Keidanren
Policy & Action

Proposal for Reinforcing Cybersecurity Measures

February 17, 2015
KEIDANREN (Japan Business Federation)

Damage from cyberattacks[1] is currently increasing its seriousness throughout the world. In response to this, Japan has been enhancing cybersecurity measures, such as the establishment of the Basic Act on Cybersecurity.

“Toward the Creation of a More Affluent and Vibrant Japan”, which was released by Keidanren on January 1, pointed out the necessity of measures to ensure cybersecurity in response to ICT that is becoming established as a global social infrastructure.

Especially cyberattacks against national critical infrastructures, etc. could cause hindrances in people's daily lives and economic activities. This is a serious issue that could lead to loss of the whole nation’s industrial competitiveness.

Keidanren therefore proposes specific actions toward reinforcing cybersecurity measures to protect critical infrastructures, etc.

1. Situations inside and outside Japan

(1) International situation

Due to the development of ICT society, cyberattacks have become threats that could greatly affect the entire world. Major cyberattacks have occurred in Estonia in 2007 and in Korea in 2009, 2011, and 2013, causing the government and corporate activities to stop. In the 2012 London Olympics, a massive number of cyberattacks occurred against the U.K.[2]

Cyberattacks are serious threats against national security. The Obama administration of the U.S. raised cyberspace as the 5th battleground, following land, sea, air, and space.

There was a cyberattack in the U.S. against Sony Pictures Entertainment in December of last year. Obama Administration determined that the source of the attack was North Korea and announced to take countermeasures against North Korea.

Furthermore, United States Central Command Twitter and YouTube

---

[1] Cyberattacks refer to unauthorized accesses, which utilize information and communication networks and information systems, data theft/destruction, execution of unauthorized programs, DDoS attacks (Distributed Denial of Service Attacks), etc. This is a general term that includes a wide range of crimes from those in which people steal corporate information to national-level attacks with the aim of terrorism and war.

[2] There were 212 million cyberattacks against the London Olympics official site during the 2-week competition period and 11,000 DDoS attacks per second.

accounts were hacked in January of this year.

In light of this situation, Obama administration announced in January that the government and private companies would enhance information sharing, etc.

(2) Domestic situation

A cyberattack against a defense-related company occurred in 2011, and the number of cyberattacks against government organizations and critical infrastructures, etc. has been continuously increasing since then. The targets of cyberattacks are widely varied from government organizations, critical infrastructures, companies, and individuals. Attacks are also carried out by a number of entities throughout the world.

In the National Security Strategy of Japan and National Defense Program Guidelines, which were established by the government in December of 2013, cyberattacks were positioned as major threats to security.

In November of last year, the Basic Act on Cybersecurity was established. Based on this act, the government established[3] the Cybersecurity Strategic Headquarters (Chief of the Headquarters: Chief Cabinet Secretary) and NISC: National center of Incident readiness and Strategy for Cybersecurity, which is the secretariat, within the Cabinet Secretariat on January 9.

There are concerns about the concentration of cyberattacks using sophisticated technologies against our government organizations, companies, etc. in the 2020 Tokyo Olympics/Paralympics. Reinforcement of cybersecurity measures is urgently needed.

2. Threat of cyberattacks

If cyberattacks shut down communication between Japan and overseas or shut down electricity/gas supplies or transportation networks/financial systems, etc., people's daily lives and economic activities will become paralyzed, preventing Japan from functioning as a nation.

The critical infrastructures (a total of 13 areas including information and communication services, financial services, aviation services, railway services, electric power supply services, gas supply services, government and administrative services, medical services, water services, logistics services, chemical industries, credit card services, petroleum industries) given by "The Basic Policy of Critical Information Infrastructure Protection (3rd Edition)" (May

[3] Currently, there are approximately 80 members of the secretariat.

19, 2014), which was established by the government's Information Security Policy Council, are the core of people's daily lives and economic activities. Each critical infrastructure mutually depends on each other, and cyberattacks could potentially impact the entire society.

(1) Characteristics of cyberattacks

Cyberattacks are carried out with botnets[4], etc. Identification of attackers and post-attack trace are difficult, and we cannot determine whether the attacks are carried out by organizations or individuals, etc.

In addition, attackers always maintain more advantageous positions due to reasons such as attackers being able to observe the defense system with the aim of achieving the target and being able to prepare the attacking means that are highly likely to succeed.

