NISD-K305-111

Technical Standards for Information Security Measures for the Central Government Computer Systems

April 18, 2012

Established by the

Information Security Measures Promotion Council

Table of Contents

Chapter 2.1 General

2.1.1.1 Positioning of Technical Standards for Measures

(1) Positioning of these Technical Standards for Measures as an enhancement of Information Security Measures for the Central Government Computer Systems

As described in the Management Standards for Information Security Measures for the Central Government Computer Systems (hereinafter referred to as the "Management Standards for Measures").

(2) Revising these Technical Standards for Measures

As stipulated in the Management Standards for Measures.

(3) Compliance with laws and regulations

As stipulated in the Management Standards for Measures.

2.1.1.2 How to use Technical Standards for Measures

(1) Structure

As stipulated in the Management Standards for Measures.

(2) Itemized measures

As stipulated in the Management Standards for Measures.

(3) Changes concerning "setting security levels

As stipulated in the Management Standards for Measures.

2.1.1.3 Classification of Information and Types of Marking

(1) Classification and marking

As stipulated in the Management Standards for Measures.

(2) Classification

As stipulated in the Management Standards for Measures.

(3) Types of marking

As stipulated in the Management Standards for Measures.

2.1.1.4 Control and Usage Restrictions in Information Handling Areas

(1) Information handling areas

As stipulated in the Management Standards for Measures.

(2) Classification of Information Handling Areas

As stipulated in the Management Standards for Measures.

(3) Management and Usage Restrictions in Each Class of Information Handling Areas

As stipulated in the Management Standards for Measures.

(4) Individual Control and Individual Usage Restrictions in a Secure Area

As stipulated in the Management Standards for Measures.

2.1.1.5 Evaluation Procedure

As stipulated in the Management Standards for Measures.

2.1.1.6 Definition of Terms

As stipulated in the Management Standards for Measures.

The following terms additionally appear in these Technical Standards for Measures.

【A】

- "Announced security hole" means a publically known security hole which has been announced by software or hardware manufacturers or vendors, or by security-related organizations such as the JPCERT Coordination Center.

【D】

- "Delivery personnel" means a person who receives items from, or passes items to employees. Such as of courier services and delivery of office equipment, etc.

【M】

- "Mobile terminals" mean terminals which can be moved as required for business purposes regardless of the shape of the terminal. A terminal that is used only at a specific location is not classified as a mobile terminal.
- "Multiple factors authentication / composite authentication" is an authentication method which uses a combination of multiple methods.

Chapter 2.2 Measures based on Clarifying Information Security Requirements

2.2.1 Information Security Functions

2.2.1.1 Authentication Functions

Compliance Requirements

(1) Introducing authentication functions

(a) For information systems which are deemed to require authentication, information system security officers must provide functions for identification and authentication.

(b) For information systems which are deemed to require authentication and secrecy of the authentication information, information system security administrators must protect authentication information from disclosure.

(i) Authentication information must be encrypted when it is stored.

(ii) Authentication information must be encrypted when it is transmitted.

(iii) If authentication information cannot be encrypted when it is stored or transmitted, the user must be notified so whenever the user sets, changes, or provides (enters) his/her own authentication information.

(c) For information systems which are deemed to require authentication and periodical change of authentication information, information system security officers must establish a function to periodically prompt users to change authentication information and one of the following additional functions.

(i) A function to check whether the user changes his/her authentication information periodically

(ii) A function to refuse continued use of the information system if the user does not change his/her authentication information periodically

(d) For information systems which are deemed to require authentication and measures against the possibility where their authentication information storage device may be accessed by third parties, information system security officers must establish a function to stop authentication using the given authentication information or given authentication information storage device, or to stop the use of information systems which use the compromised identification code.

(e) For information systems which are deemed to require authentication and deploy knowledge-based authentication, information system security officers must establish the following functions.

(i) A function to let the users set their own authentication information

(ii) A function to protect authentication information set by users from disclosure to others.

(iii) A function to ask users to set the specified security strength level or higher.

(f) For information systems which are deemed to require authentication and deploy an authentication method other than knowledge-based, ownership-based, or biological means, the information system security officer must implement an authentication method which meets all the applicable requirements in the following according to its characteristics.

(i) It must not authenticate illegitimate subjects (prevention of false acceptance).

(ii) It must not reject legitimate subjects by any reasons which are not the subject's fault (prevention of false rejection).

(iii) Legitimate subjects must not be able to grant (also issue, renew, or change; hereinafter the same in this section) or lend their authentication information to other parties easily (prevention of impersonation).

