Information Security 2011

July 8, 2011
Information Security Policy Council

Contents

I Preface

Japan has adopted a variety of information security measures with due consideration given to the viewpoints of the nation and users, based on“Information Security Strategy for Protecting the Nation” (May 11, 2010; hereafter, “ISS Strategy”) and its annual plan, “Information Security 2010” (July 22, 2010).

The surroundings of information security, however, have been changing considerably: the form of use of ICT has been changing rapidly, as indicated by the rapid spread of cloud computing,[1] social networking services (SNSs), and smartphones; the threat of new attacks represented by Stuxnet and cyber attacks against Japan’s government agencies, such as the one that occurred in September 2010, has become more complicated and sophisticated; and information leaks have occurred in government agencies. In addition, facing the national crisis caused by the Great East Japan Earthquake in March 2011, Japan has been demanding an appropriate review of the social framework including information communication systems.

On the basis of these changes in the environment, this document, “Information Security 2011,” sets forth the details of the specific efforts to be implemented in FY2011 and FY2012, so that appropriate measures can be taken.

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

[1] A new use of computer network where data services and Internet technology are located on a cluster of servers (cloud) on a network, enabling 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 to date.

II Changes in the Environment Surrounding Information Security

In the ISS Strategy, environmental changes in the background are categorized into four groups.

Those groups are (1) Increasing threats of large-scale cyber-attacks and so on; (2) Increasing dependency on ICT in socioeconomic activities; (3) Adapting to new technological innovations; and (4) Globalization etc. After the ISS Strategy was formulated in May 2010, various changes have occurred in these surroundings, and the information security strategy should adapt to those changes.

Especially, the Great East Japan Earthquake, which occurred in March 2011, was an unprecedented and complex disaster consisting of a large-scale earthquake, a giant tidal wave, a nuclear power plant accident, and so on. Immediate steps based on the Great Earthquake are now demanded in the information security field.

With the Great East Japan Earthquake and the above four environmental changes, their characteristic trends andphenomena to consider are summarized below.

<1> Increasing threats of large-scalecyber-attacks and so on (sophisticated and diversified threats against information security)

> Cyber attack cases, including distributed denial-of-service attacks (DDoS attacks) from a number of sources, made on government agencies, the private sector, etc., have been increasing. In Japan, a cyber attack was made on government agencies, etc. in September 2010. Cyber-attack methods such as expansion of botnets, sophistication of targeted e-mail attacks, which send e-mails to specific organizations or persons to conduct a phishing scam, transmit a virus, etc., are growing more clever and complex.

In recent years, computer viruses have been widespread worldwide, and the techniques such as the so-called “Gumblar-type attack” have become more sophisticated and complex year by year. As seen in a case in which a plant control system was attacked by Stuxnet from 2009 to 2010, a new threat called APT (Advanced Persistent Threat),[2] which ingeniously combines existing attack methods and enables a tailored

[2] An adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors. These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of stealing information, undermining or impeding critical aspects of a

attack to be executed, has appeared.

Large-scale ICT system failures and large-scale personal information leakages in the private sector have not been eliminated and increase in size. In FY2010, undisclosed internal information of an administrative agency was leaked, and the case developed into a big social problem.

The smartphone, cloud computing, IPv6, SNS, etc. are rapidly spreading, but they are said to have a variety of problems of information security.

As described above, threats in information security have been sophisticated and diversified, and threats of large-scale cyber attacks, etc. have been realized. It is strongly desired to improve or overcome these circumstances.

<2> Increasing dependency on ICT in socioeconomic activities

As the importance of information in socioeconomic activities and the nation's life, and as Japan's socioeconomic activities becomes more dependent on ICT, information security is one of the infrastructures that are expected to play an important role.

Increasing dependency on ICT is indicated by the following: the number of Internet users in Japan reached 94.08 million[3] at the end of 2009; the proportion of people that have ever bought something or have undertaken a financial transaction through the Internet reached 53.3%.

SNSs, smartphones, and the like are changing and innovating people's communications. Since they appeared several years ago, SNSs have attracted tens of millions of people in Japan. Smartphones are rapidly spreading. The Great East Japan Earthquake caused people to re-assess the importance of information transmission, information sharing, etc. at the time of disaster.

While information and telecommunications systems are being inseparably incorporated into the framework forming the basis of socioeconomic activities, there is a strong demand to ensure information security so that safe and secure use of those systems becomes possible.

<3> Adapting to new technological innovation

Active use of cloud computing by virtualization of computer resources,

mission; or positioning itself to carry out these objectives in the future (NIST SP800-39 "Managing Information Security Risk: Organization, Mission, and Information System View" [Appendix B GLOSSARY]).

[3] Ministry of Internal Affairs and Communications, "FY2010 Information and Communications Status Report" (July 2010).

ubiquitous terminals, use of sophisticated embedded software in intelligent home appliances, and the like have been proceeding remarkably in recent years. A variety of sensors will be placed in homes and offices in the future, and moves toward enhanced real-time sensing[4] and Context Awareness[5] utilizing positional and user information will probably accelerate.

Since there is a possibility that ubiquitous techniques, techniques that merge real and virtual worlds, and the like will grow rapidly, appropriate adaption to the information security technologies, social systems, and so on that support those techniques is demanded strongly.

<4> Globalization etc.

The so-called Jasmine Revolution triggered a wave of movements in North African countries from the end of 2010. This event has indicated again that the free cross-border distribution of information enabled by ICT could shake the framework of society. Also, the activities of WikiLeaks have presented a variety of questions, though the point of view is completely different.

The idea of cross-border distribution of information via the Internet has long been discussed, and its actual impacts on politics, societies, and the economy should be studied further.

<5> Great East Japan Earthquake

The Great East Japan Earthquake was an unprecedented and complex disaster. The large-scale earthquake, giant tidal wave, accidents at the nuclear power plant, etc. have seriously damaged the society and economy of not just East Japan alone but the whole of Japan. The existing info-communication infrastructure suffered devastating damage, and the interruption of communications delayed rescue and recovery operations and caused concern.

The interrupted distribution of information, which is the foundation of socioeconomic activities, has delayed a variety of activities. It was also reported that SNSs and other new uses of ICT were useful to share disaster information.

On the basis of the experience of the Earthquake, disaster-resistant information and telecommunications systems should be studied and re-constructed in terms of

[4] Function to measure and monitor a variety of statuses by a sensor in real time. Data obtained by home smart meters, personal heartbeat sensors, etc. are fed together through a wireless network or the like and analyzed in real time, for example.

[5] Idea that computers automatically recognize changing circumstances via sensors and networks and respond to such changes.

backup systems, reinforced emergency power sources, efficient use of cloud computing, and so forth. A drastic review of Business Continuity Plan (BCP) and the establishment of Risk Communication[6] and Risk Management[7] methods should be considered urgently.

[6] Process in which parties directly or indirectly concerned with information and telecommunications systems exchange opinions on a risk and reach an agreement

[7] A series of processes based on the PDCA cycle, to clarify a risk, evaluate the risk in terms of risk exposure, frequency of occurrence, etc., take action, and minimize damage caused by such risk

III Basic Lines

This document is formulated upon the following points based on changes in today's circumstances, in addition to the basic ideas described in "Information Security Strategy for Protecting the Nation."

<1> Basic idea of Cyberspace[8]

ICT is the foundation of socioeconomic activities, and dependency on ICT has been increasing. Use of the Internet in various forms can improve the quality of life in society and can stimulate economic activities. A global, open network is a key to promote innovation for developing the economy and improving people's lives.

The widespread use of broadband Internet connections, smartphones and cloud computing, together with the development of new technologies in recent years, have greatly increased the flow of information distributed domestically and internationally and have become basic factors in the growth of Japan's economy and further activation of the global economy. At the same time, problems concerned with the Internet, such as information security, protection of the secrecy of communications, protection of personal information, and countermeasures against violation of intellectual property rights have been revealed.

Each country has been working on national security and other problems concerned with so-called "cyberspace." It is now important to confirm the basic ideas in terms of information security.

- Building an open, interoperable, secure, and reliable cyberspace

It is important for Japan to secure a safe and reliable cyberspace, maintaining the openness and interoperability of the Internet.

A balanced approach to problems such as information security, protection of secrecy of communications, protection of personal information, and countermeasures against violation of intellectual property rights should be taken without interrupting free and cross-border distribution of information.

Thus, an open, interoperable, secure and reliable cyberspace should be built. This cannot be achieved by the efforts of a single country and should be achieved through international cooperation while making global consensuses.

The United States of America released their "International Strategy for

[8] Internet and other virtual space where information is exchanged by using ICT

Cyberspace" in May 2011 and announced their ideas about those problems. In the G8's Deauville Declaration of May 2011, key principles about the Internet were agreed.

<2> Active response to sophisticated and diversified threats against information security

As described in II, threats concerned with information security such as a large-scale cyber attack case, a new threat called APT, a large-scale system failure and the massive leakage of personal information have grown increasingly sophisticated and complex. Quick and appropriate responses to such changes are very important.

> The offensive side has an advantage over the defensive side in cyberspace. Not only has this condition not been improved, but also the advantages for the offensive side have been rising. This situation should be tackled and overcome. While the fusion of real space and cyberspace is developing, it is very important to reinforce the active approach to achieve a Game Change[9] that resolves such imbalances and to secure the strong reliability of the entire information system, or so-called New Dependability.[10]

Needless to say, an approach to each individual problem is important. However, special efforts should be made to foster public-private sector alliances and international alliances while recognizing the position of individual problems within the entire frame where shared problems that require tackling jointly have been increasing.[11]

In other words, a variety of data, contents, expertise, and the like are likely to be integrated into a network through cloud computing etc. This trend is greatly accelerating, and from that point of view, the problems to be tackled in an alliance are increasing. Since an increasing number of links are added to resources on the cyberspace and real space, more entities need to cooperate to resolve such issues.

Since threats are becoming sophisticated and diverse, Japan should assess information security accidents that have already occurred and should share reflections and lessons in order to improve Japan's information security countermeasures.

The following points require immediate emphasis.

[9] Game in Game Change is close to game theory in economics. In the information security field, changing the continued advantage of the offensive side over the defensive side by innovative approaches such as increasing the economic burden on the attacker could lead to a final solution to problems in information security.

[10] Active and dependable information security. Active information security factors, such as disabling a cyber attack, have been added to the former dependability. For details, refer to the Principles "Information Security Research and Development Strategy" (settled by the Information Security Policy Council in July 2011).

[11] In cyberspace, many factors are organically united through networks and can have a mutual influence on one another. Among problems in information security, those factors that can have a mutual influence on one another should be kept in accord when they are tackled.

- Enhancement and reinforcement of an inter-divisional Government Security Operation Coordination team (GSOC)[12]

To improve the government's response capabilities against the actualizing threats of large-scale cyber attacks cases, increasing targeted e-mail attacks, and so on, GSOC, which commenced full-scale operations in FY2008 and performs 24-hour monitoring of government's information systems must be enhanced and reinforced. The entire government should improve its emergency response capabilities against cyber attacks, especially by reinforcing capabilities of collecting information through an emergency reporting process and close coordination with the relevant parties, and by improving the ability of attack analysis.

- Immediate response to problems with smartphones concerning information security

As viruses against smartphones have now been generated, information security problems regarding the rapidly spreading smartphones have been revealed. Users are requested to recognize that the basic configuration of the smartphone is the same as that of the personal computer. Public-private sector alliances should quickly provide the environment and foundation whereby smartphones can be used safely under their functional restrictions, which differ from those of the personal computer.

