Cyber Security Policy in Japan

2003/11/06

Ministry of Economy, Trade and Industry, Japan
Office of IT Security Policy
Yasuhiro KITAURA
kitaura-yasuhiro@meti.go.jp

Copyright(C) 2003

Contents

- ✓ **Current Situation**
- ✓ **Government Policies**
- ✓ **METI's IT Security Policy**
- ✓ **"General Strategy for Information Security"**

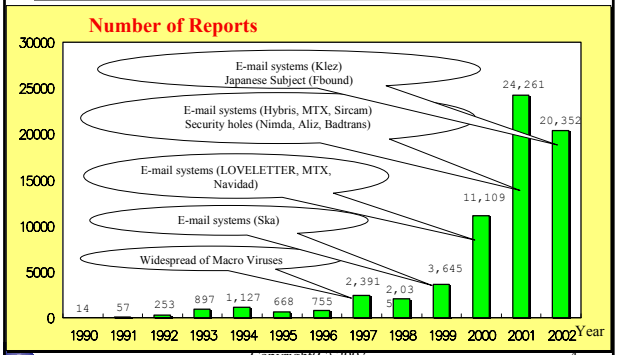
Copyright(C) 2003

Contents

- ✓ **Current Situation**
- ✓ **Government Policies**
- ✓ **METI's IT Security Policy**
- ✓ **"General Strategy for Information Security"**

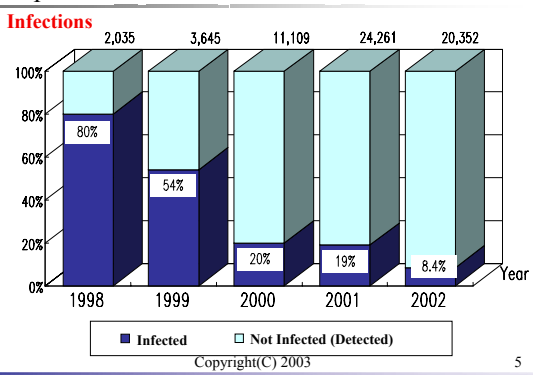
Copyright(C) 2003

Computer Virus - 1



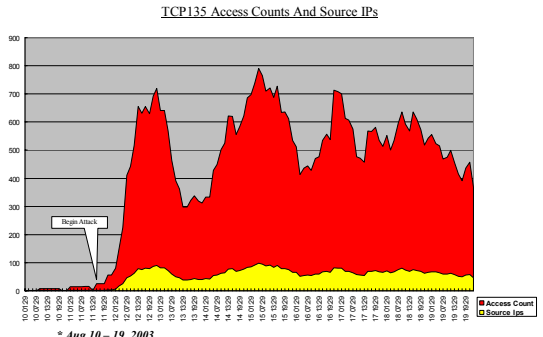
Copyright(C) 2003

Computer Virus - 2



Copyright(C) 2003

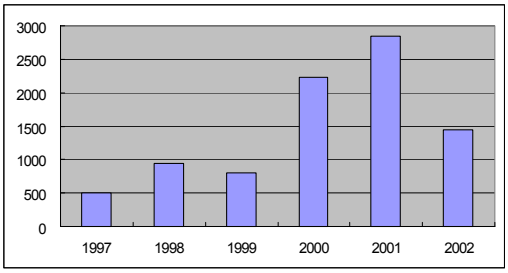
MS Blast Worm (Aug. 2003)



Copyright(C) 2003

Unauthorized Access

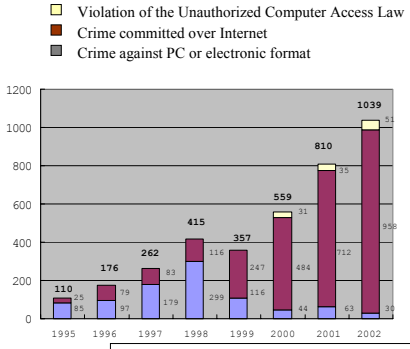
Number of Reports



From JPCERT/CC Japan Computer Emergency Response Team / Coordination Center
HP http://www.jpcert.or.jp/stat/reports.html

