NISC National Information Security Center

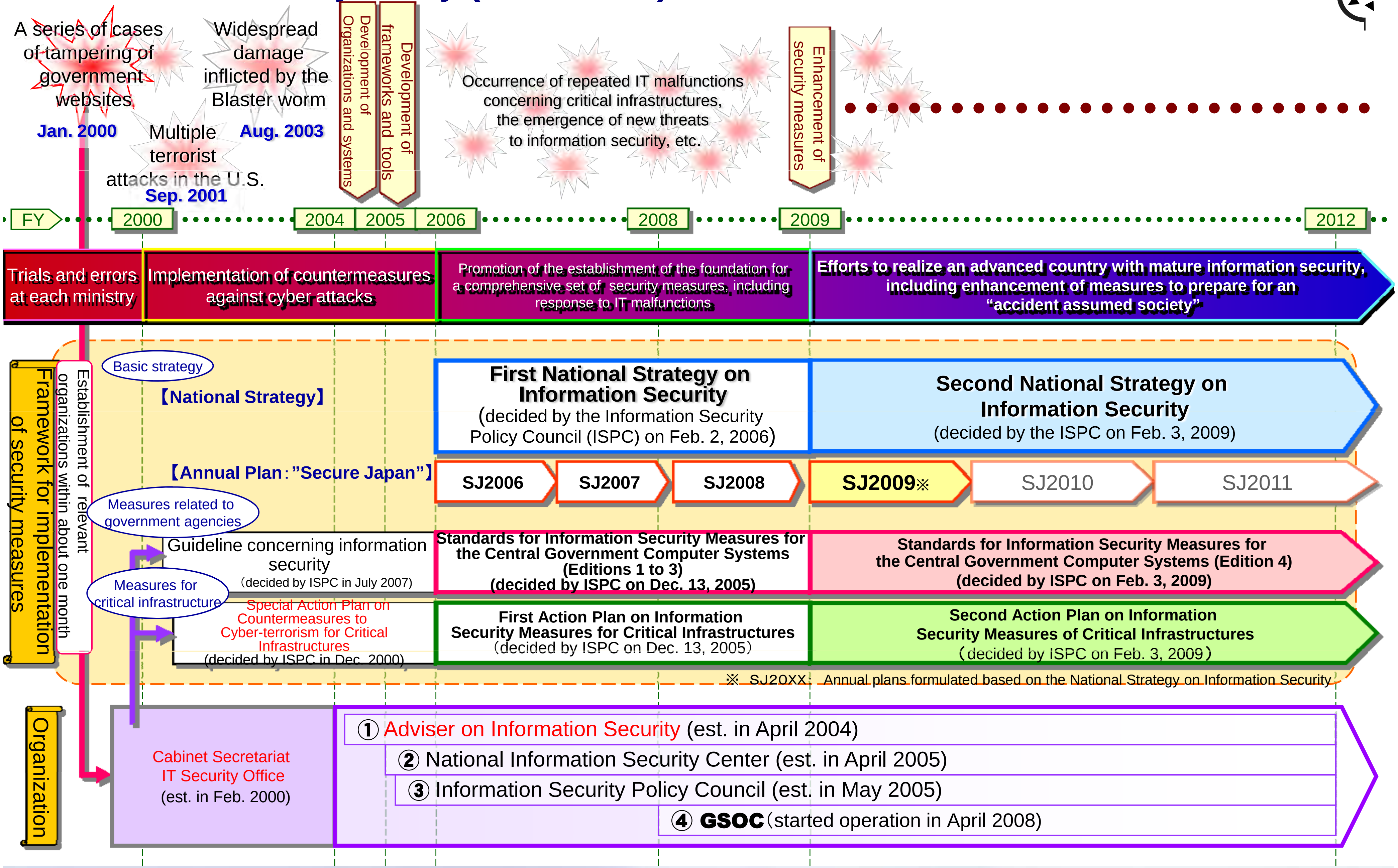
Outline of the Second National Strategy on Information Security

National Information Security Center (NISC)

http://www.nisc.go.jp/eng/index.html

Chronology of the Implementation of the Cabinet Secretariat's Information Security Policy (since 2000)

NISC



A series of cases of tampering of government websites
Jan. 2000

Multiple terrorist attacks in the U.S.
Sep. 2001

Widespread damage inflicted by the Blaster worm
Aug. 2003

Development of Organizations and systems

Development of frameworks and tools

Occurrence of repeated IT malfunctions concerning critical infrastructures, the emergence of new threats to information security, etc.

