December 13, 2005
Decision by the Information Security Policy Council

Action Plan on Information Security Measures for Critical Infrastructures

1 Purpose and Scope

The purpose of the Action Plan on Information Security Measures for Critical Infrastructures (hereinafter referred to as the "Action Plan") is as follows. Based on "Basic Stance on Information Security Measures for Critical Infrastructures (decision by Information Security Policy Council established under the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (hereinafter referred to as the IT Strategic Headquarters)", protect critical infrastructures from IT functional failures (hereinafter referred to as the "IT-malfunction") out of failures occurring in each business sector of critical infrastructures, which may have a significant impact on people's social lives and economic activities. The Action Plan shall also define independent measures which should be formulated by each business entity engaged in critical infrastructures [1] to enhance business continuity. To ensure continuing service maintenance and rapid resumption in the case of IT-malfunction occurrence, business entities engaged in critical infrastructures should flesh out the details of the measures, with making measures which should be taken by the government (especially the Cabinet Secretariat) and each critical infrastructure sector consistent with current acts and guidelines of disaster prevention plans. This would ensure information security measures of critical infrastructures under the close partnership with public and private sectors.

Each sector should actively work not only on improvement current technology and establishment of cooperation frameworks, but also on overall development of acts and systems, management and personnel involved in this activity.

2 Definition and Target of Critical Infrastructures

(1) Definition and Target Sectors of Critical Infrastructures

"Critical Infrastructures" in this Action Plan is defined as follows. "Critical

[1] "Business entities engaged in critical infrastructures" shall mean any entities specified in Attachment 1 and those composed of such entities out of business entities engaged in "Telecommunications", "Finance", "Civil aviation", "Railways", "Electricity", "Gas", "Governmental Administrative services (including local governments), "Medical services", "Water works" and "Logistics".(same as follows)

infrastructures are formed by business entities providing highly irreplaceable services and are essential for people's social lives and economic activities. If an infrastructure's function is suspended, reduced or unavailable, people's social lives and economic activities will be greatly disrupted."

Current target includes the following 10 sectors. "Telecommunications", "Finance", "Civil aviation", "Railways", "Electricity", "Gas", "Governmental /Administrative services (including local governments)", "Medical services", "Water works" and "Logistics". At each sector, business entities engaged in critical infrastructures, who are supposed to promote measures based on this Action Plan, should follow the statement in Attachment 1 in consideration of the influence on people's social lives and economic activities.

Target sectors and target business entities of "Critical Infrastructures" will be continuously reviewed to correspond to promotion and expansion of the use of IT and environmental changes of each service.

(2) Examples of threats to IT-malfunction and critical information systems in each sector

Threats to cause IT-malfunction concerned in this Action Plan include not only intentional factors such as electrical attacks using telecommunication networks and information systems (hereinafter referred to as the "cyber attack") but also unintentional factors including system failures, human errors or structural threats caused by changes of methods to apply information technology such as outsourcing, and a wide range of other factors including natural disasters such as earthquake and tsunamis, which will be explained as follows.

A. Examples of Threats to IT-malfunction

1) Threats of cyber attack causing IT-malfunction

Hacking, data falsification/destruction, rough command execution, virus attack, Denial of Service (DoS) attack, Information leakage, exploitation of critical information, etc.

2) Threats of unintentional factors causing IT-malfunction

Operational/Setting errors, program defects (bug), poor maintenance, poor internal/external audit function, outsourcing, management failure, internal fraud, etc.

3) Threats of natural disasters to IT-malfunction

IT functional failures of business entities engaged in critical infrastructures caused by electric power disruption, communication interruption and damage of computer facilities occurring due to disasters such as earthquakes, flood damage and lightning

B. Examples of Critical Information Systems in Each Sector

"Essential Information System Forming Key Components of Critical Infrastructures" (hereinafter referred to as the "Critical Information System") established under the Action Plan will be defined by individual critical infrastructures sector, assessing the degree of its influence on people's social lives and economic activities.

Details about the target Critical Information System will be defined by each business entity engaged in critical infrastructures with reference to the examples of Critical Information Systems in each sector listed in Attachment 1.

3 "Security Standards, Guidelines, etc." concerning Assurance of Information Security of Critical Infrastructures

(1) Positioning

Due to the rapid spread of IT use and growing interdependence in critical infrastructures the foundation of people's social lives and economic activities, cross-sectoral information security measures towards IT-malfunction need to be strengthened. To achieve a prompt solution to this issue, proactive measures towards IT-malfunction should be considered at peace time. At each critical infrastructure sector, appropriate information security measures should be taken promptly, considering the characteristics of relevant business sectors and business entities.

However, due to the opaque nature of the measures for information security, it is difficult to judge if those measures are enough to protect the business entities. The business entities engaged in critical infrastructures should verify their measures by themselves and improve those to protect the critical infrastructures from IT-malfunction which may have a significant impact on people's social lives and economic activities.

Hence, based on "A Principle for Formulating 'Safety Standards, Guidelines, etc.' concerning Assurance of Information Security of Critical Infrastructures" (hereinafter referred to as the "Guidelines" formulated by The National Information Security Center (NISC), each business sector shall make an effort to specify the standards for necessary or desired information security measures in the "Safety Standards, Guidelines, etc." by September 2006. Additionally, the Guidelines shall be reviewed annually or at optimal timings as required and "Safety Standards, Guidelines, etc." will be on an as-needs basis corresponding to the environmental changes surrounding information security.

(2) Formulation and Review of “Safety Standards, Guidelines, etc”

Each critical infrastructures sector shall formulate or review “Safety Standards, Guidelines, etc.” as follows.

A. Determine sectors and establish frameworks

Sectors required to formulate or review the “Safety Standards, Guidelines, etc.” shall be determined jointly by the presiding Ministries and Agencies of the relevant critical infrastructures, business entities engaged in critical infrastructures.

If there is more than one sector for the formulation, those shall work jointly to establish the frameworks to formulate or review a single or hierarchically structured “Safety Standards, Guidelines, etc.”

B. Determine target scope

Preliminary determine information assets[2] to be protected and target scope.

C. Implement risk analysis

Based on the determined target scope and assumed threats, implement risk analysis in advance.

D. Indicate target items and execution levels

Respective business entity engaged in critical infrastructures must take an objective view to indicate what measure should be taken up to what level within the “Safety Standards, Guidelines, etc.” On this occasion, each business entity engaged in critical infrastructures should consider the characteristics of its own business sector, and appropriately verify whether the standards of measures adopted by respective business entities engaged in critical infrastructures meet “Safety Standards, Guidelines, etc.”

E. Compliance to current acts

Check compliance to current laws and acts in advance to ensure consistency.

F. Consideration to interdependency and mutual support frameworks

Establish measures in consideration of interdependency and mutual support frameworks among critical infrastructures sectors and collaboration with government district offices, local governments and local organizations related to information security which are located where the business entities engaged in critical infrastructures exist.

[2] Information system and accumulated information in it

4 Strengthening the Information Sharing Frameworks

The business entities engaged in critical infrastructures hold the primary responsibility to maintain and recover their services, however, to make them work more smoothly, support should be provided by the public and private sectors.

Especially, regarding IT-malfunction, the following 3 actions shall be critical: 1. preemptive prevention of IT-malfunctions, 2. prevention of expansion of suffering and rapid resumption, and 3. prevention of recurrence through analysis/verification of causes of IT-malfunctions. The government and the like should provide necessary information if requested, and ensure the information sharing frameworks within those business entities engaged in critical infrastructures and interdependent critical infrastructures sectors.

Information for IT-malfunction includes the followings.

1) Preemptive prevention of IT-malfunctions: Information concerning threats causing a failure (including proactive measures)
2) Prevention of expansion of suffering and rapid resumption: Information required to estimate the influence range of the failure and establish a method for rapid resumption
3) Prevention of recurrence through analysis/verification of causes of IT-malfunctions: Information cooperatively collected that is helpful for ex-post analysis and the results obtained in the analysis and evaluation.

