

# 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

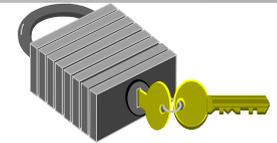
# はじめに

- 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)

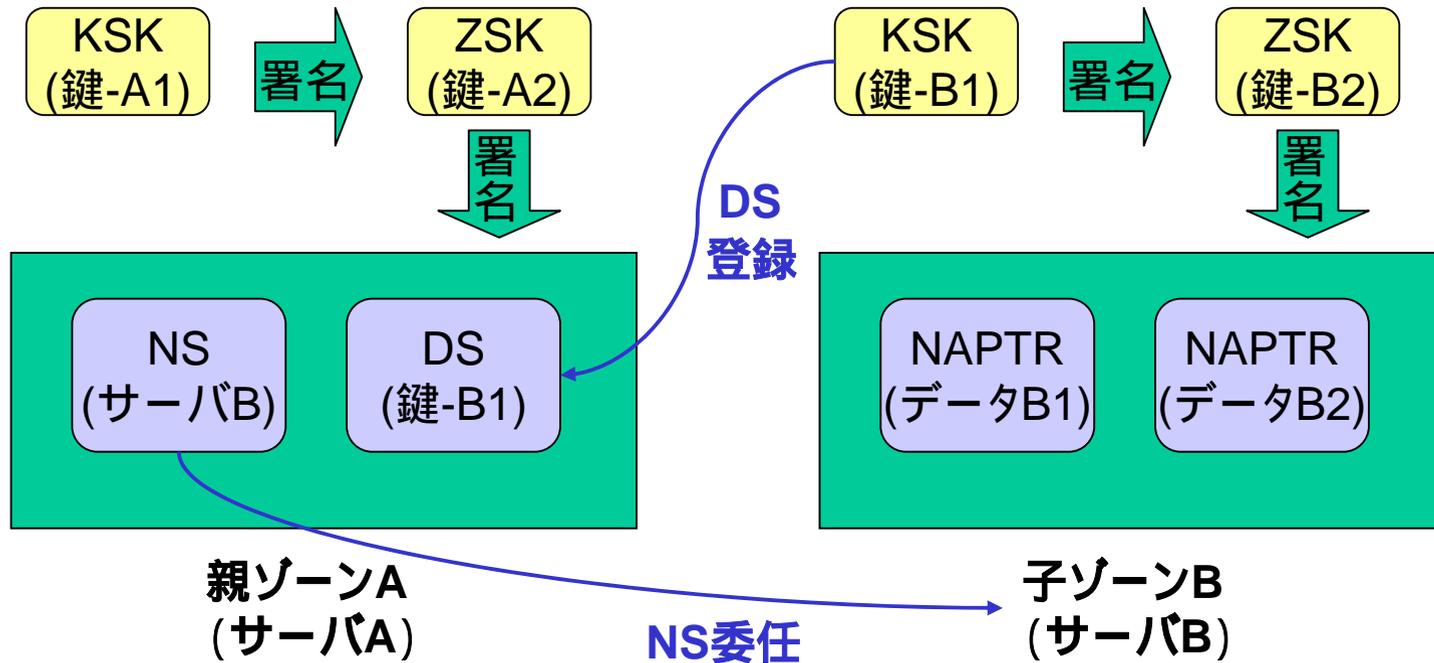


- DNSゾーンに権限を持つ管理者が、公開鍵暗号技術を用いて、自らのゾーン情報に署名を行うDNSの運用方式
  - そのゾーン情報の第3者による改ざん・騙りを検証することが可能となる技術
  - これにより、万一にも騙りを許したくないDNSレコードを守ることが可能となる
  - ENUM番号については、その性格上、関連レコードの正当性を特に保証したいものと定義される

