The Cybersecurity Policy for Critical Infrastructure Protection

June 17, 2022
Cybersecurity Strategic Headquarters
Government of JAPAN

This policy has been formulated based on the Cybersecurity Strategy formulated pursuant to the stipulations of Article 12 of the Basic Act on Cybersecurity (Act No. 104 of 2014), and also based on the stipulations of Article 14 (Ensuring Cybersecurity at Critical Social Infrastructure Providers and Other Related Entities) and Article 26, Paragraph 1, Item 5 (Functions under Jurisdiction of the Cybersecurity Strategic Headquarters) of the Act.

Table of Contents

I. Introduction

National life and socioeconomic activities fully depend on diverse social infrastructures, and information systems are being broadly utilized to enable infrastructures to properly fulfill their functions. Under such circumstances, there is a need for the public and private sectors to make all-out efforts to intensively protect critical infrastructure services (CISs), such as information and communication services, electric power supply services and financial services, whose suspension or deterioration is highly likely to have tremendous impact. The private sector should not completely count on the government, nor should the government leave everything to the private sector. Close public-private collaboration is indispensable. Therefore, the government established the Cybersecurity Policy for Critical Infrastructures Protection (the "Cybersecurity Policy"), a shared policy between the government, which bears responsibility for promoting independent measures by CI operators relating to CI cybersecurity and implementing other necessary measures, and CI operators, which independently carry out relevant protective measures, as a basic framework for CI protection, and has promoted this initiative to date.

Threats surrounding CI are becoming increasingly advanced and sophisticated year by year. On the other hand, due to differences in how systems are used in each CI field, the threats faced by each organization are becoming increasingly distinctive. In view of this situation, the government has based this Cybersecurity Policy for Critical Infrastructure Protection ("this Cybersecurity Policy") on the Fourth Edition of the "Cybersecurity Policy for Critical Infrastructure Protection" (the "Fourth Policy"), which serves as a reference for critical infrastructure protection, while also actively updating the policy to further enhance critical infrastructure protection based on public-private collaboration. This will enable critical infrastructure fields as a whole to flexibly respond to trends in future threats and changes in the environment surrounding systems and assets.

1. Purpose of CI Protection

Based on the concept of mission assurance,[1] the purpose of CI protection (CIP) is to maintain safe and continuous provision of CISs. Taking the view that natural disasters, mismanagement, cyberattacks, and changes in the environment surrounding CI constitute risks that make the continuous provision of CISs uncertain, the aim is to ensure resilience and prevent serious impact on national life and socioeconomic activities, from the dual aspects of limiting risk to acceptable levels, and in terms of preparing for CISs outages, taking appropriate action in the event of outages, and ensuring rapid restoration of services.

[1] In the Cybersecurity Strategy (Cabinet Decision of September 28, 2021), the concept of mission assurance is described as follows: "Refers to the condition in which any organization represented by companies, CI operators (excl. related entities), and government bodies understand the operations or services that they should carry out as their missions, and ensure necessary capabilities and resources to reliably execute such missions. This means that senior executives or managers of each organization should identify operations or services that represent their missions and take all responsibility for secure and sustainable provision, rather than making cybersecurity initiatives themselves the goal."

2. Envisaged Future

The future images expected to be realized through the initiatives based on this Cybersecurity Policy are set out hereunder.

(Clarification of responsibilities)

○ The purpose of CIP, the responsibilities of each stakeholder, and the items to be implemented are clarified and disseminated to all stakeholders as a common understanding.

(Organizational governance)

○ Organizational governance functions fully in order to clarify responsibilities and authorities within organizational units, allocate resources appropriately, and accurately implement PDCA cycles so as to ensure that in response to environmental changes the purpose of CIP can be achieved at all times by all organizational units.

(Ensuring optimal protection measures within the organization of each CI operator)

○ Based on the characteristics of the organization and the CISs provided, top management clarifies risks and make all persons within the organization aware of them.

○ Requirements relating to the continuous provision of CISs are clear, with standards and manuals formulated and maintained accordingly, with the status of compliance by related persons being readily assessable.

(Comprehensive measures in response to threats)

○ In order to respond precisely to changes to CI-related threats, measures are promoted for a comprehensive response capable of anticipating future changes in the environment, including the supply chain, etc.

(Communication)

○ Daily communications is conducted within each organization and among stakeholders in order to enhance measures to prevent CISs outages. In addition, in the event that CISs outages occur, thorough communication will ensure a calm response, and continued improvements will be made, leveraging experiences and applying them to future measures.

(Coexistence and co-prosperity with society)

○ Independent and proactive measures by all stakeholders contribute to nurturing a cybersecurity-focused culture and also support sustainable development of society.

○ In addition to CISs being continually provided, stakeholders work together to ensure that CIP measures are well publicized nationally and provide the public with a sense of security.

(Regular assessment and revision)

○ In addition to the measures of all stakeholders being regularly assessed, the policy will be revised

appropriately as and when necessary.

3. Consistency with the Basic Act on Cybersecurity

3.1 Positioning of the Cybersecurity Policy in the Basic Act on Cybersecurity

This Cybersecurity Policy is compiled based on the Cybersecurity Strategy, which was itself formulated pursuant to the stipulations of Article 12 of the Basic Act on Cybersecurity (Act No. 104 of 2014), and also based on the stipulations of Article 14 (Ensuring Cybersecurity at Critical Social Infrastructure Providers and Other Related Entities) and Article 26, Paragraph 1, Item 5 (Functions under Jurisdiction of the Cybersecurity Strategic Headquarters) of the Act.

3.2 Definition of cybersecurity in the Basic Act on Cybersecurity

Cybersecurity is defined in Article 2 of the Basic Act on Cybersecurity and is given to mean that the necessary measures have been taken to safely ensure the secure management of information in electronic and magnetic form, and to ensure security and reliability of information systems and of information and communications networks; and that such a status is being properly maintained and managed.

3.3 Responsibilities of stakeholders under the Basic Act on Cybersecurity

The responsibilities of stakeholders relating to CIP are stipulated in the Basic Act on Cybersecurity as follows.

(1) National government

The national government is responsible for formulating and implementing comprehensive cybersecurity policies pursuant to the stipulations of Article 4 of the Act.

(2) CI operators

CI operators in this Cybersecurity Policy means critical social infrastructure providers as stipulated in Article 12, Paragraph 2, Item 3 in the Basic Act on Cybersecurity, and are comprised specifically of CI operators (excl. related entities) and the associations they form, and local governments.

CI operators are critical social infrastructure providers as stipulated in Article 3, Paragraph 1 of the Basic Act on Cybersecurity and based on Article 6 of the Act, a CI operator (excl. related entities) bears the responsibility to deepen its interest in and understanding of the importance of cybersecurity and to endeavor independently and actively to ensure cybersecurity, as well as endeavoring to cooperate in the implementation of the cybersecurity policy that the national or local government implements, in order to stably and properly provide its services.

Based on Article 5 of the Act, local governments bear the responsibility to formulate and implement independent cybersecurity policies.

(3) Operators involved in the supply chain

Operators involved in the supply chain, etc., necessary to provide CISs refers to cyberspace-related business entities and other business entities as described in Article 7 of the Basic Act. Based on Article 7 of the Basic Act, these cyberspace-related business entities and other business entities are to endeavor independently and actively to ensure cybersecurity, as well as endeavoring to cooperate in the implementation of the cybersecurity policy that the national or local government implements, in the course of their business activities.

4. Policy Groups and Direction of Reinforcing and Refining the Components in this Cybersecurity Policy

Policy groups and direction of reinforcing and refining the components of the Cybersecurity Policy are as shown in the table.

Table Policy Groups and Direction of Reinforcing and Refining the Components of the Cybersecurity Policy

Policy groups in this Cybersecurity Policy	Relation with policy groups in the Fourth Policy	Direction for reinforcing and refining the components of the Cybersecurity Policy from the Fourth Policy
1. Enhancement of incident response capability	Integrate and reorganize sections of "[4] Risk management and preparation of incident readiness" with "[5] Enhancement of the basis for CIP"	○ In order to appropriately conduct CIP, promote the enhancement of incident response capability as part of organizational governance, given the increasing need for initiatives across entire organizations involving top management, CISOs, strategic management, and system personnel, as well as for measures by operators involved in the supply chain. ○ Promote preemptive responses to new threats such as supply chain risks, against the backdrop of significant changes in the cybersecurity environment. ○ Promote appropriate protection measures in response to risks within the organizations of individual CI operators. ○ Consider a unified public-private response with close mutual cooperation between the government and CI operators. ○ Promote an integrated response to preemptive risk management and crisis management when incidents occur.
2. Maintenance and promotion of the safety principles	Basically keep the element of "[1] Maintenance and promotion of the safety principles"	○ Clarify that safety standards, etc., that contribute to the enhancement of incident response capability and risk management are to be developed. ○ Consider survey methods capable of continuously improving the activities of CI operators.
3. Enhancement of information sharing system	Integrate and reorganize sections of "[2] Enhancement of information sharing systems" with "[3] Enhancement of incident response capability"	○ Promote mutual aid based on activation of voluntary activities by CI operators. ○ Consider development of inter-sectoral/public-private partnership frameworks through cooperation with ISAC, etc. ○ Maintain consistency with considerations on the strengthening the National CERTs/CSIRTs framework.
4. Utilization of risk management	Reorganize part of "[4] Risk management and preparation of incident readiness"	○ Top management to clarify risks to organizations based on organizational characteristics. ○ In order to support the realization of CIP policies optimized to individual organizations, in addition to revising existing manuals, set out a clear direction for the development of new guidance, including how to utilize existing standards at individual organizations. ○ Consider utilizing the activities that were conducted in public-private partnerships towards the holding of the 2020 Tokyo Olympic and Paralympic Games.
5. Enhancement of the basis for CIP	Integrate and reorganize part of "[5] Enhancement of the basis for CIP" with "[3] Enhancement of incident response capability"	○ Promote cross-sectoral exercise as a means of verifying the effectiveness of incident response capability. ○ Support the necessary activities for the police to cooperate with CI operators. ○ In cooperation with the Digital Agency implement support measures to ensure cybersecurity in local governments and semi-public sectors related to CI.

II. Executive Summary of This Cybersecurity Policy

The key points for this Cybersecurity Policy ([i] Purpose of CIP, [ii] Responsibilities of stakeholders, [iii] Basic concept, and [iv] Enhancement of incident response capability are as follows.

[i] Purpose of CIP

Based on the concept of mission assurance, the purpose of CI protection (CIP) is to maintain safe and continuous provision of CISs. Taking the view that natural disasters, mismanagement, cyberattacks, and changes in the environment surrounding CI constitute risks that make the continuous provision of CISs uncertain, the aim is to ensure resilience and prevent serious impact on national life and socioeconomic activities, from the dual aspects of limiting risk to acceptable levels, and in terms of preparing for CISs outages, taking appropriate action in the event of outages, and ensuring rapid restoration of services.

[ii] Responsibilities of stakeholders

- Responsibilities of stakeholders are based on the Basic Act on Cybersecurity (Act No. 104 of 2014).
- The national government is responsible for formulating and implementing comprehensive cybersecurity policies.
- Local governments bear the responsibility to formulate and implement independent cybersecurity policies.
- CI operators (excl. related entities) bear the responsibility to deepen their interest in and understanding of the importance of cybersecurity and to endeavor independently and actively to ensure cybersecurity, in order to stably and properly provide its services.
- Cyberspace-related business entities and other business entities shall endeavor independently and actively to ensure cybersecurity in the course of their business activities.

[iii] Basic concept

- In response to the increasingly sophisticated and complex usage of systems and the rapidly increasing threats in cyberspace, CI operators will further promote organization-wide responses, involving top management, CISOs, strategic management, and system personnel. Particular measures will be taken towards promoting cybersecurity as an important priority for management.
- CI operators will clarify the specific characteristics of their organization and implement the most appropriate CIP policies by utilizing risk management that organically combines the perspectives of all organizational levels, from top management through to system personnel.
- In order to respond precisely to changes to threats relating to CI, a comprehensive response is implemented capable of anticipating future changes in the environment, including in the supply chain, etc.

[iv] Enhancement of incident response capability

- Enhance incident response capability through a combination of preemptive risk management and crisis management.
- Incorporate cybersecurity as a management priority in the relationship between top management and experts for ensuring organizational cybersecurity.
- Based on the definition stipulated in Article 2 of the Basic Act on Cybersecurity, to ensure cybersecurity develop and operate an incident response system capable of responding not only to external attacks, but also to events related to system procurement, design, and operation.

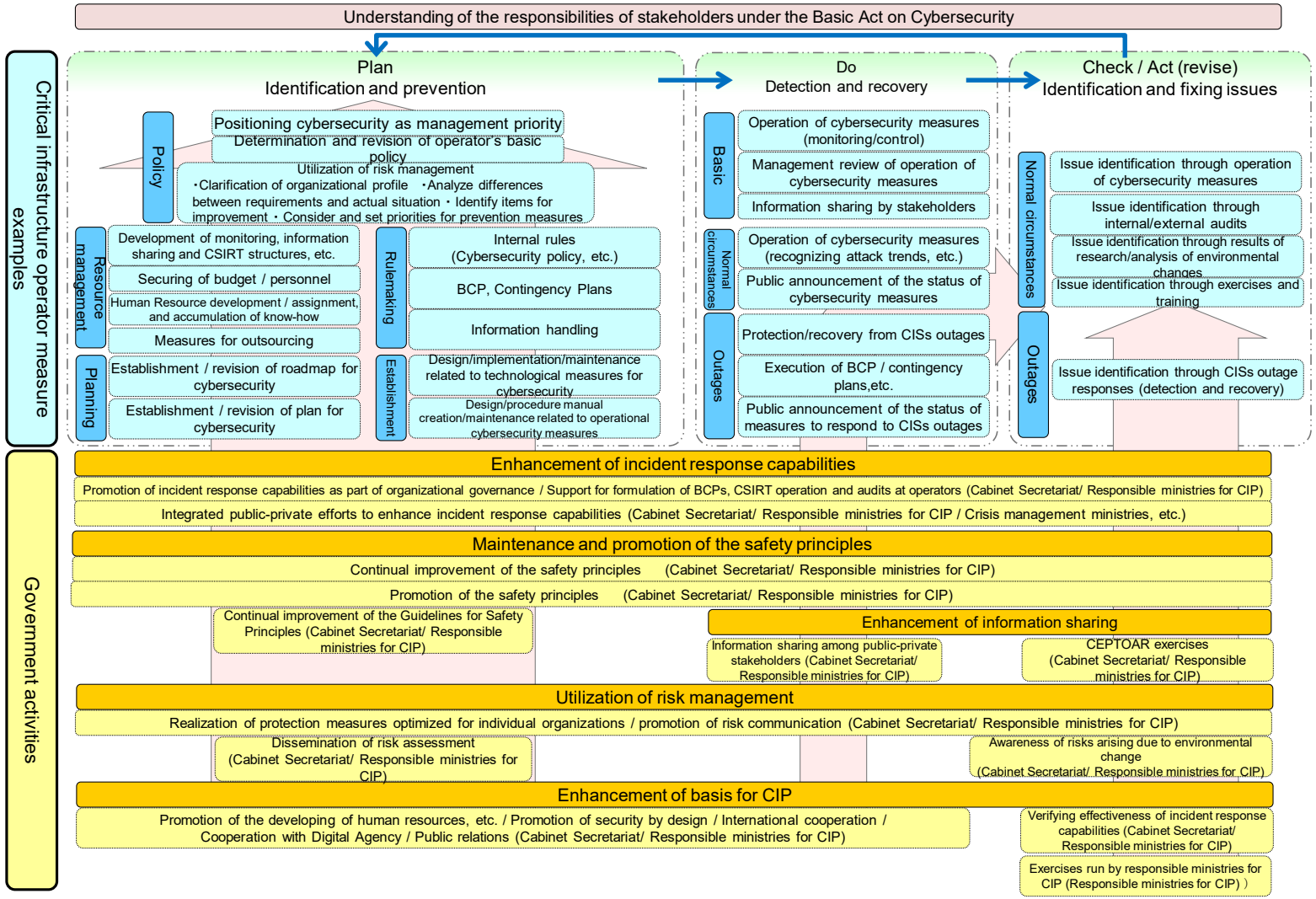


Figure 1 "Critical Infrastructure Operator Measure Examples" and "Government Activities"

III. Basic Concept Relating to Environmental Changes Surrounding CI and Cybersecurity Policy

Many of the causes of CISs outages are attributable to mismanagement, meaning that more appropriate management practices are required not just in response to external attacks, but also in terms of system procurement, design and operation. Moreover, the deepening mutual interdependence of social and economic activities is making risks more sophisticated and complex, meaning that it is important to view supply chains in their entirety. For this reason the positioning of operators involved in the supply chain, etc., necessary to provide CISs will be clarified. Furthermore, in addition to incorporating cybersecurity as part of organizational governance and fundamentally enhancing incident response capabilities, CIP policies optimized for individual organizations will be realized. When enhancing the incident response capability, the following measures will be promoted: (i) organically combining the perspectives of all organizational levels, from top management through to system personnel, and (ii) engaging in both pre-emptive response through risk management and crisis management.

