Information Security 2012

July 4, 2012
Information Security Policy Council

Contents

I Preface

Japan has adopted a range of information security measures with due consideration given to the viewpoints of the nation and users, based on the "Information Security Strategy for Protecting the Nation" (May 11, 2010; hereafter, "ISS Strategy") and its annual plan, "Information Security 2010" (July 22, 2010) and "Information Security 2011" (July 8, 2011).

However, the environment surrounding information security has been changing considerably: even in FY2011 the way information and communications technology (ICT) is used has altered significantly, as seen in the emergence of new threats, such as a prolific number of obvious targeted attacks on companies and other organizations that handle important national information on security , along with the rapid and widespread use of smart devices, cloud computing[1] and social networking services (SNS). The increase in threats related to cyber attacks is being taken as a critical issue even by major overseas nations, with each country strengthening strategic initiatives, such as the announcement of cyber security strategies by the U.S. and U.K., and growing momentum in tackling the issue by the creation of international norms and active international discussion in conferences such as the United Nations and the London Conference on Cyberspace.

Based on these changes in the environment, this document sets forth the details of the specific efforts to be implemented in FY2012 and FY2013, to ensure that appropriate measures can be taken.

Furthermore, in the case of continued changes in the environment relating to information security measures, appropriate steps will be devised and implemented within the necessary scope in response to such changes. Additionally, documentation that specifies the framework of such information security measures, such as the IS Strategy, will also be reviewed as required.

[1] In this new way of using computer networks, data services and Internet technology are located in a cluster of servers (cloud) on a network; users are able to access "no matter where, whenever required, and only the required functions" without needing to process and store anything on his/her own computer, which is different to the case so far.

II Changes in the Environment Surrounding Information Security

In the IS Strategy (May 2010), background environmental changes were categorized into four groups as follows.

(1) Increasing threats of large-scale cyber-attacks and so on; (2) Increasing dependency on ICT in socioeconomic activities; (3) Adapting to new technological innovation; and (4) Globalization etc. Following the formulation of Information Security 2011 (July 2011), another group, (5) Great East Japan Earthquake, was added.

Based on these 5 groups, this document summarizes the features of the marked changes in the environment surrounding information security of late.

(1) Occurrence and Escalation of Sophisticated Cyber Attacks

In 2011, threats of targeted attacks[2], cases of which were reported to have previously occurred overseas, emerged in Japanese government agencies. Targeted attacks generally focus on stealing information from a small number of targets by secretly entering the targeted sites. The features that expose these attacks differ in nature, as seen in the multitude of DDoS (Distributed Denial of Service) attacks that have occurred to date.

Targeted e-mail attacks use sophisticated social engineering methods, such as maliciously using current information of the attack target worded in a clever way so as to enable the user to readily open the mail. There are also attacks that use sophisticated techniques such as malware or other harmful code, which infects a computer via email and remains hidden within the information system, and also tries to infect the administration server for network users. Such attacks are expected to become even more clever and complex.

In 2011, a number of targeted attack emails were sent to government agencies, within which in some agencies the workers opened the attached files in the email causing the computer to be infected with malware or other harmful code. Targeted attack emails were also sent to the House of Representatives and House of Councilors, infecting the terminals with malware or other harmful code. The resultant damage of such attacks is continuing to spread, such as the emerging possibility of some companies handling important national

[2] Combining a number of attack methods, these attacks are launched on specific organizations and individuals using social engineering.

information being infected with malware or other harmful code via targeted attack emails and this information being subsequently stolen.

The risk of such possible sophisticated cyber attacks aimed at stealing important government information is expected to further escalate, and thus there is a strong demand for measures to improve and combat such a situation.

(2) Emergence of Risk and Growing Dependency on ICT in Socioeconomic Activities

The proliferation of mobile broadband, spread of smart phones and other smart devices and rapid widespread use of SNS in recent years is seeing an accelerated growing dependence on ICT in socioeconomic activities.

Smart phones have more sophisticated features and advanced operability compared to mobile phones[3], and allow users to access various applications and browse the same websites as those in PCs. This has lead to the rapid expansion in users of these compact and highly user-friendly smart phones. In addition to being able to be used in the same way as a PC, smart phones also feature a multitude of applications that acquire and utilize GPS positioning and other user information, and as such are inclined to accumulate the personal information of the user, compared to mobile phones. Conversely, many users recognize smart phones as having the same level of safety as mobile phones, and so they tend to have a relatively low awareness of information security compared to PC users. Moreover, the large number of smart phone users throughout the world, the fact that technology for anti-virus security software is still in the development stage, and the continuing use of operating systems (OS) which allow for the easy creation of malware or other harmful code, among other factors, make smart phones a low-cost high-return attack target for developers of malware or other harmful code. Under these circumstances, there is an increasing number of malware and other harmful code targeting smart phones and that enable the unauthorized communication of users' personal information to outside sources. Immediate measures are being called for to deal with the security of smart phones, as attacks targeting smart phones could possibly also expand from hereon to include cases of financial fraud involving the misuse of accumulated personal information.

---

[3] In this document, this term refers to conventional mobile phones other than smart phones.

In addition, considering the existence of blogs, SNS and video sharing sites and the like that tend to list personal information, as well as the full-fledged introduction and use of data centers and cloud services, there are concerns that these sites and services may become targets of cyber attacks. There are also concerns about various attacks in IPv6, which allows for a greater number of network access devices, due to the ease of establishing a direct connection to external networks, and also over security threats arising from operation misses caused by its combined use with IPv4.

In the government as well, the progression of e-government services is seeing a further rise in dependency on ICT in administrative services. In such circumstances, regarding the cryptographic algorithms (SHA-1 and RSA1024) that are widely-used in the information systems of government agencies for carrying out electronic applications, electronic bidding and other transactions, in light of the release of abstract decryption algorithms, improvements in computer processing capabilities and other advancements have raised fears that both algorithms will be decrypted. As such, the immediate migration to SHA-256 and RSA2048 is anticipated. Furthermore, considering the promotion of common government platform as well as social insurance/taxation numbering system and national ID system, the continual progressive computerization of government administration from hereon has made ensuring information security a crucial task.

Moreover, conventional control systems were considered to be highly secure, as they are independent from information-related systems and also utilize different technology. However, in recent years, the risk of control systems in terms of information security has been rising due to an increasing number of cases where these systems have adopted the same technology as information-related systems, or have been interconnected with them. Ensuring the information security of control systems, in particular those used for critical infrastructure, is directly linked to the security of the daily lives of citizens, and so immediate measures for these systems are required.

In this way, the growing dependence on ICT in socioeconomic activities has brought with it the emergence of various risks, and this necessitates the promotion of initiatives for developing an environment to enable the secure use of ICT.

(3) Emergence of New Risks Associated with New Technological Innovation

The miniaturization of communication devices and growth of network infrastructure has enabled various devices, such as home appliances, motor vehicles and sensors, to connect with networks, and for each device to exchange information with the network without the intervention of humans. Utilization of this M2M[4] system is spreading, and if continued advancements in positional information technology, interface technology, sensor technology and the like further expand the use of M2M, it is expected to create an environment where the benefits of such technologies can be enjoyed, without any particular thought, in a broad range of areas in society through the use of ICT services.

However, the preparation of an environment for the use of M2M has just started, and so it is not necessarily being conducted with information security measures in mind. In addition, the majority of devices using M2M have so far not been connected to networks, or have been designed on the premise of connection to a closed network. Therefore, the connection of such devices to the Internet and other networks will require measures for its new accompanying threats. For instance, in the case of inappropriate information security measures such as the absence of patch applications or anti-virus measures or insufficient encryption and verification functions, there are concerns that information may be leaked via these devices, or that the device itself will be subject to unauthorized control.

The information security measures in such M2M are different from the conventional information security measures for human-mediated networks, and thus require immediate consideration by the government and industry.

(4) Increasing Need for Risk Aversion Initiatives for the Failure of Crucial Information Systems

The Great East Japan Earthquake generated a multitude of damage including the loss of power, damage and destruction of buildings, and severing of networks. Learning from these lessons, a survey was conducted in the National Security Information Center (NISC[5]) on appropriate measures to be taken at the time of a disaster and the direction of risk management and so on. The report[6] listed the issues of priority measures and mid-to-long

---

[4] M2M (Abbreviation of Machine to Machine) refers to a system in which machines connected to each other in the network can exchange information and automatically achieve optimal control without human intervention. For example, each sensor and device (intelligent home appliances, vehicles, vending machines, buildings, smart phones etc.) is coordinated through the network and can perform services in a variety of fields including energy management, facilities management, aging degradation monitoring, disaster prevention, welfare, etc.

[5] Abbreviation for National Information Security Center

[6] "Study on the response situation of government agency information systems in the Great

term measures regarding items that have not yet been anticipated. These issues must be steadily addressed in working towards building a robust information communications system for use when disasters occur.

Also, in 2011, the increase in data traffic in mobile phone networks and rapid rise in transfers to specific accounts and so on were accompanied by large-scale failures in the info-communications systems of banks and mobile phone vendors. Within the increasing dependency on ICT in socioeconomic activities and growing demand for new technology and services, a high level of reliability is being demanded in info-communications systems. Accordingly, preparations in the event of a serious system failure and risk aversion initiatives for such an occurrence need to be promoted.

(5) Strengthening Initiatives in Other Countries

Within the rising number of threats in cyber space following the sophistication and diversification of cyber attacks, strategic initiatives for information security are being strengthened in other countries.

In May 2011, the International Strategy for Cyberspace was announced in the U.S. The Strategy outlined, as its basic policy, upholding the fundamental principles of the recognition of new domestic and international security- and economic-related issues, fundamental rights of freedom and privacy, and the free flow of information. Also, the Strategy stated the importance of measures to support the following as its goals to achieve: (1) Securing an open and interoperable network, (2) Enabling security and reliability, and (3) Establishing a cyberspace based on appropriate norms; and also as its future initiatives: (1) Diplomacy through cooperative partnerships with each country, (2) Defense by the dissuasion and deterrence of terrorists, criminals and threats to the nation, and (3) Development of a prosperous and safe cyberspace.

Meanwhile, in November 2011 a new cyber security strategy was also announced in the U.K., which recognized the Internet as a revolutionary technology that is essential in socioeconomic activities, while at the same time outlining its vision to secure fairness and transparency by 2015 based on the appropriate laws in order to strengthen the national security and prosperity of cyberspace, after clarifying security issues that must be

---

East Japan Earthquake" (March 2012, National Information Security Center), "Study and analysis on the disaster situation of critical infrastructure information systems in the Great East Japan Earthquake" (March 2012, National Information Security Center)

addressed. Under this vision, the U.K. Government has raised the following as measures to tackle: (1) Tackling cyber crime, (2) Strengthening the ability to recovery from cyber attacks (resilience), (3) Building an open, stable and vibrant cyberspace, and (4) Sharing cross-cutting knowledge and improving skills and capabilities.

In addition to these initiatives taken by each country, discussion is continuing on the creation of international norms to counter the various threats in a borderless cyberspace that accompany the benefits it also brings. In December 2010, a resolution was passed in the UN on matters for discussion concerning norms on national ICT usage, and on holding a Groups of Governmental Experts meeting (UN Cyber GGE[7]) in 2012-13 on "Developments in the field of information and telecommunications in the context of international security". Based on this, the December 2011 resolution clarified discussion of the aforementioned norms in the same GGE meeting. Further, the Internet was addressed in the G8's Deauville Declaration of May 2011, while in December 2011 recommendations on Internet policy principles were adopted in the OECD[8]. These and other initiatives, such as the London Conference on Cyberspace held in November 2011, confirm recognition of the need for a global international alliance to address the issues concerning cyberspace.

Japan also recognizes the importance of further strengthening its bilateral and unilateral ties on the issue of cyberspace. To this end, Japan participated in the 2011 London Conference and has proceeded with its international alliances through bilateral and unilateral frameworks. Japan also reaffirmed its agreement on the necessity of deepening bilateral The Japan-U.K. Joint Statement issued in April 2012 and Japan-U.S. Leaders Summit held in the same month.

[7] Abbreviation of Group of Governmental Experts.
[8] Abbreviation of Organisation for Economic Co-operation and Development.

III Basic Lines

Principally, the basic ideas described in "Information Security Strategy for Protecting the Nation" are considered to be appropriate as measures for addressing the environment changes outlined in II. The following points listed below are considered to require particularly focused measures in light of the marked changes occurring these days.

(1) Strengthening Measures for Sophisticated Threats to Companies and Organizations Handling Important National Information on Security

The threats of targeted attacks on companies and organizations handling important national information on security (hereinafter, "the State, etc.") have become a reality and thus measures to address these threats have become a matter of urgency.

Targeted attacks are considered to mostly have the main purpose of stealing information from within organizations. Once the State, etc. has encountered such an attack, it is possible that confidential and personal information will be stolen and thus bring about a serious state that compromises the security of the nation and lives of its citizens.

Further, such targeted attacks generally narrow down their subjects for attack, and use unknown computer viruses that cannot be detected by anti-virus software, which makes these attacks difficult to uncover. In regards to the strengthening of measures for targeted attacks, these need to not just stop at the areas focused on by conventional strategies, the so-called population strategies, but also include multistage measures such as the encryption of crucial information and exit strategies. However, a definite approach for such measures has not yet been established.

Although within these attacks are those that are difficult to uncover, information on the attacks that were somehow able to be discovered should be shared among related parties including those working on countermeasures and so on, while paying due consideration to the personal and corporate information of the attack victims, as this is thought to be effective in preparing for any further attacks.

To this end, in the State, etc., while proceeding with building a framework

for public-private sector partnerships concerning targeted attacks and continuing with the sharing, analysis and examination of information, each entity is required to establish a system having CSIRT[9] and other such functions, and ensure the staffing and enhancement of necessary personnel for emergency information security measures to cover the related agencies. It is also important to proceed with R&D and other activities and promote initiatives for effective measures to address targeted attacks.

(2) Maintaining a Safe and Secure User Environment for Addressing the Emerging Risks Associated with the Proliferation of New Information and Communications Technology Including the Full-Fledged Widespread Use of Smart Phones

Along with the increasing sophistication of ICT is the accumulation of a massive amount of information in smart phones and cloud computing, which is exchanged instantaneously via high-capacity communication lines. In the event of insufficient information security, this information can be easily stolen and exposed to the risk of misuse.

While smart phones are very user-friendly by enabling users to connect to the Internet by various routes and effortlessly download applications and other data, they also allow for the easy download of malware or other harmful code, and as such have a great deal of information security-related issues compared to mobile phones. The number of malware or other harmful code targeting smart phones is rapidly rising, and the threats surrounding smart phones are changing daily.

In these circumstances, it cannot be said that many smart phone users are sufficiently aware of the differences in information security between mobile phones and smart phones, and as such even the minimum recommended information security measures have not necessarily been fully taken. As smart phones are expected to become even more sophisticated and widespread from hereon, the necessary measures for information security should be widely informed to smart phones users as common knowledge. Also, efforts are needed to establish the required technological measures that correspond with the sophistication of smart phones and trends in smart phone-related threats. In addition, from the perspective of protecting minors, there are also calls for the consideration of effective measures for introducing into smart phones the filtering technology incorporated into mobile phones and other devices.

