JPNICにおける鍵管理
～ユーザにご利用頂くデータの品質管理～

社団法人日本ネットワークインフォメーションセンター
木村泰司

JPNICにおける「鍵管理」

- 認証局の話です
- オンラインです

運用
　6年4ヶ月目
発行数
　3657
ユーザ数（推定）
　1200
“鍵”が使われる頻度
　一日数件程度

2011年7月7日現在

指定事業者

資源申請者
証明書

クライアント認証

Web申請システム＆認証局システム

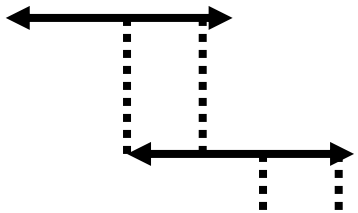
ここでいう“鍵”とは？

ユーザにご利用頂くもの		ユーザにご利用頂かないもの
署名されたデータ	公開鍵	公開鍵 私有鍵（秘密鍵）
例 署名レコード	KSK公開鍵 ZSK公開鍵	KSK公開鍵/私有鍵 ZSK公開鍵/私有鍵

鍵の設計

- 認証局の鍵
  - 鍵の用途　認証用証明書発行
  - サーバに置かない → HSM
  - キーセレモニー／バックアップ
- ライフサイクル
  - 10年（資源申請者証明書は2年）
  - キーロールオーバーを考えると10年間は使えない
- 鍵使用の承認と業務証跡
  - 紙面で記録
  - 担当部署を明記した手続き用紙
  - 一人ですべてはできない

用途	利用範囲
認証	限定
署名	流通



鍵の運用

- 記録
  - 活性化（起動）／非活性化（停止）
  - 鍵使用⇒証明書発行／失効
- 障害対応
  - 他のシステムの障害対応フローに組み込んで連絡
  - “認証設備室”での対応もあり
- 監視
  - 署名データの有効性／タンパ証跡の確認
- 改善
  - 利用するプログラムにおける鍵長やアルゴリズムの対応

これまでの運用を通じて

- 鍵管理とは
  - 鍵を使って作られる、ユーザに使って頂くデータ（署名や証明書）の品質管理の一環
    - 私有鍵が漏れたり使えなくなったりすると品質低下
- 品質管理と鍵の安全性
  - 冗長性　コピー → 品質を下げるリスク
  - 堅牢性　利用難易度高 → 使えなくなるリスク

「セキュリティと利便性はトレードオフ」というが、鍵管理は単に使いにくくなりがち。常にユーザと運用者の利便性（利用可能性）を維持する意識を持つことが重要。（と思ってやっております）