Policy for Enhancement of Information Security Measures for the Central Government Computer Systems

15 September, 2005
Decision by the Information Security Policy Council

1. Basic Recognition

(1) Current Situation

Social infrastructures supported by information technology have progressed in various sectors ranging from industrial and economic activities to administrative activities and people's social lives. In order to foster sound growth of social infrastructures, it is vital to secure and improve safety and reliability.

Under such circumstances, various problems have recently tended to accumulate and multiply, including DoS attacks on government agencies, IT-malfunction in critical infrastructures which are the basis of people's social lives and economic activities, and leakage of important information such as personal information, etc., of private businesses via the internet. In the wake of increasing threats to information security, society has the task of improving and enhancing information security measures in terms of both quality and quantity.

With respect to one of the critical infrastructures, the government and administrative services, the information handled by each information system in government agencies contains considerable highly confidential government information and information on the people and private companies, and if such information was leaked, falsified or destroyed, there would be grave consequences. Some information systems cannot afford to fail for long periods of time. Thus, ensuring information security of government agencies is a crucial issue concerning various sectors, ranging from the protection of personal rights and property, maintenance of economic activities and administrative functions as well as security.

(2) Current Status and Issues of the Government's Efforts

With respect to information security measures of government agencies, each government agency (including Cabinet Secretariat, Cabinet Legislation Bureau, National Personnel Authority, and Fair Trade Commission, the same as below) has formulated and implemented information security policies of their own and under their own control, based on the Guidelines for the Formulation of Information Security Policies (hereinafter referred to as the "former guidelines") compiled by Information Security Promotion Council on July 18, 2000. This produced some positive results: for example, consolidating the awareness of information security issues and improvement of information security levels in each government agency. However, since the

former guidelines did not address conformity and integration of measures implemented by each government agency, the content and level of measures in each agency currently varies. Also due to the lack of experts on information security, sufficient levels of information security have not been achieved as a whole government.

In order to counter such situations, it is essential to establish a framework for information security measures on the assumption of further cooperation from each government agency to promote efforts to ensure higher levels of information security as a whole government. In specific terms, it is first necessary to formulate uniform standards of information security measures (hereinafter referred to as "Standards for Measures") to be introduced at each government agency in order to raise the overall level of information security and then carry out individual measures while taking into account each agency's characteristics. Furthermore, measures to be carried out by government agencies' cooperation, should be improved to upgrade the level of measures of the government as a whole.

In progressing with information security measures in government agencies under such framework, a relationship is important not only among government agencies but also with concerned parties. In other words, since information systems of government agencies have contact with private sector, local governments, and incorporated administrative agencies via, for example, electronic applications, it is necessary to be aware of the relationship between them, and measures are expected to serve as a model for them. Moreover, since government agencies and private sector generally adopt similar systems in terms of information security, information security measures in the government should be worthy of referencing to anyone outside the government. This should be regarded as internationally significant from the viewpoint that such an approach is part of the efforts in creating a nation with the most advanced information technology (IT).

2. Basic Policies for the Enhancement of Measures

Based on the basic recognition described in Section 1, each government agency shall promote the following integrated and cross-sectoral information security measures as part of information security measures in the government. Through such initiatives, further efforts will be made to ensure uniformly high level of information security as a whole government, develop an E-Government that is trusted by the people, and maintain continuous and stable administrative systems.

(1) Formulation of Standards for Measures

Each government agency shall promote conformity and the integration of information security measures. The Information Security Policy Council (hereinafter referred to as the "ISPC") shall formulate necessary Standards for Measures and then review the standards every year in response to changes in technology and environment.

(2) Review of Information Security Policies and Others in Each Government Agency

Each government agency shall in principle make efforts to its own information security measures under its responsibility, and promote compatible information security measures as a whole government by conducting necessary reviews on current information security policies and related procedures, etc., based on the Standards for Measures.

(3) Self-Assessment, etc., of Each Government Agency

Each government agency shall periodically carry out self-assessment on implementation of information security measures, and improve measures whenever necessary.

(4) Establishment of PDCA Cycle of the Whole Government

The National Information Security Center (hereinafter referred to as the "NISC") shall, within the necessary scope, inspect and evaluate the implementation of measures in each government agency, based on the Standards for Measures. Based on those evaluations, the ISPC shall make recommendations on improvement to measures in each agency, and connect them to improvements in the Standards for Measures, which would complete a PDCA cycle (Plan/Do/Check/Act cycle) of the government as a whole.

(5) Promotion of Utilizing Systems and Others that are Effective for Ensuring Information Security

In order to promote the development of secure information systems, each government agency shall take necessary measures to ensure information security, such as introducing objectively assessed data encryption methods and products, conducting external audits, and verification of information security management systems of contractors. Furthermore, the NISC shall promote there efforts by each government agency.

(6) Improvement of Security Measures of Incorporated Administrative Agencies etc.

Each government agency shall promote upgrading the level of information security of incorporated administrative agencies that fall under its jurisdiction, based on the Standards for Measures.

(7) Cooperation between the NISC and Government Agencies in Handling New Vulnerability, etc.

The NISC shall facilitate regular communications with government agencies that support the ISPC's administration and presiding ministries and agencies of the relevant critical infrastructure, gather information on new vulnerabilities, etc., analyze vulnerabilities and information of possible threats, and provide each agency with appropriate information in a timely manner.

(8) Support and Promotion of Development of Human Resources Engaged in Information Security

In light of the lack of government officials with pertinent knowledge of information security required for the smooth promotion of information security measures in government agencies, the NISC shall support the development and securing human resources, and also provide assistance for designing information security measures for information system development.

(9) Strengthening of Other Mid and Long-Term Measures of the Government as a Whole

Besides the items above, the NISC shall commit itself to the implementation of information security measures by cooperating with the whole government agencies, including integration of required specifications concerning information security and preparation of emergency response measures in mid- fiscal year.

Measures (1) to (4) above need to be implemented comprehensively and systematically with cooperation between each agency and the NISC, and therefore, the ISPC will formulate guidelines to specify the implementation frameworks.