Cybersecurity Symposium 2015

The challenge of dealing with cyberattacks in Japan
Why do they keep happening?

September 4, 2015: Conference Hall, 1St Members' Office Building of the House of Representatives Conference report

Cybersecurity Symposium 2015 Executive Committee
Member of the House of Representatives, Mr. Takuya Hirai,
IT Strategy Mission Chairman, Liberal Democratic Party
Japan Business Federation Keidanren
Telecom – ISAC Promotion Conference,
Japan Data Communications Association
NPO Japan Network Security Association
Executive Committee Secretariat: Microsoft Japan
(Honorifics omitted)

A total of 114 applications were received for the symposium, with a capacity of 100, of which more than 90% attended on the day. The reception desk at the conference hall received requests for materials from the offices of more than 20 Members of the House of Representatives. The following is a report on this successful conference, which featured a wealth of interesting debate.

One point that was emphasized throughout the symposium was "the poor level of awareness of cybersecurity in Japan". From various discussions throughout the day, it became clear that the issue is often derided by the financial officers of corporations as "an unnecessary burden" and that many small and medium sized enterprises do not yet fully understand cybersecurity.

---

1) Cybersecurity and policy issues in Japan

Member of the House of Representatives, Mr. Takuya Hirai, IT Strategy Mission Chairman, Liberal Democratic Party

House Member Mr. Hirai opened the symposium with a confident statement. "When people hear of cybersecurity, they imagine that it's all going to be very difficult, but I feel we should try to enjoy it a bit more as we tackle this issue. As we push ahead with digitization and globalization, cybersecurity has become an essential measure for us to ensure the happiness of the people and the interests of the nation. And it's not an insurmountable ordeal. It should actually be a very positive topic."

Mr. Hirai went on to touch upon the amendment to the "My Number" national identification system law, and commented on important points that are connected to future policy issues, saying "More important than the My Number system itself is the amendment to the Personal Information Protection Law."

衆議院議員
自由民主党IT戦略特命委員長
平井 卓也
日本におけるサイバーセキュリティと政策課

"Worrying about the utilization of data as so-called 'open data', while trying to properly protect personal information, is a bit like putting your foot on the accelerator and the brake pedal at the same time. (In a world where the situation is changing from moment to moment) taking this kind of little by little adjustment approach at each turn is going to leave us with anxiety in the future. Moving forward, as we amend the Cybersecurity Basic Law, I believe it will be important to have legislation introduced by Diet members for basic laws for the promotion of the utilization of data in the public and private sectors as well." And, addressing future policy directions, with regard to the My Number scheme, Mr. Hirai said "A lot of the misunderstanding about the My Number scheme comes from people confusing it with the national identification number scheme that was proposed under the Satoh administration in 1968. But the My Number scheme is actually part of the infrastructure for the creation of an advanced IT society." So saying, Mr. Hirai stressed the importance of having a wider understanding in the development of a society that is capable of leveraging digitization.

2) Cybersecurity in the Japanese economy and the protection of critical infrastructure

Toshinori Kajiura, Chairman, Private Internet Economy Working Group, Committee of Information and telecommunication

Chairman, Cybersecurity Council, Japan Business Federation Keidanren

Continuing, Mr. Kajiura spoke on the importance of cybersecurity across all industries, from the perspective of "the development of the Internet and the economy", starting with the "Fin Tech" wave (Fin Tech, coined from "Finance and Technology", refers to IT-leveraging startups in the financial industry) that is sweeping the financial industry.

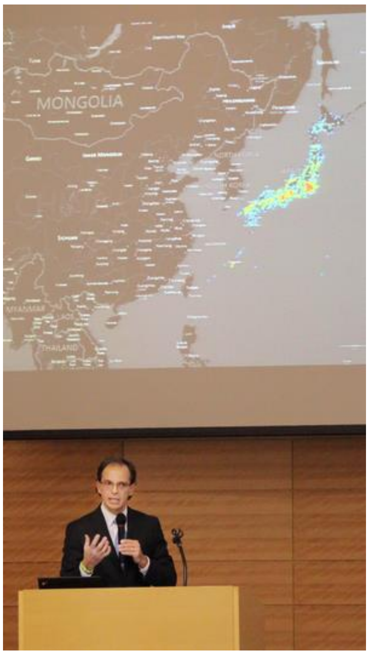
Mr. Kajiura described how "Forced Localization Measures" (referring to the exclusionary policies adopted by some countries under the pretexts of information security, national security, product safety standards and the nurturing and protection of domestic industry, etc.), which constitute a serious hindrance to market access, are becoming a point of contention.

