Provisional Translation

Cybersecurity Strategy

~Towards a world-leading, resilient and vigorous cyberspace~

June 10, 2013

Information Security Policy Council

Contents

Introduction

It has been 8 years since the National Information Security Center (NISC) was established in the Cabinet Secretariat in April of 2005 and the Information Security Policy Council (ISPC) was established in the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters) in May of the same year for the purpose of drastically strengthening measures for information security issues.

During this time, the ISPC determined the "First National Strategy on Information Security", the "Second National Strategy on Information Security" and the "Information Security Strategy for Protecting the Nation", working towards improving the level of information security within Japan while balancing between assuring free flow of information and precisely dealing with risks.

The information security environment changes extremely quickly. In the 3 years since the determination of the previous strategy, risks have become increasingly serious, more diffuse and more globalized. "Cyber attacks" against government institutions and critical infrastructures have become a reality and have become both "national security" and "crisis management" issues. At present, the introduction of the best possible measures for protecting the government institutions and critical infrastructures has become essential.

We are entering an age, where everything is connected to the internet, called the Internet of Things. This is an age where everything faces information security risks. Risks are also increasing even for control systems which are not connected to the internet. Accordingly, this means that information security measures are becoming essential for every aspect of people's daily lives. Information security has become an issue directly linked to the "stability of people's daily lives" and "economic development".

Our country is working towards constructing a "world's most advanced IT nation". The world's most advanced IT nation must also realize a "safe cyberspace" suited to the title. In order to construct a safe cyberspace within this fast changing environment, not only is ensuring information security by each individual stakeholder necessary as ever, but the contribution of every stakeholder related to cyberspace has also become necessary.

Thus, this strategy has been named the "Cybersecurity Strategy" in order to make clear the necessity to widely promote measures related to cyberspace and approach of these measures as distinguished from efforts for assuring "information security" up until now.

As this strategy recognizes that a level of measures is required greater than those that came before, it presents a variety of new issues. We expect that this strategy, including these issues, will be steadily implemented, and that this will lead to the fast realization of a "Cybersecurity Nation" with a "world-leading, resilient and vigorous cyberspace".

1. Environmental Changes

(1) Expansion and Penetration of Cyberspace

① "Merger and integration" of cyberspace and real-space

"Cyberspace," global virtual spaces such as the internet, composed of information systems, information communications networks and similar systems and which circulate large quantities of a large variety of information, have rapidly expanded and begun permeating real-space. At present, cyberspace serves as an indispensable brain and nervous system for nearly every activity including peoples' daily lives, socioeconomic activities and governmental activities, and the merger and integration of cyberspace and real-space continues.[1]

The expansion and penetration of cyberspace is a result of the propagation and advancement of information communications technologies and the progress of the use and application of those technologies. Specifically this includes the spread of broadband infrastructure to every region of the country, as well as the propagation and advancement of smart devices, IPv6, M2M[2]/sensor networks, cloud computing services and others.[3] and the use and application of these in a variety of fields including electronic commerce, medical, educational, transportation, social infrastructure management and e-government.

[1] For example, the Ministry of Internal Affairs and Communications "2012 White Paper on Information and Communications in Japan" (Hereinafter "White Paper on Information and Communications") states, "The internet has become an essential infrastructure for socioeconomic activities in global society", the National Police Agency "White Paper on Police 2012" states, "the internet has become established as an essential social infrastructure for citizens' daily lives and socioeconomic activities", and the Ministry of Defense "Defense of Japan 2012" states, "For the military, information communications serve as an infrastructure for command and control from the central command to detached units, and the IT revolution has resulted in and even greater level of reliance on information communications networks by the military."

[2] Machine to Machine. Systems where devices connected via a network reciprocally exchange information without the intervention of a human user and automatically execute the optimal controls. For example, a variety of sensor devices (home information appliances, automobiles, vending machines, buildings, smartphones, etc.) cooperate via a network to realize provision of energy management, facility management, deterioration monitoring, disaster prevention, welfare and a variety of other services in various fields.

[3] For example, the Information-technology Promotion Agency (Hereinafter "IPA"), independent administrative institution, "Information Security White Paper 2012" states, "System environments have also changed greatly in the past few years. New devices have emerged, and there have also been changes in service structure such as the opening of control systems and systems like cloud computing."

Cyberspace is essential to strengthen Japan's growth potential, and a greater level of expansion and penetration is expected in the future. For example, ITS[4] and smart grids which utilize open data and big data are necessary in order to realize the supply and demand of clean and economic energy as well as safe, convenient and economic next generation infrastructure which are vital for strengthening growth potential. The information systems, information communications networks and similar systems of which these are composed, will bring about even greater expansion and penetration of cyberspace.

In addition, cyberspace is expected to expand and penetrate even more on a global scale, and is receiving attention worldwide as a force for inducing national growth as indispensable for promoting economic growth and innovation, resolving social issues and other for other purposes.[5]

② "Increasingly serious risks" surrounding cyberspace

Cyberspace has a high degree of anonymity, with little traceable evidence, suffers from very little geographical or temporal limitations, and is capable of affecting large numbers of unspecified individuals within a short period of time.

For these reasons, the threat of so-called "cyber attacks" has continued to grow, including unauthorized intrusions via cyberspace, theft, alteration and destruction of information, information system outages and incorrect operations, malicious program execution and DDoS attacks,[6] through abuse of information communications networks, information systems and similar systems.

Among early cyber attacks, many of the threats were crimes for pleasure for the purpose of showing off, making an example, harassment and similar reasons.[7] However, attacks for financial and threat purpose soon began to

[4] Intelligent Transport Systems. Systems aimed at improving road user convenience, eliminating traffic accidents and traffic congestion, optimizing transport network management and other purposes by networking individuals, vehicles and roads. Navigation systems and automatic toll collection systems have already become commonplace. In the future the practical application of safe driving, automated driving and other systems through vehicle-vehicle and vehicle-road communications is expected.

[5] For example, the G8 Summit of Deauville "G8 Declaration Renewed Commitment for Freedom and Democracy" (May, 2011) states, "All over the world, the Internet has become essential to our societies, economies and their growth. (abridged) The Internet has become a major driver for the global economy, its growth and innovation."

[6] Distributed Denial of Services attacks.

[7] For example, the "love letter" worm, which was spread through email infections and destroyed data on

appear[8], and recently attacks aimed at stealing national and business secrets[9] and aimed at destroying critical data and systems[10] have begun to appear. Further, overseas, cyber attacks have been indicated which have been said to be linked with military operations, and it is said that a large number of foreign militaries are developing their offensive capabilities on cyberspace, and that intrusions have been made into the information communications networks and systems of other countries in order to gather information.

The techniques for cyber attacks are also becoming increasingly more complex and sophisticated. For example, in addition to website falsification and DDoS attacks aimed at stopping online services,[11] such attacks have also started to appear as drive-by download attacks using web-based infection viruses,[12] attacks on closed controlled networks which do not connect to the internet or other external networks carried out using USB memory or other means,[13] MITB attacks where malware hijacks a web browser and alters communications,[14] and targeted attacks consisting of a combination of facets including zero-day exploits and social engineering like so-called "Yari-tori type."[15] These attacks include some for which it has been pointed out that the advanced technical level and planning likely required the contributions of a government.

In addition, the scope of targets for cyber attacks has also grown from private

PCs in the first half of the 2000's.

[8] For example, statements from so-called "hacktivists" criticizing the Copyright act when illegal downloads were criminalized around June of 2012, and a variety of damages occurred including website defacement and DoS attacks on government facilities, political parties and related organizations.

[9] For example, the discovery of virus infections resulting from targeted attacks on the Diet, government institutions, defense related businesses, etc. since September of 2011.

[10] For example, the "Shamoon" virus cyber attacks which rendered computers incapable of booting by using a technique of altering the master boot record (MBR) of infected computers overseas.

[11] For example, the website defacement and DDoS attacks against government institutions and other targets which occurred in around September of 2012.

[12] For example, "Gumblar" and other attacks which struck ferociously from 2009 to 2010, aimed at web browser and OS vulnerabilities, downloading unauthorized programs such as viruses to PCs without the user's intent when browsing websites.

[13] For example, in addition to "Stuxnet," which was used for cyber attacks against uranium enrichment facilities via the internet, infection was also possible through USB memory stick connected to infected computers, making intrusions possible even into stand-alone systems isolated from the internet.

[14] Man In The Browser attack. Attacks where malware infecting a user's PC hijacks a web browser and takes advantage of a normal session to embed unauthorized operations. For example, unauthorized operations where when a user carries out a normal operation in online banking, the recipient of transferred money is changed behind the scenes.

[15] Ways to send targeted attack emails after pretending natural situations not by sending targeted attack email from the beginning, but by several exchanges of regular emails disguised as an association with business. See, the National Police Agency “Cyber attacks situation in 2012 year” (February 28, 2013)

spaces such as individuals and households to public spaces such as social infrastructure. Information communications equipment is being distributed to a variety of people, things and places through situations such as ownership of more than one device by individuals, the rapid increase in the number of individuals who bring smart devices such as smartphones, the propagation of information appliances which can be remotely operated from outside the home, BYOD[16] and use of copy machines and other multi-functional products in the workplace, installation of POS terminals and security cameras in shops and utilization of sensors and other equipment in social infrastructure and similar settings.

In Japan, up until now, in addition to risks of destruction of equipment due to natural disasters and accidents, and leaks of information and incorrect operations of systems by authorized users, measures have been implemented for dealing with cybercrimes and cyber attacks. However, risks related to cyber attacks have reached a level greatly exceeding previous expectations due to changes in purposes, techniques and other aspects. In particular, risks have continued to become remarkably more "severe", "widespread" and "globalized" and we are facing a new situation of "increasingly serious risks", which affects not only national security and crisis management but also greatly affects international competitiveness and present a fear of instilling a severe sense of anxiety and insecurity in people.

[More severe risks]

Risks which are a threat to national security as well as the lives, bodies, properties and other interests of people have appeared. The actualization of threats of targeted attacks thought to be aimed at the theft of technological and confidential information from Japanese government institutions, the defense industry, critical infrastructure providers, research institutions and other entities have also been indicated.[17]

[16] Bring Your Own Device. A situation where, in a business or other setting, employees access company information systems by their own private smartphones or other information devices, using their personal information devices to view, edit and otherwise manipulate the required information for work.

[17] For example, in addition to footnote 9, cases where TPP related information may have been leaked from government institutions, cases where issues arose related to the possible theft of technical information, etc.

In these types of incidents, there were cases where the victim was not even aware of the attack and damages, such as cases where at the point they were discovered, the information had already been stolen years earlier.[18] Further, it can also be assumed that even in some cases where damages from cyber attacks were recognized, they were not disclosed in order to prevent even further damages arising and effects on reputation and stock prices. That is to say, the cases that are currently clearly known about are only the tip of the iceberg, and it is possible that critical information related to the maintenance of the nation and businesses is even now still being thieved.

Overseas, cyber attacks aimed at traffic message display signal devices[19] and cyber attacks aimed at systems in critical infrastructures like control systems, with a degree of complexity and sophistication that raises suspicions about the involvement of government level organizations, have occurred and the risk of such attacks causing widespread and far-reaching social turmoil has become a real issue.

