Guideline for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure (5th Edition)

(Tentative Translation)

April 4, 2018
Cybersecurity Strategic Headquarters
Government of JAPAN

Introduction
(Executive Summary of This Guideline)

Positioning and Structure of This Guideline

Critical infrastructure (CI) operators have the social responsibilities of providing CI services (CISs) safely and continuously, and it is important to put in place the necessary measures based on the "Concept of Mission Assurance" set out in the Cybersecurity Policy for Critical Infrastructure Protection (4th Edition). Specifically, this involves making the necessary preparations for risks related to information security and implementing the appropriate countermeasures in the event of an emergency. The matters that should be taken into consideration in such situations should ideally be set out in Safety Principles, which provide the standard for the operation of businesses by CI operators. This guideline organizes and sets out the items that should ideally be provided for in such safety principles.

The items set out in this guideline are information security measures that follow the PDCA cycle. The formulation of these items takes into consideration the Information security Management System (ISMS), an international standard for information security, as well as information security standards related to CI sectors, such as NIST's Framework for Improving Critical Infrastructure Cybersecurity and CSMS Certification Criteria. This guideline is structured in a way that allows it to comprehensively cover all the main standards related to CI.

Matters of Importance when Implementing the PDCA Cycle for Information security Measures

- Actions required of the management

The management needs to recognize that information security risks have an impact on business operations that are based on the "Concept of Mission Assurance," adding a level of uncertainty to such operations; hence, the management has to provide instructions on the implementation of the necessary information security risk assessments in order to decide on the approach for dealing with such risks. Furthermore, in promoting the PDCA cycle for information security measures, it should strive to continuously secure and appropriately allocate the necessary resources (budget, systems, human resources, etc.). In addition, the management needs to periodically verify the effects and impact that the results of addressing information security risks have on the business, and to make decisions on the necessity of reviewing the strategy for addressing information security risks. With regard to these initiatives, it should refer to materials such as the Approaches to Cybersecurity for Corporate Management and the Cybersecurity Management Guidelines.

- Periodic implementation of information security risk assessment

Information security risks are constantly changing as a result of factors such as the occurrence of new threats and the new discovery of technological vulnerabilities, and changes in the business environment surrounding CI operators and new demands from interested parties. In view of that, there is a need to periodically implement risk assessments while taking reference from materials such as the Risk Assessment Guide Based on the Concept of Mission Assurance in Critical Infrastructure, and to reassess the impact that changes in information security risk have on the safe and sustainable provision of CISs.

- Formulation of response plans based on the characteristics of cyberattacks

During the occurrence of a cyberattack, which is one of the events that give rise to CISs outages, formulate a contingency plan beforehand, which sets out concrete policies and procedures of initial response among other details, in order to realize swiftly and appropriate initial response. At the same time, formulate a business continuity plan, which sets out the policies and procedures, among other details, of measures for recovery from the CISs outages that result from the cyberattack. In the formulation of these response plans, take into consideration the Characteristics of Cyberattack Risks as well as Considerations for Response and Countermeasures provided in this guideline.

- Making provisions for swiftly and flexible incident readiness

In addition to addressing information security risks from a medium- to long-term perspective based on the PDCA cycle, there is also a need to ensure readiness, which enables timely and flexible response to any indications of a cyberattack that are detected on a daily basis through monitoring mechanisms built by CI operators.

Index

I. Purposes and Positioning

1. The Importance of Information Security Measures for Critical Infrastructure (CI)

The people's living and socioeconomic activities of the country are underpinned by various CI services (CISs), and information systems are widely used to realize this function.

In this context, critical infrastructure, by its very nature, calls for the provision of safe and sustainable services. Hence, based on the "Concept of Mission Assurance" set out in the Cybersecurity Policy for Critical Infrastructure Protection (4th Edition) (hereinafter referred to as "4th Cybersecurity Policy"), in the protection of CI, it is important to ensure the security of the information systems necessary for the provision of services, and to reduce the possibility of the occurrence of CISs outages due to cyberattacks or other factors as far as possible. At the same time, it is also important to ensure early detection of the occurrence of outages and recovery from these outages swiftly. Furthermore, as CISs can have a severe impact in the case of a suspension or deterioration of their functions. For this reason, there is a need to provide focused protection through close cooperation between the public and private sectors.

> Concept of Mission Assurance
>
> CI services are the very basis of national life and socioeconomic activities and suspension thereof may have a direct and serious negative effect on the safety and ease of the general public. Therefore, stakeholders are required to make efforts to ensure safe and continuous provision of CI services (mission assurance).
>
> Mission assurance in this Cybersecurity Policy does not mean to oblige stakeholders to make a firm commitment to ensuring CIP or maintaining CI functions, but to have them assume their responsibilities in the process of protecting CI services and maintaining the functions thereof. This is the concept to require each stakeholder to properly make efforts for necessary cybersecurity measures.
>
> (Excerpt from the Cybersecurity Policy for Critical Infrastructure Protection (4th Edition))

For CI operators, with the necessary support from government organizations, it is desirable for the management to be actively involved, position readiness against risks related to information security as a part of their management strategy, and put in place strategic measures such as risk reduction based on the results of risk assessments (implementation of risk management for information security). In addition, through the prompt detection of cyberattacks and other risks and appropriate responses to these problems, CI operators should also develop the appropriate incident readiness, so that they can continue to ensure the safety of CISs and, as far as possible, provide CISs without any deterioration in quality or suspension of services that are unacceptable to themselves and their stakeholders.

In promoting these measures, it is particularly important for CI operators to recognize that while they are business entities, they are also socially responsible entities. In addition to the steady

implementation of information security measures that are necessary or desirable, corresponding to the characteristics of CI sectors, it is also critical that CI operators continuously improve on information security measures by following the PDCA cycle, while capturing changes in the business environment and other factors.

2. What Are "Safety Principles?"

CI operators engage in business in accordance with the relevant standards, under the legal systems that are related to their respective business domains.

Based on the above fact, this guideline names documents that serve as standards or references for the decisions and actions taken by CI operators as "Safety Principles." Safety Principles are classified into the following four categories.

[1] Mandatory standards that are stipulated by the government based on the relevant laws

[2] Recommended standards and guidelines that are stipulated by the government in accordance with the relevant laws

[3] Industry standards and guidelines that cut across industries, stipulated by industrial organizations with the aim of fulfilling the expectations of the citizens and the relevant laws

[4] Internal regulations, etc. stipulated by CI operators with the aim of fulfilling the expectations of citizens, users, and the relevant laws

*Note that documents that correspond to Safety Principles are not limited to documents drawn up for the purpose of ensuring safety.

In order to ensure the firm implementation of information security measures that are necessary or desirable for CI operators, it is required that items and standards related to information security measures be clearly presented in these Safety Principles. In short, by referring to the abovementioned [1] to [4], all parties that are involved in the CI business are expected to be able to understand what they should do, and to what extent they should do these things.

3. Positioning of the Guideline

The aim of this guideline is to support the formulation and revision of Safety Principles by organizing and setting out items that should ideally be provided for in Safety Principles, from the perspective of realizing the safe and sustainable provision of CISs, taking into account the concept of mission assurance in CI.

For this reason, this guideline sets out items for information security measures in accordance with the PDCA cycle, to enable easy referencing for CI operators when they are engaged in voluntary initiatives or continual improvements. (Figure 1 provides an overall image of the information security measures of CI in this guideline.)

As this guideline only sets out items that are highly necessary based on a cross-sectional overview of the CI sectors with a focus on information security measures, there is a need to pay attention to the following two points when the respective CI sectors or business operators formulate or revise Safety Principles.

- Depending on the CI sector or CI operator, due to reasons such as the mode of business or other factors, there is a possibility that the items prescribed in this guideline include items that do not need to be set out in Safety Principles.
- Depending on the CI sector or CI operator, due to reasons such as the mode of business or other factors, there is a possibility that items not prescribed in this guideline need to be set out in Safety Principles.

With regard to the items of the measures prescribed in this guideline and the standards for these items, each CI sector or CI operator is expected to consider which Safety Principles they should be prescribed in, taking into account factors such as the provisions of the relevant laws in each CI sector and the composition of existing Safety Principles.

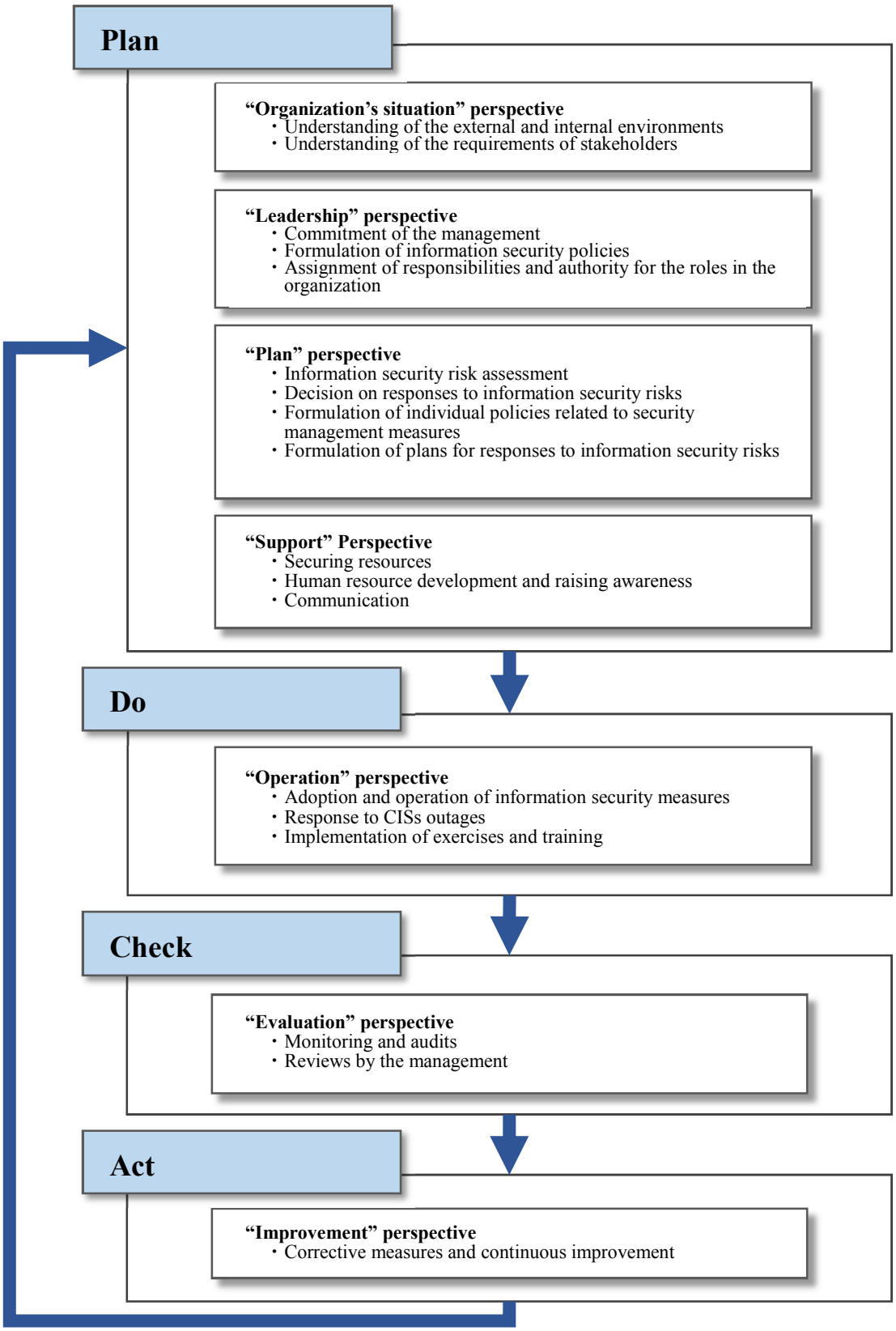


Figure 1: Overall image of information security measures in CI

4. Expectations Toward the Continual Improvements and Dissemination of Safety Principles based on This Guideline

The environment surrounding information security is changing at an increasing pace, and the importance of making continual improvements of Safety Principles that CI operators refer to, or those established by themselves, is also growing year by year.

As there is a possibility that responses to threats that have been regarded as unnecessary may become necessary going forward due to these environmental changes, CI operators are expected to regularly check on the impact of these environmental changes, and at the same time, determine the need to review Safety Principles while taking reference from this guideline.

As explained earlier, in continual improvements of Safety Principles, it is desirable to refer to various relevant standards and best practices from Japan and abroad as necessary, in addition to this guideline, taking into account that this guideline contains selected items that have been determined as being highly necessary based on a cross-sectional overview of the CI sectors.

Moreover, from the perspective of the aim to foster a sense of security among the citizens, and in light of the significant impact that CI has on the people's living, the entities responsible for the formulation of Safety Principles are expected to put constant effort into disseminating the principles to parties involved in CI businesses, and at the same time, to widely disclose and publish the contents of Safety Principles in a way that does not impede with the promotion of information security measures.

