

The Cyber/Physical Security Framework (DRAFT)

To ensure trustworthiness of a new type of supply chain in “Society 5.0”,
so-called “value creation process”

Version 1.~~10~~

Cybersecurity Division and Digital Economy Division

Commerce and Information Policy Bureau

Ministry of Economy, Trade and Industry

October~~Apr.~~ 23~~18~~, 2026~~19~~

Revision History

The revision history of the Cyber/Physical Security Framework is described below.

<u>Revision date</u>	<u>Revision details</u>
<u>April 18, 2019</u>	<u>Issued Version 1.0</u>
<u>Month X, 20XX</u>	<u>Revised to Version 1.1</u>

Background to the Revision

Approximately seven years have passed since the publication of the CPSF, and some of its measure requirements and examples no longer adequately reflect the latest cybersecurity trends.

Therefore, in this fiscal year, the CPSF has been revised primarily in Part III (Method) and the Appendices, taking into account the latest major international standards.

Risk treatment effective against new risks arising from the expanded use of AI will be considered from the next fiscal year onward, taking into account progress and trends in the development of international frameworks.

The Innovation Platform Agency, Japan (IPA) provided technical support for this revision.

Table of contents

Executive Summary	I
Introduction.....	3
1. Society realized by “Society 5.0” and “Connected Industries”.....	3
2. Increase of threats by cyberattacks.....	5
3. Intention of developing the Framework and its scope of application	6
4. Intended readers of the Framework.....	7
5. Overall structure of the Framework	8
6. Expected effects and features of the Framework	9
7. How to use the Framework.....	10
Part I (Concept): Industrial cybersecurity for connected cyber and physical systems	13
1. Efforts for “value creation process,” a “Society 5.0” supply chain in an industrial society where cyberspace and physical space are highly integrated	13
2. Model for establishing the basis for trustworthiness to ensure security in the value creation process: The three-layer and the six elements	14
2.1. Significance of the three-layer approach	17
2.2. The six elements	20
3. Identifying the risk sources in the value creation process and its policy.....	22
4. Concepts of securing trustworthiness based on the Framework	24
5. Conclusion	26
Part II (Policy): Identification of risk sources and measure requirements.....	27
1. How to proceed with risk management that considers three-layer model and six elements.....	27
1.1. Specifying the target of analysis (applying to the three-layer model).....	30
1.2. Anticipating security incidents and their impact.....	40
1.3. Analyzing risks	45
1.4. Managing risks	46
2. Relationship between risk sources and measure requirements.....	54
Part III (Method): Security measures – requirements and examples.....	57
1. Risk management using security measure requirements and examples of security measures	57
2. How to use examples of security measures	61
3. Security measure requirements	64
3.1 CPS.GV – Govern	69
3.2 CPS.ID – Identify	79
3.3 CPS.PR – Protect.....	86
3.4 CPS.DE – Detect.....	95
3.5 CPS.RS – Respond.....	99
3.6 CPS.RC – Recover.....	104
Executive Summary.....	I
Introduction.....	3
1. Society realized by “Society5.0” and “Connected Industries”.....	3

2. Increase of threats by cyberattacks	5
3. Intention of developing the Framework and its scope of application	6
4. Intended readers of the Framework	7
5. Overall structure of the Framework	8
6. Expected effects and features of the Framework	9
7. How to use the Framework	10
Part I (Concept):— Industrial cybersecurity for connected cyber and physical systems	13
1. Efforts for “value creation process,” a “Society5.0” supply chain in an industrial society where cyberspace and physical space are highly integrated	13
2. Model for establishing the basis for trustworthiness to ensure security in the value creation process: The three-layer and the six elements	14
2.1. Significance of the three-layer approach	17
2.2. The six elements	20
3. Identifying the risk sources in the value creation process and its policy	22
4. Concepts of securing trustworthiness based on the Framework	24
5. Conclusion	26
Part II (Policy):— Identification of risk sources and measure requirements	27
1. How to proceed with risk management that considers three-layer model and six elements	27
1.1. Specifying the target of analysis (applying to the three-layer model)	30
1.2. Anticipating security incidents and their impact	40
1.3. Analyzing risks	45
1.4. Managing risks	46
2. Relationship between risk sources and measure requirements	54
Part III (Method):— Security measures—requirements and examples	56
1. Risk management using security measure requirements and examples of security measures	56
2. How to use examples of security measures	60
3. Security measure requirements	63
3.1 CPS.GV—Govern	66
3.2 CPS.ID—Identify	74
3.3 CPS.PR—Protect	78
3.4 CPS.DE—Detect	85
3.5 CPS.RS—Respond	88
3.6 CPS.RC—Recover	93

Appendix A	Use case
Appendix B	Relationship between risk source and measure requirements
Appendix C	Examples of security measures according to measure requirements
Appendix D	Relationship with major overseas standards

Appendix E Glossary

Executive Summary

- The Government of Japan is proposing creation of a next-generation smart social infrastructure program named *Society 5.0*. The proposed program will provide a variety of products and services for the emerging needs of citizens. It also will provide both economic development and solutions for social challenges by integrating cyberspace and physical space. To support “Society 5.0”, the Ministry of Economy, Trade, and Industry (METI), proposed a program called *Connected Industries* which will create value by building connections between a wide variety of disparate industrial data.
- In the industrial society of “Society 5.0”, networking between companies and industries has produced “Connected Industries”, in which the connections themselves create new data opportunities, for commerce. It is now possible to construct a more flexible and dynamic supply chain that includes new entities, and as cyberspace and physical space interact with each other, it is a new process that encompasses both spaces. The supply chain itself will create new added value.
- Cybersecurity is critical to the Connected Industries program. An attacker has many more possible targets in the new, interconnected supply chain, so cyber defenses must be drastically increased.
- In addition, the interconnection of cyberspace and physical space means that cyberattacks have an increasing impact on physical infrastructure. The physical consequences of a cyberattack could be enormous.
- The initiatives proposed for Society 5.0 integrating cyberspace and physical space create great value for citizens and companies, but the risks and consequences of cyberattacks greatly increase as well. The Cyber/Physical Security Framework will guide the implementation of the Connected Industries program to reduce the risk of cyberattack.
- Because many varied entities participate in highly networked supply chains, measures adopted at a single enterprise cannot assure security across the supply chain or even within its own enterprise. Therefore, each supply chain participant must adopt “security by design” techniques in which security is one

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

- In the Framework, security measures are shown which are commonly required for all industries for the next-generation supply chain in “Society 5.0” an industrial society in which cyberspace and physical space are highly integrated. In order to ensure supply chain trustworthiness, security measure are shown from three viewpoints (“Connections between organizations”, “Mutual connections between cyberspace and physical space” and “Connections in cyberspace”).
- Companies and industries have widely varying tolerance for cybersecurity risks. The Framework is designed with this in mind and should be used as a reference document as enterprises consider their special cybersecurity approaches and needs.
- Finally new threats will emerge with advances in AI technology in the unified cyberspace and physical space. The Framework will evolve to manage new threats, and will be reviewed appropriately.

Introduction

1. Society realized by “Society 5.0” and “Connected Industries”

Practical uses of networking and IoT (Internet of Things) are advancing now worldwide, and public and private sectors are beginning cooperation on highly advanced IT in the field of manufacturing to lead the revolutionary changes of “The Fourth Industrial Revolution” such as the “Industry 4.0” program in Germany. In Japan, “The 5th Science and Technology Basic Plan”, approved in a Cabinet meeting on January 22, 2016, the Government of Japan proposed a next-generation smart society named “Society 5.0” to produce products and services that satisfy a variety of needs, and which also provides both economic development and solutions for social challenges, by closely integrating cyberspace and physical space. Furthermore, we the Ministry of Economy, Trade and Industry (METI) need to develop a new industrial structure to realize “Connected Industries”, which creates new added value for “Society 5.0”, focusing on increased and varied connections.

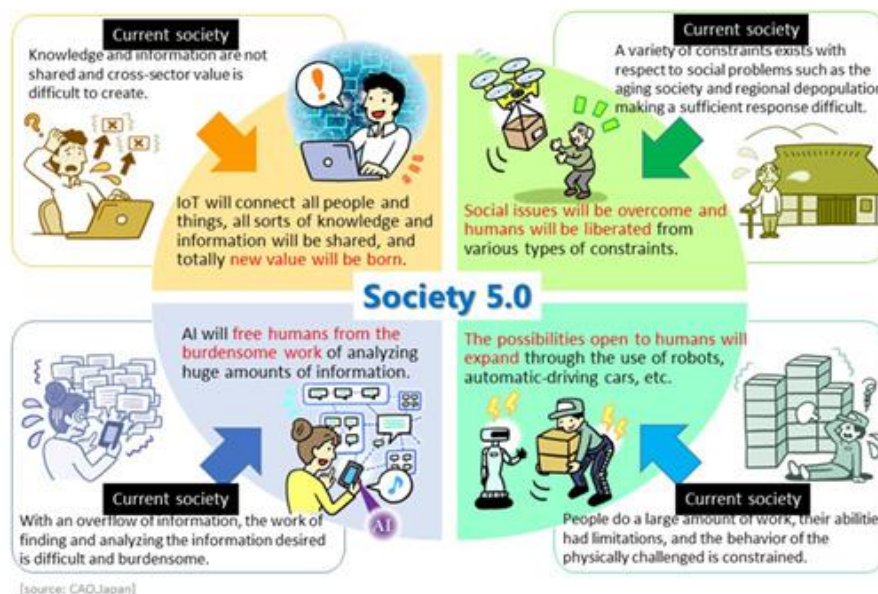


Figure i-1 Illustration of the society realized in “Society 5.0”¹

“Society 5.0” is the latest in a series of social structures. It is the next in the series of the hunting society (Society 1.0), agricultural society (Society 2.0), industrial society (Society 3.0), and information society (Society 4.0).

¹ The illustration is quoted from the introduction of “Society 5.0” by the Cabinet Office.

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

In “Society 5.0”, all people and things are connected by IoT, a wide variety of knowledge and information are shared, and new value is created. Moreover, “Society 5.0” relieves humans from the burdensome work of analyzing huge amounts of data through the use of Artificial Intelligence (AI). Furthermore, “Society 5.0” is not a society where economic and organizational systems are prioritized, but is instead a human-centered society in which AI, robots, etc. will support work formerly done by humans, and provide people with the goods and services they need, when needed, and as much as needed.

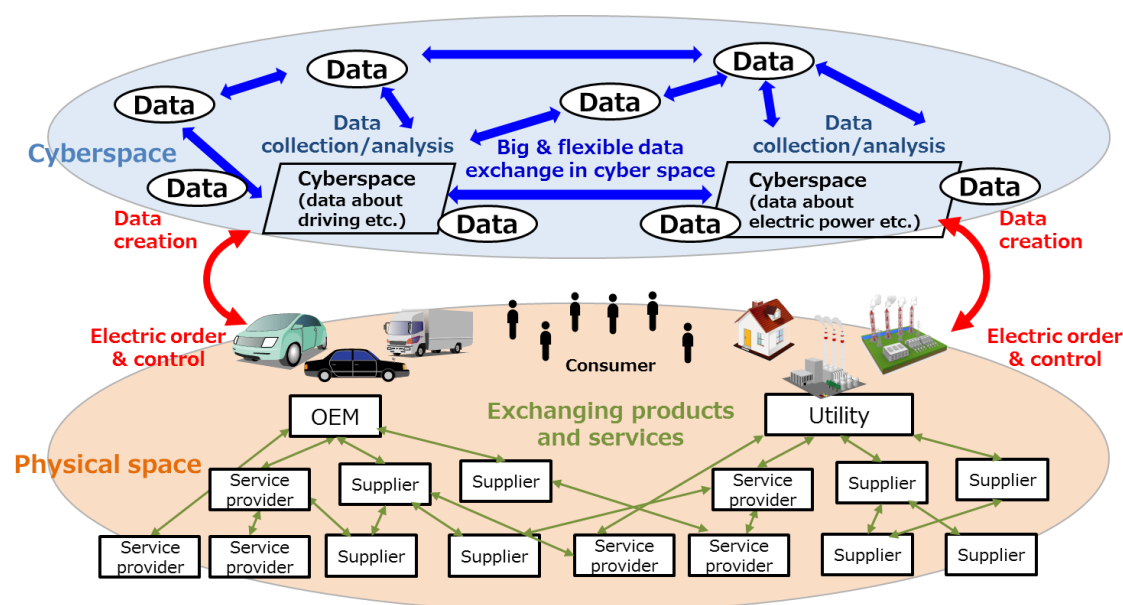


Figure i-2 Illustration of connections between components and data, etc. in Society 5.0

■ Change in the supply chain structure

In “Society 5.0”, the supply chain, which is a series of activities by companies to create added value, will also change its form. The existing supply chain was a rigid, linear structure of strict planning, including design, procuring necessary parts and services based on the design, assembling and processing, and delivering final products and services. It was deployed in a fixed and unchanging manner. In “Society 5.0”, however, where cyberspace and physical space are highly integrated, needed goods and services are provided to the

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

Supply chains straddle both cyber and physical spaces, and will change into the creation of added value through various dynamically connected items and data. In contrast with conventional standard and linear supply chain, these changed supply chains need to be viewed as the “Society 5.0” supply chain, and existing systems and procedures are to be “value creation process” so that it is distinguished from the conventional type.

2. Increase of threats by cyberattacks

In an industrial society of “Society 5.0” where cyberspace and physical space are highly integrated, cyberspace expands drastically and points of cyberattack expand; the two spaces interacting with each other increase the impact of the damages on physical space. For this reason, threats to the value creation process (a new supply chain connecting across cyberspace and physical space) are different and more complex compared to what the standard and linear supply chain faced, and will cause a wider range of damage.

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

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

important issues.

Table I-1 Features of Society 5.0 and corresponding security concerns

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

Threats to the supply chain are already arising as a real-life problem. In fact, a case was reported in which equipment of a European company was infected with ransomware. It infiltrated domestic enterprises in Japan via the supply chain, expanded the infection, and stopped some operations as a result.

Given the situation, the necessity to protect IoT and Industrial Control Systems (ICS) by supply chain management is becoming widely recognized in other countries. In the United States, the framework (Cybersecurity Framework), which provides the perspective of cybersecurity measures especially for the critical infrastructure developed by NIST² in February 2014, was revised in April 2018. In these documents, they added a description on supply chain risk management and requested to implement preventive measures to the entire supply chain and to conduct audits as needed. Note that, as of 2026, the Cybersecurity Framework (CSF) 2.0 is the latest version.

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

In the process of achieving “Society_5.0” and “Connected Industries,” the industrial and social environments are changing considerably. Along with these changes, there are more threats of cyberattacks, and new threats are

² National Institute of Standards and Technology

emerging. Now is the time to begin preparing ourselves for these new and increasing threats.

Under such problem awareness, METI has decided to formulate the “Cyber/Physical Security Framework,” build a model that appropriately identifies the risks faced in creating added value in the new industrial society, identify the risk sources, organize the overview of the required security measures, and summarize examples of measures which the industrial community can utilize as their security measures.

The Framework covers the entire model of the new industrial society and targets all entities that are working to create added value in it.

As risk sources and security measures to be identified, the following are included:

- (1) those applicable to conventional supply chains,
- (2) those that need new measures in the new industrial society model,

Security measures can be customized to each organization.

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

The reader should make use of the Framework and implement necessary security measures according to the context specific to the organization to which the reader belongs.

4. Intended readers of the Framework

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

- CISO(Chief Information Security Officer)

- Strategists and planners for supply chain creation and management teams (mostly Part I)
- Person in charge of security of the enterprises and groups involved in the value creation process
- Person in charge of development/quality assurance/design/construction of information systems and control systems
- Person in charge of data management
- Person in charge of standardization of security guideline for industrial associations

5. Overall structure of the Framework

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

- (1) Part I explains the Concept of the Framework , the followings are specified:
 - the model (the three-layer and the six elements) to identify the risk sources in terms of cybersecurity in the value creation process
 - an outline of the risks and risk sources
 - approaching the risks to ensure trustworthiness.
- (2) Part II uses the model shown in Part I to identify the risk sources and presents measure requirements for these risk sources. This part clarifies measure requirements (Policy) that each company or organization should take.
- (3) Part III organizes measure requirements shown in Part II according to a kind of measure. In addition, examples of the security measures classified based on the relative strength of security are presented in Appendix C. This part shows the specific Methods that each company or organization should actually take.

The above three part structure is also suitable for timely and appropriate review of necessary revisions. In other words, Part II will be updated in order to take more new risk sources on the progress of integration between

cyberspace and physical space. Part III will be updated in order to take up more valid measure instance by the progress of the security measure technology.

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

6. Expected effects and features of the Framework

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

(1) Expected effects in each enterprise utilizing the Framework

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

(2) Features of the Framework

- i. **It can be used to create and operate security measures for each enterprise**
 - The Framework shall allow enterprises to confirm the policy and have an actual implementation of the security measures (Part II and Part III), in addition to defining goals for security measures in the industrial society (Part I).
- ii. **It presents the necessity of security measures, and examples of measures that are appropriate for costs and risks**
 - It will identify the relation between the expected risk sources and countermeasures, and allow understanding of the costs so that the enterprises (including small- and medium-sized enterprises) which are building a value creation process can actually implement the measures.
 - It allows us to devise ways to reduce cost while maintaining an appropriate level of security by deriving security measures from the risk source (risk-based thinking), and allowing enterprises to select the right measures for their circumstances.

iii. **Contribute to international harmonization**

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

7. How to use the Framework

The Framework is intended to be referred to when an entity, who is working on creating added value in the new industrial society, “Society_5.0,” takes security measures necessary for that activity.

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

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

By referring to the three-layer approach shown in the Framework, a model can be developed for the creation of added value for each organization based on trustworthiness. Necessary characteristics and functions are noted in each layer of the three-layer approach. Specific examples of equipment are presented in Part II. Appendix A shows a typical case of use in each industry.