- Response to problems such as Stuxnet and so on for information security on control systems

Stuxnet attacked particular control systems of a critical infrastructure previously considered invulnerable because they are isolated with dedicated lines. In that context, immediate actions to protect control systems, such as SCADA[13] in critical infrastructure entities are required.

New threats, such as APT, against specific organizations or corporations have been appearing. If a control system is compromised or captured by a third party, a physical danger could immediately occur. Actions from this point of view are essential.

- Response to problems in information security concerned with cloud computing, IPv6, SNS, etc.

After the Great East Japan Earthquake, understanding of the effectiveness of

[12] Abbreviation of the Government Security Operation Coordination team

[13] Abbreviation of Supervisory Control and Data Acquisition, a type of control system used in industry. Such control systems usually include a supervisory control system, remote supervisory control equipment, a communications infrastructure, and a user interface.

cloud computing has deepened. Since various movements, such as adoption of IPv6 due to IPv4 address depletion and extended use of SNSs, are accelerating, related problems in information security have been pointed out. Measures for ensuring information security in those circumstances should be studied immediately.

<3> Measures in information security based on the Great East Japan Earthquake

A variety of measures in information security are being adopted with emphasis placed on confidentiality, integrity and availability. In the event of a large-scale disaster, it would be especially important to ensure availability (so that information or a service can be used when necessary).

Therefore, it is indispensable to study and rebuild a disaster-resistant information and telecommunications system and to review Business Continuity Plans (BCP), including remote information backup and distribution. Since security in cyberspace and physical security[14] are two sides of the same coin, BCPs should be reviewed from the assumption that a complex large-scale disaster will happen.

- Establishment of Risk Management and Risk Communication

In the event of a large-scale disaster, changing conditions changes the way people view risks. (For example, in peacetime, it is wrong to disclose personal privacy; at the time of disaster, the confirmation of people’s safety is given priority.) At the time of disaster, it is important to have the idea of dynamic risk management for adapting optimally to changing conditions. Since one risk can create new risks, all risks must be assessed until an optimum solution is obtained (risk management).

It is also important to establish a risk communication system, in which the parties concerned have the same accurate information of risks in society, understand one another and reach an agreement on practical risk management through a mixture of diverse values.

Now that the importance of risk communication and risk management has been recognized again, but knowledge in the field is not necessarily sufficient, immediate action should be taken.

- New dependability of the entire information system

In light of the Great East Japan Earthquake, the following issues in information

[14] “Physical and Environmental Security” in ISO/IEC 27001:2005. Examples are management of entry to and exit from a specific area in a site of information processing facilities, and protection against natural disasters or man-made disasters.

security should be tackled immediately: <1> Study and reconstruction of disaster-resistant information communications infrastructures; <2> ideal condition of information and telecommunications systems at the time of disaster; <3> Backup and distribution of information and telecommunications systems; <4> Establishment of risk communication and risk management; <5> New dependability of the entire information system.

These issues should be tackled with the idea of establishing a new information security policy contributing for future-oriented and creative efforts.

IV　Specific Measures

Taking into consideration the environmental changes and basic lines described in II and III, the specific measures presented below are to be steadily implemented. The measures with no specific indication of implementation period are to be implemented in FY2011.

１ Preparation for a Potential Large-Scale Cyber Attack

(1) Organizing Counteractive Arrangements

Taking into consideration the actual threat of a large-scale cyber attack case, counteractive arrangements are enriched by conducting regular trainings with an emphasis placed on cooperation and other arrangements with respective government agencies in the event of a large-scale cyber attack.

As security-related efforts, on the basis of “National Defense Program Guidelines for FY2011 and Beyond,” counteraction and response capabilities against cyber attacks are reinforced for the stable use of cyberspace.

A) Preparation of the government’s initial response to a large-scale cyber attack

(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 an 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. The training is to be conducted continually in the next fiscal year and beyond.

(b) Organization of arrangements for information analysis (Cabinet Secretariat)

Arrangements for information analysis in the event of a large-scale cyber attack case or the like are organized and enriched.

(c) Promotion of analysis of threats and methods concerning cyber attacks (Cabinet

Secretariat and concerned government agencies)

Through promotion of analysis of threats and methods concerning cyber attacks, appropriate counteraction capabilities in the event of a case should be developed.

(d) Enhancement to Systems Related to Cyberterrorism Countermeasures (National Police Agency)

In order to deal with sophisticated cyber-attack methods as a means of cyberterrorism,[15] reinforcement of the police force’s counter-cyberterrorism system is to be stepped up, such as by enhancing the information collection and analysis systems, 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.

B) Alliance between public and private sectors

(a) Enhancement of Public-Private Cooperation in Counter-Cyberterrorism for Critical Infrastructures (National Police Agency)

Besides holding enlightenment activities linked to raising 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) Enhancement to Public-Private Cooperation in Cyber-Intelligence Countermeasures[16] (National Police Agency)

Information sharing systems with corporations at a risk of becoming a target of a cyber attack is reinforced, and efforts are to be made to contribute to cyber-intelligence countermeasures.

(c) Cyberterrorism (Incident) Response Coordination and Support (Ministry of

[15] 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 highly likely to have been caused by an electronic attack.

[16] Countermeasures against espionage activities in cyberspace (cyber-intelligence).

Economy, Trade and Industry)

In response to requests from critical infrastructure providers, support will be provided to deal with information security incidents, such as coordination of actions 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.[17]

(d) New threat and attack analysis (Ministry of Economy, Trade and Industry)

The threat and measure study meetings that analyze new threats and attacks in information security established in the Information-Technology Promotion Agency (IPA) will provide analyzed results and other necessary information quickly to the users.

C) Reinforcement of protection against cyber attacks

(a) Preparation for organizing a new special cyber protection unit (Ministry of Defense)

Secure human resources for starting up a new special cyber protection unit that will become the core of integrated counteractive arrangements against cyber attacks on the Ministry of Defense or the Self-Defense Forces.

(b) Commencement of operation of cyber protection analysis equipment (Ministry of Defense)

Operation of new cyber protection analysis equipment starts, and support to cyber attack countermeasures training for Self-Defense Forces security personnel is given, and research on cyber attack countermeasures is conducted.

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

Network security analysis equipment prototyped to improve the analysis and response capabilities concerning threats and effects of cyber attacks against information systems maintained by the Ministry of Defense will be subjected to a performance confirmation test. Research for sensing cyber attacks and behavior analysis study on malware will be conducted.

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

[17] Abbreviation of Computer Security Incident Response Team.

Continuing from FY2010, besides continuously investigating the latest technological trend related to cyber attacks and cyber-attack countermeasures, an effective response will also be investigated and studied in order to ensure the security of information systems.

(e) Human Resource Development for Cyber-Attack Countermeasures (Ministry of Defense)

In the National Defense Academy, a network security education/study system is to be organized.

D) Policing cybercrimes

(a) Promotion of Efforts in Digital Forensics[18] (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, buildup of resources and equipment, cooperation with relevant institutions and the private sector through participation in relevant meetings and technical collaboration, and the enhancement to the systems related to digital forensics is to be promoted.

(b) Promotion of International Cooperation for Policing Cybercrime (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.

E) Reinforcement of international alliances against cyber attacks

(a) Establishment and reinforcement of a system for sharing information on cyber attacks with overseas countries (Cabinet Secretariat and concerned government

[18] General term for the equipment and data needed to investigate the causes, collect and analyze electronic records, and the means and technologies to clarify legal evidence following the occurrence of computer-related crimes, such as unauthorized access and confidential information leakage, or legal disputes.

agencies)

Cooperative relationships, such as an information sharing system, with overseas countries about countermeasures against cyber attacks are to be established and reinforced.

(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 FY2011 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 measures against cyberterrorism, information collection and analysis related to attack subject and method, etc., will be continuously implemented, including reinforcement of international cooperation through information exchange with relevant overseas institutions.

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

Reinforce the communication systems to collect, analyze, and share information concerning responses to cyber attacks between the Cabinet Secretariat and the concerned government agencies. Establish and reinforce information sharing systems that contribute to cyber-attack countermeasures, with relevant overseas institutions.

A) Reinforcement of the communication systems to collect, analyze, and share information concerning responses against cyber attacks

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

Further enhancement is to be made so that information that contributes to countering cyber attacks is centralized at the Cabinet Secretariat and the information is timely and appropriately shared with the respective government agencies.

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

Continuing from FY2010, GSOC, 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 System Based on the “Second Action Plan in 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 in Information Security Measures for Critical Infrastructures” (hereafter, “Second Action Plan”).

(d) Early Identification of Cyberterrorism Signs and Enhancement of Information Collection and Analysis (National Police Agency and Ministry of Justice)

In order to enhance the measures against cyberterrorism, early identification 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)A)]

B) Establishment and reinforcement of a system for sharing information on cyber attacks with overseas countries

(a) Improvement of response capabilities by sharing information concerning cyber attacks with relevant overseas institutions (Cabinet Secretariat and concerned agencies)

Through exchanges of views with relevant overseas institutions, the sharing of information related to countermeasures in response to attack subject and method of cyber attacks is to be advanced, and Japan’s response capability is to be improved.

(b) Enhancement to Cooperation with Relevant International Institutions against Cyberterrorism (National Police Agency and Ministry of Justice) [Repetition: Refer to 1(1)E)]

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 Infrastructures

As one information security measure within government agencies, reinforce the cross-sectional Government Security Operation Coordination team (GSOC), which started full-scale operations in FY2008 aiming to improve the government’s response capabilities against the actual threat of large-scale cyber attack cases and increasing targeted e-mail attacks, and has been conducting 24-hour monitoring of government agency information systems.

As a framework for making active improvements mainly by the Chief Information Security Officers (CISOs) of concerned government agencies, the “Annual Report on Information Security” (hereafter, “Information Security Report”) is to be created from this fiscal year. In a series of PDCA cycles, including the Information Security Report, information security measures are to be improved by further strengthening the efficiency of processes concerning self-assessments and priority inspections. By keeping staff informed about the “Standards for Information Security Measures for Central Government”[19] (hereafter, “Standards for Measures”) and by improving education through conducting training concerning targeted e-mail attacks, for example, the information security awareness of each staff member can be improved.

To ensure a fast response to changes in the environment surrounding government agencies, the effects of the Great East Japan Earthquake on information systems are to be analyzed and evaluated, and the Guidelines for Operation Continuity Planning of Central Government Computer Systems (formulated in March 2011) are to be improved. As security against possible sudden deterioration in the security of the

[19] The Standards for Information Security Measures for Central Government include Models for Information Security Measures for Central Government Computer Systems, Guidelines for Formulation and Implementation of Management Standards and Technical Standards for Information Security Measures for Central Government Computer Systems, Management Standards for Information Security Measures for Central Government Computer Systems, and Technical Standards for Information Security Measures for Central Government Computer Systems.

cryptographic algorithm used in the information systems of government agencies, requirements for invoking emergency measures (contingency plans) are to be determined, and any other necessary approaches are to be conducted.

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

(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, will enhance the information collection capability and analytical capabilities related to cyber attacks by stepping up cooperation with relevant collaborative institutions, and in addition, promote information sharing, such as of analysis results, and strive to improve the emergency response capability of the entire government.

b) In 2011, the emergency contact system will be checked through training, and its effectiveness will be verified.

