資料２－７（参考）

Common Standards of Information Security Measures for Government Agencies

(FY2014 Edition)

(Tentative Translation)

May XX, 2014

Information Security Policy Council

Contents

Chapter 1 General provisions

1.1 Purpose and scope of application of these standards

(1) Purpose of these standards

The fundamentals of information security are to ensure "Confidentiality", "Integrity" and "Availability" based on the degree of importance of information handled by government offices, ministries and agencies (hereinafter collectively referred to as “the ministries”), and in principle each of the ministries implements information security measures at their own responsibility. However, in light of the usage of a common ICT environment by the ministries, and the status of information exchange among the ministries, it is necessary to establish a common framework for all of the ministries to uniformly raise the level of information security at each of the ministries.

These common standards are the standards, which stipulate the measures to be employed to ensure information security at each of the ministries and measures to further raise the level of information security, within the unified framework for the ministries on the basis of the "Code of Information Security Measures for Government Agencies" (May 19, 2014 Security Policy Council resolution).

(2) Scope of application of these common standards

(a) The individuals to whom these common standards apply are all employees engaged in government administration (hereinafter referred to as "administrative employees").

(b) The information to which these common standards apply is as follows.

(I) Information recorded on information systems procured or developed by the ministries or recorded on external electronic media for official use by administrative employees (including information output from the relevant information systems recorded in hard copy documents and information input into the information systems from hard copy documents)

(II) Information recorded on other information systems or on other external electronic media and handled by administrative employees in an official duties(including information output from the relevant information systems recorded in hard copy documents and information input into the information systems from hard copy documents)

(III) Any other information in addition to (I) and (II) above related to the design or operation of information systems procured or developed by the ministries.

(c) These common standards apply to all information systems which handle information that falls within the scope of application of these common standards.

(3) Update of these common standards

In order to appropriately maintain the level of information security, it is important to accurately perceive situational changes and then review and revise information security measures

accordingly.

For this reason, these common standards shall be revised in accordance with the progress of information technologies by periodically reviewing and, adding to and modifying the content of the provisions as necessary.

(4) Legal compliance

With respect to handling of information and information systems, in addition to the provisions of these common standards, all relevant laws and standards, etc. (hereinafter referred to as "relevant laws, etc.") must also be strictly obeyed. In addition, because these relevant laws, etc. are items which must be observed as a matter of course regardless of information security measures, specific details on the observation of the relevant laws, etc. is not included herein. Government decisions and the like which are enacted based on or regarding information security and related conditions shall also be obeyed in the same manner.

(5) Measure item contents

In these common standards, measures to be implemented by the ministries are classified into 3 layers consisting of chapters, sections and items according to the purpose of the measures. Each item specifies the purpose, the significance and matters to be observed. Especially matters to be observed are items for measures to be surely obeyed in formulating and implementing the ministerial standards on information security measures. In Guidelines for Formulation and Implementation of Ministerial Standards on Information Security Measures and Groups of Individual Manuals Applied to Common Standards of Information Security Measures for Government Agencies separately prepared by the National Information Security Center for the determination of ministry measure standards, it is necessary to establish the ministry measure standards with reference to individual detailed measure implementation conditions corresponding to matters to be observed for the common standards to be prescribed, measure implementation examples, explanations etc.

1.2 Information rating classifications and handling restrictions

(1) Information rating classifications

Rating classifications for information used in the matters to be observed in these common standards are indicated according to 3 viewpoints of confidentiality, integrity and availability.

When the ministry changes rating classification of the ministry measure standards, they must confirm the relationships between rating classifications and matters to be observed in the measure standards, and the ministry must remain equivalent or superior to these common standards. In addition, when the ministry providing information to other ministries, it is necessary to appropriately convey the correspondence between the providing ministry's rating classifications and the rating classifications in these common standards.

Definition of ratings for confidentiality

Rating classification	Classification standards
Confidentiality 3 information	Of the information handled in government administration, information which requires confidentiality suitable to classified documents
Confidentiality 2 information	Of the information handled in government administration, information which does not require confidentiality suitable to classified documents but which if leaked, could possibly violate the rights of citizens, hinder the execution of government administration or poses a threat of such
Confidentiality 1 information	Information that has already been officially released, information for which no problems will occur even if it is opened, namely information other than Confidentiality 2 information and Confidentiality 3 information

Confidentiality 2 information and Confidentiality 3 information is referred to as "confidential information".

Definition of ratings for integrity

Rating classification	Classification standards
Integrity 2 information	Of the information handled in government administration (excluding hardcopy documents), information which if it is altered, erred or destroyed, could possibly violate the rights of citizens, hinder the execution of government administration (excluding insignificant cases) or poses a threat of such
Integrity 1 information	Information other than Integrity 2 information (excluding hardcopy documents)

Integrity 2 information is referred to as "critical information".

Definition of ratings for availability

Rating classification	Classification standards
Availability information 2	Of the information handled in government administration (excluding hardcopy documents), information which if it is destroyed, lost or rendered unusable, could possibly violate the rights of citizens, hinder the stable execution of government administration (excluding insignificant cases) or poses a threat of such
Availability information 1	Information other than Availability 2 information (excluding hardcopy documents)

Availability 2 information is referred to as "vital information".

"Confidential information", "critical information" and "vital information" are collectively referred to as "classified information ".

(2) Information handling restrictions

"Handling restrictions" refers to restrictions related to the handling of information and are a means of reliably ensuring the appropriate handling of information by administrative employees and include items such as duplication prohibitions, removal prohibitions, distribution prohibitions, encryption requirements, destruction after reading, etc.

It is necessary for administrative employees to appropriately handle information according to ratings; however when doing so handling restrictions are used as a means of indicating detailed handling methods in accordance with the ratings. It is necessary for the ministries to stipulate the basic definitions related to handling restrictions according to 3 viewpoints of confidentiality, integrity and availability.

1.3 Definition of Terms

The definitions of the terms used in the standards are indicated in each of the following items.

- Administrative employees: Refers to individuals who are national civil servants engaged in government administration at the ministries and other parties operating under the command of the ministries who handle information and information systems subject to the management of the ministries. The application of the designation of administrative employee varies for different employment conditions, however it does include, for example, temporary workers, etc.
- Areas requiring control measures: Refers to areas under the management of the ministries, such as ministry buildings, etc. managed by the ministries (including facilities etc. leased or loaned by external organizations) which require measures related to environment or facilities for protection of information handled within the area.
- Communication line: Refers to a system for transmission and reception of information via a specified method between multiple information systems or equipment etc. units (including items other than those procured by the ministries), and if not otherwise specified, collectively refers to communication lines used in government ministry information systems. Communication lines includes lines not directly managed by the ministries and the type of line (wired or wireless, physical line or virtual line, etc.) is irrelevant.
- Communications line equipment: Refers to equipment for connecting communication lines or connecting communication lines with information systems which carry out control etc. of the information transmitted and received via the lines. Communications line equipment includes the devices referred to as hubs, switch, routers, etc., as well as firewalls and other items.
- CSIRT: Refers to an organization established to respond to information security incidents which occur at the ministries. An acronym for Computer Security Incident Response Team.
- CYMAT: Refers to an organization established in the Cabinet Secretariat National Information Security Center which carries out mobile support for incidents related to information security which require unified response by the government in the event of a cyber-attack, etc. causing an outage in the information systems of government agencies etc., or events which pose the risk of such. It is an acronym for Cyber Incident Mobile Assistance Team (information security emergency support team).
- Deletion: See "Information deletion".
- Equipment etc.: Refers collectively to information system components (server equipment, terminals, communications line equipment, multifunction devices, specialized application equipment, software, etc.) external electronic media, etc.

- External services based on fixed terms and conditions: Refers to information processing services provided over the internet by business operators etc. outside of the ministries in accordance with an agreement, where user information is created, saved, which services user transmitted and otherwise handled on the server equipment provided by the relevant service. However, this excludes items which have margin for sufficient conditions settings related to the information security required by the user.

- Implementation procedures: Refers to specific, detailed procedures determined in advance for the implementation of measure details prescribed in ministry measure standards for individual information systems and work.

- Information: Refers to the items stipulated in (b) of "1.1(2) Scope of application of these common standards".

- Information deletion: Refers to a rendering all of the information recorded on electronic media so that it is unusable and difficult to recover. In addition to the erasure of the information itself, information deletion also includes the physical destruction of storage media, etc. Rendering of information into a state where the deletion can be cancelled or a recovery tool can be used to recover the information cannot be said to be a "condition where information is difficult to recover" and so is not considered to be information deletion.

- Information security incident: Refers to information security incidents as defined in JIS Q 27001:2006.

- Information security related provisions: Collectively refers to ministry measure standards and implementation procedures.

- Information systems: Refers to systems composed of hardware and software which are provided for information processing and communications uses and if not otherwise specified, refers to such systems which are procured or developed by the ministries (including systems for which management is outsourced).

- Labeling, etc.: Refers to measures for ensuring that all individuals handling information share the same awareness and recognition of the ratings of the relevant information. In addition to clearly indicating ratings by directly stating them in or on each piece of information, labeling, etc. includes other measures for ensuring a common awareness and recognition related to the ratings for the relevant information. As an example of other measures, for information recorded on specific information systems, in addition to clearly stating the rating of the information in the information systems regulations, etc., ensure all of the users of the relevant information system are informed of the ratings and regulations.

- Malicious program: Collectively refers to computer viruses, worms (programs which reproduce on their own without infecting other programs), spyware (programs which collect a

variety of information without the consent of the program user) and other programs which result in effects not intended by the user of the information system.

- Media: Refers to tangible items on which information is recorded or written. media includes paper and other tangible objects on which text, graphics and other information which can be understood by human senses is written (hereinafter referred to collectively as "hardcopies"), as well as media created using methods that cannot be understood by human senses such as electronic, magnetic and other methods which is provided for use in information processing by information systems (hereinafter collectively referred to as "electronic media"). In addition, electronic media includes internal electronic media built-in to server equipment, terminals, communications line equipment, etc., and external electronic media such as USB memory, external hard drives, DVD-Rs, etc.

- Ministry external communication line: Refers to communication lines other than ministry internal communication lines.

- Ministry internal communication line: Refers to communication lines provided for communication between server equipment and/or terminals managed by a single ministry, which logically means communication lines which are not connected to servers or terminals which are not under the management of the relevant ministry. Ministry internal communication lines include dedicated lines, VPN and other items where physical lines are not managed by the ministry.

- Ministry measure standards: Refers to standards for information security measures for maintaining the information security of information and information systems in the ministries.

- Mobile terminals: Refers to terminals which are required to be moved or travel for work, regardless of the type or form of the terminal.

- Outsourcing: Refers to contracting parties outside of the ministries to partially or completely carry out information processing for the said ministries. This includes all types of outsourcing, such as "mandate", "quasi-mandate" and "contracting" regardless of the type of agreement under which the outsourcing is carried out.

- Outsourcing contractor: Refers to parties outsourced to partially or completely carry out information processing for the ministries.

- Server equipment: Of the equipment components of information systems, this refers to equipment which provides services inherent to the server equipment to terminals, etc. which connect to the server equipment via communications lines or other means (including loaded software and directly connected keyboards, mouse and other peripherals as a single unit) and if not otherwise specified, refers to such server equipment which is procured or developed by the ministries.

