IoT Security Safety Framework

Securing the Trustworthiness of Mutual Connections between Cyberspace and Physical Space

Version 1.0

Cyber Security Division
Commerce and Information Policy Bureau
Ministry of Economy, Trade and Industry

Nov. 5, 2020

Table of Contents

1. Necessity of this Framework

1-1 The Second Layer in CPSF (Mutual connections between cyberspace and physical space)

1-1-1 An Introduction to CPSF

In an industrial society where cyberspace and physical space are highly integrated, the processes that generate value, namely products and services (the supply chains), are changing from the conventional rigid, linear supply chains to flexible supply chains based on diverse mutual connections. The Cyber/Physical Security Framework (CPSF) is the compilation of concepts for ensuring the security of the new industrial society by organizing both the security issues of this new value creation process and the measures needed to resolve them. The CPSF stated that "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." Further, the CPSF established three different layers and anchor points of trustworthiness. The first layer places the anchor point of trustworthiness in connections between companies; the second layer places the anchor point of trustworthiness in mutual connections between cyberspace and physical space; and the third layer places the anchor point of trustworthiness in the connections in cyberspace. Finally, the CPSF identified the security issues for the economy and society overall centered on these anchor points, and compiled measures to overcome those security issues.

1-1-2 The Positioning of the Second Layer

The second layer is a border between cyberspace and physical space, and information in that border being converted accurately, in other words, securing the accuracy of the transcription and translation function, is deemed to be the anchor point of trustworthiness in the second layer. Generally, a border between cyberspace and physical space is established by so-called “Internet of Things” (“IoT”) systems, for example, sensors and actuators which provide the aforementioned transcription and translation functions. Devices and systems connecting physical space and cyberspace such as IoT offer commercial and economic benefits to the people and organizations that use them. On the other hand, in the event of an incident, those same people and organizations incur losses and bear liabilities. Therefore, securing IoT devices and systems[1] is at the core of the prescribed security measures in the CPSF second layer. A reason why the Framework covers both IoT devices and systems is that, when reviewing security measures, it is important to consider the added value provided to users through each device or system. Such value may be provided by individual devices such as sensors or actuators, or through the system that integrates those devices and other components.

On the other hand, security issues in the second layer are not uniform. Even in the CPSF, multiple cases like the following have been shown:

- As a result of cyberattacks on functions of sensors, data from the physical space is not properly transcribed and wrong data is provided to cyberspace. Trust in any operations implemented using such data will be lost.
- Due to wrong instructions from cyberspace and/or cyberattacks on IoT devices, control of the devices in the physical space is executed incorrectly. Such incorrect commands result in safety issues such as physical harm to employees and damage to devices occur
- Functions of IoT devices and systems are interrupted due to cyberattacks, system failures, etc.

Furthermore, the CPSF mentions issues in the management of IoT devices and systems connecting cyberspace and physical space as follows:

- In organizations, it is necessary to consider multilayered measures for physical security in accordance with the importance of the role borne by IoT devices. These include separating the areas where critical IoT devices are installed from other areas in order to control access at the

[1] In the Framework, referring to ISO/IEC 20924:2018, IoT is defined as “an infrastructure of entities, people, systems and information resources interconnected with services that process and react to information from physical and cyberspace”, and IoT system is defined as “a system that provides such functions”, and IoT device as “an entity that interacts and communicates with physical space through sensing or actuating in the system”. In the Framework, we do not distinguish between IoT devices and systems, and use the term "IoT devices and systems" to refer to the units that provide added value because it is important to focus on the added value provided to users using the IoT.

border, and monitoring the critical area with surveillance cameras or other appropriate tools to detect any unauthorized actions.

- Some IoT devices, such as consumer technology installed by individuals, are difficult for organizations to control, so it is necessary to consider the risks of theft, loss, etc. and other human interaction or failure when taking measures.

Therefore, when implementing security measures in the second layer, it is necessary to take into account not only a diversity of issues related to IoT devices and systems, but also the diverse environments in which IoT devices and systems are used. The CPSF organizes these diverse risk sources and requirements through a three-layered approach, and presents examples of security measures needed in each layer. It requires a combination of measures from the perspective of functional safety and cybersecurity, all with safety as the major premise.

