# The Second Action Plan on Information Security Measures for Critical Infrastructures

"Safety as a matter of course for our daily lives"

- Safe and secure social infrastructure for everybody -

February 3, 2009

The Information Security Policy Council

# THE SECOND ACTION PLAN OF INFORMATION SECURITY MEASURES FOR CRITICAL INFRASTRUCTURES

“Safety as a matter of course for our daily lives”

- Safe and secure social infrastructure for everybody -

**I. GENERAL 4**

**1. Objective 4**
(1) Objectives of the Action Plan 4
(2) Basic direction 6
(3) Ideal future to be achieved 8

**2. Definition and scope 10**
(1) Critical infrastructure and critical infrastructure providers 10
(2) Critical infrastructure services and critical systems 10
(3) Service levels and the verification level 10
(4) IT malfunctions 11
(5) Threats 11
(6) Information security measures 11
(7) Organizations concerned 12

**3. Results of the First Action Plan 13**
(1) Maintenance and penetration of the safety standards etc 13
(2) Strengthening of information sharing systems 13
(3) Interdependency analysis 14
(4) Cross-sectoral exercises 14

**4. Points of efforts to be implemented during the period of the Second Action Plan 14**

**II. INFORMATION SECURITY MEASURES TO BE IMPLEMENTED DURING THE PERIOD OF THE PLAN 16**

**1. Maintenance and penetration of the safety standards etc 16**
(1) Continuous improvement of the guideline 16
(2) Continuous improvement of the safety standards 16
(3) Spreading the safety standards 17
(4) Promotion strategy 17

**2. Strengthening of information sharing systems 17**
(1) Organization of information to be shared 18
(2) Enhancement of information provision and liaison 18
(3) Strengthening of CEPTOARs 19
(4) The CEPTOAR Council 19
(5) Promotion strategy 20

**3. Common threat analysis 20**
(1) Continuation of interdependency analysis 21
(2) Study on common threat analysis 21

(3) Promotion strategy 21

**4. Cross-sectoral exercises 22**
(1) Conducting cross-sectoral exercises 22
(2) Promotion strategy 23

**5. Response to environmental change 23**
(1) Public relations and hearing activities 23
(2) Enhancement of risk communication 24
(3) Promotion of international cooperation 24
(4) Strengthening the basis for information security 24
(5) Promotion strategy 25

**III. MATTERS TO BE TAKEN BY ORGANIZATIONS CONCERNED 26**

**1. Promotion system 26**

**2. Schemes of each organization concerned 27**
(1) Policies of the Cabinet Secretariat 27
(2) Policies of the critical infrastructure sector-specific ministries 30
(3) Policies of the information security related ministries 32
(4) Policies of the law enforcement ministries 32
(5) Matters expected as a voluntary scheme of the related agencies 32
(6) Matters expected as voluntary measures of critical infrastructure providers 34
(7) Matters expected as voluntary measures of CEPTOARs 35
(8) Matters expected as voluntary measures of the CEPTOAR Council 36

**IV. ASSESSMENT/VERIFICATION AND REVIEW 37**

**1. The Promotional System of the Action Plan 37**
(1) Assessment and verification of the progress of the Action Plan 37
(2) Review of the results 38
(3) Review of the policies 39
(4) Supplemental survey for assessment of the result 40
(5) Evaluation of the results based on the Action Plan 41
(6) Review of the Action Plan 41

**2. Cooperation with the existing system for information sharing 41**

**ATTACHMENT: INFORMATION PROVISION AND LIAISON 43**

**1. Information on IT malfunctions 43**

**2. Information provision to critical infrastructure providers 43**
(1) Scope of critical infrastructure providers to provide information 43
(2) Information provided 43
(3) Mechanism of information provision 44
(4) Coordinated system for information provision 44
(5) Enhancement of information quality (e.g. analysis information and impact level) 45

**3. Communication from critical infrastructure providers 45**
(1) Cases require communication and information to be transmitted 45
(2) Contents for communication 46
(3) Mechanism of communication 46
(4) Ideas concerning handling of reported information 47

4. Consolidating information and sharing in emergencies such as disasters and terrorist attacks 47

APPENDIX 1. CRITICAL INFRASTRUCTURE AND IMPORTANT SYSTEM CONCERNED 48

APPENDIX 2. CRITICAL INFRASTRUCTURE SERVICES AND REVIEW LEVEL 49

APPENDIX 3. EXAMPLE OF THREATS THAT CAUSES IT MALFUNCTIONS 52

APPENDIX 4. INFORMATION SHARING 53

APPENDIX 5. REPORTING SYSTEM IN CASE OF IT MALFUNCTIONS 54

# I. General

## 1. Objective

### (1) Objectives of the Action Plan

"The Action Plan on Information Security Measures for Critical Infrastructures（determined by the Information Security Policy Council, December 13, 2005）" ("the First Action Plan" hereinafter) was to enhance the information security measures for critical infrastructures in close partnerships between the public and private sectors. The plan was proceeded by the organizations[1] concerned including the government and the 10 sectors of critical infrastructure[2], aiming at "minimizing the occurrence of IT malfunction in critical infrastructure" upon the confirmation on "the First Information Security Basic Plan (the Information Security Policy Council, February 2, 2006)" which was the mid/long-term strategy for the information security policies of Japan.

As a result, the "Guideline for the development of the "safety standards[3]" concerning the information security in critical infrastructure" ("the guideline", hereafter) was established by the end of FY2008. The safety standards for each sector based on the guideline were also established and reviewed, which was followed by the establishment of the cycle for periodical review. In addition, the establishment of information sharing systems between the public and private sectors has been promoted and the establishment of "the information sharing and analysis function (CEPTOAR[4])" (CEPTOAR, hereafter) was completed. It is followed by the promised establishment of "the Critical Infrastructure Communication Council" (the CEPTOAR-Council)（tentative name）[5] (the CEPTOAR- Council, hereafter). Furthermore, interdependency among sectors was analyzed as well as the cross-sectoral exercises are conducted based on specific scenarios to cope with the business continuity in case of IT malfunctions[6].

Accordingly, the foundation for partnerships between the organizations concerned was built up and the culture, which promotes awareness and common understanding that will help advance information security measures[7], is gradually developed in each organization concerned.

IT became more widely used, while promoting efforts to execute the First Action Plan and devices and progresses have been being made with regard to both increasing business efficiency conducted by and improving usability of service

[1] See "2. Definition and Scope" for "the organizations concerned".

[2] See "2. Definition and Scope" for "critical infrastructure providers"

[3] "Safety standards" refers to documents developed as a standard or reference for critical infrastructure providers to make various decisions and actions.

[4] CEPTOAR;Capability for Engineering of Protection, Technical Operation, Analysis and Response

[5] The Council is expected to be established by the end of 2008. The Council will be comprised of the representatives of each CEPTOAR. The official name of the Council was not determined as the time of authorizing this Action Plan because the study for the establishment of the Council is in progress. Therefore, the name of the council and the timing for the establishment is subject to change depending on the conditions of the study.

[6] See "2. Definition and Scope" for "IT malfunctions".

[7] See "2. Definition and Scope" for "information security measures".

provided by critical infrastructure providers. For users of services, opportunities are increasing to have a chance to use services enhanced by IT resulting from fulfillment of network environment and improvement of IT literacy. It is prospected that both people's social lives and economic activities would continue to develop with it's spreading use of IT and, at the same time, this means society tends to be of higher dependence on IT.

Under such circumstances, it is also expected that possibility of occurrence of IT malfunctions could increase and the scope of its potential impacts would expand. In order to ensure the stable supply of services of critical infrastructure providers and their business continuity, it is required to fulfill the framework of legal systems generally called "business laws" aiming at regulating entities running business classified into concerned sector, as well as voluntary efforts of critical infrastructure providers in consistency.

Therefore, the "Second Action Plan on information security measures for critical infrastructures" ("the Second Action Plan", hereafter) was formulated as the common action plan to encourage voluntary efforts promoted by the government and critical infrastructure providers who are responsible for protecting critical infrastructures.

As the formulation of the Second Action Plan, consideration was primarily focused on the issues found and recognized during enforcement of the First Action Plan and from it's results gained through progress of enforcement. The consideration was based on two aspects, namely, "Continuity" and "Development".

From the viewpoint of "Continuity", following the First Action Plan, policy for the consideration was assumed to "protect the critical infrastructure to prevent both people's social lives and economic activities from being seriously affected due to IT malfunctions caused by critical infrastructure providers as well as ensure the entities continuously provide services and immediately restore from IT malfunctions". It also aimed at continuously "reducing the number of occurrence of IT malfunctions at critical infrastructure as small as zero". This is the straight-forward expression of the basic posture that the organizations concerned promoting information security measures against critical infrastructures should have to make continuous efforts to prevent IT malfunctions from giving severe impacts on people's social lives and economic activities.

With regard to taking information security measures, accepting certain risks[8] may be rational because of some restrictions from the viewpoint of cost-effectiveness and usability.. In order to respond to IT malfunctions incurred by unexpected threats, there should be measures to be prepared assuming the occurrence of IT malfunctions. Considering these restrictions and uncertainty, it is necessary to promote improvement of technological development and countermeasures with regard to both preventive measures that would prevent IT malfunctions from occurring to the least possible frequency and reactive measures that would minimize negative effects resulting from the occurrence of IT malfunctions as little as possible, from the viewpoint of the above restrictions and uncertainty, as well as to improve effectiveness of these measures by equally introducing both measures.

[8] In this Action Plan, "risk" refers to possible loss or damages resulting from whole disadvantage brought by IT malfunctions and IT functional failures.

Accordingly, from the viewpoint of "Development", a rational standard was newly defined as a service level[9] with regard to critical infrastructure services[10] of each sector in order to continuously improve the effectiveness of information security measures considering the realistic conditions and characteristics of each sector. The goal of the Second Action Plan, based on this, is defined as "preventing IT malfunctions from having significant impacts on people's social lives and economic activities. "

Therefore, the Second Action Plan specifies a wide range of necessary measures for both preventive measures against IT malfunctions to "maintain services of critical infrastructure providers" and reactive measures against IT malfunctions to "ensure rapid resumption in case of IT malfunctions".

To achieve the goals, the Second Action Plan summarizes various information security measures taken by each organization concerned as a systematic framework composed of voluntary measures which should be taken by critical infrastructure providers and measures which should be taken by the government (especially the Cabinet Secretariat), related agencies[11] and other organizations. The Second Acton Plan aims at ensuring achievement of the goals as well as establishing continuous improvement cycle of this framework.

The organizations concerned with promoting information security measures against critical infrastructures must strengthen information security measures and ensure providing critical infrastructure services continuously and immediate restoration from IT malfunctions, under close cooperation with public and private sectors, based on the Second Action Plan. They also should make efforts toward steady improvement of the Second Action Plan.

In implementing security measures, each organization concerned are encouraged to actively take necessary actions to improve current technologies, maintain partnerships with other organizations, coordinate legislative and management issues, and develop human resources as well as actions mentioned in the Second Action Plan.

(2) Basic direction

Critical infrastructure providers should primarily take information security measures at their own responsibility. Each critical infrastructure provider takes measures as a business entity as well as an organization responsible for social responsibility and promote continuous improvement of the measures. The government gives necessary supports to the efforts concerning information security measures that the entities engaged in critical infrastructure promote.

On the other hand, under today's situation where various services are complicatedly cross-linked and usage of IT is widely spread, it is difficult to ensure that necessary and indispensable measures are taken against various threats based only on the information security measures taken solely by critical infrastructure providers. Therefore, it is necessary to enhance cooperation between enterprises in the same sector and ones of other sectors in order to avoid generation of blind spot regarding information security measure.

[9] See "2. Definition and Scope" for "service level".
[10] See "2. Definition and Scope" for "the critical infrastructure services".
[11] See "2. Definition and Scope" for "the related agencies"

However, as the efforts that critical infrastructure providers take are voluntary, its basic directions are diversified. Beyond such diversity, the basic directions to which each entities should conform are summarized as follows to put experiences of each entity to practical use from cross-sectoral viewpoint and to create an environment where subjective collaboration is facilitated.

Directions shown here are not intended to mandate a kind of duty against specific organizations concerned. The objective of specifying detailed directions is to encourage each organization concerned to promote voluntary collaborations, as well as to maintain a consistency of the efforts taken by each organization concerned in general.

1) Promoting introduction of advanced measures and compliance with the guideline

The degree that each critical infrastructure provider is dependent on IT and the substance of interdependencies between critical infrastructure sectors varies. Also efforts taken by each critical infrastructure sectors corresponding to such diversity are diversified. Therefore, both effort to thoroughly promote necessary measure without regard to the sector and to summarize advanced efforts that specific entity have been making and apply them to promotion of voluntary measure are important by establishing and enforcing a guideline that is the minimum standard as a criteria. It is also important to attempt cross-sectoral cooperation with regard to such schemes.

2) Harmonizing measures taken in the domain of technology, management and legislation

Regarding information security measure, its technical aspects tend to attract attention. However, it is important to not to leave the effort solely to IT department and to take such elements into consideration as appropriate allocation of resources to information security measures and internal control concerning information security measures, based on the concept of so-called "Information security governance"[12] from the viewpoint of maintaining availability of the services provided by critical infrastructure providers. It is also important to ensure the consistency of legislation and industrial rules under appropriate involvement of both public and private sectors. In addition, it is also essential to facilitate communications between the organizations concerned regarding the elements that needs to be addressed.

3) Consideration on both viewpoint of customer services and social responsibility

In terms of the critical infrastructure business, there are two types of responses that business entities are expected to take, one is from the viewpoint of customer services and the other is from that of public interests. Interest of customer and public can not always be consistent. Up to now, critical infrastructure providers have been accomplishing their responsibilities for those two subjects described above by voluntary response and it is important for the entities to continuously accomplish their accountabilities so as to promote risk communication[13] with various organizations depending on critical infrastructure and information security

[12] "Information security governance" means properly taking information security measures as part of corporate management.

[13] See II 5 (2) for "risk communication".

measures.

4) Take preventative measures against IT malfunctions but be careful not to be overconfident of preventative measures

Not only preventive measures against IT malfunctions but also the measures that will be invoked after occurrence of IT malfunctions are important to minimize negative impacts on people's social lives and economic activities from the viewpoint of protecting critical infrastructure to avoid serious impacts on people's social lives and economic activities resulting from IT malfunctions. It is important to consider measures to minimize the impacts of IT malfunctions assuming their occurence and make both public and private sectors to recognize the situations they are placed and the roles they should play.

5) Understand that information on IT malfunctions should be shared as much as possible

It is considered that information security measures taken by each critical infrastructure provider have been developed but sharing valuable information with regard to both the experiences of preventative measures and measures taken after occurrence of IT malfunctions and the threats that would be cause of IT malfunctions tends to be insufficient and less positive . However, based on the recognition that these should be a valuable information for improvement of the measures, it is important to much more promote efforts of information sharing.