In addition, the risk sources of each organization can be identified by referencing the security incidents, threats, and vulnerabilities mapped to the six elements, which are organized in Part II and Appendix B.

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

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

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

Security policy for the organization can be formulated, and security measures can be implemented with reference to security requirements and examples of measures shown in Part III and Appendix C. Part III presents security measure requirements defined so as to be consistent with the concept of international frameworks (e.g., the NIST Cybersecurity Framework (CSF) 2.0). ~~Part III presents security measures organized in consideration of the concept of NIST cybersecurity frameworks.~~ Appendix C gives examples of security measures that would satisfy each of the security requirements.

It is expected that these materials will help each of the organization's efforts, especially on the following points.

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

(3) **Building a trustworthy chain among organizations and industries**

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

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

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

1. Efforts for “value creation process,” a “Society 5.0” supply chain in an industrial society where cyberspace and physical space are highly integrated

In the “Society 5.0” and “Connected Industries” programs, the increased connectivity, data creation by IoT devices, and data analysis using AI, will result in very different supply chain and value creation models from today’s practices.

In the Framework, a Society 5.0 supply chain is defined as a “value creation process” to distinguish it from the conventional supply chain. The Framework provides a guide for security measures required by Society 5.0 and Connected Industries extended supply chain models.

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

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

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

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

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

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

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

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

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

The first layer – Connections between organizations

The second layer – Mutual connections between cyberspace and physical space

The third layer – Connections in cyberspace

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

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

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

each detailed definitions are described in 2.2.

- Organization³
- People
- Components
- Data
- Procedure
- System

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

³ To distinguish it from the general use of the word, the term “organization” is enclosed in quotation marks when used in the specific sense defined in this Framework. ~~In order to distinguish it from "organization" of general usage, when using the term "organization" as a unique meaning in this paper, " " is attached.~~

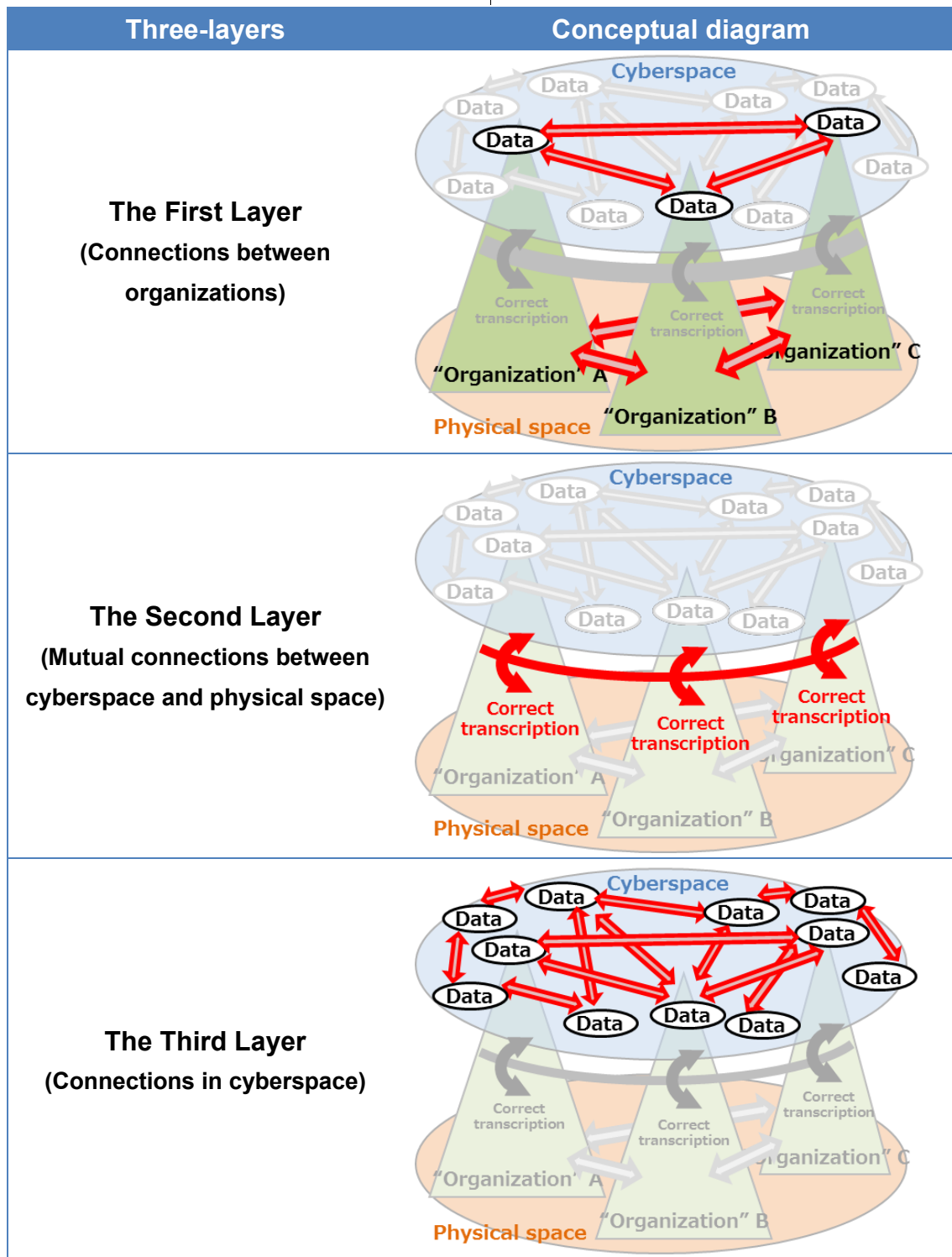


Figure 1.2-1 Three layers of the industrial society where value creation processes unwind

2.1. Significance of the three-layer approach

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

The First Layer — Connections between organizations

The first layer aims for a level that ensures trustworthiness in the organization's management.

This idea has been adopted to achieve security in the supply chain. It is based on the idea that by confirming the trustworthiness of the enterprise's management and allowing only participants whose trustworthiness is established, security can be ensured.

Certification programs such as ISMS (based on ISO/IEC 27001) center on ensuring trustworthiness in the company's management, division management, and headquarters' management, and provide a mechanism that leads to connections between companies with confirmed trustworthiness to ensure security in the supply chain. Using this approach, security policies are shared, and the trustworthiness of management is confirmed and certified. In summary, the first layer aims for a level that organizational management with shared security policy is certified as a basis for ensuring trust.

However, in an industrial society where cyberspace and physical space are integrated, it is impossible to ensure trust in the entire value creation process by only confirming the trustworthiness of the organization's management. In the second layer and the third layer of the model, there are introduction of further types of trustworthiness to ensure trustworthiness of the whole value creation process.

The Second Layer — Mutual connections between cyberspace and physical space

In an industrial society where cyberspace and physical space are highly

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

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

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

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

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

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

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

The Third Layer — Connections in cyberspace

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

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

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

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

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

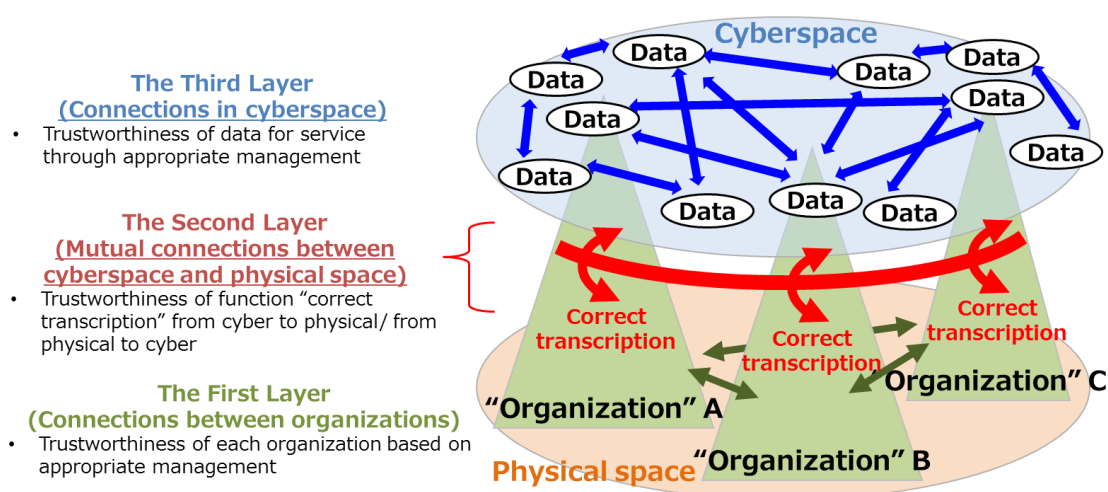


Figure 1.2-2 Significance of the three-layer model

2.2. The six elements

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

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

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

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

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

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

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

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

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

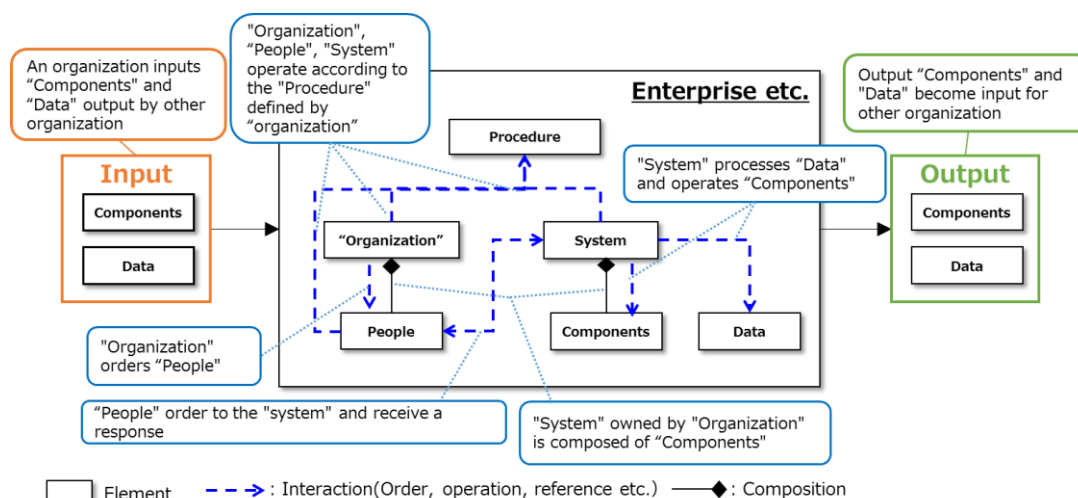


Figure 1.2-3 Relationship of six elements

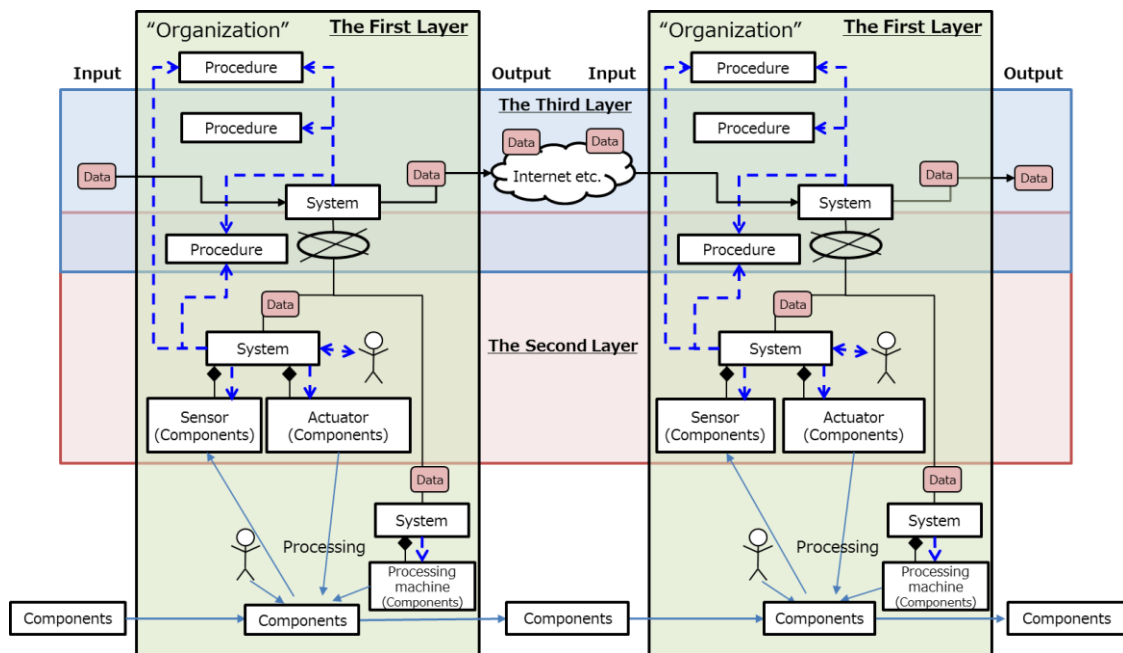


Figure 1.2-4 Relationship of six elements in the three-layer model

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

The risk sources in the value creation process will be identified and associated policies will be developed in Part II based on the three-layer model and the six elements. Part I especially shows that new risk sources appeared in the value creation process, which are different from conventional supply chains. In the first layer, management by the enterprise is the basis of trustworthiness, and security measures are implemented based on the management of each enterprise. However, as already mentioned, security measures need to be taken in the second layer and the third layer for the value creation process that spans both cyber and physical spaces.

The important point in security measures for the second layer is to ensure correct transcription on the border of cyberspace and physical space. To ensure trustworthiness of the transcription, any organization which is directly or indirectly involved in the value creation process must cooperate. This means that even organizations not directly involved in the value creation process are required to participate in implementing security measures. A multi-stakeholder approach is required.

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

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

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

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

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

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

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

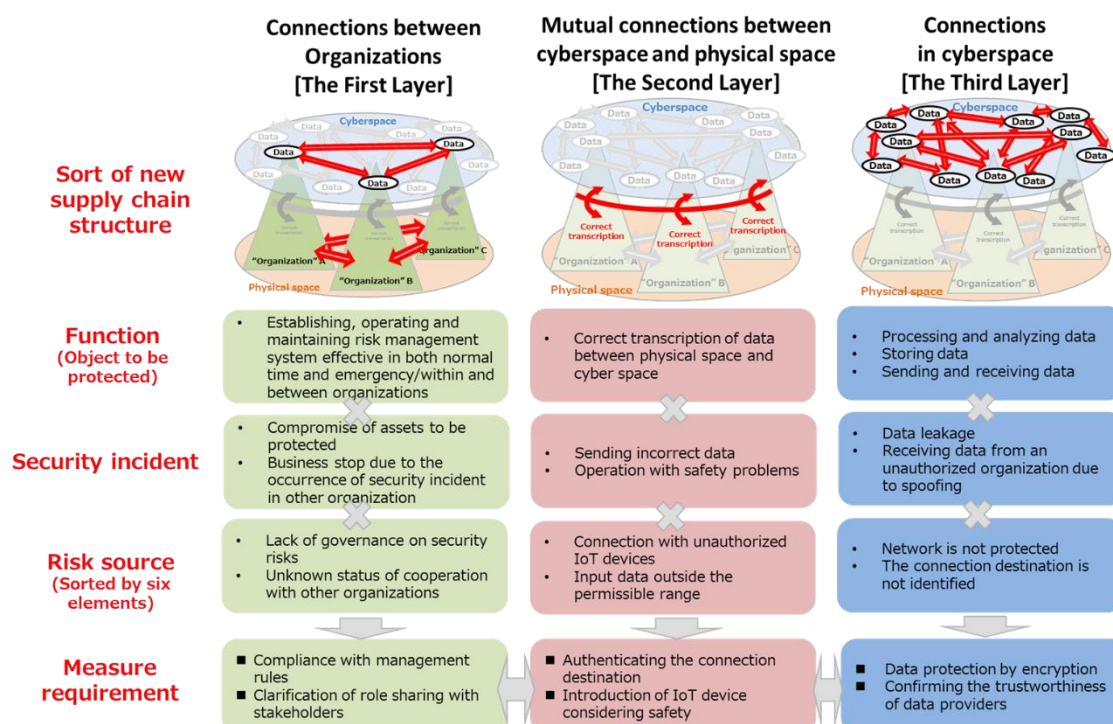


Figure 1.3-1 Overview of the measures in each layer

4. Concepts of securing trustworthiness based on the Framework

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

(1) Creation of Trust

Examples)

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

(2) Proof of Trust

Examples)

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

(3) Structuring and Maintaining of Trustworthy chain

Examples)