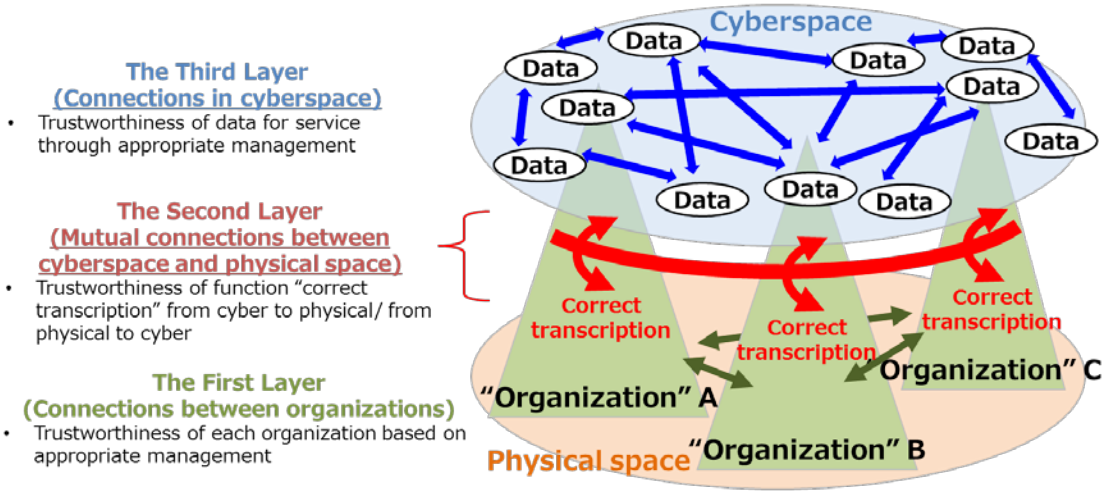

Figure 1: The three-layer model in the CPSF and the trustworthiness in each layer

1-2 Purpose of the Framework

As also mentioned in the IoT Security Guidelines,[2] IoT devices used for simple information services are different from those used in factories and social infrastructure systems, in their security level, purpose, and priority. As IoT adoption expands in the future, security measures for individual and specific IoT devices and systems in each field of use will be tailored to the peculiarities and diversity of each respective field. There is no existing uniform means to fully quantify the issues of security and safety of devices and systems connecting cyberspace and physical space. So there are concerns that

[2] The IoT Acceleration Consortium, the Ministry of Internal Affairs and Communications, and the Ministry of Economy, Trade and Industry; formulated in July 2016

unique security and safety measures, etc. will be established through separate review processes in the respective fields/industries. There is a danger that if inconsistencies arise in the respective measures, the costs of accepting and managing new mechanisms as a society will increase.

The Framework aims to avoid situations like the above by focusing on new risks brought about by the new mechanisms connecting cyberspace and physical space, and presenting the means of categorizing forms of risk and the security and safety measures for responding to those risks. In other words, its purpose is to provide the "basic common infrastructure" to enable players in different fields/industries to use the same approach for the review of the security and safety in devices and systems connecting cyberspace and physical space, and to enable society to effectively accept the new mechanisms of IoT. The purpose of the Framework is not to establish mandatory rules uniformly applying to IoT devices and systems. Note that in the Framework, IoT represents a set of devices and systems connecting cyberspace and physical space, but the Framework covers all aspects of such devices and systems.

2. Intended Readers of the Framework

Those who intend to build new mechanisms and services by constructing devices to connect cyberspace and physical space must be aware that their security issues will be diverse, and must take appropriate security measures taking into account that diversity. The more innovative the new mechanisms and services are, the greater the need to take comprehensive measures to manage the full variety of possible issues, so that the new mechanisms and services will be accepted in our society.