(3) Ideal future to be achieved

The state of the future expected to be achievement by the efforts based on the Second Action Plan is described as follows.

Each organization concerned that takes information security measures understands what kind of measure they should take based on the critical infrastructure service that they should protect and the service levels to be maintained. Each organiation concerned correctly recognizes situations they are placed and subjectively sets their own object of activity. They promote necessary efforts and conduct self review of the efforts. Also they are able to cooperate with each other voluntarily by understanding the current status of activities that other organiations carry out.

The organizations concerned understand who accumulates what kind of information, what kind of information they should share with and with whom they should share the information, and what they should do in response to the occurrence of IT malfunctions in accordance with the scale of effect of IT malfunctions. In addition to their voluntary response, they are able to make well managed response by cooperating with other organizations concerned on the necessity basis.

Specially, the concept of so-called "information security governance" penetrates well enough among critical infrastructure providers, and they understand that information security measures should be considered not only from the viewpoint of construction and operation of information system but also from that of corporate management, and therefore, they became to have a system where person in charge of system construction, system operation and corporate management properly participate in promoting information security measure. They also make efforts to explain what kind of information security measures they promote to other organiations. Furthermore, a sense of values has become matured that the attitude of sharing information as much as possible in order to strengthen information security measure against social infrastructure.

Accordingly, critical infrastructure providers have recognition that occurrence of the IT malfunctions in their own sector should not be concealed, but should be shared among the organizations concerned that promote security measures. The organizations concerned that are working on security measures are able to grasp information such as status of occurrence of IT malfunctions and share the information with external organizations through the CEPTOAR of each sector and the CEPTOAR Council and as a result, they became to cooperate with the external organizations either formally or informally.

No IT malfunctions has occurred or even if it has occurred, it does not lead to the state where significant influence exerts on people's social lives and economic activities because the organizations concerned take information security efforts with regard to the protection of critical infrastructure based on the Second Action Plan in cooperation with each other. It is widely known to the people that the organizations concerned are making efforts to protect critical infrastructure and as a result, it makes people feel at ease. Communications between various organizations completes and they are able to respond to IT malfunctions calmly with confidence.

Critical infrastructure providers appropriately perceive threats and change of the risks concerning IT malfunctions due to the advancement of implementation of various measures and environmental change, and therefore, take measures voluntarily and make necessary coordination between entities. Such close relationship among entities became one of the driving forces for continuous improvement of the measures.

Various information that contributes to information security measures became being sent to the Cabinet Secretariat through various measures based on the Second Action Plan, risk communications between the organizations concerned, and international cooperation. The Cabinet Secretariat are promoting cooperation with the organizations concerned based on the situation and shows its overall coordinating function to promote introduction of more effective measures.

In particular, recognition of unique and serious threat and the risk regarding IT malfunctions has been obtained and if it is difficult to cope with such threat and risk by critical infrastructure providers alone, the Cabinet Secretariat, the critical infrastructure special councils, and the CEPTOAR Council would immediately act in coordinative manner to study possible measure to cope with the situation and coordination would be made toward the enforcement of the measure.

Such voluntary efforts of each organization based on its self-recognition penetrate as their code of conduct and it forms the information security culture among them. In critical infrastructure sector such as individual critical infrastructure providers and the each level of the government, daily communication is enforced to enhance the preventive measures of IT malfunctions and in case of occurrence of IT malfunction, continuous improvement is promoted to surely make use of experiences gained through responding to the situation as the measures to be enforced in the future. This framework is announced to public as an action plan and assessed regularly and properly updated as required.

These efforts of information security measures promoted by each organization concerned are established as a indispensable element that support sustainable development of the society.

## 2. Definition and scope

### (1) Critical infrastructure and critical infrastructure providers

"Critical infrastructure" is the basis of people's social lives and economic activities formed by businesses that provide services which are extremely difficult to be substituted by others If its function is suspended, deteriorated or become unavailable, it could have significant impacts on people's social lives and economic activities.

In the Second Action Plan, the critical infrastructure to be protected is following ten sectors as "data communication", "finance", "airlines", "railway", "electric power", "gas", "the government and administrative services (including municipal governments)", "medical", "water service" and "logistics".

"Critical infrastructure providers" are those who are designated as "Business entities concerned" described in Appendix 1 among the entities running business that belongs to 10 sector described above and groups composed of those entities.

### (2) Critical infrastructure services and critical systems

"Critical infrastructure services" are defined as services provided by critical infrastructure providers and a series of procedures necessary to use the services which particularly needs to be protected, taking into account of the degree of impact on people's social lives and economic activities, among the services provided by critical infrastructure providers. Services of each critical infrastructure sector that should be protected under the Second Action Plan are shown in Appendix 2. Only examples of the services defined may be shown for some sectors.

"Important systems" are defined as the information systems necessary to provide critical infrastructure services and specified for each critical infrastructure provider by taking the degree of impacts on the critical infrastructure services into consideration. Examples of the important systems under the Second Action Plan are shown in Appendix 1.

Appendices 1 and 2 do not intend to limit the objects of information security measures to designated critical infrastructure services and important systems. It is necessary to take information security measures under the Second Action Plan against critical infrastructure services and important systems that are not referred here and could exert significant influences on people's social lives and economic activities.

### (3) Service levels and the verification level

In the Second Action Plan, the state where critical infrastructure services are provided and assumed to be available stably and at an allowable level for people's social lives and economic activities is called "service level". The service level is defined for each critical infrastructure providers in reference to the "verification level" of Appendix 2.

Each critical infrastructure provider is required to take information security measures aiming at maintaining the service level. It is also desirable that the service level would not be significantly different from the goal of the business continuity plan of each critical infrastructure provider.

When the critical infrastructure service level falls below a certain degree, the service will be verified and the degree shall be “the verification level”. The verification level of each sector is shown in Appendix 2.

(4) IT malfunctions

“IT malfunctions” is a failure occurred in critical infrastructure service (e.g. the state unable to maintain the service level) caused by disorder of IT functions.

Disorder of IT functions means the state that information systems required to provide critical infrastructure services and critical systems do not show expected function as designed.

The Second Action Plan requires a verification of the status of IT malfunction occurrence which deviates from the specified degree when carrying out assessment and check of the effort.

(5) Threats

In the Second Action Plan, any factors which may cause IT malfunctions are called “threat”. There are various types of threats, and the patterns of the threats are even diversified depending on the characteristics of sectors. The Second Action Plan specifies four types of threats as shown in Appendix 3.

Critical infrastructure providers are required to make sure table supply and business continuity of their critical infrastructure services as well as to take particular care on the possibilities that disorder of their IT malfunctions could be a threat to the stable supply and assurance of business continuity of critical infrastructure services provided by other critical infrastructure providers.

There are two types of threats, one is those which require measures promoted by the entire society and the other is those which measures should be enforced mainly by individual critical infrastructure providers. Particularly, the former requires an active involvement of the entities to take cross-sectoral measures.

(6) Information security measures

In the Second Action Plan, “information security measures” indicates a broad range of approach to prevent IT malfunctions occurred in critical infrastructure from exerting negative impacts on people’s social lives and economic activities. Information security measures includes measures against the functional failures of IT in addition to measures against IT malfunctions. The target incident to which information security measures will be applied is illustrated below.

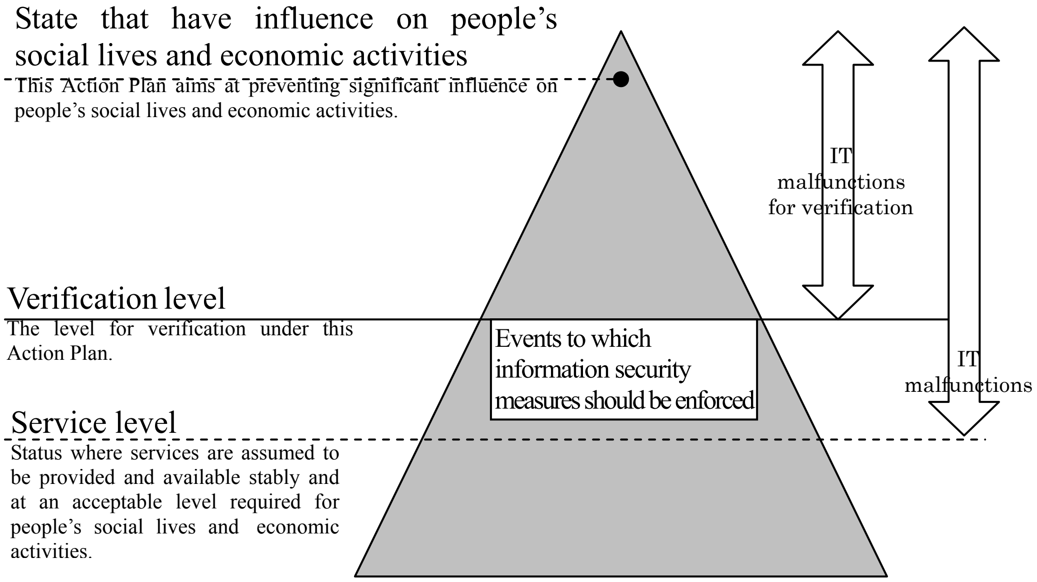

State that have influence on people's social lives and economic activities
This Action Plan aims at preventing significant influence on people's social lives and economic activities.
IT malfunctions for verification
Verification level
The level for verification under this Action Plan.
Events to which information security measures should be enforced
IT malfunctions
Service level
Status where services are assumed to be provided and available stably and at an acceptable level required for people's social lives and economic activities.

Figure: Illustration of events to which information security measures should be enforced

Generally information security measures can be categorized into two types, one is preventative measures to avoid occurrence of IT malfunctions to the least possible level and the other is measures taken after occurrence of IT malfunctions to minimize the impacts of IT malfunctions to the least possible level by ensuring an immediate restoration from the malfunctions.

From the viewpoint of preventive measures, there are two different types of methods. One is to eliminate IT functional failure itself which could cause IT malfunctions, and the other is to control impacts on the services while accepting a certain range of IT functional failure. Which measure should be enforced depends on the status.

In this case, even though IT functional failure is assumed to be accepted, if a failure to control the influence on critical infrastructure services resulted in the occurrence of IT malfunctions, measures to eliminate relevant functional failures could be needed as a post occurrence measures for improvement. Therefore, the Second Action Plan also emphasizes on information security measures against IT functional failures, as well as information security measures against IT malfunctions.

In the Second Action Plan, information security measures enforced by critical infrastructure providers are simply called "measures" and those which enforced by the government are called "policies".

### (7) Organizations concerned

"Organizations concerned" assumed to be involved in promoting information security measures under the Second Action Plan includes the Cabinet Secretariat, critical infrastructure sector-specific ministries (the Financial Services Agency, Ministry of Public Management, Home Affairs, Posts and Telecommunications, Ministry of Health, Labour and Welfare, Ministry of Economy, Trade and Industry, and Ministry of Land, Infrastructure and Transport), information security related ministries (National Police Agency, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry and Ministry of Defense), law enforcement ministries (National Police Agency, Fire and Disaster Management Agency, Japan Coast Guard, Ministry of Defense) and related agencies (National Police Agency Cyberforce, NICT[14], AIST[15], IPA[16], Telecom-ISAC Japan[17], JPCERT/CC[18] etc.), critical infrastructure providers, CEPTOARs and the CEPTOAR Council.

When each organization concerned makes an effort to promote information security measures according to each roles, it might be appropriate in some cases that the organization makes an effort solely or in cooperation with IT venders. For information sharing, the organizations concerned should cooperate in the existing information sharing system with the Cabinet Office and related government agencies as required.

## 3. Results of the First Action Plan

All the goals under the First Action Plan are expected to be achieved within the term planned. The main results are as follows. These items compose the basis of the Second Action Plan.

### (1) Maintenance and penetration of the safety standards etc

From the viewpoint to ensure business continuity and respond to trust from people with regard to critical infrastructure sectors, items to which some sort of measures are desired to be taken prior to enforcing information security measures in order to support development and revision of the safety standards of each sector was determined by the Information Security Policy Council as the guideline. Based on this guideline, each critical infrastructure sectors developed necessary or required level of information security measures as a safety standards. The guideline was reviewed and the related safety standards was also reviewed in order to make the guideline appropriate and up to date based on the change of social trends. Then, a comprehensive review cycle of the guideline and safety standards was established through the status of reviewing safety standards and conducting survey with regard to the status of the penetration of safety standards.

### (2) Strengthening of information sharing systems

“The communications procedures concerning liaison and information provisions of “the Action Plan on Information Security Measures for Critical Infrastructures” (“the communications procedures” hereinafter)” was defined as a framework for each organization of public and private sectors to promote

[14] NICT; National Institute of Information and Communications Technology, an Incorporated Administrative Agency

[15] AIST; Advanced Industrial Science and Technology, an Incorporated Administrative Agency

[16] IPA;Information-Technology Promotion Agency, Japan, an Incorporated Administrative Agency

[17] Telecom-ISAC Japan; Telecom Information Sharing and Analysis Center Japan

[18] JPCERT/CC; Japan Computer Emergency Response Team Coordination Center

cooperation and brought the information provision and liaison between the Cabinet Secretariat and the critical infrastructure sector-specific ministries into operation. "Information provision" is to provide information contributing to promoting measures implemented by critical infrastructure providers from the Cabinet Secretariat to critical infrastructure providers. "Liaison" is to communicate information regarding IT malfunctions occurred inside a critical infrastructure provider from the entity to the Cabinet Secretariat.

Meanwhile, CEPTOARs were established in each sector of critical infrastructure. In addition, the CEPTOAR Council will be established as the cross-sectoral information sharing system between each CEPTOAR that is able to act independently from government agencies.

(3) Interdependency analysis

To construct the basis for coordination between critical infrastructure sectors, "interdependency analysis" was conducted. "Static interdependency analysis" revealed mainly how critical systems depend on other critical infrastructure and "dynamic interdependency analysis" revealed how relationship between sector will change over time in case of occurrence of IT malfunctions.

(4) Cross-sectoral exercises

Gradually after conducting "research type exercises:" and "table top exercises[19]" "functional exercises[20]" was conducted. "Functional exercise" was conducted based on the scenario assuming specific cases concerning information sharing and liaison in case of emergency, with participation of critical infrastructure providers, CEPTOARs, the critical infrastructure sector-specific ministries, and the Cabinet Secretariat. Through these exercises, the methods of information sharing and liaison in case of occurrence IT malfunctions were confirmed and verified.

