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

February 2, 2006
Revised on June 14, 2007
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 against IT-malfunction[1] in critical infrastructures[2] need to be immediately 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 without interruption in order to meet national expectations.

However, effects of the information security measures are not easily quantified, it is important for the business entities engaged in critical infrastructures to promote measures to protect critical infrastructures from IT-malfunction so that it will not have a significant impact on people's social lives and economic activities while concurrently verifying by themselves if the concerned measures implemented are enough to protect the business entities and if the business entities enforce enough measures.

Hence, each business sector should clarify the standards for necessary or desired level of information security measures according to the characteristic of their business in the form of

[1] Critical 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.

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

[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".

the "Safety Standards, Guidelines, etc." Then with a voluntary effort driven by the awareness that they are responsible for operating critical infrastructures, each business entity should make efforts to comply with the "Safety Standards, Guidelines, etc." and should also examine by themselves if they meet the requirements of the Guidelines.

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, it is necessary to clearly define what measures should be taken up to what level as a document 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

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

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

Therefore, the Principles shall list items that are desired to be implemented, not only from the point of view of countermeasures against cyber terrorism but also by taking both various events that may affect providing services such as disasters, unintentional factors, and security measures for control systems that are a basis for providing critical infrastructure-related services, and countermeasures against information leakage that will cause new threats and loss of people's trust into consideration..

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 target threats assuming IT-malfunctions that are highly possible to occur listed below based on the consideration of 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

[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.

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.

In the case that disclosure of these items may increase threats to the public, it is also desirable to clearly state that concerned items are classified and why these items should not be disclosed.

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.”

In order for critical infrastructure sectors to ensure the implementation of measures against IT malfunctions, which may impede the provision of services, it shall be specified that compliance with the “Safety Standards, Guidelines, etc.” is required or desirable.

When specifying such a requirement, characteristics of each critical infrastructure sector should be considered.

(2) Target scope and assumed threats

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

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

In order to avoid uncertainty with regard to the entitiy that should 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 in accordance with the importance of the information system and information itself, as well as the status of their 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 necessary resources should also be ensured.

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 prepared resources.

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

For establishing organizations/frameworks and ensuring resources, necessary measures include basic/long-term efforts to develop and educate human resources engaged in information security, as well as specific actions necessary to ensure the effectiveness of information security measures such as providing a rule to prohibit people in specific positions from serving two or more positions concurrently, dealing with violations of the rule, defining exceptional measures, and implementing self-checks/audits.

ii) Measures with regard to information

When the business entities engaged in critical infrastructures develop information security measures, they should determine the subject 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.

[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 quality of project and promote business improvement activities on an ongoing basis.

iii) Measures based on the clarification of security requirements

With regard to the information security measures that business entities engaged in critical infrastructures should take, security functions such as access control to be adopted according to the importance of the information system should be presented from the perspective of maintaining confidentiality, integrity, and availability. In addition, security requirements should be defined to avoid threats such as security holes, malicious programs, and DoS attacks, and appropriate measures to be taken should also be provided for information systems.

a) Requirements for ensuring 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, authorization control, audit trails, load balancing, and redundancy.

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

At present, 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 that correspond to the clarified information security requirements should be defined for each installation and system according to the lifecycle.[7]

It is also important to define security measures for individual event that is considered to be implemented, such as restriction of information processing outside the organization and prevention of actions outside the organization which may diminish information security level. It is also important to consider designs for ensuring processing performance and measures for ensuring the quality of systems.

Moreover, consideration of introducing codes and products evaluated objectively should be deliberated to promote building secure information systems.

[7] It is important to understand that IT has been more widely applied and dependence to IT has become more pervasive, advanced and black boxed (dependence on IT itself has become unrecognizable, or even though dependence is evidently recognized, appropriate measures cannot be taken due to insufficient understanding of technologies and know-how).

a) Facilities and the environment

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

b) Computers

Security measures should be provided at the time of installation, operation, and termination of operation of computers.

c) Application software

Security measures should be provided at the time of introduction, operation, and termination of operation of application software.

d) Communication lines and equipments

Security measures should be provided from construction, operation to termination or suspension of operation of communication lines and equipments.