From the viewpoint of Preemptive prevention of IT-malfunctions, it is important that respective business entities engaged in critical infrastructures should provide as much information as possible to other providers at the occurrence of failure, if the failure has potential to affect other IT-malfunction.

The system of information sharing, liaison, and coordination between the public and private sectors (see Attachment 2) should be simulated with activities such as Cross-Sectoral Exercise to verify its validity. This shall enhance emergency response capability and allow you to review the system if necessary

To realize and enhance this information sharing frameworks (see Attachment 3-1), it is required to make the utmost use of features that a respective sector currently holds, clarify roles of each sector, and refrain from placing excessive burden on a specific sector.

(1) Information provision and liaisons between public and private sectors

A. Provide information to the business entities engaged in critical infrastructures etc.

1) Cooperation framework to provide information

The Cabinet Secretariat shall cooperatively work with relevant agencies and Related Organizations to collect and provide information from the presiding Ministries and Agencies of the relevant critical infrastructures to the business entities engaged in critical infrastructures.

(a) Collect a wide range of information provided from central government agencies concerning information security (National Police Agency, Japan Defense Agency, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry), Central government agencies dealing with individual cases (National Police Agency, Japan Defense Agency, Fire and Disaster Management Agency, Japan Coast Guard, etc.) and Related Organizations (Cyber Force Center of National Police Agency, NICT[3] IPA[4] ,Telecom-ISAC Japan[5] JPCERT/CC[6] ,etc.)[7]

(b) Provide damage information on the attack, in the case of being caused by terrorism, to the central government agencies dealing with individual cases, and information on attack methods to the central government agencies concerning information security.

(c) To collect and analyze information, request support to the Related Organizations if necessary.

(d) Information regarding disasters should be collected under the current information sharing frameworks among Cabinet Secretariat, Cabinet Office and other relevant agencies.

2) Enhance quality of information (Analyzed information, effect degree, etc)

Quality of information to be provided will be enhanced in consideration of the following points:

(a) Enhance accuracy of information by confirming one by one

(b) Judge importance and priority based on the above accuracy

(c) Effect estimation based on analysis of interdependence

(d) Regarding IT-malfunction caused by service interruption or degradation of other critical infrastructures sectors, perceive the statistical state of occurrence by its content and scale

[3] National Institute of Information and Communications Technology

[4] Information Technology Promotion Agency, Japan

[5] Established as "Telecom-ISAC Japan in 2002". Merged with "Nippon Information Communication Association" in 2005.

[6] Japan Computer Emergency Response Team Coordination Center

[7] Quoted from "First Proposal" (Information Security Committee on Basic Problems 3.1.3. (1)③16 November, 2004, see Footer 4) and " Review of the Role and Functions of the Government in terms of Measures to Address Information Security Issues"(decision by the IT Strategic Headquarters on 7 December, 2004; see Footer 5)," Under this plan, "Related Organizations" shall mean " Cyber Force Center of National Police Agency", NICT、IPA、Telecom-ISAC Japan、JPCERT/CC and the like.

3) Framework for providing information

Procedure for providing information from the Cabinet Secretariat to the business entities engaged in critical infrastructures via the presiding Ministries and Agencies of the relevant critical infrastructures shall be as follows:

(a) Information shall be provided to the presiding Ministries and Agencies of the relevant critical infrastructures through liaison (concurrently served by the Cabinet Secretariat) selected from each ministry and agency. Under the critical information such as early warning information, which requires prompt action, the Cabinet Secretariat shall directly inform CEPTOAR (to be described later) or individual business entities engaged in critical infrastructures as well as the presiding Ministries and Agencies of the relevant critical infrastructures.

(b) For the purpose of easy use of relevant information for the viewers, the identification method shall be improved so that they can find the category and covered range of the information by its importance, type, characteristics, etc.

(c) Liaison will arrange the information sharing frameworks for responsible sectors through CEPTOAR (to be described later).

(d) Since early warning information and the like requires special care to be handled, it is subject to the agreement of handling the information between the information provider and the Cabinet Secretariat.

4) Scope and contents of provided information

Information will be provided in order to help each business entity engaged in critical infrastructures take measures such as calling attention. Range and items covered are as follows:

(a) Range of providing information should include business entities engaged in critical infrastructures which are directly related to such information (if it is sector-specific systems, provided to the relevant sectors, if related to other sectors, provided to all the related sectors)

(b) Regarding information provision by business entities engaged in critical infrastructures, the government should take appropriate method to protect them from any losses. Contents of the information shall be limited to the items with reasonable relevance to achieve the goal of the provision.

B. Liaison from business entities engaged in critical infrastructures and the like.

1) IT-malfunction to be reported (See Attachment 3-2~4)

IT-malfunction to be reported is shown as follows. These include incidents, failures, delays of operation, etc obliged to be reported by statutes and those the business entities engaged in critical infrastructures consider to be especially critical.

(a)A case of IT-malfunction caused by cyber attack

1) When critical failure occurs in critical information systems

2) When a cyber attack is detected in critical information systems or notice of an attack is given

3) When damage is detected by cyber attack against critical information systems

(b) A case of IT-malfunction caused by unintentional factors

When critical IT-malfunction occurs in important systems

(c) A case of IT-malfunction caused by disasters

1) When critical IT-malfunction occurs in important systems

2) When IT-malfunction may occur in critical information systems due to a secondary disaster

Even if the failure does not fit any of above cases, it is preferable to consult with the presiding Ministries and Agencies of the relevant critical infrastructures or the Cabinet Secretariat if the IT-malfunction is deemed to be forestalled or prevented from further expansion (e.g. IT-malfunction which may cause further failures to other providers).

2) Information to be reported

Available contact procedures and persons must be reported to ensure communication in the event of IT-malfunction, and information known at that time shall be reported as acquired as occasion demands. Information can be accepted even if fragmentary and uncertain, and not enough to clarify the full scope.

The following shall be reported as it becomes available as occasion demands.

(a) Target Systems

Hardware, Software (Name, version, application status of patch process of the system etc.)

(b) Status of responses to the failure

1) Outline of measures (Stop and restore the system, improve security systems)
2) Reported offices (CEPTOAR (to be described later), related organizations and the central government agencies dealing with individual cases)

(c) Potentiality for affecting other business entities engaged in critical infrastructures

（d）Others

Considering the operability of each business entity engaged in critical infrastructures the Cabinet Secretariat Respective shall separately define common categories regarding IT-malfunction such as settings of each category, which will then be required to report above mentioned information.

3) How to deal with reported information

Regarding the information reported under this liaison and coordination system, except for the condition under the specific acts or a consent of the infrastructure service provider, the Cabinet Secretariat and presiding Ministries and Agencies of the relevant critical infrastructures which receive information shall handle the information as that defined by Article 5 No. 2 (b)(voluntary provided information) of Law Concerning Access to Information Held by Administrative Organs (No. 42 Act of 1999, hereinafter referred to as the “Disclosure law”), However, if the information is applied to the proviso of Information Disclosure Act, Article 5 No.2, it may be disclosed.

However, to promote information security measures for other business entities engaged in critical infrastructures, the Cabinet Secretariat shall make the reported information processed so that the provider that has reported the information will not be specified in the following cases.

(a) When a security hole or program bug, which may cause the same problem at other business entities engaged in critical infrastructures are detected

(b) When critical information systems of business entities engaged in critical infrastructures are deemed to be subject to risk, such as occurrence or notice of cyber attack and warning of disasters

C. Information providing and reporting procedures

The Cabinet Secretariat shall establish a framework for handling confidential information in order to provide and report above information.

Reporting procedure in the event of IT-malfunction occurrence shall be preliminarily clarified between business entities engaged in critical infrastructures and the presiding Ministries and Agencies of the relevant critical infrastructures, and also inside the government. More than two means of reporting, such as telephone, FAX and email, should be indicated.

Access to confidential information via internet (such as email), necessity of introducing encryption and the like shall be evaluated based on risk analysis and cost-effectiveness.

