The Second National Strategy on Information Security

Aiming for Strong "Individual" and “Society” in IT Age

February 3, 2009

National Information Security Policy Council

Table of Contents

Introduction

Information security measures have been drastically enhanced since National Information Security Center ("NISC"[1], hereafter) was established in the Cabinet Secretariat in April 2005, and Information Security Policy Council was established as a divisions of the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society ("IT Strategic Headquarters", hereinafter) in May 2005.

The enhancement plan, in specific, aims to establish a systematic plan based on the strategic way of thinking focusing on the "information security" issue as part of the e-Japan Priority Policy Program etc. It was concluded with the launch of the First National Strategy on Information Security[2] ("the First National Strategy") or the mid and long term strategy for three years from FY2006 to FY2008.

Various private and government organizations have addressed the issues over the past two years while NISC was taking a lead to improve the measures.

On the other hand, many risks remain in the current social conditions such as malfunctions of the stock trading system, automatic teller machines of financial institutions and automatic ticket gate system, a large amount of fraud of credit card information by unauthorized computer access, leakage of important information through the file exchange software and computer virus while the information technologies (IT, hereinafter) became the social infrastructure. Furthermore, there are new risks emerged everyday such as the threats of botnet which became more severe or the targeted attack (Spear attack) aiming specific organizations or individuals through the use of the social engineering. Moreover, IT in the society became further progressed, which showed a significant change from the one at the time of the First National Strategy. For instance, networking with home appliances became extremely important for our daily life in line with the start of digital broadcasting, car navigation systems connected to the network, which is now common, and promotion of the online applications of the public paperwork for general administrative procedures. Therefore, information security issues became diversified according to such trends.

Under the circumstances, the Second Plan for Information Security ("The Second National Strategy", hereafter) aiming the term in and after FY2009 is compiled as below to continue strong promotion of the measures on the information security issues by the

[1] Abbreviation of National Information Security Center.

[2] Determined by Information Security Policy Council on February 2, 2006

Japanese government based on the development of various approaches based upon the First National Strategy and the change in the social environment etc. In terms of the information security issues, the environment is changing rapidly while a sustainable scheme from mid to long term perspective is necessary. Therefore, the term for the Second National Strategy is designed for the three years (from FY2009 to FY2011), as the same manner as the First National Strategy. The annual promotion plan will also be compiled from FY2009 based on this National Strategy, in the same manner as the scheme for the First National Strategy.

The Second National Strategy was developed based on the actions taken under the First National Strategy, the primary proposal of the National Strategy Study Council as part of the Information Security Policy Council, the actions taken by the government based on the proposal, and the discussion in Council on the Protection of Critical Information of Information Security Policy Council.

Therefore, as the scheme of the information security policy under the Second National Strategy, this National Strategy is so called the overall design of the whole policy, which are supplemented by other documents concerning government agencies, critical infrastructure and policy assessment as the individual design drawings. The individual design drawings specifically include “the Standard of Information Security Measures of the Government Bodies” , “the Second Action Plan on Information Security Mearures of Critical Infrastructure” (the Second Action Plan), Assessment of “Secure Japan” Action Plan and Promotion of Rational and Sustainable Improvement of Policy” [3] and “Ideal Society and Policy Assessment for Information Security in Japan – Establishment of PDCA[4] Cycle of Information Security Policy aiming “Secure Japan”, hereinafter) (these two documents are specified as “the framework of information security policy assessments”) [5]. These documents were developed based on the discussions in the government agencies concerned and the special councils such as Critical Infrastructure Councils, which should be an action plan to specify the directions aimed under the overall drawing.

With the overview of the above policies, this National Strategy as the overall design briefly looks back the approaches under the First National Strategy including the basic policy and objectives in Chapter 1. The following will describe the current status as of

[3] Determined by Information Security Policy Council on February 2, 2007

[4] Abbreviation of Plan (planning phase) Do (implementation phase), Check (inspection phase) and Act (improvement phase)

[5] Agreed by Information Security Policy Council on February 2, 2007

2009 as a result of the review. Chapter 2 provides the assumption for the condition in 2012 for the period after the implementation of the Second National Strategy, while specifying the basic principles and objectives on the action plan under the Second National Strategy according to the status summarized in Chapter 1. Chapter 3 explains the key policies for the actions of the government for the upcoming three years under the Second National Strategy, which is followed by Chapter 4 to show the organization to promote the policies to realize and sustain the policies.

For either condition in 2009, the assumption for 2012 or key policies, this strategy reflects the structure of the First National Strategy, which has four areas of cross-field basics.. However, based on the current status, the entity that entrust its proprietary information to other entities (entity to entrust information) will be described as one distinct pillar when the perspectives of 2009 and the objectives in 2012 are discussed. In the key policy, the measures about the entity to entrust information will be included in the measures about entities which will implement measures.

One of the important messages in the Second National Strategy is to strengthen the response to "Accident Assumed Society" (Chapter 2, Paragraph 1). It means that the actions taken under the First National Strategy was implemented placing the emphasis on the preventative measures, and the Second Plan should also focus on the measures in case of emergency and preparations for restoration in a wide range. Of course, it is needless to say that all the entities concerned must continue to make the utmost efforts for the preventative measures to prevent occurrences of the information security related issues. In accordance with the Second National Strategy, all the entities are expected to promote a consistent information security measure before and after the emergencies.

Chapter 1. Actions under the First National Strategy of Information Security and the Status Report for 2009

Section 1. Actions taken under the First National Strategy of Information Security

(1) Meanings of the First National Strategy of Information Security

The First National Strategy was so called a strategy to launch the information security policies in Japan and to “give awareness" to all entities concerned. In a sense, the First National Strategy was to make the information security a key policy among other IT related policies, which made both private and government entities including the government agencies, local governments, critical infrastructure, companies and individuals to concentrate on and take actions on the issues in order to realize the safe and secure IT, since people’s life, social and economic activities currently heavily rely on IT.

In specific, the government and private entities concerned have been actively working on the measures based on “Secure Japan” the annual plan for every fiscal year to achieve the standard to prevent information security related problems[6], aiming high quality[7], high reliability[8], and safety/security.

The following is a quick review on the basic concept on the First National Strategy. Chapter 2 explains the difference of the concept between the First and Second National Strategies.

(2) Japan’s National Objective and Aim of Information Security

The First National Strategy clarified the status of the information security in conjunction with “the use of IT and realization of the national goal”. Specifically, this is to define the information security “to make the IT infrastructure as to be truly reliable and

[6] For government organizations, it is specified as 1) the government organization integral standard should be the global best standard by 2008, 2) all the government organizations implement the measures required by the government organization integral standard by early FY2009,　and for critical infrastructure “minimize almost to 0 to have IT failures in the critical infrastructure by early FY2009, for enterprises “achieve the world top class standard for the measures taken by companies concerning the information security, for individuals “aiming to minimize the number almost to 0 for individuals who have concerns in using IT.　(原文では 8)

[7] For instance, there should be no bugs. Cases when any measures can be taken for unexpected incidents (原文では 6)

[8] For instance, strong enough not to cease operation, not to break, not to stop or to be available for restoration even though the failure, even though any loads are applied due to attacks (原文では 7)

rigid" concerning 1) sustainable economic development through the use of IT[9], 2) achievement higher quality of life of people through the use of IT[10], 3) security[11] against threats related to the use of IT.

(3) Basic policy – principles of "Information Security Advanced Nation"

The First National Strategy aimed to promote actions based on the principle of "Security Nation" (to establish "Japan Model" as a pronoun of "high quality, high reliability, safety/security" and develop the principle toward the rest of the world. It eventually aimed to make Japan as the "Information Security Advanced Nation".

(4) Basic objective to be realized – to create "secure environment of IT -

The most important goal of Japan's information security is to guarantee the safety and security in using IT. The First National Strategy aimed to establish "a secure environment to use the advanced data communication network (secure IT environment, hereinafter)" specified in Basic Act on the Formation of an Advanced Information and Telecommunications Network Society (IT Fundamental Law) Article 22. The First National Strategy aimed not only to be safe but also to allow users to use IT with the feeling of security by satisfying the three conditions required including "prevention", "recognition and experience (environment to which measures were applied) " and "sustainability of business".

On the other hand, most of the objectives for different fields and actions taken under the First National Strategy focused on the preventative measures.

(5) Issues to realize the basic objective and directions for the solution - "to establish a new government and private sector collaboration model"

[9] According to the relationship between sustainable development of Japan as an economic superpower and IT, it is said " in order to take measures against globalization and distribution of business activities and maintain strong competitiveness and high productivity, it is needless to say that IT is indispensable to use. One of the key national goals is to effectively use IT as a social infrastructure further, compared to other countries, and achieve sustainable development of the country. "

[10] In conjunction with the use of IT and quality life of people, it is said that IT became essential to solve social issues that Japan is facing in the 21st century, not only for its economic activities… the important national goal is to solve social issues that Japan is facing and achieve the safe and secure quality life of people by using IT as the key means " .

[11] It is said that " IT began to be necessary or essential to use not only for economic activities but also for solving issues that Japan will face in the 21st century… one of the important national goals is to solve social issues that we are facing and achieve a safe and secure, and quality life of people by using IT as a critical tool" concerning the relationship between the goal to achieve quality of life of people and usage of IT.

The First National Strategy provides the direction for solutions of the issues[12] to establish a secure IT environment as to create “a new government and private sector collaboration model” to “implement measures by all the entities concerned in IT society with an awareness of their own responsibility with the common understanding of the importance of the information security issues and take appropriate roles depending on their positions. Accordingly, Japan should tackle against the information security issues from the comprehensive viewpoint as a nation.

(6) Basic policy on information security issues

The First National Strategy defined the basic policy for enhancement of the emphasized and strategic application of the resources to seek a solution of the information security issues from the national viewpoint of Japan. This strategy specifies four basic policies including “formulation of the common understanding of the government and private sectors concerned”, “pursuing the advanced technologies”, enhancement of public responses” and “promotion of partnership and cooperation”.

Section 2 Perspectives in 2009

Various entities of
and private sectors have taken actions for the three-year plan based on the First National Strategy to date. The following describes the current status in Japan as of 2009 after the implementations of the First National Strategy. It explains the framework of the First National Strategy, including the four areas for implementation of measures and the cross-field information security infrastructure specifically.

Meanwhile, it is important to consider not only the entity who maintain information but also the entity who entrust information, like general consumers, for the information security that is needed when information is transmitted among different entities and the information is maintained by a specific entity. While the entity to entrust information was not specified in the First National Strategy, the following shows the perspectives in 2009 concerning the entity to entrust information. This item will be further mentioned in [5] of (1) “Four Measures for Implementation”.

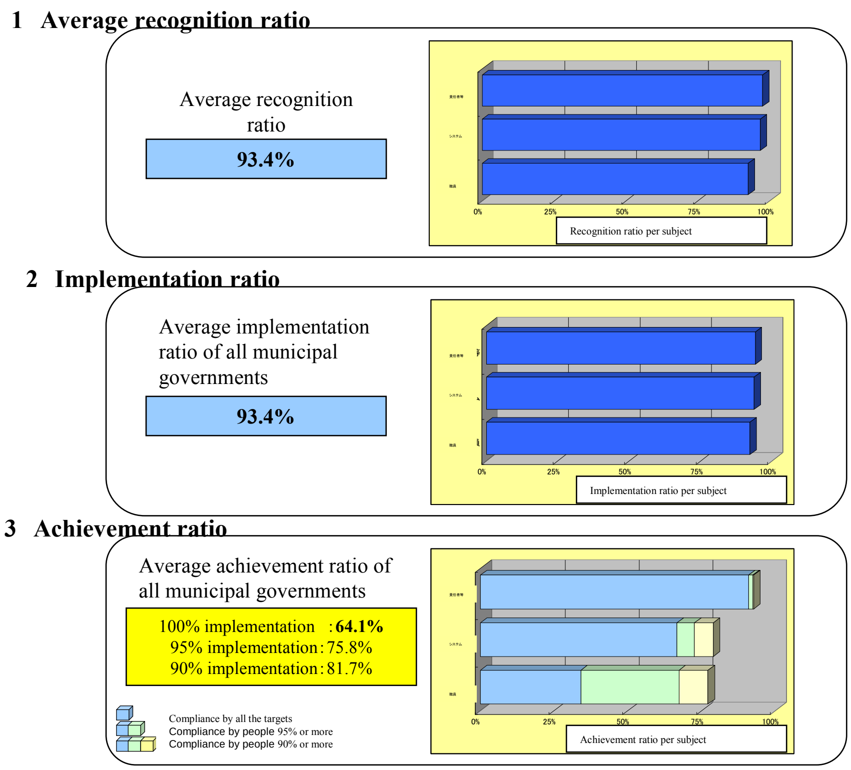
(1) Four Measures for Implementation

[12] As a issue to be considered, it is said 1) the emergency responses only to issues visible is managed and 2) each entity construe the IT society are only struggling to their own responses in the vertical structure of the organization.

[1] Government agencies and local governments

[Government agencies]

Regarding the government agencies, various measures were promoted the information security measures so as to create the two layer PDCA cycle including the PDCA cycle of government agencies and the other PDCA cycle of the entire government body focusing on the assessment and recommendations by the Information Security Policy Council. This aims to implement: 1) to make the level of the government standard the best global standard by FY2008 and 2) to implement measures at the level required by the government organization standard for all the government agencies by early FY2009 under the First National Strategy. (Figure 1)



Recognition ratio : The ratio that each municipal government can monitor the measures taken, among all the targets.
Implementation ratio : The ratio of people who took measures to these who are responsible for, among all the targets
Achievement ratio : The ratio of the items in compliance that a certain ratio of people (100%, 95% and 90%) who are responsible for, among all the target.

Figure1 Results of assessment on the government agencies status report for the measures taken (FY2007)

(Source: “Outline of the state report of government agencies (FY2007)" Information Security Policy Council Report, April 22, 2008)

As a result, the following issues remains though the basic PDCA cycles were progressed by the government agencies.

First, it can be seen that some government agencies have made the actions of the cycles not fully progressed. The information security measures should be taken by each government agency at their responsibility in principle. Therefore, the PDCA cycles should be actively promoted by the spontaneous efforts of each government agency, although it seems that they might still feel passive in making actions for some cases. They seem to implement measures just because they need to undergo the assessment in the implementation of the measures and the inspections on the results. Such organization might take an instant measure on the information security, which would not be a real solution.

Secondly, there is a lack of awareness among those who concerned to make actions spontaneously by properly understanding the risks that they face in promoting the information security measures, which is related to the above. Therefore, they are at risk that the administrative tasks could not be sustained against new threats or in case of unexpected situations, or that the information security related requirements could increased forever as pursing the perfect measures.

Thirdly, they are struggling to have an appropriate level of standard for the information security against the balance issue of the usability and cost in developing the IT system.

Most of the issues might be originated from the fact that the missions of each government agency, the information security that supports it and the relationship with the information system were not fully understood by the top management level of the government agencies. Furthermore, it is not fully recognized that the IT system would contribute to make a significant change on the work processes.

[Local governments]

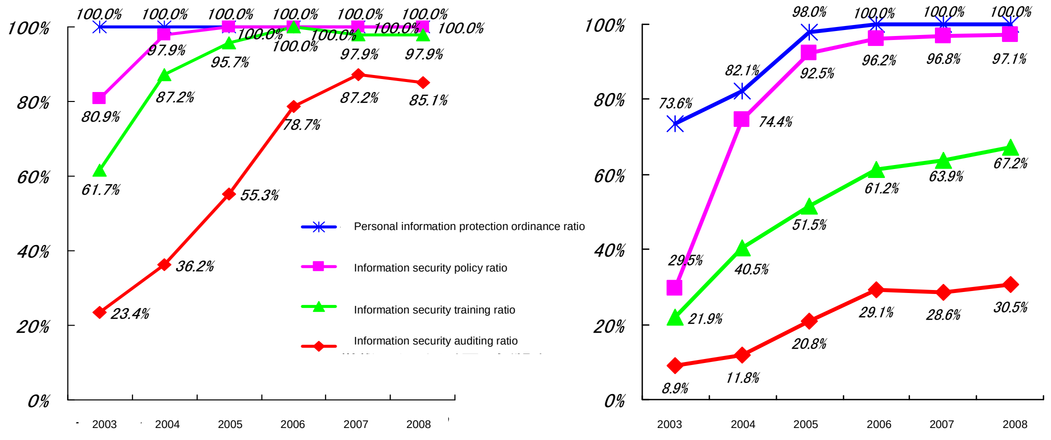
Local governments have also promoted various measures according to the First National Strategy aiming 1) to review the guidelines concerning the information security of local governments by September 2006 and promote the measures including information security audit or training, and 2) to establish the information sharing system between local government offices by the end of 2006.

