

The Cyber/Physical Security Guidelines for Factory Systems

Ver 1.0



November 16, 2022

Study Group for Industrial Cybersecurity
Working Group 1 (Systems, Technologies and Standardization)
Factory sub-working group

Change history

Issue date	Version	Overview
November 16, 2022	Ver 1.0	Ver 1.0 issued

Table of Contents

1	Introduction	1
1.1	Purpose of factory security guidelines	1
	[Reference] Examples of the effects caused by security threats in factory systems	4
1.2	Scope of guidelines.....	5
2	Assumed factory of this guideline.....	6
2.1	Assumed company	6
2.2	Assumed organizational structure.....	7
2.3	Assumed production line	7
2.4	Assumed business.....	9
2.5	Assumed data	9
2.6	Assumed zone	10
3	How to proceed with planning and introduction of security measures	14
3.1	Step 1 Organize internal and external requirements (management efforts, laws, etc.), operations, protection targets, etc.	16
3.1.1	Step 1-1 Arrangement of requirements necessary for studying and planning security measures.....	16
3.1.2	Step 1-2 Arrangement of operations	20
3.1.3	Step 1-3 Setting the importance of business.....	21
	[Reference] Importance of business (example in assumed factory)	21
3.1.4	Step 1-4 Arrangement of the protection target	22
3.1.5	Step 1-5 Setting the importance of the protection target.....	24
3.1.6	Step 1-6 Organize zones and connect zones with operations and protected objects	25
3.1.7	Step 1-7 Zones and the impact of security threats organized.....	27
	[Reference] Attacker's motive	34
	[Reference] Declaration of efforts by management.....	35
3.2	Step 2 Planning security measures	37
3.2.1	Step 2-1 Formulation of security measures policy	38
	[Reference] Example of security requirement level concept.....	38
	[Reference] Extent of measures	40
3.2.2	Step 2-2 Correspondence of security measures against assumed threats	43
	(1) Measures for system configuration	49
	(2) Physical measures.....	54
	[Reference] Concept of entry / exit management.....	58
	[Reference] Department in charge of physical security operation and management.....	59
3.3	Step 3 Implementation of security measures and constant review of plans, measures, and operation systems	61

(1) Life cycle measures	61
[Reference] Operation management system (examples).....	67
(2) Supply chain measures	71
[Reference] Security certification systems for control systems and the IoT	72
[Reference] Subcontracting promotion standards	73
[Reference] Consideration of measures in operating factories and new factories	74
[Reference] Strategy execution management	74
Annex A Terms/Abbreviations.....	77
Annex B Social Security Requirements Surrounding Factory Systems.....	82
B-1 Requirements for compliance with laws and regulations, standards and guidelines.....	82
B-1.1 Requirements for security measures based on laws and regulations	82
[Reference] Security Laws and Regulations by Industry.....	82
B-1.2 Requirements for compliance with standards and guidelines related to security..	84
[Reference] Major guidelines for security incident response	89
B-2 Requirements from national and local government	92
B-3 Requirements from industry.....	92
[Reference] Requirements by industry	92
B-4 Requirements from the market and customers.....	93
B-5 Requests from client company	94
B-6 Requests from investors.....	94
Annex C Approach to Security Measure Levels in Relevant Documents.....	95
C-1 Typical security measure evaluation criteria.....	95
C-2 Examples of definitions of the extent to which security measures are implemented	96
Annex D Related/Reference Materials	99
Annex E Checklist	102
Annex F Procurement Specification Template (Examples).....	108
Column 1: Trends in security of factories	110
Column 2: Security seen in terms of the purpose of the factory system and value of the manufacturing industry / factory	116
Column 3: Flow to smart factories	118
Column 4: Use of the cloud in factories	120
Council of this Guideline.....	121
Acknowledgments	123

Please utilize the correspondence table shown below which states the facts about factory security that we think the reader would like to know and where those answers are stated in this guideline.

	What I want to know about factory security	Where the answer is stated in this guideline
1	I would like to know what process should be followed for factory security measures.	3. How to proceed with planning and introduction of security measures (P14-P75)
2	I would like to know what kind of factory security measures are available.	3.2. Step 2: Planning security measures (P37-P60) 3.3. Step 3: Implementation of security measures, and constant review of plans, measures, and operation systems (construction of PDCA cycle) (P61-P75)
3	I would like to know what the cybersecurity environment surrounding the factory is like. I would like to know what kind of damage was done in the past by a cyberattack on a factory.	Column 1 Trends in security of factories (P110-115)
4	I would like to know about requirements that need to be considered when thinking about factory security.	Annex B Social Security Requirements Surrounding Factory Systems (P82-P94)
5	I would like to know how to manage the security of the factory.	3.3. Step 3: Implementation of security measures, and constant review of plans, measures, and operation systems (implementation of PDCA cycle) (P61-P75)
6	I would like to know what kind of approach is used in prioritizing protection targets, operations, and security measures.	Annex C Security requirement levels (P95-P98)
7	I would like to know about related industry standards and international standards. I would like to know what kinds of requests we may receive from whom when operating a factory.	Annex B Social Security Requirements Surrounding Factory Systems (P82-P94) Annex D Related/Reference Materials (P99-P101)
8	I would like to have a concrete image of the extent to which measures have been taken.	Annex E Checklist (P102-P107)
9	I would like to imagine what kind of things should be specifically included in the procurement specifications when procuring products.	Annex F Procurement Specification Template (Examples) (P108-P109)
10	I would like to know the meanings of the terms and abbreviations shown in this guideline.	Annex A Terms/Abbreviations (P77-P81)

1.1 Purpose of factory security guidelines

Factory systems (industrial control systems (ICS / OT), their constituent equipment, and connected systems / equipment)¹ have been designed on the assumption that they will not be exposed to networks such as the Internet, etc. as an internal network. However, in the flow of IoT and automation, the possibility of utilizing the operation data of individual machines and devices has expanded, and while efforts to create new added value are being promoted, new sources of security risks are also increasing due to increasing needs and opportunities for the networks of factories, etc. to be connected to networks such as the Internet, etc. Furthermore, due to the fact that factory DX (digital transformation) is being promoted, security in manufacturing sites connected in the cloud and supply chain must also be considered. On the other hand, there are also cases in which even factories thought to have few opportunities to connect to the Internet in this way receive attacks from unauthorized intruders, etc.

Moreover, cyberattacks are becoming more sophisticated and cleverer, and there are cases of specific factories being targeted by attacks with the purpose of gaining important information or money and also cases in which the victim of a chance attack not intended by the attacker is a factory.

Therefore, it is necessary to be aware of the fact that there is a possibility of receiving a cyberattack in any factory.

In particular, factories have the following characteristics, and cybersecurity measures that meet these characteristics are required.

- In addition to data protection, which is common in the IT security field, maintenance of equipment operation and ensuring safety are required².
- It is necessary to introduce step-by-step security measures for existing systems, such as when old equipment is in operation³.
- The measures to be taken differ depending on the scale and nature of the factory.

Also, in general, in manufacturing / factories, the following value is emphasized:⁴

- Ensuring safety (S: Safety)
- Business / Production Continuity (BC)
- Quality assurance (Q: Quality)
- On-time delivery / delay prevention (D: Delivery)
- Cost reduction (C: Cost)

¹ In addition to the FA (Factory Automation) system, referable content is also included in the PA (Process Automation) system, so we expect that they will be read as appropriate.

² If an abnormality occurs in the maintenance of equipment operation, etc. or ensuring safety due to a security failure, there is a possibility that our own assets will be damaged, and in addition there is a possibility of an environmental impact, etc. occurring in the neighborhood, so a duty to explain to society and the residents could also arise.

³ When introducing security measures, with stopgap measures, namely carrying out measures on occasion without considering the impact on the business, there is a possibility that the effect of the security measures will be weakened and in the end expenditure will increase, so it is desirable to firstly consider the impact on the business and then plan timely and appropriate security measures and costs expenditure.

⁴ In factories, it is common to formulate a business continuity plan for business / production continuity (BC), but it does not necessarily aim to maintain the operation of the factory, and cyberattacks deprive the control of the factory system. In this case, it may be possible to choose to actively shut down the factory system to ensure safety (S).

As shown in Table 1-1 and Figure 1-1, in the industry classifications for the Industrial Statistics Survey in the Ministry of Economy, Trade and Industry Industrial Statistics Survey, manufacturing is divided into 24 types, and the shipment value and number of establishments differs for each industry type. In this way, the classification, scale, equipment and systems possessed by the factories vary widely and the items to be implemented differ depending on the industry / industry type, so this guideline is not targeted from the perspective of a specific industry / industry type or the product to be manufactured.

Furthermore, this guideline presents the thinking and the steps which industrial groups and individual companies should refer to when planning and executing their own measures as a “Guidebook”⁵ and clearly states the measures which are thought to be the minimum necessary, from technical measures to operational and management measures against threats.

What is important is that industry groups and individual companies organize the environment of the industry / industry type surrounding their factories, weigh the environment and the values that the industry / industry type emphasizes, and maintain and develop the values. Thinking about what kind of factory security is necessary to make it possible, while referring to the ideas, steps, and countermeasures shown in this guideline, we will create guidelines according to the circumstances of the industry and industry type, and take action such as advancing security measures for the factory.

The purpose of this guideline is to raise the security level of the entire industry, especially the factory system, by planning and implementing the security measures of the factory by each industry / industry type.

As a result, it is expected that it prevents the value of BC / SQDC from being damaged by cyberattacks, and further, by ensuring security, IoT and automation are progressing, and new added value is created from the sites of many factories.

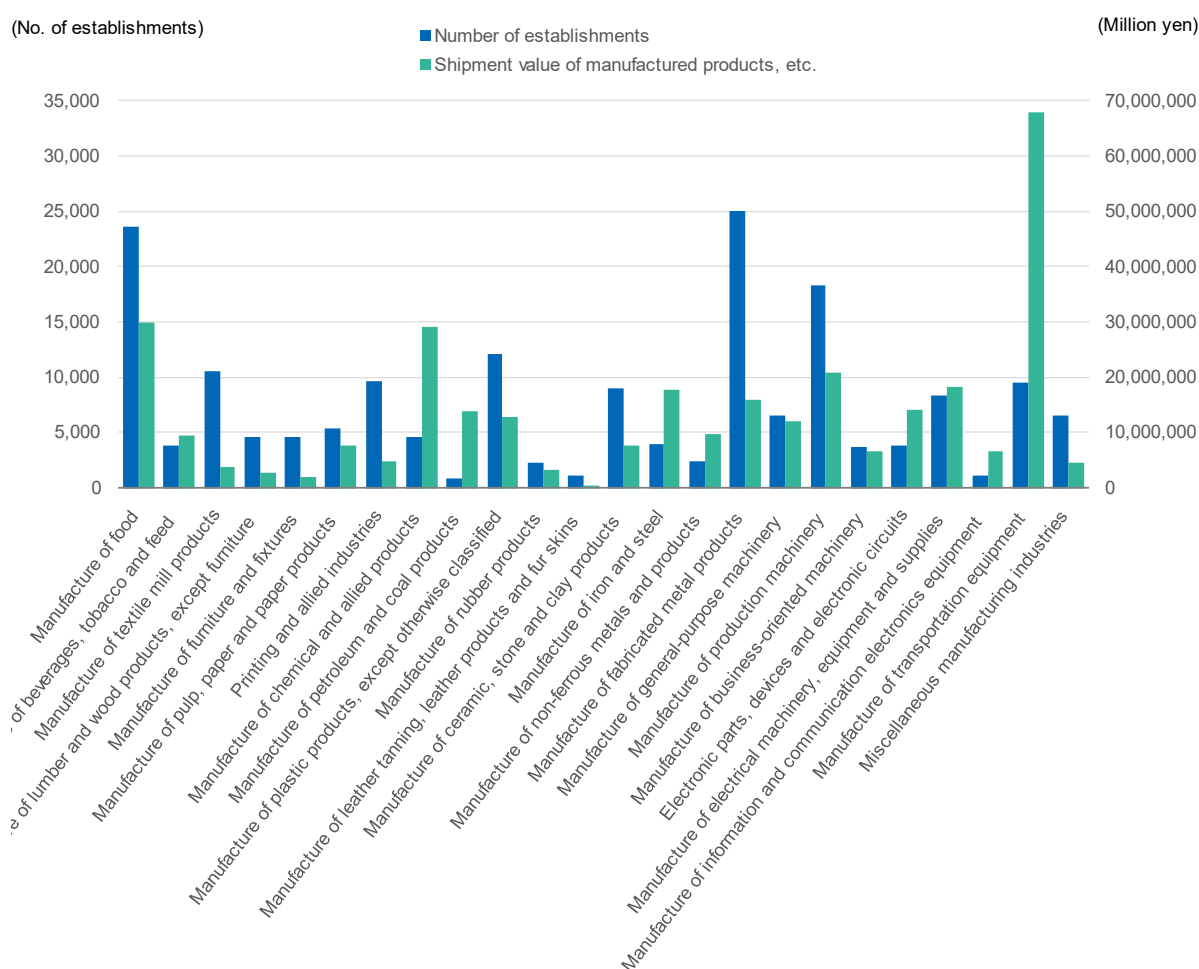
Table 1-1 Manufacturing classifications

	Classification name		Classification name
1	Manufacture of food	13	Manufacture of ceramic, stone and clay products
2	Manufacture of beverages, tobacco and feed	14	Manufacture of iron and steel
3	Manufacture of textile mill products	15	Manufacture of non-ferrous metals and products
4	Manufacture of lumber and wood products, except furniture	16	Manufacture of fabricated metal products
5	Manufacture of furniture and fixtures	17	Manufacture of general-purpose machinery
6	Manufacture of pulp, paper and paper products	18	Manufacture of production machinery

⁵ This shows the thinking which takes into consideration as much as possible the effects that security measures have on BC/SQDC, such as the effects on product costs arising from the introduction of security measures and the effects on operation and quality arising from process changes, etc.

7	Printing and allied industries	19	Manufacture of business-oriented machinery
8	Manufacture of chemical and allied products	20	Electronic parts, devices and electronic circuits
9	Manufacture of petroleum and coal products	21	Manufacture of electrical machinery, equipment and supplies
10	Manufacture of plastic products, except otherwise classified	22	Manufacture of information and communication electronics equipment
11	Manufacture of rubber products	23	Manufacture of transportation equipment
12	Manufacture of leather tanning, leather products and fur skins	24	Miscellaneous manufacturing industries

Reference) Created based on the Ministry of Economy, Trade and Industry Industrial Statistics Survey (2020 confirmation)



Reference) Created based on the Ministry of Economy, Trade and Industry Industrial Statistics Survey (2020 confirmation)

Figure 1-1 Number of establishments in the manufacturing industry, shipment value of manufactured products, etc. (2019)

[Reference] Examples of the effects caused by security threats in factory systems⁶

- Impact on product business growth and business / production continuity (BC: Business Continuity)
- Impact on factory safety (S: Safety), product quality assurance (Q: Quality), on-time delivery / delay prevention (D: Delivery), and cost reduction (C: Cost)
- Ensuring normal operation of factory systems and equipment, obstructing the realization of proper feedback control
- External leakage of information and data related to products and production (know-how)
- Expanding security issues to engineering chains, supply chains, and value chain partners using equipment from their own factories as a stepping stone
- Unintentional unauthorized external use / control by unauthorized parts or malicious functions (malware) contained in the product, obstruction of product operation, external leakage of product user information
- Impact on the health of employees due to unexpected operation of the equipment
- Impact on the lives of neighborhood residents due to disasters triggered by unexpected operation of the equipment

⁶ In order to alleviate these effects, it is necessary to ensure the security factors of the factory system and its components (the network, devices and components, functions and programs, and data), namely their availability, integrity, and confidentiality. In order to secure these security factors, the security functions for realizing authenticity, access control, accountability and non-repudiation for the system users and each of the devices, components, functions, programs, and data which comprise the system are necessary.

1.2

Scope of guidelines

The assumed readers of this guideline are mainly the following, but it is important to communicate to plan and implement security measures while recognizing the differences in positions and values between departments and departments in charge of IT related departments and production-related departments. The environment each person and department is placed in and their values vary considerably. For example, the IT related departments place importance on the performance of not only the factory systems but also the overall systems possessed by their company whereas the production sites place importance on product manufacturing delay prevention, maintenance of operation, ensuring safety, etc.

- IT related departments (information system department, security department, etc.)
- Production-related departments (production engineering department, production control department, work department, etc.)⁷
- Strategic management department (business planning, etc.)
- Audit department
- Risk management department
- Equipment system provider vendors and equipment manufacturers (including suppliers that make up the supply chain)

This guideline is mainly for business people, the intended readers, but if you think that the concept of security has not properly penetrated the management (CTO, CIO, CISO, etc.), refer to this guideline. At the same time, we expect that the intended readers will communicate appropriately with the management and other decision-makers. For the promotion of security, the construction of a system by decision-makers such as management, etc. and appropriate instructions to the organization through the system are important.

The following devices and systems are assumed to be the scope of this guideline.

- The equipment and systems covered by this guideline are industrial control systems (ICS / OT) in factories, regardless of whether they are new or existing, and do not cover office-related information systems (IT).

⁷ The person who plays a central role in the department may be, for example, the creator of equipment devices / systems and security procurement requirements, or the builder / administrator, operator, and maintenance person of the devices / systems.

Generally speaking, even if it is called a factory system, there are differences in the equipment that composes it and the system to be connected depending on the size of the scale and the products to be manufactured, but in this chapter, when presenting the security measures for the factory system, a factory is set as an assumed factory from the viewpoint of easy understanding.

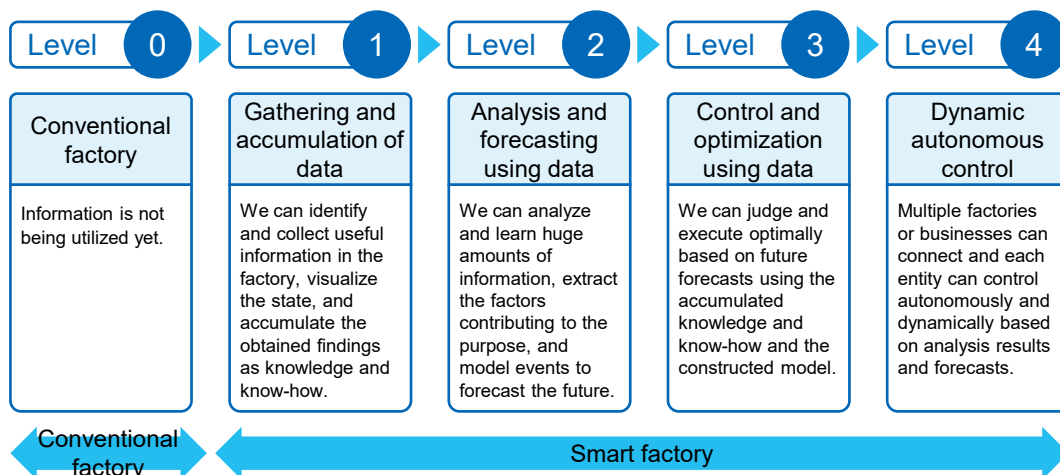
The assumed factory shows one specific example when advancing the measure steps from Chapter 3 onward, and since it is considered that there are some parts where the environment in which the reader is placed and the assumed factory do not always match, we expect that they will be read as appropriate in accordance with the environment of the reader.

2.1

Assumed company

- DX (digital transformation) is required by business owners
- Electronic device manufacturer
- There are factories at multiple bases, and products are produced at each base.
- The bases are connected to each other by the network between bases managed by the head office, but the network within the base is managed for each base.
- We have been able to identify and collect useful information in the factory, visualize the state, and accumulate the obtained findings as knowledge and know-how.⁸

⁸ In such a case, according to the Ministry of Economy, Trade and Industry's "Survey for Ensuring Cyber Security in Smart Factories", it corresponds to Level 1 of the stage of a smart factory. A smart factory is a factory that realizes advanced manufacturing management through data utilization and analysis. In general, as the level goes up, the connection with cyberspace becomes stronger, and as a result, the security risk is thought to increase, so it is important to take security measures according to the level.



Reference) Ministry of Economy, Trade and Industry "Survey for Ensuring Cyber Security in Smart Factories" (March 2021)

2.2**Assumed organizational structure**

- Production engineering / management department:
Construction and management of production line equipment (mainly managing the equipment network in Figure 2-1).
- Work department:
Operate the production line and carry out actual production based on the production plan.
- Sales department:
Implementation of product sales management and customer management.
- Materials department:
Procurement and management of materials required for production.
- Quality control department:
Carry out inspections and management to ensure the quality of products, parts and components.
- Information systems department:
We manage networks, servers, and terminals, mainly for OA (Office Automation) systems (mainly managing the information network and production management network in Figure 2-1).

The number of related organizations in an actual company may be larger than this, but in order to make it easier to understand the role of each organization, the above 6 departments are used.

2.3**Assumed production line**

- The production line produces printed circuit boards to be incorporated into electronic equipment.
- Production itself is automated, and multiple models can be produced based on production instructions.
- Factory employees carry out setup, replenishment of parts, etc.
- There are multiple production lines in the factory, and different models can be produced independently.
- Production facilities (equipment / device) is introduced from the equipment vendor, and the production engineering / management department builds and manages the production line.
- Equipment maintenance is carried out by the equipment vendor.
- In the automated warehouse, the equipment vendor remotely monitors the condition and performs on-site maintenance in preparation for maintenance.

The following is an example of a factory system including an assumed production line and its components. This guideline presents security measures using this factory system example.

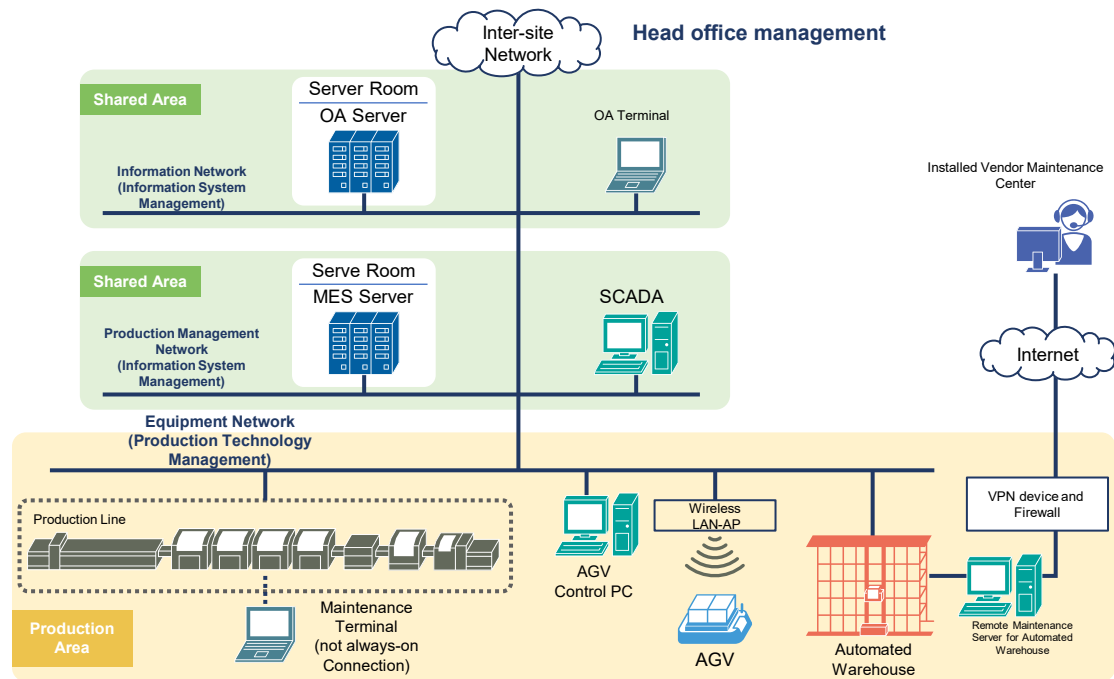


Figure 2-1 Factory system example

Network⁹

- Equipment network:¹⁰
Network to which production facilities are connected
- Production control network:
Network to which servers that perform production control are connected
- Information network:
Network to which terminals for OA business and product design are connected

Equipment / device (function / program)¹¹

- VPN equipment and firewall:
Equipment used by equipment vendors for remote access to achieve secure communication. Built-in access control function to prevent access from anywhere other than the equipment vendor's maintenance center.
- Wireless LAN-AP:
Network equipment for communication with AGVs.
- MES server:
A server that manages production plans, data on production results, and gives production instructions to production lines.
- Production line:
Equipment used to produce products.
- SCADA:
PC that monitors the production status of the production line.
- Maintenance terminal (always disconnected):
PC used for maintenance of production facilities.

⁹ Security factors include availability, integrity, and accountability.

¹⁰ In recent years, routes for directly connecting to the Internet from the equipment network and production information network without going through the information network have been increasing, but even in such cases the steps and measures shown in this guideline can be utilized. It is desirable to implement security specific to the cloud after consulting with the vendors, etc. and also referring to Column 4.

¹¹ Security factors include availability, integrity, authenticity, and accountability.

- AGV control PC:
A PC that formulates an operation plan for an AGV and controls the AGV.
- AGV:
Device to carry parts.
- Automatic warehouse:
Equipment for storing and loading and unloading parts.
- Automated warehouse remote maintenance server:
Server used by equipment vendor maintenance center to remotely maintain automated warehouse.
- OA server:
A server used for office purposes. Assuming sales management tools, in-house workflow systems, file servers, etc.
- OA terminal:
PC used for office use.

2.4**Assumed business**

- Production planning setting
- Production (+ inspection)
- Production status monitoring (on-site)
- Replenishing materials (to the site)
- Purchase parts (to warehouse)
- Productivity analysis
- Refer to traceability data
- Maintenance
- Remote maintenance

In the factory system, it is important to continue to produce products of stable quality as planned in consideration of safety, so the importance varies depending on the business.

2.5**Assumed data**

Business operations are affected by production facilities and network outages and failures, but it is expected that business operations will also be affected by the loss, falsification, and leakage of stored data.

Below we list examples of data that threatens BC / SQDC, such as production line outages and production know-how leaks, due to data loss, falsification, leaks, or temporary outages of data access.

- Production planning
- Production instructions (production model / quantity)
- Production recipe
- Production results (traceability data)
- Equipment status
- Equipment programs, parameters, drawings
- Parts inventory (on-site)
- Parts inventory (warehouse)

2.6

Assumed zone

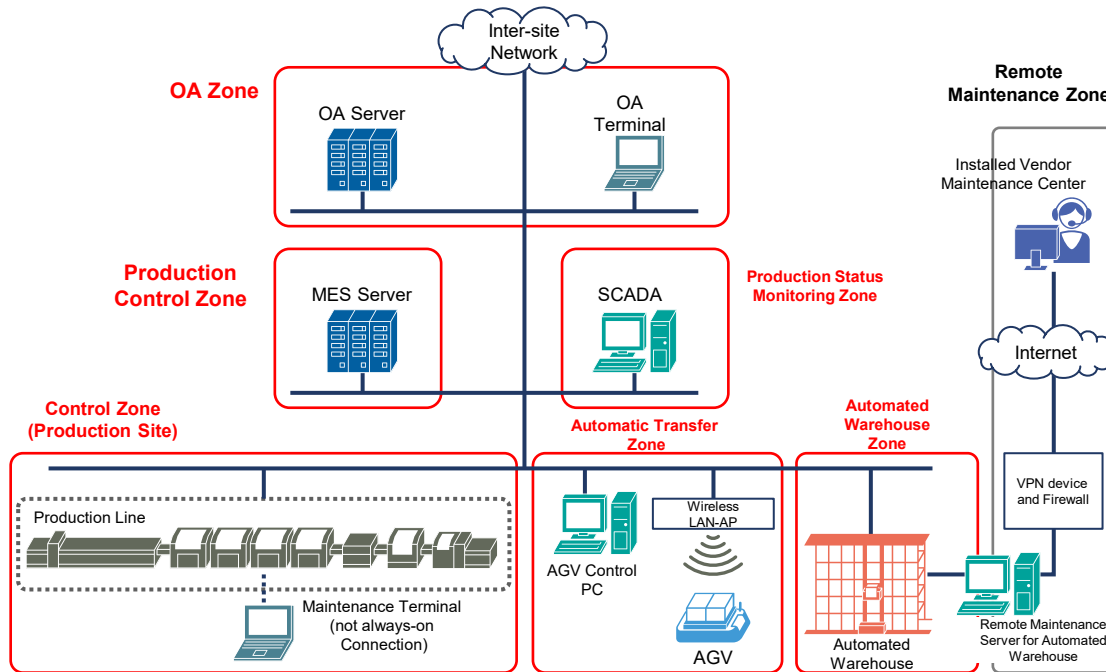


Figure 2-2 Zone definition example

The factory system assumes the following zones ¹² in consideration of business content and business importance.

Below is an overview of each zone and examples of related operations.

Table 2-1 Zone overview

	Name	Overview	Related business
1	Control zone (production site)	A production line for producing products. Zone consisting of control devices and equipment.	<ul style="list-style-type: none"> • Production (+ inspection) • Production status monitoring (on-site) • Replenishing materials (to the site) • Maintenance
2	Automatic transport zone	A zone for operating AGVs that transport parts and finished products.	<ul style="list-style-type: none"> • Replenishing materials (to the site)
3	Automated warehouse zone	A zone that operates equipment that automatically enters and exits while storing parts.	<ul style="list-style-type: none"> • Replenishing materials (to the site) • Replenishing materials (to warehouse)
4	Production control zone	A zone consisting of servers that manage production plans, traceability data, etc.	<ul style="list-style-type: none"> • Production planning setting • Production (+ inspection) • Production status monitoring (on-site)

¹² A zone is defined as an area in which the content and importance of the operations is equal. Security measures at an equal level are necessary with respect to protected assets which exist in the same zone.