II. Items That Should Ideally Be Prescribed in the Safety Principles

1. Purpose of Formulating the Safety Principles

Based on the concept of mission assurance, the safety principles set out the need to implement the PDCA cycle for information security measures in reference to the contents of the safety principles, in order to eliminate, as far as possible, the occurrence of CISs outages in CI that have an impact on the safe and continuous provision of CISs, as well as to ensure their swift recovery in the occurrence of such an event.

2. Applicable Scope

Based on the examples of applicable CI provided in "Annex 1: Applicable CI Operators and Examples of Critical Information Systems," as well as the CISs (including procedures), examples of CISs outages, and service maintenance levels provided in "Annex 2: Explanation of CISs and Examples of CISs Outages," the applicable scope for the items to be prescribed in the safety principles shall be listed.

3. Roles of Stakeholders

With regard to the stakeholders of the CI sectors within the scope of the safety principles (*refer to the Definitions and Glossary), provide a comprehensive and specific list, and clearly define the roles of each stakeholder in relation to the respective information security measures. In particular, with regard to the role of CI operators, the efforts of the management should also be included, taking reference from the section "Responsibility of Top Management" in the 4th Cybersecurity Policy and other materials.

4. Measures

In light of the fact that CI operators have the social responsibility of realizing the safe and continuous provision of CISs, review the adoption or rejection of the measure items listed in items 4.1 to 4.4, in accordance with the PDCA cycle for information security measures.

The PDCA cycle for information security measures typically follows the flow of: Plan, which involves identifying the measures based on the results of analysis; Do, which involves moving to the implementation phase, and after a certain period of time; Check, which involves evaluating the need to review the measures, and; Act, which involves putting in place improvements. However, in actual operations, depending on the results of the monitoring and detection carried out in the "Do" phase, it is necessary to be aware of the possible need to respond actively, such as by reviewing the contents of the measures urgently.

In addition, list the references that set out concrete examples of each measure in Annex 4: References for Concrete Examples of Measure Items. This provides a source of reference during

the adoption of each measure item, where necessary.

4.1. The "Plan" Perspective

4.1.1. Perspective of the Organization's Situation

(1) Understanding the External and Internal Environments

Organize information about the condition of the external environment surrounding CI operators (politics, economy, society, etc.) to which the impact on the necessary capacity for the safe and continuous provision of CISs is assumed, and the internal environment of CI operators (organizational structure, strategy, capabilities, etc.), including the situation in the near future. When doing so, it is particularly important to get an accurate grasp of the dependency between the supply-chain (suppliers, contractors, etc.) and one's own organization, by extracting and analyzing the various tasks associated with the provision of CISs.

(2) Understanding the Requirements of Stakeholders

Organize the requirements of stakeholders, customers, suppliers, contractors, etc. in relation to the information security measures put in place by CI operators (including initial response and recovery treatment during the occurrence of CISs outages). The requirements include tasks stipulated by contracts or the relevant laws of the respective business domains, and restrictions prescribed by suppliers or contractors.

The organized information, including the aforementioned status of the external and internal environments, is an element that should be taken into consideration when formulating information security policies and implementing information security risk assessments. From the perspective of raising awareness of the information security measures among employees (including staff of administrative organizations), the organized contents should be shared across the entire organization.

4.1.2. The "Leadership" Perspective

(1) Commitment of the Management

The management of CI operators evaluates information security risks[1] and declares, within and outside the organization, the appropriate response to these risks, in order to realize business management based on the "Concept of Mission Assurance," which is required of CI operators. In making the declaration, the information security policies set out in item (2) on the following page should be utilized.

[1] Refers to the risks identified by CI operators based on CISs outages caused by cyberattacks or other causes, that is, the consequences of events related to information assets (such as information, information systems, and control systems that make use of IT) that are owned, used or managed for the purpose of executing the businesses necessary for the provision of their services.

Furthermore, in addressing information security risks, the management is expected to recognize the "Responsibility of Top Management at CI Operators" prescribed below, while taking reference from the Approaches to Cybersecurity for Corporate Management [2] and the Cybersecurity Management Guidelines.[3]

【Responsibility of Top Management at CI Operators】

- Ensuring information security is a responsibility that should be fulfilled by the management; therefore, commit themselves to exerting leadership and putting in place information security measures based on the concept of mission assurance.
- Recognize that the company's activities contribute to the development of society as a whole, and put in place security measures that include the supply-chain (business partners, subsidiaries, and affiliated companies).
- From the perspective of fostering trust and a sense of security among stakeholders with regard to information security, take steps such as disclosing information about a posture of readiness for information security measures during normal times and responses when an incident occurs.
- In addition to accurately collecting the necessary information for each of the abovementioned efforts, continuously secure the necessary management resources such as budget, systems, and human resources, and allocate them appropriately based on a risk-based approach.
- Taking into account the effect that responses to information security risks have on the business and the verification results of the impact, make decisions on the need to review further strategies for addressing information security risks and the contents, at the Board of Directors' meetings and other important management meetings.

＊Partial revision and addition of items necessary for the formulation of this guideline, based on the contents set out in the 4th Cybersecurity Policy.

(2) Formulation of Information security Policies

CI operators formulate information security policies, which are official documents for internal and external parties. In the information security policies, CI operators, who have the social responsibilities of ensuring the safe and continuous provision of CISs, set out the purposes and

[2] Compiled by the Working Group for Corporate Management with a Security Mindset, established under the Human Resources Expert Panel for Dissemination and Enlightenment (decided by the Cybersecurity Strategic Headquarters on 10 February 2015). It presents the basic stance on cybersecurity for corporate management.

[3] From the perspective of protecting the company from cyberattacks, this summarizes the principles that managers need to be aware of, and the important items that should be issued as instructions to officers in charge (CISO, etc.) who are responsible for implementing information security measures. Formulated by the Ministry of Economy, Trade, and Industry (METI) and Information-technology Promotion Agency (IPA).

direction of information security measures, as well as present the commitment of the management toward fulfilling the requirements of stakeholders related to the information security measures and continual improvements on the information security measures.

The information security policies are communicated within the organization, and can also be obtained by external stakeholders where necessary. In addition to checking, at regular intervals, that the information security policies are relevant and effective, it is also necessary to check the policies in the event of any significant changes to the situation surrounding the organization.

(3) Assignment of Responsibilities and Authority for the Roles in the Organization

In order to ensure the firm implementation of information security measures, the management of CI operators decide on the departments and employees that will take on the role of promoting information security measures. At the same time, the management also assigns the corresponding responsibilities and authority within the appropriate scope, communicates the assignment to all members of the organization, and ensures that all employees have the same recognition of these responsibilities and authority.

In doing so, it is particularly important to clearly identify the risk owners from among the personnel who have the role of promoting information security measures. These risk owners have the responsibility of monitoring and addressing the risks identified through risk assessments, and are required to provide clear explanations and take responsibility for the contents of their explanations.

Besides, it is also expected to secure human resources who are able to connect the management with the practitioners, plan the information security measures based on the business strategy, and lead and direct the practitioners (CISO, etc.).

Furthermore, in cases where the organization has an environment in which control systems are operated, they are expected to consider the need for human resources for departments related to OT[4] to prevent and recover from CISs outages caused by cyberattacks or other reasons.

In addition to the abovementioned, the following roles are also possible:

- Responsible for the collection of threat information, etc. and the sharing of information with stakeholders
- Responsible for the management of security incidents (CSIRT, etc.)
- Responsible for the execution of contingency plans and business continuity plans

[4] In this guideline, it refers to operation technology such as control systems that make use of information and communication technology (IT).

- Responsible for internal audits on all information security measures
- Responsible for the management of information security measures in the supply-chain (suppliers, contractors, etc.)
- Responsible for the management of the functional requirements for security personnel, and for education and training
- Responsible for the operation of information systems (including networks)
- Responsible for the management of the respective assets (information systems, software, information, etc.)
- Responsible for the management of facilities that require physical security

4.1.3. The “Plan” Perspective

(1) Information Security Risk Assessment

In order to appropriately manage the information security risks that have an impact on the safe and continuous provision of CISs, conduct information security risk assessments by following the procedures set out below.

(i) Taking into account the constantly changing situation surrounding the organization and the needs of stakeholders, clearly define the scope and standards of the business that are necessary for providing CISs. At the same time, identify the management resources, such as information systems, that are necessary for the execution of these business. As a part of this process, analyze the organization’s risk attitude[5] and risk tolerance.[6]

(ii) Identify the information security risks for management resources such as information systems (risk identification).

(iii) While giving consideration to the risk attitude and risk tolerance, utilize the risk criteria that have been formulated with evaluating the degree of impact that the consequences of an event has on services and the business and the probability for the occurrence of an event being the axis, and verify the magnitude of the risks identified (risk analysis).

(iv) In addition to identifying risks of a magnitude that is larger than the risk criteria, identify risks that are subjected to risk treatment in consideration of individual factors (risk evaluation).

∗ The Risk Assessment Guide based on the Concept of Mission Assurance in Critical Infrastructure issued by the National center of Incident readiness and Strategy for Cybersecurity (NISC) sets out the perspective of risk assessment based on the concept of mission assurance as well as details on the abovementioned procedures. Please refer to the Guide alongside with this guideline.

∗ Depending on the business characteristics and environment of the organization, there may also be cases where applying methods from other guidebooks, etc. is more effective. For example, the Security Risk Assessment Guide for Industrial Control Systems published by the Information-Technology Promotion Agency (IPA) sets out the concrete work procedures for effective security measures as well as risk analysis methods that combine asset-based risk assessment and business risk-based (scenario-based) risk assessment methods.

[5] Refers to an organization's efforts to conduct risk assessments, and ultimately retain, take, or avoid the risks. To clarify risk attitude, clarify the degree to which CI operators take risks in the operation of their businesses. For example, "The occurrence of CISs outages accompanying the decline of service levels below 20% is to be three times or less per year."

[6] Refers to the degree of residual risk (a risk that remains after the risk treatment) that the organization or stakeholder is prepared to take on in order to achieve their objectives. Specified, for example, as, "The occurrence of CISs outages accompanying the decline of service levels above 50% is to be once a year or less."

For the safe and continuous provision of CISs, depending on the CI sectors and characteristics of the services, it is desirable to identify the risks from the perspective of HSE,[7] etc. in addition to information security risks, and to conduct an analysis and evaluation. The HSE perspective can possibly cover, for example, ensuring occupational health and safety for the employees who are responsible for the provision of CISs, ensuring the health and safety of CISs users, and reducing the environmental burden that accompanies the provision of CISs.

It is also necessary to manage risks that were not identified as subjects for risk treatment in the abovementioned methods. In cases where the said risks are managed under the responsibility of the department in charge, it is desirable to establish a system that enables the timely verification of the management status (whether or not security management measures have been introduced, etc.) in each department.

(2) Decision on Information Security Risk Treatment

Decide on the concrete method for the information security risk treatment that have been identified through the risk assessments. The options of risk treatment include mitigation,[8] avoidance,[9] transfer (sharing),[10] and retention (acceptance).[11] Taking into consideration the degree of impact that the consequences of an event has on the business and the probability for the occurrence of an event, select the option that is perceived as the most appropriate.

Next, decide on the security management measures as a means for realizing the selected method for the risk treatment. As a reference, points (A) Security for Human Resources (Outsourcing) to (J) Information Security Incident Management below present the security management measures that are expected to be incorporated into the safety principles, from the perspective of critical infrastructure protection (CIP).

The ISO/IEC 27000 Family of Standards, Framework for Improving Critical Infrastructure Cybersecurity (NIST), and CSMS Certification Criteria (IEC62443-2-1) are also some of the references that provide security management measures. In addition to these standards, it is desirable to also continuously check if any security management measures that are necessary to the organization have been overlooked, referring to examples of the introduction of security management measures by CI operators in the same industry.

(A) Security for Human Resources (Outsourcing)

[7] Refers to health, safety, and environment. In the CSMS Certification Criteria (Ver. 1.0), which is a cybersecurity management system for industrial automation and control systems, the integration of the results of the assessment of physical risks, with the results of the assessment of HSE risks and the results of cybersecurity risk assessments, is required.
[8] Applying appropriate management measures to risks.
[9] Avoiding risks by deciding not to commence or continue with activities that give rise to risks.
[10] Sharing all or part of the risks with one or more other parties.
[11] Retaining (accepting) risks through decision-making based on information.

● Matters to Be Addressed before Outsourcing (Selection/Contract Conditions)
When selecting the external contractor for tasks that are related to CISs, consider the categories of information that will be accessed as well as the risks identified, in addition to the business requirements.