Also, regarding cloud computing with its large-scale accumulation of personal and corporate information, SNS and the control systems directly linked with the security of

---

[9] Abbreviation of Computer Security Incident Response Team.

citizens' lives, initiatives for ensuring even greater information security are essential.

Further, in the near future, the utilization of smart grids and other such M2M systems is forecast to expand. As a result, large volumes of information will be exchanged without people noticing it, and this information will form the base for automatically determining the optimal operating conditions. However if the information security related to this network is infringed, it is also likely that the entire system will start to operate in a completely unpredictable manner. Therefore, ensuring information security for M2M is a crucial issue that should be addressed going forward.

(3) Reinforcement of International Alliances

There is a growing sense of danger throughout the world towards the threat of cyber attacks. As such, ensuring information security is now a common theme among countries around the globe.

In such circumstances, following on from discussion in the UN and the London Conference on Cyberspace and so on, initiatives for creating an international framework are rapidly progressing. As the speculations of each country are complex, it is paramount that Japan actively participates in the creation of an international framework including the high-level strategic communication of information, so as to ensure that a framework is created based on the national position on information security.

In addition to creating an international framework, it is also important to build international alliances. The circle of alliances established to date through a range of forums, including Japan-U.S., Japan-U.K., Japan-EU and Japan-ASEAN[10], should be widened and confirmed initiatives continued.

The domestic development of information security measures and participation in the creation of an international framework should be carried out under Japan's clear basic lines, which are also described in "Information Security 2011" and refer to securing a safe and reliable cyberspace while maintaining the openness and interoperability of the Internet. Specifically, it proposes taking a balanced approach to problems such as ensuring information security, protection of secrecy of communications, protection of personal information and countermeasures against the violation of intellectual property rights, without interrupting the free and cross-border distribution of information and while giving consideration to the social and economic benefits

[10] Abbreviation of Association of South East Asia Nations.

derived from the Internet.

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 FY2012.

1 Strengthening of Public-Private Sector Partnerships for Targeted Attacks

In strengthening the response capabilities for sophisticated cyber attacks including targeted attacks, government agencies will be made ready to tackle these issues by reinforcing the public-private sector partnerships concerning information sharing, while also preparing CSIRT and other systems in the respective government agencies and strengthening those alliances.

To enhance Japan's overall response capabilities, the government will develop advanced analysis functions, as well as build a database and analysis environment and promote R&D on sophisticated detection technology.

A Strengthening of Public-Private Sector Partnerships

(a) Further promotion of information sharing between public-private sectors (Cabinet Secretariat and concerned government agencies)

The NISC acts as a plank between the respective public-private sector and government information sharing networks operated by the respective government agencies, and strives to further promote public-private sector information sharing on cyber attacks.

(b) Strengthening of Public-Private Sector Partnerships in Cyber-Intelligence Countermeasures[11] (National Police Agency)

Carrying out initiatives to contribute to reinforcing information sharing systems with businesses and other entities that are possible targets for

[11] Refers to [Measures for espionage activities using ICT (cyber-intelligence)]

cyber attacks, and developing cyber intelligence measures.

(c) Strengthening of cyber information sharing initiatives (Ministry of Economy, Trade and Industry)

Carrying out initiatives for forming alliances with other countries and increasing the number of participating organizations concerning cyber information sharing initiatives (J-CSIP[12]).

(d) Strengthening of Telecom-ISAC Public-Private Sector Council partnership (Ministry of Internal Affairs and Communications)

Carrying out initiatives for reinforcing information sharing systems in the Telecom-ISAC public-private sector council.

(e) Establishment of Information Sharing Systems From Normal Times (Cabinet Secretariat and all government agencies)

Promoting public-private sector information sharing by building a system to enable regular meetings to be held with private sector CSIRT and SOC[13] business organizations, as well as the daily exchange of opinions.

B Preparation of Response Capabilities in Government Agencies

(a) Preparation of CSIRT Systems and Reinforcement of Alliances (Cabinet Secretariat and all government agencies)

a) In the event of a targeted attack or other such information security-related threat occurring, so as to respond automatically to such incidents, systems having CSIRT and other functions will be put in place in the respective government agencies, and work on the complete and continuous implementation of these measures.

b) The Cabinet Secretariat will carry out initiatives for the alliance and collaboration with CSIRT and the like in government agencies, as the government's CSIRT coordinator.

(b) Promotion of Information Security Measures for Companies and Organizations Handling Important National Information (Cabinet Secretariat and all government agencies)

a) When concluding a contract for the handling of important information concerning

[12] Abbreviation of Initiative for Cyber Security Information sharing Partnership of Japan.
[13] Abbreviation of Security Operation Center.

national security, the respective government agencies require the contracting party to establish and observe the information security requirements.

b) The Cabinet Secretariat, although not in a direct contractual relationship with the nation, will consider measures for companies and organizations handling important information concerning national security.

(c) Implementation of Education and Training on Targeted Attacks (Cabinet Secretariat and concerned government agencies)

The Cabinet Secretariat, with the cooperation of the respective government agencies, will implement education and training on targeted attacks for those government agencies that wish to participate, while also improving the training methods used. Feedback on the results of the training will be provided to the said government agencies; the findings obtained will be shared among all government agencies, and the results published.

(d) Strengthening of the Accumulation and Sharing of Information to Contribute to Cyber Attack Countermeasures (Cabinet Secretariat and all government agencies)

Regarding information to contribute to cyber-attack countermeasures, along with accumulation of such information by the Cabinet Secretariat, the process will be further enhanced to facilitate the even more timely and appropriate sharing of information between respective government agencies.

Further, the GSOC[14] will conduct analysis on the general trends and state of cyber attacks against government agencies, and the results of the said analysis will be regularly provided to the respective government agencies.

C R&D on Countermeasure Techniques and Analysis on Attack Methods for Enhancing Response Capabilities

(a) Development of Advanced Analysis Functions for Cyber Attacks (Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

In order to respond to cyber attacks with increasingly complex and

[14] Abbreviation of Government Security Operation Coordination team.

multifaceted attack methods, concerned public-private sector parties will each consolidate the respective information at hand and develop mechanisms with advanced analysis functions for such attacks.

(b) Information Collection and Analysis for Shedding Light on Cyber Attack Cases (National Police Agency)

In order to strengthen investigations on illegal behavior, through the analysis of computers hit by a cyber attack and fraudulent programs, information for shedding light on the perpetrators of cyber attacks cases and the methods used will be collected and analyzed on a continuous basis.

(c) Cyber Attack (Incident) Response Coordination and Support (Ministry of Economy, Trade and Industry)

In response to requests from critical infrastructure operators, support will be provided to deal with information security incidents, such as coordination of actions against the source of attack, and also for analysis of attack methods, while also utilizing the cooperative framework with international CSIRT. In 2012, a response coordination and support system specializing in incidents concerning control systems will be developed, as well as response methods for clever and persistent targeted attacks.

(d) New Threat and Attack Analysis (Ministry of Economy, Trade and Industry)

The threat and measure study meetings run by the Information-technology Promotion Agency (IPA [15]) will analyze new threats and attacks in information security and promptly provide the analyzed results and other necessary information to the users.

(e) Support for Building Infrastructure for Information Collection and Sharing (Ministry of Economy, Trade and Industry)

a) Support will be provided for building infrastructure for the collection and sharing of information, along with continuous consideration of establishing an analysis environment and owner database, for the sharing of information between concerned parties on clever and persistent targeted attacks in order to halt the spread of damage from such attacks.

b) Based on the emergence of targeted attacks, in order to prevent the leakage of personal

[15] Abbreviation of Information-technology Promotion Agency.

information caused by cyber attacks, the necessary and appropriate technological measures will be reviewed by incorporating them into the guidelines on the Act concerning Protection of Personal Information (Japan Law No. 57, 2003). Further, based on the examination results, dissemination and education on measures to prevent the leakage of personal information caused by cyber attacks will be offered to businesses that acquire and handle personal information.

c) Measures for targeted attacks through existing initiatives, such as the IPA "Information Security Assurance Consultation Corner" and JPCERT/CC[16] Incident measures, are to be continued.

(f) R&D on Countermeasure Techniques for Targeted Attacks (Ministry of Internal Affairs and Communications)

R&D on countermeasure techniques that are resistant to targeted attacks will be implemented. In 2012, the National Institute of Information and Communications Technology (NICT[17]) will develop a prototype for detection technology on abnormal communications that occur between an organization's internal and external networks, caused by malware or other harmful code which has infected an organization's internal network via a targeted attack.

(g) Examination and Exercises on a "New Information Security Safeguard Model" (Ministry of Internal Affairs and Communications)

While utilizing R&D findings and analysis results obtained from the advanced analysis of cyber attacks, the creation of a prototype for a "New Information Security Safeguard Model" based on a new concept including multilayer safeguards, exit strategies and attack prediction will be reviewed, along with practical exercises using testbeds.

D Reinforcement of International Alliances

(a) Reinforcement of Alliances Through Participation in International Conferences (Cabinet Secretariat and concerned government agencies)

In order to enhance response capabilities for cyber attacks, in 2012 the reinforcement of alliances with other countries will be promoted through

16 Abbreviation of Japan Computer Emergency Response Team/Coordination Center.

17 Abbreviation of National Institute of Information and Communications Technology.

participation in the framework of international alliances such as FIRST[18], etc.

[18] Abbreviation of Forum of Incident Response and Security Teams.

2 Preparation for a Potential Large-Scale Cyber Attack

Taking into consideration the actual threat of a large-scale cyber attack incident, counteraction is to be enhanced by initiatives such as training on initial response measures upon the occurrence of a large-scale cyber attack and the collection of information. In terms of security-related initiatives, based on the "National Defense Program Guidelines for FY2011 and Beyond," defense-related systems against cyber attacks are to be reinforced for the stable use of cyberspace. Counteraction and response capabilities will be comprehensively reinforced through cracking down on cyber crime and strengthening international alliances on response measures against cyber attacks.

A Organizing Counteractive Arrangements

(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) Enhancement of Response Capabilities by the Training of Information Security Emergency Response Personnel (Cabinet Secretariat and concerned government agencies)

Training will be conducted for officers at the Cabinet Secretariat and other government agencies to develop and maintain capabilities for responding to a large-scale cyber attack.

(c) Promotion of Analysis of Threats and Methods Concerning Cyber Attacks (Cabinet Secretariat and concerned government agencies)

Appropriate counteractive arrangements upon the occurrence of a cyber attack incident are to be developed through the promotion of analysis on threats and methods concerning such attacks.

(d) Enhancement of the Accumulation and Sharing of Information to Contribute to Cyber Attack Countermeasures (Cabinet Secretariat and all government agencies)
[Repetition: Refer to 1 B (d)]

(e) Early Identification of Cyber Attack Signs and Enhancement of Information Collection and Analysis (National Police Agency and Ministry of Justice)

In order to strengthen the measures against cyber attacks, information collection and analysis on the subject and methods of cyber attacks will be continuously implemented, such as enabling the early identification of the signs of an attack in cyberspace and the widespread collection of open-source information.

(f) Enhancement of Systems Related to Cyber Terrorism Countermeasures (National Police Agency)

In order to deal with sophisticated cyber-attack methods as a means of cyber terrorism[19], reinforcement of the police force's counter-cyber terrorism system is to be enhanced by strengthening the information collection and analysis systems, and implementing training inside and outside the department to maintain and improve the technical and response capabilities of counter-cyber terrorism personnel to deal with such incidents.

(g) Enhancement of Public-Private Cooperation in Counter-Cyber Terrorism for Critical Infrastructures (National Police Agency)

Initiatives will be taken to contribute to the enhancement of emergency response capabilities upon the occurrence of cyber terrorism by information sharing between business providers through the council for cyber terrorism countermeasures, and also implementing joint training in anticipation of such incidents occurring, while respecting the intentions of critical infrastructure operators.

[19] An electronic attack on the core system of a critical infrastructure, or serious failure in the core system of a critical infrastructure that is highly probable to have been caused by an electronic attack.

In addition, activities will be carried out for raising awareness on the dangers of cyberterrorism, based on the recent cyber attacks against Japanese government agencies, by conducting individual visits to critical infrastructure operators and providing information to corresponding to the special characteristics of each provider.

(h) Enhancement of Public-Private Cooperation in Cyber-Intelligence Countermeasures (National Police Agency) [Repetition: Refer to 1 A (b)]

B Reinforcement of Protection Against Cyber Attacks

(a) Enhancement of Planning Functions Concerning Cyber Attack Countermeasures (Ministry of Defense)

In order to respond to the increase in threats of a cyber attack, the cyber planning functions of the General Staff Office are to be enhanced.

(b) Maintenance of the Japan Ground Self-Defense Force Computer Protection System (Ministry of Defense)

Equipment for monitoring and protecting the information systems of each self-defense force will be maintained, including the Japan ground self-defense force computer protection system for the information systems of the Japan ground self-defense force.

(c) Enhancement of the Functions of Cyber Protection Analysis Equipment (Ministry of Defense)

Taking into consideration the daily advances in technology concerning cyber attacks, the enhancement of functions corresponding to technological advancements will be conducted, such as reinforcing the information collection function and analysis function of cyber protection analysis equipment, and exercise function.

(d) Promotion of Analysis, Response and Research on Cyber Attacks (Ministry of Defense)

In order to further enhance the analysis and response capabilities of the threat and impact of cyber attacks on information systems maintained in the Ministry of Defense, performance confirmation tests will be carried out on the network security analysis equipment that have been prototyped.

A behavior analysis study will also be conducted on malware and other harmful code along with research for detecting cyber attacks.

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

The latest technological trends related to cyber attacks and cyber-attack countermeasures will be studied, in addition to investigation and research on effective response measures, in order to ensure the security of information systems.

(f) Development of Human Resources and Reinforcement of Alliances with Foreign Countries (Ministry of Defense)

In an effort to develop human resources for responding to cyber attacks, an overseas study exchange program will be conducted with domestic and international graduate schools and other tertiary institutions. Participation in various conferences will also be promoted in order to strengthen the Japan-U.S. alliance.

C Policing cybercrimes

(a) Reinforcement of Preparations for Policing Increasingly Malicious and Clever Cybercrimes (National Police Agency)

In order to crack down on new type of cybercrimes that have become increasingly clever at an alarming rate, such as unauthorized access and fraudulent programs (including those targeting smart phones, etc.), internal and external training will be actively conducted for police officers nationwide involved in cybercrime investigations. In addition, preparations for materials and equipment to assist in the policing of cybercrimes are to be continued and a nationwide coordinated approach for investigating cyber crimes will be firmly established, in an effort to reinforce countermeasures for cybercrimes.

(b) Promotion of Efforts in Digital Forensics[20] (National Police Agency)

In order to appropriately deal with increasingly diverse and complex

[20] 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. Digital Forensics.

cybercrimes, the implementation of training for police officers involved in cybercrime investigations, augmentation of resources and equipment, cooperation with relevant institutions and the private sector through participation in relevant meetings and technical collaboration, and enhancement of systems related to digital forensics is to be promoted.