Copyright(C) 2003

Cyber Crime Arrests - 1



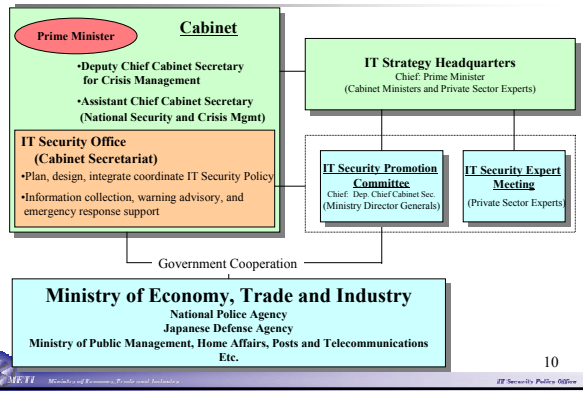
From National Police Agency (NPA) HP http://www.npa.go.jp/english/index.htm

Contents

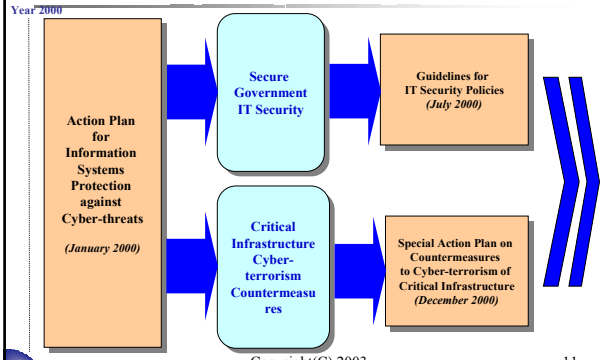
- ✓ **Current Situation**
- ✓ **Government Policies**
- ✓ **METI's IT Security Policy**
- ✓ **"General Strategy for Information Security"**

Copyright(C) 2003

Government Structure (for IT Security)

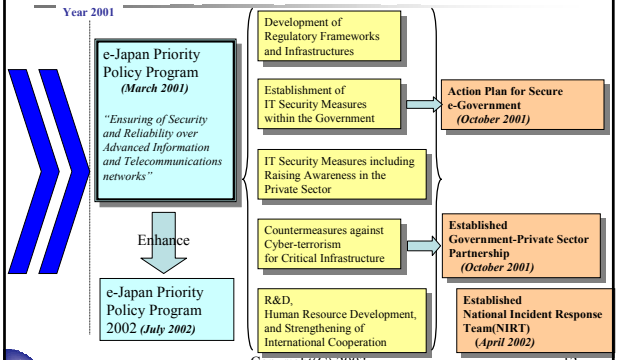


Basic IT Security Policies



Copyright(C) 2003

Basic IT Security Policies (cont'd)



Copyright(C) 2003

Action Plan (for Secure e-Government)

e-Government is scheduled to start from FY 2003
→ Network Security is essential for secure e-Gov.

Key Contents

- ✓ Implementation of Effective IT Security Policy at each Governmental Organization
- ✓ Standardization of cryptographic technology for e-Gov.
- ✓ Plan to establish effective monitoring system for e-Gov. network
- ✓ Preparing emergency response system especially at the Cabinet Secretariat by establishing CIRT
- ✓ Human resource development on IT security
- ✓ R&D for IT security key technology

Contents

- ✓ **Current Situation**
- ✓ **Government Policies**
- ✓ **METI's IT Security Policy**
  - **- General**
  - **- Evaluation of IT Products (Common Criteria, Cryptography Evaluation)**
  - **- Management (ISMS Conformity Assessment, Information Security Audit)**
- ✓ **"General Strategy for Information Security"**

METI's IT Security Policy

1 Enhancing security of the e-government

- ✓IT security evaluation (ISO/IEC15408, Common Criteria)(NITE(IPA))
- ✓evaluation of cryptography(IPA, TAO)
- ✓supporting the cabinet office(policy advice, helping NIRT, etc.)
- ✓GPKI

2 Supporting the private sectors

- ✓information sharing/analysis on computer virus & hacking(JPCERT/CC, IPA)
- ✓promoting security management(ISO/IEC17799)
- ✓promoting Security Audit scheme
- ✓promoting PKI(voluntary accreditation scheme, etc.)
- ✓training experts(national exam., etc.)
- ✓awareness raising of IT security(seminar, etc.)
- ✓establishing guidelines(against computer virus & hacking, etc.)