## 4. Points of efforts to be implemented during the period of the Second Action Plan

In the First Action Plan, in addition to the effort implemented by each critical infrastructure provider, the establishment of "a new public and private cooperation model", a system aiming at promoting cooperation of public and private sector, was moved forward from the cross-sectoral viewpoint. This enabled adding findings from the cross-sectoral viewpoint to the efforts of each critical infrastructure providers and accumulating findings from the cross-sectoral viewpoint within the Cabinet Secretariat. Also it formed a foundation to drive improvement cycle applied to the framework of the Action Plan. However, with regard to the threats that the Action Plan should to cope with and the service level that critical infrastructure providers should maintain,, metrics for verification of specific improvement was not specified.

The Second Action Plan, making use of the achievement of the First Action Plan, aims at establishing improvement cycle where the organizations concerned

[19] Table top exercise: exercise where participants discuss issues based on the same scenario around the table
[20] Functional exercise: to verify actual command and order system of organizations using simulation

share and make use of their experiences that they have been accumulating on a daily basis Therefore, the plan includes measures that promotes continuous verification of the efforts through visualization of the threats to cope with and service level to maintain. This drives farther development of “the new public and private sector cooperation model” established under the First Action Plan. In other words, objective of this effort is to enable cooperation of the organizations concerned to mutually maximize effects generated by their voluntary efforts, as well as to make individual and independent efforts implemented by each organization concerned to be a driving force that promote self-organized growth of the framework of the Action Plan itself.

This effort for improvement is conducted individually by all organizations concerned with the Second Action Plan. It means that improvement would be promoted by layered approach, such as improvement at individual critical infrastructure providers, improvement within each critical infrastructure sector and improvement of cross-sectoral policy of the governments. Although these efforts have been promoted by each organization as before, framework of the Second Action Plan aims at making these efforts to organically support with each other and to ensure effectiveness of each efforts.

As a result, the plan aims at enabling critical infrastructure providers to incorporate not only their own experiences but also their experiences regarding the entire sector and experiences regarding the cross-sectoral policies into the efforts to improve their measures. Also the plan aims at sharing experiences regarding IT malfunctions, which tends to be overlooked by other organizations, among the organizations concerned and making cooperation between the organizations concerned to be further advanced and completed one by making use of the experiences.

## II. Information security measures to be implemented during the period of the plan

During the period of the Second Action Plan, efforts are promoted based on the following five information security measures.

### 1. Maintenance and penetration of the safety standards etc

During the period of the Second Action Plan, the guideline is reviewed in terms of it's status and the level of the details of the descriptions as well as supplementing detailed descriptions from the viewpoint of the business continuity. Also not only the effort that contribute to the bottom up of promoting the completion of safety standards considering the consistency with PDCA cycle deployed by critical infrastructure providers, but also the effort from the viewpoint of developing individual advanced measures and promoting their penetration is implemented.

#### (1) Continuous improvement of the guideline

Analysis and verification of the guideline should be conducted and publicized annually or as required, in order to follow changes in social trend and to reflect new findings to the guideline in a timely manner. Consideration on the revision of guideline should be conducted every three years. However, additional consideration should be conducted as required and revision of the guideline is enforced if necessary.

On the consideration to revision of the guideline, contents of the guideline should be completed to enable verification of it's effectiveness from the cross-sectoral viewpoint based on the situational recognition with regard to the progress made for development of the business continuity plan within critical infrastructure providers and the advancement of the international standardization concerning business continuity plan.

In order to complete items that would contribute to the voluntary effort implemented by critical infrastructure providers, the guideline should be continuously completed in terms of the items described by categorizing the items described in the guideline into “items requiring consideration” and “items for reference” and showing example of specification of measures.

“Items requiring consideration” refers to items to which measures should be commonly taken in all sectors from the viewpoint of improving measures unless specific reason exists and of which necessity to be defined in the safety standards should be studied by each sector. “Items for reference” refers to items desired to be incorporated as an advanced measure and referred by each sector as an option.

“Items requiring consideration” and “items for reference” should be completed as required based on the findings and lessons obtained through the effort implemented by each critical infrastructure sector or critical infrastructure provider under the Action Plan, as well as the items of the current guideline.

#### (2) Continuous improvement of the safety standards

In order to reflect findings obtained through experience of implementing efforts, each sector should make effort to continuously improve the safety standards. The safety standards should be verified based on the guideline and the results of analysis and verification of the guideline and revision of the safety standards is enforced as necessary.

In order to promote sharing of the findings related to information security measures, standards or references with regard to information security measures should be summarized again as safety standards in a broader meaning so as to make them be shared in a possible range, in addition to the safety standards which have been the subject of verification.

It is important for the organizations concerned that have relationship to understand the status of the measures taken based on the safety standards. Therefore, voluntarily effort such as conducting information security audit or its equivalent and preparation of information security reports or its equivalent are still more recommended, and explanation for external entities regarding the information security measures implemented at each sector and by critical infrastructure providers is encouraged.

(3) Spreading the safety standards

Each critical infrastructure sector should make efforts to promote measures defined in the safety standards and complete environments that would help promote implementation of measures toward spreading the safety standards.

In order to ensure the penetration of the safety standards including “bylaws” specified by the business entities themselves, “survey concerning the status of penetration of the safety standards” should be periodically conducted. Items of investigation and subjects that conduct survey will be reviewed as necessary.

(4) Promotion strategy

A. Continuous improvement of the guideline

The guideline is revised in the initial year of the Second Action Plan. Analysis and verification of the guideline should be conducted every one year or as required and the results should be disclosed as a supplement of the guideline as necessary.

B. Continuous improvement of the safety standards

Each critical infrastructure sector should make efforts to continuously improve the safety standards. Situational recognition should be enforced with regard to the efforts taken at each critical infrastructure sector at a certain timing every year and an objective study and verification should be done on the status of improvement of the standards based on the result of the analysis and verification of the guideline and of the specific matters unique for each critical infrastructure sector as much as the Cabinet Secretariat is able to grasp.

C. Spreading the safety standards

Each critical infrastructure sector should still more make efforts to spread the safety standards including completion of the environment that would help promote implementation of measures. Objective review and understanding of the status regarding implementation of the measures, including “bylaws” specified by the business entities, should also be conducted annually at a certain time of the year.

2. Strengthening of information sharing systems

During the period of the Second Action Plan, information to be shared by the organizations concerned should be organized. The improvement of the environment, which is required for information provision and liaison between the organizations concerned, should be promoted. Furthermore, voluntary efforts made by each CEPTOAR and the CEPTOAR Council should be facilitated. The entire figure of the information sharing system is shown in Appendix 4.

(1) Organization of information to be shared

"Information concerning IT malfunctions" is a broad range of information concerning IT malfunctions and functional failures of IT which can be used to implement information security measures.

Information concerning IT malfunctions includes three aspects; 1) prevention of IT malfunctions, 2) prevention of spread of IT malfunctions and immediate restoration from IT malfunctions and 3) prevention of reoccurrence of IT malfunctions by analysis and verification of factors that caused IT malfunctions.

Information to be shared should be clarified and organized taking existing framework concerning the circulation of the information security related information into consideration, based on the changes of the threats to be responded and various social trends. In the process described above, based on the three aspects of information concerning IT malfunctions, activities of the organizations concerned and information they have and restrictions imposed by legal system and regulations should be clarified and summarized, as well as the effective way of information sharing for the critical infrastructure should be examined based on the characteristic of the information owned by the organizations concerned (e.g. timing, format and method, including viewpoint of quick responses).

Also, clarification of the necessary information and the information that can be provided should be reviewed periodically, from the cross-sectoral viewpoints, through practice of information provision and liaison.

(2) Enhancement of information provision and liaison

A. Basics of information provision and liaison

Under the First Action Plan, establishment of information sharing systems primarily focused on "communications procedures" and the completion of CEPTOARs have been promoted from the viewpoint that cooperation of each entities of public and private sectors is important in order to facilitate maintenance and restoration of the service provided by critical infrastructure providers and information sharing has already begun. Considering that the framework of information sharing system has been just established, the information provision and liaison under the Second Action Plan should basically be completed in order to further enrich the contents of the information provided based on the existing information sharing systems, and would be carried out according to the figure shown in the Attachment.

B. Enhancement of information provision and liaison

Rules concerning information sharing arranged individually by the Cabinet Secretariat, the critical infrastructure sector-specific ministries, CEPTOARs and critical infrastructure providers should be coordinated. With regard to the information provided by the Cabinet Secretariat intended to the critical infrastructure, function required to information sharing should also be examined as required in order to promote information sharing among the organizations concerned.

In order to strengthen sharing of cases and experiences, analysis should be conducted on the subject and degree that IT malfunctions would affect based on the findings obtained through the mutual dependency analysis that has been carried out under the First Action Plan and to-be-obtained findings through the common threat analysis to be conducted in the future. Also, utilizing analysis functions of related agencies should be examined.

### (3) Strengthening of CEPTOARs

As the functional requirements that CEPTOARs should have, two items described below defined in the First Action Plan should continuously be maintained and therefore the information provided by the Cabinet Secretariat is to be shared.

[1] There should be a rule agreed by the members concerned in terms of the regulations regarding how to handle information provided by the Cabinet Secretariat, non-disclosure of secret and providing information to external organizations.

[2] There should be an emergency point of contact (POC[21]) that enable communication with each member and external organizations in an emergency

In the future, extension of function is expected such as information collection, understanding and analysis by CEPTOARs, information sharing within the CEPTOARs and sending information to other CEPTOAR and the CEPTOAR Council.

Each CEPTOAR is also required to assign coordinators capable of collecting information and making decisions based on the information within the sector and to complete function of information sharing regarding cases that does not result in IT malfunction and is not regarded as an issue of current information liaison scheme and function required to enable information sharing with other CEPTOARs and with the CEPTOAR Council and these efforts should be promoted and achieved as part of the voluntary effort of the critical infrastructure.

### (4) The CEPTOAR Council

The objective of establishing the CEPTOAR Council is to provide an opportunity to promote mutual support and assistance composed of each CEPTOAR and it is desirable that ,mutual understanding and cross-sectoral information sharing of specific cases such as best practices is encouraged.

Also the CEPTOAR Council is expected to make positive efforts regarding examination of improvement of information sharing utilizing it’s characteristics, as it is allowed to act independently from government agencies so that it is expected to take actions using the, for discussion aiming improvement of information sharing patterns. In particular, as it is important for critical infrastructure providers and government agencies to share situational recognition of each organization in order to deepen the cooperative relationship with each other, it is desired that efforts would be enforced such as facilitating exchange of opinions between critical

[21] POC; Point of Contact

infrastructure providers and government agencies .

(5) Promotion strategy

A. Organization of information to be shared

Specific information to be handled and how to use it will be determined by each organization such as the Cabinet Secretariat, CEPTOARs and the CEPTOAR Council during their effort of promoting information sharing, based on the enough consideration to the characteristics of each critical infrastructure sector and the business laws.

In the process described above, the Cabinet Secretariat is assumed to play the primary role to strengthen the information sharing system and to clarify what is the useful way of information provision for critical infrastructure providers (e.g. timing, format and method, including the viewpoint of quick responses), based on the characteristic of the information owned by organizations concerned, taking the three aspects of information about IT malfunctions into consideration. Information to be shared should be examined in a timely manner based on the social environment and actual conditions of information sharing.

B. Enhancement of information provision and liaison

In order to ensure consistency of the rules concerning information sharing among the Cabinet Secretariat, the critical infrastructure sector-specific ministry, CEPTOARs, and critical infrastructure providers, “communications procedures” should be reviewed taking the opinions of the parties concerned such as CEPTOARs into consideration and also the reference materials should be arranged regarding operations based on the “communications procedures” and therefore, by showing the reference to the parties concerned, visualization of the operation of information sharing system should be encouraged. Also, as required, functions required for information sharing should be studied and the Cabinet Secretariat, the critical infrastructure sector-specific ministries, and CEPTOARs should share the result of the study.

In addition, efforts should be enforced to promote broad range of cooperation with organizations that take useful actions for improvement of information security of critical infrastructure providers.

C. Strengthening of CEPTOARs

In order to strengthen the functions of CEPTOARs, the functions of the CEPTOARs and advanced cases of effort such as activities of the CEPTOARs should be periodically introduced, and that should be contributed to strengthening of the CEPTOARs.

## 3. Common threat analysis

During the period of the Second Action Plan, the interdependency analysis aimed at identifying which critical infrastructure sector would be influenced in case of IT malfunctions occurred in the specific critical infrastructure sector should be continuously conducted and, as well, study to understand what is the potential threat common to the critical infrastructure sector should be conducted.

Therefore, the Cabinet Secretariat, the critical infrastructure sector-specific ministries, and critical infrastructure providers should promote activity for analysis in cooperation with each other while deepening cooperation with research institute based on the result of "static interdependency analysis" and "dynamic interdependency analysis" that has been conducted so far.

Note that the results of this analysis are continuously expected to be used for maintenance and restoration of the services of the critical infrastructures as described below:

[1] Providing basic materials necessary to develop more effective business continuity plan
[2] Providing basic materials that help decide the priority of the restoration in case that large-scale disaster occurs
[3] Providing foundation to facilitate collaboration between critical infrastructure sectors to prevent spread of damages due to IT malfunctions

### (1) Continuation of interdependency analysis

In order to ensure information security of the critical infrastructure, it is necessary to recognize interdependency between critical infrastructure sectors and take measures that enable flexibly responding to the problems. Thus, the interdependency analysis is necessary for both visualization of the potential risk chain and management(e.g. evasion, control, and assumption) of chain-reactive transfer of accidents and failure factors. Because of the fact described above, the interdependency analysis should be continuously conducted under the Second Action Plan.

### (2) Study on common threat analysis

While each critical infrastructure have been more depending on IT, a cross-sectoral situational recognition and analysis are further indispensable than before, in order to improve information security of critical infrastructure as an entire nation. Therefore, analysis should be conducted to understand what would be potential threats that could be common risk to each critical infrastructure sector. This analysis and the interdependency analysis are to be called altogether as common threat analysis, which is conducted to analyze broad range of target such as IT related technologies, system and environment common to critical infrastructure sectors.

### (3) Promotion strategy

Regarding the common threat analysis, in order to conduct broad range of analysis effectively, parties concerned should list up and prioritize issues at the beginning of each fiscal year and clarify the target of analysis for each year. Achievement obtained from these analysis will be summarized in annual report.

In order to improve the effectiveness of the results obtained from analysis, practical issues, methods and cooperation with research institutes should be considered for review. In terms of the cooperation with research institutes, sufficient care should be taken for management and protection of information.

Results of analysis are expected to be reflected on the maintenance and restoration of critical infrastructure service. It should also be used for preparation of the scenario of the cross-sectoral exercises, as well as for continuous improvements of the guideline and the safety standards. Furthermore, the results is expected to be widely used by each government agency including sector-specific ministry.