(iv) The authentication information must not be easily copied (prevention of reproduction).

(v) There must be means to disable individual logon at the discretion of the information system security administrator (assurance of invalidation).

(vi) Authentication must be functional whenever required without disruption (assurance of availability).

(vii) If any information or device needs to be supplied from an external source in order to add new subjects, the supply must be sufficient throughout the information system's lifetime (assurance of continuity).

(viii) The authentication information must re-issuable to the legitimate subject in a secure manner if the previously granted authentication information becomes unusable (assurance of re-issuance).

(g) For information systems which are deemed to require authentication, information system security officers must consider whether it is necessary to provide each of the following functions, and if it is deemed necessary, implement them.

(i) A multiplefactor (composite) authentication function.

(ii) A function which notifies the logon user information on the previous logon.

(iii) A function which detects or prevents illegal logon attempts.

(iv) A function which displays a notification about the use of the given information system before the user logs in to the information system.

(v) A function which prevents users from re-using the same authentication information when prompting the user for periodical change of the authentication information.

(vi) A function which requires the users to log on using individual ID codes before logging in using the shared ID code when required authentication and share an ID code with administrative permissions, information system security officers must establish.

2.2.1.2 Access Control Functions

Compliance Requirements

(1) Introducing access control functions

(a) For information systems which are deemed to require access control, information system security officers must establish a function to provide access control.

(b) For information systems which are deemed to require access control, information system security officers must consider whether it is necessary to provide each of the following functions, and if it is deemed necessary, implement them.

(i) Access control based on attributes other than those of the user and groups of which the user is a member.

(ii) Mandatory access control function.

(2) Configuring access control

(a) For information systems whose access control cannot be established by employees themselves, information system security officers must establish access control according to the Classification and marking of the information stored in the given information system.

2.2.1.3 Administrative Functions

Compliance Requirements

(1) Introducing administrative functions

(a) For information systems which are deemed to require administration, information system security officers must establish an administrative function.

(b) For information systems which are deemed to require administration, information system security officers must consider whether it is necessary to provide each of the following functions, and if it is deemed necessary, implement them.

(i) A least privilege function.

(ii) A function which re-issues authentication information automatically.

(iii) A dual locking function.

(2) Granting and managing identification codes and authentication information

(a) Administrators must issue identification codes and authentication information only to the subject who is permitted to use the information system.

(b) When an administrator issues an identification code, he/she must notify the user whether the code is shared or not.

(c) If administrators grant (issue, renew, or change; hereinafter the same in this section) an identification code with administrative permissions, they must take the following measures.

(i) Only when such permissions are required for the business or business responsibilities.

(ii) If it is possible, changing the identification code from the initial setting.

(iii) If it is possible, changing the authentication information from the initial setting.

(iv) Restricting logging in from a network.

(d) Administrators must disable the identification code of the employee when he/she no longer requires the information system. Also, administrators must check for unnecessary identification codes when adding or deleting identification codes due to personnel changes, etc.

(e) Administrators must make sure the loaned authentication information storage device is returned from the employee when he/she no longer requires the information system.

(f) Administrators must configure access control to grant the minimum necessary permissions for the given business responsibilities and needs. Also, administrators must check for inappropriate access control settings when adding or deleting identification codes due to personnel changes, etc.

(g) Administrators must consider whether it is necessary to take each of the following measures, and if it is deemed necessary, implement the measures.

(i) Granting each employee only one identification code for a single information system

(ii) Obtaining permission from the information security officer before recording which identification code was granted to who, and erasing such a record

(iii) Prohibiting a person from granting an identification code granted to him or her to another person

(h) Administrators must grant only one identification code per employee for a single information system.

(i) Administrators must record which identification code is granted to which subject. Administrators must obtain permission from their information system security officer in advance when deleting the record.

(j) Administrator must not re-use an identification code for another subject.

2.2.1.4 Audit Trail Management Functions

Compliance Requirements

(1) Introducing audit trail management functions

(a) For information systems which are deemed to require audit trails, information system security officers must establish a function which obtains the audit trails.

(b) For information systems for which the information system security officer deems to require audit trails, the information system security officer must define measures against the cases where audit trails cannot be or may not be obtained, and establish functions to apply these measures to the information systems as necessary.

(c) For information systems for which the information system security officer deems to require audit trails, the information system security officer must establish access control on the obtained audit trails to prevent illegal deletion, falsification, and access.

(d) For information systems which the information security officer deems to require audit trails, the information system security officer must consider whether it is necessary to provide each of the following functions, and if it is deemed necessary, implement them.