Enhancement of security measures

FY 2000 2004 2005 2006 2008 2009 2012

Trials and errors at each ministry

Implementation of countermeasures against cyber attacks

Promotion of the establishment of the foundation for a comprehensive set of security measures, including response to IT malfunctions

Efforts to realize an advanced country with mature information security, including enhancement of measures to prepare for an "accident assumed society"

Framework for implementation of security measures

Establishment of relevant organizations within about one month

Basic strategy

【National Strategy】

First National Strategy on Information Security (decided by the Information Security Policy Council (ISPC) on Feb. 2, 2006)

Second National Strategy on Information Security (decided by the ISPC on Feb. 3, 2009)

【Annual Plan："Secure Japan"】

SJ2006 SJ2007 SJ2008 SJ2009※ SJ2010 SJ2011

Measures related to government agencies

Guideline concerning information security (decided by ISPC in July 2007)

Standards for Information Security Measures for the Central Government Computer Systems (Editions 1 to 3) (decided by ISPC on Dec. 13, 2005)

Standards for Information Security Measures for the Central Government Computer Systems (Edition 4) (decided by ISPC on Feb. 3, 2009)

Measures for critical infrastructure

Special Action Plan on Countermeasures to Cyber-terrorism for Critical Infrastructures (decided by ISPC in Dec. 2000)

First Action Plan on Information Security Measures for Critical Infrastructures (decided by ISPC on Dec. 13, 2005)

Second Action Plan on Information Security Measures of Critical Infrastructures （decided by ISPC on Feb. 3, 2009）

※ SJ20XX: Annual plans formulated based on the National Strategy on Information Security

Organization

Cabinet Secretariat IT Security Office (est. in Feb. 2000)

① Adviser on Information Security (est. in April 2004)

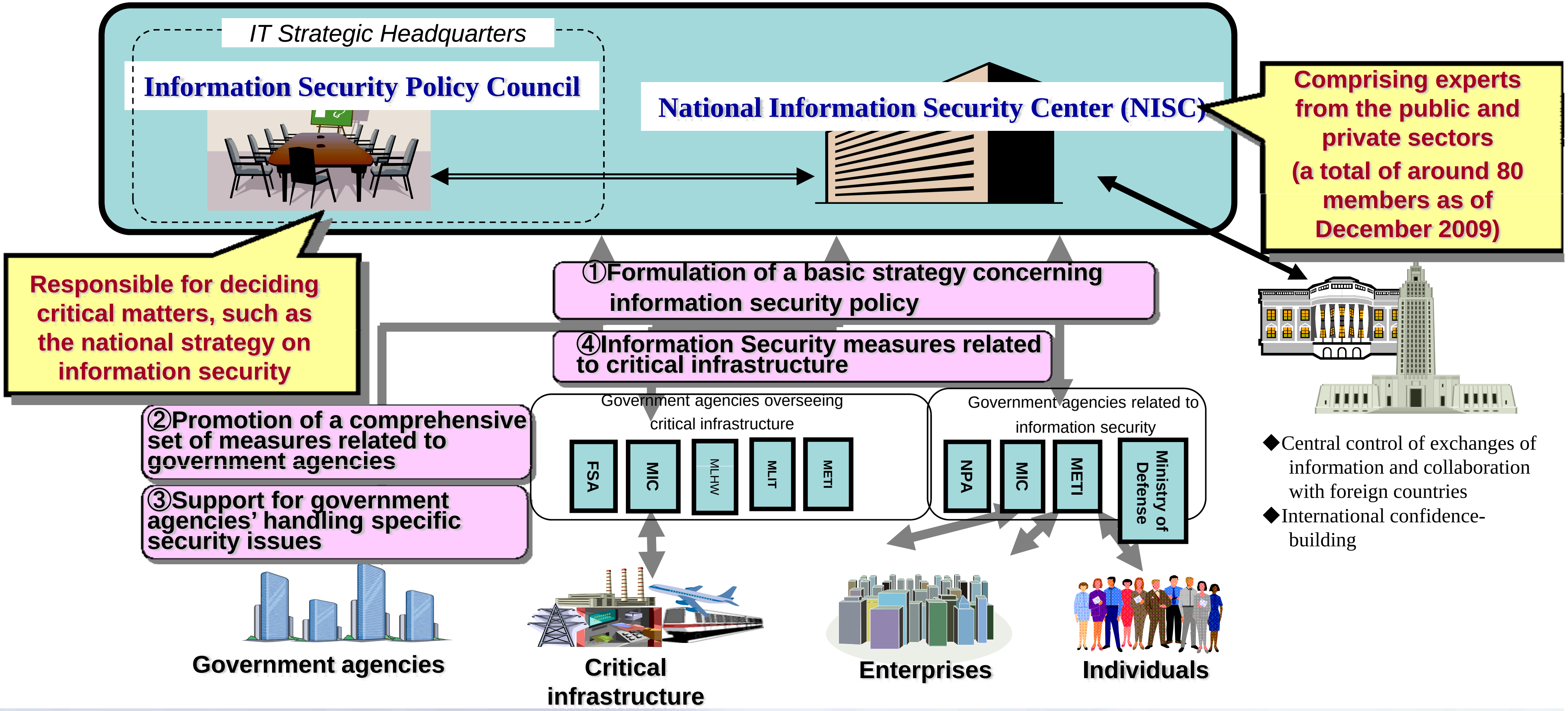
② National Information Security Center (est. in April 2005)

③ Information Security Policy Council (est. in May 2005)

④ GSOC（started operation in April 2008)