B) Enhancement of the function of Chief Information Security Officers (CISOs)

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

a) The Cabinet Secretariat is to hold regular Information Security Measures Promotion Conferences (Liaison Conference for the Chief Information Security Advisers; hereafter, "CISO Liaison Conference") comprising the chief secretaries of concerned government agencies and to upgrade the system that enables concerned government agencies to autonomously strive to unify their information security measures with responsibility under the Chief Information Security Officer.

b) The Chief Information Security Advisers Liaison Conference is to be held under the CISO Liaison Conference, as needed, 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) The Chief Information Officers of the concerned government agencies are to create Information Security Reports starting from FY2011, while making continued use of the knowledge available inside and outside the ministries and experience in the creation of the guidelines of the FY2010 Information Security Report. In this case, from the viewpoint of ensuring the objectivity and specialization of the Information Security Report, the use of an external audit system is to be promoted, as far as possible.

b) These Information Security Reports are to be compared and evaluated at the Chief Information Security Advisers Liaison Conference, the knowledge thus obtained is to be shared and fed back, and reports made public by the Chief Information Security Officers at the CISO Liaison Conference.

c) The Cabinet Secretariat, based on the Standards for Measures,[20] will evaluate in an objective manner, the implementation situation of the measures by concerned government agencies on the basis of the report on the implementation of measures and the priority inspections; coordinate the improvement of concerned government agencies' measures with that of the improvement to the Standards for Measures, through recommendations; and ensure the usage and spread of PDCA cycle across the entire government. For this reason, the means for improving the efficiency of self-assessment tasks and priority inspections (such as by improving survey items and methods) are to be investigated and presented to the relevant government agencies.

d) The Cabinet Secretariat evaluates the implementation situation of the information security measures of concerned government agencies and all government agencies in accordance with the evaluation method given above and organizes the results as an "Annual Report on Information Security in Government Agencies." Although the handling of the annual report has been stipulated in the report to the Information Security Policy Council expert committee according to the Information Security Report (September 11, 2009), the report of FY2011 and after will be released quickly after it is finalized by the CISO Liaison Conference. It will also be reported to the Information Security Policy Council as a means of promoting effective countermeasures by the whole government and of fulfilling accountability to the nation with regards to information security.

(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 FY2011, efforts are to be enhanced to ensure the security of information systems in government agencies by cooperating with the Chief Information Security

[20] Decided on by the Information Security Policy Council on April 21, 2011.

Advisers Liaison Conference and CIO Assistants Liaison Conference.

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

(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 the Information Security Policy Council of May 11, 2010), each of the concerned government agencies will further promote the streamlining of information systems and improving operational efficiency, as well as strive to improve information security measures and their efficiency by steadily implementing the centralization of maintained public web servers and mail servers by the end of FY2013.

b) The Cabinet Secretariat will continuously manage efforts 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 vulnerability checks for the main public web servers of the requesting government agencies in 2011 for the second straight year after 2010, and provide feedback on the results to government agencies. The obtained information will be shared among all government agencies, and the results will be made public and will be reflected appropriately in the items of the priority inspection in the next year, so that the level of countermeasures adopted by all the government agencies will be raised.

(C) Implementation of education and training concerning targeted e-mail attacks (Cabinet Secretariat and concerned government agencies)

The Cabinet Secretariat, in cooperation with concerned government agencies, will provide education and training concerning targeted e-mail attacks to requesting agencies in 2011, and provide feedback on the results. The obtained information will be shared among all government agencies, and the results will be made public. Education concerning information security will be improved and evaluated in comparison with the reports on the implementation of measures.

(D) Reinforcement of business continuity capabilities in government agencies (Cabinet Secretariat and all government agencies)

a) Concerned government agencies will formulate an operational continuity plan for necessary information systems by the end of FY2011 in order to ensure the continuity of administration in the event of an emergency, on the basis of the business continuity plan, utilizing the Guidelines for Operation Continuity Planning of Central Government Computer Systems formulated by the Cabinet Secretariat.

b) The Cabinet Secretariat will analyze and evaluate the effects of the Great East Japan Earthquake on information systems, in preparation for the formulation and improvement of the operation continuity plan for the information systems of concerned government agencies, and will appropriately provide information to these agencies and improve existing guidelines.

c) The Cabinet Secretariat will study the evaluation method for the information system operation continuity plan formulated by the concerned government agencies for appropriate management and so that countermeasures can be maintained to a certain level and can be continuously improved.

(E) Examination of appropriate physical security measures in government agencies (Cabinet Secretariat)

The Cabinet Secretariat will study advanced models in the private sector to make it possible to respond to environmental changes, such as the Great East Japan Earthquake, which can seriously damage physical security, and will pursue appropriate physical security measures in concerned government agencies. Then, the Cabinet Secretariat will formulate guidelines based on the current status of government agencies.

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

a) Concerned government agencies responsible for online procedures covered by the Guidelines on Risk Assessment and Digital Signature/Authentication (decision at the liaison conference of Chief Information Officers (CIOs) at government agencies on August 31, 2010) will ensure the overall effectiveness of the risk evaluation and assurance levels drawn up based on the guidelines, taking advice from persons with expertise at a liaison conference for chief information security advisors and the

CISCO Liaison Conference, and will report to the CIO liaison conference the status of implementation of the plan, for items concerning optimization of business and systems.

b) The Cabinet Secretariat will study the effectiveness of trail management, which was included as an item to note in the Guidelines on Risk Assessment and Digital Signature/Authentication, with reference to precedents, will also study the appropriate trail management in government agencies.

(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 concerning information security measures, will provide information related to the respective types of information security measures, including technical information, set up a regular investigation-and-sharing event for joint responses with concerned government agencies, and make concerted efforts to resolve any 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 of measures, taking into consideration the criteria related to specially-controlled secrets based on the “Counterintelligence Policy.”

(I) Promotion of efforts to reinforce intelligence and security systems of government agencies handling highly-confidential information (Cabinet Secretariat and concerned government agencies)

An examination commission on intelligence and security in government agencies, chaired by the Chief Cabinet Secretary, was established in December 2010. The commission has started examining security law, especially measures that are considered necessary for intelligence and security systems of government agencies handling highly-confidential information. On the basis of the commission’s conclusions, necessary efforts will be made.

(J) Promotion of Education and Awareness-Raising for Government Employees (Cabinet Secretariat, National Personnel Authority, Ministry of Internal Affairs and

Communications, 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 training 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, and is also to prepare educational materials that summarize the minimum requirements expected of government employees. Concerned government agencies are then to provide information security education.

d) The concerned government agencies are to raise awareness of recent incidents and cases related to information security by taking advantage of "e-Government Promotion Week" and the "Information Security Awareness Month," etc.

(K) Prevention of Spoofing of E-Mail 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 sender domain authentication technology, such as SPF[21] (Sender Policy Framework) to rule out malicious third parties from impersonating government agencies or their staff and harming the general public or the private sector. In addition, since e-mail may be sent to government agencies from senders impersonating government agencies or their staff, the adoption of the sender domain authentication technology should be facilitated on the receiving side.

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.

[21] Abbreviation of Sender Policy Framework. A technology for performing e-mail sender domain authentication, which enables the impersonation of the sender domain of the e-mail address of the mail sender to be detected.

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

a) Continuing into FY2011, for the domain names used when government agencies send information to the nation, the Cabinet Secretariat and Ministry of Internal Affairs and Communications encourages government agencies to use domain names guaranteed to be government agencies, in principle, (".go.jp" domain names among the generic JP domain names), and the status of the efforts will also be announced to the nation.

b) Concerned government agencies will promote the use of domain names guaranteed to be the domain names of government agencies.

D) Promotion of secure encryption usage in government agencies

(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 FY2011 to ensure the safety and reliability of 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 Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry will provide information obtained by monitoring the e-Government Recommended Ciphers to the Cabinet Secretariat when necessary, and the Cabinet Secretariat will provide necessary information quickly to the concerned government agencies. Efforts will be undertaken in accordance with the "Migration Plan of Cryptographic Algorithm SHA-1 and RSA1024 in Information Systems of Government Agencies."[22]

d) With reference to discussions made at the Cryptography Research and Evaluation Committees, the Cabinet Secretariat and concerned government agencies will study the requirements for invoking an emergency measure (contingency plan) in case of

[22] Decision at the Information Security Policy Council on April 22, 2008.

sudden deterioration of security and will decide on the requirements at the CISCO Liaison Conference.

e) Concerned government agencies will continue steadily migrating their own information systems to safer cryptographic algorithms in FY2011, in accordance with the Migration Plan.

f) The Cabinet Secretariat is to grasp the state of conformity to the Migration Plan and urges each information system to meet the requirements stipulated in the Migration Plan by the time the algorithm is switched 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 at the time of procuring a cryptographic module.

E) Ensuring information security in cloud computing

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

The Ministry of Internal Affairs and Communications is to start designing and building a “common government platform” utilizing cloud computing technology and supporting IPv6, giving consideration to 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.

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

(A) Examination of a plan for appropriate and smooth implementation of the Standards for Information Security Measures for Central Government Computer Systems (Cabinet Secretariat)

Concerned government agencies are required to implement appropriate security measures, even when an environmental situation that could seriously damage their information systems, such as the Great East Japan Earthquake, occurs. Accordingly, which risk management method should be adopted in government agencies will be studied in order to ensure appropriate and smooth implementation of the new framework of the Standards for Measures and to clarify the range of information resources held by the concerned government agencies and their handling methods and then will be formulated as guidelines. By sharing the results among the concerned government agencies, shared risk communications among the concerned government agencies will be developed.

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

In consideration of changes in technology and the environment, the Standards for Measures are to be reviewed. Particularly in FY2011, a review of the business continuity plan, physical security measures, and IPv4 rules to be observed will be carried out by taking account of new threats to information systems, revealed by the Great East Japan Earthquake, and new technological trends such as IPv6, and a revision will be prepared.

(C) 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 involved in information security on the basis of a memorandum on cooperation with 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), to enhance cooperation with the incorporated administrative agencies related to information security measures, and to reflect that to the Standards for Measures policy.

(D) Promoting the Use of Secure and Reliable IT Products (Cabinet Secretariat, Ministry of Economy, Trade and Industry, and all government agencies)

a) When procuring IT products, concerned government agencies will use products certified through the “IT Security Evaluation and Certification Scheme”[23] in order to build secure and reliable information systems, with reference to “List of Products in Evaluation based on the IT Security Evaluation and Certification Scheme” (Ministry of Economy, Trade and Industry, on April 21, 2011), on the basis of the

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

Standards for Measures.

b) The Ministry of Economy, Trade and Industry will continue to consider promoting the use of products certified by the IPA-run IT Security Evaluation and Certification Scheme, so that concerned government agencies can effectively and efficiently procure IT systems with consideration given to information security, and will facilitate their use in government agencies such as through reviewing the List.

(E) 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 provide an opportunity for an exchange of views with concerned government agencies in charge of the legal system, including the relevant departments within the Cabinet Secretariat, so as to ensure consistency between the legal system related to information security and the Standards for Measures, in order to develop closer ties among them.

(F) Promotion of secure encryption usage 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>D)]

(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>D)]

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

(A) 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 and corresponding manuals and by utilizing cloud computing.

