



Japanese Government's Efforts to Address Information Security Issues

- Focusing on the Cabinet Secretariat's Efforts -

November, 2007

<http://www.nisc.go.jp/eng/>



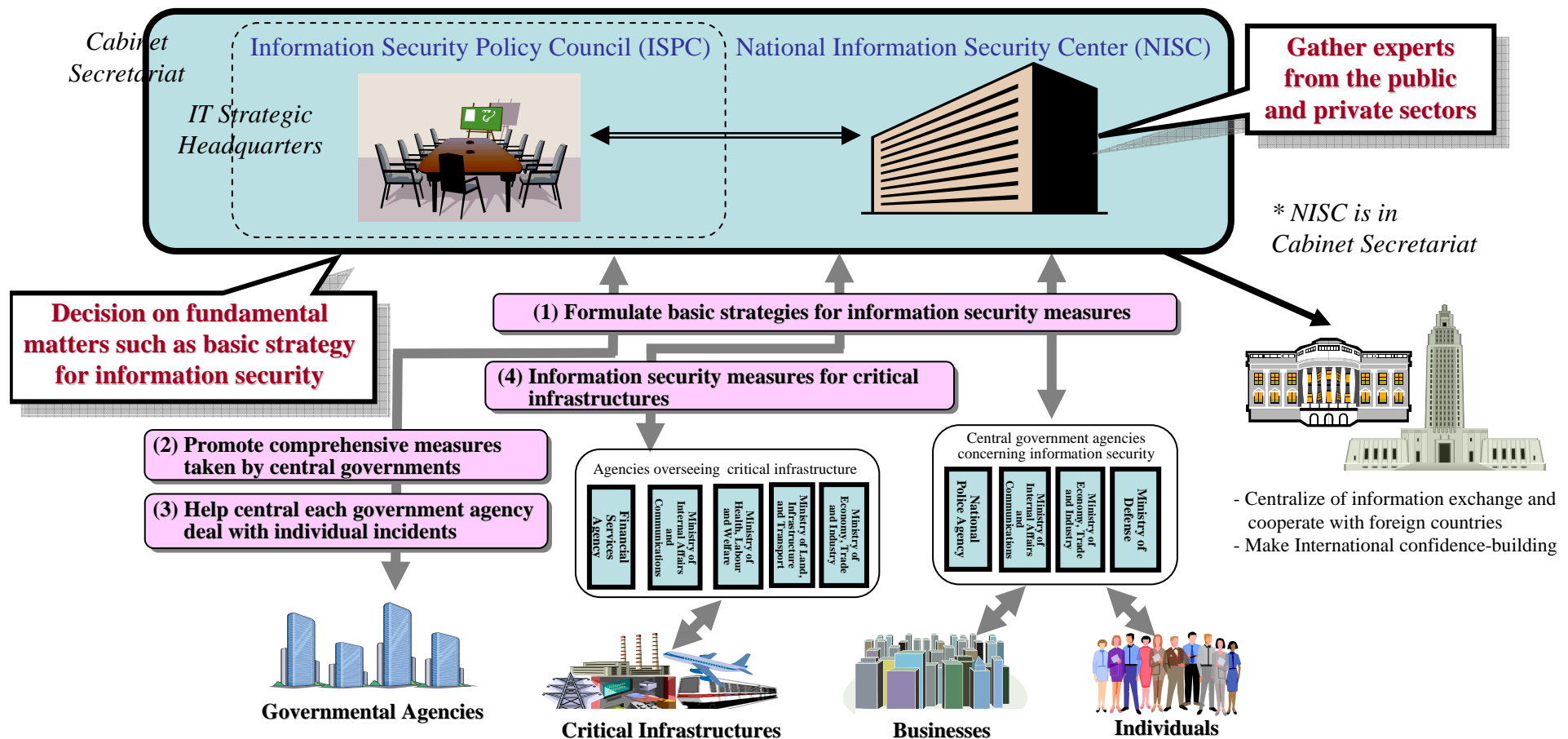
1. Structuring Governmental Core Function

Information Security Policy Council (ISPC) & National Information Security Center (NISC)

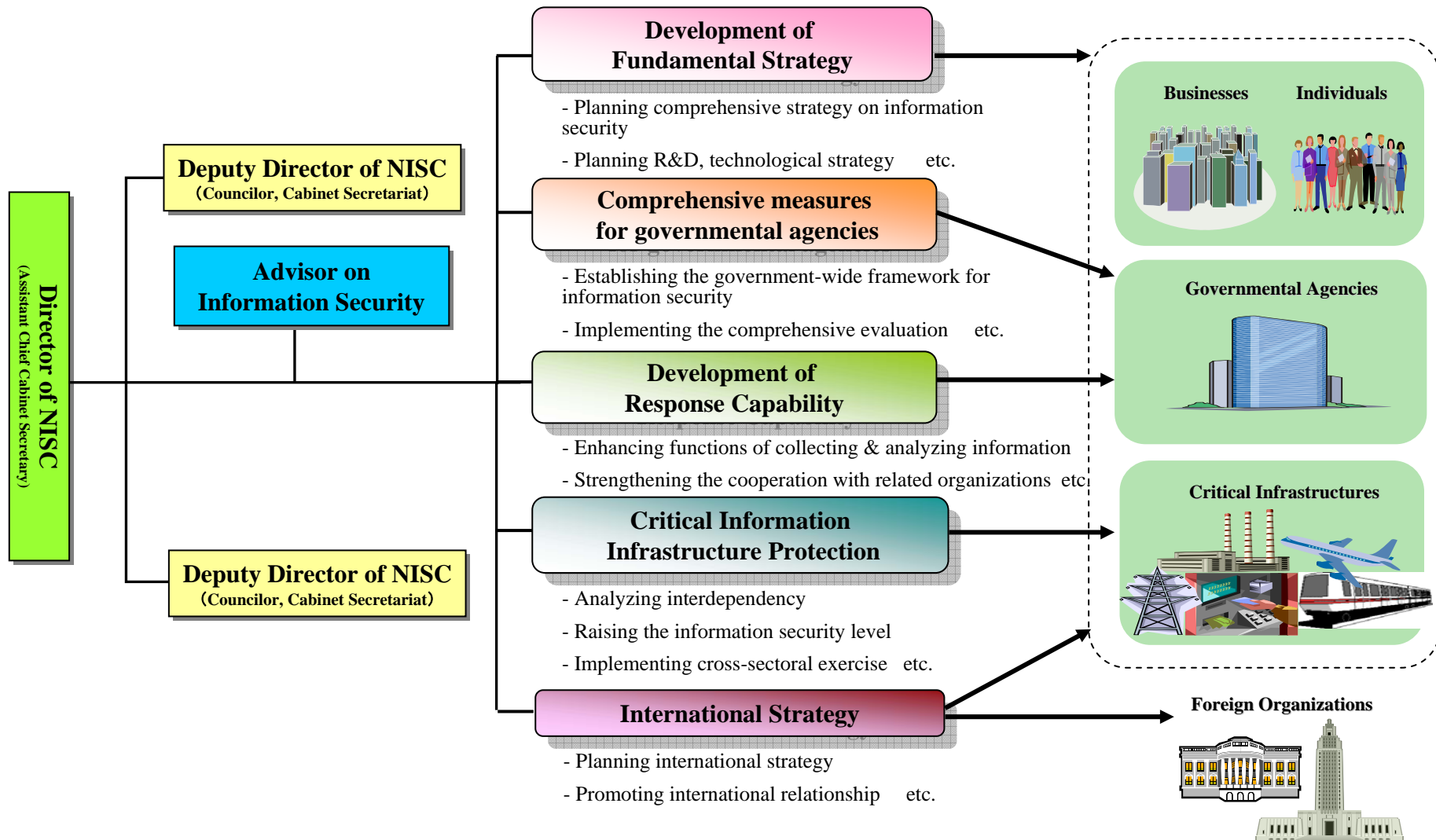
- Based on “Review of the Role and Functions of the Government in terms of Measures to Address Information Security Issues (decided by the IT Strategic Headquarters on December 7, 2004),” the government is developing essential functions and frameworks toward strengthening its core functions to address information security issues.

➤ National Information Security Center (NISC) has been established since April 25, 2005

➤ Information Security Policy Council (ISPC) has been established under the IT Strategic Headquarters since May 30, 2005



Structure and Functions of NISC





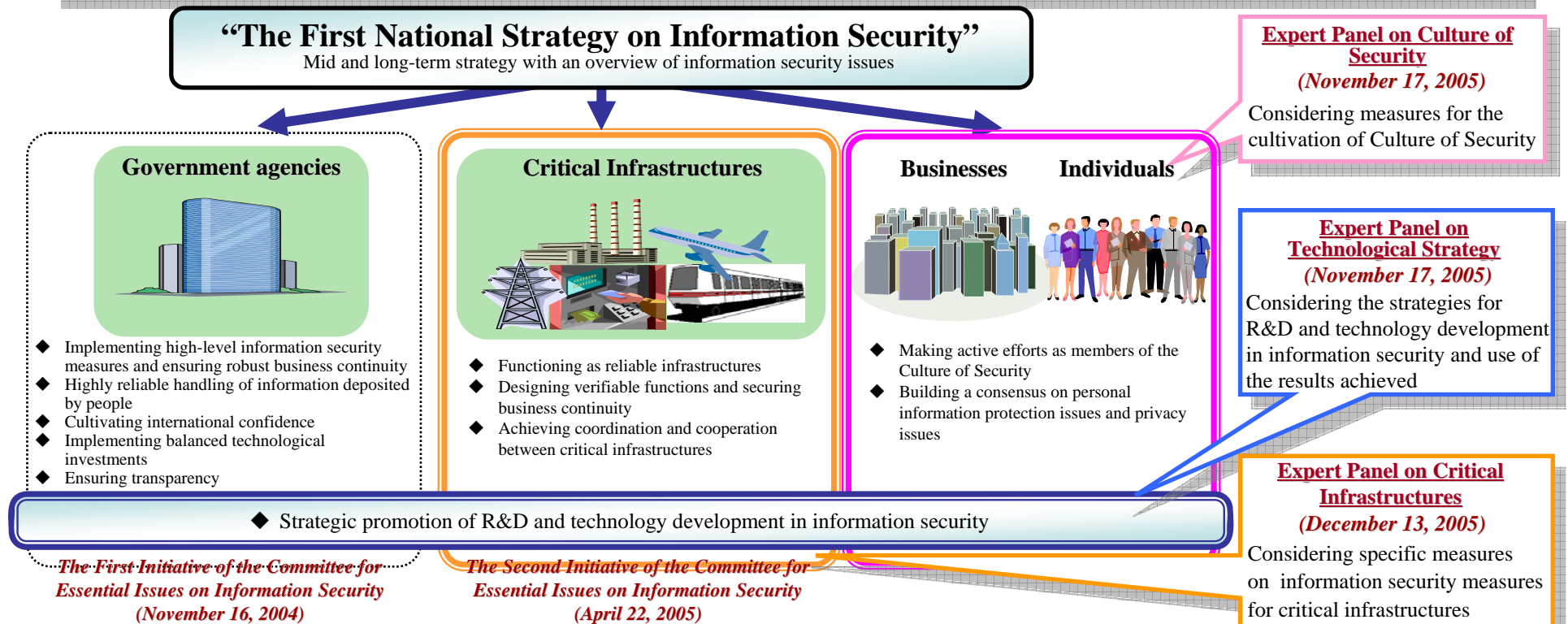
2. National Strategy and Secure Japan



2-1 First National Strategy on Information Security

Consideration for “The First National Strategy on Information Security”

- The Information Security Policy Council formulated “The First National Strategy on Information Security” as the mid and long-term strategy with an overview of information security issues.
- The following three expert panels were established to contribute to the deliberations on “The First National Strategy on Information Security.”
 - Considering measures for the cultivation of Culture of Security ➡ **Expert Panel on Culture of Security**
 - Considering the strategies for R&D and technology development in information security and use of the results achieved thereby ➡ **Expert Panel on Technological Strategy**
 - Considering specific policies on information security measures for critical infrastructures ➡ **Expert Panel on Critical Infrastructures**



Overall Picture of “The First National Strategy on Information Security”

- Aiming to Make Japan an Information Security Advanced Nation
through Establishment of a New Public-Private Partnership Model -

- As a **mid and long-term plan (“overall process schedule”)** on information security issues, the government presented (1) **basic principles** against information security issues and (2) the **direction of priority policies**.
- **The term for this plan is three years from FY2006 to FY2008.** The government also formulates a promotion plan for each fiscal year based on the medium and long-term plan.

Basic principles

- 1 Information security for providing the introduction of Japan as an economic state
- 2 Information security for more safe, secure, and better lives for the people
- 3 Information security from a new perspective of ensuring national security

<Points to be realized>

- ◆ A quarter of Japan’s economic base and commercial transactions depends on IT.
- ◆ Japan is the world’s largest broadband communication power with 80 million Internet users.
- ◆ There is a growing need for safety and security measures including disaster control manners.
- ◆ It is necessary to recognize both new threats to national security regarding IT and strength of Japan.

Primary goal to be achieved in the next three years

Establish a **“new public-private partnership model”** in which both public and private play their roles appropriately

- Under the initiative of the National Information Security Center (NISC), all entities concerned should be involved in this project -

Goals

To make Japan an **“information security advanced nation”**

[Central governments]: All government agencies should take measures according to the “Standards for Measures.”

[Businesses]: All public companies should take appropriate measures depending on risk.

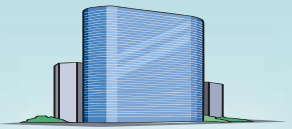



[Critical infrastructures]: The number of IT-malfunctions should be reduced as close as possible to zero.

[Individuals]: The number of “individuals who feel insecure about IT use” as close as possible to zero.

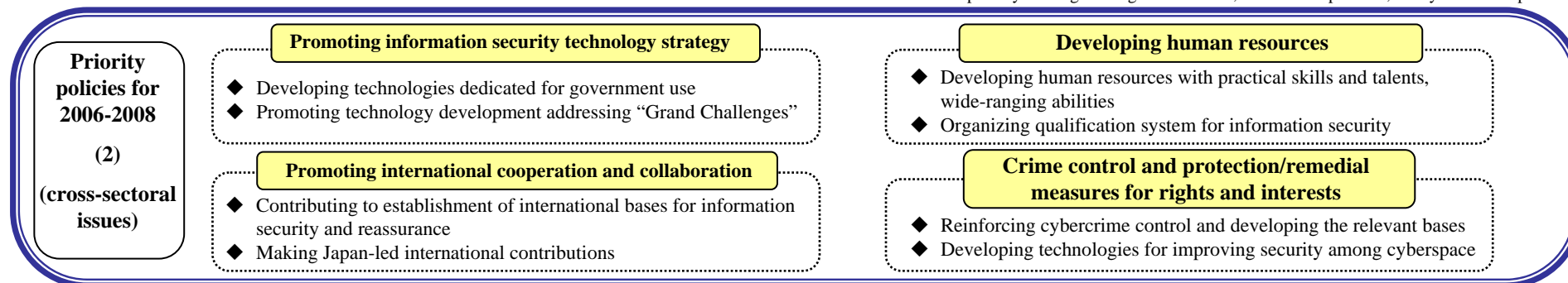
“The First National Strategy on Information Security”

- Priority Policies for the FY 2006-2008 -

- In the next three years, the government will strengthen various relevant measures based on the First National Strategy on Information Security **in order to establish a “new public-private partnership model”** in which all entities appropriately play their roles.

