インターネットにおける不正アクセスとその対策

佐野 晋
JPCERT/CC 運営委員
日本電気(株)

1998年12月16日

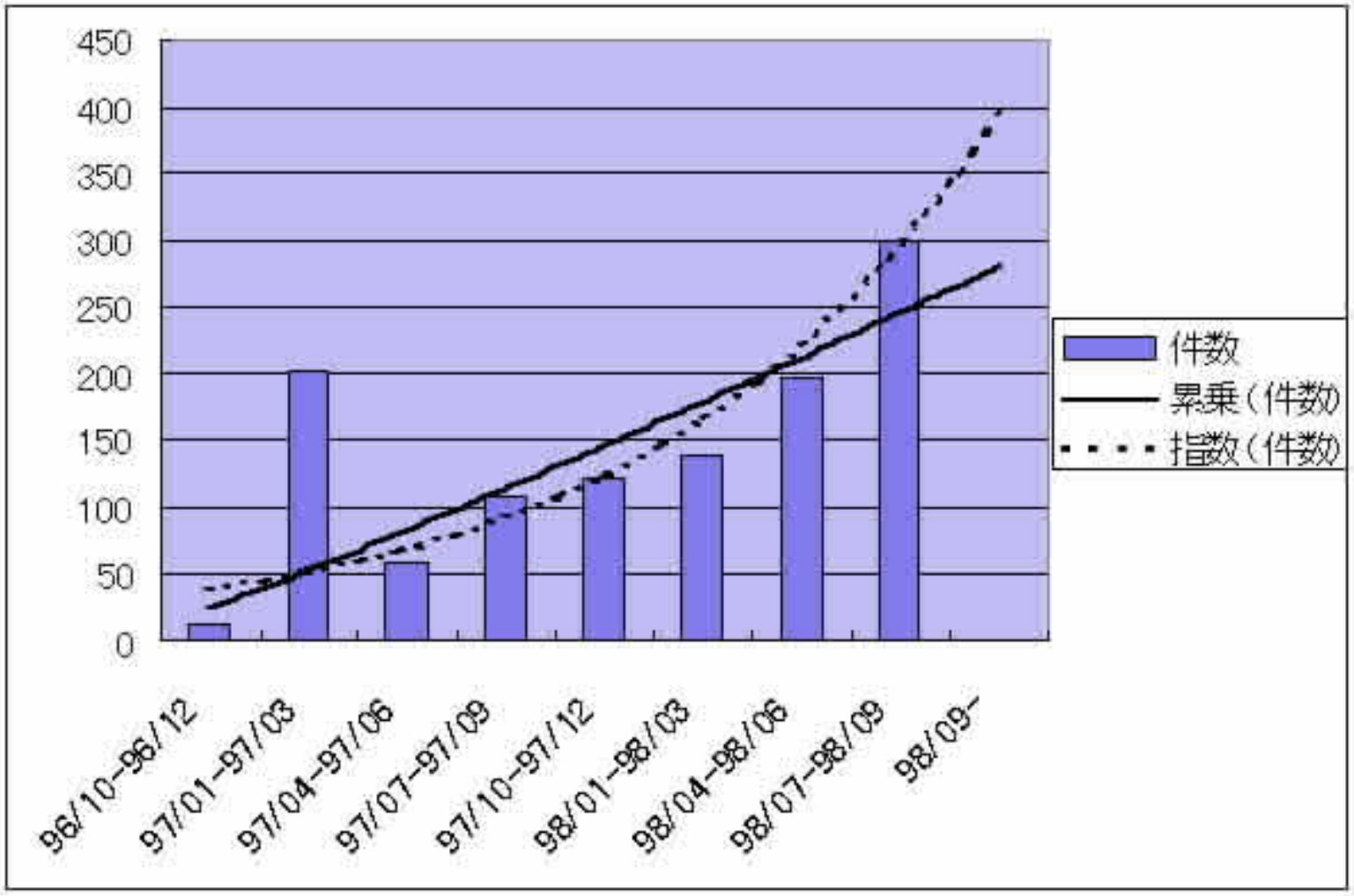
内容

- 現状
- 不正アクセスについて
  - 法律
  - 手口
- セキュリティポリシ
- 最後に

現状

JPCERT/CC報告から
http://www.jpcert.or.jp/

JPCERT/CCへの報告状況　(件数)



InternetWeek 98, Internet Security, S.Sano, 1998

JPCERT/CCへの報告状況　(サイト数)

InternetWeek 98, Internet Security, S.Sano, 1998

動向 — 1998年7月1日〜1998年9月30日

- 最新情報: http://www.jpcert.or.jp/nl/98-0004/
  - 299件, 3266サイト, 管理権限詐取 26サイト
- 主な報告
  - システムに存在するサービス/弱点の探査
  - 電子メールの不正な中継、電子メール爆撃
  - statd サーバを悪用した攻撃
  - 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
  - ネットワークやホストの運用を妨害しようとする攻撃
  - ネットニュースのコントロールメッセージを悪用した攻撃
  - パケット盗聴プログラムによる攻撃
  - Anonymous FTP サービスの不正利用
  - named サーバを悪用した攻撃

概要

- 新手の攻撃手法
  - ポートスキャン - 網羅的攻撃
- 古典的な攻撃手法
  - プログラムのセキュリティ上の弱点を利用
  - Webサーバのcgi-binの利用
  - パケット盗聴プログラムを仕込まれる
- サービスの不正利用
  - メイル中継
    - 爆弾やスパムの発信元として利用
  - アノニマスFTPの不正利用
    - 情報交換の場

スキャン (3102)

- スキャンプログラムがネットワーク上で公開
  - DNSを検索して用いてサイトを発見
  - 探索でホスト･サービスを発見
  - statd, named, nfs, X など知られた弱点を発見
  - あとは不正侵入へ
- 国内のサイトが網羅的に探索された可能性
- 被害例
  - 管理者権限でシステムへ不正侵入
- 対策
  - 不要なポート(サービス)を停止･制限
  - 関連ソフトウエアのバージョンアップなど

電子メールの不正な中継、電子メール爆撃

- 無関係なサイトへのメールの中継
  - メール爆弾, 不正メールの発信元として利用
  - CPUやネットワークの浪費
- 背景
  - ISPやユーザのスパム対策 (フィルタリング) を迂回
  - 中継サイトへの嫌がらせ, 成りすまし
- 対策
  - sendmailのバージョンアップ
  - sendmailに対して中継を制限する設定

サーバの弱点を悪用した攻撃

- statd や named などのサーバのセキュリティ上の弱点を利用
  - スタックオーバフロー
  - ファイルの流出・改ざん
  - 管理者権限でのコマンドの実行
- 対策
  - 不要ならサーバの実行を止める
  - ソフトウエアのバージョンアップ