In the future, it can be expected that the propagation of SDN[20] in telecommunications infrastructure, ITS in transportation infrastructure and smart grids in power infrastructure will result in a variety of social infrastructure being always connected to networks, and managed and controlled by software. It can thus be hypothesized that there is potential for cyber attacks targeting vulnerabilities in the software of these systems to directly result in obstruction of communications, transportation disorder, blackouts and other large scale social turmoil and possibly even deaths.[21]

from critical infrastructure providers, and cases where problems arose from the possible theft information related to space station specifications, etc. from independent administrative agencies carrying out aeronautical research and development.

[18] For example, cases where the PCs used by employees at government institutions were infected by viruses for several years resulting in leaked information.

[19] For example, in January of 2009, cyber attacks on system vulnerabilities changed the messages on signal devices in several US states to read "Zombies Ahead."

[20] Software Defined Networking. A technique for using software to create a virtual network. Allows for creation of a separate virtual network on top of a physically connected network.

[21] There has been a trend of increasing numbers of incidents each year with SCADA (Supervisory Control And Data Acquisition) which carry out system monitoring and control via computers and other types of industrial control systems, with reports of information security incidents resulting in damages both in Japan and overseas. The IPA "Report on Critical Infrastructure Control System Security and IT Service Continuance" (March, 2009), the Ministry of Economy, Trade and Industry "Cyber Security and Economy Research Committee Interim Report" (August 5, 2011).

[More widespread risks]

While the risks surrounding cyberspace become more severe, the risks are also rapidly becoming more widespread. The rapid propagation of smartphones and other devices among people,[22], expansion of M2M/sensor networks, the advent of conditions where everything is connected to the internet (Internet of Things) and other situations, have increased the spread of the risks by introducing conditions where the devices which can be targeted by cyber attacks are present in every possible place and situation around us.

Smart devices, with advanced processing functions such as smartphones, which are always turned on and connected to the internet while carried around by users, have rapidly propagated among general users. Because these devices, can use public wireless LAN and have because OS structural restrictions limit the effectiveness of security software, there have been cases[23] where users' positional information, address book information, conversational information and other information have been transmitted to external recipients via malicious applications. Offices are also faced with the same threats due to the increasing propagation of BYOD such as smartphones and other devices.

In addition, the propagation of M2M/sensor networks has spread the risks to home electronics, automobiles, multi-functional products such as copy machines, security cameras and variety of other equipment. Devices which had not formerly been intended to be connected to a network now connect to the internet and carry out control and other functions through exchange of information without any human intermediaries, presenting risks that cyber attacks against these devices could cause unexpected and unanticipated operations.

For example, there were cases where DDoS attacks against foreign

[22] Household penetration rate of smartphones is a 20 points over the previous year, a nearly 30% rapid propagation. Ministry of Internal Affairs and Communications "Communications Usage Trend Survey in 2011" (May 30, 2012. Hereinafter "Communications Usage Trend Survey.")

[23] For smartphones, malware has been verified which makes illicit fee collections, captures administrator privileges, makes telephone calls without user input, steals data or eavesdrops on communications via remote operation, transmits the personal information stored in user’s contacts to external recipients, notifies third parties of location information without consent, etc. Ministry of Internal Affairs and Communications: “Smartphone/Cloud Security Research Committee Final Report” (June 29, 2012).

government institutions, etc.,[24] used a security camera installed in a convenience store in Japan as a springboard. It has also been pointed out that there are risks of life related information and positional information including places visited being leaked through cyber attacks targeting home electronics and automobiles connected to the internet, and risks of business related and other information being leaked through use of copiers and other multi-functional devices being used as a hub for information theft in offices.[25]

Moreover, it is not only information systems connected to the internet, but also information networks and other closed, independent systems isolated from external networks such as information networks, which are subject to cyber attacks. For example, the infection with malware of control systems in critical infrastructure through USB memory sticks, resulting in inoperable infrastructure equipment, has become a real issue.[26]

It is not just the above scope of attacks that has broadened, but also the scope of who can carry out attacks in cyberspace. There are tools available which allow even individuals without significant capital or knowledge to easily carry out advanced cyber attacks, creating an environment where even non-specialists can carry out cyber attacks.

[More globalized risks]

The risks surrounding cyberspace are becoming borderless. One third of the world's population is internet users,[27] and the internet continues to propagate in both newly emerging nations as well as developing countries. In Japan, a greater level of handling is required for these borderless, globalized risks as many activities in real-space come to depend upon cyberspace.

For example, in Japan, in DDoS attacks against foreign government institutions overseas, cases have been found that personal owned home PCs

[24] The DDoS attacks against 40 government institutions and other webservers targets which occurred in South Korea in March of 2011.

[25] IPA “Report on Digital Multi-functional Devices in FY2012” (March 12, 2013)

[26] IPA "Report on 'New Types of Attacks'" (December 17, 2010)

[27] As of 2011, the worldwide number of the internet users was 2.265 billion individuals, 32.5% of the global population. The ITU Statistics “Individuals using the Internet per 100 inhabitants, 2001-2011,” & “Global numbers of individuals using the Internet, total and per 100 inhabitants, 2001-2011.”

were used as the springboards for attacks, using the PCs as servers to direct the attacks.[28] In another large-scale overseas case, at the same time as the attacks occurred, the unauthorized programs used in the attacks were also found in Japan.[29] In addition, there were also cases where advanced anonymization techniques using multiple nodes and other devices overseas, resulted in the spoofed PC owners being erroneously arrested.[30]

Overseas, issues have arisen where there is suspicion of the involvement of national governments in targeted attacks aimed at stealing secret information such as trade secrets.[31] It is not unthinkable that cyber attacks against Japan involving the participation of foreign governments could occur in the future. In addition, there are also fears of attacks on one point in a global supply chain affecting other points.

Means to commit cyber attacks can be easily obtained, and in addition to a wide variety of actors, not just nations, carrying out concealment, impersonation and other acts, these attacks can be effected from anywhere in the world. If cyber attacks can be carried out directly to Japan, then they can also be carried out in cyberspaces related to other countries and can be carried out using cyberspaces affiliated with Japan as a springboard for attacks elsewhere. There is still no accepted international common opinion on the relationship between cyber attacks and armed attacks, however the possibility of cyber attacks corresponding to armed attacks being carried out in this way is undeniable.

(2) Past Efforts

[28] In the DDoS attacks against 40 webservers at government institutions, etc. which occurred in South Korea in March of 2011, the household PCs of general users were utilized as springboards for the attack. The National Police Agency “Response to the Cyber Attacks against the South Korean Government Institutions and others in March” (September 22, 2011)

[29] According to the IPA "Computer Virus/Unauthorized Access Report Conditions and Consultation Reception Conditions [1st Quarter 2013 (January – March)] (April 16, 2013)", "Reports on the unauthorized program Trojan/MBRKill (Report name: Trojan.Jokra [2 reports/detections known cases 3]) used in the large-scale cyber attacks against South Korea were received in March 2013. If infected by this unauthorized program, it is possible the hard drive contents will be erased. It is estimated that the same unauthorized program was at least present in Japan at the same time as the occurrence of the damages in South Korea."

[30] Case where general users were impersonated by remote controlling the PCs of general users infected with the "iesys.exe" remote control virus, and their identities used to post massive amounts of death threads on internet bulletin boards and other systems. The advanced anonymizing technique Tor (The Onion Router) was maliciously used in this case.

[31] For example, “the Administration Strategy on Mitigating the Theft of U.S. Trade Secrets” (White House, Feb. 2013) and “the Annual Report to Congress” (Department of Defense, May 2013).

In Japan, the National Information Security Center (Hereinafter abbreviated as "NISC")[32] has been established in April 2005 within the Cabinet Secretariat as the command post for information security policy, to carry out the planning, proposal and general coordination related to planning of basic strategy and other centralized/cross-cutting promotion of information security measures for the public and private sectors. In addition, the Information Security Policy Council (hereinafter abbreviated as the "ISCP")[33] has been established in the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society in May of the same year for centralized/cross-cutting promotion of information security measures for the public and private sectors, and works towards improving the level of information security and strengthening ability to deal with cyber attacks for government institutions and critical infrastructure providers.

In the ISPC, the strategies were determined over the 3 stages comprehensive mid to long term plan, starting with the First National Strategy on Information Security (Hereinafter abbreviated as the "First Strategy").[34]

In the First Strategy, information security is positioned as a national goal consisting of sustainable economic development through the use and application of information communications technologies and the guarantee of safety against threats which arise from such, and promoted the shift from reacting to actualized issues to measures for preventative handling of issues from a viewpoint of forging a solid footing to deal with information security issues. In addition, the plan established a framework for various actors, including government institutions, critical infrastructure providers and business operators, where rather than each actor carrying out their own handling of issues in a vertically divided structure, each actor would maintain awareness of their own responsibilities and appropriately divide roles in accordance with the positions, situations and capacities of each actor.

[32] In accordance with Article 12 of the Cabinet Secretariat Organization Ordinance (1957 Government Ordinance No. 219) "Statute on the Establishment of the National Information Security Center" (Prime Minister, February 29, 2000).

[33] "On the Establishment of the Information Security Policy Council" (May 30, 2005 The Chair of the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society) in accordance with Article 4 of The Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (2000 Government Ordinance No. 555).

[34] February 2, 2006 Information Security Policy Council

The Second National Strategy on Information Security (Hereinafter abbreviated as the "Second Strategy"),[35] the existing preventative measures were steadily promoted while strengthening after the event handling capacities in an "accident assumed society" where promotion of rapid response and measures in the event of an emergency, would ensure business continuity.

While continuing to maintain these measures, the "Information Security Strategy for Protecting the Nation" (Hereinafter abbreviated as the "Strategy for Protecting the Nation")[36] also sets as objectives, from security and crisis management viewpoints, the achievement of capabilities, at the highest standard in the world, to respond to all cyberspace threats, and promotes the handling of environmental changes, such as the occurrence of large-scale cyber attacks overseas, the preparation of a system for managing such situations, and the construction and strengthening of a system for regular collection and sharing of information.

It can thus be said that, since the establishment of information security policy through the First Strategy, the construction of a use an application environment for information communications technologies to promote sustainable economic development and resolve social issues, strengthening of measures from security and crisis management viewpoints and implementation of "accident assumed society" measures, appropriate handling of new environmental changes, and measures based on each of these strategies, have been, in general, realized.[37]

However, cyberspace continues to rapidly expand and penetrate, and the risks surrounding cyberspace continue to increase seriously, becoming more severe, more widespread and more globalized, and as such, an entirely new level of measures is becoming necessary.

(3) Trends in the World

In international bodies such as international conferences, the United Nations,

[35] February 3, 2009 Information Security Policy Council

[36] May 11, 2010 Information Security Policy Council

[37] For example, “Evaluation for Information Security Policy in FY2011” (July 4, 2012 NISC), “Evaluation for Information Security Policy in FY2010” (July 8, 2011 NISC) & “Evaluation for Information Security Policy in FY2009” (July 22, 2010).

regional organizations, and other organizations where a wide variety of public and private actors participate,[38] active debate is being held on codes of conduct for cyberspace, application of international laws and internet governance for acts using cyberspace and other aspects of functions, roles and circumstances of cyberspace.

Other countries are also establishing national strategies on "cybersecurity"[39] in order to deal with the risks surrounding cyberspace from such viewpoints as national security and economic growth. The functions, roles and circumstances of cyberspace have quickly become a common international issue, and as such it is necessary to tackle this issue from a global point of view.

