JPCERT CC Japan Computer Emergency Response Team Coordination Center

教育現場での インターネットセキュリティ対策

「EDU-TALK SUMMER FORUM'99」
～ 学校のインターネット接続について考える～

1999.8.10

山口 英 JPCERT/CC運営委員長

JPCERT CC Japan Computer Emergency Response Team Coordination Center

概要

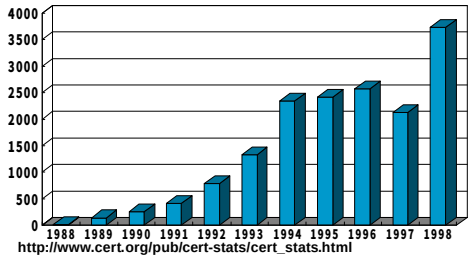
- 不正アクセスの動向
  - 発生状況, パターン, 事例
- 対策のポイント
  - 目標設定, システム管理, 教育・啓発
- 学校におけるセキュリティ対策
  - みなさんにお願いしたいこと..

JPCERT CC Japan Computer Emergency Response Team Coordination Center

不正アクセスの動向

JPCERT CC Japan Computer Emergency Response Team Coordination Center

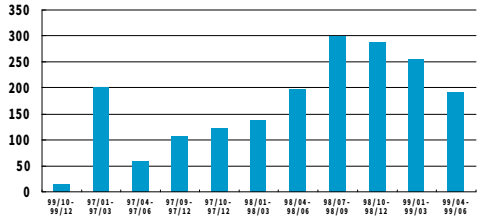
増加する不正アクセス件数



http://www.cert.org/pub/cert-stats/cert_stats.html

JPCERT CC Japan Computer Emergency Response Team Coordination Center

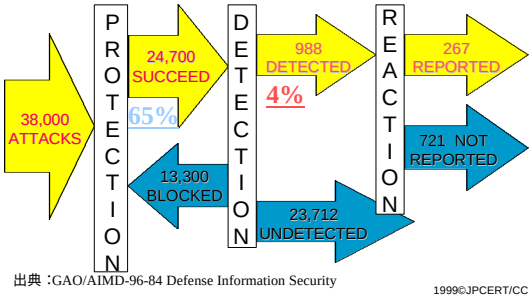
国内における状況



http://www.jpcert.or.jp/anm/stats.html

JPCERT CC Japan Computer Emergency Response Team Coordination Center

不正アクセスは検出されにくい！



出典：GAO/AIMD-96-84 Defense Information Security

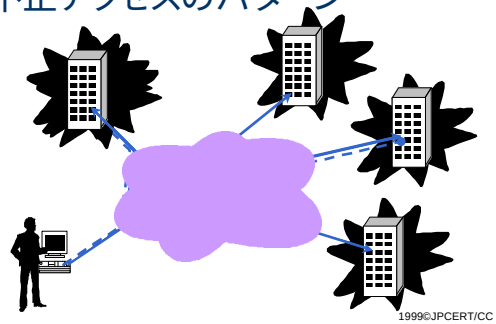
JPCERT CC Japan Computer Emergency Response Team Coordination Center

不正侵入者の組織化

- 情報交換の場
  - メーリングリスト
  - WWWサーバ, FTPサーバ
  - 雑誌
- 交換される情報
  - 手口の公開
  - 流出したパスワード 電話番号のリスト 流出した情報
  - 侵入用のソフトウェア

JPCERT CC Japan Computer Emergency Response Team Coordination Center

不正アクセスのパターン



JPCERT CC Japan Computer Emergency Response Team Coordination Center

不正アクセスのパターン

- 不正侵入
  - パスワード推測 •破り、パケット盗聴、バッファあふれ
- 踏み台 •中継
  - 電子メールやネットワークニュースの不正中継、
    Webプロキシー悪用、匿名FTP悪用、パケットの増幅(?)
- 運用妨害 業務妨害
  - パケット大量送信、電子メール爆撃、電子メール偽造、
    Webチャット潰し、ネットワークニュースのコントロールメッセージ
- 無差別攻撃
  - ポートスキャン

JPCERT CC Japan Computer Emergency Response Team Coordination Center

狙われやすいサービス

- Web
  - CGI プログラム
  - プロキシ不正利用
  - ページ書き換え
  - 運用妨害
- finger
- telnet
- NFS (statd)
- DNS (named)
- IMAP、POP
  - 不正侵入
- FTP
  - ディレクトリ不正使用
- 電子メール
  - 不正中継
- ネットワークニュース
  - 不正なポスト
  - コントロールメッセージ
- ルータ
  - 侵入、設定変更、踏み台
- and more

JPCERT CC Japan Computer Emergency Response Team Coordination Center

頻発するWebjack

- 山ほどある... (抜粋)
  - Yahoo
  - UNICEF
  - Harvard University
  - Oregon Department of Forestry
  - www.*.go.id
  - One Touch Interactive
  - First Michigan Bank
  - Bay Area She Hawks
- 有名どころでは... (抜粋)
  - CIA
  - Air Force, Army
  - WhiteHouse
  - 米国上院
- 最近、国内でも流行しはじめた!

