資料３－４（参考）

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

(Tentative Translation)

May XX, 2014
Information Security Policy Council

(This page intentionally left blank.)

Contents

I. INTRODUCTION

1. BACKGROUND

The Basic Policy for Critical Information Infrastructures (Hereinafter abbreviated as "CII") is a shared action plan for the government, which bears responsibility for the protection of the CII, and CII providers, which carry out independent measures. The plan was established to serve as the basis for a 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)" from before the establishment of the National Information Security Center (NISC).

For the action plan 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 this First Action Plan, measures were begun by the stakeholders including the government and 10 CII sectors aimed at reducing IT outages at CII to zero.

Further, the "Second Action Plan on Information Security Measures for Critical Information Infrastructure (hereinafter referred to as the "Second Action Plan") was established in 2009 indicating policies to be implemented by the nation based on the basic measures for CIIP and public-private information sharing framework constructed in the First Action Plan. The Second Action Plan continues the implementation of the "maintenance and promotion of the safety principles", "improvement of information sharing", "common threat analysis [1] " and "cross-sectoral exercises" from the First Action Plan and also newly adds policies for "response to environmental change" in order to reliable deal with ever changing social and technological environments.

In this manner, the protection of Japan's CII has a history of 13 years from the Special Action Plan and even 8 years from the action plan in its current form, and it can be judged that measures have been steadily developed based on 5 policies, beginning with the construction of a clear-cut information sharing system.

As such, while continuing to keep in accord with the "Cyber Security Strategy" (determined at the June 2013 Information Security Policy Council), the knowledge gained from the

[1] In the First Action Plan this policy was referred to as "interdependency analysis".

assessment of the Second Action Plan policy groups, including positive examples and items requiring improvement, were also appropriately reflected in the determination of the current action plan.

Furthermore, in addition to the knowledge, etc. gained in dealing with system outages and data loss during the Great East Japan Earthquake, the plan also reflects appropriate handling for the ever changing social and technological environments and trends of increasingly sophisticated and complex cyber-attacks.

2. CLARIFICATION OF THE PURPOSE OF CIIP

Presupposing the implementation of this Basic Policy, it is necessary to clarify the purposes of the protection of CII and share awareness among stakeholders.

For Cyber Security Strategy, "Assuring Free Flow of Information", "New Measures against Increasing Serious Risk", "Strengthening of Risk-based Response" and "Activities and Mutual Aid based on Social Responsibility" are indicated in the Basic Principles and the purpose of the Second Action Plan conforms with the Cyber Security Strategy.

As such, in addition to inheriting the purposes of the Second Action Plan, "carrying out the continued provision of CII services" was also added and the purpose of CII protection was further clarified.

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

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

Basic Principles for CIIP

The CII operators should implement measures for CIIP at their own responsibility.
In addition, activities through public-private cooperation should be aimed at fostering a sense of security in the people, social development, resilience and promoting international competitiveness.

- The CII operators, as the primary implementing bodies and at the position in charge of social responsibility, should respectively take measures and work for continual improvement.
- Government should support for CII operators' activities related to the measures for CIIP.
- Each CII operator should cooperate and coordinate with other stakeholders, because each CII operator can hardly handle various threats by itself.

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 safety principles

[2] Improvement of information sharing

[3] Common threat analysis

[4] Cross-sectoral exercises

[5] Response to environmental change

The results and issues of each policy are summarized below.

3.1 Outcome

On the occasion of the assessment of these policy groups, taken into account that the Second Action Plan was determined based on the most recent information surrounding CII as of 2009, assessment of results was carried out according to the assessment indexes in the Second Action Plan for the 5 policies. Consequently, for the expected targets, it can be said that the assessment showed the following definite results were achieved.

For maintenance and promotion of the safety principles, as a result of the stakeholders involved in measures for CIIP understanding the measures which they were required to implement themselves and aiming to carry out those measures under periodic self-inspection, an integrated and stable review cycle was able to be established for guides and safety principles, and the promotion, etc. of measures for CIIP was reinforced.

For improvement of information sharing, for the purpose of handling the ever-changing social and technological environments surrounding CII security measures and increasingly complex and sophisticated cyber-attacks, frameworks for sharing information to and from NISC were constructed and established through public-private partnerships, the operation of the relevant frameworks was stabilized, systems for sharing information within and between CEPTOARs were prepared, and the reception and effective utilization of required information was realized at CII operators.

For common threat analysis, as a result of carrying out examinations of common threat analysis based on determinations and analysis of cross-sectoral conditions indispensable for the maintenance and improvement of protective capability for overall CII, basic data was provided which contributed to the establishment of business continuance plans for CII operators and a portion of the analysis results were reflected in guides.

For cross-sectoral exercises, as a result of providing an opportunity for verification of

systems for mutual contact and collaboration through simulated exercises with each public-private stakeholder covering all sectors against IT outages participating, the number of organizations and individuals participating in exercises is on an upward trend, and contributions have been made to information security measures through verification of CII operator early recovery methods and business continuance plans in the event of an IT outage based on the knowledge gained through the exercises.