(B) 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)

a) The concerned government agencies are to assume in advance as far as possible that the required security measures can be assured within the system budget as a whole, and, in the preparation of procurement specifications, use the “Security Requirement Formulation Manual in Government Procurement for Information Systems” to include all the necessary security measures.

b) The Cabinet Secretariat strives to bring the Security Requirement Formulation Manual in Government Procurement for Information Systems into wide use in the government procurement for information systems by actively promoting use of the manual. How the manual is used with actual procurement specifications will be assessed, and response to user’s inquiries about actual use and assistance in operations will be provided.

c) Concerned government agencies will take measures equivalent to or beyond the use of the “Security Requirement Formulation Manual in Government Procurement for Information Systems” and will verify and report the results to the Cabinet Secretariat.

(C) Promoting the Use of a Secure and Reliable Cryptographic Module (Cabinet Secretariat and Ministry of Economy, Trade and Industry, and all government agencies) [Repetition: Refer to 2(1)<1>D)]

(D) Usage and Dissemination of the “Guidelines for Improving the Reliability of Information Systems” (Ministry of Economy, Trade and Industry)

In order to improve the reliability of all 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),” which allows visualization of the status of compliance with the guidelines, together with the “Reliability Self-Diagnosis Tool” based on the evaluation index, are to be facilitated in the private sector and within government agencies.

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

a) Besides promoting the operations of the “IT Security Assessment and Certification

Scheme," usage expansion of the scheme to include information system procurement is to be planned.

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

c) For the security functions of products subjected to the "IT Security Assessment and Certification Scheme," provision of a protection profile for each product is to be considered.

(F) Promoting the Use of Secure and Reliable IT Products (Cabinet Secretariat, Ministry of Economy, Trade and Industry, and all government agencies)
[Repetition: Refer to 2(1)<1>F)]

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

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

Continuing into FY 2011 as well, for the numbering system and national ID system related to social insurance and taxation being considered by the government across sectors, study for realizing the systems is conducted, with consideration given to enable appropriate personal information protection and information security measures and ensure security and convenience to the nation.

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

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

a) BCP formulation seminars are to be held and advisors are to be introduced to help local government employees understand the importance of business continuity and master the basics and necessity of BCP formulation in the ICT departments of local governments. Information security audit seminars are to be held to promote information security auditing.

b) The operation of a portal site in the Local Government Wide Area Network (LGWAN) is to be supported by collecting sample information security measures, collecting and analyzing information security accident information, and giving a commentary in information security, in order to promote usage.

c) If it desires, a local government will be given support to strengthen their security measures, which includes vulnerability diagnosis of the OS, middleware applications, and web applications of public servers, such as Web servers, vulnerability diagnoses of network devices, such as firewalls and routers, and advice on countermeasures.

d) If it desires, a local government will be checked for types of malware, such as Gumblar, that transmit a virus even when a web page is browsed. If that type of malware is detected, advice on countermeasures is given to support quick recovery.

e) The adoption of sender domain authentication technologies, such as SPF, will be promoted to prevent malicious third parties from impersonating local governments or their staff in e-mails apparently sent from local governments and harming the general public or private sector.

(B) Promotion of the Dissemination and Enlightenment of Information Security for Education-Related Departments of Local Governments (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)

Support is to be provided so that local government employees can attend trainings without being restricted by time and location and can acquire knowledge about information security.

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

a) Continuing from FY2010, for incorporated administrative agencies, the formulation and review of information security policy that take into consideration the set of measures in government agencies, including the Standards for Measures, will be required and the necessary support provided.

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

c) The adoption of sender domain authentication technologies, such as SPF, is to be promoted to rule out malicious third parties from impersonating incorporated administrative agencies or their staff through e-mails apparently sent from incorporated administrative agencies and harming the general public or private sector.

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

Continuing from FY2010, a system for contacting incorporated administrative agencies—including during emergencies—is to be prepared, and its effectiveness is to be validated in FY2011.

(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 other national agencies are to be actively pursued by using the Chief Information Security Advisors Liaison Conference and the like, for example.

<2> Improvement for Cyber Security Abilities in Critical Infrastructures

As information security measures for critical infrastructures, improvement of the cross-sectoral public-private sector cooperation is to be continuously pursued on the basis of the “Second Action Plan.” More specifically, the activities of the CEPTOAR Council[24] are to be promoted to improve the cross-sectoral information sharing/analysis activities concerning information security for critical infrastructures, and critical infrastructure protection measures are to be improved by analyzing threats to critical infrastructure fields and by conducting inter-divisional exercises.

Especially as a precaution against new type cyber attacks on control systems, failure analyses are to be conducted, ways of making the system resilience are to be studied, and consideration of guidelines for information sharing and formulating safety standards is to be taken.

Business Continuity Plans (BCP) are to be studied in terms of information security after the roles of the public and private sectors are clearly divided, taking the response to the Great Earthquake and the occurrence of a large-scale system failure into consideration.

In addition, international cooperation in the field of critical infrastructures protection will be promoted.

A) Improvement of the information sharing activities

(A) Classification of sharing information (Cabinet Secretariat)

a) a) According to the framework of information sharing and keeping up with changes in threats to information securities and changes in social structure/trends, continuous efforts to coordinate and strengthen for necessary information sharing are to be carried out as usual. b) The methods for information sharing useful to critical infrastructure operators are to be studied together with the issues identified in the Great Earthquake, and the results are to be compiled in FY2012.

(B) Promotion of Information Sharing between the Public and Private Sector Based on

[24] Point of cooperation and information sharing, formed by CEPTOARs (abbreviation of Capability for Engineering of Protection, Technical Operation, Analysis and Response; systems performing the functions of information sharing and analysis in different fields of critical infrastructure), established in February 2009

the Implementation Procedures of Information Sharing of the "Second Action Plan on Information Security for Critical Infrastructures" (Cabinet Secretariat)

a) In order to facilitate a resilience of critical infrastructure operators, it is important for there to be cooperative efforts by each entity in the public and private sectors, then information sharing is to be promoted through the "Information sharing procedures between public and private sectors of the Second Action Plan on Information Security Measures for Critical Infrastructures" (hereafter, "Implementation Details") under the information sharing activities based on the "Second Action Plan."

b) From the viewpoint of continuous effort to improve information sharing, the Implementation Details are to be reviewed at the end of the fiscal year by taking into consideration the progress situation of the operational situation of information sharing and coordination of necessary information sharing based on the Implementation Details, and revision is to be carried out, if required.

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

a) For the information sharing described in B) above, about each rule for information sending to and from government agencies in charge of critical infrastructures and CEPTOARs, to keep consistency with Implementation Details, and these information sharing rules are to be improved, where necessary.

b) For the rules for information sharing within CEPTOARs, government agencies in charge of critical infrastructures should support each CEPTOR activities by giving advice or other way, and check the response situation in CEPTOARs so as to ensure consistency with the Implementation Details.

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

a) In order to support the reinforcement of CEPTOAR activities, the information of the functions and the state of activities of each CEPTOAR will be compiled and published by the end FY2011 as the target under the cooperation of the government agencies in charge of critical infrastructures..

b) Under the cooperation of the government agencies in charge of critical infrastructures, opportunities are to be provided for ensuring the ability of information sharing in order to maintain and improve the information sharing activities of the CEPTOARs in each sector.

(E) Reinforcement of Public Affairs (Cabinet Secretariat)

Continuing from FY 2010, in order to enlighten the public on the importance of information security, raise the standard of information security measures, such as of critical infrastructure operators , and lift the nation's information literacy, it is continuing to encourage reinforcement of public affairs by the use of the Web and other way same as in FY2010 related to information security measures. In addition, by use of opportunities such as seminars or lectures, the action plan and related policies are to be actively publicized.

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

Under the support of government agencies in charge of critical infrastructures, in order to promptly grasp the changes in the information security environment of critical infrastructures and the means for promoting mutual risk communications, and enable robust communications and rapid actions by these organizations, the action plan for promoting mutual risk communications between critical infrastructure operators and its coordination bodies, and the government agencies in charge of critical infrastructures is to be considered. Simultaneously, it will be consider issues such as concerning the Great Earthquake (information sharing at the time of a great disaster, dynamic risk response).

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 Operators (Ministry of Economy, Trade and Industry)

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

(H) Usage and Dissemination of the "Guidelines for Improving the Reliability of Information Systems" (Ministry of Economy, Trade and Industry)[Repetition: Refer to 2(1)<1>G)]

B) Promotion of activities by the CEPTOAR Council

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

In order to ensure active 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 resilience capabilities are to be supported.

C) Organization and dissemination of Safety Standards

(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, in order to respond to changes in social trends and reflect new knowledge in a timely manner, will continue to analyze and verify the “Principles for Formulating of “Safety Standards, Guidelines, etc.” concerning Assurance of Information Security of Critical Infrastructures (Version 3)” and detailed procedure for the principles and prepare to publish supplements to the guidelines, as necessary.

b) The government agencies in charge of critical infrastructures will implement analysis and verification of “Safety Standards” in each critical infrastructure sector by the end of FY2011 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 dissemination 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 dissemination for the “Safety Standards.”

<Investigating the critical infrastructure sectors>

Assessment and verification of the implementation status, improvements arose from the Great Earthquake, and future implementation schedule for the analysis, verification and revision of “Safety Standards” are to be implemented in FY2011, and the results are to be published.

<Investigating the critical infrastructure operators>

The status of dissemination of “Safety Standards” and improvements arose from the Great Earthquake are to be examined at the start of FY2011, and the results are to be published. In addition, the planning and preparation for the investigations to be undertaken in the following year are to be implemented.

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

In order to plan for the provision of more stable ICT services, the analysis and evaluation of incident occurrence conditions or the contents reported by telecommunication operators during incident occurrence will be undertaken, and the results will be published regularly.

D) Improvement of critical infrastructure protection measures

(A) Implementation of Common Threat Analysis (Cabinet Secretariat)

As for new threats that could occur in common to critical infrastructure sectors, detailed analysis will be carried out with attention paid to the changes in the technology environment surrounding the systems, and domestic and overseas research trends, and a specific object of analysis selected.

In FY2011, internal and international examples of failures in control systems occurred due to targeted cyber attacks, which have attracted attention these days, are to be closely examined, and risk that critical systems in critical infrastructure sectors might cause an IT failure under the same type of cyber attack is to be analyzed. As a countermeasure, ways of making the robust system resilient are to be studied.

The analysis is to be implemented with the cooperation obtained from CEPTOARs, critical infrastructure operators, and government agencies in charge of the critical infrastructures, and the results are to be reported returned these 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, cross-sectoral exercise is to be carried out accordingly, and issues concerning revisions of BCPs of the operators are to be extracted.

Obtained results are to be shared among the parties concerned and are to be published as far as possible.

(C) Preparation of Support System for Reliability Improvement of Information System

Used by Critical Infrastructures (Ministry of Economy, Trade and Industry)

a) Continuing from FY2010, in order to support the voluntary efforts by critical infrastructure operators to improve the reliability of information systems, the reinforcement and sharing of fault case database, quantitative macroanalysis of the information voluntarily offered from critical infrastructure operators and its coordination bodies , 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 of manufacturers and plants and next-generation electricity supply networks (smart grids)— to create materials for the dissemination and enlightenment of information security measures for reducing the vulnerabilities of critical infrastructure control systems.

(D) Cyberattacks (Incident) Response Coordination and Support activities(Ministry of Economy, Trade and Industry) [Repetition: Refer to 1(1)B)]

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

a) In order to enhance the response abilities for critical radio communication interference incident, the centralized reception service at out of business-time for critical radio communication interference incident report is to be continuously implemented, and the system for taking quick actions on out of business-time is to be reinforced.

