Information Security 2010

[Tentative Translation]

July 22, 2010

Information Security Policy Council

Contents

I Preface

The efforts related to Japan's information security measures have been driven by the respective public and private entities based on the "First National Strategy on Information Security" (February 2, 2006) aimed at realizing a "Secure Japan" from FY2006 to FY2008, and based on the "Second National Strategy on Information Security" (February 3, 2009) that "continued and expanded" the same strategy from FY2009 onwards.

However, due to the large-scale cyber attack case in South Korea and US in July 2009, it is clear that the threat on information security has become an issue of security assurance and crisis management while the risks faced by information security are diverse, sophisticated and complex, and more difficult to ensure information security through conventional efforts.

In order to respond to this sort of changed environment with precision, the "Information Security Strategy for Protecting the Nation" (May 11, 2010; hereinafter "Strategy") was newly formulated.

In this Strategy,

[1] Enhancement to policies concerned with occurrence of cyber attacks and preparation of a system for coping;

[2] Establishment of information security measures in response to a changed environment;

[3] Moving from passive information security measures to active information security measures

are treated as basic policies, and in order to be at the world's leading edge as an "advanced information security nation" by 2020,

[1] Overcoming IT risks to realize safety and security in the nation's life;

[2] Enhancement to policies related to cyberspace security and crisis management, and cooperation with ICT policies as the foundation of socioeconomic activities;

[3] Establishment of a comprehensive policy of a 3-axial framework by adding the viewpoints of the protection of nation and users to the viewpoints of security assurance, and crisis management and economy. In particular, the promotion of information security measures that seriously consider the viewpoints of the nation and users;

[4] Establishment of information security measures that contribute to the economic growth strategy;

[5] Enhancement to international cooperation

were emphasized.

Specifically in the next 4 years, the initiatives described in the Strategy will be promoted in addition to the measures stipulated in the "Second National Strategy on Information Security."

The "Information Security 2010" (this) document corresponds to the "Secure Japan 20XX" annual plans based on the Strategy, and is to set forth the details of the specific efforts to be implemented in FY2010 and FY2011.

Furthermore, in the event of a changed environment in relation to information security measures, commensurate steps are to be formulated and implemented within the required scope in response to the changes. In addition, the document that stipulates the framework of the information security measures such as the Strategy is also to be reviewed if necessary.

II Specific Efforts

In the course of implementing information security policy, the government, needless to say, must be capable of managing any information security incident, should it occur, to ensure the nation's safety and security. In addition to this, it is essential for Japan to keep improving the "fundamental crisis management capability" of the entire country in order to cover the increasingly sophisticated and diverse information security threats. For this purpose, it is important to establish an organizational system to implement a comprehensive policy under strong leadership, through an alliance of the concerned government agencies centered around the Cabinet Secretariat. In particular, international alliances must be reinforced as unprecedented borderless incidents are now more likely to occur.

The ICT infrastructure—information systems and telecommunication services—is mainly built, provided, and used in the private sector. Taking this into account, the roles of the public and private sectors must be clearly identified in the course of building an alliance between the two sectors.

Further, the recognition of an "Accident Assumed Society" must be disseminated, and information security measures must be constantly improved to build up management expertise to survive in such a society. To do this, it is important to build up the systems to visualize and assess the results of the government's efforts and feed back these results in order to improve future measures.

Taking into consideration the above situation described in the Strategy, the specific policies presented below are to be steadily implemented. The policies with no particular indication of implementation period are to be implemented in FY2010.

1 Preparation for a Potential Large-Scale Cyber Attack

Considering that an assault similar to the 2009 July cyber attack that occurred in the United States and South Korea may be being planned against Japan, Japan must make the following arrangements: a) Organize preparatory measures to be able to manage the state under a large-scale cyber attack, in which the attack may threaten or actually cause harm to life, physical injury, or the assets of the nation, or even the country itself; and b) Reinforce the day-to-day means of collecting and distributing information utilizing the existing information sharing system between public and private sectors based on the Second Action Plan on Information Security Measures for Critical Infrastructures, and other such plans.

To implement these measures and ensure comprehensive counteraction, maintain good communications between the departments responsible for day-to-day preventative measures and the departments responsible for emergency management in the event of a large-scale cyber attack.

(1) Organizing Counteractive Arrangements

- Preparation of the government's initial response to a large-scale cyber attack

Based on the Arrangement of Government's Initial Response to an Emergency (cabinet decision on November 21, 2003) etc., organize the arrangements for the government and relevant organizations to be able to take prompt and effective initial counteraction against a large-scale cyber attack. At the same time, conduct initial response drills.

[Specific Measures]

A) Implementation of training on initial response upon occurrence of a large-scale cyber attack (Cabinet Secretariat and concerned government agencies)

Specific training is to be conducted with emphasis placed on cooperation with the respective government agencies based on "Government's Initial Response to an Emergency (Cabinet decision of Nov 21, 2003)," and through a review taking into consideration the results, preparations are to be made for a swift and appropriate initial response by the government and relevant institutions upon occurrence of a large-scale cyber attack.

In addition, efforts are to be made to continuously implement the above-described training into the following years too.

B) Reinforcement of the System against Cyberterrorism (National Police Agency)

In order to deal with sophisticated cyber-attack methods as a means of cyberterrorism[1], reinforcement to the police force's counter-cyberterrorism system is to be stepped up such as by enhancing the information collection and analysis system, and implementing training inside and outside the department to maintain and improve the technical capability and ability of counter-cyberterrorism personnel to deal with incidents.

- Alliance between public and private sectors

In the response to the state under a large-scale cyber attack, cooperation between the critical infrastructure operators is vital. Understanding and awareness of the need for such cooperation must be raised among these operators to ensure close coordination between the public and private sectors.

[Specific Measures]

A) Enhancement to Public-Private Cooperation in Counter-Cyberterrorism for Critical

[1] An electronic attack on the backbone system of a critical infrastructure, or a serious failure in the backbone system of a critical infrastructure that is very likely to have been caused by an electronic attack.

Infrastructures (National Police Agency)

Besides holding enlightenment activities linked to raising the awareness of cyberterrorism countermeasures as and when necessary taking into consideration the special characteristics of the business of critical infrastructure providers, efforts are to be made to contribute to emergency response activities during occurrence of cyberterrorism through participation in various types of exercises and implementation of joint training while respecting the intentions of critical infrastructure providers.

B) Cyberterrorism (Incident) Response Coordination and Support (Ministry of Economy, Trade and Industry)

In response to requests from critical infrastructure providers, support is provided to deal with information security incidents such as coordination against the source of attack, and support is provided for analysis of attack methods while also making use of the cooperative framework with international CSIRT.[2]

- Reinforcement of protection against cyber attacks

Following other countries' precedence in reinforcing their cyber security, reinforce the cyber defense performance against attacks.

[Specific Measures]

A) New Post of Cyber Planning and Coordination Officer (provisional title) (Ministry of Defense)

At the end of FY2010, a cyber planning and coordination officer (provisional title) will be stationed in the Joint Staff Office of the Ministry of Defense to enhance the preparedness against cyber attacks.

B) Promotion of Analysis, Response and Research Related to Cyber Attacks (Ministry of Defense)

In order to further improve the analysis and response capability on the threats and effects related to cyber attacks against information systems maintained by the Ministry of Defense, besides research and test production of network security analysis equipment, basic research will be carried out in continuation from 2009 on unauthorized access monitoring and analysis technology, cyber-attack analysis technology and active defense technology.

[2] Abbreviation for Computer Security Incident Response Team.

C) Investigation and Research on the Latest Technological Trend Related to Information Assurance (Ministry of Defense)

Continuing from FY2009, besides continuously investigating the latest technological trend related to cyber attacks and cyber-attack countermeasures, a unified response will also be investigated and researched in order to ensure information of information systems.

- Policing cybercrimes

Promote cybercrime policing through utilization of digital forensic technologies and collaborations among various investigation agencies from different countries.

[Specific Measures]

A) Promotion of Efforts on Digital Forensics[3] (National Police Agency)

In order to appropriately deal with cybercrimes of ever increasing diversity and complexity, the implementation of training for police officers involved in cybercrime investigations, the buildup of resources and equipment, the cooperation with relevant domestic institutions such as through holding of digital forensics liaison conferences, and the enhancements to the systems related to digital forensics such as public-private cooperation starting with technical collaborations are to be promoted.

B) Promotion of International Cooperation for the Policing of Cybercrimes (National Police Agency)

Besides implementing an effective information exchange with the law enforcement institutions of the various countries closely linked to Japan's cybercrime situation, the establishment of multilateral cooperative relations is to be promoted such as through active participation in international frameworks related to cybercrime countermeasures such as G8 and ICPO, and by organizing the Asia-Pacific Cybercrime Technology Information Network System Conference.

- Reinforcement of international alliances against cyber attacks

Reinforce international alliances against cyber attacks through exchanging cyber attack information and active participation in relevant international conferences.

[3] General term for the equipment and data needed for investigating the causes, collecting and analyzing electronic records, and the means and technologies to clarify the legal evidence when there is occurrence of computer-related crimes such as unauthorized access and confidential information leakage, or legal disputes.

[Specific Measures]

A) Information Exchange Related to Cyber Attacks (Cabinet Secretariat and concerned government agencies)

Information collection and analysis that contributes to cyberterrorism measures such as attack subject and method will be continuously implemented such as through bilateral information exchange with relevant overseas institutions.

B) Enhancement to Cooperation through Participation in International Conferences (Cabinet Secretariat and concerned government agencies)

In order to improve the response capability against cyber attacks, cooperation with overseas countries is to be enhanced in FY2010 through participation in international cooperation frameworks such as FIRST (Forum of Incident Response and Security Teams).

C) Enhancement to Cooperation with Relevant International Institutions against Cyberterrorism (National Police Agency and Ministry of Justice)

In order to enhance the measures against cyberterrorism, information collection and analysis related to attack subject and method, etc., will be continuously implemented such as reinforcement of international cooperation through information exchange with relevant overseas institutions.

(2) Building Up and Reinforcement of Day-to-Day Cyber Attack Information Collection and Sharing System

- Reinforcement of the communication system to collect, analyze, and share information concerning responses against cyber attacks

Reinforce the communication system to collect, analyze, and share information concerning responses to cyber attacks between the Cabinet Secretariat and the concerned government agencies.

[Specific Measures]

A) Centralization and Sharing of Information that Contributes to Countering Cyber Attacks (Cabinet Secretariat and all government agencies)

Enhancement is to be made to the system in which information that contributes to countering cyber attacks is collected by the respective government agencies to be centralized at the Cabinet Secretariat, and timely and appropriately shared with the respective government agencies as required.

B) Support of Reinforcement for Emergency Response System of the Respective Government Agencies (Cabinet Secretariat)

Continuing from FY2009, GSOC[4], besides analyzing the information and general trends related to cyber attacks against government agencies and periodically providing the analysis results to the respective government agencies, will timely and appropriately provide information such as the analysis results of attack methods required for individual measures.

C) Implementation of Information Collection and Information Sharing through Information Sharing System Based on the " Second Action Plan on Information Security Measures for Critical Infrastructures" (Cabinet Secretariat)

With regard to information related to cyber attacks against critical infrastructure providers, etc., fulfillment is planned for information collection and information sharing through the information sharing system based on the " Second Action Plan on Information Security Measures for Critical Infrastructures" (hereinafter "Second Action Plan").

D) Early Grip on Cyberterrorism Signs and Enhancement to Information Collection and Analysis (National Police Agency and Ministry of Justice)

[4] Government Security Operation Coordination team

In order to enhance the measures against cyberterrorism, early grip of terrorism signs in cyberspace is to be made possible, and information collection and analysis related to attack subject and method will be continuously implemented.

E) Enhancement to Systems Related to Cyberterrorism Countermeasures (National Police Agency) [Repetition: Refer to 1(1) • Preparation of the government's initial response to a large-scale cyber attack]

- Building up and reinforcement of the cyber attack information sharing system with other countries

Build up and reinforce the cyber attack information sharing system among relevant agencies and organizations in other countries, the Cabinet Secretariat, and the government agencies concerned.

[Specific Measures]

A) Building up and Reinforcement of the Cyber Attack Information Sharing System with other Countries (Cabinet Secretariat and concerned government agencies)

Besides promoting the enhancement to existing information sharing system with relevant organizations such as through bilateral information exchange with relevant overseas organizations and by continuously implementing the information collection and analysis that contributes to countering the attack subject and method of cyber attacks, studies are also to be made through exchange of views as to what a new information sharing system ought to be like.

B) Enhancement to Cooperation with Relevant Overseas Organizations Related to Cyberterrorism (National Police Agency and Ministry of Justice) [Repetition: Refer to 1(1) • Reinforcement of international alliances against cyber attacks]

2 Reinforcement of Information Security Policy Adapted to Changes in the Information Security Environment

(1) Information Security Infrastructure that Protects the Nation's Life

[1] Consolidation of Governmental Infrastructure

- Enhancing the function of Chief Information Security Officers

Enhance the function of Chief Information Security Officers (CISOs) in the government agencies concerned through establishing a liaison conference for CISOs and a liaison conference for Chief Information Security Advisors. Also the CISOs in each government agency must improve the information security measures being taken in their respective organizations through creating and disseminating their information security reports.

[Specific Measures]

A) Efforts toward a Higher Level of Information Security Governance (Cabinet Secretariat and all government agencies)

a) The Cabinet Secretariat is to promptly hold a liaison conference (officially called the "Information Security Measures Promotion Conference") for the chief information security officers comprising the chief secretaries of concerned government agencies, and the concerned government agencies are to autonomously strive to fulfill a system enabling unification of responsibilities for information security measures under the chief information security officer.

b) Chief Information Security Advisers Liaison Conference is to be set up under the Chief Information Security Officers Liaison Conference, and information security expertise is to be reflected in the sophistication of the efforts of concerned government agencies.

