The Basic Policy of
Critical Information Infrastructure Protection
(3rd Edition)

(Tentative Translation)

May 19, 2014
Information Security Policy Council

Last modified
2014.06.19

(This page intentionally left blank.)

Contents

I. INTRODUCTION

1. BACKGROUND

The Basic Policy[1] of Critical Information Infrastructures (hereinafter abbreviated as CII) is a shared basic policy for the government, which bears responsibility for the protection of the CII, and CII providers, which independently carry out relevant protective measures. It was established to serve as the basis for the policy related to information security measures for Japan's critical infrastructure, such as the enactment of the *"Special Action Plan on Cyber-terrorism Countermeasures for Critical Infrastructure" (concluded in the December 2000 Information Security Measure Promotion Meeting)*, prior to the establishment of the National Information Security Center (NISC).

After the establishment of the NISC, in 2005, the *"First Action Plan on Information Security Measures for Critical Information Infrastructures"* (hereinafter referred to as the *First Action Plan*) was established based on the *"Basic Orientation for Countermeasures Necessary for Protecting Critical Infrastructure from IT Outages and Ensuring Business Continuity of Critical Infrastructure Providers"* presented in the Information Security Policy Council of the same year. Based on the *First Action Plan*, relevant measures were taken by the stakeholders including the government and 10 CII sectors with a view to reducing IT outages at CII as close to zero as possible.

Furthermore, the *"Second Action Plan on Information Security Measures for Critical Information Infrastructure"* (hereinafter referred to as the *Second Action Plan*) was established in 2009 which identified policies to be implemented by the nation, based on the basic measures for CIIP and the public-private information sharing framework established by the *First Action Plan*. The *Second Action Plan* has taken over the measures of the "maintenance and promotion of the safety principles", "enhancement of information sharing", "common threat analysis[2]" and "cross-sectoral exercises" in the *First Action Plan* and also additionally identified policies for "response to environmental changes" in order to appropriately address ever-changing social and technological environment.

In this manner, the protection of Japan's CII has been carried out for 13 years since the Special Action Plan and even for 8 years since the establishment of the *Second Action Plan*. It can be concluded that relevant measures have been steadily implemented based on 5 policies such as establishing a robust information sharing system.

---

[1] The terminology "Action Plan" was used in the previous version of this document. However, taking the nature of this document into consideration, the title is renamed as "The Basic Policy of Critical Information Infrastructure Protection".

[2] In the *First Action Plan*, this was referred to as "interdependency analysis".

As such, this Basic policy appropriately reflected the lessons learned through the assessment of a group of policies identified in the *Second Action Plan* while taking into account the *Cybersecurity Strategy* (determined at the June 2013 Information Security Policy Council).

Furthermore, in addition to the lessons learned from the experience of dealing with system outages and data loss during the Great East Japan Earthquake, this Basic Policy also reflects appropriate responses to the ever-changing social and technological environment and the trends of increasingly sophisticated and complex cyber-attacks carried out in recent years.

2. CLARIFICATION OF THE PURPOSE OF CIIP

As a basis for the implementation of this Basic Policy, it is necessary to clarify the purpose of the protection of CII and to share awareness among stakeholders.

Cybersecurity Strategy identified "Ensuring Free Flow of Information", "Responding to Increasingly Serious Risks", "Enhancing Risk-based Approach" and "Acting in Partnership Based on Shared Responsibility" in its Basic Principles, and the purpose of the *Second Action Plan* are consistent with the *Cybersecurity Strategy*.

As such, in addition to maintaining the elements of the purpose of the *Second Action Plan*, the need for continuous provision of CII services was added, which further clarified the purpose of CII protection.

Purpose of "CII protection" (referred to as "CIIP")

In order to continuously provide CII services and to avoid serious effects on the public welfare and socioeconomic activities from IT outages resulting from natural disasters, cyber-attacks or other causes, all stakeholders should protect CII by reducing the risk of IT outages as much as possible and by ensuring prompt recovery from IT outages.

Basic Principles for CIIP

In the first place, CII operators should implement measures for CIIP on their own responsibility. In addition, a sense of security should be nurtured among the public and social development, resilience and international competitiveness should be promoted through activities in cooperation between Government and private sectors.

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

3. LESSONS LEARNED FROM ACTIVITIES UNDER THE SECOND EDITION

The *Second Action Plan* is composed of the following 5 policies.

[1] Maintenance and promotion of the safety principles

[2] Enhancement of information sharing system

[3] Common threat analysis

[4] Cross-sectoral exercises

[5] Response to environmental changes

Each policy's outcome and challenges are summarized as follows:

3.1 Outcome

The assessment of these policies was carried out according to the assessment indexes set in the *Second Action Plan* since the *Second Action Plan* was determined based on the most updated information regarding CII as of 2009. Consequently, for the expected targets, it can be concluded that a certain result was achieved as elaborated below.

For maintenance and promotion of the safety principles, stakeholders involved in measures for CIIP could understand and identify necessary measures which they should take independently and made efforts to carry out such measures under a periodic self-inspection. As a result, an integrated and steady review cycle was established for guidelines and the safety principles, which reinforced the promotion of measures for CIIP.

As for enhancement of information sharing, for the purpose of addressing the ever-changing social and technological environment surrounding CII security measures and increasingly complex and sophisticated cyber-attacks, frameworks for information sharing with NISC was established through cooperation between Government and private sectors, and the utilization of such frameworks was steadily achieved. In addition, information sharing within and among CEPTOARs was realized and necessary information was shared and utilized among CII operators.

For common threat analysis, as a result of carrying out examinations of common threat analysis based on analyses of cross-sectoral circumstances which is indispensable for the maintenance and enhancement of protective capability for overall CII, basic material was provided which contributed to the establishment of business continuity plans for CII operators and part of the result was reflected in guidelines.

For cross-sectoral exercises, as a result of making efforts to provide opportunities for verification of systems for communication and collaboration through simulated exercises with

the participation of both public and private stakeholders in all relevant sectors in case of IT outages, the number of organizations and individuals participating in the exercises is on an upward trend. Furthermore, it contributed to information security through verification of CII operators' manual for early recovery and business continuity plans in case of an IT outage, based on the lessons learned through the exercises.

Regarding public relations activities in particular among the response to environmental changes, materials on the results of CII information security policy, meeting materials of CII Special Committee under the Information Security Policy Council and other materials were posted and published on the Cabinet Secretariat website. In addition, lectures focusing on information security policy and other events were held. As for development of risk communication, exchanges of opinion were held among CIIP supporting agencies and a mutual understanding WG was held at a CEPTOAR council. As for promotion of international cooperation, cooperation with other foreign countries was carried out through such initiatives as participating in the Meridian[3] and the Cyber Storm Exercises[4]. Through these initiatives, relevant efforts were made to improve capabilities to perceive threats due to environmental changes.

3.2 Challenges

Through the implementation of each policy, challenges were identified which required improvement/reinforcement of the policy based on environmental changes from social/technological aspects. The principal challenges for each policy are described below.

As for maintenance and promotion of the safety principles, reexamination in conformity with measures for continued improvement in line with the PDCA cycle of CIIP measures at CII operators should be carried out. This is because measures for CIIP also have an effect not only on CII operators themselves but also on the maintenance and enhancement of protective capability for overall CII. Furthermore, there have been requests from CII operators for sharing guidelines which have prioritized items based on the actual conditions of measures.

With regard to enhancement of information sharing, necessary measures to establish an effective information sharing system include: eliminating the gap in terms of the frequency of information sharing among sectors; further elaborating "threat patterns"; establishing an emergency information sharing system to cope with IT crises, which should be the same basis of normal conditions; and studying forms of coordination with other new stakeholders.

[3] An international forum where CII supervisors from various countries meet and carry out discussions specialized for CII protection.

[4] A large scale exercise held by the U.S. government. Japan participates as a member of the IWWN (International Watch and Warning Network) when promoting international measures for handling vulnerabilities, threats and attacks.

For common threat analysis, detailed analysis of threats based on changes over time and environmental changes which have become evident is necessary. The purpose of this analysis is to improve the effects of threat analysis and to conduct reviews on how to carry out common threat analysis from the perspective of expanding the scope of such analysis to include threats which may have a major effect broadly even if not on all sectors instead of limiting the scope only to the common threats across all sectors, looking ahead to the review of the subject and role as well as the frequency of such analysis.

As for cross-sectoral exercises, the design of exercise environments is limited since the IT usage and information management at each organization differs, which makes it unlikely to realize a major expansion of the number of participants. For this reason, with a view to providing CII operators opportunities to identify shortcomings of CIIP measure, further dissemination and promotion of the outcome of the exercises across the entire CII sectors should be realized , rather than depending only on the expansion of participants. Additional issues to be addressed include: qualitative improvement of how to carry out exercises based on the assessment of results; identification of relevant stakeholders based on responses to CII IT outages; and examination of collaboration between exercises and training sponsored by and responsible ministries for CIIP and those in charge of disaster prevention.

Regarding public relations activities in particular among the response to environmental changes, reexamination of public relations activities depending on the purpose and the scope of information disclosure should be carried out, while ensuring consistency among policies in the next-term Basic Policy. For development of risk communication, challenges include: having a definition of risk management in conformity with international standards; reexamination of information sharing which takes into account the balance between the secrecy of sensitive information and the value of such information; and continued mid- to long-term examination and study of the themes of environmental changes such as new IT technologies which will be developed and utilized in the mid- to long-term and a significant impact of threat against which is expected. For promotion of international cooperation, continuous promotion of cooperation with other countries is necessary in order to quickly address increasingly globalized risks in the cyberspace that transcends national borders. It is also necessary to reinforce international cooperation through active utilization of bilateral, inter-regional and multilateral frameworks in the Asia-Pacific, such as with ASEAN, as well as with the United States and Europe.

4. ISSUES TO BE CONSIDERED

In addition to identifying the challenges in the previous section and the issues which were specified in the *Cybersecurity Strategy*, the following examinations were carried out to determine the direction of this Basic Policy based on the aforementioned challenges.

Issue 1	While CII protection continues to develop as a system, in regard to the *"In the first place, CII operators should implement measures for CIIP on their own responsibility."* in the Basic Principles, there are some CII operators which are not implementing such measures or which lack sufficient understanding on this point. What are the appropriate ways to promote effective and voluntary activities by those CII operators?

<Direction>

* The content should not be something too idealistic that are difficult for CII operators to implement in a realistic way. It should take into account the reality and be something "accomplishable" in line under the current situation. For example, expressions such as "absolute security is expected" or "100% perfection is anticipated" should be avoided.
* Basic items should be articulated in the Basic Policy so that executives and senior managers in the business community who hold the key to ensure information security at CII operators can understand the need for the implementation of the Basic Policy.
* Since both experts as well as non-experts are likely to read the Basic Policy, the Plan should be something easy to comprehend for any relevant parties so that each party understands what kind of measures are required to take under the Basic Policy.
* Clarify the PDCA cycle for maintenance and enhancement of protective capability for CII, particularly vis-à-vis small- and medium-sized CII operators as well as those operators still in the process of developing such capability, which will contribute to promoting effective and voluntary measures by those operators.
* Explain in detail the importance of risk management and the need for introducing such risk management by CII operators so as to address environmental changes in a flexible manner.
* Compile regulations across various layers which CII operators are required to understand into a certain kind of package in a way that such package can easily be shared and handed over to successors among relevant parties despite high turnover.
* Further promote public relations activities so that even after the Basic Policy is released, appropriate response will be made to address ever-changing environment and collection and provision of relevant information will be continuously carried out.

Issue 2	In regard to ever-changing social and technological environment and threats which have become increasingly serious year by year, there are concerns that measures have not been fully taken to respond in an appropriate and quick manner. What type of activities, both in the public and private sectors, will be necessary in order to appropriately address such environmental changes and threats? In addition, isn't it necessary to consider if there are any actors which should be included as stakeholders?

<Direction>

* Add relevant parties among cyberspace-related operators as stakeholders so as to ensure more robust information sharing.
* Promote greater awareness among relevant parties that activities of CII operators in cyberspace could be targeted and be exploited and that they should bear responsibility accordingly.
* Conduct examination on priority risk sources[5] across multiple areas and continual examination of mid- to long-term changes of new technologies, systems, etc., taking into account the fact that threats and vulnerabilities in each area and among CII sectors vary and that social and technological environment is constantly changing.

Issue 3	While a variety of activities have been initiated among stakeholders to address potential IT outages, there are concerns that the management and systems (public-private and public-public) in the event of a severe IT outage have not been sufficiently identified. Isn't it necessary to identify the scope of information which needs to be shared and to elaborate each stakeholder's response and coordination mechanism in the event of such a severe IT outage?

<Direction>

* Enhance an effect of exercises, training, etc., through collaboration among exercises and trainings among relevant stakeholders.
* Establish a mechanism which detects when and what kind of IT crises require special warnings among CII operators, and clarify to the possible extent who should be added as stakeholders and how they should be added to a response systems under normal circumstances (situations other than during IT crises response). (*It is not realistic to set up an entirely new system when an incident occurs.)

[5] According to *JIS Q 31000:2010*, risk source is defined as "elements which alone or in combination has the intrinsic potential to give rise to risk".

5. REVIEW OF THE SCOPE OF CII

During the process of compiling this Basic Policy, deliberation was carried out on the scope of CII, which is currently composed of 10 sectors identified in the *Second Action Plan*. Further study was carried out to determine whether new sectors should be added in the list of CII.

In addition, as for issues identified in the *Cybersecurity Strategy*[6] as something that further deliberation will be carried out on, including the scope of the CII, deliberation will continue by taking into account environmental changes and based on coordination with relevant parties.

5.1 Results

Deliberation was carried out, based on the lessons learned from the past experiences, such as during the Great East Japan Earthquake.

In the case of deliberation, we have conducted identification of sectors that had not been identified as CII in the *Second Action Plan*. But these might make same serious impacts on the public welfare and socioeconomic activities as existing CII sectors in the event of an IT outage.

As a result, several sectors were identified as necessary to be added as new CII sectors as shown in Table 1.

Table 1. Results of study on the scope of CII

Classification	Viewpoint/Necessity	Sector
Sectors to be added due to the effects in the event of an IT outage of the sectors concerned	Value and scale of the service to be provided by the sector	Credit card services
	Scale of the potential risk under a situation where the sector gets out of control	Chemical industries, petroleum industries
Sectors to be added due to the effects on the information systems of the current CII sectors	Interdependency with the current CII sectors	Petroleum industries (See above)

As a result, in this Basic Policy, the CII sectors are composed of the following 13 sectors: "information and communication services", "financial services", "aviation services", "railway services", "electric power supply services", "gas supply services", "government and administrative services (including municipal government)", "medical services", "water services", "logistics services", "chemical industries", "credit card services" and "petroleum industries".