			<ul style="list-style-type: none"> • Productivity analysis • Refer to traceability data
5	Production status monitoring zone	A zone consisting of equipment that acquires and visualizes production status and equipment information.	<ul style="list-style-type: none"> • Production status monitoring (on-site) • Productivity analysis • Refer to traceability data
6	OA zone	Zones where operations not directly related to production are performed.	<ul style="list-style-type: none"> • Production planning setting • Replenishing materials (to warehouse) • Productivity analysis
7	Remote maintenance zone	A zone for equipment vendor maintenance center to remotely monitor automated warehouses	<ul style="list-style-type: none"> • Remote maintenance

The remote maintenance zone is assumed to be the management area of the equipment vendor under the management responsibility of the production engineering / management department.

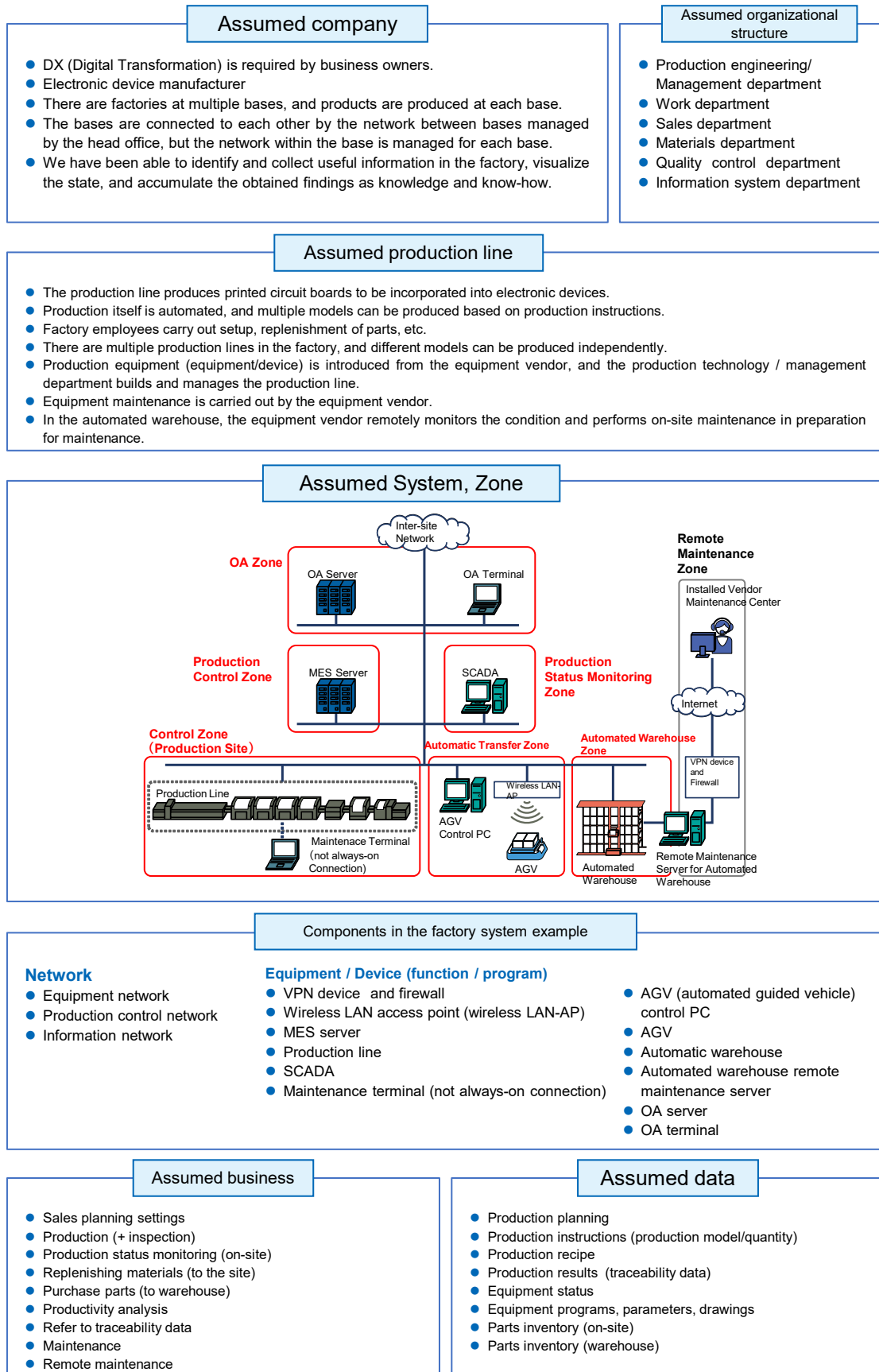


Figure 2-3 Assumed factory of this guideline

As stated in 1.1, the classification, scale, equipment and systems possessed by the factories vary widely, so even if you start from a certain abstract model and attempt to apply that model to a site to plan a policy for taking specific measures, there is a possibility that you will not be able to plan effective security measures due to exceptions occurring in which the actual state of the site and the model do not match. Therefore, in order to ensure that effective measures which do not contradict the nature of the site can be planned, rather than the approach of planning specific measures based on a certain abstract model, we present the approach of starting from the operations and protection targets of the site, setting zones in order to get a bird's eye view of the equipment and systems of the factory as large category concepts, and then planning the security measures.

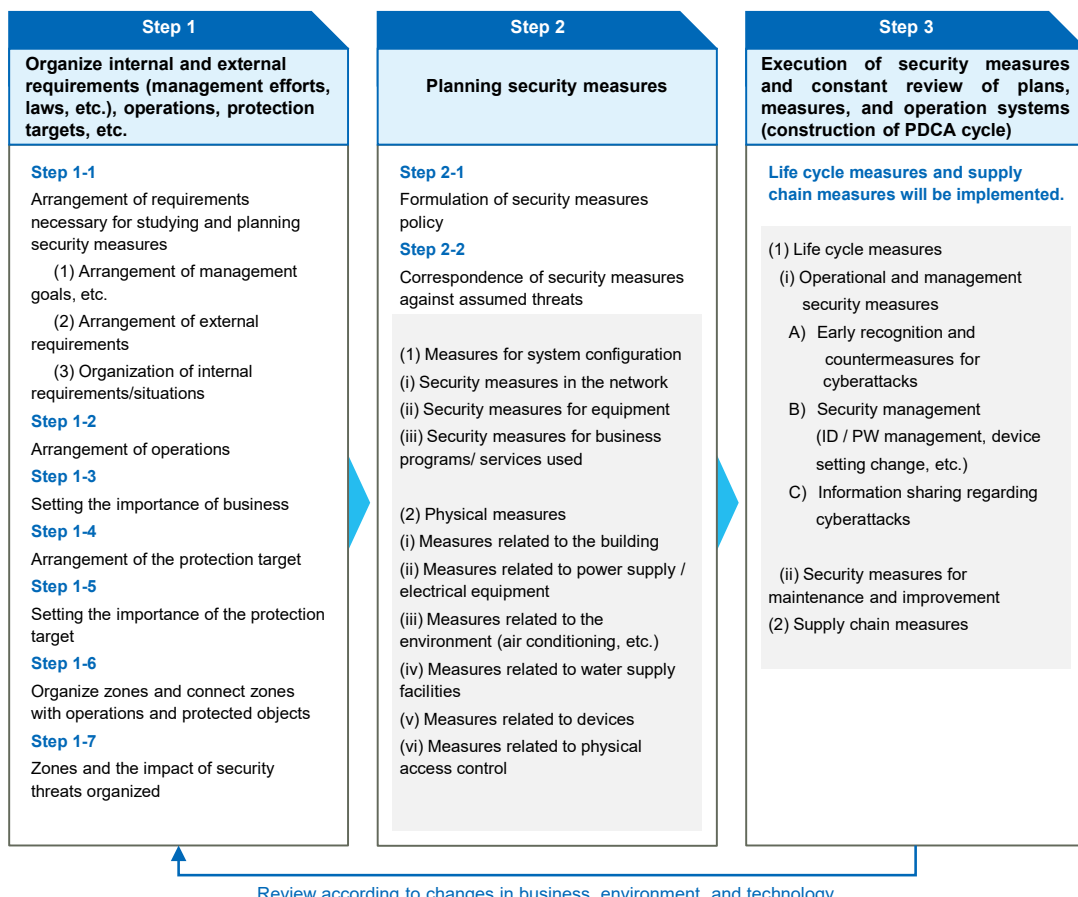
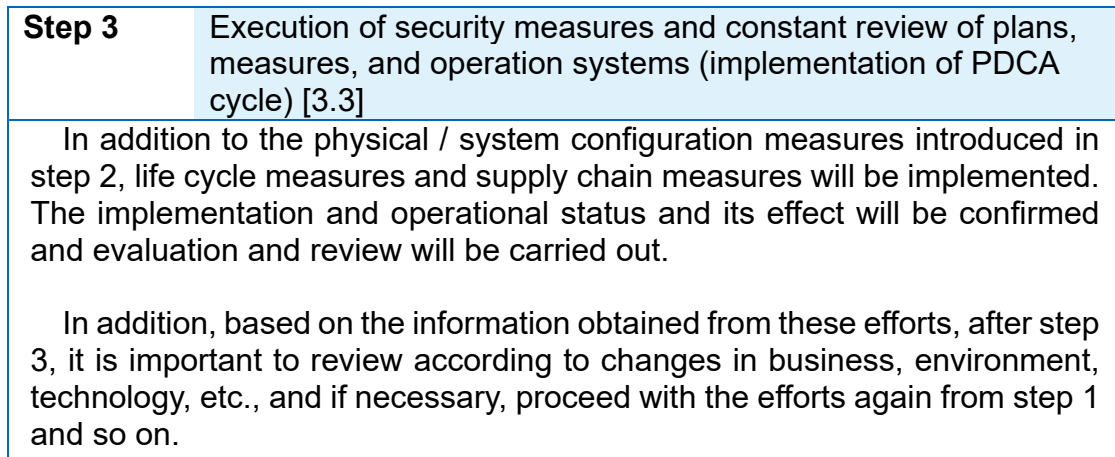
This section outlines the steps for planning and introducing security measures for factory systems¹³. What is important is continuously advancing security measures and realizing an appropriate cost. In order to realize this, it is necessary to apply the cycle from step 1 to step 3 while carrying out constant review of each step, in accordance with changes, etc. in the business environment and technology trends.

However, the contents of the table etc. in each step exemplify what can be considered based on the assumed factory defined in Chapter 2.

Since the environment set for each company and industry is different, it is necessary to organize and define the way of thinking suitable for each company and industry at each step.

Step 1	Organize internal and external requirements (management efforts, laws, etc.), operations, protection targets, etc. [3.1]
<p>Collect and organize the information necessary to make the implementation appropriate when considering the security of the factory system.</p> <ul style="list-style-type: none"> ● Step 1-1 Arrangement of requirements necessary for studying and planning security measures [3.1.1] <ul style="list-style-type: none"> (1) Arrangement of management goals, etc. (2) Arrangement of external requirements (3) Organization of internal requirements / situations ● Step 1-2 Arrangement of operations [3.1.2] ● Step 1-3 Setting the importance of business [3.1.3] ● Step 1-4 Arrangement of the protection target [3.1.4] ● Step 1-5 Setting the importance of the protection target [3.1.5] ● Step 1-6 Organize zones and connect zones with operations and protected objects [3.1.6] ● Step 1-7 Zones and the impact of security threats organized [3.1.7] <p>(Reference) Declaration of efforts by management</p> <p>It is necessary to sort out the security measures required by each company based on the environment in which each company is located and the importance of business and protection targets, which were clarified in step 1, but in order to realize the security measures, since strong leadership by the management is required, we will build the necessary system, clarify the authority necessary for its promotion, and send a message to the concerned parties.</p>	
Step 2	Planning security measures [3.2]
<p>Based on the information collected and organized in step 1, formulate a security measures policy for the factory system.</p> <ul style="list-style-type: none"> ● Step 2-1 Formulation of security measures policy ● Step 2-2 Correspondence of security measures against assumed threats 	

¹³ As for security measures, it is important to “clarify their necessity from a business perspective and implement them systematically based on unified thinking throughout the organization.”



* The level of importance is not stated because it varies depending on the environment in which each company or industry operates and it is important to assign a level of importance appropriate for each company and industry.

* The concept of importance level is also presented in international standards (IEC62443, NIST Cyber Security Framework, IoT-SSF), so it is effective to refer to this concept as well.

Figure 3-1 Steps in how to proceed with planning and introduction of security measures

3.1	Step 1	Organize internal and external requirements (management efforts, laws, etc.), operations, protection targets, etc.
------------	---------------	---

The following items will be implemented in “Organization of internal and external requirements (management efforts, laws, etc.), operations, protection targets, etc.”

3.1.1	Step 1-1 Arrangement of requirements necessary for studying and planning security measures
--------------	---

This section shows the elements necessary for studying and planning security measures.

(1) Arrangement of management goals, etc.

Organize the management goals (business expansion, business continuity, etc.) related to the security measures of the company's factory system.

In particular, whether or not a business continuity plan (BCP) has been formulated is important from the perspective of business continuity, so confirm that content. If a BCP has not been developed, implement studies of formulation of a plan together with the department in charge if necessary¹⁴.

Table 3-1 Management target items to consider when considering and planning security measures (examples of perspectives)

Management goal	Contents
Viewpoint of business growth	Enhancement and upgrading of manufacturing equipment
	Promotion of carbon neutral in factories
	Increasing the resilience of the supply chain, for example by promoting the dispersion, standardization and communalization of suppliers
Viewpoint of business continuity	Prevention of business loss due to manufacturing equipment outages and malfunctions, declining quality of the products, services outages and delays, etc.
	Prevention of a decline in trust from society due to theft or leakage of the confidential information of products, etc. or customer information
	Prevention of business outages due to the falsification or destruction of the data necessary for manufacturing
	Prevention of harm to the safety and health of employees and neighborhood residents and environmental damage such as hazardous substances emissions, etc. caused by manufacturing equipment problems or loss of control, etc.
	Prevention of harm to the safety and health of product users and environmental damage after product disposal caused by

¹⁴ Refer to the following when formulating a BCP.

• Cabinet Office, “Business Continuity Guidelines” (April 2021)

<https://www.bousai.go.jp/kyoiku/kigyoku/keizoku/pdf/guideline202104.pdf>

• Small and Medium Enterprise Agency, “Guidelines on Formulating and Implementing BCPs for Small and Medium Enterprises”

<https://www.chusho.meti.go.jp/bcp/>

	dysfunction of the factory systems or quality flaws in the products
--	---

Table 3-2 Management target items to consider when considering and planning security measures (example in an assumed factory)

Management goal	Contents	Example
Viewpoint of business growth	Flexible production line construction	Introducing AGV
	Construction of a new system for smart factories	Introduction of automated warehouse
	Improving the value of business partners and customers downstream of the supply chain	Cooperation with product delivery destinations
Viewpoint of business continuity	Prevention of business loss due to equipment outage / malfunction	Production / shipping delay prevention Prevention of manufacturing non-standard products
	Preventing safety issues	Prevention of malfunction of production facilities, automated warehouse, AGV

(2) Arrangement of external requirements

External requirements related to the security measures of the company's factory system (security law / regulation / standard / guideline compliance, requirements from the national / local government, requirements from the industry, requirements from the market / customers, requirements from business partners, requests from investors, etc.) are organized.

When arranging the external requirements, the security threats are perceived based on the standards and guidelines, etc.

Table 3-3 External requirements to be considered when considering and planning security measures (examples of perspectives)

External requirements	Contents
Business demands	Requirements from business partners
	Meeting the requirements of laws and regulations (national / local government)
	Requirements from the national government
	Requirements from the industrial world and industry
	Requirements from the market / customers
	Requirements from business partners
	Requests from investors
Standards support ¹⁵	Compliance with guidelines and standards

Table 3-4 External requirements to be considered when considering and planning security measures (example in an assumed factory)

External requirements	Contents	Example
Business demands	Transaction requirements	Requirements from product delivery destinations

¹⁵ Refer to "Annex D Related/Reference Materials" as appropriate.

	Economic security requests from the country and industry	Demand for sustainable and stable product supply
	Requirements for using other companies' services	Requirements from automated warehouse maintenance vendors
Standards support	Industry guidelines / international standards	IEC 62443 standards and others

(3) Organization of internal requirements / situations

Organize the current status of internal requirements (system, operation / management, maintenance / improvement, etc.) and systems related to the company's factory security. If the system for promoting factory security is unclear, the way of thinking will be organized at this stage, systems, rules and procedures, etc. for promoting security measures will be developed, implementation plans will be planned, and dissemination, education, etc. will be implemented.

Table 3-5 Internal requirements / grasping the situation (examples of perspectives)

Security measures	Contents
Policy and system	Security policy
	Business continuity plan (BCP)
	Security promotion system
	Security-related rules, procedures, etc.
	Security measures implementation plans, etc.
System side	Network
	Equipment, devices
	Business programs and services used
Operation / management	Security monitoring and abnormality detection
	Security management
	Information sharing
Maintenance / improvement	Security education
	Continuous risk response (confirmation, improvement and review)

Table 3-6 Internal requirements / grasping the situation (example in an assumed factory)

Security measures	Contents	Example
Policy and system	Company-wide security rules	Headquarters security guidelines
System side	Network, device/equipment configuration	Centralized management and automation of multiple production lines, introduction of AGV and automated warehouse
	Current security measures	Inter-site firewall only
Operation / management	Security monitoring	Not implemented
	Software update	Implemented only for information system department management
Maintenance / improvement	Security system maintenance	Not implemented
	Security education	Security education only on information systems (OA zone)
	Continuous risk response	Not implemented

Table 3-7 Concept of system for operating and managing factory security (examples)

Implemented by the planning / construction / management organization of the factory system (production engineering / management department, work department, etc.)	<p>In the organization that is mainly responsible for planning and building the factory system, maintenance and improvement related to security are also carried out.</p> <ul style="list-style-type: none"> • Advantages: It is possible to consider productivity improvement, etc. and study according to the current state of the factory system • Disadvantages: It is necessary to develop human resources related to security and accumulate know-how.
Implemented in IT related departments	<p>It is a form implemented by the department that implements risk management in IT systems.</p> <ul style="list-style-type: none"> • Advantages: Leverage IT department security experts. • Disadvantages: It is difficult to analyze including the impact on business because there is no knowledge of the factory system. It is difficult to plan a measures policy suitable for the factory system due to the focus on measures equal to OA. Cooperation with the site is indispensable.
Implemented by the risk management department of the entire company (risk management department, general affairs department, etc.)	<p>It is a form implemented by the department that controls risk management of a company.</p> <ul style="list-style-type: none"> • Advantages: Can be implemented as part of comprehensive risk management across the organization. Easy to implement measures across organizations. • Disadvantages: It is difficult to analyze including the impact on business because there is no knowledge of the factory system. There is a possibility of planning measures assuming that support from a public organization or investigative authority equal to a fire or intrusion will be obtained and there is a possibility that the planning of a measures policy suitable for the factory system will not be carried out appropriately under this assumption. Cooperation with the site is indispensable.
Implemented by the security control organization	<p>Under the CISO (Chief Information Security Officer), an organization (SIRT: Security Incident Response Team) that supervises security issues is set up and implemented.</p> <ul style="list-style-type: none"> • Advantages: Judgment can be made from a professional security perspective. Company-wide maintenance and improvement is possible from the perspective of security. • Disadvantages: It tends to be centered on concurrent staff, and it may be difficult to secure specialists.

3.1.2 Step 1-2 Arrangement of operations

Find out how the factory system is used in daily work.

Table 3-8 Business (example in an assumed factory)

	Business	Practitioner	Business content
1	Production planning setting	Production engineering / management department	<ul style="list-style-type: none"> Input monthly, weekly, and daily production plans from the OA terminal to the MES server.
2	Production (+ inspection)	Work department	<ul style="list-style-type: none"> Triggered by instructions from the MES server to the production line, such as the production model and production volume, setup changes are carried out at the site, and the equipment on the production line acquires recipes from the MES server and starts production. While producing using the production facilities, traceability data such as workpiece and component IDs and quality inspection information are stored in the MES server.
3	Production status monitoring (on-site)	Work department	<ul style="list-style-type: none"> SCADA and Andon in the field acquire the production status posted on the MES server and display it on the screen.
4	Replenishing materials (to the site)	Work department	<ul style="list-style-type: none"> Collect the parts inventory at the site, and if the parts are almost out of stock, transport the parts stored in the automated warehouse to the production site by AGV.
5	Purchase parts (to warehouse)	Materials department	<ul style="list-style-type: none"> After grasping the amount of parts stored in the automated warehouse and comparing it with the production plan, if the parts are almost out of stock, place an order for the parts.
6	Productivity analysis	Production engineering / management department	<ul style="list-style-type: none"> From the OA terminal, acquire production performance information such as past production volume and production defects stored in the MES server, and perform data analysis to identify areas requiring improvement.
7	Refer to traceability data	Quality control department	<ul style="list-style-type: none"> Acquire material information and quality inspection information corresponding to the production ID from the OA terminal to the MES server.
8	Maintenance	Production engineering / management department, equipment vendor	<ul style="list-style-type: none"> Physically connect maintenance terminals on the production line, adjust parameters on the production line, upgrade equipment programs, set parameters, etc. (Physical parts replacement is also performed).
9	Remote maintenance	Production engineering / management department, Equipment vendor	<ul style="list-style-type: none"> Connect to an automated warehouse, etc. via the Internet and acquire the degree of deterioration of equipment (parts, etc.). Adjust parameters as necessary.

3.1.3 Step 1-3 Setting the importance of business

Determine the importance of each kind of work for the work that uses the identified factory system. The importance of business is a factor in determining the importance / priority of security measures.

However, since the environment set for each company or industry is different, it is necessary to define the importance of work suitable for each company or industry.

[Reference] Importance of business (example in assumed factory)

Table 3-9 Importance of business (example in assumed factory)

Business importance level	Contents
Large	<ul style="list-style-type: none"> It is a business that is directly linked to stable production of products, and if this business cannot be carried out, production will be hindered on the same day. Large-scale quality deterioration occurs in an unacceptable range.
Medium	<ul style="list-style-type: none"> If this work cannot be carried out because it is indirectly related to stable production of products, production will be hindered within 2 to 3 days. Unacceptable quality deterioration occurs on a small scale.
Small	<ul style="list-style-type: none"> It is a business that is not related to stable production of products, and even if this business cannot be carried out, there is a low risk that production will be hindered. The quality of the product deteriorates to a level that does not cause any problems.

After defining the importance of a business, add the item of “importance” to the table organized in Table 3-8 and organize the relationship between business and importance.

The environment in which the individual company / industry is located varies, so illustrative examples of importance are not described in Table 3-10 below and Table 3-9. Regarding this as well, it is important that the importance be assigned appropriately for each individual company / industry and for each business.

Table 3-10 Operations and importance (example in an assumed factory)

	Business	Practitioner	Business content	Importance
1	Production planning setting	Production engineering / management department	<ul style="list-style-type: none"> Input monthly, weekly, and daily production plans from the OA terminal to the MES server. 	
..	<ul style="list-style-type: none"> ... 	

3.1.4 Step 1-4 Arrangement of the protection target

For operations for which security measures should be strengthened, identify the components (network, equipment / devices (functions / programs) / data) of the factory system that supports / implements the operations, and organize the schematic diagram of the system configuration diagram¹⁶.

In factories, components frequently change, such as changes to the production line, etc., so even in the measures implementation and operation stage in step 2 and step 3, it is required to organize and ascertain the individual components and consider the response continuously and efficiently while utilizing the automation tools, etc. if necessary.

Table 3-11 Main components (example in an assumed factory)

	Type	Component	Overview
1	Network devices and networks	VPN equipment and firewall	Equipment used by equipment vendors for remote access to achieve secure communication. Built-in firewall (access control) function to prevent access from other than the equipment vendor's maintenance center
2		Wireless LAN-AP	Network equipment for communication with AGVs
3		Equipment network	Network to which production facilities are connected
4		Production control network	Network to which servers that perform production control are connected
5		Information network	Network to which terminals for OA business and product design are connected
6	Equipment / devices	MES server	A server that manages production plans, data on production results, and gives production instructions to production lines.
7		Production line	Equipment used to produce products
8		Maintenance terminal (always disconnected)	PC used for maintenance of production facilities
9		SCADA	PC that monitors the production status of the production line
10		AGV control PC	A PC that formulates an operation plan for an AGV and controls the AGV.
11		AGV	Device to carry parts
12		Automatic warehouse	Equipment for storing and loading and unloading parts
13		Server for automated warehouse remote maintenance	Server used by equipment vendor maintenance center to remotely maintain automated warehouse
14		OA server	A server used for office purposes. Assuming sales management tools, in-house workflow systems, file servers, etc.
15		OA terminal	PC used for office use

¹⁶ It is best to organize the model numbers of the constituent devices, the vendors, the vulnerability identification information, etc. at the same time. Refer to the following.

• Information-technology Promotion Agency, Japan (IPA), Industrial Cyber Security Center of Excellence, 3rd Core Human Resource Development Program, Asset Management Project "Asset Management Guidelines in Control Systems" (June 2020)

16	Data	Production plan	Monthly / weekly / daily production plan
17		Production instructions (production model / quantity)	Instructions on what to produce on the production line. Information such as production model, production volume, corresponding recipe, etc.
18		Production recipe	Detailed information (parameters, etc.) for each production model
19		Production results (traceability data)	Past production results. Includes production status such as current production volume for production plan, ID of workpieces and parts, traceability data such as quality inspection information, etc.
20		Equipment status	Status information of production facilities (equipment). Includes cumulative usage time of jigs, last maintenance date and time, etc.
21		Equipment program / parameters / drawings	Programs set in production facilities (equipment), parameters for customizing operations, etc.
22		Parts inventory (on-site)	Model number and remaining amount of parts replenished at the production site and equipment, etc.
23		Parts inventory (warehouse)	Remaining amount of parts stored in automated warehouse, model number, shelf information, etc.

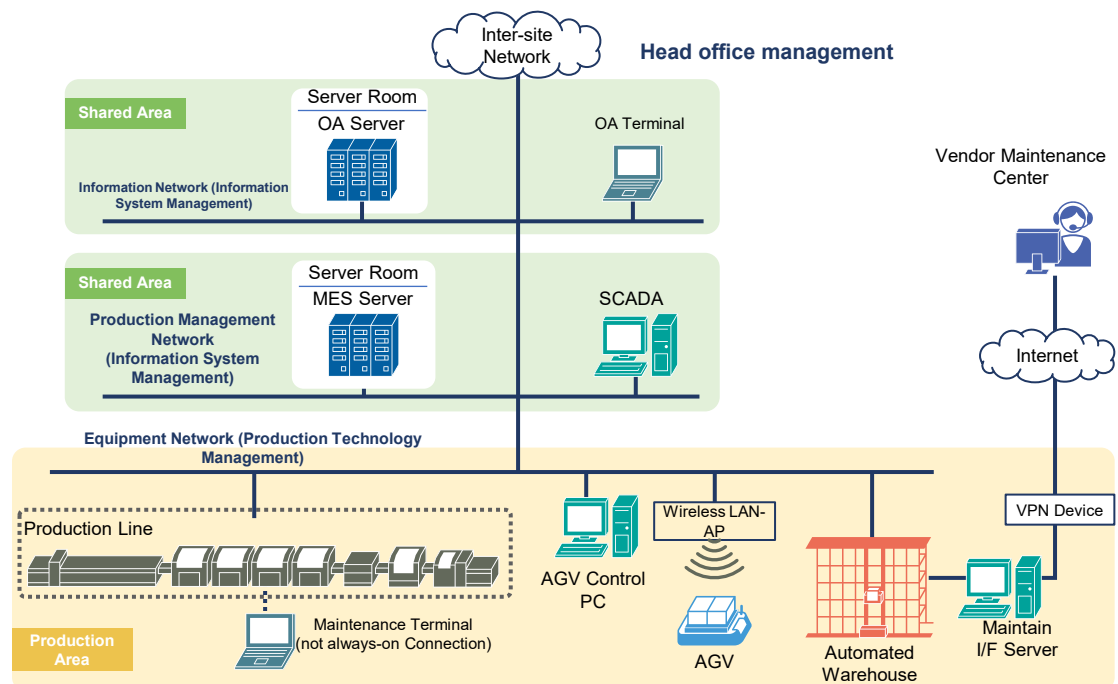


Figure 3-2 Factory system example in Chapter 2 (repost)

3.1.5 Step 1-5 Setting the importance of the protection target

From the perspective of business expansion / continuation (BC), which is the value axis that the manufacturing industry / factory emphasizes, from the perspective of safety assurance (S), quality assurance (Q), on-time delivery / delay prevention (D), and cost reduction (C), and from the perspective of the importance of the work, the importance of each of the identified protection targets will be clarified. The importance of the protected object is a factor in determining the priority of security measures. As for the concept of importance, it is effective to refer to this concept because the concept is also shown in international standards as described in Annex C.

Add the item of “importance” to the table organized in Table 3-11 and organize the relationship between protection targets and importance.

The environment in which the individual company / industry is located varies, so illustrative examples of importance are not described in Table 3-12 below. Regarding this as well, it is important that the importance be assigned appropriately for each individual company / industry.

Table 3-12 Targets to be protected and importance (example in an assumed factory)

	Type	Component	Overview	Importance
1	Network	Equipment network	Network to which production facilities are connected	
••	•••	•••	•••	

3.1.6 Step 1-6 Organize zones and connect zones with operations and protected objects

The factory system sets a zone as an area in which security measures at an equal level are required while considering the business content and business importance. Also, for each zone, connect the operations and protection targets that have been organized so far. By setting the zones, it becomes possible to see a bird's eye view of the equipment and systems of the factory as large category concepts, and when protection targets inside a certain zone receive cyberattacks, it will be possible to consider deterring the impact on different zones and minimizing the damage.

