

Introduction of Nippon CSIRT Association

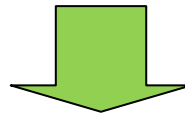
March 25, 2008

Toshio Nawa

Nippon CSIRT Association

Social Situation in Japan

- The Single CSIRT would NOT be able to handle the differing needs and to provide rapid response to computer security incident.
 - Taking advantage of Japanese business culture, norms and business practices.
 - Targeted attacks on specific companies, which is difficult to accumulate know-how on methods of responding and handling.
- Need effective mechanisms to collaborate and share information
 - There are impediments to make it come true.
- So far, each CSIRT has made steady efforts to collaborate and share information such as FIRST community.



Need to boost the mechanism of collaborating within CSIRT community

Overview



■ Official name

- Japanese name: 日本コンピュータセキュリティインシデント対応チーム協議会
- a.k.a.: 日本シーサート協議会
- a.k.a. in English: NIPPON CSIRT ASSOCIATION (NCA)
- <http://www.nca.gr.jp/>

■ Mission

- Establish collaborative environment for member CSIRTs to work on common security concerns and issues
- Member driven initiative to contribute to better secured information society

■ History

- March 27th, 2007 Founded by 6 CSIRTs (five of which are from commercial enterprises)
- July 31st, 2007 Established operational framework
- August 1st, 2007 Steering committee formed

Steering Committee

- Chair Mr. Yoshiki Sugiura @ NTT-CERT (NTT)
 - <https://www.ntt-cert.org/>
- Vice chair Dr. Masato Terada @ HIRT (Hitachi)
 - <http://www.hitachi.co.jp/hirt/>
- Mr. Mamoru Saito @ IIJ-SECT (IIJ)
 - <http://www.ij.ad.jp/development/report/security/work.html>
- Mr. Yozo Toda @ JPCERT/CC
 - <http://www.jpCERT.or.jp/>
- Mr. Hiroki Iwai @ JSOC (LAC)
 - <http://www.lac.co.jp/security/>
- Mr. Kazuyoshi Sasaki @ SBB-SIRT (Softbank BB)
 - <http://bb.softbankbb.co.jp/>
- Secretariat: JPCERT/CC

Objectives

- Develop a framework and best practices to jointly and collaboratively respond to security incidents by member CSIRTs
- Support prospective members create CSIRTs
- Support member CSIRTs improve their capabilities
- Develop best practices to share security information among member CSIRTs, considering existing (business) challenges (such as NDAs and regulations)
- Publish best practices to public

Several working groups have been kicked off to work on these issues.

Summary of Activities

- CSIRT building support for organizations
- Providing various environments for CSIRT activities
 - To boost exchange between CSIRTs
 - To study how the CSIRT should function and facilitate interaction in Japan
- Handling and supporting the activities of intra-industry incident response.
 - Sharing the each case and know-how
 - Discussion the methods of sharing information

Working group drive forward above activities, which each CSIRT would get interested or would like to focus on.

Working Groups

■ CSIRT Renaissance working group

- Brainstorm to revisit the major issues to start and manage CSIRTs
 - Occasionally having prospective members who are planning to create their CSIRTs
- Develop CSIRT materials for operations

■ Early warning working group

- Develop framework and rules for early warning among member CSIRTs
 - 5W1H (Who, What, Whom, When, Why, and How)

■ CSIRT fact sheets file working group

- Collect fact sheets from member CSIRTs
 - Mission, background, position, authority, resources, etc.
- Keep them organized and updated as reference for member CSIRTs as well as for marketing communications

Nippon CSIRT Association



To promote CSIRTs' activities



<http://www.nca.gr.jp/>