Ministry of Economy, Trade and Industry

The Challenge of Raising Business Value through Objective Evaluation of IT Security, & Japan’s IT Security Policy

September 28, 2005

TANABE, Takefumi
Deputy Director, Office of IT Security Policy
Ministry of Economy, Trade and Industry
JAPAN

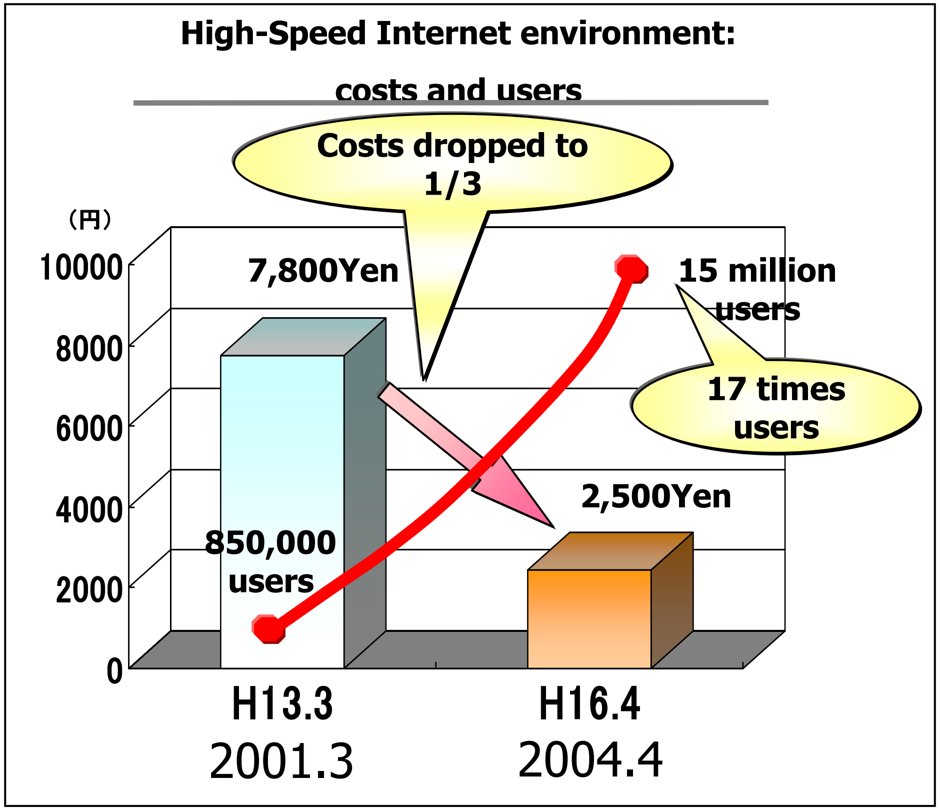
Contents

- Background
- Current situation of Japan’s IT security policy in throughout the government
- METI’s IT security policy
  - Technology -- Common Criteria / Government Procurement
  - Management -- Information Security Governance