When these added sectors participate in the existing efforts as CII, it is important for the sector to recognize why the sector was added and what is the merit of the participation without

[6] Refer to *"2. Basic Policy" - "(3) Roles of Multi-Stakeholder" - "② Roles of critical infrastructure providers"* (p. 20).

doubts, in order to understand the necessity of own initiative.

For ministries and agencies which have jurisdiction over the added sectors and for those industry groups which are candidates for serving as CEPTOAR secretariat, a pivot to ensure information sharing, explanations were made on the above viewpoints. As a result, there is shared understanding among relevant parties about the addition and the participation of new sectors as CII. Furthermore, the relevant industry groups are identifying critical information systems and service maintenance levels and preparing for the establishment of a CEPTOAR.

5.2 Relationship between existing CII sectors and added sectors

7 years have passed since the establishment of the information sharing system in FY2007. Currently, each CEPTOAR has certain experience through implementing CIIP measures and has unique qualities originating from the nature of each operation and others.

Against such backdrop, when these added sectors participate as new CEPTOARs, there is a concern that the activities of the existing CEPTOARs could be overwhelming. It is necessary for the Cabinet Secretariat to give advice to those new sectors, keeping in mind that cooperation with other CII operators in the same CII sector and CII operators in other CII sectors is important. In addition, it is also expected that at a CEPTOAR council, CEPTOARs advice will be given to the added sectors out of a spirit of mutual support, which will contribute to maintenance and enhancement of protective capability for overall CII.

6. OUTCOME OF THE REVIEW FOR THE REVISION OF BASIC POLICY

Based on the challenges and directions identified, , in the process of compiling this Basic Policy, it was decided that the basic framework of the *Second Action Plan*, which was in conformity with the *Cybersecurity Strategy*, would be maintained. However, individual policies and the implementation systems were decided to be revised, and through reinforcing and refining the components of the Basic Policy, the policy group structure shown in Table 2 was specified.

Table 2. Policy groups and direction of reinforcing and refining the components of the Basic Policy

Policy groups in this Basic Policy	Policy groups in the *Second Action Plan* and the status of each group	Direction of reinforcing and refining the components of the *Second Action Plan*
1. Maintenance and promotion of the safety principles	Keep the element of *"[1] Maintenance and promotion of the safety principles"*	- Articulate the process of reflecting the results on guidance and measures - Make an appeal based on the growth models, etc. and conduct reviews on the actual status of the implementation of relevant measures
2. Enhancement of information sharing system	Keep the element of *"[2] Enhancement of information sharing system"*	- Review and rearrange the relationship of each stakeholder in the information sharing system, including new stakeholders - Review the scope of information (threat patterns, etc.) which should be shared among relevant parties based on the increase in cyber-attack related information - Clarify crisis management system in case of IT crises based on the management under normal circumstances
3. Enhancement of incident response capability	Re-arrange the element of *"[4] Cross-sectoral exercises"*	- Enhance overall IT outage response system after developing an understanding of the overall image of CII related exercises and training - Ensure qualitative enhancement of cross-sectoral exercises in view of the need for coordination with new stakeholders
4. Risk management	Re-arrange the element after integrating a portion of *"[3] Common threat analysis"* with *"[5] Response to environmental changes"*	- Implement a mid- to long-term studies on potential risk sources which could have a major impact on multiple sectors as a result of environmental changes as well as environmental changes which could have a major impact in the future - Make an appeal for CII operators to have accurate understanding on the current circumstances and on risk management which will be the key to identify goals on their own responsibilities
5. Enhancement of the basis for CIIP	Re-arrange after excluding the sections of *"[5] Response to environmental changes"* integrated with *"[3] Common threat analysis"*	- Add reference for related international standards/norms, regulations etc. and method for utilizing those in addition to public relations and international cooperation

In order to ensure an appropriate response to major environmental changes which could take

place after this Basic Policy is issued, it is necessary to continually monitor environmental changes and identify threats from the information, and to construct systems that will enable flexible response. In addition, it is also important for the systems to be able to seamlessly shift from that of normal circumstances to that of IT crises while ensuring robust measures to enhance IT outage response systems, rather than just focusing on prevention which was apriority previously.

II. EXECUTIVE SUMMARY OF THE BASIC POLICY

The key points for this Basic Policy are as follows;

(1) Purpose of "CII protection" (referred to as "CIIP")

In order to continuously provide CII services and to avoid serious effects on the public welfare and socioeconomic activities from IT outages resulting from natural disasters, cyber-attacks or other causes, all stakeholders should protect CII by reducing the risk of IT outages as much as possible and by ensuring prompt recovery from IT outages.

(2) Basic Principles for CIIP

In the first place, CII operators should implement measures for CIIP on their own responsibility. In addition, a sense of security should be nurtured among the public and social development, resilience and international competitiveness should be promoted through activities in cooperation between Government and private sectors.

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

(3) Responsibility of the stakeholders; CII operator / government organizations / CIIP supporting agency

- All the 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 the stakeholders should understand the 5W1H (when, where, who, why, what and how) of IT outage response depending on the scale of IT outages and should be able to calmly address signs or occurrence of an IT outage. They should 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.

(4) Responsibility of CII operator's executives and senior managers

In addition to the aforementioned measures, the executives and senior managers should recognize the need for and be able to ensure the implementation of the following measures:

- Recognize risk sources with a focus on information security for the purpose of CIIP.
- Assess risk sources and set forth measures to address those risks by identifying priorities.
- Determine plans necessary for the establishment and operation of systems and the implementation of relevant policies in addition to securing management resources (e.g. budget, human resources, etc.).
- Check the status of the implementation of relevant policies through monitoring the system operation.
- Check the status of incident response capability including information sharing among relevant stakeholders through conducting exercises and trainings.

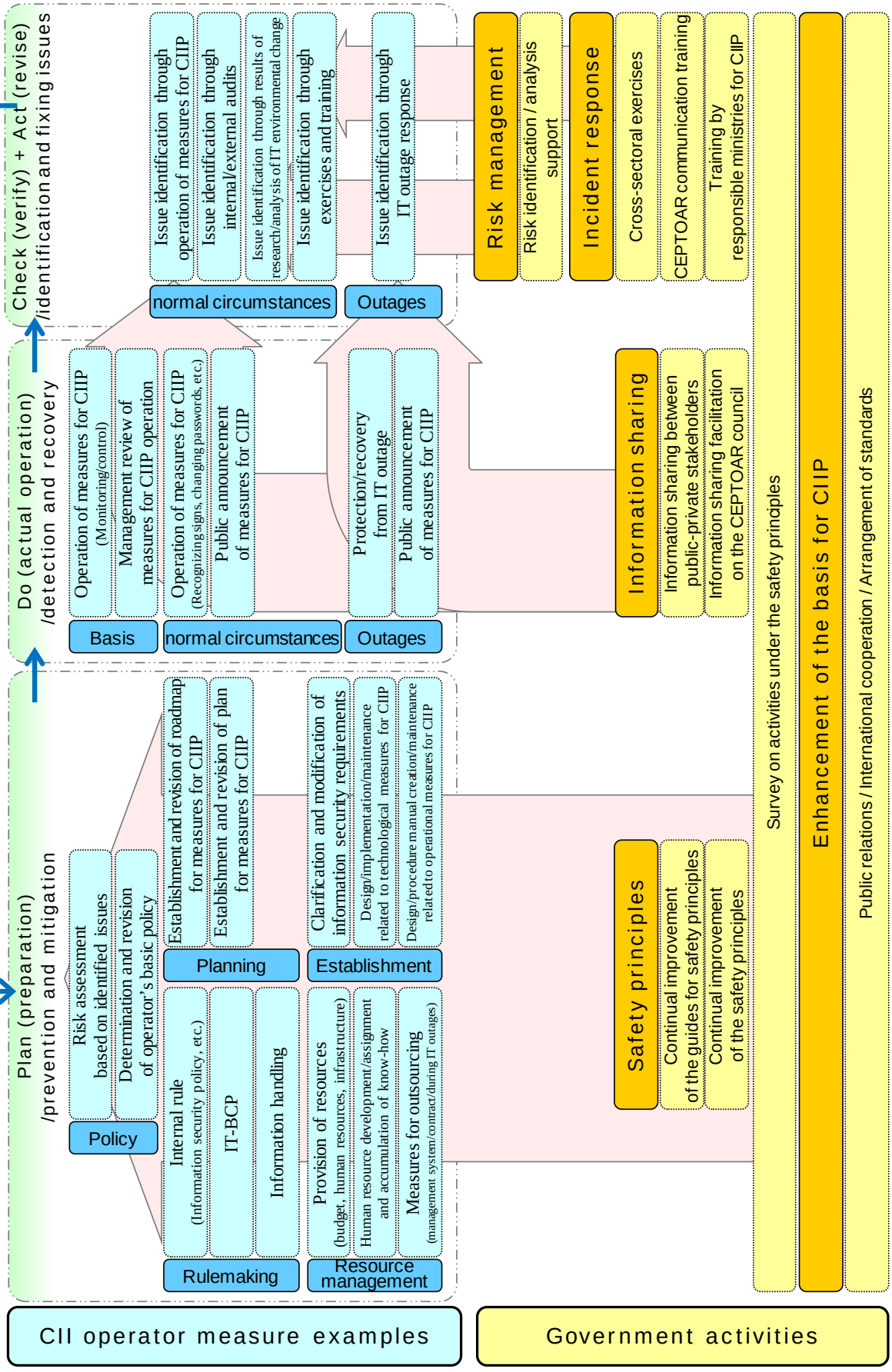


Figure 1. "CII operator measure examples" and "Government activities"

III. POLICIES FOR CIIP

1. MAINTENANCE AND PROMOTION OF THE SAFETY PRINCIPLES

During the term of this Basic Policy, the Cabinet Secretariat carries out the review the Guidelines for safety principles and related surveys so that they would conform with the PDCA cycle of CII operators and would enhance the cooperation with other policies, in order to strengthen the ability of CIIP.

Also, CII operators continuously and steadily work on measures for CIIP in accordance with their PDCA cycle, in view of importance of the measures.

1.1 Continual improvement of the Guidelines for safety principles

The Cabinet Secretariat carries out the review the Guidelines in FY 2014, in order to strengthen the ability of CIIP, especially in order to contribute to effective and autonomous activities of mid-process or small-and-medium-sized CII operators.

In detail, it arranges the orders of the items in the Guidelines in accordance with the PDCA cycle of CII operators, and adds some items, if necessary, based on knowledge from other policies etc. in this Basic Policy.

In addition, some example views on prioritization of measures for CIIP in case CII operators execute these measures, ways of gradual addition of measures for CIIP, and ones on balancing with pre-active measures and post-active measures, are described as "growth-model".

Further, the Guidelines appeal the importance of the responsibility of CII operator’s executives and senior managers regarding policy, rulemaking, planning, resource management and establishment that are essential to gradually and constantly strengthen CII operators' measures.

After FY 2015, social trends changes and newly obtained knowledge is released each fiscal year, and the revision of the Guidelines is executed every 3 year or as necessary.

1.2 Continual improvement of the safety principles

Responsible ministries for CIIP and CII operators continually improve the safety principles based on knowledge learned from experiences when taking the measures, in order to maintain or strengthen the abilities of not only individual CII operator but also overall CII.

In detail, they approach continual improvement of the safety principles through risk assessment, by identifying issues from operation of measures for CIIP, internal/external audits,

environmental change studies, exercises, training and incident responses.

In addition, when verifying the safety principles, the Guidelines as well as social trend changes and newly knowledge released by the Cabinet Secretariat is used.

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

1.3 Promotion of the safety principles

The Cabinet Secretariat carries out survey the CII operators' activities, in order to recognize the status of promotion of the safety principles at CII operators. In addition, in order to contribute to CII operators' effective and autonomous activities, survey operations will also be revised so that responses to the survey will serve as self-checks of measures.

With regard to survey itself, the activities include addition of survey items that can identify more detail conditions in CII operators and ones that can detect degrade of measures in CII operators which have excellent conditions through periodical survey, with some expansion of the coverage of the target CII operators.

With regard to survey operations, the activities include an arrangement of the questionnaire items in the survey in accordance with the PDCA cycle so that the measures and process to be enforced become explicit.

In addition, in order to supplement the survey using the questionnaire method, the Cabinet Secretariat conducts visit to CII operators.

With regard to the visit, the activities include extraction of issues from detail conditions of measures and collection of best practices, through the interviews with detail items based on the questionnaire.

For the results from the questionnaires and the visit, in principal, these will be released each fiscal year, and in addition, the obtained improvement issues reflected on each of the policies of this Basic Policy.

Survey items can be changed flexibly to the degree that such change does not impair the periodical survey.

2. ENHANCEMENT OF INFORMATION SHARING SYSTEM

While the social and technological environments surrounding CII constantly change, it is necessary to recognize these environmental changes accurately and then reflect these changes in the measures for CIIP, in order to maintain the effectiveness of measures for CIIP. In addition, it becomes more important to raise the level of measures in CIIP and cyber-attack response capability due to increasing complexity, sophistication of cyber-attacks.

As described in the Basic Principles in *"I.2. CLARIFICATION OF THE PURPOSE OF CIIP"*, CII operators should fundamentally implement measures for CIIP at their own responsibilities, however, it is difficult to verify whether a response by only itself to various threats is sufficient or not. For this reason, it is important to work on necessary measures for CIIP through cooperation by carrying out information sharing within sectors, between sectors and through public private partnership.

Based on these conditions, in the term of this Basic Policy, the Cabinet Secretariat manages the information sharing system among stakeholders including added sectors and stakeholders, further promotes information sharing, and works towards further vitalization of information sharing activities by CII operators.

2.1 Information sharing system during the term of this Basic Policy

In this Basic Policy, for the purpose of enhancement of the information sharing system during IT crises, the Information Security Policy Council (referred as "ISPC" hereinafter) decides to add the disaster prevention related ministries for disaster management, and also add cyberspace-related operators. They are consisted of system vendors, which are engaged in the design, construction, operation and maintenance of information systems required for providing CII services, security vendors, which provide measures for CIIP and platform vendors, which provide the platforms which serve as foundations. The information sharing system after these addition is represented in *"ANNEX 4-1. INFORMATION SHARING SYSTEM (NORMAL* CIRCUMSTANCES*)"* and *"ANNEX 4-2. INFORMATION SHARING SYSTEM (IT* CRISES*)"* as extended system of the former one.