2) Three prioritized items

i) Measures for ensuring business continuity from the point of view of IT-malfunctions

Critical infrastructures are basis that support people’s lives and social/economic activities in Japan. Therefore, in the case of a large IT-malfunction in critical infrastructures, it is anticipated that there will be significant effect in various fields.

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

a) Implementation of individual measures to ensure business continuity

Security measures should be provided to proactively prevent IT-malfunctions, to detect the occurrence of IT-malfunctions at an early stage, and to ensure prevention of expansion of suffering and rapid restoration 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 types of IT malfunctions, which are highly likely to occur, into consideration, and after the formulation, reviews should be done properly and the original measures should be improved as needed.

ii) Measures for preventing information leakage

Recently, leakage of confidential or critical information has occurred 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 to prevent the outbreak and recurrence of leakage.

Confidential or critical information in critical infrastructure sectors may contain personal information and with regard to personal information leakage of which 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 to be implemented that cope with the leakage of all types of information is available to read.

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 processing information to be protected.

d) Measures against threats from insiders

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

e) Developing measures for responding occurrence of information leakage

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

iii) Measures for ensuring information security when utilizing outsourcing

Recently, leakage of critical information has been occurring in critical infrastructure sectors. Information is leaked not only by the business entities themselves but also by the companies to which operation is outsourced, and, in fact, latter case is often observed.

Ensuring business continuity in critical infrastructure sectors requires the improvement of information security levels in cooperation with the companies to which operation is outsourced and it is desirable to define measures ensuring that the business entities engaged in critical infrastructures ensure information security within companies to which operation is outsourced.

a) **Frameworks for managing companies** to which operation **is outsourced**

It is necessary to clarify the scope of operation that can be outsourced, and to indicate the standards for selecting companies to which operation is outsourced, information security measures to be taken by outsourced companies, and methods by which entities engaged in critical infrastructures manage outsourced companies. These matters should be considered with reference to previous efforts that was made based on international standards.

b) Thorough implementation of measures for ensuring information security when enforcing outsourcing

Clarification of responsibilities of both signers and the conclusion of an agreement between them should be clearly identified, by signing a basic contract and incorporating contract provisions concerning enhanced measures for preventing information leakage, based on the detail of outsourced business and according to the importance of the information.

c) Developing measures for coping with IT-malfunctions

Measures to be taken by outsourced companies in the case of IT-malfunctions occurrence should be defined, along with the methods for coping with IT-malfunctions by the business entities engaged in critical infrastructures (e.g. procedures for liaising between outsourced companies and outsourcing companies, 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 types of information systems. However, examples of recent IT-malfunctions show the necessity of further ensuring the effectiveness of measures, including appropriate operation of regulations.

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

(1) Reviewing the Principles

- The Cabinet Secretariat shall review the Principles annually and 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 each critical infrastructure sector, and prepare as basic reference materials to revise the Principles.
- The status of interdependence among critical infrastructures and relevant risk information are considered to be 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 contents of “Safety Standards, Guidelines, etc.” continuously appropriate.

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 in reviewing the "Safety Standards, Guidelines, etc." as needed to keep it's contents appropriate.
  - When the presiding Ministries and Agencies and the business entities formulate or revise 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 easily. Specifically, the presiding Ministries and Agencies and the business entities shall consider clearly describing as to auditing in accordance with international standards and based on evaluation standards that is configured 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 understand the status of IT malfunction occurrence in each critical infrastructure sector and to consider the items to be included in the "Safety Standards, Guidelines, etc." in each sector in light of the development status of the "Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR)."

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

In order to assess the degree of 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 drill as needed in cooperation with the presiding Ministries and Agencies of the relevant critical infrastructures.