ETJP Phase2における DNSSEC実験運用について

2004/3/19

ETJP DNS-WG
森 健太郎
kentaro@jprs.co.jp

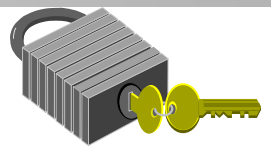
はじめに

- ETJP Phase2では、e164.jpの部分空間委任 (*1) を開始する
- これに加え、本実験運用では登録システム (https://register.etjp.jp) を通じて設定できるDNSレコードをDNSSEC対応(*2)に拡張する
  - これまで：NAPTRのみ
  - これから：NAPTR, NS(*1), DS(*2)

モチベーション

- DNSのセキュリティはENUMにおける重要な検証項目であり、参加者はより実際的なENUM実験を行える
- 本実験を通じ、運用が難しいともいわれるDNSSECに対し、feasibleな運用方式を見出したい
- レジストリ、レジストラント、DNS運用者等、それぞれの立場でDNSSEC運用ノウハウを蓄積できる

DNSSECとは（1）

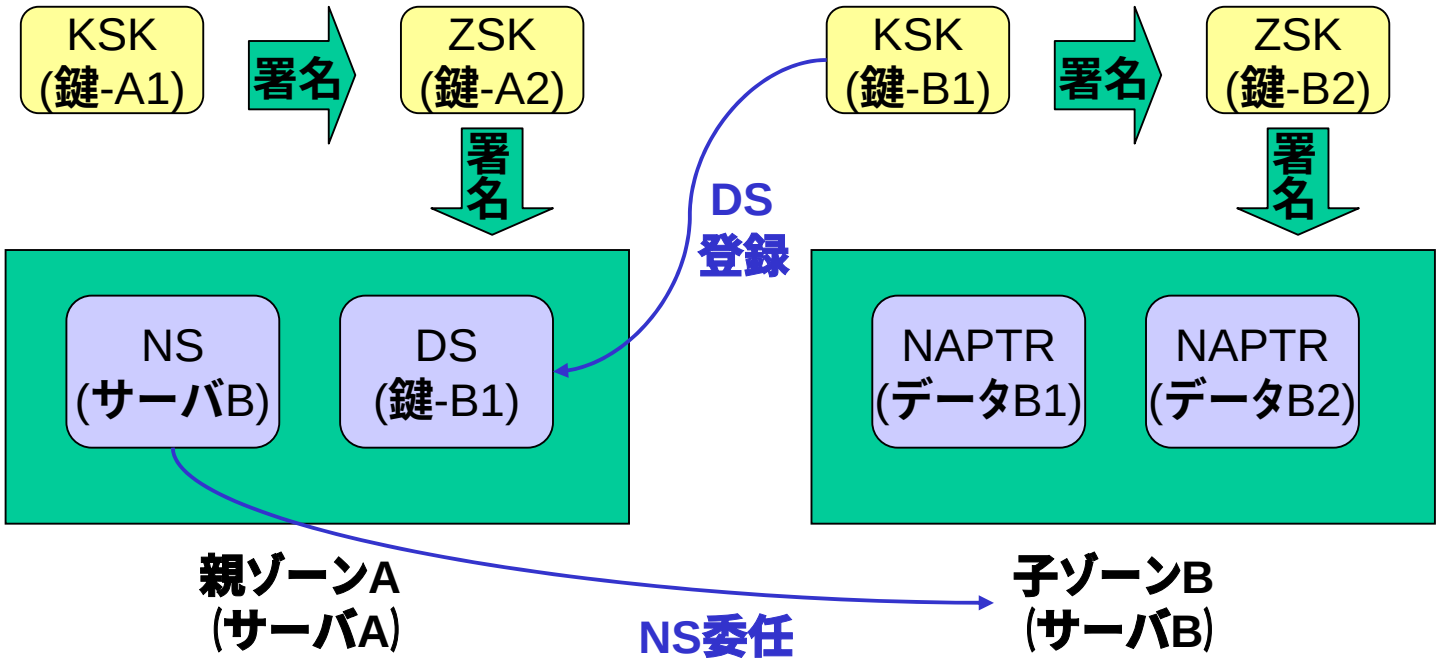


