JPCERT CC Japan Computer Emergency Response Term Coordination Center

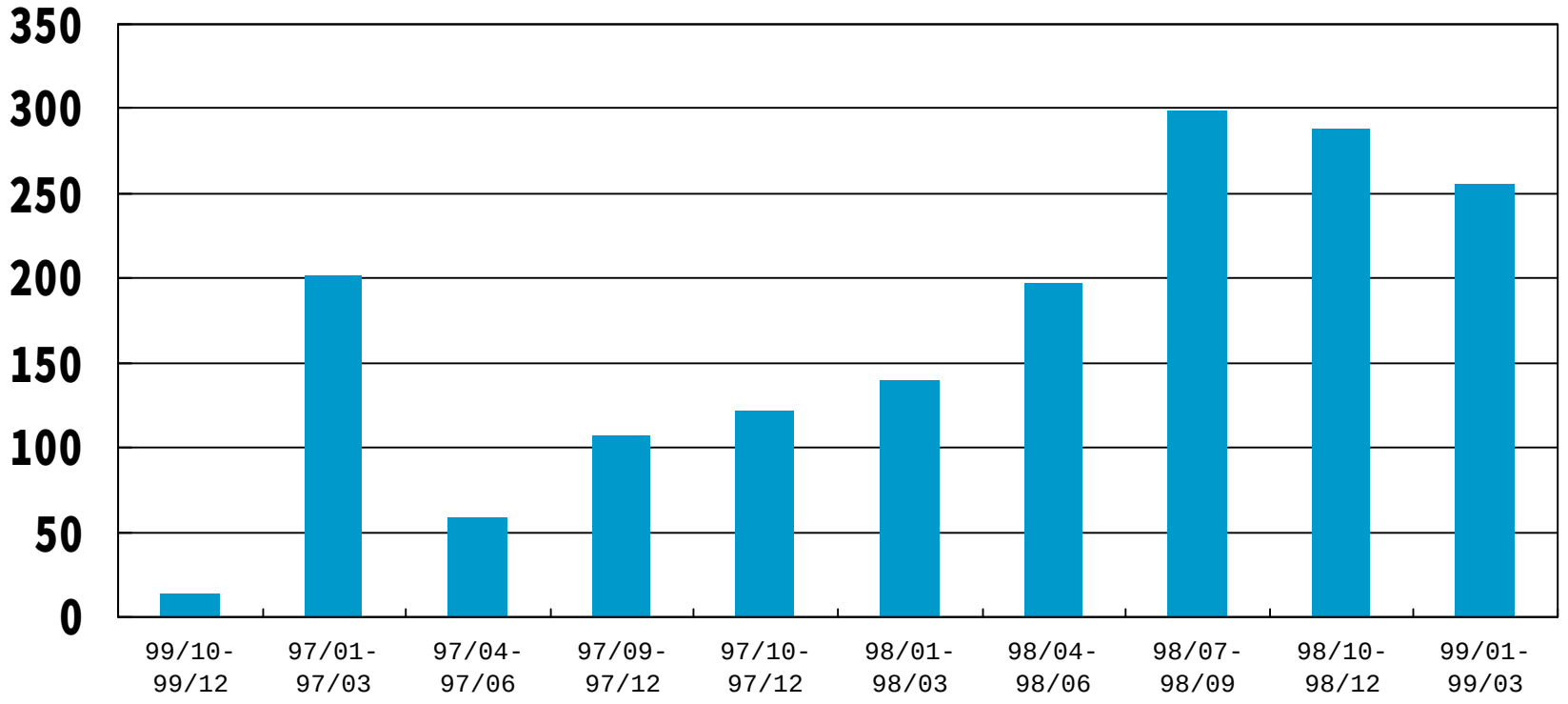
不正アクセス対策からみたネットワークオペレータとJPCERT/CCの役割（3）

JPCERT/CC
(コンピュータ緊急対応センター)

不正アクセスの動向 [1999/1～1999/3]

- システムに存在するサービス/弱点の探査 (プローブ、スキャン)
- 電子メールの不正な中継、電子メール爆撃等
- システムへの不正侵入および管理者権限詐取
- Web サーバの cgi-bin プログラムを悪用した攻撃
- IMAP サーバプログラムを悪用した攻撃
- ネットワークやホストの運用を妨害しようとする攻撃
- パケット盗聴プログラムによる攻撃
- ***automountd を悪用した攻撃*** （PCERT-E-INF-99-0002）
- ***mountd サーバを悪用した攻撃*** （PCERT-E-INF-99-0002）
- POP サーバを悪用した攻撃
- statd サーバを悪用した攻撃

不正アクセス報告件数の推移



なぜ減ったの?