## 4. Cross-sectoral exercises

Cross-sectoral exercises for the critical infrastructure should be conducted during the period of the Second Action Plan in cooperation with organizations such as critical infrastructure sector-specific ministries, critical infrastructure providers and CEPTOARs of the critical infrastructure sectors, based on the findings concerning the method for conducting cross-sectoral exercises obtained in the First Action Plan. Also, improvement of the cross-sectoral critical infrastructure protection measures should be aimed utilizing the achievement, obtained through study of exercise scenario and conducting exercise, such as “cultivation of the common recognition of cross-sectoral threats”, “strengthening of each sector’s response capabilities to it’s own sector through recognition of how other sectors responded” and “strategy to effectively operate the information sharing between the public and private sectors. Issues revealed through the exercises should be shared by sectors and organizations concerned, in order to make them useful for promoting efforts toward improvement, including issues regarding current legal system of the critical infrastructure sector and issues regarding management mechanism of critical infrastructure providers.

### (1) Conducting cross-sectoral exercises

Through understanding the latest trends concerning threats that could lead to IT malfunctions, aiming at improvement of the cross-sectoral critical infrastructure protection measures against those threats, studying exercise scenario assuming specific IT malfunctions and continuously conducting the cross-sectoral exercises based on the scenario, issues should be clarified and findings required to conduct exercise should be arranged. Prior to conducting exercise, exercise scenario and appropriate method of conducting exercise should be studied mainly by critical infrastructure providers.

Improvement of cross-sectoral critical infrastructure protection measure should be attempted by applying the issues clarified through the exercise such as the ones related to information security measures and information sharing between public and private sectors to reconsideration of information sharing system.

With regard to the rapid restoration procedures and the business continuity plan of critical infrastructure providers, efforts are expected to be promoted, by incorporating them into the exercise scenario that could be left to each sector’s option to study, from the viewpoint of achieving autonomous and effective cooperation and coordination between sectors and organizations concerned.

As exercises are effective methods to verify the validity of response to IT malfunctions, the improvement of the information security measures of critical infrastructure providers is expected by clarifying and providing the findings required for conducting exercises obtained through the cross-sectoral exercises such as scenario development and methods of operation of exercise making the findings to be useful for each critical infrastructure provider to apply them to the effort of their own sector.

### (2) Promotion strategy

Issues and findings concerning exercise scenario, deciding variables as parameter of exercise, studies and methods of conducting exercise obtained through study and conduct of exercises are clarified and summarized.

Issues and findings clarified and summarized should be reflected on development of the scenario for the next cross-sectoral exercises and consideration of exercise method, and the findings should be enhanced continuously.

These issues and findings should be disclosed to the parties concerned and shared in order to promote effort to strengthen information security measures in each critical infrastructure sector.

## 5. Response to environmental change

It is necessary to adapt information security measures promptly to environmental change in order to keep on maintaining effectiveness of information security measures as the situation such as social environment and the technological environment is changing from time to time.

Therefore, each organization concerned should make efforts to improve capability to sense environmental change that was not considered at the time the Second Action Plan was developed, through broad range of public relations to and hearing from the people, risk communication between parties concerned and international cooperation. Also, If the framework of the Second Action Plan can not solely cope with the environmental changes sufficiently, the Cabinet Secretariat should consider appropriate systems that would enable necessary response.

### (1) Public relations and hearing activities

In order to minimize the impacts of IT malfunctions, it is also important for people to be able to understand situation and calmly respond to the failure, as well as strengthening information security measures implemented by critical infrastructure providers.

Therefore, the organizations concerned with critical infrastructure protection of Japan should promote public relations with regard to the efforts taken based on the Action Plan to accomplish the accountability to the people, as well as providing information that is necessary for the people to calmly respond. Also, it is important to increase the organizations that were interested in the Second Action Plan through the public relations and hearing activity in order to gain broad range of cooperation and supports.

It is assumed that the efforts taken by the organizations concerned based on the Action Plan would broadly be announced using websites etc. In particular, conference material submitted to the critical infrastructure special councils should be disclosed as much as possible. The organizations concerned should announce their efforts taken as much as possible.

As the public hearing activity, the Action Plan should be introduced using wide range of opportunities such as seminars and efforts should be made to collect opinions from the people. Opinions would also be collected through websites, and they would be referred to promote the Action Plan, as well as be used as material to review and reconsider the Action Plan.

### (2) Enhancement of risk communication

It is important to enhance risk communication to promote mutual cooperation among the organizations concerned Risk communication is a communication made among parties concerned who should cooperate in terms of information security measures to eliminate misunderstanding and lack of understanding, share recognition of the risk which could exert other organizations. This communication is expected to lead to common recognition among different parties on the risks that should be responded in cooperative manner and measures that should be taken, and increase effects of cooperation in information security measures. It is also expected to lead to stronger relationship of mutual trust between the organizations concerned.

Therefore, it is required to attempt to increase opportunities for direct communication between the organizations concerned.

The risk communication is intended to be made within the necessary range between the organizations concerned and, for instance, it is not intend to disclose confidential information to public. Naturally, information which is concerned to lead to increase of threats due to its disclosure should be carefully handled depending on the situation.

### (3) Promotion of international cooperation

Globally, under the concept called “Critical information infrastructure”, the best practices are developed and shared to protect it. In specific, there are discussions on sharing the best practice of analysis and countermeasures concerning the threat to the control systems which support the critical information infrastructure, and analysis of the interdependency between critical information infrastructures. The Cabinet Secretariat would obtain information with regard to the latest trends through international conferences and dialogues with organizations of foreign countries, in cooperation with the the organizations concerned that actively participate in international cooperation, and make efforts to share the information obtained while paying particular attention to handling confidential information.

### (4) Strengthening the basis for information security

In order to strengthen the basis for information security, the schemes for human resource development, research and development and efforts at the regional level should be promoted respectively.

Human resource development should include exercise, training and seminars to foster personnel with advanced IT skills.

Research and development should be promoted to contribute to strengthening of the ability to respond to threat. This could be achieved by adding the viewpoint that would contribute to the entire countermeasures against IT functional failures which could be cause of IT malfunctions in the critical infrastructures to the research and development/technological development strategies concerning the information security, at the stage of studying the strategies.

For efforts at regional level, system should be developed, at a normal times, for information sharing and cooperative partnership among the government office’s local branches, local governments and critical infrastructure providers and the local information security organizations coupled with the systems of the government.

## (5) Promotion strategy

### A. Public relations and hearing activities

The web site of the National Information Security Center of the Cabinet Secretariat should be fulfilled to enable users to make unified access to the public relations information concerning the policies under the Second Action Plan. Especially, the state of the progress of the annual plan, results of verification of countermeasures and policies, and information about surveys concerning information security measures should be disclosed as much as possible.

### B. Enhancement of risk communication

Each organization concerned should make efforts for risk communication within the necessary range, and for disclosure of the information about the information security measures within the acceptable range.

### C. Promotion of international cooperation

As for international cooperation, it is necessary to continue participating in the early warning/monitoring/alert networks for critical infrastructure protection, Meridian[22] and the international efforts regarding critical infrastructure protection made at international organizations such as OECD. Through those efforts, cooperation with foreign countries would be made and international cooperation would be promoted with regard to development of the best practice concerning information security measures and conducting joint exercises that takes Japan's trend of information security into account.

### D. Strengthening the basis for information security

Each organization concerned should actively make efforts to solve issues such as improvement of current technologies, arranging cooperative systems, legal system and corporate management and comprehensive development of human resources, and share information on the status with each other in timely and appropriate manners.

[22] An international forum where discussion are facilitated specifically concerning the critical information infrastructure protection. Government officials responsible for the critical information infrastructure protection from various countries attends the meeting for discussion. The name Meridian originates from the fact that the first conference took place in Greenwich, England.

## III. Matters to be taken by organizations concerned

### 1. Promotion system

The core of the information security measures shown in the Second Action Plan includes voluntary measures that should be taken by private companies, such as the critical information infrastructure providers, and those which should be taken by the government-affiliated organizations, mainly by the Cabinet Secretariat. The organizations concerned are expected to promote the information security measures by playing their own roles as below.

The Cabinet Secretariat takes cross-sectoral measures common to each critical infrastructure sector, in cooperation with the organizations concerned. The cabinet will also promote the maintenance of the systematic information sharing system of public and private sectors for the protection of the critical infrastructure in cooperation with the organizations concerned, as well as to support each organization to improve the ability of the protection.

The critical infrastructure sector-specific ministries take measures linked with the policies of the Cabinet Secretariat to protect the critical infrastructure for the entire nation. They also make efforts to recognize the activities for the information security of critical infrastructure providers, and provide information, advice and guidance to critical infrastructure providers.

The information security related ministries take measures contributing to the critical infrastructure protection of the entire nation, which is led by the Cabinet Secretariat.

The law enforcement ministries take measures to the measures contributing to the system of the critical infrastructure protection of the entire nation, which is led by the Cabinet Secretariat.

The related agencies are expected to take policies and measures to enhance the critical infrastructure protection of the entire nation.

Critical infrastructure providers are encouraged to take measures linked with the policies of the Cabinet Secretariat and make efforts to increase the effectiveness of public and private sectors. They are also encouraged to cooperate with the activities of CEPTOARs and the CEPTOAR Council.

CEPTOARs are encouraged to enhance information sharing in their sectors in terms of the critical infrastructure protection. They are also encouraged to enhance information sharing with the Cabinet Secretariat and the critical infrastructure sector-specific ministries, as well as participating in the CEPTOAR Council to promote the cross-sectoral information sharing.

The CEPTOAR Council is encouraged to promote the cross-sectoral information sharing between the CEPTOARs.

2. Schemes of each organization concerned

(1) Policies of the Cabinet Secretariat

A) Policies on "maintenance and penetration of the safety standards etc”

[1] In addition to analyze and review the guideline annually, discussion on the revision of the guideline should take place in the initial year of the Second Action Plan and, if necessary, its results are disclosed.

[2] Supporting the continuous improvement of the safety standards in each critical infrastructure sector by presenting the results of the analysis and review of the guideline and the results of the common threat analysis.

[3] Investigation to understand the status of the continuous improvement of the safety standards are conducted annually in cooperation with the critical infrastructure sector-specific ministries, and the result is disclosed.

[4] The investigation of the penetration situation of the safety standards is conducted annually in cooperation with the critical infrastructure sector-specific ministries, and the result is disclosed.

B) Policies on "strengthening of information sharing systems”

a) Organization of information to be shared

[1] Information to be shared and the sharing method should be organized in cooperation with the organizations concerned. The results should be reviewed according to the reality, if necessary.

[2] Information from the organizations concerned is consolidated based on the information for sharing and information sharing methods, which would be provided to critical infrastructure providers.

[3] Measures necessary for enhancement of the systems obtained in the process of organizing information for sharing and items to be improved

b) Enhancement of information provision and liaison

[1] The review of the "communications procedures” should be promptly conducted to solve issues discovered in the First Action Plan period, such as the scope for information sharing, in cooperation with the organizations concerned.

[2] The reference manuals to show the interpretation for the operation of “the communications procedures” should be prepared, in cooperation with the critical infrastructure sector-specific ministries, for information to be known by CEPTOARs and critical infrastructure providers, if necessary,.

[3] The “communications procedures” and the reference manuals should be reviewed in a timely manner in cooperation with the organizations concerned.

[4] Maintenance of the information sharing system from the government to critical infrastructure providers, such as information provision by the critical infrastructure sector-specific ministries, assignment of communication personnel as a liaison at the Cabinet Secretariat.

[5] Consolidating information that should be provided to critical infrastructure providers, such as terrorist attack related information, threats, attacking methods and its recovering method related.

[6] Information should be provided to critical infrastructure providers based on

the information provided by the information security related ministries, law enforcement ministries and related agencies, and communication from critical infrastructure providers. In this case, the analysis on the objects affected, based on the interdependence analysis and the common threat analysis conducted under the Second Action Plan.

[7] Discussion takes place about the use of analysis functions of the related agencies.

[8] Discussion on the functions required for information sharing (e.g. encryption between each path) to critical infrastructure providers for cooperation with the critical infrastructure sector-specific ministries and CEPTOARs, if necessary.

[9] Discussion to increase the subjects to cooperate with the organizations to participate in the information security activities, as well as enhancing the cooperative relationship with the information security related ministries, law enforcement ministries and related agencies.

[10] In order to extract appropriate issues for research by the related agencies, the schemes of the Cabinet Secretariat and the trend of each critical infrastructure sector are communicated to related agencies in cooperation with the organizations concerned.

[11] Opportunities for confirming telecommunication functions are provided to maintain and improve the information sharing systems of CEPTOARs, as requested by CEPTOARs and on a regular basis, in cooperation with the critical infrastructure sector-specific ministries.

c) Strengthening of CEPTOARs

[1] Studies and hearing take place to understand the functions and current activities of each CEPTOAR on a regular basis, in cooperation with the critical infrastructure sector-specific ministries.

[2] Introduction of advanced functions and activities of CEPTOARs.

d) The CEPTOAR Council

[1] The Cabinet Secretariat will be the secretariat of the CEPTOAR Council for the time being.

[2] Support the operations and management in cooperation with CEPTOARs participating in the CEPTOAR Council.

[3] Enhancement of the CEPTOAR Council activities and provision of an environment required for accumulating and sharing information and know-how.

e) Others

[1] For explaining the activities to the people and society, each CEPTOAR and the CEPTOAR Council schemes are introduced in an acceptable range.

C) Policies on "common threat analysis”

[1] Preparation of action policies based on critical infrastructure providers’ intentions every year.

[2] Continuous investigation and analysis of the common threat

[3] Improvement of analysis quality in joint research with the research institutions, by pursing cooperation of external research institutions widely.

[4] Promotion of smooth information interchange and communication between

the research institutions and critical infrastructure providers.

[5] Summary of the annual analysis report is provided as a basic material to be reflected on the safety standards, and as the business continuity plan of the critical infrastructure.

D) Policies on "cross-sectoral exercises”

[1] The scenario, methods and issues on the cross-sectoral exercises are planned for implementation of the cross-sectoral exercises.

[2] By using the opportunities of the cross-sectoral exercises, the status should be reported for the results of the common threat analysis review, early restoration procedures and the business continuity plan in case of occurrence of IT malfunctions, which are voluntarily conducted by critical infrastructure providers. The results will be provided to the participants of the exercises.

[3] Improvement plan for the cross-sectoral exercise

[4] Consolidating and accumulation of findings on the cross-sectoral exercises

E) Policies on "response to environmental change”

[1] Making efforts to collect information on changes of threats and risks. Taking actions if necessary, in cooperation with the critical infrastructure sector-specific ministries.