(i) A function which automatically checks, analyzes and report the audit trails for the information systems.

(ii) A function which immediately notifies the monitoring personnel when any indication of possible information security infringement is detected from the obtained audit trails for the information systems.

(2) Obtaining and keeping the audit trails

(a) For information systems for which the information system security officer deems to require audit trails, the information system security administrator must obtain the audit trails using the function established for those information systems.

(b) For information systems for which the information security officer deems to require audit trails, the information system security administrator must keep the obtained audit trails until the expiry date and delete them without delay where the expiry date does not need extended.

(c) For information systems for which the information security officer deems to require audit trails, the information system security administrator must take designated measures when the audit trails cannot be or may not be obtained.

2.2.1.5 Assurance Functions

Compliance Requirements

(1) Introducing assurance functions

(a) For information systems which are deemed to require assurance measures, information system security officers must establish the assurance functions.

2.2.1.6 Encryption and Electronic Signatures (including Key Management)

Compliance Requirements

(1) Introducing encryption and electronic signature functions

(a) For information systems which handle confidential information (except written documents; hereinafter the same in this section), information system security officers must consider whether an encryption function are required.

(b) For information systems which are deemed to require encryption, information system security officers must establish an encryption function.

(c) For information systems which handle confidential information, information system security officers must consider whether a function to add and verify electronic signatures is required.

(d) For information systems which are deemed to require electronic signatures, information system security officers must establish a function to add and verify electronic signatures.

(e) For information systems which are deemed to require encryption or electronic signatures, information system security officers must consider whether it is necessary to provide each of the following functions, and if it is deemed necessary, implement them.

(i) Encryption module in replaceable components.

(ii) Configuration with selectable algorithms.

(iii) Selecting "Encryption Module Testing and Certification Scheme" certified products in order to use products that properly implement the selected algorithm by software or hardware, and protect the key and authentication information used for decoding encrypted information or granting digital signature.

(iv) Storing the key and authentication information used for decoding encrypted information or granting digital signatures in a tamper-proof encryption module.

(2) Management concerning encryption and electronic signatures

(a) For information systems which are deemed to require electronic signatures, information

system security officers must provide the information or means to validate the electronic signature to the relying party.

(b) For information systems which are deemed to require encryption or electronic signatures, information system security officers must obtain information on how the algorithm selected for the given system may be compromised where necessary.

2.2.2 Threats to Information Security

2.2.2.1 Security Holes

Compliance Requirements

(1) Implementing information systems

(a) Information system security officers must apply measures against announced security holes associated with the software deployed on the computer or communication equipment when it is installed or starting to operate (excluding computers and communication equipment with no announced security holes; hereinafter the same in this section).

(b) Information system security officers must take measures, if available, for computers and communication equipment even when they have no announced security holes.

(2) Operating information systems

(a) Information system security administrators must obtain information on the announced security holes associated with the software deployed on computers and communication equipment under his/her management as required.

(b) When an information system security officer obtains information on security holes associated with the software deployed on computers or communications equipment under his/her management, the information system security officer must analyze the risks the security holes imposes on the information system, determine the following items, and formulate measures against the security hole.

(i) Necessity of measures

(ii) Methods

(iii) Temporary workaround if there is no method available

(iv) Effects of measures or temporary workaround on the information system

(v) Measure implementation plan

(vi) Necessity of testing measures

(vii) Method for testing measures

(viii) Measure test plan

(c) Information system security administrators must take measures against security holes based on the measure implementation plan.

(d) Information system security administrators must record the items such are the implementation date, work description, and persons in charge when taking the measures against the security hole.

(e) Information system security administrators must obtain a file such as a patch or upgraded

software, etc. to plug the security hole (hereinafter referred to as "security update file") through a reliable source. Also, they must validate the security update file if an integrity validation procedure is provided.

(f) Information system security administrators must investigate and analyze measures for security holes and software configurations periodically and take measures if any computer or communication equipment is in an inappropriate condition.

(g) Information system security officers must share the obtained information and measures associated with security holes with other information system security officers as required.

2.2.2.2 Malware

Compliance Requirements

(1) Implementing information systems

(a) Information system security officers must install antivirus software, etc. on computers (except for computers on which no antivirus software can operate; hereinafter the same in this section.)

(b) Information system security officers must take measures against malware by using antivirus software, etc. for all possible infection routes.

(c) Information system security officers must consider whether it is necessary to install a combination of antivirus software of different types on possible infection routes of malware, and if it is deemed necessary, install the software.