(c) Promotion of International Cooperation for Policing Cybercrime (National Police Agency)

In addition to conducting effective information exchange with the respective law enforcement institutions of various countries closely linked to Japan's cybercrime situation, establishing multilateral cooperative relations will be promoted through actively participating in international frameworks related to cybercrime countermeasures such as G8 and ICPO[21], and by hosting the Asia-Pacific Cybercrime Technology Information Network System Conference.

D Reinforcement of International Alliances Against Cyber Attacks

(a) Reinforcement of an Information Sharing System on Cyber Attacks with the Relevant Institutions of Overseas Countries, and Enhancement of Response Capabilities (Cabinet Secretariat and concerned government agencies)

Cooperative relationships with overseas countries are to be established and reinforced, such as an information sharing system and so on.

(b) Reinforcement of Alliances Through Participation in International Conferences (Cabinet Secretariat and concerned government agencies)

[Repetition: Refer to 1 D (a)]

(c) Reinforcement of Alliances with Relevant International Institutions Against Cyber Terrorism (National Police Agency and Ministry of Justice)

In order to enhance measures against cyber terrorism, information collection and analysis related to attack subjects and methods and so on, will be continuously implemented, including reinforcement of international alliances through information exchange with relevant overseas institutions.

[21] Abbreviation of International Criminal Police Organization.

3 Consolidation of Government Institutions

In the event of a targeted attack or other such information security-related threat occurring, so as to respond automatically to such incidents, systems having CSIRT and other functions will be put in place in the respective government agencies. Further, in the case of the occurrence of a large-scale incident or the like that requires a prompt and precise response from the government, centering on the government CISOs[22], the government will come together to swiftly counteract the incident, and also prepare an immediate response system including setting up an information security emergency support team (CYMAT[23]) to enable automatic support by personnel with specialist skills from other government agencies.

In an effort to enhance the government's response capabilities, the cross-sectional Government Security Operation Coordination team (GSOC), which conducts 24-hour monitoring of government agency information systems, will be enriched and strengthened.

Conducted mainly by the Chief Information Security Officers (CISOs) of the respective government agencies, initiatives related to the creation and publication of the "Annual Report on Information Security" (hereafter, "Information Security Report") will be steadily implemented also in this fiscal year, and information security measures will be continuously improved by running a series of PDCA cycles. Furthermore, efforts will be made to further raise the information security awareness level of each staff member by such initiatives as education and training on targeted e-mail attacks.

In addition to the above, initiatives for preventing the identity spoofing of government institutions, etc., will be further promoted also in this fiscal year, including the introduction of measures using cryptographic technology. Also initiatives to enable a suitable and swift response to

[22] Abbreviation of Chief Information Security Officer.
[23] Abbreviation of Cyber Incident Mobile Assistant Team.

changes in the user environment of information technology surrounding government institutions will be steadily implemented, including the appropriate migration to new cryptographic algorithms, and measures for ensuring the continual operation of information systems in the event of a large-scale natural disaster and addressing the increase in usage of smart phones and cloud computing technology.

Further to this, based on the "Standards for Information Security Measures for the Central Government Computer Systems (hereinafter, "the Standards for Measure") revised in April 2012, information security measures in government institutions will be implemented and the said Standards are to be reviewed as necessary.

A Preparation of CSIRT Systems and Reinforcement of Alliances

(a) Preparation of CSIRT Systems and Reinforcement of Alliances (Cabinet Secretariat and all government agencies)

[Repetition: Refer to 1 B (a)]

(b) Establishment of Integrated Preparations Based on Government CISOs (Cabinet Secretariat and all government agencies)

In order to respond to incidents of large-scale information security threats, upon the occurrence of such an incident, the Cabinet Secretariat will establish a unified position by the government centering on the government CISOs.

(c) Establishment of an Information Security Emergency Support Team (CYMAT) (Cabinet Secretariat and all government agencies)

The Cabinet Secretariat will prepare an immediate response system including setting up an information security emergency support team (CYMAT) to enable automatic support for incidents requiring a unified response by the government, in the event of the information system failure of institutions hit by a cyber attack and subject to receiving support, or the prediction of such an attack occurring.

(d) Establishment of Information Sharing Systems from Normal Times (Cabinet Secretariat and all government agencies)

[Repetition: Refer to 1 A (e)]

B Enrichment and Reinforcement of the Government's Cross-Sectional Information Collection and Analysis System (GSOC)

(a) Enhancement of Emergency Response Capabilities Through the Operation of the Government's Cross-Sectional Information Collection and Analysis System (GSOC) (Cabinet Secretariat and all government agencies)

a) The GSOC, which commenced full-scale operations in FY2008 and performs 24-hour monitoring of government agency information systems, will renew its equipment in FY2012 and aim to strengthen its functions. Further, the collected and analyzed information in the GSOC on cyber attacks will continue to be promptly shared, and through cooperation with relevant institutions, efforts will be made to improve the emergency response capabilities of the entire government.

b) The emergency contact system will be checked through training etc., and its effectiveness will be verified.

C 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; hereinafter, "CISO Liaison Conference") comprising the chief secretaries of the respective government agencies, and strive to strengthen mutual close cooperation. The Cabinet Secretariat is to also enhance the system in which the Chief Information Security Officer is responsible for unifying information security measures.

b) The Cabinet Secretariat is to hold, in succession, the Chief Information Security Advisers Liaison Conference held under the CISO Liaison Conference, and through the expertise from a technical standpoint on common themes and the sharing of best practices, will work toward the sophistication of information security initiatives of the respective government agencies.

(b) Promotion of Efforts Related to the "Annual Report on Information Security" (Information Security Report) (Cabinet Secretariat and all government agencies)

a) The Chief Information Officers of the respective government agencies are to create independent Information Security Reports. In this event, the use of an external audit system will be promoted to ensure the objectivity and expertise of the Information Security Report.

These Information Security Reports will be compared and evaluated at the Chief Information Security Advisers Liaison Conference, and the subsequent findings will be shared and feedback given, and the Chief Information Security Officers will publicly announce the reports at the CISO Liaison Conference

b) The Cabinet Secretariat will objectively evaluate as far as possible the implementation situation of the measures in the respective government agencies, based on the latest version of the Standards for Measures[24] and on the report on the implementation of measures and priority inspections, and request the implementation of necessary measures. This will facilitate the coordination of the improvement of measures of the respective government agencies with that of the improvement to the Standards for Measures, and ensure the establishment and spread of the PDCA cycle throughout the entire government. As such, the measures for improving the efficiency of self-assessment tasks and priority inspections, such as by improving survey items and methods, are to be examined and presented to the respective government agencies.

c) The Cabinet Secretariat will evaluate the implementation situation of the information security measures of the respective government agencies and all government agencies on the basis of the aforementioned evaluation method, and will summarize the results as an "Annual Report on Information Security in Government Agencies." This Annual Report is a means for promoting effective countermeasures by the entire government and also for fulfilling accountability to the nation, and thus while also giving consideration to maintaining and ensuring information security, the Report will be promptly released and reported to the Information Security Policy Council following its finalization by the CISO Liaison Conference.

D Efficient and Continuous Improvement of Information Security Measures in Government Agency Information Systems

[24] The FY2012 version was revised by the Information Security Policy Council on April 26, 2011.

(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 respective government agencies will steadily implement the centralization of their maintained public web servers and mail servers by the end of FY2013, and through this further promote the streamlining of information systems and improvement of operational efficiency, as well as striving to enhance information security measures and increase their efficiency.

b) The Cabinet Secretariat will have a constant grasp of the situation in facilitating the steady promotion of server centralization, and report on this 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 the respective government agencies, will implement vulnerability checks for the main public web servers of the requesting government agencies and provide feedback on the results to these government agencies. The obtained information will be shared among all government agencies, and the results publicized and reflected appropriately in the following year's priority inspection items, so as to raise the level of the countermeasures adopted by all government agencies.

(c) Implementation of Education and Training on Targeted Attacks (Cabinet Secretariat and concerned government agencies)

[Repetition: Refer to 1 B (c)]

(d) Reinforcement of Business Continuity Capabilities in Government Agencies (Cabinet Secretariat and all government agencies)

a) In contributing to the maintenance, improvement and running of the operational continuity plan for the information systems of the respective government agencies, the Cabinet Secretariat will make improvements to the Guidelines for Operation Continuity Planning of Central

Government Computer Systems (Devised in March, 2011) including building robust information systems such as back up systems, while taking into consideration the experiences of the Great East Japan Earthquake.

Support will also be provided such as the review of countermeasure requirements to ensure the operational continuity of information systems in the event of a large-scale disaster and the provision of necessary information.

b) The respective government agencies will review, as required, the operational continuity plan for the information systems of each government agency formulated in FY2011, while taking into consideration the business continuity plan and utilizing the Guidelines for Operation Continuity Planning of Central Government Computer Systems formulated by the Cabinet Secretariat, from the standpoint of ensuring the continuity of administration during the occurrence of a disaster or failure.

(e) Promotion of Guidelines on Risk Assessment and Digital Signatures/Authentication in Online Procedures (Cabinet Secretariat and all government agencies)

The respective 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 (CIO[25]) at government agencies on August 31, 2010) will ensure the overall appropriateness of the risk evaluation and assurance levels derived from these guidelines, and to this end will receive and decide upon advice taken from persons with expert knowledge at the Chief Information Security Advisors Liaison Conference and the CISCO Liaison Conference, and will report to the CIO Liaison Conference the status of the reflection in the plan of items concerning the optimization of business and systems.

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

The Cabinet Secretariat, in cooperation with the respective government agencies, will steadily implement multi-layered checks for the

[25] Abbreviation of Chief Information Officer.

implementation of measures, taking into consideration the criteria related to specially-controlled secrets based on the "Basic Policy concerning Reinforcement of Counterintelligence Functions."

(g) Promotion of Efforts to Reinforce Intelligence and Security Systems of Government Agencies Handling Highly-Confidential Information (Cabinet Secretariat and concerned government agencies)

Initiatives based on the "Measures considered as necessary concerning intelligence and security systems of government agencies handling particularly highly-confidential information" (Panel[26] on intelligence and security systems, July 1, 2011)

(h) 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 enhance the uniform educational programs for government employees (general staff, management, and personnel in charge of information security measures).

b) The Cabinet Secretariat will review educational programs for personnel to enable support by CSIRT personnel from other government agencies.

c) 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.

d) The Cabinet Secretariat is to further enhance the model for educational teaching materials in accordance with the roles in information security measures, and will also prepare educational materials that summarize the minimum requirements expected of government employees. The respective government agencies will then to provide information security education.

e) The respective government agencies will strive to raise awareness of the latest incidents and cases related to information security through the opportunity of the "e-Government Promotion Week" and the "Information Security Awareness Month," etc.

---

[26] Council held under the "Study Committee on Information Preservation in the Government" (Committee Head: Cabinet Secretariat)

(i) 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 will encourage the adoption of sender domain authentication technology, to stop malicious third parties from impersonating government agencies or their staff and thus causing harm to the general public and private sector, and will also propose the further promotion of receiver-side measures and widely informing the public of such threats. In addition, the introduction of measures using cryptographic technology such as DKIM[27] and S/MIME[28] will also be positively considered.

b) The Ministry of Internal Affairs and Communications will work in partnership with the "Anti-Spam Consultation Center" established with the wide participation of those involved in spam e-mail countermeasures and the non-governmental organization, the "Japan Email Anti-Abuse Group (JEAG[29])," centered on the main domestic Internet connection service providers and mobile operators, and promote the adoption of sender domain authentication technology (Sender Policy Framework, SPF[30], and DKIM, etc.) on both the sending side and receiving side.

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

a) Regarding the domain names used when government agencies send information to the public, the Cabinet Secretariat and Ministry of Internal Affairs and Communications will, in principle, promote to the respective government agencies the use of domain names guaranteed to be those of government agencies (".go.jp" domain names among the generic JP domain names), and the status of these initiatives will also be widely announced to the public.

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

---

[27] Abbreviation of Domain Keys Identified Mail.
[28] Abbreviation of Secure / Multipurpose Internet Mail Extensions.
[29] Abbreviation of Japan Email Anti-Abuse Group.
[30] Abbreviation of Sender Policy Framework.

(k) Promotion of the Use of Digital Signatures Utilizing Government Public Key Infrastructure (Cabinet Secretariat and all government agencies)

The Cabinet Secretariat will promote initiatives to ensure the legitimacy and security and of electronic files on public websites in government agencies, through the use of digital signatures utilizing government public key infrastructure (GPKI[31]).

(l) Review of Information Security Measures Concerning the Release and Secondary Use of Administrative Information Related to Disasters (Cabinet Secretariat and concerned government agencies)

Ensuring information security measures will be reviewed on the promotion of initiatives to widely release and also enable secondary use by the public of administrative information related to the disaster, evacuation, daily life and so on, during the occurrence of a disaster.

E Promotion of Secure Encryption Usage in Government Agencies

(a) 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)

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 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 revise the "e-Government Recommended Ciphers List", based on the latest findings related to cryptographic technology.

c) The Ministry of Internal Affairs and Communications and the Ministry of Economy Trade and Industry will, as required, provide information obtained by monitoring the e-Government Recommended Ciphers to the Cabinet Secretariat. Further, the Cabinet Secretariat will promote initiatives in accordance with the "Migration Plan of Cryptographic Algorithm SHA-1 and RSA1024 in the Information Systems of Government

[31] Abbreviation of Government Public Key Infrastructure.

Agencies[32]", such as promptly providing necessary information to the respective government agencies.

d) Referring to discussions made at the Cryptography Research and Evaluation Committees, the Cabinet Secretariat and respective government agencies will review the requirements for starting emergency measures (contingency plan) in the event of a sudden decline in security, and will decide on these requirements at the CISCO Liaison Conference.

e) The respective government agencies will continue with the steady adaption and migration of their own information systems to safer cryptographic algorithms, in accordance with the Migration Plan.

f) The Cabinet Secretariat will grasp the situation in the respective government agencies on conformity to the Migration Plan, and encourage 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 highly secure cryptographic module, hereafter, in addition to promoting the IPA-run cryptographic module validation program, at the time of procuring a cryptographic module, products certified by the program will be given priority as required.

F Ensuring Information Security in Line with Changes in the ICT User Environment

(a) Reinforcement of cloud computing information security measures in the central government (Cabinet Secretariat and Ministry of Internal Affairs and Communications)

Taking into consideration the information security assurance policy, the Ministry of Internal Affairs and Communications will start to design, build and operate a "common government platform" that is compatible with IPv6 and utilizes cloud computing technology. Further, the Cabinet Secretariat will provide support, such as providing the expertise accumulated through

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

revision of the Standards for Measures, and from other related measures.

(b) Preparation of a system for the operation and management of key information systems for common usage in multiple government agencies (Cabinet Secretariat and Ministry of Internal Affairs and Communications)

The Cabinet Secretariat and Ministry of Internal Affairs and Communications will prepare and review the necessary items for the appropriate operation and management of a "common government platform", which is one of the key information systems for common usage in multiple government agencies, such as the division of responsibility and roles, system for cooperation and partnerships during normal times and emergencies, and specific measures during emergencies in the respective government agencies.