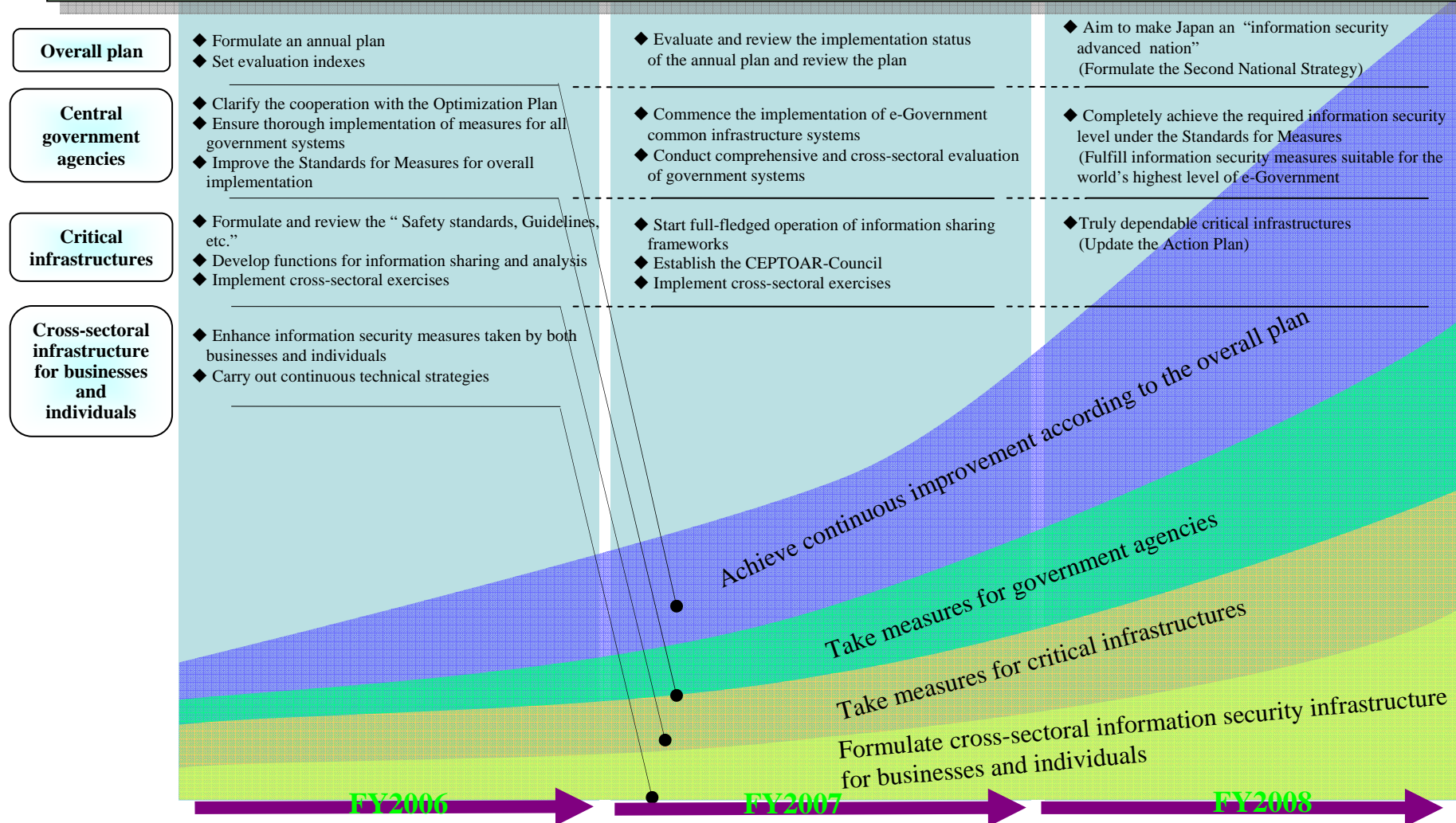
| |  Central and local governments |  Critical infrastructures |  Businesses |  Individuals |
|---|---|--|---|--|
| Role | Giving “Best Practice” for information security measures | Ensuring stable supply of their services as the basis of people’s social lives and economic activities | Implementing information security measures so as to be highly regarded by the market | Raising awareness as main players of IT society |
| Priority policies for 2006-2008 (1) (for each player) | <ul style="list-style-type: none"> ◆ Evaluating each ministry and agency based on the Standards for Measures ◆ Increasing the ability to respond to emergencies including cyber attacks | <ul style="list-style-type: none"> ◆ Developing CEPTOAR* ◆ Establishing the CEPTOAR-Council ◆ Implementing cross-sectoral exercises and analysis of interdependency | <ul style="list-style-type: none"> ◆ Promoting usage of third-party evaluation systems such as information security audit ◆ Reinforcing the framework to respond to threats regarding information security including computer viruses | <ul style="list-style-type: none"> ◆ Promoting information security education ◆ Enhancing publicity and awareness-raising by, for example, establishing an “Information Security Day” ◆ Improving the environment to provide user-friendly services |
| [Sectoral Plan] | Standards for Measures | Critical Infrastructures Action Plan | Measures promoted by Ministries and Agencies | Measures promoted by Ministries and Agencies |

* CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response



Overall Picture of Milestones in the FY 2006 - 2008

- Through combination of the “**overall process schedule**” (National Strategy) and the “**sectoral plan**,” the government aims to **develop Japan into an “information security advanced nation,”** with clearly identified milestones to be achieved in each fiscal year.



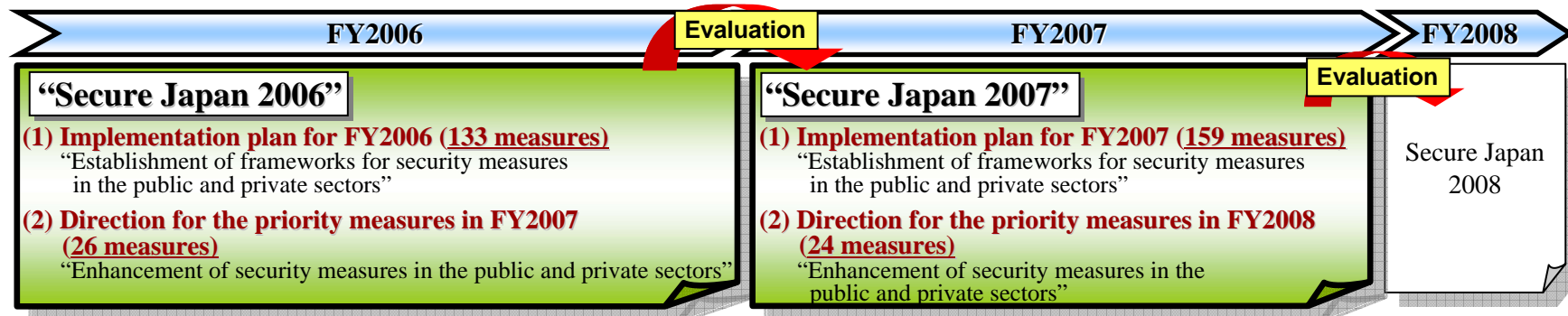
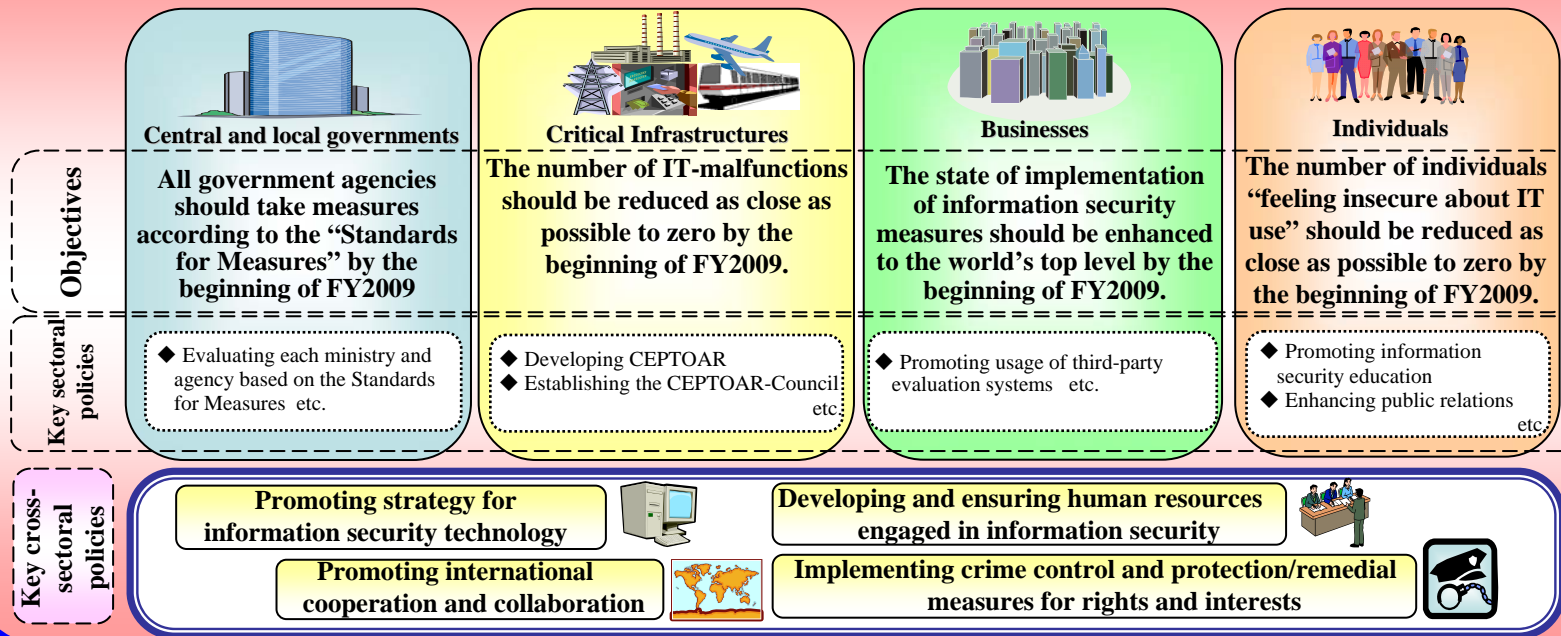


2-2 Secure Japan 2007

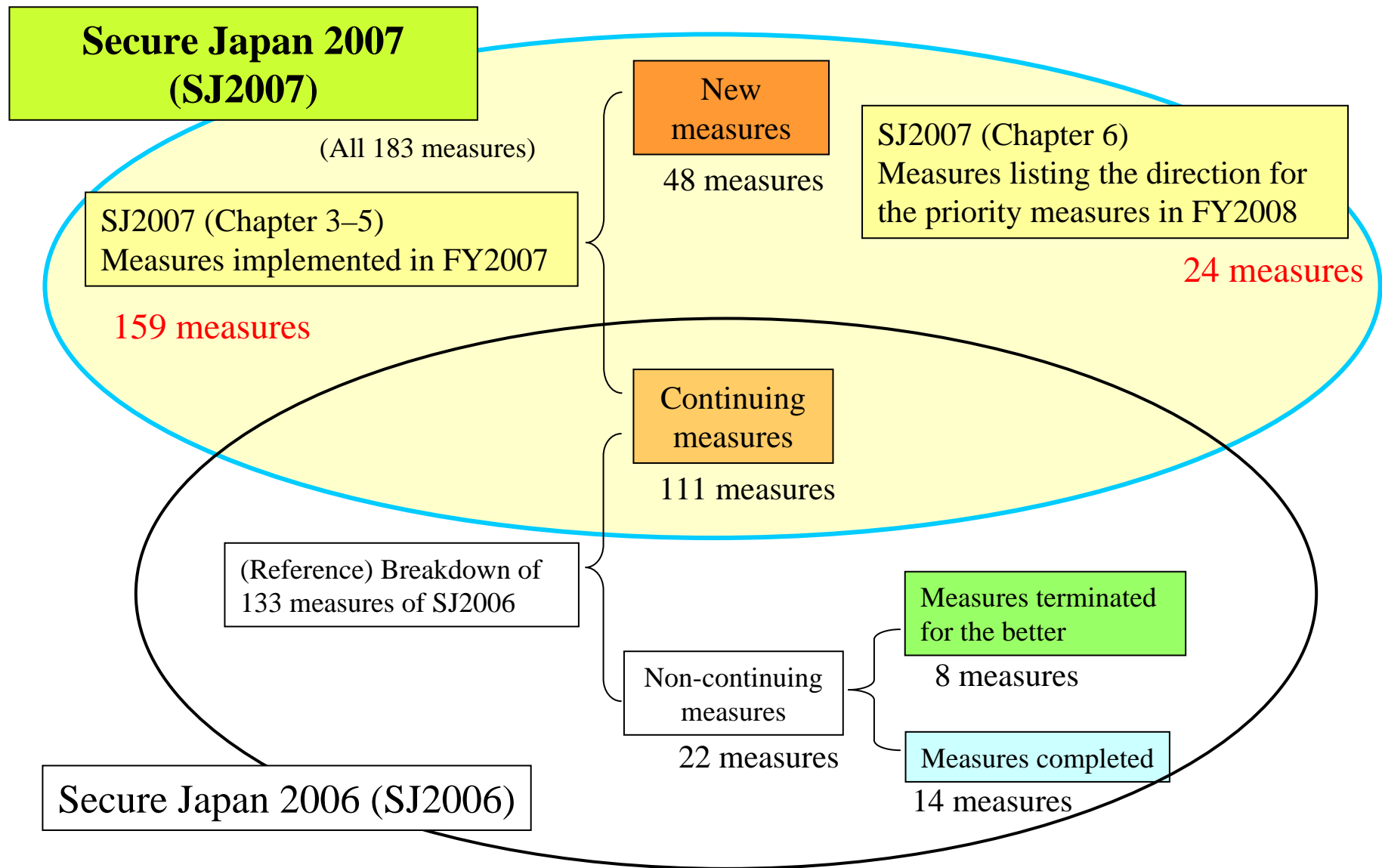
Outline of “The First National Strategy on Information Security” and position of “Secure Japan 2007”

“The First National Strategy on Information Security” (Information Security Policy Council, February 2, 2006)

Three-year program for FY2006-2008. Aimed at establishing a “new public-private partnership model” where all entities share appropriate roles.



Breakdown of Measures Listed in Secure Japan 2007



Key Points of “Secure Japan 2007”

- In light of the assessment and analysis of approaches based on Secure Japan 2006, efforts to be made in the second year are to be summarized to implement the First National Strategy on Information Security.
- Facilitating constant implementation of measures, including maintenance of the organization that enforce security measures and application of the supplementary measures to the component to which measures are insufficiently employed.
- Indicates specific action plan to be implemented in FY2007, and the direction for the priority measures in FY2008.

<Key points of “Secure Japan 2007” >

<Enhancing the efforts to implement the basic plan>

- Efforts to be made in the second year (including enhancement of efforts) to implement the First National Strategy on Information (FY2006–FY2008)

Priorities

<Direction of efforts based on the awareness and assessment of progress made by the end of FY2006>

- Extension of the effort for a thorough and solid implementation of measures within government agencies
- Enhancement of measures for implementing bodies that tend to lag behind in making efforts
- Strengthening the system and personnel to reinforce the component to which insufficient efforts were made in FY2006
- Starting a full-scale response to international issues, in light of deepening mutual dependency of each country in the international community
- As an urgent issue, promotion of efforts to enhance information security of e-government in a rapid and intensive manner

Direction
of
Efforts

Enhancement of information security measures for the central government agencies

[Primary Specific Measures]

- Establishment of the PDCA cycle and conducting a full-fledged assessment of the progress of implemented measures based on the Government Standards for Measures, and disclosure of the assessment results
- Establishment of the Government Security Operation Coordination (GSOC) concerning cyber attacks, etc. headed by the Cabinet Secretariat

Dissemination of measures for the bodies that are lagging behind in taking measures, as well as for the general public

[Primary Specific Measures]

- Providing information security education in elementary and junior- and senior-high schools
- Providing awareness-raising activities including “Internet safety lessons”
- Promoting implementation of information security measures in small- and medium-sized enterprises
- Consideration of the establishment of the CEPTOAR-Council, a cross-sector council for critical infrastructures

Intensive efforts toward strengthening the information security Platform

[Primary Specific Measures]

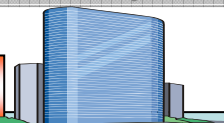
- Prioritization in securing manpower for information security in government agencies
- Intensive efforts towards global deployment of information security measures
- Security assurance at the stage of system design of e-government

➡ Direction of Priority Measures in FY2008.

