JPでの鍵管理

野口 昇二
株式会社日本レジストリサービス

2011-07-15 JANOG28@日本橋

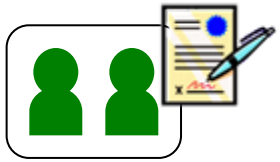
JPにおける鍵管理とは?

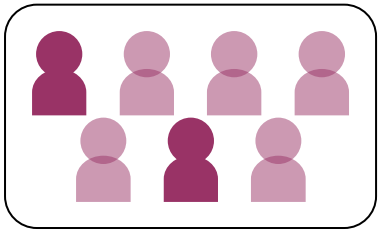
- JPドメイン名に対してDNSSEC運用を行うために必要となる署名鍵を管理すること
  - 署名鍵(KSK, ZSK)の作り方、削除の仕方
  - DNSKEYへの署名の仕方
  - .jpゾーンの署名の仕方　など
- JPドメイン名におけるDNSSEC運用ステートメント(JP DPS)
  - https://jprs.jp/doc/dnssec/jp-dps-jpn.html

JP KSKの管理 (1/4)

1. 誰が、いつ、どこで作る?

- JPRS外の方と、JPRS
  - 手順書に従い遂行しているかを、立会担当者(2名)としてJPRS外の方がチェック
  - KSKを操作する作業には、JPRSシステム部門の担当者が最低2名必要



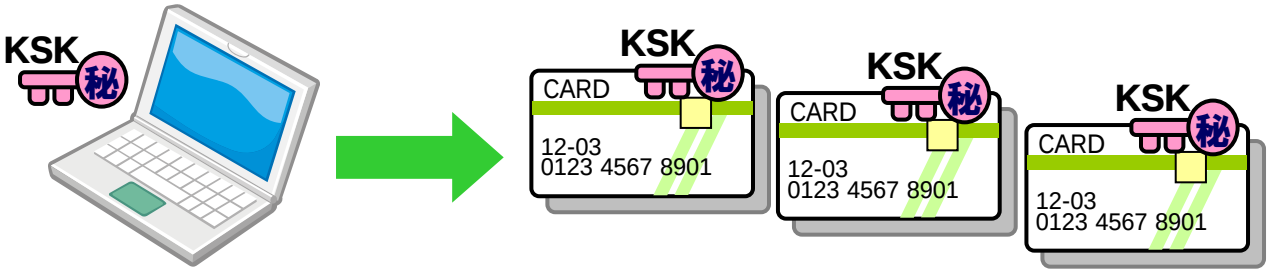


- 年1回、都内某所
  - オフラインのノートPC上で鍵を作成
  - 手順数は84手順(約5時間)

JP KSKの管理 (2/4)

2. 秘密鍵のバックアップ方法は?

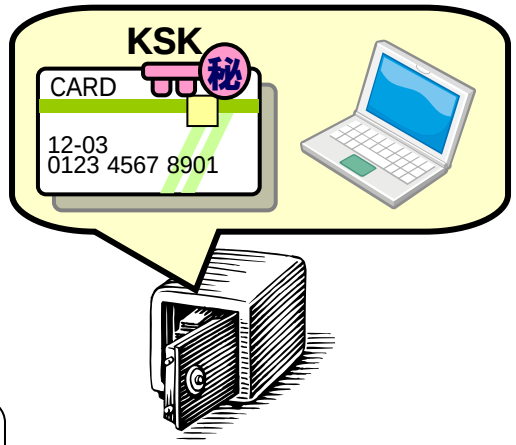
- ノートPC上でKSKを作成後、複数枚のスマートカードにKSKの秘密鍵をインポート



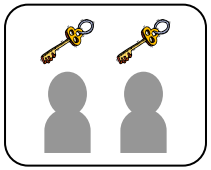
  - インポート後、ノートPC上のKSKの秘密鍵は削除

JP KSKの管理 (3/4)

3. 秘密鍵の保管場所は?



- 東京・大阪の金庫に保管
  - 鍵管理に関する業務は大阪でも継続可能
- 金庫を解錠するには、2種類の鍵が必要



  - JPRSの業務部門、システム部門が各々の鍵を管理

JP KSKの管理 (4/4)

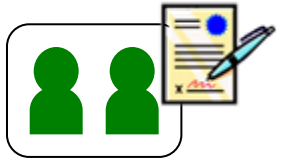
4. 作成した署名鍵(DS)の申請は?

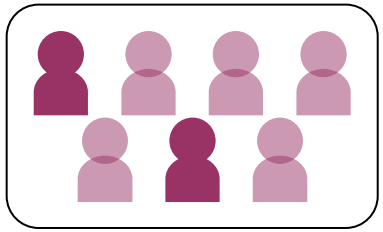
- rootへの申請は、JPRSシステム部門が実施
  - .jpのNS設定と同じ手順で申請
- rootゾーンへの反映には2～3週間程度かかる

JP ZSKの管理 (1/4)

1. 誰が、いつ、どこで作る?