** METI : Ministry of Economy, Trade and Industry*

METI's IT Security Policy (cont'd)

3 Countermeasures against Cyber-terrorism

- ✓measures based on "Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure" (communication and coordination scheme with private sectors such as electric power and gas, etc.)
- ✓promoting R&D

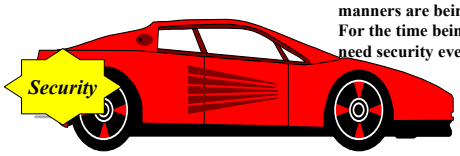
4 International Cooperation

- ✓cooperation with OECD, APEC, G8 Lyon Group, etc.
- ✓promoting info-share network of CSIRTs

** METI : Ministry of Economy, Trade and Industry*

Secure Driving on Cyber road

Traffic rules and driving manners are being developed For the time being, we still need security even more …



<Technology>
Product Evaluation
✓Common Criteria
✓Cryptography

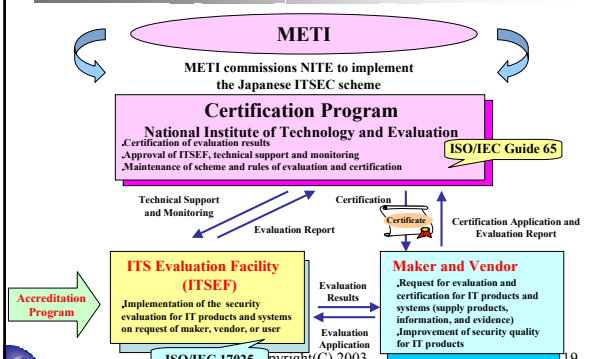
<Management>
Organization Assessment
✓ISMS Conformity Assessment
✓Security Audit

IT Security Evaluation / Certification Scheme - 1

- ✓IT Security Products Certification
- ✓Criteria : CC:Common Criteria, ISO/IEC 15408, JIS X 5070
- ✓Japanese CC scheme started from April, 2001
- ✓Secure infrastructure for e-Gov. / Recommended for e-Gov. procurements
- ✓CC is globally accepted standard to establish confidence in IT Products
- ✓CCRA (CC Recognition Arrangement) for global harmonization and collaboration in IT security evaluation and certification (since Oct 1998)
- ✓Participated CCRA on 31st October

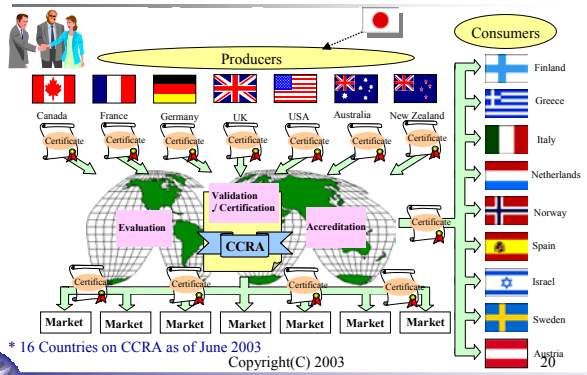
* ISO/IEC 15408 : Common Criteria for IT Security Evaluation
http://www.commoncriteria.org/

IT Security Evaluation / Certification Scheme - 2



pyright(C) 2003

IT Security Evaluation / Certification Scheme - 3



* 16 Countries on CCRA as of June 2003

Copyright(C) 2003

Cryptography Research/Evaluation - 1

Recommended ciphers for e-Government

2001

✓Requirements for e-Gov. cipher (categories and requirements)

✓Evaluations (e-Gov. cipher candidates)

October 2002

✓Draft list of e-Gov recommended ciphers

March 2003

✓e-Gov recommended ciphers list
✓Procurement Guide
✓Agreement among ministries and agencies

