space	L2_1_a, L2_1_b, L2_1_c, L2_2_a
	Attack on cyberspace from the IoT device	L2_3_b, L2_3_c
Understanding the state of data exchange across organizations	Sensitive data is not properly managed by outsourcing parties that process that data	L3_1_a, L3_1_b, L3_1_c, L3_2_a, L3_2_b, L3_4_b

Table 2.1-6 is examples of general security incidents that should be prevented in each layer of the three-layer structure.
To consider possible incidents exhaustively, enterprises should identify security incidents using the approach shown in Appendix B, and consider them concretely, taking into account the circumstances of each enterprise.

[9] For example, the security incident L1_3_b indicates the security incident (3) (b) assumed in the first layer.

Table 2.1-6 Security incidents to be assumed in each layer

Assumed security incidents in the first layer
(1) Security incidents (e.g. data leakage/tampering/destruction/unintended stop) due to inadequate risk management processes during normal operations
(a) Data that must be protected is leaked from an area managed by the organization.
(b) Data that must be protected is tampered with in an area managed by the organization.
(c) The system dealing with the data of its own organization stops due to a denial of service attack, ransomware infection etc..
(d) A security event occurs in the channel for product / service provisioning, causing unintended quality deterioration such as malfunction of a device.
(2) Noncompliance with regulations
(a) Security measures that satisfy the legal requirements for a system cannot be implemented
(3) Damage caused by security incidents expands, and the organization as well as other relevant organizations cannot continue their business properly.
(a) The organization's security incidents prevent their business from continuing properly (b) Other relevant organizations cannot continue their business properly due to the organization's security incidents (c) The organization's security incidents prevent the business of other relevant organizations from continuing properly

Assumed security incidents in the second layer
(1) Unintended operation of attacked IoT devices (e.g., incorrect measurement, improper control of things, stop of control function, measurement function)
(a) Unexpected behavior of the IoT device due to unauthorized access to its controls by exploiting a vulnerability results in unpredicted operation
(b) Unexpected behavior of the IoT device due to unauthorized access to its controls by impersonation of an authorized user results in unpredicted operation
(c) Unauthorized input to the IoT device due to unauthorized access to the system that remotely manages the IoT devices results in unpredicted operation
(d) Functions of IoT devices and communication devices stop due to attacks such as denial-of-service attack
(2) Damage to equipment, physical harm to employees, and negative impact on business operations due to operation of IoT devices (normal and abnormal operation)
(a) Behavior that threatens safety, regardless of the behavior being normal or abnormal

(3) Inaccurate transcription of physical data to cyberspace by IoT device (false measurement)	
	(a) Data is tampered with in the communication path between the IoT device and cyberspace
	(b) An unauthorized or tampered-with IoT device connects to the network and transmits incorrect data
	(c) An IoT device with low quality is connected to a network, causing failures and/or transmission of inaccurate data or transmission to unauthorized entity.
	(d) Inappropriate measurement occurs due to physical interference with measurement.

Assumed security incidents in the third layer	
(1) Data that must be protected in cyberspace are leaked.	
	(a) A related organization's protected data is leaked from a data storage area managed by the organization.
	(b) The organization's protected data is leaked from a data processing area managed by a related organization.
	(c) The organization's protected data is leaked from a data storage area managed by a related organization.
(2) Data that must be protected in cyberspace are falsified.	
	(a) Data in storage is tampered with.
	(b) Data in use is tampered with.
(3) The system that collects/processes/stores/analyzes data that must be protected in cyberspace takes an unintended action (e.g., shutdown).	
	(a) The system receives inappropriate data from an "Organization"/People/Components (due to a spoofing attack etc.). (b) The system that handles the organization's data in a related organization stops due to a denial-of-service attack. (c) The system that handles data stops whether it has been attacked or not. (d) Improper processed/analyzed results become output due to a malfunction in the data processing/analyzing system.
(4) An organization is unable to meet the security levels required by laws and regulations concerning data handling and sharing in cyberspace	
	(a) Laws and rules that prescribe data protection in cyberspace are violated. (b) The security requirements for highly confidential data to be shared only among authorized parties has not been set or met.

After the enterprise defines potential security incidents, it should estimate the business damage resulting from those incidents. One example of an approach is defined in Section 4.3, “Business damage and the business damage level” of “Security Risk Assessment Guide for Industrial Control System 2nd Edition” (IPA, 2018).
By assigning severity scores to the degree of damage for each possible security incident, appropriately prioritized risk mitigations and security measures can be realized.

1.3. Analyzing risks

Using the results of the process in section 1.1 and 1.2, the organization should explore and define attack scenarios that could lead to the identified security incidents, define the sources of threats, and assess possible damage to business. Appendix B identifies threats that may help cause particular security incidents and/or magnify the damage caused by the incidents, along with typical vulnerabilities. Hence, it can be used to identify the risk sources to be considered and to show gaps in risk coverage.
Typical vulnerabilities are identified exhaustively for the six elements shown in Figure 2.1-9. Note that, since system configurations, data flows, and details of relevant assets differ from one enterprise to another, the Framework recommends each enterprise consider their respective circumstances when exploring specific scenarios of attacks, assessing the levels of damage to business, and the risk sources.
When evaluating risk sources and selecting security measures, it is important to keep in mind that the same specific entity may correspond to six different elements in different value creation processes.For example, it may be appropriate to be evaluated PC or server not only as “System” but also as “Components”. Also, in some cases it is appropriate to evaluate software as each of “Procedure”, “Data” and “Components”.

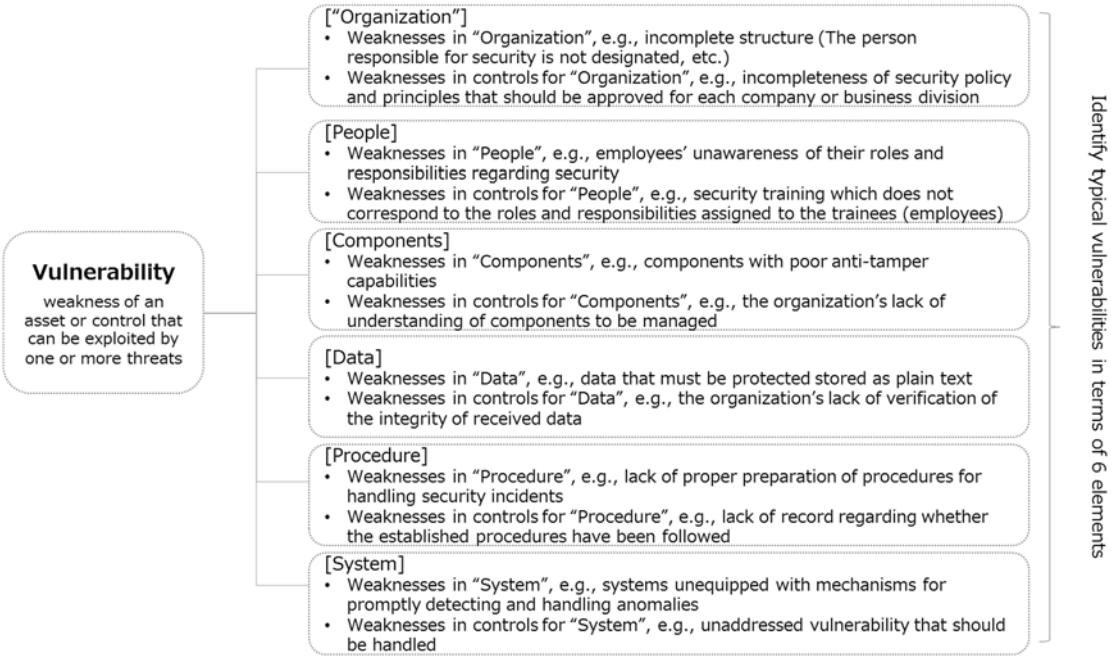


Figure 2.1-9 Identification of vulnerabilities in terms of six elements

1.4. Managing risks

Determine which action to take — aversion, reduction, transfer, or retention[10] — in order to manage the risks identified by the risk analysis conducted in 1.3 according to the level of damage each risk can cause.[11]

(1) Risk aversion: to eliminate risk by deleting risky functions or adopting entirely different means.
(2) Risk reduction: to reduce risk and/or reduce severity of impact by taking measures against the risk.
(3) Risk transfer: to transfer the risk to other entities by purchasing an insurance policy or by replacing internal products/systems/processes with those provided by other companies.
(4) Risk retention: to accept the risk without taking measures for risk reduction

[10] Cited from "Primer of safety & security design in the connected world" (IPA).
[11] The types of risk treatment described correspond to the risk treatment options presented in ISO 31000: 2018 as follows.
・ Risk aversion: Include "avoid the risk", "remove the source of the risk".
・ Risk reduction: Include "change the probabilities", "modify the consequences".
・ Risk transfer: Include "share the risk with others".
・ Risk retention: Include "increase the risk in order to pursue an opportunity", "retain the risk".

Appendix B provides a reference for risk sources corresponding to security incidents introduced in Table 2.1-6 and action to be taken, especially when the risk mitigation approach is selected from the above actions. The section "Measure requirements" is a guideline for implementing security based on the details of risk (threats and vulnerabilities). Appendix B also provides for adaption of its guidance to the particular circumstances of the organization. Since Appendix B matches specific vulnerabilities for each measure requirement, it can be used as a completeness and quality check for the risk analysis conducted by the organization.
It is particularly important to define measures for the four points of view already mentioned in the Framework.

i. Relation of multi-stakeholders who surround each organization involved in the value creation process

- It is vital to always have a whole picture of relationships between the stakeholders inside and outside the organization. It is also important to clarify the roles and responsibilities regarding cybersecurity among organizations. Definitions of stakeholders and roles that was considered in 1.1 must be promptly updated if the business partner has changed or any modifications have been made to the details of what must be done.
- ISO/IEC 27036-2:2014 mentions 5 phases shown in Figure 2.1-10 as a life cycle in relation to an individual supplier[12].

[12] With reference to this point, ISO/IEC 27036:2014 and NIST SP 800-161 are formulated as standards regarding the security measures relevant to the supply chain. In drafting this framework, NIST SP 800-161 is referred to for the identification of risk sources, and ISO/IEC 27036:2014 is referred to for the description of measure requirements and examples of security measures. Regarding this point, if it is deemed necessary to implement more enhanced measures, it is possible to refer to NIST SP 800-161 for security controls.

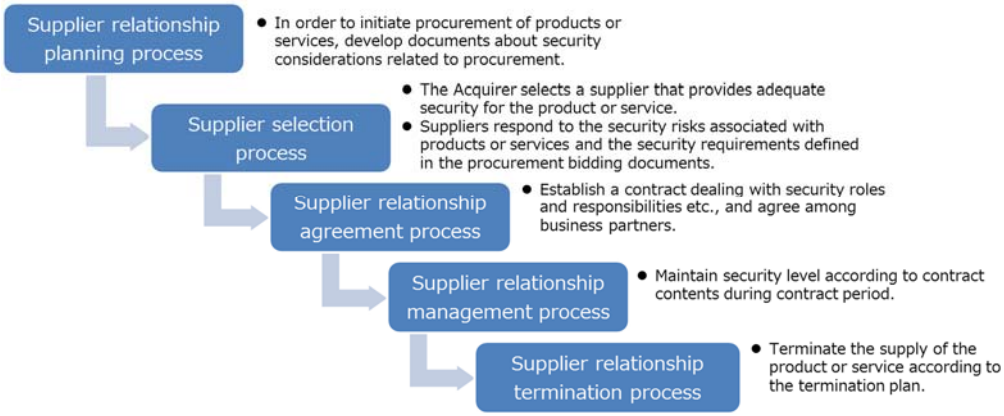


Figure 2.1-10 Life cycle in contracting with an individual supplier in ISO/IEC 27036-2:2013

- Requirements for security measures in light of the above life cycle are set out in the measure category "CPS.SC" (supply chain risk management) described in Part III. Each organization must consider stakeholder relationship management throughout the process life cycle for all categories of security measure.
  - ➢ Related measure requirements include CPS.AM-5, CPS.AM-7, CPS.BE-2, CPS.BE-3, CPS.SC-1, and CPS.SC-2. (Refer to Part III for details on each measure requirement)

ii. Integration of cyberspace and physical space through IoT devices

- If a sensor sends any measured data different than the actual one to cyberspace, or if measured data stops coming into cyberspace, the trust of the operations that use these data may be damaged.
- To avoid such damages, security measures must be taken to prevent attacks on functions of sensors. Specifically, consider using devices that do not easily shut down under attack (e.g., a denial-of-service attack), that offer a mechanism for checking data integrity, and/or that offer a function designed to guarantee the authenticity of measured data.
  - ➢ Related measure requirements include CPS.DS-6, CPS.DS-11, CPS.DS-15, and CPS.CM-4.

- As stated in 1.1, when data inputs are received from cyberspace for controlling components in physical space, security problems may lead to safety problems including physical harm. To ensure security and safety

on the interface between physical and cyberspace, it is vital to establish, at the design and procurement stages, a series of procedures to: analyze safety hazards and the sources of these risks. It is also critical to identify, based on the analysis, the business and technical processes on which security has an impact. This enables an organization to take appropriate courses of action, through the entire supplier lifecycle from planning and design/procurement through operation/maintenance/disposal, according to the analysis results.

- Ensuring safety has the utmost priority. Hence, it is necessary to combine measures taken for functional safety with cybersecurity measures in order to achieve safety. Since consideration of both safety and security aspects is required, close communication among the persons in charge of both safety and cybersecurity is essential to take appropriate actions.
  - Related measure requirements include CPS.RA-4, CPS.RA-6, CPS.PT-3, and CPS.CM-3.
  - Integrated security for safety control has been discussed in recent years in terms of international standardization. Documents available for reference regarding this subject include IEC TR 63074 and IEC TR 63069 (cf. Figure 2.1-11).[13]

[13] In addition to the IEC standards mentioned above, reference may also be made to ISO TR 22100-4: 2018 (Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects) which deals with machine safety security as well as IEC TR 63074.

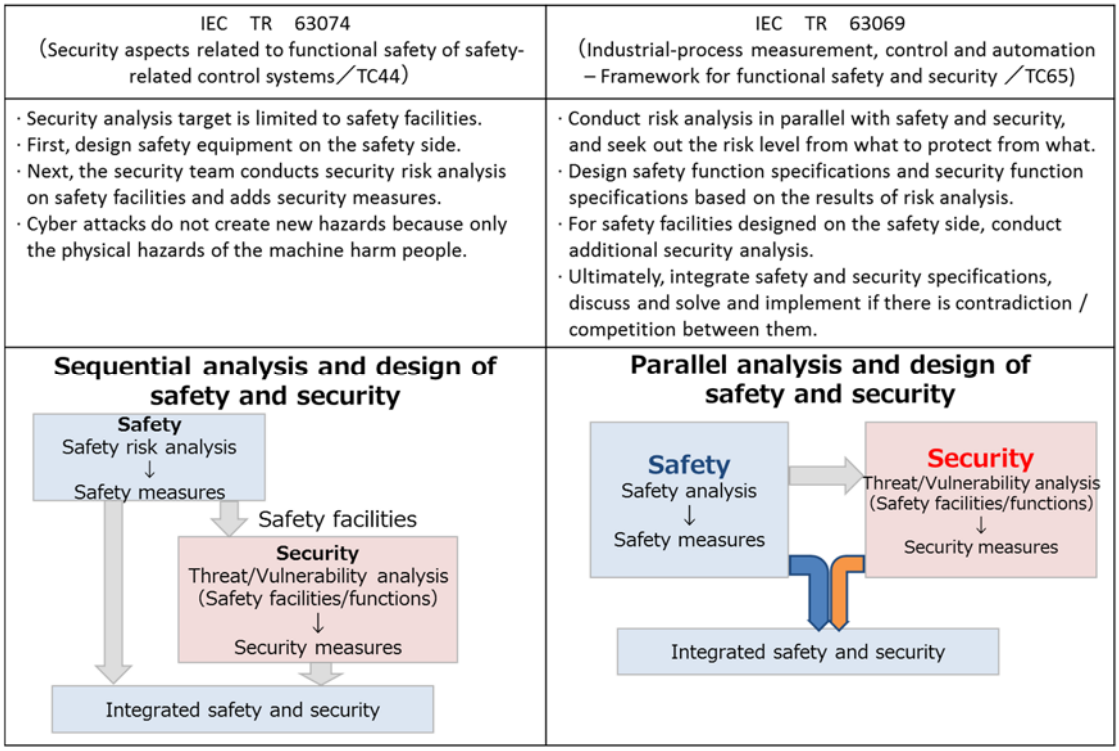


Figure 2.1-11 Status of discussion about integrated safety and security in the movement toward international standardization[14]

- In addition to logical threats, physical threats in physical space may affect cyberspace through an IoT device situated on the border between cyber and physical spaces.
- Hence, an organization must take physical security measures according to the importance of IoT devices that the organization uses. Examples of multilayered measures for physical security would be: separating the areas where critical IoT devices are installed from other areas in order to control access at the border and monitoring the critical area with surveillance cameras or other appropriate tools to detect any unauthorized actions. However, portable IoT devices carried by individuals or devices installed in households and public spaces are difficult for an organization to control. Therefore, it is important for an

[14] Created based on "Guide for for considering safety/security requirements for control systems" (IPA) and "Standard Activities of Functional Safety and Security" (Hiroo Kanamaru, "IPSJ Magazine", Vol.58, No.11, Nov.2017).

organization to consider the risks of theft and loss when taking security measures[15].

- Related measure requirements include CPS.AC-2, CPS.DS-8, CPS.IP-5, CPS.IP-6, CPS.PT-2, and CPS.CM-2.

iii. Cross-organizational data exchange

- In the case where the organization's protected data is processed, analyzed or stored by business partners, or where the organization handles the protected data of other organizations, the organization should agree with the business partners in advance on data classification, on the required security measures based on the classification, and on regular confirmation procedures including compliance auditing.
- The organization should analyze the risk in view of the characteristics of the exchanged data, the services that the business partners or the organization provide, and so on, and implement specific security requirements as appropriate.
- Even if it has implemented adequate measures, it is also important for the organization to formulate a procedure for security incident response in advance. The procedure should include notifications of all concerned parties when security incidents involving protected data are detected.
- If the organization receives data processed by other organizations, it should enable immediate response upon the detection of an anomaly, including continuously monitoring whether data is sent from authentic senders, the data does not include exploit codes, and so on.
  - Related measure requirements include CPS.SC-3, CPS.SC-4, CPS.SC-9, CPS.CM-1, CPS.CM-3, CPS.CM-4, CPS.DP-1, CPS.RP-2 and CPS.CO-1.

iv. Securing the basis of trustworthiness of each layer

- In the first layer, it is vital to specify cybersecurity requirements needed to maintain relationships and trust with the stakeholder organizations in the value creation process, and to regularly check compliance status.

[15] It is advisable to refer to the Main Point 6 in IoT Security Guidelines ver. 1.0 by the IoT Acceleration Consortium, Ministry of Internal Affairs and Communications, and the Ministry of Economy, Trade and Industry.

- An entity subject to regular checks and audits should collect the information that proves their compliance and make it available in advance or promptly upon request. This applies particularly to business partners critical to the organization's business continuity. The organization should ensure that not only direct contractors, but subcontractors and any organizations working for them, comply with the established requirements, thereby developing a chain of trust.
  - Related measure requirements include CPS.SC-3, CPS.SC-4, CPS.SC-6 and CPS.SC-8.
- The second layer requires that an IoT device's transcription function be accurate. To ensure accuracy, it is vital to maintain and enhance the soundness of security for the IoT device by taking measures throughout the device life cycle, from the design and procurement stages through the operation and disposal stages.
- The organization should take measures such as adopting security-by-design at the planning, design and procurement stages, testing security functions for verification, managing vulnerability when the device is in operation, and verifying the integrity of the device and software.
- In the case of an IoT device that is extremely important to the organization's business continuity, security requirements for the transcription functions should be in the agreement so that the organization can check if these requirements are accurately met throughout the series of processes performed by the contractor, or subcontractors, or any organizations working for them (e.g., production, transportation).
- Security practice for IoT devices has some important differences from security for traditional IT systems.[16] Though it is essential to require adequate security functions during procurement based on the principle of Security by Design, alternative measures on the part of the system should be considered if they are not available. In Appendix C, several security measure requirements such as CPS.IP-10, CPS.CM-3, CPS.CM-

[16] For example, Draft NISTIR 8228 suggests that, in order to implement security protection of IoT devices in terms of device security, data security and privacy, the characteristics specific to IoT devices, unlike traditional IT devices, should be considered with regard to the measures such as asset management, vulnerability management, access management, incident detection, data flow management.

6 describe the process of securing IoT devices. The organization should refer to these items when considering security measures for IoT devices.

- ➢ Related security measure requirements include CPS.RA-4, CPS.RA-6, CPS.DS-10, CPS.DS-12, CPS.DS-15, CPS.CM-6 and CPS.CM-7.

- The third layer requires that data in cyberspace and its processing, analysis, and storage be reliable.
- To ensure trustworthiness, it is essential that the data is reliable, in addition to the important points in the first layer and the second layer stated above. Specifically, the data should be checked to determine whether it has been falsified, is in the acceptable range (e.g., the data is free from attack code), and it has been generated by and sent from authorized elements (e.g., "organization", people, components).
- Data that is particularly important to the organization's business continuity should be checked for trustworthiness by the entity that has created and processed the data. Data sent to the organization should be quality and security checked when received (e.g., checking the data for falsification or attack code). The organization must also monitor security compliance of data processing and analysis components and systems.
  - ➢ Related measure requirements include CPS.DS-9, CPS.DS-14, CPS.AE-1, CPS.CM-3, CPS.CM-4 and CPS.CM-5.

Table 2.1-7 An example of measure requirements corresponding to the points of view considered in the risk management process

Point of view to identify the risk sources	An example of Corresponding measure requirements
Relationships with stakeholders involved in the value creation process	CPS.AM-5, CPS.AM-7, CPS.BE-2, CPS.BE-3, CPS.SC-1, CPS.SC-2, CPS.DS-13, CPS.CM-4
Integration of cyberspace and physical space through IoT devices	CPS.RA-4, CPS.RA-6, CPS.PT-3, CPS.CM-3
Cross-organizational data flows	CPS.SC-3, CPS.SC-4, CPS.SC-6, CPS.CM-1, CPS.CM-3, CPS.CM-4, CPS.DP-1, CPS.RP-2, CPS.CO-1
Securing a base level of trustworthiness in each layer	CPS.RA-4, CPS.RA-6, CPS.SC-3, CPS.SC-4, CPS.SC-6, CPS.DS-10, CPS.DS-12, CPS.CM-4, CPS.CM-5

2. Relationship between risk sources and measure requirements

Appendix B, as Table 2.2-1 below shows, lists the functions, assumed security incidents, the risk sources (threats and vulnerability) and measure requirements in each layer.

Table 2.2-1 Example of a table in Appendix B (The Third Layer)

Function	Assumed security incident	Risk sources			Measure requirements	Measure requirement ID
		Threat	Vulnerability ID	Vulnerability		
All of the following functions; - Functions to securely send and receive data - Functions to securely process and analyze data - Function to securely store data	- DoS attacks on computer equipment and communication devices (e.g., servers) that comprise a system	- DoS attack on computing devices such as servers, communication devices, etc. · Transmission of jamming waves	L3_3_b_ORG	[Organization] - The organization does not confirm the trustworthiness of contractor organizations such as data providers or data manipulators/analyzers before and after signing contracts.	Identify, prioritize, and evaluate the organizations and people that play important role relevant in each layer of the three-layer structure to sustaining the operation of the organization.	CPS.SC-2
					When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-3
	The system that handles data stops whether it has been attacked or not.	- Services provided by a system with low quality/trustworthiness	L3_3_c_SYS	[System] - A system that contains IoT devices does not have adequate resources (i.e., processing capacity, communication bandwidths, and storage capacity)	Secure sufficient resources (Ex: People, Components, System) for components and systems, and protect assets property to minimize bad effects of cyberattack (e.g., DoS attack).	CPS.DS-6

The column "Function" shows the functions of each layer summarized in Table 2.1-1, 2.1-2, 2.1-3 of 1.1 in Part II.

The column “Assumed Security Incident” shows incidents attributable mainly to security issues. These incidents may damage the layer’s functions stated in the left column, and are summarized in Table 2-1.6 of 1.1. The security incident stated may be caused by the “threat” and/or “vulnerability” shown in the “Risk Source” columns. An enterprise needs to manage any “risk source” that may have a severe impact. The requirements for security measures for the risk management action are included as “Measure Requirements.” Instances of vulnerability and measure requirements are given unique identifiers (Measure Requirement ID). They are available for reference in Part III and Appendix C, which provides examples of detailed measures.
Simple as they may be, the above descriptions follow the form of risk assessment so that enterprise can refer to them while they manage risks.

Part III (Method): Security measures – requirements and examples

1. Risk management using security measure requirements and examples of security measures

Using the analysis process for the identification of risks and security needs built in Part II, Part III and Appendix C show security measure requirements, examples of security measures corresponding to the measur requirements and the relationship with other international standards.

Part III and Appendix C are guides to the risk response phase of the risk management process. An enterprise can use the contents in this part for the following purposes:

(1) Strengthening the organization's security management

An enterprise can improve its risk management by implementing security measure requirements described in Part III and examples described in Appendix C according to the result of risk management. The process is expected to contribute to the security measures of each organization in two ways:

i. Implementation of measures that take into account the level of measures to be implemented and costs in each organization
ii. Comparisons with relevant international standards

For (i), Appendix C classifies security measures into three levels: High-Advanced/Advanced/Basic. Several factors dictate the classification, including scope of the measure (e.g., implementation only within the organization, or involving other relevant organizations), costs, and domestic/international standards. The enterprise can use these factors and classifications when deciding on the level of security measures to be implemented.

The security measures described in Appendix C are just examples. They do not exclude other security methods, nor are they absolute requirements for all organizations. It is always necessary for any organization to make its own determination of appropriate security measures based on risk assessment and analysis.

For (ii), Part III and Appendix C include points of alignment between the

measure requirements and major international standards. Especially, Appendix C organizes the comparison with the measure items of NIST SP800-171, NIST SP800-53 Rev.4, ISO/IEC 27001:2013 and IEC 62443 according to the level of examples of security measures. In addition, Appendix D organizes the correspondence relationship with the measure requiements that the Framework presents based on major international standards etc. in a table format. Implementation of the Framework is intended to help the organization simultaneously comply with these standards without requiring additional actions.

(2) Strengthening security governance over partners in the supply chain

In addition to the enterprise's own security management, it can also enhance security governance over partners in a relevant supply chain by requiring compliance with security measure requirements defined in the Framework.

Security measure requirements that state a set of processes the organization shall require from partners include CPS.SC-2, CPS.SC-3, CPS.SC-4, and CPS.SC-6. By implementing those processes effectively, organizations can ensure governance for contractors through their contract life cycle.

Since requirements for contractors will vary depending on the operations they provide, the importance of the contractor to the organization's operation, or other factors, the organization should understand all potential risks and risk sources as described in Part II.

Also, the organization may wish to maintain the security risk management of the whole supply chain by extending its control to all participants, especially when the direct contractors are important to the organization's operation. In such a case, the organization can provide the participants with specific security programs and requirements.

2. How to use examples of security measures

Appendix C lists measure requirements, examples of measures to implement those measure requirements by level, and the relationship between examples of measures and major international standards in a table format. Table 3.2-1 shows items described in Appendix C.

Table 3.2-1 Example of description in Appendix C

Measure Requirement ID	Measure Requirement	Examples of Security Measures	Subject that implements measures	NIST SP800-171	NIST SP800-53	ISO/IEC 27001 Annex A	IEC 62443
		<H-Advanced>		○	○		○
		<Advanced>			○	○	
		<Basic>			○	○	

The levels of security measures are classified as High-Advanced, Advanced, or Basic (see above 1.(1)). When the organization implements security measures classified as High-Advanced, it should also implement the security measures classified as Advanced and Basic.

The organization needs to refer to the importance assigned to the business, system, etc. that is required to be dealt with in CPS.AM-5 and CPS.BE-2, and take the appropriate measures from High-Advanced, Advanced, Basic. For example, it is possible to assign importance as shown in Table 3.2-2 from the viewpoint of confidentiality, integrity, and availability for business operations, systems, etc. Organizations need to materialize values and evaluation criteria, etc., taking into account their own specific conditions.

Table 3.2-2 Example of importance and evaluation criteria for classifying information asset based on confidentiality, integrity, availability[17]

Importance		Evaluation criteria
Confidentiality	2	The law requires appropriate management (leakage, loss or damage prevention).
		Identified as a subject of confidentiality or "Data for Limited Provision". There is a significant impact on business partners and customers if leaked.
		There is a serious impact on the organization if leaked because information that should be managed as trade secret.

[17] In particular, with regard to industrial control systems, in addition to the effects that are generally assumed in information systems in "Value" or "Evaluation criteria", the effects on safety, environment, and health are also desired to be considered.

	1	There is a significant impact on the organization's business if leaked.
	0	There is almost no impact on the organization's business even if leaked.
Integrity	2	The law requires appropriate management (leakage, loss or damage prevention).
		There is a serious impact on the organization or a significant impact on business partners and customers if it is tampered with.
	1	There is a significant impact on the organization's business if it is tampered with.
	0	There is almost no impact on the organization's business even if it is tampered with.
Availability	2	There is a serious impact on the organization or a significant impact on business partners and customers if it becomes unavailable.
	1	There is a significant impact on the organization's business if it becomes unavailable.
	0	There is almost no impact on the organization's business even if it becomes unavailable.

Similar security measure requirements may be needed at different levels. For example, "<Advanced> and <Basic>" may both require the same protection in some areas. This calls for the implementation of the same measures in <Advanced> and <Basic>. Also, the measure requirement described as "N / A" in <Basic> indicates that the implementation priority of the measure requirement is not necessarily high in cases where resources for implementation are severely limited, or when the importance of System and Components to be implemented for measures is not high.

The column "Subject that implements measures" classifies security measures[18] three ways. The subject is classified as "S" if the measures are generally implemented by a system through technical means, as "O" if the measures are implemented by an organization (e.g., by people through non-technical means), and as "O/S" if the measures are implemented by both a system and an organization.

The measures described in the "Examples of Security Measures" are just references to meet the measure requirements. It is possible to satisfy security requirement through the measures that are not described. Therefore, the

[18] The notation is in accordance with "NIST SP 800-53 Rev.5 (DRAFT) APPENDIX D".

"Examples of Security Measures" should be used for the implementation of proper measures that take into account costs in each enterprise as well as for comparisons with relevant international standards.

3. Security measure requirements

In the Framework, the measure requirements shown in Tables 3.3-2 to 3.3-21 are shown for each category.

(1) List of measure requirement categories

In the Framework, from the viewpoint of international harmonization, we defined the following 20 categories in association with the category of NIST Cybersecurity Framework Ver. 1.1.

Table 3.3-1 List of measure requirement categories and related category of NIST Cybersecurity Framework Ver. 1.1

Category name	Acronym	Related category of NIST Cybersecurity Framework Ver. 1.1
Asset Management	CPS.AM	ID.AM (Asset Management)
Business Environment	CPS.BE	ID.BE (Business Environment)
Governance	CPS.GV	ID.GV (Governance)
Risk Assessment	CPS.RA	ID.RA (Risk Assessment)
Risk Management Strategy	CPS.RM	ID.RM (Risk Management Strategy)
Supply Chain Risk Management	CPS.SC	ID.SC (Supply Chain Risk Management)
Identity Management, Authentication, and Access Control	CPS.AC	PR.AC (Identity Management and Access Control)
Awareness and Training	CPS.AT	PR.AT (Awareness and Training)
Data Security	CPS.DS	PR.DS (Data Security)
Information Protection Processes and Procedures	CPS.IP	PR.IP (Information Protection Processes and Procedures)
Maintenance	CPS.MA	PR.MA (Maintenance)
Protective Technology	CPS.PT	PR.PT (Protective Technology)
Anomalies and Events	CPS.AE	DE.AE (Anomalies and Events)
Security Continuous Monitoring	CPS.CM	DE.CM (Security Continuous Monitoring)
Detection Processes	CPS.DP	DE.DP (Detection Processes)

Response Planning	CPS.RP	RS.RP (Response Planning) RC.RP (Recovery Planning)
Communications	CPS.CO	RS.CO (Communications) RC.CO (Communications)
Analysis	CPS.AN	RS.AN (Analysis)
Mitigation	CPS.MI	RS.MI (Mitigation)
Improvements	CPS.IM	RS.IM (Improvements) RC.IM (Improvements)

(2) Alignment with major standards

The following are international standards noted in the NIST Cybersecurity Framework as compatible with each other. Part III, Appendix C and Appendix D list compatibilities of these standards with the Framework:

- NIST "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1" (NIST Cybersecurity Framework Ver. 1.1)
- Council on CyberSecurity (the Council) "The Critical Security Controls" (CIS CSC)
- ISACA "Control Objectives for Information- related Technology 5" (COBIT 5)
- ISA 62443-2-1:2010 "Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program"
- ISA 62443-3-3:2013 "Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels"
- ISO/IEC 27001:2013 "Information technology -- Security techniques -- Information security management systems – Requirements"[19]
- NIST "Special Publication 800-53 Revision 4"(SP 800-53 Rev.4)
- "Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5" (CC v3.1 Release 5)

[19] When using cloud services, it is desirable to also refer to the controls of ISO/IEC 27001: 2013 Annex A that are mentioned in "Informative references." and the items of ISO/IEC 27017: 2015 that correspond.

- Ministry of Economy, Trade and Industry (METI) and IPA "Cybersecurity Management Guidelines Ver. 2.0"
- IoT Acceleration Consortium, Ministry of Internal Affairs and Communications, METI "IoT Security Guidelines Ver. 1.0"

3.1. CPS.AM – Asset Management

Identify assets (e.g. data, people, goods, systems, zone where assets are managed, etc.) that are important to the organization's business and manage risk in accordance with its risk analysis and tolerance.

Table 3.3-2 Measure requirements in CPS.AM

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	L1_1_a_COM, L1_1_b_COM, L1_1_c_COM, L2_1_a_ORG, L2_3_b_ORG, L2_3_b_SYS	NIST Cybersecurity Framework Ver.1.1 ID.AM-1, ID.AM-2 CIS CSC 1, 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.6.2.1, A.8.1.1, A.8.1.2, A.8.1.3, A.11.2.5 NIST SP 800-53 Rev. 4 CM-8, PM-5 CC v3.1 Release5 Part 2 FMT Cybersecurity Management Guidelines Item4 IoT Security Guidelines Key Concept 3, 15
CPS.AM-2	Specify a method to ensure traceability based on the importance of the components produced by the organization's supply chain.	L1_3_a_COM, L1_3_b_COM	CC v3.1 Release5 Part 2 FIA
CPS.AM-3	Create records such as the date of production and condition of components depending on importance, and prepare and adopt internal rules regarding records of production activities in order to	L1_3_a_COM, L1_3_b_COM	

	store components for a certain period of time.		
CPS.AM-4	Create and manage appropriately network configuration diagrams and data flows within the organization.	L1_3_b_ORG, L1_3_c_ORG	NIST Cybersecurity Framework Ver.1.1 ID.AM-3 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4, 4.2.3.5 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 Cybersecurity Management Guidelines Item 4
CPS.AM-5	Create and manage appropriately a list of external information systems where the organization's assets are shared.	L1_1_a_COM, L1_1_b_COM, L1_1_c_COM, L1_3_b_ORG, L1_3_c_ORG	NIST Cybersecurity Framework Ver.1.1 ID.AM-4 CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.6.2.1, A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9 Cybersecurity Management Guidelines Item 4 IoT Security Guidelines Key Concept 3
CPS.AM-6	Classify and prioritize resources (e.g., People, Components, Data, and System) by function, importance, and business value, and communicate to the organizations and people relevant to those resources in business	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG, L3_1_a_ORG, L3_4_a_ORG	NIST Cybersecurity Framework Ver.1.1 ID.AM-5 CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 ISA 62443-2-1:2009 4.2.3.6, 4.3.4.4.3 ISO/IEC 27001:2013 A.8.2.1, A.8.2.2 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6 Cybersecurity Management Guidelines Item 4 IoT Security Guidelines Key Concept 3
CPS.AM-7	Define roles and responsibilities for cyber security across the organization and other relevant parties.	L1_3_b_ORG, L1_3_c_ORG	NIST Cybersecurity Framework Ver.1.1 ID.AM-6 CIS CSC 17, 19 COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 Cybersecurity Management Guidelines Item 4, 9 IoT Security Guidelines Key Concept 18, 19, 20

3.2. CPS.BE – Business Environment

Understand and prioritize the mission, goals, stakeholders, and activities of the organization. This information is used to convey cyber security roles, responsibilities and risk management decisions.

Table 3.3-3 Measure requirements in CPS.BE

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.BE-1	Identify and share the role of the organizations in the supply chain.	L1_3_b_ORG, L1_3_c_ORG	NIST Cybersecurity Framework Ver.1.1 ID.BE-1, ID.BE-2 COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12 Cybersecurity Management Guidelines Item 9 IoT Security Guidelines Key Concept 20
CPS.BE-2	Define policies and standard measures regarding security that are consistent with the high-priority business and operations of the organization, and share them with parties relevant to the organization's business (including suppliers and third-party providers).	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG	NIST Cybersecurity Framework Ver.1.1 ID.BE-3 COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 4 PM-11, SA-14 Cybersecurity Management Guidelines Item 6, 9
CPS.BE-3	Identify the dependency between the organization and other relevant parties and the important functions of each in the course of running the operation.	L1_3_b_ORG, L1_3_c_ORG	NIST Cybersecurity Framework Ver.1.1 ID.BE-4 COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14 Cybersecurity Management Guidelines Item 9

3.3. CPS.GV – Governance

Understand policies, procedures and processes for managing and monitoring compliance with regulations, laws, risks, internal policies, and operational requirements for the organization, and communicate them to cybersecurity risk managers.

Table 3.3-4 Measure requirements in CPS.GV

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.GV-1	Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO	NIST Cybersecurity Framework Ver.1.1 ID.GV-1, ID.GV-2 CIS CSC 19 COBIT 5 APO01.02, APO01.03, APO10.03, APO13.01, APO13.1202, DSS05.04, EDM01.01, EDM01.02 ISA 62443-2-1:2009 4.3.2.6, 4.3.2.2.1, 4.3.2.3.3 ISO/IEC 27001:2013 A.5.1.1, A.6.1.1, A.7.2.1, A.15.1.1 NIST SP 800-53 Rev. 4 -1 controls from all security control families Cybersecurity Management Guidelines Item 1, 2, 6 IoT Security Guidelines Key Concept 1, 18, 19
CPS.GV-2	Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.	L1_2_a_ORG, L1_2_a_COM, L1_2_a_SYS, L1_2_a_PRO, L1_2_a_DAT	NIST Cybersecurity Framework Ver.1.1 ID.GV-3 CIS CSC 19 COBIT 5 BAI02.01, MEA03.01, MEA03.04 ISA 62443-2-1:2009 4.4.3.7 ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 NIST SP 800-53 Rev. 4 -1 controls from all security control families CC v3.1 Release5 Part 2 FPR, FDP Cybersecurity Management Guidelines Item 1
CPS.GV-3	Understand the level of data protection required by laws and	L1_1_a_SYS, L1_1_a_DAT,	NIST Cybersecurity Framework Ver.1.1 ID.GV-3 CIS CSC 13

	arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	L1_1_b_SYS, L3_1_a_SYS, L3_1_a_DAT, L3_4_a_ORG, L3_4_a_PRO, L3_4_b_ORG, L3_4_b_PRO	ISA 62443-2-1:2009 4.3.4.4.6, 4.4.3.7 ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4
CPS.GV-4	Develop a strategy and secure resources to implement risk management regarding security.	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO	NIST Cybersecurity Framework Ver.1.1 ID.GV-4 COBIT 5 EDM03.02, APO12.02, APO12.05, DSS04.02 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.6.3 ISO/IEC 27001:2013 Clause 6 NIST SP 800-53 Rev. 4 SA-2, PM-3, PM-7, PM-9, PM-10, PM-11 CC v3.1 Release5 Part 2 FMT Cybersecurity Management Guidelines Item 2, 3 IoT Security Guidelines Key Concept 2

3.4. CPS.RA – Risk Assessment

The enterprise understands the cyber security risks to its own operations (including mission, function, image, and reputation), assets, and individuals.

Table 3.3-5 Measure requirements in CPS.RA

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.RA-1	Identify the vulnerability of the organization's assets and document the list of identified vulnerability with the corresponding asset.	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS	NIST Cybersecurity Framework Ver.1.1 ID.RA-1 CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 CC v3.1 Release5 Part 1 Cybersecurity Management Guidelines Item 4 IoT Security Guidelines Key Concept 21
CPS.RA-2	The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.), analyzes the information, and establishes a process to implement and use measures.	L1_1_a_SYS, L1_3_a_ORG, L2_1_a_ORG, L2_1_c_SYS, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 ID.RA-2, RS.AN-5 CIS CSC 4 COBIT 5 BAI08.01 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.6.1.4, A.12.6.1 NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16 Cybersecurity Management Guidelines Item 10 IoT Security Guidelines Key Concept 18, 21
CPS.RA-3	Identify and document the assumed security incidents, those impacts on the organization's assets, and the causes of those.	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS	NIST Cybersecurity Framework Ver.1.1 ID.RA-3 CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 Clause 6.1.2

			NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16 CC v3.1 Release5 Part 1 Cybersecurity Management Guidelines Item 4
CPS.RA-4	- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation. - Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS, L2_1_a_COM, L2_1_a_PRO, L2_2_a_ORG, L2_2_a_SYS	NIST Cybersecurity Framework Ver.1.1 ID.RA-4, RS.MI-3 CIS CSC 4 COBIT 5 DSS04.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.11, 4.2.3.12 ISO/IEC 27001:2013 A.16.1.6, Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-14, PM-9, PM-11 CC v3.1 Release5 Part 1 Cybersecurity Management Guidelines Item 4 IoT Security Guidelines Key Concept 4, 10, 12
CPS.RA-5	Consider threats, vulnerability, likelihood, and impacts when assessing risks.	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS	NIST Cybersecurity Framework Ver.1.1 ID.RA-5 CIS CSC 4 COBIT 5 APO12.02 ISO/IEC 27001:2013 A.12.6.1, Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16 CC v3.1 Release5 Part 1 Cybersecurity Management Guidelines Item 4 IoT Security Guidelines Key Concept 4, 7
CPS.RA-6	- On the basis of the results of the risk assessment, clearly define the details of measures to prevent possible security risks, and document the organized outcome from the scope and priorities of the measures. - React accordingly to the security risks and the associated safety risks identified as a result of the assessment conducted at	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS, L2_1_a_COM, L2_1_a_PRO, L2_2_a_SYS	NIST Cybersecurity Framework Ver.1.1 ID.RA-6, RS.MI-3 CIS CSC 4 COBIT 5 APO12.05, APO13.02 ISO/IEC 27001:2013 Clause 6.1.3 NIST SP 800-53 Rev. 4 PM-4, PM-9 CC v3.1 Release5 Part 1 Cybersecurity Management Guidelines Item 4 IoT Security Guidelines Key Concept 10, 12

	the planning and design phase of an IoT device and systems incorporating IoT devices.		

3.5. CPS.RM – Risk Management Strategy

Set priority, constraint, and risk tolerance assumptions for the organization and use it to judge investment risk.

Table 3.3-6 Measure requirements in CPS.RM

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.RM-1	Confirm the implementation status of the organization's' cyber security risk management and communicate the results to appropriate parties within the organization (e.g. senior management). Define the scope of responsibilities of the organization and the relevant parties (e.g. subcontractor), and establish and implement the process to confirm the implementation status of security risk management of relevant parties.	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L1_3_a_ORG, L1_3_b_ORG	NIST Cybersecurity Framework Ver.1.1 ID.RM-1 CIS CSC 4 COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3 NIST SP 800-53 Rev. 4 PM-9 CC v3.1 Release5 Part 2 FMT Cybersecurity Management Guidelines Item 4 IoT Security Guidelines Key Concept 12
CPS.RM-2	Determine the organization's risk tolerance level based on the result of the risk assessment and its role in the supply chain.	L1_1_a_ORG, L1_1_a_SYS, L1_1_b_ORG, L1_1_b_SYS, L1_1_c_SYS	NIST Cybersecurity Framework Ver.1.1 ID.RM-2, ID.RM-3 COBIT 5 APO12.02, APO12.06 ISA 62443-2-1:2009 4.3.2.6.5 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 SA-14, PM-8, PM-9, PM-11 Cybersecurity Management Guidelines Item 4

3.6. CPS.SC – Supply Chain Risk Management

Establish enterprise priorities, constraints, risk tolerances, and assumptions and use them to assist in analysis of supply chain risk management. Establish and implement the process of identifying, evaluating and managing supply chain risks.

Table 3.3-7 Measure requirements in CPS.SC

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.SC-1	Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG	NIST Cybersecurity Framework Ver.1.1 ID.SC-1 CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3 NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9 CC v3.1 Release5 Part 2 FMT Cybersecurity Management Guidelines Item 9
CPS.SC-2	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG, L2_3_c_ORG, L3_1_b_ORG, L3_1_c_ORG, L3_3_a_ORG, L3_3_b_ORG, L3_3_d_ORG	NIST Cybersecurity Framework Ver.1.1 ID.SC-2 COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9 CC v3.1 Release5 Part 1 IoT Security Guidelines Key Concept 14
CPS.SC-3	When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L1_1_d_ORG, L2_3_c_ORG,	NIST Cybersecurity Framework Ver.1.1 ID.SC-3 COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2

	requirements defined by the organization while considering the objectives of such contracts and results of risk management.	L3_1_b_ORG, L3_1_b_DAT, L3_1_c_ORG, L3_1_c_DAT, L3_3_d_ORG, L3_3_a_ORG,. L3_3_b_ORG, L3_3_c_ORG, L3_4_a_DAT, L3_4_b_DAT	NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM-9 CC v3.1 Release5 Part 2 FCS, FDP, FIA, FMT IoT Security Guidelines Key Concept 5, 11
CPS.SC-4	When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L1_1_d_ORG, L1_1_d_COM, L2_1_a_COM, L2_1_a_PRO, L2_2_a_ORG, L2_3_a_ORG, L2_3_c_ORG, L2_3_c_PRO, L2_3_d_ORG, L3_1_b_ORG, L3_3_a_ORG, L3_3_b_ORG, L3_3_c_ORG, L3_3_d_ORG	ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7 ISO/IEC 27001:2013 A15.1.3 CC v3.1 Release5 Part 2 FIA, FDP Cybersecurity Management Guidelines Item 9 IoT Security Guidelines Key Concept 14
CPS.SC-5	Formulate and manage security requirements applicable to members of other relevant organizations, such as business partners, who are engaged in operations outsourced from the organization.	L1_1_a_PEO, L1_1_b_PEO, L1_1_c_PEO, L2_3_b_PEO, L3_1_b_PEO, L3_1_c_PEO	ISA 62443-2-1:2009 4.3.3.2.1 NIST SP 800-53 Rev.4 PS-7, SA-21
CPS.SC-6	Conduct regular assessments through auditing, test results, or	L1_1_a_DAT, L1_1_a_PRO,	NIST Cybersecurity Framework Ver.1.1 ID.SC-4

	other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	L1_1_b_PRO, L1_1_c_PRO, L2_3_c_ORG, L2_3_c_PRO, L2_3_d_ORG, L3_1_a_DAT, L3_1_b_ORG, L3_1_b_DAT, L3_1_c_ORG, L3_1_c_DAT, L3_3_a_ORG,. L3_3_b_ORG, L3_3_c_ORG, L3_3_d_ORG, L3_4_a_DAT, L3_4_b_DAT	COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 ISA 62443-2-1:2009 4.3.2.6.7 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
CPS.SC-7	Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L1_1_d_ORG, L2_2_a_ORG, L2_3_c_ORG, L2_3_c_PRO, L3_1_b_ORG, L3_1_c_ORG, L3_3_a_ORG, L3_3_b_ORG, L3_3_c_ORG, L3_3_d_ORG	
CPS.SC-8	Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.	L1_1_d_ORG, L2_2_a_ORG, L2_3_c_ORG, L2_3_c_PRO, L3_1_b_ORG, L3_1_c_ORG, L3_3_a_ORG,	COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 ISA 62443-2-1:2009 4.3.2.6.7 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2

		L3_3_b_ORG, L3_3_c_ORG, L3_3_d_ORG,	NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
CPS.SC-9	Prepare and test a procedure for incident response with relevant parties involved in the incident response activity to ensure action for incident response in the supply chain.	L1_3_b_PEO	NIST Cybersecurity Framework Ver.1.1 ID.SC-5 CIS CSC 19, 20 COBIT 5 DSS04.04 ISA 62443-2-1:2009 4.3.2.4.3, 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.16.1.5, A.17.1.2, A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
CPS.SC-10	Develop and manage a procedure to be executed when a contract with other relevant organizations such as business partners is finished. (e.g., expiration of contract period, end of support)	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO	NIST SP 800-53 Rev. 4 SA-22
CPS.SC-11	Continuously improve the standard of security measures relevant to the supply chain, related procedures, and so on.	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO	

3.7. CPS.AC – Identity Management, Authentication and Access Control

Limiting logical and physical access to assets and related zone to approved "organization", people, goods and procedures and manage them to limit the risk of unauthorized access and to ensure only approved activities and transactions are accessible.

Table 3.3-8 Measure requirements in CPS.AC

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.AC-1	Establish and implement procedures to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	L1_1_a_COM, L1_1_a_SYS, L1_1_b_COM, L1_1_b_SYS, L1_1_c_COM, L2_3_c_SYS L3_1_a_SYS, L3_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-1 CIS CSC 1, 5, 15, 16 COBIT 5 DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 ISO/IEC 27001:2013 A.6.2.1, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-1, AC-2, IA Family-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 CC v3.1 Release5 Part 2 FAU, FIA, FMT Cybersecurity Management Guidelines Item 5
CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	L1_1_a_SYS, L1_1_c_SYS, L2_3_b_PEO, L2_3_b_SYS, L2_3_c_SYS, L2_3_d_SYS, L3_1_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-2 COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.3 1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8 CC v3.1 Release5 Part 2 FIA, FMT, FDP Cybersecurity Management Guidelines Item 5
CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).	L2_3_c_SYS, L3_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-3 CIS CSC 12, 15 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6

			ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.6, SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC--1, AC-17, AC-19, AC-20, SC-15 CC v3.1 Release5 Part 2 FCS, FIA, FMT Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Concept 8, 11, 14, 16
CPS.AC-4	Prevent unauthorized log-in to IoT devices and servers by measures such as implementing functions for lockout after a specified number of incorrect log-in attempts and providing a time interval until safety is ensured.	L2_1_b_SYS, L3_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-3 CIS CSC 12 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.11, SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.9.4.2, A.11.2.6, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15 CC v3.1 Release5 Part 2 FIA Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Concept 4
CPS.AC-5	Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions).	L1_1_a_SYS, L1_1_b_SYS, L2_1_c_SYS, L3_1_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-4 CIS CSC 3, 5, 12, 14, 15, 16, 18 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 CC v3.1 Release5 Part 2 FMT Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Concept 4
CPS.AC-6	Adopt high confidence methods of authentication where	L1_1_a_SYS,	NIST Cybersecurity Framework Ver.1.1 PR.AC-4, PR.AC-7

	appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.	L1_1_b_SYS, L2_1_c_SYS, L3_1_a_SYS	CIS CSC 3, 5, 14, 15, 16 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.7.3, 4.3.3.7.4 ISA 62443-3-3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 CC v3.1 Release5 Part 2 FMT, FIA Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Concept 8
CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).	L2_1_b_SYS, L3_1_a_DAT, L3_4_b_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-5, PR.DS-7, PR.PT-4 CIS CSC 9, 14, 15, 18 COBIT 5 DSS01.05, DSS05.02 ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7 Cybersecurity Management Guidelines Item 5
CPS.AC-8	Restrict communications by IoT devices and servers to those with entities (e.g. people, components, system, etc.) identified through proper procedures.	L2_1_b_SYS, L3_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-6 CIS CSC 16 COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 ISO/IEC 27001:2013, A.7.1.1, A.9.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3 CC v3.1 Release5 Part 2 FCO, FCS, FDP, FIA

			Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Concept 11, 14, 16
CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	L1_1_a_SYS, L1_1_b_SYS, L2_1_b_SYS, L3_1_a_SYS, L3_4_b_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-7 CIS CSC 1, 12, 15, 16 COBIT 5 DSS05.04, DSS05.10, DSS06.10 ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 CC v3.1 Release5 Part 2 FCS, FDP, FIA, FPR Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Concept 8, 14, 16

3.8. CPS.AT – Awareness and Training

Implement cybersecurity awareness education and training to internal organization staff and partners to ensure fulfillment of contractual obligations, based on relevant policies, procedures and contracts.

Table 3.3-9 Measure requirements in CPS.AT

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.AT-1	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	L1_1_a_PEO, L1_1_b_PEO, L1_1_c_PEO, L1_1_d_PEO, L1_2_a_PEO, L1_3_a_PEO, L1_3_a_DAT, L1_3_c_PEO, L3_4_a_PEO	NIST Cybersecurity Framework Ver.1.1 PR.AT-1, PR.AT-2, PR.AT-4, PR.AT-5 CIS CSC 17 ISA 62443-2-1:2009 4.3.2.4.1, 4.3.2.4.2, 4.3.2.4.6, 4.3.3.2.5, 4,3,4,5,2, 4.3.4.5.11 ISO/IEC 27001:2013 A.6.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.3.1 NIST SP 800-53 Rev. 4 AT-1, AT-2, AT-3, AT-4 Cybersecurity Management Guidelines Item 3, 5, 8
CPS.AT-2	Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.	L1_3_a_DAT L1_3_b_PEO, L3_3_a_PEO	NIST Cybersecurity Framework Ver.1.1 PR.AT-3, PR.IP-10, RS.CO-1 CIS CSC 17 COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.4.1, 4.3.2.4.2, 4.3.2.4.3, 4.3.2.4.6, 4.3.4.5.11 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-4, PS-7, SA-9, SA-16 Cybersecurity Management Guidelines Item 3, 7, 8
CPS.AT-3	Improve the contents of training and education regarding security to members of the organization and other relevant parties of high importance in security management of the organization.	L1_1_a_PEO, L1_1_b_PEO, L1_1_c_PEO, L1_3_a_PEO, L1_3_b_PEO, L1_3_c_PEO, L3_3_a_PEO,	CIS CSC 17 ISA 62443-2-1:2009 4.3.2.4.4, 4.3.2.4.5 ISO/IEC 27001:2013 A.7.2.2 NIST SP 800-53 Rev. 4 AT-1

		L3_4_a_PEO, L3_4_b_PEO	

3.9. CPS.DS – Data Security

Manage information according to the organization's risk strategy, using the core security principles of confidentiality, integrity and availability of data.

Table 3.3-10 Measure requirements in CPS.DS

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.DS-1	If the organization exchanges protected information with other organizations, agree in advance on security requirements for protection of such information.	L3_1_a_PRO, L3_4_a_DAT, L3_4_b_DAT	ISO/IEC 27001:2013 A.13.1.2, A.13.2.1, A.13.2.2, A.13.2.3 NIST SP 800-53 Rev. 4 SC-1 Cybersecurity Management Guidelines Item 5
CPS.DS-2	Encrypt information with an appropriate level of security strength, and store them.	L1_1_a_DAT, L3_1_a_DAT, L3_3_d_SYS, L3_4_b_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-1 CIS CSC 13, 14 COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 ISA 62443-3-3:2013 SR 3.4, SR 4.1, SR 4.3 ISO/IEC 27001:2013 A.8.2.3, A.10.1.1 NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28 CC v3.1 Release5 Part 2 FCA Cybersecurity Management Guidelines Item 5
CPS.DS-3	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace	L1_1_a_SYS, L1_1_b_DAT, L3_1_a_DAT, L3_2_b_DAT, L3_3_a_SYS, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-2 CIS CSC 13, 14 COBIT 5 APO01.06, DSS05.02, DSS06.06 ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2, SR 4.3 ISO/IEC 27001:2013 A.6.2.2, A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12 CC v3.1 Release5 Part 2 FCO, FCS Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Concept 14
CPS.DS-4	Encrypt information itself when sending/receiving information.	L1_1_a_DAT, L1_1_b_DAT, L3_1_a_DAT,	NIST Cybersecurity Framework Ver.1.1 PR.DS-2 CIS CSC 13, 14 COBIT 5 APO01.06, DSS05.02, DSS06.06 ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR

		L3_2_b_DAT, L3_3_d_SYS	4.2, SR 4.3 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12 CC v3.1 Release5 Part 2 FCS Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Concept 14
CPS.DS-5	Securely control encryption keys throughout their life cycle to ensure proper operation and securely transmitted, received and stored data.	L1_1_a_DAT, L3_1_a_DAT	CIS CSC 13 ISO/IEC 27001:2013 A.10.1.2 NIST SP 800-53 Rev. 4 SC-12 Cybersecurity Management Guidelines Item 5
CPS.DS-6	Secure sufficient resources (e.g., People, Components, System) for components and systems, and protect assets property to minimize bad effects of cyberattack (e.g., DoS attack).	L1_1_c_SYS, L2_1_d_SYS, L3_3_c_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-4 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ISA 62443-3-3:2013 SR 5.2, SR 7.1 ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 CC v3.1 Release5 Part 2 FCO, FRU Cybersecurity Management Guidelines Item 5
CPS.DS-7	Carry out periodic quality checks, prepare standby devices and uninterruptible power supplies, provide redundancy, detect failures, conduct replacement work, and update software for IoT devices, communication devices, circuits, etc.	L1_1_c_SYS, L2_1_d_SYS, L3_3_c_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-4 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ISA 62443-3-3:2013 SR 5.2, SR 7.5 ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 CC v3.1 Release5 Part 2 FRU Cybersecurity Management Guidelines Item 5
CPS.DS-8	When handling information to be protected or procuring devices that have an important function to the organization, select IoT devices and servers equipped with anti-tampering devices.	L1_1_d_COM, L2_3_b_COM	NIST Cybersecurity Framework Ver.1.1 PR.DS-5 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ISO/IEC 27001:2013 A.8.2.3, A.10.1.2, A.11.1.4, A.11.1.5, A.11.2.1 NIST SP 800-53 Rev. 4 PE-19

			CC v3.1 Release5 Part 2 FCS, FPT Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Concept 8
CPS.DS-9	Properly control outbound communications that send information to be protected to prevent improper data breach,	L1_1_a_DAT, L2_3_c_SYS, L3_1_a_DAT	NIST Cybersecurity Framework Ver.1.1 PR.DS-5 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ISA 62443-3-3:2013 SR 5.2 ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, SC-7, SC-8, SC-13, SC-31, SI-4 CC v3.1 Release5 Part 2 FCS, FPT Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Soncept 8
CPS.DS-10	Conduct integrity checks of software running on the IoT devices and servers at a time determined by the organization, and prevent unauthorized software from launching.	L2_3_b_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-6 CIS CSC 2, 3 COBIT 5 APO01.06, BAI06.01, DSS06.02 ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.2.4 NIST SP 800-53 Rev. 4 SC-16, SI-7 CC v3.1 Release5 Part 2 FCS, FPT Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Concept 8
CPS.DS-11	Perform integrity checking on information to be sent, received, and stored.	L1_1_b_DAT, L1_1_d_PRO, L3_2_a_DAT, L3_2_b_DAT	NIST Cybersecurity Framework Ver.1.1 PR.DS-6 CIS CSC 2, 3 COBIT 5 APO01.06, BAI06.01, DSS06.02 ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 ISO/IEC 27001:2013 A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SC-16, SI-7 CC v3.1 Release5 Part 2 FCS, FPT Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Concept 8

CPS.DS-12	Introduce an integrity check mechanism to verify the integrity of hardware.	L1_1_d_PRO, L2_3_b_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-8 COBIT 5 BAI03.05 ISA 62443-2-1:2009 4.3.4.4.4 ISO/IEC 27001:2013 A.11.2.4 NIST SP 800-53 Rev. 4 SA-10, SI-7 CC v3.1 Release5 Part 2 FCS, FPT Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Concept 8
CPS.DS-13	Confirm that IoT devices and software are genuine products during the booting-up process	L1_1_d_PRO, L2_3_c_ORG, L2_3_c_SYS	CC v3.1 Release5 Part 2 FIA, FDP, FCS Cybersecurity Management Guidelines Item 5
CPS.DS-14	Maintain, update, and manage information such as the origination of data, and data processing history, throughout the entire data life cycle.	L3_4_a_PRO, L3_4_b_PRO	ISO/IEC 27001:2013 A.18.1.3, A.18.1.4 CC v3.1 Release5 Part 2 FAU Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Concept 13
CPS.DS-15	Use products that provide measurable security in order to ensure the availability of security reporting and the trustworthiness of sensing data through integrity protection.	L2_1_a_COM, L2_1_a_PRO, L2_3_a_ORG, L2_3_d_ORG	ISO/IEC 27001:2013 A.15.1.3 NIST SP 800-53 Rev. 4 SA-12 Cybersecurity Management Guidelines Item 5

3.10. CPS.IP – Information Protection Processes and Procedures

Maintain security policies, processes, procedures, and use them to manage system and asset protection (dealing with objectives, scope, roles, responsibilities, management commitments, coordination among organizations).

Table 3.3-11 Measure requirements in CPS.IP

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.IP-1	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	L1_1_a_SYS, L1_1_b_SYS, L2_1_a_ORG, L2_1_b_COM, L2_1_b_PRO, L2_3_b_ORG, L3_1_a_SYS, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 PR.IP-1, PR.IP-3 CIS CSC 3, 9, 11 COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05, BAI01.06, BAI06.01 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3, 4.3.4.3.5, 4.3.4.3.6 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 CC v3.1 Release5 Part 2 FMT, FDP, FIA IoT Security Guidelines Key Concept 4, 15
CPS.IP-2	Restrict the software to be added after installing in the IoT devices and servers.	L1_1_a_SYS, L2_1_a_ORG, L2_1_c_SYS, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 PR.IP-1 CIS CSC 9 COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05, BAI01.06, BAI06.01 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
CPS.IP-3	Introduce the system development life cycle to manage the systems.	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG,	NIST Cybersecurity Framework Ver.1.1 PR.IP-2 CIS CSC 18 COBIT 5 APO13.01, BAI03.01, BAI03.02, BAI03.03

		L2_1_d_SYS, L3_3_c_SYS	ISA 62443-2-1:2009 4.3.4.3.3 ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 NIST SP 800-53 Rev. 4 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8SI-12, SI-13, SI-14, SI-16, SI-17 CC v3.1 Release5 Part 1/3
CPS.IP-4	Perform a periodic system backups and testing of components (e.g., IoT devices, communication devices, and circuits).	L1_3_a_DAT, L2_1_d_SYS, L3_3_c_SYS	NIST Cybersecurity Framework Ver.1.1 ID.BE-5, PR.IP-4 CIS CSC 10 COBIT 5 APO13.01, DSS01.01, DSS04.07 ISA 62443-2-1:2009 4.3.4.3.9 ISA 62443-3-3:2013 SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9 CC v3.1 Release5 Part 2 FRU, FPT_TEE, FPT_TST
CPS.IP-5	Implement physical measures such as preparing an uninterruptible power supply, a fire protection facility, and protection from water infiltration to follow the policies and rules related to the physical operating environment, including the IoT devices and servers installed in the organization.	L1_1_a_SYS, L1_1_c_SYS, L2_3_b_SYS, L2_3_d_SYS, L3_1_a_SYS	NIST Cybersecurity Framework Ver.1.1 ID.BE-5, PR.IP-5 COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 CC v3.1 Release5 Part 2 FPT, FRU Cybersecurity Management Guidelines Item 8 IoT Security Guidelines Key Concept 6
CPS.IP-6	When disposing of an IoT device and server, delete the stored data and the ID (identifier) uniquely identifying the genuine IoT devices and servers as well as important information (e.g.,	L2_3_b_DAT	NIST Cybersecurity Framework Ver.1.1 PR.DS-3, PR.IP-6 COBIT 5 BAI09.03, DSS05.06 ISA 62443-2-1:2009 4.3.4.4.4 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2,

	private key and digital certificate), or make them unreadable.		A.11.2.7 NIST SP 800-53 Rev. 4 MP-6 CC v3.1 Release5 Part 2 FCS, FIA, FDP, FMT, FPT Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Concept 6
CPS.IP-7	Assess the lessons learned from security incident response and the results of monitoring, measuring, and evaluating internal and external attacks, and improve the processes of protecting the assets.	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L2_1_a_ORG	NIST Cybersecurity Framework Ver.1.1 PR.IP-7 COBIT 5 APO11.06, APO12.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 ISO/IEC 27001:2013 A.16.1.6, Clause 9, Clause 10 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 Cybersecurity Management Guidelines Item 5
CPS.IP-8	Share information regarding the effectiveness of data protection technologies with appropriate partners.	L2_1_a_ORG	NIST Cybersecurity Framework Ver.1.1 PR.IP-8 COBIT 5 BAI08.04, DSS03.04 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4 CC v3.1 Release5 Part 1 Cybersecurity Management Guidelines Item 9 IoT Security Guidelines Key Concept 18
CPS.IP-9	Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.	L1_1_a_PEO, L1_1_b_PEO, L1_1_c_PEO,	NIST Cybersecurity Framework Ver.1.1 PR.IP-11 CIS CSC 5, 16 COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.4, 4.3.3.2.3, 4.3.3.2.6 ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 NIST SP 800-53 Rev. 4 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21 CC v3.1 Release5 Part 2 FMT, FIA IoT Security Guidelines Key Concept 4
CPS.IP-10	Develop a vulnerability remediation plan, and modify the	L1_1_a_SYS, L2_1_a_ORG,	NIST Cybersecurity Framework Ver.1.1 PR.IP-12

	vulnerability of the components according to the plan.	L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	CIS CSC 4, 18, 20 COBIT 5 BAI03.10, DSS05.01, DSS05.02 ISA 62443-2-1:2009 4.3.4.3.7 ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2 Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Concept 17, 21

3.11. CPS.MA – Maintenance

Maintain and repair components of industrial control systems and information systems according to policies and procedures.

Table 3.3-12 Measure requirements in CPS.MA

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.MA-1	- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updates with managed tools properly and in a timely manner while recording the history. - Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable.	L1_1_a_SYS, L2_1_a_ORG, L2_1_c_SYS, L3_1_a_SYS, L3_3_a_SYS L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 PR.MA-1 COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05 ISA 62443-2-1:2009 4.3.3.3.7 ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6, A.14.2.4 NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, MA-6 IoT Security Guidelines Key Concept 17
CPS.MA-2	Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.	L1_1_a_SYS, L2_1_a_ORG, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS,	NIST Cybersecurity Framework Ver.1.1 PR.MA-2 CIS CSC 3, 5 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.43.3.6.8 ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 NIST SP 800-53 Rev. 4 MA-4 CC v3.1 Release5 Part 2 FAU IoT Security Guidelines Key Concept 17

3.12. CPS.PT – Protective Technology

Based on relevant policies, procedures, contracts, manage technical solutions to ensure security and resilience of systems and assets, safety.

Table 3.3-13 Measure requirements in CPS.PT

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	L1_1_a_SYS, L2_1_b_ORG, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 PR.PT-1 CIS CSC 1, 3, 5, 6, 14, 15, 16 COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 4 AU Family CC v3.1 Release5 Part 2 FAU IoT Security Guidelines Key Concept 9, 13
CPS.PT-2	Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc..	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS, L2_1_b_COM, L2_3_b_SYS, L3_1_a_SYS, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 PR.PT-2, PR.PT-3 CIS CSC 3, 8, 11, 13, 14 COBIT 5 DSS05.02, DSS05.05, DSS05.06, DSS06.06 ISA 62443-3-3:2013 SR 2.3 ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.6, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4 ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.1.2, A.11.2.9

			NIST SP 800-53 Rev. 4 AC-3, CM-7, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
CPS.PT-3	Introduce IoT devices that implement safety functions, assuming that these devices are connected to the network.	L2_2_a_ORG	NIST Cybersecurity Framework Ver.1.1 PR.PT-5 COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 ISA 62443-2-1:2009 4.3.2.5.2 ISA 62443-3-3:2013 SR 3.6, SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6 IoT Security Guidelines Key Concept 10

3.13. CPS.AE – Anomalies and Events

Detect anomaly and understand the possible impact of the event.

Table 3.3-14 Measure requirements in CPS.AE

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.AE-1	Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.	L1_1_a_COM, L1_1_a_SYS, L1_1_b_COM L1_1_c_COM L1_3_b_ORG, L1_3_c_ORG, L2_1_b_ORG, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS,	NIST Cybersecurity Framework Ver.1.1 DE.AE-1 CIS CSC 1, 4, 6, 12, 13, 15, 16 COBIT 5 DSS03.01ISA 62443-2-1:2009 4.4.3.3 ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4 CC v3.1 Release5 Part 2 FAU, FDP Cybersecurity Management Guidelines Item 5
CPS.AE-2	Appoint a chief security officer, establish a security management team (SOC/CSIRT), and prepare a system within the organization to detect, analyze, and respond to security events.	L1_3_a_ORG	NIST Cybersecurity Framework Ver.1.1 DE.AE-2 CIS CSC 3, 6, 13, 15 COBIT 5 DSS05.07 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 ISO/IEC 27001:2013 A6.1.1, A.12.4.1, A.16.1.5 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
CPS.AE-3	Identify the security events accurately by implementing the procedure to conduct a correlation analysis of the security incidents and comparative analysis with the threat information obtained from outside the organization.	L1_1_b_SYS L1_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 DE.AE-3, RS.AN-1 CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 COBIT 5 BAI08.02 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
CPS.AE-4	Identify the impact of security events, including the impact on other relevant organizations.	L1_3_b_PRO	NIST Cybersecurity Framework Ver.1.1 DE.AE-4 CIS CSC 4, 6 COBIT 5 APO12.06, DSS03.01

			ISO/IEC 27001:2013 A.6.1.4, A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4 Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Concept 5
CPS.AE-5	Specify the criteria to determine the risk degree of security events.	L1_3_a_PRO	NIST Cybersecurity Framework Ver.1.1 DE.AE-5 CIS CSC 6, 19 COBIT 5 APO12.06, DSS03.01 ISA 62443-2-1:2009 4.2.3.10 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8 Cybersecurity Management Guidelines Item 5

3.14. CPS.CM – Security Continuous Monitoring

Detect security events and monitor systems and assets to verify the effectiveness of protection measures.

Table 3.3-15 Measure requirements in CPS.CM

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.CM-1	Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.	L1_1_a_SYS, L1_1_c_SYS, L1_3_a_SYS, L2_1_b_ORG, L2_3_c_SYS, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS,	NIST Cybersecurity Framework Ver.1.1 DE.CM-1 CIS CSC 1, 7, 8, 12, 13, 15, 16 COBIT 5 DSS01.03, DSS03.05, DSS05.07 ISA 62443-3-3:2013 SR 6.2 NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 CC v3.1 Release5 Part 2 FAU, FDP IoT Security Guidelines Key Concept 8, 13
CPS.CM-2	Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.	L1_1_a_SYS, L1_1_c_SYS, L2_3_b_PEO, L2_3_b_SYS, L2_3_d_SYS, L3_1_a_SYS	NIST Cybersecurity Framework Ver.1.1 DE.CM-2 COBIT 5 DSS01.04, DSS01.05 ISA 62443-2-1:2009 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.2.5, A.11.2.6 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20 CC v3.1 Release5 Part 2 FAU, FDP IoT Security Guidelines Key Concept 8
CPS.CM-3	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.	L1_1_b_SYS, L2_2_a_COM, L3_3_a_DAT, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 DE.CM-4, DE.CM-5 CIS CSC 4, 7, 8, 12 COBIT 5 DSS05.01 ISA 62443-2-1:2009 4.3.4.3.8 ISA 62443-3-3:2013 SR 3.2, SR 3.5 ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 4 SI-3, SI-8 CC v3.1 Release5 Part 2 FAU_SAA.2 IoT Security Guidelines Key Concept 9

CPS.CM-4	Validate the integrity and authenticity of the information provided from cyberspace before operations.	L3_3_a_DAT, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 DE.CM-4, DE.CM-5 CIS CSC 4, 7, 8, 12 COBIT 5 DSS05.01 ISA 62443-2-1:2009 4.3.4.3.8 ISA 62443-3-3:2013 SR 3.2 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.12.6.2 NIST SP 800-53 Rev. 4 SI-3, SI-8 CC v3.1 Release5 Part 2 FCS
CPS.CM-5	Monitor communication with external service providers so that security events can be detected properly.	L1_1_a_COM, L1_1_a_SYS, L1_1_b_COM L1_1_c_COM L1_3_b_ORG, L1_3_c_ORG, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS,	NIST Cybersecurity Framework Ver.1.1 DE.CM-6 COBIT 5 APO07.06, APO10.05 ISO/IEC 27001:2013 A.13.1.2, A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4 IoT Security Guidelines Key Concept 8, 9, 13
CPS.CM-6	As part of the configuration management of devices, work constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other “organization”, people, components, and systems.	L1_1_a_COM, L1_1_a_SYS, L1_1_b_COM, L1_1_c_COM, L1_3_a_SYS, L1_3_b_ORG, L1_3_c_ORG, L2_1_a_ORG, L2_1_c_ORG, L2_1_c_SYS, L2_3_b_ORG, L2_3_b_SYS, L2_3_c_SYS, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-3, DE.CM-3, DE.CM-7 CIS CSC 1, 2, 3, 5, 7, 9, 12, 13, 14, 15, 16 COBIT 5 DSS05.02, DSS05.05, DSS05.07 ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-3, CM-8, CM-10, CM-11, PE-3, PE-6, PE-20, SI-4 IoT Security Guidelines Key Concept 13
CPS.CM-7	Confirm the existence of vulnerabilities that require a	L1_1_a_SYS, L2_1_c_SYS,	NIST Cybersecurity Framework Ver.1.1 DE.CM-8

	regular check-up in IoT devices and servers managed within the organization.	L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS,	CIS CSC 4, 20 COBIT 5 BAI03.10, DSS05.01 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-5 IoT Security Guidelines Key Concept 8, 21

3.15. CPS.DP – Detection Process

Maintain and test detection processes and procedures to accurately detect abnormal security events.

Table 3.3-16 Measure requirements in CPS.DP

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.DP-1	Clarify the role and responsibility of the organization as well as service providers in detecting security events so that they can fulfill their accountabilities.	L1_3_a_ORG	NIST Cybersecurity Framework Ver.1.1 DE.DP-1 CIS CSC 19 COBIT 5 APO01.02, DSS05.01, DSS06.03 ISA 62443-2-1:2009 4.4.3.1 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14 Cybersecurity Management Guidelines Item 5
CPS.DP-2	Detect security events in the monitoring process, in compliance with applicable local regulations, directives, industry standards, and other rules.	L1_2_a_ORG, L1_3_a_ORG	NIST Cybersecurity Framework Ver.1.1 DE.DP-2 COBIT 5 DSS06.01, MEA03.03, MEA03.04 ISA 62443-2-1:2009 4.4.3.2 ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, PM-14, SA-18, SI-4, PM-14 Cybersecurity Management Guidelines Item 1
CPS.DP-3	As part of the monitoring process, test regularly if the functions for detecting security events work as intended, and validate these functions.	L1_3_a_ORG	NIST Cybersecurity Framework Ver.1.1 DE.DP-3 COBIT 5 APO13.02, DSS05.02 ISA 62443-2-1:2009 4.4.3.2 ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.14.2.8, A.14.3.1 CC v3.1 Release5 Part 2 FPT_TEE Cybersecurity Management Guidelines Item 5 IoT Security Guidelines Key Concept 9
CPS.DP-4	Continuously improve the process of detecting security events.	L1_1_b_SYS, L1_3_a_ORG	NIST Cybersecurity Framework Ver.1.1 DE.DP-5 COBIT 5 APO11.06, APO12.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14 Cybersecurity Management Guidelines Item 5

3.16. CPS.RP – Response Planning

Respond to detected security incidents and implement and maintain response and recovery processes and procedures so affected assets and systems can be properly restored and business continues uninterrupted.

Table 3.3-17 Measure requirements in CPS.RP

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (security operation process) that includes the response of Organization, People, Components, System to identify the content of response, priority, and scope of response taken after an incident occurs.	L1_1_a_SYS, L1_3_a_PEO, L1_3_a_PRO, L2_1_a_PRO, L2_1_b_PRO, L2_1_c_PRO, L2_2_a_PRO, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 ID.BE-5, PR.IP-9, DE.DP-4, RS.RP-1, RS.CO-2, RS.CO-3 CIS CSC 19 COBIT 5 APO12.06, BAI01.10 ISA 62443-2-1:2009 4.3.3.3.10, 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8 CC v3.1 Release5 Part 2 FTA Cybersecurity Management Guidelines Item 5, 7, 8 IoT Security Guidelines Key Concept 5
CPS.RP-2	As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.	L1_3_a_PEO, L1_3_a_PRO, L1_3_b_PEO, L1_3_b_PRO	NIST Cybersecurity Framework Ver.1.1 ID.BE-5, PR.IP-9, RS.CO-4, RS.CO-5 CIS CSC 19 COBIT 5 APO12.06, DSS03.04, DSS04.03 ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1, 4.3.4.5.2, 4.3.4.5.5 ISO/IEC 27001:2013 Clause 7.4, A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-4, IR-7, IR-8, IR-9, PE-17 Cybersecurity Management Guidelines Item 7, 8
CPS.RP-3	Include security incidents in the business continuity plan or emergency response plan that outlines the action plans and response procedures to take in case of natural disasters.	L1_3_a_PRO L1_3_a_DAT	NIST Cybersecurity Framework Ver.1.1 ID.BE-5, RC.RP-1 CIS CSC 10 COBIT 5 APO12.06, BAI03.02, DSS02.05, DSS03.04, DSS04.02

			ISA 62443-2-1:2009 4.3.2.5.4, 4.3.3.3.10 ISO/IEC 27001:2013 A.11.1.4, A.16.1.5, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, CP-10, IR-4, IR-8, SA-13, SA-14 Cybersecurity Management Guidelines Item 8
CPS.RP-4	Take appropriate measures on goods (products) whose quality may be affected by security incidents, especially regrading production facilities damaged by the security incident.	L1_3_b_COM	

3.17. CPS.CO – Communications

Mitigate the impact of security incidents on the organization and the whole society, and coordinate communication and recovery activities with stakeholders in and outside Japan (for example, business partners, JPCERT/CC, CSIRT of other organizations, vendors) so that they can obtain support from organizations such as law enforcement agencies.