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

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

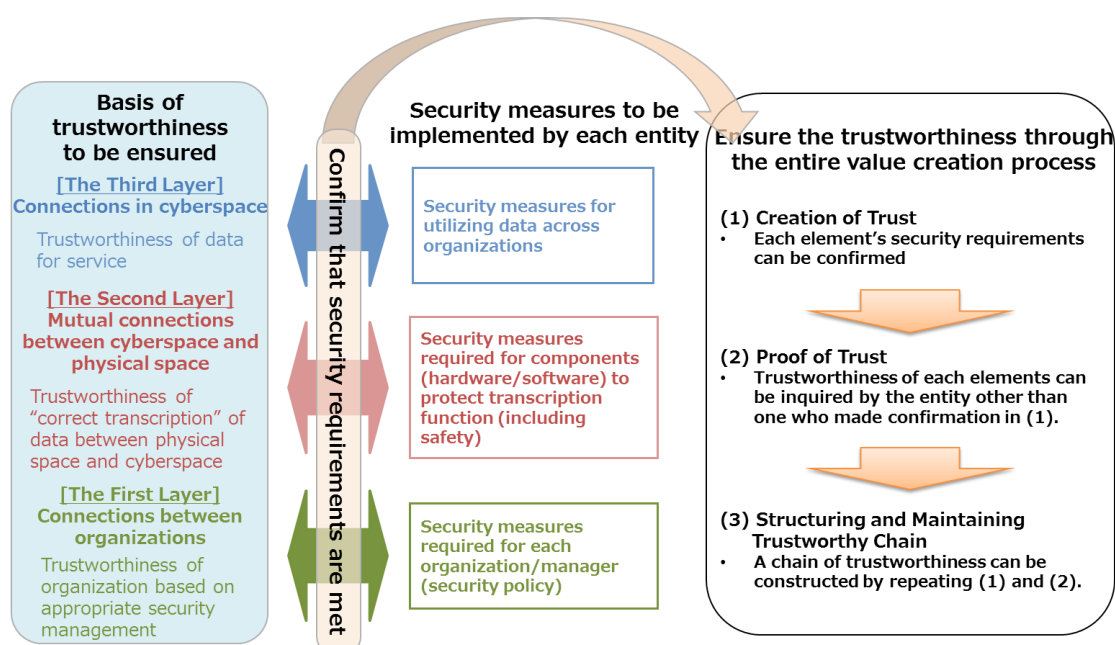


Figure 1.4-1 Concept of basis of trustworthiness

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

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

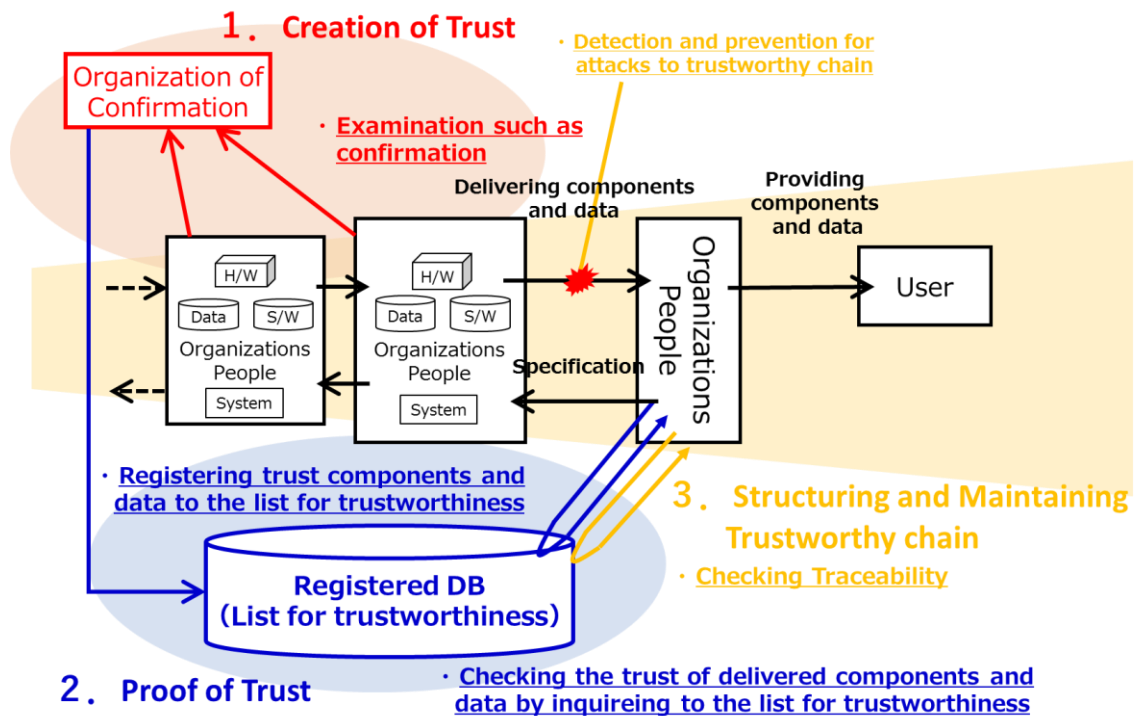


Figure. 1.4-2 Illustration of the relationship among Creation of Trust, Proof of Trust and Structuring and Maintaining of Trustworthy chain

5. Conclusion

The Framework presents security measures common among all industries of the value creation process in a proposed industrial society, "Society 5.0", where cyberspace and physical space are highly integrated. However, there are wide difference of practices and variations of allowable risks between industries, and even between companies within an industry. Security measures must take these variations into account.

Therefore, in each industry and each enterprise, please use the Framework to establish both the current level indicating the actual status of security measure implementation within its own organization and the target level indicating that to be achieved in the future. ~~Therefore, in each industry and each enterprise, please use the Framework in order to adopt appropriate security measures internally.~~

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

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

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

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

Entities involved in the value creation process can utilize the Framework by using the standard risk management process adopted in ISO 31000:2018 and ISO/IEC 27001:2022. The contents of Part II can be utilized in the risk management process, especially when scope, context, criteria, assessing risks, and treating the risks.

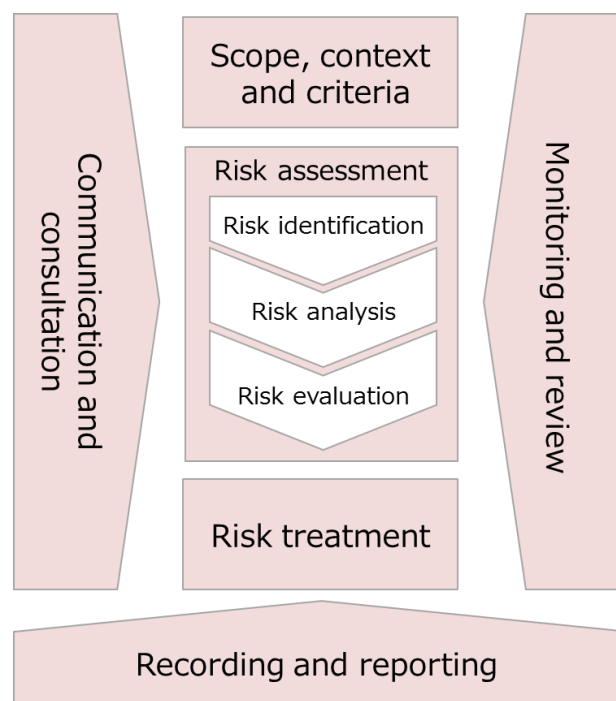


Figure 2.1-1 Typical risk management process⁴

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

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

■ Scope, context and criteria

i. Specifying the target of analysis (1.1)

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

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

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

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

iii. Analyzing risks (1.3)

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

■ Risk treatment

iv. Managing risks (1.4)

Risks are addressed based on the risk analysis results.



Figure 2.1-2 Flow of risk management⁵

⁵ Created with reference to “Security Risk Assessment Guide for Industrial Control Systems 2nd Edition” published by IPA

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

Definition of Risk: Effect of uncertainty on objectives

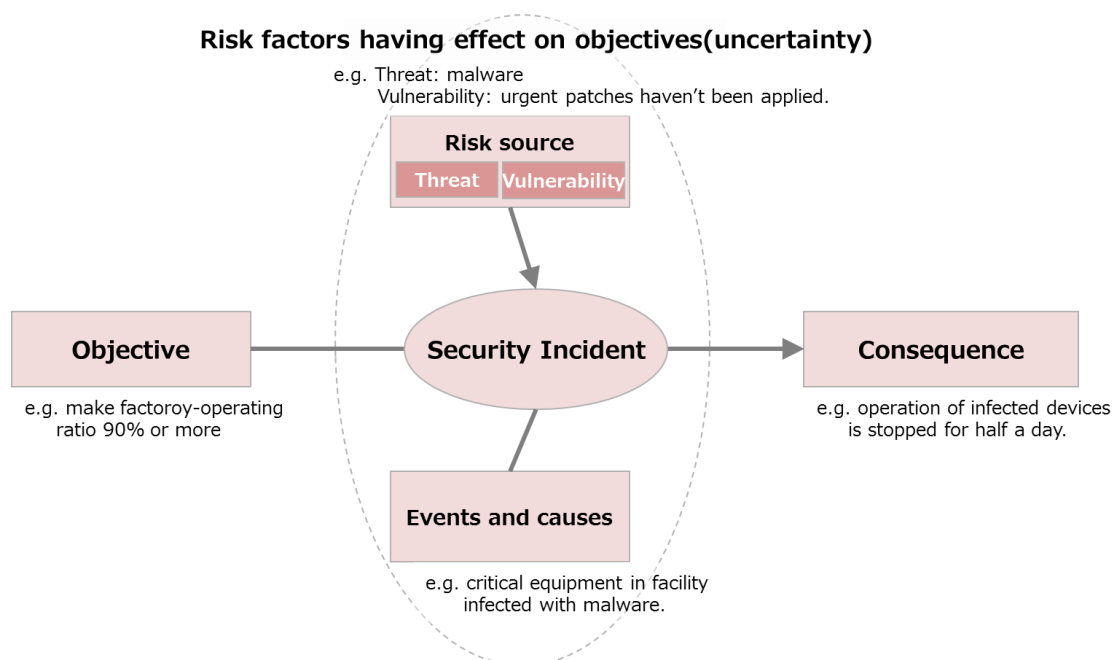


Figure 2.1-3 Concept of security risk

In particular, in order to properly assess the security risks in “Society 5.0” and implement effective treatment, the following four points should be taken into consideration through the process shown in this part. These points will be described in detail in 1.1.(2).

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

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

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

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

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

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

The target of analysis must first be identified when assessing risks. “Security Risk Assessment Guide for Industrial Control Systems 2nd Edition” (published by IPA, [2026](#)) prescribes the following for the identification of the target of analysis.

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

In an industrial society where cyberspace and physical space are integrated outside the organization, identifying the assets and the scope of analysis is expected to become more difficult. In order to implement the three items above, it is important to identify the stakeholders of the value creation process in which the organization is involved, and to grasp the flows of the items and data in both cyberspace and physical space. The Framework provides guidance to identify the target of analysis based on the three-layer model presented in Part I. The organization can determine the scope of analysis by utilizing the method in this section and then identifying the system configuration and the data flow within the scope previously defined so that understanding for the object of the risk management can be detailed⁶.

⁶ When carrying out “identifying the system configuration” and “identifying the data flow”, it is desirable to refer to Sections 3.2 and 3.3 in “Security Risk Assessment Guide for Industrial Control Systems 2nd Edition” published by IPA.

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

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

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

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

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

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

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

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

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

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

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

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

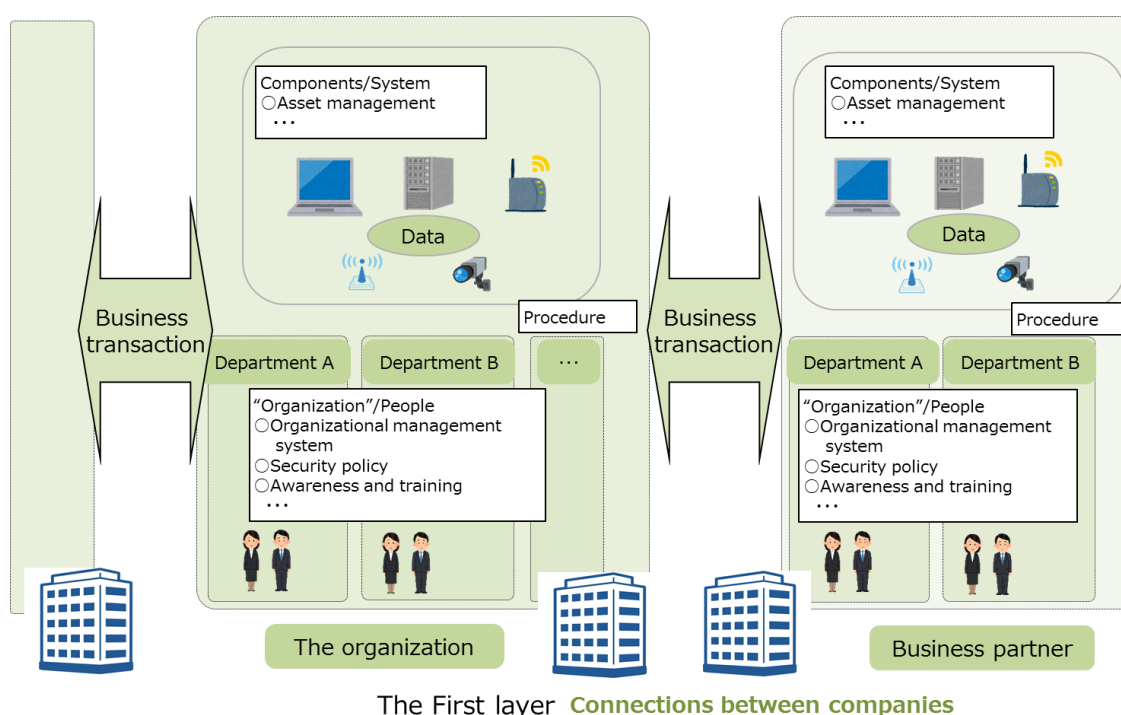


Figure 2.1-4 Targets of analysis and concrete image of analysis targets in the first layer

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

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

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

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

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

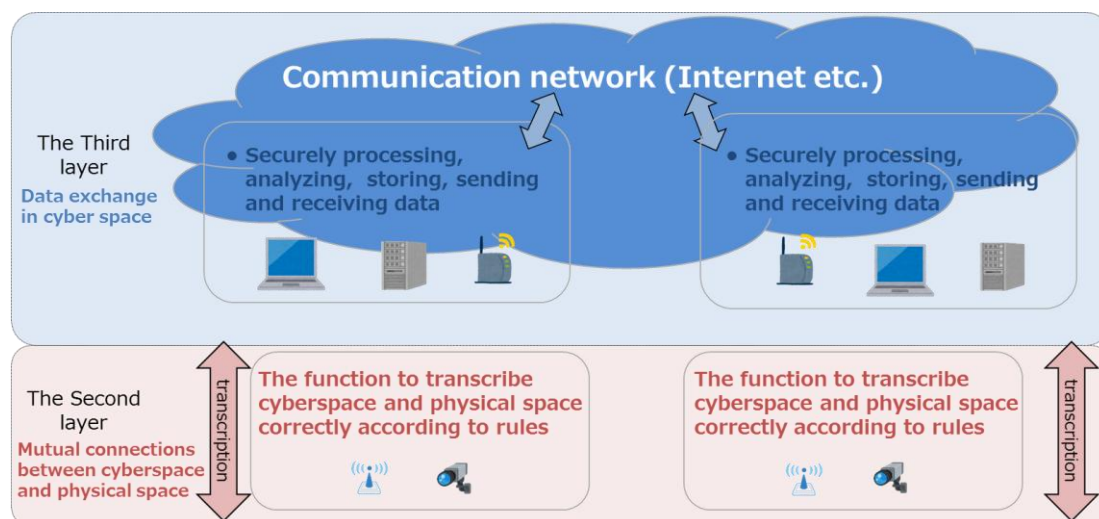


Figure 2.1-5 Functions/roles and concrete image of analysis targets in the second layer and the third layer

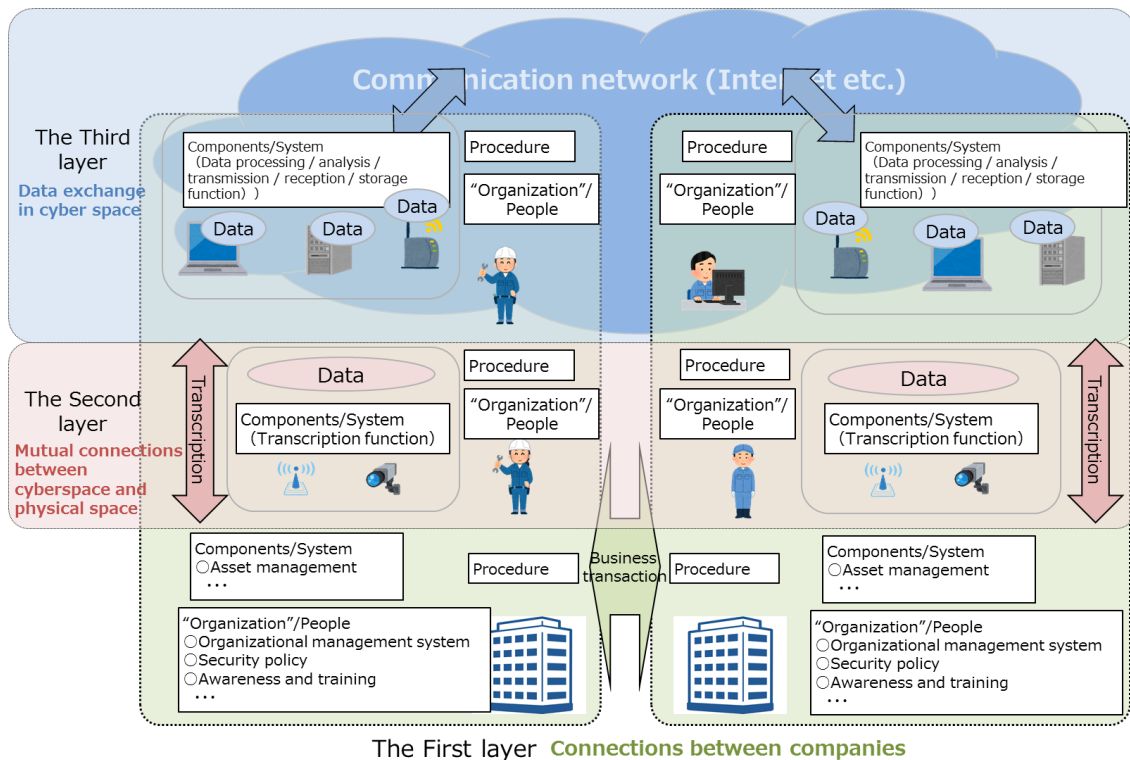


Figure 2.1-6 Concrete image of analysis targets based on the three-layer model and the six elements

