JPドメイン名におけるDNSSECについて
― JP DPSの作成を切り口に ―

森健太郎
<kentaro@jprs.co.jp>
株式会社日本レジストリサービス

本資料について

- 本資料は、2011年7月12日に開催されたJPNICセミナー「組織におけるDNSSECの姿 ～ICANN大久保智史氏を迎えて～」の講演資料を一般公開向けに加筆修正したものである
- 但し、加筆修正は必要最小限とし、セミナー開催時点を基準とした記述はそのままとした

JP DPS

- JPRSは、.jpゾーンにおけるDNSSECサービス（JP DNSSECサービス）の開始にあわせて、サービス運用方針を「JPドメイン名におけるDNSSEC運用ステートメント（JP DPS）」として文書化し、公開した*1*2
  - https://jprs.jp/doc/dnssec/jp-dps-jpn.html (日本語)
  - https://jprs.jp/doc/dnssec/jp-dps-eng.html (英語)*3

*1：レジストラ向けにはサービス開始1カ月前に先行公開

*2：署名パラメータの一部についてはより以前から公開

*3：参考訳として公開

DPSとは（JPRSの理解）

- DNSSECサービス利用者が、DNSSEC運用についての情報を得ることでサービスを選ぶ際の判断材料とするもの
- DNSSECサービス運用者が、DNSSECサービスの安全性や運用の考え方、方式、手順などを網羅的に検討する手段として活用するもの
- DPSのフレームワークは、PKIのCPS（Certification Practice Statement）を参考にしており、本資料執筆時点で以下のI-D（Internet-Draft）を用いて議論されている
  - DNSSEC Policy & Practice Statement Framework（draft-ietf-dnsop-dnssec-dps-framework）

参考：I-DにおけるDPSのセクション構造

1. INTRODUCTION
2. PUBLICATION AND REPOSITORIES
3. REQUIREMENTS FOR DNSSEC PRACTICE
4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS
5. TECHNICAL SECURITY CONTROLS
6. ZONE SIGNING
7. COMPLIANCE AUDIT
8. LEGAL MATTERS

JPRSが考えたDPS公開のメリット

- サービス品質を確認する上で、DPSのような客観的基準に照らし合わせることは有用だろう
  - セキュリティサービスとしてのDNSSECはこれまでのレジストリサービスに比して異質であるという認識
- レジストラが顧客にJP DNSSECサービスを説明するための拠所になり得る
  - JPドメイン名ユーザにJP DNSSECサービスの仕様・品質を理解して使ってもらえる
- DNSSEC対応を検討している国内事業者が業務設計する際のヒントになり得る

JPRSが考えたDPS公開のデメリット

- DPSの公開により、記載事項への厳格な遵守義務が発生するものと受け取られ、運用的自由度を損なうかもしれない（デメリット1）
- DPSの記述レベルが貧弱だと、公開することが逆効果になるかもしれない（デメリット2）

JPRSの判断

- 公開するデメリットに対してメリットの方が大きい
- デメリットについては適切に対応すればよい
  - デメリット1に対しては、JP DPSがサービスに関する契約書ではないことを明示することにした
  - デメリット2に対しては、CPS作成経験のあるPKI専門家を外部から招聘し、記載内容を検討することにした

JP DPS作成方針

- I-Dに準拠する
- JP DNSSECサービスで行わないことは記述しない
  - 実施予定の事項であっても記述せず、実施後にDPSを更新することで対応する
- JP DNSSECサービスの運用の自由度を担保できる記述にする
  - 具体的な実装方式（プロダクト名など）は記述せず抽象的表現にする
- 一方で、詳細を運用マニュアル（非公開）に記述することでクロスチェックを行い、具体性のない記述がDPSに残らないようにする
- 記述する必要のないことは記述しない