Regarding public relations activities in particular among the response to environmental change, materials on the results of CII information security policy, CII Specialist Committee meeting materials and other materials were posted and published on the Cabinet Secretariat website, and in addition information security policy related lectures and other events were held. For development of risk communication, opinion exchanges were held with CIIP supporting agencies and a CEPTOAR council mutual understanding WG was held. For promotion of international cooperation, cooperation with various countries through participation, etc. in Meridian[2] and Cyber Storm exercises[3]. Efforts were made to improve capabilities to perceive threats accompanying environmental change.

3.2 Issues

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

An issue for maintenance and promotion of the safety principles is reexamination based on conformity with measures for continued improvement in line with the PDCA cycle of measures for CIIP at CII operators because measures for CIIP also have an effect on the maintenance and improvement of protective capability for overall CII and not just CII operators themselves, and because there have been requests from CII operators for the presentation of guides prioritized based on the actual conditions of measures.

For improvement of information sharing, issues include building an effective information sharing system by eliminating the disparity in the frequency of information sharing between sectors, segmenting "threat patterns", constructing an information sharing system for times of IT crises positioned as an extension of the normal system, coordination of modes of cooperation with other stakeholders, etc.

For common threat analysis, issues include the detailed analysis of threats based on

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

[3] 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.

actualization of changes over time and environmental changes in order to improve effects and examinations related to operation in addition to handling investigations of serious threats which may have a major effect on all sectors, and not just limited to common threats across all sectors which are subject to investigation, aimed at the application and positioning of common threat analysis and review of the frequency of implementation, etc.

For cross-sectoral exercises, there are limitations to the design of exercise environments because the IT usage and information management of each organization differ, so major expansion of participant numbers for specific exercises is not feasible. For this reason, for the purpose of providing opportunities to identify CIIP measure issues at CII operators, the issue is to plan for further propagation and promotion of exercise results for the CII sector as a whole, rather than depending on expansion in the number of participants. Additional issues include, qualitative improvement of operation based on exercise assessments, study of the conditions for stakeholders taking into account handling during times of CII IT outages, and examination of cooperation with exercises and training sponsored by ministries responsible for CIIP and disaster prevention related ministries.

Regarding public relations activities in particular among the response to environmental change, issues include reexamination of public relations activities according to the scope of information disclosure and purpose under coordination with these policies and other policies in the next term action plan. For development of risk communication, issues include definition of risk management which conforms to international standards, reexamination of information sharing with regard for maintaining a balance between the secrecy of sensitive information and the information's usefulness, and continued mid to long term examination and study related to the theme of environmental change as it applies to new IT technologies, etc., for which the effect of threats is predicated to be major upon the mid to long term realization and use of said IT technologies, etc. For promotion of international cooperation, issues include continued promotion of cooperation with various countries in order to be able to quickly respond to intensifying/increasingly globalized risks in a cyberspace that transcends national borders, in addition to improvement of international cooperation through active utilization of bilateral, inter-regional and multilateral frameworks in and with the Asia-Pacific Region as well as the US and Europe, such as ASEAN.

4. DISCUSSION OF ISSUES

In addition to compiling the issues in the previous section and the issues requiring examination in Cyber Security Strategy, the following examinations were also carried out regarding the orientation of this Basic Policy based on the aforementioned issues.

Issue 1 While CII protection continues to mature as a system, in regard to the "Measures for CIIP are fundamentally items which CII operators must implement at their own responsibility" indicated in the Basic Principles, CII operators are still found which are lacking in this implementation and in the knowledge required for said implementation. What approach is suitable for promoting effective and independent activity from these types of CII operators?

<Orientation>

* Items noted should not be idealistic items which are difficult for CII operators to realize practically, but should rather take into account actual conditions, and be "accomplishable" items which are realistic. For example, expressions such as "absolute security is expected" and "100% perfection is anticipated" should be avoided.
* Basic items should be noted in the Basic Policy so that the executives and senior managers who hold the keys to measures for CIIP at CII operators are able to sufficiently understand the necessity of the items.
* What is expected of each stakeholder should be able to be discerned by reading the Basic Policy in consideration of the fact that some stakeholders may not be "experts".
* Clarify maintenance and improvement of protective capability for CII, especially the PDCA cycle which contributes to effective and independent activity by CII operators still mid-process as well as small to medium scale CII operators.
* Explain in detail regarding the importance of risk management and the necessity of its adoption as CII operators in order to allow for flexible response to environmental changes.
* Package the hierarchal regulations, etc. which CII operators are required to know and understand and format structure and content so that succession is easy to manage even for stakeholders affected by severe change.
* Continue to developer public relations activities even further after the determination of the Basic Policy in order to make possible the appropriate handling of ever-changing environments and the continued collection and provision of appropriate information.

