Principles for Formulating of "Safety Standards, Guidelines, etc." concerning Assurance of Information Security of Critical Infrastructures

February 2, 2006
Decision by the Information Security Policy Council

I. Purpose and positioning

1. For the assurance of information security of critical infrastructures

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 concerning IT-malfunction[1] in critical infrastructures[2] need to be strengthened.

To achieve a prompt solution to this issue, respective business entities engaged in critical infrastructures[3] should take appropriate information security measures promptly, considering the characteristics of relevant business sectors and business entities.

2. Needs for "Safety Standards, Guidelines, etc"

Business entities engaged in critical infrastructures are aware of the fact that people's social lives are largely dependent on their services, and they are striving daily to provide higher quality services on a constant basis in order to meet national expectations.

However, due to the opaque effects 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, each business sector should make an effort to clarify the standards for necessary or desired information security measures in the form of the "Safety Standards, Guidelines, etc." With an awareness of being a figure that plays a leading role in developing critical infrastructures, each business entity should make voluntary efforts to comply with the

---

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

[2] IT-malfunction: IT functional failures occurring in each business sector of critical infrastructures (e.g. suspension of services, or deteriorating functionality)

[3] "Business entities engaged in critical infrastructures" shall mean any entities specified in Attachment 1 of the "Action Plan on Information Security Measures for Critical Infrastructures" (decision by the Information Security Policy Council, Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society on December 13, 2005) and those composed of such business entities engaged in "Telecommunications", "Finance", "Civil aviation", "Railways", "Electricity", "Gas", "Governmental Administrative services (including local governments), "Medical services", "Water works" and "Logistics".

"Safety Standards, Guidelines, etc." and should also examine the status of their compliance.

3. What is the "Safety Standards, Guidelines, etc."?

Business entities engaged in critical infrastructures operate their businesses in compliance with a variety of national standards and guidelines under "business laws (*Gyohou*)," or a group of laws for governing the business entities[4].

In the Principles for Formulating "Safety Standards, Guidelines, etc." concerning Assurance of Information Security of Critical Infrastructures (hereinafter referred to as the "the Principles"), "Safety Standards, Guidelines, etc." shall refer to the documents formulated by the business entities and used as a standard or reference when making decisions and taking actions. More specifically, the "Safety Standards, Guidelines, etc." include:

(1) "Mandatory standards" set by the government under business laws
(2) "Recommended standards" and "guidelines" set by the government, pursuant to business laws
(3) Cross-sectoral "industry standards" and "guidelines" set by business associations that manage over the business entities, under business laws or in line with national expectations
(4) "Internal regulations" set by the business entities under business laws or in line with national expectations or expectations from their contractors.

In order to ensure that necessary information security measures are implemented, what measures should be taken up to what level needs to be clearly defined in the "Safety Standards, Guidelines, etc." It is desirable that all business entities engaged in critical infrastructures and other people concerned are able to understand "what to do," by reference to standards, guidelines, or regulations described in (1) to (4) above.

4. Positioning of the Principles

As described above, the most difficult aspect in implementing information security measures is deciding "what to do" and "up to what level."

When information security measures are implemented from the viewpoints of providing critical infrastructure-related services on an ongoing basis and living up to the confidence the public may place in critical infrastructures, some approaches need to be taken for specific items. The Principles aim to support the formulation and revision of the "Safety

[4] Under the Local Autonomy Law, local governments are carrying out their administrative activities voluntarily and comprehensively.

Standards, Guidelines, etc." by listing such items.

Therefore, the Principles shall list items for implementation, by taking the following into consideration: disasters, unintentional factors, and other events that may affect providing services, measures against cyber attacks, security measures for control systems that are a basis for providing critical infrastructure-related services, and countermeasures against information leakage resulting in newly emerging threats and people's lost confidence in critical infrastructures.

Since the importance level of each item may differ among critical infrastructure sectors and business entities, the Principles shall list the items only. Further details about each item are expected to be considered by each business sector or business entity. The Principles shall cover critical infrastructures cross-sectorally, list relevant items, especially those considered necessary, and focus on information security measures. Therefore, the following should be kept in mind:

(1) Even if some item is described in the Principles, business sectors or business entities may not be required to define the item due to the nature of business or other reasons.

(2) Even if some item is not described in the Principles, business sectors or business entities may be required to define the item due to the nature of business or other reasons.

In accordance with business laws and existing safety standards, each business sector needs to consider in what documents, out of "Safety Standards, Guidelines, etc." the items described in the Principles and execution levels thereof should be defined.

