The First National Strategy on Information Security

- "Toward the realization of a trustworthy society" -

Information Security Policy Council
2 February, 2006

Contents

Introduction

As an advanced information and telecommunication network society has become a reality, and with growing dependence on information technology (hereinafter referred to as "IT") in people's social lives and economic activities in today's Japan, it has become essential to ensure safe and secure use of IT, or, in other words, it is considerably imperative to address information security issues. According to Article 22 (Assuring security, etc, of advanced information and telecommunications networks) of the Basic Law on the Formation of an Advanced Information and Telecommunications Network Society (hereinafter referred to as the "IT Basic Law"), in formulating measures toward the formation of an advanced information and telecommunications network society, it is necessary to assure security and reliability for advanced information and telecommunications networks, protect personal information and implement other measures required so that people may use advanced information and telecommunications networks with a sense of security. Therefore, various efforts have been made since the enactment of the IT Basic Law in 2000.

However, the necessity of a fundamental strengthening of efforts in information security issues has been recognized as various social issues have surfaced recently, along with rapid growth in broadband services for information and telecommunications infrastructure and the diffusion of electronic commerce. Such social issues include the spread of computer viruses on a global scale, increase in cybercrimes[1], information system failures in critical infrastructures essential for people's social lives and economic activities, and leakages of a large volume of personal information, etc.

In such movements, the National Information Security Center (NISC) was set up within the Cabinet Secretariat in April 2005 and Information Security Policy Council within the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (hereinafter referred to as "IT Strategic Headquarters") in May 2005. The NISC and the Council have launched new activities acting as core organizations to enhance information security measures throughout Japan. It can be said that the time has come to formulate a systematic plan on information security based on a strategic vision regarding this issue, which forms a part of the e-Japan Priority Policy Program, as an individual priority issue. Based on these situations, the First National Strategy on Information Security (hereinafter referred to as the "National Strategy") has herein been set out as a mid and long-term strategy with an overview of information security issues.

[1] Cybercrime is the crime using information technology: for example, crimes using advanced information and telecommunications networks, such as the Internet and crimes targeting computers or electromagnetic records.

The National Strategy has been formulated based on the following proposals: the first[2] and second[3] initiatives of the Committee for Essential Issues on Information Security[4] set up within the Expert Panel on Information Security of the IT Strategic Headquarters[5], governmental efforts in response to these recommendations, and reports[6] of the Expert Panel on Culture of Security and the Expert Panel on Technological Strategy (both set up under the Information Security Policy Council).

Chapter 1 of the National Strategy presents the position of information security within the context of national objectives: namely, (1) continuous development of Japan, as a major economic power, and use and utilization of IT, (2) realization of better lives for the people, and use and utilization of IT, and (3) ensuring us national security from a new perspective. Under this stance, Japan's basic principles in addressing information security issues are laid down. In Chapter 2, shared roles of each responsible entity to make concerted efforts in addressing information security issues are presented. In Chapter 3, priority policies to be addressed by the central government in the next three years based on the basic principles and shared roles are explained. Finally in Chapter 4, systems and frameworks necessary for the promotion of policies to realize and maintain these efforts are described.

While information security requires continuous efforts in view of mid and long-term perspectives, the period of the National Strategy covers the next three years (namely, from fiscal 2006 to fiscal 2008), taking the rapidly changing environment surrounding information security into consideration. Meanwhile, an implementation plan is supposed to be formulated annually from fiscal 2006 on the basis of the National Strategy.

---

[2] The First Initiative of the Committee for Essential Issues on Information Security (16 November, 2004)

[3] The Second Initiative of the Committee for Essential Issues on Information Security (22 April, 2005)

[4] The Committee for Essential Issues on Information Security was set up within the Expert Panel on Information Security of the IT Strategic Headquarters on 22 July, 2004, and was abolished when Information Security Policy Council was established on 30 May, 2005.

[5] The Expert Panel on Information Security was established within the IT Strategic Headquarters on 22 January, 2001 and was abolished when Information Security Policy Council was established on 30 May, 2005.

[6] The Report of the Expert Panel on Culture of Security of the Information Security Policy Council and The Report of the Expert Panel on Technological Strategy of the Information Security Policy Council (17 November, 2005)

Chapter 1: Basic Principles

This Chapter details the national objectives of Japan that need to be encompassed in considering information security issues and basic principles in addressing information security issues.

Section 1: Position of Information Security in the Context of the National Objectives of Japan, Current Issues and Solutions

This Section highlights the national objectives of Japan that need to be encompassed in considering information security issues, the position of information security based on the objectives, basic objectives to be attained, current issues, and direction toward solutions.

(1) Position of Information Security in the Context of the National Objectives

A) National objective I－Continuous development of Japan, as a major economic power, and use and utilization of IT－

As of 2005, Japan has the second largest economy in the world in terms of Gross Domestic Product (GDP), and maintains its position as an economic super-power, extending its activities throughout the world. For Japan, a country without the endowment of natural resources, basic economic foundations have been established on the manufacturing industry, supplying high-quality products that appropriately meet the needs of the world market. However, the world economy is currently shifting its axis from *industrial economy,* which pursues material prosperity, to *information economy*, which requires adeptness in using wisdom and know-how.

As a reaction to this movement, the Japanese manufacturing industry has modified the system to secure a leading position in the globalized Industrial Economy by developing production centers all over the world. At the same time, it has been proactively responding to the protection and utilization of intellectual property, such as production patents and brand names. It is needless to say that the use and utilization of IT is indispensable in order to maintain solid international competitiveness and high productivity, responding to the globalization and diversification of corporate activities. A key national objective is to achieve the continuous development of economic activities of Japan while using IT as a social infrastructure much more effectively than any other countries.

B) National objective II－Realization of better lives for the people, and use and utilization of IT－

Besides economic reasons, the use and utilization of IT is becoming essential to

solve social issues that confront Japan in the 21st century. For example, as for the issue of an aging society with a falling birthrate, the working population is expected to decline for the next 15 years[7] and there are growing needs to establish a system to maintain the quality of services and to respond to issues with fewer people through the use of IT. Thus, more efforts have been actually made to solve the issues through the use and utilization of IT. Furthermore, it is desirable to create a safe, secure and reliable IT society adopting the perspectives of the peoples in various areas ranging from underpinning a safe life for the people, such as disaster prevention and relief measures, to healthcare, welfare and education.

As described above, a key national objective is to create a more safe, more secure, and better lives for the people by solving social issues that confront Japan through the use and utilization of IT as a significant means.

C) National objective III－Response to newly emerging threats caused by IT to Japan's national security－

Now that IT is used and utilized in people's social lives and economic activities in Japan, the response to threats such as crimes and terrorism directed toward IT or those using IT is an issue that has to be addressed to ensure the security of Japan.