(c) Preparation of a Government Information System Management Database (Cabinet Secretariat and Ministry of Internal Affairs and Communications)

In order to have a grasp of the information systems of the respective government agencies, the information asset register will be made into a database, and a government information system management database will be prepared and managed for use in detecting vulnerability and assessing risks throughout the entire government.

(d) Reinforcement of Information Security Measures for Smart Phones in the Central Government (Cabinet Secretariat)

The Cabinet Secretariat will review measures for ensuring information security during the business use of smart phones in government agencies

G 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)

To ensure the appropriate and smooth operation of the new framework for the Standards for Measures, the Cabinet Secretariat will examine the direction of information security management methods, based on the latest threats, etc.

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

The Cabinet Secretariat will conduct an appropriate review of the Standards for Measures, taking into consideration new technology and environmental changes, such as the emergence of threats of targeted attacks and the spread of smart phones and cloud computing technology.

(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 will strengthen cooperation with the incorporated administrative agencies related to information security measures, and reflect this in the Standards for Measures policy, by accumulating and utilizing the knowledge of researchers and practitioners involved in information security on the basis of a memorandum on cooperation with the incorporated administrative agencies, the National Institute of Information and Communications Technology (NICT), the National Institute of Advanced Industrial Science and Technology (AIST[33]) and the Information-Technology Promotion Agency (IPA).

(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, the respective government agencies will use products certified by the "IT Security Evaluation and Certification Scheme"[34] in order to build highly secure and reliable information systems, while referring to the "List of Products in Evaluation based on the IT Security Evaluation and Certification Scheme" (Ministry of Economy, Trade and Industry, on April 21, 2011) and on the basis of the Standards for Measures.

b) The Ministry of Economy, Trade and Industry will consider promoting

[33] Abbreviation of National Institute of Advanced Industrial Science and Technology.

[34] 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.

the use of products certified by the IPA-run IT Security Evaluation and Certification Scheme, so that the respective government agencies can effectively and efficiently procure IT systems taking into account information security, and will facilitate their use in government agencies such as through reviewing the List.

H Building Mechanisms for Appropriately Incorporating Information Security Measures into Government Agency Information Systems

(a) Enhancement of Information Security Measures for Information Systems Entrusted with Operation and Management (All government agencies)

The respective government agencies will promote initiatives to ensure information security in regards to the information systems of organizations outside government agencies that have been entrusted with operation and management, such as by using cloud computing while taking into consideration the Standards for Measures and the separate manuals, etc.

(b) Promotion of Information Security Measures for Companies and Organizations Handling Important National Information (Cabinet Secretariat and all government agencies)

[Repetition: Refer to 1 B (b)]

(c) Examination of Measures for Appropriately Incorporating Information Security Measures into Government Agency Information Systems at the Planning and Design Stage (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and all government agencies)

a) So as to ensure the necessary security measures within the overall system budget, the respective government agencies will assume their requirements in advance as far as possible, and utilize the "Security Requirement Formulation Manual in Government Procurement for Information Systems" to clearly list all the required security measures in preparing the respective procurement specifications of information systems, and to this end disseminate and educate information within the respective government agencies.

b) So as to bring the Security Requirement Formulation Manual in Government Procurement for Information Systems into wide use as a part of the government procurement of information systems, the Cabinet Secretariat

will actively strive to make the manual simpler and easier to use with more sophisticated content, and also promote the distribution and use of the manual in the respective government agencies. Support will also be provided, such as checking how the manual is used with actual procurement specifications, responding to inquiries from users about actually using the manual, and providing assistance in operations.

c) The respective government agencies will implement measures that are 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.

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

Targeting all information systems, in order to improve the reliability of all information systems from the comprehensive perspective of process management aspects including development and operations, technological aspects, organizational aspects, and so on, 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 enables visualization of the status of compliance with the guidelines, together with the "Reliability Self-Diagnosis Tool" based on the evaluation index, will be facilitated in private sector corporations and government agencies.

(e) Support for Ensuring Information Security During the Procurement of Information Systems (Ministry of Economy, Trade and Industry)

a) In addition to promoting the operations of the "IT Security Assessment and Certification Scheme," expanding utilization of the scheme to include information system procurement will be planned.

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

c) Regarding the security functions of products subject to assessment and certification in the "IT Security Assessment and Certification Scheme," preparation of a protection profile for each product will be considered.

I Study of Information Security Measures for the Social Insurance and Taxation Number System

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

In regards to the social insurance and taxation numbering system and national ID system, in order to provide assurance and convenience to the public, a study will be promoted for specifying security measures giving consideration to the appropriate protection of personal information and information security.

J Promotion of Information Security Measures in Local Governments and Incorporated Administrative Agencies, etc.

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

a) In order to help local government employees understand the importance of business continuity and acquire the basics and necessity of BCP [35] formulation in the ICT departments of local governments, BCP formulation seminars will be held and advisors introduced. Information security audit seminars will also be held to promote information security auditing.

b) The operation of a portal site in the Local Government Wide Area Network (LGWAN), which will feature commentary and the like on information security, will be supported and its utilization further promoted in an effort to enhance the compilation of examples of information security initiatives and the collection and analysis of data on information security incidents.

c) Support will be provided to interested local governments to assist in strengthening their security measures, including a vulnerability diagnosis of the OS, middleware applications, and web applications of public servers, such as Web servers, as well as assessing the vulnerability of firewalls, routers and other network devices, and also giving advice on appropriate countermeasures.

d) For those interested local governments, checks will be conducted for types of

[35] Abbreviation of Business Continuity Plan.

malware, such as Gumblar, that transmit a virus just by simply having browsed a web page. In the case of such malware being detected, advice on countermeasures will be provided to support an early 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 that appear to have been sent from local governments and which cause harm to the general public or private sector.

(b) Promotion of Initiatives Concerning Information Security in Education-Related Departments of Local Governments (Ministry of Education, Culture, Sports, Science and Technology)

To ensure information security in education-related departments, the following initiatives will be carried out.

a) Promotion of the dissemination and education of information security initiatives

b) Provide training for supervisors and other staff who will play a key role in promoting information and education at each local community, so as to facilitate initiatives for raising the ability to lead others in the use of information security and other ICT in local governments.

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

Support will 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) Requests will be made and necessary support provided for the development and review of information security policy for incorporated administrative agencies, taking into consideration the series of measures in government agencies, including the Standards for Measures.

b) In accordance with the status of the implementation of countermeasures and the business characteristics of incorporated administrative agencies, in addition to fostering initiatives for building PDCA cycles related to their own

information security measures, a clear statement of items related to information security measures will be promoted as a midterm target.

c) The adoption of sender domain authentication technologies, such as SPF and DKIM, in the sending side and receiving side will be promoted, so as to prevent malicious third parties from impersonating local governments or their staff in e-mails that appear to have been sent from local governments and which cause harm to 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)

A system for contacting incorporated administrative agencies, including during an emergency, will be prepared and its effectiveness confirmed within FY2012.

(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 will be actively promoted by using the Chief Information Security Advisors Liaison Conference and other such forums.

K Enhancement of the National Information Security Center (NISC) functions

(a) Strengthening of the NISC (Cabinet Secretariat)

Outstanding human resources from both the public and private sector will be actively employed, so as to form the core of the system for promoting information security measures throughout the entire government.

Under this system, the information sharing and analysis functions with relevant institutions will be strengthened and the collection of information enhanced. In addition, the functions for investigating and examining the required basic information and various trends in the cross-sectional promotion of information security measures will be expanded.

(b) Enhancement of Information Security Consulting Functions for the Promotion of Information Security Measures in the Respective Government Agencies (Cabinet Secretariat)

So as to provide support and meet the various needs in the promotion of information security measures in the respective government agencies, the NISC will enhance the information security consulting functions provided by the experts in the Center, such as receiving consultations concerning the Standards for Measures and offering technical advice during emergencies.

(c) Strengthening of Alliances with Relevant Institutions (Cabinet Secretariat and the Cabinet Office)

Information Security Policy Council and NSIC will closely cooperate with the IT Strategic Headquarters and also the relevant centers and councils such as the Council for National 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 through close cooperation in proposing and implementing the various policies.

4 Consolidation of Critical Infrastructure

Taking into consideration the lessons learnt from the multitude of damage incurred in critical infrastructure fields in the Great East Japan Earthquake, to enable the full anticipation of risks in information security in the Business Continuity Plan (BCP), the contents of the "Guidelines for the formulation of 'Safety Standards, etc.' on ensuring information security in critical infrastructure (3rd edition)" (hereinafter, "the Guidelines") will be enriched. Also, when analyzing and evaluating the Safety Standards, etc., attention will be given to analyzing and verifying if these Standards are in accordance with the latest environmental changes, such as targeted attacks and attacks on control systems, etc.

Also, in order to strengthen the cross-sectional information and analysis system in critical infrastructure fields, the activities of CEPTOAR[36] will be further promoted, in particular facilitation of the mutually beneficial sharing of information between businesses as well. Further, through the analysis of threats that are common to critical infrastructure fields and the implementation of cross-sectoral exercises, protection measures for critical infrastructure will be enhanced and international alliances in critical infrastructure fields will be promoted.

In addition, on the basis of the "Second Action Plan on information security measures for critical infrastructure (hereinafter, "the Second Action Plan") revised in April 2012, measures will be promoted such as the preparation and penetration of the Safety Standards, etc., and reinforcement of the information sharing system.

A Preparation and Penetration of the Safety Standards, etc.,

(a) Continual improvements of the Guidelines and the Safety Standards in critical

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

infrastructure fields (Cabinet Secretariat and government agencies in charge of critical infrastructure)

a) The Cabinet Secretariat will cooperate with relevant institutions and consider the current state of information security measures for ensuring the effectiveness of the business continuity plans of critical infrastructure operators. At that time, the disaster measures and business continuity plan guidelines under consideration at the relevant institutions will be made consistent.

In FY2012, using a field survey of the impact of the Great East Japan Earthquake on the operation of critical infrastructure information systems and its spillover effect on critical infrastructure services, based on the issues selected for incorporating into the BCP of critical infrastructure from the perspective of its stable operation, the current state of measures will be compiled.

b) So as to respond to changes in social trends and enable the timely reflection of new knowledge, the Cabinet Secretariat will analyze and examine the "Guidelines for the formulation of 'Safety Standards, etc.' on ensuring information security in critical infrastructure (3rd edition)" and the compiled measures of the Guidelines, and consider a supplement edition to the Guidelines as required.

c) Taking into consideration the Guidelines and the characteristics of each critical infrastructure field, the government agencies in charge of critical infrastructure will analyze and verify the 'Safety Standards, etc.' in each critical infrastructure field around the end of FY2012. Also, measures for the revision of the 'Safety Standards, etc.' will be implemented as required.

(b) Status Survey on the Preparation and Penetration of the 'Safety Standards, etc.'
(Cabinet Secretariat and government agencies in charge of critical infrastructure)

With the cooperation of the government agencies in charge of critical infrastructure, the state of the preparation and penetration of the 'Safety Standards, etc.' will be surveyed as follows.

{Survey in critical infrastructure fields}

In FY2012, the status of analysis, verification and revision of the 'Safety Standards, etc.', improvements based on the earthquake, attack trends, response to environmental changes such as those of information systems, and the implementation schedule going forward will be assessed and verified, and the results published.

{Survey on critical infrastructure operators}

In FY2012, the status of penetration of the 'Safety Standards, etc.', and

survey on improvements based on the earthquake will be implemented, and the results publicized. Planning and preparation for the next fiscal year's survey will also be carried out.

(c) Ensuring the Safety and Reliability of Electronic Communications Systems (Ministry of Internal Affairs and Communications)

In accordance with progression in the IP of networks, to ensure the even more stable provision of ICT services, the content of reports from electronic communications providers at the occurrence of an accident and on the situation of the accident will be analyzed and evaluated, and the results regularly publicized.

Also, taking into consideration the expansion in data traffic in mobile phone networks and large-scale disasters, the "Standards for the safety and reliability of information communications networks" will be reviewed.

B Reinforcement of the Information Sharing System

(a) Support for CEPTOAR Activities (Cabinet Secretariat)

In order to facilitate the even smoother operation of CEPTOAR Council, which are formed by each critical infrastructure field and act as a point of cooperation through the promotion of field cross-sectional information sharing, support will be provided for CEPTOAR Council activities that contribute to promoting the sharing of valuable information for critical infrastructure operators among themselves and improving the maintenance and recovery capabilities of critical infrastructure services.

(b) Preparation of information for Sharing (Cabinet Secretariat)

a) The information for sharing will be prepared and enriched based on the information sharing framework and while taking into consideration threats in information security and changes in social trends.

b) The preparation results will be compiled within FY2012, including a review of useful information sharing methods for critical infrastructure operators, and while also taking into consideration the earthquake response-related issues.

(c) Promotion of Information Sharing Based on the Implementation Details Relating to Information Liaison and Provision of the "Second Action Plan" (Cabinet Secretariat)

a) So as to facilitate the easier maintenance and recovery of the services of critical infrastructure operators, from the perspective of the importance of cooperation between each public and private sector entity, information sharing will be promoted by the Implementation Details relating to information liaison and provision of the "Second Action Plan" under the information sharing system based on the "Second Action Plan".

b) From the perspective of the continual improvement of information sharing, the Implementation Details will be reviewed at the end of FY2012 and necessary revisions made, based on the progress status of the "preparation of information for sharing" and operation status of information sharing by the implementation details.

(d) Improvement to Rules Concerning Information Sharing Based on the Implementation Details (government agencies in charge of critical infrastructure)

a) In the information sharing raised in the abovementioned (b), the information sharing rules concerning information provision from government agencies in charge of critical infrastructure to CEPTOAR, and the information sharing rules concerning information liaison from critical infrastructure operators to government agencies in charge of critical infrastructure, will each maintain consistency with the implementation details, and these information sharing rules will be revised as required.

b) Regarding the information sharing rules within CEPTOAR on information provision, so that maintaining consistency with the implementation details is to be carried out by CEPTOAR, advice and other support will be provided to CEPTOAR along with confirmation of its response situation.

(e) 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, information on the functions and the state of activities of each CEPTOAR will be compiled and published by the end FY2012, with the cooperation of the government agencies in charge of critical infrastructures.

b) With the cooperation of the government agencies in charge of critical infrastructures, opportunities will be provided for confirming the information communication functions in order to maintain and improve the information sharing system of the CEPTOARs in each field.

(f) Reinforcement of Public Affairs (Cabinet Secretariat)

So as 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, websites on information security measures and the like will be used for the reinforcement of public affairs. Also, the action plan and related policies will be actively publicized by making use of opportunities such as seminars or lectures.

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

With 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 foster a common awareness on the cooperative required risk countermeasures, as well as to enable a close collaboration and smooth response between the relevant entities, mutual risk communications will be promoted between critical infrastructure operators, relevant institutions and the government agencies in charge of critical infrastructures. During this promotion, cooperation with the CEPTOAR Council will be pursued, aiming at mutually beneficial activities for the public and private sectors.

(h) Implementation of Education Seminar for Critical Infrastructure Operators (Ministry of Economy, Trade and Industry)

Forums related to the information security of critical infrastructure systems and the like are to be held with the cooperation of the IPA and relevant organizations.