As the result, the measures have been taken in general including implementation of auditing. On the other hand, the ratio of the local government offices such as city, town and village which conduct auditing is only about 30%, which shows the delay in taking the measures due to various restrictions (Fig. 2). Although there should be various risks concerning the information security in the future, small local governments are at the risk that the critical situation would be a reality because they are not able to take sufficient measures against it in advance.

The local governments also have individual fields that would require specific relationships between the national administrative bodies and the local government organizations concerned, which could require various measures on the information security depending on the organizations. Therefore, the information security standard could vary beyond the allowable range, based no the usage of the information resources per administrative task, in terms of a local government.

In addition, it is also important to make an environment to facilitate for the local governments to easily take actions in order to strengthen the base of information security in regions, besides each local government needs to take the information security measures by their own, from the viewpoint of promotion of the information security in various regions.

Some local governments actively proceed the public relations activities and hold seminars for the information security, although some areas show a lack of human resource development of the successors to continue the activities. Therefore, the information security measures in the regions remains unpractical.



Metropolitan/prefecture

City, ward, town and village

Figure 2 Local government: Current status of information security measures
(Source: Ministry of Public Management, Home Affairs, Posts and Telecommunications

"Outline of Local Government Information management – the status of promotion of e-local governments (October, 2008)")

[2] Critical infrastructure

IT services became well proliferated in a wide range. While the First National Strategy is proceeded, it shows various measures taken and progresses in terms of the efficiency of critical infrastructure providers[13] and improvement of the serviceability. For the service users, there are more opportunities for them to use IT-based services thanks to the fulfillment of the network environment and higher IT literacy. Public lives and social economic activities are expected to grow by extending the use of IT, though which means that the society should be more depending on IT.

The government has been taking various measures in cooperation with the critical infrastructure providers aiming to minimize malfunctions of IT on the critical infrastructures under the First National Strategy. In terms of the critical infrastructure, "the Action Plan concerning Information Security Measures of the Critical infrastructure (the First Action Plan, hereinafter) was established to promote the four policies, in addition to the First National Strategy, including [1] maintenance of "safety standards etc" concerning the information security for the infrastructure (Table 1), [2] enhancement of information sharing system, [3] analyses of the interdependence and [4] execution of cross-field trainings.

This resulted in the establishment of the framework to enable collaboration of the government offices and private sectors from the viewpoint of the cross-field viewpoint, while the government supports the measures which have been taken by the critical infrastructure providers with a certain policy. However, services not applied to the First Action Plan or the safety standard have started or developed due to the trend of further dependency on IT. There are also troubles occurred, which could make a significant influence on people's life and social economic activities in Japan, due to the inapplicable services including the systems not applicable to the safety standards. Thus, it is necessary to take quick actions for information security against such changes of the environment.

[13] "Critical infrastructure provider" is according to the definition specified in "12. Definition and Scope" of "the Second Action Plan concerning Information Security Measures of Critical Infrastructure".

Table1 Safety standard list (as of February, 2008)

Field		Safety standards
Information and communication	Telecommunications	Telecommunications business law, Telecommunications business law regulations, Telecommunications business facility regulations (including pertinent notification) Safety/reliability standards of data communication network Safety standard (1st edition) concerning information security: telecommunications
	Broadcast	"Safety standards" guideline concerning information security of critical information infrastructure: broadcasting
Finance		Guide to security policy for financial institutions Safety measures standard/reference of financial institution computer system Contingency plan guide for financial institutions
Aviation	Air transport	Safety guideline concerning information security: air transport enterprises
	A.T.C.	Safety guideline concerning information security: air traffic control system
Railroad		Safety guideline concerning information security: railroad
Electricity		Guideline concerning technical standards/operation standards of electric control system etc.
Gas		Information security measure guideline of control system concerning production / supply
Government /		Guideline concerning information security policy: municipal governments
Medical treatment		Second edition of safety management guideline concerning medical information system
Water service		Safety guideline concerning information security: water service
Logistics		Safety guideline concerning information security: logistics

[3] Enterprise

With the basis of the First National Strategy, the government proceeded to make the information security solutions of private enterprises to the highest global standard by the beginning of fiscal year 2009. For instance, the number of organizations obtained the compliance of the information security management system (ISMS) has increased every year, which is the highest number compared to that of other countries in the world. (Fig. 3 and Table 2). Especially, as the information security is further required as a critical issue for enterprises from the viewpoint of the legal requirements such as personal information protection laws and responsibilities to the customers against information leakage attributed to P to P file exchange software[14] and social liability. Therefore, the number of companies that defines the rules and security policies such as confidentiality agreement or prohibition of brining personal information out of the office. (Fig. 4) In the meanwhile, the actions for strategic promotion of the information security as part of the corporate management were not fully recognized from the viewpoint of competitiveness of companies, use and protection of information assets as the valuable resources. The difference of the sense of urgency is obvious between large companies and small/mid-sized companies. (Fig. 5) Therefore, many issues have been discovered.

Firstly, it is necessary to enhance the feasibility to make the information security measures of the enterprises truly effective and promote the measures. The First National Strategy promoted to establish and operate the corporate governance by taking into account of the social responsibility and the mechanism of compliance to support the

[14] Software for file exchanges on the Internet with unidentified numbers of PCs. P to P (Peer to Peer) is a communication which requires no server for sending and receiving data.

policy among companies, from the viewpoint of the information security. Corporate compliance system has been widely recognized among the discussion on the legal requirements and social responsibilities that the companies must bear. However, the information security practice and implementation are still insufficient for some cases at present, as the corporate compliance system is just in the early stage. Therefore, the information security measures of the enterprises might not be fully effective to develop a practical effect that the measures have a positive impact on the basic objectives of companies to increase the corporate value.

Secondly, while it is inevitable that the information security measures are taken to prevent the information asset management related issues from being occurred, it would also be necessary to enhance the measures to cope with or restore the system promptly in case of emergencies. Even though the countermeasures are well taken in advance, the companies may lose the liability of their customers due to suspension of the business activities and delay for restoration if any information security related problems come to reality.

Thirdly, measures for small and medium-sized enterprises would also be required as they are unable to fully implement the information security measures due to negligence or resource shortage. Concerning the subcontract structures and a large-scale supply chain that mainly employed by large enterprises, it is indispensable for them to proceed the business activities in cooperation with small and medium-sized enterprises to strengthen the competitiveness of the industries in Japan. However, even if only one company has lack of information asset management policies, among the information flow which is the flow of goods and humans, their value information could be at risk to be leaked from the point to decrease the competitiveness of the related companies as a whole.

Fourthly, it is currently necessary to make measures to prevent the information security issues at business basis at home and abroad in order to facilitate the development of business that Japanese companies are pursing, in other words, the development of offshore outsourcing, international business (supply chain) and direct investment for foreign companies. Without these approaches that fully proceeded, it may be difficult for Japanese industries to do business in the global business environment. It means that Japanese company may not fully receive the advantages of the global business development due to the risk and cost of the information management increased, as the information should be distributed excessively for outsourcing even though they intend to use a business base overseas.

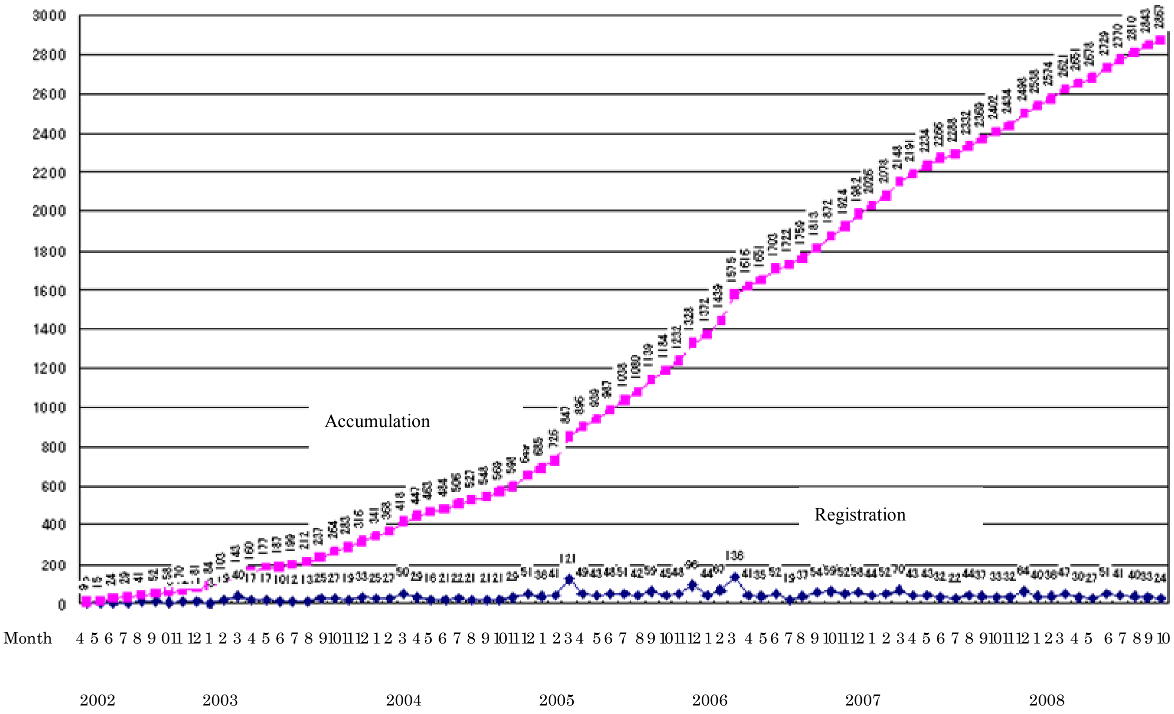


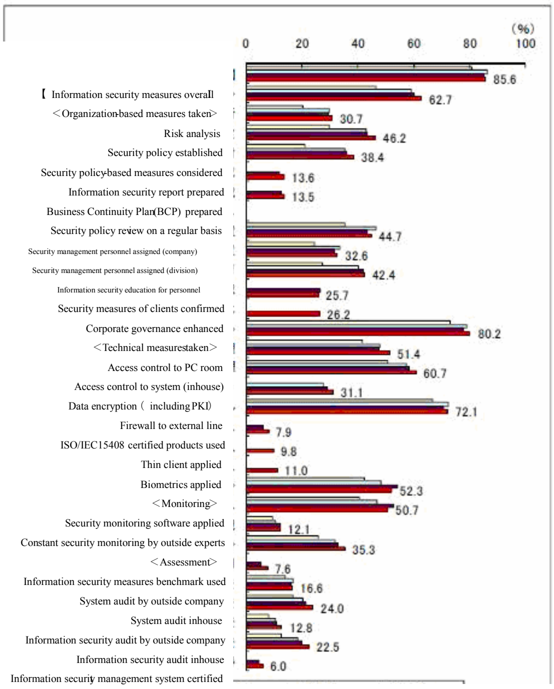
Figure 3　Transition of the number of ISMS certified organizations
(Source: JIPDEC HP, the number of registered organizations as of November 11, 2008)

Table 2　International comparisons of the number of ISMS certified organizations

Country	The number of organization	Ratio
Japan	2863	57%
India	433	9%
U.K.	368	7%
Taiwan	202	4%
China	174	3%
Germany	108	2%
U.S.A.	82	2%
Hungary	74	1%
South Korea	71	1%
Czech	66	1%
Total	4987	

* Top 10

(Source: the web page of International Register of ISMS Certificates
(as of November, 2008.))



（ Note）
1.Transition of the ratio of companies answered "implemented" for the information security measures condition.
2. Implementation ratio of general information security measures was calculat ed by the number of companies answered "implanted" for some information security measures against the number of companies answered their conditions of information security measures.
3. The implementation ratio of each category is calculated by the number of companies answered "implemented" for some security measures of the categories in question to the number of companies answered their conditions of information security measures.

Figure 4 Transition of the percentage of enterprises that execute information security measures

(Source: Ministry of Economy, Trade and Industry "Information Processing In-situ Survey Result in 2007")

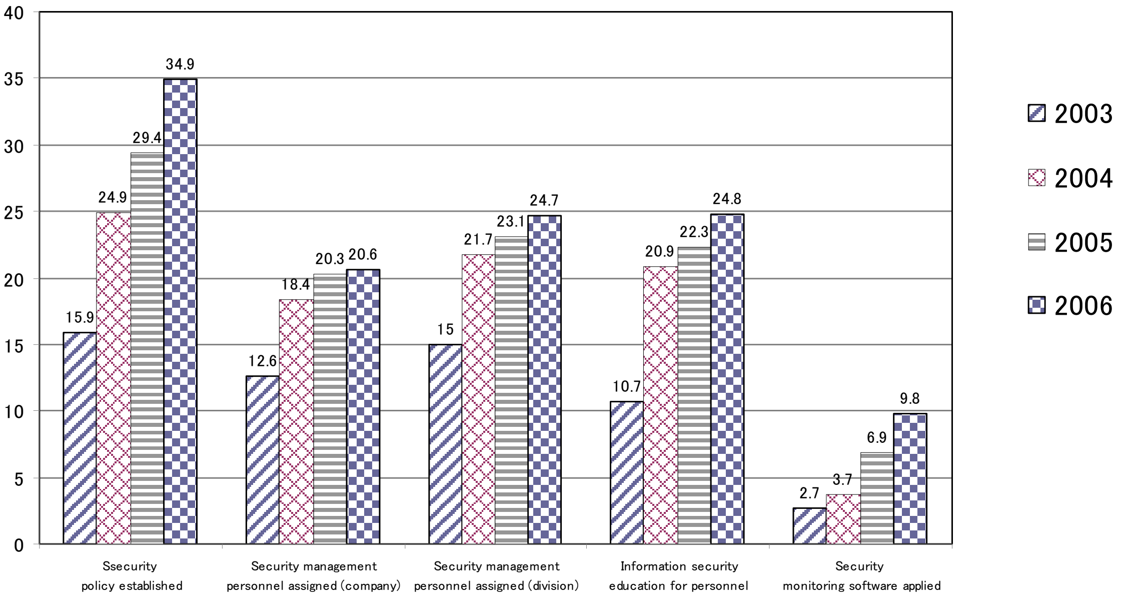


Figure 5 Difference between big enterprises and small and medium-sized enterprise Difference of measures execution rate = measures execution rate in big enterprise-measures - execution rate in small and medium-sized enterprises (Source: Ministry of Economy, Trade and Industry "Information Processing In-situ Survey in 2007")

[4] Individual

In terms of individuals, the government has proceeded the measures under the First National Strategy aiming to minimize the number of individuals who have concerns in using IT. However, the individuals who have concerns in using the Internet accounts for over 40 percent (Fig. 6).

It is not easy to make all individuals to realize the importance of the information security measures by taking into consideration of the limitation of the resources, although the measures have been taken including enhancement of public relations and outbound information against risks that the individuals would face in term of information security. It might be hard to fully prove the effects unless the means are somehow modified.

In addition, there should be individuals who would have no intention to take measures, although they realize the importance of the information security measures. Therefore, conventional measures such as public relations and distributing information might not be enough to see the positive effects.

It is also insufficient only if the individuals understand the importance of the information security measures, and take preventative measures against risks. Essentially, it is important for individuals to realize the risk to have critical damages for themselves due to problems that they might have, when uploading their personal information through online services of Internet. However, it seems that such recognition is not fully obtained among people.