Issue 2 In regard to ever-changing social and technological environments and threats which intensify year to year, there are concerns that instruction for measures which allow for appropriate and quick response, however what type of activities, both public and private, are required in order to appropriately respond to these environmental changes and threats? In addition, is it not necessary to verify if a given party should or should not be a stakeholder?

<Orientation>

* Required parties from among cyberspace-related operators shall also be added as stakeholders and information sharing shall be developed to an even greater degree.
* Promote greater recognition that there is potential of the activities of CII operators in cyberspace being targeted and used as springboards, and awareness related to the responsibility and liability related to these weaknesses.
* To recognize that threats and vulnerabilities vary for each individual CII sector and even for each CII operator, and that social and technological environments are ever-changing, and to implement investigations of priority risk sources[4] as well as to continually implement investigations of the mid to longer term changes in new technologies, systems, etc.

Issue 3 For handling of IT outages, while a variety of activities have been started among stakeholders, 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 prepared, however isn't the coordination of information which needs to be shared to and from public-private agencies and the improvement of the clear statement of each individual response and inter-agency cooperation systems necessary in the event of such a severe IT outage?

<Orientation>

* Increase the efficacy of exercises, training, etc., implemented by stakeholders, through interlinking of said exercises, training, etc.
* In addition to constructing a mechanism that recognizes that when IT crises occur, the relevant incident requires special warnings for CII operators, clarify to the greatest degree possible who shall be added to the response system and how they are to be added during normal times (conditions other than during IT crises response) (In addition, it is not realistic to setup an entirely new system in the when an incident occurs).

[4] According to "JIS Q 31000:2010", these are defined as "elements which possess the innate potential to cause risk, either as a result of the element itself or through a combination of the element with other factors".

5. REVIEW OF THE SCOPE OF CII

On the occasion of the determination of this Basic Policy, verification was carried out on the validity of the CII scopes prescribed as 10 sectors in the Second Action Plan, and further study was carried out on the addition of new sectors.

In addition, for the CII scopes, etc. which are subject to examination according to the Cyber Security Strategy[5], continued reexamination will be implemented based on coordination with relevant parties in accordance with environmental changes.

5.1 Results

Verification was carried out, with reference to the knowledge gained from past handling, such as during the Great East Japan Earthquake, on the validity of the CII scopes in the Second Action Plan, including sectors which are not positioned as CII in the Second Action Plan but which have the same or similar potential to have a serious effect on the public welfare and socioeconomic activities as existing CII sectors in the event of an IT outage in the relevant sector, and through this verification several sectors were identified as being required to be added as new CII as shown in Table 1.

Table 1. Results of study on the scope of CII

Classification	Viewpoint/Necessity	Sector
Sectors to be added with regard to the effects in the event an outage occurs with the information systems of the relevant sector	Value and scale of the provision of the service being managed	Credit card services
	Scale of the risk which resulting when control proves difficult	Chemical industries, petroleum industries
Sectors to be added with regard to the effects caused on information systems in existing CII sectors	Interdependency with existing CII sectors	Petroleum industries (See above)

As a result, in this Basic Policy, the CII sectors are 13 sectors consisting of "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".

With the participation of these added sectors as CII, it is important to eradicate doubts such as why the concerned sectors were added as CII and if there is any merit to the participation of

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

said sectors, and cultivate understand of the necessity of these sectors carrying out activities on their own initiative.

For ministries with jurisdiction over added sectors and industry groups which are potential candidates for CEPTOAR secretariats, which are central to the information sharing system, explanations are provided on the above viewpoints, agreement is obtained regarding the participation of the concerned sectors as CII and for the relevant industry groups, target critical information systems and service maintenance levels are defined and CEPTOAR establishment preparation is carried out.

5.2 Relationship between existing CII sectors and added sectors

7 years have passed since the construction of the information sharing system in FY2007, and at present each CEPTOAR has an experience amount for measures for CIIP as well as other unique qualities stemming from the nature of their operations and other factors.

In these circumstances, in the event an added sector is admitted as a new CEPTOAR, there is concern that the activities of existing CEPTOARs already active will shrink, so it is necessary for added sectors to be given advice by the Cabinet Secretariat, 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 CEPTOAR council, CEPTOARs in added sectors will be provided with advice in a spirit of mutual support, leading to maintenance and improvement of protective capability for overall CII.

6. REVIEW OUTPUT TO REVISE BASIC POLICY OF CIIP

Based on the issues identified and orientations arranged up to the preceding section, upon the determination of this Basic Policy the basic framework of the Second Action Plan, which conforms with the Cyber Security Strategy, is maintained, however individual policies and the implementation systems have been revised, and after carrying out the necessary reinforcement and improvement, the policy group structure shown in Table 2 was settled.

