Guidelines
for
IT Security Policy

(Provisional translation)

July 18, 2000

Decisions Made by IT Security Promotion Committee

Contents

I. Background

An increasing number of activities in industrial and government circles have come to depend on information systems in recent years, thus accelerating the evolution of information and network societies. The Information Technology (IT) Revolution that represents these trends is expected to help introduce the practice of electronic commerce, and implementation of the "electronic government", where approval and applications for authorization are accepted online by electronic means. We understand, however, that a big prerequisite lies with the implementation of such electronic transactions for various activities. That is, the guarantee of high levels of information security to gain great reliance from users.

The IT Revolution that involves the circulation of multitudes of information at tremendous speeds contributes to the formation of a borderless society. This also means information systems become more vulnerable to attacks from intruders known as hackers[1]. Hackers steal into target systems, via a network from outside, and tamper, extract, or destroy data inside or even crash the systems, or totally prevent their use. Actually, a number of incidents are being reported, including unauthorized access to systems by hackers, expansion of computer viruses, and many others related to information security.

Another problem that we cannot ignore lies inside the organization. As a general trend, individual employees are working on their own personal computers connected directly to the Internet. They can intentionally disclose the information they handle to the outside, or illegally access other organizations' systems.

A series of attacks on the Web-sites of several government ministries and agencies that occurred in January this year, revealed that the information security measures taken by the Government, were not always sufficient. It is a pressing matter for the Government to establish a strong system that assures security and reliability of information, for the construction of the foundation for the electronic government by fiscal 2003.

The Interagency Director-Generals' Meeting on IT Security[2] decided on the "Action Plan for Information Systems Protection against Cyberthreats" on January 21 this year. The plans detail individual actions to be taken against each specific problem conceivable. One of the actions is the proposal of the Guidelines for IT Security Policy by The IT Security Promotion Committee for each government ministry and agency. The ministries and agencies are to study the proposed guidelines and prepare their information security policies by the coming December, so that it will serve as the basis for integrated and systematic information security measures.

These guidelines are intended to provide a reference for creating the information security policy required for the guarantee of information security at each government ministry and agency. To

[1] The term "hacker" is used in extensive ways. In this guideline, it means computer users who make unauthorized access to computer systems owned by other individuals or organizations.

[2] The conference organized at the Advanced Information and Telecommunication Society Promotion Headquarters, for the enhancement of information security measures both in government and private sectors under a tight partnership among related government organizations.

be specific, they describe the basic concept of information security policies for each government ministry and agency, methods of establishing an information security policy, and maintaining and reviewing that policy.

II. Basic Concept

1. Significance

(1) Necessity of information security policies

Generally, in the conventional way of using information systems for the transaction of most administrative activities, only qualified officers or operators were allowed to access the host computer centrally placed for information processing. Information exchange with external circles as well as reports or announcements were generally made verbally or through documents printed on paper. Today, personal computer users are on a sharp increase in offices. This has created an environment where individual workers are allowed to have their information processed, or even access global networks from their own terminal, to help improve the efficiency of administrative activities and services, to a large extent. The number of personal computer users has explosively increased in society generally. The administrative information system is now within easy reach of PC users, both from inside and outside organizational networks. Implementation of the electronic government will make access to the system much easier.

Basically, simplex security measures, which control access to the information system, and to the data inside, would work as long as the source of access is limited to qualified persons. But now, the environment around the information system has changed greatly through the extensive use of general-purpose operating systems and distributed processing, together with development of the IT, and efforts made toward implementation of the electronic government. In addition, access to the system from general people has been made much easier. Expansion of the sources of access to the system also reveals the vulnerability of information systems to unauthorized access. Consequently, the conventional security management system now cannot afford to provide sufficient security, with its physical or technical security measures alone, to protect today's sophisticated networking information systems. The expansion of networking and growth in the number of portable remote terminals, that could encourage unauthorized access, could be negative factors for the systems that make them unstable. We should understand, however, these negative factors can be turned to positive ones, or benefits, if information security is afforded, by managing them appropriately. Sufficient information security has to be provided in the government for stream-lined information exchange with private organizations or foreign countries, based on mutual confidence.

Organizations should set up an integrated information security policy, and have it documented to enhance the sense of security among their staff members, thus preventing any information from being used at the personal discretion of those who handle it.

(2) Characteristics of information security

IT evolves so rapidly that the best information security measure employed at one time may not remain the best for long. Continuity is not guaranteed for any hardware or software product that represents the best information security measure at the time of installation. We should understand that information security measures are not complete by simply drawing an information security policy based on these guidelines, but they need constant attention after they are drawn.

The information security policy should also provide a system for constant information collection and security. The policy should be highly comprehensive including appropriate directions, not only about "how an information system should be protected", but also about "what actions should be taken when attacked."

Also required is that the information security policy and the regulations of their implementation, are reviewed periodically. This is an important procedure to check for the presence of any new menaces to the information assets owned by the government ministries and agencies, and for changes to their environment, so that continued measures can be taken. In consideration of rapid advances of information security technologies and hackers' skills that are increasingly becoming more sophisticated, more frequent reviews are important.

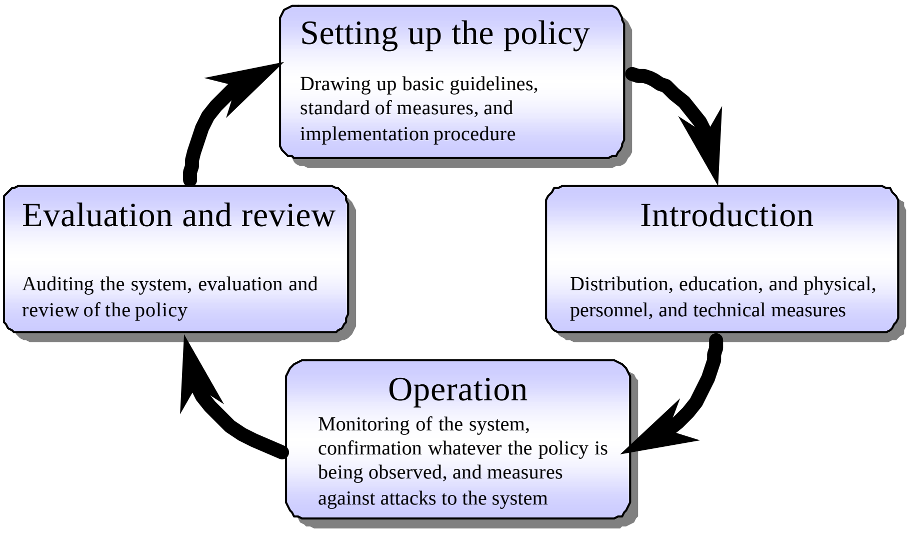

Setting up the policy
Drawing up basic guidelines, standard of measures, and implementation procedure
Introduction
Distribution, education, and physical, personnel, and technical measures
Operation
Monitoring of the system, confirmation whatever the policy is being observed, and measures against attacks to the system
Evaluation and review
Auditing the system, evaluation and review of the policy

Fig. 1 Cycle for the implementation of the information security policy

2. Government's Basic Concept of Information Security

As the social economy is going more electronic, spurred by the rapid expansion of the number of Internet users, and the trend toward electronic commerce, the demand for reducing people's work load as to making applications, notifications, and other procedures, is on an explicit increase. Expectations are high for more active communication between the administration and people. The administration environment about information is about to change rapidly. "Basic Guidelines on the Promotion of an Advanced Information and Telecommunications Society" (decided by the Advanced Information and Telecommunications Society Promotion Headquarters on November 9, 1998) aim at the implementation of a highly sophisticated information administration, or the electronic government, at the turn of the 21st century, to follow up the environment change. This means a transfer from information management using the medium paper, to security controlled electronic information management, by the positive use of information communication networks.

The government's information system connected to networks, however, is constantly exposed to the danger of being a victim of wire-tapping, unauthorized access, destruction, tampering, and other malicious actions. The government should keep providing correct information and stabilized administrative services to the people, and maintain security of the information designated as non-disclosure information, including an individual's private information under the Information Disclosure Law (Law Concerning Access to Information held by Administrative Organizations).

Based on the understanding of the matters described thus far, the security levels throughout the government should be raised in accordance with the following basic considerations:

(1) Individual ministries and agencies[3] of the government should draw-up an information security policy based on these guidelines for promoting integrated and systematic measures for security. The ministries and agencies should take the necessary actions required, in sequence, with the goal of attaining a security level appropriate for the basis of the electronic government.