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 sensors of the same facilities will be renewed in FY2011.

c) Radio wave monitoring technologies are to be examined and studied, with recent changes in radio usage environment, such as radio wave monitoring facilities sophisticated in response to broadband radio usage, taken into consideration.

E) Response to problems on information security concerning control systems

(A) Examination and implementation of Measures Based on Problems of Control Systems (Cabinet Secretariat)

Examples of failures in control systems, such as SCADA, in critical infrastructures, including overseas cases, caused by Stuxnet, are to be closely examined, and ways of making these systems invulnerable will be studied with Japan's characteristics taken into consideration. Useful information and actions that should be taken immediately, obtained from the examinations and studies, are to be shared among critical infrastructure operators through government agencies in charge of critical infrastructures. Further, if necessary, reflection to "Principles for Formulating of Safety Standards, Guidelines, etc. concerning Assurance of Information Security of Critical Infrastructures (Version 3)" is to be considered.

If a failure occurs in a control system, action must be taken to prevent the damage arise from its expanding and to resolve the problem by quickly information sharing about, for example, the response situation.

(B) Formulation of control system information security standards and establishment of an evaluation and certification system (Ministry of Economy, Trade and Industry)

A task force is to be set up to improve the information security of control systems. The task force will formulate control-system information security standards, consider international standardization, and work towards the establishment of an evaluation and certification system.

Development of human resources to be responsible for the system and to deal with incidents concerning control systems is also to be considered.

Activities to raise awareness about information security as control-system users are to be implemented.

(C) Establishment of Cooperation Framework to Deal with Vulnerabilities of Control Systems (Ministry of Economy, Trade and Industry)

Countermeasures against threats to vulnerabilities of control systems are to be effectively undertaken by collecting, sharing, and releasing information useful for security countermeasures of control systems together with concerned control system coordination bodies. .

(D) Preferential Provision of Vulnerability Information of Software and Control Systems to Critical Infrastructure Operators and Support for Security Information Management (Ministry of Economy, Trade and Industry)

a) The requirements of vulnerability handling systems that allow parties concerned with control systems to take measures in a planned way and to take safety precautions are to be reviewed to minimize risks and costs resulting from vulnerabilities found after control-system software products are launched or after systems start operating.

b) JPCERT/CC provides CEPTOARs and critical infrastructure operators with information on threats to information security against which critical infrastructure operators should take action and corresponding countermeasures, as early warning information in accordance with previous agreements.

c) Information on software vulnerabilities is to be released in a form that can be easily used.

F) Elaboration of Business Continuity Plans (BCP)

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

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

In FY2011, a survey on the actual effects of the Great Earthquake on steady-state information system operation of critical infrastructures and their ripple effects on critical infrastructure services is to be conducted. Issues to be included in the BCP of critical infrastructure in terms of steady-state information system operation will be extracted, and appropriate countermeasures designed.

G) Promotion of International Alliances in the Area of Critical Infrastructures

(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) In order to contribute to the improvement of Japan’s information security measures, information will be disseminated to relevant domestic entities with regard to IT fault incident cases and best practices obtained through international collaboration or overseas information collection. Dissemination of information from domestic entities to relevant countries is to be supported, as Japan’s international activities such as export of hardware infrastructures might be affected.

<3> Promotion of the Information Security Industry

Contribute to the stimulation and globalization of Japan’s information security industry, through establishment of new information security technologies, promotion of research and development towards world-leading information security, and human resource development.

(A) Promotion of Information Security Industry (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

What is essential to raise the level of Japan’s information security is stimulation of the information security industry.

The establishment of information security technologies for new ICT, such as cloud computing, IPv6, smartphone, SNS, and their ways of usage, promotion of research and development of world’s leading, active, and new dependable (defined as “New Dependability”) information security, and development of high-level human resources for information security, will help stimulate Japan’s information security industry and to increase its international competitiveness.

A working group is to be set up under the “Technological Strategy Special Committee for Security Technology Strategy” to study the means for stimulating Japan’s information security industry.

(B) 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 identified, and after evaluating their significance, countermeasures will be considered.

In FY2011, a medium-scale IPv6 security evaluation environment will be built in cooperation with industry, and various security evaluation tests will be conducted under various attack scenarios.

(C) Lending of Vulnerability Verification Tools for IPv6 Environment (Ministry of Economy, Trade and Industry)

To promote utilization of existing TCP/IP-related vulnerability verification tools that can verify 14 types of vulnerabilities in the IPv6 environment, dissemination and enlightenment activities will be continued.

(D) Promoting the Use of Secure and Reliable IT Products (Cabinet Secretariat, Ministry of Economy, Trade and Industry and All Government Agencies) [Repetition: Refer to 2(1)<1>F)]

(E) 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>D)]

(F) Support for Ensuring Information Security during Procurement of Information Systems (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)<1>G)]

(G) Cloud Computing Security (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)<4>B)]

<4> Reinforcement of Other Infrastructures

To ensure safe and secure ICT infrastructure in socioeconomic activities keeping up with technological innovations, address information security issues concerning smartphones, which have been spreading rapidly.

Study and promote information security measures for cloud computing, IPv6, and SNSs, which have been spreading even while their information security issues have been pointed out.

To improve and reinforce countermeasures against malware, study and establish an effective framework for protection against cyber attacks and countermeasures against targeted cyber attacks.

A) Information Security Measures Concerning Smartphones

(A) Promotion for Ensuring Security of Smartphones (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

So-called smartphones have been rapidly spreading. As the number of users increases, the number of cases of computer viruses infection has been increasing. To provide a safe and secure environment and to contribute to the worldwide market expansion, technical issues accompanying the widespread use of smartphones will be made known to the users and studied when necessary, with differences from conventional mobile phones and PCs taken into consideration.

B) Establishment and standardization of information security measures adapted to cloud computing

(A) Cloud Computing Security (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.

(B) Dissemination and Promotion of Checklist for Service Level of Cloud Computing (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 service level of cloud computing is to be disseminated and promoted.

(C) Preparation of a 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 on reliability improvements. This will 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 to the preparation of an audit framework.

In FY2011, development will be carried out on technologies for the improvement of the reliability, compatibility, energy efficiency, etc. in cloud computing. In addition, the audit framework and standards for cloud computing and security will be formulated and included in reports.

(D) R&D for Building the Most Advanced Green Cloud Computing Foundation (Ministry of Internal Affairs and Communications)

A goal is to establish by FY2012 a technology that provides a highly-reliable, high-quality cloud computing service, while devising energy saving of 20% to 30% on a normal basis and also links multiple clouds immediately to prevent important data from being lost at the time of a widespread disaster. Development and verification of constituent technologies is to be continuously conducted.

(E) R&D of Cloud-Based Security Technology (Ministry of Internal Affairs and Communications)

In order to maintain socioeconomic infrastructure using cloud computing, growing with information security issues such as information leakage still remaining, in safe and secure conditions, new information security measures technologies are to be developed.

(F) Enhancement to Information Security Measures for New Technologies (Cabinet Secretariat and Ministry of Internal Affairs and Communications) [Repetition:

Refer to 2(1)<1>E)]

C) Ensuring IPv6-related and SNS-related information security

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

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

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

(B) Building of Security Evaluation System for IPv6 Environment (Ministry of Internal Affairs and Communications) [Repetition: Refer to 2(1)<3>]

(C) Lending of Vulnerability Verification Tools for IPv6 Environment (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)<3>]

(D) Information Security Measures Concerning Use of Social Media (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

a) As the use of social media services has been spreading in recent years, attackers targeting them have been increasing. In that context, the Cabinet Secretariat will study measures for ensuring information security concerning the use of social media services and measures for making them known to the public.

b) Since the Great East Japan Earthquake, the use of social media services by public agencies, including national and local public entities, has been spreading. Accordingly, the Cabinet Secretariat, the Ministry of Internal Affairs and Communications, and the Ministry of Economy, Trade and Industry will work together to ensure that current precautions, such as a measure for preventing identity theft, are known to users, and review such precautions, as necessary.

D) Improvement and reinforcement of countermeasures against malware

I) Response to Information Security Incidents

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

Regarding measures to prevent infection by computer programs that carry out cyber attacks through remote operations (bot programs) by malicious third parties and the countermeasures for prompt and effective prevention of the sending of spam e-mail or cyber attacks from computers infected by bot programs, concerned organizations will continue their trial and study based on the framework built until FY2010.

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

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

a) To reduce the risk of cyber attacks in Japan, an international information collection network for cyber-attacks (malware infection, distributed denial-of-service attacks, etc.) is to be built, and R&D for fighting against cyber attacks is conducted with the cooperation of ISPs, universities, etc.

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 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 will 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, organizations such as JPCERT/CC that carry out coordination and support for incident responses are to promote further improvements to analytical capabilities concerning attack methods, and information sharing and collaboration involving analysis methods and incident cases among specialists.

b) For the malware samples analyzed in incident response support activities of JPCERT/CC and the analysis results, consideration will be 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 the Internet fixed-point observation information sharing system (TSUBAME).

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

Enhancements are to be devised for the popularization of CSIRT and collaboration during emergency and non-emergency times between JPCERT/CC and the CSIRTs in domestic and overseas organizations. This will be achieved through sharing between suitable parties: materials related to CSIRT structure and operations, threat information or attack information contributing to incident countermeasures and responses, and specific countermeasures information that has been previously analyzed.

II) Sample Analysis

(A) 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 defined to clarify the lawfulness of reverse engineering for information security purposes.

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

In addition to conventional passive information security measures, such as accepting notifications concerning vulnerabilities, active efforts will be made to detect cyber attacks and vulnerabilities.

(C) Measures against Targeted Cyber Attacks (Ministry of Economy, Trade and Industry)

a) Support is to be given to efforts for building a framework that allows information concerning targeted cyber attacks to be shared among information security business community including security companies and antivirus software vendors and among public agencies and also prevents damage from spreading. As part of that, a pilot project for collecting and sharing information is conducted.

b) Multiple protection measures are needed to reduce the risk of targeted cyber attacks in different phases. The measures will be organized as technical standards as early as possible, and minimum technical requirements will be examined so that it can be used in the operation of the Act on the Protection of Personal Information (Act No.

57 of 2003). On the basis of the results of examination, activities will be conducted to raise awareness of user companies for preventing targeted cyber attacks.

c) In addition, measures against targeted cyber attacks through existing services such as IPA’s “Worry-Free Information Security Consultation Service” and JPCERT/CC incident measures are to be continued.

d) Threats and attacks from the inside will be analyzed to establish measures against attacks by insiders, which could have a very serious effect on industries and society.

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 information system users and developers.

[1] Add search/statistics function for vulnerability classification information of “JVN iPedia” (vulnerability countermeasures information database), enhance the management function, and release the tool to the public.

[2] In order to reliably deploy vulnerability information to users and server managers, expand the range of support by “MyJVN” (vulnerability countermeasures support tool for information system users) to the server OS and server products. Provide a function to customize check items, working together with IPA’s reminders, so that any specific incident can be dealt with.

(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 responses 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 pre-shipment inspections) in the form of explanatory materials and seminars are to be continued.