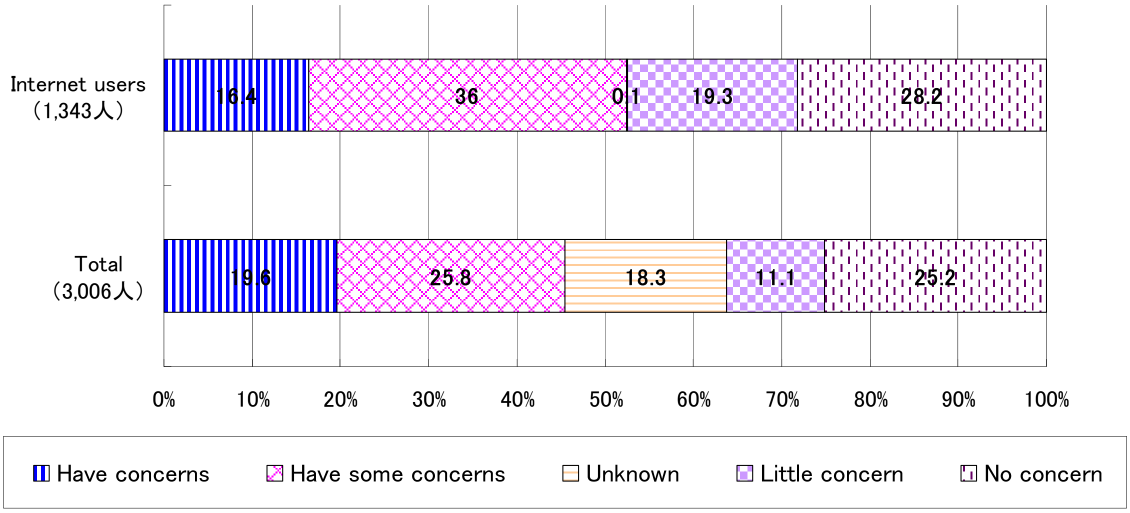


Figure 6 Concerns on using the Internet

(Source: Public opinion poll concerning security on the Internet: the Cabinet Office (2007 survey)

[5] Entity to entrust information

The number of cases which entities such as individuals and enterprises send information to others communicating through IT, with the fulfillment of the Internet shopping, development of e-government services and contracts made online or through emails. Furthermore, the information which was sent to others might be used by the third party. It is difficult to track down how the information would be sent or to whom. In this condition, it is almost impossible to restore the information, once it is leaked or inappropriately taken by others. Therefore, the entity who entrusts information should also fully understand the possibility and take appropriate actions. Otherwise, there could be a significant difference between the safety initially expected by the entity and the actual safety.

In particular, new methods were emerged as a new service pattern through the Internet, which users manage their data not by themselves but on the servers without directly managing it made by PCs (e.g. those which called cloud computing[15]) in recent years. This means that the entities should be more responsible for their awareness of the risk and what they actually send their information.

(2) Cross-field information security infrastructure

[1] Promotion of information security technological strategy

Under the First National Strategy, there are three key policies posted and take actions: [1] establishment of effective implementation systems of research and technology development, [2] focusing on and providing the environment of the information technology development and [3] promotion of “grand challenge[16] type” research and technology development to solve issues; 1) the information security technology is behind the use of IT that rapidly extending and 2) there is a lack of balance between the organizations and humans who supplement against the limitation of the existing information security technology, as one of the basic policy of "pursuing advanced technologies” under the First National Strategy.

In the three years of planning phase, some cases show the enhancement of the information security technology development and maintenance of the environment. In specific, many problem solving type of technology development to solve issues such as the cyber attack using bot were implemented, including research and development for detection, restoration and prevention of highjacks and the development of a safe environment using the virtual machine technologies, which aiming advancement of the information security.

Meanwhile, the management of organization and humans is not sufficient for its advancement. Some policies should be implemented in the future. “Effective implementation system of research and development” and “grand challenge type” research and development, which was developed in FY2007, need to be further

[15] A technology to allow users to use the information and application services without possessing/managing hardware or software, as it uses the virtual computer existing online.

[16] An integral development of various element technologies as a whole by setting a certain high target, based on the concept of sustainable research and development

promoted.

New issues have also arisen for the research and development, in line with the change of social conditions around the information security during the phase of the First National Strategy due to extension of the use and availability of IT.

Firstly, people became further dependant on IT along with the rapid proliferation and advancement of information equipment or devices such as mobile phones, mobile terminals and the RFID tag[17] and devices, as well as the diversification of network services[18], which could significantly increase the range concerning information security.

Secondly, it is more important to presume products and services[19] for easy-to-use as well as preventing any risks on information security due to misuse or error of the users, in design and development. (Fig. 7)

Thirdly, there are a number of malware[20], which is used to gain illegal economic benefits so that the conventional and the speed to discover new vulnerability and develop new attacking techniques accelerating so that the conventional security countermeasures are not sufficient to solve issues. In order to cope with the non-symmetric[21] situation of the attack and the defense sides, it is important to have an implementation system to develop technologies to tackle against dynamically changing threats and potential threats and the research and development to do it.

[17] Certification technology using wired non-contact communication and IC chip.

[18] It includes email, searching services, file storage, groupware, map service as network s

[19] Introduction of information security views to the universal design concept.

[20] Malware harmful to computers and users such as computer virus, worm, spyware.

[21] Attackers have high freedom in choosing attacking methods and are capable of making negative impacts on multiple systems at the same time, which is advantageous to users in most cases.

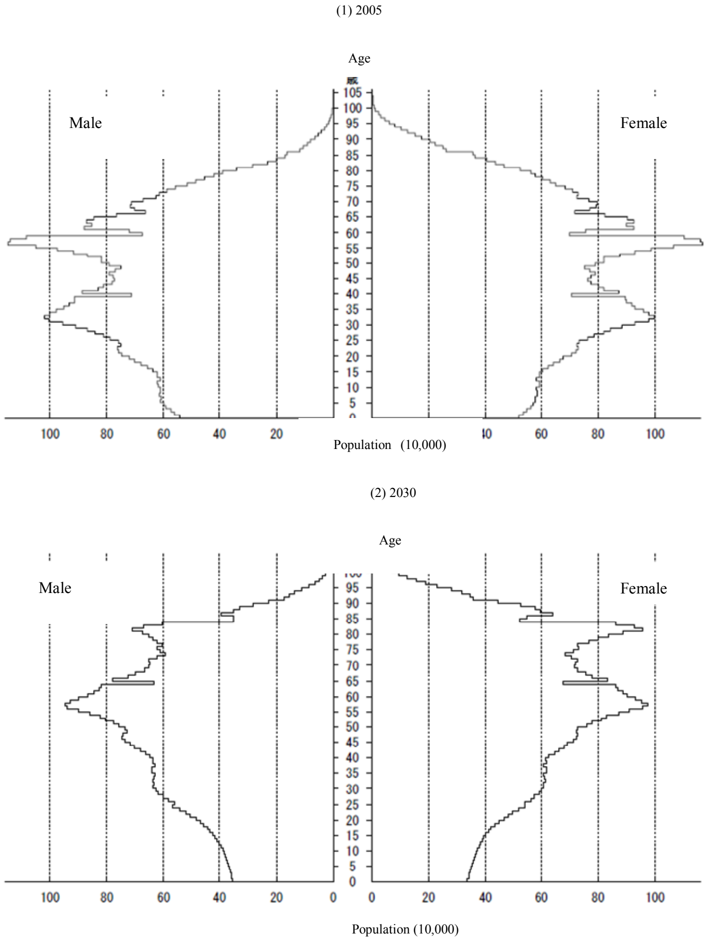


Figure 7 Changing age pyramid: Birth medium (death medium) estimate (Source: National Institute of Population and Social Security Research "Projected population of Japan (estimate in December, 2006)")

[2] Human resource development of the information security and its maintenance

For human resource development of the information security and its maintenance, various approaches were made including the studies by the personnel training and qualification scheme systematization councils for 1) development of practitioners and experts with multi-angle and comprehensive capability and 2) systemization of the qualification scheme concerning information security under the First National Strategy. As a result, the information security human resource development is currently promoted in the universities and graduate schools as well as maintenance of the framework of the career skill for the practitioners and the training programs.

In the human resource development, it is hard to see how it was achieved under the First National Strategy, since it takes time from the start the measure to achieve the results. However, there are many needs and issues related to the policies concerning the human resource development and its maintenance of the information security. For instance, the government agencies have lack of personnel involved in the information security or lack of knowledge accumulation of the findings in the government agency due to a short-term rotation of the personnel. These are the issues pointed out. Such issues pointed out have even not verified how it is important. Moreover, the personnel who are in charge of the information security also point out that it is hard for them to see a clear career path involved in the information security. If such conditions continue, the information security sections should have a difficulty to obtain excellent personnel, which leads more severe lack of personnel to promote information security.

The systematization of the qualification scheme is discussed by "Personnel training and qualification scheme systematization Council", and the qualification scheme was formed according to the report as of January, 2007 (Fig. 8). However, the information security personnel pointed out that knowledge obtained by the qualification is not the requirement to actually perform their tasks, though it is confirmed to be effective in a sense, and the insensitive to obtain the qualification is not clear enough. Therefore, the information security skills obtained by such personnel are not specifically defined, which means that it may be difficult to assign personnel to positions that suit to them.

Requirements			Information security related personnel									
Category		Sub-category	Personnel to provide Information security related products/services/solution etc. in enterprises				onnel involved in implementation of information security in government organizations and enterp					
			Personnel to provide technology related products in enterprises		Personnel to provide management related products in enterprises		anagement, preside	General official/employee	Personnel in charge of Information security measures		
			Security specialist	General	Security Consulting	Security audit			CISO or CISO supporting staff	Technology	Management
Security /literacy							α	α	α	α	α
Security policy of organization							α	α	α	α	α
Management		Management technology	C	C	A	A	γ	-	α	β	α
		Risk analysis technology	C	C	A	A	γ	-	α	β	α
		Information security policy development	C	C	A	A	γ	-	α	β	α
		Information security audit	C	C	B	A	γ	-	α	β	α
		Related knowledge	C	C	A	A	γ	-	α	β	α
		Laws and regulations	C	C	A	A	α	-	α	β	α
		Business continuity plan（BCP/BCM)	C	C	A	A	α	-	α	β	α
		Risk communication	C	C	A	C	α	-	α	β	β
		Cost effectiveness	C	C	A	B	α	-	α	β	β
		Labor plan	C	C	A	B	α	-	α	β	β
		Education/training	C	C	A	B	γ	-	α	β	α
		Physical security	C	C	A	B	γ	-	α	β	α
		Procurement management					γ	-	α	β	α
		Project management	A	B	B	C	-	-	α	α	β
		Security operation	A	B	B	B	-	-	β	α	β
Technical	Information security basic technology	Security architecture	A	B	B	B	-	-	β	α	γ
		Network infrastructure security	A	B	B	C	-	-	β	α	γ
		Secure programming technique	A	B	C	C	-	-	β	α	γ
		Security protocol	A	B	B	B	-	-	β	α	γ
		Certification	A	B	B	C	-	-	β	α	γ
		Access control	A	B	B	C	-	-	β	α	γ
		PKI	A	B	B	C	-	-	β	α	γ
		Encryption	A	B	B	C	-	-	β	α	γ
		Electronic signature	A	B	B	C	-	-	β	α	γ
		Illegal copy control/digital watermarking	A	B	B	C	-	-	β	α	γ
	Anti-virus/spyware related	Firewall	A	B	B	C	-	-	β	α	γ
		Spyware detection	A	B	B	C	-	-	β	α	γ
		Virus	A	B	B	C	-	-	β	α	γ
		Unauthorized access	A	B	B	C	-	-	β	α	γ
	Application Security	General	A	B	B	C	-	-	β	α	γ
		Web	A	B	B	C	-	-	β	α	γ
		email	A	B	B	C	-	-	β	α	γ
		DNS(Domain Name System)	A	B	B	C	-	-	β	α	γ
	OS Security	Unix、Linux	A	B	B	C	-	-	β	α	γ
		Windows	A	B	B	C	-	-	β	α	γ
		TrustedOS	A	B	B	C	-	-	β	α	γ
Level type education program			-	SV（IPA) CompTIA	CISM CISSP	CISA	-	-	SU（IPA) CISM CISSP	-	SU（IPA) CISM CISSP
Training/OJT type education program			iisec Chuo Univ. /COE CMU	iisec Chuo Univ./main /sub Kogakuin Univ. CMU	iisec CMU	-	-	-	iisec/CISO CMU	Chuo Univ. /main /sub Kogakuin Univ.	-
			-	YRP Softpia/Tec Hyogo	-	-			-	YRP Softpia/Tec Hyogo	YRP Softpia/Mgt Hyogo
			SANS/Tec	CSPM/Tec NISM SANS/Ess	SANS/Mgt	JASA			SANS/TOP	CSBM CSPM/Tec SANS/Ess	CSPM/Mgt

(1) Legend of personnel ability required for product/service/solution of information security

A Ability as a personnel directly involved in production, development and provision of the services directly linked with information security measures and have expertise of the advanced management method and use/apply these methods to the products.

B Concerning information security measures,

- Ability as a personnel who is involved in production, development and provision of the services directly linked with information security measures, and understand requirements of information security, and use/apply these methods to the products
- Ability as a personnel who is involved in the management type products to understand the methods and products other than non-management related for a certain degree and make assistance to customers

C Ability at least required as a knowledge in production, development

(2) Legend of ability required for personnel concerning information security in government organizations and

α Ability to fully understand methods and objectives of information security measures, including knowledge and skills about products provided, and use and implement it by taking a leading role in the organization.

β Ability to understand methods and objectives of information security measures, including knowledge and skills about products provided, for a certain level, and use and implement it in cooperation with outside personnel in the organization who have expertise.

γ Ability required in an organization as knowledge concerning information security

— Ability not required for assigned tasks

Figure 8 Requirements for the information security personnel and various education programs

(Source: Information Security Policy Council "Personnel training and qualification scheme systematization expert Council report" (January 23, 2007))

[3] Promotion of international partnership and cooperation

The government aimed “a constant information sharing through the establishment of POC[22] with the information security organizations of the rest of the world, (omitted) and employment of Japan’s best practice by the countries through the partnership[23]”. As a result of the policies implemented, the information security of the Cabinet Secretariat became acknowledged as its organization, though it is now required to promote the international partnership and cooperation based on specific policies. Meanwhile, the international environment around the information security has drastically changed in the past three years of the planning phase. Therefore, it is necessary to consider such changes for planning the future international partnership and cooperation schemes.

Firstly, the international partnership for information security requires discussion and countermeasure from various perspectives such as the national security, the critical information infrastructure[24] protection, continuity of the global economic activities and cyber crime prevention. Therefore, cross-field measures are necessary in addition to the conventional international cooperation for the partnership between the organizations specialized in the various areas.

Secondly, the threats such as unauthorized access, phishing, spam mails, target type attacks and infection of malvirus through websites are thought to increase in the future, which occurs all over the world beyond the borders, without effective measures taken through the international cooperation. (Table 3)

Thirdly, the confrontations in a real society could affects the cyber space further, as shown partially in the report from a specific country concerning the possibility of the attacks for stealing information from various foreign government organizations as well as the attacks to some government organizations in foreign countries to disable their services.

[22] Abbreviation of Point of Contact.

[23] “ What Japanese society should be from the viewpoint of information security. What the assessment of policies should be (February 2, 2007, confirmed by Information Security Policy Council).

[24] It is explained that the critical information infrastructure is [1] information to support critical infrastructure, [2] information infrastructure supporting the extremely critical part of e-tasks of the government or [3] all or some information infrastructure extremely important to the national economy, according to the recommendation by OECD Information Computer/Communication Policy Council and Information Security Privacy Council, “Recommendation of the Council on the Protection of Critical Information Infrastructure”. It is used without definitions by other organizations such as G8, ITU and the international conference concerning critical information infrastructure (MERIDIAN).

Fourthly, it is indispensable to use the Internet when the government agencies and the critical infrastructure providers provide the services or to issue important information, as their dependency on the information system became quite high. In the meanwhile, as the threats may occur beyond the national borders, the importance of the least role of the government offices must play is increasing to promote the cooperation of the government agencies and private sectors in order to achieve the sustainability of business from the viewpoint of information security.

Fifthly, the industrial activities became further specified and go into specific aiming the optimum procurement and production for a global scale, due to the globalization and borderless of enterprise activities. As important corporate information are exchanged beyond the national borders to cope with such corporate activities, lack of integrity, confidentiality and availability of the information through the information system may deteriorate the development of global business activities of Japanese companies if a certain level of information security standard is not secured by the local companies.

Similarly, it is obvious that the products and service qualifies provided by the supply chains are not available for verification as a series of process (supply chain) concerned with the information system design, material procurement, production and supply became globalize and complex. For some cases, there are risks of national security in terms of the information system procurement by the government organizations, without a specific measure to secure a certain level of quality such as prevention of the malware affected products from being distributed in the market.

