DNSSECの鍵管理

民田雅人
株式会社日本レジストリサービス
2010-11-22 JNSA鍵管理勉強会

内容

- DNSSECのしくみ
- DNSSEC導入に向けて
- DNSSECの鍵と信頼の連鎖
- rootゾーンの鍵管理
- TCRと私

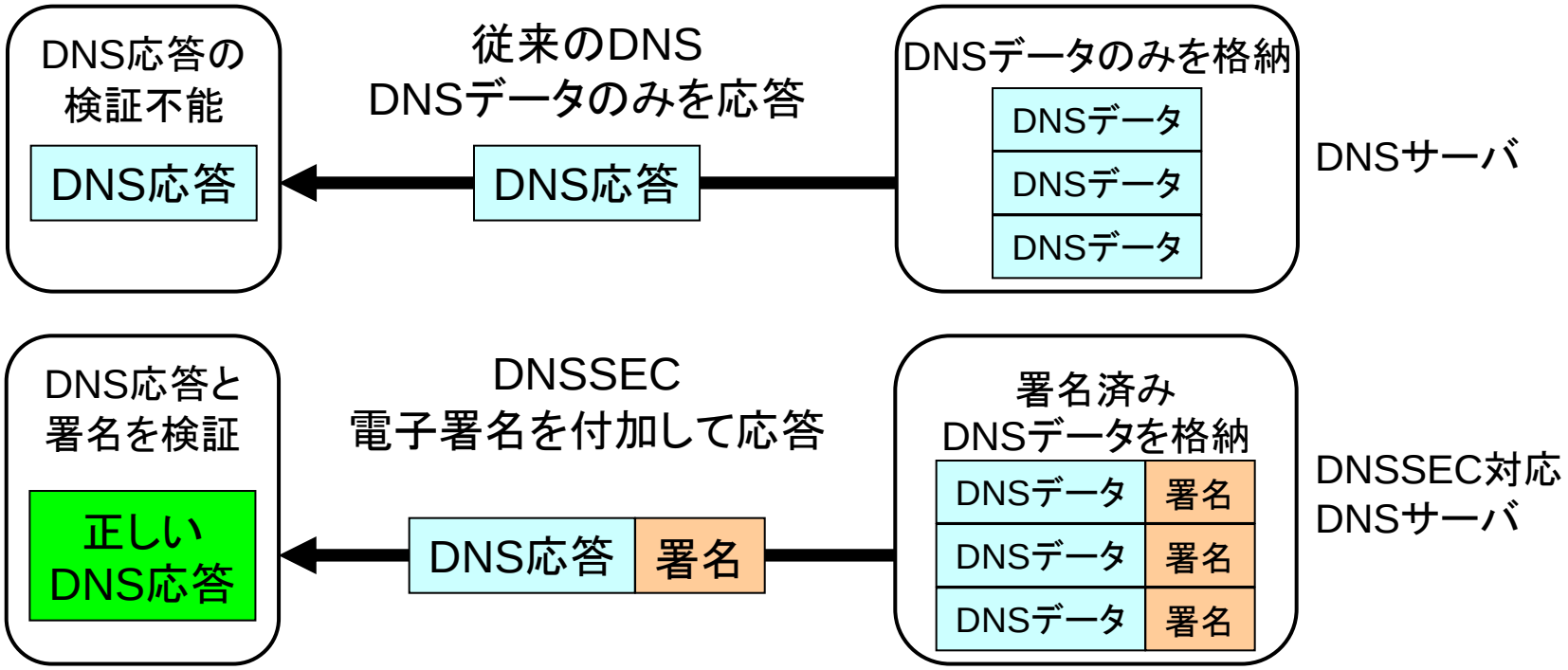
DNSSECのしくみ

DNSSECとは

- DNSセキュリティ拡張(DNS SECurity Extensions)
  - **公開鍵暗号**の技術を使い、検索側が受け取ったDNSレコードの出自・完全性(改ざんのないこと)を検証できる仕組み
  - 従来のDNSとの**互換性を維持した拡張**
  - Kaminsky型攻撃手法の発覚を1つの契機に、多くのTLDが導入開始あるいは導入予定
- キャッシュへの毒入れを防ぐことができる現実解
  - 他の技術も存在するが標準化が成されていない