Furthermore, depending on the environment in which the individual company / industry is located, it is possible that the amount will be enormous if it is attempted to strictly define the protection targets and operations. This has the disadvantages of an enormous amount of work for organizing, possible mistakes, and taking too much time, so it is organized according to the environment of the individual company / industry. We would like you to flexibly deal with the zones to be protected, the objects to be protected, the granularity of work, and the method of organizing¹⁷.

In the subsequent steps, please take the same measures as necessary.

Table 3-13 Zone overview (example in an assumed factory)

	Name	Overview	Related business	Related protection targets
1	Control zone (production site)	<ul style="list-style-type: none"> A production line for producing products. Zone consisting of control devices and equipment. 	<ul style="list-style-type: none"> Production (+ inspection) Production status monitoring (site) Replenishing materials (to the site) Maintenance 	<ul style="list-style-type: none"> Production line Maintenance terminal Router Parts inventory (on-site)
2	Automatic transport zone	<ul style="list-style-type: none"> A zone for operating AGVs that transport parts and finished products. 	<ul style="list-style-type: none"> Replenishing materials (to the site) 	<ul style="list-style-type: none"> AGV control PC Wireless LAN-AP AGV
3	Automated warehouse zone	<ul style="list-style-type: none"> A zone that operates equipment that automatically enters and exits while storing parts. 	<ul style="list-style-type: none"> Replenishing materials (to the site) Replenishing materials (to warehouse) 	<ul style="list-style-type: none"> Automated warehouse remote maintenance server Automatic warehouse Parts inventory (on-site) Parts inventory (warehouse)

¹⁷ Operational separation is more important than physical separation when setting zones. For example, in the case of wireless LANS in different buildings engaged in the same operations, if the operation and management are separated it is acceptable to separate the zones, but if they are the same it is acceptable to not separate them. In the case that a network is physically separated, there is a tradeoff with the operating cost, but it is thought that separating the zones reduces risk.

4	Production control zone	<ul style="list-style-type: none"> • A zone consisting of servers that manage production plans, traceability data, etc. 	<ul style="list-style-type: none"> • Production planning setting • Production (+ inspection) • Production status monitoring (site) • Productivity analysis • Refer to traceability data 	<ul style="list-style-type: none"> • MES server • Production instructions • Production recipe • Production results
5	Production status monitoring zone	<ul style="list-style-type: none"> • A zone consisting of equipment that acquires and visualizes production status and equipment information. 	<ul style="list-style-type: none"> • Production status monitoring (site) • Productivity analysis • Refer to traceability data 	<ul style="list-style-type: none"> • SCADA • Production results • Equipment status • Equipment programs, parameters, drawings
6	OA zone	<ul style="list-style-type: none"> • Zones where operations not directly related to production are performed. 	<ul style="list-style-type: none"> • Production planning setting • Replenishing materials (to warehouse) • Productivity analysis 	<ul style="list-style-type: none"> • OA server • OA terminal • Production plan • Production instructions
7	Remote maintenance zone	<ul style="list-style-type: none"> • A zone for equipment vendor maintenance center to remotely monitor automated warehouses. 	<ul style="list-style-type: none"> • Remote maintenance 	<ul style="list-style-type: none"> • Maintenance center • VPN equipment and firewall

* The remote maintenance zone is assumed to be the management area of the equipment vendor under the management responsibility of the production engineering / management department.

3.1.7 Step 1-7 Zones and the impact of security threats organized

Examples of threat types which have an impact on the operation of factory systems include:

- Theft of equipment, destruction and unauthorized operation of systems and equipment
- Abnormal control or shutdown of equipment
- Data theft / leakage
- Data falsification / destruction
- Reduced availability
- Used as a steppingstone for external attacks
- System / equipment failure / fault
- Employee or maintenance staff (equipment vendor) negligence
- Facilities and work environment threats
- Natural environment threat

In addition, the threat and the impact on production and business are considered to have the following relationships.

Table 3-14 General threats and production impact (examples)

	Threat type	Threat content	Impact on production and business
1	Theft of equipment, destruction and unauthorized operation of systems and equipment	Direct destruction, theft or unauthorized operation of systems or equipment due to physical intrusion	<ul style="list-style-type: none"> • Delayed delivery and increased costs due to reduced productivity • Damage due to equipment failure or theft • Destruction of systems / equipment (production suspension, etc.)
2		Destruction or unauthorized operation of systems or equipment due to direct unauthorized connection	
3		Destruction or unauthorized operation of systems or equipment using intrusion via a network ^(*) , or internal unauthorized communication (backdoor and connect back communication)	
4	Abnormal control or shutdown of equipment	Unauthorized control or shutdown of equipment	<ul style="list-style-type: none"> • Poor quality and associated brand damage • Delayed delivery and increased costs due to reduced productivity • Occurrence of personal injury or disaster due to equipment failure • Damage due to equipment failure
5		Shutdowns by applying an abnormal load to the equipment	
6		Equipment safety control outage	
7	Data theft / leakage	Unauthorized copy to USB, etc.	<ul style="list-style-type: none"> • Leakage of production information and know-how of quality assurance • Leakage of customer information and damage to related brands
8		Upload to malicious server	
9		Eavesdropping on packets (eavesdropping on communication data)	

10	Data falsification / destruction	Falsification / deletion of data or programs	<ul style="list-style-type: none"> Poor quality and associated brand damage Delayed delivery and increased costs due to reduced productivity Occurrence of personal injury or disaster due to equipment failure Damage due to equipment failure
11		Malicious changes to equipment settings	
12		Packet tampering (communication data tampering)	
13	Reduced availability	Network outage	<ul style="list-style-type: none"> Delayed delivery and increased costs due to reduced productivity Occurrence of personal injury or disaster due to loss of control of equipment Poor quality and associated brand damage
14		Network outage / capacity over	
15		Stopping equipment, servers, and PCs	
16		Lack of resources	
17	Used as a steppingstone for external attacks	Attacks on external servers / networks	<ul style="list-style-type: none"> Brand damage Delayed delivery due to line outage under investigation
18	System / equipment failure / fault	Power outage / momentary interruption / voltage fluctuation, failure / fault of power supply device / equipment	<ul style="list-style-type: none"> Delayed delivery and increased costs due to reduced productivity Occurrence of personal injury or disaster due to loss of control of equipment Damage due to equipment failure Poor quality and associated brand damage
19		Abnormalities such as temperature, humidity, static electricity, and air cleanliness due to air conditioning failure / fault	
20		Communication equipment failure / fault	
21		Equipment / server / PC failure / fault	
22	Employee or maintenance staff (equipment vendor) negligence	Abnormal (malware-infected) device connection	<ul style="list-style-type: none"> Leakage of production information and know-how of quality assurance Leakage of customer information and damage to related brands Destruction of systems / equipment (production suspension, etc.)
23		Setting / operation error	<ul style="list-style-type: none"> Poor quality and associated brand damage Occurrence of personal injury or disaster due to equipment failure Damage due to equipment failure
24	Facilities and work environment threats	Fire or spread of fire from nearby areas due to a short circuit, careless handling of fire, etc.	Delayed delivery and increased costs due to reduced productivity

25		Collapse of loaded materials, etc.	<ul style="list-style-type: none"> • Occurrence of personal injury or disaster due to loss of control of equipment • Damage due to equipment failure • Poor quality and associated brand damage
26		Explosion caused by chemicals, etc.	
27		Damage to electronic equipment caused by electromagnetic waves	
28	Natural environment threat	Leakage due to heavy rain, flood, etc.	<ul style="list-style-type: none"> • Damage caused by business / production suspension • Delayed delivery and increased costs due to reduced productivity • Occurrence of personal injury or disaster due to loss of control of equipment • Damage due to equipment failure • Poor quality and associated brand damage
29		Invasion of pests	
30		Equipment tips over or falls due to an earthquake, etc.	
31		Power outages, momentary interruptions, voltage fluctuations due to lightning strikes, floods, earthquakes, etc.	
32		Destruction of devices / equipment, etc. by fire	

(*) Unauthorized intrusion via a network is not necessarily by an attacker; there is also a possibility that it is an organization such as a maintenance company, etc. which has received an attack.

After perceiving the above kinds of latest threats concerning cybersecurity pertaining to the company's factory systems¹⁸, we will consider these threats and the impact on production and business and sort out what kind of security threats are expected for each zone and what kind of impact they will have¹⁹.

¹⁸ Refer to "[Reference] Attacker's motive" stated in this guideline.

¹⁹ There are cases in which carrying out the application of patches, etc. as measures against a security threat leads to a different threat, namely the failure of systems or equipment. When implementing security measures, it is necessary to ascertain the impact of the measures and consider the scope, schedule, etc. of the measures to minimize the impact on business and production even in the case that a failure occurs.

Table 3-15 Relationship between protected objects and related operations, threats, and impacts (examples)

	Related protection targets	Related business	Threat	Impact	Name
1	• Production line	<ul style="list-style-type: none"> • Production (+ inspection) • Production status monitoring (on-site) • Replenishing materials (to the site) 	<ul style="list-style-type: none"> • Theft of equipment, destruction and unauthorized operation of systems and equipment • Abnormal control or shutdown of equipment • Data theft / leakage • Data falsification / destruction • Reduced availability • System / equipment failure / fault • Employee or maintenance staff (equipment vendor) negligence • Facilities and work environment threats • Natural environment threat 	<ul style="list-style-type: none"> • Non-Production (+ inspection) • Non-Production status monitoring (on-site) • Non-Replenishing materials (to the site) 	Control zone (production site)
	• Maintenance terminal	• Maintenance	<ul style="list-style-type: none"> • Theft of equipment, destruction and unauthorized operation of systems and equipment • Abnormal control or shutdown of equipment • Data theft / leakage • Data falsification / destruction • Reduced availability • System / equipment failure / fault • Employee or maintenance staff (equipment vendor) negligence • Facilities and work environment threats • Natural environment threat 	• Non-Maintenance	
	• Router	<ul style="list-style-type: none"> • Production (+ inspection) • Production status monitoring (on-site) • Replenishing materials (to the site) 	<ul style="list-style-type: none"> • Theft of equipment, destruction and unauthorized operation of systems and equipment • Abnormal control or shutdown of equipment • Data theft / leakage • Data falsification / destruction • Reduced availability • System / equipment failure / fault • Employee or maintenance staff (equipment vendor) negligence • Facilities and work environment threats • Natural environment threat 	<ul style="list-style-type: none"> • Non-Production (+ inspection) • Non-Production status monitoring (on-site) • Non-Replenishing materials (to the site) 	
2	• AGV control PC	• Replenishing materials (to the site)	<ul style="list-style-type: none"> • Theft of equipment, destruction and unauthorized operation of systems and equipment • Abnormal control or shutdown of equipment • Data theft / leakage • Data falsification / destruction • Reduced availability • System / equipment failure / fault • Employee or maintenance staff (equipment vendor) negligence 	• Non-Replenishing materials (to the site)	Automatic transport zone

			<ul style="list-style-type: none"> • Facilities and work environment threats • Natural environment threat 		
	• Wireless LAN-AP	• Replenishing materials (to the site)	<ul style="list-style-type: none"> • Theft of equipment, destruction and unauthorized operation of systems and equipment • Abnormal control or shutdown of equipment • Data theft / leakage • Data falsification / destruction • Reduced availability • System / equipment failure / fault • Employee or maintenance staff (equipment vendor) negligence • Facilities and work environment threats • Natural environment threat 	• Non-Replenishing materials (to the site)	
	• AGV	• Replenishing materials (to the site)	<ul style="list-style-type: none"> • Theft of equipment, destruction and unauthorized operation of systems and equipment • Abnormal control or shutdown of equipment • Data theft / leakage • Data falsification / destruction • Reduced availability • System / equipment failure / fault • Employee or maintenance staff (equipment vendor) negligence • Facilities and work environment threats • Natural environment threat 	• Non-Replenishing materials (to the site)	
	3	• Automated warehouse remote maintenance server	<ul style="list-style-type: none"> • Theft of equipment, destruction and unauthorized operation of systems and equipment • Abnormal control or shutdown of equipment • Data theft / leakage • Data falsification / destruction • Reduced availability • System / equipment failure / fault • Employee or maintenance staff (equipment vendor) negligence • Facilities and work environment threats • Natural environment threat 	<ul style="list-style-type: none"> • Non-Replenishing materials (to the site) • Non-Replenishing materials (to the warehouse) 	Automated warehouse zone
		• Automatic warehouse	<ul style="list-style-type: none"> • Theft of equipment, destruction and unauthorized operation of systems and equipment • Abnormal control or shutdown of equipment • Data theft / leakage • Data falsification / destruction • Reduced availability • System / equipment failure / fault • Facilities and work environment threats • Natural environment threat 	<ul style="list-style-type: none"> • Non-Replenishing materials (to the site) • Non-Replenishing materials (to the warehouse) 	

4	• MES server	<ul style="list-style-type: none"> • Production planning setting • Production (+ inspection) • Production status monitoring (on-site) • Productivity analysis • Refer to traceability data 	<ul style="list-style-type: none"> • Theft of equipment, destruction and unauthorized operation of systems and equipment • Abnormal control or shutdown of equipment • Data theft / leakage • Data falsification / destruction • Reduced availability • System / equipment failure / fault • Employee or maintenance staff (equipment vendor) negligence • Facilities and work environment threats • Natural environment threat 	<ul style="list-style-type: none"> • Non-Production planning setting • Non-Production (+ inspection) • Non-Production status monitoring (on-site) • Non-Productivity Analysis Traceability Data Reference 	Production control zone
5	• SCADA	<ul style="list-style-type: none"> • Production status monitoring (on-site) • Productivity analysis • Refer to traceability data 	<ul style="list-style-type: none"> • Theft of equipment, destruction and unauthorized operation of systems and equipment • Abnormal control or shutdown of equipment • Data theft / leakage • Data falsification / destruction • Reduced availability • System / equipment failure / fault • Employee or maintenance staff (equipment vendor) negligence • Facilities and work environment threats • Natural environment threat 	<ul style="list-style-type: none"> • Non-Production status monitoring (on-site) • Non-Productivity Analysis Traceability Data Reference 	Production status monitoring zone
6	• OA server	<ul style="list-style-type: none"> • Production planning setting • Replenishing materials (to warehouse) • Productivity analysis 	<ul style="list-style-type: none"> • Theft of equipment, destruction and unauthorized operation of systems and equipment • Abnormal control or shutdown of equipment • Data theft / leakage • Data falsification / destruction • Reduced availability • System / equipment failure / fault • Employee or maintenance staff (equipment vendor) negligence • Facilities and work environment threats • Natural environment threat 	<ul style="list-style-type: none"> • Production planning setting • Non-Replenishing materials (to the warehouse) • Non-Productivity analysis 	OA zone
	• OA terminal	<ul style="list-style-type: none"> • Production planning setting • Replenishing materials (to warehouse) • Productivity analysis 	<ul style="list-style-type: none"> • Theft of equipment, destruction and unauthorized operation of systems and equipment • Abnormal control or shutdown of equipment • Data theft / leakage • Data falsification / destruction • Reduced availability • System / equipment failure / fault • Employee or maintenance staff (equipment vendor) negligence 	<ul style="list-style-type: none"> • Production planning setting • Non-Replenishing materials (to the warehouse) • Non-Productivity analysis 	

			<ul style="list-style-type: none"> • Facilities and work environment threats • Natural environment threat 		
7	<ul style="list-style-type: none"> • Maintenance center 	<ul style="list-style-type: none"> • Remote maintenance 	<ul style="list-style-type: none"> • Theft of equipment, destruction and unauthorized operation of systems and equipment • Abnormal control or shutdown of equipment • Data theft / leakage • Data falsification / destruction • Reduced availability • System / equipment failure / fault • Employee or maintenance staff (equipment vendor) negligence • Facilities and work environment threats • Natural environment threat 	<ul style="list-style-type: none"> • Remote Non-Maintenance 	Remote maintenance zone
	<ul style="list-style-type: none"> • VPN equipment and firewall 	<ul style="list-style-type: none"> • Remote maintenance 	<ul style="list-style-type: none"> • Theft of equipment, destruction and unauthorized operation of systems and equipment • Abnormal control or shutdown of equipment • Data theft / leakage • Data falsification / destruction • Reduced availability • System / equipment failure / fault • Employee or maintenance staff (equipment vendor) negligence • Facilities and work environment threats • Natural environment threat 	<ul style="list-style-type: none"> • Remote Non-Maintenance 	

[Reference] Attacker's motive

In recent cyberattacks, the purpose of the attack is clear, and there is a tendency for the attack to be relentlessly repeated until the purpose is achieved. The types of attackers are also diverse, including national-level organizations such as the military and intelligence agencies for the purpose of gathering information and vandalism, criminal groups for the purpose of ransom, and persons involved in internal fraud.

Therefore, it is important to anticipate the motives of the attacker in advance and to anticipate what kind of impact may occur on production in the unlikely event of a cyberattack.

When assuming a threat in a factory, if an attacker has a motive and makes a cyberattack on the factory system, it is expected that some abnormal event or influence will occur at the production site.

On the other hand, in factories, there are attacks aimed at money such as ransomware by criminal organizations, but the purpose may be unclear. The attacker did not intentionally aim at the factory, and it may have been a matter of chance that the attack destination ended up being the factory. Instead of thinking that your company will not be targeted by criminal organizations, it is necessary to also assume that it will be hit by a stray bullet.

In addition to cyberattacks, it is also necessary to assume threats to the natural environment, system / equipment failures / faults, employee negligence, and management deficiencies.

Below are some examples of possible motives for attackers.

Table 3-16 Attacker's motive (examples)

	Purpose	Explanation	Possible attacker
1	Social disruption	The products of the factory are important products, causing social turmoil by causing supply shortages and quality insecurity.	<ul style="list-style-type: none"> • National organizations (military, intelligence agencies, etc.) • Criminal organizations, terrorist organizations
2	Information theft	Steal trade secrets regarding high value-added products and advanced production processes at the factory.	<ul style="list-style-type: none"> • Rival companies • Criminal organization (for money)
3	Damage to corporate value	Improper functions are added to the products of the factory, which causes the quality of the products to deteriorate and damages the corporate value.	<ul style="list-style-type: none"> • Rival companies • Criminal organizations
4	Secondary damage	Aim for secondary damage such as inducing accidents on the production line, causing human and physical damage, causing leakage of chemicals and inducing environmental pollution, crafting products and stealing information from users, etc.	<ul style="list-style-type: none"> • National organizations (military, intelligence agencies, etc.) • Criminal organizations, terrorist organizations

			<ul style="list-style-type: none"> • Rival companies
5	Steppingstone	Using the production line as a steppingstone, intruding into the IT system of the company or interfering with services (leading to information theft, business obstruction, etc.).	<ul style="list-style-type: none"> • National organizations (military, intelligence agencies, etc.) • Criminal organizations, terrorist organizations • Rival companies
6	Money	Infected with ransomware and demanded money	<ul style="list-style-type: none"> • Criminal organizations, terrorist organizations
7	Harassment	Harassment due to grudges (internal fraud).	<ul style="list-style-type: none"> • Current / previous employees, business partners, etc.
8	Business disruption	Business disruption (aiming for reputational damage, raising the stock price of rival companies, etc.)	<ul style="list-style-type: none"> • Rival companies • Criminal organizations

[Reference] Declaration of efforts by management

Management leadership is important for implementing and promoting security measures. For this reason, it is important for management to clearly state and declare as an organization the security measures when the intention to promote security measures is not clear²⁰.

For example, it is necessary to clarify the establishment of a promotion organization, granting authority, purpose, policy, etc., and to make a declaration within the organization.

Example of a declaration of security efforts by management:²¹

As an electronic equipment manufacturer, it is important for Company X to provide a stable product supply. For this reason, it is important to ensure the security of production lines and products, and we will implement systematic measures.

- Purpose:
The purpose is to set implementation targets based on risk assessment from a security perspective, and to ensure implementation and continuous improvement.
- Policy:
Under the leadership of the business owners, establish a security promotion system, delegate the necessary authority to the responsible

²⁰ For management, the Cybersecurity Management Guidelines have been issued by the Ministry of Economy, Trade and Industry, and they state the three principles which management needs to recognize and the ten important items which management should direct their CISO, etc. The Cybersecurity Management Guidelines require the driving of security measures under the leadership of management for the building of a structure or process for cybersecurity risk management, identifying cybersecurity risks and implementing measures, and establishing a system to prepare for the occurrence of incidents.

²¹ The matters stated in the Cybersecurity Management Guidelines also serve as a useful reference on the occasion of a declaration of security efforts by management, so please refer to them.

persons, and carry out the necessary investment to achieve the purpose.

- **System:**
A promotion organization will be set up directly under the CEO to promote systematic measures strategically and from a unified perspective across the entire supply chain, including not only the company but also its business partners and contractors
- **Risk assessment:**
Comprehensively implement systematic measures from the perspectives of security, business continuity, and risk response.
- **Dissemination and education / training:**
Disseminate matters concerning security measures to employees and those involved in the supply chain and ensure compliance by carrying out the necessary education.
- **Communication:**
Relationships of trust will be built with the concerned parties by disclosing information concerning cybersecurity risks and measures in a timely manner.

3.2**Step 2****Planning security measures**

Based on the information collected and organized in step 1, formulate a security measures policy for the factory system.

When implementing step 2, depending on the environment of the individual company or industry, it is important to plan and implement necessary measures while considering the cost-effectiveness of the measures.

Step 2-1	Formulation of security measures policy [3.2.1]
Set the importance and priority of the zones organized in step 1 and the related operations, protection targets, and assumed threats according to the environment in which the industry or individual company is located.	
Step 2-2	Correspondence of security measures against assumed threats [3.2.2]
Organize what kind of security measures can be applied. In order to respond to threats, it is important to take measures against both the physical side and the system configuration side.	
<ul style="list-style-type: none"> (1) Measures for system configuration <ul style="list-style-type: none"> (i) Security measures in the network (ii) Security measures for equipment (iii) Security measures for business programs and services used (2) Physical measures <ul style="list-style-type: none"> (i) Measures related to the building (ii) Measures related to power supply / electrical equipment (iii) Measures related to the environment (air conditioning, etc.) (iv) Measures related to water supply facilities (v) Measures related to equipment (vi) Measures related to physical access control 	

3.2.1 Step 2-1 Formulation of security measures policy

Develop a policy for implementing security measures for factory systems. Set the importance and priority of the zones organized in step 1 and the related operations, protection targets, and assumed threats according to the environment in which the industry or individual company is located. As for the concept of importance, it is effective to refer to this concept because the concept is also shown in international standards as described in Annex C.

The environment in which the individual company / industry is located varies, so illustrative examples of importance and priority are not described in Table 3-17 below. Regarding this as well, it is important that the importance and priority be assigned appropriately for each individual company / industry.

Table 3-17 Protection target, related operations, threats, impacts, zones, importance / priority relationships (example in an assumed factory)

	Related protection targets	Related business	Threats	Impact	Name	Importance / priority
1	<ul style="list-style-type: none"> Production line 	<ul style="list-style-type: none"> Production (+ inspection) Production status monitoring (on-site) Replenishing materials (to the site) 	<ul style="list-style-type: none"> Theft of equipment, destruction and unauthorized operation of systems and equipment Abnormal control or shutdown of equipment Data theft / leakage Data falsification / destruction Reduced availability System / equipment failure / fault Employee or maintenance staff (equipment vendor) negligence Facilities and work environment threats Natural environment threat 	<ul style="list-style-type: none"> Non-Production (+ inspection) Non-Production status monitoring (on-site) Non-Replenishing materials (to the site) 	Control zone (production site)	

[Reference] Example of security requirement level concept

Factory system security measures need to be realistic from the perspective of investment costs and operating costs. Therefore, it is necessary to determine the importance (priority) of security measures according to the importance of the role played by the protected system.

Assuming that this importance is “security requirement level”, the higher the requirement level, the stronger the security measures required. The following are examples of security requirement levels, but it is desirable for each company to set the optimum level setting method.

$$\text{“Business importance”} \times \text{“threat level”} = \text{“security requirement level”}$$

Table 3-18 Business importance (examples)

Business importance	Definition
Large	Business stoppage (supply stoppage) due to the malfunction or stoppage of the system Loss of control of system / explosion Lost work accident
Medium	Business stoppage (supply delay) due to the malfunction or stoppage of the system Accidents without lost time Environmental pollution due to inappropriate drainage
Small	Business disruption due to the malfunction or stoppage of the system (no supply interruption) Increased defective rate and occurrence of complaints due to system problems Increased costs due to problems in production control

Table 3-19 Threat level [= possibility of being threatened] (examples)

Threat level	Definition
3	Highly likely to be threatened <ul style="list-style-type: none"> • Easy physical / logical access • Attacks and fraud can be carried out even by those who do not have high attack skills and knowledge. • Attacks and fraud can be carried out in a very short time
2	There is a moderate risk of being threatened <ul style="list-style-type: none"> • General restrictions on physical / logical access • Anyone with a certain level of attack skills and knowledge can carry out attacks and fraud. • It takes some time to carry out attacks and fraud
1	Less likely to be threatened <ul style="list-style-type: none"> • There are strong restrictions on physical / logical access • It is impossible to carry out attacks or fraud unless you have extremely high attack skills and advanced knowledge. • It takes a long time to carry out attacks and fraud

Table 3-20 Security requirement level (examples)

		Threat level		
		1	2	3
Business importance	Large	High	High	High
	Medium	Medium	Medium	High
	Small	Low	Low	Low

The “security requirement level” (= “business importance” x “threat level”) is the protection target when a possible security threat is received in each of the protection targets (system and its components) related to the business. From the perspective of importance / priority, it represents

- What kind of influence (and the degree of influence) may be affected, and
- The magnitude of the possibility that the effect will occur

This means that it represents the “security risk” of each protected object.

Table 3-21 Business importance, threat level, security requirement level (examples)

Zone	Related business	Business importance	Threat level	Security requirement level
Control / production line	Production, inspection	Large	2	High
Control / maintenance terminal	Production program creation	Large	1	High
Automatic transfer	Parts / parts replenishment	Large	2	High
Automatic warehouse	Parts / parts replenishment	Large	2	High
Production control	Production planning setting, production instructions	Large	2	High
Production status monitoring	Production status monitoring	Large	1	High
Remote maintenance	Remote maintenance	Large	1	High
OA	Productivity analysis	Medium	2	Medium

It is necessary to implement strong security measures (see Table 3-26, Table 3-27) according to the security requirement level for the protection targets (networks, equipment, devices, etc.) in each zone.

[Reference] Extent of measures

Since each zone has its own extent of response, such as how far to take countermeasures, examples of this concept of extent and the content of countermeasures are shown.

Table 3-22 Examples of security measures according to the security requirement level of each zone (excerpts of only major measures)

	Classification	Requirements	Low	Middle	High
1	Intrusion prevention	Prevention of intrusion from external networks	<ul style="list-style-type: none"> For communication from other zones and communication to other zones, pass only the communication permitted in advance (controlled by IP address, access port, etc.) 	<ul style="list-style-type: none"> For communication from other zones and communication to other zones, pass only the communication permitted in advance (controlled by IP address, access port, etc.) Authenticate the zone user 	<ul style="list-style-type: none"> For communication from other zones and communication to other zones, pass only the communication permitted in advance (controlled by IP address, access port, etc.) Authentication of the zone user is strictly performed by introducing multi-factor authentication.
2		Preventing direct intrusion into the inside of the zone	<ul style="list-style-type: none"> Restrict access to the zone Manage devices connected to the LAN in the zone 	<ul style="list-style-type: none"> Install equipment in the area where entry / exit control is performed 	<ul style="list-style-type: none"> Install equipment in the area where entry / exit control is performed Strictly limit the number of people entering the zone

				<ul style="list-style-type: none"> • Restrict access to the zone • Manage devices connected to the LAN in the zone 	<ul style="list-style-type: none"> • Devices connected to the LAN in the zone are restricted by device authentication.
3		Passing only permitted communication	<ul style="list-style-type: none"> • For communication from other zones and communication to other zones, pass only the communication permitted in advance (controlled by IP address, access port, etc.) 	<ul style="list-style-type: none"> • For communication from other zones and communication to other zones, pass only the communication permitted in advance (controlled by IP address, access port, etc.) • Authenticate the zone user 	<ul style="list-style-type: none"> • For communication from other zones and communication to other zones, pass only the communication permitted in advance (controlled by IP address, access port, etc.) • Authentication of the zone user is strictly performed by introducing multi-factor authentication.
4	Activity deterrence	Deterrence of fraud	<ul style="list-style-type: none"> • Authenticate the logon of the operating user and limit the operation by access control • Inform those engaged in business to monitor operations and prevent fraudulent activities. • Attach a terminal cap to unnecessary ports 	<p>In addition to low-level measures</p> <ul style="list-style-type: none"> • Log on to the server console only for administrators • Authentication of the zone user is strictly performed by introducing multi-factor authentication. • Important operations are not performed by one administrator, but are approved or separated by workflow. • Monitor unauthorized communication packets with IDS • Soft block unnecessary ports 	<p>In addition to medium level measures</p> <ul style="list-style-type: none"> • Monitor the appearance of non-stationary packets by permit list type monitoring for packets flowing through the network. • Execution control tool prevents startup of programs other than those permitted in advance • Hard block unnecessary ports
5		Log management	<ul style="list-style-type: none"> • Collecting and managing logs of monitoring terminals 	<p>In addition to low-level measures</p> <ul style="list-style-type: none"> • Collect and manage a wide variety of logs such as equipment alerts and firewalls 	<p>In addition to medium level measures</p> <ul style="list-style-type: none"> • Perform regular analysis of collected logs
6	Operation support	Alert monitoring	<ul style="list-style-type: none"> • Centrally monitor the log of the monitoring terminal with SOC and detect an abnormality. 	<p>In addition to low-level measures</p> <ul style="list-style-type: none"> • Centrally monitor logs of various servers and security devices (pointing to firewalls, 	<p>In addition to medium level measures</p> <ul style="list-style-type: none"> • Equipment alerts are centrally monitored by SOC and abnormalities are detected. • Visualize the network inside the

				IDS/IPS, etc.) with SOC and detect anomalities.	factory and detect anomalities
--	--	--	--	--	-----------------------------------

The following shows the state in which countermeasures have been taken for the example of the factory system shown in Chapter 2. The implemented measures are as follows.

