「仏作って魂入れず」

～電子署名法とHSM～

暗号屋さんの目から署名法を見ると

- CRYPTREC事務局として
  - とりあえず、“SHA1withRSA1024”から”SHAXXXwithRSA2048“への移行パスは準備したぞ！
  - 作業終了

現在のHSMの位置づけ

- EE証明書への署名のみ！
- EE証明書の鍵対生成
  - HSMは使われていない。
    - 閉鎖環境
    - 大量発行

    } 鍵対生成の安全性に関して「NG」という訳ではない。
  - CAは、ST確認のみ。
    - ST確認は、「セキュリティ設計」の妥当性確認
    - 鍵対は、CSP（Cryptographic Service Provider)で生成
      - せめて、CAVP（Cryptographic Algorithm Validation Program)で確認は、必要。

HSM

- EE証明書への署名だけ？
  - CA局の「プライベート鍵」の保管庫？
    - 問題点は次葉
  - P12形式ファイルによる配布
    - 「事故」が起きなきゃいいけどね！
    - 暗号化してあります。まさかRC2-40じゃないよね？
      - 一応、EDE 3DESでした。
  - ICカード
    - ICカードも立派な「HSM」です。
    - CC評価とCMVP両方の評価が必要
    - マイナンバーカードの採用も考慮すべし
      - 「信頼感」の問題です
    - H8/300改やZ80改→処理能力の限界
      - そろそろ機種更新しては？

電子署名法(規則)の記述

- HSMに対する要件
  - 対象:認証局の署名生成目的のHSM
  - 電子署名法、施行規則、認定に係る指針には規定がない
  - 「調査の方針」に規定
    - 「調査の方針」→政省令未満の規定
    - (1)FIPS 140-1の抄訳
      - CRYPTRECで作成した訳
    - (2)国産のHSMに対する救済策

・時代遅れ
・国際規格/JIS規格を無視→WTO協定違反か？

提言

- 電子署名法の政省令は、技術的にはほとんど無力！
  - 改正すべき時期。
  - 手続きで守れるなら、技術はいらない！
- ICカードで守られた証明書とP12形式証明書
  - 「信頼感」は同程度？？
  - 証明書のランク付けが必要ではないか