Specific Measures under “Secure Japan 2007” (1)

Strengthening Information Security Measures in the Four Implementation Fields

1. Central and local governments



17 newly introduced measures + 31 continuous measures = 48 total measures

[Objectives] The central government will make efforts aiming to upgrade the level of the Standards for Measures to the world's highest level by fiscal 2008, and to enable all the government agencies to implement measures at a level meeting the Standards for Measures by the beginning of FY2009.

- [Primary measures]**
- Establishing the PDCA cycle based on the “Standards for Measures” and conducting full-scale evaluation of the measures and publicizing the evaluation results (Cabinet Secretariat and all government agencies)
 - Cooperatively tackling to issues common for all government agencies and sharing best practices appropriately (Cabinet Secretariat and all government agencies)
 - Developing a next-generation OS environment that achieves higher security (Cabinet Secretariat, Cabinet Office, Ministry of Internal Affairs and Communications (MIC) and Ministry of Economy, Trade and Industry (METI))
 - Establishing inter-governmental response system concerning cyber attacks against government agencies (Cabinet Secretariat and all government agencies)
 - Developing manuals for information security measures in local governments (MIC)

2. Critical Infrastructures



3 newly introduced measures + 11 continuous measures = 14 total measures

[Objectives] The central government will make efforts aiming to reduce IT-malfunctions in critical infrastructures as close as possible to zero by the beginning of FY2009

- [Primary measures]**
- Reviewing the “Safety Standards, Guidelines, etc.” for securing information security in each critical infrastructure sector. (Agencies overseeing critical infrastructure)
 - Examination on the state of dissemination of the “Safety Standards, Guidelines, etc.” (Cabinet Secretariat and all government agencies)
 - Consideration to establishing “CEPTOAR-Council (tentative)” to facilitate information sharing across business entities engaged in critical infrastructures (Cabinet Secretariat and Agencies overseeing critical infrastructure)
 - Conducting cross-sectoral functional exercises to improve capability of the structure for communication and cooperation between public and private sectors. (Cabinet Secretariat and Agencies overseeing critical infrastructure)
 - Facilitating interdependency analysis for critical infrastructure sectors to improve capability to respond to IT- malfunctions and to ensure business continuity. (Cabinet Secretariat and Agencies overseeing critical infrastructure)

Specific Measures under “Secure Japan 2007” (2)

Strengthening Information Security Measures in the Four Implementation Fields (continued)

3. Businesses



11 newly introduced measures + 12 continuous measures = 23 total measures

[Objectives] The government will make efforts aiming to improving the implementation of information security measures of businesses to the world's highest level by the beginning of FY2009.

[Primary measures]

- Promoting the establishment of information security governance in private sectors (METI)
- Facilitating implementation of information security measures within small- and medium-sized companies (METI)
- Considering the quantitative evaluation method for information security-related risks (METI)
- Support for training businesses developing human resources specialize in security for information and communication (MIC)

4. Individuals



2 newly introduced measures + 16 continuous measures = 18 total measures

[Objectives] The government will make efforts aiming to reduce the number of individuals who feel insecure about IT use as close as possible to zero by the beginning of FY2009.

[Primary measures]

- Promoting information security education in elementary and lower secondary school levels (Ministry of Education, Culture, Sports, Science and Technology (MEXT))
- Increasing and improving the content of “Internet safety lessons” and continuously holding the lessons nationwide (METI and National Police Agency (NPA))
- Implementing awareness-raising lessons for parents and teachers (e-Net-Caravan) nationwide (MIC and MEXT)
- Holding events centered on “Information Security Day” (Cabinet Secretariat, NPA, MIC, MEXT and METI)
- Giving lecture on cyber security (cyber security college) nationwide intended for the persons concerned with educational institute and employees of local government (NPA)

Specific Measures under “Secure Japan 2007” (3)

| | | |
|---|--|--|
| Formation of Cross-Sectoral Information Security Infrastructure | 1. Promoting information security technology strategy  | 11 newly introduced measures + 12 continuous measures = 23 total measures |
| | [Primary measures] <ul style="list-style-type: none"> - Considering the themes for “Grand Challenge” research projects aimed at achieving long-term and fundamental technological innovations (Cabinet Secretariat, Cabinet Office, MIC and METI) - Development of next generation OS environment that realize the advanced security functions (Cabinet Secretariat and Cabinet Office) | |
| | 2. Development and securing of human resources engaged in information security  | 6 newly introduced measures + 2 continuous measures = 8 total measures |
| | [Primary measures] <ul style="list-style-type: none"> - Facilitating unified information security education in the government (Cabinet Secretariat and all government agencies) - Setting up the council for industry-academia-government collaboration to conduct deliberations on the type of advanced IT human resources needed in the industry and the methods of developing advanced IT human resources in the practical field (Ministry of Economy, Trade and Industry) | |
| | 3. Promoting international cooperation and collaboration  | 4 newly introduced measures + 7 continuous measures = 11 total measures |
| | [Primary measures] <ul style="list-style-type: none"> - Consideration of basic policy and specific measure to strategically tackle with international partnership/cooperation throughout government agencies (Cabinet Secretariat) - Internationally publicizing and spreading best practices (Cabinet Secretariat and all government agencies) | |
| | 4. Crime control and protection/remedial measures for rights and interests  | 3 newly introduced measures + 9 continuous measures = 12 total measures |
| | [Primary measures] <ul style="list-style-type: none"> - Promotion of collection and systematization of knowledge on digital forensics (NPA) - Research on foundation for protection and redemption of user's rights and benefit in cyberspace (Cabinet Secretariat) | |
| Policy Promotion System | 1. Policy Promotion System and Partnerships with Other Related Organizations | 3 newly introduced measures + 3 continuous measures = 6 total measures |
| | [Primary measures] <ul style="list-style-type: none"> - The competent agency will also expand the functions to conduct examination/consideration for various trends of basic information necessary for promoting information security measures (Cabinet Secretariat) - Improvement of information security consulting functions to promote information security measures of government agencies (Cabinet Secretariat) - Intensify the exchange of opinions with other related organizations, such as the IT Strategic Headquarters, Council on Economic and Fiscal Policy, Council for Science and Technology Policy, and Central Disaster Prevention Council . (Cabinet Secretariat and Cabinet Office) | |
| | 2. Establishment of the Structure for Continuous Improvement | 0 newly introduced measures + 5 continuous measures = 5 total measures |
| | [Primary measures] <ul style="list-style-type: none"> - Conducting evaluation of “Secure Japan 2007” and publishing the results (Cabinet Secretariat) - Considering the milestones (schedule of regular evaluation and evaluation item) toward strengthening the information security measures of government agencies (Cabinet Secretariat) - Facilitating use of evaluation criteria for information security measures and consideration for improvement of the criteria (Cabinet Secretariat, MIC and METI) | |

Specific Measures under “Secure Japan 2007” (4)

- Direction of the Measures to be implemented in FY2008 -

- Based on the improvement of the information security measures implemented in FY2007, in order to facilitate intensive activity toward FY2008, “Secure Japan 2007” identifies the direction of the measures to be implemented in FY2008, with priority on **“intensive activity to strengthen the information security foundation.”**

FY2008 : Intensive activity to strengthen the information security foundation

Intensive efforts for developing and ensuring human resources engaged in information security

- Establishing cross sectoral system that support human resource development and supporting comprehensive development and ensuring of human resource
- Program that facilitate development of advanced IT specialist
- Ensuring human resources engaged in information security within government agency with high priority

10 measures

Intensive approaches for global diffusion of information security policy

- Enhancement of function of the NISC as a point of contact
- Promoting Global Strategy to be developed in 2007.
- Strengthen capability of CSIRT and relevant organizations for global response, and advancement of information coordination

9 measures

comprehensive approaches to improving security of electoronic government

- Enhancement of measures to ensure information security of E-Government from the stages of planning and design (Security by design)
- Promotion of verification of information risks associated with E-Government and promotion of unification of verification methods
- Steady operations of GSOC and strengthening of analysis functions

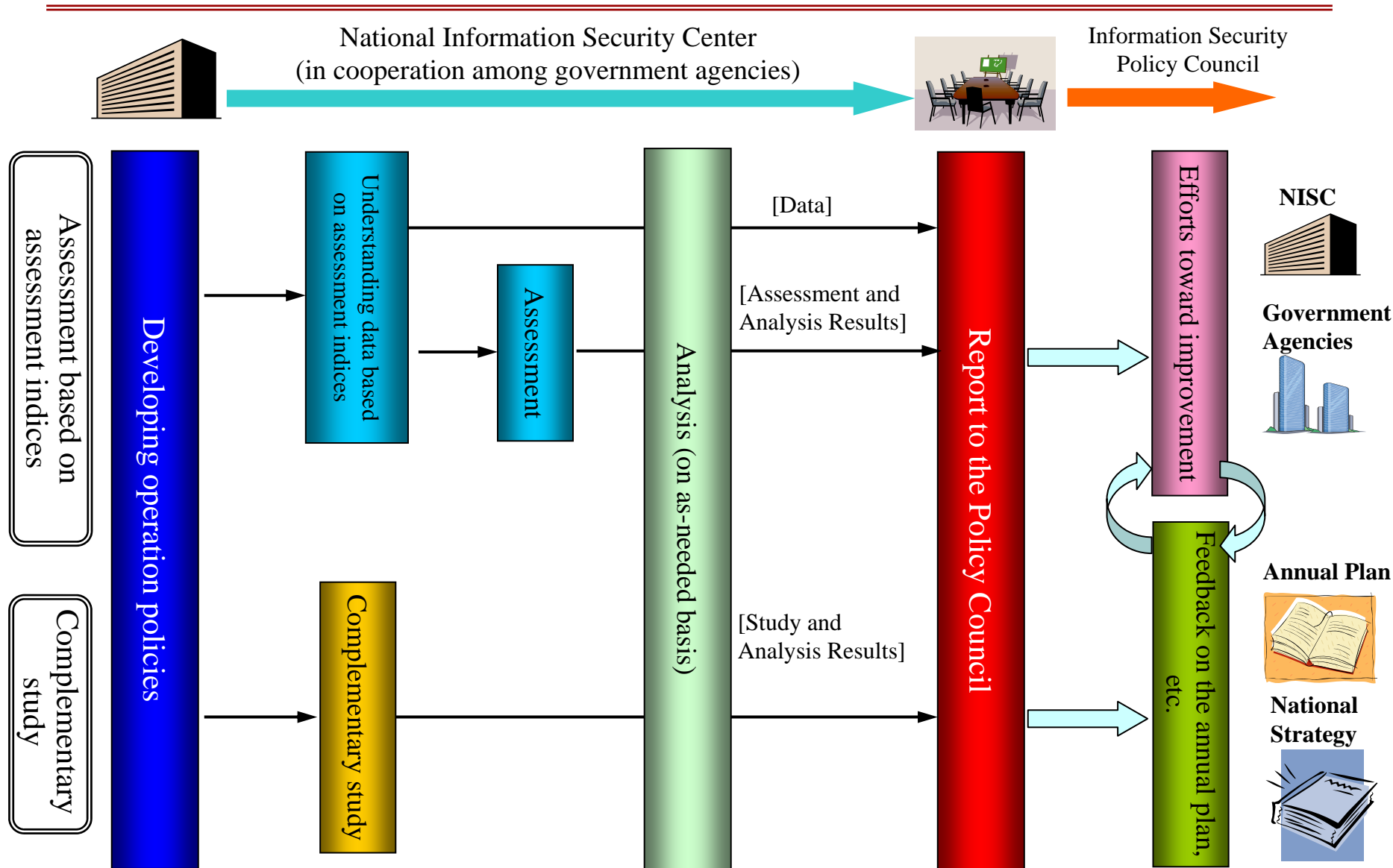
5 measures

Efforts in FY2008 (the final year of the First National Strategy)