Table 3.3-18 Measure requirements in CPS.CO

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.CO-1	Develop and manage rules regarding publishing information after the occurrence of the security incident.	L1_3_a_PRO	NIST Cybersecurity Framework Ver.1.1 RC.CO-1 CIS CSC 19 COBIT 5 EDM03.02 ISA 62443-2-1:2009 4.3.4.5.9 ISO/IEC 27001:2013 A.6.1.4, A.17.1.1, Clause 7.4 Cybersecurity Management Guidelines Item 8 IoT Security Guidelines Key Concept 18
CPS.CO-2	Include the item in the business continuity plan or contingency plan to the effect that the organization shall work to restore its social reputation after the occurrence of a high-risk security incident.	L1_3_a_PRO	NIST Cybersecurity Framework Ver.1.1 RC.CO-2 COBIT 5 MEA03.02 ISO/IEC 27001:2013 A.17.1.1, Clause 7.4 Cybersecurity Management Guidelines Item 8
CPS.CO-3	Include the item in the business continuity plan or contingency plan to the effect that the details of the recovery activities shall be communicated to the internal and external stakeholders, executives, and management.	L1_3_a_PRO	NIST Cybersecurity Framework Ver.1.1 RC.CO-3 CIS CSC 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.2.5.5, 4.3.4.5.9 ISO/IEC 27001:2013 A.17.1.1, Clause 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4 Cybersecurity Management Guidelines Item 8

3.18. CPS.AN – Analysis

Analyze the incident and its effects to ensure efficient response and support restoration activities.

Table 3.3-19 Measure requirements in CPS.AN

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.AN-1	Understand the impact of the security incident on the whole society including the organization and relevant parties such as partners based on the full account of the incident and the probable intent of the attacker.	L1_3_a_COM, L1_3_a_PRO	NIST Cybersecurity Framework Ver.1.1 RS.AN-2 CIS CSC 19 COBIT 5 DSS02.02 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISO/IEC 27001:2013 A.16.1.4, A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4 Cybersecurity Management Guidelines Item 10
CPS.AN-2	Implement digital forensics upon the occurrence of the security incident.	L1_3_a_PRO	NIST Cybersecurity Framework Ver.1.1 RS.AN-3 COBIT 5 APO12.06, DSS03.02, DSS05.07 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 ISO/IEC 27001:2013 A.16.1.7 NIST SP 800-53 Rev. 4 AU-7, IR-4
CPS.AN-3	Categorize and store information regarding the detected security incidents by the size of security-related impact, penetration vector, and other factors.	L1_3_a_PRO	NIST Cybersecurity Framework Ver.1.1 RS.AN-4 CIS CSC 19 COBIT 5 DSS02.02 ISA 62443-2-1:2009 4.3.4.5.6 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8

3.19. CPS.MI – Mitigation

Implement activities to prevent the expansion of security events, mitigate the effects, and resolve security incidents.

Table 3.3-20 Measure requirements in CPS.MI

ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.MI-1	Take measures to minimize security-related damages and mitigate the impacts caused by such incident.	L1_3_a_PRO	NIST Cybersecurity Framework Ver.1.1 RS.MI-1, RS.MI-2 CIS CSC 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4 IoT Security Guidelines Key Concept 9

3.20. CPS.IM – Improvements

Improve response and recovery activities by incorporating lessons learned from present and past decisions / response activities.

Table 3.3-21 Measure requirements in CPS.IM

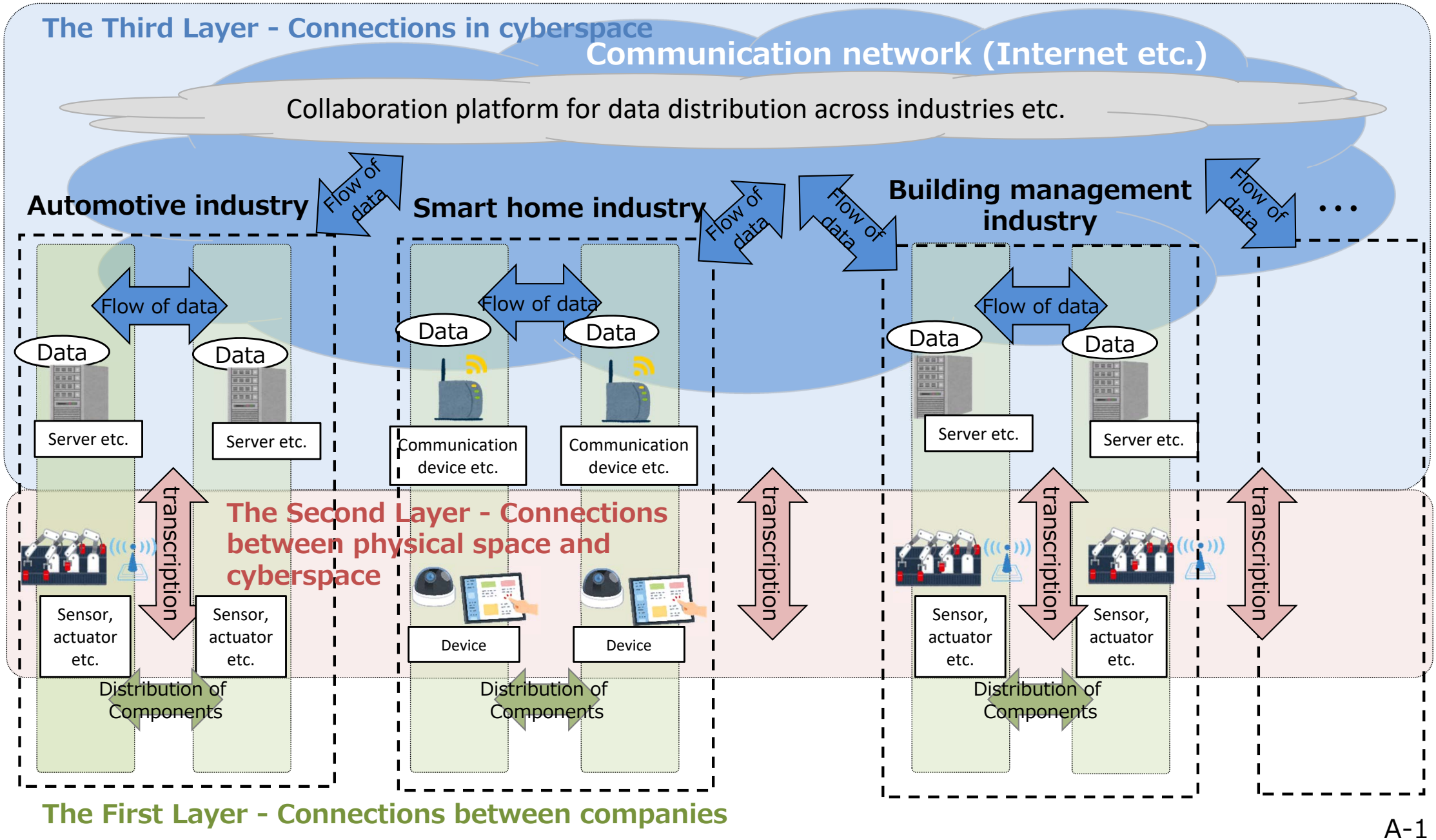
ID	Measure requirement	Relating vulnerability ID	Informative references
CPS.IM-1	Review the lessons learned from the responses to security incidents, and continuously improve the security operation process.	L1_3_a_ORG	NIST Cybersecurity Framework Ver.1.1 RS.IM-1, RS.IM-2 CIS CSC 19 COBIT 5 BAI01.13, DSS04.08 ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 Cybersecurity Management Guidelines Item 7 IoT Security Guidelines Key Concept 7
CPS.IM-2	Review the lessons learned from the responses to security incidents, and continuously improve the business continuity plan or emergency response plan.	L1_3_a_ORG	NIST Cybersecurity Framework Ver.1.1 RC.IM-1, RC.IM-2 CIS CSC 19 COBIT 5 APO12.06, BAI05.07, DSS04.08 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 Cybersecurity Management Guidelines Item 8

Appendix A. Use case

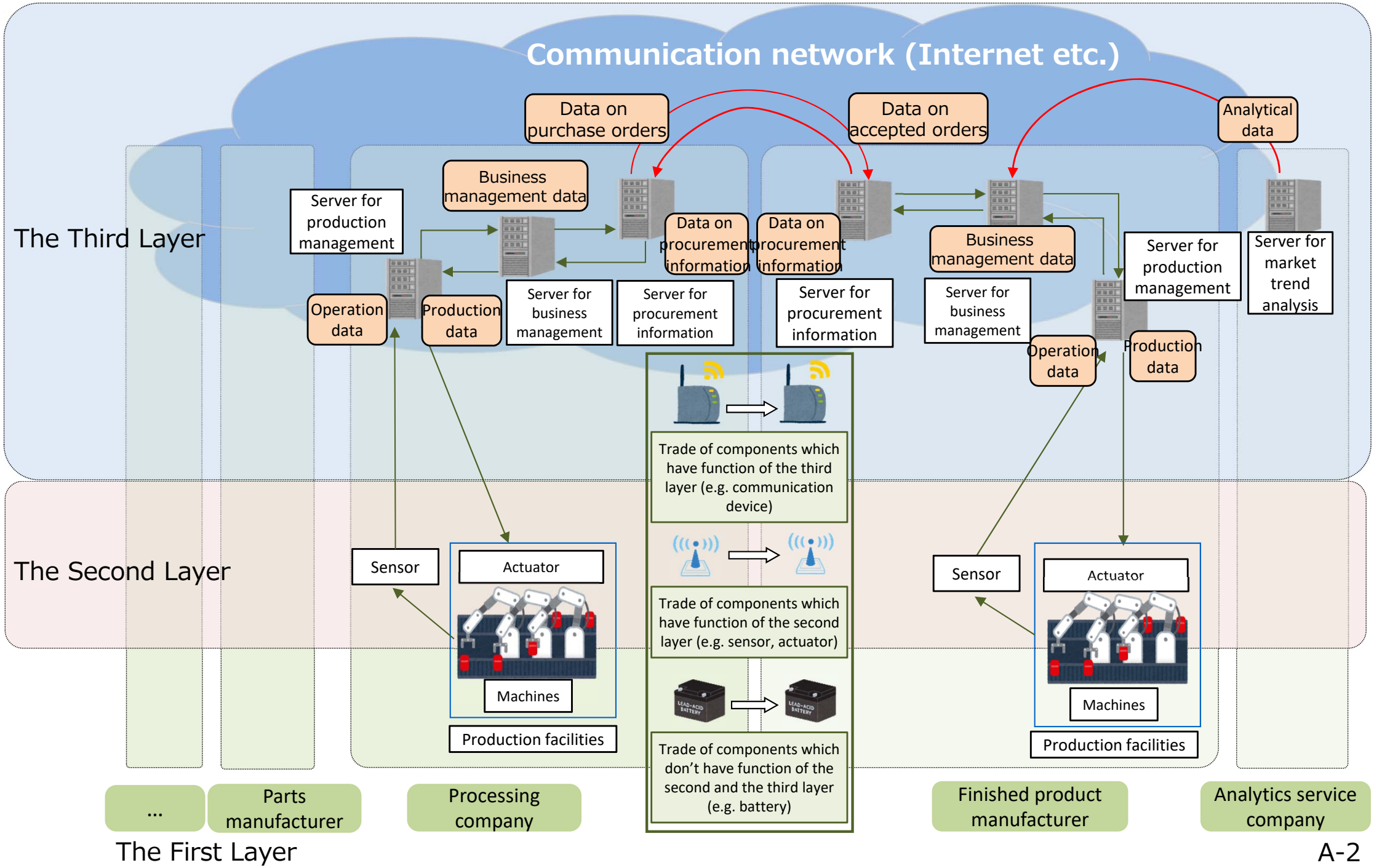
~References for specifying the targets of analysis~

Use case #1: Connections of components, data etc. in “Society5.0”

■ **In “Society5.0”,** cyberspace and physical space are highly integrated, and various **components, data etc. are distributed across companies and even among industries.**



Use case #2: Manufacturing process



Point of view in the use case #2 - Manufacturing process

1. Assumed "value creation process"

- A series of transactions in the manufacturing process; acquirer places an order for a product, and supplier produces the products based on the design drawing.

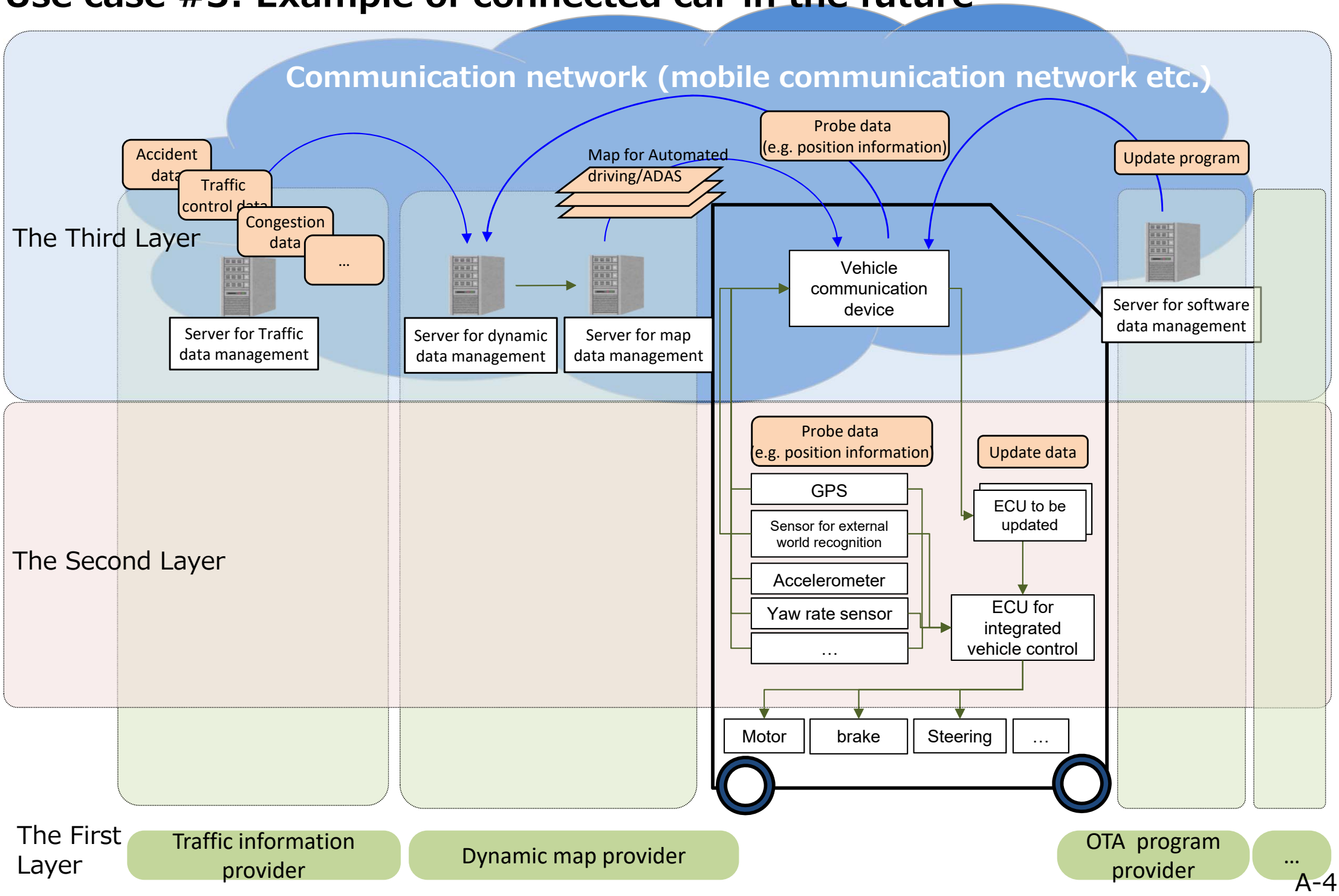
2. Features

- Along with progress toward Society5.0, the number of IoT devices will significantly increase.
- Also, there will be an increase of using external data such as market trend analysis data

3. Image of classification of elements to each layer

Layer	Example: Classification of elements to each layer in use case #2
The First Layer	• Parts manufacturer: An organization providing manufactured parts to processing company. • Processing company: An organization processing parts supplied by parts manufacturer. • Finished product manufacturer: An organization completing the product by assembling parts. • Analytics company: An organization providing finished product manufacturer with analytical data about market trends etc.
The Second Layer	• Sensor: A component monitoring the operation status of the production facilities and transducing that to electronic data. • Actuator: A component actuating the production facilities based on data about production management.
The Third Layer	• Communication device: A system component enabling connection of data among organizations. • Server for data processing: A system component performing functions such as storage, processing and analysis of data etc.. • Data to be processed －Data on procurement information: Data about order plans, transactions between organizations, etc.. －Analytical data: Analytical data about market trends etc., used for improvement of production plan.

Use case #3: Example of connected car in the future



Point of view in the use case #3 – Example of connected car in the future

1. Assumed "value creation process"

- A process that utilizes data obtained from sensors etc. to support human driving, or ultimately autonomously driving.

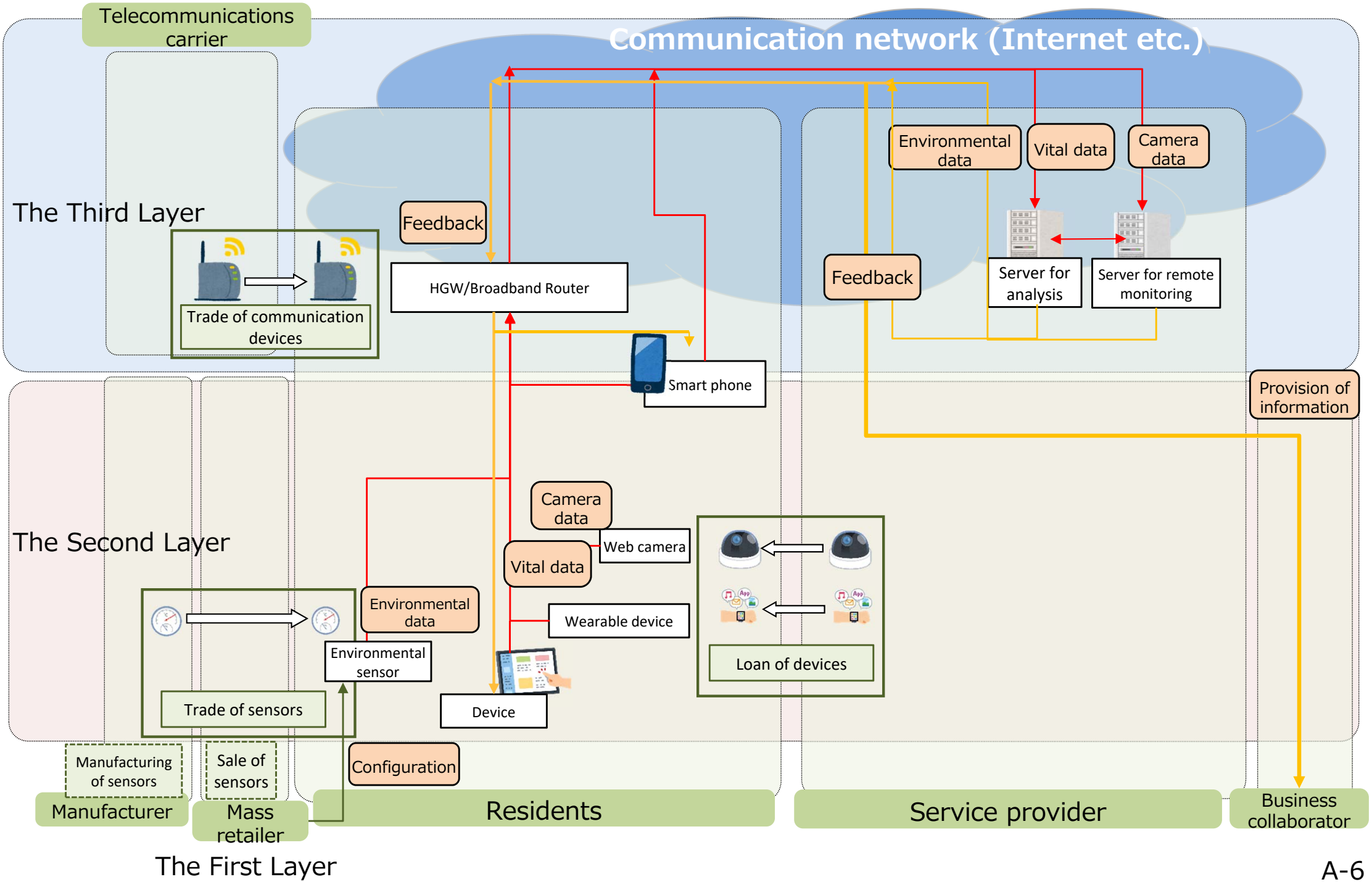
2. Features

- Along with progress of connected (automotive IoT), exchange of data inside and outside the car occurred, and connection between physical space and cyberspace and connections in cyberspace increased.
- In order to realize future automatic driving, it is possibility to require exchange of various data such as map data, congestion/traffic regulation data in addition of the surrounding data obtained by the outside world recognition sensor etc.

3. Image of classification of elements to each layer

Layer	Example: Classification of elements to each layer in use case #3
The First Layer	• Traffic information provider: An organization providing traffic control data and congestion data etc. for dynamic map provider. • Dynamic map provider: An organization analyzing probe data (e.g. position information) and, providing the result of analysis for automobiles. • OTA center: An organization providing difference data for vehicles.
The Second Layer	• ECU for driving control: A component controlling the motor, brake, steering, etc. based on information such as dynamic map. • Car proximity sensor: A component measuring the distance to the surrounding obstacles using a camera, radar, etc.. • GPS : A component for acquiring the location information of the vehicle.
The Third Layer	• Transmitter/receiver: A system component enabling connection of data among vehicles. • Server for data processing: A system component performing functions such as storage, processing and analysis of data etc.. • Data to be processed – Congestion data: Data about road congestion based on location information etc. of individual vehicle. Used to create dynamic map. – Dynamic map: Data combining map data, traffic congestion data, traffic control data, etc. used by vehicles for automatic driving.

Use case #4: Smart home



Point of view in the use case #4 - Smart home

1. Assumed "value creation process"

- A process in which services that meet the needs of residents are provided by utilizing data of daily life acquired from IoT devices etc. bought by residents or leased from service providers.

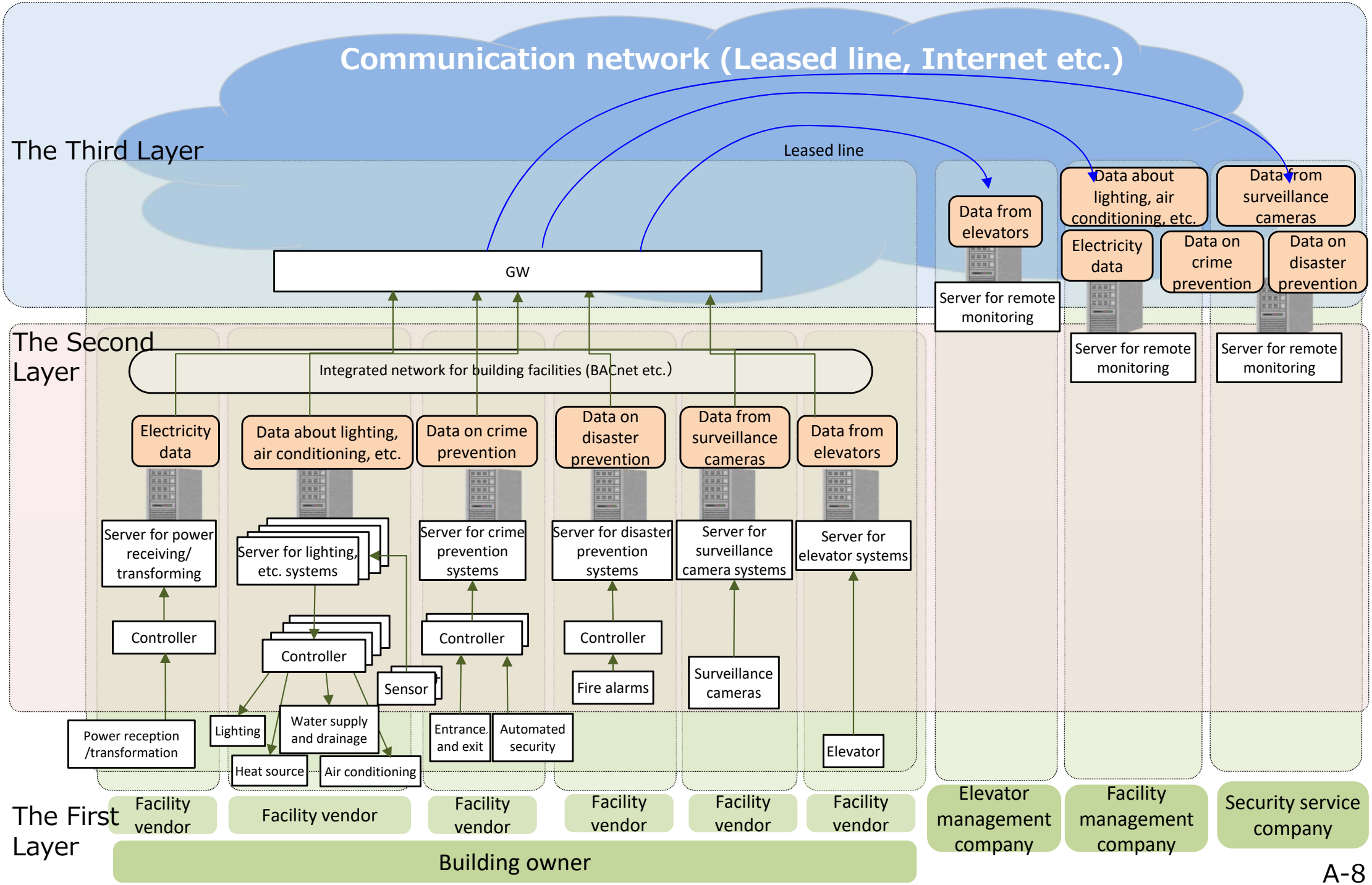
2. Features

- While consumer appliance, security camera, health equipment, etc. are connected to the Internet and becoming IoT device, data relating to daily life is exchanged through the network and, it is possible to operate IoT device via the network. So, it is important to ensure trustworthiness in the transcript operation of IoT device connecting cyberspace and physical space.
- In many cases, an administrator is not clearly determined in the maintenance of the IoT device and the management of the state.

3. Image of classification of elements to each layer

Layer	Example: Classification of elements to each layer in use case #4
The First Layer	• Residents: People that purchase or rent an IoT device and set it at home to provide data on their daily life and enjoy services based on it. • Service provider: An organization acquiring data from the household and implementing services based on it. • Telecommunications carrier: An organization providing internet and LTE network by lending communication devices to residents etc.. • Business collaborator: An organization receiving information from service provider and providing services based on it. • Manufacturer: An organization manufacturing sensors connecting to the internet etc.. • Mass retailer: An organization selling sensors, etc. manufactured by manufacturer and setting them.
The Second Layer	• Sensor, Wearable device, Web camera, Network connected appliance: A component transcripting activities in daily life into digital data. • Device: A component used for data browsing or input.
The Third Layer	• HGW : A system component enabling connection of data between a household and others. • Server for data processing: A system component performing functions such as storage, processing and analysis of data etc.. • Data to be processed – Environmental data: Data such as temperature and humidity. – Vital data: Data such as heart rate, body temperature and so on.

Use case #5: Building management



Point of view in the use case #5 - Building management

1. Assumed "value creation process"

- The process that the owner of a building signs a contract with facility management firm and utilizes data obtained from the building toward energy management and optimization of the building, and the process that the owner of the building monitors or manages it from remote site(s).

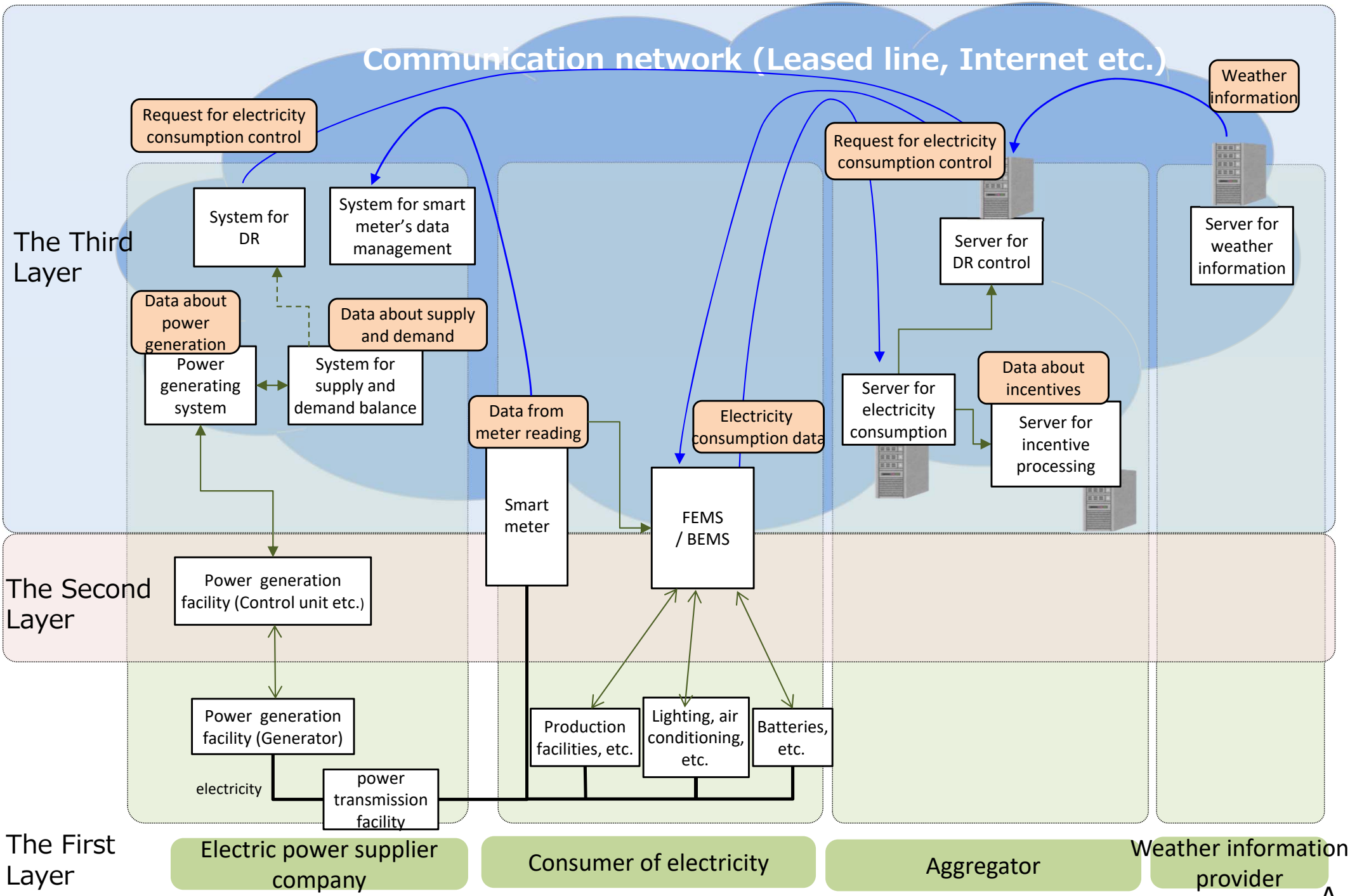
2. Features

- Evolution in IP-based communication regarding many control system(s) in the building
- Necessity in handshake of various data such as power supply data, elevation machine(s)' data to realize monitor/manage the building(s) from remote site(s)
- Many stakeholders such as elevation machines monitor firm(s) and facility management firm(s)

3. Image of classification of elements to each layer

Layer	Example: Classification of elements to each layer in use case #5
The First Layer	• Building: Objective(s) monitored/managed by building system(s) • Elevator management company: Organization that monitors/manages the operation status of elevators built in the building from remote site(s) • Facility management company: Organization that monitors/manages the power usage of the building(s) and others from remote site(s) • Security company: Organization that monitors/manages the building(s) through surveillance camera(s) or other(s)
The Second Layer	• Controller: Control device (Lighting, Heat source, Air-conditioning) • Surveillance camera: A component that monitors occurrence of emergency event(s)
The Third Layer	• Integrated network (BACnet etc.): System component toward achievement in data handshake between inside building(s)and outside building(s) • Server for data processing: A system component performing functions such as storage, processing and analysis of data etc.. • Data to be processed – Electricity data: Various power consumption of device(s) inside building(s). Data utilized by facility management firms. –Data on crime prevention: Combined data regarding such as those in an access-controlled secure room and those in automated security. Data utilized by security firm(s).

Use case #6: Electric power system (Demand response)



EMS : Energy Management System BEMS : Building EMS FEMS : Factory EMS

Point of view in the use case #6 – Electric power system (Demand response)

1. Assumed "value creation process"

- Process of demand-response toward reducing power supply through incentive

2. Features

- Increase in various data handshake as per power supply due to increasing smart-meter(s)
- Increase in the number of stakeholders in power supply due to evolution of de-regulation of power

3. Image of classification of elements to each layer

Layer	Example: Classification of elements to each layer in use case #6
The First Layer	• Electric power supplier company: An organization that requests aggregator toward reducing power usage • Consumer of electricity: An organization that executes reducing power consumption due to request toward reducing power consumption • Aggregator: An organization that requires manufacturers (plants, buildings) to reduce electric power consumption requested by electric company/companies. • Weather information provider: An organization that provides weather information to aggregators
The Second Layer	• Smart meter: A component that convert(s) electric consumption into read data • FEMS/BEMS: A system that manages energy consumption in plants or in buildings
The Third Layer	• Smart meter: System component that sends read data • Server for data processing: A system component performing functions such as storage, processing and analysis of data etc.. • Data to be processed –Weather information: Weather data such as temperature and humidity. Utilized for electric demand forecast –Request for electricity consumption control: Data such as the amount of electric power consumption. Utilized to request the reduction of power consumption from power firm(s) to aggregator(s), or from aggregator(s) to consumer(s)

Appendix B: Relationship between risk sources and measure requirements

■ Functions/Assumed Security Incidents/Risk Sources/Measure Requirements in the First Layer

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
1_1	Establishing the organizational risk management system effective in normal times and appropriately operating it.	Data that must be protected is leaked from an area managed by the organization	- Malware infection that takes advantage of a data storage system's vulnerability - Injection attack exploiting incomplete input validation (e.g. SQL injection, XSS) - Communication interception on the network - Physical intrusion by an unauthorized person into areas that need to be protected - Identity spoofing using a stolen ID/password of a proper user - Internal fraud by an authorized user	L1_1_a_ORG	[Organization] - Security risks are not managed in accordance with appropriate procedures, and other organizations needed are not involved in risk management.	Classify and prioritize resources (e.g., People, Components, Data, and System) by function, importance, and business value, and communicate to the organizations and people relevant to those resources in business.	CPS.AM-6
						Define policies and standard measures regarding security that are consistent with the high-priority business and operations of the organization, and share them with parties relevant to the organization's business (including suppliers and third-party providers).	CPS.BE-2
						Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.	CPS.SC-1
						Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.	CPS.SC-2
						Introduce the system development life cycle to manage the systems.	CPS.IP-3
				L1_1_a_PEO	[People] - People are not fully aware of the security or safety risks that may concern them.	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	CPS.AT-1
						Improve the contents of training and education regarding security to members of the organization and other relevant parties of high importance in security management of the organization.	CPS.AT-3
					[People] - The security or safety risks that involve people are not managed adequately.	Formulate and manage security requirements applicable to members of other relevant organizations, such as business partners, who are engaged in operations outsourced from the organization.	CPS.SC-5
						Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.	CPS.IP-9
				L1_1_a_COM	[Components] - The security status of components and the status of network connections are not managed appropriately (e.g. Inventory of assets, monitoring).	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	CPS.AM-1
						Create and manage appropriately a list of external information systems where the organization's assets are shared.	CPS.AM-5
						Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	CPS.AC-1
						Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.	CPS.AE-1
						Monitor communication with external service providers so that potential security events can be detected properly.	CPS.CM-5
						As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	CPS.CM-6
				L1_1_a_SYS	[System] - The organization has not implemented technical measures considering risks, or cannot confirm such implementation.	Identify the vulnerability of the organization's assets and document the list of identified vulnerability with the corresponding asset.	CPS.RA-1
						Identify and document the assumed security incidents, those impacts on the oraganization's assets, and the causes of those.	CPS.RA-3
						- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation. - Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.	CPS.RA-4
						Consider threats, vulnerability, likelihood, and impacts when assessing risks.	CPS.RA-5
						- On the basis of the results of the risk assessment, clearly define the details of measures to prevent possible security risks, and document the organized outcome from the scope and priorities of the measures.	CPS.RA-6
						Determine the organization's risk tolerance level based on the result of the risk assessment and its role in the supply chain.	CPS.RM-2
					[System] - Vulnerabilities that should be handled are left unaddressed in the system.	The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.), analyzes the information, and establishes a process to implement and use measures.	CPS.RA-2
						Restrict the software to be added after installing in the IoT devices and servers.	CPS.IP-2
						Develop a vulnerability remediation plan, and modify the vulnerability of the components according to the plan.	CPS.IP-10
						- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updateswith managed tools properly and in a timely manner while recording the history.	CPS.MA-1
						Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.	CPS.MA-2
						As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	CPS.CM-6
						Confirm the existence of vulnerability that requires a regular check-up in IoT devices and servers managed within the organization.	CPS.CM-7
					[System] - Settings in the system where the data to be protected is stored are not secure.	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	CPS.IP-1
						Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.	CPS.PT-2
					[System] - Regarding access to stored information, a request sender is not identified / authenticated in a manner suited to the level of confidentiality of such information.	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	CPS.GV-3
						Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	CPS.AC-1
						Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions)	CPS.AC-5
						Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.	CPS.AC-6
						Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	CPS.AC-9
					[System] - The organization does not take physical security measures such as access control and monitoring of areas where its IoT devices and servers are installed,	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	CPS.AC-2
						Implement physical measures such as preparing an uninterruptible power supply, a fire protection facility, and protection from water infiltration to follow the policies and rules related to the physical operating environment, including the IoT devices and servers installed in the organization.	CPS.IP-5
						Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.	CPS.PT-2
						Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.	CPS.CM-2
					[System] - The system has no mechanism for detecting and handling any abnormality related to security as soon as it arises.	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	CPS.PT-1
						Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.	CPS.AE-1
						Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.	CPS.CM-1
						- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.	CPS.CM-3
						Monitor communication with external service providers so that potential security events can be detected properly.	CPS.CM-5
						Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.	CPS.RP-1

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
				L1_1_a_DAT	[Data] - Classification concerning protection of data managed in own organization is not clear.	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	CPS.GV-3
					[Data] - Data protection at a predefined level of confidentiality is not implemented.	Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6
						Encrypt information with an appropriate level of security strength, and store them.	CPS.DS-2
						Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.	CPS.DS-3
						Encrypt information itself when sending/receiving information.	CPS.DS-4
						Securely control encryption keys throughout their life cycle to ensure proper operation and securely transmitted, received and stored data.	CPS.DS-5
						Properly control outbound communications that send information to be protected to prevent improper data breach.	CPS.DS-9
				L1_1_a_PRO	[Procedure] - Appropriate procedures for security risk management have not been established.	Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.	CPS.GV-1
						Develop a strategy and secure resources to implement risk management regarding security.	CPS.GV-4
						Confirm the implementation status of the organization's' cyber security risk management and communicate the results to appropriate parties within the organization (e.g. senior management). Define the scope of responsibilities of the organization and the relevant parties (e.g. subcontractor), and establish and implement the process to confirm the implementation status of security risk management of relevant parties.	CPS.RM-1
						When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-3
						When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-4
						Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6
						Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.	CPS.SC-7
						Develop and manage a procedure to be executed when a contract with other relevant organizations such as business partners is finished. (e.g., expiration of contract period, end of support)	CPS.SC-10
						Continuously improve the standard of security measures relevant to the supply chain, related procedures, and so on.	CPS.SC-11
						Assess the lessons learned from security incident response and the results of monitoring, measuring, and evaluating internal and external attacks, and improve the processes of protecting the assets.	CPS.IP-7
		Data that must be protected is tampered with in an area managed by the organization	- Identity spoofing using a stolen ID/password of a proper user - Man-in-the-middle attacks to falsify data on communication paths - Malware infection exploiting security vulnerabilities in the system - Internal fraud by an authorized user - Physical intrusion into the area where protection is required - Physical destruction of media handling data that needs protection	L1_1_b_ORG	[Organization] - Security risks are not managed in accordance with appropriate procedures, and other organizations needed are not involved in risk management.	Classify and prioritize resources (e.g., People, Components, Data, and System) by function, importance, and business value, and communicate to the organizations and people relevant to those resources in business.	CPS.AM-6
						Define policies and standard measures regarding security that are consistent with the high-priority business and operations of the organization, and share them with parties relevant to the organization's business (including suppliers and third-party providers).	CPS.BE-2
						Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.	CPS.SC-1
						Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.	CPS.SC-2
						Introduce the system development life cycle to manage the systems.	CPS.IP-3
				L1_1_b_PEO	[People] - People are not fully aware of the security or safety risks that may concern them.	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	CPS.AT-1
						Improve the contents of training and education regarding security to members of the organization and other relevant parties of high importance in security management of the organization.	CPS.AT-3
					[People] - The security or safety risks that involve people are not managed adequately.	Formulate and manage security requirements applicable to members of other relevant organizations, such as business partners, who are engaged in operations outsourced from the organization.	CPS.SC-5
						Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.	CPS.IP-9
				L1_1_b_COM	[Components] - The security status of components that compose information systems and Industrial control systems and the status of network connections are not managed appropriately (e.g. Inventory of assets, monitoring).	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	CPS.AM-1
						Create and manage appropriately a list of external information systems where the organization's assets are shared.	CPS.AM-5
						Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	CPS.AC-1
						Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.	CPS.AE-1
						Monitor communication with external service providers so that potential security events can be detected properly.	CPS.CM-5
						As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	CPS.CM-6
				L1_1_b_SYS	[System] - The organization has not implemented technical measures considering risks, or cannot confirm such implementation.	Identify the vulnerability of the organization's assets and document the list of identified vulnerability with the corresponding asset.	CPS.RA-1
						Identify and document the assumed security incidents, those impacts on the oraganization's assets, and the causes of those.	CPS.RA-3
						- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation. - Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.	CPS.RA-4
						Consider threats, vulnerability, likelihood, and impacts when assessing risks.	CPS.RA-5
						- On the basis of the results of the risk assessment, clearly define the details of measures to prevent possible security risks, and document the organized outcome from the scope and priorities of the measures.	CPS.RA-6
						Determine the organization's risk tolerance level based on the result of the risk assessment and its role in the supply chain.	CPS.RM-2
					[System] - Settings in the system where the data to be protected is stored are not secure.	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	CPS.IP-1
						Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.	CPS.PT-2
					[System] - Regarding access to stored information, a request sender is not identified / authenticated in a manner suited to the level of confidentiality of such information.	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	CPS.GV-3
						Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	CPS.AC-1
						Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions)	CPS.AC-5
						Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.	CPS.AC-6
						Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	CPS.AC-9
					[System] - The system does not have a mechanism to quickly detect and respond to anomalies on the network (eg. spoofing, message tampering)	Identify the security events accurately by implementing the procedure to conduct a correlation analysis of the security events and comparative analysis with the threat information obtained from outside the organization.	CPS.AE-3
						- Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.	CPS.CM-3
						Continuously improve the process of detecting security events.	CPS.DP-4

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
				L1_1_b_PRO	[Procedure] - Appropriate procedures for security risk management have not been established.	Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.	CPS.GV-1
						Develop a strategy and secure resources to implement risk management regarding security.	CPS.GV-4
						Confirm the implementation status of the organization's' cyber security risk management and communicate the results to appropriate parties within the organization (e.g. senior management). Define the scope of responsibilities of the organization and the relevant parties (e.g. subcontractor), and establish and implement the process to confirm the implementation status of security risk management of relevant parties.	CPS.RM-1
						When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-3
						When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-4
						Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6
						Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.	CPS.SC-7
						Develop and manage a procedure to be executed when a contract with other relevant organizations such as business partners is finished. (e.g., expiration of contract period, end of support)	CPS.SC-10
						Continuously improve the standard of security measures relevant to the supply chain, related procedures, and so on.	CPS.SC-11
						Assess the lessons learned from security incident response and the results of monitoring, measuring, and evaluating internal and external attacks, and improve the processes of protecting the assets.	CPS.IP-7
				L1_1_b_DAT	[Data] - Data are not protected enough in communication paths.	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.	CPS.DS-3
						Encrypt information itself when sending/receiving information.	CPS.DS-4
					[Data] - Data being handled have no mechanism to detect falsification.	Perform integrity checking on information to be sent, received, and stored.	CPS.DS-11
		The system dealing with the data of its own organization stops due to a denial of service attack, ransomware infection etc..	- DoS attacks on computer equipment and communication devices (e.g., servers) that comprise a system - Malware infection exploiting security vulnerabilities in the system - Transmission of jamming waves	L1_1_c_ORG	[Organization] - Security risks are not managed in accordance with appropriate procedures, and other organizations needed are not involved in risk management.	Classify and prioritize resources (e.g., People, Components, Data, and System) by function, importance, and business value, and communicate to the organizations and people relevant to those resources in business.	CPS.AM-6
						Define policies and standard measures regarding security that are consistent with the high-priority business and operations of the organization, and share them with parties relevant to the organization's business (including suppliers and third-party providers).	CPS.BE-2
						Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.	CPS.SC-1
						Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.	CPS.SC-2
						Introduce the system development life cycle to manage the systems.	CPS.IP-3
				L1_1_c_PEO	[People] - People are not fully aware of the security or safety risks that may concern them.	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	CPS.AT-1
						Improve the contents of training and education regarding security to members of the organization and other relevant parties of high importance in security management of the organization.	CPS.AT-3
					[People] - The security or safety risks that involve people are not managed adequately.	Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.	CPS.SC-8
						Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.	CPS.IP-9
				L1_1_c_COM	[Components] - The security status of components that compose information systems and Industrial control systems and the status of network connections are not managed appropriately (e.g. Inventory of assets, monitoring).	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	CPS.AM-1
						Create and manage appropriately a list of external information systems where the organization's assets are shared.	CPS.AM-5
						Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	CPS.AC-1
						Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.	CPS.AE-1
						Monitor communication with external service providers so that potential security events can be detected properly.	CPS.CM-5
						As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	CPS.CM-6
				L1_1_c_SYS	[System] - The organization has not implemented technical measures considering risks, or cannot confirm such implementation.	Identify the vulnerability of the organization's assets and document the list of identified vulnerability with the corresponding asset.	CPS.RA-1
						Identify and document the assumed security incidents, those impacts on the oraganization's assets, and the causes of those.	CPS.RA-3
						- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation.	CPS.RA-4
						Consider threats, vulnerability, likelihood, and impacts when assessing risks.	CPS.RA-5
						- On the basis of the results of the risk assessment, clearly define the details of measures to prevent possible security risks, and document the organized outcome from the scope and priorities of the measures.	CPS.RA-6
						Determine the organization's risk tolerance level based on the result of the risk assessment and its role in the supply chain.	CPS.RM-2
					[System] - Communications to IoT devices, servers, etc. are not properly controlled.	Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.	CPS.PT-2
						Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.	CPS.CM-1
					[System] - The system does not cope with physical interference (e.g. jamming waves) to IoT devices and servers.	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	CPS.AC-2
						Implement physical measures such as preparing an uninterruptible power supply, a fire protection facility, and protection from water infiltration to follow the policies and rules related to the physical operating environment, including the IoT devices and servers installed in the organization.	CPS.IP-5
						Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.	CPS.CM-2
					[System] - A system that contains IoT devices does not have adequate resources (i.e., processing capacity, communication bandwidths, and storage capacity)	Secure sufficient resources (e.g., People, Components, system) for components and systems, and protect assets property to minimize bad effects under cyber attack (e.g., DoS attack).	CPS.DS-6
						Carry out periodic quality checks, prepare standby devices and uninterruptible power supplies, provide redundancy, detect failures, conduct replacement work, and update software for IoT devices, communication devices, circuits, etc.	CPS.DS-7

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
				L1_1_c_PRO	[Procedure] - Appropriate procedures for security risk management have not been established.	Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.	CPS.GV-1
						Develop a strategy and secure resources to implement risk management regarding security.	CPS.GV-4
						Confirm the implementation status of the organization's' cyber security risk management and communicate the results to appropriate parties within the organization (e.g. senior management). Define the scope of responsibilities of the organization and the relevant parties (e.g. subcontractor), and establish and implement the process to confirm the implementation status of security risk management of relevant parties.	CPS.RM-1
						When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-3
						When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-4
						Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6
						Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.	CPS.SC-7
						Develop and manage a procedure to be executed when a contract with other relevant organizations such as business partners is finished. (e.g., expiration of contract period, end of support)	CPS.SC-10
						Continuously improve the standard of security measures relevant to the supply chain, related procedures, and so on.	CPS.SC-11
						Assess the lessons learned from security incident response and the results of monitoring, measuring, and evaluating internal and external attacks, and improve the processes of protecting the assets.	CPS.IP-7
		Security measures that satisfy the legal requirements for a system cannot be implemented	All threats	L1_2_a_ORG	[Organization] - The organization is unaware of legal systems with which it should comply, or it has not developed, or is not operating internal rules that conform to the legal systems.	Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.	CPS.GV-2
						Detect security events in the monitoring process, in compliance with applicable local regulations, directives, industry standards, and other rules.	CPS.DP-2
				L1_2_a_PEO	[People] - People are unaware of legal systems with which it should comply, or they do not follow internal rules that conform to the legal systems.	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	CPS.AT-1
				L1_2_a_COM	[Components] - The type of components that must receive certain protection under a legal system is not provided with the required level of protection.	Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.	CPS.GV-2
				L1_2_a_SYS	[System] - The type of system that must receive certain protection under a legal system is not provided with the required level of protection.	Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.	CPS.GV-2
				L1_2_a_PRO	[Procedure] - Established internal procedures are not designed to ensure compliance with laws and regulations.	Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.	CPS.GV-2
				L1_2_a_DAT	[Data] - The type of data that must receive certain protection under a legal system is not provided with the required level of protection.	Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.	CPS.GV-2
1_2	Continuing the business of the organization appropriately even when a security incident occurs.	The organization's security incidents prevent their business from continuing properly	All threats	L1_3_a_ORG	[Organization] - The organization has not established a framework for accurately detecting security incidents.	Appoint a chief security officer, establish a security management team (SOC/CSIRT), and prepare a system within the organization to detect, analyze, and respond to security events.	CPS.AE-2
						The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.), analyzes the information, and establishes a process to implement and use measures.	CPS.RA-2
						Clarify the role and responsibility of the organization as well as service providers in detecting security events so that they can fulfill their accountabilities.	CPS.DP-1
						Detect security events in the monitoring process, in compliance with applicable local regulations, directives, industry standards, and other rules.	CPS.DP-2
						As part of the monitoring process, test regularly if the functions for detecting security events work as intended, and validate these functions.	CPS.DP-3
						Continuously improve the process of detecting security events.	CPS.DP-4
					[Organization] - The organization has not established a framework for accurately handling security incidents.	The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.), analyzes the information, and establishes a process to implement and use measures.	CPS.RA-2
						Appoint a chief security officer, establish a security management team (SOC/CSIRT), and prepare a system within the organization to detect, analyze, and respond to security events.	CPS.AE-2
						Review the lessons learned from the responses to security incidents, and continuously improve the security operation process.	CPS.IM-1
						Review the lessons learned from the responses to security incidents, and continuously improve the business continuity plan or emergency response plan.	CPS.IM-2
				L1_3_a_PEO	[People] - People are unable to take appropriate action when a security incident arises.	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	CPS.AT-1
						Improve the contents of training and education regarding security to members of the organization and other relevant parties of high importance in security management of the organization.	CPS.AT-3
						Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.	CPS.RP-1
				L1_3_a_COM	[Components] - The scope of the organization's business (e.g., products) damaged by a security incident cannot be identified.	Specify a method to ensure traceability based on the importance of the components produced by the organization's supply chain.	CPS.AM-2
						Create records such as the date of production and condition of components depending on importance, and prepare and adopt internal rules regarding records of production activities in order to store components for a certain period of time.	CPS.AM-3
						Understand the impact of the security incident on the whole society including the organization and relevant parties such as partners based on the full account of the incident and the probable intent of the attacker.	CPS.AN-1
				L1_3_a_SYS	[System] - Devices or other tools for accurately detecting security incidents are not installed or not correctly operated.	Identify the security events accurately by implementing the procedure to conduct a correlation analysis of the security events and comparative analysis with the threat information obtained from outside the organization.	CPS.AE-3
						Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.	CPS.CM-1
						As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	CPS.CM-6

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
				L1_3_a_PRO	[Procedure] - The organization has not developed internal procedures for security incident handling.	Specify the criteria to determine the risk degree of security events.	CPS.AE-5
						Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.	CPS.RP-1
						Understand the impact of the security incident on the whole society including the organization and relevant parties such as partners based on the full account of the incident and the probable intent of the attacker.	CPS.AN-1
						Implement digital forensics upon the occurrence of the security incident.	CPS.AN-2
						Categorize and store information regarding the detected security incidents by the size of security-related impact, penetration vector, and other factors.	CPS.AN-3
						Take measures to minimize security-related damages and mitigate the impacts caused by such incident.	CPS.MI-1
					[Procedure] - Security incidents are not treated in the business continuity plan. This means a highly hazardous security incident hinders the organization's business continuity when it occurs.	Include security incidents in the business continuity plan or emergency response plan that outlines the action plans and response procedures to take in case of natural disasters.	CPS.RP-3
						Develop and manage rules regarding publishing information after the occurrence of the security incident.	CPS.CO-1
						Include the item in the business continuity plan or emergency response plan to the effect that the organization shall work to restore its social reputation after the occurrence of a high-risk security incident.	CPS.CO-2
						Include the item in the business continuity plan or emergency response plan to the effect that the details of the recovery activities shall be communicated to the internal and external stakeholders, executives, and management.	CPS.CO-3
				L1_3_a_DAT	[Data] - Data necessary to continue the business at the time of the security incident has not been properly backed up, or has been backed up but does not function properly.	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	CPS.AT-1
						Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.	CPS.AT-2
						Perform a periodical system backup and testing of components (e.g., IoT devices, communication devices, and circuits).	CPS.IP-4
						Include security incidents in the business continuity plan or emergency response plan that outlines the action plans and response procedures to take in case of natural disasters.	CPS.RP-3
		Other relevant organizations cannot continue their business properly due to the organization's security incidents	All threats	L1_3_b_ORG	[Organization] - The organization is unclear about how its components, systems, and/or data have been working with other organizations in cyberspace.	Create and manage appropriately network configuration diagrams and data flows within the organization.	CPS.AM-4
						Create and manage appropriately a list of external information systems where the organization's assets are shared.	CPS.AM-5
						Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.	CPS.AE-1
						As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	CPS.CM-6
						Monitor communication with external service providers so that potential security events can be detected properly.	CPS.CM-5
					[Organization] - The organization is unclear about how it has been working with other organizations (e.g., suppliers) in physical space.	Define roles and responsibilities for cyber security across the organization and other relevant parties.	CPS.AM-7
						Identify and share the role of the organizations in the supply chain.	CPS.BE-1
						Identify the dependency between the organization and other relevant parties and the important functions of each in the course of running the operation.	CPS.BE-3
						Confirm the implementation status of the organization's' cyber security risk management and communicate the results to appropriate parties within the organization (e.g. senior management). Define the scope of responsibilities of the organization and the relevant parties (e.g. subcontractor), and establish and implement the process to confirm the implementation status of security risk management of relevant parties.	CPS.RM-1
				L1_3_b_PEO	[People] - People in other organizations are unable to take appropriate action when the organization has a security incident.	Prepare and test a procedure for incident response with relevant parties involved in the incident response activitiy to ensure action for incident response in the supply chain.	CPS.SC-9
						Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.	CPS.AT-2
						Improve the contents of training and education regarding security to members of the organization and other relevant parties of high importance in security management of the organization.	CPS.AT-3
						As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.	CPS.RP-2
				L1_3_b_COM	[Components] - A security incident causes damage to components (products) and/or services.	Take appropriate measures on goods (products) whose quality is expected to be affected by some reasons, including its production facility damaged by the occurrence of the security incident.	CPS.RP-4
					[Components] - The organization does not retain the records of components (products) (e.g., dates of manufacture, identification numbers, and delivery destinations) delivered to/from the organization.	Specify a method to ensure traceability based on the importance of the components produced by the organization's supply chain.	CPS.AM-2
						Create records such as the date of production and condition of components depending on importance, and prepare and adopt internal rules regarding records of production activities in order to store components for a certain period of time.	CPS.AM-3
				L1_3_b_PRO	[Procedure] - Procedures for security incident handling in cooperation with other relevant organizations have not been developed.	Identify the impact of security events, including the impact on other relevant organizations.	CPS.AE-4
						As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.	CPS.RP-2
		The organization's security incidents prevent the business of other relevant organizations from continuing properly	All threats	L1_3_c_ORG	[Organization] - The organization is unclear about how its components, systems, and/or data have been working with other organizations in cyberspace.	Create and manage appropriately network configuration diagrams and data flows within the organization.	CPS.AM-4
						Create and manage appropriately a list of external information systems where the organization's assets are shared.	CPS.AM-5
						Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.	CPS.AE-1
						Monitor communication with external service providers so that potential security events can be detected properly.	CPS.CM-5
						As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	CPS.CM-6
					[Organization] - The organization is unclear about how it has been working with other organizations (e.g., suppliers) in physical space.	Define roles and responsibilities for cyber security across the organization and other relevant parties.	CPS.AM-7
						Identify and share the role of the organizations in the supply chain.	CPS.BE-1
						Identify the dependency between the organization and other relevant parties and the important functions of each in the course of running the operation.	CPS.BE-3
						Confirm the implementation status of the organization's' cyber security risk management and communicate the results to appropriate parties within the organization (e.g. senior management). Define the scope of responsibilities of the organization and the relevant parties (e.g. subcontractor), and establish and implement the process to confirm the implementation status of security risk management of relevant parties.	CPS.RM-1
				L1_3_c_PEO	[People] - People in the organizations are unable to take appropriate action when other organizations have a security incident.	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	CPS.AT-1
						Improve the contents of training and education regarding security to members of the organization and other relevant parties of high importance in security management of the organization.	CPS.AT-3
						As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.	CPS.RP-2
				L1_3_c_PRO	[Procedure] - Procedures for security incident handling in cooperation with other relevant organizations have not been developed.	As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.	CPS.RP-2

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
1_3	Products or services in physical space are received or shipped with desired quality	A security event occurs in the channel for product / service provisioning, causing unintended quality deterioration such as malfunction of a device.	- Fraudulent falsification by internal or external people with malicious intent - Insertion of a counterfeit that imitates a genuine equipment	L1_1_d_ORG	[Organization] - The organization does not confirm the trustworthiness of products and services at the time of procurement.	When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-3
						When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-4
						Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.	CPS.SC-7
						Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.	CPS.SC-8
				L1_1_d_PEO	[People] - The organizatioin's staff in charge of procurement are not fully aware of security risks related to procurement.	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	CPS.AT-1
				L1_1_d_COM	[Components] - Physical protection measures are not sufficiently applied to procured products and services.	When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-4
						When handling information to be protected or procuring devices that have an important function to the organization, useselect the IoT devices and servers equipped with anti-tampering devices.	CPS.DS-8
				L1_1_d_PRO	[Procedure] - There is no procedure for confirming the qualification of procured goods at the time of procurement of products and services.	Perform integrity checking on information to be sent, received, and stored.	CPS.DS-11
						Introduce an integrity check mechanism to verify the integrity of hardware.	CPS.DS-12
						Confirm that IoT devices and software are genuine products during the booting-up process.	CPS.DS-13

■ Functions/Assumed Security Incidents/Risk Sources/Measure Requirements in the Second Layer

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
2_Common	Both of the following functions; - Function to read events in physical space and translating them into digital data and sending the data to cyberspace in accordance with certain rules - Function to control components and displaying visualized data based on data received from cyberspace in accordance with certain rules	Unexpected behavior of the IoT device due to unauthorized access to its controls by exploiting a vulnerability results in unpredicted operation	- Malware infection using an attack tool that takes advantage of an IoT device's vulnerability	L2_1_a_ORG	[Organization] - The organization is unclear about the status of the security measures (e.g., software configurations; the status of patches applied) for its IoT devices connecting to information systems and industrial control systems.	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	CPS.AM-1
						Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	CPS.IP-1
						Restrict the software to be added after installing in the IoT devices and servers.	CPS.IP-2
						As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	CPS.CM-6
					[Organization] - The organization does not collect or analyze information about threats and vulnerability related to the IoT devices it uses.	The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.), analyzes the information, and establishes a process to implement and use measures.	CPS.RA-2
						Assess the lessons learned from security incident response and the results of monitoring, measuring, and evaluating internal and external attacks, and improve the processes of protecting the assets.	CPS.IP-7
						Share information regarding the effectiveness of data protection technologies with appropriate partners.	CPS.IP-8
						Develop a vulnerability remediation plan, and modify the vulnerability of the components according to the plan.	CPS.IP-10
						- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updateswith managed tools properly and in a timely manner while recording the history. - Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable.	CPS.MA-1
						- Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable.	CPS.MA-1
						Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.	CPS.MA-2
				L2_1_a_COM	[Components] - IoT Devices in use do not have adequate security functions.	- Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.	CPS.RA-4
						- React accordingly to the security risks and the associated safety risks identified as a result of the assessment conducted at the planning and design phase of an IoT device and systems incorporating IoT devices.	CPS.RA-6
						When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-4
						Use products that provide measurable security in order to ensure the availability of security reporting and the trustworthiness of sensing data through integrity protection.	CPS.DS-15
				L2_1_a_PRO	[Procedure] - There is no procedure, at the time of procurement, for checking whether the goods have appropriate levels of security functions.	When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-4
						Use products that provide measurable security in order to ensure the availability of security reporting and the trustworthiness of sensing data through integrity protection.	CPS.DS-15
						- Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.	CPS.RA-4
						- React accordingly to the security risks and the associated safety risks identified as a result of the assessment conducted at the planning and design phase of an IoT device and systems incorporating IoT devices.	CPS.RA-6
					[Procedure] - The response procedure after detecting malfunction of the IoT device is not defined.	Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.	CPS.RP-1
		Unexpected behavior of the IoT device due to unauthorized access to its controls by impersonation of an authorized user results in unpredicted operation	- Identity spoofing using a stolen ID of a proper host - Unauthorized access that exploits vulnerable protocols with no security means	L2_1_b_ORG	[Organization] - The organization has no mechanism for regularly checking proper use of its network.	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	CPS.PT-1
						Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.	CPS.AE-1
						Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.	CPS.CM-1
				L2_1_b_COM	[Components] - Some settings are not robust enough in terms of security (e.g., passwords, ports).	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	CPS.IP-1
						Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.	CPS.PT-2
				L2_1_b_SYS	[System] - Access control of communication partners is not robust enough.	Prevent unauthorized log-in to IoT devices and servers by measures such as implementing functions for lockout after a specified number of incorrect log-in attempts and providing a time interval until safety is ensured.	CPS.AC-4
						Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).	CPS.AC-7
						Restrict communications by IoT devices and servers to those with entities (e.g. people, components, system, etc.) identified through proper procedures.	CPS.AC-8
						Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	CPS.AC-9
				L2_1_b_PRO	[Procedure] - No procedure for security settings of an IoT device is established.	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	CPS.IP-1
					[Procedure] - The response procedure after detecting malfunction of the IoT device is not defined.	Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.	CPS.RP-1

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
		Unauthorized input to the IoT device due to unauthorized access to the system that remotely manages the IoT devices results in unpredicted operation	- Malware infection that takes advantage of a system's vulnerability - Identity spoofing using a stolen ID/password of a proper user - Unauthorized command from system managing IoT device to IoT device	L2_1_c_ORG	[Organization] - The organization is unclear about the status of the security measures (e.g., software configurations; the status of patches applied) for its system that manages IoT devices.	As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	CPS.CM-6
				L2_1_c_SYS	[System] - Access control regarding system administration authority is not robust enough.	Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions)	CPS.AC-5
						Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.	CPS.AC-6
					[System] - Access control regarding system administration authority is not robust enough.	The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.), analyzes the information, and establishes a process to implement and use measures.	CPS.RA-2
						Restrict the software to be added after installing in the IoT devices and servers.	CPS.IP-2
						- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updateswith managed tools properly and in a timely manner while recording the history.	CPS.MA-1
						- Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable.	CPS.MA-1
						Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.	CPS.MA-2
						As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	CPS.CM-6
						Confirm the existence of vulnerability that requires a regular check-up in IoT devices and servers managed within the organization.	CPS.CM-7
					[Procedure] - The response procedure after detecting malfunction of the IoT device is not defined.	Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.	CPS.RP-1
		Functions of IoT devices and communication devices stop due to attacks such as denial-of-service (DoS) attack	- DoS attacks on IoT and communication devices that comprise an IoT system	L2_1_d_SYS	[System] - A system that contains IoT devices does not have adequate resources (i.e., processing capacity, communication bandwidths, and storage capacity)	Secure sufficient resources (e.g., People, Components, system) for components and systems, and protect assets property to minimize bad effects under cyber attack (e.g., DoS attack).	CPS.DS-6
						Carry out periodic quality checks, prepare standby devices and uninterruptible power supplies, provide redundancy, detect failures, conduct replacement work, and update software for IoT devices, communication devices, circuits, etc.	CPS.DS-7
						Perform a periodical system backup and testing of components (e.g., IoT devices, communication devices, and circuits).	CPS.IP-4
					[Procedure] - The response procedure after detecting the stopping of the IoT device is not defined.	Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.	CPS.RP-1
2_1	Function to control components and displaying visualized data based on data received from cyberspace in accordance with certain rules	Behavior that threatens safety, regardless of the behavior being normal or abnormal	- Command injection by an unauthorized entity - Unacceptable input data from cyberspace - Tampering control signal by malware	L2_2_a_ORG	[Organization] - The organization does not check whether the devices have proper levels of safety functions at the time of procurement.	- Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.	CPS.RA-4
						When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-4
						Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.	CPS.SC-7
						Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.	CPS.SC-8
						Introduce IoT devices that implement safety functions, assuming that these devices are connected to the network.	CPS.PT-3
				L2_2_a_COM	[Components] - There is no mechanism for verifying data that has been input.	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.	CPS.CM-3
				L2_2_a_SYS	[System] - Safety instrument is not considered in the system being operated.	- Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.	CPS.RA-4
						- On the basis of the results of the risk assessment, clearly define the details of measures to prevent possible security risks, and document the organized outcome from the scope and priorities of the measures. - React accordingly to the security risks and the associated safety risks identified as a result of the assessment conducted at the planning and design phase of an IoT device and systems incorporating IoT devices.	CPS.RA-6
				L2_2_a_PRO	[Procedure] - The organization has no established courses of action to take when any of its devices shows a sign of compromising safety.	Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.	CPS.RP-1
2_2	Function to read events in physical space and translating them into digital data and sending the data to cyberspace in accordance with certain rules	Data is tampered with in the communication path between the IoT device and cyberspace	- Man-in-the-middle attack that tamper with data on communication channnel.	L2_3_a_ORG	[Organization] - The organization does not check whether the devices have functions to detect and prevent tampering at the time of procurement.	When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-4
						Use products that provide measurable security in order to ensure the availability of security reporting and the trustworthiness of sensing data through integrity protection.	CPS.DS-15
		An unauthorized or tampered-with IoT device connects to the network and transmits incorrect data	- A stolen and illegally modified IoT device connected to a network - Tampering by internal or external people with malicious intent - Tampering with sensor readings, thresholds, and settings	L2_3_b_ORG	[Organization] - The organization is unclear about the status of devices connected to its information system or industrial control system.	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	CPS.AM-1
						Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	CPS.IP-1
						As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	CPS.CM-6
				L2_3_b_PEO	[People] - Physical unauthorized acts to IoT devices by internal or external people can not be prevented.	Formulate and manage security requirements applicable to members of other relevant organizations, such as business partners, who are engaged in operations outsourced from the organization.	CPS.SC-5
						Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	CPS.AC-2
						Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.	CPS.CM-2
				L2_3_b_COM	[Components] - The devices used are not anti-tampering, which make it impossible to prevent physical falsification.	When handling information to be protected or procuring devices that have an important function to the organization, useselect the IoT devices and servers equipped with anti-tampering devices.	CPS.DS-8
				L2_3_b_SYS	[System] - The organization does not regularly verify the integrity of connected devices.	Conduct integrity checks of software runnning on the IoT devices and servers at a time determined by the organization, and prevent unauthorized software from launching.	CPS.DS-10
						Introduce an integrity check mechanism to verify the integrity of hardware.	CPS.DS-12
					[System] - It is not properly detected that an unauthorized device is connected to the network of the organization.	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	CPS.AM-1
						As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	CPS.CM-6
					[System] - The organization does not take physical security measures such as access control and monitoring of areas where its IoT devices are installed,	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	CPS.AC-2
						Implement physical measures such as preparing an uninterruptible power supply, a fire protection facility, and protection from water infiltration to follow the policies and rules related to the physical operating environment, including the IoT devices and servers installed in the organization.	CPS.IP-5
						Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.	CPS.PT-2
						Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.	CPS.CM-2
				L2_3_b_DAT	[Data] - The organization has no procedures for deleting data (or making data unreadable) in an IoT device before disposal.	When disposing of an IoT device and server, delete the stored data and the ID (identifier) uniquely identifying the genuine IoT devices and servers as well as important information (e.g., private key and digital certificate), or make them unreadable.	CPS.IP-6

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
		An IoT device with low quality is connected to a network, causing failures, transmission of inaccurate data or transmission to unauthorized entity .	- An IoT device with low quality connected to a network - Insertion of a counterfeit that imitates a genuine equipment	L2_3_c_ORG	[Organization] - The organization does not check whether the products are trustworthy at the time of procurement of IoT devices.	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.	CPS.SC-2
						When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-3
						When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-4
						Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6
						Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.	CPS.SC-7
						Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.	CPS.SC-8
					[Organization] - The organization does not make certain that the IoT devices and their software are official products (i.e., not falsified).	Confirm that IoT devices and software are genuine products during the booting-up process.	CPS.DS-13
				L2_3_c_SYS	[System] - Network communications (wired or wireless) from unauthorized devices can not be prevented.	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	CPS.AC-2
						Properly authorize wireless connection destinations (including users, IoT devices, and servers).	CPS.AC-3
						As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other “organization”, people, components, and systems.	CPS.CM-6
					[System] - The system cannot properly detect and block unauthorized outbound communication from the organization.	Properly control outbound communications that send information to be protected to prevent improper data breach.	CPS.DS-9
						Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.	CPS.CM-1
						As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other “organization”, people, components, and systems.	CPS.CM-6
					[System] - The organization has implemented no mechanism for checking whether the devices to be connected to cyberspace and other official devices are official products.	Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	CPS.AC-1
						Confirm that IoT devices and software are genuine products during the booting-up process.	CPS.DS-13
				L2_3_c_PRO	[Procedure] - There is no procedure for checking whether the procured products are reliable at the time of procurement of IoT devices.	When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-4
						Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6
						Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.	CPS.SC-7
						Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.	CPS.SC-8
		Inappropriate measurement occurs due to physical interference with measurement .	Inappropriate acts against transcription function by people with malicious intent	L2_3_d_ORG	[Organization] - The organization does not check whether the products are trustworthy in the measurement security at the time of procurement of IoT devices.	When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-4
						Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6
						Use products that provide measurable security in order to ensure the availability of security reporting and the trustworthiness of sensing data through integrity protection.	CPS.DS-15
				L2_3_d_SYS	[System] - The organization does not take physical security measures such as access control and monitoring of areas where its IoT devices are installed.	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	CPS.AC-2
						Implement physical measures such as preparing an uninterruptible power supply, a fire protection facility, and protection from water infiltration to follow the policies and rules related to the physical operating environment, including the IoT devices and servers installed in the organization.	CPS.IP-5
						Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.	CPS.CM-2

■ Functions/Assumed Security Incidents/Risk Sources/Measure Requirements in the Third Layer

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
3_Common	All of the following functions; - Functions to securely send and receive data - Functions to securely process and analyze data - Function to securely store data	- Denial-of-Service (DoS) attacks on computer equipment and communication devices (e.g., servers) that comprise a system	- DoS attack on computing devices such as servers, communication devices, etc. - Transmission of jamming waves	L3_3_b_ORG	[Organization] - The organization does not confirm the trustworthiness of contractor organizations such as data providers or data manipulators/analyzers before and after signing contracts.	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.	CPS.SC-2
						When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-3
						When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-4
						Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6
						Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.	CPS.SC-7
						Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.	CPS.SC-8
		The system that handles data stops whether it has been attacked or not.	- Services provided by a system with low quality/trustworthiness	L3_3_c_ORG	[Organization] - The organization does not confirm the trustworthiness of service supplier's organizations, systems, etc. before and after signing contracts.	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.	CPS.SC-2
						When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-3
						When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-4
						Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6
						Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.	CPS.SC-7
						Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.	CPS.SC-8
				L3_3_c_SYS	[System] - A system that contains IoT devices does not have adequate resources (i.e., processing capacity, communication bandwidths, and storage capacity)	Secure sufficient resources (e.g., People, Components, system) for components and systems, and protect assets property to minimize bad effects under cyber attack (e.g., DoS attack).	CPS.DS-6
						Carry out periodic quality checks, prepare standby devices and uninterruptible power supplies, provide redundancy, detect failures, conduct replacement work, and update software for IoT devices, communication devices, circuits, etc.	CPS.DS-7
						Perform a periodical system backup and testing of components (e.g., IoT devices, communication devices, and circuits).	CPS.IP-4
		Laws and rules that prescribe data protection in cyberspace are violated	- Malware infection that takes advantage of a data storage system's vulnerability - Physical intrusion by an unauthorized entity into the data storage area - Identity spoofing using a stolen ID/password of a proper user	L3_4_a_ORG	[Organization] - Responsibility in the organization for managing data to be protected is not identified.	Classify and prioritize resources (e.g., People, Components, Data, and System) by function, importance, and business value, and communicate to the organizations and people relevant to those resources in business.	CPS.AM-6
					[Organization] - The organization is not fully aware of data protection laws and regulations with which it should comply.	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	CPS.GV-3
				L3_4_a_PEO	[People] - People involved are not fully aware of how the organization's protected data should be handled for security reasons.	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	CPS.AT-1
						Improve the contents of training and education regarding security to members of the organization and other relevant parties of high importance in security management of the organization.	CPS.AT-3
				L3_4_a_PRO	[Procedure] - Necessary procedures for handling data are not established.	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	CPS.GV-3
					[Procedure] - The organization does not confirm whether the necessary procedures are followed regarding data handling.	Maintain, update, and manage information such as the origination of data and data processing history throughout the entire life cycle.	CPS.DS-14
				L3_4_a_DAT	[Data] - Personal data or other important information is distributed among multiple organizations or systems.	When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-3
						Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6
					[Data] - The organization is unaware that the data it handles is the specific type of data that must be protected.	If the organization exchanges protected information with other organizations, agree in advance on security requirements for protection of such information.	CPS.DS-1
		The security requirements for highly confidential data to be shared only among authorized parties has not been set or met.	- Malware infection that takes advantage of a data storage system's vulnerability - Physical intrusion by an unauthorized entity into the data storage area - Internal fraud by an authorized user - Identity spoofing using a stolen ID/password of a proper user	L3_4_b_ORG	[Organization] - The organization is not fully aware of data protection laws and regulations with which it should comply.	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	CPS.GV-3
				L3_4_b_PEO	[People] - People involved are not fully aware of how the organization's protected data should be handled for security reasons.	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	CPS.AT-1
						Improve the contents of training and education regarding security to members of the organization and other relevant parties of high importance in security management of the organization.	CPS.AT-3
				L3_4_b_PRO	[Procedure] - Necessary procedures for handling data are not established.	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	CPS.GV-3
					[Procedure] - The organization does not confirm whether the necessary procedures are followed regarding data handling.	Maintain, update, and manage information such as the origination of data and data processing history throughout the entire life cycle.	CPS.DS-14
				L3_4_b_SYS	[System] - The system is not designed according to the data confidentiality.	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).	CPS.AC-7
						Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	CPS.AC-9
						Encrypt information with an appropriate level of security strength, and store them.	CPS.DS-2
				L3_4_b_DAT	[Data] - Personal data or other important information is distributed among multiple organizations or systems.	When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-3
						Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6
					[Data] - The organization is unaware that the data it handles is the specific type of data that must be protected.	If the organization exchanges protected information with other organizations, agree in advance on security requirements for protection of such information.	CPS.DS-1
3_1	Functions to securely procecss and analyze data	The organization's protected data is leaked from a data processing area managed by a related organization.	- Malware infection that takes advantage of the vulnerability of a data manipulation /analysis system managed by another organization - Physical intrusion by an unauthorized entity into the data manipulation / analysis area managed by another organization - Identity spoofing using a stolen ID/password of a proper user - Protected data has been taken out improperly by another organization's entity	L3_1_b_ORG	[Organization] - The organization does not confirm the safeness and trustworthiness of data manipulation / analysis organizations and/or systems before and after signing contracts.	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.	CPS.SC-2
						When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-3
						When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-4
						Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6
						Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.	CPS.SC-7
						Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.	CPS.SC-8
				L3_1_b_PEO	[People] - The organization does not confirm, before and after signing contracts, the trustworthiness of people in organizations that undertake data manipulation / analysis.	Formulate and manage security requirements applicable to members of other relevant organizations, such as business partners, who are engaged in operations outsourced from the organization.	CPS.SC-5
				L3_1_b_DAT	[Data] - The organization's data that must be protected is distributed among multiple organizations at different levels of security.	When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-3
						Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
		Improper processed/analyzed results become output due to a malfunction in the data processing/analyzing system	- Malware infection that takes advantage of vulnerability of a data manipulation / analysis system - Unacceptable input data containing code to attack a data manipulation / analysis system	L3_3_d_ORG	[Organization] - The organization does not confirm the safeness of data manipulation / analysis organizations and/or systems before and after signing contracts.	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.	CPS.SC-2
						When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-3
						When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-4
						Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6
						Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.	CPS.SC-7
						Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.	CPS.SC-8
				L3_3_d_SYS	[System] - Settings in the system that processes and analyzes data are not secure.	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	CPS.IP-1
						Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.	CPS.PT-2
					[System] - Vulnerabilities that should be handled is left unaddressed in a data manipulation / analysis system.	The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.), analyzes the information, and establishes a process to implement and use measures.	CPS.RA-2
						Restrict the software to be added after installing in the IoT devices and servers.	CPS.IP-2
						Develop a vulnerability remediation plan, and modify the vulnerability of the components according to the plan.	CPS.IP-10
						- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updateswith managed tools properly and in a timely manner while recording the history.	CPS.MA-1
						Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.	CPS.MA-2
						As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other “organization”, people, components, and systems.	CPS.CM-6
						Confirm the existence of vulnerability that requires a regular check-up in IoT devices and servers managed within the organization.	CPS.CM-7
					[System] - Data are not protected enough in a system.	Encrypt information with an appropriate level of security strength, and store them.	CPS.DS-2
						Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.	CPS.DS-3
						Encrypt information itself when sending/receiving information.	CPS.DS-4
					[System] The system does not fully check data that serves as input.	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.	CPS.CM-3
						Validate the integrity and authenticity of the information provided from cyberspace before operations.	CPS.CM-4
					[System] - The system has no mechanism for detecting and handling any abnormality related to security as soon as it arises.	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	CPS.PT-1
						Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.	CPS.AE-1
						Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.	CPS.CM-1
						Monitor communication with external service providers so that potential security events can be detected properly.	CPS.CM-5
						Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.	CPS.RP-1
3_2	Function to securely store data	A related organization’s protected data is leaked from a data storage area managed by the organization.	- Malware infection that takes advantage of the vulnerability of a data storage system manageed by another organization - Physical intrusion by an unauthorized entity into the data storage area managed by another organization - Identity spoofing using a stolen ID/password of a proper user - Protected data has been taken out improperly by a mallicious entity of the organization	L3_1_a_ORG	[Organization] - Responsibility in the organization for managing data to be protected is not identified.	Classify and prioritize resources (e.g., People, Components, Data, and System) by function, importance, and business value, and communicate to the organizations and people relevant to those resources in business.	CPS.AM-6
				L3_1_a_SYS	[System] - Settings in the system storing data to be protected of relevant parties are not secure.	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	CPS.IP-1
						Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.	CPS.PT-2
					[System] - Vulnerabilities that should be handled is left unaddressed in the organization's system.	The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.), analyzes the information, and establishes a process to implement and use measures.	CPS.RA-2
						Restrict the software to be added after installing in the IoT devices and servers.	CPS.IP-2
						Develop a vulnerability remediation plan, and modify the vulnerability of the components according to the plan.	CPS.IP-10
						- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updateswith managed tools properly and in a timely manner while recording the history.	CPS.MA-1
						Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.	CPS.MA-2
						As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other “organization”, people, components, and systems.	CPS.CM-6
						Confirm the existence of vulnerability that requires a regular check-up in IoT devices and servers managed within the organization.	CPS.CM-7
					[System] Regarding access to stored information, a request sender is not identified / authenticated in a manner suited to the level of confidentiality of such information.	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	CPS.GV-3
						Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	CPS.AC-1
						Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions)	CPS.AC-5
						Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.	CPS.AC-6
						Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	CPS.AC-9
					[System] - The organization does not take physical security measures such as access control and monitoring of areas where its IoT devices and servers are installed.	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	CPS.AC-2
						Implement physical measures such as preparing an uninterruptible power supply, a fire protection facility, and protection from water infiltration to follow the policies and rules related to the physical operating environment, including the IoT devices and servers installed in the organization.	CPS.IP-5
						Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.	CPS.PT-2
						Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.	CPS.CM-2
					[System] - The system has no mechanism for detecting and handling any abnormality related to security as soon as it arises.	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	CPS.PT-1
						Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.	CPS.AE-1
						Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.	CPS.CM-1
						Monitor communication with external service providers so that potential security events can be detected properly.	CPS.CM-5
						Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.	CPS.RP-1
				L3_1_a_PRO	[Procedure] - There is no procedure for confirming levels of confidentiality and necessary security measures regarding data whose management is outsourced from other organizations.	If the organization exchanges protected information with other organizations, agree in advance on security requirements for protection of such information.	CPS.DS-1