Table 3 Transition of confirmed cased of unauthorized computer access

Fiscal year Category		2003	2004	2005	2006	2007
Number of recognition (case)		212	356	592	946	1,818
	Access from foreign countries	35	37	53	37	79
	Access from the country	158	303	487	855	1,684
	Origin of access not specified	19	16	52	54	55

(Source: The National Public Safety Commission, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry "Situation of research and development of technology concerning unauthorized computer access acts and access control functions" (February 29, 2008))

[4] Crime control and protection and remedy of rights and benefits

Various IT infrastructure was further established such as improvement of the cyber crime[25] control with various training programs, formulation and enhancement of investigation and analysis devices and knowledge accumulation and systemization concerning Digital Forensics[26] and the basis of public and private sector cooperation concerning cyber terrorist attacks[27] under the First National Strategy.

Moreover, as the cyber crimes easily go beyond the national borders, the government promoted active participation in the global arena such as G8, cooperation of the investigation organizations, discussions on the system in their country and information sharing concerning the investigation techniques of International Criminal Police Organization (ICPO-Interpol) and holding of Asian Pacific Regional Cyber Crime Investigation Technical Conferences.

In addition, “the draft of the law to revise part of the criminal law to deal with the internationalization and organization of the crime and advanced information processing” was submitted to the 163rd Diet (under discussion).

Besides this, a certain progress was made for the research and development concerning protection and remedy of rights on the cyberspace and the development of the basic technology to improve the safety and reliability of the cyber space etc.

As a result, the following issues remain although the infrastructure progressed for crime control, and protection and remedy of rights and profits have advanced for a certain level.

The cyber crime increases every year. Its methods became advanced and diversified, which make the investigation much more difficult. (Fig. 9)

According to the Cabinet Office survey "Public opinion poll concerning the safety on the Internet" in 2007, more than half of the Internet users (52.3%) have concerns in using the Internet (or 45.4% to all including those who do not use the Internet). With continuous implementation of the measures to be strongly taken, the anxiety of people should not be fully mitigated (Fig. 6).

In addition, there are reports of the computer network invasion and the attack to ruin the services of the foreign government organizations. In Japan, the cyber terrorism threat became realty.

[25] Crimes using the advanced data communication network such as Internet or those which using information technologies targeting electromagnetic records

[26] Generic term of means and technology to collect and analyze data and electronic records required for identification of cause or investigation in case of crimes or legal conflicts related to computers such as unauthorized access or confidential information leakage (Digital Forensics).

[27] Those which at high risk to be affected by e-attacks to the critical infrastructure fundamental systems or those which have critical failures of the critical infrastructure fundamental system

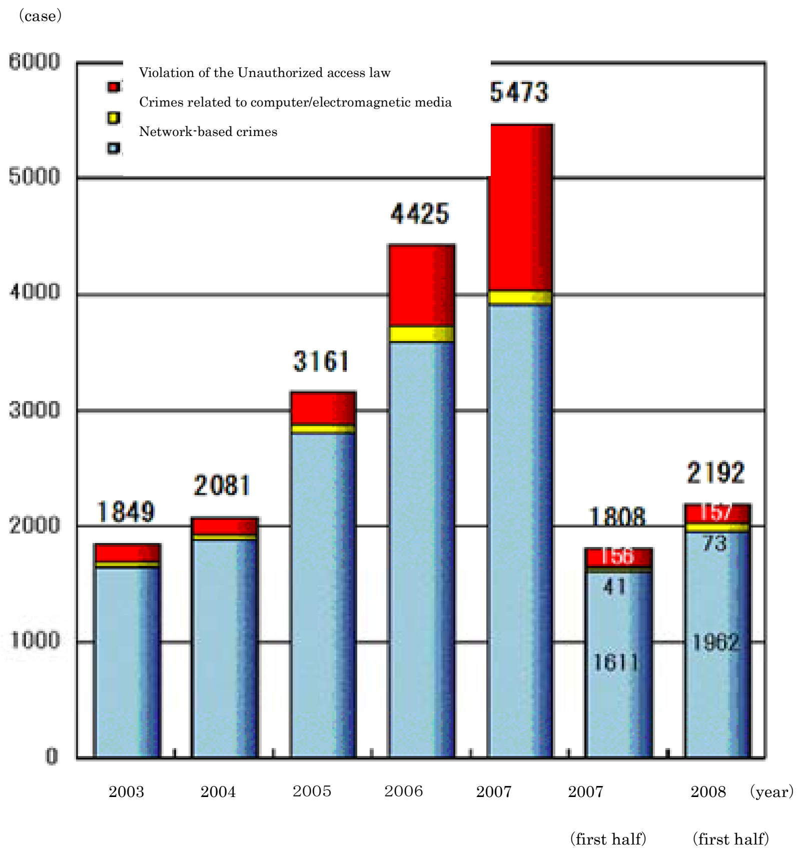


Figure 9 Transition of the number of arrest

(Source: The National Police Agency "Arrest situation of cyber crime for the first half of FY 2008"

(August 21, 2008))

Chapter 2 Basic Concept on the Second National Strategy of Information Security and the Objectivess in 2012

Section 1 Shift from the First National Strategy of Information Security

(1) Results of the measures taken under the First National Strategy of Information Security and the Status of the Second National Strategy of Information Security

The measures taken under the First National Strategy were implemented as planned at the beginning based on the conditions below. However, it is hardly said that the risks of information security is mitigated according to the reality in the current social conditions. The risks at least changed in nature, leading possibilities of large scale cyber attacks or IT defects, due to the further development of IT infrastructure, including the increase of B to B[28] and B to C[29] electronics trading online and implementation of the core information systems for various fields. This is also represented by the targeted attacks to specific organizations or individuals, or further advanced styles of cyber attacks represented by bots which is hard to detect or that the infection of malfunction is hardly recognized.

Therefore, the First National Strategy should be followed by the second by grasping the reality and taking necessary measures for improvement.

The Second National Strategy is a mid and long-term strategy which covers the entire nation according to the above.

(2) "Continuity" and "Development" from the First National Strategy

The Second National Strategy basically follows the principles of the First National Strategy from the viewpoint of "Continuance" of the First National Strategy. The First National Strategy especially focused on the preventative measures to achieve the standard to prevent the information security problems. For instance, a basic policy is defined and the countermeasures promotion policy is formulated to properly operate by specifying the rule for handling of information and technical measures in organizations. These measures should also be achieved under the Second National Strategy. It is desirable that each entity is desired to continue the utmost efforts to achieve it. In particular, the current information security standard is insufficient, such as damages incurred by malware or unauthorized access or leakage of confidential information. Therefore, the parties

[28] Abbreviation of Business to Business

[29] Abbreviation of Business to Customer

concerned must fully acknowledge that it is inevitable to improve the measures to improve the standard.

On the other hand, "development" from the First National Strategy is necessary for some cases. For instance, the level pursued under the First National Strategy was a level that was the pursuit of absolute correction[30], which is not exaggerated. In terms of the conditions of the risk related to the information security, it is not easy in reality[31]. It is because it would be necessary to consider feasibility, balance with the cost pursuing the result, and convenience against the information security (tradeoff). Moreover, the possibility of the risk to be a reality should not be ignored while the patterns of information security related risks changes every day, while pursing the absolute acceptability. Therefore, it is needless to say that the conventional measures should be constantly continued, mainly with the preventative measures, while the policy should be defined to actually take measures according to the reality. Assuming the risk being reality, it should be considered that various entities are capable of actually taking measures promptly.

The Second National Strategy continues and develops the First National Strategy from the following three viewpoints.

[1] Policies to sustainable promotion of specific measures and new issues

Firstly, it is needless to say that each entity should continue making an effort under Second National Strategy in the same manner as the approaches under the First National Strategy.

On the other hand, the measures taken under the First National Strategy mainly aimed to create the basics (framework) as a base of specific measures, as it was the start-up period of the information security field[32]. In The Second National Strategy, parties concerned should use the base (framework) developed under the First National Strategy,

[30] "Absolutely correct" under National StrategyThe Second National Strategy means perfect without any mistakes. It does not mean "integrity" (to make information or information processing method correct and perfect) which is usually used in information security related documents.

[31] "It is not easy to make the preventative measures at the level to avoid information security related issues in reality" does not mean that there should be the least possibility of failure or issues even though how much measures have been taken, or there are risks that we should admit, and it should be considered to be acceptable risk, so that it does not mean "it is not easy to make the preventative measures at the level to avoid information security related issues in reality, it is not necessary to take full countermeasures even though it is at acceptable standard). "Necessary to take measures at an appropriate level" without fail" is emphasized herein.

[32] For instance, it includes establishment of cross-governmental measures against cyber attacks, a study for the launch of CEPTOAR Council of critical infrastructure, mechanism for establishment of a public-private sector joint council for human resource development and proposal to establish a new council in international conferences.

and actually function the specific measures[33].

Moreover, it is necessary to challenge political measures against new issues that the measures were not sufficiently taken conventionally, such as measures against anxieties of using IT in the aging society which increase the possibility of misuse, increase of global movement and globalization including the increase of international development of business activities.

[2] Enhancement of measures against "Accident Assumed Society"

Secondly, The Second National Strategy has a measure with stronger correspondence against accidents, which means the enhancement of measures against “accident assumed society”. Therefore, parties concerned must take particular care for post measures against accidents such as acknowledgement and analysis of cases, communication, immediate countermeasures and restoration, assuming the cases if information security issues arise in spite of the preventative measures that have been taken. Thus, all related entities must make the utmost efforts for the preventative measures to prevent occurrence of information security related problems such as information leakage, lower quality or suspension of services of the information system occurring, while keep making efforts to cope with unexpected cases as assuming it. In case of such cases, they verify the facts such as the range and degree of influence, the level of urgency, and causes, while widely taking an immediate action and restoration measures to maintain the sustainability of business.

The entire society should understand the need of awareness, that it is not easy to achieve the information security measures to fully eliminate the possibilities of the accidents in the “accident assumed society”. Even though any issues arise, a system for the entities to have an awareness and sense of prompt measures without excessive reaction is inevitable, as well as to allow them to take an appropriate action by realizing the reality even though any issues arise.

"Accident assumed society" referred herein does not mean that people take no measures for prevention of accidents assumed or give up damages that could occur resulted from accidents.

[33] Although the enhancement of the scheme is the standard required, such as measures based on the government integral standard, there are some schemes which have improved for a certain level in a short period of time. It is necessary to rectify and improve measures in a flexible manner according to the technological innovation for IT and changes of the social system, while making an appropriate and sustainable measure for these schemes.

[3] Rationality-based approaches

Thirdly, a rationality proven approach should be achieved in "Accident assumed society", which means an effective and efficient implementation of the measures of the optimal level (the information security standard which is objectively allowable to manage changing risks[34] in various entities and the entire society) [35]. Thus, an approach backed by rationality should be made. In terms of the safety and security by the approach of information security, this method is important because it is important to achieve a balance of the cost and effects. This approach is also essential since it could maintain the usability even if the information security measures are updated, which would rather be improved thanks to the progress of the information security measures.

The full accountability is necessary for the contents and standards of the measures in order to maintain the rationality of the approach. In specific, there should be enhanced functions to identify risks or take flexible approaches to changing risks, optimal standards and responsibilities clarified.

(3) Basic Idea in The Second National Strategy of Information Security

[1] Basic Objective to be Achieved - Establishment of IT Environment with Security

One of the fundamental purposes of the information security policy is to encourage the development of the whole society by ensuring the safety and security as IT became available. Therefore, the basic goal of the First National Strategy, creating the safe environment to use IT, should be maintained as a core policy and measures should be taken for solving issues in making the policies.

The measures aimed by various entities under The Second National Strategy should lead the safety of the IT environment.

[2] Basic Principal for Measures – "Maturation of Concept "IT Security Advanced Country"

(a) Information Security Advanced Country

[34] For " accident assumed society " , the risk management method is important to predict/prevent risks, and study how to take measures to minimize potential damages or failures.

[35] It means measures to be securely implemented according to the appropriate assessment of information assets and risks, in specific.

In order to achieve the basic goal, it is necessary to advance various measures with an assumption of an ideal figure of Japan from the viewpoint of information security, as the basic principle. The First National Strategy promoted measures based on the principle a “security advanced country” or “IT security advanced nation” as described above.

However, it would be necessary to have additional elements for the concept of “Security Advanced Country” 1) stable and immediate responses and 2) the optimum standard countermeasures for development of the information security policy from the viewpoints of "enhancement of responses to "accident assumed society" and "achievement of rationality proven"). The concept of high quality and reliability under the First National Strategy meant vaguely pursuing the perfection, though it should be regarded as that they pursue higher quality and reliability to achieve the optimum information security standard required for each entity in order to avoid any information security issues in reality.

While Japan should pursue the achievement of the optimum level of actions and responses to avoid the information security problems under The FIrst National Strategy on Information Security, which is not the pursuit of absolute results. Rather than that, the goal is to be “a mature information security advanced country” to practically achieve the effective and efficient implementation of the optimum level of measures, clarification of the liability, high quality and reliability to achieve the optimum level of information security required by each entity and the safety and security of the users. The entities who might be incapable of taking information security measures[36], such as information handicapped or aged[37] should be supported by their optimum information security standard to achieve.

(b) Establishment of strong "individuals" and "society" in the IT age

In order to proceed the information security measures aiming the mature information security advanced country, various measures need to be taken. These measures are based on specific measures of IT related technologies and systems.

However, it would also require a change of the entire society as a group of individual entities to use IT with taking the information security measures implemented. In a sense, Japanese citizens and society should not pursue absolution for the security but need to:

[36] Handicapped to have difficulties to use the information and communication technologies due to various reasons under this National Strategy.

[37] Although it might be categorized as information handicapped, it is assumed to be the cases that aged have information security problems by their misuse.

1) understand that it is necessary to be prepared against the unsuccessful cases even though they aim to fully eliminate the possibilities of accidents (though the utmost efforts must be made for the countermeasures),

2) Even though any information security problems arise, the person concerned should take appropriate measures to solve the problem and the parties around him or her should understand the level of severity of the cases by understanding the real meaning of the issues and its scale of damage.

Accordingly, it is necessary for the entities of the information security measures must proceed the measures faithfully and in a transparent manner, in addition to that the citizens and the entire society accept a certain level of risk, not being the perfection, and support themselves based on the reality. This means that the establishment of strong "individual" and “society” in the IT age is inevitable, for them to spontaneously think issues rationally and subjectively.

(c) Cooperation with the world and initiative

The information security policy of our country should become more practical based on the reality to create the IT security environment, by proceeding the measures based on the principles of the mature information security advanced country. The information security policies of Japan should become more available to be accepted by the international society, which allows us to make statement or contribution to the world as a true IT advanced nation.

Japan will cooperation with the world with confidence in their methods based on the mature principles of the information advanced nation and take appropriate initiatives.

At the same time, Japan is required to pay sufficient attentions on collecting information such as the global standard measures, the most advanced technologies and new risk trends, as well as to catch up with the global standards.

[3] Measures for realization of the basic target – promotion of measures taken by the parties for implementation and awareness of the information provider

(a) "New model of the government and private sectors"

It is indispensable to maintain and develop the First National Strategy after three years from the launch, and to pursue participation of all the entities concerned in IT society with awareness and appropriate roles. The Second National Strategy is to further improve the policies through the maintenance and development of the “new government and private sector cooperation model” defined in the First National Strategy.

(b) Discussion from both sides to implement measures and to provide information (two approaches)

"The new government and private sector cooperation model" under the First National Strategy places the emphasis on the participation of all entities concerned with the IT society and lists the following entities:

1) Measures implementation entities, or the entities actually apply and take measures ([1] government agencies and local governments, [2] critical infrastructure, [3] enterprises, and [4] individual)

2) Entities to promote understanding and solutions of issues, or the entities who promote the understanding and solution of the issues by providing techniques of the measures and support the development of the environment ([1] government agencies, local governments as the entities that formulate and implement the policy, [2] elementary and primary educational institutions, higher education organizations, research and development/technical development organizations, [3] business entities and non profit organizations to create and develop IT infrastructure such as development of the information systems and provision of communication services (“information related businesses” and “information related non-profit organizations,” hereinafter), and [4] press)

This framework should be maintained under The Second National Strategy.