[United States]

In the United States, cybersecurity has been considered one of the most serious economic and national security issues facing the country,[40] and threats related to cybersecurity are treated as the most serious challenges for national security, public safety and economic development in the country's "National Security Strategy."[41] Based on this, the country established strategies for each individual field in 2011.

For example, the country has established the "International Strategy for Cyberspace,"[42] which presents a future vision of international development for

[38] For example, APEC (Asia-Pacific Economic Cooperation) Ministerial Meeting on Telecommunications and Information Industry (October 2010, Okinawa), OECD (Organization for Economic Cooperation and Development) High Level Meeting on the Internet Economy (June 2011, Paris), APT (Asia Pacific Telecommunity) Cybersecurity Forum (December 2011, Tokyo), International Conference on Cyberspace (November 2011, London; October 2012, Budapest), ITU (International Telecommunications Union) World Conferences on International Telecommunications (WCIT. December 2012, Dubai), NATO (North Atlantic Treaty Organization) CCD COE（Cooperative Cyber Defense Center Of Excellence）and The First Committee of the UN General Assembly (in charge of international security affairs and disarmament) " Developments in the field of information and telecommunications in the context of international security" government specialist group (2012-).

[39] At present there is no common definition of "cybersecurity" shared among various nations. For example, the European Network and Information Security Agency (ENISA) "National Cyber Security Strategies - Practical Guide on Development and Execution" (December 2012) states, "There is no uniform definition of 'cyber security' at the EU or international levels".

[40] The Comprehensive National Cybersecurity Initiative (White House, Jan. 2008), The Cyberspace Policy Review (White House, 2009).

[41] National Security Strategy (White House, May 2010).

[42] International Strategy for Cyberspace (White House, May 2011). Activity regions for policies indicated as priority policies requiring domestic and international as well as private and public sector cooperation include (1) economics, (2) protecting our networks, (3) law enforcement, (4) military, (5) internet

cyberspace which supports international trade, strengthens international security, promotes freedom of expression and innovation, is open and interoperable, as well as secure and reliable; the strategy for protecting economic and social values without impeding innovation in the internet business field;[43] the "Department of Defense Strategy for Operating in Cyberspace"[44] which adds cyberspace to the preexisting land, sea, air and outer space regions; and "The Cybersecurity Strategy for the Homeland Security Enterprise",[45] which aims for a cyberspace which supports secure and resilient infrastructure, brings about innovation and prosperity and protects citizen's freedoms such as privacy from the initial design stages, and also plans for the establishment of protections for critical information infrastructure and cyber-ecosystems.

[EU]

In the EU, in addition to natural disasters, terrorism and other situations, new transnational threats of economic espionage or state-sponsored cyber attacks have led to an awareness of the growing frequency and scale of cybersecurity

governance, (6) international development, (7) internet freedom.

[43] Cybersecurity, Innovation and the Internet Economy (The Department of Commerce Internet Policy Task Force, June 2011). Proposals have been made for the following as candidates for "internet/information innovation fields" for small and medium-sized enterprises providing online services and large businesses only operating on the internet, etc. which are not classified as critical information infrastructure: (1) creation of governmental approaches for minimizing vulnerabilities through creation of guidelines, etc., (2) creation of incentives for incident reporting, information sharing, etc., (3) education, research and development, (4) international cooperation including international standardization and sharing of best practices.

[44] Department of Defense Strategy for Operating in Cyberspace (July 2011). The following were indicated as initiatives, (1) Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential, (2) Employ new defense operating concepts to protect DoD networks and systems, (3) Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy, (4) Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity, (5) Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

[45] Blueprint for a Secure Cyber Future - The Cybersecurity Strategy for the Homeland Security Enterprise (Department of Homeland Security, Nov. 2011). The purposes of the strategy for protecting critical information infrastructure are (1) identify and harden critical information infrastructure, avert risk through technical innovation, etc., (2) ensure priority response and recovery by preparing for contingencies, (3) maintain shared situational awareness through information analysis, sharing and specialized cybersecurity training, (4) increase resilience to system failures, and for strengthening the cyber ecosystem are (1) improve literacy through public and private sector personnel training and outreach and awareness raising, (2) reduce vulnerabilities, improve product trust by improving usability, (3) improve interoperability between devices, build collaborative systems through security process automation, etc., (4) widely share information on security hazards, analogous to how information about wellness and disease is reported by public health officials, share information on certified equipment, etc., maintain transparency through incentives and other means.

incidents and the potential they have for inflicting major damage on national safety and economy including interrupting supply in critical services such as healthcare, power supply and automobiles, leading to the establishment of the "Cybersecurity Strategy of the European Union,"[46] which presents a comprehensive future vision related to cyber attack prevention and response, in February of 2013.

This strategy states that in order for cyberspace to remain open and free, the fundamental principles and values of fundamental human rights, democracy and rule of law should be applied in the same manner as offline, while the government should play a critical role in providing protection from incidents and malicious activities.

[UK]

In the UK, "The National Security Strategy"[47] was established in 2010 to promote growth via the internet while recognizing that as critical data and systems become more dependent on cyberspace, these circumstances bring with them new risks consisting of difficulties in detection and defense, and based on this recognition, positions cyber attacks as a threat of the highest priority.

In 2011, in order to respond to the threat of cyber attacks, the country established "The UK Cyber Security Strategy"[48] which presents a future vision enhancing prosperity, national security and a strong society under core values of liberty, fairness, transparency and the rule of law, and which draws considerable

[46] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (European Commission & High Representative of the Union for Foreign Affairs and Security Policy, Feb. 7, 2013). (1) Achieving cyber resilience, (2) Drastically reducing cybercrime, (3) Developing cyberdefence policy and capabilities related to the framework of the Common Security and Defence Policy (CSDP), (4) Develop industrial and technological resources for cybersecurity, (5) Establish a coherent international cyberspace policy for the European Union and promote EU core values, are given as priority items.

[47] A Strong Britain in an Age of Uncertainty: The National Security Strategy (Cabinet Office, Oct. 2010).

[48] The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World (Cabinet Office, Nov. 2011). States (1) Tackling cybercrime and making the UK one of the most secure places in the world to do business, (2) Making the UK more resilient to cyber attacks and better able to protect our interests in cyberspace through strengthening defences in cyberspace and improving ability to detect threats in cyberspace, (3) Helping to shape an open, vibrant and stable cyberspace which the UK public can use safely and that supports open societies through promoting an open and interoperable cyberspace, (4) Building the UK's cross-cutting knowledge, skills and capability to underpin all cyber security objectives through building a coherent cross-sector research agenda, deepening understanding of the threats, vulnerabilities and risks, and increasing ability to respond to incidents, as objectives.

economic and social value from a vibrant, resilient and secure cyberspace.

[France]

In France, "The French White Paper on Defense and National Security,"[49] a strategy on national security presented in 2008, treats cybersecurity as a new vulnerability and a key theme.

In 2011, based on this national security strategy, the "Information Systems Defense and Security Strategy"[50] was established for the purposes of making France a powerful global cyber defense nation, protecting the nation's decision making capabilities by protecting information related to state sovereignty, strengthening the cybersecurity of the nation's critical infrastructure and assuring information security in cyberspace.

[Germany]

In Germany, "The Cyber Security Strategy for Germany"[51] was established in February of 2011 to maintain and promote economic and social prosperity based on an understanding that the availability of cyberspace and the integrity, confidentiality and other factors of data within that cyberspace are among the most critical of issues for the 21st century and that the maintenance of cybersecurity is, both domestically and internationally, a common issue that

[49] The French White Paper on Defense and National Security (Conseil d'État, 2008).

[50] Information systems defense and security - France’s strategy (ANSSI, Feb. 2011). Identifies (1) Effectively anticipate and analyse the environment in order to make appropriate decisions, (2) Detect and block attacks, alert and support potential victims, (3) Enhance and perpetuate our scientific, technical, industrial and human capabilities in order to maintain our independence, (4) Protect the information systems of the State and the operators of critical infrastructures to ensure better national resilience, (5) Adapt French legislation to incorporate technological developments and new practices, (6) Develop international collaboration initiatives in the areas of information systems security, cyberdefence and fight against cybercrime in order to better protect national information systems, (7) Communicate, inform and convince to increase the understanding by the French population of the extent of the challenges related to information systems security, as areas of action.

[51] The Cyber Security Strategy for Germany (Federal Ministry of the Interior, Feb. 2011). Identifies (1) Protection of critical information infrastructures, (2) Secure IT systems in Germany, (3) Strengthening IT security in the public administration, (4) National Cyber Response Centre, (5) National Cyber Security Council, (6) Effective crime control also in cyberspace, (7) Effective coordinated action to ensure cyber security in Europe and worldwide, (8) Use of reliable and trustworthy information technology, (9) Personnel development in federal authorities, (10) Tools to respond to cyber attacks as strategic objectives and measures.

should be jointly handled by the nation, businesses and society.

[Korea]

In Korea, the "National Cyber Security Masterplan"[52] was established in August of 2011 in order to protect cyberspace by attempting to clarify the roles of relevant government institutions and preparing a system for handling cyber threats of a national level, which are becoming ever more intelligent and advanced, based on a recognition that cyber attacks have become a threat to both the people's properties and national security.

2. Basic Policy

(1) Vision to aim as a Goal

As cyberspace is connected globally, it has become critical to secure the sustainability and expansivity of cyberspace aimed at both handling the increasing serious risks surrounding cyberspace and keeping pace with the continued merger and integration with real-space for the national security and crisis management, socioeconomic development, and to assure the safety and security of the people.

For these reasons, Japan aims to construct a "world-leading," "resilient" and "vigorous" cyberspace, and incorporate this cyberspace as a social system to realize a "cybersecurity nation" as a society that is strong against cyber attacks, full of innovations and of which its people will be proud.

[52] National Cyber Security Masterplan – Protecting national cyber space from cyber attacks (National Cyber Security Center, Aug. 2011). Identifies (1) Establishing cyber threat early detection and response system, (2) Improving the level of security for critical information and facilities, (3) Developing platform that would enable a stronger cyber security, (4) Establishing deterrence against cyber provocation and strengthening international cooperation, (5) Elevating the level of security management of critical information and facilities, as major imperatives.

(2) Basic Principles

The basic principles for realizing a cybersecurity nation in Japan are as follows.

① Ensuring free flow of information

Japan has worked towards constructing a safe and reliable cyberspace in which free flow of information is ensured by ensuring openness and interoperability of cyberspace without excessively administering or regulating it.

As a result, cyberspace has provided us a variety of positive benefits including innovation, economic growth and solutions for social issues while still ensuring freedom of expression and protection of privacy.

This strategy also bases its basic principles on this ensuring free flow of information, and is imperative to counter the increasing serious risks surrounding cyberspace.

② Responding to increasingly serious risks

The risks surrounding cyberspace continue to increasingly become serious and immediate response has become necessary. In particular, the existing measures and initiatives that have been implemented in the previous strategies up until now are no longer capable of responding to these more severe, widespread and globalized risks.

If cyberspace is vulnerable to cyber attacks and other threats, it will not only prove difficult to ensure free flow of information, but it can also be assumed that it will make it impossible to maintain people's confidence in cyberspace.