The implementation of information security, aimed at by these guidelines, assumes that information, in the form of documents and other media, is appropriately managed. The ministries and agencies should provide necessary measures in this respect to attain an extremely high level of security.

(2) The ministries and agencies should stand firm on these guidelines, and make every effort to raise the information security levels at their local bureaus (Regional bureaus and departments) or semi governmental organizations.

(3) The Cabinet Secretariat (Cabinet Office) should establish a cooperative system, or enhance the system, when it exists, within the government for the solution of various problems common to the ministries and agencies. The problems may include urgent actions in response to unauthorized access, or the proliferation of computer viruses, as well as the education of talented personnel or research and development, for raising the level of security throughout the government.

(4) The ministries and agencies should have access administrators implement appropriate preventive measures against unauthorized access in compliance with the Unauthorized Computer Access Law. This is to prevent government information systems from being utilized for attacks on other information systems.

(5) Cooperation should be tightened between the state and the private sector, through enhanced information exchanges, in order to upgrade the security level of Japan's information communication infrastructure.

(6) The ministries and agencies should evaluate the current information security policy periodically and update it if necessary. They should study about the necessity of change at least one year after the policy was formulated.

[3] The Cabinet Secretariat, Cabinet Legislation Bureau, Prime Minister’s Office, and Fair Trade Commission are included.

The Cabinet Secretariat (Cabinet Office), understanding the whole picture of the implementation status of the information security policy at each ministry and agency, technologies expected in the future, conceivable threats, and other factors, should repeat evaluation and review continually.

3. Definitions

This section provides definitions of the terms that appear in these guidelines.

○ Information security
The protection of confidentiality, integrity, and availability of information assets[4]

○ Information assets
A generic name of information and the mechanism that manages information (including materials for information systems and system development, operation, and maintenance)

○ Information system
A system consisting of hardware, software, network, and recording media, that is installed in an organization for business processing

○ Information security policy (referred to as the Policy hereafter)
An integrating and systematic collection of measures for protecting the security of information assets possessed by the government ministries and agencies. It documents what types of information assets should be protected from what types of threats and how. In addition to this basic concept, the policy includes regulations about the system, organization, and operation of the information system for the protection of information security. The policy consists of the basic guidelines on information security and the standard for information security measures.

○ Guidelines for IT security policy (referred to as the guidelines hereafter)
The guidelines are part of the basic guidelines on information security for the entire government. The guidelines work as a reference manual for the ministries and agencies in drawing-up the Policy and indicates the minimum measures that each ministry and agency should provide.

[4] As defined in the standard specified by ISO (ISO 7498-2:1989)

Confidentiality: the quality of a system that ensures only the qualified persons are permitted to access the information inside
Integrity: the quality of data protected from alteration, faulty processing, and destruction or loss
Availability: the degree to which a system is ready to provide necessary information to a qualified person

(For reference)
In addition to confidentiality, integrity, and availability, ISO/IEC JTC 1/SC 27 provides definition of the following three terms that do not appear in this guideline.

Authenticity: the guarantee that the identity of a user, process, system and information, or resources, are true to their respective assertion.
Accountability: the guarantee that an action done by a subject permits a path that leads only to that subject to be traced
Reliability: the ability to provide a result that matches an intended action

○ The basic guidelines on information security (referred to as the basic course hereafter)
The basic concept of information security measures for the government ministries and agencies, detailing how and why they should protect what information assets from what dangers, to indicate their general attitude toward information security.

○ Standards of information security measures (referred to as the standard of measures hereafter)
The standards of actions and judgement to be observed to maintain information security, as specified by the basic guidelines, indicating what should be done to implement the basic guidelines.

○ Implementation procedure of information security
The procedure that indicates how the actions specified in the standard of measures, although not included in the Policy, should be performed in actual information systems or in business.

4. Target of Application

All pieces of information have to be classified according to their level of importance, so that appropriate measures can be provided for each level. Information related to the information system requires special attention different to that of the management of conventional information where paper is the major medium. The Policy has to be provided so that the document management, required of each ministry and agency, will also be implemented in the information system. It should be noted, however, that more appropriate management is required against attacks on information assets of the ministries and agencies from hackers.

The information system consists of hardware, software, data in the recording medium as well as other information, including documents like system configuration diagrams and the like. Out of these components, the target of the policy provided by the ministries and agencies, is the information electromagnetically recorded in the information system, and the operator who handles that information. Therefore, the information that comprises the information assets refers to the electromagnetically recorded information hereafter.

Generally, one integrated policy is drawn-up, which is implemented with procedures provided by individual departments. If the form of the business of a particular department requires that the policy be divided, it can be separated as needed.

Now, the number of documents that can be printed from the electromagnetic medium has drastically increased, making it easy to get multitudes of copies of the same document. Within such an environment, if any problems are found as to the conventional document management during the stage of policy making, appropriate consideration should be given to the management method.

(Example)

Target	Examples
Information system	Computer machine, basic software, application software, network, communication equipment, recording medium, system configuration diagrams, etc.
Information recorded in the system	Access log, electromagnetically recorded documents including diagrams
Personnel who handle the information	Personnel including regular workers and part time workers, temporary workers, consignees, etc.

5. Policy Disclosure

Disclosure or non-disclosure of information will be determined based on the Information Disclosure Law after it is enforced, although, the final decision is up to the judgement of the relevant ministry or agency. Generally, security problems may arise if all information is disclosed. The scope of disclosure should be determined with careful consideration.

It is important to make public that certain measures are being taken by individual ministries and agencies, as a means to indicate that the ministries and agencies are to deal with the problem. Thus it is desirable that information be made as public as possible.

6. Considerations about Policy

(1) Obtaining a clear picture of the basic guidelines under which the information security is maintained.

The information assets to be protected from the dangers they are exposed to (wire tapping, unauthorized access, and destruction, tampering, extraction and leakage of data, DoS attack, and other malicious actions) should be specified. Individual information assets should be classified according to their risk levels with consideration given to confidentiality and the environment of their use. The resulting classes of information associated with a specific degree of risk will provide a basis for working out necessary information security measures.

A system for providing information security measures should be established. It should be noted that a number of persons could be involved in the operation of an information system, including a business officer, a system administrator, and users of the system. The responsibility and authority of each person must be made known, so that appropriate information security measures will be provided within the organization.

(2) Attention should be paid to the following for continued maintenance of the policy and its review.

○ Only a policy that is introduced and maintained appropriately makes sense. Others are virtually the same as policies that were not established.

○ The Policy should be formulated with the aim of providing sufficient information security for the implementation of the electronic government whose basis is to be constructed in fiscal 2003. To provide too sophisticated a policy can make its operation difficult. The Policy should be formulated and maintained in accordance with the actual conditions. It can be reviewed, based on the application states for completion in fiscal 2003.

III. Guidelines for Information Security Policy

1. Positioning and Basic Structure of the Security Policy

The system of the Information Security Policy has a hierarchical structure as shown in Fig.2.

At the apex is "the Government's basic concepts of information security," which illustrates how the Government, as a whole, feels about the measures for information security.

The basic concepts are followed by the "basic guidelines (of each ministry and agency)," "standard of measures (of each ministry and agency)," and "implementation procedure (of each ministry and agency)" in this order. The "Information Security Policy," or the Policy, in these Guidelines refers to the "basic guidelines (of each ministry and agency)" and "standard of measures (of each ministry and agency)", and does not include the "implementation procedure (of each ministry and agency)." The "implementation procedure" covers those procedures provided in documents, and usage regulations - some earlier documents and regulations may include items about the standard of measures - concerning information systems published thus far, as well as those newly required according to the policy establishment this time (for example, emergency organization and operation of the monitoring system). For establishing the Policy from the high-order basic guidelines, the existing regulations should be reviewed.