In a wide range of areas such as food, energy, finance and fiscal affairs, which have not been recognized within the framework of national security, the awareness of threats to continuous development and to safety and security of life for the people has increasingly been raised in Japan. In order to ensure national security, it is necessary to give sufficient consideration to IT-related threats in light of the expansion of use and utilization of IT in these areas.

As described above, a key national objective is to endure Japan's national security by strengthening the system to instill greater cooperation among concerned organizations with an awareness of the emergence of new threats from such expansive use and utilization of IT so as to fully respond to these threats.

D) Position of information security in the context of the national objectives described above

The role of an information security is to make the IT infrastructure truly dependable and solid within the framework of the national objectives of Japan, as a major economic power; specifically, to maintain continuous development, to

[7] Refer to "Issues on Employment and Labor Policies under a Declining Population – Aiming for a Society in which All People Can Live With Peace of Mind" (issued in July 2005, p.47 etc.), Employment Research Corporation, Ministry of Labor, Health and Welfare

achieve better lives for the people through the use and utilization of IT, and to ensure national security from a new perspective.

In other words, we should have a perspective of what it takes to realize the continuous development of Japan, to maintain a high standing society that faces an aging population with fewer children, to improve international competitiveness and to ensure national security. And the way to achieve them is through nothing but to strengthen the efforts on the premise of the use and utilization of IT, as well as the effort to ensure that information security is responsive to the growing issues in information security, represented by the spread of computer viruses and the recent increase in the number of cybercrimes. Here lies the fundamental significance of actively and strategically addressing information security issues. In addition, the approach to the information security issues, which involves solutions to multidimensional tasks, needs to be carried out not only by individual entities, but also in a cooperative manner as a whole nation.

E) Realization of an information security advanced nation based on the ideas of a nation which should be revitalized by the value of trustworthiness

Japan has been developing by launching high quality and high reliability products into the world, being ranked as the safest nation of the world within cooperation between public and private entities and among private companies and local communities. Making use of such strengths and characteristics of Japan is particularly realized in various policies and it seems highly effective to create a nation based on potential capacity to build the “Japan Model”, regarded as a synonym for high quality, high reliability, safety and security, or just simply to create “a nation which should be revitalized by the value of trustworthiness”.

Therefore, efforts of ensuring information security are required to become a truly advanced nation in the matter of information security (realization of a “Trustworthy society”) by implementing measures suitable for the world’s most advanced information and telecommunications network society while making use of Japan’s strengths and characteristics based on the ideas of a “a nation which should be revitalized by the value of trustworthiness”. It is also essential to keep in mind that Japan’s efforts for information security would be applied on a global scale as the “Japan Model”.

(2) Basic Objectives to be Realized－ Creation of a Safe IT Environment Pursued by the IT Basic Law－

A) Creation of an environment for the safe use of IT

It is necessary to take active and strategic approaches toward information security issues under the position described above. In specific terms, it is a requirement to create a safe environment satisfying the following three conditions in IT society.

1) Preventive measures are sufficiently taken against incidents, disasters or attacks (Prevention);

2) Environment with such measures is experienced and fully utilized with sufficient understanding of the structure and technology, etc. by concerned parties (Understanding/Experience); and

3) In addition, response measures against incidents, disasters or attacks have been considered in advance, the containment and remediation of the damage are secured, and continuity of social services is ensured. (Business Continuity)

These are nothing but an embodiment of creating an environment for the safe use of IT stipulated in Article 22 of the IT Basic Law. In other words, the basic objective to be achieved through the efforts of an information security is to create an environment which is not simply safe, but which also satisfies the three conditions described above, so that users can use and utilize IT while actually feeling safety.

B) Striking a balance between convenience and security

Once the three conditions described above are met and users are able to use and utilize IT while actually feeling safety, the coexistence of convenience and security would be attempted. However, current situations show some cases where the information security measures are implemented merely for the purpose of implementing such measures. For instance, users' convenience is hampered by overemphasized information security measures taken to prevent information leakage, such as prohibition of any access to intra-organizational networks from portable computers for business purposes. It is therefore necessary to promote measures and policies to make convenience united to security.

(3) Current Issues and the Direction of Solutions－Establishment of a New Public-Private Partnership Model－

A) Current issues

The IT Basic Law, enacted in 2000, pursued the creation of an environment that

satisfies the three conditions described above; however, it is difficult to say from the users' perspective that this goal has completely been achieved, and it must also be pointed out that the process is not up to pace in an international context. Specifically, the following problems have surfaced in recent years, and the reasons for the emergence of the problems in Japan include 1) majority of measures against problems detected in recent years is designed only to solve immediate problems and 2) each entity of IT society is thoroughly engaged in its own measures confined in the bureaucratic sectionalism.

(**Example 1: Insufficient Prevention)**

There is an unending stream of serious information leakages incidents where a personal computer with file-sharing software is used for business and the computer is infected by a computer virus without being noticed. Such information leakages have been caused because personal computers are used for business without much care and, thorough preventive measures are not taken even though a significant amount of information leakages due to computer viruses has been observed before.

(Example 2: Insufficient Understanding/Experience)

Wireless LAN (Local Area Network) systems are widely spreading from companies to general households as a method of connecting to the Internet, etc. without complicated cable connections for network construction. However, when used, the characteristic of 'radio wave' has been forgotten due to too much emphasis on the convenience of 'wireless access' and understanding about the measures is insufficient, including appropriate encryption and setting up of a radio wave range. Thus, cases of interception or intrusion to the network by third parties have been observed.

(Example 3; Insufficient Measures for Business Continuity)

Cases demonstrating insufficient measures for ensuring business continuity have occurred frequently in the infrastructures supporting people's social lives and economic activities; for example, a case of forced suspension of trading of stock exchange in the international security market due to unexpected failure of the information system, and a case of cancellation of transportation services due to abortion of the flight control system caused by electricity failure in an airport-related facility, etc.

B) Direction of solutions－Establishment of a new public-private partnership model and realization of an information security advanced nation

It is necessary from now on to depart from taking measures only for immediate problems, with an aim to create an environment for the safe use of IT. In addition, it is essential to establish a new public-private partnership model in the area of information security where every entity belonging to IT society shares understanding about the importance of efforts in information security issues and implements measures under appropriate role sharing with due understanding of its own responsibility. It is also necessary to make efforts in solving information security issues based on the perspective of a whole nation. It is vital to continuously aspire to become an information security advanced nation which is constantly in the world spotlight from an international perspective under the new public-private partnership model with selective and strategic management of resources as a nation.

Section 2: Four Basic Policies to Address the Issues of Information Security in Japan

As described in the previous section, in order to attain the basic objective of creating an environment for the safe use of IT, it is necessary to establish a new public-private partnership model and to take approaches toward information security issues based on a national perspective.