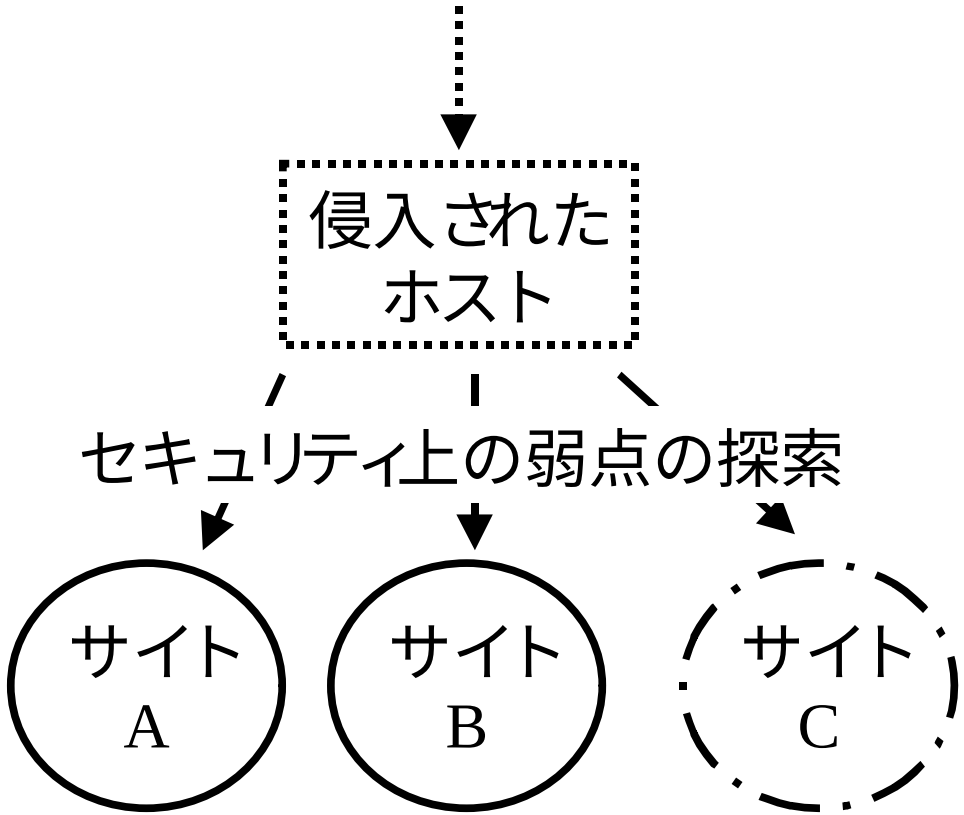
- 不正アクセスの減少
- 報告意欲の低下
  - 実害がなくなった
    - 対策済み/対応可能
    - ポートスキャン/不正な中継等の日常化
  - JPCERT/CCの対応
    - 何を期待してよいのか?
    - 何もしてくれなかった

