NISC National Information Security Center

Japanese Government's Efforts to Address Information Security Issues

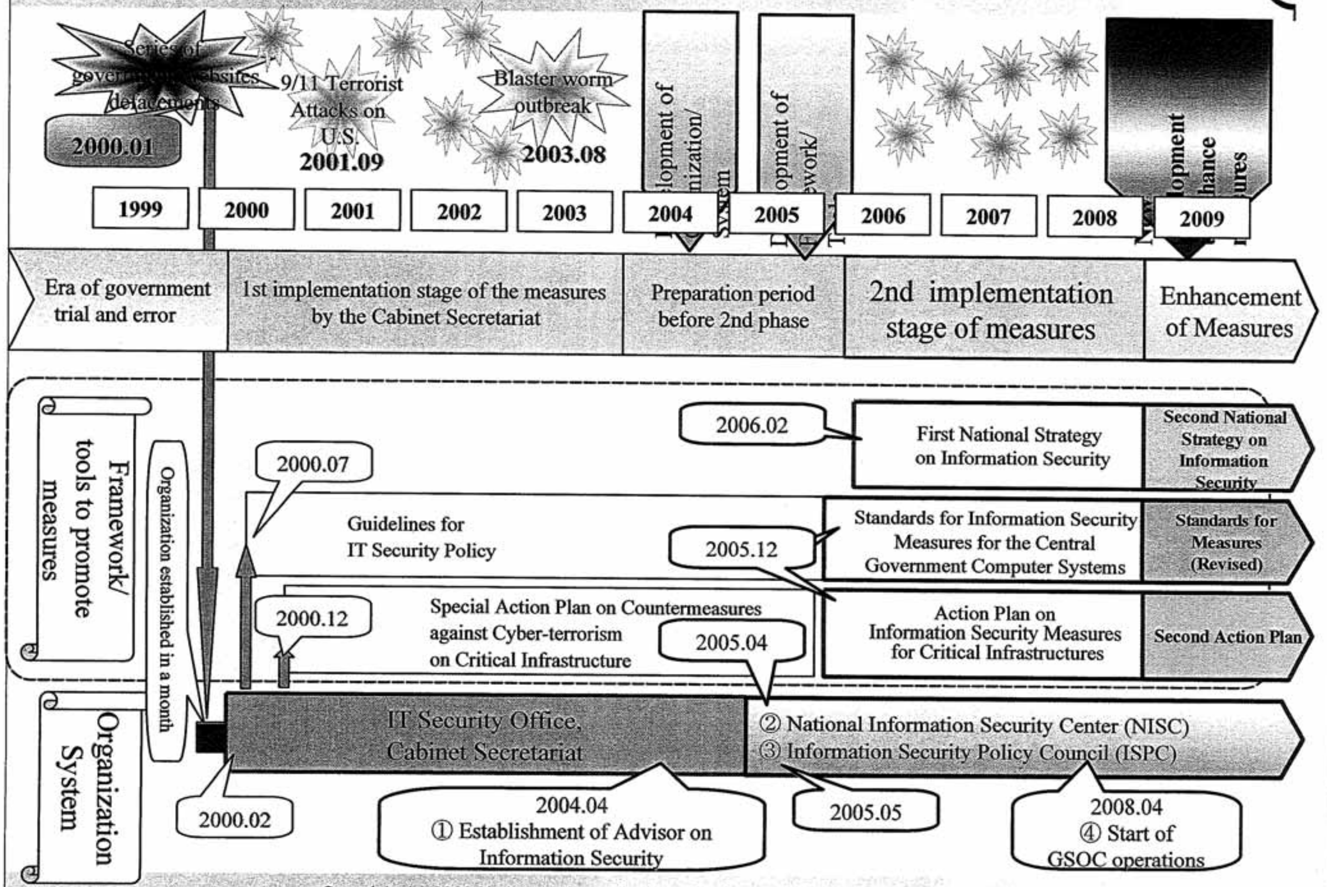
November 2009

National Information Security Center (NISC)