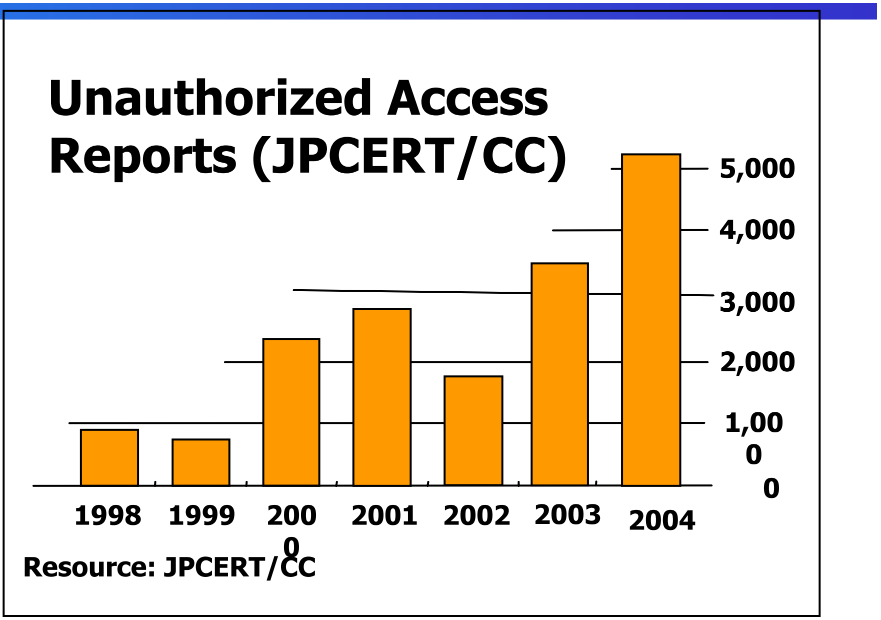
Background

METI

Dissemination of IT

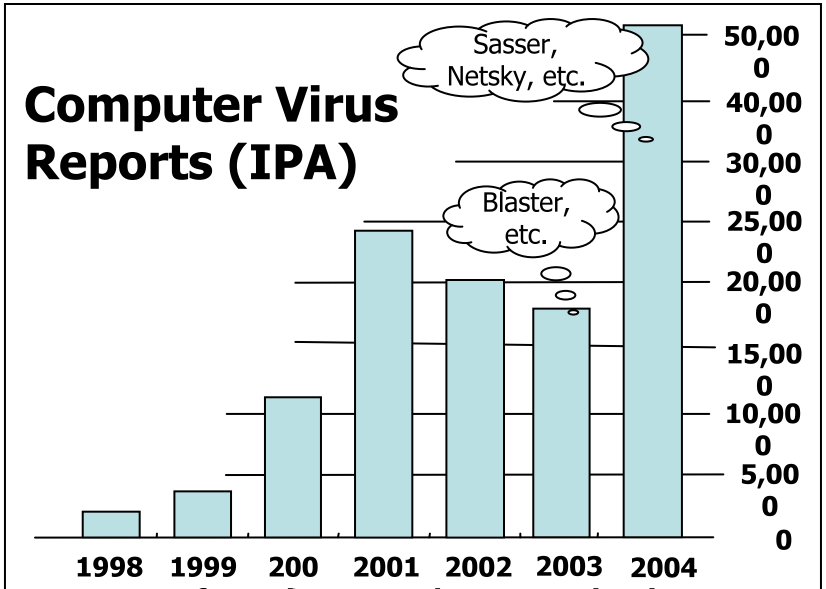


High-Speed Internet environment: costs and users



Unauthorized Access Reports (JPCERT/CC)