Speaking about Japan's domestic situation, quoting to a list of incident case studies compiled by Keidanren and the Federation's "Proposals for the strengthening of cybersecurity countermeasures. (Feb. 17, 2015)", Mr. Kajiura pointed out that Japan still lacks sufficient cybersecurity countermeasures in the whole society and also told that it is required for industry to raise an awareness such as people development and knowledge sharing.

3) Front line cybercrime countermeasures, with a focus on the US – Latest information on botnet countermeasures and other front line cybercrime countermeasures

Mr. Richard Boscovich, Senior Attorney, Digital Crimes Unit, Microsoft Corp. (with simultaneous interpreter)

The third speaker was Mr. Richard Boscovich, Senior Attorney at Microsoft's DCH (Digital Crimes Unit), who spoke about the activities of DCU in its regional headquarters throughout the world (Washington, Berlin, Beijing, Singapore, Tokyo), presenting examples of successful operations against botnet and malware, etc., in the period 2010 to 2015 (including the online financial malware Zeus, stopped in March, 2012, and Ramnit, stopped in February, 2015).



Mr. Boscovich demonstrated the Cyber Threat Intelligence Program that works to make visible the threat from malware currently active, both domestically and abroad, following more than 500 million transactions per day, and as well as describing the botnet "Citadel" that is currently active in Japan, spoke about the "Azure Active Directory Premium security report" and Microsoft's privacy policy, etc. Mr. Boscovich emphasized the importance of having a reliable infrastructure.

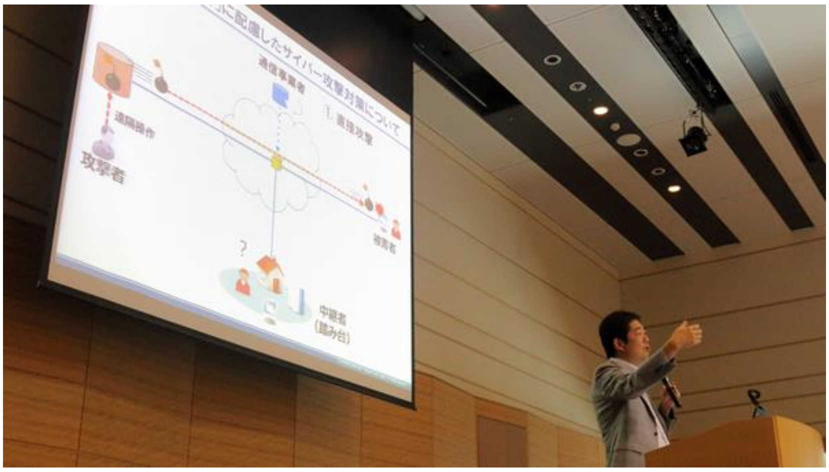
4) Dealing with cyberattacks in Japan’s communications infrastructure – Responses to cyberattacks in the communications infrastructure and the issues involved

Mr. Satoru Koyama, Steering Committee, Telecom – ISAC Promotion Conference, Japan Data Communications Association

The final speaker in the morning session, Mr. Koyama from the Telecom – ISAC Promotion Conference, spoke on the particular importance of protecting the “secrecy of communication” (guaranteed as a basic human right in Japan’s constitution, Article 21-2) as a security measure in the age of “IoT (Internet of Things)”, and presented examples of cyberattacks.

Mt. Koyama stressed the seriousness of the security situation, explaining that, while the hijacking of home routers, which exist in ordinary homes, is becoming a hotbed of crime, “The number of users that update their home router software on their own initiative is less than 1%. In contrast, if the ISPs try to provide sufficient support, the costs involved would be more than ten thousand yen per router. So, we have a situation where service charges in no way match the costs of the provision.”

“Working in cooperation with the police, it took three years to finally deal with a single case of home router hijacking. Once the age of IoT gets underway, the situation will become a lot tougher”, Mr. Koyama commented.



Mr. Koyama concluded by saying that the important thing is to “Promote the switch from a business model of simply selling devices to one of continuous service provision, and work to create systems so that we don’t end up with “IoT left to its own devices”. The concept of the Intranet of Things is also important.”

5) “New CyberSecurity Strategy”

Mr. Seitaro Fujita, Cabinet Councilor, National Center of Incident readiness and Strategy for Cybersecurity

Following the lunch break, Mr. Seitaro Fujita, Cabinet Councilor, National Center of Incident readiness and Strategy for Cybersecurity, took the stage.