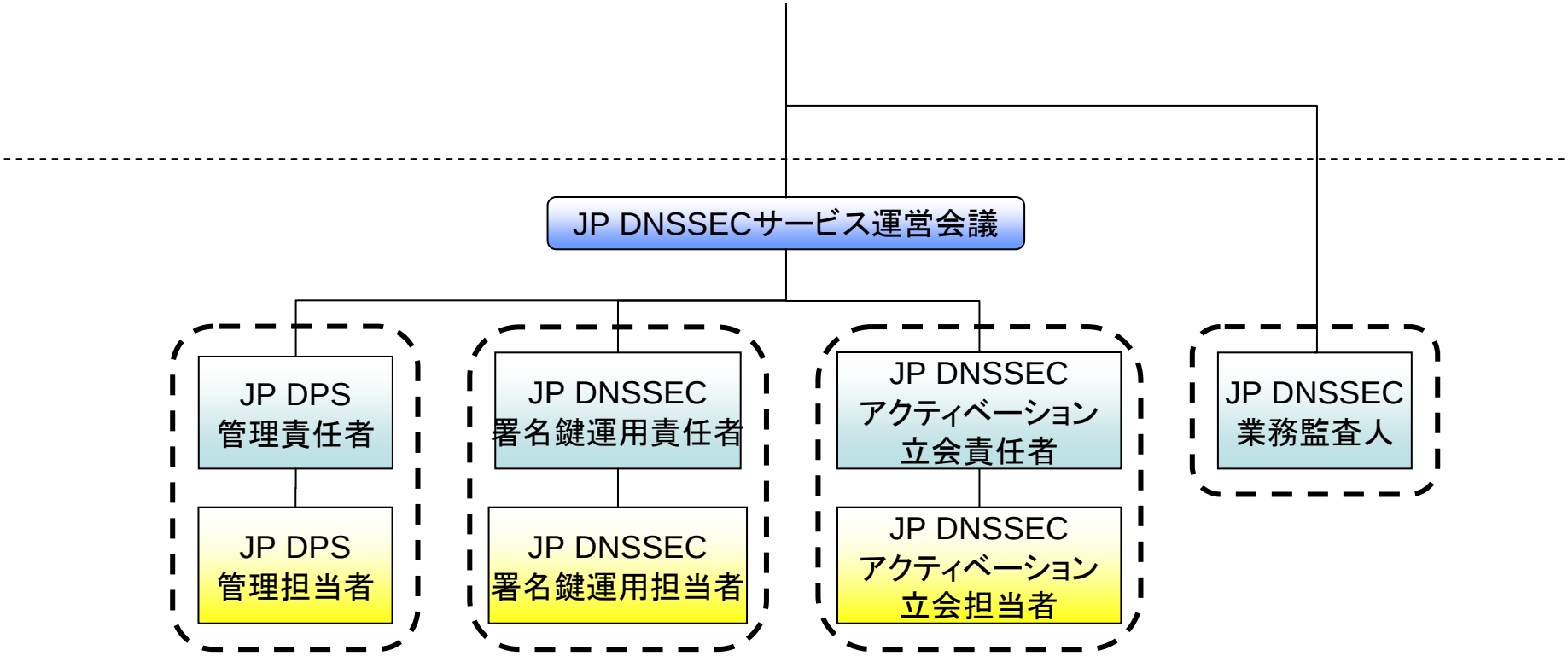
JPRSにおける作業（1/2）

- JP DPS検討チームの編成
  - サービス設計者、業務担当者、システム運用者、システム開発者、監査人、法務担当者、PKI専門家（外部）をチームに含めた
- DPSのI-D、他TLD等のDPSの読み込み
  - DNSSEC Policy & Practice Statement Framework (I-D)
  - .seゾーンのDPS
  - rootゾーンのDPS
  - .netゾーンのDPS
- 国内PKI認証局のCPSの読み込み
  - JPNICのCPS
- JP DNSSECサービスパラメータの決定
  - RFC、I-Dの調査(RFC 4641, draft-ietf-dnsop-rfc4641bis)
  - 他TLD採用パラメータの調査

JPRSにおける作業（2/2）

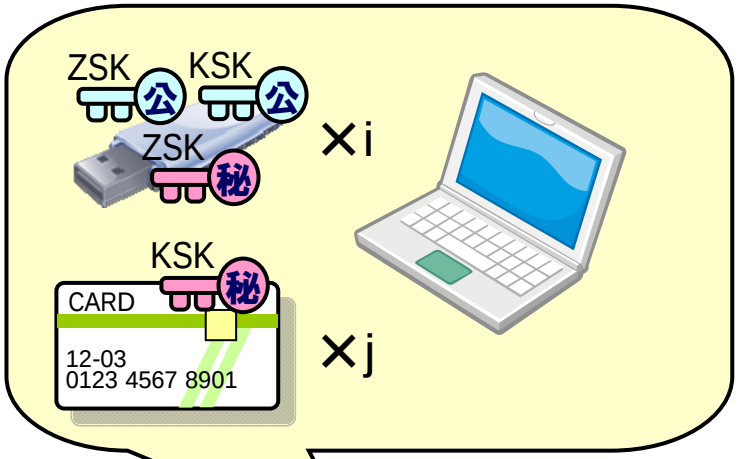
- JP DNSSECサービス運用体制の構築
- JP DPS本体の記述
- JP DPS記載事項に準じたより詳細な運用マニュアルの作成
- JP DPSへの準拠性を検証するための内部監査項目の設定