- Specialized application equipment: Refers to components particular to specialized usage in information systems such as video conferencing systems, IP phone systems and network camera systems, and also refers to items which are equipped with internal electronic media.
- Terminals: Of the equipment components of information systems, this refers to equipment which is directly operated by administrative employees for the purpose of information processing (including loaded software and directly connected keyboards, mouse and other peripherals as a single unit) and if not otherwise specified, refers to such server equipment which is procured or developed by the ministries. Terminals include mobile terminals.
- The ministries: Collectively refers to agencies as stipulated by law established within the Cabinet or under the jurisdiction of the Cabinet, the Imperial Household Agency, agencies stipulated in Article 29 Item 1 or Item 2 of the Cabinet Office Establishment Act (Law No. 89 1999), agencies stipulated in Article 3 Item 2 of the National Government Organization Act (Law No. 120 1948) and agencies which fall under these agencies.

Chapter 2 Basic framework for information security

2.1 Introduction and planning

2.1.1 Preparation of organizations and systems

Purpose/significance

Information security measures are realized by all of the administrative employees engaged in tasks relevant to information security fully understanding the authority and responsibility conferred to them in accordance with the administrative organization and job duties, and fully carrying out all tasks considered their responsibility. For this reason, it is necessary to clarify these authorities and responsibilities and prepare the required organizations and systems. In particular, the chief information security officer must exercise overall control within the organization and carry out promotion to ensure that measures are systematically implemented throughout the entire organization in order to reliably advance information security measures. .

In addition, the chief information security officer shall be able to mandate portions of the duties affiliated with the authority of the position to the officers stipulated in the common standards.

Matters to be observed

(1) Establishment of a chief information security officer

ⓐ The ministries shall establish 1 individual as a chief information security officer to serve as a controlling manager for duties related to information security within the ministries.

(2) Establishment of an information security committee

ⓐ The chief information security officer shall establish departments which promote the ministries' information security and information security committees which are composed of representatives from the departments who carry out other administrative duties as organizations with the function of carrying out deliberations on the ministries' measure standards etc.

(3) Establishment of an information security audit controller

ⓐ The chief information security officer shall assign 1 individual as an information security audit controller to oversee work related to audits implemented based on the instructions of the chief information security officer.

(4) Establishment of a controlling information security officer, information security officers, etc.

ⓐ The chief information security officer shall assign 1 individual for each organization group for which it is possible to employ information security measures of the same quality, as judged by characteristics, etc., as an information security officer. Of these information security officers, 1 controlling information security officer shall be appointed as an assistant

to the chief information security officer.

(b) The information security officers shall appoint 1 area information security officer for each of the areas stipulated in matters to be observed 3.2.1(2)(a) to oversee information security measure duties in each relevant area.

(c) The chief information security officer shall assign 1 individual as a section information security officer to oversee work related to information security for each section.

(d) The chief information security officer shall assign an information system security officer as the individual responsible for work related to information security measures for information systems under their jurisdiction before the planning of the relevant information system begins.

(5) Establishment of a chief information security advisor

(a) The chief information security officer shall appoint an individual with specialist knowledge and experience related to information security as a chief information security advisor and stipulate the duties of the chief information security advisor including advising the chief information security officer.

(6) Establishment of systems in preparation for information security incidents

(a) The chief information security officer shall establish a CSIRT and clarify its duties.

(b) The chief information security officer shall appoint members of the CSIRT from among administrative employees recognized as possessing specialized knowledge or aptitude. From among these officers, a CSIRT officer shall be appointed as the individual responsible for managing information security incidents in the ministries.

(c) The chief information security officer shall establish a system to immediately report to the chief information security officer in the event of an information security incident.

(d) The chief information security officer shall appoint the employees to be assigned to the CYMAT.

(7) Roles for which holding of additional posts simultaneously is prohibited

(a) The simultaneous holding of the following roles shall be prohibited for administrative employees in the operation of information security measures.

(I) Roles as applicant for approval or authorization (hereinafter collectively referred to as "approval etc.") and the role granting the relevant approval etc. (hereinafter referred to as "approval authorities etc.")

(II) Roles as individual subject to audit and undergoing audit

(b) When applying for approval etc., if an administrative employee is the approval authority etc., or it is otherwise determined that the relevant approval authority etc. is unsuitable for judgment of the approval etc., the relevant approval authority etc. shall apply for and receive approval etc. from their superior or other appropriate individual.

2.1.2 Establishment of ministry measure standards and measure promotion plan

Purpose/significance

In order to continue to maintain an appropriate standard for the ministries' information security, and comprehensively reduce information security risks, it is important to establish measure standards to be observed by the ministries and systematically implement those measures based on the effects of risk assessment related to information security.

Matters to be observed

(1) Establishment of ministry measure standards

(a) The chief information security officer shall establish ministry measure standards conforming to the common standards through deliberation by the information security committee.

(2) Establishment of a measure promotion plan

(a) The chief information security officer shall establish a plan to comprehensively promote information security measures (hereinafter referred to as the "measure promotion plan") through deliberation by the information security committee. In addition, the measure promotion plan shall include an overall policy based on the results of risk assessment related to the work of the ministries, handled information and possessed information systems, as well as policies and important points for the initiatives indicated below.

(I) Information security related training

(II) Self-inspection of information security measures

(III) Information security audits

(IV) Initiatives for promotion of technical measures related to information systems

(V) Any other important initiatives related to information security measures other than the initiatives in the preceding items

2.2 Operation

2.2.1 Operation of information security related provisions

Purpose/significance

It is necessary for the ministries to establish specific, detailed implementation procedures in order to implement the measures stipulated in the ministry measure standards.

As there is a risk of measures not being implemented if implementation procedures are not prepared or if there are oversights in the content of the implementation procedures, it is important for the chief information security officer shall instruct the controlling information security officer to prepare the implementation procedures, receive periodic reports of the results and maintain an accurate understanding of conditions.

Matters to be observed

(1) Preparation and operation of implementation procedures related to information security measures

ⓐ The controlling information security officer shall prepare the implementation procedures related to information security officers in the ministries (excluding situations where the individual charged with preparing these common standards is separately stipulated), oversee work related to the implementation procedures and report on the preparation conditions to the chief information security officer.

ⓑ The controlling information security officer shall prepare regulations for management related to hiring, dismissal and personnel transfers in information security measures.

ⓒ The information security officers or section information security officer shall report any information security related provision issues or problems reported by administrative employees to the controlling information security officer.

(2) Handling of violations

ⓐ In the event an administrative employee learns of a serious violation of the information security related provisions, the details shall be reported to the information security officer.

ⓑ In the event an information security officer receives a report of a serious violation of the information security related provisions, or learns of a serious violation on their own, the information security officer shall instruct the violator and other required parties of the need for the maintenance of information security in addition to reporting the violation to the chief information security officer.

2.2.2 Exceptional measures

Purpose/significance

There are situations where alternative methods are employed which differ from the details of the prescribed measures or where the prescribed measures are not implemented due to the execution of the information security related provisions significantly hindering the appropriate execution of administrative affairs or for other reasons. In order to handle such situations, it is necessary to establish procedures for exceptional measures.

Matters to be observed

(1) Preparation of exceptional measure procedures

(a) The chief information security officer shall stipulate the individual to carry out screening of applications for the utilization of exceptional measures (hereinafter referred to as the "approver") as well as the procedures for the screening.

(b) The controlling information security officer shall prepare a ledger for records of the enactment of exceptional measures and periodically obtain reports of the status of applications from the approver.

(2) Employment of exceptional measures

(a) The administrative employees shall apply for employment of the prescribed exceptional measures from the approver in accordance with the established screening procedures. However, in the event the administrative affairs requires urgency, if the relevant regulations can be handled with sufficient respect, and methods to substitute for the information security related provision regulations can be immediately instituted, or not implementing the prescribed methods is otherwise unavoidable, the application may be made immediately after the occurrence.

(b) The approver shall carry out screenings of the application for the employment of exceptional measures by administrative employees in accordance with the screening procedures and make a determination on whether or not to approve the application.

(c) The approver shall record the application status of the exceptional measures in a ledger and report the status to the controlling information security officer.

(d) The controlling information security officer shall investigate additions or revision of the information security related provisions based on the status of applications for exceptional measures and report to the chief information security officer.

2.2.3 Training

Purpose/significance

Even if the information security related provisions are appropriately maintained, if the

administrative employees are not familiar with the content, and the content is not strictly observed, it is not possible to expect the level of information security to improve. For this reason, it is necessary to deepen the knowledge of all administrative employees through information security training, and implement information security measures appropriately.

Matters to be observed

(1) Preparation of training systems etc.

ⓐ The controlling information security officer shall establish a training implementation plan for information security measures based on the measure promotion plan and prepare a system for its implementation.

(2) Training implementation

ⓐ The section information security officer shall appropriately carry out training related to the information security related provisions for the administrative employees.

ⓑ The administrative employees shall appropriately undergo training in accordance with the training implementation plan.

ⓒ The section information security officer shall appropriately carry out training for the CYMAT and CSIRT affiliated employees.

ⓓ The controlling information security officer shall report on the implementation status of the training related to the information security measures to the chief information security officer.

2.2.4 Handling of information security incidents

Purpose/significance

In the event an information security incident is discovered, it must be immediately reported to the chief information security officer and measures must be implemented to prevent the spread of damages and for recovery. In addition, once the handling of the information security incident is completed, it is important to deduce lessons should from the occurrence of the information security incident which can be utilized in the future by investigating causes, etc., and connect these lessons to revision of the systems, procedures, etc. for handling such incidents and preventing recurrence.

Matters to be observed

(1) Advance preparation for information security incidents

ⓐ The controlling information security officer shall prepare procedures for reporting to the ministry stakeholders, including the reporting point of contact, in the event an information security incident is discovered, and notify the administrative employees of the procedures.

ⓑ The controlling information security officer shall establish response procedures, including information sharing with parties outside the ministries, in the event an information security

incident is discovered.

(c) In preparation for information security incidents, the controlling information security officer shall establish an emergency contact network which includes emergency contacts, contact methods and contact details for information systems deemed especially important to the execution of work.

(d) The controlling information security officer shall investigate the necessity of training for information security incident handling, and establish a training system and details for information systems deemed especially important to the execution of work.

(e) The controlling information security officer shall establish a point of contact for receiving reports about information security incidents from parties outside of the ministries, and inform parties outside of the ministries of the contact methods for the point of contact.

(2) Reporting and handling when an information security incident is discovered

(a) The administrative employees shall report to the ministries reporting point of contact when an information security incident is discovered and act in accordance with the instructions received.

(b) The CSIRT officer shall verify the circumstances in the event an information security incident is discovered, and immediately report on the information security incident to the chief information security officer.

(c) The CSIRT shall provide the relevant information security officers with instructions and advice on the implementation of emergency measures to prevent the spread of damages in the event of the discovered information security incident as well as for recovery from the information security incident.

(d) In the event an information security incident is discovered, the information system security officers shall carry out appropriate handling of the information systems under their jurisdiction in accordance with the handling procedures stipulated by the ministries or the instructions or advice of the CSIRT.

(e) In the event the discovered information security incident is related to multiple information systems used and shared by multiple ministries (Excluding information systems managed and operated by a single ministry from hardware to applications. Hereinafter referred to as the "information systems constituting common infrastructure".), and in the event there are operation and management regulations stipulated for the relevant information systems constituting common infrastructure, the information system security officer shall carry out appropriate response in accordance with the relevant operation and management regulations.