1. Changes in the Cybersecurity Environment Surrounding CI

Since the publication of the Fourth Policy that was determined in fiscal 2017, the environment surrounding cybersecurity has undergone significant changes. In particular, in the first year of the 2020s, the world was faced with a series of discontinuous changes due to the impact of the COVID-19 pandemic, which resulted in the accelerated use of digital technologies. What is more, the 2020s are like to be a "Digital Decade" in which great strides are made toward the realization of Society 5.0, in which cyberspace is integrated with physical space at an advanced level. Meanwhile, the uncertainty surrounding cyberspace is constantly growing and changing in nature. Changes in the international community are accelerating and becoming more complex, including emerging interstate competition. This is accompanied by the progress of information and communications technology, as well as a deepening interdependence of complex economic and social activities. It was against this backdrop that in 2021 the Tokyo 2020 Olympic and Paralympic Games (hereinafter referred to as the "Tokyo Games") were held, and the Digital Agency was established to lead the formation of a digital society.

It was amidst such changes in the environment that on September 28, 2021 the new Cybersecurity Strategy was approved by the Cabinet. This strategy stipulates that the efforts undertaken together by the public and private sectors to build response capabilities and promote risk management in preparation for the Tokyo Games will be utilized to improve cybersecurity in Japan. In addition, the strategy stipulates that in the basic development and management principles for the information systems of the national government, local governments, and semi-public sector to be formulated by the Digital Agency, the basic principles for cybersecurity will also be set out and implemented. The strategy also

stipulates that amidst an increasingly severe security environment surrounding Japan, the government's overall ability to respond seamlessly would be fundamentally enhanced, in order to defend against and deter cyberattacks, and improve capabilities to recognize the situation in cyberspace.

Focusing on CI, service outages attributable to environmental changes have already begun to occur in some areas. The risks of CISs outages are diverse and not limited to cyberattacks, also including natural disasters and outages arising from human error, etc. In particular, service outages that could have been prevented with proper organizational management are becoming more noticeable. Furthermore, advances in inter-system connectivity means that the scale of the impact of service outages is becoming increasingly large.

2. Scope of CIP

When CI operators provide CISs based on various related laws and ordinances, it is necessary that they recognize themselves to be actors in CIP and engage in CIP-related activities accordingly. To this end the responsible ministries for CIP clarify the CI operators in various CI sectors, so that they are able to identify themselves as CI operators. In addition, the Cabinet Secretariat and responsible ministries for CIP review the scope of CIP while taking into account changes in the environment surrounding cyber security, events that have occurred, and their impact.

With regard to the CI sectors and systems subject to such measures, following on from the Fourth Policy and as shown in Annex 1, there are a total of 14 CI sectors: information and communication services, financial services, aviation services, airports, railway services, electric power supply services, gas supply services, government and administrative services, medical services, water services, logistics services, chemical industries, credit card services, and petroleum industries. As in the Fourth Policy, CISs and service maintenance levels continue to be set out in Annex 2.

Furthermore, in order to ensure the overall safety and security of cyberspace as it becomes increasingly public, interconnected and interrelated, all organizations involved in CI are expected to act responsibly, taking an overall view of the entire supply chain, while recognizing that risks are becoming increasingly sophisticated and complex as economic and social activities become more interdependent. To this end, operators involved in the supply chain, etc., necessary to provide CISs will also be considered to bear responsibilities stipulated in Article 7 of the Basic Act on Cybersecurity (cyberspace-related business entities and other business entities) and to engage in responsible activities.

3. Cybersecurity as part of organizational governance

Conventionally it has often been the case that system personnel alone have engaged in activities relating to cybersecurity. However, against a backdrop of accelerating utilization of digital technologies brought about by advances in digital transformation (DX), there are more and more matters that required the attention of top management, such as the identification of risks and consideration of

countermeasures based on a holistic view of an entire organization. For example, some of the main factors behind CISs outages in recent years have been natural disasters and mismanagement, with mismanagement in particular being the cause of many. In order to reduce the number of similar incidents that occur repeatedly and could have been prevented with proper management, activities across entire organizations are critically important. To this end activities will be promoted to incorporate cybersecurity as an integral part of organizational governance.

4. Realization of CIP policies optimized to individual organizations

As risks are becoming more sophisticated and complex, the required level of cybersecurity and activities are diverging depending on the particular sector and operator involved. Furthermore, advances in DX are expected to significantly change the environment surrounding CI and associated risks in the future. Accordingly, in order to enhance the effectiveness of cybersecurity it is not enough to simply refer to uniform safety standards, etc., but is rather of ever-increasing importance to clarify the characteristics of individual organizations and implement appropriate CIP policies through risk management that organically combines the perspectives of all levels from top management through to system personnel.

To that end, after having not only responded to service outages after they have occurred, but also having appropriately understood for each organization the nature of the CISs concerned and their relationship with society as they change in the future, activities will be promoted to enable organizations to clarify the risks of CISs outages arising from natural disasters, mismanagement and cyberattacks, etc., and respond to them. This will also include the supply chains and overseas bases necessary for the promotion of the CISs concerned.

IV. Activities During the Term of This Cybersecurity Policy

1. Enhancement of Incident Response Capability

The recent situation for cybersecurity in CI has increasingly come to require an integrated organizational response, including top management, CISO, strategic management, and system personnel. CI operators are required to incorporate cybersecurity into organizational governance and promote the enhancement of incident response capability, including devising and maintaining appropriate preventive measures and response measures when damage occurs that are best suited to the organization concerned.

This Cybersecurity Policy clearly identifies the laws and ordinances relating to cybersecurity, and promotes measures for the enhancement of incident response capability in government and at CI operators.

1.1 Incident response capability as part of organizational governance

Recent causes of disruptions to the provision of CISs include natural disasters, mismanagement and cyberattacks, and as many of these could have been avoided if appropriate organizational management had been in place, it is necessary to appropriately engage in response capability management across entire organizations.

Although appropriate responsibility and authority need to be clarified at each level of the organization at CI operators, and the entire organization must make an integrated organizational response to CIP, top management commitment is necessary to include a CIP perspective as one of the organizational operational risks.

In this Cybersecurity Policy the Cabinet Secretariat sets out the rules in the Guidelines for Safety Principles relating to organizational governance that will contribute to enhancing incident response capability.

Based on this Cybersecurity Policy and the formulated Guidelines for Safety Principles, CI operators make efforts to improve the incident response capability of their organizations.

(1) Important perspectives in organizational governance

In order to enhance incident response capability as part of organizational governance, four perspectives[2] are required as set out in the *Q&A Handbook on Cybersecurity Laws and Regulations Ver 1.0* (March 2, 2020; NISC).

① Relationship between internal control systems and cybersecurity

Organizational capabilities relating to cybersecurity could be said to be part of the internal control systems of an organization. The obligation of top management to construct internal control systems

[2] Specifically from Q3 to Q6.

could therefore feasibly incorporate an obligation to ensure appropriate cybersecurity.

In terms of the kind of structures that need to be developed, there is no single fixed template, but rather a decision needs to be made by each organization, taking into consideration various circumstances, such as the necessity, effectiveness, and cost of implementation, which will vary according to the scale and characteristics of the business operations operated by each organization. In addition, it is not necessary for organizational decision-making bodies to determine the fine details of cybersecurity structures and capabilities, but rather to determine the basic policy of the organization.

② Cybersecurity and the responsibilities of directors, etc.

In the event that due to cybersecurity structures determined by an organization's decision-making bodies not being appropriate for the scale and nature of the business of the organization concerned the information possessed by the organization has been leaked, falsified or lost (deleted), or damaged (destroyed) causing damage to the company concerned, top management involved in deciding such structures could be held liable for damages based on negligence of duty. In addition, the same also applies to cases where even if the cybersecurity structures were appropriate in and of themselves, those structures were not operated as actually stipulated, and that this was known to top management (or auditors), or they could have known about such a situation if warned, but left the situation unattended for a long period.

In the event that the leakage, etc. of personal information causes damage to third parties, then where top management or auditors are maliciously or grossly negligent in neglecting to perform their duties, they shall also be liable for damages to third parties.

③ Audits, etc. in order to ensure appropriateness of cybersecurity structures

Measures to ensure that cybersecurity structures within an organization are appropriate include various audits, such as internal audits, information security audits, and system audits, as well as whistleblowing, information disclosure and the establishment of CSIRT.

④ Cybersecurity and information disclosure

Disclosing organizational information relating to cybersecurity serves to fulfil an organization's accountability to society, and it can also be expected to be fairly evaluated by stakeholders as a sign of a company's proactive efforts to engage in security measures as priority management issue from an organizational perspective. Furthermore, such disclosure can also be expected to lead to enhancement of cybersecurity measures within the organization concerned.

Therefore, it is desirable for organizations to disclose their cybersecurity activities by actively utilizing existing disclosure systems.

(2) Responsibilities of top management, CISO and other roles in CIP

As DX has progressed IT has transformed from having the role of an information system to become

a part of business infrastructure, and IT failures now have a direct impact on business. To date IT-related risks have been considered as individual and distinct systemic issues, but it is now necessary to redefine them as a major business-related risk. In other words, it is essential for top management to understand the impact IT failures could have on business and all potential failures need to be managed as acceptable risks.

Given this situation, it is necessary to integrate the specialist and technical issues relating to cybersecurity with the business operation issues that are faced by top management, after having first clearly defined roles and responsibilities across an organization as a whole, including top management, CISO, strategic management, and system personnel, and also at operators involved in the supply chain. However, top management do not necessarily possess the requisite cybersecurity-related knowledge. It is therefore important for them to appoint CISOs and others who are capable of tackling IT risks from a managerial standpoint as part of the top management team, and have them play a role in business operations.

1.2 Activities to enhance incident response capability

In the promotion of DX, incorporating cybersecurity into products and services contributes to enhancing corporate competitiveness and forms the basis for maintaining and developing corporate activities. To that end the Cabinet Secretariat is encouraging those involved in the provision of products and services at companies to recognize security by design as a common value. It is also promoting proactive responses to new threats such as supply chain risk, and encouraging stakeholders to take measures to enhance security throughout the supply chain, transcending organizational boundaries. To that end the Cabinet Secretariat sets out information on the importance of BCP/IT-BCP, contingency plans, CSIRT, and audit systems, etc., and policies on their formulation, so that CI operators, including both large-scale operators as well as small and medium operators, can effectively develop such capabilities. In addition, in cooperation with the responsible ministries for CIP the Cabinet Secretariat considers support measures tailored to organizations in each CI sector, so that CI operators can develop such measures.

Risks of service outages present different challenges depending on the sector or business concerned. To that end, each organization must assess the risks it faces and implement appropriate CIP measures. The Cabinet Secretariat promotes appropriate CIP measures in response to risks within the organizations of individual CI operators. As part of these efforts, through cybersecurity-related guidelines the Cabinet Secretariat works to raise awareness among CI operators about the most effective measures to take, based on top management-led establishment of structures, and the latest cyberattack tactics and damage status, etc. In order to share any issues that arise when implementing the measures, as well as best practices, and also the latest threat and incident-related information, the Cabinet Secretariat works to further expand the information-sharing network between the private and public sectors, such as by building information sharing platforms, while also actively utilizing independent administrative

agencies with cybersecurity-related knowledge, and agencies that possess incident information sharing and analysis functions, including the Information Sharing and Analysis Center (ISAC).

(1) BCP/IT-BCP

From the perspective of implementing mission assurance, it is necessary for CI operators to develop and maintain business continuity plans (BCP) and IT-specific BCP (IT-BCP) as part of their risk management initiatives. In addition to formulating policies and measures to prevent cyber incidents, CI operators develop IT-BCP as part of their BCP in order to contain adverse business continuity-related impacts to an acceptable level. If system outages escalate to impact an entire organization, it is necessary to ensure that the IT-BCP functions as initially planned, after which a smooth transition can be made at some point to the BCP. When developing a BCP for a particular organization it is necessary to ensure seamless interconnectivity between IT-BCP and BCP.

(2) Effective operation of CSIRT

CI operators are required to establish CSIRT and enhance and strengthen structures to make them capable of responding accurately at all times, from normal circumstances through to incidents. A CSIRT is structure established to monitor information systems and other systems for any security problems that may occur in companies or government agencies, etc., and to analyze the causes and investigate the scope of impact if a problem should occur. Not only does the CSIRT respond to incidents when outages have occurred, it also works to prevent cybersecurity incidents, collect relevant information, and detect outages.

(3) Utilization of the safety principles

CI operators engage in reviews of internal regulations in their own organizations by referring to guidelines compiled for the CI sector. This is expected to lead to an improvement in organizational structures and capability. Details are set out in “2. Maintenance and promotion of the safety principles” below.

(4) Enhancement of information sharing system

To ensure that they can respond to cybersecurity trends that change on a daily basis, CI operators engage in efforts to further enhance public-private and internal-external sectoral information sharing systems. Details are set out in “3. Enhancement of information sharing system” below.

(5) Utilization of risk management

CI operators must understand the risks according to the characteristics of their own organizations, set targets for improvement based on the current situation, and have a functioning mechanism capable of implementing continuous improvements. Details are set out in “4. Utilization of risk management” below.

(6) Response to outages

At times when outages occur it is important to move to implement BCP/IT-BCP and contingency plans, which have been formulated based on issues identified in the process of risk management. In addition, given the recent speed of change in the cybersecurity-related environment, it is necessary to also give consideration to responses to unanticipated crises. It is expected that CI operators will make an integrated response to risk management and crisis management.

Furthermore, in order to respond appropriately and swiftly at times of outages, CI operators are required to ensure that no inconsistencies arise in the transfer of information between stakeholders concerned. Accordingly they are expected to work to enhance communications on a daily basis.

In addition, the latest threats and vulnerabilities obtained from the operations of systems personnel can also lead to assessment and improvement in CIP measures. CI operators are expected to apply management policies to overcome any risks relating to discovered threats or vulnerabilities.

(7) Audit and verification

CI operators must implement audit and verification activities in order to verify the operational status of their incident response capabilities relating to CISs outages within their own organizations and the status of appropriate management policies based on risk assessment.

Internal and external audits could be implemented depending on the entity conducting the audit, and as a part of the work of top management the kind of audit that is considered to be most effective for the organization concerned is determined and implemented. In internal audits in particular, efforts should be made to clarify the roles of the audit department so as to assist in improvements to incident response capability within the organization.