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

[Repetition: Refer to 3 H (d)]

C Enhancement of Critical Infrastructure Protection Measures

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

As for new threats that may commonly occur in critical infrastructure fields, while focusing on changes in the technological environment of systems, specific targets for analysis will be selected and a detailed analysis will be done, taking into consideration domestic and overseas research trends and

other factors.

In FY2012, as an information security measure for simultaneous and multiple damage to critical infrastructure as was seen in the Great East Japan Earthquake, review and sophistication of mutual interdependence taking into account changes in the technological and social environments will be examined.

When implementing the analysis, those results will be shared among the relevant parties with the cooperation of CEPTOAR, critical infrastructure operators and government agencies in charge of critical infrastructures.

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

With the cooperation of CEPTOARs and critical infrastructure operators, exercise scenarios anticipating the occurrence of a specific IT fault and related cross-sectoral exercises will be implemented, cross-sectoral, and issues to assist in revising the BCPs of the operators will be selected.

In FY2012, in addition to implementing effective exercises by examining the way of giving advice in the creation of even more practical scenarios and implementation of exercises, initiatives will be promoted to further activate information sharing by stimulating the exchange of opinions following the exercises, and for sharing and promoting the exercise results as well as expanding the exercise participants.

The obtained results will be shared among the relevant parties, and published as far as possible.

(c) Cyber Exercises in Individual Fields (Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry

a) Cyber exercises will be conducted, consisting of the implementation of mock cyber attacks targeting critical infrastructure fields (communications, electricity, gas, etc.)

b) In addition to enabling the security evaluation of control systems and accumulation of knowledge on security measures, these cyber exercises can also provide hints on security measures of control systems in Japan.

(d) Preparation of a Support System for Improving the Reliability and

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

a) So as to support the voluntary efforts by critical infrastructure operators to improve the reliability of information systems, the maintenance and sharing of a fault-case database, quantitative macroanalysis of the information voluntarily offered, and provision of accumulated information to CEPTOARs will be carried out.

b) Regarding the international standards currently being formulated on security in control systems, the items requested by Japan will be jointly written. Also, international cooperation on the evaluation and authentication of security in control systems will be facilitated, work on the translation of existing standards will commence, and consideration will be given for enabling the easier authentication of domestic products.

(e) Cyber Attack (incident) Response Coordination and Support (Ministry of Economy, Trade and Industry)

[Repetition: Refer to 1(C) c)]

(f) Enhancement of Measures for Interference in Critical Radio Communications (Ministry of Internal Affairs and Communications)

a) In order to strengthen the response to an incident of interference in critical radio communications, the outside-business hours centralized reception service for incident reports on critical radio communication interference will be continuously implemented, and the outside-business hours swift response system for such incidents will be reinforced.

b) So as to maintain radio wave usage discipline, the performance of remotely-operated radio wave monitoring facilities will improved, and sensors of the same facilities will be renewed in FY2012.

c) Investigative research on radio wave monitoring technologies will be carried out while taking into consideration recent changes in the radio usage environment, such as the sophistication and higher functionality of radio wave monitoring facilities.

D Response to Information Security Issues Concerning Control Systems

(a) Formulation of Information Security Standards for Control Systems and Establishment of an Evaluation and Authentication System (Ministry of Economy, Trade and Industry)

Setting the Tohoku region as the principal implementation site, in FY2012 cyber security verification facility for control systems will be built with the cooperation of the U.S.

Also, in this verification facility, research will be carried out on evaluation and authentication methods, and international standardization to help strengthen competitiveness will be facilitated. Accordingly, initiatives will be promoted towards realizing international mutual recognition between evaluation and authentication institutions.

(b) Establishment of Cooperative Framework for Responding to Vulnerabilities and Incidents Concerning Control Systems (Ministry of Economy, Trade and Industry)

Working together with the associated organizations of control systems, countermeasures for threats, such as vulnerabilities and incidents concerning control systems, will be smoothly carried out through the collection, sharing, and release of information useful in promoting the security countermeasures of control systems.

a) Support for preferential provision of vulnerability information of software and control systems for critical infrastructure operators and security information management (Ministry of Economy, Trade and Industry) A review will be conducted on the requirements of vulnerability handling systems that enable relevant parties of control systems to carry out planned responses and safety countermeasures, in order to minimize the risks and costs resulting from vulnerabilities found following the distribution of control-system software products and the operation of systems.

b) JPCERT/CC will provide CEPTOARs or critical infrastructure operators with information on information security-related threats that may require critical infrastructure operators to take action against and corresponding countermeasures, as early warning information based on a previous agreement.

c) Efforts will continue to be made for releasing user-friendly information on software-related and other such vulnerabilities.

E Promotion of International Alliances in Critical Infrastructure Fields

(a) Promotion of International Alliances in Critical Infrastructure Fields
(Cabinet Secretariat, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

a) International alliances in critical infrastructure fields will be promoted, such as by positively participating in the activities of Meridian[37], which aims at facilitating international information sharing and collaboration for the protection of critical infrastructures.

b) So as to facilitate improvements in Japan's information security countermeasures, information will be released to relevant domestic entities on data concerning IT fault cases and best practices obtained through the collection of information from abroad and international alliances.

[37] International meeting on critical infrastructure.

5 Response to the Diversification and Sophistication of ICT

(1) Ensuring Security in the Rapidly Growing Spread of New Services

Measures will be taken to ensure information security in the rapidly growing spread of new services such as smart phones, cloud computing, IPv6 and SNS, through various initiatives including standardization and investigative research, while giving consideration to the impact on the socioeconomic activities that are dependant on these services.

A Measures to Ensure Information Security of Smart Phones, etc.

(a) Promotion for Ensuring Information Security of Smart Phones through Public-Private Sector and International Alliances (Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

a) With the cooperation of the public-private sector, technical issues and other factors will be considered and necessary countermeasures taken regarding the problems in information security accompanying the spread of smart phones, etc.

b) Information will continue to be actively exchanged in forums such as international conferences and bilateral meetings, in order to form international alliances and grasp specific threats and issues as well as consider countermeasures.

c) Dissemination and education initiatives for users, countermeasures from the service operation aspect and technical measures in the government and business operators will be regularly compiled, and the information released.

(b) Reinforcement of Information Security Measures for Smart Phones in the Central Government

[Repetition: Refer to 3 F (d)]

(c) Promoting the Use of Safe and Secure Wireless LAN via Smart Phones, etc. (Ministry of Internal Affairs and Communications)

So as to respond to the rapid rise in mobile traffic resulting from the spread of smart phones, etc., while ensuring appropriate information

security by users, measures for wireless LAN offloading will be examined and the efficient use of mobile wavelengths facilitated.

(d) Examination of Filtering Methods in Smart Phones, etc. (Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

The way of filtering methods in smart phones and other devices will be examined.

(e) Promotion of the Dissemination and Education of Information Security Measures for Smart Phones, etc. (Cabinet Secretariat, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

Taking into consideration the rapid spread of smart phones and other devices, the comprehensive dissemination and education for users on information security measures for smart phones, etc., will be promoted.

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

So as to raise knowledge and awareness on information security, exercises and other initiatives will be implemented nationwide for the related staff of educational institutions, local government employees and general users of the Internet, with a range of content including the current state of cyber crimes and cases of arrest, and familiar threats such as crimes of malicious use of smart phones and other information terminals and SNS and other latest ICT.

(g) Analysis of New Threats and Attacks (Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

Computer viruses and other malicious code targeting smart phones will be acquired and analyzed, and used in various initiatives such as R&D, the examination of countermeasures, and the release of information

(h) Response to Cyber Crimes Targeting Smart Phones Users, etc. (National Police Agency)

The policing of cyber crimes targeting smart phones users, etc. will be strengthened and efforts made for the centralization of information through reinforcing alliances with information security operators. Also, taking into consideration the actual state of such crimes clarified through policing, the release of information for enhancing information security

measures for general users will be promoted.

B Measures to Ensure the Information Security of Cloud Computing

(a) Promotion of Information Security for Cloud Computing as a Social Foundation (Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

Security-related issues on cloud computing, which is starting to be used as a social foundation, will be studied and necessary countermeasures taken.

(b) Reinforcement of Cloud Computing Information Security Measures in the Central Government (Cabinet Secretariat and Ministry of Internal Affairs and Communications)

[Repetition: Refer to 3 F (a)]

(c) Preparation of a System for the Operation and Management of Key Information Systems for Common Usage in Multiple Government Agencies (Cabinet Secretariat and Ministry of Internal Affairs and Communications)

[Repetition: Refer to 3 F (b)]

(d) Dissemination and Promotion of a Check List for the 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 the assurance criteria of service contents, scope and quality, etc. (e.g.: service availability ratio, reliability level, data management method, security level, etc.) between the cloud provider and the cloud user will be encouraged so as not to overburden the service-providing side. Also, a checklist for service level of cloud computing will be disseminated and promoted.

(e) 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 and improving reliability to ensure secure and stable operations, so that 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 the business settings of enterprises and government agencies. The preparation of an environment for an audit framework will also be considered.

In FY2012, development will be carried out on technologies for improving reliability, compatibility, energy efficiency, and other factors in cloud computing.

(f) R&D for Building a Cloud Computing Foundation Adaptable to Widespread Disasters (Ministry of Internal Affairs and Communications)

R&D will be promoted towards building a cooperative base between highly reliable clouds capable of large-scale energy conserving and which can ensure the swift evacuation of critical data from clouds in disaster areas to safe clouds in remote areas and continuation of business during widespread disasters.

(g) R&D on Security Technology for Cloud Computing Data Transfer and Facilitation in Providing for a Disaster (Ministry of Internal Affairs and Communications)

While cloud computing is useful for storing information to enable the continuation of business and other work processes during a disaster, it has also been pointed out as not having clearly defined storage places and processing methods for data and for its information security issues such as information leakages. In light of this, R&D will be carried out on technology to prevent information leakages so as to facilitate the spread of cloud computing.

(h) Initiatives for the International Standardization of Cloud Computing (Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

Japan will participate in international meetings hosted under ISO/IEC JTC1/SC27, ITU-T SG17 etc., which are international standardization activities in the information security field, and will actively participate in the planning so that Japan's R&D findings, IT environment, standards, guidelines and other factors are taken into consideration and reflected in international standards.

C Ensuring IPv6-Related and SNS-Related Information Security

(a) Promotion of Measures for Addressing the Other Issues Associated with IPv4 Address Depletion (Ministry of Internal Affairs and Communications)

In the sharing environment for IPv4 addresses that is expected to be introduced due to IPv4 address depletion, so as to ensure a sufficiently secure and reliable communication, technical issues concerning information security will be studied and the necessary countermeasures promoted.

(b) Building of an Information Security Verification Environment for IPv6 Networks (Ministry of Internal Affairs and Communications)

Specific security issues, such as the threats and vulnerabilities accompanying the migration to IPv6, will be extracted, and using the existing verification environment, the required information security measures will be considered after assessing the level of importance of these issues.

In FY2012, taking into consideration the results of the FY2011 verification environment evaluation test, information security measures for IPv6 networks will be systematically examined, and effective evaluations using the verification environment will be carried out by the NICT.

(c) Lending of Vulnerability Verification Tools in the IPv6 Environment (Ministry of Internal Affairs and Communications)

Dissemination and education activities will be continually carried out so as to facilitate the use of known TCP/IP vulnerability verification tools that can verify 14 types of vulnerabilities in the IPv6 environment.

(d) Information Security Measures for SNS Usage(Cabinet Secretariat, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

In light of the increasing number of attacks targeting SNS that have followed its expanding use in recent years, the Cabinet Secretariat, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry will give consideration to ensuring information security for SNS usage, and make widely known important points to keep in mind as required.

(e) Promotion of Information Security for Wireless LAN (Ministry of Internal Affairs and Communications)

a) Taking into consideration the increase in the number of wireless LAN users, expanding user groups and changes in the usage format due to the rapid spread of smart phones and other devices, the "For the secure use of wireless LAN" (December 2007, Ministry of Internal Affairs and Communications), which are guidelines for wireless LAN users, will be revised. Also, appropriate information security measures for wireless LAN will be provided to users, and efforts made for the dissemination and education of these measures.

b) In light of the progressive introduction of wireless LAN also in companies and other organizations, related guidelines will be formulated which will describe the items for consideration (operation management, procurement, technology) when introducing and operating wireless LAN in companies and other organizations.

(f) Examination of Information Security Measures for Multi-Function Printers (Ministry of Economy, Trade and Industry)

Information security issues and countermeasures for multi-function printers will be given immediate consideration, as their usage continues to expand.

(2) Modality of Information Security in M2M

Appropriate information security measures will be examined and R&D promoted on smart grids and other M2M, which are expected to be in full-fledged widespread use from hereon.

(a) Examination of the Way of Information Security in M2M and Ppromotion of R&D (Cabinet Secretariat, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

Taking into consideration that any loss of information confidentiality and completeness in M2M may bring about not only confusion in society but also damage it's trust in the ICT base, the way of information security in M2M will be examined, and R&D also from the perspective of ensuring information security will be promoted.

(b) Examination of the Way of Information Security in Smart Grids (Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

So as to ensuring information security in smart grids and other M2M, the issue will be examined through seminars and other such forums.

(c) R&D for Ensuring Information Security in Smart Grids (Ministry of Economy, Trade and Industry)

R&D will be carried out also from the perspective of ensuring information security in smart grids and other M2M.

(d) R&D on Information Security Technology in Resource-Conserving Devices (Ministry of Internal Affairs and Communications)

When collecting data using sensors and smart meters, etc., ensuring the information security and protecting the privacy of this data are serious issues. As such, R&D will be carried out on lightweight cryptographic technology that can be installed in such resource-conserving devices and authentication/privacy protection technology in large-scale nodes.

(3) Other Responses to the Sophistication and Diversification of Threats

In order to adequately respond to the sophistication and diversification of threats, in addition to maintaining and improving response capabilities for information security incidents and tackling countermeasures for software vulnerabilities, efforts will be made for preparing an environment to promote initiatives on information security measures for small and medium-sized enterprises, and facilitating secure e-commerce.

A Reinforcement of Response to Information Security Incidents

(a) Promotion of Initiatives for Stopping Cyber Attacks (Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

Regarding measures to prevent infection by computer programs (bot programs) that carry out cyber attacks through remote operations by malicious third parties and the countermeasures to swiftly and effectively prevent the sending of spam e-mail or cyber attacks from computers infected by bot programs, ongoing initiatives will be implemented by the relevant organizations, using the framework built by FY2010 as a base. Also, measures will be considered to enable the participation of Internet service providers (ISP) in the planning of these information security measures for users.

In addition, necessary information on Japan's initiatives will be exchanged with relevant overseas organizations.