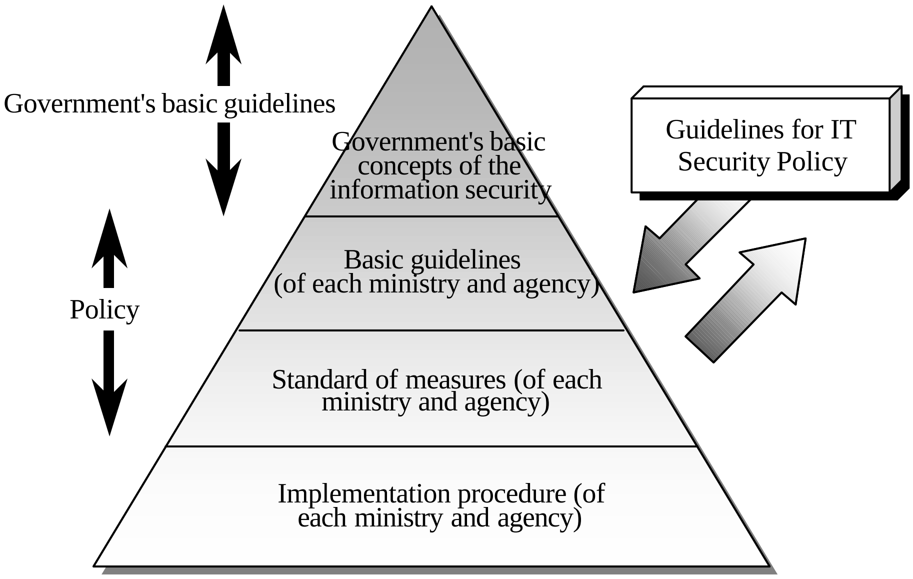

Government's basic guidelines
Policy
Government's basic concepts of the information security
Basic guidelines (of each ministry and agency)
Standard of measures (of each ministry and agency)
Implementation procedure (of each ministry and agency)
Guidelines for IT Security Policy

Fig.2 Positioning of the Policy

2. Procedure for Setting up the Policy

This section describes the procedure for setting up the Policy and the matters to be decided for the Policy.

(1) Outline of the procedure

As shown in Fig. 3, the Policy shall be set up according to the steps of: ① establishing the organization and system for setting up the Policy, ② mapping the basic guidelines under such an organization and system, ③ analyzing the risks, ④ formulating the standard of measures, and ⑤ deciding the Policy formally in each ministry and agency.

Each ministry and agency shall ⑥ formulate an implementation procedure to rationalize the matters set forth in the standard for countermeasures based on its specific Policy.

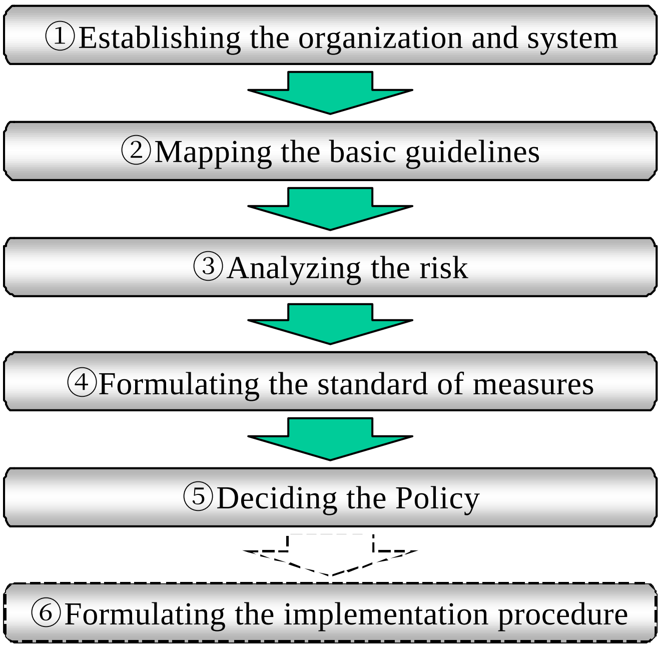

①Establishing the organization and system
②Mapping the basic guidelines
③Analyzing the risk
④Formulating the standard of measures
⑤Deciding the Policy
⑥Formulating the implementation procedure

Fig.3 Outline of Policy setup procedure

(2) Organization and system for setting up the Policy

For setting up the Policy, an organization needs to be established that is formed by chiefs of concerned departments and bureaus, administrators of information systems, persons who have technical knowledge and expertise about information security and other people. By establishing this organization (hereafter called the “Information Security Committee” in these Guidelines), the commitment of the organization executives to policy making and the responsibility of each member are made clear. To attain this object, the purposes, authorities, name, operation, members, etc. of the Information Security Committee shall be defined in the Policy. Although it is considered that the concerned persons in all departments and bureaus will take part in the Policy, because it deals with various issues about information, the key members of the Committee should include the following persons concerned.

- Persons in information system related sections (such as LAN management sections)
- Technical experts (experts with technical knowledge inside and outside the Government)
- Persons in audit related sections (such as sections conducting policy evaluation, internal audit and general affairs section of secretariat

- Persons in document related sections
- Persons in personnel related sections
- Persons in accounting related sections
- Persons in public relations related sections
- Persons in government building management sections

In the course of setting up the Policy, candidates for information security personnel in each department and section should be incorporated into the organization. In addition, it is important that an environment should be created which enables the Policy to be understood by the staff, by hearing their opinions and explaining problems to them appropriately.

Some of the Policy formulating work can be consigned to a subordinate group (Policy formulating group) with the approval of the Information Security Group. In the case of need, outside people can join the group. For easy operation of the Policy formulating group, the executives should organize the group formally, using official appointments, so that the people of the ministries and agencies can recognize that the work of the group is based on an order of the executives.

(Example)

Information Security Committee

This Committee is formed by representatives of the following organizations:

- Chairman Chief secretary
- Information System Section
- General Affairs Section of Secretariat
- Documentation Section of Secretariat
- Secretary Section
- Accounting Section
- Public Relations Section

Miscellaneous duties of the Committee are assumed by the Information System Section.

In addition, as the persons who represent the interests of each department and bureau, staff of the section of each bureau, and the section in charge of the A system (A Section), shall participate in formulating the tasks of the Policy.

Staff of the Policy Formulating Work Group (Work Group on IT security policy) shall coordinate with the various departments and bureaus in the ministries and agencies, and promote an understanding of the Policy among those departments and bureaus.

(3) Mapping the basic guidelines

It is required as the basic guidelines that the formulation of the basic policies should take countermeasures to guarantee the information security of the information system of the ministry and agency.

These basic guidelines shall indicate each ministry and agency's basic concepts for information security, including the purpose, target, etc. of the information security measures.

It also includes the definitions of terminology required to understand the Policy.

Note that the basic guidelines should not be updated frequently because they determine the basic direction concerning information security.

(4) Analyzing the risk

① General

Identifying the information assets to be protected, and evaluating the risk to those assets, is called risk analysis. Although there are various methods for risk analysis, we would like to outline the following procedure for specific risk analysis that is our concern.

(a) Look over the information assets held by each ministry and agency, classify them by importance and determine the level of required security for each asset.

(b) Investigate the threats surrounding the information assets of each ministry and agency, determine the scale of the risk, based on the frequency of threat occurrence, and the amount of damage caused by the threat.
Note that the scale of risk generally refers to the product of frequency of threat occurrence, and the amount of damage caused by the threat.

(c) Formulate the standard countermeasures so that the scale of risk falls below the level of required security, and implement risk management as appropriate.

When changes are made to the information assets, or if the risk to the information assets is varied, risk analysis is made again for the relevant information assets, and the Policy is reviewed as required. Also in respect to regular review of the Policy, the work should begin with risk analysis. In addition, if vulnerability is found in any information assets, action should be promptly taken if necessary.

Although the materials describing the results of risk analysis shall be saved as the basic materials for setting up the Policy, their saving should be placed under strict management because they contain analysis of system vulnerability.