For these reasons, in addition to the individual handling measures up until now, consisting of advance and after the event measures and preparation of response systems, a new mechanism through multi-layered efforts is necessary as a social system that can promptly and appropriately address the changing risks associated with the revolution in information communications technologies and other factors.

③ Enhancing of risk-based approach

Up until now Japan has pursued a policy of having each individual actor, including government institutions, critical infrastructure providers, businesses and individuals, exert the maximum efforts to each handle their own information security for the purpose[53] of elevating the capabilities to deal with all threats surrounding cyberspace to highest level in the world.

However, as the critical information and information systems which need to be protected become more and more dependent on cyberspace, the threat posed by cyber attacks is also increasing as techniques become more complex and sophisticated. In these conditions, it is necessary to continue the measures being carried out by each individual actor, while also dynamically implementing handling with appropriate and timely allocation of resources as a social mechanism for responding to ever-changing risks.[54]

Such actions as improving the recognition and analysis functions for incidents related to cyber attacks, integrating these functions, advancing threat analysis capabilities by promoting information sharing, strengthening of cooperation between CSIRT[55] for each actor and between international CSIRT[56] are all critical, and it is necessary to strengthen risk-based approach based on the characteristics of the risks through dynamically responding capabilities brought about by these actions.

④ Acting in partnership based on shared responsibilities

[53] “The Strategy for Protecting the Nation” states "Concretely, Japan must improve its ability to respond to all types of ICT threats, including cyber attacks, to the world’s highest level" as one of its “Targets to Achieve”.

[54] For example, carrying out quick and well-informed "dynamic defense process collaboration" (OODA loop) through repetition of a pattern of Observe, Orient, Decide, and Act. Refer to the "Proposal for Promotion of Information Security Policy in the Ministry of Internal Affairs and Communications" (April 5, 2013 Information Security Advisory Board).

[55] Computer Security Incident Response Team. A system at businesses and government organizations for monitoring to check if any security issues exist with information systems and for carrying out investigations including cause analysis and extent of impact in the event an incident occurs.

[56] JPCERT Coordination Center (Japan Computer Emergency Response Team Coordination Center, hereinafter abbreviated as "JPCERT/CC") works to further cooperation between both domestic and international CSIRT and carries out incident response.

Diverse entities such as the government, public, academic, industrial and private sectors in Japan have enjoyed the benefit of the expanding cyberspace on which every activity in real-space is dependent.

Accordingly, as the risks surrounding cyberspace have become increasingly serious, it becomes necessary for each entity to carry out their own information security measures in an independent and proactive fashion as part of their social responsibilities to realize a world-leading, resilient and vigorous cyberspace.

Especially, as risks become more widespread, the extent of damages can spread far and wide through cyberspace, and in addition to measures by each individual actor, it is important that the whole of society participated in the "cyberspace hygiene" as a preventative information security measure against unauthorized intrusions, malware infections, vulnerabilities as factors for these incidents and other risks.

In this regard, the multi-stakeholders in cyberspace need to fulfill each responsibilities corresponding to their respective roles in the society while mutually cooperating and assisting with each other including international cooperation and cooperation between the public and private sectors.

(3) Roles of multi-stakeholder

In the previous strategies, each actor would maintain awareness of their own responsibilities and appropriately divide roles in accordance with their positions, situations and capacities. Specifically, information security measures were promoted by indicating the roles and methods[57] expected of the "Measure Implementation Entities," who actually applied and implemented the information security measures for their own, and the "Entities to Promote Understanding and Solutions to Issues," who provided support for the measures

[57] From the First Strategy onward, as a "New Public-Private Partnership Model", a framework was constructed consisting of "Measure Implementation Entities", which in turn consist of (1) "Central Government/Local Governments", (2) "Critical Infrastructures", (3) "Businesses" and (4) Individuals", and "Entities to Promote Understanding and Solutions to Issues", in turn consisting of (1) "Central Government/Local Governments" as Policy Implementing Entities, (2) "Educational Institutions/Research Institutions" including elementary and secondary schools, higher education institutions, research and development institutions and technological research institutions, (3) "Information-Related Businesses" which provide information system construction, communications services and other IT foundation construction and provision, and (4) "Media."

in technical and environmental arrangement aspects and promoted issue understanding and resolution.

In addition to the actors above, from the Second Strategy onward, measures were promoted which also focused on "Entities to Entrust Information," who entrust their own information etc., and "Entities to Maintain Information," who were entrusted with said information etc., seeking to break individual and society away from the pursuit of absolution for the information security,[58] for the establishment of strong “individual” and “society” to spontaneously think issues.

Based on the new situation of the advanced merger and integration of cyberspace and real-space and the increasing serious risks surrounding cyberspace, this strategy seeks to break away from the previous framework based on a premise of each actor existing in a vertically divided structure, and instead indicates the roles of each stakeholder based on a view that each actor dependent on cyberspace is both a measure implementer and at the same time also an entity to promote understanding and solutions to issues.

It is thus imperative to strengthen the dynamic response capabilities of society as a whole by having the wide variety of actors who depend on cyberspace to each continue to perform their own roles while also mutually cooperating and providing mutual aid.

① Roles of government

The government must strengthen the basic functions of the nation related to cyberspace. Specifically, it is necessary for the nation to implement cyberspace crime countermeasures and "defense of cyberspace" to protect the cyberspace related to the nation from cyber attacks involving the participation of foreign governments, etc., beginning with cyberspace related diplomacy such as actively participating in the formation of relevant international rulemaking.

In addition, as an actor which operates information systems containing its

[58] In the Second Strategy "Entities to Entrust Information" "include both parties that actually provide information and parties that may potentially provide information", and "all actors are potential information providers". In addition, "Entities to Maintain Information" "essentially refers to the same scope as "Measure Implementation Entities."

own critical information and implements information security measures closely worked with the promotion of e-government, the nation is responsible for strengthening of measures for government institutions, closely related independent administrative agencies, government affiliated corporations and other similar organizations as well as using those measures to provide leadership and guidance for the measures of other actors. At the same time, the nation must also strengthen and enhance the ability to cope with cyber attacks and work to ensure that damages are minimized in the event government institutions and others are targeted by cyber attacks.

Furthermore, in order to ensure that other actors, including government institutions themselves, can fulfill their roles to the greatest possible extent, the government must work to strengthen the functions of the NISC as a command post, promote collaboration among relevant actors including between ministries, while also proactively preparing new systems, developing advanced technologies, carrying out demonstration project, cultivating high level human resources, improving literacy and others.

② Roles of critical infrastructure providers

Any impairment or disruption of the functions of "critical infrastructure,"[59] which is the basis of people’s social lives and economic activities formed by businesses that provide services which are extremely difficult to be substituted by others, due to cyber attacks and others, has the potential to cause serious damages the lives of people and so on.

For this reason, presently, Japan requires initiatives for "critical infrastructure providers" in the 10 fields of information and communications, finance, aviation, railways, electricity, gas, government and administrative services (including local public authorities), medical services, water and logistics, in accordance with measures in government institutions and others. It is necessary to even further strengthen measures at these and other providers in hereafter.

[59] Defined as "the basis of people’s social lives and economic activities formed by businesses that provide services which are extremely difficult to be substituted by others. If its function is suspended, deteriorated or become unavailable, it could have significant impacts on people’s social lives and economic activities." in the "The Second Action Plan on Information Security Measures for Critical Infrastructures" (February 3, 2009 Information Security Policy Counci, amended April 26, 2012).

In addition, there are fields which have not been considered critical infrastructure within Japan up until now, but for which any impediment or disruption of the information systems for the relevant services, etc., has the potential to have a major effect on the lives of people and socioeconomic activities. Specifically these include smart cities and smart towns, ITS and other transportation control systems and other new network type systems, as well as the defense industry and energy related industries, etc. which are considered critical infrastructures in the United States.[60]

Hereafter, the government must, based on the positioning of the information systems in these fields which have not been considered critical infrastructure up until now, consider the measures for these fields based on the scope of critical infrastructure and the characteristics or each field, and if the scope of critical infrastructure is revised, ensure that the necessary measures are implemented in these systems, etc. which are newly designated as critical infrastructure providers.

③ Roles of private companies, educational institutions and research institutions

Private companies, educational institutions and research institutions possess intellectual property related information such as technological information, financial information, manufacturing technology information and drawings, as well as personal information such as client lists, personnel information and educational information, and other critical information.

There is potential for the socioeconomic development of Japan to be hindered in the event that these critical information, which is also the source of Japan's international competitiveness, is theft, destroyed, etc. as the result of a cyber attacks and others. Consequently, in addition to individual information security measures at private companies, educational institutions and research institutions, collective measures, such as sharing of information, etc. related to cyber attacks through industrial organizations and other hubs, are expected. Furthermore, it is

[60] Applicable to 18 fields and defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" in the Critical Infrastructure Protection Act of 2001.

expected that measures will be improved by obtaining assessments, audits and management standards from third party specialist agencies when each individual actor implements information security measures.

In addition, as the actors serving as the core for technology development and human resource cultivation, it is expected that private companies, educational institutions and research institutions will work together in industry-government-academia collaboration to provide the advanced technologies and high level human resources that will constitute a world-leading, resilient and vigorous cyberspace in Japan.

④ Roles of individual users, small and medium-sized enterprises

General users and small and medium-sized enterprises, which make up the majority of businesses in Japan[61] and serve as the core of the supply chain make practical use of new information communications technology services every day in order to improve convenience, make operations more efficient and speed up service provision and others.

Fact such as approximately 80% of the total population are internet users[62], and the internet usage of all businesses is nearly 100%,[63] show that the scope of requirement for information security measures is extremely wide, however the such devices as smartphones and PCs used by general users, etc. are security holes and if targeted by cyber attacks, have the potential to inflict damages on other stakeholders through cyberspace.

Up until now, measures for general users have been carried out through independent effort. Hereafter, it is important that in addition to the understanding that "they are responsible for protecting themselves,"[64] general

[61] According to the Ministry of Internal Affairs and Communications "2009 Economic Census – Basic Study," the number of small and medium-sized enterprises (number of companies and sole proprietorships) is 4,201,000 businesses, making up 99.7% of all businesses, and the number of small and medium-sized enterprises is 1,775,000, making up 99.3% of all companies.

[62] According to the Communications Usage Trend Survey, the number of individuals estimated to have used the internet in 2011 was 96,100,000, making up 79.1% of the total population.

[63] According to the Communications Usage Trend Survey, the business internet usage rate at the end of 2011 was 98.8%.

[64] In the First Strategy, for the roles of individuals as Measure Implementation Entities it is stated "it is necessary to cultivate awareness about information security to the same level as a general safety rule like 'you should not talk to strangers'. Individuals are expected to act with clear recognition of basic principle of

users must also make efforts to implement measures based on an awareness of "not bothering others."[65] As such, it can be expected that among general users, there will be continued utilization of the activities of each actor, and that fomenting this awareness and improving literacy will lead to autonomous implementation of measures.

In addition, for those small and medium-sized enterprises which are involved in the handling of Japan's critical information and systems through such relationships as contracts with critical infrastructure providers or businesses with leading-edge technology, etc., in addition to each business' individual information security measures, measures for sharing information related to cyber attacks, etc. are expected.

