JPCERT/CC Activities Overview

October 1, 2019 - December 31, 2019

JPCERT Coordination Center

January 21, 2020

Activity Overview Topics

－ Topic 1－ Activities concerning Emotet malware infections

JPCERT/CC received numerous inquiries regarding Emotet malware infections from late October 2019. Many of the inquiries concerned infections caused by a malicious Word document attached to a spoofed e-mail made to look like it was sent by an existing organization or person. Emotet steals e-mail content and contact information from the computer it infects. The stolen information could then be exploited to create a malicious e-mail and send it to a business partner and so on impersonating the infected party. If an infected computer is inside an organization, it could be used to send a large amount of e-mails that spread infection outside the organization. According to published information of related damage, Emotet also downloads other malware, causes Trickbot infection to steal financial information, and leads to infection with ransomware that encrypts the data stored on the computer.

While responding to individual inquiries, JPCERT/CC also issued a security alert and CyberNewsFlash on November 27, 2019 to alert the public and prevent the further spread of damage due to Emotet infections. Since JPCERT/CC still continued to receive numerous inquiries, on December 2, 2019 it posted a blog article on JPCERT/CC Eyes compiling FAQs that can be used by individuals and organizations with suspected Emotet infections.

■Security alert
Alert Regarding Emotet Malware Infection
https://www.jpcert.or.jp/english/at/2019/at190044.html

■CyberNewsFlash
Information about Emotet malware infection activities (Japanese)
https://www.jpcert.or.jp/newsflash/2019112701.html

■JPCERT/CC Eyes
How to Respond to Emotet Infection (FAQ)
https://blogs.jpcert.or.jp/en/2019/12/emotetfaq.html

－ Topic 2－ Japanese translation of "PSIRT Services Framework Version 1.0" released

Product Security Incident Response/Readiness Team (PSIRT) is gaining attention as a function that plays a leading role within an organization in the event that a security issue is identified in a product it provides, ensuring that countermeasures are implemented smoothly within the organization. However,

there was hardly any published materials available in Japan providing knowledge about how to establish and operate a PSIRT.

In the interest of providing useful information, JPCERT/CC worked with Software ISAC (Computer Software Association of Japan) to produce a Japanese translation of "PSIRT Services Framework v1.0," a document created by FIRST to provide guidelines for the establishment and operation of a PSIRT, and released it on FIRST's website.

> Japanese translation of the PSIRT Services Framework Version 1.0
> https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.0_jp.pdf

This document lists the services and functions that a PSIRT needs to provide, while also explaining their purposes and the benefits they offer. The document will help solve any difficulties encountered when establishing or operating a PSIRT.