JPCERT CC Japan Computer Emergency Response Team Coordination Center

インシデント対応チームの必要性

～守るだけがセキュリティではない～

JPCERT コーディネーションセンター
山賀正人
office@jpcert.or.jp

2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

JPCERT/CC の紹介

2003/07/10

© 2003 JPCERT/CC

JPCERT CC Japan Computer Emergency Response Team Coordination Center

JPCERT/CC とは

- Japan Computer Emergency Response Team Coordination Center
- 1996年10月設立の民間の非営利団体
  1992年ころにボランティアではじまったグループを起源とするエンジニア集団
- 日本で最初に FIRST に加盟した CSIRT
  国際的に認知されている組織

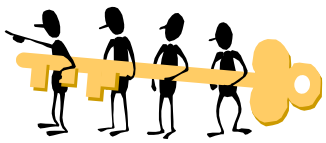
2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

CSIRT とは

Computer Security Incident Response Team

- 1988年11年「Morris worm 事件」
- 米国カーネギーメロン大学の CERT/CC (Computer Emergency Response Team Coordination Center)
  - CERT という単語は CERT/CC の登録商標
- 現在では世界中に多数の組織
  - CERTCC-KR (韓国)
  - AusCERT (オーストラリア)
  - CERT-Renater (フランス)
  ……
- 組織によって形態・対応内容は様々
- RFC 2350 参照



2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

FIRST とは

http://www.first.org/

- Forum of Incident Response and Security Teams
- 1990年 CERT/CC などが中心となって設立
- 世界中の CSIRT 同士の交流を目的にした組織

  http://www.first.org/team-info/
  - 情報の共有
  - インシデント対応 (Incident Response) の国際協力

JPCERT CC Japan Computer Emergency Response Team Coordination Center

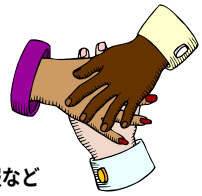
Computer Security Incident とは

- コンピュータセキュリティに関係する人為的事象で、意図的および偶発的なもの
- 弱点探索、リソースの不正使用、サービス運用妨害行為など
- 『不正アクセス (行為)』は狭義に規定された

JPCERT CC Japan Computer Emergency Response Team Coordination Center

JPCERT/CC の業務

- 窓口対応
  - 情報提供の受付
  - 一般的な技術情報の紹介
  - 関連組織への連絡
    国内と国外との間の連絡など
- 技術情報の日本語による発信
  - 注意喚起、緊急報告、技術メモ、メールマガジン、統計情報など
    メーリングリストと Web による公開
  - ベンダなどとの連携
  - セミナーなどによる啓発活動
- 国際連携
  - FIRST に加盟し、日本を代表して国際的に活動している組織
  - アジア太平洋地域におけるセキュリティ対策組織を集めた国際会議を主催
    (APSIRC: Asia Pacific Security Incident Response Coordination Conference)



JPCERT CC Japan Computer Emergency Response Team Coordination Center

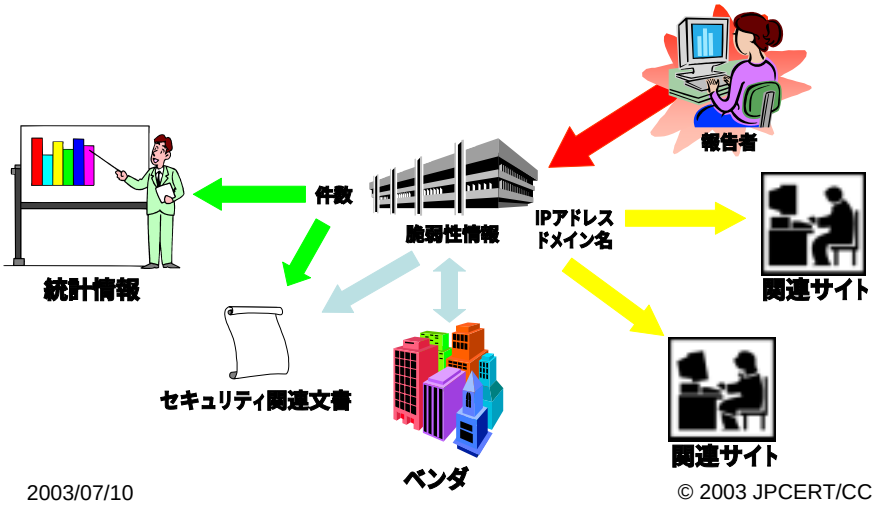
APCERT

http://www.apcert.org/

- Asia Pacific Computer Emergency Response Team
  - アジア太平洋地域の CSIRT フォーラム
  - Steering Committee Member
  - Secretariat
  - 年次定例会議としての APSIRC