総括

- 大多数は知られた手口
  - 知られた防御策の徹底が重要
  - 事前の工夫で影響の低減が可能
- それでも完璧な対応は困難
  - インシデントへの具体的な準備が必要
    - 被害を最小限にする計画
  - ポリシをベースに一貫性のある対策を

Our Contact

* E-mail: info@jpcert.or.jp
(Hotline:03-5575-7762
Fax: 03-5575-7764
: WWW: http://www.jpcert.or.jp/

Mailing List:
http://www.jpcert.or.jp/announce.html

不正アクセスとは

- インターネットにおける不正アクセスの特徴
- 法律の問題
- 手口

背景

- 利用範囲の拡大
  - 業務, 取り引き, 公共サービス, …
  - 経済的価値を持った情報 → 犯罪の可能性
- ユーザの広がり

  「インタネットの常識」の変化
  - コミュニティの拡大/多様化

    いい人も悪い人も
  - スキルの多様化

    技術者から子どもまで
  - 個人ユーザの増加

    無免許で自動車運転 ！！

インターネットでの不正アクセスの特性

- 広域性
  - 地球規模でのコンピュータネットワーク
  - ☛ 国境を越えた侵入
- オープン
  - 何でもつながる，誰でもつなげられる
  - プロトコル仕様公開
  - ☛ 解析，ツール開発の容易さ
- 高速性，定額料金
  - ☛ 反復的なアタック，力ずくのアタック
- 匿名性
  - 侵入者の身元を隠す
- 犯罪や不正が見えない
  - 目撃者や隠しカメラがない

脅威

- 外部･内部からのシステム不正侵入
  - コンピュータ資源の不正利用
  - 妨害，破壊
  - 悪戯
  - 踏み台
- 情報の改ざん･盗聴など
  - なりすまし
  - メッセージの偽造
  - 情報漏洩，改ざん，破壊

何から守るのか？

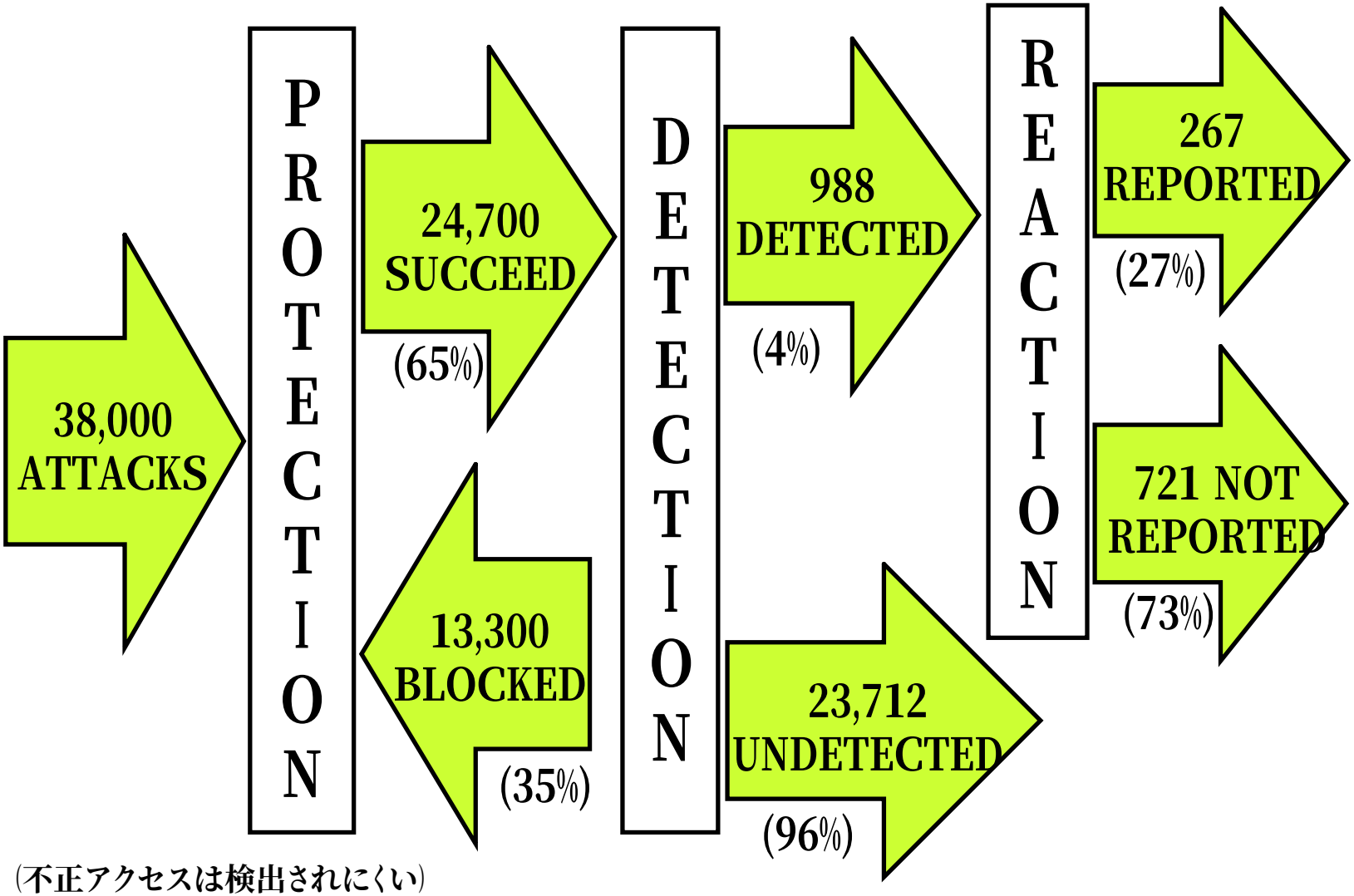
- システム運用からみると
  - 可用性(Availability)…正常な運用の維持
  - 侵入の防止，踏み台の防止
- 情報からみると
  - 機密性(Confidentiality)…盗聴の防止
  - 完全性(Integrity)…改ざんの防止と検知
  - 真正性(Authenticity)…送信者の正当性

現実は

- 手口は
  - 複雑化，高度化，巧妙化，組織化
  - 古典的な手口も
- インタネットブームによる安易な接続
  - 十分に認識されていない，対策が十分でない
  - 漠然とした不安
- 技術の問題
  - イタチごっこ
  - 情報不足，技術者不足
  - 未熟な技術，製品が十分でない

InternetWeek 98, Internet Security, S.Sano, 1998

検出は難しい



(不正アクセスは検出されにくい)

出典: GAO: Information Security, AIMD-96-84, May 1996
InternetWeek 98, Internet Security, S.Sano, 1998

インターネットにおけるシステム不正侵入

- 複数の組織が関連，国際的
  - 対策にあたっては関係者間の調整が必要
- 侵入の手口は高度，組織的
  - 対策も高度，組織的に
- 実時間
  - 緊急の対策が必要
- 影響が広範囲
  - インターネット全体の緊急連絡網が必要
- 関係組織と調整しながら緊急対応を行う専門組織が必要