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
				L3_1_a_DAT	[Data] - Classification concerning protection of data commissioned by relevant parties is not identified.	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	CPS.GV-3
					[Data] - Data protection at a predefined level of confidentiality is not implemented.	Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6
						Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).	CPS.AC-7
						Encrypt information with an appropriate level of security strength, and store them.	CPS.DS-2
						Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.	CPS.DS-3
						Encrypt information itself when sending/receiving information.	CPS.DS-4
						Securely control encryption keys throughout their life cycle to ensure proper operation and securely transmitted, received and stored data.	CPS.DS-5
						Properly control outbound communications that send information to be protected to prevent improper data breach.	CPS.DS-9
		The organization's protected data is leaked from a data storage area managed by a related organization.	- Malware infection that takes advantage of the vulnerability of a data storage system manageed by another organization - Physical intrusion by an unauthorized entity into the data storage area managed by another organization - Identity spoofing using a stolen ID/password of a proper user - Protected data has been taken out improperly by a mallicious entity of the organization	L3_1_c_ORG	[Organization] - The organization does not confirm the safeness of data storage organizations and/or systems before and after signing contracts.	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.	CPS.SC-2
						When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-3
						Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6
						Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.	CPS.SC-7
						Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.	CPS.SC-8
				L3_1_c_PEO	[People] - The organization does not confirm, before and after signing contracts, the trustworthiness of people in organizations that undertake data manipulation.	Formulate and manage security requirements applicable to members of other relevant organizations, such as business partners, who are engaged in operations outsourced from the organization.	CPS.SC-5
				L3_1_c_DAT	[Data] - The organization's data that must be protected is distributed among multiple organizations at different levels of security.	When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-3
						Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6
		Data in storage is tampered with	- Identity spoofing using a stolen ID/password of a proper user	L3_2_a_DAT	[Data] - Data being stored do not have a mechanism to detect falsifications.	Perform integrity checking on information to be sent, received, and stored.	CPS.DS-11
3_3	Functions to securely send and receive data	Data in use is tampered with.	- Identity spoofing using a stolen ID/password of a proper user - Man-in-the-middle attacks to falsify data on communication paths	L3_2_b_DAT	[Data] - Data are not protected enough in communication paths.	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.	CPS.DS-3
						Encrypt information itself when sending/receiving information.	CPS.DS-4
					[Data] - Data being used do not have a mechanism to detect falsifications.	Perform integrity checking on information to be sent, received, and stored.	CPS.DS-11
		The system receives inappropriate data from an Organization/People/Components (due to a spoofing attack etc.).	- Identity spoofing by an unauthorized organization/person/component/system to use an ID of a proper entity - Inappropriate data from authorized components and system that have been tampered with	L3_3_a_ORG	[Organization] - The organization does not confirm the trustworthiness of the data sender organizations such as data providers or data manipulators/analyzers before and after signing the contracts.	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.	CPS.SC-2
						When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-3
						When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	CPS.SC-4
						Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	CPS.SC-6
						Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.	CPS.SC-7
						Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.	CPS.SC-8
				L3_3_a_PEO	[People] - A contractor's employees responsible for the outsourced work are not fully aware of how the organization's protected data should be handled for security reasons.	Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.	CPS.AT-2
						Improve the contents of training and education regarding security to members of the organization and other relevant parties of high importance in security management of the organization.	CPS.AT-3
				L3_3_a_SYS	[System] - Vulnerabilities that should be handled is left unaddressed in a data collection / analysis system.	The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.), analyzes the information, and establishes a process to implement and use measures.	CPS.RA-2
						Restrict the software to be added after installing in the IoT devices and servers.	CPS.IP-2
						Develop a vulnerability remediation plan, and modify the vulnerability of the components according to the plan.	CPS.IP-10
						- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updateswith managed tools properly and in a timely manner while recording the history.	CPS.MA-1
						- Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable.	CPS.MA-1
						Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.	CPS.MA-2
						As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	CPS.CM-6
						Confirm the existence of vulnerability that requires a regular check-up in IoT devices and servers managed within the organization.	CPS.CM-7
					[System] - Communication channel is not appropriately protected.	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.	CPS.DS-3
					[System] - The organization's system has no mechanism for detecting and handling any abnormality related to security as soon as it arises.	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	CPS.PT-1
						Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.	CPS.AE-1
						Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.	CPS.CM-1
						Monitor communication with external service providers so that potential security events can be detected properly.	CPS.CM-5
						Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.	CPS.RP-1
					[System] - The system does not identify or authenticate the person on the other end of communication in cyberspace when the communication starts.	Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	CPS.AC-1
						Properly authorize wireless connection destinations (including users, IoT devices, and servers).	CPS.AC-3
						Prevent unauthorized log-in to IoT devices and servers by measures such as implementing functions for lockout after a specified number of incorrect log-in attempts and providing a time interval until safety is ensured.	CPS.AC-4
						Restrict communications by IoT devices and servers to those with entities (e.g. people, components, system, etc.) identified through proper procedures.	CPS.AC-8
						Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	CPS.AC-9
				L3_3_a_DAT	[Data] - No mechanism for filtering data sent from the other endpoint of communication is installed or operated.	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.	CPS.CM-3
						Validate the integrity and authenticity of the information provided from cyberspace before operations.	CPS.CM-4

Appendix C: Examples of security measures according to measure requirements

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.
- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.
- The subject that implements measures is classifed as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).
- In the description of the examples of measures, the documents described in “related standards, etc.” which are assigned to each requirement in Part 3 and a part of the corresponding items (shown as “Reference Guidelines” in the table) are referred.
- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	L1_1_a_COM, L1_1_b_COM, L1_1_c_COM, L2_1_a_ORG, L2_3_b_ORG, L2_3_b_SYS	<High-Advanced> -The organization identifies assets constituting its information systems and industrial control systems (hardware, including IoT devices; software; and information) uniquely, assigns a responsible person to each asset. And the organization maintains/manages lists periodically, or at the request of the operator including configuration information of assets (e.g., names, version information, license information, and location) while recognizing situations in real time. - The information system regularly audits whether the actual configuration grasped conforms to the baseline configuration defined by the organization, and responds appropriately. (Example: blocking unplanned connections except those permitted by the organization as an exception) -The information system and industrial control system implement and operate a mechanism which automatically detects and responses to unauthorized assets.	O/S	○ (3.4.2)	○ (In addition to the following, CM-8(1), CM-8(2), CM-8(3), CM-8(5))	○ (In addition to the following, A.8.1.3)	-	-
			<Advanced> - Maintain/manage lists including configuration information of assets (e.g., names, version information, license information, and location) by reviewing and updating them periodically. - The organization makes a list of removable media (e.g., USB memory sticks) that can be used on system components (information system or industrial control system), and manages the use of them. - The organization uses only removable media (e.g. USB memory) permitted in the organization. Also, if there is no identifiable ownwer of portable storage devices, the organization prohibits the use of such devices. - The organization controles access to the media that contain highly confidential data, and properly grasps and manages the usage of the media taken outside of the controlled areas.	O	○ (3.4.1, 3.8.5, 3.8.7, 3.8.8)	○ (CM-8, PM-5)		○ (4.2.3.4)	○ (SR 7.8)
			<Basic> - The organization identifies assets constituting its information system and industrial control system (hardware, software and information), assigns a responsible person to each asset, and documents a list of them. - It is desirable to list all the assets held, but if the target is huge, consider narrowing down the target assets through integration (grouping) of the analysis target and exclusion from the analysis target. - The organization sets priorities to the identified assets based on the importance of them in its business operation.	O			○ (A.8.1.1, A.8.1.2)		
CPS.AM-2	Specify a method to ensure traceability based on the importance of the components produced by the organization's supply chain.	L1_3_a_COM, L1_3_b_COM	<High-Advanced> - When traceability is a requirement, the organization manages a unique identification to outputs (products) and maintains documented necessary information for enabling traceability. ・It is desirable for the organization to consider a method of unique identification in accordance with the rules applicable to different industries such as cross-industry common numbering rules. [Reference] “ISO 9001:2015” 8.5.2 Identification and Traceability	O	-	-	-	-	-
			Common among <Advanced> and <Basic> - The organization prioritizes the products of the organization into multiple stages from the viewpoint of the following example. - Extent of the impact in the supply chain when problems (e.g. regarding product quality) are found. - Magnitude of the impact on the business of the organization when problems (e.g. regarding product quality) are found. - The organization specifies an appropriate method of identifying outputs (e.g., adding serial numbers) such as adding numbers depending on the importance of the components produced by the organization on its supply chain. - The organization identifies the conditions of outputs related to the requirements for monitoring and measuring throughout the processes of manufacturing and providing services.	O	-	-	-	-	-
CPS.AM-3	Create records such as the date of production and condition of components depending on importance, and prepare and adopt internal rules regarding records of production activities in order to store components for a certain period of time.	L1_3_a_COM, L1_3_b_COM	<High-Advanced> - The organization prepares internal rules related to production activities, and based on the possibility that records of produced components may be later audited in accordance with its importance, shares awareness with partners regarding importance in prior, and ensures an appropriate level of record management. - It is desirable that records of production activities that are created and managed can be quickly searched by production date, classification of components (e.g., product name), and the like.	O	-	-	-	-	-
			Common among <Advanced> and <Basic> - The organization creates a record such as the date of production and condition of components depending on the importance of the produced component on the supply chain, and prepares and manages internal rules of production activities in order to store components for a certain period of time. - The organization considers the following when creating or updating the above records. -Making an appropriate identification and description (eg title, date, documenter, reference number) -Recording in appropriate format (e.g., language, software version, charts) and media (e.g., paper, electronic media) -Obtaining appropriate reviews and approvals for relevance	O	-	-	-	-	-
CPS.AM-4	Create and manage appropriately network configuration diagrams and data flows within the organization.	L1_3_b_ORG, L1_3_c_ORG	<High-Advanced> - The organization implements/manages an automated mechanism for monitoring and managing system configurations, communication network configurations, and data flows of their information systems and industrial control systems in real time.	O	-	○ (In addition to the following, CM-2(2), CM-2(3))	○ (A.13.2.1, A13.2.2)	-	-
			<Advanced> - The organization states the characteristics of the interface, security requirements, and characteristics of transmitted data for network connection in a diagram in the associated documents.	O	-	○ (In addition to the following, CA-9)		-	-
			<Basic> - The organization documents and stores system configurations, communication network configurations, and data flows of an information systems and an industrial control systems in a range managed by the organization (for example, in units of business establishments). - The organization reviews related documents periodically or when there is a change in system configurations, network configurations, or data flows and updates them as necessary.	O	-	○ (CM-2, CM-2(1))		○ (4.2.3.4, 4.2.3.5)	-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.AM-5	Create and manage appropriately a list of external information systems where the organization's assets are shared.	L1_1_a_COM, L1_1_b_COM, L1_1_c_COM, L1_3_b_ORG, L1_3_c_ORG	<High-Advanced> - The system makes a list of external information services in use and manages the users, devices as well as serviced in use in real time. - The system uses a mechanism to give notice to the system administrator when an unpermitted external information system service is detected. - The organization identifies functions, ports, protocols, and other services which are necessary for using services offered by external providers.	O/S	○ (3.12.4)	○ (In addition to the following, SA-9(2))	○ (In addition to the following, A.13.1.2)	-	-
			<Advanced> - The organization sets conditions for allowing other organizations which own or operate external information systems to do the following: a. Accessing an information system in the organization from an external information system b. Processing, saving, or transmitting information under the control of the organization using an external information system - The organization restricts a use of storage in an external system the organization owns to an authorized one.	O	○ (3.1.20, 3.1.21, 3.12.4)	○ (In addition to the following, AC-20)		-	-
			<Basic> - The organization makes a list of external information system services in use and defines roles and responsibilities as users in each service. [Reference] Appendix A "Concret examples of contract provisions and commentaries" of "Guidebook for using Cloud Security Guideline" (METI, 2013) could be referred to regarding the points to consider when stipulating in the contract the roles and responsibilities of users especially in terms of usage of cloud service.	O	-	○ (SA-9)	○ (A.6.1.1)	-	-
CPS.AM-6	Classify and prioritize resources (e.g., People, Components, Data, and System) by function, importance, and business value, and communicate to the organizations and people relevant to those resources in business.	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG, L3_1_a_ORG, L3_4_a_ORG	Common among <High-Advanced> and <Advanced> - The organization considers business requirements and legal requirements which share or restrict data when classifying resources of the information system and industrial control system (data, components processing data, system, etc). - The person responsible for an asset is responsible for the classification of the data. - The organization includes classification rules and classification review standards after time passes in a resource classification system.	O	-	○ (RA-2、SA-14)	○ (A.6.1.1)	-	-
			<Basic> - The organization sets priorities on identified information assets according to importance to the organization. - When related laws or regulations require us to follow a certain classification for resources of the organization (e.g., system and data), apply an appropriate classification to the asset.	O	-	○ (RA-2、SA-14)		○ (4.2.3.6, 4.3.4.4.3)	-
CPS.AM-7	Define roles and responsibilities for cyber security across the organization and other relevant parties.	L1_3_b_ORG, L1_3_c_ORG	Common among <High-Advanced> and <Advanced> - In preparation for damages caused by security incidents, the organization considers risk transfer by using cyber insurance, etc., in addition to implementing security measures designated by business partners.	O	-	-	○ (A.6.1.1, A.15.1.1)	-	-
			<Basic> - In a contract with a contractor or an outsourcer, the organization specifies the scope of the responsibilities of the organization and that of the business partner (state the disclaimer and an upper limit on agreed compensation for damages) in case of a damage caused by a security incident in the business. - To increase the effectiveness of the requirements related to security which a business partner requires or is required to satisfy in a contract, it is desirable that the organization makes an agreement in meeting the requirements, identifying deficiencies and details of actions, paying expenses, and using an alternative when they cannot be satisfied at the time of the contract or in the early stage of the contract.	O	-	○ (SA-4)		○ (4.3.2.3.3)	-
CPS.BE-1	Identify and share the role of the organizations in the supply chain.	L1_3_b_ORG, L1_3_c_ORG	<High-Advanced> - The organization estimates the details and scale of the impacts on direct partners and the entire supply chain in case of a security issue incident which has a harmful effect on the business in the organization.	O	-	○ (CP-2, SA-14)	-	-	-
			<Advanced> - The organization graphically represents the overview of a supply chain related to the organization, with clarification of the roles in the entire organization by considering the component flow, data flow, etc., between organizations. - The organization shares the above results with related organizations (suppliers to the organization, related departments within the organization, and customers of the organization).	O	-	-	-	-	-
			<Basic> - The organization graphically represents the overview of the business connections among suppliers to the organization, related departments within the organization, and customers of the organization, with clarification of the roles in the organization by considering component flow, data flow, etc., between organizations. - The organization shares the above results with related organizations (suppliers to the organization, related departments within the organization, and customers of the organization).	O	-	-	-	-	-
CPS.BE-2	Define policies and standard measures regarding security that are consistent with the high-priority business and operations of the organization, and share them with parties relevant to the organization's business (including suppliers and third-party providers).	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG	Common among <High-Advanced> and <Advanced> - The organization defines its missions and business processes and gives priorities to actions, in consideration of risks to its business, its assets, persons, other organizations, etc. - The organization informs other organizations of their roles and responsibilities specified in its security policies.	O	-	○ (PM-11、SA-14)	○ (A.5.1.1)	○ (4.2.2.1, 4.2.3.6)	-
			<Basic> - The organization should identify in advance the core businesses that should be continued and restored in priority, and the operations considered to be important. In addition, identify and prioritize important resources (relevant parties, People, Components, Data, System, etc.) and functions from the viewpoint of business continuity. - The organization classifies and prioritizes resources particularly in industrial control systems, taking into consideration whether adverse effects on health, safety and environment (HSE) may occur due to malfunction or stoppage.	O	-	-	-	-	-
CPS.BE-3	Identify the dependency between the organization and other relevant parties and the important functions of each in the course of running the operation.	L1_3_b_ORG, L1_3_c_ORG	<High-Advanced> - The organization identifies the functions of the following support utilities for the continuation of its business and the dependence relationship between them. - Communication service - Electrical power equipment (including power cables) - Among the above identified utilities, for those which have important roles for the continuation of its business, the organization examines the possibility of taking measures as follows: - Establishment of alternative communication services - Physical protection of electrical power equipment and power cables - Preparation of short-term permanent power supply equipment - When examining the possibility of using an alternative communication service, the organization considers the following: - Identify the requirements on the availability of the organization (including the target recovery time) when examining a contract with a communication service provider. - Reduce the possibility of sharing a single point of failure with a primary communication service.	O	-	○ (In addition to the following, CP-8, CP-8(1), CP-8(2), PE-9, PE-11)	○ (In addition to the following, A.11.2.2)	-	-
			<Advanced> - The organization identifies the requirements for the capacity/capability of an applicable system according to the requirements for its availability stipulated in CPS.AM-6. - In order to fulfill the required system performance, the organization monitors/adjusts the use of resources in the information systems and industrial control systems in operation, and pre-estimates the storage capacity/performance required in the future.	O	-	○ (SC-5(2))	○ (A.12.3.1)	-	-
			<Basic> - The organization identifies suppliers that are in important dependency in continuing their business.	O	-	-	-	-	-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.GV-1	Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO	<High-Advanced> - While sharing the basic policy with operations used in a conventional IT environment, the organization formulates security policies and operational procedures by fully considering the characteristics of a site on which an IoT device is installed. [Reference] For example, IEC 62443-2-1, a security management standard for industrial automation and control systems (IACS), requires formulation of cyber security policies at an upper level for an IACS environment.	O	-	○ (controls from all security control families)	○ (A.12.1.1)	○ (4.3.2.3.3, 4.3.2.2.1, 4.3.2.6)	-
			<Advanced> - The organization formulates a series of lower level security policies, such as the policies and implementation procedures of the following individual topics, to support policies at a higher level. a) Access control and authentication b) Physical security measures c) System development and maintenance d) Management of external contractors e) Classification and handling of information - The organization formulates a series of security policies by fully considering the organization's a) business strategies, b) related rules, laws, regulations, and contracts, and c) environments under threats to security to sufficiently reflect the actual situation of the organization. - The organization reviews and updates a security plan according to changes in its a) business strategies, b) related rules, laws, regulations, and contracts, and c) environments under threats to security. [Reference] To formulate a policy at a more detailed level, refer to related standards such as ISO/IEC 27002 for identification of fields which require the policy, and refer to more detailed guidelines.	O	-		○ (A.5.1.1, A12.1.1)		-
			<Basic> - The organization formulates a basic security policy at the highest level of its series of security policies, obtains an approval of the management, and operates it appropriately. - The organization reviews and updates the security policy periodically (e.g., once a year).	O	-		○ (A.5.1.1)		-
CPS.GV-2	Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.	L1_2_a_ORG, L1_2_a_COM, L1_2_a_SYS, L1_2_a_PRO, L1_2_a_DAT	Common among <High-Advanced>, <Advanced> and <Basic> - Within the organization's business activities, clearly identify all related laws, regulations, and contractual requirements in the context of security as well as the organization's effort to fulfill these requirements, document them, and maintain those documents at their latest. - The organization defines and documents detailed management measures and details of responsibilities to satisfy the requirements. - The controller identifies all laws and regulations which are applied to each organization to satisfy requirements related to the type of business. - When the organization operates businesses in other countries, the controller considers to comply with the laws and regulations in all related countries.	O	-	○ (controls from all security control families)	○ (A.6.1.3, A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5)	○ (4.4.3.7)	-
CPS.GV-3	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	L1_1_a_SYS, L1_1_a_DAT, L1_1_b_SYS, L3_1_a_SYS, L3_1_a_DAT, L3_4_a_ORG, L3_4_a_PRO, L3_4_b_ORG, L3_4_b_PRO	Common among <High-Advanced>, <Advanced> and <Basic> - The organization identifies and documents all legal requirements and contract requirements related to data protection for each system and each organization and the organization's activities to satisfy these requirements, and update them to the latest. - The organization classifies its data appropriately according to the classification of the identified rules. - The organization takes measures for systems, components, etc., handling the applicable data in accordance with the requirements of the identified rules. When the implementation of a measure is considered difficult, measures such as tokenization of an applicable data in the organization may be considered. (e.g., tokenization of card information due to the Installment Sales Law)	O	○ (3.1.22)	○ (controls from all security control families)	○ (A.8.2.1, A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5)	○ (4.3.4.4.6)	-
CPS.GV-4	Develop a strategy and secure resources to implement risk management regarding security.	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO	Common among <High-Advanced> and <Advanced> - The organization formulates a comprehensive risk management strategy in the short to medium term (e.g. 1 to 5 years) to manage risks to the organization's business, capital, persons, and other organizations caused by operating and using a system. - The organization reviews and updates the risk management strategy in the short to medium term periodically or as necessary.	O	-	○ (In addition to the following, PM-3, PM-9)	○ (Clause 6)	○ (4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3)	-
			<Basic> - The organization determines the security requirements in an information system, industrial control system or a system service and decides, documents, and assigns resources necessary for protecting the system or the system service. - The organization states each security budget item in the organization's plans and budget-related materials.	O	-	○ (SA-2)		-	-
CPS.RA-1	Identify the vulnerability of the organization's assets and document the list of identified vulnerability with the corresponding asset.	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS	<High-Advanced> - The organization conducts vulnerability diagnosis at planned timings such as planned stopping so as not to adversely affect the operation of the system managed by the organization. And then, identify and list vulnerabilities that exist in the system owned by the organization. - It is desirable to conduct a penetration test periodically to recognize an existing vulnerability in a system it manages. - When conducting vulnerability diagnosis, it is desirable to use a vulnerability diagnosis tool that can immediately update the vulnerability of the system to be diagnosed. - The organization develops mechanisms to temporarily permit privileged access to a inspector in vulnerability diagnosis to more thoroughly identify vulnerabilities.	O	-	○ (In addition to the following, CA-8, RA-5(1), RA-5(5))	○ (A.12.6.1)	○ (In addition to the following, 4.2.3.7, 4.2.3.9)	-
			<Advanced> - The organization carries out a vulnerability diagnosis to recognize vulnerabilities existing in the information system which has high importance and makes a list of them. - In the operation phase of an information system owned by the organization, the organization uses a vulnerability diagnosis tool to periodically identify its system vulnerability within vulnerabilities collected from various sources, which are supposed to be related to the organization. The organization shall add the identified vulnerability and its impact degree to a list. [Reference] Japan Vulnerability Notes (https://jvn.jp/) and other sources of information are available for reference to obtain information regarding vulnerability. Also, CVSS (https://www.ipa.go.jp/security/vuln/CVSS.html Illustrated by IPA) could be used as a referential indicator to evaluate the impact level of vulnerability.	O	-	○ (RA-5, RA-5(2))		○ (4.2.3.12, 4.3.4.4.5)	-
			<Basic> - The organization recognizes vulnerabilities in the information systems that the organization manages using documents which are baselines of security measures.	O	-	-	-	-	-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.RA-2	The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.), analyzes the information, and establishes a process to implement and use measures.	L1_1_a_SYS, L1_3_a_ORG, L2_1_a_ORG, L2_1_c_SYS, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> - The organization establishes a security measure organization managing comprehensively the systems including industrial control systems, IoT systems, etc., and takes security measures integrally within the organization. - The person in charge of security updates knowledge about security in both an information system and industrial control system to the latest by attending workshops and meetings related to security and by maintaining an appropriate communication structure with security professional associations/institutions. - Mainly analyze the products/services that the company offers to check if any new vulnerability is contained, and if detected, submit related information to IPA.	O	-	○ (In addition to the following, PM-15)	○ (In addition to the following, A.6.1.4)	○ (4.3.2.3.2)	-
			<Advanced> - The organization, with a chief security officer at the center, establishes a security management team mainly for information systems and IoT systems with high business importance, and prepares a structure for handling security measures within the organization. - The organization collects information on vulnerabilities, threats, etc., from organizations, including the Information-technology Promotion Agency (IPA), JPCERT/CC, industry ISAC, and business partners (device vendors and software vendors), and determines the necessity of actions by comparing to the organization's asset list.	O	-	○ (In addition to the following, PM-16)		○ (4.2.3.9, 4.2.3.12)	-
			<Basic> - For both information systems and industrial control systems, the organization appoints a chief security officer and a person responsible for security measures to clarify the security roles and responsibilities within the organization. - The organization checks security-related cautions offered by device vendors and software vendors, and notifies stakeholders within the organization about them.	O	-	○ (SI-5)	○ (A.6.1.1)	○ (4.3.2.3.2)	-
CPS.RA-3	Identify and document the assumed security incidents, those impacts on the oraganization's assets, and the causes of those.	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS	<High-Advanced> - The organization updates security knowledge to the latest by attending workshops and meetings related to security and by maintaining an appropriate communication structure with security professional associations/institutions. - As necessary, the organization utilizes services provided by experts, obtains information that only some experts can know, and uses them to identify threats.	O	-	○ (In addition to the following, PM-15)	○ (In addition to the following, A.6.1.4)	-	-
			<Advanced> - The organization collects information including newly released attacking trends, malware behaviors, and malicious IP addresses/domains (external intelligence). - The organization evaluates the reliability of the obtained threat information, impacts on the organization, etc., selects vulnerabilities to be handled, and documents threats to be handled.	O	-	○ (PM-16)	-	○ (4.2.3.9, 4.2.3.12)	-
			<Basic> - The orgainzation recognizes threats to the security of the organization and the possibility of occurrence using baseline documents for identifying security threats.	O	-	-	○ (Clause 6.1.2)	-	-
CPS.RA-4	- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation. - Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS, L2_1_a_COM, L2_1_a_PRO, L2_2_a_ORG, L2_2_a_SYS	<High-Advanced> - When developing a new device or a new component which may have an impact on a physical space such as components of an industrial control system, the organization collects/analyzes accident case studies of conventional products and others to identify safety-related hazards. - The organization analyzes a situation where a hazard leads to harm and identifies the possibility of occurrence and the severity of the harm to estimate a possible risk especially regarding an industrial control system. At the time, it is desirable to check whether there is any hazard caused by a security issue. - The organization updates the risk assessment if there is a significant change in the industrial control system or the environment in which it operates, or the other change that affects the security state of the industrial control system.	O	-	-	○ (A.12.6.1, A.18.2.2, A.18.2.3)	-	-
			<Advanced> - The organization updates a risk assessment when there is a big change in a system or an environment where a system is running (including identification of a new threat or vulnerability) or when any situation which impacts the security status of a system occurs. - When planning/designing a new system using an IoT device, the organization identifies existing assets and assets to be protected in the system to be implemented and organizes security measures according to use and configuration of the system. When handling a component or a system with a long life cycle and a component or a system requiring availability, consideration in security measures at a phase before designing is especially important. - When considering security measures applied to purchased products and services, the organization makes sure that the levels of measures correspond to the importance of such products and services.	O	○ (3.11.1)	○ (In addition to the following, SA-12(2))		○ (4.2.3.9, 4.2.3.12)	-
			<Basic> - The organization defines a security risk assessment process and applies it periodically (e.g., once a year). - Establish and maintain security risk criteria. - Identify security risks in the following way. 1) Clarify the target of analysis. 2) Identify incidents (including changes in circumstances) and their causes. - Analyze security risks in the following way. 1) Evaluate possible results when the above identified risks occur. 2) Evaluate the possibility of the actual occurrence of the above identified risks. - Refer to the risk criteria, determine a risk level, and prioritize the risk. - The organization documents and stores the information security risk assessment process. [Reference] An "asset-based" method and a "business damage-based" method are known as security risk assessment methods.	O	-	○ (RA-3)	○ (Clause 6.1.2, A.18.2.2, A.18.2.3)		-
CPS.RA-5	Consider threats, vulnerability, likelihood, and impacts when assessing risks.	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS	<High-Advanced> - The organization uses automated mechanisms for risk assessment (e.g. assessment of the scope of impact) as they receive information about newly identified threats and vulnerabilities. - The organization securely shares with their stakeholders in the supply chain the information about threats and vulnerabilities that may have significant impacts on relevant parties as well as the organization.	O	-	-	-	-	-
			<Advanced> - The organization updates a risk assessment when there is a big change in an information system or an environment where an information system is running (including identification of a new threat or vulnerability) or when any situation which impacts the security status of a system occurs. In that case, give priority to an information system or industrial control system with high importance. * Implementation details common to CPS.RA-4	O	-	○ (RA-3)	○ (A.12.6.1)	-	-
			<Basic> - The organization defines a security risk assessment process and applies it periodically (e.g., once a year). - Establish and maintain security risk criteria. - Identify security risks in the following way. 1) Clarify the target of analysis. 2) Identify incidents (including changes in circumstances) and their causes. - Analyze information security risks in the following way. 1) Evaluate possible results when the above identified risks occur. 2) Evaluate the possibility of the actual occurrence of the above identified risks. - Refer to the risk criteria, determine a risk level, and prioritize the risk. - The organization documents and stores the information security risk assessment process. * Implementation details common to CPS.RA-4	O	-		○ (Clause 6.1.2)	-	-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.RA-6	- On the basis of the results of the risk assessment, clearly define the details of measures to prevent possible security risks, and document the organized outcome from the scope and priorities of the measures. - React accordingly to the security risks and the associated safety risks identified as a result of the assessment conducted at the planning and design phase of an IoT device and systems incorporating IoT devices.	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS, L2_1_a_COM, L2_1_a_PRO, L2_2_a_SYS	<High-Advanced> - On the basis of the results of the hazard analysis performed in CPS.RA-4, mainly for the industrial control system, the organization appropriately treats the source of a risk which may lead to a critical hazard as necessary. [Reference] Security integration in safety control has been particularly discussed in recent years in terms of international standardization, and IEC TR 63074, IEC TR 63069, etc., are available for reference.	O	-	-	○ (A.5.1.2)	-	-
			<Advanced> - The organization securely stores the documented information on security risk management processes. - When the organization selects a measure according to the risk assessment results, it is desirable that the organization documents the measure to be taken and the reason why the measure is adopted. - When applying the measure, the organization formulates a security risk management plan and obtains an approval from the risk owner. - The organization reviews the security risk handling plan and checks that the applicable plan conforms to the priority order of the entire organization's risk management strategy. - The organization informs applicable external business operators regarding security measures necessary for a new system including an IoT device which are extracted in CPS.RA-4 as required specifications. - The organization verifies whether the security measures defined in the required specifications and contracts are implemented at the time of deployment of the systems including an IoT device via User Acceptance Test (UAT). If there is anything unclear, confirm with the external business operator.	O	○ (3.12.4)	○ (PM-4)	○ (Clause 6.1.3, Clause 8.3, A.5.1.2)	-	-
			<Basic> - The organization considers the risk assessment results and selects handling measures to identified risks. - The organization formulates a security risk treatment implementation plan. - The organization obtain an approval from the risk owner for acceptance of the security risk.	O	-	-		-	-
CPS.RM-1	Confirm the implementation status of the organization's' cyber security risk management and communicate the results to appropriate parties within the organization (e.g. senior management). Define the scope of responsibilities of the organization and the relevant parties (e.g. subcontractor), and establish and implement the process to confirm the implementation status of security risk management of relevant parties.	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L1_3_b_ORG, L1_3_c_ORG	<High-Advanced> - When formulating and revising a risk management strategy, the organization performs an interview regarding risk management strategies with highly important business partners to align awareness on security risks and necessary measures. In that case, it is desirable to handle the following: - Major security risks related to the business of the organization and continuance of the business - Details and scale of impact on the business partner when the above risks are manifested - Handling policy for the above security risks - (When the risk management strategy is revised) Changes in the internal and external conditions and important point to be changed from the previous versions	O	-	-	-		-
			<Advanced> - The organization formulates a comprehensive risk management strategy to manage risks to the organization's business, capital, persons, and other organizations caused by operating and using information system and industrial control system. - The organization implements the risk management strategy while keeping consistency in the entire organization. - The organization reviews and updates the risk management strategy periodically or when it is necessary to cope with an organizational change. - The organization's management periodically reviews the following aspects of the organization's risk management strategy that are concerned with security. - How many attacks are you facing (detected) (Detection number by anti-virus products/IDS, latest threat trends etc.) - Is the status of security measures implimentation as planned? (Application rate of security measures to be implemented such as anti-malware and security patch application etc.) -Did you allow the attacker (including insider) to intrude? (Description of an event suspected of external intrusion or internal fraud through security monitoring activities) -What is the state of security that is not directly related to information systems or industrial control systems (Retirement, loss of PC and devices, occurrence of physical theft etc.) - The organization documents and stores the results of reviews by the management.	O	-	○ (PM-9)	○ (Clause 9.3)	○ (4.3.4.2)	-
			<Basic> - The organization identifies the person responsible for security risk management both in information systems and in industrial control systems. - The organization identifies the scope of security risks responsible for in its business.	O	-	-	-	-	-
CPS.RM-2	Determine the organization's risk tolerance level based on the result of the risk assessment and its role in the supply chain.	L1_1_a_ORG, L1_1_a_SYS, L1_1_b_ORG, L1_1_b_SYS, L1_1_c_SYS	<High-Advanced> - The organization determines the risk tolerance level of the organization by capturing risk situations related to supply chains performed in CPS.BE-1 and based on the given results of the risk assessments performed in CPS.RA-4. - The organization interviews important business partners who may have suffer from an undesirable impact because of a security incident in the organization to discuss about the organization's risk tolerance level.	O	-	○ (In addition to the following, SA-14)	-	-	-
			<Advanced> - The organization determines the risk tolerance level of the organization by capturing actual risk situations of supply chains performed in CPS.BE-1 <Advanced> and based on the given results of the risk assessments performed in CPS.RA-4.	O	-		○ (Clause 6.1.3, Clause 8.3)	○ (4.3.2.6.5)	-
			<Basic> - The organization determines the risk tolerance level based on the given results of the risk assessments performed in CPS.RA-4. - The organization obtains approvals to remaining risks from the owners of the risks. - The organization documents the risk management results and safely maintains lists of risk tolerance criteria and accepted risks.	O	-	○ (PM-8)			-
CPS.SC-1	Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG	Common among <High-Advanced> and <Advanced> - The organization, in reference to security measure criteria regarding supply chain, prepares and provides to potential partners tender documents such as ITT (Invitation To Tender) and RFP (Request For Proposal). Especially, it is advisable that the following items be included in the tender documents. 1) Specifications of products or services to be procured 2) Security requirements that the supplie should comply with during the supply period of the products or services 3) Service levels and the indices to comply with during the supply period of the products or services 4) Penalties that the purchaser may impopse if the supplier breach security requirements 5) Confidentiality clauses to protect the data transmitted during the supplier selection process, the systems, etc. - The organization prepares procedures for continuously monitoring the conditions in the business partners' compliance with the security management measures. - To take precautions against cases where a security incident in a business partner impacts the organization, in a written contract, clarify where responsibility lies between the external business operator and the organization, and describe the compensation for a damage to the organization for which the external business operator is responsible.	O	-	○ (In addition to the following, SA-9(2))	○ (In addition to the following, A.15.2.1)	-	-
			<Basic> - The organization formulates security measure criteria applicable to business partners (especially those handling the organization's data or providing a foundation for handling the data) according to appropriate laws and regulations and makes agreement with the details.	O	-	○ (SA-9)	○ (A.15.1.1, A.15.1.2)	○ (4.3.4.4.1)	-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.SC-2	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG, L2_3_c_ORG, L3_1_b_ORG, L3_1_c_ORG, L3_3_a_ORG, L3_3_b_ORG, L3_3_d_ORG	<High-Advanced> - The organization determines its core business that must continue/recover before any other operations in prior and identifies and prioritizes important resources (other relevant organizations, employees, items, data, systems, etc.) and functions vital for continuing applicable businesses. - In case of the occurrence of a security incident in business partners which has harmful business impacts, the organization estimate the details of the impacts on the organization and its occurrence level and scale. * Related requirements of countermeasures include CPS.AM-6 and CPS.BE-2.	O	-	○ (In addition to the following, SA-14)	○ (A.15.1.1, A.15.1.2)	○ (In addition to the following, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.10)	-
			<Advanced> - The organization identifies the business partners in the supply chains which can impact the organization's missions/business processes and confirms whether applicable partners can fulfill the security roles and responsibilities specified in the organization's security policies.	O	-			○ (4.2.3.1, 4.2.3.2, 4.2.3.4, 4.2.3.6, 4.2.3.12, 4.2.3.13, 4.2.3.14, 4.3.4.2)	-
			<Basic> - The organization should identify in advance the core businesses that should be continued and restored in priority, and the operations considered to be important. In addition, identify and prioritize important resources (relevant parties, People, Components, Data, System, etc.) and functions from the viewpoint of business continuity. - When the organization is assumed to use an IoT device for a long period of time, the organization selects a business partner (device vendor) that has adequate organizations of management (Ex: service desk(s), maintainance system) from which long-term support can be expected. - The organization confirms with the partner (the device vendor) whether to replace a device at the end of support before implementing a system. - When the organization selects a business partner (service provider), it is desirable to select a service provider who operates and manages IT services efficiently and effectively. - It has acquired ITSMS certification based on JIS Q 20000. - It has implemented the equivalent measures to ITSMS certification based on self declaration of comformity.	O	-	○ (SA-4)		-	-
CPS.SC-3	When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L1_1_d_ORG, L2_3_c_ORG, L3_1_b_ORG, L3_1_b_DAT, L3_1_c_ORG, L3_1_c_DAT, L3_3_d_ORG, L3_3_a_ORG,. L3_3_b_ORG, L3_3_c_ORG, L3_4_a_DAT, L3_4_b_DAT	<High-Advanced> - In a contract with a business partner who provides systems/components/services, the organization requires the partner the following listed below: - Create evidence of the implementation of the security assessment plan, and submit results of security tests/evaluations. - Develop a plan for remedying defects identified during security testing / evaluation - Disclose a plan for defect remediation and its implementation status - It is desirable that the organization applies necessary requirements among those for security measures to directly consigned parties and accompanying requirements to reconsigned parties by considering the scales of risks originating from the supply chains.	O	-	○ (In addition to the following, SA-11)	○ (A.13.2.4, A.15.1.2)	-	-
			<Advanced> - In accordance with the missions/business needs of the organization, state the following requirements, descriptions, and criteria in a procurement contract of a system, component, or service. - Requirements for security measures - Requirements for security-related documents - Requirements for protection of security-related documents - Confidentiality clauses - Implementation body and method of each handling: reporting destination at the time of incident occurrence, reporting details, initial reaction, investigation, recovery, etc. - Conditions to allow to confirm the observance to the security requirement which is inspected and defined by the organization or the authorized third party. - How to handle an information asset at the end of the contract - The organization requires business partners, in a procurement contract, to implement security requirements that comply with applicable laws and regulations, implement additional measures when they are recognized necessary because of the characteristics of the contracted duty, etc. - It is desirable to consider the following items in advance when determining security requirements based on laws and regulations and requiring business partners to comply with them. - Identification of potential risks in terms of legal regulations that may arise due to difference of applicable laws between the organization and the business partner - Negative impacts on the contract in terms of security due to legal and regulatory obligations applicable to the business partner	O	-	○ (In addition to the following, SA-4)		○ (4.3.2.6.4, 4.3.2.6.7)	-
			<Basic> - The organization requires business partners to implement security requirements that complies with applicable laws and regulations. - The organization confirms that the business partner has declared "SECURITY ACTION" in the process of selecting and evaluating a contractor. * "SECURITY ACTION" is an initiative in Japan that small and medium-sized enterprises declare themselves to work on information security measures.	O	-	○ (SA-9)			-
CPS.SC-4	When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L1_1_d_ORG, L1_1_d_COM, L2_1_a_COM, L2_1_a_PRO, L2_2_a_ORG, L2_3_a_ORG, L2_3_c_ORG, L2_3_c_PRO, L2_3_d_ORG, L3_1_b_ORG, L3_3_a_ORG, L3_3_b_ORG, L3_3_c_ORG, L3_3_d_ORG	<High-Advanced> - The organization or a third party tests the procured devices to see whether the security requirements stipulated in the contract are fulfilled. - The organization checks throughout the entire relevant supply chain (including reconsigned organizations) as to whether the devices especially important for their operation are manufactured under appropriate procedures by organizations that have quality and security management ability above a certain level.	O	-	-	○ (In addition to the following, A.14.3.1)	-	-
			<Advanced> - The organization specifies in the contract the security requirements that the products and services procured from the partner should comply with, such as the following. - Specific certifications related to security (e.g., ISMS certification 、ISASecure EDSA certification, Japan Information Technology Security Evaluation and Certification Scheme (JISEC) have been gained. - The vendor itself confirms that it has implemented the security measures in accordance with the standards of specific certifications related to security - It has implemented the necessary security requirements from the design phase (security by design) based on the results of risk analysis, etc., and test them. - It is desirable that the organization should, at the phase of planning procurement, secure a budget for security requirements regarding products or services themselves, or protection of assets used for procurement and supply of such products or services. - The organization formulates, manages and improves security measurement rules to evaluate procurement or supply of products or services, including the following. - Target for measurement - Method and frequency of reporting on measures taken - Measures to be taken when measures are not implemented - The organization checks means of detecting (or preventing) falsifications and leakages during shipments and whether or not the IoT devices and software being delivered have been operated without authorization. - Goods: security courier, protection seal, etc. - Digital transfer: encryption, hash of the entire transmitted data, etc.	O	-	-	○ (A.8.3.3, A.14.1.1, A.14.2.9, A.15.1.3)	-	-
			<Basic> - During procurement, the organization confirms whether the IoT devices which the organization possesses are genuine products by checking the label. - By utilizing IDs, secret keys, and electronic certificates included in the IoT devices and software, an organization confirms that procured devices are genuine products. - The organization will confirm the following when selecting relevant parties for the provision of products and services. -The product/service support period is sufficient, including the distribution of security patches. -The response after the support period has been identified.	O	-	-	-	-	-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.SC-5	Formulate and manage security requirements applicable to members of other relevant organizations, such as business partners, who are engaged in operations outsourced from the organization.	L1_1_a_PEO, L1_1_b_PEO, L1_1_c_PEO, L2_3_b_PEO, L3_1_b_PEO, L3_1_c_PEO	<High-Advanced> - The organization prepares a procedure to continuously monitor whether the security requirements from the contractee are complied with by the staff of the contractor, and to enable notification to the organization's personnel in charge in the case where irregular behavior is found.	O	-	○ (PS-7)	○ (A.16.1.2, A.16.1.5)	-	-
			<Advanced> - The organization trains the staff on information security aspects of supplier relationships to particularly ensure that the handling of confidential information is correctly understood. - The organization regularly confirms that it complies with the security requirements from the contractee in conducting the contracted work.	O	-			-	-
			<Basic> - The organization identifies and evaluates the staff who access, disclose or change the data related to the contracted work that should not be disclosed or changed such as confidential data or intellectual property. - After the contract with the contractor is finished, the organization immediately terminates the rights that are temporarily granted to the personnel of the contractor such as access rights to its facilities.	O	-			-	-
CPS.SC-6	Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	L1_1_a_DAT, L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L2_3_c_ORG, L2_3_c_PRO, L2_3_d_ORG, L3_1_a_DAT, L3_1_b_ORG, L3_1_b_DAT, L3_1_c_ORG, L3_1_c_DAT, L3_3_a_ORG,. L3_3_b_ORG, L3_3_c_ORG, L3_3_d_ORG, L3_4_a_DAT, L3_4_b_DAT	<High-Advanced> - The organization adopts an automatic mechanism integrating review, analysis, and report that supports the investigation and addresses procedures for deviation or signs of deviation from contract matters. - The organization uses a mechanism that allows it to list and check whether obligatory matters stipulated in the contract are fulfilled, matters which are concerned with security management of the organization and security functions implemented in the products and services that will be delivered, especially for important clients and reconsigned organizations. - State of compliance with security management measures of the external service provider is regularly checked by external audits and field surveys conducted by the outsourcer. - The important business partners and if possible their re-contractors etc. investigate whether there is any sign of attack related or any fact of information leakage, and regularly report the result to the organization.	O	○ (In addition to the following, 3.3.5)	○ (In addition to the following, AU-6(1), AU-6(3))	○ (A.12.7.1, A.14.3.1, A.15.2.1)	-	-
			<Advanced> - The organization checks whether requirements that are prescribed in the contract with the client can be audited on the system. - The information system provides a function that allows for audit records to be created for events defined above that can be audited on the system. - The organization shall be able to maintain consistency in security audits with other organizations that require information on the audit. - The organization regularly reviews and analyzes audit records that are made manually or automatically by the system, and checks whether there is any deviation or sign of deviation from contract matters. - State of compliance with security management measures of the external service provider is regularly checked by internal audits that are conducted by the client using a checklist.	O	○ (3.3.1)	○ (AU-2, AU-6, AU-12, SA-9)		○ (4.3.2.6.7, 4.3.4.3.1)	○ (SR 6.1)
			<Basic> - Acquisition certificate of various authentications and systems (e.g., ISMS, CSMS, privacy mark) are checked as an alternative method to confirm the implementation of required security measures.	O	-	-	-	-	-
CPS.SC-7	Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L1_1_d_ORG, L2_2_a_ORG, L2_3_c_ORG, L2_3_c_PRO, L3_1_b_ORG, L3_1_c_ORG, L3_3_a_ORG, L3_3_b_ORG, L3_3_c_ORG, L3_3_d_ORG	<High-Advanced> - The organization formulates and manages a procedure to execute the following when nonconformity by the partner is found at an audit or test. 1） Identify and assess the influence in terms of security arising from such nonconformity. 2） Decide whether to review the security requirements defined in the contract. 3） Decide the corrective action to be taken to achieve the acceptable security level within the procured products and services. 4） Agree with the partner on the above .	O	-	-	-	-	-
			<Advanced> - The organization formulates and manages a procedure to, when nonconformity by the partner is found at an audit or test, require the partner to make a remediation plan and to confirm the implementation status of the plan as needed.	O	-	-	-	-	-
			<Basic> - The organization is aware of the risk to its own organization due to the failure of its products and services when the non-conformances in its audits or tests on products and services occurs.	O	-	-	-	-	-
CPS.SC-8	Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.	L1_1_d_ORG, L2_2_a_ORG, L2_3_c_ORG, L2_3_c_PRO, L3_1_b_ORG, L3_1_c_ORG, L3_3_a_ORG, L3_3_b_ORG, L3_3_c_ORG	<High-Advanced> - The organization uses a trail storage system with the following features to flexibly fulfill the needs of clients and other related organizations, such as a third-party auditing institution, on a real-time basis. - Eligibility of the subject audit trail for the contract matter can be verified quickly. - Only authorized entities such as clients and outsourced auditing agencies can access the system. - Stored data has reliable trails such as time stamps and electronic signatures.	O	-	-	○ (A.12.4.1, A.18.1.3)	-	-
			<Advanced> - The organization takes measures so that those records among the audit records generated by the system that are acquired over a long period of time can be obtained with certainty. - In order to protect audit records from the following threats, it is desirable for the system to apply access control with high granularity to the items and systems in which audit records are stored. - Change format of recorded message - Change or delete log file - Exceed storage space of log file medium	O/S	-	○ (In addition to the following, AU-9, AU-11(1))		○ (4.3.2.6.7)	○ (SR 6.1)
			<Basic> - The organization preserves audit records for an appropriate period of time so as to satisfy the requirements of laws and regulations.	O	-	○ (AU-11)			-
CPS.SC-9	Prepare and test a procedure for incident response with relevant parties involved in the incident response activitiy to ensure action for incident response in the supply chain.	L1_3_b_PEO	<High-Advanced> - The organization assumes the course of action for security incidents of the supply chain and prepares a procedure that adjusts incident responses between the organization and other organizations that are concerned with the supply chain. - The organization assumes the course of action for security incidents of the supply chain and implements tests that adjust incident responses with other organizations that are concerned with the supply chain. [Reference] Violations in the security incidents of supply chain include violations on system components, IT products, development processes, developers, distribution processes, and warehouse facilities.	O	○ (3.6.1, 3.6.3)	○ (In addition to the following, IR-4, IR-4(10))	-	-	○ (In addition to the following, SR 3.3)
			<Advanced> - The organization adjusts the incident response process of an external service provider that contains important features in order to continue its business, as well as adjusting the organization’s incident response process to meet the incident response requirements. - The organization tests the incident response process that requires cooperation between the organization and external service providers.	O	○ (3.6.1, 3.6.3)	(CP-2, CP-2(7))	-	○ (4.3.2.5.7)	○ (SR 2.8, SR 6.1, SR 7.3, SR 7.4)
			<Basic> - The organization is aware of security incidents that may occur in the organization and their potential consequences.	O	-	-	-	-	-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.SC-10	Develop and manage a procedure to be executed when a contract with other relevant organizations such as business partners is finished. (e.g., expiration of contract period, end of support)	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO	<High-Advanced> - The organization assures that, after a contract is finished, it deletes in a timely manner logical and physical access rights that are granted to the contractor to access and handle the organizations's resources necessary for the supply of products or services.	O	-	-	-	-	-
			<Advanced> - The organization agrees with the present business partner whether the supply of the products or services should be cancelled or they should be returned to the organization or the other business partner. - The organization communicate with the stakeholders who are influenced by the supply of the products or services to provide information on the discontinuation. - The organization executes the discontinuation of the supply of the products or services in accordance with the discontinuation plan. - The organization agrees with business partners on the accomplishment of the discontinuation of the supplied products or services.	O	-	-	-	-	-
			<Basic> - The organization always keeps track of when contracts with relevant parties, such as business partners, are terminated.	O	-	-	-	-	-
CPS.SC-11	Continuously improve the standard of security measures relevant to the supply chain, related procedures, and so on.	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO	Common among <High-Advanced>, <Advanced> and <Basic> - The organization continuously monitor the performance of business partners related to security, review and amend as needed the security measure criteria regarding the supply chain and related procedures based on the latest trends of security threats and regulations.	O	-	-	-	-	-
CPS.AC-1	Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	L1_1_a_COM, L1_1_a_SYS, L1_1_b_COM, L1_1_b_SYS, L1_1_c_COM, L2_3_c_SYS L3_1_a_SYS, L3_3_a_SYS	<High-Advanced> - The organization introduces and operates, for example, the following automated mechanisms for managing accounts in their own information systems and industrial control systems. -Automatically collect account information periodically from the system to be managed -Automatically change password of privileged account - The industrial control system supports integrated account management. - After a certain period of time, the system automatically invalidates temporary accounts, emergency accounts, and accounts not in use on their system. - The information system automatically audits and reports account validation and invalidation that is associated with creation, change, and deletion of accounts in the system used by the organization.	O/S	-	○ (In addition to the following, AC-2 (1), AC-2 (2), AC-2 (3), AC-2(4))	○ (In addition to the following, A.9.2.4, A.9.2.5)	-	-
			<Advanced> - The organization must obtain approval from the management supervisor when creating a system account. - With regard to the shared user account, a user who can know authentication information is managed in a list or the like, and the range of using the account can be identified. - The organization monitors the usage of system accounts used in an information system. - If an account needs change or becomes unnecessary, the organization notifies the management supervisor. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used. - The organization notifies the user (or the person in charge of management) when the password is changed in an information system and an industrial control system. - If the information system resets the credentials for reasons such as user"s forgetting credentials, the information system confirms securely that the account is its own to prevent unauthorized tampering with the credentials by a malicious party.	O/S	-	○ (AC-2)		-	-
			<Basic> - The organization appoints a management supervisor for the accounts in its information system and industrial control system. - The organization decides and selects types of system accounts necessary (e.g., general user/system administrator/shared user/temporary user), with consideration of their mission and business functions. - The organization creates and enables system accounts as per the procedure, and changes, disables and deletes them as needed. - The organization develops a policy of credentials (e.g. password, security key) for its own information systems and industrial control systems, and implements a function that cannot be set up unless the credential satisfies the policy. The following is an example of the content of the policy. - Devolop and operate the requirements for passwords in order to ensure the minimum required complexity. - When new credentials are created, change them to at least the number of characters defined by the organization. - Store and transmit only cryptographically protected credentials. - Prohibit reuse of the same credentials for the period that the organization defines. - The organization allows its members to use temporary credentials exceptionally when logging on to the system when they have forgotten credentials, if they change immediately to a strong password. - The organization does not share user identification information among multiple system users in an information system and an industrial control system except when multiple users function as a single group.	O	-		○ (A.9.1.1, A.9.2.1, A.9.2.2, A.9.2.6)	○ (4.3.3.5.1)	○ (SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9)
CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	L1_1_a_SYS, L1_1_c_SYS, L2_3_b_PEO, L2_3_b_SYS, L2_3_c_SYS, L2_3_d_SYS, L3_1_a_SYS	<High-Advanced> - The organization regulates service wires and transmission paths that are related to their IoT devices and servers by physical access. - The organization regulates output devices of its system by physical access. - The organization monitors alarms and monitoring devices (e.g., surveillance cameras) for physical intrusions into the areas within the physical security boundaries.	O	-	○ (In addition to the following, PE-4, PE-5, PE-6 (1))	○ (In addition to the following, A11.1.1.4, A11.2.3)	○ (4.3.3.3.2, 4.3.3.3.8)	-
			<Advanced> - The organization monitors physical accesses to the areas within the physical security boundaries and regularly reviews the audit log. - The organization keeps the records of visitor's access to the areas within the physical security boundaries and regularly reviews them.	O	○ (3.10.2, 3.10.4, 3.10.5)	○ (In addition to the following, PE-6, PE-8)	○ (In addition to the following, A.11.1.1, A.11.1.5)		-
			<Basic> - The organization maintains upkeep of the access list for areas where their IoT devices and servers are located and issues permission certificates necessary for access. - The organization defines physical security boundaries at its facilities, and implement access control according to the security requirements of assets placed within the boundaries and the results of risk assessment. - The organization monitors the work of temporarily authorized party within the physical security boundaries, such as by authorized attendants or monitoring cameras.	O	○ (3.10.1, 3.10.3)	○ (PE-2, PE-3, PE-8)	○ (A.9.2.6, A.11.1.2, A.11.1.3, A.11.1.6, A.11.2.8, A.11.2.9)		-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).	L2_3_c_SYS, L3_3_a_SYS	<High-Advanced> - The information system and the industrial control system automatically monitor or regulate remote access to its system. - The information system and the industrial control system allow only for remote access routed by the regulated access points. - The information system allows privileged command via remote access only for those purposes based on specified requirements. - The information system records reasons why the users accessing the system which handles highly confidential data execute privileged commands and access security information by remote access. - The information system protects wireless access to the system which handles highly confidential data by using user and device authentication in addition to encryption. - The information system blocks remote activation of devices such as white boards, cameras, and microphones connected via networks which may handle highly confidential data. Signs of the devices in use are provided to the users of these devices.	S	○ (In addition to the following, 3.1.12, 3.1,13, 3.1.14, 3.1.15, 3.1.17, 3.1.19, 3.10.6, 3.13.12, 3.13.15)	○ (In addition to the following, AC-17(1), AC-17(2), AC-17(3), AC-17(4), AC-18(1), AC-19(5))	-	-	○ （In addition to the following, SR 1.13）
			<Advanced> - The organization regulates the mobile devices used in the organization and establishes setting requirements, connection requirements, and implementation guidelines for mobile devices. - The organization establishes rules of approval for connecting mobile devices used in the organization to its system.	O	○ (In addition to the following, 3.1.18)	○ (In addition to the following, AC-19)	○ (In addition to the following, A.6.2.1)	-	○ （SR 1.1, SR 1.2, SR 2.6）
			<Basic> - The organization establishes usage regulations, configuration requirements, and implementation guidelines for each type of approved remote access. - The organization in principle prohibits unauthorized wireless connections. - The organization establishes rules of approval for remote access to an information system and an industrial control system. - The organization authorizes wireless access to its system in advance of the approval.	O	○ (3.1.16)	○ (AC-17, AC-18)	○ (A.6.2.2)	-	
CPS.AC-4	Prevent unauthorized log-in to IoT devices and servers by measures such as implementing functions for lockout after a specified number of incorrect log-in attempts and providing a time interval until safety is ensured.	L2_1_b_SYS, L3_3_a_SYS	<High-Advanced> - The information system and the industrial control system (excluding some cases where immediacy of response is required) sets a limit to the number of continuous login attempts on its system. If the user fails to log in, he or she will only be able to re-login after the administrator removes the restriction.	S	○ (3.1.8)	○ (AC-7)	○ (A.9.4.2)	-	○ （SR 1.11）
			<Advanced> - The information system and the industrial control system set a limit on the number of continuous login attempts on its system. If the user fails to log in, he or she will not be able to re-login for a certain period of time. - The information system and industrial control system lock the session manually or automatically if the system's non-operation continues beyond the time set by the organization. * In the industrial control system, it may be desirable not to lock session when it is assumed that a session in which an operator is required to respond immediately in an emergency may be conducted.	S				-	○ （SR 1.11, SR 1.13, SR 2.6）
			<Basic> - N/A	-	-	-	-	-	-
CPS.AC-5	Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions)	L1_1_a_SYS, L1_1_b_SYS, L2_1_c_SYS, L3_1_a_SYS	<High-Advanced> - The organization specifies administrators who use the security functions (e.g., access authority setting) and regulates privileged accounts in its system. - The information system adopts a system monitoring mechanism to check the use of privileged functions. - The information system prohibits non-privileged users from executing privileged functions on the system by invalidating, avoiding, and changing security measures that are changed and implemented by non-privileged users. - The organization can minimize the number of users who can use the system administrator's authority in an emergency to minimize the damage caused by the security incident. - The organization can prevent even system administrators from stopping critical services and protected processes through the server to minimize the damage caused by security incidents.	O/S	○ (In addition to the following, 3.1.6, 3.1.7)	○ (In addition to the following, AC-6(1), AC-6(2), AC-6(5), AC-6(9), AC-6(10))	○ (A.6.1.2, A.9.2.3, A.9.4.1, A.9.4.4)	-	-
			<Advanced> - The organization implements access control in the information system and the industrial control system based on separation of duties (e.g., user / system administrator). - The organization adopts a general rule on the minimum authority of specific duties. - Segregate authority of general user from that of administrator. (Require users to use the system with a non-privileged account when using a non-security function.) - Minimize authority for duties not in charge. - The organization separates and stipulates duties that are assigned by the person in charge.	O	○ (3.1.4, 3.1.5, 3.13.3)	○ (AC-3, AC-5, AC-6, SC-2)		○ (4.3.3.2.7)	-
			<Basic> - The organization implements access control based on separation of duties (e.g. user/system administrator) in the highly confidential information system of the organization. - If the separation of duties is difficult to implement due to the shortage of human resources, etc., it is desirable to take alternative measures such as, when a person other than the pre-designated official performs the specific duties, requiring another person to monitor the performance of such duties.	O	-	-	-	-	○ （SR 2.1）
CPS.AC-6	Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.	L1_1_a_SYS, L1_1_b_SYS, L2_1_c_SYS, L3_1_a_SYS	<High-Advanced> - The system uses a multifactor authentication in its system for access to the system or network with non-privileged accounts. - Regarding an information system that handles highly confidential data, access to the system and network with privileged or non-privileged accounts in the system, uses an authentication mechanism that can tolerate attacks of replay. [Reference] It is desirable to refer to NIST SP 800 63-3 regarding strength of authentication methods and appropriate use cases.	S	○ (In addition to the following, 3.5.4)	○ （下In addition to the following, IA-2(2), IA-2(8), IA-2(9))	○ (In addition to the following, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4)	-	○ （SR 2.1）
			<Advanced> - In consideration of the risk of unauthorized login to the privileged account in the system, the organization in principle prohibits login to the privileged account via the network when it is not possible to implement a sufficient confidence methods of authentication. - The information system requires a multifactor authentication in its system for access to the system or network with privileged accounts when cannot implement actions such as invalidating the administrator account for the system. - In principle, the organization invalidates the default administrator account in the information system. - The information system permits the necessary minimum privileged authority to the user account when performing privileged operations.	S	○ (In addition to the following, 3.5.3)	○ (In addition to the following, IA-2(1), IA-2(3))		-	
			<Basic> - Regarding access to the system and network with privileged or non-privileged accounts in the system, the organization uses an authentication method that uniquely identifies the access.	O/S	○ (3.5.1)	○ (IA-2)	○ (A.9.2.1)	-	

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).	L2_1_b_SYS, L3_1_a_DAT, L3_4_b_SYS	<High-Advanced> - The information system and the industrial control system monitor and control communications on the networks composing internal business systems of the organization. - Regarding the network which the system that handles highly confidential data is connected to, the organization shall deny network communications as a default and shall only allow connection of approved communication traffic. - The organization physically or logically separates the network of high importance industrial control systems from the network of control systems with lower importance. - If the information system that handles highly confidential data is connected to a remote device, the organization is to prevent multiple and simultaneous local connections between the device and the system, as well as prevent access to external network resources by other connections.	S	○ (In addition to the following, 3.1.3, 3.13.6, 3.13.7)	○ (In addition to the following, SC-7(5), SC-7(7))	○ (In addition to the following, A.13.1.1, A.13.1.3, A.14.1.2, A.14.1.3)	-	-
			<Advanced> - The information system and industrial control system monitor and regulate connection of external and internal boundaries of the network to which the system is connected (in the case of industrial control systems, boundaries with information systems). - The organization installs boundary protection devices to promote effective security in the system and connects to external networks via the device.	O/S	-	○ (In addition to the following, SC-7)		○ (4.3.3.4.2, 4.3.3.4.3)	○ (SR 3.1, SR 3.8)
			<Basic> - The organization establishes a data flow regulation policy that defines the range in which data flow within information systems and industrial control system is permitted and the range in which data flow between systems is permitted, and regulates the flow by segregating the network appropriately. - The organization logically or physically segments the control system's network from the network composing of the information system. [Reference] Implement physical segmentation in environments physically separated from other networks. Alternatively, in environments physically close to other networks, it is possible to implement logical segmentation in consideration of the cost of the measure.	O/S	○ (3.1.3)	○ (AC-4)	○ (A.12.1.4, A.13.2.1)	○ (4.3.3.4.1)	
CPS.AC-8	Restrict communications by IoT devices and servers to those with entities (e.g. people, components, system, etc.) identified through proper procedures.	L2_1_b_SYS, L3_3_a_SYS	Common among <High-Advanced>, <Advanced> and <Basic> - The organization assigns identifiers to its IoT devices and servers, as well as managing the identification by preventing re-use of identifiers and invalidating identifiers after a certain period of time. - Before connecting their IoT devices and servers to the network, the information system and the industrial control system prepare a mechanism that uniquely identifies and authenticate these devices. - Communication using IoT devices is denied as default. The protocol to be used is authorized as an exception.	O/S	○ (3.5.5, 3.5.6, 3.8.2)	○ (IA-4)	○ (A.7.1.1, A.9.2.1)	○ (4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.3)	○ (SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1)
CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	L1_1_a_SYS, L1_1_b_SYS, L2_1_b_SYS, L3_1_a_SYS, L3_4_b_SYS	<High-Advanced> - The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.	S	○ (In addition to the following, 3.1.11)	○ (In addition to the following, IA-2, IA-5(2), AC-12)	○ (A.9.3.1, A.9.4.3, A.9.4.5)	○ (In addition to the following, 4.3.3.6.3, 4.3.3.6.5, 4.3.3.6.7)	○ (In addition to the following, 、SR 1.9)
			<Advanced> - The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.	O/S	○ (3.1.1, 3.1.2, 3.1.9, 3.1.10, 3.5.2, 3.5.7, 3.5.8, 3.5.9, 3.5.10, 3.5.11)	○ (IA-5, IA-5(1), IA-6, AC-8, AC-11, AC-11(1))		○ (4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.4, 4.3.3.6.6, 4.3.3.6.8, 4.3.3.6.9)	○ (SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.10)
			<Basic> - The organization develops a policy of credentials (e.g. password, security key) for its own information systems and industrial control systems, and implements a function that cannot be set up unless the credential satisfies the policy. The following is an example of the content of the policy. - Devolop and operate the requirements for passwords in order to ensure the minimum required complexity. - When new credentials are created, change them to at least the number of characters defined by the organization. - Store and transmit only cryptographically protected credentials. - Prohibit reuse of the same credentials for the period that the organization defines. - The organization allows its members to use temporary credentials exceptionally when logging on to the system when they have forgotten credentials, if they change immediately to a strong password. - Information system and industrial control system limit the transactions and functions that can be performed to authenticated users.	O/S	-	-	-	-	-
CPS.AT-1	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	L1_1_a_PEO, L1_1_b_PEO, L1_1_c_PEO, L1_1_d_PEO, L1_2_a_PEO, L1_3_a_PEO, L1_3_a_DAT, L1_3_c_PEO, L3_4_a_PEO	<High-Advanced> - The organization provides security awareness trainings to all necessary personnel so that they will recognize and report signs of internal fraud.	O	○ (In addition to the following, 3.2.3)	○ (In addition to the following, AT-2(2))	○ (A.7.2.1, A.7.2.2)	-	-
			<Advanced> - The organization regularly provides basic security awareness training to all members of staff. The organization can, for example, educate the following matters in addition to the contents explaining general matters. -Procedure to response when you receive a suspicious email -Notes on using mobile devices (e.g. Notes on connecting to a public wireless LAN) -Notes on using SNS - The organization creates a program for each role (e.g., system/software developper, purchasing personnel, system administrator, personnel in charge of security measures) to train information security personnel and to improve their skills. The program is conducted regularly on applicable personnel. - The organization regularly reviews records of security education and training.	O	○ (3.2.1)	○ (In addition to the following, AT-3)		○ (4.3.2.3.4, 4.3.2.4.1, 4.3.2.4.2, 4.3.2.4.6, 4.3.3.2.5, 4.3.4.5.4, 4.3.4.5.11)	-
			<Basic> - The organization provides basic security awareness training to new staff, or when necessary due to changes made to the information systems and the industrial control systems which the organization uses. - The organization records and manages the contents and results of security education and training for member in the organization.	O	-	○ (AT-2)			-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.AT-2	Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.	L1_3_b_PEO, L1_3_a_DAT, L3_3_a_PEO	<High-Advanced> - The organization monitors its personnel and related organizations that may be involved in the security incident for the accomplishment status of the roles assigned to the personnel in charge.	O		-	-	-	-
			<Advanced> - The organization requests the giving of training (e.g. simulation assuming actual incident) and security education appropriate to execution of the roles assigned to the personnel in charge to related organizations that may be involved in the security incident and confirms the training/education implementation status. - The organization regularly reviews the records of education and training for persons in charge of relevant parties that are highly important in its own security management.	O	○ (In addition to the following, 3.2.2)	-	-	○ （In addition to the following, 4.3.2.4.3, 4.3.4.5.11）	-
			<Basic> - The organization requests the giving of training (e.g. simulation assuming actual incident) and security education appropriate to execution of the roles assigned to the personnel in charge to their personnel, and confirms the training/education implementation status. - The organization records and manages the contents and results of security education and training for member in the organization.	O	○ (3.2.1)	-	-	○ （4,3,2,4,1, 4.3.2.4.2, 4.3.2.4.6）	-
CPS.AT-3	Improve the contents of training and education regarding security to members of the organization and other relevant parties of high importance in security management of the organization.	L1_1_a_PEO, L1_1_b_PEO, L1_1_c_PEO, L1_3_a_PEO, L1_3_b_PEO, L1_3_c_PEO, L3_3_a_PEO, L3_4_a_PEO,	Common among <High-Advanced> and <Advanced> - The organization continuously verifies the effects of education and training in order to ensure that the member of the organization and persons of relevant parties in charge have a better understanding of security. - The organization refers to the results of the review of security education and training records and improves the contents of education and training in light of new or changing threats and vulnerabilities.	O	-	○ (AT-1)	○ (A.7.2.2)	○ (4.3.2.4.4, 4.3.2.4.5)	-
			<Basic> - The organization will conduct questionnaires and simple tests to confirm the subject's understanding of the content and confirm the results after conducting security education and training.	O	-			-	-
CPS.DS-1	If the organization exchanges protected information with other organizations, agree in advance on security requirements for protection of such information.	L3_1_a_PRO, L3_4_a_DAT, L3_4_b_DAT	Common among <High-Advanced> and <Advanced> - The organization specifies concrete security measure requirements considering importance of exchanged data and assumed risks, and requires business partners to implent them. - The organization permits outsourcing of data handling operation to subcontractors only if it confirms that such subcontractors have implemented security measures whose level is equivalent to those required to direct business partners.	O	-	-	-	-	-
			<Basic> - The organization regulate how to handle the data that business partners may handle by concluding a non-disclosure agreement. - The organization prohibits direct business partners from subcontracting operations related to data management.	O	-	-	-	-	-
CPS.DS-2	Encrypt information with an appropriate level of security strength, and store them.	L1_1_a_DAT, L3_1_a_DAT, L3_3_d_SYS, L3_4_b_SYS	<High-Advanced> - The organization selects products that have been authenticated based on Cryptographic Module Validation Program (CMVP) in order to suitably implement selected algorithms to software and hardware, and to protect keys, identification codes, and entity authentication information that is used to decrypt encrypted information or to grant electronic signatures. - The organization protects are encrypts data to the appropriate strength when that data is taken outside of the organization. - The organization uses IoT devices that can encrypt and store data in internal memory.	O/S	○ (In addition to the following, 3.8.6, 3.13.11, 3.13.8)	○ （In addition to the following, SC-12(1)）	○（A.8.2.3）	-	-
			<Advanced> - The organization examines safety and trustworthiness that are necessary, selects an algorithm, encrypts information (data) to the appropriate strength, and stores the information. If an algorithm on the CRYPTREC Ciphers List can be selected, the organization uses it to encrypt information (data) to the appropriate strength and stores the information. - The organization considers the level of security and trustworthiness required for the information, chooses an algorithm, and encrypts and stores high importance information handled by industrial control systems with appropriate strength without causing unacceptable impact on performance. [Reference] Regarding encryption technologies whose security and implementation performance are confirmed, "Cryptography Research and Evaluation Committees （CRYPTREC）" releases to the public the list of such technologies recommended for use that are sufficiently used in the market or are considered to spread in the future. It is desirable that the organization should refer to the list as needed when procuring systems that should implement encryption functions.	O/S	○ (In addition to the following, 3.13.16)	○ （In addition to the following, SC-28）		-	○ （SR 3.4, SR 4.1）
			<Basic> - The organization examines safety and trustworthiness that are necessary, selects an algorithm, encrypts important information (data) handled by information systems to the appropriate strength, and stores the information.	O/S	○ (3.13.10)	○ （SC-12）		-	
CPS.DS-3	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.	L1_1_a_SYS, L1_1_b_DAT, L3_1_a_DAT, L3_2_b_DAT, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> - The organization protects th networks composing the information system and industrial control system that handles important data by implementing encrytion of communication channels or by alternative physical measures.	O/S	○ (3.13.15)	○ (下記に加えてSC-12(1))	○ (A.10.1.1,A.13.2.1, A.13.2.3, A.14.1.2)	-	○ （SR 3.1, SR 3.8, SR 4.1, SR 4.2, SR 4.3）
			<Advanced> - The information system employs an cryptographic mechanism and encrypt communciation paths. [Reference] For encryption of communication paths, there are several methods such as IP-VPN, Ipsec-VPN, SSL VPN. It is desirable that the organization should select the method considering the importance of the data transmitted in the communication paths, the budget, and so on.	S	○ (3.13.15)	○(SC-8(1), SC-12)		-	
			<Basic> - N/A	-	-	-	-	-	-
CPS.DS-4	Encrypt information itself when sending/receiving information.	L1_1_a_DAT, L1_1_b_DAT, L3_1_a_DAT, L3_2_b_DAT, L3_3_d_SYS	<High-Advanced> - The system /IoT apparatus introduces the code module which it can implement without even little resource losing availability, and it is desirable to encrypt the communication data from a high apparatus of the importance at appropriate strength. - The information system encrypts all data transmitted outside the organization with appropriate strength, not limited to high or low importance.	S	-	-	○ (A.10.1.1, A.13.2.1, A.13.2.3, A.14.1.2)	-	○ （SR 3.1, SR 3.8, SR 4.1, SR 4.2, SR 4.3）
			<Advanced> - The organization encrypts information with appropriate strength when transmitting highly confidential information to an external organization or the like.	O	-	○ (SC-8(1))		-	
			<Basic> - N/A	-	-	-	-	-	-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.DS-5	Securely control encryption keys throughout their life cycle to ensure proper operation and securely transmitted, received and stored data.	L1_1_a_DAT, L3_1_a_DAT	<High-Advanced> - If the user loses the key, the organization maintains the availability of the information by reissuing key or the like. - It is desirable to consider authenticity of the public key as well as to securely control the secret key and private key. This authentication process is carried out using the public key certificate issued normally by a certificate authority. It is desirable that the certificate authority should be a recognized organization that implements appropriate measures and procedures to provide the required reliablity.	O/S	-	○ (In addition to the following, SC-12(1))	○ (A10.1.2)	-	-
			<Advanced> - It is desirable that the organization should set out a policy and procedure regarding the following items to take immediate and appropriate measures when the private key is imperiled. - A structure to take measures against imperilment of the private key (including the stakeholders, roles, cooperation with contractors) - Criteria to judge whether the private key is imperiled or is in danger of imperilment - To investigate the cause of imperilment of the private key, and to attempt to remove the cause - Suspension of the services using the key - To create a new pair of keys and issue a certificate for the new key - Disclosure of information regarding imperilment of the private key (Notified parties, a method of notification, disclosure policy, etc.) [Reference] It is desirable to refer to the group of standards of ISO/IEC 11770, NIST SP 800-57 Part 1 Rev.4, and so on for the details about key management.	O	○ (3.13.10)	○ (SC-12)		-	○ (SR 1.9, SR 4.3)
			<Basic> - It is desirable that the organization should protect all encryption keys from modification and loss.	O				-	
CPS.DS-6	Secure sufficient resources (e.g., People, Components, system) for components and systems, and protect assets property to minimize bad effects under cyber attack (e.g., DoS attack).	L1_1_c_SYS, L2_1_d_SYS, L3_3_c_SYS	Common among <High-Advanced> and <Advanced> - The information system and industrial control system manage spare storage space, bandwidth, and other spares (People, Components, System) and minimize the impact of service denial attacks that send a large amount of information. For example, if services provided by an attacked system can not be stopped due to maintaining the level of availability, etc., in order to continue important functions, it is necessary to take the following measures. - Automatic or manual migration to standby system - Automatic or manual segregation of system components attacked by adversal actor - In order to ensure that required system performance is satisfied, use of resources must be monitored and adjusted. In addition, storage capacity and performance required in the future must be pre-estimated. - The organization shall: (a) Use a monitoring tool which the organization specifies in order to find signs of service jamming attacks on the information system. (b) Monitor resources of information system and industrial control system identified by the organization and judge whether sufficient resource is secured to prevent effective service jamming attacks.	S	-	○ (In addition to the following, SC-5(2)、SC-5(3))	○ (In addition to the following, A.12.1.3)	-	○ (SR 5.2)
			<Basic> - By implementing the security measures which the organization decides on, the information system and the industrial control system minimize the impact or protect from the impact of service denial attacks which the organization specifies, or from attacks on references to sources of these information, while performing a fallback operation	S	-	○ (SC-5)	○ (A.17.2.1)	-	
CPS.DS-7	Carry out periodic quality checks, prepare standby devices and uninterruptible power supplies, provide redundancy, detect failures, conduct replacement work, and update software for IoT devices, communication devices, circuits, etc.	L1_1_c_SYS, L2_1_d_SYS, L3_3_c_SYS	Common among <High-Advanced> and <Advanced> - The organization prepares short-term uninterrupted power supply which supports the switching of the information system to an alternative power source that can be used for a long period of time when the primary power source is lost.	O	-	○ (PE-11)	○ (A.11.2.2、A.11.2.3、A.11.2.4、A.12.1.3、A.17.2.1)	-	○ (SR 5.2, SR 7.5)
			<Basic> - In order to ensure that required performance of an information system and an industrial control system is satisfied, use of resources must be monitored and adjusted. In addition, storage capacity and performance that are required in the future are pre-estimated. - The organization protects devices from power outages and other failures that are attributable to malfunctions in the support utility. - The organization protects communication cables and power cables that transmit data or that support information service from interception, interference, and harm. - The organization properly maintaines devices to ensure continuous availability and integrity.	O	-	-		-	-
CPS.DS-8	When handling information to be protected or procuring devices that have an important function to the organization, useselect the IoT devices and servers equipped with anti-tampering devices.	L1_1_d_COM L2_3_b_COM	<High-Advanced> - When handling information that shall be protected or when procuring devices that have a function important to the organization, the organization procures devices that use anti-tampering devices. - When storing encryption keys for the cryptographic mechanism used in the information system and the industrial control system, the organization uses anti-tampering devices.	O	-	○ (SC-12)	○ (A.10.1.2)	-	○ (SR 5.2)
			<Advanced> - N/A	-	-	-	-	-	-
			<Basic> - N/A	-	-	-	-	-	-
CPS.DS-9	Properly control outbound communications that send information to be protected to prevent improper data breach.	L1_1_a_DAT, L2_3_c_SYS, L3_1_a_DAT	<High-Advanced> - The industrial control system shuts down, isolates the malicious code or notifies the administrator when detecting such code through IDS/IPS. - The organization/system analyzes the regular patterns of its systems' communication status and security alerts to create and use a profile that summarizes typical patterns of communication and security alerts, thereby enabling the detection of unknown threats and suspicious behavior (communication). - The information system prevents fraudulent and unexpected transfer of information via common system resources.	S	○ (3.13.4)	○ (In addition to the following, SC-4)	○ (A.13.2.1)	-	-
			<Advanced> - The information system blocks or isolates any malicious code for it detected through an IDS/IPS, or notifies the administrator of the code. - The organization collects information including newly released attacking trends, malware behaviors, and malicious IP addresses/domains (external intelligence). When necessary, the organization excutes responces to restrict communications to highly dangerous IP addresses or domains or so.	O/S	○ (3.13.1)	○ (SC-7)		-	○ (SR 5.2)
			<Basic> - The organization detects unusual data communications (e.g., too large data size, unexpected communication destination) outbound the organization, and limits such execution of communications when necessary.	O/S	-	-		-	-
CPS.DS-10	Conduct integrity checks of software runnning on the IoT devices and servers at a time determined by the organization, and prevent unauthorized software from launching.	L2_3_b_SYS	<High-Advanced> - The organization uses an automated tool that notifies the information system administrator when an inconsistency is found during integrity verification. - The organization uses tools to prevent the launch of the software if malicious software is detected. - The organization incorporates detection capacity into its incident response capacity to detect unauthorized changes that are made to the settings and security, such as an unauthorized promotion of system authority.	O/S	-	○ (In addition to the following, SI-7(2), SI-7(7))	○ (A.12.2.1)	-	-
			<Advanced> - The information system regularly inspects the integrity of the software and firmware. - The information system and the industrial control system prevent activation of unregistered software by registering in advance software that is permitted to activate.	S	-	○ (SI-7, SI-7(1))		-	○ (SR 3.1, SR 3.3, SR 3.4, SR 3.8)
			<Basic> - N/A	-	-	-		-	-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.DS-11	Perform integrity checking on information to be sent, received, and stored.	L1_1_b_DAT, L1_1_d_PRO, L3_2_a_DAT, L3_2_b_DAT	<High-Advanced> - The organization detects tampering with data transmitted from IoT devices, servers, etc. in industrial control systems, if possible, using integrity checking tools. - The organization incorporates detection capacity into its incident response capacity to detect unauthorized changes that are made to the settings and security, such as an unauthorized promotion of system authority.	O	-	○ (In addition to the following, SI-7(7))	○ (A.14.1.2, A.14.1.3)	-	-
			<Advanced> - The organization uses an integrity verification tool in an information system to detect any unauthorized changes that are made to communications data transmitted from IoT devices and servers. - The information system regularly inspects the integrity of the stored data. - The information system supports the technology of authenticating the sending domain in e-mail, and detects spoofing and tampering of e-mail.	O/S	-	○ (SI-7, SI-7(1))		-	○ (SR 3.1, SR 3.3, SR 3.4, SR 3.8)
			<Basic> - N/A	-	-	-	-	-	-
CPS.DS-12	Introduce an integrity check mechanism to verify the integrity of hardware.	L1_1_d_PRO, L2_3_b_SYS	<High-Advanced> - The organization detects hardware tampering (insertion of hardware/trojan) based on the difference between the genuine and counterfeit side channel information of the IC chip. - The organization detects hardware tampering (insertion of a hardware trojan) through testing physically readable ID of chip generated with the technology of PUF (Physically Unclonable Function).	O	-	-	-	-	-
			<Advanced> - The organization uses tools that detect unauthorized changes made to hardware components, labels that cannot be replicated easily, and verifiable serial numbers so that integrity can be verified. - By monitoring the site with surveillance cameras, the organization shall be able to detect physical tampering on the hardware that is significant to its operation.	O	-	○ (PE-6, SA-10(3))	-	○ (4.3.4.4.4)	-
			<Basic> - N/A	-	-	-	-	-	-
CPS.DS-13	Confirm that IoT devices and software are genuine products during the booting-up process.	L1_1_d_PRO, L2_3_c_ORG, L2_3_c_SYS	<High-Advanced> - The organization utilizes a tool having an automated mechanism to periodically check that the IoT device and installed software are genuine, using the device serial number, hash value, and the like.	O	-	-	-	-	-
			<Advanced> - The organization regularly checks that the IoT devices and the installed software are genuine products by using the serial numbers and hash values of the devices.	O	-	-	-	-	-
			<Basic> - During procurement and inventory count, the organization confirms that the IoT devices which the organization possesses are genuine products by checking the label.	O	-	-	-	-	-
CPS.DS-14	Maintain, update, and manage information such as the origination of data and data processing history throughout the entire life cycle.	L3_4_a_PRO, L3_4_b_PRO	<High-Advanced> - The organization checks whether or not there is an entity that does not implement the countermeasures that meet the level requested by the organization to the outsourced organization among the supply chain in the cyberspace where data managed by the organization is processed.	O	-	-	-	-	-
			<Advanced> - The organization links the source of the data obtained from other organizations or individuals/IoT devices outside of the organization to the data concerned and manages the entire lifecycle of the data from acquisition to deletion. - The organization identifies the source of data that is utilized by the organization and the organization/personnel that processed the data concerned.	O	-	-	-	-	-
			<Basic> - The organization links the source of the data obtained from other organizations or individuals outside of the organization to the data concerned, and manages the entire lifecycle of the data from acquisition to deletion.	O	-	-	-	-	-
CPS.DS-15	Use products that provide measurable security in order to ensure the availability of security reporting and the trustworthiness of sensing data through integrity protection.	L2_1_a_COM, L2_1_a_PRO, L2_3_a_ORG, L2_3_d_ORG	Common among <High-Advanced> and <Advanced> - When adopting a device (sensor) that has network connectivity, digitalizes dynamics in physical space, and transmits them to cyberspace, it is desirable to procure the said device with consideration of the following points: - Whether function that uses integrity verification tools to detect unauthorized changes made to communications data is implemented or not; - Whether the device has a unique ID identifiable by other IoT devices and servers, or has a certificate that can prove its genuineness through mutual authentication with the destination; - Whether or not the device's resource is at a level which can maintain the availability when subjected to a denial-of-service attack of a certain scale; - Whether or not it has tolerance against physical attacks.	O	-	○ (SC-5, SC-6, SI-7)	-	-	-
			<Basic> - The organization procures IoT devices (e.g. sensor) that are resistant to physical attacks.	O	-	-	-	-	-
CPS.IP-1	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	L1_1_a_SYS, L1_1_b_SYS, L2_1_a_ORG, L2_1_b_COM, L2_1_b_PRO, L2_3_b_ORG, L3_1_a_SYS, L3_3_d_SYS	<High-Advanced> - Before making changes to IoT devices and servers that are subjects of configuration management, the organization tests and approves these changes as well as creates a document on the changes. - The organization uses an automated mechanism to manage, apply, and confirm settings of IoT devices and servers from a single location. - The organization integrates security change management procedures particularly for industrial control systems, into existing process safety management procedures.	O	-	○ (In addition to the following, CM-3(2))	○ (A.12.1.2, A.12.5.1)	-	○ (SR 7.6)
			<Advanced> - When changes are made to the IoT devices and servers that are subjects of configuration management, the organization analyzes the impact the change has on security, decides whether the change can be made or not, and creates a document on the procedure. - The organization limits personnel who can make changes to approved IoT devices and servers (restricted access). - The organization makes changes to approved IoT devices and servers, as well as implements, records, and monitors those changes. - The organization uses a secure recovery method (e.g. entering a security code known only to the user before the change is implemented) if they forget the password of their accounts, IoT device and servers. - The organization regularly reviews policies and procedures for operation and change management to ensure that changes do not adversely affect the availability or safety of information system and industrial control system.	O	○ (In addition to the following, 3.4.3, 3.4.4, 3.4.5)	○ (In addition to the following, CM-3, CM-4, CM-5)		○ (4.3.4.3.2, 4.3.4.3.3)	
			<Basic> - Upon determining the most restrictive setting criteria that conform to their operation, the organization creates a document on the initial setting procedures and setting details for the IoT devices and servers that will be introduced and adjusts the settings according to the document. - The organization checks initial setting values of IoT devices before installing them, and adjusts the settings appropriately if they do not comply with the policy stipulated in CPS.AC-1. - The organization checks and records software installed in IoT devices before introducing them.	O	○ (3.4.2)	○ (CM-6)		-	