- DNSゾーンに権限を持つ管理者が、公開鍵暗号技術を用いて、自らのゾーン情報に署名を行うDNSの運用方式
  - そのゾーン情報の第3者による改ざん･騙りを検証することが可能となる技術
  - これにより、万一にも騙りを許したくないDNSレコードを守ることが可能となる
  - ENUM番号については、その性格上、関連レコードの正当性を特に保証したいものと定義される

DNSSECとは（2）

- 実験で採用する方式ではDS（Delegation Signer）と呼ばれるレコードを使用
  - ゾーン管理者は、2つの鍵を使用する
    - ZSK(Zone Signing Key):自ゾーンに署名を行う鍵
    - KSK(Key Signing Key): 自らのZSKに署名を行う鍵
    - 鍵が分かれているのは、運用上の便宜を図るため
  - DSの実体は、委任先ゾーンのKSK
  - 詳細はRFC3658

DNSSECとは（3）



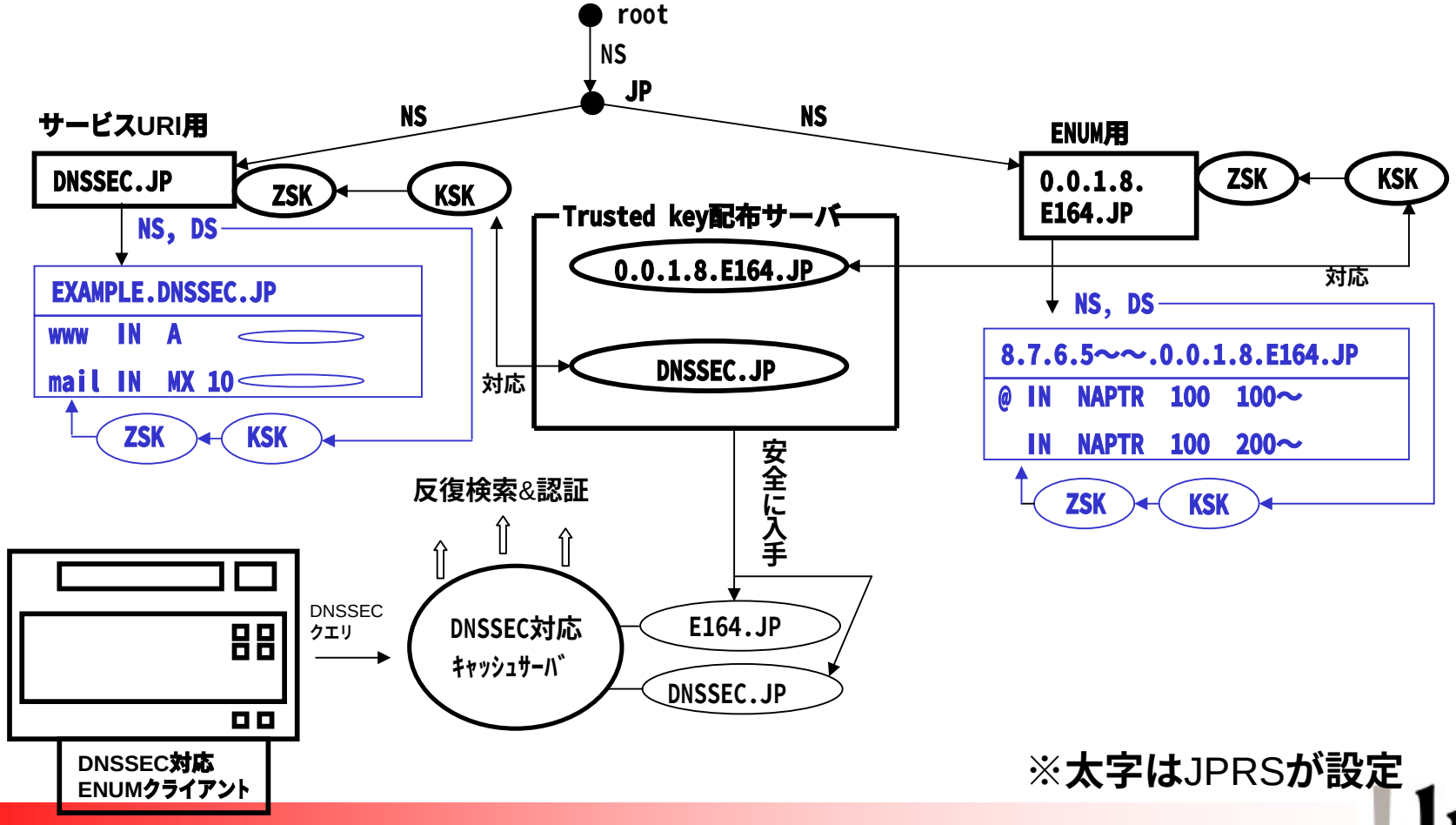
- この方式を各階層の管理者が採用することで、DNSツリー上に存在する全レコードの正当性が保証できるようになる