However, implementation of measures is not sufficient only with the policy, from the viewpoint to establish the strong “individual” and “society” in the IT age to achieve the rationality-based approaches as well as for enhancement of countermeasures against “accident assumed society". Some information assets that had to be protected by the information security measures were given not only by an entity to implement the measures but also from other entities. Although all entities concerned in the process of information exchanges aim to get rid of the possibilities of accidents, they should deepen the understanding of the risks for unsuccessful cases.

Therefore, The Second National Strategy will cover the side to entrust information as the objects of its policies. as well as the side to implement measures[38] including measures implementation entities[39]. The Second National Strategy will explicitly deals;

3) An entity to entrust information[40] such as personal data etc. (and an entity to maintain information[44] at the other end).

Therefore, The Second National Strategy adopt the following two approaches:

1) the conventional approach under the First National Strategy focusing on the entity to support the measures and the one to directly implement the measures, and to supplement and strengthen this approach,

2) new approach assuming the entity to entrust information.

[4] Policy fields for the implementation of measures under the Second National Strategy of Information Security

Accordingly, the field of policies to implement measures for development the safe and secure IT environment in the future may be categorized from some aspects. It shows the policy fields of The Second National Strategy should have multi-aspects for a certain extent.

(a) Actions from identification of issues, preventative measures, and post-actions

The actions include a series of response from the identification of issues, preventative measures and post-actions after an occurrence of problems, which should contribute to

[38] “Entity that promote understanding and solution of issues (”Measures supporting entity“, hereinafter)” under the First National Strategy is included as well as measures implementation entities.

[39] The First National Strategy lists the following four entities as the entity to actually apply measures and implement them.: government agencies, local governments, critical infrastructure, enterprises and individuals.

[40] Including the entities that actually entrust information and would potentially. In other words. all the entities can be entities to entrust information.

[44] It refers to the same scope as the measures implementation entity, in effect.

[46] Information security governance aimed by the government agencies means the corporate governance, effectively promoting the information security measures as part of the corporate governance of government agencies under this National Strategy.

the improvement of the information security policy being one with higher effectiveness to cope with the problems.

(b) Actions from technical aspects as well as the system and the human related

Promotion of the information security measures would require a comprehensive approach from technical aspects related to the measures, as well as systems and human related aspects. Such balanced measures are required. The Second National Strategy also applies a comprehensive measure from technical to human resource development. The system including disciplines will also be studied.

(c) Actions from promotion of the information security to international activities for the information security

Given the fact that IT is used beyond the national borders, the information security policy only for domestic use is not sufficient. While domestic measures should be advanced, it should be improved to the policy organically in line with the measures for the international relations.

(d) Actions ranging from the field directly related to individual entities such as daily life and economic activities of Japanese citizens to those which deeply related to the nation as a whole such as security and culture of Japan

The information security policy related field to act under The Second National Strategy includes matters which have direct and significant relations to daily lives of individual entities such as promotion of cautions for individuals to use IT and how to manage personal information obtained through economic activities of enterprises. In addition, there are fields related to the national affairs including international information sharing of threats on the information security, which is critical for the national security, and fostering Japanese culture which the information security is the key.

Section 2 Objectives in 2012

The following explains the objectives of Japan in 2012 when The Second National Strategy will be ended after three years of actions. This is based on the four implementation fields and four cross-field foundation, in the same manner as the status in 2009. The entity to send information is described in (5) “the four fields to take measures” for convenience.

(1) Four field to take measures

[1] Government agencies and local governments

[Government agencies]

Due to the use of IT for administrative fields for improvement of convenience or people and simplification of administrative affairs as well as promotion of the advancement, people will pay more attentions on the safe and secure e-government and their requirement on the information security should further increase. Therefore, the government agencies should take the information security measures as a model pattern for various organizations at home and abroad and make the utmost efforts to aim the information security standard to provide safe, secure and effective administrative operations and services to live up to the expectations of the people.

Parties concerned will take measures aiming the following as of 2012 under The Second National Strategy as the milestone for the future.

First is "the enhancement of the organization and the system for the establishment of the information security governance in the government agencies"[46]. In 2012, all government agencies would have established the system to actively take information security measures, and the rational actions have been taken to establish the information security governance of the government agencies by establishing the mechanism properly integrate the information security policies onto their information systems. Under the circumstance, the government promotes the information security personnel human resource development and securing as scheduled and the actions to take appropriate information security measures in a timely manner, including the budget making. There should also be a mechanism to accumulate and use technical knowledge.

Second is "enhancement of the post-action capabilities in the government agencies". In 2012, measures have been taken for post-accidents with care such as the information system in case of disasters or failure of the information systems owned by the government agencies depending on the priority or importance of the administrations supported by the information system, and the sustainable business plan was specified for necessary systems. In the case of accidents, the emergency responses and restoration should be focused through the cooperation of the organizations concerned.

[Local governments]

Under The Second National Strategy, the government makes utmost efforts aiming implementation of the desired information security measures for various local governments and for a wide range of administrative fields.

The social conditions that the local governments would face in 2012 are as follows concerning the information security. Many local governments start to feel the difficulties to maintain the investment for the information security including the information security at the current level, due to decrease of population and severe financial conditions. Therefore, they are actively looking for a way to effectively secure necessary function and security in their system with a certain cost, through partnership between local governments. As the administrative affairs of the local governments is in a significantly wide range, the desired level information security should be secured for various fields, and the local governments themselves are also desired to actively take on the information security issues due to the advancement of decentralization.

The parties concerned should further proceed the future measures aiming the information security of the local governments according to the social conditions assumed in 2012 as follows.

First is “advancement of the information security measures over the entire administrative affairs in a wide range, regardless of the scale of local governments”. In 2012, there should be a cooperative relationship between the government, local government agencies, public and private sectors and NPO etc. to support the challenges of the local governments including small governments such as cities, towns, and villages. Under the circumstance, local governments proceed their own measures which suited to their scale, so that desirable measures should have been taken by most of the local governments including small-sized local bodies which are lag behind to implement the measures due to various restrictions. In particular, for promotion of the measures for small-sized local bodies, although it is desirable to have an effective measure, another effective method started to apply actions that were proven to be successful. Effective measures with limited resources are actively pursued such as collaboration of local governments to consider the measures to be taken.

Moreover, the information security related measures would have been taken for the fields that local governments hardly handle, according to the individual relationship between the organizations concerned of the national government and local governments by 2012.

Second is “activation of the activities which take place in regions from the viewpoint of information security. In 2012, there should be an environment designed for the local governments to promote local activities from the viewpoint of information security. This movement results in the base to foster human resources who have knowledge to play a key role on the information security measures in the regions.

[2] Critical infrastructure

The government has the Second Action Plan for the critical infrastructure, including the spontaneous measures desired for the critical infrastructure providers to take and those which desired for the government and related organizations, mainly the Cabinet Office, as the systematic framework. The government aims to minimize IT failures in the critical infrastructure[47] by the framework of the public and private sectors as specified in the Second Action Plan, protect the critical infrastructure to prevent significant influences on the daily lives of the citizens and the social economic activities as well as to confirm the availability of the services of the critical infrastructure providers and immediate measures for restoration against the IT failures.

The information security measures of the critical infrastructure are summarized in the Second Action Plan, which includes the spontaneous actions of the critical infrastructure providers. Therefore, it is not appropriate for the critical infrastructure providers to be mandated to take actions assuming the status in 2012. The plan only shows the future expected to be achieved, for showing the direction of the entities concerned including the critical infrastructure providers.

It is assumed that the entities concerned in the information security measures under the Second Action Plan will take actions aiming “to prevent significant influences of IT failures on the people’s daily lives and socioeconomic activities". The government therefore should make utmost efforts to achieve the goal for the future as below:

First is “establishment of a subjective approach and cooperation of the government agencies and critical infrastructure providers”. The entities concerned with the information security measures understand the necessary measures that they should take according to the critical infrastructure services and the service level required. The entities concerned correctly recognize their status and define their own targets subjectively. They

[47] National StrategyThe Second National Strategy defines “IT failure” as “those which are resulted from failure of the IT functions, among “debug occurred in the critical infrastructure (e.g. the status unavailable to maintain a certain service level).

are taking necessary measures as their own, and review the activities on a constant basis. They are also able to understand the status of action of other entities for voluntarily cooperating each other.

The entities concerned understand who have what information, who and what information should be shared with and what they should do depending on the scale of the IT failure. They are able to cooperate with other related entities for cooperation as required to take measures in an integrated manner, in addition to their spontaneous countermeasures.

Second is “generalization of the value of the information sharing concerning the IT troubles”. They understand the need of study from the corporate management, not only from the viewpoint of the maintenance and operation of the information system for the information security, as the sense of the so-called “information security governance” is fully penetrated so that the responsible persons of the system maintenance and corporate management both appropriately involve in the issues as well as trying to announce the information security measures of the infrastructure whenever possible. The value of the maximum information sharing is actively appreciated for enhancement of the information security measures for the social infrastructure.

In this system, the critical infrastructure providers recognize that IT failures in their business should not be concealed but need to be shared by the parties concerned who seeks the solution. Parties concerned who are taking measures are able to obtain the information such as the occurrence of IT failures, share the information with external entities concerned through the information sharing framework established under the First Action Plan such as the CEPTOAR for each field or CEPTOAR council for official or unofficial cooperation.

Third is “the generality of the quick response system to the environmental changes”. Various information at home and abroad concerning the information security of the critical infrastructure comes to the Cabinet Secretariat through various policies of the government, risk communication between the entities concerned and international partnership and cooperation. The Cabinet Secretariat cooperates with the entities concerned accordingly, to take on the general coordination to further promote effective measures.

In particular, if significant threats or risks concerning IT failures are recognized and it is difficult to solve these issues only by the critical infrastructure providers, the Cabinet Secretariat, the critical infrastructure special Council and the CEPTOAR council study on the solutions and cooperate to achieve the solution in a prompt manner.

[3] Enterprises

The government continues to make utmost efforts aiming the world leading class of standards of the information security measures in the enterprises under The Second National Strategy.

As a result, it is thought that the society that the enterprises face should be as follows in 2012, concerning the information security.

The working population decreased due to retirement so-called "baby boomers generation". The business operation model should be shifted to ones with effective and high productivities due to the advancement of IT for business activities by then. Therefore, the dependency on IT of corporate management rises further, which increased the importance of the information security on the corporate management. Moreover, it became much more necessary to have efficient business operations using offshore business bases, so that the outsourcing and direct investment to overseas bases increased, as well as specific categorization and expertise of corporate activities for the optimum production in the international market due to globalization of economy. Therefore, people start to recognize the necessity to take a full scale information security measures in East Asia regions where especially have a close relationship with Japan, as well as India and Middle East to secure these bases as a safe and secure business hubs. In addition, as Japanese economy is now part of the global Supply Chain Management network, Japanese companies are required to take the information security measures. Especially, it is currently an immediate issue for small and medium-sized enterprises who have strong global competitiveness in terms of manufacturing to take the measures.

In the society of the year 2012, the parties concerned will take the following measures aiming the following for the corporate information security policies.

First is “the standardization of the recognition as part of the corporate management concerning the information security governance[48], and the tool to use it”. By 2012, companies should fully understand the importance of the corporate information security, including the management, and the systems required for promotion of the measures are established. The information security is considered to be a critical element in corporate management, in line with the financial control. As the importance of information security governance varies depending on the companies according to level of the information

[48] The information security governance of companies, which is aimed under this National Strategy, means that the information security measures would be properly implemented as part of the corporate management.

assets in use, companies who use the information assets frequently further recognize the importance of the information security governance, including their management, as they fully have the status information on the in-house security measures though the external auditing etc. For the measures, as the balance of the cost and usability is also significantly important, entities concerned to support the policy are actively conduct various activities to promote the measures, while the various products or services taking care of such factors, are available.

Second is "development of emergency responses and the business sustainability for enhancement of the response to "accident assumed society". By 2012, companies further take preventative measures for the information security itself. Large scale companies or enterprises with a large importance of information security are also developing the post-response systems.

Third is "development of appropriate measures in each enterprise ranging from large enterprises to small and medium-sized enterprises". By 2012, appropriate and necessary measures are taken regardless of the size of companies, such as provision of the useful tools for small and medium-sized enterprises which had lag behind of the information security measures in the past.

Fourth is "advancement of the information security measures of Japanese Company offshore bases, regardless of countries". By 2012, the government and Japanese companies fully recognize the importance of prevention of various information security related issues and take measures, including the leakage of the customer information in their business hubs overseas. Moreover, the Japanese government and the governments of the business hubs share the sense of importance of the measures to provide a secure and safe IT environment for enterprises in cooperation of the public and private sectors.

[4] Individual

The government continues to make the utmost efforts to minimize the number of individuals who have concerns in using IT[49].

As a result, the society that the individuals face in 2012 concerning the information security is assumed to be as follows.

[49] The goal herein is an objective to be realized in the area of individuals to create a secure IT environment under IT Basic Laws Article 22. This does not mean that the individuals would have no concerns in using IT as a result of the negligence in the sense of risk using IT.

Thanks to the rapid increase of IT available in educational institutions and enterprises, a wide range of people from youth to the senior citizen have computer literacy. Given the fact, using computers is not a special thing for them in their daily lives, as most of households have broadband Internet services. In line with this, various devices including IT electric appliances or game machines are connected to the Internet to create various services which are widely available for our daily lives. Moreover, the expansion of the Internet based services enables various interactive communication after the complete transition of the broadcasting from analog to digital in 2011 and new mobile communication services with higher technologies for the network connection. The network-based terminals in our daily lives such as mobile phones are also advanced in terms of the performance.

Parties concerned take measures aiming the following for the individuals in the society of 2012.

First is “expansion of the IT use of the individuals with improvement of the sense of security”. Individuals became more relying on IT in their daily lives as they actively use the network services for personal computers, mobile phones, TV and game machines, etc. At the same time, many individuals come to acknowledge the troubles on information security related to mobile phones and house electric appliances with built-in systems, not only personal computers. Therefore, the products with high reliability became popular. If any troubles occur with IT, most of the individuals are capable of making an appropriate measures based on the information provided by the vendors.

Second is “improvement of the balanced sense of security which is for both service providers and users”. There are many opportunities for individuals to provide their personal or confidential information to others in using services and the companies and organizations that run the services are paying attention on the protection of personal information. Disclaimers of risks including personal information policy and information protection level are common for the services. On the other hand, the number of individuals who determine whether the information should be provided or not is increasing, as they understand the benefits and risks to use the information, regardless of the difference of the volume of risk information of the service users and providers, or asymmetric phenomenon of risk information.

Third is “start of the measures to individual who understand the risks but take no measures”. There should be individuals unprotected even though they understand the risk in using the services, as well as those which has no literacy in IT. In order to solve the issue, the service providers abolished the information security management system relied on the users in cooperation each other, as they start recognizing the importance of responsibilities in providing their services and products as the first step of the countermeasures.

[5] Entities to entrust information

While the entire society pursues a rationality-based approach in the information security under The Second National Strategy, the government aims to make utmost efforts allowing the entire society to consider their own issues concerning the information security from the subjective aspects, including the entities to send the countermeasure information. As a result, Japan is assumed to be as following in 2012, for the entity to entrust information.

First is "improvement of the sense of the entity to entrust information as a whole" The individual entities are enabled to pay a certain attention unconsciously on the necessity of information to be sent as an electronic data and acceptability of the risks in case of accidents through the promotional activities and provision of a model agreement.

Second is "achievement of the technical development for the information security for those who have lack of knowledge for the countermeasures against accidents. The development of technologies contributes to protection of the information sent, without measures taken intentionally. [reference: (2) 1] promotion of the information security technological strategy in 2012]

(2) Cross-field information security base

[1] Promotion of information security technological strategy

The dependency on IT has risen in the whole society and the coverage and importance of the information security have significantly increased. The government should make the utmost efforts to make Japan's research and development of the information security to be proceeded most effectively or efficiently in the world, under The Second National Strategy. As a result, the society should be as below in 2012 in terms of the research and development, and technological development concerning the information security.

NGN[50] (next generation network) and IPv6[51] would have advanced by 2012. The advancement of the fusion of the point-to-point communication and the mobile communication, a safe portal websites to apply various functional components including authentication, charge, rights management and customer data management became available so that the third party started to increase new services, other than that of carriers. Moreover, all the television broadcastings include the ground wave has shifted to digital, to allow a wide range of use of the data broadcasting and interactive services using the advantages of the fusion of communication and broadcasting. As a result, the network services such as SaaS[52] and ASP[53] became further diversified for the specific uses of enterprises and individuals, as well as a high added-value trend thanks to the collaboration of the services.