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.IP-2	Restrict the software to be added after installing in the IoT devices and servers.	L1_1_a_SYS, L2_1_a_ORG, L2_1_c_SYS, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> - The organization restricts software by using a list of software that is permitted to be executed on the information system and industrial control system (whitelist) or list of prohibited software (blacklist). Or, unpermitted software shall not be installed.	O/S	○ (In addition to the following, 3.4.8)	○ (In addition to the following, CM-7(4), CM7-(5))	○ (In addition to the following, A.12.5.1)	-	-
			<Advanced> - The organization adopts and manages a mechanism that manages software installation that is performed by users on the organization's system (information system or industrial control system) and monitors the events.	O/S	○ (3.4.9)	○ (CM-11)	○ (A.12.6.2)	○ (4.3.4.3.2, 4.3.4.3.3)	-
			<Basic> - The organization establishes a policy on software installation performed by users on the organization's system (information system or industrial control system) and has the users follow it.	O	-	-			○ (SR 7.6)
CPS.IP-3	Introduce the system development life cycle to manage the systems.	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG, L2_1_d_SYS, L3_3_c_SYS	<High-Advanced> - The organization explicitly presents the following requirements when procuring the system; - Requirements for security functions; - Requirements for security strength; - Requirements for security warranty; - Requirements for security-related documents; - Requirements for protection of security-related documents; - Description on the development environment of the system and the environment which the system is planned to operate under; - Acceptance criteria	O	-	○ (In addition to the following, SA-4)	○ (In addition to the following, A.6.1.5, A.14.2.2, A.14.2.5)	-	-
			<Advanced> - The organization manages the system in accordance with the system development lifecycle, which includes items of consideration regarding information security, and undergoes an information security risk management process throughout the entire system development lifecycle.	O	-	○ (In addition to the following, SA-3)		○ (4.3.4.3.3)	○ (SR 7.3, SR 7.4)
			<Basic> - The organization applies the general rules of the system's security engineering to specifications, design, development, introduction, and changes in building the system.	O	○ (3.13.2)	○ (SA-8)	○ (A.14.1.1, A.14.2.1, A.14.2.6)		
CPS.IP-4	Perform a periodical system backup and testing of components (e.g., IoT devices, communication devices, and circuits).	L1_3_a_DAT, L2_1_d_SYS, L3_3_c_SYS	<High-Advanced> - The organization confirms the trustworthiness of the medium and integrity of the information by regularly testing the backup information.	O	-	○ (In addition to the following, CP-9(1))	○ (In addition to the following, A.14.3.1)	○ (4.3.4.3.9)	-
			<Advanced> - The organization backs up their system documents according to the prescribed timing and frequency. - The organization protects the confidentiality, integrity, and availability of the information backed up on the storage base.	O	○ (3.8.9)	○ (CP-9)	○ (In addition to the following, A.18.1.3)		-
			<Basic> - The organization backs up information on user level and system level that is included in its information systems or industrial control systems according to the prescribed timing and frequency.	O			○ (A.12.3.1)		-
CPS.IP-5	Implement physical measures such as preparing an uninterruptible power supply, a fire protection facility, and protection from water infiltration to follow the policies and rules related to the physical operating environment, including the IoT devices and servers installed in the organization.	L1_1_a_SYS, L1_1_c_SYS, L2_3_b_SYS, L2_3_d_SYS, L3_1_a_SYS	<High-Advanced> - The organization adopts an automatic fire suppression system if a staffer is not stationed full time at a facility where its system is located.	O	-	○ (In addition to the following, PE-13, PE-15)	○ (A.11.1.4, A.11.2.1, A.11.2.2)	-	-
			<Advanced> - The organization maintains machine safety of equipment located within the area of their IoT devices and servers by using an uninterruptible power supply. - The organization adopts and maintains equipment and systems that run on an independent power supply which detect and extinguishes fire. - The organization have shut-off valves or isolation valves to protect areas with their IoT decides and servers from damages such as water leakages.	O				○ (4.3.3.3.1, 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6)	-
			<Basic> - The organization adopts a system that maintains the temperature and humidity of the area with its IoT devices and servers being within the acceptable level. - The organization regularly monitors the temperature and humidity of the area with its IoT devices and servers.	O	-	○ (PE-14)		-	-
CPS.IP-6	When disposing of an IoT device and server, delete the stored data and the ID (identifier) uniquely identifying the genuine IoT devices and servers as well as important information (e.g., private key and digital certificate), or make them unreadable.	L2_3_b_DAT	<High-Advanced> - The organization defines classifications including security categories of data saved in an IoT device or server to be scrapped, and introduces a mechanism for using the proper technique for deleting data with the strength and integrity needed or making the data unreadable according to the definition.	O	○ (3.8.3)	○ (MP-6)	○ (In addition to the following, A.8.2.3)	-	○ (SR 4.2)
			<Advanced> - The organization establishes a procedure for scrapping its equipment including IoT devices and servers, deletes data saved in the equipment or makes the data unreadable in accordance with the procedure, and makes sure that the action has been done successfully.	O			○ (A.8.3.1, A.8.3.2, A.11.2.7)	-	
			<Basic> - The organization deletes data that has been saved in its IoT devices or servers to be scrapped, or makes the data unreadable.	O				-	
CPS.IP-7	Assess the lessons learned from security incident response and the results of monitoring, measuring, and evaluating internal and external attacks, and improve the processes of protecting the assets.	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L2_1_a_ORG	<High-Advanced> - The organization has its security assessed by a third party.	O	-	○ (下In addition to the following, CA-2(1))	○ (A.16.1.6, A.18.2.1, Clause 9.1, Clause 9.2, Clause 10.1, Clause 10.2)	-	-
			<Advanced> - The organization draws up a security assessment plan before the assessment is carried out that includes the following so as to ensure that its security is assessed properly and systematically: - Security measures for assessment; - Assessment procedures for measuring the effectiveness of security measures; - Settings and mechanisms for carrying out the security assessment; - Methods of putting together the results of the security assessment and applications of the results.	O	○ (3.12.1)	○ (CA-2)		○ (4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8)	-
			<Basic> - The organization regularly evaluates whether its security measures have achieved expected results (i.e., security assessment) and reports the conclusions to the chief security officer, in addition to the evaluation of whether the measures are correctly implemented and managed. - The organization makes improvements on its security measures based on the results of the security assessment.	O					-
CPS.IP-8	Share information regarding the effectiveness of data protection technologies with appropriate partners.	L2_1_a_ORG	<High-Advanced> - The organization prepares a setting through an automated mechanism at just the right time that enables it and its appropriate partners to interactively share new information about data protection technologies or information about the effectiveness of the protection technologies.	O	○ (3.14.4)	○ (AC-21)	○ (A.16.1.6)	-	-
			<Advanced> - The organization prepares a setting that enables it to share new information about data protection technologies or information about the effectiveness of the protection technologies with its partners at just the right time.	O				-	-
			<Basic> - The organization prepares a setting that enables it to acquire new information about data protection technologies or information about the effectiveness of the protection technologies from its appropriate partners.	O	-	-		-	-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.IP-9	Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.	L1_1_a_PEO, L1_1_b_PEO, L1_1_c_PEO	Common among <High-Advanced> and <Advanced> - The organization makes changes to its staff members' rights to access certain systems and/or rooms on the premises when they are reshuffled or transferred internally. - To minimize impacts when a staff member leaves the organization, designate backup members regarding important duties as a supplier including operation and maintenance. - The organization identifies conditions in which re-screening is required such as changes in access authority to their own systems, and re-screen if necessary. - The organization conducts an interview on information security when personnel leave. - The organization ensures that responsibilities for security are met, particularly of personnel handling sensitive information, throughout the whole process from hiring to retirement.	O	○ (3.9.1 3.9.2)	○ (In addition to the following, PS-5)	○ (In addition to the following, A.7.2.3, A.7.3.1)	○ (下In addition to the following, 4.3.3.2.3, 4,3,3,2,4)	-
			<Basic> - The organization identifies the responsibility for security of personnel in the employment contract. The organization states that this responsibility should be sustained for a reasonable period of time after the termination of employment, in order to prevent information leakage after the termination of employment. - The organization reviews a staff member before granting him or her access to its systems. - The organization conducts the following when a staff member resigns or retires: - Disables the staff member's access to its systems within a certain period; - Disables the authentication and credentials related to the staff member; - Collects all system-related things for security that the staff member has used; - Retains access to the information about the organization and information systems that have been managed by the individual who is leaving.	O		○ (PS-3, PS-4)	○ (A.7.1.1, A.7.1.2, A.7.2.1, A.8.1.4)	○ (4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.6, 4.3.4.4.2)	-
CPS.IP-10	Develop a vulnerability remediation plan, and modify the vulnerability of the components according to the plan.	L1_1_a_SYS, L2_1_a_ORG, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> - The organization adopts and administers an automated mechanism for managing the status of defect correction.	O	-	○ (In addition to the following, SI-2(2))	○ (In addition to the following, A.14.2.3)	-	-
			<Advanced> - The organization defines tolerable risk by identifying through investigations and tests the impacts of patch application on the functions of other software applications and services on operations of IoT devices and servers. - The organization conducts tests to measure the effectiveness of corrections and the possibility of any secondary adverse effects, corrects the defects, and manages the corrections as part of the configuration management.	O	○ (3.14.3)	○ (SI-2)		○ (4.3.4.3.7)	-
			<Basic> - The organization systematically identifies, reports and responds to vulnerabilities in its own information systems and industrial control systems. The organization considers the following when formulating a plan. - Seriousness of threats or vulnerabilities - Risk in responding to vulnerabilities [Reference] It may be difficult to carry out application of security patches in a timely manner or application of patches itself to IoT devices in consideration of availability and functions of devices. In such cases, it is desirable to avoid occurrence of security incidents by thoroughly taking measures against threats (e.g. minimization of functions, strengthening of network monitoring).	O	-	-	○ (A.12.6.1)		-
CPS.MA-1	- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updateswith managed tools properly and in a timely manner while recording the history. - Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable.	L1_1_a_SYS, L2_1_a_ORG, L2_1_c_SYS, L3_1_a_SYS, L3_3_a_SYS L3_3_d_SYS	<High-Advanced> - The organization gives prior approval for the use of devices and/or tools needed for maintenance to update its IoT devices and servers, and conducts monitoring. - The organization inspects the devices and/or tools for maintenance brought in by the staff members who update its IoT devices and servers in order to make sure that no inappropriate or unauthorized changes will be made. - The organization inspects the media used for maintenance to update its IoT devices and servers in order to make sure that the media contain no malicious code before they are used. - The organization introduces an IoT device designed to remotely update different software programs (OS, driver, application) at the same time.	O	○ (3.7.1, 3.7.2, 3.7.4)	○ (In addition to the following, MA-3, MA-3(1), MA-3(2))	○ (In addition to the following, A.11.2.4, A.11.2.5, A.11.2.6, A.14.2.4)	○ (4.3.3.3.7)	-
			<Advanced> - The organization plans maintenance work such as updating its IoT devices and servers, implements the plan, checks the work done, and documents the entire maintenance. - The organization gives prior approval for maintenance work such as updating its IoT devices and servers, and conducts monitoring. - The organization gives prior approval for travel from its premises for any maintenance work away from its premises, such as updating its IoT devices and servers. It also takes necessary actions before the travel, such as deleting relevant saved data. - The organization checks all security measures that may have been affected by maintenance work, such as updating its IoT devices and servers, after the work is complete in order to make sure that the relevant equipment works correctly. - The organization keeps the records of maintenance work done, such as updating its IoT devices and servers. - The organization establishes a process for authorizing maintenance staff in order to keep the list of authorized maintenance organizations or staff members updated.	O	○ (In addition to the following, 3.7.1, 3.7.2, 3.7.4)	○ (In addition to the following, MA-2)			-
			<Basic> - The organization makes sure that a maintenance staff member sent unattended to do maintenance work on its information system and industrial control system has the necessary access rights. - The organization appoints its staff member with the access rights and technical skills needed so as to supervise maintenance work done by a staff member without the necessary access rights.	O	○ (3.7.6)	○ (MA-5)	○ (A.11.1.2)		-
CPS.MA-2	Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.	L1_1_a_SYS, L2_1_a_ORG, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	Common among <High-Advanced> and <Advanced> - The organization documents the policy and procedure relating to establishing and implementing a connection designed for remote maintenance, and implements the connection in accordance with the policy and procedure. - The organization provides authentication required for network access that it specifies when remote maintenance is carried out. It also ensures that the session and network connection are terminated when the remote maintenance is complete.	O	○ (3.7.5)	○ (In addition to the following, MA-4(2))	○ (In addition to the following, A.15.1.1)	-	-
			<Basic> - The organization develops and agrees to an implementation plan for remote maintenance before carrying out the maintenance, and checks the results of the maintenance done. - The organization keeps the records of remote maintenance done.	O		○ (MA-4)	○ (A.11.2.4, A.15.2.1)	○ (4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8)	-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	L1_1_a_SYS, L2_1_b_ORG, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> - In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g. OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related audit logs for some of the IoT devices that an organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specs of the IoT devices, such as using a log management system different than the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.	O/S	○ (In addition to the following, 3.3.7)	○ (In addition to the following, AU-6(1), AU-11(1))	○ (In addition to the following, A.12.4.4)	○ (In addition to the following, 4.4.2.4)	○ (In addition to the following, SR 2.10)
			<Advanced> - The information system and the industrial control system uses a cryptographic mechanism in order to ensure the integrity of an audit log and audit tool each. - The organization grants control over an audit log only to users assigned in accordance with the rules about security-related internal responsibility. - The information system issues an alert when an incident of failure takes place in the audit process.	O/S	○ (In addition to the following, 3.3.4, 3.3.8, 3.3.9)	○ (In addition to the following, AU-9(3), AU-9(4))	○ (In addition to the following, A.12.4.2)	○ (4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.3.3.3.9, 4.3.3.5.8)	○ (SR 2.8, SR 2.9, SR 2.11, SR 2.12)
			<Basic> - The organization specifies what is to be audited based on its risk management strategy and risk assessment results, and sees if the systems can acquire audit logs that show who did what and when in connection with the subjects of an audit. - The system generates an audit log prescribed from various system components. - The organization reviews and analyze a system's audit log regularly to see if there are any signs of security incidents that may cause damage to the organization, and make a report to the system administrator where necessary. - The organization confirms that the impact of audit activities on the performance of industrial control systems is tolerable.	O/S	○ (3.3.1, 3.3.2, 3.3.3)	○ (AU-2, AU-3, AU-6, AU-11)	○ (A.12.4.1, A.12.4.3, A.12.7.1)		
CPS.PT-2	Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS, L2_1_b_COM, L2_3_b_SYS, L3_1_a_SYS, L3_3_d_SYS	<High-Advanced> - The organization identifies software programs that are not allowed to be executed on a system. - Manage a "black list" or "white list" so that the software programs not allowed on the system cannot be executed. - The organization regularly review and update the black list or the white list. - The system blocks the execution of these programs in accordance with the specified rules.	O/S	○ (In addition to the following, 3.4.7, 3.4.8)	○ (In addition to the following, CM-7(2), CM-7(4))	○ (A.8.2.2, A.8.3.1)	-	-
			<Advanced> - The organization reviews the functions and services provided by its systems and items in order to identify the functions and services that could be deleted. - The organization uses network scanning tools, intrusion detection and prevention systems, and endpoint protection (e.g., a firewall, host-based intrusion detection system) in order to detect and prevent the use of banned functions, ports, protocols, and services. - The organization minimizes the functions and services of devices connected to the network such as multifunction printers in additional to typical IoT devices and servers.	O	○ (In addition to the following, 3.4.6)	○ (In addition to the following, CM-7)		○ (4.3.3.5, 4.3.3.7)	-
			<Basic> - The organization manages peripherals in use (e.g., USB flash drives) using a management ledger and keep them in a locked place. - The organization checks external storage devices connected to IoT devices or servers (e.g., USB flash drives) using antivirus software, use USB flash drives that can be checked for viruses, or take any appropriate action. - The organization plugs USB ports and serial ports out of use to physically block them.	O	○ (3.8.1, 3.8.4)	○ (MP-2, MP-3, MP-4)			○ (SR 2.3, SR 7.7)
CPS.PT-3	Introduce IoT devices that implement safety functions, assuming that these devices are connected to the network.	L2_2_a_ORG	<High-Advanced> - The organization adopt intrinsic safe designing to handle hazards of high severity, thereby minimizing damage (e.g., a design that lowers the energy of a hazard in order to limit an impact of an accident).	O	-	-	○ (A.16.1.6)	-	-
			<Advanced> - The organization carries out a security risk assessment that considers the aspect of safety (CPS.RA-4) in order to be clear about whether or not to need measures to ensure the physical safety of the assessed system, and to be clear about the levels of the measures. - The organization reduces hazards through intrinsic safe designing. If any hazard of high severity persists through this process, it is advisable to take alternative measures such as the following: - Ensure safety using an add-on such as safety a safety device; - Adopt a space design that keeps staff members away from hazardous devices. - The industrial control system operates in a predetermined manner when normal operation cannot be maintained due to a cyber attack etc.	O/S	-	-	-	-	○ (SR 3.6, SR 7.1, SR 7.2)
			<Basic> - N/A	-	-	-	-	-	-
CPS.AE-1	Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.	L1_1_a_COM, L1_1_a_SYS, L1_1_b_COM L1_1_c_COM L1_3_b_ORG, L1_3_c_ORG, L2_1_b_ORG, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> - The organization uses a mechanism for automatically collecting information about network configurations and the software configurations of devices in order to monitor the most recent status at all times. - The information system forces the application of users' access rights approved (by the administrator) in order to control data flows within a system (and between interconnected systems). - The organization physically or logically separates a network of industrial control systems with high importance from a network of industrial control systems with lower importance. - The organization/system analyzes the regular patterns of its systems' communication status and security alerts to create and use a profile that summarizes typical patterns of communication and security alerts, thereby enabling the detection of unknown threats and suspicious behavior (communication).	O/S	○ (In addition to the following, 3.1.3, 3.14.1, 3.14.6, 3.14.7)	○ (In addition to the following, AC-4, CM-2(2), SI-4, SI-4(13))	-	-	-
			<Advanced> - As part of its configuration management, the organization identifies and documents the configuration that serves as the latest baseline of an information system and an industrial control system. - If any changes are made to the baseline configuration of an information system and industrial control system, promptly update the baseline configuration so that the most recent status is available at all times. - The organization allows one system to connect to a different system only after it determines that connecting the system to the other system is safe enough in terms of security measures. - The industrial control system provides services to the network of control systems without connecting to networks other than industrial control systems. - The organization exercises discretionary access control according to the user's access rights in order to control data flows within an information system (and between interconnected systems).	O/S	-	○ (In addition to the following, CA-3)	-	○ (4.4.3.3)	-
			<Basic> - The organization documents information that serves as a baseline including an information system's and an industrial control system's network configuration, assets, information about device setups and configurations, and regularly checks the document to see if its content remains relevant. - The organization logically or physically segments the control system's network from the network composing of the information system. [Reference] Implement physical segmentation in environments physically separated from other networks. Alternatively, in environments physically close to other networks, it is possible to implement logical segmentation in consideration of the cost of the measure.	O	○ (3.4.1)	○ (CM-2)	-		-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.AE-2	Appoint a chief security officer, establish a security management team (SOC/CSIRT), and prepare a system within the organization to detect, analyze, and respond to security events.	L1_3_a_ORG	<High-Advanced> - The organization efficiently analyzes audit logs collected through 24-h, 365-day security monitoring by using an automated analysis tool. - It is desirable for the organization to include not only its conventional IT environment but also its control system and IoT devices in the scope of security monitoring. - It is desirable for the organization to regularly evaluate the maturity of its security measure organizations in order to continue improving its security-related operations, including security monitoring and the ways incidents are handled. [Reference] For example, SIM3 (Security Incident Management Maturity Model) is available as metrics for the evaluation of security organizations (SOC/CSIRT).	O/S	-	○ (In addition to the following, SI-4(2), SI-4(5))	○ (In addition to the following, A.12.4.1, A.16.1.5)	-	-
			<Advanced> - The organization refers to risk assessment results and, considering the following angles, establishes what to monitor and what to include in correlation analysis. - The scope of systems to monitor - Which device logs should be collected for analysis (see CPS.AE-3) - The organization regularly reviews audit logs collected through monitoring. - The organization continues to collect and manage information about assets, device configurations, and network configurations in order to evaluate its security status. - The organization examines the results of correlation analysis and other data to accurately detect security events that must be addressed and take action in accordance with the security operation process. See CPS.RP-1 for details of the process. - The organization regularly reports the state of organizational and system security to the chief security officer or other appropriate staff members. It is desirable that the regular report should include the following shown below: - Results of log analysis (e.g., the number of incidents handled; summaries of typical incidents that have been handled; threats that have emerged; issues in monitoring); - Policy for future improvements in monitoring.	O/S	○ (3.6.1, 3.12.2, 3.14.6, 3.14.7)	○ (CA-7, IR-4, SI-4)		○ (4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8)	○ (SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2)
			<Basic> - The organization identifies who the chief security officer/contact person is in both information system and industrial control system so that the officer/contact person can handle security-related internal and external communications.	O	-	-	○ (A.6.1.1)	-	-
CPS.AE-3	Identify the security events accurately by implementing the procedure to conduct a correlation analysis of the security events and comparative analysis with the threat information obtained from outside the organization.	L1_1_b_SYS, L1_3_a_SYS	<High-Advanced> - The organization conducts a trend analysis examining the latest information about threats, vulnerability, and assessments of security management measures carried out several times in order to determine whether the activities for continuous monitoring need any correction. - The organization carries out policy tuning (management of signatures to apply) and maintenance for devices such as IDS, IPS, and SIEM on its own. - The organization creates custom signatures used for sensors on its own. - In order to properly detect security events that are likely to adversely affect the organization, the organization collects and analyzes logs of edge devices such as IoT devices in addition to the logs of devices presented in <Advanced>, if possible.	O	○ (In addition to the following, 3.14.4)	○ (In addition to the following, CA-7(3))	○ (A.12.4.1)	-	-
			<Advanced> - It is desirable that the organization should monitor mainly logs of the devices listed below for real-time analysis to appropriately detect security events highly likely to have an adverse effect on its own organization . This will require the handling of many different logs. Hence, it is necessary to normalize logs to store them in the same database or to use SIEM for efficient analysis. It is also advisable to handle information about network flows if it is available. - Logs and network flows from network systems, e.g., firewalls - Logs from security devices, e.g., IPS/IDS - Access logs of web servers - Logs from various systems, e.g., ActiveDirectory; DNS - Logs related to users' terminals	S	○ (3.12.3)	○ (CA-7)		-	○ (SR 6.1)
			<Basic> - The organization checks each notice from firewalls and endpoint security products in order to identify security events that may have an adversal impact on the organization.	O				-	-
CPS.AE-4	Identify the impact of security events, including the impact on other relevant organizations.	L1_3_b_PRO	<High-Advanced> - The organization adopts an automatic mechanism for quantifying and monitoring the form, scale, and cost of a security event that has occurred. - The organization has its security measure organizations (SOC/CSIRT) analyze the functions of the malware, or program, or script that is placed by an attacker if any is found in a security event that has occurred. - The organization constructs a hypothesis about the profile of the attacker (e.g., his/her organization; the purpose of the organization's activities). [Reference] It is envisaged that the impact assessment of a security event would be difficult in an environment where multiple systems are interconnected to comprise a "system of systems". The document "Observations about the Impact Assessment of an Internet of Things (IoT) Incident" (Cloud Security Alliance, 2016) is an advanced attempt to examine issues relating to the impact assessment. It attempts to assess an impact according to the characteristics of the device or the service and to the number of devices.	O/S	-	-	○ (In addition to the following, A.16.1.6)	-	-
			<Advanced> - The organization works with IPA, JPCERT/CC, the industry's ISAC, and a security vendor to collect information, thereby interlinking and sharing information about threats and vulnerability to obtain a whole picture of the security event. - The organization requests an external security vendor to analyze the functions of the malware, or program, or script placed by an attacker if any is found in a security event that has occurred.	O	○ (3.6.1)	○ (IR-4, IR-4(8))	○ (A.6.1.4)	-	-
			<Basic> - N/A	-	-	-	-	-	-
CPS.AE-5	Specify the criteria to determine the risk degree of security events.	L1_3_a_PRO	<High-Advanced> - The organization determines its core business that must continue/recover before any other operations in prior and identifies and prioritizes important resources (other relevant organizations, employees, items, data, systems, etc.) and functions vital for continuing applicable businesses. * CPS.AM-6 and CPS.BE-2 include examples of similar measures. - The organization uses an automated mechanism designed to help track security events and collect and analyze information about threats and vulnerability related to incidents, so that it applies the findings to classification (triage) of security events.	O	-	○ (In addition to the following, CP-2(8), IR-5(1))	○ (A.16.1.4)	○ (4.2.3.10)	-
			<Advanced> - The organization classifies security events, taking into account the recovery time objectives for the systems, the order of priority in recovery, and metrics in the process of its security operation.	O	-	○ (In addition to the following, CP-2)		-	-
			<Basic> - The organization specifies security events that must be reported, considering the level of the impact the security event has. [Reference] For example, the following document is available for reference when an organization decides on a measure of the severity of the impact of a security event. - "SP 800-61 rev.1" (NIST, 2008) Prioritization of the 3.2.6 Incident	O	-	○ (IR-8)		-	-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.CM-1	Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.	L1_1_a_SYS, L1_1_c_SYS, L1_3_a_SYS, L2_1_b_ORG, L2_3_c_SYS, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> - The information system routes communications to the network to which a recipient's IP address belongs via a proxy server authenticated on a controlled interface. - The information system and the industrial control system monitor and control the use of mobile code. - The information system monitors and controls the use of protocols used for audio and video transmission (e.g. VoIP).	S	○ (In addition to the following, 3.13.13, 3.13.14)	○ (In addition to the following, SC-7(8))	-	-	-
			<Advanced> - The organization monitors and controls communications at the boundary between industrial control system and information system. - The organization creates a network segment isolated from access to the internal network ("demilitarized zone [DMZ]") between the internal network and external networks (e.g., the Internet). - The information system is connected to an external network or system only via a controlled interface that consists of a boundary protection system placed according to the organization's security architecture. - The information system ensures that each external communications service is provided via a controlled interface (e.g., a gateway, router, and firewall). - The organization establishes a communications control policy for each controlled interface (e.g., a gateway, router, and firewall). - The system on a controlled interface rejects network communication by default and permits it as an exception. - The organization monitors communications at the external boundaries of the information system and at major internal boundaries within the information system for large amounts of communication from a particular source or multiple sources, and takes appropriate action when necessary (e.g., blocking of communication from a specific IP address).	O/S	○ (In addition to the following, 3.13.6)	○ (In addition to the following, SC-7(4), SC-7(5))	-	-	○ (SR 6.2)
			<Basic> - The organization monitors and controls communications on the information system's external boundary as well as on the key internal boundary within the information system.	O	○ (3.13.1, 3.13.5)	○ (SC-7)	-	-	
CPS.CM-2	Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.	L1_1_a_SYS, L1_1_c_SYS, L2_3_b_PEO, L2_3_b_SYS, L2_3_d_SYS, L3_1_a_SYS	<High-Advanced> - The organization tracks and monitors the locations and relocation of important assets within the scope of its management of particularly important assets.	O	-	○ (In addition to the following, PE-20)	-	-	-
			<Advanced> - The organization reviews the relevant audit log regularly or when an incident or a sign of an incident appears if a physical access log from access control is available while 24-h monitoring is not conducted through security cameras or by any other means. - A person in charge accompanies a visitor into the area where the organization's assets that must be protected are directly accessible (e.g., an office) in order to monitor the visitor's behavior. - The organization monitors through security cameras or by other means physical access to its facilities that are vital for its operations and house IoT devices and servers, thereby enabling early detection of any physical security incidents and immediate action. - If the above physical security measures may be difficult to implement for items such as IoT devices and servers that may be critical to the organization's operation because they are in a remote location or for any other reasons, consider using tamper-resistant equipment (CPS.DS-6) or taking any other appropriate measures to enhance the physical security properties of the equipment itself.	O	○ (3.10.4, 3.10.5)	○ (PE-3, PE-6)	○ [A.11.1.1, A.11.1.2, A.11.1.3]	-	-
			<Basic> - If the organization is unable to control access to, or provide video surveillance service for, the areas that should allow only limited physical access because of issues of costs and other reasons, it takes alternative manual measures, such as that its employee in charge accompany a visitor on the premises. - The organization implements physical security measures to control access to designated areas in the facility that do not be allowed for the general public to access. - The organization verifies the access authority of the personnel before permitting the physical access and collects and manages the records of entry and exit.	O				-	-
CPS.CM-3	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.	L1_1_b_SYS, L2_2_a_COM, L3_3_a_DAT, L3_3_d_SYS	<High-Advanced> - IoT devices, or systems that contain these devices, examine information output from software programs or applications to see if it matches the expected content in order to prepare for certain attacks that may have a consequence different to a normally expected outcome (e.g., command injection). - The information system automatically updates the logic to detect malicious code through an IDS/IPS. - The information system detects exploit codes that attacks unknown vulnerabilities by installing on endpoints (especially, IoT devices and servers with various functions) detection/restoration software using technologies of behavioral detection of malware. - The information system executes real-time scanning of files from external sources.	S	○ (In addition to the following, 3.14.4, 3.14.5)	○ (In addition to the following, SI-10, SI-15)	○ (A.12.2.1)	-	○ (SR 3.2)
			<Advanced> - The information system blocks or isolates any malicious code for it detected through an IDS/IPS, or notifies the administrator of the code. - The information system detects exploit codes by installing on endpoints (IoT devices, servers, and so on) detection/restoration software using technologies of pattern matching of malware. - The organization considers implementing whitelist-type malware protection for IoT devices with limited functions. * Especially regarding IoT devices and control devices, OS to which anti-malware software can be applied may not be used. It is desirable for the organization to confirm whether devices to be introduced are compatible with anti-malware software at the phase of procurement and to select compatible ones. If it is difficult to procure devices compatible with anti-malware software, it is desirable to take alternative measures such as introducing/strengthening a malware detection mechanism on a network.	S	○ (3.14.2, 3.14.3)	○ (SI-3)		-	
			<Basic> - Information system and industrial control system verify the effectiveness of input data by checking whether the data conforms to a specified format or content.	S	-	-	-	-	○ (SR 3.5)
CPS.CM-4	Validate the integrity and authenticity of the information provided from cyberspace before operations.	L3_3_a_DAT, L3_3_d_SYS	<High-Advanced> - The organization introduces the concept of "whitelisting" for data entry in order to specify known items and systems considered trustworthy as the sources of input data, and the format allowed for the input data. - IoT devices and servers begin communication with other IoT devices only after the devices are mutually authenticated successfully so that the source of data is always clear. - The information system and the industrial control system protect the authenticity of communications sessions.	S	○ (In addition to the following, 3.14.5)	○ (In addition to the following, SI-10(5))	○ (A.13.2.1, A13.2.3)	-	○ (SR 3.2)
			<Advanced> - The information system uses an integrity verification tool to detect any unauthorized changes that are made to communications data transmitted from IoT devices and servers. - IoT devices and servers that are acknowledged as critical to the organization's operations begin communication with other IoT devices only after the devices are mutually authenticated successfully so that the source of data is always clear.	S	○ (3.14.5)	○ (In addition to the following, SI-7)		-	
			<Basic> - N/A	-	-	-	-	-	-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.CM-5	Monitor communication with external service providers so that potential security events can be detected properly.	L1_1_a_COM, L1_1_a_SYS, L1_1_b_COM L1_1_c_COM L1_3_b_ORG, L1_3_c_ORG, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS,	<High-Advanced> - The organization requires its provider of external information system services to make clear the functions, ports, and protocols needed for the use of the services, along with other services. - The organization monitors whether the matters made clear as stated above are observed.	O/S	-	○ (In addition to the following, SA-9(2))	○ (In addition to the following, A.13.1.2, A.15.2.2)	-	-
			<Advanced> - The organization documents its security requirements for the staff from its external service provider and system developer, and includes the requirements in the agreement. - The organization requires its external service provider and system developer to contact it when any of its staff members who have authorizations for its system are transferred or when their employment terminates. - It is desirable that the organization should manage changes to services offered by its external service provider, taking account of relevant information about operations, the importance of its business systems and processes, and re-assessed risks. - The organization monitors whether its external service provider and system developer complies with the requirements. - The organization monitors access to its system by its external service provider and system developer in order to detect any unauthorized access by these external businesses that results from an action or failure to act. - The organization reports the results of the monitoring of activities by its external service provider and system developer to the appropriate system administrator.	O/S	○ (3.14.6, 3.14.7)	○ (In addition to the following, PS-7, SI-4)		-	-
			<Basic> - The organization requires its provider of external information system services and system developer to draw up and introduce security requirements such as those related to the following in accordance with the rules which the organization is subject to or which apply to the provider and developer. - Adequate security measures to take (e.g., measures that deserve ISMS Certification) - Proper management of data in operation - Proper data erasure when the use of the services ends	O	-	○ (SA-9)	○ (A.14.2.7)	-	-
CPS.CM-6	As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other “organization”, people, components, and systems.	L1_1_a_COM, L1_1_a_SYS, L1_1_b_COM L1_1_c_COM L1_3_a_SYS, L1_3_b_ORG, L1_3_c_ORG, L2_1_a_ORG, L2_1_c_ORG, L2_1_c_SYS, L2_3_b_ORG, L2_3_b_SYS, L2_3_c_SYS, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> - The organization uses a mechanism for automatically detecting unauthorized hardware, software, or firmware in a system, if any. - The information system regularly audits whether the actual configuration grasped conforms to the baseline configuration defined by the organization, and responds appropriately. (Example: blocking unplanned connections except those permitted by the organization as an exception) - The information system and the industrial control system disable network access by any unauthorized components that have been detected, separate these components from the network, or take any primary action, and notify the system administrator of the components. - The organization records past versions of baseline configurations (eg, hardware, software, firmware, configuration files, configuration records) to enable rollback of baseline configurations of information systems. - When a control device or IoT device does not have a rollback function for firmware etc., it is desirable for an organization to have a spare control device or IoT device. - It is envisaged that some IoT devices cannot connect to the existing asset management system. Hence, manage assets and configurations with the possibility of operating more than one asset management system in mind, within the organization’s manageable bounds. *A related measure requirement is CPS.AM-1.	O/S	-	○ (In addition to the following, CM-8(3))		-	-
			<Advanced> - It is desirable that the organization should update the list of information about its assets and configurations when it installs or deletes new assets or when it updates its system. - The information system ensures that each external communications service is provided via a controlled interface (e.g., a gateway, router, and firewall). - The organization establishes a communications control policy for each controlled interface (e.g., a gateway, router, and firewall). - The system on a controlled interface rejects network communication by default and permits it as an exception. - The information system and the industrial control system terminate the network connection after a session ends, or when a session remains inactive for a certain length of time. - The organization monitors communication on controlled interfaces in order to detect any communication to unapproved items or systems, or communication that conveys an inappropriate content.	O/S	○ （In addition to the following, 3.4.1, 3.4.3, 3.13.9, 3.14.6, 3.14.7)	○ (In addition to the following, CM-3, CM-8(1), SC-7(4), SC-7(5), SI-4)		-	-
			<Basic> - The organization creates a ledger to manage model numbers of assets that includes servers, software versions, and the expiration of support services. Take regular inventory. - The organization regularly checks whether necessary measures are taken during operation (e.g., checking IoT devices for any unauthorized use or theft; applying a patch; checking logs) and the state of IoT devices.	O	○ (3.4.1)	○ (CM-8)		-	-
CPS.CM-7	Confirm the existence of vulnerability that requires a regular check-up in IoT devices and servers managed within the organization.	L1_1_a_SYS, L2_1_c_SYS, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> - The organization conducts vulnerability diagnosis at planned timings such as planned stopping so as not to adversely affect the operation of the system managed by the organization. And then, identify and list vulnerabilities that exist in the system owned by the organization. - When using tools to conduct vulnerability diagnosis, the organization should use tools that can quickly update the vulnerability database of the system being diagnosed. - The organization updates the vulnerability of scanned systems regularly, or when newly-identified weaknesses are reported. - The organization implements a system for authorizing privileged access to the relevant system components in connection with the specified vulnerability scanning.	O	○ (In addition to the following, 3.11.2)	○ (In addition to the following, RA-5(1), RA-5(2), RA-5(5))	○ (A.12.6.1)	○ （下記に加えて, 4.2.3.7）	-
			<Advanced> - The organization has its systems and applications scanned for vulnerability regularly, or when any newly-found weaknesses that affect the systems and/or applications are reported. - The organization uses a tool for vulnerability scanning. Applying the standard methods that meet the following means that part of the vulnerability management process should be open to automation. - List defects in the platform and software, and wrong setups. - Format a checklist and test procedure. - Assess the impact of the vulnerability. - The organization corrects identified weaknesses through risk assessment within an appropriate period. - The organization shares the information acquired through the above process with other system administrators in the organization, thereby learning about similar weaknesses found in the other information systems, and correct them as necessary. [Reference] Japan Vulnerability Notes (https://jvn.jp/) and other sources of information are available for reference to obtain information regarding vulnerability. Also, CVSS (https://www.ipa.go.jp/security/vuln/CVSS.html Illustrated by IPA) could be used as a referential indicator to evaluate the impact level of vulnerability.	O	○ (3.11.2, 3.11.3)	○ (RA-5)			-
			<Basic> - The organization regularly has its systems and applications scanned for vulnerability.	O				○ (4.2.3.1)	-
CPS.DP-1	Clarify the role and responsibility of the organization as well as service providers in detecting security events so that they can fulfill their accountabilities.	L1_3_a_ORG	Common among <High-Advanced>, <Advanced> and <Basic> - The organization determines the log information that would help detect security events and thus should be collected based on its strategies relating to risk management and assessment results. - The organization ascertains that its business partner (service provider) has an audit log that records activity of service users, exception handling, and security events that the provider has acquired. - The organization ascertains that the audit log acquired by its service provider records activity of service users, exception handling, and security events, and is protected in a proper way.	O	○ (3.12.3)	○ (CA-7, PM-14)	○ (A.6.1.1, A.12.4.1)	○ (4.4.3.1)	-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.DP-2	Detect security events in the monitoring process, in compliance with applicable local regulations, directives, industry standards, and other rules.	L1_2_a_ORG, L1_3_a_ORG	Common among <High-Advanced>, <Advanced> and <Basic> - The organization sees if any legal system, industry standards, or agreements with customers that are related to monitoring services exist and, if any do, learn what constraints are imposed. - The organization conducts monitoring in accordance with the rules learned above to detect any security events. - The organization regularly reviews its monitoring activities to make sure that they conform to the rules.	O	○ (3.12.3)	○ (CA-7, PM-14)	○ (A.18.2.2)	○ (4.4.3.2)	-
CPS.DP-3	As part of the monitoring process, test regularly if the functions for detecting security events work as intended, and validate these functions.	L1_3_a_ORG	<High-Advanced> - The organization conducts a trend analysis examining the latest information about threats, vulnerability, and assessments of security management measures carried out several times in order to determine whether the activities for continuous monitoring need any correction. - The organization introduces known and harmless test cases to its systems to test its mechanism for detecting malware. - The organization regularly tests the mechanism it uses for intrusion detection monitoring. The frequency of the test depends on the type of tool the organization uses and the way the tool is installed.	O/S	-	○ (In addition to the following, CA-7(3), SI-3(6), SI-4(9))	○ (In addition to the following, A.14.3.1)	-	-
			<Advanced> - The organization establishes and manages a procedure for a regular review of its system monitoring activities to see if they conform to the organization's risk management strategy and the order of priority for actions to handle risks. - The organization calculates the percentages of false detections and false negatives when correlation analysis of information pertaining to the security of network devices or endpoints is conducted, thereby checking the validity of the detection mechanism regularly.	O	-	○ (CA-7, PM-14)	○ (A.14.2.8)	○ (4.4.3.2)	○ (SR 3.3)
			<Basic> - N/A	-	-	-	-	-	-
CPS.DP-4	Continuously improve the process of detecting security events.	L1_1_b_SYS, L1_3_a_ORG	<High-Advanced> - The organization creates and tunes detection rules based on various information as sources in order to improve its detection ability. - Developing the rules of correlation analysis - Developing own signature of IPSs or IDSs - Developing the organization's own black list - The organization/system analyzes the patterns of its system's communication and security alerts to create and use a profile that summarizes typical patterns of communication and security alerts, thereby tuning its efforts to reduce the numbers of false detections and false negatives.	O/S	-	○ (In addition to the following, SI-4(13))	○ (A.16.1.6)	-	-
			<Advanced> - The organization prepares and manages a procedure for regularly reporting the state of organizational and system security to its appropriate staff members (e.g., management). It is desirable that the organization should define the reporting as an occasion for becoming aware of the latest threats or threats to remaining risks so that the organization acts to enhance its security. - For example, if alerts such as those shown below are issued and there is a sign of increasing security risks, raise the level of the system's monitoring activities based on information from reliable sources. * The list below is an excerpt from "Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT Version 1.0" (ISOG-J, 2018). ・ Characteristics of the attack ➢ Form of the attack; contents of relevant communications ➢ Core attack code ・ Traces of the attack ➢ Contents of the damaged communications ➢ Logs that remain in the server or the hands of clients ➢ Other characteristics that remain in the server or the hands of clients ・ Detected names in the security products	O	○ (3.14.6, 3.14.7)	○ (CA-7, SI-4)		○ (4.4.3.4)	-
			<Basic> - N/A	-	-	-	-	-	-
CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.	L1_1_a_SYS, L1_3_a_PEO, L1_3_a_PRO, L2_1_a_PRO, L2_1_b_PRO, L2_1_c_PRO, L2_2_a_PRO, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> - If the information system and the industrial control system receive any invalid data, they operate as stated in an expected manner in conformity with the purpose of the organization and system.	S	-	(In addition to the following, SI-10(3), SI-17)	○ (A.16.1.5)	-	-
			<Advanced> - The organization includes contents regarding what to do to detect, analyze, contain, reduce, and recover from incidents in its security operation manual. - Keep a record of all incidents and how they have been handled. - Decide whether the organization should report the fact to any external organization of an incident that has occurred and how it has been handled.'	O	-	○ (In addition to the following, IR-8)		○ (4.3.4.5.1)	-
			<Basic> - The organization develops and manages a process of security operation it should follow when a security incident arises that it must address. It is advisable to include contents such as the following in the process: - Response procedure for the person who received the incident report - Instructions and orders, and how to prioritize actions in an emergency; - Incident response; - Incident impact assessment and damage analysis; - Information gathering, selecting information that the organization needs; - Communication and announcement to relevant internal personnel; - Communication with relevant external organizations; - The system (especially, industrial control system) shuts down, issues an alert to the administrator, or takes other fail-safe actions if any abnormality (e.g., malfunction) occurs in IoT devices or servers. [Reference] "SP 800-61 rev.1" (NIST, 2008) is available for reference to determine the process for handling security incidents that have arisen.	O/S	○ (3.6.1)	○ (IR-4)			-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.RP-2	As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.	L1_3_b_PEO, L1_3_b_PRO, L1_3_c_PEO, L1_3_c_PRO	<High-Advanced> - The organization assumes the course of action for security incidents of the supply chain and prepares a procedure that adjusts incident responses between the organization and other organizations that are concerned with the supply chain. - The organization adjusts the incident response process of an external service provider that contains important features in order to continue its business, as well as adjusting the organization's incident response process to meet the incident response requirements. - The organization interlinks information regarding threats and vulnerabilities with how individual security incidents have been handled so as to improve its understanding of the situations. [Reference] Violations in the security incidents of supply chain include violations on system components, IT products, development processes, developers, distribution processes, and warehouse facilities.	O	-	○ (In addition to the following, CP-2(7), IR-4(4), IR-4(10))	○ (In addition to the following, A.17.1.2)	-	-
			<Advanced> - The organization determines an alternative processing site in case the availability of its primary processing site has been compromised by a security incident. - The organization sets forth in the service agreement that if its primary processing function becomes unavailable, certain operations are moved to resume at the alternative processing site within the recovery time objective that the organization specifies in order to ensure that it continues to perform its critical missions and operational functions. - The organization designates an alternative processing site away from its primary processing site in order to mitigate the vulnerability to the same threats. - The organization prepares internal resources for incident handling assistance (e.g., help desk; CSIRT). These resources offer advice and support related to security incident handling and reporting for system users of the information system and industrial control system, and are an integral part of organizational ability to handle incidents.	O	-	○ (In addition to the following, CP-7, CP-7(1), CP-7(2), CP-7(3), IR-7)		○ (4.3.2.5.2, 4.3.2.5.3, 4.3.4.5.1, 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.5)	-
			<Basic> - If any security incident that requires handling is found, report it promptly to relevant organizations such as IPA and JPCERT/CC in order to receive advice about providing assistance in handling, identifying how the incident has occurred, analyzing the tactic, and preventing any recurrence.	O	-	○ (IR-6)	○ (A.16.1.1, A.16.1.2)	-	-
CPS.RP-3	Include security incidents in the business continuity plan or emergency response plan that outlines the action plans and response procedures to take in case of natural disasters.	L1_3_a_PRO, L1_3_a_DAT	Common among <High-Advanced> and <Advanced> - The organization will establish a system of business continuity in emergency for information systems, industrial control systems and managers of related processes. This system defines the priority of the system for recovering operation when an event occurs that causes interruption in business continuity. - The organization develops and manages a business continuity plan or an emergency response plan specifically for security incidents with certain characteristics, such as that the damage the incident inflicts is less obvious than that caused by a disaster, making it difficult to specify when the business continuity plan should be carried out, or that identifying the cause of the incident has high priority. - The organization ensures that the business continuity plan or emergency response plan it develops specifically for security incidents goes along with the organization-wide policy on business continuity.	O	-	○ (CP-2)	○ (A.17.1.1)	○ (4.3.2.5.4)	-
			<Basic> - N/A	-	-	-	-	-	-
CPS.RP-4	Take appropriate measures on goods (products) whose quality is expected to be affected by some reasons, including its production facility damaged by the occurrence of the security incident.	L1_3_b_COM	Common among <High-Advanced> and <Advanced> - The organization provides an overview of a security incident for relevant external entities including business partners and end users, and collects detailed information about damage inflicted by the incident. - The organization coordinates actions related to recovery and post-incident processing with relevant external entities involved in the supply chain. It is advisable to identify the items for handling in accordance with the approaches included in CPS.AM-2 and CPS.AM-3.	O	○ (3.6.2)	○ (In addition to the following, IR-4, IR-4(10))	○ (A.17.1.1)	-	-
			<Basic> - The organization considers stating what to do with items produced after the incident in the business continuity plan or emergency response plan, taking into account the type of the organization's business. Note that the business continuity plan or emergency response plan may not be for security incidents.	O	-	○ (CP-2)		-	-
CPS.CO-1	Develop and manage rules regarding publishing information after the occurrence of the security incident.	L1_3_a_PRO	Common among <High-Advanced>, <Advanced> and <Basic> - The organization develops and manages rules regarding publishing of information after a security incident that cover the following: - What information should be published? - Timing of publishing of the information; - Who is in charge of publishing the information? - The process for publishing the information.	O	-	-	○ (Clause 7.4)	○ (4.3.4.5.9)	-
CPS.CO-2	Include the item in the business continuity plan or emergency response plan to the effect that the organization shall work to restore its social reputation after the occurrence of a high-risk security incident.	L1_3_a_PRO	Common among <High-Advanced>, <Advanced> and <Basic> - The organization sets up a single point of contact for the media and business partners requesting information, thereby ensuring consistency in communication with them. - The organization remains aware of the positive side of providing a detailed explanation about damage caused by a security incident while considering the confidentiality of the important information.	O	-	-	-	-	-
CPS.CO-3	Include the item in the business continuity plan or emergency response plan to the effect that the details of the recovery activities shall be communicated to the internal and external stakeholders, executives, and management.	L1_3_a_PRO	Common among <High-Advanced> and <Advanced> - The organization provides an overview of a security incident for relevant external entities including the regulatory authorities, business partners, and end users, and collects detailed information about damage inflicted by the incident. - The organization coordinates actions related to recovery and post-incident processing with relevant external entities involved in the supply chain. An example of these actions is recalling items produced when a security incident in the production system has occurred.	O	○ (3.6.1)	○ (In addition to the following, IR-4, IR-4(10))	○ (A.17.1.2)	-	-
			<Basic> - The organization specifies roles and responsibilities taken when any security incident that may affect it occurs, along with the personnel who are assigned to these roles and responsibilities and their contact information. - The organization provides an overview of a security incident and an explanation about damage inflicted by the incident for the personnel responsible for decision-making associated with business continuity in order to ensure that the right decision is made.	O	-	○ (CP-2)		○ (4.3.2.5.5, 4.3.4.5.9)	-
CPS.AN-1	Understand the impact of the security incident on the whole society including the organization and relevant parties such as partners based on the full account of the incident and the probable intent of the attacker.	L1_3_a_COM, L1_3_a_PRO	<High-Advanced> - The information system adopts an automatic mechanism for quantifying and monitoring the form, scale, and cost of a security incident that has occurred. - The organization has its security measure organizations (SOC/CSIRT) analyze the functions of the malware, or program, or script that is placed by an attacker if any is found in a security incident that has occurred. - The organization constructs a hypothesis about the profile of the attacker (e.g., his/her organization; the purpose of the organization's activities). [Reference] It is envisaged that the impact assessment of a security incident would be difficult in an environment where multiple systems are interconnected to comprise a "system of systems". The document "Observations about the Impact Assessment of an Internet of Things (IoT) Incident" (Cloud Security Alliance, 2016) is an advanced attempt to examine issues relating to the impact assessment. It attempts to assess an impact according to the characteristics of the device or the service and to the number of devices.	O/S	-	-	○ (In addition to the following, A.16.1.6)	-	-
			<Advanced> - The organization works with IPA, JPCERT/CC, the industry's ISAC, and a security vendor to collect information, thereby interlinking and sharing information about threats and vulnerability to obtain a whole picture of the security incident. - The organization requests an external security vendor to analyze the functions of the malware, or program, or script placed by an attacker if any is found in a security incident that has occurred.	O	○ (3.6.1)	○ (IR-4, IR-4(8))	○ (A.6.1.4)	○ (4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8)	-
			<Basic> - N/A	-	-	-	-	-	-

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measures	Reference Guidelines				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 Annex A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.AN-2	Implement digital forensics upon the occurrence of the security incident.	L1_3_a_PRO	<High-Advanced> - The information system provides a procedure for processing an audit record regarding critical security incidents.	S	○ (3.3.6)	○ (AU-7, AU-7(1))	○ (A.16.1.7)	-	○ (In addition to the following, SR 2.10)
			<Advanced> - The organization establishes procedures for identifying, collecting, acquiring, and saving proof according to the medium, device, and the state of the device (e.g., whether it is switched on or off). - It is desirable that the organization should retain the following evidence after the occurrence of any serious security incident: - Identification data (e.g., the location of the incident, date and time of the occurrence, serial numbers on the items, host name, MAC address, IP address); - The titles and names of the people who have collected and processed the evidence; their contact information; - Date and time the evidence was saved.	O				-	○ (SR 2.8, SR 2.9, SR 2.11, SR 2.12, SR 3.9, SR 6.1)
			<Basic> - The organization establishes and manages procedures for identifying, collecting, acquiring, and saving data that may serve as proof.	O				-	-
CPS.AN-3	Categorize and store information regarding the detected security incidents by the size of security-related impact, penetration vector, and other factors.	L1_3_a_PRO	<High-Advanced> - The organization uses an automated mechanism designed to help track security incidents and collect and analyze information about threats and vulnerability related to incidents, so that it applies the findings to classification (triage) of security incidents.	O	-	○ (In addition to the following, CP-2(8), IR-5(1))	○ (A.16.1.3, A.16.1.4)	-	-
			<Advanced> - The organization classifies security incidents, taking into account the recovery time objectives for the systems, the order of priority in recovery, and metrics in the process of its security operation. - The organization tracks and documents security incidents that may affect it. "SP 800-61 rev.1" lists the following as examples of points of view that may be taken when an organization documents a security incident. - The present state of the incident - Overview of the incident - The course of action the organization has taken to deal with the incident - Other contact information of relevant personnel (e.g., the system owner, system administrator) - List of proof collected during the investigation - Comments by the staff in charge of dealing with the incident - Next steps	O	○ (3.6.1)	○ (In addition to the following, CP-2, IR-5)		○ (4.3.4.5.6)	-
			<Basic> - The organization should identify in advance the core businesses that should be continued and restored in priority, and the operations considered to be important. In addition, identify and prioritize important resources (relevant parties, People, Components, Data, System, etc.) and functions from the viewpoint of business continuity. * Similar measures are described in CPS.AM-6 and CPS.BE-2. - The organization specifies incidents that must be reported, considering the level of the impact the security event has. [Reference] For example, the following document is available for reference when an organization decides on a measure of the severity of the impact of a security incident. - "SP 800-61 rev.1" (NIST, 2008) Prioritization of the 3.2.6 Incident	O	-	○ (IR-8)			-
CPS.MI-1	Take measures to minimize security-related damages and mitigate the impacts caused by such incident.	L1_3_a_PRO	<High-Advanced> - The organization uses an automated mechanism for assisting with the process of security incident handling. - The organization interlinks information regarding threats and vulnerabilities with how individual security incidents have been handled so as to improve its understanding of the situations. [Reference] As examples of information expected to be useful in reducing the impact of an incident being handled and in recovery from the incident, "Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT Version 1.0" (ISOG-J, 2018) lists the following: - Configuration requirements for security products and related systems to block any attacks; - How to disable attacks (e.g., patching; changing setups); - How to recover a damaged system;	O/S	-	○ (In addition to the following, IR-4(1), IR-4(4))	○ (A.16.1.5)	-	-
			Common among <Advanced> and <Basic> - The organization (or its members) takes courses of action to reduce security incidents (e.g., shutting down the system; cutting off the system from a wired/wireless network; cutting off a modem cable; disabling certain functions) in accordance with prescribed procedures. [Reference] Courses of action to reduce the impact of a security incident may vary according to the nature of the incident (e.g., according to the threat that has emerged, such as a denial-of-service attack, malware infection, or unauthorized access). For example, It is advisable to refer to "SP 800-61 rev.1" (NIST, 2008) for detailed information about courses of action to reduce the impact of an incident.	O	○ (3.6.1)	○ (IR-4)		○ (4.3.4.5.6, 4.3.4.5.10)	○ (SR 5.1, SR 5.2, SR 5.4)
CPS.IM-1	Review the lessons learned from the responses to security incidents, and continuously improve the security operation process.	L1_3_a_ORG	<High-Advanced> - It is desirable for the information system to adopt an automatic mechanism for quantifying and monitoring the form, scale, and cost of a security incident that has occurred.	S	-	-	○ (A.16.1.6)	–	–
			Common among <Advanced> and <Basic> - It is advisable to use information about threats and vulnerability acquired from security incident assessment for the purpose of identifying incidents that may recur or have a major impact. - Incorporate the lessons learned from the experience of handling of security incidents into the business continuity plan or emergency response plan and the education or training, thereby making necessary changes. NIST SP 800-61 shows the following as examples of points of view that may be taken when selecting the lessons. - Exactly when and what happened; - How well the staff and management handled the incident; - Whether they followed documented procedures; - Whether that was appropriate; - What information was immediately needed; - Whether any steps or actions might have hindered recovery; - What different actions the staff and management would take if the same incident recurred; - What corrective measures would prevent the occurrence of similar incidents in the future; - What additional tools and resources would be needed to detect, analyze, and reduce incidents in the future.	O	○ (3.6.2)	○ (IR-4)		○ (4.3.4.5.10)	–
CPS.IM-2	Review the lessons learned from the responses to security incidents, and continuously improve the business continuity plan or emergency response plan.	L1_3_a_ORG	Common among <High-Advanced>, <Advanced> and <Basic> - The organization makes sure that the procedures for business continuity and the functions of relevant measures go along with the business continuity policy for higher positions. - The organization incorporates the lessons learned from the experience of handling of security incidents into the business continuity plan or emergency response plan and the education or training, thereby making necessary changes.	O	○ (3.6.2)	○ (IR-4)	○ (A.17.1.3)	-	-

Appendix D: Relationship with major overseas standards

D.1 Mapping NIST Cybersecurity Framework v1.1 subcategories to Cyber/Physical Security Framework

NIST Cyberseucurity Framework Ver 1.1			Cyber/Physical Security Framework	
Function	Subcategory-ID	Subcategory	Measure Requirement ID	Measure Requirement
Identify (ID)	AM-1	Physical devices and systems within the organization are inventoried	CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.
	AM-2	Software platforms and applications within the organization are inventoried		
	AM-3	Organizational communication and data flows are mapped	CPS.AM-4	Create and manage appropriately network configuration diagrams and data flows within the organization.
	AM-4	External information systems are catalogued	CPS.AM-5	Create and manage appropriately a list of external information systems where the organization's assets are shared.
	AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	CPS.AM-6	Classify and prioritize resources (e.g., People, Components, Data, and System) by function, importance, and business value, and communicate to the organizations and people relevant to those resources in business.
	AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	CPS.AM-7	Define roles and responsibilities for cyber security across the organization and other relevant parties.
	BE-1	The organization's role in the supply chain is identified and communicated	CPS.BE-1	Identify and share the role of the organizations in the supply chain.
	BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated		
	BE-3	Priorities for organizational mission, objectives, and activities are established and communicated	CPS.BE-2	Define policies and standard measures regarding security that are consistent with the high-priority business and operations of the organization, and share them with parties relevant to the organization's business (including suppliers and third-party providers).
	BE-4	Dependencies and critical functions for delivery of critical services are established	CPS.BE-3	Identify the dependency between the organization and other relevant parties and the important functions of each in the course of running the operation.
	BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	CPS.AT-1	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.
			CPS.AT-2	Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.
			CPS.IP-5	Implement physical measures such as preparing an uninterruptible power supply, a fire protection facility, and protection from water infiltration to follow the policies and rules related to the physical operating environment, including the IoT devices and servers installed in the organization.
			CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.
			CPS.RP-2	As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.
			CPS.RP-3	Include security incidents in the business continuity plan or emergency response plan that outlines the action plans and response procedures to take in case of natural disasters.
	GV-1	Organizational cybersecurity policy is established and communicated	CPS.GV-1	Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.
	GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners		
	GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	CPS.GV-2	Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.
	GV-4	Governance and risk management processes address cybersecurity risks	CPS.GV-4	Develop a strategy and secure resources to implement risk management regarding security.
	RA-1	Asset vulnerabilities are identified and documented	CPS.RA-1	Identify the vulnerability of the organization's assets and document the list of identified vulnerability with the corresponding asset.
	RA-2	Cyber threat intelligence is received from information sharing forums and sources	CPS.RA-2	The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.), analyzes the information, and establishes a process to implement and use measures.

Appendix D.1 - Mapping NIST CSF to CPSF

NIST Cyberseucurity Framework Ver 1.1			Cyber/Physical Security Framework	
Function	Subcategory-ID	Subcategory	Measure Requirement ID	Measure Requirement
	RA-3	Threats, both internal and external, are identified and documented	CPS.RA-3	Identify and document the assumed security incidents, those impacts on the oraganization's assets, and the causes of those.
	RA-4	Potential business impacts and likelihoods are identified	CPS.RA-4	- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation. - Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.
	RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	CPS.RA-5	Consider threats, vulnerability, likelihood, and impacts when assessing risks.
	RA-6	Risk responses are identified and prioritized	CPS.RA-6	- On the basis of the results of the risk assessment, clearly define the details of measures to prevent possible security risks, and document the organized outcome from the scope and priorities of the measures. - React accordingly to the security risks and the associated safety risks identified as a result of the assessment conducted at the planning and design phase of an IoT device and systems incorporating IoT devices.
	RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	CPS.RM-1	Confirm the implementation status of the organization's' cyber security risk management and communicate the results to appropriate parties within the organization (e.g. senior management). Define the scope of responsibilities of the organization and the relevant parties (e.g. subcontractor), and establish and implement the process to confirm the implementation status of security risk management of relevant parties.
	RM-2	Organizational risk tolerance is determined and clearly expressed	CPS.RM-2	Determine the organization's risk tolerance level based on the result of the risk assessment and its role in the supply chain.
	RM-3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis		
	SC-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	CPS.SC-1	Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.
	SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	CPS.SC-2	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.
	SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	CPS.SC-3	When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.
	SC-4	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	CPS.SC-6	Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.
	SC-5	Response and recovery planning and testing are conducted with suppliers and third-party providers	CPS.SC-9	Prepare and test a procedure for incident response with relevant parties involved in the incident response activitiy to ensure action for incident response in the supply chain.
Protect (PR)	AC-1	Identities and credentials are issued, managed , verified, revoked, and audited for authorized devices and, users and processes	CPS.AC-1	Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.
	AC-2	Physical access to assets is managed and protected	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.
	AC-3	Remote access is managed	CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).
			CPS.AC-4	Prevent unauthorized log-in to IoT devices and servers by measures such as implementing functions for lockout after a specified number of incorrect log-in attempts and providing a time interval until safety is ensured.
	AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	CPS.AC-5	Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions)
			CPS.AC-6	Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.
	AC-5	Network integrity is protected, (e.g., network segregation , network segmentation)	CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).
	AC-6	Identities are proofed and bound to credentials and asserted in interactions	CPS.AC-8	Restrict communications by IoT devices and servers to those with entities (e.g. people, components, system, etc.) identified through proper procedures.

Appendix D.1 - Mapping NIST CSF to CPSF

NIST Cyberseucurity Framework Ver 1.1			Cyber/Physical Security Framework	
Function	Subcategory-ID	Subcategory	Measure Requirement ID	Measure Requirement
	AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	CPS.AC-6	Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.
			CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).
	AT-1	All users are informed and trained	CPS.AT-1	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.
	AT-2	Privileged users understand their roles and responsibilities		
	AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	CPS.AT-2	Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.
	AT-4	Senior executives understand their roles and responsibilities	CPS.AT-1	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.
	AT-5	Physical and cybersecurity personnel understand their roles and responsibilities		
	DS-1	Data-at-rest is protected	CPS.DS-2	Encrypt information with an appropriate level of security strength, and store them.
	DS-2	Data-in-transit is protected	CPS.DS-3	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.
			CPS.DS-4	Encrypt information itself when sending/receiving information.
	DS-3	Assets are formally managed throughout removal, transfers, and disposition	CPS.IP-6	When disposing of an IoT device and server, delete the stored data and the ID (identifier) uniquely identifying the genuine IoT devices and servers as well as important information (e.g., private key and digital certificate), or make them unreadable.
	DS-4	Adequate capacity to ensure availability is maintained	CPS.DS-6	Secure sufficient resources (e.g., People, Components, system) for components and systems, and protect assets property to minimize bad effects under cyber attack (e.g., DoS attack).
			CPS.DS-7	Carry out periodic quality checks, prepare standby devices and uninterruptible power supplies, provide redundancy, detect failures, conduct replacement work, and update software for IoT devices, communication devices, circuits, etc.
	DS-5	Protections against data leaks are implemented	CPS.DS-8	When handling information to be protected or procuring devices that have an important function to the organization, useselect the IoT devices and servers equipped with anti-tampering devices.
			CPS.DS-9	Properly control outbound communications that send information to be protected to prevent improper data breach.
	DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	CPS.DS-10	Conduct integrity checks of software runnning on the IoT devices and servers at a time determined by the organization, and prevent unauthorized software from launching.
			CPS.DS-11	Perform integrity checking on information to be sent, received, and stored.
	DS-7	The development and testing environment(s) are separate from the production environment	CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).
	DS-8	Integrity checking mechanisms are used to verify hardware integrity	CPS.DS-12	Introduce an integrity check mechanism to verify the integrity of hardware.
	IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	CPS.IP-1	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.
			CPS.IP-2	Restrict the software to be added after installing in the IoT devices and servers.
	IP-2	A System Development Life Cycle to manage systems is implemented	CPS.IP-3	Introduce the system development life cycle to manage the systems.
	IP-3	Configuration change control processes are in place	CPS.IP-1	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.
	IP-4	Backups of information are conducted, maintained, and tested	CPS.IP-4	Perform a periodical system backup and testing of components (e.g., IoT devices, communication devices, and circuits).
	IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met	CPS.IP-5	Implement physical measures such as preparing an uninterruptible power supply, a fire protection facility, and protection from water infiltration to follow the policies and rules related to the physical operating environment, including the IoT devices and servers installed in the organization.

Appendix D.1 - Mapping NIST CSF to CPSF

NIST Cyberseucurity Framework Ver 1.1			Cyber/Physical Security Framework	
Function	Subcategory-ID	Subcategory	Measure Requirement ID	Measure Requirement
	IP-6	Data is destroyed according to policy	CPS.IP-6	When disposing of an IoT device and server, delete the stored data and the ID (identifier) uniquely identifying the genuine IoT devices and servers as well as important information (e.g., private key and digital certificate), or make them unreadable.
	IP-7	Protection processes are improved	CPS.IP-7	Assess the lessons learned from security incident response and the results of monitoring, measuring, and evaluating internal and external attacks, and improve the processes of protecting the assets.
	IP-8	Effectiveness of protection technologies is shared	CPS.IP-8	Share information regarding the effectiveness of data protection technologies with appropriate partners.
	IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.
			CPS.RP-2	As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.
	IP-10	Response and recovery plans are tested	CPS.AT-2	Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.
	IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	CPS.IP-9	Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.
	IP-12	A vulnerability management plan is developed and implemented	CPS.IP-10	Develop a vulnerability remediation plan, and modify the vulnerability of the components according to the plan.
	MA-1	Maintenance and repair of organizational assets isare performed and logged with approved and controlled tools	CPS.MA-1	- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updateswith managed tools properly and in a timely manner while recording the history. - Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable.
	MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	CPS.MA-2	Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.
	PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.
	PT-2	Removable media is protected and its use restricted according to policy	CPS.PT-2	Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.
	PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities		
	PT-4	Communications and control networks are protected	CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).
	PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	CPS.PT-3	Introduce IoT devices that implement safety functions, assuming that these devices are connected to the network.
Detect (DE)	AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	CPS.AE-1	Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.
	AE-2	Detected events are analyzed to understand attack targets and methods	CPS.AE-2	Appoint a chief security officer, establish a security management team (SOC/CSIRT), and prepare a system within the organization to detect, analyze, and respond to security events.
	AE-3	Event data are collected and correlated from multiple sources and sensors	CPS.AE-3	Identify the security events accurately by implementing the procedure to conduct a correlation analysis of the security events and comparative analysis with the threat information obtained from outside the organization.
	AE-4	Impact of events is determined	CPS.AE-4	Identify the impact of security events, including the impact on other relevant organizations.
	AE-5	Incident alert thresholds are established	CPS.AE-5	Specify the criteria to determine the risk degree of security events.
	CM-1	The network is monitored to detect potential cybersecurity events	CPS.CM-1	Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.
	CM-2	The physical environment is monitored to detect potential cybersecurity events	CPS.CM-2	Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.

Appendix D.1 - Mapping NIST CSF to CPSF

NIST Cyberseucurity Framework Ver 1.1			Cyber/Physical Security Framework	
Function	Subcategory-ID	Subcategory	Measure Requirement ID	Measure Requirement
	CM-3	Personnel activity is monitored to detect potential cybersecurity events	CPS.CM-6	As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other “organization”, people, components, and systems.
	CM-4	Malicious code is detected	CPS.CM-3	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.
			CPS.CM-4	Validate the integrity and authenticity of the information provided from cyberspace before operations.
	CM-5	Unauthorized mobile code is detected	CPS.CM-3	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.
			CPS.CM-4	Validate the integrity and authenticity of the information provided from cyberspace before operations.
	CM-6	External service provider activity is monitored to detect potential cybersecurity events	CPS.CM-5	Monitor communication with external service providers so that potential security events can be detected properly.
	CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	CPS.CM-6	As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other “organization”, people, components, and systems.
	CM-8	Vulnerability scans are performed	CPS.CM-7	Confirm the existence of vulnerability that requires a regular check-up in IoT devices and servers managed within the organization.
	DP-1	Roles and responsibilities for detection are well defined to ensure accountability	CPS.DP-1	Clarify the role and responsibility of the organization as well as service providers in detecting security events so that they can fulfill their accountabilities.
	DP-2	Detection activities comply with all applicable requirements	CPS.DP-2	Detect security events in the monitoring process, in compliance with applicable local regulations, directives, industry standards, and other rules.
	DP-3	Detection processes are tested	CPS.DP-3	As part of the monitoring process, test regularly if the functions for detecting security events work as intended, and validate these functions.
	DP-4	Event detection information is communicated	CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.
	DP-5	Detection processes are continuously improved	CPS.DP-4	Continuously improve the process of detecting security events.
Respond (RS)	RP-1	Response plan is executed during or after an incident	CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.
	CO-1	Personnel know their roles and order of operations when a response is needed	CPS.AT-2	Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.
	CO-2	Incidents are reported consistent with established criteria	CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.
	CO-3	Information is shared consistent with response plans		
	CO-4	Coordination with stakeholders occurs consistent with response plans	CPS.RP-2	As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.
	CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness		
	AN-1	Notifications from detection systems are investigated	CPS.AE-3	Identify the security events accurately by implementing the procedure to conduct a correlation analysis of the security events and comparative analysis with the threat information obtained from outside the organization.
	AN-2	The impact of the incident is understood	CPS.AN-1	Understand the impact of the security incident on the whole society including the organization and relevant parties such as partners based on the full account of the incident and the probable intent of the attacker.
	AN-3	Forensics are performed	CPS.AN-2	Implement digital forensics upon the occurrence of the security incident.

