Cybersecurity Strategy in Japan and Countermeasures for Cyber Threats by MEXT

November 1, 2016

Tsuyoshi Enomoto
Director, Information Science and Technology
(Eiji Ishida, Acting Director on behalf)
Recent Major Cyberattacks in Japan and the world

Japanese Governmental Organizations

- Japan Health Insurance Association: 1.25 million personal data of pension breached by cyberattacks
- PCs had been infected by malware in the Ministry of Justice

Private Entity

- DDoS Attacks on banks and securities firms with ransom and extortion
- Increased number of “Phishing” incidents

Global Cases

- Cyberattack disables French TV channels, takes over social media sites (France)
- Cyberattack on Website of Canada government (Canada)
- OPM Announces More Than 21 Million Affected by Second Data Breach (US)
- Hackers successfully ground 1,400 passengers (Poland)
New “Cybersecurity Basic Act” on November 6th, 2014

• “Basic Act”
• Initiated by the Diet members, NOT by the Cabinet
• Definition of the term “Cybersecurity”
• Basic principles for the promotion of cybersecurity policy
• Legislative backgrounds for the Cybersecurity Strategy
• Upgrading governmental institutional framework for enhancing national cybersecurity
Cybersecurity Framework in Japan

**Cabinet**

**Prime Minister**

**Cybersecurity Strategic Headquarters**

- **Director General**
  - Chief Cabinet Secretary
- **Vice Director General**
  - Minister in charge of Cybersecurity
- **Members**
  - Chair at National Public Safety Commission
  - Minister of MIC
  - Minister of MOFA
  - Minister of METI
  - Minister of MOD
  - Experts (Private entities including Universities)

**Secretariat**

**National Center of Incident Readiness and Strategy for Cybersecurity (NISC)**

- Renamed on Jan 9th 2015 by Basic Act

**National Security Council (NSC)**

- 5 Member Ministries of CSS HQ
  - NPA (Cyber Crime)
  - MIC (Communication & Network policy)
  - MOFA (Diplomatic policy)
  - METI (Information policy)
  - MOD (National Security)

**IT Strategic Headquarters**

- Close cooperation

**Other relevant Ministries**

- Critical Infrastructures
  - FSA (Financial Industry)
  - MIC (Local Gov, Telecom)
  - MHLW (Medical, Water)
  - METI (Electricity, Gas, Chemistry, Credit Card, Petroleum)
  - MLIT (Aviation, Railway, Logistics)

- Others
  - MEXT (Cybersecurity education)

**Critical Infrastructures**

**Governmental bodies (Ministries)**

**Private Entities**

**Individuals**
History of Cybersecurity Strategy

**IT Strategy**
- e-Japan Strategy 2001.1
- e-Japan Strategy II 2003.7
- New IT Reform Strategy 2006.1
- i-Japan Strategy 2015 2009.7
- New Strategy on Information and Communications Technology 2010.5
- New IT Strategy IT Strategic Headquarters June 2013

**Cyber Security Strategy**
- Mid/long-term Plan
- Annual Plan

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>First National Strategy on Information Security 2006.1</td>
</tr>
<tr>
<td>2008</td>
<td>The Basic Policy of Critical Information Infrastructure Protection Dec. 2005</td>
</tr>
<tr>
<td>2011</td>
<td>New Management Standards 5/19/2014</td>
</tr>
<tr>
<td>2013</td>
<td>3rd Edition 5/19/2014</td>
</tr>
<tr>
<td>2014</td>
<td>Cybersecurity Strategy ISPC, June 2013</td>
</tr>
<tr>
<td>2015</td>
<td>New Cybersecurity Strategy scheduled in summer 2015</td>
</tr>
</tbody>
</table>

- Focused on responding to cyber incidents
- Construction of comprehensive infrastructure for counteracting cyber incidents
- Active cyber security measures against cyber attacks
- Responding to new environmental changes
- Risk-based approach

