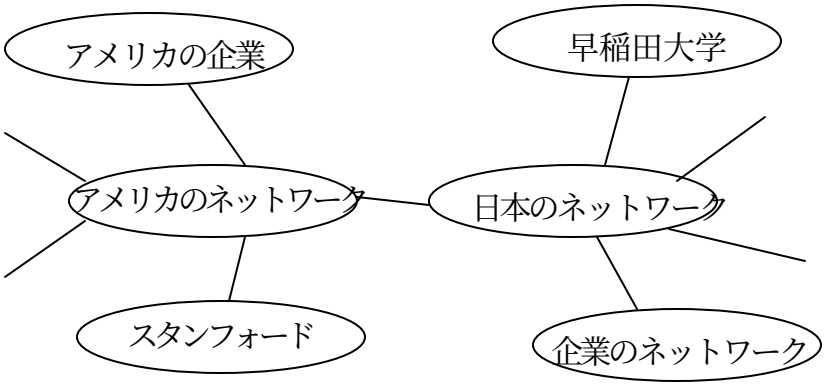
セキュリティとインターネット

中島　達夫

インターネットとは?

世界中がつながっていく



インターネットで何ができる?

- 情報収集，電子メイル，i-mode.…
- インターネット放送
- インターネット電話

→ 世界中の誰とでもコミュニケーション

→ 世界中の情報にアクセス

→ 世界中の機器を制御

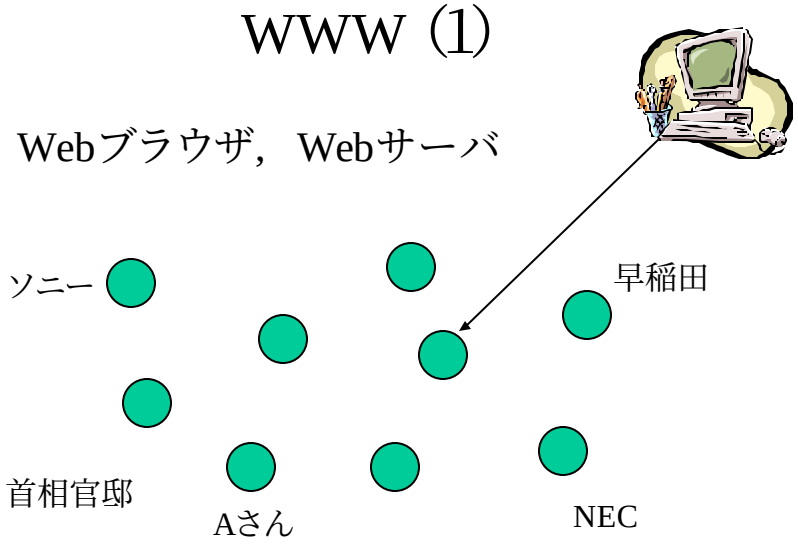
インターネットは便利なツール

- 研究者として
  - 電子メイル – 海外の人とも簡単にコミュニケーション
  - インターネット放送 – 海外での講演をインターネットで
  - WWW – 論文の収集

→ 様々な情報が増えている.

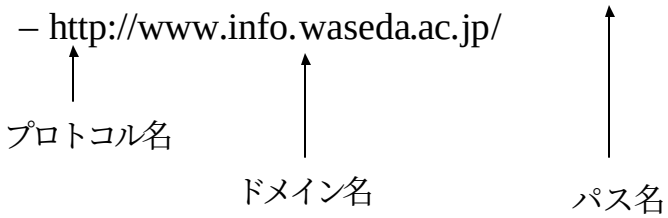
WWW (1)

- Webブラウザ，Webサーバ



WWW (2)

- URL(Uniform Resource Locator)
  - protocol://domain name/path name
  - http://www.dcl.info.waseda.ac.jp/tatsuo/
  - http://www.info.waseda.ac.jp/



情報検索

- Google
  - キーワードでの検索
  - http://www.google.co.jp/
- Yahoo
  - カテゴリによる検索
  - http://www.yahoo.co.jp/

実際に検索してみよう

- ANAのホームページを探して羽田から千歳行きの便の時間を調べる.
- セキュリティに関する国際会議とその開催地をしらべる
- ドイツのベルリンにあるホテルを捜す
- Javaに関する本を探す
- 村岡洋一先生の最近の動向を調査する.