(f) For the information systems of the ministries, in the event an information security incident is discovered, the CSIRT shall immediately contact the Cabinet Secretariat National Information Security Center regarding the event. In addition, in the event the discovered information security incident is a cyber-attack or may be a cyber-attack, the police shall be contacted/given reports as necessary based on the details of the relevant information security incident. In addition, in large scale cyber-attacks and other situations resulting in, or

potentially resulting in significant damages to the public welfare, people's health, property or to the country itself, reports shall be carried out in accordance with the "Regarding initial response to large scale cyber-attacks (March 19, 2010, Deputy Chief Cabinet Secretary for Crisis Management Resolution)".

(g) The CSIRT shall carry out information sharing with relevant agencies, including the ministries, in regard to information security incidents.

(h) When receiving support from the CYMAT, the CSIRT shall provide information necessary to receive the support.

(3) Investigation of causes and recurrence prevention for information security incidents

(a) When the information security officer receives instructions from the CSIRT, they shall, in accordance with the relevant instructions or recommendation, carry out investigation of the cause of the information security incident, consider measures to prevent recurrence, and submit a report to the chief information security officer.

(b) When the chief information security officer receives a report on an information security incident from an information security officer, the chief information security officer shall verify the content of the report and instruct on the measures which need to be implemented in order to prevent recurrence.

2.3 Inspection

2.3.1 Self-inspection of information security measures

Purpose/significance

In order to guarantee the effectiveness of information security measures, it is necessary to inspect status of observation etc. of the information security related provisions, and analyze and form an understanding of the results of the inspection.

Self-inspection is not only carried only to verify that the measures which should be implemented by administrative employees according to their roles are actually being implemented, but also in order to verify the level of information security for the entire organization, and it is therefore important that the self-inspections are implemented appropriately.

In addition, it is necessary for each involved party to implement the required reform measures within the scope of the responsibility of each of their roles based on the results of the self-inspection.

Matters to be observed

(1) Establishment of self-inspection plan and preparation of procedures

ⓐ The controlling information security officer shall establish a fiscal year self-inspection plan based on the measure promotion plan.

ⓑ The information security officers shall prepare self-inspection forms and self-inspection implementation procedures for each of the administrative employees.

(2) Self-inspection implementation

ⓐ The information security officers shall instruct the implementation of administrative employee self-inspections based on the fiscal year self-inspection plan.

ⓑ The administrative employees shall carry out the self-inspections using the self-inspection forms and self-inspection implementation procedures instructed by the information security officer.

(3) Assessment and improvement of the self-inspection results

ⓐ The controlling information security officer and information security officers shall analyze and assess the results of the administrative employees' self-inspections. The controlling information security officer shall report the assessment results to the chief information security officer.

ⓑ The chief information security officer shall carry out overall assessment of the self-inspection results, and provide instructions for improvement to the controlling information security officer and information security officers regarding any obvious problem points with the self-inspection results.

2.3.2 Information security audits

Purpose/significance

In order to guarantee the effectiveness of information security measures, it is necessary to not only have self-inspections carried out by the parties carrying out the information security measures, but also to have audits of information security measures carried out by independent parties.

In addition, it is important for the chief information security officer to instruct the information security officers to enact necessary measures based on the problems which were made clear from the audit results.

Matters to be observed

(1) Establishment of an audit implementation plan

ⓐ The information security audit controller shall establish an audit implementation plan in accordance with the measure promotion plan.

ⓑ In the event the information security audit controller receives instructions from the chief information security officer to implement audits other than the audits planned in the measure promotion plan based on changes in the status of information security, the information security audit controller shall establish an additional audit implementation plan.

(2) Audit implementation

ⓐ The information security audit controller shall, in accordance with the audit implementation plan, instruct the auditors to implement audits which include the following items and report the results to the chief information security officer as an audit report.

(I) That appropriate items have been established to fulfill the common standards in the ministry measure standards

(II) That the implementation procedures are in accordance with the ministry measure standards

(III) That the actual operation in the division being audited is in accordance with the information security related provisions, through verification of the appropriateness of self-inspections, etc.

(3) Management based on audit results

ⓐ The chief information security officer shall instruct the information security officers to establish management plans for indicated items based on the details of audit reports.

ⓑ The information security officers shall establish management plans for the items cited as requiring improvement from the chief information security officer in accordance with the audit report and report on the said establishment.

2.4 Review

2.4.1 Review of information security measures

Purpose/significance

The environments surrounding information security are ever-changing, and if these changes are not appropriately responded to, the level of information security will not be able to be maintained. For this reason, it is necessary to carry out periodic review of the information security related provisions, which serve as the basis for the ministries' information security measures, based on the issues arising from actual operations, the results of self-inspections and audits, and other factors.

In addition, it is also important to review initiatives in order to further promote initiatives related to information security by comprehensively assessing the results of self-inspections and audits.

Matters to be observed

(1) Review of information security related provisions

ⓐ In addition to carrying out comprehensive assessment of the operation of information security as well as the results of self-inspections and audits, the chief information security officer shall carry out required review of ministry measure standards through deliberation by the information security committee based on significant changes related to information security, etc.

ⓑ Based on the results of the operation of information security, self-inspections and audits, the controlling information security officer shall review the implementation procedures related to information security measures and instruct the party who prepared the regulations to review them, and report the results of the review to the chief information security officer.

(2) Review of the measure promotion plan

ⓐ In addition to carrying out comprehensive assessment of the operation of information security measures, inspections and audits, the chief information security officer shall carry out periodic review of the measure promotion plan through deliberation by the information security committee based on significant changes related to information security, etc.

Chapter 3 Information handling

3.1 Information handling

3.1.1 Information handling

Purpose/significance

During the execution of administrative affairs, the creation, obtainment, usage, saving, provision, transport, transmission, deletion, etc. of information (hereinafter referred to as " use, or otherwise handle" in this section) is necessary, and in order to maintain the information security of a given piece of information, it is necessary for all administrative employees who will use, or otherwise handle the relevant information to implement appropriate measures based on the characteristics of the information at every stage of the information's lifecycle. For this reason, it is necessary for the administrative employees to indicate the rating and handling restrictions for the relevant information through labeling etc. at the point at which it is created or obtained as a measure to ensure a common awareness and recognition of the information, and also implement measures in accordance with the rating and handling restrictions of the said information.

Matters to be observed

(1) Establishment of regulations on information handling

(a) The controlling information security officer shall establish regulations on handling of information including the following, and ensure the administrative employees are informed of the regulations.

(I) Definition of ratings and handling restrictions for the information

(II) Procedures for labeling etc. of the information's ratings and handling restrictions

(III) Procedures for the succession and review of the informations ratings and handling restrictions

(2) Prohibition on the use, or otherwise handle of information for unrelated purposes

(a) The administrative employees shall only use, etc. the information within the scope required for the execution of the administrative affairs for which they are responsible.

(3) Determination and labeling, etc. of information ratings and handling restrictions

(a) At the time of information creation, or when information created by parties outside the ministries is obtained, the administrative employees shall establish ratings and handling restrictions based on the predetermined definitions for ratings and handling restrictions, and indicate these ratings and handling restrictions by labeling etc.

(b) In the event information is classified as Confidentiality 3 information, the period for which the information will be handled as Confidentiality 3 information shall be indicated by labeling etc.

(c) In the event ratings and handling restrictions are already established for the referenced or obtained information, the administrative employees shall inherit and maintain the ratings and handling restrictions related to the confidentiality of the information.

(d) In the event it may be necessary to revise the ratings and handling restrictions of information due to reasons of corrections, additions, deletions, or for other reasons, the administrative employees shall confirm the details of the revisions by consulting with the party which determined the rating and handling restrictions for the information (including those who inherited the decision), or with their superior (hereinafter referred to as the "deciders" in this section) and carry out revision based on the results.

(4) Information usage and saving

(a) The administrative employees shall appropriately handle information in accordance with the ratings and handling restrictions indicated by labeling etc. for the relevant information.

(b) In the event administrative employees will carry out information processing of Confidentiality 3 information outside of the areas requiring control measures, the authorization of the information system security officer and section information security officer shall be obtained.

(c) In the event the administrative employees will carry out information processing of classified information outside of the areas requiring control measures, required safety control measures shall be implemented.

(d) The administrative employees shall appropriately manage information according to the information's ratings and handling restrictions through measures such as setting access restrictions for information being saved.

(e) When using USB memory or other external electronic media to handle information, the administrative employees shall handle the said media in accordance with stipulated usage procedures.

(5) Provision and official release of information

(a) In the event information is to be officially released, the administrative employees shall verify that the relevant information is rated as Confidentiality 1 information.

(b) In the event it is necessary to provide information to parties outside the scope of the handling restrictions, the administrative employees shall consult with the party which decided the ratings and handling restrictions for the relevant information, etc. and determine the handling according to the decisions made through the consultation. In addition, the provider of the information shall implement measures such as conveying important considerations in the handling of the relevant information in order to ensure the information is handled appropriately in accordance with the ratings and handling restrictions applied to the relevant information.

(c) In the event Confidentiality 3 information is to be provided to parties outside the scope of the handling restrictions, the administrative employees shall obtain the authorization of the

section information security officer.

(d) In the event electronic records are to be provided or officially released, the administrative employees shall enact measures to prevent unexpected leaks from related records (refers to revision history, document properties, etc.) or other sources.

(6) Transportation and transmission of information

(a) In the event Confidentiality 3 information, critical information or vital information is to be physically transported or transmitted using ministry external communication lines outside of the areas requiring control measures, the administrative employees shall obtain the authorization of the section information security officer.

(b) In the event classified information or storage media containing such information is to be taken outside of the areas requiring control measures, administrative employees shall determine transportation methods based on careful consideration of security, and implement appropriate measures to maintain security in accordance with the ratings and handling restrictions of the relevant information. However, in the event the information is to be taken into an area requiring control measures of another ministry and only to an area stipulated by the controlling information security officer the relevant area can be treated as an area requiring control measures for the relevant information.

(c) In the event electronic records which are classified as classified information are to be transmitted via email or other means, the administrative employees shall determine transmission methods based on careful consideration of security, and implement appropriate measures to maintain security in accordance with the ratings and handling restrictions of the relevant information.

(7) Information erasure

(a) In the event information stored on electronic media is no longer necessary for administrative affairs, the administrative employees shall immediately erase the said information.

(b) When disposing of electronic media, the administrative employees shall ensure the media content is completely deleted so that no information remains on the media and none of the information can be recovered.

(c) In the event hardcopies of confidential information is to be disposed of, the administrative employees shall render the said hardcopies into a state from which recovery is difficult.

(8) Information backup

(a) Administrative employees shall backup information using appropriate methods in accordance with the information's rating.

(b) Administrative employees shall designate storage locations, storage methods, storage periods and other details for backups of acquired information and carry out appropriate management of the backups in accordance with the ratings and handling restrictions of the

information.

(c) Administrative employees shall erase, delete or dispose of information backups which have exceeded their prescribed storage period using appropriate methods in accordance with point (7) of this item.

3.2 Management of information handling areas

3.2.1 Management of information handling areas

Purpose/significance

For equipment environments such as server equipment, terminals, etc., where many and unspecified persons have direct physical access to the equipment, there is a risk of malicious individuals gaining access to the equipment through impersonation and physically damaging or destroying the equipment, or removing server equipment, terminals or other equipment maliciously which could result in information leaks or other incidents. Other potential threats to equipment environments include damage to information systems resulting from disasters, etc.