(2) Countermeasures against cyberattacks

Cyberattack technologies advance every day, and preventing all attacks is not realistic, considering technologies and countermeasure cost, etc. In case of cyberattacks, damage control to minimize the damage is critical; and it is necessary to accurately comprehend the attacks and swiftly respond to them. Furthermore, the establishment of cybersecurity measure policies, which are suitable for each company's business, etc., is also required.

(3) Expansion in attack targets

In addition to information systems, which are connected to external internet, control systems that are often utilized in closed status within organizations can also be targets of attack.

The objectives of cyberattacks have been expanding from the conventional information theft and falsification to impacting the entire society by shutting the functions of critical infrastructures, etc. Control systems, which support critical infrastructures, etc., are separated from the internet, but cybersecurity measures are becoming important.

As devices, such as smartphones, that provide services by connecting to the internet have been prevailing, potential cyberattack targets have also been expanding. It is expected that the attack targets will further expand as smart cars become more popular and IoT[5] develops in the future.

---

[4] Network of computers which have been infected by viruses, etc.
[5] Internet of Things: Structure to connect various "things" to the internet to mutually communicate or exchange information.

3. Cybersecurity measures against critical infrastructures, etc.

To respond to major cyberattacks that target critical infrastructures, etc., collaboration not only with the direct attack target companies but also with government organizations and other critical infrastructure operators, etc. will be necessary. The government needs to make clear its intention to protect critical infrastructures, etc. from cyberattacks and to improve deterrent capabilities.

Public and private collaboration should also be reinforced in preparation for cyberattacks. In case of an actual major cyberattack, it is difficult to respond to the attack by the target company alone. Therefore, the government should take the lead to take countermeasures.

(1) Specific policies

① Enhancement of information sharing

In order to share information against cyberattacks between public and private entities, it is important to proactively utilize the CEPTOAR-Council[6], in which critical infrastructure operators, etc. collaborate. The Cabinet Secretariat provides support for its operations and activities as well as establishing an environment necessary to enhance the activities. There are a number of other committee bodies[7], and further enhancement of information sharing systems, in which these committee bodies can collaborate, is required. The CEPTOAR-Council must continue ensuring the effectiveness through the support mainly provided by the Cabinet Secretariat.

It is necessary to consider specific methods for public and private entities to share information and knowledge regarding cyberattack damage, response, prevention, etc. When sharing such information, security of confidentiality between relevant parties must be considered.

② Implementation of training

We must specifically consider how the collaboration between public and private entities should be promoted depending on the seriousness of

---

[6] CEPTOAR (Capability for Engineering of Protection, Technical Operation, Analysis and Response) - Council): Council to share/analyze information which consists of representatives of each critical infrastructure area.

[7] J-CSIP: Initiative for Cyber Security Information sharing Partnership of Japan (Ministry/agency in charge: Ministry of Economy, Trade and Industry), Cyber Intelligence Information Sharing Network (Ministry/agency in charge: National Police Agency), Cyber Defense Council (Ministry/agency in charge: Ministry of Defense), Telecom-ISAC Japan (Ministry/agency in charge: Ministry of Internal Affairs and Communications), etc.

cyberattacks. For example, factors to consider include the scope of the attack, if it's continuous and over a long term, if it involves a series of attacks, whether or not it would lead to functional failure. It is necessary to establish the decision-making standard and response guidelines against major cyberattacks. It is necessary for public and private entities to continuously and jointly promote cybersecurity training and demonstrations.

③ Technology development and system operation

In order to enhance defense capabilities against cyberattacks, the following technologies must be developed.

- Technology to detect cyberattacks before the attacks, to disable them, and to prevent damage
- Technology that enables us to accurately and swiftly detect a series of attacks and to trace the attacker after the attack
- Information sharing technology that automatically and swiftly communicates information regarding unauthorized destinations, which are used in the attack, as well as information regarding the attack, etc. to relevant organizations and companies
- Technology to maintain system functions in response to attacks on control systems
- Cutting-edge defense technology, including attack pattern analysis
- Technology to anonymize and share information

Development of these important technologies should be included in the 5th Science and Technology Basic Plan (FY2016 – FY2020), which is scheduled to be established by the government in March of next year.

It is important to establish reliable defense systems and to continuously operate them as well as to enhance the systems' capabilities through practice, attack analysis, etc. It is necessary to consider incentives for private companies to work on such technology development and system operation.