CI operators are expected to ensure that the results of verification are reported to top management, and that any improvements are implemented as necessary.

(8) Other activities

Other activities implemented by CI operators that contribute to enhancing incident response capability including holding exercises, human resource development and international cooperation. Details are set out in “5. Enhancement of the basis for CIP” below.

1.3 Integrated public-private efforts to enhance incident response capability

National life and socioeconomic activities fully depend on diverse social infrastructures, and information systems are being broadly utilized to enable infrastructures to properly fulfill their functions. Under such circumstances, there is a need for the public and private sectors to make all-out efforts to intensively protect critical infrastructure services (CISs), such as information and communication services, electric power supply services and financial services, whose suspension or deterioration is highly likely to have tremendous impact. The private sector should not completely count on the

government, nor should the government leave everything to the private sector. Close public-private collaboration is indispensable.

The security environment surrounding Japan is becoming increasingly severe and the Cybersecurity Strategy (approved by the Cabinet September 28, 2021) stipulates that it is vital to secure Japan's resilience against cyberattacks and increase Japan's ability to defend the nation from cyberattacks (defense capabilities), deter cyberattacks (deterrence capabilities), and be aware of the situation in cyberspace (situational awareness capabilities), while fundamentally enhancing the government's overall ability to respond seamlessly. These are to be embodied in CIP.

In terms of defense capabilities, further improvements are made in this Cybersecurity Policy to ensure the commitment of government agencies and CI operators from the viewpoint of mission assurance, and to enable CI operators to work on CIP measures that are optimized for their own particular organizations.

It is important to ensure effective deterrence capabilities in order to respond accurately to heightened threats. To this end, through collaborations based on mutual trust between public and private organizations, in addition to further enhancing situational awareness capabilities, efforts will continue to be made to enhance abilities to detect, investigate, and analyze cyberattacks in order to identify and hold attackers accountable, and to strengthen deterrence capabilities. Also towards this goal, activities from the perspective of security will be enhanced, through flexible mutual cooperation among relevant organizations according to their various roles.

1.4 Review of the protection scope of CI

In order to achieve CIP for the purpose of mission assurance, "protection as plane" including supply chains need to be ensured in consideration of the current status of interdependency among CI sectors and dependency on external services (services provided by outsources or other peripheral businesses other than conventional CI operators) and in light of environmental changes, a situation such that the advancement and expansion of new technologies are increasing risks and possible damage for socioeconomic systems as a whole.

Efforts are being made to encourage CEPTOAR participation in existing CI sectors, ascertain the current status of external services on which existing CI sectors are highly dependent, and review the scope of CI to be protected. However, in the meantime, new types of businesses in multiple sectors have come to join CEPTOARs or have come to receive certain information (such as newsletters compiling disclosed information) from the Cabinet Secretariat and new moves to seek collaboration beyond the existing business fields are observed. The Cabinet Secretariat continues the review of the CIP scope in order to realize "protection as plane" for ensuring safe and continuous provision of CI services, while flexibly responding to changes in social environment.

In addition, given the increased need for a security perspective in the protection of national life and socioeconomic activities, working with stakeholders the Cabinet Secretariat continuously reviews the

scope of CI sectors in order to strengthen measures in CI sectors where information sharing should be promoted for protection purposes and enable proper protection of services that should be newly positioned as CI.

2. Maintenance and Promotion of the Safety Principles

In view of the changing environment surrounding CI and the diversification of threats, it is necessary for CI operators to understand the risks that apply to their own organizations and to realize a situation in which it is possible to implement CIP measures optimized for their organizations. To that end stakeholders are expected to engage in activities to maintain and promote the safety principles.

The structure relating to safety principles is shown in Figure 2. Specifically, based on cooperation with responsible ministries for CIP, the Cabinet Secretariat stipulates measures towards ensuring cybersecurity that are commonly required in all sectors, which are compiled as the Guidelines for Safety Principles for Ensuring CI Security (hereafter the "Guidelines for Safety Principles"). Furthermore, the Cabinet Secretariat formulates manuals to specifically demonstrate the procedures stipulated in the Guidelines for Safety Principles (hereafter "manuals") and guidance and other related documents that set out individual measures and other items to bear in mind. Based on the Guidelines for Safety Principles and manuals, "regulations" stipulated by the government in compliance with relevant laws, "recommendations" and "guidelines" developed by the government according to relevant laws, "standards" and "guidelines" in the whole-sector developed by sector-specific groups to respond to relevant laws and public expectations, and "internal policies" prepared by CI operators themselves to respond to relevant laws and expectations of public and customs are all formulated (hereafter referred to collectively as the "safety principles").

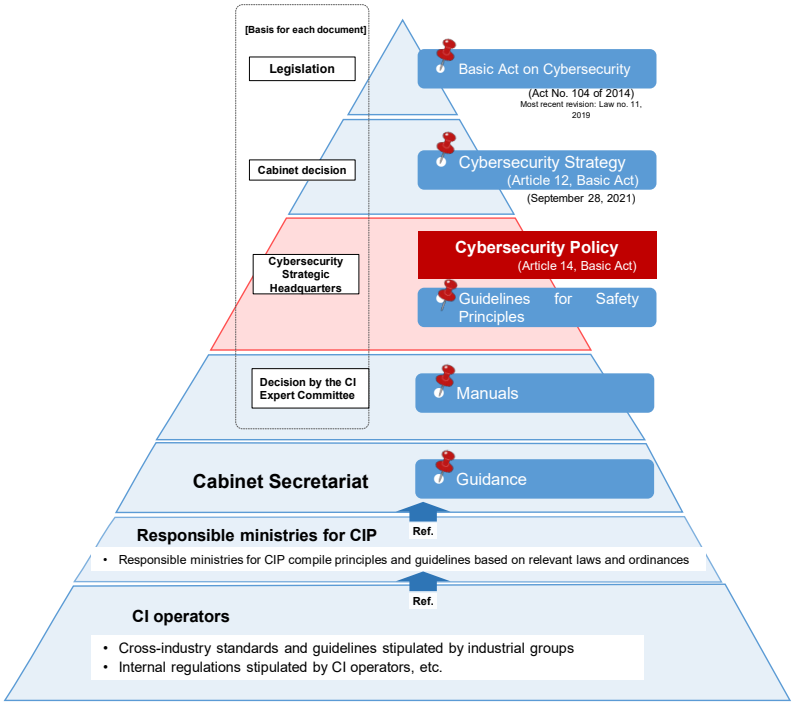


Figure 2. Structure for safety principles relating to CIP

2.1 Continual improvement of the Guidelines for Safety Principles

Particularly from the perspective of enhancing incident response capability, the Cabinet Secretariat reviews the Guidelines for Safety Principles and manuals. These reviews are conducted in principle once every three years. However, this principle does not apply in cases in which significant changes in social trends bring about a situation in which the current Guidelines for Safety Principles and manuals are rendered inadequate for purpose. Furthermore, guidance, which comprises related documents to the Guidelines for Safety Principles and manuals, will be revised in a timely manner based on operational knowledge obtained, in order to enable a prompt response to the significant changes in the surrounding environment and incidents, of which the recent increase in the number of ransomware attacks is just one example. In addition, if there are any international standards or overseas guidelines that could provide a source of reference for Japan, then consideration shall be given to adopting such measures as appropriate.

Matters relating to the Guidelines for Safety Principles that are to be newly developed during the term of this Cybersecurity Policy are as follows.

(1) Development of standards relating to organizational governance

With a view to enhancing the description of measures to incorporate cybersecurity as part of organizational government, the following items that are set out in the *Q&A Handbook on Cybersecurity Laws and Regulations Ver 1.0* (March 2, 2020) will be used to enhance the descriptions detailed in the Guidelines for Safety Principles: (i) Relationship between internal control systems and cybersecurity; (ii) Cybersecurity and the responsibilities of directors, etc.; (iii) Audits, etc. in order to ensure

appropriateness of cybersecurity structures; and (iv) Cybersecurity and information disclosure.

(2) Development of standards relating to supply chains

Descriptions in the Guidelines for Safety Principles concerning the response to supply chain risks will be enhanced, in light of the heightened risks relating to cascading CISs outages originating in supply chains, such as: (i) risk of unauthorized functions becoming embedded in products during supply chain processes; (ii) risk of supply disruption of equipment and services due to political and economic conditions; and (iii) risk relating to handling or availability of information in cloud services or similar external services.

(3) Development of standards for continual improvements specific to individual organizations

Basic concepts relating to measures optimized for individual organizations will be incorporated in the Guidelines for Safety Principles, and documentation will be compiled that sets out specific implementation methods.

(4) Development of other standards

In order to respond swiftly to cyberattacks and other threats to control systems at plants and factories, the importance of developing cross-organizational IT and OT, and developing OT security human resources will be highlighted.

2.2 Continual improvement of the safety principles

When it is responsible ministries for CIP that establish safety principles themselves, based on revisions to the Guidelines for Safety Principles, the ministries work to continually improve these safety principles, also taking sector-specific risks into account. At such times the effectiveness of activities is maximized through a process of advance adjustment of role allocation between the Cabinet Secretariat and the responsible ministries for CIP. When it is CI operators that are establishing safety principles, they work to continually improve these safety principles so as to comply with the stipulations of relevant laws and ordinances, and based on revisions to the Guidelines for Safety Principles.

Specifically, based on knowledge learned from experiences of each CI operators' incident responses, efforts are made to ensure that safety principles are optimized for each CI sector and organization through a process of risk assessment, by identifying issues from operation of measures intended to ensure cybersecurity, internal/external audits, results of studies and analyses of environmental changes concerning IT, exercises, training and CISs incident responses. When verifying the safety principles, the Guidelines for Safety Principles as well as social trend changes and new knowledge released by the Cabinet Secretariat are to be used.

The Cabinet Secretariat carries out surveys on the improvement of the safety principles by the responsible ministries for CI each fiscal year and releases the results thereof. In addition, the Cabinet Secretariat also provides advice where necessary on safety principles that are formulated by responsible

ministries for CIP.

2.3 Promotion of the safety principles

With the aim of understanding in detail the degree to which effective incident response capabilities are being developed at CI operators, the Cabinet Secretariat conducts surveys and analyses on the development status of safety principles at CI operators and activities and measures being implemented to ensure cybersecurity. The results are in principle published annually and utilized in improving the various measures set out in this Cybersecurity Policy.

Given the diversity and complexity of risks in different CI sectors and organizations it is increasingly important to more accurately understand the actual status of countermeasures being taken by individual organizations and the degree of top management involvement. To that end it is necessary to switch to survey methods that can be used to promote voluntary activities at CI operators. The Cabinet Secretariat is collaborating with responsible ministries for CIP on new survey methods, considering the best methods for promoting voluntary activities at CI operators. The aim is to realize the formulation of new methods by the end of FY2023.

In specific terms, rational and effective research methods will be investigated that could be used to make continual improvements that contribute to ensuring cybersecurity, by repeating the following: (i) self-assessments relating to cybersecurity status; (ii) analysis of any discrepancies between the expected situation and requirements and reality at individual organizations; (iii) prioritization of measures that are lacking at individual organizations, based on analysis outcomes; and (iv) implementation of specific measures.

2.4 Clarification of documentation relating to the safety principles

In order to further promote understanding of the Guidelines for Safety Principles and the safety principles, the Cabinet Secretariat compiles a list and also clarifies the relationship between the various documents.

3. Enhancement of Information Sharing System

While the social and technological environments surrounding CI and trends of cybersecurity are changing from moment to moment, individual CI operators' independent activities have limits in maintaining high security levels. Cross-sectoral efforts for information sharing in collaboration between the public and private sectors are indispensable. Broadly sharing information on CISs outages and information on threats and vulnerabilities and developing prompt countermeasures by a larger number of CI operators contribute not only to minimizing damage caused by the threats and vulnerabilities concerned, but also to deterring new cyberattacks and preventing system failures. Given such a backdrop, efforts for smoother information sharing have been made under former Cybersecurity Policies and it is important to deepen understanding of the significance and necessity of such efforts and promote measures for activating information sharing continuously under this Cybersecurity Policy.

To this end, efforts are being made to further enhance public-private and internal-external sectoral information sharing systems to ensure that individual CI operators can respond to cybersecurity trends that change on a daily basis.

Based on the concept that mutual assistance originates from self-help efforts, and that public assistance is designed to promote self-help and mutual (reciprocal) assistance efforts, mutual assistance for information sharing is promoted on the premise of active voluntary efforts by CI operators.

3.1 Information sharing system during the term of this Cybersecurity Policy

The information sharing system built under Cybersecurity Policies to date has become fully rooted among stakeholders and therefore should be further developed and disseminated. To this end the Cabinet Secretariat engages in the operation of the information sharing system and implements revisions as necessary, working to enable CI operators to positively utilize shared information in their risk management and incident responses.

The basis for the information sharing system is that CI operators submit information to the Cabinet Secretariat via responsible ministries for CIP, and the Cabinet Secretariat shares information with CI operators via the responsible ministries for CIP and the CEPTOARs. Given that it was thought that one of the reasons hindering active information sharing from CI operators was the concern that reporting to responsible ministries for CIP about incidents, Signs/*Hiyari-Hatto* events or system failures, for which reporting is not required under relevant laws could lead to the issuance of disciplinary guidance, the information sharing system enables CI operators to not only report directly to responsible ministries for CIP, but also provides the option of reporting via the CEPTOAR secretariat, which enables data anonymization, regarding events for which reporting is not required under relevant laws. This means that CI operators can select the means for reporting on their own, depending on the content, and this is expected to break down psychological barriers and prompt information sharing not legally required. Additionally, information is gathered in each CEPTOAR secretariat and functions of CEPTOARs will be strengthened as each CEPTOAR becomes able to spread gathered information promptly within each

sector as necessary.

Furthermore, the establishment of an emergency hotline between the Cabinet Secretariat and CI operators is expected to achieve speed and efficient information sharing.

In addition, cybersecurity related agencies offer support for the collection and analysis of information on domestic and foreign incidents and incident responses from a neutral standpoint apart from individual companies, and therefore, it is effective and preferable that the Cabinet Secretariat, CI operators and cybersecurity related agencies, which have abundant knowledge on cybersecurity, closely collaborate with each other. Cybersecurity related agencies are expected to play a major role in Japan's information sharing system through anonymizing information based on consent of data sources and sharing such anonymized information positively with stakeholders.

Based on the stipulations of Article 28, Paragraph (3) of the Basic Act on Cybersecurity, mechanisms that enable the chief of the Cybersecurity Strategic Headquarters to make recommendations to the heads of responsible ministries for CIP, based on materials and information relating to cybersecurity at CI operators provided to the Cybersecurity Strategic Headquarters from the heads of responsible ministries for CIP or the heads or representatives of CI operators pursuant to the stipulations of Article 32 (Submission of Materials) and Article 33 (Submission of Materials and Other Cooperation) of the Basic Act, are appropriately operated by the Cabinet Secretariat (NISC).

In addition, in the event of a CISs crisis due to a disaster or terror attack, etc., stakeholders should closely collaborate with each other in accordance with "Regarding the Government Initial Response System for Emergencies" (November 21, 2003, Cabinet resolution), while properly sharing information based on this Cybersecurity Policy.

Based on the above, the information sharing system during the term of this Cybersecurity Policy is represented in "ANNEX 4-1. INFORMATION SHARING SYSTEM (NORMAL CIRCUMSTANCES)" and also by extension “ANNEX 4-2. INFORMATION SHARING SYSTEM (CISs CRISIS),” and the roles of individual stakeholders are in "ANNEX 4-3. RESPONSIBILITIES OF EACH STAKEHOLDER". Examples of critical information systems and CISs outages are indicated in "ANNEX 1. SCOPE OF CI OPERATORS AND CRITICAL INFORMATION SYSTEM EXAMPLES" and "ANNEX 2. EXPLANATION OF CI SERVICES AND SERVICE MAINTENANCE LEVELS."

