Japanese Government Cyber Security Strategy

Shinsuke AKASAKA
Director, ICT Security Office,
Ministry of Internal Affairs and Communications
January 21st 2015
1. ICT Security Trend

2. ICT Security Measures of the Japanese Government

3. ICT Security Measures of MIC
1. ICT Security Trend
ICT technologies such as the Internet form the base of social economic activities as well as a key to each country’s growth. However, damage to ICT technologies is more serious because threats to information security are now smarter and more complicated.

Crime for pleasure
- Show off
- Harassment etc.

Economic crime and organized crime
- Pecuniary motive
- Planned crime

Risk is increased by change in attack purpose

Increasing damage caused by malware infection and unauthorized access

Sophistication of cyber attack
2000
2005
2010

Conspicuous attack
The attack is immediately detected and it is possible to take counter measures.

Inconspicuous attack
Since discovery of the attack is delayed, damage is expanded and prolonged.

Crime for pleasure
Economic crime and organized crime

DDoS attack
Illegal remittance

Infection by network
Advanced Persistent Threat attack

Infection by Website
Infection by e-mail addressed to specific target

Unauthorized access
Infection by Website
Infection by e-mail addressed to specific target
Increase of ICT Security Threat 2

Observational data by NICTER (Network Incident analysis Center for Tactical Emergency Response)

<table>
<thead>
<tr>
<th>Year</th>
<th>Total annual number of packets observed</th>
<th>Number of IP addresses observed</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>Approx. 0.31 billion</td>
<td>Approx. 16 thousand</td>
</tr>
<tr>
<td>2006</td>
<td>Approx. 0.81 billion</td>
<td>Approx. 100 thousand</td>
</tr>
<tr>
<td>2007</td>
<td>Approx. 1.99 billion</td>
<td>Approx. 100 thousand</td>
</tr>
<tr>
<td>2008</td>
<td>Approx. 2.29 billion</td>
<td>Approx. 120 thousand</td>
</tr>
<tr>
<td>2009</td>
<td>Approx. 3.57 billion</td>
<td>Approx. 120 thousand</td>
</tr>
<tr>
<td>2010</td>
<td>Approx. 5.65 billion</td>
<td>Approx. 120 thousand</td>
</tr>
<tr>
<td>2011</td>
<td>Approx. 4.54 billion</td>
<td>Approx. 120 thousand</td>
</tr>
<tr>
<td>2012</td>
<td>Approx. 7.79 billion</td>
<td>Approx. 190 thousand</td>
</tr>
<tr>
<td>2013</td>
<td>Approx. 12.88 billion</td>
<td>Approx. 210 thousand</td>
</tr>
</tbody>
</table>

Observed by NICT (National Institute of Information and Communications Technology)

Number of threats to government agencies and critical infrastructure

Number of threats by sensor monitoring

<table>
<thead>
<tr>
<th>Year</th>
<th>FY2010</th>
<th>FY2011</th>
<th>FY2012</th>
<th>FY2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of threats</td>
<td>Approx. 0.48 M</td>
<td>Approx. 0.66 M</td>
<td>Approx. 1.08 M</td>
<td>Approx. 5.08 M</td>
</tr>
</tbody>
</table>

Top 10 countries (hosts)

<table>
<thead>
<tr>
<th>Country name</th>
<th>Number of hosts</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>中国(CN)</td>
<td>43,346</td>
<td>50%</td>
</tr>
<tr>
<td>韩国(KR)</td>
<td>6,384</td>
<td>7%</td>
</tr>
<tr>
<td>美国(US)</td>
<td>4,851</td>
<td>6%</td>
</tr>
<tr>
<td>日本(JP)</td>
<td>3,083</td>
<td>4%</td>
</tr>
<tr>
<td>台湾(TW)</td>
<td>2,988</td>
<td>3%</td>
</tr>
<tr>
<td>巴西(BR)</td>
<td>2,376</td>
<td>3%</td>
</tr>
<tr>
<td>俄罗斯( RU)</td>
<td>2,314</td>
<td>3%</td>
</tr>
<tr>
<td>香港(HK)</td>
<td>1,978</td>
<td>2%</td>
</tr>
<tr>
<td>印度(IN)</td>
<td>1,614</td>
<td>2%</td>
</tr>
<tr>
<td>泰国(TH)</td>
<td>1,422</td>
<td>2%</td>
</tr>
</tbody>
</table>

