JPCERT-PR-2016-02
Issued: 2016-07-14

JPCERT/CC Activities Overview [April1, 2016 – June30, 2016]

Activity Overview Topics

－Topic 1－　JPCERT/CC staff member reelected to the FIRST Board of Directors

Ever since JPCERT/CC joined the Forum of Incident Response and Security Teams (FIRST), an international group of CSIRTs, in 1998, it has played an active part in the group's activities. As part of this effort, a number of JPCERT/CC staff members have contributed to the group's operations as members of its Board of Directors. Koichiro Komiyama, Manager of the Global Coordination Division and a member of the FIRST Board of Directors since June 2014, was reelected for a second term of office in the election held at the Annual General Meeting on June 16. He will be serving in this capacity for another 2 years. Komiyama's reelection can be taken as an indication that his contributions as seen in his performance as a director in charge of conferences and his work supporting the establishment of CSIRTs in Africa and Asia have been highly regarded by the members.

Activities to support the establishment of CSIRTs in Africa, which JPCERT/CC launched in 2009 as part of its international contribution, have earned broad recognition among members in the African region as well as the international CSIRT community. With regard to these activities, Suguru Yamaguchi, a former member of the JPCERT/CC Board, Komiyama, and JPCERT/CC as a whole have been awarded the AfricaCERT Meritorious Service Award in June.

Komiyama commented on his reelection to the FIRST Board of Directors and receipt of the AfricaCERT Meritorious Service Award: "I am grateful for the opportunity to be able to continue working for the international organization FIRST and the CSIRT community to further enhance the impact of their activities. To this end, I will work to spread the network throughout Africa and other regions."

FIRST.Org, Inc., Board of Directors
https://www.first.org/about/organization/directors

AfricaCERT Meritorious Service Award presented to JPCERT/CC, Suguru Yamaguchi, and Koichiro Komiyama, Senior Analyst of the Global Coordination Division
https://www.jpcert.or.jp/english/pub/2016/PR20160617_africacert-award.html

－Topic 2－ 2015 Fact-Finding Survey Report on the Establishment and Operation of CSIRTs published

During the last fiscal year, JPCERT/CC conducted a questionnaire survey and interviews of Nippon CSIRT Association (NCA) members to investigate the organizational structures, membership structures, and status of policy establishment of CSIRTs. The findings have been put together into a report that will serve as a valuable reference for those looking to establish a CSIRT and published in June.

As organizations are faced with the need to prepare for the growing problem of cyber attacks, CSIRTs are gathering attention as an organizational structure that will play a key role in responding effectively to security incidents. However, CSIRTs come in various forms depending on such factors as the culture of the parent organization and the technical backgrounds of the appointed members. This report introduces relevant facts concerning various CSIRTs in Japan with the hope that it will provide useful guidance to organizations seeking to newly establish a CSIRT as well as to those already operating a CSIRT and considering to take it to the next level. We hope that the report will be widely used as a reference material to help establish CSIRTs and improve their activities.

－Topic 3－ JPCERT/CC publishes a document for investigating traces of activities left behind by attackers

JPCERT/CC investigated tools and commands that attackers will likely to use once they infiltrate a network and conducted tests to verify the traces that remain on a Windows operating system when those tools and commands are executed. The findings have been put together into a report titled “A Report on an Investigation into Traces of Attack Tool Execution for Incident Investigations” and published on June 28, 2016.

In cyber attacks of recent years, machines infected with malware are often used as a springboard for infecting other machines and infiltrating internal servers. These cases confirm that nowhere in the network of an organization is safe from possible infiltration. In the event of such incidents, investigations must cover numerous areas and be conducted rapidly without overlooking crucial events. Organizations require the means to ascertain the full extent of the damage as accurately as possible, and to collect facts needed to formulate a remedy.

While the configuration of networks that become the target of attacks varies considerably from organization to organization, a certain pattern exists in the methods used by the attackers, who often use the same tools.

JPCERT/CC conducted an investigation based on its experience to find out what kinds of logs are generated when common attack tools are executed, and what settings will ensure the logs will contain sufficient information, and summarized the findings in a report. The report offers material that will be useful for experts and non-experts alike in incident investigations.

－Topic 4－ OWASP web application security requirements translated and published in Japanese

As part of its activities to prevent vulnerabilities in advance, JPCERT/CC has published guides for the development of secure products, coding protocols, and materials describing cases of vulnerabilities. During this quarter, JPCERT/CC published a Japanese translation of the OWASP Application Security Verification Standard (ASVS) Version 3.0, a set of web application security requirements established by the Open Web Application Security Project (OWASP).

OWASP ASVS is a document that standardizes verification requirements concerning web application securities. OWASP started working on its formulation in 2008 and has subsequently released several versions. The document has been widely used by web application developers, security venders that diagnose vulnerabilities, and others both inside and outside Japan.

In Version 3.0, security requirements for secure web applications are laid out under 19 categories, including authentication, session management, and access control, and it comes with an annex containing a comparative list of PCI-DSS v3.0 and ASVS 3.0.

Most of the vulnerabilities that JPCERT/CC coordinated with developers were related to web applications and the web interface of embedded equipment with Internet connectivity, and in this quarter as well, vulnerabilities related to web applications accounted for more than half of the vulnerabilities announced on Japan Vulnerability Notes. We hope that the publication of the Japanese version of ASVS v3.0.1 will allow more people in the web application community to utilize ASVS and lead to the reduction of vulnerabilities.

－Topic 5－ Letter of thanks presented to persons who made significant contributions to cyber security activities

With the aim of minimizing damage caused by cyber security incidents (herein, "incidents") taking place in Japan , JPCERT/CC undertakes support activities to help respond to incidents, early warning activities to help prevent incidents, malware analysis, coordination activities related to vulnerabilities in software products, and other relevant activities. To ensure these activities are promoted smoothly and effectively, information and various assistance provided by individuals are necessary.

At JPCERT/CC, we have established a system for presenting letters of thanks as a sign of our deep appreciation to those individuals who have made particularly significant contributions with respect to cyber security activities. On June 30, 2016, we presented a letter of thanks and a commemorative shield to Takuya Kashiwamura of Toshiba I.S. Corporation, who provided various information that helps gain a broad perspective on attacks and understand how patterns of attacks change in relation to web defacements, etc., that redirect victims to ransomware and banking trojans that have recently been doing considerable damage in Japan as well.