In addition, the ISPC reviews CII sectors' critical information systems and service maintenance levels including those in newly added sectors. The results are shown in *"ANNEX 1. SCOPE OF CII OPERATORS AND CRITICAL INFORMATION SYSTEM EXAMPLES"* and *"ANNEX 2. CII SERVICES AND SERVICE MAINTENANCE LEVELS"*.

During the term of this Basic Policy, the stakeholders manage the information sharing system according to their respective position and responsibilities. In addition, it is expected that cyberspace-related operators implement measures required for the maintenance of information

security, such as sharing of vulnerability information and preventing spread of damages in the event of IT outages resulting from cyber-attacks.

2.2 Promotion of information sharing

For arrangement of information to be shared, it is important to identify and arrange information that should be shared among stakeholders, including government organizations and CII operators, from aspects of "proactive prevention of IT outages", "prevention of the spread damages and quick recovery from IT outages", and "prevention of recurrence through analysis and verification of IT outage causes".

When establishing this Basic Policy, the Cabinet Secretariat has carried out revision of *"ATTACHMENT: "INFORMATION SHARING TO NISC" AND "INFORMATION SHARING* FROM NISC*"* and *"ANNEX 3. CATEGORIES OF EVENTS AND CAUSES FOR INFORMATION SHARING TO NISC"* based on the above 3 aspects regarding the information sharing system during normal times and during IT crises, in order to contribute to CIIP including proactive prevention of IT outages.

In detail, the ISPC has revised event[7] items based on the information security C.I.A[8] viewpoint and formed detailed cause items based on new threats, etc. in *"ANNEX 3. CATEGORIES OF EVENTS AND CAUSES FOR INFORMATION SHARING TO NISC"*, in order to grasp situation of IT outage rapidly and accurately. In *"ATTACHMENT: "INFORMATION SHARING TO NISC" AND "INFORMATION SHARING* FROM NISC*"*, the ISPC has clarified the coverage of information sharing, including handling of IT outage predictive information, in order to eliminate the disparity in the frequency of information sharing between sectors.

During the term of this Basic Policy, the Cabinet Secretariat carries out information sharing to and from NISC in accordance with the attachment, cooperate with stakeholders and promote this information sharing system, with the expectation that information sharing among stakeholders contribute to CII operation and their verification of measures, and proactive prevention of IT outages. In addition, in the event any environmental change occurs, it attempts to review the information system as appropriate.

[7] An Information Security Event is defined as *"The occurrence of a specific condition in systems, services or networks. Specific condition refers to an unknown condition which may be related to potential violations of information security policy, management measure failures or security."* in *ISO/IEC 27000:2013*.

[8] Stands for Confidentiality, Integrity and Availability.

2.3 Promotion of CII operators activities

It is expected that enrichment of information sharing between CEPTOARs as well as the activities of the CII operators themselves enhances further vitalization of CII operator activities.

In detail, it is expected that CII operators proactively work towards their own information sharing activities as well as they construct and enhance IT failure response systems, such as CSIRT[9],. It is also expected between CEPTOARs that they continue to share information provided by the Cabinet Secretariat, regarding agreements for handling of those provided information, maintenance of confidentiality and provision of information outside of constituent members, rules decided upon by constituent members will be applied, and the continued sharing of information provided by the Cabinet Secretariat is expected with a PoC[10] established allowing contact between constituent members and with non-members in case of emergency.

It is also expected that sharing activities is further activated through establishment of coordinators who will carry out information collection and decision making within CEPTOARs, sharing of predictive information and IT outage examples during normal times and enhancement of functions required for information sharing between CEPTOARs and with the CEPTOAR council.

The CEPTOAR council is an independent body, not positioned below other agencies, including government, so information mutually shared based on independent determinations by each CEPTOAR[11].

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

2.4 Responsibilities of each stakeholder in the information sharing system

The information sharing system is composed of an information sharing system for normal times and an expanded information sharing system for times of IT crises, and the roles of IT stakeholders during times of IT crises are also an expansion of their roles during normal times.

The overall image of information sharing during normal times and during IT crises is shown

[9] Computer Security Incident Response Team. A system for monitoring to check if any security issues exist with information systems and for carrying out investigations including cause analysis and extent of impact in the event an incident occurs.

[10] PoC: Point of Contact.

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

in *"ANNEX 4-1. INFORMATION SHARING SYSTEM (NORMAL* CIRCUMSTANCES)*"* and *"ANNEX 4-2. INFORMATION SHARING SYSTEM (IT* CRISES)*"* and the roles of each stakeholder are as follows.

2.4.1 Responsibilities of each stakeholder in the information sharing during normal circumstances

The roles of each stakeholder in the information sharing system during normal times are as follows.

(1) CII operators

Information sharing related to IT outages and cyber-attacks shall generally be carried out by the relevant CEPTOAR. In addition, responsible ministries for CIIP shall carry out information sharing related to IT outages and cyber-attacks as necessary. In the event there are any criminal damages, reports shall be made to the crisis management ministries based on independent decisions.

(2) CEPTOAR

Cooperates with the CEPTOAR council, responsible ministries for CIIP and CIIP supporting agencies to carry out mutual sharing of IT outage and cyber-attack related information, recovery method information, early warning information, etc.

(3) the 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 range of information sharing aimed at CII operator service maintenance and recovery.

(4) Responsible ministries for CIIP

Carry out sharing to the Cabinet Secretariat (NISC) of IT outage and cyber-attack related information received from CII operators over which the ministries have jurisdiction. Also carry out information sharing to CEPTOAR under the jurisdiction of the ministries as necessary. Carries out information sharing to CEPTOAR under the jurisdiction of the ministries for IT outage and cyber-attack related information, recovery method information and early warning information received from the Cabinet Secretariat (NISC).

(5) Cabinet Secretariat (NISC)

Carries out reciprocal sharing of IT outage and cyber-attack related information and recovery method information with responsible ministries for CIIP, CIIP supporting agencies from whom requests for cooperation were received in advance and cyberspace-related operators.

2.4.2 Responsibilities of each stakeholder in the information sharing during IT crises

In the event of an IT crisis resulting from disaster, terrorism or similar causes, collection and sharing of information related to the emergency shall be carried out between relevant ministries in accordance with *"Regarding the Government Initial Response System for Emergencies"* (November 21, 2003, Cabinet resolution). If the situation worsens and shifts to IT crisis response, the centralization of information in the crisis management ministries and the disaster prevention related ministries is important, so the information sharing system shall be laid out as follows.

(1) Cabinet Secretariat (Situations Response and Crisis Management)

Is integrated with the Cabinet Secretariat (NISC) and collects damage information provided by the crisis management ministries and the disaster prevention related ministries as well as response conditions information and carried out reciprocal information sharing with the Cabinet Secretariat (NISC).

(2) Cabinet Secretariat (NISC)

Is integrated with the Cabinet Secretariat (NISC) and carries out reciprocal sharing of various related information and recovery method related information with responsible ministries for CIIP, CIIP supporting agencies from which requests for cooperation were received in advance as well as cyberspace-related operators.

(3) Responsible ministries for CIIP

In addition to roles during normal times, shall also cooperate with system for IT crisis response as necessary.

(4) CII operators

In addition to roles during normal times, shall also construct system for IT crisis response as stipulated by CII operators.

(5) CEPTOAR

In addition to roles during normal times, shall also construct system for IT crisis response as stipulated by each CEPTOAR.

(6) the CEPTOAR council

In addition to roles during normal times, shall also construct system for IT crisis response as stipulated by each CEPTOAR.

3. ENHANCEMENT OF INCIDENT RESPONSE CAPABILITY

During the term of this Basic Policy, in addition to cross-sectoral exercises in the Second Basic Policy, relevant exercises and trainings in order to improve IT incident response capability and verification, are positioned as part of a policy of strengthening IT incident response systems. And the Basic Policy attempts to maintain and improve capability for CIIP as a whole by understanding the mutual relationships among these exercises and trainings and linking them.

Among the exercises and trainings, based on the achievement until now, the Basic Policy aims at continuing to enhance the positioning of cross-sectoral exercises as core means of strengthening the IT incident response system in CII sectors. In detail, the cross-sectoral exercises should be mutually linked and complement the CEPTOAR training and other exercises and training implemented by responsible ministries for CIIP, and enhance the vertical-directional systems within each CII sector and the horizontal-directional systems between CII sectors in order to reap synergistic benefits.

In addition, because rapid crisis management becomes necessary in order to prevent spread of damages, stakeholders implement measures and support policies to improve the IT incident response capability of CII operators, while continuing to clarify the roles and enhance cooperation between stakeholders.

3.1 Improvement of cross-sectoral exercises

During the term of this Basic Policy, the Cabinet Secretariat continues to implement the cross-sectoral exercises, which are the only initiative in Japan, while constantly improving them in order to contribute to the maintenance and improvement of protective capability for CII through the promotion of the relevant exercise results to the entire CII sector.

In implementing cross-sectoral exercises, in line with the 3 objectives given in the Second Basic Policy, those are "formation of a common awareness of cross-sectoral threats", "improving the response capability of one's own sector by understanding the response conditions of other sectors" and "acquiring policies for operating public-private information sharing more effectively", the Basic Policy aims to enhance cross-sectoral exercises using accumulated operation methods and results in order to contribute to the enhancement of the incident response system.

3.1.1 Planning of cross-sectoral exercises

During the term of this Basic Policy, the Cabinet Secretariat surveys plans for exercises including participation of stakeholders closely related to the maintenance of IT systems

possessed by CII operators, as well as knowledge and issues obtained through exercise operation issues from other policies, and latest trends related to risk sources which are a cause of IT outages, in order to improve continually cross-sectoral exercises.

In addition, the Cabinet Secretariat carries out verification aimed at improvement of the exercise results assessment process, in order to contribute to the further enhancement of verification related to CII operator measures for CIIP, IT outage early recovery process and IT-BCP.

The Cabinet Secretariat provides knowledge and issues obtained through the exercises as basic data to other policies in this Basic Policy.

3.1.2 Promotion of lessons learned from cross-sectoral exercises

During the term of the Second Basic Policy, the number of exercise participants steadily increased, and the percentage of participants who assessed the exercises as meaningful exceeded 80%. The Basic Policy aims at the promotion of exercise results in CII sectors through promoting new participation from individuals who had not yet participated in the exercises. However, as there is a limitation of participation increase to some degree, it is necessary to promote increasing the number of participation and provide activities targeting CII operators that do not participate in the exercises, in order to further propagate and promote exercise results to overall CII.

For this activity, the Cabinet Secretariat creates and releases explanation materials regarding the merits of exercises which can contribute to the promotion of increase understanding by executives and senior managers, and make appeals to overall CII sectors, and thereby promote implementation of exercises in each CII sector and at each CII operator.

In addition, the Cabinet Secretariat promotes survey the arrangement and sharing of implementation, assessment and advising methods accumulated from past exercises in order to contribute to the support of exercise implementation by individual CII operators.

3.1.3 Response to IT outages from physical causes

In actual IT incident response, it may include IT outages resulting from physical causes, and depending on the circumstances it may be necessary to share information not only with the various ministries and business information security departments, but also with disaster and crisis management departments.

Hereafter, the Cabinet Secretariat, when making response to relevant IT outages subject to verification, when necessary in creation of scenarios, study the conditions for utilization of knowledge from the disaster prevention related ministries and cooperation with the crisis management supervisors at responsible ministries for CIIP and CII operators.

3.1.4 Cooperation with responsible ministries for CIIP

It is expected to work to maintain and improve effective and efficient protective capability for CII by implementing these exercises and training to reciprocally cooperate with and complement the cross-sectoral exercises, while exercises and training contributing to CIIP implemented by the responsible ministries for CIIP have different expected results from the cross-sectoral exercises implemented by the Cabinet Secretariat.

For this reason, the Cabinet Secretariat and responsible ministries for CIIP consider conditions for clarification and mutual cooperation of verification purposes and the main targets for the exercises implemented by each exercises in order to improve the response capability of CII operators.

As an example of verification survey items, it would be possible to target information sharing and collaborative response between CII operators, CEPTOAR, responsible ministries for CIIP and the Cabinet Secretariat as verification targets in cross-sectoral exercises, and to target IT incident response procedures using actual systems at CII operators and contact systems in each sector for checking and verification in exercises by the responsible ministries for CIIP.

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 CIIP.

In implementation CEPTOAR training, the Cabinet Secretariat aims to enhance substantial training content while also incorporating requests from CEPTOAR and to realize information sharing training which is suited to actual conditions, bearing in mind response during IT outages.

In addition, the Cabinet Secretariat considers collaboration, as necessary, such as setting conditions based on the verification details of cross-sectoral exercises between cross-sectoral exercises and CEPTOAR training, because the participation of a large number of CII operators can be expected in CEPTOAR training.

4. RISK MANAGEMENT

CII operators should establish objectives related to information security and deploy the objectives within their organizations in order to achieve business goals such as stable provision of CII services to the people and business continuance.

On the other hand, as the social and technological environments surrounding CII continually change, the dependence on cyberspace of information systems used in the CII and of the data utilized in these systems continues to increase.

In these conditions, the effects of IT failures caused by risk sources, such as the threats and vulnerabilities lurking in cyberspace, also increase, and if and IT failure did occur, it could make provision of CII services difficult.

For this reason, it is necessary for CII operators to carry out not only comprehensive management of risks deriving from risk sources related to information security but also just the symptomatic measures for IT failures, aimed at achieving business goals.

In order to focus on risk management methods at CII operators, the "common threat analysis" and "development of risk communication" (one of the policy of "response to environmental change") in the *Second Action Plan* are more comprehensively considered and activities related to risk management carried out by each CII operator are newly implemented.

4.1 Basic view of risk management

Risk management should be independently implemented by each CII operator. However, in circumstances where each stakeholder does not have common risk management views or terms for information sharing and discussion, there is a possibility that the activities in this Basic Policy will not be effectively utilized in the risk management of each CII operator.

For this reason, it is preferable for each stakeholder to utilize the internationally standard views of management and related terminology definitions for information security etc. in the term of this Basic Policy.