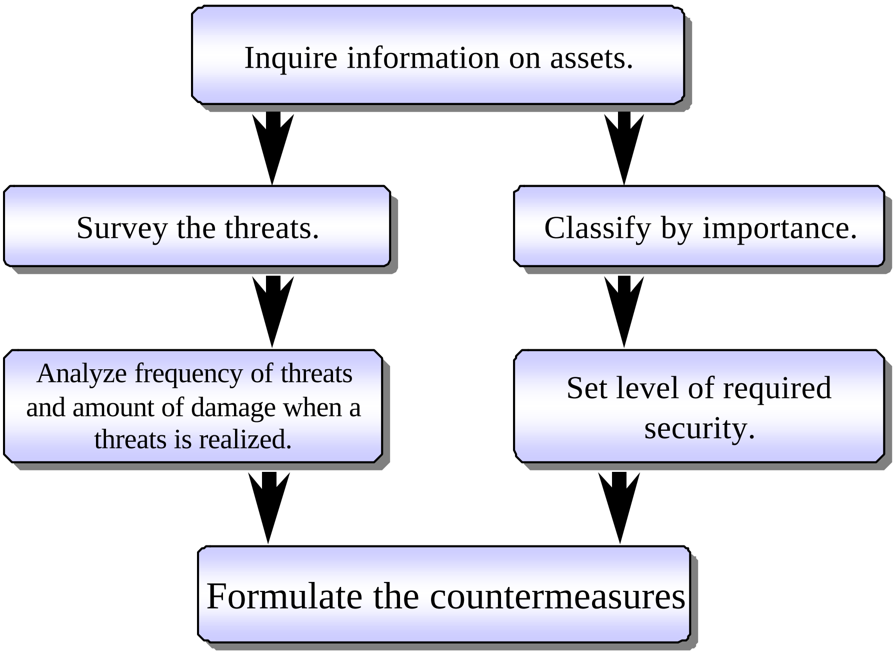

Inquire information on assets.
Survey the threats.
Classify by importance.
Analyze frequency of threats and amount of damage when a threats is realized.
Set level of required security.
Formulate the countermeasures

Fig. 4 Flow of risk analysis

② Inquiry to information assets

To identify the information assets to be protected, inquiries should be made as to where the assets are located, by whom they are managed, and how they are dealt with.

The following is an example of a questionnaire showing specific inquiry items. Besides such a questionnaire, materials that describe the results of risk analysis should also be prepared.

(Example)

Questionnaire concerning information assets (Inventory concerning information assets)	
Name of information asset	
Use	
Administrator	
User (access right)	
Place of saved (installation)	
Term of saved (installation)	
Importance	I, II, III, IV Confidentiality [I, II, III, IV] Integrity [I, II, III, IV] Availability [I, II, III, IV]

③ Classification by importance

The inquired information assets are examined for classification in terms of three aspects of importance, or confidentiality, integrity and availability.

This classification provides the standard for deciding how each information asset is handled and protected. The level of required security for each information asset is determined by this standard.

(Three aspects of importance)

(a) Confidentiality: Importance based on the secret contained in the information asset

(b) Integrity: Importance concerning the integrity and accuracy of the information asset

(c) Availability: Importance concerning the availability and continuity of the information asset

(Example)

Degree of importance

I: Violation of security exerts a serious influence on the life, property, and privacy of the nation.

II: Violation of security exerts a serious influence as to the execution of administrative affairs.

III: Violation of security exerts a slight influence on the execution of administrative affairs.

IV: Violation of security exerts little influence.

(Example)

The level of required security based on the importance of information assets (The level is set considering the three aspects of the importance mentioned above.)

Importance I → <u>Level 1 of required security</u>
Importance II → <u>Level 2 of required security</u>
Importance III → <u>Level 3 of required security</u>
Importance IV → <u>Level 4 of required security</u>

④ Risk assessment

Risk assessment shall be performed for all inquiries as to information assets.

(a) Investigations shall be made into threats in the surrounding physical, technical, and human environments.

(Examples of threats)

Physical threats: intrusion, destruction, failure, power stoppage, disaster, etc.

Technical threats: unauthorized access, tapping, computer virus, tampering, deletion, DoS attack, disguise, etc.

Human threats: abusing extraction, misconduct, inappropriate management of passwords, etc.

(b) Magnitude of risks to the threats that each information asset is facing shall be assessed from (a) frequency of the threats and (b) scale of damage when a threat occurs.

Instead of directly examining the frequency of the threats and the scale of damage, the vulnerability of information assets (taken for frequency) and the importance of information assets (taken for scale of damage) can be examined for convenience.

The magnitude of risk shall be examined with all threats to each information asset.

(Example)

(Assessment levels set in phase of frequency and scale of damage)

(a) Frequency of the threat

A: The threat occurs at a considerable frequency. (The vulnerability is very serious.)

B: The threat occurs at times. (The vulnerability is serious.)

C: The threat occurs incidentally. (The vulnerability is slight.)

D: The threat occurs scarcely. (There is little vulnerability.)

(b) Scale of damage when the threat is realized.

There is a method that approximates the scale of damage to the ranking of importance. (This method assumes that the higher the importance is, the greater the damage becomes.) To determine the scale of damage strictly by this method, the three aspects of importance shall be taken into consideration.

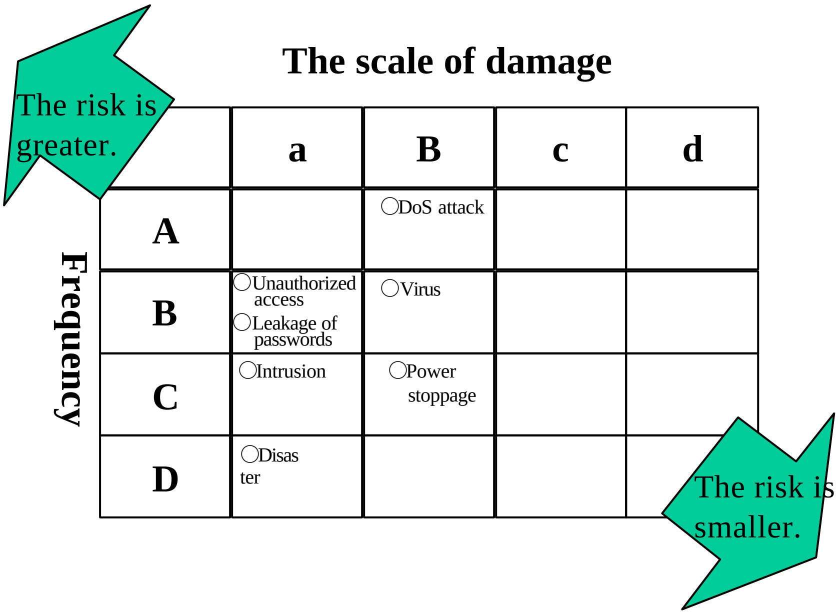
<Scale of damage>

a: The same as importance I.

b: The same as importance II.

c: The same as importance III.

d: The same as importance IV.



	a	B	c	d
A		○DoS attack		
B	○Unauthorized access ○Leakage of passwords	○Virus		
C	○Intrusion	○Power stoppage		
D	○Disaster			

Fig.5 Risk analysis(example)

⑤ Countermeasures against risks

The scale of the risk for each threat to an information asset evaluated by the risk assessment is compared with the level of required security for the standard of information security measures.

When the standard of information security measures is determined, it should aim at satisfying the level of required security by reducing the frequency of threat and the scale of damage. The measures to reduce the frequency of threat and the scale of damage should include those that prevent threats. The measures should also include procedures that guard the information, keep the information from tampering, and enable the information to be used continuously, when damage actually occurred. In addition, prompt recovery in the case of a fault should be taken into consideration.

In formulating measures to attain the level of required security considering the importance of information assets, it is noted that the frequency of threats should become lower, and the damage (or the risk) should become smaller, as the level of required security becomes higher.

For example, the methods of reducing the scale of the risk to the level of required security are divided into the following three types.

(a) Method to reduce the scale of the risk by reducing the scale of the damage, for example, by granting access rights only to those who need to access the information.

(b) Method to reduce the scale of the risk by reducing the frequency of threats, for example, by permitting logins from the console only.

(c) Method to reduce the scale of the risk by reducing both the scale of damage and the frequency of threats, for example, by detecting tampering of information systems.

The measures to be determined specifically should be effective and efficient, paying due consideration to the convenience of users, according to information assets and their threats.

(Example) Examining the standard of measures (unauthorized access)

Results of risk assessment (Frequency of occurrence = B, scale of damage = a)

↓

The standard of measures are examined to reduce the risk of unauthorized access

○ Granting access rights only to those who need to access the information

○ Permitting logins from the console only

○ Introducing correction programs (patches)

○ Monitoring and recording access logs

○ Detecting tampering of information systems

○ Protecting information assets by emergency action

↓

Reduce of risk (Frequency of occurrence = C, scale of damage = c)

(5) Formulating the standard of measures

Individual measures for each information asset, which are obtained as the result of risk assessment, should be organized to formulate the standard of measures.