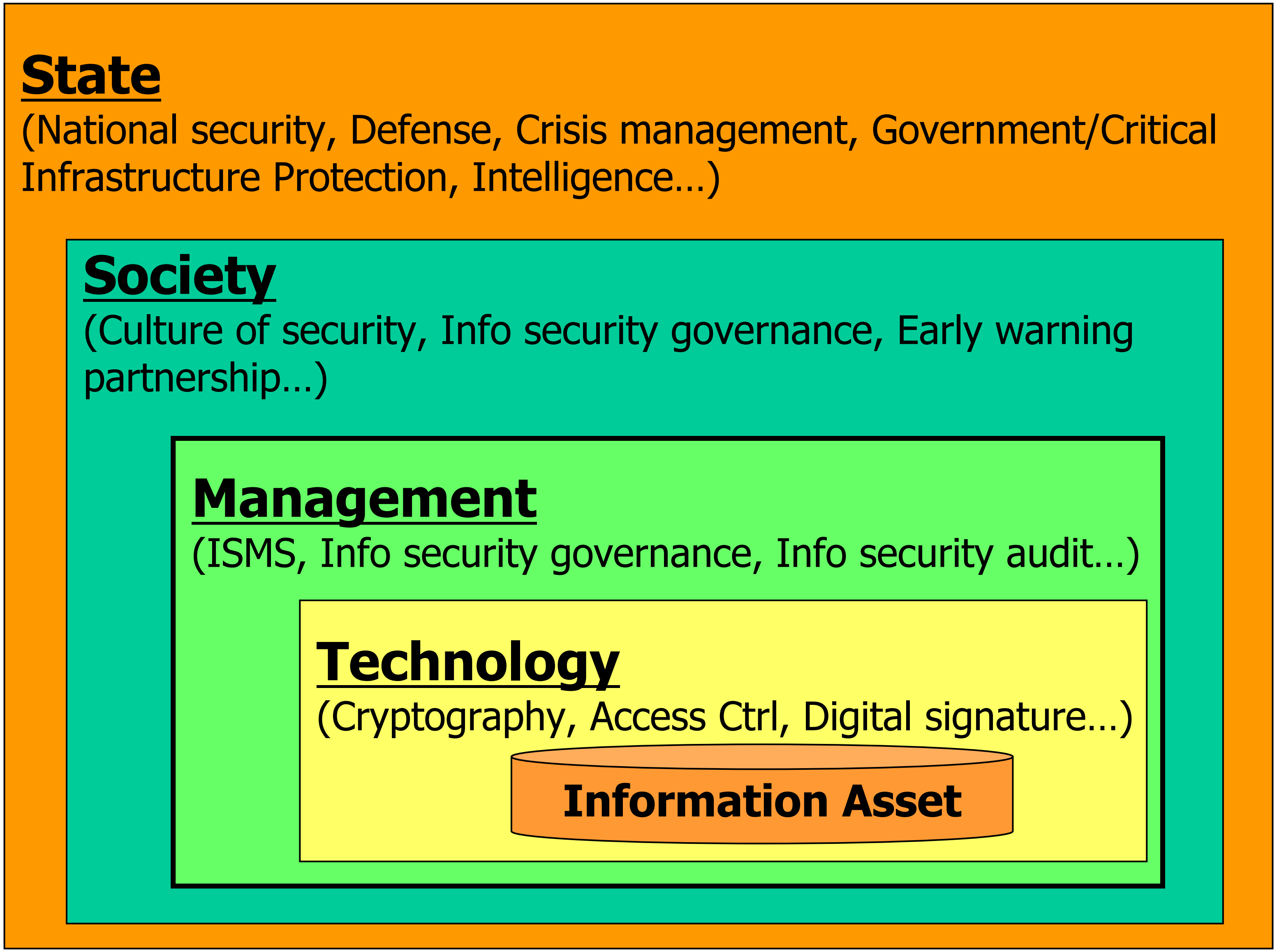
Resource: JPCERT/CC



Computer Virus Reports (IPA)

Resource: Information Promotion Agency (IPA)

The Layers of IT Security Measures



State

(National security, Defense, Crisis management, Government/Critical Infrastructure Protection, Intelligence…)

Society

(Culture of security, Info security governance, Early warning partnership…)

Management

(ISMS, Info security governance, Info security audit…)

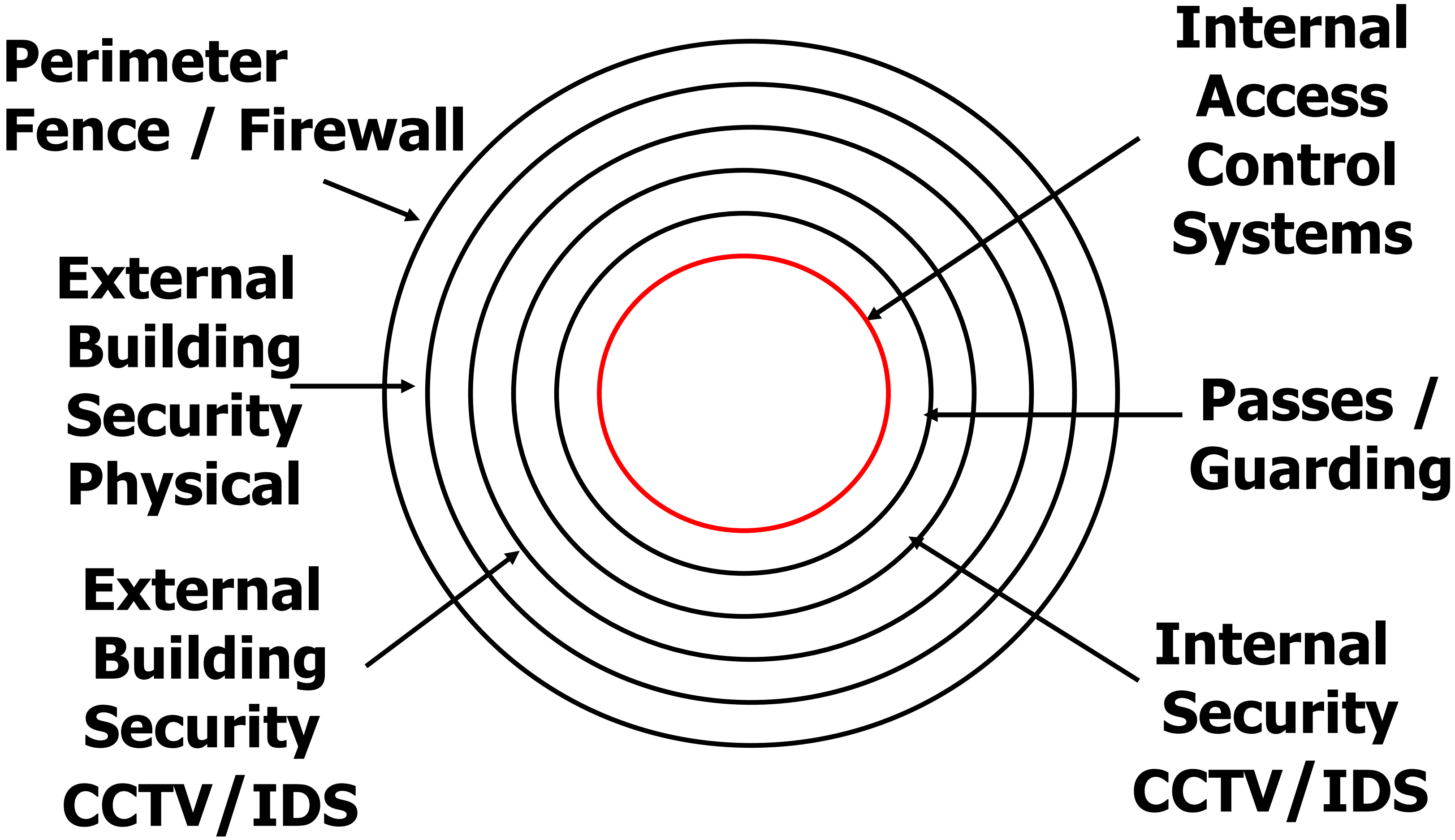
Technology

(Cryptography, Access Ctrl, Digital signature…)