Table 2. Policy groups and orientation of reinforcement and improvement in the Basic Policy

Policy groups in this Basic Policy	Policy groups and response in the Second Action Plan	Orientation of reinforcement and improvement from the Second Action Plan
1. Maintenance and promotion of safety principles	Generally in accordance with "[1] Maintenance and promotion of the safety principles"	- Indicates process of the reflection of the results of other policies in guides and measure editions - Solicitation for growth models, etc. resulting from guides and studies of actual measure conditions
2. Improvement of information sharing	Generally in accordance with "[2] Improvement of information sharing"	- Revision of the positioning of each stakeholder in the information sharing system, including new stakeholders, and rearrangement of relationships between stakeholders - Revision of information (threat patterns, etc.) which should be shared based on increased cyber-attack related information - Clarification of crisis management system for times of IT crises bearing in mind handling during normal times
3. Improvement of incident response	Arrangement of "[4] Cross-sectoral exercises"	- General improvement of IT outage response system after developing an understanding of the overall image of CII related exercises and training - Qualitative improvement of cross-sectoral exercises bearing in mind cooperation with new stakeholders
4. Risk management	Arrangement after integrating a portion of "[3] Common threat analysis" with "[5] Response to environmental change	- Implementation of mid to long term studies on risk sources with the potential to have a major impact on multiple sectors as a result of environmental change and environmental change which is anticipated to have a major impact in the future - Appeal for CII operators to maintain an accurate awareness of their own current circumstances and for risk management required when proactively determining activity goals
5. Enhancement of the basis for CIIP	Arrangement after excluding the sections of "[5] Response to environmental change" integrated with "[3] Common threat analysis"	- Addition of related international standards/norms, arrangement of and regulations etc. which should be references and indication of utilization methods in addition to public relations and international cooperation

Also, in order to allow for appropriate response even in the event of major environmental change after the determination of the Basic Policy, it is necessary to continually monitor environmental change, identify threats from the information gathered, and construct systems that allow for flexible response. In addition, it is also important for the systems to be able to seamlessly shift from normal times to times of IT crises response while ensuring that initiatives

related to the improvement of outage response systems are solid, rather than just the proactive prevention on which priority was previously placed.

II. EXECUTIVE SUMMARY OF THE BASIC POLICY

The key points for this basic policy are as follows;

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

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

(2) Basic Principles for CIIP

The CII operators should implement measures for CIIP at their own responsibility.
In addition, activities through public-private cooperation should be aimed at fostering a sense of security in the people, social development, resilience and promoting international competitiveness.

- The CII operators, as the primary implementing bodies and at the position in charge of social responsibility, should respectively take measures and work for continual improvement.
- Government should support for CII operators' activities related to the measures for CIIP.
- Each CII operator should cooperate and coordinate with other stakeholders, because each CII operator can hardly handle various threats by itself.

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

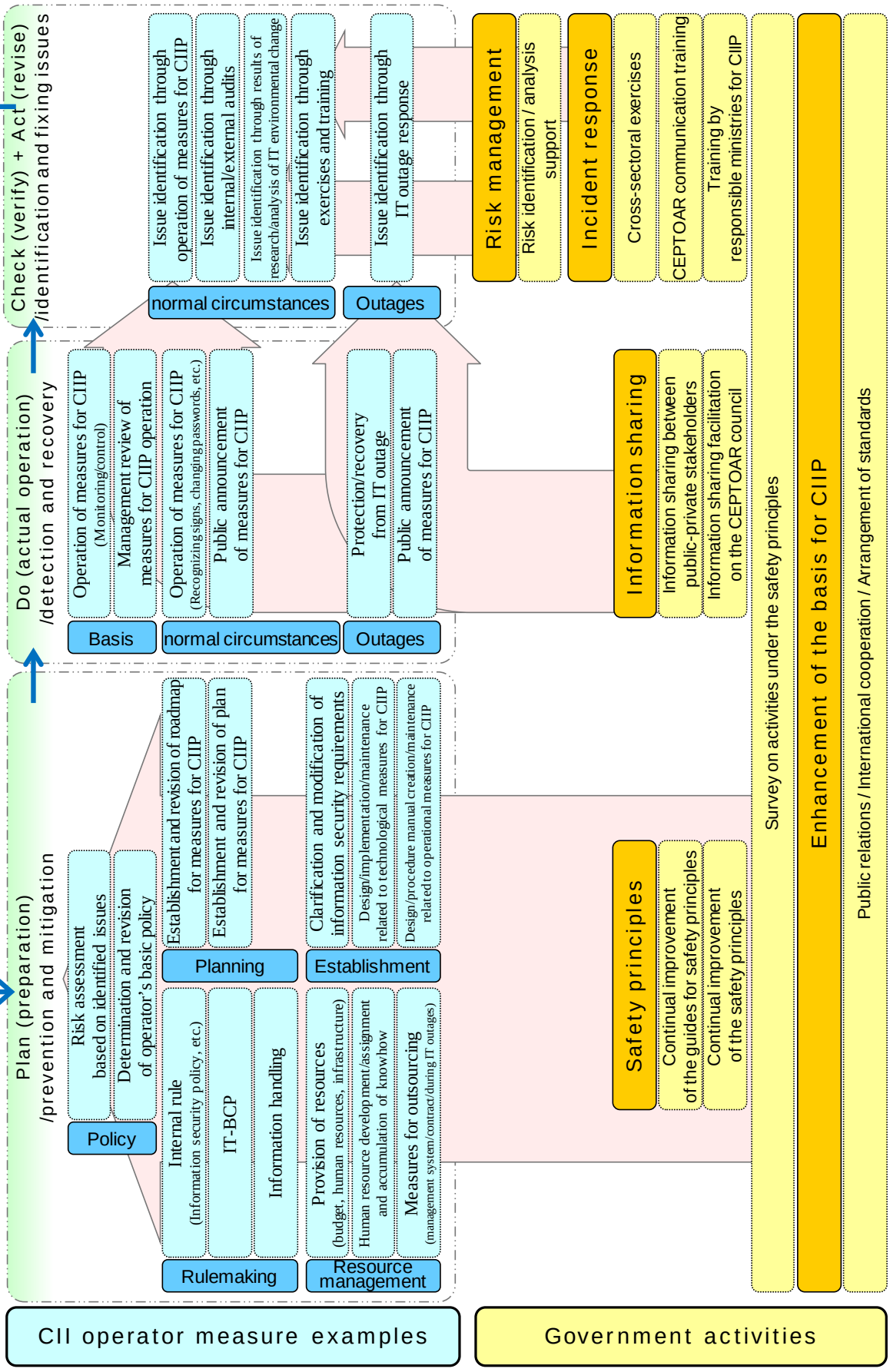
- All the stakeholders periodically verify the progress of own measures and policies in each required initiative and correctly recognize their current circumstances, and proactively determine the goals of activities. Also, they proactively cooperate with each other, recognizing of the activity conditions of other stakeholders.
- All the stakeholders understand the 5W1H of IT outage response in accordance with its scale and can calmly cope in the event of signs or occurrence of an IT outage. They can cooperate with other stakeholders and carry out cooperated response in addition to having enough communication between various stakeholders that carry out proactive response.