B) Promotion of Efforts Related to "Annual Report on Information Security" (information security report) (Cabinet Secretariat and all government agencies)

a) Concerned government agencies' chief information officers are to create information security reports starting from FY2010 while making use of the knowledge available inside and outside the ministries and taking into consideration the guidelines for creating the information security reports. In this case, from the viewpoint of ensuring the information security report is objective, the use of external audit system is to be promoted as far as possible.

b) The created information security reports, besides being compared and evaluated at the Chief Information Security Advisers Liaison Conference, the knowledge thus obtained is to be shared and fed back, and those reported by the chief information security officers at the Chief Information Security Officers Liaison Conference, published at well-prepared government agencies.

- Enhancement and reinforcement of an inter-divisional Government Security Operation Coordination team

The Government Security Operation Coordination team (GSOC), which commenced full-scale operation in FY2008, conducts 24-hour monitoring of government agency information systems. Enhance the ability of the GSOC to collect information by organizing an emergency communication system and close coordination with the relevant parties, and ability to analyze attacks, in order to improve the emergency response capabilities against cyber attacks, etc. of the entire government.

(Note) GSOC: Government Security Operation Coordination team

[Specific Measures]

A) Fulfillment and Enhancement of the Government's Cross-Sectional Information Collection and Analysis System in GSOC etc. (Cabinet Secretariat and all government agencies)

a) GSOC, which commenced full-scale operations in FY2008 and performs 24-hour monitoring of government agency information systems, enhances the information collection capability and analytical capability related to cyber attacks by stepping up cooperation with relevant collaborative institutions and promoting exchange of views with overseas government agencies, and in addition, promotes information sharing such as analysis results and strives to improve the emergency response capability of the entire government.

b) In 2010, the emergency contact system will be checked through exercise, and its effectiveness will be ensured.

- Efficient and continuous improvement of information security measures in government agency information systems

Rationalize the information systems utilized by government agencies and streamline their operations by a range of means, including integrating the servers of different agencies in order to help improve the performance and efficiency of information security measures. Also each agency must constantly review and assess their information security measures to ensure continued improvement.

[Specific Measures]

A) Efficient and Continuous Improvement of Information Security Measures in Government Agency Information Systems (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and all government agencies)

a) Based on the "Formulation of Centralization Plan for Public Web Servers and Mail Servers of Government Agencies" (Report to Information Security Policy Council of May 11, 2010), each of the concerned government agencies will further promote the streamlining and operational efficiency of information systems as well as strive for the improvement and efficiency of information security measures by steadily implementing the centralization of maintained public web servers and mail servers by end of FY2013.

b) The Cabinet Secretariat is to continuously have a grip on the situation toward steady promotion of server centralization, and report to the Information Security Policy Council.

B) Implementation of Vulnerability Checks for Public Web Servers (Cabinet Secretariat and Concerned Government Agencies)

The Cabinet Secretariat, under the cooperation of concerned government agencies, will implement the vulnerability checks in 2010 for the main public web servers of the desiring government agencies, and provide feedback on the results to the government agencies.

C) Enhancement to Cooperation between the Cabinet Secretariat and Assistant to Chief Information Officer (CIO) of Concerned Government Agencies (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and all government agencies)

In FY2010, efforts are to be enhanced to ensure the security of information systems in government agencies by cooperating with the newly established Chief Information Security Advisers Liaison Conference and CIO Assistants Liaison Conference.

D) Promotion for the Formulation of Business Continuity Plan (Cabinet Secretariat and all government agencies)

a) From the viewpoint of ensuring administrative continuity in times of disasters and failures, the concerned government agencies are to promote the formulation of business continuity plan for required information systems.

b) The Cabinet Secretariat is to undertake the required efforts to create the guidelines by the end of FY2010 to support the formulation of business continuity plans by each of the government agencies concerned by end of 2011.

E) Promotion of Guidelines on Risk Assessment and Digital Signature/Authentication for e-Government (Cabinet Secretariat and all government agencies)

a) The Cabinet Secretariat is to undertake the required efforts to formulate the "Guidelines on Risk Assessment and Digital Signature/Authentication."

b) In order to ensure the overall effectiveness of the risk evaluation and assurance level drawn up based on the guidelines, the concerned government ministries presiding over the online procedures targeted by the guidelines, besides receiving advice at the Information Security Measures Promotion Conference from those with expertise and making decisions, are to report to the CIO Liaison Conference on the situation of reflecting business and system optimization in the plans.

F) Fixation and Spread of PDCA Cycle in the Entire Government (Cabinet Secretariat and all government agencies)

a) The Cabinet Secretariat, based on the Standards for Measures, is to evaluate in an objectively comparable manner the implementation situation of the measures by concerned government agencies on the basis of the report on the implementation of measures, link up the improvement of concerned government agencies' measures with that of the improvement to the Standards for Measures through recommendations, and ensure the fixation and spread of PDCA cycle in the entire government. For this reason, the means for further efficiency of self-assessment tasks such as by improving the survey item and method are to be investigated, and presentations be made to concerned government agencies.

b) The result of the evaluations is to be published in consideration of the maintenance and assurance of information security in order to fulfill the explanatory obligations to the nation besides promoting effective measures for the government as a whole.

G) Enhancement to Information Sharing within the Entire Government (Cabinet Secretariat and all government agencies)

In order to support the promotion of information security measures at concerned government agencies, the Cabinet Secretariat, in relation to common operational issues of the information security measures, is to provide information related to the respective types of information security measures including technical information, newly set up an investigation-and-sharing place for joint responses with concerned government agencies, and make concerted efforts to resolve the issues.

H) Information Security Measures for Systems Handling Specially-Controlled Secrets (Cabinet Secretariat and concerned government agencies)

The Cabinet Secretariat, in cooperation with concerned government agencies, is to steadily implement efforts toward building a multi-layered checking mechanism for the implementation situation of measures taking into consideration the criteria related to specially-controlled secrets based on the "Counterintelligence Policy."

I) Promotion of Education and Awareness-Raising for Government Employees (Cabinet Secretariat, National Personnel Authority, and all government agencies)

a) The Cabinet Secretariat and the Ministry of Internal Affairs and Communications will fulfill the need for standard educational programs for government employees (general staff, management, and personnel in charge of information security measures).

b) With regard to joint trainings for government employees upon employment, the Cabinet Secretariat and the National Personnel Authority will endeavor to provide educational opportunities incorporating contents relating to information security.

c) The Cabinet Secretariat is to further enrich the model for educational teaching materials in correspondence with the roles in information security measures. In reference to this, the concerned government agencies are to prepare the educational teaching materials corresponding to the roles.

d) The concerned government agencies are to raise awareness of recent incidents and cases related to information security by taking advantage of the e-government promotion week and the information security month, etc.

J) Prevention of Spoofing of E-mails Sent by Government Agencies (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and all government agencies)

a) The Cabinet Secretariat and all government agencies are to push for the adoption of the sender domain authentication technology such as SPF (Sender Policy Framework) to rule out malicious third parties from impersonating government agencies or their staff and harm the general public or the private sector.

b) The Ministry of Internal Affairs and Communications will cooperate with the "Anti-Spam Consultation Center" established with wide participation by those involved with spam e-mail countermeasures and the "Japan Email Anti-Abuse Group (JEAG)" which is a non-governmental organization centered around the main domestic internet connection service providers and mobile operators, and will facilitate the adoption of sender domain authentication technology.

K) Promoting the Use of Domain Names Guaranteed to be the Domain Names of Government Agencies (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and all government agencies)

Continuing into FY2010, for the domain names used when government agencies send information to the nation, besides striving to use domain names (".go.jp" domain names among the generic JP domain names) guaranteed to be government agencies in principle, the status of the efforts will also be widely made known to the nation.

- Promotion of secure encryption usage in government agencies

Continue to renew the E-government recommended ciphers currently in use by government agencies, as specified in the renewal guidelines. The integrity of the E-government recommended ciphers must be constantly monitored and examined, and if any of the ciphers are identified to be no longer sufficiently robust, they should be replaced with alternative ciphers immediately. The plan to achieve this must be formulated and a contingency plan, which stipulates responses against sudden deterioration of cipher integrity, must also be prepared.

[Specific Measures]

A) Promotion of secure cipher usage in government agencies (Cabinet Secretariat, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry, and all government agencies)

a) The Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry will monitor the e-Government Recommended Ciphers, and will carry out investigation, research, and creation of standards in FY2010 to ensure the safety and reliability of the e-Government Recommended Ciphers.

b) The Ministry of Internal Affairs and Communications, and the Ministry of Economy, Trade and Industry will steadily implement efforts toward revising the "e-Government Recommended Ciphers List."

c) The Cabinet Secretariat, the Ministry of Internal Affairs and Communications, and the concerned government agencies, besides promoting efforts in accordance with the "Migration Plan of Cryptographic Algorithm SHA-1 and RSA1024 in Information Systems of Government Agencies"[5], will also consider contingency planning as preparation for the sudden deterioration of security.

d) The Cabinet Secretariat is to grasp the response situation to the migration guideline at

[5] Decision at Information Security Policy Council of April 22, 2008

concerned government agencies, and press for the compliance of each information system with the stipulated requirements of the migration guideline until the start of replacement to a new cryptographic algorithm.

B) Promoting the Use of a Secure and Reliable Cryptographic Module (Cabinet Secretariat, Ministry of Economy, Trade and Industry, and all government agencies)

In order to promote the use of a secure cryptographic module, hereafter, besides promoting the IPA-run cryptographic module validation program, products certified through the program will be accorded priority as and when necessary in the event of procuring a cryptographic module.

- Ensuring information security in cloud computing[6]

Identify the means to ensure information security required to efficiently utilize cloud computing, which enables the integration and rationalization of government agency information systems, for electronic governmental administration.

Also, organize the telework environment in government agencies after due study of advanced security measure model cases.

[Specific Measures]

A) Enhancement to Information Security Measures for New Technologies (Cabinet Secretariat and Ministry of Internal Affairs and Communications)

For "common government platform" utilizing cloud computing technology, the Ministry of Internal Affairs and Communications is to clarify the required specifications including information security assurance policy, and the Cabinet Secretariat is to implement support such as providing expertise accumulated through revision of Standards for Measures and other related measures.

- Review of the Standards for Information Security Measures for Central Government Computer Systems

As well as encouraging the thorough implementation of the current Standards for Information Security Measures for Central Government Computer Systems, review the said Standards in view of recent changes in ICT and the related environment, as appropriate, in order to be prepared for new information security threats.

[6] A new computer network where data services and internet technology are located on a cluster of servers (cloud) on the network, and enables the user access "no matter where, whenever required, and only the required functions" without processing or storing anything on his/her computer as is the case until now.

[Specific Measures]

A) Implementation of Review for the Standards for Measures (Cabinet Secretariat)

In consideration of changes to technology and environment, the Standards for Measures are to be reviewed. Particularly in FY2010, a review will be carried out by taking into consideration the new technological trends such as the cloud computing, and revisions will be made to the Standards for Measures (Fifth Edition).

B) Enhancement to Cooperation with Incorporated Administrative Agencies Related to Information Security Measures (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

The Cabinet Secretariat is to accumulate and utilize the knowledge of researchers and practitioners from information security organizations and incorporated administrative agencies such as the National Institute of Information and Communications Technology (NICT), the National Institute of Advanced Industrial Science and Technology (AIST) and the Information-Technology Promotion Agency (IPA), and in order to reflect to the Standards for Measures policy, build collaborative system using existing framework, and enhance cooperation between the Cabinet Secretariat and the incorporated administrative agencies related to information security measures.

C) Ensuring Consistency with the Legal System Related to Information Security (Cabinet Secretariat, Cabinet Office, Ministry of Internal Affairs and Communications, and concerned government agencies)

The Cabinet Secretariat is to promote the required adjustments with concerned government agencies in charge of the legal system starting with relevant departments within the Cabinet Secretariat so as to ensure consistency between the legal system related to information security and the Standards for Measures.

D) Promoting the Use of Secure and Reliable IT Products (Cabinet Secretariat and all government agencies)

Continuing into FY2010, in order to build a secure and reliable information system, products certified through the "IT Security Assessment and Certificate System[7]" will be accorded priority based on the Standards for Measures when procuring IT products.

[7] In relation to IT products and systems, it refers to having the security functions and targeted security assurance level evaluated by a third party based on the ISO/IEC 15408 international standard for information security, and having the results publicly verified and published in principle.

E) Support for System Selection and Procurement with Information Security Considerations (Cabinet Secretariat and Ministry of Economy, Trade and Industry)

a) In order to effectively and efficiently procure IT systems with consideration given to information security, the concerned government agencies in 2010 will continue to consider promoting the use of products certified by the IPA-run IT Security Assessment and Certificate System, and facilitate their use in government agencies.

b) While also giving consideration to the situation in overseas countries, clarification will be carried out in the case of "critical security requirements" which are part of the requirements related to the need of obtaining certification of "IT Security Assessment and Certificate System" and " Japan Cryptographic Module Validation Program" when procuring government information systems stipulated in the Standards for Measures, and contribution be made toward reflecting in the said Standards for Measures.

F) Promoting the Use of Secure Encryption in Government Agencies (Cabinet Secretariat, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry, and all government agencies) [Repetition: Refer to 2(1)[1] • Promotion of secure encryption usage in government agencies]

G) Promoting the Use of a Secure and Reliable Cryptographic Module (Cabinet Secretariat, Ministry of Economy, Trade and Industry, and all government agencies) [Repetition: Refer to 2(1)[1] • Promotion of secure encryption usage in government agencies]

- Building up a mechanism to enable thorough implementation of information security measures in government agency information systems

Identify methods to incorporate information security measures in government agency information systems from the planning stage. Also specify the information security requirements that must be included in such information systems. Inform the details of such measures and requirements through official notices.