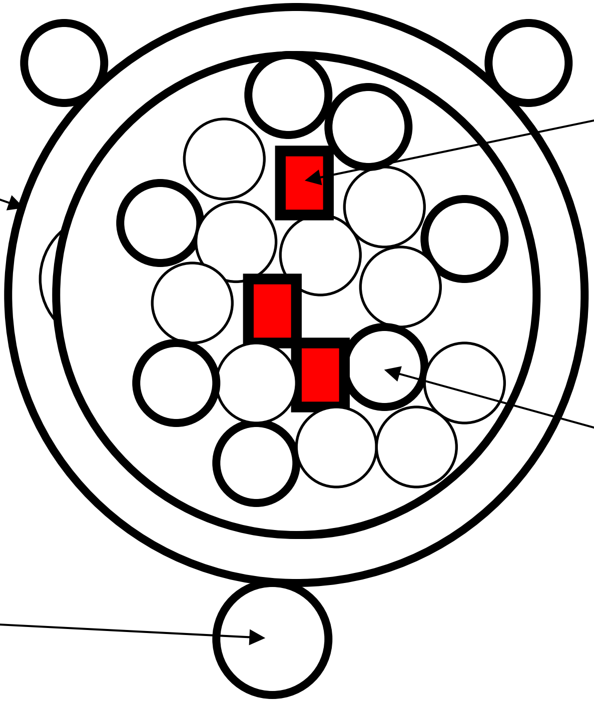
Information Asset

Security Principles: ‘The Onion Skin’

METI


Perimeter Fence / Firewall
External Building Security Physical
External Building Security CCTV/IDS
Internal Access Control Systems
Passes / Guarding
Internal Security CCTV/IDS

Security Principles: ‘The Pomegranate’