従来のDNS vs DNSSEC

- DNSサーバが応答に電子署名を付加し出自を保証
- 問合せ側でDNS応答の改ざんの有無を検出できる

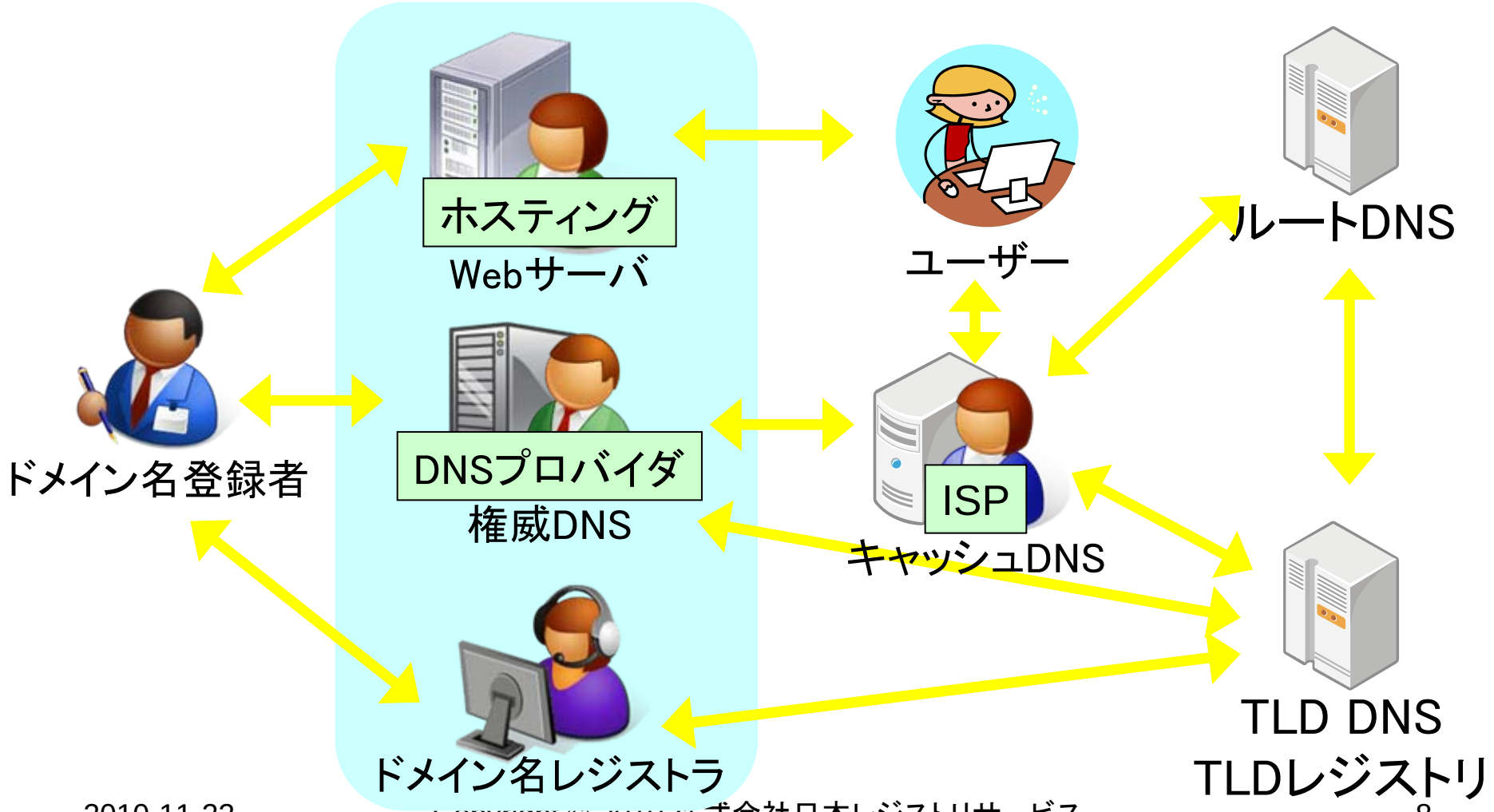


DNSSECのスコープ

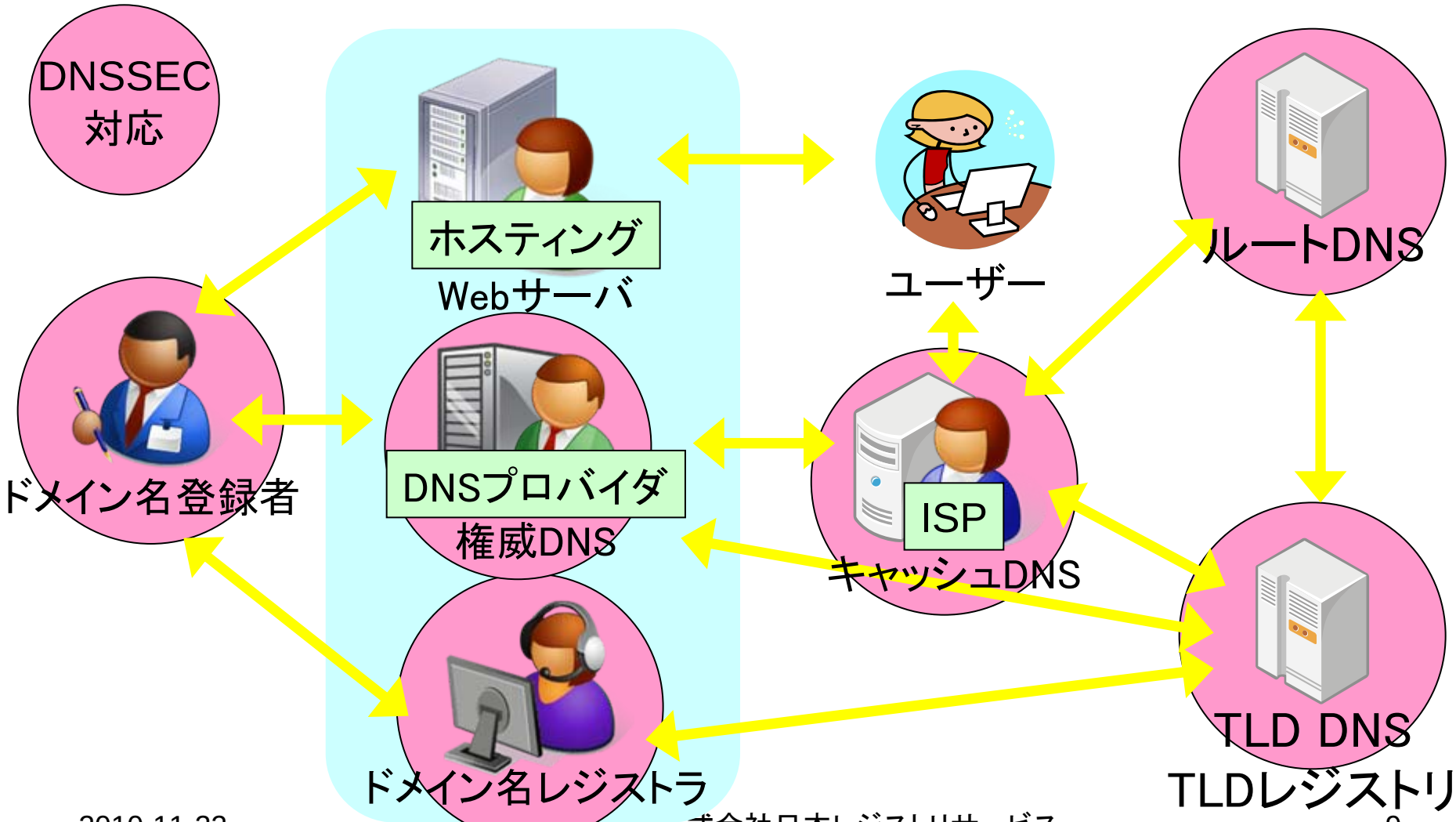
- 対象としているもの
  - DNS問合せの応答が、ドメイン名の正当な管理者からのものであることの確認
    ⇒ **出自の保証**
  - DNS問合せの応答における、DNSレコードの改変の検出
    ⇒ **完全性の保証**
- 対象としていないもの
  - 通信路におけるDNS問合せと応答の暗号化
    ※DNSレコードは公開情報という考え方から