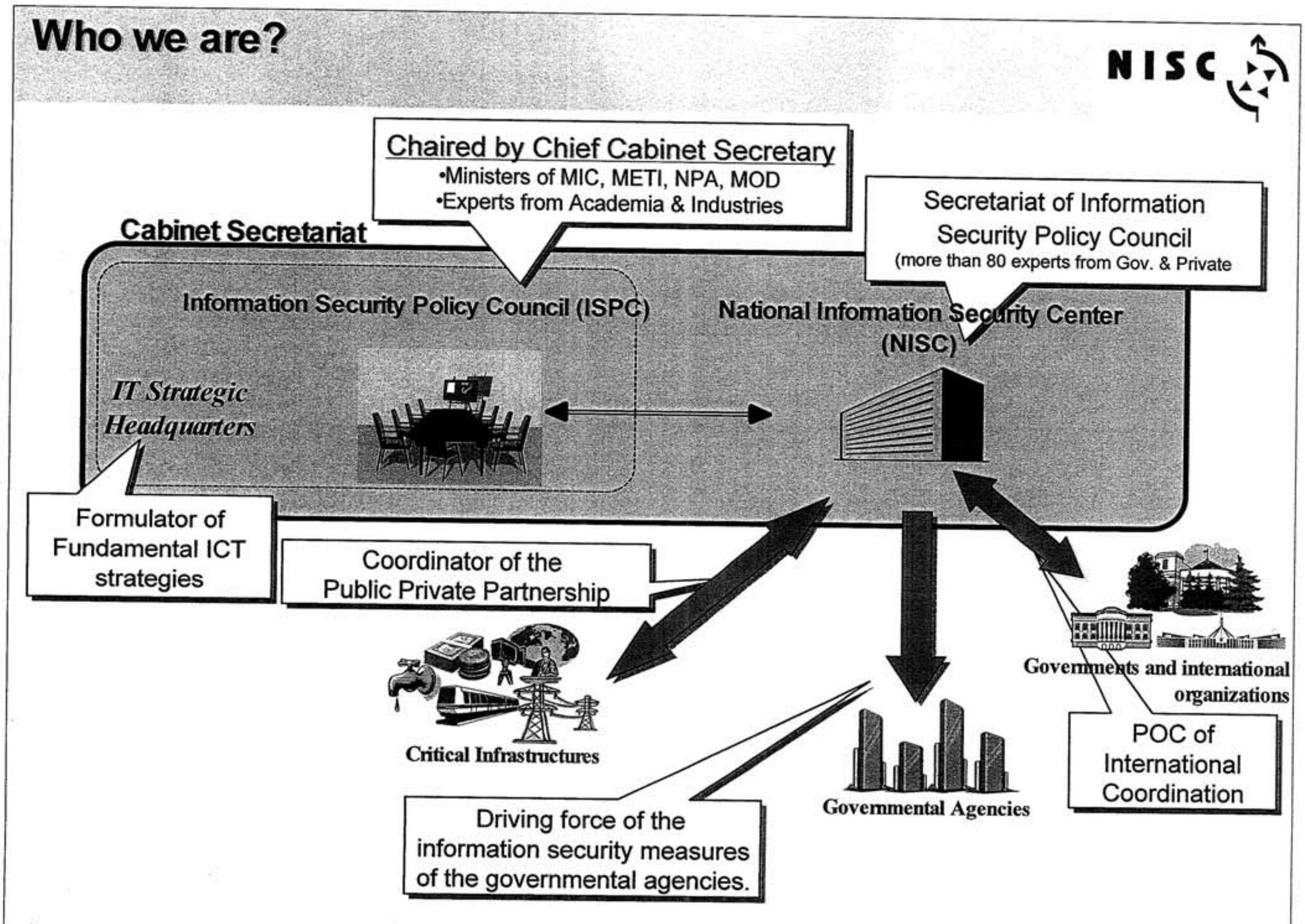
http://www.nisc.go.jp/

Development of information security policies of the Cabinet Secretariat (Outlook after 2000)