[2] The web site concerning the public relations for the information security measures is established.

[3] Supporting the risk communication among critical infrastructure providers

[4] Construction of the linkage system to respond to disasters and physical terrorism, etc.

[5] While collecting the best practices of various foreign countries, the trend and standardization of international organizations concerning the information security polices should be recognized.

[6] By collecting information on international threats and vulnerabilities, the information is provided to the organizations concerned.

[7] Introducing the opportunities to enhance the international cooperation such as joint exercises to critical infrastructure providers in cooperation with the government agencies and international organizations of foreign countries

[8] Promotion of human resource development of personnel with the advanced information security skills, through the cross-sectoral exercises.

F) Schemes to enhance the Cabinet Secretariat’s own functions

[1] Using information collected and analyzed according to "the support of government agencies” which specified in "Aiming for review of the roles and functions of the government tacking the information security problems” (IT Strategy Headquarters, December 7, 2004)

[2] Maintaining environmental change to secure confidentiality and to conduct a secure information exchange from the aspects of human and physical related, for handling confidential cooperate information of each critical infrastructure sector

[3] Enhancing the central function to coordinate critical infrastructure providers in case of emergency such as IT malfunctions

[4] Enhancing research activities on the measures taken by the organizations concerned, and environmental change required for information security measures

(2) Policies of the critical infrastructure sector-specific ministries

A) Policies on "maintenance and penetration of the safety standards etc”

[1] Providing information on the standard and the guideline which may be newly specified as a safety standard to the Cabinet Secretariat.

[2] Revising the safety standards as required, in addition to the analysis and verification of the safety standard on a constant basis, if the safety standards are specified by their own.

[3] Supporting the analysis and the verification of the safety standards for each critical infrastructure sector, if the safety standards are not specified by their own.

[4] Penetration of the safety standards including the environment to be created to take measures for critical infrastructure providers.

[5] Cooperating with the Cabinet Secretariat to annually assess the situation of continuous updates of the safety standards.

[6] Cooperating with the Cabinet Secretariat for the annual survey of the penetration situation of the safety standards.

B) Policies on "strengthening of information sharing systems”

a) Revew of the criteria for information to be shared

[1] Cooperating to review the criteria for information to be shared and its sharing method

[2] If CEPTOARs independently reviews the criteria for information to be shared and the information sharing method, supporting CEPTOARs.

b) Enhancement of information provision and liaison

[1] Cooperation with the Cabinet Secretariat for enhancement of the system to properly collect, provide and share information.

[2] Maintenance of a close partnership for information sharing with critical infrastructure providers

[3] Maintenance of the information sharing rules between critical infrastructure sector-specific ministries and CEPTOARs, and between critical infrastructure sector-specific ministries and critical infrastructure providers, as well as updates of the policies including pursuing the consistency with “the communications procedures”.

[4] Enhancement of information provision and liaison, review of “the communications procedures” by the Cabinet Secretariat for the improvement of the operation, the development of the reference manuals on operations of the communications procedures, and cooperation to announce the information to CEPTOARs and critical infrastructure providers.

[5] Discussion with CEPTOARs as necessary and cooperating with the Cabinet Secretariat about the functions required for information sharing in providing information to critical infrastructure providers (e.g. encryption of data between each path)

[6] Communicating with the Cabinet Secretariat according to “the communications procedures” and the information sharing rules between critical infrastructure providers concerning IT malfunctions related report from critical infrastructure providers.

[7] For provision of information from the Cabinet Secretariat, providing information to CEPTOARs according to “the communications procedures”

and the information sharing rules with CEPTOAR.

[8] Collection of information which should be provided to critical infrastructure providers, depending on the capabilities and functions owned (e.g. information on terrorism and threats, attacking and restoration methods)

[9] Cooperating with the Cabinet Secretariat whey they provide opportunities for communication to CEPTOARs.

c) Strengthening of CEPTOARs

[1] Cooperation for investigation and hearing to understand the functions and current activities of each CEPTOAR that is conducted by the Cabinet Secretariat

[2] Support CEPTOARs to enhance the functions

d) The CEPTOAR Council

[1] Supporting the CEPTOAR Council

[2] Exchanging opinions as requested by the CEPTOAR Council

C) Policies on "common threat analysis”

[1] Coordinating with critical infrastructure providers to facilitate smooth cooperative relationship between the Cabinet Secretariat and critical infrastructure providers

[2] Providing information to the Cabinet Secretariat on the objects that require the common threat analysis, or information necessary for the common threat analysis.

[3] Evaluation of the basic materials provided as a result of the common threat analysis

[4] Utilize to the policies the basic material provided as a result of the common threat analysis

D) Policies on "cross-sectoral exercises”

[1] Providing Information on the scenario, methods for implementation and issues for review, which are required for the cross-sectoral exercises to the Cabinet Secretariat.

[2] Cooperation in making scenarios, methods for implementation and issues for review of the cross-sectoral exercises, and implementation of the cross-sectoral exercises

[3] Participation in the cross-sectoral exercises

[4] Supporting CEPTOARs and critical infrastructure providers in the cross-sectoral exercises.

[5] Cooperation for study on the improvement methods of the cross-sectoral exercises

[6] Making efforts to use the results of the cross-sectoral exercises to policy making, as required.

E) Policies on "response to environmental change”

[1] Providing to the Cabinet Secretariat information contributing to the public relations and hearing on the information security measures.

[2] Supporting the risk communication among critical infrastructure providers

[3] Construction of the linkage system to respond to disasters and physical terrorism, etc.

(3) Policies of the information security related ministries

A) Policies on "strengthening of information sharing systems”

[1] Collecting information such as terrorism, threats, attack and restoration methods, depending on the ability and function to have.

[2] Promoting the cooperation with the Cabinet Secretariat for enhancing the system to collect, provide, and share information, and actively provide information to the Cabinet Secretariat.

[3] Cooperation of review of the "communications procedures” which is conducted by the Cabinet Secretariat for enhancement and improvement of operation, information provision and liaison.

[4] Exchanging opinions as requested by the CEPTOAR Council

B) Schemes to enhance the ministries’ own functions

[1] Continuous execution of the schemes by the information security related ministries such as improvement of response abilities

(4) Policies of the law enforcement ministries

A) Policies on "strengthening of information sharing systems”

[1] Collecting information such as terrorism, threats, attack and restoration methods, depending on the ability and function to have.

[2] Promoting the cooperation with the Cabinet Secretariat for enhancing the system to collect, provide, and share information, and actively providing information to the Cabinet Secretariat.

[3] Cooperation of review of the "communications procedures” which is conducted by the Cabinet Secretariat for enhancement and improvement of operation for information provision and liaison.

[4] Exchanging opinions as requested by the CEPTOAR Council

B) Schemes to enhance the ministries’ own functions

[1] Continuous execution of the schemes by the law enforcement ministries concerning measures against cyber terrorism such as improvement of response abilities

(5) Matters expected as a voluntary scheme of the related agencies

A) Policies and measures on "strengthening of information sharing systems”

[1] Cooperation in the schemes to organize information for sharing specified by the Cabinet Secretariat and its sharing method

[2] Cooperation of review of the "communications procedures” which is conducted by the Cabinet Secretariat for enhancement and improvement of operation, information provision and liaison.

[3] Actively providing information to the Cabinet Secretariat.

[4] Supplemental information sharing upon agreement with critical infrastructure providers or CEPTOARs to share information

[5] Cooperation in discussion for enhancement of the analysis conducted by the Cabinet Secretariat

[6] Exchanging opinions as requested by the CEPTOAR Council

B) Policies and measures on "cross-sectoral exercises”

[1] Providing information to the Cabinet Secretariat on threats to incur IT malfunctions, and IT malfunctions case studies, which are required to carry out cross-sectoral exercises.

C) Schemes contributing to information security measures by each related agency

[1] The National Police Agency Cyberforce is to enhance the capabilities of personnel to collect various relevant information, as well as to train personnel with advanced IT skills.

[2] NICT conducts the research and development of the integrated technology concerning preparatory measures against various attacks on the cyber space, responses to incidents, post-measures, safety assessment of the encryption protocol and new sectors of application of the encryption technologies

[4] AIST conducts the a comprehensive research and development such as hardware, software, security analysis of the encryption technology used herein, and assessment technologies and proposals for new security technologies

[5] IPA collect and analyze information to promote the sharing of information about IT malfunctions and related experiences, in addition to development of the software engineering including the common references to quantitatively assess the reliability of information systems, and creation of the checklist according to the countermeasures against malfunctions for improvement of the reliability of information systems and implementation of the information security measures. IPA also designs and implements the test categories and items concerning the information security for The Information Technology Engineers Examination (ITEE) as well as to provide the knowledge items concerning the information security for various skill standards, and promote it for penetration. Moreover, the tasks include the information collection and analysis concerning domestic and international information security for critical infrastructure and promotion activities concerning the management methods of information security for the critical information infrastructure providers. The research and development concerning the safety assessment of the encryption protocol and the encryption protocol safety assessment are also conducted.

[5] Telecom-ISAC Japan provides the opportunities for cooperation concerning the information security actions of the cross-sectoral communication between the enterprises led by the telecommunications carrier to collect, analyze and share network incident information. It also conduct the verification of functions and enhancement of cooperation to strengthen the response capabilities against cyber attacks to the telecommunications carriers. The tasks also includes schemes for promotion of the network security literacy of the end users, contribution to making the policies for human resource development of the network security and studies on technical and operational issues concerning protection of the data communication networks.

[6] JPCERT/CC conducts coordination between parties concerned to cope with incidents, threat analysis of attacks and support activities concerning the study of countermeasures based on the information provided by critical infrastructure providers and their requests. It also widely collect and analyze vulnerability related information concerning controlling systems, software products and protocol, and threat related information such as attacks to

specific websites, and provide the information to critical infrastructure providers, CEPTOARs, the CEPTOAR Council or Cabinet Secretariat as "early-warning information” on the basis of prior agreement with critical infrastructure providers. The tasks also include promotional activities concerning the information security management type countermeasures for critical infrastructure providers.

(6) Matters expected as voluntary measures of critical infrastructure providers

A) Measures on "maintenance and penetration of the safety standards etc”

[1] Revising the safety standards as required, in addition to the analysis and verification of the safety standard on a constant basis, if the safety standards are specified by their own.

[2] Cooperating to track the status of continuous updates of the safety standards conducted by the Cabinet Secretariat every year, if the safety standards are specified by their own.

[3] Discussion on implementation of the information security measures based on the safety standards, as well as maintenance of the environment to actually take the countermeasures

[4] Considering if the information security audit or equivalent or information security report or equivalent should be conducted or prepared as a voluntary action

[5] Making efforts to enrich the explanation to outside organizations on the information security measures.

[6] Cooperating the Cabinet Secretariat on their survey of the safety standard penetration conducted annually.

B) Measures on “strengthening of information sharing systems”

[1] Properly operating the handling rules of information within CEPTOARs and participate in activities as a CEPTOAR member.

[2] Communicating information as required in case of IT malfunctions, while maintaining the information sharing system.

[3] Collection of information to be provided to critical infrastructure providers (e.g. information related to terrorism and threat, and information on attack and restoration methods) corresponding to ability and function to have

[4] Supplementary information sharing based on the mutual agreement with related agencies

[5] Conducts of activities as requested by the CEPTOAR Council

C) Measures on "common threat analysis”

[1] Proposing threats which are difficult to analyze by their own but worth to analyze as a common threat as an object of the common threat analysis every year.

[2] Smooth information exchanges and communication with the Cabinet Secretariat, and outside research institutions who are jointly participating in the common threat analysis.

[3] Actively providing practical information necessary for the common threat analysis to the Cabinet Secretariat.

[4] Participating in the discussion and studies on the common threat analysis.

[5〕Assessment of the basic materials provided as a result of the common threat analysis

[6] Use of the basic information provided as a result of the common threat analysis to the business continuity plan.

D) Schemes for "cross-sectoral exercises”

[1] Providing the information on the scenario, methods and issues on the cross-sectoral exercises required for implementation of the cross-sector type exercises to the Cabinet Secretariat.

[2] Cooperating in planning the cross-sectoral exercise scenario, methods and issues, and implementation of the cross-sectoral exercises

[3] Participation in the cross-sectoralexercise

[4] Cooperation for studies to improve the cross-sectoral exercise

[5] Making efforts to use the results of the cross-sectoral exercises, for developing the early restoration procedures and the business continuity plan in case of occurrence of IT malfunctions, as necessary.

E) Measures on "response to environmental change”

[1] Studying if the schemes for the information security should be introduced for the people.

[2] Making efforts to enhance the risk communication between organizations concerned that directly relate to information security measures of the critical infrastructure services.

(7) Matters expected as voluntary measures of CEPTOARs

A) Measures on "strengthening of information sharing systems”

[1] Organization of the information shared within CEPTOARs and the sharing method of information within CEPTOARs, in cooperation with the critical infrastructure sector-specific ministries. The contents should be reviewed according to the reality, as necessary.

[2] Information provision and sharing within CEPTOARs and with other CEPTOARs based on the organized information and the information sharing method.

[3] Cooperation for the "communications procedures” conducted by the Cabinet Secretariat for information provision, enhancement of communication and improvement of communication.

[4] Cooperating with the Cabinet Secretariat and the critical infrastructure sector-specific ministries concerning the functions required for information sharing while providing information to critical infrastructure providers (e.g. encryption of data between each path)

[5] Periodic confirmation of information communication functions

[6] Providing information to critical infrastructure providers based on the information handling rules within CEPTOARs concerning information provided by the Cabinet Secretariat

[7] Supplementary information sharing based on mutual agreement with the related agencies

[8] Enhancement and fulfillment of function of CEPTOARs

[9] Cooperation in investigation and hearings to understand functions and current activities of each CEPTOAR that are conducted by the Cabinet Secretariat

[10] Participation in the CEPTOAR Council

B) Measures on "common threat analysis”

[1] Participating in voluntary activities of critical infrastructure providers concerning the common threat analysis.

C) Measures on "cross-sectoral exercises”

[1] Participation in the cross-sectoral exercises

(8) Matters expected as voluntary measures of the CEPTOAR Council

A) Measures on "strengthening of information sharing systems”

[1] Organization of the information for sharing and its sharing method

[2] Studies on various measures including review of the “communications procedures” conducted by the Cabinet Secretariat, proposals for improvement of reference materials, and improvement of the system to provide information to critical infrastructure providers

[3] Studies concerning improvement of the consideration of matters such as functions requested by the Cabinet Secretariat in the information provided by critical infrastructure providers (e.g. encryption of data between each path)

[4] Promotion of the cross-sectoral type information sharing through mutual understanding and sharing information on specific cases such as best practices, based on the information for sharing and its information sharing method.