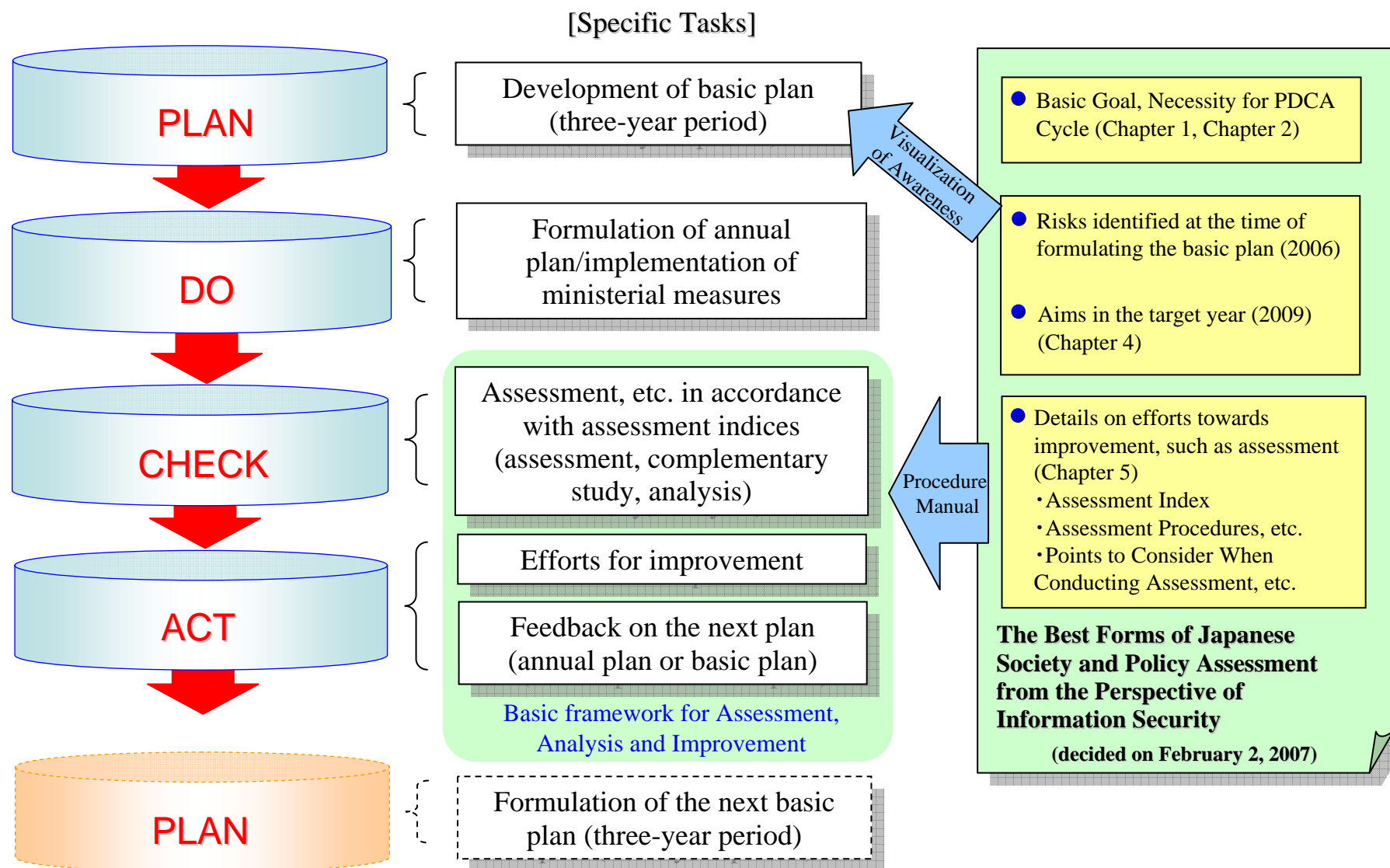


2-3 Framework for Assessment and Improvement of Information Security Measures

Basic Framework for Assessment and Analysis based on Assessment Indices



PDCA cycle for Information Security Measures





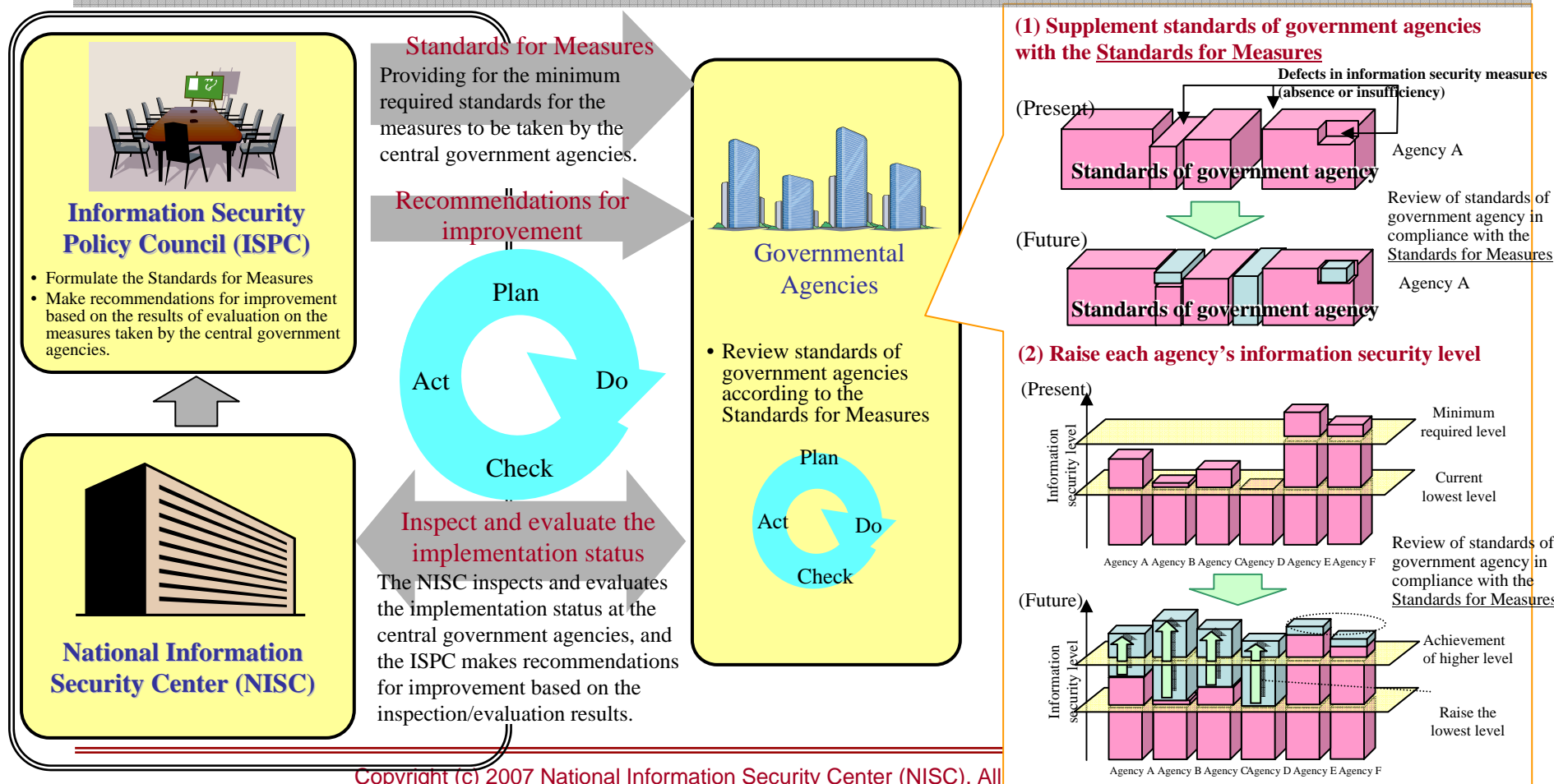
3. Efforts made based on Secure Japan 2007



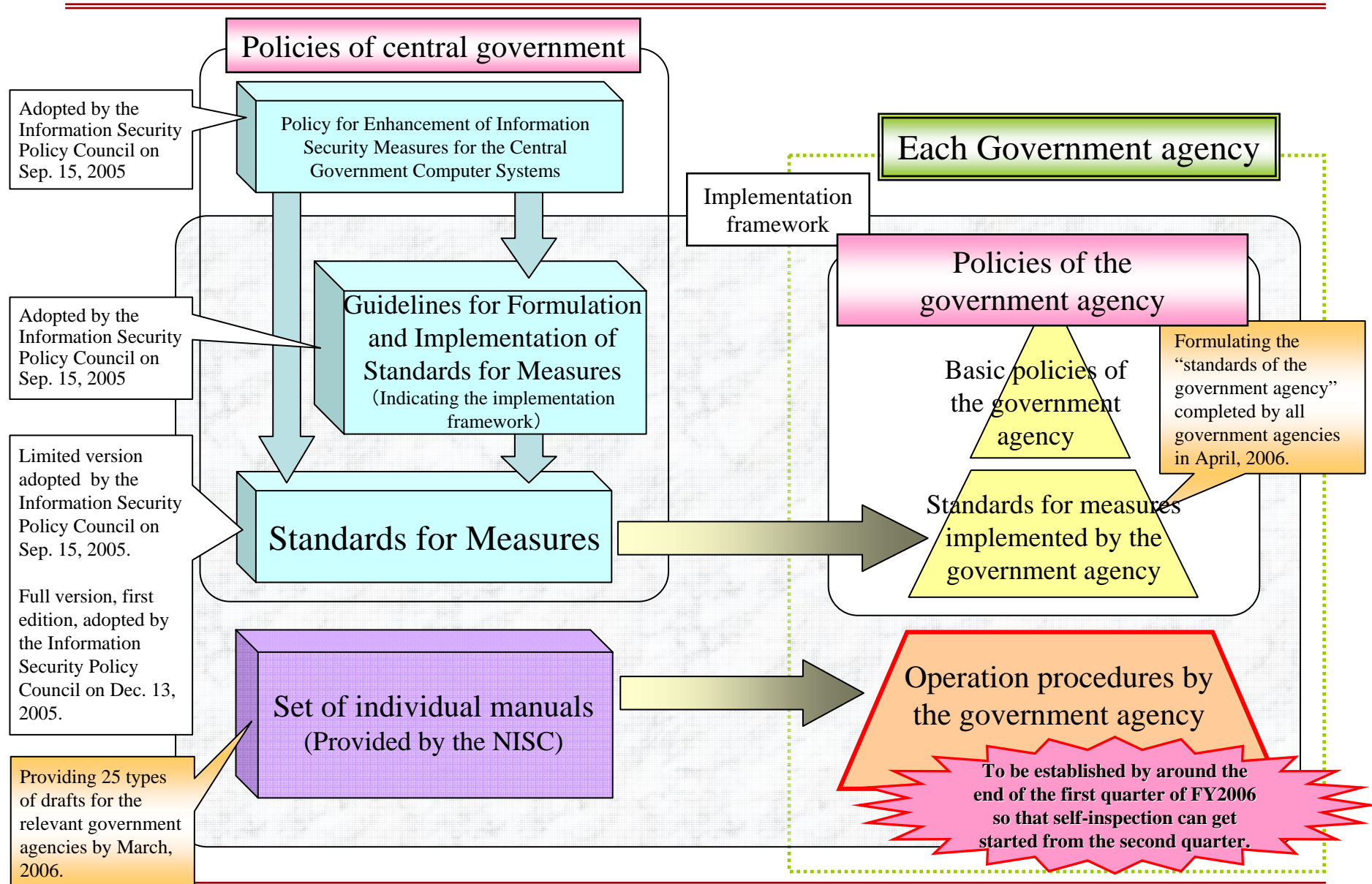
3-1 Standards for Information Security Measures for the Central Government Computer Systems

Outline of “Standards for Information Security Measures for the Central Government Computer Systems”

- **To achieve sectoral plan for raising the information security level of the whole government**, the government formulates the **“Standards for Information Security Measures for the Central Government Computer Systems” (“Standards for Measures”)**.
- Each government agencies implements measures according to **the Standards for Measures, and the NISC inspects and evaluates the implementation status at the central governments. The ISPC makes recommendations for improvement** based on the inspection/evaluation results.



Framework of Information Security Measures of the Government





3-2 Critical Infrastructure Protection

Outline of “Action Plan on Information Security Measures for Critical Infrastructures”

- The “**Special Action Plan on Countermeasures to Cyber-terrorism for Critical Infrastructures**,” formulated in December 2000, provided the first-ever framework for public and private sector cooperation in protecting seven critical infrastructure sectors from the growing threat of cyber-terrorism.
- However, because of the rapid spread in IT use and increased IT dependence in the critical infrastructure sectors as well as growing interdependence between these critical infrastructures, a new action plan was formulated based on the “**Basic Concept on Information Security Measures for Critical Infrastructures (adopted by the ISPC on September 15, 2005)**.”

Reviewing the target sectors and threats

| Basic Stance | Action Plan |
|--|--|
| <ul style="list-style-type: none"> ➤ Critical infrastructure sectors expanded to ten by adding medical services, water works, and logistics. ➤ Assumed threats expanded from “cyber attacks” to also cover “unintentional factors” such as human errors and “disasters.” | <ul style="list-style-type: none"> ➤ Ten sectors* designated as critical infrastructure sectors and boundaries of the target essential services clearly demarcated. ➤ Examples shown of assumed threats and the critical information systems in each sector. |

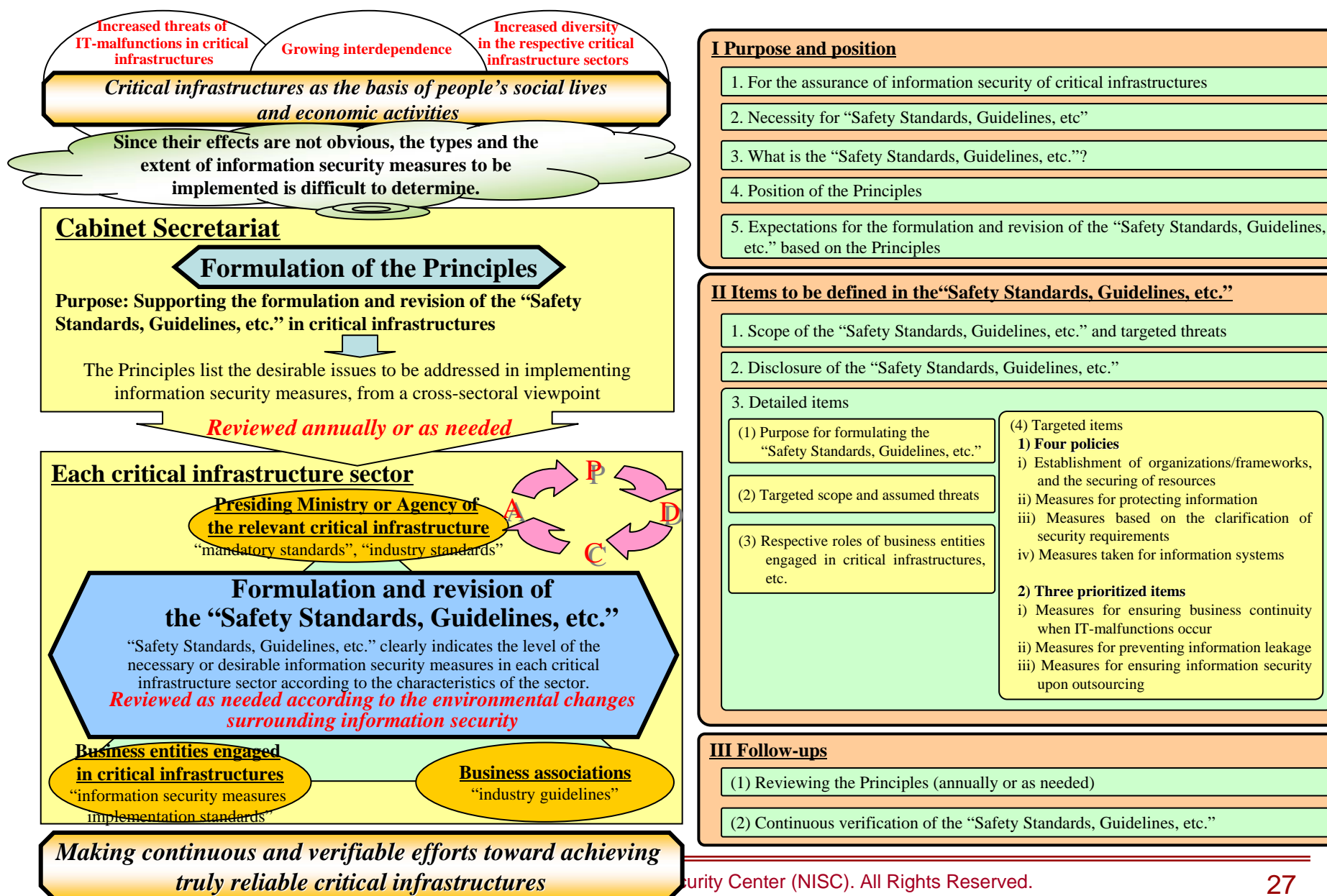
Building a new framework

| | |
|--|---|
| 1. Raising the information security level <ul style="list-style-type: none"> ➤ “Safety Standard, Guidelines, etc.” on technical standards and operational standards will be formulated and reviewed. | <ul style="list-style-type: none"> ➤ The National Information Security Center (NISC) will formulate the “A Principle for Formulation of ‘Safety Standards, Guidelines, etc.’ concerning Assurance of Information Security of Critical Infrastructures” by the end of fiscal 2005. ➤ Each infrastructure sector will make efforts to clearly indicate the necessary or desirable standards for information security measures in the “Safety Standard, Guidelines, etc.” based on the above Principle by around September 2006. |
| 2. Strengthening the information sharing frameworks <ul style="list-style-type: none"> ➤ The information sharing frameworks will be reorganized and strengthened, and the quantity and quality of the available information will be increased. ➤ Information-sharing organizations such as a “ISAC (Information sharing and analysis center)” (tentative) will be established in the respective critical infrastructure sectors. ➤ Cross-sectoral information sharing will be promoted (e.g., establishment of the “CEPTOAR-Council” [tentative]). | <ul style="list-style-type: none"> ➤ The systems of information sharing, liaison, and coordination between the public and private sectors, such as the liaison system used at times of IT-malfunctions, are prescribed in detail. ➤ Efforts will be made to develop CEPTOAR** in each critical infrastructure sector by the end of fiscal 2006.*** ➤ The discussion about the establishment of the “CEPTOAR-Council” (tentative) will be initiated within the Cabinet Secretariat. |
| 3. Analyses of interdependency <ul style="list-style-type: none"> ➤ Cross-sectoral status assessment (e.g., analyses of interdependency) of the critical infrastructures will be conducted under the initiative of the NISC. | <ul style="list-style-type: none"> ➤ The effects and the implementation flow of analyses of interdependency are outlined. ➤ Trial analyses of interdependency will be conducted under the initiative of the NISC, starting in fiscal 2006. |
| 4. Implementation of cross-sectoral exercises <ul style="list-style-type: none"> ➤ Cross-sectoral exercises will be implemented every fiscal year based on concrete threat scenarios corresponding to the assumed threats. | <ul style="list-style-type: none"> ➤ “Exercises for research” and “tabletop exercises” will be implemented in fiscal 2006 and “functional exercises” in fiscal 2007. ➤ “Exercise implementation plans” will be drawn up in the Cabinet Secretariat. The plans will be made under the supervision of the Cabinet Secretariat with participation by the respective critical infrastructures. |

* Telecommunications, finance, civil aviation, railways, electricity, gas, government/administrative services (including local governments), medical services, water works, and logistics.