In detail, the Cabinet Secretariat, as far as possible, utilizes views based on the framework[12] noted in Table 3 below and the terminology definitions used in the framework in the activities implemented by the Cabinet Secretariat and in related materials.

[12] Refer to *JIS Q 31000:2010* and *"Risk Management - Principles and Inventories for Risk Management / Risk Assessment methods and tools"* released by ENISA (European Union Agency for Network and Information Security).

Table 3. 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	

In addition, it is expected that CII operators will utilize the guidebooks[13] created by the Cabinet Secretariat in their own organization's risk management.

However, this activity does not require each stakeholder to conform with international standards, but rather is aimed at contributing to an increase in the level of information security and more optimized risk management already being implemented at CII operators by referring to the views and terminology definitions applied by the Cabinet Secretariat.

4.2 Support for risk management

Risk management is generally optimized by each CII operator individually to suit their organization. On the other hand, in risk assessment[14] and risk communication and consultation[15], there are some activities which cannot be handled easily by only CII operator, such as cross-sectoral study/analysis and opinion exchanges.

For this reason, the Cabinet Secretariat carries out cross-sectoral activities as follows, and supports risk management implemented at CII operators by sharing the results of cross-sectoral studies/ analyses and providing opportunities for cross-sectoral opinion exchanges.

4.2.1 Risk assessment

The Cabinet Secretariat analyzes conditions and trends of major facilities and technologies in regard to changes in the environments surrounding CII sectors, as well as risk sources inherent to major facilities and technologies and new risks derived from the risk sources (hereinafter referred to collectively as "new risk sources and risks").

In addition, the Cabinet Secretariat analyzes the influence of effects of IT outages.

In detail, the following activities are carried out, also taking into account viewpoints of the

[13] In *"5.3.3 5.3.3 Preparation of guidance to apply international standards"*, it is specified that guidebooks, etc. which interpret international standards, shall be prepared as necessary.

[14] According to *JIS Q 31000:2010*, this is defined as *"overall process of risk identification, risk analysis and risk evaluation"*.

[15] Refer to *"4.2.2 Risk communication and consultation"* for definition.

efficiency of each study/analysis and mutual reflection with other policies, and the results of the studies/analyses are provided to CII operators.

(1) Environmental change studies

In the environmental change studies implemented in the *Second Action Plan*, it turned out that the adoption ratios of cloud, smartphone/tablet device and remote maintenance were high and the adoption of BYOD[16] and big data would increase going forward in CII sectors.

In this Basic Plan, based on these changes, the Cabinet Secretariat carries out environmental change studies including analysis of new risk sources and risks as well as condition surveys for new technologies and systems which are expected to introduce to CII sectors into mid to long term, such as M2M and smart communities. In addition, the Cabinet Secretariat carries out this study across years, because these changes will be appeared over time. With regard to these studies, new risk sources and risks which could have a major effect, even if they are common across specific sectors (ex. Control systems, accounting systems and information systems) will also be targeted.

In the event new risk sources and risks are identified through these studies, or in the event new CII sectors are added, detailed investigation and analysis of commonality across these sectors shall be carried out as necessary.

(2) Interdependency analysis

As utilization of IT continues to develop in each CII sectors and interdependent relationships between sectors continue to grow, the understanding of interdependency in CII sectors becomes more important for effective recovery measures in the event of an IT outage.

For this reason, in this Basic Policy, the Cabinet Secretariat carries out interdependency analysis, including restudy or reanalysis based on the results from the *First Action Plan* and the *Second Action Plan* in the event of changes in interdependency due to environmental changes or addition of new CII sectors.

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

In the event new CII sectors are added, IT dependency studies will also be carried out as a part of interdependency analysis.

4.2.2 Risk communication and consultation

Risk communication and consultation is defined as *"continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue*

[16] Bring Your Own Device. A situation where, in a business or other setting, employees access company information, using their personal information devices to view, edit and otherwise manipulate the required information for work.

with stakeholders regarding the management of risk".[17]

The Cabinet Secretariat supports risk communication and consultation implemented by stakeholders related to CII protection for the purposes of contributing to the development of cross-sectoral information and opinions exchanges among them.

In detail, the CEPTOAR council and cross-sectoral exercises are utilized to provide opportunities for information and opinion exchange maintaining cooperation with each stakeholder.

This activity also promotes the collection of information necessary for the study/analysis in this policy.

4.3 Establishing a process of synergizing the relevant policies

The Cabinet Secretariat shall provide the results of studies and analysis in this policy as basic data for other policies for the purpose of contributing to the other policies in this Basic Policy.

In addition, new risk sources and risk required cross-sectoral measures appeared from results of the implementation of other policies are subject to the studies/analyses of this policy.

[17] Refer to *JIS Q 31000:2010*.

5. ENHANCEMENT OF THE BASIS FOR CIIP

As the social and technological environments etc. surrounding CII continue to constantly change, as shown in Figure 1, it is necessary to enhance common foundation activities which support the entire Basic Policy, for maintenance of the effectiveness of measures for CIIP. The activities include establishment of basic plan, human resource development/assignment, external explanations of measures for CIIP and identification of issues for risk sources resulting from IT related environmental change.

Therefore, during the term of this Basic Policy, the Cabinet Secretariat prepares guides on international standards, etc. related information security and relevant regulations related to CIIP in order to allow stakeholders to reference suitable, related regulations, etc. as necessary, in addition to continuing the cooperation with other stakeholders, public relations activities and international cooperation from Second Basic Policy.

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

5.1 Public relations activities

In order to minimize the effects of IT outages to the smallest degree possible, it is important to not only raise the standard of measures for CIIP implemented by CII operators, but also to ensure that the people are able to calmly respond to such outages based information on the situation.

Therefore, each stakeholder attends to continue to provide explanations to the people through the publicity of the activities based on this Basic Policy, in order to contribute to a calm response from the people.

In order to raise the level of measures for CIIP implemented by CII operators, it is important to obtain a wide range of cooperation and support for the initiatives based on this Basic Policy.

The Cabinet Secretariat continues to carry out public relations activities through publicity through websites and newsletters, lectures and other means. When doing these activities, the publicity should be structured so as to achieve awareness and understanding of the initiatives of this Basic Policy.

5.2 International cooperation

In cyberspace, risks have been growing in borderless domain, it is required to further respond to these global risks which have no national boundary, and it becomes necessary to

positively contribute to capacity building so that our country would improve the level of international measures for CIIP as well as ourself.

Therefore, the Cabinet Secretariat cooperates with responsible ministries for CIIP and the CIIP supporting agencies and continue to enhance international cooperation through active utilization of bilateral, inter-regional and multilateral frameworks such as those with the US and Europe, ASEAN and Meridian. When doing these activities, it actively provides case examples, best practices and other items obtained through international cooperation to domestic stakeholders.

In addition, diversified and multilateral international cooperation is also expected at CII operators as a result of the deployment of initiatives related to measures for CIIP being deployed to other companies in the same industry overseas, identification of overseas trends, etc.

5.3 Maintenance of reference of standards and guides

To maintain the effectiveness of measures for CIIP, it is important that stakeholders are able to reference relevant documents and regulations where necessary when examining means to do so. The initiatives of the Cabinet Secretariat related to the preparation of these regulations etc. are as follows.

5.3.1 Issuance of the reference book for CIIP

The Cabinet Secretariat compiles relevant documents including the *Cybersecurity Strategy* and this Basic Policy for common reference by stakeholders, and issue the compiled documents as the "Collection of regulations related to measures for CIIP" for the purpose of equalizing the knowledge base of stakeholders involved in CIIP.

5.3.2 Systematic arrangement of relevant standards and guides

For related regulations for CIIP, the Cabinet Secretariat, with the cooperation of the other stakeholders, arranges domestic and overseas related regulations and clearly states the results in order to refer appropriate version when necessary.

5.3.3 Preparation of guidance to apply international standards

As the social and technological environments etc. surrounding CII continue to constantly change, in order to quickly and flexibly respond to these changes, it may be effective in case that the stakeholders utilize appropriate relevant regulations identified from the results compiled from *"5.3.2 Systematic arrangement of relevant standards and guides"*, particularly the international standards, etc.

However, when attempting to utilize the international standards, etc. which set out general

principles based on the above compiled results, reinterpretation may be necessary for items that would not be able to directly apply to.

The Cabinet Secretariat, with the cooperation of other stakeholders, compiles guides as necessary in order to allow for the relevant international standards etc. to be applied to fast and flexible response.

In keeping with the fact that international guidebooks, etc. related to CIIP do not currently exist, the Cabinet Secretariat considers proposal of the guidebooks, etc. compiled as part of this policy to the various countries of ASEAN and for ISO and other international standards as a means of global contribution.

5.3.4 Promotion of assessment and certification system for CIIP

The Cabinet Secretariat, with the cooperation of other stakeholders, support[18] the expansion of third party certification systems for control equipment and systems regarding the circumstances of the adoption of assessment and certification which conforms with international standards related to control equipment and systems under further consideration.

[18] Implemented with cooperation from the Technological Research Association Control System Security Center (CSSC) which works on the adoption of third party certification systems for control equipment and systems.

IV. ACTIVITIES TO BE TAKEN BY STAKEHOLDERS

The information security policy groups indicated in this Basic Policy are supported by independent measures which it is preferable for CII operators to handle, and policies which it is preferable for government organizations etc., centering on the Cabinet Secretariat, to implement. It is expected that stakeholders will each promote measures for CIIP using the following as a basis.

1. ACTIVITIES BY CABINET SECRETARIAT

(1) Maintenance and promotion of the safety principles

a) During the first fiscal year of this Basic Policy and as necessary thereafter, implement studies related to the amendment of the Guidelines for safety principles after strengthening links to other policies and officially release the results.

b) As necessary, implement studies related to the changes in social trends and newly obtained knowledge after strengthening links to other policies and officially release the results.

c) Support the continued improvement of the CII sector safety principles through a) and b) above.

d) Continue to obtain the cooperation of the responsible ministries for CIIP, implement studies every year to determine the conditions of the continued improvement of the safety principles in each CII sector and officially release the results.

e) Continue to obtain the cooperation of the responsible ministries for CIIP, implement studies every year on the conditions of the promotion of the safety principles and officially release the results.

(2) Enhancement of information sharing system

a) Increase promotion and revise when necessary through operation of the information sharing system during normal times and during IT crises.

b) Collect information to be provided to CII operators and share information from NISC in an appropriate and timely manner.

c) Continue to obtain the cooperation of the responsible ministries for CIIP, periodically implement studies, hearings, etc. in order to determine the conditions, etc. of each CEPTOAR's functions and activities.

d) Introduce advanced CEPTOAR functions and activities.

e) Continue cooperating with CEPTOAR participating in the CEPTOAR council and implement support for management and activities.

f) Prepare environments required for enhancement of CEPTOAR council activities, and

accumulate and share know-how.

g) Build individual cooperation with cyberspace-related operators as necessary, and implement appropriate and timely information sharing from NISC during IT outages.

(3) Enhancement of incident response capability

a) Determine other ministries' IT outage handling exercises and training information, investigate cooperation conditions.

b) Continue to obtain the cooperation of the responsible ministries for CIIP, periodically and when requested by CEPTOARs, provide opportunities for verification (CEPTOAR training) of CEPTOAR information communication functions.

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

d) Study measures for improving cross-sectoral exercises.

e) Utilize the opportunities for cross-sectoral exercises, determine the conditions of risk analysis results verification, early recovery procedures implemented by CII operators during IT outages, and IT-BCP etc. studies, and provide the results to exercise participants, etc.

f) Collect, accumulate and provide knowledge related to cross-sectoral exercise implementation methods, etc.

g) Diffuse and spread knowledge related to CII protection gained from cross-sectoral exercises.

(4) Risk management

a) Cultivate a shared awareness among stakeholders by presenting guidebooks which interpret international standards, definition usage and standard views for risk management.

b) Support risk management at CII operators through the study and analysis of this policy.

c) Provide the results of the studies and analysis in this policy as basic data to be reflected in the safety principles.

d) Support the risk communication and consultation of CII operators through CEPTOAR council and cross-sectoral exercises.

(5) Enhancement of the basis for CIIP

a) Carry out public relations activities through publicity through websites and newsletters.

b) Implement public relations activities through lectures, etc.

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

d) Actively provide case examples, best practices and other items acquired through international cooperation with domestic stakeholders.

e) Compile relevant documents for common reference by stakeholders, and issue a collection of regulations for the purpose of equalizing the knowledge base of stakeholders involved in CII protection.

f) Arrange and visualize related regulations.

g) Compile guidebooks as necessary in order to allow for international standards etc. to be applied to fast and flexible response.

h) Support the expansion of third party certification systems for control equipment and systems.

2. ACTIVITIES BY RESPONSIBLE MINISTRIES FOR CIIP

(1) Maintenance and promotion of the safety principles

a) Provide information, etc. related to the safety principles which can be newly positioned as the Guidelines for safety principles to the Cabinet Secretariat.

b) When the organization determining the safety principles, in addition to implementing periodic analysis and verification of the safety principles, amend the safety principles as necessary.

c) When not the organization determining the safety principles, support the analysis and verification of the safety principles for each CII sector.

d) Carry out promotion of safety standards for CII operators including environmental arrangement for packaging measures.

e) Cooperate with building an understanding of the conditions of the safety principles implemented by the Cabinet Secretariat every year.

f) Cooperate with studies of the conditions of the promotion safety principles implemented by the Cabinet Secretariat every year.

(2) Enhancement of information sharing system

a) Continue to cooperate with the Cabinet Secretariat and operate the information sharing system.

b) Maintain a close information sharing system with CII operators.

c) Carry out information sharing to the Cabinet Secretariat of reports related to IT outages received from CII operators.

d) Cooperate with studies and hearings implemented by the Cabinet Secretariat for determining the conditions of activities and functions of each.

e) Support the development of CEPTOAR functions.

f) Support the CEPTOAR council.

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

(3) Enhancement of incident response capability

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

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

c) Participate in cross-sectoral exercises.

d) Support participation in CEPTOAR and CII operator cross-sectoral exercises.

e) Cooperate with study of measures for improving cross-sectoral exercises.

f) As necessary, utilize results of cross-sectoral exercises in policies.

g) Cooperate with mutual collaboration between exercises and training which contributes to CII protection implemented by the responsible ministries for CIIP and cross-sectoral exercises.