⑤ Roles of cyberspace-related operators

The majority of the device manufacturers, internet access providers, network operators, software developers and other organizations responsible for the equipment, networks, applications, etc. that make up cyberspace, are private sector. In addition, the majority of organizations responsible for providing the tools for handling risks surrounding cyberspace are also private sector.

In the strategies up until now, the "information related businesses", which actually provide direct tools to each entity for the implementation of information security measures, have been responsible for eliminating any vulnerabilities in the products and services they provided to the greatest extent possible, in addition become positioned increasingly as important actors from a viewpoint of providing safer, more reliable products and others to improve international competitiveness.[66]

protecting themselves on their own."

[65] The message of the Director of the Secretariat during the implementation of International Cyber Security Campaign of September 28, 2012, states, "Being lax about information security measures does not result in damages to just yourself, but also to other people. Use smartphones and computers safely and in peace of mind by steadily implementing information security measures."

[66] The First Strategy states, "Information-related businesses are ones that actually provide direct services to central government and local governments, critical infrastructures, businesses, and individuals for the implementation of measures, and assume a role to help the enhancement of information security infrastructure of Japan. Therefore, they need to re-acknowledge that they are responsible for eliminating the vulnerability of their products and services as much as possible and make efforts to offer safer and more secure products and service. In doing so, the information-related businesses should have a positive

However, it is difficult to eliminate all software vulnerabilities in products, etc., during the development stage, and it is difficult to handle every aspect of the risks diffused through cyberspace, upon which various actors depend, simply through measures implemented by each actor, such as general users.

Accordingly, it is expected that in addition to the "cyberspace-related operators", who provide the products, services, technologies, etc. related to cyberspace, endeavoring to ensure that no vulnerabilities are created in these products, services, technologies, etc. at the time of development, that they will also implement measures to maintain the cyberspace hygiene by preventing the spread of damages through eliminating vulnerabilities by implementing appropriate countermeasures when such vulnerabilities are discovered after development and by such measures as recognizing and analyzing incidents related to cyber attacks.

In addition, at present there is a large degree of dependence on foreign providers for products etc. related to information security measures., and a shortage of security personnel within Japan, and thus it is important for cyberspace-related operators to create a market through development of advanced technologies and products, cultivation of human resources with high abilities and the use and application of these resources for information security measures in order to strengthen the international competitiveness of Japan's "cybersecurity industry" .

3. Areas of Efforts

In order to construct a world-leading, resilient and vigorous cyberspace, and realize a cybersecurity nation, the government will continue to implement measures appropriate to an "accident assumed society" , continue to collaborate with other actors domestically, and relevant other countries and international organization, etc. and promote the measures stated below in the 3 year period until FY2015.

Specific objectives for proceeding with the following measures include

perspective that the provision of safe and secure services would eventually lead to the improvement of their international competitiveness."

increasing the coverage of cyber attacks related information sharing networks in government institutions and critical infrastructure fields, improving CSIRT installation, malware infection[67] and people's anxieties,[68] in addition increasing the number of nations possible of participating in international incident coordination[69] and the numbers of partners such as nations for international collaboration and dialog on response to cyber attacks by 30% increase by FY2015. Also, doubling the size of domestic information security market[70] and halving the deficiency ratio in security professionals as goals for 2020.

In addition, as cybersecurity has become a common global issue, it is necessary to investigate and analyze overseas trends in policy, etc. related to cyber-attack incidents and cybersecurity while also exchanging information and carrying out other collaboration with various other foreign governments and countries when implementing the following measures.

The government will revise the "Groups of Standards for Information Security Measures for Central Government Computer Systems",[71] "The Second Action Plan on Information Security Measures for Critical Infrastructures" (hereinafter abbreviated as the "Second Action Plan"),[72] the "Information Security Research and Development Strategy",[73] the "Information Security Human Resource Development Program"[74] and the "Information Security Outreach and Awareness Program"[75] and other policy documents, establish new

[67] For example, in Microsoft's "Security Intelligence Report", a CMM (Computers Cleaned per Mille. Indicates the number of PCs for which malware or unwanted software was removed per 1,000 executions of malicious software removal tools.) index is used to compare the conditions of various countries throughout the world. Japan's infection rate for the year of 2012 was 1 or less (0.7-0.9).

[68] For example, in the White Paper on Information and Communications, in regards to anxiety about internet usage, in 2011 the rate of household respondents who answered "I am worried about virus infection" was 72.8% and the rate of business respondents who answered "We have concerns about virus infection" was 41.4%, the highest ever for either of these responses.

[69] For example, currently at JPCERT/CC , there are approximately 80 countries with whom direct cooperation for incident coordination can be carried out between contact CSIRT.

[70] For example, in current conditions, the scale of the Japanese information security market (products and services) is 5,853,000,000 dollars (2010), 2nd place following the United States, making up 0.107% of Japan's GDP for 2010), a level closely matching that of the United States and the UK. In addition, in regards to the structure of the market, in Japan the market for services (4,425,000,000 dollars) is largest than the market for products (1,428,000,000 dollars). The Ministry of Economy, Trade and Industry "Information Security Market Survey."

[71] Includes the "Standards for Information Security Measures for Central Government Computer Systems" April 21, 2011, Information Security Policy Council, Amended April 26, 2012), etc.

[72] February 3, 2009 Information Security Policy Council, amended April 26, 2012.

[73] July 8, 2011 Information Security Policy Council

[74] July 8, 2011 Information Security Policy Council

[75] July 8, 2011 Information Security Policy Council

plans, etc. as is necessary.

(1) Construction of "Resilient" Cyberspace

In order to maintain the sustainability of cyberspace, in addition to reinforcing measures for responding to cyber attacks, Japan aims to construct "resilient" cyberspace and enhance its defensive and recovery capabilities against cyber attacks and other cyber incidents by improving such functions as for recognition and analysis of cyber attacks and for information sharing related to incidents .

① Measures in government institutions

Government institutions and other related organizations will improve the level of information security related to information and information systems and also strengthen and enhance its preparations to cope with cyber attacks.

[Improvement of the level of information security related to information and information systems]

A unified mechanism shall be strengthened at government institutions in order to emphasize information security measures according to their degree of importance and other factors for information such as state secrets and information systems, by establishing risk assessment methods related to management of cyber attacks such as targeted attacks. Further, an environment will be arranged to assure appropriate information security suited to the diverse working arrangements of government employees, including telework and BYOD, while continuing to adhere to disciplines. Additionally, usage of SNS will be allowed when providing important information to people with Japan bearing responsibility and enforcing discipline.

The government shall strengthen the measures for its government-wide information system. Specifically, a government information system infrastructure which is resilient against cyber attacks and large scale disasters shall be constructed through such measures as converting government information systems into the government common platform as its cloud computing service.[76] Moreover, for the social security and tax number systems, strengthening of information security shall be promoted for the information sharing infrastructure system and related systems[77] managed and operated by government institutions, local authorities and related organizations. In addition, measures shall be implemented to assure information security for promoting open data in e-government.[78]

For government institution information systems, information security technological standardization and results of conformity with such are required at the design, manufacturing, installation and other stages, and strengthening of measures for existing known but unresolved vulnerabilities, use of compromised technologies, malware embedding and other supply chain risks. Specifically, these should be examined within the scope of approved in international agreements for the conditions of government procurement including utilization of conformity assessment systems based on international standards[79] and application of required measures for assuring national security[80] in the Agreement on Government Procurement. The use of technologies which have undergone safety assessment[81] shall be promoted for encryption technologies. Additionally, information security measures shall be promoted in close collaboration with promotion of e-government.

Information security shall be strengthened for handling of the critical information on national safety by operators other than the government institutions. For this type of information, information security conditions are guaranteed for outsourcing to information processors, standard procurement and

[76] Began operations starting in March 2013.

[77] "Act Related to the Usage of Numbers for Identification of Specified Individuals in Administrative Procedures" (Number System Act) established at the Diet on May 24, 2013.

[78] "E-Government Open Data Strategy" (July 4, 2012, IT Strategic Headquarters).

[79] An example of IT security evaluation and certification schemes for international trade is CCRA (Common Criteria Recognition Agreement).

[80] WTO Agreement on Government Procurement. One of several agreements attached to the WTO agreement which came into force in January of 1995, binding only for the WTO member nations who separately ratified it. Exclusions of application are prescribed in Article 23 for cases of protecting serious profits for reasons of national security, etc.

[81] The " e-Government Recommended Ciphers List" (CRYPTREC (Cryptography Research and Evaluation Committees) Ciphers List) was decided in March of 2013 through assessment of the encryption technologies used in e-Government in the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry.

subsidiary businesses,[82] however in addition to this, reporting of incident information related to cyber attacks to the ordering ministries and sharing of information between the operators shall be promoted. In addition, a framework shall be constructed allowing for the utilization of risk assessment methods in the above-noted government institutions.

For independent administrative agencies, government affiliated corporations and other entities with a close relationship to the government, information security will be strengthened for supply chain risks based on government institution measures. Reporting of incident information to ministries with jurisdiction over the entity, voluntarily reporting to ministries handling the case and sharing of information with related institutions shall be promoted in order to prevent spread of damages while strengthening functions for recognizing cyber attacks related incidents.

[Strengthening and enhancement of preparations to cope with cyber attacks]

Drastic improvements shall be made to capabilities for recognizing and analyzing cyber attacks at government institutions, etc. and countermeasures in the event of incidents shall be strengthened and enhanced.

Specifically, the GSOC[83] shall be fundamentally strengthened, and items subject to monitoring expanded further, technologies and organizational frameworks shall be prepared for effective collection and advanced analysis of incident information from monitored sites, and a system will be prepared to use the results of attack method analysis etc. in order to improve risk assessment methods above mentioned. In addition, a system shall be established to share the collected incident information, analysis results and other information with government institutions being monitored, as well as with critical related institutions such as critical infrastructure providers.

[82] "Regarding Notation of Information Security Requirements in Procurement" was released to the various ministries, etc. on January 24, 2012 based on the results of the studies of the "Subcommittee for Strengthening Public-Private Collaboration" established in the Information Security Measure Promotion Council (CISO Council) which is in turn established in the Information Security Policy Meetings.

[83] Government Security Operation Coordination team. Formed in order to strengthen government institutions capability to deal with emergencies related to information security issues such as external cyber attacks and put into operation in April of 2008.

The collaboration among the GSOC, the CYMAT[84] and the CSIRT of each government institution at the time of incident occurrence shall be strengthened in order for immediate sharing of incident information and a full readiness system by the government together. In addition, in anticipation of large-scale cyber attacks[85] and these possibilities countermeasures for the occurrence of incidents, such as initial response training, have been established[86] in Japan already, and attempts have been made to strengthen information collection and aggregation systems for both normal and incident occurrence circumstances. Hereafter, further strengthening of countermeasures, such as annual implementation of training for handling of large-scale cyber attacks with participation of relevant government institutions and other related entities shall also be carried out.

In addition to strengthening the handling capabilities of the government for both normal and emergency situations, it is also necessary to engage in the securing and cultivation of human resources in order to promote international collaboration. Specifically, proactive employment of outstanding external human resources, promotion of personnel exchanges between public and private sectors and among ministries, and improvement of continual development of capabilities through personnel rotations. Additionally, the cultivation such as trainings of the personnel in both the CSIRT in each government institution, etc. and the CYMAT should be strengthened in order to carry out prompt and precise response.