(b) Promotion of Efforts toward Cyber-Attack Prevention and Early Countermeasures (Ministry of Internal Affairs and Communications)

a) So as to reduce the risk of cyber attacks in Japan and combat cyber attacks (malware infection, distributed denial-of-service attacks, etc.) that have been causing increasing damage in recent years, an international network for the collection of information on cyber-attacks and malware, etc., will be built, with the cooperation of domestic and overseas ISPs, universities and other organizations. Also, in collaboration with other countries, R&D and substantiative experiments will be conducted on technology to enable the prediction of and immediate response to cyber attacks occurring.

b) At the FY2011 Japan-U.S. Policy Cooperation and Dialogue on the Internet economy,

an agreement was reached with the U.S. to share data on cyber attacks and accelerate the cooperative relationship in R&D fields. Taking this into account, in order to effectively implement R&D on technology to enable the prediction of and immediate response to cyber attacks occurring, concrete talks between Japan and the U.S. will proceed in FY2012.

c) The Japan-EU Internet Security Forum will be held in FY2012, in which discussion will proceed on issues such as carrying out efforts with the EU towards collaborative research for reducing cyber attacks on the network.

d) Alliances with other ASEAN countries will be promoted, using as a foothold the sharing of observation data with Indonesia on cyber attacks that have already been launched.

(c) Promotion of Efforts toward the Avoidance of Harmful Sites (Ministry of Internal Affairs and Communications)

The results of the substantiative experiments carried out until FY2011 will be applied to the mechanisms for users to avoid accessing harmful sites that distribute malware, which will developed with the collaboration of telecommunication providers.

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

a) In order to ensure prompt information sharing of and smooth response to computer viruses, unauthorized access and vulnerabilities among relevant parties, IPA and JPCERT/CC will enhance the “computer security early warning system” in a format that is capable of responding to changes in threats. Specifically, in order to respond to computer viruses and other attack methods that have become increasingly clever in recent years, JPCERT/CC and other organizations that carry out coordination and support for incident responses will promote even more sophisticated analytical capabilities for attack methods, and information sharing and collaboration on analysis methods and incident cases among experts.

b) Regarding the malware samples analyzed in the incident response support activities of JPCERT/CC and the analysis results, consideration will be given to effective utilization methods such as appropriate mutual sharing with domestic and overseas relevant institutions having similar information and linkage with the operations of the Internet fixed-point observation information sharing system (TSUBAME).

c) In FY2012, a response coordination and support system specifically for incidents concerning control systems will be prepared, along with response methods for clever and

persistent targeted attacks.

d) Regarding efforts toward carrying out requests made through the Council of Anti-Phishing Japan and JPCERT/CC for shutting down phishing sites and other measures, consideration will be given to review of the requirements based also on the revised Anti-Unauthorized Access Law.

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

Efforts will be made for the popularization of CSIRT and strengthening of cooperation 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 information such as materials on CSIRT structure and operations, attack-related information or threat information contributing to incident countermeasures and responses, and specific countermeasures information that includes the analysis of requirements.

(f) Consideration toward the Formulation of a Model Agreement and Standard Contract for SOC Operators (Cabinet Secretariat, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

Efforts will be made toward the formulation of a model agreement and standard contract to enable SOC operators to share information on threats that occur with other institutions.

(g) R&D on Information Security Technology for Ensuring a Secure and Reliable Network (Ministry of Internal Affairs and Communications)

With the aim of realizing a world where anyone can safely and securely naturally use IC networks that are supported by security technology which users are unaware of, R&D will be carried out on network security technology that sophisticatedly integrates theoretical and practical aspects, such as world-class leading technology for the observation, analysis, counteraction and prevention of cyber attacks, technology for the design, assessment and optimal construction of secure networks, and next-generation cryptographic base technology, etc.

In FY2012, the NICT will carry out basic development on the observation and analysis technology for drive-by-down load attacks, in

aiming to build a new security framework for combating these attacks.

(h) Initiatives for Information Leakage Countermeasures (Ministry of Economy, Trade and Industry)

a) So as to tackle countermeasures for information leakages including personal data, the general public will be provided with "Anti-information leakage tools" having various functions, such as preventing the leakage of information by file-sharing software.

b) Also, efforts will be made to collect information on new methods and techniques in information leakages, and necessary information such as on countermeasures, etc., will be provided to the general public.

(i) Consideration of the Prevention of Security Incidents Caused by Insider Misconduct (Ministry of Economy, Trade and Industry)

Consideration will be given to measures for the prevention of information security incidents used by insider attacks.

B Software Vulnerability Countermeasures

(a) Collection and Provision of Information on Vulnerabilities (Ministry of Economy, Trade and Industry)

Efforts will be made for not only the coordination and provision of information on vulnerabilities based on the receipt of usual notifications and other documents, but also to facilitate the active self-detection of vulnerabilities and cyber attacks to this end.

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

a) JPCERT/CC activities related to education activities on the importance of software vulnerability management and support for vulnerability management in user organizations will be boosted, such as by sending software vulnerability information in a format can be automatically incorporated into management tools.

b) The functions of "MyJVN" (vulnerability countermeasures support tool for information system users), which facilitates the steady roll out vulnerability information to users and server managers, and the database (JVN iPedia) coordinated to date by the relevant organizations will be expanded, so as to promote the even more reliable implementation of vulnerability countermeasures by information system users and

developers.

c) The cyber security reminder service 'icat' will be provided, which releases software vulnerability information on a timely basis.

(c) 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) Based on the METI Notice[38] , notifications of vulnerability information will be received and the receipt situation regularly announced, in addition to cooperating with relevant parties while promoting vulnerability countermeasures and providing vulnerability information to Website operators and software product developers.

b) In order to minimize the response cost and damage occurrence risk accompanying the vulnerabilities discovered in software products and information systems following product distribution or system operations, in addition to reviewing the existing framework of the system (vulnerability handling system) that enables prompt responses to software product vulnerabilities, initiatives will be continued by the JPCERT/CC for facilitating the disclosure and dissemination of points for consideration by product developers from the perspective 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.

c) Efforts will be made for facilitating the dispersion of coding standards to development sites concerning languages frequently used in embedded software that cannot easily be modified after distribution.

d) Developers will be provided with vulnerability verification tools for TCP/IP and SIP protocols used by developers of embedded devices and intelligent home appliances.

e) In order to support the self-learning of Website operators and product developers on the necessity of vulnerability countermeasures and countermeasure methods, efforts will be made for dissemination and education using as a set "How to Secure Your Website" and the hands-on and practical learning tool "AppGoat."

f) In light of the growth in services using vehicle-embedded software and the strengthening collaboration between external networks and vehicles resulting from the spread of smart phones and other devices, the latest security-related activities concerning vehicles and information security issues on electric vehicles will be studied, in working towards the dissemination of information security countermeasures for vehicles.

[38] Standards for handling software vulnerability information (Ministry of Economy, Trade and Industry Notice No. 235, July 7, 2004)

g) The dissemination and education of vulnerability detection technology for information system vulnerabilities will be facilitated through proactively detecting vulnerabilities.

(d) Establishment of a Common Evaluation Index for Assessing Reliability (Ministry of Economy, Trade and Industry)

In order to further promote quality control through quantitative data in system development projects, common tools will be established to enable the mutual use of quantitative data and the respective evaluation indexes formulated by relevant industrial organizations, and activities to facilitate their widespread use will be promoted.

(e) Reinforcement of the System LSI Security Evaluation and Authentication System (Ministry of Economy, Trade and Industry)

In FY2012, R&D will be steadily carried out for improving security evaluation and authentication technology based on domestic ISO/IEC15408, regarding LSI systems using IC cards, etc.

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

To assist in the early discovery of and response to vulnerabilities of web applications, the "Website Vulnerability Log Analytical Inspection Tool" (iLogScanner), which analyzes logs and inspects traces of external attacks, will be provided to corporate Website operators.

(g) Establishment of a Cooperation Framework for Responding to Vulnerabilities and Incidents of Control Systems (Ministry of Economy, Trade and Industry)

[Repetition: Refer to 4 D (b)]

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

[Repetition: Refer to 4 D (c)]

(i) Clarification of the Lawfulness of Reverse Engineering of Software for 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 taken to clarify the lawfulness of reverse engineering for information security purposes.

C Promotion of Secure Electronic Trading

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

Taking into account the study results of the "Study committee concerning enforcement of the Electronic Signatures and Authentication Law" held in FY2007, consideration will be given to measures for facilitating the use of electronic signatures in companies.

D Supporting Information Security Measures in Small-to-Middle Sized Businesses

(a) Promotion of Information Security Measures in Small-and-Medium Enterprises (Ministry of Economy, Trade and Industry)

a) The "Information Security Leadership Nurturing Seminars for Small-To-Middle Sized Businesses" targeting those in a position to lead small-and-medium enterprises will be held, and through alliances with small-and-medium organizations, cooperation will be given for other information security seminars held by these organizations, so as to improve the security level of such enterprises.

b) Dissemination of the information security measures guidelines for small-and-medium enterprises created in FY2008 will be facilitated, with the aim of legitimizing the cost burden for information security measures and promoting the measures in small-and-medium enterprises, which can face difficulties in carrying out 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 lead small-and-medium enterprises that attended the "Information Security Leadership Nurturing Seminars for Small-To-Middle Sized Businesses," will receive information security consultations using training courses etc., and will also introduce and provide education materials and guidance tools created by the

IPA, etc.

b) Tools for supporting the provision of information on information security will be provided to small-and-medium enterprises.

(c) Maintaining a Tax System to Facilitate Information Security Investment in Small-and-Medium Enterprises (Ministry of Economy, Trade and Industry)

In order to facilitate information security measures in small-and-medium enterprises, a tax system will be maintained for facilitating investment in information security in small-and-medium enterprises.

E Enhancement of Spam E-mail Measures

(a) Enhancement of Spam E-mail Measures (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Consumer Affairs Agency)

[Only e) is repetition: Refer to 3 D (i)]

a) In order to deal with ever increasing spam e-mails, which are becoming increasingly clever and malicious, clear steps will be taken 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 industry groups such as "JEAG" —a private-sector group established under the initiatives of major domestic Internet connection service providers and mobile phone operators—the introduction of effective technologies for the prevention of spam e-mail transmission, such as blocking of port 25 and sender domain authentication (SPF, DKIM,etc.), will be facilitated.

c) In order to deal with spam e-mail sent from overseas, which occupies a large portion of the spam e-mails received in Japan, collaboration with overseas enforcement agencies in charge of spam e-mail measures will be enhanced, and alliances with the private sector will be promoted on international spam e-mail measures.

d) In addition, the "Project for Eliminating Spam E-Mail" (from February 2005) will be carried out 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 will encourage the adoption of sender domain authentication technology, to stop malicious third parties from impersonating government agencies or their staff and thus causing harm to the general

public and private sector, and will also propose the further promotion of receiver-side measures and widely informing the public of such threats. In addition, the introduction of measures using cryptographic technology such as DKIM and S/MIME will also be actively considered.

F Promoting Intellectual Property Protection

(a) 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) From the perspective of deterring content infringing copyright from spreading globally on the Internet, examination within an international framework will be carried out to build a mechanism for sharing information on the rightful copyright holders.

b) Through bilateral government 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[39])), countries where piracy problems are found will be urged to reinforce measures against content infringing copyright. Also, so as to encourage overseas providers to delete content infringing copyright, use of the Content Overseas Distribution Association (CODA[40]) by the private sector will be promoted.

[39] Abbreviation of International Intellectual Property Protection Forum.
[40] Abbreviation of Content Overseas Distribution Association.

6 Promotion of R&D and Industry Development

Based on the "Information Security R&D Strategy" and its roadmap, R&D will be promoted on active and highly reliable (dependable) information security technology, such as establishing a new defense model and realizing a secure communication environment.

Through establishing methods for utilizing information security technology compatible with new ICT and by facilitating world-leading R&D on information security, Japan will contribute to activating the domestic information security industry and strengthening its international competitiveness.

A Promotion of R&D

(a) Promotion of R&D for the "Information Security R&D Strategy" (Cabinet Secretariat and concerned government agencies)

Based on the "Information Security R&D Strategy", R&D will promoted for ensuring new dependability of the entire information and telecommunications system, performing Zero-Day Defense[41] based on the behavioral analysis of attackers, realizing the flexibility management of personal information, establishing a foundation for facilitating R&D, and systematizing security theory. Also, the progress status of these R&D initiatives will be confirmed, at which time consideration will be given to the establishment of a scientific evaluation framework as a foundation for stimulating information security research.

(b) Examination of the Way of Information Security in M2M and Promotion of R&D (Cabinet Secretariat, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

[Repetition: Refer to 5 (2) (a)]

[41] 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.

(c) R&D for Ensuring Information Security in Smart Grids (Ministry of Economy, Trade and Industry)

[Repetition: Refer to 5 (2) (c)]

(d) R&D on Countermeasure Techniques for Targeted Attacks (Ministry of Internal Affairs and Communications)

[Repetition: Refer to 1 C (f)]

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

With a view to implementation by around FY2020, R&D will be promoted for New-Generation Network infrastructure technologies with superior optimal quality, security and disaster-resistant corresponding to user requirements by overcoming IP network limitations. In FY2012, the detailed design of a system based on the grand design relating to the new-generation network of FY2011 will be tackled.

(f) R&D on Security Technology for Cloud Computing Data Transfer and Facilitation in Providing for a Disaster (Ministry of Internal Affairs and Communications)

[Repetition: Refer to 5 (1) B (g)]

(g) Realization of a Secure Communication Environment by Utilization of Communication Protocol Using Cryptographic and Authentication Technology (Ministry of Internal Affairs and Communications)

Studies and substantiative experiments will be undertaken to establish evaluation methods on communication protocol security using cryptographic and authentication technology, towards the realization of a secure communication environment.

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

R&D will be carried out at the NICT to establish a quantum information communication network technology, including quantum cryptography with information-theoretic safety (unconditional safety of cryptography in the information-theoretic sense).

(i) R&D on Information Security Technology for Ensuring a Secure and Reliable Network (Ministry of Internal Affairs and Communications)

[Repetition: Refer to 5 (3) A (g)]

(j) 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, R&D will be carried out towards establishing an evaluation method to verify whether the communication protocols installed in routers and other network devices are highly secure.

Using the results obtained by the NICT in FY2011, in FY2012 the NICT will expand the evaluation methods, and assess the practicality of system-based communication protocol evaluation methods.

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

So as to promote R&D into cyber security, a test bed will be built that allows for the safe external use of attack traffic, malware samples, and other security data sets.

In FY2012, the NICT will make the test bed more sophisticated such as by adding malware analysis functions by applying virtual technology, and also operate the test bed in collaboration with external organizations.

(l) Building of an Information Security Verification Environment for IPv6 Networks (Ministry of Internal Affairs and Communications)

[Repetition: Refer to 5 (1) C (b)]

(m) New Technological Development for Strengthening the Information Infrastructure to Support Innovation Creation (Ministry of Education, Culture, Sports, Science and Technology)

Regarding the information infrastructure to support innovation as a scientific technological base, new R&D will start from FY2012 on strengthening disaster resistance (introduction of a dispersion system and self-recovery functions, etc.) so as to further facilitate the reinforcement of functions to contribute to achieving issues such as making the information infrastructure more disaster resistant.

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

Taking into consideration the emerging situation of information security-related accidents that may give rise to risks involving the lives and fortunes of citizens and the stagnation of overall economic activity, in line with the development of information technology as social infrastructures, R&D on new-generation information security technologies will continue in FY2012 in aiming towards the fundamental resolution of these basic issues, rather than using stopgap measures.