NISC

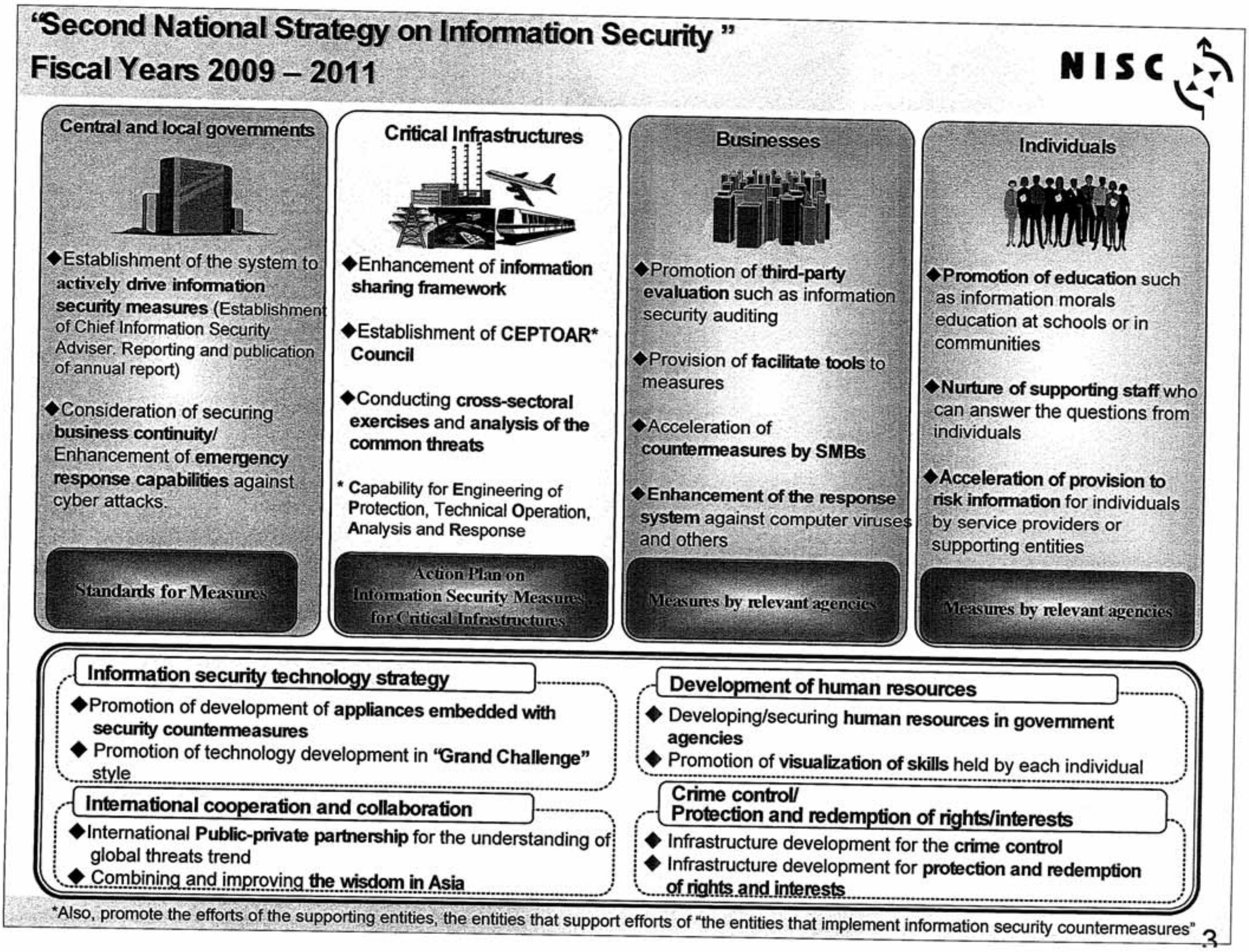

Series of government websites defacements
2000.01
9/11 Terrorist Attacks on U.S.
2001.09
Blaster worm outbreak
2003.08
lopment of nization/ System
opment of ework/
lopment hance ures
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
Era of government trial and error
1st implementation stage of the measures by the Cabinet Secretariat
Preparation period before 2nd phase
2nd implementation stage of measures
Enhancement of Measures
Framework/ tools to promote measures
Organization established in a month
2006.02
First National Strategy on Information Security
Second National Strategy on Information Security
2000.07
Guidelines for IT Security Policy
Standards for Information Security Measures for the Central Government Computer Systems
2005.12
Standards for Measures (Revised)
2000.12
Special Action Plan on Countermeasures against Cyber-terrorism on Critical Infrastructure
2005.04
Action Plan on Information Security Measures for Critical Infrastructures
Second Action Plan
Organization System
IT Security Office, Cabinet Secretariat
② National Information Security Center (NISC)
③ Information Security Policy Council (ISPC)
2000.02
2004.04
① Establishment of Advisor on Information Security
2005.05
2008.04
④ Start of GSOC operations

Who we are?


NISC
Chaired by Chief Cabinet Secretary
•Ministers of MIC, METI, NPA, MOD
•Experts from Academia & Industries
Secretariat of Information Security Policy Council
(more than 80 experts from Gov. & Private
Cabinet Secretariat
Information Security Policy Council (ISPC)
National Information Security Center (NISC)
IT Strategic Headquarters
Formulator of Fundamental ICT strategies
Coordinator of the Public Private Partnership
Critical Infrastructures
Governmental Agencies
Governments and international organizations
POC of International Coordination
Driving force of the information security measures of the governmental agencies.

* MIC: Ministry of Internal Affairs and Communications, METI: Ministry of Economy, Trade and Industry, NPA: National Police Agency, MOD: Ministry of Defense

"Second National Strategy on Information Security" Fiscal Years 2009 – 2011



Central and local governments

◆Establishment of the system to **actively drive information security measures** (Establishment of Chief Information Security Adviser. Reporting and publication of annual report)

◆Consideration of securing **business continuity/** Enhancement of **emergency response capabilities** against cyber attacks.