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

In addition to the above responsibility, the executives and senior managers should also recognize the necessity of and be capable of implementing the following.

- Recognizing risk sources focusing on information security for the above purpose.
- Assessing the above risk sources and determining policy including prioritization.
- Determining plans necessary for the establishment and operation of systems and implementation of relevant policies in addition to continually ensuring management resources; budget, human resources, infrastructure and etc.
- Verifying the execution of relevant policies through monitoring of the system operation.
- Verification and improvement of incident response including information sharing with other stakeholders through 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 Guides 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 Guides for safety principles

The Cabinet Secretariat carries out the review the Guides 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 Guides 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 Guides 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 Guides 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 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 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 Guides 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 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. IMPROVEMENT OF INFORMATION SHARING

While the social and technological environments surrounding CII constantly change, it is necessary to determine 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, and further promotes information sharing, in addition to working towards further vitalization of information sharing activities by CII operators.

2.1 Information sharing system during the term of this Basic Policy

When establishing 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 disaster prevention related ministries for disaster management, and also add cyberspace-related operators, consisting 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 (NORMAL CIRCUMSTANCES)" and "ANNEX 4-2. INFORMATION SHARING (IT CRISES)" as extended system of the former one.

In addition, the ISPC reviews CII sector 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 operate the information sharing system according to their respective position and role. In addition, it is expected that cyberspace-related operators implement measures required for the maintenance of information

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

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 agencies 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. EVENT CATEGORIES AND CAUSE CATEGORIES IN 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[6] items based on the information security C.I.A[7] viewpoint and formed detailed cause items based on new threats, etc. in "ANNEX 3. EVENT CATEGORIES AND CAUSE CATEGORIES IN 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.

[6] 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".

[7] 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[8],. 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[9] 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[10].

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

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 in "ANNEX 4-1. INFORMATION SHARING (NORMAL CIRCUMSTANCES)" and

[8] 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.

[9] PoC: Point of Contact.

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

"ANNEX 4-2. INFORMATION SHARING (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 agencies. 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. IMPROVEMENT OF INCIDENT RESPONSE

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 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[11] 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.

[11] 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[12] 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[13] and risk communication and consultation[14], 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

[12] 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.

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

[14] 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[15] 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 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 with

[15] 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.

stakeholders regarding the management of risk".[16]

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 Mutual reflection of the results of this policy and other 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.

[16] 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 "Information Security Strategy" and "Basic Policy on Information Security Measures for Critical Information Infrastructures" 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[17] 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.

[17] 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. ITEMS TO BE UNDERTAKEN 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 agencies 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 FOR 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 guides 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 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) Improvement of information sharing

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 knowhow.

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

(3) Improvement of incident response

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 FOR RESPONSIBLE MINISTRIES FOR CIIP

(1) Maintenance and promotion of the safety principles

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

b) When the organization determining the safety principles, in addition to implementing periodic analysis and verification of 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 etc. implemented by the Cabinet Secretariat every year.

