The Cybersecurity Policy for Critical Infrastructure Protection

(4th Edition)

(Tentative Translation)

April 18, 2017
(Revised July 25, 2018)
Cybersecurity Strategic Headquarters
Government of JAPAN

Table of Contents

I. Introduction

1. Direction for Establishing the Cybersecurity Policy

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 (CI) services, 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. As safe and continuous provision of CI services is required due to their nature, Critical Infrastructure Services (CISs) outage risks due to cyberattacks on indispensable information systems must be reduced to the extent possible, and at the same time, efforts for early detection of and swift recovery from outages are of great importance in protecting them.

Therefore, the government established the Cybersecurity Policy for Critical Infrastructures Protection (the "Cybersecurity Policy"), a shared policy between the government, which bears responsibility for protection, and CI operators, which independently carry out relevant protective measures, as a basic framework for CI protection, and has promoted this initiative.

This framework was originally formulated with the establishment of the "Special Action Plan on Cyber-terrorism Countermeasures for Critical Infrastructure" (concluded in the December 2000 Information Security Measure Promotion Meeting; the "Special Action Plan") and had served as the basis for the policy related to cybersecurity measures for Japan's critical infrastructure for over 16 years, up until the establishment of the preceding Basic Policy of Critical Information Infrastructure Protection (3rd Edition) (concluded by the Information Security Policy Council in May 2014 and revised by the Cybersecurity Strategic Headquarters in May 2015; the "Third Policy"). Certain achievements have been made, while reflecting the lessons learned from the experience of dealing with system outages and data loss during the Great East Japan Earthquake and appropriate responses having been made to an ever-changing social and technological environment and the increasingly sophisticated and complex cyberattacks in recent years, and through necessary reviews based on assessment of measures implemented under this framework.

Considering these backgrounds, the Cybersecurity Policy of Critical Infrastructure Protection (4th Edition) ("this Cybersecurity Policy") was established while maintaining the basic framework for CIP. Based on the basic concept of the Basic Act on Cybersecurity (Act No. 104 of 2014), assessment of the Third Policy described later, and the Cybersecurity Strategy (Cabinet resolution in September 2015), this Cybersecurity Policy maintains the basic structure consisting of the five key policies in the Third Policy which have become deeply rooted among stakeholders. In the meantime, changes in cyberattacks targeting CI and in the background social and technological environment are significant, and information technology (IT) has come to be increasingly incorporated in socioeconomic systems integrally with operational technology (OT)[1] such as control systems. Additionally, IoT systems, which may be targeted

[1] Hereinafter, operational technology for control systems using IT is simply indicated as OT.

in cyberattacks, are also becoming more widely used. Ahead of the Olympic and Paralympic games to be held in Tokyo in 2020 (the "Olympic and Paralympic games"), risks surrounding CI may be increasing. Therefore, this Cybersecurity Policy specifies priorities and aims to enhance and improve measures in each key policy.

2. Structure of This Cybersecurity Policy

The structure of this Cybersecurity Policy and outlines of each Chapter are as indicated in Table 1.

For responsible entities for respective initiatives based on this Cybersecurity Policy, please refer to Chapter IV.

Table 1 Structure of This Cybersecurity Policy

Chapter	Outlines
I. Introduction	Directions for establishing this Cybersecurity Policy based on the results of the assessment of the Third Policy, and principles and ideas for implementing this Cybersecurity Policy
II. Executive Summary of This Cybersecurity Policy	[i] Purpose of CIP, [ii] Basic principles, [iii] Responsibility of stakeholders, and [iv] Responsibility of CI operators' executives and senior managers in promoting this Cybersecurity Policy
III. Policies for CIP	Policies for carrying out cybersecurity measures and details of concrete measures for each of the five key policies of this Cybersecurity Policy
IV. Activities Taken by Stakeholders	Regarding cybersecurity measures (III. above), concrete measures that each stakeholder takes or is expected to take
V. Assessment and Verification	Policies and methods for the assessment and verification of this Cybersecurity Policy
VI. Revision of This Policy	Policies for the revision of this Cybersecurity Policy based on the results of the assessment (V. above)

3. Assessment of the Third Policy

The Third Policy is composed of the following five key policies.

[1] Maintenance and promotion of the safety principles

[2] Enhancement of information sharing system

[3] Enhancement of incident response capability

[4] Risk management

[5] Enhancement of the basis for CIP

After analytical assessment for each key policy (assessment of the results and clarification of issues), comprehensive assessment was conducted for the entirety of the Third Policy (assessment of the achievement and clarification of issues in light of the purpose (envisaged future) during the term).

The comprehensive assessment is outlined as follows.

< Envisaged Future >

Voluntary activities based on each stakeholder's awareness of their responsibilities are disseminated as their respective code of conduct and such behavior contributes to forming cybersecurity culture.

< Assessment >

The Third Policy clearly indicates the basic principle, stating that cybersecurity measures should be taken by CI operators on their own responsibility, and then presents this envisaged future.

With the aim of promoting voluntary efforts by CI operators, the Guidelines for Establishing Safety Principles for Ensuring CI Security and Attachment thereof (the "Guidelines for Safety Principles") were revised in line with the PDCA (Plan-Do-Check-Act) cycle. Each CI sector guideline and codes of conduct of respective CI operators such as internal policies are now being reviewed on a voluntary basis in response to the revision of the Guidelines for Safety Principles.

Given these, it is considered that the PDCA cycle itself, which allows CI operators to judge the necessity of review and make improvements independently, is prevailing as their code of conduct.

However, the activities of "Check" and "Act" in the PDCA cycle are not sufficiently established, nor can be recognized to have been disseminated to the degree that they are accepted as the code of conduct, as shown in the results of the survey concerning the dissemination of safety principles, which was conducted by the Cabinet Secretariat with the aim of ascertaining the current status of cybersecurity measures. The establishment of these activities is one of the remaining challenges.

In the future, it is hoped that such behavior based on the abovementioned code of conduct is disseminated among all stakeholders, encouraging them to continue efforts in line with this, and cybersecurity culture is thus formed among them.

< Envisaged Future >

Stakeholders communicate with each other on a regular basis with the aim of strengthening measures in preparation for any CISs outages and are making improvements to their measures constantly in order to reflect experience concerning incident responses in their future efforts.

< Assessment >

Active information sharing between the public sector and the private sector is steadily progressing, with an increasing number of reports being made from CI operators to responsible ministries and the National Center of Incident Readiness and Strategy for Cybersecurity (NISC).

Regarding information sharing in the private sector, the secretariat of the CEPTOAR council was transferred to the private sector, thereby enhancing their independence and positive attitude in information sharing among CEPTOARs. Additionally, members of each CEPTOAR have increased and broader information exchanges have been contributing to enriching knowledge on cybersecurity and creating ties among responsible personnel. The development of a better environment for communication among stakeholders has thus been steadily advancing. Furthermore, ISACs[2] have been organized in some sectors and information sharing and countermeasures against cyberattacks are progressing.

Cross-sectoral exercises and training by CEPTOARs are also being conducted continuously to enhance incident response capability. Participants are increasing significantly and response scenarios are made more and more sophisticated. These activities are found to have contributed to enhancing response capability in line with the needs of CI operators.

In the meantime, as threats are becoming increasingly serious, it is required to continue to improve communication methods qualitatively and quantitatively through their classification and specification in light of respective purposes in

[2] ISAC: Information Sharing and Analysis Center

order to further strengthen preventive measures against CISs outages. On the other hand, it should also be said that efforts to reflect experience of CISs outages in future measures in a cross-sectional manner are not necessarily sufficient although efforts have been made to enhance incident response capability through exercises and training. This needs to be addressed. Additionally, in order for CIP covering a broader area ("protection as plane"), constant improvements through analysis and sharing of case examples are indispensable and efforts therefor must be continued.

< Envisaged Future >

The fact that stakeholders are collaboratively making efforts for CIP is widely understood by the general public and this gives them peace of mind. Well-established communication among diverse stakeholders enables them to take calm responses in the event of CISs outage.

< Assessment >

Stakeholders have reliably come to have better communication as mentioned above. Additionally, the Third Policy and the achievement thereunder are publicized and videos of cross-sectoral exercises are publicly made available online. In this manner, PR activities have been carried out with the aim of reassuring the general public by having them better understand diverse efforts being made based on the Third Policy.

On the other hand, public concern over CIP cannot be fully relieved partly due to increasing news reports on information leakage caused by targeted mail attacks. Such concern needs to be eliminated.

Efforts to enhance incident response capability have been made through constantly checking the current status of incident response through exercises and training as mentioned above. Collaboration with overseas organizations, etc., such as information sharing under various frameworks, has also been promoted.

In order to reassure the general public and ensure calm responses upon CISs outages, it is necessary to continue and strengthen these efforts in collaboration with diverse entities in and outside Japan, while sharing collected and analyzed information on new risks, sources of risks and the latest incidents among stakeholders, and actively providing information to the general public based on the concept of mission assurance.

< Envisaged Future >

These efforts are publicized as the Cybersecurity Policy and are assessed regularly and revised properly as needed.

< Assessment >

Cybersecurity measures have been compiled and publicized as the Cybersecurity Policy since 2000 and the progress of the activities thereunder in each fiscal year has been checked and verified from the perspective of measuring the output of individual activities. Activities during the Cybersecurity Policy term have also been assessed once every three to five years from the perspective of measuring the outcome, i.e., to what extent society has come closer to the envisaged future, and the Cybersecurity Policy has been reviewed based on the results of the assessment.

Through these efforts, CIP in Japan has been implemented steadily for 16 years since the establishment of the Special Action Plan, or for 11 years under the current style of the First Policy to the Third Policy, and has been progressing steadily based on the five key policies. Therefore, it can be said that the Cybersecurity Policy and activities thereunder have been properly reviewed through regular assessments.

The basic framework for CIP should be maintained as the Cybersecurity Policy and efforts need to be continued into the future based thereon.

< Envisaged Future >

These efforts being made by stakeholders have become steadily rooted as measures contributing to the sustainable development of society.

< Assessment >

Efforts based on the Cybersecurity Policy are found to have been progressed steadily as mentioned above.

Therefore, the basic structure consisting of the five key policies in the Third Policy, which have deeply taken root among stakeholders, should be maintained and activities under each policy should be strengthened. In light of the status of cyberattacks targeting CI and background changes in the social and technological environment, and based on the concept of mission assurance, due consideration should be given to [i] further promotion of leading activities by some operators for protecting CI as a whole, [ii] enhancement of information sharing structure toward the Olympic and Paralympic games, and [iii] promotion of incident readiness based on risk management. These points should be positioned as policy priorities in this Cybersecurity Policy and concrete activities under each of the five key policies need to be enhanced and improved while keeping them in mind.

4. Outcome of the Review for the Revision of this Cybersecurity Policy

As explained above, the basic structure consisting of the five key policies in the Third Policy, which have taken deep root among stakeholders, are maintained in this Cybersecurity Policy, in light of the issues extracted through the assessment of the Third Policy and the Cybersecurity Strategy. It was decided to first clarify the purpose of CIP and decide policy priorities, in light of the status of cyberattacks targeting CI and background changes in the social and technological environment and also based on the concept of mission assurance, and then consider enhancement and improvement of activities under this Cybersecurity Policy.

4.1 Purpose of CIP

This Cybersecurity Policy maintains the purpose of CIP under the Third Policy but clearly states "ensuring safe and continuous provision of CI services" as the top priority based on the concept of mission assurance.

4.2 Concept of Mission Assurance

CI services are the very basis of national life and socioeconomic activities and suspension thereof may have a direct and serious negative effect on the safety and ease of the general public. Therefore, stakeholders are required to make efforts to ensure safe and continuous provision of CI services (mission assurance).

Mission assurance in this Cybersecurity Policy does not mean to oblige stakeholders to make a firm commitment to ensuring CIP or maintaining CI functions, but to have them assume their responsibilities in the process of protecting CI services and maintaining the functions thereof. This is the concept to require each stakeholder to properly make efforts for necessary cybersecurity measures.

