JCIC
Japan Cybersecurity
Innovation Committee

March 9th, 2018

Cybersecurity Information Sharing Survey

[Outline]

- Major countries of the world are encouraging the sharing of information on cybersecurity by enacting national cybersecurity laws and regulations. Japan should maintain a close watch on the status of these countries to see whether these laws and regulations enhance their cybersecurity levels and whether public-private partnerships are being conducted in a successful manner.

Country / Region	Information Sharing Policy
US	Encouraged cybersecurity information sharing by enacting Executive Order 13691 in 2015. Following that, severe regulations, such as the obligation to report a breach of cybersecurity to the authorities within 72 hours, were enacted in some sectors.
EU	Published GDPR[1], which requires notification of a PII breach within 72 hours. A private company that violates GDPR faces a massive fine. The *NIS*[2] *directive* instructed EU countries to enact cybersecurity laws to secure their critical infrastructures.
UK	The UK government can impose fines of up to £17 million on critical infrastructure organizations that fail to implement appropriate cybersecurity safeguards.
Singapore	Critical Information Infrastructures need to report cybersecurity incidents to the Cyber Security Agency (CSA). The maximum penalty for a failure to do so is a fine of up to $100,000 or a prison term of up to two years.
South Korea	When cyber incidents occur in the private sector, the incident details are reported to the National Intelligence Service (NIS) via the Ministry of Science, ICT and Future Planning.

- For its part, Japan should consider creating laws or regulations to address the need to give notification of a cybersecurity breach and also define penalties for inappropriate cybersecurity safeguards. In reality, Japan needs a step-by-step approach because there are a lot of reporting lines for cybersecurity incidents, and they change depending on what information has been stolen. As a first step, the Japanese government needs to clarify the reporting lines, reporting content (required information), and reporting format.
- Human resources in Japan are wasted by having to sort through cybersecurity information from a lot of different information sources, which equates to a large amount of incident information. An automated indicator sharing system is needed and should be implemented in both the public sector and the private sector.

[1] General Data Protection Regulation

[2] Network and Information Security

1. Japan is lagging in private-private partnerships

Japan was ranked 11th globally in the International Telecommunication Union's (ITU) Global Cybersecurity Index (GCI)[3] in 2017. The GCI is a survey that measures the commitment of countries to cybersecurity. The survey evaluates cybersecurity according to five criteria—legal, technical, organizational, capacity building and cooperation—when assessing a country's commitment.

The survey made it clear that Japan had not yet matured in the area of cybersecurity metrics, incentive mechanisms, and public-private initiatives (see Figure 1). In comparison, leading cybersecurity countries all conduct a national cybersecurity assessment on a regular basis and determine if stricter and more severe regulations are necessary in order to enhance their national cybersecurity level.

(Figure 1) Global Cybersecurity Index

#	Member State	**GCI Score**	**Cybersecurity metrics**	**Incentive mechanisms**	**Public-private partnership**
1	Singapore	0.925	🟩	🟩	🟩
2	United States of America	0.919	🟩	🟩	🟨
3	Malaysia	0.893	🟩	🟩	🟩
4	Oman	0.871	🟩	🟩	🟩
5	Estonia	0.846	🟩	🟨	🟨
6	Mauritius	0.830	🟩	🟩	🟩
7	Australia	0.824	🟩	🟨	🟥
8	Georgia	0.819	🟩	🟩	🟩
8	France	0.819	🟨	🟩	🟨
9	Canada	0.818	🟩	🟨	🟩
10	Russian Federation	0.788	🟩	🟩	🟩
11	Japan	0.786	🟥	🟥	🟥

Note: 🟩 Leading 🟨 Maturing 🟥 Initiating

[3] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx

2. Current status of and issues with cybersecurity information sharing in Japan

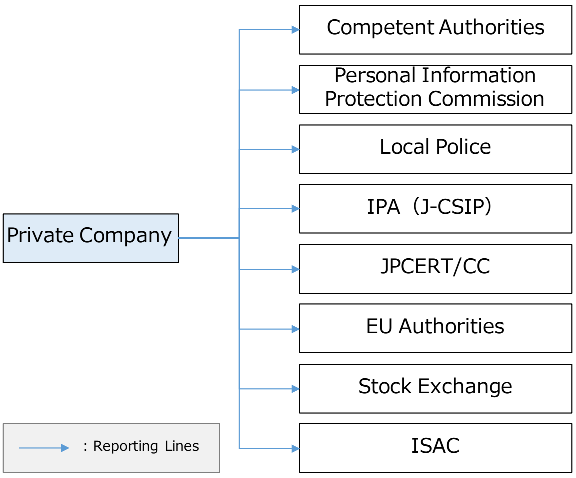
[Current status of Japan's cybersecurity information sharing]

In order to enhance cybersecurity and public-private information sharing, the Japanese Diet (parliament) adopted the Cybersecurity Basic Act in November 2014, and an amendment to the Act was promulgated in April 2016. Unlike the leading cybersecurity countries, Japan has not drafted laws or regulations addressing the need to give notification of a cybersecurity breach within 72 hours, nor outlined penalties for inappropriate cybersecurity safeguards.

Before creating stricter and harsher cybersecurity laws in Japan, the Japanese government needs to define to which authorities organizations should report such a breach and what should be reported. This is necessary because there are a lot of reporting lines and they will likely change according to what information has been stolen (see Figure 2).

As Figure 3 shows, cybersecurity incidents have been reported to different public organizations, such as local police, the IPA (Information-technology Promotion Agency, Japan) and the JPCERT/CC (Japan Computer Emergency Response Team/Coordination Center). The types of reports differed slightly different, so we should not jump to any conclusions, but this is evidence that there are a lot of reporting lines in Japan.

(Figure 2) The reporting lines of breach notifications in Japan



(Figure 3) Number of breach notifications and inquiries (From April to September 2017)

Organization Name	Type of Breach Notification and Inquiry	Total
Local Police	Number of inquiries about cyber attacks[4]	6,848
IPA（J-CIPS）	Number of inquiries regarding information sharing[5]	1,270
JPCERT/CC	Number of inquiries notifications of breaches and vulnerabilities[6]	10,221

[4] http://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_kami_cyber_jousei.pdf

[5] https://www.ipa.go.jp/security/J-CSIP/index.html

[6] https://www.jpcert.or.jp/ir/report.html

Diverse information sources and the huge amount of incident information are also an issue. Human resources in Japan are wasted by having to sort through and select pertinent cybersecurity information—despite the lack of a cybersecurity workforce.

An automated indicator sharing system that enables a reduction in human resources has recently been set in place. In 2017, the NISC (National Center of Incident readiness and Strategy for Cybersecurity in Japan) joined the Automated Indicator Sharing (AIS) program, which is led by US Department of Homeland Security (DHS), but the use of the AIS program has never been popular in Japan.

[Japanese cybersecurity information sharing issues]

- Japan should consider passing laws or regulations making it mandatory to report a cybersecurity breach within 72 hours and should enforce penalties for inappropriate cybersecurity safeguards. As a first step, the Japanese government needs to clarify the reporting lines, the contents of the information to be reported, and the reporting format.
- An automated indicator sharing system is needed and should be implemented in both the public sector and the private sector. The Japanese government should lead such an automated information sharing system.

－ Legal Notice －

- ■ The JCIC does not take responsibility for the correctness, up-to-datedness, or quality of the information provided in any report.
- ■ The permission of the copyright owner must be obtained, in principle, provided that such permission is not required under certain circumstances permitted by law. When reusing a JCIC report, please identify the source such as [Source: JCIC].
- ■ JCIC contact information：info@j-cic.com