Country name | Number of packets | Percentage |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>中国(CN)</td>
<td>1,214,956</td>
<td>37%</td>
</tr>
<tr>
<td>美国(US)</td>
<td>555,109</td>
<td>17%</td>
</tr>
<tr>
<td>台湾(TW)</td>
<td>209,114</td>
<td>6%</td>
</tr>
<tr>
<td>俄罗斯( RU)</td>
<td>142,925</td>
<td>4%</td>
</tr>
<tr>
<td>韩国(KR)</td>
<td>122,770</td>
<td>4%</td>
</tr>
<tr>
<td>印度(IN)</td>
<td>95,948</td>
<td>3%</td>
</tr>
<tr>
<td>加拿大(CA)</td>
<td>94,700</td>
<td>3%</td>
</tr>
<tr>
<td>香港(HK)</td>
<td>93,522</td>
<td>3%</td>
</tr>
<tr>
<td>法国(FR)</td>
<td>90,051</td>
<td>3%</td>
</tr>
<tr>
<td>俄罗斯( RU)</td>
<td>84,056</td>
<td>3%</td>
</tr>
</tbody>
</table>

Attack source (Time September 4, 2014)
2. ICT Security Measures of the Japanese Government
Promotion Framework for ICT Security Measures in Japan

**MIC**

- Promoting attack detection and prevention, and reducing virus infection, from the viewpoint of protecting the telecommunication network through collaboration with ISPs (Internet Service Providers).

**MOFA**

- Strengthening international cooperation

**MOD**

- Strengthening capacity and preparations of the Self-Defense Forces in cyber space
- Cyber defense Corps (approx. 100 members) was installed

**METI**

- Promoting security measures of control systems such as electricity and gas, and software/hardware.

**NPA**

- Promoting crackdown on cyber crime, cyber attack, etc.

**NISC (National Institute of Information and Communications Technology)**

- National center of Incident readiness and Strategy for Cybersecurity
  - Formulating the “Cybersecurity Strategy” and leading comprehensive coordination of each ministry
  - Conducting monitoring of government network by operating GSOC (Government Security Operation Coordination team)

**IPA (Information-technology Promotion Agency)**

**JPCERT/CC (Japan Computer Emergency Response Team Coordination Center)**

Ministries and agencies having jurisdiction over critical infrastructure

- FSA (Finance), MIC (ICT, Local government), MHLW (Medical care, Water), MLIT (Aviation, Railway, Logistics), METI (Power, gas, credit, petroleum, chemical)
Cybersecurity Basic Act

The Prime Minister
Formulates a draft “CSS”
Offers opinions on direction and supervision of ministries

Cybersecurity Strategic Headquarters

1. Formulate the “Cybersecurity Strategy” (CSS)
2. Evaluate (including audit) the implementation of information security measures by national administrative organs.
3. Measures evaluation (including examinations for cause) event of significant.
4. Lead comprehensive coordination of cybersecurity policies (including government budget) of each ministry.

<Organization>
General manager: Chief Cabinet Secretary
Deputy general manager: Minister of State
Headquarters members:
Chairman of National Public Safety Commission,
Minister of Internal Affairs and Communications,
Minister of Foreign Affairs, Minister of Economy,
Trade and Industry, Defense Minister,
Other minister designated by the Prime Minister,
and Experts that Prime Minister appointed.

Obligated to submit materials, etc.
Recommendation
Report collection about measures based on the recommendation

Local governments,
Independent Administrative Agencies,
National Universities, etc.

National Administrative Organizations, etc.

IT Strategic HQs
Focus on promoting measures for the formation of Advanced Information and Telecommunications Network Society.

Submission of “Cybersecurity Strategy” to a Cabinet meeting for approval

National Security Council
Discussion on important issues regarding national security.

Close cooperation on important issues related to national security
Asks cooperation (e.g. necessary materials)
Main Points of Draft “CYBERSECURITY BASIC ACT” (Outline)

   1 Objectives
   2 Definitions: Cybersecurity
   3 Basic principles
   4 Responsibilities of the central government
   5 Responsibilities of local government
   6 Responsibilities of critical infrastructure providers
   7 Responsibilities of cyber-related businesses and other businesses
   8 Responsibilities of education and research institutions
   9 Endeavors of citizen
   10 Legal measures
   11 Development of administrative organs