As such, it is necessary to maintain the security of areas where information is handled, such as offices, conference rooms and server rooms, through physical measures and access control, in order to maintain the security of the information and information systems handled in the areas.

Matters to be observed

(1) Establishment of standards for measures in areas requiring control measures

ⓐ The controlling information security officer shall stipulate the scope of areas requiring control measures.

ⓑ The controlling information security officer shall stipulate standards for measures for areas requiring control measures which include the following in accordance with the characteristics of the relative areas.

(I) Physical measures such as lockable doors, partitions and other facility preparations to prevent unauthorized individuals from easily entering the areas

(II) Access control measures to restrict access by unauthorized individuals and to prevent wrongful acts in the event of access by authorized individuals

(2) Establishment of measures for each area

ⓐ The information security officers shall stipulate areas for each facility and environment for which measures will be implemented in accordance with the measure standards prescribed by the controlling information security officer.

ⓑ For the areas to be controlled, the area information security officers shall determine the measures to be implemented in the relevant areas with consideration for the measure standards stipulated by the controlling information security officer, the surrounding environments and the details of the work carried out in the relevant areas.

(3) Implementation of measures in areas requiring control measures

ⓐ The area information security officers shall implement the measures decided for the areas they control. Measures shall be enacted to ensure the administrative employees are aware of and understand the measures which the administrative employees shall implement.

(b) The area information security officers shall implement physical measures to protect information systems which handle vital information from disasters.

(c) The administrative employees shall make use of areas in accordance with the measures prescribed by the area information security officers for the area being used. In addition, in the event administrative employees will allow individuals from outside the ministries access to an area requiring control measures, the administrative employees shall ensure that the individuals from outside the ministries also use the area in accordance with the prescribed measures.

Chapter 4 Outsourcing

4.1 Outsourcing

4.1.1 Outsourcing

Purpose/significance

When entrusting development of information systems, development of application programs, etc. to parties which are outside of the ministries, it is difficult for the administrative employees to directly manage the information security measures of such outsourcing contractors. In this case, it is necessary to specify the information measures required of the outsourcing contractors on procurement specifications etc., and include these requirement as contract conditions, in order to ensure that information security measures which conform to the ministry measure standards are reliably implemented by the outsourcing contractors.

There are wide variety of outsourcing types, as shown in the following examples, however in all circumstances, when concluding an agreement with an outsourcing contractor, it is important to clarify the scope of the duties being outsourced as well as the scope of responsibility of the outsourcing contractor, and form a consensus on the details of information security measures between both parties to the agreement.

In addition, for cases where administrative affairs is executed by making use of ”external services based on fixed terms and conditions”, this can be considered as a type of outsourcing, however, for cases where it is difficult to conclude special agreements with the outsourcing contractors and there is not sufficient room to set sufficient conditions for information security, it is necessary to strictly abide by the stipulations in 4.1.2 "Usage of external services based on fixed terms and conditions".

<Outsourcing examples>

- Information system development and construction
- Development of application programs, web contents, etc. (hereinafter collectively referred to as "applications and contents".
- Operation of information systems
- Information processing works using external services such as public clouds, etc.
- Support of work operations (statistics, tabulations, data entry, media conversion, etc.)
- Project management support, etc.
- Investigations/research (investigations, research, inspections, etc.)
- Leasing (information systems, data centers, communication lines, etc.)

Matters to be observed

(1) Establishment of regulations for outsourcing

(a) The controlling information security officer shall establish regulations for outsourcing which include the following.

(I) Standards for determining the scope of information systems that can be outsourced

and the scope of information and information systems which outsourcing contractors are authorized to access

(II) Standards for the selection of outsourcing contractors

(2) Outsourcing contracts

(a) The information system security officers or section information system security officers shall select outsourcing contractors in accordance with the selection standards and selection procedures. In addition, implementation of information security measures which include the following shall be considered as criteria for the selection of outsourcing contractors and shall be included in specification details.

(I) Prohibition of use of information provided to outsourcing contractors for unrelated purposes

(II) Information security measure implementation details and management systems as outsourcing contractors

(III) Management systems to ensure no undesirable changes are made by the outsourcing company, the employees of the said company, secondary and successive subcontractors or any other parties

(IV) Provision of information related to outsourcing contractors' capital ties, officers, outsourcing locations and also information on the individuals carrying out the outsourcing including affiliations and expertise (information security related qualifications, training results, etc.), past performance and nationality

(V) Procedures for handling information security incidents

(VI) Procedures for verifying execution of information security measures and other contact stipulations

(VII) Management procedures for situations where execution of information security measures is insufficient

(b) The information system security officers or section information security officers shall include the following in specifications as necessary based on the ratings, etc. of the information to be handled in outsourcing.

(I) Acceptance of information security audits

(II) Guarantee of service level

(c) When consigning any portion of outsourcing contractors' duties to subcontractors, the information system security officers or section information security officers shall require that outsourcing contractors guarantee that the measures in (a) and (b) above are implemented in order to ensure sufficient information security against any threats that may occur as a result of any secondary or subsequent subcontracting.

(3) Implementation of measures in outsourcing

(a) The information system security officers or section information security officers shall verify the status of the implementation of information security measures by outsourcing

contractors in accordance with the outsourcing contracts.

(b) In the event the information system security officers or section information security officers recognize the occurrence of information security incidents or use of information for unrelated purposes, etc. in the course of the outsourcing works, they shall implement required measures, including discontinuing the relevant service and require the implementation of any necessary measures by outsourcing contractors in accordance with the outsourcing contracts.

(c) When the outsourced works are completed, the information system security officers or section information system security officers shall verify that the information handled during the outsourcing is reliably returned or deleted.

(4) Handling of information in outsourcing

(a) The administrative employees shall observe the following when providing information to outsourcing contractors.

(I) That, when providing classified information to outsourcing contractors, only the minimum required information is provided and the information is provided via secure procedures determined in advance.

(II) That, in the event the provided classified information becomes unnecessary at the outsourcing contractors, it is reliably returned or deleted.

(III) That, in the event of the awareness of information security incidents or use of information for unrelated purposes during outsourcing, such affairs shall be immediately reported to the information system security officers or section information security officers.

4.1.2 Usage of external services based on fixed terms and conditions

Purpose/significance

When administrative affairs is to be carried out through usage of external services based on fixed terms and conditions, information security measures must be ensured through measures such as concluding the items stipulated in 4.1.1 "Outsourcing" as special agreements. However, there are many cases where use of such services includes high risk, such as inability to conclude special agreements for use of external services based on fixed terms and conditions, inability to set sufficient conditions the required information security, no guarantee of service continuity, unknown data management locations and backup methods, etc., are unknown, so such services should not be used when there is potential that confidential information will be handled. In cases where the use of such services is unavoidable, despite the provisions of 4.1.1 "Outsourcing", determination of use should be carried out only after sufficient consideration of risk and it is important that information security measures be reliably implemented.

Matters to be observed

(1) Establishment of regulations for usage of external services based on fixed terms and conditions

(a) The controlling information security officer shall establish regulations regarding the use of external services based on fixed terms and conditions which include the following. In addition, regulations shall prohibit the handling of confidential information in the usage of the relevant services.

(I) The scope of work for which external services based on fixed terms and conditions can be used

(II) The external services based on fixed terms and conditions which can be used for work

(III) Usage and operation procedures

(b) The information security officers shall appoint supervisors for each service used when using external services based on fixed terms and conditions.

(2) Implementation of measures in usage of external services based on fixed terms and conditions

(a) The administrative employees apply for usage of external services based on fixed terms and conditions after confirming that the risks of fixed terms and conditions of the said service can be accepted, and only use the said services after implementing appropriate measures.

4.1.3 Dissemination of information via social media services

Purpose/significance

A wide variety of social media services where uses disseminate and create information, including blogs, social networking services, video sharing sites, etc., have become common on the internet. These services have also come to be used by government agencies for purposes such as active PR activities. However, because the use of social media services unavoidably includes the usage of external services based on fixed terms and conditions, and government domain names cannot be used, the risk of accounts impersonating government agencies is unavoidable. In addition, it is also possible that conditions could arise where necessary information is not able to be disseminated in the event an account of a government agency is hijacked or the social media service being used cancels service with no notice. For this reason, when widely providing important information, such as vital information, it is necessary for the information to be provided in a manner which allows for the public or other parties requiring the relevant information to check a primary information source, such as by first posting the information to websites managed by the ministries themselves and then providing it on the social media service as well. It is also necessary for the provider of the information to implement measures, such as measures against impersonation and spoofing, to prevent any confusion of the public occurring as a result of false information.

Because technological development of social media services, such as expended functionality and added services is intensive, it is necessary to always quickly respond to changes in external environments, such as trends and tendencies of the operators of the relevant services.

Matters to be observed

(1) Measures during dissemination of information via social media services

(a) The controlling information security officer shall establish information security measure related operation procedures which include the following, on the assumption that social media services will be made use of through formal ministry account.

(I) Measures shall be implemented against impersonation and spoofing, such as clealy stating the organization operating the account, in order to make clear that the information distributed through the ministry account is actually being distributed by the relevant ministry.

(II) Measures shall be implemented against unauthorized access, such as appropriate management of passwords and other entity authentication information.

(b) The information security officers shall appoint supervisors for each social media service used when using social media services are used by the ministries for the dissemination of information.

(c) When administrative employees will use social media services for the provision of vital information to the public, the relevant information shall be made available for viewing on formal websites of the ministries.

Chapter 5 Information system lifecycles

5.1 Maintenance of documents, etc. related to information systems

5.1.1 Maintenance of ledgers, etc. related to information systems

Purpose/significance

In order to maintaining the level of information security for information systems under the jurisdiction of the ministries as well as appropriately and quickly responding to information security incidents, it is important to prepare and maintain information related to information security measures for information systems under the jurisdiction of the ministries through information system ledgers which allow for fast verification of procurement specifications, setting information and other details related to the components of information systems.

Matters to be observed

(1) Maintenance of information system ledgers

(a) The controlling information security officer shall prepare information system ledgers for items related to the information system security requirements for all information systems.

(b) When information systems are newly constructed or updated, the information security officers shall record or describe the details related to the security requirements for the relevant information system ledgers, and report the relevant details to the controlling information security officer.

(2) Maintenance of information system related documents

(a) The information system security officers shall prepare information system related documents which completely cover all of the following as documents required for the implementation of information security measures for the information systems under their jurisdiction.

(I) Information related to server equipment and terminals which compose the information systems

(II) Information related to communications lines and communications line equipment which composes the information systems

(III) Procedures related to the maintenance of the level of information security for each information system component

(IV) Response procedures for the event of the discovery of an information security incident

5.1.2 Establishment of regulations for procurement of equipment etc.

Purpose/significance

There are risks to the confidentiality, integrity and availability of information handled by information systems in circumstances where procured equipment etc., is not equipped with required security functions, undesirable changes occurred during the manufacturing process of the relevant equipment etc., or the information security measures are not maintained after the procurement of the relevant equipment etc.

In order to manage these type of issues, it is necessary to establish selection standards for equipment etc. as well as procedures for verification and inspection at the time of delivery, in order to carry out procurement of equipment etc. in accordance with the ministry measure standards.

Matters to be observed

(1) Establishment of regulations for procurement of equipment etc.