Perimeter defence

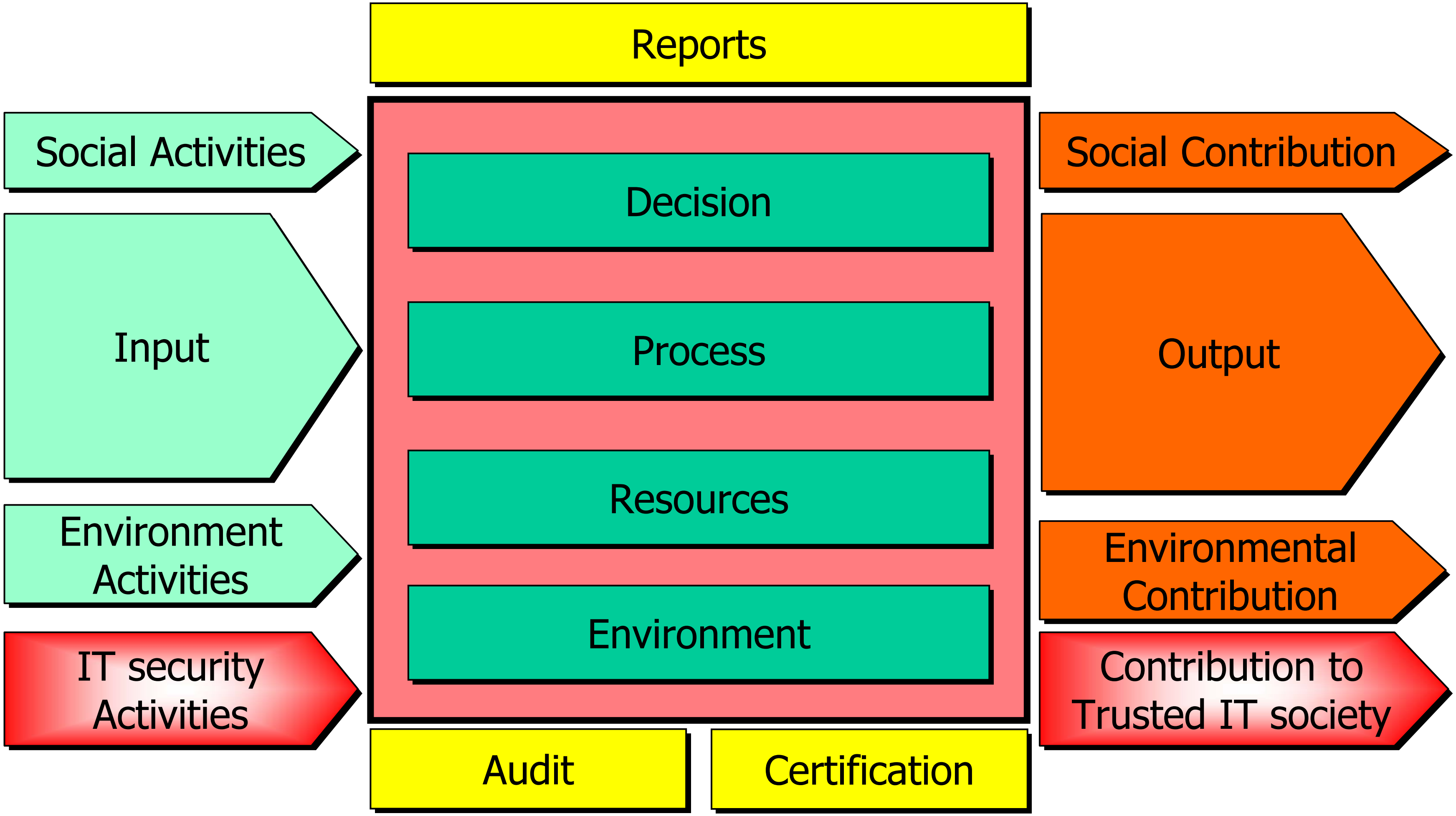
Top secret

Secret

High risk

Business Environment Surrounding Management

METI



Reports

Social Activities

Input

Environment Activities

IT security Activities

Decision

Process

Resources

Environment

Social Contribution

Output

Environmental Contribution

Contribution to Trusted IT society

Audit

Certification

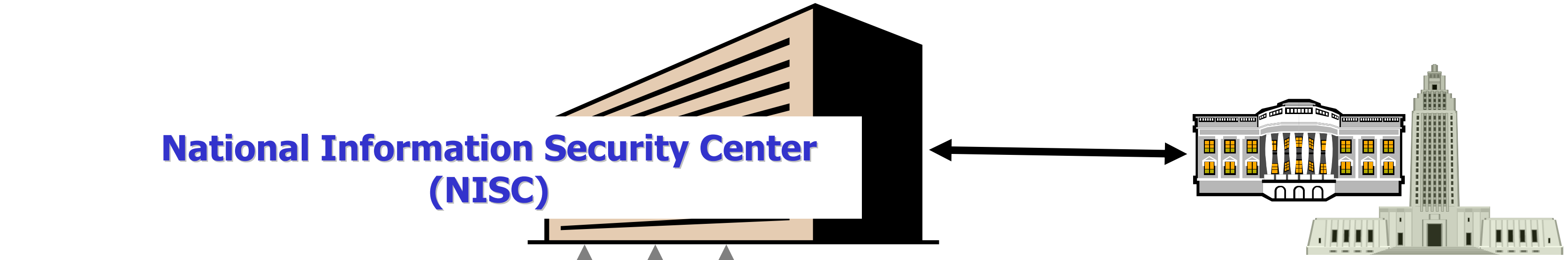
Convenience vs. Risk (Vulnerability)

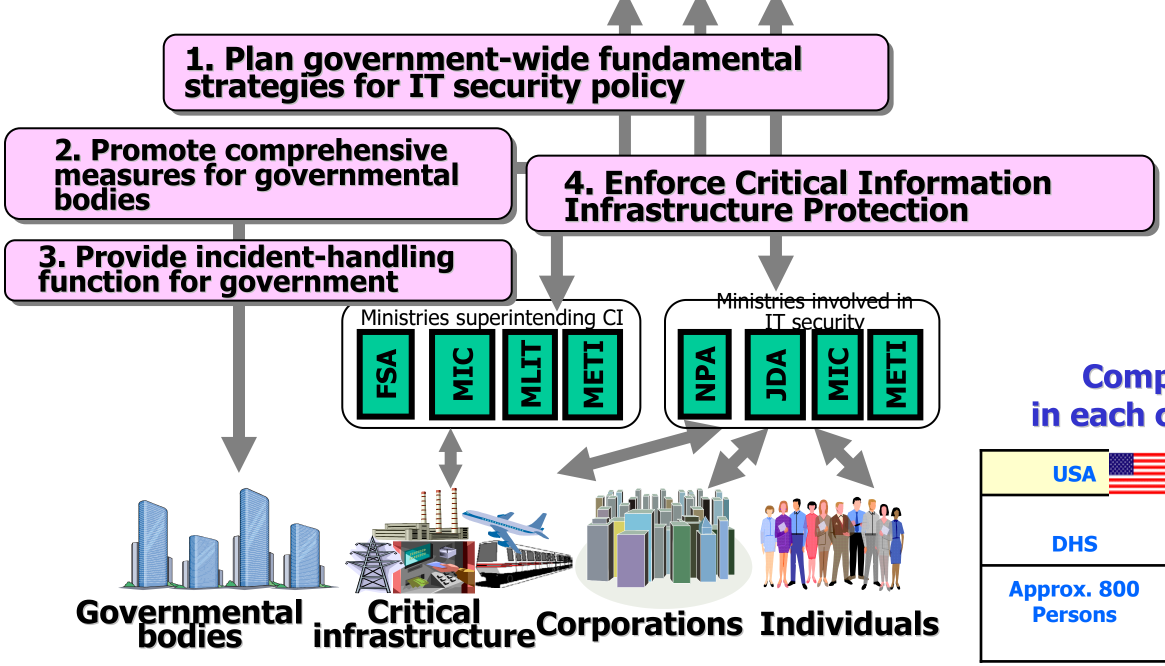
	Information on paper	Digital media
Copy	**Deteriorates due to repeated photo-copying**	**No deterioration via digital copying**
Modification	**Difficult**	**Easy**
Visibility	**Yes**	**No**
Transmission	**Costly (time, money)**	**Inexpensive (time, money)**
Storage	**The bigger the volume, the more space required**	**Smaller space compared to paper storage**
Long-term Retention	**Yes**	**?**