インターネットとセキュリティ

- インターネット上にあらゆる情報が蓄えられる.
- 個人情報など機密情報がすべての人に知られないようにする必要がある.

  → セキュリティ

  → 情報学科のすべての学生はセキュリティに関する基礎知識を持っているべき.

セキュリティ

- セキュリティとは?
- どのくらい危ないのか?
  - パスワードの盗難
  - telnetのパスワード
  - ウイルス
  - 成りすまし
    - メイルシステム，ファイルサーバ
  - ファイヤウォールの必要性
- 暗号化: 公開鍵暗号

セキュリティとは?

- 機密性（Confidentiality)
  - 人に知られないようにする.
- データ保全性 (Data　Integrity)
  - 誰かにデータが変更されていないか?
- 可用性（Availability)
  - システムは利用可能か?
- 一貫性（Consistency)
  - システムは正しく動作しているか?

どのくらい危ないのか?

- 他人になりすまして悪意のメイルを送る
  - 中傷メイル，ウイルスなど.
  - ウイルス入りメイルを成りすましにより送ることにより システムが崩壊した場合だれが責任を取るのか?
- なりすましにより機密データを盗み出す.
  - パスワードが盗まれることにより機密データが盗まれた場合誰の責任か?
  - セキュリティの穴をつかれて業務が滞った場合，システム管理者は責任をとるのか?
- インターネットの便利さは危険さととなりあわせ
  - 危なさを知らないととんでもないことになるかも！

パスワードの盗難

- 簡単に他人に成りすますことができる.
  - 共有ファイルへのアクセス（機密へのアクセス)
  - なりすましによりメイルの送信
  - ファイルの消去，改変，作成
- パスワードは定期的に変更しないと総当りなどの手段を用い簡単に当てられる.

telnetのパスワード

- 遠隔ログインコマンド（telnet)はパスワードをプレーンテキストとして送る.
  - ネットワークモニタによりパスワードを盗むことが簡単にできる.
  - 従業員が家庭からtelnetによる会社の計算機のアクセスを許すとき，なにがおきるのか?
    - パスワードが盗まれ機密が漏れたとき，危険を考慮しなかったシステム管理者の責任は?

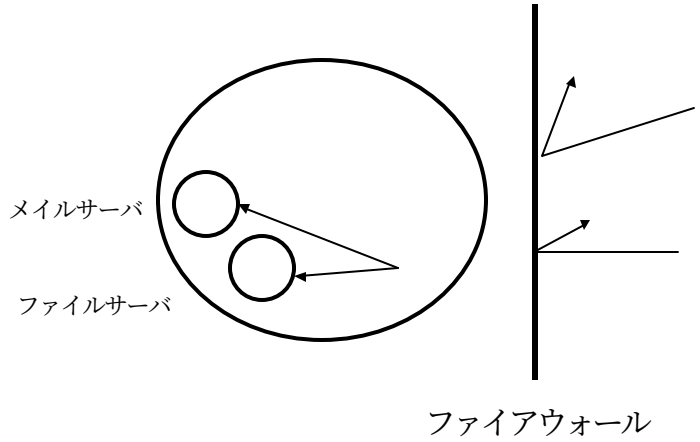
ウイルス

- メイルに添付されたウイルス
  - 添付ファイルを開くことによりアドレス帖に含まれる人全員にウイルス入りメイルを転送する.
  - 友人からのメイルと思い添付ファイルを開くとシステムがクラッシュする.
- ダウンロードされたファイルに含まれたウイルス
  - Webブラウザに含まれるウイルスはクレジットカード番号をメイルで送ってしまうかも知れない.
  - オープンソースを改変し，悪意のWebサーバからダウンロードさせることにより実現.

なりすまし

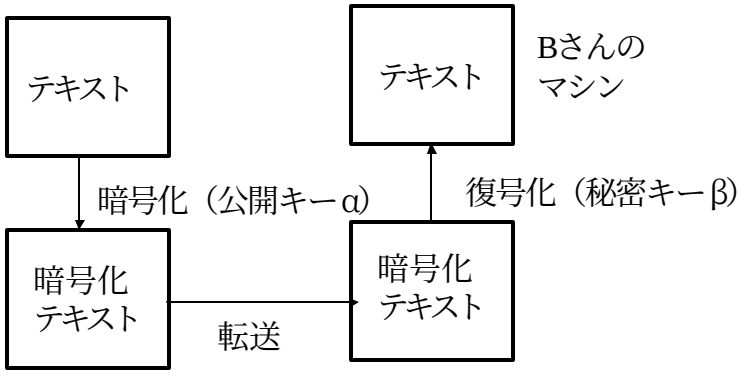
- ファイルシステム
  - NFSなどの分散ファイルシステムは簡単に他人になりすますことができる.
  - 共有ファイルのアクセス.
- メイルシステム
  - SMTPは簡単に他人に成りすましてメイルを送ることを可能とする.
  - 悪意のメイルの送信