Next step

✓Monitoring and revision of the list
✓Cryptographic module evaluation criteria

Copyright(C) 2003

Cryptography Research/Evaluation - 2

e-Government recommended cyphers list

February 20, 2003

Category of technique		Name
Public-key cryptographic techniques	Signature	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	Confidentiality	RSA-OAEP
		RSAES-PKCS1-v1_5 (Note5)
	Key agreement	DH
		ECDH
		PSEC-KEM (Note5)
Symmetric-key cryptographic techniques	64-bit block ciphers (Note 3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES (Note4)
	128-bit block ciphers	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
	Stream ciphers	SC2000
		MUGI
		MULTI-S01
Others	Hash function	128-bit RC4 (Note5)
		RIPEMD-160 (Note5)
		SHA-1 (Note6)
		SHA-256
		SHA-384
		SHA-512
	Pseudo-random number generator (Note7)	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.5
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

Prepared by MPHPT and METI

Notes

(Note1) Use of this is permitted for the time being because it was used in SSL3.0/TLS1.0.

(Note2) On the assumption that this is used in the KEM(Key Encapsulation Mechanism)-DEM (Data Encapsulation Mechanism) configuration

(Note3) If any ciphers with a longer block length are available when constructing a new e-Government system, 128-bit block ciphers are preferable.

(Note4) Using the 3-key Triple DES is permitted for the time being under the following conditions:
1) It is specified as FIPS 46-3
2) It is positioned as the de facto standard.

(Note5) It is assumed that the 128-bit RC4 will be used only for SSL3.0/TLS1.0 or higher. If any other cipher listed above is available, it should be used instead.

(Note6) If any ciphers with a longer hash value are available when constructing a new e-Government system, it is preferable that a 256-bit (or more) hash function be selected. However, this does not apply in cases where the hash function to be used has already been designated according to the public-key cryptographic specifications.

(Note7) Since pseudo-random number generators do not require interoperability due to their usage characteristics, no problems will be generated from the use of a cryptographically secure pseudo-random number generating algorithm. Therefore, these algorithms are examples.

Copyright(C) 2003

ISMS Conformity Assessment Scheme

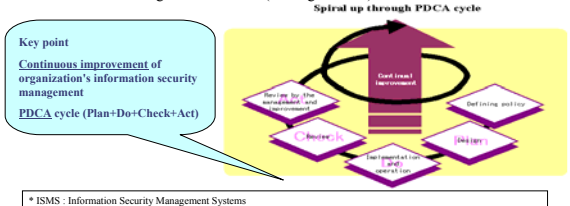
✓ISO/IEC 17799:2000 (Code of practice for information security management)

✓Provides guidance for information security management to identify necessary area of information security where organizations need to protect their information assets

✓ISMS Conformity Assessment Scheme started from April, 2002 (by JIPDEC)

✓ISMS Certified organizations : 180 (19 August 2003)

Spiral up through PDCA cycle



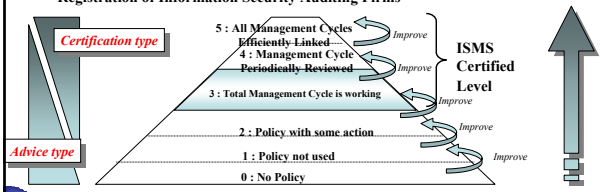
* ISMS : Information Security Management Systems
* Japan Information Processing Development Corporation (JIPDEC) http://www.isms.jipdec.or.jp/en/

Copyright(C) 2003

IT Security Audit Scheme

- ✓ **Started in April 2003.**
- ✓ **Based on ISO/IEC17799**
- ✓ **Organized by METI and JASA (Japan Information Security Audit Association)**
- ✓ **Two elements:**
  - **- Formulation of Information Security Auditing Standards**
  - **- Registration of Information Security Auditing Firms**

Improve Security Management



Copyright(C) 2003

Contents

- ✓ **Current Situation**
- ✓ **Government Policies**
- ✓ **METI's IT Security Policy**
- ✓ **"General Strategy for Information Security"**

Copyright(C) 2003

General Strategy for Information Security (announced October 10, 2003)
Greater competitiveness and general national security of Japan as economic and cultural power through realization of the world's top-class "reliability" in society

Key Points

Development as "nervous system" of entire society = encounter with risks on the new dimension
IT development as lifeline and social infrastructure

Examples: Unauthorized access in power grid in US; assault on water supply control system in Australia; vulnerability found in financial system as a result of cyber-terrorism drill in the US