(1) Efforts required for CI operators

The top management of CI operators must be actively involved in deciding business strategies incorporating preparedness for cybersecurity risks and taking measures to reduce such risks strategically based on the results of risk assessment. They need to put in place an appropriate incident readiness to continue CI services even in the case of receiving a cyberattack, etc., ensuring safety of their CI services and preventing suspension or quality loss unacceptable for themselves and other stakeholders to the extent possible. Top management should develop internal control systems concerning cybersecurity measures and must fulfill accountability to their own stakeholders concerning the fact that they are properly taking measures for mission assurance.

(2) Efforts required for government organizations

Government organizations are required to set or review the scopes of CI and CI services to be protected as the basis to support national life and socioeconomic activities, in collaboration with diverse stakeholders, and to offer necessary support to CI operators for their abovementioned efforts. Government organizations must also fulfill accountability to the general public concerning the fact that efforts are being made properly through the assessment of this Cybersecurity Policy and PR activities.

4.3 Priorities in This Cybersecurity Policy

The following three priorities are to be reflected in activities under each policy.

4.3.1 Promotion of leading activities by CI operators (classification of CI operators in light of interdependency)

The utilization of ICT is increasingly spreading among CI operators and interdependency among sectors has become deeper. In some sectors that are highly depended upon by other CISs and may cause a big impact in the case of outages even for a relatively short period of time (such as electric power supply services, information and communication services, and financial services), CI operators have voluntarily promoted highly advanced cybersecurity measures, centered on major operators belonging to the relevant sectors. In order to protect CI as a whole from increasingly sophisticated cyberattacks, etc., such leading activities need to be further enhanced and promoted and should also be disseminated to other CI operators within these sectors and those in other CI sectors. Therefore, this point is reflected in activities under this Cybersecurity Policy.

4.3.2 Enhancement of information sharing structure toward the Olympic and Paralympic games

Looking ahead to big international events, such as the Olympic and Paralympic games, Japan is attracting the attention of the international community but at the same time may also be subject to malicious attacks, posing a possibility that risks of cyberattacks, etc. may increase. In order to surely protect these international events and CI from heightened threats of cyberattacks, stakeholders need to detect threats early and take prompt and appropriate countermeasures based on helpful and practical information. Therefore, this point is reflected in the activities for the enhancement of information sharing structure under this Cybersecurity Policy.

Assuming that these activities are to be handed down as a legacy after the Olympic and Paralympic games, modeling of know-how and other knowledge concerning the formulation of relevant systems will be discussed.

4.3.3. Promotion of incident readiness based on risk management

Considering the fact that cyberattacks targeting CI are becoming more and more serious and in light of background changes in the social and technological environment, CI operators are required to develop appropriate incident readiness against cyberattacks, etc. so that they can continue the provision of CI services while ensuring safety of their services and preventing suspension or quality loss unacceptable for themselves and other stakeholders to the extent possible. Additionally, it is necessary to enhance and promote efforts for risk assessment, risk communication and consultation, monitoring and review in the process of risk management in order to develop appropriate incident readiness from the viewpoint of mission assurance. Therefore, this point is reflected in the activities for the risk management and development of incident readiness under this Cybersecurity Policy.

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

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

Table 2 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 Third Policy	Direction of reinforcing and refining the components of the Cybersecurity Policy
1. Maintenance and promotion of the safety principles	Basically keep the element of "[1] Maintenance and promotion of the safety principles" in the Third Policy	○ Improve the safety principles prioritizing the importance of the preparation of incident readiness, including awareness and behavior required for top management and the formulation of contingency plans, and the development of organizations and human resources while keeping OT in mind

		○ Continue efforts for appropriately improving institutional frameworks as necessary for maintaining safety, such as through positioning cybersecurity measures as safety regulations among relevant laws and embodying the service maintenance level in relevant laws from the viewpoint of mission assurance ○ Review items of the questionnaire survey so that the survey leads to further improvement and dissemination of the safety principles among CI operators
2. Enhancement of information sharing system	Basically keep the element of "[2] Enhancement of information sharing system" in the Third Policy	○ Further promote information sharing ・Eliminate obstacles that hinder information sharing by diversifying the contact formation (addition of a new route for information provision via the CEPTOAR secretariat, which enables data anonymization) ・ Promote efficient and effective responses through information sharing based on severity schema on CISs outages ・Develop the information sharing system to allow opening of a hotline to achieve prompt and efficient sharing of information on cyberattacks, 24 hours a day, 365 days a year ・Share awareness among stakeholders regarding the inclusion of OT and IoT in the scope of information sharing to and from NISC by clarifying the relevant scope
3. Enhancement of incident response capability	Basically keep the element of "[3] Enhancement of incident response capability" in the Third Policy	○ Continuously improve cross-sectoral exercises and CEPTOAR training that would be more practical for CI operators ○ Promote voluntary exercises by CI operators by broadly disseminating knowledge and know-how obtained through cross-sectoral exercises and providing a virtual exercise environment
4. Risk management and development of incident readiness	Basically keep the element of "[4] Risk management" in the Third Policy and develop the element as "Risk management and preparation of incident readiness"	○ Expand the scope of measures and add those for assisting preparation of incident readiness based on the results of risk assessment from the viewpoint of mission assurance (including measures aimed at the Olympic and Paralympic games) ○ Promote "risk communication and consultation" and "monitoring and review," which are significant from the viewpoint of mission assurance
5. Enhancement of the basis for CIP	Basically keep the element of "[5] Enhancement of the basis for CIP" in the Third Policy	○ Continue review of the scope of information sharing within and outside the CI sectors ○ Positively provide information obtained from international conferences, etc. to stakeholders ○ Promote security by design ○ Make appeals to the management layer of CI operators ○ Assist human resources development (cooperation among government, industry and academia for specific human resources development)

II. Executive Summary of This Cybersecurity Policy

The key points for this Cybersecurity Policy ([i] Purpose of CIP, [ii] Basic principles, [iii] Responsibility of stakeholders, such as CI operators, government organizations, and cybersecurity related agencies, and in particular, [iv] Responsibility of top management) are as follows.

[i] Purpose of CIP

The purpose of CIP is to maintain safe and continuous provision of CI services, based on the concept of mission assurance, by preventing serious impact on national life and socioeconomic activities caused by any CISs outages resulting from cyberattacks, natural disasters or other causes to the extent possible and ensuring prompt recovery from outages.

[ii] Basic concept

In the first place, CI operators should implement cybersecurity measures on their own responsibility, but collaborative efforts among stakeholders are indispensable on the basis of mission assurance for all CIs. Therefore, the purpose of CIP should be achieved through all-out efforts by diverse stakeholders, thereby nurturing a sense of security among the general public, promoting social growth and resilience, and strengthening international competitiveness.

- CI operators should respectively take measures and make efforts for continuous improvement of those measures as entities providing services and bearing social responsibilities.
- Government organizations should provide necessary support for cybersecurity measures of CI operators.
- Each CI operator should cooperate and coordinate with other stakeholders due to the limit of each operator's individual cybersecurity measures to address various threats.

[iii] Responsibility of stakeholders

- All stakeholders should periodically check the progress of their own measures and policies as part of relevant efforts and accurately recognize the current circumstances, and proactively determine the goals of relevant activities. In addition, stakeholders should enhance their cooperation with each other, taking into account the status of other stakeholders' relevant activities.
- All stakeholders should understand the 5W1H (when, where, who, why, what and how) of responses to CISs outages depending on the scale thereof and should be able to calmly address signs or occurrence of any CISs outages. They should also be capable to cooperate with other stakeholders and respond in a cooperative and concerted manner in addition to ensuring robust communication among various stakeholders and taking proactive measures.

[iv] Responsibility of top management

In addition to the above, top management should understand the necessity of the following matters and take relevant measures.

- Recognize their responsibility for ensuring cybersecurity and exert their leadership in cybersecurity measures from the viewpoint of mission assurance
- With the awareness that their individual efforts also contribute to the development of society as a whole, take cybersecurity measures while involving their supply chains (business partners, subsidiaries and affiliated companies, etc.)
- Develop incident readiness even in normal times and disclose information on responses properly in the event of an incident from the perspective of gaining trust and nurturing a sense of security among stakeholders
- Constantly secure management resources, such as budgets, structure and personnel, necessary for the abovementioned measures and appropriately allocate them from a risk-based perspective