Establishment of Information Security Policy Council and National Information Security Center

- Japan developed the functions and systems in order to strengthen the government's core functions related to information security issues in response to the adoption of "Toward Review of Government's Roles and Functions related to Information Security Issues" (decided by the IT Strategic Headquarters in December 7, 2004)
  - **Established the National Information Security Center (NISC) on April 25, 2005.**
  - **Established the Information Security Policy Council under the IT Strategic Headquarters on May 30, 2005.**



IT Strategic Headquarters

Information Security Policy Council

National Information Security Center (NISC)

Comprising experts from the public and private sectors (a total of around 80 members as of December 2009)

Responsible for deciding critical matters, such as the national strategy on information security

①Formulation of a basic strategy concerning information security policy

④Information Security measures related to critical infrastructure

②Promotion of a comprehensive set of measures related to government agencies

③Support for government agencies' handling specific security issues

Government agencies overseeing critical infrastructure

FSA | MIC | MLHW | MLIT | METI

Government agencies related to information security

NPA | MIC | METI | Ministry of Defense

◆Central control of exchanges of information and collaboration with foreign countries
◆International confidence-building

Government agencies

Critical infrastructure

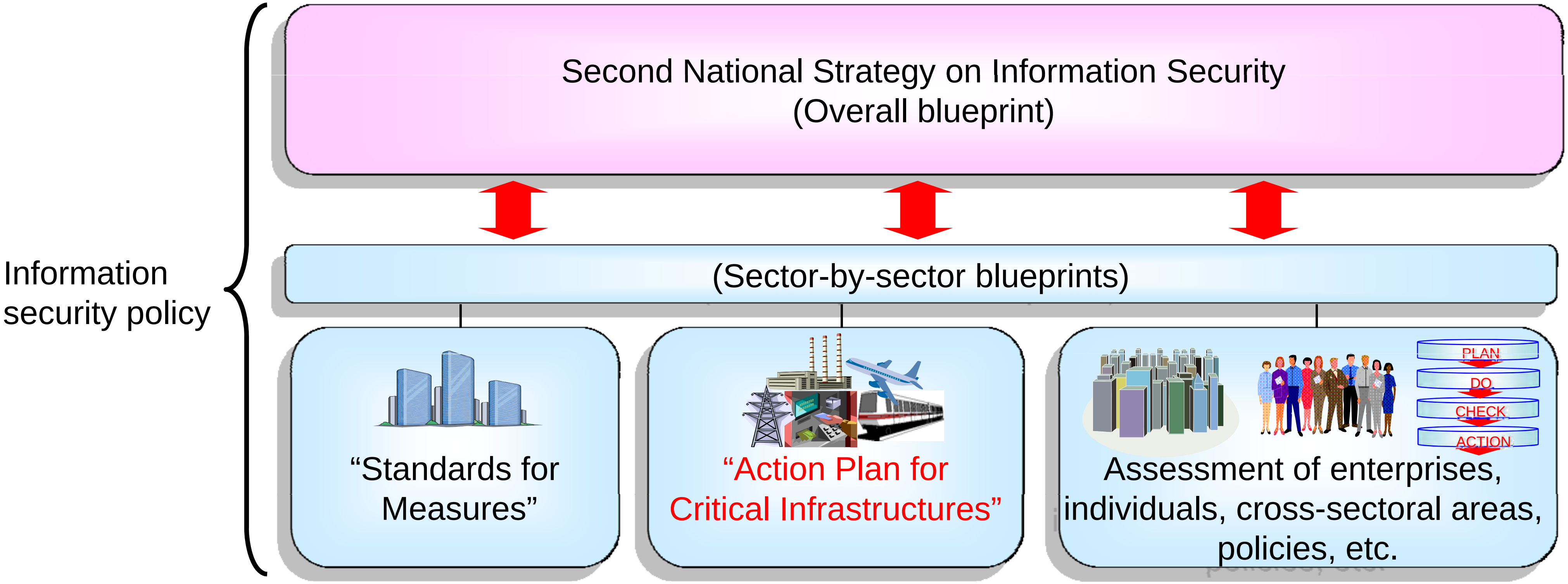
Enterprises

Individuals

Second National Strategy on Information Security as the "overall blueprint" of the security policy and sector-by-sector "blueprints"

○Information security policy is implemented based on the combination of the Second National Strategy on Information Security, which serves as the overall design of the policy, and sector-by-sector blueprints.

○Policy implementation based on this combination avoids a vertically compartmentalized approach focusing on individual sectors and enables Japan as a whole to appropriately deal with the increasingly complex information security issues from cross-sectoral and cross-policy area perspectives.



Information security policy

Second National Strategy on Information Security
(Overall blueprint)

(Sector-by-sector blueprints)

"Standards for Measures"

"Action Plan for Critical Infrastructures"

Assessment of enterprises, individuals, cross-sectoral areas, policies, etc.