(2) Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR)

Information provided by the government for preemptive prevention of IT-malfunctions, prevention of expansion of suffering, rapid resumption, and prevention of recurrence will be appropriately made available to business entities engaged in critical infrastructures and will be shared among them. This will eventually contribute to upgrading of the capacity to maintain and reconstruct services of each business entity engaged in critical infrastructures. In order to serve this purpose, the government will promote the development of Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR) within each critical infrastructure sector. Among the ten sectors defined in this Action Plan, some may include far different business categories within one sector. In this case, those sectors can include multiple CEPTOAR by group of critical infrastructures service providers with many in common.

A. Function/Role

1) Contact section for information provided by the government

When receiving information from the Cabinet Secretariat via presiding Ministries and Agencies of the relevant critical infrastructures, CEPTOAR shall promptly provide the information to its member business entities engaged in critical infrastructures

2) Sharing information with Related Organizations

Information implementing those defined above 1), such as detailed information in accordance with IT usage of each critical infrastructure sector, shall be directly provided under the agreement between Related Organizations and CEPTOARs in other sectors and the like, if such agreement exists.

B. Requirements for CEPTOAR

CEPTOAR must meet the following feature requirements.

1) CEPTOAR shall have established rules among its members, based on the mutual

agreement on the handling of information provided by the Cabinet Secretariat, confidentiality and information provision to outsiders.

2) CEPTOAR shall have an established Point of Contact (POC) to communicate with its members and outsiders in the event of emergency.

In the future, it is desirable that a coordinator who collects information and judges situations should be located within the sector.

Considering characteristics of each sector, it would be possible to add further requirements by forming efficient and effective systems utilizing the current information sharing system for IT-malfunction.

C. CEPTOAR Establishment Measure

The optimal measure should be applied to develop CEPTOAR through the consultations between the presiding Ministries and Agencies of the relevant critical infrastructures and the business entities. This shall include utilizing functions of current business entities and supporting for their system establishment, according to characteristics and situations of each critical infrastructure sector.

D. Goal of Establishment

Consultations between the presiding Ministries and Agencies of the relevant critical infrastructures and the business entities shall be started as soon as possible to complete the establishment of CEPTOAR for each critical infrastructure sector by the end of FY 2006. Regarding newly added sectors, mutual agreement between presiding Ministries and Agencies of the relevant critical infrastructures and the business entities should be made by the end of FY 2006 (To be established in FY 2007).

E. Future Movement

Under this Action Plan, information sharing should be encouraged within a sector or among multiple sectors, based on mutual understanding and agreement between concerned entities, regarding enhancement of information security measures towards critical infrastructures in Japan. On a long-term basis, to facilitate, ensure and secure this information sharing, legal system including information disclosure and confidentiality should be consolidated.

(3) CEPTOAR-Council (tentative)

A. Establishing a Cross-Sectoral Information Sharing Environment

To enhance information security measures for critical infrastructures throughout the whole country, business entities engaged in critical infrastructures should encourage cross-sectoral information sharing with other providers to utilize a wide range of knowledge for their maintenance and recovery. For this reason, "CEPTOAR-Council" (tentative) shall be established as a council for cross-sectoral information sharing between CEPTOAR

B. Formation and Functions of "CEPTOAR Council" (tentative)

"CEPTOAR Council" (tentative) is a council formed by representatives from each CEPTOAR and aims to share common information among several sectors and cross-sectoral best practices out of information regarding maintenance and recovery of services provided by each critical infrastructure sector.

C. Procedure for Establishment

Establish a council formed by representatives from CEPTOAR with meetings held in FY 2006 with the cooperation of the Cabinet Secretariat.

5. Analysis of Interdependence

Ensuring of information security for critical infrastructures, causal analysis of IT-malfunction, and recovery from it has been traditionally dealt with each sector. However, expansion of IT usage increases interdependency among critical infrastructures sectors.

With this increasing interdependency, cross-sectoral understanding and analysis shall become essential to improve information security measures for critical infrastructures throughout the whole country.

Hence, Analysis of Interdependence to investigate how IT-malfunction affects from one sector to other sectors as well as what threats may occur in each sector.

Result of this Analysis of Interdependence shall be utilized to improve information security for critical infrastructures and bring about the following effects.

1) Providing basic materials required for establishing a more effective Business Continuity Plan (BCP)
2) Provide basic materials to determine order of priority for recovery in the event of large-scale disasters
3) Establish foundation to encourage cooperation among critical infrastructures sectors to prevent expansion of suffering caused by IT-malfunction

(1) Purpose of Analysis of Interdependence

To ensure information security for critical infrastructures, not only considering respective sectors, but also evaluating understanding and resiliency[8] of interdependency among sectors shall be required. Therefore, Analysis of Interdependence shall be required for managing a diffusion of incident and failure due to the prominence of potential risk-chain (linear and nonlinear).

With cooperation from business entities engaged in critical infrastructures and presiding Ministries and Agencies of the relevant critical infrastructures, the Cabinet Secretariat shall conduct the Analysis of Interdependence across critical infrastructures sectors based on investigation and evaluation of current methods for the Analysis of Interdependence and consideration of modeling a dependent structure.

Results from this analysis shall be reflected to establishment and review of "Safety Standards, Guidelines, etc." for critical infrastructures, decision making in the event of establishing a Business Continuity Plan, and policies and inspections of presiding Ministries and Agencies of the relevant critical infrastructures.

(2) How to Conduct Analysis of Interdependence

To conduct Analysis of Interdependence and ensure information security for critical infrastructures, basic design should be made by the following procedures.

A. Start the trial run as soon as possible to visualize and understand interdependency and its vulnerability among critical infrastructures sectors. (Awareness)

B. Modeling dependent structure and introducing systems such as "CEPTOAR-Council" (tentative), establish the system to detect vulnerability and forestall potential failures. (Prevention)

C. Promote as continuing efforts towards protection system for critical infrastructures (corresponding to internal and external interdependent factors). (Protection)

D. Expand functions to make the system available for decision-making in the event of occurrence of an incident or failure. (Response)

E. Provide information such as interdependent factors and degree of influence, which

[8] Fault tolerance and recovery feature

should be considered when simulating redesign of business operation and system in the event of recovery. (Recovery)

F. Through the Cross-Sectoral Exercises, evaluate the analysis of interdependence. (Validation)

(3) Obtaining required information

To obtain realistic results from the analysis of interdependence, more realistic conditions and the like shall be essential to be added.

The following two methods shall be considered to obtain such information. One is to be provided by each business entity engaged in critical infrastructures and another is that the Cabinet Secretariat and presiding Ministries and Agencies of the relevant critical infrastructures shall obtain information from domestic and overseas examples, documentation research, advice from domestic and overseas researchers, and overseas governmental agencies.

(4) Commencing Time and Executing Timing

Run the trial within FY 2006, then conduct when major update or change is made to core systems or business processes of any business entities engaged in critical infrastructures

6. Cross-Sectoral Exercise

Based on a model of a specifically envisioned threat scenario, a theme will be picked every year and the Cross-Sectoral Exercise will be performed under cooperation among presiding ministries of each critical infrastructure, each business entity engaged in critical infrastructures and CEPTOAR in each critical infrastructure sector, etc.

In FY 2006, under the following operation procedures and systems, "the Exercise for research" and "the tabletop exercise[9]" will be performed and CEPTOAR will be started. Then "the functional exercise[10]" will be gradually performed in FY 2007. Through these exercises, besides evaluating functions, consider problems of current legal systems and obstructions from management systems of business entities engaged in critical infrastructures as well as specifically envisioned threats arising from those problems or obstructions.

(1) Operation procedures

[9] Exercise in which participants discuss a certain scenario in conference format

[10] Exercise to simulate command and judgment line of actual organization and evaluate it

Gradually implemented plan shall be performed to understand concepts of exercise and create concrete subjects.

A. The goal in FY 2006

1) Perform exercises which focus on setting concepts and projects and understanding methods of the exercise ("the exercise for research")
2) Perform "the tabletop exercise" to find discussion topics by a group of similar business operation or sharing cross-sectorally common issues
3) Through "the tabletop exercise", posit specifically envisioned threats and scenarios in response to them in each group of common sectors
4) Also consider starting each CEPTOAR

B. The goal in FY 2007

1) After starting each CEPTOAR, conduct "the functional exercises" based on an exercise scenario by each group of common sectors to investigate technical and organization operational issues.
2) Based on results from the investigation, enlarge the range of cross-sectorally common issues if required.

