Keidanren
Policy & Action

Second Proposal for Reinforcing Cybersecurity Measures

January 19, 2016
KEIDANREN (Japan Business Federation)

1. Introduction

Damage from cyberattacks is increasing its seriousness throughout the world. Cybersecurity is an important key to protecting citizens' safety and security. The Basic Act on Cybersecurity came into effect in Japan, and the Cybersecurity Strategic Headquarters was established in January of last year. They are not only required to promote close collaboration with the National Security Council and the IT Strategic Headquarters, but also given more authorities over each ministry/agency. Furthermore, the government's promotion structure has been enhanced with the increase in personnel and budget for the NISC (National center of Incident readiness and Strategy for Cybersecurity) in the Cabinet Secretariat. In response to the new promotion structure, Keidanren published the "Proposals for Reinforcing Cybersecurity Measures" in February of last year in order to protect critical infrastructures, etc. from cyberattacks.

On the other hand, the number of cyberattacks against government organizations and companies, etc. continues to increase in Japan[1]. In May of last year, personal information of approximately 1.25 million people leaked from Japan Pension Service due to a cyberattack. This heightened the awareness that further enhancement of measures is required in order for citizens to live safely. Serious failures in communication, broadcasting, finance, etc. have been occurring in many countries overseas.

Cyberspace is also an important place to realize growth strategies through creation of the innovations. While development of the economy and society is expected due to IoT (Internet of Things), in which various "things" are connected to the internet, measures to promote the utilization of ICT are becoming increasingly important. In addition, Japan is approaching a critical phase as Japan prepares to safely host the G7 Summit (Ise-Shima Summit), which will be held in May of this year, and the 2020 Tokyo Olympics/Paralympics. In response to these issues, the government established a new Cybersecurity Strategy on September 4 of last year.

In response to the strategy, Keidanren has published the second proposal regarding the enhancement of government-industry-academia collaboration and specific efforts by the economic industry considering the Tokyo Olympics/Paralympics.

---

[1] The number of threats of targeted attacks against government organizations has doubled in FY2014 compared to the previous year. (The number of reports from sensor monitoring, etc. was 139 in FY2013 and 264 in FY2014. The number of cautions for suspicious email, etc. was 381 in FY2013 and 789 in FY2014. Source: NISC materials)

2. Significance of cybersecurity

In order to realize a safe society in which citizens can live safely, the cybersecurity of public organizations must be ensured. Activities of not only central government ministries and agencies, but also independent administrative corporations and quasi-governmental corporations, such as Japan Pension Service, are closely involved with people's lives. Enhancement of comprehensive measures within organizations, which promote such public operations, is important. Furthermore, enhancement of measures involving local public organizations is also required in preparation for the deployment of policies to improve citizens' convenience, such as the introduction of the Individual Number system.

The business community aims to sustainably develop the economy and society through the utilization of ICT. In order to create new industries and businesses with IoT, we should ensure cybersecurity in the utilization of systems and products, which connect to the internet.

The extent of the risks[2] of cyberattacks is also increasing, such as problems in companies' business operations, loss of reliability due to information leaks, and deterioration of competitiveness. Therefore, companies also focus on cybersecurity measures.

In order for the global economy to develop, free international flow of information in cyberspace is necessary. Therefore, it is necessary to ensure cybersecurity, so that data, which is deployed on the internet, can be transferred safely and smoothly beyond the borders of nations. Furthermore, measures that inhibit international trade rules for the purpose of security measures should be corrected.

3. Cybersecurity measures

(1) Information sharing

In order for the entire society to enhance its resistance against cyberattacks, the first step is for government organizations and companies to collaborate and share information regarding attack threats and best practices in which they appropriately responded to attacks, etc. In terms of public-private collaboration, two-way information sharing is required not only for companies to provide attack information but also for the government to provide threat information, analysis results, etc. that companies and the government acquire on their own.

Collaboration between private companies requires cross-industrial collaboration as well as expanding the existing information sharing systems in each industry to

[2] Include risks in which victims of cyberattacks potentially become attackers for third parties.

other industries. ISAC[3] has already been established for information sharing in each industry of communication and finance. Support should be provided by public and private entities so that other industries can also promote such activities. Promotion of information sharing, which utilizes such systems, is especially required in 13 critical infrastructure areas (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). It is also necessary to promote the collaboration between CSIRT[4] in companies that are relevant to critical infrastructures and to share information, respond to incidents, and promote training. Therefore, operation and activities of the CEPTOAR-Council[5] will continue to require NISC's support.

Cybersecurity of the entire society will be enhanced if companies other than critical infrastructures share/analyze information and respond to incidents in a similar manner as ISAC and CSIRT.

In order for companies to provide appropriate information to the government and relevant organizations, a system to maintain confidential information is required. For example, it is necessary that information sharing methods by anonymizing information, etc. are agreed upon between public and private entities as well as between private companies[6].