Therefore, the Framework should be used as a reference when creating new mechanisms and services to implement security measures for the new risks. It should also be a reference for users of those new mechanisms and services to understand the associated risks they are incurring. The following are some examples of possible Framework users:

- People who intend to utilize IoT to build new mechanisms and services connecting cyberspace and physical space
- People developing IoT devices and systems using those kinds of new mechanisms and services
- People creating management systems and environments for those new mechanisms and services
- People who are using those kinds of new mechanisms and services

3. Basic Structure of the Framework

3-1 Concepts in the Background of the Basic Structure

There are a variety of forms of new mechanisms connecting cyberspace and physical space and a variety of security issues arising from them. Furthermore, the types of possible harm if an incident actually occurs are extremely diverse. Therefore, applying uniform security requirements to the devices and systems that comprise those kinds of mechanisms, even supposing those requirements have been satisfied, is not sufficient to respond to the diverse security issues, and users will not be appropriately protected.

The key point when reviewing the second layer security measures is what kind of approach to take with respect to this diversity.

As a technique for approaching the point of contention regarding the “diversity” of new mechanisms and services connecting cyberspace and physical space, the Framework utilizes three axes consolidating the basic concepts pertaining to ascertaining the risks and the measures to those risks with regards to the devices and systems comprising these mechanisms (hereinafter referred to as “devices and systems connecting physical space and cyberspace”), categorizes them, and organizes the content of the appropriate measures to make proposals to enable them to be compared and reviewed.

3-2 Organization of Hidden Risks in Devices and Systems Connecting Physical Space and Cyberspace

Events that can result in a harmful incident involving devices and systems connecting physical space and cyberspace are extremely diverse. Incidents may impact human life, privacy, damage of assets, living environment, etc. In other words, hidden risks in devices and systems connecting physical space and cyberspace are diverse.

However, when reviewing security measures for devices and systems connecting physical space and cyberspace, it is extremely complex to analyze every possible harmful event. Therefore, it is necessary to focus on a small number of standards by extracting some common characteristics from the events that receive an impact, so that the hidden risks in the devices and systems connecting physical space and cyberspace can be organized in a simple form.

For that reason, the Framework decided to abstract and organize a variety of events receiving an impact on a variety of life safety, privacy/honor, assets, living environments, and economic activities, or the impact of harmful rumors, etc. into the following two standards and establish them as two axes

carrying out categorization of the devices and systems connecting physical space and cyberspace based on hidden risks in said devices and systems.

3-2-1 The First Axis: Degree of Difficulty of Recovery from the Incident

This first axis measures risks based on the difficulty of recovery from the incident. Regarding the difficulty of recovery, firstly, it is necessary to think about the impact on life safety more than anything else. Needless to say, if human life is lost, it cannot be recovered. Furthermore, in the case that a severe physical disability occurs as a result of the incident, there are quite a few cases in which it cannot be concluded that a full recovery is possible. Even supposing recovery is possible, there are cases in which early recovery is possible and cases in which recovery takes time. This kind of evaluation criteria regarding whether or not recovery from the incident is possible and, in the case that recovery is possible, whether or not early recovery is possible, is established as the first axis.

This first axis is similar in approach to safety measures and prohibited actions that are regulated by law in fields such as product and industrial safety, and to current security practice for existing system structures.

As shown above, the first axis firstly organized the concepts based on the point of contention of avoiding situations in which recovery of human lives/bodies is impossible, but information pertaining to privacy/honor of individual people includes sensitive information that would cause damage to the concerned individual that could not be recovered once the information was revealed, so events of the kind pertaining to the protection of information that caused unrecoverable damage to this kind of concerned individual can also be organized into issues that can be ascertained by the first axis.

Note that risks can be interpreted using both the degree of the impact of the incident and the likelihood of the incident. But the Framework instead takes the approach of carrying out the categorization based on the degree of the impact in the case that an incident has occurred, without considering the likelihood, which is comparatively difficult to compute, so that categorization taking into account the diversity of the devices and systems connecting physical space and cyberspace can be carried out easily.

However, it is appropriate to consider the likelihood when organizing specific requirements based on the Framework and based on discussions in the industry.