Information security measures of the past

- Priority on security in economic transactions
- Stopgap measures
- Lack of central government organization in cyber-security
- Assure security in e-commerce
- Develop encryption standards
- Organization for gathering accident/incident data (JPCERT & NIRT)
- Action on international standardization
- Support in developing security technologies
- Improvement of cyber-force

General Strategy on Information Security

Basic Goal — *Development of world's top class " high-trust society"*

Reinforcement of international competitiveness / Improvement in general security

---Based on Japan's strengths as economic and cultural power, the development of "high-trust society" should be the goal of the national strategy. The resources should be invested in "information security measures" which is indispensable for building high-trust society

Strategy 1 — *Development of lithe "social system accepting accidents to occur" (assurance of outstanding capability at recovery and localizing damages)*

---> Thorough countermeasures for averting accidents (prevention), localizing damages, and optimizing recovery on the presumption that "there is no absolute safety in the field of information security."

Strategy 2 — *Reinforcement of public-sector action to strengthen trustworthiness of Japanese society*

---> Reinforcement of public-sector action in both technological and government system infrastructures in order to make "high-trust" as Japan's strength

Strategy 3 — *Concerted action to reinforce Cabinet functions*

Approaches

Intensive study through dialogue and interaction

General strategy from a broad perspective
(1) Information security issues from the standpoint of general security assurance
(2) System and roles of government/private sectors for strategic improvement

Copyrig

Arguments in technology and system founded on real issues
(1) What are the risks on the new dimension that must be addressed in real situations?
(2) Assessment of the current state of counter actions and international comparison
(3) Future issues and proposals of new concrete measures

Strategy 1: Development of lithe "social system that accepts accident/incident occurrence" (assurance of outstanding recovery capability and damage localization)

Current status

[Preventive measures]

Current measures

Strengthening measures to protect national/local governments and critical infrastructures

- Development of core organization for vulnerability analysis
- Promotion of security auditing and information security rating
- Development of rules concerning use of encryption & authentication technologies in some areas
- Development of security guidelines for IT products
- Increase public awareness of the importance of information security
- Security alerts to be issued in a manner similar to weather forecasts
- Legislation for measures against cyber-crimes

[Incident handling (development of system to minimize damage)]

Current measures

- **Cyber-terrorism drills** organized jointly by government and key infrastructure bodies
- **Development of accident data sharing system for each critical infrastructure**
- **Development of incident data sharing system for national/local governments**
- **Development of guidelines for service maintenance and restoration in case of incident**
  National and local governments and critical infrastructure
- **Establishment of "Investigating Committee for Incidents in Critical Infrastructure System"**
  #Similar to "Air and Rail Accident Study Committee"
- **Startup of data sharing and cooperation organization in the IT industry**
- **Proposal of damage reduction models** based on damage insurance, technologies and contracts

Principal conclusions to date

Security manpower development: Organized training at emergency-action bodies, certification of professionals, development of standards for skills and training personnel encountering actual issues

---

Strategy 2: Reinforcement of public-sector action to strengthen trustworthiness of Japanese society

Reinforcement of Japan's economic competitiveness ⟵ "High-trust Society" ⟶ ***Improvement of general national security as economic and cultural power***

- Highly competitive group of business corporations making maximum use of advantages of the information economy
- Development of security infrastructure essential to become cutting-edge IT nation as described in e-Japan Strategy II

Example: Problems of declining birth rate and aging population resolved by cost-cutting through efficient medical care and creating more jobs for the aged in SoHo work scheme.

- Increase in direct foreign investment through outstanding reliability

Industrial structure with device technologies and "commitment" in manufacturing and quality

Highly-reliable IT infrastructure & IT use

Outstanding security

Society of outstanding ethical standards through uniform and thorough communication

- Society resistant to cyber-terrorism by reducing vulnerability
- Improvement in food & energy security through utilization of IT
- International contribution through export of security infrastructure and dissemination of Japanese-style model society of outstanding reliability

Principal conclusions to date

Development of lithe "society that accepts accident/incident occurrence" (assurance of outstanding recoverability and damage localization) = See "Strategy 1"