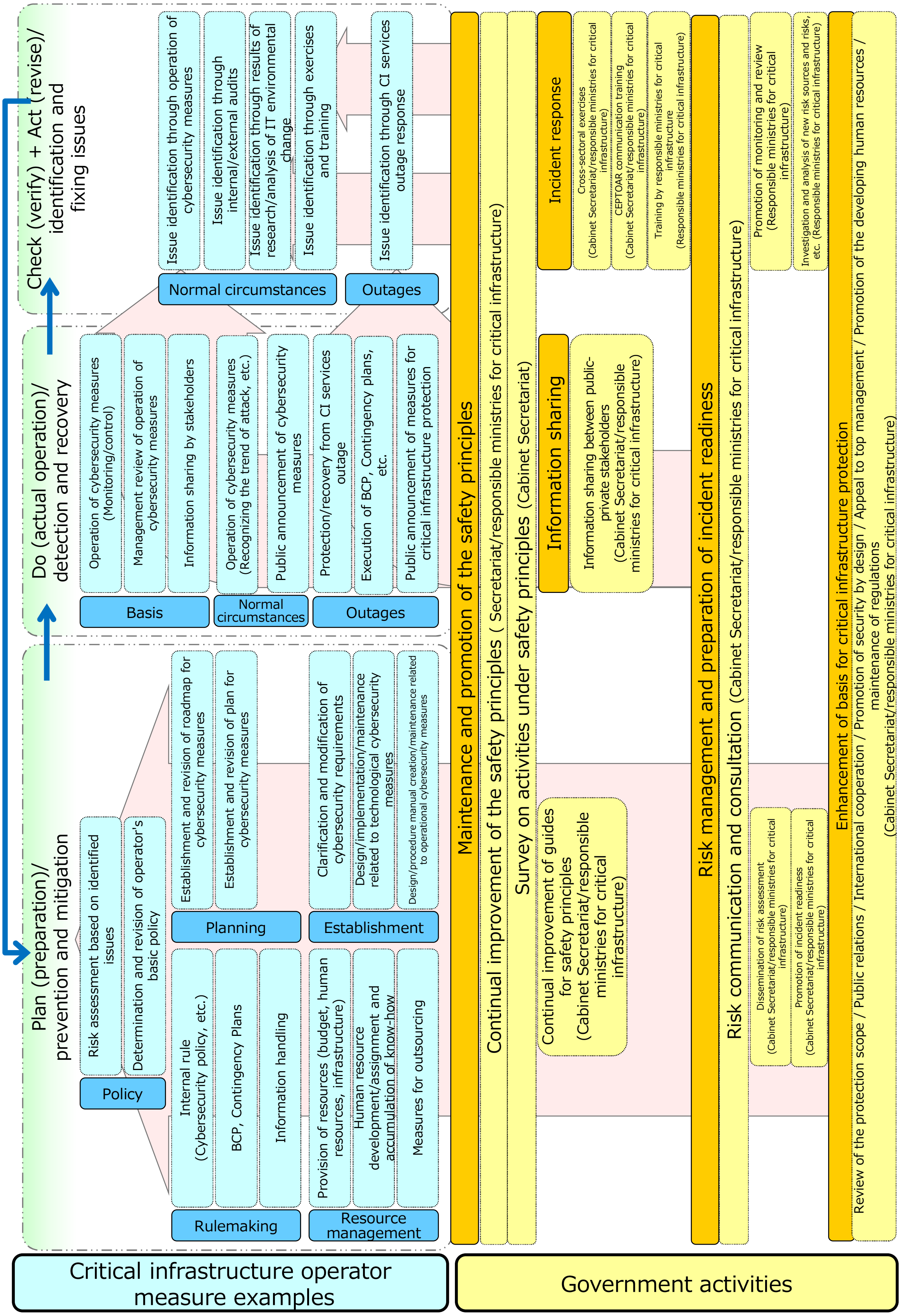

Plan (preparation)/ prevention and mitigation
Policy
Risk assessment based on identified issues
Determination and revision of operator's basic policy
Rulemaking
Internal rule (Cybersecurity policy, etc.)
BCP, Contingency Plans
Information handling
Planning
Establishment and revision of roadmap for cybersecurity measures
Establishment and revision of plan for cybersecurity measures
Resource management
Provision of resources (budget, human resources, infrastructure)
Human resource development/assignment and accumulation of know-how
Measures for outsourcing
Establishment
Clarification and modification of cybersecurity requirements
Design/implementation/maintenance related to technological cybersecurity measures
Design/procedure manual creation/maintenance related to operational cybersecurity measures
Do (actual operation)/ detection and recovery
Basis
Operation of cybersecurity measures (Monitoring/control)
Management review of operation of cybersecurity measures
Information sharing by stakeholders
Normal circumstances
Operation of cybersecurity measures (Recognizing the trend of attack, etc.)
Public announcement of cybersecurity measures
Outages
Protection/recovery from CI services outage
Execution of BCP, Contingency plans, etc.
Public announcement of measures for critical infrastructure protection
Check (verify) + Act (revise)/ identification and fixing issues
Normal circumstances
Issue identification through operation of cybersecurity measures
Issue identification through internal/external audits
Issue identification through results of research/analysis of IT environmental change
Issue identification through exercises and training
Outages
Issue identification through CI services outage response
Maintenance and promotion of the safety principles
Continual improvement of the safety principles (Secretariat/responsible ministries for critical infrastructure)
Survey on activities under safety principles (Cabinet Secretariat)
Continual improvement of guides for safety principles (Cabinet Secretariat/responsible ministries for critical infrastructure)
Information sharing
Information sharing between public-private stakeholders (Cabinet Secretariat/responsible ministries for critical infrastructure)
Incident response
Cross-sectoral exercises (Cabinet Secretariat/responsible ministries for critical infrastructure)
CEPTOAR communication training (Cabinet Secretariat/responsible ministries for critical infrastructure)
Training by responsible ministries for critical infrastructure (Responsible ministries for critical infrastructure)
Risk management and preparation of incident readiness
Risk communication and consultation (Cabinet Secretariat/responsible ministries for critical infrastructure)
Dissemination of risk assessment (Cabinet Secretariat/responsible ministries for critical infrastructure)
Promotion of incident readiness (Cabinet Secretariat/responsible ministries for critical infrastructure)
Promotion of monitoring and review (Responsible ministries for critical infrastructure)
Investigation and analysis of new risk sources and risks, etc. (Responsible ministries for critical infrastructure)
Enhancement of basis for critical infrastructure protection
Review of the protection scope / Public relations / International cooperation / Promotion of security by design / Appeal to top management / Promotion of the developing human resources / maintenance of regulations (Cabinet Secretariat/responsible ministries for critical infrastructure)
Critical infrastructure operator measure examples
Government activities

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

III. Policies for CIP

1. Maintenance and Promotion of the Safety Principles

Cybersecurity measures commonly required in all sectors were compiled as the Guidelines for Safety Principles for Ensuring CI Security and revisions have been made as necessary. In line with the Guidelines, all CI sector guidelines and internal policies, etc. of respective CI operators are now being reviewed, and the safety principles as a whole are being developed in this manner.

The safety principles have been disseminating among CI operators as the rules on cybersecurity measures, which further encourages efforts necessary for ensuring safe and continuous provision of CI services.

During the term of this Cybersecurity Policy, the Cabinet Secretariat carries out the review of the Guidelines and continual improvement of the safety principles, and surveys their promotion status in order to maintain and enhance CIP capability.

Also, CI operators continuously and steadily work on cybersecurity measures in accordance with their PDCA cycle, in view of the importance thereof.

1.1 Continual improvement of the Guidelines for Safety Principles

The Cabinet Secretariat carries out the review of the main section and measures section of the Guidelines for safety principles as well as the manual (the "Manual for Prioritization of Information Security Measures") with the aim of maintaining and enhancing CIP capability, especially measures related to top management, development of incident readiness including formulation of contingency plans, and measures integrating not only IT but also OT.

Specifically, responsibility of top management is clarified to require them to take the initiative in the formation of cybersecurity culture and the implementation of the PDCA cycle in carrying out cybersecurity measures by the use of the "Cybersecurity Management Guidelines," etc. The reviewed Guidelines additionally describe the necessity of preparation of incident readiness through the establishment of BCPs and contingency plans based on the concept of mission assurance and efforts for ensuring cybersecurity, which is indispensable for properly responding to IT, as a basic factor for internal control (such as internal audits and penetration tests).

The significance of developing a cross-sectoral organization consisting of a unit responsible for IT and a unit responsible for OT and nurturing personnel required therefor is also emphasized for the purpose of promptly responding to threats of cyberattacks to control systems of plants and factories, in addition to the need to formulate a Computer Security Incident Response Team (CSIRT[3]).

Furthermore, as a part of the efforts for information sharing, the implementation of case studies concerning past incident responses is presented as a recommendation so that respective CI operators surely reflect other operators' experience of response to CISs outages in their future cybersecurity measures.

[3] Computer Security Incident Response Team: A mechanism to monitor information systems for information security problems, and analyze the causes and investigate affected areas, etc. if any problem is detected

The main section, measures section, and manual are to be reviewed once every three years in principle, but this does not apply when any significant changes beyond expectations occur in social trends, etc. In particular, looking toward the Olympic and Paralympic games in 2020, reviews are to be conducted on a timely basis.

1.2 Continual improvement of the safety principles

CI operators and responsible ministries for CI continually improve the safety principles based on knowledge learned from experiences of each CI operators' incident responses in order to maintain and enhance the protective capability of CI as a whole.

In detail, they make continual improvement of the safety principles through risk assessment, by identifying issues from operation of cybersecurity measures, 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 as well as social trend changes and new knowledge released by the Cabinet Secretariat are to be used.

Additionally, the Cabinet Secretariat and responsible ministries for CI continue efforts for appropriately improving institutional frameworks as necessary for maintaining safety, by means such as through positioning cybersecurity measures as safety regulations among relevant laws and embodying the service maintenance level in relevant laws so that appropriate cybersecurity measures are surely taken from the viewpoint of mission assurance.

The Cabinet Secretariat carries out survey on the improvement of the safety principles by the responsible ministries for CI each fiscal year and releases the results thereof.

1.3 Promotion of the safety principles

The Cabinet Secretariat conducts a questionnaire survey and visits to CI operators every year for the purpose of examining their concrete measures and further accurately ascertaining how the safety principles have been promoted among CI operators. Survey items are to be reviewed as needed to better promote the safety principles and improve CI operators' activities.

Specifically, survey items that enable more detailed and accurate understanding of the current status and survey items for ascertaining the level of reaching the envisaged future are to be added. Furthermore, questionnaires are designed to enable CI operators to conduct a self-check and ascertain their own achievement levels, issues and solutions through responding to questions.

Visits to CI operators are also conducted with the aim of verifying hypotheses formed on the results of the questionnaire survey and collecting best practices.

Results of these questionnaire survey and visits are released every fiscal year, in principle, and are utilized for the improvements of measures under this Cybersecurity Policy.

2. 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 attackers and resulting prompt countermeasures by a larger number of CI operators contribute not only to minimizing damage caused by the relevant attack but also to deterring further cyberattacks.

Given such backdrop, efforts for smoother information sharing have been made under former Cybersecurity Policies and a certain outcome is observed in activated information sharing in some sectors, but information sharing among the entirety of the CI is not necessarily sufficient yet. Therefore, 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.

The Japanese government basically considers that CI operators should assume the primary responsibility for cybersecurity measures and should mutually cooperate with other stakeholders voluntarily. Accordingly, the Cabinet Secretariat preferentially makes efforts to develop an environment to enable the public and private sectors to easily share information in a cross-sectoral manner.

2.1 Information sharing system during the term of this Cybersecurity Policy

As many big international events, such as the Olympic and Paralympic games, are scheduled to be held in Japan, cyberattacks against CI are expected to be increased qualitatively and quantitatively and it is urgently necessary to develop an information sharing system among relevant entities promptly. The information sharing system built under the Third Policy has become fully rooted among stakeholders and therefore should be further developed and disseminated. The Cabinet Secretariat will consider means for improving the information sharing system and formulating new schemes as follows to enable CI operators to positively utilize shared information in their risk management and incident responses.

Under the former information sharing system, CI operators were supposed to submit information to the Cabinet Secretariat via responsible ministries and this partially hindered activation of information sharing as CI operators were afraid of being subject to disciplinary guidance by government organizations as a result of reporting signs of incidents, *Hiyari-Hatto* events or system failures, for which reporting is not required under relevant laws. Therefore, this information sharing system is to be revised to newly introduce, in addition to the conventional means to have CI operators directly make reports to responsible ministries, a new route for information sharing via the CEPTOAR secretariat, which enables data anonymization, regarding events for which reporting is not required under relevant laws. CI operators will be able to 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 will come to be gathered in each CEPTOAR secretariat and functions of CEPTOARs will be strengthened as each CEPTOAR will become able to spread gathered information promptly within each sector as necessary.

Furthermore, the information sharing system will be developed to allow the opening of a hotline between the Cabinet Secretariat and CI operators in an emergency to achieve prompt and efficient information sharing on cyberattacks, 24 hours a day, 365 days a year.

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.

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.

Given these, the information sharing system during the term of this Cybersecurity Policy is represented in "ANNEX 4-1. INFORMATION SHARING SYSTEM" and the roles of individual stakeholders are in "ANNEX 4-2. RESPONSIBILITIES OF EACH STAKEHOLDER". Diversification of reporting routes will be promoted on a trial basis even before the introduction of the new information sharing system. 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 CI SERVICE OUTAGE EXAMPLES."

The abovementioned measures are steadily promoted and construction of a system to share information with stakeholders will be developed while CISs outages and threat 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 threat to cybersecurity covering multiple sectors, such as IoT.

2.2 Further promotion of information sharing

The Cabinet Secretariat continuously reviews the protection scope of CI (including the expansion of the scope of information sharing) in light of changes in the social and technological environment and interdependency among CI sectors, while clarifying information to be shared among CI operators, in order to further activate information sharing during the term of this Cybersecurity Policy.

Information to be shared is defined, as in the Third Policy, to be "information concerning system failures, including CISs outages, signs and *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". However, as affected areas and concrete actions differ depending on the seriousness of CISs outages and the significance of related information, this Cybersecurity Policy cites examples of the severity schema on CISs outages in the ATTACHMENT and the Cabinet Secretariat considers materialization of such criteria for the purpose of promoting awareness sharing among stakeholders and ensuring prompt and effective information sharing. Through these efforts, the Cabinet Secretariat works on promoting effective information sharing among stakeholders based on concrete criteria with regard to information on cyberattacks, etc. that are highly likely to have an expansive influence within and outside the relevant sector. In addition, considering the recent trend that cyberattacks have come to target control systems, which used to be considered closed and safe, this Cybersecurity Policy clearly states that attacks to control systems, including IoT systems that are expected to be further disseminated in the future, are also included in the information to be shared.

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 under the reviewed information sharing system. When any change occurs in the environment, the system is to be reviewed as needed.

Review of the protection scope of CI is also continued in order to achieve "protection as plane" covering a broader area for the purpose of ensuring safe and continuous provision of CI services (refer to 5.1(1) below for details).

2.3 Promotion of CI operators' activities

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

In particular, CI operators should proactively work towards their own information sharing activities, in addition to constructing and enhancing CISs outage response structure, such as CSIRT. CEPTOARs are also expected to continue sharing information provided by the Cabinet Secretariat as during the term of the Third Policy, 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 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. ISACs have already been organized in some sectors that are carrying out leading activities, 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 will contribute to further activating information sharing among CI operators and their further positive activities for cybersecurity measures.