① Configuration

The standard of measures should be configured as follows:

(i) Organization and system

(ii) Classification and management of information

(a) Management responsibilities for information

(b) Classification and management of information

(iii) Physical security

(iv) Human security

(a) Role, responsibility, and exemption

(b) Education and training

(c) Reporting of incidents and defects

(d) Password management

(e) Employment of part-time and temporary staff, and their employment agreement

(v) Technical security

(a) Management of computers and networks

(b) Access control

(c) Development, implementation and maintenance of systems

(d) Countermeasures against computer viruses

(e) Collection of security information

(vi) Operation

(a) Monitoring of information systems and making sure of policy observation (operation management)

(b) Considerations in operation management

(c) Contingency plan

(d) Operation agreement for consignment to outside contractors

(vii) Compliance of laws

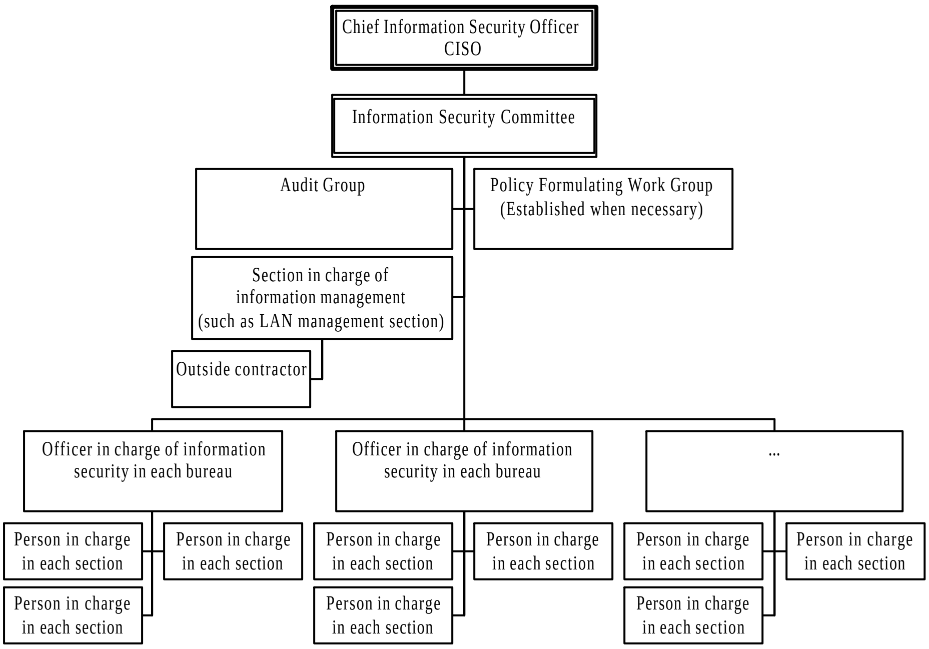
(viii) Action against violation of information security policy

(ix) Evaluation and review

② Organization and system

For the organization and system to maintain information security, it is important that executives should take initiative in promoting the protection of information security. To realize this purpose, it is required that the person who takes the final responsibility for information security (Chief Information Security Officer: CISO[5]) is selected and his / her responsibility and authority are made clear. Specifically, the Information Security Committee, headed by the CISO, should assume the responsibilities for establishing a system that ensures the observation of Policy on a daily basis, investigating and reviewing the improvements (gaps from the real world) at the time of implementation and carrying out of education activities.

[5] Chief Information Security Officer


Chief Information Security Officer
CISO
Information Security Committee
Audit Group
Policy Formulating Work Group
(Established when necessary)
Section in charge of
information management
(such as LAN management section)
Outside contractor
Officer in charge of information security in each bureau
Officer in charge of information security in each bureau
…
Person in charge in each section
Person in charge in each section
Person in charge in each section
Person in charge in each section
Person in charge in each section
Person in charge in each section
Person in charge in each section
Person in charge in each section
Person in charge in each section

* Relationship between the emergency liaison system and the system in ordinary times should be defined clearly.

Fig. 6 Example of organizational chart for information security

③ Classification and management of information

Methods of information management are decided according to the classification of information management used in the risk analysis.

(i) Management responsibility of information

Persons who bear management responsibility are determined for each information item. The responsibilities for both those who manage it and those who use it should be studied, and the responsibilities and roles should be defined for each.

The information administrator, who will take the management responsibility for the documents prepared in that section, should be formally selected for each section. Documents and e-mail messages that are being prepared should be managed properly by individual persons.

(Example)

Each department, bureau, or section should assume managerial responsibility, as the information administrator, for any information it prepares.

Information prepared by Bureau A → General affairs section of Bureau A

Information prepared by Section X, Bureau A → Section X, Bureau A

Information prepared by a ministry → General affairs section of the minister's secretariat (or the section decided as the information administrator)

(ii) Classification and management of information

For the information held by the ministries and agencies, the classification and management are decided, based on the results of the classification of information assets, provided in the risk analysis.

Specifically, provisions should be made, not only for classification of information and indication about the classification of information, but also for the granting of access rights, encryption, management of media, changing or discarding of information, effective period of classification, etc., as methods of information management.

If information that has been classified is copied or transmitted, the reproduced information should also be managed in accordance with its original classification.

(Example)

A Principle

Whether the information held in this ministry should be made public or not is determined by the Information Disclosure Law (Law Concerning Access to Information held by Administrative Organizations).
(For information that is considered improper to make public, such as information concerning the privacy of individuals or information that may create a problem of information security, provisions should be made as required.)

B Indication about the classification of information

For printed matter, displays on monitors, storage media (labels for FD, etc.), and file names, necessary indications of their classification should be made, paying due consideration to measures that prevent third parties from recognizing the importance of information.

C Management of information (determined by the classification)

(a) Granting of access rights and encryption
Access rights should be determined by the classification of the information.
Information that was classified as ‘secret’ should always be encrypted and saved strictly, separate from its encryption key.

(b) Management of media
Secret information storage media (FD, MO, CD-R, DAT, MT, DVD-RAM, etc.) should be saved in places that can be locked.

(c) Management of information change or discard
Changing or discarding of information should be made with the approval of the information administrator. The history data, including the date of when changed or discarded, the name of the person in charge, the contents of the processing should be held. Deletion of secret information should be performed by a method that disables the recovery of deleted information (reformatting of the medium, for example).

④ Physical security

To protect information systems and places where they are installed from unauthorized entry, damage, and disturbance, physical measures such as installation of proper facilities, entry/exit management, and anti-theft measures for PCs in office rooms, should be decided.

To prevent information leakage using mobile communication devices, necessary measures should be studied, paying consideration to the future proliferation of such devices.

(Example)

> For network devices including computers, proper physical measures should be taken in accordance with classification of importance (I, II, III, and IV) used in risk analysis.
>
> I Use of double keys and IC authentication cards, installation of monitor cameras and antimagnetic walls, thorough management of entry/exit, installation of fire-extinguishing facilities and protection of wiring
>
> II securing devices by chains, and protection of wiring
>
> III ...
>
> These devices should be properly managed by the section in charge.

⑤ Human security

Increase of information security does not always go together with an increase of convenience, and may not be easily understood by users. This requires that necessary measures should be decided for human security, so that adequate education can be provided.

(i) Role, responsibility, and exemption

As a part of the “target of application” decided in the basic guidelines, the role and responsibility of each person being targeted, (who assumes the responsibility and role of the executives and staff) should be determined together with their relationship to outside contractors (including the relationship to program developers).

For exemption, necessary provisions for smooth application of the Policy should be determined, including the clause, that the responsibility for information security failure will be discharged, if the person in charge notifies of failure on his or her initiative.

(a) Chief Information Security Officer (CISO)

The CISO should assume authority and responsibility for information security as a whole. It should also have the decision authority concerning important matters on operation.

(b) Officers in charge of information security (executives and other leaders)

Information security officers should be selected in each section, department and bureau. Their duties and responsibilities should include formulating a line of command in their organizations, and collecting and processing opinions of their people. For example, personnel in each section should report a violation against or a problem with the Policy to the officer in charge of information security for advice or direction. The officer in charge should decide whether a violation or problem should be reported to CISO.

(c) System administrator

The system administrator, who carries out daily management and operation functions of an information system, is a necessary part of the system. The authority exercised by the administrator has a great deal of influence on information security. So it is required to clearly define the role and responsibilities of the administrator, and to formulate a mechanism in which the management work is done jointly by several system administrators. This will allow each administrator's work to be checked by others, in order to prevent abuse of their authority.