Under the circumstances, enterprises actively use the network services for efficiency and restructuring of the tasks, for various purposes including online conference, work records and travel expense reporting. People also use the benefits of various services without being keen on the location or type of terminals. In the offices and home, home electric appliances such as lighting fixtures and air conditioning units are connected to the network in addition to the personal computer, information electric appliances and game machines through the home server.

Thus, in spite of the improvement of usability, there are threats in the information security increased such as unauthorized computer access etc. The current major concern is how to protect the entire life of people, not only computers and information. As the services provided only became popular for interaction, it would be difficult for users where the confidential information, personal information and certified information is stored and where such information should go to, as well as the categorization of causes of the failures. Therefore, it is more important to provide reliable products and services at a reasonable cost under the environment.

In addition, young people and aged are now further exposed to the risks of the information security due to the popularity of IT in the daily life. Therefore, security devices which the information security measures are fully proven in advance are available as a category of the information security. The products have been proven for its functions of the information security instead of useful functions or freedom of use.

In the society in 2012, the parties concerned will take measures aiming the following

[50] Abbreviation of Next Generation Network

[51] Abbreviation of Internet Protocol version 6

[52] Abbreviation of Software as a Service

[53] Abbreviation of Application Service Provider

for the information security technological strategies.

Specifically, first is “provision of terminals and information appliances which require no information security measures taken by the users”. The security measures using anti-virus software and vulnerability correction programs were taken by users. The measures also were taken to allow the users to acknowledge the importance of information security. By 2012, while continuing the measures to improve the sense of urgency for information security through promotional activities, the users have secure information environment without any burden to them. From the viewpoint of the risk management of the information security against the cases of mistakes or misunderstanding of aged due to their aging of memory, IT products should be available with appropriate information security settings in advance for delivery, for instance. Safe and secure equipment and software taking care of the accessibility standards are available.

Second is “popularity and establishment of the development methods focusing on security at the design phase”. By 2012, the information security is widely recognized as a factor that should be considered from the design stage, in the same manner as the quality requirements of the software and system for its reliability and performance. Establishment of the method to develop software in an efficient and safe manner, and accumulation of know-how and human resources through the development phase using the method have contributed to the extension of the scope for information security measures and prior evasion of the vulnerability and serious defects with reasonable costs. Moreover, for instance, the development of such methods are considered to be an important added value factor of products in the field that Japanese companies provides advanced equipment and services, such as mobile phone and embedded equipment including IC card/ This increases the international competitiveness of the Japanese companies.

Third is “commonality of the patterned description and assessment methods of the risk”. Such commonality enabled prompt risk information sharing concerning software and information systems. The commonality also significantly contributes to objective assessments of the danger of new threats, establishment of efficient methods of secure software development and determination of the rationality of information security measures, etc.

[2] Information security personal development and maintenance

Under The Second National Strategy, the government and various entities take various measures to encourage excellent personnel to the area of information security, regardless of public and private sectors, as the importance of IT security personnel is fully recognized in the society and the jobs are attractive to people, with the increase of IT dependency of the entire society. As a result, the society will be as below in 2012 in terms of human resource development and its maintenance concerning information security.

First is "increase of needs for IT security personnel by the government agencies and commencement of the measures". The government agencies have higher needs for the personnel who support information security and acknowledgement of the importance of such human resourced, backed by the increase of threats in information security. With the increase of the sense of needs, a roadmap to foster and secure the information security personnel required by the government agencies were developed, and the information security personnel training and maintenance are actively promoted according to the roadmap.

Second is "increase of needs for IT security personnel by the private enterprises and commencement of the measures". As the IT dependency of private companies further increased for efficiency of work, they are in need of information security specialists who are capable of coping with the advancement in information technologies, in terms of the information security which became the key factor of corporate management by this time. The government provides the environment and infrastructure for the information security personnel so the enterprises promote the training and maintenance of the information security personnel.

Third is "development of environments concerning the information security capability improvement". Information security sections of enterprises, including the private organizations, present information security qualifications as the requirements or advantageous factors for recruitment. Therefore, there is an environment to improve the capability of personnel involved in the information security business to begin. From the viewpoint of the personnel in the information security, it may be an incentive for them to improve their capability to clearly show their career paths with the requirements for qualifications. On the other hand, there is a sign that both public and private organizations that employ experienced personnel in information security have a sense of need for education of personnel to be specialized in the information security.

[3] Promotion for international partnership and cooperation

Through the measures taken by governments to realize a secure IT environment globally under The Second National Strategy, Japanese government makes the utmost efforts to make the public and private sector cooperative schemes being the most advanced practice contributing to the world.

Under the current circumstance, the global situation that Japan is facing for information security will be as follows in 2012. As IT became common in people's lives all over the world, users enjoy various communications beyond the national borders. As a result, IT is widely recognized as a tool to bring about the global innovation beyond national borders with an amazingly low cost, compared to the conventional practices for all entities. IT even enables malicious users to act globally at a low cost. IT-based large scale data storage and business management could also make large scale influences incurred by negligence or accidence, which results in a significant affects beyond the national borders.

In the area of the critical information infrastructure, IT is widely used not only in the business management using the information systems upon pressures from the competition between enterprises due to deregulation and needs for the improvement of usability of consumers, as well as the trading with consumers. The critical infrastructure enterprises to provide the borderless services are further required to consider the information security policies of various countries other than the dependency of entities and connectability of the users beyond the national borders. In order to cope with the situation, Japan started to cooperate with other governments who took measures from the early stage and makes efforts to apply the most advanced best practices adapted to the environment in Japan for securing the business continuity. Moreover, the government also promotes an organic partnership at home and abroad such as presenting the advantages of the government and private sector cooperative systems in Japan under the Second Action Plan.

In terms of the enterprise activities, globalization has led specific categorization and specialization in the business activities, as well as the increase of offshore outsourcing and direct investment to foreign countries. Quite a number of products and services are manufactured or provided through the IT-based global supply chain. Economic activities are conducted beyond the national borders so that the roles of global companies are increasing from the viewpoint of promoting the information security measures in the world.

As it is obvious in the requirements of corporate governance and enhancement of the governance on the financial auditing, the information security could also be the matter for regulation or governance if business activities of enterprises are required to be controlled under a certain regulation and governance. However, the government considers the support and promotion of globalization of corporate activities as an important issue, and continues their efforts to provide a secure and safe IT environment for enterprises by controlling the regulations and governance concerning the information security not to be excessive, through intergovernmental cooperation beyond the national borders and cooperation between public and private sectors.

In terms of the individuals, the IT population increases mainly for young people all over the world. The individual users in the world are able to access unlimited number of information through IT, which enables them to do free activities for social, cultural and political activities beyond the national borders. On the other hand, there is a rapid increase of unprotected users against IT related risks, in countries which the use of IT rapidly increases, which may also rapidly increase the needs for restrictions on IT services to cope with such issues. Japan continues the efforts to promote the balanced information security policies in terms of freedom and control between the public and private sectors.

Accordingly, the proliferation of IT encourages people to have free idea and actions of worldwide and results in new creation and innovation of things. On the other hand, IT will become an important item that the government should play the least role to maintain the usability.

The parties concerned should take measures aiming the following international cooperation and alliance of the information security by assuming the status in 2012.

First is “implementation of the policies which cope with globalization and linkage to the world". The government understands that a domestic policy concerning the information security could make an influence of the global activities of entities including enterprises. The government also carefully pays attention on the trends of other governments and international agencies to reflect necessary elements to the policies in Japan. At the same time, policies of Japanese government called the best practice are employed by countries, regions in a close relationship and even globally, and the government provides an environment of the domestic information security, which should also be needed by the rest of the world. Accordingly, the actions taken at home and abroad have an organic linkage.

Second is “exercise of the initiative in Asia in the information security field”. The Cabinet Secretariat Information Security Center (NISC) strengthens the function as POC, in the same manner as the First National Strategy, and conducts the activities as a key for international information linkage concerning the information security policy and operation. Especially, Japan is regarded as the gateway for Asia to Europe and America. In terms of information security, recognized as an information security advanced country in Asia.

Third is “contribution at the global level to formulate the information security culture”. Not only policymakers involved in the information security policy and the enterprises that the information security would directly affect their credibility, but also personnel in a wider range of policies and all IT users, should have a higher sense of importance of the information security for its promotion. Therefore, Japanese government makes efforts, in cooperation with international organizations and other countries, for improvement of the sense of information security at a global standard.

[4] Crime control and protection/remedy of the rights and benefits.

Under The Second National Strategy, the government should continue utmost efforts aiming to create a safe and secure cyber space through advancement of the crime control and protection/remedy of the rights and profits

With the efforts, the society in Japan should be as below in 2012.

IT improves the convenience of people in their daily life and it is functioned as a social infrastructure. Therefore, cyber crimes or violation of rights and benefits could make a serious influence on people in Japan. Under the circumstances, the patterns of cyber crimes became advanced and diversified. Therefore, it is inevitable to properly promote the crime control measures to maintain the safety and reliability of the cyberspace.

Therefore, the cyber crime control is currently strongly advanced. Moreover, the sense of importance for measures against cyber crimes such as preventative measures, prevention of increase victims or measures to prevent information leakage has risen among people, compared to the past, and the individuals and society are actively taking measures on crime control and information security.

In addition, the development and penetration of various information security technologies provides more options for people to choose to improve the safety and reliability of the cyber space.

The society in 2012 should be as below concerning cyber crime control and remedy of the rights and profits, which the parties concerned should take the measures in the future.

First is “enhancement of crime control measures”. In order to achieve the safe and secure cyber space, it is critical to arrest cyber criminals in an immediate and appropriate manner as well as to promote the measures for the crime control. Therefore, the government is strongly promoting the measures for the crime control. In addition, they also promote the development of infrastructure against the increasing threats of terrorist attacks in the cyber space.

Second is “improvement of the awareness and fulfillment of knowledge for countermeasures”. It is important for individuals to obtain the knowledge to avoid the cyber crimes and implement it in order to create a strong IT society against the crimes and violation of the rights and profits. Therefore, the government is promoting effective public relations concerning the issue.

Third is “maintenance of the infrastructure for protection and remedy of the rights and profits”. In order for people to use the cyber space in safe and security, it is inevitable to have the protection measures of the rights and benefits in the cyber space. The government continues to maintain the infrastructure for protection and remedy of the rights and profits in the cyber space, while particular care is taken on the fundamental human rights.

Chapter 3. Important Policies for the Next Three Years[54]

Section 1. Promotion of measures in the four measures and steady implementation of the objectives of the policy.

(1) Four areas of measures

[1] Government agencies and local governments

［Government agencies］

The government agencies maintain the integral standard of the government organizations determined in the period of the First National Strategy and the framework of assessment/recommendation based on the standard, and specifically takes actions for the following measures.

(a) Establishment of the system for the information security measures for all government agencies to actively involve in

1) Enhancement of the management in each process of PDCA cycle

Each government agency have a system to supervise the information security of the organizations under the chief information security personnel, to establish the information security governance, at the information system project management section (PMO) or other section having the equivalent authorities. Moreover, the chief information security adviser who has a special knowledge and assist the chief information security personnel should be assigned, as well as there should be staff members to reflect the orders and advices of these experts under the organization above in a prompt and secure manner.

Government agencies develop “Annual Report for Information Security” (Information Security Report) for describing the information security policies, objective indicators such as numerical data such as the objectives, plan, achievement and assessment of the information security to show whether PDCA cycle is effectively functioned in each government agency, while identifying the current status of their information system. This is provided to confirm the credibility of the government agencies with people, from the

[54] The schemes for entities to entrust information will be included in the section closely related in the existing policy structure (four implementation fields, cross-field 4 types) for convenience.

viewpoint to clarifying the liability concerning the information security measures.

The chief information security advisor participates in preparing the report and actively promotes the use of the external audit system for government agencies that are applicable. The information security report prepared should be submitted and disclosed in the occasions such as “Information Security Measures Promotion Council” provided under the Information Security Policy Council.

A guideline for the information security reports of the government agencies should be established to have a well balanced information security measure of each government agency, from the viewpoint to promote fulfillment and improvement of the policy. The quantitative assessment should also be made for the information security report developed by each government agency for reporting the result to the Information Security Policy Council. Moreover, a council for the chief information security advisers of each government agency to meet should be formed for comparison and assessment of the information security report, as well as for active exchanges of knowledge and feedback obtained through the opportunities.

The government integral standard should be reviewed annually to make the information security measures updated and suitable for the current status, based on the changes of technologies and environment.

In terms of the information security measures concerning the system for the government agencies to handle confidential information (special confidentiality), the measures based on the standard concerning the special confidentiality based on the “Basic Policy concerning the enhancement of the counter intelligence functions” [55], while following the PDCA cycle based on the government integral standard. The government agencies should take measures at their responsibility above, and the status of implementation checking mechanism must be developed by the Cabinet Secretariat and related government agencies in cooperation, as Counter Intelligence Center is taking a lead.

2) The human resource development and maintenance of the government agencies and motivation building of the personnel

The information security related tasks by the government agencies are studied and reviewed to summarize the skill required for personnel who would involve in these tasks.

[55] Determined by Counter Intelligence Promotion Council on August 9, 2007.

For each government agency, a specific plan concerning the training, assignment and appointment of the in-house human resources concerning the information security measure, based on the skills summarized, should be specified in “IT personnel human resource development and assignment implementation plan” prepared based on “the guidelines of IT human resources and assignment at administrative bodies[56]” to promote.

Moreover, in order to promote the use of private specialists concerning the security countermeasures, a strategic outsourcing to use the chief information security advisors and the support staffs should be proceeded, as well as the positive use of staffs including the employment system with limited assignment.

In each government agency, the improvement strategy of higher motivation of the information security of all employees including the management, should be proceeded with a close cooperation between the human resource division and the information system division, including promotion of the human resource development using the public and private sectors personnel exchange system, as well as the descriptions concerning the information security for the training for various level of jobs.

3) Budget related to conduct the information security measures in a timely manner

Although each government agency should make assumptions as much as possible to take the information security measures in a prompt manner and take actions such as making a contract for maintenance agreements to enable a timely and appropriate responses, it is necessary to take care for effective use of the budget with close cooperation between the finance division and the information system division, as well as the use of “result-oriented projects” [57] to be considered to use.

4) Enhancement of the information security measures committed for operation and management

In each government agency, it is required to guarantee the compliance of the information security policies of the government agencies to commit, as well as whether it is appropriately operated, according to an appropriate agreement based on the government integral standards concerning the information system committed to the

[56] Determined by the chief information officer (CIO) conference for each government agency on April 13, 2007,

[57] In order to effectively use the limited financial resources, a quantitative goal is made for post-operation assessment. The budget execution should aim a success of projects by taking flexible measures depending on the characteristics of the projects.

external organizations of the government agencies for operation and management.

5) Formulation of the mechanism to accumulate and use the technical findings

In order to promote the information security measures, a mechanism should be created to collectively use the findings of the researchers and practioners such as the related independent administrative agencies and information security related groups in order to use the technical and special knowledge and experiences concerning the information security in Japan.

6) Consistency with the laws and regulations concerning the information security

A necessary adjustment should be made to achieve the consistency of the laws and regulations assumed to have a close relationship with the information security and the government agency integral standards, including the document control laws which are under study.

(b) Establishment of the system which the information security measures are properly integrated into the information system for the entire government.

When various information systems are established for the government agencies, a mechanism to promote the security to encourage the integration of the information security measures from the planning and design phase (Security by Design) and the optimum measures for the tasks and systems should be designed, not only for the establishment and operation phases of the information systems. In this case, a method to promote mitigation of TCO (Total Cost of Ownership: the total expenses for maintenance and management and introduction of the system etc.) for the entire government should be studied.

Various information which would be a reference for designing the information security measures required for procurement of the information system and goods should be presented to use it.

(c) Improvement of convenience and security level of e-government

From the viewpoint of the improvement of the security level, as well as to improve the convenience of the administrative services and promote the efficiency and advancement of the administrative operations, the system security functions concerning e-government should be discussed. For those which are related to the interface with the users, it is required to study the method to actually use it, upon consideration of the cost effectiveness, in order to improve the convenience of the users and secure the safety.