Standards for Measures

Critical Infrastructures

◆Enhancement of **information sharing framework**

◆Establishment of **CEPTOAR* Council**

◆Conducting **cross-sectoral exercises** and **analysis of the common threats**

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

Action Plan on Information Security Measures for Critical Infrastructures

Businesses

◆Promotion of **third-party evaluation** such as information security auditing

◆Provision of **facilitate tools** to measures

◆Acceleration of **countermeasures by SMBs**

◆**Enhancement of the response system** against computer viruses and others

Measures by relevant agencies

Individuals

◆**Promotion of education** such as information morals education at schools or in communities

◆**Nurture of supporting staff** who can answer the questions from individuals

◆**Acceleration of provision to risk information** for individuals by service providers or supporting entities

Measures by relevant agencies

Information security technology strategy

◆Promotion of development of **appliances embedded with security countermeasures**

◆ Promotion of technology development in **"Grand Challenge"** style

International cooperation and collaboration

◆International **Public-private partnership** for the understanding of global threats trend

◆ Combining and improving **the wisdom in Asia**

Development of human resources

◆ Developing/securing **human resources in government agencies**

◆ Promotion of **visualization of skills** held by each individual

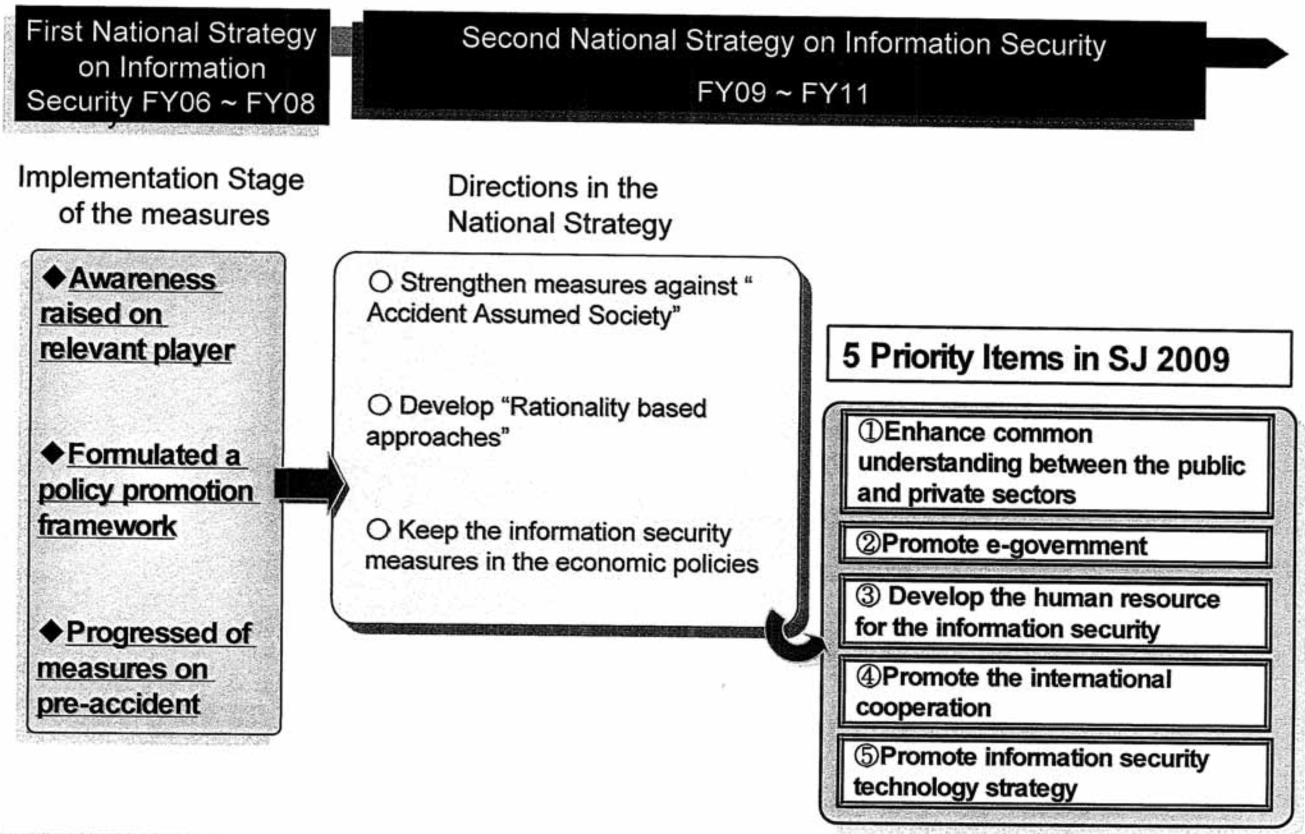
Crime control/ Protection and redemption of rights/interests