Clarify the information security requirements that demand third party assessment or certification in order to encourage the usage of such assessed or certified products.

[Specific Measures]

A) Budgetary Efforts (all government agencies)

The concerned government agencies, in relation to information security measures, are to assume in advance as far as possible that the required security measures can be assured in the system budget as a whole, and in the procurement of information systems, in order to reliably implement the required security measures, efforts are to be made such as to state the requirements in the requirement specifications as far as possible and also to replace maintenance agreement with one that allows for a timely and appropriate response.

B) Enhancement to Information Security Measures for Information Systems with Outsourced Operations and Management (all government agencies)

The concerned government agencies are to make efforts to ensure the security for information systems having operations and management entrusted to organizations outside the government agencies by taking into consideration the Standards for Measures.

C) Consideration of the Means for Awareness for Incorporation of Information Security Measures Starting at the Planning and Design Stage (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and all government agencies)

For the means for awareness for the incorporation of information security measures starting at the planning and design stages (Security by Design) of the information systems, in FY2010, in relation to government procurement related to information system, consideration will be given to the building of a mechanism that suitably incorporates information security measures in the information systems, and the information security requirements that ought to be incorporated into the information systems will be gathered together.

D) Promoting the Use of a Secure and Reliable Cryptographic Module (Cabinet Secretariat, Ministry of Economy, Trade and Industry, and all government agencies) [Repetitions: Refer to 2(1)[1] • Promotion of secure encryption usage in government agencies; 2(1)[1] • Review of the Standards for Information Security Measures for Central Government Computer Systems]

E) Usage and Dissemination of the "Guidelines for Improving the Reliability of Information Systems" (Ministry of Economy, Trade and Industry)

For all information systems, in order to improve the reliability of the information systems from the overall viewpoints of process management aspects such as development and operations, technological aspects, organizational aspects, etc., the usage and dissemination of the "Guidelines for Improving Reliability of Information Systems (Second Version)" and the "Evaluation Index concerning Improvement of the Reliability of Information Systems (First Version)" that allows visualization of the status of compliance with the guidelines are to be facilitated.

F) Support for Ensuring Information Security during Procurement of Information Systems (Ministry of Economy, Trade and Industry)

a) In order to support the tasks of those procuring information systems, tools are to be developed to provide information on the technical security requirements of the main components of the information systems.

b) Besides promoting the operations of the "IT security assessment and authentication system," the usage expansion of the scheme to information system procurement is to be planned.

c) The operations of the "Japan Cryptographic Module Validation Program" and the "Japan Cryptographic Algorithm Validation Program" are to be promoted.

G) Promoting the Use of Safe and Reliable IT Products (Cabinet Secretariat and all government agencies) [Repetition: Refer to 2(1)[1] • Review of the Standards for Information Security Measures for Central Government Computer]

H) Support for System Selection and Procurement with Information Security Considerations (Cabinet Secretariat and Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)[1] • Review of the Standards for Information Security Measures for Central Government Computer]

- Determining appropriate information security for the common number system for social insurance and taxation

In the course of discussions concerning the common number system for social insurance and taxation, identify problems and possible solutions concerning the system so that appropriate information security measures concerning private information protection can be adopted.

[Specific Measures]

A) Study on Information Security Measures for Social Insurance and Taxation Numbering System and National ID System (Cabinet Secretariat and concerned government agencies)

For the numbering system and national ID system related to social insurance and taxation being considered by the government across sectors, consideration is given to enable the adoption of appropriate privacy assurance measures and information security measures and ensure security and convenience to the nation.

- Implementation of information security measures in local governments and incorporated administrative agencies, etc.

In the course of reviewing the Standards for Information Security Measures for Central Government Computer Systems, encourage action concerning information security measures to be undertaken in local governments and incorporated administrative agencies, etc.

[Specific Measures]

A) Dissemination and Enlightenment for Improvement to the Level of Information Security Measures in Local Governments (Ministry of Internal Affairs and Communications)

a) In order to strive to facilitate the formulation of business continuity plan of ICT departments in local governments, implementation of information security audit, creation of information resource register, implementation of risk analysis, etc., the holding of seminars related to business continuity plan and the dispatch of internal audit advisers will be implemented. In addition, the Guidelines for the Formulation of Information Security Policies will be reviewed.

b) The fulfillment of the invitation for information security best practices and model cases, and the collection and analysis of information security incident report is to be devised, and for the portal sites inside LGWAN (local government wide area network), operational support is to be given such as by providing information security explanations, and greater usage is to be facilitated.

B) Promotion of the Dissemination and Enlightenment of Information Security for Education-Related Departments of Local Governments (Ministry of Internal Affairs and Communications, and Ministry of Education, Culture, Sports, Science and Technology)

In order to ensure information security at education-related departments, support is to be given for the dissemination and enlightenment of information security efforts.

C) Enrichment of Information Security Training for Local Government Employees (Ministry of Internal Affairs and Communications)

The implementation and content enrichment of information security e-learning are to be facilitated to enable all local government employees to have lessons without being restricted by time and location.

D) Promotion of Information Security Measures in Incorporated Administrative Agencies (government agencies in charge of incorporated administrative agencies)

a) Continuing from FY2009, for the incorporated administrative agencies being managed, besides demanding the formulation and review of information security policy by taking into consideration the set of measures in government agencies including the Standards for Measures, necessary support is to be given.

b) In accordance with the implementation situation of countermeasures and the business specificity of the incorporated administrative agencies, besides promoting efforts for building PDCA cycle related to own information security measures, clear statement of items related to information security measures is to be promoted as midterm target.

E) Preparation of an Emergency System for Contacting Incorporated Administrative Agencies (Cabinet Secretariat and government agencies in charge of incorporated administrative agencies)

Continuing from FY2009, a system for contacting incorporated administrative agencies including during emergencies is to be prepared, and its effectiveness is to be validated in FY2010.

F) Cooperation with governmental Agencies other than Administrative Agencies (Cabinet Secretariat)

In order to appropriately respond to information security issues common to administrative agencies as well as governmental agencies other than administrative agencies, information exchange and cooperation with national agencies other than administrative agencies are to be actively pursued.

[2] Reinforcement of Critical Infrastructures

The critical-infrastructure-related entities must maintain their services based on the Second Action Plan on Information Security Measures for Critical Infrastructures, and ensure the smooth recovery from system failures. Additionally, these entities must be prepared for potential information security threats against critical infrastructures that are significantly important to the nation's life.

(Reinforcement of "inter-divisional public and private sector alliance")

The critical infrastructures increasingly depend on ICT, and at the same time, information security threats against such critical infrastructures are also advancing and diversifying. Taking these facts into account, the following issues must be addressed to reinforce information security measures in the critical infrastructures, under a close public and private sector alliance with clear roles assigned to each sector.

- Reinforcement of the information sharing system

To reinforce the information sharing system to support information security measures concerning the critical infrastructures, the environment necessary for notices and communications must be organized based on the roles given thus far to the public and private sectors.

[Specific Measures]

A) Organization of Information Subject to Sharing (Cabinet Secretariat)

a) In order to contribute to the simplification of the maintenance and restoration of the services of critical infrastructure providers, based on the information sharing framework described in B) below and taking into consideration the changes in social trends and information security threats, information that ought to be shared is to be organized, and continuous organization and enrichment of the information to be shared are to be carried out.

b) Based on the collection of information desired to be shared that arose from the study in FY2009, besides checking the information maintained by relevant entities and organizing the restrictions applicable to sharing, the methods (such as method, format, and timing including readiness viewpoint) for sharing information useful to critical infrastructure providers are to be studied per information maintained by the relevant entities in FY2010. In addition, the results of organizing are to be gathered together as a whole and published with end of FY2011 as the target.

B) Promotion of Information Sharing Based on the Implementation Details of Information Communication and Information Sharing of "The Second Action Plan on Information Security for Critical Infrastructures" (Cabinet Secretariat)

a) In order to have a simpler maintenance and restoration of the services of critical infrastructure providers, from the viewpoint of the importance of the cooperation of the respective entities in the public and private sectors, information sharing is to be promoted through the "The communications procedures concerning liaison and information provisions of the Second Action Plan on Information Security Measures for Critical Infrastructures" (hereinafter "Implementation Details") under the information sharing system based on the "Second Action Plan."

b) From the viewpoint of continuous improvement of the information sharing, by the end of FY2010 to FY2011, the Implementation Details are to be reviewed by taking into consideration the progress situation of the "organization of information subject to sharing" and the operational situation of information sharing based on the Implementation Details, and revision is to be carried out if required.

C) Improvements of Rules for Information Sharing Based on Implementation Details (government agencies in charge of critical infrastructures)

a) For the information sharing described in B) above, the rules for sharing information by government agencies in charge of critical infrastructures related to information to be provided to CEPTOARs[8] and the rules for sharing information by providers of critical infrastructures related to information communicated to the government agencies in charge of critical infrastructures, consistency with Implementation Details is to be maintained, and these information sharing rules are to be improved where necessary.

b) For the rules for sharing information related to information to be provided within CEPTOARs, the response situation in CEPTOARs is to be checked besides providing support such as giving advice to CEPTOARs so as to have the CEPTOARs maintain consistency with Implementation Details.

D) CEPTOAR Reinforcement and Training (Cabinet Secretariat and government agencies in charge of critical infrastructures)

a) In order to support the reinforcement of CEPTOARs, besides gathering and sharing with each CEPTOAR the functions and the state of activities of each CEPTOAR with the cooperation of the government agencies in charge of critical infrastructures, publication is to be carried out with the end FY2010 as the target.

b) With the cooperation of the government agencies in charge of critical infrastructures, opportunity is to be provided for checking the information understanding faculty in

[8] CEPTOAR : Capability for Engineering of Protection, Technical Operation, Analysis and Response

order to maintain and improve the information sharing system of the CEPTOARs in each sector.

E) Fulfillment of PR and Public Hearing Activities (Cabinet Secretariat)

In order to enlighten on the importance of information security, raise the standard of information security measures such as of critical infrastructure providers, and lift the nation's information literacy, the use of the Web, etc. related to information security measures expanded in FY2009 and the fulfillment of PR and public hearing are to be devised. In addition, the action plan and the policies based on the action plan are to be actively publicized by making use of opportunities presented by seminars and lectures.

F) Enhancement to Risk Communication (Cabinet Secretariat and government agencies in charge of critical infrastructures)

Besides promptly grasping the changes in the information security environment of critical infrastructures, the means for promoting mutual risk communication by critical infrastructure providers, relevant organizations and government agencies in charge of critical infrastructures are to be investigated with the cooperation of the government agencies in charge of critical infrastructures so as to foster common awareness for the risk measures that ought to be collaboratively dealt with, and enable a smooth response and close collaboration between relevant entities. When investigating, activities mutually beneficial for the public and private sectors are to be targeted, and cooperation with the CEPTOAR Council is to be devised.

G) Implementation of Enlightenment Seminar for Critical Infrastructure Providers (Ministry of Economy, Trade and Industry)

Forums related to information security of critical infrastructures, etc. are to be held with the cooperation of IPA and relevant organizations.

H) Building of a Collaborative System to Deal with Vulnerabilities in Control Systems (Ministry of Economy, Trade and Industry)

Based on the activities of the "Control System Vendor Security Information Sharing Task Force" started up in FY2008 with JPCERT/CC as the secretariat, smooth responses to threats against control system vulnerabilities are to be devised through the promotion of the collection and sharing of information that contributes to the promotion of security measures in control systems. In addition, verification of the effectiveness of tools capable of evaluating the security level of control systems is to be carried out.

I) Prioritized Provision of Information Related to Vulnerabilities of Software and Control Systems to Critical Infrastructure Providers and Support for Information Management Related to Information Security (Ministry of Economy, Trade and Industry)

a) For software products and control systems, in order to minimize the cost or risks arising from vulnerabilities discovered after product distribution or system operation, required review will be carried out on the vulnerability handling systems that enable prompt responses and implementation of user countermeasures.

b) The information related to countermeasures and information security threats that may require countermeasures by critical infrastructure providers is to be provided by JPCERT/CC to CEPTOARs or critical infrastructure providers as early warning information based on prior agreement.

c) Dissemination of information related to the vulnerability of software, etc. is to be in an easy-to-use format.

J) Usage and Dissemination of "Guidelines for Improving the Reliability of Information Systems" (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)[1] • Building up a mechanism to enable thorough implementation of information security measures in government agency information systems]

- Promotion of the CEPTOAR Council

Promote the Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR) Council's activities to enhance and strengthen information sharing and analysis functions concerning information security across the business domains within each critical infrastructure sector.

[Specific Measures]

A) Support for the "CEPTOAR Council" (Cabinet Secretariat)

In order to ensure smoother operations of the "CEPTOAR Council" started up in February 2009 as a place for mutual help activities comprising each critical infrastructure sector, the activities of the "CEPTOAR Council" such as the promotion of cross-sectoral information sharing with the objective of contributing to the improvement of service maintenance and restoration capability are to be supported.

- Organization and dissemination of Safety Standards

Analyze and verify guidelines to formulate the Safety Standards to organize and disseminate the said Safety Standards among the critical infrastructure operators and their business domains; adapt to changes in the trends of socioeconomic activities; reflect new knowledge; and continuously improve the Standards.