(d) Studies concerning the enhancement of the sustainability and emergency response capabilities of the government agencies

While the business sustainability plan was established by government agencies for the potential risk of earthquake in the metropolitan area according to “Metropolitan Area Earthquake Guidelines” (September 2005) specified by the Central Disaster Prevention Council, the government agencies should determine the necessity and priority of the disaster and defect measures of the information system owned by them, as well as specify the task sustainability plan as necessary. Moreover, a cross-field direction of the information backup system should be considered as well as the critical system owned by the government agencies.

From the viewpoint of enhancement of the response recovery in emergency, the government should improve the emergency response against cyber attacks etc., to strengthen the national security, through the analysis of communication system and the response planning functions in case of emergency, to deepen the cooperation with the government agencies and international organizations related at home and abroad, based on the GSOC[58] which started the full scale operation in FY2008.

(e) Promotion of the information security measures of independent administrative agencies etc.

Government agencies who supervise the independent administrative agencies specify the items concerning the information security measures in the mid-term target and establish a system to take on the information security measures as an organization, in order to promote the information security measures of the independent administrative agencies. Each independent administrative agency establish PDCA cycle concerning their own information security measures based on a series of countermeasures taken by the government agencies, including the government integral standards, depending on the task characteristics and implementation status of the countermeasures. The independent administrative agencies and government agencies who supervise the independent administrative agencies should establish an effective communication network, for both normal state and emergency.

[58] Abbreviation of Government Security Operation Coordination team

(f) Promotion of other various information security measures

1) IPv6 for the government information system

The government agencies should make a plan and start to apply IPv6 at the occasions of the new development (introduction) or update of various information systems as planned, from the viewpoint of the need to implement leading measures against the running out of IPv4 addresses. Particularly, the information system for direct communication with the outside organizations, such as the e-government system, should have IPv6 by 2010 in principle. In this case, it is necessary to cope with the information security issues in the transition phases from IPv4 to IPv6.

2) Prevention of falsification of government agencies

In order to easily identify the legitimate government organizations or officials of government agencies, to prevent any harmful actions to general people or private companies by a malice third party who disguise as a government agency or official of a government agency, the measures should be promoted concerning the isoelectronic certificate such as electric signature attached to emails from government agencies, or the guaranteed domains to identify government agencies for emails and web servers.

3) Promotion of secure encryption for government agencies

To ensure the safety and reliability of the e-government, the safety of recommended codes used by the government agencies should be constantly observed and studied. Various tasks should also be proceeded by organizations concerned for revision of the current “e-government recommended encryption code list” in FY2013, based on a technological trend and international approaches. Moreover, the experiences when "the guidelines for transition from the encryption algorithm SHA-1 and RSA1024 used in the information system of the government agencies"[59] should be properly succeeded to update the non-secure encrypted codes to a secure one in a prompt manner.

［Local governments］

(a) Promotion of rational and independent information security measures including small-scale local governments

[59] Determined by Information Security Policy Council on April 22, 2008.

The measures should be promoted aiming the implementation of a desired information security for all local governments, including small-scale organizations. The measures includes, in specific, promotion of the risk analysis of the information assets which is the basis for making measures and auditing, studies on the development for information security policies, review of the guidelines before auditing and proliferation of the guideline[60] which is effective to develop the business continuity plan. In terms of human resources, a joint workshop or local seminars should be held for education of officials who are in charge of the measures.

(b) Assistance for local governments to cooperate in taking information security measures

Considering the limitation of resources available for investment to the information security measures of local governments, the programs to achieve the partnership between local governments should be supported for effective implementation of the measures. The support includes the introduction of the best practices and creation of model cases for local governments nationwide. Workshops or study groups should also be held to promote the understanding of the chiefs of local governments to improve the awareness of the management of the organizations, for instance, a study on dispatching advisors for mutual auditing.

(c) Strengthening entities who assists measures taken by local government

It is effective to strengthen the entities who assist the measures to be taken by local governments in order to promote the measures. Therefore, while developing the cooperative systems of all entities who possess knowledge and findings concerning the information security such as holding a joint workshop of public/private sectors and NPO, the support system for local offices should also be enhanced by using the portal website in LGWAN (Local Government Wide Area Network).

(d) Promotion of measures in a wide administrative area for local governments to handle

The information security measures in a wide range of administrative areas of local governments to handle should be promoted by considering the individual relationship between the national administrative bodies and the organizations of local governments in

[60] "Guidelines for ICT Business Continuity Plan of Local Governments", Ministry of Public Management, Home Affairs, Posts and Telecommunications (August 2008)

charge of the information security. For instance, it should be possible to fully consider the aspects of information security when applying an IT infrastructure in educational institutions, providing information of effective measures for information security to local educational boards and promoting the awareness of local educational boards for information security by introducing them the best practice cases.

(e) Promotion of mutual use of the best practices between local governments, or between local governments and government agencies

It is effective to use the best practices between the local governments to use each other to promote the information security measures of about 1800 local governments. Therefore, the information sharing between the local governments should be promoted by using the portal site installed in LGWAN (Local Government Wide Area Network). Moreover, to share the best practice in length of the local government and various hierarchies such as the chiefs of the local organizations and onsite officials, workshops and study groups should be held.

In addition, as mutual use of the best practices with government agencies, or public organizations, is also expected in the same manner as mutual governments, the measures toward the movement will be studied.

(f) Promotion and support of personnel for the information security measures of local governments

For human resource development for information security measures in regions, it is effective to promote the activities by the local governments. Therefore, the government should make an environment to facilitate such activities for local governments. For instance, reference documents which can be used in training programs should be developed concerning the information security and introduced to local governments to use in educational programs for residents to learn the information security. Moreover, based on the concept of Teaching Teachers (education and promotion of personnel to be instructors), there should be measures to promote such human resource development in the regions.

[2] Critical infrastructure

Entitiess concerning the information security measures of the critical infrastructure are expected to maintain various critical IT infrastructure services respectively under the Second Action Plan and provide a prompt restoration in case of failure of IT. Moreover, the status to implement information security measures should be annually reviewed to assess the action plans and continue to improve the measures. Specific actions related to this are specified in the Second Action Plan, while the following is the outline.

(a) Maintenance and penetration of "Safety Standard etc."

The guidelines specified under the First National Strategy should be reviewed in detail in terms of supplemental descriptions, status of the guidelines and detail levels of the descriptions from the viewpoint of the business continuity. Not only the measures contributing to the bottom-up for promotion of the safety standards based on the consistency with PDCA cycles of the critical infrastructure providers, advanced measures should be reviewed every three years to take measures to penetrate the policy.

(b) Enhancement of information sharing system

Information shared between related entities including CEPTOAR and CEPTOAR Council formed under the First Action Plan should be organized to promote the environment required for information provision and communication, as well as to promote the fulfillment of the voluntary activities of each CEPTOAR and CEPTOAR Council.

(c) Common threat analysis

The interdependence analysis should be continuously conducted to study how the influence spreads to other critical infrastructure when any IT troubles occur with a certain critical infrastructure that has been implemented under the First Action Plan. It is also necessary to identify what the potential threats would be common for the critical infrastructure areas.

(d) Cross-field trainings

Based on the knowledge and findings of the cross-field training method, which was obtained in the First Action Plan, cross-field trainings should be conducted assuming failures of IT, in cooperation of government agencies who supervise critical infrastructure, each critical infrastructure providers and CEPTOARs in each critical infrastructure area.

(e) Adaptation to environmental changes

In order to adapt the information security measures to changes of social and technological environments, it is necessary to improve the capability to detect any change of the environment, which could not be assumed when the Second Action Plan was established. If the framework of the Second Action Plan alone is not sufficient to cope with the changes of the environment, the Cabinet Secretariat should pursue a system available to take necessary measures.

[3] Enterprises

(a) Information security governance as “part of corporate management”

In order to make the information security governance as corporate management, measures should be taken to achieve it, as well as to promote the activities for corporate management and to develop a rational information security governance process model. While enhancing the system to improve the awareness of corporate management, the tools including the information security management system (ISMS) compliance assessment, information security auditing, IT security assessment and certification, encrypt module test and certification systems, information security reporting model and information security measures benchmarks should be further proliferated, developed and improved aiming to make various measures common among people. In addition, the evaluation of the information security measures level, using these systems and results of the third party assessment, should be one of the requirements for tendering as required, for the bidders of the government procurement of the information systems etc. Moreover, in order not to make the information security governance measures too much burden on enterprises, it is necessary to promote the study on how to actually use a method to measure the investment efficiency. In order to make the information security governance be “part of corporate management factors”, there are issues which should be organized in line with the related laws and regulations. Therefore, the analysis and summary should be made for the related laws and regulations to promote a method to be used as a guideline.

(b) Promotion goods and services for improvement of the information security of enterprises and its activities

An environment for enterprises to easily choose necessary information security measures should be provided to promote the information security measures for enterprises. Following the First National Strategy, IT security evaluation and certification should be promoted as well as the research aiming the practical use of the quantitative evaluation technique concerning the information security related risks.

It is also necessary to enhance the approaches of the entities who support the measures, in order to promote the provision of goods and services contributing to the improvement of information security and its activities. It includes promotion to use SaaS and ASP to facilitate the measures, enhancement of measures against spam emails, encryption and authentication technologies, and promotion of the security assessment system for the transition of NGN/IPv6. It is also important to have a viewpoint to promote goods and services taking care of TCO for such actions.

(c) Human resource development and maintenance of information security of enterprises

Public relations and promotion for the human resource development seminars are conducted since it is inevitable to foster and maintain the personnel who are responsible for the information security measures of enterprises, since corporate management began to understand the importance of the information security measures. In terms of the measures, it is essential to foster and maintain personnel flexible to changes of the environment, such as IT services, the human resources who are capable of making decisions based on a broad view on the entire management of enterprises. In this case, it is important to consider the career path for the information security personnel to aim. Accordingly, the common career skill framework for consistency of various skill standards as an objective personnel assessment mechanism, and the Information Technology Engineer Test, and the frameworks related to human resource development and various certification of private sectors will be promoted according to an appropriate role classification of public and private sectors. Curriculums for advanced information security personnel development, teacher training through the industry, academia cooperation and systems to fulfill the internship programs will also be provided.

Through the development of the model career development plan concerning the information security for engineers and support for the experts community, it is necessary to foster and maintain the personnel who are capable of handling the information security of the enterprises in a wide range.

In addition, the human resource development for personnel capable of practically implement the information security measures, while identifying the risks related to law compliances, information assets and business continuity, as well as practioners who are able to cope with the transition to new environments such as NGN/IPv6, which will be a future issue to consider.

(d) Business continuity for enhancement of response ability to "accident assumed society" and emergency response systems

In order to conduct appropriate and effective measures against information security issues such as computer virus or vulnerability, it is necessary to establish the communication system for information sharing for both normal state and emergency, and means to strengthen the relationship among the entities. In order to securely confirm the business continuity, promotion of the business continuity plan by enterprises should be promoted, as well as the proliferation of the business continuity plan guidelines and improvement measures. In addition, necessary emergency response systems should also be promoted to take prompt and effective measures in case of information security related issues.

(e) Promotion of information security measures of small and medium-sized enterprises

In order to promote information security measures of small and medium-sized enterprises, which might be easily lagged behind due to lack of resources such as personnel, budget and IT infrastructure, there should be an environment for the enterprises to easily choose appropriate measures among various options. For instance, the information security benchmark used to measure an appropriate information security level should be kept improved. There should also be a standardized checklist to be developed and proliferated among them to show their information security level as an objective assessment.

It is also necessary to take effective approaches to promote the security measures of small and medium-sized enterprises, such as providing easy and low cost security tools. Therefore, measures should be taken for provision and promotion of SaaS and ASP, and presentation and promotion of information security measures standard by these service providers.

In addition, it is also necessary to promote information security measures through various promotion and development activities such as holding seminars, in order to deepen the understanding on the information security for corporate management of small and medium-sized enterprises and information security personnel.

(f) Promotion of information security policies to support global business development of Japanese Companies

For Japanese companies to seek a global business development, it is necessary to promote the measures for information security in various business bases overseas. For instance, international partnership and cooperation to formulate a secure network information network should be promoted, as well as making an environment for smooth outsourcing, in the countries and regions closely related to the business of Japanese companies, such as Asia.

[4] Individuals

(a) Enhancement and promotion of information security education

Education and enlightenment for children, students and parents should be promoted, as their perception on risks and recognition of importance of the information security measures are insufficient, although they are keen to use IT. Under the circumstances, education of the information morality[61] should be promoted in educational institutions and communities.

An environment should be provided for individuals or customers to recognize risks which could be incurred through the use of various IT services and prevent them from being suffered from damages due to the risks. Security measures to individuals, provision of risk and countermeasures information by the service providers and entities supporting the measures should be promoted, as well as emergency responses to accidents.

(b) Effective proliferation and promotion activities to bottom-up the individuals

Promotion and public relation activities should be proceeded by government agencies concerned in cooperation to enhance the recognition of the importance of information security for individuals. In order to achieve higher awareness of the security of general users including individuals who has lack of computer literacy, there should be a scheme to educate the supporters to give them appropriate feedbacks to any questions and door-to-door operations, as well as for creation of regional network of groups.

(c) Measures for improvement of the information security including individuals with difficulties taking IT security measures

It is inevitable to improve the information security level for users including individuals who has lack of IT literacy including those who take no measures even though they realize the need of measures, with assistance of an entity to support the information security measures. Therefore, it is necessary to enhance the anti-spam email measures

[61] Information morality is “thoughts and attitude as a base of an appropriate activity in the international society” (High School Education Guidelines, Information)

and information security measures to be conducted as a preventative measure by telecommunications carriers.

(2) Enhancement and development of cross-field information security infrastructure

[1] Promotion of information security technological strategy

In order to achieve the goal for 2012, it is necessary to promote voluntary research and development by the private organizations and the universities. The collaboration of industry, academia and government is also important while they play their own roles. The government should also focus on items which could be hard to implement by private sectors and universities, while it is quite important, such as the areas of high risk, high public natures, fundamentals, or creation of an environment to support research and development common in diversified areas.

(a) Emphasizing and diversity of information security technology development

Research and development/technical development should be promoted aiming to achieve the environment for users to use IT with a sense of security, as well as for enhancement of IT as an infrastructure. As the economic conditions become severe, it is further required to promote research and development, and technology development from the aspects to pursue higher productivity using IT, and to secure a leading or advantageous status in the field. In specific, various measures should be promoted to achieve a safe and secure equipment and user environment that the information security measures are fully taken in advance, without any burden to users.

Meanwhile, the government should actively involve in the areas that strategically maintained as a country, such as areas that enterprises has no access due to no possibility of market, an advanced development to tackle potential risks, areas which would require a tremendous amount of development costs and fundamental researches, in order to make sure the diversity of research and development, and technology development.

(b) Promotion of "grand challenge type" research and development and technology development

In terms of the information security measures, there are measures not fully taken yet even though its urgency, or ones that need to be realized in mid and long perspectives for a drastic technological innovation. In order to deal with such difficult issues, "grand challenge type" research and development and technology development should be promoted.

Prompt measures should be taken by integration and installation of key technologies to solve the urgent issues. There are some cases that measures have been taken but even successful results of new technologies are not used since the institutions and education are not sufficiently provided. Thus, it is effective to promote a comprehensive measure in line with the advancement of organization and human, and enlightenments to the users.

For promotion of a mid and long term research and development and the technology development, an image of ideal society in the future should be predicted to study information security technologies which should be necessary. The results of the study should be used for exploring the themes of research and development then should be developed based on the study of the information security technology. In specific, as it is difficult to establish a method to design the information security to a product from the design phase or to accumulate the development know-how in a short term and many findings and knowledge would be required, it is desirable to have a mid and long-term vision, its implementation system, and the support environment

(c) Efficient implementation system of research and development and technology development and maintenance of base

In the project supported by the country, the procedure for using the result achieved on the way of the project at the planning phase of the research and development and the technology development (process) should be incorporated into maximize the effect of the investment, and the contents of the project should be publicized further. While a trend of drastic change of the environment around information security, it is necessary to assess the impacts from any changes of social conditions and technical innovation, introduce a mechanism to enable a flexible project management which may be adapted to change of schedules if necessary, and take an immediate response to new threats.

In addition to direct challenges of research and development and technological development, the environment of the research and development support should be positively promoted by cooperation of public and private companies, concerning the particularity of the information security field. It includes commonality of the description pattern of risks and its evaluation method, design and sharing the information security related database, and creation of the separate work bench[62] to support and accelerate the research and development.