DNSSEC導入に向けて

DNS関係者と各情報の流れ



DNSSEC対応が必要な関係者



DNSEC対応作業の概要

- ドメイン名登録者
  - DNSSEC導入の決定
- ドメイン名レジストラ
  - 鍵情報の上位レジストリへの取次ぎ
- TLD DNS、ルートDNS
  - 権威DNSサーバのDNSSEC対応化
  - ゾーンへの署名
- DNSプロバイダ
  - 権威DNSサーバのDNSSEC対応化
  - 秘密鍵・公開鍵を作成し、ゾーンに署名
- ISP
  - キャッシュDNSサーバのDNSSEC対応化
  - (キャッシュDNSサーバでの)署名の検証

世界のDNSSEC導入の概況

(2010年11月8日現在)

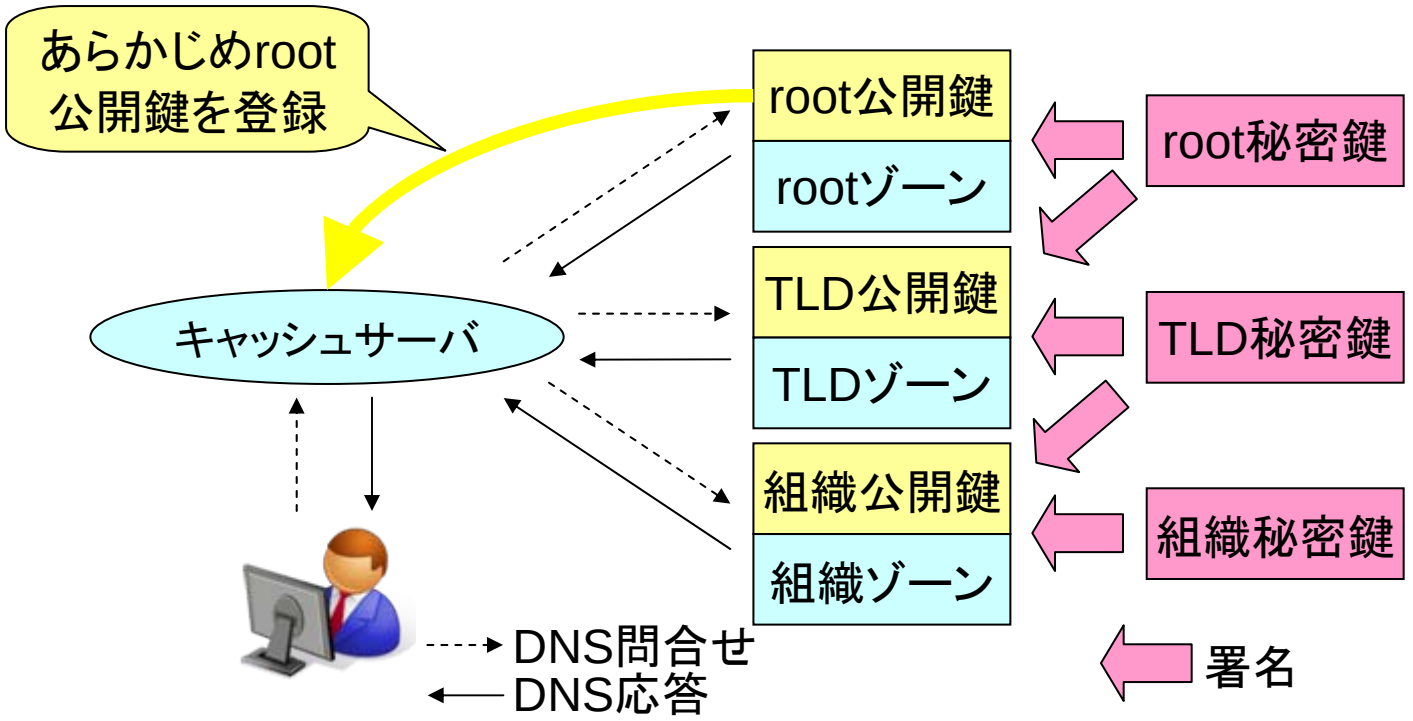
- rootゾーン
  - 2010年7月15日よりDNSSECの正式運用開始
- DNSSEC導入済TLD
  - rootゾーンにある全294のTLDのうち
  - 62のTLDが署名済み
  - 46のTLDがrootゾーンにDSを登録済み
  - (2009年末は10のTLDが署名済みだったのみ)
- 今後の状況
  - jpは2010年10月17日に署名開始、2011年1月16日より登録受付サービス開始
  - com は2011年前半 / netは2010年末に導入予定
  - 導入予定のTLDは多数