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

c) Vulnerability verification tools for TCP/IP and SIP protocols used by developers of embedded devices and intelligent home appliances are to be continuously provided to developers.

d) In order to support the self-learning of Website operators and product developers on the necessity of countermeasures and countermeasure methods, efforts for proliferation and enlightenment are made based on “How to Secure Your Website” and the experiential and practical learning tool “AppGoat.”

e) Information security issues that can occur on automobiles, where vehicle-mounted systems may be sophisticated and network access through external connection devices may be provided in the future, and corresponding countermeasures will be studied.

f) In order for the early detection of vulnerabilities in the embedded systems of digital TV sets, where Internet access is increasing, and take appropriate measures, a vulnerability detection service will be set up, trial operations will start, and other vulnerability measures for embedded products will be promoted.

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

In order that the vulnerabilities of web applications can be discovered early, the “Website Vulnerability Log Analytical Inspection Tool” (iLogScanner), which analyzes logs and inspects traces of external attacks, is to be continuously provided to corporate Website operators.

(D) Preferential Provision of Vulnerability Information of Software and Control Systems to Critical Infrastructure Providers and Support for Security Information Management (Ministry of Economy, Trade and Industry) [Repetition: Refer to

2(1)<2>E)]

(E) Establishment of Cooperation Framework to Deal with Vulnerabilities of Control Systems (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)<2>E)]

IV) Other Related Efforts

(A) Efforts concerning Information Leakage Measures (Ministry of Economy, Trade and Industry)

a) In order to deal with information leakage measures, including that of personal information, information leakage countermeasures tool, possessing functions to prevent information leakages through file-sharing software are to be continuously provided to the general public.

b) Information regarding new data leakage methods is to be collected, and countermeasures and other necessary information is to be provided to the general public.

(B) 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 FY2011, the index for visualizing software quality will be prepared, and proposals will be made to the International Organization for Standardization.

(C) Promotion of DNSSEC[25] Introduction (Ministry of Internal Affairs and Communications)

Continuing from FY2010, PR activities will be implemented towards the smooth introduction of DNSSEC.

(D) Enhancement of Spam E-Mail Measures (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Consumer Affairs Agency) [Only e) is repetition:

[25] Abbreviation of Domain Name System Secure Extensions. Expanded specifications for ensuring appropriate DNS response.

Refer to 2(1)<1>C)]

a) In order to deal with ever increasing spam e-mails, which are increasingly ingenious and malicious, steps are to be defined to steadily enforce the Act on Regulation of Transmission of Specified Electronic Mail and the Act on Specified Commercial Transactions.

b) With the cooperation of the “JEAG” industry group—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, which is effective in the prevention of spam e-mail transmission, are 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 collaboration with overseas enforcement agencies in charge of spam e-mail measures, cooperation with the private sector on international spam e-mail measures is to be promoted.

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

e) The Cabinet Secretariat and all government agencies are to push for the adoption of sender domain authentication technology, such as SPF (Sender Policy Framework), to rule out malicious third parties from impersonating government agencies or their staff and harming the general public or the private sector. In addition, since e-mail may be sent to government agencies from senders impersonating government agencies or their staff, the adoption of sender domain authentication technology is to be facilitated on the receiving side.

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

(A) 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)<4>D)]

(B) Preparation of Security Evaluation and Certification 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 evaluations and certification based on ISO/IEC 15408 domestically, preparation of a standard smart card for vulnerability evaluation, nurturing of skilled personnel survey, etc. are to be steadily implemented.

(C) Preferential Provision of Vulnerability Information of Software and Control Systems to Critical Infrastructure Providers and Support for Security Information Management (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)<2>E)]

(D) Establishment of Cooperation Framework to Deal with Vulnerabilities of Control Systems (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)<2>E)]

(E) Formulation of Control System Information Security Standards and Establishment of an Evaluation and Certification System (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)<2>E)]

(F) Support for Ensuring Information Security during Procurement of Information Systems (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)<1>G)]

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

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

a) The "Information Security Leadership Nurturing Seminars for Small-To-Middle Sized Businesses," targeted at those in a position to guide small-to-middle sized businesses, are to be held, and cooperation is to be given for other information security seminars held by small and medium enterprises, so that improvements to the security level of such businesses is to be secured.

b) 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, which can face difficulties in undertaking information security measures.

(B) 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 who underwent the "Information Security Leadership Nurturing Seminars for Small-To-Middle Sized Businesses," besides providing information security consultations using training courses, are to introduce and provide enlightenment materials and guidance tools created by the IPA, etc.

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

G) Promoting Safe Electronic Trading

(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.

H) Promoting intellectual property protection

(B) Deterring of Copyright Infringement on the Internet (Ministry of Internal Affairs and Communications, Ministry of Education, Culture, Sports, Science and Technology, and Ministry of Economy, Trade and Industry)

a) In order to deter content infringing copyright from spreading globally on the Internet, international examinations will be conducted to build a system for sharing information on copyright holders.

b) Through bilateral talks and dispatch of the Joint Public-Private Intellectual Property Protection Mission (composed of the Japanese Government and the International Intellectual Property Protection Forum (IIPPF)), a country where a piracy problem is found will be requested to reinforce measures against content infringing copyright. To request overseas providers to delete content infringing copyright, use of the Content Overseas Distribution Association (CODA) by the private sector is to be encouraged.

(C) Expansion of Signatory Countries to the ACTA (Anti-Counterfeiting Trade Agreement (provisional name)) (Ministry of Foreign Affairs, Ministry of Economy, Trade and Industry, Ministry of Education, Culture, Sports, Science and Technology, Ministry of Internal Affairs and Communications, Ministry of Justice, Ministry of Finance)

In order to protect brand equity internationally, Asian and other overseas countries are to be encouraged to join the ACTA.

<5> Enhancement of the Functions of the National Information Security Center (NISC)

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

A) Enhancement of the NISC's Comprehensive Coordination Functions

(A) Strengthening of the 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 used fully.

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

(B) Fulfillment of Information Security 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 its information security consulting functions by the experts of the center in order to respond to the various needs toward promoting the information security measures of the concerned government agencies, including the responses related to the Standards of Measures, the emergency responses, and so on.

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

Information Security Policy Council and NSIC willclosely cooperate with not only the IT Strategic Headquarters but the relevant centers and councils such as the Council on the Realization of the New 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) Reinforcement of the Nation and Users Protection

To raise awareness about IT risks among the nation and users and build a community where they can take information security measures individually, enhance and reinforce awareness-raising activities on the basis of the "Information Security Outreach and Awareness Program." The "Outreach/Awareness and Human Resource Development Committee" is to be set up to clarify the central functions concerning awareness raising. To serve the international community, international alliances concerning awareness raising will be actively promoted.

Continue enhancing information security consultation services, promoting personal information protection, and reinforcing cybercrime policing countermeasures.

<1> Conducting and Information Security Campaign

(A) Promotion of "Information Security Outreach and Awareness Program" (Cabinet Secretariat and concerned government agencies)

a) On the basis of the "Information Security Awareness-Raising Program," measures included in the program are to be steadily promoted.

b) In order to heighten awareness of the importance of information security and deepen the understanding of each person in the country, as a tool for allowing each person to recognize objectively the phases of each measure, the preparation of a self-examination checklist for the nation and users will be considered.

c) Attention is to be paid not to unnecessarily arouse uneasiness in the elderly, and the preparation of documents describing information security measure for elderly people in plain language will be considered.

d) Company executives should understand that management must conduct risk management as well as security management through the information systems department of the company. A program for raising awareness of company executives is to be studied.

(B) Installations of the "Outreach/Awareness and HR Development Committee" (Cabinet Secretariat and concerned government agencies)

Under the "Information Security Policy Council, an "Outreach/Awareness and HR Development Committee" (provisional name) is to be set up to clarify the central function concerning awareness raising on information security. The committee will contribute suggestions, and make evaluations on awareness-raising or human resource development measures concerning information security.

Under the “Outreach/Awareness and HR Development Committee” (provisional name), a “Public-Private Sector Alliance Working Group” (provisional name) will be set up to promote awareness-raising programs. The working group will plan and promote public-private sector alliance projects.

(C) Fulfillment of “Information Security Awareness Month” (Cabinet Secretariat and concerned government agencies)

In order to heighten the information security awareness and deepen the understanding of each person in the country, the “Information Security Awareness Month” will be further publicized, and the related events held during that period will be improved.

(D) Consideration of Holding “Information Security Awareness Month” in October (Cabinet Secretariat and concerned government agencies)

In order to further promote international alliances in the future, it will be considered to change Japan’s “Information Security Awareness Month” from February to October or to hold a new “International-Alliance Information Security Awareness Week” (provisional name) in October while maintaining the “Information Security Awareness Month” in February.

(E) 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, Ministry of Education, Culture, Sports, Science and Technology)

a) 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 “Website on Information Security Awareness Raising,” “@police,” “Information Security Site for the People,” “Internet Safety Classes,” “Council of Anti-Phishing Japan,” “Japan’s Anti-Phishing Council,” and “Worry-Free Information Security Consultation Service,” 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 people who are indifferent to information security.

b) During the Informatization Month of FY2011, in order to honor individuals and corporations who have made a significant contribution from the viewpoint of information security, the “Information Promotion Contribution Award” will be held.

c) Continuing from FY2010, a course ("e-Net Caravan") mainly targeting guardians, educators, elementary, junior high, and high school students for enlightening children about the safe and secure use of the Internet, will be held nationwide in cooperation with telecommunication organizations.

d) 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.

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

In the radio frequency 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, the regional Bureaus of Telecommunications will implement publicity and enlightenment for stores selling devices that use radio frequencies.

(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) Human behavior for promoting information security measures will be surveyed and subjected to social-scientific analysis.

c) The information security situation and outlook of FY2010 will be gathered into the "Information Security White Paper 2011" and published.

(H) Support for Ensuring Information Security during Procurement of Information Systems (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)<1>G)]

(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 non-functional requirement items, including requirements related to reliability, performance or security, efforts will be pursued with the cooperation of relevant industries on the usage and dissemination of methods for appropriately agreeing between users and vendors.

(J) Collection and Sharing of Cases such as Information Security Accidents (Cabinet Secretariat)

In order to prevent information security accidents from occurring and to take appropriate measures against such accidents, it is important to verify past information security accidents and share the lessons learned from them. Existing released cases are to be collected, and a method of collecting anonymous cases that cannot be released in terms of trade secrets or privacy protection will be considered. The collection of information security accidents will be publicized so that many people can use this data.

<2> Suggestion to Set Up an “Information Security Safety Support Service” (tentative name)

(A) Improvement of “Information Security Consultation Service” (Cabinet Secretariat and concerned government agencies)

Information security consultation services provided by concerned government agencies will be improved from the viewpoint of the nation and users, by strengthening cooperation among them or by improving the consultation system. The Consumer Affairs Agency, the Cabinet Secretariat, and concerned government agencies in charge of consumer protection will work together to upgrade the consultation services to consumers.

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

The operation of the “Worry-Free Information Security Consultation Service,” redesigned as a general consultation service concerning malware and unauthorized access from the former consultation service, will be continued. Consultations for information security faced by computer users will be expanded, and the service is to be widely publicized to the nation.

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

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

The raising of information security levels across the entire nation is to be carried out by nurturing and utilizing knowledgeable people (Information Security Supporters) close to users in local areas.

<3> Promotion of Personal Information Protection

A) Reviewing the Act on the Protection of Personal Information

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

For the Personal Information Protection Act, from FY2011 onwards, consideration is to be given to deliberations on issues with a view to amending the law.