National Information Security Center（NISC)

METI

- ➢The National Information Security Center (NISC) was established on April 25, 2005 based on a decision by the IT Strategy Headquarters on Dec. 7, 2004.
- ➢NISC has been launched as Japan’s central entity for IT security issues.




1. Plan government-wide fundamental strategies for IT security policy
2. Promote comprehensive measures for governmental bodies
3. Provide incident-handling function for government
4. Enforce Critical Information Infrastructure Protection
Ministries superintending CI
FSA
MIC
MLIT
METI
Ministries involved in IT security
NPA
JDA
MIC
METI
Governmental bodies
Critical infrastructure
Corporations
Individuals

- Total coordination for information exchange with other countries
- Fostering international confidence through NISC’s activities

※FSA: Financial Services Agency
MIC: Ministry of Internal Affairs and Communications
MLIT: Ministry of Land Infrastructure and Transport
METI: Ministry of Economy, Trade and Industry
NPA: National Police Agency
JDA: Japan Defense Agency

Comparison of national security center in each country from a personnel perspective

USA	France	UK	Japan
DHS	DCSSI	NISCC	NISC
Approx. 800 Persons	Approx. 100 Persons	Approx. 70 Persons	Approx. 35 Persons (by this July)

Components of METI's IT Security Policy

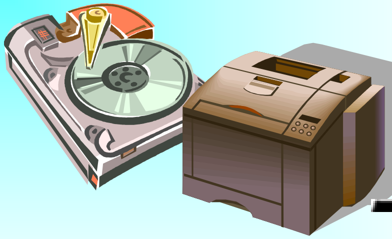
METI

I

National Institute of Advanced Industrial Science and Technology
AIST

IPA

JISEC



Technological Measures

II

Japan information processing
JIPDEC
Development Corporation

JASA 特定非営利活動法人 日本セキュリティ監査協会 Japan Information Security Audit Association

Security Management

III

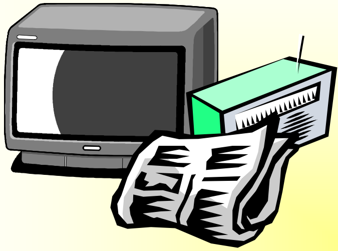
JPCERT/CC

IPA

Early Warning (Info sharing, Emergency response)