The abovementioned measures are steadily promoted and the construction of a system to share information with stakeholders will be developed while CISs outages and threat and vulnerability information is aggregated in the Cabinet Secretariat in a cross-sectoral manner and analyzed using the information sharing system mentioned above, in order to make it possible to promptly and properly respond to any cybersecurity threat or vulnerability covering multiple sectors.

3.2 Further promotion of information sharing

Information to be shared is defined, as in Cybersecurity Policies to date, to be "information concerning system failures, including CISs outages, Signs/*Hiyari-Hatto* events (hereinafter, referred to as "information on system failures")" based on the idea indicated in "ATTACHMENT: INFORMATION SHARING TO NISC AND INFORMATION SHARING FROM NISC" and "ANNEX 3. CATEGORIES OF EVENTS AND CAUSES FOR INFORMATION SHARING TO NISC". Cyberattacks have also been confirmed as targeting control systems, which among information systems used to be considered safe by virtue of having air gaps and not possessing any external connections. The Cybersecurity Policy identifies the scope of information to be shared also with regard to such threats and vulnerabilities, including IoT, the dissemination of which continues to advance.

During the term of this Cybersecurity Policy, stakeholders are requested to conduct information sharing to and from NISC and thus promote information sharing in line with the ATTACHMENT. When any change occurs in the environment, the system is to be reviewed as needed.

Maintaining consistency with considerations on the enhancing of the framework for National CERTs/CSIRTs[3] and as a part of its development, the Cabinet Secretariat will further promote cooperation with the Cybersecurity Council and other bodies.

3.3 Promotion of CI operators' activities

Enrichment of information sharing within and between CEPTOARs is expected for further invigorating activities of CI operators, in addition to individual efforts by CI operators themselves.

In particular, CI operators are expected to proactively work towards their own information sharing activities, and under top management leadership construct and enhance CISs outage response structures, such as CSIRT, including for operators involved in supply chains, etc. Given that through the implementation of their own efforts to collect information CI operators are expected to enhance their understanding of the information and become more adept at using it effectively, it is anticipated that this will activate information collection by CI operators. In addition, CEPTOARs are also expected to continue sharing information provided by the Cabinet Secretariat as during the term of Cybersecurity Policies to date, while applying rules decided upon by constituent members regarding agreements on the handling of such provided information, maintenance of confidentiality and provision of information to parties outside the constituent members, under a situation where a PoC[4] is established to allow contact between constituent members and with non-members in case of emergency.

It is also expected that efforts for further activating sharing activities are made such as through appointing coordinators who will carry out information collection and decision making within

[3] Overall coordination functions whereby the government promotes a series of activities in an integrated manner in response to serious cyberattacks, from information collection and analysis to investigation and assessment, implementation of alerts and countermeasures, and subsequent policy planning and measures to prevent recurrence of such cyberattacks.

[4] PoC: Point of Contact.

CEPTOARs, sharing predictive information and CISs outage examples during ordinary situations, and enhancing functions required for information sharing between CEPTOARs and with the CEPTOAR council. In addition, ISACs have already been organized in some sectors, and sharing, examination and analysis of information within respective ISACs and information sharing with foreign ISACs are now being promoted. Promoting participation in ISACs and information sharing among different ISACs, including consideration of the development of an intersectoral and public-private cooperation framework that includes automation through ISAC cooperation, etc., is expected to contribute to further activating information sharing among CI operators and their further positive activities for cybersecurity measures.

The CEPTOAR council is an independent body, not positioned below other agencies, including government organizations, so information is to be mutually shared based on independent determinations by each CEPTOAR.[5]

In this sense, it is expected that CI operators' activities, such as further enhancement of information sharing between CEPTOARs, are further vitalized through autonomous and wide ranging activities which contribute to the enhancement of service maintenance and recovery capacity at CI operators through the proactive involvement of each CEPTOAR.

3.4 CEPTOAR communication training

The Cabinet Secretariat continues CEPTOAR training based on the procedures for information sharing to and from NISC for the purpose of maintenance and improvement of protective capability of the "vertical-directional information sharing" systems in each sector between CEPTOAR and responsible ministries for CI.

Considering that many CI operators have already participated in CEPTOAR training, and from the perspective of effectively utilizing these training opportunities, the Cabinet Secretariat further enhances the content of the training, while responding to requests from CEPTOARs and responsible ministries for CI. Concrete means include consideration of cross-sectoral exercises as necessary, and verification of emergency systems and means for communication. In this manner, CEPTOAR communication training better fitting the actual state is to be sought.

[5] According to CEPTOAR council charter (CEPTOAR council foundation preparatory committee and NISC).

4. Utilization of Risk Management

Risk management activities are necessary in order to make a systematic response to risks that disrupt the continual provision of CISs, which is the purpose of CIP.

During the term of this Cybersecurity Policy, in order to realize "IV. 1.2 Activities to enhance incident response capability," stakeholders shall utilize risk management appropriately. In addition, the Cabinet Secretariat shall compile guidance in order to continually improve optimal CIP measures at CI operators, and provide assistance relating to such guidance.

In a situation in which risks relating to CISs are changing dynamically, including recent environmental changes and technological innovations, etc., in order to deal accurately with risks and bring them within acceptable limits, the involvement of top management is critically important. To this end it is important for organizations to properly recognize the impact that any suspension of the continual provision of CISs would have on management of their operations, and foster awareness of the need to make organization-wide efforts, visualizing this awareness through the promotion, monitoring and measurement of continual activities, and making improvements accordingly.

4.1 Promotion of risk management

In order to accurately tackle risk management initiatives CI operators must understand the characteristics (profile) of their own organization, and also engage in repeated PDCA cycles and promote continual activities (processes) to ensure CIP policies optimized to individual organizations.

In particular, it is clear that advances in DX will significantly change the environment surrounding CI and associated risks in the future, and therefore in order to effectively implement continual improvements while ensuring continual provision of CISs, it is necessary for CI operators to understand the risks their organizations are facing and their degree of severity, and initiate new improvements by starting to clarify the characteristics (profile) of their organization's CISs.

(1) Direction for realization of CIP policies optimized to individual organizations

① Clarification of organizational profiles

A profile refers to the organizational characteristics of a CI operator, including business policies, strategies, and information assets, etc. related to the continual provision of CISs.

Combining an organization's profile with risk management activities to date makes it easier to clarify the risks an organization faces, and provides basic data in order to determine the scope and extent of improvement plans.

In normal circumstances a profile clarifies the actual situation and the envisaged future of an organization.

- Actual situation including current status of CIP policies implementation (As Is)
- Targeted envisaged future (To Be)

② Identifying items for improvement and determining the extent of application

It is necessary to identify items for improvement in order to reconcile any discrepancies between targets and actual situation. It is necessary for CI operators to consider the CIP policies that need to be implemented by adopting an approach based on the perspectives described below, and prioritize the extent of their application, based on assessment standards within the organization.

i. Improvements relating to information asset risks
ii. Improvements relating to reliable service provision
iii. Improvements relating to detection of outages when they occur
iv. Improvements relating to responses to outages
v. Improvements relating to restoration of functions disrupted due to outages

At such times it is necessary not to develop plans and other measures with the goal of implementing many CIP policies or raising the priority of risk response to a high level, but rather the ultimate goal should be to focus on reducing the risks particular to the individual organization, and realizing appropriate CIP policies.

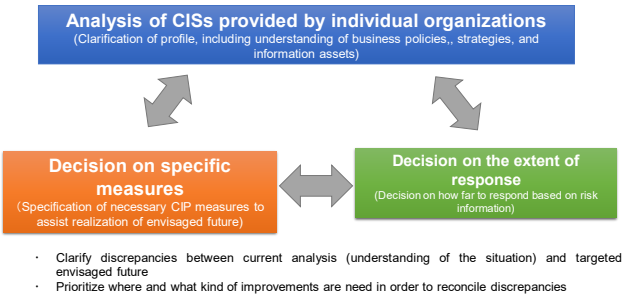


Fig. 3 Realization of CIP policies optimized for individual organizations (conceptual diagram)

As shown in Figure 3, by analyzing the current status of their own organizations, CI operators can clarify the risks that need to be addressed in the continual provision of CISs, clearly delineate the extent to which they need to respond, and decide on the specific countermeasures optimized for their organizations. Such a concept is flexible and reproducible, and is intended to contribute to further enhancing the identification, assessment, and management of risk in individual organizations, and to build on risk management activities implemented to date.

(2) Actualization of CIP policies optimized to individual organizations

In order to assist CI operators in efforts to realize CIP policies as detailed in the previous paragraph, the Cabinet Secretariat revises manuals, in addition to developing new guidance, including on how existing principles and standards, etc., can be utilized at individual organizations. Such guidance, etc. is formulated to be performance-based so that stakeholders can quickly and accurately implement improvements toward the realization of CIP policies optimized to individual organizations, and the status of achievement of these policies needs to be able to be monitored and be quantifiable. In addition to ensuring that guidance, etc. is utilized at individual organizations, consideration also needs to be given

to engaging in improvements as necessary with the related industries and responsible ministries for CIP, etc.

(3) Continuation of existing risk management-related activities

It is necessary for CI operators to continue to engage in efforts to confirm whether various risk management-related activities at individual organizations are effectively and efficiently functioning to realize CIP policies optimized to each individual organization. This should be confirmed through audits and other activities conducted by each organization on its own initiative.

The Cabinet Secretariat encourages CI operators to participate in the CEPTOAR council and utilize cross-sectoral exercises, etc., and continue to enhance opportunities to disclose risk-related information and engage in joint considerations with stakeholders. Furthermore, by advancing public-private risk management-related activities in the run-up to the Tokyo Games, the Cabinet Secretariat contributed to facilitating their smooth operation. Consideration will be given to how CI operators can actively utilize the experience and know-how gained from the Tokyo Games and consider specific methods and means to such ends.

4.2 Understanding risks arising from environmental change

With the increasing complexity of supply chains, it is anticipated that the diverse services that are provided in cyberspace will become even more deeply mutually interrelated and interconnected among stakeholders. Moreover, changes that are occurring in a discontinuous manner due to the COVID-19 pandemic and other factors may generate concerns about such risks emerging in unexpected ways and it is therefore necessary to be aware of the constant changes in the social environment. To this end it is necessary to understand risks associated with environmental change in order to aim to optimize responses across society as a whole.

As detailed below, the Cabinet Secretariat implements studies to understand risks associated with environmental change and studies to ascertain the information about interconnectivity and interrelatedness, and provide the results of such studies to CI operators. The results are also utilized to improve the measures in this Cybersecurity Policy.

(1) Environmental change studies

The changes being brought about in cyberspace by the progress of DX based on digital innovation also have the potential to magnify risks in a way not previously anticipated. The Cabinet Secretariat carries out current status studies on environmental changes as well as analyses of new risk sources and risks arising from environmental change, focusing on new technologies and systems that are expected to penetrate CI sectors in the medium- to long-term, as well as rules related thereto. As these studies and analyses produce better results when conducted over time in accordance with environmental changes, the Cabinet Secretariat conducts them continuously by flexibly changing the targets and scopes.

(2) Interdependency studies

The Cabinet Secretariat carries out studies relating to interdependency, investigating which other CI sectors would be impacted in the event of a CISs outage, with a view to eliminating the challenges faced by CI operators, such as understanding cross-sectoral risks. When implementing such interdependency studies it is necessary for the Cabinet Secretariat, responsible ministries for CIP, and CI operators to work together on collating the necessary information, and cooperate in the advancement of activities, and the Cabinet Secretariat works to organize more effective methods and procedures for analyzing interdependency.

5. Enhancement of the Basis for CIP

As the social and technological environment and cybersecurity trends surrounding CI continue to constantly change, in order to improve cybersecurity standards across the nation it is important to raise public awareness about cybersecurity at an individual level and enhance the level of national cybersecurity overall, by enhancing incident response capabilities at CI operators and engaging in human resources development targeting a broad range of people.

As shown in Figure 1 "Critical Infrastructure Operator Measure Examples" and "Government Activities" it is indispensable to enhance common foundation activities which support the entirety of this Cybersecurity Policy, for maintaining the effectiveness of cybersecurity measures. The activities include establishment of basic plans, development of human resources and career paths/proper personnel allocation, external explanations of activities aimed at ensuring cybersecurity, and identification of issues for new risks and risk sources resulting from environmental changes.

Therefore, during the term of this Cybersecurity Policy, the Cabinet Secretariat is working to promote human resources development that will contribute to the verification of the effectiveness of incident response capabilities across the CI sector as a whole, and the maintenance and improvement of the CIP capabilities. In addition, following on from the Fourth Policy, the Cabinet Secretariat continues to conduct public relations activities, while also promoting security by design, engaging in international collaboration, and cooperating with other stakeholders.

Particularly in terms of verifying the effectiveness of incident response capabilities, by implementing cross-sectoral exercises the Cabinet Secretariat confirms whether the incident response capabilities of stakeholder organizations are functioning effectively as a whole, with the aim of implementing improvements.

The Cabinet Secretariat also provides the knowledge obtained through the implementation of this policy for application in other policies in this Cybersecurity Policy.

5.1 Verification of the effectiveness of incident response capability

Aiming to ensure resilience in the continual provision of CISs, it is necessary to conduct verification of incident response capability and its effectiveness. Depending on the purpose of verification CI operators are required to identify challenges and engage in improvement activities through a variety of measures including daily operations, outage response, diagnostics, testing, internal and external audits, exercises and training, etc.

The Cabinet Secretariat continues to implement cross-sectoral exercises, with a view to ensuring the resilience of the continual provision of CISs. Cross-sectoral exercises are implemented in cooperation between the Cabinet Secretariat and responsible ministries for CIP, and opportunities are provided to CI operators to continually verify and improve incident response capabilities across entire organizations.

(1) Improving incident response capability through cross-sectoral exercises

By preparing exercises that take into account incident response capabilities that CI operators work to enhance on an ongoing daily basis the Cabinet Secretariat conducts verification of the effectiveness of CI operators' incident response capabilities. In the process of preparations the Cabinet Secretariat plans exercise scenarios that CI operators implement cross-organizationally, with the involvements of employees and top management, based on knowledge and challenges identified from the implementation of exercises to date, other measures, and the latest trends relating to risk sources that are the cause of CISs outages.

Aiming to promote voluntary activities by CI operators, the Cabinet Secretariat provides exercise programs that enable participants to experience simulations of some cross-sectoral exercises.

In addition, aiming to contribute to the enhancement of incident response capability, the Cabinet Secretariat provides the knowledge and challenges identified through exercises as a source of reference for other policies in this Cybersecurity Policy.

In preparation for cross-sectoral exercises, CI operators should implement knowledge gathering about risks at each individual organization and participate in exercises. After participation in cross-sectoral exercises, it is then necessary through analysis and verification of the identified issues for CI operators to review whether the organization's capabilities, internal rules and regulations, and risk management are functioning effectively, and implement improvements accordingly. For this reason CI operators are expected to utilize cross-sectoral exercises to continually verify the effectiveness of daily activities to enhance incident response capabilities and implement improvements accordingly. Moreover, with the aim of facilitating activities to verify effectiveness CI operators are expected to cooperate with planning of cross-sectoral exercise scenarios, implementation methods and verification issues, etc. and implementation of cross-sectoral exercises.

(2) Promotion of the lessons learned from cross-sectoral exercises

The Cabinet Secretariat works to share good practices by participants in the exercises that have been accumulated to date, and also share issues that require attention that have emerged during the exercises, as well as further disseminating and promoting the outcomes of exercises with the CI sector as a whole.