JPCERT CC Japan Computer Emergency Response Team Coordination Center

報告された情報のゆくえ



2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

技術文書の情報源

- 関係組織が公開している情報
  - CSIRT (CERT/CC, CIAC, AusCERT など)
  - ベンダなど
- 独自に調査研究した情報
- ***窓口に届いた情報***

2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

JPCERT/CC ではできないこと

- 個別サイトに対する監視やコンサルティング
- 個々のアプリケーションについてのコンサルティング
- 非技術的な支援
  - 紛争の調停、対応の強制
  - 捜査、犯人追及、証拠物件の押収
  - 法律面での支援 (損害賠償請求など)

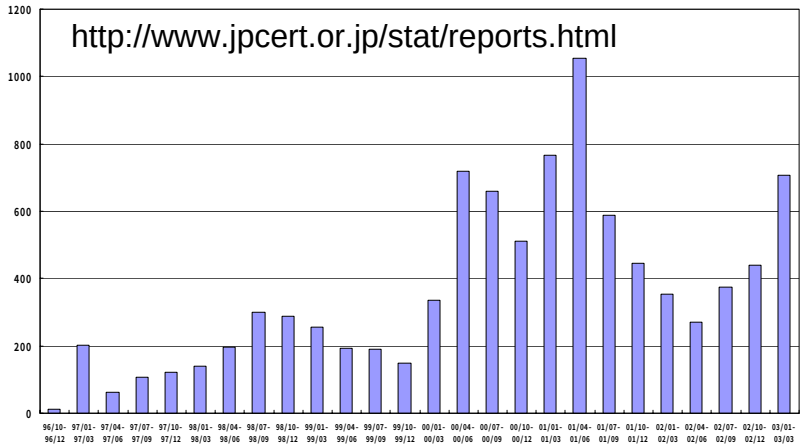
強制力のある組織ではない

JPCERT CC Japan Computer Emergency Response Team Coordination Center

最近の統計情報から

JPCERT CC Japan Computer Emergency Response Team Coordination Center

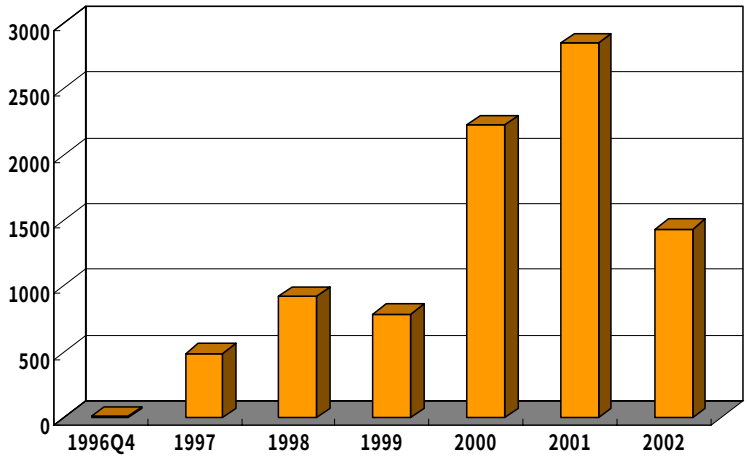