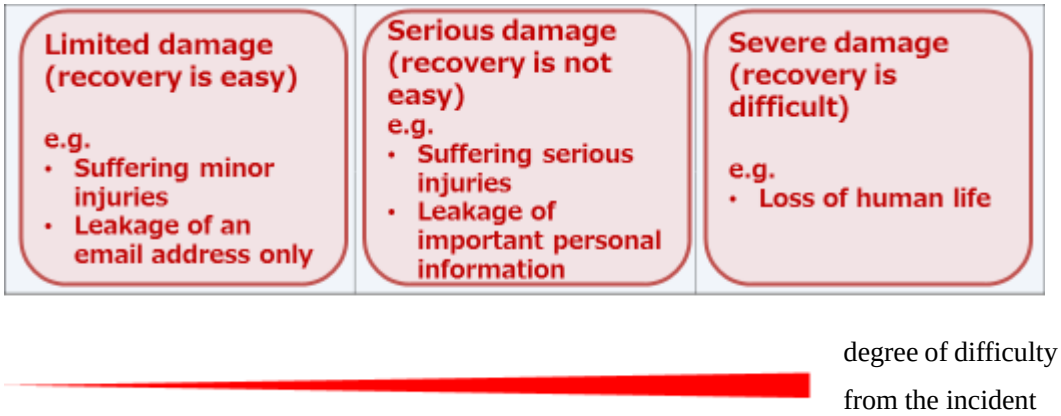

Figure 2: Image of the degree of difficulty of recovery from the incident

3-2-2 The Second Axis: Degree of Economic Impact of the Incident (conversion into monetary value)

The second axis standardizes monetary value converted from the size of the impact of the incident, excluding the aspect of the possibility and difficulty of recovery from the impact of the incident.

This standard is not concerned with recovery from the impact of life safety and privacy incidents in the kinds of cases discussed in 3-2-1. Rather it supposes that it is possible to ascertain the recovery from that impact converted into a monetary value, including factors such as damage to assets, impacts on economic activities and society, etc. by mapping them onto the second axis.

The second axis should be considered independently from the first axis, and even if there are devices and systems connecting physical space and cyberspace that are ascertained to have a low degree of difficulty of recovery in the first axis, they might be categorized as having an extremely high degree of economic impact on the second axis. On the other hand, there is a high likelihood that incidents on determined to have a high degree of difficulty of recovery in the organization in the first axis will be applicable to a similar high monetary value in the form of compensation money, etc.

Figure 3: Image of the degree of the economic impact of the incident

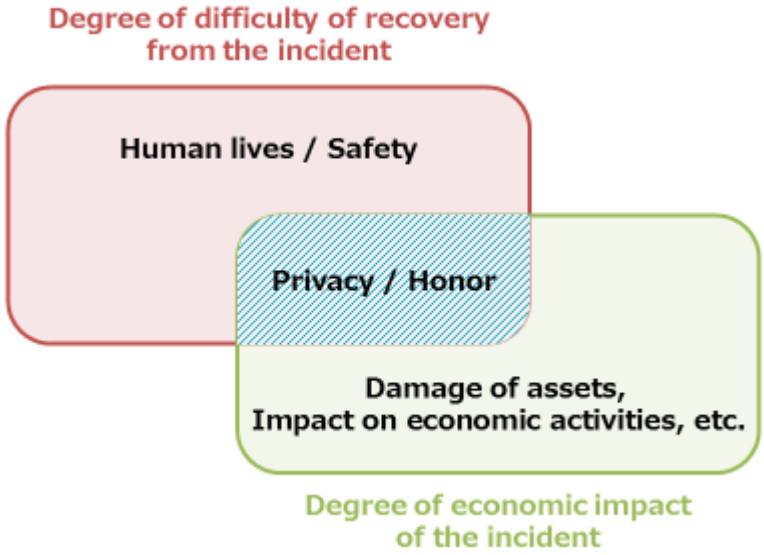

Figure 4: Organization of the privacy/honor that can be organized in the first axis

3-2-3 Categorization of Devices and Systems Connecting Physical Space and Cyberspace

Based on the aforementioned two axes, it is possible to map the devices and systems connecting physical space and cyberspace based on the hidden risks in said devices and systems.

For example, it is possible to categorize nine segments (categories) in accordance with the risks, by organizing the risks from the perspective of difficulty of recovery in the form of limited damage (recovery is easy), serious damage (recovery is not easy), and severe damage (recovery is difficult) on the first axis, and organizing the risks from the perspective of economic impact in the form of limited economic impact, serious economic impact, and catastrophic economic impact on the second axis.

