Introduction of Nippon CSIRT Association

January 29, 2008

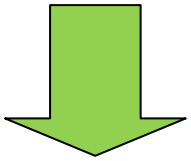
Yoshiki SUGIURA

Steering committee chair

Nippon CSIRT Association

社会的な状況

- コンピュータセキュリティインシデントへの迅速な対応が、単独の シーサート では困難になってきている
  - 日本国内の企業事情を巧みに利用
  - 対応ノウハウの蓄積困難な、特定の組織を狙った標的型攻撃
- 連携が必要だが、阻害する要因も多数
- その問題を超えて、FIRST コミュニティなど、個別のシーサート同士の地道な連携が行われてきた。



連携を活性化し、
地道な活動を発展させる必要性。

Overview

- Official 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
  - aka:日本シーサート協議会
  - aka 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.iij.ad.jp/development/report/security/work.html
- Mr. Yozo Toda @ JPCERT/CC
  - http://www.jpcert.org.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

CSIRT 日本シーサート協議会

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.

活動概要

- 一般企業及び組織への シーサート 構築支援活動
- さまざまな場の提供
  - 異なる シーサート 間の交流の場
  - シーサート 間の連携のあり方に関する検討の場
- 企業内セキュリティインシデントへの対応、支援
  - 事例情報提供、対策情報提供、共有方法検討等

ワーキンググループにより、それぞれの シーサート が興味を持つ、或いは注力したい分野に特化した活動を推進する。

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

具体的な活動(WGを中心として)

- 組織内シーサート課題検討
  - シーサート協議会のメンバー、及び組織内シーサートの構築や運用を考えている方々とのディスカッションを通じ、組織内シーサートの構築や運用に必要な課題 を抽出する。その上で、それらの課題に対応した、各シーサートの活動の一助ともなる、シーサート構築及び運用に必要なマテリアル等の作成を目指す。
- 早期警戒情報共有
  - 緊密かつ信頼関係のあるシーサート間においてコンピュータセキュリティインシデントに関する脅威情報を共有する。
- CSIRT FACT Sheet FILE
  - 日本国内の各シーサートの活動の背景情報(目的、組織内での位置、権限、人員、予算など)を整理して共有することで、既存のチームの改善や、新しいシーサート構築の支援に役立つ資料の作成を目指す。
- インシデント事例共有
  - 各チームで取り扱っているインシデント事例を共有する。異なる組織間でのインシデント情報共有のための問題抽出と、課題解決する。優れた対策などは一般に向けても公開を検討する。

Nippon CSIRT Association

To promote CSIRTs' activities

CSIRT
日本シーサート協議会

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