(d) Staff and other personnel

- Obligation to observe the information security measures

A provision should be set forth that places the staff under an obligation to observe the contents of the Policy and the implementation procedure, (individual manuals will do) in order to have the information security measures function effectively. The staff is also required to give advice when they have questions or opinions about the Policy.

- Management concerning external consignment

When the ministries and agencies consign development and operation management of information systems to outside contractors (including subcontractors), it is recognized that the obligation to observe the Policy and the implementation procedure is imposed on those contractors according to the target of application. Provisions are thus required to have the contractors observe the Policy and the implementation procedure, to provide education for this purpose, and to include a damage compensation clause to the contracts in cases where the Policy or procedure is not observed.

Because the contractors may deal with important information in terms of security, they should pay due consideration to the technical abilities and credibility of their personnel who handle such information.

- Part-time and temporary workers

It is prescribed that part-time and temporary workers should assume responsibility and a role in the manner that is applied to other staff members.

- Miscellaneous

It should be noted that when staff or part-time and temporary workers who work for information security leave the work because of personnel changes or retirement, the information known to the staff or other workers poses a security problem.

(ii) Education and training

Part of implementation of the Policy may be realized automatically by technical actions incorporated in information systems. A greater portion of implementation, however, depends on the decision and activities of the persons in charge and users in the organization. Thus to raise and maintain security consciousness, education and training should be provided, based on a plan so that all people in the organization, including the executives, recognize the importance of information security, and understand and carry out the Policy.

Education and training are important to protect information systems against unauthorized accesses, computer viruses, information leakage by insiders, attacks from the outside, etc.

Specifically, research study meetings, seminars, and other educational activities should be provided. Training programs for new employees should also be provided.

(iii) Reporting of incidents and defects

If a member of the staff becomes aware of an incident concerning information security or a defect of an information system, s/he should promptly report it to the information security officer, in order to receive directions, without attempting to solve the incident or defect themselves. A provision should be made, concerning the obligation to report incidents and defects and reporting method, to localize the damage of an incident or defect.

(iv) Password management

To prevent unauthorized access, it should be set forth, that all persons who use information systems should manage their passwords strictly. Passwords may be used to control access to networks or to classified documents. It is noted that, not only measures concerning passwords for access control but also measures concerning password management at each terminal or for documents, should be provided.

(Example)

① The password should be kept secret.

② Notes on passwords should not be taken unless the notes are saved securely.

③ If an information system or passwords might be exposed to risk, the passwords should be changed.

④ The password should be of a proper length, and the character string should be a one that cannot be easily associated. (Details are decided in the implementation procedure.)

⑤ Each password should be changed when a predetermined period has elapsed or when the predetermined number of accesses is reached (old password should not be used). The password for the administrator should be changed more frequently.

⑥ Users should not have their passwords used by other users.

⑦ Passwords should not be stored in mobile communication devices.

(v) Employment of part-time and temporary staff and their employment agreement

It is required to have part-time and temporary staff understand the observance of the Policy clearly in terms of information security. In particular, when they need to work with PCs, the access management of those PCs and their authority to the information system, should be defined clearly to prevent unauthorized access by the staff.

Therefore, provisions should be set forth that, for example, the Policy is made known to the part-time and temporary staff and the staff sign a written consent.

⑥ Technical security

(i) Management of computers and networks

Considerations and regulations should be set forth concerning the operation management procedures of information systems, network management, protection of storage media, data exchange with other organizations.

Methods of handling and managing devices should also be determined based on the results of risk analysis.

(Example)

> Information should be managed as follows according to the classification of information assets.
>
> I
>
> - All accesses should be logged and the log data should be held for a predetermined period. Log data should be analyzed regularly for monitoring.
> - When an information system is changed, the contents, necessity and schedule of the change, should be reported to the administrator for approval. Before the changed system is installed on the production machine, the operation of the system should be validated on another machine. For updating, the current state should be stored, so that immediate recovery will be possible. These should be done outside business hours.
> - In order to make it possible to take prompt action in an emergency, spare systems should be provided for the systems that are identified as an especially important system by the Information Security Committee.
> - The emergency spare systems should be validated at least once every quarter.
> - Education for managers should be provided regularly.
> - Information systems should be backed up regularly.
>
> II
>
> - For operations that the Information Security Committee identify as those that might seriously effect information systems, all accesses should be logged and the log data should be held for a predetermined period.
> - When an information system is changed, the contents, necessity and schedule of the change should be reported to the administrator. If the administrator considers that the change would seriously effect information systems, the most important procedure should be changed outside business hours after preparing for recovery from the current state If the influence to the information system

is considered to be trivial, the change is made under instructions from the administrator.

- Information systems should be backed up regularly.

III

- When an information system is connected to the network, necessary items should be reported to the administrator according to the Instruction Manual for approval of the connection created by the administrator.

The configuration of each information system should be defined in the corresponding implementation procedure manual.

IV

- Handling can be made freely. No network connection should be made without approval.

The following are examples of regulations concerning the use of information systems.

(Example)

Regulations concerning the use of information systems

○ Prohibition of non-business use of information systems

Use of an information system or network resource is permitted only when it is made for business purposes. Access to information systems, use of mail addresses, and access to the Internet for non-business purposes, are not allowed.

○ Prohibition of extraction of business data

The staff should not bring class I business data out of the ministry or agency. The staff should not take media on which personally owned data is stored to a place where class information assets are installed. This regulation does not apply when the chief of an organization to which the staff member belongs (such as a section chief or room chief) gave permission to that effect.

For example, the following activities require permission: – bringing the information stored in a mobile terminal or storage medium out of the ministry or agency, taking personal information into an office where the above information is installed, transferring personal data over a network (sending and receiving data to and from the address of a private person by e-mail, and so forth).

○ Prohibition of installation of unauthorized software

The staff should not install software that is not authorized by the section of information system management on their PCs given to them from the ministry or agency. Among pieces of information strictly prohibited by that section are monitoring software for eavesdropping the information over the network, security-related software for scanning the network status, and hacking software.

Software to increase the efficiency of work can be used by permission of the officer in charge of information security.

○ Prohibition of change of device configuration

The staff should not make any device addition or change to their PCs given to them from the ministry or agency. The addition of a modem or other similar devices to connect to other environments (such as the Internet) over a network or making a mechanism to allow access from outside the ministry or agency should be prohibited

(ii) Access control

Access to information should be permitted based on the business requirements. Access permission should include provisions about the authority and responsibility of the users. The password management procedure on the system administrator's side, and the authority of the system administrator, should also be defined. For important information systems, specific access control for individual systems (access control using special personal authentication, for example) should be defined. The standard of permitting connection from outside users, (or connection from a mobile terminal) and requirements for accessing information and information systems, should also be defined.

In addition, for connection from local bureaus (Regional bureaus and departments) via leased lines, measures such as access control to increase security should be taken depending on the conditions of those lines.

(Example)

○ Registration of users
Formal procedures for registering users or canceling user registration should be used to authorize or cancel access rights to information systems.

○ Considerations for logging in and logging out
(The procedure for login and logout should be defined in the implementation procedure.)

○ Limitation of automatic mail transfer

○ Granting access rights to servers

(iii) Development, implementation and maintenance of systems

When an information system is developed, introduced, or updated, risk analysis should be made according to the Policy to define the necessary items for taking proper information security measures. Security items for the consignee of system development should also be defined.

When new devices, software, storage media, or services are introduced for the information system, they should be checked in advance for any failure or defect that might compromise the security of the system. In addition, their specifications should be dealt with carefully.

If a device is discarded or repaired, an appropriate measure should be taken to prevent leakage of the information in the device. For example, if a hard disk drive is to be discarded, the contents should be completely deleted before it is discarded.

(Example)

> Obligation to submit the source code, regulation of reconsignment contracts, conformity with ISO15408 standard, checking for security hole, etc.

Regulations concerning a monitoring system and the correction of information systems should be prescribed to ensure security during maintenance.

(Example)

> A 24-hour monitoring system for information systems, guidelines for installing correction programs (patch programs), time of installing such programs, etc.

