# Information Security Policies in Japan

Mabito YOSHIDA

IT Security Office,
Information and Communications Policy Bureau,
Ministry of Internal Affairs and Communications (MIC)

29 June 2005

# Contents

MIC
Ministry of Internal Affairs and Communic

# I The Growing Telecommunications Market and the Pressing Need to Provide Information Security

# Importance of Information Security

**Progress of IT in Social and Economic Activity**

Expansion of e-Commerce market scale (in 2003)

- Business-to-business (B to B) : 77.43 trillion (increase of 67.2% on the previous year)
- Business-to-consumer (B to C) : 4.43 trillion (increase of 65% on the previous year)

**Spread and Development of the Internet**

Population penetration rate :
over 60% (79.5 million) (as of Dec. 2004)

Number of broadband subscribers :
18.6 million subscribers (as of Dec. 2004)

**Increased Dependency on ICT**

**Security Breaches** → **Serious Damage**

# The threats we face to Internet security

- method of attack

  → more complicated or sophisticated

- damage

  → more widespread and worsening

- new threats

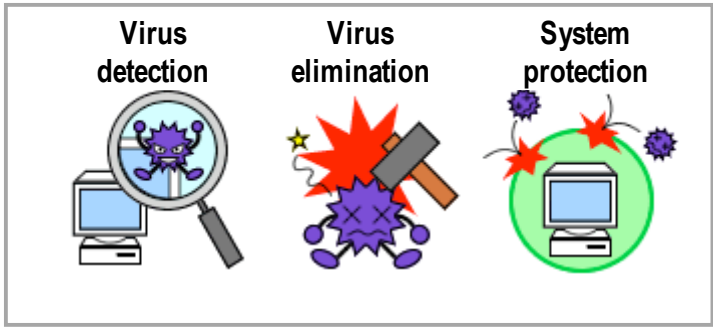
  → botnet, phishing, pharming…..

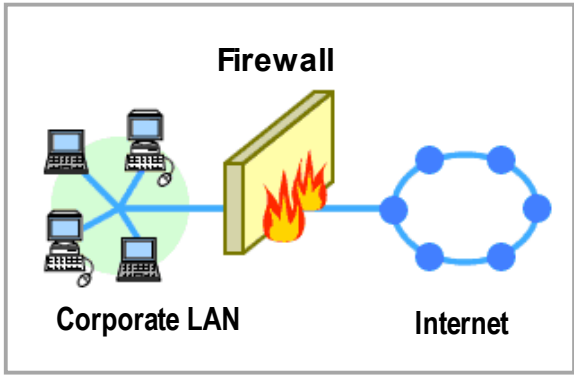
- motive

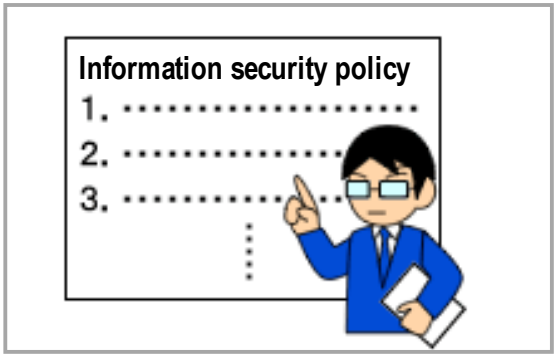
  → profit

# Implementation of Security Measures by Corporations

- Virus measures
  - 99.8% of companies have implemented virus measures
- Measures against illegal access
  - 88.8% of companies have implemented a firewall
  - 11.2% of companies have implemented client-side firewall software
- Drawing-up security policies
  - "Already implemented" 35.6%
  - "Currently devising" 20.8%
  - "Investigating how to draw up" 32.9%




Source: MIC "Survey of Actual Trends on Information Security" (July 2004)

# Implementation of Security Measures by individual users

- Anti-virus
  - 56.7% of individual users were using anti-virus software.
    (not using: 34.8%, do not know about anti-virus software: 8.5%)
  - Reasons for not using anti-virus software (multiple response)
    (1) Expensive: 42.2%  (2) Do not believe they will be infected: 36.7%
    (3) License period has expired: 10.2%