(d) Information system security officers must consider whether it is necessary to take measures to prevent malware from spreading on possible infection routes, and if it is deemed necessary, implement the measures.

(2) Operating information systems

(a) Information system security administrators must try to collect information on malware, determine whether any measures are required, and instruct employees to take measures where necessary.

(b) Information system security officers must confirm and review the status of measures against malware as appropriate.

2.2.2.3 Denial of Service Attacks

Compliance Requirements

(1) Implementing information systems

(a) For information systems which handle vital information (limited to information systems with computers, communication equipment, or communication lines which are accessed via the Internet; hereinafter the same in this section), information system security officers must use the functions, that are implemented on the computers or communication equipment to provide services, to protect the system from denial of service attacks.

(b) For information systems which handle vital information, information system security officers must design the systems to minimize the impact of denial of service attacks.

(c) For information systems which handle vital information, information system security officers must identify the monitoring scope among computers, communication equipment, and communication lines which may suffer denial of service attacks, and define the monitoring procedure and the retention period of the monitoring records.

(d) For information systems which handle vital information, information system security officers must establish the response procedure and communication system with the communications service provider who provides the Internet connection, on assumption where measures on computers and communication equipment are not sufficient to avoid denial of service attacks with a large number of access.

(e) For information systems which handle vital information, information system security officers must consider whether it is necessary to implement devices to eliminate or mitigate the impact of denial of service attacks on the computers, communication equipment, or communication lines, and if it is deemed necessary, implement them.

(f) For information systems which handle vital information, information system security officers must consider whether it is necessary to secure the means to effectively apply measures against denial of service attacks, and if it is deemed necessary, secure them.

(g) For information systems which handle vital information, information system security officers must consider whether it is necessary to provide redundancy for computers, communication equipment or communication lines that are required to provide services, and if it is deemed necessary, provide it.

(2) Operating information systems

(a) For information systems which handle vital information, information system security administrators must monitor the computer, communication equipment, and communication line in accordance with the monitoring procedure and keep the monitoring records if the

monitoring procedure is defined.

2.2.2.4 Stepping Stone

Compliance Requirements

(1) Implementing information systems

(a) Information system security officers must take measures to prevent information systems (limited to information systems with computers, communication equipment or communication lines which are connected to communication lines external to the government facility such as Internet; hereinafter the same in this section) from being used as a stepping stone.

(b) Information system security officers must design the information systems to minimize the impact of the system being used as the stepping stone.

(c) Information system security officers must consider whether it is necessary to define the monitoring procedure to determine whether information systems are being used as a stepping stone, and the retention period of the monitoring records, and if it is deemed necessary, define it.

(2) Operating information systems

(a) For information systems that require monitoring, information system security administrators must monitor them in accordance with the monitoring procedure and keep monitoring records.

2.2.2.5 Measures against Targeted Attacks

Compliance Requirements

(1) Implementing information systems

(a) Information system security officers must take measures to prevent invasion and spread of malware caused by targeted attacks on information systems.

(b) Information system security officers must take measures to prevent information systems connected to communication lines external to government agencies such as the Internet from being used for targeted attacks.

(2) Operating information systems

(a) Information system security officers must take measures to prevent invasion and spread of malware caused by targeted attacks on information systems.

Chapter 2.3 Measures for Information System Components

2.3.1 Facilities and Environment

2.3.1.1 Control and Usage Restrictions of Information Handling Areas by Class

Compliance Requirements

(1) Measures for restricting entry

(a) Area information system security officers must take the following measures for each class according to Annex 1 to restrict entry. When determining individual control measures, these measures must also be considered.

(i) Measures for preventing suspicious individuals from entering Information Handling Areas.

(ii) Measures for physically isolating the Information Handling Areas and take measures to manage entry and exit for information systems that handle classified information.

(2) Measures for permitting entry

(a) Area information system security officers must take the following measures for each class according to Annex1 to permit entry. When determining individual control measures, these measures must also be considered.

(i) Measures for confirming that persons entering an area requiring control measures are persons permitted entry.

(ii) Measures for confirming that persons exiting from an area requiring control measures are persons permitted entry.

(iii) Measures for preventing a person permitted entry from letting persons not permitted entry enter an area requiring control measures and exit from the area.

(iv) Measures for permitting entry to persons who regularly enter.

(v) Establishing procedures for making changes in persons permitted regular entry.

(vi) Measures for recording and monitoring all persons entering and exiting from areas requiring control measures.

