

Japanese Information Security Status - Environment and Policies -

Kei Harada, Senior Researcher

IT Security Center, Information-technology Promotion Agency, Japan

Japan is aiming to establish the most advanced and secure Information technology oriented society and e-government (e-Japan). This paper reviews current IT security environment in Japan, such as Computer Virus incidents report, cyber crime, etc. Then it also explains IT security policies adopted by Japanese Government to overcome issues and problems to achieve above goals of Japan.

1. Introduction

There are two important and independent concepts, “safety” and “security”. “Safety” means being free of danger or injury, and “security” means to make safe or secure.

However, Japanese doesn't have specific Japanese terminology for “security”. This is because that in the old days Japanese did not distinguish these two concepts, since safety was ubiquitous and free like water or air.

Therefore Japanese have not been aware of making effort to realize safe and secure status, and it is very important and hard to raise awareness regarding security at the age of lots of unknown and unpredicted threats.

2. Japan's Information Security Environment

2.1 Incidents and Crimes

Fig.1 shows computer virus incident reported to IPA/ISEC (Information-technology Promotion Agency, Japan, IT security Center). Year 2000, 2001 and 2002 were terrible years as similar to the global phenomena. The worst year was 2001 because of Sircam, Nimda and Badtrans. Note that

these numbers of reports are tips of an iceberg since less than 10% of small or medium companies reported these kinds of incidents to the official organization unless they suffered real damage. Individuals and home users show similar attitudes.

Fig. 1 Computer Virus Incidents Reports

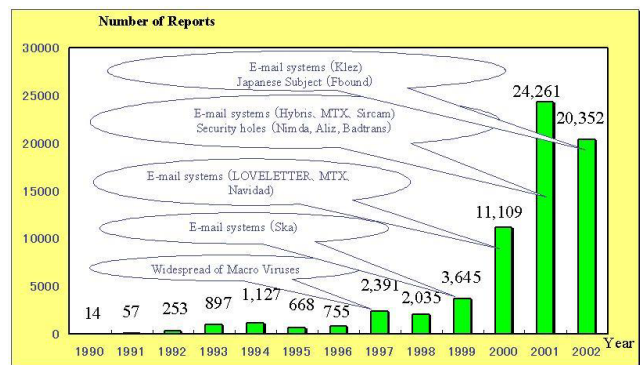


Fig.2 shows the virus infection rate compared to the number of reports. It is a good phenomenon that though the number of virus incident reports increases rapidly, the infection rate becomes lower. More than half were damaged before 1999, but less than 10% were damaged in the year 2002. The main reason of lowering infection rate might be the improved user awareness due to various educational efforts both in public and private

sectors.

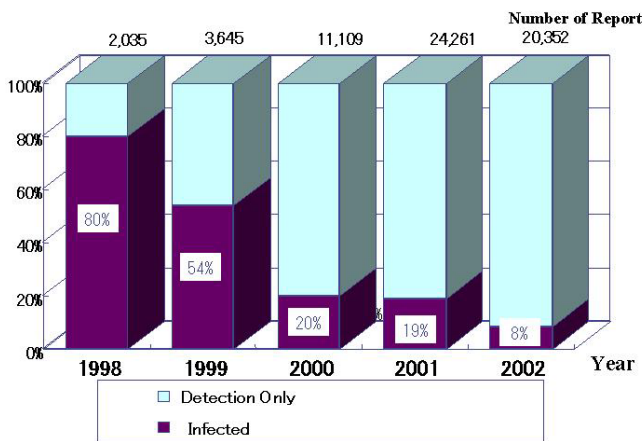


Fig. 2 Virus infection Rate

Fig.3 shows the unauthorized access incidents reported to JPCERT/CC (Japanese Computer Emergency Response Team Coordination Center). Unauthorized accesses are reported to JPCERT and IPA/ISEC, but JPCERT receives more reports than IPA/ISEC.

Similar to the Virus report, recent three years were very bad years, however the situation improved in last year. This is because worms altering the homepage disappear in 2002

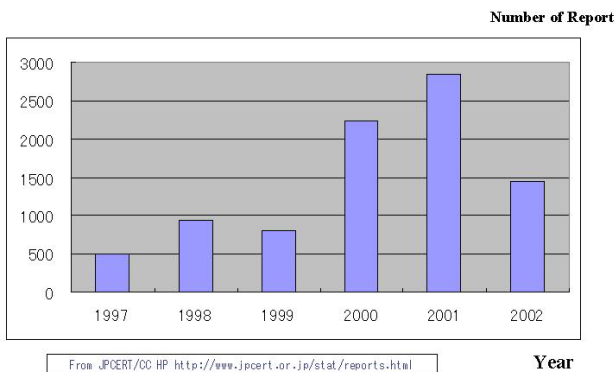


FIG. 3 Unauthorized Access Incidents

Fig.4 shows the number of arrests by Japanese Police. Unfortunately these numbers is steadily increasing. These days, most of cyber crimes are committed in Internet area.