- Passing only permitted communication by installing a firewall (FW) between each of the OA zone, production control zone, production status monitoring zone, control zone, automatic transport zone, and the automated warehouse zone and the other zones
- Restricted entry to the OA zone and production control zone and user authentication

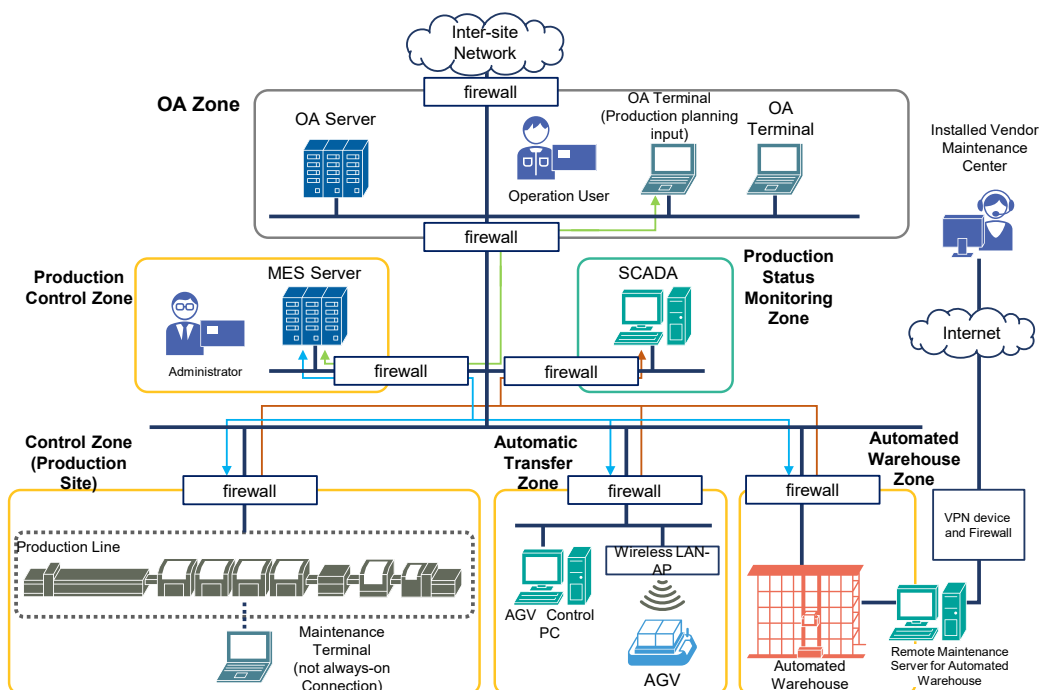


Figure 3-3 Measures for requirements in each zone (examples)

3.2.2 Step 2-2 Correspondence of security measures against assumed threats

With reference to the overall picture of threats and security measures shown in Table 3-24, connect the zones, protection targets, operations, threats, impacts and countermeasures organized so far.

Regarding the individual security measures, the measures are exemplified in the following (1) Measures for system configuration and (2) Physical measures, so while referring to these as appropriate, and depending on the environment of the individual company or industry, it is important to plan and implement necessary measures while considering the cost-effectiveness of the measures.

Table 3-23 Protected objects, related operations, threats, impacts, zones, importance / priority, countermeasures (example in an assumed factory: excerpt from production line only)

	Related protection targets	Related business	Threat	Impact	Name	Importance / Priority	Measures
1	Production line	<ul style="list-style-type: none"> • Production (+ inspection) • Production status monitoring (on-site) • Replenishing materials (to the site) 	<ul style="list-style-type: none"> • Theft of equipment, destruction and unauthorized operation of systems and equipment 	<ul style="list-style-type: none"> • Non-Production (+ inspection) • Non-Production status monitoring (on-site) • Non-Replenishing materials (to the site) 	Control zone (production site)		(2) (v) Measures related to equipment (2) (vi) Measures related to physical access control
			<ul style="list-style-type: none"> • Abnormal control or shutdown of equipment 				(1) (i) Measures in the network (1) (ii) Measures for equipment
			<ul style="list-style-type: none"> • Data theft / leakage 				(1) (i) Measures in the network (1) (ii) Measures for equipment
			<ul style="list-style-type: none"> • Data falsification / destruction 				(1) (i) Measures in the network (1) (ii) Measures for equipment
							(2) (v) Measures related to equipment
							(1) (i) Measures in the network (1) (ii) Measures for equipment

			• Abnormal control or shutdown of equipment				(1) (i) Measures in the network (1) (ii) Measures for equipment
			• Reduced availability				(1) (i) Measures in the network (1) (ii) Measures for equipment
			• System / equipment failure / fault				(2) (ii) Measures related to power supply / electrical equipment
							(1) (ii) Measures for equipment
			• Employee or maintenance staff (equipment vendor) negligence				(2) (v) Measures related to equipment
							(1) (ii) Measures for equipment
			• Facilities and work environment threats				(2) (i) Measures related to the building (2) (v) Measures related to equipment
• Natural environment threat		(2) (i) Measures related to the building (2) (ii) Measures related to power supply / electrical equipment (2) (v) Measures related to equipment					
		(1) (ii) Measures for equipment					

Table 3-24 Overview of security measures (examples) that respond to assumed threats

	Threat type	Threat content	Countermeasure type	Countermeasures
1	Theft of equipment, destruction and unauthorized operation of systems and equipment	Physical intrusion	(2) Physical measures	(2) (vi) Measures related to physical access control
2		Direct unauthorized connection/access to equipment	(2) Physical measures	(2) (v) Measures related to equipment
			(1) Measures for system configuration	(1) (i) Measures in the network (1) (ii) Measures for equipment
3		Unauthorized access via a network or using unauthorized communication internally	(1) Measures for system configuration	(1) (i) Measures in the network
4	Abnormal control or destruction of equipment	Unauthorized control or shutdown of equipment	(1) Measures for system configuration	(1) (i) Measures in the network
5		Shutdowns by applying an abnormal load to the equipment		(1) (ii) Measures for equipment
6		Equipment safety control outage		
7	Data theft / leakage	Unauthorized copy to USB, etc.	(2) Physical measures	(2) (v) Measures related to equipment
			(1) Measures for system configuration	(1) (ii) Measures for equipment
8		Unauthorized upload to server	(1) Measures for system configuration	(1) (i) Measures in the network (1) (ii) Measures for equipment
9		Eavesdropping on packets (eavesdropping on communication data)	(1) Measures for system configuration	(1) (i) Measures in the network (1) (ii) Measures for equipment
10	Data falsification / destruction	Falsification / deletion of data or programs	(1) Measures for system configuration	(1) (ii) Measures for equipment
11		Malicious changes to / deletion of equipment settings		
12		Packet tampering (communication data tampering)	(1) Measures for system configuration	(1) (i) Measures in the network (1) (ii) Measures for equipment
13		Network outage		

14	Reduced availability	Network outage / capacity over	(1) Measures for system configuration	(1) (i) Measures in the network
15		Stopping equipment, servers, and PCs		(1) (ii) Measures for equipment
16		Lack of resources		
17	Used as a steppingstone for external attacks	Attacks on external servers / networks	(1) Measures for system configuration	(1) (i) Measures in the network (1) (ii) Measures for equipment
18	System / equipment failure / fault	Power outage / momentary interruption / voltage fluctuation, failure / fault of power supply device / equipment	(2) Physical measures (1) Measures for system configuration	(2) (ii) Measures related to power supply / electrical equipment (1) (ii) Measures for equipment
19		Abnormalities such as temperature, humidity, static electricity, and air cleanliness due to air conditioning failure / fault	(1) Measures for system configuration	(1) (ii) Measures for equipment
20		Communication equipment failure / fault		
21		Equipment / server / PC failure / fault		
22	Employee or maintenance staff (equipment vendor) negligence	Abnormal (malware-infected) device connection	(2) Physical measures (1) Measures for system configuration	(2) (v) Measures related to equipment (1) (ii) Measures for equipment
23		Setting / operation error	(1) Measures for system configuration	(1) (ii) Measures for equipment
24	Facilities and work environment threats	Fire or spread of fire from nearby areas due to a short circuit, careless handling of fire, etc.	(2) Physical measures	(2) (i) Measures related to the building
25		Collapse of loaded materials, etc.		(2) (v) Measures related to equipment
26		Explosion caused by chemicals, etc.		
27		Damage to electronic equipment caused by electromagnetic waves		
28	Natural environment threat	Inundation / leakage due to heavy rain, flood, etc.	(2) Physical measures	(2) (i) Measures related to the building

29		Invasion of pests		(2) (v) Measures related to equipment
30		Equipment tips over or falls due to an earthquake, etc.		
31		Power outages, momentary interruptions, voltage fluctuations due to lightning strikes, floods, earthquakes, etc.	(2) Physical measures	(2) (ii) Measures related to power supply / electrical equipment
			(1) Measures for system configuration	(1) (ii) Measures for equipment
32		Destruction of devices / equipment, etc. by fire	(2) Physical measures	(2) (i) Measures related to the building
				(2) (v) Measures related to equipment

The specific security measures that can be assumed are shown below. In order to respond to threats, it is important to take measures against both the system configuration side and the physical side, not just one of them, so please refer to the specific measures.

After planning the measures against the system configuration side and the physical side, in order to keep the remaining risks concerning cybersecurity within an acceptable range, taking risk management measures such as formulating a measures policy (examples: taking out cyber insurance as a risk transfer, consideration of a security risk response in the business continuity plan (BCP),²² etc.), among others, can be considered.

In SMEs, there are cases where the information-related area and the factory-related area are not separated. I would like you to take measures according to the situation while referring to the security information for SMEs²³ as appropriate.

Furthermore, it is necessary to note that life cycle measures (operational and management measures and measures for maintenance and improvement) are also important in order to improve the effect of the measures against the system configuration side and the physical side.

- (1) Measures for system configuration
 - (i) Security measures in the network
 - (ii) Security measures for equipment
 - (iii) Security measures for business programs and services used
- (2) Physical measures
 - (i) Measures related to the building
 - (ii) Measures related to power supply / electrical equipment
 - (iii) Measures related to the environment (air conditioning, etc.)
 - (iv) Measures related to water supply facilities
 - (v) Physical measures related to equipment
 - (vi) Measures related to physical access control

²² For example, formulation of the initial response and restoration procedures, arrangement of alternative methods, risk communication with interested parties, and carrying out training and exercises to ensure its effectiveness can be considered. (Regarding training assuming cyberattacks, also refer to step 3 (1) Life cycle measures (ii) Measures for maintenance and improvement)

²³ For example, the Information-technology Promotion Agency, Japan (IPA) has published "Guidelines for Information Security Measures for Small and Medium-sized Enterprises". In addition, the Ministry of Economy, Trade and Industry and the Information-technology Promotion Agency, Japan (IPA), in collaboration with local industry groups (chambers of commerce, etc.) and companies, etc., carry out "cyber security Otasuketai (support team) services" by registered private businesses.

(1) Measures for system configuration

For threats such as unauthorized intrusion and data leakage via the network, it is necessary to take measures mainly in terms of system configuration in the network. In addition, it is necessary to take measures mainly on the system side for threats such as unauthorized connection / access on the device, data falsification, and abnormal setting / control of the device.

System security measures consider the following three perspectives.

- **Intrusion prevention:**
Prevention of unauthorized intrusion into factory systems.
- **Activity deterrence:**
Even if the intrusion cannot be prevented and the intrusion is successful, the attack activity is deterred
- **Operation support:**
Supporting operations to detect and deal with activities such as intrusions and attacks into factory systems at an early stage.

Table 3-25 Overview of the purpose of security measures in the system configuration

	Purpose		Overview
1	Intrusion prevention	Preventing intrusion into the network	Prevents intrusion from external networks, unauthorized device connections to internal networks, etc.
2		Prevention of intrusion into equipment / devices	Prevents intrusion through external media and networks, and intrusion by unauthorized persons
3	Activity deterrence	Unnecessary communication interruption in the network	Deters communication outside the design specifications
4		Deterring illegal program execution and illegal file operations on equipment / devices	Deters execution, writing to files, and references other than the specified program
5		Deterrence of unauthorized use of equipment / devices	Deterring the use of equipment / devices other than the specified users (including equipment / device functions / programs / data / interfaces)
6	Operation support	Identification / visualization	Identify protection targets, manage configurations, and visualize status
7		Abnormality detection	Report an alert when an unauthorized intrusion or activity is detected
8		Analysis	Logs are recorded, collected, and analyzed for cause analysis in the event of a failure.
9		Recovery	Recovery from business failure status due to malware infection to normal status

These measures will be implemented for the “network”, “equipment / devices such as equipment and computers”, and “business programs / services used” that make up the factory system.

The contents of each measure are explained below.

(i) Security measures in terms of system configuration in the network

Factory systems are often configured to link with peripheral functions via a network in order to control the entire system in an integrated manner, centering

on control devices and equipment, so it is necessary to take into consideration this characteristic in security measures.

In the case that there is a security flaw in a factory at another network-connected base, there is a possibility that the threat could spread to different factories using that factory as a point of intrusion.

As measures in the network, for the purpose of “preventing unauthorized equipment / devices from being connected,” “preventing unauthorized data or programs from flowing in from other networks” and “preventing unexpected or abnormal communication from occurring”

- Configuration division: logical and physical division of the network
- Restrictions on connected devices: network device (switch, router) settings
- Internal concealment: introduction of a gateway
- Communication data limit: introduction of a firewall (FW), Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)
- User restrictions: settings for network devices and security devices (ID / password settings, authentication, etc.)
- Communication monitoring / control: communication status visualization / monitoring, introduction of an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), filtering
- Configuration management: management of connected devices
- Vulnerability countermeasures: vulnerability information collection / diagnosis, measures (software update, patch application, etc.)
- Log acquisition: log acquisition and cooperation, construction of a mechanism for analysis (a function for early detection of abnormalities, for example, behavior detection, etc.)

Etc. can be considered.

Table 3-26 exemplifies the consistent relationship between the items that can be considered as specific measures in the assumed factory, the measures for each security strength for each item, and the purpose of the security measures in terms of system configuration.

Depending on the environment of the individual company or industry, the security strength and countermeasures may not always match the contents of Table 3-26, but in any case, depending on the environment of the individual company or industry, it is important to plan and implement necessary measures while considering the cost-effectiveness of the measures.

Table 3-26 Security measures in the network (examples)

(The table is for illustrative purposes only, so it may be necessary to carefully examine the content based on the individual company or industry)

Countermeasure items	Measures for each security strength			Purpose		
	Minimum	Middle	High	Intrusion prevention	Activity deterrence	Operation support
Configuration division	—	Logical domain subdivision by VLAN, etc.	Physical domain split	○	○	

Restrictions on connected devices	—	IP, MAC restrictions	+ Logical proof of connected device + Ensuring the reliability of the connected device	○	○	
Internal concealment	—	NAT, stealth	Unauthorized communication prevention (gateway)	○		
Communication data limit	Source / Destination Restriction (FW)	+ Communication telegram type restriction, + telegram content analysis / abnormality detection (IDS)	+ Telegram content analysis / Abnormal communication block (IPS)	○	○	
User restrictions	Delete unnecessary users, formulate password policy ²⁴	+ Personal ID authentication (1 factor authentication)	+ Multi-factor authentication	○	○	
Communication monitoring / control	—	Communication status visualization / monitoring (NDR), abnormality detection (IDS)	+ Abnormal communication block (IPS, filtering)	○	○	○
Configuration management	—	Connected device management and visualization	+ Configuration management and visualization in the device			○
Vulnerability countermeasures	Vulnerability information collection	+ Vulnerability diagnosis, intrusion possibility	+ Software update (security patch application) [or virtual	○	○	

²⁴ It is desirable to stipulate the password policy in accordance with the environment of the factory. For example, in cases when there is frequent personnel turnover, etc., (regular) changing of the password is effective, but in cases when changing the passwords of all of the devices subject to management is difficult, etc., it is acceptable to set difficult passwords to use the devices.

		inspection + workaround	measures (IPS, virtual patch, etc.)]			
Log acquisition	Get in-device log (consider the impact on the processing load)	+ IDS log linkage	+ Development of a mechanism for log analysis			○

(ii) Security measures in terms of system configuration of equipment

As a measure for the system configuration of the device²⁵, for the purpose of “preventing the installation / introduction of an unauthorized program in the device” and “preventing the execution of an unauthorized program or command in the device”,

- Device settings
- Security software implementation
- Introduction of external security devices
- Use of functions to detect intrusions into the network at an early stage etc. can be considered.

Table 3-27 exemplifies the consistent relationship between the items that can be considered as specific measures, the measures for each security strength for each item, and the purpose of the security measures in terms of system configuration²⁶.

Depending on the environment of the individual company or industry, the security strength and countermeasures may not always match the contents of Table 3-27, but in any case, depending on the environment of the individual company or industry, it is important to plan and implement necessary measures while considering the cost-effectiveness of the measures.

Table 3-27 Security measures for equipment (examples)

(The table is for illustrative purposes only, so it may be necessary to carefully examine the content based on the individual company or industry)

Countermeasure items	Measures for each security strength			Purpose		
	Minimum	Middle	High	Intrusion prevention	Activity deterrence	Operation support
Communication restrictions	Unnecessary service blockage	+ Communication destination restrictions	+ Introduction of FW	○	○	
Unnecessary port	Terminal cap	+ Soft blockage (service stop, USB class restriction, etc.)	+ Hard blockage (completely unavailable)	○	○	

²⁵ Devices such as production facilities and computers in factories includes equipment that uses general-purpose OS / software such as servers, operation terminal PCs, printers, and high-performance equipment, and equipment that is built using original OS / software. However, here we assume a device that uses a general-purpose OS / software.

²⁶ IoT devices in factories have characteristics which differ from those of conventional control equipment and devices. When considering the security of IoT devices, refer to the following.

- IoT Acceleration Consortium, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry, “IoT Security Guidelines” (July 2016)
- Ministry of Economy, Trade and Industry, “IoT Security and Safety Framework: Securing the Trustworthiness of Mutual Connections between Cyberspace and Physical Space (IoT-SSF)” (November 2020)

Usage port	—	Inspection of media brought in (externally inspect visually and using management slips, etc.)	+ System check, etc. of media brought in (inspect up to the contents and programs using virus checks, etc.)	○	○	
Communication / connected device authentication	—	IP, MAC, device ID authentication	+ Logical proof of the other device (by encryption)	○	○	
Send / receive data protection	—	Encryption, encryption key management	+ Strict protection of encryption key	○	○	
User restrictions	Delete unnecessary users, formulate password policy	+ Personal ID authentication (1 factor authentication)	+ Multi-factor authentication	○	○	
Execution program protection	—	Program tampering measures	+ Utilization of protection tools ²⁷	○	○	
Execution program control	Stop / delete unnecessary programs, manage user groups	+ Group execution authority grant, user authority operation	+ Utilization of execution control tool ²⁸	○	○	
File protection	Manage users groups	+ Encryption	+ Utilization of protection tools		○	
Resource protection (CPU, memory, disk)	—	Regular confirmation	+ Utilization of protection tools		○	
Configuration management	—	Configuration management and visualization in the device	+ Setting information management / visualization			○
Vulnerability countermeasures	Vulnerability information collection	+ Vulnerability diagnosis, intrusion possibility inspection, application of mitigation measures	+ Software update (security patch application ²⁹) [or virtual measures (IPS, virtual patch, etc.)]	○	○	

²⁷ Malware countermeasure functions are included in the protection tools and execution control tool of “execution program protection.”

²⁸ Malware countermeasure functions are included in the execution control tool of “execution program control.”

²⁹ In order to ascertain the application status of the patches and stipulate and implement application plans for the unapplied patches, it is necessary to consider the utilization, etc. of automation tools and carry out patch management.

Log acquisition	Get system log (consider the impact on the processing load)	+ Get operation log / log linkage	+ Development of a mechanism for log analysis			○
Backup (data, equipment)	—	Regular offline data backup	+ Securing switching equipment			○
Ensuring power availability	—	Introducing UPS	+ Introduction of private power generation equipment			○

(iii) Security measures for business programs and services used

In factory systems, necessary functions may be realized by using various packaged software, building functions by original programs, and using services provided by external vendors. When using such services, for example, it is conceivable to confirm from the following viewpoints.

Table 3-28 Items to be confirmed in business programs and services (examples)

(The table is for illustrative purposes only, so it may be necessary to carefully examine the content based on the individual company or industry)

Packaged software	<ul style="list-style-type: none"> • Are the functional specifications related to security described? • Is the set value of the setting item related to security described? • Is there a description of what to do if a security problem occurs?
Original programs	<ul style="list-style-type: none"> • Is the functional specification considering security? • Are security rules in place when building the program?
External service	<ul style="list-style-type: none"> • Are security specifications presented? • Is the set value of the setting item related to security described? • Are there any arrangements regarding the impact of security damage?

(2) Physical measures

For threats such as natural environment threats and physical intrusions, it is mainly necessary to take physical measures. The main measures are to physically protect production facilities and control systems, such as building structures, strengthening fire protection and waterproofing, locking management of power supply equipment and control systems, entry / exit management, and backup³⁰.

(i) Measures related to the building

The factory building is a building in which production facilities, automatic transportation / warehouse equipment, building equipment, etc. are arranged in each room centered on the production site. Inside the building are the production system, automatic transportation / warehouse system, and inter-system network that are indispensable for production. And it is necessary to

³⁰ It is necessary to consider not only the production facilities / control system itself but also the building facility measures for the cyber security measures of the factory. For facility measures, refer to "Guidelines for Cyber-Physical Security Measures for Building Systems".

provide the optimum environment and infrastructure for stable and continuous operation of the devices and equipment that comprise them.

Table 3-29 Measures related to the building (examples)

Waterproofing measures	<p>It is expected that the factory building will be flooded through the gaps in the walls and ducts due to heavy rain and floods. It is also necessary to consider that the water stoppage treatment capacity will decrease due to deterioration over time after the factory starts operation.</p> <p>For example, it is desirable to take necessary measures by referring to the following examples.</p> <ul style="list-style-type: none"> • Water stop treatment with caulking, mortar, etc. should be applied to the parts where pipes, cables, etc. penetrate the outer wall of the building. • Do not install water handling rooms (toilets, etc.) or piping in the attic of the server room or in the adjacent room. • From the hazard map published by the government and recent weather conditions, do not provide a penetration part at a position lower than the assumed submergence level at the time of flood damage. • Equipped with a leak detection mechanism for buried ducts where water tends to stay due to leaks and toll-free access.
Measures against invasion of pests	<p>It is assumed that harmful organisms such as mice will enter the opening of the cable duct and piping rack of the building, and the production line will be stopped or the entire factory will be shut down due to electric leakage due to contact with the electric cable or short circuit.</p> <p>For example, it is desirable to consider measures against the invasion of pests by referring to the following examples.</p> <ul style="list-style-type: none"> • Completely separate unclean places such as sewage tanks and animal breeding grounds by partition walls, etc. • In order to prevent the invasion of small animals such as mice, install screen doors and wire mesh covers on windows and intake / exhaust ports that are open to the outside. • Automatically open / close doors and front rooms should be installed at the entrances and exits that are open to the outside.

(ii) Measures related to power supply / electrical equipment

Factories and production facilities affect product production and quality not only during power outages, momentary interruptions, and voltage fluctuations, but also during legal inspections, equipment expansion / removal, and power supply equipment / devices failures. It is necessary to build highly reliable electrical equipment. For this reason, measures such as

- Construction of equipment monitoring system that links production facilities, automated guided vehicle / warehouse equipment, etc. with BAS (Building Automation System)
- Construction of highly reliable power supply equipment configuration etc. can be considered.

In addition, due to cyberattacks, power supply / electrical equipment is attacked, and not only production lines but also production management / monitoring systems and information systems (OA) systems are becoming more and more damaged. In the case of equipment for which power supply stoppage is unacceptable due to the importance of production facilities and lines, the configuration of electrical equipment related to this is not limited to equipment

stoppages and failures due to production line troubles and cyberattacks. It is necessary to have a facility configuration with redundancy so that power supply can be continued even during regular inspections.

(iii) Measures related to the environment (air conditioning, etc.)

For the environment of the factory production line, automatic transportation / warehouse equipment, etc., and the environment of the server room (computer room, etc.) where the equipment that comprises various systems and networks is installed, it is necessary to consider various conditions such as

- Cooling by air conditioning³¹
- Humidity, static electricity suppression, air cleanliness

At this time, regarding the selection of the cooling method and specifications of the air conditioner, there are methods such as calculating the heat load of the device, calculating the load from the external environment and the load due to internal heat generation, and calculating the cooling load³², so after the calculation, the specifications and number of air conditioners will be finalized, and construction of a server room in which a cooling method suitable for the heat load is selected can be considered.

In addition, it is necessary to take measures that anticipate not only equipment failures and malfunctions but also threats such as cyberattacks and unauthorized operations so that air conditioning stops and abnormalities do not occur.

In addition, it is also necessary to take measures when an abnormality occurs in the control of exhaust and air cleaning so that the exhaust to the outside does not adversely affect the natural environment.

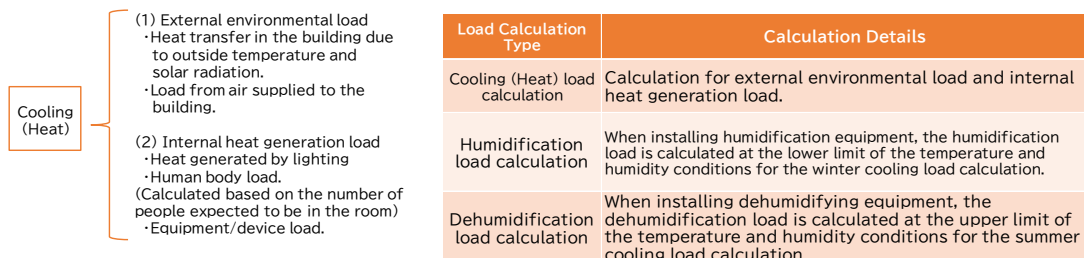


Figure 3-4 Method of calculating heat load of air conditioning equipment

(iv) Measures related to water supply facilities

In factories there is some equipment which does not operate without water. Most of the cooling water used for equipment is a circulation type, and if the circulation is stopped, the cooling efficiency may decrease or the equipment may be stopped in the worst case. For example, it is conceivable to take measures such as³³

- Redundancy of cooling water piping
- Pump redundancy
- Reduce downtime by controlling the number of units

In addition, it is necessary to take measures when the water supply

³¹ It is common to install air conditioning equipment to cool the server room.

³² Although it depends on the seasonal conditions, in cold regions where humidification is required and in hot and humid areas where dehumidification is required, the humidification load and dehumidification load are also calculated, respectively.

³³ Since it may freeze in winter, taking anti-freezing measures could be considered.

equipment is stopped, and it is conceivable to design it so that it can be stopped not only when the water supply equipment is stopped or broken due to an abnormality but also when the equipment is maintained such as pump maintenance.

- Installation of standby system such as spare equipment and piping system
- Installation of bypass line for automatic valve to control flow rate

It is necessary to take measures when an abnormality occurs in the control of water flow related to drainage and water purification so as not to cause environmental pollution not only for water but also for sewerage.

(v) Physical measures related to equipment

It is conceivable to take security measures for the equipment used in the factory system³⁴, depending on the installation location and the importance of the usage work, and also considering the operational aspect.

Table 3-30 Measures related to equipment (examples)

Tipping over / fall prevention	Measures to prevent equipment from tipping over or falling due to earthquakes, etc.
Anti-theft ³⁵	<p>Measures to prevent device theft by unauthorized intruders and internal unauthorized persons</p> <ul style="list-style-type: none"> • Fixable calculators and production line control devices: Implementation of necessary fixation. Consider the installation location for equipment and devices related to particularly important work. • Mobile devices and portable storage devices: Setting of storage method and usage method as goods management method. Conduct regular audits.
Prevention of abuse	<p>Measures to prevent the use of stolen equipment for invading and attacking FA factory systems.</p> <ul style="list-style-type: none"> • Construction of a mechanism to detect stolen devices as unauthorized devices and prevent communication and data exchange even if they are connected to the network. • Similarly, even if the stolen external storage device is connected to the device, it will be detected as an unauthorized device and a mechanism will be built to prevent communication and data exchange.
Prevention of information theft	Construction of a mechanism such as data encryption to prevent the stolen storage device from using the information stored inside.
Prevention of internal fraud / negligence	Physical and logical blockage of unnecessary interfaces / ports (LAN, USB, etc.) in order to prevent malicious networks and devices from being connected to devices intentionally or accidentally inside the factory, being infected by malware, or increasing the number of entrances to cyberattacks.

(vi) Measures related to physical access control

Physical access control refers to protection against physical access to

³⁴ For example, there are computers connected to the network (servers and personal computers) and production line control devices. Moreover, there are mobile devices utilizing wireless and mobile phone networks, devices which are installed in isolation without being connected to a network and link data to other devices using portable memory devices (USB memory, SSD memory, etc.) and devices such as HDD/NAS, etc. which connect to a network.