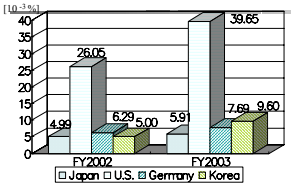
Reinforcement of infrastructure that supports entire society from the national perspective
•Development of secure info-communication infrastructure with attention to risks pertaining to centralization and dependence (such as operating system, GPS, etc.)
•Government/private cooperation to fight cyber-crimes and study into personal data protection based on new technologies

Greater sophistication of software manufacturing technologies in dissemination of secure programming technologies
Preservation and reinforcement of industrial infrastructure related to basic technologies (ex. device)

Review into public-sector action (review of the government involvement in this area)
•Increase in public spending in areas effective for "security" and "safe economic activities"
•Measures to promote market function in private sector-led areas, such as introducing standards for "showing risks"

Strategy 3: Concerted Action to Reinforce Cabinet Functions

[Government budget on information security vis-à-vis GDP]



[Information security divisions in foreign governments]

United States: Creation of Department of Homeland Security (DHS) -- currently in development
National Security Agency (NSA): Workforce undisclosed
National Institute of Standards and Technologies (NIST): 50
United Kingdom: Communications & Electronic Security Group: 300
Germany: Federal Bureau of Information Technology and Security (BSI): 390
South Korea: Korean Institute of Security Assurance (KISA): 300
France: Central Bureau of Information System Security (DCSSI): 90
Japan: Cabinet Security Measures Promotion Office: 9
(NIRT: 17; expert research team: 11) (not full-time)
JPCERT/CC: 10
IPA Security Center: 30

Notes:
Figures mean the number of people in charge

Principal conclusions to date

Dramatic increase in functions and workforce ofCabinet Security Office
•Security audit for public organizations and intrusion tests
•Development of system for centralized gathering of incidents data for national government, local governments and critical infrastructures
•Planning to develop technologies for preservation of government secrets, etc.

Creation of organization for concerted government action
•Clarification of roles for each ministry and organizations; adjustment of redundant operations by Cabinet Office
•Data sharing and concerted action by "Information Security Policy Committee" crossing all ministries and government organizations
•Assessment of the state of implementation of the "General Strategy" by "Information Security Policy Advisory Council" consisting of experts

---

Reference 1: Examples of Information System Failures (summary from media reports and other materials)

	Computer viruses and worms	Unauthorized access	Human error
National and local governments	Virus infection of LAN equipment at UK Ministry of Defense and LAN shut down for three days (April 2003) Blaster warm affects PCs at Setagaya-ku, Osaka Prefecture, Yamaguchi Prefecture, Japan Post and others (August 2003)	Opponents to the war in the rack organized mail assaults on public sites of the US Army, U.S. Navy in the UK home office, making access from the outside impossible (March 2003)	Operation error caused to failure of online services by Niihama city government and interruption in government services such as issue of resident certificates, tax payment certificates, reference service, etc.
Key infrastructure	US railway signal system affected by worm, causing confusion and stoppage of trains on three routes near Washington DC (August 2003) SQL Slammer worm spreads rapidly, temporarily shutting down the Internet in South Korea (January 2003)	DDoS attack on 13 root DNS servers around the world, causing temporary impact on nine (October 2002) Unauthorized access by outsider into California's power grid system (June 2001) Person who gained access into municipal power supply control system in Queensland, Australia, dumped 1,000,000 l of untreated sewage water into rivers and coasts (March 2000)	System integration due to merger of major banks caused large-scale system failures, such as non-processing of banks transfers. Restoration required approximately a month. (April 2002) Database server failure cost shutdown of Internet banking services (May 2003) Programming error in flight plan data processing system to shut down, causing delay for nearly 200 flights and nationwide confusion in airline operations (March 2003) Shutdown of stock exchange transaction system and stock quotation system (July 2003)
Businesses and private individuals	"I Love You" virus spreads in networks around the world, filling mail servers (May 2000)	DDoS assault on leading US sites cost failure of services at a number of commercial sites for 30 minutes to three hours (February 2000)	Error in customer registration system settings made new mobile phone subscriptions and processing of model changes impossible for five days (March 2002)

Copyright(C) 2003

Reference 2: Examples of Information System Failures (summary from media reports and other materials)