- The Basic Policy of Critical Information Infrastructure Protection Dec. 2005
- New Management Standards 5/19/2014
- Cybersecurity Strategy ISPC, June 2013
- New Cybersecurity Strategy scheduled in summer 2015
- Renewed based on the New Act!
New “Cybersecurity Strategy of Japan”

1 Understanding of Cyberspace
- Blessings of Cyberspace: Generating infinite values, essential foundation for our socio-economic activity
- “Hyper-connected and converged society” is coming
- Cyber threats are becoming more serious and being perceived as national security matters

2 Objective
- Develop and advance free, fair, and secure cyberspace subsequently contribute to:
  1) Socio-economic vitalization
  2) Safe and secure society
  3) International Peace and Stability, National Security

3 Principle
- 1. Free Flow of Information
- 2. Rule of Law
- 3. Openness
- 4. Self-governance
- 5. Cooperation among Multi Stakeholders

4 Policy Measure

1) Socio-Economic Vitalization and Sustainable Development
- Not cost, but investment
  - Creating Secure IoT System
  - Promoting Management with cybersecurity mindset
  - Improving Business Environment

2) Realizing a Safe and Secure Society for the People
- Foundation for 2020, further
  - Protecting People and Society
    - Enhancing capability and countermeasure
  - Protecting CII
    - Enhancing information sharing public with private
  - Protecting Governmental Agencies
    - Strengthening defense and management audit

3) Peace and Stability of International Community and Japan’s National Security
- Proactive contribution to peace in cyberspace
  - Ensure Japan’s National Security
    - Improving Cyber capabilities
  - International Peace and Stability
    - Rule of law in cyberspace, confidence building
  - International Partnership
    - Cooperation in a wide range of area

Cross Cutting
- R&D
  - Improving detection and protection capabilities
- Human Resources
  - Developing multi-talent, practical training, promoting skill standards

5 Organization
- Enhancement cooperation with public and private sector, Institution building toward the Tokyo Olympic and Paralympic Games in 2020
Countermeasures for Cyber Threats by MEXT

**Training for Security at Universities/Tertiary Colleges**

**Education Network for Practical Information Technologies (enPiT)**

- Enhance capacity building outcomes in the field of security
- Develop education networks in collaboration with industry and academia
- Promote practical education including a problem-solving learning method

**Interuniversity Collaborative Information Security Platform**

- Build a system to respond to cyber attack incidents jointly by NII and national universities
- Build a system to detect cyber attacks on SINET5 to analyze contents and provide information on the urgency of a cyber attack to national universities and institutes
- Conduct hands-on training to technical staff of national universities and institutes in charge of information security on the actual SINET5
- SINET5: Science Information Network 5 among universities and institutes

**Advanced Integrated Intelligence Platform Project (AIP)**

AIP Center, RIKEN
- Pushes forward R&D of innovative AI platform technologies, aiming at practical application in collaboration with concerned Ministries

Strategic Basic Research Programs, JST
- Supports unique young researchers in the AI field and challenging questions paving the pathway to pioneering innovation including cybersecurity
Education Network for Practical Information Technologies (enPiT) – Security

[Outline of education]

◎ **Basic knowledge learning**: Learning common subjects (2 mandatory credits) and basic subjects (4 credits) to develop basic ability

◎ **Short intensive camp**: Intensive training course held in summer at 5 partner universities, providing various programs including encryption technology, system technology, response to risk and risk management, to develop the practical ability through exercises using actual environment and data in cooperation with the companies and other organizations

◎ **Distributed PBL**: Selecting 5 advanced subjects (2 credits for each) to learn latest problems in the field and develop applied skills usable in the field

[Example of PBL themes]

Setting exercise themes to learn a broad range of latest technologies and knowledge
- Exercise of system attacks and defense
- Exercise of hardware security
- Response to incidents and basic CSIRT exercise, etc.