The role of each entity to this end is provided in the next chapter. As its premises, four basic policies towards the selective and strategic management of resources are provided below. To be more specific, all of the four basic policies need to be shared and implemented by all concerned entities: namely, (1) the penetration of a common recognition among public and private entities, (2) pursuing advanced technology, (3) strengthening the response capacity of public sector, and (4) promotion of partnership and cooperation.

(1) Penetration of a common recognition among Public and Private Entities

As a major premise for ensuring information security of individual entity, autonomous efforts in line with the behavioral principles of each entity are essential. In order to promote autonomous efforts, the formation of a common recognition is necessary about for what and to what degree of risk each entity will take information security measures.

(2) Pursuing Advanced Technology

As described in the previous section, it is necessary to promote information security measures constantly encompassing elements of the most advanced R&D and

technology development in order to confront the wave of new information security threats, instead of taking measures only for immediate problems.

In doing so, it is important: 1) to be aware of the risk of relying on a single source of technology or single infrastructure and then to make improvements, and 2) to introduce Internet Protocol version 6 (IPv6) and to make further efforts in R&D and technology development from the perspective of establishing a new infrastructure itself having the built-in function of information security, in addition to technical solutions to existing infrastructure problems.

(3) Strengthening the Response Capacity of Public Sector

As described in the previous section, in order to further consolidate Japan's strength as an information security advanced nation to the level of comparative advantage, it is essential to strategically improve the response capacity of public sector. In specific terms, for example, the following elements are necessary:

1) The public sector's initiative in implementing measures by actively following "Best Practice" of public and private organizations in both Japan and abroad;

2) Establishment of social infrastructure with diversity; and

3) Promotion of efforts from an aspect of national security and risk management, such as the strengthening of the national defense, enhancement of countervailing power against crimes and terrorism, and reinforcement of disaster relief measures in view of the emergence of new threats caused by the expansion of use and utilization of IT.

When improving the response capacity of public sector, it is indispensable to constantly consider ensuring human rights, transparency and legality of public activities.

(4) Promotion of Partnership/Cooperation

As described in the previous section, in order to establish a "new public-private partnership model", it is necessary to seek partnership and cooperation of each public and private entity in Japan and to implement measures by bringing together their collective wisdom.

In addition, the issues confronting Japan, the world's broadband leader, are matters the rest of the world will face in the future. In view of the responsibility for finding solutions as a top, efforts for international cooperation and contribution are also indispensable. In doing so, it is necessary to present the "Japan Model" of information security by formulating the outcome of Japan in such a way as to be applicable to other countries through, for example, the introduction of a system in which entities implementing information security measures are evaluated.

It is also necessary to take internationally responsible actions, while being constantly aware of the fact that IT infrastructure is always connected to the world, 24 hours a day, 365 days a year.

Chapter 2: Role of Each Entity for Establishing a New Public-Private Partnership Model

As described in the previous chapter, in efforts for information security, it is essential for each entity belonging to IT society to participate in the creation of an environment for the safe use of IT and to create a new public-private partnership model while being aware of their own responsibility and playing separate roles suitable for their own context. In order to promote a framework in which all entities can participate, it is important that each entity is specifically aware of how much influence its own commitment will have on the creation of an environment for the safe use of IT and what activities are expected to be carried out.

There are entities that actually adopt and implement measures as a component of IT society (the first group). The National Strategy stipulates that it is effective to divide the implementing entities into four areas: namely A) central government/local governments, B) critical infrastructures[8], C) businesses, and D) individuals. We should then consider suitable measures to be taken by each entity.

Besides the above, there are entities that indirectly support the methods of environmental development and promote understanding and solutions to the issues (the second group), when the entities in the four areas actually adopt and implement the measures. The National Strategy stipulates that the following four entities are to play a key role in promoting understanding of and solving the issues: A) central government and local governments as entities formulating and implementing policy measures, B) elementary and secondary educational institutions, higher educational institutions, and research & development and technology development institutions (hereinafter referred to as “educational institutions/research institutions”) C) business entities and non profit organizations that build and provide IT infrastructures, including the development of information systems and provision of telecommunication services (hereinafter referred to as “information-related businesses” and “information-related NPOs”), and D) the Media[9].

This Chapter explains the modality of roles and partnerships expected of each entity in the four areas that actually adopt and implement measures (the first group) and for each of the four entities that promote understanding and solutions to issues (the second group).

[8] Critical infrastructures are formed by business entities providing highly irreplaceable services and are essential for people’s social lives and economic activities. If its function is suspended, reduced or unavailable, people’s social lives and economic activities will be greatly disrupted, and the same below.

[9] ‘Media’ hereto refers to news organizations, such as newspaper, television, and radio, etc.

Section 1: Role of Measure Implementation Entities

(1) Central Government/Local Governments

The information dealt with by central government and local governments includes various types of information ranging from highly confidential information to personal or corporate information collected under laws and regulations, all of which could inflict extremely serious consequences if leakage, falsification or destruction of information, etc. occurs. As more and more administrative services associated with individuals and companies being provided online due to the advancement of E-Government/E-Local Governments, failures of some information systems must be avoided at all costs.

In other words, ensuring information security of central government and local governments is the primary issue related to various fields ranging from protecting rights and properties of individuals, maintaining people's social lives and economic activities and administrative functions, and ensuring national security of Japan. Therefore, central government agencies are required to implement measures by constructive use of "Best Practice" of public and private organizations in both Japan and abroad and to constantly maintain the world's highest level of information security measures. Local governments are expected to further improve the information security measures in line with the efforts made by central government agencies.

In doing so, central government agencies need to undertake inter-agency efforts in cooperation with each other, such as sharing of outcomes and integration of measures, etc., since all central government agencies conduct the affairs of the nation of Japan and some of the information systems are shared and contain many similar attributes, even though business and information systems of each body may differ. The same can be said about local governments, and inter-local government cooperation is necessary.

Meanwhile, it is also imperative to pay attention to the fact that there are characteristic differences between local governments and central government. The former, which exist in different sizes, provide community-oriented municipal services and handles much personal information, whereas the latter is a large-scale body in charge of the establishment of infrastructures at a national level.

(2) Critical Infrastructures

Critical infrastructures are literally the basis for people's social lives and economic activities and the most important task is to ensure stable services by protecting them from any threats. Particularly, as evidenced by the examples of

recent big earthquakes, as IT has progressed and interdependency has increased, situations have emerged where critical infrastructures of the whole nation are no longer secured by individual measures taken by each business entity engaged in critical infrastructures[10]. Thus, further enhancement of cross-sectoral information security measures to deal with IT-malfunction[11] of critical infrastructures has become an urgent issue.