Appendix D.1 - Mapping NIST CSF to CPSF

NIST Cyberseucurity Framework Ver 1.1			Cyber/Physical Security Framework	
Function	Subcategory-ID	Subcategory	Measure Requirement ID	Measure Requirement
	AN-4	Incidents are categorized consistent with response plans	CPS.AN-3	Categorize and store information regarding the detected security incidents by the size of security-related impact, penetration vector, and other factors.
	AN-5	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	CPS.RA-2	The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.), analyzes the information, and establishes a process to implement and use measures.
	IM-1	Response plans incorporate lessons learned	CPS.IM-1	Review the lessons learned from the responses to security incidents, and continuously improve the security operation process.
	IM-2	Response strategies are updated		
	MI-1	Incidents are contained	CPS.MI-1	Take measures to minimize security-related damages and mitigate the impacts caused by such incident.
	MI-2	Incidents are mitigated		
	MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks	CPS.RA-4	- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation. - Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.
			CPS.RA-6	- On the basis of the results of the risk assessment, clearly define the details of measures to prevent possible security risks, and document the organized outcome from the scope and priorities of the measures. - React accordingly to the security risks and the associated safety risks identified as a result of the assessment conducted at the planning and design phase of an IoT device and systems incorporating IoT devices.
Recovery (RC)	RP-1	Recovery plan is executed during or after a cybersecurity incident	CPS.RP-3	Include security incidents in the business continuity plan or emergency response plan that outlines the action plans and response procedures to take in case of natural disasters.
	IM-1	Recovery plans incorporate lessons learned	CPS.IM-2	Review the lessons learned from the responses to security incidents, and continuously improve the business continuity plan or emergency response plan.
	IM-2	Recovery strategies are updated		
	CO-1	Public relations are managed	CPS.CO-1	Develop and manage rules regarding publishing information after the occurrence of the security incident.
	CO-2	Reputation is repaired after an incident	CPS.CO-2	Include the item in the business continuity plan or emergency response plan to the effect that the organization shall work to restore its social reputation after the occurrence of a high-risk security incident.
	CO-3	Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	CPS.CO-3	Include the item in the business continuity plan or emergency response plan to the effect that the details of the recovery activities shall be communicated to the internal and external stakeholders, executives, and management.

D.2 Mapping NIST SP 800-171 controls to Cyber/Physical Security Framework

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
ACCESS CONTROL	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).	・AC-2 Account Management ・AC-3 Access Enforcement ・AC-17 Remote Access	CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.
	3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	・AC-2 Account Management ・AC-3 Access Enforcement ・AC-17 Remote Access	CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.
	3.1.3	Control the flow of CUI in accordance with approved authorizations.	・AC-4 Information Flow Enforcement	CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).	H-Advanced	- The information system and the industrial control system monitor and control communications on the networks composing internal business systems of the organization. - Regarding the network which the system that handles highly confidential data is connected to, the organization shall deny network communications as a default and shall only allow connection of approved communication traffic. - The organization physically or logically separates the network of high importance industrial control systems from the network of control systems with lower importance. - If the information system that handles highly confidential data is connected to a remote device, the organization is to prevent multiple and simultaneous local connections between the device and the system, as well as prevent access to external network resources by other connections.
						Basic	- The organization establishes a data flow regulation policy that defines the range in which data flow within information systems and industrial control system is permitted and the range in which data flow between systems is permitted, and regulates the flow by segregating the network appropriately. - The organization logically or physically segments the control system's network from the network composing of the information system. [Reference] Implement physical segmentation in environments physically separated from other networks. Alternatively, in environments physically close to other networks, it is possible to implement logical segmentation in consideration of the cost of the measure.
				CPS.AE-1	Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.	H-Advanced	- The organization uses a mechanism for automatically collecting information about network configurations and the software configurations of devices in order to monitor the most recent status at all times. - The information system forces the application of users' access rights approved (by the administrator) in order to control data flows within a system (and between interconnected systems). - The organization physically or logically separates a network of industrial control systems with high importance from a network of industrial control systems with lower importance. - The organization/system analyzes the regular patterns of its systems' communication status and security alerts to create and use a profile that summarizes typical patterns of communication and security alerts, thereby enabling the detection of unknown threats and suspicious behavior (communication).
	3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	・AC-5 Separation of Duties	CPS.AC-5	Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions)	H-Advanced	- The organization specifies administrators who use the security functions (e.g., access authority setting) and regulates privileged accounts in its system. - The information system adopts a system monitoring mechanism to check the use of privileged functions. - The information system prohibits non-privileged users from executing privileged functions on the system by invalidating, avoiding, and changing security measures that are changed and implemented by non-privileged users. - The organization can minimize the number of users who can use the system administrator's authority in an emergency to minimize the damage caused by the security incident. - The organization can prevent even system administrators from stopping critical services and protected processes through the server to minimize the damage caused by security incidents.
						Advanced	- The organization implements access control in the information system and the industrial control system based on separation of duties (e.g., user / system administrator). - The organization adopts a general rule on the minimum authority of specific duties. - Segregate authority of general user from that of administrator. (Require users to use the system with a non-privileged account when using a non-security function.) - Minimize authority for duties not in charge. - The organization separates and stipulates duties that are assigned by the person in charge.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts	・AC-6 Least Privilege ・AC-6(1) Least Privilege Authorize Access to Security Functions ・AC-6(5) Least Privilege Privileged Accounts	CPS.AC-5	Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions)	H-Advanced	- The organization specifies administrators who use the security functions (e.g., access authority setting) and regulates privileged accounts in its system. - The information system adopts a system monitoring mechanism to check the use of privileged functions. - The information system prohibits non-privileged users from executing privileged functions on the system by invalidating, avoiding, and changing security measures that are changed and implemented by non-privileged users. - The organization can minimize the number of users who can use the system administrator's authority in an emergency to minimize the damage caused by the security incident. - The organization can prevent even system administrators from stopping critical services and protected processes through the server to minimize the damage caused by security incidents.
						Advanced	- The organization implements access control in the information system and the industrial control system based on separation of duties (e.g., user / system administrator). - The organization adopts a general rule on the minimum authority of specific duties. - Segregate authority of general user from that of administrator. (Require users to use the system with a non-privileged account when using a non-security function.) - Minimize authority for duties not in charge. - The organization separates and stipulates duties that are assigned by the person in charge.
	3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	・AC-6(2) Least Privilege Non-Privileged Access for Nonsecurity Functions	CPS.AC-5	Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions)	H-Advanced	- The organization specifies administrators who use the security functions (e.g., access authority setting) and regulates privileged accounts in its system. - The information system adopts a system monitoring mechanism to check the use of privileged functions. - The information system prohibits non-privileged users from executing privileged functions on the system by invalidating, avoiding, and changing security measures that are changed and implemented by non-privileged users. - The organization can minimize the number of users who can use the system administrator's authority in an emergency to minimize the damage caused by the security incident. - The organization can prevent even system administrators from stopping critical services and protected processes through the server to minimize the damage caused by security incidents.
	3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	・AC-6(9) Least Privilege Auditing Use of Privileged Functions ・AC-6(10) Least Privilege Prohibit Non-Privileged Users from Executing Privileged Functions				
	3.1.8	Limit unsuccessful logon attempts.	・AC-7 Unsuccessful Logon Attempts	CPS.AC-4	Prevent unauthorized log-in to IoT devices and servers by measures such as implementing functions for lockout after a specified number of incorrect log-in attempts and providing a time interval until safety is ensured.	H-Advanced	- The information system and the industrial control system (excluding some cases where immediacy of response is required) sets a limit to the number of continuous login attempts on its system. If the user fails to log in, he or she will only be able to re-login after the administrator removes the restriction.
						Advanced	- The information system and the industrial control system set a limit on the number of continuous login attempts on its system. If the user fails to log in, he or she will not be able to re-login for a certain period of time. - The information system and industrial control system lock the session manually or automatically if the system's non-operation continues beyond the time set by the organization. * In the industrial control system, it may be desirable not to lock session when it is assumed that a session in which an operator is required to respond immediately in an emergency may be conducted.
	3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	・AC-8 System Use Notification	CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.
	3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.	・AC-11 Session Lock ・AC-11(1) Session Lock Pattern-Hiding Displays	CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.
	3.1.11	Terminate (automatically) a user session after a defined condition.	・AC-12 Session Termination	CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.1.12	Monitor and control remote access sessions.	・AC-17(1) Remote Access Automated Monitoring / Control	CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).	H-Advanced	- The information system and the industrial control system automatically monitor or regulate remote access to its system. - The information system and the industrial control system allow only for remote access routed by the regulated access points. - The information system allows privileged command via remote access only for those purposes based on specified requirements. - The information system records reasons why the users accessing the system which handles highly confidential data execute privileged commands and access security information by remote access. - The information system protects wireless access to the system which handles highly confidential data by using user and device authentication in addition to encryption. - The information system blocks remote activation of devices such as white boards, cameras, and microphones connected via networks which may handle highly confidential data. Signs of the devices in use are provided to the users of these devices.
				CPS.CM-1	Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.	Advanced	- The organization monitors and controls communications at the boundary between industrial control system and information system. - The organization creates a network segment isolated from access to the internal network ("demilitarized zone [DMZ]") between the internal network and external networks (e.g., the Internet). - The information system is connected to an external network or system only via a controlled interface that consists of a boundary protection system placed according to the organization's security architecture. - The information system ensures that each external communications service is provided via a controlled interface (e.g., a gateway, router, and firewall). - The organization establishes a communications control policy for each controlled interface (e.g., a gateway, router, and firewall). - The system on a controlled interface rejects network communication by default and permits it as an exception. - The organization monitors communications at the external boundaries of the information system and at major internal boundaries within the information system for large amounts of communication from a particular source or multiple sources, and takes appropriate action when necessary (e.g., blocking of communication from a specific IP address).
						Basic	- The organization monitors and controls communications on the information system's external boundary as well as on the key internal boundary within the information system.
				CPS.CM-5	Monitor communication with external service providers so that potential security events can be detected properly.	H-Advanced	- The organization requires its provider of external information system services to make clear the functions, ports, and protocols needed for the use of the services, along with other services. - The organization monitors whether the matters made clear as stated above are observed.
						Advanced	- The organization documents its security requirements for the staff from its external service provider and system developer, and includes the requirements in the agreement. - The organization requires its external service provider and system developer to contact it when any of its staff members who have authorizations for its system are transferred or when their employment terminates. - It is desirable that the organization should manage changes to services offered by its external service provider, taking account of relevant information about operations, the importance of its business systems and processes, and re-assessed risks. - The organization monitors whether its external service provider and system developer complies with the requirements. - The organization monitors access to its system by its external service provider and system developer in order to detect any unauthorized access by these external businesses that results from an action or failure to act. - The organization reports the results of the monitoring of activities by its external service provider and system developer to the appropriate system administrator.
	3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	・AC-17(2) Remote Access Protection of Confidentiality / Integrity Using Encryption	CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).	H-Advanced	- The information system and the industrial control system automatically monitor or regulate remote access to its system. - The information system and the industrial control system allow only for remote access routed by the regulated access points. - The information system allows privileged command via remote access only for those purposes based on specified requirements. - The information system records reasons why the users accessing the system which handles highly confidential data execute privileged commands and access security information by remote access. - The information system protects wireless access to the system which handles highly confidential data by using user and device authentication in addition to encryption. - The information system blocks remote activation of devices such as white boards, cameras, and microphones connected via networks which may handle highly confidential data. Signs of the devices in use are provided to the users of these devices.
				CPS.DS-3	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.	Advanced	- The information system employs an cryptographic mechanism and encrypt communciation paths. [Reference] For encryption of communication paths, there are several methods such as IP-VPN, Ipsec-VPN, SSL VPN. It is desirable that the organization should select the method considering the importance of the data transmitted in the communication paths, the budget, and so on.
	3.1.14	Route remote access via managed access control points.	・AC-17(3) Remote Access Managed Access Control Points	CPS.CM-1	Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.	H-Advanced	- The information system routes communications to the network to which a recipient's IP address belongs via a proxy server authenticated on a controlled interface. - The information system and the industrial control system monitor and control the use of mobile code. - The information system monitors and controls the use of protocols used for audio and video transmission (e.g. VoIP).
						Advanced	- The organization monitors and controls communications at the boundary between industrial control system and information system. - The organization creates a network segment isolated from access to the internal network ("demilitarized zone [DMZ]") between the internal network and external networks (e.g., the Internet). - The information system is connected to an external network or system only via a controlled interface that consists of a boundary protection system placed according to the organization's security architecture. - The information system ensures that each external communications service is provided via a controlled interface (e.g., a gateway, router, and firewall). - The organization establishes a communications control policy for each controlled interface (e.g., a gateway, router, and firewall). - The system on a controlled interface rejects network communication by default and permits it as an exception. - The organization monitors communications at the external boundaries of the information system and at major internal boundaries within the information system for large amounts of communication from a particular source or multiple sources, and takes appropriate action when necessary (e.g., blocking of communication from a specific IP address).
	3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	・AC-17(4) Remote Access Privileged Commands / Access	CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).	H-Advanced	- The information system and the industrial control system automatically monitor or regulate remote access to its system. - The information system and the industrial control system allow only for remote access routed by the regulated access points. - The information system allows privileged command via remote access only for those purposes based on specified requirements. - The information system records reasons why the users accessing the system which handles highly confidential data execute privileged commands and access security information by remote access. - The information system protects wireless access to the system which handles highly confidential data by using user and device authentication in addition to encryption. - The information system blocks remote activation of devices such as white boards, cameras, and microphones connected via networks which may handle highly confidential data. Signs of the devices in use are provided to the users of these devices.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.1.16	Authorize wireless access prior to allowing such connections.	･AC-18 Wireless Access	CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).	H-Advanced	- The information system and the industrial control system automatically monitor or regulate remote access to its system. - The information system and the industrial control system allow only for remote access routed by the regulated access points. - The information system allows privileged command via remote access only for those purposes based on specified requirements. - The information system records reasons why the users accessing the system which handles highly confidential data execute privileged commands and access security information by remote access. - The information system protects wireless access to the system which handles highly confidential data by using user and device authentication in addition to encryption. - The information system blocks remote activation of devices such as white boards, cameras, and microphones connected via networks which may handle highly confidential data. Signs of the devices in use are provided to the users of these devices.
						Advanced	- The organization regulates the mobile devices used in the organization and establishes setting requirements, connection requirements, and implementation guidelines for mobile devices. - The organization establishes rules of approval for connecting mobile devices used in the organization to its system.
						Basic	- The organization establishes usage regulations, configuration requirements, and implementation guidelines for each type of approved remote access. - The organization in principle prohibits unauthorized wireless connections. - The organization establishes rules of approval for remote access to an information system and an industrial control system. - The organization authorizes wireless access to its system in advance of the approval.
	3.1.17	Protect wireless access using authentication and encryption.	･AC-18(1) Wireless Access Authentication and Encryption	CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).	H-Advanced	- The information system and the industrial control system automatically monitor or regulate remote access to its system. - The information system and the industrial control system allow only for remote access routed by the regulated access points. - The information system allows privileged command via remote access only for those purposes based on specified requirements. - The information system records reasons why the users accessing the system which handles highly confidential data execute privileged commands and access security information by remote access. - The information system protects wireless access to the system which handles highly confidential data by using user and device authentication in addition to encryption. - The information system blocks remote activation of devices such as white boards, cameras, and microphones connected via networks which may handle highly confidential data. Signs of the devices in use are provided to the users of these devices.
	3.1.18	Control connection of mobile devices.	･AC-19 Access Control for Mobile Devices	CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).	H-Advanced	- The information system and the industrial control system automatically monitor or regulate remote access to its system. - The information system and the industrial control system allow only for remote access routed by the regulated access points. - The information system allows privileged command via remote access only for those purposes based on specified requirements. - The information system records reasons why the users accessing the system which handles highly confidential data execute privileged commands and access security information by remote access. - The information system protects wireless access to the system which handles highly confidential data by using user and device authentication in addition to encryption. - The information system blocks remote activation of devices such as white boards, cameras, and microphones connected via networks which may handle highly confidential data. Signs of the devices in use are provided to the users of these devices.
						Advanced	- The organization regulates the mobile devices used in the organization and establishes setting requirements, connection requirements, and implementation guidelines for mobile devices. - The organization establishes rules of approval for connecting mobile devices used in the organization to its system.
				CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.
	3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	･AC-19(5) Access Control for Mobile Devices Full Device / Container-Based Encryption	CPS.DS-2	Encrypt information with an appropriate level of security strength, and store them.	H-Advanced	- The organization selects products that have been authenticated based on Cryptographic Module Validation Program (CMVP) in order to suitably implement selected algorithms to software and hardware, and to protect keys, identification codes, and entity authentication information that is used to decrypt encrypted information or to grant electronic signatures. - The organization protects are encrypts data to the appropriate strength when that data is taken outside of the organization. - The organization uses IoT devices that can encrypt and store data in internal memory.
						Advanced	- The organization examines safety and trustworthiness that are necessary, selects an algorithm, encrypts information (data) to the appropriate strength, and stores the information. If an algorithm on the CRYPTREC Ciphers List can be selected, the organization uses it to encrypt information (data) to the appropriate strength and stores the information. - The organization considers the level of security and trustworthiness required for the information, chooses an algorithm, and encrypts and stores high importance information handled by industrial control systems with appropriate strength without causing unacceptable impact on performance. [Reference] Regarding encryption technologies whose security and implementation performance are confirmed, "Cryptography Research and Evaluation Committees （CRYPTREC）" releases to the public the list of such technologies recommended for use that are sufficiently used in the market or are considered to spread in the future. It is desirable that the organization should refer to the list as needed when procuring systems that should implement encryption functions.
	3.1.20	Verify and control/limit connections to and use of external systems.	･AC-20 Use of External Systems ･AC-20(1) Use of External Systems Limits on Authorized Use	CPS.AM-5	Create and manage appropriately a list of external information systems where the organization's assets are shared.	H-Advanced	- The system makes a list of external information services in use and manages the users, devices as well as serviced in use in real time. - The system uses a mechanism to give notice to the system administrator when an unpermitted external information system service is detected. - The organization identifies functions, ports, protocols, and other services which are necessary for using services offered by external providers.
						Advanced	- The organization sets conditions for allowing other organizations which own or operate external information systems to do the following: a. Accessing an information system in the organization from an external information system b. Processing, saving, or transmitting information under the control of the organization using an external information system - The organization restricts a use of storage in an external system the organization owns to an authorized one.
	3.1.21	Limit use of organizational portable storage devices on external systems.	･AC-20(2) Use of External Systems Portable Storage Devices	CPS.AM-5	Create and manage appropriately a list of external information systems where the organization's assets are shared.	Advanced	- The organization sets conditions for allowing other organizations which own or operate external information systems to do the following: a. Accessing an information system in the organization from an external information system b. Processing, saving, or transmitting information under the control of the organization using an external information system - The organization restricts a use of storage in an external system the organization owns to an authorized one.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.1.22	Control CUI posted or processed on publicly accessible systems.	・AC-22 Publicly Accessible Content	CPS.GV-3	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	Basic	- The organization identifies and documents all legal requirements and contract requirements related to data protection for each system and each organization and the organization's activities to satisfy these requirements, and update them to the latest. - The organization classifies its data appropriately according to the classification of the identified rules. - The organization takes measures for systems, components, etc., handling the applicable data in accordance with the requirements of the identified rules. When the implementation of a measure is considered difficult, measures such as tokenization of an applicable data in the organization may be considered. (e.g., tokenization of card information due to the Installment Sales Law)
AWARENESS AND TRAINING	3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	・AT-2 Security Awareness Training ・AT-3 Role-Based Security Training	CPS.AT-1	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	H-Advanced	- The organization provides security awareness trainings to all necessary personnel so that they will recognize and report signs of internal fraud.
						Advanced	- The organization regularly provides basic security awareness training to all members of staff. The organization can, for example, educate the following matters in addition to the contents explaining general matters. -Procedure to response when you receive a suspicious email -Notes on using mobile devices (e.g. Notes on connecting to a public wireless LAN) -Notes on using SNS - The organization creates a program for each role (e.g., system/software developper, purchasing personnel, system administrator, personnel in charge of security measures) to train information security personnel and to improve their skills. The program is conducted regularly on applicable personnel. - The organization regularly reviews records of security education and training.
				CPS.AT-2	Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.	Advanced	- The organization requests the giving of training (e.g. simulation assuming actual incident) and security education appropriate to execution of the roles assigned to the personnel in charge to related organizations that may be involved in the security incident and confirms the training/education implementation status. - The organization regularly reviews the records of education and training for persons in charge of relevant parties that are highly important in its own security management.
						Basic	- The organization requests the giving of training (e.g. simulation assuming actual incident) and security education appropriate to execution of the roles assigned to the personnel in charge to their personnel, and confirms the training/education implementation status. - The organization records and manages the contents and results of security education and training for member in the organization.
	3.2.2	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	・AT-2 Security Awareness Training ・AT-3 Role-Based Security Training	CPS.AT-1	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	Advanced	- The organization regularly provides basic security awareness training to all members of staff. The organization can, for example, educate the following matters in addition to the contents explaining general matters. -Procedure to response when you receive a suspicious email -Notes on using mobile devices (e.g. Notes on connecting to a public wireless LAN) -Notes on using SNS - The organization creates a program for each role (e.g., system/software developper, purchasing personnel, system administrator, personnel in charge of security measures) to train information security personnel and to improve their skills. The program is conducted regularly on applicable personnel. - The organization regularly reviews records of security education and training.
				CPS.AT-2	Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.	Advanced	- The organization requests the giving of training (e.g. simulation assuming actual incident) and security education appropriate to execution of the roles assigned to the personnel in charge to related organizations that may be involved in the security incident and confirms the training/education implementation status. - The organization regularly reviews the records of education and training for persons in charge of relevant parties that are highly important in its own security management.
	3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	・AT-2(2) Security Awareness Training Insider Threat	CPS.AT-1	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	H-Advanced	- The organization provides security awareness trainings to all necessary personnel so that they will recognize and report signs of internal fraud.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
AUDIT AND ACCOUNTABILITY	3.3.1	Create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	・AU-2 Audit Events ・AU-3 Content of Audit Records ・AU-3(1) Content of Audit Records Additional Audit Information ・AU-6 Audit Review, Analysis, and Reporting ・AU-12 Audit Generation	CPS.SC-6	Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	H-Advanced	- The organization adopts an automatic mechanism integrating review, analysis, and report that supports the investigation and addresses procedures for deviation or signs of deviation from contract matters. - The organization uses a mechanism that allows it to list and check whether obligatory matters stipulated in the contract are fulfilled, matters which are concerned with security management of the organization and security functions implemented in the products and services that will be delivered, especially for important clients and reconsigned organizations. - State of compliance with security management measures of the external service provider is regularly checked by external audits and field surveys conducted by the outsourcer. - The important business partners and if possible their re-contractors etc. investigate whether there is any sign of attack related or any fact of information leakage, and regularly report the result to the organization.
						Advanced	- The organization checks whether requirements that are prescribed in the contract with the client can be audited on the system. - The information system provides a function that allows for audit records to be created for events defined above that can be audited on the system. - The organization shall be able to maintain consistency in security audits with other organizations that require information on the audit. - The organization regularly reviews and analyzes audit records that are made manually or automatically by the system, and checks whether there is any deviation or sign of deviation from contract matters. - State of compliance with security management measures of the external service provider is regularly checked by internal audits that are conducted by the client using a checklist.
				CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	H-Advanced	- In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g. OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related audit logs for some of the IoT devices that an organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specs of the IoT devices, such as using a log management system different than the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.
						Advanced	- The information system and the industrial control system uses a cryptographic mechanism in order to ensure the integrity of an audit log and audit tool each. - The organization grants control over an audit log only to users assigned in accordance with the rules about security-related internal responsibility. - The information system issues an alert when an incident of failure takes place in the audit process.
						Basic	- The organization specifies what is to be audited based on its risk management strategy and risk assessment results, and sees if the systems can acquire audit logs that show who did what and when in connection with the subjects of an audit. - The system generates an audit log prescribed from various system components. - The organization reviews and analyze a system's audit log regularly to see if there are any signs of security incidents that may cause damage to the organization, and make a report to the system administrator where necessary. - The organization confirms that the impact of audit activities on the performance of industrial control systems is tolerable.
	3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	・AU-2 Audit Events ・AU-3 Content of Audit Records ・AU-3(1) Content of Audit Records Additional Audit Information ・AU-6 Audit Review, Analysis, and Reporting ・AU-12 Audit Generation	CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	H-Advanced	- In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g. OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related audit logs for some of the IoT devices that an organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specs of the IoT devices, such as using a log management system different than the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.
						Advanced	- The information system and the industrial control system uses a cryptographic mechanism in order to ensure the integrity of an audit log and audit tool each. - The organization grants control over an audit log only to users assigned in accordance with the rules about security-related internal responsibility. - The information system issues an alert when an incident of failure takes place in the audit process.
						Basic	- The organization specifies what is to be audited based on its risk management strategy and risk assessment results, and sees if the systems can acquire audit logs that show who did what and when in connection with the subjects of an audit. - The system generates an audit log prescribed from various system components. - The organization reviews and analyze a system's audit log regularly to see if there are any signs of security incidents that may cause damage to the organization, and make a report to the system administrator where necessary. - The organization confirms that the impact of audit activities on the performance of industrial control systems is tolerable.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.3.3	Review and update audited events.	・AU-2(3) Audit Events Reviews and Updates	CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	H-Advanced	- In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g. OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related audit logs for some of the IoT devices that an organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specs of the IoT devices, such as using a log management system different than the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.
						Advanced	- The information system and the industrial control system uses a cryptographic mechanism in order to ensure the integrity of an audit log and audit tool each. - The organization grants control over an audit log only to users assigned in accordance with the rules about security-related internal responsibility. - The information system issues an alert when an incident of failure takes place in the audit process.
						Basic	- The organization specifies what is to be audited based on its risk management strategy and risk assessment results, and sees if the systems can acquire audit logs that show who did what and when in connection with the subjects of an audit. - The system generates an audit log prescribed from various system components. - The organization reviews and analyze a system's audit log regularly to see if there are any signs of security incidents that may cause damage to the organization, and make a report to the system administrator where necessary. - The organization confirms that the impact of audit activities on the performance of industrial control systems is tolerable.
	3.3.4	Alert in the event of an audit process failure.	・AU-5 Response to Audit Processing Failures	CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	H-Advanced	- In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g. OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related audit logs for some of the IoT devices that an organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specs of the IoT devices, such as using a log management system different than the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.
						Advanced	- The information system and the industrial control system uses a cryptographic mechanism in order to ensure the integrity of an audit log and audit tool each. - The organization grants control over an audit log only to users assigned in accordance with the rules about security-related internal responsibility. - The information system issues an alert when an incident of failure takes place in the audit process.
	3.3.5	Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	・AU-6(3) Audit Review, Analysis, and Reporting Correlate Audit Repositories	CPS.SC-6	Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	H-Advanced	- The organization adopts an automatic mechanism integrating review, analysis, and report that supports the investigation and addresses procedures for deviation or signs of deviation from contract matters. - The organization uses a mechanism that allows it to list and check whether obligatory matters stipulated in the contract are fulfilled, matters which are concerned with security management of the organization and security functions implemented in the products and services that will be delivered, especially for important clients and reconsigned organizations. - State of compliance with security management measures of the external service provider is regularly checked by external audits and field surveys conducted by the outsourcer. - The important business partners and if possible their re-contractors etc. investigate whether there is any sign of attack related or any fact of information leakage, and regularly report the result to the organization.
				CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	H-Advanced	- In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g. OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related audit logs for some of the IoT devices that an organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specs of the IoT devices, such as using a log management system different than the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.
						Basic	- The organization specifies what is to be audited based on its risk management strategy and risk assessment results, and sees if the systems can acquire audit logs that show who did what and when in connection with the subjects of an audit. - The system generates an audit log prescribed from various system components. - The organization reviews and analyze a system's audit log regularly to see if there are any signs of security incidents that may cause damage to the organization, and make a report to the system administrator where necessary. - The organization confirms that the impact of audit activities on the performance of industrial control systems is tolerable.
	3.3.6	Provide audit reduction and report generation to support on-demand analysis and reporting.	・AU-7 Audit Reduction and Report Generation	CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	H-Advanced	- In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g. OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related audit logs for some of the IoT devices that an organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specs of the IoT devices, such as using a log management system different than the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	・AU-8 Time Stamps ・AU-8(1) Time Stamps Synchronization with Authoritative Time Source	CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	H-Advanced	- In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g. OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related audit logs for some of the IoT devices that an organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specs of the IoT devices, such as using a log management system different than the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.
	3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	・AU-9 Protection of Audit Information	CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	H-Advanced	- In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g. OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related audit logs for some of the IoT devices that an organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specs of the IoT devices, such as using a log management system different than the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.
						Advanced	- The information system and the industrial control system uses a cryptographic mechanism in order to ensure the integrity of an audit log and audit tool each. - The organization grants control over an audit log only to users assigned in accordance with the rules about security-related internal responsibility. - The information system issues an alert when an incident of failure takes place in the audit process.
	3.3.9	Limit management of audit functionality to a subset of privileged users.	・AU-9(4) Protection of Audit Information Access by Subset of Privileged Users	CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	H-Advanced	- In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g. OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related audit logs for some of the IoT devices that an organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specs of the IoT devices, such as using a log management system different than the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.
						Advanced	- The information system and the industrial control system uses a cryptographic mechanism in order to ensure the integrity of an audit log and audit tool each. - The organization grants control over an audit log only to users assigned in accordance with the rules about security-related internal responsibility. - The information system issues an alert when an incident of failure takes place in the audit process.
CONFIGURATION MANAGEMENT	3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	・CM-2 Baseline Configuration ・CM-6 Configuration Settings ・CM-8 System Component Inventory ・CM-8(1) System Component Inventory Updates During Installations / Removals	CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	Advanced	- Maintain/manage lists including configuration information of assets (e.g., names, version information, license information, and location) by reviewing and updating them periodically. - The organization makes a list of removable media (e.g., USB memory sticks) that can be used on system components (information system or industrial control system), and manages the use of them. - The organization uses only removable media (e.g. USB memory) permitted in the organization. Also, if there is no identifiable ownwer of portable storage devices, the organization prohibits the use of such devices. - The organization controles access to the media that contain highly confidential data, and properly grasps and manages the usage of the media taken outside of the controlled areas.
						Basic	- The organization identifies assets constituting its information system and industrial control system (hardware, software and information), assigns a responsible person to each asset, and documents a list of them. - It is desirable to list all the assets held, but if the target is huge, consider narrowing down the target assets through integration (grouping) of the analysis target and exclusion from the analysis target. - The organization sets priorities to the identified assets based on the importance of them in its business operation.
				CPS.CM-6	As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	Advanced	- It is desirable that the organization should update the list of information about its assets and configurations when it installs or deletes new assets or when it updates its system. - The information system ensures that each external communications service is provided via a controlled interface (e.g., a gateway, router, and firewall). - The organization establishes a communications control policy for each controlled interface (e.g., a gateway, router, and firewall). - The system on a controlled interface rejects network communication by default and permits it as an exception. - The information system and the industrial control system terminate the network connection after a session ends, or when a session remains inactive for a certain length of time. - The organization monitors communication on controlled interfaces in order to detect any communication to unapproved items or systems, or communication that conveys an inappropriate content.
						Basic	- The organization creates a ledger to manage model numbers of assets that includes servers, software versions, and the expiration of support services. Take regular inventory. - The organization regularly checks whether necessary measures are taken during operation (e.g., checking IoT devices for any unauthorized use or theft; applying a patch; checking logs) and the state of IoT devices.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	・CM-2 Baseline Configuration ・CM-6 Configuration Settings ・CM-8 System Component Inventory ・CM-8(1) System Component Inventory Updates During Installations / Removals	CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	H-Advanced	-The organization identifies assets constituting its information systems and industrial control systems (hardware, including IoT devices; software; and information) uniquely, assigns a responsible person to each asset. And the organization maintains/manages lists periodically, or at the request of the operator including configuration information of assets (e.g., names, version information, license information, and location) while recognizing situations in real time. - The information system regularly audits whether the actual configuration grasped conforms to the baseline configuration defined by the organization, and responds appropriately. (Example: blocking unplanned connections except those permitted by the organization as an exception) -The information system and industrial control system implement and operate a mechanism which automatically detects and responses to unauthorized assets.
				CPS.IP-1	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	Advanced	- When changes are made to the IoT devices and servers that are subjects of configuration management, the organization analyzes the impact the change has on security, decides whether the change can be made or not, and creates a document on the procedure. - The organization limits personnel who can make changes to approved IoT devices and servers (restricted access). - The organization makes changes to approved IoT devices and servers, as well as implements, records, and monitors those changes. - The organization uses a secure recovery method (e.g. entering a security code known only to the user before the change is implemented) if they forget the password of their accounts, IoT device and servers. - The organization regularly reviews policies and procedures for operation and change management to ensure that changes do not adversely affect the availability or safety of information system and industrial control system.
						Basic	- Upon determining the most restrictive setting criteria that conform to their operation, the organization creates a document on the initial setting procedures and setting details for the IoT devices and servers that will be introduced and adjusts the settings according to the document. - The organization checks initial setting values of IoT devices before installing them, and adjusts the settings appropriately if they do not comply with the policy stipulated in CPS.AC-1. - The organization checks and records software installed in IoT devices before introducing them.
	3.4.3	Track, review, approve/disapprove, and audit changes to organizational systems.	・CM-3 Configuration Change Control	CPS.IP-1	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	Advanced	- When changes are made to the IoT devices and servers that are subjects of configuration management, the organization analyzes the impact the change has on security, decides whether the change can be made or not, and creates a document on the procedure. - The organization limits personnel who can make changes to approved IoT devices and servers (restricted access). - The organization makes changes to approved IoT devices and servers, as well as implements, records, and monitors those changes. - The organization uses a secure recovery method (e.g. entering a security code known only to the user before the change is implemented) if they forget the password of their accounts, IoT device and servers. - The organization regularly reviews policies and procedures for operation and change management to ensure that changes do not adversely affect the availability or safety of information system and industrial control system.
				CPS.CM-6	As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	Advanced	- It is desirable that the organization should update the list of information about its assets and configurations when it installs or deletes new assets or when it updates its system. - The information system ensures that each external communications service is provided via a controlled interface (e.g., a gateway, router, and firewall). - The organization establishes a communications control policy for each controlled interface (e.g., a gateway, router, and firewall). - The system on a controlled interface rejects network communication by default and permits it as an exception. - The information system and the industrial control system terminate the network connection after a session ends, or when a session remains inactive for a certain length of time. - The organization monitors communication on controlled interfaces in order to detect any communication to unapproved items or systems, or communication that conveys an inappropriate content.
	3.4.4	Analyze the security impact of changes prior to implementation.	・CM-4 Security Impact Analysis	CPS.IP-1	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	Advanced	- When changes are made to the IoT devices and servers that are subjects of configuration management, the organization analyzes the impact the change has on security, decides whether the change can be made or not, and creates a document on the procedure. - The organization limits personnel who can make changes to approved IoT devices and servers (restricted access). - The organization makes changes to approved IoT devices and servers, as well as implements, records, and monitors those changes. - The organization uses a secure recovery method (e.g. entering a security code known only to the user before the change is implemented) if they forget the password of their accounts, IoT device and servers.
	3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	・CM-5 Access Restrictions for Change				
	3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	・CM-7 Least Functionality	CPS.PT-2	Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.	H-Advanced	- The organization identifies software programs that are not allowed to be executed on a system. - Manage a "black list" or "white list" so that the software programs not allowed on the system cannot be executed. - The organization regularly review and update the black list or the white list. - The system blocks the execution of these programs in accordance with the specified rules.
						Advanced	- The organization reviews the functions and services provided by its systems and items in order to identify the functions and services that could be deleted. - The organization uses network scanning tools, intrusion detection and prevention systems, and endpoint protection (e.g., a firewall, host-based intrusion detection system) in order to detect and prevent the use of banned functions, ports, protocols, and services. - The organization minimizes the functions and services of devices connected to the network such as multifunction printers in additional to typical IoT devices and servers.
	3.4.7	Restrict, disable, and prevent the use of nonessential functions, ports, protocols, and services.	・CM-7(1) Least Functionality Periodic Review ・CM-7(2) Least Functionality Prevent program execution	CPS.PT-2	Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.	H-Advanced	- The organization identifies software programs that are not allowed to be executed on a system. - Manage a "black list" or "white list" so that the software programs not allowed on the system cannot be executed. - The organization regularly review and update the black list or the white list. - The system blocks the execution of these programs in accordance with the specified rules.
	3.4.8	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	・CM-7(2) Least Functionality Unauthorized Software/ Blacklisting ・CM-7(5) Least Functionality Authorized Software/ Whitelisting	CPS.IP-2	Restrict the software to be added after installing in the IoT devices and servers.	H-Advanced	- The organization restricts software by using a list of software that is permitted to be executed on the information system and industrial control system (whitelist) or list of prohibited software (blacklist). Or, unpermitted software shall not be installed.
				CPS.PT-2	Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.	H-Advanced	- The organization identifies software programs that are not allowed to be executed on a system. - Manage a "black list" or "white list" so that the software programs not allowed on the system cannot be executed. - The organization regularly review and update the black list or the white list. - The system blocks the execution of these programs in accordance with the specified rules.
	3.4.9	Control and monitor user-installed software.	・CM-11 User-Installed Software	CPS.IP-2	Restrict the software to be added after installing in the IoT devices and servers.	H-Advanced	- The organization restricts software by using a list of software that is permitted to be executed on the information system and industrial control system (whitelist) or list of prohibited software (blacklist). Or, unpermitted software shall not be installed.
						Advanced	- The organization adopts and manages a mechanism that manages software installation that is performed by users on the organization's system (information system or industrial control system) and monitors the events.
IDENTIFICATION AND AUTHENTICATION	3.5.1	Identify system users, processes acting on behalf of users, or devices.	・IA-2 Identification and Authentication (Organizational Users) ・IA-5 Authenticator Management	CPS.AC-8	Restrict communications by IoT devices and servers to those with entities (e.g. people, components, system, etc.) identified through proper procedures.	Basic	- The organization assigns identifiers to its IoT devices and servers, as well as managing the identification by preventing re-use of identifiers and invalidating identifiers after a certain period of time. - Before connecting their IoT devices and servers to the network, the information system and the industrial control system prepare a mechanism that uniquely identifies and authenticate these devices. - Communication using IoT devices is denied as default. The protocol to be used is authorized as an exception.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.	･IA-2 Identification and Authentication (Organizational Users) ･IA-5 Authenticator Management	CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.
	3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	･IA-2(1) Identification and Authentication (Organizational Users) Network Access to Privileged Accounts ･IA-2(2) Identification and Authentication (Organizational Users) Network Access to Non-Privileged Accounts ･IA-2(3) Identification and Authentication (Organizational Users) Local Access to Privileged Accounts	CPS.AC-6	Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.	H-Advanced	- The system uses a multifactor authentication in its system for access to the system or network with non-privileged accounts. - Regarding an information system that handles highly confidential data, access to the system and network with privileged or non-privileged accounts in the system, uses an authentication mechanism that can tolerate attacks of replay. [Reference] It is desirable to refer to NIST SP 800 63-3 regarding strength of authentication methods and appropriate use cases.
						Advanced	- In consideration of the risk of unauthorized login to the privileged account in the system, the organization in principle prohibits login to the privileged account via the network when it is not possible to implement a sufficient confidence methods of authentication. - The information system requires a multifactor authentication in its system for access to the system or network with privileged accounts when cannot implement actions such as invalidating the administrator account for the system. - In principle, the organization invalidates the default administrator account in the information system. - The information system permits the necessary minimum privileged authority to the user account when performing privileged operations.
	3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	･IA-2(8) Identification and Authentication (Organizational Users) Network Access to Privileged Accounts-Replay Resistant ･IA-2(9) Identification and Authentication (Organizational Users) Network Access to Non-Privileged Accounts-Replay Resistant	CPS.AC-6	Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.	H-Advanced	- The system uses a multifactor authentication in its system for access to the system or network with non-privileged accounts. - Regarding an information system that handles highly confidential data, access to the system and network with privileged or non-privileged accounts in the system, uses an authentication mechanism that can tolerate attacks of replay. [Reference] It is desirable to refer to NIST SP 800 63-3 regarding strength of authentication methods and appropriate use cases.
	3.5.5	Prevent reuse of identifiers for a defined period.	･IA-4 Identifier Management	CPS.AC-1	Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	Advanced	- The organization must obtain approval from the management supervisor when creating a system account. - With regard to the shared user account, a user who can know authentication information is managed in a list or the like, and the range of using the account can be identified. - The organization monitors the usage of system accounts used in an information system. - If an account needs change or becomes unnecessary, the organization notifies the management supervisor. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used. - The organization notifies the user (or the person in charge of management) when the password is changed in an information system and an industrial control system. - If the information system resets the credentials for reasons such as user"s forgetting credentials, the information system confirms securely that the account is its own to prevent unauthorized tampering with the credentials by a malicious party.
						Basic	- The organization appoints a management supervisor for the accounts in its information system and industrial control system. - The organization decides and selects types of system accounts necessary (e.g., general user/system administrator/shared user/temporary user), with consideration of their mission and business functions. - The organization creates and enables system accounts as per the procedure, and changes, disables and deletes them as needed. - The organization develops a policy of credentials (e.g. password, security key) for its own information systems and industrial control systems, and implements a function that cannot be set up unless the credential satisfies the policy. The following is an example of the content of the policy. - Devolop and operate the requirements for passwords in order to ensure the minimum required complexity. - When new credentials are created, change them to at least the number of characters defined by the organization. - Store and transmit only cryptographically protected credentials. - Prohibit reuse of the same credentials for the period that the organization defines. - The organization allows its members to use temporary credentials exceptionally when logging on to the system when they have forgotten credentials, if they change immediately to a strong password. - The organization does not share user identification information among multiple system users in an information system and an industrial control system except when multiple users function as a single group.
				CPS.AC-8	Restrict communications by IoT devices and servers to those with entities (e.g. people, components, system, etc.) identified through proper procedures.	Basic	- The organization assigns identifiers to its IoT devices and servers, as well as managing the identification by preventing re-use of identifiers and invalidating identifiers after a certain period of time. - Before connecting their IoT devices and servers to the network, the information system and the industrial control system prepare a mechanism that uniquely identifies and authenticate these devices. - Communication using IoT devices is denied as default. The protocol to be used is authorized as an exception.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.5.6	Disable identifiers after a defined period of inactivity.	・IA-4 Identifier Management	CPS.AC-1	Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	Advanced	- The organization must obtain approval from the management supervisor when creating a system account. - With regard to the shared user account, a user who can know authentication information is managed in a list or the like, and the range of using the account can be identified. - The organization monitors the usage of system accounts used in an information system. - If an account needs change or becomes unnecessary, the organization notifies the management supervisor. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used. - The organization notifies the user (or the person in charge of management) when the password is changed in an information system and an industrial control system. - If the information system resets the credentials for reasons such as user"s forgetting credentials, the information system confirms securely that the account is its own to prevent unauthorized tampering with the credentials by a malicious party.
						Basic	- The organization appoints a management supervisor for the accounts in its information system and industrial control system. - The organization decides and selects types of system accounts necessary (e.g., general user/system administrator/shared user/temporary user), with consideration of their mission and business functions. - The organization creates and enables system accounts as per the procedure, and changes, disables and deletes them as needed. - The organization develops a policy of credentials (e.g. password, security key) for its own information systems and industrial control systems, and implements a function that cannot be set up unless the credential satisfies the policy. The following is an example of the content of the policy. - Devolop and operate the requirements for passwords in order to ensure the minimum required complexity. - When new credentials are created, change them to at least the number of characters defined by the organization. - Store and transmit only cryptographically protected credentials. - Prohibit reuse of the same credentials for the period that the organization defines. - The organization allows its members to use temporary credentials exceptionally when logging on to the system when they have forgotten credentials, if they change immediately to a strong password. - The organization does not share user identification information among multiple system users in an information system and an industrial control system except when multiple users function as a single group.
	3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	・IA-5(1) Authenticator Management Password-Based Authentication	CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.
	3.5.8	Prohibit password reuse for a specified number of generations.	・IA-5(1) Authenticator Management Password-Based Authentication	CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.
	3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	・IA-5(1) Authenticator Management Password-Based Authentication	CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.5.10	Store and transmit only cryptographically-protected passwords.	・IA-5(1) Authenticator Management Password-Based Authentication	CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.
	3.5.11	Obscure feedback of authentication information.	・IA-6 Authenticator Feedback	CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.
INCIDENT RESPONSE	3.6.1	Establish an operational incident-handling capability for organizational systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.	・IR-2 Incident Response Training ・IR-4 Incident Handling ・IR-5 Incident Monitoring ・IR-6 Incident Reporting ・IR-7 Incident Response Assistance	CPS.SC-9	Prepare and test a procedure for incident response with relevant parties involved in the incident response activitiy to ensure action for incident response in the supply chain.	H-Advanced	- The organization assumes the course of action for security incidents of the supply chain and prepares a procedure that adjusts incident responses between the organization and other organizations that are concerned with the supply chain. - The organization assumes the course of action for security incidents of the supply chain and implements tests that adjust incident responses with other organizations that are concerned with the supply chain. [Reference] Violations in the security incidents of supply chain include violations on system components, IT products, development processes, developers, distribution processes, and warehouse facilities.
						Advanced	- The organization adjusts the incident response process of an external service provider that contains important features in order to continue its business, as well as adjusting the organization's incident response process to meet the incident response requirements. - The organization tests the incident response process that requires cooperation between the organization and external service providers.
				CPS.AE-2	Appoint a chief security officer, establish a security management team (SOC/CSIRT), and prepare a system within the organization to detect, analyze, and respond to security events.	Advanced	- The organization refers to risk assessment results and, considering the following angles, establishes what to monitor and what to include in correlation analysis. - The scope of systems to monitor - Which device logs should be collected for analysis (see CPS.AE-3) - The organization regularly reviews audit logs collected through monitoring. - The organization continues to collect and manage information about assets, device configurations, and network configurations in order to evaluate its security status. - The organization examines the results of correlation analysis and other data to accurately detect security events that must be addressed and take action in accordance with the security operation process. See CPS.RP-1 for details of the process. - The organization regularly reports the state of organizational and system security to the chief security officer or other appropriate staff members. It is desirable that the regular report should include the following shown below: - Results of log analysis (e.g., the number of incidents handled; summaries of typical incidents that have been handled; threats that have emerged; issues in monitoring); - Policy for future improvements in monitoring.
				CPS.AE-4	Identify the impact of security events, including the impact on other relevant organizations.	Advanced	- The organization works with IPA, JPCERT/CC, the industry's ISAC, and a security vendor to collect information, thereby interlinking and sharing information about threats and vulnerability to obtain a whole picture of the security event. - The organization requests an external security vendor to analyze the functions of the malware, or program, or script placed by an attacker if any is found in a security event that has occurred.
				CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.	Basic	- The organization develops and manages a process of security operation it should follow when a security incident arises that it must address. It is advisable to include contents such as the following in the process: - Response procedure for the person who received the incident report - Instructions and orders, and how to prioritize actions in an emergency; - Incident response; - Incident impact assessment and damage analysis; - Information gathering, selecting information that the organization needs; - Communication and announcement to relevant internal personnel; - Communication with relevant external organizations; - The system (especially, industrial control system) shuts down, issues an alert to the administrator, or takes other fail-safe actions if any abnormality (e.g., malfunction) occurs in IoT devices or servers. [Reference] "SP 800-61 rev.1" (NIST, 2008) is available for reference to determine the process for handling security incidents that have arisen.
				CPS.CO-3	Include the item in the business continuity plan or emergency response plan to the effect that the details of the recovery activities shall be communicated to the internal and external stakeholders, executives, and management.	Advanced	- The organization provides an overview of a security incident for relevant external entities including the regulatory authorities, business partners, and end users, and collects detailed information about damage inflicted by the incident. - The organization coordinates actions related to recovery and post-incident processing with relevant external entities involved in the supply chain. An example of these actions is recalling items produced when a security incident in the production system has occurred.
				CPS.AN-1	Understand the impact of the security incident on the whole society including the organization and relevant parties such as partners based on the full account of the incident and the probable intent of the attacker.	Advanced	- The organization works with IPA, JPCERT/CC, the industry's ISAC, and a security vendor to collect information, thereby interlinking and sharing information about threats and vulnerability to obtain a whole picture of the security incident. - The organization requests an external security vendor to analyze the functions of the malware, or program, or script placed by an attacker if any is found in a security incident that has occurred.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.AN-3	Categorize and store information regarding the detected security incidents by the size of security-related impact, penetration vector, and other factors.	Advanced	- The organization classifies security incidents, taking into account the recovery time objectives for the systems, the order of priority in recovery, and metrics in the process of its security operation. - The organization tracks and documents security incidents that may affect it. "SP 800-61 rev.1" lists the following as examples of points of view that may be taken when an organization documents a security incident. - The present state of the incident - Overview of the incident - The course of action the organization has taken to deal with the incident - Other contact information of relevant personnel (e.g., the system owner, system administrator) - List of proof collected during the investigation - Comments by the staff in charge of dealing with the incident - Next steps
				CPS.MI-1	Take measures to minimize security-related damages and mitigate the impacts caused by such incident.	Basic	- The organization (or its members) takes courses of action to reduce security incidents (e.g., shutting down the system; cutting off the system from a wired/wireless network; cutting off a modem cable; disabling certain functions) in accordance with prescribed procedures. [Reference] Courses of action to reduce the impact of a security incident may vary according to the nature of the incident (e.g., according to the threat that has emerged, such as a denial-of-service attack, malware infection, or unauthorized access). For example, It is advisable to refer to "SP 800-61 rev.1" (NIST, 2008) for detailed information about courses of action to reduce the impact of an incident.
	3.6.2	Track, document, and report incidents to appropriate organizational officials and/or authorities.	･IR-2 Incident Response Training ･IR-4 Incident Handling ･IR-5 Incident Monitoring ･IR-6 Incident Reporting ･IR-7 Incident Response Assistance	CPS.RP-4	Take appropriate measures on goods (products) whose quality is expected to be affected by some reasons, including its production facility damaged by the occurrence of the security incident.	Advanced	- The organization provides an overview of a security incident for relevant external entities including business partners and end users, and collects detailed information about damage inflicted by the incident. - The organization coordinates actions related to recovery and post-incident processing with relevant external entities involved in the supply chain. It is advisable to identify the items for handling in accordance with the approaches included in CPS.AM-2 and CPS.AM-3.
				CPS.CO-2	Include the item in the business continuity plan or emergency response plan to the effect that the organization shall work to restore its social reputation after the occurrence of a high-risk security incident.	Basic	- The organization sets up a single point of contact for the media and business partners requesting information, thereby ensuring consistency in communication with them. - The organization remains aware of the positive side of providing a detailed explanation about damage caused by a security incident while considering the confidentiality of the important information.
				CPS.AN-3	Categorize and store information regarding the detected security incidents by the size of security-related impact, penetration vector, and other factors.	Advanced	- The organization classifies security incidents, taking into account the recovery time objectives for the systems, the order of priority in recovery, and metrics in the process of its security operation. - The organization tracks and documents security incidents that may affect it. "SP 800-61 rev.1" lists the following as examples of points of view that may be taken when an organization documents a security incident. - The present state of the incident - Overview of the incident - The course of action the organization has taken to deal with the incident - Other contact information of relevant personnel (e.g., the system owner, system administrator) - List of proof collected during the investigation - Comments by the staff in charge of dealing with the incident - Next steps
	3.6.3	Test the organizational incident response capability.	･IR-3 Incident Response Testing ･IR-3(2) Incident Response Testing Coordination with Related Plans	CPS.SC-9	Prepare and test a procedure for incident response with relevant parties involved in the incident response activitiy to ensure action for incident response in the supply chain.	H-Advanced	- The organization assumes the course of action for security incidents of the supply chain and prepares a procedure that adjusts incident responses between the organization and other organizations that are concerned with the supply chain. - The organization assumes the course of action for security incidents of the supply chain and implements tests that adjust incident responses with other organizations that are concerned with the supply chain. [Reference] Violations in the security incidents of supply chain include violations on system components, IT products, development processes, developers, distribution processes, and warehouse facilities.
						Advanced	- The organization adjusts the incident response process of an external service provider that contains important features in order to continue its business, as well as adjusting the organization's incident response process to meet the incident response requirements. - The organization tests the incident response process that requires cooperation between the organization and external service providers.
				CPS.AT-1	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	H-Advanced	- The organization regularly provides basic security awareness training to all members of staff. The organization can, for example, educate the following matters in addition to the contents explaining general matters. -Procedure to response when you receive a suspicious email -Notes on using mobile devices (e.g. Notes on connecting to a public wireless LAN) -Notes on using SNS - The organization creates a program for each role (e.g., system/software developper, purchasing personnel, system administrator, personnel in charge of security measures) to train information security personnel and to improve their skills. The program is conducted regularly on applicable personnel. - The organization regularly reviews records of security education and training.
						Advanced	- The organization provides basic security awareness training to new staff, or when necessary due to changes made to the information systems and the industrial control systems which the organization uses. - The organization records and manages the contents and results of security education and training for member in the organization.
MAINTENANCE	3.7.1	Perform maintenance on organizational systems.	･MA-2 Controlled Maintenance ･MA-3 Maintenance Tools ･MA-3(1) Maintenance Tools Inspect Tools ･MA-3(2) Maintenance Tools Inspect media	CPS.MA-1	- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updateswith managed tools properly and in a timely manner while recording the history. - Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable.	H-Advanced	- The organization gives prior approval for the use of devices and/or tools needed for maintenance to update its IoT devices and servers, and conducts monitoring. - The organization inspects the devices and/or tools for maintenance brought in by the staff members who update its IoT devices and servers in order to make sure that no inappropriate or unauthorized changes will be made. - The organization inspects the media used for maintenance to update its IoT devices and servers in order to make sure that the media contain no malicious code before they are used. - The organization introduces an IoT device designed to remotely update different software programs (OS, driver, application) at the same time.
						Advanced	- The organization plans maintenance work such as updating its IoT devices and servers, implements the plan, checks the work done, and documents the entire maintenance. - The organization gives prior approval for maintenance work such as updating its IoT devices and servers, and conducts monitoring. - The organization gives prior approval for travel from its premises for any maintenance work away from its premises, such as updating its IoT devices and servers. It also takes necessary actions before the travel, such as deleting relevant saved data. - The organization checks all security measures that may have been affected by maintenance work, such as updating its IoT devices and servers, after the work is complete in order to make sure that the relevant equipment works correctly. - The organization keeps the records of maintenance work done, such as updating its IoT devices and servers. - The organization establishes a process for authorizing maintenance staff in order to keep the list of authorized maintenance organizations or staff members updated.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.7.2	Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	･MA-2 Controlled Maintenance ･MA-3 Maintenance Tools ･MA-3(1) Maintenance Tools Inspect Tools ･MA-3(2) Maintenance Tools Inspect media	CPS.MA-1	- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updateswith managed tools properly and in a timely manner while recording the history. - Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable.	H-Advanced	- The organization gives prior approval for the use of devices and/or tools needed for maintenance to update its IoT devices and servers, and conducts monitoring. - The organization inspects the devices and/or tools for maintenance brought in by the staff members who update its IoT devices and servers in order to make sure that no inappropriate or unauthorized changes will be made. - The organization inspects the media used for maintenance to update its IoT devices and servers in order to make sure that the media contain no malicious code before they are used. - The organization introduces an IoT device designed to remotely update different software programs (OS, driver, application) at the same time.
						Advanced	- The organization plans maintenance work such as updating its IoT devices and servers, implements the plan, checks the work done, and documents the entire maintenance. - The organization gives prior approval for maintenance work such as updating its IoT devices and servers, and conducts monitoring. - The organization gives prior approval for travel from its premises for any maintenance work away from its premises, such as updating its IoT devices and servers. It also takes necessary actions before the travel, such as deleting relevant saved data. - The organization checks all security measures that may have been affected by maintenance work, such as updating its IoT devices and servers, after the work is complete in order to make sure that the relevant equipment works correctly. - The organization keeps the records of maintenance work done, such as updating its IoT devices and servers. - The organization establishes a process for authorizing maintenance staff in order to keep the list of authorized maintenance organizations or staff members updated.
	3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	･MA-2 Controlled Maintenance	CPS.IP-6	When disposing of an IoT device and server, delete the stored data and the ID (identifier) uniquely identifying the genuine IoT devices and servers as well as important information (e.g., private key and digital certificate), or make them unreadable.	H-Advanced	- The organization defines classifications including security categories of data saved in an IoT device or server to be scrapped, and introduces a mechanism for using the proper technique for deleting data with the strength and integrity needed or making the data unreadable according to the definition.
						Advanced	- The organization establishes a procedure for scrapping its equipment including IoT devices and servers, deletes data saved in the equipment or makes the data unreadable in accordance with the procedure, and makes sure that the action has been done successfully.
						Basic	- The organization deletes data that has been saved in its IoT devices or servers to be scrapped, or makes the data unreadable.
	3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	･MA-3(2) Maintenance Tools Inspect media	CPS.MA-1	- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updateswith managed tools properly and in a timely manner while recording the history. - Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable.	H-Advanced	- The organization gives prior approval for the use of devices and/or tools needed for maintenance to update its IoT devices and servers, and conducts monitoring. - The organization inspects the devices and/or tools for maintenance brought in by the staff members who update its IoT devices and servers in order to make sure that no inappropriate or unauthorized changes will be made. - The organization inspects the media used for maintenance to update its IoT devices and servers in order to make sure that the media contain no malicious code before they are used. - The organization introduces an IoT device designed to remotely update different software programs (OS, driver, application) at the same time.
						Advanced	- The organization plans maintenance work such as updating its IoT devices and servers, implements the plan, checks the work done, and documents the entire maintenance. - The organization gives prior approval for maintenance work such as updating its IoT devices and servers, and conducts monitoring. - The organization gives prior approval for travel from its premises for any maintenance work away from its premises, such as updating its IoT devices and servers. It also takes necessary actions before the travel, such as deleting relevant saved data. - The organization checks all security measures that may have been affected by maintenance work, such as updating its IoT devices and servers, after the work is complete in order to make sure that the relevant equipment works correctly. - The organization keeps the records of maintenance work done, such as updating its IoT devices and servers. - The organization establishes a process for authorizing maintenance staff in order to keep the list of authorized maintenance organizations or staff members updated.
	3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	･MA-4 Nonlocal Maintenance	CPS.MA-2	Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.	Advanced	- The organization documents the policy and procedure relating to establishing and implementing a connection designed for remote maintenance, and implements the connection in accordance with the policy and procedure. - The organization provides authentication required for network access that it specifies when remote maintenance is carried out. It also ensures that the session and network connection are terminated when the remote maintenance is complete.
						Basic	- The organization develops and agrees to an implementation plan for remote maintenance before carrying out the maintenance, and checks the results of the maintenance done. - The organization keeps the records of remote maintenance done.
	3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	･MA-5 Maintenance Personnel	CPS.SC-5	Formulate and manage security requirements applicable to members of other relevant organizations, such as business partners, who are engaged in operations outsourced from the organization.	H-Advanced	- The organization prepares a procedure to continuously monitor whether the security requirements from the contractee are complied with by the staff of the contractor, and to enable notification to the organization's personnel in charge in the case where irregular behavior is found.
						Advanced	- The organization trains the staff on information security aspects of supplier relationships to particularly ensure that the handling of confidential information is correctly understood. - The organization regularly confirms that it complies with the security requirements from the contractee in conducting the contracted work.
				CPS.MA-1	- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updateswith managed tools properly and in a timely manner while recording the history. - Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable.	Advanced	- The organization plans maintenance work such as updating its IoT devices and servers, implements the plan, checks the work done, and documents the entire maintenance. - The organization gives prior approval for maintenance work such as updating its IoT devices and servers, and conducts monitoring. - The organization gives prior approval for travel from its premises for any maintenance work away from its premises, such as updating its IoT devices and servers. It also takes necessary actions before the travel, such as deleting relevant saved data. - The organization checks all security measures that may have been affected by maintenance work, such as updating its IoT devices and servers, after the work is complete in order to make sure that the relevant equipment works correctly. - The organization keeps the records of maintenance work done, such as updating its IoT devices and servers. - The organization establishes a process for authorizing maintenance staff in order to keep the list of authorized maintenance organizations or staff members updated.
						Basic	- The organization makes sure that a maintenance staff member sent unattended to do maintenance work on its information system and industrial control system has the necessary access rights. - The organization appoints its staff member with the access rights and technical skills needed so as to supervise maintenance work done by a staff member without the necessary access rights.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement		Example of Security Measures
MEDIA PROTECTION	3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	･MP-2 Media Access ･MP-4 Media Storage ･MP-6 Media Sanitization	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	H-Advanced	- The organization regulates service wires and transmission paths that are related to their IoT devices and servers by physical access. - The organization regulates output devices of its system by physical access. - The organization monitors alarms and monitoring devices (e.g., surveillance cameras) for physical intrusions into the areas within the physical security boundaries.
						Advanced	- The organization monitors physical accesses to the areas within the physical security boundaries and regularly reviews the audit log. - The organization keeps the records of visitor's access to the areas within the physical security boundaries and regularly reviews them.
						Basic	- The organization maintains upkeep of the access list for areas where their IoT devices and servers are located and issues permission certificates necessary for access. - The organization defines physical security boundaries at its facilities, and implement access control according to the security requirements of assets placed within the boundaries and the results of risk assessment. - The organization monitors the work of temporarily authorized party within the physical security boundaries, such as by authorized attendants or monitoring cameras.
				CPS.PT-2	Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.	H-Advanced	- The organization identifies software programs that are not allowed to be executed on a system. - Manage a "black list" or "white list" so that the software programs not allowed on the system cannot be executed. - The organization regularly review and update the black list or the white list. - The system blocks the execution of these programs in accordance with the specified rules.
						Advanced	- The organization reviews the functions and services provided by its systems and items in order to identify the functions and services that could be deleted. - The organization uses network scanning tools, intrusion detection and prevention systems, and endpoint protection (e.g., a firewall, host-based intrusion detection system) in order to detect and prevent the use of banned functions, ports, protocols, and services. - The organization minimizes the functions and services of devices connected to the network such as multifunction printers in additional to typical IoT devices and servers.
						Basic	- The organization manages peripherals in use (e.g., USB flash drives) using a management ledger and keep them in a locked place. - The organization checks external storage devices connected to IoT devices or servers (e.g., USB flash drives) using antivirus software, use USB flash drives that can be checked for viruses, or take any appropriate action. - The organization plugs USB ports and serial ports out of use to physically block them.
	3.8.2	Limit access to CUI on system media to authorized users.	･MP-2 Media Access ･MP-4 Media Storage ･MP-6 Media Sanitization	CPS.AC-8	Restrict communications by IoT devices and servers to those with entities (e.g. people, components, system, etc.) identified through proper procedures.	Basic	- The organization assigns identifiers to its IoT devices and servers, as well as managing the identification by preventing re-use of identifiers and invalidating identifiers after a certain period of time. - Before connecting their IoT devices and servers to the network, the information system and the industrial control system prepare a mechanism that uniquely identifies and authenticate these devices. - Communication using IoT devices is denied as default. The protocol to be used is authorized as an exception.
				CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.
	3.8.3	Mark media with necessary CUI markings and distribution limitations.	･MP-2 Media Access ･MP-4 Media Storage ･MP-6 Media Sanitization	CPS.IP-6	When disposing of an IoT device and server, delete the stored data and the ID (identifier) uniquely identifying the genuine IoT devices and servers as well as important information (e.g., private key and digital certificate), or make them unreadable.	H-Advanced	- The organization defines classifications including security categories of data saved in an IoT device or server to be scrapped, and introduces a mechanism for using the proper technique for deleting data with the strength and integrity needed or making the data unreadable according to the definition.
						Advanced	- The organization establishes a procedure for scrapping its equipment including IoT devices and servers, deletes data saved in the equipment or makes the data unreadable in accordance with the procedure, and makes sure that the action has been done successfully.
						Basic	- The organization deletes data that has been saved in its IoT devices or servers to be scrapped, or makes the data unreadable.
	3.8.4	Sanitize or destroy system media containing CUI before disposal or release for reuse.	･MP-3 Media Marking	CPS.AM-6	Classify and prioritize resources (e.g., People, Components, Data, and System) by function, importance, and business value, and communicate to the organizations and people relevant to those resources in business.	Advanced	- The organization considers business requirements and legal requirements which share or restrict data when classifying resources of the information system and industrial control system (data, components processing data, system, etc). - The person responsible for an asset is responsible for the classification of the data. - The organization includes classification rules and classification review standards after time passes in a resource classification system.
						Basic	- The organization sets priorities on identified information assets according to importance to the organization. - When related laws or regulations require us to follow a certain classification for resources of the organization (e.g., system and data), apply an appropriate classification to the asset.
	3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	･MP-5 Media Transport	CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	Advanced	- Maintain/manage lists including configuration information of assets (e.g., names, version information, license information, and location) by reviewing and updating them periodically. - The organization makes a list of removable media (e.g., USB memory sticks) that can be used on system components (information system or industrial control system), and manages the use of them. - The organization uses only removable media (e.g. USB memory) permitted in the organization. Also, if there is no identifiable ownwer of portable storage devices, the organization prohibits the use of such devices. - The organization controles access to the media that contain highly confidential data, and properly grasps and manages the usage of the media taken outside of the controlled areas.
						Basic	- The organization identifies assets constituting its information system and industrial control system (hardware, software and information), assigns a responsible person to each asset, and documents a list of them. - It is desirable to list all the assets held, but if the target is huge, consider narrowing down the target assets through integration (grouping) of the analysis target and exclusion from the analysis target. - The organization sets priorities to the identified assets based on the importance of them in its business operation.
	3.8.6	Implement cryptographic mechanisms to protect the confidentiality of information stored on digital media during transport outside of controlled areas unless otherwise protected by alternative physical safeguards.	･MP-5(4) Media Transport Cryptographic Protection	CPS.DS-2	Encrypt information with an appropriate level of security strength, and store them.	H-Advanced	- The organization selects products that have been authenticated based on Cryptographic Module Validation Program (CMVP) in order to suitably implement selected algorithms to software and hardware, and to protect keys, identification codes, and entity authentication information that is used to decrypt encrypted information or to grant electronic signatures. - The organization protects are encrypts data to the appropriate strength when that data is taken outside of the organization. - The organization uses IoT devices that can encrypt and store data in internal memory.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.8.7	Control the use of removable media on system components.	・MP-7 Media Use	CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	Advanced	- Maintain/manage lists including configuration information of assets (e.g., names, version information, license information, and location) by reviewing and updating them periodically. - The organization makes a list of removable media (e.g., USB memory sticks) that can be used on system components (information system or industrial control system), and manages the use of them. - The organization uses only removable media (e.g. USB memory) permitted in the organization. Also, if there is no identifiable ownwer of portable storage devices, the organization prohibits the use of such devices. - The organization controles access to the media that contain highly confidential data, and properly grasps and manages the usage of the media taken outside of the controlled areas.
						Basic	- The organization identifies assets constituting its information system and industrial control system (hardware, software and information), assigns a responsible person to each asset, and documents a list of them. - It is desirable to list all the assets held, but if the target is huge, consider narrowing down the target assets through integration (grouping) of the analysis target and exclusion from the analysis target. - The organization sets priorities to the identified assets based on the importance of them in its business operation.
	3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	・MP-7(1) Media Use Prohibit Use Without Owner	CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	Advanced	- Maintain/manage lists including configuration information of assets (e.g., names, version information, license information, and location) by reviewing and updating them periodically. - The organization makes a list of removable media (e.g., USB memory sticks) that can be used on system components (information system or industrial control system), and manages the use of them. - The organization uses only removable media (e.g. USB memory) permitted in the organization. Also, if there is no identifiable ownwer of portable storage devices, the organization prohibits the use of such devices. - The organization controles access to the media that contain highly confidential data, and properly grasps and manages the usage of the media taken outside of the controlled areas.
						Basic	- The organization identifies assets constituting its information system and industrial control system (hardware, software and information), assigns a responsible person to each asset, and documents a list of them. - It is desirable to list all the assets held, but if the target is huge, consider narrowing down the target assets through integration (grouping) of the analysis target and exclusion from the analysis target. - The organization sets priorities to the identified assets based on the importance of them in its business operation.
	3.8.9	Protect the confidentiality of backup CUI at storage locations.	・CP-9 System Backup	CPS.IP-4	Perform a periodical system backup and testing of components (e.g., IoT devices, communication devices, and circuits).	Advanced	- The organization backs up their system documents according to the prescribed timing and frequency. - The organization protects the confidentiality, integrity, and availability of the information backed up on the storage base.
						Basic	- The organization backs up information on user level and system level that is included in its information systems or industrial control systems according to the prescribed timing and frequency.
PERSONNEL SECURITY	3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	・PS-3 Personnel Screening ・PS-4 Personnel Termination ・PS-5 Personnel Transfer	CPS.IP-9	Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.	Advanced	- The organization makes changes to its staff members' rights to access certain systems and/or rooms on the premises when they are reshuffled or transferred internally. - To minimize impacts when a staff member leaves the organization, designate backup members regarding important duties as a supplier including operation and maintenance. - The organization identifies conditions in which re-screening is required such as changes in access authority to their own systems, and re-screen if necessary. - The organization conducts an interview on information security when personnel leave. - The organization ensures that responsibilities for security are met, particularly of personnel handling sensitive information, throughout the whole process from hiring to retirement.
						Basic	- The organization identifies the responsibility for security of personnel in the employment contract. The organization states that this responsibility should be sustained for a reasonable period of time after the termination of employment, in order to prevent information leakage after the termination of employment. - The organization reviews a staff member before granting him or her access to its systems. - The organization conducts the following when a staff member resigns or retires: - Disables the staff member's access to its systems within a certain period; - Disables the authentication and credentials related to the staff member; - Collects all system-related things for security that the staff member has used; - Retains access to the information about the organization and information systems that have been managed by the individual who is leaving.
	3.9.2	Ensure that CUI and organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	・PS-3 Personnel Screening ・PS-4 Personnel Termination ・PS-5 Personnel Transfer	CPS.IP-9	Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.	Advanced	- The organization makes changes to its staff members' rights to access certain systems and/or rooms on the premises when they are reshuffled or transferred internally. - To minimize impacts when a staff member leaves the organization, designate backup members regarding important duties as a supplier including operation and maintenance. - The organization identifies conditions in which re-screening is required such as changes in access authority to their own systems, and re-screen if necessary. - The organization conducts an interview on information security when personnel leave. - The organization ensures that responsibilities for security are met, particularly of personnel handling sensitive information, throughout the whole process from hiring to retirement.
						Basic	- The organization identifies the responsibility for security of personnel in the employment contract. The organization states that this responsibility should be sustained for a reasonable period of time after the termination of employment, in order to prevent information leakage after the termination of employment. - The organization reviews a staff member before granting him or her access to its systems. - The organization conducts the following when a staff member resigns or retires: - Disables the staff member's access to its systems within a certain period; - Disables the authentication and credentials related to the staff member; - Collects all system-related things for security that the staff member has used; - Retains access to the information about the organization and information systems that have been managed by the individual who is leaving.
PHYSICAL PROTECTION	3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	・PE-2 Physical Access Authorizations ・PE-5 Access Control for Output Devices ・PE-6 Monitoring Physical Access	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	Basic	- The organization maintains upkeep of the access list for areas where their IoT devices and servers are located and issues permission certificates necessary for access. - The organization defines physical security boundaries at its facilities, and implement access control according to the security requirements of assets placed within the boundaries and the results of risk assessment. - The organization monitors the work of temporarily authorized party within the physical security boundaries, such as by authorized attendants or monitoring cameras.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	・PE-2 Physical Access Authorizations ・PE-5 Access Control for Output Devices ・PE-6 Monitoring Physical Access	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	Advanced	- The organization monitors physical accesses to the areas within the physical security boundaries and regularly reviews the audit log. - The organization keeps the records of visitor's access to the areas within the physical security boundaries and regularly reviews them.
				CPS.CM-2	Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.	Advanced	- The organization reviews the relevant audit log regularly or when an incident or a sign of an incident appears if a physical access log from access control is available while 24-h monitoring is not conducted through security cameras or by any other means. - A person in charge accompanies a visitor into the area where the organization's assets that must be protected are directly accessible (e.g., an office) in order to monitor the visitor's behavior. - The organization monitors through security cameras or by other means physical access to its facilities that are vital for its operations and house IoT devices and servers, thereby enabling early detection of any physical security incidents and immediate action. - If the above physical security measures may be difficult to implement for items such as IoT devices and servers that may be critical to the organization's operation because they are in a remote location or for any other reasons, consider using tamper-resistant equipment (CPS.DS-6) or taking any other appropriate measures to enhance the physical security properties of the equipment itself.
						Basic	- If the organization is unable to control access to, or provide video surveillance service for, the areas that should allow only limited physical access because of issues of costs and other reasons, it takes alternative manual measures, such as that its employee in charge accompany a visitor on the premises. - The organization implements physical security measures to control access to designated areas in the facility that do not be allowed for the general public to access. - The organization verifies the access authority of the personnel before permitting the physical access and collects and manages the records of entry and exit.
	3.10.3	Escort visitors and monitor visitor activity.	・PE-3 Physical Access Control	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	Basic	- The organization maintains upkeep of the access list for areas where their IoT devices and servers are located and issues permission certificates necessary for access. - The organization defines physical security boundaries at its facilities, and implement access control according to the security requirements of assets placed within the boundaries and the results of risk assessment. - The organization monitors the work of temporarily authorized party within the physical security boundaries, such as by authorized attendants or monitoring cameras.
	3.10.4	Maintain audit logs of physical access.	・PE-3 Physical Access Control	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	Advanced	- The organization monitors physical accesses to the areas within the physical security boundaries and regularly reviews the audit log. - The organization keeps the records of visitor's access to the areas within the physical security boundaries and regularly reviews them.
				CPS.CM-2	Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.	Advanced	- The organization reviews the relevant audit log regularly or when an incident or a sign of an incident appears if a physical access log from access control is available while 24-h monitoring is not conducted through security cameras or by any other means. - A person in charge accompanies a visitor into the area where the organization's assets that must be protected are directly accessible (e.g., an office) in order to monitor the visitor's behavior. - The organization monitors through security cameras or by other means physical access to its facilities that are vital for its operations and house IoT devices and servers, thereby enabling early detection of any physical security incidents and immediate action. - If the above physical security measures may be difficult to implement for items such as IoT devices and servers that may be critical to the organization's operation because they are in a remote location or for any other reasons, consider using tamper-resistant equipment (CPS.DS-6) or taking any other appropriate measures to enhance the physical security properties of the equipment itself.
						Basic	- If the organization is unable to control access to, or provide video surveillance service for, the areas that should allow only limited physical access because of issues of costs and other reasons, it takes alternative manual measures, such as that its employee in charge accompany a visitor on the premises. - The organization implements physical security measures to control access to designated areas in the facility that do not be allowed for the general public to access. - The organization verifies the access authority of the personnel before permitting the physical access and collects and manages the records of entry and exit.
	3.10.5	Control and manage physical access devices.	・PE-3 Physical Access Control	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	Advanced	- The organization monitors physical accesses to the areas within the physical security boundaries and regularly reviews the audit log. - The organization keeps the records of visitor's access to the areas within the physical security boundaries and regularly reviews them.
				CPS.CM-2	Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.	Advanced	- The organization reviews the relevant audit log regularly or when an incident or a sign of an incident appears if a physical access log from access control is available while 24-h monitoring is not conducted through security cameras or by any other means. - A person in charge accompanies a visitor into the area where the organization's assets that must be protected are directly accessible (e.g., an office) in order to monitor the visitor's behavior. - The organization monitors through security cameras or by other means physical access to its facilities that are vital for its operations and house IoT devices and servers, thereby enabling early detection of any physical security incidents and immediate action. - If the above physical security measures may be difficult to implement for items such as IoT devices and servers that may be critical to the organization's operation because they are in a remote location or for any other reasons, consider using tamper-resistant equipment (CPS.DS-6) or taking any other appropriate measures to enhance the physical security properties of the equipment itself.
						Basic	- If the organization is unable to control access to, or provide video surveillance service for, the areas that should allow only limited physical access because of issues of costs and other reasons, it takes alternative manual measures, such as that its employee in charge accompany a visitor on the premises. - The organization implements physical security measures to control access to designated areas in the facility that do not be allowed for the general public to access. - The organization verifies the access authority of the personnel before permitting the physical access and collects and manages the records of entry and exit.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.10.6	Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).	・PE-17 Alternate Work Site	CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).	H-Advanced	- The information system and the industrial control system automatically monitor or regulate remote access to its system. - The information system and the industrial control system allow only for remote access routed by the regulated access points. - The information system allows privileged command via remote access only for those purposes based on specified requirements. - The information system records reasons why the users accessing the system which handles highly confidential data execute privileged commands and access security information by remote access. - The information system protects wireless access to the system which handles highly confidential data by using user and device authentication in addition to encryption. - The information system blocks remote activation of devices such as white boards, cameras, and microphones connected via networks which may handle highly confidential data. Signs of the devices in use are provided to the users of these devices.
RISK ASSESSMENT	3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	・RA-3 Risk Assessment	CPS.RA-4	- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation. - Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.	Advanced	- The organization updates a risk assessment when there is a big change in a system or an environment where a system is running (including identification of a new threat or vulnerability) or when any situation which impacts the security status of a system occurs. - When planning/designing a new system using an IoT device, the organization identifies existing assets and assets to be protected in the system to be implemented and organizes security measures according to use and configuration of the system. When handling a component or a system with a long life cycle and a component or a system requiring availability, consideration in security measures at a phase before designing is especially important. - When considering security measures applied to purchased products and services, the organization makes sure that the levels of measures correspond to the importance of such products and services.
	3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	・RA-5 Vulnerability Scanning ・RA-5(5) Vulnerability Scanning Privileged Access	CPS.CM-7	Confirm the existence of vulnerability that requires a regular check-up in IoT devices and servers managed within the organization.	H-Advanced	- The organization conducts vulnerability diagnosis at planned timings such as planned stopping so as not to adversely affect the operation of the system managed by the organization. And then, identify and list vulnerabilities that exist in the system owned by the organization. - When using tools to conduct vulnerability diagnosis, the organization should use tools that can quickly update the vulnerability database of the system being diagnosed. - The organization updates the vulnerability of scanned systems regularly, or when newly-identified weaknesses are reported. - The organization implements a system for authorizing privileged access to the relevant system components in connection with the specified vulnerability scanning.
						Advanced	- The organization has its systems and applications scanned for vulnerability regularly, or when any newly-found weaknesses that affect the systems and/or applications are reported. - The organization uses a tool for vulnerability scanning. Applying the standard methods that meet the following means that part of the vulnerability management process should be open to automation. - List defects in the platform and software, and wrong setups. - Format a checklist and test procedure. - Assess the impact of the vulnerability. - The organization corrects identified weaknesses through risk assessment within an appropriate period. - The organization shares the information acquired through the above process with other system administrators in the organization, thereby learning about similar weaknesses found in the other information systems, and correct them as necessary. [Reference] Japan Vulnerability Notes (https://jvn.jp/) and other sources of information are available for reference to obtain information regarding vulnerability. Also, CVSS (https://www.ipa.go.jp/security/vuln/CVSS.html Illustrated by IPA) could be used as a referential indicator to evaluate the impact level of vulnerability.
						Basic	- The organization regularly has its systems and applications scanned for vulnerability.
	3.11.3	Remediate vulnerabilities in accordance with assessments of risk.	・RA-5 Vulnerability Scanning	CPS.RA-6	- On the basis of the results of the risk assessment, clearly define the details of measures to prevent possible security risks, and document the organized outcome from the scope and priorities of the measures. - React accordingly to the security risks and the associated safety risks identified as a result of the assessment conducted at the planning and design phase of an IoT device and systems incorporating IoT devices.	Advanced	- The organization securely stores the documented information on security risk management processes. - When the organization selects a measure according to the risk assessment results, it is desirable that the organization documents the measure to be taken and the reason why the measure is adopted. - When applying the measure, the organization formulates a security risk management plan and obtains an approval from the risk owner. - The organization reviews the security risk handling plan and checks that the applicable plan conforms to the priority order of the entire organization's risk management strategy. - The organization informs applicable external business operators regarding security measures necessary for a new system including an IoT device which are extracted in CPS.RA-4 as required specifications. - The organization verifies whether the security measures defined in the required specifications and contracts are implemented at the time of deployment of the systems including an IoT device via User Acceptance Test (UAT). If there is anything unclear, confirm with the external business operator.
						Basic	- The organization considers the risk assessment results and selects handling measures to identified risks. - The organization formulates a security risk treatment implementation plan. - The organization obtain an approval from the risk owner for acceptance of the security risk.
				CPS.CM-7	Confirm the existence of vulnerability that requires a regular check-up in IoT devices and servers managed within the organization.	Advanced	- The organization has its systems and applications scanned for vulnerability regularly, or when any newly-found weaknesses that affect the systems and/or applications are reported. - The organization uses a tool for vulnerability scanning. Applying the standard methods that meet the following means that part of the vulnerability management process should be open to automation. - List defects in the platform and software, and wrong setups. - Format a checklist and test procedure. - Assess the impact of the vulnerability. - The organization corrects identified weaknesses through risk assessment within an appropriate period. - The organization shares the information acquired through the above process with other system administrators in the organization, thereby learning about similar weaknesses found in the other information systems, and correct them as necessary. [Reference] Japan Vulnerability Notes (https://jvn.jp/) and other sources of information are available for reference to obtain information regarding vulnerability. Also, CVSS (https://www.ipa.go.jp/security/vuln/CVSS.html Illustrated by IPA) could be used as a referential indicator to evaluate the impact level of vulnerability.
						Basic	- The organization regularly has its systems and applications scanned for vulnerability.
SECURITY ASSESSMENT	3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	・CA-2 Security Assessments ・CA-5 Plan of Action and Milestones ・CA-7 Continuous Monitoring ・PL-2 System Security Plan	CPS.IP-7	Assess the lessons learned from security incident response and the results of monitoring, measuring, and evaluating internal and external attacks, and improve the processes of protecting the assets.	Advanced	- The organization draws up a security assessment plan before the assessment is carried out that includes the following so as to ensure that its security is assessed properly and systematically: - Security measures for assessment; - Assessment procedures for measuring the effectiveness of security measures; - Settings and mechanisms for carrying out the security assessment; - Methods of putting together the results of the security assessment and applications of the results.
						Basic	- The organization regularly evaluates whether its security measures have achieved expected results (i.e., security assessment) and reports the conclusions to the chief security officer, in addition to the evaluation of whether the measures are correctly implemented and managed. - The organization makes improvements on its security measures based on the results of the security assessment.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	･CA-2 Security Assessments ･CA-5 Plan of Action and Milestones ･CA-7 Continuous Monitoring ･PL-2 System Security Plan	CPS.RA-6	- On the basis of the results of the risk assessment, clearly define the details of measures to prevent possible security risks, and document the organized outcome from the scope and priorities of the measures. - React accordingly to the security risks and the associated safety risks identified as a result of the assessment conducted at the planning and design phase of an IoT device and systems incorporating IoT devices.	Advanced	- The organization securely stores the documented information on security risk management processes. - When the organization selects a measure according to the risk assessment results, it is desirable that the organization documents the measure to be taken and the reason why the measure is adopted. - When applying the measure, the organization formulates a security risk management plan and obtains an approval from the risk owner. - The organization reviews the security risk handling plan and checks that the applicable plan conforms to the priority order of the entire organization's risk management strategy. - The organization informs applicable external business operators regarding security measures necessary for a new system including an IoT device which are extracted in CPS.RA-4 as required specifications. - The organization verifies whether the security measures defined in the required specifications and contracts are implemented at the time of deployment of the systems including an IoT device via User Acceptance Test (UAT). If there is anything unclear, confirm with the external business operator.
	3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	･CA-2 Security Assessments ･CA-5 Plan of Action and Milestones ･CA-7 Continuous Monitoring ･PL-2 System Security Plan	CPS.RA-4	- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation. - Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.	H-Advanced	- When developing a new device or a new component which may have an impact on a physical space such as components of an industrial control system, the organization collects/analyzes accident case studies of conventional products and others to identify safety-related hazards. - The organization analyzes a situation where a hazard leads to harm and identifies the possibility of occurrence and the severity of the harm to estimate a possible risk especially regarding an industrial control system. At the time, it is desirable to check whether there is any hazard caused by a security issue. - The organization updates the risk assessment if there is a significant change in the industrial control system or the environment in which it operates, or the other change that affects the security state of the industrial control system.
						Advanced	- The organization updates a risk assessment when there is a big change in a system or an environment where a system is running (including identification of a new threat or vulnerability) or when any situation which impacts the security status of a system occurs. - When planning/designing a new system using an IoT device, the organization identifies existing assets and assets to be protected in the system to be implemented and organizes security measures according to use and configuration of the system. When handling a component or a system with a long life cycle and a component or a system requiring availability, consideration in security measures at a phase before designing is especially important. - When considering security measures applied to purchased products and services, the organization makes sure that the levels of measures correspond to the importance of such products and services.
						Basic	- The organization defines a security risk assessment process and applies it periodically (e.g., once a year). - Establish and maintain security risk criteria. - Identify security risks in the following way. 1) Clarify the target of analysis. 2) Identify incidents (including changes in circumstances) and their causes. - Analyze security risks in the following way. 1) Evaluate possible results when the above identified risks occur. 2) Evaluate the possibility of the actual occurrence of the above identified risks. - Refer to the risk criteria, determine a risk level, and prioritize the risk. - The organization documents and stores the information security risk assessment process. [Reference] An "asset-based" method and a "business damage-based" method are known as security risk assessment methods.
	3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	･CA-2 Security Assessments ･CA-5 Plan of Action and Milestones ･CA-7 Continuous Monitoring ･PL-2 System Security Plan	CPS.AM-5	Create and manage appropriately a list of external information systems where the organization's assets are shared.	H-Advanced	- The system makes a list of external information services in use and manages the users, devices as well as serviced in use in real time. - The system uses a mechanism to give notice to the system administrator when an unpermitted external information system service is detected. - The organization identifies functions, ports, protocols, and other services which are necessary for using services offered by external providers.
						Advanced	- The organization sets conditions for allowing other organizations which own or operate external information systems to do the following: a. Accessing an information system in the organization from an external information system b. Processing, saving, or transmitting information under the control of the organization using an external information system - The organization restricts a use of storage in an external system the organization owns to an authorized one.
				CPS.RA-6	- On the basis of the results of the risk assessment, clearly define the details of measures to prevent possible security risks, and document the organized outcome from the scope and priorities of the measures. - React accordingly to the security risks and the associated safety risks identified as a result of the assessment conducted at the planning and design phase of an IoT device and systems incorporating IoT devices.	Advanced	- The organization securely stores the documented information on security risk management processes. - When the organization selects a measure according to the risk assessment results, it is desirable that the organization documents the measure to be taken and the reason why the measure is adopted. - When applying the measure, the organization formulates a security risk management plan and obtains an approval from the risk owner. - The organization reviews the security risk handling plan and checks that the applicable plan conforms to the priority order of the entire organization's risk management strategy. - The organization informs applicable external business operators regarding security measures necessary for a new system including an IoT device which are extracted in CPS.RA-4 as required specifications. - The organization verifies whether the security measures defined in the required specifications and contracts are implemented at the time of deployment of the systems including an IoT device via User Acceptance Test (UAT). If there is anything unclear, confirm with the external business operator.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
SYSTEM AND COMMUNICATIONS PROTECTION	3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	・SC-7 Boundary Protection ・SA-8 Security Engineering Principles	CPS.DS-9	Properly control outbound communications that send information to be protected to prevent improper data breach.	H-Advanced	- The industrial control system shuts down, isolates the malicious code or notifies the administrator when detecting such code through IDS/IPS. - The organization/system analyzes the regular patterns of its systems' communication status and security alerts to create and use a profile that summarizes typical patterns of communication and security alerts, thereby enabling the detection of unknown threats and suspicious behavior (communication). - The information system prevents fraudulent and unexpected transfer of information via common system resources.
						Advanced	- The information system blocks or isolates any malicious code for it detected through an IDS/IPS, or notifies the administrator of the code. - The organization collects information including newly released attacking trends, malware behaviors, and malicious IP addresses/domains (external intelligence). When necessary, the organization excutes responces to restrict communications to highly dangerous IP addresses or domains or so.
				CPS.CM-1	Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.	H-Advanced	- The information system routes communications to the network to which a recipient's IP address belongs via a proxy server authenticated on a controlled interface. - The information system and the industrial control system monitor and control the use of mobile code. - The information system monitors and controls the use of protocols used for audio and video transmission (e.g. VoIP).
						Advanced	- The organization monitors and controls communications at the boundary between industrial control system and information system. - The organization creates a network segment isolated from access to the internal network ("demilitarized zone [DMZ]") between the internal network and external networks (e.g., the Internet). - The information system is connected to an external network or system only via a controlled interface that consists of a boundary protection system placed according to the organization's security architecture. - The information system ensures that each external communications service is provided via a controlled interface (e.g., a gateway, router, and firewall). - The organization establishes a communications control policy for each controlled interface (e.g., a gateway, router, and firewall). - The system on a controlled interface rejects network communication by default and permits it as an exception. - The organization monitors communications at the external boundaries of the information system and at major internal boundaries within the information system for large amounts of communication from a particular source or multiple sources, and takes appropriate action when necessary (e.g., blocking of communication from a specific IP address).
						Basic	- The organization monitors and controls communications on the information system's external boundary as well as on the key internal boundary within the information system.
	3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	・SC-7 Boundary Protection ・SA-8 Security Engineering Principles	CPS.IP-3	Introduce the system development life cycle to manage the systems.	Basic	- The organization applies the general rules of the system's security engineering to specifications, design, development, introduction, and changes in building the system.
	3.13.3	Separate user functionality from system management functionality.	・SC-2 Application Partitioning	CPS.AC-5	Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions)	H-Advanced	- The organization specifies administrators who use the security functions (e.g., access authority setting) and regulates privileged accounts in its system. - The information system adopts a system monitoring mechanism to check the use of privileged functions. - The information system prohibits non-privileged users from executing privileged functions on the system by invalidating, avoiding, and changing security measures that are changed and implemented by non-privileged users. - The organization can minimize the number of users who can use the system administrator's authority in an emergency to minimize the damage caused by the security incident. - The organization can prevent even system administrators from stopping critical services and protected processes through the server to minimize the damage caused by security incidents.
						Advanced	- The organization implements access control in the information system and the industrial control system based on separation of duties (e.g., user / system administrator). - The organization adopts a general rule on the minimum authority of specific duties. - Segregate authority of general user from that of administrator. (Require users to use the system with a non-privileged account when using a non-security function.) - Minimize authority for duties not in charge. - The organization separates and stipulates duties that are assigned by the person in charge.
	3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	・SC-4 Information in Shared Resources	CPS.DS-9	Properly control outbound communications that send information to be protected to prevent improper data breach.	H-Advanced	- The industrial control system shuts down, isolates the malicious code or notifies the administrator when detecting such code through IDS/IPS. - The organization/system analyzes the regular patterns of its systems' communication status and security alerts to create and use a profile that summarizes typical patterns of communication and security alerts, thereby enabling the detection of unknown threats and suspicious behavior (communication). - The information system prevents fraudulent and unexpected transfer of information via common system resources.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	・SC-7 Boundary Protection	CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).	H-Advanced	- The information system and the industrial control system monitor and control communications on the networks composing internal business systems of the organization. - Regarding the network which the system that handles highly confidential data is connected to, the organization shall deny network communications as a default and shall only allow connection of approved communication traffic. - The organization physically or logically separates the network of high importance industrial control systems from the network of control systems with lower importance. - If the information system that handles highly confidential data is connected to a remote device, the organization is to prevent multiple and simultaneous local connections between the device and the system, as well as prevent access to external network resources by other connections.
						Basic	- The organization establishes a data flow regulation policy that defines the range in which data flow within information systems and industrial control system is permitted and the range in which data flow between systems is permitted, and regulates the flow by segregating the network appropriately. - The organization logically or physically segments the control system's network from the network composing of the information system. [Reference] Implement physical segmentation in environments physically separated from other networks. Alternatively, in environments physically close to other networks, it is possible to implement logical segmentation in consideration of the cost of the measure.
				CPS.CM-1	Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.	H-Advanced	- The information system routes communications to the network to which a recipient's IP address belongs via a proxy server authenticated on a controlled interface. - The information system and the industrial control system monitor and control the use of mobile code. - The information system monitors and controls the use of protocols used for audio and video transmission (e.g. VoIP).
						Advanced	- The organization monitors and controls communications at the boundary between industrial control system and information system. - The organization creates a network segment isolated from access to the internal network ("demilitarized zone [DMZ]") between the internal network and external networks (e.g., the Internet). - The information system is connected to an external network or system only via a controlled interface that consists of a boundary protection system placed according to the organization's security architecture. - The information system ensures that each external communications service is provided via a controlled interface (e.g., a gateway, router, and firewall). - The organization establishes a communications control policy for each controlled interface (e.g., a gateway, router, and firewall). - The system on a controlled interface rejects network communication by default and permits it as an exception. - The organization monitors communications at the external boundaries of the information system and at major internal boundaries within the information system for large amounts of communication from a particular source or multiple sources, and takes appropriate action when necessary (e.g., blocking of communication from a specific IP address).
						Basic	- The organization monitors and controls communications on the information system's external boundary as well as on the key internal boundary within the information system.
	3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	・SC-7(5) Boundary Protection Deny by Default / Allow by Exception	CPS.AC-8	Restrict communications by IoT devices and servers to those with entities (e.g. people, components, system, etc.) identified through proper procedures.	Basic	- The organization assigns identifiers to its IoT devices and servers, as well as managing the identification by preventing re-use of identifiers and invalidating identifiers after a certain period of time. - Before connecting their IoT devices and servers to the network, the information system and the industrial control system prepare a mechanism that uniquely identifies and authenticate these devices. - Communication using IoT devices is denied as default. The protocol to be used is authorized as an exception.
				CPS.CM-1	Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.	H-Advanced	- The information system routes communications to the network to which a recipient's IP address belongs via a proxy server authenticated on a controlled interface. - The information system and the industrial control system monitor and control the use of mobile code. - The information system monitors and controls the use of protocols used for audio and video transmission (e.g. VoIP).
						Advanced	- The organization monitors and controls communications at the boundary between industrial control system and information system. - The organization creates a network segment isolated from access to the internal network ("demilitarized zone [DMZ]") between the internal network and external networks (e.g., the Internet). - The information system is connected to an external network or system only via a controlled interface that consists of a boundary protection system placed according to the organization's security architecture. - The information system ensures that each external communications service is provided via a controlled interface (e.g., a gateway, router, and firewall). - The organization establishes a communications control policy for each controlled interface (e.g., a gateway, router, and firewall). - The system on a controlled interface rejects network communication by default and permits it as an exception. - The organization monitors communications at the external boundaries of the information system and at major internal boundaries within the information system for large amounts of communication from a particular source or multiple sources, and takes appropriate action when necessary (e.g., blocking of communication from a specific IP address).
	3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e. split tunneling).	・SC-7(7) Boundary Protection Prevent Split Tunneling for Remote Devices	CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).	H-Advanced	- The information system and the industrial control system monitor and control communications on the networks composing internal business systems of the organization. - Regarding the network which the system that handles highly confidential data is connected to, the organization shall deny network communications as a default and shall only allow connection of approved communication traffic. - The organization physically or logically separates the network of high importance industrial control systems from the network of control systems with lower importance. - If the information system that handles highly confidential data is connected to a remote device, the organization is to prevent multiple and simultaneous local connections between the device and the system, as well as prevent access to external network resources by other connections.
	3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	・SC-8 Transmission Confidentiality and Integrity ・SC-8(1) Transmission Confidentiality and Integrity Cryptographic or Alternate Physical Protection	CPS.DS-2	Encrypt information with an appropriate level of security strength, and store them.	H-Advanced	- The organization selects products that have been authenticated based on Cryptographic Module Validation Program (CMVP) in order to suitably implement selected algorithms to software and hardware, and to protect keys, identification codes, and entity authentication information that is used to decrypt encrypted information or to grant electronic signatures. - The organization protects are encrypts data to the appropriate strength when that data is taken outside of the organization. - The organization uses IoT devices that can encrypt and store data in internal memory.
						Advanced	- The organization examines safety and trustworthiness that are necessary, selects an algorithm, encrypts information (data) to the appropriate strength, and stores the information. If an algorithm on the CRYPTREC Ciphers List can be selected, the organization uses it to encrypt information (data) to the appropriate strength and stores the information. - The organization considers the level of security and trustworthiness required for the information, chooses an algorithm, and encrypts and stores high importance information handled by industrial control systems with appropriate strength without causing unacceptable impact on performance. [Reference] Regarding encryption technologies whose security and implementation performance are confirmed, "Cryptography Research and Evaluation Committees （CRYPTREC）" releases to the public the list of such technologies recommended for use that are sufficiently used in the market or are considered to spread in the future. It is desirable that the organization should refer to the list as needed when procuring systems that should implement encryption functions.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	･SC-10 Network Disconnect	CPS.CM-6	As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other “organization”, people, components, and systems.	Advanced	- It is desirable that the organization should update the list of information about its assets and configurations when it installs or deletes new assets or when it updates its system. - The information system ensures that each external communications service is provided via a controlled interface (e.g., a gateway, router, and firewall). - The organization establishes a communications control policy for each controlled interface (e.g., a gateway, router, and firewall). - The system on a controlled interface rejects network communication by default and permits it as an exception. - The information system and the industrial control system terminate the network connection after a session ends, or when a session remains inactive for a certain length of time. - The organization monitors communication on controlled interfaces in order to detect any communication to unapproved items or systems, or communication that conveys an inappropriate content.
	3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	･SC-12 Cryptographic Key Establishment and Management	CPS.DS-5	Securely control encryption keys throughout their life cycle to ensure proper operation and securely transmitted, received and stored data.	Advanced	- It is desirable that the organization should set out a policy and procedure regarding the following items to take immediate and appropriate measures when the private key is imperiled. - A structure to take measures against imperilment of the private key (including the stakeholders, roles, cooperation with contractors) - Criteria to judge whether the private key is imperiled or is in danger of imperilment - To investigate the cause of imperilment of the private key, and to attempt to remove the cause - Suspension of the services using the key - To create a new pair of keys and issue a certificate for the new key - Disclosure of information regarding imperilment of the private key (Notified parties, a method of notification, disclosure policy, etc.) [Reference] It is desirable to refer to the group of standards of ISO/IEC 11770, NIST SP 800-57 Part 1 Rev.4, and so on for the details about key management.
						Basic	- It is desirable that the organization should protect all encryption keys from modification and loss.
	3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	･SC-13 Cryptographic Protection	CPS.DS-2	Encrypt information with an appropriate level of security strength, and store them.	H-Advanced	- The organization selects products that have been authenticated based on Cryptographic Module Validation Program (CMVP) in order to suitably implement selected algorithms to software and hardware, and to protect keys, identification codes, and entity authentication information that is used to decrypt encrypted information or to grant electronic signatures. - The organization protects are encrypts data to the appropriate strength when that data is taken outside of the organization. - The organization uses IoT devices that can encrypt and store data in internal memory.
						Advanced	- The organization examines safety and trustworthiness that are necessary, selects an algorithm, encrypts information (data) to the appropriate strength, and stores the information. If an algorithm on the CRYPTREC Ciphers List can be selected, the organization uses it to encrypt information (data) to the appropriate strength and stores the information. - The organization considers the level of security and trustworthiness required for the information, chooses an algorithm, and encrypts and stores high importance information handled by industrial control systems with appropriate strength without causing unacceptable impact on performance. [Reference] Regarding encryption technologies whose security and implementation performance are confirmed, “Cryptography Research and Evaluation Committees （CRYPTREC）” releases to the public the list of such technologies recommended for use that are sufficiently used in the market or are considered to spread in the future. It is desirable that the organization should refer to the list as needed when procuring systems that should implement encryption functions.
	3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	･SC-15 Collaborative Computing Devices	CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).	H-Advanced	- The information system and the industrial control system automatically monitor or regulate remote access to its system. - The information system and the industrial control system allow only for remote access routed by the regulated access points. - The information system allows privileged command via remote access only for those purposes based on specified requirements. - The information system records reasons why the users accessing the system which handles highly confidential data execute privileged commands and access security information by remote access. - The information system protects wireless access to the system which handles highly confidential data by using user and device authentication in addition to encryption. - The information system blocks remote activation of devices such as white boards, cameras, and microphones connected via networks which may handle highly confidential data. Signs of the devices in use are provided to the users of these devices.
	3.13.13	Control and monitor the use of mobile code	･SC-18 Mobile Code	CPS.CM-1	Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.	H-Advanced	- The information system routes communications to the network to which a recipient’s IP address belongs via a proxy server authenticated on a controlled interface. - The information system and the industrial control system monitor and control the use of mobile code. - The information system monitors and controls the use of protocols used for audio and video transmission (e.g. VoIP).
	3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	･SC-19 Voice over Internet Protocol				
	3.13.15	Protect the authenticity of communications sessions.	･SC-23 Session Authenticity	CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).	H-Advanced	- The information system and the industrial control system automatically monitor or regulate remote access to its system. - The information system and the industrial control system allow only for remote access routed by the regulated access points. - The information system allows privileged command via remote access only for those purposes based on specified requirements. - The information system records reasons why the users accessing the system which handles highly confidential data execute privileged commands and access security information by remote access. - The information system protects wireless access to the system which handles highly confidential data by using user and device authentication in addition to encryption. - The information system blocks remote activation of devices such as white boards, cameras, and microphones connected via networks which may handle highly confidential data. Signs of the devices in use are provided to the users of these devices.
				CPS.DS-3	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.	H-Advanced	- The organization protects th networks composing the information system and industrial control system that handles important data by implementing encrytion of communication channels or by alternative physical measures.
						Advanced	- The information system employs an cryptographic mechanism and encrypt communciation paths. [Reference] For encryption of communication paths, there are several methods such as IP-VPN, Ipsec-VPN, SSL VPN. It is desirable that the organization should select the method considering the importance of the data transmitted in the communication paths, the budget, and so on.
	3.13.16	Protect the confidentiality of CUI at rest.	･SC-28 Protection of Information at Rest	CPS.DS-2	Encrypt information with an appropriate level of security strength, and store them.	H-Advanced	- The organization selects products that have been authenticated based on Cryptographic Module Validation Program (CMVP) in order to suitably implement selected algorithms to software and hardware, and to protect keys, identification codes, and entity authentication information that is used to decrypt encrypted information or to grant electronic signatures. - The organization protects are encrypts data to the appropriate strength when that data is taken outside of the organization. - The organization uses IoT devices that can encrypt and store data in internal memory.
						Advanced	- The organization examines safety and trustworthiness that are necessary, selects an algorithm, encrypts information (data) to the appropriate strength, and stores the information. If an algorithm on the CRYPTREC Ciphers List can be selected, the organization uses it to encrypt information (data) to the appropriate strength and stores the information. - The organization considers the level of security and trustworthiness required for the information, chooses an algorithm, and encrypts and stores high importance information handled by industrial control systems with appropriate strength without causing unacceptable impact on performance. [Reference] Regarding encryption technologies whose security and implementation performance are confirmed, “Cryptography Research and Evaluation Committees （CRYPTREC）” releases to the public the list of such technologies recommended for use that are sufficiently used in the market or are considered to spread in the future. It is desirable that the organization should refer to the list as needed when procuring systems that should implement encryption functions.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
SYSTEM AND INFORMATION INTEGRITY	3.14.1	Identify, report, and correct information and system flaws in a timely manner.	・SI-2 Flaw Remediation ・SI-3 Malicious Code Protection ・SI-5 Security Alerts, Advisories, and Directives	CPS.AE-1	Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.	H-Advanced	- The organization uses a mechanism for automatically collecting information about network configurations and the software configurations of devices in order to monitor the most recent status at all times. - The information system forces the application of users' access rights approved (by the administrator) in order to control data flows within a system (and between interconnected systems). - The organization physically or logically separates a network of industrial control systems with high importance from a network of industrial control systems with lower importance. - The organization/system analyzes the regular patterns of its systems' communication status and security alerts to create and use a profile that summarizes typical patterns of communication and security alerts, thereby enabling the detection of unknown threats and suspicious behavior (communication).
	3.14.2	Provide protection from malicious code at appropriate locations within organizational systems.	・SI-2 Flaw Remediation ・SI-3 Malicious Code Protection ・SI-5 Security Alerts, Advisories, and Directives	CPS.CM-3	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.	H-Advanced	- IoT devices, or systems that contain these devices, examine information output from software programs or applications to see if it matches the expected content in order to prepare for certain attacks that may have a consequence different to a normally expected outcome (e.g., command injection). - The information system automatically updates the logic to detect malicious code through an IDS/IPS. - The information system detects exploit codes that attacks unknown vulnerabilities by installing on endpoints (especially, IoT devices and servers with various functions) detection/restoration software using technologies of behavioral detection of malware. - The information system executes real-time scanning of files from external sources.
						Advanced	- The information system blocks or isolates any malicious code for it detected through an IDS/IPS, or notifies the administrator of the code. - The information system detects exploit codes by installing on endpoints (IoT devices, servers, and so on) detection/restoration software using technologies of pattern matching of malware. - The organization considers implementing whitelist-type malware protection for IoT devices with limited functions. * Especially regarding IoT devices and control devices, OS to which anti-malware software can be applied may not be used. It is desirable for the organization to confirm whether devices to be introduced are compatible with anti-malware software at the phase of procurement and to select compatible ones. If it is difficult to procure devices compatible with anti-malware software, it is desirable to take alternative measures such as introducing/strengthening a malware detection mechanism on a network.
	3.14.3	Monitor system security alerts and advisories and take appropriate actions in response.	・SI-2 Flaw Remediation ・SI-3 Malicious Code Protection ・SI-5 Security Alerts, Advisories, and Directives	CPS.IP-10	Develop a vulnerability remediation plan, and modify the vulnerability of the components according to the plan.	Advanced	- The organization defines tolerable risk by identifying through investigations and tests the impacts of patch application on the functions of other software applications and services on operations of IoT devices and servers. - The organization conducts tests to measure the effectiveness of corrections and the possibility of any secondary adverse effects, corrects the defects, and manages the corrections as part of the configuration management.
				CPS.CM-3	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.	H-Advanced	- IoT devices, or systems that contain these devices, examine information output from software programs or applications to see if it matches the expected content in order to prepare for certain attacks that may have a consequence different to a normally expected outcome (e.g., command injection). - The information system automatically updates the logic to detect malicious code through an IDS/IPS. - The information system detects exploit codes that attacks unknown vulnerabilities by installing on endpoints (especially, IoT devices and servers with various functions) detection/restoration software using technologies of behavioral detection of malware. - The information system executes real-time scanning of files from external sources.
						Advanced	- The information system blocks or isolates any malicious code for it detected through an IDS/IPS, or notifies the administrator of the code. - The information system detects exploit codes by installing on endpoints (IoT devices, servers, and so on) detection/restoration software using technologies of pattern matching of malware. - The organization considers implementing whitelist-type malware protection for IoT devices with limited functions. * Especially regarding IoT devices and control devices, OS to which anti-malware software can be applied may not be used. It is desirable for the organization to confirm whether devices to be introduced are compatible with anti-malware software at the phase of procurement and to select compatible ones. If it is difficult to procure devices compatible with anti-malware software, it is desirable to take alternative measures such as introducing/strengthening a malware detection mechanism on a network.
	3.14.4	Update malicious code protection mechanisms when new releases are available.	・SI-3 Malicious Code Protection	CPS.IP-8	Share information regarding the effectiveness of data protection technologies with appropriate partners.	H-Advanced	- The organization prepares a setting through an automated mechanism at just the right time that enables it and its appropriate partners to interactively share new information about data protection technologies or information about the effectiveness of the protection technologies.
						Advanced	- The organization prepares a setting that enables it to share new information about data protection technologies or information about the effectiveness of the protection technologies with its partners at just the right time.
				CPS.AE-3	Identify the security events accurately by implementing the procedure to conduct a correlation analysis of the security events and comparative analysis with the threat information obtained from outside the organization.	H-Advanced	- The organization conducts a trend analysis examining the latest information about threats, vulnerability, and assessments of security management measures carried out several times in order to determine whether the activities for continuous monitoring need any correction. - The organization carries out policy tuning (management of signatures to apply) and maintenance for devices such as IDS, IPS, and SIEM on its own. - The organization creates custom signatures used for sensors on its own. - In order to properly detect security events that are likely to adversely affect the organization, the organization collects and analyzes logs of edge devices such as IoT devices in addition to the logs of devices presented in <Advanced>, if possible.
				CPS.CM-3	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.	H-Advanced	- IoT devices, or systems that contain these devices, examine information output from software programs or applications to see if it matches the expected content in order to prepare for certain attacks that may have a consequence different to a normally expected outcome (e.g., command injection). - The information system automatically updates the logic to detect malicious code through an IDS/IPS. - The information system detects exploit codes that attacks unknown vulnerabilities by installing on endpoints (especially, IoT devices and servers with various functions) detection/restoration software using technologies of behavioral detection of malware. - The information system executes real-time scanning of files from external sources.
	3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	・SI-3 Malicious Code Protection	CPS.CM-3	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.	H-Advanced	- IoT devices, or systems that contain these devices, examine information output from software programs or applications to see if it matches the expected content in order to prepare for certain attacks that may have a consequence different to a normally expected outcome (e.g., command injection). - The information system automatically updates the logic to detect malicious code through an IDS/IPS. - The information system detects exploit codes that attacks unknown vulnerabilities by installing on endpoints (especially, IoT devices and servers with various functions) detection/restoration software using technologies of behavioral detection of malware. - The information system executes real-time scanning of files from external sources.
				CPS.CM-4	Validate the integrity and authenticity of the information provided from cyberspace before operations.	H-Advanced	- The organization introduces the concept of "whitelisting" for data entry in order to specify known items and systems considered trustworthy as the sources of input data, and the format allowed for the input data. - IoT devices and servers begin communication with other IoT devices only after the devices are mutually authenticated successfully so that the source of data is always clear. - The information system and the industrial control system protect the authenticity of communications sessions.
						Advanced	- The information system uses an integrity verification tool to detect any unauthorized changes that are made to communications data transmitted from IoT devices and servers. - IoT devices and servers that are acknowledged as critical to the organization's operations begin communication with other IoT devices only after the devices are mutually authenticated successfully so that the source of data is always clear.