³⁵ Even if the theft prevention measures are implemented, equipment may still be stolen. Therefore, it is conceivable to take measures to prevent unauthorized use so that the theft does not affect business or corporate trust.

industrial control systems / equipment such as production facilities and computers, and information systems associated with them. Specifically, measures such as the following can be considered:


- Installation of dedicated room (server room / computer room) for industrial control system / equipment
- Introduction of entry / exit management system
- Installation of surveillance cameras
- Construction of management / monitoring system

[Reference] Concept of entry / exit management

The basis of physical access control is entry / exit management. It is necessary to manage entry / exit based on a function that refuses entry / entry for persons who do not have entry / entry authority and allows entry / entry only for persons with legitimate authority and a function that can confirm whether the entry / exit is certainly made at an appropriate time after entry / entry. If only the management of visitors is performed mainly to prevent unauthorized intrusion, it is sufficient to assign and manage people at the reception desk, but cases in which it is necessary to divide the rooms in the factory into access levels according to their purpose and implement "room level" entry / exit management for the employees too, and cases regarding rooms for which it is necessary to ensure a high degree of confidentiality of ensuring that it is possible to lock the room as necessary and then installing equipment / devices for performing authentication of people (authentication equipment / devices using ID cards, biometric information, etc.) are conceivable. Moreover, in order to manage the behavior of people, it is desirable to implement personal authentication and then link that authentication with terminal access authentication and ascertaining of the position within the site.

In order to centrally manage in bulk, we will introduce an entry / exit management system and consider appropriate access level classification. The table below is a reference example of how to divide rooms / areas according to access level, physical access control, and management methods. If necessary, it is conceivable that each company will consider how to subdivide the area and target people according to the access level, and how to control and manage access, with reference to this. Not only physical measures but also measures such as giving reminders to visitors and getting them to wear name tags at all times, etc. can be considered.

Table 3-31 Area division according to access level (examples)



Access Level	Area Name	Area Summary	Target Person
1	General/ Visitor Area	Areas for entering the site/factory building from around the site (Reception desk/Reception room, etc.)	Visitors/ Internal Personnel
2	Office/ Production Area	Areas where internal personnel work and produce on a full-time basis (Production area/Office/Internal meeting room, etc.)	Internal Personnel
3	High Security Area	Areas where highly important systems, Information/Data are Stored/Handled (Centralized monitoring room, Server room, etc.)	Internal Personnel (Production manager/ Employees involved in maintenance)

Table 3-32 Areas subdivided by access level and access control / management methods for target users

Area Name	Management/Access Control Methods	Doors to use	Authentication Method
General/Visitor Area	<ul style="list-style-type: none"> ·All persons entering the factory must wear name tags at all times. ·Nametags for internal personnel must have a picture of the person's face. ·Distinguish between Regular employees/Non-Regular employees by the color of the strap. ·Visitors must wear visitor's name tags. 	Gate-type Opening/Closing doors (Open/Close each time one person passes through)	Personal authentication by IC card distributed to each individual.
Office/Production Area	<ul style="list-style-type: none"> ·Lock the door at all times and specify who is allowed to enter. ·Appoint a manager and manage the occupants. ·All visitors must wear name tags at all times. 	General Opening/Closing doors (Locked by an electric lock when the door is closed)	<ul style="list-style-type: none"> ·Personal authentication by IC card distributed to each individual ·Authentication by PIN
High Security Area	<ul style="list-style-type: none"> ·Not allowed to be adjacent to General/Visitor Area. ·Locked at all times and record of entry and exit kept. ·Have security officers stationed near entrances and exits to monitor them at all times and keep monitoring records for a certain period of time. 	Robust Opening/Closing doors (Locked by an electric lock when the door is closed)	<ul style="list-style-type: none"> ·Personal authentication by IC card distributed to each individual ·Authentication by biometric information such as fingerprints

(vii) Other items that require daily operation and management

Some physical security measures require daily operation and management. For example, the following operational and management items can be considered³⁶.

- Management and confirmation of the actual condition and whether the function of the target countermeasure is maintained
- Monitoring / confirmation of operational status and presence / absence of abnormalities
- Periodic audit of operation / management status and various settings
- Prohibition of unnecessary / unauthorized removal of equipment from the factory
- Prohibition of unnecessary / unauthorized devices being brought into factories and production lines etc.

[Reference] Department in charge of physical security operation and management

In many cases, the departments that handle physical security operations and management differ depending on the target.

- Building entry / exit management (door opening / closing, surveillance cameras, take-out management): General Affairs Department, Security Department, etc.
- Introduction and installation of measures in the factory: Production engineering / management department, etc.
- Countermeasures operation in the factory: work department, etc.

In order to ensure security as a company, it is necessary for these organizations to plan, design, introduce, operate, and manage in cooperation, rather than acting independently.

Especially for operation and management, it is necessary to clarify the role and cooperation measures of each organization in the entire life cycle

³⁶ In some cases, it is possible to utilize a mechanism for centralized and concentrated implementation from a remote location, labor saving, and automation.

of various setting registration / change-monitoring-detection / understanding of abnormal (illegal) signs-analysis-countermeasures.

3.3	Step 3	Implementation of security measures and constant review of plans, measures, and operation systems
------------	---------------	--

In step 3, the security measures planned in step 2 will be executed and measures will be taken in the life cycle and in consideration of the supply chain.

Based on the information obtained from these efforts, after step 3, it is important to implement the PDCA cycle from step 1 to step 3 of reviewing the plans, measures, and operational status according to changes in business, environment, technology, etc., and if necessary, promoting the efforts again from step 1.

When implementing step 3, depending on the environment of the individual company or industry, it is important to plan and implement the necessary measures while considering the cost-effectiveness of the measures.

(1) Life cycle measures

Even if security measures are introduced in terms of physical / system configuration, it can be said that it is difficult to prevent 100 percent of attacks on the system due to the evolution of attack methods on the system. For this reason, depending on the situation of the industry or individual company, in addition to measures in terms of physical / system configuration, it is also important to take measures for early detection as an effort to minimize damage in the event of intrusion or attack activity and measures over the life cycle, such as measures to respond promptly and deter attack activities.

As life cycle measures after starting operation, show

- (i) Operational and management security measures
- (ii) Security measures for maintenance and improvement

(i) Operational and management security measures

As necessary measures in terms of operation and management, three viewpoints are assumed and examples of each are shown.

- A) Early recognition and countermeasures for cyberattacks (OODA process)
- B) Security management (ID / PW management, device setting change, etc.)
- C) Information sharing³⁷

A) Early recognition and countermeasures for cyberattacks

In order to detect and understand system abnormalities caused by cyberattacks at an early stage, it is conceivable to add monitoring from the perspective of cyberattacks on a series of management operations which are dealt with by noticing unusual signs from the behavior of alerts, measured values, indicated values, etc. from devices. In addition, in order to realize prompt responses, it is conceivable to prepare roles, systems, and procedures in advance in anticipation of signs of abnormality, problems, and damage.

When a factory system fails, it is not immediately clear that the cause is a cyberattack. It is important to determine the cases in which coordinating with the security department is necessary and the conditions, standards, and

³⁷. ISAC (Information Sharing and Analysis Center) is an information sharing organization related to cyberattacks. ISACs are installed in several industrial fields such as electric power, finance, ICT, transportation, and automobiles.

procedures for that coordination, based on the situation of the failure of the factory system.

For example, as a model that organizes a series of efforts to recognize and respond to cyberattacks, there is “Observe-Orient-Decide-Act” [OODA process].

Table 3-33 OODA Process

Observe	<p>The following two types of monitoring can be considered as monitoring related to security.</p> <ul style="list-style-type: none"> • By analogy with traditional alerts: Monitor whether equipment failures (stops, malfunctions) and alerts are related to cyberattacks. When an alert occurs, it is necessary to investigate and organize the possibility that the cause is not only a conventional failure but also a cyberattack, and share it with the operator (organization). • Security alert: Monitor for security alerts from security devices and security software. When installing anti-virus (malware) software, firewall (FW) or Intrusion Detection System (IDS) / Intrusion Prevention System (IPS), etc. to the network, it is important for the operator to be able to recognize messages such as alerts from each. As a concrete measure, we will clarify “what cyberattacks can be found” and who will confirm (recognize) the messages issued by these security measures. <p>From the stage when an alert is generated and detected, it is important to contact and share with the company-wide risk management department and cooperate with the entire company in order to take an early response as an entire company from the viewpoint of business continuity.</p>
Orient	<p>As an analysis related to security, it is necessary to analyze the “impact on operations / business” assuming a cyberattack, the “cause” of abnormalities and problems, and the “countermeasures” from the information obtained by monitoring. As information necessary for analysis, it is necessary to organize / understand in advance information related to the relationship between operations and systems and the system configuration (devices, programs, data, network). In order to carry out this analysis, it is important to collaborate with experts who have knowledge of cyberattacks, so if necessary, establish a method of collaborating with security experts in advance.</p>
Decide	<p>As a security-related decision, it is necessary to formulate countermeasures and make decisions on what to implement based on the information obtained from monitoring and the results of analysis. It is necessary to establish in advance a system that enables accurate and prompt decisions, policies / judgment³⁸ criteria, and contact information / means.</p> <p>In order to expedite this decision, it is important to organize / grasp in advance the information in the factory system of the relationship between “operations” and “systems (devices / network)” and the degree of impact / destination when the “operations” or “systems” are damaged, etc. and establish a policy / judgment standard for what should be prioritized.</p>
Act	<p>As actions related to security, it is necessary to contact / instruct related departments (including company-wide risk management,</p>

³⁸ Based on the requirements such as recovery time objective, recovery point objective (recovery point, backup), maximum allowable time, etc. specified in the factory business continuity plan, it is conceivable to set policies / judgment criteria regarding the use of alternative means including the recovery method for the factory system and the utilization of human responses / other production bases.

	information systems, general affairs, legal affairs, finance, public relations, etc.) according to the measures decided by judgment, reliably implement the measures, and verify whether the expected effect has been obtained. For that purpose, it is important to clearly define in advance the system, roles, procedures, and contact information / means when a cyberattack occurs and countermeasures are implemented. In addition, it is desirable to prepare for the format for issuing contact / instructions and for managing the status of countermeasures.
--	--

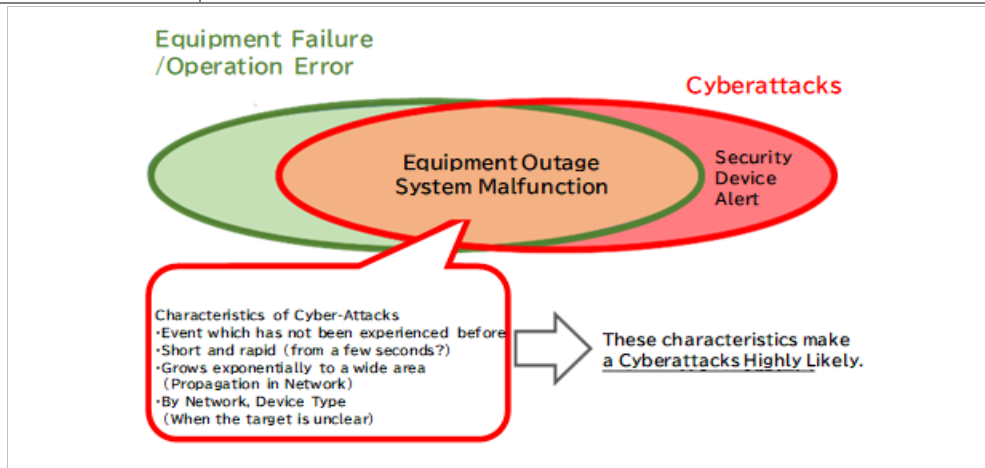


Figure 3-5 Investigating and organizing the causes of alerts

Table 3-34 Assuming security-related possibilities as an alert generation factor

Occurrence event		Occurrence factors		
Device	Content	Target	Presumed factors	Security related
Monitoring system	XX device stop alert	XX device	Device failure	
			Device stop due to unauthorized instruction	○
		Network	False signal	○

Table 3-35 Classification of security alerts and corresponding contents

Device	Message type		
	Type	Notification timing	Corresponding content
FW	Communication refusal	At the time of recognition	Confirmation of target device
IDS	Unauthorized communication	At the time of analysis	Confirmation of target device and communication contents

The content of the analysis in Orient and the content of the judgment in Decide are shown below. The content to be analyzed and the content of judgment differ depending on whether the timing of obtaining information is the “sign stage” or the “damage occurrence stage”³⁹.

³⁹ Efforts to deal with security-related abnormalities and damage are called “security incident response.” The existing guidelines also organize the functions, roles, systems, policies, and procedures required for incident response, see Annex B for details.

Table 3-36 Analysis content in Orient and judgment content in Decide

	Analysis content in Orient	Judgment content in Decide
Sign stage	<ul style="list-style-type: none"> • Since it is an event discovered at a stage where there is no impact on business, we analyze mainly preventive maintenance. • Estimating business damage that may occur, estimating the cause, and examining impact prevention methods (preventive maintenance measures) 	<ul style="list-style-type: none"> • Determine preventive maintenance measures while considering the impact on the production line in operation
Damage occurrence stage	<ul style="list-style-type: none"> • Since it is at the stage where the impact on the business is occurring, the analysis focuses on early convergence. • Examination of cause estimation, impact minimization method (measures for damage occurrence target, damage expansion prevention measures), system / business / business recovery method 	<ul style="list-style-type: none"> • Decide measures to prevent damage and prevent damage from spreading in cooperation with system / business / business recovery (in addition to containment measures; finally, elimination measures will be implemented) • Contact information for various stakeholders (customers, business partners, etc.) that may be affected

The security incident response is implemented in accordance with the following workflow.

- 1) Detection / contact reception: contact from the person who detected the incident, the concerned parties, or an external specialized security organization to the specialized security department
- 2) Response decision: information concerning the incident is collected in the specialized security department, and a decision is made regarding whether or not a response is necessary
- 3) Incident response: in the case that a response becomes necessary, the specialized security department takes the lead in planning the response plan and implementing the response

As appropriate, the status is reported to the management, and if necessary a response by the company is decided

In the case that there has been an impact on our customers or society, etc., information is released through press releases, etc.

B) Security management

As management work necessary for operating security measures, it is conceivable to create and implement the operation rules listed below and the standard procedures based on them and to thoroughly inform the concerned parties.

In order to carry out these management tasks, it is desirable to regularly inform and educate users about operational rules related to the use of equipment and media, entry and exit, etc.⁴⁰

As measures to combat human error, it is desirable to consider measures against negligence and fatigue in operations concerning security and measures

⁴⁰ It is desirable for employees to become able to notice anomalies through email virus response training, etc.

against flaws, etc. in the rules, awareness, and education concerning security.

Table 3-37 Security management work (examples)

Management target		Purpose	Operation rules	Information that needs to be managed
1	User	Prevention of access to equipment / devices by unauthorized persons	Registration / deletion based on user change request, confirmation / deletion depending on usage status	User list by equipment / device (ID, authority)
2	Connected device	Preventing unauthorized equipment / devices from connecting to the network	Registration / deletion based on connection change request, confirmation / deletion depending on usage status	List of registered devices by network (items are based on the ledger)
3	Executed program	Control programs that are allowed to run in the computer	Rules linked with configuration management rules	Execution program for each piece of equipment / device (finally supported by tools)
4	Media	Prevention of connection of unauthorized media and prevention of leakage of media information	Centralized management from purchase to disposal of media and management of usage status (including clearing and virus inspection)	Media list Usage management by medium (items are based on ledger)
5	Equipment / device backup	After being infected by a security incident, it recovers to an uninfected state	Backup standard considering recovery for each piece of equipment / device	Backup history
6	Entering / exiting / person	Preventing unauthorized persons from entering the controlled area	Registration / deletion based on visitor change request, confirmation / deletion depending on usage status	List of entry permission by area
7	Books	Protecting system information such as design documents and system configuration diagrams	Rules utilizing the concept of information management such as ISMS, etc.	Books

8	Patches	Collection of information concerning patches, understanding and management of application status	Consider patch application as promptly as possible, consider application plans for unapplied patches	Information concerning patches
---	---------	--	--	--------------------------------

C) Information sharing

Obtaining information on cyberattacks in a timely manner leads to appropriate preparation and effective security measures for individual companies, and providing information on cyberattacks obtained by individual companies to the industry and government leads to protection from cyberattacks in industry and society as a whole.

Specifically, the following measures are conceivable:

- Information sharing between industry groups and CSIRTs and reflection in appropriate industry standards
- Obtain vulnerability information from Information-technology Promotion Agency, Japan (IPA), JPCERT Coordination Center, etc. and introduce it into your company's security measures
- Obtain information by participating in community activities such as the Nippon CSIRT Association and introduce it into your company's security measures

In many cases threats in factory systems are discussed with the focus on the IT environment inside the factory, but it is difficult to obtain threat information concerning high-risk industrial machinery and networks connecting industrial machinery in Japan, so it is necessary to note that there are differences in the information that is available depending on the industry type and target. In order to obtain and share as much information as possible in this kind of situation, it is desirable to carry out information sharing through industries and communities, etc. regarding information contributing to the measures of each company, such as threat information and effective measures, etc.⁴¹ Note the point that it is necessary to conclude a maintenance contract in advance so that threat information regarding industrial machinery, etc. can be obtained from the vendor.

⁴¹ For healthy community activity, it is necessary for the participants to not only obtain but also provide information. It is desirable for companies which possess information to transmit the necessary information in the community.

[Reference] Operation management system (examples)

Early detection and response to cyberattacks are important for maintaining business continuity and corporate trust. However, in order to operate and manage security, it is necessary to improve the system, secure personnel, and improve support tools.

Therefore, it is necessary to consider the level of development of the operation and management system. Examples of this system development are presented. Although operation systems can be outsourced, there is a possibility that outsourcing all of the management system will result in the chain of command breaking down, so it is necessary to note that the management responsibility must always remain with the company.

- Operation in existing system operation / maintenance organization
- Operation in the operation organization of the IT department
- Outsourced operation
- Operation in your own organization

(1) Operation in existing system operation / maintenance organization

In the current organization that operates and maintains the existing system, operation and management related to cybersecurity is also a form that is implemented. Organizations centered on the OT departments of each business division and factory also fall under this category.

- Advantages:
Can be handled in combination with conventional failures.
- Disadvantages:
Absence of security experts. Difficult to respond immediately outside normal working hours.

(2) Operation and management in the operation organization of the IT department

When the IT department has already implemented the security operation and management of the OA system, etc., the IT department also implements the security operation and management of the factory system.

- Advantages:
Take advantage of IT department security experts.
If you are monitoring 24 hours a day, you can respond immediately.
- Disadvantages:
Traditional failure-related events that normally occur also occur.
Analysis, including the impact on business, is difficult due to lack of knowledge of factory system.

(3) Outsourced operation and management

This is a form in which all or part of security operation and management is outsourced to an external organization.

- Advantages:
No need for security experts in-house.
- Disadvantages:
Only the contract details are outsourced, and cooperation with the operation and management of the factory system is required.

(4) Operation and management in your own organization

This is a form involving newly establishing an organization for operating and managing the security of the factory system. There may be a committee-like structure consisting of members of the OT department and IT department (or security department) of each business division / factory.

- Advantages: All can be operated and managed comprehensively.
- Disadvantages: Need to train specialists. Requires operation and management personnel.

(ii) Security measures for maintenance and improvement

Maintenance / improvement security measures include confirming the implementation and operational status of the security measures and their effect⁴² and then collecting information related to changes in the environment surrounding the factory system, evaluating the security measures taking into account the perspective of ensuring BC / SQDC, and if necessary reviewing and updating physical, system, and operation / management security measures.

Attack methods are evolving day by day, and while new security weaknesses in factory systems and equipment are becoming apparent, collecting, grasping, and responding to information related to new attack methods and vulnerabilities⁴³ enables prevention of attacks on factory systems and damage.

Furthermore, in order to maintain and continue security measures, it is important for people involved in factory systems to have security skills according to their respective positions in order to improve the skills of organizations and human resources. For that reason,

- Carrying out regular education and dissemination with respect to employees involved in factory systems is desirable in order to encourage their understanding regarding the risks of cyberattacks and the matters to be implemented pertaining to the security measures necessary in the operations⁴⁴.
- With respect to employees with the duty of ensuring the security of the factory systems, the education concerning the latest security threats and vulnerabilities and organizationally and technologically effective measures which is necessary for ensuring the security of factory systems, and understanding of the rules and procedures for responding appropriately when cyberattacks occur and simulated training, etc. are effective.
- With respect to providers of equipment and services pertaining to factory systems, it is necessary to understand and implement the security necessary for the delivered equipment and services, so it is necessary for the vendors carrying out the maintenance and operation to receive education enabling them to thoroughly implement the security measures necessary when carrying out maintenance.

⁴² There is also the method of confirming and evaluating the implementation and operational status of security measures based on risk management from an independent and specialist position in the form of an audit, and some companies utilize the method of an audit in their reviews.

⁴³ In order to carry out a higher level of response to a vulnerability, it is effective to utilize indicators such as KEV (known exploited vulnerability) and EPSS (the likelihood that a vulnerability will be exploited), etc. to assign the order of priority of vulnerabilities on a risk basis.

⁴⁴ It is desirable for employees to become able to notice anomalies by carrying out training themselves.

Table 3-38 Activities necessary for maintenance and improvement (examples)

Obtaining information on changing security threats / attack methods, vulnerabilities, and technologies	<p>For example, the following organizations publish threat / vulnerability information and security technical information.</p> <ul style="list-style-type: none"> Japan Computer Emergency Response Team Coordination Center https://www.jpcert.or.jp/ Information-technology Promotion Agency, Japan (IPA) https://www.ipa.go.jp/security/index.html <p>As external security information sharing organizations, there are Nippon CSIRT Association, ISAC, which is established and operated by industry, IPA's Initiative for Cybersecurity Information Sharing Partnership of Japan (J-CSIP), etc.</p>
Obtaining vulnerability information on the equipment used and software	<p>The vulnerability information of general-purpose products of devices and software is disclosed above, but it is necessary to confirm the handling of vulnerability information of devices and software other than general-purpose products and the provision of mitigation measures with each product manufacturer.</p>
Skill improvement and training of human resources	<p>In many cases, security education for people engaged in factory systems is not conducted except for OA-related security education (such as dissemination by e-mail), and so far, the frequency of cyberattacks in factory systems has been high. It is difficult to act properly when it actually occurs.</p> <p>In addition, the skill itself may be lost due to the regular transfer of people. Therefore, it is essential to maintain and improve security skills based on the actual factory system.</p> <p>For example, in addition to email virus response training for employees and basic security education for employees with the duty of ensuring security, it is conceivable to repeatedly carry out simulated training by generating cyberattacks⁴⁵, and it is conceivable that due to this people involved in factory systems will accumulate, maintain, and improve the necessary skills from their respective positions.</p> <p>In many cases, security education for people engaged in factory systems is not conducted except for OA-related security education (such as dissemination by e-mail), and so far, the frequency of cyberattacks in factory systems has been high. It is difficult to act properly when it actually occurs.</p> <p>In addition, the skill itself may be lost due to the regular transfer of people. Therefore, it is essential to maintain and improve security skills based on the actual factory system.</p> <p>For example, in addition to email virus response training for employees and basic security education for employees with the duty of ensuring security, it is conceivable to repeatedly carry out simulated training by generating cyberattacks, and it is conceivable that due to this people</p>

⁴⁵ Regarding simulated training concerning security targeting control systems, programs are provided in the Information-technology Promotion Agency, Japan's Industrial Cyber Security Center of Excellence (ICSCoE), the Control System Security Center (CSSC), etc. Furthermore, several private companies are also providing simulated training services using virtual environments.

	<p>involved in factory systems will accumulate, maintain, and improve the necessary skills from their respective positions.</p> <p>Moreover, the training of human resources who can judge the abilities of the suppliers, whether the security necessary for the delivered equipment and services has been implemented, and whether it is at an acceptable security level is also necessary.</p>
Regular confirmation, improvement and review activities	<p>It is important to regularly confirm whether or not the implemented security measures are being operated effectively, and to carry out improvements and reviews based on the confirmation results.</p> <p>It is necessary to confirm whether education for operating the security appropriately and systems which prevent inappropriate operation have been put in place, etc. Furthermore, in the case that the security operation does not match the actual state of the business, it is also important to design the business so that the employees can operate the security easily.</p>

(2) Supply chain measures

As supply chains expand, there are increasing numbers of cases in which companies with poor security measures are targeted by cyberattacks inside supply chains which contain both large companies and small and medium-sized enterprises (SMEs). It is also necessary for SMEs with limited budgets for measures and limited human resources to advance security measures in their factories to protect their own businesses. As globalization progresses, supply chains are also globalizing. Many manufacturing companies which possess factories are engaged in their business not only in Japan but also globally, so it is necessary for them to consider the global situation and advance measures in compliance with the legal systems, standards and guidelines, etc. of each country. It is important to consider security measures for the entire supply chain because security risks in the supply chain⁴⁶ can affect the engineering chain, supply chain, and value chain partners without being contained to one factory⁴⁷.

In this guideline, the main points to be considered for each are illustrated from the following points of view:

- Purchased products / parts
- Outsourcing
- System development consignment
- Cooperation system

Since the structure of the supply chain and the surrounding environment vary depending on the situation of the industry and individual companies, it is desirable to carefully examine the items and consider the specification of each item as appropriate, and if necessary, request security measures from business partners and suppliers and confirm the status of measures⁴⁸. There are cases in which customers voluntarily make changes which could damage the security policy after the supply has delivered the products / parts and systems to the customer, so it is necessary for the suppliers to deal with this problem by exchanging documents with the customers regarding the content that it is possible for both parties to implement and the scope of their responsibilities.

Table 3-39 Main confirmation points for business partners and suppliers (examples)

Purchased products / parts	<p>Check the following points when purchasing products / parts⁴⁹.</p> <ul style="list-style-type: none"> ● Does the maintenance scope include the provision of security vulnerability information and patches? ● Is there a system in place to respond to security threats? <p>Also, is the contract form available for immediate response at the time of request?</p>
----------------------------	---

⁴⁶ In cyberattacks targeting factories, there are cases where more vulnerable small and medium-sized enterprises and overseas factories are first attacked / invaded, and then the factories of the large companies with which they cooperate are attacked / invaded. In these kinds of cases, damage from the cyberattacks occurs in both the large companies and the small and medium-sized enterprises, so it is necessary to advance cooperative security measures in a form which achieves consistency in the responses of each party and is based on their own respective business continuity plans.

⁴⁷ According to "10 Major Security Threats 2021" (Independent Administrative Institution Information-technology Promotion Agency, Japan), "Attacks exploiting supply chain weaknesses" which target business partners with weak supply chain security, rather than directly attacking companies with strong security measures are the fourth largest threat in the organization.

⁴⁸ The Robot Revolution / Industrial IoT Initiative Council has formulated the "RRI Supply Chain Questionnaire Ver.1.0" to easily evaluate whether the procurement source meets the security level expected of the supplier at the time of procurement. This questionnaire consists of 25 questions based on the Ministry of Economy, Trade and Industry's "Cyber/Physical Security Framework" and can be used regardless of the size or industry type of the company.

RRI Supply Chain Questionnaire <https://www.jmfrri.jp/document/library/1890.html>

⁴⁹ In the case of applying patches to vulnerabilities detected in the delivered manufacturing equipment, it is desirable to clarify the responsibility, etc. at the time when the trouble occurs.

	<ul style="list-style-type: none"> • Is the function implementation and verification⁵⁰ implemented from the security perspective of the product / part? • Have arrangements considering the risk of information leakage at the time of disposal been implemented?
Outsourcing	<p>Check the following points when outsourcing part of the work related to the system.</p> <ul style="list-style-type: none"> • Are security requirements for workers specified? Also, are the requirements the same as or more stringent than your own? • Is security education implemented for workers? Also, is the content of the education to be implemented the same as or stricter than that of the company? • In the case that subcontracting is permitted, is the security management of the subcontractors being implemented? Also, is the content of the security management the same as or stricter than that of the company?
System development consignment	<p>When outsourcing part of system development, it is necessary to confirm the following points.</p> <ul style="list-style-type: none"> • Are there requirements for security considerations in each phase of the development process? • Is the confirmation of security specifications and implementation status stated at the time of acceptance of the deliverable? • Are there any requirements regarding confidentiality of handled information? • Is it stated that the information will be destroyed at the end of the consignment? • Are security requirements for the development environment listed? • Are audit requirements listed?
Cooperation system	<p>Check the following points when linking the factory system with other systems and cloud services.</p> <ul style="list-style-type: none"> • Is it stated that information related to security is linked with the department that manages the linked system? • Is the scope of responsibility in the event of a security failure stated? • If a security failure occurs, is there a description of cooperation for solving the problem? • Is there a description of joint implementation of security training? • Are rules and arrangements concerning the handling and protection of shared information stipulated?

[Reference] Security certification systems for control systems and the IoT

Certification refers to the evaluation of products and services, etc. based on specific requirements (criteria, standards, regulations) and a guarantee in writing by a third party if they are in compliance.

In control systems of the kinds used in factories, there are certification systems based on the IEC 62443 series of standards, and in Japan there is the EDSA certification implemented by the Control System Security Center (CSSC). Furthermore, for IoT products, in Japan there are certification systems based on the rules for terminal equipment, etc. (Ministerial Ordinance) (Article 34-10, the so-called “technical suitability”) and the CCDS Certification Program implemented by the Connected Consumer Device

⁵⁰ “Equipped with security functions”, “security inspection / diagnosis”, “product security authentication”, etc.

Security Council (CCDS) General Incorporated Association, etc.

Certification enables confirmation that a certain standard of security has been secured, so employing these products is effective for strengthening the security of factory systems, and it is also possible to utilize them as a condition at the time of procurement.

[Reference] Subcontracting promotion standards

The following items are described when responding to computerization in the subcontracting promotion standards established by the Small and Medium Enterprise Agency based on the provisions of Article 3, Paragraph 1 of the Act on the Promotion of Subcontracting Small and Medium-sized Enterprises as general standards for subcontractors and parent businesses in order to promote subcontracting SMEs.