B) Adapting to an international framework

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

In FY2011, Japan will attend the meeting of the OECD Committee for Working Party on Information Security and Privacy under the Committee for Information, Computer and Communications Policy and the meeting of the APEC Electronic Commerce Steering Group's Data Privacy Subgroup, and assess considerations on cross-border issues of privacy law enforcement in the OECD and the efforts of APEC Data Privacy Pathfinder projects, etc. Japan will also consider the responses and measures required of the nation from the viewpoint of international cooperation, and international understanding of Japan's personal information protection laws will be sought.

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

While taking into consideration the trends of existing international discussions such as in the OECD and APEC, consideration is to be given to research collaboration on measures for data privacy protection through international conferences, such as the ASEAN-Japan Information Security Policy Meeting, following rapid changes in the related environment.

<4> Tightening Policing against Cybercrime

A) Organization of a cybercrime policing infrastructure

(A) Enhancement of 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, preparedness to appropriately tackle cybercrimes will be enhanced, for example, by promoting the preparation of resources, equipment, and materials for policing cybercrime.

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

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

In order to enhance public-private cooperation for appropriately dealing with cybercrime, 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 to be given to cooperation between the government and the information security industry.

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

(F) Promptness of International Investigative Mutual Assistance Using Central Authority System[26] (Ministry of Justice and National Police Agency)

In principle, mutual legal assistance treaties or accords came into force between

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

Japan-US, Japan-South Korea, Japan-China, Japan-HK, Japan-EU, and Japan-Russia making mutual assistance obligatory. Under these treaties or accords, central authorities are set up to pursue promptness of mutual assistance through direct communications for assistance between the central authorities without the requirement of proceeding through the usual diplomatic channels. Hereafter, consideration will be given to the conclusion of further mutual legal assistance treaties.

B) Crime prevention campaign

(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 FY2010 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 occurrences 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 such as 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)

a) Besides creating leaflets for junior high school and senior high school students for the prevention of criminal damage related to dating sites publicity and enlightenment such as those on basic countermeasures, cybercrime methods and countermeasures carried on the National Police Agency Websites in response to the various problems of Internet users will be implemented.

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 supporting the nurturing of cyber volunteers to promote volunteer activities in cyberspace.

(3) Reinforcement of International Alliances

To reinforce bilateral relationships between Japan and the US, study and review specific cooperation items through frameworks such as Japan-US cyber security meeting, Japan-US Policy Dialogue on Internet economy, and other bilateral meetings. Promote alliances with concerned European states, such as the UK, and organizations/agencies, such as the European Commission.

For alliances with the ASEAN region, measures based on the alliance framework are to be implemented steadily, and at the fourth Japan-ASEAN Information Security Policy Meeting, past efforts will be evaluated and future cooperation will be discussed.

In the international alliance field, cooperation concerning measures against cyber incidents, public-private sector alliances and international alliances for critical infrastructure protection, cooperation on awareness raising in the information security field, and cooperation on human resource development will be promoted.

<1> Strengthening Alliances with the United States, ASEAN, and the EU (Strengthening Bilateral Relationship and Ties with ASEAN)

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

In order to build close cooperation in information security policies between regions, in FY2011, enhancement of strategic bilateral cooperation, such as discussions on collaboration in individual fields concerning information security will be planned by holding bilateral meetings such as Japan-US cyber security meeting and Japan-US Policy Dialogue on Internet economy. Talks to build collaboration concerning information security with European countries such as UK are planned, and information security will be discussed in Japan-EU ICT policy dialogues.

(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 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 the ICT 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 continuously with various ASEAN countries through the ASEAN-Japan Information Security Policy Meeting.

a) Steady promotion of items decided at the Third ASEAN-Japan Information Security Policy Meeting (FY2011)
b) Holding the Fourth ASEAN-Japan Information Security Policy Meeting in Malaysia (FY2011) and the Fifth ASEAN-Japan Information Security Policy Meeting in Japan (FY2012)
c) Holding the ASEAN-Japan Government Networks Security Workshop 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 (FY2011)
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. (FY2011)
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 (FY2011)

(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 Outsource Countries (Ministry of Economy, Trade and Industry)

In FY2011, 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.

Operations for functional changes to the Asian information security benchmark and dissemination and information exchange concerning Asian countries will be started.

(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 that have deep relations with the business activities of Japanese companies, the building up and operations of CSIRT, as well as collaborative support, are to be carried out. In FY2011, dissemination and enlightenment of CSIRT establishment seminars and technical support activities are to be carried out.

(H) Support for Enhancement of the 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 FY2011, based on the experience of support activities for CSIRT establishment accumulated in JPCERT/CC, the operations technology for incident response jobs 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.

(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 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 trends 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)<4>D)]

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

(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 (Organization for Economic Co-operation and Development), ASEAN (Association of Southeast Asian Nations), EU (European Union), and G8 (Group of Eight), the field of incident response—like FIRST (Forum of Incident Response and Security Teams), the field of national security guarantee—like ARF (ASEAN Regional Forum), and the field of ICT use—like ITU (International Telecommunications Union) and ACF (APT Cybersecurity 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 Information Security Evaluation and Certification Technology in the Asian Region (Ministry of Economy, Trade and Industry)

At the third meeting (scheduled to be held in November 2011) 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 agreements 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 the evaluation and certification systems in the various Asian countries and the technology and trends in this field.

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

Japan will participate in international meetings hosted under ISO/IEC JTC 1/SC 27, ITU-T SG17 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.

(E) Cloud Computing Security (Ministry of Economy, Trade and Industry) [Repetition: Refer to 2(1)<4>B)]

<3> Enhancement of the NISC’s Function as a Point of Contact

(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 strengthened in relation to the basic ideas and strategy of 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 Websites, such as by publishing English editions of the Information Security Strategy, and this document, on the NISC Web site in FY2011.

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 used as feedback.

(4) Furtherance of Technological Strategies, etc.

On the basis of the “Information Security Research and Development Strategy,” promote R&D of active, dependable information security technologies that realize “Game-Change” and lead the world to implement a safe and secure ICT system that can create new values as a foundation supporting society.

On the basis of the “Information Security Human Resource Development Program,” make active approaches to nurture information security-related human resources.

<1> Strategic Furtherance of Information Security Research and Development

(A) Promotion of Studies on “Information Security Research and Development Strategy” (Cabinet Secretariat and concerned government agencies)

On the basis of the “Information Security Research and Development Strategy,” R&D is conducted to ensure new dependability of the entire information and telecommunications system, to perform Zero-Day Defense[27] based on behavior analysis of attackers, to implement flexibility management of personal information, to establish R&D facilitation foundation, and to systematize security theory, and the progress is confirmed. When the progress confirmed, the establishment of a scientific evaluation framework as a foundation for stimulating information security study is to be considered.

(B) R&D of Cloud-Based Security Technology (Ministry of Internal Affairs and Communications) [Repetition: Refer to 2(1)<4>B)]

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

From FY2010, R&D is to be continued to establish a quantum information communication network technology, including quantum cryptography with information-theoretic safety (unconditional safety of cryptography in the information-theoretic sense).

[27] Term meaning a defense technology corresponding to a zero-day attack (attack at a vulnerability in OS or application before a patch for correcting the vulnerability is provided). More specifically, an active defense technology that reads the optimization of cyber attack countermeasures by profiling the attacker or by analyzing behavior models.

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

With the object of realizing a society in which everyone can use information communication networks safely and securely without being aware of the security technologies in the background, NICT is conducting R&D on the world's most advanced cyber attack observation/analysis/countermeasure/prevention technology, secure-network design/evaluate/optimize technology, next-generation fundamental cryptography technology, and other network security technologies that combine theory with practice in a sophisticated manner.

In FY2011, by using the test environment of the user support system for malware structured in the previous year, a demonstration experiment will be conducted with general users who have applied to participate in the experiment, and the validity of the system will be tested.

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

In ensuring the security of information communication networks, NICT will aim to establish an evaluation method to verify whether the communication protocols installed in network devices, such as routers, are secure in FY2012, and design details of the evaluation method, expand them, and build an evaluation system verification base by using the results obtained in FY2010.

(F) Building of a Cyber Security Research Test Bed (Ministry of Internal Affairs and Communications)

To promote R&D into cyber security, NICT will build a test bed that allows attack traffic, malware samples, and other security data sets to be used safely.

In FY2011, basic studies will be conducted on a filtering function and a sanitizing function for secure use of data sets, and a prototype will be developed.

(G) Building of Security Evaluation System for IPv6 Environment (Ministry of Internal Affairs and Communications) [Repetition: Refer to 2(1)<3>]

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

With a view to implementation around FY2020, R&D will be promoted for new-generation network infrastructure technologies capable of ensuring the most appropriate quality, security and disaster-resistant in response to user requirements by overcoming the IP network limits. In FY2011, by organically combining the constituent technologies, system configuration technologies and platform configuration technologies that can provide a variety of network services will be developed.

(I) 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 ICT society of the highest global standard by disseminating the software traceability concept as a means 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 the end of FY2011. In FY2011, the last year of this research, the following will be implemented to build an infrastructure for the dissemination of software tags.

[1] Determination of specifications to use as the basis of tag operation, utilizing analyses conducted in the applicability testing of software tags and release of them in reference installations.

[2] Evaluation of basic software tag generation tools, facilitation of cooperation with tools for expansion, visualization, and evaluation, and organization of requirements of the actual basic service.

[3] Activities for adoption of software tags as an international standard.

[4] Study on the applicability of software tags from the legal viewpoint and organization of user-vendor conflict resolutions

(J) 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 continued to FY2011 with the aim of solving basic issues rather than treating the symptoms. This is in order to have ensured continuing freedom from information system incidents that could cause the stagnation of all economic activities, or risks that could affect the nation's life or property.

(K) Preparation of a Green and Secure Cloud Computing Environment (Ministry of

Economy, Trade and Industry) [Repetition: Refer to 2(1)<4>B)]

<2> Development of Information Security Human Resources

(A) Promotion of "Information Security Human Resource Development Program" (Cabinet Secretariat and concerned government agencies)

On the basis of the information security human resource development program describing measures for cultivating and securing information security human resources in the medium and long-term, an expert committee on awareness-raising and human resource development will be setup, leading-edge information security researchers and engineers will be trained, and human resource development, public-private sector partnership, international collaboration, and other measures will be steadily promoted in government agencies, the private sector, and educational agencies.

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

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

(C) Study in Information Security Expert Development Framework (Ministry of Economy, Trade and Industry)

a) In order to nurture advanced IT experts, including information security experts, enhancements are to be established to the industry-academia partnership system by verifying a platform built for independent, continuous industry-academia implementation.

b) In order to nurture advanced IT experts, including information security experts, a next-generation model of the advanced IT experts desired in the IT service industry will be described and publicized, including examples of potential new IT service businesses, so that students and young engineers can picture their future career paths.

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

d) In order to nurture security experts, 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), the council responsible for implementing the examination, together with the cooperation of specific countries (Philippines, Vietnam, Thailand, Myanmar, Malaysia, and Mongolia) in which the examination system has been established, will implement a unified examination system for Asia by bringing in the system from Japan. Also, by expanding ITPEC efforts, Japan's IT skills standards will also be disseminated.

(D) Publicity for Information Security Certifications (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 experts, including information security experts, the Information Technology Engineers Examination, which measures the skills of experts in various information fields, including the information security field, is to be promoted.