5. Expectations for the formulation and revision of "Safety Standards, Guidelines, etc." based on the Principles

The Principles do not take into consideration what safety standards and guidelines exist for each critical infrastructure sector or business entity. Therefore, some business sectors or business entities may already have their own safety standards and guidelines covering all of the items described in the Principles.

The Principles aim to support the formulation and revision of safety standards and guidelines so that at least minimum information security measures may be taken. Therefore, safety standards and guidelines set by each business sector or business entity need to be reviewed as needed in order to be more advanced and comprehensive, and also need to cover items as described in the Principles in order to achieve more advanced security levels.

From this viewpoint, it is desirable to actively refer to domestic or foreign standards and best practices, as well as, where necessary, the Standards for Information Security Measures

for the Central Government Computer Systems (hereinafter referred to as the “Standards for Measures”) and relevant documents.

II. Items to be defined in “Safety Standards, Guidelines, etc.”

1. Scope of “Safety Standards, Guidelines, etc.” and target threats

It is desirable to define all elements which will be closely related with the business continuity of the business entities engaged in critical infrastructures in the case of IT -malfunction as the scope of protection. For example, the following shall be protected.

(1) Information assets (Information systems and information stored therein)

(2) Transactions[5] or business processes occurring among information systems

(3) Management of information systems

It is also desirable to define the target threats from assumptions of IT-malfunctions, such as those listed below, and by considering the characteristics of each critical infrastructure sector, such as their impact on business continuity.

(1) IT-malfunction due to cyber attacks

Hacking, data falsification, rough command execution, information disturbance, virus attack, Denial of Service (DoS) attack, information leakage, etc.

(2) IT-malfunction due to unintentional factors

Defects (bugs) in programs and system specifications, operational errors, failures, information leakage, etc.

(3) IT-malfunction due to disasters

IT functional failures 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.

2. Disclosure of the “Safety Standards, Guidelines, etc.”

Critical infrastructures have an enormous social responsibility and have a significant impact on people's social lives. Therefore, from the viewpoint of manifesting efforts in critical infrastructure sectors to achieve a safe and comfortable society, it is desirable to establish provisions concerning the disclosure of the “Safety Standards, Guidelines, etc.” and to actually disclose them as much as possible.

[5] A processing unit integrating two or more relevant processes. Transactions are used to manage a series of processes as a single event such as the processing of deposits and withdrawals in the computer systems of financial institutions.

It is also desirable to state clearly the nondisclosure of the items whose disclosure may increase threats to the public, as well as to provide the reasons.

3. Detailed items

It is advisable to include the following items in the "Safety Standards, Guidelines, etc." The "Safety Standards, Guidelines, etc." should be formulated or revised with due consideration for its effectiveness and rationality.

(1) Purpose for formulating "Safety Standards, Guidelines, etc."

IT-malfunctions may impede the provision of services in critical infrastructure sectors. In order to ensure implementing measures against IT-malfunctions, the necessity of compliance with the "Safety Standards, Guidelines, etc." shall be defined by taking the characteristics of each business sector into account.

(2) Target scope and assumed threats

The scope of protection and assumed threats shall be defined and described as concretely as possible.

(3) Respective roles of business entities engaged in critical infrastructures, etc.

In order to be clear that entities take each measure, respective roles should be defined for presiding Ministries and Agencies, infrastructure sectors, and the business entities.

(4) Target items

The following four pillars and three prioritized items should be included in "Safety Standards, Guidelines, etc." (Some of the prioritized items included in any of the four pillars may be described.) Measures should be taken flexibly in accordance with the importance of the information system and information itself, as well as the status of utilization.

1) Four pillars

i) Establishment of organizations/frameworks, and the securing of resources

In order to allow business entities engaged in critical infrastructures to operate on the PDCA cycle[6] for information security measures, appropriate organizations and frameworks should be established for the administration of security measures, and

[6] The PDCA cycle is a typical management cycle and consists of "plan," "do," "check," and "act" processes to be implemented in that order. The completion of one turn of the cycle flows into the beginning of the next. The PDCA cycle aims to maintain/improve project quality and promote business improvement activities on an ongoing basis.

necessary resources should also be secured.

Information security measures will succeed only when all relevant staff members understand their authority and responsibility according to their positions and assignments, and fulfill their obligations by using the reserved resources.

Therefore, it is necessary to clearly indicate the information security measures organizations and frameworks are enforcing, as well as how they are securing resources.

