Topic IV: Dealing with Cyber-attacks

As well as working to clarify the true state of cyber-attack cases, police are also endeavoring to prevent damage due to cyber-attacks.

As the Internet becomes an established part of social infrastructure essential to citizens' lifestyles and socioeconomic activities, incidences of cyber-attack against Japan's administrative agencies and private businesses, etc. are occurring. In particular, threats such as cyber-terrorism attacks that disable the functions of critical systems in key infrastructure and paralyze social functions, and cyber-intelligence activities using information and communications technologies are issues that can affect public safety and national security.

(1) Structure within the Police

Police are promoting comprehensive cyber-attack countermeasures by establishing a cross-departmental structure consisting of personnel from departments such as security, community safety, and info-communications within the NPA and prefectural police/prefectural info-communications departments.

In addition, technological units named "Cyberforce", established in every regional police bureau to provide the technological foundation for cyber-attack countermeasures, are implementing technological support for the prefectural police. Furthermore, the Cyberforce Center, established in the NPA to act as the control tower for the cyberforces nationwide, is operating under a 24-hour system, and is engaged in maintaining a predictive understanding of cyber-terrorism, analyzing and providing gathered information, analyzing malware attached to targeted e-mail, and issuing instructions to cyberforces as well as other activities.

Cyberforce Center

(2) Promoting Cyber-Terrorism Countermeasures

1) Status

To date, Japan has not experienced any damage due to cyber-terrorism such as social disruption caused by a cyber-attack targeting the critical systems of key infrastructure. However, there have been cyber-attacks on websites of government agencies, etc. that have interfered with browsing and other functions.

Case: In September 2011, major chat-sites in China such as "YY Chat" called on people to mount a cyber-attack on the occasion of the 80th anniversary of the Manchurian Incident, and in what are considered related cyber-attacks, browsing interference occurred on the National Personnel Authority/Cabinet Office websites and the websites of numerous private organizations were defaced.

Attack tools distributed over the Internet

2) Countermeasures

In order to prevent cyber-terrorism and to deal accurately with incidents when they occur, the police are pressing forward with various efforts such as coordination with key infrastructure businesses.

i) Information Provision through Door-to-Door Visits

Police are visiting every key infrastructure business, etc. separately to provide information on cyber-terrorism threats and information security, and are also requesting that they provide prompt reports to police when an incident occurs.

Cyber-Terrorism and Key Infrastructure

Cyber terrorism

- Electronic attack on critical systems of key infrastructure
- Major impairment of function in critical systems of key infrastructure that is highly likely to have been caused by electronic attack

Key infrastructure

- Infrastructure in the various fields of information and communication, finance, aviation, railways, electricity, gas, government/administrative services (incl. local public authorities), healthcare, water services and logistics

ii) Joint training

Police are working to improve emergency response capability by conducting joint training with key infrastructure businesses, etc. against envisioned incidents.

iii) Cyber Terrorism Countermeasure Council

Cyber Terrorism Countermeasure Councils comprised of the police and key infrastructure businesses, etc. have been established in all prefectures to distribute information from the police, host lectures by private-sector experts, and conduct exchanges of views and information sharing between participating businesses.

(3) Promotion of Counter Cyber Intelligence

1) Status

The threat of cyber intelligence has increased in recent years, and a number of targeted e-mail attacks against administrative agencies and private sector businesses, etc. occurred during 2011.

Case: In September 2011, Mitsubishi Heavy Industries was subjected to a cyber-attack and about 80 computers in factories, etc. producing state-of-the-art submarines, missiles, and nuclear power plants were found to have been infected with malware enabling information to be stolen from an external location.

Case: Following revelations that computers in the House of Representatives and the House of Councillors were infected with malware enabling information to be stolen from an external location, countermeasures headquarters were set up by the House of Representatives Secretariat in October 2011 and the House of Councillors Secretariat in November 2011, with police participation in both.

Cyber Terrorism Countermeasure Council

2) Countermeasures

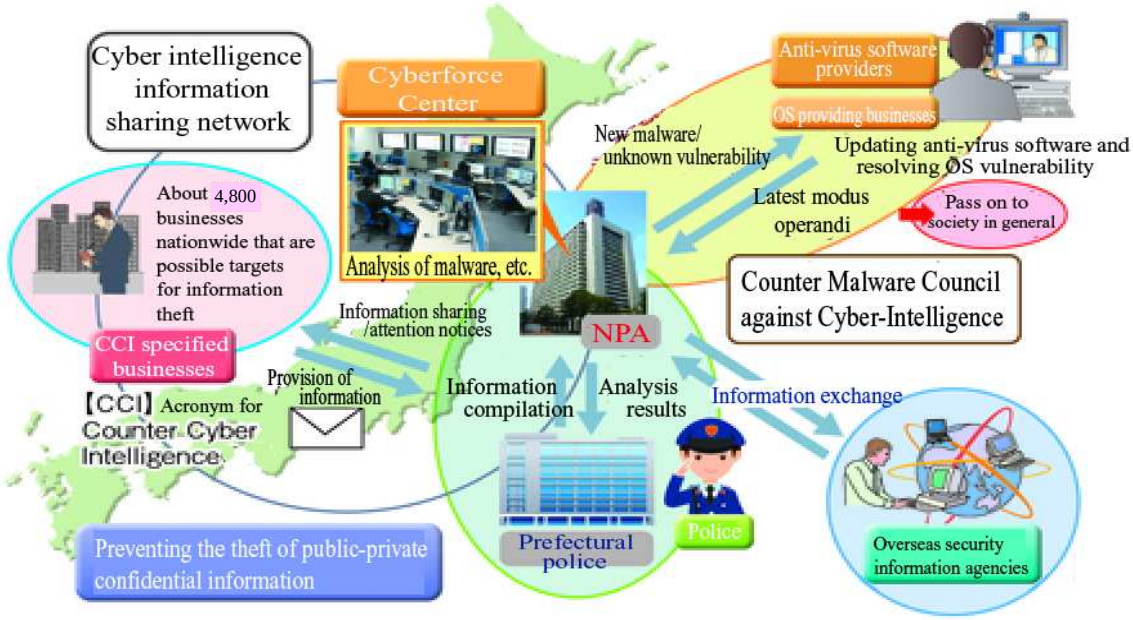
Police are working to prevent damage from the theft of information and enhancing coordination with overseas investigation agencies to reveal the true situation behind cyber intelligence activities.

i) Cyber Intelligence Information Sharing Network

In August 2011, the police constructed an information sharing network between businesses, etc. nationwide to undertake information sharing in relation to cyber-attacks that are thought to have been conducted with the intention of stealing information. As well as the compilation and analysis of information provided by businesses, etc. via the network, police are sending attention notices to businesses, etc. based on analysis results.

ii) Counter Malware Council against Cyber-Intelligence

In August 2011, the police established a council with anti-virus software providers, etc. to share information related to malware countermeasures.



Counter Cyber Intelligence Diagram

Police provide information related to malware that commercially available anti-virus software is not able to detect in order to improve information security measures.

Column: Targeted e-Mail Attacks

Targeted e-mail attacks are cyber-attacks designed to steal information by infecting recipient computers with malware that cannot be detected by commercially available anti-virus software, attached to e-mails that are sent out under the guise of legitimate business related messages.