2. Cybersecurity Strategy
   12 Cybersecurity Strategy

3. General Policy
   13 Assurance of cybersecurity at national administrative organs
   14 Promotion of voluntary measures of cybersecurity at critical infrastructure providers
   15 Promotion of voluntary activities of private enterprises and educational organizations
   16 Cooperation with multiple stakeholders, and so forth
   17 Cybercrime control and prevention of damage spread
   18 Response to matters of great concern to national security
   19 Enhancement of industrial development and international competitiveness
   20 Promotion of R&D
   21 Reservation of human resources
   22 Promotion and development of Education/learning
   23 Promotion of international cooperation

4. Cybersecurity Strategic Headquarters

5. Miscellaneous
New Information Security Human Resource Development Program (established in May 19, 2014)

Subject shown on the Cybersecurity Strategy
To handle increasing serious risks and improve the level of information security,
- It is important to raise the skill level of cybersecurity professionals within a nation and discover and cultivate exceptional personnel in the field.
- A framework is necessary for practical application of training throughout all of society.

Measure Plan

Create the virtuous circle of demand and supply of human resource to improve the level of information security.

【Demand】Awareness Reform of Executive Management

【Management of organization】
- Promoting reform of management’s awareness and efforts to let them recognize information security as business strategy.
- Encouraging investment in an organization through public requirements about information security of products & services.

【Leaders of workers】
- Improvement of communication ability about information security from the view point of the business strategy.

【Supply】Quantitative Increase and Qualitative Improve of Human Resource

- Encouraging existing ICT engineers to recognize information security as an essential ability, and Reviewing to make training materials and to arrange the evaluation criteria, qualification, etc. (ICT engineer with security)
- Discovery and development of human resources with high expertise and outstanding ability, and taking them active roles.
- Arrangement of an environment to study through international experiences and sharing information to develop global level human resources.
- Leading Strengthening of recruitment and development of officers that can respond to risks in governmental organization.
- Enhancement practical ICT education in educational institutions, and improvement of teachers’ skill of information security.
3. ICT Security Measures of MIC
Overview of MIC’s ICT Security Measures

Looking ahead to holding a safe and secure Tokyo Olympic and Paralympic Games in 2020, MIC promotes multi-lateral Cyber security projects.

- Conducting the following projects from perspectives such as network defense and enhancement of ICT security for users.

**ICT security measures for organizations**

Conducting “CYDER” project to develop skills through experiences of practical cyber defense for public office and organizations such as critical infrastructure providers since FY2013.

**ICT security measures for internet users**

Conducting “ACTIVE” project to prevent malware infection by collaborating with major ISPs for general internet users since FY2013.

**Promotion of international cooperation**

Conducting “PRACTICE” project to make predictions and quick response to cyber-attacks through collaboration with ASEAN states and other countries since 2010.

- In the future, promoting IT security measures by responding ICT environmental change such as the full-fledged spread and expansion of Internet of Things (IoT), also looking ahead to Tokyo Olympics in 2020.

**ICT security measures for M2M**

*M2M security demonstration projects: Newly requested in budget FY2015
MIC’s project for strengthening cyber-security capability in Japan

- Practical large-scale cyber exercises for LAN administrators in government agencies and critical information infrastructure providers.
- Strengthening ability to tackle Advanced Persistent Threat
- 215 people from 62 organizations such as national government agencies (e.g., MOD, NISC, MOFA, MOJ), incorporated administrative agencies and private businesses (critical infrastructure sectors), etc. participated in groups of three or four people through fifteen CYDER session.

Plan to share our experiences with international partners
ACIVE Project overview

- “ACTIVE (Advanced Cyber Threats response Initiative)” is a project of providing comprehensive countermeasures against malware by collaborating with ISPs, anti virus vendors, and so on.

- Aiming at preventing malware infection and cleansing malware, ACTIVE will alert Internet users who don’t recognize malware infection.

(i) Approach for preventing malware infection

1. Listing information on malignancy websites.
2. Alerting users when they are accessing malignancy websites.
3. Alerting administrator of malignancy websites.

(ii) Approach for malware extermination

1. Identifying user’s PCs infected by malware.
2. Sending an alert email to the users to make them aware of current infected condition.
3. Exterminating malware by complying with instructions in the email.
A malware called “GameOver Zeus (GOZ)”, which is designed to steal money by unauthorized money transfer from internet banking, has widely spread in the world.

Japan has been collaborating with Federal Bureau of Investigation (FBI) and Europe Police Union (EUROPOL) to cleanse GOZ malware since June 2014.