- OS updates (for Microsoft Windows )
  - Users who do not know about Windows update: 31%
  - Users who know about Windows updates: 69%
    Those who install as soon as the distribution is ready: 55.6%
  - Reasons for not doing Windows updates (multiple response)
    (1) Bothersome: 38%  (2) Not really necessary: 37.5%
    (3) Taking time to download: 35%

**From the 2nd Survey report concerning with telecommunications service monitor in 2003 (April 2004)**

MIC
Ministry of Internal Affairs and Communic

# II Promotion of Information Security Policies by the Government

# Framework of Information Security Policies

## 1. IT Basic Law (2000)

Article 22 – In formulating measures on the construction of an advanced information and telecommunications network society, it is necessary to **guarantee safety and reliability of advanced information and telecommunications networks**, protect personal information data and implement other necessary measures to ensure that the public can use advanced information and telecommunications networks with a sense of security.

## 2. e-Japan Strategy II (July 2003)

- Development of next-generation telecommunications infrastructures
- **Development of safe and secure IT environment**
- Promotion of R&D to create next-generation knowledge
- Promotion of IT human resources development and advancement of learning
- Development of new international relationships via IT technologies

## 3. e-Japan II priority programs 2004 (June 2004)

## 4. IT Policy Package (Feb 2005)

# Committee for Essential Issues on Information Security

**period**

July 2004 - May 2005

**purpose**

Formulating of national strategy on information security by collecting opinions of experts and proposing it to IT Strategy Headquarters.

**tasks**

**1. To review the framework of overall policies on information security**

**2. To improve Government information security**

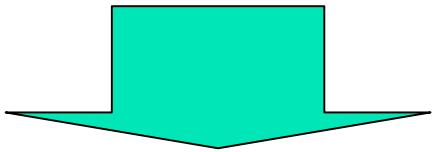
**3. To improve the information security of critical infrastructures**

**Composition**

| | | |
|---|---|---|
| (**Chairman**) | Akinobu KANASUGI | President, NEC |
| (**Members**) | Yasuhiko ITO | Senior Vice President (CTO), KDDI |
| | Shigeki GOTO | Professor, Waseda University |
| | Jitsuro TERASHIMA | President, Mitsui Global Strategic Studies Institute |
| | Naoshi NAKAMURA | Vice-President, NTT DATA |
| | Jun MURAI | Professor, Keio University |

# First Recommendations (November 2004)

- To address information security issues, the government should establish:
  - ① Basic strategies on information security policy and enforcement authority
  - ② More effective cordination within the government to compile and enforce measures to ensure information security in government networks



- The following two new organizations should be set up:
  - ① Information Security Policy Meeting
  - ② National Information Security Center (NISC)

# Information Security Policy Council

- Establishment: 30th May 2005
- Member:

  Chief Cabinet Secretary (chair)  Minister of State for IT (acting chair)

  Chairman of the National Public Safety Commission

  Minister of State for Defense  Minister of MIC  Minister of METI

  Intellectuals in the private sector (6)
- Missions:

(1)To develop basic strategy (mid-and-long term plan, annual plan) for the information security policy

(2)To undertake prior assessment of information security policy based on the basic strategy

(3)To undertake ex post facto assessment of information security policy and its publication

(4)To develop safety guidelines for information security that are uniform throughout government

(5)To recommend information security policies of each ministries based on the government-wide safety guideline