In the outsourcing agreement between the organization and the contractor, incorporate the contractor's responsibility for implementing information security measures that fulfill the information security requirements of the organization, the responsibility for providing education and training to raise the awareness of employees, and the responsibility and tasks associated with effective information security even after the end of the contract.

As there may be cases where the review of contract wording is necessary depending on the results of the risk assessments that have been implemented continuously, it is desirable for the security department or legal department to regularly establish spaces for the exchange of information.

● Matters to Be Addressed during the Contract Period
To ensure the steady execution of information security requirements by the contractor, regularly verify the implementation status of measures by the contractor, and request for the necessary improvements to be put in place.

(B) Asset Management
● Responsibility for Assets
After specifying assets such as information systems, software, and information that are associated with the provision of CISs, draw up an asset record that clearly sets out the parties responsible for the management of and the usage limit of each asset (scope within which use is permitted), and maintain and manage this record. Along with this, also draw up network configuration diagrams, data flow charts, and other figures. In cases where facilities such as information systems and their operation are replaced by services provided by an external supplier (for example, a supplier of IT services or of the components of IT infrastructure), draw up a list of services, and maintain and manage this list.

● Categories of Information and the Handling of Information
With regard to the information handled by CI operators, corresponding to the level of importance, legal requirements, impact on sense of security among citizens, and other factors, assign ratings to the information from the perspective of confidentiality, integrity, and availability, and label the information medium (paper, electronic).

Define and implement the necessary handling restrictions (for example, prohibition of duplication, prohibition of taking out, and prohibition of distribution), based on the life cycle of the information, such as creation, access, use, storage, transmission, provision, and deletion.

(C) Access Control

● Management of User Access

In order to appropriately manage the users accessing information systems and information, etc. that is associated with the provision of CISs, as well as their access rights, clearly define the application routes, authorizer, and worker in relation to the official processes of the registration, change, and deletion of users and their access rights. At the same time, periodically review the access right of users during operation. In particular, manage strictly the assignment and use of privileged access rights to information systems.

●Access Control for Information Systems, etc.

Based on the principles of the least privilege and the separation of duty, restrict the access to information and to information systems that are associated with the provision of CISs (including remote access).

Establish systems that ensure compliance with secure log-on procedures (for example, restriction on the number of failed log-in) and the use of strong passwords (for example, type and number of characters to strengthen security). At the same time, depending on the level of importance of the information systems and information, consider also utilizing advanced means of authentication, such as multi-factor authentication.

(D) Encryption Codes

● Information Management that Makes Use of Encryption Codes

When making use of encryption technology to protect the confidentiality of information that is associated with the provision of CISs, formulate policies for the use of encryption codes and management policies for the keys that are used for the codes (encryption keys). Pay attention to the presence of Japanese and foreign laws and regulations related to encryption technology.

(E) Physical and Environmental Security

● Domains that Require Security

To protect domains with information and information systems that are associated with the provision of CISs (domains that require the ensuring of information security and safety), establish a physical security boundary. At the same time, build a system to monitor the physical environment, and to conduct the appropriate entry/exit management, in order to allow access only to authorized employees and contractors.

From the perspective of preventing malicious activities, restrict the carrying in of unauthorized items into this domain. In addition, it is also effective to restrict personnel from working alone for CI operators that are able to secure multiple workers for the task.

● Management of Devices

Set up devices that are associated with the provision of CISs (such as information systems) in a way that reduces opportunities for unauthorized access, while, at the same time, carrying out maintenance appropriately to continuously maintain availability and integrity. Lay out communications cables and power cables in consideration of the possibility of interception and damage.

To prevent the leakage of confidential information led by the theft of devices such as removable external storage devices, restrict the use of such devices, and establish systems for the prior authorization of the taking out of such devices. Consider also the possibility of information leakage through the disposal and reuse of the devices.

(F) Security Management during Operation

● Procedures of Operation and Responsibilities

Prepare procedure manuals on the operation of information systems that are associated with the provision of CISs while taking into account the points of ensuring the operations fulfill security standards in addition to ensuring accuracy in work.

With regard to changes to the information systems and peripheral equipment (maintenance, repairs, etc.), as adverse impact on information security measures during implementation is also conceivable, define the processes for managing changes in advance, including procedures for authorizing the persons-in-charge, and implement changes based on these processes. In principle, the tools used for maintenance and repairs should be authorized and managed.

Furthermore, from the perspective of preventing unauthorized access to the operating environment of CISs, segregate the operating environment from other environments such as the development and test environments.

● Protection from Malware

As malware, which infects information systems through means such as targeted attack e-mails or USB drives, can potentially cause CISs outages, take preemptive steps to establish systems to detect and guard against malware. At the same time, establish measures and procedures to achieve early recovery even in cases of a malware infection. Also consider the possibility for

malware infection through the computers and devices brought in by contractors, which is difficult for CI operators to manage directly.

For critical information systems with a high level of priority, it is also desirable to make use of multi-engine malware detection software that is expected to improve the detection rate of malware, as well as whitelist-type malware disabling functions, which are characterized by their ability to address unknown threats while at the same time reducing load on the systems.

●Back-ups
Establish back-up policies and procedures in advance for system images and data, based on the possibility of mistaken deletion of important data or the anomalous condition of information systems associated with the provision of CISs (including improper data encryption by ransomware, etc.). From the perspective of ensuring availability, a sufficient volume of back-ups should be made.

As the back-ups that have been made should be usable without any issues where necessary, periodically carry out backup recovery tests.

●Maintaining Logs
From the perspective of monitoring illegal access and operations for information systems that are associated with the provision of CISs, maintain event logs of the information systems and work logs of the personnel in charge of operations. When considering the capacity for the log storage device, the availability of the logs should also be considered.

In addition, manage the logs to prevent intentional tampering or deletion by malicious persons or malware. At the same time, check for the presence of any fraudulent behavior in relation to the logs through periodic checks corresponding to the nature of the logs.

● Management of Operation Software
Software that is used in information systems associated with the provision of CISs is exposed to the potential of attacks that exploit any vulnerable configuration settings. As such, grasp and understand, as far as possible, the individual settings, and strive to ensure safety.

In the event of the occurrence of CISs outages or when the signs of a cyberattack are identified, systematically implement updates to versions that are eligible for support, so that it is possible to receive prompt support from a software vendor. In cases where it is difficult to update to a version that is eligible for support, put in place complementary measures to prevent CISs outages and cyberattacks.

● Management of Technological Vulnerability

Collect, on a regular basis, information on technological vulnerabilities of information systems provided by information security related agencies, and check for any impact on information systems that are in operation. Periodical implementation of scans for vulnerabilities is also expected.

To address technological vulnerabilities, establish work policies and contents in advance, taking into account the need to check for the impact of applying patches on existing information systems. For example, even in situations that call for applying patches urgently, organize the verification test items that should be carried out at the minimum, and implement these tests. In cases where applying patches is difficult even in the event of an emergency, put in place complementary measures such as strengthening the monitoring of information systems.

(G) Security of Communications

● Management of Network Security

From the perspective of protecting the confidentiality and integrity of information handled by information systems that are associated with the provision of CISs, ensure strong network security through means such as using dedicated lines and encryption technology, segregation of networks, maintaining logs, and detecting cyberattacks through monitoring.

● Transmission of Information

When using means of communication such as e-mail, electronic data interchange (EDI), and instant messaging services, to transmit important information associated with the provision of CISs, organize in advance the policies and procedures related to ensuring security, such as confidentiality and integrity. At the same time, work to reach an agreement with the stakeholders who are the recipient party in these transmissions regarding the policies and procedures.

(H) System Acquisition, Development, and Maintenance

● Acquisition of Systems Based on Information Security Requirements

When acquiring or developing new information systems associated with the provision of CISs, and when improving existing information systems, conduct a review that incorporates requirements for information security among the requirements for the system, based on the concept of "security by design."[12] (Where necessary, also conduct a review that incorporates requirements from the perspective of the aforementioned HSE.) As third-party authentication systems that comply with international standards on the security of information systems are

[12] Refers to policies aimed at ensuring information security from the planning and design phases.

also available depending on the CI sector, consider also utilizing authenticated information systems where necessary.

Establish policies, procedures, and environments to realize the development or building of systems that take information security into consideration. In particular, when checking the acceptance of the information system, in addition to checking the requirements related to information security, also consider the need to conduct a vulnerability diagnostic test corresponding to the level of importance of the information system. Furthermore, when outsourcing system development, periodically check with the contractor on the status of compliance with development policies that take information security into consideration.

(I) Supplier Relations

● Information Security in Supplier Relations

In cases where facilities such as information systems that are associated with the provision of CISs, as well as their operation, are replaced by services provided by external suppliers (for example, suppliers of IT services and the components of IT infrastructure), organize information security requirements to reduce the risk of access to the assets of CI operators by suppliers and their subcontractors, and obtain the agreement of the suppliers to these requirements in advance.

In cases where different levels of suppliers are present, improve information security in the supply-chain by ensuring that a certain supplier expects the supplier at the level below them to comply with the same requirements.

● Management of Service Provision by Suppliers

To ensure compliance with the information security requirements that have been agreed upon, constantly monitor the provision of services by suppliers, and conduct reviews and audits on reports drawn up by the suppliers. Due to the need to reassess risks, manage changes in the services provided by suppliers.

(J) Information Security Incident Management

●Management and Improvement of Information Security Incidents

To respond promptly and effectively to information security incidents that have an impact on the safe and continuous provision of CISs, define who the responsible managers of incidents are, and establish procedures such as reporting to internal and external parties and collecting evidence.

In addition, establish systems that enable the application of knowledge gained through incident

responses toward ensuring readiness for future incidents.

(3) Formulation of Individual Policies for Security Management Measures
Consolidate standards, such as actions that should be complied with and decisions in individual security management measures that have been decided upon during the process of addressing information security risks, as separate policies (for example, access control policy, information classification policy, etc.), and transmit these within the organization. Where necessary, also communicate these to contractors.

In the same way as information security policies, verify the validity and effectiveness of the contents of separate policies at regular intervals, and check them in the event that any significant environmental changes have occurred.

(4) Formulation of Plans for Addressing Information Security Risks
Formulate plans for addressing information security risks, which set out goals based on the contents of the information security policies and the criteria for determining the status of achievement of the goals, as well as implementation items and schedule toward the introduction of the security management measures that have been decided upon.

4.1.4. The “Support” Perspective
(1) Securing Resources
In promoting the PDCA cycle for information security measures, or in other words, the establishment, implementation, maintenance, and continual improvement of the PDCA cycle, clearly define the resources required (human resources, budget, etc.), and allocate them appropriately within the organization under the leadership of the management.

From the perspective of addressing the issue of a decline in the standard of information security measures due to environmental changes, the management strives to continuously secure the necessary resources.

(2) Human Resource Development and Awareness-Raising
With regard to the security personnel who will be responsible for promoting information security measures, from the perspective of securing and maintaining the capacity and number of staff necessary for the safe and continuous provision of CISs, it is important to consider beforehand the career paths and wage policies of these security personnel within the CI operator.

Furthermore, as the employees of CI operators fulfill their obligations and responsibilities based on the respective individual information security policies and security management measures,

provide employees with sufficient education and training in the area of information security (where necessary, the training can also be conducted by a contractor). In particular, in developing security personnel who will be responsible for promoting information security measures, it is also expected to utilize, for example, human resource development programs conducted by government organizations and training programs provided by security vendors, participate in exercises and training in collaboration with stakeholders (*refer to 4.2.1. (3)), and obtain qualifications such as the Registered Information Security Specialist certificate. These initiatives are also effective in the objective evaluation and verification of the status of progress in human resource development.

In addition to promoting understanding of information security policies, it is also important to raise awareness through methods such as presenting examples of the consequences that could arise in the event that inadequate efforts are put in, in order to make employees themselves recognize the importance and need to be involved in such information security measures.

(3) Communication

It is important to establish regular opportunities for dialogue between the management, which is responsible for addressing information security risks, and the practitioners, who promote information security measures under the supervision (instructions, monitoring, evaluation, etc.) of the management, and to vitalize communication. When doing so, it is important for the practitioners to share accurate information and offer suggestions through opportunities for dialogue, so as to enable the management to get an accurate grasp of the status in addressing information security risks, and to make accurate decisions and adjustments in responding to that status.

From the perspective of realizing the safe and continuous provision of CISs across the entire CI sector that the organization belongs to, it is also effective to exchange opinions with other stakeholders, including other CI operators and responsible ministries for CIP and agencies with jurisdiction, on the respective roles and the sharing of responsibility, and structure of information sharing and reporting.

4.2. The “Do” Perspective

4.2.1. The Operational Perspective

(1) Introduction and Operation of Information Security Measures

(A) The Introduction of Security Management Measures, and Establishment and Execution of Operational Processes

Based on the plans for addressing information security risks, move forward on the introduction of the security management measures that have been decided upon in the information security

risk treatment, and establish and execute processes to ensure the effective and secure operation of these measures.