DNSSEC普及に関連した動き
KIDNS (Keys In DNS)

- DNSで証明書を公開するアイデア
  - CERT RR (RFC 4398 2006年 Obsoletes RFC 2538)
- DNSSECの実用化にともない、現在実用化の検討が始まっている
  - DNSSECによってDNSレコードが信用できる
    ⇒ DNSにある証明書も信用できる
  - 従来の自己証明書では、本当にそのサイトのものかどうか確認が困難だが、DNSはそのサイトのもの
  - ドメイン名の一致を重要な目的とする証明書では、DNSで自己署名証明書を配布するほうがリーズナブル?

DNSSECの鍵と信頼の連鎖

DNSSECの信頼の連鎖の概念図



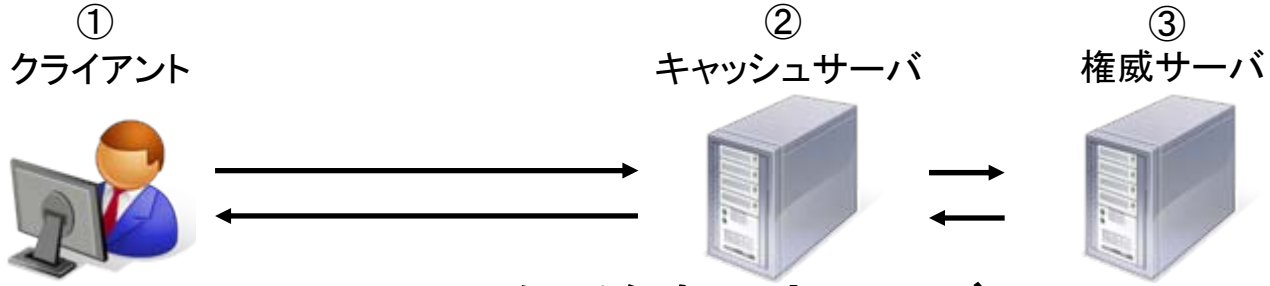
- 秘密鍵で、自ゾーンと下位ゾーンの公開鍵に署名
- root公開鍵をキャッシュサーバに登録することで、rootから組織ゾーンまでの信頼の連鎖を確立

