JPCERT CC®

JPCERT Coordination Center

JPCERT/CC Activities Overview Topics

January 1, 2024 ～ March 31, 2024

JPCERT Coordination Center

April 18, 2024

Activity Overview Topics

－Topic1－ JPCERT/CC Launched a Contact Form for Consultation from First Responders

As cyber attacks grow increasingly sophisticated and ransomware attacks increase, there are increasing cases where a quick decision must be made on initial incident response based on fragmentary information. In these cases, it is often difficult to make the initial move based on the knowledge of the affected organization and first responder (a security vendor, operation and maintenance company, or other entity that assists with the initial response) alone. In light of these circumstances, the Japanese Ministry of Economy, Trade and Industry (METI) released "Guidelines for Handling and Utilizing Attack Technology Information" on March 11, 2024. These guidelines are intended to facilitate information sharing among expert organizations that support the incident handling of affected organizations. In formulating these guidelines, JPCERT/CC worked with METI to serve as a joint secretariat and was also responsible for creating a draft.
However, these guidelines alone do not enable immediate sharing of information among expert organizations, and such activities are limited even today. To help bridge information sharing among expert organizations and first responders, we opened a new contact form on March 25 that responds to consultation from organizations supporting damage investigations, such as security vendors and system operators, as well as organizations affected by cyber attacks.

JPCERT/CC incident consultation and information sharing (for affected organizations and maintenance and investigation vendors) (Japanese)
https://www.jpcert.or.jp/ir/consult.html

METI "Guidelines for Handling and Utilizing Attack Technology Information" (Japanese)
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/cyber_attack/20231122_report.html

In addition, we released an analysis report titled "Why We Need to Share Information among First Responders on Ransomware Attack," in conjunction with the start of consultation form. This report analyzes the issues in the incident handling of recent ransomware attacks, as well as how the incidents should ideally be handled. The initial response to a ransomware attack calls for faster analysis and decision-making than in other incident handling, and if the initial response is handled poorly, the impact will spread, including delays in the recovery of operations. At JPCERT/CC, we are working to provide case study information by publishing reports and other means, as part of activities to raise awareness about "Guidelines for Handling and Utilizing Attack Technology Information" to promote information sharing among expert organizations, in addition to responding to consultations and providing information for the information sharing activities.

JPCERT/CC Eyes: Why We Need to Share Information among First Responders on Ransomware Attack (Japanese)
https://blogs.jpcert.or.jp/ja/2024/03/ransom_incident_and_infosharing.html

－Topic2－ JSAC2024 Conference for Security Analysts Held

JPCERT/CC held JSAC2024 at the sola city Conference Center from January 25 to 26, 2024. 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 attack incidents.

Last year's conference was held in a hybrid format combining physical and virtual conferences, but this year's conference, marking its seventh, was held only in a physical format. Six presentations were given as part of the conference's Lightning Talk sessions, in addition to 17 presentations including three workshops. Through these sessions, technologies related to incident analysis and handling, including malware analysis and incident response cases, and new technical insights and analysis tools originally developed by the presenters were shared.

The conference drew 389 participants (out of 471 prior registrants), and active discussions were held. Participants have commented that the conference is helping raise the level of security analysts. Going forward, we will consider improvements based on feedback to make the conference meaningful for even more participants.

Some presentation materials of JSAC2024 are available on the JSAC2024 website. An overview of the conference is also provided on JPCERT/CC Eyes.

JSAC2024
https://jsac.jpcert.or.jp/en/index.html

JPCERT/CC Eyes: JSAC2024 -Day 1
https://blogs.jpcert.or.jp/en/2024/03/jsac2024day1.html

JPCERT/CC Eyes: JSAC2024 -Day 2-
https://blogs.jpcert.or.jp/en/2024/04/jsac2024day2.html

JPCERT/CC Eyes: JSAC2024 -Workshop & Lightning talk-
https://blogs.jpcert.or.jp/en/2024/04/jsac2024-workshop-lightning-talk.html

－Topic3－ ICS Security Conference 2024 Held

On February 7, 2024, ICS Security Conference 2024 was held online, attracting 419 participants. Following the opening remarks by Masahiro Uemura, Deputy Director-General for Cybersecurity and Information Technology Management at METI, which co-hosted the event, seven presentations were given, including three that were adopted through a call for presentation.

First, JPCERT/CC gave a review of the year while sharing information about various developments concerning ICS security and its current situation. Then, presentations followed, addressing various topics such as security risks hidden in the computer numerical control of machine tools and their countermeasures, network monitoring methods that can easily be employed at ICS user organizations, issues related to the implementation of security policies for ICS and their countermeasures, the need for incident handling preparations and importance of collaboration among stakeholders, and creation of scenarios for incident response training undertaken by ICS security personnel at 10 manufacturing companies. Notable features of this year's conference included sharing a number of activities that ICS user companies can engage in step by step, and sharing collaborative initiatives undertaken by several ICS user companies in a panel discussion held late in the program.

According to the questionnaire survey conducted after the event (208 valid responses), the participants represented a diverse mix of professionals at rates roughly unchanged from last year: 38.5% ICS users, 8.7% ICS vendors, 11.5% ICS equipment vendors, 7.2% ICS engineering firms and 4.3% researchers. As the conference was held online again this year, participants could join from across the country. Prior registrants reached the quota faster this year than usual, indicating the high level of interest in ICS security events held by JPCERT/CC. Also, 97.6% of the survey respondents said they would like to participate in the event again in the future. Based on the results of this year's conference, we will continue to plan events that contribute to the activities of ICS security personnel.

Presentation materials are available on the JPCERT/CC website. An overview of the conference is reported in a blog article on JPCERT/CC Eyes.

JPCERT/CC Eyes: ICS Security Conference 2024
https://blogs.jpcert.or.jp/en/2024/04/ics-conference2024.html