Results of the “First National Strategy on Information Security” and Goals of the “Second National Strategy on Information Security” (Vision)

1. First National Strategy (’06–’08)

Results

Launch of information security policy

◆**Awareness among relevant people increased.**

→ Risk of information leakage due to the use of peer-to-peer software

→ Risk of information theft through cyber attacks

→ Risk of system malfunctions leading to the suspension of business operations

◆**A framework for policy promotion established.**

→ Promotion of measures based on “Standards for Measures” and assessment thereof

→ Information-sharing between operators of critical infrastructures

→ Establishment of a framework for information-sharing between Japan and the U.S. and between Japan and ASEAN

◆**Some progress was made in preventive measures (for problem prevention)**

→ However, new risks arise day after day and they constantly change.

2. Second National Strategy (’09 –’11)

Goals

Continuation and further development of policy

◆**Preventive measures taken routinely.**

Ex-post measures and recovery activities can be implemented quickly and calmly if a problem arises

◆ **Entities that entrust information, as well as entities that manage information, will be covered by the measures.**

Composition of “Second National Strategy on Information Security”

Chapter 1

Actions under the First National Strategy on Information Security and the Status Report for 2009

1 Actions taken under the First National Strategy of Information Security (descriptions of the concept of the First National Strategy on Information Security, etc.)

2 Perspectives in 2009 (examination of the situation resulting from the various actions taken under the First National Strategy)

Chapter 2

Basic Concept of the Second National Strategy of Information Security and the Objectives in 2012

1 Basic Concept of the Second National Strategy of Information Security (descriptions of the concept of the Second National Strategy using a comparison with the First National Strategy as necessary)

2 Objectives in 2012 (descriptions of what the situation will be like after the effective period of the strategy as a result of the various measures taken under the Second National Strategy)

Chapter 3

Important Policies for the Next Three Years

1 Promotion of measures in the four areas and steady implementation of the objectives of the policy (descriptions of central and local governments, critical infrastructure, enterprises and individuals)

2 Enhancement and development of cross-field information security infrastructure (descriptions of technologies, human resources, international cooperation and anti-crime measures)

Chapter 4

Promotional Scheme of Policies and Sustainable Improvement

1 Promotional schemes of policies

2 Relationships with other related organizations

3 Sustainable improvement structure

Overall Picture of the Second National Strategy on Information Security [1]

○As a medium- and long-term plan concerning overall information security issues (overall design), the Second National Strategy on Information Security (draft) sets forth 1) the basic concept and 2) the direction of important policies with regard to the measures to be taken by Japan.

○Specifically, it covers the three years from fiscal 2009 to fiscal 2011. As previously, the “Secure Japan,” a policy implementation plan for each year, will be formulated, and the implementation status of measures and social changes in each year will be assessed.

“Development” and “continuity” from the First National Strategy

1. Continued promotion of specific measures and policy actions to deal with new issues
   (Continued use of various frameworks for implementation of measures established under the First National Strategy)
2. Challenges in realizing an “Accident Assumed Society”
   （To be always prepared for a problem that might occur despite the implementation of sufficient preventive measures.
3. Rationality-based approach
   (implementation of measures that are rational (optimal) relative to the value of information assets and the degree of risk)

Overall Picture of the Second National Strategy on Information Security [2]

Basic Concept of the Second National Strategy

●Primary goal → Establishment of a safe IT environment

(Same objective as the one under the First National Strategy. Implementation of the provision of Article 22 of the IT Basic Law)

●Basic principle for the implementation of measures → Maturation of the concept of "Information Security Advanced Nation"

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

(The goal is not to pursue absolutely infallible security but to achieve security based on the implementation of an optimal level of measures. → In order to depart from the pursuit of absolutely infallible security, it is essential to change the mindset of the people and society as a whole.

●Measures to achieve the primary goal → New model of collaboration between the public and private sectors＋Promotion of measures that gives consideration to information providers (as well as entities that implement security measures)

(Under the First National Strategy, a new model of collaboration between the public and private sectors that involves entities that implement security measures and those that support the measures was pursued. In light of the changes in the circumstances, measures that give consideration to information providers will also be taken.)

Overall Picture of the Second National Strategy on Information Security [3]

Policy Areas where Measures are Taken under the Second National Strategy

●Measures covering from the identification of issues to the implementation of preventive and ex-post actions
（In addition to the implementation of preventive actions, preparation for ex-post actions will be made in case a problem should arise.)