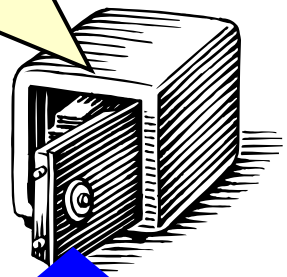
参考：JP DNSSECサービス運営体制（4章）



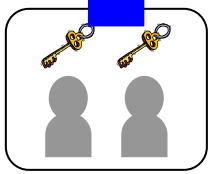
参考：JPにおける署名鍵管理（5章）

「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





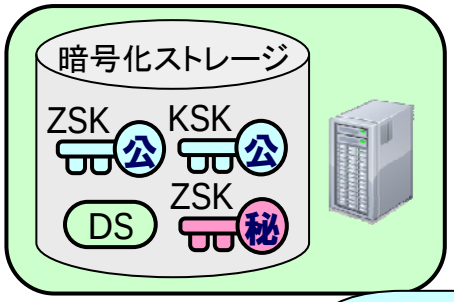
複数の
鍵で同時に
作業しなければ
開錠できない



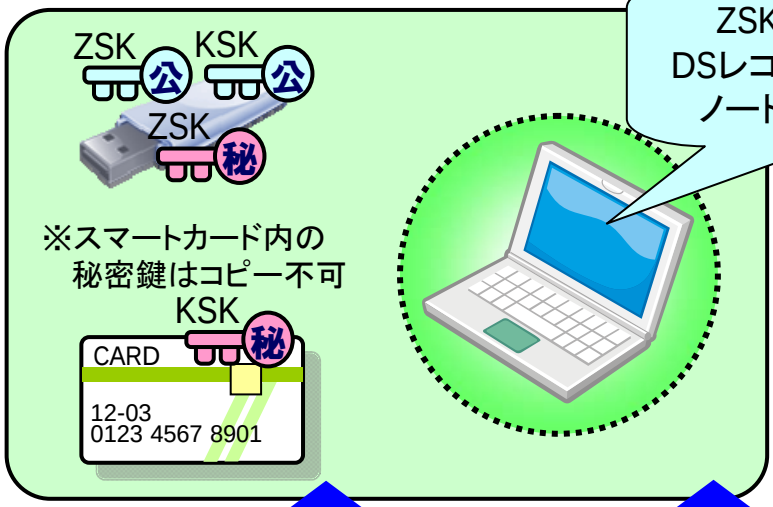
署名鍵運用担当者
＋アクティベーション立会担当者

USBストレージを
利用してコピー

.jpゾーン管理サーバー

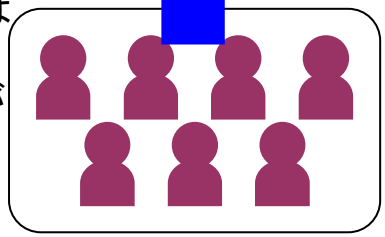


JP DNS



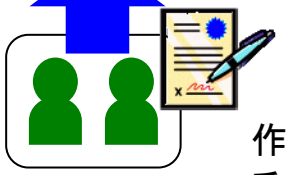
ZSK、KSKの作成、
DSレコードの作成などを
ノートPC上でおこなう

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）



複数人揃わなければ
USBメモリ、スマート
カードの読み込みが
できない

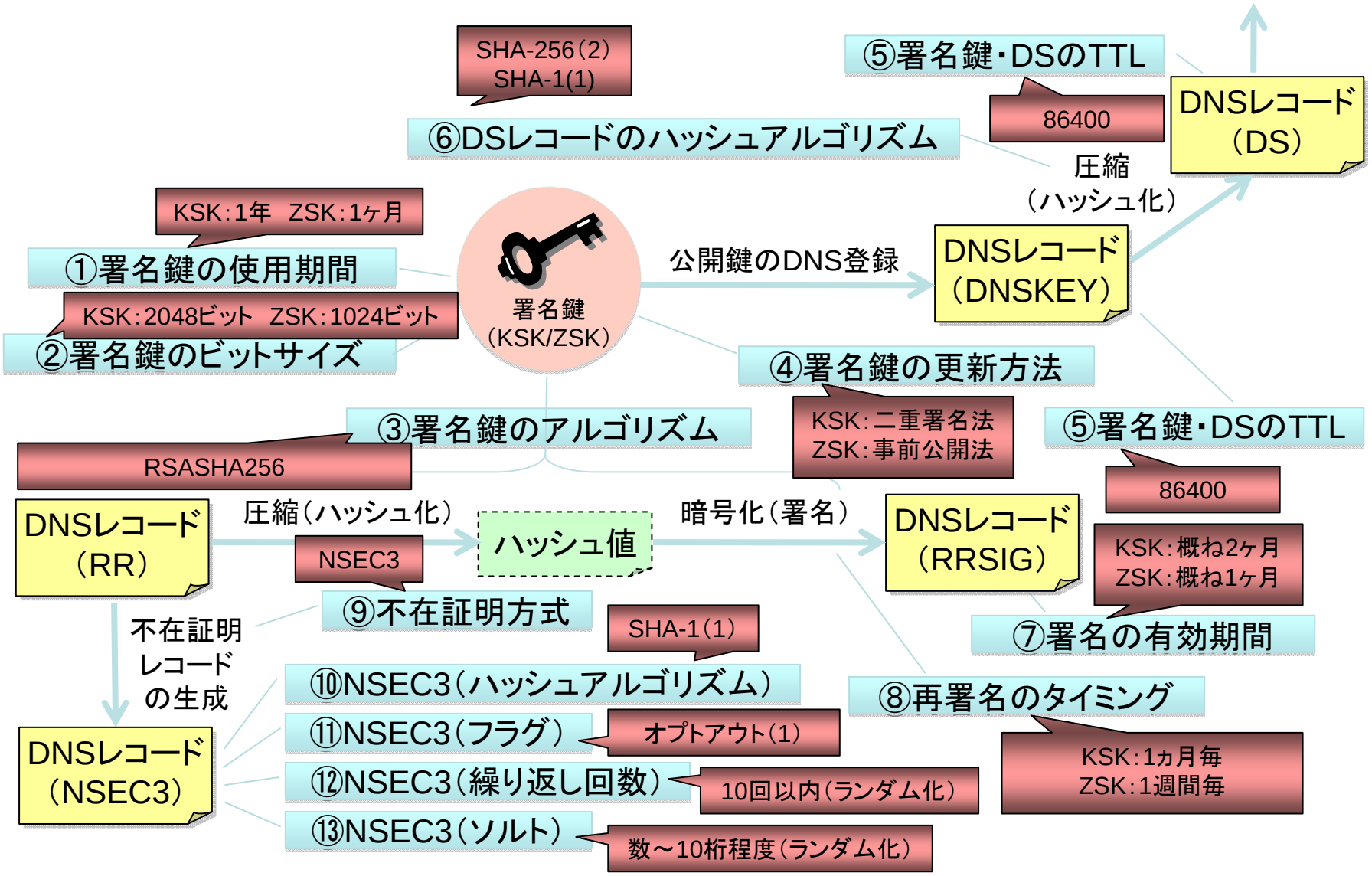
署名鍵運用担当者



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

参考：JP DNSSECサービスのパラメータ（6章）



苦労譚

- 新技術（DNSSEC）に関する記述を多数含む文書の公開において、何をどこまでやればよいかの判断が難しかった
- DPS文書作成のみでなく、体制構築や運用マニュアルの作成を行いながらDPS記載事項の裏づけを図ったため、作業量が増大した
- DPSフレームワークには、HSM (Hardware Security Module)の利用を前提に考えられているような部分があり、HSMを使用しない場合(Smartcard＋金庫)の記述が難しかった
- DNSSECは既存のレジストリサービスの拡張であるため、DPSと既存のサービス文書群との整合性確保や記載事項の切り分けに苦労した

