# TCRと私

民田雅人
株式会社日本レジストリサービス
2010-07-21 dnsops.jp BoF@品川

# ICANNのKSK管理

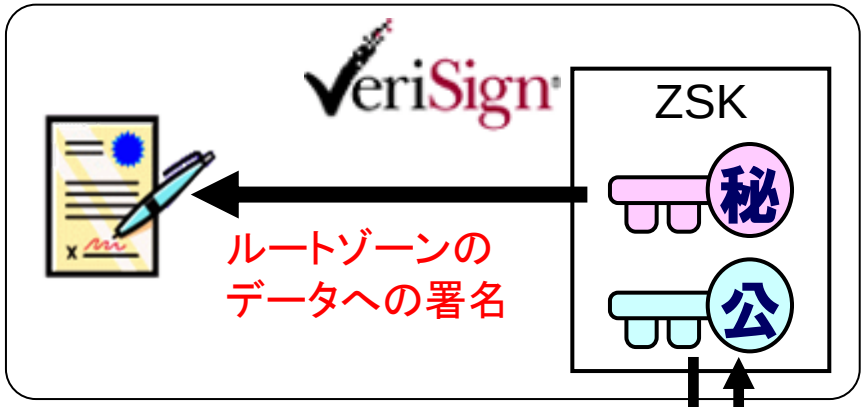
- USの東海岸と西海岸にKSK管理のための専用の施設を用意
  - 東: Culpeper, Virginia
  - 西: El Segundo, California
  - ほぼ同仕様で相互にバックアップ可
- TCRを選出し、KSK管理を公正化
  - ICANNだけではKSKを操作できない状況を確立
  - TCR: Trusted Community Representatives
    ⇒ 信頼できるコミュニティの代表

# TCRの役割

- Crypto Officer (CO) - 東西の各拠点に7人
  - 拠点にあるHSMを稼動させるのに必要な、スマートカードを保存してある金庫の鍵を保持
  - Key Ceremonyへの立会い役も兼ねる
  - HSM: Hardware Security Module
- Recovery Key Share Holder (RKSH) - 7人
  - 万が一東西の両施設が利用不能になった場合にKSKを復元するためのスマートカードを保持
- Backup COとBackup RKSH
  - 各COやRKSHの交代役

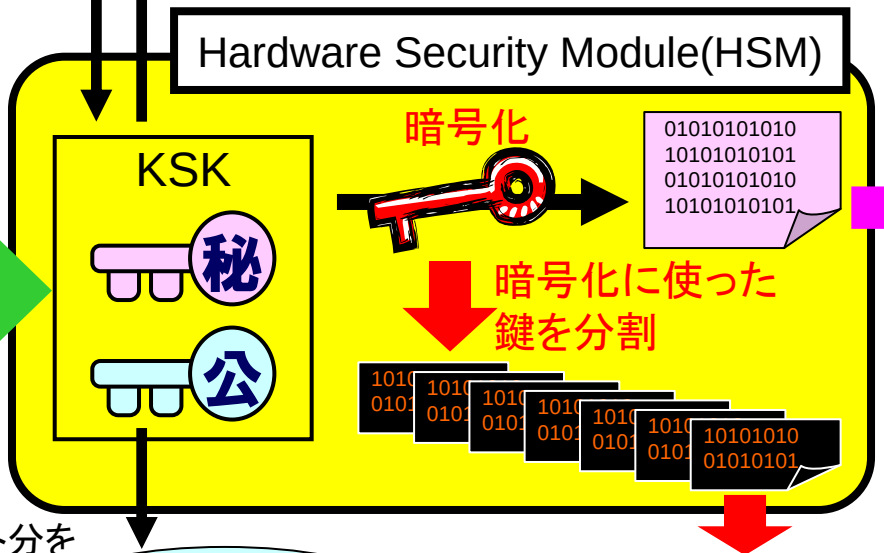
# ルートゾーンにおけるKSKの管理イメージ

ICANNの東西の拠点が同時にダウンしても、RKSHが預かるスマートカード7枚のうちの5枚と、ICANNが保管する暗号化KSKバックアップの双方を新しいHSMに入力することにより、KSKが入ったHSM(図中央の黄色い箱)を復旧できる