(o) Promotion of R&D on Technology to Automatically Derive Appropriate Information Security Settings in Systems (Ministry of Internal Affairs and Communications)

When ensuring appropriate information security in networks, it is important to have comprehensive information security management that considers this from start to finish. To this end, the NICT will carry out R&D on risk evaluation and verification technology in the entire network, in aiming towards automatically deriving optimal information security settings in each structural component (node) of the network.

In FY2012, the required information security knowledge base for deriving optimal structures will be built.

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

[Repetition: Refer to 5 (1) B (e)]

B　Promotion of the Information Security Industry

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

Stimulation of the information security industry is essential in order to raise the level of Japan's information security.

The establishment of information security technologies and usage methods for new ICT, such as cloud computing, IPv6, smart devices and SNS, promotion of R&D on world-leading active and highly reliable (defined as "New Dependability") information security, and development of high-level human resources for information security, will help to stimulate Japan's information security industry and raise its international competitiveness.

The working group set up under the "Technological Strategy Special Committee" will study measures for stimulating Japan's information security industry.

(b)　Formulation of Information Security Standards for Control Systems and Establishment of an Evaluation and Authentication System (Ministry of Economy, Trade and Industry)

[Repetition: Refer to 4 D (a)]

7 Development of Information Security Human Resources

Regarding the development of information security human resources, as proposed in the "Immediate issues based on the information security HR development program in and after 2012", necessary measures will be steadily promoted for developing four categories of human resources: corporate information security personnel, information security industry personnel, leading-edge researchers and technical experts, and government agency information security personnel.

A Corporate Information Security Personnel, Information Security Industry Personnel, Leading-Edge Researchers and Technical Experts

(a) Spread Cross-Sectional Career Path Model and Promote HR Development Planning (Ministry of Economy, Trade and Industry, and concerned government agencies)

Promote human resource development planning in companies, along with the dissemination of information security personnel career path model created by the IPA.

(b) Organize Skills, Qualifications, and Training Programs (Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

The skills and related qualifications required in information security-related businesses and educational programs will be organized and publicized.

(c) Promoting the Placement of CISOs (Ministry of Economy, Trade and Industry)

From the perspective of promoting information security, the roles and competencies required in CISOs will be coordinated, and efforts made towards their further placement.

(d) Promotion of Recurrent Education (Ministry of Education, Culture,

Sports, Science and Technology)

Support will be provided for accepting adult students at higher education institutions.

(e) Human Resource Development Utilizing the NISC and Incorporated Administrative Agencies (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

The National Information Security Center (NISC), National Institute of Information and Communications Technology (NICT), National Institute of Advanced Industrial Science and Technology (AIST), and Information-technology Promotion Agency, Japan (IPA) will hold liaison meetings for strengthening alliances with the objective of performing the core function of producing outstanding human resources.

(f) Temporary Acceptance of Private-Sector Security Human Resources by Government Agencies (Cabinet Secretariat and related government agencies)

Government agencies and incorporated administrative agencies will form a hub to develop information security human resources and shape a wide network through creating opportunities that allow for the reciprocal experience of security-related businesses in industry, academia and government sector.

(g) Education on Information Security in Universities (Cabinet Secretariat, Ministry of Internal Affairs and Communications, Ministry of Education, Culture, Sports, Science and Technology, and Ministry of Economy, Trade and Industry)

a) Provide support for practical high-level education via cooperation with universities and industries.

b) The latest information on information security will be actively provided to universities and other institutions, so as to contribute to the placement of information security-related research departments.

(h) Promotion of R&D on the “Information Security R&D Strategy” (Cabinet Secretariat and related government agencies)

[Repetition: Refer to 6 (A) a]

(i) Holding Seminars for the Management Layer (Cabinet Secretariat, Ministry of Internal Affairs and Communications, Ministry of Education, Culture, Sports, Science and Technology, and Ministry of Economy, Trade and Industry)

Dissemination and education will be carried out by making use of a range of opportunities, such as holding seminars for the management layer, personnel managers and staff in charge of employment in companies, along with also utilizing conferences sponsored by economic organizations, etc.

Support will also be provided for activities of the Information Security Governance Council.

(j) Holding Competitions on Information Security (Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

a) The security camps will be further enriched.

b) Consideration will be given to holding competitions in which information security personnel can compete on their practical skills.

c) Consideration will be given to dissemination and education leading to facilitating the employment of those who achieve excellent results in the competitions and other events.

(k) Enhancement of Awards and Other Recognition(Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

a) Awards will be presented to individuals and companies etc., that have made significant contributions from the perspective of ensuring information security.

b) The “Exploratory IT human resources project” will be implemented.

(l) Support for the Participation of Leading-Edge Researchers in International Conferences (Cabinet Secretariat and related government agencies)

Human resources that can perform on a global scale will be developed through providing support for participation international conferences and the hosting of such conferences in Japan, etc.

B Government Agency Information Security Personnel

(a) Preparation of CSIRT Systems and Reinforcement of Alliances (Cabinet Secretariat and all government agencies)

[Repetition: Refer to 1 B (a)]

(b) Rotation of Government Personnel (Cabinet Secretariat and concerned government agencies)

Consideration will be given to personnel rotation so that information security personnel can be involved in work that relates to information security for a long time, such as staff exchanges between the information security divisions of each government agency and the NISC.

(c) Utilizing Outstanding External Human Resources (Cabinet Secretariat and concerned government agencies)

Consideration will be given to the way of utilizing external human resources involved in information security, through public and private sector staff exchanges and other initiatives.

(d) Promotion of Education and Awareness-Raising for Government Employees (Cabinet Secretariat, National Personnel Authority, Ministry of Internal Affairs and Communications, and all government agencies)

[Repetition: Refer to 3 D (h)]

(e) Confirmation of Civil Servant Knowledge of Information Security-Related Knowledge upon Hiring (Cabinet Secretariat and concerned government agencies)

Request relevant government agencies to confirm the information security-related knowledge of applicants for public servants.

(f) Development of Human Resources and Reinforcement of Alliances with Foreign Countries (Ministry of Defense)

[Repetition: Refer to 2 B (f)]

(g) Promotion of Human Resource Development in Critical Infrastructure Operators (Cabinet Secretariat and concerned government agencies)

Government-based initiatives will be promoted for the development of human resources in critical infrastructure, such as the placement of CSIRTs in organizations, the employment and training of staff that can firmly respond to information security risks, and the raising of information security awareness and competencies in staff.

Also, the cross-sectional implementation of research programs in each CEPTOAR will be considered.

C Cross-Cutting Issues that Span Personnel Categories

(a) Education on Information at the Primary and Secondary Education Levels (Ministry of Education, Culture, Sports, Science and Technology)

a) Taking into consideration revisions of the course of study, in accordance with the development stage, education on information morals, including information security, will be actively promoted.

b) Consideration will be given to providing opportunities for training and exchanging information on teaching methods for supervisors and key persons with central roles in promoting information education in each region. This is to ensure the facilitation in local government of initiatives for improving leadership for ICT usage including the basic knowledge on information security of all staff involved in primary- and secondary-level education, as well as the managers of education boards and schools.

(b) Investigation to Examine in Information in the National Center Test for University Admissions (Ministry of Education, Culture, Sports, Science and Technology)

Request the National Center for University Entrance Examinations to give consideration to examining the subject of information in the National Center Test for University Admissions, taking into account the current situation of high school education and the views of persons related to high schools and universities.

(c) Provision of the Latest Information on Information Security for Universities (Cabinet Secretariat, Ministry of Internal Affairs and

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

The latest findings and news on information security will be provided to help the implementation of education on information security in universities. As a part of this, information will also be provided for facilitating consideration of the holding information security-related lectures in MBA courses, as well as introducing recognition of credit based on the passing of examinations and acquisition of qualifications on information security based on the university's autonomous decision, and also introducing study programs on qualifications.

(d) Promotion of Industry-Academia Collaboration in Information Security-Related Education (Ministry of Education, Culture, Sports, Science and Technology, and Ministry of Economy, Trade and Industry)

a) Support will be provided for the implementation of internships and PBL[42], and building a system to promote practical education through industry-academia collaboration

b) Support will be provided for the matching of universities and students with companies, based on a practical internship model.

c) The database of classes and teaching materials jointly created through cooperation between industry and education will be enriched, and its usage facilitated.

(e) Consideration of Sharing Incident Cases on Information Security (Cabinet Secretariat, Ministry of Economy, Trade and Industry, and concerned government agencies)

Consider means to provide incident cases on information security summarized in the IPA etc., as learning materials while taking into account information providers.

(f) Development of Lawyers Knowledgeable in Information Security (Cabinet Secretariat and concerned government agencies)

Using external human resources and other efforts, consideration will be given to the development of relevant persons in the judiciary who are capable of leading in the information security field.

[42] Abbreviation of Project Based Learning.

(g) Popularization and Publicizing of Information Security Certifications (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

a) So as to enhance the development of advanced IT human resources including those in information security, efforts will be made towards the further popularization and publicizing of the Information Technology Engineers Examination in measuring the skills of human resources in information security and other types of information fields.

b) From the perspective of enriching the number of information security experts in the private sector, efforts will be made towards the further popularization and publicizing of qualifications and educational programs on private sector information security.

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

Human resources with information security audit knowledge and capable of fairly and objectively evaluating information security measures from outside and within the organization are to be nurtured.

(i) Consideration of an 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 human 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[43], 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.

8 Enhancement of Information Security Literacy

In order to ensure that the public and users can confirm the existence of IT risks and voluntarily carry out information security countermeasures, based on the "Information Security Outreach and Awareness Program", dissemination and education activities will be enhanced and enriched, including improving the Information Security Awareness Month. In particular, dissemination and education activities will be carried out taking into consideration environmental changes and the full-fledged spread of smart phones.

Also, consultation services on information security and initiatives for the protection of personal information will be continued, in addition to efforts made toward facilitating publicizing and education for the deterrence of crimes and preparing a base for the policing of cybercrimes, along with establishing information security governance.

A Enrichment and Enhancement of Dissemination and Education Activities

(a) Promotion of the "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 will be steadily promoted.

b) So as to heighten each citizen's awareness of information security, the use of a self-examination checklist will be promoted as a tool for allowing individuals to objectively recognize which phase the measures they have implemented are in.

c) Taking care not to unnecessarily arouse uneasiness in the elderly, the use of materials for elderly people that easily explain information security measures in simple language will be promoted.

d) Information will be provided so as to ensure appropriate risk judgment on information security by corporate management, and raise their awareness of information security.

(b) Enhancement of the "Information Security Awareness Month" (Cabinet Secretariat

and concerned government agencies)

Taking into account the results of the "Information Security Awareness Month" held so far, consideration will be given to methods for the effective dissemination of information and strengthening public-private sector alliances, and efforts will be made toward further publicizing and enhancing initiatives for the "Information Security Awareness Month".

(c) Implementation of Dissemination and Education Activities Utilizing International Alliances (Cabinet Secretariat and concerned government agencies)

So as to further promote international alliances, dissemination and education activities utilizing international alliances will be carried out in October, and dissemination and education in Japan will be strengthened in cooperation with other countries.

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

[Only f) is a repetition: Refer to 5 (1) A (e)]

a) In order to raise the information security awareness of citizens, taking into consideration the rapidly increasing sophistication and complexity of information security threats, appropriate information will be provided to each citizen through efforts such as the "Website on Information Security Awareness Raisin", "@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" . These efforts will focus on IT beginners as well as people who are indifferent to information security.

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

c) A course ("e-Net Caravan") targeting guardians, educators, elementary, junior high, and high school students for educating children about the safe and secure Internet use, will be held nationwide in cooperation with telecommunication organizations, etc.

d) As a joint undertaking with the Korea Internet & Security Agency (KISA[44]), submissions of slogans and posters for raising awareness on information security measures will be collected and selected works will be published, and efforts will be made for fostering and enhancing information security awareness in the country's younger generation.

e) So as to facilitate the further dissemination and education of information security, a portal site will be built featuring a compilation of related public-private sector materials on information security measures, and widely publicized to the general public.

f) Taking into consideration the rapid spread of smart phones and other devices, the comprehensive dissemination and education for users on information security measures for smart phones, etc., will be promoted.

(e) Education on Information at the Primary and Secondary Education Levels (Ministry of Education, Culture, Sports, Science and Technology)

[Repetition: Refer to 7 C (a)]

(f) Consideration of Questions for Information Subjects in then National Center Test for University Admissions (Ministry of Education, Culture, Sports, Science and Technology)

[Repetition: Refer to 7 C (b)]

(g) Enhancement of Publicity and Education Activities for the Maintenance of Radio Frequency Usage Discipline (Ministry of Internal Affairs and Communications)

In the period for enhancing the publicity and education of protecting the radio frequency usage environment held each June, publicity and education on strengthening countermeasures for unauthorized wireless stations is carried out through various types of media with the cooperation of concerned government agencies.

In addition, the regional Bureaus of Telecommunications will implement publicity and education for sales outlets and manufacturers of devices that use radio frequencies.

(h) Provision of Various Tools and Analyses that Contribute to Information

[44] Abbreviation of Korea Internet & Security Agency.

Security Measures (Ministry of Economy, Trade and Industry)

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

b) The information security situation and outlook will be compiled into the "Information Security White Paper" and published.

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

[Repetition: Refer to 3 H (e)]

(j) Usage and Dissemination of Methods 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 those related to reliability, performance or security, efforts will be made in collaboration with relevant industries on the usage and dissemination of methods for ensuring appropriate agreement between users and vendors.

(k) Collection and Sharing of Cases of Information Security Accidents, etc. (Cabinet Secretariat)

In order to prevent information security accidents and to take appropriate measures in the event of such accidents occurring, it is important to verify and reflect on past information security accidents and share the lessons learned from them. To this end, existing released cases will be collected, and consideration given to a method for collecting anonymous cases that cannot be released from the standpoint of trade secrets or privacy protection. Also, the collection of information security accidents will be disseminated so that many people can access and use this data.

B Consideration of a "Worry-Free Information Security Consultation Service" (tentative name)

(a) Improvement of "Information Security Consultation Service" (Cabinet Secretariat and concerned government agencies)

From the perspective of the public and users, improvements will be made to the consultation system of the information security consultation services already set up in the respective government agencies, by strengthening

cooperation among them and other efforts. The Consumer Affairs Agency, the Cabinet Secretariat, and concerned government agencies in charge of consumer protection will collaborate and give consideration to enhancing the response capabilities of consultation services for consumers.

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

The "Worry-Free Information Security Consultation Service," which is a general consultation service concerning malware and unauthorized access, will be operated. Also, consultations for information security faced by computer users will be expanded, and this service will be widely publicized to the public.

Furthermore, information received in the consultations will be reflected in measures for encouraging computer users to take precautions, etc.

(c) Developing and Using Information Security Supporters (Ministry of Internal Affairs and Communications)

Efforts will be made to raise information security levels across the entire nation by developing and utilizing knowledgeable people (Information Security Supporters) close to users in local areas.

C Promotion of Personal Information Protection

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

For the Act on the Protection of Personal Information, from FY2012 onwards, consideration will be given to deliberations on issues with a view to amending the law.