This category can be utilized when reviewing appropriate measures for the respective devices and systems. As stated above, the security issues of devices and systems connecting physical space and cyberspace are diverse, so the appropriate measures in the respective devices and systems are not uniform either. However, there is a tendency for the impact of an incident to be larger for devices and systems generally categorized on the top right, so stronger measures are thought to be necessary, while on the other hand it is possible to organize those categorized on the bottom left so that it is sufficiently possible to use minor measures. The details are stated in 3-3.

Note that here we carried out a mapping of the devices and systems as an example, but focusing on the functions provided by the devices and systems comprising the services to carry out the mapping could also be considered. The units of the devices and systems can be established optionally when carrying out the mapping. Furthermore, even if it was the same device and system, its importance and issues, the impact of the incident, etc. differ greatly depending on its purpose, including what kinds of environment it will be used in, what kind of role it will have in that environment, the skills possessed by the people who will use it, etc. For that reason, it is necessary to note that even for the same device and system, the mapping can differ depending on the form of use and other factors.

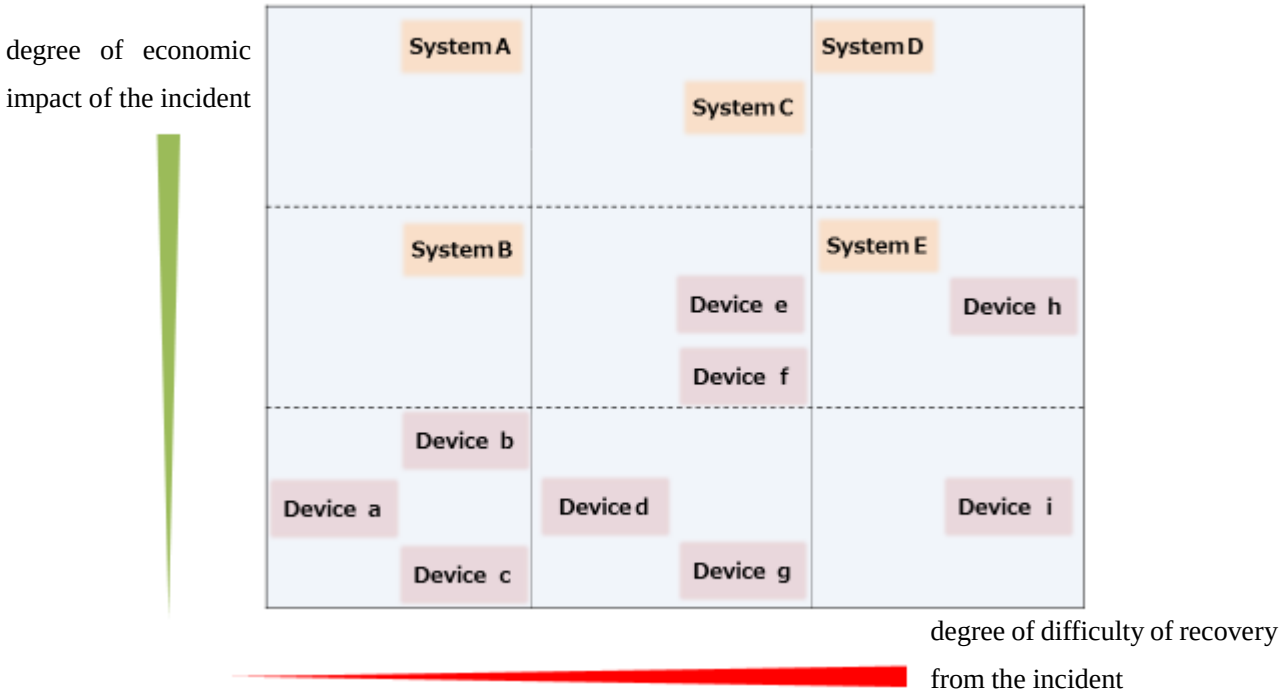

Figure 5: Image of the categorization of devices and systems connecting physical space and cyberspace

(* Even for the same device, the mapping destination can differ depending on the form of use, etc. For example, cases in which Device g and Device h are the same device and system with a different form of use, etc. are possible.)