JPCERT/CC へのインシデント報告件数の推移



2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

JPCERT/CC へのインシデント報告件数の推移

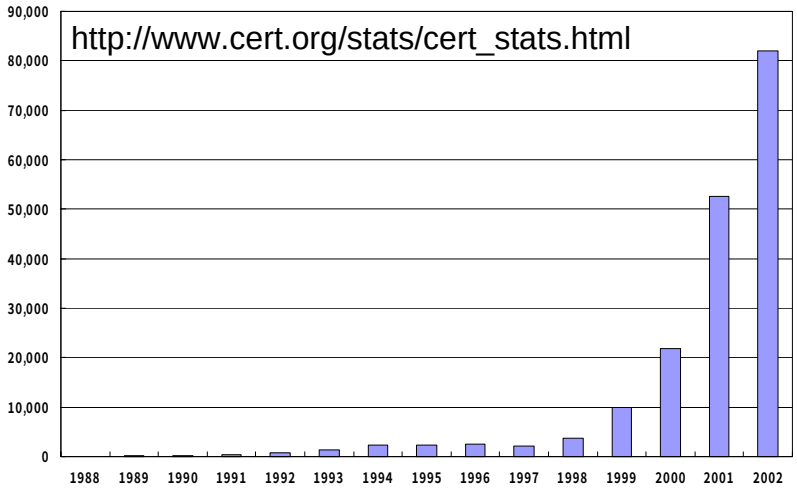


2003/07/10

© 2003 JPCERT/CC

JPCERT CC Japan Computer Emergency Response Team Coordination Center

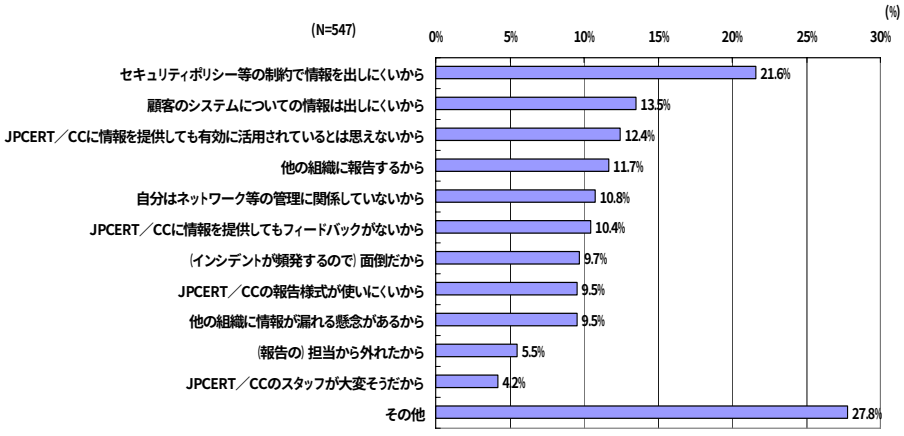
米国 CERT/CC へのインシデント報告件数の推移



2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

報告しない（しなくなった）理由



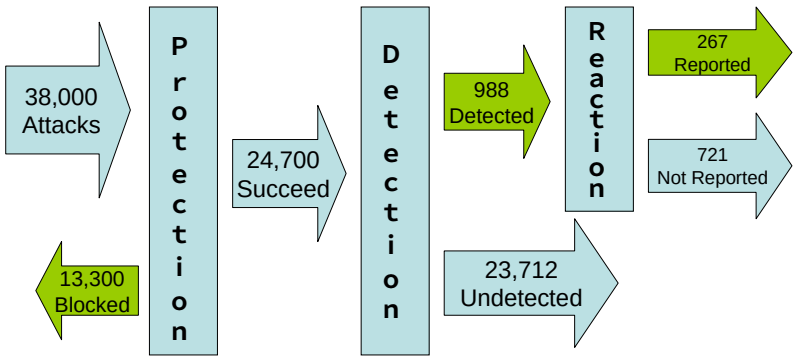
2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

参考資料

GAO (The United States General Accounting Office) **の文書**

INFORMATION SECURITY:
Computer Attacks at Department of Defense Pose Increasing Risks
http://www.gao.gov/archive/1996/ai96084.pdf