In addition, with the aim of promoting the participation in exercises of CI operators from each CI sector, materials are prepared and published that explain the benefits of experiencing various roles during the exercises, and the benefits of being able to effectively utilize the exercises as an opportunity for dialogue with top management through advance preparations for the exercises and also in post-exercise improvements.

(3) Cooperation with responsible ministries for CIP

Although the effect of CIP exercises and training conducted by responsible ministries for CIP and private organizations such as ISACs may differ from the cross-sectoral exercises conducted by the

Cabinet Secretariat, taking into account the main targets, clarification of verification purposes and the ideal form of mutual cooperation for the various exercises being implemented, where necessary by implementing such exercises in a manner that is mutually cooperative and complementary with cross-sectoral exercises, it is expected that efficient and effective CIP capabilities will be maintained and improved.

In responding to CISs outages there is a possibility that information may need to be shared not only among responsible ministries for CIP and CI operators' cybersecurity departments, but also with disaster prevention and risk management departments. Therefore the Cabinet Secretariat and responsible ministries for CIP engage in collaboration with such other departments concerned as necessary, based on stakeholders' needs.

In addition, the Cabinet Secretariat plans and organizes exercises, considering the participation of not only CI operators but also other stakeholders closely relating to the maintenance of CI operators' information systems and businesses outside CI sectors that support the provision of CI services.

5.2 Promotion of the development of human resources

Stakeholders should promote efforts based on the Cybersecurity Strategy (approved by the Cabinet September 28, 2021). Concrete measures for human resources development are as follows.

(1) Development of strategic management

Against a backdrop of increasingly complex and sophisticated cyberattacks, in order for CI operators to realize mission assurance it is important to engage in efforts across entire organizations to boost awareness of cybersecurity and implement appropriate intra-organizational cooperation.

In addition to raising awareness of the necessity of organizational governance in implementing security control measures appropriate to the organization and enhancing incident response capability, through incident response capability improvement processes, etc. the Cabinet Secretariat promotes the development of strategic management personnel capable of dealing with management and business threats arising from cybersecurity-related risks, and also working closely with top management, etc.

(2) Promotion of inter-departmental cooperation

In light of recent threats, such as attacks targeting control systems, etc., it is important that not only IT management departments but also OT management departments, legal affairs departments, and public relations departments, etc., be duly aware of the necessity of ensuring cybersecurity.

The Cabinet Secretariat promotes the construction of an organizational structure that enables cross-sectoral collaboration of personnel with diverse roles and abilities in carrying out measures and ensuring cybersecurity.

When building such structures at CI operators, it is expected that based on the situation of personnel transfers and staffing allocations within an organization, efforts will be made through the entire

organization to promote and raise awareness about cybersecurity.

(3) Promotion of industry-academia-government collaboration

In industry-academia-government collaboration, the Cabinet Secretariat promotes specific human resource development measures, including defining requirements for security experts, nurturing working level and technical personnel with the requisite practical response capabilities, providing exercises and training relating to cybersecurity, and promoting qualification acquisition. At CI operators it is expected that even in activities outside of the organization concerned, opportunities for engaging in various exercises and training and sharing information will be actively utilized, so that security personnel within the organization can acquire a broad range of knowledge.

5.3 Promotion of security by design

In order to realize a safe and secure IoT environment, from the planning stages it is necessary to incorporate a cybersecurity perspective in system lifecycles (planning, design, development, operation, disposal) and appropriately incorporate security requirements in system specifications. In light of serious security incidents that have been repeatedly occurring in the development of new IT businesses recently, it is critically important to implement security by design, which ensures cybersecurity for systems relating to operations, products and services from the planning and design stages.

The Cabinet Secretariat works to disseminate ideas to enable CI operators to implement security by design when developing new businesses, and in addition to promoting the development of organizational structures that enable CI operators to accurately collect information and utilize knowledge, promotes sharing of examples of good practices for security by design.

In addition, it is expected that CI operators will duly bear in mind the implementation of security by design as they engage in activities that aim to ensure cybersecurity across a system's entire lifecycle.

5.4 Promotion of international cooperation

With both the pace and complexity of changes in the international community increasing, threats in cyberspace are also increasing from an international perspective, such cases being observed where organizations with advanced cyber capabilities are alleged to have conducted cyberattacks on CI in other countries. Under these circumstances, countries recognize the importance of strengthening cooperation and collaboration with their allies and like-minded countries.

Therefore, the Cabinet Secretariat cooperates with responsible ministries for CI and the cybersecurity related agencies to enhance cooperation and partnership with the governments of other countries, and promote the sharing of knowledge and capacity building assistance, etc. Specifically, the Cabinet Secretariat actively introduces cross-sectoral exercises and other examples of Japan's unique initiatives through multilateral frameworks such as those with U.S.-Australia-India and ASEAN, as well as bilateral consultations with the United States and other like-minded countries, inter-CSIRT cooperation,

and speeches to overseas cybersecurity policymakers. Such cooperative relationships serve as the basis for information sharing concerning cyberattacks, foreign threats, incident responses, and best practices, and also contribute to enhancing international CIP capability. The information thus obtained from foreign countries that will contribute to enhancing Japan's CIP capability is to be positively provided to domestic stakeholders.

CI operators are also expected to make efforts to secure human resources capable of promoting international cooperation, and engage in diversified and multilateral international cooperation by ascertaining overseas trends through participation in international conferences and expansion of their initiatives related to cybersecurity measures to foreign companies in the same industry, and sharing information with foreign ISACs, etc.

5.5 Strengthening cybercrime countermeasures

Given the increasingly public nature of cyberspace, the Cybersecurity Strategy (approved by the Cabinet September 28, 2021) states that by encouraging victims of cybercrimes to report to the police and notify public agencies, the national government will eliminate factors and environments that tolerate cybercrimes. A Cyber Affairs Bureau, which will be responsible for a unified policy on matters relating to cyber incidents and a National Cyber Unit, which will be a national investigation unit, will be established at the National Police Agency, and working in cooperation with prefectural police departments that are engaged in community-based activities, these organizations will promote activities to ensure security across police departments nationwide.

The Cabinet Secretariat will cooperate with the National Policy Agency to support the necessary cooperation activities between the police and CI operators, and will ensure the safety and reliability of cyberspace surrounding CI operators.

5.6 Ensuring security in cooperation with the Digital Agency

While the establishment of the Digital Agency has helped to advance the formation of a digital society, it is important to improve awareness about cybersecurity in response to cloud technologies and zero trust architecture, and also foster trust in the technological infrastructure and data that together comprise cyberspace.

The Cabinet Secretariat will work together with the Digital Agency on the necessary activities to realize the provision of advanced and appropriately secured CISs, and to provide support for ensuring cybersecurity in local governments and the semi-public sector related to CI.

5.7 Promotion of public relations activities

(1) Making information accessible and easy to understand for the public

In order to minimize the impact of CISs outages to the smallest degree possible, it is important to not only raise the standard of cybersecurity measures implemented by CI operators, but also to ensure a

calm response of the society as a whole, including other companies involved in the supply chain, and the general public, in accordance with the situation of outages. Therefore, stakeholders should actively inform the general public of the framework of the Cybersecurity Policy and their activities in order to contribute to a calm response from the general public.

The Cabinet Secretariat continues efforts to broadly publicize activities under this Cybersecurity Policy to deepen understanding of the general public through providing information on its website, and via social media, newsletters and lectures, and will also study more effective PR channels and how to make information more accessible and easy to understand for the public.

(2) Development of related documents and regulations

To maintain the effectiveness of cybersecurity measures, it is important to ensure that stakeholders are able to reference relevant documents and regulations where necessary when examining means therefor.

The Cabinet Secretariat therefore publishes a collection of the rules and regulations relating to CIP for the purpose of equalizing the knowledge base of stakeholders involved in CIP, and with the cooperation of other stakeholders organizes and discloses relevant domestic and overseas regulations.

(3) Promotion of public hearing activities

While on the one hand the continuing penetration of the digital economy and the promotion of digital reforms are giving rise to a constant stream of new technologies and new digital services that are permeating society, so too is it anticipated that cyberattacks will become more organized and sophisticated, and the methods used in such attacks will become more diverse and advanced.

In order to promote appropriate responses to these increasingly complex and sophisticated cyberattacks, through various studies and seminars, etc., the Cabinet Secretariat ascertains the status of each sector and collects information on technology trends and reflects such information in policies as required.

V. Activities Taken by Stakeholders

1. Cabinet Secretariat

(1) Items relating to enhancement of incident response capability

(i) Create rules relating to organizational governance.

(ii) Support for activities at CI operators to develop BCP/IT-BCP, CSIRT and auditing structures.

(iii) Promote the utilization of agencies, etc., that have ISAC, etc., incident information sharing and analysis functions at CI operators.

(iv) Improve capabilities relating to threat detection, investigation, and analysis.

(v) Improve defense capabilities, deterrence capabilities and situational awareness.

(vi) Continue efforts for reviewing the scope of protection including supply chains and continuously offer cooperation and proposals for initiatives by relevant ministries (not limited to responsible ministries for CIP), in light of the necessity of "protection as plane" for mission assurance.

(2) Items relating to maintenance and promotion of the safety principles

(i) Revise the Guidelines for Safety Principles and officially release the results with the aim of promoting measures cited in this Cybersecurity Policy

(ii) Revise documents relating to guidance, etc., as necessary in a timely manner, based on changes in social trends and newly obtained knowledge, and officially release the results

(iii) Support continued improvements of the CI sector safety principles through (i) and (ii) above

(iv) Obtain cooperation of responsible ministries for CIP to implement studies every year to ascertain the conditions of continued improvements of the safety principles in each CI sector, and officially release the results

(v) Obtain cooperation of responsible ministries for CIP and CI operators to implement studies every year on the status of maintenance of the safety principles at CI operators and activities and methods towards ensuring cybersecurity, and officially release the results. Consult with responsible ministries for CIP and promptly consider and materialize optimal methods that will encourage voluntary activities by CI operators

(vi) Utilize the results of the studies in (v) above in improving activities under this Cybersecurity Policy

(vii) Organize a list of documents related to the maintenance of safety principles and clarify the relationship between these documents

(3) Items relating to enhancement of information sharing system

(i) Operate the information sharing system during normal circumstances and upon a CISs crisis and review the system as necessary

(ii) Collect information to be provided to CI operators and share information from NISC in an appropriate and timely manner

(iii) Collect and analyze information on domestic and overseas incidents and cooperate with cybersecurity related agencies that are offering support

(iv) Appropriately operate the mechanisms of recommendations, etc. prescribed in the Basic Act on Cybersecurity

(v) Promote the establishment of a mechanism to collect information on CISs outages, risks and vulnerabilities in a cross-sectoral manner and secure resources necessary for the operation of the mechanism

(vi) Maintain consistency with considerations on enhancing of the frameworks for National CERTs/CSIRTs

(vii) Obtain cooperation of responsible ministries for CIP to periodically implement studies, hearings, etc. for ascertaining conditions of each CEPTOAR's functions and activities; Introduce leading CEPTOAR activities

(viii) Offer support to the CEPTOAR secretariat and CI operators through the provision of the environment necessary for information sharing

(ix) Continue cooperating with CEPTOAR participating in the CEPTOAR council and implement support for management and activities of the council

(x) Prepare environments required for enhancement of activities of the CEPTOAR council and for accumulation and sharing of know-how

(xi) Individually make collaboration with cyberspace-related operators as necessary to provide appropriate information on a timely basis in the event of CISs outages

(xii) Provide appropriate information on a timely basis to businesses in and outside CI sectors that are newly incorporated in the scope of information sharing

(xiii) Obtain cooperation of responsible ministries for CIP to provide opportunities for verification of CEPTOAR information communication functions (CEPTOAR training), periodically or upon requests from CEPTOARs

(4) Items relating to utilization of risk management

(i) Review existing manuals so that they can be utilized by CI operators in their risk assessment and formulate new guidance.

(ii) Promote participation in the CEPTOAR council and utilization of cross-sectoral exercises among CI operators, and provide opportunities to disclose risk-related information and engage in joint considerations with stakeholders.

(iii) Consider how CI operators can actively utilize the experience and know-how gained from the Tokyo Games and consider specific methods and means to such ends

(iv) Provide the results of the studies. in this policy as data to be reflected in CI operators' risk management implementation and maintenance of the safety principles

(v) Utilize the results of the studies, etc. in this policy as data to be reflected in other activities under this Cybersecurity Policy

(5) Items relating to enhancement of the basis for CIP

(i) Plan cross-sectoral exercise scenarios, implementation methods and verification issues, etc. capable of verifying the effectiveness of incident response capability, and implement cross-sectoral exercises

(ii) Plan company-wide implementation of exercise scenarios that go beyond duties and positions

(iii) Study measures for improving cross-sectoral exercises

(iv) In order to promote voluntary activities by CI operators, provide exercise programs that enable participants to experience simulations of some cross-sectoral exercises

(v) Utilize the opportunities provided by cross-sectoral exercises to implement verification of the effectiveness of incident response capability, etc.

(vi) Diffuse and promote knowledge related to CIP gained from cross-sectoral exercises

(vii) Obtain information on other ministries and private-sector organizations' exercises and training for CISs outage responses and consider means for collaboration with other ministries

(viii) Promote human resources development through cultivation of strategic management personnel, interdepartmental cooperation and industry-academia-government collaborations

(ix) Promote the implementation of security by design among CI operators

(x) Enhance cooperation and collaboration with governments of all countries, etc. and promote knowledge sharing and capacity building assistance, etc.

(xi) Work with the National Police Agency and support the necessary activities for cooperation between the police and CI operators

(xii) Work with the Digital Agency to realize the provision of advanced and appropriately secured CISs, and implement the necessary activities for assistance towards ensuring cybersecurity at local governments and quasi-public sector organizations related to CI.

(xiii) Carry out PR activities by providing information via the website, social media, issuing newsletters and holding lectures

(xiv) Publish collections of regulations relating to CIP, organize the related regulations and make them visible

(xv) Listen to public opinions through various surveys and seminars, etc.

2. Responsible Ministries for CIP

(1) Items relating to enhancement of incident response capability

(i) Support for activities at CI operators to develop BCP/IT-BCP, CSIRT and auditing structures.

(ii) Improve capabilities relating to threat detection, investigation, and analysis.

(iii) Improve defense capabilities, deterrence capabilities and situational awareness.

(iv) Continue efforts for achieving "protection as plane" for mission assurance

(v) Continually review the scope of CI operators that are the actual implementers of activities in the CI sector

(2) Items relating to maintenance and promotion of the safety principles

(i) Provide information, etc. related to the safety principles that can be newly positioned as the Guidelines for Safety Principles to the Cabinet Secretariat

(ii) When the relevant ministry has established the safety principles, it should revise them as necessary, in addition to implementing periodic analysis and verification thereof

(iii) Support the analysis and verification of the safety principles for each CI sector

(iv) Promote dissemination of the safety principles among CI operators including environmental arrangement for packaging measures

(v) Cooperate with the Cabinet Secretariat every year with its efforts to ascertain the conditions of continued improvements of the safety principles, etc.

(vi) Cooperate with the Cabinet Secretariat every year in considering and implementing the survey methods on the status of maintenance of the safety principles at CI operators and activities and methods towards ensuring cybersecurity.

(3) Items relating to enhancement of information sharing system

(i) Cooperate with the Cabinet Secretariat and operate the information sharing system during normal circumstances and upon a CISs crisis

(ii) Maintain a system of close information sharing with CI operators and review it as necessary

(iii) Carry out information sharing to the Cabinet Secretariat regarding reports related to system failures received from CI operators

(iv) Cooperate with the Cabinet Secretariat with surveys and hearings for ascertaining the conditions of activities and functions of each CEPTOAR

(v) Support the development of CEPTOAR functions

(vi) Support the CEPTOAR council

(vii) Implement opinion exchanges, etc. when requested by the CEPTOAR council, etc.

