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 (2)

JPCERT/CC
(コンピュータ緊急対応センター)

広範囲なスキャニング

- Finger、TELNET、IMAP、POP、HTTP、NFS、DNS、X のサービスへ接続を試みる
- ツールを使っているもよう
  - 日本のドメインを攻撃する例を紹介している
- 以下のドメインから報告を頂いています
  - or.jp, ac.jp, co.jp
  - 広範囲のホストが影響を受けている可能性がある
  - もしかして、日本全体？

メールの不正中継

- 相変わらず多数の報告を受け取っています
- 2つのパターン
  (1) 中継に利用される
  (2) 勝手に名前を騙られる
  (1) → (2) という例もある
- 全てのサイトで対策を施す必要がある

smurf

- IP Denial of Service attack
- ときどき見かける
- Ingress Filtering
  - RFC 2267

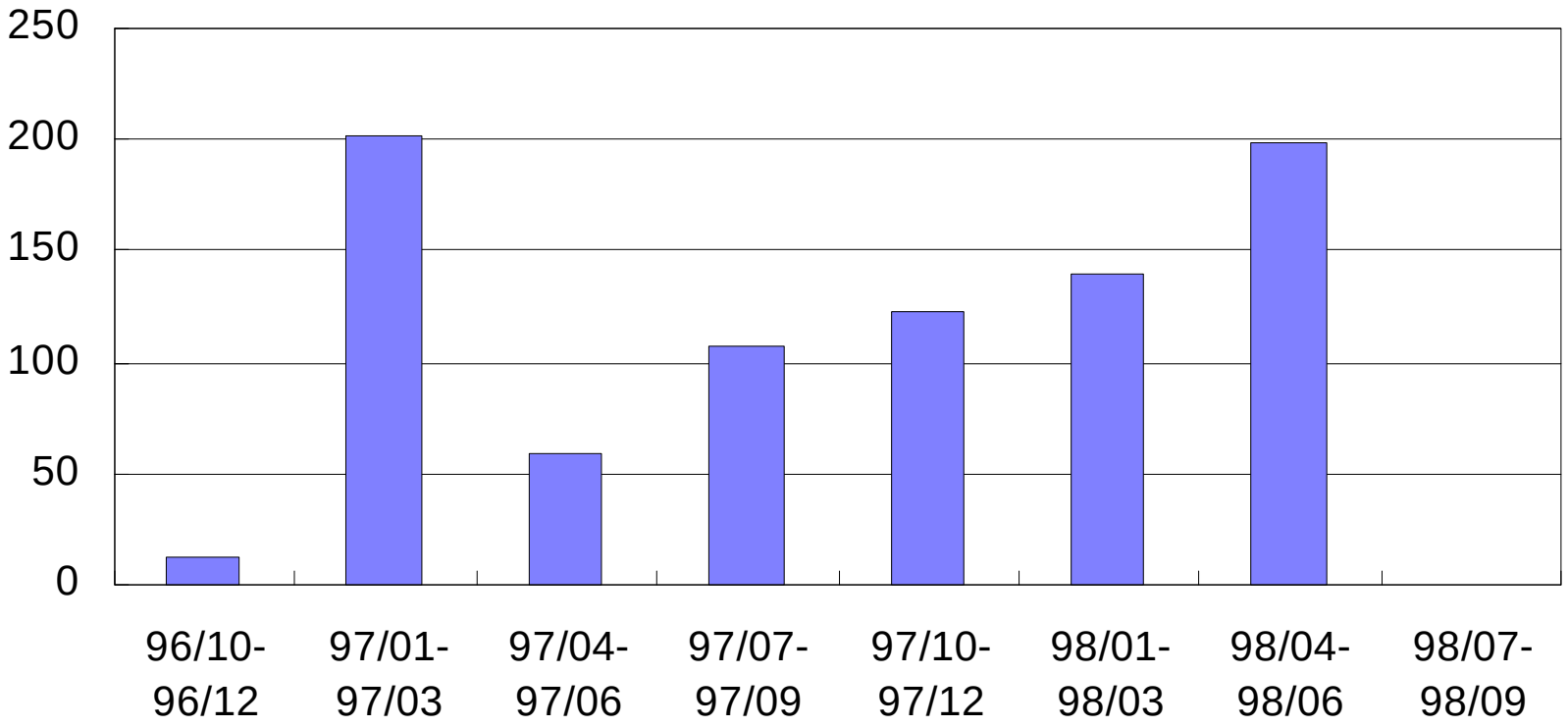
不正アクセスの動向 [997/10～1997/12]

- IMAP サーバプログラムを悪用したアタック
- Webサーバのcgi-binプログラムを悪用した攻撃
- システムへの不正侵入
- 電子メールの不正な中継と電子メール爆撃

不正アクセスの動向 [998/1〜1998/3]

- Anonymous (匿名) FTP サービスを悪用したアタック
- システムへの不正侵入および管理者権限詐取
- 電子メールの不正な中継と電子メール爆撃
- 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アタック
- ネットワークやホストの運用を妨害しようとする攻撃
- ネットワークニュースサーバ (INN) を悪用したアタック
- statd サーバを悪用した攻撃
- パケット盗聴プログラムによる攻撃

不正アクセス報告件数の推移



海外との連携強化 (FIRST加盟)

- 名称
  - the Forum of Incident Response and Security Teams
- 目的
  - メンバー間の協調、迅速な対応、情報共有等
- 組織
  - Steering Committee、Secretariat
- 構成メンバー
  - 政府、民間組織、研究機関
  - 73 組織が参画 (Jul. 3, 1998 現在)
    - 民間企業の顧客や特定の政府機関向け等あり
    - National IRTのない国がまだまだ沢山ある！！

海外との連携強化 (FIRST加盟)

- イベント
  - FIRST Conference and Workshop on Computer Security Incident Handling and Response
    - 10th Conference
    - Monterrey, Mexico、22 - 26 June 1998
- FIRST への参画
  - メンバー登録 (作業中)
  - メンバー間の情報交換
  - 国際貢献

アジア太平洋地域におけるIRT構築支援

- 名称
  - APCIRC
    - Asia Pacific Security Incident Response Coordination
  - APNGのワーキンググループ
- 目的
  - AP地域におけるIRTフォーラム
  - 情報共有
  - IRTの構築を支援する
- メンバー
  - 日本、韓国、シンガポール、オーストラリア
- 現在は活動準備段階

JPCERT/CCからのお願い

- JPNICデータベースの更新
  - インシデントの連絡先として
- Network Operations Mailbox
  - RFC2142

JPCERT/CC
ー情報提供のお願いー

- 1.不正アクセスを受けたサイト
- 2.あなたの連絡先
- 3.影響を受けたホストの情報
- 4.不正アクセスの内容

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
  - F A X: 03(5575)7764