(3) Measures for Managing Visitors

(a) Area information security officers must take the following measures for each class according to Annex 1 to manage visitors. When determining individual control measures, these measures must also be considered.

(i) Measures for confirming the name, organization, purpose of the visit, and the name

and department of the employee who receives the visit.

(ii) Measures for recording the name, organization, purpose of the visit, the name and department of the employee who receives the visit, the date of the visit, and the time of entry and exit.

(iii) Establishing a procedure for the visited employee to examine whether the visitor may enter the area requiring control measures

(iv) Measures for restricting the area where the visitors may enter.

(v) Measures for ensuring that the visited employee accompanies the visitor in the secure area.

(vi) Measures for visually distinguish visitors and persons who are authorized regular entry.

(4) Securing computers and communication equipment

(a) For information systems that handle classified information, area information security officers must take the following measures for each class according to Annex 1 to prevent theft and illegal removal of computers and communication equipment that are installed and used at a specific location. When determining individual control measures, these measures must also be considered.

(b) For information systems that handle classified information, area information security officers must take the following measures for each class according to Annex 1 to manage the installation of computers and communication equipment. When determining individual control measures, these measures must also be considered.

(i) Measures for physically isolating the Information Handling Areas where computers and communication equipment are installed.

(ii) Measures for protecting display devices of computers and communication equipment from others' eyes.

(iii) Measures for protecting cables including power cables and communication cables from threats such as damage and eavesdropping.

(iv) Measures against information leakage caused by electromagnetic waves emitted from information systems.

(5) Measures for managing works

(a) Area information security officers must take the following measures for each class according to Annex 1 to monitor works in an area requiring control measures. When determining individual control measures, these measures must also be considered.

(6) Measures for restricting entry

(a) Employees must always be able to be identified in areas requiring control measures.

(7) Measures for restricting carrying in, out, and using items

(a) Area information security officers must take the following measures for each class according to Annex 2 as usage restriction measures on carrying in and out items related to information systems handling classified information. When determining individual control measures, these measures must also be considered.

(i) Measures for carrying in and out items related to information systems.

(ii) Preserving records on carrying in and out items related to information systems.

(iii) Restricting carrying computers, communication equipment, electromagnetic storage media, and storage equipment (including those recording voice, video, and images) into an area requiring control measures.

(b) When taking pictures, shooting video, or making voice recordings, the employee must obtain or request permission from the area information security officer for each class according to Annex 2. When determining individual usage restriction measures, individual usage restriction must also be imposed.

(8) Measures for restricting parcels

(a) Area information security officers must take the following measures for each class according to Annex 2 when passing to or receiving from delivery service. When determining individual control measures, these measures must also be considered.

(9) Measures against disasters and failures

(a) For information systems that handle classified information, area information security officers must take physical measures to protect computers and communication equipment from natural and artificial disasters.

(b) For information systems that handle classified information, area information security officers must take measures to shut down the power supply to computers and communication equipment after ensuring the safety of employees when necessary when disaster or failure occurs.

2.3.2 Computers

2.3.2.1 Common Measures for Computers

Compliance Requirements

(1) Installing computers

(a) For computers which handle vital information, information system security officers must obtain computers with considerations to the required system performance including the future perspective.

(b) For information systems which handle classified information, information system security officers must locate computers in areas requiring control measures. However, this is not required for mobile terminals approved by the information system security officer.

(c) For information systems which handle vital information, information system security officers must examine whether redundancy configuration is required for computers which provide services, and must establish the redundancy configuration for the given computers.

(d) Information system security officers must define the software that can be used on the computer and the software that cannot be used.

(2) Operating computers

(a) Employees must not use computers for any purposes other than business purposes.

(b) Employees must take measures to protect computers from illegal operations while they are away from their desks.

(c) Employees must not use software that is prohibited on the computer. If it is necessary to use software that has not been specified as software permitted on the computer, approval from the information system security officer must be obtained.

(d) Information system security officers must periodically examine the state of all software products used on computers under their management and consider whether it is necessary to make improvements on computers which are in an inappropriate condition, and if it is deemed necessary, take actions.

(3) Disposing of computers

(a) Information system security officers must erase all the information on electromagnetic storage media in the computer when disposing of a computer.

2.3.2.2 Terminals

Compliance Requirements

(1) Installing terminals

(a) For mobile terminals which handle classified information, information system security officers must enable the same protective measures as for terminals used within areas requiring control measures, even when the mobile terminals are used outside areas requiring control measures.

(b) Employees must obtain approval from their information system security officer to use mobile terminals.

(c) For mobile terminals which handle confidential information, information system security officers must provide an encryption function for information stored in electromagnetic storage media.