GAO/AIMD-96-84 Defense Information Security

JPCERT CC Japan Computer Emergency Response Team Coordination Center

インシデントタイプ別分類

JPCERT CC Japan Computer Emergency Response Team Coordination Center

インシデントの分類

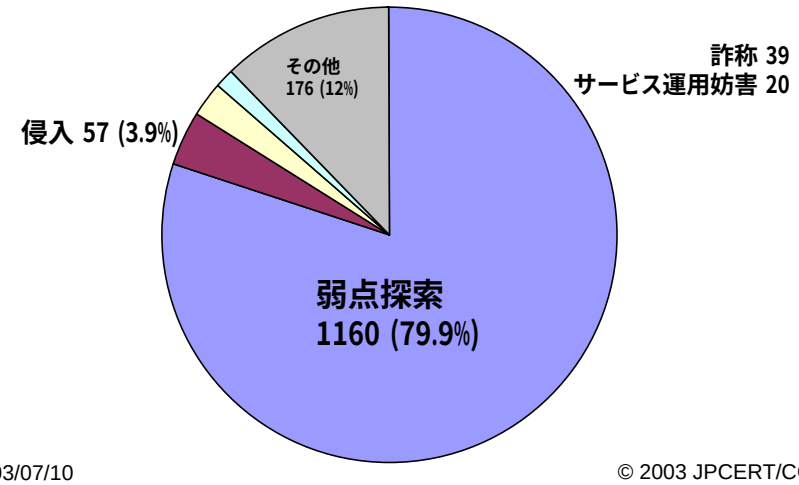
報告者の視点で分類

- **サービス運用妨害** (DoS: Denial of Service)
  - **分散型サービス運用妨害** (DDoS: Distributed Denial of Service)
- **詐称 (電子メール)**
- **サービスの悪用、不正中継**
- **侵入、無権限アクセス**
- **弱点探索 (スキャン、プローブ)**
- **その他** (JPCERT/CC **で扱えないものなど**)

2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

2002年インシデントタイプ別分類



2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

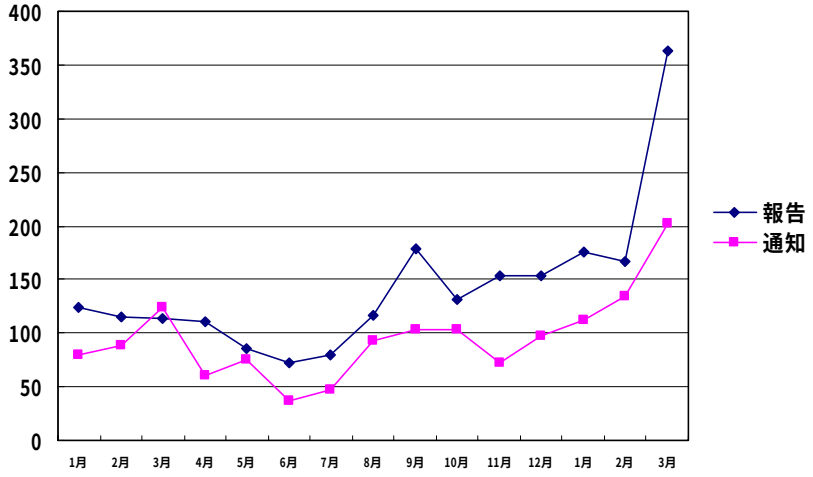
弱点探索は、より深刻なインシデントの発生を示している。

弱点探索のアクセス元は多くの場合、踏み台として悪用されている。

2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

報告件数および通知件数の推移



2003/07/10

© 2003 JPCERT/CC

JPCERT CC Japan Computer Emergency Response Team Coordination Center

各インシデントタイプについて

2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

サービス運用妨害 (DoS)

ネットワーク帯域などの資源を消費させ、サービス不能に導く。一般的に攻撃元は詐称されている。

例) SYN Flood 攻撃、UDP Flood 攻撃、Smurf 攻撃など

完全に防ぐ方法はない

- ルータなどによるパケットフィルタリング
- ネットワークの監視など

2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

分散型サービス運用妨害 (DDoS)

第三者の複数のコンピュータに Agent と呼ばれるプログラムを侵入させ、それらを使って大量のデータを一斉に攻撃対象のコンピュータやネットワークに送信することでサービスを妨害する。

完全に防ぐ方法はない

- Agent を侵入させられないために
  - 最新のパッチの適用
  - 不必要なサービスの停止または削除

JPCERT CC Japan Computer Emergency Response Team Coordination Center

詐称

- 電子メールの From: 欄の偽造
  - 他人へのなりすまし
  - 返答メールが偽造されたアドレスに送付

完全に防ぐ方法はない

メールアドレスを必要以上に公にしない

JPCERT CC Japan Computer Emergency Response Team Coordination Center

サービスの悪用

- メールサーバプログラムの不正中継

  SPAM メールの配送に使われ、送信元と見なされてしまう。
- プロクシサーバの不正利用
  - なりすまし (アクセス元アドレスの隠蔽など)
  - BBS, チャット などへの書き込み