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

In FY2012, 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[45] 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 perspective of international cooperation, and seek international understanding of Japan's personal information protection laws.

D Promoting Preparedness for Cybercrime Policing

(a) Reinforcement of Preparations for Policing Increasingly Malicious and Clever Cybercrimes (National Police Agency)

[Repetition: Refer to 2 C (a)]

(b) Promotion of Efforts in Digital Forensics (National Police Agency)

[Repetition: Refer to 2 C (b)]

(c) Strengthening Cooperation with the Private Sector for Maintaining the Order and Security of Cyberspace (National Police Agency)

So as to maintain the order and security of cyberspace, initiatives to facilitate public-private cooperation will be promoted through the committees comprising of respective local prefectural police organizations and relevant providers.

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

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

(e) Promotion of International Cooperation for Policing Cybercrime (National Police Agency)

[Repetition: Refer to 2 C (c)]

[45] Abbreviation of Asia -Pacific Economic Cooperation.

(f) Promptness of International Investigative Mutual Assistance Using Central Authority System[46] (Ministry of Justice and National Police Agency)

In principle, mutual legal assistance treaties and accords have come into force between Japan-US, Japan-South Korea, Japan-China, Japan-HK, Japan-EU, and Japan-Russia making mutual assistance obligatory. Under these treaties and accords, central authorities are set up to pursue the promptness of mutual assistance through direct communications for assistance between the central authorities, without needing to proceed through the usual diplomatic channels. Consideration will be given to the conclusion of further mutual legal assistance treaties from hereon.

E Promotion of Publicizing and Education for Crime Deterrence

(a) Education 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)

Based on the Unauthorized Computer Access Law revised in March 2012, efforts will be reinforced for policing acts of unauthorized access, phishing, and unauthorized acquisition and storage of another person's identification code, in addition to providing the latest information on specific methods used for the unauthorized access of information security-related provider organizations, and publicizing the status of R&D on access control functions and occurrences of unauthorized access. Through these and other initiatives, measures will be further promoted for the prevention of unauthorized access with public-private sector cooperation, so as to spread knowledge and education on protection from unauthorized access.

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

[Repetition: Refer to 5 (1) A (f)]

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

a) In addition to creating leaflets for junior and senior high school students for the prevention of criminal damage related to dating sites and distributing

[46] Refer 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.

them at the respective local prefectural police organizations, publicity and education will be carried out such as listing on the National Police Agency Websites basic countermeasures and cybercrime methods and countermeasures in response to the various problems of Internet users.

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

(d) Promoting the Development of Cyber Volunteers (National Police Agency)

In order to facilitate volunteer activities in cyberspace, investigative research will be carried out on the way of developing and supporting cyber crime volunteers, and further efforts made toward fostering a safe and secure Internet space.

F 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 will be established while taking overseas trends taken into consideration and reducing the burden on businesses concerning corporate information security.

b) In FY2012, the Information Security Governance Committee, which facilitates the dissemination and education of information security governance and provides support for its introduction, will make efforts for the sharing of findings between participating enterprises concerning information risk management.

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

a) The "Survey on the Actual Information Processing Situation 2012" 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) So as to reduce the burden of registrants and improve the convenience of users, consideration will be given to the electronic filing of business audit ledgers, and the use of guaranteed audits will also be facilitated. In FY2012, a study on making business audit ledgers more convenient will be carried out and a report compiled on issues such as how necessary the ledgers are in reducing the burden of registrants and improving the convenience of users. In addition, through the holding of seminars, etc., efforts will be made to deepen the understanding on guaranteed audits and facilitate their usage.

c) An Information Security Report model will be disseminated to contribute to the protection of the rights and interest of the public and holding of information, and facilitate measures for the appropriate management of information and prevention of information leakage in enterprises. In FY2012, efforts will be made for the dissemination of the Information Security Report model through referrals to individual enterprises and so on.

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

From the perspective 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 users and vendors and clarification of roles and responsibilities will be promoted through dissemination activities, with the cooperation of industry groups relevant to both users and vendors.

G Preventing Social Confusion Caused by Information System Failures

(a) Strengthening of Explanatory Skills on Quality to Users on the Safety and Reliability of Information Systems (Ministry of Economy, Trade and Industry)

From the perspective of preventing confusion and damage to society caused by software bugs in information systems, while making verification technology more sophisticated, a framework for the comprehensive third party evaluation and authentication of the safety and reliability of products, systems and services that perform key functions using software will be introduced by FY2013 as a target, and the ability to explain about quality to users will be strengthened.

9 System Organization

Efforts will be made for improving the safety and reliability of cyberspace, such as preparation toward the early conclusion of the Convention on Cybercrime, the smooth enforcement of the Cyber Penal Code and revised Anti-Unauthorized Access Law.

A Examination of a System for Improving the Safety and Reliability of Cyberspace

(a) Smooth Enforcement of the Cyber Penal Code (Ministry of Justice)

Taking into account the promulgation of the "Law for Partial Revision of the Penal Code, etc. to Respond to Advancement of Information Processing, etc." (Cyber Penal Code) for dealing appropriately with cybercrimes and concluding the Convention on Cybercrime, preparations regarding procedural law will proceed toward smooth enforcement[47].

(b) Preparation toward Conclusion of the Convention on Cybercrime (Ministry of Foreign Affairs)

Preparations will proceed in cooperation with respective government agencies and toward the early conclusion of the Convention on Cybercrime.

(c) Promotion of Countermeasures for the Prevention of Unauthorized Access, such as the Appropriate Operation of the Revised Anti-Unauthorized Access Law (National Police Agency, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

[Repetition: Refer to 8 E (a)]

(d) Clarification of the Lawfulness of Reverse Engineering of Software for Security Assurance (Ministry of Education, Culture, Sports, Science and Technology)

[Repetition: Refer to 5 (3) B (i)]

(e) Facilitation and Spread of Electronic Signature Use in Businesses (Ministry of

[47] Enforcement date: June 22, 2012

Internal Affairs and Communications, Ministry of Justice and Ministry of Economy, Trade and Industry)

[Repetition: Refer to 5 (3) C (a)]

B Examination of Comparing Information Security Systems between 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 their cooperative measures.

１０ Reinforcement of International Alliances

Regarding the reinforcement of bilateral relationships, in addition to working toward building a framework to further enhance unified government involvement while deepening discussions in the Japan-US Cyber Security Meeting and Japan-US Policy Cooperation Dialogue on Internet Economy, study and review of specific cooperation items will be carried out through frameworks such as the Japan-UK Cyber Conference and other bilateral meetings. Also, for alliances with Europe, cooperation will be promoted with the European Commission and other relevant European countries.

For the ASEAN region, alliances will be further strengthened through the promotion of joint awareness and education activities on information security, development of human resources, technical support, research cooperation, and the 5th Japan-ASEAN Information Security Policy Meeting to be held in Tokyo, etc.

In the field of multinational alliances, cooperation concerning measures against cyber incidents, public-private sector alliances and international alliances for critical infrastructure protection, collaboration on awareness raising in the information security field, and cooperation on human resource development will be promoted, in addition to actively contributing to the creation of international behavioral norms in cyberspace.

A High-Level Strategic Initiatives

(a) Enhancement of High-Level Strategic Initiatives (Cabinet Secretariat, Ministry of Foreign Affairs and concerned government agencies)

So as to ensure Japan's position is reflected as much as possible in the creation of international norms, high-level encouragement and initiatives will be strengthened in international discussions on cyberspace.

B Strengthening Alliances with the United States, European and Asian Nations, and ASEAN

(a) Enhancing Bilateral Policy Dialogue on Information Security Policies (Cabinet Secretariat and concerned government agencies)

In FY2012, efforts will be made to reinforce strategic bilateral alliances with the US, such as holding talks on collaboration in individual fields concerning information security through building a framework to further enhance unified government involvement, while hosting bilateral meetings such as the Japan-US Cyber Security Meeting and Japan-US Policy Dialogue on Internet Economy, etc. Also, utilizing Japan-EU ICT policy dialogue and other forums, discussions will be held on information security, such as talks toward building a cooperative framework on cyber fields including information security with European nations as well, through holding the Japan-EU Internet Security Forum in addition to the UK and Japan-UK Cyber Conferences. Information exchange and talks on cyber fields will also be actively held with Asian nations.

(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, protecting the reliability of ICT infrastructures supporting economic activities and technological innovations, and the drafting of a cross-sectional information security policies by the government, alliances with various ASEAN countries will be enhanced through the ASEAN-Japan Information Security Policy Meeting,etc.

a) Steady promotion of items decided at the Fourth ASEAN-Japan Information Security Policy Meeting (FY2012)

b) Holding the 5th ASEAN-Japan Information Security Policy Meeting in Tokyo (FY2012)

c) Holding the 4th ASEAN-Japan Government Network Security Workshop in Brunei

d) Holding training related to national strategy formulation and government networks security for government staff of various ASEAN countries in Japan (FY2012)

e) Jointly hold awareness raising and education events with various ASEAN countries (FY2012)

f) Facilitating mutual sharing of experiences and findings cultivated by network operators in Japan and ASEAN member countries by holding workshops, etc. (FY2012)

g) In order to contribute to cooperation in the areas of research and technology, facilitate the exchange of experts in network security fields in Japan and ASEAN member countries (FY2012)

(c) Promotion of Information Security Cooperation in APEC (Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

a) In the Okinawa Declaration, which was decided in the APEC Ministerial Meeting on the Telecommunications and Information Industry (TELMIN) and outlines the common objectives for APEC concerning the telecommunications field, taking into account the inclusion of promoting a safe and secure ICT environment, cooperation on awareness and education and R&D in the network security field will be facilitated between Japan and each APEC region and nation.

b) Applying Japan's accumulated experience in support activities for building CSIRT, through APCERT and other international frameworks, support will be provided to each APEC region and nation for the building, operation and collaboration of CSIRTs responsible for external and internal coordination.

(d) Holding Training and Seminars for Developing Countries (Ministry of Internal Affairs and Communications)

Taking into consideration international alliances with APT[48] member countries and others in the network security field, training and seminars will be held for the relevant government staff of these countries and telecommunications providers on trends, technology and policies in information security.

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

In FY2012, technical seminars held by JPCERT/CC for coding methods without weaved-in vulnerabilities will be implemented centered around the

[48] Abbreviation of Asia-Pacific Telecommunity.

various countries, such as those 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)

Functional changes to the Asian information security benchmark will be made, and dissemination and information exchange to Asian countries will be started.

(g) Support for Building 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, support will be provided for the setting up and operation of CSIRTs, along with collaborative support. In FY2012, dissemination and education of CSIRT establishment seminars, as well as technical support activities, will be carried out.

(h) Support for Enhancement of the CSIRT Systems 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 CSIRTs responsible for external and internal coordination in each country, as well as support for cooperation, will be carried out. In FY2012, based on the experience of support activities for the establishment of CSIRTs accumulated in JPCERT/CC, support will be provided such as for the operations technology for incident response work and the sharing of experiences related to cooperation and operations between CSIRTs.

b) The incident response cooperation between JPCERT/CC and each country's CSIRT will be further enhanced through the activities of FIRST (Forum of Incident Response and Security Teams), IWWN[49], and APCERT, as well as activities such as incident response exercises in the Asia-Pacific region.

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

[49] Abbreviation of International Watch and Warning Network.

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

b) In order to consider and formulate effective countermeasures against cyber attacks, the techniques and methods used in the attacks, as well as their trends and regional characteristics, will be analyzed, and the way of sharing the analysis methods and results will be studied with the participation and/or cooperation of members primarily from CSIRTs in the Asian region.

(j) Promotion of International Cooperation for Policing Cybercrime (National Police Agency)

[Repetition: Refer to 2 C (c)]

(k) Promotion of Efforts toward Cyber-Attack Prevention and Early Countermeasures (Ministry of Internal Affairs and Communications)

[Repetition: Refer to 5 (3) A (b)]

(l) Promotion for Ensuring the Information Security of Smart Phones through Public-Private Sector and International Alliances (Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

[Repetition: Refer to 5 (1) A (a)]

(m) Enhancement of Spam E-mail Measures (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Consumer Affairs Agency)

[Repetition: Refer to 5 (3) E (a)]

C Promotion of International Collaboration and Cooperation through VariousIinternational Meetings and Enhancement of an Information Sharing System

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

Active participation will be pursued in international conferences covering various fields, such as critical infrastructure protection (Meridian), global

economic activities (APEC, OECD, ASEAN),international information sharing (IWWN),incident response (FIRST), national security guarantee (ARF[50]), and ICT use (ITU[51], ACF[52]). Also, active information sharing related to critical infrastructure protection, global efforts including standardization, incident response, and cyber-attack countermeasures, will be carried out. Furthermore, by participating in the Budapest Conference on Cyberspace scheduled to be held in FY2012, Japan will actively contribute to international collaboration and cooperation for issues in the various cyberspace-related fields, including the security field.

(b) Participation in the Planning of International Discussions in the Field of Security Assurance through the Dispatch of Government Experts to Government Experts Meeting on "Developments in the field of telecommunications and information in the context of international security" (Cabinet Secretariat, Ministry of Foreign Affairs and concerned government agencies)

On the basis of the request from the United Nations (UN), Japan will actively contribute to the creation of behavioral norms in cyberspace field and discussion themes in the area of security assurance, such as by the dispatch of government experts to the government experts meeting set up in accordance with the UN General Assembly resolution "Developments in the field of telecommunications and information in the context of international security".

(c) Participation in the Planning of Creating International Norms Concerning Cyberspace (Cabinet Secretariat, Ministry of Foreign Affairs and concerned government agencies)

Regarding the international discussion on cyberspace that has intensified since last year, Japan will show active involvement in the creation of international norms and discussions on the application of international laws in cyberspace, by utilizing various forums such as bilateral meetings and exchanges of opinion, as well as international conferences and other such multi-settings.

---

[50] Abbreviation of ASEAN Regional Forum.
[51] Abbreviation of International Telecommunications Union.
[52] Abbreviation of APT Cybersecurity Forum.

(d) Support for Enhancement of the CSIRT Systems Responsible for External and Internal Coordination in Each Country and Enhancement of Cooperation (Ministry of Economy, Trade and Industry)
[Repetition: Refer to 10 B (h)]

(e) Efforts for Improving Information Security Evaluation and Authentication Technology in the Asian Region (Ministry of Economy, Trade and Industry)

Information will be exchanged on information security evaluation and authentication technology and trends, with the aim of promoting the international mutual recognition agreement for information security evaluation and authentication in the Asian region

(f) Participation in the Planning of International Standardization in the 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.

(g) Initiatives for the International Standardization of Cloud Computing (Ministry of Economy, Trade and Industry)
[Repetition: Refer to 5 (1) B (h)]

(h) Promotion of Information Security Cooperation in APEC (Ministry of Internal Affairs and Communications)
[Repetition: Refer to 10 B (c)]

D　Enhancement of the NISC's Function as a Point of Contact

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

a)　As an international POC[53], 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, positive PR activities will be rolled out through Websites[54], such as by publishing an English edition of this document on the NISC Web site in FY2012.

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

[53] Abbreviation of Point of Contact.
[54] http://www.nisc.go.jp/eng/index.html