電子署名者 : Japan Computer Emergency Response Team Coordination Center
DN : c=JP, st=Tokyo, l=Chiyoda-ku, email=office@jpcert.or.jp, o=Japan Computer Emergency Response Team Coordination Center, cn=Japan Computer Emergency Response Team Coordination Center
日付 : 2015.06.30 10:24:23 +09'00'

JPCERT-PR-2015-02
Issued: 2015-04-16

JPCERT/CC Activities Overview [January 1, 2015 – March 31, 2015]

Activity Overview Topics

－Topic 1－ Partnership forged with NISC on international collaborative activities and information sharing

On February 10, JPCERT/CC entered into a partnership with the National center of Incident readiness and Strategy for Cybersecurity (herein, "NISC") with the aim of contributing to the effective promotion of cybersecurity measures in Japan. This partnership mainly concerns international collaborative activities and information sharing.

JPCERT/CC will work to enhance its framework for cooperation with NISC so that it can fulfill the aim of the partnership as a "relevant organization that communicates and coordinates with related parties in and outside the country in the event of a cybersecurity-related event" stipulated in Paragraph 1, Article 31 of the Cybersecurity Basic Act (Act No. 104 of 2014), and as a "relevant organization for emergency response concerning cybersecurity" stated in 3(2)iv. of the "Guidelines for Enhancing the Framework for Promoting Cybersecurity in Japan" (finalized on November 25, 2014).
Requests for coordination of incident response and related information submitted to JPCERT/CC, as well as notifications and other communications provided by JPCERT/CC, will continue to be handled in the same manner as before, and will not be affected by the partnership.

(Press Release)
JPCERT/CC Partners with NISC on International Collaborative Activities and Information Sharing
https://www.jpcert.or.jp/pr/2015/pr150001.html (Japanese Only)

*Please refer to the following URLs for policies on the handling of information provided to JPCERT/CC.

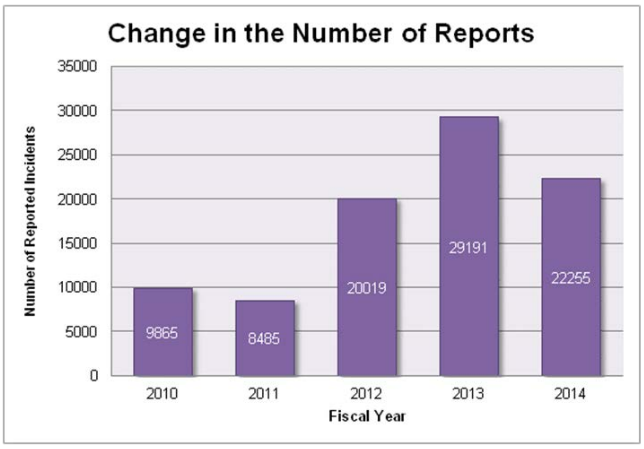
- Incident report: https://www.jpcert.or.jp/english/ir/form.html
- ICS incident report: https://www.jpcert.or.jp/english/cs/controlsystemsecurity.html
- Vulnerability Handling Guidelines: https://www.jpcert.or.jp/english/vh/guidelines.html
- Privacy policy: https://www.jpcert.or.jp/english/privacy.html

－Topic 2－ Number of incident reports in FY2014 fell 24% year-on-year, while the number of cases coordinated rose 10% to 9,684