(B) Detection of Events That Lead to CISs Outages, and Making Prompt Decisions to Tackle the Problem

In addition to building mechanisms that are capable of the early detection of events that could lead to CISs outages (such as cyberattacks and the anomalous condition of information systems) by grasping the baseline for data that shows the operational status of information systems related to the provision of CISs and combining multiple monitoring results such as alerts and logs, continue sharing events with the relevant departments, etc. following detection, and establish operational processes such as triage (conducting an impact analysis of events such as cyberattacks, and assigning degree of priority for responses).

Through the aforementioned monitoring and detection systems, in situations where specific signs of cyberattack have been identified, it is important to make a prompt decision on the advisability of taking action against the cyberattack through security management measures that have already been introduced (deployment of monitoring functions). At the same time, corresponding to the results of the decision, it is also important to implement dynamic response measures, such as by reviewing the security management measures that have already been introduced (including tuning work for the various devices), or by introducing new security management measures.

(C) Threat Information, Its Analysis, and Verification of Information on Countermeasures

Verify the threat information that is provided regularly by information security related agencies and information on the analysis and countermeasures on the threat information. In cases where the threat information is assessed to have a high degree of urgency, conduct an information security risk assessment urgently, and decide on the need for additional risk treatment measures.

(D) Participation in Information Sharing Activities for Sectors with a High Level of Expertise

With cyberattackers constantly coming up with new means to carry out cyberattacks, the possibility for high-level cyberattacks that target specific CI sectors is also conceivable. Hence, one of the countermeasures is to participate in information sharing activities for sectors with a high level of expertise, such as ISAC,[13] and to apply the information collected through these activities to daily efforts toward risk treatment.

[13] Abbreviation for Information Sharing and Analysis Center. The ICT-ISAC JAPAN includes ICT-ISAC, Financials ISAC Japan, and JE-ISAC, among others.

(2) Addressing CISs Outages

(A) Formulation of Contingency Plans and Business Continuity Plans in Preparation for Cyberattacks

In the event of CISs outages, in addition to securing safety, it is also necessary to restore conditions to an acceptable level within an acceptable timeframe. As such, it is important to ensure incident readiness in preparation against the occurrence of CISs outages.

In view of that, formulate a contingency plan,[14] which sets out the policies for initial response (response during an emergency), and the business continuity plan,[15] which sets out the policies for recovery measures aimed at ensuring continuity of the business (or formulate plans that sets out the same policies as these plans), and establish the necessary organizational systems to execute these plans.

In particular, when formulating or revising contingency plans and business continuity plans with the aim of ensuring readiness against cyberattacks, which is one of the events that can lead to CISs outages, it is recommended to refer to Annex 3: Characteristics of Cyberattack Risks Associated with Incident Readiness, and Matters to Be Considered in the Response and Countermeasures. CI operators that have already prepared a business continuity plan should also draw up a separate plan aimed at achieving complete restoration from the target restoration level to normal service level (business recovery plan).

(B) Establishment of CSIRT, etc., and Agreement with the Relevant Departments on Division of Labor and Other Matters

One of the organizational systems that are necessary for the execution of contingency plans and business continuity plans that take into consideration the characteristics of cyberattack risks, is the establishment of CSIRT[16] (or an organization that fulfills the same functions) internally within the CI operators. It is important for an organization such as CSIRT to agree on the division of labor and response procedures with the relevant departments beforehand.

In particular, for CI operators that have operating environments such as control systems, it is necessary to be fully aware of the possibility that the OT-related department will require specialized knowledge to deal with the situation during the occurrence of CISs outages.

[14] In the 4th Cybersecurity Policy, it refers to plans that specifically set out beforehand, from the implementation aspect, the policies, procedures, and readiness on the initial response (emergency response) that should be taken by the management and employees after the occurrence of CISs outages in a CI operator, or after identifying the possibility for the occurrence of CISs outages.

[15] In the 4th Cybersecurity Policy, it refers to plans that aim to restore CISs that have been impacted by CISs outages in a CI operator to an acceptable level within an acceptable timeframe, based on the concept of mission assurance, and which sets out beforehand the target level, order of priority, and other policies, procedures, and readiness toward recovery.

[16] Abbreviation for Computer Security Incident Response Team. Refers to an organization established to deal with incidents related to computer security, such as information system failures caused by cyberattacks. There are cases where CSIRT is established as a permanent organization and where it is established only during the occurrence of an incident, depending on the operator.

From the perspective of dealing promptly with cyberattacks, it is recommended to consider the need to establish, from times of normalcy, incident readiness, which includes organizations that have specialized knowledge of information security. For example, it is effective to collaborate with cyberspace-related operators and information security related agencies.

(C) Preventing the Spread of Damage and Restoring Services Based on the Response Plans
In cases where events such as a cyberattack are actually detected, and it is decided that response is necessary based on the results of triage, follow the contingency plan and business continuity plan to put in place response measures, including detailed analysis of the event (including forensics of the information system), sharing of information and coordination with the stakeholders (including PR activities directed toward customers), and efforts to prevent the spread of damage and restore services.

With regard to new lessons drawn through the response to CISs outages, incorporate these into the continual improvement processes in the contingency plan and business continuity plan, with the aim of applying these lessons drawn to future response activities and countermeasures.

(3) Conducting Exercises and Training
Periodically conduct exercises and training to ensure the effectiveness of the response plans to CISs outages (contingency plan, business continuity plan, etc.), and to improve the skills of the personnel responsible for putting the measures in action. From the perspective of improving overall protective capability for CIP, it is also recommended to conduct joint exercises and training with CI operators in the same industry, supply-chain, and stakeholders, as well as to examine case studies (studies of past incident responses by other operators).

Joint exercises and training include the cross-sectoral exercises organized by NISC, as well as other programs organized by stakeholders such as responsible ministries for CIP and information security related agencies.

4.3. The “Check” Perspective
4.3.1. The Evaluation Perspective
(1) Monitoring and Auditing
Ensure that the respective initiatives are progressing as planned by monitoring the progress toward the achievement of goals that have been set based on the information security policy, progress of the plans for information security risk treatment, and the progress of education and training aimed at improving awareness of information security.

Risk owners should also periodically monitor changes in the risks accompanying in the

introduction and operation of security management measures (such as changes in the frequency of occurrence of events, changes in the degree of impact that the consequences of events have, etc.). In addition to visualizing the changes in the status of individual risks, it is also expected that monitoring allows them to grasp the changes to the risk status for the organization as a whole.

Furthermore, check that periodical internal audits are conducted (in cases where it is difficult to do so, risk owners should conduct self-inspections at the very least), PDCA cycle for information security measures is built appropriately based on information security policies, and it is maintained in an effective state. In addition to putting effort into nurturing the internal audit personnel necessary for this, it is also expected to check the situation where necessary with the support of external parties who possess advanced expertise.[17]

(2) Review by the Management

The management of CI operators make use of system audits and other resources, periodically check the status of information security measures for the organization, and identify areas where improvements or reviews are necessary. In doing so, in addition to the results of monitoring and audits conducted, also verify the status of measures taken based on the previous review results, changes in the external and internal environments, and feedback from stakeholders.

Document the review results, check the current status of the resources needed for improvements and reviews (human resources, budget, etc.), and issue instructions for improvements and reviews.

4.4. The “Act” Perspective

4.4.1. The Improvement Perspective

(1) Corrective Measures and Continual Improvements

Based on the results of monitoring and auditing, in cases where the target has not been achieved, progress has been delayed, or where points needing improvements have been identified for security management measures, as well as in cases where the management has issued instructions for improvements, implement the necessary measures promptly, and establish measures to prevent recurrence in the future. Repeat this process to enhance the effectiveness of information security measures.

Periodically summarize the implementation status of the PDCA cycle for information security measures in an information security report. Through opportunities for dialogue between the

[17] In METI’s Information Security Audit System, the Registry System for ledger of Information Security Audit Firms, which registers the entities engaged in information security audits (audit companies, information security vendors, system vendors, information security specialist companies, system audit companies, etc.), is prepared and published.

management of CI operators and stakeholders, which utilizes the said report, identify the requirements of stakeholders and apply these to improving the PDCA cycle.

Annex 1: Scope of CI Operators and Critical Information System Examples

CI sectors	Applicable CI operators (Note 1)	Applicable critical information system examples
Information and communication services	- Major electronic communications operators - Major terrestrial base broadcast operators - Major cable television operators	- Network systems - Operation support systems - Organization/operation systems
Financial services - Banking services - Life insurance services - General insurance services - Securities services	- Banks, credit unions, labor credit unions, agricultural cooperatives, etc. - Financial settlement agencies - Electronic credit record agencies - Life insurance services - General insurance services - Securities firms - Financial product exchanges - Money transfer agencies - Financial product clearing agencies etc.	- Accounting systems - Financial securities systems - International systems - External connection systems - Financial institution internetwork systems - Electronic credit record agency systems - Insurance service systems - Securities trading systems - Exchange systems - Money transfer systems - Clearance systems etc.
Aviation services	- Major scheduled air transport operators	- Flight systems - Reservation/boarding systems - Maintenance systems - Cargo systems
Railway services	- Major railway operators including JR companies and major private railway companies	- Railway traffic control systems - Power supply control systems - Seat reservation systems
Electric power supply services	- General electric power transmission and distribution operators and major power producers, etc.	- Electric power control systems - Smart meter systems
Gas supply services	- Major gas supply operators	- Plant control systems - Remote monitoring and control systems
Government and administrative services	- Various ministries and government offices - Local governments	- Various ministry and local government information systems (handling of e-government and e-municipalities)
Medical services	- Medical facilities (Excluding small scale facilities)	- Medical examination record management systems, etc. (electronic patient record systems, remote diagnostic imagining systems, electric medical equipment, etc.)
Water services	- Water service operators and city water service providers (Excluding small scale facilities)	- Water utility and water supply monitoring systems - Water utility control systems, etc.
Logistics services	- Major logistics operators	- Collection and delivery management systems - Cargo tracking systems - Warehouse management systems
Chemical industries	- Major petrochemical facilities	- Plant control systems
Credit card services	- Major credit card services operators, etc.	- Credit card payment systems
Petroleum industries	- Major petroleum refinery facilities and petroleum wholesalers	- Sales order management system - Product management system - Shipping management system etc.

Note 1: The operators listed here are CI operators for which measures should be implemented on a priority basis, and review of the applicable operators is to be carried out based on changes in the business environment and progressive dependence on IT, when the Cybersecurity Policy is revised.

Annex 2: Explanation of CI Services and CI Service Outage Examples

(As of March 2018) (Note 4)

CI sectors	CI services (including procedures)(Note 1)		Examples of CISs outages caused by system failures	Laws and guidelines pertaining to CISs outages reports (Service maintenance levels(Note 2))
	name	Explanation of services (including services) (Relevant laws)		
Information and communication services	- Electrical communication services	- Intermediary for communications of other parties using telecommunication facilities and provision of telecommunications facilities for the communications of other parties (Article 2 of the Telecommunications Business Act)	- Suspension of telecommunications services - Hindrance to safe and stable supply of telecommunications services	- Article 28 (report of suspension of business) of the Telecommunications Business Act - Article 58 (serious accidents requiring reporting) of the Regulation for Enforcement of the Telecommunications Business Act [Service maintenance level] - There should be no accident wherein any trouble in telecommunication facilities causes suspension or quality deterioration of services for more than two hours, affecting 30,000 or more users.
	- Broadcasting services	- Electrical communications broadcast aimed at direct reception by the public (Article 2 of the Broadcast Act)	- Suspension of broadcasting services	- Articles 113 and 122 (report of serious accident) of the Broadcast Act - Article 125 (serious accidents requiring reporting) of the Regulation for Enforcement of the Broadcast Act [Service maintenance level] - There should be no accident wherein any failure in base broadcasting facilities causes a broadcast outage for more than 15 minutes. - There should be no accident wherein any failure in specified terrestrial base broadcasting facilities or base broadcast station facilities causes a broadcast outage for more than15 minutes (or for more than 2 hours for relay station wireless facilities).