用語:バリデータ(Validator)

- DNSSECにおいて、バリデータは署名の検証を行うもの(プログラム、ライブラリ)を指す
- バリデータの所在
  - キャッシュサーバが署名検証を行う場合、キャッシュサーバがバリデータそのもの
    ⇒ 現状、もっとも一般的なDNSSECのモデル
  - WEBブラウザ等のDNS検索を行うアプリケーションが直接署名検証を行うモデルも考えられる

DNSSEC化による名前解決モデルの変化

- 従来のDNSでの名前解決モデル



- DNSSECでの名前解決モデル

  - 多くの場合バリデータは②に実装
  - バリデータが①に実装されていても問題ない

DNSSECで利用する2種類の鍵とDS

- 2種類の鍵
  - ZSK (Zone Signing Key)
    ゾーンに署名するための鍵
  - KSK (Key Signing Key)
    ゾーン内の公開鍵情報に署名するための鍵
- DS (Delegation Signer）
  - 上位ゾーンに登録するKSKと等価な情報

ZSK

- 比較的暗号強度の低い鍵
  - 例えばRSAで1024bit等の鍵を使う
- 暗号強度が低い
  - 署名コストが低いため、大規模ゾーンの署名にも適応できる
  - 安全確保のため、ある程度頻繁に鍵を更新する必要がある
- 鍵更新は親ゾーンとは関係なく独立で行える