(a) The controlling information security officer shall establish selection standards for the equipment etc. The implementation of management to ensure no undesirable changes are carried out during the lifecycle, including the development etc., of the equipment etc. and the ability of the ministries to verify the said management status, may be added as one of the selection standards if necessary.

(b) The controlling information security officer shall establish procedures for verification and inspection of information security measures at the time of delivery of the equipment etc..

5.2 Measures at each stage of information system lifecycles

5.2.1 Information system plan and requirement definitions

Purpose/significance

In order to appropriately maintain information security throughout the entire information system lifecycle, at the information system planning stage, it is necessary to establish a system that allows for the implementation of information security maintenance for information systems, and define requirements for a variety of information security risks based on the information system lifecycle.

Security requirement vagueness, excess or deficiency can lead to a variety of detriments, such as increased costs resulting from excessive information security measures, unfair competitive bidding caused by differences in proposal details as a result of variation in interpretations of requirements, reworking in design and development processes, and occurrence of information security incidents after commencement of operations.

For these reasons, it is important to examine measures for estimated threats against information systems after taking into consideration the work for which the information system will be used, the information handled in the work, the individuals handling the information, and environments and methods, etc. used for information processing, and appropriately incorporate necessary security requirements in specifications.

In addition, it is also important to take measures for preventing the introduction of vulnerabilities into the constructed information systems into account before construction, during the planning stage.

It is also necessary for the provisions of 4.1.1 "Outsourcing" to also be observed in situations where information system construction, operation and maintenance is outsourced.

Matters to be observed

(1) Implementation system guarantee

ⓐ The information system security officers shall require the supervisors controlling the information systems to guarantee implementation systems that allow for maintenance of information security throughout the entire information system lifecycle.

ⓑ When constructing information systems using information systems constituting common infrastructure, the information system security officers shall require the supervisors controlling the information systems to prepare systems in accordance with the operation and management regulations stipulated by the ministries which prepare the information systems constituting common infrastructure and carry out operation and management.

(2) Establishment of information system security requirements

ⓐ The information system security officers shall establish information security requirements which include the following, based on the purpose of the construction of the information systems, requirements of the work the systems will be used for, ratings of the information that will be handled by the relevant information systems, and other factors.

(I) Entity authentication, access control, authorization management, log management, and encryption function etc. security function requirements that will be incorporated into the information system

(II) Requirements for operation management functions such as monitoring during information system operation

(III) Measures requirements for information system related vulnerabilities

(b) The information system security officer shall establish security requirements based on the "Guidelines on Risk Assessment and Digital Signatures/ Authentication for e-Government" for systems which provide online procedures such as applications and submissions between the public, businesses and the government.

(c) When procuring equipment etc., information system security officers shall refer to the "Security requirements list for procurement of IT products ", and after analyzing threated in the usage environment, establish requirements for security to counter the information security threats which exist for the relevant equipment etc.

(d) When using information systems constituting common infrastructure to construct information systems, information system security officers shall appropriately establish security requirements based on operation and management regulations related to information security measures for information systems constituting common infrastructure to ensure that the level of information security for the entire information systems constituting common infrastructure is not lowered.

(3) Measures for the outsourcing of information system construction

(a) When outsourcing the construction of information systems, information system security officers shall include in the procurement specifications the following items to be implemented by the outsourcing contractors to ensure the outsourced work is carried out appropriately.

(I) Appropriate implementation of information system security requirements

(II) Implementation of test necessary from an information security standpoint

(III) Implementation of information security measures related to information system development environment and development process

(4) Measures for the outsourcing of information system operation and maintenance

(a) When outsourcing the operation and maintenance of information systems, the information system security officers shall include the requirements for the security functions included in the information systems to be appropriate implemented in the procurement specifications to ensure the outsourced work is carried out appropriately.

5.2.2 Information system procurement and construction

Purpose/significance

When procuring or constructing information systems, in order to appropriately implement information security measures based on prescribed security requirements, it is necessary to implement information security measures in the procurement of equipment etc. conforming to selection standards the information system development process.

In addition, at the time of delivery of equipment etc. or at the time of reception of information systems, it is necessary to carry out inspections in accordance with the established inspection procedures to ensure that the security functions for protecting information when the relevant information system is operated and the management functions for the security functions are appropriately incorporated in information systems.

Matters to be observed

(1) Measures for the selection of equipment etc.

ⓐ In the selection of equipment etc., the information system security officers shall verify the conformity of the equipment etc. to the selection standards and use the results as one factor in the determination of the selection of the equipment etc.

(2) Measures for the construction of information systems

ⓐ In the construction of information systems, the information system security officers shall implement measures necessary from an information security standpoint.

ⓑ When transitioning to the operation and maintenance stage of the constructed information system, the information system security officers shall implement necessary measures related to transition procedures and transition environments from an information security standpoint.

(3) Measures for delivery inspections

ⓐ In verification and inspection at the time of delivery of equipment etc. or at the time of reception of information systems, the information system security officers shall verify that the information security measure related requirements are fulfilled in accordance with the inspection procedures stipulated in specifications etc.

5.2.3 Information system operation and maintenance

Purpose/significance

When transitioning to the information system operation stage, in order for the security requirements determined in the planning or procurement/construction stage to be appropriately carried out, it is necessary to establish a personnel operation system, periodically verify that the equipment etc. parameters are set correctly, and implement management etc. of work records related

top operation and maintenance.

In general, the majority of information security incidents which occur for information systems occur during operation, so it is also important to monitor the operation status of information systems in order to verify the effectiveness information security measures for information systems.

In addition, it is also necessary for information security measures to be appropriately implemented in the maintenance of information systems in the same manner as in their operation. Even in situations where maintenance work is individually outsourced, it is necessary to implement appropriate measures for information security measures based on ministry measure standards.

Matters to be observed

(1) Measures for information system operation and maintenance

ⓐ In the operation and maintenance of information systems, information system security officers shall appropriately utilize the security functions included in information systems.

ⓑ When carrying out operation of information systems constructed using information systems constituting common infrastructure, the information system security officers shall appropriately operate the information system in accordance with the operation and management regulations for the information systems constituting common infrastructure under an operation management system in accordance with the division of responsibility of the ministry which prepare the information systems constituting common infrastructure and carry out operation and maintenance, in order to prevent the level of information security for all information systems constituting common infrastructure from being lowered.

ⓒ The information system security officers shall manage records on work related to the operation and maintenance of information system in order to allow for traceability in the event incidents such as wrongful acts or unintended access to information systems occur.

5.2.4 Updating and disposal of information systems

Purpose/significance

When updating or disposing of information systems, it is necessary to prevent highly confidential information recorded on the information systems from being leaked externally during the disposal or recycling processes.

In the event highly confidential information is recorded on information systems or ratings and handling restrictions are not completely understood, it is necessary to implement measures for the total deletion of the recorded information.

Matters to be observed

(1) Measures for the updating and disposal of information systems

ⓐ When updating or disposing of information systems, the information system security officers shall appropriately implement the following measures with regard to the rating and

handling restrictions of the information saved on the relevant information systems.

(I) Information security measures for transfer of information during updates the information systems

(II) Deletion of unnecessary information when disposing of information systems

5.2.5 Review of measures for information systems

Purpose/significance

The environments surrounding information security are ever-changing, and if new threats which emerge are not appropriately responded to, the level of information security will not be able to be maintained. For this reason, it is necessary to periodically review the information security measures for information systems, and carry out timely review when drastic changes occur in external environments.

Matters to be observed

(1) Review of measures for information systems

(a) Information system security officers shall consider review when appropriate based on the status of the appearance of new threats, operation, monitoring, etc., and implement required measures for information security measures for information systems.

5.3 Information system operation continuity plan

5.3.1 Guarantee of the maintenance and coordinated operation of information system operation continuity plan

Purpose/significance

It is necessary to ensure the continuity of work which poses a serious threat to the public safety and benefit if interrupted, even during emergencies, and work continuity plans are established and operated at the ministries accordingly.

Meanwhile, to continue operation of information systems during times of emergency, it is important to examine and establish measures related to information security during emergencies.

It is also necessary to ensure coordination so that there are no inconsistencies between the items prescribed in the work continuity plan and information system operation continuity plan prescribed requirements, and the information security related provision prescribed requirements.

Matters to be observed

(1) Guarantee of the maintenance and coordinated operation of information system operation continuity plan

ⓐ When preparing an operation continuity plan for information systems which support priority work during emergencies at the ministries, the controlling information security officer shall investigate measures for information security during emergencies.

ⓑ When carrying out information system operation continuity plan education and training, and maintenance and improvement, the controlling information security officer shall verify if the measures related to information security during emergencies are operable.

Chapter 6 Information system security requirements

6.1 Information system security functions

6.1.1 Entity authentication functions

Purpose/significance

It is necessary to introduce entity authentication functions in order to prevent information security incidents such as information leaks or destruction, information system outages and so forth from being causes by individuals with no access privileges.

In addition, the users of government agency information systems, for example when providing public oriented services, are not only or always administrative employees. ID codes and entity authentication information should be protected regardless of the type of user, and measures such as information for calling attention, etc. are required.

Matters to be observed

(1) Adoption of entity authentication functions

ⓐ In order to manage access to information, information system security officers shall identify entities, and establish functions for carrying out entity authentication when verification of the correct entity is necessary.

ⓑ In information systems which carry out entity authentication, information system security officers shall implement measures to prevent illegal acts resulting from leaks of entity authentication information etc. and measures against illegal entity authentication attempts.

6.1.2 Access control functions

Purpose/significance

In cases where multiple entities use information systems to access specified information, it is necessary to restrict the relevant information to only those entities which require access for work purposes. As such, it is necessary to give careful consideration to ensure that access controls are appropriately implemented regarding what information is accessible by what entities in information systems.

Matters to be observed

(1) Adoption of access control functions

ⓐ When it is necessary for access to information handled by information systems, to be controlled based on entities, the information system security officers shall establish functions which carry out access control for the relevant information systems.

ⓑ When introducing access control functions, information system security officers shall take

into consideration the strength and convenience of information security, and establish requirements for information security necessary for access control functions such as control based on usage time and terminals used as well as access control based on users or groups to which the users belong.

(2) Implementation of appropriate access control

(a) For information systems where administrative employees are unable to carry out access control by themselves, information system security officers shall appropriately implement access control in accordance with the ratings and handling restrictions of the information saved on the relevant information systems.

6.1.3 Authority management functions

Purpose/significance

As a management function in information systems, in general administrator authority is granted privileges which allow access to all operations. There is concern that in the event the relevant privileges are obtained by malicious third parties etc., the information security functions can be rendered null though leak or falsification of entity authentication information or illegal changes of the settings related to information systems.

As such, it is necessary to adopt authority management functions which assign administrator privileges to only limited entities to prevent illegal usage.

Matters to be observed

(1) Adoption of authority management functions

(a) When it is necessary to carry out entity authentication for the entities using information systems, the information system security officers shall establish functions to manage the authority required for realizing management of the information systems.

(b) When adopting authority management functions, information system security officers shall implement measures to minimize damages in the event administrator privileges are obtained without authorization by malicious third parties etc., and measures to prevent illegal and incorrect internal operations.

(2) Management of the assignment of ID codes and entity authentication information

(a) Information system security officers shall appropriately assign ID codes and entity authentication information to all entities using information systems, and implement measures to ensure appropriate management.