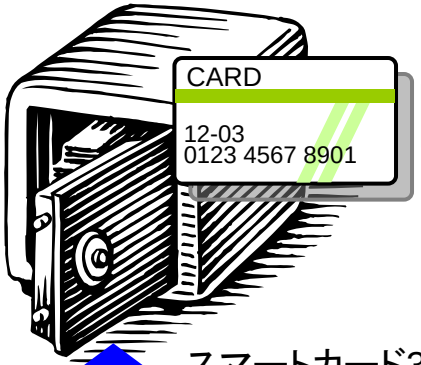

鍵を入力

署名済鍵を出力




保管

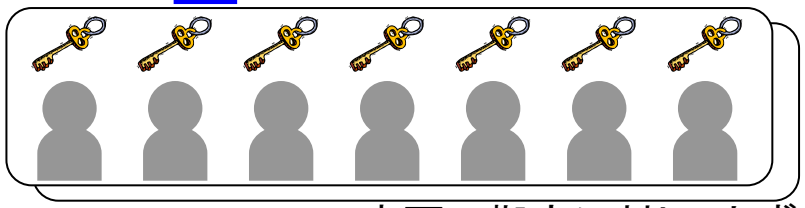

金庫の中のカードをHSMに挿すことで、HSMの中にあるKSKを使うことができる



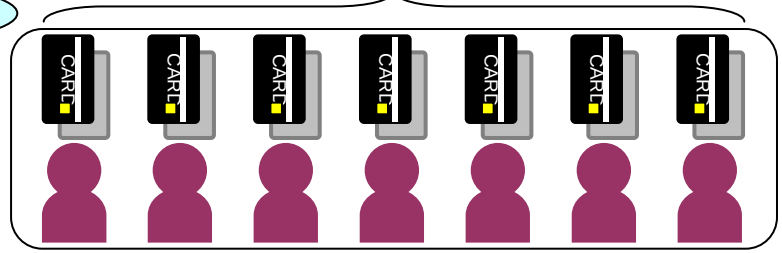

スマートカード3セット分を
3つの鍵で取り出す

外部に公開

分割した鍵データを
スマートカードに記録し
1枚ずつ保持する



Crypto Officer(CO):東西の拠点に対し7人ずつ




Recovery Key Share Holder(RKSH):7人

# TCR選出まで (1/2)

- TCRは立候補 (4/23の〆切直前に応募)
  - 自分がどういう奴かを記述
  - 推薦者を3〜4人選んで連絡先を伝える
  - 希望する役割を選ぶ
    CO, RKSH, Backup, どれでも可
- しばらくして自宅住所を聞かれた
  - 当然ながら英語表記の自宅住所を記述
  - Google Mapsに入れても英語表記じゃダメなので、念のため検索後のURLも一緒に送ってみる

# TCR選出まで (2/2)

- 15年間に渡って犯罪に関与していない、現在も関係していない、裁判中で無い旨の宣誓書に署名して送り返せ
  - 署名してスキャンしてPDFを送る
- 推薦人に「立候補者をいつから知っている」「10段階評価で適正はいくつだと思うか」などの問い合わせがある
  - 各推薦人がそれぞれ回答する

# TCRに選出される

- 5/26 朝 : メールが届く
  - あなたはTCRのうち西海岸ファシリティ担当のCOに選出されたことをお伝えします
  - 6/16に東海岸でKSK Ceremonyを開催します
  - 7/12に西海岸でKSK Ceremonyを開催します
  - すぐに旅行の手配をして下さい、そしてその状況を連絡して下さい

⇒ 東海岸の場合、スケジュールが厳しい

# COとしてKSK Ceremony 2に参加
# KSK Ceremony 2の様子等

- 「rootゾーンのKSK管理」
  -- ICANN KSK Ceremony 2参加記 --

  @DNSSEC 2010 サマーフォーラム

  http://dnssec.jp/wp-content/uploads/2010/07/20100721-dnssec-root_ksk-minda.pdf

- ルートゾーンにおけるKSKの管理方法

  http://jprs.jp/dnssec/doc/root_tcr.html

# KSK Ceremony 2の~~戦利~~記念品

# Q and A

JAPAN REGISTRY SERVICES