[Specific Measures]

A) Continuous Improvement of the "Safety Standards" Formulation Policy and the "Safety Standards" in Critical Infrastructure Sectors (Cabinet Secretariat and government agencies in charge of critical infrastructures)

a) The Cabinet Secretariat, with the cooperation of government agencies in charge of critical infrastructures, is to analyze and verify the guidelines, and decide on the "Principles for Formulating of "Safety Standards, Guidelines, etc." concerning Assurance of Information Security of Critical Infrastructures (Version 3)."

b) The Cabinet Secretariat, in order to respond to changes in social trends and reflect the new knowledge in a timely manner, will continue to analyze and verify the guidelines and prepare to publish the supplement to the guidelines in 2011 or thereafter as and when necessary.

c) The government agencies in charge of critical infrastructures will implement analysis and verification of "Safety Standards" in each critical infrastructure sector with end of FY2010 as the target by taking into consideration the guidelines and the specificity of each critical infrastructure sector. In addition, measures to revise the "Safety standards" as and when necessary are to be implemented.

B) Investigating the Thoroughness of Preparations for "Safety Standards" (Cabinet Secretariat and government agencies in charge of critical infrastructures)

With the cooperation of the government agencies in charge of critical infrastructures, the following investigations are to be carried out into the thoroughness of preparations for the "Safety Standards."

<Investigating the critical infrastructure sectors>

The grasping and verification of implementation situation and future implementation schedule for the analysis, verification and revision of "Safety Standards" are to be implemented in FY2010, and the results are to be published.

<Investigating the critical infrastructure providers>

The status of spread of "Safety Standards" is to be examined at the start of FY2010, and the results are to be published. In addition, the planning and preparation for the investigations of the following year is to be implemented.

C) Safety and Reliability Assurance of Telecommunication Systems for IP Networks (Ministry of Internal Affairs and Communications)

In order to plan for the provision of more stable ICT services in response to the progress of IP networks, what system preparation ought to be for the analysis and evaluation of the incident occurrence conditions or the contents reported by telecommunication providers during incident occurrence will continue to be studied with FY2010 as the target.

- Improvement of critical infrastructure protection measures

Improve the information security measures by critical infrastructure operators, etc. through constant efforts to analyze the threats against each business domain and by conducting regular cross-divisional emergency drills, so that the damage that may be caused by a serious failure can be isolated and minimized.

Further, such operators must consider to make the overall system (including controlling functions) more robust to ensure service continuity in the case of failure.

[Specific Measures]

A) Implementation of Common Threat Analysis (Cabinet Secretariat)

As for the threats occurring in common to critical infrastructure sectors, detailed investigation and analysis will be carried out for the five common threats classified in the analysis of FY2009 with commonality taken into consideration in FY2010. In particular, attention will be paid to threats brought by the changes in technology environment surrounding the system. In addition, the domestic and overseas research trends related to these are to be examined.

When implementing, besides getting the government agencies in charge of critical infrastructures, CEPTOARs and critical infrastructure providers to cooperate, the analysis results are to be passed back to these concerned parties.

B) Implementation of Cross-Sectoral Exercises (Cabinet Secretariat and government agencies in charge of critical infrastructures)

With the cooperation of CEPTOARs and critical infrastructure providers, exercise scenario that assumes the occurrence of a specific IT fault is to be created and cross-sectoral exercise carried out based on this, followed by the extraction of issues and organization of knowledge for conducting the exercise. Furthermore, the issues and the knowledge gained are to be shared with the relevant parties, and published where possible.

C) Response to Changes in Environment Highly Likely to Affect Critical Infrastructures (Cabinet Secretariat)

In order to detect changes in environment that are highly likely to result in major effects to information security measures, besides investigating the technological trends, consideration is given toward making the systems including control systems to be more robust so as to ensure service continuity even if a fault occurs.

In FY2010, basic investigation is to be carried out on the effects on the robustness of critical systems caused by changes in environment such as the introduction of IPv6 and the opening up of control systems.

D) Preparation of Support System for Reliability Improvement of Information System Used by Critical Infrastructures (Ministry of Economy, Trade and Industry)

a) Continuing from FY2009, in order to support the voluntary efforts by critical infrastructure providers to improve the reliability of information systems, the preparation and sharing of fault case database, quantitative macroanalysis of the information offered voluntarily, and provision of accumulated information to CEPTOARs are to be carried out.

b) Investigations are to be carried out on the domestic and overseas situations of security measures such as the control systems and next-generation transmission networks (smart grids) of the manufacturers and plants to create materials for the dissemination and enlightenment of information security measures for reducing vulnerabilities of critical infrastructure control systems.

E) Coordination and Support for Cyber-Attack (Incident) Response (Ministry of Economy, Trade and Industry) [Repetition: Refer to 1(1) • Alliance between public and private sectors]

F) Enhancement to Measures for Interference to Critical Radio Communications (Ministry of Internal Affairs and Communications)

a) Based on 3-year plan for radio wave monitoring system fulfillment and enhancement, in order to enhance the response during occurrence of critical radio communication interference incident, the centralization throughout the country for holidays and nighttime will be implemented for critical radio communication interference reporting starting from October 2010.

b) In order to maintain radio wave usage discipline, the improvement of performance of the radio wave monitoring facilities through remote operations will be devised, and the sensors of the same facilities will be renewed in FY2010.

c) In order to raise the sophistication and functionality of radio wave monitoring facilities, broadband monitoring technologies will be examined and researched.

- Elaboration of Business Continuity Plans

The critical infrastructure operators etc. are currently creating their respective Business Continuity Plans (BCPs). In collaboration with relevant parties, discuss the optimum information security measures that are consistent with other disaster countermeasures, considering possible information security threats (e.g. large-scale cyber attacks, earthquakes, and epidemics) and include the measures in the said BCPs.

[Specific Measures]

A) Enhancement to Business Continuity Plan (BCP) (Cabinet Secretariat)

Consideration is given to cooperation with relevant institutions on how information security measures ought to be to ensure the effectiveness of business continuity plans of critical infrastructure providers. In this case, consistency with the disaster countermeasures considered by relevant institutions and the guidelines for business contingency plans is to be devised.

Issues will be extracted in FY2010, and how countermeasures ought to be will be gathered in FY2011.

- Promotion of international alliances in the area of critical infrastructures

Utilizing international conferences, such as "Meridian" (an international process for Governments worldwide to discuss critical information infrastructure protection at policy level), learn and utilize good practices adopted by different countries. Also participate in international emergency drills to reinforce international alliances concerning critical infrastructure.

[Specific Measures]

A) Promotion of International Collaboration in Critical Infrastructure Sectors (Cabinet Secretariat)

a) International collaboration in critical infrastructure sectors is to be facilitated such as through active participation in the activities of IWWN (International Watch and Warning Network) and Meridian with the objective of facilitating international information sharing and collaboration to protect critical information infrastructures.

b) Participation as a member of IWWN in the Cyber Storm exercises (Cyber Storm III) to be held on a global scale in the autumn of 2010. In addition, preparations are to be carried out aimed at holding the IWWN conference in Japan in 2011.

c) In order to contribute to the improvement of Japan's information security measures, information will be disseminated to relevant domestic entities with regard to the IT fault incident cases and best practices obtained through international collaboration or overseas information collection.

[3] Reinforcement of Other Infrastructures

- Improvement and reinforcement of countermeasures against malware

In order to reinforce the measures against malware infections, maintain and improve counteractive capabilities against information security incidents and strengthen the information security measures taken by individuals on their PCs by promoting security awareness. At the same time, improve the functionality of the systems that collect and analyze information concerning security threats, and enhance network security measures as well, through raising awareness among Internet Service Providers (ISPs)[9] and their users. Further, international alliances in this field should also be promoted.

Take immediate action to clarify the legality of downloading or reverse engineering to analyze suspected malware samples. Also, any information concerning vulnerabilities and related remedies must be distributed promptly as a preventive measure against malicious activities.

[Specific Measures]

I) Response to Information Security Incident

A) Building of a Framework toward Stopping Cyber Attacks (Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

For the measures to prevent the infection with computer programs (bot programs) that carry out cyber attacks through remote operations by malicious third parties and the countermeasures for prompt and effective stopping of the sending of spam e-mail or cyber attacks from computers infected by bot programs, trials and studies encompassing the technical and countermeasure aspects are to be carried out with the objective of building a comprehensive mechanism by end FY2010 so as to enable individuals to respond without a sense of imposition.

In addition, exchange of required information with relevant overseas organizations about Japan's efforts is to be implemented.

B) Promotion of Effort toward Cyber-Attack Prevention and Early Countermeasures and Avoidance of Harmful Sites (Ministry of Internal Affairs and Communications)

a) With the cooperation of ISPs, a collection network for cyber-attack information is to be built, and consideration is given to the building of a framework toward prevention and early countermeasures against cyber attacks.

b) With the collaboration of telecommunication providers, proof of concept is to be carried out for a mechanism for users to avoid accessing harmful sites that distribute

[9] Abbreviation for Internet Service Provider.

malware.

C) Enhancement to Computer Security Early Warning System (Ministry of Economy, Trade and Industry)

a) In order to ensure prompt information sharing of computer viruses, unauthorized access and vulnerabilities among concerned users as well as to ensure smooth responses, IPA and JPCERT/CC are to enhance the "computer security early warning system" in a format that can respond to changes in threats. Specifically, in order to respond to the ingenuity of attack methods such as that of recent computer viruses, the organizations such as JPCERT/CC that carry out coordination and support for incident responses are to promote further raising the analytical capability on attack methods, and information sharing and collaboration involving analysis methods among specialists.

b) For the malware sample analyzed in incident response support activities of JPCERT/CC and the analysis results, consideration is given to effective usage methods such as appropriate mutual sharing with domestic and overseas relevant institutions in possession of similar information and linkage with the operations of internet fixed-point observation information sharing system (TSUBAME).

D) Popularization of Emergency Response Team in Organizations and Enhancement of Collaborative System (Ministry of Economy, Trade and Industry)

Enhancement is to be devised for the popularization of CSIRT and collaboration during emergency and normal times between JPCERT/CC and the CSIRTs in domestic and overseas organizations through sharing of materials related to CSIRT structure and operations, threat information or attack information contributing to incident countermeasures and responses, and specific countermeasures information added with required analysis between suitable parties.

II) Sample Analysis

A) Study on Virus Detection and Response Technologies for Malware Obfuscation (Cabinet Secretariat)

Development of technologies capable of dealing with sophisticated and diverse attacks is to be promoted for dealing with the appearance of types hard to be detected even by new antivirus software due to malware obfuscation and modularization. In FY2010, issues in the R&D of malware sample analysis and countermeasures are to be examined.

B) Clarification on the Lawfulness of Reverse Engineering of Software due to Security Assurance (Ministry of Education, Culture, Sports, Science and Technology)

Based on the report by the Subdivision on Copyright of the Council for Cultural Affairs, steps will be promptly worked out to clarify the lawfulness of reverse engineering for information security purposes.

C) Malware Information Collection and Provision (Ministry of Economy, Trade and Industry)

a) The system (TIPS) for automated access to web sites on the internet, malware collection and analysis, and accumulation of analysis results will be continuously operated, and the information will be provided to the general users. In addition, in order to carry out accurate information collection and analysis, and provision in concert with new viral infection manners through web sites and portable media (USB memory, etc.), enhancement to the functions of countermeasure tools such as TIPS including zero-day attack countermeasures is to be carried out.

b) From the viewpoint of the spread of information security measures, collaboration is to be carried out with virus countermeasures vendors using malware samples held by IPA or obtained from other operations and the sample analysis results.

D) Provision of Explanation of Targeted Attack Method and Countermeasures Information (Ministry of Economy, Trade and Industry)

Besides analyzing attack methods and formulating countermeasures while collaborating with relevant institutions and implementing the collection and analysis of samples of targeted attacks in response to each of IPA's "suspicious mail emergency call" and JPCERT/CC's incident response, necessary information will be provided.

III) Software Vulnerability Countermeasures

A) Support for Management of Software Vulnerabilities (Ministry of Economy, Trade and Industry)

a) JPCERT/CC activities related to enlightenment activities on the importance of software vulnerability management and support for vulnerability management in user organizations are to be stepped up such as by sending software vulnerability information in a format that is automatically incorporated into management tools.

b) Besides continuing to provide information that contributes to the vendor or user judging the importance and priority of measures by quantitatively comparing the seriousness of the vulnerability under internationally consistent criteria, enhancements are to be made to existing tools to facilitate a more reliable implementation of vulnerability countermeasures by the information system users and developers.

[1] Add search function for vulnerability classification information of "JVN iPedia" (vulnerability countermeasures information database) and start enhancing the management function.

[2] In order to reliably deploy the vulnerability information to users and server managers, besides expanding the OS supported by "MyJVN" (vulnerability countermeasures support tool for information system users), provide the function to check the software version and security settings at the same time.

B) Promotion of Safe Use of Software and Information Systems and Promotion of Measures to Reduce the Occurrence of Vulnerabilities (Ministry of Economy, Trade and Industry)

a) In order to minimize the response cost and damage occurrence risk accompanying the vulnerabilities discovered in software products and information systems after product distribution or system operations, besides reviewing the existing framework of the system (vulnerability handling system) that enables prompt response against the vulnerabilities of software products, the efforts by JPCERT/CC for devising the disclosure and dissemination of points to be considered by product developers from the viewpoint of information security at each stage such as software product and information system design, programming, and preshipment inspection in the form of explanatory materials and seminars are to be continued.

b) With regard to languages frequently used in embedded software that is not easy to modify after distribution, efforts are to be made to plan for the implementation of secure coding seminars and the spread of coding standards to development locations.

c) Besides continuously providing the developers with vulnerability verification tools for TCP/IP and SIP protocols used by the developers of embedded devices and intelligent home appliances, deal with newly discovered vulnerabilities.

d) In order to support the self-learning of website operators and product developers on the necessity of countermeasures and countermeasure methods, the experiential and practical learning tool "Vulnerabilities Practice Tool for Developers" is to be developed and released.

e) Consideration is given to technology to automatically collect and monitor the threat information exchanged and give alarm when necessary.

f) Consideration is given to vulnerability handling systems that enable the planning of prompt response against software product vulnerabilities.