Article 3 Matters concerning the introduction of facilities or equipment of subcontractors, improvement of technology, and business sharing

5) Active response to computerization

- (1) Subcontractors shall proactively respond to the following items in addition to necessary security measures in order to improve efficiency by reviewing business processes, including improving management capacity, reducing the amount of work, and speeding up work.
 - (i) Deployment of responsible persons for computerization and improvement of in-house systems (including promotion of digitization of operations)
 - (ii) Electronic ordering through EDI (electronic data interchange) common to small and medium-sized enterprises
 - (iii) Electronic payment, etc. (utilization of Internet banking, electronically recorded loans, Zengin EDI system, etc.)
- (2) In order to support the efforts of the subcontractor in the previous item, the parent company shall respond to the requests of the subcontractor, provide guidance on improving management capabilities, provide standard computers, software, and databases, train operators, and cooperate in advice and support for security measures, and provision of information on computerization support measures by the national and local governments. In addition, from the perspective of improving efficiency by reviewing the business processes of the entire supply chain, it shall actively encourage the introduction of electronic ordering and electronic payment, etc. while giving consideration to the next item, and also endeavor to connect itself to the system related to standardized electronic ordering or electronic payment.

Reference) Small and Medium Enterprise Agency website
<https://www.chusho.meti.go.jp/keiei/torihiki/shinkoukijyun.htm#zenbun>

[Reference] Consideration of measures in operating factories and new factories

When taking security measures for a factory system, it is necessary to consider whether the target factory system is “in operation”, “about to be updated”, or “being planned”.

(1) When it is in operation

It is necessary to consider and plan security measures in consideration of the impact of system renovation due to the introduction of security measures. Regarding system configuration measures, while giving priority to measures that do not affect the factory system in operation, if measures that have an impact are required, consider introducing them during the periodic system outage period (maintenance period, etc.) of the factory system. In addition, consider supplementing them by enhancing physical measures and life cycle measures.

(2) When it is about to be updated

Regarding system configuration measures, it is necessary to take measures to ensure that there is no difference in the strength of the measures between the part to be updated and the part to be continuously used in the factory system. If it is difficult to introduce system configuration measures to the existing part, consider supplementing them by enhancing physical measures and life cycle measures so that the existing part does not become a loophole for attacks or fraud.

(3) When it is being planned

In the case of a new installation, there is an advantage that it is easier to introduce security measures compared to operating or existing factory systems. On the other hand, factory systems are often used for a long period of time (10 years or more), during which time new equipment is introduced and maintenance of initially introduced equipment expires. Therefore, when considering and planning security measures, it is necessary to anticipate future changes as much as possible.

[Reference] Strategy execution management

Clarify control measures to ensure that the formulated strategy is realized.
Clarify plans to be implemented in the future based on the formulated overall policy.

At the time of planning, in order to obtain the intended effect, the system responsible for the purpose, policy, and promotion of the plan should be clarified, and the implementation plan, cost, and personnel plan should be clarified for each target effect.

In the progress confirmation, confirm the progress status for the implementation plan and check if there is any change in the information collected and organized in step 1 which is the premise of the implementation plan, namely “organization related to management goals”, “consideration of external requirements”, and “understanding internal requirements / status”.

<Examples of viewpoints>

Organization related to management goals:

- Enhancement of product lineup, flexible production line construction
- New connection with another smart factory
- Improvement of factory energy efficiency
- Stronger environmental consideration, etc.

Consideration of external requirements:

- Economic security requirements
- Formulation of new international standards, etc.

Understanding internal requirements / status:

- Review of company-wide security rules
- Changes in network configuration, equipment / devices configuration, and changes in security measures
- Change of security monitoring range, software update
- Changes in security system, enhancement of security education, etc.

With these changes, it may be necessary to review the importance of protected assets and operations.

In addition, threats are constantly changing due to the evolution of cyberattacks around organizations and the sophistication of attacks. As for countermeasures, there are cases where countermeasures that could not be implemented until now can be realized at low cost or with low load due to technological progress.

Based on this result, the plan will be reviewed if necessary, and the implementation will be carried out continuously and adaptively with the consent of the management.

Annexes

Annex A Terms/Abbreviations

AGV <<Automatic Guided Vehicle>>

CISO <<Chief Information Security Officer>>

CMMI <<Capability Maturity Model Integration>>

CPS <<Cyber Physical System>>

CPU <<Central Processing Unit>>

CSIRT <<Computer Security Incident Response Team>>

CSR <<Corporate Social Responsibility>>

FA <<Factory Automation>>

FW <<Firewall>>

ICS <<Industrial Control System>>

IDS <<Intrusion Detection System >>

IP Address <<Internet Protocol Address>>

IPS <<Intrusion Prevention System>>

ISMS <<Information Security Management System>>

LAN <<Local Area Network>>

NIST <<National Institute of Standards and Technology>>

OA <<Office Automation>>

OODA <<Observe, Orient, Decide, Act>>

OT <<Operational Technology, control and operating technology>>

SCADA <<Supervisory Control And Data Acquisition>>

SIRT <<Security Incident Response Team>>

SOC <<Security Operation Center>>

SSD <<Solid State Drive>>

VLAN <<Virtual Local Area Network, Virtual LAN>>

VPN <<Virtual Private Network>>

Access control

Controlling the authority and permission for users to be able to access the resources of computer systems. [IPA Network Security-Related Glossary]

Access port

A port allocated to only one VLAN.

Encryption key

The data which serves as a key, used when encrypting or decrypting data.

Interface

In hardware and software, the places which connect different devices and systems and the standards, procedures, etc. for exchanges of information, etc. between two parties. Input and output of the place that constitutes a contact point between the computer and the user.

Engineering chain

The chain consisting of research and development, product design, process design, and production, etc. [Ministry of Economy, Trade and Industry “White Paper on Manufacturing Industries” 2020 edition]

External storage media

External storage media capable of reading and writing data. USB memory, optical media such as DVDs, CDs, etc., external hard disks, etc.

Availability

Ensures timely accessibility and usability when necessary. [IPA Network Security-Related Glossary]

Integrity

This is correctness and completeness and ensures that the data and the information systems storing the data are accurate and complete. [IPA Network Security-Related Glossary]

Confidentiality

The characteristics of data and information systems which are disclosed only to authorized people or entities and processed using the authorized methods at the authorized times. Ensures that users without authority (unauthorized users) cannot access the information. [IPA Network Security-Related Glossary]

Client

A computer or software that requests a service such as a function or information, etc. from a server and receives the service.

Gateway

In a computer network, a function or device for connecting to different networks of a protocol (means of communication).

Command

Instructions and orders for processing to be performed in a computer. In addition

to commands from people to computers, there are also commands given from computers to peripheral devices and between software.

Supply chain

The chain consisting of ordering, production control, production, distribution and sales, after-sales service, etc. [Ministry of Economy, Trade and Industry “White Paper on Manufacturing Industries” 2020 edition]

Authenticity

The fact that users, information, etc. are exactly what they claim to be.

Vulnerability

This refers to the existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved [IPA Network Security-Related Glossary]

Accountability

To be able to identify actions with respect to information assets and the users who carried out the actions and to be able to track them back into the past.

Segment

The scope of the individual networks dividing up the entire network.

Software

Instructions, programs and data for operating a computer.

Disk

A thin disc-shaped data storage medium such as a hard disk or CD / DVD / BD (Blu-ray Disc), etc. or an auxiliary storage device.

Device ID

An identifier for identifying a device, expressed as a character string consisting of alphanumeric characters.

Traceability

Makes the distribution route traceable from raw material procurement to production, consumption and / or disposal

Internal control report

A report in which the manager evaluates whether the internal control of a company is functioning effectively based on the Financial Instruments and Exchange Act and describes the results.

Hardware

The physical devices that make up the system, such as the computer, etc.

Value chain

On the assumption that the main activity of a company is to add value to purchased raw materials, etc., five activities are defined as main activities: purchasing logistics, manufacturing, shipment logistics, sales and marketing,

and services; and four activities are defined as support activities: general management (infrastructure), personnel and labor management, procurement activity, and technology development.

Non-repudiation

Makes it impossible to repudiate after the fact the taking of a certain action.

Firewall

This is the concept of protecting a specific network segment at the point where it connects to other networks, and typically involves protecting the internal intranet from the external Internet. [IPA Network Security-Related Glossary]

Firmware

The software which controls computer systems embedded in electronic equipment.

Feedback control

A control method that improves control quality by feeding back the output (control amount) to the input (target value) side in the control system.

Free access

Double flooring for storing power supplies, wiring for communication, etc.

Penetration test

A test which attempts to penetrate inside a network from outside the network. [IPA Network Security-Related Glossary]

Port

An input / output outlet for devices such as computers, etc. and programs to connect to and communicate with other external devices and programs.

Whitelist / permit list

A list definition of “safe targets” used in methods to prevent cyberattacks by preventing unauthorized program execution, communication, and operation.

Wireless LAN

A LAN which is connected using wireless communication.

Wireless LAN access point

A device which wirelessly connects terminals to send and receive data.

Memory

A device that stores programs and data in a computer.

Ransomware

A general term for malware which makes the data in a terminal or server unusable using encryption, etc. and displays a threatening message urging the user to pay a ransom in exchange for recovery of the data.

Securities reports

The disclosed materials concerning corporate information such as the listed

companies that issue shares, etc., as provided for in the Financial Instruments and Exchange Act. The company overview, business status, and financial statements, etc. are disclosed.

Annex B Social Security Requirements Surrounding Factory Systems

B-1 Requirements for compliance with laws and regulations, standards and guidelines

B-1.1 Requirements for security measures based on laws and regulations

In terms of laws and regulations, if a company suffers damage due to a director's failure to maintain a cybersecurity system, the individual director may be held liable for negligence of duties to the company⁵¹ or for damages to third parties⁵² for breach of his/her duty of care⁵³ or duty of loyalty⁵⁴. In addition, if a company or system fails to respond promptly and appropriately to a cyberattack, it may be held liable for tortious behavior as well.

In past court cases concerning the above-mentioned claims for damages, when a company did not implement security measures that met the 'Technical standards of the time', the management was held liable for 'negligence of duty' as a 'Breach of the duty of care of a good manager'. The 'Technical standards of the time' include the contents described in security measure guidelines, mainly government guidelines.

In addition, the "The Basic Act on Cybersecurity" is the fundamental law for cybersecurity in Japan, which establishes the basic principles, clarifies the responsibilities of the government, formulates cybersecurity strategies, and stipulates other matters that form the basis of such policies for promoting cybersecurity measures in a comprehensive and efficient manner.

Based on this law, the government is to establish a Cybersecurity Strategy, which is a basic plan for cybersecurity, and the government also required critical infrastructure providers, etc. to promote the assurance of cybersecurity as a basic measure.

[Reference] Security Laws and Regulations by Industry

- Security Laws and Regulations in the Electric Power Sector

In the Electric Power Sector, in the United States, companies that own large-scale power generation and transmission facilities in North America are required to comply with the CIP (Critical Infrastructure Protection) standard developed by the North American Electric Reliability Corporation (NERC) in the United States.

Similarly, in Europe, the NIS Directive (EU2016/1148) has been defined and enforced as a legal regulation mandating security measures for critical infrastructure operators. In the Electric Power Sector, in addition to generation/transmission operators, the Directive also covers retail sellers (assuming they are responsible for the installation of smart meters, etc.).

In Japan, Article 39 of the Electricity Business Act and the Ministerial Ordinance establishing technical standards for electric facilities stipulate cybersecurity for General Transmission and Distribution Business, Electricity

⁵¹ Article 423, Paragraph 1 of the Companies Act

⁵² Article 429, Paragraph 1 of the Companies Act

⁵³ Article 330 of the Companies Act, Article 644 of the Civil Code

⁵⁴ Article 355 of the Companies Act

transmission business and Computers that manage the operation of electric facilities used for specified power transmission and distribution projects and power generation projects require compliance with the technical standards.

As required by these power generation/transmission and distribution companies, the companies/factories that produce the products that make up the power generation and transmission/distribution facilities are also required to take the necessary measures to ensure the security of products.

- Security Laws and Regulations in the Automotive Sector

In the automotive sector, the United Nations World Forum on Harmonization of Vehicle Standards (WP29) defined rules for vehicle cybersecurity and software updates, and the international standard ISO/SAE 21434 was defined based on these rules. These rules will first apply to new OTA (onboard program alteration via radio) compatible vehicles released in Japan after July 2022, and will eventually be applicable and mandatory for all vehicles after May 2026.

Companies/factories that produce automobiles are also required to have processes (Systems, Management/Operation, Maintenance/Improvement) to ensure security in accordance with the stipulated CSMS (Cybersecurity Management System).

- Security Laws and Regulations in the Medical Device Sector

In the medical device sector, the U.S. requires confirmation of cybersecurity measures in the review of FDA (U.S. Food and Drug Administration) 510(k) applications for premarket approval required to sell medical devices. Criteria including the 'Content of Premarket Submissions for Management of Cybersecurity in Medical Devices' are specified in the guidance documents.

Similarly in Europe, the EU Medical Device Regulation (MDR) including security requirements has been commenced and applied as a legal regulation mandating security measures for medical devices.

In Japan, the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices requires risk management based on JIS T14971 (equivalent to ISO 14971) for medical devices, the 2020 revision of JIS T14971 also requires security measures. After September 30, 2023, when the transitional measures expire, compliance with JIS T14971:2020 is mandatory.

In addition, the Ministry of Health, Labor and Welfare's Department of Pharmaceutical Sciences and Living Hygiene has issued a document entitled "Publication of Guidance on the Principles and Practices of Medical Device Cybersecurity by the International Medical Device Regulatory Authority Forum (IMDRF) (request for dissemination)". It has been shown that IMDRF guidance will be introduced to medical device manufacturers and distributors by about 2023. Examination based on this guidance will start from 2022 at the earliest, and it is expected that cybersecurity measures for medical devices will be required. By the way, IMDRF's Medical Device Cybersecurity WG is chaired by the US FDA's Head of Medical Device Cybersecurity Guidance, which is led by the United States. In addition, the above ISO 14971 is referred to in the IMDRF guidance as a risk management principle for medical devices.

Companies/factories that produce medical devices are also required to have a risk management process (Systems, Mechanism, Management/Operation, Maintenance/Improvement) throughout the entire product life cycle to ensure the security of medical devices in compliance with regulations.

- **Security Laws and Regulations in the Critical Infrastructure Sector**

In the critical infrastructure sector, in the U.S. the Department of Homeland Security (DHS) has taken the lead in developing plans to ensure security in Energy (electricity, gas, oil), Nuclear facilities, Defense Industrial Base, Government facilities, Agriculture/Food, Medical/Public Healthcare, Finance, Water and sewage, Chemical, Commercial Facilities, Critical Manufacturing, Dams, Information Technology, Telecommunications, Emergency Services and Transportation/Logistics, and government and industry have jointly implemented security measures in each sector to promote the project. As for laws and regulations, the situation is still limited to a few sectors.

In Europe, the NIS Directive (EU2016/1148) is defined and enforced as a legal regulation that mandates security measures for critical infrastructure providers. Essential entities: Energy (Electricity, Oil, Gas), Transportation, Medical care, Water and sewage, Space, etc. Important entities: Postal/Shipping, Waste disposal, Chemicals, Food, Manufacturing (Medical equipment, Computers and Electronic products, Electrical equipment, Machinery equipment, Automobiles, Other transportation equipment).

In Japan, cybersecurity measures for critical infrastructure have become increasingly important from the perspective of national and economic security.

Critical infrastructure refers to 14 fields: Information Telecommunications, Finance, aviation, Airports, Railroads, Electricity, Gas, Government/Administrative Services (including Local Governments), Healthcare, Water, Logistics, Chemicals, Credit, and Petroleum.

Companies/factories that produce products such as industrial control equipment that make up critical infrastructure must also take the necessary measures to ensure product security.

B-1.2 Requirements for compliance with standards and guidelines related to security

To realize security measures in a factory system, it is necessary to consider what security measures should be implemented and to what extent. Reference information for this examination includes domestic and international standards, guidelines, laws, and regulations, as well as requirements stipulated by suppliers.

The following is a representative list.

(1) Global standards

(i) Common and typical standards

- IEC 62443 series of standards:

Defines overall security from control system management to systems

and components.

- ISO/IEC 27000 series:
Defines the management of cybersecurity.
- IEC 61508:
Functional safety standard for electrical, electronic and electro-programmable (devices / systems).

(ii) Standard for each sector

- ISO / SAE 21434:
Regulations on Automobile Security.
- ISO 14971:
Regulations on risk management and security related to medical devices.
- IEC 62278:
Safety regulations for the Railroads sector.
(RAMS: Reliability, Availability, Maintainability, Safety)
- IEC 62351:
Power System Management and Related Information Exchange Data and Communications Security.

(2) Overseas standards / guidelines

(i) The United States

Guidelines established and published by the National Institute of Standards and Technology (NIST) are often used.

Typical examples are 'NIST CSF' and 'NIST SP 800 series'.

- NIST CSF (Cybersecurity Framework):
This guideline mainly stipulates countermeasures and responses to cyberattacks.
It is classified and presented as "identification-defense-detection-response-recovery".
- NIST SP 800 series:
Guidelines for government procurement systems, some of which specify security requirements. These guidelines are often referenced not only in government procurement, but also in general systems. The following is a representative list.
 - SP 800-30: Provides guidance on conducting risk assessments.
 - SP 800-53: Security and Privacy Controls for Government Systems and Organizations.
 - SP 800-82: Based on SP 800-53, presents control measures for industrial control systems (ICS).
 - SP 800-115: Presents a basic technical guide for assessing information security.
 - SP 800-161: Based on SP 800-53, presents supply chain controls.
 - SP 800-171: Based on SP 800-53, provides controls for contractors handling government information.

(ii) Europe (EU)

The EU defines the security requirements necessary to protect the IT / OT systems and information handled in the member states.

- NIS Directive (Directive on Security of Network and Information Systems):

This directive is on the security of networks and information systems. It specifies cybersecurity requirements for systems for mission-critical service operators (including Industrial Systems) and Digital Service providers. Each EU country has drawn up its own regulations based on this Directive. A revision was proposed in December 2020, and it is planned to strengthen the measures (e.g., use of certified products) in anticipation of IoT and DX-enabled supply chains.

■ **GDPR (General Data Protection Regulation):**

This regulation provides for the protection of personal data and privacy within the EU.

Because this regulation is for people in the EU, similar treatment outside the EU area is required. Common rules for the EU area.

(3) Domestic guidelines in Japan

(i) General overall security-related policies, guidelines, etc. in Japan

Table B-1 General overall security-related policies, guidelines, etc. in Japan

Publisher	Document name	Overview
National center of Incident readiness and Strategy for Cybersecurity	Cybersecurity Strategy	Overall policy as a government. Revised in September 2021.
	Action Plan on Cybersecurity for Critical Infrastructures	A basic framework for protecting critical infrastructures. Revised in June 2022.
Ministry of Economy, Trade and Industry	Cybersecurity Management Guidelines	This guideline organizes management's role and what should be done.
	The Cyber/Physical Security Framework (CPSF)	This framework organizes the image of security measures for the entire supply chain in 'Society 5.0' and 'Connected Industries' which integrate cyber and physical space.
	IoT Security Safety Framework -Ensuring the reliability of the connection between physical space and cyberspace- (IoT-SSF)	This framework organizes the concept of ensuring the reliability of the connection between physical and cyberspace in 'Society 5.0' and 'Connected Industries'.
	"Guide for security verification to ensure cybersecurity of devices" [Separate Volume 1] Detailed Explanation of Threat Analysis and Security Verification [Separate Volume 2] Explanation of Threat Analysis and Security Verification for Equipment Manufacturers.	This shows the matters that the verification service provider should carry out in the security verification that verifies the security of the device. Separate volume 1 organizes specific examples of threat analysis and ideas of effective verification methods, and comprehensively and in detail shows the matters and methods that verification service providers should implement. Separate volume 2 provides verification knowledge, including proactive measures, to manufacturers who develop, manufacture, and sell IoT devices, etc., when the manufacturer becomes a verification requester.

	Control System Security Risk Analysis Guide (IPA: Information-technology Promotion Agency, Japan)	This guide presents security risk derivation methods.
	Control system safety and security requirement definition guide (IPA: Information-technology Promotion Agency, Japan)	This guide organizes study points and procedures for ensuring the safety and security of control systems.
	IoT Safety/Security Design Tutorial (IPA: Information-technology Promotion Agency, Japan)	A guidebook for the 'Safety Design', 'Security Design' and 'Visualization' necessary for IoT products / services.
	IoT Safety/Security Development Guidelines (IPA: Information-technology Promotion Agency, Japan)	This guideline presents risks and guidelines pertaining to the countermeasures to consider when developing IoT products.
	Security Design Guide in IoT Development (IPA: Information-technology Promotion Agency, Japan)	This guide organizes security threats and countermeasures anticipated in IoT devices and use environments.
	Approaches for Embedded System Information Security (IPA: Information-technology Promotion Agency, Japan)	This guide presents specific guidelines for security initiatives which should be considered at each phase of the lifecycle of embedded systems connected to the network.
	Security in devices using embedded software (IPA: Information-technology Promotion Agency, Japan)	This organizes an approach to avoiding security risks posed by embedded devices.
Japan Business Federation (Keidanren)	Declaration of Cyber Security Management	The Declaration expresses the commitment of the business community to contribute to the creation of a safe / secure cyberspace by promoting cybersecurity measures with the participation of all.
	Cyber Risk Handbook for Japanese Corporate Directors	This guide organizes the issues that directors should consider when reviewing / discussing how to address the business risks posed by security threats and presents five principles of cyber risk management.

(ii) Security-related Policies, Guidelines, etc. by Industry and Product

Table B-2 Security-related Policies, Guidelines, etc. by Private sector, Industry and Product

Publisher	Document Name	Overview
Ministry of Economy, Trade and Industry (Study Group for Industrial Cybersecurity)	Guidelines for Cyber Physical Security Measures in Building Systems	This guideline organizes common security measures for all subsystems comprising a building system.

WG1 (Systems, Technologies and Standardization) Building SWG)		
The Japan Electric Association	Guidelines for Power Control System Security	This guideline organizes regulations on requirements for security measures to implemented by electric utilities for the purpose of ensuring cybersecurity of power control systems, etc.
	Guidelines for Smart Meter System Security	This guideline organizes requirements for security measures to be implemented by general transmission and distribution companies for the purpose of ensuring the security of smart meter systems.
Ministry of Economy, Trade and Industry	Cybersecurity Guidelines for ERAB (Energy Resource Aggregation Business)	This guideline organizes guidelines for cybersecurity measures to be taken by operators participating in ERAB.
	Cybersecurity Measures Guidelines for Electric Retail Utilities	This guideline organizes guidelines for retail electricity providers to implement cybersecurity measures appropriate to their business models.
JAMA (Japan Automobile Manufacturers Association, Inc.) and JAPIA (Japan Auto Parts Industries Association)	JAMA/JAPIA Cybersecurity Guidelines	The purpose of this guideline is to promote the improvement of cybersecurity measures and efficient inspection of the level of measures in the entire Automotive Industry.
CCDS (Connected Consumer Device Security Council)	CCDS Security Guidelines for Product Categories Automotive On-board Devices	This guideline summarizes the design and development process that should be considered from design to post-product release to implement appropriate security measures in automotive on-board devices.
	CCDS Security Guidelines for Product Categories Smarthomes	This guideline organizes countermeasure guidelines and security requirements based on the components and life cycle in the smart home field.
	IoT Devices Security Requirements Guidelines	These are the security requirement guidelines commonly applicable to IoT devices which are issued by an industry organization that conducts research and studies on security technologies for critical life devices used in daily life, provides guidelines and certification systems, and examines standardization.

	IoT Devices Security Requirements and Countermeasure Policies Checklist	This is a checklist of countermeasure policies for compliance with the requirements of the Security Requirements Guidelines.
	CCDS IoT device security implementation guideline (software update function)	This guideline organizes Security requirements for the implementation of 'Software Updates' and provides guidance to manufacturers in designing secure IoT devices.
Ministry of Economy, Trade and Industry (Study Group for Industrial Cybersecurity WG1 (Systems, Technologies and Standardization) Smart Home SWG	Guidelines for cyber physical security measures for the safety and security of smart homes	This guideline summarizes the concept of cyber and physical security measures in the smart home and the minimum measures that each stakeholder should consider.
IoT Acceleration Consortium	IoT security guidelines	This guideline summarizes the thinking for considering appropriate cybersecurity measures for IoT devices, systems and services according to risk without specifying the field.
Ministry of Internal Affairs and Communications	Smart City Security Guidelines (Version 2.0)	This is a summary of the concept of smart city security and the security measures recommended to be implemented in order to realize a smart city.
	Telework security guidelines	This guideline summarizes the telework realization method and security measures presented.
Japan Smartphone Security Association (JSSEC)	JSSEC IoT Security Checklist Version 2.1	This checklist comprehensively summarizes the security matters which should be considered by a general company when using (introducing) the IoT.

[Reference] Major guidelines for security incident response

Table B-3 Major Guidelines for Security Incident Response

No.	Publisher	Document Name	Overview, References
1	NIST	SP 800-61: "Computer Security Incident Handling Guide" Revision 2	This guideline organizes policies, plans, procedures, information sharing, systems, and functions / services required for security incident response, and presents procedures (detection, analysis, containment, eradication, recovery, and post-incident activities) and inter-organizational coordination / information sharing details.

			https://www.nist.gov/privacy-framework/nist-sp-800-61
2	Information-technology Promotion Agency, Japan (IPA), NRI Secure Technologies	Computer Security Incident Handling Guide	Japanese translation of 'NIST SP 800-61: "Computer Security Incident Handling Guide" Revision 1'. https://www.ipa.go.jp/files/000025341.pdf
3	JPCERT/CC (Coordination Center)	CSIRT Guide	This guideline organizes the concept of a CSIRT (Computer Security Incident Response Team), roles, structure, inter organizational collaboration, preparation details, and an overview of incident response tasks. https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20211130.pdf
4	JPCERT/CC (Coordination Center)	Incident Handling Manual	This guideline organizes the basic flow of security incident response and presents response details according to typical incident types. https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20211130.pdf
5	JPCERT/CC (Coordination Center)	Internal CSIRT building support material	This guideline organizes the significance and merits of establishing an incident response system and the importance of planning for incident response in advance are explained for the purpose of providing information necessary for planning / building an internal CSIRT. It also summarizes the role model of an internal CSIRT, defines the definition and scope of internal CSIRT activities, and classifies the forms and characteristics of internal CSIRT. And it provides the process of building an internal CSIRT. https://www.jpcert.or.jp/csirt_material/build_phase.html
6	JPCERT/CC (Coordination Center)	Handbook for Computer Security Incident Response Teams (CSIRTs)	Japanese translation of 'Carnegie Mellon University / Software Engineering Institute (CMU/SEI) "Handbook for Computer Security Incident Response Teams (CSIRTs)". This handbook organizes the basic framework of CSIRTs (mission, clients, positioning), functions / services, exchange information, policy formulation methods, and quality assurance methods, and presents the contents of incident response services and organizational operations. https://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf

7	Japan Network Security Association (JNSA), Information Security Operation providers Group Japan (ISOG-J)	Textbook for security response organization (SOC/CSIRT)	<p>This handbook presents the significance of the existence, functions, roles, structure, and maturity of the security response organization (SOC/CSIRT), as well as the necessary human resource skills and training methods.</p> <p>https://isog-j.org/output/2017/Textbook_soc-csirt_v2.1.pdf</p>
8	Information Security Operation providers Group Japan (ISOG-J)	Textbook and Handbook for security response organization (SOC/CSIRT)	<p>This handbook is an easy to understand summary of the content of the 'Security Response Organization (SOC/CSIRT) Textbook' and covers the roles of security response organizations and their maturity models.</p> <p>https://isog-j.org/output/2017/Textbook_soc-csirt_handbook_v1.0.pdf</p>

B-2 Requirements from national and local government

It is necessary to take into account the security requirements of national and local governments when considering / planning security measures for factory systems.

When considering security measures, it is necessary to check whether there are any problems related to existing laws (e.g., Industrial Safety and Health Act, Basic Act on the Environment, etc.) and guidelines.

Security requirements are sometimes stipulated when systems interact with each other, such as when exchanging information with national or local governments via a factory system.

In addition, requirements for security measures for the product itself or for ensuring security in the production system / process of the product may be clearly specified in the procurement standards for products introduced by the national or local government.

B-3 Requirements from industry

Japan Business Federation published “Declaration of Cyber Security Management” to express that the business community will contribute to the creation of a safe / secure cyberspace by promoting cybersecurity measures with the participation of all members, and Japan Business Federation’s “Cyber Risk Handbook for Japanese Corporate Directors” organizes matters to consider when directors consider / discuss measures to deal with corporate management risks caused by security threats and provides five principles of cyber risk management.

[Reference] Requirements by industry

- Electric Power Industry

In the Electric Power Industry, Japan Electrical Technology Standards Committee (JESC), Ministry of Economy, Trade and Industry's Study Group for Industrial Cybersecurity WG1 Electric Power SWG, ERAB (Energy Resource Aggregation Business) Study Group establish Security Guidelines for Power Control Systems, for Smart Meters, and Electricity retailers, for ERAB (Energy Resource Aggregation Business), and Japan Electricity Information Sharing and Analysis Center (JE-ISAC) consists of electric power companies, facilitates security information collection / analysis / sharing, and Security-related initiatives are promoted / required mainly by the Agency for Natural Resources and Energy and The Federation of Electric Power Companies of Japan.

- Automotive industry

In the Automotive Industry, JAMA (Japan Automobile Manufacturers Association) and JAPIA (Japan Auto Parts Industries Association) establish Security Guidelines for Automotive Industry, and J-Auto-ISAC (Japan Automotive ISAC) promotes collection, analysis and sharing of security information. Security-related initiatives are promoted / required mainly by

JAMA (Japan Automobile Manufacturers Association) and JAPIA (Japan Auto Parts Industries Association).