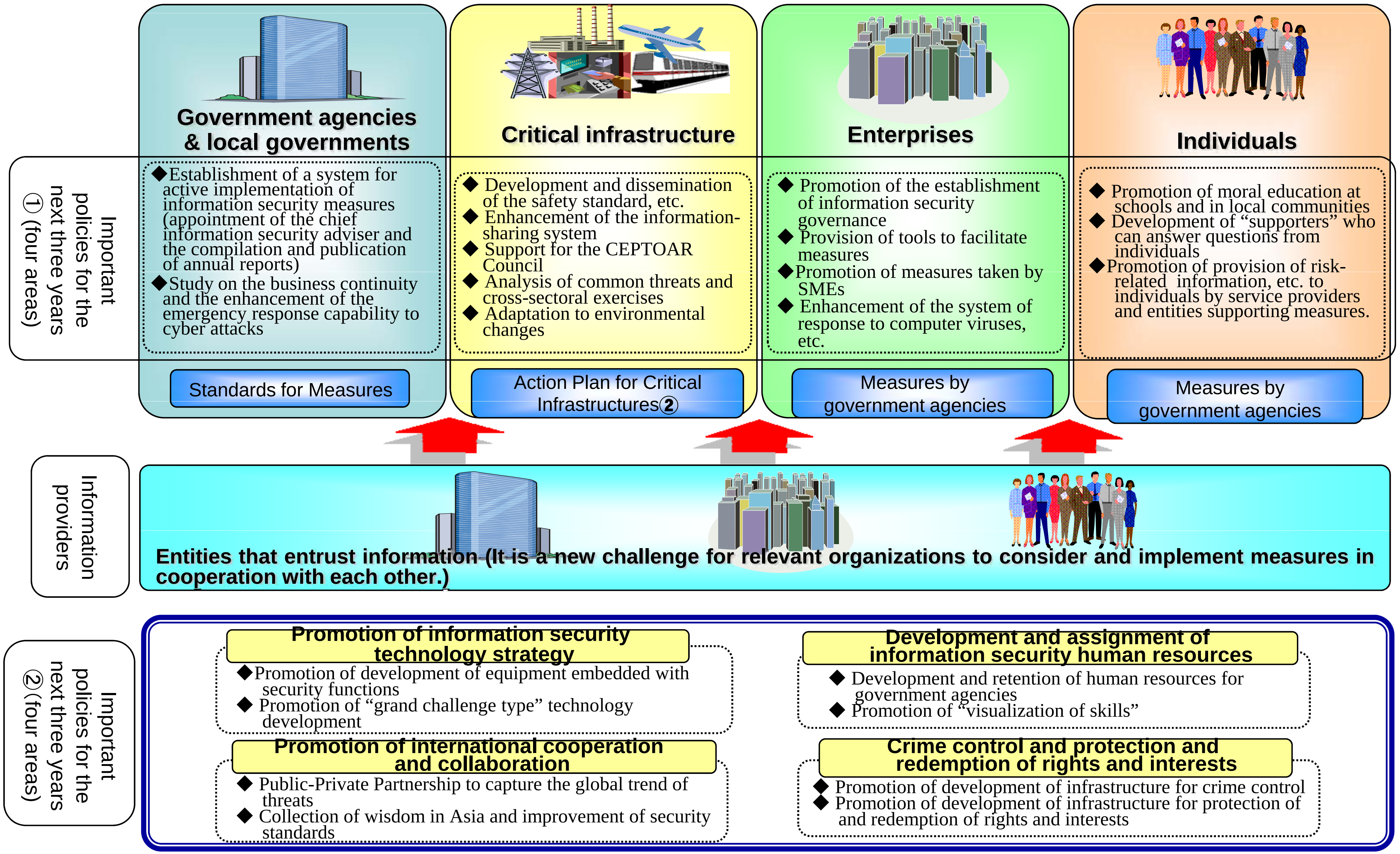
●Measures covering from technical matters to institutional and personnel-related matters
（A wide range of measures, from technology development to human resource development, will be taken.)

●Measures covering from the implementation of domestic activities to international activities for the purpose of ensuring information security
(As the cross-border utilization of IT has become commonplace, domestic and international measures will be organically linked with each other.)

●Measures taken in policy areas closely related to individual entities, such as daily life and economic activity and those closely related to the nation as a whole, such as national security and culture.
(Given that information security issues are fairly wide-ranging, measures will be flexibly taken across different policy areas from various perspectives.)

Measures Based on the Second National Strategy on Information Security – Important Policies for the Next Three Years –

NISC



Important policies for the next three years ① (four areas)

Government agencies & local governments

- ◆Establishment of a system for active implementation of information security measures (appointment of the chief information security adviser and the compilation and publication of annual reports)
- ◆Study on the business continuity and the enhancement of the emergency response capability to cyber attacks

Standards for Measures

Critical infrastructure

- ◆ Development and dissemination of the safety standard, etc.
- ◆ Enhancement of the information-sharing system
- ◆ Support for the CEPTOAR Council
- ◆ Analysis of common threats and cross-sectoral exercises
- ◆ Adaptation to environmental changes

Action Plan for Critical Infrastructures②

Enterprises

- ◆ Promotion of the establishment of information security governance
- ◆ Provision of tools to facilitate measures
- ◆Promotion of measures taken by SMEs
- ◆ Enhancement of the system of response to computer viruses, etc.

Measures by government agencies

Individuals

- ◆ Promotion of moral education at schools and in local communities
- ◆ Development of "supporters" who can answer questions from individuals
- ◆Promotion of provision of risk-related information, etc. to individuals by service providers and entities supporting measures.

Measures by government agencies

Information providers

Entities that entrust information (It is a new challenge for relevant organizations to consider and implement measures in cooperation with each other.)