C) Safety Improvement of Corporate Web Sites (Ministry of Economy, Trade and Industry)

The vulnerabilities of web applications are to be discovered early, and in order to be helpful in coping, the "Website Vulnerability Log Analytical Inspection Tool" (iLogScanner) that analyzes the log and inspects traces of external attacks is to be continuously provided to corporate website operators. In FY2010, for iLogScanner in particular, additional response to new attack patterns, addition of access log formats to be detected, and addition of log analysis function of Web Application Firewall (WAF (target is ModSecurity)) are to be carried out and released within the fiscal year.

D) Prioritized Provision of Information Related to Vulnerabilities of Software and Control Systems to Critical Infrastructure Providers and Support for Information Management Related to Information Security (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)[2] • Reinforcement of the information sharing system]

E) Building of Collaborative System for Dealing with Control System Vulnerabilities (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)[2] • Reinforcement of the information sharing system]

IV) Other Related Efforts

A) Investigation and Information Dispatch on Service Interference Attack Countermeasures (Ministry of Economy, Trade and Industry)

Consideration are to be given to service disruptions and methods of countering attacks such as DDoS (Distributed Denial-of-Service) which may disrupt corporate activities that use the web, and the study results are to be provided to those in charge of corporate countermeasures to be helpful in dealing with DDoS attacks.

B) Efforts toward Information Leakage Measures (Ministry of Economy, Trade and Industry)

In order to deal with information leakage measures including that of personal information, information leakage countermeasures tool possessing the function to prevent viral infection through file-sharing software is to be provided to the general public.

C) Promotion of DNSSEC Introduction (Ministry of Internal Affairs and Communications)

In FY2010, PR will be implemented toward a smooth introduction of DNSSEC (expanded specifications for ensuring properness of DNS response).

D) Establishment of the Common Evaluation Index for Reliability Assessment (Ministry of Economy, Trade and Industry)

In order to further promote quality control through quantitative data in system development projects, common rules are to be established to enable mutual use of evaluation indices and quantitative data formulated by relevant industry groups, and activities for wide dissemination are to be promoted. In FY2010, the index for visualizing software quality will be prepared, and proposal will be made to the International Organization for Standardization.

E) Enhancement to Spam E-mail Measures (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Consumer Affairs Agency) [Only e) is repetition: Refer to 2(1)[1] • Efficient and continuous improvement of information security measures in government agency information systems]

a) In order to deal with ever increasing spam e-mails which are increasingly ingenious and malicious, steps are to be worked out to steadily enforce the Act on Regulation of Transmission of Specified Electronic Mail with an opt-in format introduced by amending the law in 2008, and the Act on Specified Commercial Transactions.

b) With the cooperation of the "JEAG" industry group which is a private-sector group established under the initiatives of major domestic internet connection service providers and mobile phone operators, the introduction of technologies such as blocking of port 25 and sender domain authentication that are effective in the prevention of spam e-mail transmission is to be facilitated.

c) In order to deal with spam e-mail sent from overseas which makes up a large portion of the spam e-mails received in Japan, besides enhancing the collaboration with overseas enforcement agencies in charge of spam e-mail measures, cooperation of the private sector on international spam e-mail measures is to be promoted.

d) Besides, the "Project for Eliminating Spam E-mail" (from February 2005) is to be continuously implemented to facilitate steps such as notifying the internet connection service provider used for sending spam e-mail of information related to illegal spam e-mail and requesting suspension of usage.

e) The Cabinet Secretariat will push for the adoption of the sender domain authentication technology such as SPF (Sender Policy Framework) to rule out malicious third parties from impersonating government agencies or their staff and harm the general public or the private sector.

- Establishment and standardization of Information security measures adapted to cloud computing

Discuss and formulate guidelines concerning the information security requirements for building, operating, and using services based upon cloud computing, together with guidelines concerning information handling for each field in which cloud computing technology is likely to be applied.

[Specific Measures]

A) Investigation on Information Security Assurance Policy for Cloud Computing (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

Consideration is given to guidelines on information security requirements for the building, operation and usage of cloud services, usage guidelines for data centers related to the advance of cloud technology, and disclosure authorization system for information related to the safety and reliability of data centers. The system for promoting the formulation of guidelines is to be prepared in FY2010.

B) Cloud Computing Security (Ministry of Economy, Trade and Industry)

For cloud computing which is expected to witness usage expansion in future, items that ought to be given security consideration when used by small-to-middle sized businesses are to be studied. In addition, they are to be reflected in information security audits. Furthermore, efforts are to be pursued toward international standardization.

C) Formulation of Checklist for Service Level of Cloud (Ministry of Economy, Trade and Industry)

In order to clarify the entity responsible for data protection and service quality when using cloud computing, a common recognition format for assurance criteria of service contents, scope, quality, etc. (e.g.: service availability ratio, reliability level, data management method, security level, etc.) between the cloud provider and the cloud user is to be urged so as not to overburden the service providing side, and a checklist for cloud/service/level is to be prepared.

D) R&D on a Highly-Reliable and Energy-Saving Network Control Technology Supporting Cloud Services (Ministry of Internal Affair and Communications)

By FY2012, while devising energy saving for the entire network, R&D on a highly-reliable and energy-saving network control technology that links clouds are to be carried out with the objective of establishing leading technologies so that the highly-reliable high-quality cloud services can be used by anyone.

- Ensuring the IPv6-related information security

To address the issues concerning IPv6-related information security, identify concrete information security problems by utilizing the related verification environments, and cultivate human resources to ensure a smooth migration to IPv6.

[Specific Measures]

A) Preparation of a Test Bed for Acquiring IPv6 Operation Techniques (Ministry of Internal Affairs and Communications)

Continuing into FY2010, in order to devise improvements to the operations technique of private-sector network operators as well as to nurture and guarantee IPv6 talents, an experimental IPv6 network (test bed) having the complexity of actual network level is to be prepared.

B) Security Measures for IPv4/v6 Mixed Environment (Ministry of Internal Affairs and Communications)

Information security technology issues common to the public and private sectors are to be organized so as to ensure appropriate security in the IPv4/v6 mixed environment.

In addition, as it is necessary for the internet service providers to provide IPv6 connection service to individual users, information on the IPv6 connection service provision situations of the internet service providers is to be provided on web sites.

- Ensuring information security in networks of intelligent home appliances, mobile terminals, electronic tags, and sensors

A range of devices, including intelligent home appliances, mobile terminals, electronic tags, and sensors, are now being connected to various networks. To ensure the information security of such networks: prepare safety assessment procedures, including verification tools for developers, and establishing a safety assessment system; eliminate technological obstacles; and create new usage guidelines.

[Specific Measures]

A) Study on Security Assurance Policy of Intelligent Home Appliances, Mobile Terminals, Electronic Tags, and Sensor Networks

As information security assurance policy when whatever thing is connected to the network, verification tool and safety assessment system for developers are to be prepared. In FY2010, information security technology issues in ubiquitous environment are to be organized.

B) Promotion of Safe Use of Software and Information Systems and Promotion of Measures to Reduce the Occurrence of Vulnerabilities (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)[3] • Improvement and reinforcement of countermeasures against malware]

C) Preparation of Security Assessment and Certificate System for System LSI (Ministry of Economy, Trade and Industry)

By FY2011, for system LSI used in IC cards, in order to carry out the required system preparations so as to be able to perform security evaluation and certification based on ISO/IEC 15408 domestically, in FY2010 in continuation from the previous fiscal year, the preparation of common use facilities for security evaluation and certification, nurturing of talent, development of technology, survey, etc. are to be steadily implemented.

D) Prioritized Provision of Information Related to Vulnerabilities of Software and Control Systems to Critical Infrastructure Providers and Support for Information Management Related to Information Security (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)[2] • Reinforcement of the information sharing system; 2(1)[3] • Improvement and reinforcement of countermeasures against malware]

E) Building of Collaborative System for Dealing with Control System Vulnerabilities (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)[2] • Reinforcement of the information sharing system]

F) Support for Information Security Assurance during Information System Procurement (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)[1] • Building up a mechanism to enable thorough implementation of information security measures in government agency information systems]

- Ensuring information security in medical and education fields

Identify the means to promote information security measures in the medical and educational fields, such as establishing guidelines for medical/educational bodies and the nation for utilizing ICT safely and securely.

[Specific Measures]

A) Efforts toward Popularization of ASP/SaaS in the Medical and Education Sectors (Ministry of Internal Affairs and Communications)

The following materials are to be created for use by ASP[10]/SaaS[11] service providers and users, and popularization efforts are to be pursued.

a) Reference example for SLA[12] that organized items of agreement demanded in the provision of service by ASP/SaaS providers to medical institutions based on the "Guidelines for Information Disclosure concerning ASP/SaaS Security and Reliability for Medical Information"

b) Guidelines organized for items that ought to be abided by or given attention when the ASP/SaaS providers roll out the service for the education sector (school sector)

- Supporting information security measures in small-to-middle sized businesses

Organize arrangements to encourage small-to-medium sized business to invest in strategic ICT with advanced information security. Also support them to do so through providing information concerning information security and consultancy services utilizing incorporated administrative agencies and relevant organizations.

[10] Application Service Provider

[11] Software as a Service

[12] Service Level Agreement

[Specific Measures]

A) Popularization of Information Systems with Assured Advanced Information Security in Small-to-Middle Sized Businesses (Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

a) Information system investments with assured advanced information security in small-to-middle sized businesses are to be facilitated through planning for the dissemination and enlightenment of small-and-medium enterprise infrastructure enhancement taxation system.

b) A system as the infrastructure for software provision service (SaaS) using the internet and that allow cheap and easy business efficiency and operational improvements even in small-and-medium and the security management application running on it are to be popularized.

B) Promotion of Information Security Measures in Small-to-Middle Sized Businesses (Ministry of Economy, Trade and Industry)

a) The "information security leadership nurturing seminar for small-to-middle sized businesses" targeted at those in a position to guide small-to-middle sized businesses and the "information security seminar" targeted at small-and-medium local enterprises are to be held, and improvement to the security level of small-to-middle sized businesses is to be devised by having information security knowledge acquired at the seminars.

b) The dissemination of the information security measures guidelines for small-to-middle sized businesses created in FY2008 is to be facilitated with the objective of rationalizing the cost burden for information security measures and promoting the measures in small-to-middle sized businesses that are facing difficulty in promoting information security measures.

C) Information Security Consultation Service Targeted at Small-and-Medium Enterprises and Provision of Appropriate and Accurate Information (Ministry of Economy, Trade and Industry)

a) Those in a position to guide the small-to-middle sized businesses that went through the "information security leadership nurturing seminar for small-to-middle sized businesses," besides providing information security consultations using training courses, are to introduce and provide the enlightenment materials and guidance tools created by IPA, etc.

b) IPA will consider developing tools and provide to those in a position to guide the small-to-middle sized businesses as support for information security consultations.

In 2010, IPA will support consultations by local NPOs and those in a position to guide the small-to-middle sized businesses, and consideration will be given to the cooperation policies between the respective entities and the information provision for each entity.

- Promoting safe electronic trading

To protect important financial information - such as credit card details - implement information security measures that meet international security standards. Formulate information security standards for Web sites that operate electronic trading and encourage such operators to ensure compliance with the said standards. Also keep implementing the new information leakage prevention measures.

[Specific Measures]

A) Facilitation and Spread of Electronic Signature Use in Business (Ministry of Internal Affairs and Communications, Ministry of Justice, and Ministry of Economy, Trade and Industry)

Taking into consideration the study results of the "Study Committee Concerning Enforcement of the Electronic Signature and Authentication Law" held in FY2007, consideration will be given to the spread and facilitation policies for the use of electronic signatures in business.

- Promoting intellectual property protection

To protect the intellectual property owned by corporations etc., raise intellectual property protection awareness utilizing the Anti-Counterfeiting Trade Agreement (ACTA) and implementing contents copyright infringement measures on the Internet based on the Intellectual Property Promotion Plan 2010 (formulated May 2010).

[Specific Measures]

A) Enhancement to Access Control Avoidance Regulation (Ministry of Education, Culture, Sports, Science and Technology, Ministry of Economy, Trade and Industry, and Ministry of Finance)

Besides introducing regulation on specific avoidance of access control for protection of authored works while preparing appropriate exclusion stipulations so as not to invite the withering of product development and R&D, regulations for access control avoidance devices are to be enhanced through the expansion of target actions (provision of manufacturing and avoidance services), expansion of target devices (relaxation of the "only" requirements), criminalization, and the introduction of border control taking these into consideration.

For this reason, specific system reform will be completed in FY2010 taking into consideration the legal and technical viewpoints.

B) Facilitation of Infringement Measures of Providers (Ministry of Internal Affairs and Communications)

An effective mechanism is to be set up in FY2010 to devise new measures (for example, sending warning mail or detection using technical means) against infringement of contents on the internet by joint actions of the provider and copyright owner. In addition to devising the verification of current law on provider liability limitation, the necessity of revision to the system in order to ensure effectiveness is to be considered and a conclusion reached in FY2010. Furthermore, necessary steps are to be worked out taking into consideration the progress of the various efforts.

C) Expansion of Signatory Countries at or after Conclusion of ACTA Negotiations (Ministry of Foreign Affairs, Ministry of Internal Affairs and Communications, Ministry of Justice, Ministry of Finance, Ministry of Education, Culture, Sports, Science and Technology, and Ministry of Economy, Trade and Industry)

Besides concluding the negotiations of the Anti-Counterfeiting Trade Agreement (ACTA) in FY2010, the reach of worldwide protection is to be widened through the expansion of signatory countries for major countries and territories and bilateral agreements after the conclusion.

[4] Enhancement of the Functions of the National Information Security Center (NISC)

- Enhancement of NISC's comprehensive coordination functions

Enhance NISC's advanced functions to gather and analyze information concerning information security in order to enhance expertise and reinforce the public-private sector alliance.

