Information Security Strategy for Protecting the Nation

May 11, 2010
Information Security Policy Council

I. Preface

The information security policy of Japan has, to date, been implemented by both governmental and private bodies based on the Second National Strategy on Information Security (February 3, 2009) resolved by the Information Security Policy Council (Chairperson: Chief Cabinet Secretary).

After the Second National Strategy on Information Security was resolved, a large-scale cyber attack took place in the United States and South Korea in July 2009. Also, numerous incidents of large-scale private information leaks occurred one after another.

The large-scale cyber attack in the United States and South Korea particularly alerted Japan—where many aspects of economic activities and social life are increasingly dependent upon Information and Communication Technology (ICT)—to the fact that a threat to information security could be a threat to national security and require effective crisis management.

Such information security risks are becoming more diversified, advanced, and complex, and many conventional means of security fail to ensure information safety. In light of this, the United States appointed a Cybersecurity Coordinator to strengthen the national information security management, and other countries followed the United States in implementing strategic information security measures.

In order to accurately respond to such changes in the information security environment, the Japanese government needs to take new initiatives adapted to the major changes in the information security environment as well as continuing to manage the implementation of the Second National Strategy on Information Security being undertaken by governmental/private entities. In particular, the government is responsible for overcoming IT risks, that is, risks concerning usage of ICT, through reinforcing the protection for the critical infrastructures that support socioeconomic activities and which are closely connected to the nation’s day-to-day life. The government should also take organized and immediate action to ensure national security and effective crisis management.

This strategy is a comprehensive approach that includes the Second National Strategy on Information Security and applies to the next four years (FY2010 to FY2013). Based on this strategy, Secure Japan 20XX, an annual security plan will be implemented. Evaluations of this strategy will take place regularly and changes will be made as necessary.

II. Basic Approach

(1) Basic Policies

As well as continuing the implementation of the Second National Strategy on Information Security conducted by public/private entities, the following actions must be taken in regards to information security policy: Identifying the new measures that must be conducted by the government under the basic policies listed below; and organized implementation of the urgent measures to ensure national security and effective crisis management.

<1> Reinforcement of policies taking account of possible outbreaks of cyber attacks and establishment of a counteractive organization

To protect the nation from any cyber attacks that may risk the national security and prompt crisis management, the general mode of readiness must be reinforced and an organization to efficiently counteract any such cyber attacks must be established.

<2> Establishment of policies adapted to changes in the information security environment

As socioeconomic activities become increasingly dependent on ICT, a wider range of devices are being connected to networks and information is becoming freely available beyond national borders. This in turn increases the risks concerning information security more than ever. Thus it is necessary to establish an information security policy that can flexibly adapt to environmental changes, such as emerging information security risks and threats and which can protect the life of the nation.

<3> Establishing active rather than passive information security measures

Conventional information security measures have tended to remain as symptomatic treatment that addresses individual risks whenever they arise, and often fail to address the actual cause. As ICT advances, information security measures that will

bring fundamental solutions to such problems must be strategically identified. At the same time, by utilizing the Plan-Do-Check-Act (PDCA) cycle and other methods, organizational structures that enable entities to actively implement new information security measures—differing from the current passive attitude—must be established.

(2) Background

The following changes in the information security environmental were taken into account to determine the above basic policies.

<1> Increase in threats such as large-scale cyber attacks

In July 2009, a large-scale Distributed Denial-of-Service (DDoS) attack took place against government and commercial services in the United States and South Korea from the extremely high number of bot-infected PCs, mainly within South Korea. Although this DDoS attack did not directly target Japanese information systems, it is undeniable that some large-scale cyber attack may be being planned against Japanese information systems using a large network consisting of bot-infected PCs, in the same manner as the above-mentioned July 2009 attack. Further, the methods of attack are growing more sophisticated and complicated each year, as represented by the so-called “gumblar attack” that affected numerous Web sites inside Japan. Considering the fact that many critical infrastructures are now controlled by systems utilizing ICT, the necessity of establishing effective information security to ensure the nation’s safety is increasing.

At the same time, evidences point out that the underground markets, where information concerning credit cards and bank accounts are traded, are being formed and many internet-related crimes seem to be induced by financial gain. Further, numerous incidents of the leakage of private information from corporations continue, and there are cases where the information owners have suffered from the malicious usage of such leaked information.

<2> New environmental changes

(i) Increasing dependency on ICT in socioeconomic activities

(Relationship with socioeconomic activities)

The role of “information” in socioeconomic activities has increased and such socioeconomic activities depend more and more on ICT. In such circumstances, information security can be seen as a part of the social infrastructure. In order to

utilize ICT to solve a range of challenges that Japan faces, such as economic growth, the aging society, and global environmental issues, it is indispensable to develop a safe and secure ICT usage environment that takes into account recent trends whereby a vast range of devices is now being networked. The globalization of economic activities are progressing through overseas business operations and overseas outsourcing of manufacturing and development. To encourage global corporate activities and expand the supply chain (manufacturing and quality control) management utilizing ICT, while protecting the value of information assets owned by Japanese corporations, establishing a safe and secure ICT usage environment both inside and outside of Japan, and improving the information security level in overseas settings are the key issues. Also, corporate intellectual property and other intellectual property, such as music and videos, are now being traded over the Internet. It is necessary to ensure the safety and security of the ICT infrastructure that supports “the knowledge-information society” to appropriately protect such information assets.