InternetWeek 98, Internet Security, S.Sano, 1998

不正侵入者のコミュニティ・組織化

- 情報交換
  - メイリングリスト, WWWサーバ, FTPサーバ, FAQ, 雑誌
  - 関連するセキュリティ情報
- 情報
  - 手口の公開
  - 流出したパスワード, 電話番号のリスト,
  - 侵入用のソフトウエア

対策

- 防衛側も情報が
  - 不正アクセス技術の収集と対策

- 組織化
  - ユーザコミュニティ
  - ベンダ, システムインテグレータとの強調
  - 緊急対応チーム (IRT)の組織化
    - 組織内
    - ISP, ユーザグループなどのコミュニティ
    - 国レベル
    - 国際レベル

■法律の問題

不正アクセスの定義

- 不法又は有害な意図をもって行われる権限外のアクセスや傍受

  「コンピュータ関連犯罪－立法政策の分析」, OECD, 1986

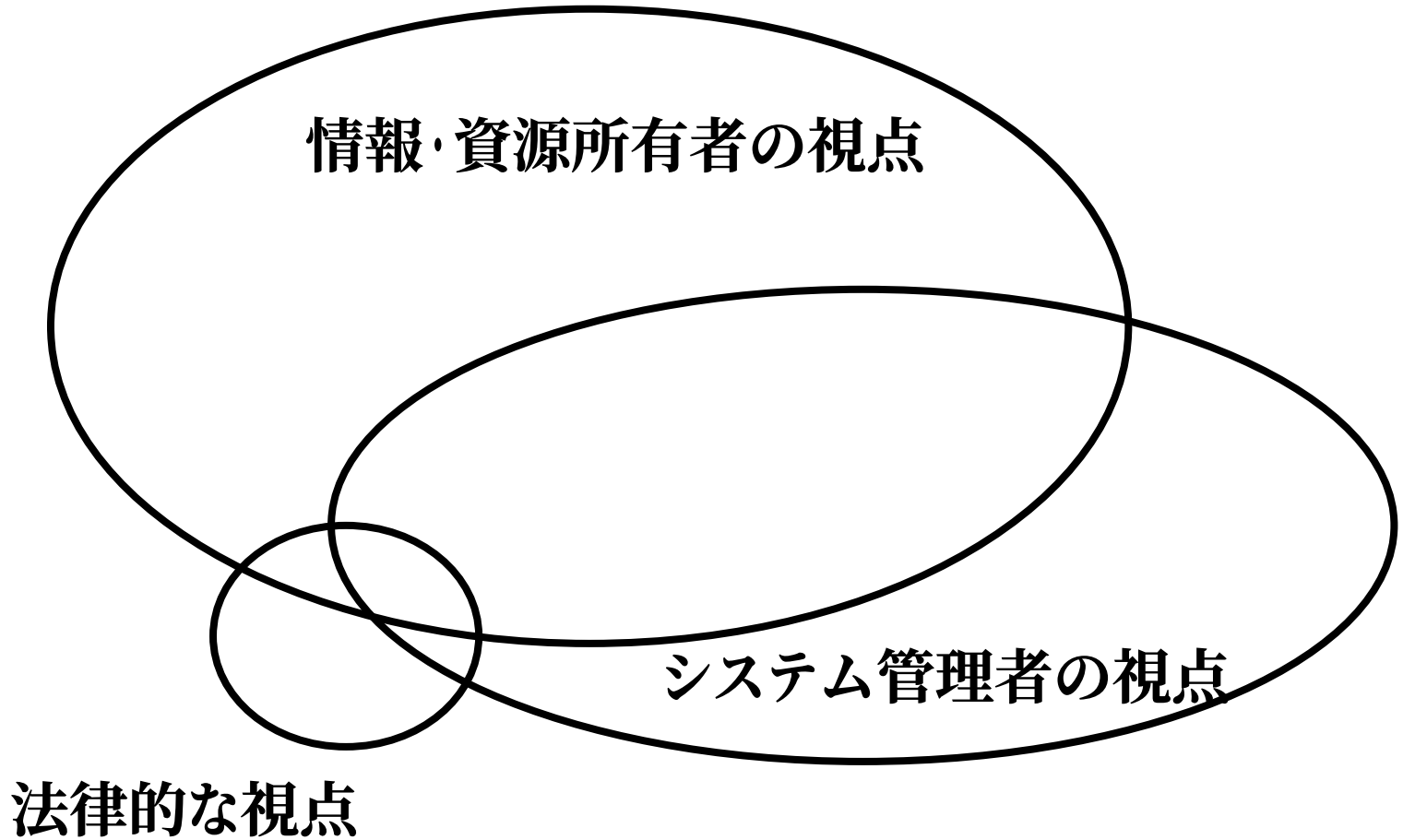
- 不正な手段により, ユーザ以外のものが行うアクセス又はユーザが行う権限外のアクセス

  「情報システム安全対策指針」, 平成9年国家安全委員会告示第9号

- システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと。

  「コンピュータ不正アクセス対策基準」, 平成8年通商産業省告示第362号

不正アクセス　－みっつの視点



InternetWeek 98, Internet Security, S.Sano, 1998

日本で違法となる不正行為の例

- 貯金元帳ファイルへの不正データの入力など
  - 電子計算機使用詐欺(刑法246-2)
  - 電子計算機損壊等業務妨害(刑法234-2)
- データベースやファイルのデータ消去など
  - 電磁的記録不正作出(刑法161-2)
  - 電磁的記録毀棄(刑法258, 259)
  - 器物損壊(刑法261)
  - 電子計算機損壊等業務妨害(刑法234-2)
- 詐欺, 猥褻図画陳列など
  - 詐欺(刑法246)
  - 猥褻図画陳列(刑法175)
- ソフトウエアの不正コピー, 薬物売買など
  - 著作権法違反
  - 覚せい剤取締法違反

日本で違法にならない不正行為の例

- パスワードを入手
  - パスワード類推
  - ソフトによる検出
  - 盗聴
- パスワードの売買
- システムへの侵入
  - 他人宛のメールを読む，パスワードを盗む，売る
  - コンピュータの無権限使用

法整備は検討されているが，定義は難しい

InternetWeek 98, Internet Security, S.Sano, 1998

不正アクセス法に関する公開コメント

- 警察庁が1998年11月17日に案を発表
  - http://www.npa.go.jp/
  - 12月16日が締め切り
- 背景
  - インターネット犯罪に対抗するため不正アクセスの可罰化
  - コンピュータ犯罪の国際連携
- 論点
  - 犯罪を防止するため，不正アクセスを禁止するということ
  - 対象計算機を限定
  - アクセスコントロール，不正アクセスの定義
  - 対象計算機の利用者の義務

警察庁の不正アクセス法案 (98・11・17)