(2) Operation systems

A. Operation System for "exercise for research"

1) "The operation plan for exercise for research" shall be made by the Cabinet Secretariat.
2) Under the direction of the Cabinet Secretariat, each critical infrastructure sector shall follow the plan.

B. Operation system for "tabletop exercise"

1) "The operation plan for tabletop exercise" shall be made by the Cabinet Secretariat.
2) Under the direction of the Cabinet Secretariat, temporary tasks for the tabletop exercise shall be set and each critical infrastructure shall follow the plan.

C. Operation system for the functional exercise (FY2007)

1) Form "the exercise planning team" by the Cabinet Secretariat, each presiding Ministry and Agency of the relevant critical infrastructures and each CEPTOAR.

2) The exercise planning team shall make a "functional exercise plan[11]."

7. Issues to be addressed by each entity, and entity cross-sectoral measures

(1) Issues to be addressed by the Cabinet Secretariat

A. Cross-sectoral measures for critical infrastructures sectors

The Cabinet Secretariat, with the cooperation of relevant agencies, shall perform the following in a cross-sectoral fashion.

1) Continuously investigate and analyze threats, mechanisms of malfunction occurrence and measures against them

2) Start a coupled system with measures against disasters and physical terrorism, etc.

3) Perform Analysis of Interdependence

4) Plan and perform "Cross-Sectoral Exercise" with a theme picked in each fiscal year.

5) Support each critical infrastructure sector to start and review "Safety Standards, Guidelines, etc."

6) Based on results from the Analysis of Interdependence evaluate "Safety Standards, Guidelines, etc."

B. Developing systematic information sharing frameworks

With the cooperation of relevant agencies, the Cabinet Secretariat shall drive forward the development of systematic information sharing frameworks for public and private sectors to protect critical infrastructures.

1) Summarize information such as information concerning terrorism, threats and methods of attack and recovery, which shall be provided to business entities engaged

[11] A functional exercise plan defines the plan for controlling the exercise scenario and the role that CEPTOAR and/or the business entities engaged in critical infrastructures should play.

in critical infrastructures,

2) Develop information providing frameworks from the government to business entities engaged in critical infrastructures

(a) Provide organized/summarized information to business entities engaged in critical infrastructures via presiding Ministries and Agencies of the relevant critical infrastructures.

(b) Based on the priority set by results from Analysis of Interdependence, enhance the frameworks to provide information about vulnerability, etc.

(c) When providing information, summarize relevant information for user's convenience. Then conduct systematical numbering according to the importance (degree of effect).

(d) Enhance cooperation among central government agencies concerning information security, central government agencies dealing with individual cases and other Related Organizations.

3) Start a center with functions for coordinating communication among business entities engaged in critical infrastructures in the occurrence of IT-malfunction emergency.

4) Support each entity to start "CEPTOAR Council" (tentative)

C. Supporting each entity to improve its protection capability

The Cabinet Secretariat shall drive forward the following measures to support each entity to improve its protection capability.

1) Through Cross-Sectoral Exercises, develop personnel with advanced skills

2) Responsible persons from presiding Ministries and Agencies of the relevant critical infrastructures shall also work in liaison at the Cabinet Secretariat.

D. Enhance functions of the Cabinet Secretariat

National Information Security Center (NISC) shall drive forward the following measures to start the above A, B and C in FY2006 officially.

1) Utilize information collected and analyzed to "Help central government agencies deal with individual cases" (decision by IT Strategic Headquarters on 7 December, 2004, 2.3)

2) Place a contact person from each critical infrastructure sector to ensure expertise for intensified coordination with liaison from presiding Ministries and Agencies of the relevant critical infrastructures.

3) For handling of corporate information in each critical infrastructure sector, secure confidentiality from personnel and material aspects and improve the environment of exchanging highly reliable information.

(2) Issues to be addressed by respective business entities engaged in critical infrastructures and presiding Ministries and Agencies of the relevant critical infrastructures

A. Functions to be established/enhanced by each business entity engaged in critical infrastructures and presiding Ministries and Agencies of the relevant critical infrastructures

Each business entity engaged in critical infrastructures and presiding Ministry and Agency of the relevant critical infrastructures shall make efforts to establish the following functions.

1) Overall Efforts

To enhance the capability of protecting critical infrastructures in our whole nation, each presiding Ministry and Agency of the relevant critical infrastructures shall address the following issues in conjunction with measures promoted by the Cabinet Secretariat.

(a) Establish a cooperating system with measures against disasters and physical terrorism

(b) With cooperation of the Cabinet Secretariat, plan and conduct "Cross-Sectoral Exercise" with a theme picked in each fiscal year.

(c) Support and evaluate each critical infrastructure sector to establish or review "Safety Standards, Guidelines, etc."

2) Develop Systematic Information Sharing Frameworks

To realize effective connection/coordination frameworks of each business entity engaged in critical infrastructures and presiding Ministry and Agency of the relevant critical infrastructures shall address the following issues in conjunction with measures promoted by the Cabinet Secretariat.

(a) Collect information to be provided for business entities engaged in critical infrastructures according to the capability and functions (information concerning terrorism, threats and methods of attack and recovery)

(b) Provide information from the Cabinet Secretariat to each business entity engaged in critical infrastructures via each CEPTOAR.

(c) Promote information sharing within each business entity engaged in critical infrastructures (such as establishing CEPTOAR)

(d) In response to "Review of Possible Threats", enlarge the range of information of IT-malfunctions from business entities engaged in critical infrastructures from incidents, failures and delay of operation which are required to report by law to those which the business entity regards as especially critical.

(e) Responsible person from presiding Ministries and Agencies of the relevant critical infrastructures shall also work in liaison at the Cabinet Secretariat.

B. Framework to be established by each business entity engaged in critical infrastructures

To establish the above functions promptly and effectively, each business entity engaged in critical infrastructures shall address the following issues.

1) In conjunction with establishment of a framework at the Cabinet Secretariat, establish frameworks for encouraging information sharing within each critical infrastructure sector (establishing CEPTOAR) and developing/reviewing "Security Standards, Guidelines, etc." and start activities from FY2006.

2) At the same time, consider promotion cross-sectoral information sharing (such as setting up CEPTOAR-Council" (tentative).

3) Establish intensified information sharing frameworks with presiding Ministries and Agencies of the relevant critical infrastructures.

C. Frameworks to be established by presiding Ministries and Agencies of the relevant critical infrastructures

To establish the above functions promptly and effectively, each presiding Ministry and Agency of the relevant critical infrastructures shall address the following issues.

1) Establish frameworks for encouraging information sharing within each critical infrastructure sector (establishing CEPTOAR) and a support system for developing/reviewing "Safety Standards, Guidelines, etc."

2) Consider establishing a system to support cross-sectoral information sharing (such as

setting up CEPTOAR-Council" (tentative).

3) Establish intensified information sharing frameworks with business entities engaged in critical infrastructures.

4) Support and advice from presiding Ministries and Agencies of the relevant critical infrastructures to business entities engaged in critical infrastructures

(3) Issues to be addressed by central government agencies concerning information security

Central government agencies concerning information security which have been dealing with information security issues as their policies shall address the following issues to implement protection plans of critical infrastructures in Japan, which is led by the Cabinet Secretariat

A. Collect information to be provided for business entities engaged in critical infrastructures according to the capability and functions (information concerning terrorism, threats and methods of attack and recovery)

B. Corporate with the Cabinet Secretariat to enhance the framework of collecting, providing and sharing appropriate information.

C. Central government agencies concerning information security shall continuously make efforts to address relevant issues such as improving capability to deal with them.

(4) Issues to be addressed by central government agencies dealing with individual cases

Central government agencies dealing with individual cases such as cyber terrorism shall address the following issues to encourage protection system for critical infrastructures in Japan, which is led by the Cabinet Secretariat.