[5] Exchanging opinions to further share the common recognition of both parties, as requested by government agencies or by their own in order to deepen the cooperative relationship with the government agencies.

## IV. Assessment/Verification and Review

### 1. The Promotional System of the Action Plan

#### (1) Assessment and verification of the progress of the Action Plan

In order to securely proceed the actions and continuously update it under the Second Action Plan, the progress should be assessed and verified. The continuous improvement should focus on sharing experiences of the organizations concerned obtained through their own actions to share each other, and use the lessons for improvement of their scheme to follow. Although IT malfunctions should be avoided, it is important to recognize that experiences in preventing IT malfunctions or limiting the range of influences in case of IT malfunctions should be used for the future development of each organization.

Naturally, the person concerned who causes an IT malfunctions should identify the cause and responsibility to improve his/her schemes. However, the assessment and verification in the Second Action Plan focuses on extracting lessons useful for the future improvement of measures based on various experiences, for improvement of the schemes of each organization concerned, rather than mainly pursing the cause and responsibility.

The assessment and verification in the progress report of the Second Action Plan should cope with two aspects: "measuring the output (achievement) ” and “measuring the outcome (result)” which show how the society comes to the ideal figure for the future. The assessment should be made upon the review of such objective indicators, whatever possible.

The Second Action Plan refers to “verification” as a confirmation of each action based on the objective indicators concerning the progress, while “assessment” is to review the rationality of the actions compared to the goal.

The verification from “aspects to measure the achievements (output)” should focus on the individual information security measures based on the Second Action Plan. The core of the information security measures under the Second Action Plan has multiple layers in structure comprising of various organizations, which would make the indicators for verification vary. However, there should be indicators for verification of the measures implemented by critical infrastructure providers, and the other for review of policies developed by the government agencies in general. These verifications are conducted by the Cabinet Secretariat in cooperation with critical infrastructure providers and critical infrastructure sector-specific ministries.

The assessment of the measures implemented by individual critical infrastructure providers should be conducted by the providers themselves in principle, considering the fact that the assessment should be a voluntary action. The assessment of policies by the government agencies should be conducted by the Information Security Policy Council.

In this case, it is important to recognize that the indicator of each core of the information security measures should be properly interpreted in terms of the actual meaning of the figure, not be confused of the volume or increase/decrease of the figure itself.

The evaluation and verification from the "aspect to measure the result (outcome) ” should focus on the goal and ideal future of the Second Action Plan. In considering that various information security measures could have results relating each other under the Action Plan, this is not solely for assessment and verification of the individual information security measures but for the entire framework of the information security measures or the framework of the Second Action Plan in a comprehensive and analytical manner.

It is also important to understand the status beyond the individual achievements of each core of the information security measures, for assessment of the framework of the Action Plan. Therefore, supplemental investigation should be conducted to collect supplemental information required for the assessment.

Reviews of achievements of measures, achievements of policies and supplemental investigation should be conducted by the Information Security Policy Council every year, while surveys required for the review will be conducted by the Critical Infrastructure Special Committee in corporation of the critical infrastructure sector-specific ministries.

As assessments of the results based on the Action Plan are, due to its nature, difficult to study its improvement scheme immediately through tracking down the change of every year, it should be conducted once every three years by the Critical Infrastructure Special Committee in corporation of the critical infrastructure sector-specific ministries.

(2) Review of the results

Critical infrastructure providers are taking information security measures on a daily basis as the figure that have a primary responsibility for constant supply of the critical infrastructure services. In order to continue and update the scheme, as well as to improve the support of the government for critical infrastructure providers, it is important to conduct an objective review on the results of the information security measures each other.

In the reviews of measures, the occurrence of IT malfunctions should be reviewed in terms of the critical infrastructure services for which each critical infrastructure sector has defined the verification level, following to the goal of the Second Action Plan “IT malfunctions should not exert a significant influence on people’s social lives and economic activities” with the verification of the occurrence of IT malfunctions beyond the verification level for the critical infrastructure services which are the targets for review of each critical infrastructure sector. The critical infrastructure services and the review level are as shown in Appendix 2. The specific goal is the total number of IT malfunctions beyond the acceptable level in the ten sectors, as recognized by the Cabinet Secretariat.

It should be noted that it is inappropriate to assess measures by comparing the occurrence of IT malfunctions per service provider or sector, as long as the measures of the individual providers include ones voluntary taken based on their own corporate policies. Therefore, the assessment of the measures should be based on the self-assessment by critical infrastructure providers, for them to voluntary take measures for improvement. It is also desired to identify the status of their self-assessment if possible.

(3) Review of the policies

The policies of the Second Action Plan, shown in II, are the policies to improve the effectiveness of information security measures which are encouraged to be implemented by critical infrastructure providers. While the First Action Plan focused on making the framework of these policies, the Second Action Plan is to review the effectiveness of each policy based on the fact that the frameworks will be completed as planned.

The review of the achievement of the policies aims to reveal the contribution of the policies developed for each core item of the information security to the information security measures implemented by critical infrastructure providers. Specific indicators are as below.

A) Maintenance and penetration of the safety standards etc

"Maintenance and penetration of the safety standards etc" is expected to achieve fulfillment of various measures by critical infrastructure providers, and its steady practice. Therefore, indicators should be designed as focusing on the fulfillment of the guideline and items of the safety standard and a secure implementation of the schemes based on the safety standard of individual providers. Specific indicators include the number of action items shown in the guideline and reference materials, the number of critical infrastructure providers who are taking the self-assessment on a constant basis according to the safety standard, and the assessment by critical infrastructure providers of the guideline.

B) Strengthening of information sharing systems

The results expected through "enhancement of the information sharing system" is the situation that critical infrastructure providers enjoy and use. This situation is expected to result from activities such as reviewing criteria for information to be shared among the organization concerned, developing the environment required for providing information and communication, and enhancing the voluntary activities of each CEPTOAR and the CEPTOAR Council. Therefore, there should be an indicator focusing on the fulfillment of the information to be shared by the information sharing system and a certain information sharing system. The specific indicators include the number of information announced by the Cabinet Secretariat, the number of information shared by CEPTOARs etc, and the number of critical infrastructure providers which were appreciated in terms of the information shared which is worth to be information security measures.

C) Common threat analysis

The goal expected with the "common threat analysis" is to provide basic materials contributing to making the continuous improvement of the guideline and the business continuity plan of critical infrastructure providers. Therefore, the indicators are designed at the beginning of every fiscal year, focusing on the achievement at the end of fiscal year for review items under the common threat analysis established in consideration of the necessity of critical infrastructure providers. Specific indicators include the number of items reviewed, as well as the result of assessments by critical infrastructure providers of each review results.

D) Cross-sectoral exercises

Achievements expected with "the cross-sectoral exercises" include early restoration procedures by critical infrastructure providers in case of occurrence of IT malfunctions, and contribution to review of the business continuity plans. In order to effectively use the findings obtained through the exercises to the business continuity in case of the actual IT malfunctions and early restoration activities, exercises on a situation similar to the reality is important. It is also desired to have as much players as possible who play various roles. Therefore, the indicators should be defined as focusing on whether the increase of participants of the exercises and findings obtained through the exercises are contributing to the schemes of critical infrastructure providers. Specific indicators include the total number of participants of the exercises and the number of critical infrastructure providers who appreciated that the findings obtained through the exercises is worth to be the information security measures of the organization concerned.

E) Response to environmental change

Among the policies shown in “response to environment change”, the achievements expected with "public relations and hearing activities” are to confirm understanding of people in a wide range for the framework of the Action Plan and to increase the participants of the Second Action Plan other than the organizations concerned. Therefore, there should be an indicator focusing on the fulfillment of the opportunities for them to recognize the Second Action Plan. Specific indicators include the level of satisfaction of the website contents, and the number of seminars to introduce the Action Plan.

Among the policies shown in “responses to environment change”, the achievements expected with "risk communication” is to improve the understanding of each organization concerned on their activities and creation of the environment to facilitate its partnership. Therefore, the indicator should be designed as focusing on fulfillment of the communication opportunities between organizations concerned. A specific indicator is the number of opportunities of communication between the organizations concerned such as the CEPTOAR Council and cross-sectoral exercises.

F) Enhancement of research activities

It is important to understand how these measures were used for measures taken by critical infrastructure providers. The Cabinet Secretariat collects the statistic information which are voluntarily taken by the organizations concerned, and attempt to fulfill their research activities. In this case, the Cabinet Secretariat should understand the settings of the service level of critical infrastructure providers within a possible range to improve the effectiveness of the policies on the countermeasures. In order to do this, it is necessary to take particular care to avoid excessive workloads to critical infrastructure providers.

(4) Supplemental survey for assessment of the result

Although a result review using indicators is essential to see the actual situation, it only shows one aspect of the fact. It is necessary to make a supplemental survey for aspects invisible from the indicators, in order to assess the outcome expected by the Second Action Plan, under the conditions close to the reality. Therefore, a supplemental survey was conducted for the cases such as IT malfunctions, so as to obtain information for assessment of the policies and measures based on the

Second Action Plan.

The supplementation survey is supposed to be conducted annually. The results should be disclosed whenever possible.

### (5) Evaluation of the results based on the Action Plan

The results of the Action Plans should be assessed, considering the ideal future figure aimed under the Second Action Plan.

In terms of the ideal state for the future, it is difficult to make an analytical assessment how much the results of each measure and policy contributed to the result. Furthremore, it is not appropriate to assess various actions in a uniform manner with the same time sequence, since there are time lags between the actions taken, such as each policy and measure, and the achievement. Accordingly, a general evaluation was made for the Action Plan itself as the sum, not analyzing individual policies and measures under the Second Action Plan how the Action Plan contributes to the results.

In the assessment of the results of the Action Plan, it was to evaluate whether the schemes under the Action Plan are suited to the achievement of the outcome of the Second Action Plan as a whole, as the Cabinet Secretariat summarized the results of review on the measures, policies and the supplemental survey. In this case, it is important to focus on how to improve the actions in a balanced fashion of the entire plan, not only focusing on individual measures and aspects beyond the policies.

### (6) Review of the Action Plan

The Second Action Plan was based on the results of measures, policies, supplemental survey and items for assessment ("assessment" hereinafter). Meanwhile, based on the changes of social conditions concerning IT services including threats and IT malfunctions, the Action Plan should be reviewed every three years, or as required. In the term of the Second Action Plan, the plan should be reviewed over at least twelve months after two years from the launch.

Factors for review in particular includes the goal and its basic direction, the scope of critical infrastructure providers, the scope of the organizations concerned, addition and abolishment of measures and policies, examples of potential threats expected, the scope of the critical infrastructure services, the service level, review level and assessment indicators. In line with this, it is necessary to review the definition of terms and the scope of the Action Plan as required.

For review of the Second Action Plan, it is necessary to study the plan while considering the characteristics of each sector and actions taken, as well as the fact that the measures taken by the service providers are voluntary. In case of unexpected events beyond the scope of the Second Action Plan, it is important to have preparation to respond against such unexpected conditions.

The Critical Infrastructure Special Committee shall review the Action Plan. Upon agreement of the committee, the Information Security Policy Council will determine the new action plan to follow.

## 2. Cooperation with the existing systems for information sharing

There are existing information sharing systems, other than the framework of information sharing under the Second Action Plan, in terms of emergency measures and disaster prevention. In case of occurrence of IT malfunctions under the circumstance assumed by the existing information sharing system, it is desired to have link the Second Action Plan and these systems of information sharing. Therefore, the Cabinet Secretariat should study on measures for smooth information sharing in cooperation with government agencies concerned.

Attachment: Information provision and liaison

## 1. Information on IT malfunctions

"Information concerning IT malfunctions" refers to information on the information security measures related to IT malfunctions and disabilities in general.

IT malfunctions information includes three aspects 1) prevention of IT malfunctions, 2) prevention of IT malfunctions from spreading expansion and ensuring immediate restoration and 3) prevention of reoccurrence through analysis and review of the factors of IT malfunctions. The government must provide the information in an appropriate and proper manner to critical infrastructure providers. The information sharing system of such information also must be enhanced between critical infrastructure providers, and between the critical infrastructure sectors in the relationship of interdependence.

Various aspects of information concerning IT malfunctions are as below:

1) Prevention
Information concerning threats of failure (including the protective measures)

2) Avoidance of extension and restoration
Information related to the transmission of impacts after occurrence of malfunctions and restoration of the normal status

3) Prevention of reoccurrence
Joint actions to collect information concerning post-analysis and results of analysis and review.

## 2. Information provision to critical infrastructure providers

### (1) Scope of critical infrastructure providers to provide information

The scope of information provided from the Cabinet Secretariat to critical infrastructure providers is assumed to be a critical infrastructure sector thought by the Cabinet Secretariat to be related to the information in question, within the scope acceptable to the information source as specified in advance. When the Cabinet Secretariat perceives that the information should be shared beyond the acceptable scope for information sharing as specified by the information source, the change of scope for the information may be coordinated with the information source.

### (2) Information provided

Various information provided by the information security related ministries concerned, law enforcement ministries and related agencies should be collected for analysis and only those which assumed to be effective for information security measures would be provided.

If information provided by critical infrastructure providers applies to [1] or [2] below, such information should be provided upon taking an appropriate measure such as processing the information to conceal the identification of critical infrastructure provider as the information source, in order to prevent them from being suffered from any disadvantages.

[1] If there is a risk that critical infrastructure provider obtained information concerning security holes and program bugs, which could affect other critical infrastructure providers with problems related to the information.

[2] If the critical system of other critical infrastructure providers could be at risk such as cases of occurrence of cyber attacks or its announcement, as well as any damages expected due to disasters are expected.

(3) Mechanism of information provision

Information should be provided from the Cabinet Secretariat to critical infrastructure providers through the critical infrastructure sector-specific ministries as below:

[1] If the Cabinet Secretariat provides information, it should be provided through the liaison (or the Cabinet Secretariat) assigned for each sector by the critical infrastructure sector-specific ministries. In this case, they should improve the identification patterns to facilitate the users of information to refer the information which they need at a glance, by listing the classification and scope of information depending on the priority and contents.

[2] The liaison of the critical infrastructure sector-specific ministries conveys information to the point of contact (POC) of CEPTOARs.

[3] CEPTOARs aim to share information between critical infrastructure providers who are the members of the CEPTOARs.

[4] In case of early warning information, especially in urgency, the Cabinet Secretariat directly provide such information to CEPTOARs or the individual critical infrastructure providers, and distribute the information to the liaisons of the critical infrastructure sector-specific ministries at the same time, regardless of the procedures (3) [1] – [3]. Meanwhile, the identification patterns should be standardized should be subject to the procedure of [1]. In terms of the early warning information etc. there should be an agreement between the information source and the Cabinet Secretariat on how to use the information due to its nature of information to be handled with care.