各章記載におけるexperiences（1/2）

1. INTRODUCTION
   - DNSSECとDPSに関する一般的導入を書いたのみで比較的容易
2. PUBLICATION AND REPOSITORIES
   - 文書の公開場所・管理方法を書いたのみで容易
3. REQUIREMENTS FOR DNSSEC PRACTICE
   - 既存のレジストリサービスから継承される概念が多く、既存文書との整合性確保にやや苦慮
4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS
   - PKI的概念が多く、専門家の協力を得なければ難しかった
   - 業務体制の記述など、実際の体制構築を伴うものがあり、労力がかかった
   - 既存のレジストリサービスから継承される概念があり、既存文書との整合性確保にやや苦慮

各章記載におけるexperiences（2/2）

5. TECHNICAL SECURITY CONTROLS
   - システム設計作業と同時並行的に記載したため調整に労力がかかった
6. ZONE SIGNING
   - RFCや他TLDの運用状況が参考になり、比較的容易
7. COMPLIANCE AUDIT
   - DPSは契約書ではないというスタンス、準拠性に関する取扱いは既存のレジストリ契約文書（ICANN-JPRS-政府）において言及されているとの考えから、あえて詳細を書かないことに
   - このため、比較的容易
8. LEGAL MATTERS
   - DPSは契約書ではないというスタンス、法的事項に関する取扱いは既存のレジストリ契約文書（JPRS-レジストラ-登録者）において言及されているとの考えから、あえて詳細を書かないことに
   - このため、比較的容易

所感

- 記載の前提となる体制などを整備することを含めれば、DPSの記述は決して容易ではない
- しかし、客観的なフレームワークにより自らのサービスを確認することは、特にDNSSECのようなセキュリティサービスの導入においては有用である
- 多くの組織がDPSを公開し、業界全体にDNSSEC運用情報が蓄積することで、よりよいプラクティスの考案・発見につながることを期待する

jPRS
JAPAN REGISTRY SERVICES