Mr. Fujita presented some details of the “New Cybersecurity Strategy” that had just been approved by the Cabinet that morning, and also spoke on the cybersecurity measures being adopted by government agencies, etc., in the light of the Japan Pension Service information leakage incident that occurred in June, 2015.

The number of threats made against government agencies in 2014, announced at the end of August, 2015, was 264 for incidents reported by sensor monitoring, etc., approximately double the number of the previous year. The number of alerts regarding suspicious emails was 789, a significant increase on the 381 cases reported in the previous year.

While these numbers are expected to increase in 2015, Mr. Fujita commented on some important steps that are being taken, such as the “strengthening of government-wide initiatives”, “strengthening of initiatives relating to critical infrastructure”, and “promotion of policy dialogue aimed at international cooperation”, etc.

6) Panel discussion on cyberattacks
The challenge of dealing with cyberattacks – Why do they keep happening?

■Moderator:

Masakazu Takahashi (Vice President, NPO Japan Network Security Association)

■Panelists:

Mineyuki Fukuda (Member of the House of Representatives, Cabinet Ministerial Aide, Executive Director IT Strategy Mission, Liberal Democratic Party)

Mamoru Saito (Telecom – ISAC Promotion Conference, Japan Data Communications Association)

Toshinori Kajiura (Internet and Economy Working Group Chairman, Cybersecurity Council Chairman, Japan Business Federation Keidanren

Takashi Manabe (Board Member, Chief of Analysis Center, JPCERT Coordination Center)

Richard Boscovich (Senior Attorney, Digital Crime Unit, Microsoft Corporation)

The final session, a panel discussion, was joined by House Member and Cabinet Ministerial Aide, Mr. M. Fukuda.

Moderator, Mr. M. Takahashi, started off the panel discussion by summarizing with a series of thought-provoking statements, such as “Approximately 90% of businesses have already been targeted.” “Once they know they have been the victims of an attack, when they trace back to find out exactly when this was, the median is ‘about 240 days ago.’” and “Cybersecurity damages world-wide are around 360 trillion yen per year.” “The damage per incident is 420 million yen.” The panelists responded with many comments full of ideas and suggestions.

“(Travelling in my home constituency) I speak with ordinary people in a variety of capacities, and I hear from many of them that “Cybersecurity is something for big companies to take care about”. Some people also say “We don’t have any information that is worth stealing. We don’t need any security.” In order to change this situation, we need to have cybersecurity understood more widely. I think it’s important that we explain security in a way that is more easily understood by the general public.” (Mr. Fukuda)

Mr. Fukuda touched on some of the many challenges that exist, such as the difficulty faced by government agencies in securing the kind of talented individuals necessary for cybersecurity. He also spoke forcefully on the attitude of the Cabinet as it worked to resolve the proposed amendment.

“We’re not working to develop our IT provision in order to create an uncomfortable country. Including the revision of the Cyber Security Basic Law, we have been working to create a country where people can feel safe and at ease.”

Mr. T. Manabe from JPCERT Coordination Center explained that "In Japan, it was the discovery in 2011 of incidences of targeted attacks against companies in heavy industry that gave extra momentum to the implementation of countermeasures", and presented various examples of "targeted attacks", such as "watering hole attacks" and "update hijack attacks", etc.

In his final statements, Mr. Manabe echoed the concerns raised by Mr. Fukuda, saying, "In our activities, we recognize that the biggest hurdle that we have to overcome is not a technical issue, and it is not even the presence of the attackers. It is this "difference in awareness" that exists between us and the companies those are needed to respond to such incidents. I feel that overcoming this obstacle is our first mission."

Mr. M. Saito from Telecom – ISAC Promotion Conference spoke about a scan survey that had been conducted since 2012 with the help of ISAC volunteers to try to find out just how many of the "clearly vulnerable home routers" being sold in Japan there are. "A rough estimate puts the number in Japan at 1.2 million routers that can be used by criminals as the springboards for their attacks," revealing just how dangerous the situation is.

Continuing, Mr. Saito presented the theory that "Just like triage is carried out for infectious disease, holistic countermeasures should be required for protection against incident in the field of cybersecurity."

The panel discussion concluded with a wrap-up by the moderator, Mr. Takahashi, on the inter-dependency of information infrastructures, information sharing across segment boundaries, effective countermeasures, cloud devices and other developments in the IT environment, the importance of management, and security initiatives with regard to policies based on growth strategies.

真鍋敬

真鍋敬
福田峰

ICTにかかわる相互依存性