(d) For mobile terminals which handle classified information, information system security officers must define measures to prevent theft and to mitigate damage caused by the theft.

(e) Information system security officers must consider whether it is necessary to build information systems using terminals on which employees cannot save information, and if it is deemed necessary, take pertinent measures.

(2) Operating terminals

(a) Employees must take measures to prevent theft when using mobile terminals which handle classified information.

(b) When taking mobile terminals which handle confidential information out of areas requiring control measures, employees must examine whether they should encrypt the confidential information in the electromagnetic storage media in the mobile terminal, and encrypt the information if it is deemed necessary.

(c) Employees must not connect terminals to any communication lines other than those approved by their information system security officer.

(d) Information system security administrators must consider whether it is necessary to synchronize terminal clocks with the standard time of information systems, and if it is deemed necessary, take pertinent measures.

2.3.2.3 Servers

Compliance Requirements

(1) Installing servers

(a) When maintenance work on servers is carried out via a communication line, information system security officers must examine whether the communications should be concealed, and establish a function to conceal transmitted information if it is deemed necessary. Communications must be concealed if the maintenance work is carried out via a communication line external to the government facility.

(b) Information system security administrators must consider whether it is necessary to establish either load distribution or server redundancy configuration for servers which provide services while handling vital information, and if it is deemed necessary, take pertinent measures.

(2) Operating servers

(a) Information system security officers must confirm configuration changes on servers periodically. Also, they must identify the impact of such changes on the servers and take measures.

(b) For servers which handle vital information, information system security administrators must take necessary measures to restore them.

(c) Information system security administrators must record operations and management of servers such as the date of the work, the server, work descriptions, and the engineer.

(d) Information system security administrators must synchronize server clocks with the standard time of information systems.

(e) Information system security administrators must consider whether it is necessary to monitor the security status of servers, and if it is deemed necessary, take pertinent measures.

(f) For servers which handle vital information, information system security administrators must consider whether it is necessary to monitor the system status, and if it is deemed necessary, take pertinent measures to detect any failures.

2.3.3 Application Software

2.3.3.1 E-mail

Compliance Requirements

(1) Introducing e-mail services

(a) Information system security officers must configure e-mail servers not to relay unsolicited e-mails.

(b) Information system security officers must provide a function which authenticates employees for sending and receiving e-mails from e-mail clients to and from e-mail servers.

(c) Information security officers must take measures to prevent email address spoofing.

(2) Operating e-mail services

(a) Employees must use e-mail services which are provided by their government agencies or outsourced e-mail servers when sending and receiving e-mails containing business information. However, this is not applicable to those who have obtained approval for information processing by external information systems.

(b) Employees must display received e-mail contents in the way where scripts are not executed on the computer.

2.3.3.2 Web

Compliance Requirements

(1) Introducing web servers

(a) Information system security officers must configure security settings on web servers appropriately. Measures including the following must be applied as appropriate security functions.

(i) Appropriately restrict functions of web servers.

(ii) Appropriately configure access control on information stored on web servers.

(iii) Appropriately manage identification codes.

(iv) Examine risks of information leakage by communication eavesdropping, and provide an authentication function by encryption and electronic certificate where it is deemed necessary.

(b) For information systems which handle confidential information, information system

security officers must identify information to be stored on web servers and confirm no confidential information other than the identified information is stored on these web servers.

(2) Developing web applications

(a) Information system security officers must assure appropriate information security by establishing a function to include security measures in web application development. Measures including the following must be applied as appropriate security functions.

(i) Do not prevent users from checking URL.

(ii) Appropriately carry out authentication and access control.

(iii) Restrict file paths which are used by web applications.

(iv) Remove any illegal input data.

(v) Remove any illegal output data.

(vi) Implement safe session management.

(3) Operating web services

(a) Employees must configure security on web clients appropriately to assure information security.

(b) Employees must check the distributor of the software using electronic signatures when downloading software on a computer running a web client.

(c) Employees must confirm the following when they upload confidential information to an online form displayed on a website.

(i) The information is encrypted.

(ii) The website is legitimately the one provided by the assumed organization.

(d) Information system security officers must consider whether it is necessary to restrict external websites which can be viewed by employees, and if it is deemed necessary, take pertinent measures, and review the restriction periodically.

2.3.3.3 Domain Name System (DNS)

Compliance Requirements

(1) Introducing DNS

(a) Information system security officers must take measures against stoppage of name resolution on the DNS content server which provides the name resolution service of information systems which handle vital information.

