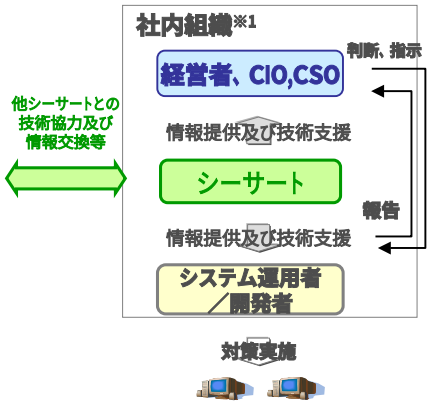
# 日本シーサート協議会の活動の状況について

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
運営委員長　杉浦芳樹
2007年11月22日



## シーサート(CSIRT)とは

●インターネットにおけるセキュリティ脅威の増大に対応すべく、**脆弱性の発見、インシデント等に応じたセキュリティ維持を適切に実施・管理**する“セキュリティ運用”が、近年重要となっている。
●専門家による組織的な活動を行う部隊であるシーサートは各組織に配置される。

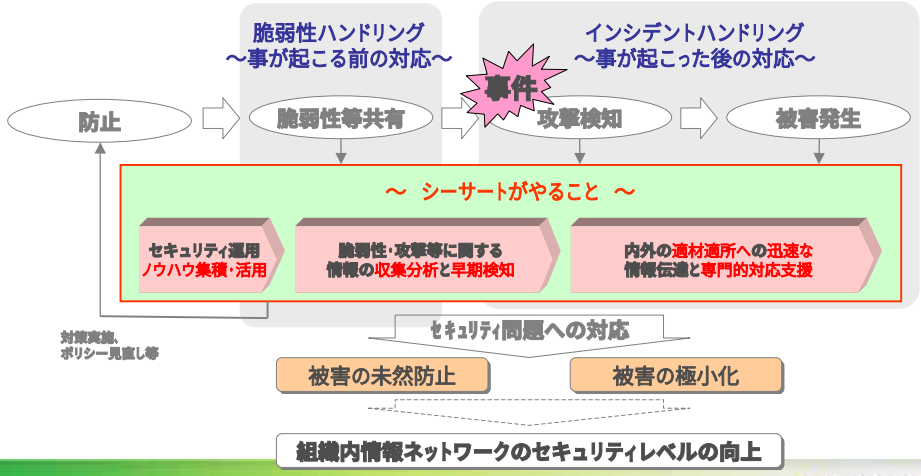



※1. 内部統制および、提供サービスに関わるセキュリティ運用体制

| 機能 | 主な役割 |
|---|---|
| セキュリティ管理者 | 対応の判断・指示、対策実施の管理 |
| シーサート | 対応の調整、技術支援、情報収集・分析・提供 |
| システム運用者／開発者 | 対策実施（パッチ適用、バージョンアップ、設定変更等） |

# シーサート(CSIRT)とは

◆シーサートは、組織内のインシデント・脆弱性について、セキュリティ管理者、システム運用者、外部のシーサート等と連携して、調整技術支援するチーム。







# シーサート(CSIRT)とは

情報セキュリティインフラを強固に構築したとしても、侵入や事故などの発生が起こらないという保証はない。また、インシデントが発生した場合、確認、解析、対応が早ければ、ダメージを最小限に抑えることができる。このような対応をするためには、組織だって動くチームが必要となる。そのようなチームがシーサートである。

- チームもしくは機能で対応
- ノウハウの蓄積および管理
- シーサート同士での情報交換・連携
- シーサートが必要な背景
  - インシデントの増加
  - インシデントの複雑化
  - 脆弱性情報の管理の必要性
  - CSIRT自体もコストがかかるが、長い目で見た場合は全体的なコストダウンに