(4) Coordinated systems for information provision

The Cabinet Secretariat should cooperate with the information security related ministries, law enforcement ministries and related agencies in collecting information to be provided to critical infrastructure providers, and provide the information to critical infrastructure providers through the critical infrastructure sector-specific ministries.

[1] Consolidating a wide range of information provided by the information security related ministries, law enforcement ministries and related agencies.

[2] Providing information of disasters assumed due to terrorist attacks to the law enforcement ministries, and provision of information concerning the attacking method to the information security related ministries concerned.

[3] Requesting cooperation of the related agencies as necessary for collection and analysis of information

[4] Disaster related information should be collected and shared under the control of the existing information sharing system between the Cabinet Secretariat, the Cabinet Office, and other related ministries.

(5) Enhancement of information quality (e.g. analysis information and impact level)

The following should be considered for information to be provided in order to improve the quality.

[1] Improvement of accuracy by cross-checking of information

[2] Determination of priority and importance based on the above.

[3] Interdependence analysis conducted under the First Action Plan and prediction of influences based on the common threat analysis

[4] For IT malfunctions incurred by suspension or poor performance of other critical infrastructure sectors, or those which due to the common threats, its statistical data should be obtained from the status and scale.

3. Communication from critical infrastructure providers

(1) Cases require communication and information to be transmitted

Communication is required for the cases [1] to [4] below, if reporting is mandated under the laws and regulations and when critical infrastructure providers determines the cases as particularly critical.

[1] By intentional factors including cyber attacks
A) IT malfunctions occurred
B) Cyber attacks are detected or its announcement for an attack was received
C) Damages due to cyber attacks are detected
E) IT disabilities were confirmed, threats occurred and other events occurred which would require countermeasures by other critical infrastructure providers for its critical level

[2] Non-intentional factors

A) IT malfunctions occurred
B) IT disabilities were confirmed, threats occurred and other events occurred which would require countermeasures by other critical infrastructure providers for its critical level

[3] Disasters and sickness

A) IT malfunctions occurred
B) IT malfunctions are expected due to the secondary damages
C) IT disabilities were confirmed, threats occurred and other events occurred which would require countermeasures by other critical infrastructure providers for its critical level

[4] Influences of malfunctions of other sectors
A) IT malfunctions occurred
B) IT disabilities were confirmed, threats occurred and other events occurred which would require countermeasures by other critical infrastructure providers for its critical level

Even for events not applied for any conditions above, it is desirable to consult with the critical infrastructure sector-specific ministries or the Cabinet Secretariat if it is effective to prevent IT malfunctions and avoid the spread of damages, or when it is uncertain whether the above conditions could apply, such as the cases that malfunctions of each critical infrastructure providers could make a ripple effect on IT malfunctions of other critical infrastructure providers, or they are at risk to be impacted.

(2) Contents for communication

Information confirmed should be announced as available except cases which require a communication means available in case of IT malfunctions or when information is required to ensure communication between liaisons. In this case, the contents of information may be partial or unconfirmed before revealing the entire information.

The common classification and category concerning IT malfunctions, which are required for communication from the critical infrastructure sector-specific ministries to the Cabinet Secretariat, are subject to “the action item” specifically defined. The “communications procedures” should be reviewed as necessary by taking consideration of the operability of each critical infrastructure provider.

(3) Mechanism of communication

Information should be transmitted from critical infrastructure providers to the Cabinet Secretariat through critical infrastructure sector-specific ministries.

[1] Critical infrastructure providers should contact the critical infrastructure sector-specific ministries according to the reporting system as shown in Appendix 5.

[2] The report received from critical infrastructure providers should be given from the liaison that is in charge of the sector in report of the critical infrastructure sector-specific ministry to the Cabinet Secretariat.

[3] The Cabinet Secretariat should properly identify and manage the report and handle it in an acceptable range of information sharing system specified by the information source.

(4) Ideas concerning handling of reported information

In terms of handling of information reported under the current reporting system, the Cabinet Secretariat and the critical infrastructure sector-specific ministries who received the information should handle the information according to the laws concerning disclosure of information owned by the administrative organizations in principle (the law, 1999, No. 42 "Administrative Information Disclosure Law", hereinafter) Article 5, No. 2 B (optional information) , unless otherwise specified under the laws and regulations or when it is accepted by critical infrastructure providers who is reporting). Such information, however, may be disclosed when it applies to the notes of the Administrative Information Disclosure Law Article 5, No.2.

4. Consolidating information and sharing in emergencies such as disasters and terrorist attacks

In case of emergency such as disasters and terrorist attacks, the Cabinet Secretariat and the related government agencies should consolidate and share the information according to "Initial action of the government for emergency" (determined by the Cabinet, November 21, 2003), regardless of the descriptions specified as 1 to 3 above.

## Appendix 1. Critical infrastructure and important system concerned

| Critical infrastructure sector | | IT malfunctions and examples of its influence | Target critical infrastructure providers, etc (note 1) | Examples of target critical important systems (note 2) |
|---|---|---|---|---|
| Information communication | | ・Suspension of telecommunication service<br>・Malfunctions of telecommunication services to affects its safety and constant supply etc.<br>・Suspension of broadcasting services | ・Major telecommunications carrier<br>・Major broadcasting companies | ・Network system<br>・Operation support system<br>・News and program production system<br>・Programming and operation system |
| Finance | Bank<br>Life insurance and Damage insurance<br>Securities company<br>Financial product exchange | ・Stoppage of deposit withdrawal, fund transfer such as crediting and loan process.<br>・Stoppage of the paying of insurance amount<br>・Stoppage of the buying and selling of valuable securities, etc | ・Bank cooperative banks, credit cooperative, agricultural cooperative, etc<br>・Life insurance, damage insurance, and securities companies, etc.<br>・Financial products exchange etc. | ・Accounting system<br>・The capital bond system<br>・International system<br>・External connection system<br>・Insurance business system<br>・Securities breakage system<br>・Exchange system etc.<br>(including the services using the open network) |
| Airlines | | ・Delay and cancellation of service<br>・Obstacles to hinder the safety service of aircraft etc. | ・Major airline transportation provider<br>・The Ministry of Land, Infrastructure and Transport(air traffic control and weather) | ・Operation system<br>・Reservation and boarding system<br>・Maintenance system<br>・Cargo system<br>・Air traffic control system<br>・Weather information system |
| Railway | | ・Delay and suspension of train operation<br>・Obstacle to hinder the safety and stable service of trains etc. | ・Main railway companies such as JR and major railway companies, etc. | ・Computer-assisted traffic control system<br>・Power management system<br>・Seat reservation system |
| Electric Power | | ・Suspension of electric power supply<br>・Obstacles to hinder the safety operation of power plant etc. | ・General electric power companies, The Japan Atomic Power Company Co. and J-Power Co. | ・Control system<br>・Operation monitoring system |
| Gas | | ・Suspension of gas supply<br>・Obstacles to hinder the safety operation of gas plant etc. | ・Major gas supplier | ・Plant control system<br>・Remote monitoring and control system |
| Government and Administrative service | | ・Obstacles to hinder the government and administrative services<br>・Leakage, tapping, and falsification of personal identifier information | ・Each government ministry and agency<br>・Local governments | ・Information system of each government ministry and agency and local governments (responses to e-government and e-municipality) |
| Medical services | | ・Obstacle to hinder diagnosis and treatment supports | ・Medical institution | ・Management system of diagnosis and treatment records (so-called e-carte and remote image diagnosis) |
| Water service | | ・Suspension of supply of water from the water service<br>・Supply of water in poor quality etc. | ・Water supply companies and city water supply provider (except small-sized companies ) | ・Monitoring system of water facilities and tap water.<br>・Control system etc. of water facilities |
| Logistics | | ・Delay and suspension of transportation<br>・Unable to track down the whereabouts of cargo | ・Major distribution companies | ・Collection and delivery management system<br>・Cargo tracking system<br>・Warehouse management system |

Note 1. Targeted critical inftastructures providers shown in this table are business entities engaged in critical inftastructures which should be intensively implemented with relevant measures. In the future, considering the degree of changing in the business environment and IT dependency, target business entities shall be reviewed..

Note 2. Details of target critical information systems shall be determined by critical infrastructure providers in consideration of examples of threats and dangers.

## Appendix 2. Critical infrastructure services and review level

| Critical infrastructure sector | | Critical infrastructure service (including the procedure) (note) | | Verification level | |
|---|---|---|---|---|---|
| | | Name | Explanation of services (including the procedure) (Related law) | Object and standard | Remarks |
| Information communication | | ・ Telecommunication services | ・ Mediate others communications through telecommunication systems, and provide other telecommunication equipment for the communication of others. (Telecommunications Business Act, Article 2) | ・ Malfunctions of the telecommunication systems should not lead suspension of the services or degradation of quality for 2 hours or more to 30,000 or more users. | ・It is subject to Regulations for Enforcement of the Telecommunications Business Act, Article 58. |
| | | ・Broadcasting | ・Transmission of radio communication to aim direct reception by the public (Broadcast Act, Article 2) | ・ Malfunctions of IT should not lead suspension of broadcasting services | |
| Finance | Bank | ・Deposit withdrawal<br>・Lending<br>・Foreign exchange | ・Deposits or acceptances of deposit for installment savings account, etc.(Banking Service Act Article 10 Section 1.1)<br>・Discount of lending or bill of the capital (Banking Service Act Article 10 Section 1.2)<br>・Exchange trading (Banking Service Act Article 10 Section 1.3) | ・Malfunctions of IT should not lead delay or suspension of refund of the deposits<br>・Malfunctions of IT should not lead delay or suspension of the lending accepted for loans<br>・Malfunctions of IT should not lead delay or suspension of exchange (bank transfer) | ・See "Supervision guidelines for major banks".<br>・Except the case when quick replacement with other systems and equipment should avoid practical impacts on the system (e.g. even though some ATM is disabled, other ATMs in the same branch or other branches in neighbor, or the machines at the windows are available). |
| | Life Insurance | ・Payment of premium<br>・Payment of insurance etc. | ・Acceptance of claim for insurance etc.<br>・Examination of insurance premium payment etc.<br>・Payment of premium etc. | ・Malfunctions of IT should not lead delay or suspension of payment of insurance etc. | ・"Supervision guidelines for insurance companies".<br>・Quick replacement with other systems and equipment should avoid practical impacts on the system. |
| | Damage insurance | ・Payment of premium etc. | ・Accident report received<br>・Investigation for damages<br>・Payment of premium etc. | ・Malfunctions of IT should not lead delay or suspension of the payment of insurance etc. | ・"Supervision guidelines for insurance companies".<br>・Quick replacement with other systems and equipment should avoid practical impacts on the system. |
| | Securities companies<br>Financial products exchange | ・Buying and selling of securities etc.<br>・ Mediation of buying/selling of securities etc., breakage and representation | ・ Buying and selling of securities, market derivatives transaction or foreign market derivatives transaction (Financial Products Trading Act, Article 2, Section 8.1)<br>・Mediation, breakage or representation of buying and selling, market derivatives transaction or foreign market derivatives transaction | ・Malfunctions of IT should not lead delay or suspension of clearance and payment of cancellation fee of the securities received for guarantee etc. etc. | ・See "Comprehensive Supervisor Guidelines for Financial Products Dealers.<br>・Except when no practical influence occurs by a quick replacement of other system and equipment (e.g. the buying and selling is available and the transaction is completed in time by starting the substitution system equivalent to the system in failure, in case of the selling and buying system during the operating hours. |

| Critical infrastructure sector | | Critical infrastructure service (including the procedure) (note) | | Verification level | |
|---|---|---|---|---|---|
| | | Name | Explanation of services (including the procedure) (Related law) | Object and standard | Remarks |
| | | ・ Breakage of liquidation such as securities etc.<br>・ Establishment of financial products market | (Financial Products Trading Act, Article 2, Section 8.2)<br>・Brokerage of liquidation of securities etc. (Financial Products Trading Act, Article 2, Section 8.5)<br>・Providing with market facilities for buying and selling or market derivatives transaction of securities and business according to establishment of other exchange financial products market (Financial Products Trading Act, Article 2, Section 14,16, Article 80 and 84) | ・Malfunctions of IT should not lead delay or suspension of the buying and selling or the market derivatives transaction etc. of securities. | ・See the Cabinet Office Ordinance Article 112 Section 7 concerning the financial products exchange |
| Airlines | | ・Passenger and cargo air transportation services<br>・ Air traffic control service<br>・Weather forecast distribution<br>・Reservation, ticketing, boarding/cargo procedures<br>・Operation and maintenance<br>・Flight planning | ・Business to transport passengers and cargo with fee using aircraft as demanded by others (Civil Aeronautics Act Article 2)<br>・Securing of proper, safe, use, smooth air traffic of airspace (Civil Aeronautics Act Article 95,2)<br>・Distribution of weather forecast or warning to comply with the use of aircrafts (Meteorological Service Act Article 14)<br>・ Reservation of air passengers and cargo<br>・Ticketing and collection of fare<br>・Air passenger's check-in, boarding, and baggage loading<br>・ Inspection and maintenance of aircraft<br>・Flight planning and submission to Japan Civil Aviation Bureau | ・ Malfunctions of IT should not lead cancellation of the regular flights which could affect the transportation of passengers and freight. | |
| Railway | | ・Passenger transportation service<br>・Ticketing and entrance/exit processes | ・Business to transport passengers and freight by railway as demanded by others (Railway Business Act, Article 2)<br>・Reservation of seats, sales of tickets and confirmation of tickets at the entrance/exit of the station | ・ Malfunctions of IT should not lead suspension of train operation which could affect transportation of passengers | |