(b) Information system security officers must define a procedure to operate and manage the domain information stored on the DNS content server.

(c) Information system security officers must take measures on the DNS cache server to maintain appropriate response to name resolution requests.

(d) Information system security officers must take measures on the DNS content server to prevent information leakage through the name resolution service when resolving the names which are internal use only.

(e) For DNS servers which provide name resolution service to important information systems, information system security officers must consider whether it is necessary to configure the content server to add electronic signatures when providing domain name information, and the cache server to verify the electronic signatures when resolving names, and if it is deemed necessary, take pertinent measures.

(2) Operating DNS

(a) Information system security officers must maintain consistency of domain information among servers when installing multiple DNS content servers.

(b) Information system security officers must verify the domain information on the DNS content server as necessary according to the operational and management procedures of domain information.

2.3.4 Communication Lines

2.3.4.1 Common Measures for Communication Lines

Compliance Requirements

(1) Implementing communication lines

(a) Information system security officers must examine the associated risks before implementing communication lines.

(b) For information systems which handle vital information, information system security officers must examine and ensure capabilities of the communication lines and communication equipment to provide required communication performance including the future perspective.

(c) Information system security officers must define software products necessary for communication equipment to operate. However, this is not applicable for communication equipment whose software is difficult to replace.

(d) Information system security officers must group computers that are connected to communication lines and separate them on the communication line.

(e) Information system security officers must examine purposes of communications between the grouped computers, assign communication equipment according to the purposes, and establish access control and route control.

(f) For information systems which handle confidential information, information system security officers must examine whether the communications should be concealed, and establish a function to conceal communications if it is deemed necessary.

(g) For information systems which handle classified information, information system security officers must examine physical security of lines for communications and select appropriate communication lines.

(h) Information system security officers must ensure security of connections of communication equipment which are used for remote maintenance and diagnosis services.

(i) Information system security officers must install communication equipment in areas requiring control measures.

(j) Information system security officers must resolve the security level and service level at the contract exchange when using leased line services provided by telecommunications carriers.

(k) For information systems which handle vital information, information system security officers must examine whether redundancy configuration is required for communication lines and communication equipment which provide services, and must establish the

redundancy configuration for the given communication lines and communication equipment.

(l) Information system security officers must consider whether it is necessary to authenticate the communicating computers, and if it is deemed necessary, take pertinent measures.

(2) Operating communication lines

(a) Information system security administrators must obtain approval from the information system security officer when changing software on communication equipment.

(b) Information system security administrators must record operations and management of communication lines and communication equipment such as the date of the work, the given communication lines and equipment, and the engineer.

(c) If a situation arises where ensuring information system security is difficult, the information system security officer must change the configuration from sharing a communication line with other information systems to using a separate and closed communication line.

(d) Employees must not connect computers and communication equipment to communication lines without approval from their information system security officer.

(e) Information system security administrators must synchronize clocks on communication equipment with the standard time of information systems.

(f) For information systems which handle vital information, information system security officers must take measures to restore the operational status of the communication equipment.

(g) Information system security officers must consider whether it is necessary periodically examine the state of all software products required for operations of communication equipment under their management and make improvements on communication equipment which are in an inappropriate condition, and if it is deemed necessary, take pertinent measures. However, this is not applicable for communication equipment whose software is difficult to replace.

(h) Information system security administrators must take measures to protect communication equipment from illegal operations.

(3) Disposing of communication lines

(a) Information system security officers must erase all the information on electromagnetic storage media in the communication equipment when disposing of communication equipment.

2.3.4.2 Management of Communication Lines in the Government Facilities

Compliance Requirements

(1) Implementing communication lines in government facilities

(a) Information system security officers must consider whether it is necessary to take measures to confirm that the computer is approved for connection to a communication line before logically connecting it to the communication line after physically connecting it to the communication line, and if it is deemed necessary, take pertinent measures.

(2) Operating communication lines in government facilities

(a) Information system security officers must review the access control configurations periodically and at changes in communication requirements.

(b) For information systems which handle vital information, information system security administrators must consider whether it is necessary to confirm and analyze the utilization and status of communication lines daily to measure or detect degradation or abnormality in the communication lines, and if it is deemed necessary, take pertinent measures.

(c) Information system security administrators must consider whether it is necessary to monitor the information that is sent or received via communication lines in the government agency, and if it is deemed necessary, take pertinent measures.

(3) Measures on communication lines

(a) When implementing a VPN environment, information system security officers must examine whether measures including the following are required and take measures if it is deemed necessary.