単なるサーバプログラムの設定ミス

2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

侵入

- パスワード管理の甘さ
- 主に**バッファオーバーフローの脆弱性**を悪用
  - 配列の大きさをチェックせずにデータを格納してしまう、プログラム上のミスが原因

    例) C言語の関数 strcpy(), strcat(), sprintf() など
  - プログラムの異常停止を伴う
  - 挿入したマシン語の実行
    - 管理者権限の取得
    - データ改ざん
    - バックドアの設置など

2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

侵入を防ぐには

- 最新のパッチを適用
- 不必要なサービスを停止または削除
- ルータなどによるパケットフィルタリング
- サービスを提供する相手の制限 (アクセス制御)
  - IP spoofing からの防御も重要

自ネットワークのアドレスを詐称したパケットの外部からの侵入を防ぐ

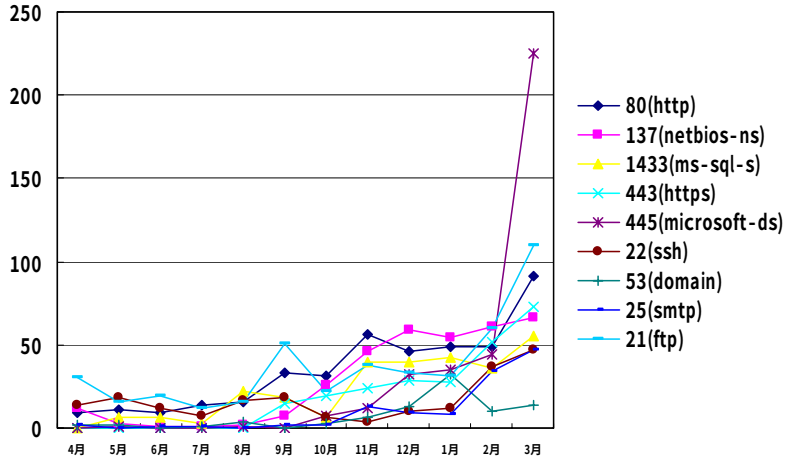
JPCERT CC Japan Computer Emergency Response Team Coordination Center

スキャン、プローブ
(弱点探索)

- ほとんどの場合実害はない
- インシデントの兆候 (?)
  - 侵入の試み (?)
  - 新たな脆弱性の発見の兆し (?)
  - バックドア設置の確認 (?)