Important policies for the next three years ②(four areas)

Promotion of information security technology strategy

- ◆Promotion of development of equipment embedded with security functions
- ◆ Promotion of "grand challenge type" technology development

Development and assignment of information security human resources

- ◆ Development and retention of human resources for government agencies
- ◆ Promotion of "visualization of skills"

Promotion of international cooperation and collaboration

- ◆ Public-Private Partnership to capture the global trend of threats
- ◆ Collection of wisdom in Asia and improvement of security standards

Crime control and protection and redemption of rights and interests

- ◆ Promotion of development of infrastructure for crime control
- ◆ Promotion of development of infrastructure for protection of and redemption of rights and interests

※In addition, measures related to supporting entities (entities that support entities implementing information security measures).

Measures related to Government Agencies under the Second National Strategy on Information Security

Measures taken under the First National Strategy on Information Security:
“Establishment of the PDCA cycle for each government agency and government agencies as a whole (for the purpose of implementation of measures that meet a level required by the Standards for Measures by government agencies)”
→The processes of the cycle have not yet become fully active (driven by the spontaneous efforts of each government agency) in some cases. In addition, there is a lack of awareness of the need to implement security measures based on an appropriate understanding of risks.

Under the Second National Strategy

- Enhancement of organizations and systems for the establishment of information security governance at government agencies
- Enhancement of government agencies’ capability to take ex-post actions

○Appointment of the chief information security adviser and compilation and publication of annual reports by each government agency

○Development of a mechanism to collectively utilize the knowledge of researchers and practitioners at relevant incorporated administrative agencies and other organizations

○Development of a mechanism for incorporating security measures into information systems with cost reduction in mind.

○Reinforcement of Business Continuity and Emergency Response in Government Agencies (formulation of operational sustainability plans, studies on back-up systems and enhancement of emergency communications systems and the capability to analyze cyber attacks)

○Promotion of Measures for Incorporated Administrative Agencies (specification of issues related to security measures in the medium-term goal and development of effective systems for communications with relevant government agencies)

○Promotion of the use of secure encryption by government agencies

Measures related to Local Governments under the Second National Strategy on Information Security

Measures taken under the First National Strategy

"Review of the guidelines for ensuring information security at local governments, development of systems for information-sharing among local governments, etc."

→Some small local governments are lagging in implementing measures. From the viewpoint of promoting information security at the local community level, it is important to create a favorable environment for local governments to implement security measures so as to strengthen the foundation for information security.

Under the Second National Strategy

- **Implementation of desirable measures in a wide range of administrative fields for each local government**
- **Creation of a favorable environment for local governments to promote activities conducted from the viewpoint of information security**

○Promotion of rational and voluntary information security measures by local governments, including small ones, and promotion of cooperation between local governments

The government will promote the application of desired information security measures in all local governments including small local governments. Specifically, the government will promote the risk analysis of information assets which are subject to measures and audit, examination of information security policy development, review of guidelines in preparation for an audit, and spread of the guidelines to contribute towards development of a business continuity plan11. With regard to human resources, a joint workshop and local seminars should be organized to improve the ability of the staff that is in charge of these measures.

In addition, the government will support efforts to introduce best practices to local governments nationwide and demonstrate model cases for them. Moreover, it will hold study group meetings to improve awareness and understanding among local government chiefs.

○ Strengthening of entities supporting local governments in implementation of measures

In order to promote the implementation of security measures by local governments, it is effective to strengthen entities that support local governments. Therefore, while developing a system for cooperation between all organizations possessing knowledge useful for information security by holding joint workshops involving the public and private sectors as well as NPOs, the government will reinforce the system for supporting local governments using portal web sites within the LGWAN (Local Government Wide Area Network).

○Development of a favorable environment for the training of information security personnel at local governments

For the training of local government personnel capable of implementing information security measures, promotions of such training by local governments are effective. Therefore, the government will develop a favorable environment for local governments to conduct such promotion activity. Specifically, the government will compile and provide reference materials which can be used in seminars so as to encourage local governments to hold educational seminars on information security. Also, the government will promote the training of tutors in order to enhance human resource development.

Measures related to critical infrastructure under the Second National Strategy on Information Security

Measures Taken under the First National Strategy: Promotion of activities to minimize IT malfunctions to almost zero.

→The government steadily promoted such measures as the development of safety standards, enhancement of information-sharing systems and cross-sectoral training. Meanwhile, new services that were not covered by the First Action Plan have been started and expanded in line with society’s increasing dependence on IT. There have been IT system malfunctions that could significantly affect the people’ s lives and socio-economic activities, including with regard to systems to which the safety standards are not applicable.

Under the Second National Strategy

•Protection of critical infrastructure to prevent significant effects on the people’s lives and socio-economic activities
•Assurance of the availability of the services provided by infrastructure operators and the implementation of quick restoration work in the event of an IT system malfunction.