Table 1 shows the breakdown of cyber crime.

The largest number is Child prostitution and child pornography. These crimes are increasing with spreading of cellular phone since most of Japanese cellular phone customers are using Internet service via cellular phone. Number of arrests regarding fraud is just above 100 in the year 2002, however police is aware of increase of its number due to spreading usage of e-commerce and internet-auction. Since Police received more than 19 thousand claims in year 2002 and more than a thirds were related to these areas.

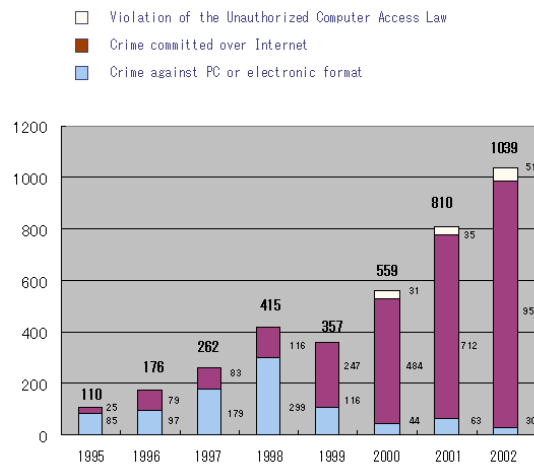


Fig. 4 Cyber Crime Arrests

Table 1 Breakdown of Cyber Crime

Category	Year 2000	Year 2001	Year 2002
Internet Facilitated Crime	484	712	958
Child Prostitution and Child Pornography	121	245	408
Distribution of Obscene Object	154	103	109
Fraud	53	103	112
Defamation	30	42	27
Infringement of Copyright	29	28	31
Intimidation	17	40	33
Others	80	151	238
Crime against Computer or Data	44	63	30
Unauthorized Computer Access	31	35	51
Total	559	810	1039

2.2 Attitudes in Private Sector

The following three figures are cited from research report by MPHP (the Ministry of Public Management, Home Affairs, Post and Telecommunication) published in September 2002. Large company stands for Tokyo Stock Exchange listed companies, while small stands for companies less than 300 employees randomly selected from "Corporate Quarterly Handbook". "Trend" includes Established and some of "Preparing".

Fig. 5 reveals that almost no security policy in small companies in Japan. Less than 10% of them established their security policies. Even for large companies, nearly half of which already established or started to plan, this activity is quite new. Most companies do not have more than 4 years of this activity.

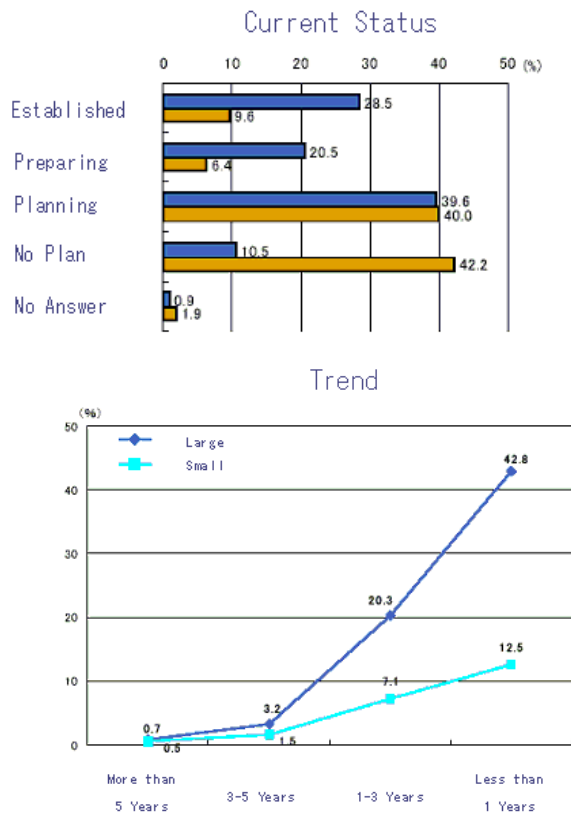


Fig. 5 Security Policy in Private Companies

companies. "Security audit" means audit or assessment relating to Information Security, including security policy, network design, system operation and so on. This graph illustrates that very limited Japanese companies are aware of security audit. For Japanese companies, 20% of large companies and 7.2% for small or medium companies. The reasons why they do not audit information security are; "No knowledge; 50%", "Unnecessary ; 38%". We have to improve this situation.