(i) Establishing the application procedures for commencing and terminating the use

(ii) Encrypting the information

(iii) Identifying the communicating computers or authenticating the users

(iv) Obtaining and managing the authentication records

(v) Restricting the scope of communication lines which are accessible via VPN

(vi) Assuring the confidentiality of the VPN connection method

(vii) Managing the computers which use VPN

(b) When implementing a wireless LAN environment, information system security officers must examine whether measures including the following are necessary, and take measures if they are deemed necessary. Communications must be encrypted if the wireless LAN environment handles confidential information.

(i) Establishing the application procedures for commencing and terminating the use

(ii) Encrypting the information
(iii) Identifying the communicating computers or authenticating the users
(iv) Obtaining and managing the authentication records
(v) Restricting the scope of communication lines which are accessible via the wireless LAN
(vi) Prohibiting connections with others communication lines while being connected to the wireless LAN
(vii) Assuring the confidentiality of the wireless LAN connection method
(viii) Managing the computers and communication equipment which are connected to the wireless LAN

(c) When implementing a remote access environment using public telephone networks, information system security officers must examine whether measures including the following are required, and take measures if it is deemed necessary.
(i) Establishing the application procedures for commencing and terminating the use
(ii) Identifying and authenticating the communicating users or caller numbers
(iii) Obtaining and managing the authentication records
(iv) Restricting the scope of communication lines which are accessible by remote access connections
(v) Prohibiting connections with other communication lines while in remote access
(vi) Assuring confidentiality of the remote access method
(vii) Managing the computers which is used for remote access

2.3.4.3 Connecting to Communication Lines Outside the Government Facilities

Compliance Requirements

(1) Connecting internal lines to external lines

(a) Information system security officers must obtain approval from the information security officer to connect a communication line inside the government facility to a communication line outside the government facility.

(b) If an information system security officer determined that information system security cannot be assured if a communication line inside the government facility is connected to a communication line outside the government facility, he/she must implement a communication line inside the government facility separate from other internal communication lines which are shared with other information systems, or separate from external lines.

(2) Operating communication lines inside the government facilities which are connected to communication lines outside the government facilities

(a) If a situation arises where ensuring information system security is difficult, the information system security officer must change the configuration from an internal communication line which is shared with other information systems, or an external line, to a separate communication line.

(b) Information system security officers must review the access control configurations periodically and at changes in communication lines.

(c) For information systems which handle vital information, information system security administrators must confirm and analyze the utilization and status of communication lines daily to measure or detect degradation or abnormality in the communication lines.

(d) Information system security administrators must monitor the information that is sent or received between communication lines inside the government facilities and communication lines outside the government facilities.

Chapter 2.4 Measures for Individual Issues

2.4.1 Miscellaneous

2.4.1.1 Measures for Introducing IPv6 Technology to Information Systems

Compliance Requirements

(1) Measures to prevent vulnerability during IPv6 communication

(a) For devices and software procured as a product in the components of an information system to be built that are expected to perform communications with IPv6 technology (hereinafter referred to as "IPv6 communications"), if there are several candidates that provide the security functions required in the field of the pertinent product, and there are Phase-2 conformity products based on the IPv6 Ready Logo Program, information system security officers must select one of such products as a component of the information system.

(b) For information systems to be built that are expected to perform communications with IPv6 technology, information system security officers must take measures to prevent threats to direct accessibility with a global IP address.

(c) For information systems to be built that are estimated to perform communications with IPv6 technology, information system security officers must implement filtering to restrict unauthorized communication.

(d) When implementing a communication function which uses IPv6 technology (hereinafter referred to as "IPv6 communications") in an information system, information system security officers must take necessary measures to prevent security threats the IPv6 transition imposes on other information systems.

(e) For information systems to be built that are estimated to perform communications with IPv6 technology, information system security officers must take measures to prevent security problems due to the use of devices and software that do not support IPv6.

(2) Preventing and monitoring unintended IPv6 communications

(a) For information systems that are used only between government agencies or within an agency, information system security officers must take measures to prevent IPv6 communications on all computers and communication equipment connected to communication lines on which IPv6 communications are not intended.

(b) For information systems that are used only between government agencies or within an agency, information system security officers must consider whether it is necessary to

monitor communication lines on which IPv6 communications are not intended, and if it is deemed necessary, take pertinent measures, and if any IPv6 communications are detected, identify the device and take necessary measures to shut down the IPv6 communications.

Annexes

Annex 1 Class Control of Information Handling Areas

Annex 2 Class Usage Restrictions of Information Handling Areas