(4) Risk management

a) Provide to the Cabinet Secretariat information related to the application required for study and analysis in this policy or information needed for the relevant study and analysis.

b) Apply to the studies and analysis policies in this policy.

c) Support the risk communication and consultation of CII operators.

(5) Enhancement of the basis for CIIP

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

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

c) Cooperate with the Cabinet Secretariat and arrange and visualize related regulations.

d) Cooperate with the Cabinet Secretariat and compile guidebooks as necessary in order to allow for international standards etc. to be applied to fast and flexible response.

e) Cooperate with the Cabinet Secretariat and support the expansion of third party certification systems for control equipment and systems.

3. ACTIVITIES BY INFORMATION SECURITY RELATED MINISTRIES

(1) Enhancement of information sharing system

a) Continue to cooperate with the Cabinet Secretariat and operate the information sharing system.

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

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

4. ACTIVITIES BY CRISIS MANAGEMENT MINISTRIES

(1) Enhancement of information sharing system

a) Continue to cooperate with the Cabinet Secretariat and operate the information sharing system during IT crises.

b) Collect disaster information, terrorism related information, etc.

c) Carry out information sharing to the Cabinet Secretariat as necessary.

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

(2) Enhancement of incident response capability

a) Implement support measures for improving IT outage response capability when requested by CII operators.

5. VOLUNTARY ACTIVITIES BY CII OPERATORS

(1) Maintenance and promotion of the safety principles

a) When the organization determining the safety principles, in addition to implementing periodic analysis and verification of the safety principles, amend the safety principles as necessary.

b) When the organization determining the safety principles, cooperate with building an understanding of the conditions of the safety principles implemented by the Cabinet Secretariat every year.

c) Study environmental arrangement for packaging measures and implementing measures for CIIP based on the safety principles.

d) Identify issues from operation of measures for CIIP, internal and external audits, environmental change studies/analysis results related to IT, exercises/training and response to IT outages, and continually amend safety principles through risk assessment.

e) Cooperate with studies of the conditions of the promotion safety principles implemented by the Cabinet Secretariat every year.

(2) Enhancement of information sharing system

a) Continue to cooperate with the CEPTOAR council, CEPTOARs and the responsible ministries for CIIP, and operate the information sharing system.

b) Carry out information sharing to the NISC as necessary during IT outages.

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

d) Carry out supplemental information sharing based on consensus with the CIIP supporting agencies.

e) Implement activities in the CEPTOAR council.

(3) Enhancement of incident response capability

a) Utilize, etc. verification (CEPTOAR training) etc. information communication functions provided by the Cabinet Secretariat and enhance own information sharing system.

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

c) Participate in cross-sectoral exercises.

d) Cooperate with study of measures for improving cross-sectoral exercises.

e) Utilize the results of cross-sectoral exercises for early recovery method and IT-BCP etc. initiatives as necessary in the event of own IT outages.

(4) Risk management

a) Promote and enhance risk management in own organization.

b) Utilize the basic information provides as the results of the study and analysis of this policy in own organization's risk assessment.

c) Develop risk communication and consultation between stakeholders directly involved in measures for CIIP.

d) Propose environmental changes and risk sources which are difficult to analyze oneself but for which there is a value for conducting study and analysis as targets for the study and analysis of this policy.

e) Participate in the discussion and examination of the study and analysis of this policy.

(5) Enhancement of the basis for CIIP

a) Promote diverse and multilateral international cooperation through the deployment of initiatives related to measures for CIIP being deployed to other companies in the same industry overseas, determination of overseas trends, etc.

b) Cooperate with the Cabinet Secretariat and arrange and visualize related regulations.

c) Cooperate with the Cabinet Secretariat and compile guidebooks as necessary in order to allow for international standards etc. to be applied to fast and flexible response.

d) Cooperate with the Cabinet Secretariat and support the expansion of third party certification systems for control equipment and systems.

6. VOLUNTARY ACTIVITIES BY CEPTOAR

(1) Enhancement of information sharing system

a) Continue to cooperate with the CEPTOAR council, CII operators and the responsible ministries for CIIP, and operate the information sharing system.

b) Carry out information sharing from NISC to CII operators in accordance with the information handling rules for information provided from the Cabinet Secretariat.

c) Carry out supplemental information sharing based on consensus with the CIIP supporting agencies.

d) Enhance and develop CEPTOAR functions.

e) Cooperate with studies and hearings implemented by the Cabinet Secretariat for determining the conditions of activities and functions of each.

f) Participate in the CEPTOAR council.

(2) Enhancement of incident response capability

a) Carry out periodic verification of information communication functions.

b) Support participation and development of results in CII operator cross-sectoral exercises.

c) Participate in cross-sectoral exercises.

(3) Risk management

a) Support independent initiative for the CII operators which make up own CEPTOAR.

7. VOLUNTARY ACTIVITIES BY THE CEPTOAR COUNCIL

(1) Enhancement of information sharing system

a) Continue to cooperate with each CEPTOAR and operate the information sharing system.

b) Carry out arrangement of information to be shared and sharing methods.

c) Promote cross-sectoral information sharing through sharing of specific examples of mutual understanding and best practice.

d) 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

a) Participate in cross-sectoral exercises as necessary.

8. VOLUNTARY ACTIVITIES BY CIIP SUPPORTING AGENCIES

(1) Enhancement of information sharing system

a) Continue to cooperate with the Cabinet Secretariat and operate the information sharing system.

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

c) Carry out supplemental information sharing based on consensus with the CII operators carrying out the information sharing or the CEPTOAR.

d) Cooperate with the examination of enhancement of analysis functions implemented by the Cabinet Secretariat.

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

(2) Enhancement of incident response capability

a) Provide information, related to IT outage case examples required for cross-sectoral exercises to the Cabinet Secretariat.

(3) Enhancement of the basis for CIIP

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

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

9. VOLUNTARY ACTIVITIES BY CYBERSPACE-RELATED OPERATORS

(1) Enhancement of information sharing system

a) Cooperate with initiatives for preparing information to be subject to sharing by the Cabinet Secretariat and the sharing methods for said information.

b) Carry out proactive information sharing to the Cabinet Secretariat as necessary during IT crises.

V. ASSESSMENT, VERIFICATION AND REVISION

For assessment of this Basic Policy, verification of results during the term of the Basic Policy is carried out from 2 viewpoints consisting of verification of the progress each fiscal year from a "view of measuring output", which looks at what kind of output each initiative has generated, and verification of results during the term of the Basic Policy from a "view of measuring outcomes", which looks at what degree society has actually moved closer to the ideal future image as a result of the initiatives of this Basic Policy. During this, use objective indexes as much as possible for progress verification and for verification of results carry out comparison with the goals of this Basic Policy which are the ideal future image.

In addition, the "verification" in this Basic Policy, shall refer to the use of indexes to objectively verify actual conditions related to progress of each of the initiatives.

1. GOALS TO BE ACHIEVED DURING THE TERM OF THIS BASIC POLICY

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

* The independent initiatives of each stakeholder based on the stakeholder's own awareness prevail in the codes of conduct of each stakeholder and the resulting behavioral patterns form a culture of information security.
* Communication for enhancing measures for preventing IT outages is carried out between stakeholders on a daily basis, and continual improvements are carried so that experience gained in the event of an IT outage can be reliably utilized in future measures.
* The CII protection initiatives cooperatively carried out by stakeholders are widely known to the public providing a sense of security. In addition, there is substantial communication between a wide variety of stakeholders allowing for calm coping in the event of an IT outage.
* These types of initiatives are officially released as a Basic Policy which undergoes periodic assessment and is appropriately revised as necessary.
* Each of the stakeholder initiatives is reliably established as an item which supports continued development of society.

Hereafter, detailed future images are described.

1.1 For all stakeholders

Detailed future images common to all stakeholders are as follows.

* The stakeholder possesses an accurate awareness of its own conditions and independently establishes its own activity goals.

* All required initiatives are progressing and periodic verification is carried out on the progress of the stakeholder's own measures and policies. The stakeholder is also able to maintain an understanding of the activity conditions of and proactively cooperate with other stakeholders.
* In response during IT outages, it is understood who should be collecting what kinds of information, who should be sharing what kinds of information and what the stakeholder themselves should be doing in accordance with the scale of the IT outage.
* In addition to being able to carry out independent response, the stakeholder is able to cooperate with other stakeholders when necessary to carry out controlled response.

1.2 For CII operators

Detailed future images for CII operators are as follows.

* There is sufficient saturation of the following items related to "information security governance".
  - Measures for CIIP are examined not just from information system construction and operation perspectives, but also from a business management perspective.
  - A system exists which allows for the appropriate involvement of each of the parties responsible for system construction and operation and business management.
  - There is an understanding of the measures to be implemented based on the CII services which require protection and service maintenance level.
  - Efforts are made to carry out external explanations of measures for CIIP.
  - A sense of values is cultivated in which carrying out information sharing to the greatest degree possible in order to improve the standard of measures for CIIP is viewed positively.
  - There is an awareness that the occurrence of IT outages is not something to be hidden but should instead be shared with stakeholders involved in measures at CII operators.
* There is sufficient saturation of the following items related to "issue identification", "risk assessment" and "improvement of measures".
  - Based on this Basic Policy, stakeholders cooperate to carry out measures for CIIP related to CII protection and are aware of remaining risks in their own measures and the extent of those risks.
  - Risk changes related to risk sources and IT outages resulting from developments of various measures and environmental changes are suitably detected, measures are independently advanced for each and necessary adjustment is carried out.
  - Appropriate measures are able to be enacted even in the event of an IT outage and as a result the risk of the IT outage having a serious effect on the public welfare and

socioeconomic activities is minimized to the greatest degree possible.

- These initiatives server as one driving force for the continued improvement of the measures.

* There is sufficient saturation of the following items related to "information sharing".
  - There is an understanding of IT outage conditions, relevant information is shared externally through each sector's CEPTOAR and CEPTOAR council as necessary, and official or unofficial cooperation is carried out.

1.3 For Cabinet Secretariat

Detailed future images for the Cabinet Secretariat are as follows.

* Works as a comprehensive coordination function for advancing more effective measures. Diverse information which contributes to measures for CIIP is able to be collected through the policy groups of this Basic Policy and cooperation is carried out with stakeholders based on the relevant information.
* Has obtained an understanding of risks related to serious risk sources and IT outages in particular, and quickly implements organic cooperation and coordination aimed at studying and realizing resolutions in the event the management of such is difficult for CII operators alone.

2. CONTINUAL IMPROVEMENT BASED ON ASSESSMENT AND VERIFICATION DURING EACH FISCAL YEAR

In order to steadily advance the initiatives based on this Basic Policy and carry out continual improvement, confirmation and verification shall be carried out on the progress of the Basic Policy. In continual improvement, each stakeholder shares the experiences they gain through their initiatives with the stakeholders as a whole, and focus is on utilizing these experiences to reciprocally improve each other's initiatives. IT outages should be avoided, however it is important to recognize that experience protecting against IT outages and experience limiting the scope of the effects in the event of an IT outage serve as provisions for the future.

While obvious, the party for which the IT outage occurs must bear responsibility for and determine the cause of the IT outage and strive to improve their own initiatives. However, in the assessment and verification of this Basic Policy, the principal focus is not placed on assigning responsibility and investigating causes, but rather on identifying lessons that can be used to improve future initiatives, and utilizing these to improve the initiatives of all stakeholders.

3. METHODOLOGY FOR ASSESSMENT AND VERIFICATION DURING EACH FISCAL YEAR

The confirmation and verification carried out each fiscal year from "view of measuring output" is carried out with a focus on the policy groups for individual measures for CIIP in accordance with this Basic Policy. Because all of the measures for CIIP policy groups based on this Basic Policy are all multilayered among multiple stakeholders, a wide variety of items can be imagined as indexes for use in verification, however broad categorizations will be set of indexes used for comprehensive confirmation and verification of measures by CII operators and indexes used for confirmation and verification of policies by government organizations. For the indexes for each measure for CIIP policy group, it is important to appropriately interpret the meaning of the values rather than to be overly-focused on the quantity or any fluctuations.

The confirmation and verification carried out each fiscal year from "view of measuring output" is carried out with a focus on the policy groups for individual measures for CIIP in accordance with this Basic Policy. Because all of the measures for CIIP policy groups based on this Basic Policy are all multilayered among multiple stakeholders, a wide variety of items can be imagined as indexes for use in verification, however broad categorizations will be set of indexes used for comprehensive confirmation and verification of measures by CII operators and indexes used for confirmation and verification of policies by government organizations. For the indexes for each measure for CIIP policy group, it is important to appropriately interpret the meaning of the values rather than to be overly-focused on the quantity or any fluctuations.

In addition, confirmation and verification of own measures by individual CII operators shall be considered an independent process, and in general it is preferable for the CII operator to carry out implementation every fiscal year.

3.1 Indexes for the assessment and verification of activities by CII operators

As the party with the most fundamental responsibility for the stable provision of CII services, CII operators must deal with measures for CIIP on a daily basis. In order to continually and steadily improve this initiatives and in order to make the support provided by the government for the initiatives of the CII operators more effective, it is important to objectively verify the the outcomes of the measures for CIIP.

The comprehensive confirmation and verification of the measures is the confirmation and verification of the conditions of the occurrence of IT outages for each CII sector based on the "preventing serious effects on the public welfare and socioeconomic activities due to IT

outages" which is the goal of this Basic Policy. The applicable CII services and service maintenance levels are as shown in *"ANNEX 2. CII SERVICES AND SERVICE MAINTENANCE LEVELS"*. Detailed indexes are figures from all IT outage case sectors recognized by the Cabinet Secretariat.

The measures of individual CII operators include independent measures based on the management decisions of each, and it is therefore inadequate to assess measures through comparison with IT outage conditions for each CII operator or each sector. For this reason, it is reasonable that assessment of measures should be carried out through self-assessment by the CII operators, and that each CII operator should work towards their own improvement. In addition, if possible, it is preferable that the conditions of the implementation of the self-assessment be made clear.

3.2 Indexes for the assessment and verification of activities by government organizations

The policies of this Basic Policy are as shown in *"III. POLICIES FOR CIIP"*, however these are all items for which government support is carried out to improve the effectiveness of measures for CIIP by CII operators. During the term of this Basic Policy, the method for verifying the effectiveness of each policy was revised while continuing to follow the indexes used in the Second Basic Policy.

The confirmation and verification of policies is the verification of the contribution to the measures for CIIP of CII operators for each measures for CIIP policy, and the detailed indexes are as follows.