- JPRSが作成
  - 手順書に従い遂行しているかを、立会担当者として業務部門の担当者がチェック
  - ZSKを操作する作業には、JPRSシステム部門の担当者が最低2名必要





- 月1回、都内某所
  - オフラインのノートPC上で作成
  - 手順数は66手順(約3時間)

JP ZSKの管理 (2/4)

2. DNSKEYへの署名はどこで行われる?

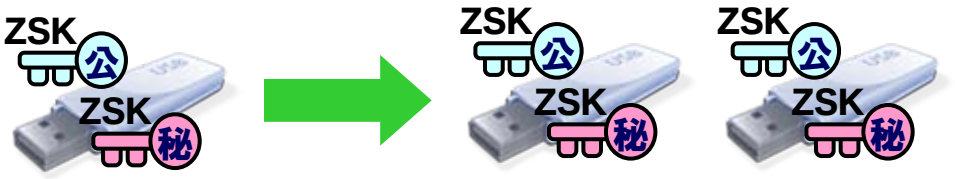
- ノートPCに接続したスマートカード
- 署名はスマートカード内部で実施
  - KSKの秘密鍵は外部には出てこない

- 署名結果は、USBストレージを経由して、.jpゾーンの管理サーバーへ移送

JP ZSKの管理 (3/4)

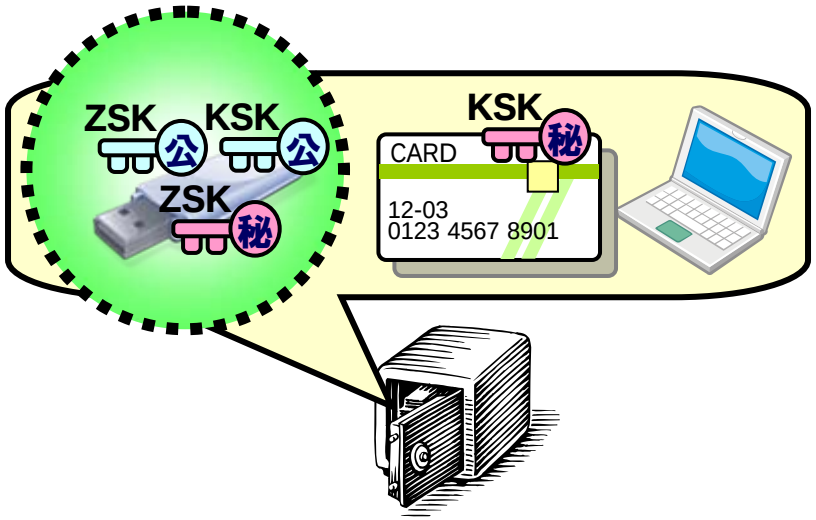
3. 秘密鍵のバックアップ方法は?

- 暗号化USBストレージ上でZSKを作成
- 複数のUSBストレージへコピー



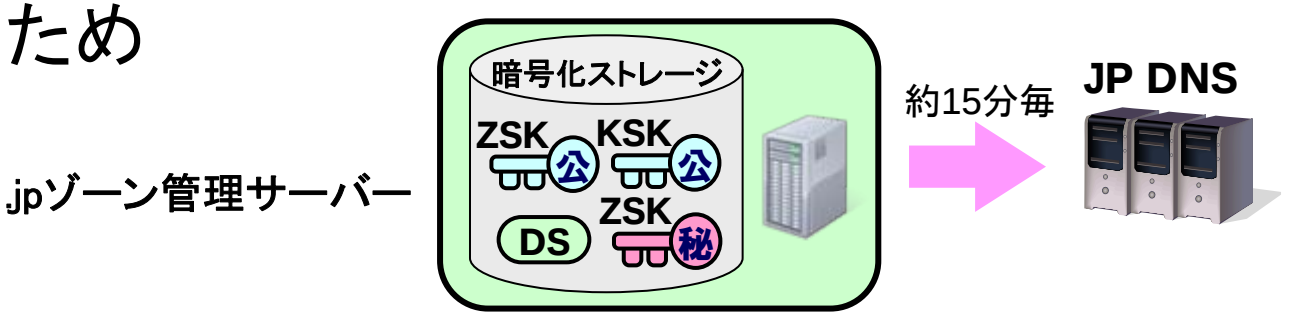
JP ZSKの管理 (4/4)

4. 秘密鍵の保管場所は?