[2] Human resource development and maintenance of information security

[62] An experimental system simulating the network to study malware by actually using it. This environment is separated from actual Internet so that the malware is physically disabled.

personnel

(a) Human resource development, maintenance of personnel for government agenc, and motivation improvement (supplement)

The information security required for the government agencies will be studied and reviewed to summarize the skills required for personnel concerned with the tasks.

Based on the skills presented, each government agency should specify and promote plans of “IT human resource development and maintenance action plan” prepared according to “human resource development and maintenance guidelines of IT personnel in administrative bodies” for specific plans concerning the training and assignment of personnel in-house in terms of the information security measures.

Government agencies promote strategic outsourcing to use chief information security advisors and its support staffs to use specialists from private sectors concerning information security measures, and actively use the contract-based employment system.

In each government agency, the personnel division and information system division should promote the policy to motivate all the personnel, including management officials, for the information security in cooperation, through the trainings for each level of personnel to study information security related matters, other than the promotion of human resource development using the public and private sector personnel exchange system, with a close cooperation between the human resources division and information system division.

(b) Human resource development and maintenance of information security personnel in enterprises (supplement)

Public relations and education for human resource development should be promoted such as seminars, as it is inevitable to develop and maintain personnel who are capable of the promotion of information security measures of enterprises. The corporate management should also increase their understanding on the information security measures. In terms of the measures, it is also inevitable to develop and maintain personnel who have skills to make decisions with a broad view of the entire management of enterprises, or those who are flexible to adapt to changes of the environment such as application of new IT solutions. In this case, it is also important to take into consideration of the career path for the information security personnel to aim. Accordingly, under the appropriate categorization of roles of public and private sectors, the government should promote the common career skill framework that attempts consistency of various skill standards, as an objective human resource assessment mechanism, and the use of information processing engineers test in compliance with the mechanism, as well as the framework concerning human resource development provided by private enterprises and various certification tests. Curriculums to educate advanced information security personnel through industry-academia activities should be developed. A system to improve the system of internship should also be provided.

Moreover, through the development of the model career path concerning the information security for engineers and the support to specialists' community, it is necessary to develop and maintain the personnel who are capable of handling the information security matters of enterprises in a broad view.

It is also necessary to promote the human resource development for practitioners who can cope with a new environment through transition of NGN/IPv6, which would be the future issue, or those who are capable of taking practical information security measures, while identifying the risks concerning compliance to the laws, information assets and business continuity.

(c) Visualization of skills of information security

In order to establish the information security scheme backed by capable personnel, though the recruitment of personnel in the information security area, it will be effective to motivate the information security personnel to recognize that their higher capability would make the success in their jobs from a long term perspective, as well as to allow them to design their own career path.

Therefore, the government should implement the policies to visualize the skills of personnel, clarifying the skill requirements in a real world. For example, the scheme includes visualization of the relationship between the information security certification system/education and skill requirements in daily tasks, and the career path which the information personnel would aim. It may also include visualization of skill requirements to outside organizations through the common career skill frameworks：ITSS[63] and the use of various effective frameworks used by private sectors for human resource development.

[3] Promotion of for international partnership and cooperation

In order to achieve a certain result in 2012, though the actions under The Second

[63] Abbreviation of IT Skill Standards（Information Technology Skill Standards）

National Strategy of Information Security, various policies should be promoted in consideration of the characteristics of regions as well as the policies, operation and standards, from the six aspects below.

(a) Enhancement of POC function concerning information security policies and promotion of information sharing

Following the First National Strategy, NISC continues efforts to clarify the roles as POC that handles the information security policies in a cross-field manner at various international organizations and forums, and enhance the functions.

The schemes are approached from the three aspects. Firstly, collection and coverage of the latest trends at the occasions of international conferences related to the information security to discuss the issues from various aspects such as the national security, the critical information infrastructure protection, continuity of global economic activities, and cyber crime prevention. In order to achieve it, the function to cover and collect the information of international conferences from a cross-opportunity manner, as which requires accumulation of trusts and visualized contribution. Secondly, the trend information obtained and collected through a high reliability will be meaningful once it is shared by organizations and parties concerned in Japan as necessary. Based on the fact above, NISC attempts to share information based on an appropriate rule to government organizations in Japan as POC, and aims to make a meaningful contribution to policy making and implementation of the government related organizations. Thirdly, it aims to make a global contribution by making official announcements of matters required or appropriate through POC, from the viewpoint to create a safe and secure IT environment in the world.

(b) Cooperation of public and private sectors, and effective and efficient international cooperative activities to review the global trend of threats

For a safe and secure cyber space, not only the government but also entities such as national CSIRTs[64], ISPs[65], CSIRTs of various enterprises or research institutions have been promoting a close international relationship. The government focuses on the fields that they have the strong point under the situation. The government will also create a pubic and private sector cooperative activities to effectively and efficiently proceed the information security related international activities, such as the information collection of

[64] Abbreviation of Computer Security Incident Response Team

[65] Abbreviation of Internet Service Provider

the global trend of threats and responses to various incidents as a nation, so as to establish a supplemental and mutual support relationship with organizations concerned in Japan for the international cooperative activities.

In specific, there are three aspects to consider. Firstly, the public and private cooperative system of Japanese government should be actively announced to foreign countries to clarify the roles of public and private sectors in terms of international cooperation. Secondly, through the coordination between public and private sectors, the collaboration scheme in Japan should be enhanced to identify the information which is allowed to be announced to the world. Thirdly, the international information sharing scheme should be organized to improve the reliable relationship with the government and non-governmental organizations in the world to accelerate the speed of information sharing.

Fields that Japanese government can take advantages in particular are opinion exchanges concerning the latest policy trends, which have been conducted with various foreign governments conventionally. For instance, it includes information sharing of the risks such as threats on government agencies and critical infrastructure and vulnerability, and international cooperative scheme against incidents in terms of the government and critical infrastructure. Such scheme should be proceeded by making use of the existing international activities by the organizations concerned.

(c) Collection of wisdom in Asia and improvement of information security standards (achievement of One-Asia)

The threats such as unauthorized access, phishing, junk emails, targeted type attacks and infection of malware through websites could occur beyond the national borders, which also have a common characteristics for some extent in regions where close relationship in terms of geography, culture, and politics. Therefore, as it is obvious in some regions such as Europe and the United States, there has been inter-regional cooperation. Accordingly, the following schemes should be achieved in order to promote the cooperation between countries against threats in Asia and to enhance the information security measures.

Actions will be taken from the three viewpoints. First is to recognize the necessity of the link of people so that the experts and researchers would be actively fostered to conduct the research and analysis of the treat trends in Asia in cooperation with Japan. Second is a support to the schemes to create a function to obtain threat trends information as a joint action in Asia, which has been discussed by international organizations and international forums in a manner to create a significant benefit to Japan. Third is to enhance the relationship with the United States and European countries which have been constructed during the term of the First National Strategy, and actively send the feedbacks of information or lessons which was taken through sharing and joint operation of the best practices to Asian regions.

In promoting the schemes, efficiency is the first priority to make cooperative relationship with organizations concerned as well as to use the existing framework at the maximum.

(d) Information security corresponding to globalization of economic activities

The government should create a business environment to achieve a safety and secure global economic activity of Japanese enterprises. This means that the government aims to protect information assets in the business hubs offshore and maintain high business continuity.

For instance, first is to aim creating a system to achieve a high standard information security measure at business hubs of Japanese companies. Second is to create a highly reliable network environment to secure its availability. Third is to aim promoting the schemes for a consistent information security over the entire supply chain for production processes for IT products and services, while not disturbing the globalization, and to secure reliability. Such approaches should contribute to the improvement of international competitiveness of products and services of Japan which receive high reputation for the quality of information security.

The government uses the opportunities for direct discussion with regions where particularly have close relationship and proceed the schemes through an active participation on the activities of international organizations to actively support developing countries and regions.

(e) Achievement of strategic contribution of our country including standardization

An integral standard making and standardization concerning the information security measures have been conducted by various international organizations. Recently, the standardization is promoted not only technical fields as in the past, but also policy making. The discussion is in a wide range. Even though showing the information security alone, it is quite difficult for the government to involve in all the activities among a number of those. On the other hand, Japan has quite a number of related organizations including enterprises, to conduct the scheme through a continuous participation and contribution to it.

International contribution through the international organizations should require a seamless relationship with parties concerned overseas. Therefore, the government aims to obtain information of the trends of standardization or establishment of the guidelines of international organizations, as well as to create a system making a strategic contribution, in cooperation with the organizations concerned in Japan who participates in the standardization schemes.

(f) Accumulation of information security culture

Accumulation of the information security cultures is regarded as one of the objectives of the First National Strategy. This topic started to gain an attention globally through discussion between the international organizations in a close relationship with Japan in terms of the fields of information system and the Internet.

In order to truly accumulate the information security culture, it is necessary for corporate management of the enterprises to be more conscious, as well as that the scheme through the information sharing of the high level of government organizations in the world. The Japanese government aims to use the high-end opportunities such as G8 and APEC in cooperation with other countries.

Such accumulation of the common understanding, the government aims to create an environment to send messages from the high level of the government officials, not only for cooperative operations in case of incidents.

Table 4 shows the overall view of various measures for promotion of international partnership and cooperation.

Table 4. Various measures for promotion of international partnership and cooperation

Field	Regional	Global
Policy	(c) Collection of wisdom and improvement of information security standard in Asia. (achievement of One-Asia) (d) Confirmation of information security corresponding to globalization of economic activities	(d) Confirmation of information security corresponding to globalization of economic activities (f) Fostering the information security culture
Operation	(c) Collection of wisdom and improvement of information security standard in Asia. (achievement of One-Asia)	(b) Establishment of public and private sectors collaboration to know the threats in the world and promotion of international cooperative activities in an efficient and effective manner
Standardization	(e) Achievement of strategic contribution of Japan including standardization	

(Note) Policy (a) is not specified herein as it is the premise of all policy implementation.

[4] Crime control and protection and remedy of the rights and profits

(a) Promotion of infrastructure for crime control

Enhancement of crime control, performance improvement and promotion of international cooperation by legal authorities should be further promoted.

In addition, information sharing is required as it is inevitable to identify the cause and process of crimes. The government should also promote the schemes for public and private sectors cooperation to create a strong IT infrastructure against crimes, through promotion to create a favorable cooperative relationship between the legal authorities and victims in order to arrest the criminals and minimize damages of the victims.

Countermeasures against cyber terrorisms should also be strengthened as above by taking consideration of the characteristics.

(b) Promotion of enlightenment of announcing to public for crime control

It is required to further improve the public relations concerning the damages incurred, methods and specific countermeasures against the crimes in order to prevent people from being impacted by cyber crimes.

(c) Promotion of infrastructure for protection and remedy of rights and profits

While taking a particular care on the fundamental human rights of people, the government should make efforts to provide an infrastructure for protection and remedy of the rights and profits in the cyber space. For instance, this scheme includes promotion of information disclosure concerning the measures to protect and remedy rights and profits of the entity to entrust information by the one who receives the information, and development and proliferation of the technologies to improve the safety and reliability of the cyber space.

Chapter 4. Promotional scheme of policies and sustainable improvement

Section 1. Promotion scheme of policies

Developing "a secure IT environment" while aiming for "a mature and advanced country in information security" would require participation of all entities in the scheme as well as the common understanding. of all entities in the scheme The government attempts to establish strong "individuals" and "society" in IT age, as shown in Chapter 2, and is required to allocate resources appropriately as a whole nation to promote integrated and cross-sectoral information security measures of the public and private sector, mainly with the key policies of Chapter 3.

(1) Enhancement and role of the Cabinet Secretariat Information Security Center (NISC)

NISC continues to strengthen its role to be a core to effectively function the promotional scheme of the entire government, as a system to collect the best intelligence both at home and abroad, in the same manner as the actions under the First National Strategy. It is also required to strengthen the measures for them to play a role as the international POC concerning the cross-field information security issues.

In addition, NISC should use the personnel in the government in a flexible manner at the maximum as well as making efforts to use the personnel from private sectors as all the findings and intelligence are accumulated in the private enterprises concerning international security. They also aim to maintain and improve their performances. At the same time, NISC is also required to continue efforts for the government officials' human resource development as the key organization.

As shown in this National Strategy, policy making of information security is in a wide range. Therefore, NISC should be a joint with various organizations that are in charge of the related area, as well as promoting the optimization of the cooperative relationship with parties concerned for solutions per issue, and actively participate in the activities to realize the maximization of the problem solving capability of Japan against information security issues as a country.

(2) Enhancement and roles of local authorities

Government agencies should continue to fulfill and enhance the system concerning the information security policy of related fields of the local governments under the framework to promote the information security policy by Information Security Policy Council and NISC. For fulfillment and enhancement of the system, effective policies should be used in a flexible manner at the maximum, including active assignments of human resources of private companies as required. While taking a particular care to avoid vertical system of assignments in the organizations, it is necessary to make efforts to implement various policies to promote integral and cross-field information security policies by both public and private sectors.

(3) Timely and appropriate monitoring the changes and actions to new issues

The change of the information security field is fast from various aspects including threats and technologies. Therefore, it is important to monitor the changing status in a timely and appropriate manner as well as to take immediate and proper actions against newly emerging issues. Moreover, it is also indispensable to study new policy making schemes which could be a new trend.   It is also necessary to take new measures for the entities to send information.

Thus, various organizations and parties including NISC should act in cooperation. The expert councils, which will be launched as required under the Information Security Policy Council, should also be used to enhance the system to study various issues from a broad view concerning laws, technology and promotion in an active and flexible manner.

Section 2. Relationship with other related organizations

The Second National Strategy defines a mid and long term strategy for the information security issues of Japan as a whole. The information security policy should be related to people’s lifestyles and socioeconomic activities in a wide range so that it is necessary to cooperate with various organizations concerned in the same manner as that of the First National Strategy for implementation.

Among various organizations concerned, the information security policy is considered to be one of the key IT policies in terms with the relationship with IT Strategy Headquarters. It should also be noted that The Second National Strategy practically refers to the information security issues of “New IT revolution strategy”. It is also essential to further cooperate with Ministry of Internal Affairs and Communications Administrative Management Bureau for the schemes related to the administrative information system.

In the relationship with the Central Disaster Prevention Council, it is necessary to have collaboration for the critical infrastructure among the other critical security policies. Moreover, it is necessary to confirm that the research and development and technological development related and general science technologies, among the information security policies, should be promoted in consistency, in terms of the relationship with Council for Science and Technology Policy. In terms of the relationship with Quality of Life Policy Council, it is also required to confirm a full cooperation with them to work on the schemes concerning entities who send information, from the viewpoint of personal information protection etc.

Information Security Policy Council and NISC will promote the information security policies in full cooperation with these councils.

Section 3. Sustainable improvement structure

Information security issues gain many risk factors day by day, and the speed of its change is fast. Therefore it is necessary to assess the effects of the policies and improve as necessary. Therefore, the government uses the structure for a sustainable improvement below, following the actions under the First National Strategy.

(1) Development and its assessment of “Annual Plan”

The government launches the programs for various policies annually as “Annual Plan (Secure Japan 20XX)” to achieve the programs under The Second National Strategy. The implementation status is then assessed in line with the changes of social conditions to disclose the results. Its supplementation survey should also be conducted as required. The result of the survey should also be announced as “Assessment of Information Security Policy of FY20XX”. This scheme is according to the framework specified in the framework document such as Information Security Policy Assessment in detail.

The policies should be also advanced smoothly, as it is inevitable for organizations concerned other than the government to take measures. From this viewpoint, the milestones should be set for some fiscal years for items which the mid and long term planning are required. It should not necessarily be a single year plan.

(2) Execution of approaches for emergency correspondence in the middle of a fiscal year

The government executes the schemes to respond to emergencies such as unexpected accidents, disasters and attacks as well as new risk factors, even though they are in the middle of “Annual Plan” implemented.

(3) Improvement of assessment index

The assessment index concerning the information security for each countermeasure is defined under the framework document of information security policies, though the government will continue to make efforts to improve the assessment index according to the method specified in the framework document[66].

(4) Review of The Second National Strategy of Information Security

The government shall review The Second National Strategy in three years, or as necessary for changes of the environment even in the middle of the term.

[66] The scope of the critical infrastructure has been improved for the assessment indicator in the Second Action Plan. Therefore, the assessment indicator in the framework document should be considered based on the assessment indicator of the Second Action Plan.