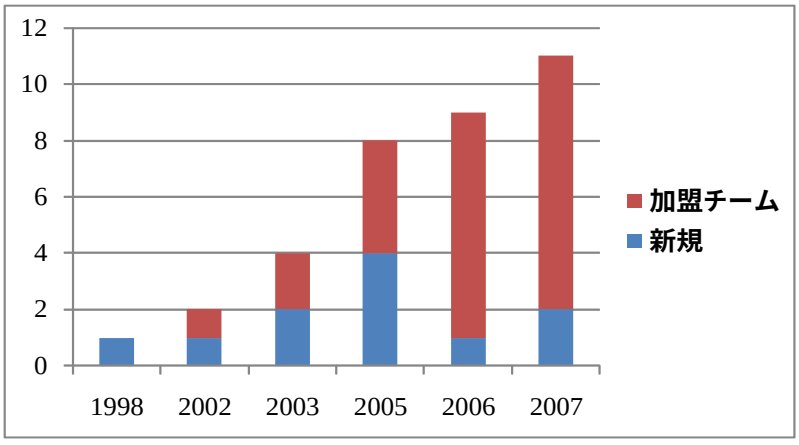
## シーサートの歴史（FIRST を中心として）

- 1988年 ワーム事件
- そのすぐ後にCERT/CCとCIAC設立
- 1989年 Wank Worm事件
- 1990年 FIRST設立
- 1996年 JPCERT/CC設立
- 1998年 JPCERT/CC FIRST加盟(日本初)
- 2007年 現在 FIRST 加盟チーム約190

FIRST: Forum of Incident Response and Security Teams
世界中のシーサートとセキュリティチームが参加する団体
参加チームの地域、業種などは様々




## 日本のシーサートの現状 (FIRST加盟状況から)




FIRST: Forum of Incident Response and Security Teams
世界中のシーサートとセキュリティチームが参加する団体
参加チームの地域、業種などは様々

## 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。**




## 日本シーサート協議会 組織概要

- 設立
  - 2007年3月
- 名称
  - 正式名称:
    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
  - 略称:日本シーサート協議会
  - 英語名:NIPPON CSIRT ASSOCIATION
  - ウェブ: http://www.nca.gr.jp/
- 使命
  - 本協議会の全会員による緊密な連携体制等の実現を追及することにより、会員間に共通する課題の解決を目指す
  - 社会全体のセキュリティ向上に必要な仕組みづくりの促進を図る

## 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

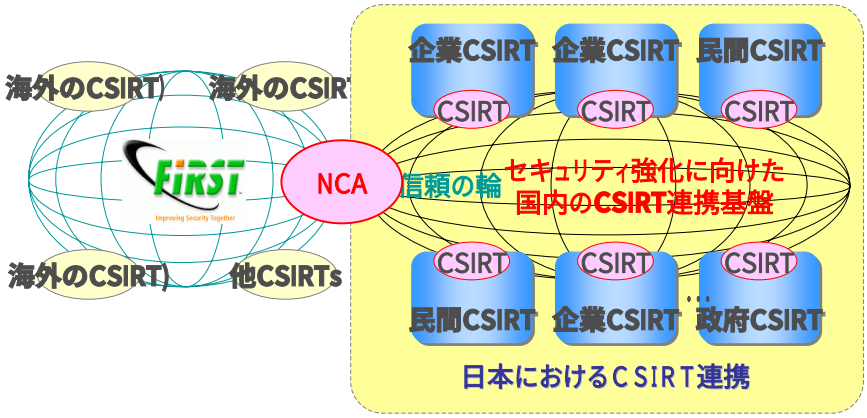
**ワーキンググループにより、それぞれの シーサート が興味を持つ、或いは注力したい分野に特化した活動を推進する。**




## 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。

# 日本シーサート協議会




FIRSTの連携だけでなく国内も




# 会員募集開始

- 日本国内で活動するシーサートであること
- 本協議会の使命及び活動内容に賛同していること
- 本協議会から得た情報を適切に取り扱うことができること

入会に関する情報は以下をご参照ください。
ウェブ: http://www.nca.gr.jp/admission/index.html
問合せ先:
日本シーサート協議会事務局
Email: nca-sec@jpcert.or.jp
電話: 03-3518-4600
（日本シーサート協議会事務局担当を呼び出してください）

# 最後に

シーサート同士の積極的なコミュニケーションを図ることによって、ともに、よりよいセキュリティ対応を考え、そして、実現していきましょう！

CSIRT
日本シーサート協議会
http://www.nca.gr.jp/