** Capability for Engineering of Protection, Technical Operation, Analysis and Response
 *** The plan for the new sectors is to build the basic consensus on CEPTOAR development by the end of 2006 fiscal year and launch the actual development in fiscal 2007.

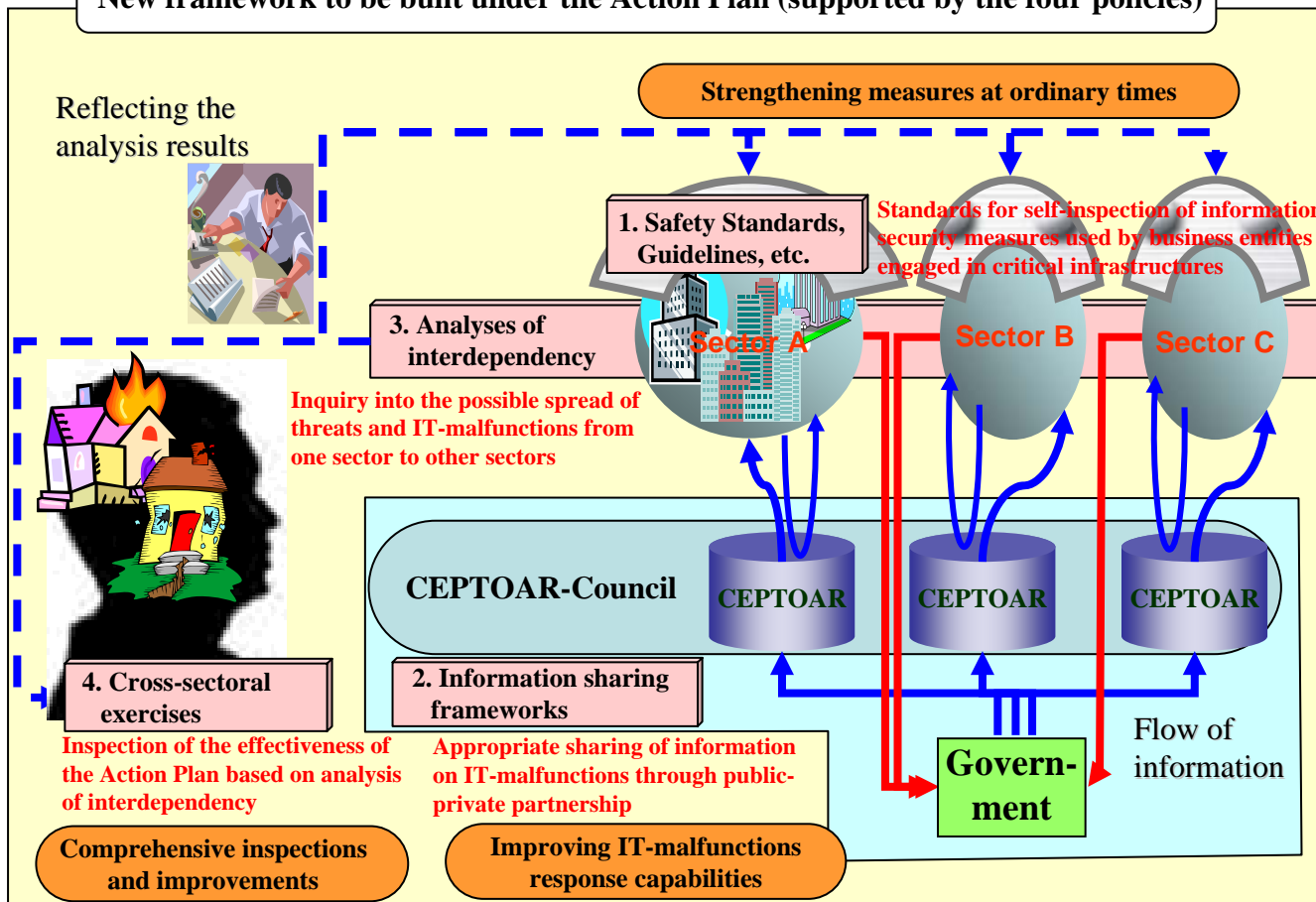
Outline of Principles for Formulating the “Safety Standards, Guidelines, etc.” concerning Assurance of Information Security of Critical Infrastructures



Critical Infrastructures Action Plan

- As respective design drawings for **raising the information security level of the ten critical infrastructure sectors** (telecommunication, finance, civil aviation, railways, electricity, gas, administrative services, medical services, water works, and logistics), the government formulates the **“Action Plan on Information Security Measures for Critical Infrastructures.”**
- The Action Plan aims to **protect critical infrastructures** not only from (1) cyber attacks but also from (2) suspended services and reduced function caused by dysfunction of IT arising from unintentional factors and (3) those arising from disasters (**IT-malfunctions**).

New framework to be built under the Action Plan (supported by the four policies)



- 1. Safety Standards Guidelines, etc.**
Safety standard guidelines to be formulated by the Cabinet Secretariat in 2006
Safety standards to be formulated and reviewed for each sector by September 2006
- 2. Information sharing frameworks**
Functions for information sharing and analysis to be developed for each sector by the end of FY2006 (basic agreements to be made for the sectors of medical services, water works, and logistics by the end of FY2006)
- 3. Analysis of Interdependency**
Trial analysis of interdependency to be started by the Cabinet Secretariat in FY2006
- 4. Cross-sectoral exercises**
“Exercises for research” and “tabletop exercises” to be implemented by the Cabinet Secretariat in FY2006
“Functional exercises” to be implemented by the Cabinet Secretariat in FY2007

Making a new framework for critical infrastructure protection based on public-private partnership through the implementation of the Action Plan

Outline of the “Detailed Rules on Information Connection/Provision under the ‘Action Plan on Information Security Measures for Critical Infrastructures’ ”

- **Critical infrastructures**,^(*1) which serve as the basis of people’s social lives and economic activities, **have recently faced frequent IT-malfunctions**^(*2) including information system failures related to securities trading and aviation, and leakage of important confidential information.
- The “Action Plan on Information Security Measures for Critical Infrastructures” was formulated as an overall plan for protecting critical infrastructures against IT-malfunctions (adopted by the ISPC on Dec. 13, 2005).
- Among the items covered, the “Detailed Rules on Information Connection/Provision” provide for the specific items to be implemented by the framework centering on the Cabinet Secretariat, in order to promote smooth information sharing under the cooperation between the public and private sectors.

(*1) 10 critical infrastructure sectors: telecommunications, finance, civil aviation, railways, electricity, gas, government/administrative services, medical services, water works, and logistics

(*2) “IT-malfunction” is any malfunction (suspended services, reduced function, etc.) that occurs in the operation of critical infrastructures caused by a dysfunction of IT.



Action Plan on Information Security Measures for Critical Infrastructures

(Adopted by the ISPC on December 13, 2005)

[Four policies]

1. Improving the “Safety Standards, Guidelines, etc.”
2. Establishing the information sharing system

(1) Information provision/connection between public and private sectors

- (2) CEPTOAR
- (3) CEPTOAR-Council

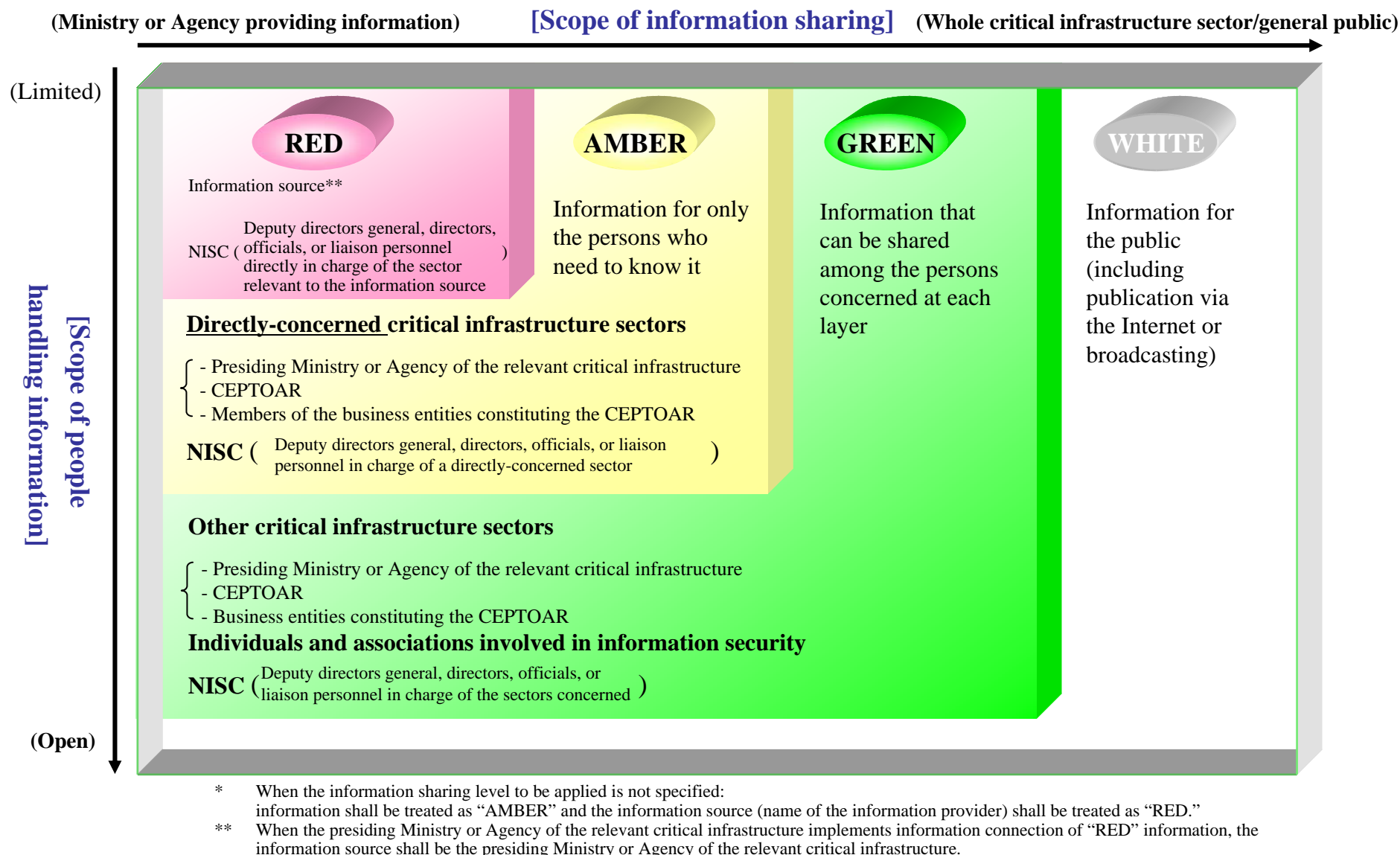
3. Implementing analysis of interdependence
4. Implementing cross-sectoral exercises

Detailed Rules on Information Connection/Provision

- Promoting smooth information sharing with cooperation between the public and private sectors so as to make it easier for business entities engaged in critical infrastructures to maintain and restore their services
- Stipulating rules on information provision/connection between the NISC and the presiding Ministries and Agencies of the relevant critical infrastructures
 - Setting the extent of information sharing (using the Traffic Light Protocol [see the following page])
 - Setting the procedures for information connection
 - Setting the common classification/categorization concerning IT-malfunctions for information connection
 - Acquiring statistical information on occurrences of IT-malfunctions
 - Setting the procedures for information provision

Implementing information connection/provision concerning IT-malfunctions in the respective critical infrastructure sectors

(Reference) Outline of the Traffic Light Protocol





3-3 International Cooperation/Contribution concerning Information Security

Circumstances toward the Efforts for International Cooperation/Contribution

○ Consideration at Information Security Policy Council

- At the meeting of Information Security Policy Council etc, committee member with professional expertise repeatedly presented opinion that "Adoption of Japanese efforts for information security on an International Scale is necessary."
- Based on the "First National Strategy on Information Security", it is clearly described to establish basic concepts for strategic commitment to international cooperation/contribution in "Secure Japan 2007".

○ Consideration at Council on Economic and Fiscal Policy

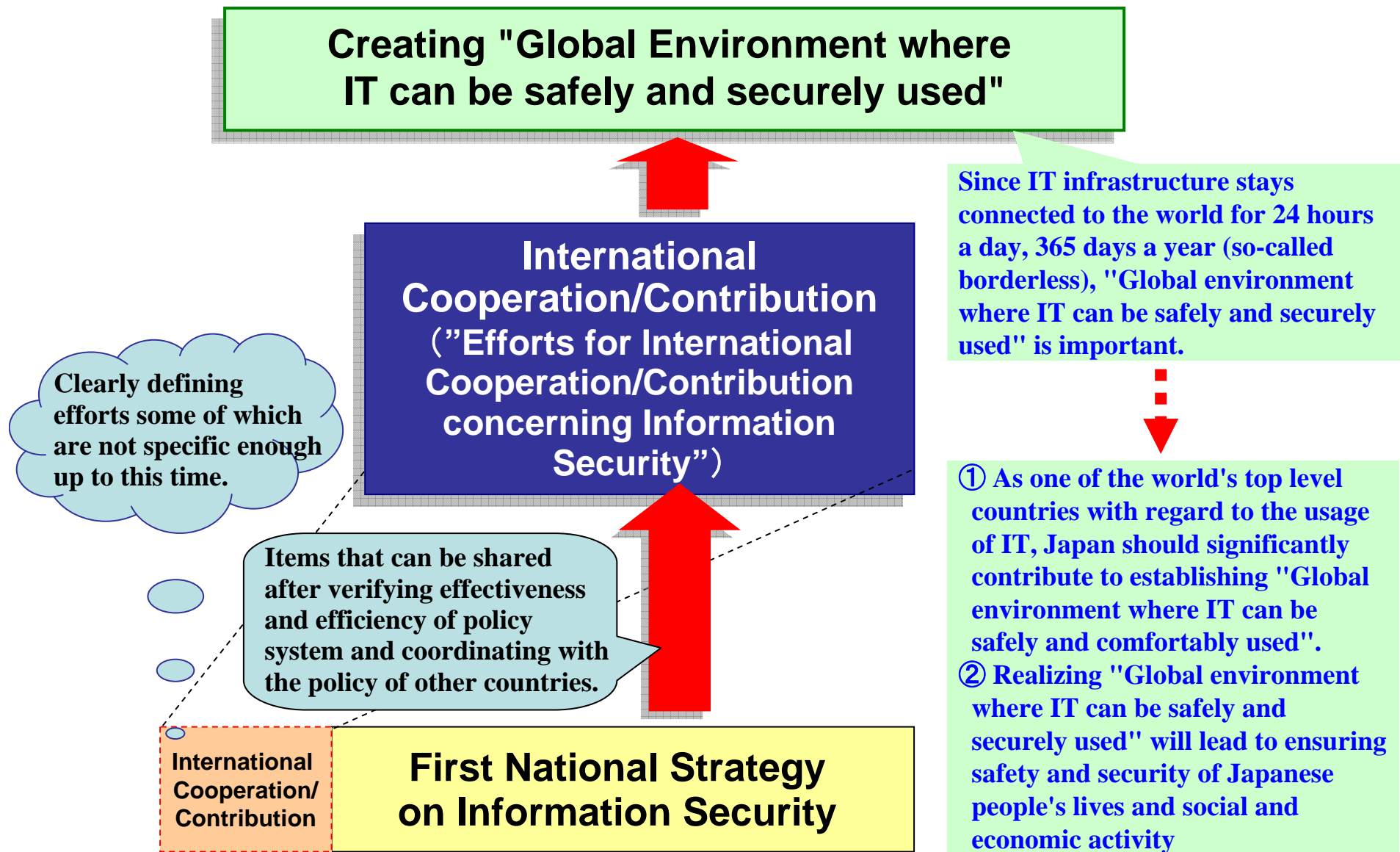
- On April 20, 2007, Chief Cabinet Secretary announced "Importance of security infrastructure which support innovation of productivity by utilizing IT - facilitating domestic measures and adoption of Japanese measures on an International Scale -".
- Decision was made to establish international strategy for cooperation/contribution concerning information security by July 2007 in the "Program for Enhancing Growth Potential" (April 25, 2007).
- In the Structural Reform of the Japanese Economy : Basic Policies for Macroeconomic Management (June 19, 2007, so-called "Honebuto" policy), it is clearly described that cooperation/contribution with relevant countries to improve information security posture will be promoted.