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

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

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

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

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

ii. Integration of cyberspace and physical space through IoT devices

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

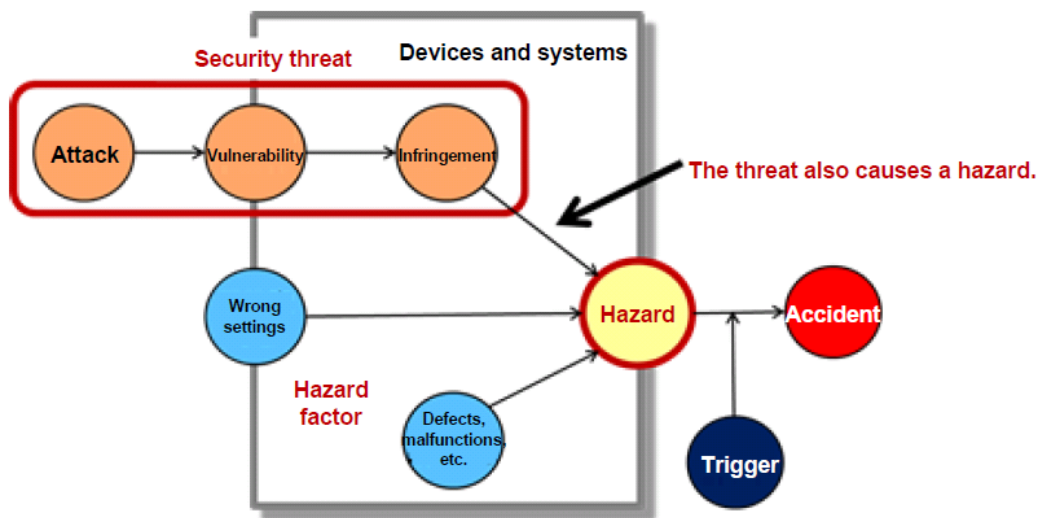


Figure 2.1-7 Model of security problems affecting safety⁷

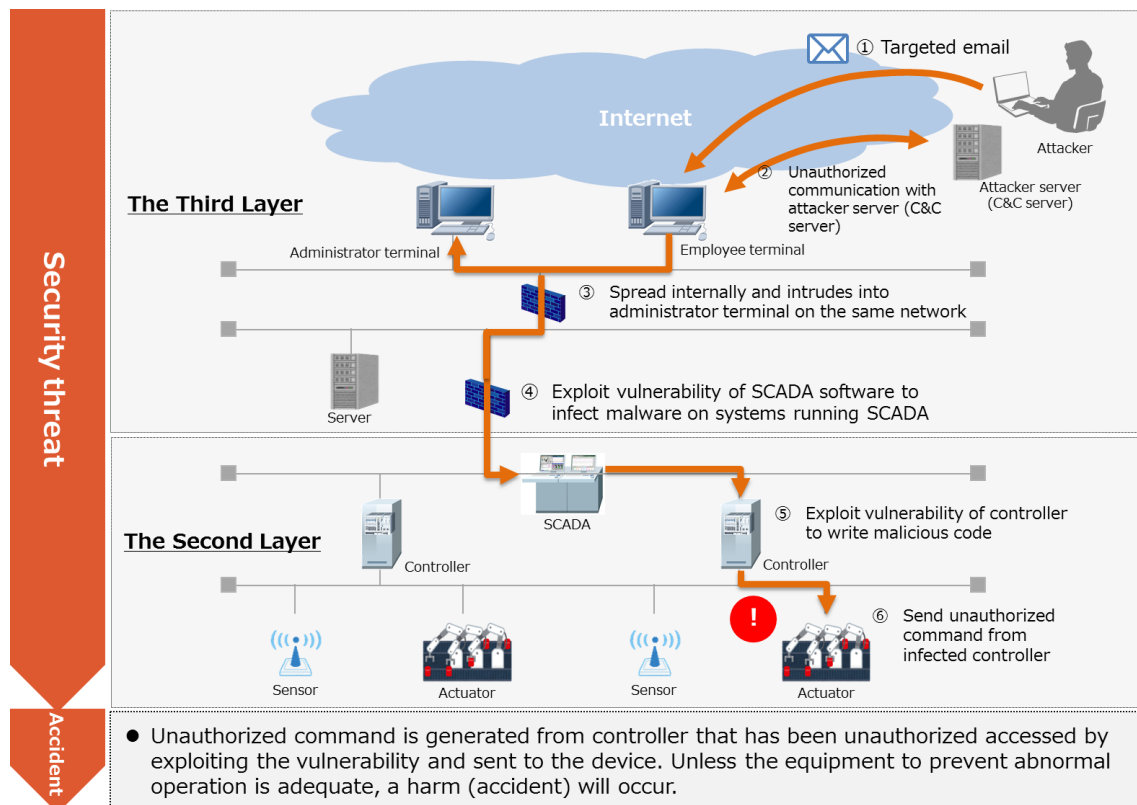


Figure 2.1-8 Example of security problems affecting safety

⁷ Cited from IoT Acceleration Consortium, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry “IoT Security Guidelines Ver.1.0”

iii. Cross-organizational data exchange

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

iv. Securing the basis of trustworthiness of each layer

- As mentioned in Part I, in “Society 5.0”, in order to produce the targeted value, it is important to take measures considering not only the viewpoint of the trustworthiness of the organizational management that has conventionally been taken in to consideration, but the plural viewpoints such as the accuracy of the transcription function through IoT devices in the second layer, and the trust of the data itself pertaining to the value creation process in the third layer.
- Therefore, in identifying the target of analysis, it is important to identify the factors that are connected with the basis of trustworthiness. In the above implementation, the measures described in i. to iii. in this section are effective.

1.2. Anticipating security incidents and their impact

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

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

incidents in consideration of each item described in the column “Adverse effect on functions” in Table 2.1-4.

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

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

		intended (malfunction, unintended stop, etc.)
--	--	---

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

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

Aspects not adequately considered	Security incidents that may occur	Security incidents ⁸ relevant in [Appendix B]
Understanding the relationships of stakeholders inside and outside the organization	Business is not continued appropriately when security incidents occur at a certain point in the value creation process	L1_3_b, L1_3_c
Understanding new security incidents that may arise from the integration of cyberspace and physical space	Incidents that may affect safety occur at the point of contact (IoT device) between cyberspace and physical space	L2_1_a, L2_1_b, L2_1_c, L2_2_a
	Attack on cyberspace from the IoT device	L2_3_b, L2_3_c
Understanding the state of data exchange across organizations	Sensitive data is not properly managed by outsourcing parties that process that data	L3_1_a, L3_1_b, L3_1_c, L3_2_a, L3_2_b, L3_4_b

Table 2.1-6 is examples of general security incidents that should be prevented in each layer of the three-layer structure.

To consider possible incidents exhaustively, organizations should identify security incidents using the approach shown in Appendix B, and consider them concretely, taking into account the circumstances of each organization.

⁸ For example, the security incident L1_3_b indicates the security incident (3) (b) assumed in the first layer.

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

Assumed security incidents in the first layer	
(1) Security incidents (e.g. data leakage/tampering/destruction/unintended stop) due to inadequate risk management processes during normal operations	
	(a) Data that must be protected is leaked from an area managed by the organization.
	(b) Data that must be protected is tampered with in an area managed by the organization.
	(c) The system dealing with the data of its own organization stops due to a denial-of-service (DoS) attack, ransomware infection etc..
	(d) A security event occurs in the channel for product / service provisioning, causing unintended quality deterioration such as malfunction of a device.
(2) Noncompliance with regulations	
	(a) Security measures that satisfy the legal requirements for a system cannot be implemented
(3) Damage caused by security incidents expands, and the organization as well as other relevant organizations cannot continue their business properly.	
	(a) The organization's security incidents prevent their business from continuing properly
	(b) Other relevant organizations cannot continue their business properly due to the organization's security incidents
	(c) The organization's security incidents prevent the business of other relevant organizations from continuing properly
Assumed security incidents in the second layer	
(1) Unintended operation of attacked IoT devices (e.g., incorrect measurement, improper control of things, stop of control function, measurement function)	
	(a) Unexpected behavior of the IoT device due to unauthorized access to its controls by exploiting a vulnerability results in unpredicted operation
	(b) Unexpected behavior of the IoT device due to unauthorized access to its controls by impersonation of an authorized user results in unpredicted operation
	(c) Unauthorized input to the IoT device due to unauthorized access to the system that remotely manages the IoT devices results in unpredicted operation
	(d) Functions of IoT devices and communication devices stop due to attacks such as DoS attack
(2) Damage to equipment, physical harm to employees, and negative impact on business operations due to operation of IoT devices (normal and abnormal operation)	
	(a) Behavior that threatens safety, regardless of the behavior being normal or abnormal

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

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

After the organization defines potential security incidents, it should estimate the business damage resulting from those incidents. One example of an approach is defined in Section 4.3, “Business damage and the business damage level” of “Security Risk Assessment Guide for Industrial Control Systems 2nd Edition” (IPA, 202618).

By assigning severity scores to the degree of damage for each possible security incident, appropriately prioritized risk mitigations and security measures can be realized.

1.3. Analyzing risks

Using the results of the process in section 1.1 and 1.2, the organization should explore and define attack scenarios that could lead to the identified security incidents, define the sources of threats, and assess possible damage to business. Appendix B identifies threats that may help cause particular security incidents and/or magnify the damage caused by the incidents, along with typical vulnerabilities. Hence, it can be used to identify the risk sources to be considered and to show gaps in risk coverage.

~~Typical vulnerabilities are identified exhaustively for the six elements shown in Figure 2.1-9.~~ Figure 2.1-9 shows an attempt to identify typical vulnerabilities more comprehensively from the perspective of the six components. Note that, since system configurations, data flows, and details of relevant assets differ from one enterpriseorganization to another, the Framework recommends each enterpriseorganization consider theirits respective circumstances when exploring specific scenarios of attacks, assessing the levels of damage to business, and the risk sources.

When evaluating risk sources and selecting security measures, it is important to keep in mind that the same specific entity may correspond to six different elements in different value creation processes. For example, it may be appropriate to be evaluated PC or server not only as “System” but also as “Components”. Also, in some cases it is appropriate to evaluate software as each of “Procedure”, “Data” and “Components”.

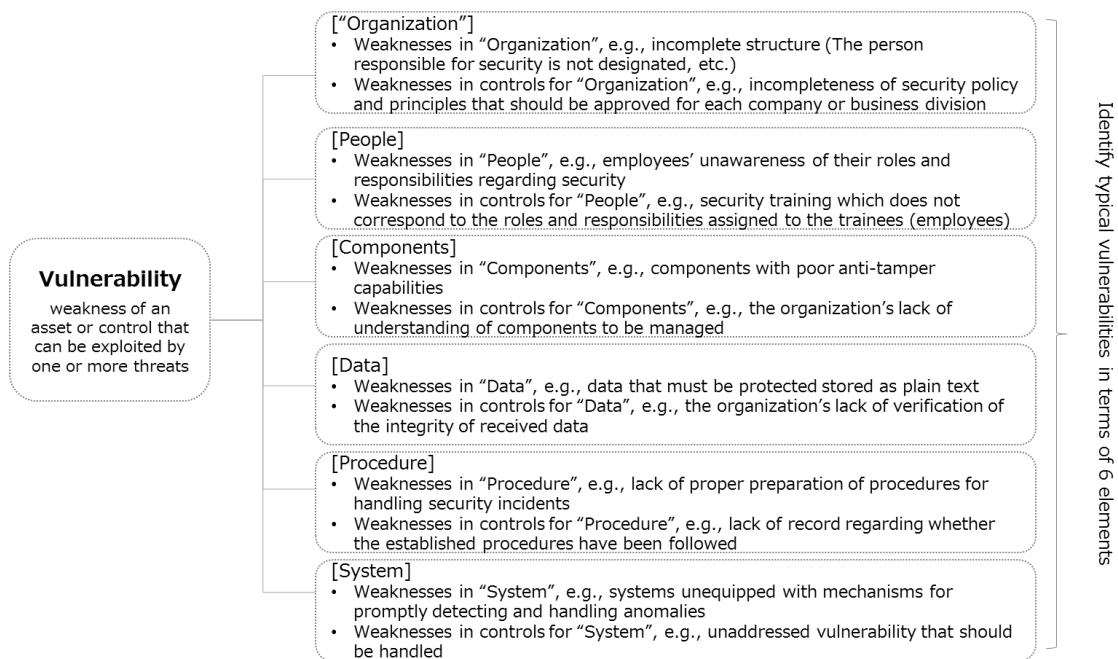


Figure 2.1-9 Identification of vulnerabilities in terms of six elements

1.4. Managing risks

Determine which action to take — aversion, reduction, transfer, or retention⁹ — in order to manage the risks identified by the risk analysis conducted in 1.3 according to the level of damage each risk can cause.¹⁰

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

⁹ Cited from "Primer of safety & security design in the connected world" (IPA).

¹⁰ The types of risk treatment described correspond to the risk treatment options presented in ISO 31000: 2018 as follows.

- Risk aversion: Include "avoid the risk", "remove the source of the risk".
- Risk reduction: Include "change the probabilities", "modify the consequences".
- Risk transfer: Include "share the risk with others".
- Risk retention: Include "increase the risk in order to pursue an opportunity", "retain the risk".

Appendix B provides a reference for risk sources corresponding to security incidents introduced in Table 2.1-6 and action to be taken, especially when ~~the risk mitigation~~reduction approach is selected from the above actions. ~~The “Measure requirements” column serves as a guideline for implementing security based on the details of risk (threats and vulnerabilities). The section “Measure requirements” is a guideline for implementing security based on the details of risk (threats and vulnerabilities).~~ Appendix B also provides for adaptation of its guidance to the particular circumstances of the organization. Since Appendix B ~~matches~~maps specific vulnerabilities to each measure requirement, it can be used as a completeness and quality check for the risk analysis conducted by the organization.

It is particularly important to define measures for the four points of view already mentioned in the Framework.

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

- It is vital to always have a whole picture of relationships between the stakeholders inside and outside the organization. It is also important to clarify the roles and responsibilities regarding cybersecurity among organizations. Definitions of stakeholders and roles that was considered in 1.1 must be promptly updated if the business partner has changed or any modifications have been made to the details of what must be done.
- ISO/IEC 27036-2:20~~22~~14 describes the five phases shown in Figure 2.1-10 as a life-cycle in relation to an individual supplier¹¹.

¹¹ ~~With reference to this point, ISO/IEC 27036-3:2023 and NIST SP 800-161 Rev. 1, Update 1 have been published as standards regarding the security measures relevant to the supply chain. In drafting this Framework, NIST SP 800-161 was leveraged to identify risk sources. Regarding this point, if it is deemed necessary to implement more enhanced measures, it is possible to refer to NIST SP 800-161 Rev. 1, Update 1 for security controls. With reference to this point, ISO/IEC 27036:2014 and NIST SP 800-161 are formulated as standards regarding the security measures relevant to the supply chain. In drafting this framework, NIST SP 800-161 is referred to for the identification of risk sources, and ISO/IEC 27036:2014 is referred to for the description of measure requirements and examples of security measures. Regarding this point, if it is deemed necessary to implement more enhanced measures, it is possible to refer to NIST SP 800-161 for security controls.~~

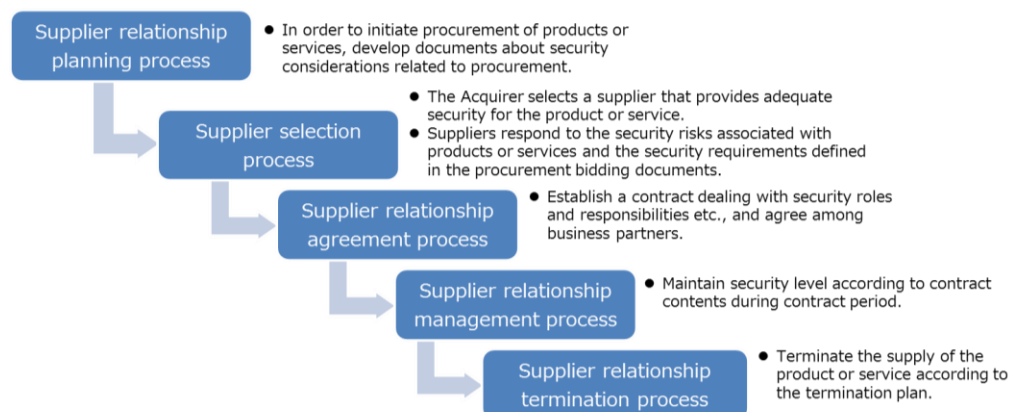


Figure 2.1-10 Lifecycle in contracting with an individual supplier in ISO/IEC 27036-2:2022

- Requirements for security measures in light of the above life-cycle are set out in the measure category “CPS.GV.SC” (supply chain risk management) described in Part III. Each organization must consider stakeholder relationship management throughout the process lifecycle for all categories of security measures.
- Related measure requirements include CPS.GV.OC-03, CPS.GV.RR-02, CPS.GV.PO-01, CPS.GV.SC-04, CPS.GV.SC-05, and CPS.ID.AM-03. ~~CPS.AM-5, CPS.AM-7, CPS.BE-2, CPS.BE-3, CPS.SC-1, and CPS.SC-2.~~ (Refer to Part III for details on each measure requirement.)

ii. Integration of cyberspace and physical space through IoT devices

- If a sensor sends any measured data different than the actual one to cyberspace, or if measured data stops coming into cyberspace, the trust in the operations that use these data may be damaged.
- To avoid such damages, security measures must be taken to prevent attacks on functions of sensors. Specifically, consider using devices that do not easily shut down under attack (e.g., DoS attack), that offer a mechanism for checking data integrity, and/or that offer a function designed to guarantee the authenticity of measured data.
- Related measure requirements include CPS.PR.DS-02, CPS.PR.DS-03, CPS.PR.PS-03, CPS.PR.IR-04, and CPS.DE.CM-07. ~~CPS.DS-6, CPS.DS-11, CPS.DS-15, and CPS.CM-4.~~

- As stated in 1.1, when data inputs are received from cyberspace for controlling components in physical space, security problems may lead to safety problems including physical harm. To ensure security and safety on the interface between physical and cyberspace, it is vital to establish, at the design and procurement stages, a series of procedures to: analyze safety hazards and the sources of these risks. It is also critical to identify, based on the analysis, the business and technical processes on which security has an impact. This enables an organization to take appropriate courses of action, through the entire supplier lifecycle from planning and design/procurement through operation/maintenance/disposal, according to the analysis results.
- Ensuring safety has the utmost priority. Hence, it is necessary to combine measures taken for functional safety with cybersecurity measures in order to achieve safety. Since consideration of both safety and security aspects is required, close communication among the persons in charge of both safety and cybersecurity is essential to take appropriate actions.
 - Related measure requirements include [CPS.ID.RA-03](#), [CPS.ID.RA-04](#), [CPS.ID.RA-06](#), [CPS.PR.PS-03](#), and [CPS.DE.CM-08](#).~~CPS.RA-4~~, ~~CPS.RA-6~~, ~~CPS.PT-3~~, and ~~CPS.CM-3~~.
 - Integrated security for safety control has been discussed in recent years in terms of international standardization. Documents available for reference regarding this subject include IEC ~~TSR~~ 63074:[2023](#) and IEC TR 63069:2019 (cf. Figure 2.1-11). ¹²

¹² In addition to the IEC standards mentioned above, reference may also be made to ISO TR 22100-4: 2018 (Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects) which deals with machine safety security as well as IEC ~~TSR~~ 63074:[2023](#).