The establishment of organizations/frameworks and the securing of resources include basic/long-term efforts such as the development and education of human resources engaged in information security, as well as concrete measures such as the provision of a rule (to ensure the effectiveness of information security measures) stating that people in specific positions are prohibited from assuming two or more positions at the same time, punishments for those who violate the rule, and the establishment of exceptions.

ii) Measures for protecting information

When the business entities engaged in critical infrastructures develop information security measures, they should determine the matters to be complied with at each stage of the information lifecycle, and present measures for protecting information in the course of the duties of each staff member.

a) Information rating

From the perspective of maintaining confidentiality, integrity, and availability, information rating and handling restrictions (e.g. inhibition of reproduction, outside use, or redistribution) should be defined in order to handle information in an appropriate manner according to the importance of the information.

b) Information handling

Necessary security measures should be implemented at each stage of the information lifecycle, including information preparation, acquisition, utilization, storage, transfer, provision, and deletion.

iii) Measures based on the clarification of security requirements

In order to allow business entities engaged in critical infrastructures to take appropriate security measures according to the importance of the information, access control and other security technologies to be adopted should be presented from the

perspective of maintaining confidentiality, integrity, and availability. In addition, security requirements should be defined to combat security holes, malicious programs, and DoS attacks, and appropriate measures to be taken should also be provided for information systems.

a) Requirements for information security

Security requirements to be adopted for information systems should be defined from the viewpoint of providing basic security functions such as the authentication of users and equipment, access control, authority control, and audit trails.

b) Threats to information security

Security requirements to be adopted for information systems should be defined against various threats such as security holes, malicious programs, and DoS attacks.

iv) Measures taken for information systems

Information systems used for control and business purposes have been increasing in importance for the continuity of businesses and services related to critical infrastructures.

Therefore, security measures should be provided for each information installation and system according to the lifecycle, and in compliance with clarified information security requirements.

Security measures for each event deemed necessary should also be provided, such as the restriction of outside information processing and the prevention of outside actions which may diminish information security levels.

Moreover, the introduction of codes and products evaluated objectively should be considered to promote building reliable information systems.

a) Facilities and the environment

Security measures, such as the monitoring of entering and exiting, the establishment of a safety zone, and responses to a blackout, should be provided for in the environment and facilities related to the installation and operation of information systems.

b) Electrical computers

Security measures should be provided for the installation, use, and termination of use of electrical computers.

c) Application software

Security measures should be provided for the introduction, use, and termination of use of application software.

d) Communication lines and devices

Security measures should be provided for the construction, use, and termination or suspension of use of communication lines and devices.

2) Three prioritized items

i) Measures for ensuring business continuity when IT-malfunctions occur

Critical infrastructures are a basis for supporting the Japanese people's social lives and economic activities. In fact, a large IT-malfunction in critical infrastructures will affect various fields significantly.

Therefore, in order to continue or resume critical infrastructure-related services after the occurrence of an IT-malfunction, more efforts should be made to ensure business continuity, and comprehensive measures should be provided for coping with IT-malfunctions.

a) Implementation of respective measures to ensure business continuity

Security measures should be provided for preemptive prevention of IT-malfunctions, to detect the occurrence of IT-malfunctions at an early stage, and to prevent the expansion of suffering, and rapid resumption in the case of an occurrence of IT-malfunction.

b) Consideration for consistency with business continuity plans

Business continuity plans should be formulated by taking various IT-malfunctions, which are highly likely to occur, into consideration.

ii) Measures for preventing information leakage

Recently, leakage of confidential or critical information has been occurring in critical infrastructure sectors. Since such leakage may result in the suspension or deterioration of the functionality of critical infrastructures, appropriate measures should be taken in each sector.

Confidential or critical information in critical infrastructure sectors may contain

personal information. Even if such personal information will not cause the suspension or deterioration of the functionality of critical infrastructures, appropriate security measures should be described in the “Safety Standards, Guidelines, etc.” ensuring consistency with the “Guideline for Protection of Personal Information” formulated or to be formulated in each relevant sector. It is desirable that measures be available to cope with the leakage of all types of information.

a) Classifying information to be protected into categories

The information to be protected against leakage should be classified into categories and be defined.

b) Managing information to be protected

Security measures should be provided for the safe handling (preparation, acquisition, utilization, storage, transfer, provision and deletion) of information to be protected and media that contain such information.

c) Measures against threats arising from illegal access

Security measures should be provided to prevent the theft and loss of computers or removable recording media that contain information to be protected, information leakage from computers or removable recording media, and information leakage from Websites, e-mail servers, or other applications handling information to be protected.

d) Measures against threats from insiders

Security measures should be provided to prevent insiders from leaking internal information, to ensure the traceability of information leakage, to improve information security literacy, and to reduce errors in information handling.

e) Developing measures for when information leakage occurs

The systems and procedures for coping with information leakage should be defined.

iii) Measures for ensuring information security by outsourcing

Recently, leakage of critical information has been occurring in critical infrastructure sectors. Such information is leaked not only by the business entities themselves but also by their outsourcing, and, in fact, information leakage by outsourcing is often observed.