A. Collect information to be provided for business entities engaged in critical infrastructures according to the capability and functions (information concerning terrorism, threats and methods of attack and recovery)

B. Corporate with the Cabinet Secretariat to enhance the framework of collecting, providing and sharing appropriate information.

C. Central government agencies dealing with individual cases shall continuously make efforts to address cyber terrorism related issues such as improving capability to deal with them.

(5) Other issues to be addressed by other relevant agencies, and Related Organizations.

Other than the above-mentioned sectors, as a nation, the following issues should be concerning the enhancement of the protection system for critical infrastructures.

Provide information, which implements information providing/sharing frameworks based on public-private partnership, to business entities engaged in critical infrastructures and CEPTOAR.

(6) Enhance Foundation of Information Security

A. Develop skilled personnel

For higher education institutions (especially graduate schools), consider establishing a system to develop personnel with multifaceted ability or recurrent education such as exchanging a certain number of students/working adults from different sectors. Aggressively support to establish new graduate schools or courses which aim to develop relevant personnel.

Through exercises, training and seminars, personnel with advanced IT skills shall be developed mainly by presiding Ministries and Agencies of the relevant critical infrastructures and business entities engaged in critical infrastructures.

B. Encourage R & D by using results achieved

When establishing a strategy for R & D/technical development in information security field, consider overall measures against “IT Functional Failure” which may result in IT-malfunctions for critical infrastructures, to encourage R & D which strengthens capability to deal with threats evolving on a day-to-day basis.

C. Encourage local efforts

During working hours, establish information sharing and connection/coordination systems among relevant government district offices, local governments, business entities engaged in critical infrastructures and local organizations related to information security in conjunction with the government system.

D. International Coordination

The government shall encourage international coordination towards information security such as measures against cyber terrorism of OCED and G8.

Also, the government and business entities engaged in critical infrastructures shall take action to collect information regarding overseas information security, and with due caution of handling confidential information, actively join the early-warning/monitoring/alarming network for protecting critical infrastructures to enhance international coordination including exchanging information with overseas Related Organizations and joint trainings.

8 Promoting systems for Action Plans

(1) Evaluation/verification of progress

Progress of this Action Plan shall be evaluated/verified by Information Security Policy Council every year.

(2) Reviewing Action Plan

Considering results from evaluation or verification of the progress, this Action Plan shall be reviewed every 3 years (2 years after the establishment of the plan, take 12 months to review it in consideration of the results), or if required.

(3) Challenges for the future

The purpose of this Action Plan shall protect people's social lives and economic activities from IT-malfunctions. To achieve this purpose, the government and private sectors shall be required to play their responsible roles to establish independent measures for critical infrastructures and those for the government and each critical infrastructure sector led by the Cabinet Secretariat through the close liaison with public and private sectors.

On a mid and long term basis, since the injection of resources throughout the whole nation is continuously encouraged from a wide range of sectors to develop information security measures for critical infrastructures while keeping uniqueness of business entities engaged in critical infrastructures, it shall be required to consider necessary measures such as developing a legal system to facilitate further information sharing.

9 Others

When a decision on this Action Plan is made, “Special Action Plan on Countermeasures to cyber-terrorism for Critical Infrastructures” (Decision by Infomation Security Policy Council on 15 December, 2000) shall be discarded.

Attachment 1

Target critical information systems for each critical infrastructure sector

Sector		Threats, risks such as information system failure and illegal operation	Target business entities engaged in critical infrastructures, etc (Note 1)	Examples of target critical information system (Note 2)
Telecommunications		Stoppage of telecommunication service Problems with safe and stable supply of telecommunication service Stoppage of broadcasting service	Main telecommunication companies Main broadcasting companies	* Network System * Operation Support System * News/Program system * Programming/Operating System
Finance	Bank Life Insurance Damage Insurance Securities company Stock exchange	Stoppage of deposit withdrawal, fund transfer such as crediting and loan process * Stoppage of the paying of insurance amount * Stoppage of the buying and selling of valuable securities, etc.	Banks, cooperative banks, credit cooperative, agricultural cooperative, etc. * Life insurances, damage insurances, securities companies, etc. * Stock exchange, etc	*Accounting system * Fund bill system * International system * External connection system * Insurance system *Stock exchange system * Exchange system, etc (including services using open networks)
Civil aviation		*Delay and Cancellation of Operation *Problems with safe operation of aircrafts	*Main scheduled air carriers *Ministry of Land, Infrastructure and Transport (Air control, weather)	* Operation System * Booking and boarding system * Maintenance system * Cargo system * Air control system * Weather information system
Railways		* Delay and cancellation of train operation *Problems with safe and stable operation of trains	* Main railway companies such as each JR company and major private railway companies	* Train traffic control system * Electricity management system * Seat reservation system
Electricity		Stopping of electrical power * Problems with safety operation of electrical power plants, etc.	* General electrical power suppliers, Japan Atomic Power Co. and Electric Power Development Co., Ltd.	* Plant Control system * Plant Operation and monitoring system

Gas	* Stoppage of gas supply * Problems with safety operation of gas plants, etc	* Major gas suppliers	* Plant control system * Remote monitor/control system
Governmental/ Administrative services	* Problems with governmental/administrative services Leakage, sniffing and falsifying of personal information	*Each ministry and agency * Local governments	*Information system of each ministry and agency and local governments (corresponding to e-Government/ e-municipality)
Medical services	* Problems with operation at practice support division	* Medical institutions	* Electronic medical charts management system * Remote medicine system
Water works	* Stoppage of water supply by water line *Water supply with inappropriate water quality	* Water supply enterprises and city water supply enterprises (except for small scale ones)	* Monitoring system for water utilities and tap water. * Control system for water utilities, etc.
Logistics	*Delay and cancellation of transportation * Difficulty in tracing location of cargo	*Major distribution companies	* Management system for delivery and collection * Cargo tracing system * Warehouse management system

Note1 Targeted business entities shown in this table are business entities engaged in critical infrastructures 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 business entities engaged in critical infrastructures in consideration of examples of threats and dangers.