JPCERT CC Japan Computer Emergency Response Team Coordination Center

JPCERT/CC Japan Computer Emergency Response Team Coordination Center

不正アクセス対策のポイント

JPCERT/CC Japan Computer Emergency Response Team Coordination Center

不正アクセス対策のポイント

- 完全な対策はない…
- 目標を設定する
  - 必要なサービスは何か
- システム管理に求められるもの
  - セキュリティポリシーの策定と施行
  - 不正アクセス発生時の緊急体制の整備
- 利用者(生徒)に対する教育・啓発

JPCERT/CC Japan Computer Emergency Response Team Coordination Center

不正アクセス対策のポイント

- 完全な対策はない…
  - 変化が激しい
    - 昨日は安全でも今日も安全とは限らない
  - 本質的に防御できないものもある
  - それでも注意すれば「だいたいは」防げる
    - ほとんどの不正アクセスは既知の手口である
    - 事前の工夫によって影響を低減できる

JPCERT CC Japan Computer Emergency Response Team Coordination Center

不正アクセス対策のポイント

- 目標を設定する
  - 必要なサービスのみ提供
    - 利用者が求めるサービスの調査
    - リスク分析
  - 不必要なサービスは停止
    - 利用しないプログラムは使用不可能に
  - バランスを考慮
    - 利用者が 秘密の抜け穴」を作る

JPCERT CC Japan Computer Emergency Response Team Coordination Center

不正アクセス対策のポイント
～ システム管理に求められるもの

- セキュリティポリシーの策定と施行
  - 保護対象の明確化
  - 脅威・リスクの把握
  - 対策コストの設定
- 運用状況を記録し、定常的に検査
- 最新のセキュリティ情報を入手し、メンテナンス
- セキュリティポリシーの見直し(改訂)

JPCERT CC Japan Computer Emergency Response Team Coordination Center

不正アクセス対策のポイント
～ システム管理に求められるもの

- 不正アクセス発生時の緊急体制
  - 責任者と対応者
  - 連絡手順
  - 作業の優先順位
  - 復旧手順
  - 外部との窓口

JPCERT/CC Japan Computer Emergency Response Team Coordination Center

不正アクセス対策のポイント
～ 利用者(生徒)への教育・啓発

- リスクの存在を理解させる
- 利用者としての責任を理解させる
  - セキュリティポリシーの遵守
  - 異状の報告

(例)
  - パスワード
  - 電子メールアドレス（ユーザ名）

JPCERT/CC Japan Computer Emergency Response Team Coordination Center

学校におけるセキュリティ対策

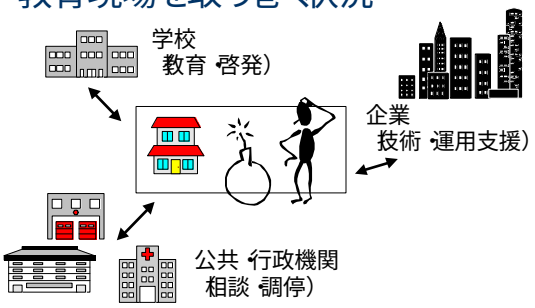
JPCERT/CC Japan Computer Emergency Response Team Coordination Center

学校の特殊性

- システム運用・利用に関わる人たちが多い
  - 教員
  - 学生
  - 教育委員会
  - 保護者
- コンセンサスの形成が必須
  - セキュリティはシステム運用・利用に関わる全ての人の問題
  - 相互理解は必須

JPCERT CC Japan Computer Emergency Response Team Coordination Center

教育現場を取り巻く状況



JPCERT CC Japan Computer Emergency Response Team Coordination Center

まず考えるべきことは

- 役割分担とコミュニティの立ち上げ
  - 行政, 学校, 家庭
  - 立場・役割・サービス
  - 「何に責任を持つのか」という点に関する相互理解
  - 抜け落ちている役割を作り出さない
- 相互のコミュニティ間の調整
  - 技術交換
  - 緊急時の協調体制の確立

JPCERT CC Japan Computer Emergency Response Team Coordination Center

その他の注意点

- ある日、いきなり管理者になってしまったとき
  - ひとりで悩まない！
  - 近場で、コミュニティを作ろう
  - 勉強しよう
  - パブリック・リソースの利用
- ある日、困った問題が起こったとき
  - 緊急対応体制を作ろう
  - 教育機関のための支援機関があるといいなぁ
  - JPCERT/CC もご支援します

JPCERT CC Japan Computer Emergency Response Team Coordination Center

JPCERT/CCについて

JPCERT CC Japan Computer Emergency Response Team Coordination Center

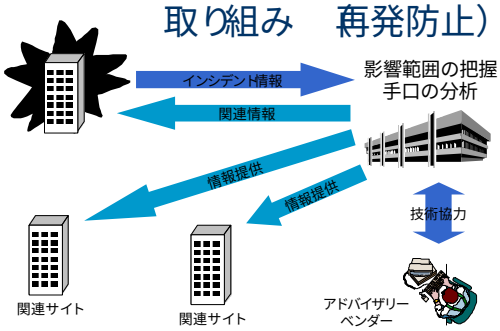
JPCERT/CC の役割

- コンピュータセキュリティインシデント対応機関
  - 1996年10月事務所開設
  - 不正アクセスの届出受付と対応
  - セキュリティ関連情報の提供
- コーディネーションセンター
  - 中立・民間・非営利
    - 特別な権限なし
  - 技術面での活動
- 各国 CSIRT との協調
  - Aug.98 に FIRST 加盟

1999©JPCERT/CC

JPCERT CC Japan Computer Emergency Response Team Coordination Center

取り組み　再発防止）



1999©JPCERT/CC

JPCERT CC Japan Computer Emergency Response Team Coordination Center

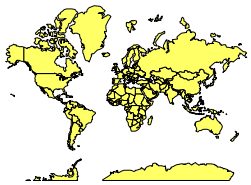
取り組み　予防）

1999©JPCERT/CC

JPCERT CC Japan Computer Emergency Response Team Coordination Center

取り組み　国際的な連携）

- FIRST への加盟
  (Forum of Incident Response and Security Teams)
  → 加盟組織間での円滑な情報交換
- APSIRC での活動
  (Asia Pacific Security and Incident Response Coordination)



1999©JPCERT/CC