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

(2) Improvement of information sharing

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) Improvement of incident response

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 FOR INFORMATION SECURITY MINISTRIES

(1) Improvement of information sharing

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 FOR CRISIS MANAGEMENT MINISTRIES

(1) Improvement of information sharing

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) Improvement of incident response

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

5. VOLUNTARY ACTIVITIES FOR 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 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 etc. 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 etc. implemented by the Cabinet Secretariat every year.

(2) Improvement of information sharing

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) Improvement of incident response

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 FOR CEPTOAR

(1) Improvement of information sharing

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) Improvement of incident response

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 FOR THE CEPTOAR COUNCIL

(1) Improvement of information sharing

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 agencies or based on own proposals.

(2) Improvement of incident response

a) Participate in cross-sectoral exercises as necessary.

8. VOLUNTARY ACTIVITIES FOR SECURITY SUPPORT ORGANIZATIONS

(1) Improvement of information sharing

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) Improvement of incident response

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 FOR IT/ICS/SECURITY VENDORS

(1) Improvement of information sharing

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 OF 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 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 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 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 agencies. 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 agencies. 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 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 by government agencies

The policies of this Basic Policy are as shown in "III. MEASURES 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 etc. 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 Improvement of information sharing

The outcomes expected from "improvement of information sharing" 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 Improvement of incident response

The outcomes expected from "improvement of incident response" 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 FOR THE BASIC POLICY BASED ON ASSESSMENT OF 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 agencies, etc., and enhancement of a system for sharing this type of information among CII operators and interdependent CII sectors.

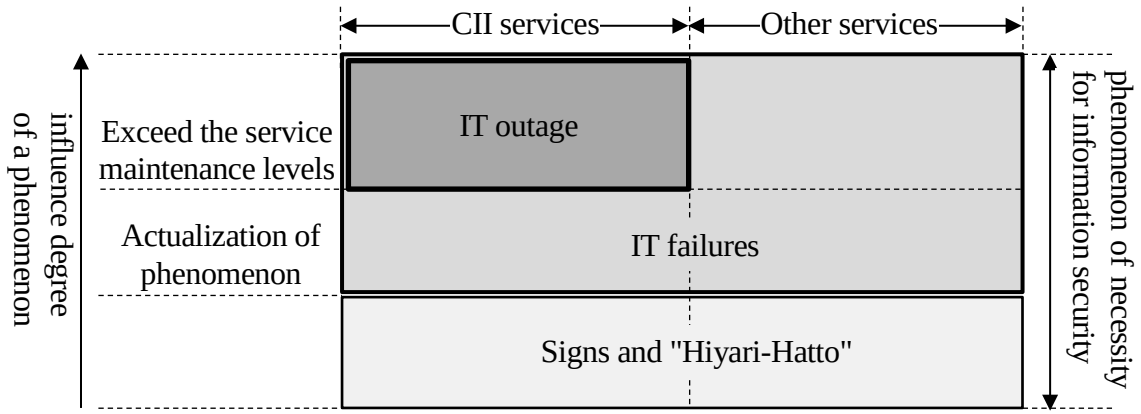
The various aspects of information related to IT failures, etc. include the following.

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 of 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 of 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 disaster prevention related ministries in addition to information sharing system during normal times.

3.5 Improvement of the quality of the information

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)"