3-3 Organization of the desired security and safety requirements

As stated in 3-2-3 above, it is possible to utilize the first axis and the second axis to categorize the devices and systems connecting physical space and cyberspace based on their risks, but it is difficult to review specific measures for the acceptance of new mechanisms and services by our society with this mapping alone. For that reason, the Framework establishes the third axis for the perspectives of desired security and safety requirements to organize the proper security measures for devices and systems connecting physical space and cyberspace.

The third axis is orthogonal to the plane formed by the first axis and the second axis, and constitutes the third dimension of the matrix. It fulfills the role of showing the perspectives of the desired security and safety requirements in the respective categories organized by the first axis and the second axis.

The third axis organizes the means of securing security and safety from the following four perspectives.

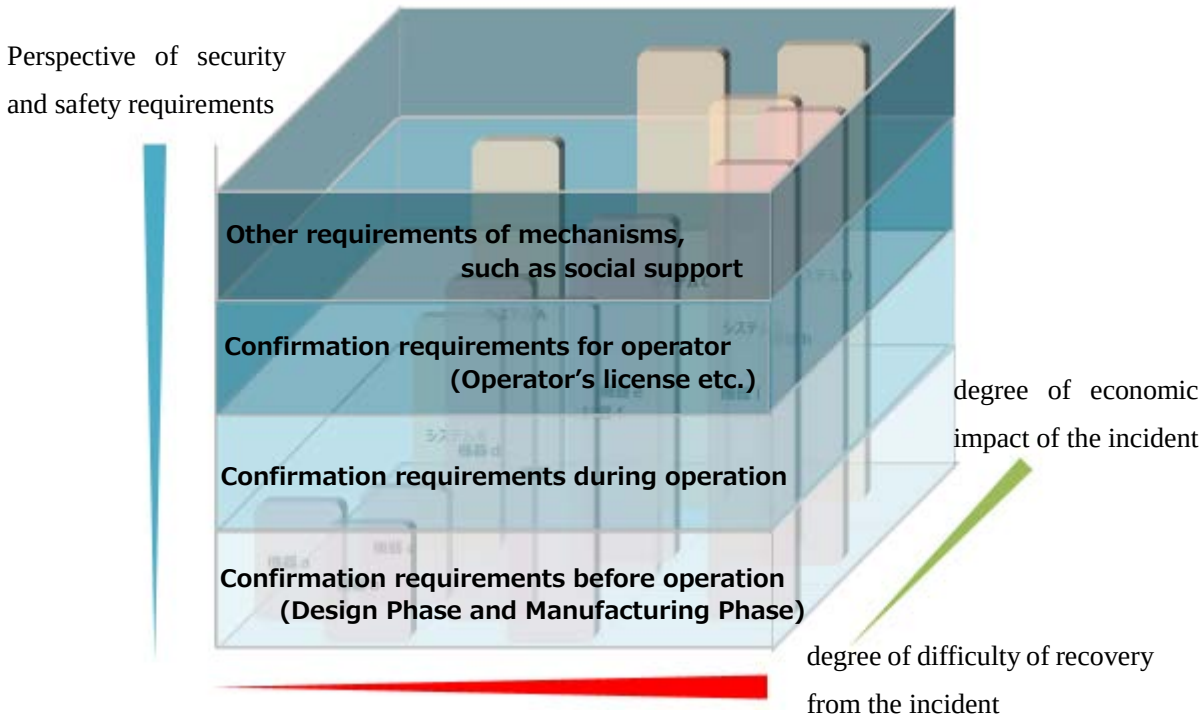

Figure 6: Image of the perspectives of the desired security and safety requirements based on the category

3-3-1 The First Perspective: Confirmation of Requirements Before Operation (Design Phase and Manufacturing Phase)

At the phase the devices and systems connecting physical space and cyberspace are manufactured and actually provided for utilization before, it is required to confirm that the necessary security and safety measures have been taken for the devices and systems themselves, and/or that the producers, suppliers, and inspectors of said devices and systems, and in some cases the production equipment and factories satisfy the necessary ability or capacity conditions, etc.