6.1.4 Maintenance and management of logs

Purpose/significance

Information system logs are materials which record system operation history, user access history and other required information and are important tools for detecting illegal intrusions, illegal operations and information security incidents (including signs of such) by malicious third parties etc. In addition, in the event an information security issue occurs related to information systems, the relevant logs serve as important materials for identifying and clarifying issues in ex-post facto investigations. As such, logs must be appropriately maintained for information systems in accordance with specifications and in a manner that prevents the alteration, loss etc. of the logs.

Matters to be observed

(1) Maintenance and management of logs

ⓐ Information system security officers shall maintain and obtain logs for information systems when it is necessary to verify that the information systems are used correctly and to verify that no illegal intrusions or operations, etc. have occurred.

ⓑ Information system security officers shall stipulate the information items to be maintained in logs, log storage periods, log information handling methods from the viewpoint of classified information and response methods in the event logs cannot be acquired or maintained, and carry out appropriate management of logs.

ⓒ Information system security officers shall establish functions for periodically inspecting and analyzing maintained logs, and implement inspections and analysis to determine the presence of items such as any illegal intrusions by malicious third parties etc. or illegal operations.

6.1.5 Encryption and digital signatures

Purpose/significance

Encryption and digital signatures are effective means of preventing leaks and falsification of information handled by information systems, and it is necessary to appropriately incorporate them as functions in information systems.

When adopting encryption and digital signature functions, it is necessary to take into consideration the appropriateness of the algorithms to be used, response methods in the event the relevant algorithm is compromised during operation and appropriate management of key information.

Matters to be observed

(1) Adoption of encryption and digital signature functions

ⓐ Information system security officers shall implement the following measures to prevent

leak and falsification of information handled by information systems.

(I) For information systems handling confidential information, examining the necessity of encryption functions and establishing the said functions if determined necessary.

(II) For information systems handling critical information, examining the necessity of functions for assignment and verification of digital signatures, and establishing the said functions if determined necessary.

(b) Information system security officers shall, after referring to the "e-Government Recommended Ciphers List" for which safety and implementation performance have been verified by the Cryptography Research and Evaluation Committees and related committees (CRYPTREC), stipulate the encryption and digital signature algorithms to be used in information systems, including the following items.

(I) Encryption and digital signature algorithms from the "e-Government Recommended Ciphers List" should be used for encryption and digital signature algorithms to be used by administrative employees when possible.

(II) When adopting encryption and digital signatures for new construction or updating of information systems, unless otherwise absolutely necessary, algorithms listed in the "e-Government Recommended Ciphers List" shall be adopted.

(III) Emergency response procedures shall be stipulated for the possibility of the algorithms used for encryption and digital signature being compromised.

(IV) Management procedures shall be established for decryption of encrypted information and assignment of digital signatures.

(c) Information system security officers shall stipulate algorithms and operation methods for encryption and digital signatures in the ministries which comply with the intent of digital signatures when using digital signatures and the use of Governmental Public Key Infrastructure (GPKI) digital certificates when applicable certificates are available.

(2) Management related to encryption and digital signatures

(a) Information system security officers shall implement the following measures to ensure the use of encryption and digital signatures in appropriate conditions.

(I) In information systems where digital signatures are assigned, information and methods for verifying the validity of digital signatures shall be provided to relying parties through safe methods.

(II) In information systems where encryption is carried out, and where digital signatures are assigned or verified, information regarding the compromise of the algorithms selected for encryption and digital signatures shall be periodically obtained and shared with administrative employees where necessary.

6.2 Measures against information security threats

6.2.1 Measures against software vulnerabilities

Purpose/significance

Potential threats against government agency information systems include attacks such as third party intrusions into information systems resulting in theft or destruction of important government information, and third party disruption of information systems subjecting the systems to excessive loads. Situations where third party intrusions occur in services provided for the public resulting in leakage of personal information are particularly damaging to the public trust in the government.

In general, these types of attacks assume the abuse of software vulnerabilities in the server equipment, terminals and communications line equipment constituting information systems. As such, it is necessary to quickly and appropriate deal with software vulnerabilities in government agency information systems.

In addition, the same type of vulnerabilities can exist in the hardware constituting information systems, so it is necessary to refer to the regulations of 5.2.2 "Information system procurement and construction" and implement required measures.

Matters to be observed

(1) Implementation of measures against software vulnerabilities

ⓐ When installing or commencing operation of server equipment, terminals and communications line equipment, information system security officers shall implement measures against publicly disclosed vulnerabilities in the software used in the relevant devices.

ⓑ At stages where there is no publicly disclosed information concerning vulnerabilities, but there are measures which are applicable to server equipment, terminals and communications line equipment, the information system security officers shall implement the relevant measures.

ⓒ In the event information on vulnerabilities related to the software used on server equipment, terminals and communications line equipment is obtained, the information system security officers shall establish a measure plan for vulnerabilities related to the software and implement measures after taking into consideration the effect on information systems of the application of patches or upgrading software versions.

ⓓ The information system security officers shall periodically verify the status of measures against vulnerabilities in software used on server equipment, terminals, communications line equipment and developed software, and implement measures if it is found that there are vulnerabilities against which no measures are implemented.

6.2.2 Measures against malicious programs

Purpose/significance

If information systems are infected by malicious programs, there are potential threats that the infected information system will be damaged or that the important information stored on the relevant information system will be externally leaked. In addition, information systems infected by malicious programs can be used as springboards to spread infection to other information systems, transmit spam email, carry out denial of service attacks, and be used to carry out targeted attacks, posing a risk of causing damages outside of the relevant information system as well. In order to proactively prevent these types of incidents, it is necessary to appropriately implement measures against malicious programs.

Matters to be observed

(1) Implementation of measures against malicious programs

(a) Information system security officers shall install malicious program removal tool, etc. on server equipment and terminals. However, this shall exclude situations where no such malicious program removal tool, etc. exists which can run on the relevant server equipment and terminals.

(b) Information system security officers shall implement measures using malicious program removal tool, etc. for all assumed potential infection routes for malicious programs.

(c) Information system security officers shall maintain an appropriate awareness of malicious program countermeasure conditions and deal with them accordingly.

6.2.3 Measures against denial of service attacks

Purpose/significance

Potential threats against information systems which can be access from the internet include third party denial of service attacks which prevent the services from being available to users. For this reason, for government agency information systems which can be accessed from the internet, it is necessary to implement measures to ensure the continued availability of the systems in the event of a denial of service attack.

Matters to be observed

(1) Implementation of measures against denial of service attacks

(a) For information systems which handle vital information (Limited to those information systems accessible from the internet. The same hereafter in this section.), information system security officers shall implement measures against denial of service attacks using functions of the server equipment terminals and communications line equipment necessary to provide services or using measures provided by business operators, etc.

(b) For information systems which handle vital information, information system security officers shall construct information systems which include measures for minimizing damages in the event of a denial of service attack.

(c) For information systems which handle vital information, information system security officers shall identify items which should be monitored for server equipment, terminals, communications line equipment and communication lines subject to denial of service attacks and carry out monitoring accordingly.

6.2.4 Measures against targeted attacks

Purpose/significance

Targeted attacks are tenacious attacks which target specific organizations, where after carrying out careful investigation of the relevant organization's work practices and other internal information, a combination of a variety of attack methods is used, optimized for attacking the relevant organization. Typical examples include attack activities where an intrusion is made inside the organization, the scope of the intrusion is expanded and important information is stolen or destroyed. This series of attack activities can also be carried out using as yet unknown methods, so perfect detection and prevention is difficult.

As such, it is necessary to prepare against targeted attacks through a system of multiple protection information security measures consisting of measures to reduce targeted attack intrusions into the organization (gateway measures), and measures for early detection of intrusions, increasing the difficulty of expanding the scope of intrusions, and detection and response of unauthorized external communications (internal measures).

Matters to be observed

(1) Implementation of measures against targeted attack

(a) Information system security officers shall implement measures (gateway measures) to reduce targeted attack intrusions into the organization in information systems.

(b) Information system security officers shall implement measures for the early detection of intrusions, increasing the difficulty of expanding the scope of intrusions, detection of and response to unauthorized external communications (internal measures).

6.3 Creation and provision of applications and content

6.3.1 Measures for the creation of applications and content

Purpose/significance

Applications and content are prepared and widely used throughout the ministries for provision of information, administrative procedures, opinion collection and other administrative services. A decline in the level of information security of user terminals must be avoided when users make used of these applications and content. It is necessary for information security measures to be implemented when the ministries provide applications and content.

It is also necessary for the provisions of 4.1.1 "Outsourcing" to be observed in situations where application and content development and provision is outsourced.

Matters to be observed

(1) Establishment of regulations related to the creation of applications and content

ⓐ The controlling information security officer shall establish regulations for preventing acts which may lead to a decreased level of information security outside of the ministries when providing applications and content.

(2) Establishment of security requirements for applications and content

ⓐ Information system security officers shall include the following in specifications in order to avoid causing a decreased level of information security for information system users outside of the ministries.

(I) The provided applications and content shall not include malicious programs.

(II) The provided applications and content shall not include any vulnerability.

(III) Excepting circumstances where provision of contents in an executable program format is unavoidable, executable program format content shall not be provided.

(IV) If the use of digital certificates or other means of verifying the validity and no modification of the provided applications and content is available, it shall be provided to the applications and content recipients.

(V) Application and content development should be carried out with provision methods stipulated so that there is no requirement for OS or software versions with vulnerabilities to use the applications and content or any other setting changes, or requirements of OS and software users which decreases their level of information security.

(VI) Applications and content should be developed so that they do not include any functions which provides the information of users outside of the ministries or any other privacy related information to third parties against the user's intentions.

ⓑ When administrative employees outsource the development or creation of applications and content, the details of the preceding items shall be included in the procurement

specifications.

6.3.2 Measures for the provision of applications and content

Purpose/significance

Websites or other systems are prepared and provided for use by the public etc. at the ministries for administrative services such as provision of information, administrative procedures and opinion collection. Because these services are generally used via the internet, it is important that the public etc. be able to verify that those services are actually provided by the ministries. In addition, if websites impersonating government agencies are not dealt with, this will result not only in loss of faith in the government agencies, but also lure the public etc. to unauthorized websites where there is a risk of being infected by malicious programs, so it is necessary to implement measures against these types of situations.

Matters to be observed

(1) Use of government domain names

ⓐ Information system security officers shall include in specifications for information systems, the use of .go.jp domain names (hereinafter referred to as "government domain names") in order to allow for users to confirm that websites provided for users outside of the ministries are actually provided by the ministries. However, this shall not apply to the circumstances presented in 4.1.3.

ⓑ When administrative employees outsource the creation of websites aimed at users outside of the ministries, the use of government domain names shall be included in the procurement specifications as stated in the preceding item.

(2) Prevention of luring users to malicious websites

ⓐ Information system security officers shall implement measures to prevent users from being lured to malicious websites impersonating ministry websites via search sites, etc.

(3) Notification of applications and content outside of the ministries

ⓐ The following measures shall be implemented when administrative employees provide notification of applications and content provided by entities outside of the ministries.

(I) The name of the organization managing the applications and content shall be clearly stated.

(II) The date and time the applications and content location validity (linked URL domain name period of validity, etc.) was verified or the period for which the said information is guaranteed.

(III) When sending notification by email, a government domain name email address shall be clearly stated as the point of contact for inquiries related to the notification

details, or a government domain name digital signature shall be added to the notification email.