CI sectors		CI services (including procedures)(Note 1)		Examples of CISs outages caused by system failures	Laws and guidelines pertaining to CISs outages reports (Service maintenance levels(Note 2))
		name	Explanation of services (including services) (Relevant laws)		
		- CATV services	- Electrical communications broadcast aimed at direct reception by the public (Article 2 of the Broadcast Act)	- Suspension of broadcasting services	- Article 137 (report of serious accident) of the Broadcast Act - Article 157 (serious accidents requiring reporting) of the Regulation for Enforcement of the Broadcast Act [Service maintenance level] - There should be no accident wherein any trouble in telecommunication facilities used for cable broadcasting causes a broadcast outage for more than two hours, affecting 30,000 or more users.
Financial services	Banking services	- Deposits - Loans - Exchange	- Receipt of deposits or periodic deposits (Article 10, paragraph (1), item (i) of the Banking Act) - Lending of loans or discounting of bills (Article 10, paragraph (1), item (ii) of the Banking Act) - Currency exchange (Article 10, paragraph (1), item (iii) of the Banking Act)	- Delay and suspension of deposit payments - Delay and suspension of loan services - Delay and suspension of fund transfers including bank transfers	- Comprehensive Guideline for Supervision of Major Banks - Comprehensive Guideline for Supervision of Small- and Medium-Sized and Regional Financial Institutions - Comprehensive Guideline for Supervision of Affiliated Financial Institutions
		- Financial settlements	- Financial settlements (Article 2, paragraph (5) of the Act on Financial Settlements)	- Delay and suspension of financial settlements	- Comprehensive Guideline for Supervision of Settlement/Money Transfer Agencies
		- Electronic records, etc.	- Electronic records (Article 56 of the Electronically Recorded Monetary Claims Act) - Information provision related to fund settlement (Articles 62 and 63 of the Electronically Recorded Monetary Claims Act)	- Delay and suspension of electronic records and information provision related to fund settlement	- Guideline for Administrative Processes Vol 3.: Financial Companies (12 Electronic credit record agency relationships)
	Life insurance services	- Insurance claim etc. payments	- Receipt of insurance claim etc. payment demands - Insurance claim etc. payment screenings - Insurance claim etc. payments	- Delay and suspension of insurance claim etc. payments	- Comprehensive Guidelines for the Supervision of Insurance Companies
	General insurance services	- Insurance claim etc. payments	- Accident reception - Damage investigations etc. - Insurance claim etc. payments	- Delay and suspension of insurance claim etc. payments	- Comprehensive Guidelines for the Supervision of Insurance Companies

CI sectors	CI services (including procedures)(Note 1)		Examples of CISs outages caused by system failures	Laws and guidelines pertaining to CISs outages reports (Service maintenance levels(Note 2))
	name	Explanation of services (including services) (Relevant laws)		
Securities services	- Negotiable securities trading etc. - Transaction mediation, commission and representation for negotiable securities trading etc. - Negotiable securities etc. settlement commission	- Negotiable securities trading, market derivatives trading or foreign market derivatives trading (Article 2, paragraph (8), item (i) of the Financial Instruments and Exchange Act) - Mediation, commission or representation for negotiable securities trading, market derivatives trading or foreign market derivatives trading (Article 2, paragraph (8), item (ii) of the Financial Instruments and Exchange Act) - Negotiable securities etc. settlement commission (Article 2, paragraph (8), item (v) of the Financial Instruments and Exchange Act)	- Delay and suspension of negotiable securities trading	- Comprehensive Guidelines for the Supervision of Financial Instruments Business Operators, etc.
	- Establishment of financial product markets	- Provision of market facilities for negotiable securities trading or market derivatives trading, and other work related to the establishment of financial product markets (Article 2, paragraphs (14) and (16) and Articles 80 and 84 of the Financial Instruments and Exchange Act)	- Delay and suspension of negotiable securities trading and market derivatives trading	- Article 112 of the Cabinet Office Ordinance on Financial Instruments Exchanges, etc.
	- Money transfer services	- Work related to transfer of corporate bonds, etc. (Article 8 of the Act on Book-Entry Transfer of Company Bonds, Shares, etc.)	- Delay and suspension of transfer of corporate bonds, shares, etc.	- Article 19 (report of accident) of the Act on Book-Entry Transfer of Company Bonds, Shares, etc. - Article 17 (accidents) of the Order on Supervision of General Book-Entry Institutions - Comprehensive Guideline for Supervision of Settlement/Money Transfer Agencies
	- Financial product debt underwriting	- Liability assumption work through underwriting or renewal of debt based on negotiable securities trading etc. targeted transactions (Article 2, paragraph (28) of the Financial Instruments and Exchange Act)	- Delay and suspension of settlement of financial instruments trading	- Article 188 (obligation to prepare, archive, and report documents related to the business of financial instruments business operators) of the Financial Instruments and Exchange Act - Article 48 (documents to be submitted in connection with the business of financial instrument clearing organizations) of the Cabinet Office Ordinance on Financial Instruments Clearing Organizations, etc. - Comprehensive Guideline for Supervision of Settlement/Money Transfer Agencies

CI sectors	CI services (including procedures)(Note 1)		Examples of CISs outages caused by system failures	Laws and guidelines pertaining to CISs outages reports (Service maintenance levels(Note 2))
	name	Explanation of services (including services) (Relevant laws)		
Aviation services	- Air transportation services for passengers and cargo	- Work providing transport of passengers or cargo for charge using airplanes based on demands of other people (Article 2 of the Civil Aeronautics Act)	- Hindrance to safe flight of airplanes - Flight delay and cancellation	- Safety Guideline for Ensuring Information Security for Air Transport Operators
	- Reservations, ticketing, boarding/loading procedures	- Air traveler reservations, air cargo reservations - Airline ticket issuance, fee collection - Airline passenger check-in and boarding, air cargo loading		
	- Flight maintenance	- Airplane inspection and maintenance		
	- Flight plan creation	- Creation of flight plans and submission to Japan Civil Aviation Bureau		
Railway services	- Passenger transport services	- Work providing transport of passengers or cargo for charge using railways based on demands of other people (Article 2 of the Railway Business Act)	- Delay and suspension of railway operation - Hindrance to safe railway transport	- Articles 19 and 19-2 (report of accident) of the Railway Business Act - Article 5 (report of railway accident) of the Railway Accident Reporting Code
	- Ticketing, entry and exit procedures	- Seat reservation, boarding ticket checks on boarding and exiting the train		
Electric power supply services	- General electric power transmission and distribution services - Electric power generation services (services exceeding a certain scale)	- Work adjusting power generation quantity and transporting and supplying electric power in the service area (Article 2, paragraph (8) of the Electric Business Act) - Electric power generation for the retail electricity business, general electricity transmission and distribution business, or specified electricity transmission and distribution business (Article 2, paragraph (14) of the Electric Business Act)	- Electric power supply outages - Hindrance to safe operation of power plants	- Article 3 of the Electricity related Reporting Code [Service maintenance level] - There should be no accident wherein any system failure causes hindrance to supply of over 100,000kilowatts of electric power for more than ten minutes.
Gas supply services	- General gas pipeline services	- Business whereby the service provider provides a Wheeling Service in its service area by using pipelines that it independently maintains and operates (Article 2 of the Gas Business Act)	- Gas supply outages - Hindrance to safe operation of gas plants	- Article 4 of the Gas related Reporting Code [Service maintenance level] - There should be no accident wherein any system failure causes hindrance to supply of gas to 30 or more houses.

CI sectors	CI services (including procedures)(Note 1)		Examples of CISs outages caused by system failures	Laws and guidelines pertaining to CISs outages reports (Service maintenance levels(Note 2))
	name	Explanation of services (including services) (Relevant laws)		
	- Gas manufacturing services	- Business of manufacturing gas using a Liquefied Gas Storage Facility, etc. that the manufacturer independently maintains and operates, which satisfies the requirements specified by Ordinance of the Ministry of Economy, Trade and Industry (Article 2 of the Gas Business Act)		
Government and administrative services	- Local government administration services	- Local administration, other administration work carried out in accordance with laws or government ordinances (Article 2, paragraph (2) of the Local Autonomy Act)	- Hindrance to local government and administrative service operations - Hindrance to protection of residents' rights and interests	
Medical services	- Medical examination	- Examination and treatment	- Hindrance to work of medical examination support departments - Malfunction of medical equipment threatening human life	- Guideline on Safety Management of Medical Information Systems
Water services	- Supply of water through water services	- Work supplying drinking water through piping or other structures to meet general demand (Articles 3 and 15 of the Water Supply Act)	- Water supply outages - Supply of water of unsuitable quality	- Appropriate Implementation of Health Risk Management and Provision of Information Related to Damages to Water Supply Facilities and Water Quality Incidents (Notice issued by the Director of the Water Supply Division, Health Service Bureau, Ministry of Health, Labour and Welfare dated October 25, 2013) - Information Security Guideline for the Water Sector
Logistics services	- Motor truck transportation business - Shipping business - Port transportation business - Warehousing business	- Work providing transport of cargo for charge using motor trucks based on demands of other people (Article 2 of the Motor Truck Transportation Business Act) - Work proving transport of cargo using ships (Article 2 of the Marine Transportation Act) - Work loading and unloading cargo to and from ships at ports based on demands of other people (Article 2 of the Port Transportation Business Act) - Work storing deposited goods in warehouses (Article 2 of the Warehousing Business Act)	- Delay and suspension of shipping - Difficulties in tracking cargo location	- Safety Guideline for Ensuring Information Security for the Logistics Sector

CI sectors	CI services (including procedures)(Note 1)		Examples of CISs outages caused by system failures	Laws and guidelines pertaining to CISs outages reports (Service maintenance levels(Note 2))
	name	Explanation of services (including services) (Relevant laws)		
Chemical industries	- Petrochemical industries	- Production, processing and trade of petrochemical products	- Plant outages - Long-term suspension of product supply	- Safety Principles for Ensuring Information Security for the Petrochemical Sector
Credit card services	- Credit card settlement services	Credit card settlement services (Article 2, paragraph (3), items (i) and (ii) and Article 35-16, paragraph (2) of the Installment Sales Act)(Note 3)	- Delay and suspension of credit card settlement services, and large-scale leakage of credit card information	- Information Security Guideline for the Credit CEPTOAR (*) Regulations will be specified in the basic policy for supervision based on the Installment Sales Act (deferred payment section) in the future.
Petroleum industries	- Petroleum products supply services	- Import, refining, distribution and sale of petroleum	- Oil supply outages - Hindrance to safe operation of refineries	- Safety Guideline for Ensuring Information Security for the Petroleum Sector

Note 1: Excluding services wherein IT is not at all utilized

Note 2: For sectors without any specific standards concerning CISs outages, the service maintenance level is to ensure no CISs outages caused by system failures.

Note 3: Under the amended Installment Sales Act (to be enforced as of the day specified by Cabinet Order within one year and six months from the date of promulgation (December 9, 2016)), Article 2, paragraph (3), items (i) and (ii) and Article 35-16, paragraph (1), item (ii) and paragraph (2)

Note 4: The contents provided in Annex 2 are current as of March 2018. Where necessary, verify the latest updates on laws and regulations with the responsible ministries.

Annex 3: Characteristics of Cyberattack Risks and Matters to Be Considered in the Treatment and Countermeasures that Are Associated with Incident Readiness

The characteristics of cyberattack risks as well as the treatment and countermeasures to be considered, presented from the following page, should be taken into consideration by CI operators when formulating or revising mainly contingency plans (hereinafter, “CP”) and business continuity plans (hereinafter, “BCP”).

The definitions of CP and BCP are as described in section 4.2.1. (2) (A) of this document. However, as there are cases where the names, scope of description, and timing for the start of the operations may differ depending on the sector or operator, it is necessary to consider, in response to the situation of the respective operators, the target documents that should be formulated or revised in consideration of the characteristics and other factors presented on the following pages (hereinafter referred to as “applicable target documents”).

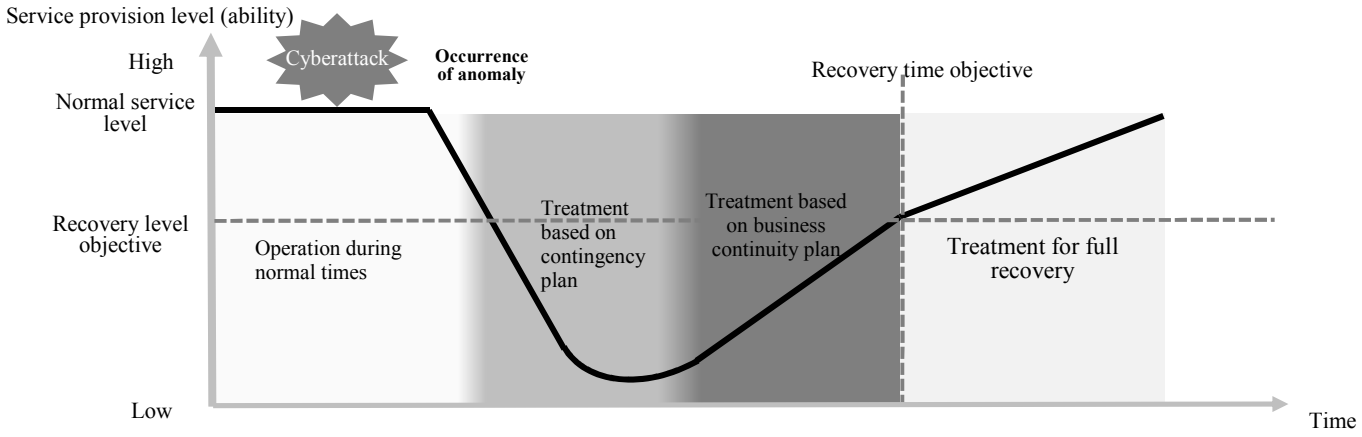
Figure 1 shows an example of the flow from the occurrence of a cyberattack to recovery, as a reference when considering the applicable target documents. Both examples shown in Figure 1 (examples 1 and 2) show the series of processes from the occurrence of an anomaly due to a cyberattack, followed by decline in service levels with time, and then to recovery in service levels after treatment based on the CP and BCP.