(viii) Cooperate with the CEPTOAR council and CI operators with their information sharing activities

(ix) Cooperate when the Cabinet Secretariat provides opportunities for verification of information communications functions (CEPTOAR training)

(4) Items relating to utilization of risk management

(i) Cooperate with the Cabinet Secretariat, CI operators and other stakeholders in the implementation of their risk assessments

(ii) Provide the necessary cooperation to the Cabinet Secretariat in disseminating the guidance from the Cabinet Secretariat to CI operators and in otherwise promoting the dissemination of risk assessment

(iii) Support risk communication of CI operators

(iv) Offer support to CI operators as necessary for their efforts in implementing monitoring and review

(v) Provide the Cabinet Secretariat with information related to targets of studies, etc. in this policy and information needed for the relevant studies, etc.; If studies conducted by responsible ministries for CIP relate to studies in this policy, make collaboration with the Cabinet Secretariat as necessary

(vi) Utilize the results of the studies in concrete measures

(5) Items relating to enhancement of the basis for CIP

(i) Cooperate with planning of cross-sectoral exercise scenarios, implementation methods and verification issues, etc. and implementation of cross-sectoral exercises

(ii) Support CEPTOARs and CI operators in their participation in cross-sectoral exercises

(iii) Participate in cross-sectoral exercises

(iv) Utilize results of cross-sectoral exercises in policies as necessary

(v) Cooperate with study of measures for improving cross-sectoral exercises

(vi) Cooperate with mutual collaboration between exercises and training which contribute to CIP implemented by responsible ministries for CIP and cross-sectoral exercises

(vii) Support development of cybersecurity experts through related exercises and education

(viii) Promote the implementation of security by design among CI operators

(ix) Work with the Cabinet Secretariat to enhance cooperation and collaboration with governments of all countries, etc. and promote knowledge sharing and capacity building assistance, etc.

(x) Cooperate with the Cabinet Secretariat and compile relevant regulations and make them visible

3. Cybersecurity Related Ministries

(1) Items relating to enhancement of incident response capability

(i) Improve capabilities relating to threat detection, investigation, and analysis.

(ii) Improve defense capabilities, deterrence capabilities and situational awareness.

(2) Items relating to enhancement of information sharing system

(i) Cooperate with the Cabinet Secretariat and operate the information sharing system during normal circumstances and upon a CISs crisis

(ii) Collect information, etc. related to attack methods and recovery methods and carry out information sharing to the Cabinet Secretariat

(iii) Implement opinion exchanges, etc. when requested by the CEPTOAR council, etc.

4. Crisis Management Ministries and Disaster Prevention Related Ministries

(1) Items relating to enhancement of incident response capability

(i) Improve capabilities relating to threat detection, investigation, and analysis.

(ii) Improve defense capabilities, deterrence capabilities and situational awareness.

(2) Items relating to enhancement of information sharing system

(i) Cooperate with the Cabinet Secretariat and operate the information sharing system during normal circumstances and upon a CISs crisis

(ii) Collect disaster information, terrorism related information, etc.

(iii) Carry out information sharing to the Cabinet Secretariat as necessary

(iv) Implement opinion exchanges, etc. when requested by the CEPTOAR council, etc.

(3) Items relating to enhancement of the basis for CIP

(i) Cooperate with planning of cross-sectoral exercise scenarios, implementation methods and verification issues, etc. and implementation of cross-sectoral exercises

(ii) Implement support measures for improving CISs outage response capability when requested by CI operators

(iii) Cooperate with study of measures for improving cross-sectoral exercises

(iv) Cooperate as necessary with mutual collaboration between exercises and training which contribute to CIP implemented by responsible ministries for CIP and cross-sectoral exercises

5. CI Operators

(1) Items relating to enhancement of incident response capability

(i) Make a unified organizational response, based on the roles and responsibilities of top management, CISOs, strategic management, and system personnel

(ii) Make an integrated response to risk management and crisis management

(iii) Develop systems such as BCP, IT-BCP and CSIRT, capable of responding to incidents when

they occur

(iv) Implement management policies in day-to-day operations that are capable of dealing with any threats and vulnerabilities that are discovered

(v) Implement audits that are considered to be effective for the specific organization and utilize the results of such audits

(2) Items relating to maintenance and promotion of the safety principles

(i) When the relevant operator has established the safety principles, it should revise them as necessary, in addition to implementing periodic analysis and verification thereof

(ii) When the relevant operator has established the safety principles, it should cooperate with the Cabinet Secretariat every year with its efforts to ascertain the conditions of continued improvements of the safety principles, etc.

(iii) Consider activities for ensuring cybersecurity and the development of an environment to facilitate such activities, based on the safety principles

(iv) Conduct a self-assessment of the current status of cybersecurity and analyze any disparities between anticipated status and conditions at the organization concerned; Use the analysis results to continually improve safety principles by prioritizing and repeatedly implementing measures to overcome aspects found to be insufficient in the organization

(v) Cooperate each year with a survey implemented by the Cabinet Secretariat

(3) Items relating to enhancement of information sharing system

(i) Cooperate with the CEPTOAR council, CEPTOARs, responsible ministries for CIP, and the Cabinet Secretariat and operate the information sharing system during normal circumstances and upon a CISs crisis

(ii) Carry out information sharing to NISC regarding system failures

(iii) Collect information, etc. related to attack methods and recovery methods

(iv) Carry out supplemental information sharing based on consensus with the cybersecurity related agencies

(v) Carry out activities at the CEPTOAR council

(vi) Utilize verification of information communication functions (CEPTOAR training) provided by the Cabinet Secretariat and enhance own information sharing systems

(4) Items relating to utilization of risk management

(i) For CIP policies optimized to individual organizations, repeat Plan, Do, Check, Act (PDCA) cycles and implement continual improvements

(ii) Initiate measures to understand the risks faced by individual organization and their extent, and clarify the characteristics (profile) of each organization's provision of CISs

(iii) Implement ongoing verification through audits and other measures implemented on the initiative of each individual organization to ascertain whether risk management initiatives in the organization are functioning effectively and efficiently to realize CIP policies optimized to the organization

(iv) Utilizing participation in the CEPTOAR council and cross-sectoral exercises among CI operators, disclose risk-related information and engage in joint considerations with stakeholders

(v) Provide the Cabinet Secretariat with information related to targets of studies in this policy and information needed for the relevant studies.

(vi) Utilize the information provided as the results of the studies, etc. in this policy for the purposes of risk management in each organization

(5) Items relating to enhancement of the basis for CIP

(i) Cooperate with planning of cross-sectoral exercise scenarios, implementation methods and verification issues, etc. and implementation of cross-sectoral exercises

(ii) In preparation for cross-sectoral exercises implement knowledge gathering about risks at each individual organization

(iii) Participate in cross-sectoral exercises

(iv) After participation in cross-sectoral exercises, through analysis and verification of the identified issues review whether the organization’s capabilities, internal rules and regulations, and risk management are functioning effectively, and implement improvements.

(v) Utilize cross-sectoral exercises to continually verify the effectiveness of daily activities to enhance incident response capabilities and implement improvements

(vi) Cooperate with study of measures for improving cross-sectoral exercises

(vii) Based on personnel transfers and staffing allocations within an organization implement human resource development activities that will contribute to promoting and raising awareness about cybersecurity through the entire organization

(viii) Conduct human resource development activities that enable security personnel in the organization to gain a broad range of knowledge

(ix) Ensure cybersecurity across entire system lifecycles, with due consideration given to the implementation of security by design

(x) Secure human resources capable of leading international cooperation, and promote diversified and multilateral international cooperation by ascertaining overseas trends through expansion of domestic CI operators' initiatives related to cybersecurity measures to foreign companies in the same industry

(xi) Cooperate with the Cabinet Secretariat and compile relevant regulations and make them visible

6. CEPTOARs and CEPTOAR Secretariat

(1) Items relating to enhancement of incident response capability

(i) Positively offer cooperation for the review of the CIP scope to include supply chains for achieving "protection as plane" for mission assurance

(2) Items relating to enhancement of information sharing system

(i) Cooperate with the CEPTOAR council, CI operators, responsible ministries for CIP, and the Cabinet Secretariat and operate the information sharing system during normal circumstances and upon a CISs crisis

(ii) Carry out information sharing from the Cabinet Secretariat to CI operators in accordance with the CEPTOAR information handling rules for information provided from the Cabinet Secretariat

(iii) Regarding reports from CI operators, provide them to responsible ministries for CIP via the CEPTOAR secretariat after data anonymization as necessary, and also provide them to constituent members, thereby strengthening respective CEPTOARs' information sharing system

(iv) Carry out supplemental information sharing based on consensus with the cybersecurity related agencies

(v) Enhance and develop CEPTOAR functions

(vi) Cooperate with the Cabinet Secretariat with surveys and hearings for ascertaining the conditions of activities and functions of each CEPTOAR

(vii) Participate in the CEPTOAR Council

(viii) Carry out periodic verification of information communication functions

(3) Items relating to utilization of risk management

(i) Support proactive efforts among CI operators that comprise the CEPTOAR concerned. Also, cooperate with the Cabinet Secretariat, responsible ministries for CIP, other CEPTOARs and other stakeholders as necessary.

(4) Items relating to enhancement of the basis for CIP

(i) Support CI operators' participation in cross-sectoral exercises

(ii) Participate in cross-sectoral exercises as necessary

(iii) Support efforts to diffuse and spread knowledge related to CIP gained from cross-sectoral exercises

7. CEPTOAR Council

(1) Items relating to enhancement of information sharing system

(i) Cooperate with respective CEPTOARs and operate the information sharing system during normal circumstances and upon a CISs crisis

(ii) Carry out arrangement of information to be shared and sharing methods

(iii) Promote cross-sectoral information sharing through sharing of specific examples of mutual understanding and best practices

(iv) In order to strengthen cooperative relationships with stakeholders, hold opinion exchanges to promote sharing of the situational awareness of both parties based on requests from government organizations or based on own proposals

(2) Items relating to enhancement of the basis for CIP

(i) Participate in cross-sectoral exercises as necessary

8. Cybersecurity Related Agencies

(1) Items relating to enhancement of information sharing system

(i) Cooperate with the Cabinet Secretariat and operate the information sharing system during normal circumstances and upon a CISs crisis

(ii) Collect information, etc. related to attack methods and recovery methods and carry out information sharing to the Cabinet Secretariat

(iii) Carry out supplemental information sharing based on consensus with the CI operators or CEPTOARs and also share the relevant information with stakeholders after data anonymization if consent of data sources is obtained

(iv) Cooperate with the Cabinet Secretariat with the examination of enhancement of analysis functions

(v) Implement opinion exchanges, etc. when requested by the CEPTOAR council

(2) Items relating to utilization of risk management

(i) Support proactive efforts among CI operators that comprise the CEPTOAR concerned. Also, cooperate with the Cabinet Secretariat, responsible ministries for CIP, other CEPTOARs and other stakeholders as necessary.

(3) Items relating to enhancement of the basis for CIP

(i) Provide information related to CISs outage case examples required for cross-sectoral exercises to the Cabinet Secretariat

(ii) Work with the Cabinet Secretariat to enhance cooperation and collaboration with governments of all countries, etc. and promote knowledge sharing and capacity building assistance, etc.

9. Cyberspace-related Operators

(1) Items relating to enhancement of information sharing system

(i) Cooperate with the Cabinet Secretariat with the initiatives for preparing information to be subject to sharing and sharing methods for said information

(ii) Carry out proactive information sharing to the Cabinet Secretariat during normal circumstances and upon a CISs crisis

VI. Assessment and Verification

Assessment and verification of this Cybersecurity Policy are conducted from the following two perspectives.

○ Assessment from the perspective of measuring the outcome

Assessment is conducted from the perspective of measuring to what extent society has come closer to the envisaged future through activities based on this Cybersecurity Policy. Assessment here means to check the validity of activities based on this Cybersecurity Policy in light of the envisaged future and extract issues to be addressed for the purpose of improving individual policies.

○ Verification from the perspective of measuring the output

Verification is conducted from the perspective of measuring the results brought about by individual activities based on this Cybersecurity Policy with the aim of ensuring their steady progress and continued improvements. Verification here means to check the progress of individual activities during each fiscal year objectively and decide basic policies from the following fiscal year onward.

1. Assessment of This Cybersecurity Policy

1.1 Assessment

Assessment from the perspective of measuring the outcome (assessment of this Cybersecurity Policy) is conducted in light of "2. Envisaged Future" in "I. Introduction" of this Cybersecurity Policy. Considering that the outcome is brought about as a result of mutually related various initiatives based on this Cybersecurity Policy, assessment should be conducted not for each policy separately but for the entirety of measures contributing to CIP, in other words, comprehensively for the overall framework of this Cybersecurity Policy.

Assessment of this Cybersecurity Policy is conducted by the Cybersecurity Strategic Headquarters, and surveys and reviews necessary therefor are conducted by the CI Expert Committee with cooperation of responsible ministries for CIP.

Assessment of the Cybersecurity Policy is generally conducted once every three years, in principle, because assessment of annual changes cannot easily lead to improvements due to the nature of the Cybersecurity Policy. This principle of conducting assessment once every three years does not apply when any significant changes beyond expectations occur in social trends, etc.

1.2 Supplementary studies

When carrying out assessment of the framework of this Cybersecurity Policy, it is important to carry out comprehensive assessment after appropriately ascertaining the conditions which cannot be completely identified only through individual outputs and the outcomes of policy groups. For this reason, in order to collect the supplementary information required for assessment, supplementary studies are to be carried out

every fiscal year in principle. Study results are to be publicized to the extent possible.

2. Verification of This Cybersecurity Policy

2.1 Verification

Verification from the perspective of measuring output (verification of the progress in each fiscal year) is conducted for policy groups indicated in "IV. Activities Within the Term of this Policy" (hereinafter "activities under this Cybersecurity Policy").

Verification of this Cybersecurity Policy is conducted by the Cabinet Secretariat every fiscal year under the initiative of the Cybersecurity Strategic Headquarters with cooperation of CI operators and responsible ministries for CIP. The results are referred to the Cybersecurity Strategic Headquarters after deliberations at the CI Expert Committee.

2.2 Verification of measures taken by CI operators

As the party with the most fundamental responsibility for the safe and continuous provision of CI services, CI operators implement cybersecurity measures on a daily basis. In order to continually and steadily improve such initiatives and in order to make government's support for CI operators' initiatives more effective, it is important to objectively verify the outcome of the implemented cybersecurity measures.

Based on the purpose of CIP, i.e., ensuring safe and continuous provision of CI services, the conditions of the countermeasures and responses to CISs outages in each CI sector is to be verified.

Measures of individual CI operators include independent initiatives based on the management decisions of each operator, and it is therefore appropriate for each CI operator to work toward their own self-improvement. CI operators should also verify their readiness for CISs outages, and when they encounter CISs outages, they should assess their responses by themselves and should preferably disclose their self-assessment if possible.

2.3 Verification of policies by government organizations

The activities of government organizations under this Cybersecurity Policy are all formulated to promote independent activities or other necessary measures relating to cybersecurity being implemented by CI operators.

Verification of policies is to be based on their contribution to the cybersecurity measures taken by CI operators under this Cybersecurity Policy to ensure cybersecurity.

VII. Revision of This Cybersecurity Policy

Revision of this Cybersecurity Policy is conducted by the Cybersecurity Strategic Headquarters, based on the assessment of this Cybersecurity Policy, and surveys and reviews necessary therefor are conducted by the CI Expert Committee with cooperation of responsible ministries for CIP.

Revision of the Cybersecurity Policy is generally conducted once every three years, in principle, however this does not apply when any significant changes beyond expectations occur in social trends, etc.