(iv) Countermeasures against computer viruses

Preparation of the system to cope with computer viruses, regulations to be observed by the staff and others, should be set forth as the countermeasures against viruses. The actions to be taken when a computer virus is found are defined as an action against an intrusion into an information system.

(Example)

> ① Installation of unauthorized software should be prohibited. (This relates to compliance of laws.)
>
> ② When to receive data files or software files from an external network, anti-virus software should be executed at both the server and terminal.
>
> ③ The vaccine program should be updated to the latest version, and the virus information should be updated frequently at both the server and terminal.
>
> ④ The contents of important software, information systems, and information should be checked regularly.

(v) Collection of security information

Because security holes are likely to be found on a daily basis, security information should be corrected regularly. For this purpose, an information collection system, information analysis procedure, and sources of information collection need to be decided. If a serious security hole is found, action should be promptly taken.

⑦ Operation

(i) Monitoring of information systems and making sure of policy observation (operation management)

To ensure the effectiveness of the Policy and to prevent the Policy from being abused by attacks to other information systems via the Internet, constant checking is essential. Specifically, it should be checked through network monitoring, that users of information system are observing the Policy, and if unauthorized access is made to an information system via the Internet. Thus self-checking by each person in the target of policy application and network monitoring by self-monitoring devices, etc. of the information management section should be defined. This helps ensure the observance, the evaluation of the problems, and the coordination of the Policy with the actual conditions.

To implement operation management properly, it is required to formulate an organization that does not impose too much burden on particular persons. The organization is also required to provide a quick action in the case of a failure, and to monitor the system constantly even during the failure.

Acquisition and analysis of the access log should also be defined clearly. The access log should be maintained safely to prevent deletion or tampering of data or other unauthorized operations.

Detailed items (such as retention period of the access log and number of persons in charge of monitoring) should be defined in the implementation procedure.

(ii) Considerations in operation management

Operations of system and security management software, including the browsing of users' e-mail messages, should not violate the privacy of users. Due consideration should be paid to the fact that the security measures may effect the privacy of the staff. From this standpoint, provisions should be made as to the time, conditions, and organization that allow the use of the security procedure.

Desirably, this issue receives the good understanding of users.

(Example)

> The system administrator can only see personal e-mail messages in the presence of the executive in charge or another selected person when the executive has admitted that a problem may occur with information security.

(iii) Contingency plan

Specific actions to be taken when the information security was, or might be violated, should be formulated as a plan of emergency measures.

This plan includes a series of operations to take necessary actions, such as liaison when the information asset was violated, perpetuating the evidence, localizing the damage, and recovering quickly and smoothly from the damage and to take measures for preventing recurrence of security violation.

In particular, measures should be reviewed thoroughly through validation and training, so that the following actions can be conducted easily: – deciding measures based on examination of the cause, identifying the offender, perpetuating the evidence to prepare for receiving legal measures and quick recovery.

In addition, actions are required to prevent the damage from diffusing to the information asset held by you or to outside information assets. If some persons are damaged by the leakage of their information, notice should be promptly given to them.

Close contact should be kept with the police and other agencies concerned if the case in question constitutes an infringement of the Law Concerning Prohibition of Illegal Access to Computer Systems (Unauthorized Computer Access Law).

As well, easy-to-understand emergency manuals for administrators and users should be prepared as an implementation procedure.

○ Items to be included in the plan of emergency measures

(a) Liaison

The place for making contact, person in charge of liaison and communication means

(Example) Person in charge of information summarization (place for making contact), section or department of information asset management, liaison system in the ministry or agency, Branch for IT Security, Cabinet Office for National Security Affairs and Crisis Management, agencies concerned including the policy, and others

(b) Survey of the case

The survey method and survey items to understand the violation case should be decided.

(Example) Classifying the symptoms, identifying the cause, determining the scope of damage or influence, and recording

(c) Coping with the case

Criteria of deciding actions, the person who assumes the responsibility, the person in charge of implementation, implementation procedure, etc. are determined.

(Example) Notification, disconnecting the network, shutting down the information system, obtaining the logs (access log, action log, etc.), recovery, and checking for recurrence

(d) Measure to prevent the recurrence of security violation

The violation case should be surveyed to decide the measure to prevent the recurrence of a security violation.

(Example) Reporting to the information security committee, risk analysis in relation to the case, and formulating the measure to prevent the recurrence of security violation (including evaluation of the Policy)

(iv) Operation agreement for consignment to outside contractors

When the information system is operated by outside consignees, the agreements for consigning the system operation should be defined clearly, and a checking system should be formulated. For example, the organization for system operation should include provisions for the following actions: – when a message to increase attention (Advisory class message) is issued from CERT/CC[6], JPCERT/CC[7], etc., the notification to that effect should be sent to information security section at once. Accesses recorded in the log should be classified according to the degree of risk and accesses requiring attention should be informed immediately to the contractor through the emergency network.

⑧ Compliance of laws

A provision is made about the observance of the related laws. Laws and administrative guidance to be observed should be enumerated so that they are not violated They include the Copyright Act, the Law Concerning Prohibition of Illegal Access to Computer Systems (Unauthorized Computer Access Law), and the Act for Protection of Computer Processed Personal Data held by Administrative Organizations.

⑨ Actions taken against violation of information security policy

The Policy stipulates that the persons who made violation of the Policy and their superior officers can be punished under the National Public Service Law, depending on the seriousness of the violation. This stipulation is included in order to suppress the actions of those who intend to make light of the Policy and the implementation procedure and to maintain the required level of information security.

If any actions that may infringe information security are observed in business, the superior of the officer who made the infringement, should immediately order the person who made the actions to stop using the terminal.

⑩ Assessment and review

It should be provided that assessment and review of the Policy be performed periodically in response to the evaluation of the Policy and information security measures, and to cope with alteration of the information system and emergence of new threats. The Information Security Committee should decide the implementation of assessment and review of the Policy by right of the committee.

[6] CERT® Coordination Center (http://www.cert.org/)

[7] JPCERT/CC (http://www.jpcert.or.jp)

(i) Auditing

Information security of the information system should be audited, and the results should be reflected in the assessment and review of the Policy.

The auditors should be qualified persons with expertise. For fair auditing, auditors who have no direct connection with the system to be audited are desirable.

(ii) Inspection

As for the implementation states of information security measures in accordance with the Policy, questionnaires should be issued to the users, or autonomous inspections should be made. The results should be used when the Policy is updated to a more practical one.

(iii) Updating the Policy

Updating the Policy, as in the case of setting up the Policy, requires a procedure that justifies updating. The assessments by specialists of information security should be utilized at that time, and reference to opinions of the related departments and bureaus is required.

The Policy should define a procedure that includes opinions about the update draft from the related departments and bureaus reflected in the Policy, and provide that the Policy has to be decided by the Information Security Committee.

(6) Decision of the Policy

The set up Policy draft requires a procedure that justifies the draft. The assessments by specialists of information security should be used at that time and reference to the opinions of related departments and bureaus is required.

The Policy should define a procedure to include opinions about the draft from the related departments and bureaus reflected in the Policy, and provide that the Policy has to be decided by the government ministries and agencies.

3. Introduction

(1) Outline of introduction

The Policy should be thoroughly known to the related persons before its operation is started so that the Policy can be positively implemented.

(2) Preparation of implementation procedure

The implementation procedure provides how the contents of the Policy should be put into operation for actual work or in the information system. The implementation procedure is equivalent to a manual that defines what each person who should observe the Policy must do to maintain information security according to the information handled and the work to be done. Therefore, the implementation procedure has to be determined for individual cases when necessary, according to the actual working environment. It should be provided that the existing regulations could be used where applicable.

It shall be allowed that the implementation procedure be set up, updated, and abolished by the relevant departments and bureaus without approval from the Information Security Committee.

(3) Conformity to the Policy

The Information Security Committee has the information security officer verify that the implementation procedure, and what are actually implemented, conform to the Policy before it is put into operation. The Committee collects and studies information about conformity to the Policy and provides appropriate advice or actions for the operation of the Policy in advance.

The officer in charge of information security should verify that the physical, human, and technical information security measures, as well as the emergency action plan and the implementation procedure introduced for all information assets s/he is responsible for, conform to the Policy.

(4) Distribution and briefing

The Information Security Committee distributes prints of the Policy or holds briefing about the Policy to make the Policy known to related personnel. Each department and bureau will be responsible for making the implementation procedure known to related personnel.