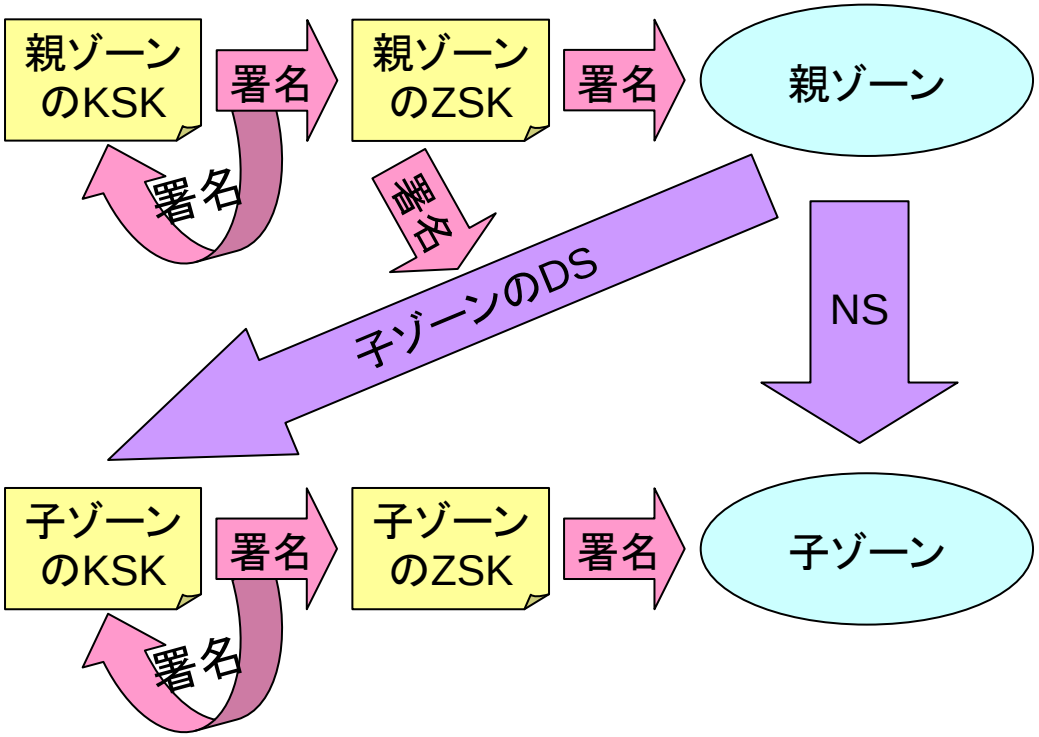
KSK

- 比較的暗号強度の高い鍵
  - 例えばRSAで2048bitの鍵を使う
- 暗号強度が高い
  - 利用期間を長くできるため、鍵更新の頻度を低くできる
  - 署名コストは高いが、少数の鍵情報のみを署名対象とするため問題にはならない
- KSK公開鍵と暗号論的に等価な情報(DS)を作成し、親ゾーンに登録する
  - **KSKを変更する場合、同時にDSも更新する**

DS

- KSK公開鍵を、SHA-1/SHA-256等のハッシュ関数で変換したDNSレコード
  ⇒ KSK公開鍵と等価の情報
- 親ゾーンの委任ポイントに、
  NSと共に子ゾーンのDS情報を登録
  - 親ゾーンの鍵でDSに署名してもらうことで、信頼の連鎖を形成する

DNSSECの信頼の連鎖



- 公開鍵暗号による信頼の連鎖を形成
- キャッシュサーバが、KSKの公開鍵を使って署名を検証
  ⇒ **トラストアンカー**
  - キャッシュサーバにはrootゾーンのKSK公開鍵を登録する

DSとNSの本質的な違い

- NS : 委任先DNSデータが存在する(可能性のある)**サーバを指し示す**
- DS: 委任先**DNSデータを直接指し示す**
  - DSは子ゾーンのKSKと等価な情報
- NSの指し示すドメイン名がDNSSEC非対応であってもDNSSECの検証は問題無い

```
jpゾーンでの例
example.jp. IN NS  ns0.example.ad.jp.
example.jp. IN DS  2260 8 2 CC83B074566.............
```

  - example.ad.jpドメイン名はDNSSEC対応していなくても、example.jpドメイン名はDNSSEC検証可能

DNSSEC運用

- 鍵更新
  - 同じ鍵を長期間使い続けるのはリスクとなる
  - 定期的な鍵更新を行う
    例)　ZSK ⇒ RSA1024bitで1ヶ月
    KSK ⇒ RSA2048bitで1年
- 再署名
  - 署名には有効期限があるため、期限に達する前に署名期限を更新する
  - 定期的な**ゾーン全体の再署名**が必要となる

rootゾーンの鍵管理

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

rootゾーンの特別な事情

- 現在のrootゾーンの管理者
  - ゾーン情報の管理　　ICANN (実作業はIANA)
  - ゾーンデータの作成　　VeriSign
  - ゾーン情報変更などの承認　DoC(米国商務省)
- rootゾーンのDNSSEC化での作業分担
  - KSK管理 ⇒ ICANN
  - ZSK管理 ⇒ VeriSign

    ⇒ これら組織だけでは、公正な管理とは言い難い

ICANNのKSK管理

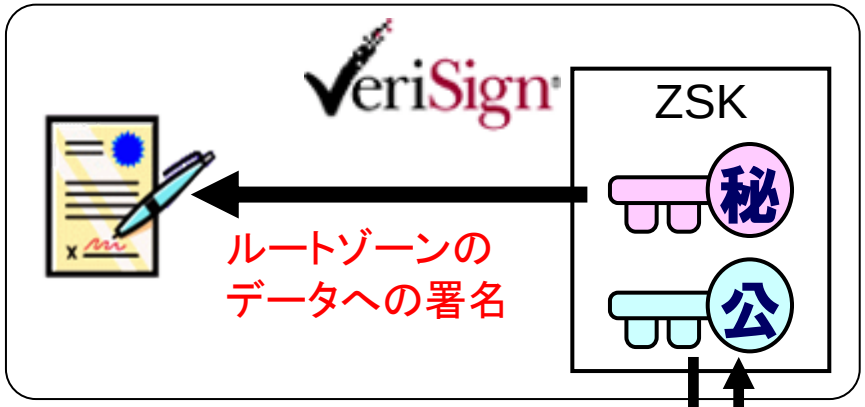
- TCRを選出し、KSK管理を公正化
  - ICANNだけではKSKを操作できない状況を確立
  - TCR: Trusted Community Representatives
    ⇒ 信頼できるコミュニティの代表
- USの東海岸と西海岸にKSK管理のための専用の施設を用意
  - 東: Culpeper, Virginia
  - 西: El Segundo, California
  - ほぼ同仕様で相互にバックアップ可

