

## **JPCERT/CC Activities Overview**

**July 1, 2020 ~ September 30, 2020**



**JPCERT Coordination Center  
October 15, 2020**

## Activity Overview Topics

### **—Topic 1— Security alert issued based on a summary of security trends under current work style changes**

Since April 2020, the way people work has been changing, with more people working from home due to the impact of COVID-19. As companies adopt irregular attendance systems and reduce office work, the situation continues to present challenges in responding to incidents and vulnerabilities. Under these circumstances, JPCERT/CC has identified many serious vulnerabilities in some systems and products enabling remote connection since June 2020. In addition, the Emotet malware has resumed its campaigns in July 2020, and JPCERT/CC has identified e-mails causing infection.

In light of these circumstances, JPCERT/CC released CyberNewsFlash “Looking Back on April to August 2020” (Japanese) on August 24. This blog article summarizes information about serious vulnerabilities and attacks with a wide range of impact, and calls on organizations to review the settings and update status of their servers and other network equipment and discuss measures to prevent Emotet infection. Moreover, JPCERT/CC has individually notified organizations and administrators that were found to be using products and versions affected by vulnerabilities.

It is anticipated that organizations will continue to be required to address security issues under irregular work environments, and JPCERT/CC will continue to provide information and undertake activities that will help prevent damage.

### **—Topic 2— JPCERT/CC 2020 letter of thanks presented to members of 5 organizations for contributions in vulnerability handling and incident reports**

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

Mitsuaki Akiyama of NTT Secure Platform Laboratories, one of the persons who received a letter of thanks this year, contributed in new coordination activities that involve more stakeholders, in addition to conventional one-to-one coordination between JPCERT/CC and the relevant vendor, by offering great

cooperation in ensuring smooth coordination with stakeholders and preparing advisories in coordination activities related to vulnerabilities in software products and so on.

Takeshi Imai of the Kyushu Branch of Internet Initiative Japan Inc., Takashi Ishihara of RIKEN, Japan, Yusuke Osumi of Yahoo Japan Corporation, and ITCCERT of IT Planning Division, ITOCHU Corporation contributed by submitting numerous reports that helped with malware analysis and in reducing damage caused by domestic cyber attacks.