(6)To cope with respond to emergency incidents in the middle of a year

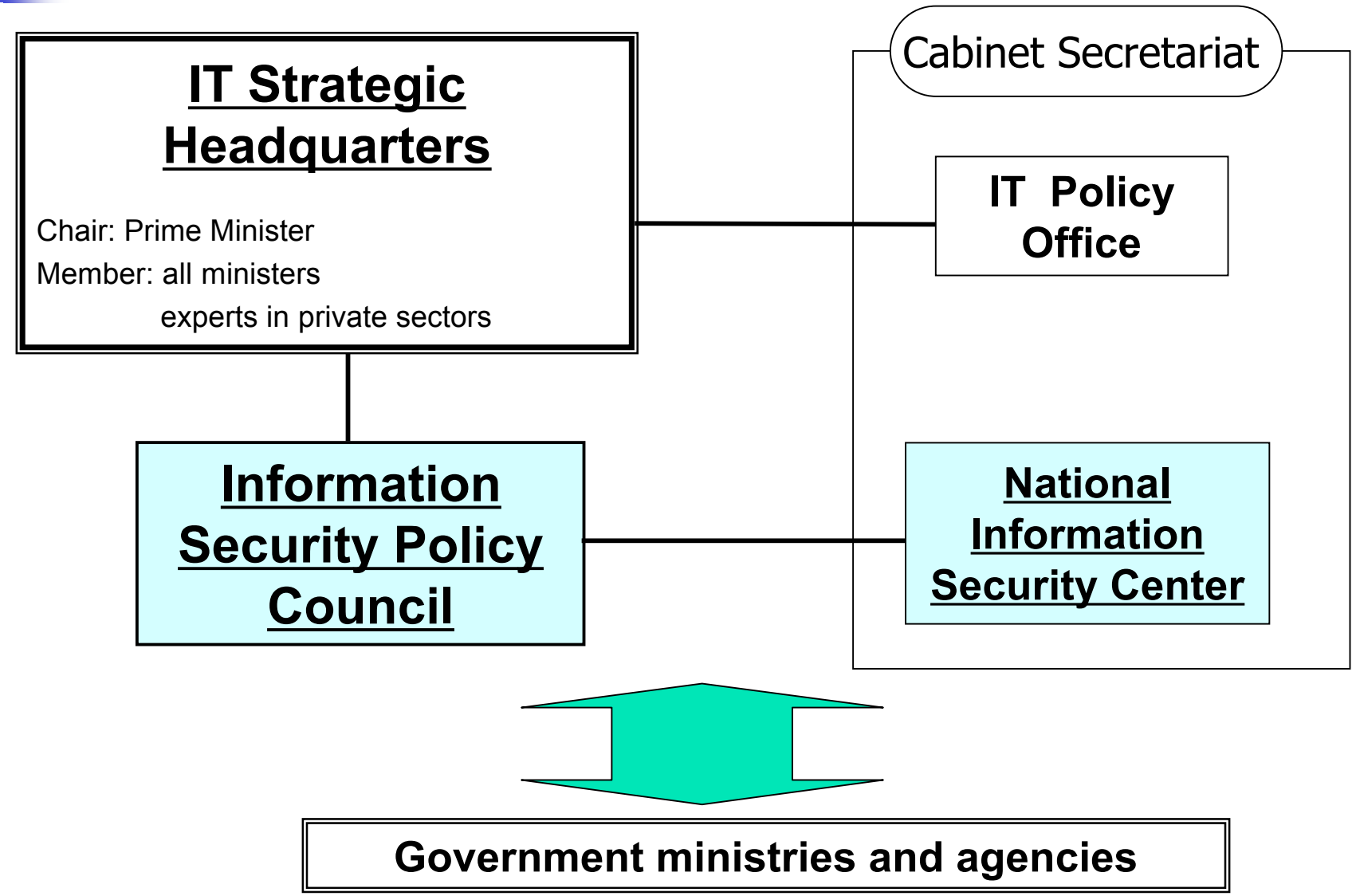
# National Information Security Center (NISC)

- Establishment: 25 April 2005
- Member:

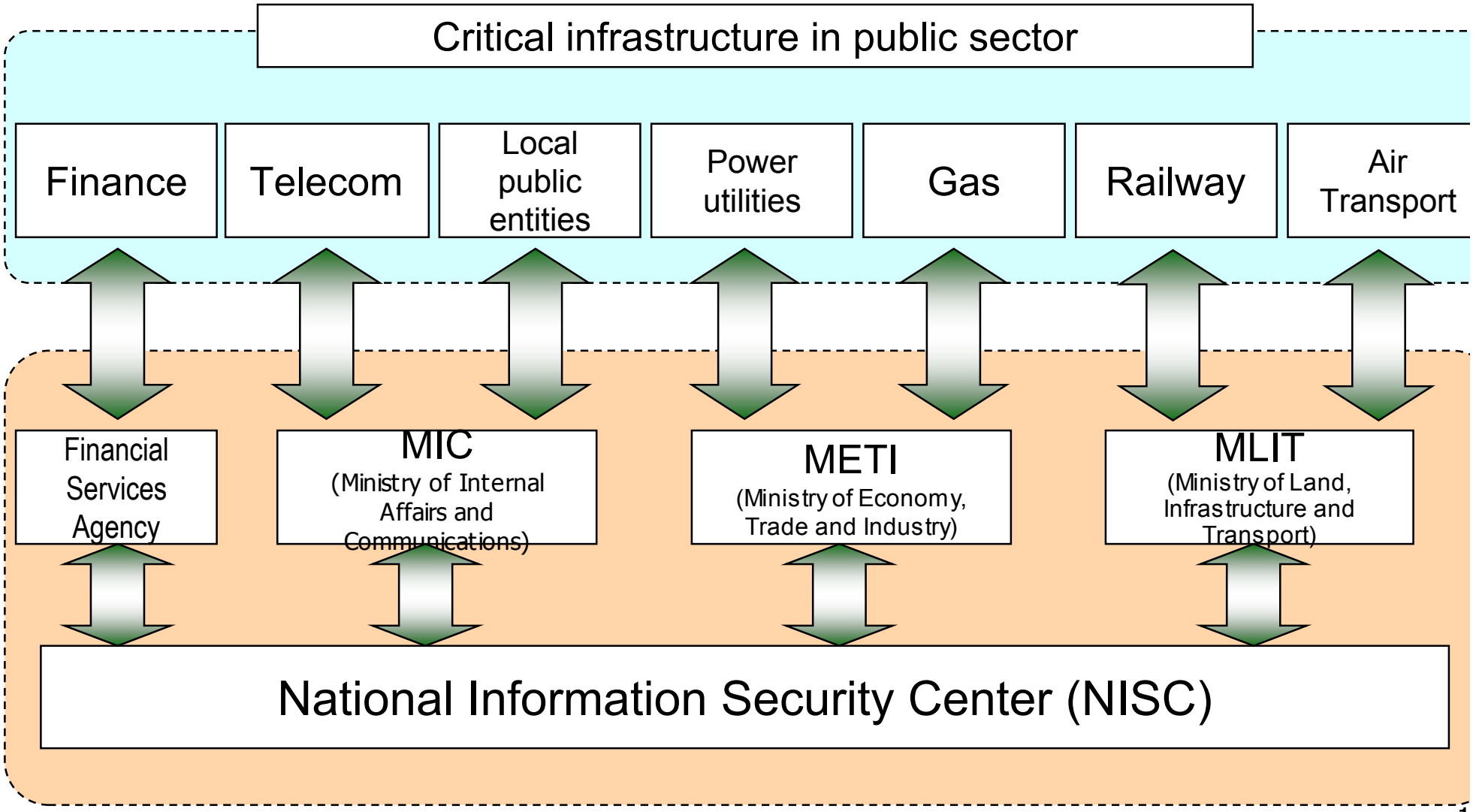
  Director General (interlocking of the Assistant Chief Cabinet Secretary)
  Deputy Director General (2)
  Advisor on information security
  Staff: 35 (→60 , in 2006)
- Mission:

  (1) Planning a basic strategy for information security policy
  (2) Promoting comprehensive measures on information security concerning government organizations
  (3) Supporting these government organizations in an appropriate way when information security incidents occur
  (4) Strengthening information security of critical infrastructures

# New government structure for information security



# Liaison/Collaboration System for Critical Infrastructure



# Second Recommendations (1/2)

## Expansion of "critical infrastructure"

(1) "Medical service", "water" and "distribution " should be added to the existing definition of "critical infrastructure" (finance, communications, local authorities, electricity, gas, rail transport and air transport).