[Features]

◎ Development of practical skills: 5 partner universities jointly provide SecCap curriculum where students learn latest technologies and knowledge in the security field through specific experience

◎ A broad range of courses: Covering a broad range of fields including encryption technology, web server and network security technology, and social scientific knowledge such as legal system and risk management

◎ Career development: Participants prepare learning programs coordinated independently and voluntarily toward career to aim for

---

Practical security human resources: Practical leaders who can lead security measures for information assets and information distribution, related to the foundation of social/economic activities, in terms of technology and management.

**Establishing education network of 24 universities and 14 companies**

(As of the end of March 2016)

<table>
<thead>
<tr>
<th>University/College</th>
<th>2013 (result)</th>
<th>2014 (result)</th>
<th>2015 (result)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of universities</td>
<td>Number of teachers</td>
<td>Number of companies</td>
<td>Number of participating students</td>
</tr>
<tr>
<td>2013 (result)</td>
<td>9 [63]</td>
<td>9</td>
<td>65 (Initial target: 60)</td>
</tr>
<tr>
<td>2014 (result)</td>
<td>17 [72]</td>
<td>10</td>
<td>84 (Initial target: 80)</td>
</tr>
<tr>
<td>2015 (result)</td>
<td>24 [70]</td>
<td>14</td>
<td>113 (Initial target: 90)</td>
</tr>
</tbody>
</table>

(As of the end of March 2016)
Objectives of operation

To conduct the following projects to build a system for responding to cyber attack incidents jointly by the National Institute of Informatics (NII), national universities and institutes:

1) Building a system to detect cyber attacks on SINET5 to analyze observed communications and provide information on the urgency of a cyber attack, etc. to national universities and institutes.

2) Conducting hands-on training to technical staff of national universities and institutes in charge of information security using SINET5 environment to improve the ability to respond to cyber attacks.

1) Support for building a security system (Based on the request from a national university or institute)

Outline of operation

SINET5 informs the detection of a cyber attack to a university or institute if a request for detection has been made. If not, the cyber attack to that university or institute is not detected.

1. The information on the attack detected in the cyber attack detection system is transferred to the information security manager and/or personnel of a university or institute*.
   * Where to send information is determined in consultation with the university or institute.

2. Upon receiving the information, the university or institute conducts research and analysis on the attack using the alarm monitoring system provided by the NII or an independent attack detection system, etc.

3. Based on research and analysis results, the university or institute determines the response such as shutdown of the network on its own responsibility. The NII disconnects the network of the university or institute from SINET5 upon request.

4. The detection of attacks is automated, and no communications are checked by the NII staff (the NII provides information according to the urgency determined by alert generations on the cyber attack detection system).

5. If the university or institute asks technical support for analysis to the NII, communications may be observed as required with the consent of the university or institute.

2) Development of human resources for cyber security

Outline of operation

Target: Technical staff of universities and institutes in charge of information security

Content of training: Analytical methodologies of and responses to cyber attacks

Method: In the SINET5 environment:

1. Practical OJT (on-the-job training) at the NII
2. Remote technical training by connecting the local site to the NII via VPN*

*VPN: Virtual Private Network
1) Support for building a security system (Based on the request from a university or institute)

- Automated monitoring
- Automated analysis
- Cyber attack detection system
- Transfer of detected information
- NII (National Institute of Informatics)
- University A
- Storage of attack-related data
- Technical support for joint analysis
- Use of data
- Conduct research and analysis on transferred information
- Take necessary actions such as shutdown of network

2) Development of human resources for cyber security

- Internet
- Cyber attack detection system
- Actual contents
- University B
- Leaning basic techniques in OJT
- University D
- NII
- OJT on VPN
- In-service training
- Remote technical training
- University A
- University C
- University B
- University D
Global trends

- Significant technological breakthrough in the Artificial Intelligence
  - AI that has features of autonomous capture of features of something / self evolving
- Accumulation of big data / dissemination of more quality sensors / IoT in variety of fields
- Needs for cybersecurity to counter emerging high level/sophisticated cyber threats

MIC, MEXT, METI are collaborating to take actions for R&D and practical application of AI technologies
Thank you very much