◆ Infrastructure development for the **crime control**

◆ Infrastructure development for **protection and redemption of rights and interests**

*Also, promote the efforts of the supporting entities, the entities that support efforts of "the entities that implement information security countermeasures"

Advanced National Strategy on Information Security



First National Strategy on Information Security FY06 ~ FY08

Second National Strategy on Information Security FY09 ~ FY11

Implementation Stage of the measures

- ◆**Awareness raised on relevant player**
- ◆**Formulated a policy promotion framework**
- ◆**Progressed of measures on pre-accident**

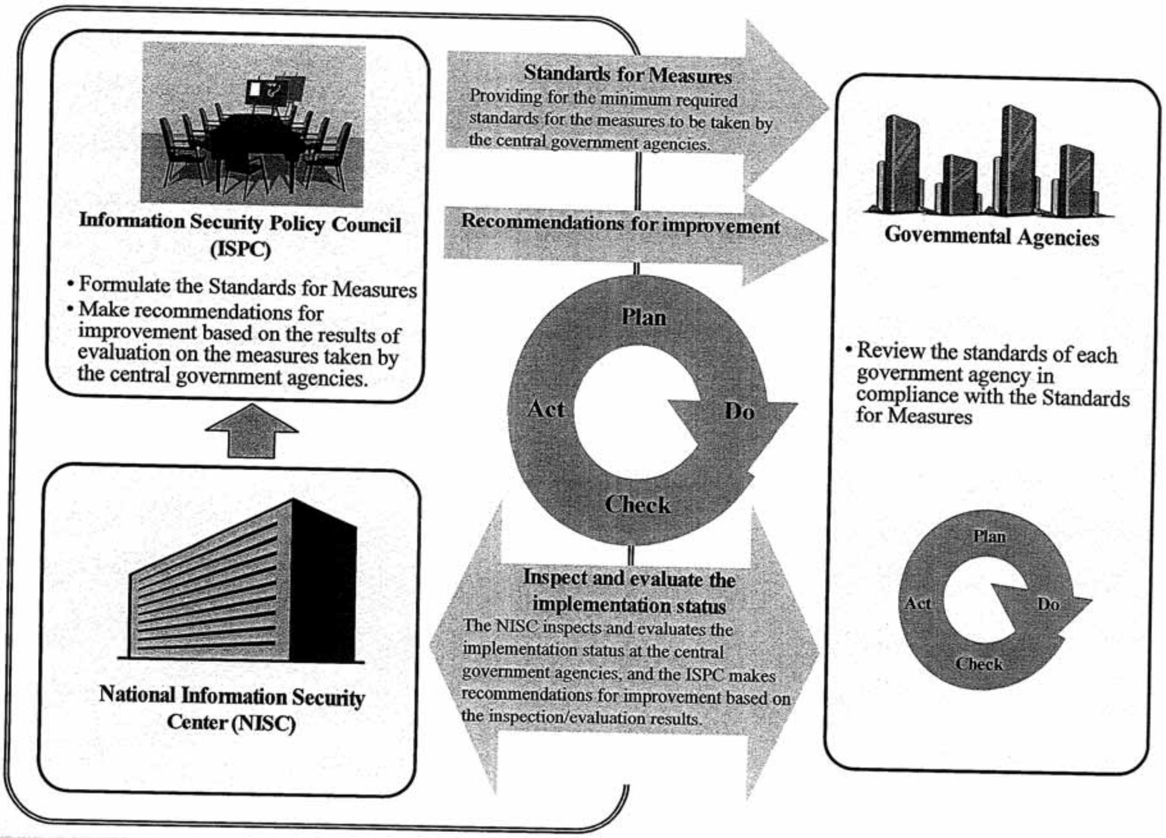
Directions in the National Strategy

- ○ Strengthen measures against " Accident Assumed Society"
- ○ Develop "Rationality based approaches"
- ○ Keep the information security measures in the economic policies

5 Priority Items in SJ 2009

- **①Enhance common understanding between the public and private sectors**
- **②Promote e-government**
- **③ Develop the human resource for the information security**
- **④Promote the international cooperation**
- **⑤Promote information security technology strategy**

Improvement based on PDCA cycle for the government agencies



Information Security Policy Council (ISPC)

- Formulate the Standards for Measures
- Make recommendations for improvement based on the results of evaluation on the measures taken by the central government agencies.