## Expansion of "threats"

(2) Unintentional factors like human error and natural disasters should be regarded as "threats" as well as cyber attacks.

# Second Recommendations (2/2)

Development a new information security framework

(3) Strengthening of cross-sectoral information security

(ex) cross-sectoral interdependency analysis

(4) Strengthening of framework for information sharing and providing among critical infrastructures

(ex) ・To establish information sharing system like ISAC (Information Sharing & Analysis Center) in each sector.

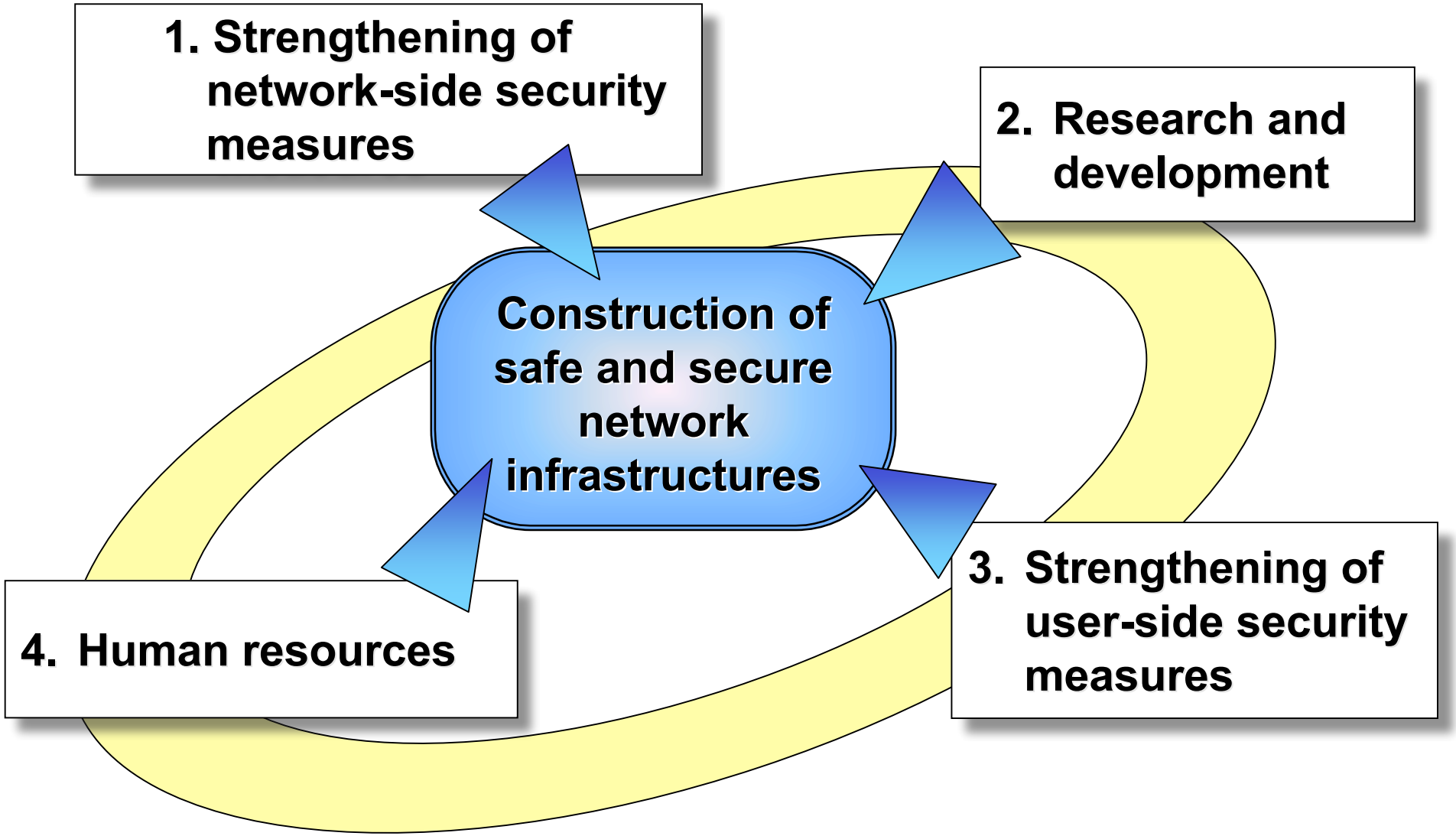
・To promote cross-sectoral information sharing