○ Establishing efforts for international cooperation/contribution

- Based on the effort and coordination made at that time, intermediary report was submitted at the policy council held on August 3, 2007.
- Based on the discussion at policy council, with promptly adding specific measures and gaining cooperation of relevant agencies, efforts for international cooperation/contribution will be established.

Positioning and Basic Concept of “Efforts for International Cooperation/Contribution concerning Information Security”



“Efforts for International Cooperation/Contribution concerning Information Security”

～5 Directions of the Efforts～

○Promoting cooperation/contribution toward improvement of business environment of Asian region where economic relationships are continuously being deepened (Secure Asian Business Environment Initiative)

- Through the cultivation of security culture and improvement of the level of information security measures, developing an environment that enables safe and secure business activity.
- Performing cooperation/contribution such as human resource developments, awareness raising of the general users, spreading the best practice of information security measures and promoting voluntary outreaching activities by regional countries.

○Contributing to consideration and discussion concerning new rights with regard to information security

- Contribution to global discussion from the point of view of relations with IT usage without any limitation and redemption of the person who suffered from the threat resulting from IT usage.

○Promoting efforts to respond to the threats such as cyber attack (ICT Risk-free Initiative)

- Sharing awareness at high level of international forum with regard to threats resulting from IT such as cyber attack and actively attending to and thus contributing to the discussion to appropriately respond to the threats.
- Continuously promoting multinational discussion with regard to measures against cyber crimes that will be committed across border.

○Contributing to global rule and standard with regard to information security

- Understanding advanced field concerning Japan's efforts on information security and identifying ongoing rules that can be referred as the best practices.
- Actively participating in discussion held at international forums and thus contributing to the activity.

○Actively submitting proposal to and participating in discussion at various international forums

- More active participation and involvement with existing global frameworks in order to share necessary information timely and appropriately.
- Making effort to take the initiative in multinational forums by hosting a multinational forum and leading a discussion among them.

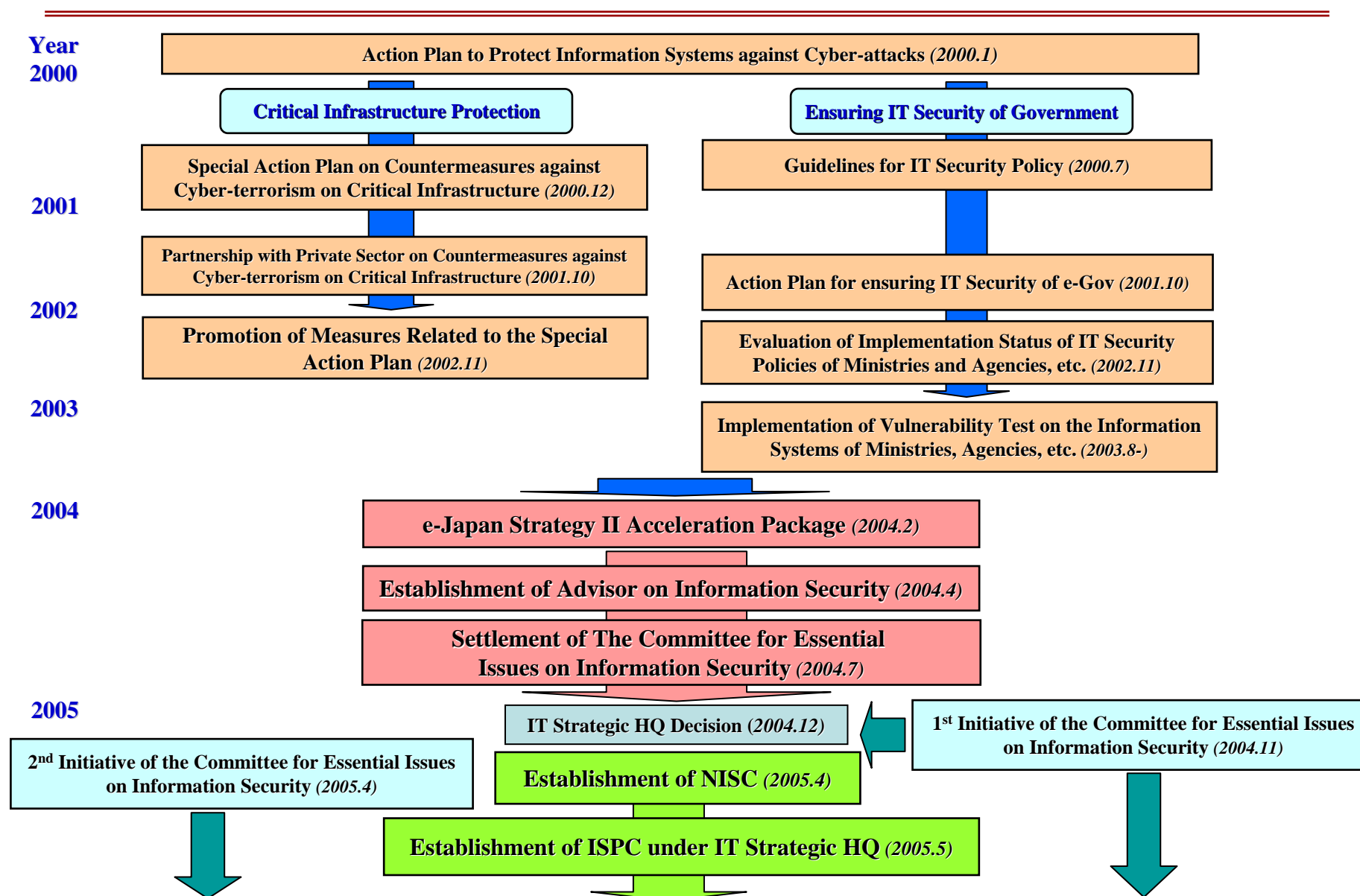


APPENDIX

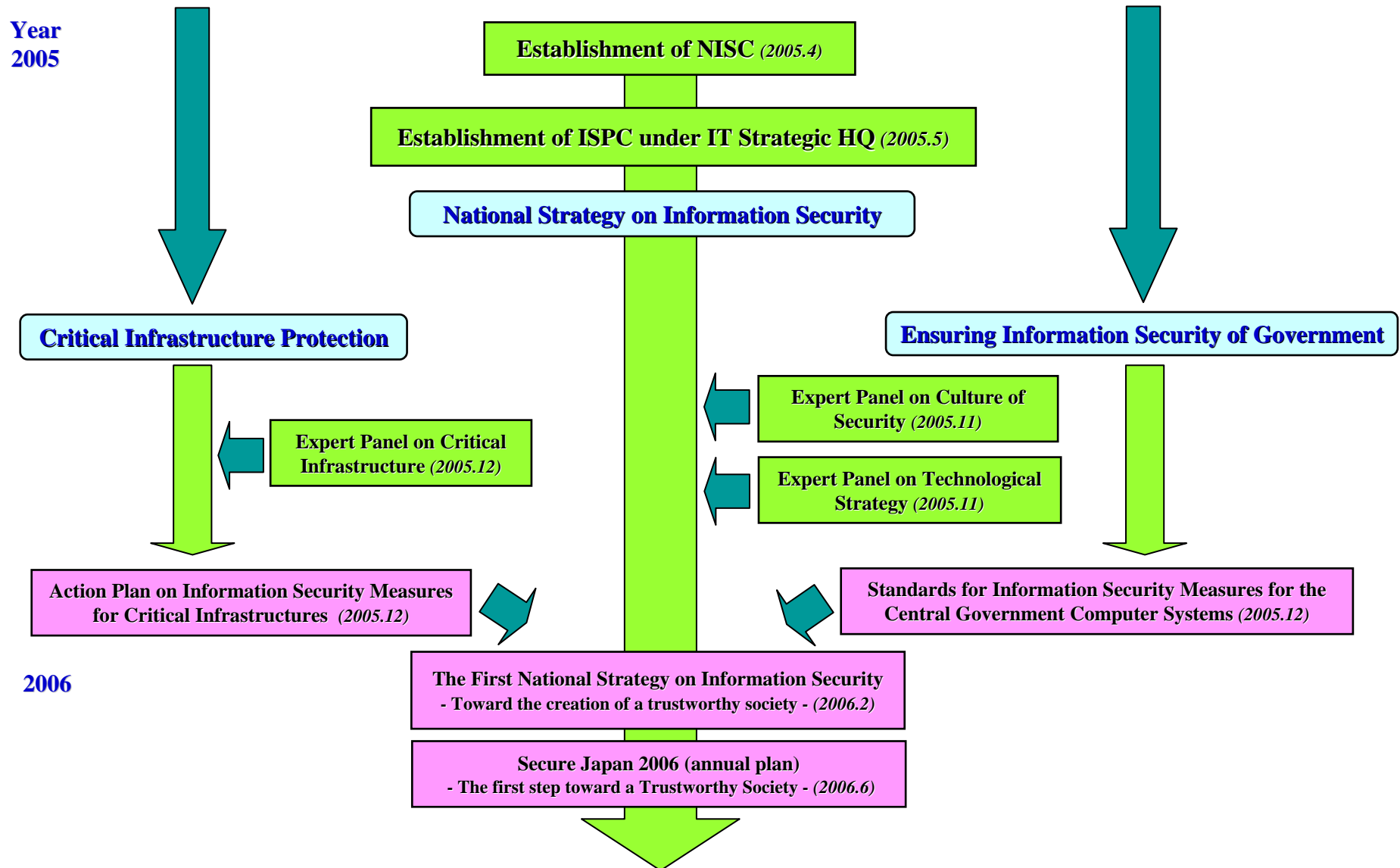


History and Agenda of Information Security Policy Council

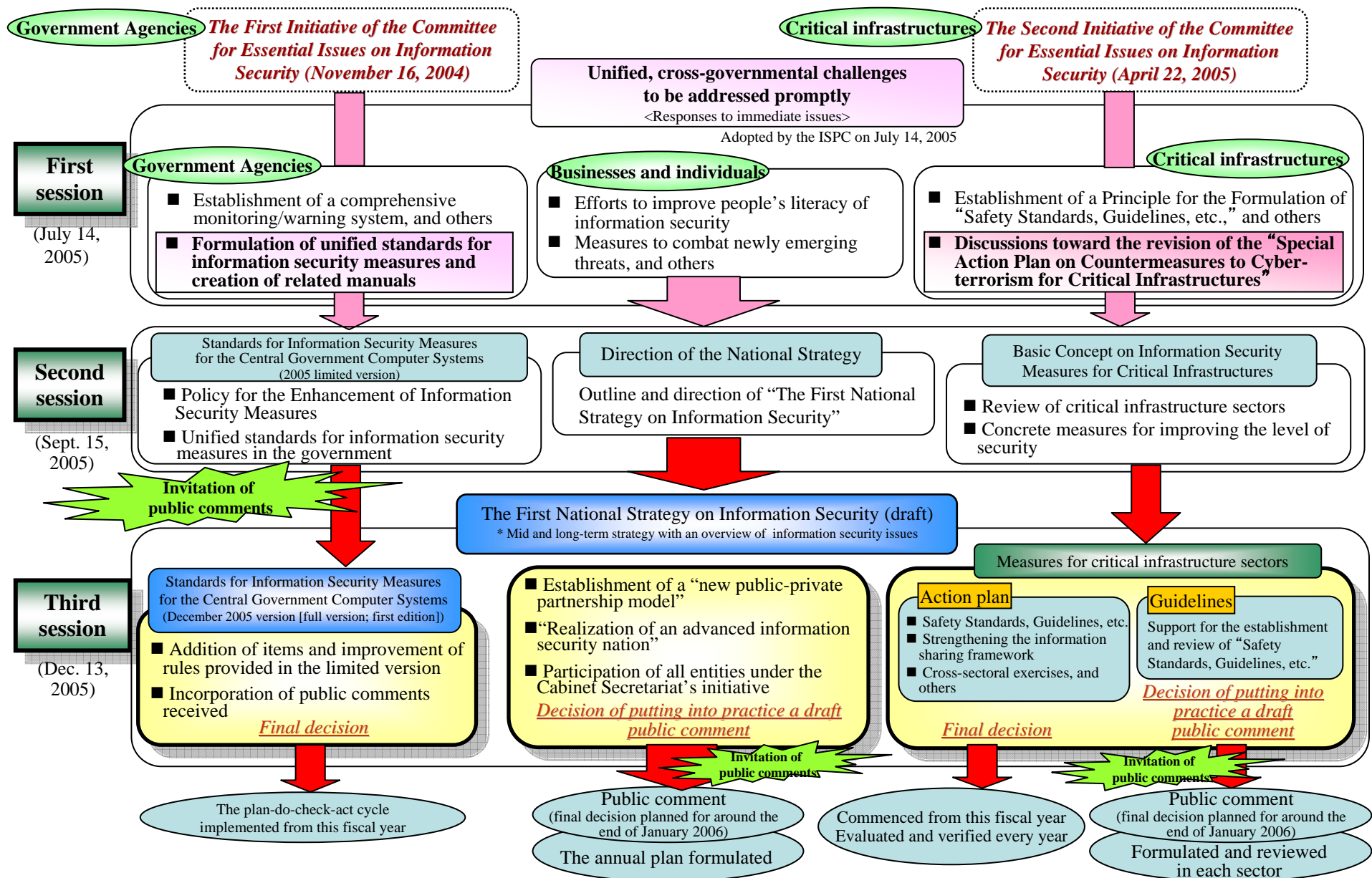
History of Information Security Policy Planning at Government