(2) Human resource development

The foundation that supports cybersecurity is human resources, and human resource employment and development are required in various industries, mainly including critical infrastructure areas. First of all, it is important to clarify the requirements of human resources based on the roles that the business community must play. It will be necessary to develop not only personnel in charge of operating information systems, but also human resources who can respond to incidents in

---

[3] ISAC (Information Sharing and Analysis Center): Institution which shares/analyzes security-related information.

[4] CSIRT (Computer Security Incident Response Team): Team that responds to computer security-related incidents.

[5] 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.

[6] In financial ISAC, there are rules for information provider to specify the scope in which the information is shared.

relevant divisions. In addition, not only human resources with technical knowledge, but also human resources with knowledge of laws, economy, and international politics, etc. will be required. Based on these issues, the “Cross-industrial Cybersecurity Human Resource Development Committee”[7], which is comprised of 40 major companies mainly including critical infrastructure areas, has been considering the requirements for human resources that are in line with the characteristics and reality of industries/companies in Japan.

Educational institutions, such as universities and technical colleges, are required to offer education according to the required level of human resources. In addition, local universities collaborating with local public organizations and local companies and producing human resources by utilizing their advantages would also lead to enhancement of cybersecurity awareness and local rejuvenation. Furthermore, the cultivation of ethical views will also be required in elementary and secondary education to enhance literacy and utilize technologies correctly.

Formulation of systems and standards to assess human resources, which are developed by educational institutions, will help companies employ specialized jobs according to the level they seek and clarify career paths. In addition, utilization of domestic and overseas qualification systems is also effective, such as the establishment of a registration system based on the Information Security Specialist Examination and the introduction of the Information Security Management Examination.

In order to promote the activities of human resources in companies, assessment and treatment must be reviewed. It will be necessary to clarify assessment and establish career paths for a wider scope of human resources from those who work with practical level operation/management involving security to system developers, in addition to top-level human resources and white-hat hackers. On the other hand, the government should also employ talented human resources through appropriate treatment, etc. according to the level of expertise.

In addition, the enhancement of the existing human resources capabilities and activities as well as organizational review will be important in companies. Due to the fact that a wide variety of human resources will be required according to the capabilities, field, and work contents, the government, industry, and academia must collaborate to establish an ecosystem[8] that can develop and maintain human

---

[7] “Cross-industrial Cybersecurity Human Resource Development Committee” interim report (http://cyber-risk.or.jp/sansanren/).

[8] Ecosystem to develop/maintain human resources: System for development and employment through government-industry-academia collaboration in which

resources.

(3) Establishment of systems with high security levels

① Social systems

Critical infrastructures, such as information and communication services, electric power supply services, and financial services, are social systems that provide services that greatly impact people's daily lives and economic activities. Public and private entities must closely collaborate with each other to protect these services in particular, so that their functions do not shut down or slow down.

In terms of critical infrastructures, an enhancement of cybersecurity measures and a review of the scope, etc. will be required. For example, some of these aspects will include the addition of ITS[9] and smart cities as part of critical social infrastructures as well as the addition of peripheral facilities of critical infrastructures to ensure effectiveness.

Furthermore, risk analysis of critical infrastructures is required in order to establish effective security systems and promote demonstrations/training.

In case of emergencies, in which major cyberattacks against the government or critical infrastructures result in disruption of people's daily lives, a system in which sophisticated human resources can flexibly function between government, industry, and academia will be important, so that the right people can work in the right places.

② Technology development and system operation

It is necessary to promote technology developments and system operations that link to systems, which become varied as a result of threat advancement, development of IoT, etc., and to swiftly respond to attacks that occur. Enhancement in measures is necessary not only for information systems, but also control systems, which are not connected to the internet.

Some of the technology development issues are detection of malicious communications, behavior analysis, attack prediction analysis, information sharing technologies, system function maintenance, information protection, anonymization of information, and quick recovery. Industry expects that the 5th Science and Technology Basic Plan by the government will clearly indicate these items as

---

required security human resources are employed/maintained not only in ICT companies and security-related operators, but also in user companies in the business community respectively. Refer to ("Cross-industrial Cybersecurity Human Resource Development Committee" interim report).

[9] ITS (Intelligent Transportation Systems)

critical technology development issues.

In terms of operation, daily operation in anticipation for cyberattacks will be important in order to stably operate systems. For example, this involves information maintenance and utilization, etc., such as system operation and various logs.

In addition, it is also important to minimize damage through swift responses, etc., considering the fact that complete defense against attacks is difficult.

Government must consider incentives for private companies to work on such technology developments and system operations.