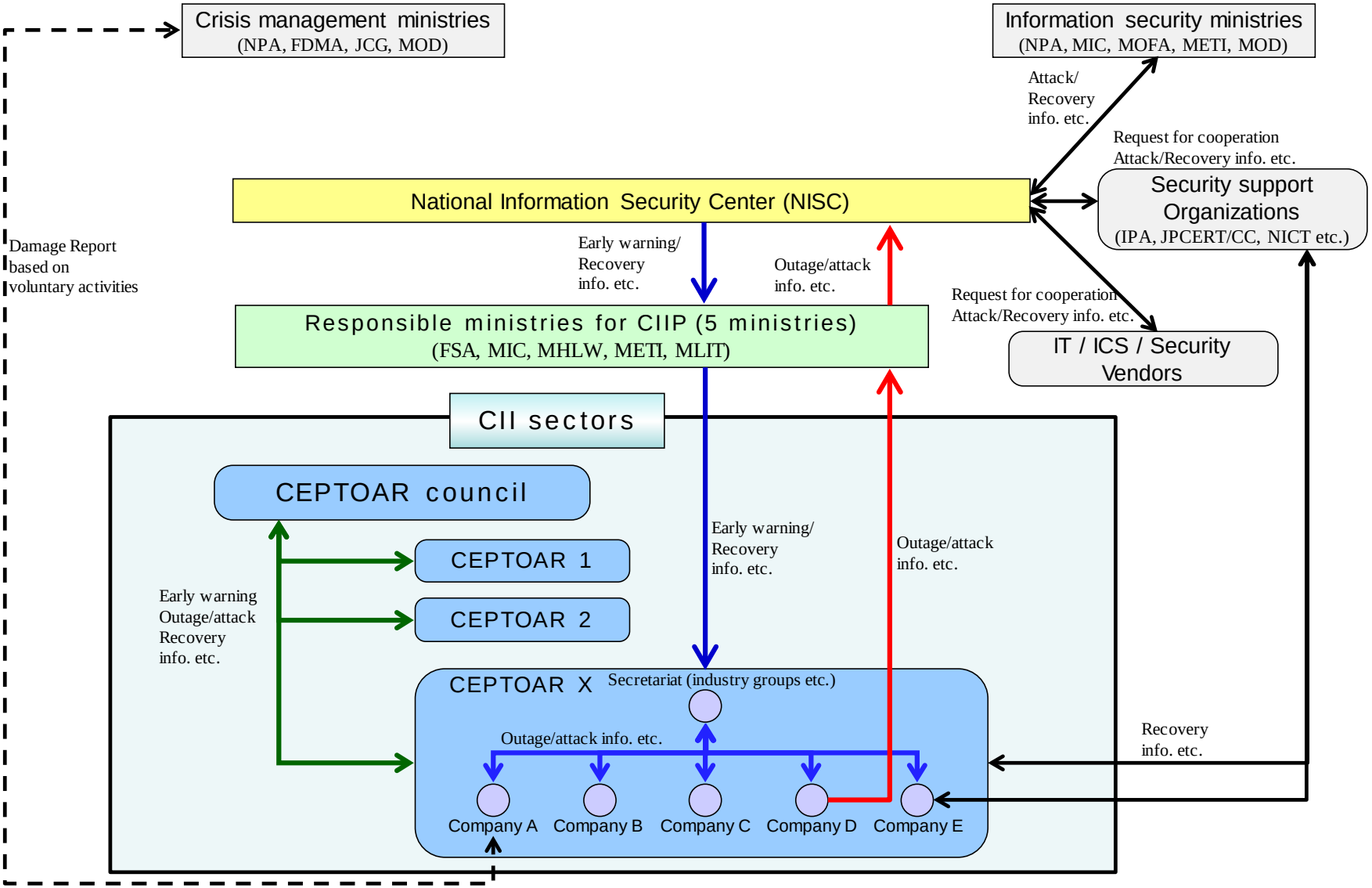
Note 1 CII services and service maintenance levels for CII sectors newly added (chemical industries, credit card services and petroleum industries sectors) in this Basic Policy are stipulated separately.
Note 2 Services which make absolutely no use of IT are outside the scope of application.

ANNEX 3. EVENT CATEGORIES AND CAUSE CATEGORIES IN INFORMATION SHARING TO NISC

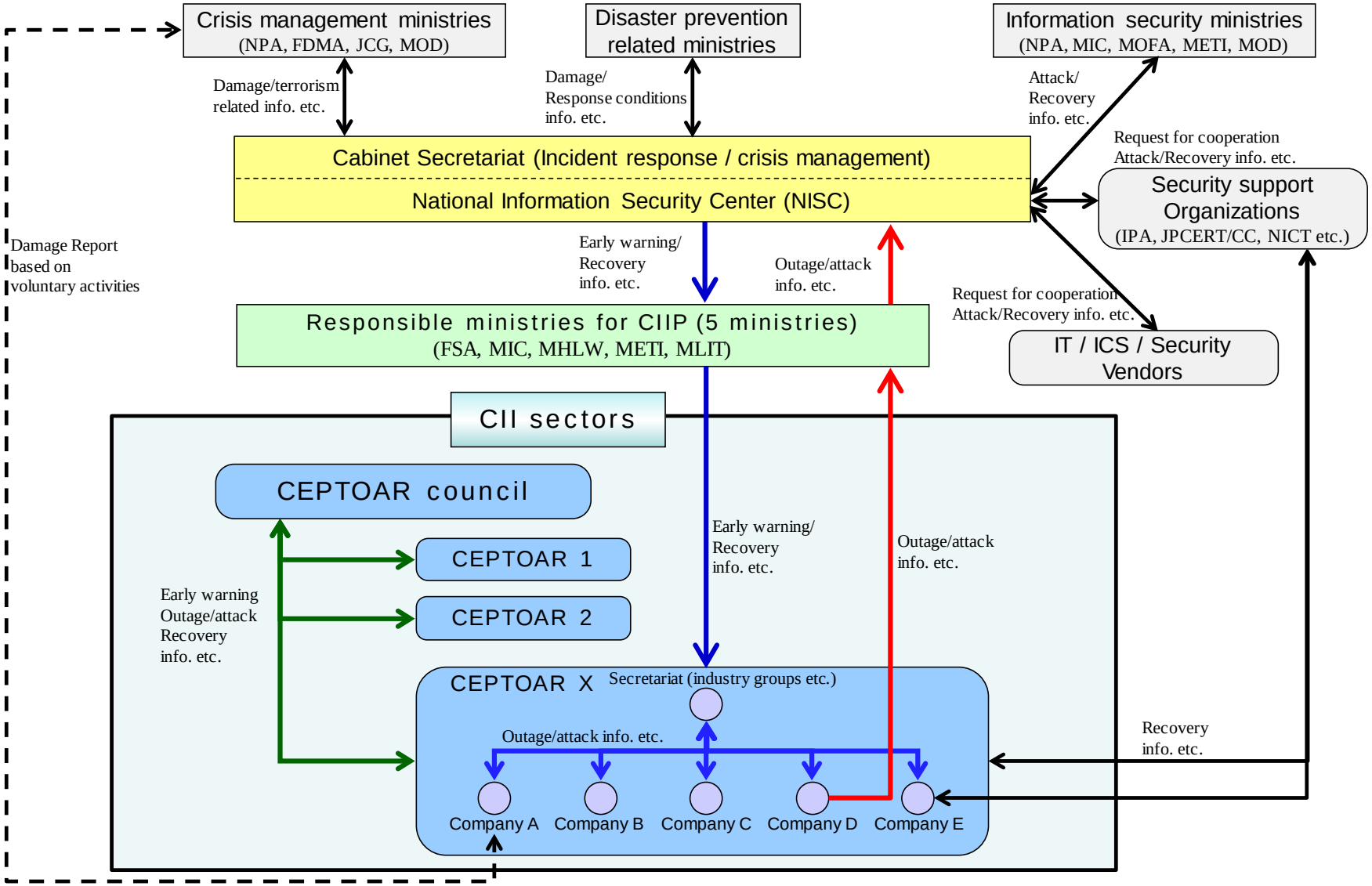
Event Categories		Event Example	Description
Events that have not occurred yet		Signs, Hiyari-Hatto	Signs such as cyber-attack warnings or Hiyari-Hatto (potentially serious damage) without occurrence of events that threaten confidentiality, integrity or availability such as minor mistakes or receipt of 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
		Other	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.
Other	Threats and vulnerabilities other than those above, unknown causes, etc.