Additionally, expansion of internal and external information sharing should be maintained through the expansion of constituent members of respective CEPTOARs and establishment of new CEPTOARs. Qualitative and quantitative improvements are expected for sharing information handled by CI operators, covering not only IT but also OT, for the purpose of ensuring collaboration with domestic and foreign diverse entities, and safe and continuous provision of CI services.

[4] PoC: Point of Contact

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.

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

3. Enhancement of Incident Response Capability

During the term of this Cybersecurity Policy, efforts for comprehensively strengthening the CISs outage response structure are continued based on the achievement of various exercises and training that have been conducted under the Third Policy for the purpose of improvement and verification of incident response capability.

Cross-sectoral exercises are further improved, while maintaining the current mechanism incorporating CI operators' needs, as core means of strengthening the incident response system in CI sectors, by reviewing and revising exercise scenarios in consideration of the latest attack techniques. More specifically, cross-sectoral exercises will be improved so that they better fit the actual state of CI operators' incident handling and internal rules. Furthermore, cross-sectoral exercises should be mutually linked and complement CEPTOAR training and other exercises and training implemented by responsible ministries for CI, and the vertical-directional systems within each CI sector and the horizontal-directional systems between CI sectors should be enhanced to reap synergistic benefits.

3.1 Improvement of cross-sectoral exercises

During the term of this Cybersecurity Policy, the Cabinet Secretariat continues to implement cross-sectoral exercises, which are initiatives unique to Japan bringing together all CI operators, while constantly improving them in order to contribute to the maintenance and improvement of CIP capability through the dissemination of the results of the exercises to overall CI sector.

In this process, accumulated operation methods and outcome should be fully utilized to enhance the content of the exercises so that these cross-sectoral exercises surely contribute to strengthening the incident response system.

3.1.1 Qualitative improvement in planning cross-sectoral exercises

During the term of this Cybersecurity Policy, the Cabinet Secretariat positively takes measures to ensure that the exercises incorporate knowledge and issues obtained through exercise operation in the past, issues revealed in other policies and exercises conducted by other organizations, as well as the latest trends related to risk sources which may cause CISs outages, with the aim of continually improving cross-sectoral exercises. 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.

The Cabinet Secretariat also continues improving exercise processes in order to contribute to the further enhancement of verification related to CI operators' cybersecurity measures, CISs outage early recovery process and IT-BCP.

Additionally, the Cabinet Secretariat provides knowledge and issues obtained through these exercises as reference data for other policies in this Cybersecurity Policy.

3.1.2 Promotion of lessons learned from cross-sectoral exercises

During the term of the Third Policy, the number of exercise participants increased significantly, and the percentage of participants who assessed the exercises as meaningful exceeded 80%. This Cybersecurity Policy continuously aims to disseminate exercise results in CI sectors through encouraging participation of individuals who had not yet participated in the exercises. However, as there is a certain limitation on participation increase, it is necessary, in addition to encouraging new participation, to nurture human resources so that exercise participants can voluntarily hold individual exercises in their companies or in the relevant sector that are carried out based on know-how of cross-sectoral exercises, in order to further propagate and promote exercise results to overall CI.

For this activity, the Cabinet Secretariat creates and releases explanation materials regarding the merits of exercises, thereby increasing understanding and encouraging active participation of top management in overall CI sectors to promote implementation of exercises in each CI sector and at each CI operator.

In addition, the Cabinet Secretariat works to provide a virtual exercise environment with the aim of developing and sharing implementation, assessment and advising methods accumulated from past exercises in order to contribute to the support of exercise implementation by individual CI operators.

3.1.3 Cooperation with responsible ministries for CI

Although expected effects differ between exercises and training for CIP conducted by responsible ministries and cross-sectoral exercises conducted by the Cabinet Secretariat, carrying out these exercises in a manner to cooperate with and complement each other is expected to contribute to efficient and effective maintenance and enhancement of CIP capability.

For this reason, the Cabinet Secretariat and responsible ministries for CI positively work on materializing ideal mutual cooperation and clarifying verification purposes and the main targets for each exercise in order to surely improve CI operators' incident response capability.

Additionally, in collaboration with private organizations, such as ISACs, that have already been established in some CI sectors, the Cabinet Secretariat will make it clear what exercises are truly effective for participating operators and ideal means for information cooperation.

Various factors including physical obstruction need to be considered in responding to CISs outages and there is a possibility that information may need to be shared not only among responsible ministries for CI and CI operators' cybersecurity departments but also with disaster prevention and risk management departments. Therefore, collaboration with such other departments should also be sought as necessary, based on stakeholders' needs.

3.2 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 provision of customized simulation information on characteristics of each sector and on latest attack trends also with the aim of calling for attention, implementation of unannounced training in all CEPTOARs, and verification of emergency systems and means for communication. In this manner, CEPTOAR communication training better fitting the actual state is to be sought.

4. Risk Management and Preparation of Incident Readiness

Cases of personal information leakage caused by cyberattacks or information system failures and economic loss due to suspension of CI services have come to be frequently reported along with the increase in ICT utilization. Damage to the real world is becoming more and more serious. It is necessary to note that highly sophisticated cyberattacks, such as zero-day attacks targeting undisclosed vulnerability, and internal fraud "can no longer be prevented completely in advance."

Under such circumstances, CI operators should inevitably position preparedness for cybersecurity risks in their business strategy and strategically take risk response measures based on the results of risk assessment. From the viewpoint of mission assurance, they need to put in place appropriate risk assessment-based incident readiness to ensure safe and continuous provision of CI services even in the event of a cyberattack, etc. It is also important for them to build a mechanism under which these activities as a whole (risk management) function sustainably and effectively.[6]

In order to prioritize measures to be taken by CI operators based on the concept of mission assurance, this Cybersecurity Policy expansively positions the key policy "risk management" under the Third Policy as "risk management and preparation of incident readiness," and newly introduces measures for supporting CI operators' initiatives for strengthening internal control to enable proper decision making based on risk assessment and their voluntary and autonomous efforts for preparing incident readiness for business continuity, while maintaining measures for risk management under the Third Policy.

4.1 Basic view of risk management

Risk management should be independently implemented by each CI operator. However, in circumstances where information sharing and discussions based on common risk management views or terms are not observed among stakeholders, there is a possibility that the activities in this Cybersecurity Policy will not be effectively utilized in the risk management of each CI operator.

For this reason, it is preferable for each stakeholder to utilize the internationally standard views of risk management and related terminology definitions for cybersecurity etc. In details, views based on the framework shown in Table 3 below and the terminology definitions used therein should be adopted to the extent possible in concrete activities and related materials.

[6] From the viewpoint of mission assurance, CI operators should conduct risk assessment to comprehensively ascertain impacts on the provision of CI services, taking into account not only the influence of system failures directly relating to CI services but also spillover effects of indirectly related system failures.

Table 3 Standard Risk Management Process (example)

Risk management		
	Establishing the context of organization	
	Risk assessment	
		Risk identification
		Risk analysis
		Risk assessment
	Risk treatment	
	Risk acceptance	
	Risk communication and consultation	
	Monitoring and review	

4.2 Promotion of risk management

Risk management should basically be optimized by each CI operator individually to suit their organization. The significance of risk assessment seems to have been widely recognized by many CI operators as suggested by the fact that an increasing number of CI operators mention the implementation of risk assessment in cybersecurity basic policies they voluntarily establish. On the other hand, some CI operators, despite being aware of the significance, have yet to conduct risk assessment due to such reasons as the lack of knowledge on concrete measures. The concept and implementation methods of risk assessment have not been necessarily disseminated sufficiently. It is also true that some activities, such as cross-sectoral study/analysis and opinion exchanges, are not easily carried out solely within individual CI operators.

Therefore, the Cabinet Secretariat takes the following measures to promote risk management of CI operators.

4.2.1 Dissemination of risk assessment

It is necessary to maintain safe and continuous provision of CI services, which are fulfilling indispensable roles and functions in socioeconomic systems. Accordingly, what should be prioritized is the concept of mission assurance, under which CI operators fulfill expected roles and functions and conduct risk assessment for the purpose of ensuring safety of CI services they provide and continue providing services by preventing suspension or quality loss unacceptable for themselves and other stakeholders to the extent possible, and promote risk countermeasures under top management's comprehensive judgement based on the results of risk assessment, thereby aiming to achieve their goals.

Given these, the Cabinet Secretariat endeavors to encourage more and more CI operators to conduct risk assessment based on the concept of mission assurance. Concrete activities are as follows.

(i) Disseminate the purpose and methods of risk assessment based on the concept of mission assurance widely among relevant entities by encouraging them to refer to the Risk Assessment Guidelines for Mission Assurance[7] in risk assessment looking toward the Olympic and Paralympic games, and also promote such risk assessment at related briefing sessions and lectures

[7] Guidelines established by the Cabinet Secretariat in September 2016, targeting providers of CI services that may exert significant influence on the operation of the Olympic and Paralympic games

(ii) Generalize the Risk Assessment Guidelines for Mission Assurance so that they can be utilized by CI operators in their risk assessment also in normal times and improve the Manual for Prioritization of Information Security Measures, thereby further disseminating the purpose and methods of risk assessment based on the concept of mission assurance widely among CI operators

Through these activities, it is expected that individual CI operators' risk assessment will achieve a certain standard and a certain level of accuracy in the future.

4.2.2 Investigation and analysis of new risk sources and risks, etc.

In light of changes in the environment surrounding CI sectors, the Cabinet Secretariat conducts surveys on the current status and trends of major facilities and technologies from the perspective of cybersecurity, and analyses new risk sources inherent to such facilities and technologies and risks arising therefrom (hereinafter referred to as "new risk sources and risks").

Additionally, the Cabinet Secretariat continues analysis of spillover effects of CISs outages. In detail, the following activities are carried out, also taking into account viewpoints of the efficiency of each study/analysis and mutual reflection with other policies, and the results of the studies/analyses are provided to CI operators and are also utilized for improving measures under this Cybersecurity Policy.

(1) Environmental change studies

The Cabinet Secretariat carries out current status studies on environmental changes including analyses of new risk sources and risks, targeting IoT, FinTech, and other new technologies and systems expected to spread in CI sectors in the medium- and long-term, as well as institutions 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. New risk sources and risks that are common only across specific sectors, such as control systems or information systems, but could have a significant influence if not on all sectors will also be targeted.

When any new risk sources and risks are identified through these studies and analyses or any new CI sectors are newly targeted, analysis of commonality across these sectors are to be carried out as a detailed investigation, as necessary.

(2) Interdependency analysis

As utilization of ICT continues to develop in each CI sector and interdependent relationships among CI sectors and with other sectors continue to grow, the understanding of interdependency in CI sectors becomes more and more important for conducting risk assessment and taking effective recovery measures in the event of CISs outages.

For this reason, in this Cybersecurity Policy, the Cabinet Secretariat continuously carries out interdependency analysis, and also conducts restudy or reanalysis based on the results of the analyses under preceding Cybersecurity Policies if there are any changes in interdependency due to environmental changes or addition of new CI sectors.

In addition, as the degree of IT dependency in CI sectors is closely related to interdependency analysis, detailed IT dependency studies are also periodically implemented.

If any new CI sectors are added, IT dependency studies will also be carried out along with interdependency analysis.

4.2.3 Promotion of incident readiness

For mission assurance, in the event of CISs outages, CI operators are required to ensure the safety of affected CI services and restore them to an acceptable level within an acceptable period of time. Therefore, CI operators need to develop incident readiness in preparation for CISs outages.

Given these, the Cabinet Secretariat promotes preparation of incident readiness by CI operators. Additionally, looking toward the Olympic and Paralympic games, the Cabinet Secretariat also promotes preparation of incident readiness by related parties. Concrete activities are as follows.