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	・SI-4 System Monitoring ・SI-4(4) System Monitoring Inbound and Outbound Communications Traffic	CPS.DS-9	Properly control outbound communications that send information to be protected to prevent improper data breach.	H-Advanced	- The industrial control system shuts down, isolates the malicious code or notifies the administrator when detecting such code through IDS/IPS. - The organization/system analyzes the regular patterns of its systems' communication status and security alerts to create and use a profile that summarizes typical patterns of communication and security alerts, thereby enabling the detection of unknown threats and suspicious behavior (communication). - The information system prevents fraudulent and unexpected transfer of information via common system resources.
						Advanced	- The information system blocks or isolates any malicious code for it detected through an IDS/IPS, or notifies the administrator of the code. - The organization collects information including newly released attacking trends, malware behaviors, and malicious IP addresses/domains (external intelligence). When necessary, the organization excutes responces to restrict communications to highly dangerous IP addresses or domains or so.
				CPS.AE-1	Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.	H-Advanced	- The organization uses a mechanism for automatically collecting information about network configurations and the software configurations of devices in order to monitor the most recent status at all times. - The information system forces the application of users' access rights approved (by the administrator) in order to control data flows within a system (and between interconnected systems). - The organization physically or logically separates a network of industrial control systems with high importance from a network of industrial control systems with lower importance. - The organization/system analyzes the regular patterns of its systems' communication status and security alerts to create and use a profile that summarizes typical patterns of communication and security alerts, thereby enabling the detection of unknown threats and suspicious behavior (communication).
				CPS.AE-2	Appoint a chief security officer, establish a security management team (SOC/CSIRT), and prepare a system within the organization to detect, analyze, and respond to security events.	Advanced	- The organization refers to risk assessment results and, considering the following angles, establishes what to monitor and what to include in correlation analysis. - The scope of systems to monitor - Which device logs should be collected for analysis (see CPS.AE-3) - The organization regularly reviews audit logs collected through monitoring. - The organization continues to collect and manage information about assets, device configurations, and network configurations in order to evaluate its security status. - The organization examines the results of correlation analysis and other data to accurately detect security events that must be addressed and take action in accordance with the security operation process. See CPS.RP-1 for details of the process. - The organization regularly reports the state of organizational and system security to the chief security officer or other appropriate staff members. It is desirable that the regular report should include the following shown below: - Results of log analysis (e.g., the number of incidents handled; summaries of typical incidents that have been handled; threats that have emerged; issues in monitoring); - Policy for future improvements in monitoring.
				CPS.CM-5	Monitor communication with external service providers so that potential security events can be detected properly.	Advanced	- The organization documents its security requirements for the staff from its external service provider and system developer, and includes the requirements in the agreement. - The organization requires its external service provider and system developer to contact it when any of its staff members who have authorizations for its system are transferred or when their employment terminates. - It is desirable that the organization should manage changes to services offered by its external service provider, taking account of relevant information about operations, the importance of its business systems and processes, and re-assessed risks. - The organization monitors whether its external service provider and system developer complies with the requirements. - The organization monitors access to its system by its external service provider and system developer in order to detect any unauthorized access by these external businesses that results from an action or failure to act. - The organization reports the results of the monitoring of activities by its external service provider and system developer to the appropriate system administrator.
				CPS.CM-6	As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	Advanced	- It is desirable that the organization should update the list of information about its assets and configurations when it installs or deletes new assets or when it updates its system. - The information system ensures that each external communications service is provided via a controlled interface (e.g., a gateway, router, and firewall). - The organization establishes a communications control policy for each controlled interface (e.g., a gateway, router, and firewall). - The system on a controlled interface rejects network communication by default and permits it as an exception. - The information system and the industrial control system terminate the network connection after a session ends, or when a session remains inactive for a certain length of time. - The organization monitors communication on controlled interfaces in order to detect any communication to unapproved items or systems, or communication that conveys an inappropriate content.
				CPS.DP-4	Continuously improve the process of detecting security events.	Advanced	- The organization prepares and manages a procedure for regularly reporting the state of organizational and system security to its appropriate staff members (e.g., management). It is desirable that the organization should define the reporting as an occasion for becoming aware of the latest threats or threats to remaining risks so that the organization acts to enhance its security. - For example, if alerts such as those shown below are issued and there is a sign of increasing security risks, raise the level of the system's monitoring activities based on information from reliable sources. * The list below is an excerpt from "Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT Version 1.0" (ISOG-J, 2018). ・Characteristics of the attack ➢ Form of the attack; contents of relevant communications ➢ Core attack code ・Traces of the attack ➢ Contents of the damaged communications ➢ Logs that remain in the server or the hands of clients ➢ Other characteristics that remain in the server or the hands of clients ・Detected names in the security products

NIST SP 800-171			NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework			
FAMILY	ID	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	3.14.7	Identify unauthorized use of organizational systems.	・SI-4 System Monitoring	CPS.DS-9	Properly control outbound communications that send information to be protected to prevent improper data breach.	H-Advanced	- The industrial control system shuts down, isolates the malicious code or notifies the administrator when detecting such code through IDS/IPS. - The organization/system analyzes the regular patterns of its systems' communication status and security alerts to create and use a profile that summarizes typical patterns of communication and security alerts, thereby enabling the detection of unknown threats and suspicious behavior (communication). - The information system prevents fraudulent and unexpected transfer of information via common system resources.
						Advanced	- The information system blocks or isolates any malicious code for it detected through an IDS/IPS, or notifies the administrator of the code. - The organization collects information including newly released attacking trends, malware behaviors, and malicious IP addresses/domains (external intelligence). When necessary, the organization excutes responces to restrict communications to highly dangerous IP addresses or domains or so.
				CPS.AE-1	Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.	H-Advanced	- The organization uses a mechanism for automatically collecting information about network configurations and the software configurations of devices in order to monitor the most recent status at all times. - The information system forces the application of users' access rights approved (by the administrator) in order to control data flows within a system (and between interconnected systems). - The organization physically or logically separates a network of industrial control systems with high importance from a network of industrial control systems with lower importance. - The organization/system analyzes the regular patterns of its systems' communication status and security alerts to create and use a profile that summarizes typical patterns of communication and security alerts, thereby enabling the detection of unknown threats and suspicious behavior (communication).
				CPS.AE-2	Appoint a chief security officer, establish a security management team (SOC/CSIRT), and prepare a system within the organization to detect, analyze, and respond to security events.	Advanced	- The organization refers to risk assessment results and, considering the following angles, establishes what to monitor and what to include in correlation analysis. - The scope of systems to monitor - Which device logs should be collected for analysis (see CPS.AE-3) - The organization regularly reviews audit logs collected through monitoring. - The organization continues to collect and manage information about assets, device configurations, and network configurations in order to evaluate its security status. - The organization examines the results of correlation analysis and other data to accurately detect security events that must be addressed and take action in accordance with the security operation process. See CPS.RP-1 for details of the process. - The organization regularly reports the state of organizational and system security to the chief security officer or other appropriate staff members. It is desirable that the regular report should include the following shown below: - Results of log analysis (e.g., the number of incidents handled; summaries of typical incidents that have been handled; threats that have emerged; issues in monitoring); - Policy for future improvements in monitoring.
				CPS.CM-5	Monitor communication with external service providers so that potential security events can be detected properly.	Advanced	- The organization documents its security requirements for the staff from its external service provider and system developer, and includes the requirements in the agreement. - The organization requires its external service provider and system developer to contact it when any of its staff members who have authorizations for its system are transferred or when their employment terminates. - It is desirable that the organization should manage changes to services offered by its external service provider, taking account of relevant information about operations, the importance of its business systems and processes, and re-assessed risks. - The organization monitors whether its external service provider and system developer complies with the requirements. - The organization monitors access to its system by its external service provider and system developer in order to detect any unauthorized access by these external businesses that results from an action or failure to act. - The organization reports the results of the monitoring of activities by its external service provider and system developer to the appropriate system administrator.
				CPS.CM-6	As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.	Advanced	- It is desirable that the organization should update the list of information about its assets and configurations when it installs or deletes new assets or when it updates its system. - The information system ensures that each external communications service is provided via a controlled interface (e.g., a gateway, router, and firewall). - The organization establishes a communications control policy for each controlled interface (e.g., a gateway, router, and firewall). - The system on a controlled interface rejects network communication by default and permits it as an exception. - The information system and the industrial control system terminate the network connection after a session ends, or when a session remains inactive for a certain length of time. - The organization monitors communication on controlled interfaces in order to detect any communication to unapproved items or systems, or communication that conveys an inappropriate content.
				CPS.DP-4	Continuously improve the process of detecting security events.	Advanced	- The organization prepares and manages a procedure for regularly reporting the state of organizational and system security to its appropriate staff members (e.g., management). It is desirable that the organization should define the reporting as an occasion for becoming aware of the latest threats or threats to remaining risks so that the organization acts to enhance its security. - For example, if alerts such as those shown below are issued and there is a sign of increasing security risks, raise the level of the system's monitoring activities based on information from reliable sources. * The list below is an excerpt from "Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT Version 1.0" (ISOG-J, 2018). ・Characteristics of the attack ➢ Form of the attack; contents of relevant communications ➢ Core attack code ・Traces of the attack ➢ Contents of the damaged communications ➢ Logs that remain in the server or the hands of clients ➢ Other characteristics that remain in the server or the hands of clients ・Detected names in the security products