Chapter 7 Information system components

7.1 Terminals, server equipment, etc.

7.1.1 Terminals

Purpose/significance

When using terminals, there is a risk of saved information being leaked due to external factors such as malicious programs infection or illegal intrusions. In addition, there is also a risk of information security incidents occurring as a result of internal factors such as malicious programs infection resulting from inappropriate usage or negligence by administrative employees. For use of mobile terminals, there is an increased possibility of information leaks resulting from theft, loss or other causes. It is thus necessary to implement measures in consideration of these items.

In addition to the matters to be observed in this section, it is necessary to also observe the terminal related items in the entity authentication, access control, authority management and log management functional measures stipulated in 6.1 "Information system security functions", and the matters to be observed in 6.2.1 "Measures for software vulnerabilities", 6.2.2 "Measures against malicious programs" and 7.3.2 "IPv6 communication lines".

Matters to be observed

(1) Measures for the introduction of terminals

(a) For terminals which handle classified information, information system security officers shall implement measures to protect against physical threats such as terminal theft, unauthorized removal, unauthorized operation by third parties, and surreptitious viewing of display devices.

(b) For mobile terminals handling confidential information outside of areas requiring control measures, information system security officers shall implement measures to prevent information being stolen by third parties in the event the terminal itself is stolen.

(c) In order to prevent increase possibility of potential vulnerabilities as a result of use of various software, information system security officers shall stipulate the software which is approved for use on terminals as well as software for which use is prohibited.

(2) Measures for the operation of terminals

(a) Information system security officers shall carry out periodic review of the software which is approved for use on terminals as well as software for which use is prohibited.

(b) Information system security officers shall periodically investigate the status of all software used on terminals within their jurisdiction, and implement corrective measures in the event any terminals are discovered in unsuitable condition.

(3) Measures for the termination of terminal operation

(a) Information system security officers shall delete all information on terminal electronic media when terminating the operation of terminals.

7.1.2 Server equipment

Purpose/significance

Large quantities of information are often saved on email servers, webservers, file servers and various other server equipment, and as a result the effect of any leak or falsification of the relevant information tends to be more severe than for terminals. In addition, as the functions of server equipment are often used via communication lines, there is a higher potential for malicious programs infection and unauthorized intrusions. In the event that government agency server equipment was ever user as a relay point for unauthorized access or spam email transmission, it would result in a serious loss of faith by the public. Because server equipment is also used by a large number of users simultaneously, the interruption of related functions would result in greater impact. It is thus necessary to implement measures in consideration of these items.

In addition to the matters to be observed in this section, it is also necessary to also observe the server equipment related items in the entity authentication, access control, authority management and log management functional measures stipulated in 6.1 "Information system security functions", and the matters to be observed in 6.2.1 "Measures for software vulnerabilities", 6.2.2 "Measures against malicious programs ", 6.2.3 "Measures for denial of service attacks" and 7.3.2 "IPv6 communication lines". For email servers, webservers and DNS servers in particular, in addition to the common measures noted in this section, the matters to be observed for each in 7.2 "Email, web, etc.", must also be observed.

Matters to be observed

(1) Measures for the introduction of server equipment

(a) For server equipment which handles classified information, information system security officers shall implement measures to protect against physical threats such as server equipment theft, unauthorized removal, unauthorized operation by third parties, and surreptitious viewing of display devices.

(b) In order to prevent incidents where services cannot be provided due to outages, excessive access or other causes for information systems handling vital information stability, information system security officers shall secure availability by using redundant configurations for the server equipment used to provide services and through other means with consideration for future prospects.

(c) In order to prevent increase possibility of potential vulnerabilities as a result of use of various software, information system security officers shall stipulate the software which is approved for use on server equipment as well as software for which use is prohibited.

(d) Information system security officers shall implement measures to prevent the leak of information transmitted and received during maintenance of server equipment through communication lines.

(2) Measures for the operation of server equipment

(a) Information system security officers shall carry out periodic review of the software which is approved for use on server equipment as well as software for which use is prohibited.

(b) Information system security officers shall periodically verify the status of the software and architecture of all server equipment within their jurisdiction, and implement corrective measures in the event any server equipment is discovered in unsuitable condition.

(c) Information system security officers shall implement measures monitoring unauthorized acts, unauthorized access and other unintended occurrences on server equipment. This shall not apply in circumstances where it is deemed unnecessary based on server equipment usage environments or other factors.

(d) For server equipment handling vital information, information system security officers shall implement measures required to restore server equipment to normal operating status, such as creation of backups of information.

(3) Measures for the termination of server equipment operation

(a) Information system security officers shall delete all information on server equipment electronic media when terminating the operation of server equipment.

7.1.3 Multifunction devices and specialized application equipment

Purpose/significance

Devices which include multiple functions of printers, faxes, scanners, copiers, etc., in a single device (hereinafter referred to as "multifunction devices") are used at the ministries. Many multifunction devices are connected to ministry internal communication lines as well as public telephone network and other communication lines for use, and when so connected a variety of services operate including web management screens, file transfer, file sharing, and remote maintenance, so there are a variety of potential threats as well.

In addition, information for specialized purposes, such as video conferencing systems, IP phone systems and network camera systems, is also used at the ministries. In these information systems, in addition to the use of general purpose devices, specialized application equipment particular to the system is also used, and there may be potential threats for the relevant devices based on the characteristics of the devices, the information handled, usage methods, communication connection conditions and other factors.

As such, it is also important to treat multifunction devices and specialized application equipment as information system components, clarify the responsible parties for the devices and implement

appropriate measures.

Matters to be observed

(1) Multifunction devices

ⓐ When procuring multifunction devices, information system security officers shall establish appropriate security requirements for the devices in accordance with the functions the devices are equipped with, the installation environments, ratings and handling restrictions of the information to be handled by the devices.

ⓑ Information system security officers shall appropriately configure the functions the multifunction devices are equipped with as measures against information security incidents which could occur during the operation of the multifunction devices.

ⓒ Information system security officers shall delete all information on multifunction device electronic media when terminating the operation of multifunction devices.

(2) Specialized application equipment

ⓐ For specialized application equipment, information system security officers shall implement measures in accordance with the characteristics of the relevant devices when there are potential threats resulting from the information handled, usage methods, communication connection conditions and other factors.

7.2 Email, web, etc.

7.2.1 Email

Purpose/significance

Transmission and reception of email is the exchange of information, so in addition to risks related to confidentiality, such as information being leaked through inappropriate usage, there are also risks of administrative employees using email being entangled in damages for wrongful acts carried through email abuse, such as impersonation by malicious third parties etc. Appropriate email server management is required in order to avoid these problems.

In addition to the matters to be observed in this section, it is necessary to also observe the matters to be observed related to server equipment in 7.1.2 "server equipment".

Matters to be observed

(1) Measures for the introduction of email

(a) Information system security officers shall configure email servers so that they cannot be used as unauthorized relays for email.

(b) Information system security officers shall prepare functions for entity authentication when email clients send email to and receive email from email servers.

(c) Information system security officers shall implement measures to prevent email impersonation.

7.2.2 Web

Purpose/significance

Webservers which are publicly access on the internet are at constant risk of attack. There is potential for a variety of damages, including alteration of web content (information publicly presented as a web site), webservers being rendered unusable or intrusions into webservers, so it is necessary to combine and implement appropriate measures.

In addition to the matters to be observed in this section, it is necessary to also observe the matters to be observed related to server equipment in 7.1.2 "server equipment".

Matters to be observed

(1) Measures for the introduction of webservers

(a) In the management and configuration of webservers, information system security officers shall implement measures to secure information security which include the following.

(I) Unnecessary functions which the webserver includes shall be stopped or restricted.

(II) The entities responsible for editing web content shall be restricted.

(III) The released web content shall be the minimum required.

(IV) The terminals to be used for editing web content shall be restricted and appropriately managed using ID codes and entity authentication information.

(V) In situations where information related to individual service users is transmitted and other situations where it is necessary to implement measures to prevent the leak of information as a result of tapping during transmission, an authentication function shall be configured using encryption functions or digital certificates.

(b) Information system security officers shall identify information saved on webservers, and verify that no information that is not required for the provision of services is saved on the servers.

(2) Measures for the development and operation of web applications

(a) In the development of web applications, information system security officers shall implement measures for eliminating already known types of web application vulnerabilities. In addition, periodic review shall be conducted of these measures during operation as well to ensure there are no oversights, and appropriate management shall be implemented in the event any oversight is found with the measures.

7.2.3 Domain name system (DNS)

Purpose/significance

A domain name system (DNS: Domain Name System) is a system which serves as network infrastructure by receiving queries from terminals and other clients (DNS clients) and providing a response on the corresponding relationships of domain names, host names and IP addresses. If DNS availability is lost, it will no longer be possible to use web, email and other services which use host names and domain names. In addition, in the event the integrity of the information provided by a DNS is lost and incorrect information is provided, there is potential for damages such as the terminals and other DNS clients being connected to malicious servers. In addition, because a portion of the measures against email impersonation using domains managed by the DNS as addresses are handled by the DNS, the detection of impersonation (spoofed) email will not be possible if this service is not available. Appropriate DNS server management is required in order to avoid these problems.

In addition to the matters to be observed in this section, it is necessary to also observe the matters to be observed related to server equipment in 7.1.2 "server equipment".

Matters to be observed

(1) Measures for the adoption of DNS

(a) For DNS content servers which provide name resolution to information systems which handle vital information, information system security officers shall implement measures to ensure there is no interruption of name resolution.

(b) For DNS caching servers, information system security officers shall implement measures to ensure appropriate response to name resolution queries.

(c) When DNS content servers are used only to provide resolution of names used only by the ministries, information system security officers shall implement measures to ensure the relevant information is not leaked outside the ministries.

(2) Measures for the operation of DNS

(a) When installing multiple DNS content servers, the information system security officers shall maintain consistency between the servers regarding the information related to the managed domains.

(b) Information system security officers shall periodically verify that the domain related information managed on DNS content servers is accurate.

7.3 Communication lines

7.3.1 Communication lines

Purpose/significance

As the vast majority of unauthorized access and denial of service attacks targeting server equipment and client terminals are carried out through the communication lines and communications line equipment connected to the relevant server equipment and terminals, it is necessary to carry out sufficient investigation of risks at the time of construction of the information system and implement required countermeasures. It is necessary to implement the required measures with sufficient regard for the fact that information security risks differ based on the communication line operating entity, such as communications provider public lines and ministry dedicated lines, as well as the physical type of line, such as wired or wireless LAN lines.

In addition, the configuration and conditions of connected information systems for communications lines may differ at the time operation of the information system is started and after the system has been operating for a given period of time, and attack methods are also expected to change, so there is a possibility that the measures estimated at the time of the information system's construction will become insufficient. For this reason, it is important to continually implement measures during the operation of communication lines as well.

Matters to be observed

(1) Measures for the introduction of communication lines

ⓐ During the construction of the communication lines, information system security officers shall select appropriate line types based on the ratings and handling restrictions of the information to be handled by the information systems to be connected to the relevant communication lines, and implement the measures necessary for communication lines to avoid any impact from information security incidents.

ⓑ Information system security officers shall implement functions of access control and route control for server equipment and terminal in communication line.

ⓒ When connecting information systems handling confidential information to communication lines, if it may be necessary to maintain the confidentiality of the communication details, information system security officers shall implement measures allowing for the maintenance of the confidentiality of the communication details.

ⓓ When administrative employees connect information systems to communication lines, even if the relevant information systems are approved for connection, the information system security officers shall implement measures for verification.