JPCERT CC Japan Computer Emergency Response Team Coordination Center

2002年度スキャン報告の推移



2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

スキャン報告の件数と脆弱性情報の公開やワームなどの広まりには相関がある。

スキャン情報の、より効率的な収集方法については現在検討中

2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

インシデント対応チームの必要性

2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

守るだけがセキュリティではない。

- 人為的ミス (パッチの適用忘れなど)
- 未知 (公知になっていない) の脆弱性の悪用

「100% **安全**」はありえない。

いかに素早くインシデントに気づき、
対応できるか、が重要

2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

インシデントを発見する手順の明確化

- ログの取得内容の整理
- ログの確認
- 異常事態発生時の報告の仕組み

など

管理者のためのセキュリティ推進室

インシデントレスポンス入門

http://www.jpcert.or.jp/magazine/atmarkit/

2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

万が一の事態が起こった後の対応手順の明確化

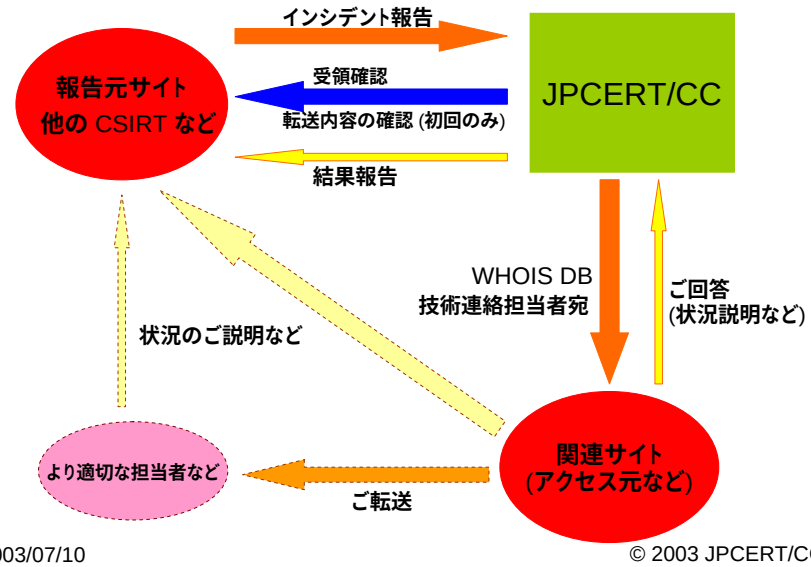
- 連絡体制
- 原因の究明
- 復旧
- 再発防止
- 関連サイトとの連絡

など

2003/07/10

JPCERT/CC Japan Computer Emergency Response Team Coordination Center

JPCERT/CC によるインシデント対応の流れ



2003/07/10

JPCERT/CC Japan Computer Emergency Response Team Coordination Center

インシデント関連情報の共有

2003/07/10

JPCERT CC Japan Computer Emergency Response Team Coordination Center

何故情報を共有すべきなのか?

- 世の中で一体何が被害を広めているのか?
  - この不審なアクセスは自分のところだけ?
  - 意図的なもの? それとも単なる操作ミス?
- 未知の脆弱性の発見
  - 被害の拡大を未然に防げる

JPCERT CC Japan Computer Emergency Response Team Coordination Center

CSIRT 間の連携の必要性

- 情報共有 (インシデント対応) を円滑に
  - 情報管理ポリシーは組織ごとに異なる
  - 違いを相互に認め合った上での情報交換
- sensitive な情報のやり取りには信頼が第一

JPCERT CC Japan Computer Emergency Response Team Coordination Center

世界的な動き

- **業界ごとに** ISAC (Information Sharing and Analysis Center) **設立**
  - **米国** IT-ISAC http://www.it-isac.org/
  - **日本でも** Telecom-ISAC **などの設立の動き**
    http://www.soumu.go.jp/s-news/2003/pdf/030210_2.pdf

JPCERT CC Japan Computer Emergency Response Team Coordination Center

最後に

JPCERT CC Japan Computer Emergency Response Team Coordination Center

最近の特徴

- 手口そのものは昔から大きく変わっていない
  - 複合的な攻撃
  - 誰でも使えるツール (rootkit など)
- 一般家庭の (高速な) 常時接続が浸透
  - 被害の拡大 (広範囲、高スピード)
  - 誰でも攻撃の対象になってしまう
- サーバ構築が容易
  - セットアップしたまま放置 (試験運用したサーバなどに多く見られる)
  - 標準で様々なサービスが有効
  - ルータなどのネットワーク機器も同じ

JPCERT CC Japan Computer Emergency Response Team Coordination Center

被害者＝加害者？

- ワーム
- DDoS の Agent
- MTA やプロクシサーバの不正中継
  - SPAM メールの送信元に悪用
  - なりすましによる誹謗中傷の書き込み
  - などなど…
- 本当に「悪い奴」は捕まらない
  - 踏み台にされたサイトに損害賠償請求????

JPCERT CC Japan Computer Emergency Response Team Coordination Center

攻撃から守るには

- 不要なサービスの停止
  - 使わないものはアンインストールするなど
- 最新のセキュリティ情報の入手
  - セキュリティ関連のパッチの適用
- ネットワークの監視
- サービスの運用ポリシー (アクセス制御など)
- その他 (IP spoofing からの防御など)

JPCERT CC Japan Computer Emergency Response Team Coordination Center

JPCERT/CC 発行の技術メモ

http://www.jpcert.or.jp/ed/

コンピュータセキュリティインシデントに対する
一般的な対応方法についての説明

サイトごとのポリシー策定などの参考に

JPCERT CC Japan Computer Emergency Response Team Coordination Center

JPCERT/CC へのアクセス

✉ E-mail:	**info@jpcert.or.jp**
💻 Web:	**http://www.jpcert.or.jp/**
報告様式:	**http://www.jpcert.or.jp/form/**
ﾒｰﾘﾝｸﾞﾘｽﾄ:	**http://www.jpcert.or.jp/announce.html**
☎ **ﾌｧｯｸｽ**:	03-3518-2177 (**変更されました**)

※ **電話によるインシデント報告は受け付けておりません。**

2003/07/10