IEC TR 63074 (Security aspects related to functional safety of safety-related control systems / TC44)	IEC TR 63069 (Industrial-process measurement, control and automation – Framework for functional safety and security / TC65)
· Security analysis target is limited to safety facilities. · First, design safety equipment on the safety side. · Next, the security team conducts security risk analysis on safety facilities and adds security measures. · Cyber attacks do not create new hazards because only the physical hazards of the machine harm people.	· Conduct risk analysis in parallel with safety and security, and seek out the risk level from what to protect from what. · Design safety function specifications and security function specifications based on the results of risk analysis. · For safety facilities designed on the safety side, conduct additional security analysis. · Ultimately, integrate safety and security specifications, discuss and solve and implement if there is contradiction / competition between them.
Sequential analysis and design of safety and security	Parallel analysis and design of safety and security

Figure 2.1-11 Status of discussion about integrated safety and security in the movement toward international standardization¹³

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

¹³ Created based on “Guide for considering safety/security requirements for control systems” (IPA) and “Standard Activities of Functional Safety and Security” (Hiroo Kanamaru, “IPSJ Magazine”, Vol.58, No.11, Nov.2017).

organization to consider the risks of theft and loss when taking security measures¹⁴.

- Related measure requirements include CPS.PR.AA-07, CPS.PR.PS-02, CPS.PR.PS-06, CPS.PR.PS-12, CPS.PR.IR-02, and CPS.DE.CM-05.~~CPS.AC-2, CPS.DS-8, CPS.IP-5, CPS.IP-6, CPS.PT-2, and CPS.CM-2.~~

iii. Cross-organizational data exchange

- In the case where the organization's protected data is processed, analyzed or stored by business partners, or where the organization handles the protected data of other organizations, the organization should agree with the business partners in advance on data classification, on the required security measures based on the classification, and on regular confirmation procedures including compliance auditing.
 - The organization should analyze the risk in view of the characteristics of the exchanged data, the services that the business partners or the organization provide, and so on, and implement specific security requirements as appropriate.
 - Even if it has implemented adequate measures, it is also important for the organization to formulate a procedure for security incident response in advance. The procedure should include notifications of all concerned parties when security incidents involving protected data are detected.
 - If the organization receives data processed by other organizations, it should enable immediate response upon the detection of an anomaly, including continuously monitoring whether data is sent from authentic senders, the data does not include exploit codes, and so on.
- Related measure requirements include CPS.GV.SC-02, CPS.GV.SC-06, CPS.GV.SC-07, CPS.GV.SC-08, CPS.DE.CM-01, CPS.DE.CM-03, CPS.DE.CM-07, CPS.RS.MA-04, and CPS.RC.CO-01.~~CPS.SC-3, CPS.SC-4, CPS.SC-9, CPS.CM-1, CPS.CM-3, CPS.CM-4, CPS.DP-1, CPS.RP-2 and CPS.CO-1.~~

¹⁴ It is advisable to refer to the Main Point 6 in IoT Security Guidelines Ver. 1.0 by the IoT Acceleration Consortium, Ministry of Internal Affairs and Communications, and the Ministry of Economy, Trade and Industry, as well as Cyber Security for Consumer Internet of Things: Baseline Requirements (ETSI EN 303 645 V3.1.3 (2024-09)) by ETSI.

iv. Securing the basis of trustworthiness of each layer

- In the first layer, it is vital to specify cybersecurity requirements needed to maintain relationships and trust with the stakeholder organizations in the value creation process, and to regularly check compliance status.
- An entity subject to regular checks and audits should collect the information that proves their compliance and make it available in advance or promptly upon request. This applies particularly to business partners critical to the organization's business continuity. The organization should ensure that not only direct contractors, but subcontractors and any organizations working for them, comply with the established requirements, thereby developing a chain of trust.
 - Related measure requirements include CPS.GV.SC-06, CPS.GV.SC-07, CPS.GV.SC-08, and CPS.GV.SC-12.~~CPS.SC-3, CPS.SC-4, CPS.SC-6 and CPS.SC-8.~~
- The second layer requires that an IoT device's transcription function be accurate. To ensure accuracy, it is vital to maintain and enhance the soundness of security for the IoT device by taking measures throughout the device lifecycle, from the design and procurement stages through the operation and disposal stages.
- The organization should take measures such as adopting security by design at the planning, design and procurement stages, testing security functions for verification, managing vulnerability when the device is in operation, and verifying the integrity of the device and software.
- In the case of an IoT device that is extremely important to the organization's business continuity, security requirements for the transcription functions should be in the agreement so that the organization can check if these requirements are accurately met throughout the series of processes performed by the contractor, or subcontractors, or any organizations working for them (e.g., production, transportation).
- Security practice for IoT devices has some important differences from security for traditional IT systems.¹⁵ Though it is essential to require

¹⁵ For example, ~~Draft~~ NISTIR 8228 suggests that, in order to implement security protection of IoT devices in terms of device security, data security and privacy, the characteristics specific to IoT devices, unlike traditional IT devices, should be considered with regard to the measures such as asset management, vulnerability management, access management, incident detection, data flow management.

adequate security functions during procurement based on the principle of security by design, alternative measures on the part of the system should be considered if they are not available. In Appendix C, several security measure requirements such as [CPS.PR.PS-08](#), [CPS.DE.CM-02](#), [CPS.DE.CM-04](#), [CPS.DE.CM-08](#)~~CPS.IP-10~~, ~~CPS.CM-3~~, ~~CPS.CM-6~~ describe the process of securing IoT devices. The organization should refer to these items when considering security measures for IoT devices.

➤—Related measure requirements include [CPS.ID.RA-03](#), [CPS.ID.RA-04](#), [CPS.ID.RA-06](#), [CPS.PR.PS-01](#), [CPS.PR.PS-03](#), [CPS.PR.PS-07](#), [CPS.DE.CM-02](#), [CPS.DE.CM-04](#), and [CPS.DE.CM-06](#).~~CPS.RA-4~~, ~~CPS.RA-6~~, ~~CPS.DS-10~~, ~~CPS.DS-12~~, ~~CPS.DS-15~~, ~~CPS.CM-6~~ and ~~CPS.CM-7~~.

- The third layer requires that data in cyberspace and its processing, analysis, and storage be reliable.
- To ensure trustworthiness, it is essential that the data is reliable, in addition to the important points in the first layer and the second layer stated above. Specifically, the data should be checked to determine whether it has been falsified, is in the acceptable range (e.g., the data is free from exploit code), and it has been generated by and sent from authorized elements (e.g., “organization”, people, components).
- Data that is particularly important to the organization’s business continuity should be checked for trustworthiness by the entity that has created and processed the data. Data sent to the organization should be quality and security checked when received (e.g., checking the data for falsification or exploit code). The organization must also monitor security compliance of data processing and analysis components and systems.

➤—Related measure requirements include [CPS.ID.AM-01](#), [CPS.PR.AA-02](#), [CPS.PR.DS-05](#), [CPS.PR.IR-01](#), [CPS.DE.CM-03](#), [CPS.DE.CM-07](#), and [CPS.DE.CM-08](#).~~CPS.DS-9~~, ~~CPS.DS-14~~, ~~CPS.AE-1~~, ~~CPS.CM-3~~, ~~CPS.CM-4~~ and ~~CPS.CM-5~~.

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

Point of view to identify the risk sources	An example of Corresponding Measure Requirements
--	--

Relationships with stakeholders involved in the value creation process	<u>CPS.GV.OC-03, CPS.GV.RR-02,</u> <u>CPS.GV.PO-01, CPS.GV.SC-04,</u> <u>CPS.GV.SC-05, CPS.ID.AM-03</u> ~~CPS.AM-5,~~ ~~CPS.AM-7, CPS.BE-2, CPS.BE-3, CPS.SC-~~ ~~1, CPS.SC-2, CPS.DS-13, CPS.CM-4~~
Integration of cyberspace and physical space through IoT devices	<u>CPS.ID.RA-03, CPS.ID.RA-04, CPS.ID.RA-</u> <u>06, CPS.PR.AA-07, CPS.PR.DS-02,</u> <u>CPS.PR.DS-03, CPS.PR.PS-02, CPS.PR.PS-</u> <u>03, CPS.PR.PS-06, CPS.PR.PS-12,</u> <u>CPS.PR.IR-02, CPS.PR.IR-04, CPS.DE.CM-</u> <u>05, CPS.DE.CM-07, CPS.DE.CM-08</u> ~~CPS.RA-4, CPS.RA-6, CPS.PT-3, CPS.CM-3~~
Cross-organizational data flows	<u>CPS.GV.SC-02, CPS.GV.SC-06,</u> <u>CPS.GV.SC-07, CPS.GV.SC-08,</u> <u>CPS.DE.CM-01, CPS.DE.CM-03,</u> <u>CPS.DE.CM-07, CPS.RS.MA-04,</u> <u>CPS.RC.CO-01</u> ~~CPS.SC-3, CPS.SC-4,~~ ~~CPS.SC-6, CPS.CM-1, CPS.CM-3, CPS.CM-~~ ~~4, CPS.DP-1, CPS.RP-2, CPS.CO-1~~
Securing a base level of trustworthiness in each layer	<u>CPS.GV.SC-06, CPS.GV.SC-07,</u> <u>CPS.GV.SC-08, CPS.GV.SC-12, CPS.ID.AM-</u> <u>01, CPS.ID.RA-03, CPS.ID.RA-04,</u> <u>CPS.ID.RA-06, CPS.PR.AA-02, CPS.PR.DS-</u> <u>05, CPS.PR.PS-01, CPS.PR.PS-03,</u> <u>CPS.PR.PS-07, CPS.PR.IR-01,</u> <u>CPS.DE.CM-02, CPS.DE.CM-03,</u> <u>CPS.DE.CM-04, CPS.DE.CM-06,</u> <u>CPS.DE.CM-07, CPS.DE.CM-08</u> ~~CPS.RA-4,~~ ~~CPS.RA-6, CPS.SC-3, CPS.SC-4, CPS.SC-~~ ~~6, CPS.DS-10, CPS.DS-12, CPS.CM-4,~~ ~~CPS.CM-5~~

2. Relationship between risk sources and measure requirements

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

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

Function	Assumed security incident	Risk sources			Measure Requirements	Measure Requirement ID
		Threat	Vulnerability ID	Vulnerability		
All of the following functions: - Functions to securely send and receive data - Functions to securely process and analyze data - Functions to securely store data	- DoS attacks on computer equipment and communication devices (e.g., servers) that comprise a system	- DoS attack on computing devices such as servers, communication devices, etc. - Transmission of jamming waves	L3_3_b_ORG	[Organization] - The organization does not confirm the trustworthiness of contractor organizations such as data providers or data manipulators/analyzers before and after signing contracts.	~~Identify and prioritize the organizations and people that play an important role relevant in each layer of the three-layer structure to sustain business operations. Identify, prioritize, and evaluate the organizations and people that play important role relevant in each layer of the three-layer structure to sustaining the operation of the organization.~~	~~CPS.GV.SC-04CPS-SC-2~~
					Before concluding contracts with suppliers and other third parties, evaluate the cybersecurity management posture of said suppliers and third parties, and take necessary measures to mitigate risks as needed. When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.	~~CPS.GV.SC-06CPS-SC-3~~

	The system that handles data stops whether it has been attacked or not.	- Services provided by a system with low quality/trustworthiness	L3_3_c_SYS	[System] - A system that contains IoT devices does not have adequate resources (i.e., processing capacity, communication bandwidths, and storage capacity)	~~Secure sufficient resources (e.g., people, components, and systems) to minimize the impact of attacks and maintain critical functions, even in the event of cyberattacks such as ransomware or denial-of-service (DoS) attacks.~~ Secure sufficient resources (Ex: People, Components, System) for components and systems, and protect assets property to minimize bad effects of cyberattack (e.g., DoS attack).	~~CPS.PR.IR-04~~ CPS-DS-6
--	---	--	------------	---	--	----------------------------------

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

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

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

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

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

Part III and Appendix C are guides not only to the risk response phase, but also to the entire risk management process.~~Part III and Appendix C are guides to the risk response phase of the risk management process.~~ An enterprise organization can use the contents in this part for the following purposes:

(1) Strengthening the organization's security management

As stated in Part II, Section 1.4, an enterprise organization can improve its ~~risk~~ security management by implementing security measure requirements described in Part III and examples described in Appendix C in accordance with the results of the risk assessment and by properly executing risk management processes. As described in “Introduction: 7. How to use the Framework,” the process is expected to contribute to the security measures of each organization in two ways:

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

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

The security measures described in Appendix C are just examples. They do not exclude other security methods, nor are they absolute requirements for

all organizations. It is always necessary for any organization to make its own determination of appropriate security measures based on risk assessment and analysis.

For (ii), Appendix C includes points of alignment between the measure requirements and major international standards. It organizes the comparison with the measure items across standards such as NIST SP 800-171, NIST SP 800-53 Rev. 5, ISO/IEC 27001:2022, and IEC 62443 according to the level of examples of security measures. ~~Especially, Appendix C organizes the comparison with the measure items of NIST SP800-171, NIST SP800-53 Rev.4, ISO/IEC 27001:2013 and IEC 62443 according to the level of examples of security measures.~~ In addition, Appendix D organizes the correspondence relationship with the measure requirements that the Framework presents based on major international standards etc. in a table format. Implementation of the Framework is intended to help the organization simultaneously comply with these standards without requiring additional actions.

(2) Setting current and target levels

Organizations can use the measure requirements presented in Part III and the examples of security measures shown in Appendix C to understand the current level of their security measures and set their target level. The current level reflects the current implementation status of the organization's security measures, while the target level indicates the implementation status of security measures that the organization should achieve in the future. Specifically, the level classifications of security measure examples shown in Appendix C (High-Advanced, Advanced, and Basic) can serve as a reference for setting such levels.

Organizations first set the classification level to be achieved as their target level, based on factors including their business characteristics, risk profile, and available resources. Next, organizations determine their current level by verifying the extent to which the example measures shown in Appendix C have been implemented. After that, by analyzing the gap between the target level and the current level, it becomes possible to clarify the measures that the organization should prioritize, leading to improvements in the organization's security management.

Furthermore, it is important for organizations to periodically review their

current and target levels, taking into account the status of implementation of measures and changes in the risk environment.

While the Framework provides the examples of security measures in Appendix C as a reference when setting current and target levels, adopting these indicators is not mandatory. Organizations can also flexibly utilize maturity indicators, control levels, or similar metrics used in other cybersecurity-related guidelines and frameworks.

(3) Improving communication in risk management

This framework can be utilized to improve communication in risk management among senior management, managers, and practitioners (see Figure 3.1-1).

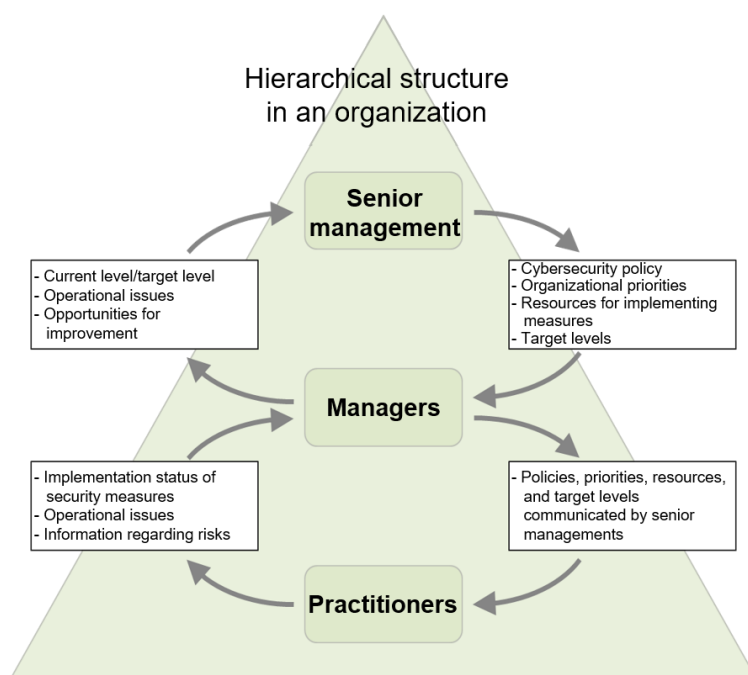


Figure 3.1-1 Improving risk management communication using the CPSF

Practitioners collect information regarding the implementation status of security measures, operational issues, and risks in their own organization, and share it with managers. (This corresponds to measure requirements such as CPS.GV.OV-02 and CPS.GV.RM-06.)

Based on the information shared by practitioners, managers assess the current level and set the target level as shown in the preceding section (2), analyze the gaps to organize issues and opportunities for improvement, and

share them with senior management. (This corresponds to measure requirements such as CPS.GV.OV-02 and CPS.GV.RM-06.)