(5) Implementation of comprehensive and cross-secotral exercise on critical infrastructure protection

MIC
Ministry of Internal Affairs and Communic

# III Information Security Policies in the Telecommunications Field

# Overview of Information Security Policies in the Telecommunications Field



# Telecom-ISAC Japan

■ Established: July 2002

■ Purpose:
To collect and analyze information on incidents occurred in the service infrastructure of telecommunications operators, and to share the results within the industry.

■ Function:
(1) Reporting and discussing system vulnerabilities
(2) Providing countermeasures and their best practices
(3) Providing Information about threats, e.g. cyber attacks/crimes, and their damages

■ Members:
NTT Communications, KDDI, Japan Telecom, PoweredCom, NEC, IIJ, Nifty, Yahoo!, Panasonic, Hitachi, Yokogawa Electric, Oki Electric

#"ISAC" originally means "Information Sharing and Analysis Center".

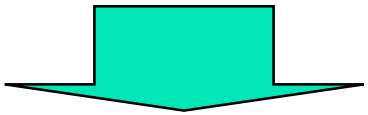
## Enhancement of Information Security Manegemnt in Telecom field

**(Present)**

- **Safety and Security Standards for Information and Telecommunications Networks (Ministerial notification)**

  ---A basic and general guideline

  Including some information security items, but not specific



- **MIC is currently considering the development of new standards/guidelines based on the revision work on ITU-T X.1051 (ISMS-T)**

# Revision work on ISMS-T (X.1051) in Japan

## ISO/IEC JTC1/SC27

ISO/IEC 17799

ISMS General
(e.g. BS 7799 Part 2 )

Objective

Control

X.1051
(ISMS-T)

Objective

Control

**Telecom Implementation Requirements**

## ITU-T Question7/SG17

**Revision of X.1051 has been started in Japan from March 2005**

**Based on:**

* **ISO/IEC 17799 (2005)**
* **Additional Requirements for Telecom (e.g. lawful constraint)**

- Security policy (New)
- Organising information security
- Asset management
- Human resources security
- Physical & environmental Security
- Communications & operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management (New)
- Business continuity management (New)
- Compliance (New)

# Research and Development of Security Technologies

(1) Enhancement of capabilities for analyzing influence of viruses on network

(2) Strengthening R&D on technologies for ensuring security of telecommunications infrastructures

- Wide-area monitoring system technologies and high-precision trace back technology
- Countermeasure against Botnet

(3) Establishment of bases for security technology

- Establishment of the Information Security Center at the National Institute of Information and Communications Technology (NICT)

# Promoting awareness of user-side security

## ○ Provision of Security Information on MIC website


Internet security information has been provided on the MIC website since March 2003.

## ○ Internet Access Service "Safe and Security Mark"


In dealing with the system of Internet Access Service, the "Safe and Security Mark" is provided to ISPs notifying security information to their users and enlightening their users.

## ○ Tax Deduction System

Tax deductions for private companies that introduce systems for preventing illegal access to their networks.

# Promotion of Human Resources Development

- Japan still needs more than **120,000 experts**

(Source) Telecommunications Software Forum Report (Dec. 2003)

**Measures (examples)**

## ○ Human resources development through certification systems

- Since 2001, a subject on information security has been added to the national examination for “Chief Telecommunications Engineer's Licenses for Transmission, Switching Technology and Line Technology ”.
- Since 2001, “Network Information Security Manager (NISM)” program has been founded by 7 business associations (including the Telecommunications Carrier Association), as a private security certification.

## ○ Support programs for human resources development

- Setting up programs to grant subsidies to organizations that promote human resources development in the telecommunications field in 2001.

MIC
Ministry of Internal Affairs and Communica

world summit
on the information society
Geneva 2003 - Tunis 2005

# Thank you!