[Specific Measures]

A) Strengthening of NISC (Cabinet Secretariat)

In order to become the center of the promotion system for information security measures for the entire government, outstanding talents regardless of whether from the public sector or private sector are to be roped in.

Under this system, the fulfillment of information collection as well as the information sharing and analysis function with relevant institutions is to be enhanced, and its function as the center for the promotion of cross-sectoral information security measures maintained. In addition, the functions for investigating and studying the various trends and basic information required in the promotion of information security measures based on the PDCA cycle is to be expanded.

B) Fulfillment of Information Security and Consulting Functions for the Promotion of Information Security Measures of Concerned Government Agencies (Cabinet Secretariat)

In order to support the promotion of the information security measures of the concerned government agencies, NISC will continuously strive to fulfill the information security and consulting functions through the experts of the center in order to respond to the various needs toward promoting the information security measures of the concerned government agencies such as the responses related to the Standards of Measures, and the emergency responses.

C) Strengthening of Cooperation with Relevant Organizations (Cabinet Secretariat, and Cabinet Office)

The IT Strategic Headquarter will from the outset closely cooperate with the relevant centers and councils such as the Council for the Formulation of a Growth Strategy, the Council for Science and Technology Policy, the Central Disaster Prevention Council, and the Intellectual Property Strategy Headquarters, and will uniformly promote the information security measures for the entire government by closely cooperating in proposing or implementing the various policies.

(2) Reinforced Protection of the Nation/Users

[1] Conducting and Information Security Campaign

To raise awareness about IT risks among the nation/users and encourage them to take information security measures individually, an information security awareness campaign must be conducted. From February 2010, every February will be called "Information Security Month" and a campaign implemented. To enhance the effect of such campaign, a "Comprehensive Program for Awareness-raising" must be formulated.

[Specific Measures]

A) Implementation of "Information Security Month" (Cabinet Secretariat and concerned government agencies)

In order to heighten the information security concerns and deepen the understanding of each person in the country, the dissemination and enlightenment activities related to information security will be enhanced with February of each year being designated as the "information security month."

B) Investigating the Information Security Dissemination and Enlightenment Method (Cabinet Secretariat)

In order to dispel the uneasiness of the people in relation to information security, basic policies and specific measures are to be considered for promoting the dissemination and enlightenment activities by cooperating with the public and private sectors while taking into consideration the international efforts related to information security, and the "Comprehensive Program for Awareness-raising" will be formulated and published by March 2011.

C) Promotion of Dissemination and Enlightenment through Various Types of Media (Cabinet Secretariat, National Police Agency, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry, and Ministry of Education, Culture, Sports, Science and Technology)

a) As a joint undertaking with the Korea Internet & Security Agency (KISA), slogans and posters for raising the awareness of information security measures will be invited and selected works will be published, and the nurturing and improvements of information security awareness in the country's younger generation will be devised.

b) During the Information Security Month of FY2010, in order to honor individuals and corporations who contributed greatly from the viewpoint of information security, the "Information Promotion Contribution Award (information security promotion category)" will be held.

c) The "Council for the Promotion of Safe and Secure Information and Communication" will invite "slogans for the safe and secure use of infocom" and select and award works including best work (the Minister of Internal Affairs and Communications Award).

d) In order to improve the nation's information security awareness, in FY2010, appropriate information will be provided to each person in the country through efforts such as "@police," "information security site for the people," "internet safety classes," "Council of Anti-Phishing Japan," and "Council of Anti-Phishing Japan" taking into consideration the situation of information security threats of rapidly increasing sophistication and complexity. These efforts will focus not only on IT beginners, but also on active IT users who are not too concerned with information security.

e) Continuing from FY2009, a course ("e-Net Caravan") mainly targeting guardians and educators for enlightening children toward the safe and secure use of the internet, will be held nationwide in cooperation with telecommunication organizations.

D) Promotion of Dissemination and Enlightenment of Information Security Measures through Multi-country Meetings (Cabinet Secretariat and concerned government agencies)

In order to plan for raising the awareness on information security of each country and cooperation in talent development through the settings of multi-country meetings such as APEC-TEL-WG, Meridian (international meeting on critical infrastructures), and ASEAN-Japan Information Security Policy Meeting, efforts are to be actively implemented toward raising international awareness with the cooperation of each country.

E) Facilitation of Publicity of the Provider Liability Limitation Law and Related Guidelines (Ministry of Internal Affairs and Communications)

In 2010, the publicity by industry groups of the provider liability limitation law and related guidelines through web sites will be supported.

F) Enhancement to Publicity and Enlightenment Activities for Maintenance of Radio Wave Usage Discipline (Ministry of Internal Affairs and Communications)

In the radio wave usage environment protection publicity and enlightenment period in June of each year, publicity and enlightenment through various types of media will be implemented with the cooperation of concerned government agencies.

In addition, during June to August and October to November of 2010, besides the publicity and enlightenment for stores selling devices that use radio waves, the regional Bureaus of Telecommunications will implement internet banner advertising with regard to the checking of "technical standard compliance mark".

G) Provision of Various Tools and Analyses that Contribute to Information Security Measures (Ministry of Economy, Trade and Industry)

a) The information security measures benchmark system will continue to be provided.

b) The "Latest Security Information Navi (Security Information RSS portal)" that collects and accumulates RSS related to information security sent from major web news sites will continue to be provided, and information collection related to information security measures through the Web will be supported.

c) Survey and social science analysis will be carried out on the risk in the promotion of information security measures as well as the human action and investment against risks.

d) Costs and results of countermeasures, and the positioning of countermeasure actions in the social system will be clarified through workshops held jointly with relevant domestic organizations.

e) The information security situation and outlook of FY2009 will be gathered into the "Information Security White Paper 2010" and published.

H) Support for Information Security Assurance during Information System Procurement (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)[1] • Building up a mechanism to enable thorough implementation of information security measures in government agency information systems]

I) Usage and Dissemination of Method of Agreeing to Non-Functional Requirements (Ministry of Economy, Trade and Industry)

In order to improve the reliability of information systems, for the non-functional requirement[13] items including requirements related to reliability, performance or security, efforts will be pursued with the cooperation of relevant industries on the usage and

[13] The requirement items related to the performance and quality of information system and software such as response time, time restriction on batch processing, or usability are called non-functional requirements.

dissemination of methods for appropriately agreeing between users and vendors.

[2] Suggestion to Set Up the "Information Security Safety Support Service" (tentative name)

Consider establishing an Information Security Safety Support Service (tentative name) in order to provide the nation/users with a consultation service concerning information security, as well as to provide support to local NPOs that work towards improving information security standards among the nation/users.

[Specific Measures]

A) Suggestion to Set Up "Information Security Consultation Service (tentative name)" (Cabinet Secretariat and concerned government agencies)

In order to provide consultations related to information security to the nation and users, the Cabinet Secretariat, with FY2010 as the target, will consider what the "Information Security Safety Support Service (tentative name)" ought to be while using existing framework.

B) Information Security Consultation Service and Appropriate and Accurate Information Dispatch (Ministry of Economy, Trade and Industry)

General consultation service for malware such as fake antivirus software is to be added to the consultation service set up by IPA for computer viruses, and besides expanding the consultations for information security faced by computer users, the service is to be widely publicized to the nation.

Furthermore, the information covered by consultations is to be reflected in the measures for arousing computer users' precautions.

C) Nurturing and Using Information Security Supporter (Ministry of Internal Affairs and Communications)

The raising of information security of the whole nation is to be carried out by nurturing and using knowledgeable people (information security supporter) around users through creation of teaching materials related to information security and support for holding training courses and certification testing.

[3] Promotion of Personal Information Protection

- Promotion of appropriate usage of privacy protection technology

To prevent any occurrence of a large-scale private information leakage, promote appropriate usage of privacy protection technology including setting access rights, managing authentication information, cipher, and anonymization, etc.

[Specific Measures]

A) Study on Appropriate Usage Method of Privacy Protection Technology (Cabinet Secretariat)

From the viewpoint of preventing large-scale personal information leakage, consideration is given to the appropriate usage methods of privacy protection technology such as access rights setup, authentication information management, cipher, and anonymization.

B) Efforts on Information Leakage Countermeasures (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)[3] • Improvement and reinforcement of countermeasures against malware]

- Review of private information protection guidelines for each industry

To prevent the leakage of private information from corporations, encourage firms to encrypt such data. Review the current privacy protection practices in each industry, taking account of their respective characteristics, aiming to give an incentive for corporations to make full use of ciphering methods. Some possible incentives include simplifying incident management procedures when a leak has occurred but when appropriate technological safety measures have been applied to such information.

[Specific Measures]

A) Study on Review of Personal Information Protection Guidelines for Each Industry (Cabinet Secretariat and concerned government agencies)

With June 2011 as target, from the viewpoint of preventing information leakages such as that of personal information from enterprises, in order to facilitate the appropriate ciphering of information, a study is to be carried out on what incentive ought to be given to industries while taking into consideration the specificity of each industry such as by simplifying the procedures if appropriate technical security management measures were implemented for the leaked personal information.

B) Review of "Guidelines for Personal Information Protection in Telecommunications Businesses" Related to Safety Management Measures (Ministry of Internal Affairs and Communications)

In the event of loss of a portable computer and the like, if appropriate technical protection measures were adopted for the leaked personal information, the relaxation of a portion of the procedure (notification to affected persons, announcement of facts, report to the government agency in charge) demanded of businesses is to be clarified in the guidelines.

- Adapting to the international framework

To encourage the appropriate and safe international use of private information, study the information security schemes conducted in a range of international frameworks, such as the Organisation for Economic Cooperation and Development (OECD), the Asia-Pacific Economic Cooperation (APEC), and the European Union (EU). Based on such study, build up international coordination such as through cooperating on cross-border legal enforcement concerning privacy protection. At the same time, gain the understanding of other countries' with regard to Japan's legal system and examine the actions that Japan should take concerning international data privacy protection, while maintaining consistency between Japan's legal system and those of other countries in relation to this issue.

[Specific Measures]

A) Responding to International Efforts on Personal Information Protection (Consumer Affairs Agency)

In FY2010, Japan will attend the meeting of the OECD Committee for Working Party on Information Security and Privacy's under the Committee for Information, Computer and Communications Policy and the meeting of the APEC Electronic Commerce Steering Group's Data Privacy Subgroup, grasp the considerations on cross-border issues of privacy law enforcement in OECD and the efforts of APEC Data Privacy Pathfinder projects, etc. and besides considering the responses and measures required of Japan from the viewpoint of international cooperation, international understanding of Japan's personal information protection laws will be sought.

B) Study toward Research Collaboration of Measures for Data Privacy Protection (Cabinet Secretariat)

While taking into consideration the trends of existing international discussions such as in OECD and APEC, consideration is given toward research collaboration on measures for data privacy protection through international conferences such as the ASEAN-Japan

Information Security Policy Meeting following rapid changes in environment.

- Reviewing the Act on the Protection of Personal Information

Review the Act on the Protection of Personal Information, identifying any specific problems in consideration of reforming the law.

[Specific Measures]

A) Reviewing the Act on the Protection of Personal Information (Consumer Affairs Agency and concerned government agencies)

For the Personal Information Protection Act, from FY2010 onwards, consideration is given to deliberations on issues with a view of amending the law.

[4] Tighten Policing against Cybercrime

• Organization of a cybercrime policing infrastructure

Reinforce cybercrime policing, as well as organize infrastructural arrangements, such as utilization of digital forensic technology and strengthening international coordination.

Further, build close alliances between the public and private sectors to realize a crime-resistant society, such as by forming a mutually cooperative relationship between legal institutions and the public (victims of crime) sufficient to gain information to identify the causes of problems and elucidate criminal processes, which may then lead to the arrest of suspects and minimization of damage.

[Specific Measures]

A) Enhancement to the Preparedness for Cybercrime Policing (National Police Agency)

Besides actively implementing training inside and outside the department for nationwide police staff engaged in cybercrime investigation, the preparedness to appropriately tackle cybercrimes will be enhanced such as by promoting the preparation of resources, equipment and materials for policing cybercrimes.

B) Promotion of Digital Forensic Efforts (National Police Agency) [Repetition: Refer to 1(1) • Policing cybercrimes]

C) Enhancement to Cooperation with the Private Sector for Maintenance of Cyberspace Safety and Discipline (National Police Agency)

In order to enhance public-private cooperation for appropriately dealing with cybercrimes, efforts to set up internet cafe liaison councils in the respective local prefectural police organizations will be promoted.

D) Promotion of Efforts toward Public-Private Cooperation for a Crime-Resistant IT Society (National Police Agency)

The Comprehensive Security Measures Conference comprising knowledgeable persons, relevant providers, PTA representatives, etc. will be held, and consideration is given to what the cooperation between the government and information security industry ought to be.

E) Promotion of International Cooperation for Cybercrime Policing (National Police Agency) [Repetition: Refer to 1(1) • Policing cybercrimes]

F) Promptness of International Investigative Mutual Assistance Using Central Authority System[14] (Ministry of Justice)

In principle, mutual legal assistance treaties or accords came into force between Japan-US, Japan-South Korea, Japan-China and Japan-HK making mutual assistance obligatory, and under these treaties or accords, central authorities are set up to pursue promptness of mutual assistance through direct communications for mutual assistance between the central authorities without going through the diplomatic channels. In addition, respective mutual legal assistance treaties or accords were also signed in May and December of 2009 between Japan-Russia and Japan-EU which were approved by Japan's parliament in April 2010. Hereafter, besides aiming for the treaties or accords to come into force, consideration will be given to the conclusion of more mutual legal assistance treaties.

- Crime prevention campaign

Raise the awareness of self defense against cybercrimes among the nation as a preventative measure. To this end, promote a range of crime prevention campaigns, including providing information security lectures.