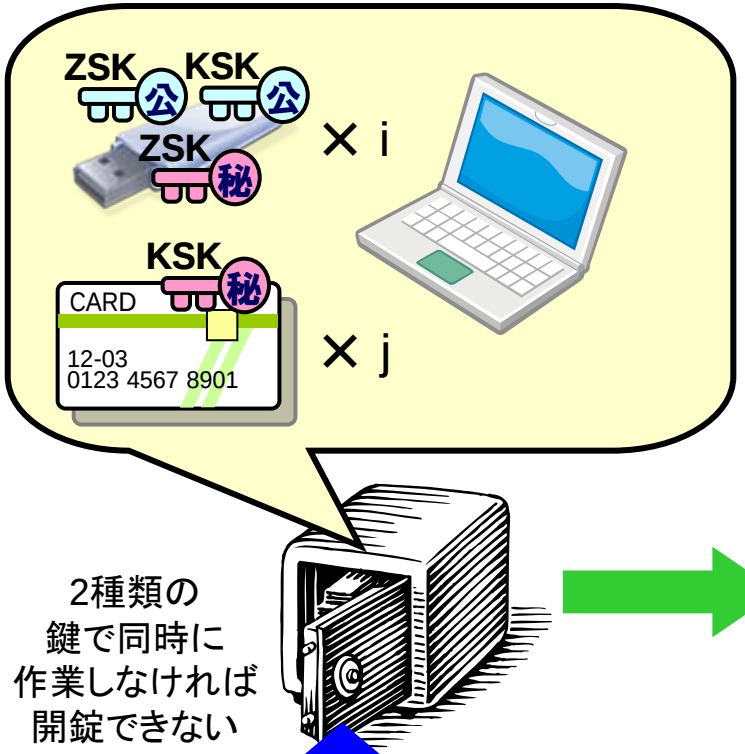
- KSKと同じ金庫に保管

- .jpゾーン管理サーバーにも格納
  - 約15分間隔での.jpゾーンへの署名が必須のため

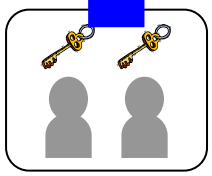


JPにおける署名鍵管理

「USBメモリ(i)、スマートカード(j)、ノートPC」×k拠点
※実際に利用するのはそれぞれ1つで、他は予備



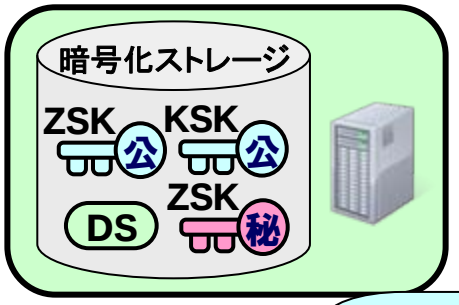
2種類の
鍵で同時に
作業しなければ
開錠できない



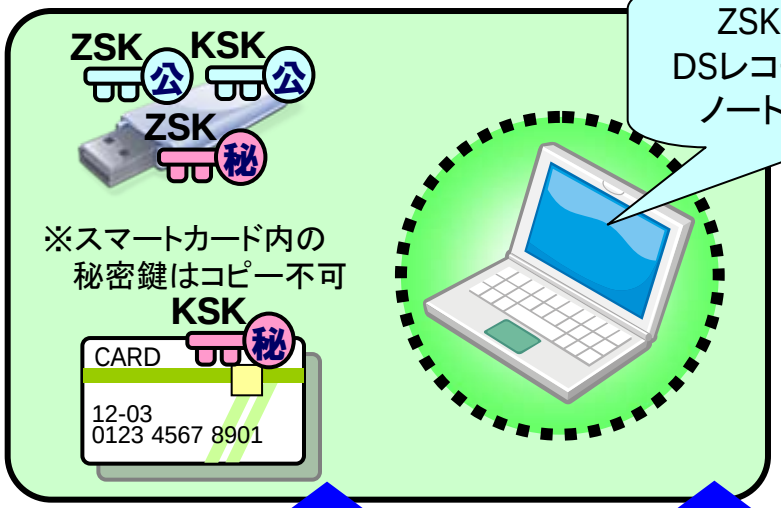
署名鍵運用担当者
+アクティベーション立会担当者
(JPRS)

USBストレージを
利用してコピー

jpゾーン管理サーバー



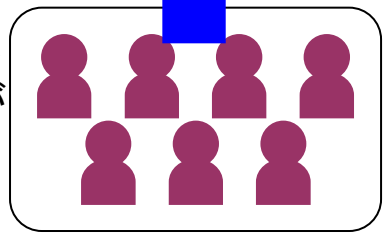
JP DNS



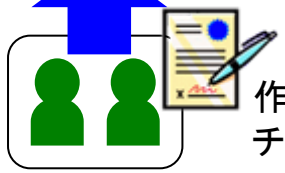
ZSK、KSKの作成、
DSレコードの作成などを
ノートPC上でおこなう

ノートPCには
ネットワーク接続
の機能がない
(オフラインで利用)

2人揃わなければ
USBメモリ、スマート
カードの読み込みが
できない



署名鍵運用担当者
(JPRS)



アクティベーション
立会担当者(*)

作業を監視し
チェックシート
に記述

(*)KSK作成のときは
JPRS外から招聘