National Information Security Center (NISC)

Standards for Measures
Providing for the minimum required standards for the measures to be taken by the central government agencies.

Recommendations for improvement

Inspect and evaluate the implementation status
The NISC inspects and evaluates the implementation status at the central government agencies, and the ISPC makes recommendations for improvement based on the inspection/evaluation results.

Governmental Agencies

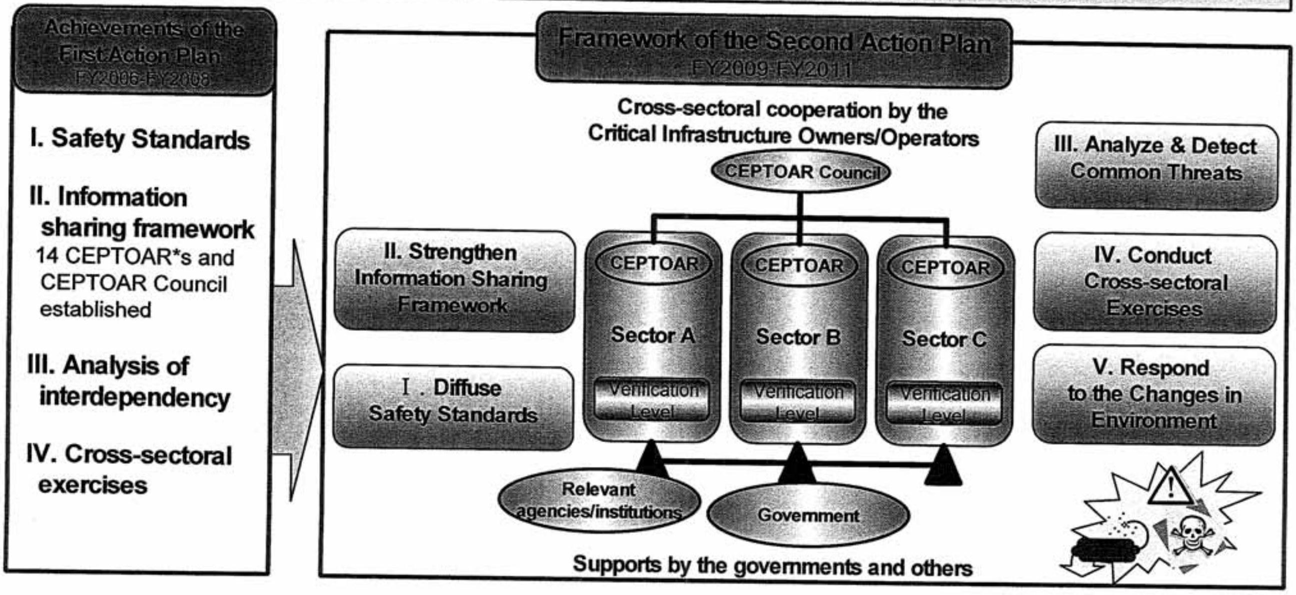
- Review the standards of each government agency in compliance with the Standards for Measures

Overview of "the Second Action Plan on Information Security Measures for Critical Infrastructures"

NISC

- **Preventing IT malfunctions from affecting the lives of citizens and the socioeconomic activities** by Public Private Partnership
- Setup of **a verification level** in each critical infrastructure service*
- Improve the capabilities **to respond to the changes in the environment**

* 10 sectors; Information and communications, Finance, Aviation, Railways, Electricity, Gas, Governments and governmental services (incl. local governments), Medical services, Water services, and Logistics