In Example 1, treatment has been commenced based on the BCP at an early timing, in order to ensure the early recovery of services. By contrast, in Example 2, treatment has been commenced based on the BCP, after services have been suspended intentionally as a safety measure, and after the implementation of treatment according to safety management provisions. In both examples, the CP and BCP are applicable target documents for which the characteristics and other factors presented on the following pages should be taken into consideration. Treatment based on safety regulations, as shown in Example 2, focuses on reducing and suppressing damage, and generally does not change whether or not the cause of damage is a cyberattack. On the other hand, in cases where IT is used in the treatment, it would be preferable to consider the characteristics and other factors presented on in the following pages.

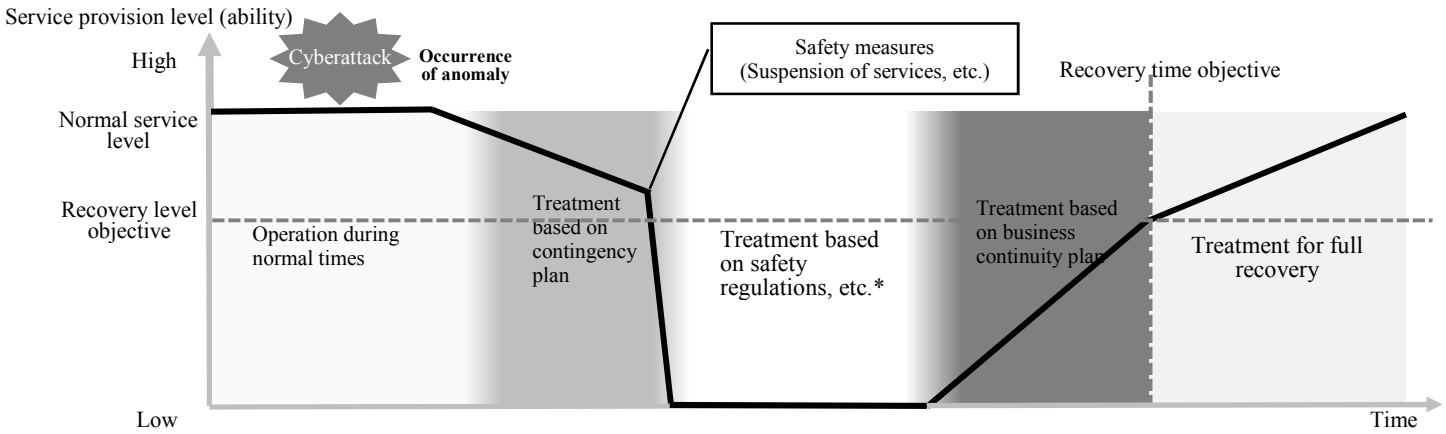
Figure 1: Example of Flow from the Occurrence of a Cyberattack to Recovery

(Various other flows, apart from the following, are also possible.)

Example 1: In the case of working toward swift recovery of services



Example 2. In the case of treatment based on safety regulations, etc. before the start of recovery work (treatment of damage in the case of disaster, accidents, or other emergencies)



* Treatment based on safety regulations, etc. refers to treatment that focuses on reducing and suppressing damage, and generally does not change whether or not the cause of damage is a cyberattack. On the other hand, in cases where IT is used in the treatment, it would be preferable to consider the characteristics of cyberattack risks.

The characteristics of cyberattack risks described hereafter are mutually connected, and the matters to be considered for a certain characteristic may also be effective on other characteristics. Consequently, in the formulation or revision of the CP and BCP, in addition to the matters to be considered with regard to a specific characteristic, it is also necessary to review the treatment and countermeasures based on matters to be considered for other characteristics.

Characteristics of Cyberattack Risks (i)

The presence of attackers, and diverse motives of attack

Cyberattacks, unlike natural disasters, are caused by attackers with a motive. The motives of attack are becoming increasingly diverse, including stealing money and/or information, declaration of principles or assertions, and suspension of services through the destruction of systems. Attacks carried out through various means, corresponding with the diverse range of attackers and motives of attack, are conceivable, ranging from attacks planned and carried out by organizations to attacks carried out through internal criminal acts. However, in many cases it is difficult to identify the attacker and motive of attack beforehand.

Matters to Be Considered with Regard to Response and Countermeasures

[Basic point of view]
Recognition of cyberattack risks, and formulation of scenarios leading up to the occurrence of damage

[Matters to be considered in the formulation and revision of CP and BCP]

- Identify the threat of a cyberattack that could lead to CISs outages in the organization (such as targeted attacks using malware and DDoS attacks) as well as the impact of such an attack. For attacks that have a particularly significant impact on the business, draw up scenarios leading up to the occurrence of damage, and consider the treatment to that scenario.
  - *Example of scenario leading up to the occurrence of damage*
    Due to devices infected with malware (terminals, USB drives, etc.) brought in by maintenance personnel, malware infects the information systems within the organization, and further via the network, invades critical information systems that are the ultimate target of the attack, leading to manipulation and destruction of the system, and leakage of confidential information. As a result, a serious impact on the continuation of services and businesses is made.
- Even in cases where there are concerns for the occurrence of a cyberattack, such as in cases that advanced notification of an attack, suspicions of information leakage, or indicative signs of an attack (such as suspicious communications and increase in logs) is detected, consider the possibility for the need to take steps, such as moving to an alert status in preparation for the occurrence of an attack or outage, or carrying out emergency inspections of the countermeasure status.
  - *Examples of situations where there are concerns for the occurrence of a cyberattack*
    Suggestions of a DDoS attack on systems that provide CISs through the Internet, in which money or the suspension of specific business activities is demanded.

Characteristics of Cyberattack Risks (ii)

Growing sophistication of means of attack

The means of cyberattacks are constantly evolving and becoming increasingly sophisticated. Some possible attacks include attacks that are difficult to avoid simply through countermeasures that are based on existing technology, such as attacks that target new vulnerabilities, and attacks that are carried out using new means that business operators have not anticipated at all.

In the event that an attack is carried out using new means, there is a possibility that the organization will not be able to accurately grasp the degree and scope of its impact.

Matters to Be Considered with Regard to Response and Countermeasures

[Basic point of view]
Regular gathering of information on the means of attack, and timely reviews of CP and BCP

[Matters to be considered when formulating or revising the CP and BCP]

- With regard to the means of attack, regularly gather information provided by stakeholders such as JPCERT/CC, verify if the new means of attack can be handled based on the existing CP and BCP, and revise the plans where necessary.
- When information about new means of attack are obtained, quickly verify the status of countermeasures put in place by the organization, the effectiveness of these measures, and the presence of any damage. At the same time, strengthen the monitoring functions and systems for a certain period of time in preparation for an attack on the organization.
- In order to keep up with the growing sophistication of the means of cyberattacks, add human resources with adequate knowledge and ability to make judgements in the area of cybersecurity to the systems when formulating or revising CP and/or BCP, and during treatment. Where necessary, actively utilize external specialist organizations.
- Even in situations where the scope of impact and other information are not accurately grasped, review the necessary items to be investigated and the order of priority for the investigation when formulating the CP and BCP, so as to maintain the minimum required service level in the provision of CISs.

(Countermeasures during normal times, in preparation for the activation of CP and BCP)

- When a new means of attack is identified as a cyberattack risk, take thorough steps to familiarize key personnel, who may be involved in the treatment when the plans are activated, with the management policies of the risks in question, and the CP and BCP that have been revised.

Characteristics of Cyberattack Risks (iii)

Possibility of an attack that could lead to the rapid spread of damage

Damage from cyberattacks could potentially spread rapidly via networks that originate from the location, which was hit by the attack. There are cases where damage spreads when the malware that has infected a specific terminal duplicates itself on different terminals on the network within the same organization, cases where damage from a cyberattack that has hit an external contractor spreads to the systems within the company, or cases where the company's systems are operated illegally and used for an attack on another company, thereby making the company the perpetrator of the attack.

Matters to Be Considered with Regard to Response and Countermeasures

[Basic point of view]
Response to spread of damage that also takes into consideration means that lead to service interruptions

[Matters to be considered in the formulation and revision of CP and BCP]

- To prevent the spread of damage from a cyberattack, consider measures such as blocking off communication or suspending critical information systems. Get a good grasp of the configuration of networks and systems, and review in advance the points for such blocking or suspension measures.
- When blocking off communications or suspending systems, clarify the parties responsible for making the decision to implement such measures, as there is a possibility that they could have a significant impact on the continuation of CISs. Furthermore, in order to make an accurate judgement, organize information such as the timing and period when suspension of services can be carried out, the scope of impact in the event of suspension, and whether there are any alternative means, when formulating the plans.
- As some information necessary for investigations may become unobtainable after blocking off or suspension, gather the information prior to blocking off or suspension, as far as time permits. Examples of such information that should be collected include memory data and process data that would be lost as a result of the blocking off or suspension, and logs that would be inaccessible during the blocking off or suspension. Consider the methods and procedures for acquiring such information, corresponding with the environment.
- Consider sharing information about the status of response with external contractors for whom there is a possibility for the mutual spread of damage from a cyberattack, and consider disclosing the status of response with users of CISs. The characteristic information for which disclosure should be considered in the event of a cyberattack

includes the means of attack as identified through the response and investigation, the cause of damage (software vulnerability, misconfiguration, etc.), and status of response to the attack (temporary measures to prevent the spread of damage, fundamental measures to address the cause of damage), occurrence of secondary damage to customers, etc., and possibility of future occurrences.

(Countermeasures during normal times, in preparation for the activation of CP and BCP)

- Consider, where necessary, the introduction of countermeasures in preparation for the spread of an attack. Examples of countermeasures include the segregation of network segments (isolation of critical information systems), IPS/proxy servers (blocking off suspicious external communications), and EDR[1] (specification of the scope of impact and isolation of the damaged terminals).

[1] Abbreviation of Endpoint Detection and Response.

Characteristics of Cyberattack Risks (iv)

Possibility of a persistent attack

It is possible for a cyberattack to continue persistently until its goal is accomplished. Some possible cases include cases where the same attack is carried out and the same damage incurred during system recovery when the system is returned with no specific measures taken to the state it was in before the damage, cases where an attack is carried out once again during system recovery, and cases where an attack is carried out once again after countermeasures have been taken to deal with the attack, using means to avoid those countermeasures.

Even in closed environments that are not connected to the Internet or environments that are comprised of systems with a low level of versatility, there can also be cases where an attack is carried out after the collection of information about the system configuration and specifications through various means, over a long period of time.

Matters to Be Considered with Regard to Response and Countermeasures

[Basic point of view]
Consideration of the possibility for the recurrence of a cyberattack and characteristics of the environment

[Matters to be considered in the formulation and revision of CP and BCP]

- Analyze, identify, and respond to (applying patches, removing malware, rebuilding systems, etc.) the causes of the damage (software vulnerability, misconfiguration, etc.) before engaging in the recovery of CISs. Even when restoring services that make use of an emergency system, put the system into operation only after putting in place measures to counter an attack by the same means on the emergency system.
- In preparation for coming under another cyberattack during recovery, separate the system into a team that is responsible for taking countermeasures against the cyberattack, and a team that is responsible for the recovery of CISs. At the same time, review the division of roles and method of coordination and cooperation.
- In cases where signs of a persistent cyberattack are identified (such as repeated attack attempts over a long period of time, recurrence of an attack after measures have been put in place) as a result of investigations based on log analysis and other means, strengthen monitoring functions and systems for a certain period of time even after the recovery of CISs.
- If system recovery must be carried out in situations where the cause of damage has not been identified adequately, make assumptions for the possibility that programs, etc. created by the attacker remain, and strengthen monitoring functions and systems on the

peripheral systems in addition to the system that had suffered damage.

- For response in an environment where systems with a low level of versatility are present, take the following restrictions into consideration: restrictions on the measures that can be taken on the systems in that environment (such as the inability to apply patches due to concerns for the adverse impact on system operations); restrictions on the equipment and networks that can be used in the response (such as difficulties in connecting the investigation equipment or analyzing communications due to special communications specifications); restrictions on the personnel who can be involved (such as the need for personnel who understand the unique system specifications).

(Countermeasures during normal times, in preparation for the activation of CP and BCP)

- Consider the necessary countermeasures, such as monitoring, after recognizing the possibility that damage caused by a cyberattack can be incurred even in a closed environment or systems with a low level of versatility.