[Specific Measures]

A) Enlightenment for Protection from Unauthorized Access, and Dissemination of Knowledge (National Police Agency, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

Continuing from FY2009 and based on the Unauthorized Computer Access Law, enlightenment for protection against unauthorized access and dissemination of knowledge will be pursued through efforts such as the disclosure of occurrence situation of unauthorized access as well as the R&D situation for access control functions.

B) Implementation of Information Security Courses (National Police Agency)

In order to plan for the improvement of information security awareness and knowledge, lectures with topics including cybercrime situations and arrest cases are to be held throughout the country targeted at educators, local government staff, and general users of the internet.

C) Promotion of Cybercrime Damage Prevention Measures (National Police Agency)

[14] Refers to a system for provision of mutual assistance between central authorities without going through the diplomatic channels by designating a specific authority as the central authority.

a) Besides creating leaflets for junior high school and senior high school students for the prevention of criminal damages related to dating sites and creating pamphlets for the prevention of cybercrime damages, and having the respective local prefectural police distribute them, publicity and enlightenment such as those on basic countermeasures, cybercrime methods and countermeasures carried on the National Police Agency web sites in response to the various troubles of internet users will be implemented in addition to the pamphlets.

b) For the National Police Agency's security portal site "@police," publicity and enlightenment activities will be promoted to deter cybercrime such as by appropriately providing vulnerability reports for various types of software and information related to information security such as internet fixed-point observation data in response to changes in conditions.

D) Promoting the Nurturing of Cyber Volunteers (National Police Agency)

Efforts toward the fostering of a safe and secure internet space will be promoted by devising the facilitation for nurturing cyber volunteers through the setup of volunteer activities and nurturing policies in cyberspace.

(3) Reinforcement of International Alliances

[1] Strengthening Alliances with the United States, ASEAN, and EU (Strengthening Bilateral Relationships and Ties with ASEAN)

Strategically strengthen political alliances with other countries through bilateral Conference on Cyber Security (between the United States and Japan) and the ASEAN-Japan Information Security Policy Meeting. Build practical networks by helping to establish overseas Computer Security Incident Response Teams (CSIRTs) and holding seminars on information security measures.

In addition to the above initiatives, build a new bilateral alliance with those countries in which Internet usage is rapidly expanding.

[Specific Measures]

A) Enhancing Bilateral Policy Dialogs Related to Information Security Policies (Cabinet Secretariat and concerned government agencies)

In order to build close cooperation on information security policies between regions, in FY2010, enhancement of strategic bilateral cooperation such as discussions on collaboration in individual fields will be planned by holding bilateral meetings such as with US and ASEAN countries. In addition, a study toward building relations with various European countries is to be initiated.

B) Enhancement to ASEAN-Japan Cooperation through Promotion of ASEAN-Japan Information Security Policy Meeting (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

In order to speed up the efforts toward the building of a secure business environment in the Asian region with deepening economic relations with Japan, the protection of the reliability of infocom infrastructure that supports economic activities and technology innovations, and the drafting of a cross-sectoral information security policy by the government, cooperation will be enhanced with various ASEAN countries through the ASEAN-Japan Information Security Policy Meeting.

a) Steady promotion of items decided at the Second ASEAN-Japan Information Security Policy Meeting (FY2010/2011)

b) Holding the Third ASEAN-Japan Information Security Policy Meeting in Japan (FY2010)

c) Holding the ASEAN-Japan Government Networks Security Workshop in Vietnam (the Second, FY2010) and in Japan (the Third, FY2011)

d) Holding training related to national strategy formulation and government networks security for government staff of various ASEAN countries in Japan (FY2010)
e) Jointly hold dissemination and enlightenment events with various ASEAN countries (FY2011)
f) Facilitating mutual sharing of experience and knowledge cultivated by network operators of the Japan and ASEAN member countries by holding workshops, etc. (FY2010)
g) In order to contribute to specific research cooperation, researchers and research institutions involved in network security research activities in Japan and ASEAN member countries are to be designated (FY2010)

C) Promotion of Information Security Cooperation in APEC (Ministry of Internal Affairs and Communications)

R&D collaboration in the field of network security among Japan and countries in the APEC region is to be promoted.

D) Holding Trainings and Seminars for Developing Countries (Ministry of Internal Affairs and Communications)

Information security training is to be implemented for the government staff and telecommunication providers of developing countries.

E) Implementation of Secure Coding Seminars in Software Development Outsourcee Countries (Ministry of Economy, Trade and Industry)

In FY2010, technical seminars held by JPCERT/CC for coding methods without weaved-in vulnerabilities are to be implemented centered around the various countries such as in the ASEAN region to which Japan's enterprises outsource the development of embedded software.

F) Promotion of the Building of Secure Business Environment in the Asian Region (Ministry of Economy, Trade and Industry)

Based on the "Asian knowledge economy initiative" advocated by Japan at the 2008 ASEAN-Japan Economic Ministers Meeting, besides giving consideration to the policies and efforts for promoting the building of a secure investment and business environment in the Asian region, dialogs with relevant parties will be implemented.

In addition, in relation to the assessment and certificate system for information security products, measures in line with international practices will be urged.

G) Support for Building up and Operating CSIRT in Overseas Organizations (Ministry of Economy, Trade and Industry)

Keeping in mind the countries and territories such as those in the Asia Pacific region which have deep relations with the business activities of Japanese businesses, the building up and operations of CSIRT as well as collaborative support are to be carried out. In FY2010, dissemination and enlightenment of CSIRT establishment seminars and technical support activities are to be carried out.

H) Support for Enhancement of CSIRT System Responsible for External and Internal Coordination in Each Country and Enhancement of Cooperation (Ministry of Economy, Trade and Industry)

a) In the Asia-Pacific region, the setting up and operations of CSIRT responsible for external and internal coordination in each country as well as support for cooperation are to be carried out. In FY2010, based on the experience of support activities for CSIRT establishment accumulated in JPCERT/CC, the operations technology for incident response job and experience related to cooperation and operations between CSIRTs will be shared.

b) The incident response cooperation between JPCERT/CC and each country's CSIRT is to be further enhanced through the activities of FIRST (Forum of Incident Response and Security Teams), IWWN and APCERT, as well as activities such as incident response exercise in the Asia-Pacific region. In FY2010, participation in Cyber Storm III is scheduled as IWWN community, and further enhancement to the cooperation with overseas CSIRT member teams is planned using this opportunity.

I) Facilitation of Sharing Early Warning Information in the Asia-Pacific Region (Ministry of Economy, Trade and Industry)

a) With regard to the internet fixed-point observation information sharing system (TSUBAME) for the Asia-Pacific region, efforts for linking the joint analysis and malware analysis cooperation between the operations entity JPCERT/CC and the relevant organizations of each participating country are to be promoted.

b) In order to formulate effective protective measures against cyber attacks, the techniques and methods used in the attacks as well as their trend and regional characteristics will be analyzed, and the method of sharing the analysis method and the analysis results is to be studied with the participation and/or cooperation of members primarily from the Asian region's CSIRTs,.

J) Enhancement to Spam E-mail Countermeasures (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Consumer Affairs Agency) [Repetition: Refer to 2(1)[3] • Improvement and reinforcement of countermeasures against malware]

[2] Building an Information Sharing System through International Conferences, such as APEC, ARF, ITU, Meridian, and IWWN

Actively participate in international conferences in different areas, including APEC, ASEAN Regional Forum (ARF), International Telecommunications Union (ITU), Meridian, International Watch and Warning Network (IWWN), Forum for Incident Response and Security Teams (FIRST), and Asia Pacific Computer Emergency Response Teams (APCERT), to build an information sharing system with overseas organizations.

[Specific Measures]

A) Promotion of International Collaboration and Cooperation in Multilateral Frameworks (Cabinet Secretariat and concerned government agencies)

Active participation in international conferences in the various fields such as the field of critical infrastructure protection like Meridian, the field of global economic activities like APEC (Asia-Pacific Economic Cooperation), OECD (Organisation for Economic Co-operation and Development) and ASEAN (Association of Southeast Asian Nations), the field of incident response like FIRST (Forum of Incident Response and Security Teams), and the field of national security guarantee like ARF (ASEAN Regional Forum) will be pursued, and active information sharing relating to critical infrastructure protection, global efforts including standardization, incident response, and cyber-attack countermeasures will be carried out.

B) Support for Enhancement of CSIRT System Responsible for External and Internal Coordination in Each Country and Enhancement of Cooperation (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(3)[1]]

C) Efforts for the Improvement of the Information Security Evaluation and Certification Technology in the Asian Region (Ministry of Economy, Trade and Industry)

At the second meeting (scheduled to be held at Kuala Lumpur in July 2010) of the AISEC (Asian IT Security Evaluation and Certification) Forum established with IPA as the main entity and with the purpose of promoting international mutual recognition agreement regarding information security evaluation and certification in the Asian region, information exchange will be carried out with regard to the support for the establishment of evaluation and certification system in the various Asian countries and the technology and trends of security evaluation and certification.

D) Participation in the Planning of International Standardization in Information Security Field (Ministry of Economy, Trade and Industry)

Japan will participate in international meetings hosted under ISO/IEC JTC 1/SC 27 which are international standardization activities in the information security field, and will actively participate in the planning so that Japan's IT environment/standards/guidelines/etc. are taken into consideration and reflected in international standards.

[3] Enhancement of the NISC's Function as a Point of Contact

As an international Point of Contact (POC) in regard to comprehensive information security issues, NISC must reinforce its alliances with the relevant overseas organizations in terms of information security policy, which includes sharing information about good information security practices conducted in different countries and measures taken to safeguard their critical infrastructures.

[Specific Measures]

A) Cooperation with Each Country through Enhancement of International Contact Function (Cabinet Secretariat)

a) As an international POC (point of contact), international PR and information dispatch will be endeavored in relation to the basic idea and strategy of the information security policy of Japan which is a developed information security country as well as the best practices in the public and private sectors. For example, active PR activities will be rolled out through web sites such as by publishing the English editions of the Strategy and this document on the NISC web site in FY2010.

b) The trends of standardization and international organizations related to information security policy grasped at conferences, overseas best practices, information related to threats, vulnerabilities, etc. will be shared with relevant domestic organizations and passed back.

(4) Furtherance of Technological Strategies etc.

[1] Strategic Furtherance of Information Security Research and Development

To strategically propel information security research and development, taking account of US movements, formulate a new information security research and development strategy.

This strategy should address: overcoming ICT vulnerability, including Internet usage, to ensure user safety; development of information security technology adapted to new ICT, including IPv6, cloud computing, intelligent home appliances, mobile terminals, and sensor networks, etc.; research and development of information security technology that can counteract against increasingly sophisticated and diversified attacks (R&D to Solve Grand Challenges in Information Security); and the dissemination of such technologies. Also, reinforce and disseminate system design management measures that can handle real-life information security threats.

[Specific Measures]

A) Formulation of New Information Security R&D Strategy (Cabinet Secretariat)

In order to strategically promote information security R&D taking into consideration the trends of US cyber security enhancement legislations, a new information security R&D strategy is to be formulated with June 2011 as the target.

B) Study on the "Grand Challenge" Theme and Promotion Framework (Cabinet Secretariat, Cabinet Office, National Police Agency, Ministry of Internal Affairs and Communications, Ministry of Education, Culture, Sports, Science and Technology, Ministry of Economy, Trade and Industry, and Ministry of Defense)

Under the cooperation of the Council for Science and Technology Policy and the Information Security Policy Council taking into consideration the study results of "Study on the way of government participation for the R&D of information security technology" carried out in FY2009, consideration will be given to the design of the entire framework for promoting the "Grand Challenge" R&D and technology development, and the technical issues and systemic issues in realizing this in FY2010. In addition, consideration will be given to specific measures to be taken (not just showing the technical method, but including the creation of framework to obtain information required in analysis) to resolve these issues.

C) Study on Improvement of Investment Balance in R&D and Technology Development (Cabinet Secretariat, Cabinet Office, National Police Agency, Ministry of Internal

Affairs and Communications, Ministry of Education, Culture, Sports, Science and Technology, Ministry of Economy, Trade and Industry, and Ministry of Defense)

For R&D and technology development of information security, in order not to have under-investment and over-investment in the respective areas, under collaboration with the Council for Science and Technology Policy, the implementation situation of R&D and technology development related to information security in Japan through industry-government-academia will be examined and the public-private efforts situation and technical progress situation will be organized with February 2011 as the target.

D) Study on Improvement Policy in R&D Project Management and Evaluation (Cabinet Secretariat, Cabinet Office, and Ministry of Education, Culture, Sports, Science and Technology)

In order to overcome the non-efficient aspect caused by "moving target" which is a characteristic of information security R&D, besides continuing with the system review task so that the changes to research plan can be carried out flexibly in response to new changed conditions arising at the research stage, consideration is given, under collaboration with the Council for Science and Technology Policy, to effective policies with the purpose of stimulating innovation R&D and facilitating the use of R&D results.

E) R&D of Information Security Measures Technology in Large-Scale Virtual Server Environment (Ministry of Internal Affairs and Communications)

In order to maintain socioeconomic infrastructure using large-scale virtual server environment, growing with information security issues such as information leakage still remaining in safe and secure conditions, new information security measures technologies such as privacy protection processing technology and security level visualization technology are to be developed by end of FY2012. In the initial year (FY2010), besides carrying out basic design of each constituent technology and unit evaluation, consideration will be given to the interface between each constituent technology and the integrated testing model.

F) R&D on Information Security Technology that Contributes to Network Security and Reliability Assurance (Ministry of Internal Affairs and Communications)

In NICT, R&D related to technologies for ensuring overall information security for assuring the security and reliability of the network itself as well as the information flowing through the network will be implemented.