Regarding the security and safety measures, there are cases in which their content is established by the suppliers themselves and cases in which they are forcibly established by laws and regulations, etc. Furthermore, the methods for confirming that their content has been satisfied also take a variety of forms, including self-declaration, certification by a third party, etc., and the actual confirmation method is established based on the desired expertise and objectivity of the confirmation level.

3-3-2 The Second Perspective: Confirmation of Requirements During Operation

Even if proper security and safety measures are confirmed before the operation of the devices and systems, there is a possibility of unanticipated problems on the devices and systems due to breakdowns that occur during operation, implemented updates and maintenance of software, etc. In order to confirm whether those kinds of problems have occurred, it is required to inspect the devices and systems after the commencement of operation, taking into consideration their life cycle and service period.

These are security and safety measures during operation, so it is possible to secure a higher level of security and safety for devices and systems. On the other hand, it is necessary to satisfy the condition that the owners and operators of the devices and systems are involved or the ownership rights and/or management rights of the devices and systems remain on the supplier side, etc. In order to seek reliable implementation, it is necessary to implement non-technical and procedural mechanisms, such as clarifying the roles and responsibility demarcation points for each stakeholder. Note that inspections are covered here as well -- a variety of forms of inspection can be adopted, such as voluntary inspections, inspections by third parties, etc.

3-3-3 The Third Perspective: Confirmation Requirements for Operators etc. (Operator's License etc.)

When an incident can be caused by misuse or erroneous operation of devices and systems, and it cannot be prevented by the security and safety measures for the devices and systems alone, it is required to confirm that the persons who manage and operate the devices and systems possess the abilities necessary to operate and manage them appropriately. For example, in the case of automobiles, the person driving is required to obtain a driver's license proving that they possess a certain level of skill and knowledge, and social mechanisms have been constructed for the acceptance by society of skills that bring about large benefits socially even though the impact would be large in the case that an incident occurred. Note that operators in this context may include those who do not directly operate the system, such as service providers.

3-3-4 The Fourth Perspective: Other Requirements of Mechanisms (e.g., Social Support)

If the impact of an incident could be extremely large, meaning that it would not easy for the owners and/or users of devices and systems to compensate individually, it is required to prepare a social safety net, such as mandatory insurance.

For example, in the case of automobiles, a person who owns and drives an automobile is required to acquire a driver's license, and in addition, must enroll in Compulsory Automobile Liability Insurance. Due to this, a social safety net has been constructed so that even in the case that the financial resources of a driver who caused an accident are not sufficient, a minimum level of compensation is provided to any persons who were harmed.

Note that each of the four perspectives in the third axis is not necessarily completely independent of the other. For example, in order to avoid the occurrence of an incident due to misuse and erroneous operation by a user, it is necessary to conduct a review based on the characteristics of the devices and systems. From this review, it can be determined whether it is appropriate to realize this through confirmation of the abilities of the person carrying out the operation and management, as in the third perspective, or appropriate to impose an obligation to provide information such as an instruction manual to the user before the sale, as in the first perspective. When providing information such as instruction manuals to the user, it is necessary to consider how to improve the accessibility of that information. Also, it is not necessary to quantify requirements from all perspectives. For example, the measures could be driven and fulfill requirements from the first and third perspectives, even if there is no requirement from the second perspective. It can also be assumed that when the implementation of measures from a certain perspective takes much time, it can be temporarily substituted with the measures from another perspective. As shown in this example, since a risk involving multiple stakeholders can be dealt with from multiple perspectives, the burden on the stakeholders concerned should be examined comprehensively through methods such as sharing of information among all stakeholders of the risks to each individual stakeholder. Therefore, although direct measures for devices and systems are obviously important, it is not necessary for a single stakeholder to address all of the requirements, and it would be difficult to uniformly seek to specify the specific requirements required in all cases within a given perspective.

Furthermore, each perspective was established based on differences in the concepts for the content concerning security and safety requirements, so even for the same perspective, the individual security and safety measures that are specifically required are not uniform.