A communication and partnership system between public and private sectors has been established as a major measure against malfunctions caused by intentional factors such as cyber attacks, etc.; however, many IT-malfunctions experienced in the real world are human errors or caused by various other threats such as disasters, etc., and it is therefore necessary to prepare countermeasures for such threats in the future.

Operations of most of the critical infrastructures are conducted by private business entities in each business sector under the license of the presiding Ministries and Agencies of the relevant critical infrastructure. Information security measures have also been undertaken mainly by presiding Ministries and Agencies for each area. Thus, when looking over the entire critical infrastructure, approach, background and level of measures for information security, each exhibits quite different characteristics, complicated by diversity of the business environment and structure in each sector. In light of increasing interdependence among critical infrastructures, it is necessary to reconstruct a new public-private partnership system encompassing cross-sectoral efforts in addition to bureaucratic sectoral efforts, in both aspects of improving information security of critical infrastructure and simultaneously enhancing capacity to respond to IT-malfunctions (e.g. preemptive prevention, prevention of expansion of suffering and rapid resumption, and prevention of recurrence), while giving due consideration to the characteristics of each business sector and business entity engaged in critical infrastructures.

(3) Businesses

Businesses are the key players in economic development under globalization, and at the same time, they are the main bodies to provide products and services that support the IT infrastructure. Therefore, it is necessary to implement information security measures from these aspects. The measures are to be implemented on the

[10] "Business entities engaged in critical infrastructures" are defined in "1. Objectives and Scope" of Action Plan on Information Security Measures of Critical Infrastructures" (decision made on 13 December, 2005 by the Information Security Policy Council), and the same below.

[11] "IT-malfunction" is any malfunction (suspended services, reduced function, etc.) occurred in the operation of critical infrastructure caused by dysfunction of IT, and the same below.

premise of initiatives based on the business judgment of each company. However, in a highly networked IT society, there is the possibility that problems caused by an incident in one company can spread to the entire society. And, accumulation degree of information of a large number of individuals has been increasing. Thus, businesses are expected to undertake measures more actively as members of IT society, as well as to contain their own damage and observe laws, with realization that the companies are responsible for information security measures.

It is also important to create a cycle in which active implementation of measures by businesses indirectly influences the awareness of individuals about information security.

(4) Individuals

Individuals tend to be less aware of the fact that they are actually causing troubles to others by taking no information security measures, unless they themselves fall victim. Each individual is also responsible as a member of IT society regardless of gender or age, and it is necessary to cultivate awareness about information security to the same level as a general safety rule like “you should not talk to strangers”. Individuals are expected to act with clear recognition of basic principle of protecting themselves on their own.

However, each generation of internet users, 80 million in total, has different level of understanding about information security and the IT system is hard to understand for the people. Therefore, it is indispensable to compensate the limitation of self-responsibility; furthermore, support from other entities in this area is more crucial than any other implementation area of measures.

Section 2: Roles of Entities to Promote Understanding and Solutions to Issues

(1) Central Government/Local Governments－As Policy Implementing Entities－

In order to enhance information security infrastructures of the whole of Japan, the central government, being responsible for policy formulation and implementation, is required to formulate and implement policies regarding institutional development, public relations, attention rousing, introduction of new technologies, and development of an educational environment more actively than ever before.

In doing so, even though each governmental agency needs to formulate and implement policies in accordance with its own role, it is also vital to formulate the policies that are nationally consistent and can allocate resources selectively and strategically, and to eliminate non-strategic and bureaucratic sectional efforts.

Meanwhile, when formulating and implementing policies regarding information security issues, the government should aim to become a small but efficient government. At the same time, the government should also give consideration to the point that it is not always effective for the government to increase its involvement; instead, the government should make efforts in two different manners: 1) encouraging businesses and other entities to carry out competitive activities and independent efforts, and 2) taking the initiative to implement necessary measures because of insufficient market mechanisms, etc.

In order to enhance regional information security infrastructure, local governments are also expected to actively contribute to increasing public relations, attention rousing and forming partnership and cooperation between public and private sector etc.

(2) Educational Institutions/Research Institutions

As described in Section 1-(4) of this Chapter, individuals should improve literacy of information security regardless of gender or age, when enhancing the national information security infrastructure. To that end, it is necessary to promote cross-generational education in information security starting as early as elementary and secondary schools. Therefore, elementary and secondary schools, adult education institutions and teachers education institutions are expected to implement programs to raise awareness of information security up to the same level as general safety rules, more actively than ever before.

Research institutions such as higher education institutions, including universities, and independent administrative institutions are the basis for advanced research development and human resource development associated with information security. More active roles are expected to be played as the R&D and technology development base in line with national strategic policies and more active efforts are expected to be made to develop human resources with multidisciplinary and comprehensive capacity and foster educators of information security.

Furthermore, all educational and research institutions need to actively make efforts in relation to information security of their own, which would set good examples for others, in view of the fact that these institutions offer a place of education and research activities in a given environment and a place for fostering the basic competencies of teachers, etc.

(3) Information-Related Businesses and Information-Related Non Profit Organizations

Information-related businesses are ones that actually provide direct services to

central government and local governments, critical infrastructures, businesses, and individuals for the implementation of measures, and assume a role to help the enhancement of the information security infrastructure of Japan. Therefore, they need to re-acknowledge that they are responsible for eliminating the vulnerability of their products and services as much as possible and make efforts to offer safer and more secure products and services. In doing so, the information-related businesses should have a positive perspective that the provision of safe and secure services would eventually lead to the improvement of their international competitiveness.

Information-related NPOs have been set up to conduct activities on a nationwide or regional basis, which is highly appreciated from the point of view of promotion of appropriate use and utilization of IT, improvement of users' capacity to respond to problems, and strengthening of a partnership in the private sector. Such NPOs are expected to continue active efforts in the future. They are also expected to contribute to educational campaigns on information security, provision of information on warnings, threats, and vulnerability, etc., and contribute to practical human resource development needed in Japan. Also, some of the information-related NPOs have already launched efforts to further international partnership and cooperation, and more positive activities are expected from the perspective of international partnership and cooperation.

(4) Media

Media has the function to directly send information to each entity implementing measures, including businesses and individuals. Media has a significant impact on the formation of a common recognition among individual entities about for what purpose information security measures should be taken and on the understanding and sharing with the peoples about the necessity of solid strengthening of the whole IT society. Therefore, it is necessary to create an environment where the media covers not only incidences and accidents concerning information security, but also a wide range of information pertaining to information security, such as good examples of information security measures and the necessity of the solid strengthening of a whole IT society.

Chapter 3: Priority Policies to Be Addressed in the Next Three Years －Establishing a New Public-Private Partnership Model－

In order to enable every entity belonging to IT society to establish an environment for the safe use of IT under the appropriate division of roles described in the previous Chapter, the central government will make comprehensive efforts in the following priority policies in the next three years to establish a new public-private partnership model.