ファイヤウォールの必要性



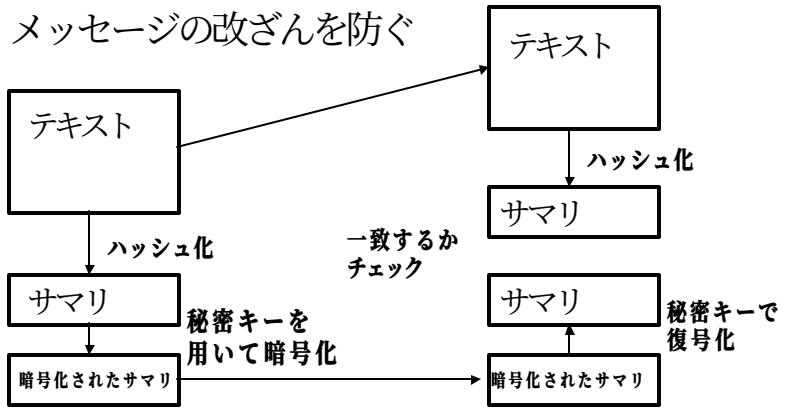
暗号アルゴリズム (1)

- 公開鍵方式



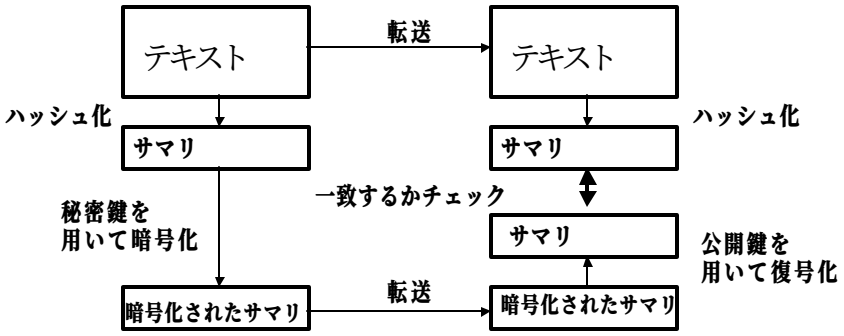
暗号アルゴリズム (2)

- ハッシュアルゴリズム
  - メッセージの改ざんを防ぐ



暗号化アルゴリズム (3)

- 公開鍵を用いた電子署名



X.509電子署名書 (1)

Data:
Version: 0
Serial Number: 02:41:00:00:01
Signature Algorithm: MD2 digest With RSA Encryption
Issuer: C=US, O=RSA Data Security, Inc.,
OU=Secure Server….
Validity:
Not Before: Wed Nov 9 15:54:17 1994
Not After: Fri Dec 31 15:54:17 1999
Subject: C=JP, O=Waseda University,
OU=Dept. Info. and Comp. Sci.
Subject Public Key Info:
Public Key Algorithm : RSA Encryption
Public Key:
Modules:
00:92:ce:…..…
Exponent: 65537 (0x10001)
Signature Algorithm: MD2 digest with RSA encryption
Signiture:
88:d1:d1:79…….

X.509電子署名書 (2)

特徴

- Issuerの証明書の公開鍵を用いて署名されている.
- 証明書がIssuerが発行した証明書であることが保証される.

問題点

- 保証機関はどこまで証明書の正当性を保証するのか?
- 最終的にはユーザがSubjectフィールドを見て正当性をチェックする必要がある.
- ベンチャーソフト会社を信用できるか?
- ActiveXコンポーネントなどのダウンロードの安全性は？

最後に

- セキュリティは1つの技術では実現できない.
  - セキュアネットワーク
  - セキュアOS
  - セキュアアプリケーション
  - オペレーション，社会的問題等
- 広い知識が重要である.