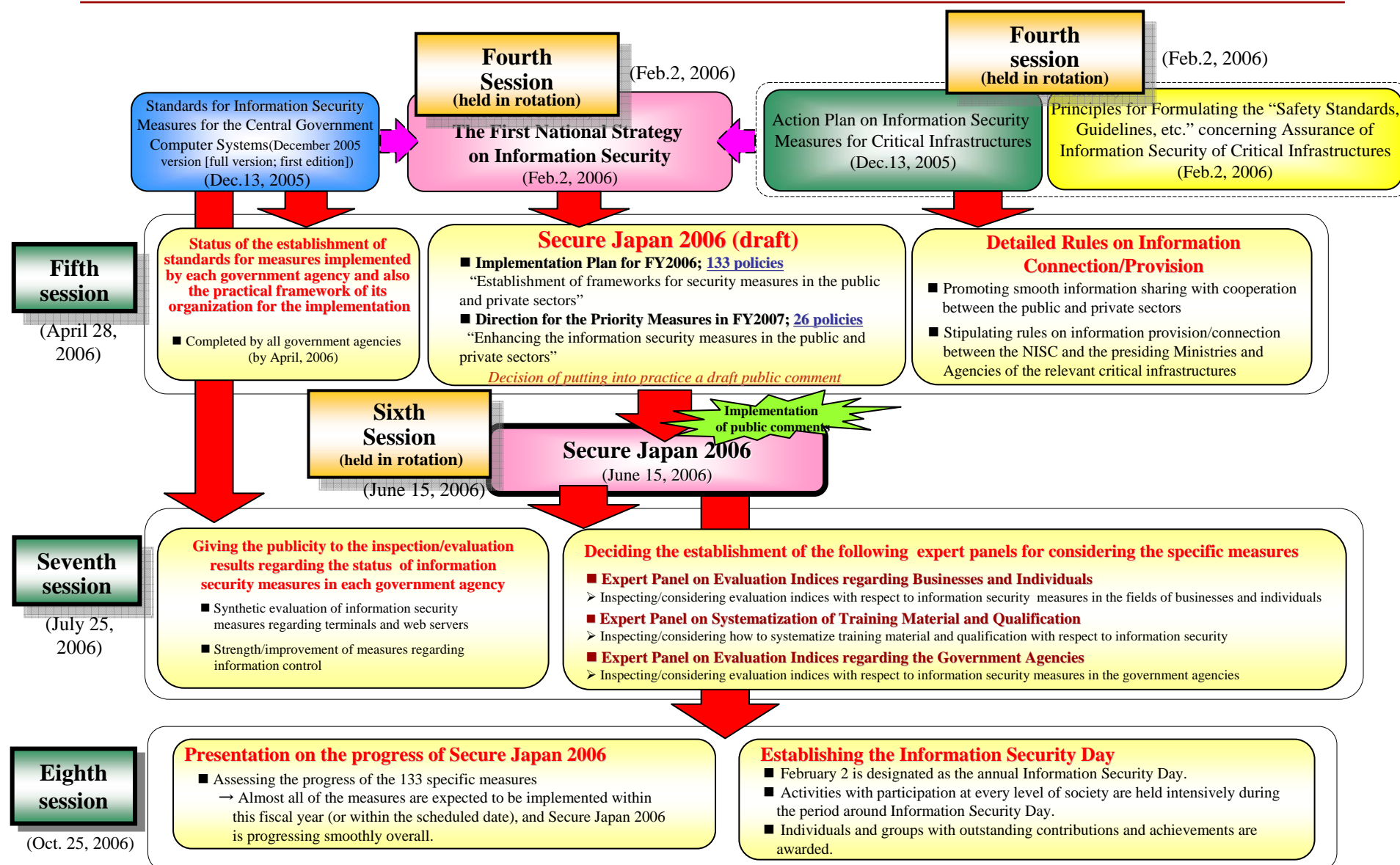
History of Information Security Policy Planning at Government (cont'd)



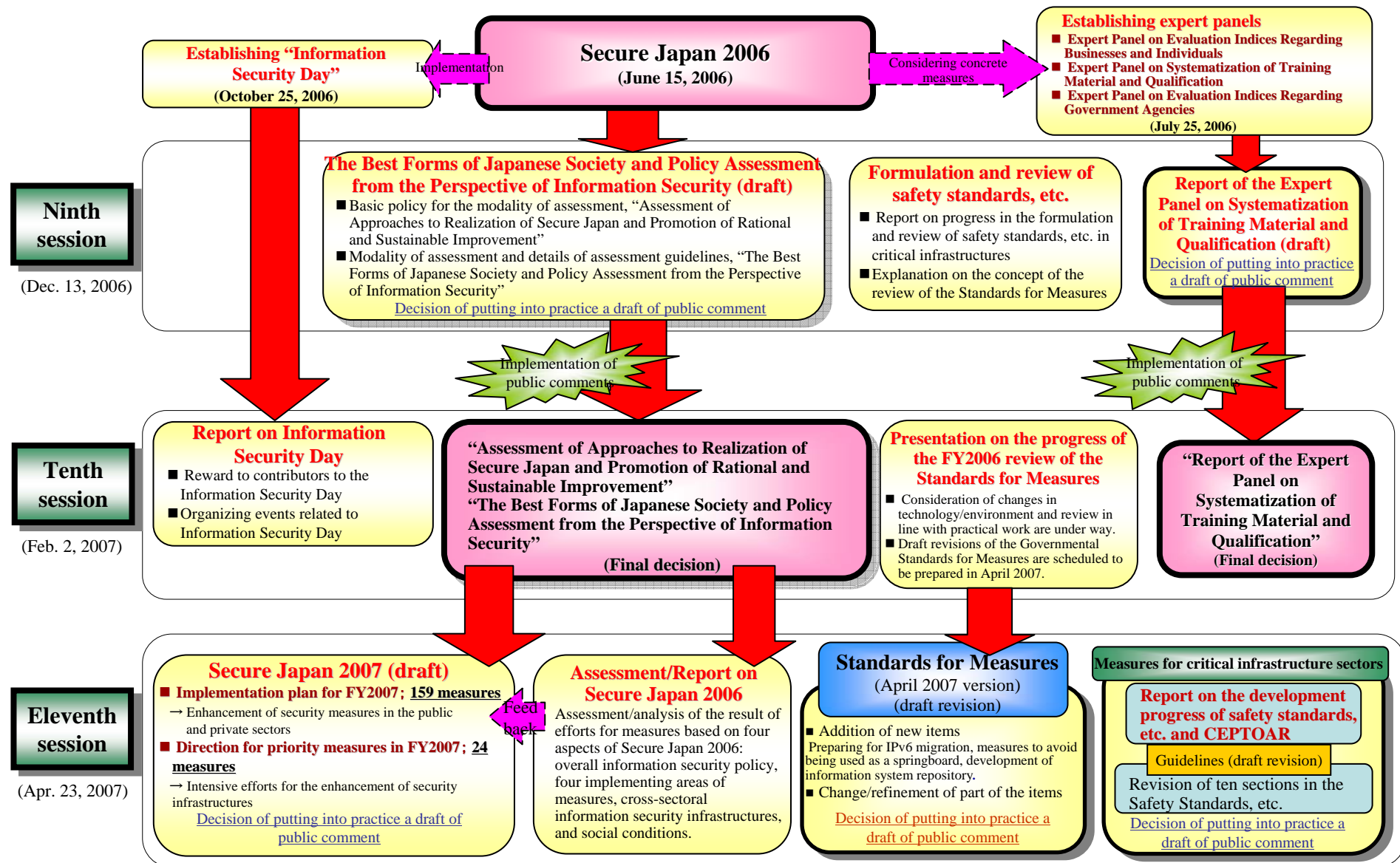
Agenda Overview - the Information Security Policy Council



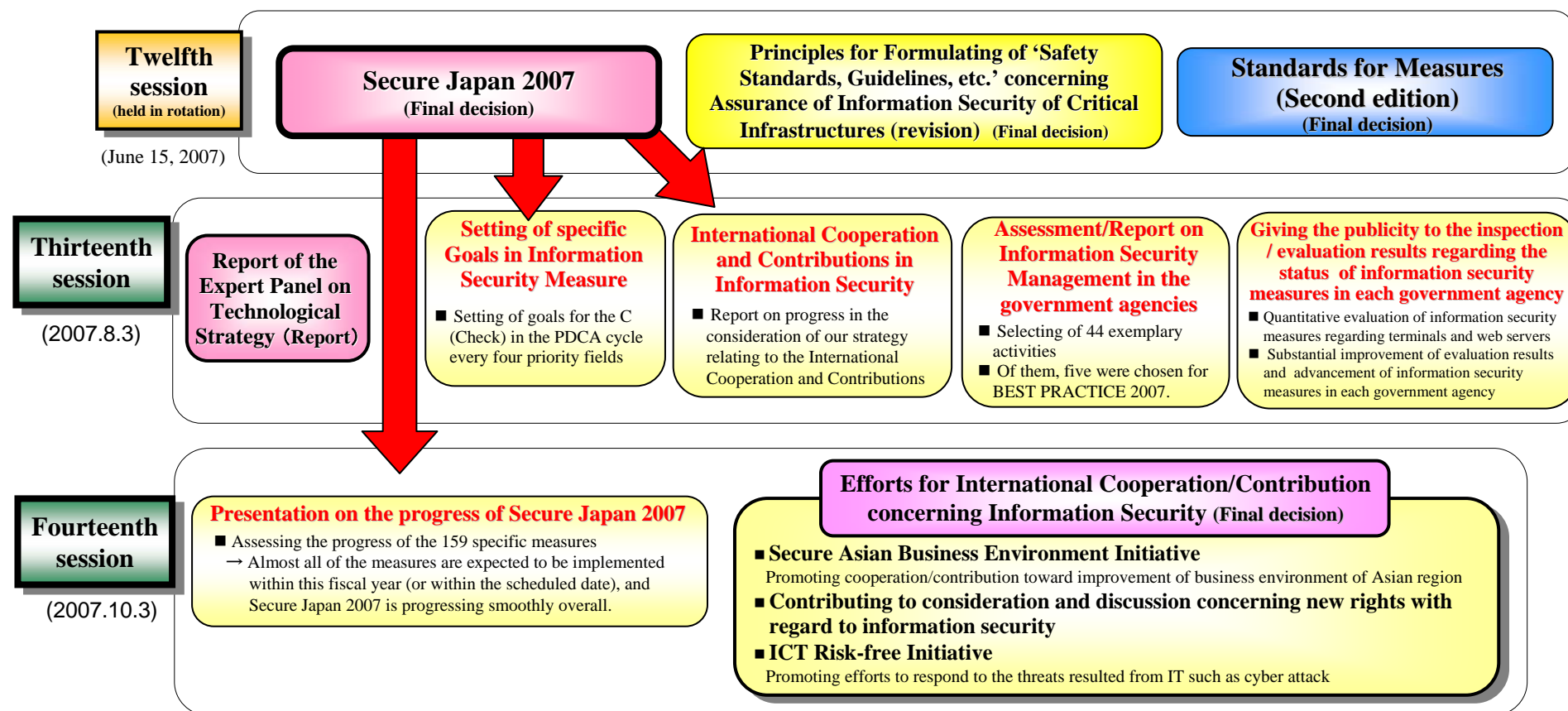
Agenda Overview - the Information Security Policy Council (cont'd)



Agenda Overview - the Information Security Policy Council (cont'd)



Agenda Overview - the Information Security Policy Council (cont'd)





Efforts made based on Secure Japan 2006

“Information Security Day”

Decisions made at the eighth session of the Information Security Policy Council on October 25, 2006

From the point of view of disseminating/enlightening widely to the general public on the importance of information security,

- **February 2 has been designated as annual “Information Security Day.”** (* Date on which the First National Strategy on Information was decided)
- **During the period before and after Information Security Day, various related events will be intensively held under cooperation among government agencies and other related organizations and institutions.**
- **The Chair will award individuals and groups that have been committed to the promotion of information security and have particularly made outstanding contributions and achievements.**

[Details of the efforts for Information Security Day in FY2006]

Awarding the Information Security Day Award Winners

The Selection Committee was set up in the National Information Security Center, Cabinet Secretariat to compile the list of the award nominees, based on the recommendations made by the relevant ministries that promote Information Security Day (National Police Agency, Ministry of Internal Affairs and Communications, Ministry of Education, Culture, Sports, Science and Technology, and Ministry of Economy, Industry and Trade) and the private and public efforts recognized by the Cabinet Secretariat, pursuant to the decisions made at the eighth session of the Policy Council.

The Chairman selected the winner of the award from the list of the nominees.

[Award Winners]

Shigeo Tsujii (president, institute of information security)

Norihisa Doi (professor, Chuo University)

Hiroyuki Kuwako (Chairman, Business Morals and Internet Committee, Telecom Services Association)

Akinobu Kanasugi (the deceased, former president, NEC Corporation)

Toyonaka City, Osaka (local government)

Events related to Information Security Day

With help widely from public and private sectors, events centered on Information Security Day were held. Awareness of information security is expected to increase at every level of society.

○ **Total number of events: 311**

○ **Event Period**

From January 26 to March 2, 2006

○ **Locations of Events: 47 prefectures throughout Japan**

○ **Types of Events**

Seminars, lectures, TV commercials, radio programs, etc.

Cross-sectoral Exercises in the Critical Infrastructure Sectors

Implemented on February 7, 2007 in line with the concept of Information Security Day, in view of establishing a framework for the public and private sectors to work together and improving its effectiveness

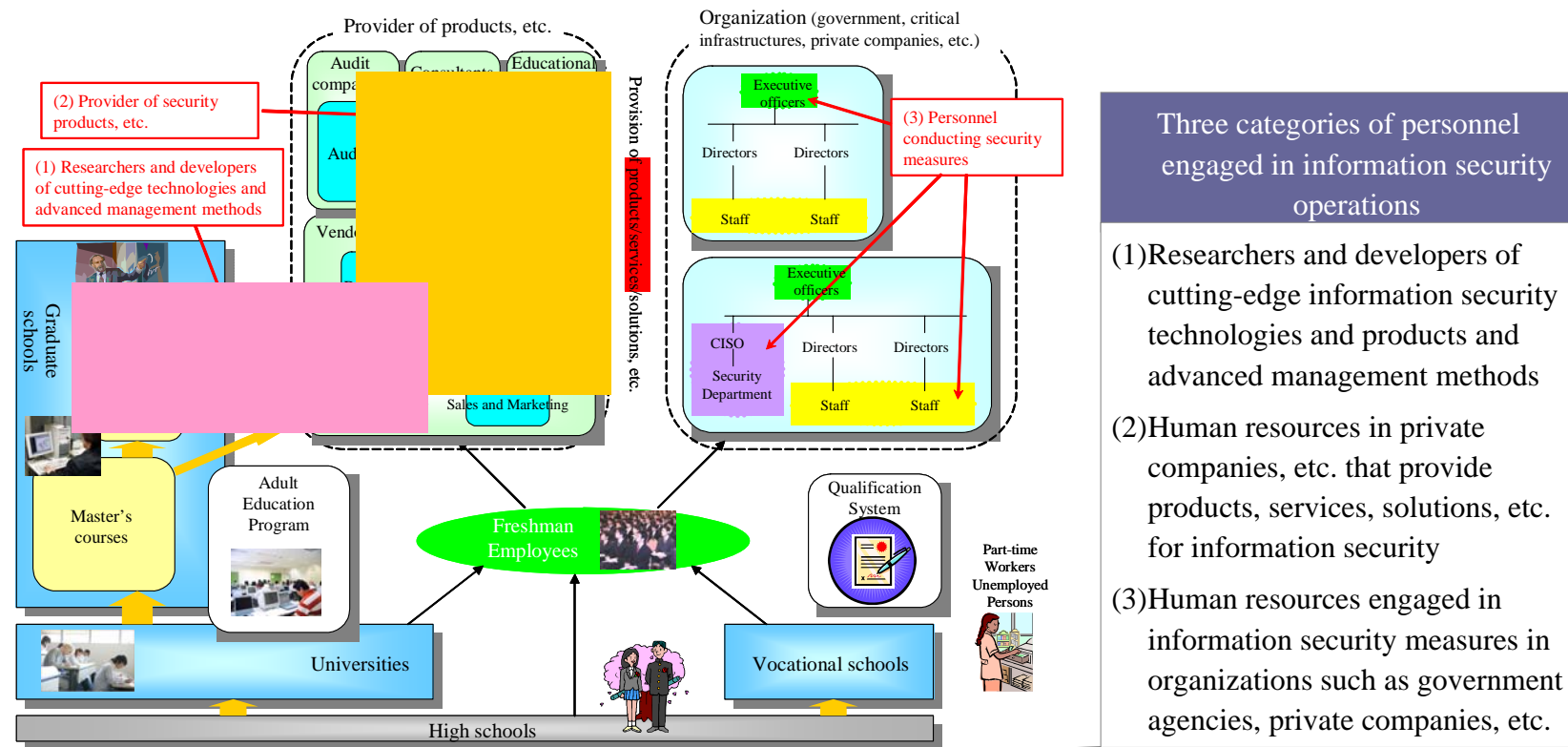
Overview of the Report of the Expert Panel on Systematization of Training Material and Qualification

(1) Process of Discussions at the Committee

In principle, it is necessary to examine the best forms of measures for human-resource development from the long term view point by the state as a whole, including the forms of education in the practice of elementary and secondary education.