While information gathering activities are actively carried out against Japan, recently methods of using targeted attacks by email to steal information from government institutions, etc., have become more complex and sophisticated, and the risks of critical information in government institutions being leaked is

[84] CYber incident Mobile Assistant Team (Information security emergency support team). Established in the NISC in June of 2012, and provides technical support and advice related to preventing spread of damages, recovery, cause investigation and recurrence prevention in the event of cyber-attacks against ministries or other agencies under the National Information Security Center director who is the government CISO.

[85] Refers to cyber-attack conditions or potential conditions which result in serious harm to the lives, health or finances of citizens, or to national territory, or poses the thread of causing such harm. For example, conditions such as cyber-attacks resulting in injury or loss of life or serious interruptions in the supply of critical infrastructure services.

[86] Based on "The Government Initial Response System for Emergencies" (November 21, 2003, Cabinet decision), "The Initial Response for Large-scale Cyber Attacks" (March 19, 2010, Deputy Chief Cabinet Secretary for Crisis Management) etc.

increasing. Therefore construction of a stronger information assurance system is necessary by such measures as intensified cooperation with foreign institutions while greatly promoting measures for gathering, analysis and sharing of counter-intelligence related information in cyberspace with each government institution working closely.

② Measures in critical infrastructure providers

In the critical infrastructure field, it is necessary to ensure that people's lives, socioeconomic activities, government activities and all activities can stably and reliable continue, and thus it is necessary to implement information security measures in accordance with such as government institutions do based on the characteristics of the information systems requiring protection.

Specifically, for critical infrastructure, in order to focus on information security based on risk assessment methods for critical infrastructure providers and other related organizations, it is necessary to extract risks desirable to take measures in a cross-cutting fashion across fields through understanding and assessment of the establishment and changes of the latest safety standards in each infrastructure field[87] and through risk analysis, and to establish processes to reflect these results in the guides[88] for safety standards in each field.

The sharing such information as failures, cyber attacks, threats and vulnerabilities between critical infrastructure providers and CEPTOAR[89] shall be continuously promoted. About information on targeted attacks for which sharing across industries is difficult, a confidentiality agreement-based information sharing system shall be developed and expanded.[90] In addition, for

[87] "Safety standards" refers to documents specified as reference materials or standards when critical infrastructure providers make determinations and carry out actions (The Second Action Plan).

[88] "Guides" refers to "Principles for Formulating of 'Safety Standards, Guidelines, etc.' concerning Assurance of Information Security of Critical Infrastructures" and the "Countermeasures Edition" of the same as well as follow-up documents.Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR). System for sharing and analyzing information in the 10 critical infrastructure fields.

[89] Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR). System for sharing and analyzing information in the 10 critical infrastructure fields.

[90] For example, the J-CSIP：Initiative for Cyber Security Information Sharing Partnership of Japan, is a measure by IPA and private organization for the countermeasures against targeted cyber attacks as measures related to critical infrastructure providers.

rapid reporting by critical infrastructure providers to the ministries with jurisdiction over their places of business, voluntarily reporting to ministries handling the case, and information sharing with related organizations, promotion shall be carried out with regard for personal information and confidential information. Moreover, promotion shall be carried out for cyber exercises between critical infrastructure providers, cyberspace-related operators and such related entities as relevant CSIRTs based on a premise of confidential relationships between private organizations, in order to strengthen collaborative response capabilities for cyber attacks.

In addition to strengthening handling of supply chain risks in critical infrastructure fields, it is also important to introduce evaluation and certification of information security. Specifically, promotion of collaboration through information sharing of vulnerability information and attack information, etc. between critical infrastructure providers and cyberspace-related operators, examination of how to introduce evaluation and certification modeled on international standards for procurement and operation of SCADA and other control system equipment and systems, and promotion of measures aimed at establishing institutions for evaluation and certification of control system equipment and systems.

There are fields which are not currently considered critical infrastructure fields in Japan, but for which any failure of the information systems has the potential to have as a great an effect on the lives of people and socioeconomic activities as any such failure in the existing 10 critical infrastructure fields. Hereafter it is necessary to examine the scope of critical infrastructure and measures according to the characteristics of each field based on the positioning of the information systems in the relevant infrastructure.

Based on the above, a new action plan will be determined once the Second Action Plan is reviewed.

In addition, on the assumption of large-scale cyber attacks countermeasures for the occurrence of incidents, such as initial response training, have been established in Japan already, and attempts have been made to strengthen information collection and aggregation systems for both normal and incident occurrence circumstances. Hereafter, in order for the public and private sectors to be able to collaborate and carry out appropriate measures in the event of large-scale cyber attacks, further strengthening of countermeasures, such as annual implementation of training for handling of large-scale cyber attacks shall also be carried out by relevant parties, using cases in other countries as reference where necessary.

③ Measures in private companies, educational institutions and research institutions

Recognition and analysis capabilities for such incidents as cyber attacks while sharing of such information shall be strengthened at private companies, educational institutions and research institutions which handle critical information such as important trade secrets and other business secrets, intellectual property information and personal information, which is the source of Japan's international competitiveness. In addition information security measures at overseas destination of the businesses shall be promoted.

For small and medium-sized enterprises, for which the ensuring of information security specialist personnel and sufficient investment is becoming difficult, it is necessary to arrange an environment for strengthening such cyber attack related functions as incident recognition capabilities. Specifically, systems will be arranged for sharing of information and consultations between small and medium-sized enterprises, tax systems which promote information security investment and other incentives will be examined, guidelines and tool which are easy to use to improve information security will be prepared, and transition to a common usage system with guaranteed information security by such technologies as cloud computing will be promoted.

In addition to promoting the analysis of information on incidents recognized at small and medium-sized enterprises as well as sharing of countermeasure information etc., implementing practical defense exercises which examine defense models for cyber attacks and utilize practice test beds for not just large scale companies but also for small and medium-sized enterprises and so on, will improve capability to respond to and deal with cyber attacks.

Capability to respond dynamically in the event of incidents to prevent the spread of damage will be improved at private companies, research institutions and other related organizations, construction of CSIRTs will be promoted, and the capability to respond collaboratively between CSIRTs will be strengthened.

As management uncertainty increases for businesses as a result of intensifying of the risks surrounding cyberspace, for the possibility and other factors of incidents related to cyber attacks in listed companies, the possibility of disclosing business risks to investors will be examined while continuing to give consideration to maintaining fair competitive conditions. During this examination, the potential and conditions for a framework for promoting incentives to disclose including sharing relevant information, will also be considered.

In addition, for educational institutions, in order to reduce the work, increase efficiency and improve the quality of educational activities in elementary and middle school education, the usage and application of information communications technologies continues to progress as a result of increased informatization in such fields as school affairs. Therefore propagation and education related to information security will be promoted to the actors responsible for establishing schools such as local public authorities in order to assure information security, including response to cyber attacks.

④ Cyberspace hygiene

As the merger and integration of cyberspace and real-space continues, it is becoming more important for preventative measures to be implemented against unauthorized intrusions, malware infections, and other events by the various actors who mutually depend on cyberspace. However, as risks continue to increase seriously, it is becoming more difficult for general users such as individuals to carry out measures through independent efforts alone, and the active support of other actors is necessary to reinforce those measures.

For comprehensive and intensive outreach and awareness raising aimed at cultivating awareness in general users such as individuals and businesses, relevant events are held as part of "Information Security Awareness Month", which is held in February of every year, and the "International Cyber Security

Campaign", held in October of every year. Hereafter, in addition to carrying out measures throughout the entire government, measures will be carried out aimed at fomenting an increased awareness in general users in order to make cyberspace hygiene a national movement as one part of this endeavor, such measures will include, for example, coordination with software education, which forms the basis of information security, such as the Open University of Japan "Informatics Course,"[91] issuing of awards for distinguished services as a part of newly established "Cyber Clean Day" (provisional name).

Further, for daily effective outreach and awareness, in addition to carrying out such measures as promotion for collection of vulnerability related information and cooperation with various internet fixed point observation systems, frameworks will be examined for visualizing the degree of vulnerability of Japan's cyberspace, degree of malware infections and other overall trends, as well as for carrying out appropriate outreach to general users.

It is necessary to improve the capability to respond to attacks for cyberspace as a whole, and provide effective precautions and other useful measures to general users through cooperation between government institutions and cyberspace-related operators and improvement of functions for recognizing and analyzing cyber attacks related incidents. Specifically, through such activities as the "Cyber attacks Analysis Council,"[92] in addition to mobilizing each institution's specialist capabilities and collected information and carrying out advanced analysis while maintaining the confidential relationships with the incident information providers and other related players, capability to respond to cyber attacks will be strengthened by utilizing the information in carrying out various measures, for example, individual incident handling, providing precautions to general users, examination of mid to long term countermeasures and research and development.

[91] The Informatics Course has been established, starting from April of 2013, in order to provide students with the skills to solve problems from an information point of view in addition to learning on information processing, from the 5 areas of software, information mathematics, multimedia, human interface and intelligence infrastructure.

[92] Composed of the Ministry of Internal Affairs and Communications, the Ministry of Economy, Trade and Industry, the National Institute of Information and Communications Technology (Hereinafter abbreviated as "NICT"), the IPA, Telecom-ISAC Japan, and JPCERT/CC in order to implement the advanced analysis necessary for defense against cyber-attacks.

As countermeasures against network type bot viruses, at the CCC,[93] which is a public/private partnerships implemented with the cooperation of ISPs,[94] measures were carried out to provide general users with precautions. Hereafter, a framework will be constructed for the implementation by ISPs and other related entities of the creation of a database for storing information on malicious sites which distribute malware and providing precautions to general users who attempt to access malicious sites and other measures. In addition promotion will be carried out for advancement of database functions including strengthening of functions for detecting malicious sites.

For the behavior of potential malware, in addition to carrying out development of technologies for quick and advanced detection, based on the increased complexity and sophistication of cyber attacks and other increasing serious risk surrounding cyberspace, examinations will be carried out on flexible operations of relevant systems with consideration for confidentiality of communications and other interests such as the potential for communication analysis for information security purposes.

In an environment where components of home information appliances, medical equipment, automobiles, and social infrastructure such as communications networks are controlled by embedded software, there is a potential threat to people's lives if there is any troubles such as failures in these software. Taking these conditions into account, and while attempting to maintain international coordination, in addition to examining systems for handling vulnerabilities in software related to these items, promotion will be carried out for strengthening of the explanatory capabilities for software quality so that cyberspace-related operators who provide these devices and services are able to provide users with sufficient explanations of software quality.

⑤ Crime Countermeasures for Cyberspace

In order to be able to respond to the various situations that may potentially

[93] Cyber Clean Center. Implemented as a project from FY2006 to FY2010 through the cooperation of the Ministry of Internal Affairs and Communications, the Ministry of Economy, Trade and Industry, Telecom-ISAC Japan, JPCERT/CC and the IPA.

[94] Internet Service Provider. Internet connection service providers who provide internet connections to general user and business customers utilizing fiber optic lines and other means.

occur in cyberspace in the future, it is necessary to strengthen the countermeasures against cyber attacks which may affect the national security and crisis management by strengthening capabilities to deal with cybercrimes and utilizing the knowledge and capabilities of private sector operators.

