JPCERT/CC Activities Overview [October 1, 2016 － December 31, 2016]

Activity Overview Topics

－Topic 1－　　**APCERT Annual General Meeting & Conference 2016 Held (October 24-27)**

APCERT is a community formed mainly by CSIRTs that represent each economy of the Asia Pacific region. JPCERT/CC has served as its Secretariat and played leadership roles as a member of the Steering Committee. The Annual General Meeting of APCERT was held in Tokyo from October 24 to 27, with JPCERT/CC playing host. Among the 28 Operational Members representing each economy, 23 teams (including JPCERT/CC) participated. The APCERT Annual General Meeting & Conference has been held every year with the aim of sharing information about recent Internet security trends and incident responses taken in each economy, as well as results of investigations and research. This was the first time the meeting was held in Tokyo since APCERT was founded in 2003. As the host team, JPCERT/CC planned the meeting and led the entire proceedings.

The Open Conference for the general public held on October 27 was participated by about 150 people from approximately 30 countries and regions, who were mostly participants from APCERT member organizations, CSIRTs both in Japan and abroad, and organizations related to cyber security.

Please refer to the following web page for details about the APCERT Annual General Meeting & Conference 2016.

APCERT Annual General Meeting & Conference 2016
https://www.apcert.org/apcert2016/

－Topic 2－　　**JPCERT/CC's new initiative on ICS security**

Cyber threats faced by industrial control systems (ICS) are growing year by year, and as seen in the massive power outage that occurred in Ukraine at the end of 2015, cyber attacks causing serious damage to ICS have been occurring overseas.

Given the increased cyber threats to ICS, JPCERT/CC started a new ICS security assessment service and published the following 2 documents concerning ICS security during this quarter, as part of its efforts to promote ICS security countermeasures.

- Publication of the "Asset Owner Fact-finding Survey on ICS Security" (in Japanese)
- Start of Industrial Control System Self-assessment Tool (J-CLICS) download service and publication of

Using the ICS security assessment service that JPCERT/CC started in December 2016 targeting domestic asset owners, asset owners will be able to gain a comprehensive understanding of the current problem areas in the corporate structure, policies and systems from a third-person point of view. Through the provision of this service, JPCERT/CC will also gain an understanding of the actual state of ICS security among asset owners, and use improvement measures that become evident as a result to promote the widespread adoption and awareness of ICS security.

During this quarter, JPCERT/CC conducted advance assessments and coordination targeting 3 organizations and gave prior explanations, in preparation for the start of service in the next quarter.

JPCERT/CC also published the "2015 Asset Owner Fact-finding Survey on ICS Security," which summarized the results of a questionnaire survey conducted for the purpose of understanding how Japanese asset owners view security and the security measures they implement.

This survey report summarizes the responses of 318 organizations that own ICS assets to 12 questions concerning ICS network configurations and security measures undertaken to safeguard those facilities.

JPCERT/CC also started a download service to make the Industrial Control System Self-assessment Tool (J-CLICS), which used to be provided individually to domestic companies and organizations that applied, more widely available.

An English version of the J-CLICS is now offered as well for use at overseas offices of Japanese companies and so forth.

Industrial Control System Self-assessment Tool (J-CLICS)
https://www.jpcert.or.jp/english/cs/jclics.html

－Topic 3－　　**JPCERT/CC staff member joins the CVE Board**

Today, a code called CVE numbers is assigned when publishing vulnerability information of software, etc. in order to help identify vulnerabilities. JPCERT/CC started assigning CVE numbers[*1] to vulnerabilities announced through the Information Security Early Warning Partnership in May 2008. In 2010, JPCERT/CC was designated as a CVE Numbering Authority (CNA), which refers to an organization that has the authority to assign CVE numbers on its own. JPCERT/CC has thus been working closely with the Common Vulnerability and Exposures (CVE) project managed and maintained by MITRE of the US.

The CVE project has a meeting body called the CVE Board, which makes decisions about management policies, etc. and discusses how to run its global operation of assigning CVE numbers quickly, steadily and without causing confusion. Recently, Takayuki Uchiyama, an information security analyst who belongs to the Vulnerability Coordination Group, was nominated and then elected to the CVE Board following a vote by its members.

On being elected to the CVE Board, Uchiyama says, "I look forward to bringing to the table the knowledge I acquired through the vulnerability information distribution activities of Japan's Information Security Early Warning Partnership, as well as similar efforts in the Asia Pacific region, and thereby help strengthen the CVE system and make the global distribution of vulnerability information even more effective."

New CVE Board Member from JPCERT/CC
https://cve.mitre.org/data/board/archives/2016-12/msg00006.html

JPCERT/CC celebrates its 20th anniversary

October 1, 2016 marked the 20th anniversary of the start of JPCERT/CC's activities. We would like to take this opportunity to thank all those around the world who have supported us along the way in our efforts to reduce incident damage. We remain committed to technology and relationships of trust between individuals as we continue our work.
We look forward to your continued guidance and support.