Internationally, the United Nations World Forum on Harmonization of Vehicle Standards (WP29) defines rules for Vehicle Cybersecurity and software updates, which must be approved in accordance with the laws and regulations of each country.

In addition, CCDS (Connected Consumer Device Security Council) establishes Security Guidelines for Automotive On-board Devices.

- Medical Device Industry

In Medical Device Industry, internationally the International Medical Device Regulators Forum (IMDRF) establishes cybersecurity guidance for medical devices, and the Pharmaceutical Safety and Environmental Health Bureau of Ministry of Health, Labour and Welfare requires compliance with the guidance.

In addition, the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices requires medical devices to comply with risk management and security measures based on JIS T14971 (equivalent to ISO 14971).

- Housing Industry

In the housing industry, the Smart Home Subcommittee of JEITA (Japan Electronics and Information Technology Industries Association) and the Ministry of Economy, Trade and Industry's Study Group for Industrial Cybersecurity WG1 Smart Home SWG establish security guidelines for smart homes and promote / require security-related initiatives.

And CCDS (Connected Consumer Device Security Council) establishes Security Guidelines for Smart Homes and operates programs to inspect conformity to the guidelines for Smart Homes and issue a certification mark. This program requires self-inspection or third-party conformity inspection, and the results of the conformity inspection are managed by CCDS.

B-4 Requirements from the market and customers

It is necessary to consider security-related requirements from the Market / Customers when considering and planning security measures for factory systems.

The provision and establishment of standards and guidelines pertaining to the security requirements of industrial control systems is progressing, and in such an environment, the Market / Customers may require security measures in accordance with 'IEC 62443 series of standards' and 'NIST SP 800 series' pertaining to cybersecurity referenced globally, and the security guidelines for each Industry sector by METI.

These Market / Customers requirements can be viewed from the following three perspectives.

- Security for Factory lines

The security requirements prepared with respect to the lines which manufacture the products of the business partners and the systems that cooperate with the business partners may be shown.

- Security for Corporate Behavior such as information management and

security management of factory system

As one of the points to evaluate corporate value, it may confirm whether information management and security management in the factory system has been established⁵⁵.

- Security for Product

It may be confirmed that the software and components used in the product are guaranteed to be free of security issues.

B-5 Requests from client company

Client Company may request security measures f when considering / planning security measures for Factory Systems.

In some cases, Client Company may request security measures for in the production process so that supplied products / parts do not contain unauthorized hardware or software.

B-6 Requests from investors

Investors⁵⁶ may request security measures when considering / planning security measures for factory systems.

⁵⁵ In evaluation of business-to-business transactions, it may be important that necessary security management has been established.

⁵⁶ Investors have come to regard cybersecurity risk as one of the management risks of a company and statement of security measures information is required as risk disclosure in securities reports, internal control reports, CSR reports, etc.

Based on such social demands, the Ministry of Internal Affairs and Communications has also formulated / published the "Handbook on Disclosures of Information on Cybersecurity Measures" to promote the disclosure of information related to cybersecurity measures of private companies.

Annex C Approach to Security Measure Levels in Relevant Documents

C-1 Typical security measure evaluation criteria

Typical security measure evaluation criteria include

- (1) Security level in the IEC 62443 series of standards
- (2) Evaluation criteria in NIST Cybersecurity Framework
- (3) IoT Security Safety Framework (IoT-SSF) (Ministry of Economy, Trade and Industry)

(1) IEC 62443 series of standards

The threat level is evaluated from five perspectives that indicate the degree to which the threat is caused by a skilled attacker. Specifically, the threat is qualitatively evaluated as Level 1-4 in terms of the attacker's malicious intent, means of attack, resources used, skill level, and motivation.

Table C-1 Security Levels in the IEC 62443 Series of Standards (Threat Level)

Level	Malice	Means	Resources	Skill	Motivation
1	Not malicious	—	—	—	—
2	Malicious	Simple	Low	Generic	Low
3	Malicious	Sophisticated	Moderate	IACS-specific	Moderate
4	Malicious	Sophisticated	Extended	IACS-specific	High

For attackers with low security levels, countermeasures are based on the assumption of simple attacks in which many attackers utilize publicly known techniques. On the other hand, an attacker with a high security level is assumed when the countermeasures are designed for an attack by a limited number of people or organizations using sophisticated and complex attack techniques, including internal crimes.

(2) NIST cybersecurity framework

In the U.S. under the NIST (National Institute of Standards and Technology) cybersecurity framework, the level rating is based on management maturity. A low level represents a state of implementation based on individual (or individual organization or project) discretion. A high level indicates that the PDCA management cycle is implemented in a timely manner and the cycle is reviewed.

Table C-2 Security Levels in NIST Cybersecurity Framework

Level	Content	Practical Example
Tier 1	Partial	Partially implemented
Tier 2	Risk Informed	Implemented based on risk assessment
Tier 3	Repeatable	Conduct periodic reviews
Tier 4	Adaptable	Reviewed at each event

(3) METI IoT Security Safety Framework (IoT-SSF)

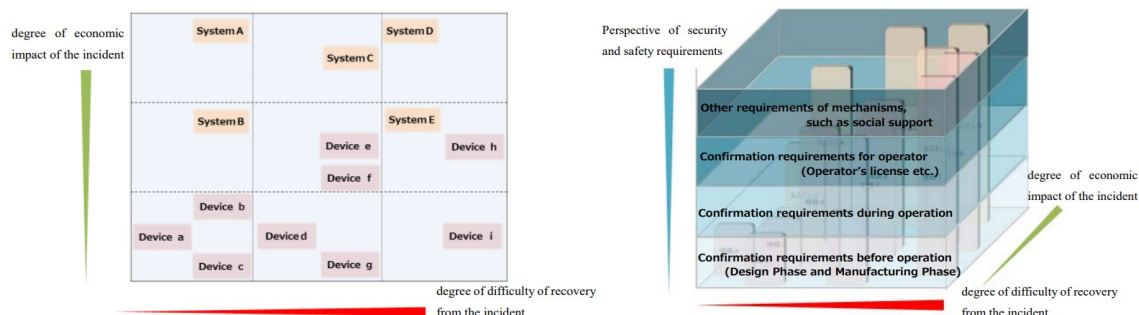
In METI IoT Security Safety Framework, the 'Security and Safety requirement level (risk)' for IoT devices and systems is defined along two axes: 'Axis 1: Degree of difficulty in recovering the impact of an incident that has occurred' and Axis 2 'Degree of economic impact of the incident (in terms of monetary

value)'.

Axis 1 is expressed in three levels: 'Limited damage (easy recovery)', 'Severe damage (not easy recovery)', and 'Fatal damage (Difficult recovery)'.

Axis 2 is expressed at three levels: 'Limited economic impact', 'Significant economic impact', and 'Catastrophic economic impact'.

By mapping the above two axes into a two-dimensional table, the 'Security and Safety requirement level' of systems and equipment can be organized. Furthermore, the perspective of security and safety requirements, which is the third dimension, has set up a framework to examine countermeasures from four perspectives including social support.



Reference) Ministry of Economy, Trade and Industry "IoT Security Safety Framework"

Figure C-1 Image of security and safety requirement perspectives required for each category

Perspective 1: Security and safety verification requirements for equipment and systems connecting the physical and cyber worlds prior to operation (e.g., during the design and manufacturing phases).

Perspective 2: Security and safety verification requirements for equipment and systems connecting physical and cyber during operation.

Perspective 3: Requirements for confirmation of the competence of persons operating and managing equipment and systems.

Perspective 4: Other requirements for social support and other mechanisms.

C-2 Examples of definitions of the extent to which security measures are implemented

The extent to which security measures are implemented should be defined by each party in accordance with the situation of the industry and the individual company, referring to these standards. The key point is to define a level that can be implemented while taking into account the difference between the current situation and the situation of standards and guidelines in the world.

As an example, the extent to which security are implemented is organized by the three perspectives of security measures: 'system', 'operation', and 'management'.

(1) Examples of the extent of measures concerning systems

This is intended to evaluate 'How well the system can be protected from security threats'. Below are examples of the levels to be set. Each business operator is requested to configure the most appropriate level for its own internal use.

Table C-3 Examples of configuration using the IEC 62443 series of standards levels in contrast to security requirement levels

Extent of measures	Corresponding request level	Countermeasures
1	Low	Security Level 1
2	Middle	Security Level 2
3	High	Security Level 3 and 4

Table C-4 Examples of settings for stepwise expansion of targeted threats

Extent of measures	Contents
1	Countermeasures for intrusion from OA systems
2	Countermeasures against external attacks against the control system
3	Countermeasures for internal crimes involving the control system

(2) Examples of the extent of measures concerning operation

The purpose of this is to evaluate 'Whether the OODA process can be smoothly implemented'. The level should be set from the viewpoint of 'How quickly the system can recognize and respond appropriately when a cyberattack occurs'.

Table C-5 Examples of settings focused on the abilities of operators

Examples of ability to respond when problems occur.

Extent	Monitoring	Judgment	Decision	Action
1	Real time detection (Security device)	No stipulation	No stipulation	No stipulation
2	Real time detection (Security device)	Education and training of operators	Development of internal systems	Development of intradepartmental cooperation
3	Real time detection (+ Abnormal business behavior)	Accumulation and utilization of judgment knowledge	Development of decision making system	Development of BCP coordination system

Table C-6 Examples of settings combining complex items

Examples of a complex combination of Operator skills, Organizational knowledge, Information provided to operators, and establishment of mechanisms / structure to support operators.

Extent	Skills	Knowledge	Information		Mechanism / structure	Image
			System	Threats		
1	—	—	—	—	—	Depends on operator skills
2	Education	—	Failure information	—	Procedure available	Organize procedures
3	Training	Training	Security information	—	Develop analytical tools	Goals within the organization
4	Comprehensive training	Accumulation	Security information	obtain	Develop partnerships with external organizations	Compliance with international standards

(3) Examples of the extent of measures concerning management

The purpose of this is to evaluate 'whether optimal reviews are being conducted based on various types of information'. Below are examples of the extents to be set. Each business operator is requested to set the most appropriate configuration for its own internal use.

Table C-7 Examples of use of NIST Cybersecurity Framework levels

Extent	Contents
1	Depends on individual and partially implemented
2	Implemented based on risk assessment
3	Periodically review
4	Confirm changes in risk based on each piece of information from inside and outside the company and review each event

Table C-8 Examples of utilizing management maturity

Utilize CMMI (Capability Maturity Model Integration), which is recognized as a management maturity level.

Extent	Contents
1	Depends on individual
2	Implemented under basic management by organization
3	Implemented based on standard rules in place as an organization
4	Confirm changes in risk based on information from inside and outside the company and review as needed
5	Repeatedly implement the optimized state while making improvements in light of the goals

Annex D Related/Reference Materials

The materials related to the matters stated in this guideline are shown in the list below.

Charter of Trust / Common risk-based approach for the Digital Supply Chain

Ten fundamental principles to foster three important objectives to make the digital world more secure

Edgecross Consortium / User Security Guidelines

Guidelines to ensure safety and security by indicating security points to be considered when constructing FA systems

EU NIS Directive

Rules for the security of networks and information systems aimed at raising the level of cybersecurity in the EU

EU GDPR

General Data Protection Regulation: GDPR

European Union (EU) regulations aimed at ensuring the fundamental human right to protect personal information (data)

IEC 62443

IEC (The International Electrotechnical Commission)

Defines overall security from control system management to systems and components.

It is comprised of several sub-standards, which are still being studied and standardized.

IEC TS 62443-1-1:2009 <https://webstore.iec.ch/publication/7029>

IEC 62443-2-1:2010 <https://webstore.iec.ch/publication/7030>

IEC TR 62443-2-3:2015 <https://webstore.iec.ch/publication/22811>

IEC 62443-2-4:2015 <https://webstore.iec.ch/publication/61335>

IEC TR 62443-3-1:2009 <https://webstore.iec.ch/publication/7031>

IEC 62443-3-3:2013 <https://webstore.iec.ch/publication/7033>

IEC 62443-4-1:2018 <https://webstore.iec.ch/publication/33615>

IEC 62443-4-2:2019 <https://webstore.iec.ch/publication/34421>

ISO/SAE 21434

(For Automobiles)

An engineering standard that defines cybersecurity requirements across the entire vehicle lifecycle.

NIST Cybersecurity Framework (CSF)

A Framework for Improving Critical Infrastructure Cybersecurity.

NIST CSF (Manufacturing Profile) IR 8183

Provides a risk-based approach to managing cybersecurity activities and mitigating cyber risks to manufacturing systems.

NIST SP 800 series

Computer security-related reports published by NIST CSD (Computer Security Division). Documents compiled for use by U.S. government agencies in implementing security measures.

Ministry of Economy, Trade and Industry / Cybersecurity Management Guidelines

Guidelines for promoting cybersecurity measures under the leadership of management for large enterprises and small and medium-sized enterprises (excluding small businesses).

Ministry of Economy, Trade and Industry / Cyber/Physical Security Framework

Summarizes the contents of addressing supply chain security requirements extended by “Society 5.0” and “Connected Industries”.

Ministry of Economy, Trade and Industry / IoT Security Safety Framework -Ensuring the reliability of the connection between physical space and cyberspace-

Summarizes the contents of ensuring the reliability of the connection between physical space and cyberspace in “Society 5.0” and “Connected Industries”.

Ministry of Economy, Trade and Industry / Guidelines for cyber physical security measures in building systems

Summarizes the contents of common security measures for all subsystems that make up the building system. It is helpful as a reference for security measures for common spaces in condominiums and other buildings.

Ministry of Economy, Trade and Industry / White Paper on Manufacturing Industries

White Paper on Manufacturing Infrastructure (White Paper on Manufacturing Industries)

An annual report based on Article 8 of the Basic Act on the Promotion of Core Manufacturing Technology.

Ministry of Economy, Trade and Industry / “Guide for security verification to ensure cybersecurity of devices”**[Separate Volume 1] Detailed Explanation of Threat Analysis and Security Verification, [Separate Volume 2] Explanation of Threat Analysis and Security Verification for Equipment Manufacturers**

This shows the matters that the verification service provider should carry out in the security verification that verifies the security of the device.

Separate volume 1 organizes specific examples of threat analysis and ideas of effective verification methods, and comprehensively and in detail shows the matters and methods that verification service providers should implement.

Separate volume 2 provides verification knowledge, including proactive measures, to manufacturers who develop, manufacture, and sell IoT devices, etc., when the manufacturer becomes a verification requester.

Information-technology Promotion Agency, Japan (IPA) / “Control System Security Risk Analysis Guide-Implementation and Utilization of Risk

Assessment in Security Measures-”

To deepen understanding of the overall picture of risk analysis, to provide procedures and guidance for conducting specific risk analysis, and to provide know-how on risk analysis practiced at IPA.

* This document serves as a reference for examining the importance of protected assets in this guideline.

CCDS (Connected Consumer Device Security Council) / IoT Device Security Requirements Guidelines

Guidelines for security requirements commonly applicable to IoT devices, issued by an industry organization that conducts research and studies on security technologies for critical life devices used in daily life, provides guidelines and certification systems, and examines standardization.

IoT Devices Security Requirements and Countermeasure Policies Checklist

Policy checklist of countermeasures for compliance with the requirements of the Security Requirements Guidelines.

CCDS (Connected Consumer Device Security Council) / CCDS IoT device security implementation guideline (software update function)

Guidelines that provide specific security requirements for implementing “Software Updates” and provide guidance for manufacturers to design secure IoT devices.

CCDS (Connected Consumer Device Security Council) / CCDS Product Sector Security Guidelines Smart Home Edition

Defines specific countermeasure guidelines and security requirements based on components and life cycles in the smart home sector.

CCDS (Connected Consumer Device Security Council) / CCDS Product Sector Security Guidelines On-Board Unit

This guideline summarizes the design and development process that should be considered from design to post-product release to implement appropriate security measures in vehicle equipment.

University of Tokyo Green ICT Project / Edgecross Consortium Joint Factory Security WG / Factory Security Guidelines Overview

Guidelines for the consideration and implementation of security measures for factory FA and other industrial control systems (ICS / OT), organized based on manufacturing / factory values.

Annex E Checklist

The following checklist is provided to give an image of the specific implementation content of the measures indicated in this guideline that we particularly would like you to implement and to enable you to confirm whether those measures have been achieved. The items for confirmation in the checklist are examples for illustration only and it is acceptable for the reader to add or delete items or amend the content of the items in accordance with your own situation.

The achievement level of these items is evaluated according to '1: Not implemented', '2: Partially implemented', '3: Implemented', '4: Implemented, control procedures are documented and automated, and measures are periodically reviewed', and '5: Implemented, control procedures are documented and automated, and reviewed as needed' to check the current status regularly. It is acceptable to use simplified standards for the achievement level in accordance with the situation of the reader.

Table E-1 Checklist⁵⁷

Category	No.	Confirmation item	Achievement	Reference
Preparation	0-1	The management goals, external requirements, and internal requirements / status necessary for considering and planning security measures in factory systems are organized.		3.1.1 Step 1-1
	0-2	The operations and protection targets in factory systems are organized and their levels of importance are set. Based on these results the zones are set and connected with the operations and protection targets, and their impacts with the security threats are organized.		3.1.1 Step 1-2 to Step 1-7
	0-3	Based on the results of collecting and organizing information such as the internal and external requirements concerning factory systems and the operations, protection targets, zones, etc., the security measure policy for the factory system is formulated and the correspondence of security measures against assumed threats is carried out.		3.2 Step 2-1 Step 2-2

⁵⁷ The following terms in the checklist apply to the following in Figure 2-1.

Factory networks: equipment network, production management network, and information network

Networks in the factory: equipment network and production management network

Factory systems: factory networks and connected systems

Systems in the factory: networks in the factory and connected systems

Organizational measures	1-1	The decision maker (factory manager, company manager, etc.) or management is aware of the need for security of factory systems, is in a position to obtain cooperation in terms of sufficient budget and personnel allocation.		3.1.1(3) Organization of internal requirements / situations
	1-2	Cooperation and linkage arrangements are in place between the information system division, production-related divisions, and other relevant divisions and departments to ensure the security of factory systems.		3.1.1(3) Organization of internal requirements / situations
	1-3	The factory system security review organization and the person in charge are prepared, and the responsibilities and business contents are clarified.		3.1.1(3) Organization of internal requirements / situations
	1-4	A business continuity plan (BCP) is formulated, a person in charge in the event of a factory security accident is prepared, and responsibilities and business contents are clarified.		3.1.1(1) Arrangement of management goals, etc. 3.1.1(3) Organization of internal requirements / situations
	1-5	Provide on-site training such as receiving regular information and holding study sessions on trends in threats related to factory security.		3.3(1) Life cycle measures
Operational measures (system related, etc.)	2-1	The risks to the business in the event of a system breach or outage are considered.		3.1.1(1) Arrangement of management goals, etc.
	2-2	Dedicated security policies in the factory system are specified and recognized.		3.1.1(3) Organization of internal requirements / situations
	2-3	E-mail and Internet access from systems in the factory is prohibited by the policy.		3.1.1(3) Organization of internal requirements / situations
	2-4	Responsible person's response to the occurrence of security anomalies in the factory system is clarified.		3.1.1(3) Organization of internal

				requirements / situations
	2-5	On-site workers understand and are trained on how to respond to security anomalies in factory systems.		3.3(1) Life cycle measures
	2-6	A ledger of devices (servers, client terminals, network equipment, facilities, etc.) connected to the factory network is created, including the use of information asset detection tools, and a system configuration diagram is created.		3.1.4 Arrangement of the protection target
	2-7	If a wireless LAN is installed in the factory, a system is in place to create a ledger of devices authorized to connect to the network and reject unauthorized devices.		3.1.4 Arrangement of the protection target 3.2.2(1) Measures for system configuration
	2-8	Attack methods and vulnerabilities which make it possible to infiltrate the system are identified and vulnerabilities are responded to or mitigation measures are taken. (Examples of methods of identifying vulnerabilities: Periodic vulnerability assessments and penetration tests (tests of whether infiltration is possible), ascertaining of the model information and firmware information of embedded devices (PLCs, IoT devices, etc.) and regular confirmations of their vulnerability information, etc. (* 1))		3.2.2(1) Measures for system configuration
	2-9	Stipulation and operation of rules concerning the use and bringing of external storage media (USB memory, flash devices) and portal media into the factory.		3.3(1) Life cycle measures
	2-10	There are rules stipulating the concepts of password settings including password strength and expiration dates for systems in the factory. (Excluding terminals such as display units that		3.2.2(1) Measures for system configuration

		require emergency response related to safety.)		
	2-11	Old accounts (e.g., retirees, transferees, etc.) that are not in use with access rights to systems in the plant are deleted promptly.		3.2.2(1) Measures for system configuration
	2-12	For connected devices in the factory network, there is a procedure to verify in advance that they are not infected with viruses.		3.2.2(1) Measures for system configuration
	2-13	Backups are made with the assumption of complete restoration of system functions, the backup data is stored in a protected location, and tests of restoration from backup data are conducted periodically. In addition, the procedure is clarified.		3.2.2(1) Measures for system configuration
Technical measures	3-1	Anti-virus software or application white lists (permit lists) are installed on terminals where anti-virus measures can be installed, and some alternative measures (e.g., USB-type anti-virus) are installed on terminals where installation is not possible.		3.2.2(1) Measures for system configuration
	3-2	Security patches are applied as promptly as possible to serious vulnerabilities of the application / operating system (OS). Or alternative measures are in place.		3.2.2(1) Measures for system configuration
	3-3	Services and applications using the terminal operating system (OS) are kept to the minimum necessary, and unused services and ports are stopped or disabled.		3.2.2(1) Measures for system configuration
	3-4	Sufficient measures, such as level classification, are taken for physical access to important factory equipment (examples: surveillance cameras, warning systems). Or alternative operational measures are in place such as access control and escort of relevant personnel to outside visitors.		3.2.2(2) Physical measures

	3-5	Within the factory network, network segment management is conducted according to security level (e.g., VLANs).		3.2.2(1) Measures for system configuration
	3-6	Protective measures such as authentication (e.g. two-factor authentication, etc.), restriction of connectable devices ^(*) for each remote user, restriction of the times when connection is allowed, detection of abnormalities such as device connection outside maintenance periods, etc., and network intrusion protection are taken when external Internet access is possible for the purpose of remote maintenance of factory systems, etc.		3.2.2(1) Measures for system configuration
	3-7	A network detection / protection system is in place to identify suspicious communications on networks in the factory (including the boundary with the information system and remote access).		3.2.2(1) Measures for system configuration
	3-8	Event logs of logins, operation histories, etc. of systems in the factory are collected. Those logs are periodically analyzed or stored for the required number of days.		3.2.2(1) Measures for system configuration
Factory System Supply Chain Management	4-1	A liaison and coordination system has been established with control system vendors and construction companies to respond to security incidents in factory systems.		3.3(2) Supply chain measures
	4-2	Conducting security training for subcontractors involved in factory system maintenance, etc. at the time of contract commencement and regularly.		3.3(2) Supply chain measures
	4-3	A system for communication and coordination with control system vendors / builders is in place to ensure that information is shared promptly when security vulnerabilities related to		3.3(2) Supply chain measures

		delivered factory systems are discovered.		
	4-4	Aware of threats to factory systems in the supply chain (subcontractors, production subsidiaries, etc.), the degree of impact, and the status of response (e.g., implementation of internal and / or external audits, etc.).		3.3(2) Supply chain measures
	4-5	Has a process to determine whether the factory system equipment to be delivered meets certain security standards ⁵⁸ , and an acceptance inspection.		3.3(2) Supply chain measures
	4-6	Security requirements are clarified in the design specification requirements for new system implementation.		3.3(2) Supply chain measures

(*1) As a consequence of the spread of telework, the number of cases in which VPNs are used to connect to an internal network from outside is increasing, but in recent years cyberattacks which exploit vulnerabilities in VPN equipment have been seen continuously. Many of these vulnerabilities are vulnerabilities which were revealed in the past, and they have resulted in a large amount of damage despite the fact that the status of the countermeasures is published by the vendors, so it is important to collect and identify vulnerability information in the equipment and systems of factories you are using yourself and respond in a timely manner.

(*2) It is desirable to confirm whether the soundness of a connected device has been secured before permitting access.

⁵⁸ The anticipated security standards with respect to delivered factory system equipment are whether it is possible to change the default settings (ID, password, etc.) of the equipment, whether or not there are software update functions, whether the authentication information, etc. is stored safely, whether the minimum operational continuity and a smooth recovery are possible when a failure occurs, whether the data can be erased at the time of disposal, etc.

Annex F Procurement Specification Template (Examples)

For building a secure factory, it is important to present security requirements to suppliers in advance when procuring products and services to be used in the factory, and to conclude a procurement contract on that basis. There are three major categories of security requirements that should be considered when procuring products and services.

- (1) Supplier's security management system
- (2) Security measures for products and services
- (3) Security measures related to the life cycle of products and services
 - (i) Security measures during engineering and development
 - (ii) Security measures related to the supplier's supply chain
 - (iii) Security measures during manufacturing and distribution
 - (iv) Security measures related to maintenance, service, and disposal

Of these, (1) is the kind of content that is added as a screening item at the time of vendor registration for purchasing and is from the perspective of whether the vendor can be trusted as a business partner, apart from the procurement of individual products. It can be regarded as part of the credit screening managed by purchasing. As evaluation indicators, depending on the size of the target supplier and the importance of the product sought, there are the Guidelines for Information Security Measures for Small and Medium-sized Enterprises (IPA), Cybersecurity Management Guidelines (METI, IPA), ISO / IEC 27001 (Information Security Management System), and so on.

Example 1: Examples of Security Requirements for Control Equipment Suppliers

X.X Security requirements to be provided by the supplier

Self-assessment of Information Security Measures Guidelines for SMEs, 3rd Edition (IPA) and declaration of a two-star SECURITY ACTION.

Also (2) and (3) are individual security requirements for products / services procured from suppliers. (2) is the security requirements that the product / service should have. For example, if the equipment is used in a factory, the security functions required for the equipment should be enumerated according to the security level to be achieved, such as access control based on authority, login authentication, etc.

Example 2: Examples of Security Requirements in PLC Procurement Specifications

X.X Implement penetration testing

Implement penetration testing using publicly available vulnerabilities and attack methods to reduce security risks.

Control equipment such as PLCs may not have the physical resources to implement security features. In such cases, it is important to obtain information from suppliers to clarify the requirements the equipment to be procured meets, and the requirements and implementation methods that require additional measures. By doing so, flexible choices can be made, such as temporary risk acceptance, based on an understanding of the risks.

With respect to publicly available vulnerabilities and attack methods, there are cases in which the confirmation is possible with desktop study even without implementing penetration testing. Furthermore, even during use of the control equipment after it has been delivered, it is important to present draft measures and mitigation measures to reduce security risks with respect to the detected vulnerabilities and attack methods.

Next, (3) is the security requirements for the product / service lifecycle. These requirements are designed to reduce security risks that occur during the lifecycle of products and services, including development, manufacturing, distribution, operation, and disposal. Depending on the equipment to be procured, some of these requirements may not be required, so you are requested to sort and select the requirements if necessary.

Example 3: Examples of Security Requirements for PLC Product Lifecycle

X.X Security Requirements during Development

X.X.1 Development Environment

X.X.1.1 Development staff management

X.X.1.2 Physical security of the development environment

X.X.1.3 Security measures for development environment

X.X.1.4 Development Software Management

X.X Security Requirements for OSS Used

X.X.1 Implementation of License Management

X.X.2 Implementation of Vulnerability Management

X.X Security Requirements during Manufacturing / Distribution

X.X.1 Security during Distribution

Record maintained of what distribution route was used to deliver the product from the manufacturing site.

Take measures to prevent tampering with equipment, such as opening stickers.

X.X Security requirements for maintenance and disposal

X.X.1 Firmware update at version change

X.X.2 Response when vulnerabilities are discovered

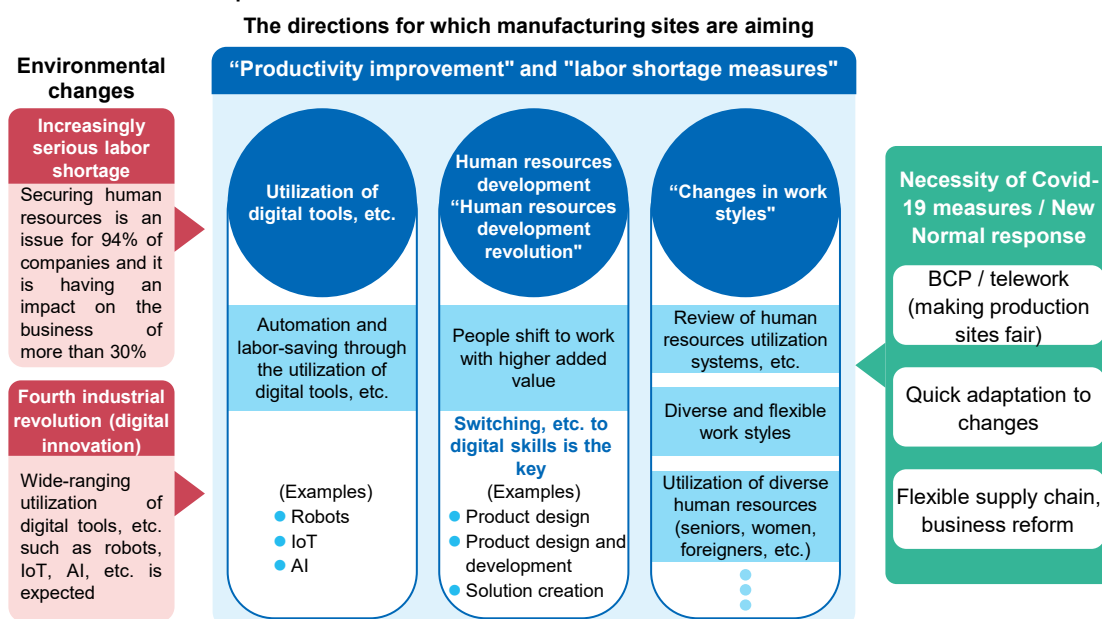
X.X.2.1 Report

X.X.2.2 Action

Column 1: Trends in security of factories

(1) Environmental trends surrounding the manufacturing industry / factories

Manufacturers / factories are under constant pressure to improve productivity and pressed to take measures to cope with the recent labor shortages and changes in work styles. Moreover, the need to respond to Covid-19 (the new coronavirus infection) measures and the New Normal (Lifestyle) has intensified this trend, so telework including production sites for business continuity, rapid adaptation to environmental changes, a flexible supply chain, and business reform, etc. are required.



