JPCERT-PR-2019-01
Issued: 2019-01-16

JPCERT/CC Activities Overview [October 1, 2018 – December 31, 2018]

Activity Overview Topics

ー Topic 1ー "2017 Fact-finding Survey Report on the Establishment and Operation of CSIRTs" published

On December 18, JPCERT/CC published the "2017 Fact-finding Survey Report on the Establishment and Operation of CSIRTs," which summarizes the results of a fact-finding survey on the establishment and operation of Computer Security Incident Response Teams (CSIRTs) in Japan, with the cooperation of the Nippon CSIRT Association (NCA).

2017 marked the 10th anniversary of NCA, which has grown from an initial membership of 6 organizations to 322 (as of December 28, 2018), indicating how many domestic organizations have established and are now operating a CSIRT. This trend is driven by the wide range of cyber attacks seen in recent years, including the distribution of ransomware, list-based attacks and targeted attacks. In the Cybersecurity Management Guidelines Ver 2.0, published in November 2017, the Ministry of Economy, Trade and Industry advises businesses to make the establishment of a CSIRT system a management agenda to be addressed as a cyber security measure. This, too, has helped promote moves toward the establishment of CSIRTs.

In the two years since the previous survey, the environment has changed considerably, with more organizations operating a CSIRT and cyber attacks becoming more sophisticated. To gain a clear understanding of domestic CSIRT activities under this new environment, JPCERT/CC has followed up on the 2015 survey with a second questionnaire survey.

As did the previous survey, this report reviews the situation with regard to the establishment and operation of CSIRTs, analyzes the challenges that existing CSIRTs need to tackle to move on to the next step, and based on this analysis presents three tasks for CSIRTs to work on: 1) interaction with CSIRTs of other organizations, 2) enhancement of services for identifying the causes of incidents, and 3) involvement in business continuity and disaster recovery plans as CSIRT. JPCERT/CC hopes that the report will provide useful guidance to organizations seeking to newly establish a CSIRT, as well as to those planning to upgrade organizations already operating a CSIRT to take it to the next stage.

2017 Fact-Finding Survey Report on the Establishment and Operation of CSIRTs [Japanese]
https://www.jpcert.or.jp/research/CSIRT-survey.html
https://www.jpcert.or.jp/research/20181218_CSIRT-survey2017.pdf

ー Topic 2ー　JPCERT Coordination Center official blog "JPCERT/CC Eyes" launched

On October 23, 2018, JPCERT/CC launched its official blog "JPCERT/CC Eyes." This blog will serve as a platform for JPCERT/CC to quickly provide information about trends observed by its Internet threat monitoring system (TSUBAME), the latest on events and conferences held both in Japan and overseas, and of course findings from analysis and investigations conducted by JPCERT/CC.
Please note that past articles of each content were also moved to the new blog.

JPCERT/CC Eyes—JPCERT Coordination Center official blog (English)
https://blogs.jpcert.or.jp/en/
JPCERT/CC Eyes—JPCERT Coordination Center official blog (Japanese)
https://blogs.jpcert.or.jp/ja/

Notice of office relocation

On November 26, 2018, JPCERT/CC moved its office to a new location. The new address, phone and fax number are listed below.
We are taking this move as an opportunity to renew our commitment to meeting the expectations of everyone who relies on our services, and we intend to redouble our efforts to this end. We ask for your continued support in the years to come.

Address:
8F Tozan Building, 4-4-2 Nihonbashi-Honcho, Chuo-ku, Tokyo 103-0023 JAPAN

Phone: +81-3-6271-8901
Fax: +81-3-6271-8908