ATTACHMENT: INFORMATION SHARING TO NISC AND INFORMATION SHARING FROM NISC

1. Information Related to System Failures

Information related to system failures, including CISs outages, and Signs/*Hiyari-Hatto* events (hereinafter referred to as "information related to system[6] failures") needs to be handled with consideration given to the following three aspects: [i] proactive prevention of CISs outages, [ii] prevention of the spread damages and quick recovery from CISs outages, and [iii] prevention of recurrence through analysis and verification of CISs outage causes. Government organizations must provide such information to CI operators properly as necessary, while there is also a need to further enhance information sharing systems among CI operators and among interdependent CI sectors.

As Signs/*Hiyari-Hatto* events with no visible phenomena may eventually lead to CISs outages involving multiple CI sectors and CI operators, they should also be included in the scope of information sharing, in addition to actualized system failures.

Therefore, the scope of information sharing in this Cybersecurity Policy is as shown in the figure below.

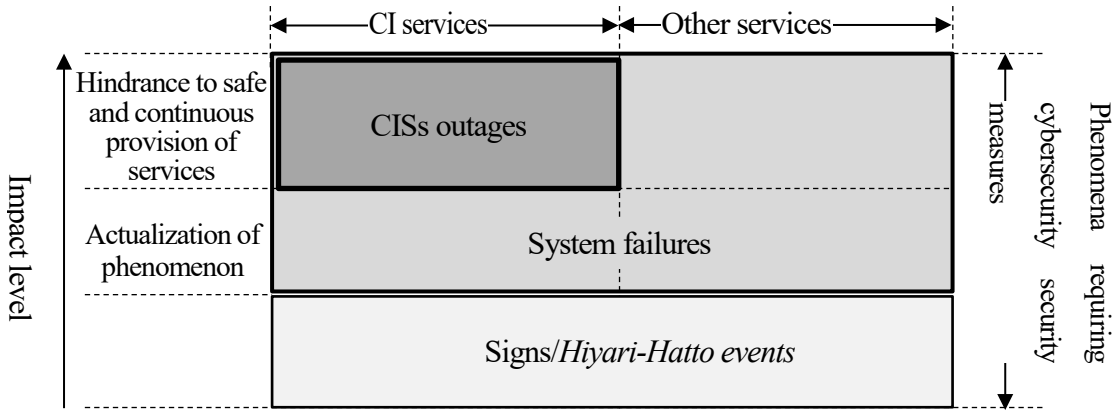


Figure. Scope of Information Sharing

[6] It should be noted that the term "system" here includes not only so-called information systems, but also control systems used in plants or for system monitoring in various CI sectors, as well as IoT systems, etc. whose utilization is spreading rapidly.

2. Information Sharing to NISC from CI Operators

2.1 Cases requiring information sharing to NISC

Of information related to system failures,[7] CI operators should conduct information sharing to NISC in any of the following cases. In detail, CI operators should report events and causes identified at that time as needed and such information provided before the complete picture is identified may be fragmentary or uncertain.

(i) Cases where the relevant event requires a report to responsible ministries for CIP under laws and regulations

(ii) Cases where stakeholders recognize the relevant event's serious impact on national life and CI services, and where the relevant CI operator considers it appropriate to share information of said event

(iii) Other cases where the relevant CI operator considers it appropriate to share information on the relevant event

When it is not clear whether or not any of the above is applicable, CI operators should preferably consult with responsible ministries for CIP or the Cabinet Secretariat.

2.2 Framework for information sharing to NISC

The procedures for information sharing from CI operators to the Cabinet Secretariat via responsible ministries for CIP are as follows.

(i) CI operators classify events and causes based on "ANNEX 3. CATEGORIES OF EVENTS AND CAUSES FOR INFORMATION SHARING TO NISC" and share information to responsible ministries for CIP in accordance with "ANNEX 4-1. INFORMATION SHARING SYSTEM (NORMAL CIRCUMSTANCES)" and therefore by extension "ANNEX 4-2. INFORMATION SHARING SYSTEM (CISs CRISIS)

(ii) The personnel of responsible ministries for CIP appointed for each jurisdictional sector (liaison to the Cabinet Secretariat) shares the information received from the CI operators of the relevant sector to the Cabinet Secretariat.

(iii) The Cabinet Secretariat appropriately manages the shared information and handles the information within the scope of information sharing permitted by data sources.

(iv) When there is an urgent need, regardless of procedures (i) and (ii), CI operators immediately share information to responsible ministries for CIP and make a report to the Cabinet Secretariat simultaneously.

As shown in ANNEX 4-1 and ANNEX 4-2, regarding Signs/*Hiyari-Hatto* events, or system failures for which reporting is not legally required, CI operators may share them to responsible ministries for CIP and to NISC after data anonymization via the CEPTOAR secretariat.

[7] Meaning information on system failures, including CISs outages, and Signs/*Hiyari-Hatto* events.

2.3 Handling of information shared to NISC

The Cabinet Secretariat and responsible ministries for CIP that received information shared to NISC do not disclose it in principle, where not otherwise specified by laws and regulations or agreed to by the CI operator submitting the information. Said information is handled as the information (non-disclosure information) prescribed in Article 5, item (ii), (b) of the Act on Access to Information Held by Administrative Organs (Act No. 42 of 1999). If said information falls under the information prescribed in the proviso to said item[8], the information may be disclosed. This does not apply when falling under the cases requiring information sharing from NISC as explained in 3.1 below.

[8] Information which is found necessary to be disclosed in order to protect a person's life, health, livelihood, or property

3. Information Sharing from NISC

3.1 Cases requiring information sharing from NISC

If it is found that the case falls under any of the following as a result of collecting and analyzing information on system failures provided broadly from responsible ministries for CIP, cybersecurity related ministries, crisis management ministries, disaster prevention related ministries, cybersecurity related agencies, cyberspace-related operators, and CI operators, the Cabinet Secretariat provides relevant information positively.[9]

(i) Cases where the obtained information is regarding a security hole, program bug, etc. and it is recognized that serious problems related to said information may occur at other CI operators

(ii) Cases where there is a cyber-attack or advance notice of such an attack, where there are predicted damages from a disaster, or where it is otherwise recognized that the information poses a risk to the critical information systems of other CI operators

(iii) Other cases where information sharing is considered to be effective for CI operators' cybersecurity measures

The Cabinet Secretariat provides information after taking appropriate measures, such as anonymizing or otherwise processing information, so as not to cause any disadvantage to data sources.

The scope to which the Cabinet Secretariat provides information is limited to CI sectors that are found to have a relevant connection with said information by the Cabinet Secretariat, within the scope permitted in advance by data sources. If the Cabinet Secretariat considers it necessary to share information beyond the scope permitted by data sources, necessary change to the scope is to be discussed and adjusted with data sources.

3.2 Framework for information sharing from NISC

The procedures for information sharing from the Cabinet Secretariat to CI operators via responsible ministries for CIP are as follows.

(i) When the Cabinet Secretariat shares information, such sharing is carried out through liaisons to the Cabinet Secretariat for respective jurisdictional sectors of responsible ministries for CIP. At that time, appropriate information identification methods are devised so that information receivers can recognize the classification and scope of handling of the information based on its degree of importance and content, and can utilize the information easily.

(ii) Liaisons of responsible ministries for CIP convey the information to the relevant CEPTOAR's point of contact (PoC).

(iii) CEPTOARs convey the information to CI operators which make up respective

[9] With regard to the information to be provided, the accuracy thereof should be enhanced through cross-check of data, or otherwise, efforts should be made to improve the quality of information. Concrete measures include studies of CISs outages caused by suspension or deterioration of services in CI sectors, and estimates of possible impacts of CISs outages due to common risk sources on other CI sectors, etc.

CEPTOARs.

(iv) In particularly urgent cases, such as the case of early warning information, etc., regardless of procedures (i) to (iii), the Cabinet Secretariat directly provides the information to CEPTOARs or individual CI operators and releases reports to liaisons of responsible ministries for CIP simultaneously. However, procedures (i) should be followed for the adjustment of information identification methods.

3.3 Cooperation for information sharing from NISC

In the collection of information provided to CI operators through responsible ministries for CIP and in sharing of information to CI operators, the Cabinet Secretariat cooperates with cybersecurity related ministries, crisis management ministries, disaster prevention related ministries, cybersecurity related agencies and cyberspace-related operators as follows.

(i) Collect a wide range of information provided by cybersecurity related ministries, crisis management ministries, disaster prevention related ministries, and cybersecurity related agencies

(ii) Collect additional information related to CISs outages from cyberspace-related operators as necessary

(iii) Request cooperation from cybersecurity related agencies and cyberspace-related operators in the collection and analysis of information as necessary

(iv) For information on CISs crises, collect and share information under the information sharing system composed of the Cabinet Secretariat, crisis management ministries and the disaster prevention related ministries, in addition to under the information sharing system during normal circumstances.

ANNEX 1 SCOPE OF CI OPERATORS AND CRITICAL INFORMATION SYSTEM EXAMPLES

CI sectors	Applicable CI operators (Note 1)	Applicable critical information system examples (Note 2)
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 - Payment 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. - Major fund transfer businesses - Major prepaid payment instruments (third-party issuer) 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
Airport	- Major airport and airport building operators	- Vigilance, guard and monitoring systems - Flight information systems - Baggage handling 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	- Local governments	- Local government information systems
Medical services	- Medical facilities (Excluding small scale facilities)	- Medical examination record management systems, etc. - Medical examination support systems - Community medical care support systems
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 ・Major settlement agencies ・Designated credit information agencies etc.	・Credit card payment-related systems (intermediation of comprehensive credit card purchases and intermediation of two-month installment purchases) ・Credit information provision and collection systems
Petroleum industries	- Major petroleum refinery facilities and petroleum wholesalers	- Sales order management system - Product management system - Shipping management system

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.

Note 2 The operators listed here are examples and do not constitute a comprehensive list.

ANNEX 2 EXPLANATION OF CI SERVICES AND SERVICE MAINTENANCE LEVELS

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 procedures) (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).
	- 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.

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 procedures) (Relevant laws)		
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
		- Clearing services for interbank funds transfer	- Clearing services for interbank funds transfer (Article 2, paragraph (10) of the Payment Services Act)	- Delay and suspension of clearing services for interbank funds transfer	- Comprehensive Guideline for Supervision of Financial Market Infrastructures
		- Electronic records, etc.	- Electronic records (Article 56 of the Electronically Recorded Monetary Claims Act) - Information provision related to Payment services (Articles 62 and 63 of the Electronically Recorded Monetary Claims Act)	- Delay and suspension of information provision related to electronic records and payment services	- 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 (Article 97, paragraph (1) of the Insurance Business Act) - Insurance claim etc. payment screenings (Article 97, paragraph (1) of the Insurance Business Act) - Insurance claim etc. payments (Article 97, paragraph (1) of the Insurance Business Act)	- 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 (Article 97, paragraph (1) of the Insurance Business Act) - Damage investigations etc. (Article 97, paragraph (1) of the Insurance Business Act) - Insurance claim etc. payments (Article 97, paragraph (1) of the Insurance Business Act)	- Delay and suspension of insurance claim etc. payments	- Comprehensive Guidelines for the Supervision of Insurance Companies
	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.

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 procedures) (Relevant laws)		
		- 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
	Payment services	- Fund transfer services	- Currency exchange (Article 2, paragraph (2) of the Payment Services Act)	・Delay and suspension of payment services ・Delay and suspension of fund transfers including bank transfers	- Guideline for Administrative Processes Vol 3.: Financial Companies (14 Fund transfer services providers-related)
		- Issuance of third-party prepaid payment instruments	- Issuance of third-party prepaid payment instruments (Article 3, paragraphs (1) and (5) of the Payment Services Act)	・Delay and suspension of payment services	- Guideline for Administrative Processes Vol 3.: Financial Companies (5 Prepaid payment instrument issuer-related)
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 the Aviation Sector
		- 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		

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 procedures) (Relevant laws)		
Airport	- Ensuring security at the airport - Improvement of convenience at the airport	- Ensuring airport security by vigilance and guard - Accurate and prompt information provision to airport users - Inspection and transport of checked baggage to aircraft	- Deterioration of airport security due to the occurrence of trouble with the vigilance and guard - Deterioration of convenience due to the occurrence of trouble with the information provision - Delay or stop of inspection and delivery of checked baggage to aircraft	- Safety guideline for Ensuring Information Security for the Airport Sector
Railway services	- Passenger transport services - Ticketing, entry and exit procedures	- Work providing transport of passengers or cargo for charge using railways based on demands of other people (Article 2 of the Railway Business Act) - Seat reservation, boarding ticket checks on boarding and exiting the train	- 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 - Safety guideline for Ensuring Information Security for the Railway Sector
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 (1) , item(viii) 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 (1),item(xiv) 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 - Gas manufacturing 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, paragraph (5) of the Gas Business Act) - 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, paragraph (9) 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.
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	- Guideline for information security policy for local governments

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 procedures) (Relevant laws)		
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
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 services	- Credit card payment-related systems (intermediation of comprehensive credit card purchases and intermediation of two-month installment purchases) (Article 2, paragraph (3) and Article 35-16, paragraph (2) of the Installment Sales Act) ・Specific credit information services (Article 35-3-36 of the Installment Sales Act)	- Delay and suspension of credit services - Large-scale leakage of credit card information	- The basic policy for supervision based on the Installment Sales Act (deferred payment section) - Information Security Guideline for the Credit CEPTOAR
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

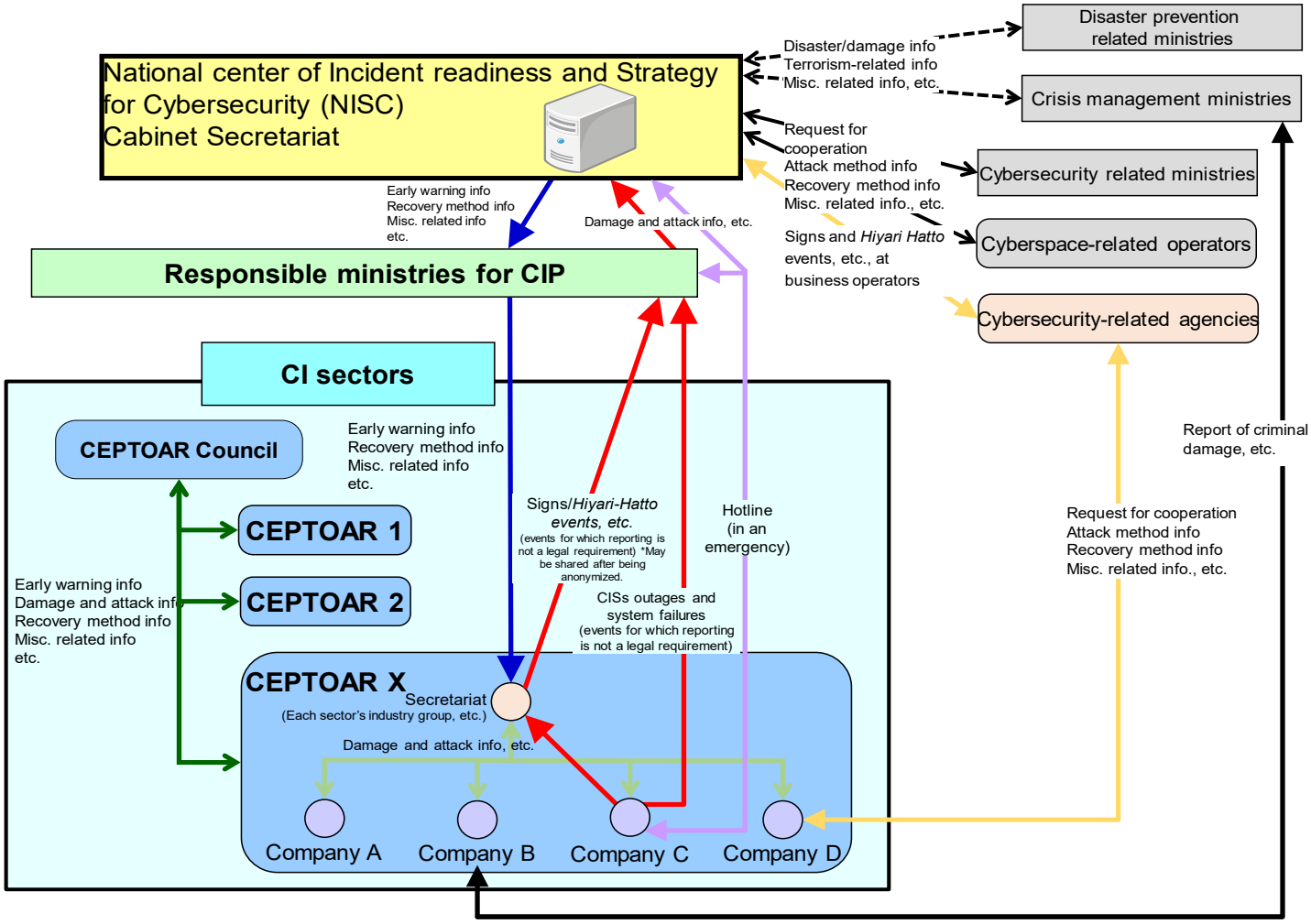
Note 1: Excluding services wherein IT is not at all utilized
Note 2: For sectors without any specific standards concerning CISs outages, the service maintenance level is to ensure no CISs outages caused by system failures.