- 趣旨
  - 犯罪の防止を目的として不正アクセスを禁止
- 対象となる電子計算機の条件
  - 事業の用に供されている
  - 公衆回線接続されている
  - 利用者識別情報等(ID・パスワード)により利用者を制限する措置(アクセスコントロール)を講じているもの
- 不正アクセスは
  - 他人のID・パスワードを冒用する行為
  - システムのセキュリティのホールを攻撃する行為
  - ☛ 反復・継続して不正アクセスを行った場合等については罰則を加重

つづき

- 不正アクセスを助長する行為の禁止
  - 電子計算機に係る他人の利用者識別情報等を無断で提供する行為 (ID屋等) の禁止
  - 上記行為の中止等を命ずることができ，命令に違反する場合は罰則
- 対象となる計算機使用者の義務
  - パスワードの適切な管理，アクセス・コントロールの高度化などの不正アクセスの防止策を講じる
  - アクセスログを取り，3ヵ月の保存
  - 不正アクセスを知った場合，公安委員会に届ける
- 不正アクセスを防止するための民間活動の援助
  - 防止するための情報提供などの援助を行う
  - 必要な事例分析事務を専門家に委託できる

■不正アクセスの手口

不正アクセスの例

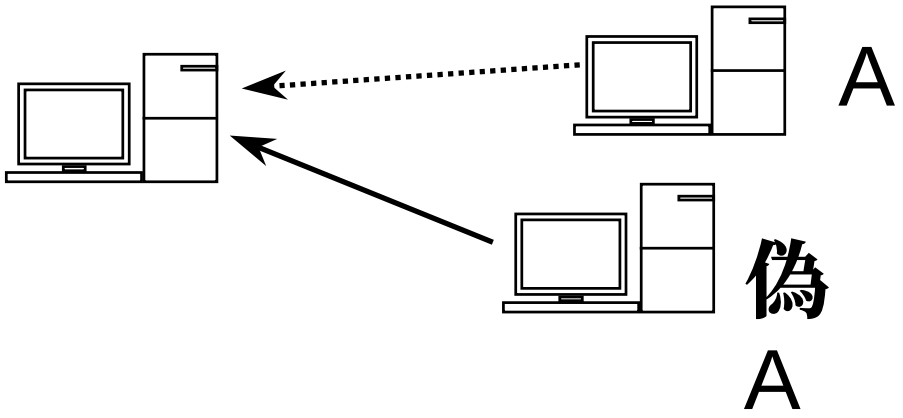
- IPパケット偽造によるなりすまし
- 制御パケットの偽造による運用妨害
- ネットワーク盗聴
- WWWサーバの情報改ざん
- 通信の乗っ取り
- セキュリティホール(脆弱性)の利用
- 電子メイル攻撃，電子メイル偽造
- システム侵入

セキュリティホールの利用

- セキュリティホール
  - プログラムの誤りによる侵入経路
    - 論理ミス (条件もれ, 境界条件, 競合条件)
    - バッファあふれ
    - 隠し機能
  - 設定の誤りによる侵入経路
    - 設定ファイル, 設定パラメータ
- プログラム
  - OS— システムコール, NFS,
  - 各種アプリケーション — statd, named, sendmail,
  - 通信プロトコル — long IP パケット, SYN攻撃

なりすまし

- 第3者のふりをして侵入やメッセージ発信
  - パスワード入手・推測
  - IPアドレス偽造
  - メイルアドレスの偽造
- 対策
  - 認証の強化，アクセス経路の制限
  - 利用履歴の確認