Attachment 2

Reporting system for IT-malfunction Occurrence

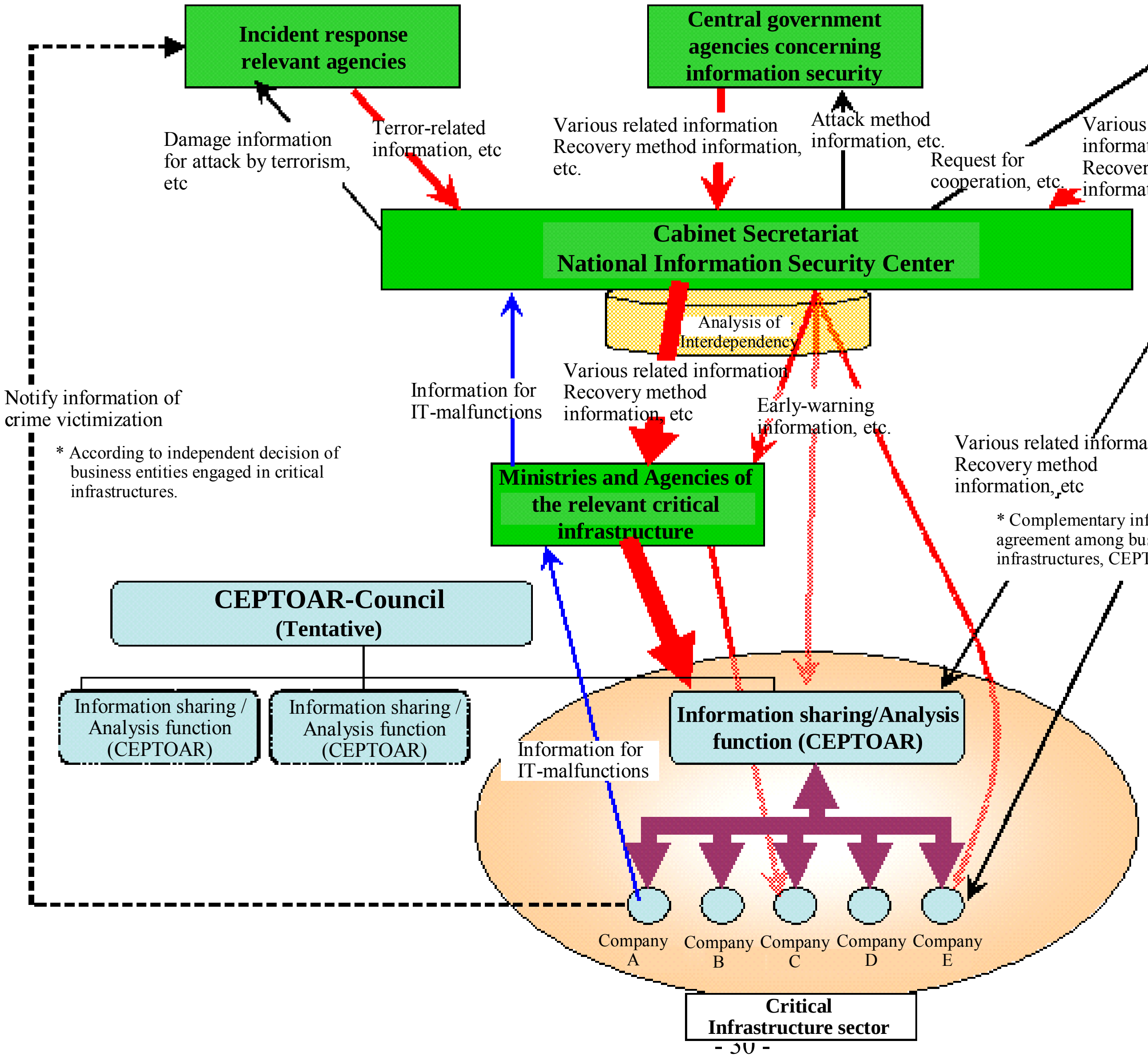
Sector		Current Reporting system	Emergency reporting system for IT-malfunction Occurrence	Security measures of sectors which share information security relevant information
Telecommunications		(1) Business entity engaged in critical infrastructures → Government * Based on Telecommunications Service Law, report information such as stoppage of operation to Minister of Internal Affairs and Communications * On the Basic Law on Natural Disasters, report information such as damage situation of telecommunications facilities from emergency measures on natural disasters *Report information such as incidents of broadcast interruption, critical wireless interference to Ministry of Internal Affairs and Communications (2) Government → Business entity engaged in critical infrastructures , and among business entities engaged in critical infrastructures * Notify/share emergency information for virus occurrence among the industry and Ministry of Internal Affairs and Communications	(1) Business entity engaged in critical infrastructures → Government * Utilize the current system to report (2) Government → Business entity engaged in critical infrastructures * Utilize the current system to report	* Utilize the information sharing system for virus occurrence to implement
Finance	Bank Life Insurance, Accident Insurance Securities company Stock exchange	(1) Business entity engaged in critical infrastructures → Government * Based on business laws, report information such as service delay/cancellation to Prime Minister (Financial Services Agency) (2) Government → Business entity engaged in critical infrastructures , and among business entities engaged in critical infrastructures	(1) Business entity engaged in critical infrastructures → Government * Utilize the current system to implement (2) (2) Government → Business entity engaged in critical infrastructures * Report through business entities organizations	* Implement through business entities organizations such as Japan Bankers Association, Center for Financial Industry Information Systems (FISC)

Civil aviation	(1) Business entity engaged in critical infrastructures → Government * Based on Aviation Law, report information regarding air accidents to Minister of Land. (2) Government → Business entity engaged in critical infrastructures, and among business entities engaged in critical infrastructures * Place of liaison for IT-malfunction * Share information regarding defects in sky marshal system among related organizations (within an airport)	(1) Business entity engaged in critical infrastructures → Government * In the event of accident, report in accordance with the current accident reporting system * Regarding IT-malfunction before it becomes an accident, report on the reporting system for IT-malfunction (2) Government → Business entity engaged in critical infrastructures * Directly report to business entities engaged in critical infrastructures through the liaison	
Railways	(1) Business entity engaged in critical infrastructures → Government, Government → Business entity engaged in critical infrastructures * Based on report regulations on railroads accidents, report information relating to railroad operation accidents to Minister of Land. * Establish a reporting system for IT-malfunction (2) Among Business entities engaged in critical infrastructures * Nothing special	(1) Business entity engaged in critical infrastructures → Government, Government → Business entity engaged in critical infrastructures * In the event of an accident, implement in accordance with the current reporting system	
Electricity	(1) Business entity engaged in critical infrastructures → Government * Based on anti-disaster operation plan, regulations on reporting electrical power related issues, report information regarding accidents of electrical power plants to Minister of economy, trade and industry. (2) Government → Business entity engaged in critical infrastructures , and among business entities engaged in critical infrastructures * Nothing special	(1) Business entity engaged in critical infrastructures → Government * Utilize the current system to report (2) Government → Business entity engaged in critical infrastructures * Implement through business entity organization	* Implement through business entity organization

Gas	(1) Business entity engaged in critical infrastructures → Government * Based on Enforcing Regulations for Gas Utility Industry Law, report information such as certain scale of gas supply failure to Minister of economy, trade and industry (2) Government → Business entity engaged in critical infrastructures, and among business entities engaged in critical infrastructures * Based on “Guidelines for relief measures”, the measures against gas supply failure caused by natural disasters, report to the entire industry	(1) Business entity engaged in critical infrastructures → Government * Utilize the current system to implement (2) Government → Business entity engaged in critical infrastructures * Implement through business entity organization	* Implement through the committee in the industry
Governmental/ Administrative services	(1) Each ministry and agency → Cabinet Secretariat * Report based on “Emergency report for information system of governmental agencies” (2) Cabinet Secretariat → Each ministry and agency * Provide information based on “Emergency report for information system of governmental agencies” (3) Local governments → Government * Provide information based on “Emergency report for information system of local governments” (4) Government → Local governments * Provide information based on “Emergency report for information system of local governments”	(1) Each ministry0and agency → Cabinet Secretariat, Cabinet Secretariat → Each ministry * Report on the reporting system for inside the government (2) Local governments → Government, Government → Local governments * Utilize the current reporting system to report.	* Report on the reporting system for inside the government
Medical services	(1) Business entity engaged in critical infrastructures → Government, etc. (2) Government, etc. → Business entities engaged in critical infrastructures	(1) Business entity engaged in critical infrastructures → Government, etc. (2) Government, etc. → Business entities engaged in critical infrastructures	

Water works	(1) Business entity engaged in critical infrastructures → Government, etc. (2) Government, etc. → Business entities engaged in critical infrastructures	(1) Business entity engaged in critical infrastructures → Government, etc. (2) Government, etc. → Business entities engaged in critical infrastructures	
Logistics	(1) Business entity engaged in critical infrastructures → Government * Based on Trucking Business Law, Law on Freight and Express Business and Warehouse Business Law, report information such as critical car accidents, critical cargo accidents and warehouse fire to Minister of Land, Infrastructure and Transportation (2) Government → Business entity engaged in critical infrastructures. * Public agencies specified by Basic Law on Natural Disasters（Cabinet Secretariat）	(1) Business entity engaged in critical infrastructures → Government (2) Government → Business entity engaged in critical infrastructures	* Implement through business entity organization

Attachment 3-1



Incident response relevant agencies

Central government agencies concerning information security

Related Organizations

Damage information for attack by terrorism, etc

Terror-related information, etc

Various related information Recovery method information, etc.

Attack method information, etc.

Request for cooperation, etc.

Various related information Recovery method information, etc

Cabinet Secretariat National Information Security Center

Analysis of Interdependency

Notify information of crime victimization

* According to independent decision of business entities engaged in critical infrastructures.

Information for IT-malfunctions

Various related information Recovery method information, etc

Early-warning information, etc.