However, since the improvement of information security measures is an urgent issue, the committee conducts intensive discussions and provides recommendations on the issues to be addressed and tackled at an early stage with an aim to improve the level of measures by developing human resources currently available in Japan.

It is necessary to secure and improve the awareness and capacity of players who engaged with their operations in various social and economic activities, in order to promote the overall information security



Three categories of personnel engaged in information security operations


- (1) Researchers and developers of cutting-edge information security technologies and products and advanced management methods
- (2) Human resources in private companies, etc. that provide products, services, solutions, etc. for information security
- (3) Human resources engaged in information security measures in organizations such as government agencies, private companies, etc.

In each human resource category, current situations and issues are analyzed and necessary response measures are considered.

Framework of Critical Infrastructure Measures

~Promotion through Organic Coordination of Four Measures~

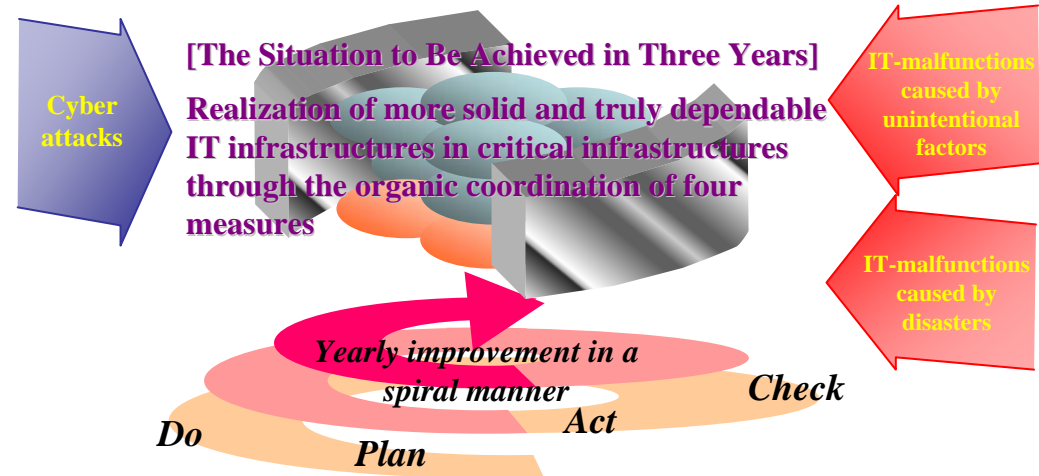
- As respective design drawings for raising the information security level of the ten critical infrastructure sectors (telecommunication, finance, civil aviation, railways, electricity, gas, administrative services, medical services, water works and logistics), the government formulates the “Action Plan on Information Security Measures for Critical Infrastructures.”
- The Action Plan aims to protect critical infrastructures not only from (1) cyber attacks but also from (2) suspended services and reduced function caused by dysfunction of IT arising from unintentional factors and (3) those arising from disasters (IT-malfunctions). Promotion through organic coordination of four measures, while maintaining close relations between public and private sectors.



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

[Four policies]

1. Enhancement of the “Safety Standards, Guidelines, etc.”
2. Establishment of the information sharing system
3. Implementation of analysis of interdependence
4. Implementation of cross-sectoral exercises



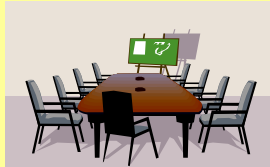
[Current Situations]

- Importance of an approach to foster common awareness about basic concepts of critical infrastructures protection and required measures, taking the characteristics of threats causing IT malfunctions into account
- Necessity of expanding potential supposed threats and enhancing measures against events that may potentially have a large-scale impact on a wide area
- Necessity of enhancing information security measures within the framework of communication/cooperation and information sharing

[Objectives] The central government will make efforts aiming to reduce the number of occurrence of IT-malfunctions in critical infrastructures as close as possible to zero by the beginning of FY2009

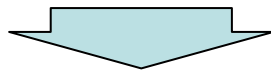
Formulation and Review of Safety Standards, Guidelines, etc. for Critical Infrastructures

Formulation and review of the Safety Standards, etc. were completed in all the areas within FY2006, including the areas in which there had not been Safety Standards, Guidelines, etc. at the time of the formulation of the action plan.



The Fourth Session of the Information Security Policy Council (February 2, 2006)

A decision was made on the “Principles for Formulating ‘Safety Standards, Guidelines, etc.’ concerning Information Security Assurance of Critical Infrastructures”



Critical infrastructures

Stipulation of the required or desirable level of information security measures in the ‘Safety Standards, Guidelines, etc.’



| Sectors | Names in the Safety Standards, Guidelines, etc. [Main body of issuance] | Formulation/Review Status |
|-------------------------|--|---------------------------|
| Telecommunication | Telecommunication Business Act, Regulations for Enforcement of the Telecommunication Business Act, and Regulations for Telecommunications Facilities for Telecommunications Business, etc. (including related notices) | Implementation Completed |
| | Standards for Information and Communication Network Security/Reliability [MIC] Safety Standards for Information Security Assurance in Telecommunication (1st edition) [ISeCT] (*1) | |
| | Guidelines for Formulating “Safety Standards, Guidelines, etc.” for Information Security Assurance of Information Infrastructure in Broadcasting [Japan Broadcasting Corporation (NHK), National Association of Commercial Broadcasters in Japan] | Implementation Completed |
| Finance | Manual for Formulating Security Policies in Financial Institutions, etc. [FISC] (*2) FISC Security Guidelines on Computer Systems for Financial Institutions [FISC] Manual for Formulating Contingency Plan in Financial Institutions, etc. [FISC] | Implementation Completed |
| Civil aviation | Safety Guidelines for Information Security Assurance in Air Cargo Business [MLIT] Safety Guidelines for Information Security Assurance in Air Traffic Control System [MLIT] | Implementation Completed |
| Railways | Safety Guidelines for Information Security Assurance in Railway Area [Railway businesses, etc.] | Implementation Completed |
| Electricity | Guidelines for Technical Levels/Operation Standards in Electronic Control System, etc. [Federation of Electric Power Companies] | Implementation Completed |
| Gas | Guidelines for Information Security Measures for Control Systems for Production/Supply [Japan Gas Association] | Implementation Completed |
| Administrative services | Guidelines for Information Security Policy in Local Governments [MIC] | Implementation Completed |
| Medical services | Guidelines concerning Safety Control of Medical Information Systems [MHLW] | Implementation Completed |
| Water works | Information Security Guidelines for Water Systems [MHLW] | Implementation Completed |
| Logistics | Safety Guidelines for Information Security Assurance in Distribution Systems [MLIT] | Implementation Completed |

(*1) ISeCT: Information Security Conference on Telecommunications (*2) FISC: Center for Financial Industry Information Systems

Revision of the “Principles for Formulating ‘Safety Standards, Guidelines, etc.’ concerning Information Security Assurance of Critical Infrastructures”

By regularly following the occurrences of [stationary] IT malfunctions, analyses and examinations were conducted on the cross-sectoral issues related to the measures commonly found in each critical infrastructure; then, the revisions in the Principles were made on the following points (June 2007).

1. Analysis of occurrences of stationary IT malfunctions

(1) Suspension/reduction of services due to system malfunction

- Load balancing and redundancy to ensure availability
- Ensuring processing performance and system quality as an exemplification of measures

(2) Communication disruption due to Taiwan earthquake

- The threats which may cause IT failure do not always come from within the country

(3) Information leakage by using file-swapping software

- Prevention of occurrence and recurrence
- Preventive measures against information leakage applied for contractors

Revised parts

● “Four pillars: iii) Measures based on the clarification of security requirements”

● “Four pillars: iv) Measures taken for information systems”

● “Four pillars: iv) Measures taken for information systems”

● “Three prioritized items: ii) Measures for preventing information leakage”

● “Three prioritized items: iii) Measures for ensuring information security by outsourcing”

2. Examination of related documents

(1) Safety Standards, Guidelines, etc. in each critical infrastructure

- Conducting self-assessments and audits

● “Four pillars: i) Establishment of organizations/frameworks, and the securing of resources”

3. Examination of changes in social conditions (environment)

(1) Movements regarding risk management

- Deployment of PDCA cycle (Business Continuity Plan)

(2) Movements in the overall critical infrastructures

- IT-dependent black-boxing and expansion and advancement of the scope of application

(3) Efforts based on the Action Plan for Critical Infrastructures

- Consensus on the development of CEPTOAR

● “Three prioritized items: i) Measures for ensuring business continuity when IT-malfunctions occur”

● “Four pillars: iv) Measures taken for information systems”

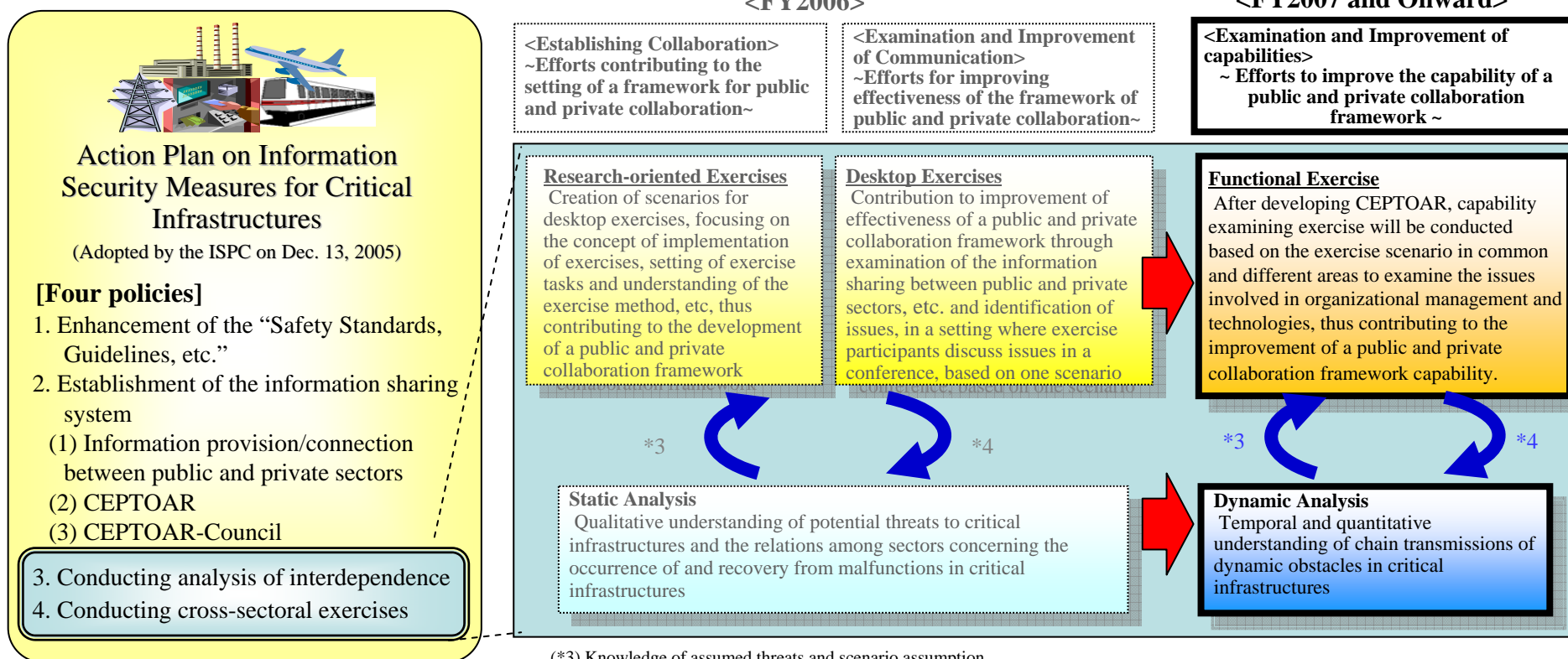
● “Follow-ups”

Overview of “Cross-sectoral Exercise” and “Analysis of Mutual Dependency” in Critical Infrastructures

- ◆ With respect to “Cross-sectoral Exercise” and “Analysis of Mutual Dependency,” functional exercises (*1) will be conducted in FY2007 based on the practical scenario in common and in different areas to examine the issues in organizational management and technologies. Mutual dependency will be analyzed to deepen the discussion about types of threats, causal relationships between threats and malfunctions, and relationships between malfunctions and business continuity, and to examine and conduct dynamic analyses of those elements, following consideration of the conducting method.
- ◆ In FY2007, study groups will be set up in the Information Security Center, Cabinet Secretariat in order to conduct specific discussions in line with the action plan, with the help of competent agencies of critical infrastructures, business entities associated with critical infrastructures, CEPTOAR, etc. The study groups (*2) will consist of intellectuals with professional knowledge, competent agencies of critical infrastructures, business entities associated with critical infrastructures, CEPTOAR, etc.

(*1) Exercises to examine in a simulated manner using the command and decision-making function of the actual organization

(*2) The Cross-sectoral Exercise Study Group consists of exercise coordinators, and researchers and specialists with knowledge on systems and functions in various sectors, such as disaster prevention, crisis management, risk management and BCP. The Study Group for Analysis of Mutual Dependency consists of researchers and experts with knowledge on systems and functions in such areas as mutual dependency analysis, and researchers and experts in BCP, etc.



Review of the FY2007 Standards for Measures

The following revisions were made at the Information Security Policy Council - 12th session (June 2007):

1. Feedback of the changes in technology and environment

1) Responses to the deployment of IPv6 into information systems (6.2.3) (new)

Addition of measures for information systems where IPv4 and IPv6 co-exist, in response to the penetration of IPv6 products

2) Measures to avoid being used as a springboard (4.2.4) (new)

Addition of measures to prevent the government information systems from being used by a third party for unintended purposes (springboard)

3) Use of encryption module test and authentication system (4.1.6)

Stipulation in view of full-scale use of an encryption module test and authentication system in Japan based on ISO/IEC 19790

2. Review, etc. for practical operation

1) Development of an information system repository (4.3.1) (new)

Regarding government agency information systems, rule is added defining that information handled by those systems must be managed and classified in an integrated fashion.

2) Review of rules concerning handling information (1.1.3 3.2.4 3.2.5, etc.)

Review of the scope of confidentiality class-2, approval/notification procedures for transfer/provision of information

3) Enhancement of physical measures of information systems (5.1.1)

Changing the category of “physical isolation and access control of information systems and theft-prevention measures” from the Enhanced Requirements to the Basic Requirements

4) Stipulation of an information security auditing system (2.3.2)

Positioning of the information auditing system and clarification of the relationship with self-assessment

5) Stipulation of the management and control method of data encryption (4.1.6)

Stipulation that the management and control method of data encryption shall be determined by the government, instead of being selected at the discretion of each employee

6) Other

Improvement in the wording