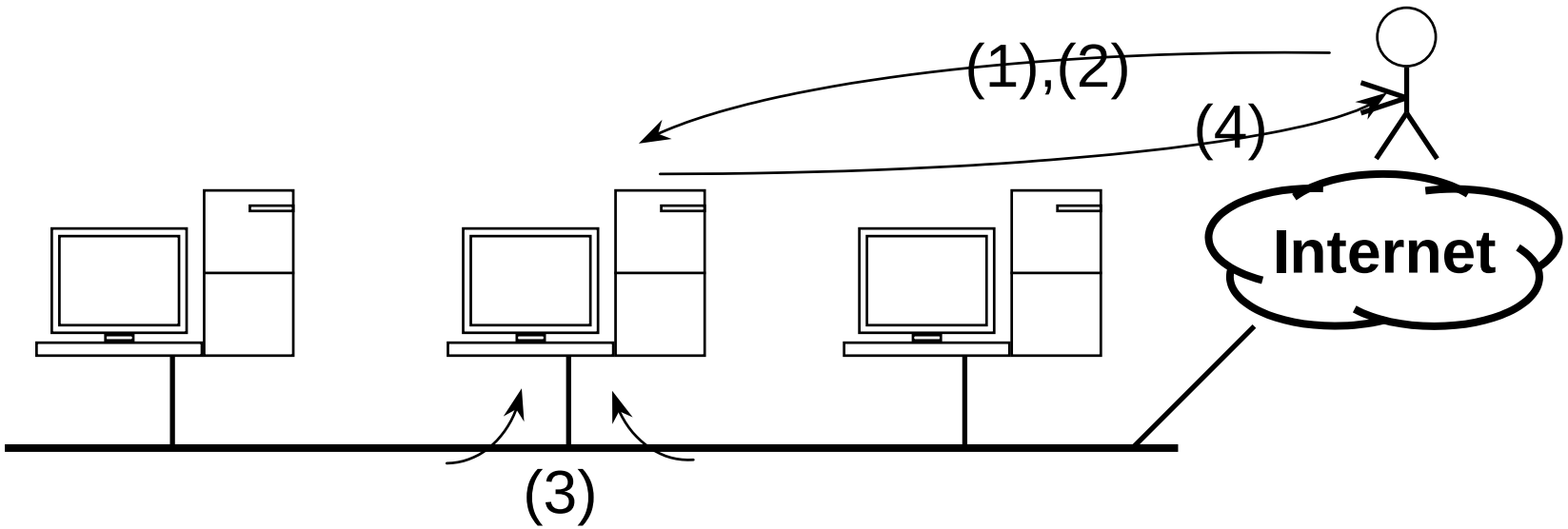


盗聴・コネクションハイジャック

- 盗聴
  - ネットワークの盗聴・モニタリング
  - ワークファイル，ディスクの残がい
- コネクションハイジャック
  - TCPセッションの横取り

スニーファ攻撃

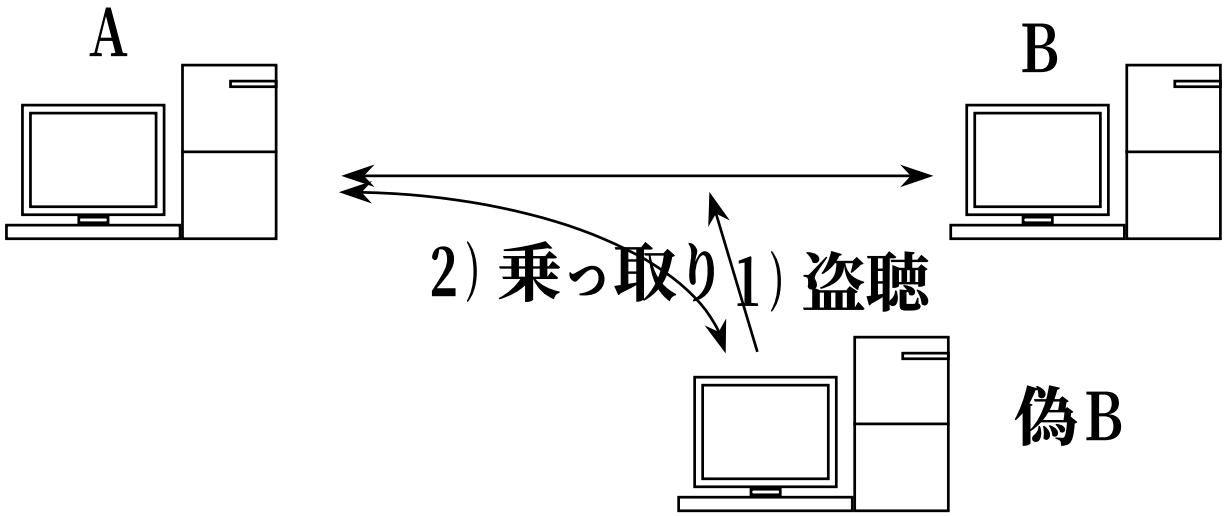
① 組織内ノードに侵入
② ネットワーク監視プログラムをインストール
③ 通信情報からログイン名とパスワードを抽出
④ 侵入者に転送



InternetWeek 98, Internet Security, S.Sano, 1998

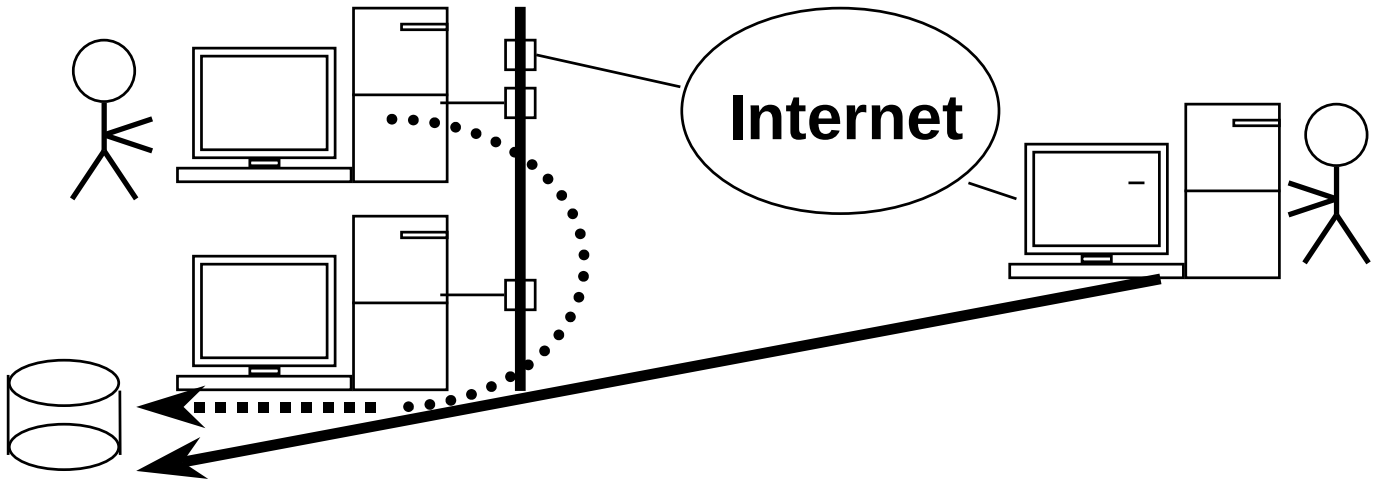
コネクションハイジャック

- 第3者が通信をのっとる
  - 認証完了後に確立した(論理的)通信路を乗っ取り，通信相手のふりをする



NFSの利用

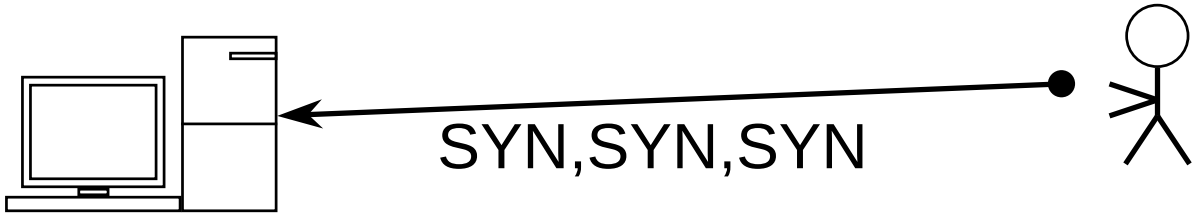
- NFS(ネットワークファイルシステム)
  - 本来ローカルエリアネットワークを前提に設計
  - 高速性, 信頼できるコンピュータ
- 不要に外から利用できると, 不正アクセスへ



InternetWeek 98, Internet Security, S.Sano, 1998

サービス妨害攻撃

- 不正なパケットを偽造してシステムの正常なシステムの運用を妨害
  - 異常に長いIPパケット (OSのバグ)
    - 通常のコマンドで生成可能
  - 制御パケット (SYN) の偽造 (プロトコルの問題)
    - 偽造コマンドが雑誌に公開
  - アプリケーションプログラムへの執拗な要求
    - (例) メール爆弾