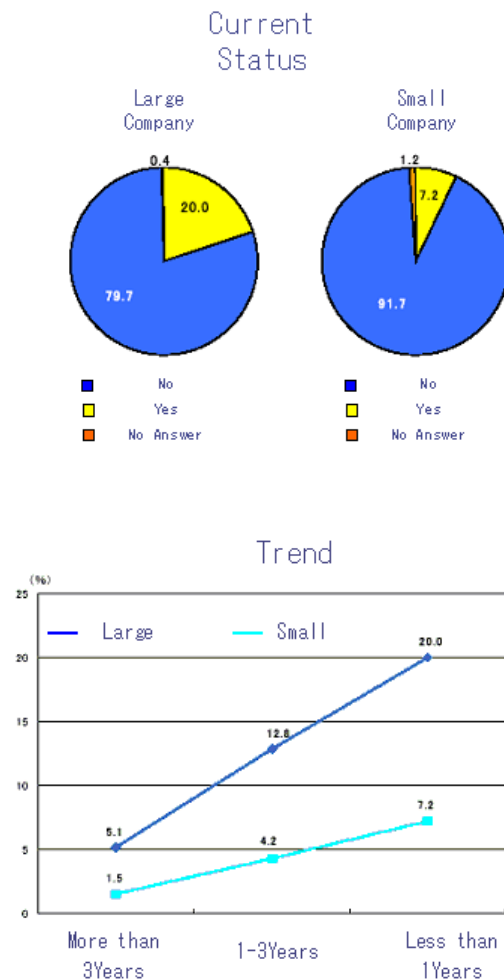


Fig. 6 Security Audit in Private Companies

Fig. 6 shows security audit in private

Fig. 7 shows the usage of cryptographic technologies in private companies. Large companies started to use or plan to use cryptography technologies. But only 14% of small companies are using them. Even small companies using Cipher do not apply them to EDI or EC to which confidentiality is essential.

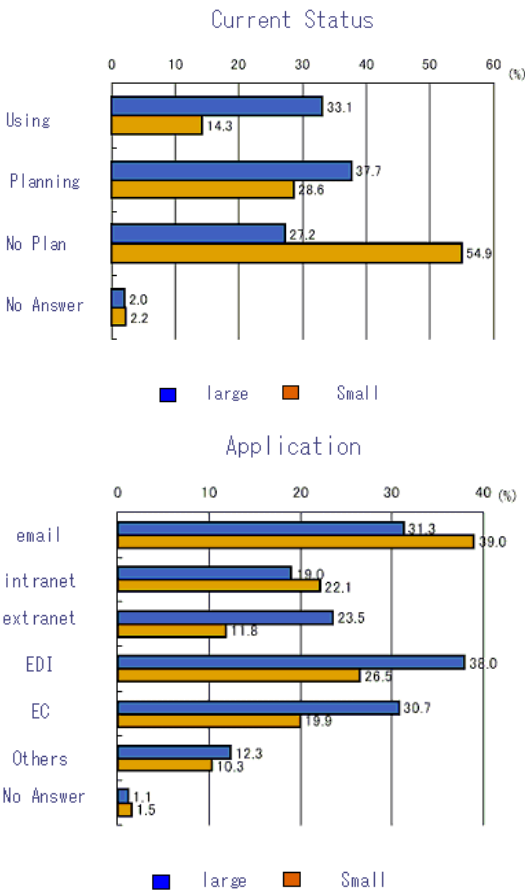


Fig. 7 Crypto Usage in Private Companies

3. Government’s IT Security Policies

3.1 Government Structure for IT Security

Fig. 8 illustrates Japanese government structure for IT security. The Cabinet secretariat coordinates the Government cooperation regarding IT security policy, among National Police Agency, Japanese Defense Agency, Ministry of Public Management, Home Affairs, Posts and

telecommunications, Ministry of Economy, Trade and Industry and so on.

Overall IT strategy is discussed at IT Strategy Headquarters headed by the prime minister Jun-ichiro Koizumi

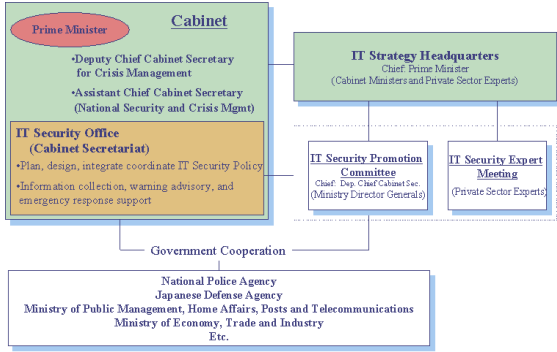


Fig. 8 Government Structure for IT Security

3.2 Action Plan for Information Systems

Protection against Cyber threats

The Government of Japan as a whole started to address IT security in 1999. Its first outcome was “Action Plan for Information Systems Protection against Cyberthreats,” which was released in January 2000. This plan outlined the necessity for the following:

- Constructing a governmental structure to respond to cyber threats
- Establishing IT security policy
- Developing cyber-terrorism countermeasures to protect critical infrastructures
- Putting the government in-line with the transition to an e-government by fiscal year 2003.