Various related information Recovery method information, etc

Ministries and Agencies of the relevant critical infrastructure

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

CEPTOAR-Council (Tentative)

Information sharing / Analysis function (CEPTOAR)

Information sharing / Analysis function (CEPTOAR)

Information sharing/Analysis function (CEPTOAR)

Information for IT-malfunctions

Company A

Company B

Company C

Company D

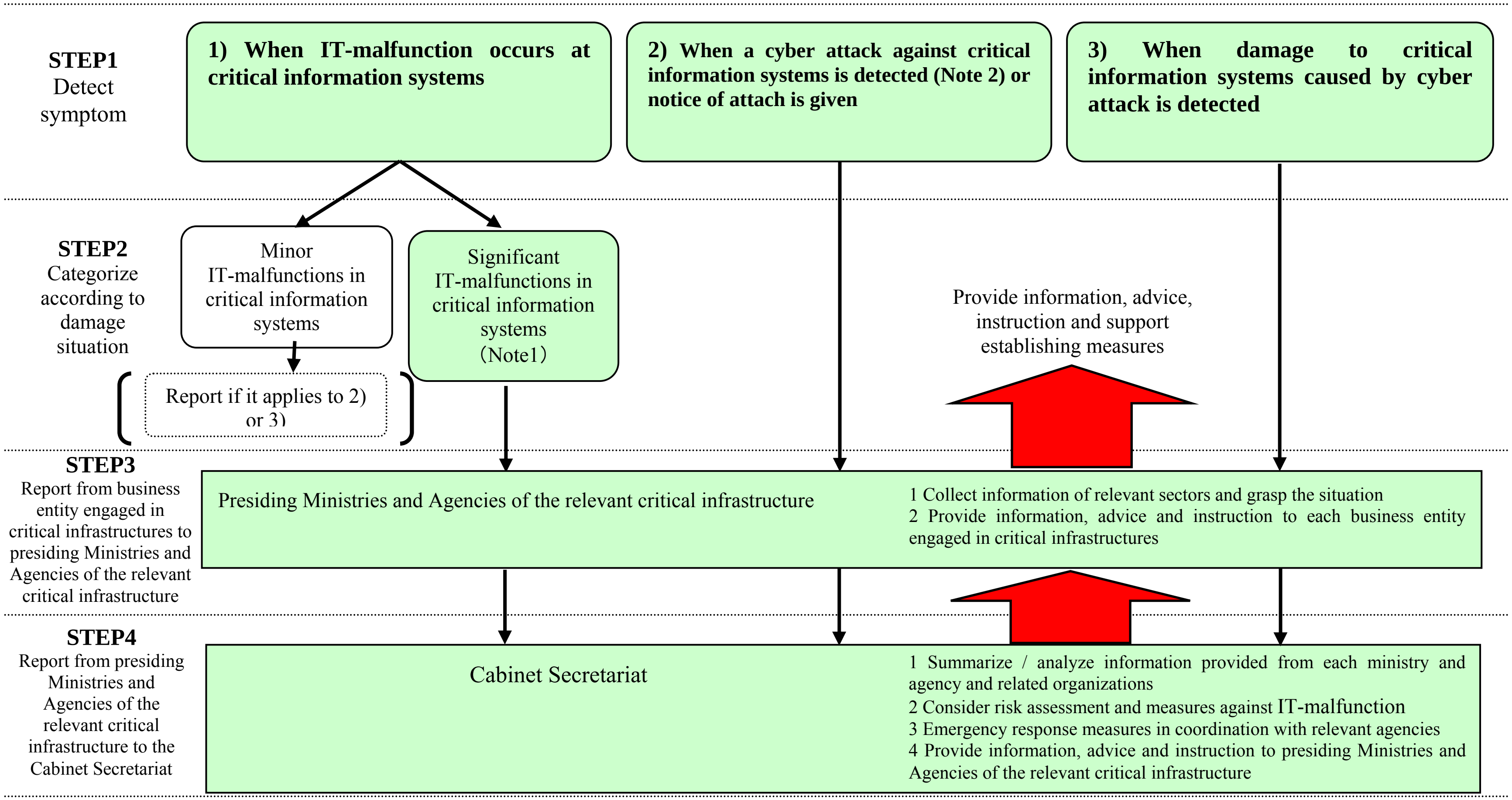
Company E

Critical Infrastructure sector

Note: This diagram shows the future flow of information required for service maintenance or recovery of critical infrastructures, which is based on an appropriate system of providing for / sharing with business entities engaged in critical infrastructures. The arrow (···▶) basically indicates a range not covered in this diagram, however, it is shown for reference, to clarify meaning of other arrows.

Attachment 3-2

IT-malfunctions required to be reported (Cyber attack)



STEP1
Detect symptom

1) When IT-malfunction occurs at critical information systems

2) When a cyber attack against critical information systems is detected (Note 2) or notice of attach is given

3) When damage to critical information systems caused by cyber attack is detected

STEP2
Categorize according to damage situation

Minor IT-malfunctions in critical information systems

Report if it applies to 2) or 3)

Significant IT-malfunctions in critical information systems （Note1）

Provide information, advice, instruction and support establishing measures

STEP3
Report from business entity engaged in critical infrastructures to presiding Ministries and Agencies of the relevant critical infrastructure

Presiding Ministries and Agencies of the relevant critical infrastructure

1 Collect information of relevant sectors and grasp the situation
2 Provide information, advice and instruction to each business entity engaged in critical infrastructures

STEP4
Report from presiding Ministries and Agencies of the relevant critical infrastructure to the Cabinet Secretariat

Cabinet Secretariat

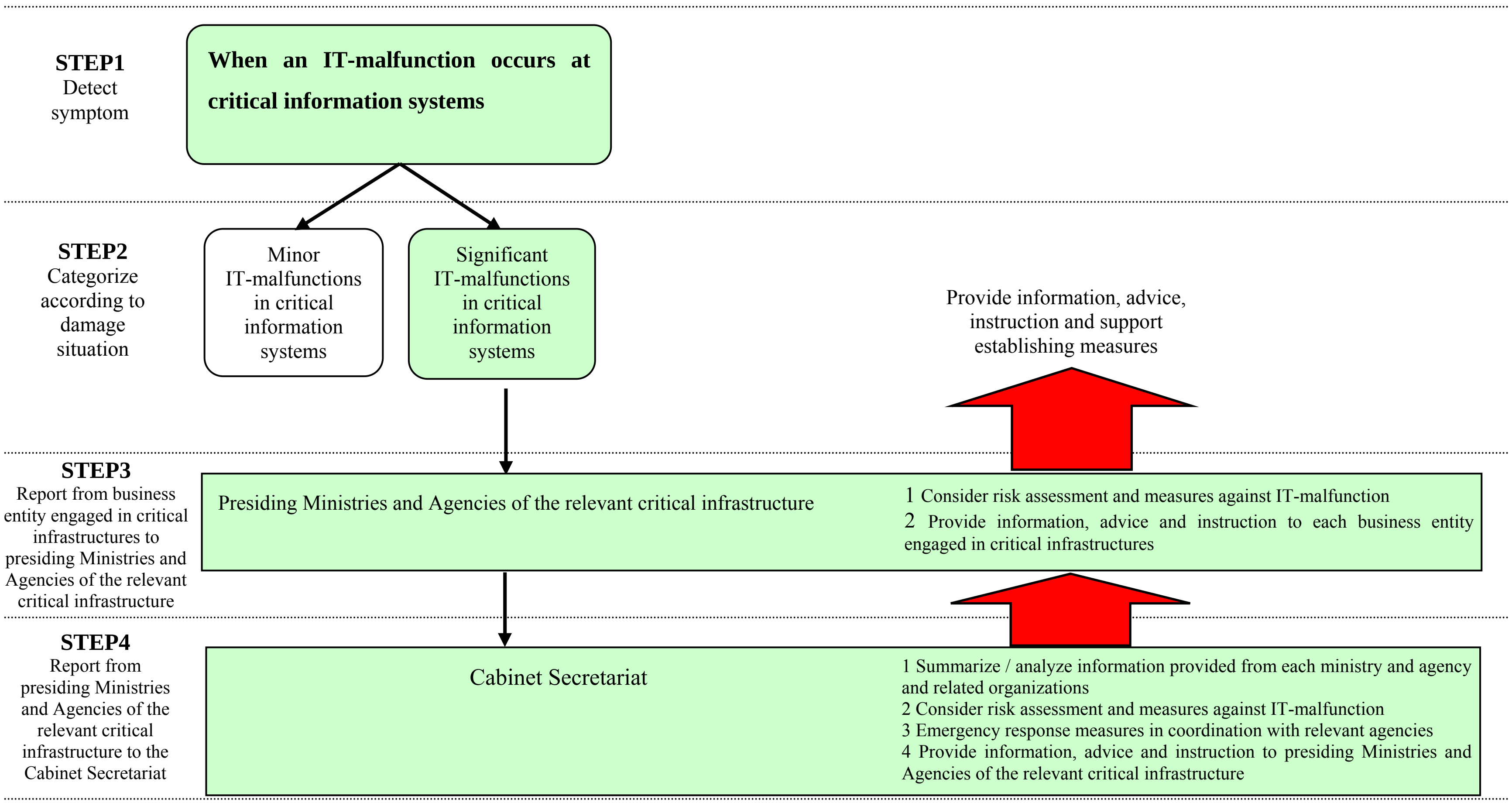
1 Summarize / analyze information provided from each ministry and agency and related organizations
2 Consider risk assessment and measures against IT-malfunction
3 Emergency response measures in coordination with relevant agencies
4 Provide information, advice and instruction to presiding Ministries and Agencies of the relevant critical infrastructure