In FY2010, with regard to the technologies for broadening and speeding up incident analysis, the system rollout to collaborating organizations, building of test environment, and proof of concept will be implemented. In addition, the test environment for comprehensive user security support system will be built.

G) R&D Related to Sophistication of the Security Verification Technology for Infocom Components (Ministry of Internal Affairs and Communications)

In ensuring the security of information communication networks in FY2012, NICT will aim to establish an evaluation method to verify whether the communication protocols installed in network devices such as routers are secure, and carry out basic study on the evaluation method and basic design for the evaluation system in FY2010.

H) Building of Small-Scale Attack Reproduction Test Bed and Malware Isolation Analysis Test Bed (Ministry of Internal Affairs and Communications)

In NICT, by building the test bed for explaining cyber attacks, verifying countermeasures technology and generating data sets, the infrastructure for promoting advanced analysis capability and countermeasures technology for progressively sophisticated and ingenious cyber attacks and malware will be built.

In FY2010, after testing the α version of small-scale attack reproduction test bed built in the previous fiscal year, the β version prototype will be built taking into consideration the evaluation results. In addition, the journal data set recorded using the α version will be presented to scientific conferences.

I) Building of Security Evaluation System for IPv6 Environment (Ministry of Internal Affairs and Communications)

In NICT, specific security issues such as threats and vulnerabilities that accompany the migration to IPv6 will be extracted, and countermeasures considered after evaluating the significance.

In FY2010, using the IPv6 verification environment (test bed) developed the previous fiscal year, verification and evaluation tests will be carried out to grasp the security threats in the network.

J) R&D Related to New-Generation Network Infrastructure Technology (Ministry of Internal Affairs and Communications)

With a view of implementation around FY2020, R&D will be promoted for new-generation network infrastructure technologies capable of ensuring the most appropriate quality and security in response to user requirements by overcoming the IP network limits. In FY2010, the R&D on the constituent technologies for dynamic network will be moved forward, and the final evaluation for the results carried out and announced. Furthermore, technology evaluation of prototypes for virtual nodes that allow the provision of multiple networks on the same infrastructure will be carried out on the test bed.

K) R&D on Quantum Communication Network Technology (Ministry of Internal Affairs and Communications)

With the aim of realizing safe, secure and convenient information communication services, R&D will be carried out toward realizing quantum information communication networks provided with such security where the quantum cryptography is guaranteed to be very secure and undecryptable even with whatever future technology (unconditional security). In FY2010, R&D will be carried out on the optical detection technology and multiwavelength quantum technology required for the transmission of quantum keys, the multivalue technique of quantum noise concealed cryptography, etc.

L) Development and Dissemination of Software Structure Conditions Visualization Technology (Ministry of Education, Culture, Sports, Science and Technology)

In order to realize a safe and secure infocom society of the highest global standard by disseminating the software traceability concept as a way of enhancing the ability to deal with an "accident assumed society," the technology that adds a "software tag" to software products to allow management/verification by the software ordering party so as to determine whether the software development has been carried out in the proper steps through collection of verification data (empirical data) related to software developed by multiple vendors including those located offshore will be developed by end of FY2011.

In FY2010, taking into consideration the research result thus far, the following will be implemented to build an infrastructure for the dissemination of software tag.

[1] Addition/installation of software tag data, test production/improvement/function expansion of visualization tools, and release of the tools.

[2] Implementation of applicability testing of software tag.

[3] Revision of software tag standard, and implementation of activities so as to be adopted in international standards.

[4] Study on the applicability of software tags from the legal viewpoint.

M) R&D on New-Generation Information Security Technologies (Ministry of Economy, Trade and Industry)

In tandem with information technology becoming social infrastructures, R&D on new-generation information security technologies will be invited and implemented in FY2010 with the aim of solving basic issues rather than treating the symptoms in order to have a continual situation of not having accident arising in information systems bringing about stagnation of all economic activities or risks that affect the nation's life or property.

N) Preparation of Green and Secure Cloud Computing Environment (Ministry of Economy, Trade and Industry)

R&D will be carried out on technologies related to energy saving in cloud computing as well as reliability improvements that ensure secure and stable operations in the business settings of enterprises and government agencies where users can safely and securely use highly efficient and highly reliable information systems that can flexibly be scaled to fit the management or business strategy. In addition, consideration will be given for the preparation of audit framework environment.

In FY2010, development will be carried out on technologies for the improvement of the reliability, compatibility, energy efficiency, etc. of cloud computing. In addition, the audit framework and standards for cloud computing and security will be formulated and included in reports.

[2] Cultivation of Information Security Human Resources

To improve the information security knowledge standard of general users, cultivate human resources who can provide information security support services for general users.

Utilize general human assessment and education tools and practical training methods developed through university-industry collaboration to train information security experts. Also formulate a possible career path for such experts to present as a career model to gain public understanding and encourage people to follow it.

Create an information security expert training schedule plan across different industries, taking account of establishing the system to secure information security expert candidates over the medium to long term.

[Specific Measures]

A) Facilitation for Nurturing of Information Security Experts (Cabinet Secretariat, and Ministry of Economy, Trade and Industry)

a) Human resources (hereafter referred to as talents) with information security audit knowledge and capable of fairly and objectively evaluating information security measures from without and within the organization are to be nurtured.

b) IPA, in order to build a security evaluation system for systems using security LSI and deal with standards related to next-generation cryptographic module testing, will nurture talents for evaluating tamper resistance including side-channel attacks against security LSI.

B) Study on Information Security Talent Development Framework (Ministry of Economy, Trade and Industry)

a) In order to nurture advanced IT talents including information security talents, enhancements are to be made to the industry-academia partnership system for promoting the verification of educational programs targeting teaching staff produced by industry and the verification of practical internships using industry-academia benchmarking.

b) In order to nurture advanced IT talents including information security talents, model career development plan per job category capable of placing students and young engineers on a future career path will be publicized and disseminated. In addition, besides supporting the creation of career path for security talents in user businesses by newly formulating model career path development plan for information system talents in user businesses, publicity and dissemination will also be directed at CIO talents.

c) Based on a common career and skills framework, the skills standard of advanced IT engineers including information security talents are to be further raised and standardized.

d) In order to nurture security talents especially in Asia, with regard to the Information Technology Engineers Examination that is mutually recognized by 11 Asian countries and territories, ITPEC (IT Professionals Examinations Council), which is the council for implementing the exam with the cooperation of countries (Philippines, Vietnam, Thailand, Myanmar, Malaysia, and Mongolia) in which the examination system has been established by bringing in Japan's Information Technology Engineers Examination system, is implementing a unified examination for Asia, and besides expanding the ITPEC efforts, Japan's IT skills standards will also be disseminated.

C) Publicity for Information Security Qualifications (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

a) In order to enhance the nurturing of advanced IT talents including information security talents, further spread of the Information Technology Engineers Examination that measures the skills of talents in the various information fields including the information security field is to be devised.

b) From the viewpoint of making available information security experts to the private sector, the publicity for private sector qualifications relating to information security is to be devised.

D) Lead IT Specialist Development Promotion Program (Ministry of Education, Culture, Sports, Science and Technology)

a) The formation of base locations at graduate schools for developing and implementing advanced security talent development programs through industry-academia collaboration for the purpose of building an environment in which the nation can safely and securely use IT is to be supported.

b) With regard to the results obtained through the development and implementation of various education programs at each base location, besides striving for a more effective and efficient dissemination and rollout, support will be given for the task of further refining the teaching materials.

E) Holding Trainings and Seminars for Developing Countries (Ministry of Internal Affairs and Communications) [Repetition: Refer to 2(3)[1]]

F) Nurturing and Using Information Security Supporter (Ministry of Internal Affairs and Communications) [Repetition: Refer to 2(2)[2]]

G) Promotion for Formulation of Roadmap for Information Security Talent Development (Cabinet Secretariat)

What the nurturing and securement policy for information security talents ought to be will be considered from the medium-to-long term viewpoint and gathered into a roadmap with June 2011 as the target.

[3] Establishment of Information Security Governance

Raise information security awareness among business management so that information security governance may be included as one of the business management requirements through an awareness raising campaign. This aims to ensure that information security is taken into account when formulating BCPs or replacing business computing systems (such as accounting systems), and when conducting information security audits. Also, establish some measures to ensure information security is implemented in any newly introduced risk management methods within businesses.

[Specific Measures]

A) Promotion for Establishment of Information Security Governance (Ministry of Economy, Trade and Industry)

a) New information security governance in businesses is to be established while the burden of businesses in relation to corporate information security is reduced and overseas trends taken into consideration.

b) In FY2010, when the new information security governance in enterprises is introduced, policies for clearly positioning information security are to be considered and gathered into reports.

c) For the "Guidelines for Improving Reliability of Information Systems(Second Version)" revised with enhancements to IT governance and operational aspects in FY2008 and the "Evaluation Index concerning Improvement of the Reliability of Information Systems (First Version)" that visualizes the status of compliance with the guidelines, usage and dissemination are to be facilitated in private sector enterprises and government agencies.

d) In FY2010, actual project data evaluated based on evaluation index is to be collected and analyzed, and the tool to enable sharing of the analysis results released with FY2011 as the target.

B) Support for Information Security Measures in Enterprises (Ministry of Economy, Trade and Industry)

a) The "Survey on Actual Information Processing Situation 2010" will examine the usage status of information security audit system, information security management system compliance evaluation system and information security measures benchmark in enterprises, the checking status on the implementation of information security measures at transaction counterparties (including outsourcing and consignment), and the implementation status of ISO/IEC15408 certified products.

b) In order to reduce the burden of registrants and improve the convenience of users, consideration will be given to electronic filing of business audit ledger. In addition, the use of guaranteed audit will also be facilitated. In FY2010, what the business audit ledger ought to be like in order to reduce registrant burden and improve the user convenience will be determined by the survey committee related to improving the convenience of business audit ledger, and gathered into reports. In addition, the understanding on guaranteed audit will be deepened through the holding of seminars, and usage will be facilitated.

c) An appropriate information management and information leakage prevention policy will be facilitated in enterprises, and an information security report model will be disseminated to contribute to the protection of the rights and interest of the people taking custody of information. In FY2010, effort will be put into the dissemination of the information security report model by inquiring to individual enterprises.

C) Usage and Spread of "Information System, Model Transaction, Contract Document" (Ministry of Economy, Trade and Industry)

From the viewpoint of improving the reliability of information systems, the "Information System, Model Transaction and Contract Document (First Edition)" (published in 2007), "Information System, Model Transaction and Contract Document (Supplementary Edition)" (published in 2008), "Model Transaction and Contract Document Learned through e-Learning" (published in 2009) and "Collection of Problems in Information Systems and Software Transactions" (published in 2010) published by the Ministry of Economy, Trade and Industry for proceeding with the visualization of transactions between user and vendor and clarification of roles and responsibilities will be promoted through dissemination activities with cooperation of industry groups relevant to both user and vendor.

(5) Organization of Legal System concerning Information Security

[1] Identify Measures to Improve Cyberspace Safety and Reliability

Clarify any issues necessary for the early conclusion of the Convention on Cybercrime, push forward the legal framework, and reform the policing of computer virus activities. At the same time, actively discuss the legal/social system requirements to improve cyberspace safety and reliability, such as measures to clarify access rights to sensitive information and measures to prevent information leakage.

[Specific Measures]

A) Promotion of Legislative Readiness to Appropriately Respond to Cybercrimes (Ministry of Justice)

Since cybercrimes should be handled in an appropriate manner, legislative readiness to conclude the Convention on Cybercrimes is to be promoted. (The "Legislative Draft to Amend a Portion of the Penal Code to Deal with the Internationalized and Organized Crimes and the Sophistication of Information Processing" was submitted to the 163rd Diet session and deliberated. However, as the bill was scrapped with the dissolution of the House of Representatives in July 2009, consideration is to proceed with what sort of legislative readiness is required to conclude the treaty.)

B) Study on System for Improving Cyberspace Security and Reliability (Cabinet Secretariat)

The issues related to the system for improving cyberspace security and reliability such as the policy for clarifying access rights to sensitive information and the policy for preventing information leakages are to be considered.

C) Usage and Dissemination of the "Policies for Information Disclosure Concerning Safety and Reliability of Data Centers" (Ministry of Internal Affairs and Communications)

Taking into consideration the "Policies for Information Disclosure Concerning Safety and Reliability of Data Centers (First Version)" (formulated and published in February 2009), consideration is given toward the establishment of information disclosure approval system and its dissemination and usage are to be devised.

D) Usage and Dissemination of the "Certification System for Information Disclosure Concerning Safety and Reliability of ASP and SaaS" (Ministry of Internal Affairs and

Communications)

In order to simplify the comparison, evaluation and selection of services when using ASP/SaaS, the dissemination and usage of Certification System for Information Disclosure Concerning Safety and Reliability of ASP and SaaS operated by private sector organizations are to be devised based on the "Guidelines for information Disclosure Concerning Safety and Reliability of ASP and SaaS."

E) Clarification on the Lawfulness of Reverse Engineering of Software due to Security Assurance (Ministry of Education, Culture, Sports, Science and Technology) [Repetition: Refer to 2(1)[3] • Improvement and reinforcement of countermeasures against malware]

F) Spread and Facilitation for Use of Electronic Signature in Businesses (Ministry of Internal Affairs and Communications, Ministry of Justice, and Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)[3] • Promoting safe electronic trading]

[2] Comparison of Information Security Legal Systems of Different Countries

In the furtherance of international alliances and cooperation concerning information security, analyze the differences between the legal systems that cover information security in different countries and clarify the problems and means to align such differences.

[Specific Measures]

A) Examining Security Law System of Different Countries (Cabinet Secretariat)

By starting survey on the legal system of various Asian countries was received in FY2010, and proceeding to survey and analysis of the legal systems of major countries in FY2011, consideration will be given to the issues surrounding each country and the measure of cooperation.