3.2.1 Maintenance and promotion of the safety principles

The outcomes expected from "maintenance and promotion of the safety principles" are the stakeholders being involved in measures for CIIP understanding the measures which they are required to implement themselves and the further development of index and safety principle items and the reliable practical application of the items for the purpose of having the required initiatives carried out under periodic self-assessment. For this reason, indexes are set which focus on the development of the indexes and safety principle items and the reliable implementation of initiatives based on the safety principles of the CII operators.

<Detailed indexes>

* Number of measure items recorded in the index
* The ratio of CII operators carrying out periodic self-assessment based on the safety principles, etc. determined through studies on the promotion of the safety principles
* Opinions and requests from CII operators on indexes

3.2.2 Enhancement of information sharing system

The outcomes expected from "enhancement of information sharing system" are the ability to receive the information required by CII operators through complete enhancement of the independent activities of each CEPTOAR and CEPTOAR council in addition to information sharing based on the latest information sharing system as well as information sharing to and from NISC. For this reason, indexes are set which focus on the development of information shared with the prepared information sharing system.

<Detailed indexes>

* Number of cases of information sharing to and from NISC by the Cabinet Secretariat
* Number of occasions of information exchanges by CEPTOAR council and cross-sectoral exercise stakeholders
* Number of cases of information sharing in the CEPTOAR council

3.2.3 Enhancement of incident response capability

The outcomes expected from "enhancement of incident response capability" are contributions to the improvement of management capability technical aspects and verification of the validity of information sharing to and from NISC between stakeholders required for verification of CII operator implemented early recovery procedures during IT outages and IT-BCP through participation in exercises and training centering on cross-sectoral exercises. For this reason, indexes are set which focus on the contribution to CII operator initiatives of knowledge gained through participation in exercises and training in addition to the promotion of exercise results, construction of realistic exercise environments and cross-sectoral exercises.

<Detailed indexes>

* Number of participants in cross-sectoral exercises
* Ratio of participants who assess the information obtained through exercises as having contributed to the measures for CIIP of the organization to which they belong
* Participation in exercises and training implemented both inside and outside the organization, including cross-sectoral exercises

3.2.4 Risk management

The outcomes expected from "risk management" are the promotion and enhancement of risk management implemented by CII operators. For this reason, indexes are set which focus on consultation as well as risk assessment and risk communication supported by the Cabinet Secretariat from among the risk management processes implemented by CII operators.

<Detailed indexes>

* Number of cases of interdependency analysis and environmental change studies implemented by the Cabinet Secretariat
* Number of occasions of provision of opportunities for information exchange by

CEPTOAR council and cross-sectoral exercise stakeholders

3.2.5 Enhancement of the basis for CIIP

The outcomes expected from "enhancement of the basis for CIIP" are: for "public relations activities", obtaining the greatest degree of understanding from the public in relation to the framework of the Basic Policy and expanding the scope of those cooperating with this Basic Policy beyond just stakeholders; for "international cooperation", support and development of opportunities for information exchanges with various countries through bilateral, inter-regional and multilateral frameworks; and for "preparation of norms, standards and regulations, etc. for reference", the usage of the prepared regulations, etc. by CII operators. For this reason, indexes are set which focus on the development of opportunities to publicize this Basic Policy and international cooperation as well as the status of the preparation of the regulations, etc.

<Detailed indexes>

* Number of times information is dispatched through newsletters, etc.
* Number of times lectures, etc. related to the Basic Policy are held
* Number of times information exchanges etc. are held through bilateral, inter-regional and multilateral frameworks
* Conditions of preparation of guidebooks etc. which contribute to CII protection
* Expansion conditions of third party certification systems for control equipment and systems

4. RIVISION OF THE BASIC POLICY BASED ON THE ASSESSMENT OF THE OUTCOMES

The assessment carried out from the "view of measuring outcomes" is carried out in comparison with the goals of this Basic Policy which are the ideal future image. During this, in consideration that the various initiatives based on this Basic Policy are mutually related and to realize output and outcomes, assessment is not carried out for each individual initiative, but rather for overall initiatives which contribute to the maintenance and improvement of protective capability for CII, and so is thus carried out comprehensively and analytically for the framework of this Basic Policy.

When carrying out assessment of the framework of this Basic Policy, it is important to carry out assessment after appropriately determining the conditions which cannot be completely determined through only the individual output and outcomes of policy groups. For this reason, in order to collect the supplementary information required for assessment, supplementary studies shall be carried out one per fiscal year in principle.

In addition, for assessment management, as it is difficult to examine improvement measures immediately even if changes are tracked each year, so in principle 1 time per 3 years assessment shall be carried out by the Information Security Policy Council, and the studies and examination required shall be carried out by the CII Specialist Committee through cooperation from the responsible ministries for CIIP.

As such, for the revision of the Basic Policy based on the assessment of outcomes as well, in principle 1 time per 3 years the assessment shall be carried out by the Information Security Policy Council, and the studies and examination required shall be carried out by the CII Specialist Committee through cooperation from the responsible ministries for CIIP.

The limitation of 1 time per 3 years shall not apply in the event of any events occurring outside the assumptions of this Basic Policy such as serious changes in social trends.

ATTACHMENT: "INFORMATION SHARING TO NISC" AND "INFORMATION SHARING FROM NISC"

1. INFORMATION RELATED TO IT FAILURES, ETC

"Information related to IT failures, etc." is an extensive variety of information which contributes to measures for CIIP related to IT failures, including IT outages, signs and "Hiyari-Hatto".Information related to IT failures, etc. includes 3 aspects of (1) proactive prevention of IT outages, (2) prevention of the spread damages and quick recovery from IT outages, and (3) prevention of recurrence through analysis and verification of IT outage causes, and must be provided suitably and appropriately to CII operators by government organizations, etc., and enhancement of a system for sharing this type of information among CII operators and interdependent CII sectors.

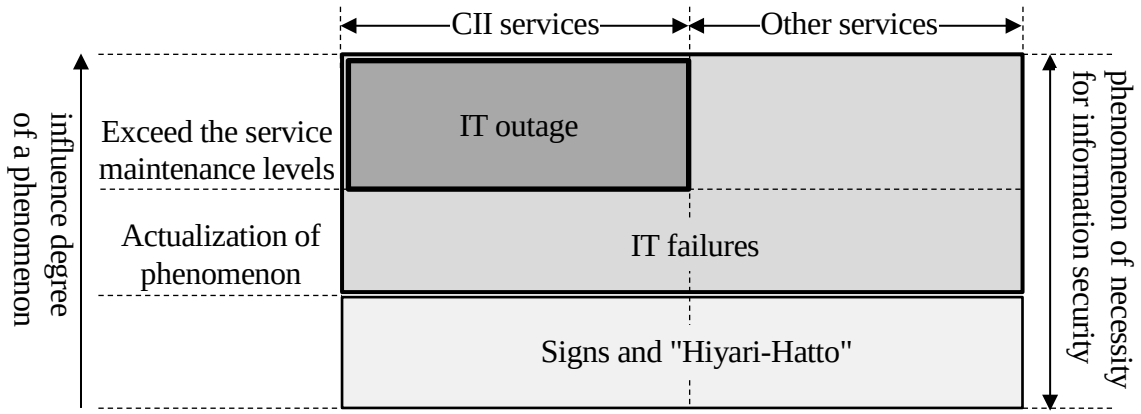
The various aspects of information related to IT failures, etc. include the following.

a) Proactive prevention: Information related to causes of IT failures (including protective measures, etc.)
b) Prevention of spread, and recovery: Information which contributes to effect propagation prediction and recovery after IT outages
c) revention of recurrence: Collaborative collection of information which contributes to ex-post analysis as well as analysis and verification results

In addition, by signs and "Hiyari-Hatto", although the phenomenon is not actualizing, when it actualizes, resulting in IT failure is also considered. Therefore, it is required like the IT failure to also make an omen into the object of information sharing.

Therefore, the scope of information sharing in this basic policy is as being shown in the figure 2.

figure 2. Scope of information sharing



2. INFORMATION SHARING TO NISC FROM CII OPERATORS

2.1 In case of "information sharing to NISC"

Occasions when information sharing to NISC is necessary shall be situations where IT failures, including IT outages, signs or Hiyari-Hatto are confirmed, situations where reporting is required by laws, etc., or situations CII operators have determined that sharing of information is appropriate.

In the event it is uncertain whether or not the above are applicable, it is recommended that the responsible ministries for CIIP or Cabinet Secretariat be consulted.

2.2 Contents of "information sharing to NISC"

The details of information sharing to NISC shall be the on demand reporting of identified events and causes at the time of the report. It is acceptable if the information at this time is fragmentary or indefinite because the complete picture has yet to be identified.

In addition, the setting of common classifications and categories for IT failures, etc. required when information sharing to NISC is carried out from the responsible ministries for CIIP to the Cabinet Secretariat, shall be carried out with consideration for the operability etc. of each CII operator.

2.3 Framework for "information sharing to NISC"

The procedures for sharing of information to NISC from CII operators to the Cabinet Secretariat through the responsible ministries for CIIP are as follows.

a) CII operators shall share information to the responsible ministries for CIIP in accordance with the contact system illustrated in *"ANNEX 5. COMMUNICATION CHANNELS UNDER IT OUTAGES"*.

b) The responsible ministries for CIIP liaison shall share the information received from the CII operator of the relevant sector to the Cabinet Secretariat.

c) The Cabinet Secretariat shall appropriately manage the shared information, and handle the information within the information sharing scope specified by the information source.

2.4 Handling of "information sharing to NISC"

For the handling of information shared to NISC, the Cabinet Secretariat and the responsible ministries for CIIP that received the information shall in principle, where not otherwise specified by law or agreed to by the CII operator submitting the information, handle said information as the information (voluntarily provided information) prescribed in Article 5 Item

2 of the Act on Access to Information Held by Administrative Organs (Law 42 of 1991). In cases where the relevant information is subject proviso in the same item, the information may be publically disclosed.

3. INFORMATION SHARING FROM NISC TO CII OPERATORS

3.1 Scope of CII operators subject to "information sharing from NISC"

The scope of provision of information to CII operators from the Cabinet Secretariat shall be the CII sectors which the Cabinet Secretariat deems the information relevant to, from among the information sharing scope specified by the information provider in advance. In cases where the Cabinet Secretariat deems it is necessary to share information outside of the information sharing scope specified by the information provider, it shall be able to coordinate the change of the sharing scope with the information provider.

3.2 Contents of "information sharing from NISC"

Information sharing from NISC shall be carried out for information considered to be effective for CII operator measures for CIIP from a wide range of information which is collected and analyzed from information provided by responsible ministries for CIIP, information security related ministries, CIIP supporting agencies and cyberspace-related operators.

In addition, if the information provided from the CII operators is applicable to a) or b) below, information sharing shall be carried out after employing appropriate measures such as processing the information so that the providing CII operator cannot be identified in order to prevent the CII operator providing the information from suffering any disadvantage as a result.

a) If the obtained information is regarding a security hole, program bug, etc. and it is recognized that said information could cause problems at other CII operators.
b) If there is a cyber-attack or advance notice of such an attack, if there are predicted damages from a disaster, or when it is otherwise recognized that the information poses a risk to the critical information systems of other CII operators.

3.3 Framework for "information sharing from NISC"

The procedures for sharing of information from NISC to CII operators from the Cabinet Secretariat through the responsible ministries for CIIP are as follows.

a) When the Cabinet Secretariat shares information from NISC, such sharing shall be carried out through liaisons to the Cabinet Secretariat for each sector under the jurisdiction of the responsible ministries for CIIP. At this time, the individual receiving the information shall enact appropriate identification methods for the information to allow for the information to be easily and so that the information classification and scope of handling according to the information's degree of importance, content, and other factors, can be recognized at a glance.
b) The responsible ministries for CIIP liaison shall convey the information to the CEPTOAR point of contact (PoC).

c) The CEPTOAR shall convey the information to the CII operators which make up the CEPTOAR.

d) In particularly urgent cases, such as early warning information, etc., regardless of steps a) to c), the Cabinet Secretariat shall directly provide the information to the CEPTOAR or individual CII operators and report to the individual critical infrastructure operators or scepter directly from the Cabinet Secretariat, and simultaneously report to the responsible ministries for CIIP liaison. However, normalization of identification methods shall be carried out in accordance with step a).

3.4 Cooperation for "information sharing from NISC"

In the collection of information provided to CII operators through responsible ministries for CIIP and in sharing of information to CII operators, the Cabinet Secretariat shall cooperate with the information security related ministries, CIIP supporting agencies and cyberspace-related operators as follows.

a) Collect a wide range of information provided by information security related ministries and CIIP supporting agencies.

b) Collect additional information etc. related to IT outages from cyberspace-related operators as necessary.

c) Request cooperation from CIIP supporting agencies and cyberspace-related operators in the collection and analysis of information as necessary.

d) For information during IT crises, collection and sharing of information under an information sharing system composed of the Cabinet Secretariat, crisis management ministries and the disaster prevention related ministries in addition to information sharing system during normal times.

3.5 Improvement of the quality of the information to be shared

Attempts will be made to improve the quality of the information provided while continuing to take the following points into account.

a) Improve accuracy by comparing information.

b) Determine the degree of importance and priority of information according to a).

c) Impact forecasts for other CII sectors for IT outages which occur as a result of CII sector service stoppage/decline and IT outages which occur as a result of risk sources common across sectors.

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

CII sectors (Note 1)	Applicable CII operators (Note 2)	Applicable critical information system examples (Note 3)	Examples of IT outages and effects
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	・Electrical communications outages ・Outages etc. related safe and stable provision of electrical communications services ・Broadcast service outages
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.	- Stoppages of deposit payments, fund transfers including bank transfers and loans - Financial settlement outages - Stoppages of information provision related to electronic records and fund settlements - Insurance claim payment stoppages - Securities trading stoppages - Corporate bond/stock transfer stoppages - Financial product clearing stoppages etc.
Aviation services	- Major scheduled air transport operators - Ministry of Land, Infrastructure, Transport and Tourism (air traffic control/weather)	- Flight systems - Reservation/boarding systems - Maintenance systems - Cargo systems - Air traffic control systems - Meteorological information systems	- Flight delays and cancellations - Obstacles to safe flight of airplanes, etc.
Railway services	- Major railway operators including JR companies and major private railway companies	- Railway traffic control systems - Power supply control systems - Seat reservation systems	- Railway traffic delays and cancellations - Obstacles to safe railway transport, etc.
Electric power supply services	- General electric power supply services, Japan Atomic Power, Electric Power Development	- Control systems - Operation monitoring systems	- Power supply stoppages - Obstacles to safe operation of power plants
Gas supply services	- Major gas supply operators	- Plant control systems - Remote monitoring and control systems	- Gas supply stoppages - Obstacles to safe operation of gas plants
Government and administrative services	- Various ministries and government offices - Local government	- Various ministry and local government information systems (handling of e-government and e-municipalities)	- Obstacles to government and administrative service operations - Leak, theft and alteration of personnel information
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.)	- Obstacles to work in medical examination support departments
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.	- Stoppages of water supply - Supply of water of unsuitable quality, etc.
Logistics services	- Major logistics operators	- Collection and delivery management systems - Cargo tracking systems - Warehouse management systems	- Shipping delays and cancellations - Difficulties tracking cargo location

Note 1 Applicable CII operators and critical information system examples for CII sectors newly added (chemical industries, credit card services and petroleum industries sectors) in this Basic Policy are stipulated separately.