(i) Promote CI operators' formulation of BCPs and contingency plans based on the concept of mission assurance, and establishment of organizational structures for implementing them; In order to avoid risks caused by a failure to implement BCPs and contingency plans as planned, also promote activities to give education and exercises for assuring and verifying the effectiveness of these plans

(ii) Build a core organization responsible for the sharing of incident information among stakeholders ahead of the Olympic and Paralympic games (the "Olympic and Paralympic CSIRT (provisional title)"), and utilize knowledge obtained in the process of developing this organization, such as through the clarification of responsibilities of the government and stakeholders, as a legacy in carrying out activities mentioned in (i) above

Contingency plans in this Cybersecurity Policy refer to plans formulated in advance with regard to policies, procedures, preparations, 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, and the intended purpose is to minimize influence of CISs outages through proper actions based thereon. Initial responses (emergency responses) include suspension of CI services for ensuring safety based on the nature of the respective CI and the results of risk assessment. BCPs refer to plans formulated in advance with regard to the CI service restoration levels, priorities, and other policies, procedures, preparations, etc. so as to ensure that CI operators can restore CI services affected by CISs outages to an acceptable level within an acceptable period of time from the viewpoint of mission assurance.

4.2.4 Promotion of risk communication and consultation

Risk communication and consultation is defined as a "continual and iterative process that an organization conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risks."[8] This process is necessary from the viewpoint of mission assurance for each organization in setting their purpose regarding CI services to be indicated as the maintenance level of their services and in making decisions regarding both risks facing such purpose and their risk management. In the coming interconnected and converged information society, this process is also important in consensus building between CI operators and stakeholders regarding the division of roles and responsibilities concerning risks and CI operators' fulfilment of their expected responsibilities in providing CI services.

[8] JIS Q 31000:2010

The Cabinet Secretariat promotes risk communication and consultation implemented by stakeholders related to CI protection with the aim of encouraging information and opinion exchanges among internal stakeholders and also contributing to the development of cross-sectoral information and opinion exchanges. Concrete activities are as follows.

(i) Promote risk communication and consultation among top management, cybersecurity departments, departments responsible for information systems and control systems, user departments, and other internal stakeholders

(ii) Utilize the CEPTOAR council and cross-sectoral exercises and promote enhancement of information and opinion exchanges in cooperation with diverse stakeholders, and collect information necessary for studies and analyses of new risk sources and risks

4.2.5 Promotion of monitoring and review

The status ascertained as a result of risk assessment is expected to change over time. In order to identify any circumstances or other factors that may change or invalidate risk assessment results and properly respond to fluctuations in risks, it is necessary to create a mechanism to manage risks in an appropriate manner such as constantly monitoring and revising risk assessment results as needed or otherwise, and maintain risk management functions continuously and effectively.

Therefore, the Cabinet Secretariat promotes CI operators' monitoring and review of their risk management and incident readiness. More specifically, the Cabinet Secretariat provides key points for audits compiled based on the viewpoint of mission assurance to assist CI operators' voluntary internal audits, etc., thereby promoting their monitoring and review.

4.3 Establishment of a process of synergizing the relevant policies

The Cabinet Secretariat utilizes the results of studies and analyses of the abovementioned measures in activities under other key policies as reference data for the purpose of contributing to other policies in this Cybersecurity Policy.

In addition, the Cabinet Secretariat conducts studies and analyses as necessary regarding new risk sources and risks requiring cross-sectoral measures that are revealed as a result of implementing other policies.

5. Enhancement of the Basis for CIP

As the social and technological environment surrounding CI continue to constantly change, it is necessary to raise public awareness about cybersecurity and create shared awareness through making appeals to the top management of CI operators, etc. in order to enhance the level of cybersecurity of the whole nation.

As shown in Figure "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 cybersecurity measures and identification of issues for new risks and risk sources resulting from IT related environmental changes.

Therefore, during the term of this Cybersecurity Policy, the Cabinet Secretariat continues review of the scope of information sharing in and outside CI sectors as under the Third Policy, cooperates with other stakeholders in PR activities, international collaboration and awareness-raising activities targeting top management, and also prepares manuals on CIP-related regulations so that stakeholders can easily refer to appropriate regulations on a timely basis.

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 Review of the protection scope of CI

(1) Activities towards "protection as plane"

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 to cover a broader area for ensuring safe and continuous provision of CI services, while flexibly responding to changes in social environment.

(2) Activities from the perspective of securing national security

Threats of increased cyberattack damage and changes in the social and technological environment in recent years have increased the need of a security perspective in the protection of national life and socioeconomic activities. It is necessary to continuously review the scope of CI sectors in order to strengthen measures in sectors where information sharing should be promoted and properly protect services that should be newly positioned as CI services.

The Cabinet Secretariat has endeavored to ascertain the current status through hearings, etc. with stakeholders, and will continue the review of the protection scope of CI, not limited to the conventional CI sectors, in light of changes in the social environment. The review covers companies significant for ensuring security,[9] companies holding advanced technology and other intellectual property or business secrets important for strengthening Japan's international competitiveness, and other stakeholders whose cybersecurity measures need to be enhanced.

Regarding (1) and (2) above, measures for newly added sectors and businesses are to be enhanced by stages in accordance with their status.

5.2 Promotion of public relations activities

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 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, issuing newsletters and holding lectures, and also studies more effective PR channels.

As cybersecurity is subject to new threats and appropriate responses arising from environmental changes and technological innovation are required, it is necessary to collect information on new technologies and schema whose introduction is being discussed at an early stage and consider responses accordingly.

The Cabinet Secretariat ascertains the status of each sector and collects information on technology trends, etc. through visit surveys, workshops and seminars to reflect such latest conditions on policies as needed.

Additionally, the Cabinet Secretariat continues efforts to obtain understanding and cooperation of the top management of CI operators and related other businesses with the aim of further disseminating the concept of mission assurance and achieving "protection as plane."

5.3 Promotion of international cooperation

In cyberspace, risks have been growing in the borderless domain, and it is internationally required to further respond to these borderless risks and positively contribute to capacity building for the purpose of improving the international level of cybersecurity measures, not limited to the national levels.

[9] Including companies for which physical protection of nuclear materials or other measures are required

Therefore, the Cabinet Secretariat cooperates with responsible ministries for CI and the cybersecurity related agencies and continues to enhance international cooperation by communicating Japan's initiatives through active utilization of bilateral, inter-regional and multilateral frameworks.

Specifically, the Cabinet Secretariat actively introduces Japan's unique initiatives such as cross-sectoral exercises through talks and speeches using frameworks with the US and Europe, ASEAN and Meridian, thereby strengthening international cooperation. Such cooperative relationships serve as the basis for information sharing concerning 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.

In addition, CI operators are also expected to make efforts for 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.

5.4 Promotion of security by design

The Cabinet Secretariat promotes the concept of security by design, which means to prioritize security from the stage of system planning and designing, as a common value among stakeholders. CI operators should promote use of products certified under a third-party certification system in compliance with international standards when procuring and operating control systems and related equipment based on the concept of security by design.

5.5 Appeal to top management

As observed in the Cybersecurity Management Guidelines and the Basic Approach to Cybersecurity for Corporate Management, cybersecurity measures have come to be emphasized as significant managerial issues. Top management of CI operators is expected to properly recognize the necessity and implement the following actions.

(i) Recognize top management's responsibility for ensuring cybersecurity and exert their leadership in cybersecurity measures from the viewpoint of mission assurance

(ii) With the awareness that their individual efforts also contribute to the development of society as a whole, take cybersecurity measures while involving their supply chains (business partners, subsidiaries and affiliated companies, etc.)

(iii) Develop incident readiness even in normal times and disclose information on responses properly in the event of an incident from the perspective of gaining trust and nurturing a sense of security among stakeholders

(iv) Constantly secure management resources, such as budgets, systems and personnel, necessary for the abovementioned measures and devise risk-based allocation thereof; For CI, whose systems are large in scale and whose lifecycles are relatively long, top management should responsibly secure and allocate management resources in a planned manner from the medium- and long-term perspective.

Given the above, the Cabinet Secretariat and responsible ministries for CI should encourage the top management of CI operators to develop awareness about CIP and endeavor to obtain knowledge through such activities to make critical infrastructure protection measures further fit the actual state and be more effective.

5.6 Promotion of the development of human resources

Each stakeholder should promote efforts based on the Comprehensive Policies for the Development of Cybersecurity Experts (Cybersecurity Strategic Headquarters resolution in March 2016) and carry out concrete activities based on the Cybersecurity Experts Development Program (Cybersecurity Strategic Headquarters resolution in April 2017). Concrete measures for human resources development are as follows.

(i) First raise awareness and promote understanding of the top management of CI operators, and then present cybersecurity measures based on each company's business policies and foster personnel who can bridge CIP-related departments within the company to make comprehensive adjustments and lead working-level officials

(ii) Considering the latest circumstances where cybersecurity measures are required for OT management departments and legal affairs departments, etc., not only for directly related IT management departments, promote the construction of an organizational structure that enables cross-sectoral collaboration of personnel with diverse roles and abilities in carrying out cybersecurity measures

(iii) In industry-academia-government collaboration, clarify the definition of required security experts and promote concrete human development measures, such as providing exercises and training, and qualification acquisition.

5.7 Ensuring Security in relation to the My Number System

In order to ensure cybersecurity regarding local governments and CI operators that handle people's individual numbers under the My Number System, government organizations offer necessary support and consider required measures, while CI operators handling individual numbers should make required efforts to ensure cybersecurity.

5.8 Maintenance of reference of standards and guides

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. Additionally, ahead of the Olympic and Paralympic games, risk assessment guidelines, etc. also need to be prepared. The initiatives of the Cabinet Secretariat related to the preparation of these regulations etc. are as follows.

(1) Issuance of the reference book for CIP

The Cabinet Secretariat compiles relevant documents including the Cybersecurity Strategy and this Cybersecurity Policy for common reference by stakeholders, and issues the compiled documents as the "Collection of Regulations Related to Information Security Measures" for the purpose of equalizing the knowledge base of stakeholders involved in CIP.

(2) Systematic visualization of relevant standards and guides for CIP

Regarding related regulations for CIP, the Cabinet Secretariat, with the cooperation of other stakeholders, surveys and compiles domestic and overseas regulations and clearly discloses the results so that appropriate versions of such regulations can be referred to as needed.

IV. Activities Taken by Stakeholders

1. Activities by the Cabinet Secretariat

(1) 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) Implement studies on changes in social trends and newly obtained knowledge as necessary, 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 CI 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; Continue efforts, together with responsible ministries for CI, for appropriately improving institutional frameworks, such as positioning cybersecurity measures as safety regulations among relevant laws as necessary for maintaining safety and embodying the service maintenance level in relevant laws for ensuring implementation of proper cybersecurity measures from the viewpoint of mission assurance

(v) Obtain cooperation of responsible ministries for CI and CI operators to implement studies every year on the conditions of the dissemination of the safety principles, and officially release the results

(vi) Utilize the results of the survey on the dissemination of the safety principles in improving activities under this Cybersecurity Policy

(2) 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 and risks in a cross-sectoral manner and secure resources necessary for the operation of the mechanism

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

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

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

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

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

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

(3) Enhancement of incident response capability

(i) Obtain information on other ministries' exercises and training for CISs outage responses and consider means for collaboration with other ministries

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

(iii) Plan cross-sectoral exercise scenarios, implementation methods and verification issues, etc. and implement cross-sectoral exercises

(iv) Study measures for improving cross-sectoral exercises

(v) On occasions of cross-sectoral exercises, ascertain conditions of risk analysis results verification, early recovery procedures implemented by CI operators during CISs outages, and IT-BCP etc. studies, and provide the results to exercise participants

(vi) Collect, accumulate and provide knowledge related to cross-sectoral exercise implementation methods, etc. (development of a virtual exercise environment, etc.)

