Japanese Information Security Status
- Environment and Policies -

February 3, 2003

Kei Harada
IT Security Center (ISEC)
Information-technology Promotion Agency, Japan (IPA)

This document is based on public information, including the site of the Prime Minister of Japan and his Cabinet (http://www.kantei.go.jp/), etc. This translation is not official, but provisional.
Presentation Contents

- Introduction
- Japan’s Information Security Environment
- Japan’s Government Policies
- Conclusion and Next Step
- Reference, Contact Information
Safety and Security

**Known Problems/Threats**

- “Security” = “Safety” ???
- Safety is FREE like Water or Air
- Nobody pays for “Safety” or “Security”
- Low Awareness

**Now**

- Internet, Virus, Cyber Crime
- Threats - “Unknown”, “Unpredictable”
- Protect by yourself
- Growing Awareness

**Unknown Problems/Threats**
IPA Overview

IPA Information-technology Promotion Agency, Japan

Quasi-governmental organization under Ministry of Economy, Trade and Industry (METI), IPA will be restructured into “Independent Administrative Institution”

**Established:** October, 1970

**Mission:** Information processing technology promotion

**Personnel:** About 170

- **R&D and Support**
  - IT Security Technology
  - Advanced Software Technology
  - E-Commerce Technology
  - E-Government Support

- **Credit Guarantee**
  - To Information Technology Company
  - Development, equipment purchase

- **Education & Training**
  - Develop Training Materials
  - Educational Support

- **IT Security Center**
  - Mission: IT Security Enhancement
  - Established in 1997
  - Current personnel 35
Japan’s Information Security Environment
Computer Virus Reported to IPA /ISEC (1)

Number of Reports

- E-mail systems (Klez)
- Japanese Subject (Fbound)
- E-mail systems (Hybris?MTX?Sircam)
- Security holes (Nimda, Aliz, Badtrans)
- Widespread of Macro Viruses
- E-mail systems (LOVELETTER?MTX?Navidad)
- E-mail systems (Ska)


- 1990: 14
- 1991: 57
- 1992: 253
- 1993: 897
- 1994: 1,127
- 1995: 668
- 1996: 755
- 1997: 2,391
- 1998: 2,035
- 1999: 3,645
- 2000: 11,109
- 2001: 24,261
- 2002: 20,352

Copyright(C) 2003 Information-technology Promotion Agency, Japan All rights reserved.
Computer Virus Reported to IPA /ISEC (2)

Infection

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of Report</th>
<th>Infection</th>
<th>Detection Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>1998</td>
<td>2,035</td>
<td>80%</td>
<td>20%</td>
</tr>
<tr>
<td>1999</td>
<td>3,645</td>
<td>80%</td>
<td>20%</td>
</tr>
<tr>
<td>2000</td>
<td>11,109</td>
<td>20%</td>
<td>80%</td>
</tr>
<tr>
<td>2001</td>
<td>24,261</td>
<td>20%</td>
<td>80%</td>
</tr>
<tr>
<td>2002</td>
<td>20,352</td>
<td>20%</td>
<td>80%</td>
</tr>
</tbody>
</table>

Copyright(C) 2003 Information-technology Promotion Agency, Japan  All rights reserved.
Unauthorized Access Reported to JPCERT/CC

Year

Number of Report

Copyright(C) 2003 Information-technology Promotion Agency, Japan  All rights reserved.
Current Status of Cyber Crime

- Violation of the Unauthorized Computer Access Law
- Crime against PC or electronic format
- Crime committed over Internet

<table>
<thead>
<tr>
<th>Year</th>
<th>Violation</th>
<th>Crime against PC or electronic format</th>
<th>Crime committed over Internet</th>
</tr>
</thead>
<tbody>
<tr>
<td>1995</td>
<td>85</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>1996</td>
<td>110</td>
<td>97</td>
<td>29</td>
</tr>
<tr>
<td>1997</td>
<td>262</td>
<td>179</td>
<td>83</td>
</tr>
<tr>
<td>1998</td>
<td>299</td>
<td>116</td>
<td>16</td>
</tr>
<tr>
<td>1999</td>
<td>357</td>
<td>110</td>
<td>47</td>
</tr>
<tr>
<td>2000</td>
<td>559</td>
<td>484</td>
<td>75</td>
</tr>
<tr>
<td>2001</td>
<td>810</td>
<td>63</td>
<td>110</td>
</tr>
</tbody>
</table>