ANNEX 3. CATEGORIES OF EVENTS AND CAUSES FOR INFORMATION SHARING TO NISC

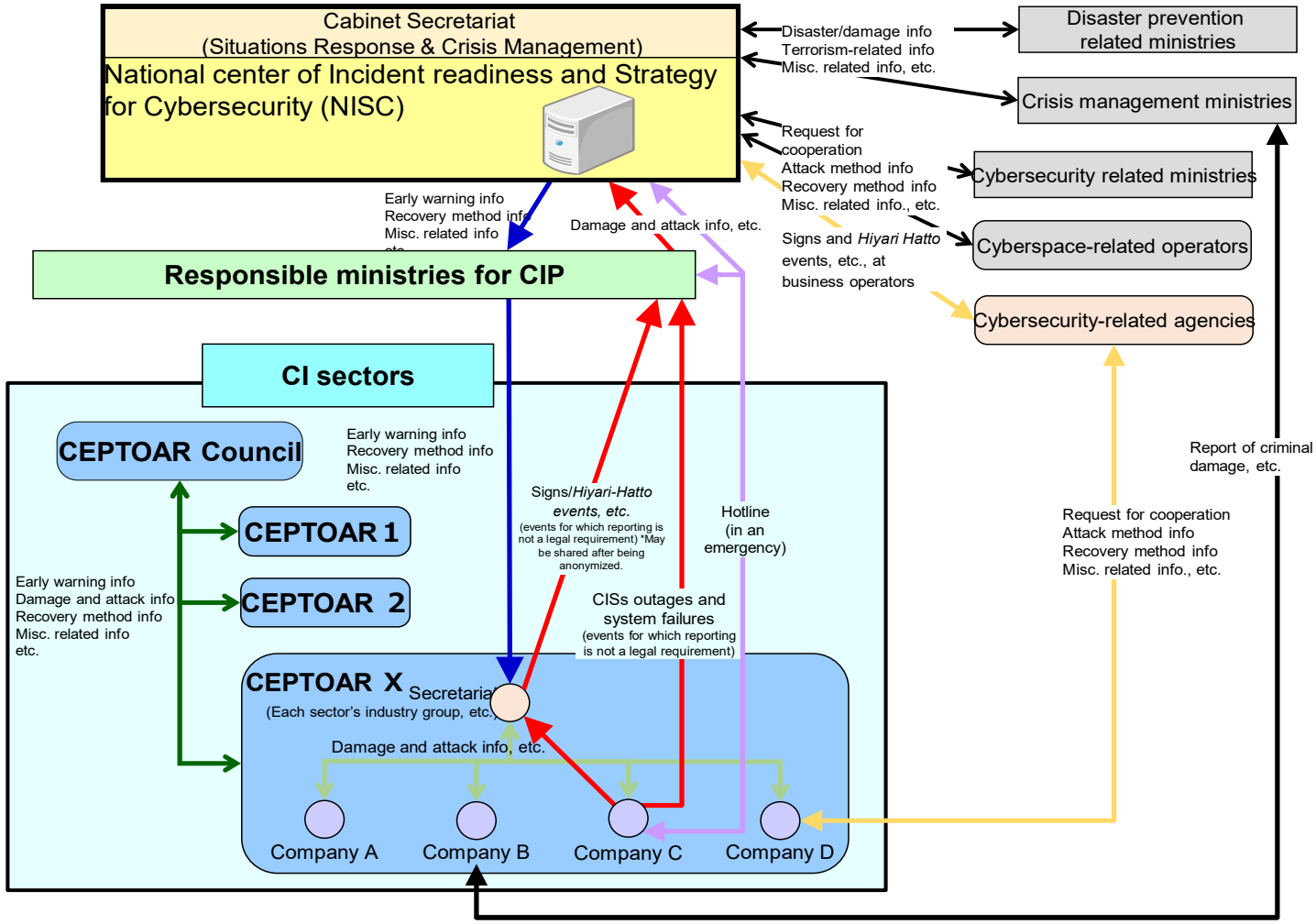
Event Categories		Event Examples	Description
Events that have not occurred yet		Signs/ *Hiyari-Hatto* events	Signs such as cyber-attack warnings, or *Hiyari-Hatto* events (potentially serious damage) without occurrence of events that threaten confidentiality, integrity or availability, such as minor mistakes or receipt of malware attached to suspicious emails.
Events that have occurred	Events that threaten confidentiality	Information leakage	Events that threaten confidentiality, such as the leakage of organization's confidential information
	Events that threaten integrity	Data corruption	Events that threaten integrity, such as website defacement or corruption of organization's confidential information
	Events that threaten availability	Problems in using systems	Events that threaten availability, such as loss of stable operation of control systems or inability of viewing websites
	Events that can lead to those above	Malware infections	Infection of systems by malware
		Execution of unauthorized code	Execution of unauthorized code exploiting the vulnerability of systems
		System intrusions	Intrusions into systems caused by cyber-attacks
		Others	Events other than those above

Cause Categories	Cause Examples
Deliberate causes	Receipt of suspicious emails, fraudulent of user IDs, mass access such as DDoS attacks, unauthorized acquisition of information, internal fraud, lack of appropriate system operation, etc.
Accidental causes	Mistaken user operation, mistaken user management, execution of suspicious files, viewing of suspicious websites, unsupervised work by outsourcing contractor, failure of equipment, vulnerabilities, cascading effect from other sectors' failures, etc.
Environmental causes	Disasters, illnesses, etc.
Others	Threats and vulnerabilities other than those above, unknown causes, etc.

ANNEX 4-1. INFORMATION SHARING SYSTEM (NORMAL CIRCUMSTANCES)



ANNEX 4-2. INFORMATION SHARING SYSTEM (RESPONSE TO CISs CRISIS)



ANNEX 4-3. RESPONSIBILITIES OF EACH STAKEHOLDER IN INFORMATION SHARING SYSTEM

Stakeholder	Responsibilities during normal circumstances	Responsibilities during a CISs crisis [Note]
○ Cabinet Secretariat (Situations Response & Crisis Management)	The Cabinet Secretariat shares information on CI-related incidents with NISC.	In addition to fulfilling responsibilities during normal circumstances, the Cabinet Secretariat collects information on damage and responses provided by crisis management ministries and disaster prevention related ministries, integrally with NISC, and mutually shares information with NISC.
○ Cabinet Secretariat (NISC)	NISC shares information on system failures mutually with responsible ministries for CIP, cybersecurity related ministries, crisis management ministries, disaster prevention related ministries, cybersecurity related agencies, and cyberspace-related operators, etc.	Integrated with the Cabinet Secretariat responsible for situations response and crisis management, NISC shares information on system failures mutually with responsible ministries for CIP, cybersecurity related ministries, crisis management ministries, disaster prevention related ministries, cybersecurity related agencies, and cyberspace-related operators, etc.
○ Responsible ministries for CIP	Responsible ministries for CIP provide information on system failures received from CI operators under jurisdiction to NISC and relevant CEPTOARs as needed. They also provide information on system failures received from NISC to relevant CEPTOARs.	In addition to fulfilling responsibilities during normal circumstances, responsible ministries for CIP cooperate with the CISs crisis response system as necessary.
○ CEPTOAR council	The CEPTOAR council is an independent body, not ranked below other agencies, including government organizations. Cooperation is carried out based on independent decisions by each CEPTOAR. Each CEPTOAR actively participates based on independent decisions and carries out a wide scope of information sharing aimed at CI operator service maintenance and recovery.	In addition to fulfilling responsibilities during normal circumstances, the CEPTOAR council constructs a CISs crisis response structure as necessary and collaborates with CEPTOARs and other related organizations.
○ CEPTOAR secretariat	The CEPTOAR secretariat collaborates with responsible ministries for CIP, crisis management ministries, disaster prevention related ministries, cybersecurity related agencies, the CEPTOAR council and CI operators, and mutually shares information on system failures.	In addition to fulfilling responsibilities during normal circumstances, the CEPTOAR secretariat constructs a CISs crisis response system as necessary and collaborates with the Cabinet Secretariat and other related organizations.
○ CI operators	CI operators share information on system failures within respective CEPTOARs as necessary and provide such information to responsible ministries for CIP based on the "ATTACHMENT: INFORMATION SHARING TO NISC AND INFORMATION SHARING FROM NISC," and when there are any criminal damages, also make a report to relevant crisis management ministries based on independent decisions.	In addition to fulfilling responsibilities during normal circumstances, CI operators construct a CISs crisis response system as necessary and collaborate with the Cabinet Secretariat and other related organizations.

Note: In the event of a CISs crisis due to a disaster or terror attack, etc., relevant ministries should collect and share information in accordance with "Regarding the Government Initial Response System for Emergencies" (November 21, 2003, Cabinet resolution).

ANNEX 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	CI refers to sectors that comprise the backbone of national life and economic activities formed by businesses providing services that are extremely difficult to be substituted; if the function of the services is suspended or deteriorates, it could have a significant impact on national life and economic activities.
CI operators	Refers to "critical social infrastructure providers and other related entities" as stipulated in Article 12, paragraph (2), item (iii) of the Basic Act on Cybersecurity. Includes CI operators (excl. related entities), the associations they form and local governments.
CI operators (excl. related entities)	Refers to "critical social infrastructure providers" as stipulated in Article 3, paragraph (1) of the Basic Act on Cybersecurity. These are operators whose businesses form the backbone of national life and economic activities and if the functioning of the services were to be suspended or deteriorated could have a significant impact on national life and economic activities. Specifically, of the operators engaged in CI-related businesses, those operators designated in the "Applicable CI operators" column of "ANNEX 1. SCOPE OF CI OPERATORS AND CRITICAL INFORMATION SYSTEM EXAMPLES" (excluding local governments).
CI sectors	14 sectors with CI designated for each business type; specifically, as follows: "information and communication services," "financial services," "aviation services," "airport 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 national life and economic activities
CISO	Chief Information Security Officer; Refers to a person responsible for overseeing information security of information systems and networks, management of confidential information and personal information, etc. in companies or government agencies, etc.
CISs crisis	Large-scale CISs outages which require intensive response by the government such as the establishment of the Cabinet Response Office at the Crisis Management Center in the Prime Minister's Office
CISs outages	Situation where system failures hinder safe and continuous provision of CI services
Contingency plans	Plans formulated in advance with regard to policies, procedures, readiness, etc. for initial responses (emergency responses) to be taken by top management and officials, etc. immediately after CI operators recognize the occurrence or a possibility of CISs outages.
Crisis management ministries	The National Police Agency (NPA); Fire and Disaster Management Agency (FDMA); Japan Coast Guard (JCG); Ministry of Defense (MOD)
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.
CSIRT	Computer Security Incident Response Team; A structure established to monitor information systems and other systems for any security problems that may occur in companies or government agencies, etc., and to analyze the causes and investigate the scope of impact if a problem should occur.
Cybersecurity	Refers to cybersecurity as described in Article 2 of the Basic Act on Cybersecurity, namely that the necessary measures have been taken to safely ensure the secure management of information in electronic and magnetic form, and to ensure security and reliability of information systems and of information and communications networks; and that such a status is being properly maintained and managed.

Cybersecurity related agencies	National Institute of Information and Communications Technology (NICT); Information-Technology Promotion Agency (IPA); Japan Computer Emergency Response Team Coordination Center (JPCERT/CC); Japan Cybercrime Control Center (JC3).
Cybersecurity related ministries	The National Police Agency (NPA); Digital Agency, 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.
Cyberspace-related business entities	Of the cyber-related business entities stipulated in Article 7 of the Basic Act on Cybersecurity system vendors, which are engaged in the supply chain-related delivery of equipment, and the design, construction, operation and maintenance of information systems required for providing CI services; security vendors, which provide security measures such as antivirus software of those information systems; and platform vendors and operators that provide external services such as cloud services, 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
Guidelines for Safety Principles	Cybersecurity measures, which contain high-priority items and/or advanced items which should serve as a reference, collected with an overlook on all the CI sectors, in order to contribute to preparation and revision of safety principles Main section is approved by the Cybersecurity Strategic Headquarters.
Information sharing	The mutual provision and sharing among relevant entities of information on system failures (information including that on CISs outages and possible system failures and Signs/*Hiyari-Hatto* events) and information that will contribute to ensuring cybersecurity This includes both information sharing to NISC and information sharing from NISC.
Information sharing from NISC	The provision of information for contributing to cybersecurity 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 possible system failures and Signs/*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
IT-BCP	Business continuity plan (including relevant manuals) related to the information systems to provide CI services, and other business continuity plan.
National CERTs/CSIRTs	Overall coordination functions whereby the government promotes a series of activities in an integrated manner in response to serious cyberattacks, from information collection and analysis to investigation and assessment, implementation of alerts and countermeasures, and subsequent policy planning and measures to prevent recurrence of such cyberattacks.
Responsible ministries for CIP	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)

Safety principles	Collective term for "regulations" stipulated by the government in compliance with relevant laws, "recommendations" and "guidelines" developed by the government according to relevant laws, "standards" and "guidelines" in the whole-sector developed by sector-specific groups to respond to relevant laws and public expectations, and "internal policies" prepared by CI operators themselves to respond to relevant laws and expectations of public and customs; However, safety principles do not include the "Guidelines for Safety Principles."
Service maintenance level	Based on the concept of mission assurance, the level at which CI services are judged to be provided safely and continuously
Signs/*Hiyari-Hatto* events	Events that may cause or may have caused system failures although there are not or have not been any failures in reality
Stakeholders	The Cabinet Secretariat; responsible ministries for CIP; cybersecurity related ministries; crisis management ministries; disaster prevention related ministries; CI operators; CEPTOARs and CEPTOAR secretariat; CEPTOAR council; cybersecurity related agencies; cyberspace-related operators.
Supply chain	In general, this refers to the flow of goods and information in business activities from upstream to downstream, so to speak, from the point of receiving and placing orders with suppliers and procurement of materials, through to inventory management and product delivery. In addition to these, the supply chain in IT may also include the product design stage, and the operation, maintenance, and disposal of information systems, etc.
System failures	Events that information systems of CI operators do not or cannot perform as expected at the time of their design