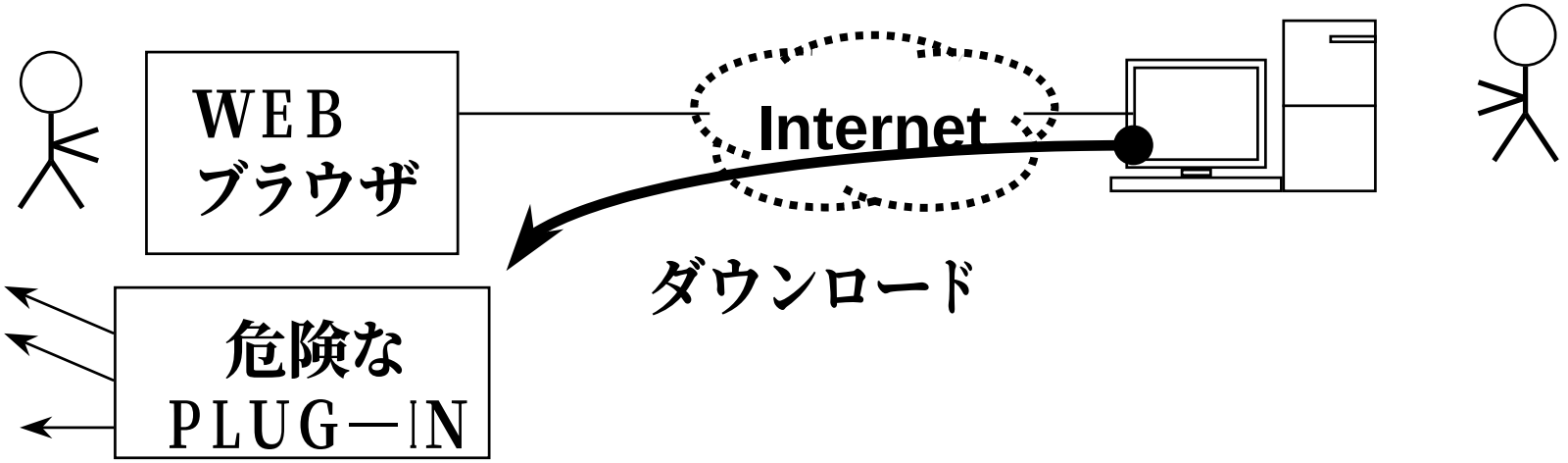


WEBの内容改ざん

- WEBサーバに侵入して内容を改ざん
  - インパクトのある不正アクセス
- 侵入方法
  - 通常のホストへの侵入
  - WWWサーバの設定上の問題を利用
    - CGI(Common Gateway Interface)プログラムの穴

WEBブラウザ

- 危ない plug-in コマンドをダウンロードさせる
  - ユーザが実行
  - JAVA, ActiveX, . . .



ソーシャルエンジニアリング・アタック

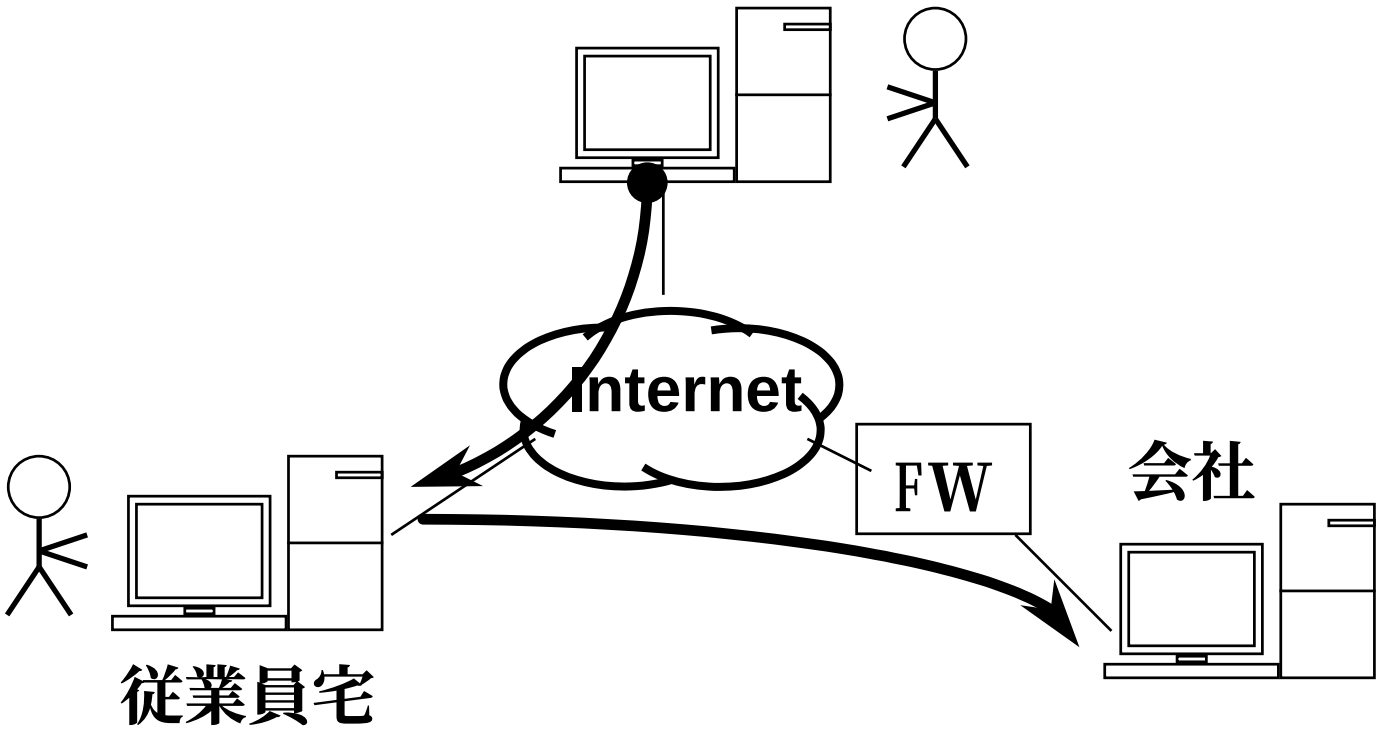
- 利用者・運用者をだます
  - ファイルをメイルで送って欲しい
  - パスワードを忘れた
  - 緊急にアカウントが欲しい
  - 私はXXXだ.

踏台

- 第3者を経由してシステムに侵入
  - ウィークパス … 制限の弱いホスト，ネットワークを経由
  - 侵入元，侵入経路を特定しにくくする
- 知らない間に加害者に加担
  - 弱いシステムは自分だけの問題ではない
- 対策
  - 踏台にあったシステムを一つずつ解消

踏み台の例

- 従業員の家のコンピュータを踏み台にして会社に侵入
  - この場合ファイアウオールは非力



InternetWeek 98, Internet Security, S.Sano, 1998

セキュリティ　ポリシ

- セキュリティポリシとは
- セキュリティポリシの策定
- セキュリティ施策
- インシデント対応

セキュリティポリシとは

セキュリテイ対策のサイクル

- ポリシ策定･見直し ← 要求, リスク予測, 最新技術状況
- 実施計画･見直し
- 実施
  - 技術的対策
  - 広報･教育･トレーニング
- 監査
  - 監視･検出 → インシデント対策

セキュリティポリシ

- 管理範囲(組織)内のコンピュータシステムのセキュリティに関する目的，方針，運用管理手順などを記述した文書
  - ＝セキュリティ施策に対する「基本仕様書」

- 類似の用語
  - 方針，指針，規定，規約，ルール
  - 計画，手順
  - ガイドライン，クライテリア，フレームワーク
  - アーキテクチャ

セキュリティポリシ

- 目的
  - 関係者での合意と情報の共有
  - 関係者の役割と責任の明確化
  - 実施計画のベース
  - 監査やレビューのレファレンス
- 組織によって異なる
  - 情報の価値の評価，リスクの予測
  - 管理体制の違い