Characteristics of Cyberattack Risks (v)

Possibility for the occurrence of simultaneous and multiple attacks

In the case of cyberattacks, regardless of the physical distance, attacks can be carried out simultaneously on targets spreading out across a wide area. Some possible cases include cases where attacks are carried out simultaneously on multiple business locations of an organization, cases where attacks are carried out simultaneously on the organization's system and supplier's systems, and cases where attacks are carried out simultaneously on main systems and emergency systems.

Matters to Be Considered with Regard to Response and Countermeasures

[Basic point of view]
Response to simultaneous and multiple attacks, based on the premise of cooperation with stakeholders

[Matters to be considered in the formulation and revision of CP and BCP]

- In the event where multiple incidents occur simultaneously, it is necessary to assess the need and order of priority for response based on factors such as the impact on business, risk tolerance, and resources necessary for response. Hence, clarify the assessment criteria when formulating the plans.
- In preparation for a cyberattack on suppliers or external contractors who is involved in the provision of CISs, verify the status of preparation of CP and BCP by suppliers and external contractors, as well as the contents of cooperation with the organization during response.
- Consider the possibility for the occurrence of the same cyberattack on multiple CI operators. Through the industry organizations, CEPTOAR, and information security related agencies of each sector, actively share information that contributes to the prevention of damage in other organizations, such as the means by which one's own organization came under a cyberattack, the source of attack, and any characteristic indicators, and strive to prevent the further occurrence of damage across the entire sector.

(Countermeasures during normal times, in preparation for the activation of CP and BCP)

- Consider measures to reduce the possibility of the main system and emergency system becoming unavailable at the same time. Examples of such measures include blocking off communications other than those necessary for the business (such as data copies and back-ups between the main system and emergency system), and segregation of the networks of the main system and emergency system.
- Based on the assumption of situations in which it becomes difficult to maintain CISs

through the systems, prepare alternative means such as manual function controls, substitute work processes carried out by personnel, and the provision of alternative services.

- With regard to the means for information sharing with concerned parties within and outside the organization, consider the possibility that the means for information sharing used during normal times, such as e-mail, may become unavailable due to the impact of the cyberattack, and prepare in advance multiple means of information sharing.

Characteristics of Cyberattack Risks (vi)

Possibility for the occurrence of attacks that are difficult to detect

In cases where inadequate measures for detection are put in place against cyberattacks, there is a possibility for a sustained attack over a long period of time without the attack being recognized. There are cases where detection is avoided through the deletion of logs that lead to the detection of illegal acts, and cases where figures that are different from the actual figures are displayed in order to make it appear as if the systems were operating normally. The longer it takes to detect an attack, the greater the possibility for the spread of damage. Even after an attack is detected, there are many cases where it is difficult to identify the attackers and objective of the attack.

Matters to Be Considered with Regard to Response and Countermeasures

[Basic point of view]
Clarification of disclosure procedures for information, etc. that are related to impact investigations

[Matters to be considered in the formulation and revision of CP and BCP]

- In countering attacks with scope of impact that maintenance operators such as system vendors have difficulty in identifying, there may be cases where requests for cooperation in investigation are made to external incident response organizations or external security vendors. In such situations, it may sometimes be necessary to disclose logs or equipment that has been breached. Hence, clarify the necessary procedures (person responsible for disclosure, assessment criteria, organizations to which disclosure is permitted, and means of provision in order to transmit the information, including confidential information, safely), the information to be disclosed (log items, format, etc.) and any restrictions (types of information that cannot be disclosed, such as confidential information or personal information, etc.).

(Countermeasures during normal times, in preparation for the activation of CP and BCP)

- To investigate indicators of anomaly caused by an attack, have a good grasp of the configuration of critical information systems, and of the operations of the system during normal times as well as the contents of its output logs. Put in place measures to protect the systems against the tampering with and deletion of logs.
- To investigate attacks that have not been detected for a long period of time by tracing them back to the past, store various logs obtained during normal times for a certain period. Review the storage period by taking into consideration the storage period for logs recommended by information security related agencies and security vendors. Refer to publicly available information from information security related agencies, and verify

the situation for the acquisition of recommended logs from normal times for investigative purposes, while also considering acquiring such logs, where necessary.

Characteristics of Cyberattack Risks (vii)

Possibility for the occurrence of an attack that triggers an erroneous judgement or response

A cyberattack can trigger an erroneous judgement or response. Examples of such cases include cases where alerts and figures that are different from reality being displayed on the management systems used for monitoring and control, leading to erroneous judgement, and cases where unauthorized changes are made to the system (such as reducing figures through the operation for increasing figures, system not coming to a stop through the operation used for stopping the system) aiming for system operations undertaken in response to an outage to cause unintended actions.

Matters to Be Considered with Regard to Response and Countermeasures

[Basic point of view]
Get an accurate grasp of the situation through the combined use of various types of monitoring information

[Matters to be considered in the formulation and revision of CP and BCP]

- At the stage where the scope of impact of the cyberattack has not yet been identified, consider the possibility that the impact of the attack may have spread to the management systems, and verify if there are any indicators of tampering or misalignment between different sources of monitoring information.
- In cases where there is suspicion that the management systems have been tampered with, consider multiple procedures for response, such as monitoring and control using other reliable means, including visual confirmation of the status of provision of CISs, and physical control operations by hand.

(Countermeasures during normal times, in preparation for the activation of CP and BCP)

- Consider the structure and mechanisms for verifying if any unauthorized changes have been made to the systems. An example of items that should be checked include hardware configuration (connection devices, etc.), software configuration, file configuration, and system settings.
- Prepare multiple means for monitoring, in preparation for the display of monitoring information that differs from reality, as a result of a cyberattack on the monitoring functions of CISs.

Annex 4: References for Concrete Examples of Measures

Measures	References for concrete examples
4.1. The “Plan” Perspective	—
4.1.1. Perspective of the Organization’s Situation	—
(1) Understanding the External and Internal Environments	• Information Security Management Standard (2016 Revised version), 4.4.2.1
(2) Understanding the Requirements of Stakeholders	• Information Security Management Standard (2016 Revised version), 4.4.3.1 • JIS Q 27002:2014, 18.1.1
4.1.2. The “Leadership” Perspective	—
(1) Commitment of the Management	• Approaches to Cybersecurity for Corporate Management • Cybersecurity Management Guidelines Ver.2.0 • IoT Security Guidelines ver.1.0, Key Concept 1
(2) Formulation of Information Security Policies	• JIS Q 27002:2014, 5.1.1, 5.1.2
(3) Assignment of Responsibilities and Authority for the Roles in the Organization	• Information Security Management Standard (2016 Revised version), 4.4.1.2
4.1.3. The “Plan” Perspective	—
(1) Information Security Risk Assessments	• Risk Assessment Guide Based on the Concept of Mission Assurance in Critical Infrastructure • Security Risk Assessment Guide for Industrial Control Systems • CSMS Certification Criteria Ver.2.0, 4.2, 4.3 • CSMS User Guide Ver.1.2, 3.1, 4.1 - 4.4, 6.1 • IoT Security Guidelines ver.1.0, Key Concept 3 - 7
(2) Decision to Address Information Security Risks	—
(A) Security for Human Resources (Outsourcing)	—
● Matters to be Addressed Before Outsourcing (Selection/Contract Conditions)	• JIS Q 27002:2014, 7.1.1, 7.1.2, 7.2.1, 7.2.2, 7.3.1 • Common Standards for Information Security Measures for Government Agencies (FY2016), 4.1.1 • Guidelines for the Formulation of Standards for Countermeasures by Government Organizations (FY2016), 4.1.1 • Guide for the Formulation of Specifications for Supply Chain Risk Treatment in Information Security for External Contractors, 3.1, 3.2
● Matters to be Addressed During the Contract Period	
(B) Asset Management	—
● Responsibility for Assets	• JIS Q 27002:2014, 8.1.1 - 8.1.4
● Categories of Information and the Handling of Information	• JIS Q 27002:2014, 8.2.1 - 8.2.3 • Common Standards for Information Security Measures for Government Agencies (FY2016), 3.1.1 • Guidelines for the Formulation of Standards for Countermeasures by Government Organizations (FY2016), 3.1.1
(C) Access Control	—
● Management of User Access	• JIS Q 27002:2014, 9.2.1 - 9.2.6 • Common Standards for Information Security Measures for Government Agencies (FY2016), 6.1.3 • Guidelines for the Formulation of Standards for Countermeasures by Government Organizations (FY2016), 6.1.3
● Access Control for Information Systems, etc.	• JIS Q 27002:2014, 9.4.1 - 9.4.3 • Common Standards for Information Security Measures for Government Agencies (FY2016), 6.1.1, 6.1.2 • Guidelines for the Formulation of Standards for Countermeasures by Government Organizations (FY2016), 6.1.1, 6.1.2
(D) Encryption Codes	—
● Information Management that Makes Use of Encryption Codes	• JIS Q 27002:2014, 10.1.1, 10.1.2, 18.1.5 • Common Standards for Information Security Measures for Government Agencies (FY2016), 6.1.5

	• Guidelines for the Formulation of Standards for Countermeasures by Government Organizations (FY2016), 6.1.5 • Export Trade Control Order, Appended Table 1, Item 9(7) Information security equipment or components therefor
(E) Physical and Environmental Security	—
● Domains that Require Security	• JIS Q 27002:2014, 11.1.1 - 11.1.6 • Common Standards for Information Security Measures for Government Agencies (FY2016), 3.2.1 • Guidelines for the Formulation of Standards for Countermeasures by Government Organizations (FY2016), 3.2.1 • IoT Security Guidelines ver.1.0, Key Concept 2
● Management of Devices	• JIS Q 27002:2014, 11.2.1, 11.2.3, 11.2.5 • Common Standards for Information Security Measures for Government Agencies (FY2016), 7.1.1, 7.1.2 • Guidelines for the Formulation of Standards for Countermeasures by Government Organizations (FY2016), 7.1.1, 7.1.2 • IoT Security Guidelines ver.1.0, Key Concept 2
(F) Security Management During Operation	—
● Procedures of Operation and Responsibilities	• JIS Q 27002:2014, 12.1.1, 12.1.2, 12.1.4
● Protection from Malware	• JIS Q 27002:2014, 12.2.1
● Back-ups	• JIS Q 27002:2014, 12.3.1
● Maintaining Logs	• JIS Q 27002:2014, 12.4.1 - 12.4.4 • Common Standards for Information Security Measures for Government Agencies (FY2016), 6.1.4 • Guidelines for the Formulation of Standards for Countermeasures by Government Organizations (FY2016), 6.1.4 • Use and method of analysis of log in relation to response against advanced cyberattack • IoT Security Guidelines ver.1.0, Key Concept 2
● Management of Operation Software	• JIS Q 27002:2014, 12.5.1 • Common Standards for Information Security Measures for Government Agencies (FY2016), 5.2.3, 6.2.1 • Guidelines for the Formulation of Standards for Countermeasures by Government Organizations (FY2016), 5.2.3, 6.2.1
● Management of Technological Vulnerability	• JIS Q 27002:2014, 12.6.1 • Common Standards for Information Security Measures for Government Agencies (FY2016), 6.2.1 • Guidelines for the Formulation of Standards for Countermeasures by Government Organizations (FY2016), 6.2.1 • IoT Security Guidelines ver.1.0, Key Concepts 17, 18, 21
(G) Security of Communications	—
● Management of Network Security	• JIS Q 27002:2014, 13.1.1 - 13.1.3 • Common Standards for Information Security Measures for Government Agencies (FY2016), 7.3.1 • Guidelines for the Formulation of Standards for Countermeasures by Government Organizations (FY2016), 7.3.1
● Transmission of Information	• JIS Q 27002:2014, 13.2.1 - 13.2.3 • Common Standards for Information Security Measures for Government Agencies (FY2016), 7.1.3, 7.2.1 • Guidelines for the Formulation of Standards for Countermeasures by Government Organizations (FY2016), 7.1.3, 7.2.1
(H) System Acquisition, Development, and Maintenance	—
● Acquisition of Systems Based on Information Security Requirements	• JIS Q 27002:2014, 14.1.1 - 14.1.3, 14.2.1 - 14.2.9, 14.3.1 • Common Standards for Information Security Measures for Government Agencies (FY2016), 5.2.1, 5.2.2 • Guidelines for the Formulation of Standards for