IV

IPA



NPO 日本ネットワークセキュリティ協会
Japan Network Security Association
JNSA

Japan information processing
JIPDEC
Development Corporation

Awareness, Training, and Education

Evaluation Framework

Technology

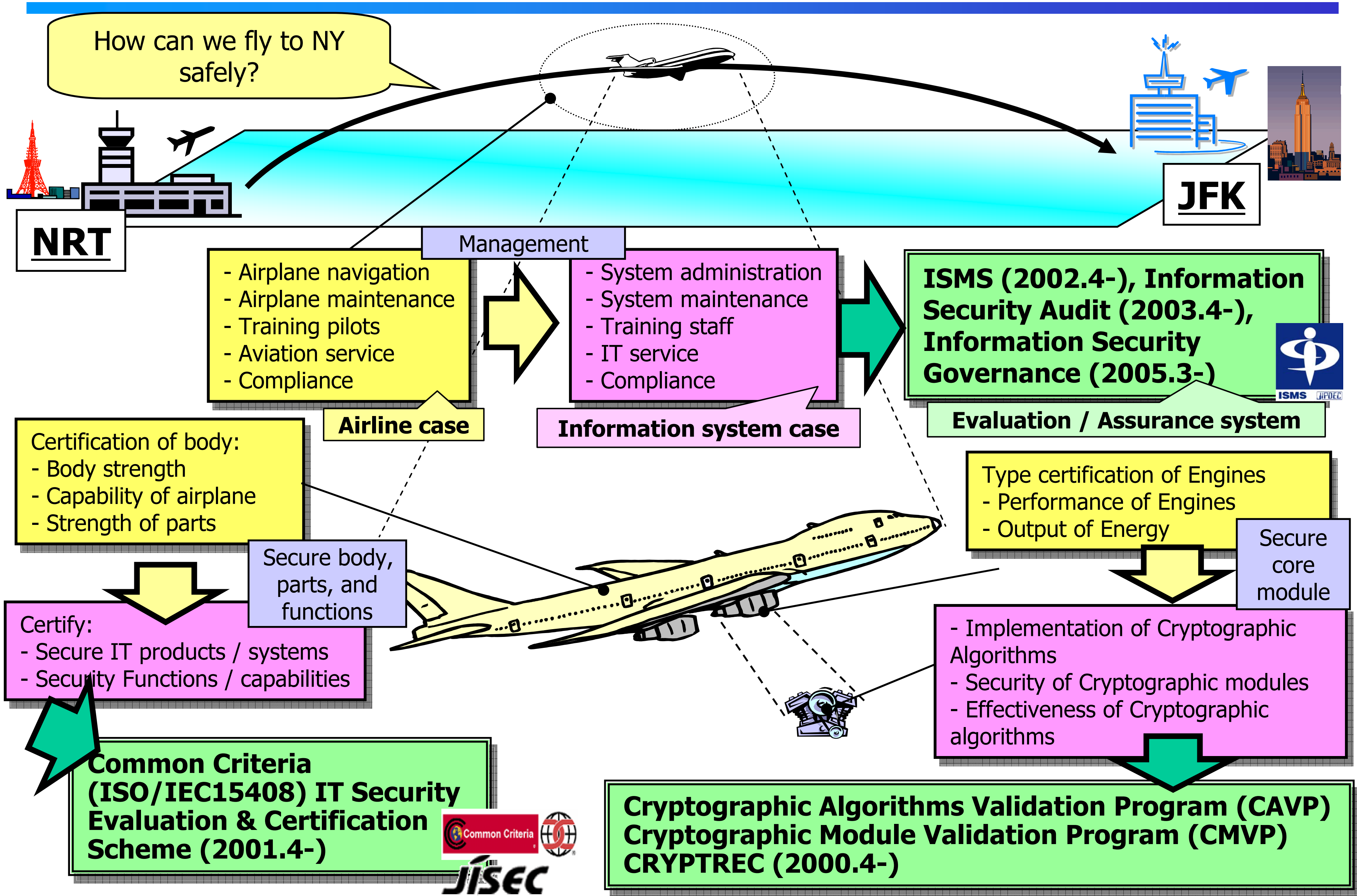
- IT security evaluation & certification scheme (ISO/IEC 15408, CC) – IT products/systems
- CRYPTREC (Cryptography Research & Evaluation Committee) – Cryptographic Algorithms
- Cryptographic Module Validation Program (CMVP) (not prepared yet)

Management

- Information Security Management System (ISMS) based on JIS X 5080 (ISO/IEC 17799, etc)
- Information Security Audit
- Information Security Governance

Understanding Assurance Scheme in IT Systems
-- Example of Airline Security Matching IT Security --

METI



How can we fly to NY safely?

NRT

JFK

Management

- Airplane navigation
- Airplane maintenance
- Training pilots
- Aviation service
- Compliance

Airline case

- System administration
- System maintenance
- Training staff
- IT service
- Compliance

Information system case

ISMS (2002.4-), Information Security Audit (2003.4-), Information Security Governance (2005.3-)

Evaluation / Assurance system

Certification of body:
- Body strength
- Capability of airplane
- Strength of parts

Secure body, parts, and functions

Certify:
- Secure IT products / systems
- Security Functions / capabilities

Common Criteria (ISO/IEC15408) IT Security Evaluation & Certification Scheme (2001.4-)

Type certification of Engines
- Performance of Engines
- Output of Energy

Secure core module

- Implementation of Cryptographic Algorithms
- Security of Cryptographic modules
- Effectiveness of Cryptographic algorithms

Cryptographic Algorithms Validation Program (CAVP)
Cryptographic Module Validation Program (CMVP)
CRYPTREC (2000.4-)

Assurance Level

- Self declaration
- Evaluation by a counterpart
- Evaluation by a trusted third party

Technology

Common Criteria

Government Procurement

Incentive(s)

Current Situation

- Since 2001, the Japanese Government **should** procure information systems under IT security evaluation & certification scheme (CC).
- NISC is building up Common Standards for Government Information Systems.
  - Sept. 1st Edition
  - Dec. Complete Edition

NSTISSP No.11 (Excerpts) -- U.S. Case --

- (6) Since 1 January 2001, preference is to be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting national security information) which have been evaluated and validated, as appropriate, in accordance with:
  - The International **Common Criteria** for Information Security Technology Evaluation Mutual Recognition Arrangement;
  - The National Security Agency (NSA) /National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program; or
  - The NIST Federal Information Processing Standard (FIPS) validation program.
- (7) Effective 1 July 2002, the acquisition of all COTS IA and IA-enabled IT products to be used on the systems specified in paragraph (6), **shall be limited only to those which have been evaluated and validated** in accordance with the criteria, schemes, or programs specified in the three sub-bullets of paragraph (6).