Also, in accordance with the policy directions presented here, the government will formulate an implementation plan, or 'Annual Plan', for more specific measures to realize the National Strategy.

Section 1: Strengthening Information Security Measures in the Four Implementation Fields

As described in Chapter 2, Section 1, the National Strategy stipulates that it is effective to consider the content of the measures by dividing the management and implementation entities into four fields when implementing reinforced measures overall for information security infrastructure in Japan: A) central government/local governments, B) critical infrastructures, C) businesses, and D) individuals. The central government is required to make comprehensive efforts in promoting measures in each of the four fields of implementation in accordance with the role played by each entity mentioned in Section 1 of the previous Chapter.

(1) Central Government/Local Governments

As described in Chapter 2, Section 1, the central government needs to implement measures by constructive use of "Best Practice" of public and private organizations in both Japan and abroad and constantly maintain the highest level of information security measures. Local governments need to further improve the information security measures in line with the efforts made by central government agencies.

However, when looking at the current situations, central government agencies have grappled with such issues as discrepancies in information security levels being particularly vulnerable to threats from within, insufficient efforts in emergency response and business continuity, and paucity of human resources with highly specialized knowledge to deal with increasingly complex information security issues. Issues of local governments include insufficient measures against IT-malfunctions and information leakage, and underdeveloped information sharing systems among local governments.

Therefore, the central government will make efforts in the next three years, aiming

1) to upgrade the level of the Standards for Measures[12] to the world's highest level by fiscal 2008 and 2) to enable all the government agencies to implement measures at the level meeting the Standards for Measures by the start of the fiscal year 2009. Local governments will make efforts in the next three years, aiming 1) to review the guidelines for ensuring information security in local governments and promote such measures as information security audit and training, etc. by approximately September 2006, and 2) to organize information sharing systems of local governments by the end of fiscal 2006. These efforts focus on the following policies:

A: Central Government

A) Establishment of the Standards for Measures and of the PDCA Cycle through Evaluations/Recommendations Based on the Standards

In order to upgrade the level of information security measures of government agencies to the world's highest level, the Standards for Measures shall be reviewed annually in accordance with changes in technologies and environment.

A Plan-Do-Check-Act Cycle (PDCA Cycle) of the whole government will be created by (1) inspecting and evaluating the implementation of security measures at the government agencies within the necessary scope, based on the Standards for Measures, and (2) linking the recommendations obtained from the evaluations to the improvement of the measures and to the upgrading of the Standards for Measures. Moreover, the results of evaluations are disclosed with due regard to maintenance/ensuring of information security.

Furthermore, since contents, experience and other related knowledge of government agencies are desired to serve as a reference to companies, local governments and incorporated administrative agencies, the knowledge shall be disclosed and disseminated in an understandable manner as "Best Practice". It is also important to give sufficient consideration to assurance of the level of information security measures of contractor.

B) Improvement of Security Measures of Incorporated Administrative Agencies, etc.

Upgrading of the level of information security of incorporated administrative agencies and the like shall be promoted based on the Standards for Measures. Particularly, the incorporated administrative agencies will formulate security

[12] Standards for Measures refer to "Standards for Information Security Measures for the Central Government Computer Systems" (decision made on 13 December, 2005 by the Information Security Policy Council), and the same below.

policies if they have not done so yet, in accordance with current situations of information assets and risks of each institution. If security policies have already been set forth, the incorporated administrative agencies will review them.

C) Strengthening and Consideration of Mid and Long-Term Security Measures

The government will make efforts for the implementation of information security measures that should be done in cooperation with all government agencies, such as standardization of required specifications on information security, emergency responses in the middle of a fiscal year, as well as the following security measures:

(a) Coordination with development of common operations and systems among all or some Ministries and Agencies to be optimized

In optimization of common operations and systems among all or some Ministries and Agencies, the government will promote newly developed (installed) systems in such a way as to standardize required specifications on information security and use highly reliable products through the clarification of information security functions, while seeking coordination with the Standards for Measures, etc.

(b) Consideration for the introduction of a new system (function) contributing to security enhancement and its realization

Toward establishment of the next generation E-Government, it is essential to consider the construction/development of a common platform for the basis of operations and systems of the entire government. In order to strengthen the security platform, the government will consider a comprehensive way of installing a new system (function), such as an IPv6, IC card for identification of government officials, data encryption, electronic signature, and biometrics, etc., and promote the realization of the system.

Particularly, in order to expedite the use of IPv6 in the information system of all government agencies, information and telecommunications equipment and software will be made compatible to IPv6 in principle by fiscal 2008, in accordance with the new development (installation) or modification of information system of each government agencies.

(c) Prevention of spoofing as a government agency

In order to prevent a malicious third party from spoofing a government agency, inflicting damage to the people or private companies, etc., an extensive

use of digital certification and use of domain names[13] that certify the identity of government agencies will be promoted to make the genuine government agencies easily identifiable.

(d) Promotion of the use of safe data encryption in government agencies

In order to ensure safety and reliability of E-Government, the safety of recommended cryptographic methods used by E-Government will continuously be monitored and studied and appropriate method of using data encryption will be considered in accordance with the advancement of technologies as well as international movements.

D) Reinforcement of Governmental Capacity of Emergency Response to Cyber Attacks, etc.

Efforts are necessary to promptly and appropriately respond to emergencies, such as cyber attacks, and adapt to technology or environmental changes. Specific measures to that end are to promptly share information among the government bodies and analyze the information in an integrated manner, and at the same time, it is necessary to strengthen the response capacity by improving the capacity of related responding agencies, by developing a response systems, and by incorporating the knowledge obtained from the emergency responses in the past into the improvement of Standards for Measures or human resource development of the government, etc.

E) Human Resource Development of Government Agencies

In order to proceed with information security measures of the entire government in an integrated manner and in view of the importance of development and securing of human resources with necessary knowledge and expertise, the government will promote the development of officials in charge of information system management of government agencies, utilization of human resources with expertise in information security, efforts in human resource development in cooperation with educational institutions, and the awareness raising of both executive and general officers. All officers specializing in information security operations in the information system management sections of government agencies will eventually obtain qualifications in information security.

[13] Domain name that certifies the identity of government agency refers to “go.jp” among the organizational type jp domain name, or to the domain name reserved as the one associated the administration and others among the Japanese domain names in the general use jp domain name.

B: **Local Governments**

A) Review of the guidelines for ensuring information security

Guidelines for ensuring information security of local governments will be reviewed, and at the same time, implementation of measures will be promoted based on the relevant guidelines in each local government.

