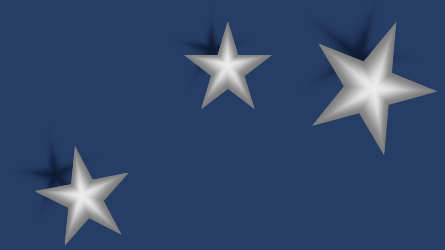
情報処理システム論 (16)

オープンネットワークの時代

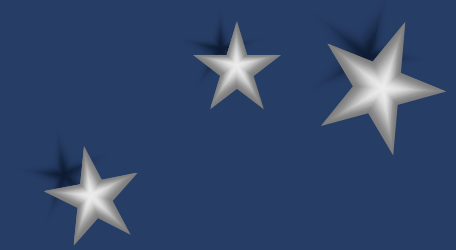
- だれもが自由にアクセス可能
- セキュリティの考慮が必要

- 銀行などの閉じた独自ネットワークとはちがう



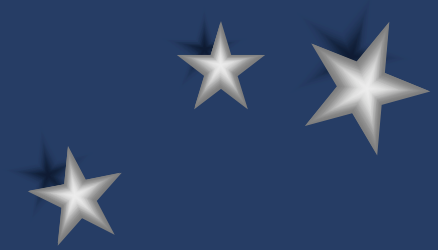
ネットワークのセキュリティ

- 不正侵入 (Cracker) の阻止
- 情報の秘密を守る
  - 暗号化
- ホストや個人の認証
  - デジタル署名
  - オンライン取り引きへの応用
  - アクセス制御や課金にも利用
- コンピュータ・ウィルス / ワームの排除
- 利用者の信頼性



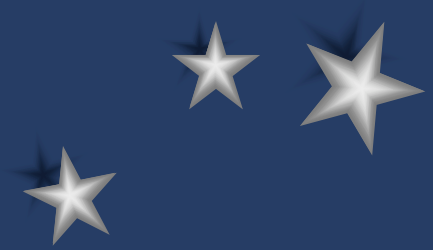
主な事件

- 1988: Internet Worm
  - インターネット上の7000以上のホストが被害
- 1989: カッコウの卵
- 1993: N.Y.City Internet 侵入
- 1995: ミトニック (テイクダウン)
- 1996: Word Macro Virus



不正の種類

- 情報の破壊
  - データの消去、システムの破壊
- 情報の漏洩 (盗聴)
  - パスワード、機密情報
- 情報の改変
  - 改竄、なりすまし
- 利用不能攻撃
- 資源の不正使用
  - ディスク領域、CPU 時間



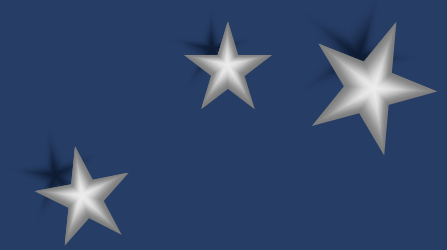
悪質プログラム

- ウィルス
  - 感染と破壊
- バクテリア
  - 自己増殖
- ワーム
  - ネットワーク自己複製
- 落とし戸
  - 秘密の入り口
- ロジック爆弾
  - 時限起動
- トロイの木馬
  - 他のプログラムに紛れ込ませる

不正侵入の糸口

- メールサーバ (sendmail) の穴
- WWWサーバの穴
- 無名ホストでも安心はできない
  - 絨毯探索（ローラー作戦）

- 踏み台としての利用
  - 追跡を困難にする
- 裏の情報網



パスワードの入手

- パスワード・クラック
  - 暗号化されたパスワードの入手
    - サーバの誤設定をつく
    - 総当たり作戦による解読
  - 類推と試行錯誤
    - 「War Game」
- ネットワーク・モニタリング
  - telnet や POP は危険
- 偽装ログインプログラムの利用
  - Windows NT は Ctl-Alt-Del で対策

悪いパスワード

- 短い (6文字程度だと全数チェックが簡単)
- 辞書に載ってる
- その人から連想できる事柄
- 有名人 (アイドル) の名前
- 簡単なバリエーション
  - 繰り返し、逆転、capitalize

  → 必ず記号や数字を混ぜる
- 紙に書いてある！

使い捨てパスワード

- リプレイ・アタック (再利用攻撃)の防止
- 毎回異なるパスワードを用いる
  - 同期型
    - 時間やカウンタなどから計算する
  - Challenge/Response 型
    - サーバから送られる種を元に計算する
      - PPP の CHAP, APOP
- 専用カード (ハード)
- ノートパソコン(ソフト)

使い捨てパスワード専用カード

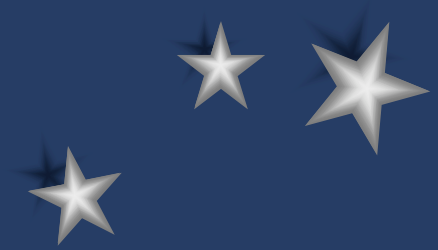
SecurID

SafeWord

進んだパスワード交換方式

- **公開鍵暗号方式の利用**
  - SSH (Secure Shell)
  - PET (Privacy Enhanced Telnet)
  - SSL Telnet (Secure Socket Layer)

- **VPN で全体的に暗号化**
  - IP Sec



ホスト認証

- **IPアドレスの信頼性**
  - IP Spoofing Attack
  - アドレス認証だけでは信頼できない
- **ホスト名の信頼性**
  - IP アドレスとの対応づけ
  - ネームサーバのセキュリティに依存

サポートとソース・コード

- サポートが買えることが信頼性につながるか
  - サポートの遅れ
  - 不誠実なサポート
- ソースコードの公開の是非
  - 問題発見が早い
    - 解決のため
    - 悪用のため
  - 自力で解決できる
    - だれかが解決してくれる（普及したソフト）

防御のコスト

セキュリティ × 使い易さ ＝ コスト(技術)

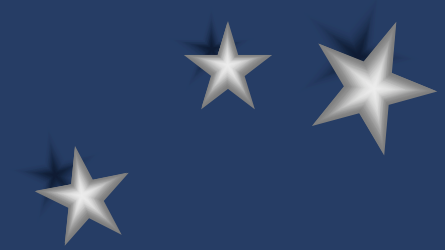
- 何を守るか
  - 情報
  - 機密
  - 復旧コスト
- 何から守るか
  - 外部
  - 内部

セキュリティ向上のための努力

- こまめな情報の入手
- すばやい対策
- 新しい技術の導入
  - ファイアウォル
    - 1個所で守る
- ユーザ教育
  - パスワードを破られないように
- ログ (記録) を採る
  - 不正なアクセスの監視と排除

暗号方式 (次回)

- 共有鍵方式
- 公開鍵方式
- デジタル署名
  - 1方向関数 (落とし戸関数)
- ブラインド・署名



参考文献

- カッコウはコンピュータに卵を産む
  - クリフォード・ストール
- テイクダウン
  - 下村努 / ジョン・マーコフ
- セキュア・コマース
  - Vijay Ahuja / 小野哲男 監訳
  - HBJ出版局、ISBN 4-8337-4733-2