ネットワークセキュリティと暗号

郵政省 通信総合研究所 通信システム部 非常時通信研究室

大野浩之 (*hohno@ohnolab.org*)

ネットワークセキュリティと暗号

- ネットワークセキュリティを確保するためには，暗号技術は必須である．
- 暗号技術は，今後ますます必要となる．

暗号技術とインターネット

- SSL(Secure Socket Layer)/ TLS(Transport Layer Security: RFC2246)
- IPsec(RFC1826, 1827など)
- ssh(secure shell)
- PGP(Pretty Good Privacy: RFC1991)
- S/MIME(RFC2633)

暗号技術とインターネット

- SSL(Secure Socket Layer)/ TLS(Transport Layer Security: RFC2246)
  - 主にWWWのセキュリティ確保
    - Netscape Navigator/Communicator
    - Internet Exploer
  - サーバ側認証に公開鍵暗号方式
  - 公開鍵の配布にCAを用いる
  - 通信の暗号化に対称鍵暗号方式

暗号技術とインターネット

- IPsec(RFC1826，1827など)
  - VPN等ネットワーク層でのセキュリティ確保
    - 各種VPN製品
  - DH法による鍵交換
  - 計算機の認証に公開鍵が利用可能
  - 通信の暗号化に対称鍵暗号方式

暗号技術とインターネット

- ssh(secure shell)
  - リモートシェル(rsh)のセキュリティ確保
    - OpenSSH
    - TeraTermPro with TTSSH
  - リモート側計算機、ユーザの認証に公開鍵暗号方式
  - 通信の暗号化に対称鍵暗号方式

暗号技術とインターネット

- PGP(Pretty Good Privacy: RFC1991)
  - 電子メールのセキュリティ確保
    - Mew
    - EudoraPro
    - WinBiff...
  - ユーザの認証に公開鍵暗号方式
  - 公開鍵の配布方法は規定されていない
  - メール本体の暗号化に対称鍵暗号方式

暗号技術とインターネット

- S/MIME(RFC2633)
  - 電子メールのセキュリティ確保
    - Netscape Communicator
    - EudoraPro
    - WinBiff...
  - ユーザの認証に公開鍵暗号方式
  - 公開鍵の配布にCAを用いる事が前提条件
  - メール本体の暗号化に対称鍵暗号方式

これからのインターネットと暗号技術

- GPKI(Government Public Key Infrastructure)
  - 政府による公開鍵インフラの整備
- 著作権保護技術
  - 現状はさまざまな技術の提案がされている状態
- ISO15408
  - ITセキュリティ評価基準

これからのインターネットと暗号技術

- IPv6
  - IPsec標準装備
  - セキュリティ意識の向上が期待できる
- 無線LAN
  - IEEE 802.11 対称鍵方式
  - Bluetooth
- Smart Celluer Phone
  - WAP　... SSLサポート
  - i-mode ... SSLサポート予定

インターネット技術者/研究者からのコメント

- さまざまな研究が行なわれ，新しい暗号技術がぞくぞくと提供されていることはわかる．
- しかし，研究動向，各々の技術の特徴，利用方法，実装状況などを追いきれない．

暗号技術者/研究者からのコメント(予想)

- インターネット技術者/研究者の需要を必ずしも予測できていない?

*** 提案 ***

- お互いの「不満」を解消できるようにできないか.