D.3 Mapping ISO/IEC 27001 controls to Cyber/Physical Security Framework

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
A.5 Information security policies	A.5.1 Management direction for information security	A.5.1.1 Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	CPS.BE-2	Define policies and standard measures regarding security that are consistent with the high-priority business and operations of the organization, and share them with parties relevant to the organization's business (including suppliers and third-party providers).	Advanced	- The organization defines its missions and business processes and gives priorities to actions, in consideration of risks to its business, its assets, persons, other organizations, etc. - The organization informs other organizations of their roles and responsibilities specified in its security policies.
				CPS.GV-1	Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.	Advanced	- The organization formulates a series of lower level security policies, such as the policies and implementation procedures of the following individual topics, to support policies at a higher level. a) Access control and authentication b) Physical security measures c) System development and maintenance d) Management of external contractors e) Classification and handling of information - The organization formulates a series of security policies by fully considering the organization's a) business strategies, b) related rules, laws, regulations, and contracts, and c) environments under threats to security to sufficiently reflect the actual situation of the organization. - The organization reviews and updates a security plan according to changes in its a) business strategies, b) related rules, laws, regulations, and contracts, and c) environments under threats to security. [Reference] To formulate a policy at a more detailed level, refer to related standards such as ISO/IEC 27002 for identification of fields which require the policy, and refer to more detailed guidelines.
						Basic	- The organization formulates a basic security policy at the highest level of its series of security policies, obtains an approval of the management, and operates it appropriately. - The organization reviews and updates the security policy periodically (e.g., once a year).
		A.5.1.2 Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	CPS.RA-6	- On the basis of the results of the risk assessment, clearly define the details of measures to prevent possible security risks, and document the organized outcome from the scope and priorities of the measures. - React accordingly to the security risks and the associated safety risks identified as a result of the assessment conducted at the planning and design phase of an IoT device and systems incorporating IoT devices.	H-Advanced	- On the basis of the results of the hazard analysis performed in CPS.RA-4, mainly for the industrial control system, the organization appropriately treats the source of a risk which may lead to a critical hazard as necessary. [Reference] Security integration in safety control has been particularly discussed in recent years in terms of international standardization, and IEC TR 63074, IEC TR 63069, etc., are available for reference.
						Advanced	- The organization securely stores the documented information on security risk management processes. - When the organization selects a measure according to the risk assessment results, it is desirable that the organization documents the measure to be taken and the reason why the measure is adopted. - When applying the measure, the organization formulates a security risk management plan and obtains an approval from the risk owner. - The organization reviews the security risk handling plan and checks that the applicable plan conforms to the priority order of the entire organization's risk management strategy. - The organization informs applicable external business operators regarding security measures necessary for a new system including an IoT device which are extracted in CPS.RA-4 as required specifications. - The organization verifies whether the security measures defined in the required specifications and contracts are implemented at the time of deployment of the systems including an IoT device via User Acceptance Test (UAT). If there is anything unclear, confirm with the external business operator.
						Basic	- The organization considers the risk assessment results and selects handling measures to identified risks. - The organization formulates a security risk treatment implementation plan. - The organization obtain an approval from the risk owner for acceptance of the security risk.
A.6 Organization of information security	A.6.1 Internal organization	A.6.1.1 Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	CPS.AM-5	Create and manage appropriately a list of external information systems where the organization's assets are shared.	H-Advanced	- The system makes a list of external information services in use and manages the users, devices as well as serviced in use in real time. - The system uses a mechanism to give notice to the system administrator when an unpermitted external information system service is detected. - The organization identifies functions, ports, protocols, and other services which are necessary for using services offered by external providers.
						Advanced	- The organization sets conditions for allowing other organizations which own or operate external information systems to do the following: a. Accessing an information system in the organization from an external information system b. Processing, saving, or transmitting information under the control of the organization using an external information system - The organization restricts a use of storage in an external system the organization owns to an authorized one.
						Basic	- The organization makes a list of external information system services in use and defines roles and responsibilities as users in each service. [Reference] Appendix A "Concret examples of contract provisions and commentaries" of "Guidebook for using Cloud Security Guideline" (METI, 2013) could be referred to regarding the points to consider when stipulating in the contract the roles and responsibilities of users especially in terms of usage of cloud service.
				CPS.AM-6	Classify and prioritize resources (e.g., People, Components, Data, and System) by function, importance, and business value, and communicate to the organizations and people relevant to those resources in business.	Advanced	- The organization considers business requirements and legal requirements which share or restrict data when classifying resources of the information system and industrial control system (data, components processing data, system, etc). - The person responsible for an asset is responsible for the classification of the data. - The organization includes classification rules and classification review standards after time passes in a resource classification system.
						Basic	- The organization sets priorities on identified information assets according to importance to the organization. - When related laws or regulations require us to follow a certain classification for resources of the organization (e.g., system and data), apply an appropriate classification to the asset.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.AM-7	Define roles and responsibilities for cyber security across the organization and other relevant parties.	Advanced	- In preparation for damages caused by security incidents, the organization considers risk transfer by using cyber insurance, etc., in addition to implementing security measures designated by business partners.
						Basic	- In a contract with a contractor or an outsourcer, the organization specifies the scope of the responsibilities of the organization and that of the business partner (state the disclaimer and an upper limit on agreed compensation for damages) in case of a damage caused by a security incident in the business. - To increase the effectiveness of the requirements related to security which a business partner requires or is required to satisfy in a contract, it is desirable that the organization makes an agreement in meeting the requirements, identifying deficiencies and details of actions, paying expenses, and using an alternative when they cannot be satisfied at the time of the contract or in the early stage of the contract.
				CPS.DP-1	Clarify the role and responsibility of the organization as well as service providers in detecting security events so that they can fulfill their accountabilities.	Basic	- The organization determines the log information that would help detect security events and thus should be collected based on its strategies relating to risk management and assessment results. - The organization ascertains that its business partner (service provider) has an audit log that records activity of service users, exception handling, and security events that the provider has acquired. - The organization ascertains that the audit log acquired by its service provider records activity of service users, exception handling, and security events, and is protected in a proper way.
		A.6.1.2 Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	CPS.AC-5	Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions)	H-Advanced	- The organization specifies administrators who use the security functions (e.g., access authority setting) and regulates privileged accounts in its system. - The information system adopts a system monitoring mechanism to check the use of privileged functions. - The information system prohibits non-privileged users from executing privileged functions on the system by invalidating, avoiding, and changing security measures that are changed and implemented by non-privileged users. - The organization can minimize the number of users who can use the system administrator's authority in an emergency to minimize the damage caused by the security incident. - The organization can prevent even system administrators from stopping critical services and protected processes through the server to minimize the damage caused by security incidents.
						Advanced	- The organization implements access control in the information system and the industrial control system based on separation of duties (e.g., user / system administrator). - The organization adopts a general rule on the minimum authority of specific duties. - Segregate authority of general user from that of administrator. (Require users to use the system with a non-privileged account when using a non-security function.) - Minimize authority for duties not in charge. - The organization separates and stipulates duties that are assigned by the person in charge.
		A.6.1.3 Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	CPS.GV-2	Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.	Basic	- Within the organization's business activities, clearly identify all related laws, regulations, and contractual requirements in the context of security as well as the organization's effort to fulfill these requirements, document them, and maintain those documents at their latest. - The organization defines and documents detailed management measures and details of responsibilities to satisfy the requirements. - The controller identifies all laws and regulations which are applied to each organization to satisfy requirements related to the type of business. - When the organization operates businesses in other countries, the controller considers to comply with the laws and regulations in all related countries.
		A.6.1.4 Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	CPS.RA-2	The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.), analyzes the information, and establishes a process to implement and use measures.	H-Advanced	- The organization establishes a security measure organization managing comprehensively the systems including industrial control systems, IoT systems, etc., and takes security measures integrally within the organization. - The person in charge of security updates knowledge about security in both an information system and industrial control system to the latest by attending workshops and meetings related to security and by maintaining an appropriate communication structure with security professional associations/institutions. - Mainly analyze the products/services that the company offers to check if any new vulnerability is contained, and if detected, submit related information to IPA.
						Advanced	- The organization, with a chief security officer at the center, establishes a security management team mainly for information systems and IoT systems with high business importance, and prepares a structure for handling security measures within the organization. - The organization collects information on vulnerabilities, threats, etc., from organizations, including the Information-technology Promotion Agency (IPA), JPCERT/CC, industry ISAC, and business partners (device vendors and software vendors), and determines the necessity of actions by comparing to the organization's asset list.
				CPS.RA-3	Identify and document the assumed security incidents, those impacts on the oraganization's assets, and the causes of those.	H-Advanced	- The organization updates security knowledge to the latest by attending workshops and meetings related to security and by maintaining an appropriate communication structure with security professional associations/institutions. - As necessary, the organization utilizes services provided by experts, obtains information that only some experts can know, and uses them to identify threats.
				CPS.AE-4	Identify the impact of security events, including the impact on other relevant organizations.	Advanced	- The organization works with IPA, JPCERT/CC, the industry's ISAC, and a security vendor to collect information, thereby interlinking and sharing information about threats and vulnerability to obtain a whole picture of the security event. - The organization requests an external security vendor to analyze the functions of the malware, or program, or script placed by an attacker if any is found in a security event that has occurred.
				CPS.AN-1	Understand the impact of the security incident on the whole society including the organization and relevant parties such as partners based on the full account of the incident and the probable intent of the attacker.	Advanced	- The organization works with IPA, JPCERT/CC, the industry's ISAC, and a security vendor to collect information, thereby interlinking and sharing information about threats and vulnerability to obtain a whole picture of the security incident. - The organization requests an external security vendor to analyze the functions of the malware, or program, or script placed by an attacker if any is found in a security incident that has occurred.
		A.6.1.5 Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	CPS.IP-3	Introduce the system development life cycle to manage the systems.	H-Advanced	- The organization explicitly presents the following requirements when procuring the system; - Requirements for security functions; - Requirements for security strength; - Requirements for security warranty; - Requirements for security-related documents; - Requirements for protection of security-related documents; - Description on the development environment of the system and the environment which the system is planned to operate under; - Acceptance criteria
						Advanced	- The organization manages the system in accordance with the system development lifecycle, which includes items of consideration regarding information security, and undergoes an information security risk management process throughout the entire system development lifecycle.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	A.6.2 Mobile devices and teleworking	A.6.2.1 Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	H-Advanced	-The organization identifies assets constituting its information systems and industrial control systems (hardware, including IoT devices; software; and information) uniquely, assigns a responsible person to each asset. And the organization maintains/manages lists periodically, or at the request of the operator including configuration information of assets (e.g., names, version information, license information, and location) while recognizing situations in real time. - The information system regularly audits whether the actual configuration grasped conforms to the baseline configuration defined by the organization, and responds appropriately. (Example: blocking unplanned connections except those permitted by the organization as an exception) -The information system and industrial control system implement and operate a mechanism which automatically detects and responses to unauthorized assets.
						Advanced	- Maintain/manage lists including configuration information of assets (e.g., names, version information, license information, and location) by reviewing and updating them periodically. - The organization makes a list of removable media (e.g., USB memory sticks) that can be used on system components (information system or industrial control system), and manages the use of them. - The organization uses only removable media (e.g. USB memory) permitted in the organization. Also, if there is no identifiable ownwer of portable storage devices, the organization prohibits the use of such devices. - The organization controles access to the media that contain highly confidential data, and properly grasps and manages the usage of the media taken outside of the controlled areas.
						Basic	- The organization identifies assets constituting its information system and industrial control system (hardware, software and information), assigns a responsible person to each asset, and documents a list of them. - It is desirable to list all the assets held, but if the target is huge, consider narrowing down the target assets through integration (grouping) of the analysis target and exclusion from the analysis target. - The organization sets priorities to the identified assets based on the importance of them in its business operation.
				CPS.AM-5	Create and manage appropriately a list of external information systems where the organization's assets are shared.	H-Advanced	- The system makes a list of external information services in use and manages the users, devices as well as serviced in use in real time. - The system uses a mechanism to give notice to the system administrator when an unpermitted external information system service is detected. - The organization identifies functions, ports, protocols, and other services which are necessary for using services offered by external providers.
						Advanced	- The organization sets conditions for allowing other organizations which own or operate external information systems to do the following: a. Accessing an information system in the organization from an external information system b. Processing, saving, or transmitting information under the control of the organization using an external information system - The organization restricts a use of storage in an external system the organization owns to an authorized one.
				CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).	Advanced	- The organization regulates the mobile devices used in the organization and establishes setting requirements, connection requirements, and implementation guidelines for mobile devices. - The organization establishes rules of approval for connecting mobile devices used in the organization to its system.
				CPS.IP-2	Restrict the software to be added after installing in the IoT devices and servers.	H-Advanced	- The organization restricts software by using a list of software that is permitted to be executed on the information system and industrial control system (whitelist) or list of prohibited software (blacklist). Or, unpermitted software shall not be installed.
						Advanced	- The organization adopts and manages a mechanism that manages software installation that is performed by users on the organization's system (information system or industrial control system) and monitors the events.
						Basic	- The organization establishes a policy on software installation performed by users on the organization's system (information system or industrial control system) and has the users follow it.
				CPS.CM-2	Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.	Advanced	- The organization reviews the relevant audit log regularly or when an incident or a sign of an incident appears if a physical access log from access control is available while 24-h monitoring is not conducted through security cameras or by any other means. - A person in charge accompanies a visitor into the area where the organization's assets that must be protected are directly accessible (e.g., an office) in order to monitor the visitor's behavior. - The organization monitors through security cameras or by other means physical access to its facilities that are vital for its operations and house IoT devices and servers, thereby enabling early detection of any physical security incidents and immediate action. - If the above physical security measures may be difficult to implement for items such as IoT devices and servers that may be critical to the organization's operation because they are in a remote location or for any other reasons, consider using tamper-resistant equipment (CPS.DS-6) or taking any other appropriate measures to enhance the physical security properties of the equipment itself.
						Basic	- If the organization is unable to control access to, or provide video surveillance service for, the areas that should allow only limited physical access because of issues of costs and other reasons, it takes alternative manual measures, such as that its employee in charge accompany a visitor on the premises. - The organization implements physical security measures to control access to designated areas in the facility that do not be allowed for the general public to access. - The organization verifies the access authority of the personnel before permitting the physical access and collects and manages the records of entry and exit.
				CPS.CM-3	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.	Advanced	- The information system blocks or isolates any malicious code for it detected through an IDS/IPS, or notifies the administrator of the code. - The information system detects exploit codes by installing on endpoints (IoT devices, servers, and so on) detection/restoration software using technologies of pattern matching of malware. - The organization considers implementing whitelist-type malware protection for IoT devices with limited functions. * Especially regarding IoT devices and control devices, OS to which anti-malware software can be applied may not be used. It is desirable for the organization to confirm whether devices to be introduced are compatible with anti-malware software at the phase of procurement and to select compatible ones. If it is difficult to procure devices compatible with anti-malware software, it is desirable to take alternative measures such as introducing/strengthening a malware detection mechanism on a network.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
		A.6.2.2 Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).	Advanced	- The organization regulates the mobile devices used in the organization and establishes setting requirements, connection requirements, and implementation guidelines for mobile devices. - The organization establishes rules of approval for connecting mobile devices used in the organization to its system.
						Basic	- The organization establishes usage regulations, configuration requirements, and implementation guidelines for each type of approved remote access. - The organization in principle prohibits unauthorized wireless connections. - The organization establishes rules of approval for remote access to an information system and an industrial control system. - The organization authorizes wireless access to its system in advance of the approval.
				CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.
				CPS.DS-3	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.	H-Advanced	- The organization protects th networks composing the information system and industrial control system that handles important data by implementing encrytion of communication channels or by alternative physical measures.
						Advanced	- The information system employs an cryptographic mechanism and encrypt communciation paths. [Reference] For encryption of communication paths, there are several methods such as IP-VPN, Ipsec-VPN, SSL VPN. It is desirable that the organization should select the method considering the importance of the data transmitted in the communication paths, the budget, and so on.
				CPS.CM-3	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.	Advanced	- The information system blocks or isolates any malicious code for it detected through an IDS/IPS, or notifies the administrator of the code. - The information system detects exploit codes by installing on endpoints (IoT devices, servers, and so on) detection/restoration software using technologies of pattern matching of malware. - The organization considers implementing whitelist-type malware protection for IoT devices with limited functions. * Especially regarding IoT devices and control devices, OS to which anti-malware software can be applied may not be used. It is desirable for the organization to confirm whether devices to be introduced are compatible with anti-malware software at the phase of procurement and to select compatible ones. If it is difficult to procure devices compatible with anti-malware software, it is desirable to take alternative measures such as introducing/strengthening a malware detection mechanism on a network.
A.7 Human resource security	A.7.1 Prior to employment	A.7.1.1 Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	CPS.AC-8	Restrict communications by IoT devices and servers to those with entities (e.g. people, components, system, etc.) identified through proper procedures.	Basic	- The organization assigns identifiers to its IoT devices and servers, as well as managing the identification by preventing re-use of identifiers and invalidating identifiers after a certain period of time. - Before connecting their IoT devices and servers to the network, the information system and the industrial control system prepare a mechanism that uniquely identifies and authenticate these devices. - Communication using IoT devices is denied as default. The protocol to be used is authorized as an exception.
				CPS.IP-9	Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.	Advanced	- The organization makes changes to its staff members' rights to access certain systems and/or rooms on the premises when they are reshuffled or transferred internally. - To minimize impacts when a staff member leaves the organization, designate backup members regarding important duties as a supplier including operation and maintenance. - The organization identifies conditions in which re-screening is required such as changes in access authority to their own systems, and re-screen if necessary. - The organization conducts an interview on information security when personnel leave. - The organization ensures that responsibilities for security are met, particularly of personnel handling sensitive information, throughout the whole process from hiring to retirement.
						Basic	- The organization identifies the responsibility for security of personnel in the employment contract. The organization states that this responsibility should be sustained for a reasonable period of time after the termination of employment, in order to prevent information leakage after the termination of employment. - The organization reviews a staff member before granting him or her access to its systems. - The organization conducts the following when a staff member resigns or retires: - Disables the staff member's access to its systems within a certain period; - Disables the authentication and credentials related to the staff member; - Collects all system-related things for security that the staff member has used; - Retains access to the information about the organization and information systems that have been managed by the individual who is leaving.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
		A.7.1.2 Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	CPS.IP-9	Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.	Advanced	- The organization makes changes to its staff members' rights to access certain systems and/or rooms on the premises when they are reshuffled or transferred internally. - To minimize impacts when a staff member leaves the organization, designate backup members regarding important duties as a supplier including operation and maintenance. - The organization identifies conditions in which re-screening is required such as changes in access authority to their own systems, and re-screen if necessary. - The organization conducts an interview on information security when personnel leave. - The organization ensures that responsibilities for security are met, particularly of personnel handling sensitive information, throughout the whole process from hiring to retirement.
						Basic	- The organization identifies the responsibility for security of personnel in the employment contract. The organization states that this responsibility should be sustained for a reasonable period of time after the termination of employment, in order to prevent information leakage after the termination of employment. - The organization reviews a staff member before granting him or her access to its systems. - The organization conducts the following when a staff member resigns or retires: - Disables the staff member's access to its systems within a certain period; - Disables the authentication and credentials related to the staff member; - Collects all system-related things for security that the staff member has used; - Retains access to the information about the organization and information systems that have been managed by the individual who is leaving.
	A.7.2 During employment	A.7.2.1 Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	CPS.AT-1	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	H-Advanced	- The organization provides security awareness trainings to all necessary personnel so that they will recognize and report signs of internal fraud.
						Advanced	- The organization regularly provides basic security awareness training to all members of staff. The organization can, for example, educate the following matters in addition to the contents explaining general matters. -Procedure to response when you receive a suspicious email -Notes on using mobile devices (e.g. Notes on connecting to a public wireless LAN) -Notes on using SNS - The organization creates a program for each role (e.g., system/software developper, purchasing personnel, system administrator, personnel in charge of security measures) to train information security personnel and to improve their skills. The program is conducted regularly on applicable personnel. - The organization regularly reviews records of security education and training.
						Basic	- The organization provides basic security awareness training to new staff, or when necessary due to changes made to the information systems and the industrial control systems which the organization uses. - The organization records and manages the contents and results of security education and training for member in the organization.
				CPS.IP-9	Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.	Advanced	- The organization makes changes to its staff members' rights to access certain systems and/or rooms on the premises when they are reshuffled or transferred internally. - To minimize impacts when a staff member leaves the organization, designate backup members regarding important duties as a supplier including operation and maintenance. - The organization identifies conditions in which re-screening is required such as changes in access authority to their own systems, and re-screen if necessary. - The organization conducts an interview on information security when personnel leave. - The organization ensures that responsibilities for security are met, particularly of personnel handling sensitive information, throughout the whole process from hiring to retirement.
						Basic	- The organization identifies the responsibility for security of personnel in the employment contract. The organization states that this responsibility should be sustained for a reasonable period of time after the termination of employment, in order to prevent information leakage after the termination of employment. - The organization reviews a staff member before granting him or her access to its systems. - The organization conducts the following when a staff member resigns or retires: - Disables the staff member's access to its systems within a certain period; - Disables the authentication and credentials related to the staff member; - Collects all system-related things for security that the staff member has used; - Retains access to the information about the organization and information systems that have been managed by the individual who is leaving.
		A.7.2.2 Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	CPS.AT-1	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.	H-Advanced	- The organization provides security awareness trainings to all necessary personnel so that they will recognize and report signs of internal fraud.
						Advanced	- The organization regularly provides basic security awareness training to all members of staff. The organization can, for example, educate the following matters in addition to the contents explaining general matters. -Procedure to response when you receive a suspicious email -Notes on using mobile devices (e.g. Notes on connecting to a public wireless LAN) -Notes on using SNS - The organization creates a program for each role (e.g., system/software developper, purchasing personnel, system administrator, personnel in charge of security measures) to train information security personnel and to improve their skills. The program is conducted regularly on applicable personnel. - The organization regularly reviews records of security education and training.
						Basic	- The organization provides basic security awareness training to new staff, or when necessary due to changes made to the information systems and the industrial control systems which the organization uses. - The organization records and manages the contents and results of security education and training for member in the organization.
		A.7.2.3 Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	CPS.IP-9	Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.	Advanced	- The organization makes changes to its staff members' rights to access certain systems and/or rooms on the premises when they are reshuffled or transferred internally. - To minimize impacts when a staff member leaves the organization, designate backup members regarding important duties as a supplier including operation and maintenance. - The organization identifies conditions in which re-screening is required such as changes in access authority to their own systems, and re-screen if necessary. - The organization conducts an interview on information security when personnel leave. - The organization ensures that responsibilities for security are met, particularly of personnel handling sensitive information, throughout the whole process from hiring to retirement.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	A.7.3 Termination and change of employment	A.7.3.1 Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	CPS.IP-9	Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.	Advanced	- The organization makes changes to its staff members' rights to access certain systems and/or rooms on the premises when they are reshuffled or transferred internally. - To minimize impacts when a staff member leaves the organization, designate backup members regarding important duties as a supplier including operation and maintenance. - The organization identifies conditions in which re-screening is required such as changes in access authority to their own systems, and re-screen if necessary. - The organization conducts an interview on information security when personnel leave. - The organization ensures that responsibilities for security are met, particularly of personnel handling sensitive information, throughout the whole process from hiring to retirement.
A.8 Asset management	A.8.1 Responsibility for assets	A.8.1.1 Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	H-Advanced	-The organization identifies assets constituting its information systems and industrial control systems (hardware, including IoT devices; software; and information) uniquely, assigns a responsible person to each asset. And the organization maintains/manages lists periodically, or at the request of the operator including configuration information of assets (e.g., names, version information, license information, and location) while recognizing situations in real time. - The information system regularly audits whether the actual configuration grasped conforms to the baseline configuration defined by the organization, and responds appropriately. (Example: blocking unplanned connections except those permitted by the organization as an exception) -The information system and industrial control system implement and operate a mechanism which automatically detects and responses to unauthorized assets.
						Advanced	- Maintain/manage lists including configuration information of assets (e.g., names, version information, license information, and location) by reviewing and updating them periodically. - The organization makes a list of removable media (e.g., USB memory sticks) that can be used on system components (information system or industrial control system), and manages the use of them. - The organization uses only removable media (e.g. USB memory) permitted in the organization. Also, if there is no identifiable ownwer of portable storage devices, the organization prohibits the use of such devices. - The organization controles access to the media that contain highly confidential data, and properly grasps and manages the usage of the media taken outside of the controlled areas.
						Basic	- The organization identifies assets constituting its information system and industrial control system (hardware, software and information), assigns a responsible person to each asset, and documents a list of them. - It is desirable to list all the assets held, but if the target is huge, consider narrowing down the target assets through integration (grouping) of the analysis target and exclusion from the analysis target. - The organization sets priorities to the identified assets based on the importance of them in its business operation.
		A.8.1.2 Ownership of assets	Assets maintained in the inventory shall be owned.	CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	H-Advanced	-The organization identifies assets constituting its information systems and industrial control systems (hardware, including IoT devices; software; and information) uniquely, assigns a responsible person to each asset. And the organization maintains/manages lists periodically, or at the request of the operator including configuration information of assets (e.g., names, version information, license information, and location) while recognizing situations in real time. - The information system regularly audits whether the actual configuration grasped conforms to the baseline configuration defined by the organization, and responds appropriately. (Example: blocking unplanned connections except those permitted by the organization as an exception) -The information system and industrial control system implement and operate a mechanism which automatically detects and responses to unauthorized assets.
						Advanced	- Maintain/manage lists including configuration information of assets (e.g., names, version information, license information, and location) by reviewing and updating them periodically. - The organization makes a list of removable media (e.g., USB memory sticks) that can be used on system components (information system or industrial control system), and manages the use of them. - The organization uses only removable media (e.g. USB memory) permitted in the organization. Also, if there is no identifiable ownwer of portable storage devices, the organization prohibits the use of such devices. - The organization controles access to the media that contain highly confidential data, and properly grasps and manages the usage of the media taken outside of the controlled areas.
						Basic	- The organization identifies assets constituting its information system and industrial control system (hardware, software and information), assigns a responsible person to each asset, and documents a list of them. - It is desirable to list all the assets held, but if the target is huge, consider narrowing down the target assets through integration (grouping) of the analysis target and exclusion from the analysis target. - The organization sets priorities to the identified assets based on the importance of them in its business operation.
		A.8.1.3 Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	H-Advanced	-The organization identifies assets constituting its information systems and industrial control systems (hardware, including IoT devices; software; and information) uniquely, assigns a responsible person to each asset. And the organization maintains/manages lists periodically, or at the request of the operator including configuration information of assets (e.g., names, version information, license information, and location) while recognizing situations in real time. - The information system regularly audits whether the actual configuration grasped conforms to the baseline configuration defined by the organization, and responds appropriately. (Example: blocking unplanned connections except those permitted by the organization as an exception) -The information system and industrial control system implement and operate a mechanism which automatically detects and responses to unauthorized assets.
						Advanced	- Maintain/manage lists including configuration information of assets (e.g., names, version information, license information, and location) by reviewing and updating them periodically. - The organization makes a list of removable media (e.g., USB memory sticks) that can be used on system components (information system or industrial control system), and manages the use of them. - The organization uses only removable media (e.g. USB memory) permitted in the organization. Also, if there is no identifiable ownwer of portable storage devices, the organization prohibits the use of such devices. - The organization controles access to the media that contain highly confidential data, and properly grasps and manages the usage of the media taken outside of the controlled areas.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
		A.8.1.4 Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	CPS.IP-9	Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.	Advanced	- The organization makes changes to its staff members' rights to access certain systems and/or rooms on the premises when they are reshuffled or transferred internally. - To minimize impacts when a staff member leaves the organization, designate backup members regarding important duties as a supplier including operation and maintenance. - The organization identifies conditions in which re-screening is required such as changes in access authority to their own systems, and re-screen if necessary. - The organization conducts an interview on information security when personnel leave. - The organization ensures that responsibilities for security are met, particularly of personnel handling sensitive information, throughout the whole process from hiring to retirement.
						Basic	- The organization identifies the responsibility for security of personnel in the employment contract. The organization states that this responsibility should be sustained for a reasonable period of time after the termination of employment, in order to prevent information leakage after the termination of employment. - The organization reviews a staff member before granting him or her access to its systems. - The organization conducts the following when a staff member resigns or retires: - Disables the staff member's access to its systems within a certain period; - Disables the authentication and credentials related to the staff member; - Collects all system-related things for security that the staff member has used; - Retains access to the information about the organization and information systems that have been managed by the individual who is leaving.
	A.8.2 Information classification	A.8.2.1 Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	CPS.AM-6	Classify and prioritize resources (e.g., People, Components, Data, and System) by function, importance, and business value, and communicate to the organizations and people relevant to those resources in business.	Advanced	- The organization considers business requirements and legal requirements which share or restrict data when classifying resources of the information system and industrial control system (data, components processing data, system, etc). - The person responsible for an asset is responsible for the classification of the data. - The organization includes classification rules and classification review standards after time passes in a resource classification system.
						Basic	- The organization sets priorities on identified information assets according to importance to the organization. - When related laws or regulations require us to follow a certain classification for resources of the organization (e.g., system and data), apply an appropriate classification to the asset.
				CPS.GV-3	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	Basic	- The organization identifies and documents all legal requirements and contract requirements related to data protection for each system and each organization and the organization's activities to satisfy these requirements, and update them to the latest. - The organization classifies its data appropriately according to the classification of the identified rules. - The organization takes measures for systems, components, etc., handling the applicable data in accordance with the requirements of the identified rules. When the implementation of a measure is considered difficult, measures such as tokenization of an applicable data in the organization may be considered. (e.g., tokenization of card information due to the Installment Sales Law)
		A.8.2.2 Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	CPS.PT-2	Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.	H-Advanced	- The organization identifies software programs that are not allowed to be executed on a system. - Manage a "black list" or "white list" so that the software programs not allowed on the system cannot be executed. - The organization regularly review and update the black list or the white list. - The system blocks the execution of these programs in accordance with the specified rules.
						Advanced	- The organization reviews the functions and services provided by its systems and items in order to identify the functions and services that could be deleted. - The organization uses network scanning tools, intrusion detection and prevention systems, and endpoint protection (e.g., a firewall, host-based intrusion detection system) in order to detect and prevent the use of banned functions, ports, protocols, and services. - The organization minimizes the functions and services of devices connected to the network such as multifunction printers in additional to typical IoT devices and servers.
						Basic	- The organization manages peripherals in use (e.g., USB flash drives) using a management ledger and keep them in a locked place. - The organization checks external storage devices connected to IoT devices or servers (e.g., USB flash drives) using antivirus software, use USB flash drives that can be checked for viruses, or take any appropriate action. - The organization plugs USB ports and serial ports out of use to physically block them.
		A.8.2.3 Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.DS-2	Encrypt information with an appropriate level of security strength, and store them.	H-Advanced	- The organization selects products that have been authenticated based on Cryptographic Module Validation Program (CMVP) in order to suitably implement selected algorithms to software and hardware, and to protect keys, identification codes, and entity authentication information that is used to decrypt encrypted information or to grant electronic signatures. - The organization protects are encrypts data to the appropriate strength when that data is taken outside of the organization. - The organization uses IoT devices that can encrypt and store data in internal memory.
						Advanced	- The organization examines safety and trustworthiness that are necessary, selects an algorithm, encrypts information (data) to the appropriate strength, and stores the information. If an algorithm on the CRYPTREC Ciphers List can be selected, the organization uses it to encrypt information (data) to the appropriate strength and stores the information. - The organization considers the level of security and trustworthiness required for the information, chooses an algorithm, and encrypts and stores high importance information handled by industrial control systems with appropriate strength without causing unacceptable impact on performance. [Reference] Regarding encryption technologies whose security and implementation performance are confirmed, "Cryptography Research and Evaluation Committees （CRYPTREC）" releases to the public the list of such technologies recommended for use that are sufficiently used in the market or are considered to spread in the future. It is desirable that the organization should refer to the list as needed when procuring systems that should implement encryption functions.
						Basic	- The organization examines safety and trustworthiness that are necessary, selects an algorithm, encrypts important information (data) handled by information systems to the appropriate strength, and stores the information.
				CPS.IP-6	When disposing of an IoT device and server, delete the stored data and the ID (identifier) uniquely identifying the genuine IoT devices and servers as well as important information (e.g., private key and digital certificate), or make them unreadable.	H-Advanced	- The organization defines classifications including security categories of data saved in an IoT device or server to be scrapped, and introduces a mechanism for using the proper technique for deleting data with the strength and integrity needed or making the data unreadable according to the definition.
	A.8.3 Media handling	A.8.3.1 Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	H-Advanced	-The organization identifies assets constituting its information systems and industrial control systems (hardware, including IoT devices; software; and information) uniquely, assigns a responsible person to each asset. And the organization maintains/manages lists periodically, or at the request of the operator including configuration information of assets (e.g., names, version information, license information, and location) while recognizing situations in real time. - The information system regularly audits whether the actual configuration grasped conforms to the baseline configuration defined by the organization, and responds appropriately. (Example: blocking unplanned connections except those permitted by the organization as an exception) -The information system and industrial control system implement and operate a mechanism which automatically detects and responses to unauthorized assets.
						Advanced	- Maintain/manage lists including configuration information of assets (e.g., names, version information, license information, and location) by reviewing and updating them periodically. - The organization makes a list of removable media (e.g., USB memory sticks) that can be used on system components (information system or industrial control system), and manages the use of them. - The organization uses only removable media (e.g. USB memory) permitted in the organization. Also, if there is no identifiable ownwer of portable storage devices, the organization prohibits the use of such devices. - The organization controles access to the media that contain highly confidential data, and properly grasps and manages the usage of the media taken outside of the controlled areas.
				CPS.IP-6	When disposing of an IoT device and server, delete the stored data and the ID (identifier) uniquely identifying the genuine IoT devices and servers as well as important information (e.g., private key and digital certificate), or make them unreadable.	H-Advanced	- The organization defines classifications including security categories of data saved in an IoT device or server to be scrapped, and introduces a mechanism for using the proper technique for deleting data with the strength and integrity needed or making the data unreadable according to the definition.
						Advanced	- The organization establishes a procedure for scrapping its equipment including IoT devices and servers, deletes data saved in the equipment or makes the data unreadable in accordance with the procedure, and makes sure that the action has been done successfully.
						Basic	- The organization deletes data that has been saved in its IoT devices or servers to be scrapped, or makes the data unreadable.
				CPS.PT-2	Minimize funcions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.	H-Advanced	- The organization identifies software programs that are not allowed to be executed on a system. - Manage a “black list” or "white list" so that the software programs not allowed on the system cannot be executed. - The organization regularly review and update the black list or the white list. - The system blocks the execution of these programs in accordance with the specified rules.
						Advanced	- The organization reviews the functions and services provided by its systems and items in order to identify the functions and services that could be deleted. - The organization uses network scanning tools, intrusion detection and prevention systems, and endpoint protection (e.g., a firewall, host-based intrusion detection system) in order to detect and prevent the use of banned functions, ports, protocols, and services. - The organization minimizes the functions and services of devices connected to the network such as multifunction printers in additional to typical IoT devices and servers.
						Basic	- The organization manages peripherals in use (e.g., USB flash drives) using a management ledger and keep them in a locked place. - The organization checks external storage devices connected to IoT devices or servers (e.g., USB flash drives) using antivirus software, use USB flash drives that can be checked for viruses, or take any appropriate action. - The organization plugs USB ports and serial ports out of use to physically block them.
		A.8.3.2 Disposal of media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	CPS.IP-6	When disposing of an IoT device and server, delete the stored data and the ID (identifier) uniquely identifying the genuine IoT devices and servers as well as important information (e.g., private key and digital certificate), or make them unreadable.	H-Advanced	- The organization defines classifications including security categories of data saved in an IoT device or server to be scrapped, and introduces a mechanism for using the proper technique for deleting data with the strength and integrity needed or making the data unreadable according to the definition.
						Advanced	- The organization establishes a procedure for scrapping its equipment including IoT devices and servers, deletes data saved in the equipment or makes the data unreadable in accordance with the procedure, and makes sure that the action has been done successfully.
						Basic	- The organization deletes data that has been saved in its IoT devices or servers to be scrapped, or makes the data unreadable.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
		A.8.3.3 Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	CPS.SC-4	When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	H-Advanced	- The organization or a third party tests the procured devices to see whether the security requirements stipulated in the contract are fulfilled. - The organization checks throughout the entire relevant supply chain (including reconsigned organizations) as to whether the devices especially important for their operation are manufactured under appropriate procedures by organizations that have quality and security management ability above a certain level.
						Advanced	- The organization specifies in the contract the security requirements that the products and services procured from the partner should comply with, such as the following. - Specific certifications related to security (e.g., ISMS certification、ISASecure EDSA certification, Japan Information Technology Security Evaluation and Certification Scheme (JISEC) have been gained. - The vendor itself confirms that it has implemented the security measures in accordance with the standards of specific certifications related to security - It has implemented the necessary security requirements from the design phase (security by design) based on the results of risk analysis, etc., and test them. - It is desirable that the organization should, at the phase of planning procurement, secure a budget for security requirements regarding products or services themselves, or protection of assets used for procurement and supply of such products or services. - The organization formulates, manages and improves security measurement rules to evaluate procurement or supply of products or services, including the following. - Target for measurement - Method and frequency of reporting on measures taken - Measures to be taken when measures are not implemented - The organization checks means of detecting (or preventing) falsifications and leakages during shipments and whether or not the IoT devices and software being delivered have been operated without authorization. - Goods: security courier, protection seal, etc. - Digital transfer: encryption, hash of the entire transmitted data, etc.
A.9 Access control	A.9.1 Business requirements of access control	A.9.1.1 Access control policyAccess control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	CPS.AC-1	Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	H-Advanced	- The organization introduces and operates, for example, the following automated mechanisms for managing accounts in their own information systems and industrial control systems. -Automatically collect account information periodically from the system to be managed -Automatically change password of privileged account - The industrial control system supports integrated account management. - After a certain period of time, the system automatically invalidates temporary accounts, emergency accounts, and accounts not in use on their system. - The information system automatically audits and reports account validation and invalidation that is associated with creation, change, and deletion of accounts in the system used by the organization.
						Advanced	- The organization must obtain approval from the management supervisor when creating a system account. - With regard to the shared user account, a user who can know authentication information is managed in a list or the like, and the range of using the account can be identified. - The organization monitors the usage of system accounts used in an information system. - If an account needs change or becomes unnecessary, the organization notifies the management supervisor. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used. - The organization notifies the user (or the person in charge of management) when the password is changed in an information system and an industrial control system. - If the information system resets the credentials for reasons such as user"s forgetting credentials, the information system confirms securely that the account is its own to prevent unauthorized tampering with the credentials by a malicious party.
						Basic	- The organization appoints a management supervisor for the accounts in its information system and industrial control system. - The organization decides and selects types of system accounts necessary (e.g., general user/system administrator/shared user/temporary user), with consideration of their mission and business functions. - The organization creates and enables system accounts as per the procedure, and changes, disables and deletes them as needed. - The organization develops a policy of credentials (e.g. password, security key) for its own information systems and industrial control systems, and implements a function that cannot be set up unless the credential satisfies the policy. The following is an example of the content of the policy. - Devolop and operate the requirements for passwords in order to ensure the minimum required complexity. - When new credentials are created, change them to at least the number of characters defined by the organization. - Store and transmit only cryptographically protected credentials. - Prohibit reuse of the same credentials for the period that the organization defines. - The organization allows its members to use temporary credentials exceptionally when logging on to the system when they have forgotten credentials, if they change immediately to a strong password. - The organization does not share user identification information among multiple system users in an information system and an industrial control system except when multiple users function as a single group.
		A.9.1.2 Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	CPS.AC-6	Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.	H-Advanced	- The system uses a multifactor authentication in its system for access to the system or network with non-privileged accounts. - Regarding an information system that handles highly confidential data, access to the system and network with privileged or non-privileged accounts in the system, uses an authentication mechanism that can tolerate attacks of replay. [Reference] It is desirable to refer to NIST SP 800 63-3 regarding strength of authentication methods and appropriate use cases.
						Advanced	- In consideration of the risk of unauthorized login to the privileged account in the system, the organization in principle prohibits login to the privileged account via the network when it is not possible to implement a sufficient confidence methods of authentication. - The information system requires a multifactor authentication in its system for access to the system or network with privileged accounts when cannot implement actions such as invalidating the administrator account for the system. - In principle, the organization invalidates the default administrator account in the information system. - The information system permits the necessary minimum privileged authority to the user account when performing privileged operations.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	A.9.2 User access management	A.9.2.1 User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	CPS.AC-1	Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	H-Advanced	- The organization introduces and operates, for example, the following automated mechanisms for managing accounts in their own information systems and industrial control systems. -Automatically collect account information periodically from the system to be managed -Automatically change password of privileged account - The industrial control system supports integrated account management. - After a certain period of time, the system automatically invalidates temporary accounts, emergency accounts, and accounts not in use on their system. - The information system automatically audits and reports account validation and invalidation that is associated with creation, change, and deletion of accounts in the system used by the organization.
						Advanced	- The organization must obtain approval from the management supervisor when creating a system account. - With regard to the shared user account, a user who can know authentication information is managed in a list or the like, and the range of using the account can be identified. - The organization monitors the usage of system accounts used in an information system. - If an account needs change or becomes unnecessary, the organization notifies the management supervisor. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used. - The organization notifies the user (or the person in charge of management) when the password is changed in an information system and an industrial control system. - If the information system resets the credentials for reasons such as user"s forgetting credentials, the information system confirms securely that the account is its own to prevent unauthorized tampering with the credentials by a malicious party.
						Basic	- The organization appoints a management supervisor for the accounts in its information system and industrial control system. - The organization decides and selects types of system accounts necessary (e.g., general user/system administrator/shared user/temporary user), with consideration of their mission and business functions. - The organization creates and enables system accounts as per the procedure, and changes, disables and deletes them as needed. - The organization develops a policy of credentials (e.g. password, security key) for its own information systems and industrial control systems, and implements a function that cannot be set up unless the credential satisfies the policy. The following is an example of the content of the policy. - Devolop and operate the requirements for passwords in order to ensure the minimum required complexity. - When new credentials are created, change them to at least the number of characters defined by the organization. - Store and transmit only cryptographically protected credentials. - Prohibit reuse of the same credentials for the period that the organization defines. - The organization allows its members to use temporary credentials exceptionally when logging on to the system when they have forgotten credentials, if they change immediately to a strong password. - The organization does not share user identification information among multiple system users in an information system and an industrial control system except when multiple users function as a single group.
				CPS.AC-8	Restrict communications by IoT devices and servers to those with entities (e.g. people, components, system, etc.) identified through proper procedures.	Basic	- The organization assigns identifiers to its IoT devices and servers, as well as managing the identification by preventing re-use of identifiers and invalidating identifiers after a certain period of time. - Before connecting their IoT devices and servers to the network, the information system and the industrial control system prepare a mechanism that uniquely identifies and authenticate these devices. - Communication using IoT devices is denied as default. The protocol to be used is authorized as an exception.
		A.9.2.2 User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	CPS.AC-1	Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	H-Advanced	- The organization introduces and operates, for example, the following automated mechanisms for managing accounts in their own information systems and industrial control systems. -Automatically collect account information periodically from the system to be managed -Automatically change password of privileged account - The industrial control system supports integrated account management. - After a certain period of time, the system automatically invalidates temporary accounts, emergency accounts, and accounts not in use on their system. - The information system automatically audits and reports account validation and invalidation that is associated with creation, change, and deletion of accounts in the system used by the organization.
						Advanced	- The organization must obtain approval from the management supervisor when creating a system account. - With regard to the shared user account, a user who can know authentication information is managed in a list or the like, and the range of using the account can be identified. - The organization monitors the usage of system accounts used in an information system. - If an account needs change or becomes unnecessary, the organization notifies the management supervisor. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used. - The organization notifies the user (or the person in charge of management) when the password is changed in an information system and an industrial control system. - If the information system resets the credentials for reasons such as user"s forgetting credentials, the information system confirms securely that the account is its own to prevent unauthorized tampering with the credentials by a malicious party.
						Basic	- The organization appoints a management supervisor for the accounts in its information system and industrial control system. - The organization decides and selects types of system accounts necessary (e.g., general user/system administrator/shared user/temporary user), with consideration of their mission and business functions. - The organization creates and enables system accounts as per the procedure, and changes, disables and deletes them as needed. - The organization develops a policy of credentials (e.g. password, security key) for its own information systems and industrial control systems, and implements a function that cannot be set up unless the credential satisfies the policy. The following is an example of the content of the policy. - Devolop and operate the requirements for passwords in order to ensure the minimum required complexity. - When new credentials are created, change them to at least the number of characters defined by the organization. - Store and transmit only cryptographically protected credentials. - Prohibit reuse of the same credentials for the period that the organization defines. - The organization allows its members to use temporary credentials exceptionally when logging on to the system when they have forgotten credentials, if they change immediately to a strong password. - The organization does not share user identification information among multiple system users in an information system and an industrial control system except when multiple users function as a single group.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
		A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	CPS.AC-5	Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions)	H-Advanced	- The organization specifies administrators who use the security functions (e.g., access authority setting) and regulates privileged accounts in its system. - The information system adopts a system monitoring mechanism to check the use of privileged functions. - The information system prohibits non-privileged users from executing privileged functions on the system by invalidating, avoiding, and changing security measures that are changed and implemented by non-privileged users. - The organization can minimize the number of users who can use the system administrator's authority in an emergency to minimize the damage caused by the security incident. - The organization can prevent even system administrators from stopping critical services and protected processes through the server to minimize the damage caused by security incidents.
						Advanced	- The organization implements access control in the information system and the industrial control system based on separation of duties (e.g., user / system administrator). - The organization adopts a general rule on the minimum authority of specific duties. - Segregate authority of general user from that of administrator. (Require users to use the system with a non-privileged account when using a non-security function.) - Minimize authority for duties not in charge. - The organization separates and stipulates duties that are assigned by the person in charge.
				CPS.AC-6	Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.	H-Advanced	- The system uses a multifactor authentication in its system for access to the system or network with non-privileged accounts. - Regarding an information system that handles highly confidential data, access to the system and network with privileged or non-privileged accounts in the system, uses an authentication mechanism that can tolerate attacks of replay. [Reference] It is desirable to refer to NIST SP 800 63-3 regarding strength of authentication methods and appropriate use cases.
						Advanced	- In consideration of the risk of unauthorized login to the privileged account in the system, the organization in principle prohibits login to the privileged account via the network when it is not possible to implement a sufficient confidence methods of authentication. - The information system requires a multifactor authentication in its system for access to the system or network with privileged accounts when cannot implement actions such as invalidating the administrator account for the system. - In principle, the organization invalidates the default administrator account in the information system. - The information system permits the necessary minimum privileged authority to the user account when performing privileged operations.
		A.9.2.4 Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	CPS.AC-1	Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	H-Advanced	- The organization introduces and operates, for example, the following automated mechanisms for managing accounts in their own information systems and industrial control systems. -Automatically collect account information periodically from the system to be managed -Automatically change password of privileged account - The industrial control system supports integrated account management. - After a certain period of time, the system automatically invalidates temporary accounts, emergency accounts, and accounts not in use on their system. - The information system automatically audits and reports account validation and invalidation that is associated with creation, change, and deletion of accounts in the system used by the organization.
						Advanced	- The organization must obtain approval from the management supervisor when creating a system account. - With regard to the shared user account, a user who can know authentication information is managed in a list or the like, and the range of using the account can be identified. - The organization monitors the usage of system accounts used in an information system. - If an account needs change or becomes unnecessary, the organization notifies the management supervisor. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used. - The organization notifies the user (or the person in charge of management) when the password is changed in an information system and an industrial control system. - If the information system resets the credentials for reasons such as user"s forgetting credentials, the information system confirms securely that the account is its own to prevent unauthorized tampering with the credentials by a malicious party.
		A.9.2.5 Review of user access rights	Asset owners shall review users' access rights at regular intervals.	CPS.AC-1	Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	H-Advanced	- The organization introduces and operates, for example, the following automated mechanisms for managing accounts in their own information systems and industrial control systems. -Automatically collect account information periodically from the system to be managed -Automatically change password of privileged account - The industrial control system supports integrated account management. - After a certain period of time, the system automatically invalidates temporary accounts, emergency accounts, and accounts not in use on their system. - The information system automatically audits and reports account validation and invalidation that is associated with creation, change, and deletion of accounts in the system used by the organization.
						Advanced	- The organization must obtain approval from the management supervisor when creating a system account. - With regard to the shared user account, a user who can know authentication information is managed in a list or the like, and the range of using the account can be identified. - The organization monitors the usage of system accounts used in an information system. - If an account needs change or becomes unnecessary, the organization notifies the management supervisor. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used. - The organization notifies the user (or the person in charge of management) when the password is changed in an information system and an industrial control system. - If the information system resets the credentials for reasons such as user"s forgetting credentials, the information system confirms securely that the account is its own to prevent unauthorized tampering with the credentials by a malicious party.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
		A.9.2.6 Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	CPS.AC-1	Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.	H-Advanced	- The organization introduces and operates, for example, the following automated mechanisms for managing accounts in their own information systems and industrial control systems. -Automatically collect account information periodically from the system to be managed -Automatically change password of privileged account - The industrial control system supports integrated account management. - After a certain period of time, the system automatically invalidates temporary accounts, emergency accounts, and accounts not in use on their system. - The information system automatically audits and reports account validation and invalidation that is associated with creation, change, and deletion of accounts in the system used by the organization.
						Advanced	- The organization must obtain approval from the management supervisor when creating a system account. - With regard to the shared user account, a user who can know authentication information is managed in a list or the like, and the range of using the account can be identified. - The organization monitors the usage of system accounts used in an information system. - If an account needs change or becomes unnecessary, the organization notifies the management supervisor. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used. - The organization notifies the user (or the person in charge of management) when the password is changed in an information system and an industrial control system. - If the information system resets the credentials for reasons such as user"s forgetting credentials, the information system confirms securely that the account is its own to prevent unauthorized tampering with the credentials by a malicious party.
						Basic	- The organization appoints a management supervisor for the accounts in its information system and industrial control system. - The organization decides and selects types of system accounts necessary (e.g., general user/system administrator/shared user/temporary user), with consideration of their mission and business functions. - The organization creates and enables system accounts as per the procedure, and changes, disables and deletes them as needed. - The organization develops a policy of credentials (e.g. password, security key) for its own information systems and industrial control systems, and implements a function that cannot be set up unless the credential satisfies the policy. The following is an example of the content of the policy. - Devolop and operate the requirements for passwords in order to ensure the minimum required complexity. - When new credentials are created, change them to at least the number of characters defined by the organization. - Store and transmit only cryptographically protected credentials. - Prohibit reuse of the same credentials for the period that the organization defines. - The organization allows its members to use temporary credentials exceptionally when logging on to the system when they have forgotten credentials, if they change immediately to a strong password. - The organization does not share user identification information among multiple system users in an information system and an industrial control system except when multiple users function as a single group.
				CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	H-Advanced	- The organization regulates service wires and transmission paths that are related to their IoT devices and servers by physical access. - The organization regulates output devices of its system by physical access. - The organization monitors alarms and monitoring devices (e.g., surveillance cameras) for physical intrusions into the areas within the physical security boundaries.
						Advanced	- The organization monitors physical accesses to the areas within the physical security boundaries and regularly reviews the audit log. - The organization keeps the records of visitor's access to the areas within the physical security boundaries and regularly reviews them.
						Basic	- The organization maintains upkeep of the access list for areas where their IoT devices and servers are located and issues permission certificates necessary for access. - The organization defines physical security boundaries at its facilities, and implement access control according to the security requirements of assets placed within the boundaries and the results of risk assessment. - The organization monitors the work of temporarily authorized party within the physical security boundaries, such as by authorized attendants or monitoring cameras.
	A.9.3 User responsibilities	A.9.3.1 Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	CPS.AC-4	Prevent unauthorized log-in to IoT devices and servers by measures such as implementing functions for lockout after a specified number of incorrect log-in attempts and providing a time interval until safety is ensured.	H-Advanced	- The information system and the industrial control system (excluding some cases where immediacy of response is required) sets a limit to the number of continuous login attempts on its system. If the user fails to log in, he or she will only be able to re-login after the administrator removes the restriction.
						Advanced	- The information system and the industrial control system set a limit on the number of continuous login attempts on its system. If the user fails to log in, he or she will not be able to re-login for a certain period of time. - The information system and industrial control system lock the session manually or automatically if the system's non-operation continues beyond the time set by the organization. * In the industrial control system, it may be desirable not to lock session when it is assumed that a session in which an operator is required to respond immediately in an emergency may be conducted.
				CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.
				CPS.IP-1	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	Basic	- Upon determining the most restrictive setting criteria that conform to their operation, the organization creates a document on the initial setting procedures and setting details for the IoT devices and servers that will be introduced and adjusts the settings according to the document. - The organization checks initial setting values of IoT devices before installing them, and adjusts the settings appropriately if they do not comply with the policy stipulated in CPS.AC-1. - The organization checks and records software installed in IoT devices before introducing them.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	A.9.4 System and application access control	A.9.4.1 Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	CPS.AC-5	Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions)	H-Advanced	- The organization specifies administrators who use the security functions (e.g., access authority setting) and regulates privileged accounts in its system. - The information system adopts a system monitoring mechanism to check the use of privileged functions. - The information system prohibits non-privileged users from executing privileged functions on the system by invalidating, avoiding, and changing security measures that are changed and implemented by non-privileged users. - The organization can minimize the number of users who can use the system administrator's authority in an emergency to minimize the damage caused by the security incident. - The organization can prevent even system administrators from stopping critical services and protected processes through the server to minimize the damage caused by security incidents.
						Advanced	- The organization implements access control in the information system and the industrial control system based on separation of duties (e.g., user / system administrator). - The organization adopts a general rule on the minimum authority of specific duties. - Segregate authority of general user from that of administrator. (Require users to use the system with a non-privileged account when using a non-security function.) - Minimize authority for duties not in charge. - The organization separates and stipulates duties that are assigned by the person in charge.
				CPS.AC-6	Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.	H-Advanced	- The system uses a multifactor authentication in its system for access to the system or network with non-privileged accounts. - Regarding an information system that handles highly confidential data, access to the system and network with privileged or non-privileged accounts in the system, uses an authentication mechanism that can tolerate attacks of replay. [Reference] It is desirable to refer to NIST SP 800 63-3 regarding strength of authentication methods and appropriate use cases.
						Advanced	- In consideration of the risk of unauthorized login to the privileged account in the system, the organization in principle prohibits login to the privileged account via the network when it is not possible to implement a sufficient confidence methods of authentication. - The information system requires a multifactor authentication in its system for access to the system or network with privileged accounts when cannot implement actions such as invalidating the administrator account for the system. - In principle, the organization invalidates the default administrator account in the information system. - The information system permits the necessary minimum privileged authority to the user account when performing privileged operations.
		A.9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	CPS.AC-4	Prevent unauthorized log-in to IoT devices and servers by measures such as implementing functions for lockout after a specified number of incorrect log-in attempts and providing a time interval until safety is ensured.	H-Advanced	- The information system and the industrial control system (excluding some cases where immediacy of response is required) sets a limit to the number of continuous login attempts on its system. If the user fails to log in, he or she will only be able to re-login after the administrator removes the restriction.
						Advanced	- The information system and the industrial control system set a limit on the number of continuous login attempts on its system. If the user fails to log in, he or she will not be able to re-login for a certain period of time. - The information system and industrial control system lock the session manually or automatically if the system's non-operation continues beyond the time set by the organization. * In the industrial control system, it may be desirable not to lock session when it is assumed that a session in which an operator is required to respond immediately in an emergency may be conducted.
		A.9.4.3 Password management system	Password management systems shall be interactive and shall ensure quality passwords.	CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.
		A.9.4.4 Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	CPS.AC-5	Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions)	H-Advanced	- The organization specifies administrators who use the security functions (e.g., access authority setting) and regulates privileged accounts in its system. - The information system adopts a system monitoring mechanism to check the use of privileged functions. - The information system prohibits non-privileged users from executing privileged functions on the system by invalidating, avoiding, and changing security measures that are changed and implemented by non-privileged users. - The organization can minimize the number of users who can use the system administrator's authority in an emergency to minimize the damage caused by the security incident. - The organization can prevent even system administrators from stopping critical services and protected processes through the server to minimize the damage caused by security incidents.
						Advanced	- The organization implements access control in the information system and the industrial control system based on separation of duties (e.g., user / system administrator). - The organization adopts a general rule on the minimum authority of specific duties. - Segregate authority of general user from that of administrator. (Require users to use the system with a non-privileged account when using a non-security function.) - Minimize authority for duties not in charge. - The organization separates and stipulates duties that are assigned by the person in charge.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.AC-6	Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.	H-Advanced	- The system uses a multifactor authentication in its system for access to the system or network with non-privileged accounts. - Regarding an information system that handles highly confidential data, access to the system and network with privileged or non-privileged accounts in the system, uses an authentication mechanism that can tolerate attacks of replay. [Reference] It is desirable to refer to NIST SP 800 63-3 regarding strength of authentication methods and appropriate use cases.
						Advanced	- In consideration of the risk of unauthorized login to the privileged account in the system, the organization in principle prohibits login to the privileged account via the network when it is not possible to implement a sufficient confidence methods of authentication. - The information system requires a multifactor authentication in its system for access to the system or network with privileged accounts when cannot implement actions such as invalidating the administrator account for the system. - In principle, the organization invalidates the default administrator account in the information system. - The information system permits the necessary minimum privileged authority to the user account when performing privileged operations.
		A.9.4.5 Access control to program source code	Access to program source code shall be restricted.	CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.
A.10 Cryptography	A.10.1 Cryptographic controls	A.10.1.1 Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	CPS.DS-2	Encrypt information with an appropriate level of security strength, and store them.	H-Advanced	- The organization selects products that have been authenticated based on Cryptographic Module Validation Program (CMVP) in order to suitably implement selected algorithms to software and hardware, and to protect keys, identification codes, and entity authentication information that is used to decrypt encrypted information or to grant electronic signatures. - The organization protects are encrypts data to the appropriate strength when that data is taken outside of the organization. - The organization uses IoT devices that can encrypt and store data in internal memory.
						Advanced	- The organization examines safety and trustworthiness that are necessary, selects an algorithm, encrypts information (data) to the appropriate strength, and stores the information. If an algorithm on the CRYPTREC Ciphers List can be selected, the organization uses it to encrypt information (data) to the appropriate strength and stores the information. - The organization considers the level of security and trustworthiness required for the information, chooses an algorithm, and encrypts and stores high importance information handled by industrial control systems with appropriate strength without causing unacceptable impact on performance. [Reference] Regarding encryption technologies whose security and implementation performance are confirmed, "Cryptography Research and Evaluation Committees （CRYPTREC）" releases to the public the list of such technologies recommended for use that are sufficiently used in the market or are considered to spread in the future. It is desirable that the organization should refer to the list as needed when procuring systems that should implement encryption functions.
				CPS.DS-3	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.	H-Advanced	- The organization protects th networks composing the information system and industrial control system that handles important data by implementing encrytion of communication channels or by alternative physical measures.
						Advanced	- The information system employs an cryptographic mechanism and encrypt communciation paths. [Reference] For encryption of communication paths, there are several methods such as IP-VPN, Ipsec-VPN, SSL VPN. It is desirable that the organization should select the method considering the importance of the data transmitted in the communication paths, the budget, and so on.
				CPS.DS-4	Encrypt information itself when sending/receiving information.	H-Advanced	- The system /IoT apparatus introduces the code module which it can implement without even little resource losing availability, and it is desirable to encrypt the communication data from a high apparatus of the importance at appropriate strength. - The information system encrypts all data transmitted outside the organization with appropriate strength, not limited to high or low importance.
						Advanced	- The organization encrypts information with appropriate strength when transmitting highly confidential information to an external organization or the like.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
		A.10.1.2 Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	CPS.DS-5	Securely control encryption keys throughout their life cycle to ensure proper operation and securely transmitted, received and stored data.	H-Advanced	- If the user loses the key, the organization maintains the availability of the information by reissuing key or the like. - It is desirable to consider authenticity of the public key as well as to securely control the secret key and private key. This authentication process is carried out using the public key certificate issued normally by a certificate authority. It is desirable that the certificate authority should be a recognized organization that implements appropriate measures and procedures to provide the required reliablity.
						Advanced	- It is desirable that the organization should set out a policy and procedure regarding the following items to take immediate and appropriate measures when the private key is imperiled. - A structure to take measures against imperilment of the private key (including the stakeholders, roles, cooperation with contractors) - Criteria to judge whether the private key is imperiled or is in danger of imperilment - To investigate the cause of imperilment of the private key, and to attempt to remove the cause - Suspension of the services using the key - To create a new pair of keys and issue a certificate for the new key - Disclosure of information regarding imperilment of the private key (Notified parties, a method of notification, disclosure policy, etc.) [Reference] It is desirable to refer to the group of standards of ISO/IEC 11770, NIST SP 800-57 Part 1 Rev.4, and so on for the details about key management.
						Basic	- It is desirable that the organization should protect all encryption keys from modification and loss.
				CPS.DS-8	When handling information to be protected or procuring devices that have an important function to the organization, useselect the IoT devices and servers equipped with anti-tampering devices.	H-Advanced	- When handling information that shall be protected or when procuring devices that have a function important to the organization, the organization procures devices that use anti-tampering devices. - When storing encryption keys for the cryptographic mechanism used in the information system and the industrial control system, the organization uses anti-tampering devices.
A.11 Physical and environmental security	A.11.1 Secure areas	A.11.1.1 Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	H-Advanced	- The organization regulates service wires and transmission paths that are related to their IoT devices and servers by physical access. - The organization regulates output devices of its system by physical access. - The organization monitors alarms and monitoring devices (e.g., surveillance cameras) for physical intrusions into the areas within the physical security boundaries.
						Advanced	- The organization monitors physical accesses to the areas within the physical security boundaries and regularly reviews the audit log. - The organization keeps the records of visitor's access to the areas within the physical security boundaries and regularly reviews them.
				CPS.CM-2	Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.	H-Advanced	- The organization tracks and monitors the locations and relocation of important assets within the scope of its management of particularly important assets.
						Advanced	- The organization reviews the relevant audit log regularly or when an incident or a sign of an incident appears if a physical access log from access control is available while 24-h monitoring is not conducted through security cameras or by any other means. - A person in charge accompanies a visitor into the area where the organization's assets that must be protected are directly accessible (e.g., an office) in order to monitor the visitor's behavior. - The organization monitors through security cameras or by other means physical access to its facilities that are vital for its operations and house IoT devices and servers, thereby enabling early detection of any physical security incidents and immediate action. - If the above physical security measures may be difficult to implement for items such as IoT devices and servers that may be critical to the organization's operation because they are in a remote location or for any other reasons, consider using tamper-resistant equipment (CPS.DS-6) or taking any other appropriate measures to enhance the physical security properties of the equipment itself.
						Basic	- If the organization is unable to control access to, or provide video surveillance service for, the areas that should allow only limited physical access because of issues of costs and other reasons, it takes alternative manual measures, such as that its employee in charge accompany a visitor on the premises. - The organization implements physical security measures to control access to designated areas in the facility that do not be allowed for the general public to access. - The organization verifies the access authority of the personnel before permitting the physical access and collects and manages the records of entry and exit.
		A.11.1.2 Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	H-Advanced	- The organization regulates service wires and transmission paths that are related to their IoT devices and servers by physical access. - The organization regulates output devices of its system by physical access. - The organization monitors alarms and monitoring devices (e.g., surveillance cameras) for physical intrusions into the areas within the physical security boundaries.
						Advanced	- The organization monitors physical accesses to the areas within the physical security boundaries and regularly reviews the audit log. - The organization keeps the records of visitor's access to the areas within the physical security boundaries and regularly reviews them.
						Basic	- The organization maintains upkeep of the access list for areas where their IoT devices and servers are located and issues permission certificates necessary for access. - The organization defines physical security boundaries at its facilities, and implement access control according to the security requirements of assets placed within the boundaries and the results of risk assessment. - The organization monitors the work of temporarily authorized party within the physical security boundaries, such as by authorized attendants or monitoring cameras.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.CM-2	Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.	H-Advanced	- The organization tracks and monitors the locations and relocation of important assets within the scope of its management of particularly important assets.
						Advanced	- The organization reviews the relevant audit log regularly or when an incident or a sign of an incident appears if a physical access log from access control is available while 24-h monitoring is not conducted through security cameras or by any other means. - A person in charge accompanies a visitor into the area where the organization's assets that must be protected are directly accessible (e.g., an office) in order to monitor the visitor's behavior. - The organization monitors through security cameras or by other means physical access to its facilities that are vital for its operations and house IoT devices and servers, thereby enabling early detection of any physical security incidents and immediate action. - If the above physical security measures may be difficult to implement for items such as IoT devices and servers that may be critical to the organization's operation because they are in a remote location or for any other reasons, consider using tamper-resistant equipment (CPS.DS-6) or taking any other appropriate measures to enhance the physical security properties of the equipment itself.
						Basic	- If the organization is unable to control access to, or provide video surveillance service for, the areas that should allow only limited physical access because of issues of costs and other reasons, it takes alternative manual measures, such as that its employee in charge accompany a visitor on the premises. - The organization implements physical security measures to control access to designated areas in the facility that do not be allowed for the general public to access. - The organization verifies the access authority of the personnel before permitting the physical access and collects and manages the records of entry and exit.
		A.11.1.3 Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	H-Advanced	- The organization regulates service wires and transmission paths that are related to their IoT devices and servers by physical access. - The organization regulates output devices of its system by physical access. - The organization monitors alarms and monitoring devices (e.g., surveillance cameras) for physical intrusions into the areas within the physical security boundaries.
						Advanced	- The organization monitors physical accesses to the areas within the physical security boundaries and regularly reviews the audit log. - The organization keeps the records of visitor's access to the areas within the physical security boundaries and regularly reviews them.
						Basic	- The organization maintains upkeep of the access list for areas where their IoT devices and servers are located and issues permission certificates necessary for access. - The organization defines physical security boundaries at its facilities, and implement access control according to the security requirements of assets placed within the boundaries and the results of risk assessment. - The organization monitors the work of temporarily authorized party within the physical security boundaries, such as by authorized attendants or monitoring cameras.
				CPS.CM-2	Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.	H-Advanced	- The organization tracks and monitors the locations and relocation of important assets within the scope of its management of particularly important assets.
						Advanced	- The organization reviews the relevant audit log regularly or when an incident or a sign of an incident appears if a physical access log from access control is available while 24-h monitoring is not conducted through security cameras or by any other means. - A person in charge accompanies a visitor into the area where the organization's assets that must be protected are directly accessible (e.g., an office) in order to monitor the visitor's behavior. - The organization monitors through security cameras or by other means physical access to its facilities that are vital for its operations and house IoT devices and servers, thereby enabling early detection of any physical security incidents and immediate action. - If the above physical security measures may be difficult to implement for items such as IoT devices and servers that may be critical to the organization's operation because they are in a remote location or for any other reasons, consider using tamper-resistant equipment (CPS.DS-6) or taking any other appropriate measures to enhance the physical security properties of the equipment itself.
						Basic	- If the organization is unable to control access to, or provide video surveillance service for, the areas that should allow only limited physical access because of issues of costs and other reasons, it takes alternative manual measures, such as that its employee in charge accompany a visitor on the premises. - The organization implements physical security measures to control access to designated areas in the facility that do not be allowed for the general public to access. - The organization verifies the access authority of the personnel before permitting the physical access and collects and manages the records of entry and exit.
		A.11.1.4 Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	H-Advanced	- The organization regulates service wires and transmission paths that are related to their IoT devices and servers by physical access. - The organization regulates output devices of its system by physical access. - The organization monitors alarms and monitoring devices (e.g., surveillance cameras) for physical intrusions into the areas within the physical security boundaries.
				CPS.IP-5	Implement physical measures such as preparing an uninterruptible power supply, a fire protection facility, and protection from water infiltration to follow the policies and rules related to the physical operating environment, including the IoT devices and servers installed in the organization.	H-Advanced	- The organization adopts an automatic fire suppression system if a staffer is not stationed full time at a facility where its system is located.
						Advanced	- The organization maintains machine safety of equipment located within the area of their IoT devices and servers by using an uninterruptible power supply. - The organization adopts and maintains equipment and systems that run on an independent power supply which detect and extinguishes fire. - The organization have shut-off valves or isolation valves to protect areas with their IoT decides and servers from damages such as water leakages.
						Basic	- The organization adopts a system that maintains the temperature and humidity of the area with its IoT devices and servers being within the acceptable level. - The organization regularly monitors the temperature and humidity of the area with its IoT devices and servers.
		A.11.1.5 Working in secure areas	Procedures for working in secure areas shall be designed and applied.	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	H-Advanced	- The organization regulates service wires and transmission paths that are related to their IoT devices and servers by physical access. - The organization regulates output devices of its system by physical access. - The organization monitors alarms and monitoring devices (e.g., surveillance cameras) for physical intrusions into the areas within the physical security boundaries.
						Advanced	- The organization monitors physical accesses to the areas within the physical security boundaries and regularly reviews the audit log. - The organization keeps the records of visitor's access to the areas within the physical security boundaries and regularly reviews them.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
		A.11.1.6 Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	H-Advanced	- The organization regulates service wires and transmission paths that are related to their IoT devices and servers by physical access. - The organization regulates output devices of its system by physical access. - The organization monitors alarms and monitoring devices (e.g., surveillance cameras) for physical intrusions into the areas within the physical security boundaries.
						Advanced	- The organization monitors physical accesses to the areas within the physical security boundaries and regularly reviews the audit log. - The organization keeps the records of visitor's access to the areas within the physical security boundaries and regularly reviews them.
						Basic	- The organization maintains upkeep of the access list for areas where their IoT devices and servers are located and issues permission certificates necessary for access. - The organization defines physical security boundaries at its facilities, and implement access control according to the security requirements of assets placed within the boundaries and the results of risk assessment. - The organization monitors the work of temporarily authorized party within the physical security boundaries, such as by authorized attendants or monitoring cameras.
	A.11.2 Equipment	A.11.2.1 Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	CPS.IP-5	Implement physical measures such as preparing an uninterruptible power supply, a fire protection facility, and protection from water infiltration to follow the policies and rules related to the physical operating environment, including the IoT devices and servers installed in the organization.	H-Advanced	- The organization adopts an automatic fire suppression system if a staffer is not stationed full time at a facility where its system is located.
						Advanced	- The organization maintains machine safety of equipment located within the area of their IoT devices and servers by using an uninterruptible power supply. - The organization adopts and maintains equipment and systems that run on an independent power supply which detect and extinguishes fire. - The organization have shut-off valves or isolation valves to protect areas with their IoT decides and servers from damages such as water leakages.
						Basic	- The organization adopts a system that maintains the temperature and humidity of the area with its IoT devices and servers being within the acceptable level. - The organization regularly monitors the temperature and humidity of the area with its IoT devices and servers.
		A.11.2.2 Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	CPS.BE-3	Identify the dependency between the organization and other relevant parties and the important functions of each in the course of running the operation.	H-Advanced	- The organization identifies the functions of the following support utilities for the continuation of its business and the dependence relationship between them. - Communication service - Electrical power equipment (including power cables) - Among the above identified utilities, for those which have important roles for the continuation of its business, the organization examines the possibility of taking measures as follows: - Establishment of alternative communication services - Physical protection of electrical power equipment and power cables - Preparation of short-term permanent power supply equipment - When examining the possibility of using an alternative communication service, the organization considers the following: - Identify the requirements on the availability of the organization (including the target recovery time) when examining a contract with a communication service provider. - Reduce the possibility of sharing a single point of failure with a primary communication service.
				CPS.DS-7	Carry out periodic quality checks, prepare standby devices and uninterruptible power supplies, provide redundancy, detect failures, conduct replacement work, and update software for IoT devices, communication devices, circuits, etc.	Advanced	- The organization prepares short-term uninterrupted power supply which supports the switching of the information system to an alternative power source that can be used for a long period of time when the primary power source is lost.
						Basic	- In order to ensure that required performance of an information system and an industrial control system is satisfied, use of resources must be monitored and adjusted. In addition, storage capacity and performance that are required in the future are pre-estimated. - The organization protects devices from power outages and other failures that are attributable to malfunctions in the support utility. - The organization protects communication cables and power cables that transmit data or that support information service from interception, interference, and harm. - The organization properly maintaines devices to ensure continuous availability and integrity.
				CPS.IP-5	Implement physical measures such as preparing an uninterruptible power supply, a fire protection facility, and protection from water infiltration to follow the policies and rules related to the physical operating environment, including the IoT devices and servers installed in the organization.	H-Advanced	- The organization adopts an automatic fire suppression system if a staffer is not stationed full time at a facility where its system is located.
						Advanced	- The organization maintains machine safety of equipment located within the area of their IoT devices and servers by using an uninterruptible power supply. - The organization adopts and maintains equipment and systems that run on an independent power supply which detect and extinguishes fire. - The organization have shut-off valves or isolation valves to protect areas with their IoT decides and servers from damages such as water leakages.
						Basic	- The organization adopts a system that maintains the temperature and humidity of the area with its IoT devices and servers being within the acceptable level. - The organization regularly monitors the temperature and humidity of the area with its IoT devices and servers.
		A.11.2.3 Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	H-Advanced	- The organization regulates service wires and transmission paths that are related to their IoT devices and servers by physical access. - The organization regulates output devices of its system by physical access. - The organization monitors alarms and monitoring devices (e.g., surveillance cameras) for physical intrusions into the areas within the physical security boundaries.
				CPS.DS-7	Carry out periodic quality checks, prepare standby devices and uninterruptible power supplies, provide redundancy, detect failures, conduct replacement work, and update software for IoT devices, communication devices, circuits, etc.	Advanced	- The organization prepares short-term uninterrupted power supply which supports the switching of the information system to an alternative power source that can be used for a long period of time when the primary power source is lost.
						Basic	- In order to ensure that required performance of an information system and an industrial control system is satisfied, use of resources must be monitored and adjusted. In addition, storage capacity and performance that are required in the future are pre-estimated. - The organization protects devices from power outages and other failures that are attributable to malfunctions in the support utility. - The organization protects communication cables and power cables that transmit data or that support information service from interception, interference, and harm. - The organization properly maintaines devices to ensure continuous availability and integrity.
		A.11.2.4 Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	CPS.DS-7	Carry out periodic quality checks, prepare standby devices and uninterruptible power supplies, provide redundancy, detect failures, conduct replacement work, and update software for IoT devices, communication devices, circuits, etc.	Advanced	- The organization prepares short-term uninterrupted power supply which supports the switching of the information system to an alternative power source that can be used for a long period of time when the primary power source is lost.
						Basic	- In order to ensure that required performance of an information system and an industrial control system is satisfied, use of resources must be monitored and adjusted. In addition, storage capacity and performance that are required in the future are pre-estimated. - The organization protects devices from power outages and other failures that are attributable to malfunctions in the support utility. - The organization protects communication cables and power cables that transmit data or that support information service from interception, interference, and harm. - The organization properly maintaines devices to ensure continuous availability and integrity.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.MA-1	- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updateswith managed tools properly and in a timely manner while recording the history. - Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable.	H-Advanced	- The organization gives prior approval for the use of devices and/or tools needed for maintenance to update its IoT devices and servers, and conducts monitoring. - The organization inspects the devices and/or tools for maintenance brought in by the staff members who update its IoT devices and servers in order to make sure that no inappropriate or unauthorized changes will be made. - The organization inspects the media used for maintenance to update its IoT devices and servers in order to make sure that the media contain no malicious code before they are used. - The organization introduces an IoT device designed to remotely update different software programs (OS, driver, application) at the same time.
						Advanced	- The organization plans maintenance work such as updating its IoT devices and servers, implements the plan, checks the work done, and documents the entire maintenance. - The organization gives prior approval for maintenance work such as updating its IoT devices and servers, and conducts monitoring. - The organization gives prior approval for travel from its premises for any maintenance work away from its premises, such as updating its IoT devices and servers. It also takes necessary actions before the travel, such as deleting relevant saved data. - The organization checks all security measures that may have been affected by maintenance work, such as updating its IoT devices and servers, after the work is complete in order to make sure that the relevant equipment works correctly. - The organization keeps the records of maintenance work done, such as updating its IoT devices and servers. - The organization establishes a process for authorizing maintenance staff in order to keep the list of authorized maintenance organizations or staff members updated.
				CPS.MA-2	Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.	Advanced	- The organization documents the policy and procedure relating to establishing and implementing a connection designed for remote maintenance, and implements the connection in accordance with the policy and procedure. - The organization provides authentication required for network access that it specifies when remote maintenance is carried out. It also ensures that the session and network connection are terminated when the remote maintenance is complete.
						Basic	- The organization develops and agrees to an implementation plan for remote maintenance before carrying out the maintenance, and checks the results of the maintenance done. - The organization keeps the records of remote maintenance done.
		A.11.2.5 Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	Advanced	- Maintain/manage lists including configuration information of assets (e.g., names, version information, license information, and location) by reviewing and updating them periodically. - The organization makes a list of removable media (e.g., USB memory sticks) that can be used on system components (information system or industrial control system), and manages the use of them. - The organization uses only removable media (e.g. USB memory) permitted in the organization. Also, if there is no identifiable ownwer of portable storage devices, the organization prohibits the use of such devices. - The organization controles access to the media that contain highly confidential data, and properly grasps and manages the usage of the media taken outside of the controlled areas.
				CPS.CM-2	Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.	H-Advanced	The organization tracks and monitors the locations and relocation of important assets within the scope of its management of particularly important assets.
		A.11.2.6 Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	CPS.CM-2	Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.	Advanced	- The organization reviews the relevant audit log regularly or when an incident or a sign of an incident appears if a physical access log from access control is available while 24-h monitoring is not conducted through security cameras or by any other means. - A person in charge accompanies a visitor into the area where the organization's assets that must be protected are directly accessible (e.g., an office) in order to monitor the visitor's behavior. - The organization monitors through security cameras or by other means physical access to its facilities that are vital for its operations and house IoT devices and servers, thereby enabling early detection of any physical security incidents and immediate action. - If the above physical security measures may be difficult to implement for items such as IoT devices and servers that may be critical to the organization's operation because they are in a remote location or for any other reasons, consider using tamper-resistant equipment (CPS.DS-6) or taking any other appropriate measures to enhance the physical security properties of the equipment itself.
		A.11.2.7 Secure disposal or reuse of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	CPS.IP-6	When disposing of an IoT device and server, delete the stored data and the ID (identifier) uniquely identifying the genuine IoT devices and servers as well as important information (e.g., private key and digital certificate), or make them unreadable.	H-Advanced	- The organization defines classifications including security categories of data saved in an IoT device or server to be scrapped, and introduces a mechanism for using the proper technique for deleting data with the strength and integrity needed or making the data unreadable according to the definition.
						Advanced	- The organization establishes a procedure for scrapping its equipment including IoT devices and servers, deletes data saved in the equipment or makes the data unreadable in accordance with the procedure, and makes sure that the action has been done successfully.
						Basic	- The organization deletes data that has been saved in its IoT devices or servers to be scrapped, or makes the data unreadable.
		A.11.2.8 Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	H-Advanced	- The organization regulates service wires and transmission paths that are related to their IoT devices and servers by physical access. - The organization regulates output devices of its system by physical access. - The organization monitors alarms and monitoring devices (e.g., surveillance cameras) for physical intrusions into the areas within the physical security boundaries.
						Advanced	- The organization monitors physical accesses to the areas within the physical security boundaries and regularly reviews the audit log. - The organization keeps the records of visitor's access to the areas within the physical security boundaries and regularly reviews them.
						Basic	- The organization maintains upkeep of the access list for areas where their IoT devices and servers are located and issues permission certificates necessary for access. - The organization defines physical security boundaries at its facilities, and implement access control according to the security requirements of assets placed within the boundaries and the results of risk assessment. - The organization monitors the work of temporarily authorized party within the physical security boundaries, such as by authorized attendants or monitoring cameras.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
		A.11.2.9 Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.	H-Advanced	- The organization regulates service wires and transmission paths that are related to their IoT devices and servers by physical access. - The organization regulates output devices of its system by physical access. - The organization monitors alarms and monitoring devices (e.g., surveillance cameras) for physical intrusions into the areas within the physical security boundaries.
						Advanced	- The organization monitors physical accesses to the areas within the physical security boundaries and regularly reviews the audit log. - The organization keeps the records of visitor's access to the areas within the physical security boundaries and regularly reviews them.
						Basic	- The organization maintains upkeep of the access list for areas where their IoT devices and servers are located and issues permission certificates necessary for access. - The organization defines physical security boundaries at its facilities, and implement access control according to the security requirements of assets placed within the boundaries and the results of risk assessment. - The organization monitors the work of temporarily authorized party within the physical security boundaries, such as by authorized attendants or monitoring cameras.
A.12 Operations security	A.12.1 Operational procedures and responsibilities	A.12.1.1 Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.	CPS.GV-1	Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.	H-Advanced	- While sharing the basic policy with operations used in a conventional IT environment, the organization formulates security policies and operational procedures by fully considering the characteristics of a site on which an IoT device is installed. [Reference] For example, IEC 62443-2-1, a security management standard for industrial automation and control systems (IACS), requires formulation of cyber security policies at an upper level for an IACS environment.
						Advanced	- The organization formulates a series of lower level security policies, such as the policies and implementation procedures of the following individual topics, to support policies at a higher level. a) Access control and authentication b) Physical security measures c) System development and maintenance d) Management of external contractors e) Classification and handling of information - The organization formulates a series of security policies by fully considering the organization's a) business strategies, b) related rules, laws, regulations, and contracts, and c) environments under threats to security to sufficiently reflect the actual situation of the organization. - The organization reviews and updates a security plan according to changes in its a) business strategies, b) related rules, laws, regulations, and contracts, and c) environments under threats to security. [Reference] To formulate a policy at a more detailed level, refer to related standards such as ISO/IEC 27002 for identification of fields which require the policy, and refer to more detailed guidelines.
		A.12.1.2 Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	CPS.IP-1	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	H-Advanced	- Before making changes to IoT devices and servers that are subjects of configuration management, the organization tests and approves these changes as well as creates a document on the changes. - The organization uses an automated mechanism to manage, apply, and confirm settings of IoT devices and servers from a single location. - The organization integrates security change management procedures particularly for industrial control systems, into existing process safety management procedures.
						Advanced	- When changes are made to the IoT devices and servers that are subjects of configuration management, the organization analyzes the impact the change has on security, decides whether the change can be made or not, and creates a document on the procedure. - The organization limits personnel who can make changes to approved IoT devices and servers (restricted access). - The organization makes changes to approved IoT devices and servers, as well as implements, records, and monitors those changes. - The organization uses a secure recovery method (e.g. entering a security code known only to the user before the change is implemented) if they forget the password of their accounts, IoT device and servers. - The organization regularly reviews policies and procedures for operation and change management to ensure that changes do not adversely affect the availability or safety of information system and industrial control system.
						Basic	- Upon determining the most restrictive setting criteria that conform to their operation, the organization creates a document on the initial setting procedures and setting details for the IoT devices and servers that will be introduced and adjusts the settings according to the document. - The organization checks initial setting values of IoT devices before installing them, and adjusts the settings appropriately if they do not comply with the policy stipulated in CPS.AC-1. - The organization checks and records software installed in IoT devices before introducing them.
		A.12.1.3 Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	CPS.DS-6	Secure sufficient resources (e.g., People, Components, system) for components and systems, and protect assets property to minimize bad effects under cyber attack (e.g., DoS attack).	Advanced	- The information system and industrial control system manage spare storage space, bandwidth, and other spares (People, Components, System) and minimize the impact of service denial attacks that send a large amount of information. For example, if services provided by an attacked system can not be stopped due to maintaining the level of availability, etc., in order to continue important functions, it is necessary to take the following measures. - Automatic or manual migration to standby system - Automatic or manual segregation of system components attacked by adversal actor - In order to ensure that required system performance is satisfied, use of resources must be monitored and adjusted. In addition, storage capacity and performance required in the future must be pre-estimated. - The organization shall: (a) Use a monitoring tool which the organization specifies in order to find signs of service jamming attacks on the information system. (b) Monitor resources of information system and industrial control system identified by the organization and judge whether sufficient resource is secured to prevent effective service jamming attacks.
				CPS.DS-7	Carry out periodic quality checks, prepare standby devices and uninterruptible power supplies, provide redundancy, detect failures, conduct replacement work, and update software for IoT devices, communication devices, circuits, etc.	Advanced	- The organization prepares short-term uninterrupted power supply which supports the switching of the information system to an alternative power source that can be used for a long period of time when the primary power source is lost.
						Basic	- In order to ensure that required performance of an information system and an industrial control system is satisfied, use of resources must be monitored and adjusted. In addition, storage capacity and performance that are required in the future are pre-estimated. - The organization protects devices from power outages and other failures that are attributable to malfunctions in the support utility. - The organization protects communication cables and power cables that transmit data or that support information service from interception, interference, and harm. - The organization properly maintaines devices to ensure continuous availability and integrity.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
		A.12.1.4 Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).	H-Advanced	- The information system and the industrial control system monitor and control communications on the networks composing internal business systems of the organization. - Regarding the network which the system that handles highly confidential data is connected to, the organization shall deny network communications as a default and shall only allow connection of approved communication traffic. - The organization physically or logically separates the network of high importance industrial control systems from the network of control systems with lower importance. - If the information system that handles highly confidential data is connected to a remote device, the organization is to prevent multiple and simultaneous local connections between the device and the system, as well as prevent access to external network resources by other connections.
						Advanced	- The information system and industrial control system monitor and regulate connection of external and internal boundaries of the network to which the system is connected (in the case of industrial control systems, boundaries with information systems). - The organization installs boundary protection devices to promote effective security in the system and connects to external networks via the device.
						Basic	- The organization establishes a data flow regulation policy that defines the range in which data flow within information systems and industrial control system is permitted and the range in which data flow between systems is permitted, and regulates the flow by segregating the network appropriately. - The organization logically or physically segments the control system's network from the network composing of the information system. [Reference] Implement physical segmentation in environments physically separated from other networks. Alternatively, in environments physically close to other networks, it is possible to implement logical segmentation in consideration of the cost of the measure.
	A.12.2 Protection from malware	A.12.2.1 Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	CPS.DS-10	Conduct integrity checks of software runnning on the IoT devices and servers at a time determined by the organization, and prevent unauthorized software from launching.	H-Advanced	- The organization uses an automated tool that notifies the information system administrator when an inconsistency is found during integrity verification. - The organization uses tools to prevent the launch of the software if malicious software is detected. - The organization incorporates detection capacity into its incident response capacity to detect unauthorized changes that are made to the settings and security, such as an unauthorized promotion of system authority.
						Advanced	- The information system regularly inspects the integrity of the software and firmware. - The information system and the industrial control system prevent activation of unregistered software by registering in advance software that is permitted to activate.
				CPS.CM-3	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.	H-Advanced	- IoT devices, or systems that contain these devices, examine information output from software programs or applications to see if it matches the expected content in order to prepare for certain attacks that may have a consequence different to a normally expected outcome (e.g., command injection). - The information system automatically updates the logic to detect malicious code through an IDS/IPS. - The information system detects exploit codes that attacks unknown vulnerabilities by installing on endpoints (especially, IoT devices and servers with various functions) detection/restoration software using technologies of behavioral detection of malware. - The information system executes real-time scanning of files from external sources.
						Advanced	- The information system blocks or isolates any malicious code for it detected through an IDS/IPS, or notifies the administrator of the code. - The information system detects exploit codes by installing on endpoints (IoT devices, servers, and so on) detection/restoration software using technologies of pattern matching of malware. - The organization considers implementing whitelist-type malware protection for IoT devices with limited functions. * Especially regarding IoT devices and control devices, OS to which anti-malware software can be applied may not be used. It is desirable for the organization to confirm whether devices to be introduced are compatible with anti-malware software at the phase of procurement and to select compatible ones. If it is difficult to procure devices compatible with anti-malware software, it is desirable to take alternative measures such as introducing/strengthening a malware detection mechanism on a network.
	A.12.3 Backup	A.12.3.1 Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	CPS.BE-3	Identify the dependency between the organization and other relevant parties and the important functions of each in the course of running the operation.	H-Advanced	- The organization identifies the functions of the following support utilities for the continuation of its business and the dependence relationship between them. - Communication service - Electrical power equipment (including power cables) - Among the above identified utilities, for those which have important roles for the continuation of its business, the organization examines the possibility of taking measures as follows: - Establishment of alternative communication services - Physical protection of electrical power equipment and power cables - Preparation of short-term permanent power supply equipment - When examining the possibility of using an alternative communication service, the organization considers the following: - Identify the requirements on the availability of the organization (including the target recovery time) when examining a contract with a communication service provider. - Reduce the possibility of sharing a single point of failure with a primary communication service.
						Advanced	- The organization identifies the requirements for the capacity/capability of an applicable system according to the requirements for its availability stipulated in CPS.AM-6. - In order to fulfill the required system performance, the organization monitors/adjusts the use of resources in the information systems and industrial control systems in operation, and pre-estimates the storage capacity/performance required in the future.
				CPS.IP-4	Perform a periodical system backup and testing of components (e.g., IoT devices, communication devices, and circuits).	H-Advanced	- The organization confirms the trustworthiness of the medium and integrity of the information by regularly testing the backup information.
						Advanced	- The organization backs up their system documents according to the prescribed timing and frequency. - The organization protects the confidentiality, integrity, and availability of the information backed up on the storage base.
						Basic	- The organization backs up information on user level and system level that is included in its information systems or industrial control systems according to the prescribed timing and frequency.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	A.12.4 Logging and monitoring	A.12.4.1 Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	CPS.SC-8	Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.	H-Advanced	- The organization uses a trail storage system with the following features to flexibly fulfill the needs of clients and other related organizations, such as a third-party auditing institution, on a real-time basis. - Eligibility of the subject audit trail for the contract matter can be verified quickly. - Only authorized entities such as clients and outsourced auditing agencies can access the system. - Stored data has reliable trails such as time stamps and electronic signatures.
						Advanced	- The organization takes measures so that those records among the audit records generated by the system that are acquired over a long period of time can be obtained with certainty. - In order to protect audit records from the following threats, it is desirable for the system to apply access control with high granularity to the items and systems in which audit records are stored. - Change format of recorded message - Change or delete log file - Exceed storage space of log file medium
						Basic	- The organization preserves audit records for an appropriate period of time so as to satisfy the requirements of laws and regulations.
				CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	H-Advanced	- In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g. OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related audit logs for some of the IoT devices that an organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specs of the IoT devices, such as using a log management system different than the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.
						Advanced	- The information system and the industrial control system uses a cryptographic mechanism in order to ensure the integrity of an audit log and audit tool each. - The organization grants control over an audit log only to users assigned in accordance with the rules about security-related internal responsibility. - The information system issues an alert when an incident of failure takes place in the audit process.
						Basic	- The organization specifies what is to be audited based on its risk management strategy and risk assessment results, and sees if the systems can acquire audit logs that show who did what and when in connection with the subjects of an audit. - The system generates an audit log prescribed from various system components. - The organization reviews and analyze a system's audit log regularly to see if there are any signs of security incidents that may cause damage to the organization, and make a report to the system administrator where necessary. - The organization confirms that the impact of audit activities on the performance of industrial control systems is tolerable.
				CPS.AE-2	Appoint a chief security officer, establish a security management team (SOC/CSIRT), and prepare a system within the organization to detect, analyze, and respond to security events.	H-Advanced	- The organization efficiently analyzes audit logs collected through 24-h, 365-day security monitoring by using an automated analysis tool. - It is desirable for the organization to include not only its conventional IT environment but also its control system and IoT devices in the scope of security monitoring. - It is desirable for the organization to regularly evaluate the maturity of its security measure organizations in order to continue improving its security-related operations, including security monitoring and the ways incidents are handled. [Reference] For example, SIM3 (Security Incident Management Maturity Model) is available as metrics for the evaluation of security organizations (SOC/CSIRT).
						Advanced	- The organization refers to risk assessment results and, considering the following angles, establishes what to monitor and what to include in correlation analysis. - The scope of systems to monitor - Which device logs should be collected for analysis (see CPS.AE-3) - The organization regularly reviews audit logs collected through monitoring. - The organization continues to collect and manage information about assets, device configurations, and network configurations in order to evaluate its security status. - The organization examines the results of correlation analysis and other data to accurately detect security events that must be addressed and take action in accordance with the security operation process. See CPS.RP-1 for details of the process. - The organization regularly reports the state of organizational and system security to the chief security officer or other appropriate staff members. It is desirable that the regular report should include the following shown below: - Results of log analysis (e.g., the number of incidents handled; summaries of typical incidents that have been handled; threats that have emerged; issues in monitoring); - Policy for future improvements in monitoring.
				CPS.AE-3	Identify the security events accurately by implementing the procedure to conduct a correlation analysis of the security events and comparative analysis with the threat information obtained from outside the organization.	H-Advanced	- The organization conducts a trend analysis examining the latest information about threats, vulnerability, and assessments of security management measures carried out several times in order to determine whether the activities for continuous monitoring need any correction. - The organization carries out policy tuning (management of signatures to apply) and maintenance for devices such as IDS, IPS, and SIEM on its own. - The organization creates custom signatures used for sensors on its own. - In order to properly detect security events that are likely to adversely affect the organization, the organization collects and analyzes logs of edge devices such as IoT devices in addition to the logs of devices presented in <Advanced>, if possible.
						Advanced	- It is desirable that the organization should monitor mainly logs of the devices listed below for real-time analysis to appropriately detect security events highly likely to have an adverse effect on its own organization . This will require the handling of many different logs. Hence, it is necessary to normalize logs to store them in the same database or to use SIEM for efficient analysis. It is also advisable to handle information about network flows if it is available. - Logs and network flows from network systems, e.g., firewalls - Logs from security devices, e.g., IPS/IDS - Access logs of web servers - Logs from various systems, e.g., ActiveDirectory; DNS - Logs related to users' terminals
						Basic	- The organization checks each notice from firewalls and endpoint security products in order to identify security events that may have an adversal impact on the organization.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.DP-1	Clarify the role and responsibility of the organization as well as service providers in detecting security events so that they can fulfill their accountabilities.	Basic	- The organization determines the log information that would help detect security events and thus should be collected based on its strategies relating to risk management and assessment results. - The organization ascertains that its business partner (service provider) has an audit log that records activity of service users, exception handling, and security events that the provider has acquired. - The organization ascertains that the audit log acquired by its service provider records activity of service users, exception handling, and security events, and is protected in a proper way.
		A.12.4.2 Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	H-Advanced	- In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g. OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related audit logs for some of the IoT devices that an organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specs of the IoT devices, such as using a log management system different than the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.
						Advanced	- The information system and the industrial control system uses a cryptographic mechanism in order to ensure the integrity of an audit log and audit tool each. - The organization grants control over an audit log only to users assigned in accordance with the rules about security-related internal responsibility. - The information system issues an alert when an incident of failure takes place in the audit process.
		A.12.4.3 Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	H-Advanced	- In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g. OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related audit logs for some of the IoT devices that an organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specs of the IoT devices, such as using a log management system different than the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.
						Advanced	- The information system and the industrial control system uses a cryptographic mechanism in order to ensure the integrity of an audit log and audit tool each. - The organization grants control over an audit log only to users assigned in accordance with the rules about security-related internal responsibility. - The information system issues an alert when an incident of failure takes place in the audit process.
						Basic	- The organization specifies what is to be audited based on its risk management strategy and risk assessment results, and sees if the systems can acquire audit logs that show who did what and when in connection with the subjects of an audit. - The system generates an audit log prescribed from various system components. - The organization reviews and analyze a system's audit log regularly to see if there are any signs of security incidents that may cause damage to the organization, and make a report to the system administrator where necessary. - The organization confirms that the impact of audit activities on the performance of industrial control systems is tolerable.
		A.12.4.4 Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	H-Advanced	- In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g. OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related audit logs for some of the IoT devices that an organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specs of the IoT devices, such as using a log management system different than the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	A.12.5 Control of operational software	A.12.5.1 Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	CPS.IP-1	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	H-Advanced	- Before making changes to IoT devices and servers that are subjects of configuration management, the organization tests and approves these changes as well as creates a document on the changes. - The organization uses an automated mechanism to manage, apply, and confirm settings of IoT devices and servers from a single location. - The organization integrates security change management procedures particularly for industrial control systems, into existing process safety management procedures.
						Advanced	- When changes are made to the IoT devices and servers that are subjects of configuration management, the organization analyzes the impact the change has on security, decides whether the change can be made or not, and creates a document on the procedure. - The organization limits personnel who can make changes to approved IoT devices and servers (restricted access). - The organization makes changes to approved IoT devices and servers, as well as implements, records, and monitors those changes. - The organization uses a secure recovery method (e.g. entering a security code known only to the user before the change is implemented) if they forget the password of their accounts, IoT device and servers. - The organization regularly reviews policies and procedures for operation and change management to ensure that changes do not adversely affect the availability or safety of information system and industrial control system.
						Basic	- Upon determining the most restrictive setting criteria that conform to their operation, the organization creates a document on the initial setting procedures and setting details for the IoT devices and servers that will be introduced and adjusts the settings according to the document. - The organization checks initial setting values of IoT devices before installing them, and adjusts the settings appropriately if they do not comply with the policy stipulated in CPS.AC-1. - The organization checks and records software installed in IoT devices before introducing them.
				CPS.IP-2	Restrict the software to be added after installing in the IoT devices and servers.	H-Advanced	- The organization restricts software by using a list of software that is permitted to be executed on the information system and industrial control system (whitelist) or list of prohibited software (blacklist). Or, unpermitted software shall not be installed.
	A.12.6 Technical vulnerability management	A.12.6.1 Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	CPS.RA-1	Identify the vulnerability of the organization's assets and document the list of identified vulnerability with the corresponding asset.	H-Advanced	- The organization conducts vulnerability diagnosis at planned timings such as planned stopping so as not to adversely affect the operation of the system managed by the organization. And then, identify and list vulnerabilities that exist in the system owned by the organization. - It is desirable to conduct a penetration test periodically to recognize an existing vulnerability in a system it manages. - When conducting vulnerability diagnosis, it is desirable to use a vulnerability diagnosis tool that can immediately update the vulnerability of the system to be diagnosed. - The organization develops mechanisms to temporarily permit privileged access to a inspector in vulnerability diagnosis to more thoroughly identify vulnerabilities.
						Advanced	- The organization carries out a vulnerability diagnosis to recognize vulnerabilities existing in the information system which has high importance and makes a list of them. - In the operation phase of an information system owned by the organization, the organization uses a vulnerability diagnosis tool to periodically identify its system vulnerability within vulnerabilities collected from various sources, which are supposed to be related to the organization. The organization shall add the identified vulnerability and its impact degree to a list. [Reference] Japan Vulnerability Notes (https://jvn.jp/) and other sources of information are available for reference to obtain information regarding vulnerability. Also, CVSS (https://www.ipa.go.jp/security/vuln/CVSS.html Illustrated by IPA) could be used as a referential indicator to evaluate the impact level of vulnerability.
				CPS.RA-4	- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation. - Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.	H-Advanced	- When developing a new device or a new component which may have an impact on a physical space such as components of an industrial control system, the organization collects/analyzes accident case studies of conventional products and others to identify safety-related hazards. - The organization analyzes a situation where a hazard leads to harm and identifies the possibility of occurrence and the severity of the harm to estimate a possible risk especially regarding an industrial control system. At the time, it is desirable to check whether there is any hazard caused by a security issue. - The organization updates the risk assessment if there is a significant change in the industrial control system or the environment in which it operates, or the other change that affects the security state of the industrial control system.
						Advanced	- The organization updates a risk assessment when there is a big change in a system or an environment where a system is running (including identification of a new threat or vulnerability) or when any situation which impacts the security status of a system occurs. - When planning/designing a new system using an IoT device, the organization identifies existing assets and assets to be protected in the system to be implemented and organizes security measures according to use and configuration of the system. When handling a component or a system with a long life cycle and a component or a system requiring availability, consideration in security measures at a phase before designing is especially important. - When considering security measures applied to purchased products and services, the organization makes sure that the levels of measures correspond to the importance of such products and services.
				CPS.RA-5	Consider threats, vulnerability, likelihood, and impacts when assessing risks.	Advanced	- The organization updates a risk assessment when there is a big change in an information system or an environment where an information system is running (including identification of a new threat or vulnerability) or when any situation which impacts the security status of a system occurs. In that case, give priority to an information system or industrial control system with high importance. * Implementation details common to CPS.RA-4
				CPS.IP-10	Develop a vulnerability remediation plan, and modify the vulnerability of the components according to the plan.	H-Advanced	- The organization adopts and administers an automated mechanism for managing the status of defect correction.
						Advanced	- The organization defines tolerable risk by identifying through investigations and tests the impacts of patch application on the functions of other software applications and services on operations of IoT devices and servers. - The organization conducts tests to measure the effectiveness of corrections and the possibility of any secondary adverse effects, corrects the defects, and manages the corrections as part of the configuration management.
						Basic	- The organization systematically identifies, reports and responds to vulnerabilities in its own information systems and industrial control systems. The organization considers the following when formulating a plan. - Seriousness of threats or vulnerabilities - Risk in responding to vulnerabilities [Reference] It may be difficult to carry out application of security patches in a timely manner or application of patches itself to IoT devices in consideration of availability and functions of devices. In such cases, it is desirable to avoid occurrence of security incidents by thoroughly taking measures against threats (e.g. minimization of functions, strengthening of network monitoring).