ⓔ Information system security officers shall install communications line equipment in areas requiring control measures. However, when installation in areas requiring control measures is difficult, measures shall be implemented to protect from damage by third parties and unauthorized usage, such as implementing physical protection measures.

(f) Information system security officers shall implement measures to allow for the continued operation of communication lines to which information systems handling vital information are connected.

(g) When connecting ministry internal communication lines to the internet, public communication lines and other ministry external communication lines, information system security officers shall implement measures to maintain the information security of the ministry internal communication lines and the information systems connected to the relevant ministry internal communication lines.

(h) Information system security officers shall implement measures for monitoring of details of communications transmitted and received between ministry internal communication lines and ministry external communication lines.

(i) Information system security officers shall stipulate the software required for the operation of the communications line equipment and establish authorization application procedures for any changes to the software. However, this shall not apply for communications line equipment for which changing software is difficult.

(j) Information system security officers shall maintain information security of remote access lines for maintenance and diagnostics.

(k) When using carrier services, information system security officers shall conclude agreements with the operator contracting the construction of the information system as a measure to ensure information security and the service level agreement for the relevant communication lines.

(2) Measures for the operation of communication lines

(a) Information system security officers shall implement measures required to prevent information security incidents during the operation of the communications line equipment.

(b) Information system security officers shall appropriately apply route control and access control and review the route control and access control settings periodically or when there are any changes to the communication lines and communications requirements.

(c) Information system security officers shall periodically investigate the statue of the software required for the operation of the communications line equipment, and implement corrective measures in the event any communications line equipment is discovered in unsuitable condition, such as having unauthorized software installed.

(d) In the event the maintenance of information security for the information systems become difficult, for any communications lines the relevant information systems share with other information systems, in order to protect the other information systems on the shared line, information system security officers shall change the architecture to a separate, independent and exclusive communication line.

(3) Measures for the termination of communication line operation

(a) When operation of communications line equipment is terminated, in order to prevent the

leak of information that was saved during the operation of the communications line equipment which composed the relevant communication lines, when the relevant communications line equipment is reused or disposed of after the termination of operation, the information systems security officers shall implement appropriate measures such as the deletion of all information that was recorded on the electronic media of the relevant communications line equipment.

(4) Measures for introduction of remote access environments

ⓐ When preparing VPN lines, information system security officers shall implement measures required to ensure information security, such as user entity authentication and encryption of communication details.

ⓑ When constructing remote access environments via public telephone networks, information system security officers shall implement measures required to ensure information security, such as user entity authentication and encryption of communication details.

(5) Measures for introduction of wireless LAN environments

ⓐ When constructing ministry internal communication lines using wireless LAN technologies, in addition to common measures for construction of communication lines, information system security officers shall implement encryption of communication routes in order to maintain the confidentiality of communication details, and implement other measures required for the maintenance of information security.

7.3.2 IPv6 communication lines

Purpose/significance

Initiatives are progressing for complying with the internet standard IPv6 communications protocol at government agencies, however the adoption of the IPv6 communication protocol brings with it a number of issues requiring consideration including direct arrival of packets from global IP addresses, and the coexistence of the two protocols during the shift from the IPv4 communications protocol to the IPv6 communications protocol.

In recent years, a large number of server equipment, terminal and communications line equipment products have been released which come standard equipped with communications which utilize IPv6 technology (hereinafter referred to as "IPv6 communications"), and there is the possibility that IPv6 communications that are not intended by operators are occurring on communications networks which as a result pose a risk of being exploited as a means for unauthorized access, so it is necessary to implement required countermeasures.

Further changes are expected for IPv6 technologies in the future, however because the development of information security measures is expected to accompany the propagation of IPv6

technologies, it is important that close observation be carried out at the ministries of IPv6 information security measure related technology trends and these trends be appropriately responded to.

Matters to be observed

(1) Measures related to information systems which carry out IPv6 communications

ⓐ When constructing information systems which will carry out communications using IPv6 technologies, for equipment etc. procured as products, information system security officers shall select ,if possible, Phase-2 IPv6 Ready Logo Program compliant products.

ⓑ For information systems constructed information assuming IPv6 communication based on the characteristics, etc. of IPv6 communication, information system security officers shall carry out verification of threats and vulnerabilities including the following items, and implement required measures.

(I) Threats related to direct arrival via global IP addresses

(II) Threats related to unauthorized access stemming from incomplete IPv6 communication environment settings

(III) Vulnerabilities which occur as a result of process consideration oversights when IPv4 communications and IPv6 communications are implemented concomitantly in information systems

(IV) Vulnerabilities which occur as a result of process consideration oversights in the handling of IPv6 addresses in applications

(2) Monitoring and control of unintended IPv6 communications

ⓐ When connecting server equipment, terminals and communications line equipment to communication lines for which IPv6 communication was not planned, the information system security officers shall implement measures to control IPv6 communications in order to prevent information security threats from unexpected IPv6 communication packet arrival via automatic tunneling functions and unauthorized IPv6 communications received from the relevant lines.

Chapter 8 Information system usage

8.1 Information system usage

8.1.1 Information system usage

Purpose/significance

In addition to administrative processing on terminals, administrative employees use a variety of information systems to carry out administrative affairs, including email and the web. If these systems are not appropriately used, there is a risk of an information security incident occurring.

For this reason, it is necessary to prepare regulations related to information system usage, and ensure administrative employees use the systems in accordance with the said regulations.

Matters to be observed

(1) Establishment of regulations related to information system usage

ⓐ The controlling information security officer shall establish regulations related to information security in regard to use of ministry information systems.

ⓑ For classified information, based on the assumption of information processing outside of the areas requiring control measures, the controlling information security officer shall establish regulations and approval procedures related to safety control measures based on risks such as leakage of information from terminals taken out of areas requiring control measures and from used communication lines.

ⓒ The controlling information security officer shall establish usage procedures related to the handling of information using external electronic media such as USB memory.

(2) Measures to support information system users' observance of regulations

ⓐ Information system security officers shall consider the scope of support from viewpoints of both information security risk and work efficiency, and construct information systems which possess the relevant functions in order to support the administrative employees' observance of regulations.

(3) Basic measures when using information systems

ⓐ Administrative employees shall not use information systems for any purposes other than the execution of administrative affairs.

ⓑ Administrative employees shall not connect the ministries' information systems to any communication lines other than those for which connection is authorized by the information system security officers.

ⓒ Administrative employees shall not connect information systems which are not authorized by the information system security officers to ministry internal communication lines.

ⓓ Administrative employees shall not use software which is prohibited for use on

information systems. In addition, if the use of software other than the authorized software is required for the execution of work, the approval of the information system security officers shall be obtained.

(e) Administrative employees shall implement measures to protect the information systems from unauthorized operations if there is any risk of unauthorized operations by third parties, for example, when leaving the locations where information systems are installed.

(f) When processing information using mobile devices handling classified information, administrative employees shall implement stipulated safety control measures.

(g) When removing information systems handling Confidentiality 3 information, critical information or vital information from areas requiring control measures, administrative employees shall obtain the authorization of the information system security officers or section information security officers.

(4) Measures when using email and web

(a) When sending and receiving email containing confidential information, administrative employees shall use email servers operated or outsourced by the ministries.

(b) When sending information via email to individuals outside of the ministries, administrative employees shall use government domain names for the domain name to be used in the relevant email. However, this shall not apply in cases where the relevant administrative employee is already known to the relevant individual from outside the ministries.

(c) In the event suspicious email is received, the administrative employees shall manage it according to predetermined procedures.

(d) When it is necessary to review the settings of web browsers, administrative employees shall not change any settings which may have an effect on information security.

(e) When downloading software onto server equipment running web clients, or terminals, administrative employees shall verify the distributor of the relevant software using digital signatures.

(f) When entering and submitting confidential information in forms on viewed websites, administrative employees shall verify the following.

(I) That the submitted content is encrypted

(II) That the recipient of information is the organization expected for the relevant website

(5) Handling of ID codes and entity authentication information

(a) Administrative employees shall not use ID codes other than the ID code assigned to them in entity authentication to access information systems.

(b) Administrative employees shall appropriately manage the ID codes assigned to them.

(c) In the event an administrative employee is assigned an ID code with administrator privileges, the employee shall only use the relevant ID code when carrying out work as an administrator.

(d) Administrative employees shall ensure the thorough management of their own entity authentication information.

(6) Measures when using encryption and digital signatures

(a) When encrypting information and when assigning digital signatures to information, administrative employees shall do so in accordance with the prescribed algorithms and methods.

(b) For use of keys used to decrypt encrypted information or assign digital signatures, administrative employees shall carry out usage in accordance with the prescribed key management procedures and appropriately manage the said keys.

(c) For keys used to decrypt encrypted information, administrative employees shall carry out backups of the key in accordance with the prescribed key backup procedures.

(7) Prevention of malicious programs infection

(a) Administrative employees shall strive to implement measures related to malicious programs infection.

(b) In the event an administrative employee discovers that an information system has potentially been infected with malicious program, the employee shall immediately disconnect the information system from any communication lines and implement required measures.

8.2 Use of terminals not provided by the ministries

8.2.1 Use of terminals not provided by the ministries

Purpose/significance

Administrative affairs should be carried out on terminals provided by the ministries. However, there are cases, due to business trips or being out of the office, where use of terminals not provided by the ministries for information processing is unavoidable. In such cases, in the event not information security measures are required of administrative employees because the relevant terminal is not supplied by the ministries, there is a risk that the level of information security for the relevant terminal does not meet the ministry measure standards.

As such, in situations where this is possible, it is necessary for procedures and safety control measure regulations to be established beforehand, and that such usage be carried out under the strict management of the ministries in order to allow for the safe use of terminals not provided by the ministries by administrative employees.

In addition, as maintenance of the same level of information security is required for terminals not supplied by the ministries as for mobile terminals supplied by the ministry, it is necessary to reference 7.1.1 "Terminals", establish regulations and enforce safety control measures to ensure administrative employees implement safety management.

Matters to be observed

(1) Preparation and management of regulations for the use of terminals not provided by the ministries

ⓐ The controlling information security officer shall establish procedures of approval etc. to carry out information processing related to administrative affairs on terminals not provided by the ministries.

ⓑ For confidential information, the controlling information security officer shall establish regulations related to safety control measures for the implementation of information processing carried out on terminals not supplied by the ministries.

ⓒ Information security officers shall appoint a supervisor to manage the implementation status of safety control measures related to information processing of administrative affairs on terminals not provided by the ministries.

ⓓ For terminals not provided by the ministries that will handle confidential information, the supervisor stipulated in the preceding item implement measures to prevent the theft of information resulting from theft or loss of the terminal, or malicious programs infection and ensure the administrative employees appropriately carry out safety control measures.

(2) Measures for the use of terminals not provided by the ministries

ⓐ When carrying out information processing related to administrative affairs using terminals not provided by the ministries, the administrative employees shall obtain the approval of the

supervisor designated in the matters to be observed of 8.2.1(1)(c).

(b) When handling confidential information on terminals not provided by the ministries, administrative employees shall obtain the authorization of the section information security officers.

(c) When carrying out information processing related to administrative affairs on terminals not provided by the ministries, administrative employees shall carry out the said usage in accordance with the procedures stipulated at the ministries and in accordance with the safety control measures.

(d) When information processing objectives have been completed, administrative employees shall erase confidential information from terminals not provided by the ministries.