	Unauthorized access, operation, etc.	Human error
National & local governments	Web sites of Science and Technology Agency, Ministry of Home Affairs, Public Management, Posts and Telecommunications, and Ministry of Transport tampered (January 2000) Part-time worker at company involved in development of computer system for Uji City steals and sells citizen registry data for approximately 210,000 (May 2000) NASDA system invaded, with corporate secrets and other confidential information stolen (December 2001)	Defect possibly leaking credit card number found at Postal Service Center site (October 2002) Part of development data on Defense Agency system leaked (August 2002) Yokkaichi City employee disposed of PC still containing personal data at garbage collection site (May 2003)
Key infrastructure	Optical disk containing history for approximately 1700 patients was stolen at a hospital in Wakayama Prefecture, and personal data including history of dead infants was shown on an Internet site (1999) An employee of a hospital in Australia entered the hospital's computer system and tampered prescription data for patients, resulting in patient death (1995) Personal data leaked from registry of blood donors at the Nagano Prefecture Red Cross Blood Donation Center (July 2003)	Record for 100 patients at a Kochi Prefecture hospital was lost, possibly disposed of by mistake (August 2003) Information on 74 customers, including name, address, date of birth, policy value, etc., leaked from life insurance company (July 2003)
Business enterprises and private individuals	The computer system of a US credit card processing company was invaded, with credit card numbers for some 8 million holders stolen (February 2003) A subcontractor employee took out personal data for approximately 90,000 workers registered with the manpower service and sold information on the Internet web site (January 1998) Data for approximately 560,000 convenience store membership card holders leaked (May 2003) Key-logging software was installed at an Internet cafe, with password to Internet bank account obtained and resulting in the legal transfer of ¥16 million (March 2003) Kokubunji City legislator posted a photo, real name, date of birth, and slanderous information on his former girlfriend and was arrested for libel (April 2000)	Information on approximately 50,000 customers at a beauty treatment company became available for viewing on the Internet (May 2002) ISP run by a PC shop had the names, addresses, telephone numbers, credit card numbers, etc., for 299 customers available for viewing on the Internet (June 2001)

Reference WEB sites & Contacts

Reference WEB sites – 1

Japan's IT security policies

- IT Security Office (Cabinet Secretariat) http://www.bits.go.jp/en/index.html
- Ministry of Economy, Trade and Industry (METI) http://www.meti.go.jp/english/
- Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHP) http://www.soumu.go.jp/english/
- National Police Agency http://www.npa.go.jp/english/index.htm
- Japanese Defense Agency http://www.jda.go.jp/e/index_.htm

METI's IT security policy

http://www.meti.go.jp/english/policy/index_other.html

http://www.meti.go.jp/english/special/CyberSecurity/index.html

MPHP - Information & Communications Statistics Database

http://www.johotsusintokei.soumu.go.jp/english/index.html

- White Paper 2002 - Information and Communications in Japan (Summary) (July 2002)
- Number of Internet Users(As of January 31,2002)
- Information about the Spread of DSL services(May 2002)
- Information Security Countermeasure Survey (Sep. 2002) *Japanese Only*

Reference WEB sites - 2

- **IPA / IT Security Center (ISEC)**
  - http://www.ipa.go.jp/security/index-e.html
  - Information Security Survey 2001 (Summary)
    - http://www.ipa.go.jp/security/fy13/report/security_survey/survey2001en.pdf
  - Computer virus incident reports
    - http://www.ipa.go.jp/security/english/anti-virus-e.html
- **Independent Administrative Institutions (IAI)**
  - **National Institute of Advanced Industrial Science and Technology (AIST)**
    - http://www.aist.go.jp/index_en.html
  - **National Institute of Technology and Evaluation(NITE)**
    - http://www.nite.go.jp/index-e.html
    - Japan IT Security Evaluation & Certification Scheme
    - http://www.nite.go.jp/asse/english/its/index.htm
  - **Communications Research Laboratory (CRL)**
    - http://www.crl.go.jp/overview/index.html

Thank you for your attentions

http://www.meti.go.jp/policy/netsecurity/

Office of IT Security Policy, METI, Japan

Tel: +81-3-3501-0397

Fax: +81-3-3501-6639

e-mail: kitaura-yasuhiro@meti.go.jp