○**Development and promotion of safety standards** (The government will review and revise the guideline that was formulated under the First Action Plan, including the addition of supplementary provisions concerning business continuity. It will also promote the improvement of the safety standards with due consideration of consistency with the PDCA cycle of the operators of critical infrastructures.)

○**Enhancement of the information-sharing system** (The government will organize information shared among relevant organizations, including CEPTOARs and the CEPTOAR-Council, and create an environment necessary for providing and communicating information.)

○**Analysis of common threats** (The government will identify and analyze threats common to various sectors, including the interdependence between different critical infrastructure areas.)

○**Cross-sectoral exercises** (In order to enhance the protection of critical infrastructures, the government will identify challenges by conducting cross-sectoral exercises based on scenarios assuming specific system malfunctions.

○**Adaptation to environmental changes** (In order to swiftly adjust information security measures according to changes in social and technological environments, efforts will be made to improve the capability of detecting such changes.

Measures related to Enterprises under the Second National Strategy on Information Security

Measures taken under the First National Strategy: Improvement of the implementation of information security measures to the world’s highest level

→The number of companies certified for ISMS has been increasing year after year, with Japanese companies accounting for nearly 60% of all ISMS-certified companies around the world. However, ISMS-certified Japanese companies are not necessarily promoting security as a management strategy. Moreover, the information security gap between large companies and small and medium-size enterprises (SMEs) is widening. Information security has become important for the outsourcing of operations to foreign contractors and international business transactions.

Under the Second National Strategy

- **Widespread recognition of information security governance as part of corporate management**
- **Promotion of emergency response system and ensuring business continuity**
- **Promotion of measures related to SMEs and international measures**

○**Establishment of information security governance as part of management** (The government will promote the spread, development and improvement of the ISMS, benchmarking tools, etc., and sort out relevant laws and regulations.)

○**Assurance of business continuity and enhancement of the emergency response system** (The government will promote the development of business continuity plans through the spread of relevant guidelines and reinforce the emergency response system.)

○**Promotion of information security measures at SMEs** (The government will develop a favorable environment for SMEs to easily select appropriate measures. It will also promote the use of SaaS and ASP.)

○**Promotion of policies to support global business expansion of Japanese enterprises** (Efforts will be made to establish information security at overseas business bases of Japanese enterprises.)

Measures related to Individuals under the Second National Strategy on Information Security

NISC

Measures Taken under the First National Strategy:" Minimizing the number of individuals who have concerns about using IT to almost zero."

→There are still many individuals who have concerns about using the Internet.

Under the Second National Strategy

•Continued implementation of measures to realize a society in which individuals feel secure about IT use

•Implementation of measures to encourage entities that entrust information to consider information security issues proactively.

○ Enhancement and promotion of education of individuals about information security

The government will promote education/enlightenment activities for children, students and guardians who are actively using IT but who may not necessarily be adequately aware of the risks involved or may not recognize the importance of information security measures. Therefore, education on information ethics* will be promoted in schools and local communities.

In addition, the government will develop an environment that enables individuals, as consumers, to recognize the risks that could arise from the use of various services so as to avoid suffering damage from the risks. In addition to the enlightenment activities for individuals, the government will promote the appropriate provision of information related to risks and security measures by service providers and organizations assisting the implementation of measures as well as their efforts to handle IT system malfunctions.

○Effective awareness-promotion and enlightenment activities intended to raise individuals' security level

The government will promote awareness-promotion and enlightenment activities intended to raise individuals' security level through cooperation between relevant government agencies in order to implement security measures more effectively. Also, in order to effectively increase the security level of general users, including individuals who are not necessarily well-versed in IT, the government will promote both the training of "supporters," who can provide appropriate advice and deal with inquiries, and the establishment of local organization networks.

※Information moral is the "attitude and way of thinking that constitute the basis of appropriate conduct in an information society" (High School Curriculum Guidelines, Information Edition).

Measures related to Promotion of Technology Strategy under the Second National Strategy on Information Security

NISC

Measures taken under the First National Strategy:
Implementation of ①establishment of an effective development system, ②prioritization of technology development and improvement of the technology development environment and ③promotion of “Grand Challenge” development projects, with the pursuit of advanced technology as a basic policy

→Further promotion is necessary with regard to ① and ③. In addition, there are new challenges that have accompanied social changes (increasing dependence on IT, changes in the social structure and the emergence of new threats)

Under the Second National Strategy

- **Aiming to make Japan’s research and development the most effective and efficient in the world.**

(Provision of terminals and information appliances that do not require users to take information security measures, widespread dissemination of development techniques that incorporate security features in the designing stage and the standardization of the risk description and evaluation methods)

○ Prioritization of information security technology development projects and the maintenance of diversities

The government will place priority on the development of safe and secure equipment and a user environment that do not impose an excessive burden on users in terms of implementing security measures.

On the other hand, in order to ensure diversity in research and technical development, the government will be actively involved in fields and activities that should be promoted as a national strategy, including fields neglected by enterprises due to a lack of market growth and pioneering development activity intended to deal with risks that could arise in the future.