コンピュータセキュリティ インシデントハンドリング

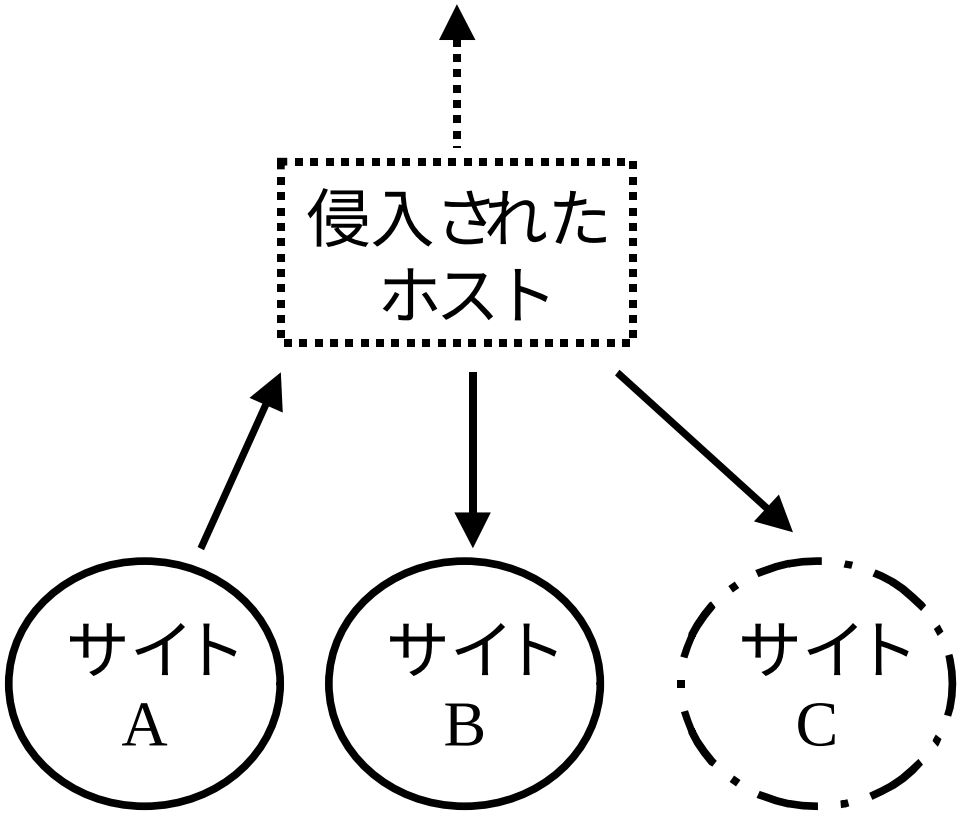
- コンピュータセキュリティインシデントとは
  - 個別の不正アクセス
  - 一連の不正アクセス
- 何をするのか?
  - 報告の受付
    解決/再発防止への**技術的な支援**
  - 関連サイト/組織への連絡
    拡大防止のための通知/情報交換

⇒情報の収集/分析

典型的なインシデント



JPCERT/CCの対応



報告:サイトA

分類 侵入後、踏み台として使われた

発生日時 6月23日10時

...
Jun 23 10:00:00 asite statd[123]: statd: open of /var/statmon/sm/;
...

発見方法 攻撃先からの通知

要望 解決に協力してほしい

その他 侵入者はポートスキャンを実行している

サイトAへの対応

① ログ等の情報の収集
- 侵入経路/影響範囲
- 提供された情報をもとに対応する

② 解決方法の紹介
- パッチ/バージョンアップ
- 再発防止

③ 関連サイトへの連絡/情報開示の確認
- JPCERT/CCから通知するには開示許可が必要

解析

① 関連サイトの抽出

- サイトAから提供された情報
- 他のサイトからの報告

③ 関連サイトへの連絡/情報開示の確認

- JPCERT/CCから通知するには開示許可が必要

報告:サイトB

分類 ポートスキャン

発見方法 ログの監視

```
...
Jun 23 12:34:00 bsite telnetd[12]: connect from 192.168.100.1
Jun 23 12:34:00 bsite popper[13]: @[192.168.100.1]: -ERR POP EOF received
...
```

要望 攻撃元に連絡してほしい

条件 全ての情報を開示してよい

その他 タイムゾーンはJST、時刻は正確

JPCERT/CCがすること できること

- 個別サイトに対する技術的な支援
  - 不正アクセスを受けたサイトに解決方法を紹介する
  - 不正アクセスを受けている可能性のあるサイトに通知する
- コミュニティに対する情報提供
  - 不正アクセスの動向を調査して報告する
  - 緊急報告等の文章を発行する

JPCERT/CCがしないこと できないこと

- 個別サイトに対する
  - リモートチェック
  - コンサルティング
- 非技術的な支援
  - 法律や組織のポリシーに関わる問題
  - 犯人の特定/捜査
- 強制力を持っていない
  - 許可のない情報の開示
  - 加圧

JPCERT/CCへのアクセス

- WWW (World Wide Web) & FTP
  - URL: http://www.jpcert.or.jp/
  - URL: ftp://ftp.jpcert.or.jp/
- 情報提供用メーリングリスト
  - URL: http://www.jpcert.or.jp/announce.html
- コンタクト情報
  - 電子メール: info@jpcert.or.jp
  - 電 話: 03(5575)7762
  - ＦＡＸ: 03(5575)7764