Industry has hopes of the efforts toward these issues through the social implementation of the “Research and Development Plan to Ensure Cybersecurity in Critical Infrastructures” by the Cross-ministerial Strategic Innovation Promotion Program (SIP), which is being promoted by relevant ministries and agencies under the leadership of the Cabinet Office. Furthermore, the IoT Acceleration Consortium, which is being promoted through the joint efforts of public and private entities, is required to consider highly secure systems.

(4) Promotion of international cooperation

The main parties of cyberattacks are globally active, and the number of attacks by international terrorism organizations is also increasing. In light of this situation, international cooperation must be the first step. While it is difficult for the government to directly provide information to companies regarding responses to attacks which take place outside of Japan, provision of the latest information from the government within the possible scope will be necessary in order to prepare for sophisticated attacks prior to such attacks.

Public and private entities are required to proactively participate in international discussions regarding cybersecurity so that Japan can ensure free international flow of information in cyberspace with the aim of promoting international cooperation.

The government should also make efforts to enhance cooperation with other countries in the field of security. With the U.S., promotion of cyber defense cooperation was incorporated in the “Guidelines for Japan-U.S. Defense Cooperation”, which was revised by the Japanese and the U.S. governments, in April of last year for the first time. In addition to this, Japan should enhance internet economy policy cooperation dialogues and cyber dialogues and work on human resource exchanges, information sharing, joint training, and technology

development, etc., between public and private entities[10].

With Europe, Japan should work on exchanging opinions between public and private entities based on the establishment of the system regarding information sharing[11]. With ASEAN and other countries in the Asia-Pacific region, international cooperation is required to build a capacity (capacity building), including human resources in the cyber area. In the future, Japan should also promote information sharing with Latin America and Middle Eastern and African countries as much as possible.

(5) Response to the Tokyo Olympics/Paralympics

The Tokyo Olympics/Paralympics will be held in 2020. The success of this event will be a touchstone for Japan to host major international events. As the number of cyberattacks is concerned to increase in the future, comprehensive measures for event venues and systems that are directly involved with them as well as peripheral facilities and systems that are indirectly involved with them, etc. will be required.

First of all, relevant companies should establish CSIRT and enhance the information sharing network in preparation for cyberattacks. CSIRT, which will be the core, should immediately be established under the government or an organizational committee. Next, relevant organizations, including government organizations and core CSIRT, will be required to participate and thoroughly promote demonstrations/training in order to jointly detect attacks and defend against them in preparation for various attacks. Through these efforts, information and responses to attacks on organizations will be swiftly shared, which will lead to prevention of new attacks and reduction of damage.

Development of students would not be sufficient for human resources who will be able to respond to threats of cyberattacks surrounding the 2020 Tokyo Olympics/Paralympics. The effective measure would be to enhance the capabilities of the existing human resources in the business community. By identifying human resources with great potentials within the business community, enhancing their basic knowledge, and enhancing onsite training, etc., human resources can be enhanced. The government and educational institutions will be required to provide

---

[10] The joint declaration in the “52nd Japan-U.S. Business Conference”, which was held in Washington D.C. in December of 2015, announced that Japanese and U.S. governments and business communities should promote discussions on public and private cooperation in the cyber field.

[11] Direction to mandate business reports from critical infrastructure operators and service providers was established based on the Network and Information Security Directive.

incentives and education/training for companies to develop human resources.

The government and relevant organizations, mainly including NISC, should immediately formulate a detailed roadmap for the establishment of such systems and necessary measures, and implement the roadmap with all their energy.

We can utilize the foundation established for the Tokyo Olympics/Paralympics to protect Japan from cyberattacks even after 2020.

4. Business Community's Efforts

The business community will position cybersecurity as an important risk management task in business management, promote the fact, and reform the awareness of the top management.

Specifically, the business community will voluntarily and swiftly promote the establishment of CISO [12], etc. as well as supporting organizations/systems, information sharing, human resources development, and system enhancement, etc. In terms of employment and development of security human resources, we will also consider career paths and treatment, and aim to establish a human resource development ecosystem. The business community will refer to the “Cybersecurity Management Guidelines”, which were formulated by the government in December of last year, and aim to establish corporate management systems, comply with rules, and enhance employee literacy. The business community will review organizations, so that security-related divisions and other relevant divisions can closely collaborate with each other. We will also work on measures not only within a single company but also by involving supply chains.

The business community will voluntarily disclose information regarding our efforts toward cybersecurity, considering the aspect that information disclosure also enhances corporate values due to our accountability for stakeholders.

In terms of business, the business community will develop/operate systems and provide products/services based on the concept of “security by design”. The business community will also continuously design systems, such as risk assessment and scope of compensation, etc. and provide cybersecurity insurance.

Through these activities, the business community will realize a social system that is resistant against cyberattacks and contribute to the enhancement of Japan’s cybersecurity.

[12] CISO (Chief Information Security Officer)