○Promotion of “grand challenge type” research and development and technology development

○Development of systems and infrastructures for efficient implementation of research and technology development

In addition to promoting the incorporation of the procedures for using the results obtained midway through projects into development plans, the government will promote the public disclosure of the contents and implementation status of projects.

A flexible project management mechanism that allows changes to plans where necessary will be introduced. Moreover, the government will support and speed up R&D activities based on the standardization of the risk description and evaluation methods, the development and sharing of a database related to information security, and the setting up of a separate workbench.

Measures related to Development and Retention of Human Resources under the Second National Strategy on Information Security

NISC

Measures taken under the First National Strategy
“Development of practitioners and experts with multi-faceted and comprehensive capabilities “Organization of the qualification systems concerning information security”

→As it takes much time before visible results are achieved in human resource development, the results have not yet become clear.
→Meanwhile, there are needs for measures to develop human resources and needs for a mechanism for clarifying the skills possessed by workers in relation to business processes.

Under the Second National Strategy

- **Continued implementation of measures to develop human resources through the use of public-private frameworks, qualification tests, etc.**
- **Establishment of a mechanism for clarifying the skills**

○ Development and retention of information security-related human resources at enterprises

It is essential to foster and retain personnel capable of flexibly adapting to changes in the surrounding environment, such as new IT services, and those capable of making decisions from the broad perspective of overall corporate management. In this case, it is also important to take into consideration the career path that the trained information security personnel aim for. Therefore, the government will promote the development of a common career skill framework that ensures consistency between the standards for various skills as an objective human resource assessment mechanism through the joint efforts of the public and private sectors. It will also promote the use of the Information-Technology Engineers Examination, and frameworks and qualification tests concerning human resource development in private sectors that comply with the above-mentioned common career skill framework.

The government will make efforts to develop and retain human resources capable of playing the central role in corporate information security by developing an information security-related model career development plan for engineers and by supporting the experts’ community.

○Promotion of visualization of skills possessed by information security personnel

In addition to clarifying the skills required in actual jobs, the government will implement policy measures to make it easy for outsiders to understand the skills possessed by information security personnel. Among such measures are creating a mechanism for clarifying the relationship between the information security qualification system/education system and the skills required by actual jobs and the career path sought by information security personnel as well as using the Common Career/Skill Framework:ITSS20 and various effective frameworks for human resource development in the private sector in order to enable outsiders to understand the skills possessed by such personnel.

Measures related to Promotion of International Cooperation and Collaboration under the Second National Strategy on Information Security

Measures taken under the First National Strategy:
“Aim to establish the POC (Point of Contact) with foreign organizations related to information security and share information periodically and to ensure, through international cooperation, that Japan’s best practices are adopted by other countries.

→Although recognition has grown, it is necessary to promote international partnership and cooperation based on more concrete measures.

Under the Second National Strategy

- Aiming to ensure that Japan’s information security-related efforts centering on public- private partnership contribute to the world as the world’s most advanced best practices. (Implementation of policies in coordination with other countries so as to ensure organic linkage between efforts made in Japan and abroad, the exercise of the initiative in efforts made in Asia and contribution to the fostering of information security culture at the global level.)

○ Enhancement of POC functions and promotion of information sharing within Japan based on appropriate rules

○ Establishment of public-private partnership with relevant organizations to grasp the global trend of threats

○Collection of knowledge and wisdom (development of experts and researchers) and improvement of information security in Asia

○ Assurance of information security adapted to the globalization of economic activities

○Realization of strategic contributions by Japan to the international community, including those made through standardization-related efforts

Measures related to Crime Control and Protection and Redemption of Rights and Interests under the Second National Strategy on Information Security

Measures taken under the First National Strategy: Japan aimed to promote the development of infrastructure for crime control and protection and redemption of rights and interests (improvement of the crime control capability, improvement of necessary equipment, enhancement of international cooperation, establishment of legislation for the conclusion of the U.N. Convention against Transnational Organized Crime and investigation and research concerning the protection and redemption of rights and interests).

→Although the development of the infrastructure made some progress, the number of cyber crimes is increasing and the crime techniques are becoming more and more sophisticated and diverse. As cyber attacks on the websites of foreign governments have been reported, it is necessary to further strengthen the infrastructure.

Under the Second National Strategy

- Aiming to enable safe and secure use of cyberspace (further strengthening crime control, conducting effective PR activities and promoting the development of the infrastructure for protection and redemption of rights and interests)

○ **Promotion of the development of infrastructure for crime control** (The government will further promote the enhancement of the crime control system and capability of the law enforcement institutions, public-private cooperation to arrest suspects and limit the extent of crime damage and preparations against cyber terrorism.)

○ **Promotion of PR and enlightenment for the deterrence of crime**
(The government will further promote the provision of specific information so as to prevent the people from becoming victims of cyber crime.)

○ **Promotion of the development of infrastructure for protection and redemption of rights and interests** (The government will promote the disclosure of information concerning efforts for the protection and redemption of entrusted information by entities to which information is entrusted, It will also promote the development and dissemination of technologies that improve the safety and reliability of cyberspace.)