Achievements of the First Action Plan FY2006-FY2008

I. Safety Standards

II. Information sharing framework
14 CEPTOAR*s and CEPTOAR Council established

III. Analysis of interdependency

IV. Cross-sectoral exercises

Framework of the Second Action Plan FY2009-FY2011

Cross-sectoral cooperation by the Critical Infrastructure Owners/Operators

CEPTOAR Council

II. Strengthen Information Sharing Framework

Ⅰ. Diffuse Safety Standards

CEPTOAR — Sector A — Verification Level

CEPTOAR — Sector B — Verification Level

CEPTOAR — Sector C — Verification Level

III. Analyze & Detect Common Threats

IV. Conduct Cross-sectoral Exercises

V. Respond to the Changes in Environment

Relevant agencies/institutions

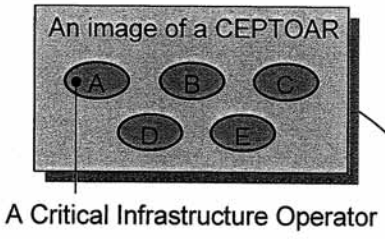
Government

Supports by the governments and others

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

CEPTOARs and the CEPTOAR Council

NISC

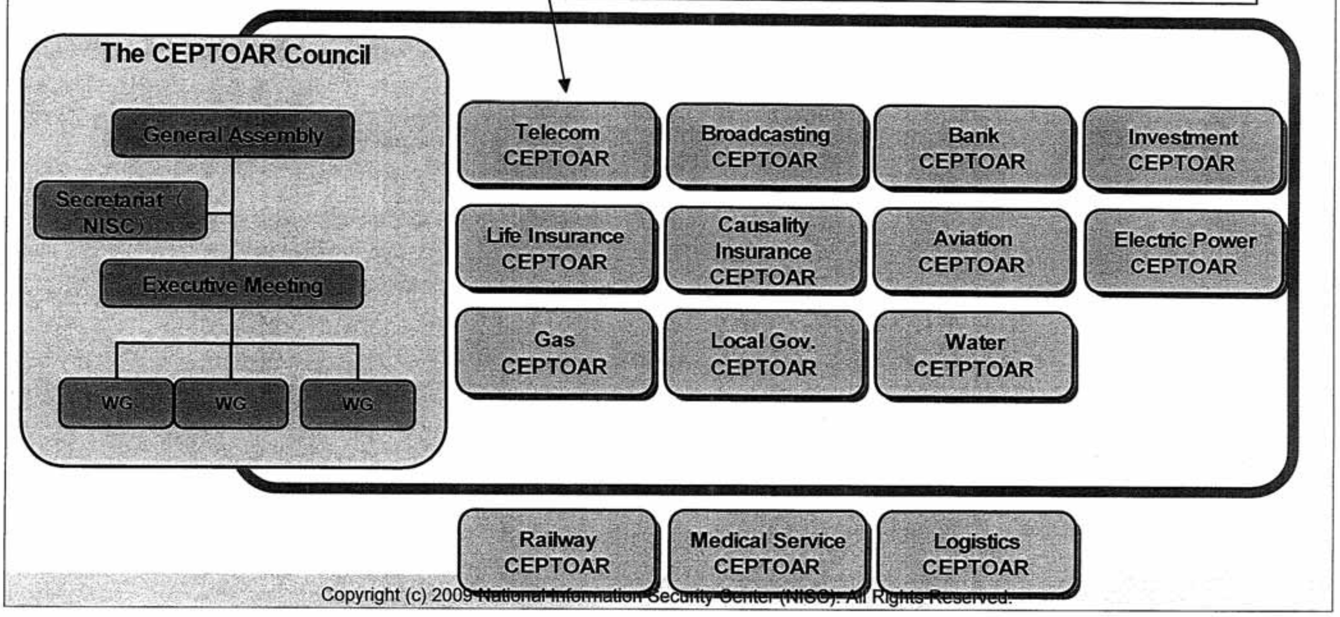


An image of a CEPTOAR

A Critical Infrastructure Operator

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

The CEPTOAR Council:(2009.2~)
the private organization for voluntary information sharing formed by CEPTOARs