必要となる手順

1. 子ゾーンは、自ゾーンについてのKSK,ZSKを作成し、自らのゾーンをZSKで署名
2. 親ゾーンにKSK（DS）を送付、同時に自らのNSを通知
3. DNSSECによるゾーン委任のため、親ゾーンは通知されたNSと対応するDSを自ゾーンに設定し、自らのZSKで署名する

※別途、詳細なマニュアルを整備（後述）

本実験のシステム構成図



※太字はJPRSが設定

計画概要（1）

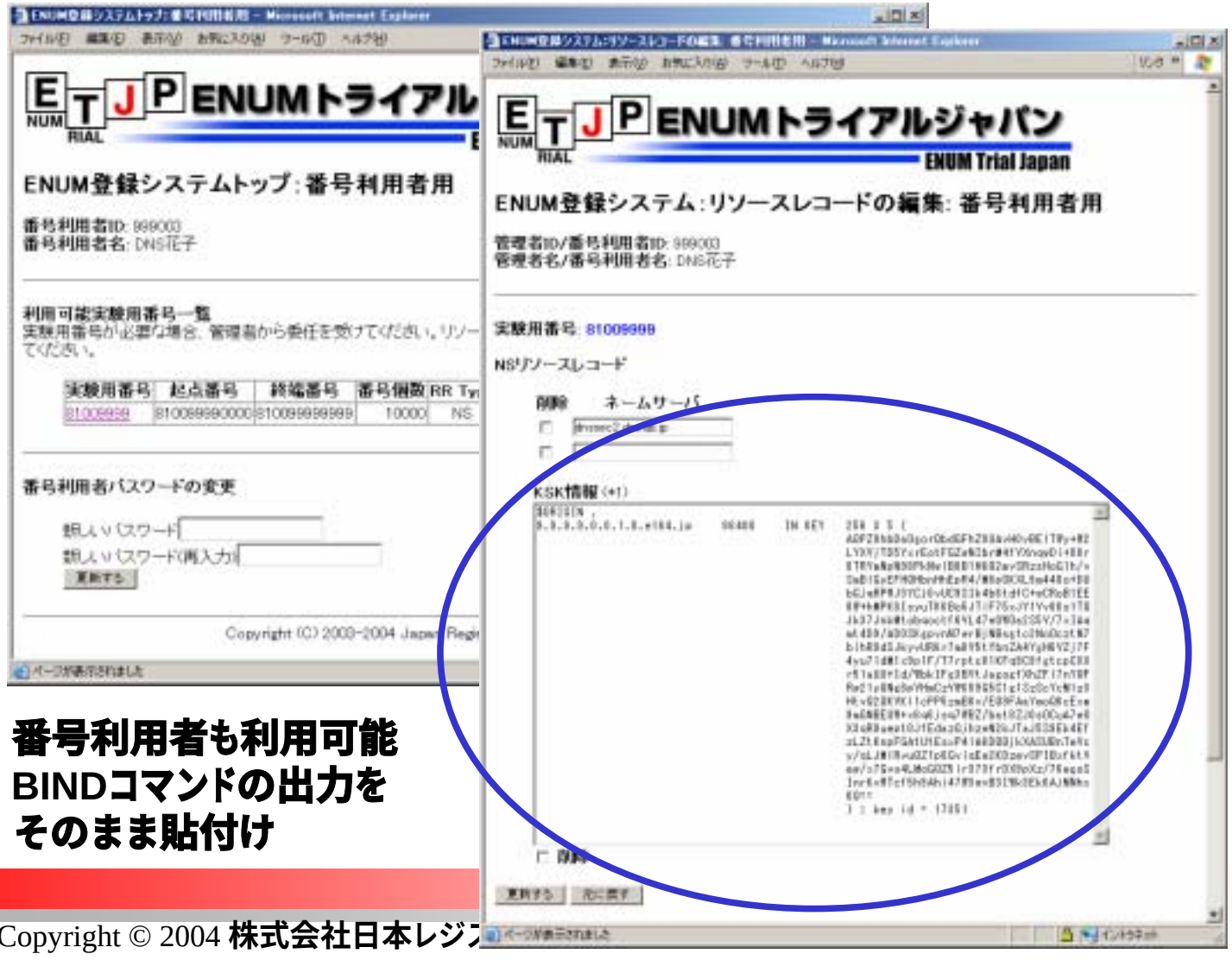
- 実験ドメイン名空間として
  - 0.0.1.8.e164.jp
  - dnssec.jp