(Protection of the nation and users)

As the role of “information” becomes more significant in the nation’s life and dependency on ICT increases, the government must take action to protect the nation’s information assets and ensure information security with a greater focus than ever before to protect the rights and benefits of the entire nation as an ICT user. It is also important to establish an environment whereby each entity across the nation can actively employ its own information security measures with full awareness of IT risks. Approximately 80% of the nation currently reports that they are not confident about information security. To encourage their usage of ICT, an early solution to promote increased confidence is essential.

(ii) Adapting to new technological innovation

Innovations in ICT and ensuring information security must be carried out simultaneously. Development of cloud computing technology, new Internet technologies such as IPv6, intelligent home appliances, mobile terminals, the spread of electronic tagging systems, and major improvements in computing performance that could lead to a compromise of encryption—innovations in both ICT and business that utilizes information technology are progressing boundlessly. It is essential to establish an information security policy that accurately takes account of such innovation in ICT as well as the spread of other new technologies.

(iii) Globalization etc.

The amount of information exchanged beyond borders is increasing as international economic activities and borderless services over the Internet become commonplace. This reveals differences between each country's legal system concerning the protection of private information and information security, and presents a challenge to such borderless information trading.

(3) Key Actions

To realize the government's information security measures, the following concrete actions based on the Basic Policies mentioned in (1) above must be implemented.

<1> Overcome IT risks to realize safety and security in the nation's life

As socioeconomic activities increase their dependency on ICT, the threats against information security also grow bigger. The first key action under such circumstances is to overcome IT risks in order to realize safety and security in the nation's life. This is achieved mainly through reinforcement of the critical infrastructures that support socioeconomic activities, which are closely connected to the nation's day-to-day life. From the fact that large-scale cyber attack incidents are becoming more frequent, cyberspace is now the key area in which to protect Japan's national security and implement effective crisis management. Thus, policies that strengthen the national security of cyberspace and increase crisis management expertise must be urgently established.

<2> Implementation of a policy that strengthens national security and crisis management expertise in cyberspace, and integrity with ICT policy as the foundation of socioeconomic activities

Implementation of policies to strengthen national security and crisis management expertise in cyberspace must maintain integrity with the policy that is enforced under the principles of the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society, which stipulates promoting the usage of ICT as the foundation of socioeconomic activities.

<3> Establishment of a triadic policy that comprehensively covers the viewpoints of national security, crisis management, and nation/user protection. An information security policy with a focus on the nation's/users' viewpoint is particularly important.

As well as setting up an information security policy that improves national security and crisis management expertise in cyberspace and also encourages the usage of ICT as the foundation of socioeconomic activities, an information security policy that values the nation's/users' viewpoint mush be established, reverting to the principle that the benefits from ICT must benefit the entire nation.

<4> Establishment of an information security policy that contributes to the economic growth strategy

A safe and secure telecommunication environment with high reliability is indispensable to encourage ICT usage, and provision of such an environment as the foundation of socioeconomic activities should encourage the strategic investment and utilization of ICT. This then will help encourage Japan's economic growth and resolve the problems that Japan faces. An information security policy that will contribute to such an economic growth strategy must be promoted and established.

<5> Building up international alliances

Free circulation of information across borders will increase global convenience, but at the same time, a new obstacle that has not been encountered so far has arisen: the legal differences concerning ICT in different countries. Therefore, it is important to bring into alignment the ICT-related legal systems in different countries, and thus international alliances and coordination in terms of information security policy must be ensured. Such international alliances must cover a wide range of information security policy—including private information protection.

III. Targets to Achieve

○ By 2020, the vulnerability related to the use of ICT, for example, Internet and information systems, must be overcome for Japan to become the world's foremost "advanced information security country" through establishing an environment where the entire nation can use ICT safely (an environment where high quality, reliability, safety, and security are ensured).

Concretely, Japan must improve its ability to respond to all types of ICT threats, including cyber attacks, to the world's highest level, and widen and reinforce the government's incident management ability to guarantee the nation's safety and

security. Further, Japan must build an environment where the nation can actively utilize ICT without concerns regarding information security reliability.

○ The concrete measures required to achieve the above targets are listed in the following section. These will be implemented over the next four years, along with the measures stipulated in the Second National Strategy on Information Security (FY2009 to FY2011), aiming to eliminate the nation's anxieties regarding information security.