B) Promotion of information security auditing

With respect to information security measures implemented by each local government, information security auditing will be promoted in order to contribute to the continuous improvement to the level of measures through evaluation and review of their effectiveness.

C) Promotion of establishment of "Information Sharing and Analysis Center of Local Government" (tentative)

In order to contribute to preemptive prevention of IT-malfunctions and its expansion, prompt resumption and prevention of recurrence and to improve the security level of all local governments, the government will promote the establishment of "Information Sharing and Analysis Center of Local Government" (tentative). The Center will have functions of gathering, analyzing and sharing of information on security of local governments and sharing of information provided by the central government and others.

D) Support for training of officers, etc.

In addition to the above, the government will support the development and introduction of advanced technologies and staff training, etc., in efforts to try to strengthen the security of local governments.

(2) Critical Infrastructures

With respect to critical infrastructures, as described in Chapter 2, Section 1, from the viewpoint that a stable supply of services is the priority issue, it is important to implement measures so as to prevent any IT-malfunction in each business from causing critical damage to people's social lives and economic activities of the country. However, the current situations indicate such problems as a lack of consideration for the measures against IT-malfunctions caused by incidents other than intentional acts, such as cyber attacks, etc., and an insufficiently structured information sharing system between public and private sectors. Therefore, with the purpose of reducing IT-malfunctions in critical infrastructures as close as possible to zero by the beginning of fiscal 2009, the government will exert efforts focusing on

the following policies in the next three years. Meanwhile, information security measures for critical infrastructures are separately set forth in the "Action Plan on Information Security Measures for Critical Infrastructures" (decision made on December 13, 2005 by the Information Security Policy Council), and more specific measures will be implemented in line with the Action Plan.

A) Improvement of "Safety Standards" on information security assurance for critical infrastructures

Based on the "A Principle for Formulating of 'Safety Standards, Guidelines, etc.'[14] concerning Assurance of Information Security of Critical Infrastructures"[15], the level of necessary or desirable information security in each critical infrastructure sector will be stipulated in the Safety Standards, Guidelines, etc.. The guidelines will be reviewed annually or whenever necessary, and Safety Standards, Guidelines, etc. will be reviewed on an as-needed basis in accordance with changes in environment surrounding information security.

B) Enhancement of information sharing system

The government and other entities will provide information concerning IT-malfunctions to business entities engaged in critical infrastructures timely and appropriately, and will enhance the information sharing system among the business entities engaged in each critical infrastructure sector and among the interdependent critical infrastructure sectors. This is in view of the following aspects: 1) preemptive prevention of IT-malfunctions, 2) prevention of expansion of suffering and rapid resumption, and 3) prevention of recurrence through analysis/verification of causes of IT-malfunctions.

(a) Development of an environment for information provision/connection between public and private sectors

In cooperation among related organizations, information, such as caution, to be provided to business entities engaged in critical infrastructures to contribute to the measures taken by them will be collected and provided through CEPTOAR (to be hereinafter described), etc..

The government will promote the development of an environment in which business entities engaged in critical infrastructures provide the government with

[14] Safety Standards, Guidelines, etc. refer to documents formulated as criteria or references used by business entities engaged in critical infrastructures for making various decisions and actions.

[15] Guidelines for Formulating of 'Safety Standards, Guidelines, etc.' concerning Assurance of Information Security of Critical Infrastructures (decision made on 2 February, 2006 by the Information Security Policy Council)

information on incidents, failures, and operational delays, etc., to be submitted under laws and regulations, as well as with unique and crucial information deemed to be disclosed to the government.

(b) Development of CEPTOAR (Capability for Engineering of Protection, Technical Operation, Analysis and Response) in each critical infrastructure

Information provided by the government for preemptive prevention of IT-malfunctions, prevention of expansion of suffering and rapid resumption, and prevention of recurrence will be appropriately made available to business entities engaged in critical infrastructures and will be shared among them. This will eventually contribute to the upgrading of capacity to maintain and reconstruct services of each business entities engaged in critical infrastructures. In order to serve this purpose, the government will promote the development of Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR) within each critical infrastructure sector.

(c) Promotion of establishment of "CEPTOAR-Council (tentative)"

In order to promote cross-sectoral information sharing among business entities engaged in critical infrastructures and utilize knowledge for maintenance and resumption of services, the government will promote the establishment of "CEPTOAR-Council (tentative)" as an instrument for cross-sectoral information sharing among each CEPTOAR.

C) Implementation of analysis of interdependence

In order to grasp the cross-sectoral situation toward improving critical infrastructure measures throughout the entire nation, the government will make efforts to get a grip of what the potential threats are in each critical infrastructure and of interdependence as to what impact will ripple through other critical infrastructures when an IT-malfunction occurs in a critical infrastructure.

D) Implementation of cross-sectoral exercises

Based on a stereotype of a specifically envisioned threat scenario, cross-sectoral exercises will be performed under cooperation among presiding ministries of each critical infrastructure, each business entities engaged in critical infrastructures and CEPTOAR in each infrastructure sector. Through the exercises, effectiveness and propriety of each measure, such as safety standards, guidelines, etc., an information sharing frameworks, functions for information sharing and analysis, analysis of interdependency, will be periodically evaluated in stages. Furthermore, through these exercises and other training and seminar sessions, personnel with

advanced IT skills will be developed and secured, primarily for presiding ministries of each critical infrastructure and business entities engaged in critical infrastructures.

(3) Businesses

As described in Chapter 2, Section 1, it is necessary to implement measures from the aspect that businesses are leading players in economic growth in the globalized world, and also provide products and services that support IT,. However, current situations indicate that businesses are confronted with problems; for example, security measures are not being linked to market valuation and human resources in information security within businesses are insufficiently developed and secured. In order to counter the situation, the government will expend efforts focusing on the following priority policies for the next three years with purpose of improving the implementation of information security measures of businesses to the world's highest level by the beginning of fiscal 2009.

A) Development of an environment that will link information security measures of businesses to market valuation

The government will promote the establishment and operation of corporate governance with consideration for corporate social responsibility and an internal control framework that supports the governance from the perspective of information security. To that end, efforts will be made to disseminate and improve the Information Security Measures Benchmark, Information Security Report Model, and Guidelines for Formulating a Business Continuity Plan. Furthermore, evaluation on the level of information security will be made one of the conditions for public bidding for information system, etc., if necessary. The evaluation will be able to use, for example, the said systems or third party evaluation results. In addition, consistency of the government's approach concerning information security will be ensured.

B) Promotion of the provision of high quality products and services related to information security

The information security measures have characteristics that their functions different from original business are to be implemented according to risks, the measures themselves are hard to visualize, etc. Due to these characteristics, it is necessary to create an environment so that businesses are able to easily choose necessary measures to implement. To that end, the government will make efforts to promote the provision of high quality products and services related to

information security through the promotion of the use of third party evaluations, such as IT security evaluation and certification system, the Compatibility Assessment System for Information System Management Systems (ISMS), information security audits, in addition to the promotion of study on quantitative evaluation technique for information security-related risks of businesses.

