JPCERT/CC Activities Overview

January 1, 2019 ～ March 31 , 2019

JPCERT Coordination Center
April 11, 2019

Activity Overview Topics

ー Topic 1ー " Research on Latin American and Caribbean CSIRT Trends (FY2018)" published

JPCERT/CC has published the " Research on Latin American and Caribbean CSIRT Trends (FY2018)," which summarizes the results of a research regarding the CSIRTs of Latin American and Caribbean nations as well as organizational structure and other matters concerning cyber security, based on published literature and local interviews.

Cyber attacks occur irrespective of national borders. In some cases, attacks are carried out from an overseas network against Japanese users, while in other cases they are carried out from a network in Japan against users overseas. In the coordination and resolution of these cross-border incidents, information sharing and cooperation between CSIRTs, which serve as national liaisons, are indispensable. For this reason, JPCERT/CC has been making efforts to enhance partnerships with overseas CSIRTs to enable smooth response to incidents requiring cross-border cooperation, through participation in FIRST, APCERT and other international CSIRT communities With regard to the Latin American and Caribbean regions, which are among the remotest areas from Japan, while there has been information sharing in the past in response to incidents, there are very few documents that provide structured information in Japanese about the CSIRTs and systems and other matters concerning cyber security in each country. As such, the actual situation in these regions was not fully understood.

This report describes the results of a research into the status of partnerships among CSIRTs in the Latin American and Caribbean regions led by the Organization of American States (OAS) and Latin America and Caribbean Network Information Centre (LACNIC). It also sheds light on the activities of National CSIRTs in Mexico and Brazil, the 2 countries where the most advanced cyber security initiatives in the region are undertaken, and the cyber threats they are faced with. The research was conducted based on published literature and local interviews.

ー Topic 2ー Japan Security Analyst Conference 2019 held

The Japan Security Analyst Conference 2019 (JSAC2019) was held on January 18, 2019 at the Ochanomizu sola city Conference Center. This conference was held with the aim of sharing information about ever-changing attack methods and new analytical techniques, to help improve the technical capabilities of security analysts who analyze and handle cyber attacks. Two hundred and ninety-seven security analysts participated in this second conference. In response to the call for papers, 18 applications (domestic: 12; overseas: 6) were submitted, of which 8 were chosen to be presented at the conference. The presentations covered technologies for incident analysis and response, including malware analysis and incident handling, and provided information about the presenters' own new technological discoveries and analysis methods. While the previous conference also had participants from overseas, this year's conference featured presentations by overseas analysts as well, taking JSAC a step further in terms of internationalization.

Presentation materials from JSAC2019 are made available excluding some speeches, and snapshots of the presentations are provided on JPCERT/CC Eyes as well. JPCERT/CC will continue to provide information and engage in activities that are useful to experts who analyze and handle incidents.

Japan Security Analyst Conference 2019（Japanese）
https://jsac.jpcert.or.jp/
Japan Security Analyst Conference 2019 -Part 1-
https://blogs.jpcert.or.jp/en/2019/02/jsac2019report1.html
Japan Security Analyst Conference 2019 -Part 2-
https://blogs.jpcert.or.jp/en/2019/02/jsac2019report2.html

ー Topic 3ー ICS Security Conference 2019 is held

On February 15, 2019, JPCERT/CC held the ICS Security Conference 2019 in Asakusabashi, Tokyo. About 300 visitors who registered in advance attended the conference, representing a diverse mix of professionals: 30% asset owners, 11% ICS equipment vendors, 15% ICS vendors, 11% ICS engineering firms and 5% researchers. When the first conference was held 10 years ago, ICS vendors accounted for most of the participants.

In recent years, however, asset owners have come to occupy a significant portion of the participants, indicating that the importance of recognizing cyber security risks, collecting information needed to continue the company's business safely and taking action accordingly has become widely understood. At the conference, speeches were given on 7 topics, including 2 that were submitted in response to the call for papers. The presentations discussed the latest threat information and scenarios to be anticipated regarding ICS security, trends related to guidelines and standardization and initiatives undertaken in relation to cyber security in the maritime, railway and insurance fields, methods for handling cyber security in a functional safety system, and security countermeasure guides for the introduction of industrial IoT, among other subjects.