ANNEX 4-1. INFORMATION SHARING (NORMAL CIRCUMSTANCES)



ANNEX 4-2. INFORMATION SHARING (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

IT-BCP	Business continuity plan (including relevant manuals) related to the information systems to provide CII services. And other Business continuity plans.
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".
IT failures	Events that information systems for CII do not or cannot perform as expected at the time of their design.
Safety principles	Collective measures for CIIPs including "regulations" stipulated by the government in compliance with industry laws, "recommendations" and "guidelines" developed by the government according to industry laws, "standards" and "guidelines" in the whole-sector developed by industry groups to respond to industry laws and public expectations, and "internal policies" prepared by CII operators themselves to respond to the expectations of industry law, the public and customs. However, safety principles do not include guides stipulated by the Cabinet Secretariat.
Stakeholders	The Cabinet Secretariat, responsible ministries for CIIP, information security ministries, crisis management ministries, CII operators, CEPTOAR, CEPTOAR council, Security support organizations and IT/ICS/Security Vendors.
IT/ICS/Security Vendors	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, and platform vendors, which provide the platforms which serve as foundations, including hardware and software.
Crisis management ministries	The National Police Agency (NPA), Fire and Disaster Management Agency (FDMA), Japan Coast Guard (JCG) and Ministry of Defense (MOD).
Guides 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 sectors, in order to contribute to preparation and revision of safety principles. Main section is approved by the ISPC. Measures section contains detail measures as an example.
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 services	Services and/or a set of procedures necessary to utilize those services designated in "ANNEX 2. CII SERVICES AND SERVICE MAINTENANCE LEVELS" in each CII sector, taking in to account that the extent of impact to national life and economic activities.
CII operators	Of the operators affiliated with CII sectors, the operators and groups composed of the relevant operators designated in "Applicable CII operators" in "ANNEX 1. SCOPE OF CII OPERATORS AND CRITICAL INFORMATION SYSTEM EXAMPLES".
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).
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".
Critical information systems	Of the information system required to provide CII services, the systems stipulated by CII operators in light of the degree of impact they have on the CII services. Examples shown in "ANNEX 1. SCOPE OF CII OPERATORS AND CRITICAL INFORMATION SYSTEM EXAMPLES".
Information sharing	The mutual sharing of information such as experience, knowledge and knowhow to associates and within and between organizations and members. Includes both information sharing to NISC and information sharing from NISC.

Information systems	All systems which based on IT such as systems for business processing, control field equipment, monitoring and control systems.
Security support organizations	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).
Information security 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).
Measures for CIIP	A wide range of activities for preventing IT outages from affecting the life of people and socioeconomic activities.
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.
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	A committee made up of representatives of each CEPTOAR which carries out information sharing between CEPTOARs. An independent body, not positioned under other agencies, including government agencies.
IT crises	IT outages which require centralized response by the government such as the establishment of Prime Minister's Cabinet Response Offices in the Prime Minister's Crisis Management Center.
Hiyari-Hatto	Unexpected and unpredictable events which did not lead to IT failures, but which had the potential to directly cause IT failures.
Disaster prevention related ministries	The government agencies 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.