(Note 1) ”Critical IT-malfunction” shall include incidents, failures and delay of operation which are required to be reported by law as well as those which the business entity engaged in critical infrastructures regards as especially critical.

(Note 2) “When a cyber attack is detected” shall mean only “When no actual damage is occurred but the attack with high potential to cause the damage is detected” (See Attachment 4)

Attachement3-3

IT-malfunctions required to be reported (Unintentional Factors)



STEP1
Detect symptom

When an IT-malfunction occurs at critical information systems

STEP2
Categorize according to damage situation

Minor IT-malfunctions in critical information systems

Significant IT-malfunctions in critical information systems

Provide information, advice, instruction and support establishing measures

STEP3
Report from business entity engaged in critical infrastructures to presiding Ministries and Agencies of the relevant critical infrastructure

Presiding Ministries and Agencies of the relevant critical infrastructure

1 Consider risk assessment and measures against IT-malfunction
2 Provide information, advice and instruction to each business entity engaged in critical infrastructures

STEP4
Report from presiding Ministries and Agencies of the relevant critical infrastructure to the Cabinet Secretariat

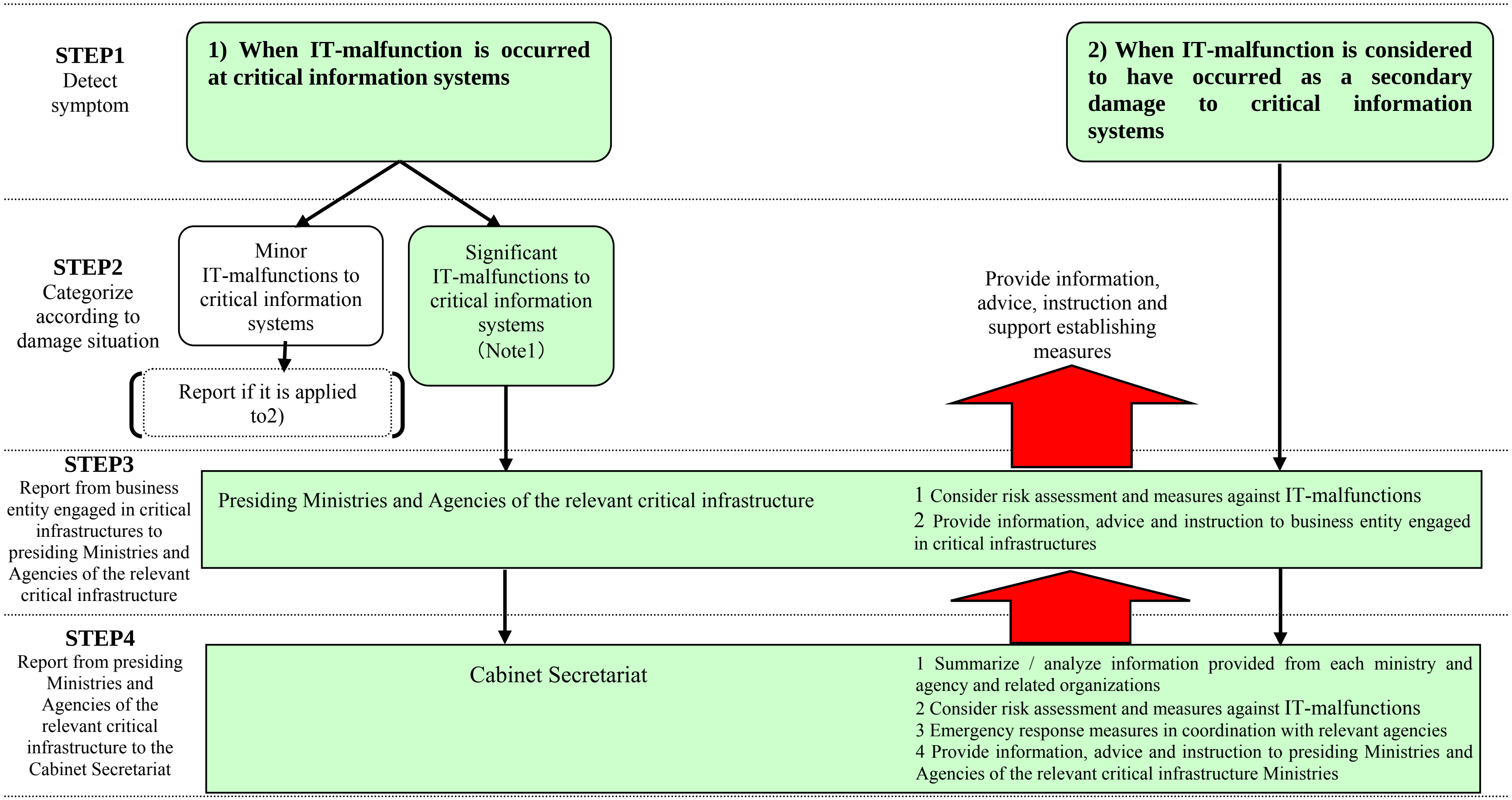
Cabinet Secretariat

1 Summarize / analyze information provided from each ministry and agency and related organizations
2 Consider risk assessment and measures against IT-malfunction
3 Emergency response measures in coordination with relevant agencies
4 Provide information, advice and instruction to presiding Ministries and Agencies of the relevant critical infrastructure

(Note 1) ”Critical IT-malfunction” shall include incidents, failures and delay of operation which are required to be reported by law as well as those which the business entity engaged in critical infrastructures regards as especially critical.

Attachmment3-4

IT-malfunctions required to be reported (Disasters)



STEP1
Detect symptom

1) When IT-malfunction is occurred at critical information systems

2) When IT-malfunction is considered to have occurred as a secondary damage to critical information systems

STEP2
Categorize according to damage situation

Minor IT-malfunctions to critical information systems

Report if it is applied to2)

Significant IT-malfunctions to critical information systems （Note1）

Provide information, advice, instruction and support establishing measures

STEP3
Report from business entity engaged in critical infrastructures to presiding Ministries and Agencies of the relevant critical infrastructure

Presiding Ministries and Agencies of the relevant critical infrastructure

1 Consider risk assessment and measures against IT-malfunctions
2 Provide information, advice and instruction to business entity engaged in critical infrastructures

STEP4
Report from presiding Ministries and Agencies of the relevant critical infrastructure to the Cabinet Secretariat

Cabinet Secretariat

1 Summarize / analyze information provided from each ministry and agency and related organizations
2 Consider risk assessment and measures against IT-malfunctions
3 Emergency response measures in coordination with relevant agencies
4 Provide information, advice and instruction to presiding Ministries and Agencies of the relevant critical infrastructure Ministries

(Note 1) ”Critical IT-malfunction” shall include incidents, failures and delay of operation which are required to be reported by law as well as those which the service provider regards as especially critical.