The CEPTOAR Council

General Assembly

Secretariat（NISC）

Executive Meeting

WG — WG — WG

Telecom CEPTOAR

Broadcasting CEPTOAR

Bank CEPTOAR

Investment CEPTOAR

Life Insurance CEPTOAR

Causality Insurance CEPTOAR

Aviation CEPTOAR

Electric Power CEPTOAR

Gas CEPTOAR

Local Gov. CEPTOAR

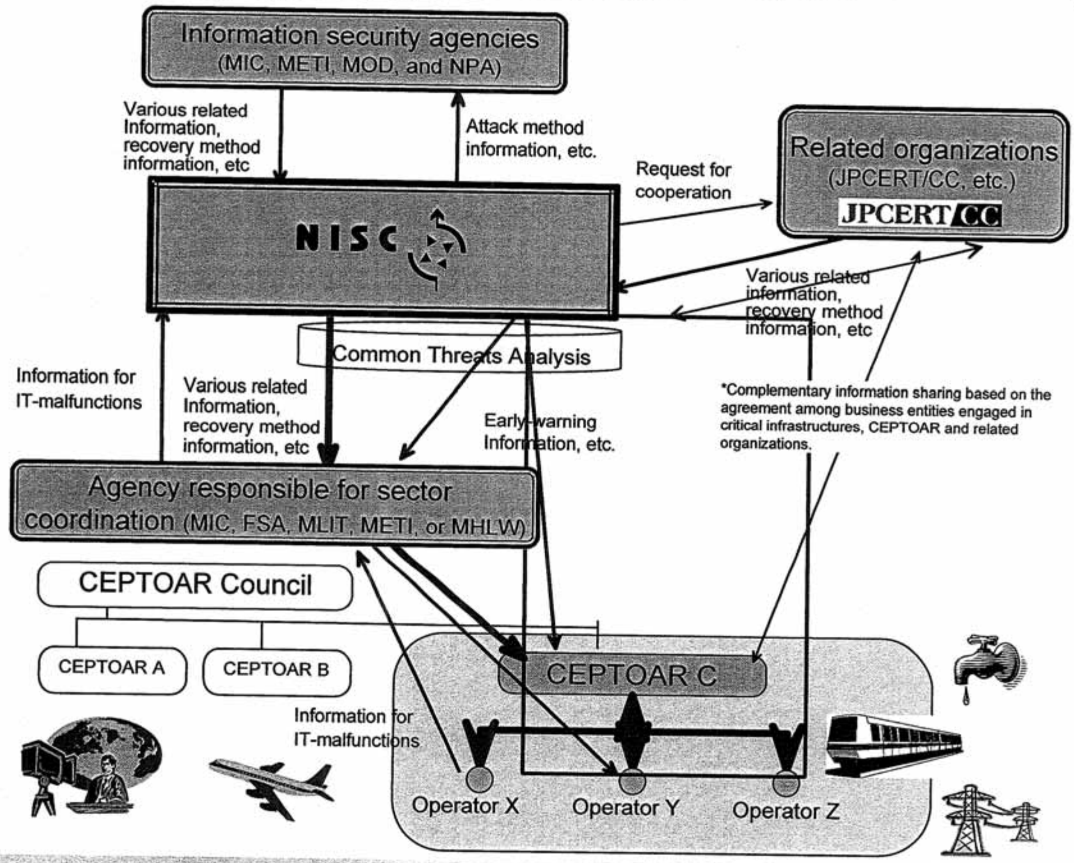
Water CETPTOAR

Railway CEPTOAR

Medical Service CEPTOAR

Logistics CEPTOAR

Structure for Effective Information Sharing



Information security agencies (MIC, METI, MOD, and NPA)

Various related Information, recovery method information, etc

Attack method information, etc.

NISC

Request for cooperation

Related organizations (JPCERT/CC, etc.)

JPCERT/CC

Various related information, recovery method information, etc

Common Threats Analysis

Information for IT-malfunctions

Various related Information, recovery method information, etc

Early-warning Information, etc.

*Complementary information sharing based on the agreement among business entities engaged in critical infrastructures, CEPTOAR and related organizations.

Agency responsible for sector coordination (MIC, FSA, MLIT, METI, or MHLW)

CEPTOAR Council

CEPTOAR A

CEPTOAR B

CEPTOAR C

Information for IT-malfunctions

Operator X

Operator Y

Operator Z

Conducting Cross-Sectoral Exercises

The First National Strategy on Information Security

<2006>
Building Public Private Partnership

Seminar
Understood exercise concepts, scenarios, and procedures

Tabletop Exercise
Discussed response to a hypothetical disaster in a meeting style

<2007>
Enhancing Partnership Mechanisms

Functional Exercise
Adopted a DDoS attack scenario and simulated the response by email

<2008>
Improving Efficiency of Partnership

Functional Exercise
In the realistic situation in which the cause of the incident was hidden, identified the cause using information sharing and proceeded to recover and continue the service

Lessons learned about procedures for cross-sectoral exercises

The Second National Strategy on Information Security

Improving Cross-Sectoral Measures for Critical Infrastructure Protections

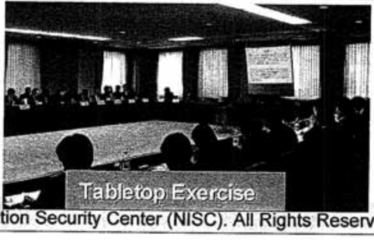
Target

Sharing the understanding of cross-sectoral threats	Enhancing response in one's sector by knowing response in other sectors	Achieving more effective information sharing between public and private sectors

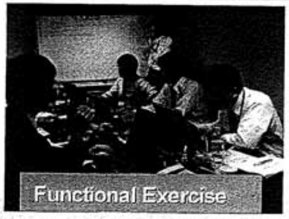
Expectations

Policies for Cross-Sectoral Exercises

1. Plan scenarios, processes and conduct exercises
2. Recognize the progress of recovery processes and business continuity plans and share them with participants
3. Improve scenario development
4. Share lessons learned about exercise methods



Tabletop Exercise



Functional Exercise