Business continuity in critical infrastructure sectors requires the improvement of

information security levels in cooperation with outsourcing. Therefore, it is desirable that the business entities develop measures to ensure information security by outsourcing.

a) Frameworks for managing outsourcing

It is necessary to clarify the scope of outsourcing, and to indicate the standards for selecting outsourcing, information security measures to be taken by outsourcing, and methods for the business entities' management of outsourcing. These matters should be examined with reference to previous examples based on international standards.

b) Thorough implementation of measures for ensuring information security in adopting outsourcing services

The respective responsibilities of both signers and the conclusion of an agreement between them should be clearly defined, by entering into a basic contract and incorporating into the contract appropriate provisions concerning information security based on the types of outsourcing and according to the importance of the information.

c) Developing measures for coping with IT-malfunctions

Measures to be taken by outsourcing against IT-malfunctions should be defined, along with the methods for coping with the malfunctions by the business entities engaged in critical infrastructures (e.g. procedures for liaising between outsourcers and outsourcing, or methods for resolving troubles in cooperation with each other).

III. Follow-ups

In order to ensure information security in each critical infrastructure sector, it is fundamental for each business entity, with the principle of self-protection, to take responsibility for information assets that the entity controls over, and to take information security measures suitable for their respective corporate structures and information system types. However, examples of recent IT-malfunctions show the necessity of further ensuring the effectiveness of measures, including the management of regulations in an appropriate manner.

Therefore, the follow-ups below shall be conducted to promote information security measures.

(1) Reviewing the Principles

- The Cabinet Secretariat shall review the Principles annually or at optimal timings as required.

- Being well-informed of the status of the occurrence of regular IT-malfunction incidents, the Cabinet Secretariat shall analyze and examine cross-sectoral issues common to critical infrastructure sectors, and develop the results into basic reference materials to amend the Principles.
- The status of interdependence among critical infrastructures and relevant risk information are considered important in examining measures for ensuring business continuity by the business entities. Therefore, if the Cabinet Secretariat implements an analysis of interdependence in cooperation with the presiding Ministries, Agencies of the relevant critical infrastructures, and business entities, results can be provided as basic reference materials used for reviewing the Principles and the "Safety Standards, Guidelines, etc." in each critical infrastructure sector.

(2) Continuous inspection of "Safety Standards, Guidelines, etc."

The following inspections shall be done to keep the "Safety Standards, Guidelines, etc." continuously relevant.

1) Reviewing "Safety Standards, Guidelines, etc."

The "Safety Standards, Guidelines, etc." should be reviewed on an as-need basis corresponding to the environmental changes surrounding information security. Therefore, the following entities shall promote efforts based on their respective roles.

- **Cabinet Secretariat**
  - The Cabinet Secretariat shall follow the status of the formulation of the "Safety Standards, Guidelines, etc.," in cooperation with the presiding Ministries and Agencies of the relevant critical infrastructures.
  - On an ongoing basis, the Cabinet Secretariat shall provide the presiding Ministries and Agencies of the relevant critical infrastructures with reference materials and information required to review the "Safety Standards, Guidelines, etc."

- **The presiding Ministries and Agencies of the relevant critical infrastructures and the business entities engaged in critical infrastructures**
  - The presiding Ministries and Agencies of the relevant critical infrastructures and the business entities engaged in critical infrastructures shall work together to review the "Safety Standards, Guidelines, etc." as needed to keep it suitable to its purpose.
  - When the presiding Ministries and Agencies and the business entities formulate or review the "Safety Standards, Guidelines, etc." they should work together so that the

business entities may consider their own safety standards in compliance with the "Safety Standards, Guidelines, etc." and check the effectiveness of each measure more easily. Specifically, the presiding Ministries and Agencies and the business entities shall consider defining auditing based on evaluation standards set in compliance with international standards and corresponding to the characteristics of each critical infrastructure sector in the "Safety Standards, Guidelines, etc."

- The presiding Ministries and Agencies shall work together with the business entities to be aware of the status of occurrence of IT-malfunctions in each critical infrastructure sector, and to consider the items to be included in the "Safety Standards, Guidelines, etc." in each sector.

2) Assessing the status of compliance with "Safety Standards, Guidelines, etc."

In order to assess their compliance with the "Safety Standards, Guidelines, etc." business entities engaged in critical infrastructures shall inspect, by themselves, the status of the implementation of information security measures on a regular basis, and improve the measures as needed. In addition, from the viewpoint of ensuring the effectiveness of each measure, they shall implement exercise and training as needed in cooperation with the presiding Ministries and Agencies of the relevant critical infrastructures.