The government will also make efforts to streamline the evaluation of third parties and to promote an environment so that there are incentives to accelerate the investment in businesses which utilize high quality information security-related products, etc.

C) Securing/Development human resources engaged in information security of businesses

Understanding of top management about information security and human resource engaged in information security within businesses are still insufficient. Therefore, the government will make efforts to increase understanding of top management about information security through improvement of the environment in which information security measures of businesses are linked with market valuation, and to promote nationwide PR activities for personnel in charge of information systems. Furthermore, more efforts will be expended to maintain motivation of personnel in charge of information security measures in each company.

D) Strengthening systems to rapidly respond to computer viruses and vulnerability, etc.

In order to appropriately respond to information security issues of businesses, it is necessary to make efforts to achieve rapid information sharing, and smooth formulation and dissemination of measures among concerned parties, including information-related businesses. To that end, the government will set up a communication system and enhance a coordinated response system to rapidly respond to computer viruses or vulnerabilities, etc, with proactive cooperation of information-relate businesses.

(4) Individuals

As described in Chapter 2, Section 1, in terms of measures for individuals, it is first necessary to be cognizant of the fact that the level of understanding of 80 million internet users about information security is varied. And then, it is required for all concerned parties to take various measures to support the improvement in literacy on information security of individuals regardless of age or gender in

accordance with their own situations. However, current situations indicate an environment has yet to be created in which an individual considers information security as a must. Moreover, the environment is still so immature that the limit of personal responsibility cannot be complemented despite the fact that the framework of IT is not easily understandable for the peoples. Therefore, the government will make efforts focusing on the following policies in the next three years with the purpose of reducing the number of individuals who feel insecure about IT use as close as possible to zero by the beginning of fiscal 2009.

A) Enhancement/promotion of information security education

The government will promote information security education from primary and secondary schools and inter-generation information security education.

B) Enhancement/promotion of PR activities/information transmission

The following efforts will be promoted: continuous implementation of nationwide PR activities and information transmission; holding of events recognized as landmarks (creation of “Information Security Day”, etc.), establishment of a framework of the routine campaigns/information provisions (consideration of implementation of Information Security Forecast (tentative)), dissemination of National Strategies on information security of Japan both nationally and internationally.

C) Promotion of an environment in which individuals are able to use information-related products and services without much burden

The government will promote an environment where information-related businesses can develop and supply products and services (“Information Security Universal Design”) which individuals can use without much burden while enjoying highly advanced information security functions.

Section 2: Formation of Cross-Sectoral Information Security Infrastructure

In order to promote the formation of awareness as to for what purpose and to what degree of risks each individual takes information security measures, and in order to maintain continuous and rigid information security measures of public and private sectors, it is necessary to construct an infrastructure of the whole society as its base. To that end, the government is required to comprehensively address policies from the perspectives of the promotion of the strategy concerning information security technology, development and securing of human resources engaged in information security, promotion of international partnership and cooperation, crime control, and protection and redemption

of rights and interests.

(1) Promotion of Strategy concerning Information Security Technology

In order to create an environment for the safe use of IT described in Chapter 1, advancement of technology in information security and the use and utilization of IT with understanding of the technology are essential. However, current situations indicate two problems; 1) development of information security technology cannot respond to the rapidly expanding use and utilization of IT, and 2) the balance between technology and organizational/human management methods that complement the limit of existing information security technology has been lost.

Therefore, the government will make efforts focusing on the following policies of technology strategy concerning information security in the next three years, while clarifying the division of roles between the government and private sector.

A) Establishment of an implementation system effective for research and development (R&D) and technology development

In order to implement R&D and technology development effectively and efficiently with limited investments, the government will try to grasp the current situations and conduct periodical reviews of R&D and technology development of information security of Japan. Furthermore, in order to improve investment efficiency, the government will establish a system to perform R&D and technology development, keeping in mind the use of outcomes, and to launch new R&D and technology development efforts on the premise of outcomes being used by the government.

B) Prioritization of information security technology development and improvement of the environment

In order to advance information security technology and upgrade the organizational/human resource management methods, the government will promote R&D and technology development to achieve mid and long-term objectives that are tied to enhancement of IT infrastructure. At the same time, with respect to R&D and technology development for which short term objectives have been laid out, the government will evaluate the investment efficiency and inject a well-balanced investment. The government will take an active role as an incubator for emerging R&D programs for which efforts of the private sectors are not expected although high investment efficiency is predicted.

C) Promotion of the 'Grand Challenge' project for research and development (R&D) and technology development

Information security measures require built-in R&D which is based on mid and long-term perspective, not just measures for immediate problems. Therefore, for the R&D and technology development of information security, the government will pursue not only technology development for short-term solutions to issues, but also the Grand Challenge R&D project and technology development aiming to realize fundamental technology innovation with a long-term perspective.

(2) Development/Securing of Human Resources Engaged in Information Security

Factors required to create an environment for the safe use of IT described in Chapter 1 are the implementation of information security measures by implementation entities and the development and securing of human resources that can support advanced R&D and technology development concerning information security.

In doing so, it is important to develop highly competent information security engineers. In addition, due consideration must be given to the fact that it is necessary to develop operators and specialists with multidisciplinary and comprehensive capacity, such as chief information security officers (CISO) with wide knowledge and keen insight in each organization, personnel in charge of operation of information systems and legal personnel and others within each organization. Also important is to realize that it requires a long time to develop human resources, and the development of human resources that excel in an international arena is required.

Therefore, the government will make efforts in human resource development for the measures of government agencies (Chapter 3, Section 1-(1) A E)), human resource development of the measures for critical infrastructures (Chapter 3, Section 1-(2) D)), and human resource development for businesses (Chapter 3, Section 1-(3) C)) in the next three years, and at the same time, will make efforts focusing on the following policies.

A) Development of businesspersons and specialists with multidisciplinary and comprehensive capability

In information security-related higher education institutions (primarily graduate schools), proactive efforts will be promoted for the development and securing of human resources with multidisciplinary and comprehensive capability by, for example, accepting students and adults of other areas as well as providing

recurrent education[16].

B) Systematization of a qualification system concerning information security

The government will clearly define the appropriate skills required for highly competent information security engineers, CISO in each organization, and personnel in charge of the information systems of each organization, and promote systematization of a qualification systems concerning information security.