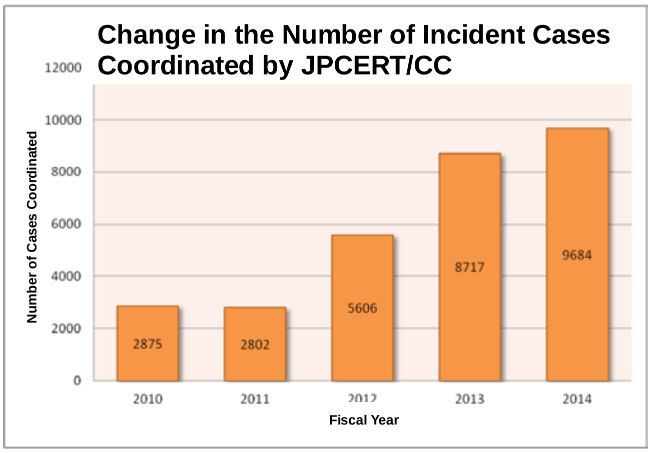
The number of incidents reported during this quarter was 6,869, and the number of cases coordinated(*) was 3,088. When compared with the previous quarter, the number of reports and the number of cases coordinated both increased by 10% and 32%, respectively. Year-on-year, the total number of reports increased by 40%, and the number of cases coordinated increased by 55%.
Of the incidents reported during this quarter, those categorized as incidents that search for vulnerabilities in systems accounted for 54.3%, and those categorized as website defacement made up 14.4%.

As for incidents that search for vulnerabilities in systems, a large number of the DNS communication sources has been confirmed to be hosts in Japan that have become open resolvers. Because open resolvers can be used to carry out DDoS attacks, JPCERT/CC has been contacting organizations and users managing such hosts to request that they review the settings of servers, routers, and other relevant devices.

While the number of incidents reported during FY2014 (from April 2014 to March 2015) fell by 24% from 29,191 in the previous fiscal year to 22,255, the number of cases coordinated rose by 10% from 8,718 to 9,684. These changes are presumably due to the decrease in the number of reports concerning website defacements that occur in large numbers, and the increase in the number of cases requiring multiple coordination activities per incident report.



[Figure 1: Number of incident reports (by fiscal year)]



[Figure 2: Number of cases of incidents coordinated (by fiscal year)]

*"Number of cases coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by asking the site administrator or its relevant parties to conduct an investigation and address any issues.

JPCERT/CC Incident Handling Report [January 1, 2015 – March 31, 2015]
https://www.jpcert.or.jp/english/doc/IR_Report2014Q4_en.pdf

－Topic 3－ Educational activities on ICS security — ICS Security Conference 2015 and 4 security seminars held

On February 12, ICS Security Conference 2015 was held in Tokyo, attracting 264 participants. The 7th Conference held this year featured lectures on activities undertaken for ICS security along the theme of "understanding present conditions, and preparing for the future," as well as other programs designed to promote information exchange that will lead to future activities to improve security.

In addition, ICS security seminars were held in Okayama, Fukuoka, Nagoya and Tokyo between December 2014 and February 2015. In these seminars, JPCERT/CC discussed points that need to be considered in future ICS security measures, using the results of research and investigation conducted by JPCERT/CC on how we should proceed with the much-needed security measures in an ICS environment.

ICS Security Conference 2015
https://www.jpcert.or.jp/event/ics-conference2015.html (Japanese Only)

－Topic 4－ APCERT conducts 11th joint cyber exercise

On March 18, Asia Pacific Computer Emergency Response Team (APCERT) carried out a joint cyber exercise to test the ability to respond immediately to cyber attacks. These annual exercises are conducted with the aim of strengthening collaboration between CSIRTs in each economy in responding to incidents that occur in the Asia Pacific region and have a broad impact across national borders.

The theme of the 11th joint cyber exercise was "Cyber Attack beyond Traditional Sources" In addition to APCERT member teams, Egypt, Tunisia and Morocco also participated from the Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT), resulting in a total of 28 teams participating from 22 economies.

JPCERT/CC participated in these exercises both as a player (participant) and as a coordinator of the exercise called ExCon to facilitate its smooth execution.

(APCERT MEDIA RELEASE)
APCERT EMBARKS ON CYBER ATTACKS BEYOND TRADITIONAL SOURCES
http://www.apcert.org/documents/pdf/APCERTDrill2015PressRelease_Final.pdf