暗号アルゴリズム移行問題

-- 認証局、証明書、電子署名からのアプローチ --

富士ゼロックス株式会社
システム要素技術研究所
稲田 龍
<Ryu.Inada@fujixerox.co.jp>

概要

- 標準化(IETF)のでは
- 認証局としての立場
- 証明書の立場
- 電子署名の利用に関しての立場

標準化(IETF)では

- アルゴリズム独立なプロトコルの定義が行われつつあるが……
  - 新プロトコルは問題は少ない
  - 旧プロトコルの大半はRSA/SHA-1が前提
    - 特にSHA-1べったりの実装が多く見られる
- IETFとはいえ、実装者の意見が少ない
  - 新しいプロトコルを定義する場だからすでに動かしているところは興味がない?
- 古いプロトコルでの運用の問題
  - すでに運用を行っているものをとめるのは困る
    - 脆弱であることがわかっているSSLv2もとめるのはかなり抵抗がある

認証局の立場

- アルゴリズム移行にあたり
  - 暗号･ハッシュのパラメータの設定
  - クライアントの対応
    - Windows Vista/IE 7などはサポートしている
      - FireFoxはどうだろう?
    - OpenSSLもサポートできるようだ
    - HTTPSサーバはどうだろう?
      - IISは出来そう。
      - Apacheも何とかなりそう。
  - 旧アルゴリズムと新アルゴリズムで認証局の連続性を保つべきか否か
    - アルゴリズムが違うとKey Rollover出来たっけ?

証明書の立場

- 利用するアルゴリズムの表現方法
  - OIDはどうなるのか?
  - パラメータは?
  - 認証局はどうなるか?

電子署名の立場

- 長期間にわたる署名の場合
  - 長期保存に関しては、規格上複数の署名できる枠組みがあるが……
    - 署名の連鎖にしても、過去の日付でFakeの署名をつけられたものを新たに新アルゴリズムで署名されたらどうなる?
- 短期間の署名の場合
  - 安全な(?)アルゴリズムをその時使えばよいが……問題は、安全なアルゴリズムを選択できるのか？
- 法的な問題
  - 電子署名法
    - DSA/RSAしか(現実的には)選択できないのでは?
  - e文書法
    - 現行法では最長10年の保存義務があるけど……

商標など

- Windows**はマイクロソフト株式会社の登録商標です。**
- RSA**は**RSA, The Security Division of EMC **登録商標です。**