Internet Topics: Nippon CSIRT Association

■ The Nippon CSIRT Association and its Activities

The Nippon CSIRT Association*[1] was established in March 2007 with the goal of improving the incident response capability of members through collaboration and the exchange of information between Computer Security Incident Response Teams (CSIRTs) in Japan. There were six members when the association was first established, but at the time of writing this number has grown to 19*[2].

Although there are a variety of definitions for CSIRT*[3], here it is regarded as a team that has organizations and groups it serves (constituency) that conducts activities aimed at improving the security of its constituents through resolving the security incidents they face, detecting incidents at an early stage, and providing warning information via analysis results, etc. It also serves as a point of contact for cooperation with external organizations in the course of carrying out these activities. The current Nippon CSIRT Association is made up of a wide variety of members, from information security vendors to IT-related businesses and ISPs such as IIJ.

The working groups implemented by groups of members serve as the action units of the association. A broad range of activities are carried out, such as the sharing of live incident information, surveys on countermeasure technologies, evaluation of information exchange methods, clarifying issues relating to CSIRTs, and collaboration with external organizations. For example, the sharing of actual incident information involves not only exchanging this information with members, but also releasing general warnings summarizing the information that was obtained*[4].

■ International Collaboration Workshop

The Nippon CSIRT Association collaborates with other related organizations both domestic and international as part of its external collaboration activities. For example, in collaboration with the international forum of CSIRTs FIRST*[5], a workshop*[6] was held in Japan, and last year a symposium on international collaboration*[7] was held independently. Anti-malware and botnet specialists from the Shadowserver Foundation*[8] and Honeynet Project*[9] were invited to this workshop to give presentations regarding observation data gathered on the front line as well as response methods, and this provided an opportunity for a lively exchange of opinions. A closed environment was also built at the event site to simulate the construction of environments for actually capturing malware and to let attendees experience control of a botnet, providing insight not normally available (Figure 1).

■ Regarding Admission into the Nippon CSIRT Association

In this section we have shed some light on the activities of the Nippon CSIRT Association. Currently most of the teams participating in this organization are IT specialists, but soliciting the broader participation of other teams who work toward the same goals could provide a synergistic effect, bringing together a wealth of knowledge about incidents that occur and contributing to their prompt settlement. Groups such as the information systems department of a general corporation could be considered a type of CSIRT, and we would encourage all those interested in the activities presented here to consider admission*[10].

CSIRT
日本シーサート協議会

Author:
Mamoru Saito
Manager of the Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division.

Figure 1: The International Collaboration Workshop Instructors David Watson of the Honeynet Project (left), and Richard Perlotto of the Shadowserver Foundation (right).

[1] Nippon CSIRT Association (http://www.nca.gr.jp/) (in Japanese).

[2] Nippon CSIRT Association member list (http://www.nca.gr.jp/member/index.html) (in Japanese). IIJ's CSIRT IIJ-SECT has been a member since the establishment of the association.

[3] See the "CSIRT FAQ" from U.S. CERT/CC (http://www.cert.org/csirts/csirt_faq.html) or "What is CSIRT" from EU ENISA (http:// www.enisa.europa.eu/act/cert/support/guide2/introduction/what-is-csirt), for example. CSIRT activities at ISPs such as IIJ are also discussed in RFC3013 (BCP46) (http://www.ietf.org/rfc/rfc3013.txt).

[4] For example, Gumblar countermeasures (http://www.nca.gr.jp/2010/netanzen/index.html), PushDo (http://www.nca.gr.jp/2010/pushdo-ssl-ddos/index.html), and Stuxnet (http://www.nca.gr.jp/2010/stuxnet/index.html) (in Japanese).

[5] See Vol.3 of this report under "Internet Topics: The 21st Annual First Conference" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol03_EN.pdf) for more information about FIRST.

[6] Joint Workshop of Security 2008, Tokyo (http://www.nca.gr.jp/jws2008/index.html) (in Japanese).

[7] See the participation report for the NCA 2010 event International Collaboration Workshop (http://www.nca.gr.jp/2010/event/index.html) (in Japanese) for more information.

[8] The Shadowserver Foundation (http://www.shadowserver.org/wiki/).

[9] The Honeynet Project (https://www.honeynet.org/).

[10] See the Nippon CSIRT Association participation guide (http://www.nca.gr.jp/admission/index.html) (in Japanese) for more information about admission qualifications and procedures. A recommendation from an existing member organization is required for admission. IIJ also provides these recommendations.