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

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

(F) Nurturing and Utilizing Information Security Supporters (Ministry of Internal Affairs and Communications) [Repetition: Refer to 2(2)<2>]

(G) Human Resource Development for Cyber-Attack Countermeasures (Ministry of Defense) [Repetition: Refer to 1(1)C)]

<3> Establishment of Information Security Governance

(A) Promoting the 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 on businesses in relation to corporate information security is to be reduced and overseas trends taken into consideration.

b) In FY2011, when new information security governance in enterprises is introduced, measures for clearly positioning information security are to be considered and a report is to be written.

c) For the “Guidelines for Improving the 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),” which visualizes the status of compliance with the guidelines, together with the “Reliability Self-Diagnosis Tool,” usage and dissemination are to be facilitated in private sector enterprises and in government agencies.

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

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

a) The “Survey on the Actual Information Processing Situation 2010” will examine the usage status of information security audit systems, information security management compliance evaluation systems, and information security measures benchmark in enterprises, the checking status on the implementation of information security measures at transaction counterparties (including outsourcing and consignments), 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 ledgers. In addition, the use of guaranteed audits will also be facilitated. In FY2011, in order to reduce registrant burden and improve the user convenience, the design of the business audit ledger 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 audits 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 those people taking custody of information. In FY2011, effort will be put into the dissemination of the Information Security Report model by inquiries to individual enterprises.

(C) Usage and Spread of the “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 the cooperation of industry groups relevant to both users and vendors.

(5) Organization of System concerning Information Security

Prepare appropriate laws for dealing with cybercrime, and actively discuss a system that improves cyberspace safety and reliability.

<1> Identify Measures to Improve Cyberspace Safety and Reliability

(A) Smooth Enforcement of Cyber Penal Code (Ministry of Justice)

Since the "Law for Partial Revision of the Penal Code, etc. to Respond to Advancement of Information Processing, etc." (Cyber Penal Code), which has been prepared to deal with cybercrimes appropriately and to conclude the Convention on Cybercrime, was promulgated, newly added clauses such as the criminalization of creation of a virus will be publicized, and its procedural law will be prepared for smooth enforcement.

(B) Cooperation toward Conclusion of the Convention on Cybercrime (Ministry of Foreign Affairs)

Since the domestic law needed for the Convention on Cybercrime was promulgated (not yet enforced) in June 2011, preparation for early conclusion of the Convention will be made with cooperation with concerned government agencies.

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

On the basis of "Issues for Improving Cyberspace Security and Reliability" (March 2011), continued study is conducted on issues on a system for improving cyberspace security and reliability to meet the changing situation concerning information security.

(D) 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)<4>D)]

(E) 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) [Repetition: Refer to 2(1)<4>G)]

<2> Comparison of Information Security Systems of Different Countries

(A) Examining Security Law Systems in Different Countries (Cabinet Secretariat)

By proceeding to survey and analyze the legal systems of major countries, consideration will be given to the issues surrounding each country and the measure of cooperation.

V　Information Security Policies after the Great East Japan Earthquake

For restoration and reconstruction following the Great East Japan Earthquake and for new growth, efforts will be made to improve security and reliability at the time of large-scale disaster from experience in accordance with the extent of the damage, by building a disaster-resistant information and telecommunications system in terms of information security, establishing risk management and risk communications, and ensuring new dependability of the entire information system.

１ Building a Disaster-Resistant Information and Telecommunications System

(A) Study on Appropriate Physical Security Measures in Government Agencies (Cabinet Secretariat)

To respond to serious environmental changes, such as the Great East Japan Earthquake, that can have an enormous influence on physical security, the Cabinet Secretariat will survey advanced examples in the private sector and will study appropriate physical security measures in concerned government agencies. Then, guidelines will be formulated on the basis of the actual conditions in government agencies.

(B) Examination of a Plan for Appropriate and Smooth Implementation of the Standards for Information Security Measures for Central Government Computer Systems (Cabinet Secretariat)

Concerned government agencies are required to implement appropriate security measures even when an environmental change that could seriously damage their information systems, such as the Great East Japan Earthquake, occurs. Accordingly, a risk management method suitable for government agencies will be studied in order to ensure appropriate and smooth implementation of the new framework of the Standards for Measures, and to clarify the range of information resources held by the concerned government agencies and their handling methods. Guidelines will then be formulated. By sharing the results among the concerned government agencies, shared risk communication among the concerned government agencies will be developed.

(C) Enhancement of Business Continuing Capabilities (Cabinet Secretariat and all government agencies)

a) In order to ensure business continuity plans, concerned government agencies will formulate the plans needed to continue the operation of necessary information systems by the end of FY2011, from the viewpoint of ensuring the continuity of administration in times of disaster or failure, by making use of the "Guidelines for Operation Continuity Planning of Central Government Computer Systems," formulated by the Cabinet Secretariat.

b) For appropriate management concerning maintenance and continued improvement of the levels of measures, the Cabinet Secretariat will study the evaluation method of the information system operation continuity plans formulated by concerned government agencies.

(D) Re-Examination of IT Systems in Critical Infrastructure Sectors (Cabinet Secretariat)

In critical infrastructure sectors, the damage to information systems caused by the Great Earthquake, its effect on critical infrastructure services, emergency countermeasures and restoration work undertaken by corresponding enterprises, and their effect will be examined and analyzed. Since the chain of damage had a major effect in the last Great Earthquake, interdependence among critical infrastructure sectors specified in the investigation into the past will be verified.

On the basis of the results of verification, considering how supply chains should be ensured, the minimal functions of IT systems that should be maintained in times of large-scale disaster, measures for making systems invulnerable to maintain such functions, measures for preventing data from being completely lost, and the like, will be studied successively, and be reflected into the review of safety standards and examination of the BCP in terms of information systems in the future. These will also be verified through opportunities for inter-sectoral practices.

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

a) To support the individual efforts of critical infrastructure providers to improve their information systems continuously from FY2010, a database of fault incident cases will be organized and maintained, and accumulated information that is analyzed quantitatively and macroscopically will be provided to CEPTOARs.

b) In preparation for creating materials for promoting information security measures for reducing vulnerabilities in control systems of critical infrastructures, the security of control systems and smart grids of manufacturers and plant industry at home and overseas will be investigated.

(F) Examination of Requirements for Information and Telecommunications System Immediately Following a Large-Scale Disaster (Cabinet Secretariat and Ministry of Internal Affairs and Communications)

The current pressing need is to establish an information and telecommunications system that can respond to the situation in the fastest possible time in an unimaginably chaotic state immediately after the occurrence a large-scale disaster.

At the time of the Great Earthquake Information it was the reported that the transmission and information sharing methods that people most used included safety confirmation by SNSs or the Internet, which was unprecedented in Japan.

By investigating and analyzing the status of information transmission after the occurrence of the Great Earthquake, the roles of industry, government, academy, and individuals in information transmission immediately after the occurrence of the disaster will be re-defined from the viewpoint of risk communications, and the requirements for information systems and information transmission in an emergency will be assessed. This will be studied together with the other items included in the annual plan.

(G) Improvement of Disaster Resistance of Information Security Technologies (Cabinet Secretariat)

In order to enable secure and accurate information transmission and information sharing in times of disaster, the Cabinet Secretariat will verify issues concerning information security technologies, such as authentication methods and encryption methods in times of disaster, from the experience acquired from the Great Earthquake, and will improve the disaster resistance of information security technologies.

２ Establishment of Risk Management and Risk Communication

(A) Analysis and Evaluation of the Effect of the Great East Japan Earthquake on Information Systems (Cabinet Secretariat)

In order to formulate and improve the information system operation continuity plans of government agencies, the Cabinet Secretariat will analyze and evaluate the effect of the Great East Japan Earthquake on the information systems and will provide information to the government agencies and will utilize information for studies to enhancing business continuation capabilities.

(B) Study on Risk Management Method Based on Experience Acquired from the Great East Japan Earthquake (Cabinet Secretariat)

Accurate information on potential risks in times of disaster should be given quickly to concerned parties, and the concerned parties need to create an agreement in advance. For that purpose, the effectiveness of risk communications and a risk management method based upon it will be studied from the experience acquired from the Great East Japan Earthquake.

(C) Study on a Flexible Management Method for Personal Information (Cabinet Secretariat and concerned government agencies)

To realize flexible management of digitized personal information, a study on practical measures and management methods will be promoted.

(D) Improvement of Mutual Coordination among Critical Infrastructures (Cabinet Secretariat)

On the basis of a survey concerning the Great Earthquake, how the measures based on the Business Continuity Plan were changed when the disaster surpassing our imagination occurred and how critical infrastructures or sectors cooperated in emergency measures or restoration measures, will be studied. This will also assess dynamic risk management, in which the risk level varies according to the situation, and extract useful information that should be shared to encourage cooperation among critical infrastructures or sectors in times of large-scale disaster or major fault incidents.

(E) Facilitation of Risk Communications among Critical Infrastructure Fields (Cabinet Secretariat and government agencies in charge of critical infrastructures)

Since multiple critical infrastructure fields in a large cross-sectoral scale were hit by the Great Earthquake, risk communications among critical infrastructure fields will be facilitated in order to share the lesson and the experience from a large-scale disaster. Through this activity, an understanding of dynamic risk management will be deepened. This activity will be implemented in cooperation with government agencies in charge of critical infrastructures, other concerned agencies, and the CEPTOAR Council.

(F) Reflection of Knowledge Related to Earthquake Disaster in Guidelines for Formulating Safety Standards (Cabinet Secretariat and government agencies in charge of critical infrastructures)

In order to efficiently utilize the knowledge acquired from the experience of the Great Earthquake, the "Principles for Formulating of "Safety Standards, Guidelines, etc." concerning Assurance of Information Security of Critical Infrastructures (third edition)" and the countermeasures of the principles will be analyzed and verified on the basis of lessons acquired from risk communications among critical infrastructure fields, and if necessary, the principles will be improved.

(G) Study of Risk Management in Critical Infrastructure Fields (Cabinet Secretariat)

Based on the survey and analysis concerning the Great Earthquake in critical infrastructure fields, risk management will be examined from the perspective of making systems invulnerable and maintaining data integrity. The effectiveness of acquired knowledge will be verified in cross-sectoral exercises, and effective issues may be incorporated into the BCP for secure information system operations.

Ensuring New Dependability Across the Entire Information System

(A) Promoting the Information Security Research and Development Strategy (Cabinet Secretariat and concerned government agencies)

In order to ensure the new dependability of information systems, R&D of fundamental information security technologies for next-generation networks where real space and virtual space are combined, and technologies for building a network architecture that can automatically recover from damage, will be promoted to realize a disaster-resistant information and telecommunications system as stated in the "Information Security Research and Development Strategy."

(B) Promoting R&D of Technologies for Ensuring Automatic System Security Configurations (Ministry of Internal Affairs and Communications)

In order to establish technologies for implementing and verifying correct security configurations, which are important to ensure information security, the NICT will promote R&D on security architectures for selecting appropriate security technologies automatically and configuring an optimum secure network.

(C) R&D for Building the Most Advanced Green Cloud Infrastructure (Ministry of Internal Affairs and Communications)

A further goal is to establish by FY2012 a technology that provides a highly-reliable, high-quality cloud service, incorporating energy saving of 20% to 30% on a normal basis, and which can also link multiple clouds immediately to prevent important data from being lost at a time of widespread disaster. Development and verification of constituent technologies are to be continuously conducted.

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

With a view to implementation around FY2020, R&D will be promoted for new-generation disaster-resistant network infrastructure technologies capable of ensuring the most appropriate quality and security in response to user requirements by overcoming IP network limits. In FY2011, by organically combining constituent technologies, system configuration technologies and platform configuration technologies that can provide a variety of network services will be developed.