Based on this plan, the Cabinet Secretariat established the “Guidelines for IT Security” in July 2000 and “Special Action Plan on Countermeasures to Cyberterrorism of Critical Infrastructure” in December 2000.

3.3 e-Japan Priority Policy Program

In March 2001 IT Strategy Head quarters established an important policy “e-Japan Priority Policy Program” which should be in place by fiscal year 2005.

It consists of the following:

- Preparation of Regulatory Frameworks and an Infrastructure
- Establishment of IT Security Measures within the Government
- IT Security Measures and Raising of Public Awareness in the Private Sector
- Countermeasures against Cyber-terrorism for Critical Infrastructure
- R&D, Human Resource Development, and Strengthening of International Collaboration

As results of this action plan,

- Action Plan to Secure IT Security of e-Government was established in October 2001
- Government-Private Sector Partnership was established in October 2001
- National Incident Response Team (NIRT) was established in April 2002

Key contents of “Action Plan to Secure IT Security of e-Government” are as follows:

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

“e-Japan Priority Policy Program” was enhanced to “e-Japan Priority Policy Program 2002” in July

2002.

3.4 METI's IT Security Policies

The followings are IT Security Policies METI, the Ministry of Economy, Trade and Industry, are taking:

Regarding e-Government,

- The establishment and operation of IT security evaluation and certification scheme, of which NITE, National Institute of Technology and Evaluation serves as a Certification Body (CB). IPA is technically supporting CB as a subcontractor.
- Evaluation of cryptographic techniques is being carried out by IPA and TAO, Telecommunications Advancement Organization, MPHP's agency, asking Top-class Cryptographic researcher not only in Japan but also in the world.
- Supporting the cabinet secretariat (policy advice, helping NIRT, etc.)
- Promotion and operation of GPKISupport the Private sector

- Information sharing/analysis on computer virus & hacking (JPCERT/CC, IPA)
- Promoting security management (ISO/IEC17799)
- Promoting PKI (voluntary accreditation scheme, etc.)
- Training experts (national exam. etc.)
- Awareness raising of IT security (seminar, etc.)
- Promoting R&D
- Establishing guidelines (against computer virus & hacking, etc.)

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

International cooperation

- Cooperation with OECD, APEC, G8 Lyon Group, etc.
- Promoting info-share network of CSIRTs

4. Conclusion and the next steps

4.1 Conclusion

The outcome from activities of IT security taken by Japanese government are summarized as follows:

(1) Government Cooperation

- Japanese Government Organizations are cooperating to establish the most advanced and secure Information technology oriented society and e-Government.

(2) Improving and enforcing Laws

- Computer Crimes Criminal Law Revised
- Unauthorized Access Prohibition Law
- Digital Signature Law

(3) Established Schemes and Structures

- Cyber-Police Force in 2001 to combat cyber terrorism
- NIRT created April 2002. Fortunately Fortunately, no large-scale incident NIRT should respond seriously has happened since its creation.
- IT Security Evaluation and Certification Scheme was established in April, 2001 and 2 products were certified and 3 Security Target were confirmed
- Conformity Assessment Scheme for ISMS was established in April 2002 and more than 70 organizations were certified and 6

evaluation facilities were accredited.

4.2 Next Steps

The effort regarding IT security of Japan should be strengthened and continued, especially in the following aspects:

(1) Secure Reliability of e-Government

- Promoting security audit (establishing model standard)
- List of e-Government recommended Ciphers and Procurement Guide

(2) Improving and enforcing Laws

- Legislation for personal information protection
- Cyber-crime legislation (ratifying the convention)

(3) Enhance Human and Technological Resources

- Training experts (establishing skill standard)
- Promoting electronic authentication

(4) International Collaboration

- Participating in CCRA
- APEC/CERT Collaboration

--END--

References

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/police_e.htm
- Japanese Defense Agency http://www.jda.go.jp/e/index_.htm

2. 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>

3. MPHP

- Information & Communications Statistics Database
http://www.soumu.go.jp/joho_tsusin/eng/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*

4. 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>

5. 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)
 - 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>