セキュリティ対策の関係者と役割

- 組織内
  - ユーザ
  - ネットワーク管理者
  - 意志決定者
    - 組織の中間管理職
    - 情報管理部門
    - 経営者(情報や資源の所有者)
- 組織外部
  - コンサルタント，運用委託会社
  - プロバイダ，ベンダー
  - 緊急対応チーム
  - 警察

InternetWeek 98, Internet Security, S.Sano, 1998

合意が重要

- 経営者(意志決定者)の合意がないと
  - 権限の拠り所がなくなる
  - 実施が曖昧になる
  - 緊急時の判断が遅れる
- システム管理者の合意がないと
  - 実行不可能
- ユーザの合意がないと
  - 多くの抜け穴が発生

ポリシがないと

- 意志決定ができない
  - 機能，利便性の判断
  - セキュリティ対策の判断
- 施策の判断ができない
  - ツールの選択，設定ができない
  - なにをチェックするかわからない
  - どのようにアクセス制限するのかわからない
- 施策の妥当性が確認できない
- 関係者の合意がとれない
  - 共通の価値判断，リスク予測，目的が共有できない
  - 共通の理解が得られない
- 一貫性のないセキュリティ施策
  - コストアップ
  - リスク増加

InternetWeek 98, Internet Security, S.Sano, 1998

参考文献

- Site Security Handbook
  FYI8, RFC2196
  Sept, 1998
  Editor: B. Fraser, SEI/CMU
  - RFC1244の改定

- コンピュータ不正アクセス対策基準解説書
  日本情報処理開発発行

セキュリティポリシの策定

策定のポイント

- 基本アプローチ
  - 守る対象の候補の列挙
  - 守る対象の抽出･決定
  - 予期される脅威の列挙
  - 保護する手段の実施
  - レビュと改善
- 費用対効果の問題
  - 防御のコスト < 損害のリスク+復旧のコスト
    - 実際の通貨価値に基づく損失
    - 評判、信用、他の無形の損失

対象を見誤ると無駄

- 守るべき対象は?
- なにから守るか?
- どのように守るか?
- 必要以上のコストをかけていないか?
- 脅威のリスクの見積りがすくなすぎないか?

まもるべき対象の特定

- まもるべき対象はなにか
  - 機密情報
  - 価値のある情報
  - 知的財産権のある情報
  - ハードウエア
  - バックアップメディア
  - サプライ品(紙, 磁気メディア)
  - その他セキュリティ問題によって影響をうけるもの
- すべてを列挙することが重要
  - その中から取捨選択
  - 組織によって異なる

脅威とリスクの推定

- 資産への脅威を明確にする
  - 資源、情報への不正アクセス
  - 意図しない、不正な情報の公開
  - 情報の改ざん
  - 破壊
  - CPU資源の利用
  - 踏台
  - サービス妨害

  →どのような脅威から資産を守ろうとしているのか
- 具体的な損失の可能性を予測

目標設定 - 相反する要素のトレードオフで決定

- サービスの提供 対 セキュリティ -
  - サービスの提供によるリスク
  - セキュリティ対策の実施
- 操作性 対 セキュリティ
  - パスワードなし操作性の良いシステム
  - 高度なパスワード対策, 操作性はおちるが安全性は向上

目標設定 — 投資対効果

- セキュリティ対策のコスト
  - 経済的コスト(機材やソフトウエアの購入，オペレーションコスト)
  - 性能の低下(暗号，復号化のオーバヘッド)
  - サービスの制限，操作性の低下
- リスク
  - 機密情報の流出
  - 法律的損失
  - プライバシーの侵害
  - データの喪失
  - サービスが不能に
  - 信頼の低下

InternetWeek 98, Internet Security, S.Sano, 1998

ポリシの必要条件

- 文書として表明可能
- 実現可能
- ユーザ、管理者、経営管理者の責任の範囲の明確な定義
- 関係者のレビューと合意・理解
- 専門家(技術者，弁護士など)のレビュー
- 柔軟性
- ポリシの定期的なメンテナンスの手順

ポリシの項目

- 新技術や機器導入のポリシ
- プライバシー ポリシー
- 資源へのアクセスポリシー
- 責任のポリシー
- 認証のポリシ
- アベーラビリティの表明
- 保守のポリシ
- 運用者の権限
- 違反の報告のポリシー
- サポートのポリシ

ポリシの柔軟性の確保

- コンセプトと実現方法や環境との分離
  - 変更の容易さ
- 更新方式の文書化
  - 手続き
  - 参画する人
- 例外の明確化
  - 一般原則での例外

セキュリティ施策

セキュリティ施策の設計

- ポリシに基づいて，具体的な計画を立案
  - システムの構成
  - サービスの選別
  - システム基盤のセキュリティ施策
  - サービスごとのセキュリティ施策
  - 履歴の記録・管理保存
  - 異常検出方式，手順
  - トレーニング

システム構成

- ネットワークの構成
- マシン配置，各サービスの分担
- セキュリティ区分とネットワークトポロジの一致
  - ファイアウオール
  - 区画間のフィルタリング

サービスの選別

- 本当に必要なサービスを選別
  - サービスが増えるとセキュリティの複雑さは指数的に増加
  - デフォルトオフ (deny all) の考え方が重要
- どこで提供するか
- 利用者はだれか
- どのようにアクセスするのか
- 担当する管理者は?

セキュリティ施策

- 基盤
  - ルータ，ネットワーク，基本サーバの保護
  - 盗聴や妨害に対する対応
- サービス
  - 各サービスごとに施策を策定
  - アクセスコントロールの方式と設定
  - 認証の方式は
  - 機密保護の方式は，設定は
  - 改ざん防止の方式は，設定は

履歴(ログ)の記録保存

- 利用履歴
  - システムログ, アカウンティング情報, コンソールメッセージ
- 例えば
  - ログインとログアウト
  - スーパー ユーザー アクセス
  - 重要なシステムの変更
  - 重要なサービス処理の記録
  - 許可されない処理の要求の記録
- 目的
  - 不正アクセスの調査, 検出
  - 不正アクセスの証拠

履歴保存の問題

- 安全なところへ
  - 破壊されない
  - 流出しない
  - ログの停止が難しいところ
- 緊急時にアクセスできるところ
- 保存場所
  - ローカルホストのファイル
  - リモートホストのファイル
  - 追記型のデバイスに記録
  - ラインプリンタ

  → 重要なものであれば複数の方式を組み合わせる

バックアップ

- 目的
  - インシデント後の回復のため
  - インシデント解析のため
- ポイント
  - インシデント前のバックアップの確保がポイント
    - 履歴保存
  - バックアップメディアの管理
  - バックアップメディアの改ざん防止

履歴保存，バックアップメディアの注意

- 問題点
  - 保存期間
  - レベル
  - プライバシ
- メディアの不正アクセス
  - 盗難
  - 書き換え
  - 改ざん

→ 厳重な保存が必要

トレーニング

- トレーニングの必要性
  - セキュリティ動向は変化が激しい
  - 「ユーザ」が最大のセキュリティホールである
- 全てのユーザをトレーニングする
  - 一般ユーザ
  - システム管理者
- 最新のトレーニングを受ける
  - 繰り返して受ける
  - 試験も:-)