  を使用
- 今回はこれより上流の空間はDNSSEC対応しない
  - 従い、これらゾーンのKSK鍵を“DNSSEC対応”キャッシュサーバに認証済み公開鍵として登録
  - キャッシュサーバは、本来は実験参加組織ごとに必要
    - KSK鍵は公開サーバで配布され、設定は比較的容易だが‥
    - DNSSEC対応の公開キャッシュサーバも別途用意
- DNSコンテンツサーバはBIND９の専用バージョン
  - bind9.3.0s20021217

計画概要（2）

- 0.0.1.8.e164.jpでは、委任ドメイン名空間に対しNS,DSを設定
- 各組織は自ゾーン(登録済みの実験用番号)に署名を行う
- dnssec.jp以下も同様
  - 0.0.1.8.e164.jpゾーン以下のNAPTR(URI) 指定のドメイン名として使用されることを想定
  - 参加者ごとに1つのサブドメインが利用可能
  - 但し、こちらの使用は任意

DSの登録



- 番号利用者も利用可能
- BINDコマンドの出力を
  そのまま貼付け

DNSSEC対応ENUMクライアント

- 視覚的に各空間のDNSSEC対応状況を確認できる
  - アプリケーション⇔DNS系でDNSSEC対応となる
- すでにETJP公開済みのENUMクライアントを拡張
  - これまでのものは、NAPTRレコードのURIに応じて事前定義されたWindowsアプリケーションを起動するもの
  - アプリを立ち上げる前にDNSSEC検証状況が見えるよう改修
- 5月完成予定

関連マニュアル

- DNSSEC超入門
- dnssec-intro I-D翻訳
- DNSSECテストベッド(e164.jp配下)
  参加マニュアル
- DNSSECテストベッド(dnssec.jp配下)
  参加マニュアル

※ドキュメントタイトルは若干変更することがあります
※正式なURL等はシステム公開時にお知らせします

ということで・・

- **是非実験にご参加ください！**
- **問題点などがあれば是非ご報告を**
  - **ご意見については可能な限り運用システムに反映します**