Note that implementation costs are dependent on the particular measures required. Costs for solutions that address requirements only up to the second perspective will not necessarily be lower than those which address all four perspectives. In addition, since the implementation of measures is directly

related to cost, it is appropriate to consider the likelihood of incidents in which particular measures are designed to prevent.

It is possible to make the Framework more sophisticated by organizing in detail the specific security and safety requirements for each perspective in each field.

4. How to utilize the Framework

In the future, it is predicted that a wide variety of new mechanisms and services will be realized by connecting cyberspace and physical space. Utilizing the Framework enables the builders of those services to categorize, analyze, and mitigate the hidden risks of devices and systems connecting physical space and cyberspace, to quantify perspectives of the desired security and safety requirements for each category, and to make comparisons among categories. Due to this, even if reviews are carried out with separate processes, it is possible to ensure the consistency of the perspectives and content of the security and safety measures required in the respective devices and systems.

What must be noted when doing this is that the effect and size of the impact differs depending on the purpose of the IoT devices and systems.

In other words, the Framework does not determine certain perspectives of security and safety requirements with respect to certain specific devices and systems. Instead, it is a framework for appropriately analyzing the impact in the case that an incident has occurred from the perspective of the user of the mechanisms and services, categorizing them in accordance with the first axis and the second axis, and utilizing the third axis to appropriately review the perspectives and content of the security and safety requirements.

In order to utilize the Framework effectively, it is required to organize use cases to refine the means of categorization using the first axis and the second axis, and to develop an environment in which the perspectives and content of the security and safety requirements can be compared using the third by accumulating use cases. Therefore, going forward, it is necessary to put in place the fundamental conditions for proceeding with the development of a systematic response to appropriately implement security and safety measures in a society where the IoT is widely utilized and cyberspace and physical space are highly integrated, by organizing specific mechanisms and services as use cases based on the Framework.

5. References

The Framework is developed with reference to the following standards and other documents based on the three-layer model introduced in Parts I and II of the Cyber/Physical Security Framework.

- The Cyber/Physical Security Framework Version 1.0
  Cyber Security Division Commerce and Information Policy Bureau Ministry of Economy, Trade and Industry
  April 2019

- Guidelines for Cyber-Physical Security Measures for Building Systems Version 1.0
  Sub-Working Group for Buildings Working Group 1 (Systems, Technologies, and Standardization) Study Group for Industrial Cybersecurity
  June 2019

- IoT Security Guidelines Ver. 1.0
  IoT Acceleration Consortium, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry
  July 2016

- ISO/IEC 20924:2018
  “Information technology — Internet of Things (IoT) — Vocabulary”
  December 2018

- ISO/IEC 27001:2013
  “Information technology — Security techniques — Information security management systems — Requirements”
  October 2013

- IEC 61508:2010
  “Functional safety of electrical/electronic/programmable electronic safety-related systems”
  April 2010

- IEC 62443-2-1:2010
  “Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program”
  November 2011

- IEC 62443-3-3:2013
  “Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels”
  August 2013

- ETSI EN 303 645 V2.1.1
  “CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements”
  ETSI
  June 2020

- REGULATION (EU) 2019/881（Cybersecurity Act）
  THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION
  April 2019

- SB-327 “Information privacy: connected devices”
  The State of California
  September 2018

- Cybersecurity Framework Version1.1
  NIST
  April 2018

- NISTIR 8200
  “Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)”

NIST

November 2018

- NISTIR 8228

  “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks”

  NIST

  June 2019

- NISTIR 8259

  “Foundational Cybersecurity Activities for IoT Device Manufacturers”

  NIST

  May 2020

- NISTIR 8267 (Draft)

  “Security Review of Consumer Home Internet of Things (IoT) Products”

  NIST

  October 2019

- NISTIR 8276 (Draft)

  “Key Practices in Cyber Supply Chain Risk Management: Observations from Industry”

  NIST

  February 2020

- White Paper “Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)”

  NIST

  April 2020

- Code of Practice for Consumer IoT Security

  UK Department for Digital, Culture, Media & Sport

  October 2018

- Internet of Things (IoT) Security Policy Platform Statement
  Internet Society (ISOC) IoT Security Policy Platform
  November 2019