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

民田雅人
株式会社日本レジストリサービス
2010-07-21
DNSSEC 2010 サマーフォーラム@品川

ICANN KSK Ceremony

- キーセレモニー【Key ceremony】
  - 認証局のための秘密鍵と公開鍵のペアを作成するためのプロセス。
    ベリサインでは幾重もの物理セキュリティとアクセス権限で守られた部屋の内でキーセレモニーを行うことで、鍵の危殆化を防いでいます。
    (ベリサイン PKI用語集より引用)
- ICANN KSK Ceremony
  - rootゾーンのKSKの秘密鍵と公開鍵を作成するプロセス

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

各施設にあるもの

- セレモニールーム
  - アクセス制限された作業スペース
  - 作業者と立会者が入室
  - 机、モニタ(50”ぐらい)、プリンター、シュレッダー
  - 監視カメラ
- セーフルーム
  - アクセス制限のさらに高いスペース
  - 金庫2台
  - 監視カメラ

金庫1

- セレモニーに使うハードウェア一式の保管庫
- PC、HSM、OSブート用DVD、USBメモリ等
  - 各機材はTEBで保管
- TEB: Tamper Evident Bag
  - シリアル番号付の封印できるビニール袋
  - 保存前にシリアル番号を記録して封印し、開封前にシリアル番号を確認し、前回の保存から未開封であることを担保
  - 開封時は袋を破るため、1回限りの使い捨て

金庫2

- HSMの稼動に必要なスマートカードを保管
  - スマートカードもTEBに入れて保管
- スマートカードは7セットあり、HSMを稼動させるのに3セット必要
- 内部はスマートカードを保存するためのスロットに分かれており、各スロットに物理**鍵**
- **鍵**を7人のCrypto Officerがそれぞれ保管

KSK Ceremonyに使うPC

- インターネットからはオフラインのノートPC
- KSK Ceremony用のスペシャル品
  - HDD無し、無線LAN無し、Bluetooth無し
  - Ethernet有り、USB有り、DVDドライブ有り
  - EthernetはHSMと接続
- OSはDVDで起動
  - CentOS 5.5
- 必要な情報はUSBメモリに記録

KSK Ceremony 1

- 東海岸:2010-06-16 Culpeper, Virginia
  - KSKの生成
  - VeriSignが用意したZSK(DNSKEY)への署名(2010年7月～9月)
  - 東側担当COへの鍵の引渡し
  - RKSHへのスマートカードの引渡し
- 同じデータセンター内で多くの人がカメラ経由で状況を見守る

KSK Ceremony 2

- 西海岸：2010-07-12 El Segundo, California
  - 東側で作成したKSKのHSMへのインポート
  - VeriSignが用意した次のZSK (DNSKEY)への署名 (2010年10月～12月)
  - 西側担当COへの鍵の引渡し
- 両方共成功しrootゾーンの正式署名開始
  - 東側が成功しても、西側が成功しないとrootゾーンのDNSSEC化は行われないことになっていた

各セレモニーの手順書と実時間

- 東側: 253ステップ　6時間の予定が8時間で終了
- 西側: 199ステップ　予定通り6時間で終了
  - 記載内容は細かく、非常口の参加者への案内等も記載
  - 以下はOS起動後のPCの次の手順部分から抜粋

38	CA presses "CTRL+ALT+F2" to get a console prompt and logs in as root.

39	CA enters the commands
	`system-config-display --noui`
	and
	`killall Xorg`
	CA ensures that external display works.

素朴な疑問
東で作成したKSKはどうやって西へ?

- 東で、RKSHが保持するものと同じスマートカードを1セット余計に作成しTEBに保存
- 東のHSMの暗号化されたバックアップと、上記カード(開封前にTEBのシリアル番号を確認)し、西のHSMへ復元
- 利用後のスマートカードは、セレモニーの一手順として、参加者の面前でシュレッダーで破棄
  - RKSHのみが必要な情報を保持する状況を担保

KSK Ceremony 2の記念写真

参考

- ICANN KSK Ceremony
  - http://dns.icann.org/ksk/
  - http://dns.icann.org/ksk/ceremony/
- IANA DNSSEC Information
  - http://www.iana.org/dnssec/
- Root DNSSEC
  - http://www.root-dnssec.org/

Q and A

JAPAN REGISTRY SERVICES