By using ACTIVE project, it alerts internet users who have devices infected by GOZ malware within Japan.
PRACTICE Project Overview

- R&D for catching symptoms and quick response to cyber-attacks, based on international collaboration.

R&D

Global Monitoring
Real-time capturing of attack traffic by using “darknet sensors” located in many foreign regions.

Analysis
Based on data-mining and correlation technologies, collected data/traffic is deeply analyzed.

Field Trial

Quick Response
Symptoms and new malware behavior will be an effective trigger of quick response.

As of Jan. 2015, 8 foreign countries have participated in the PRACTICE project. It is expected to cover more than 10 countries by the end of 2015.

We have succeeded in finding some symptoms of Cyber-Attacks through R&D of analyzing Cyber attacks such as DDoS.

Symptoms will be utilized in the actions taken by ISPs for their Early Response. The actions will be direct action (e.g. Filtering / Port Blocking) and/or being connected with ISP readiness against Cyber-Attacks among international participants.
The ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation (Tokyo, September 2014)
- The first Ministerial level meeting among ASEAN-Japan on theme of security.
- Japan proposed a cooperation on the following projects:
  ① JASPER (Japan-ASEAN Security Partnership)
     i) PRACTICE: a project for capturing cyber attack symptoms by using sensors located in cooperating countries and Japan.
     ii) DAEDALUS: a project for alerting to cooperating countries when it captures traffic from a device infected with a virus within the cooperating countries.
  ② ASEAN-Japan Cybersecurity Capacity Building Initiatives

ASEAN-Japan Information Security Policy Meeting
- Held the first meeting in 2009, and held the seventh meeting in Tokyo on October 7th, 8th last year.
- Discussed the concretization of the agendas from the ASEAN-Japan Ministerial policy meeting.

### Technical Collaboration (JASPER)

#### PRACTICE
- 3 countries (September, 2013)
- 5 countries (September, 2014)

#### DAEDALUS
- Start of program (September, 2013)
- 5 countries (September, 2014)

**Next step**
Plan to share findings and feedback of analysis

### Capacity Building

ASEAN-Japan Cybersecurity Capacity Building Initiatives
- Experts arrived in Indonesia (By September 2014)
- Training
  - The ASEAN-Japan Information Security Workshop 2014 for ISPs
  (October 1st and 2nd 2014)
Cooperation status with other countries

Thailand (Electronic Transactions Development Agency)

USA (United States Department of Homeland Security)

Singapore (Infocomm Development Authority of Singapore)

India (Department of Telecommunications)

Laos (Lao Computer Emergency Response Team, Ministry of Posts and Telecommunications)

EU (the Communications Networks, Content & Technology (DG-CONNECT), European Commission)

Thailand (Electronic Transactions Development Agency)

Philippines (Advanced Science and Technology Institute)

Republic of Maldives (Communications Authority of Maldives)

Malaysia (Malaysian Communications and Multimedia Commission)

Malaysia (Malaysian Communications and Multimedia Commission)

Singapore (Infocomm Development Authority of Singapore)

Indonesia (Ministry of Communications and Information Technology)

Netherlands (Delft University of Technology)
MIC’s ICT Security Measures for Tokyo 2020 Olympic and Paralympic Games

Promoting IT security measures looking ahead to ICT environmental changes in 2020 and contributing to achieving the safe and secure operation of Tokyo 2020 Olympics and Paralympic Games etc.

Experience in London 2012 Olympics, Paralympics

◆ Captured a large number of cyber attacks targeting London Olympic Games.
  "During the games, there were approx. 200 million malicious access, and DDoS attack of approximately 11 thousands access per second against the official Olympics website.
  "Based on prior information which indicated a cyber attack targeting the power supply monitoring control system of the opening ceremony stadium, operator had changed the control system from network operation to manual.

Efforts for Tokyo 2020 Olympics, Paralympics

◆ By 2020 when Tokyo Olympic Games will be held, ICT environmental changes such as the spread of IoT (Internet of Things) are expected to occur. Hence, we need to consider ICT security measures based on the assumption of appearance of new methods of attacks.
◆ To prepare for ICT environmental changes, we are conducting the following activities:
  "Enhancement of response framework for cyber attack (Sharing information of incidents status and symptoms of cyber attacks among ISPs and relevant organizations for cooperative response to cyber attack etc.
  "Promoting IT security projects such as solving problems in Machine to Machine (M2M) systems (Conducting R&D and field experiment projects against cyber attacks in the area of M2M systems).
Thank you for your kind attention.