(vii) Diffuse and spread knowledge related to CIP gained from cross-sectoral exercises

(viii)Promote individual human resources development as company-wide activities through encouraging implementation of exercise scenarios beyond duties and positions

(4) Risk management and preparation of incident readiness

(i) The following activities relating to risk assessment for the Olympic and Paralympic games

a. Provide the Risk Assessment Guidelines for Mission Assurance to entities conducting relevant risk assessment

b. Independently or jointly hold briefing sessions and lectures concerning risk assessment

(ii) Generalize the Risk Assessment Guidelines for Mission Assurance so that they can be utilized by CI operators in their risk assessment also in normal times and improve the Manual for Prioritization of Information Security Measures as necessary

(iii) Provide the results of the studies and analyses in this policy as data to be reflected in CI operators' risk assessment and development of the safety principles

(iv) Utilize the results of the studies and analyses in this policy as data to be reflected in other activities under this Cybersecurity Policy

(v) Offer support as necessary for promoting risk communication and consultation of CI operators among internal stakeholders

(vi) Support risk communication and consultation of CI operators via the CEPTOAR council and through cross-sectoral exercises

(vii) Offer support to CI operators such as through compiling and presenting points to be incorporated in BCPs and contingency plans and viewpoints for verifying their effectiveness based on the concept of mission assurance (viii)Build a core organization responsible for the sharing of incident information among stakeholders ahead of the Olympic and Paralympic games

(ix) Compile key points for audits concerning risk management and incident readiness and provide them to CI operators

(5) Enhancement of the basis for CIP

(i) 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 CI), in light of the necessity of "protection as plane" for mission assurance

(ii) Carry out PR activities through providing information on the website, issuing newsletters and holding lectures

(iii) Listen to public opinions through visit surveys, workshops and seminars

(iv) Enhance international cooperation through active utilization of bilateral, inter-regional and multilateral frameworks

(v) Actively provide case examples and best practices obtained through international cooperation to domestic stakeholders

(vi) In collaboration with responsible ministries for CI, make appeals to the top management of CI operators and obtain knowledge therefrom at the same time to utilize such knowledge in improving activities under this Cybersecurity Policy

(vii) Compile relevant documents for common reference by stakeholders and issue the compiled documents as a collection of regulations for the purpose of equalizing the knowledge base of stakeholders involved in CIP

(viii) Compile relevant regulations and make them visible

(ix) Encourage CI operators to use products certified under a third-party certification system

2. Activities by Responsible Ministries for CI

(1) 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; Continue efforts, together with the Cabinet Secretariat, for appropriately improving institutional frameworks as necessary for maintaining safety, by means such as through positioning cybersecurity measures as safety regulations among relevant laws and embodying the service maintenance level in relevant laws for ensuring implementation of proper cybersecurity measures from the viewpoint of mission assurance

(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 with a survey on the dissemination of the safety principles, etc.

(2) 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

(3) Enhancement of incident response capability

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

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

(iii) Participate in cross-sectoral exercises

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

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

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

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

(4) Risk management and preparation of incident readiness

(i) Cooperate with the Cabinet Secretariat, CI operators and other stakeholders in their risk assessment looking toward the Olympic and Paralympic games

(ii) Cooperate with the Cabinet Secretariat in disseminating the generalized Risk Assessment Guidelines for Mission Assurance and the improved Manual for Prioritization of Information Security Measures to CI operators and in otherwise promoting the dissemination of risk assessment

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

(iv) Utilize the results of the studies and analyses in concrete activities

(v) Support risk communication and consultation of CI operators

(vi) Offer support to CI operators as necessary for their efforts for developing incident preparedness and monitoring and review

(5) Enhancement of the basis for CIP

(i) Cooperate with the Cabinet Secretariat and enhance international cooperation through active utilization of bilateral, inter-regional and multilateral frameworks

(ii) Cooperate with the Cabinet Secretariat and actively provide domestic stakeholders with case examples, best practices and other items acquired through international cooperation

(iii) Cooperate with the Cabinet Secretariat and make appeals to the top management of CI operators

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

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

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

(vii) Encourage CI operators to use products certified under a third-party certification system

3. Activities by Cybersecurity Related Ministries

(1) 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. Activities by Crisis Management Ministries and Disaster Prevention Related Ministries

(1) 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.

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

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

(2) Enhancement of incident response capability

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

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

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

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

5. Voluntary Activities by CI Operators

(1) 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 environmental arrangement for packaging and implementing cybersecurity measures based on the safety principles

(iv) Identify issues from operation of cybersecurity measures, internal and external audits, environmental change studies/analysis results related to IT, exercises/training and response to CISs outages, and continually amend the safety principles through risk assessment

(v) Cooperate with the Cabinet Secretariat every year with a survey on the dissemination of the safety principles, etc.

(2) Enhancement of information sharing system

(i) Cooperate with the CEPTOAR council, CEPTOARs, responsible ministries for CI, 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) Rating of seriousness of cases involving IT and OT

(3) Enhancement of incident response capability

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

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

(iii) Participate in cross-sectoral exercises

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

(v) Utilize the results of cross-sectoral exercises for own procedures for early recovery in the event of ICSs outages and IT-BCP etc. as necessary

(4) Risk management and preparation of incident readiness

(i) When the relevant operator conducts risk assessment for the Olympic and Paralympic games, conduct said risk assessment and implement required responses based on the results thereof; Make necessary collaboration with the Cabinet Secretariat and other stakeholders, such as information sharing and opinion exchanges, in this process

(ii) Promote and strengthen risk assessment based on the concept of mission assurance; Ensure allocation of resources and develop own organizational structure required therefor

(iii) Utilize the reference information provided as the results of the studies and analyses in this policy in own risk assessment

(iv) Carry out the following for promoting and strengthening risk communication and consultation among stakeholders directly or indirectly involved in risk management in providing CI services

a. Enhance risk communication and consultation among top management, cybersecurity departments, departments responsible for information systems and control systems, user departments, and other internal stakeholders; Ensure allocation of resources and develop own organizational structure required therefor

b. Enhance risk communication and consultation among stakeholders by fully utilizing opportunities for information sharing, such as the CEPTOAR council and cross-sectoral exercises

(v) Propose environmental changes and risk sources which are difficult to analyze oneself but are worth studying and analyzing as targets for the studies and analyses in this policy

(vi) Participate in the discussion and examination of the studies and analyses in this policy

(vii) Carry out the following for developing incident readiness

a. Develop BCPs and contingency plans based on the concept of mission assurance, create an organizational structure for implementing these plans, and verify their effectiveness

b. When the relevant operator conducts risk assessment for the Olympic and Paralympic games, cooperate with stakeholders with relationships to the core organization responsible for incident information sharing (the "Olympic and Paralympic CSIRT (provisional title)")

(viii) Promote the strengthening of monitoring and review, such as the implementation of internal audits based on key points for audits provided by the Cabinet Secretariat (including audits voluntarily outsourced to external organizations)

(5) Enhancement of the basis for CIP

(i) 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

(ii) Understand the necessity of the matters indicated in "Responsibility of CI operators' executives and senior managers" and implement them

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

(iv) Consider the use of products certified under a third-party certification system for control systems and related equipment

(v) Secure and allocate management resources, such as budgets, systems and personnel, necessary for cybersecurity measures in a planned manner

6. Voluntary Activities by CEPTOARs and the CEPTOAR Secretariat

(1) Enhancement of information sharing system

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

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

(iii) Regarding reports from CI operators, provide them to responsible ministries for CI 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

(2) Enhancement of incident response capability

(i) Carry out periodic verification of information communication functions

(ii) Support CI operators' participation in cross-sectoral exercises and development of the results thereof

(iii) Participate in cross-sectoral exercises

(3) Risk management and preparation of incident readiness

(i) Support independent initiative of CI operators that make up own CEPTOAR; Cooperate with the Cabinet Secretariat, responsible ministries for CI, other CEPTOARs, etc. as necessary

(4) Enhancement of the basis for CIP

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

7. Voluntary Activities by the CEPTOAR Council

(1) 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) Enhancement of incident response capability

(i) Participate in cross-sectoral exercises as necessary

8. Voluntary Activities by Cybersecurity Related Agencies

(1) 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) Enhancement of incident response capability

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

(3) Risk management and preparation of incident readiness

(i) Support independent initiative of CI operators that make up CEPTOARs; Cooperate with the Cabinet Secretariat, responsible ministries for CI, etc. as necessary

(4) Enhancement of the basis for CIP

(i) Cooperate with the Cabinet Secretariat and enhance international cooperation through active utilization of bilateral, inter-regional and multilateral frameworks

(ii) Cooperate with the Cabinet Secretariat and actively provide case examples, best practices and other items acquired through international cooperation to domestic stakeholders

9. Voluntary Activities by Cyberspace-related Operators

(1) 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

V. 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 achievements during the term of this Cybersecurity Policy (goals of this Cybersecurity Policy) in the process of reaching the envisaged future (ultimate purpose of the Cybersecurity Policy) 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 using prescribed indicators 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 the goals 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 CI.

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. However, as the Olympic and Paralympic games are scheduled in 2020, this Cybersecurity Policy should be assessed on a timely basis. 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 Envisaged future

1.2.1 Outline of the envisaged future

The future images expected to be realized through the initiatives based on this Cybersecurity Policy are as follows.

○ Voluntary activities based on each stakeholder's awareness of their responsibilities are disseminated as their respective code of conduct and such behavior contributes to forming cybersecurity culture.

○ Stakeholders communicate with each other on a regular basis with the aim of strengthening measures in preparation for any CISs outages and are making improvements to their measures constantly in order to reflect experience concerning incident responses in their future efforts.

○ The fact that stakeholders are collaboratively making efforts for CIP is widely understood by the general public and this gives them peace of mind. Well-established communication among diverse stakeholders enables them to take calm responses in the event of CISs outage.

○ These efforts are publicized as the Cybersecurity Policy and are assessed regularly and revised properly as needed.

○ These efforts being made by stakeholders have become steadily rooted as measures contributing to the sustainable development of society.

1.2.2 Detailed future visions for respective stakeholders

(1) For all stakeholders

Detailed future visions common to all stakeholders are as follows.

○ Stakeholders possess accurate awareness of their own status and independently establish their own activity goals.

○ All required initiatives are progressing and periodic verification is carried out individually on the progress of one's own measures and policies. Stakeholders are also able to proactively cooperate with other stakeholders, while mutually maintaining an understanding of their activity conditions.

○ In responses during CISs outages, stakeholders understand who should collect what kinds of information, with whom they should share what kinds of information, and what they themselves should do in accordance with the scale of the CISs outages.

○ In addition to independent responses, stakeholders are able to carry out controlled responses in collaboration with other stakeholders as necessary.

(2) CI operators

Detailed future visions for CI operators are as follows.

○ The following matters related to cybersecurity governance are fully disseminated among CI operators.

—Cybersecurity measures are examined not just from information system construction and operation perspectives, but also from a business management perspective.

—CI operators have put in place a system that allows appropriate involvement of each of the parties responsible for system construction and operation and business management.

—CI operators understand what measures they themselves should implement in accordance with the CI services they should protect and their service maintenance level.

—CI operators are endeavoring to disclose information on their approach to cybersecurity measures during normal times and their responses upon occurrence of an incident.

—The attitude to share information as much as possible for enhancing the levels of cybersecurity measures is positively evaluated as a common value.

—CI operators share an awareness that the occurrence of CISs outages is not something to be hidden but something that should instead be shared among internal stakeholders involved in cybersecurity measures.

○ The following matters related to issue identification, risk assessment and improvement of measures are fully disseminated among CI operators.

—Based on this Cybersecurity Policy, stakeholders cooperate to carry out cybersecurity measures and are aware of remaining risks in their own measures and the extent of cybersecurity measures.

—Properly detecting changes in risk sources resulting from the development of various measures and environmental changes and changes in risks in relation to CISs outages, CI operators are voluntarily carrying out independent measures and making adjustments as necessary.

—CI operators have become able to take appropriate measures in preparation for CISs outages, and as a result, the risk of their serious impact on the national life and socioeconomic activities is minimized to the greatest degree possible.

—These initiatives serve as a driving force for the continued improvements of the measures.

○ The following matters related to information sharing are fully disseminated among CI operators.