(3) Promotion of International Partnerships and Cooperation

As globalization of the use and utilization of IT and economic activities has increased, it has become important to improve information security infrastructure to make the benefits available to society. In doing so, the following efforts are important: 1) to address issues while maintaining international cooperation since the threats to information security have become borderless, increased and diversified, and 2) to present the "Japan Model" of information security to the outside world since the problems that Japan confronts as the world's leading broadband country are the ones other countries will face in the future and since Japan holds the position of growing responsibility for solving problems as the world's top runner.

Based on the perspectives above, the government will make efforts focusing on the following policies in the next three years with respect to international partnership and cooperation in the information security area.

A) Contribution to the establishment of internationally safe/secure infrastructure and the development of an environment

The government will empower partnerships such as information exchange with related organizations of other countries, through active participation in early warning, monitoring and alarm raising networks, etc. for the protection of critical infrastructures, in addition to the promotion of cooperation within a multinational framework, such as OECD and G8. In doing so, the government will clarify the function of Point of Contact (POC) of Japan to deal with cross-sectoral information security issues and to promote more effective and smooth coordination.

Furthermore, the government will contribute to the cultivation of culture and the improvement of literacy at an international level, and the development of an environment on an international scale.

[16] Recurrent education refers to distribution of educational opportunities for individuals, mostly people in workforce, after they have left formal education.

B) International contribution of Japan in the area of information security

While making use of the strengths of Japan, the government will actively perform its role through the creation of high value-added innovation, international utilization of technology development with foresight, dissemination and enlightenment of “Best Practice”, and contribution to the development of international standards.

(4) Crime Control and Protection and Redemption of Rights and Interest

In order to create an environment for the safe use of IT, it is necessary to ensure that cyberspace is safe and reliable to use by, for example, preventing cybercrimes before they happen, keeping the cybercriminals in check, and protecting and redeeming the damaged rights and interests in cyberspace.

With the above in mind, the government will make efforts focusing on the following policies in the next three years.

A) Development of infrastructure to control cybercrimes and to protect and redeem rights and interests

The government will upgrade the standard of cybercrime investigation of law enforcement institutions and reinforce its system. At the same time, the government will crack down on cybercrimes through the amendment of the law systems along with the conclusion of cybercrime agreements and the strengthening of international cooperation. In addition, the government will further develop infrastructure for the protection and redemption of rights and interests in cyberspace, while giving due consideration to other rights and interests: namely, basic human rights, including confidentiality of communications.

B) Development and dissemination of technologies to increase safety and reliability in cyberspace

The government will promote the development and dissemination of identification technology to identify the user at the other end of the communication line is under the approval of all the concerned parties in communications as well as in terms of the technology to improve safety and reliability in other cyberspace contexts.

Chapter 4: Policy Promotion System and Structure of Continuous Improvement

The government will make efforts focusing on the policies described in the previous Chapters in the next three years based on the following systems and continuous structures.

Section 1: Policy Promotion System

Participation of every entity is necessary in order to achieve the objective to become an information security advanced nation through a new public-private partnership model and to create an environment for the safe use of IT. Therefore, the government is required to increase the official capacity to respond as described in the Basic Principles in Chapter 1 and on the other hand, it is also necessary to allocate resources appropriately as a whole nation to promote integrated and cross-sectoral information security measures of the public and private sectors, while coordinating the role of the government explained in Chapter 2 Section 2, and focusing on the priority policies described in Chapter 3.

(1) Enhancement of the National Information Security Center (NISC)

The National Information Security Center (NISC) aims to reinforce the functions of the promotional system of the government so that the system will perform effectively for the compilation of the highest wisdom of both within and outside Japan. The NISC assumes the following tasks: preparation of basic strategies regarding information security policies of the whole government, designing of technological strategies concerning information security led by new R&D and technology development on the premise that the government will utilize the outcomes, inspection and evaluation of information security measures of the government, analysis of interdependency as to the information security measures among critical infrastructures, formulation and review of Guidelines for Formulation of ‘Safety Standards, Guidelines, etc.’ concerning Information Security Assurance of Critical Infrastructures, promotion of cross-sectoral exercises, and acting as an international Point of Contact (POC) on the cross-sectoral issues of information security, etc.

Furthermore, since a lot of knowledge on information security has been accumulated in the private sectors, the NISC will actively strive for utilization of manpower therein, and at the same time, will aim to function as a center for human resources development of government officials.

(2) Enhancement of Ministries and Agencies

In order to actively promote information security measures of the whole

government, having the Information Security Policy Council and the NISC as its core, Ministries and Agencies will be committed to the improvement and strengthening of the information security system of its own. At the same time, in trying to change the traditionally bureaucratic sectional system, Ministries and Agencies will make efforts to implement every measure so that integrated and cross-sectoral information security measures will be facilitated in public and private sectors.

Section 2: Partnerships with Other Related Organizations

The National Strategy stipulates mid and long-term strategies in view of the information security issues in Japan; however, information security is widely associated with people's social lives and economic activities, and it is necessary to pursue cooperation with various related organizations in implementing the strategies.

It is required to pay particular attention to the following facts; in terms of the relationship with IT Strategic Headquarters, information security policies are to be positioned as one of the primary factors of IT policies in various related organizations; and the National Strategy is to practically assume the part of the information security-related elements of the IT New Reform Strategy. In terms of the relationship with the Council for Science and Technology Policy, it is necessary to make sure that factors related to R&D and technology development within information security policies are consistent with the science and technology policies of the government. Thus, Information Security Policy Council and NISC will promote information security policies in cooperation with each other.

Section 3: Establishment of the Structure of Continuous Improvement

The situations surrounding the issues on information security change rapidly; for example, new risk factors can emerge one after another and unexpected incidents, disasters and attacks can occur. It is thus necessary to constantly evaluate and improve the effectiveness of the policies. The government is required to construct bases for the continuous improvement as below.

(1) Formulation and Evaluation of the Annual Plan

In order to realize the National Strategy, the government will formulate the Annual Plan as an implementation plan of more specific measures every fiscal year, evaluate the implementation, and disclose the results as much as possible.

Meanwhile, in order to smoothly promote the measures, such as when a case must be responded to by related organizations other than the government, the government

will consider a milestone setting that covers several fiscal years, for those requiring mid and long term plans, without adhering to an annual plan.

(2) Implementing Measures to Respond to Emergencies during Execution of the Annual Plan

The government, while even executing annual plan, will implement measures to respond to emergencies in the event of incidents, disasters or attacks, etc.

(3) Development of Evaluation Criteria

No definite evaluation criteria for information security in each implementation area of measures have been set up thus far. However, since these criteria are indispensable for the evaluation of the degree of diffusion of information security measures in each implementation area, the government will promptly consider the criteria, aiming to utilize them for the evaluation of the implementation of the National Strategy.

(4) Review of the National Strategy

The government will review the National Strategy every three years, and will do so even in the middle of the period of implementation in the event of change in circumstances.