35
## Breakdown of Cyber Crime

<table>
<thead>
<tr>
<th>Category</th>
<th>Year 2000</th>
<th>Year 2001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Facilitated Crime</td>
<td>484</td>
<td>712</td>
</tr>
<tr>
<td>Child Prostitution and Child Pornography</td>
<td>121</td>
<td>245</td>
</tr>
<tr>
<td>Distribution of Obscene Object</td>
<td>154</td>
<td>103</td>
</tr>
<tr>
<td>Fraud</td>
<td>53</td>
<td>103</td>
</tr>
<tr>
<td>Defamation</td>
<td>30</td>
<td>42</td>
</tr>
<tr>
<td>Infringement of Copyright</td>
<td>29</td>
<td>28</td>
</tr>
<tr>
<td>Intimidation</td>
<td>17</td>
<td>40</td>
</tr>
<tr>
<td>Others</td>
<td>80</td>
<td>151</td>
</tr>
<tr>
<td>Crime against Computer or Data</td>
<td>44</td>
<td>63</td>
</tr>
<tr>
<td>Unauthorized Computer Access</td>
<td>31</td>
<td>35</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>559</strong></td>
<td><strong>810</strong></td>
</tr>
</tbody>
</table>
Security Policy, Private Company

Current Status
- Established
- Preparing
- Planning
- No Plan
- No Answer

Trend
- Large
- Small
- 3-5 Years
- 1-3 Years
- More than 5 Years
- Less than 1 Year

Usage of Cryptography

[Bar charts showing usage percentages for various applications are present.]
Japanese Government’s IT Security Policies
Government Structure for IT Security

Cabinet

Prime Minister

- Deputy Chief Cabinet Secretary for Crisis Management
- Assistant Chief Cabinet Secretary (National Security and Crisis Mgmt)

IT Security Office (Cabinet Secretariat)
- Plan, design, integrate coordinate IT Security Policy
- Information collection, warning advisory, and emergency response support

IT Strategy Headquarters
Chief: Prime Minister
(Cabinet Ministers and Private Sector Experts)

IT Security Promotion Committee
Chief: Dep. Chief Cabinet Sec. (Ministry Director Generals)

IT Security Expert Meeting
(Private Sector Experts)

Government Cooperation

National Police Agency
Japanese Defense Agency
Ministry of Public Management, Home Affairs, Posts and Telecommunications
Ministry of Economy, Trade and Industry
Etc.
Basic IT Security Policies

Year 2000

- Secure Government IT Security
- Critical Infrastructure Cyber-terrorism Countermeasures
- Guidelines for IT Security Policies (July 2000)
- Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure (December 2000)
Basic IT Security Policies (cont’d)

Year 2001

e-Japan Priority Policy Program (March 2001)
“Ensuring of Security and Reliability over Advanced Information and Telecommunications networks”

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


Action Plan to Secure IT Security of e-Government (October 2001)

Established Government-Private Sector Partnership (October 2001)

Established National Incident Response Team (NIRT) (April 2002)

Year 2002

e-Japan Priority Policy Program 2002 (July 2002)

Enhance
E-government is scheduled to start from FY 2003
Network Security is essential for a secure e-government

Key Contents
• Implementation of Effective IT Security Policy at each Governmental Organization
• Standardization of cryptographic technology regarding e-gov.
• Plan to establish effective monitoring system for e-gov. 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
## METI’s IT Security Policy (1)

### 1. Enhancing Security of the E-government

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

### 2. Supporting the Private Sector Activities

- 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.)
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
Conclusion and the Next Steps
Conclusion

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 (National Police Agency)
- National Incident Response Team (NIRT, Cabinet Secretariat)
- IT Security Evaluation and Certification Scheme (Based on ISO 15408, METI)
- Conformity Assessment Scheme for Information Security Management Systems (ISMS, Based on ISO 17799, supported by METI)
Next Steps

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
References and Contact information
References (1)

Japan's IT security policies

- 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]

METI's IT security policy

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

MPHP - Information & Communications Statistics Database

- 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*
References (2)

- **IPA / IT Security Center (ISEC)**
  
  [http://www.ipa.go.jp/security/index-e.html](http://www.ipa.go.jp/security/index-e.html)

- **Information Security Survey 2001 (Summary)**
  

- **Computer virus incident reports**
  

- **Independent Administrative Institutions (IAI)**

  - **National Institute of Advanced Industrial Science and Technology (AIST)**
    

  - **National Institute of Technology and Evaluation (NITE)**
    
    [http://www.nite.go.jp/index-e.htm](http://www.nite.go.jp/index-e.htm)
    
    Japan IT Security Evaluation & Certification Scheme
    

  - **Communications Research Laboratory (CRL)**
    
    [http://www.crl.go.jp/overview/index.html](http://www.crl.go.jp/overview/index.html)
Contact Information

IPA/ISEC

http://www.ipa.go.jp/security/index-e.html

Email: isec-info@ipa.go.jp

2-28-8 HonKomagome, Bunkyo-ku, Tokyo 113-6591 Japan
Tel: +81-3-5978-7508  Fax: +81-3-5978-7518

Kei Harada,
Senior Researcher
IT Security Center (ISEC),
Information-technology Promotion Agency, Japan (IPA)

k-harada@ipa.go.jp