How to Build Up “Trusted” Systems?

- New Technology
- Common Technology
- Evaluated / Certified Technology

- In any case, we have to account for “why our systems are secure.”
  - From technology side -> Common Criteria
  - From management side

Incentive

- The Development Bank of Japan has low-interest loan programs for:
  - Companies which invest in IT products/systems certified under CC.
  - Companies which invest in systems developing IT products/systems to be certified under CC in the future.

Management

Information Security Management

The Government’s Role

- Because the risk that an IT incident will occur is not obvious, it is difficult for private companies to invest in information security.

  ⇨ Need for criteria for decisions about investment in information security?

- There is every possibility that existing measures and efforts to cope with information security do not effectively fit a company’s management.

  ⇨ Need for mechanism by which measures and efforts to ensure information security are directly connected to the proper evaluation of a private company?

- Private companies are not fully aware of the need to ensure business continuity.

  ⇨ From the viewpoint of business continuity, need to decide the procedure for incident response in advance?

The government creates a mechanism for private companies to implement information security on an appropriate level !!

Towards “Information Security Governance”

METI

- In September 2004, the Ministry of Economy, Trade and Industry (METI) started a group for the study of information security governance in private enterprises, and its final report was released to the public on METI’s website on March 31st, 2005.
- Here, ***“Information Security Governance”*** means to construct and put into practice, from the viewpoint of information security, **(i) Corporate Governance which takes CSR into consideration**, and **(ii) a mechanism of internal control to support it**.
- In order that information security governance takes root in private companies, METI has examined **effective and practical tools and measures** in this study group.

(i) Information Security Benchmark
(ii) Information Security Report
(iii) BCP Guideline

Practical Tools (i) ~ Information Security Benchmark

- **Background:**
  Most private companies do not know the extent of the appropriate security level of information security.
- **Target:**
  Mainly small and medium-sized enterprises (SMEs) which have not yet taken security measures, or have taken only simple measures

- Develop **an online self-check tool** which consists of 40 evaluation items for a self-check, and **establish three-level security benchmarks and recommended measures**.
- Each company can **answer the self-evaluation items via internet**, and evaluate its own information security level **by comparison with the 3-level recommended benchmarks** (high/middle/low).
- As a result of the self-check, the company can see **the difference between its current security level and the recommended level**, and put the recommended measures into practice.

Practical Tools (ii) ~ Information Security Report Model

- Through the **"Information Security Report Model,"** a private company discloses its own information, such as its information security policy and/or its actual security measures which have been taken so far, **as part of IR (Investor Relations) activities to explain compliance and CSR**.
- A private company can **autonomously** choose the items mentioned in the "Information Security Report" **according to its own circumstances**.
- A company can insert "the Information Security Report" in other reports such as a CSR report, and can also publish it as a one-volume edition.

- Fulfill minimum accountability to stakeholders
  - Explain how small the risk to IT is
  - Win stakeholders' trust in the company
- Create added value for company's business
  - **Improve business value and ensure competitive advantage**

- **A company's efforts** to ensure information security **are appropriately evaluated by various stakeholders**, including customers, investors, and the government.

Practical Tools (iii) ~ BCP Guideline

METI

- Background:
  - Requests by various stakeholders

    ~ customers, clients, consumers, local communities, shareholders
  - Unexpected risks

    ~ terrorism, IT incidents
  - Risks due to natural disasters

    ~ earthquakes, flood damage

- Ensuring business continuity is the most important task.

- Draw up a guideline for BCP (Business Continuity Plan) in order to maintain continuous management and operation.
- The BCP Guideline introduces methods and procedures to draw up BCP, items which a company ought to consider, case studies, etc.
- It is important to diffuse BCP effectively within a company, and to reflect BCP in their risk management.

Our Goal

- Create an environment where private companies' efforts to ensure information security are directly connected with appropriate evaluation of their business value.
- Promote secure and safe e-commerce in cross-border transactions by diffusing Information Security Governance among private companies.
- For each element of the security framework, we try to establish a "fair measurement of security."

Takefumi Tanabe

Ministry of Economy, Trade and Industry,
JAPAN