Based on the analysis results and related information shared by managers, senior management makes decisions on or reviews organizational goals, priorities, resources, etc., and disseminates the outcomes to practitioners through managers. (This corresponds to measure requirements such as CPS.GV.RR-02 and CPS.GV.OV-01.)

Continuously executing this series of processes leads to improved risk management communication throughout the entire organization.

Current and target levels can be utilized as common indicators for sharing security risks, the priority of security measures to be implemented, and improvement status among senior management, managers, and practitioners. This makes it possible to form a shared understanding of risks across the entire organization, supporting decision-making and continuous improvement.

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

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

Security measure requirements that state a set of processes the organization shall require from partners include CPS.GV.SC-01, CPS.GV.SC-05, CPS.GV.SC-06, CPS.GV.SC-07, CPS.GV.SC-08, CPS.GV.SC-09, CPS.GV.SC-10, and CPS.GV.SC-11.~~CPS.SC-2, CPS.SC-3, CPS.SC-4, and CPS.SC-6.~~¹⁶ By implementing those processes effectively, organizations can ensure governance for contractors through their contract lifecycle.

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

Also, the organization may wish to maintain the security risk management

¹⁶ When requiring partners to implement security measures, it is important to present not only specific measure requirements, but also the comprehensive overview, including the objectives and policies of the organization's supply chain risk management as well as the security standards required of partners. Implementing initiatives based on CPS.GV.SC-01 and CPS.GV.SC-05 enables organizations to communicate these details to partners.

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

2. How to use examples of security measures

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

Table 3.2-1 Example of description in Appendix C

Measure Requirement ID	Measure Requirement	Examples of Security Measures	Subject that implements measures	NIST SP 800-171	NIST SP 800-53	ISO/IEC 27001 Annex A	IEC 62443
		<High-Advanced>	O/S	○	○		○
		<Advanced>	O		○	○	
		<Basic>	O		○	○	

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

The organization needs to refer to the importance assigned to the business, system, etc. that is required to be dealt with in CPS.GV.SC-04~~CPS.AM-5~~ and CPS.ID.AM-04~~CPS.BE-2~~, and take the appropriate measures from High-Advanced, Advanced, Basic. For example, it is possible to assign importance as shown in Table 3.2-2 from the viewpoint of confidentiality, integrity, and availability for business operations, systems, etc. Organizations need to materialize values and evaluation criteria, etc., taking into account their own specific conditions.

Table 3.2-2 Example of importance and evaluation criteria for classifying information asset based on confidentiality, integrity, availability¹⁷

Importance		Evaluation criteria
Confidentiality		The law requires appropriate management (leakage, loss or damage prevention).
	~~32~~	Identified as a subject of confidentiality or “Data for Limited Provision”. There is a significant impact on business partners and customers if leaked.
		There is a serious impact on the organization if leaked because information that should be managed as trade secret.
	~~24~~	There is a significant impact on the organization's business if leaked.
	~~10~~	There is almost no impact on the organization's business even if leaked.
Integrity	~~32~~	The law requires appropriate management (leakage, loss or damage prevention). There is a serious impact on the organization or a significant impact on business partners and customers if it is tampered with.
	~~24~~	There is a significant impact on the organization's business if it is tampered with.
	~~10~~	There is almost no impact on the organization's business even if it is tampered with.
Availability	~~32~~	There is a serious impact on the organization or a significant impact on business partners and customers if it becomes unavailable.
	~~24~~	There is a significant impact on the organization's business if it becomes unavailable.
	~~10~~	There is almost no impact on the organization's business even if it becomes unavailable.

Similar security measure requirements may be needed at different levels. For example, “<Advanced> and <Basic>” may both require the same protection in some areas. This calls for the implementation of the same measures in

¹⁷ This description references the approach outlined on page 29 and “Appendix 6: Asset Management Ledger (Sample)” of the Information Security Measures Guidelines for Small and Medium sized Enterprises, Version 3.1 (IPA, 2023). In particular, with regard to industrial control systems, in addition to the effects that are generally assumed in information systems in “Importance” or “Evaluation criteria”, the effects on safety, environment, and health should also be considered.

<Advanced> and <Basic>. Also, the measure requirement described as “N / A” in <Basic> indicates that the implementation priority of the measure requirement is not necessarily high in cases where resources for implementation are severely limited, or when the importance of System and Components to be implemented for measures is not high.

The column “Subject that implements measures” classifies security measures¹⁸ three ways. The subject is classified as “S” if the measures are generally implemented by a system through technical means, as “O” if the measures are implemented by an organization (e.g., by people through non-technical means), and as “O/S” if the measures are implemented by both a system and an organization.

The measures described in the “Examples of Security Measures” are just references to meet the measure requirements. It is possible to satisfy security requirement through the measures that are not described. Therefore, the “Examples of Security Measures” should be used for the implementation of proper measures that take into account costs in each organization as well as for comparisons with relevant international standards.

3. Security measure requirements

~~Tables 3.3-2 to 3.3-23 show the measure requirements for each category. In the Framework, the measure requirements shown in Tables 3.3-2 to 3.3-23 are shown for each category.~~

In the Framework, from the viewpoint of international harmonization, the measures to be implemented in the risk management process are organized into a structure consisting of Functions, Categories, and Measure Requirements, drawing upon the concepts of international frameworks.

The six Functions outlined below categorize cybersecurity activities at the highest level.

- i Govern (GV): Establishes the organization’s cybersecurity risk management strategy, policy, and roles. It also helps inform the direction and prioritization of activities across other Functions, taking into account the organization’s mission and stakeholder expectations.

¹⁸ The notation is in accordance with “NIST SP 800-53 Rev.5 APPENDIX C”.

- ii Identify (ID): Identifies the organization's assets, suppliers, and cybersecurity risks, and prioritizes efforts based on risk. It also identifies opportunities for improvement in policies, plans, processes, procedures, and practices that support risk management.
- iii Protect (PR): Implements safeguards based on identified assets and risks to prevent or reduce the likelihood and impact of the occurrence of adverse security events.
- iv Detect (DE): Finds and analyzes anomalies, indicators of compromise, and other potentially adverse events indicating the occurrence of cyberattacks and security incidents.
- v Respond (RS): Manages, analyzes, mitigates, and reports on detected security incidents to contain their impact.
- vi Recover (RC): Restores assets and operations affected by security incidents.

Categories and Measure Requirements represent progressive elaborations of each Function. Note that the sequence of Functions, Categories, and Measure Requirements does not indicate the implementation order or priority of the measures. Additionally, it should be noted that specific implementation methods for satisfying Measure Requirements may vary depending on the organization's business characteristics, risk profile, available resources, and other factors.

(1) List of measure requirement categories

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

Table 3.3-1 Structure of measure requirements in this Framework~~List of measure requirement categories and related category of NIST Cybersecurity Framework Ver. 1.1~~

<u>Function</u>	<u>Category</u> Category name	<u>Category ID</u> Acronym	<u>Measure Requirement ID</u> Related category of NIST— Cybersecurity Framework Ver. 1.1
<u>Govern</u> (GV)	<u>Organizational Context</u>	<u>GV.OC</u>	<u>CPS.GV.OC</u>
	<u>Asset Management</u>	<u>CPS.AM</u>	<u>ID.AM (Asset Management)</u>
	<u>Risk Management Strategy</u> <u>Business Environment</u>	<u>GV.RM</u> <u>CPS.BE</u>	<u>CPS.GV.RM</u> <u>ID.BE (Business Environment)</u>

<u>Function</u>	<u>Category</u> <u>Category-name</u>	<u>Category ID</u> <u>Acronym</u>	<u>Measure Requirement ID</u> <u>Related-category of NIST–</u> <u>Cybersecurity Framework Ver. 1.1</u>
	<u>Roles, Responsibilities, and Authorities</u> <u>Governance</u>	<u>GV.RR</u> CPS.GV	<u>CPS.GV.RR</u> ID.GV (Governance)
	<u>Policy</u> <u>Risk Assessment</u>	<u>GV.PO</u> CPS.RA	<u>CPS.GV.PO</u> ID.RA (Risk Assessment)
	<u>Oversight</u> <u>Risk Management Strategy</u>	<u>GV.OV</u> CPS.RM	<u>CPS.GV.OV</u> ID.RM (Risk Management Strategy)
	<u>Cybersecurity Supply Chain Risk Management</u> <u>Supply Chain Risk–</u> <u>Management</u>	<u>GV.SC</u> CPS.SC	<u>CPS.GV.SC</u> ID.SC (Supply Chain Risk Management)
<u>Identify</u> <u>(ID)</u>	<u>Asset Management</u> <u>Identity Management,–</u> <u>Authentication, and Access–</u> <u>Control</u>	<u>ID.AM</u> CPS.AC	<u>CPS.ID.AM</u> PR.AC (Identity Management and– Access Control)
	<u>Risk Assessment</u> <u>Awareness and Training</u>	<u>ID.RA</u> CPS.AT	<u>CPS.ID.RA</u> PR.AT (Awareness and Training)
	<u>Improvement</u> <u>Data Security</u>	<u>ID.IM</u> CPS.DS	<u>CPS.ID.IM</u> PR.DS (Data Security)
<u>Protect</u> <u>(PR)</u>	<u>Identity Management,–</u> <u>Authentication, and Access</u> <u>Control</u> <u>Information Protection–</u> <u>Processes and Procedures</u>	<u>PR.AA</u> CPS.IP	<u>CPS.PR.AA</u> PR.IP (Information Protection Processes and Procedures)
	<u>Awareness and Training</u> <u>Maintenance</u>	<u>PR.AT</u> CPS.MA	<u>CPS.PR.AT</u> PR.MA (Maintenance)
	<u>Data Security</u> <u>Protective Technology</u>	<u>PR.DS</u> CPS.PT	<u>CPS.PR.DS</u> PR.PT (Protective Technology)
	<u>Platform Security</u> <u>Anomalies and Events</u>	<u>PR.PS</u> CPS.AE	<u>CPS.PR.PS</u> DE.AE (Anomalies and Events)
	<u>Technology Infrastructure</u> <u>Resilience</u> <u>Security Continuous–</u>	<u>PR.IR</u> CPS.CM	<u>CPS.PR.IR</u> DE.CM (Security Continuous– Monitoring)

<u>Function</u>	<u>Category</u> <u>Category-name</u>	<u>Category ID</u> <u>Acronym</u>	<u>Measure Requirement ID</u> <u>Related-category of NIST</u> <u>Cybersecurity Framework Ver. 1.1</u>
	Monitoring		
<u>Detect</u> <u>(DE)</u>	<u>Continuous Monitoring</u> <u>Detection Processes</u>	<u>DE.CM</u> <u>CPS.DP</u>	<u>CPS.DE.CM</u> <u>DE.DP (Detection Processes)</u>
	<u>Adverse Event Analysis</u> <u>Response Planning</u>	<u>DE.AE</u> <u>CPS.RP</u>	<u>CPS.DE.AE</u> <u>RS.RP (Response Planning)</u> <u>RC.RP (Recovery Planning)</u>
<u>Respond</u> <u>(RS)</u>	<u>Incident Management</u> <u>Communications</u>	<u>RS.MA</u> <u>CPS.CO</u>	<u>CPS.RS.MA</u> <u>RS.CO (Communications)</u> <u>RC.CO (Communications)</u>
	<u>Incident Analysis</u> <u>Analysis</u>	<u>RS.AN</u> <u>CPS.AN</u>	<u>CPS.RS.AN</u> <u>RS.AN (Analysis)</u>
	<u>Incident Response</u> <u>Reporting and</u> <u>Communication</u> <u>Mitigation</u>	<u>RS.CO</u> <u>CPS.MI</u>	<u>CPS.RS.CO</u> <u>RS.MI (Mitigation)</u>
	<u>Incident Mitigation</u> <u>Improvements</u>	<u>RS.MI</u> <u>CPS.IM</u>	<u>CPS.RS.MI</u> <u>RS.IM (Improvements)</u> <u>RC.IM (Improvements)</u>
<u>Recover</u> <u>(RC)</u>	<u>Incident Recovery Plan</u> <u>Execution</u>	<u>RC.RP</u>	<u>CPS.RC.RP</u>
	<u>Incident Recovery</u> <u>Communication</u>	<u>RC.CO</u>	<u>CPS.RC.CO</u>

~~(2) Alignment with major standards~~

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

- ~~* NIST “Framework for Improving Critical Infrastructure Cybersecurity—Version 1.1” (NIST Cybersecurity Framework Ver. 1.1)~~
- ~~* Council on CyberSecurity (the Council) “The Critical Security Controls” (CIS CSC)~~
- ~~* ISACA “Control Objectives for Information-related Technology 5” (COBIT 5)~~
- ~~* ISA 62443-2-1:2010 “Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program”~~
- ~~* ISA 62443-3-3:2013 “Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels”~~
- ~~* ISO/IEC 27001:2013 “Information technology -- Security techniques -- Information security management systems -- Requirements”¹⁹~~
- ~~* NIST “Special Publication 800-53 Revision 4” (SP 800-53 Rev.4)~~
- ~~* “Common Criteria for Information Technology Security Evaluation—Version 3.1 Revision 5” (CC v3.1 Release 5)~~
- ~~* Ministry of Economy, Trade and Industry (METI) and IPA “Cybersecurity Management Guidelines Ver. 2.0”~~
- ~~* IoT Acceleration Consortium, Ministry of Internal Affairs and Communications, METI “IoT Security Guidelines Ver. 1.0”~~

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

3.1 CPS.GV – Govern

The organization establishes its cybersecurity risk management strategy, policy, and roles. It also helps inform the direction and prioritization of activities across other Functions, taking into account the organization's mission and stakeholder expectations.

3.1.1 CPS.GV.OC – Organizational Context CPS.AM – Asset Management

The organization understands the context surrounding cybersecurity risk management decision-making (e.g., mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements). Identify assets (e.g. data, people, goods, systems, zone where assets are managed, etc.) that are important to the organization's business and manage risk in accordance with its risk analysis and tolerance.

Table 3.3-2 Measure requirements for the **GV.OC** category

ID	Measure Requirement
<u>CPS.GV.OC-01</u> ~~CPS.AM-4~~	<u>The organization understands its mission and uses it to inform cybersecurity risk management decisions.</u> ~~Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.~~
<u>CPS.GV.OC-02</u> ~~CPS.AM-2~~	<u>The organization understands legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil liberties obligations—as well as industry guidelines, and establishes internal rules that appropriately reflect and address these requirements or guidelines.</u> ~~Specify a method to ensure traceability based on the importance of the components produced by the organization's supply chain.~~
<u>CPS.GV.OC-03</u> ~~CPS.AM-3~~	<u>The organization identifies dependencies and critical functions across both its own organization and related external entities to sustain business operations, and shares them with those external entities.</u> ~~Create records such as the date of production and condition of components depending on importance, and prepare and adopt internal rules regarding records of production activities in order to store components for a certain period of time.~~
~~CPS.AM-4~~	~~Create and manage appropriately network configuration diagrams and data flows within the organization.~~
~~CPS.AM-5~~	~~Create and manage appropriately a list of external information systems where the organization's assets are shared.~~
~~CPS.AM-6~~	~~Classify and prioritize resources (e.g., People, Components, Data, and System) by function, importance, and business value, and communicate to the organizations and people relevant to those resources in business~~

~~CPS-AM-7~~

~~Define roles and responsibilities for cyber security across the organization and other relevant parties.~~

3.1.2 CPS.GV.RM – Risk Management StrategyCPS.BE – Business Environment

To support decision-making regarding operational risk, the organization establishes its priorities, constraints, risk tolerance, risk appetite, and assumptions, and communicates them to relevant stakeholders. Understand and prioritize the mission, goals, stakeholders, and activities of the organization. This information is used to convey cyber security roles, responsibilities and risk management decisions.

Table 3.3-3 Measure requirements for the **GV.RM** category

ID	Measure Requirement
CPS.GV.RM-01 CPS.BM-4	The organization defines risk management objectives and agrees on them with relevant stakeholders. Identify and share the role of the organizations in the supply chain.
CPS.GV.RM-02 CPS.BM-2	The organization develops a cybersecurity strategy to ensure effective cybersecurity risk management. Define policies and standard measures regarding security that are consistent with the high-priority business and operations of the organization, and share them with parties relevant to the organization's business (including suppliers and third-party providers).
CPS.GV.RM-03 CPS.BM-3	The organization establishes its risk appetite and risk tolerance, and communicates them across the organization. Identify the dependency between the organization and other relevant parties and the important functions of each in the course of running the operation.
CPS.GV.RM-04	The organization integrates cybersecurity risk management activities and their outcomes into the organizational risk management process, managing cybersecurity risks within that process.
CPS.GV.RM-05	The organization formulates policies regarding risk response options and their operations, and shares them within the organization.
CPS.GV.RM-06	The organization establishes and maintains lines of communication across the organization regarding cybersecurity risks, including risks posed by partners and other third parties.
CPS.GV.RM-07	The organization standardizes methodologies for assessing, documenting, classifying, and prioritizing cybersecurity risks, and shares them within the organization.
CPS.GV.RM-08	The organization identifies strategic opportunities (positive risks for the organization), clarifies their characteristics, and integrates them into organizational cybersecurity risk deliberations.

3.1.3 CPS.GV.RR – Roles, Responsibilities, and AuthoritiesCPS.GV – Governance

The organization establishes and communicates cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement. Understand policies, procedures and processes for managing and monitoring compliance with regulations, laws, risks, internal policies, and operational requirements for the organization, and communicate them to cybersecurity risk managers.