IV. Concrete Measures

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

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

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

1 Preparation for a Potential Large-Scale Cyber Attack

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

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

(1) Organizing Counteractive Arrangements

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

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

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

- Policing cybercrimes
  Promote cybercrime policing through utilization of digital forensic technologies

and collaborations among various investigation agencies from different countries.

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

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

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

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

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

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

<1> Consolidation of governmental infrastructure

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

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

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

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

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

- Promotion of secure encryption usage in government agencies

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

- Ensuring information security in cloud computing

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

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

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

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

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

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

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

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

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

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

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

<2> Reinforcement of critical infrastructures

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

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

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

- Reinforcement of the information sharing system

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

- Promotion of the CEPTOAR Council

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

- Organization and dissemination of Safety Standards

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

- Improvement of critical infrastructure protection measures

  Improve the information security measures by critical infrastructure operators, etc. through constant efforts to analyze the threats against each business domain and by conducting regular cross-divisional emergency drills, so that the damage

that may be caused by a serious failure can be isolated and minimized.

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

- Elaboration of Business Continuity Plans

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

- Promotion of international alliances in the area of critical infrastructures

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

<3> <u>Reinforcement of other infrastructures</u>

- Improvement and reinforcement of countermeasures against malware

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

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

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

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

- Ensuring the IPv6-related information security

  To address the issues concerning Pv6-related information security, identify concrete information security problems by utilizing the related verification environments, and cultivate human resources to ensure a smooth migration to IPv6.

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

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

- Ensuring information security in medical and education fields

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

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

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

- Promoting safe electronic trading

  To protect important financial information—such as credit card

details—implement information security measures that meet international security standards. Formulate information security standards for Web sites that operate electronic trading and encourage such operators to ensure compliance with the said standards. Also keep implementing the new information leakage prevention measures.

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

<4> Enhancement of the functions of the National Information Security Center (NISC)

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

(2) Reinforced Protection of the Nation/Users

<1> Conducting an information security campaign

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

<2> Suggestion to set up the "Information Security Safety Support Service" (tentative name)

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

<3> Promotion of private information protection

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

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

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

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

<4> Tighten policing against cybercrime

- Organization of a cybercrime policing infrastructure
  Reinforce cybercrime policing, as well as organize infrastructural arrangements, such as utilization of digital forensic technology and strengthening international

coordination.

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

- Crime prevention campaign

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

(3) Reinforcement of International Alliances

<1> Strengthening alliances with the United States, ASEAN, and EU countries (strengthening bilateral relationships and ties with ASEAN)

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

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

<2> Building an information sharing system through international conferences, such as APEC, ARF, ITU, Meridian, and IWWN

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

<3> Enhancement of the NISC's function as a point of contact

As an international Point of Contact (POC) in regard to comprehensive information security issues, NISC must reinforce its alliances with the relevant overseas

organizations in terms of information security policy, which includes sharing information about good information security practices conducted in different countries and measures taken to safeguard their critical infrastructures.

(4) Furtherance of Technological Strategies etc.

<1> Strategic furtherance of information security research and development

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

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

<2> Cultivation of information security human resources

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

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

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

<3> Establishment of information security governance

Raise information security awareness among business management so that information security governance may be included as one of the business management requirements through an awareness raising campaign. This aims to ensure that information security is taken into account when formulating BCPs or

replacing business computing systems (such as accounting systems), and when conducting information security audits. Also, establish some measures to ensure information security is implemented in any newly introduced risk management methods within businesses.

(5) Organization of Legal System concerning Information Security

<1> Identify measures to improve cyberspace safety and reliability

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

<2> Comparison of information security legal systems of different countries

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

Attachment

○ Glossary

Terms	Description
Cyberspace	Virtual space on the Internet or other computer systems where information is exchanged using ICT.
Cybercrime	Crimes that utilize ICT, such as those using advanced information and communication networks (e.g. the Internet) and those targeting electromagnetic records.
Critical infrastructures Critical infrastructure operators, etc.	A critical infrastructure is defined in the Second Action Plan on Information Security Measures for Critical Infrastructures as infrastructures in the following sectors: Information and Communications; Banking and Finance; Aviation; Railway; Electricity; Gas; Government and Municipal Services (including local governments); Medical; Water Supply; and Distribution. Critical infrastructure operators refers to those specified within the *Target Operators* in Attachment 1 of the *Second Action Plan* from among the operators in the 10 sectors listed above; an organization comprising the said specified operators.
Digital forensic technology	Technology and methods to elucidate evidence to be utilized for legal purposes. Such technology and methods are used to collect and analyze electronic records, data, and equipment to investigate computer-related crimes (e.g. unauthorized accesses and confidential information leakage) or disputes, and identify the criminal process.
Bot	A computer program designed to enable a computer to be remotely controlled for malicious purposes. Various types of damage can be caused by a malicious attacker remote controlling bot-infected computers, such as distribution of large amounts of spam e-mails, attacking specific Web sites, other nuisance activities, and information theft.
Malware	Malicious software that causes damage to computers and their users. Malware includes computer viruses, worms, spyware, etc.