Note 2 The operators listed here are CII operators for which measures should be implemented on a priority basis, and review of the applicable operators shall be carried out based on changes in the business environment and progressive dependence on IT, when the Basic Policy is revised.

Note 3 The details of the applicable critical information systems are stipulated by CII operators based examples of IT outages and their effects.

ANNEX 2. CII SERVICES AND SERVICE MAINTENANCE LEVELS

CII sectors (Note1)		CII services (including procedures) (Note 2)		Service maintenance levels	
		Name	Explanation of services (including procedures) (Relevant laws)	Applicability/standards	Remarks
Information and communication services		- Electrical communication services	- Use of electrical communication facilities to act as an intermediary for others communications and providing other electrical communications facilities for the communications of other parties (Telecommunications Business Act Article 2)	- No trouble should occur causing continued loss of service for 2 hours or more for 30,000 or more users due to stoppages or deterioration of quality of service provision as a result of electrical communications facility trouble	- In accordance with Article 58 of the Ordinance for Enforcement of the Telecommunications Business Act
		- Broadcasting services	- Electrical communications broadcast aimed at direct reception by the public (Article 2 of the Broadcast Act)	- No trouble should occur causing continued stoppage of broadcasting for 15 minutes or longer as a result of trouble with base broadcasting facilities - No trouble should occur causing continued stoppage of broadcasting for 15 minutes or longer (2 hours or more for relay station wireless facilities) as a result of trouble with base broadcasting facilities and specified terrestrial base broadcasting facilities	- In accordance with the Ordinance for Enforcement of the Broadcast Act from Item 1 to Item 3
		- CATV services	- Electrical communications broadcast aimed at direct reception by the public (Article 2 of the Broadcast Act)	- No trouble should occur causing continued loss of service for 2 hours or more for 30,000 or more users as a result of broadcasting stoppages resulting from cable television facility trouble	- In accordance with Article 157 of the Ordinance for Enforcement of Broadcast Act
Financial services	Banking services	- Deposits - Loans - Exchange	- Receipt of deposits or periodic deposits (Article 10 Item 1-1 of the Banking Act) - Lending of loans or discounting of bills (Article 10 Item 1-2 of the Banking Act) - Currency exchange (Article 10 Item 1-3 of the Banking Act)	- No delay or stoppage of deposit repayment should occur as a result of IT failures - No delay or stoppage of execution of loan agreements should occur as a result of IT failures - No delay or stoppage of currency exchange (bank transfer) should occur as a result of IT failures	- Refer to the "Comprehensive Guideline for Supervision of Major Banks, etc." - Excluding situations where no practical effect occurs as a result of quick substitution by other systems/equipment (for example, even if a number of ATMs were suspended, if other ATMs or windows were available at the same or neighboring branches)
		- Financial settlements	- Financial settlements (Article 2 Item 5 of the Act concerning Financial Settlements)	- No delay or stoppage of financial settlements should occur as a result of IT failures	- Refer to the "Comprehensive Guideline for Supervision of Settlement/Money Transfer Agencies" - Excluding situations where no practical effect occurs as a result of quick substitution by other systems/equipment

CII sectors (Note1)		CII services (including procedures) (Note 2)		Service maintenance levels	
		Name	Explanation of services (including procedures) (Relevant laws)	Applicability/standards	Remarks
		- 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)	- No delay or stoppage of information provision related to electronic record and fund settlement should occur as a result of IT failures	- Refer to "Guideline for Administrative Processes Vol 3.: Financial Companies (12 Electronic credit record agency relationships)"
	Life insurance	- Insurance claim etc. payments	- Receipt of insurance claim etc. payment demands - Insurance claim etc. payment screenings - Insurance claim etc. payments	- No delay or stoppage of insurance claim etc. payment should occur as a result of IT failures	- Refer to "Comprehensive Guidelines for the Supervision of Insurance Companies" - Excluding situations where no practical effect occurs as a result of quick substitution by other systems/equipment
	General insurance	- Insurance claim etc. payments	- Accident reception - Damage investigations etc. - Insurance claim etc. payments	- No delay or stoppage of insurance claim etc. payment should occur as a result of IT failures	- Refer to "Comprehensive Guidelines for the Supervision of Insurance Companies" - Excluding situations where no practical effect occurs as a result of quick substitution by other systems/equipment
	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 Item 8-1 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 Item 8-2 of the Financial Instruments and Exchange Act) - Negotiable securities etc. settlement commission (Article 2 Item 8-5 of the Financial Instruments and Exchange Act)	- No delay or stoppage of disposal of securities received for guarantee, cancellation payments, etc. should occur as a result of IT failures	- Refer to the "Comprehensive Guidelines for Supervision of Financial Instruments Business Operators, etc." - Excluding situations where no practical effect occurs as a result of quick substitution by other systems/equipment (for example, situations where if the order system is suspended outside of market hours, replacement systems are quickly activated which are equivalent to the concerned system allowing for orders in time for market hours.)
		- Establishment of financial product markets	- Provision of market facilities for the trading of negotiable securities or market derivatives trading, and other work related to the establishment of financial product markets (Article 2 Item 14 and 16 and Article 80 and 84 of the Financial Instruments and Exchange Act)	- No delay or stoppage of trading of negotiable securities or market derivatives trading, etc. should occur as a result of IT failures	- Refer to Article 112 Item 7 of the Cabinet Office Ordinance on Financial Instruments Business, 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.)	- No delay or stoppage of transfer of corporate bonds or shares should occur as a result of IT failures	- Refer to the "Comprehensive Guideline for Supervision of Settlement/Money Transfer Agencies" - Excluding situations where no practical effect occurs as a result of quick substitution by other systems/equipment

CII sectors (Note1)	CII services (including procedures) (Note 2)		Service maintenance levels	
	Name	Explanation of services (including procedures) (Relevant laws)	Applicability/standards	Remarks
	- Financial product debt underwriting	- Liability assumption work through underwriting or renewal of debt based on negotiable securities trading etc. targeted transactions (Article 2 Item 28 of the Financial Instruments and Exchange Act)	- No delay or stoppage of financial product settlement should occur as a result of IT failures	- Refer to the "Comprehensive Guideline for Supervision of Settlement/Money Transfer Agencies" - Excluding situations where no practical effect occurs as a result of quick substitution by other systems/equipment
Aviation services	- Air transportation services for passengers and cargo - Air traffic control service - Distribution of meteorological information - Reservations, ticketing, boarding/loading procedures - Flight maintenance - Flight plan creation	- Work providing transport of passengers or cargo for charge using airplanes based on demands of other people (Article 2 Civil Aeronautics Act) - Appropriate usage of airspace and space and smooth maintenance of air traffic (Article 95-2 of the Civil Aeronautics Act) - Distribution of forecasts, warnings, etc. adapted for airplane use (Article 14 of the Meteorological Service Act) - Air traveler reservations, air cargo reservations - Airline ticket issuance, fee collection - Airline passenger check-in and boarding, air cargo loading - Airplane inspection and maintenance - Creation of flight plans and submission to Japan Civil Aviation Bureau	- No obstacles should be caused for transport of passengers on scheduled flights due to IT failures	- Handled in the agreement related to "CEPTOAR in the aviation services 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 Railway Business Act) - Seat reservation, boarding ticket checks on boarding and exiting the train	- No obstacles should be caused for transport of passengers on as a result of suspended trains due to IT failures	- In accordance with Article 5 of the Railway Accident Reporting Code (Private railway accident etc. reports)
Electric power supply services	- General electric power supply service	- Work supplying electric power to meet general demand (Article 2 and Article 18 of the Electric Business Act)	- No supply problem incidents of over 10 minutes for supply power of 100,000 kilowatts or more should occur as a result of IT outages	- In accordance with Article 3 of the Electricity related Reporting Code
Gas supply services	- General gas supply service	- Work supplying gas through piping to meet general demand (Article 2 of the Gas Business Act)	- No supply problem incidents effecting supply to 30 or more houses should occur as a result of IT outages	- In accordance with Article 112 of the Gas Ordinance for Enforcement of the Gas Business Act

CII sectors (Note1)	CII services (including procedures) (Note 2)		Service maintenance levels	
	Name	Explanation of services (including procedures) (Relevant laws)	Applicability/standards	Remarks
Government and administrative services	- Local government administration services	- Local administration, other administration work carried out in accordance with laws or government ordinances (Article 2 Item 2 of the Local Autonomy Act)	- No obstruction of the protection of resident Ⅰ rights and gains should occur as a result of IT failures - System recovery should be accomplished within a time period allowing for guarantee of resident safety and security	
Medical services	- Medical examination	- Examination and treatment	- No danger to human life shall occur as a result of incorrect operation of medical equipment. - No obstruction of the continued provision of medical care should occur as a result of IT failures.	- All efforts must be made to maintain the level of medical examination and treatment regardless of the degree of IT dependence.
Water services	- Supply of water through water services	- Work supplying drinking water through piping or other structures to meet general demand (Article 3 and Article 15 of the Water Supply Act)	- No interruption or decrease of water supply, abnormal quality water supply or serious problems in systems should be caused for supply of water as a result of suspended IT failures	- Important system problems refers to problems with control systems (water purification plant monitoring and control systems, pumping station operation systems, water mobilization systems, etc.) which have a serious impact on water supply in the event of a system shutdown - In accordance with "appropriate implementation of health risk management and provision of information related to damages to water supply facilities and water quality incidents" (October 25, 2013) "6.(2) In the event of information system outages in water supply"
Logistics services	- Logistics services	- Transport and storage of cargo	- No interruption of cargo transport or loss of cargo should occur as a result of IT failures	- Handled in the "agreement related to information sharing and analysis functions in the logistics sector (CEPTOAR)"

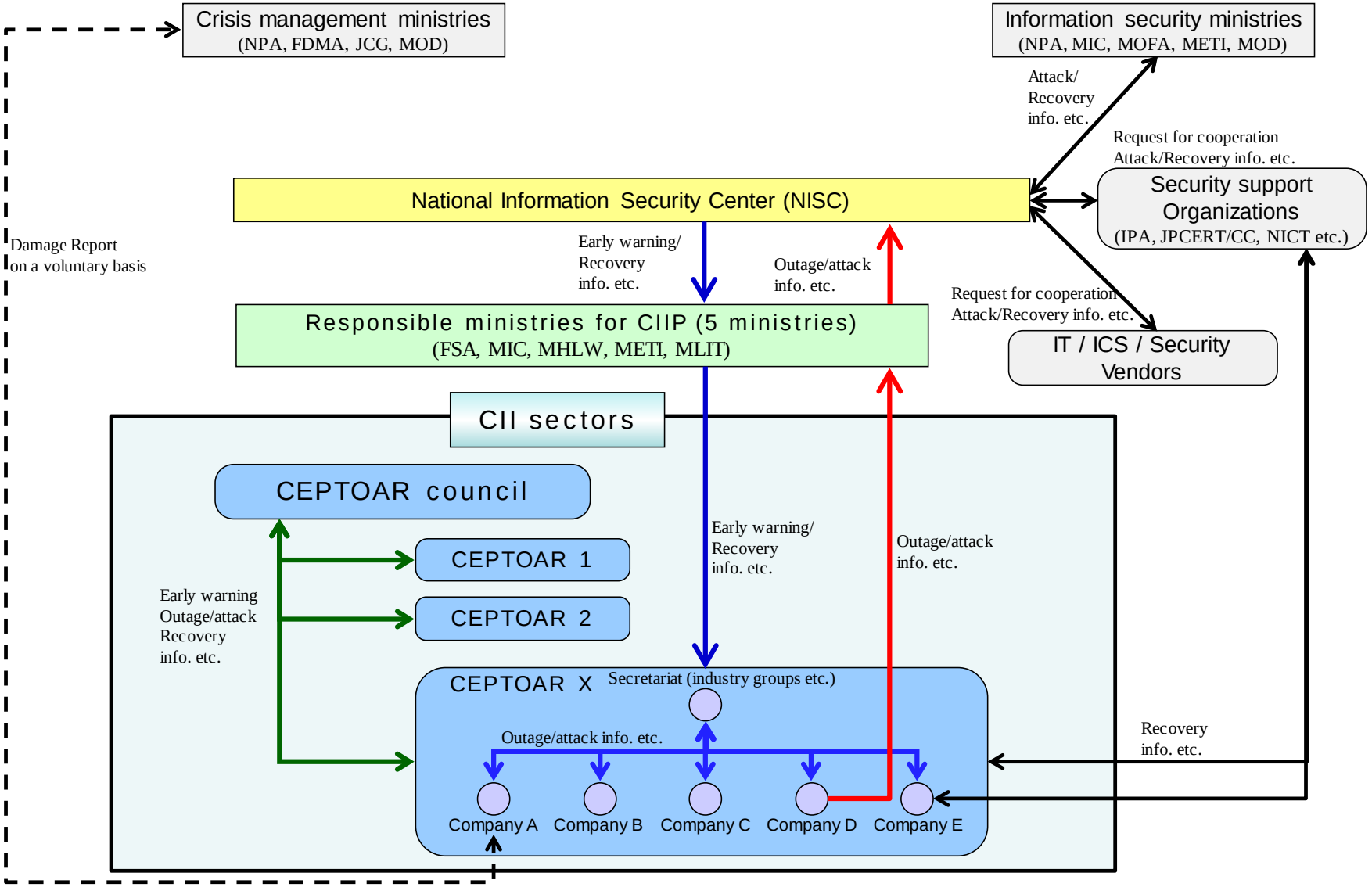
Note 1 CII services and service maintenance levels for CII sectors newly added (chemical industries, credit card services and petroleum industries sectors) in this Basic Policy are stipulated separately.
Note 2 Services which make absolutely no use of IT are outside the scope of application.