It is desirable that the necessary part of the Policy is made known to outside consignees to have them agree to the conformance to the Policy.

The implementation procedure is confidential. The related persons, including outside consignees, should handle the procedure under strict control.

4. Operation

Establishment of organizations or systems, monitoring, actions taken at the time of intrusion, and other measures, should be provided for positive operation of the Policy.

(1) Operation management

Persons in charge of information security in information management sections and the departments and bureaus, (bureaus and departments) should make sure that physical, human and technical information security measures are implemented appropriately under the Information Security Committee.

If a violation of the measures that could cause a serious problem for information security is found, actions should be taken in accordance with a plan of emergency measures.

These actions must be managed with tight control ready for use for the assessment or review of the Policy because they can serve, not only as proof of violation, but as materials for measuring the practicability of the Policy.

(2) Actions taken in case of intrusion

① Training

Training should be performed regularly for smooth implementation of a plan of emergency measures. The results of the training are used for assessment and review of the plan.

② Notes for liaison

The method of liaison should be invulnerable to problems of information security. (Use of e-mail for forwarding sensitive information should be avoided to protect it from eavesdropping.)

It is desirable that more than one communication means be provided around the clock for contacting the persons in charge of information security.

③ Notes for investigation

Investigation must not cause liaison any delay.

④ Notes for taking actions

The scope of a person in charge for taking actions without the permission of the responsible person should be defined. Appropriate considerations should be given to a case where the responsible person cannot be reached, and the authority has to be entrusted to his replacement and an ex post facto report is needed.

⑤ Prevention of repeated intrusions

As for prevention of repeated intrusions, the results of discussion of the matters related to the Policy, various actions, a plan of emergency measures, and the assessment and review of the implementation procedure should be indicated, with attention paid to the result of risk analysis about the intrusion that occurred.

5. Assessment and Review

Regular assessment and review of the standard of measures are important. It should be done in consideration of the evaluation of the Policy and the information security measure, changes of the information system and emergence of new threats. The assessment and review should be done under the Information Security Committee to keep the Policy practical and keep the information security level high.

(1) Auditing

If an external auditing organization is used, sufficient consideration should be given to its credit. It should capture weak points of the information system subject to the audit.

(2) Updating the Policy

Updating the Policy for the first time after its introduction requires special consideration. Since differences between the Policy and the reality have to be considered, it is desirable to capture the actual states by canvassing opinions from the sections concerned, or by other means. Updating the Policy should begin with risk analysis to make it practical. Information about new methods of attacking systems should be collected for reference purposes for updating the Policy.

The updated Policy has to be distributed and applied. This requires as much trouble as that required when the Policy was introduced. Efforts should be made to seek efficient methods.

(3) Reflection to the Guidelines

The results of assessment and review must be reflected in these guidelines.

Ⅳ. Appendix

1. Glossary

CD-R (Compact Disk Recordable)	A recording medium in the form of a compact disk on which data can be written only once
DAT (Digital Audio Tape)	A recording medium in the form of a magnetic tape on which data is stored electromagnetically
DoS attack (Denial of Service)	An attack to disable a service by applying too much load on the computer or network or by accessing through a security hole
DVD-RAM (Digital Versatile Disk-Random Access Memory)	A recording medium in the form of a DVD on which rewritable data is stored
FD (Floppy Disk)	A recording medium in the form of a flexible disk
HDD (Hard Disk Drive)	A recording medium in the form of a hard disk
IT (Information Technology)	Information technology
LAN (Local Area Network)	A network or segment that links terminals located within a limited area (the government ministries and agencies, for example)
MO (Magneto-Optical disk)	A recording medium in the form of a magneto optical disk
MT (Magnetic Tape)	A recording medium in the form of a magnetic tape
Access	An action to use information assets stored within a computer system
Access authority	An authority that permits access to information assets
Computer virus	A program designed to do harm to programs and databases owned by others. It has at least one of the self- contagion function, incubation function, and symptom-presentation function
Server	Software or hardware that offers intended services
System software	A program intended to manage an information system
Security management software	A program designed for information security management
Security hole	A bug of software that poses a problem of information security
Source code	An original program written in a programming language
Software	A generic name of programs and data
Display	An output device in the form of a CRT or CLD
Data	Electromagnetically stored information
Network	A group of nodes and lines that are interconnected for communication
Network resources	Resources that comprise a network

Hardware	Generic name for computer devices
Password	A code that authenticates the user
Hacking software	A program designed to attack information assets
Backup	A copy of a program or data stored in a separate medium
File	A set of programs or data stored in memory or storage devices
Host computer	A computer in a network, or the central processing computer in a centralized information system
Mail address	An address to which an e-mails are sent
Modem (MOdulater-DEModulater)	Located between an analog communication line and digital lines connected to a computer for modulation and demodulation of voice signals and digital data signals
Mobile terminal	A portable information system like cellular phone
Risk	Danger that an information system is exposed to
Logout	The procedure by which a user ends access to a computer system
Login	The procedure by which a user begins access to a computer
Vaccine software	A program that checks computer viruses, prevents the viruses, or restores an infected computer
Patch program	Additional software that corrects defects (in information security) in software
Electromagnetic recording	A recording method by electronic and magnetic means that human senses cannot recognize, for use in information processing
Unauthorized access	Access to a computer system from non-users of the system using an unauthorized action specified in a Item 2, Article 3 of the Law Concerning Prohibition of Illegal Access to Computer Systems (Unauthorized Computer Access Law) or other illegal actions or access to a computer system from the user beyond the permitted scope
Law Concerning Prohibition of Illegal Access to Computer Systems (Unauthorized Computer Access Law)	The law that prohibits unauthorized access to computer systems (Law #128, 1999)

2. For Reference

(1) Standards of security and reliability of information communication network (Notification of the Ministry of Posts and Telecommunications, 1987)

(2) Standards of Measures against Computer Viruses (Notification of the Ministry of International Trade and Industry, 1995)

http://www.miti.go.jp/kohosys/topics/10000098/esecu07j.pdf

(3) Standards of Measures against Unauthorized Access to Computers (Notification of the Ministry of International Trade and Industry, 1996)

http://www.miti.go.jp/kohosys/topics/10000098/esecu06j.pdf

(4) Standards of System Auditing (Official Announcement of the Ministry of International Trade and Industry, 1996)

http://www.miti.go.jp/kohosys/topics/10000098/esecu08j.pdf

(5) Guidelines of Information System Security (Notification of the National Public Safety Commission, 1997)

http://www.npa.go.jp/soumu2/kokuji.htm

(6) Guidelines of Administration Information System Safety (Approved on July 30, 1999 by the Board of Managers, Liaison Conference for the Ministries and Agencies Concerning Administration Information System (Inter-ministerial Meeting of Government Information Systems Division-Directors)

http://www.somucho.go.jp/gyoukan/kanri/990816c.htm

(7) BS7799 Information security management

(8) ISO/IEC 15408 (Security technology – Evaluation Standards of Information Technology Security)

(9) ISO/IEC TR 13335 Information technology – Guidelines for the management of IT security – (GMITS)

(10) Manual for Formulating Security Policies at Banking Facilities (Banking Information System Center Foundation (The Center for Financial Industry Information Systems)

http://www.fisc.or.jp/ippan_3.htm

(11) RFC2196 Site Security Handbook

http://www.ipa.go.jp/SECURITY/rfc/RFC.html

(12) CIRCULAR NO. A-130 Security of Federal Automated Information Resources

http://www.whitehouse.gov/OMB/circulars/a130/a130.html

(13) Special Publication 800-12 An Introduction to Computer Security: The NIST Handbook

http://csrc.nist.gov/nistpubs/

(14) Special Publication 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems

http://csrc.nist.gov/nistpubs/

(15) Special Publication 800-18 Guide for Developing Security Plans for Information Technology Systems (1998)

http://csrc.nist.gov/nistpubs/

(16) Practices for Securing Critical Information Assets (2000)

http://www.ciao.gov/CIAO_Document_Library/Practices_For_Securing_Critical_Information_Assets.pdf

(17) NIST Special Publication 800-20 Internet Security Policy: A Technical Guide

http://csrc.nist.gov/nistpubs/

(18) Information Security: Computer Hacker Information Available on the Internet. Statement of Jack L Brock Jr. and Keith A Rhodes. Testimony before the Permanent Subcommittee on Investigations, USGAO.