トレーニング内容

- 一般ユーザ向け
  - セキュリティポリシの徹底
  - ユーザの責任とは
  - 個人情報におけるセキュリティ上の脅威とリスク
  - 正しいコンピュータの使い方
- 管理者向け
  - セキュリティポリシの徹底
  - システム管理者の責任
  - システム運用におけるセキュリティ上の脅威とリスク
  - 最新のセキュリティ技術

インシデント対応

インシデントの対処

- 不正アクセス発生時の手順を事前に計画
  - その場では速やかな決断が必要
  - 決断の失敗が大きな損失をうむ可能性
  - 決断するプロセス(=決定者)の明確化
- 想定される事態に対して
  - それぞれの判断方針と手順を策定
  - 対策に必要な事前の対策，準備
  - 必要なら予行演習も

決断のポイント

- 想定される個々の事象に対して
  - サービスを止めるか，継続させるか
  - 解析を優先させるか，回復を優先させるか
  - だれに連絡し，どう連係するか
  - 事実を公開するか，秘密にするか
- 被害の最小化
  - 顧客対策
  - 経済的な損失
  - マスコミ対策
  - 法律的対策
  - 被害を受けた関連サイトへの法律的責任

インシデント対策に関連するポリシの項目

- インシデントに対処する際の目的と目標事項
- インシデント発生時の通知先，通知方法
  - 連絡網，連絡手段(24時間356日)
  - システム管理者，担当者
  - 法執行機関と調査機関
  - コンピュータ セキュリティ インシデント対処チーム
  - 被害を受けた関連サイト
  - ベンダ，プロバイダ
  - 内部のコミュニケーション
  - 報道機関

(つづき)

- インシデント判定手順
  - 判定方法, 判定基準
  - 種類の特定
  - インシデントの影響とダメージを評価(推定)
  - その後の対策方針の決め方

(つづき)

- 対処手順
  - 関係者への連絡･通知
  - 証拠とログの保存ー破壊からの防止，証拠能力の維持
  - システムの隔離，被害の拡大防止
  - 問題解決 ― 原因の究明と解決
  - システム回復
  - フォローアップ
- インシデント対策後の対応
  - 見直し

インシデントの判定

- 兆候
  - システム クラッシュ
  - システムの再起動
  - メッセージログ，コンソールに異常が記録
  - 性能の低下
  - 知らない新規ユーザーアカウントができている
  - 知らないファイルができている，ファイルがなくなっている
  - アカウンティング情報やシステムログの不整合
  - ファイル長や更新日付の変化
  - ログインできなくなった
  - 標準のコマンドがなくなった，所定の動作をしなくなった
  - :

InternetWeek 98, Internet Security, S.Sano, 1998

CERTのチェックリスト

1) ログファイルの確認
2) setuid, setgid付きファイルの不正作成を確認
3) システムバイナリファイルの不正変更の確認
4) ネットワーク監視プログラムの不正利用の確認
5) cronやatで実行されるプログラムの確認
6) 不正なサーバの不正な追加を確認
7) パスワードファイルの調査
8)ネットワーク設定ファイルの不正変更を確認
9) 隠れファイルの作成を確認
10) さらに関連するLAN上の計算機も確認

方針の決定

- ダメージと影響範囲の評価，対策の方針を決定
  - 事前の計画と専門家の判断が重要
  - 対策に必要な時間の算定
- トレードオフの判断，具体的な方針の決定
  - 回復 vs 解析
  - サービス停止時間
  - 守るべき情報は
  - 外部との関係
  - ：

優先度の指針を策定

たとえば

⑴ 人命と人の安全を守る
⑵ 機密情報を守る
⑶ 顧客情報を守る
⑷ 他のサイトへの延焼を守る
⑸ 知的財産, 経営情報 などの情報を守る
⑹ システムのダメージ(破壊や書き換え)を防ぐ
⑺ システムの正常な運用を維持する

問題解決 — 原因の究明と解決

- 弱点の除去
  - 同じ設定は同じ結果をまねく
- 手口がわかった場合
  - 他の弱点はないかの検討が重要
- 手口がわからない場合
  - 推定して対策
  - 部分的停止
  - ログの強化によるトラップ

システム回復

- 方針
  - 一時的に全サービスを停止するか?
  - 部分的な回復を試みならがサービスを継続させるか?
- 被害や手口が明確な場合
  - その部分の対応
- そうでない場合
  - 最悪の常態を想定する必要も
  - システムの再インストールが重要
    - バックアップが鍵

報道機関対策

- 発表のルート
  - 広報担当者の活用
    - 報道機関や記者の選択，適切な対応を期待
  - タイミング
    - 検出直後?
    - 対策中?
    - 対策完了後?
- 内容
  (1) 詳細についての技術的なレベルは低く
  (2) 推測を含めない
  (3) 証拠能力が守られること
- 報道機関の論理に振り回されない

InternetWeek 98, Internet Security, S.Sano, 1998

内部犯の場合

- エンドユーザ
  - 権限を制限
  - 他の不正の可能性
  - 上司，人事勤労部門との連係
- システム管理者
  - システム全体を見直しが必要
- 元従業員
  - 以前の権限を調査し停止
  - その権限でできる事項を調査
  - モデム電話番号
  - 法律的な対応

事後

- フォローアップ
  - インシデント対応手順と対策の再確認と評価，分析
  - リスク，コストの算定
  - 必要な対応がとれたことの確認
  - 同じ侵入が再発していないことの確認
  - 報告書の作成
- 対策後
  - 再発防止
  - 法律的対応
  - リスクアセスメントの再定義
  - ポリシの見直し

継続すべき活動

- IRTからのアドバイザリ情報の調査と適用
- ベンダからのセキュリティ情報(ex パッチ)の調査と適用
- システムの設定・変更情報の監視と個別の対応
- 最新技術情報の入手と関係者での技術共有
  - メイリングリスト
  - WWW
  - 雑誌
  - :
- 定期的にポリシと手続きの遵守状況の第3者によるチェック
- 定期的なポリシーと手続きのレビューと見直し

最後に

最後に

- 関係者を巻き込んで合意を取る試みを
  - 意識と問題点の共通理解が重要
  - 責任の分担が必要
    - 情報管理･経営的重大事の判断は技術者の役割？
    - ユーザへの自己責任の意識を
  - 結果を文書すなわち，セキュリティポリシの作成へ
    - 最初から完全を狙わないで，できるところから

- 一貫性を意識せよ
  - 無駄な努力はしていないか
  - 「穴」はないか

  →レファレンスが必要

(つづき)

- インシデントのイメージトレーニングを
  - 完全な防御は無理
  - できれば手順書を
- よいアドバイザを確保
  - 技術者
  - 法律専門家
- 勉強しましょう

おわり