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

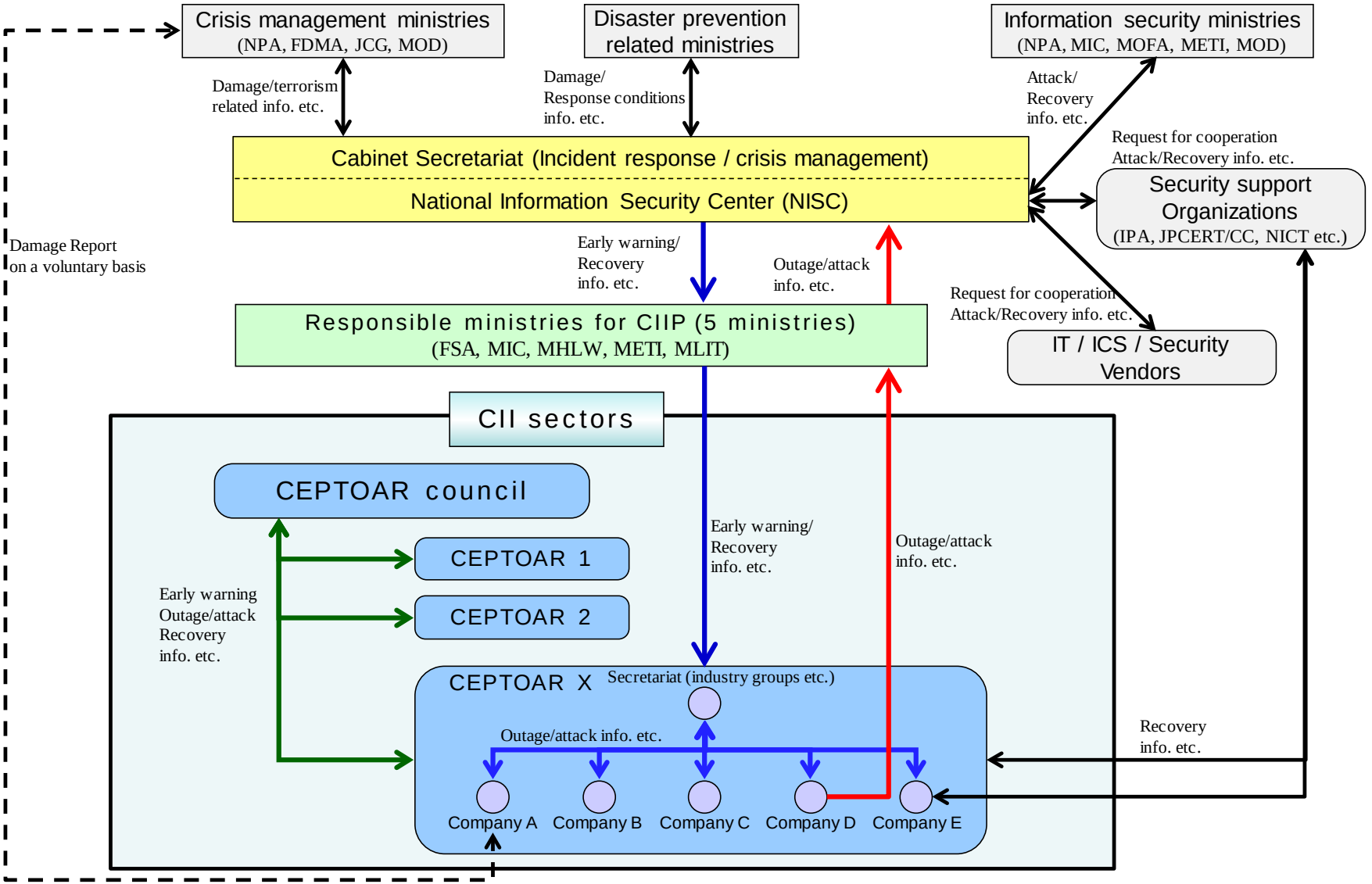
Event Categories		Event Example	Description
Events that have not occurred yet		Signs, Hiyari-Hatto	Signs such as cyber-attack warnings or Hiyari-Hatto (potentially serious damage) without occurrence of events that threaten confidentiality, integrity or availability such as minor mistakes or receipt of 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 DoS attacks, unauthorized acquisition of information, internal fraud, lack of appropriate system operation, etc.
Accidental causes	Mistaken user operation, mistaken user management, execution of suspicious files, viewing of suspicious websites, unsupervised work by outsourcing contractor, failure of equipment, vulnerabilities, cascading effect from other sectors' failures, etc.
Environmental causes	Disasters, illnesses, etc.
Others	Threats and vulnerabilities other than those above, unknown causes, etc.

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



ANNEX 4-2. INFORMATION SHARING SYSTEM (IT CRISES)



ANNEX 5. COMMUNICATION CHANNELS UNDER IT OUTAGES

CII sectors (Note)	Existing communication channels	Emergency communication channels under IT outages
Information and communication services	(1) CII operators->Government - Reporting of business stoppages etc. to the Minister of Internal Affairs and Communications in accordance with the Telecommunications Business Act - Reporting of broadcast stoppage incidents, serious wireless communications disturbances, etc. to the Ministry of Internal Affairs and Communications (2) Government->CII operators, Between CII operators - Reporting and sharing of virus outbreak and other emergency information within the industry and with the Ministry of Internal Affairs and Communications	(1) CII operators->Government - Implemented using existing contact system (2) Government->CII operators - Implemented using the T-CEPTOAR, broadcast CEPTOAR and cable TV CEPTOAR contact system - Implemented using existing contact system
Financial services: Banking services, Life insurance services, General insurance services, Securities services	(1) CII operators->Government - Reporting of service delays and stoppages to the Prime Minister (Financial Services Agency) in accordance with industry laws (2) Government->CII operators, Between CII operators	(1) CII operators->Government - Implemented using existing contact system (2) Government->CII operators - Implemented using banking services etc. CEPTOAR contact system - Implemented using securities services CEPTOAR contact system - Implemented using life insurance services CEPTOAR contact system - Implemented using general insurance services CEPTOAR contact system - Implemented through other industry associations, etc.
Aviation services	(1) CII operators->Government - Reporting of airplane accidents to the Minister of Land, Infrastructure and Transport in accordance with the Civil Aeronautics Act (2) Government->CII operators, Between CII operators - Establishment of IT outage related point of contact - Sharing of information related to aviation service security systems to relevant agencies (by airport)	(1) CII operators->Government - Implemented using the existing incident reporting system in the event of an incident - Implemented using aviation services sector CEPTOAR contact system for IT outages not resulting in accidents (2) Government->CII operators - Implemented using aviation services sector CEPTOAR contact system - CII operators directly contacted through point of contact
Railway services	(1) CII operators->Government, Government->CII operators - Reporting of railway operation accidents etc. to the Minister of Land, Infrastructure and Transport in accordance with the Railway Accident Reporting Code - Preparation of an IT outage related contact system (2) Between CII operators - None	(1) CII operators->Government, Government->CII operators - Implemented using the existing incident reporting system in the event of an incident - Implemented using railway services CEPTOAR contact system

CII sectors (Note)	Existing communication channels	Emergency communication channels under IT outages
Electric power supply services	(1) CII operators->Government - Reports related to supply problem incidents to the Minister of Economy, Trade and Industry in accordance with the Electricity related Reporting Code (2) Government->CII operators, Between CII operators - Establishment of IT outage related point of contact	(1) CII operators->Government - Implemented using existing contact system (2) Government->CII operators - Implemented using the contact system for information sharing and analysis functions related to IT outages in power supply - CII operators directly contacted through point of contact
Gas supply services	(1) CII operators->Government - Reporting of gas supply problem incidents over a certain size to the Minister of Economy, Trade and Industry in accordance with the Ordinance for Enforcement of the Gas Business Act (2) Government->CII operators, Between CII operators - Notification within the same industry in the event of the occurrence of gas supply problems as a result of disasters in accordance with the Japan Gas Association "relief measures outline"	(1) CII operators->Government - Implemented using existing contact system (2) Government->CII operators - Implemented using gas supply services CEPTOAR contact system - Implemented through CII operators
Government and administrative services	(1) Various ministries and government offices->Cabinet Secretariat - Information sharing to NISC in accordance with "Regarding communications related to government information systems during emergencies" (April 17, 2000) (2) Cabinet Secretariat->Various ministries and government offices - Information sharing from NISC in accordance with "Regarding communications related to government information systems during emergencies" (April 17, 2000) (3) Local government->Government - Information sharing from NISC in accordance with "Regarding response reporting and preparation of an emergency contact system for the occurrence of information security incidents (Notification)" (4) Government ->Local government - Information sharing from NISC in accordance with "Regarding response reporting and preparation of an emergency contact system for the occurrence of information security incidents (Notification)"	(1) Various ministries and government offices->Cabinet Secretariat, Cabinet Secretariat->Various ministries and government offices - Implemented using the internal government contact system (2) Local government->Government, Government->Local government - Implemented using local government CEPTOAR contact system - Implemented using existing contact system
Medical services	(1) CII operators->Government, etc. (2) Government, etc.->CII operators	(1) CII operators->Government, etc. (2) Government, etc.->CII operators - Implemented using medical services CEPTOAR contact system
Water services	(1) CII operators->Government, etc. (2) Government, etc.->CII operators	(1) CII operators->Government, etc. (2) Government, etc.->CII operators - Implemented using the water supply CEPTOAR IT outage information handling related guideline contact system

CII sectors (Note)	Existing communication channels	Emergency communication channels under IT outages
Logistics services	(1) CII operators->Government - Reporting of accidents etc. to the Minister of Land, Infrastructure and Transport in accordance with various industry laws (2) Government->CII operators - Designated public agencies stipulated in the Cabinet Office Disaster Countermeasures Basic Act	(1) CII operators->Government - Implemented using the existing incident reporting system in the event of an incident - Implemented using logistics CEPTOAR contact system for IT outages not resulting in accidents (2) Government->CII operators - Implemented using logistics services CEPTOAR contact system

Note : Contact systems for CII sectors newly added (chemical industries, credit card services and petroleum industries sectors) in this Basic Policy are stipulated separately.

ANNEX 6. DEFINITIONS / GLOSSARIES

CEPTOAR	Capability for Engineering of Protection, Technical Operation, Analysis and Response. Functions which provide information sharing and analysis at CII 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.
CII	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.
CII operators	Operators designated in "Applicable CII operators" in *"ANNEX 1. SCOPE OF CII OPERATORS AND CRITICAL INFORMATION SYSTEM EXAMPLES"* and groups composed of those designated operators.
CII sectors	"information and communication services", "financial services", "aviation services", "railway services", "electric power supply services", "gas supply services", "government and administrative services (including local government)", "medical services", "water services", "logistics services", "chemical industries", "credit card services" and "petroleum industries".
CII services	Services and/or a set of procedures provided by CII operators necessary to utilize those services designated in *"ANNEX 2. CII SERVICES AND SERVICE MAINTENANCE LEVELS"* in each CII sector, taking into account that the extent of impact to national life and economic activities.
CIIP supporting 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), Telecom Information Sharing And Analysis Center Japan (Telecom-ISAC Japan), and Japan Computer Emergency Response Team Coordination Center (JPCERT/CC).
Crisis management ministries	The National Police Agency (NPA), Fire and Disaster Management Agency (FDMA), Japan Coast Guard (JCG) and Ministry of Defense (MOD).
Critical information systems	Information systems required to provide CII services, designated in each CII operator, taking into account of the degree of impact to its CII service. Examples shown in *"ANNEX 1. SCOPE OF CII OPERATORS AND CRITICAL INFORMATION SYSTEM EXAMPLES"*.
Cyberspace-related operators	System vendors, which are engaged in the design, construction, operation and maintenance of information systems required for providing CII services, security vendors, which provide measures for CIIP 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 Article 2 Item 3 of the Disaster Countermeasures Basic Act (Act No. 223 of 1961) which carry are related to information collection during disasters.
Guidelines for safety principles	Measures for CIIP, which contain high-priority items and/or advanced items expected as a reference, collected with an overlook on all the CII sectors, in order to contribute to preparation and revision of safety principles. Main section is approved by the Information Security Policy Council. Measures section contains detail measures as an example.
Hiyari-Hatto	Unexpected and unpredictable events which did not lead to IT failures, but which had the potential to directly cause IT failures.
Information security related ministries	The National Police Agency (NPA), Ministry of Internal Affairs and Communications (MIC), Ministry of Foreign Affairs (MOFA), Ministry of Economy, Trade and Industry (METI) and Ministry of Defense (MOD).
Information sharing	The mutual sharing of information such as experience, knowledge and know-how by transferring to associates and communicating among organizations and members. It includes both information sharing to NISC and information sharing from NISC.

Information sharing from NISC	The provision of information for contributing to measures for CIIP from the Cabinet Secretariat to CII operators.
Information sharing to NISC	The provision of information related to IT outage, IT failures and Signs/Hiyari-Hatto at CII operators from the CII 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 CII services, and other Business continuity plan.
IT crises	IT 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.
IT failures	Events that information systems for CII do not or cannot perform as expected at the time of their design.
IT outage	IT failures which lead to fall short of the "service maintenance levels" as shown in *"ANNEX 2. CII SERVICES AND SERVICE MAINTENANCE LEVELS"*.
Measures for CIIP	A wide range of activities for preventing IT outages from affecting the national life and economic activities.
Responsible ministries for CIIP	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), and Ministry of Land, Infrastructure, Transport and Tourism (MLIT).
Safety principles	Collective measures for CIIPs including "regulations" stipulated by the government in compliance with sector-specific laws, "recommendations" and "guidelines" developed by the government according to sector-specific laws, "standards" and "guidelines" in the whole-sector developed by sector-specific groups to respond to sector-specific laws and public expectations, and "internal policies" prepared by CII operators themselves to respond to sector-specific laws and expectations of public and customs. However, safety principles do not include the "Guidelines for safety principles".
Stakeholders	The Cabinet Secretariat, responsible ministries for CIIP, information security related ministries, crisis management ministries, CII operators, CEPTOAR, CEPTOAR council, CIIP supporting agencies and cyberspace-related operators.