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
  - セレモニー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

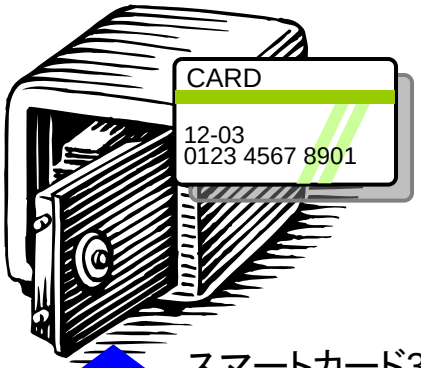


鍵を入力

署名済鍵を出力

Hardware Security Module(HSM)

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



KSK

秘

公

暗号化

01010101010
10101010101
01010101010
10101010101

保管

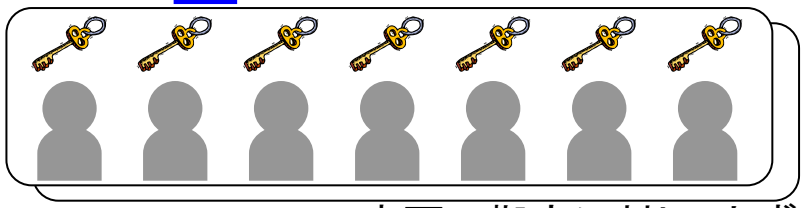
暗号化KSK
バックアップ

暗号化に使った鍵を分割

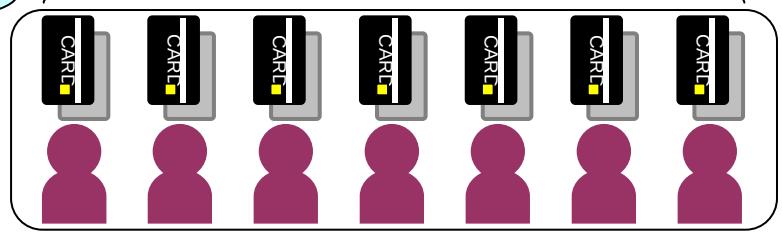
分割した鍵データをスマートカードに記録し1枚ずつ保持する

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



Crypto Officer(CO):東西の拠点に対し7人ずつ



Recovery Key Share Holder(RKSH):7人

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
  - 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COがそれぞれ保管
- 金庫1,2 とも、セーフルームに入る権限とは別の人が金庫を開ける権限を持っている

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
- 両方とも成功し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

その後のKSK Ceremony

- KSK Ceremony 3　　終了
  - 2010-11-01 Culpeper, Virginia (東海岸)
- KSK Ceremony 4　　次回
  - 2011-02-07 El Segundo, California (西海岸)
- 3ヶ月間隔で東と西で交互に行われる
  - rootゾーンはZSKの鍵更新間隔が3ヶ月

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

TCRと私

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、現在も関与していない、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

⇒ 7/12のICANN KSK Ceremony 2に参加

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/
- DNSSEC関連情報 / JPRS
  http://jprs.jp/dnssec/
- ルートゾーンにおけるKSKの管理方法
  http://jprs.jp/dnssec/doc/root_tcr.html
- DNSSEC技術実験報告書 機能・性能確認編
  http://jprs.jp/dnssec/doc/DNSSEC-testbed-report-fpv1.0.pdf

Q and A

JAPAN REGISTRY SERVICES