④ Enhancement of human resources

In order to respond to cyberattacks, which are becoming increasingly sophisticated, it is necessary to develop top-level human resources and white-hat hackers with the highest technical skills. It is also important to increase human resources, who operate security systems, and enhance their skills. Government, industry, and academic entities should collaborate with each other to establish career paths for such security human resources. It is also necessary to consider a system to smoothly employ human resources, including

international human resource exchanges, in each company and ministry/agency.

Japan lacks security human resources in terms of both quality and quantity[8], so it is important for government, industry, and academic entities to collaborate with each other to ensure more human resources. Therefore, continuous and long-term efforts are required, and it is necessary to promote the activities of talented young people and women, etc.

⑤ Promotion of international cooperation

Cyberattacks are occurring throughout the world, and information available in Japan cannot sufficiently respond to them. Information should be shared with overseas government organizations and companies to promote international cooperation. For example, Japan must share information with other countries, such as Europe and the U.S., and promote cyber defense cooperation and joint demonstrations.

In order to ensure the security of cyberspace, the government needs to proactively participate in the formulation of international standards regarding cyberattacks in the UN. It is required to trace and identify attackers and enhance deterrence against cyberattacks by considering international systems for appropriate response.

In addition, Japan should improve its cybersecurity by promoting exchanges and sharing knowledge between specialists by hosting international conferences on cybersecurity in Japan.

⑥ Review of critical infrastructure areas

The current 13 areas of critical infrastructures should be reviewed to add areas, etc. as necessary. Smart cities, smart towns, and new network services, such as ITS[9], are some of the areas which could greatly impact people's daily lives and economic activities if information systems fail.

⑦ Enhancement of internet safety

Enhancement of internet safety would help prevent cyberattacks. Therefore, it is necessary for users, including individuals, to deepen their knowledge regarding internet use. Public and private entities should inform people of

---

[8] According to the Information-technology Promotion Agency, Japan, there are 265,000 security people in Japan. However, they calculate that 160,000 of them lack the capabilities and 80,000 more people are required, meaning that a total of 240,000 people (160,000 + 80,000) are lacking.

[9] Intelligent Transport Systems

methods to determine harmful email and websites, methods to respond to virus infections, and the necessity to introduce and update appropriate defense means, for example.

(2) Establishment of government system

It is necessary to centralize the division, which will represent the government and respond to damages in critical infrastructure operators, in case of cyberattacks against critical infrastructures, etc.

Rather than each relevant ministry/agency requesting reports from companies, the government should centralize the functions so that the government can aggregate information in the Cabinet Secretariat, enhance the executive capabilities of each ministry/agency, and establish a system that enables collaborative and swift responses.

Cybersecurity Strategic Headquarters is granted stern authorities based on the Basic Act on Cybersecurity. It is required to organize relevant ministries/agencies against cyberattacks, which target government organizations, critical infrastructures, etc., and to execute leadership. Cybersecurity Strategic Headquarters is required to closely collaborate with the National Security Council and the IT Strategic Headquarters and be proactively involved, including appropriately exercising their right to recommend to relevant ministries/agencies.

4. Business Community's Efforts

Cybersecurity is an important issue[10] that affects companies' reliable reputation and business continuation for not only critical infrastructure-related companies but also all companies. In addition, companies will respond to the situation, in which the targets to be protected expand from information systems to control systems and new devices, such as smartphones, and even IoT.

The business community will position cybersecurity not only as a technical issue but also as an important management task and aim to reform the awareness of the top management. We will make efforts to reform organizations and develop human resources by establishing CISOs (chief information security officers), etc. and promoting cross-sectoral information sharing and opinion exchanges between business fields under the strong leadership of the top management. Each company will establish a CSIRT[11] that responds to

[10] It also affects intellectual properties, such as trade secret, as well as personal information protection, etc.

emergencies and enhance collaboration with the CSIRTs of companies in the same business field.

In terms of human resource development, a system will start in FY2015[12] in which companies provide support (through donations, lecturer dispatching, provision of practical know-how, provision of demonstration environments and places, etc.) for companies and universities/graduate schools to collaborate and deploy security seminars to develop sophisticated security human resources.

These efforts by the business community will contribute to the enhancement of national cybersecurity.

[11] Computer Security Incident Response Team: Team that responds to incidents involving computer security.

[12] Donated courses in joint efforts by NTT/Waseda University and NEC/Japan Advanced Institute of Science and Technology will start in April of 2015.