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.CM-7	Confirm the existence of vulnerability that requires a regular check-up in IoT devices and servers managed within the organization.	H-Advanced	- The organization conducts vulnerability diagnosis at planned timings such as planned stopping so as not to adversely affect the operation of the system managed by the organization. And then, identify and list vulnerabilities that exist in the system owned by the organization. - When using tools to conduct vulnerability diagnosis, the organization should use tools that can quickly update the vulnerability database of the system being diagnosed. - The organization updates the vulnerability of scanned systems regularly, or when newly-identified weaknesses are reported. - The organization implements a system for authorizing privileged access to the relevant system components in connection with the specified vulnerability scanning.
						Advanced	- The organization has its systems and applications scanned for vulnerability regularly, or when any newly-found weaknesses that affect the systems and/or applications are reported. - The organization uses a tool for vulnerability scanning. Applying the standard methods that meet the following means that part of the vulnerability management process should be open to automation. - List defects in the platform and software, and wrong setups. - Format a checklist and test procedure. - Assess the impact of the vulnerability. - The organization corrects identified weaknesses through risk assessment within an appropriate period. - The organization shares the information acquired through the above process with other system administrators in the organization, thereby learning about similar weaknesses found in the other information systems, and correct them as necessary. [Reference] Japan Vulnerability Notes (https://jvn.jp/) and other sources of information are available for reference to obtain information regarding vulnerability. Also, CVSS (https://www.ipa.go.jp/security/vuln/CVSS.html Illustrated by IPA) could be used as a referential indicator to evaluate the impact level of vulnerability.
						Basic	- The organization regularly has its systems and applications scanned for vulnerability.
		A.12.6.2 Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	CPS.IP-2	Restrict the software to be added after installing in the IoT devices and servers.	H-Advanced	- The organization restricts software by using a list of software that is permitted to be executed on the information system and industrial control system (whitelist) or list of prohibited software (blacklist). Or, unpermitted software shall not be installed.
						Advanced	- The organization adopts and manages a mechanism that manages software installation that is performed by users on the organization's system (information system or industrial control system) and monitors the events.
						Basic	- The organization establishes a policy on software installation performed by users on the organization's system (information system or industrial control system) and has the users follow it.
	A.12.7 Information systems audit considerations	A.12.7.1 Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	CPS.SC-6	Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	H-Advanced	- The organization adopts an automatic mechanism integrating review, analysis, and report that supports the investigation and addresses procedures for deviation or signs of deviation from contract matters. - The organization uses a mechanism that allows it to list and check whether obligatory matters stipulated in the contract are fulfilled, matters which are concerned with security management of the organization and security functions implemented in the products and services that will be delivered, especially for important clients and reconsigned organizations. - State of compliance with security management measures of the external service provider is regularly checked by external audits and field surveys conducted by the outsourcer. - The important business partners and if possible their re-contractors etc. investigate whether there is any sign of attack related or any fact of information leakage, and regularly report the result to the organization.
						Advanced	- The organization checks whether requirements that are prescribed in the contract with the client can be audited on the system. - The information system provides a function that allows for audit records to be created for events defined above that can be audited on the system. - The organization shall be able to maintain consistency in security audits with other organizations that require information on the audit. - The organization regularly reviews and analyzes audit records that are made manually or automatically by the system, and checks whether there is any deviation or sign of deviation from contract matters. - State of compliance with security management measures of the external service provider is regularly checked by internal audits that are conducted by the client using a checklist.
				CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	H-Advanced	- In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g. OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related audit logs for some of the IoT devices that an organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specs of the IoT devices, such as using a log management system different than the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.
						Advanced	- The information system and the industrial control system uses a cryptographic mechanism in order to ensure the integrity of an audit log and audit tool each. - The organization grants control over an audit log only to users assigned in accordance with the rules about security-related internal responsibility. - The information system issues an alert when an incident of failure takes place in the audit process.
						Basic	- The organization specifies what is to be audited based on its risk management strategy and risk assessment results, and sees if the systems can acquire audit logs that show who did what and when in connection with the subjects of an audit. - The system generates an audit log prescribed from various system components. - The organization reviews and analyze a system's audit log regularly to see if there are any signs of security incidents that may cause damage to the organization, and make a report to the system administrator where necessary. - The organization confirms that the impact of audit activities on the performance of industrial control systems is tolerable.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
A.13 Communications security	A.13.1 Network security management	A.13.1.1 Network controls	Networks shall be managed and controlled to protect information in systems and applications.	CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).	H-Advanced	- The information system and the industrial control system monitor and control communications on the networks composing internal business systems of the organization. - Regarding the network which the system that handles highly confidential data is connected to, the organization shall deny network communications as a default and shall only allow connection of approved communication traffic. - The organization physically or logically separates the network of high importance industrial control systems from the network of control systems with lower importance. - If the information system that handles highly confidential data is connected to a remote device, the organization is to prevent multiple and simultaneous local connections between the device and the system, as well as prevent access to external network resources by other connections.
						Advanced	- The information system and industrial control system monitor and regulate connection of external and internal boundaries of the network to which the system is connected (in the case of industrial control systems, boundaries with information systems). - The organization installs boundary protection devices to promote effective security in the system and connects to external networks via the device.
				CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).	H-Advanced	- The information system and industrial control system require authentication using a public key infrastructure (PKI) , especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions. [Reference] For the strength of authentication schemes and appropriate use cases, it is advisable to refer to NIST SP 800-63-3.
						Advanced	- The organization checks the user's identity and authenticates using a mechanism that has sufficient strength for the risk of the transaction (security-related risks for the user, privacy risks, etc.). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - The organization sets the expiration date of the credential and manages whether the password over the expiration date is used.
				CPS.DS-3	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.	H-Advanced	- The organization protects th networks composing the information system and industrial control system that handles important data by implementing encrytion of communication channels or by alternative physical measures.
						Advanced	- The information system employs an cryptographic mechanism and encrypt communciation paths. [Reference] For encryption of communication paths, there are several methods such as IP-VPN, Ipsec-VPN, SSL VPN. It is desirable that the organization should select the method considering the importance of the data transmitted in the communication paths, the budget, and so on.
				CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	H-Advanced	- In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g. OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related audit logs for some of the IoT devices that an organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specs of the IoT devices, such as using a log management system different than the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.
						Basic	- The organization specifies what is to be audited based on its risk management strategy and risk assessment results, and sees if the systems can acquire audit logs that show who did what and when in connection with the subjects of an audit. - The system generates an audit log prescribed from various system components. - The organization reviews and analyze a system's audit log regularly to see if there are any signs of security incidents that may cause damage to the organization, and make a report to the system administrator where necessary. - The organization confirms that the impact of audit activities on the performance of industrial control systems is tolerable.
		A.13.1.2 Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	CPS.SC-4	When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	H-Advanced	- The organization or a third party tests the procured devices to see whether the security requirements stipulated in the contract are fulfilled. - The organization checks throughout the entire relevant supply chain (including reconsigned organizations) as to whether the devices especially important for their operation are manufactured under appropriate procedures by organizations that have quality and security management ability above a certain level.
						Advanced	- The organization specifies in the contract the security requirements that the products and services procured from the partner should comply with, such as the following. - Specific certifications related to security (e.g., ISMS certification、ISASecure EDSA certification, Japan Information Technology Security Evaluation and Certification Scheme (JISEC) have been gained. - The vendor itself confirms that it has implemented the security measures in accordance with the standards of specific certifications related to security - It has implemented the necessary security requirements from the design phase (security by design) based on the results of risk analysis, etc., and test them. - It is desirable that the organization should, at the phase of planning procurement, secure a budget for security requirements regarding products or services themselves, or protection of assets used for procurement and supply of such products or services. - The organization formulates, manages and improves security measurement rules to evaluate procurement or supply of products or services, including the following. - Target for measurement - Method and frequency of reporting on measures taken - Measures to be taken when measures are not implemented - The organization checks means of detecting (or preventing) falsifications and leakages during shipments and whether or not the IoT devices and software being delivered have been operated without authorization. - Goods: security courier, protection seal, etc. - Digital transfer: encryption, hash of the entire transmitted data, etc.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.CM-5	Monitor communication with external service providers so that potential security events can be detected properly.	H-Advanced	- The organization requires its provider of external information system services to make clear the functions, ports, and protocols needed for the use of the services, along with other services. - The organization monitors whether the matters made clear as stated above are observed.
						Advanced	- The organization documents its security requirements for the staff from its external service provider and system developer, and includes the requirements in the agreement. - The organization requires its external service provider and system developer to contact it when any of its staff members who have authorizations for its system are transferred or when their employment terminates. - It is desirable that the organization should manage changes to services offered by its external service provider, taking account of relevant information about operations, the importance of its business systems and processes, and re-assessed risks. - The organization monitors whether its external service provider and system developer complies with the requirements. - The organization monitors access to its system by its external service provider and system developer in order to detect any unauthorized access by these external businesses that results from an action or failure to act. - The organization reports the results of the monitoring of activities by its external service provider and system developer to the appropriate system administrator.
						Basic	- The organization requires its provider of external information system services and system developer to draw up and introduce security requirements such as those related to the following in accordance with the rules which the organization is subject to or which apply to the provider and developer. - Adequate security measures to take (e.g., measures that deserve ISMS Certification) - Proper management of data in operation - Proper data erasure when the use of the services ends
		A.13.1.3 Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).	H-Advanced	- The information system and the industrial control system monitor and control communications on the networks composing internal business systems of the organization. - Regarding the network which the system that handles highly confidential data is connected to, the organization shall deny network communications as a default and shall only allow connection of approved communication traffic. - The organization physically or logically separates the network of high importance industrial control systems from the network of control systems with lower importance. - If the information system that handles highly confidential data is connected to a remote device, the organization is to prevent multiple and simultaneous local connections between the device and the system, as well as prevent access to external network resources by other connections.
						Advanced	- The information system and industrial control system monitor and regulate connection of external and internal boundaries of the network to which the system is connected (in the case of industrial control systems, boundaries with information systems). - The organization installs boundary protection devices to promote effective security in the system and connects to external networks via the device.
	A.13.2 Information transfer	A.13.2.1 Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	CPS.AM-4	Create and manage appropriately network configuration diagrams and data flows within the organization.	H-Advanced	- The organization implements/manages an automated mechanism for monitoring and managing system configurations, communication network configurations, and data flows of their information systems and industrial control systems in real time.
						Advanced	- The organization states the characteristics of the interface, security requirements, and characteristics of transmitted data for network connection in a diagram in the associated documents.
						Basic	- The organization documents and stores system configurations, communication network configurations, and data flows of an information systems and an industrial control systems in a range managed by the organization (for example, in units of business establishments). - The organization reviews related documents periodically or when there is a change in system configurations, network configurations, or data flows and updates them as necessary.
				CPS.AM-5	Create and manage appropriately a list of external information systems where the organization's assets are shared.	H-Advanced	- The system makes a list of external information services in use and manages the users, devices as well as serviced in use in real time. - The system uses a mechanism to give notice to the system administrator when an unpermitted external information system service is detected. - The organization identifies functions, ports, protocols, and other services which are necessary for using services offered by external providers.
						Advanced	- The organization sets conditions for allowing other organizations which own or operate external information systems to do the following: a. Accessing an information system in the organization from an external information system b. Processing, saving, or transmitting information under the control of the organization using an external information system - The organization restricts a use of storage in an external system the organization owns to an authorized one.
				CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).	H-Advanced	- The information system and the industrial control system monitor and control communications on the networks composing internal business systems of the organization. - Regarding the network which the system that handles highly confidential data is connected to, the organization shall deny network communications as a default and shall only allow connection of approved communication traffic. - The organization physically or logically separates the network of high importance industrial control systems from the network of control systems with lower importance. - If the information system that handles highly confidential data is connected to a remote device, the organization is to prevent multiple and simultaneous local connections between the device and the system, as well as prevent access to external network resources by other connections.
						Advanced	- The information system and industrial control system monitor and regulate connection of external and internal boundaries of the network to which the system is connected (in the case of industrial control systems, boundaries with information systems). - The organization installs boundary protection devices to promote effective security in the system and connects to external networks via the device.
						Basic	- The organization establishes a data flow regulation policy that defines the range in which data flow within information systems and industrial control system is permitted and the range in which data flow between systems is permitted, and regulates the flow by segregating the network appropriately. - The organization logically or physically segments the control system's network from the network composing of the information system. [Reference] Implement physical segmentation in environments physically separated from other networks. Alternatively, in environments physically close to other networks, it is possible to implement logical segmentation in consideration of the cost of the
				CPS.DS-3	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.	H-Advanced	- The organization protects th networks composing the information system and industrial control system that handles important data by implementing encrytion of communication channels or by alternative physical measures.
						Advanced	- The information system employs an cryptographic mechanism and encrypt communciation paths. [Reference] For encryption of communication paths, there are several methods such as IP-VPN, Ipsec-VPN, SSL VPN. It is desirable that the organization should select the method considering the importance of the data transmitted in the communication paths, the budget, and so on.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.DS-4	Encrypt information itself when sending/receiving information.	H-Advanced	- The system /IoT apparatus introduces the code module which it can implement without even little resource losing availability, and it is desirable to encrypt the communication data from a high apparatus of the importance at appropriate strength. - The information system encrypts all data transmitted outside the organization with appropriate strength, not limited to high or low importance.
						Advanced	- The organization encrypts information with appropriate strength when transmitting highly confidential information to an external organization or the like.
				CPS.CM-4	Validate the integrity and authenticity of the information provided from cyberspace before operations.	H-Advanced	- The organization introduces the concept of "whitelisting" for data entry in order to specify known items and systems considered trustworthy as the sources of input data, and the format allowed for the input data. - IoT devices and servers begin communication with other IoT devices only after the devices are mutually authenticated successfully so that the source of data is always clear. - The information system and the industrial control system protect the authenticity of communications sessions.
						Advanced	- The information system uses an integrity verification tool to detect any unauthorized changes that are made to communications data transmitted from IoT devices and servers. - IoT devices and servers that are acknowledged as critical to the organization's operations begin communication with other IoT devices only after the devices are mutually authenticated successfully so that the source of data is always clear.
		A.13.2.2 Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	CPS.AM-4	Create and manage appropriately network configuration diagrams and data flows within the organization.	H-Advanced	- The organization implements/manages an automated mechanism for monitoring and managing system configurations, communication network configurations, and data flows of their information systems and industrial control systems in real time.
						Advanced	- The organization states the characteristics of the interface, security requirements, and characteristics of transmitted data for network connection in a diagram in the associated documents.
						Basic	- The organization documents and stores system configurations, communication network configurations, and data flows of an information systems and an industrial control systems in a range managed by the organization (for example, in units of business establishments). - The organization reviews related documents periodically or when there is a change in system configurations, network configurations, or data flows and updates them as necessary.
				CPS.DS-1	If the organization exchanges protected information with other organizations, agree in advance on security requirements for protection of such information.	Advanced	- The organization specifies concrete security measure requirements considering importance of exchanged data and assumed risks, and requires business partners to implent them. - The organization permits outsourcing of data handling operation to subcontractors only if it confirms that such subcontractors have implemented security measures whose level is equivalent to those required to direct business partners.
						Basic	- The organization regulate how to handle the data that business partners may handle by concluding a non-disclosure agreement. - The organization prohibits direct business partners from subcontracting operations related to data management.
		A.13.2.3 Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	CPS.DS-3	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.	H-Advanced	- The organization protects th networks composing the information system and industrial control system that handles important data by implementing encrytion of communication channels or by alternative physical measures.
						Advanced	- The information system employs an cryptographic mechanism and encrypt communciation paths. [Reference] For encryption of communication paths, there are several methods such as IP-VPN, Ipsec-VPN, SSL VPN. It is desirable that the organization should select the method considering the importance of the data transmitted in the communication paths, the budget, and so on.
				CPS.DS-4	Encrypt information itself when sending/receiving information.	H-Advanced	- The system /IoT apparatus introduces the code module which it can implement without even little resource losing availability, and it is desirable to encrypt the communication data from a high apparatus of the importance at appropriate strength. - The information system encrypts all data transmitted outside the organization with appropriate strength, not limited to high or low importance.
						Advanced	- The organization encrypts information with appropriate strength when transmitting highly confidential information to an external organization or the like.
				CPS.CM-4	Validate the integrity and authenticity of the information provided from cyberspace before operations.	H-Advanced	- The organization introduces the concept of "whitelisting" for data entry in order to specify known items and systems considered trustworthy as the sources of input data, and the format allowed for the input data. - IoT devices and servers begin communication with other IoT devices only after the devices are mutually authenticated successfully so that the source of data is always clear. - The information system and the industrial control system protect the authenticity of communications sessions.
						Advanced	- The information system uses an integrity verification tool to detect any unauthorized changes that are made to communications data transmitted from IoT devices and servers. - IoT devices and servers that are acknowledged as critical to the organization's operations begin communication with other IoT devices only after the devices are mutually authenticated successfully so that the source of data is always clear.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
		A.13.2.4 Confidentiality or nondisclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	CPS.SC-3	When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	H-Advanced	- In a contract with a business partner who provides systems/components/services, the organization requires the partner the following listed below: - Create evidence of the implementation of the security assessment plan, and submit results of security tests/evaluations. - Develop a plan for remedying defects identified during security testing / evaluation - Disclose a plan for defect remediation and its implementation status - It is desirable that the organization applies necessary requirements among those for security measures to directly consigned parties and accompanying requirements to reconsigned parties by considering the scales of risks originating from the supply chains.
						Advanced	- In accordance with the missions/business needs of the organization, state the following requirements, descriptions, and criteria in a procurement contract of a system, component, or service. - Requirements for security measures - Requirements for security-related documents - Requirements for protection of security-related documents - Confidentiality clauses - Implementation body and method of each handling: reporting destination at the time of incident occurrence, reporting details, initial reaction, investigation, recovery, etc. - Conditions to allow to confirm the observance to the security requirement which is inspected and defined by the organization or the authorized third party. - How to handle an information asset at the end of the contract - The organization requires business partners, in a procurement contract, to implement security requirements that comply with applicable laws and regulations, implement additional measures when they are recognized necessary because of the characteristics of the contracted duty, etc. - It is desirable to consider the following items in advance when determining security requirements based on laws and regulations and requiring business partners to comply with them. - Identification of potential risks in terms of legal regulations that may arise due to difference of applicable laws between the organization and the business partner - Negative impacts on the contract in terms of security due to legal and regulatory obligations applicable to the business partner
						Basic	- The organization requires business partners to implement security requirements that complies with applicable laws and regulations. - The organization confirms that the business partner has declared "SECURITY ACTION" in the process of selecting and evaluating a contractor. * "SECURITY ACTION" is an initiative in Japan that small and medium-sized enterprises declare themselves to work on information security measures.
A.14 System acquisition, development and maintenance	A.14.1 Security requirements of information systems	A.14.1.1 Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	CPS.SC-4	When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	H-Advanced	- The organization or a third party tests the procured devices to see whether the security requirements stipulated in the contract are fulfilled. - The organization checks throughout the entire relevant supply chain (including reconsigned organizations) as to whether the devices especially important for their operation are manufactured under appropriate procedures by organizations that have quality and security management ability above a certain level.
						Advanced	- The organization specifies in the contract the security requirements that the products and services procured from the partner should comply with, such as the following. - Specific certifications related to security (e.g., ISMS certification、ISASecure EDSA certification, Japan Information Technology Security Evaluation and Certification Scheme (JISEC) have been gained. - The vendor itself confirms that it has implemented the security measures in accordance with the standards of specific certifications related to security - It has implemented the necessary security requirements from the design phase (security by design) based on the results of risk analysis, etc., and test them. - It is desirable that the organization should, at the phase of planning procurement, secure a budget for security requirements regarding products or services themselves, or protection of assets used for procurement and supply of such products or services. - The organization formulates, manages and improves security measurement rules to evaluate procurement or supply of products or services, including the following. - Target for measurement - Method and frequency of reporting on measures taken - Measures to be taken when measures are not implemented - The organization checks means of detecting (or preventing) falsifications and leakages during shipments and whether or not the IoT devices and software being delivered have been operated without authorization. - Goods: security courier, protection seal, etc. - Digital transfer: encryption, hash of the entire transmitted data, etc.
				CPS.IP-3	Introduce the system development life cycle to manage the systems.	H-Advanced	- The organization explicitly presents the following requirements when procuring the system; - Requirements for security functions; - Requirements for security strength; - Requirements for security warranty; - Requirements for security-related documents; - Requirements for protection of security-related documents; - Description on the development environment of the system and the environment which the system is planned to operate under; - Acceptance criteria
						Advanced	- The organization manages the system in accordance with the system development lifecycle, which includes items of consideration regarding information security, and undergoes an information security risk management process throughout the entire system development lifecycle.
						Basic	- The organization applies the general rules of the system's security engineering to specifications, design, development, introduction, and changes in building the system.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
		A.14.1.2 Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).	H-Advanced	- The information system and the industrial control system monitor and control communications on the networks composing internal business systems of the organization. - Regarding the network which the system that handles highly confidential data is connected to, the organization shall deny network communications as a default and shall only allow connection of approved communication traffic. - The organization physically or logically separates the network of high importance industrial control systems from the network of control systems with lower importance. - If the information system that handles highly confidential data is connected to a remote device, the organization is to prevent multiple and simultaneous local connections between the device and the system, as well as prevent access to external network resources by other connections.
						Advanced	- The information system and industrial control system monitor and regulate connection of external and internal boundaries of the network to which the system is connected (in the case of industrial control systems, boundaries with information systems). - The organization installs boundary protection devices to promote effective security in the system and connects to external networks via the device.
				CPS.DS-3	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.	H-Advanced	- The organization protects th networks composing the information system and industrial control system that handles important data by implementing encrytion of communication channels or by alternative physical measures.
						Advanced	- The information system employs an cryptographic mechanism and encrypt communciation paths. [Reference] For encryption of communication paths, there are several methods such as IP-VPN, Ipsec-VPN, SSL VPN. It is desirable that the organization should select the method considering the importance of the data transmitted in the communication paths, the budget, and so on.
				CPS.DS-4	Encrypt information itself when sending/receiving information.	H-Advanced	- The system /IoT apparatus introduces the code module which it can implement without even little resource losing availability, and it is desirable to encrypt the communication data from a high apparatus of the importance at appropriate strength. - The information system encrypts all data transmitted outside the organization with appropriate strength, not limited to high or low importance.
						Advanced	- The organization encrypts information with appropriate strength when transmitting highly confidential information to an external organization or the like.
				CPS.DS-11	Perform integrity checking on information to be sent, received, and stored.	H-Advanced	- The organization detects tampering with data transmitted from IoT devices, servers, etc. in industrial control systems, if possible, using integrity checking tools. - The organization incorporates detection capacity into its incident response capacity to detect unauthorized changes that are made to the settings and security, such as an unauthorized promotion of system authority.
						Advanced	- The organization uses an integrity verification tool in an information system to detect any unauthorized changes that are made to communications data transmitted from IoT devices and servers. - The information system regularly inspects the integrity of the stored data. - The information system supports the technology of authenticating the sending domain in e-mail, and detects spoofing and tampering of e-mail.
		A.14.1.3 Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).	H-Advanced	- The information system and the industrial control system monitor and control communications on the networks composing internal business systems of the organization. - Regarding the network which the system that handles highly confidential data is connected to, the organization shall deny network communications as a default and shall only allow connection of approved communication traffic. - The organization physically or logically separates the network of high importance industrial control systems from the network of control systems with lower importance. - If the information system that handles highly confidential data is connected to a remote device, the organization is to prevent multiple and simultaneous local connections between the device and the system, as well as prevent access to external network resources by other connections.
						Advanced	- The information system and industrial control system monitor and regulate connection of external and internal boundaries of the network to which the system is connected (in the case of industrial control systems, boundaries with information systems). - The organization installs boundary protection devices to promote effective security in the system and connects to external networks via the device.
				CPS.AC-8	Restrict communications by IoT devices and servers to those with entities (e.g. people, components, system, etc.) identified through proper procedures.	Basic	- The organization assigns identifiers to its IoT devices and servers, as well as managing the identification by preventing re-use of identifiers and invalidating identifiers after a certain period of time. - Before connecting their IoT devices and servers to the network, the information system and the industrial control system prepare a mechanism that uniquely identifies and authenticate these devices. - Communication using IoT devices is denied as default. The protocol to be used is authorized as an exception.
				CPS.DS-3	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.	H-Advanced	- The organization protects th networks composing the information system and industrial control system that handles important data by implementing encrytion of communication channels or by alternative physical measures.
						Advanced	- The information system employs an cryptographic mechanism and encrypt communciation paths. [Reference] For encryption of communication paths, there are several methods such as IP-VPN, Ipsec-VPN, SSL VPN. It is desirable that the organization should select the method considering the importance of the data transmitted in the communication paths, the budget, and so on.
				CPS.DS-11	Perform integrity checking on information to be sent, received, and stored.	H-Advanced	- The organization detects tampering with data transmitted from IoT devices, servers, etc. in industrial control systems, if possible, using integrity checking tools. - The organization incorporates detection capacity into its incident response capacity to detect unauthorized changes that are made to the settings and security, such as an unauthorized promotion of system authority.
						Advanced	- The organization uses an integrity verification tool in an information system to detect any unauthorized changes that are made to communications data transmitted from IoT devices and servers. - The information system regularly inspects the integrity of the stored data. - The information system supports the technology of authenticating the sending domain in e-mail, and detects spoofing and tampering of e-mail.
				CPS.CM-4	Validate the integrity and authenticity of the information provided from cyberspace before operations.	H-Advanced	- The organization introduces the concept of "whitelisting" for data entry in order to specify known items and systems considered trustworthy as the sources of input data, and the format allowed for the input data. - IoT devices and servers begin communication with other IoT devices only after the devices are mutually authenticated successfully so that the source of data is always clear. - The information system and the industrial control system protect the authenticity of communications sessions.
						Advanced	- The information system uses an integrity verification tool to detect any unauthorized changes that are made to communications data transmitted from IoT devices and servers. - IoT devices and servers that are acknowledged as critical to the organization's operations begin communication with other IoT devices only after the devices are mutually authenticated successfully so that the source of data is always clear.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
	A.14.2 Security in development and support processes	A.14.2.1 Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.	CPS.IP-3	Introduce the system development life cycle to manage the systems.	H-Advanced	- The organization explicitly presents the following requirements when procuring the system; - Requirements for security functions; - Requirements for security strength; - Requirements for security warranty; - Requirements for security-related documents; - Requirements for protection of security-related documents; - Description on the development environment of the system and the environment which the system is planned to operate under; - Acceptance criteria
						Advanced	- The organization manages the system in accordance with the system development lifecycle, which includes items of consideration regarding information security, and undergoes an information security risk management process throughout the entire system development lifecycle.
						Basic	- The organization applies the general rules of the system's security engineering to specifications, design, development, introduction, and changes in building the system.
		A.14.2.2 System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	CPS.IP-1	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	H-Advanced	- Before making changes to IoT devices and servers that are subjects of configuration management, the organization tests and approves these changes as well as creates a document on the changes. - The organization uses an automated mechanism to manage, apply, and confirm settings of IoT devices and servers from a single location. - The organization integrates security change management procedures particularly for industrial control systems, into existing process safety management procedures.
						Advanced	- When changes are made to the IoT devices and servers that are subjects of configuration management, the organization analyzes the impact the change has on security, decides whether the change can be made or not, and creates a document on the procedure. - The organization limits personnel who can make changes to approved IoT devices and servers (restricted access). - The organization makes changes to approved IoT devices and servers, as well as implements, records, and monitors those changes. - The organization uses a secure recovery method (e.g. entering a security code known only to the user before the change is implemented) if they forget the password of their accounts, IoT device and servers. - The organization regularly reviews policies and procedures for operation and change management to ensure that changes do not adversely affect the availability or safety of information system and industrial control system.
				CPS.IP-3	Introduce the system development life cycle to manage the systems.	H-Advanced	- The organization explicitly presents the following requirements when procuring the system; - Requirements for security functions; - Requirements for security strength; - Requirements for security warranty; - Requirements for security-related documents; - Requirements for protection of security-related documents; - Description on the development environment of the system and the environment which the system is planned to operate under; - Acceptance criteria
						Advanced	- The organization manages the system in accordance with the system development lifecycle, which includes items of consideration regarding information security, and undergoes an information security risk management process throughout the entire system development lifecycle.
		A.14.2.3 Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	CPS.IP-1	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.	H-Advanced	- Before making changes to IoT devices and servers that are subjects of configuration management, the organization tests and approves these changes as well as creates a document on the changes. - The organization uses an automated mechanism to manage, apply, and confirm settings of IoT devices and servers from a single location. - The organization integrates security change management procedures particularly for industrial control systems, into existing process safety management procedures.
						Advanced	- When changes are made to the IoT devices and servers that are subjects of configuration management, the organization analyzes the impact the change has on security, decides whether the change can be made or not, and creates a document on the procedure. - The organization limits personnel who can make changes to approved IoT devices and servers (restricted access). - The organization makes changes to approved IoT devices and servers, as well as implements, records, and monitors those changes. - The organization uses a secure recovery method (e.g. entering a security code known only to the user before the change is implemented) if they forget the password of their accounts, IoT device and servers. - The organization regularly reviews policies and procedures for operation and change management to ensure that changes do not adversely affect the availability or safety of information system and industrial control system.
				CPS.IP-10	Develop a vulnerability remediation plan, and modify the vulnerability of the components according to the plan.	H-Advanced	- The organization adopts and administers an automated mechanism for managing the status of defect correction.
						Advanced	- The organization defines tolerable risk by identifying through investigations and tests the impacts of patch application on the functions of other software applications and services on operations of IoT devices and servers. - The organization conducts tests to measure the effectiveness of corrections and the possibility of any secondary adverse effects, corrects the defects, and manages the corrections as part of the configuration management.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
		A.14.2.4 Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.	Advanced	- Maintain/manage lists including configuration information of assets (e.g., names, version information, license information, and location) by reviewing and updating them periodically. - The organization makes a list of removable media (e.g., USB memory sticks) that can be used on system components (information system or industrial control system), and manages the use of them. - The organization uses only removable media (e.g. USB memory) permitted in the organization. Also, if there is no identifiable ownwer of portable storage devices, the organization prohibits the use of such devices. - The organization controles access to the media that contain highly confidential data, and properly grasps and manages the usage of the media taken outside of the controlled areas.
				CPS.MA-1	- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updateswith managed tools properly and in a timely manner while recording the history. - Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable.	H-Advanced	- The organization gives prior approval for the use of devices and/or tools needed for maintenance to update its IoT devices and servers, and conducts monitoring. - The organization inspects the devices and/or tools for maintenance brought in by the staff members who update its IoT devices and servers in order to make sure that no inappropriate or unauthorized changes will be made. - The organization inspects the media used for maintenance to update its IoT devices and servers in order to make sure that the media contain no malicious code before they are used. - The organization introduces an IoT device designed to remotely update different software programs (OS, driver, application) at the same time.
						Advanced	- The organization plans maintenance work such as updating its IoT devices and servers, implements the plan, checks the work done, and documents the entire maintenance. - The organization gives prior approval for maintenance work such as updating its IoT devices and servers, and conducts monitoring. - The organization gives prior approval for travel from its premises for any maintenance work away from its premises, such as updating its IoT devices and servers. It also takes necessary actions before the travel, such as deleting relevant saved data. - The organization checks all security measures that may have been affected by maintenance work, such as updating its IoT devices and servers, after the work is complete in order to make sure that the relevant equipment works correctly. - The organization keeps the records of maintenance work done, such as updating its IoT devices and servers. - The organization establishes a process for authorizing maintenance staff in order to keep the list of authorized maintenance organizations or staff members updated.
		A.14.2.5 Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	CPS.IP-3	Introduce the system development life cycle to manage the systems.	H-Advanced	- The organization explicitly presents the following requirements when procuring the system; - Requirements for security functions; - Requirements for security strength; - Requirements for security warranty; - Requirements for security-related documents; - Requirements for protection of security-related documents; - Description on the development environment of the system and the environment which the system is planned to operate under; - Acceptance criteria
						Advanced	- The organization manages the system in accordance with the system development lifecycle, which includes items of consideration regarding information security, and undergoes an information security risk management process throughout the entire system development lifecycle.
		A.14.2.6 Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	CPS.IP-3	Introduce the system development life cycle to manage the systems.	H-Advanced	- The organization explicitly presents the following requirements when procuring the system; - Requirements for security functions; - Requirements for security strength; - Requirements for security warranty; - Requirements for security-related documents; - Requirements for protection of security-related documents; - Description on the development environment of the system and the environment which the system is planned to operate under; - Acceptance criteria
						Advanced	- The organization manages the system in accordance with the system development lifecycle, which includes items of consideration regarding information security, and undergoes an information security risk management process throughout the entire system development lifecycle.
						Basic	- The organization applies the general rules of the system's security engineering to specifications, design, development, introduction, and changes in building the system.
		A.14.2.7 Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	CPS.SC-6	Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	H-Advanced	- The organization adopts an automatic mechanism integrating review, analysis, and report that supports the investigation and addresses procedures for deviation or signs of deviation from contract matters. - The organization uses a mechanism that allows it to list and check whether obligatory matters stipulated in the contract are fulfilled, matters which are concerned with security management of the organization and security functions implemented in the products and services that will be delivered, especially for important clients and reconsigned organizations. - State of compliance with security management measures of the external service provider is regularly checked by external audits and field surveys conducted by the outsourcer. - The important business partners and if possible their re-contractors etc. investigate whether there is any sign of attack related or any fact of information leakage, and regularly report the result to the organization.
						Advanced	- The organization checks whether requirements that are prescribed in the contract with the client can be audited on the system. - The information system provides a function that allows for audit records to be created for events defined above that can be audited on the system. - The organization shall be able to maintain consistency in security audits with other organizations that require information on the audit. - The organization regularly reviews and analyzes audit records that are made manually or automatically by the system, and checks whether there is any deviation or sign of deviation from contract matters. - State of compliance with security management measures of the external service provider is regularly checked by internal audits that are conducted by the client using a checklist.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.CM-5	Monitor communication with external service providers so that potential security events can be detected properly.	H-Advanced	- The organization requires its provider of external information system services to make clear the functions, ports, and protocols needed for the use of the services, along with other services. - The organization monitors whether the matters made clear as stated above are observed.
						Advanced	- The organization documents its security requirements for the staff from its external service provider and system developer, and includes the requirements in the agreement. - The organization requires its external service provider and system developer to contact it when any of its staff members who have authorizations for its system are transferred or when their employment terminates. - It is desirable that the organization should manage changes to services offered by its external service provider, taking account of relevant information about operations, the importance of its business systems and processes, and re-assessed risks. - The organization monitors whether its external service provider and system developer complies with the requirements. - The organization monitors access to its system by its external service provider and system developer in order to detect any unauthorized access by these external businesses that results from an action or failure to act. - The organization reports the results of the monitoring of activities by its external service provider and system developer to the appropriate system administrator.
						Basic	- The organization requires its provider of external information system services and system developer to draw up and introduce security requirements such as those related to the following in accordance with the rules which the organization is subject to or which apply to the provider and developer. - Adequate security measures to take (e.g., measures that deserve ISMS Certification) - Proper management of data in operation - Proper data erasure when the use of the services ends
		A.14.2.8 System security testing	Testing of security functionality shall be carried out during development.	CPS.DP-3	As part of the monitoring process, test regularly if the functions for detecting security events work as intended, and validate these functions.	H-Advanced	- The organization conducts a trend analysis examining the latest information about threats, vulnerability, and assessments of security management measures carried out several times in order to determine whether the activities for continuous monitoring need any correction. - The organization introduces known and harmless test cases to its systems to test its mechanism for detecting malware. - The organization regularly tests the mechanism it uses for intrusion detection monitoring. The frequency of the test depends on the type of tool the organization uses and the way the tool is installed.
						Advanced	- The organization establishes and manages a procedure for a regular review of its system monitoring activities to see if they conform to the organization's risk management strategy and the order of priority for actions to handle risks. - The organization calculates the percentages of false detections and false negatives when correlation analysis of information pertaining to the security of network devices or endpoints is conducted, thereby checking the validity of the detection mechanism regularly.
		A.14.2.9 System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	CPS.SC-4	When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	H-Advanced	- The organization or a third party tests the procured devices to see whether the security requirements stipulated in the contract are fulfilled. - The organization checks throughout the entire relevant supply chain (including reconsigned organizations) as to whether the devices especially important for their operation are manufactured under appropriate procedures by organizations that have quality and security management ability above a certain level.
						Advanced	- The organization specifies in the contract the security requirements that the products and services procured from the partner should comply with, such as the following. - Specific certifications related to security (e.g., ISMS certification、ISASecure EDSA certification, Japan Information Technology Security Evaluation and Certification Scheme (JISEC) have been gained. - The vendor itself confirms that it has implemented the security measures in accordance with the standards of specific certifications related to security - It has implemented the necessary security requirements from the design phase (security by design) based on the results of risk analysis, etc., and test them. - It is desirable that the organization should, at the phase of planning procurement, secure a budget for security requirements regarding products or services themselves, or protection of assets used for procurement and supply of such products or services. - The organization formulates, manages and improves security measurement rules to evaluate procurement or supply of products or services, including the following. - Target for measurement - Method and frequency of reporting on measures taken - Measures to be taken when measures are not implemented - The organization checks means of detecting (or preventing) falsifications and leakages during shipments and whether or not the IoT devices and software being delivered have been operated without authorization. - Goods: security courier, protection seal, etc. - Digital transfer: encryption, hash of the entire transmitted data, etc.
	A.14.3 Test data	A.14.3.1 Protection of test data	Test data shall be selected carefully, protected and controlled.	CPS.SC-4	When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	H-Advanced	- The organization or a third party tests the procured devices to see whether the security requirements stipulated in the contract are fulfilled. - The organization checks throughout the entire relevant supply chain (including reconsigned organizations) as to whether the devices especially important for their operation are manufactured under appropriate procedures by organizations that have quality and security management ability above a certain level.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.SC-6	Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	H-Advanced	- The organization adopts an automatic mechanism integrating review, analysis, and report that supports the investigation and addresses procedures for deviation or signs of deviation from contract matters. - The organization uses a mechanism that allows it to list and check whether obligatory matters stipulated in the contract are fulfilled, matters which are concerned with security management of the organization and security functions implemented in the products and services that will be delivered, especially for important clients and reconsigned organizations. - State of compliance with security management measures of the external service provider is regularly checked by external audits and field surveys conducted by the outsourcer. - The important business partners and if possible their re-contractors etc. investigate whether there is any sign of attack related or any fact of information leakage, and regularly report the result to the organization.
						Advanced	- The organization checks whether requirements that are prescribed in the contract with the client can be audited on the system. - The information system provides a function that allows for audit records to be created for events defined above that can be audited on the system. - The organization shall be able to maintain consistency in security audits with other organizations that require information on the audit. - The organization regularly reviews and analyzes audit records that are made manually or automatically by the system, and checks whether there is any deviation or sign of deviation from contract matters. - State of compliance with security management measures of the external service provider is regularly checked by internal audits that are conducted by the client using a checklist.
				CPS.IP-4	Perform a periodical system backup and testing of components (e.g., IoT devices, communication devices, and circuits).	H-Advanced	- The organization confirms the trustworthiness of the medium and integrity of the information by regularly testing the backup information.
				CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.	H-Advanced	- In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g. OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related audit logs for some of the IoT devices that an organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specs of the IoT devices, such as using a log management system different than the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.
						Advanced	- The information system and the industrial control system uses a cryptographic mechanism in order to ensure the integrity of an audit log and audit tool each. - The organization grants control over an audit log only to users assigned in accordance with the rules about security-related internal responsibility. - The information system issues an alert when an incident of failure takes place in the audit process.
A.15 Supplier relationships	A.15.1 Information security in supplier relationships	A.15.1 Information security in supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	CPS.AM-7	Define roles and responsibilities for cyber security across the organization and other relevant parties.	Advanced	- In preparation for damages caused by security incidents, the organization considers risk transfer by using cyber insurance, etc., in addition to implementing security measures designated by business partners.
						Basic	- In a contract with a contractor or an outsourcer, the organization specifies the scope of the responsibilities of the organization and that of the business partner (state the disclaimer and an upper limit on agreed compensation for damages) in case of a damage caused by a security incident in the business. - To increase the effectiveness of the requirements related to security which a business partner requires or is required to satisfy in a contract, it is desirable that the organization makes an agreement in meeting the requirements, identifying deficiencies and details of actions, paying expenses, and using an alternative when they cannot be satisfied at the time of the contract or in the early stage of the contract.
				CPS.SC-1	Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.	Advanced	- The organization, in reference to security measure criteria regarding supply chain, prepares and provides to potential partners tender documents such as ITT (Invitation To Tender) and RFP (Request For Proposal). Especially, it is advisable that the following items be included in the tender documents. 1) Specifications of products or services to be procured 2) Security requirements that the supplie should comply with during the supply period of the products or services 3) Service levels and the indices to comply with during the supply period of the products or services 4) Penalties that the purchaser may impopse if the supplier breach security requirements 5) Confidentiality clauses to protect the data transmitted during the supplier selection process, the systems, etc. - The organization prepares procedures for continuously monitoring the conditions in the business partners' compliance with the security management measures. - To take precautions against cases where a security incident in a business partner impacts the organization, in a written contract, clarify where responsibility lies between the external business operator and the organization, and describe the compensation for a damage to the organization for which the external business operator is responsible.
						Basic	- The organization formulates security measure criteria applicable to business partners (especially those handling the organization's data or providing a foundation for handling the data) according to appropriate laws and regulations and makes agreement with the details.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.SC-2	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.	H-Advanced	- The organization determines its core business that must continue/recover before any other operations in prior and identifies and prioritizes important resources (other relevant organizations, employees, items, data, systems, etc.) and functions vital for continuing applicable businesses. - In case of the occurrence of a security incident in business partners which has harmful business impacts, the organization estimate the details of the impacts on the organization and its occurrence level and scale. * Related requirements of countermeasures include CPS.AM-6 and CPS.BE-2.
						Advanced	- The organization identifies the business partners in the supply chains which can impact the organization's missions/business processes and confirms whether applicable partners can fulfill the security roles and responsibilities specified in the organization's security policies.
						Basic	- The organization should identify in advance the core businesses that should be continued and restored in priority, and the operations considered to be important. In addition, identify and prioritize important resources (relevant parties, People, Components, Data, System, etc.) and functions from the viewpoint of business continuity. - When the organization is assumed to use an IoT device for a long period of time, the organization selects a business partner (device vendor) that has adequate organizations of management (Ex: service desk(s), maintainance system) from which long-term support can be expected. - The organization confirms with the partner (the device vendor) whether to replace a device at the end of support before implementing a system. - When the organization selects a business partner (service provider), it is desirable to select a service provider who operates and manages IT services efficiently and effectively. - It has acquired ITSMS certification based on JIS Q 20000. - It has implemented the equivalent measures to ITSMS certification based on self declaration of comformity.
				CPS.MA-2	Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.	Advanced	- The organization documents the policy and procedure relating to establishing and implementing a connection designed for remote maintenance, and implements the connection in accordance with the policy and procedure. - The organization provides authentication required for network access that it specifies when remote maintenance is carried out. It also ensures that the session and network connection are terminated when the remote maintenance is complete.
		A.15.1.2 Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	CPS.SC-1	Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.	Advanced	- The organization, in reference to security measure criteria regarding supply chain, prepares and provides to potential partners tender documents such as ITT (Invitation To Tender) and RFP (Request For Proposal). Especially, it is advisable that the following items be included in the tender documents. 1) Specifications of products or services to be procured 2) Security requirements that the supplie should comply with during the supply period of the products or services 3) Service levels and the indices to comply with during the supply period of the products or services 4) Penalties that the purchaser may impopse if the supplier breach security requirements 5) Confidentiality clauses to protect the data transmitted during the supplier selection process, the systems, etc. - The organization prepares procedures for continuously monitoring the conditions in the business partners' compliance with the security management measures. - To take precautions against cases where a security incident in a business partner impacts the organization, in a written contract, clarify where responsibility lies between the external business operator and the organization, and describe the compensation for a damage to the organization for which the external business operator is responsible.
						Basic	- The organization formulates security measure criteria applicable to business partners (especially those handling the organization's data or providing a foundation for handling the data) according to appropriate laws and regulations and makes agreement with the details.
				CPS.SC-2	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.	H-Advanced	- The organization determines its core business that must continue/recover before any other operations in prior and identifies and prioritizes important resources (other relevant organizations, employees, items, data, systems, etc.) and functions vital for continuing applicable businesses. - In case of the occurrence of a security incident in business partners which has harmful business impacts, the organization estimate the details of the impacts on the organization and its occurrence level and scale. * Related requirements of countermeasures include CPS.AM-6 and CPS.BE-2.
						Advanced	- The organization identifies the business partners in the supply chains which can impact the organization's missions/business processes and confirms whether applicable partners can fulfill the security roles and responsibilities specified in the organization's security policies.
						Basic	- The organization should identify in advance the core businesses that should be continued and restored in priority, and the operations considered to be important. In addition, identify and prioritize important resources (relevant parties, People, Components, Data, System, etc.) and functions from the viewpoint of business continuity. - When the organization is assumed to use an IoT device for a long period of time, the organization selects a business partner (device vendor) that has adequate organizations of management (Ex: service desk(s), maintainance system) from which long-term support can be expected. - The organization confirms with the partner (the device vendor) whether to replace a device at the end of support before implementing a system. - When the organization selects a business partner (service provider), it is desirable to select a service provider who operates and manages IT services efficiently and effectively. - It has acquired ITSMS certification based on JIS Q 20000. - It has implemented the equivalent measures to ITSMS certification based on self declaration of comformity.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.SC-3	When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	H-Advanced	- In a contract with a business partner who provides systems/components/services, the organization requires the partner the following listed below: - Create evidence of the implementation of the security assessment plan, and submit results of security tests/evaluations. - Develop a plan for remedying defects identified during security testing / evaluation - Disclose a plan for defect remediation and its implementation status - It is desirable that the organization applies necessary requirements among those for security measures to directly consigned parties and accompanying requirements to reconsigned parties by considering the scales of risks originating from the supply chains.
						Advanced	- In accordance with the missions/business needs of the organization, state the following requirements, descriptions, and criteria in a procurement contract of a system, component, or service. - Requirements for security measures - Requirements for security-related documents - Requirements for protection of security-related documents - Confidentiality clauses - Implementation body and method of each handling: reporting destination at the time of incident occurrence, reporting details, initial reaction, investigation, recovery, etc. - Conditions to allow to confirm the observance to the security requirement which is inspected and defined by the organization or the authorized third party. - How to handle an information asset at the end of the contract - The organization requires business partners, in a procurement contract, to implement security requirements that comply with applicable laws and regulations, implement additional measures when they are recognized necessary because of the characteristics of the contracted duty, etc. - It is desirable to consider the following items in advance when determining security requirements based on laws and regulations and requiring business partners to comply with them. - Identification of potential risks in terms of legal regulations that may arise due to difference of applicable laws between the organization and the business partner - Negative impacts on the contract in terms of security due to legal and regulatory obligations applicable to the business partner
						Basic	- The organization requires business partners to implement security requirements that complies with applicable laws and regulations. - The organization confirms that the business partner has declared "SECURITY ACTION" in the process of selecting and evaluating a contractor. * "SECURITY ACTION" is an initiative in Japan that small and medium-sized enterprises declare themselves to work on information security measures.
		A.15.1.3 Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	CPS.SC-4	When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	H-Advanced	- The organization or a third party tests the procured devices to see whether the security requirements stipulated in the contract are fulfilled. - The organization checks throughout the entire relevant supply chain (including reconsigned organizations) as to whether the devices especially important for their operation are manufactured under appropriate procedures by organizations that have quality and security management ability above a certain level.
						Advanced	- The organization specifies in the contract the security requirements that the products and services procured from the partner should comply with, such as the following. - Specific certifications related to security (e.g., ISMS certification、ISASecure EDSA certification, Japan Information Technology Security Evaluation and Certification Scheme (JISEC) have been gained. - The vendor itself confirms that it has implemented the security measures in accordance with the standards of specific certifications related to security - It has implemented the necessary security requirements from the design phase (security by design) based on the results of risk analysis, etc., and test them. - It is desirable that the organization should, at the phase of planning procurement, secure a budget for security requirements regarding products or services themselves, or protection of assets used for procurement and supply of such products or services. - The organization formulates, manages and improves security measurement rules to evaluate procurement or supply of products or services, including the following. - Target for measurement - Method and frequency of reporting on measures taken - Measures to be taken when measures are not implemented - The organization checks means of detecting (or preventing) falsifications and leakages during shipments and whether or not the IoT devices and software being delivered have been operated without authorization. - Goods: security courier, protection seal, etc. - Digital transfer: encryption, hash of the entire transmitted data, etc.
	A.15.2 Supplier service delivery management	A.15.2.1 Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	CPS.SC-1	Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.	Advanced	- The organization, in reference to security measure criteria regarding supply chain, prepares and provides to potential partners tender documents such as ITT (Invitation To Tender) and RFP (Request For Proposal). Especially, it is advisable that the following items be included in the tender documents. 1） Specifications of products or services to be procured 2） Security requirements that the supplie should comply with during the supply period of the products or services 3） Service levels and the indices to comply with during the supply period of the products or services 4） Penalties that the purchaser may impopse if the supplier breach security requirements 5） Confidentiality clauses to protect the data transmitted during the supplier selection process, the systems, etc. - The organization prepares procedures for continuously monitoring the conditions in the business partners' compliance with the security management measures. - To take precautions against cases where a security incident in a business partner impacts the organization, in a written contract, clarify where responsibility lies between the external business operator and the organization, and describe the compensation for a damage to the organization for which the external business operator is responsible.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.SC-6	Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.	H-Advanced	- The organization adopts an automatic mechanism integrating review, analysis, and report that supports the investigation and addresses procedures for deviation or signs of deviation from contract matters. - The organization uses a mechanism that allows it to list and check whether obligatory matters stipulated in the contract are fulfilled, matters which are concerned with security management of the organization and security functions implemented in the products and services that will be delivered, especially for important clients and reconsigned organizations. - State of compliance with security management measures of the external service provider is regularly checked by external audits and field surveys conducted by the outsourcer. - The important business partners and if possible their re-contractors etc. investigate whether there is any sign of attack related or any fact of information leakage, and regularly report the result to the organization.
						Advanced	- The organization checks whether requirements that are prescribed in the contract with the client can be audited on the system. - The information system provides a function that allows for audit records to be created for events defined above that can be audited on the system. - The organization shall be able to maintain consistency in security audits with other organizations that require information on the audit. - The organization regularly reviews and analyzes audit records that are made manually or automatically by the system, and checks whether there is any deviation or sign of deviation from contract matters. - State of compliance with security management measures of the external service provider is regularly checked by internal audits that are conducted by the client using a checklist.
				CPS.MA-2	Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.	Advanced	- The organization documents the policy and procedure relating to establishing and implementing a connection designed for remote maintenance, and implements the connection in accordance with the policy and procedure. - The organization provides authentication required for network access that it specifies when remote maintenance is carried out. It also ensures that the session and network connection are terminated when the remote maintenance is complete.
						Basic	- The organization develops and agrees to an implementation plan for remote maintenance before carrying out the maintenance, and checks the results of the maintenance done. - The organization keeps the records of remote maintenance done.
				CPS.CM-5	Monitor communication with external service providers so that potential security events can be detected properly.	H-Advanced	- The organization requires its provider of external information system services to make clear the functions, ports, and protocols needed for the use of the services, along with other services. - The organization monitors whether the matters made clear as stated above are observed.
						Advanced	- The organization documents its security requirements for the staff from its external service provider and system developer, and includes the requirements in the agreement. - The organization requires its external service provider and system developer to contact it when any of its staff members who have authorizations for its system are transferred or when their employment terminates. - It is desirable that the organization should manage changes to services offered by its external service provider, taking account of relevant information about operations, the importance of its business systems and processes, and re-assessed risks. - The organization monitors whether its external service provider and system developer complies with the requirements. - The organization monitors access to its system by its external service provider and system developer in order to detect any unauthorized access by these external businesses that results from an action or failure to act. - The organization reports the results of the monitoring of activities by its external service provider and system developer to the appropriate system administrator.
						Basic	- The organization requires its provider of external information system services and system developer to draw up and introduce security requirements such as those related to the following in accordance with the rules which the organization is subject to or which apply to the provider and developer. - Adequate security measures to take (e.g., measures that deserve ISMS Certification) - Proper management of data in operation - Proper data erasure when the use of the services ends
		A.15.2.2 Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	CPS.CM-5	Monitor communication with external service providers so that potential security events can be detected properly.	H-Advanced	- The organization requires its provider of external information system services to make clear the functions, ports, and protocols needed for the use of the services, along with other services. - The organization monitors whether the matters made clear as stated above are observed.
						Advanced	- The organization documents its security requirements for the staff from its external service provider and system developer, and includes the requirements in the agreement. - The organization requires its external service provider and system developer to contact it when any of its staff members who have authorizations for its system are transferred or when their employment terminates. - It is desirable that the organization should manage changes to services offered by its external service provider, taking account of relevant information about operations, the importance of its business systems and processes, and re-assessed risks. - The organization monitors whether its external service provider and system developer complies with the requirements. - The organization monitors access to its system by its external service provider and system developer in order to detect any unauthorized access by these external businesses that results from an action or failure to act. - The organization reports the results of the monitoring of activities by its external service provider and system developer to the appropriate system administrator.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.1 Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	CPS.RP-2	As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.	H-Advanced	- The organization assumes the course of action for security incidents of the supply chain and prepares a procedure that adjusts incident responses between the organization and other organizations that are concerned with the supply chain. - The organization adjusts the incident response process of an external service provider that contains important features in order to continue its business, as well as adjusting the organization's incident response process to meet the incident response requirements. - The organization interlinks information regarding threats and vulnerabilities with how individual security incidents have been handled so as to improve its understanding of the situations. [Reference] Violations in the security incidents of supply chain include violations on system components, IT products, development processes, developers, distribution processes, and warehouse facilities.
						Advanced	- The organization determines an alternative processing site in case the availability of its primary processing site has been compromised by a security incident. - The organization sets forth in the service agreement that if its primary processing function becomes unavailable, certain operations are moved to resume at the alternative processing site within the recovery time objective that the organization specifies in order to ensure that it continues to perform its critical missions and operational functions. - The organization designates an alternative processing site away from its primary processing site in order to mitigate the vulnerability to the same threats. - The organization prepares internal resources for incident handling assistance (e.g., help desk; CSIRT). These resources offer advice and support related to security incident handling and reporting for system users of the information system and industrial control system, and are an integral part of organizational ability to handle incidents.
						Basic	- If any security incident that requires handling is found, report it promptly to relevant organizations such as IPA and JPCERT/CC in order to receive advice about providing assistance in handling, identifying how the incident has occurred, analyzing the tactic, and preventing any recurrence.
		A.16.1.2 Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	CPS.SC-5	Formulate and manage security requirements applicable to members of other relevant organizations, such as business partners, who are engaged in operations outsourced from the organization.	H-Advanced	- The organization prepares a procedure to continuously monitor whether the security requirements from the contractee are complied with by the staff of the contractor, and to enable notification to the organization's personnel in charge in the case where irregular behavior is found.
						Advanced	- The organization trains the staff on information security aspects of supplier relationships to particularly ensure that the handling of confidential information is correctly understood. - The organization regularly confirms that it complies with the security requirements from the contractee in conducting the contracted work.
						Basic	- The organization identifies and evaluates the staff who access, disclose or change the data related to the contracted work that should not be disclosed or changed such as confidential data or intellectual property. - After the contract with the contractor is finished, the organization immediately terminates the rights that are temporarily granted to the personnel of the contractor such as access rights to its facilities.
				CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.	Advanced	- The organization includes contents regarding what to do to detect, analyze, contain, reduce, and recover from incidents in its security operation manual. - Keep a record of all incidents and how they have been handled. - Decide whether the organization should report the fact to any external organization of an incident that has occurred and how it has been handled.'
						Basic	- The organization develops and manages a process of security operation it should follow when a security incident arises that it must address. It is advisable to include contents such as the following in the process: - Response procedure for the person who received the incident report - Instructions and orders, and how to prioritize actions in an emergency; - Incident response; - Incident impact assessment and damage analysis; - Information gathering, selecting information that the organization needs; - Communication and announcement to relevant internal personnel; - Communication with relevant external organizations; - The system (especially, industrial control system) shuts down, issues an alert to the administrator, or takes other fail-safe actions if any abnormality (e.g., malfunction) occurs in IoT devices or servers. [Reference] "SP 800-61 rev.1" (NIST, 2008) is available for reference to determine the process for handling security incidents that have arisen.
				CPS.RP-2	As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.	H-Advanced	- The organization assumes the course of action for security incidents of the supply chain and prepares a procedure that adjusts incident responses between the organization and other organizations that are concerned with the supply chain. - The organization adjusts the incident response process of an external service provider that contains important features in order to continue its business, as well as adjusting the organization's incident response process to meet the incident response requirements. - The organization interlinks information regarding threats and vulnerabilities with how individual security incidents have been handled so as to improve its understanding of the situations. [Reference] Violations in the security incidents of supply chain include violations on system components, IT products, development processes, developers, distribution processes, and warehouse facilities.
						Advanced	- The organization determines an alternative processing site in case the availability of its primary processing site has been compromised by a security incident. - The organization sets forth in the service agreement that if its primary processing function becomes unavailable, certain operations are moved to resume at the alternative processing site within the recovery time objective that the organization specifies in order to ensure that it continues to perform its critical missions and operational functions. - The organization designates an alternative processing site away from its primary processing site in order to mitigate the vulnerability to the same threats. - The organization prepares internal resources for incident handling assistance (e.g., help desk; CSIRT). These resources offer advice and support related to security incident handling and reporting for system users of the information system and industrial control system, and are an integral part of organizational ability to handle incidents.
						Basic	- If any security incident that requires handling is found, report it promptly to relevant organizations such as IPA and JPCERT/CC in order to receive advice about providing assistance in handling, identifying how the incident has occurred, analyzing the tactic, and preventing any recurrence.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
		A.16.1.3 Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	CPS.AN-3	Categorize and store information regarding the detected security incidents by the size of security-related impact, penetration vector, and other factors.	H-Advanced	- The organization uses an automated mechanism designed to help track security incidents and collect and analyze information about threats and vulnerability related to incidents, so that it applies the findings to classification (triage) of security incidents.
						Advanced	- The organization classifies security incidents, taking into account the recovery time objectives for the systems, the order of priority in recovery, and metrics in the process of its security operation. - The organization tracks and documents security incidents that may affect it. "SP 800-61 rev.1" lists the following as examples of points of view that may be taken when an organization documents a security incident. - The present state of the incident - Overview of the incident - The course of action the organization has taken to deal with the incident - Other contact information of relevant personnel (e.g., the system owner, system administrator) - List of proof collected during the investigation - Comments by the staff in charge of dealing with the incident - Next steps
						Basic	- The organization should identify in advance the core businesses that should be continued and restored in priority, and the operations considered to be important. In addition, identify and prioritize important resources (relevant parties, People, Components, Data, System, etc.) and functions from the viewpoint of business continuity. * Similar measures are described in CPS.AM-6 and CPS.BE-2. - The organization specifies incidents that must be reported, considering the level of the impact the security event has. [Reference] For example, the following document is available for reference when an organization decides on a measure of the severity of the impact of a security incident. - "SP 800-61 rev.1" (NIST, 2008) Prioritization of the 3.2.6 Incident
		A.16.1.4 Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	CPS.AE-5	Specify the criteria to determine the risk degree of security events.	H-Advanced	- The organization determines its core business that must continue/recover before any other operations in prior and identifies and prioritizes important resources (other relevant organizations, employees, items, data, systems, etc.) and functions vital for continuing applicable businesses. * CPS.AM-6 and CPS.BE-2 include examples of similar measures. - The organization uses an automated mechanism designed to help track security events and collect and analyze information about threats and vulnerability related to incidents, so that it applies the findings to classification (triage) of security events.
						Advanced	- The organization classifies security events, taking into account the recovery time objectives for the systems, the order of priority in recovery, and metrics in the process of its security operation.
						Basic	- The organization specifies security events that must be reported, considering the level of the impact the security event has. [Reference] For example, the following document is available for reference when an organization decides on a measure of the severity of the impact of a security event. - "SP 800-61 rev.1" (NIST, 2008) Prioritization of the 3.2.6 Incident
				CPS.AN-3	Categorize and store information regarding the detected security incidents by the size of security-related impact, penetration vector, and other factors.	H-Advanced	- The organization uses an automated mechanism designed to help track security incidents and collect and analyze information about threats and vulnerability related to incidents, so that it applies the findings to classification (triage) of security incidents.
						Advanced	- The organization classifies security incidents, taking into account the recovery time objectives for the systems, the order of priority in recovery, and metrics in the process of its security operation. - The organization tracks and documents security incidents that may affect it. "SP 800-61 rev.1" lists the following as examples of points of view that may be taken when an organization documents a security incident. - The present state of the incident - Overview of the incident - The course of action the organization has taken to deal with the incident - Other contact information of relevant personnel (e.g., the system owner, system administrator) - List of proof collected during the investigation - Comments by the staff in charge of dealing with the incident - Next steps
						Basic	- The organization should identify in advance the core businesses that should be continued and restored in priority, and the operations considered to be important. In addition, identify and prioritize important resources (relevant parties, People, Components, Data, System, etc.) and functions from the viewpoint of business continuity. * Similar measures are described in CPS.AM-6 and CPS.BE-2. - The organization specifies incidents that must be reported, considering the level of the impact the security event has. [Reference] For example, the following document is available for reference when an organization decides on a measure of the severity of the impact of a security incident. - "SP 800-61 rev.1" (NIST, 2008) Prioritization of the 3.2.6 Incident
		A.16.1.5 Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	CPS.SC-5	Formulate and manage security requirements applicable to members of other relevant organizations, such as business partners, who are engaged in operations outsourced from the organization.	H-Advanced	- The organization prepares a procedure to continuously monitor whether the security requirements from the contractee are complied with by the staff of the contractor, and to enable notification to the organization's personnel in charge in the case where irregular behavior is found.
						Advanced	- The organization trains the staff on information security aspects of supplier relationships to particularly ensure that the handling of confidential information is correctly understood. - The organization regularly confirms that it complies with the security requirements from the contractee in conducting the contracted work.
						Basic	- The organization identifies and evaluates the staff who access, disclose or change the data related to the contracted work that should not be disclosed or changed such as confidential data or intellectual property. - After the contract with the contractor is finished, the organization immediately terminates the rights that are temporarily granted to the personnel of the contractor such as access rights to its facilities.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.AE-2	Appoint a chief security officer, establish a security management team (SOC/CSIRT), and prepare a system within the organization to detect, analyze, and respond to security events.	H-Advanced	- The organization efficiently analyzes audit logs collected through 24-h, 365-day security monitoring by using an automated analysis tool. - It is desirable for the organization to include not only its conventional IT environment but also its control system and IoT devices in the scope of security monitoring. - It is desirable for the organization to regularly evaluate the maturity of its security measure organizations in order to continue improving its security-related operations, including security monitoring and the ways incidents are handled. [Reference] For example, SIM3 (Security Incident Management Maturity Model) is available as metrics for the evaluation of security organizations (SOC/CSIRT).
						Advanced	- The organization refers to risk assessment results and, considering the following angles, establishes what to monitor and what to include in correlation analysis. - The scope of systems to monitor - Which device logs should be collected for analysis (see CPS.AE-3) - The organization regularly reviews audit logs collected through monitoring. - The organization continues to collect and manage information about assets, device configurations, and network configurations in order to evaluate its security status. - The organization examines the results of correlation analysis and other data to accurately detect security events that must be addressed and take action in accordance with the security operation process. See CPS.RP-1 for details of the process. - The organization regularly reports the state of organizational and system security to the chief security officer or other appropriate staff members. It is desirable that the regular report should include the following shown below: - Results of log analysis (e.g., the number of incidents handled; summaries of typical incidents that have been handled; threats that have emerged; issues in monitoring); - Policy for future improvements in monitoring.
				CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (securith operation process) that includes the response of Organization, People, Componens, System to identify the content of response, priority, and scope of response taken after an incident occurs.	H-Advanced	- If the information system and the industrial control system receive any invalid data, they operate as stated in an expected manner in conformity with the purpose of the organization and system.
						Advanced	- The organization includes contents regarding what to do to detect, analyze, contain, reduce, and recover from incidents in its security operation manual. - Keep a record of all incidents and how they have been handled. - Decide whether the organization should report the fact to any external organization of an incident that has occurred and how it has been handled.'
						Basic	- The organization develops and manages a process of security operation it should follow when a security incident arises that it must address. It is advisable to include contents such as the following in the process: - Response procedure for the person who received the incident report - Instructions and orders, and how to prioritize actions in an emergency; - Incident response; - Incident impact assessment and damage analysis; - Information gathering, selecting information that the organization needs; - Communication and announcement to relevant internal personnel; - Communication with relevant external organizations; - The system (especially, industrial control system) shuts down, issues an alert to the administrator, or takes other fail-safe actions if any abnormality (e.g., malfunction) occurs in IoT devices or servers. [Reference] "SP 800-61 rev.1" (NIST, 2008) is available for reference to determine the process for handling security incidents that have arisen.
				CPS.MI-1	Take measures to minimize security-related damages and mitigate the impacts caused by such incident.	H-Advanced	- The organization uses an automated mechanism for assisting with the process of security incident handling. - The organization interlinks information regarding threats and vulnerabilities with how individual security incidents have been handled so as to improve its understanding of the situations. [Reference] As examples of information expected to be useful in reducing the impact of an incident being handled and in recovery from the incident, "Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT Version 1.0" (ISOG-J, 2018) lists the following: - Configuration requirements for security products and related systems to block any attacks; - How to disable attacks (e.g., patching; changing setups); - How to recover a damaged system;
						Basic	- The organization (or its members) takes courses of action to reduce security incidents (e.g., shutting down the system; cutting off the system from a wired/wireless network; cutting off a modem cable; disabling certain functions) in accordance with prescribed procedures. [Reference] Courses of action to reduce the impact of a security incident may vary according to the nature of the incident (e.g., according to the threat that has emerged, such as a denial-of-service attack, malware infection, or unauthorized access). For example, It is advisable to refer to "SP 800-61 rev.1" (NIST, 2008) for detailed information about courses of action to reduce the impact of an incident.
		A.16.1.6 Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	CPS.IP-7	Assess the lessons learned from security incident response and the results of monitoring, measuring, and evaluating internal and external attacks, and improve the processes of protecting the assets.	H-Advanced	- The organization has its security assessed by a third party.
						Advanced	- The organization draws up a security assessment plan before the assessment is carried out that includes the following so as to ensure that its security is assessed properly and systematically: - Security measures for assessment; - Assessment procedures for measuring the effectiveness of security measures; - Settings and mechanisms for carrying out the security assessment; - Methods of putting together the results of the security assessment and applications of the results.
						Basic	- The organization regularly evaluates whether its security measures have achieved expected results (i.e., security assessment) and reports the conclusions to the chief security officer, in addition to the evaluation of whether the measures are correctly implemented and managed. - The organization makes improvements on its security measures based on the results of the security assessment.
				CPS.IP-8	Share information regarding the effectiveness of data protection technologies with appropriate partners.	H-Advanced	- The organization prepares a setting through an automated mechanism at just the right time that enables it and its appropriate partners to interactively share new information about data protection technologies or information about the effectiveness of the protection technologies.
						Advanced	- The organization prepares a setting that enables it to share new information about data protection technologies or information about the effectiveness of the protection technologies with its partners at just the right time.
						Basic	- The organization prepares a setting that enables it to acquire new information about data protection technologies or information about the effectiveness of the protection technologies from its appropriate partners.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.DP-4	Continuously improve the process of detecting security events.	H-Advanced	- The organization creates and tunes detection rules based on various information as sources in order to improve its detection ability. - Developing the rules of correlation analysis - Developing own signature of IPSs or IDSs - Developing the organization's own black list - The organization/system analyzes the patterns of its system's communication and security alerts to create and use a profile that summarizes typical patterns of communication and security alerts, thereby tuning its efforts to reduce the numbers of false detections and false negatives.
						Advanced	- The organization prepares and manages a procedure for regularly reporting the state of organizational and system security to its appropriate staff members (e.g., management). It is desirable that the organization should define the reporting as an occasion for becoming aware of the latest threats or threats to remaining risks so that the organization acts to enhance its security. - For example, if alerts such as those shown below are issued and there is a sign of increasing security risks, raise the level of the system's monitoring activities based on information from reliable sources. * The list below is an excerpt from "Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT Version 1.0" (ISOG-J, 2018). ・Characteristics of the attack ➢ Form of the attack; contents of relevant communications ➢ Core attack code ・Traces of the attack ➢ Contents of the damaged communications ➢ Logs that remain in the server or the hands of clients ➢ Other characteristics that remain in the server or the hands of clients ・Detected names in the security products
				CPS.IM-1	Review the lessons learned from the responses to security incidents, and continuously improve the security operation process.	H-Advanced	- It is desirable for the information system to adopt an automatic mechanism for quantifying and monitoring the form, scale, and cost of a security incident that has occurred.
						Basic	- It is advisable to use information about threats and vulnerability acquired from security incident assessment for the purpose of identifying incidents that may recur or have a major impact. - Incorporate the lessons learned from the experience of handling of security incidents into the business continuity plan or emergency response plan and the education or training, thereby making necessary changes. NIST SP 800-61 shows the following as examples of points of view that may be taken when selecting the lessons. - Exactly when and what happened; - How well the staff and management handled the incident; - Whether they followed documented procedures; - Whether that was appropriate; - What information was immediately needed; - Whether any steps or actions might have hindered recovery; - What different actions the staff and management would take if the same incident recurred; - What corrective measures would prevent the occurrence of similar incidents in the future; - What additional tools and resources would be needed to detect, analyze, and reduce incidents in the future.
		A.16.1.7 Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	CPS.AN-2	Implement digital forensics upon the occurrence of the security incident.	H-Advanced	- The information system provides a procedure for processing an audit record regarding critical security incidents.
						Advanced	- The organization establishes procedures for identifying, collecting, acquiring, and saving proof according to the medium, device, and the state of the device (e.g., whether it is switched on or off). - It is desirable that the organization should retain the following evidence after the occurrence of any serious security incident: - Identification data (e.g., the location of the incident, date and time of the occurrence, serial numbers on the items, host name, MAC address, IP address); - The titles and names of the people who have collected and processed the evidence; their contact information; - Date and time the evidence was saved.
						Basic	- The organization establishes and manages procedures for identifying, collecting, acquiring, and saving data that may serve as proof.
A.17 Information security aspects of business continuity management	A.17.1 Information security continuity	A.17.1.1 Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	CPS.RP-3	Include security incidents in the business continuity plan or emergency response plan that outlines the action plans and response procedures to take in case of natural disasters.	Advanced	- The organization will establish a system of business continuity in emergency for information systems, industrial control systems and managers of related processes. This system defines the priority of the system for recovering operation when an event occurs that causes interruption in business continuity. - The organization develops and manages a business continuity plan or an emergency response plan specifically for security incidents with certain characteristics, such as that the damage the incident inflicts is less obvious than that caused by a disaster, making it difficult to specify when the business continuity plan should be carried out, or that identifying the cause of the incident has high priority. - The organization ensures that the business continuity plan or emergency response plan it develops specifically for security incidents goes along with the organization-wide policy on business continuity.
				CPS.RP-4	Take appropriate measures on goods (products) whose quality is expected to be affected by some reasons, including its production facility damaged by the occurrence of the security incident.	Advanced	- The organization provides an overview of a security incident for relevant external entities including business partners and end users, and collects detailed information about damage inflicted by the incident. - The organization coordinates actions related to recovery and post-incident processing with relevant external entities involved in the supply chain. It is advisable to identify the items for handling in accordance with the approaches included in CPS.AM-2 and CPS.AM-3.
						Basic	- The organization considers stating what to do with items produced after the incident in the business continuity plan or emergency response plan, taking into account the type of the organization's business. Note that the business continuity plan or emergency response plan may not be for security incidents.
		A.17.1.2 Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	CPS.RP-2	As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.	H-Advanced	- The organization assumes the course of action for security incidents of the supply chain and prepares a procedure that adjusts incident responses between the organization and other organizations that are concerned with the supply chain. - The organization adjusts the incident response process of an external service provider that contains important features in order to continue its business, as well as adjusting the organization's incident response process to meet the incident response requirements. - The organization interlinks information regarding threats and vulnerabilities with how individual security incidents have been handled so as to improve its understanding of the situations. [Reference] Violations in the security incidents of supply chain include violations on system components, IT products, development processes, developers, distribution processes, and warehouse facilities.
						Advanced	- The organization determines an alternative processing site in case the availability of its primary processing site has been compromised by a security incident. - The organization sets forth in the service agreement that if its primary processing function becomes unavailable, certain operations are moved to resume at the alternative processing site within the recovery time objective that the organization specifies in order to ensure that it continues to perform its critical missions and operational functions. - The organization designates an alternative processing site away from its primary processing site in order to mitigate the vulnerability to the same threats. - The organization prepares internal resources for incident handling assistance (e.g., help desk; CSIRT). These resources offer advice and support related to security incident handling and reporting for system users of the information system and industrial control system, and are an integral part of organizational ability to handle incidents.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
				CPS.CO-3	Include the item in the business continuity plan or emergency response plan to the effect that the details of the recovery activities shall be communicated to the internal and external stakeholders, executives, and management.	Advanced	- The organization provides an overview of a security incident for relevant external entities including the regulatory authorities, business partners, and end users, and collects detailed information about damage inflicted by the incident. - The organization coordinates actions related to recovery and post-incident processing with relevant external entities involved in the supply chain. An example of these actions is recalling items produced when a security incident in the production system has occurred.
						Basic	- The organization specifies roles and responsibilities taken when any security incident that may affect it occurs, along with the personnel who are assigned to these roles and responsibilities and their contact information. - The organization provides an overview of a security incident and an explanation about damage inflicted by the incident for the personnel responsible for decision-making associated with business continuity in order to ensure that the right decision is made.
		A.17.1.3 Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	CPS.IM-2	Review the lessons learned from the responses to security incidents, and continuously improve the business continuity plan or emergency response plan.	Basic	- The organization makes sure that the procedures for business continuity and the functions of relevant measures go along with the business continuity policy for higher positions. - The organization incorporates the lessons learned from the experience of handling of security incidents into the business continuity plan or emergency response plan and the education or training, thereby making necessary changes.
	A.17.2 Redundancies	A.17.2.1 Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	CPS.DS-6	Secure sufficient resources (e.g., People, Components, system) for components and systems, and protect assets property to minimize bad effects under cyber attack (e.g., DoS attack).	Advanced	- The information system and industrial control system manage spare storage space, bandwidth, and other spares (People, Components, System) and minimize the impact of service denial attacks that send a large amount of information. For example, if services provided by an attacked system can not be stopped due to maintaining the level of availability, etc., in order to continue important functions, it is necessary to take the following measures. - Automatic or manual migration to standby system - Automatic or manual segregation of system components attacked by adversal actor - In order to ensure that required system performance is satisfied, use of resources must be monitored and adjusted. In addition, storage capacity and performance required in the future must be pre-estimated. - The organization shall: (a) Use a monitoring tool which the organization specifies in order to find signs of service jamming attacks on the information system. (b) Monitor resources of information system and industrial control system identified by the organization and judge whether sufficient resource is secured to prevent effective service jamming attacks.
						Basic	- By implementing the security measures which the organization decides on, the information system and the industrial control system minimize the impact or protect from the impact of service denial attacks which the organization specifies, or from attacks on references to sources of these information, while performing a fallback operation
				CPS.DS-7	Carry out periodic quality checks, prepare standby devices and uninterruptible power supplies, provide redundancy, detect failures, conduct replacement work, and update software for IoT devices, communication devices, circuits, etc.	Advanced	- The organization prepares short-term uninterrupted power supply which supports the switching of the information system to an alternative power source that can be used for a long period of time when the primary power source is lost.
						Basic	- In order to ensure that required performance of an information system and an industrial control system is satisfied, use of resources must be monitored and adjusted. In addition, storage capacity and performance that are required in the future are pre-estimated. - The organization protects devices from power outages and other failures that are attributable to malfunctions in the support utility. - The organization protects communication cables and power cables that transmit data or that support information service from interception, interference, and harm. - The organization properly maintaines devices to ensure continuous availability and integrity.
A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.1 Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	CPS.GV-2	Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.	Basic	- Within the organization's business activities, clearly identify all related laws, regulations, and contractual requirements in the context of security as well as the organization's effort to fulfill these requirements, document them, and maintain those documents at their latest. - The organization defines and documents detailed management measures and details of responsibilities to satisfy the requirements. - The controller identifies all laws and regulations which are applied to each organization to satisfy requirements related to the type of business. - When the organization operates businesses in other countries, the controller considers to comply with the laws and regulations in all related countries.
				CPS.GV-3	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	Basic	- The organization identifies and documents all legal requirements and contract requirements related to data protection for each system and each organization and the organization's activities to satisfy these requirements, and update them to the latest. - The organization classifies its data appropriately according to the classification of the identified rules. - The organization takes measures for systems, components, etc., handling the applicable data in accordance with the requirements of the identified rules. When the implementation of a measure is considered difficult, measures such as tokenization of an applicable data in the organization may be considered. (e.g., tokenization of card information due to the Installment Sales Law)
				CPS.DP-2	Detect security events in the monitoring process, in compliance with applicable local regulations, directives, industry standards, and other rules.	Basic	- The organization sees if any legal system, industry standards, or agreements with customers that are related to monitoring services exist and, if any do, learn what constraints are imposed. - The organization conducts monitoring in accordance with the rules learned above to detect any security events. - The organization regularly reviews its monitoring activities to make sure that they conform to the rules.
		A.18.1.2 Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	CPS.GV-2	Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.	Basic	- Within the organization's business activities, clearly identify all related laws, regulations, and contractual requirements in the context of security as well as the organization's effort to fulfill these requirements, document them, and maintain those documents at their latest. - The organization defines and documents detailed management measures and details of responsibilities to satisfy the requirements. - The controller identifies all laws and regulations which are applied to each organization to satisfy requirements related to the type of business. - When the organization operates businesses in other countries, the controller considers to comply with the laws and regulations in all related countries.
				CPS.GV-3	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	Basic	- The organization identifies and documents all legal requirements and contract requirements related to data protection for each system and each organization and the organization's activities to satisfy these requirements, and update them to the latest. - The organization classifies its data appropriately according to the classification of the identified rules. - The organization takes measures for systems, components, etc., handling the applicable data in accordance with the requirements of the identified rules. When the implementation of a measure is considered difficult, measures such as tokenization of an applicable data in the organization may be considered. (e.g., tokenization of card information due to the Installment Sales Law)

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
		A.18.1.3 Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	CPS.GV-2	Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.	Basic	- Within the organization's business activities, clearly identify all related laws, regulations, and contractual requirements in the context of security as well as the organization's effort to fulfill these requirements, document them, and maintain those documents at their latest. - The organization defines and documents detailed management measures and details of responsibilities to satisfy the requirements. - The controller identifies all laws and regulations which are applied to each organization to satisfy requirements related to the type of business. - When the organization operates businesses in other countries, the controller considers to comply with the laws and regulations in all related countries.
				CPS.GV-3	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	Basic	- The organization identifies and documents all legal requirements and contract requirements related to data protection for each system and each organization and the organization's activities to satisfy these requirements, and update them to the latest. - The organization classifies its data appropriately according to the classification of the identified rules. - The organization takes measures for systems, components, etc., handling the applicable data in accordance with the requirements of the identified rules. When the implementation of a measure is considered difficult, measures such as tokenization of an applicable data in the organization may be considered. (e.g., tokenization of card information due to the Installment Sales Law)
				CPS.SC-8	Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.	H-Advanced	- The organization uses a trail storage system with the following features to flexibly fulfill the needs of clients and other related organizations, such as a third-party auditing institution, on a real-time basis. - Eligibility of the subject audit trail for the contract matter can be verified quickly. - Only authorized entities such as clients and outsourced auditing agencies can access the system. - Stored data has reliable trails such as time stamps and electronic signatures.
						Advanced	- The organization takes measures so that those records among the audit records generated by the system that are acquired over a long period of time can be obtained with certainty. - In order to protect audit records from the following threats, it is desirable for the system to apply access control with high granularity to the items and systems in which audit records are stored. - Change format of recorded message - Change or delete log file - Exceed storage space of log file medium
						Basic	- The organization preserves audit records for an appropriate period of time so as to satisfy the requirements of laws and regulations.
				CPS.IP-4	Perform a periodical system backup and testing of components (e.g., IoT devices, communication devices, and circuits).	H-Advanced	- The organization confirms the trustworthiness of the medium and integrity of the information by regularly testing the backup information.
						Advanced	- The organization backs up their system documents according to the prescribed timing and frequency. - The organization protects the confidentiality, integrity, and availability of the information backed up on the storage base.
		A.18.1.4 Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	CPS.GV-2	Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.	Basic	- Within the organization's business activities, clearly identify all related laws, regulations, and contractual requirements in the context of security as well as the organization's effort to fulfill these requirements, document them, and maintain those documents at their latest. - The organization defines and documents detailed management measures and details of responsibilities to satisfy the requirements. - The controller identifies all laws and regulations which are applied to each organization to satisfy requirements related to the type of business. - When the organization operates businesses in other countries, the controller considers to comply with the laws and regulations in all related countries.
				CPS.GV-3	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	Basic	- The organization identifies and documents all legal requirements and contract requirements related to data protection for each system and each organization and the organization's activities to satisfy these requirements, and update them to the latest. - The organization classifies its data appropriately according to the classification of the identified rules. - The organization takes measures for systems, components, etc., handling the applicable data in accordance with the requirements of the identified rules. When the implementation of a measure is considered difficult, measures such as tokenization of an applicable data in the organization may be considered. (e.g., tokenization of card information due to the Installment Sales Law)
		A.18.1.5 Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	CPS.GV-2	Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.	Basic	- Within the organization's business activities, clearly identify all related laws, regulations, and contractual requirements in the context of security as well as the organization's effort to fulfill these requirements, document them, and maintain those documents at their latest. - The organization defines and documents detailed management measures and details of responsibilities to satisfy the requirements. - The controller identifies all laws and regulations which are applied to each organization to satisfy requirements related to the type of business. - When the organization operates businesses in other countries, the controller considers to comply with the laws and regulations in all related countries.
				CPS.GV-3	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.	Basic	- The organization identifies and documents all legal requirements and contract requirements related to data protection for each system and each organization and the organization's activities to satisfy these requirements, and update them to the latest. - The organization classifies its data appropriately according to the classification of the identified rules. - The organization takes measures for systems, components, etc., handling the applicable data in accordance with the requirements of the identified rules. When the implementation of a measure is considered difficult, measures such as tokenization of an applicable data in the organization may be considered. (e.g., tokenization of card information due to the Installment Sales Law)
	A.18.2 Information security reviews	A.18.2.1 Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	CPS.IP-7	Assess the lessons learned from security incident response and the results of monitoring, measuring, and evaluating internal and external attacks, and improve the processes of protecting the assets.	H-Advanced	- The organization has its security assessed by a third party.
						Advanced	- The organization draws up a security assessment plan before the assessment is carried out that includes the following so as to ensure that its security is assessed properly and systematically: - Security measures for assessment; - Assessment procedures for measuring the effectiveness of security measures; - Settings and mechanisms for carrying out the security assessment; - Methods of putting together the results of the security assessment and applications of the results.
						Basic	- The organization regularly evaluates whether its security measures have achieved expected results (i.e., security assessment) and reports the conclusions to the chief security officer, in addition to the evaluation of whether the measures are correctly implemented and managed. - The organization makes improvements on its security measures based on the results of the security assessment.

ISO/IEC 27001:2013 Annex A				Cyber/Physical Security Framework			
Security Controls ID			Controls	Measure Requirement ID	Measure Requirement	Example of Security Measures	
		A.18.2.2 Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	CPS.RA-4	- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation. - Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.	H-Advanced	- When developing a new device or a new component which may have an impact on a physical space such as components of an industrial control system, the organization collects/analyzes accident case studies of conventional products and others to identify safety-related hazards. - The organization analyzes a situation where a hazard leads to harm and identifies the possibility of occurrence and the severity of the harm to estimate a possible risk especially regarding an industrial control system. At the time, it is desirable to check whether there is any hazard caused by a security issue. - The organization updates the risk assessment if there is a significant change in the industrial control system or the environment in which it operates, or the other change that affects the security state of the industrial control system.
						Advanced	- The organization updates a risk assessment when there is a big change in a system or an environment where a system is running (including identification of a new threat or vulnerability) or when any situation which impacts the security status of a system occurs. - When planning/designing a new system using an IoT device, the organization identifies existing assets and assets to be protected in the system to be implemented and organizes security measures according to use and configuration of the system. When handling a component or a system with a long life cycle and a component or a system requiring availability, consideration in security measures at a phase before designing is especially important. - When considering security measures applied to purchased products and services, the organization makes sure that the levels of measures correspond to the importance of such products and services.
						Basic	- The organization defines a security risk assessment process and applies it periodically (e.g., once a year). - Establish and maintain security risk criteria. - Identify security risks in the following way. 1) Clarify the target of analysis. 2) Identify incidents (including changes in circumstances) and their causes. - Analyze security risks in the following way. 1) Evaluate possible results when the above identified risks occur. 2) Evaluate the possibility of the actual occurrence of the above identified risks. - Refer to the risk criteria, determine a risk level, and prioritize the risk. - The organization documents and stores the information security risk assessment process. [Reference] An “asset-based” method and a “business damage-based” method are known as security risk assessment methods.
		A.18.2.3 Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization’s information security policies and standards.	CPS.RA-4	- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation. - Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.	H-Advanced	- When developing a new device or a new component which may have an impact on a physical space such as components of an industrial control system, the organization collects/analyzes accident case studies of conventional products and others to identify safety-related hazards. - The organization analyzes a situation where a hazard leads to harm and identifies the possibility of occurrence and the severity of the harm to estimate a possible risk especially regarding an industrial control system. At the time, it is desirable to check whether there is any hazard caused by a security issue. - The organization updates the risk assessment if there is a significant change in the industrial control system or the environment in which it operates, or the other change that affects the security state of the industrial control system.
						Advanced	- The organization updates a risk assessment when there is a big change in a system or an environment where a system is running (including identification of a new threat or vulnerability) or when any situation which impacts the security status of a system occurs. - When planning/designing a new system using an IoT device, the organization identifies existing assets and assets to be protected in the system to be implemented and organizes security measures according to use and configuration of the system. When handling a component or a system with a long life cycle and a component or a system requiring availability, consideration in security measures at a phase before designing is especially important. - When considering security measures applied to purchased products and services, the organization makes sure that the levels of measures correspond to the importance of such products and services.
						Basic	- The organization defines a security risk assessment process and applies it periodically (e.g., once a year). - Establish and maintain security risk criteria. - Identify security risks in the following way. 1) Clarify the target of analysis. 2) Identify incidents (including changes in circumstances) and their causes. - Analyze security risks in the following way. 1) Evaluate possible results when the above identified risks occur. 2) Evaluate the possibility of the actual occurrence of the above identified risks. - Refer to the risk criteria, determine a risk level, and prioritize the risk. - The organization documents and stores the information security risk assessment process. [Reference] An “asset-based” method and a “business damage-based” method are known as security risk assessment methods.

Appendix E: Glossary

(1) Actuator

<Internet of Things> IoT device that changes one or more properties of a physical entity in response to a valid input. [ISO/IEC 20924:2018]

(2) Anti-tampering devices

Device with an anti-tamper property. When used with devices, “anti-tamper” is used to describe that it is difficult to read or falsify the internal structure or stored data of the device.

(3) Audit

Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. [ISO/IEC 27000:2018]

(4) Authentication

Provision of assurance that a claimed characteristic of an entity is correct. [ISO/IEC 27000:2018]

(5) Authenticity

Property that an entity is what it claims to be. [ISO/IEC 27000:2018]

(6) Availability

Property of being accessible and usable on demand by an authorized entity. [ISO/IEC 27000:2018]

(7) Basis of trustworthiness

Point of view to ensure trustworthiness.

(8) Biometric authentication

Authentication method which identifies person by physical characteristics such as finger patterns, hand vein patterns, iris patterns or voiceprints.

(9) CC (Common Criteria)

Framework to evaluate if products and systems related to information technology are appropriately designed and properly implemented in terms of security. These criteria are defined as the international standard ISO/IEC 15408.

(10) Chief Security Officer

Person who has the highest responsibility in the operation and control of the security management systems in an organization.

(11) Confidentiality

Property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [ISO/IEC 27000:2018]

(12) CSIRT (Computer Security Incident Response Team)

A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability). [NIST SP 800-61 Rev.2]

(13) CSMS (Cyber Security Management System)

Management system of the cyber security designed for industrial automation and its control systems. The requirements are defined in the international standard IEC62443-2-1.

(14) Cyberattack

Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. [ISO/IEC 27000:2018]

(15) Cybersecurity

To prevent the leak or falsification of electronic data as well as the malfunction of IT or control systems against expected behavior.

(16) Cyberspace

Virtual space in computer systems or networks. It uses digital data to create value.

(17) Digital certificate

Data which certifies that the public key for digital signature analysis is authentic, and issued by a certification authority (CA).

(18) EDSA (Embedded Device Security Assurance) certification

Certification program related to security assurance for control devices. EDSA is developed and operated by the ISA Security Compliance Institute (ISCI) based on IEC 62443-4-2. The program evaluates the security on three aspects, namely, security at each phase of software development, implemented security features, and communication robustness test.

(19) Entity

Thing (physical or non-physical) having a distinct existence. [ISO/IEC 15459-3:2014]

(20) Firewall

Software, devices or systems installed at the border between a certain computer/network and external network in order to protect the internal network from external attack by relaying and monitoring the internal/external communication.

(21) Functional safety

Part of the overall safety of EUC (controlled devices) and EUC control systems that depend on the normal functions of E/E/PE (electric/electronic/programmable electronic) safety systems and other risk mitigation measures. [IEC 61508-4 Ed.2]

(22) Harm

Injury or damage to the health of people, or damage to property or the environment. [ISO/IEC Guide 51:2014]

(23) Hazard

Potential source of harm. [IEC 61508-4:2010]

(24) Hash function

Function which maps strings of bits of variable (but usually upper bounded) length to fixed-length strings of bits, satisfying the following two properties:

— for a given output, it is computationally infeasible to find an input which maps to this output;

— for a given input, it is computationally infeasible to find a second input which maps to the same output. [ISO/IEC 10118-1:2016]

(25) Hash value

String of bits which is the output of a hash-function. [ISO/IEC 27037:2012]

(26) Identifier

Information that unambiguously distinguishes one entity from other entities in a given identity context. [ISO/IEC 20924:2018]

(27) IDS (Intrusion Detection System)

System which monitors the external communication conducted by a server or network and alerts its controllers via e-mail when detecting unauthorized access (such as attack or intrusion attempt).

(28) Industrial control system

An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes. [NIST SP 800-53 Rev.4]

(29) Integrity

Property of accuracy and completeness. [ISO/IEC 27000:2018]

(30) IoT (Internet of Things)

Infrastructure of interconnected entities, people, systems and information resources together with services which processes and reacts to information from the physical space and cyberspace. [partly changes the definition in ISO/IEC 20924:2018]

(31) IoT device

Entity of an IoT system that interacts and communicates with the physical space through sensing or actuating.

NOTE: An IoT device can be a sensor or an actuator. [partly changes the definition in ISO/IEC 20924:2018]

(32) IPS (Intrusion Prevention System)

System which monitors the external communication conducted by a server or network and prevents attack by detecting unauthorized access (such as attack or intrusion attempt).

(33) ISMS (Information Security Management System)

Framework to operate a system by determining the required security level, establishing a plan and distributing resources through its own risk assessment in order to manage an organization. The requirements are defined in the international standard ISO/IEC 27001.

(34) ITSMS (IT Service Management System)

Framework designed for IT service providers to maintain or improve their service quality by managing their services based on the PDCA cycle. The requirements are defined in international standard ISO/IEC 20000-1.

(35) Malware

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. [NIST SP 800-53 Rev.4]

(36) Multifactor authentication

Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See Authenticator. [NIST SP 800-53 Rev.4]

(37) Multi-stakeholder process

Process in which three or more stakeholders have meetings to have discussions on an equal footing, thereby understanding each other for consensus building in order to solve a problem that could not be solved by one or two stakeholder(s). [Cabinet Office of Japan]

(38) Mutual authentication

One of the authentication methods, in which two parties authenticate with each other.

(39) Objective

Result to be achieved. [ISO/IEC 27000:2018]

(40) Physical Space

The real world. Expression to distinguish between cyberspace and world composed of substances.

(41) Private key

Secret key in the public-private key cryptosystem, a pair of different keys is used for the encryption and decryption. The private key is the one not released to the public.

(42) Process

Set of interrelated or interacting logical or physical activities which transforms inputs into outputs.

(43) Protocol

Predetermined mass of rules and steps for parties, so that more than one party can smoothly transmit signals, data and information with one another.

(44) Public key

Key of an entity's asymmetric key pair, which can be made public.

NOTE: In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key can only be available to all members of a pre-specified group. [ISO/IEC 19790:2012]

(45) Redundancy

Existence of a means in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information. [ISO/IEC 2382:2015]

(46) Resilience

The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs. [NIST SP 800-53 Rev.4]

(47) Risk

Effect of uncertainty on objectives. [ISO/IEC 27000:2018]

(48) Risk management

Coordinated activities to direct and control an organization with regard to risk. [ISO 31000:2018]

(49) Risk source

Element which alone or in combination has the potential to give rise to risk. [ISO 31000:2018]

(50) Safety

State of being protected from recognized hazards that are likely to cause harm. [ISO/IEC Guide 51:2014]

(51) Security-by-design

To introduce the measures (e.g. threat analysis, security architecture, external specification analysis and privacy impact assessment) to ensure security at the planning and designing stages for a device or system.

(52) Security event

Identified occurrence of a system, service or network state indicating a possible breach of security policy or failure of controls, or a previously unknown situation that can be security relevant.

(53) Security incident

Single or a series of unwanted or unexpected security events that have a significant probability of compromising business operations and threatening information security.

(54) Security measure organization (SOC/CSIRT)

Structure which continuously collects and analyzes the vulnerability information in or out of an organization in order to determine the appropriate scope and priority of measures against a security incident to be monitored. Security measure organization includes organizations and functions such as SOC and CSIRT. [Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT Version 1.0 (ISOG-J, 2018)]

(55) Security operation process

Document which specifies the prompt preventive measures beforehand against the security incidents to be detected.

(56) Security policy

Top management's intentions and direction formally expressed regarding security of the organization, and rules to take security measures based on such intentions and direction.

(57) Security risk

Possibility of some effects on the objectives of the organization, relevant parties such as partners, or the whole society caused by the malfunctions related to security.

(58) Security rule

What defines the details on the measures against possible security risks clarifying each scope and priority.

(59) Sensor

<Internet of Things> IoT device that measures one or more properties of one or more physical entities and outputs digital data that can be transmitted over a network. [ISO/IEC 20924:2018]

(60) Service

Output of an organization with at least one activity necessarily performed between the organization and the customer. [ISO 9000:2015]

(61) Service Provider

A provider of basic services or value-added services for operation of a network - generally refers to public carriers and other commercial enterprises. [NIST IR 4734]

(62) SOC (Security Operation Center)

A team composed primarily of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents. [RFC 2350, CNSS Instruction No. 4009]

(63) Stakeholder

Person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity. [ISO/IEC 27000:2018]

(64) Supplier

Organization or an individual that enters into agreement with the acquirer for the supply of a product or service. [ISO/IEC 27036-1:2014]

(65) Supply chain

Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer. [ISO 28001:2007, NIST SP 800-53 Rev.4]

(66) Threat

Potential cause of an unwanted incident, which can result in harm to a system or organization. [ISO/IEC 27000:2018]

(67) Time-stamp

Time variant parameter which denotes a point in time with respect to a common time reference. [ISO/IEC 18014-1:2008]

(68) Trust

Degree to which a user or other stakeholder has confidence that a product or system will behave as intended. [ISO/IEC 25010:2011]

(69) Trustworthiness

Property of deserving trust or confidence. In the context of IoT, property of deserving trust or confidence within the entire lifecycle of an Internet of Things implementation to ensure security, privacy, safety, reliability and resiliency. [ISO/IEC 20924:2018]

(70) Vulnerability

Weakness of an asset or control (3.14) that can be exploited by one or more threats. [ISO/IEC 27000:2018]

(71) Vulnerability remediation plan

A plan to perform the remediation of one or more threats or vulnerabilities facing an organization's systems. The plan typically includes options to remove threats and vulnerabilities and priorities for performing the remediation. [NIST SP 800-40 Ver.2.0]