—CI operators have information on conditions of the occurrence of CISs outages, and relevant information is shared with external stakeholders through each sector's CEPTOARs and CEPTOAR council as necessary. Official or unofficial cooperation is thus carried out.

(3) Cabinet Secretariat

Detailed future visions for the Cabinet Secretariat are as follows.

○ The Cabinet Secretariat fulfills a comprehensive coordination function for advancing more effective measures. Diverse information which contributes to cybersecurity measures has come to be accumulated at the Cabinet Secretariat through the key policies under this Cybersecurity Policy and cooperation with stakeholders based on relevant information is being mobilized.

○ The Cabinet Secretariat has obtained an understanding of risks related to serious risk sources and CISs outages, in particular. When it is difficult for CI operators alone to address such risks, organic cooperation and coordination for studying and implementing resolutions can promptly be organized.

1.3 Goals of this Cybersecurity Policy

Goals to be achieved during the term of this Cybersecurity Policy for realizing the envisaged future are as follows.

(1) Goals under the key policy "maintenance and promotion of the safety principles"

The outcome expected under this key policy is that stakeholders involved in cybersecurity measures understand what they themselves should do in accordance with the safety principles and steadily carry out required activities while periodically self-checking the achievements, and such behavior has been established as their code of conduct.

(2) Goals under the key policy "enhancement of information sharing system"

The outcome expected under this key policy is that CI operators can receive and utilize necessary information through enhancement of information sharing based on the latest information sharing system and information sharing to and from NISC, and strengthening of autonomous activities of each CEPTOAR.

(3) Goals under the key policy "enhancement of incident response capability"

The outcome expected under this key policy is that CI operators' incident response capability is enhanced through the participation in cross-sectoral exercises and other exercises and training, and resulting verification of the CISs outage early recovery process and IT-BCP, verification of the effectiveness of information sharing among stakeholders required therefor, and technological improvement of response capability.

(4) Goals under the key policy "risk management and preparation of incident readiness"

The outcome expected under this key policy is that CI operators have come to conduct risk assessment based on the concept of mission assurance in light of new risk sources and risks and have developed their incident readiness through promoting and enhancing their risk management measures, and the overall risk management including these processes functions sustainably and effectively.

(5) Goals under the key policy "enhancement of the basis for CIP"

The outcome expected under this key policy is as follows.

○ Efforts for reviewing the scope of protection are continued in light of the environmental changes and interdependence of sectors inside and outside CI, and activities are promoted in accordance with the conditions of respective operators.

○ PR activities aim to broaden the understanding of the general public and people other than stakeholders concerning the framework of the Cybersecurity Policy and are properly carried out in line with technological trends.

○ International cooperation, such as information exchanges and assistance and awareness-raising activities, is enhanced through active utilization of bilateral, inter-regional and multilateral frameworks.

○ Developed reference of standards and guides has disseminated and been fully utilized by CI operators.

1.4 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.

Supplementary studies aim to obtain materials for checking the validity of CI operators' initiatives based on this Cybersecurity Policy, such as issues of their cybersecurity measures and good practices, by way of following up samples of their concrete responses to CISs outages.

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 "III. Policies for CIP." Because all of the cybersecurity measures based on this Cybersecurity Policy are multilayered among multiple stakeholders, a wide variety of items can be imagined as indexes for use in verification. However, verification is to be conducted analytically after roughly classifying and setting both indexes to be used for verification of measures under this Cybersecurity Policy taken by CI operators and indexes to be used for verification of policies by government organizations. For the indexes for each measure for CIP policies under this Cybersecurity Policy, it is important to appropriately interpret the meaning of the values rather than to be overly-focused on the quantity or any fluctuations.

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 CI. 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 inappropriate to assess measures through comparison of CISs outage conditions for each CI operator or each sector. For this reason, it is reasonable to carry out assessment of measures based on self-assessment by CI operators, and each CI operator should work towards their own 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

Under key policies of this Cybersecurity Policy, the government offers support in order to improve the effectiveness of cybersecurity measures taken 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.

Detailed indexes are set as follows based on the "Goals of this Cybersecurity Policy" above.

(1) Indexes for the key policy "maintenance and promotion of the safety principles"

○ Ratio of CI operators carrying out cybersecurity measures, which serve as the baseline as ascertained through the survey of the dissemination of the safety principles

○ Ratio of CI operators carrying out leading cybersecurity measures as ascertained through the survey of the dissemination of the safety principles

(2) Indexes for the key policy "enhancement of information sharing system"

○ Number of cases of information sharing to and from NISC

○ Number of constituent members of each CEPTOAR

(3) Indexes for the key policy "enhancement of incident response capability"

○ Number of participants in cross-sectoral exercises

○ Ratio of participants who assess the knowledge obtained through exercises as having contributed to the cybersecurity measures of the organization to which they belong

○ Participation in exercises and training implemented both inside and outside the organization, including cross-sectoral exercises

(4) Indexes for the key policy "risk management and preparation of incident readiness"

○ Number of copies of Risk Assessment Guidelines for Mission Assurance distributed (or when it is publicized on the website, number of accesses to the relevant webpage), and number of participants in briefing sessions and lectures concerning risk assessment

○ Number of cases of interdependency analysis and environmental change studies implemented by the Cabinet Secretariat

○ Number of occasions of provision of opportunities for information exchanges for the CEPTOAR council and cross-sectoral exercise stakeholders

○ Number of cases of the development of incident readiness and the implementation of audits based on the key points indicated by the Cabinet Secretariat in the results of the survey on the dissemination of risk management

(5) Indexes for the key policy "enhancement of the basis for CIP"

○ Number of times of communicating information on the website and through newsletters and lectures, etc.

○ Number of times of collecting information through visit surveys, workshops and seminars

○ Number of times of information exchanges through bilateral, inter-regional and multilateral frameworks

○ Conditions of preparing guidebooks that contribute to CIP

○ Degree of expansion of a third party certification system for control systems and related equipment

VI. 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 CI.

Revision of the Cybersecurity Policy is generally conducted once every three years, in principle, together with the assessment of the Cybersecurity Policy. However, as the Olympic and Paralympic games are scheduled in 2020, this Cybersecurity Policy should be revised after the games are over. 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 and *Hiyari-Hatto* events (hereinafter referred to as "information related to system[10] 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 or *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.

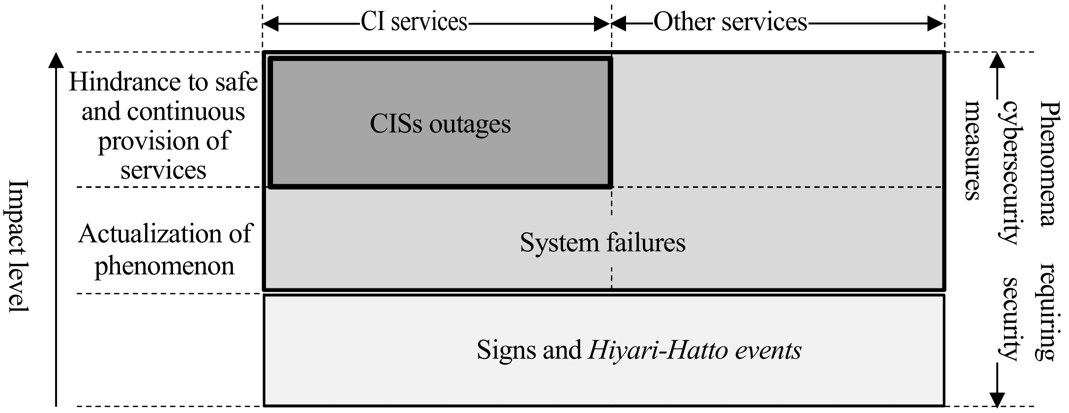

CI services
Other services
Hindrance to safe and continuous provision of services
Actualization of phenomenon
Impact level
CISs outages
System failures
Signs and *Hiyari-Hatto events*
Phenomena requiring cybersecurity measures
security

Figure. Scope of Information Sharing

[10] 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 expected to spread rapidly in the future.

Considering that the affected area and incident response activities are different depending on the severity of CISs outages and the importance of related information, severity schema on CISs outages are established as follows and concrete discussion is to be commenced with the aim of ensuring sharing of awareness among stakeholders and enabling quick decision making on incident response.

Table. Severity Schema on CISs Outages (draft)

Severity	Definition
Level 5 Emergency	Poses an imminent threat to wide-scale critical infrastructure services
Level 4 Severe	Likely to result in a significant impact on critical infrastructure services
Level 3 High	Likely to result in a demonstrable impact on critical infrastructure services
Level 2 Medium	May affect critical infrastructure services
Level 1 Low	Unlikely to affect critical infrastructure services

It is expected that stakeholders' efforts for information sharing and incident responses based on the abovementioned severity schema will clarify and deepen their understanding of shared information and assist their efficient and effective activities.

2. Information Sharing to NISC from CI Operators

2.1 Cases requiring information sharing to NISC

Of information related to system failures,[11] 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 CI 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 CI 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 CI 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 CI in accordance with "ANNEX 4-1. INFORMATION SHARING SYSTEM."

(ii) The personnel of responsible ministries for CI 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 CI and make a report to the Cabinet Secretariat simultaneously.

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

[11] Meaning information on system failures, including CISs outages, and signs and *Hiyari-Hatto* events

2.3 Handling of information shared to NISC

The Cabinet Secretariat and responsible ministries for CI 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[12], the information may be disclosed. This does not apply when falling under the cases requiring information sharing from NISC as explained 3.1 below.

[12] 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 CI, 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.[13]

(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 CI 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 CI. 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 severity and can utilize the information easily.

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

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

(iv) In particularly urgent cases, such as the case of early warning information, etc., regardless of procedures (i)

[13] For 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, estimates of possible impacts of CISs outages due to common risk sources on other CI sectors, and judgment of severity based on these studies and estimates.

to (iii), the Cabinet Secretariat directly provides the information to CEPTOARs or individual CI operators and releases reports to liaisons of responsible ministries for CI 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 CI 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 ordinary situations

ANNEX 1. SCOPE OF CI OPERATORS AND CRITICAL INFORMATION SYSTEM EXAMPLES

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

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

ANNEX 2. EXPLANATION OF CI SERVICES AND CI SERVICE OUTAGE EXAMPLES

CI sectors	CI services (including procedures)[Note 1]		Examples of CISs outages caused by system failures	Laws and guidelines pertaining to CISs outages reports (Service maintenance levels[Note 2])
	name	Explanation of services (including services) (Relevant laws)		
Information and communication services	- Electrical communication services	- Intermediary for communications of other parties using telecommunication facilities and provision of telecommunications facilities for the communications of other parties (Article 2 of the Telecommunications Business Act)	- Suspension of telecommunications services - Hindrance to safe and stable supply of telecommunications services	- Article 28 (report of suspension of business) of the Telecommunications Business Act - Article 58 (serious accidents requiring reporting) of the Regulation for Enforcement of the Telecommunications Business Act [Service maintenance level] - There should be no accident wherein any trouble in telecommunication facilities causes suspension or quality deterioration of services for more than two hours, affecting 30,000 or more users.
	- Broadcasting services	- Electrical communications broadcast aimed at direct reception by the public (Article 2 of the Broadcast Act)	- Suspension of broadcasting services	- Articles 113 and 122 (report of serious accident) of the Broadcast Act - Article 125 (serious accidents requiring reporting) of the Regulation for Enforcement of the Broadcast Act [Service maintenance level] - There should be no accident wherein any failure in base broadcasting facilities causes a broadcast outage for more than 15 minutes. - There should be no accident wherein any failure in specified terrestrial base broadcasting facilities or base broadcast station facilities causes a broadcast outage for more than15 minutes (or for more than 2 hours for relay station wireless facilities).
	- 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 services) (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
		- Financial settlements	- Financial settlements (Article 2, paragraph (5) of the Act on Financial Settlements)	- Delay and suspension of financial settlements	- Comprehensive Guideline for Supervision of Settlement/Money Transfer Agencies
		- Electronic records, etc.	- Electronic records (Article 56 of the Electronically Recorded Monetary Claims Act) - Information provision related to fund settlement (Articles 62 and 63 of the Electronically Recorded Monetary Claims Act)	- Delay and suspension of electronic records and information provision related to fund settlement	- Guideline for Administrative Processes Vol 3.: Financial Companies (12 Electronic credit record agency relationships)
	Life insurance services	- Insurance claim etc. payments	- Receipt of insurance claim etc. payment demands - Insurance claim etc. payment screenings - Insurance claim etc. payments	- Delay and suspension of insurance claim etc. payments	- Comprehensive Guidelines for the Supervision of Insurance Companies
	General insurance services	- Insurance claim etc. payments	- Accident reception - Damage investigations etc. - Insurance claim etc. payments	- Delay and suspension of insurance claim etc. payments	- Comprehensive Guidelines for the Supervision of Insurance Companies
	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 services) (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
Aviation services	- Air transportation services for passengers and cargo	- Work providing transport of passengers or cargo for charge using airplanes based on demands of other people (Article 2 of the Civil Aeronautics Act)	- Hindrance to safe flight of airplanes - Flight delay and cancellation	- Safety Guideline for Ensuring Information Security for Air Transport Operators
	- Reservations, ticketing, boarding/loading procedures	- Air traveler reservations, air cargo reservations - Airline ticket issuance, fee collection - Airline passenger check-in and boarding, air cargo loading		
	- Flight maintenance	- Airplane inspection and maintenance		
	- Flight plan creation	- Creation of flight plans and submission to Japan Civil Aviation Bureau		