Table 3.3-4 Measure requirements for the **GV.RR** category

ID	Measure Requirement
CPS.GV.RR-01 CPS.GV-4	Organizational senior management is responsible and accountable for cybersecurity risk, fostering a culture that is risk-aware, ethical, and continually improving. Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.
CPS.GV.RR-02 CPS.GV-2	The organization establishes roles, responsibilities, and authorities related to its cybersecurity risk management and communicates them within the organization. Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.
CPS.GV.RR-03 CPS.GV-3	The organization appoints a security manager, establishes a security response organization (SOC/CSIRT), and maintains a structure to detect, analyze, and respond to security incidents within the organization. Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.
CPS.GV.RR-04 CPS.GV-4	The organization allocates necessary resources commensurate with its cybersecurity strategy, roles, responsibilities, and policies. Develop a strategy and secure resources to implement risk management regarding security.
CPS.GV.RR-05	The organization incorporates security-related matters (e.g., revoking access privileges and screening employees) into measures that address role changes resulting from personnel transfers.

3.1.4 CPS.GV.PO – PolicyCPS.RA – Risk Assessment

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

Table 3.3-5 Measure requirements for the GV.PO category

ID	Measure Requirement
<u>CPS.GV.PO-01</u> <u>CPS.RA-1</u>	<u>The organization formulates security policies based on its organizational context, cybersecurity strategy, and priorities, communicates them within the organization and to relevant external parties (including suppliers and third-party providers, as needed), and implements them.</u> <u>Identify the vulnerability of the organization's assets and document the list of identified vulnerability with the corresponding asset.</u>
<u>CPS.GV.PO-02</u> <u>CPS.RA-2</u>	<u>The organization periodically reviews its security policies and updates them as necessary, based on changes in requirements, threats, technology, and the organization's mission.</u> <u>The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.), analyzes the information, and establishes a process to implement and use measures.</u>
<u>CPS.RA-3</u>	<u>Identify and document the assumed security incidents, those impacts on the organization's assets, and the causes of those.</u>
<u>CPS.RA-4</u>	<u>- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation.</u> <u>- Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.</u>
<u>CPS.RA-5</u>	<u>Consider threats, vulnerability, likelihood, and impacts when assessing risks.</u>
<u>CPS.RA-6</u>	<u>- On the basis of the results of the risk assessment, clearly define the details of measures to prevent possible security risks, and document the organized outcome from the scope and priorities of the measures.</u> <u>- React accordingly to the security risks and the associated safety risks identified as a result of the assessment conducted at the planning and design phase of an IoT device and systems incorporating IoT devices.</u>

3.1.5 CPS.GV.OV – OversightCPS.RM – Risk Management Strategy

The organization monitors the progress and outcomes of cybersecurity risk management activities across the organization, using this information to review and improve its risk management strategy. ~~Set priority, constraint, and risk tolerance assumptions for the organization and use it to judge investment risk.~~

Table 3.3-6 Measure requirements for the **GV.OV** category

ID	Measure Requirement
<u>CPS.GV.OV-01</u> ~~CPS.RM-1~~	<u>The organization reviews the outcomes of its cybersecurity strategy and, taking into account these results and changes in the internal and external context, revises the cybersecurity strategy as well as enterprise-wide strategy and direction as necessary.</u> ~~Confirm the implementation status of the organization's' cyber security risk management and communicate the results to appropriate parties within the organization (e.g. senior management). Define the scope of responsibilities of the organization and the relevant parties (e.g. subcontractor), and establish and implement the process to confirm the implementation status of security risk management of relevant parties.~~
<u>CPS.GV.OV-02</u> ~~CPS.RM-2~~	<u>The organization reviews the implementation status of its cybersecurity risk management and updates it as necessary.</u> ~~Determine the organization's risk tolerance level based on the result of the risk assessment and its role in the supply chain.~~

3.1.6 CPS.GV.SC – Supply Chain Risk Management ~~CPS.SC – Supply Chain Risk Management~~

~~The organization, in collaboration with its stakeholders, identifies, establishes, manages, monitors, and improves cybersecurity supply chain risk management processes. Establish enterprise priorities, constraints, risk tolerances, and assumptions and use them to assist in analysis of supply chain risk management. Establish and implement the process of identifying, evaluating and managing supply chain risks.~~

Table 3.3-7 Measure requirements for the **GV.SC** category

ID	Measure Requirement
<u>CPS.GV.SC-01</u> ~~CPS.SC-4~~	<u>The organization establishes supply chain risk management programs, strategies, objectives, policies, and processes, and operates them upon agreement with organizational stakeholders.</u> ~~Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.~~
<u>CPS.GV.SC-02</u> ~~CPS.SC-2~~	<u>The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary.</u> ~~Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.~~
<u>CPS.GV.SC-03</u> ~~CPS.SC-3~~	<u>The organization integrates cybersecurity supply chain risk management into its cybersecurity and enterprise risk management, risk assessment, and improvement processes.</u> ~~When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.~~
<u>CPS.GV.SC-04</u> ~~CPS.SC-4~~	<u>The organization identifies and prioritizes organizations and people that play an important role relevant in each layer of the three-layer structure to sustain business operations.</u> ~~When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.~~

<u>CPS.GV.SC-05</u> ~~CPS.SC-5~~	<u>The organization establishes supply chain cybersecurity standards considering the lifecycle of business relationships, clearly defines the scope of responsibilities, and agrees on them with partners through contracts or other means.</u> ~~Formulate and manage security requirements applicable to members of other relevant organizations, such as business partners, who are engaged in operations outsourced from the organization.~~
<u>CPS.GV.SC-06</u> ~~CPS.SC-6~~	<u>Before concluding contracts with suppliers and other third parties, the organization evaluates the cybersecurity management posture of said suppliers and third parties, and takes necessary measures to mitigate risks as needed.</u> ~~Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.~~
<u>CPS.GV.SC-07</u> ~~CPS.SC-7~~	<u>When entering into contracts with other relevant organizations such as business partners, the organization considers its objectives and risk management outcomes, verifying that products and services provided by them conform to the organization's security requirements.</u> ~~Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.~~
<u>CPS.GV.SC-08</u> ~~CPS.SC-8~~	<u>The organization periodically evaluates other relevant organizations such as business partners using audits, test results, or other forms of assessment to confirm that they are fulfilling their contractual obligations.</u> ~~Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.~~
<u>CPS.GV.SC-09</u> ~~CPS.SC-9~~	<u>The organization establishes and implements procedures to be followed when non-compliance with contractual requirements is identified through audits or testing of other relevant organizations such as business partners.</u> ~~Prepare and test a procedure for incident response with relevant parties involved in the incident response activity to ensure action for incident response in the supply chain.~~
<u>CPS.GV.SC-10</u> ~~CPS.SC-10~~	<u>The organization monitors the implementation of supply chain security measures across the lifecycle of technology products and services.</u> ~~Develop and manage a procedure to be executed when a contract with other relevant organizations such as business partners is finished. (e.g., expiration of contract period, end of support)~~
<u>CPS.GV.SC-11</u> ~~CPS.SC-11~~	<u>The organization establishes and implements procedures to be followed upon the termination of contracts with partners and other parties.</u> ~~Continuously improve the standard of security measures relevant to the supply chain, related procedures, and so on.~~

CPS.GV.SC-12

The organization collects and securely retains information (data) to demonstrate that it is fulfilling its contractual obligations to other relevant organizations and individuals, ensuring it can be disclosed to an appropriate extent when necessary.

3.2 CPS.ID – Identify

The organization identifies its assets, suppliers, and cybersecurity risks, and prioritizes efforts based on risk. It also identifies opportunities for improvement in policies, plans, processes, procedures, and practices that support risk management.

3.2.1 CPS.ID.AM – Asset ManagementCPS.AC – Identity Management, Authentication and Access Control

The organization identifies assets necessary for achieving business purposes (e.g., data, hardware, software, systems, facilities, services, and personnel) and manages these assets according to their importance to the organization's objectives and strategy. Limiting logical and physical access to assets and related zone to approved "organization", people, goods and procedures and manage them to limit the risk of unauthorized access and to ensure only approved activities and transactions are accessible.

Table 3.3-8 Measure requirements for the ID.AM category

ID	Measure Requirement
CPS.ID.AM-01 CPS.AC-4	The organization develops and appropriately manages inventories of hardware, software, and their management information (e.g., name, version, network address, designated manager, and license information) that comprise its system. Establish and implement procedures to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.
CPS.ID.AM-02 CPS.AC-2	The organization develops and appropriately manages communication network diagrams and data flow diagrams within the organization. Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.
CPS.ID.AM-03 CPS.AC-3	The organization develops and appropriately manages inventories of external information systems connected to its organizational assets. Properly authorize wireless connection destinations (including users, IoT devices, and servers).
CPS.ID.AM-04 CPS.AC-4	The organization categorizes and prioritizes resources (e.g., components, data, and systems) based on their function, criticality, and business value, defines management responsibilities, and communicates them to relevant organizations and people involved in their operation. Prevent unauthorized log-in to IoT devices and servers by measures such as implementing functions for lockout after a specified number of incorrect log-in attempts and providing a time interval until safety is ensured.
CPS.ID.AM-05 CPS.AC-5	The organization develops and appropriately manages inventories of data and metadata in its possession.

	Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions).
<u>CPS.ID.AM-06</u> ~~CPS.AC-6~~	<u>The organization manages systems, hardware, software, services, and data throughout their entire lifecycle, from acquisition to disposal.</u> ~~Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.~~
<u>CPS.ID.AM-07</u> ~~CPS.AC-7~~	<u>The organization establishes identification methods to ensure traceability according to the importance of the components it produces within the supply chain.</u> ~~Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).~~
<u>CPS.ID.AM-08</u> ~~CPS.AC-8~~	<u>The organization prepares and implements internal rules regarding records of production activities in order to create records concerning production date and time, conditions, and states, and store them for a certain period according to importance.</u> ~~Restrict communications by IoT devices and servers to those with entities (e.g. people, components, system, etc.) identified through proper procedures.~~
~~CPS.AC-9~~	~~Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).~~

3.2.2 CPS.ID.RA – Risk AssessmentCPS.AT – Awareness and Training

The organization understands the cybersecurity risks to its personnel and assets. Implement cybersecurity awareness education and training to internal organization staff and partners to ensure fulfillment of contractual obligations, based on relevant policies, procedures and contracts.

Table 3.3-9 Measure requirements for the ID.RA category

ID	Measure Requirement
CPS.ID.RA-01 CPS.AT-1	The organization identifies vulnerabilities in its assets and manages them by linking them to the corresponding assets. Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.
CPS.ID.RA-02 CPS.AT-2	The organization establishes a process to collect, analyze, respond to, and utilize vulnerability and threat information from internal and external sources (e.g., internal tests, security information, and security researchers). Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.
CPS.ID.RA-03 CPS.AT-3	- The organization identifies and documents potential security incidents, their impacts, and their causal factors regarding organizational assets. - From the planning and design stages of IoT devices and IoT-integrated systems, the organization verifies that no unacceptable known security risks exist, incorporating safety hazard perspectives. Improve the contents of training and education regarding security to members of the organization and other relevant parties of high importance in security management of the organization.
CPS.ID.RA-04	The organization identifies the potential impact and likelihood of threats exploiting vulnerabilities by periodically conducting risk assessments to evaluate the effectiveness of security rules for component management, including their implementation methods.
CPS.ID.RA-05	The organization shares information regarding the effectiveness of protective technologies with appropriate partners.

<u>CPS.ID.RA-06</u>	- Based on risk assessments, the organization clearly defines response measures for potential security risks, documents the defined scope and priorities of response actions, monitors the implementation progress, and communicates this status to relevant parties. - The organization appropriately addresses security and associated safety risks identified through the assessment in the planning and design stages of IoT devices and IoT-integrated systems.
<u>CPS.ID.RA-07</u>	The organization assesses the risk impact posed by significant organizational changes and security requirement exceptions, and records and manages the results.

3.2.3 CPS.ID.IM – ImprovementCPS.DS – Data Security

The organization improves its cybersecurity risk management processes, procedures, and activities. ~~Manage information according to the organization's risk strategy, using the core security principles of confidentiality, integrity and availability of data.~~

Table 3.3-10 Measure requirements for the **ID.IM** category

ID	Measure Requirement
<u>CPS.ID.IM-01</u> ~~CPS.DS-4~~	<u>The organization continuously improves its cybersecurity management posture under normal and adverse conditions, including the perspectives outlined in CPS.ID.IM-02 and subsequent requirements.</u> ~~If the organization exchanges protected information with other organizations, agree in advance on security requirements for protection of such information.~~
<u>CPS.ID.IM-02</u> ~~CPS.DS-2~~	<u>The organization continuously improves supply chain security standards and associated procedures.</u> ~~Encrypt information with an appropriate level of security strength, and store them.~~
<u>CPS.ID.IM-03</u> ~~CPS.DS-3~~	<u>The organization continuously improves security training and education programs for its personnel and designated contacts at critical partner organizations.</u> ~~Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace~~
<u>CPS.ID.IM-04</u> ~~CPS.DS-4~~	<u>The organization continuously improves asset protection processes by integrating lessons learned from security incident response as well as from monitoring, measuring, and assessing internal and external attacks.</u> ~~Encrypt information itself when sending/receiving information.~~
<u>CPS.ID.IM-05</u> ~~CPS.DS-5~~	<u>The organization applies lessons learned from the analysis of detected events such as alerts and logs, to continuously improve security event detection processes.</u> ~~Securely control encryption keys throughout their life cycle to ensure proper operation and securely transmitted, received and stored data.~~
<u>CPS.ID.IM-06</u> ~~CPS.DS-6~~	<u>The organization incorporates lessons learned from responses to security incidents to continuously improve its incident response plan.</u> ~~Secure sufficient resources (e.g., People, Components, System) for components and systems, and protect assets properly to minimize bad effects of cyberattack (e.g., DoS attack).~~
<u>CPS.ID.IM-07</u> ~~CPS.DS-7~~	<u>The organization incorporates lessons learned from responses to security incidents to continuously improve its business continuity plan or emergency response plan.</u>

	Carry out periodic quality checks, prepare standby devices and uninterruptible power supplies, provide redundancy, detect failures, conduct replacement work, and update software for IoT devices, communication devices, circuits, etc.
~~CPS.DS-8~~	When handling information to be protected or procuring devices that have an important function to the organization, select IoT devices and servers equipped with anti-tampering devices.
~~CPS.DS-9~~	Properly control outbound communications that send information to be protected to prevent improper data breach,
~~CPS.DS-10~~	Conduct integrity checks of software running on the IoT devices and servers at a time determined by the organization, and prevent unauthorized software from launching.
~~CPS.DS-11~~	Perform integrity checking on information to be sent, received, and stored.
~~CPS.DS-12~~	Introduce an integrity check mechanism to verify the integrity of hardware.
~~CPS.DS-13~~	Confirm that IoT devices and software are genuine products during the booting-up process
~~CPS.DS-14~~	Maintain, update, and manage information such as the origination of data, and data processing history, throughout the entire data life cycle.
~~CPS.DS-15~~	Use products that provide measurable security in order to ensure the availability of security reporting and the trustworthiness of sensing data through integrity protection.

3.3 CPS.PR – Protect

The organization implements safeguards based on identified assets and risks to prevent or reduce the likelihood and impact of the occurrence of adverse security events.

3.3.1 CPS.PR.AA – Identity Management, Authentication, and Access Control CPS.IP – Information Protection Processes and Procedures

The organization limits access to physical and logical assets to authorized users, services, and hardware, and manages it commensurate with the assessed risk of unauthorized access. ~~Maintain security policies, processes, procedures, and use them to manage system and asset protection (dealing with objectives, scope, roles, responsibilities, management commitments, coordination among organizations).~~

Table 3.3-11 Measure requirements for the **PR.AA** category

ID	Measure Requirement
<u>CPS.PR.AA-01</u> <u>CPS.IP-1</u>	<u>The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.</u> ~~Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.~~
<u>CPS.PR.AA-02</u> <u>CPS.IP-2</u>	<u>The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).</u> ~~Restrict the software to be added after installing in the IoT devices and servers.~~
<u>CPS.PR.AA-03</u> <u>CPS.IP-3</u>	<u>The organization prevents unauthorized logins to IoT devices, servers, and related assets by implementing mechanisms such as account lockout after a specified number of failed authentication attempts and enforcing delays on subsequent login attempts until security conditions are verified.</u> ~~Introduce the system development life cycle to manage the systems.~~
<u>CPS.PR.AA-04</u> <u>CPS.IP-4</u>	<u>The organization protects, transmits, receives, and verifies information regarding authenticated entities (ID assertions).</u> ~~Perform a periodic system backups and testing of components (e.g., IoT devices, communication devices, and circuits).~~
<u>CPS.PR.AA-05</u> <u>CPS.IP-5</u>	<u>The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.</u> ~~Implement physical measures such as preparing an uninterruptible power supply, a fire-protection facility, and protection from water infiltration to follow the policies and rules related to the physical operating environment, including the IoT devices and servers installed in the organization.~~

~~CPS.PR.AA-06~~ ~~CPS.IP-6~~	~~The organization periodically reviews granted access privileges and remediates unnecessary or excessive permissions.~~ ~~When disposing of an IoT device and server, delete the stored data—and the ID (identifier)—uniquely identifying the genuine IoT devices and servers as well as important information (e.g., private key and digital certificate), or make them unreadable.~~
~~CPS.PR.AA-07~~ ~~CPS.IP-7~~	~~The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.~~ ~~Assess the lessons learned from security incident response and the results of monitoring, measuring, and evaluating internal and external attacks, and improve the processes of protecting the assets.~~
~~CPS.IP-8~~	~~Share information regarding the effectiveness of data protection technologies with appropriate partners.~~
~~CPS.IP-9~~	~~Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.~~
~~CPS.IP-10~~	~~Develop a vulnerability remediation plan, and modify the vulnerability of the components according to the plan.~~

3.3.2 CPS.PR.AT – Awareness and TrainingCPS.MA – Maintenance

The organization provides cybersecurity awareness and training to its personnel so they can perform their cybersecurity-related duties. ~~Maintain and repair components of industrial control systems and information systems according to policies and procedures.~~