Specifically, in addition to strengthening investigative and analysis capabilities through the employment of personnel with specialized knowledge and capabilities and carrying out effective education and training and research on new technologies, system preparation will be carried out through expansion of organizations such as the Cyber Attack Analysis Center, the Cyber Attack Special Investigations Unit and the Unauthorized Program Analysis Center, information collection and analysis equipment will be enhanced and strengthened and preparation of equipment including the advancement of internet monitoring systems, will be carried out.

For strengthening of measures utilizing the knowledge and capabilities of private sector operators, starting with the creation of the Japanese NCFTA,[95] new information sharing frameworks will be constructed with anti-virus vendors related to new types of viruses, measures for sharing information through cooperation with the private sector, including the "Council to Prevent Unauthorized Communications as a Cyber Intelligence Measure,"[96] shall be strengthened, and cooperation related to sharing of technical information for electronic devices subject to analysis will be strengthened as means of promoting information sharing. Moreover, in addition to promoting joint private and public sector cybercrime prevention measures, such as strengthening cyber patrols and promoting measures to prevent damages related to smartphone

[95] National Cyber-Forensics and Training Alliance. A non-profit organization established in the United States and made up of members from the FBI, private sector businesses and academic institutions. Carries out training of personnel for investigatory agencies, including those overseas, related to cybercrime related information collection and analysis.

[96] In addition to the "Council to Prevent Unauthorized Communications as a Cyber Intelligence Measure", which carries out sharing of information, etc., related to cyber attacks thought to be planned to steal information from operators providing services for dealing with security matters or security monitoring services, other examples include the "Cyber-terrorism Countermeasures Council", provides information related to cyber-terrorism from the police, talks by private sector experts, opinion exchanges between member operators and information sharing and is composed of critical infrastructure providers and other members from every prefecture. In addition, the "Cyber Intelligence Information Sharing Network" has been formed as a network for sharing information related to cyber-attacks thought to be planned in order to steal information, and the "Unauthorized Program Countermeasures Council" has been established to carry out sharing of information related to unauthorized program countermeasures between anti-virus software providers, etc.

applications, efforts will also be made to utilize private sector knowledge and capabilities in investigations such as commission of method analysis to private sector operators.

Consideration will be given to measures for preserving logs such as communication histories, and promotion of digital forensics at relevant operators in order to assure traceability for cybercrimes after the fact. Regarding saving of communication histories in particular, consideration will be carried out on their use in cybercrime investigations with due consideration given to the confidentiality of communications, types of effective communication histories for security, burdens of the communications operator saving the logs, storage periods of logs in foreign countries, and the diverse opinions of people as general users,.

For criminal investigation and police fields, systems for control and other functions will be strengthened through human resource development and other means in order to appropriately deal with cybercrimes.

⑥ Defense of Cyberspace

It is important for Japan to strengthen overall response capabilities for the event of targeted attacks aimed at theft or destruction of critical information such as national secrets, cyber attacks carried out as part of an armed attack by foreign governments[97] and other national level cyber attacks for which the involvement of foreign governments is suspected.

Specifically, in addition to clarification of the roles of institutions and strengthening of systems related to functions such as recognition of incidents related to ordinary cyber attacks, collection and sharing information such as incident information, and advanced analysis of collected and shared information which can contribute to the identification of the actors behind attacks, the collaboration between these institutions shall be strengthened.

Cyberspace is a new "domain" just as land, sea, air and space in which a

[97] The Prime Minister's response to the Lower House plenary session on March 4, 2013 stated, "a variety of discussions and debated are still ongoing regarding the relationship between cyber attacks and an armed attack and others, and it is difficult to provide a categorical answer at this time."

variety of activities, such as intelligence, offence and defense, are carried out by organizations such as the Self Defense Force and the effective use of this domain is important, and as a vital infrastructure which support various activities in the actual domain such as land, utilized for policy making and unit mobilization and other tasks, the secure use of cyberspace is critical.

Above all, in the event that cyber attacks are carried out as part of an armed attack, the Ministry of Defense and the Self Defense Force are tasked with responding to these, and in order to execute this, the Self Defense Force must first ensure that appropriate measures against cyber attacks are implemented on its own systems. Specifically this means implementing measures aimed at strengthening the Self Defense Force's capabilities and preparedness in cyberspace, including improving of surveillance abilities in DII[98] networks, realistic exercises in an environment that simulates conditions of the MOD systems, alert capabilities by improving such functions as of the security and analysis devices for cyber defense, establishing organization through the new addition of a Cyber Defense unit (provisional name), steadily retaining talented personnel with advanced expertise, and carrying out advanced research and development.

The roles of the relevant organizations during times of emergency including the way of mutual support shall be arranged, for example, the roles of the Ministry of Defense, the Self Defense Force and other government institutions regarding cyber attacks against such information systems as critical infrastructure systems other than defense related systems, and the roles of cyberspace-related operators regarding unauthorized communications from overseas, while preparation of organizations, frameworks for sharing of information including classified information and systems shall be carried out. During this examination, the application of individual specific international laws will be considered.

(2) Construction of "Vigorous" Cyberspace

In order to maintain the expansivity of cyberspace, Japan aims to construct

[98] Defense Information Infrastructure.

"vigorous" cyberspace through the activation of industry which plays a central role in responding to cyber attacks, developing advanced technologies, carrying out training and fostering of human resources and literacy, and other measures, and aims to strengthen the creativity and knowledge which will allow it to independently respond to the risks surrounding cyberspace.

① Activation of industry

In order to promptly and appropriately respond to new risks while taking in new growth markets and gathering information on cyber attacks and other useful information in overseas markets, it is necessary to strengthen the international competitiveness of Japan's cybersecurity industry, which is highly dependent on foreign technologies, services and products.

Advanced technology, products, and services and the leading researchers and technical experts who create them constitute vital infrastructure for the propagation and advancement of information communications technologies as well as the development of their use and application. As the usage and application of information communications technologies becomes more important in the improvement of innovation and productivity in a variety of fields through the expansion of the base of information communication technologies utilization and in the use of big data to create new businesses, advanced research and development on information security as an integral part of these utilization and preparation of systems including international standardization and evaluation and certification, are necessary.

Specially, efforts will be made to strengthen research and development in such as M2M-based smart community, smart grid, smart city and smart town related information security technologies, advanced secure device technologies for promoting new services utilizing personal data, anonymization and encryption technologies, technologies for controlling entire networks through large quantities of various types of data by software, and technologies for identifying individuals in cyberspace.

Hereafter, products and services which utilize information communication technologies will be faced with requirements for cybersecurity related reliability in international transactions, and it can be assumed that the importance of international standardization, evaluation and certification, and information security auditing will grow in order to provide proof of this reliability. For this reason, it is necessary for Japan to proactively participate in and work on international standardization and the creation of international mutual recognition frameworks for evaluation and certification[99] in order to ensure that Japan's businesses are in an advantageous position in international trade.[100] In addition, it is necessary to support related private sectors and to develop a function for evaluation and certification in Japan. Specifically, progress should be made in international standardization of cloud computing services, enactment of common international security requirements for multi-functional devices, and preparation of evaluation and certification bodies for industrial control systems focusing on security verification facilities.[101]

Having the government proactively carry out the procurement of products which utilize new technologies promotes private sector businesses, product development, practical application and acquisition of overseas markets while also fostering venture businesses. In addition, promotion will be carried out for cooperation which overcomes the boundaries between industry and organizations and global development of businesses with latent potential in order to have companies in Japan which are strong enough to stand on an equal footing with global competition in the cybersecurity field.

The clarification of the application of copyright laws regarding reverse engineering for security purposes, and the reform of laws and regulations which may hinder industrial activation such as the realization of advanced services through analysis of big data, are critical.

② Research and development

The risks surrounding cyberspace are expected to change rapidly as a result of

[99] For example, footnote No.79.

[100] ISO/IEC 27001 Information Security Management System (ISMS) is a major cyber security international standard and approximately 4,000 organizations have been certified in Japan in the 10 years since 2002.

[101] The Technological Research Association Control System Security Center (CSSC) was established on March 6, 2012.

the increasing complexity and sophistication of cyber attacks, and preexisting information security measures may result in delays in establishment and implementation of effective measures and suffer from rapid decreases in efficacy. For this reason, it is important to create information security technologies that are creative and imaginative to counter these changing risks.

Specifically, for the purposes of Japan maintaining and improving its own leading research and development, the research and development and practical testing of technologies aimed at improving the cyber attack detection and advanced analysis functions at research institutions and relevant organizations[102] shall be accelerated.

In particular, in addition to introducing theoretical approaches to information security research such as encryption research in order to allow for the establishment of effective and innovative technologies for dealing with the diversifying and more advanced cyber attacks, such as latent malware. In addition development will be carried out on leading technologies for countering near future cyber-attacks. Development of semiconductor devices which support security is also important.

Further, in order to protect people's information and rights, social systems, leading technologies aimed at establishing information security measure technologies related to inhibiting IC operation errors will be developed. Research and development will also be carried out on technologies for assuring the reliability of entire network systems which include the various individual data of which big data is realized through the propagation of SDN, as well as the software used to process these data.

The knowledge obtained through this research and development will be shared between industry, academia and the government, and used to promote the improvement of Japan's defensive capabilities. In addition, these measures can also be expected to contribute to the cultivation of advanced information security personnel throughout all of Japan, and because these technologies could potentially become something that could be deployed worldwide, this could also

[102] For example, "CYREC" (CYbersecurity REsearch Center), a cybersecurity research and development base collecting information from all of Japan, was constructed and put into full operation in April 2013 aimed at improving analysis capabilities at the NICT.

lead to the creation of a new industry starting in Japan, leading to economic growth.

③ Human resource development

In these conditions where all of Japan's activities are dependent on cyberspace, it is difficult to handle increasing serious risks simply through the cultivation of human resources to carry out countermeasures to protect one's own organizations at measure implementation entities such as the government institutions and businesses. As such, it is necessary to widen the base of these advanced and international personnel due to the expansion of the use and application of information communication technologies through the expansion and penetration of cyberspace.

At present, it is said that approximately 265,000 individuals are employed in information security within Japan, however there is a potential deficiency of approximately 80,000 such security personnel. In addition, of these 265,000 individuals, the number of individuals who actually possess the required level of skills is thought to be slightly over 105,000, meaning that some sort of education or training is necessary for the remaining 160,000 individuals.[103]

In addition to it being necessary to resolve this deficiency in the number of security personnel that can be utilized in existing information communications technology, the expansion of information communication technologies accompanying the expansion and penetration of cyberspace will become an issue that must be dealt with, resulting in an even greater deficiency of security personnel in the future, making the recruitment, training, and use of these personnel even more necessary.

In addition to proactive measures being required to handle this deficiency in personnel, another large issue is the ensuring of personnel who possess exceptional capabilities which cannot be acquired through training alone. In regard to this securing of personnel, private and public sectors will collaborate to implement training camps to discover and cultivate the outstanding individuals who have not only creative and original ideas and technologies in the

[103] IPA estimate.

software related fields, but also the capabilities to apply them, as well as competitions which will test the practical skills of information security personnel.

In order to raise the skill level of cybersecurity professionals within Japan, and to discover and cultivate exceptional personnel in the field, a framework is necessary for practical application of training throughout all of society. Specifically, there are a wide variety of personnel labeled information security personnel, and the skills required vary greatly depending upon the attributes of the specific personnel, so the required skills and knowledge will be clarified through improvement and utilization of skill standards.

