情報処理の概念

#11 システムと通信の安全性 / 2002 (秋)

一般教育研究センター 安田豊

セキュリティ問題

- システムの安全性
  - いかにして確保するか
- 二つの安全性
  - 通信上の安全性
  - 内部処理システムの安全性
- 両者を分けて考えよ

システムの安全性

- 二つの安全性
- 内部の処理システムの安全性
  - 記録されるデータを第三者に渡さない
  - システムを止めない
- 通信の安全性
  - 流れるデータを第三者に見せない
  - 通信が切れない
- 技術的には両者は別のもの
  - むやみに危険と言ってみても何の役にも立たない
  - まずは理解することから

内部処理システムの安全性

- まずはハードウェア確保
  - 耐震性、耐火性
  - バックアップ、冗長性
  - 入室管理、なりすまし（いわゆる社会工学）
- それでも起きる
  - 社員による内部犯行もある

クラッカーが大手企業システムに侵入、セコムネットら10社から入札情報、社員個人情報が流出、情報を売買か？(1998)

ポイント

- 社内の人間による内部システムの不正利用は以前からある
  - なくならないし、問題ではあるが今回はとりあげない。（そもそもコンピュータを使わないシステムでの不正と本質的に同じ）
- このクラスでは
  - ネットワーク越しの不正利用に注目

内部処理システムの安全性

- システム不正侵入
  - 昨今は「不正アクセス」と呼ばれる事が多い
  - 不正アクセス行為の禁止等に関する法律 2000年2月施行
- 一般に、
  - オープンネットに接続されたシステムの、
  - ソフトウェアの不備(バグ)を入り口として、
  - 相手のシステムに自分のやらせたい処理をさせる
- インターネット接続システムが増えた
  - 不用意にバグをさらしているシステムも増えた
  - 大学なども多く侵入されている

システム不正侵入

- 原理的には
  - オープンネットにつながない事で止められる場合もあるが、、
  - 残念ながら、ソフトウェアの不備はなくならない
- 技術武装しかない
  - 防御、侵入検知など多方面で備える
  - いたちごっこになる
- それにしても現在のシステムは脆弱すぎ
  - オープンな文化で育った Unix / Internet の弱さ

システムダウン

- DDoS 攻撃
  - 資料
  - 現在では日常的に行われるようになった
  - 「週に4000回以上」2001.5 カリフォルニア大学
  - script kiddy による安直な攻撃
- システム侵入されたマシンが踏み台に
  - Worm などの自動侵入も増えている

通信の原理

- 通信とは
  - システム間のデータ受け渡し方法の一つ
  - 電気や光の信号によって受け渡す
  - データ化ルールを送受信者間で共有
- 通信の安全性とは
  - 通信路（線路）を流れるデータの内容 (情報) を第三者に渡さない（漏らさない）
  - 閉鎖された通信路での対策は比較的簡単
  - インターネットのようなオープンネットでは困難
  - 例： Web でクレジットカード番号を入力

傍受

- 通信の傍受は技術的には多くの場合可能
  - 傍受そのものは犯罪ではない場合が多い（例：国内の無線）
- デジタル情報である限り複製が可能
- 複製してもオリジナルに改変を与えない
  - 複製されたことが判らない
  - 複製とオリジナルは完全に同一
    - つまり複製、オリジナルという概念そのものがない
- 傍受を防ぐことができない

暗号

- では暗号化で対策
  - 傍受されても中身が判らないようにする
- 暗号
  - 通信では符号化するシステムと復号するシステムが異なる
  - 当事者以外に復号できなくする
  - 復号ルール（の一部）を秘密にする
  - データは読めるが、当事者以外には中身がわからない

暗号

- 通信に関わる脅威
  - 秘密情報の取得だけではない
  - なりすましや改竄など
- 現時点では暗号技術の応用で対応
  - 公開鍵暗号技術
  - 誰もが公開鍵で暗号化でき、彼だけが秘密鍵で解読できる
  - 彼だけが秘密鍵で暗号化でき、誰もが公開鍵で検証(復号)できる
- 認証局・電子署名

暗号

- 利用例
  - SSL : ほとんどの Web 取引で利用
  - 電子署名 (電子署名・認証法 2001.4.1 施行)
- 問題点
  - 法規制の対象
  - 国によっては暗号は兵器と見なされる（た）
  - 数学的強さと計算量問題「期限付きの鍵」
  - ICカードで処理できる鍵＝弱い鍵
- それでも普及は間違いない

安全性

- 安全性とは何か？
  - 道で撃たれないのはヨロイを着ているから？
  - 総合的なリスクコントロールが重要
    - 法律・摘発・罰則・保険など （教育も重要）
    - 全て合わせてモータリゼーションを支える
    - コンピュータとネット化された社会でも同様
  - 道路にセキュリティシステムはない
    - 現金輸送車はそれなりにガードされている
    - それは常識である（今は常識もない）

エシュロン

- 受信基地、衛星を用いた民間通信傍受網
  - 電話、FAX、電子メイル対象
  - 米国主導で英、豪、カナダ、ニュージーランド
  - 参加国は入手した情報を共有
- 産業スパイの防止
  - すでにテレビ会議などを国際通信網で利用している会社は少なくない
  - CIAは関与を否定
- 個人情報の監視そのものがEU規約の人権侵害
  - EU加盟国の参加は規約違反

エシュロン

- 欧州議会は調査委員会を設置
  - その存在を断定
  - 米国に対して欧州人権規約を尊重するよう要請するべきと結論
- 米国は公式には認めず
- 個人の通信暗号化を示唆
  - 暗号通信システムの商品化などが進むか
- ネットや技術は個人や企業を対等な立場に
  - 問題もまた対等に、個人に突きつけられる