CI sectors	CI services (including procedures)(Note 1)		Examples of CISs outages caused by system failures	Laws and guidelines pertaining to CISs outages reports (Service maintenance levels(Note 2))
	name	Explanation of services (including services) (Relevant laws)		
Airport	- Securing security at the airport - Improvement of convenience at the airport	- Securing airport security by vigilance and guard - Accurate and prompt information provision to airport users - Inspection and transport of checked baggage to aircraft	- Degradation of airport security due to the occurrence of trouble with the vigilance and guard - Degradation of convenience due to the occurrence of trouble with the information provision - Delay and stop of inspection and delivery of checked baggage to aircraft	- Safety guideline for securing information security in 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
Electric power supply services	- General electric power transmission and distribution services - Electric power generation services (services exceeding a certain scale)	- Work adjusting power generation quantity and transporting and supplying electric power in the service area (Article 2, paragraph (8) of the Electric Business Act) - Electric power generation for the retail electricity business, general electricity transmission and distribution business, or specified electricity transmission and distribution business (Article 2, paragraph (14) of the Electric Business Act)	- Electric power supply outages - Hindrance to safe operation of power plants	- Article 3 of the Electricity related Reporting Code [Service maintenance level] - There should be no accident wherein any system failure causes hindrance to supply of over 100,000kilowatts of electric power for more than ten minutes.
Gas supply services	- General gas supply services	- Work supplying gas through piping to meet general demand (Article 2 of the Gas Business Act)	- Gas supply outages - Hindrance to safe operation of gas plants	- Article 112 of the Regulation for Enforcement of the Gas Business Act [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	
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

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

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

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

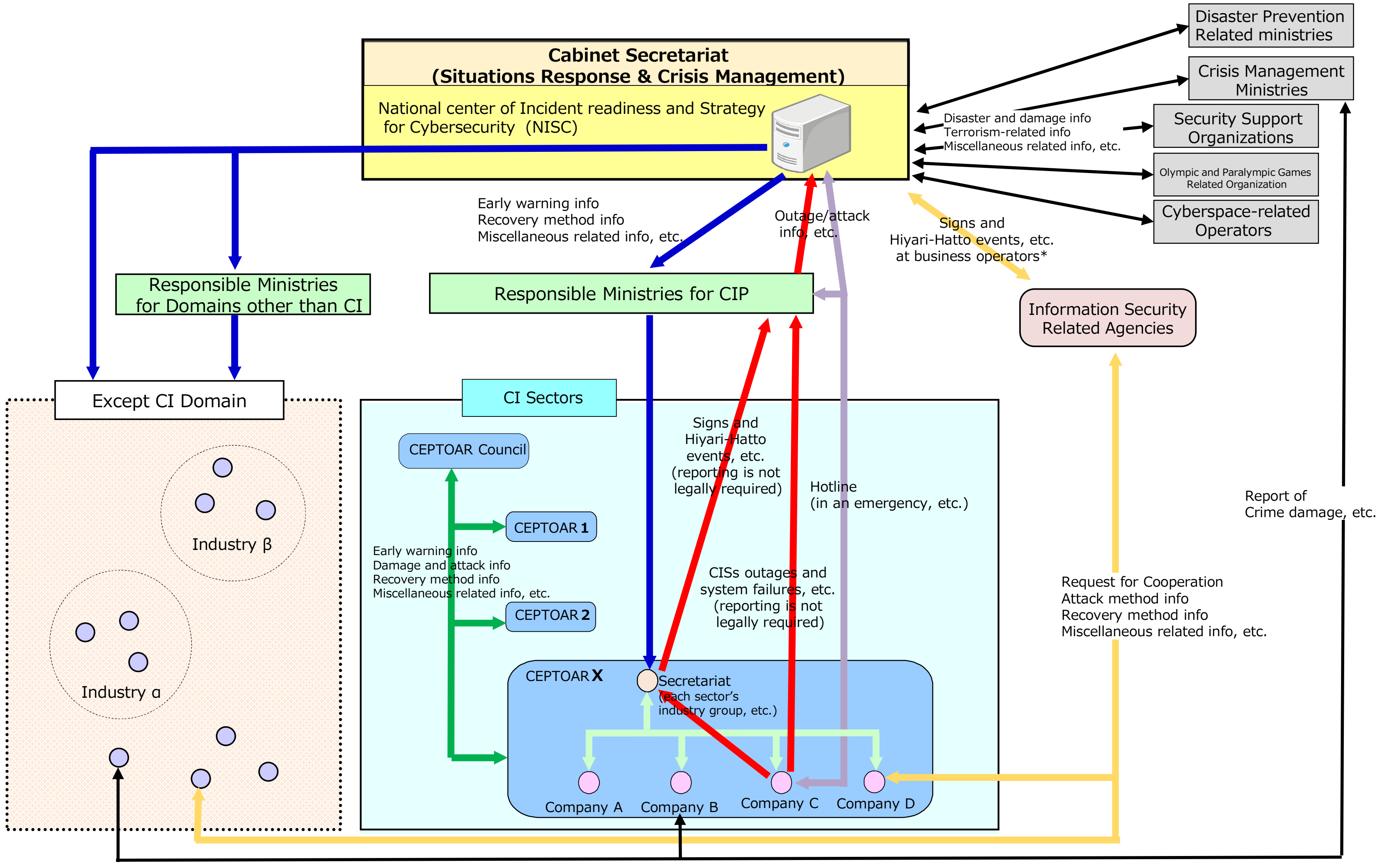
Note 3: Under the amended Installment Sales Act (to be enforced as of the day specified by Cabinet Order within one year and six months from the date of promulgation (December 9, 2016)), Article 2, paragraph (3), items (i) and (ii) and Article 35-16, paragraph (1), item (ii) and paragraph (2)

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, detection of vulnerability of systems, 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


Cabinet Secretariat
(Situations Response & Crisis Management)
National center of Incident readiness and Strategy for Cybersecurity (NISC)
Disaster Prevention Related ministries
Crisis Management Ministries
Security Support Organizations
Olympic and Paralympic Games Related Organization
Cyberspace-related Operators
Disaster and damage info
Terrorism-related info
Miscellaneous related info, etc.
Early warning info
Recovery method info
Miscellaneous related info, etc.
Outage/attack info, etc.
Signs and Hiyari-Hatto events, etc. at business operators*
Responsible Ministries for Domains other than CI
Responsible Ministries for CIP
Information Security Related Agencies
Except CI Domain
Industry β
Industry α
CI Sectors
CEPTOAR Council
CEPTOAR 1
CEPTOAR 2
CEPTOAR X
Early warning info
Damage and attack info
Recovery method info
Miscellaneous related info, etc.
Signs and Hiyari-Hatto events, etc. (reporting is not legally required)
Hotline (in an emergency, etc.)
CISs outages and system failures, etc. (reporting is not legally required)
Secretariat (each sector's industry group, etc.)
Company A
Company B
Company C
Company D
Request for Cooperation
Attack method info
Recovery method info
Miscellaneous related info, etc.
Report of Crime damage, etc.

* Information can be shared after data anonymization.

ANNEX 4-2. RESPONSIBILITIES OF EACH STAKEHOLDER IN INFORMATION SHARING SYSTEM

Stakeholder	Responsibilities during normal circumstances	Responsibilities during a CISs crisis
○ 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 CI, 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 CI, cybersecurity related ministries, crisis management ministries, disaster prevention related ministries, cybersecurity related agencies, and cyberspace-related operators, etc.
○ Responsible ministries for CI	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 CI 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 CI, 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 CI 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.

* 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	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, deteriorates or becomes unavailable, it could have a significant impact on the national life and economic activities.
CI operators	Operators designated in "Applicable CI operators" in "ANNEX 1. SCOPE OF CI OPERATORS AND CRITICAL INFORMATION SYSTEM EXAMPLES" and groups composed of those designated operators
CI sectors	Sectors regarding CI designated for each business type; Specifically, as follows: "information and communication services," "financial services," "aviation services," “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
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
Cybersecurity measures	A wide range of activities for preventing CISs outages from affecting the national life and economic activities
Cybersecurity related agencies	The National Police Agency Cyber Force; National Institute of Information and Communications Technology (NICT); National Institute of Advanced Industrial Science and Technology (AIST); Information-Technology Promotion Agency (IPA); ICT Information Sharing And Analysis Center Japan (ICT-ISAC Japan); Japan Computer Emergency Response Team Coordination Center (JPCERT/CC); Japan Cybercrime Control Center (JC3)
Cybersecurity related ministries	The National Police Agency (NPA); Ministry of Internal Affairs and Communications (MIC); Ministry of Foreign Affairs (MOFA); Ministry of Economy, Trade and Industry (METI); Secretariat of the Nuclear Regulation Authority(*); Ministry of Defense (MOD) * The ministry engaging in cybersecurity-related duties from the perspective of ensuring safety of nuclear power plants

Cyberspace-related operators	System vendors, which are engaged in the design, construction, operation and maintenance of information systems required for providing CI services; security vendors, which provide cybersecurity measures such as antivirus software of those information systems; and platform vendors, which provide the platforms which serve as foundations, including hardware and software of those information systems
Disaster prevention related ministries	The government organizations and ministries stipulated in Article 2, item (iii) of the Basic Act on Disaster Control Measures (Act No. 223 of 1961) which engage in information collection in the event of a disaster
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. Measures section contains detail measures as an example.
Information sharing	The mutual provision and sharing among relevant entities of information on system failures (information including that on CISs outages and any signs of possible system failures and *Hiyari-Hatto* events) and information that will contribute to ensuring 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 any signs of possible system failures and *Hiyari-Hatto* events) at CI operators from the CI operators to the Cabinet Secretariat
Information systems	All systems based on IT such as systems for business processing, control field equipment, monitoring and control systems
IT-BCP	Business continuity plan (including relevant manuals) related to the information systems to provide CI services, and other business continuity plan
Responsible ministries for CI	Financial Services Agency (FSA); Ministry of Internal Affairs and Communications (MIC); Ministry of Health, Labour and Welfare (MHLW); Ministry of Economy, Trade and Industry (METI); Ministry of Land, Infrastructure, Transport and Tourism (MLIT)
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 CI; cybersecurity related ministries; crisis management ministries; disaster prevention related ministries; CI operators; CEPTOARs; CEPTOAR council; cybersecurity related agencies; cyberspace-related operators
System failures	Events that information systems of CI operators do not or cannot perform as expected at the time of their design