Consideration, will be carried out, in accordance with the diversity of needs for information security personnel, about such issues as a qualification/capability assessment system based on security levels, which include enhancing specialized educational curriculums at universities and other learning institutions for practical training programs, strengthening of industry and academia cooperation, and the need for improvement and new establishment of official certification and skill assessment systems, while utilizing the skill standards.

Because the training of personnel who can perform globally is important, in addition to supporting participation in international conferences and study abroad at specialist graduate schools and other related organizations overseas, invitations to and holding of international conferences within Japan will also be promoted.

It is also necessary for the discovery and training of personnel to lead directly to their employment and utilization. For this purpose, government institutions shall take the initiative in appointing external information security personnel.

④ Literacy Improvement

In Japan, cyberspace is expanding and penetrating into every generation from the youth bracket to the elderly, every situation including individuals, families, workplaces and public facilities, and everyday life and socioeconomic activities of real-space. In this way, all general people coexist with cyberspace, and it is thus necessary to continually work to improve the literacy of very broad base of general people. In addition, this also contributes to creating a foundation for the cultivation of advanced personnel.

Specifically, it is necessary to plan awareness raising activities starting from the elementary and middle school education stages, and implement participatory awareness raising projects such as motto and poster contests. At the elementary and middle school education stages, depending upon the development stages of the student children, learning activities have be enhanced so that computers and information communications networks and other information tools can be used for instruction in each subject, positive promotion has be carried out for education on information morals, including information security. Hereafter, practical measures united with the utilization of information communication technologies in various fields of education, such as use of digital textbooks for students and education on software programming, will be promoted.

Information security measures for the elderly will so become even more important in the future, so environments will be prepared for the cultivation and utilization of information security related supporters and detailed follow up for the elderly.

Smart devices, especially smartphones, which are always turned on and connected to the internet while carried around by users, handle a variety of information about the user such as position information, however structural restrictions limit the effectiveness of information security software, so further improvement of individual literacy is required.

Specifically, with the shift to smartphones, the majority of the expanded usage rates are for SNS,[104] and it is planned to collaborate with relevant operators to implement effective measures for smartphone use. In addition, a framework will be constructed which allows users to understand the risks of smartphone applications and make determinations regarding these use on their own.

Taking into account the rapid progress of information communication

[104] According to the White Pater on Information and Communications, the changes in usage rates before and after the shift to smart phones for SNS increased greatly from 37.9% before the transition to 62.6% after the transition.

technologies, it is necessary to update information related to measures to improve the literacy of general users in a timely fashion. For this reason, it is important that government institutions collect information through measures for responding to cyber attacks, analyze this information and then provide the information nationwide in a format that is easy to understand for general users.

(3) Construction of "World-leading" Cyberspace

In order to keep up with a global cyberspace, "world-leading" cyberspace shall be constructed and attempts shall be made to strengthen contribution and outreach capabilities in the global strategic space by strengthening ministerial level dispatches, active participation in the international rulemakings, active outreach into overseas markets, capacity building support and confidence building measures.

① Diplomacy

In Japan, free flow of information in cyberspace is a basic policy, and the basic values such as freedom of expression are assured through this policy, providing a variety of benefits including economic growth.

Because it is impossible for Japan to handle risks which have expanded to a global scale on its own, it is important to multilaterally build and strengthen partnerships with other nations and regions which share the same basic values including the basic policy, democracy, respect for basic human rights, and the rule of law. For this reason, it is necessary to carry out diplomacy which promotes a balanced approach to constructing a safe and reliable cyberspace in by not applying excessive administration or restrictions by the state while maintaining its openness and interoperability.

For the application of international laws to acts using cyberspace, it is important that existing international laws continue to be applied to acts using cyberspace in terms of maintaining a degree of order in cyberspace, and the deliberation will continue on how to apply specific international laws such as the Charter of the United Nations and the International Humanitarian Law to conducts in cyberspace.

While cyber attacks for which the involvement of foreign governments is suspected have actually occurred overseas, because it is difficult to identify perpetrators of cyber attacks, it is necessary to steadily implement confidence-building measures in order to avoid unexpected escalation that are not intended by parties, for instance as a result of misidentification of attackers.

In addition to continuing discussions and dialogs with countries with whom Japan has carried out bilateral discussions and dialogs so far, Japan will also expand to holding discussions and dialogs or opinion exchanges with other countries and regions as well. In addition, the country will actively participate in multi country discussions and meetings including regional frameworks such as the ARF[105] and other related committees in the United Nations, in addition to various cybersecurity related conferences with participation from multiple stakeholders other than just government institutions and "face to face" participation in the global community.

In order to rapidly and appropriately respond to cyber attacks, cooperation with the United States, in which Japan is in an alliance based on the Japan-U.S. Security Arrangements, is vital. Based on the understanding that the variety of issues surrounding cyberspace recently are pressing matters for both national security and economy, further discussion on sharing threat information, detailed measures including joint training exercises for critical infrastructure protection and other area, and creation of international rulemakings, shall be carried out through future dialogs such as the Japan-U.S. Cyber Dialogue.

② Global outreach

In a global cyberspace, vulnerable countries and regions are targeted as springboards from which to launch cyber attacks. The conditions, related to cybersecurity such as technological capabilities for responding to incidents including cyber attacks, are various from country to country. Therefore it is expected that each is construction a given capabilities such as for handling

[105] ASEAN Regional Forum. A forum aimed at improving the security environment of the Asia-Pacific region through dialogs and cooperation related to political and security issues.

incidents, in terms that this will lead to the formation of a common understanding in international society and serve as a deterrent for cyber attacks.

Consequently, it is important to build relationships in with newly emerging nations as well as developing countries in ASEAN and other regions in which those countries and Japan can develop together, and actively provide support for building the capabilities to deal with cyber attacks against these countries and regions.

Specifically, this includes providing support for the building of CSIRT in each nation, security management knowhow support, international awareness raising, developing a network to collect information about cyber attacks by collaborating with other nations, then implementing research and development projects on technologies for prediction and quick response to cyber attacks and expanding the participant countries.

Also, introduction of best practices such as the botnet countermeasure projects through public-private partnership, implementation of joint projects, and conducting tabletop exercises with overseas operators, will be promoted.

About the encryption assessment project[106] working to assure safety and reliability in electronic government and other fields, the results will be announced both domestically and abroad, while the use of encryption technologies will be promoted.

In addition, in international trade, cybersecurity safety is coming to be required for products and services which utilize various information communication technologies. Therefore in order to ensure that Japan does not find itself at a disadvantage in its strong fields, such as multi-functional devices including copiers and control systems, Japan will actively participate in and work on international standardization of security and the creation of international frameworks for mutual recognition of evaluation and certification, from a viewpoint of activation of industry,.

Further, Japan will require that the practices often seen in newly emerging nations and other regions of using information security as an excuse for import restrictions and measures for giving preferential treatment to domestic goods be

[106] CRYPTREC.

made to conform to international trade rules. Also, Japan will work towards the promotion of the international development of Japanese businesses by working to assure the compliance with relevant domestic and overseas systems. For example, consideration will be held for actively contributing to the establishment of harmonized international rules through the support of preparation of systems in newly emerging countries and other region, and domestic systems for international distribution of personal data.

③ International cooperation

Attempts will be made to strengthen international collaboration in order to effectively respond to cybercrime, which can easily be carried out across national borders. Specifically, information related to cybercrimes will be continuously exchanged with foreign investigating organizations in addition to dispatching staff to improve collaboration with foreign investigation agencies as well as to learn the latest in investigative techniques.

In the event the cooperation of foreign investigation agencies is required in order to gather evidence, mutual legal assistance will be proactively requested of these agencies and an international investigation promoted in an appropriate manner.

Regarding international cooperation related to cybercrime countermeasures, Japan has ratified the Convention on Cybercrime,[107] and will work to strengthen rapid and effective mutual investigations and other cooperation between law enforcement agencies including increasing the number of countries party to the convention.

In addition, the promotion of sharing of information through international collaboration, and understanding of international trends in incidents related to cyber attacks is important. Specifically, in addition to strengthening collaboration[108] at the operation level for promotion of sharing of incident

[107] "Convention on Cybercrime." Ratified in the Japanese Diet in April of 2004, coming into effect on November 1, 2012 through the enactment of the "Law for Partial Revision of the Penal Code, etc. to Respond to Increase in International and Organized Crimes and Advancement of Information Processing" (2011 Law No. 74, the so-called "Cyber Penal Code") in June of 2011.

[108] For CSIRT international cooperation, there is the international conference FIRST (Forum of Incident Response and Security Teams), with participation from the NISC, the National Police Agency Cyber Force

information related to cyber attacks between CSIRTs, supporting the cultivation or human resources related to cybercrime investigations and prosecution as well as the preparation of the criminal justice systems in various countries.

In order to avoid unexpected situations arising out of mutual distrust, it is important to implement confidence-building measures. For this reason, Japan shares its basic stance and best practices. Further, in addition to maintaining a mutual contact system for incident occurrence from times of peace, collaborative international research projects and responding exercises on cyber attacks among multiple nations shall also be implemented.

Moreover, this will also contribute to international collaboration with the various countries, promoting the preparation of an international network through redundancy of international connects between Japan and overseas.

4. Promotion Systems and others

(1) Promotion Systems

The NISC is strengthening its functions as Japan's command post for constructing a world-leading, resilient and vigorous cyberspace. Specifically, in addition to drastically strengthening of the GSOC, the organization will also strengthen its collection of information such as incidents which are related to cyber attacks, analysis and publicity related to the current situations of relevant measures of governments and actual circumstances of domestic and overseas cybersecurity related trends, and dynamic ability to respond to through organic collaboration among the various functions distributed throughout related specialist organizations such as government institutions, independent administrative agencies and others. When implementing these changes, CSIRT functions, which serve as the point of contact for international incident handling within Japan, will also be considered.

Based on the above, the NISC will be the "Cybersecurity Center" (tentative)

Center, IPA, JPCERT/CC for cooperation between CSIRT from various countries, and APCERT (Asia Pacific Computer Emergency Response Team) for cooperation between CSIRT in the Asia-Pacific region.

around FY2015 by preparing the required organizational structure, including authorities and securing of human resources through personnel management such as employment and cultivation of specialist personnel.

The promotion of information sharing related to cyber attacks is necessary as a basis for the organic collaboration between relevant organizations including government institutions and critical infrastructure providers. On these occasions, a framework will be prepared to maintain confidentiality of information, in accordance with the purposes of sharing information, the details of the shared information, and the scope of the parties sharing the information while continuing to use existing frameworks as well.

(2) Evaluation etc.

In order to ensure the appropriate implementation of the various measures implemented in accordance with this strategy, and to ensure organic collaboration between the measures, a management aimed at the achievement of the mid to long term goal of realizing a cybersecurity nation will be carried out, while, based on this strategy, the annual plans for each year starting from FY2013 and an international strategy on cybersecurity will be developed.

In addition, in order to appropriately respond to domestic and overseas environmental changes and to maintain the continued improvement of this strategy, any measures based on this strategy and objectives management, evaluation for this strategy and the annual plans shall be carried out. During the evaluation, the progress of the various measures and others will be evaluated from a people's point of view.