Table 3.3-12 Measure requirements for the **PR.AT** category

ID	Measure Requirement
<u>CPS.PR.AT-01</u> ~~CPS.MA-4~~	<u>The organization conducts appropriate training and education for all personnel to carry out their assigned roles and responsibilities to minimize the occurrence and impact of security incidents, and maintains records of such activities.</u> ~~–Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updates with managed tools properly and in a timely manner while recording the history.~~ ~~–Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable.~~
<u>CPS.PR.AT-02</u> ~~CPS.MA-2~~	<u>The organization provides appropriate training and security education to designated personnel of external partners critical to security management, who may be involved in security incident response for the organization, enabling them to fulfill their assigned roles, and maintains records of such activities.</u> ~~Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.~~

3.3.3 CPS.PR.DS – Data SecurityCPS.PT – Protective Technology

The organization protects data based on its strategy to ensure the confidentiality, integrity, and availability of information. ~~Based on relevant policies, procedures, contracts, manage technical solutions to ensure security and resilience of systems and assets, safety.~~

Table 3.3-13 Measure requirements for the **PR.DS** category

ID	Measure Requirement
<u>CPS.PR.DS-01</u> ~~CPS.PT-4~~	<u>The organization accurately understands the required level of data protection mandated by various laws, regulations, and agreements regarding data shared exclusively among relevant organizations, establishes data classification methods based on respective requirements, and appropriately protects data commensurate with its classification throughout the entire lifecycle.</u> ~~Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.~~
<u>CPS.PR.DS-02</u> ~~CPS.PT-2~~	<u>The organization protects the confidentiality, integrity, and availability of data-at-rest.</u> ~~Minimize functions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.~~
<u>CPS.PR.DS-03</u> ~~CPS.PT-3~~	<u>The organization protects the confidentiality, integrity, and availability of data-in-transit.</u> ~~Introduce IoT devices that implement safety functions, assuming that these devices are connected to the network.~~
<u>CPS.PR.DS-04</u>	<u>The organization protects the confidentiality, integrity, and availability of data-in-use.</u>
<u>CPS.PR.DS-05</u>	<u>The organization maintains, updates, and manages data provenance, including data sources and processing history, throughout the entire lifecycle.</u>
<u>CPS.PR.DS-06</u>	<u>The organization performs routine backups of data (e.g., component configurations and operational data), protects backup data, and tests restoration capabilities.</u>

3.3.4 CPS.PR.PS – Platform SecurityCPS.AE – Anomalies and Events

The organization manages hardware, software (e.g., firmware, operating systems, and applications), and services across physical and virtual platforms to ensure confidentiality, integrity, and availability, consistent with its strategy. ~~Detect anomaly and understand the possible impact of the event.~~

Table 3.3-14 Measure requirements for the **PR.PS** category

ID	Measure Requirement
<u>CPS.PR.PS-01</u> ~~CPS.AE-1~~	<u>The organization evaluates the authenticity and integrity of hardware and software prior to acquisition and deployment, and verifies their integrity during operation.</u> ~~Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.~~
<u>CPS.PR.PS-02</u> ~~CPS.AE-2~~	<u>When procuring devices that process sensitive information or have important functions for its organization, the organization utilizes tamper-resistant devices.</u> ~~Appoint a chief security officer, establish a security management team (SOC/CSIRT), and prepare a system within the organization to detect, analyze, and respond to security events.~~
<u>CPS.PR.PS-03</u> ~~CPS.AE-3~~	<u>The organization utilizes products that implement appropriate security measures to ensure the trustworthiness of sensing data by preserving measurement availability and integrity.</u> ~~Identify the security events accurately by implementing the procedure to conduct a correlation analysis of the security incidents and comparative analysis with the threat information obtained from outside the organization.~~
<u>CPS.PR.PS-04</u> ~~CPS.AE-4~~	<u>The organization deploys IoT devices that implement security safeguards designed for network connectivity.</u> ~~Identify the impact of security events, including the impact on other relevant organizations.~~
<u>CPS.PR.PS-05</u> ~~CPS.AE-5~~	<u>The organization integrates secure software development practices (e.g., security reviews during the design stage, application of secure coding rules, and pre-release vulnerability assessments) into the system development lifecycle and verifies their implementation.</u> ~~Specify the criteria to determine the risk degree of security events.~~
<u>CPS.PR.PS-06</u>	<u>The organization establishes and applies configuration management practices for hardware and software of IoT devices, servers, and related assets (including minimizing functionality by physically or logically disabling unnecessary network, USB, and serial ports).</u>
<u>CPS.PR.PS-07</u>	<u>The organization prevents the installation and execution of unauthorized software.</u>
<u>CPS.PR.PS-08</u>	<u>The organization develops a vulnerability remediation plan and remediates component vulnerabilities in accordance with the plan.</u>

<u>CPS.PR.PS-09</u>	<u>The organization applies security-critical updates for IoT devices, servers, and related assets in a timely manner using managed tools while appropriately recording history.</u>
<u>CPS.PR.PS-10</u>	<u>The organization performs maintenance on its own IoT devices, servers, and related assets with prior approval from the department that owns the target component or system, logging maintenance activities and preventing unauthorized access.</u>
<u>CPS.PR.PS-11</u>	<u>To appropriately detect security incidents, the organization determines and documents the scope and types of events for audit logging, and continuously records and reviews logs.</u>
<u>CPS.PR.PS-12</u>	<u>Upon the disposal of IoT devices, servers, and related assets, the organization deletes or renders unreadable all internally stored data, unique identifiers of legitimate devices and systems, and critical security information (e.g., private keys and digital certificates).</u>

3.3.5 CPS.PR.IR – Technical Infrastructure Resilience ~~CPS.CM – Security Continuous Monitoring~~

The organization manages security architectures to ensure the confidentiality, integrity, and availability of its assets, as well as organizational resilience, consistent with organizational strategy. ~~Detect security events and monitor systems and assets to verify the effectiveness of protection measures.~~

Table 3.3-15 Measure requirements for the **PR.IR** category

ID	Measure Requirement
<u>CPS.PR.IR-01</u> ~~CPS.CM-4~~	<u>The organization protects networks and environments from unauthorized access and use by implementing network segmentation (e.g., separating development/test environments from production environments, and isolating IoT device environments from other networks within the organization).</u> ~~Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.~~
<u>CPS.PR.IR-02</u> ~~CPS.CM-2~~	<u>The organization implements physical safeguards to comply with policies and rules regarding the physical operating environment of its IoT devices, servers, and related assets, such as ensuring uninterruptible power supplies, fire protection equipment, and flood protection measures.</u> ~~Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.~~
<u>CPS.PR.IR-03</u> ~~CPS.CM-3~~	<u>The organization implements mechanisms to achieve requirements for the continuous operation of systems and services under normal and adverse conditions.</u> ~~– Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. – Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.~~
<u>CPS.PR.IR-04</u> ~~CPS.CM-4~~	<u>The organization secures sufficient resources (e.g., people, components, and systems) to minimize the impact of attacks and maintain critical functions, even in the event of cyberattacks such as ransomware or denial-of-service (DoS) attacks.</u> ~~Validate the integrity and authenticity of the information — provided from cyberspace before operations.~~
~~CPS.CM-5~~	~~Monitor communication with external service providers so that security events can be detected properly.~~

~~CPS-CM-6~~	~~As part of the configuration management of devices, work constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.~~
~~CPS-CM-7~~	~~Confirm the existence of vulnerabilities that require a regular check-up in IoT devices and servers managed within the organization.~~

3.4 CPS.DE – Detect

The organization finds and analyzes anomalies, indicators of compromise, and other potentially adverse events indicating the occurrence of cyberattacks and security incidents.

3.4.1 CPS.DE.CM – Continuous MonitoringCPS.DP – Detection Process

The organization monitors assets to find anomalies, indicators of compromise, and other potentially adverse events. ~~Maintain and test detection processes and procedures to accurately detect abnormal security events.~~

Table 3.3-16 Measure requirements for the **DE.CM** category

ID	Measure Requirement
<u>CPS.DE.CM-01</u> ~~CPS.DP-1~~	<u>The organization monitors networks and network services to properly detect security events.</u> ~~Clarify the role and responsibility of the organization as well as service providers in detecting security events so that they can fulfill their accountabilities.~~
<u>CPS.DE.CM-02</u> ~~CPS.DP-2~~	<u>The organization monitors the operational status of hardware and software across IoT devices, servers, and related assets, as well as network connection status, to properly detect security events.</u> ~~Detect security events in the monitoring process, in compliance with applicable local regulations, directives, industry standards, and other rules.~~
<u>CPS.DE.CM-03</u> ~~CPS.DP-3~~	<u>The organization monitors communications with external service providers to properly detect security events.</u> ~~As part of the monitoring process, test regularly if the functions for detecting security events work as intended, and validate these functions.~~
<u>CPS.DE.CM-04</u> ~~CPS.DP-4~~	<u>The organization monitors the activities of internal and external personnel, including their access to and operations on elements (components, systems, etc.), to properly detect security events.</u> ~~Continuously improve the process of detecting security events.~~
<u>CPS.DE.CM-05</u>	<u>The organization implements appropriate physical access settings, logging, and monitoring, commensurate with the criticality of IoT devices, servers, and related assets.</u>
<u>CPS.DE.CM-06</u>	<u>The organization periodically scans its IoT devices, servers, and related assets to identify vulnerabilities requiring remediation.</u>
<u>CPS.DE.CM-07</u>	<u>The organization verifies the integrity and authenticity of information received from cyberspace prior to operation.</u>
<u>CPS.DE.CM-08</u>	<u>The organization deploys IoT devices that detect anomalies or suspend operations by comparing commanded operations with actual operational outcomes.</u> <u>The organization verifies that information received from cyberspace does not contain malicious code and remains within permissible operating parameters prior to execution.</u>

CPS.DE.CM-09

As part of its monitoring operations, the organization periodically tests and validates whether functions detecting security events operate as intended.

3.4.2 CPS.DE.AE – Adverse Event AnalysisCPS.RP – Response Planning

The organization analyzes anomalies, indicators of compromise, and other potentially adverse events to detect cybersecurity incidents. Respond to detected security incidents and implement and maintain response and recovery processes and procedures so affected assets and systems can be properly restored and business continues uninterrupted.

Table 3.3-17 Measure requirements for the **DE.AE** category

ID	Measure Requirement
<u>CPS.DE.AE-01</u> ~~CPS.RP-1~~	<u>The organization analyzes potential security events to understand their details.</u> ~~Develop and implement previously the procedure of response after detecting incidents (security operation process) that includes the response of Organization, People, Components, System to identify the content of response, priority, and scope of response taken after an incident occurs.~~
<u>CPS.DE.AE-02</u> ~~CPS.RP-2~~	<u>The organization accurately identifies security incidents by implementing procedures to correlate security events and analyze them against external threat information.</u> ~~As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.~~
<u>CPS.DE.AE-03</u> ~~CPS.RP-3~~	<u>The organization identifies the impact of security events, including the adverse effects on relevant external organizations.</u> ~~Include security incidents in the business continuity plan or emergency response plan that outlines the action plans and response procedures to take in case of natural disasters.~~
<u>CPS.DE.AE-04</u> ~~CPS.RP-4~~	<u>The organization establishes criteria for determining whether a security event constitutes an incident, and declares an incident when the criteria are met.</u> ~~Take appropriate measures on goods (products) whose quality may be affected by security incidents, especially regrading production facilities damaged by the security incident.~~

3.5 CPS.RS – Respond

The organization manages, analyzes, mitigates, and reports on detected security incidents to contain their impact.

3.5.1 CPS.RS.MA – Incident ManagementCPS.CO – Communications

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

Table 3.3-18 Measure requirements for the **RS.MA** category

ID	Measure Requirement
<u>CPS.RS.MA-01</u> CPS.CO-4	To clarify response actions, priorities, and remediation scope following the occurrence of a security incident, the organization predefines and implements response procedures (security operation processes) for the organization, people, components, and systems after detecting an incident. Develop and manage rules regarding publishing information after the occurrence of the security incident.
<u>CPS.RS.MA-02</u> CPS.CO-2	The organization verifies that events reported as security incidents are not false positives or duplicate reports, and validates their legitimacy as incidents. Include the item in the business continuity plan or contingency plan to the effect that the organization shall work to restore its social reputation after the occurrence of a high-risk security incident.
<u>CPS.RS.MA-03</u> CPS.CO-3	The organization classifies and prioritizes detected security incidents based on the severity of impact, entry route, and other factors. Include the item in the business continuity plan or contingency plan to the effect that the details of the recovery activities shall be communicated to the internal and external stakeholders, executives, and management.
<u>CPS.RS.MA-04</u>	Once a security incident is declared, the organization executes incident response in accordance with predefined procedures, coordinating with other relevant organizations such as business partners.
<u>CPS.RS.MA-05</u>	The organization takes appropriate actions for components (products) suspected of having quality defects, such as those produced using equipment damaged during a security incident.
<u>CPS.RS.MA-06</u>	The organization determines the initiation of recovery based on predetermined criteria, taking into account the characteristics of the security incident and the impact of recovery activities on business operations.

3.5.2 CPS.RS.AN – Incident AnalysisCPS.AN – Analysis

The organization conducts incident investigations to support effective incident response, root cause determination, and recovery. ~~Analyze the incident and its effects to ensure efficient response and support restoration activities.~~

Table 3.3-19 Measure requirements for the **RS.AN** category

ID	Measure Requirement
<u>CPS.RS.AN-01</u> ~~CPS.AN-1~~	<u>The organization collects data and metadata related to security incidents (including the history of actions taken during incident response), preserves their integrity, and retains them in a state where acquisition sources, timestamps, and related provenance can be referenced.</u> ~~Understand the impact of the security incident on the whole society including the organization and relevant parties such as partners based on the full account of the incident and the probable intent of the attacker.~~
<u>CPS.RS.AN-02</u> ~~CPS.AN-2~~	<u>After a security incident occurs, the organization conducts digital forensics to identify the root cause. In doing so, it preserves records of the investigation process in a tamper-resistant manner.</u> ~~Implement digital forensics upon the occurrence of the security incident.~~
<u>CPS.RS.AN-03</u> ~~CPS.AN-3~~	<u>Based on the full scope of the security incident and the inferred intent of the threat actor, the organization assesses the impact on society as a whole, including the organization itself and relevant external organizations.</u> ~~Categorize and store information regarding the detected security incidents by the size of security-related impact, penetration vector, and other factors.~~

3.5.3 CPS.RS.CO – Incident Response Reporting and Communication **CPS.MI – Mitigation**

The organization shares information regarding incident response activities with internal and external stakeholders and coordinates with them in accordance with statutory, regulatory, and policy requirements. Implement activities to prevent the expansion of security events, mitigate the effects, and resolve security incidents.

Table 3.3-20 Measure requirements for the RS.CO category

ID	Measure Requirement
<u>CPS.RS.CO-01</u> CPS.MI-1	<u>The organization develops and implements rules governing internal communication and external disclosure after the occurrence of a security incident.</u> ~~Take measures to minimize security-related damages and mitigate the impacts caused by such incident.~~
<u>CPS.RS.CO-02</u>	<u>Based on established rules, the organization escalates incidents to executive decision-makers within the organization and relevant external entities as necessary.</u>

3.5.4 CPS.RS.MI – Incident MitigationCPS.IM – Improvements

The organization performs activities to prevent expansion of an adverse event and mitigate its impact. ~~Improve response and recovery activities by incorporating lessons learned from present and past decisions / response activities.~~

Table 3.3-21 Measure requirements for the RS.MI category

ID	Measure Requirement
<u>CPS.RS.MI-01</u> ~~CPS.IM-1~~	<u>The organization minimizes the spread of damage from security incidents, eradicating causes or mitigating adverse impacts.</u> ~~Review the lessons learned from the responses to security incidents, and continuously improve the security operation process.~~
~~CPS.IM-2~~	~~Review the lessons learned from the responses to security incidents, and continuously improve the business continuity plan or emergency response plan.~~

3.6 CPS.RC – Recover

The organization restores assets and operations affected by security incidents.

3.6.1 CPS.RC.RP – Incident Recovery Plan Execution

The organization performs restoration activities to return systems and services affected by security incidents to their normal operating state.

Table 3.3-22 Measure requirements for the RC.RP category

ID	Measure Requirement
<u>CPS.RC.RP-01</u>	<u>The organization incorporates security incidents into its business continuity plan or emergency response plan, which defines response policies and procedures for natural disasters.</u>
<u>CPS.RC.RP-02</u>	<u>The organization takes into account critical business functions and the results of cybersecurity risk management when establishing post-incident operational policies.</u>
<u>CPS.RC.RP-03</u>	<u>Upon deciding to initiate the recovery phase, the organization executes recovery based on predetermined recovery plans.</u>
<u>CPS.RC.RP-04</u>	<u>The organization verifies the integrity of backups and other recovery assets prior to use.</u>
<u>CPS.RC.RP-05</u>	<u>The organization verifies the integrity of restored assets, recovers systems and services, and confirms that they are in a normal operational state.</u>
<u>CPS.RC.RP-06</u>	<u>The organization declares the completion of incident recovery based on predetermined criteria and completes the documentation related to the incident.</u>

3.6.2 CPS.RC.CO – Incident Recovery Communication

The organization communicates and coordinates with internal and external stakeholders regarding recovery activities following security incidents.

Table 3.3-23 Measure requirements for the RC.CO category

ID	Measure Requirement
<u>CPS.RC.CO-01</u>	<u>The organization establishes and maintains rules regarding information exchange aimed at recovery after the occurrence of a security incident.</u>
<u>CPS.RC.CO-02</u>	<u>The organization incorporates provisions to restore public trust and organizational reputation after the occurrence of a security incident into its business continuity plan or emergency response plan.</u>
<u>CPS.RC.CO-03</u>	<u>The organization specifies within its business continuity or emergency response plans that recovery activities must be communicated to internal and external stakeholders, officers, and management.</u>

Published by

Cybersecurity Division and Digital Economy Division

Commerce and Information Policy Bureau

Ministry of Economy, Trade and Industry (METI)

Technical Support

Innovation Platform Agency, Japan (IPA)