	Countermeasures by Government Organizations (FY2016), 5.2.1, 5.2.2 • Guide for the Formulation of Specifications for Supply Chain Risk Treatment in Information Security for External Contractors, 4.1, 4.2 • List of Requirements for Ensuring Security in Procurement of IT Products • Guidebook for the Utilization of the List of Requirements for Ensuring Security in Procurement of IT Products • Manual for the Formulation of Security Requirements in the Government Procurement of Information Systems • IoT Security Guidelines ver.1.0, Key Concepts 8 - 16
(I) Supplier Relations	—
● Information Security in Supplier Relations	• JIS Q 27002:2014, 15.1.1 - 15.1.3 • Common Standards for Information Security Measures for Government Agencies (FY2016), 4.1.1, 4.1.4 • Guidelines for the Formulation of Standards for Countermeasures by Government Organizations (FY2016), 4.1.1, 4.1.4
● Management of Service Provision by Suppliers	• JIS Q 27002:2014, 15.2.1, 15.2.2 • Common Standards for Information Security Measures for Government Agencies (FY2016), 4.1.1, 4.1.4 • Guidelines for the Formulation of Standards for Countermeasures by Government Organizations (FY2016), 4.1.1, 4.1.4
(J) Information Security Incident Management	—
● Management and Improvement of Information Security Incidents	• JIS Q 27002:2014, 16.1.1, 16.1.2, 16.1.6, 16.1.7 • Common Standards for Information Security Measures for Government Agencies (FY2016), 2.2.4 • Guidelines for the Formulation of Standards for Countermeasures by Government Organizations (FY2016), 2.2.4
(3) Formulation of Separate Policies for Security Management Measures	• JIS Q 27002:2014, 5.1.1, 5.1.2
(4) Formulation of Plans for Addressing Information Security Risks	• Information Security Management Standard (2016 Revised version), 4.4.8.4, 4.4.8.5
4.1.4. The “Support” Perspective	—
(1) Securing Resources	• Information Security Management Standard (2016 Revised version), 4.5.1.1, 4.5.1.2
(2) Human Resource Development and Awareness-Raising	• Information Security Management Standard (2016 Revised version), 4.5.2.3, 4.5.2.4, 4.5.2.6 - 4.5.2.8
(3) Communication	• Information Security Management Standard (2016 Revised version), 4.5.3.1 • JIS Q 27014:2015, 5.3.2 - 5.3.4
4.2. The “Do” Perspective	—
4.2.1. The Operational Perspective	—
(1) Introduction and Operation of Information Security Measures	• JIS Q 27002:2014, 16.1.1, 16.1.2, 16.1.4, 16.1.5 • Preparing for Advanced Persistent Threats (APT): A Process Guide for Companies and Organizations • Incident Handling Manual
(2) Addressing CISs Outages	• JIS Q 22301:2013 • JIS Q 27002:2014, 17.1.1 - 17.1.3, 17.2.1 • Guidelines for Information System Operation Continuity Planning in Central Government Agencies ~ A Guide to Formulation (2nd Edition) • IT-BCP Formulation Model • CSIRT Material
(3) Conducting Exercises and Training	• JIS Q 22301:2013, 8.5 • JIS Q 27002:2014, 17.1.3
4.3. The “Check” Perspective	—
4.3.1. The Evaluation Perspective	—
(1) Monitoring and Audits	• Information Security Management Standard (2016 Revised version), 4.6.2.2, 4.6.2.3 • JIS Q 19011:2012

(2) Review by the Management	• Information Security Management Standard (2016 Revised version), 4.6.3.1 - 4.6.3.3 • JIS Q 27014:2015, 5.3.2 - 5.3.6
4.4. The “Act” Perspective	—
4.4.1. The Improvement Perspective	—
(1) Corrective Measures and Continual Improvements	• Information Security Management Standard (2016 Revised version), 4.7.1.1 - 4.7.1.7 • JIS Q 27014:2015, 5.3.5

Definitions / Glossaries

CEPTOAR	Capability for Engineering of Protection, Technical Operation, Analysis and Response; Functions which provide information sharing and analysis at CI operators, and organizations which serve as these functions
CEPTOAR council	The council composed of representatives of each CEPTOAR which carries out information sharing between CEPTOARs; An independent body, not positioned under other agencies, including government organizations
CI	The backbone of people's living and economic activities formed by businesses providing services that are extremely difficult to be substituted; If the function of the services is suspended, deteriorates or becomes unavailable, it could have a significant impact on the people's living and economic activities.
CI operators	Operators designated in "Applicable CI operators" in "Annex 1. Scope of CI Operators and Critical Information System Examples " and groups composed of those designated operators
CI sectors	Sectors regarding CI designated for each business type; Specifically, as follows: "information and communication services," "financial services," "aviation services," "railway services," "electric power supply services," "gas supply services," "government and administrative services (including local government)," "medical services," "water services," "logistics services," "chemical industries," "credit card services" and "petroleum industries"
CI services (CISs)	Services and/or a set of procedures provided by CI operators necessary to utilize those services that are designated as those to be protected in particular for each CI sector, taking into account the extent of their impact on people's living and economic activities
CISs outages	Situation where system failures hinder safe and continuous provision of CI services *With regard to the causes that could give rise to CISs outages, or in other words, threats that should be subjected to Safety Principles, concrete examples are provided in the Annex 2: Examples of Events That Give Rise to Consequences (Threats) from NISC's Risk Assessment Guide based on the Concept of Mission Assurance in Critical Infrastructure
Consequences of an event	The end of an event that has an impact on the objective
Critical information systems	Information systems required to provide CI services, designated for each CI operator, taking into account of the degree of impact on its CI services
Crisis management ministries	The National Police Agency (NPA); Fire and Disaster Management Agency (FDMA); Japan Coast Guard (JCG); Ministry of Defense (MOD)
Cyberattack risk	Risks that can arise in the business as a result of cyberattacks
Cyberspace-related operators	System vendors, which are engaged in the design, construction, operation and maintenance of information systems required for providing CI services; security vendors, which provide information security measures such as antivirus software of those information systems; and platform vendors, which provide the platforms which serve as foundations, including hardware and software of those information systems
Disaster prevention related ministries	The government organizations and ministries stipulated in Article 2, item (iii) of the Basic Act on Disaster Control Measures (Act No. 223 of 1961) which engage in information collection in the event of a disaster

Event	Emergence or changes in a certain series of peripheral situations
Information security related agencies	The National Police Agency Cyber Force; National Institute of Information and Communications Technology (NICT); National Institute of Advanced Industrial Science and Technology (AIST); Information-Technology Promotion Agency (IPA); ICT Information Sharing And Analysis Center Japan (ICT-ISAC Japan); Japan Computer Emergency Response Team Coordination Center (JPCERT/CC); Japan Cybercrime Control Center (JC3)
Information security related ministries	The National Police Agency (NPA); Ministry of Internal Affairs and Communications (MIC); Ministry of Foreign Affairs (MOFA); Ministry of Economy, Trade and Industry (METI); Secretariat of the Nuclear Regulation Authority(*); Ministry of Defense (MOD) * The ministry engaging in cybersecurity-related duties from the perspective of ensuring safety of nuclear power plants
Information sharing	The mutual provision and sharing among relevant entities of information on system failures (information including that on CISs outages and any signs of possible system failures and *Hiyari-Hatto* events) and information that will contribute to ensuring information security This includes both information sharing to NISC and information sharing from NISC.
Information sharing from NISC	The provision of information for contributing to information security measures from the Cabinet Secretariat to CI operators
Information sharing to NISC	The provision of information on system failures (information including that on CISs outages and any signs of possible system failures and *Hiyari-Hatto* events) at CI operators from the CI operators to the Cabinet Secretariat
Information systems	All systems based on IT such as systems for business processing, control field equipment, monitoring and control systems
Responsible ministries for CI	Financial Services Agency (FSA); Ministry of Internal Affairs and Communications (MIC); Ministry of Health, Labour and Welfare (MHLW); Ministry of Economy, Trade and Industry (METI); Ministry of Land, Infrastructure, Transport and Tourism (MLIT)
Service maintenance level	Based on the concept of mission assurance, the level at which CI services are judged to be provided safely and continuously
Stakeholders	The Cabinet Secretariat; responsible ministries for CI; information security related ministries; crisis management ministries; disaster prevention related ministries; CI operators; CEPTOARs; CEPTOAR council; information security related agencies; cyberspace-related operators
System failures	Events that information systems of CI operators do not or cannot perform as expected at the time of their design

References

- ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements.
- ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security management.
- ISO/IEC 27014:2013, Information technology – Security techniques – Governance of information security.
- ISO 31000:2009, Risk management – Principles and guidelines.
- ISO 22301:2012, Societal security – Business continuity management systems – Requirements.
- ISO 19011:2011, Guidelines for auditing management systems.
- NISC, KIGYO KEIEI NO TAME NO SAIBA-SEKYURITEI NO KANGAEKATA, 2016-08-02. https://www.nisc.go.jp/conference/cs/jinzai/dai03/pdf/03shiryou01.pdf
- METI, Independent administrative agency Information-technology Promotion Agency(IPA), Cybersecurity Management Guidelines Ver.2.0, METI, 2017-11-16. http://www.meti.go.jp/english/press/2017/1116_001.html
- RISUKU MANEJIMENTO KIKAKU KATSUYO KENTO KAI, Editor-in-Chief Kazuhico Noguchi, ISO 31000:2009 RISUKU MANEJIMENTO KAISETSU TO TEKIYO GAIDO, NIHON KIKAKU KYOKAI, Japanese Standards Association, 2010-02-25.
- Independent administrative agency Information-technology Promotion Agency(IPA), Technology Headquarters Security Center, Security Risk Assessment Guide for Industrial Control Systems, 2017-10-02. https://www.ipa.go.jp/files/000065768.pdf
- National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity Ver.1.0, 2014-05. https://www.nist.gov/cyberframework/framework
- General Incorporated Foundation JIPDEC, CSMS Certification Criteria (IEC62443-2-1) Ver.2.0, Information Security Management System Accreditation Center, 2016-10-04. https://isms.jp/csms/std/index.html
- General Incorporated Foundation JIPDEC, CSMS User Guide (IEC62443-2-1) Ver1.2, Information Security Management System Accreditation Center, 2016-10-04. https://isms.jp/csms/std/index.html
- METI, JOHO SEKYURITEI KANRI HYOJUN (HEISEI 28 NEN KAISEI BAN), 2016-03-01.

http://www.meti.go.jp/press/2015/03/20160301001/20160301001-1.pdf

- IoT Acceleration Consortium, MIC, METI, IoT Security Guidelines Ver.1.0, 2016-07.
  http://www.iotac.jp/wp-content/uploads/2016/01/IoT-Security-Guidelines_ver.1.0.pdf
- Cybersecurity Strategic Headquarters, Common Standards for Information Security Measures for Government Agencies (FY2016), 2016-08-31.
  https://www.nisc.go.jp/eng/pdf/Common Standards(FY2016).pdf
- NISC, FUSHOCHO TAISAKU KIJUN SAKUTEI NO TAME NO GAIDORAIN (HEISEI 28 NENDO BAN), 2016-08-31.
  https://www.nisc.go.jp/active/general/pdf/guide28.pdf
- NISC, GAIBU ITAKU TOU NI OKERU JOHO SEKYURITEI JO NO SAPURAITIE-N/RISUKU TAIO NO TAME NO SHIYOSHO SAKUTEI TEBIKISHO, 2016-10-25.
  https://www.nisc.go.jp/active/general/pdf/risktaiou28.pdf
- General Incorporated Association JPCERT/CC, Use and method of analysis of log in relation to response against advanced cyber attack, 2015-11-17.
  https://www.jpcert.or.jp/research/apt-loganalysis.html
- METI, List of Requirements for Ensuring Security in Procurement of IT Products, 2018-02-28.
  http://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf
- Independent administrative agency Information-technology Promotion Agency(IPA), Guidebook for the Utilization of the List of Requirements for Ensuring Security in Procurement of IT Products, 2018-02-28.
  https://www.ipa.go.jp/security/it-product/guidebook.html
- NISC, JOHO SHISUTEMU NI KAKARU SEIFU CHOTATSU NI OKERU SEKYURITEI YOKEN SAKUTEI MANYUARU, 2015-05-21.
  https://www.nisc.go.jp/active/general/sbd_sakutei.html
- General Incorporated Association JPCERT/CC, Preparing for Advanced Persistent Threats (APT): A Process Guide for Companies and Organizations, 2016-03-31.
  https://www.jpcert.or.jp/research/apt-guide.html
- General Incorporated Association JPCERT/CC, INSHIDENTO HANDORINGU MANYUARU, CSIRT MATERIARU UNYO FE-ZU, 2015-11-26.
  https://www.jpcert.or.jp/csirt_material/operation_phase.html
- NISC, CHUOH SHOCHO NI OKERU JOHO SHISUTEMU UNYO KEIZOKU KEIKAKU GAIDORAIN –SAKUTEI TEBIKISHO-, 2012-05.
  https://www.nisc.go.jp/active/general/itbcp-guideline.html
- NISC, IT-BCP SAKUTEI MODERU, 2013-06
  https://www.nisc.go.jp/active/general/itbcp-guideline.html

- General Incorporated Association JPCERT/CC, CSIRT MATERIARU. https://www.jpcert.or.jp/csirt_material/