Reference) Created based on the Ministry of Economy, Trade and Industry "2018 White Paper on Manufacturing Industries"

Figure I-1 Environmental trends surrounding the manufacturing industry / factories (1/4)

On the other hand, in the era of the 4th Industrial Revolution globally, it is necessary from the perspective of global competition to promote the realization of Cyber-Physical Systems (CPSs) that integrate cyberspace (computer networks) and physical space (control systems and devices on factory floors), analyze big data collected from physical space using artificial intelligence (AI), and feedback the results to physical space.

Examples of the realization of cyber-physical systems (CPSs) have various purposes such as automation of the production process to improve productivity, real-time feedback of inspection data analysis results to improve product quality, direct, fast and precise feedback of customer needs from sales / maintenance / after-sales service to product planning / design / production, and eliminating delays in supply-demand adjustment between sales and production and between production and parts purchasing for inventory optimization.

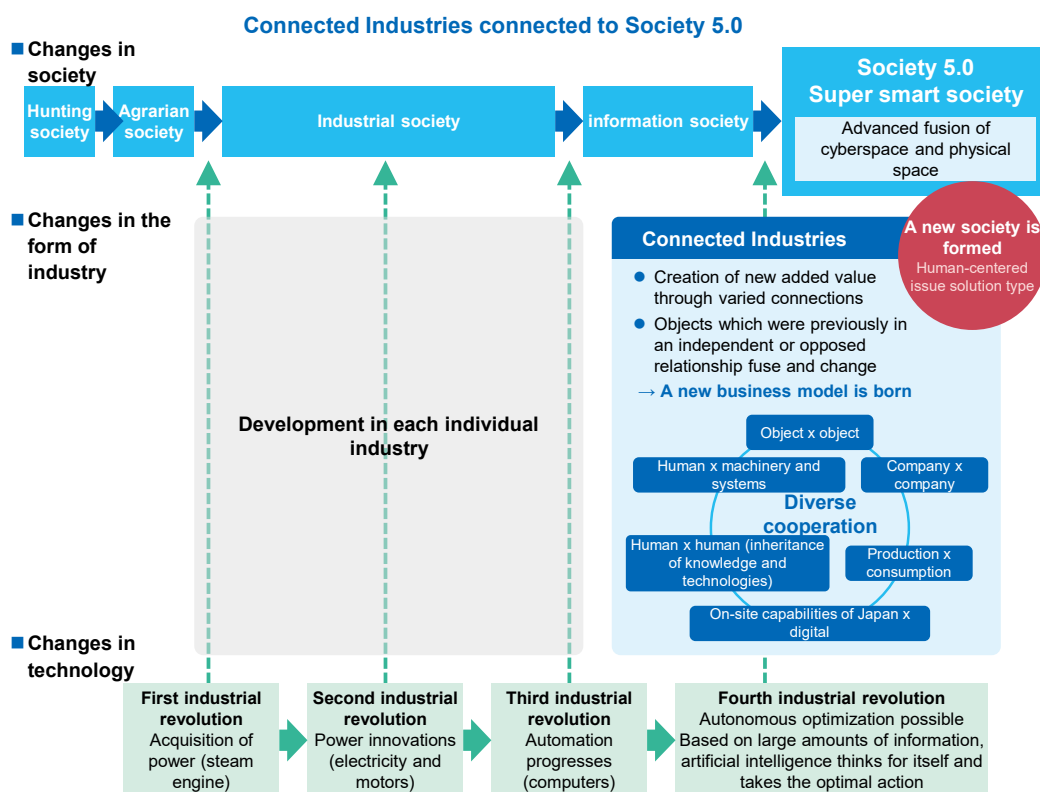


Figure I-2 Environmental trends surrounding the manufacturing industry / factories (2/4)

The arrival of "Society 5.0" with an advanced fusion of cyberspace and physical space

- Japan is proposing the realization of a super smart society called **"Society 5.0"** which provides goods and services meticulously responding to diverse needs and combines economic development with the solution of social issues through an **advanced fusion of cyberspace and physical space**.
- In **"Society 5.0"** the forms of the series of activities for creating added value (the supply chain) are changed to more flexible and dynamic forms. Supply chains with these new forms are defined as **value creation processes**.
- On the other hand, due to the fusion of cyberspace and physical space, the threat of cyberattacks is growing.

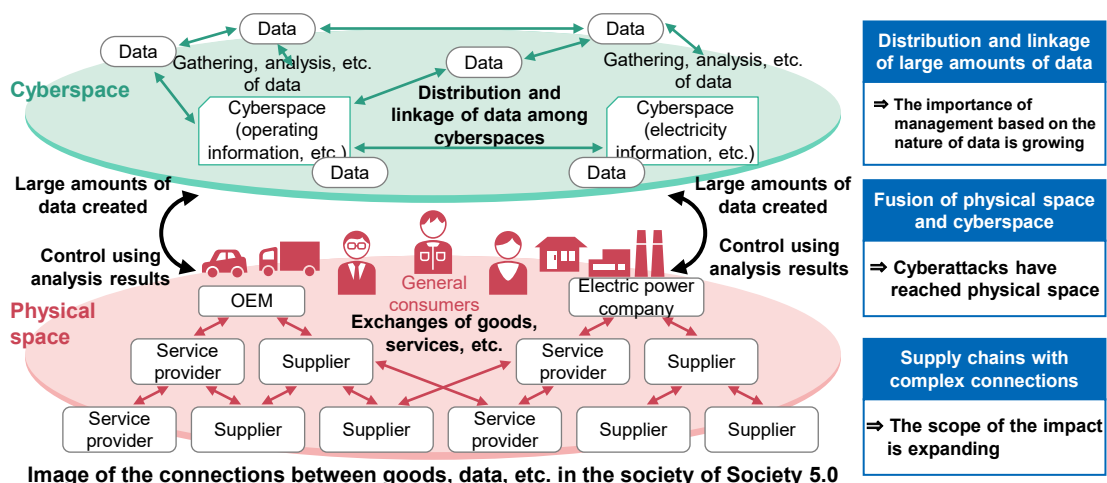


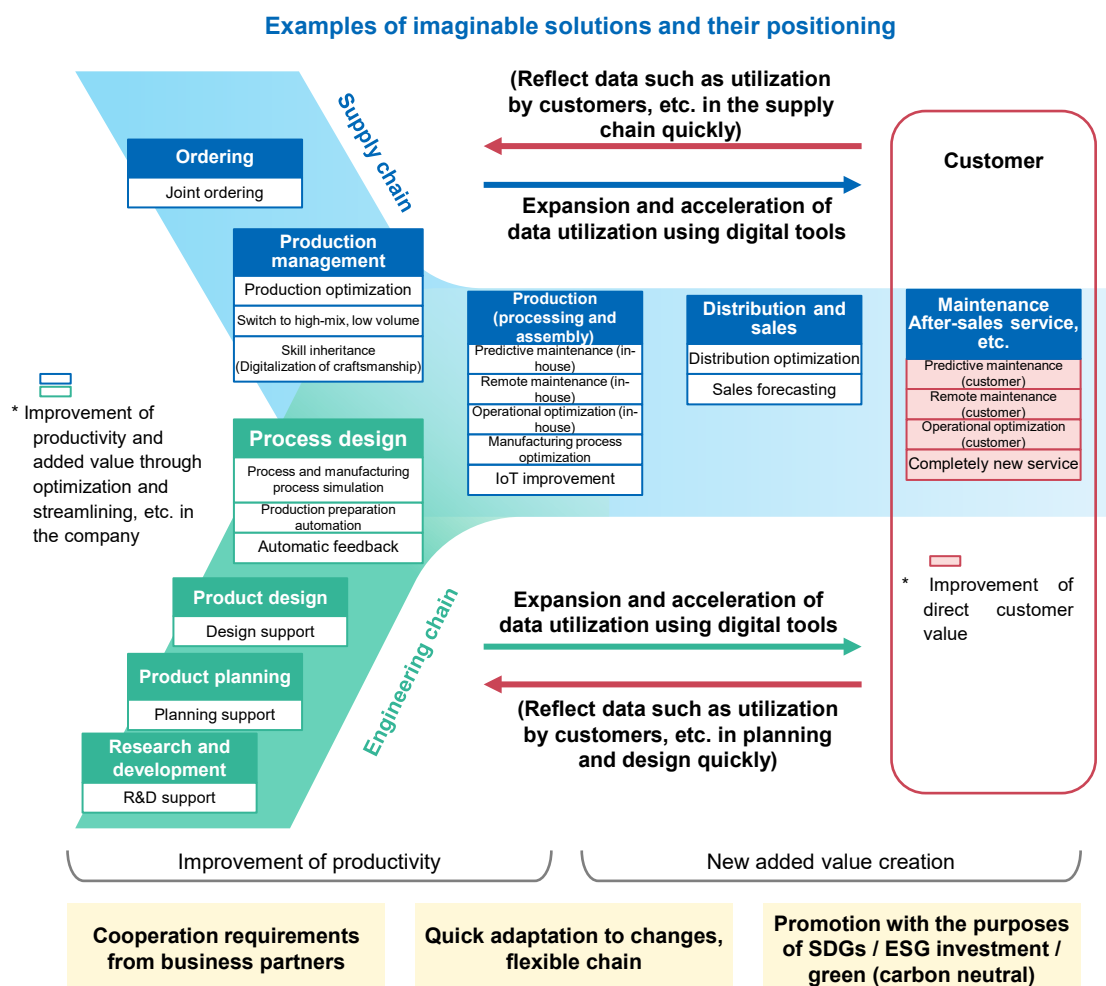
Image of the connections between goods, data, etc. in the society of Society 5.0

Reference) Created based on the Ministry of Economy, Trade and Industry "2018 White Paper on Manufacturing Industries"

Reference) Ministry of Economy, Trade and Industry "Cyber/Physical Security Framework"

Figure I-3 Environmental trends surrounding the manufacturing industry / factories (3/4)

This Cyber-Physical fusion is not confined to a single factory, but covers the Engineering chain, Supply chain and even the linkage of the Value chain which requires collaboration from business partners and the realization of dynamic and flexible chains. The promotion of CPS realization and digital transformation (DX) for the purpose of SDGs / ESG investment / Green (Carbon Neutral) is also becoming more important.



Reference) Created based on the Ministry of Economy, Trade and Industry “2020 White Paper on Manufacturing Industries”

Figure I-4 Environmental trends surrounding the manufacturing industry / factories (4/4)

(2) Trends in the Environment Related to the Security of Industrial Control Systems in Factories

Security risks for Factory systems have been increasing since around 2010, with cyberattacks (attacks compromising system security) targeting industrial control systems and resulting serious damage such as production stoppages / damage to facilities occurring frequently. Looking at the percentage of attacks against control system-related networks using ransomware, in 2018 the percentage generally stayed below 2% each month, but in 2020 it often exceeded 4%, and in some months it exceeded 10%. (“Ransomware in ICS Environments – Dragos 2020”)

For example, ransomware (a type of malicious software) that has become popular in recent years is increasing the number of cases of damage such as factory shutdown. In August 2018, at a major overseas semiconductor manufacturing company, about 10,000 PCs in the factory were infected with malware, and operations were suspended, resulting in an opportunity loss of about 19 billion yen⁵⁹. In addition, in March 2019, at a major overseas aluminum manufacturing company, the production control system in the information system was infected with ransomware, the operations at the manufacturing bases, including overseas bases, were temporarily suspended, and its financial damage amounted to billions of yen⁶⁰. In this way, as the cooperation between factory systems and information systems deepens, the actual situation is that the effects of cyberattacks extend to the operation of factories.

There are two major factors that cause this situation.

- (i) The factory's industrial control system / equipment is vulnerable and lacks security measures, making it vulnerable to cyberattacks.
- (ii) The attacker's motive is suitable for the industrial control system / equipment of the factory.

The attacker considers that the attack effect is high enough for the victim to take the impact of the attack seriously, and the more vulnerable the attack target is, the easier it is to aim for easy success in the attack, but it is the industrial control system / equipment of a factory that balances these.

Many factories think that “it is okay because the industrial control system / equipment of our factory is not connected to the Internet or internal LAN (network)” or “it is okay because it does not communicate with the external network”. However, even if the system / device is not physically directly connected to an external network such as the Internet or company LAN (or the system / device does not communicate with the external network), the reality is that it is indirectly connected via the factory employees or the maintenance personnel of the system / equipment vendors and it can suffer damage due to cyberattacks. In addition, unauthorized operations and negligence by factory employees are increasingly leading to security problems.

In the case of ransomware infection of a major semiconductor manufacturing company mentioned above, the infection spread due to connecting to the network in the factory without virus scanning of a tool brought into the factory due to internal negligence⁶¹.

As just described, due to these increasing security risks in factories, an increasing number of suppliers and product users in the U.S., Europe, and elsewhere are demanding security measures for factory products and manufacturing processes, and Standards and Guidelines are being developed to serve as criteria for such measures.

⁵⁹ “Control system-related cyber incident cases 6-2018 Suspension of operations of a semiconductor manufacturing company due to ransomware” (Information-technology Promotion Agency, Japan) <https://www.ipa.go.jp/files/000085317.pdf>

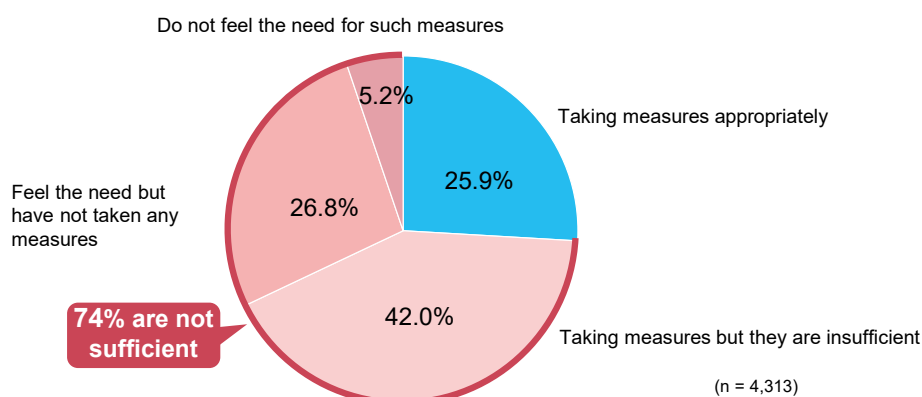
⁶⁰ “Control system-related cyber incident cases 5-2019 suspension of operations due to ransomware” (Information-technology Promotion Agency, Japan) <https://www.ipa.go.jp/files/000080702.pdf>

⁶¹ “Control system-related cyber incident cases 6-2018 Suspension of operations of a semiconductor manufacturing company due to ransomware” (Information-technology Promotion Agency, Japan) <https://www.ipa.go.jp/files/000085317.pdf>

(3) Trends in the Implementation of Security Measures for Industrial Control Systems in Factories

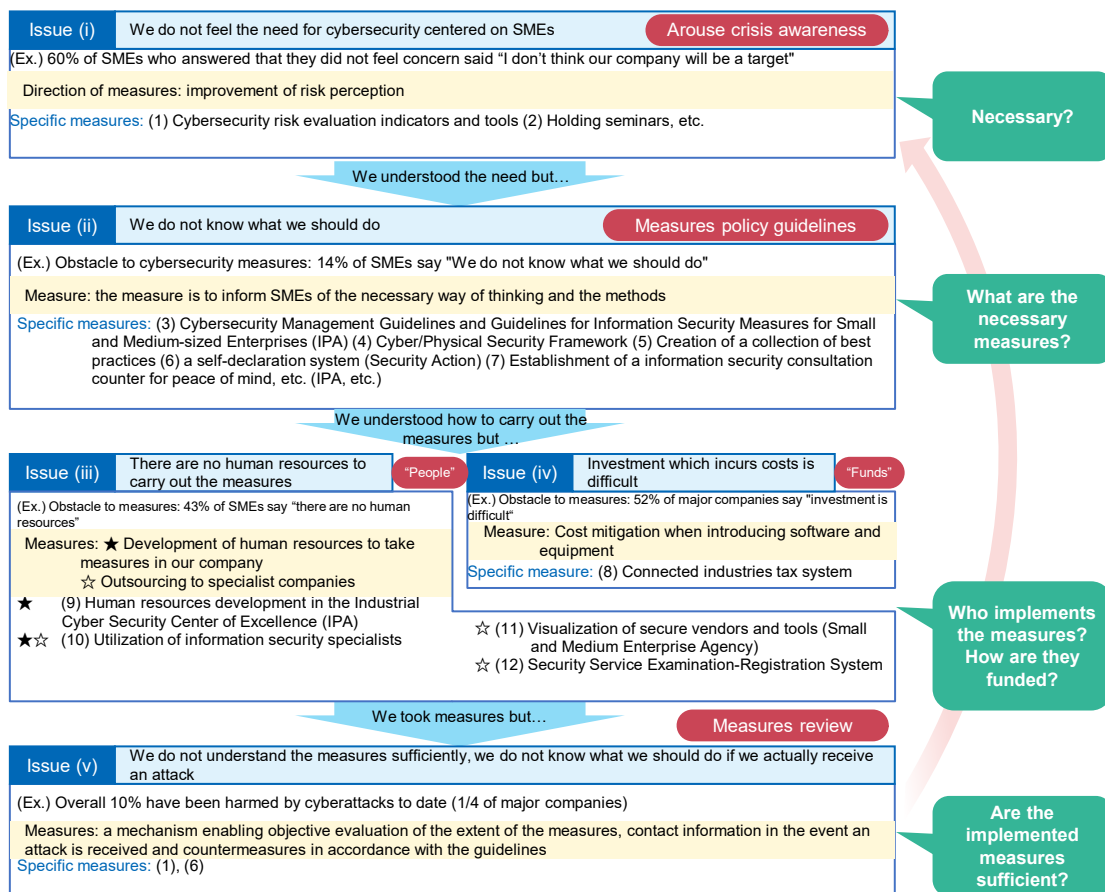
According to the Ministry of Economy, Trade and Industry's '2018 White Paper on Manufacturing Industries', the reasons that the implementation of security measures in factories is not progressing can be divided into four stages.

- (i) Mainly many small and medium-sized companies are at the stage where they do not properly recognize / understand the necessity of security measures for industrial control systems / equipment in factories.
- (ii) Many companies are at the stage of not knowing what kind of measures are necessary.
- (iii) Many companies do not have the skilled human resources and budget to implement the necessary measures.
- (iv) At the stage where it is not clear whether the measures implemented are sufficient or not, or do not know what to do if the measures are insufficient and the company is a victim of a cyberattack.



Reference) Created based on the Ministry of Economy, Trade and Industry "2018 White Paper on Manufacturing Industries"

Figure I-5 Status of security measures in manufacturing / factories



Reference) Created based on the Ministry of Economy, Trade and Industry "2018 White Paper on Manufacturing Industries"

Figure I-6 Status of security measures in manufacturing / factories

Column 2: Security seen in terms of the purpose of the factory system and value of the manufacturing industry / factory

(1) Security seen in terms of the purpose / function of the factory system itself, product business expansion / continuation, and on-time delivery

A factory system is a system for increasing productivity, reducing costs (C: Cost) and producing products stably and continuously in order to achieve growth of the products business and continuity of the business / production (BC: Business Continuity), and its stable and continuous operation is required. In other words, availability of the system and its components is required. This is also necessary to meet deadlines and prevent delays (D: Delivery). Some security threats may damage availability, and security measures are required to prevent / control them. In other words, security measures are needed to prevent / control security threats from preventing product business growth / continuity (BC), for on-time delivery / delay prevention (D) and for cost reduction (C).

(2) Security seen in terms of Factory Safety and Product Quality assurance

To ensure factory safety (S: Safety) and product quality (Q: Quality), factory systems and equipment must be kept in a state of normal operation. In other words, integrity of systems and equipment functions / controls is required. Security threats include those which compromise functional / control integrity, and security measures are needed to prevent / control them. In other words, security measures are necessary to prevent / control security threats from interfering with plant safety (S) and product quality (Q).

(3) Security seen in terms of ensuring normal operation of Factory Systems and proper feedback control

For factory systems and equipment to maintain normal operation, the data that sets and instructs how to function and control the systems and equipment must be correct, i.e., the data must not be corrupted or falsified. In other words, the Integrity of the setting and instruction data related to the function and control of the system and equipment is required. In addition, for the purpose of optimizing / automating / autonomizing the control / operation / management of factory systems and equipment, feedback control according to the operating status of the systems and equipment must be realized, and therefore it is necessary to collect / analyze / monitor data related to the operating status of the system and equipment, and to realize operations that change settings / instructions related to the way the system and equipment functions / is controlled based on the current status. For this loop to function correctly, the data to be collected from the system and equipment must be correct, i.e., the data must not be corrupted or falsified. That is to say, the Integrity of data collected from systems and devices is required. Some security threats may damage the integrity of data, and security measures are required to prevent / control them. In other words, security measures are needed to prevent / control security threats from preventing the normal operation of factory systems and equipment and the realization of proper feedback control.

(4) Security seen in terms of protecting information and data related to products and production

For Product business, preventing competitors from imitating the advantages of your own company's products to ensure differentiation and competitive advantage is important, and it is necessary to prevent information and data related to products and production (know-how) from being leaked to outside parties.

In other words, confidentiality of information and data related to products and production is required. Some security threats may damage the confidentiality of data, and security measures are required to prevent / control them.

In other words, security measures are required to prevent / control external leakage of information and data related to products and production (know-how) due to security threats.

(5) Security seen in terms of product security quality assurance and manufacturing responsibility

Recently, in the process of manufacturing a product in a factory, the hardware and software used as components of the product may sometimes unintentionally contain unauthorized items containing security threats, and the security threats contained in the product after product shipment may cause problems such as unauthorized use and control of the product from outside parties, obstruction of the operation of the product, and leakage of information of the product user to outside parties. In order to ensure no one will be held responsible for the manufacture of the products, security measures must be taken in the factory production process for the products to prevent the inclusion of such unauthorized hardware and software components in the positioning of the quality assurance (Q) of products. In other words, product components must be free of malicious functions (Malware) and the Integrity and Authenticity of the components is required. Some security threats may damage the Integrity and Authenticity of products and components, and security measures are required to prevent / control them.

In other words, security measures are needed to prevent / control unauthorized use or control of the product by outside parties due to security threats unintentionally contained in the product components, to prevent / control interference with the operation of the product, and to prevent / control leakage of product users' information to outside parties, in order to ensure no one will be held responsible for the manufacture of the products.

Column 3: Flow to smart factories

Factory systems are aiming for further progress in the future, and there is a growing need to improve lines / Equipment facilities and link them to various systems using the latest ICT (Information and Communication Technology) and automation technologies such as robots, as well as remote monitoring / control and production management systems for equipment, increasing opportunities for factory systems to connect to information systems and the Internet, and for cooperation with other companies, other offices, and other bases, but also creating new risks.

This section describes the flows of the four usage forms and the points which must be taken into consideration pertaining to the security risks associated with each.

(1) Lines / facilities improvement

Robots and automatic equipment are introduced to improve the flexibility of the line and to reform production.

Robots and automated equipment often have calculators built into the equipment, and in addition, they are often connected externally using open wireless communication technologies such as wireless LANs, which may pose new risks.

Figure III -1 Expansion of FA control system usage forms

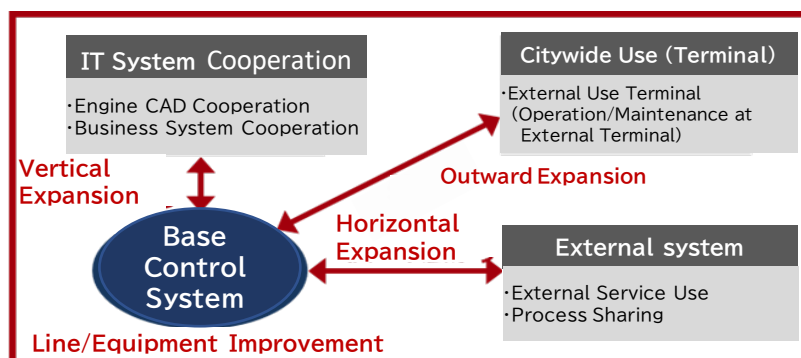


Table III-1 Examples of risks associated with Lines / Equipment Facilities

Events for which consideration is required	Risk
Built-in computer in the device	<ul style="list-style-type: none"> • There is the same risk as a computer
Use of a wireless LAN, etc. to cooperate with outside parties	<ul style="list-style-type: none"> • Expanded risk of external network connection.

(2) Cooperation with IT systems (vertical expansion)

This is a format which cooperates with the analysis system of the engineering department for the purpose of production reform based on on-site data, etc. Also Factory systems are improved based on the analysis results.

Table III-2 Examples of risks associated with IT system cooperation

Event for which consideration is required	Risk
Connect FA system and OA system networks.	<ul style="list-style-type: none"> Expanded mutual risk due to differences in security measures between OA and FA systems.
Data from FA system exists in OA system.	<ul style="list-style-type: none"> Expanded risk of information falsification / leakage due to different system user management.

(3) Use in the city (expansion to the outside)

This is a format in which factory systems are monitored, controlled, and maintained by connecting to on-site equipment via remote access or mobile terminals.

Table III-3 Examples of risks associated with use in the city

Event for which consideration is required	Risk
Connection via external network	<ul style="list-style-type: none"> Attacks from external networks.
Use of external equipment	<ul style="list-style-type: none"> Insufficient management of equipment used Insufficient user management

(4) External system cooperation (horizontal expansion)

Cooperate with the production lines and systems of other companies (other offices and other bases) to build and cooperate with an integrated factory system that includes other companies.

Table III-4 Examples of risks associated with external system cooperation

Event for which consideration is required	Risk
Different security policies	<ul style="list-style-type: none"> Possible attacks due to differences in acceptable risk.
Response in the case that there has been impact due to Cyber-Attacks	<ul style="list-style-type: none"> Smooth coordination of security operations (OODA process) is difficult. Unclear scope of responsibility.

Column 4: Use of the cloud in factories

As a consequence of the growing need for remote maintenance and the progress of data utilization in factories, there are cases of construction of a route which can connect directly to the Internet from the control zone or production control zone without going via the OA zone. These connections pose risks such as unauthorized intrusion and malware infections, etc. via the Internet, so mechanisms for monitoring the systems and networks are necessary in each of the zones.

In addition, in the case of carrying out data accumulation, analysis operations, etc. with an external cloud, it is necessary to consider security measures when using the cloud.

The matters stated in “Information Security Management Guidelines for Using Cloud Services” (Ministry of Economy, Trade and Industry) serve as a useful reference for the security measures necessary when using cloud services. When using cloud services, it is necessary to understand the scope of service provision and scope of responsibility of the “cloud services provider” and then take the security measures necessary as a “cloud services user.” In particular, among the risks in cloud services, the maximum acceptable outage time, the incident response, the business continuity of the cloud business operator itself, etc. should be considered as points pertaining to the business of factory systems.

Council of this Guideline

Study Group for Industrial Cybersecurity WG1 (Systems, Technologies and Standardization) Factory SWG members

* Honorific titles omitted, in alphabetical order

Akihiko Iwasaki	Senior Manager for Security Japan Electronics and Information Technology Industries Association
Chair Hiroshi Esaki	Professor Graduate School of Information Science and Technology The University of Tokyo
Hiroshi Sasaki	Director OT Business Development Division Fortinet Japan G.K.
Hirotsada Takahashi	Senior Manager OT Security Business OT Product Management Group Trend Micro Incorporated
Ichiro Murase	Executive Director Technology Research Association Control System Security Center
Kenji Watanabe	Professor Nagoya Institute of Technology Department of Architecture, Civil Engineering and Industrial Management Engineering
Koichi Saita	Manager IT Division Information Systems Department 5th Section FANUC Corporation
Masahiko Kuwata	Senior Professional Software Advanced Technologist (Cyber Security) Digital Network Division (& Cyber Security Business Department Technology Services Division, & Smart Edge Division,) NEC Corporation
Masue Shiba	Chief Specialist Cyber Security Technology Center Toshiba Corporation (Industrial Security Action Group Robot Revolution & Industrial IoT Initiative (RRI))
Takeo Enomoto	Member of the Electrical and Safety Standards Committee Technical Committee Standardization Committee Japan Machine Tool Builders' Association (JMTBA) (Manager, Nagoya Works Drive System Department Mitsubishi Electric Corporation)
Takeshi Fujiwara	Vice General Manager Machine Tool Control Development Division Connectivity Department DMG MORI B.U.G CO.,LTD.
Toshihiko Nakano	Evangelist

	Control Platform Management Division Omika Office Security
	Hitachi, Ltd.
Yuji Ichioka	General Manager
	Software Systems Division, Nagoya Works,
	Mitsubishi Electric Corporation (*FY2022 onward)
(Hiroshi Nishiyuki	General Manager
	FA System Solutions Department
	Mitsubishi Electric Corporation (*Until FY2021))
Yutaka Matsubara	Associate Professor
	Nagoya University Graduate school of informatics

Acknowledgments

This guideline was created with reference to the items to be considered by the University of Tokyo Green ICT Project-GUTP, Edgecross Consortium Joint Factory Security WG, and the contents of “Factory Security Guidelines Overview”. Thank you for your cooperation.