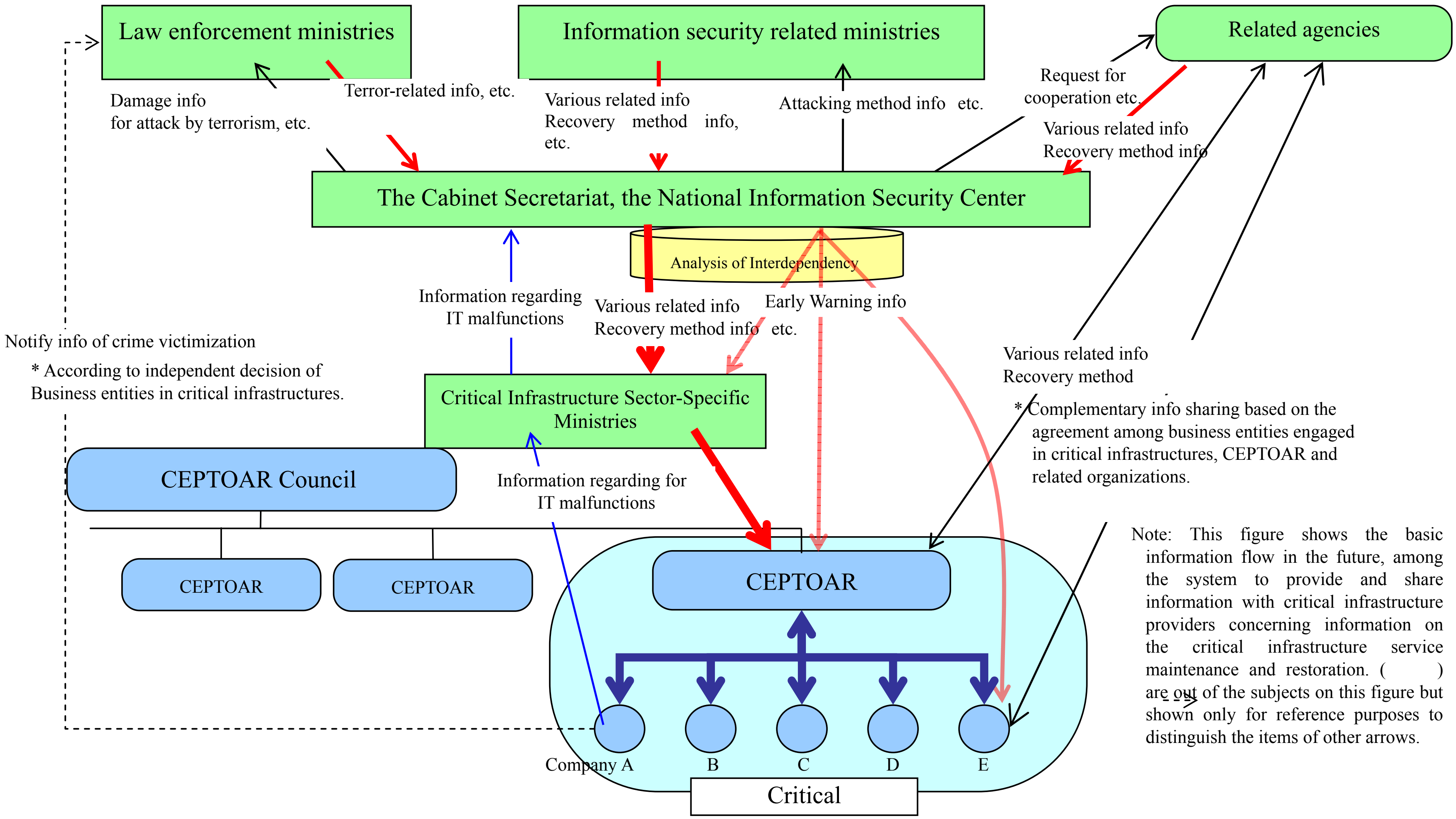
| Critical infrastructure sector | Critical infrastructure service (including the procedure) (note) | | Verification level | |
|---|---|---|---|---|
| | Name | Explanation of services (including the procedure) (Related law) | Object and standard | Remarks |
| Electrical Power | ・Public electric power supply industry | ・The business to supply electricity as demanded by public (Electricity Business Act, Article 2 and 18) | ・Malfunctions of IT should not lead power supply failure for 10 minutes or more, over 100,000 kw | ・It is subject to Electricity related report regulation Article 3. |
| Gas | ・General gas business | ・The business to supply gas through conduits as demanded by public (Gas Business Act Article 2) | ・Malfunctions of IT should not lead failure of gas supply for 30 or more households | ・It is subject to Gas Business Act Ordinance Article 112. |
| Government and Administrative services | ・ Administrative service of municipal governments | ・Those which processed under the laws and ordinances concerning clerical and other tasks in local governments (the Local Government Act Article 2, Section 2) | ・Malfunction of IT should not lead incur any violation against protection of citizen rights and benefits of residents<br>・Restore the system within a time to ensure the safety and security of the residents | Example: For various communications services on the websites<br>・No leakage of personal information.<br>・The system should be able to be restored as normal within 24 hours in case of suspension of services or generation of incorrect information. |
| Medical services | ・Medical treatment | ・Acts of medical examination and treatment, etc.<br>・Record and filing of diagnosis record and various diagnosis and treatment records, etc. | ・Malfunction of IT should not lead negative impacts should occur on filing diagnostic records. | ・Acts of medical examination and treatment may continue regardless of the dependency of IT<br>・Filing is subject to the Medical Practitioners Act Article 24 , Section 2, no immediate action required. |
| Water service | ・Supply of water with water services | ・The business to provide drinking water through piping and other work pieces as demanded by public. (the Water Service Act, Article 3, Section 15) | ・Malfunction of IT should not lead obstacles occur to water supply, including suspension or reduction of water supply, abnormal water quality or significant system failure. | ・Significant system malfunctions is assumed to include troubles for the control system with a large influence on water supply due to system stop (e.g. monitoring and control system at the filtration plants, operating system of the pumping station, and system for the water transportation, etc.) |
| Logistics | ・Logistics | ・Transportation and storage of freight | ・ Malfunction of IT should not lead suspension of operation or loss of freight. | |

Note: The services not using IT are not included in the goals of this Action Plan.

Appendix 3. Example of threats that causes IT malfunctions

| Pattern of threat | Example of threats | |
|---|---|---|
| | Threats which requires countermeasures for the entire society | Threat that individual critical infrastructure providers take measures |
| [1] Intentional factors including cyber Attack | Denial of service attacks that happen frequently in a cross-sectoral manner, intrusion, and fraud of important information, etc. | Intrusion, data falsification, destruction, unauthorized command execution, virus attack, denial of service attack (DoS:Denial of Service), information leakage, and fraud of important information and internal fraud etc. |
| [2]Non-intentional factors | Social environment change and systemic revision (example: The Year 2000 issue, lack of effects of encryption and shift to IPv6) which could lead a large scale operation and setting mistakes, bugs on programs and incomplete maintenance | Operation and setting mistakes, bugs on programs and incomplete maintenance, lack of internal and external auditing, lack of external vendor management, lack of management capabilities, equipment failure etc. |
| [3] Disaster and disease | Destruction of power supply equipment, communication facilities, water systems and computer facilities due to large scale earthquake, flooding (e.g. Metropolitan area earthquake and flood of Arakawa River), etc. | Destruction of power supply equipment, communication facilities, water systems and computer facilities due to disasters of earthquake, flood, stroke of lightning, fire, etc. |
| [4] Propagate from troubles in another sector | A large scale suspension of operation of power supply, communication lines, water service supplies (those which confirmed as a result of the interdependence analysis) etc. | A large scale suspension of operation of power supply, communication lines, water service supplies (those which confirmed as a result of the interdependence analysis) etc. |

## Appendix 4. Information sharing


Law enforcement ministries
Information security related ministries
Related agencies
Damage info
for attack by terrorism, etc.
Terror-related info, etc.
Various related info
Recovery method info, etc.
Attacking method info etc.
Request for cooperation etc.
Various related info
Recovery method info
The Cabinet Secretariat, the National Information Security Center
Analysis of Interdependency
Information regarding IT malfunctions
Various related info
Recovery method info
Early Warning info
etc.
Various related info
Recovery method
Notify info of crime victimization
Critical Infrastructure Sector-Specific Ministries
CEPTOAR Council
Information regarding for IT malfunctions
CEPTOAR
CEPTOAR
CEPTOAR
Company A
B
C
D
E
Critical

* According to independent decision of Business entities in critical infrastructures.

* Complementary info sharing based on the agreement among business entities engaged in critical infrastructures, CEPTOAR and related organizations.

Note: This figure shows the basic information flow in the future, among the system to provide and share information with critical infrastructure providers concerning information on the critical infrastructure service maintenance and restoration. ( - - > ) are out of the subjects on this figure but shown only for reference purposes to distinguish the items of other arrows.

## Appendix 5. Reporting system in case of IT malfunctions

| Critical infrastructure sector | | Existing reporting system | Reporting system in case of IT malfunctions | System of discussion concerning security countermeasures in each sector |
|---|---|---|---|---|
| Information communication | | (1) From Critical infrastructure providers to government<br>・Report of suspension of business etc. to the Minister for Public Management, Home Affairs, Posts and Telecommunications based on Telecommunications Business Act<br>・Report of damage situation etc. of telecommunication equipment in case of disaster emergency response based on Disaster Measures Basic Act<br>・Contacts of broadcasting discontinuance accidents and important radio communication obstruction, etc. to the Ministry of Internal Affairs, Posts and Telecommunications<br>(2) From Government to critical infrastructure provider etc. and between critical infrastructure providers<br>・Communication and information sharing of emergency such as computer virus, between the Ministry of Internal Affairs, Posts and Telecommunications industry. | (1) From Critical infrastructure providers to government<br>・An existing reporting system is used for communication.<br>(2) From Government to critical infrastructure providers<br>・The reporting system of T-CEPTOAR is used for communication.<br>・The reporting system of the system of the information sharing in broadcasting is used for communication.<br>・An existing reporting system is used for communication. | ・The system of sharing information on computer virus is used for communication. |
| Finance | Bank<br>Life insurance<br>Damage insurance<br>Securities<br>Financial products exchange | (1) From Critical infrastructure providers to government<br>・Reports of service delay and suspension, etc. to the Prime Minister (the Financial Services Agency) based on the business law<br>(2) From Government to critical infrastructure provider etc. and between critical infrastructure providers. | (1) From Critical infrastructure providers to government<br>・An existing reporting system is used for communication.<br>(2) From Government to critical infrastructure provider etc<br>・The reporting system of the bank CEPTOAR etc. is used for communication.<br>・The reporting system of the bond CEPTOAR is used for communication.<br>・The reporting system of the life insurance CEPTOAR is used for communication.<br>・The reporting system of nonlife the insurance CEPTOAR are used for communication.<br>・Communication through other business groups | ・Conducted through business groups such as Japanese Bankers Association and Finance Information System Center (FISC). |

| Critical infrastructure sector | Existing reporting system | Reporting system in case of IT malfunctions | System of discussion concerning security countermeasures in each sector |
|---|---|---|---|
| Aviation | (1) From Critical infrastructure providers to government<br>･Report to the Minister of Land, Infrastructure and Transport concerning aircraft accidents based on the aviation law<br>(2) From Government to critical infrastructure provider etc. and between critical infrastructure providers.<br>･Contacts concerning IT malfunctions<br>･Information on the troubles of the system of the Airlines security is shared by related organizations (per airport) | (1) From Critical infrastructure providers to government<br>･An existing system of accidents report is used in case of accidents<br>･ IT malfunctions not incurring accidents are reported through IT malfunctions communication system<br>･It executes it by the reporting system of the IT malfunctions for the IT malfunctions that doesn't arrive at the accident.<br>(2) From Government to critical infrastructure providers<br>･The reporting system of the CEPTOAR in the Airlines sector is used for communication.<br>･Direct communication to critical infrastructure providers through the liaison | |
| Railway | (1) From Critical infrastructure providers to government, government →critical infrastructure providers<br>･Report to the Minister of Land, Infrastructure and Transport concerning railway operation accidents based on the reporting regulation for the railway accidents<br>･Reporting system required concerning IT malfunctions<br>(2) Between critical infrastructure providers<br>･Not particular | (1) From Critical infrastructure providers to government, government →critical infrastructure providers<br>･The existing accident reporting system is used for communication in case of accidents<br>･The reporting system of the railway CEPTOAR is used for communication. | |
| Electric power | (1) From Critical infrastructure providers to government<br>･Contact to the Minister of Economy, Trade and Industry concerning supply failure accidents based on the reporting rule of electricity<br>(2) From Government to critical infrastructure provider etc. and between critical infrastructure providers<br>･Contacts concerning IT malfunctions | (1) From Critical infrastructure providers to government<br>･ An existing reporting system is used for communication.<br>(2) From Government to critical infrastructure providers<br>･The reporting system for information sharing and analysis concerning IT malfunctions with electrical power is used for communication.<br>･Direct communication to critical infrastructure providers through the liaison | ･Conducted through business groups |

| Critical infrastructure sector | Existing reporting system | Reporting system in case of IT malfunctions | System of discussion concerning security countermeasures in each sector |
|---|---|---|---|
| Gas | (1) From Critical infrastructure providers to government<br>･Report to the Minister of Economy, Trade and Industry concerning a certain gas supply failure based on the gas business law enforcement rule.<br>(2) From Government to critical infrastructure provider etc. and between critical infrastructure providers<br>･Reporting in the industry based on Gas Association "Rescue Measures Guidelines" in case of gas supply failure due to disasters | (1) From Critical infrastructure providers to government<br>･ An existing reporting system is used for communication<br>(2) From Government to critical infrastructure providers<br>･The reporting system of the GAS CEPTOAR is used for communication.<br>･Communication through business groups. | ･Conducted through councils etc. in the industry |
| Government and administrative services | (1) Each government agency → the Cabinet Secretariat<br>･Report based on "Report concerning information system of government agency in emergency etc."<br>(2) The Cabinet Secretariat → each government agency<br>･Information provision for emergency based on “Emergency communication concerning the information system of government agencies”<br>(3) Municipal governments → government<br>･Information provision based on “Emergency communication concerning the information system of municipal governments "<br>(4) Government → municipal governments<br>･Information provision based on “Emergency communication concerning the information system of municipal governments" | (1) Each government agency → the Cabinet Secretariat, The Cabinet Secretariat → each government agency<br>(1) Each government agency → the Cabinet Secretariat and the Cabinet Secretariat → each government agency<br>･The reporting system in the government divisions for communication<br>(2) Municipal governments → government, government → municipal governments<br>･ The reporting system of the municipality CEPTOAR is used for communication.<br>･ An existing reporting system is used for communication | ･Conducted through internal communication system in the governments |
| Medical | (1) Critical infrastructure providers → government etc.<br>(2) Government etc. → critical infrastructure provider etc. | (1) Critical infrastructure providers → government etc.<br>(2) Government etc. → critical infrastructure providers<br>･The reporting system of the medical services CEPTOAR is used for communication | |
| Water service | (1) Critical infrastructure providers → government etc.<br>(2) Government etc. → critical infrastructure provider etc. | (1) Critical infrastructure providers → government etc.<br>(2) Government etc. → critical infrastructure providers<br>･ The reporting system of the water service CEPTOAR is used for communication | |
| Logistics | (1) Critical infrastructure providers → government etc.<br>･Report to the Minister of Land, Infrastructure and Transport based on each business law concerning such as accidents<br>(2) Government → critical infrastructure providers<br>･Designated public organizations of transport specified under the Disaster Countermeasures Act of the Cabinet Office | (1) → Critical infrastructure providers → government<br>(2) Government → critical infrastructure provider etc.<br>･Implemented through the communication system of the logistics related CEPTOAR | ･Implemented through the provider groups. |