## 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)



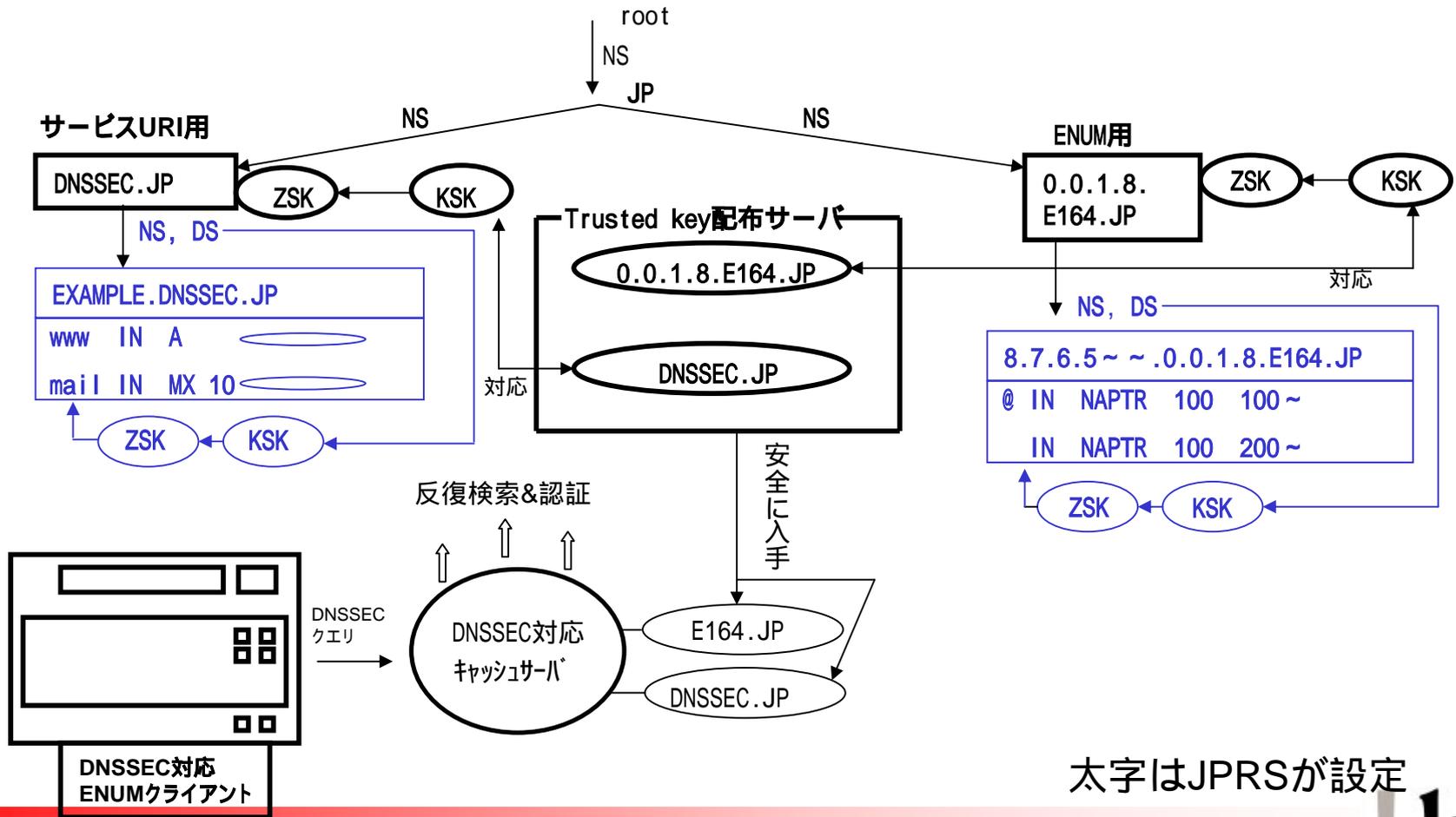
- この方式を各階層の管理者が採用することで、DNSツリー上に存在する全レコードの正当性が保証できるようになる

## 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



# 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、これらの使用は任意

# DSの登録

ENUM登録システムトップ: 番号利用者用

番号利用者ID: 899003  
番号利用者名: DNS花子

利用可能実験用番号一覧  
実験用番号が必要な場合、管理者から委任を受けてください。リソースをご利用ください。

実験用番号	起点番号	終端番号	番号個数	RR	Ty
81008998	81008990000	81008999999	10000	NS	

番号利用者パスワードの変更

記入のパスワード  
記入のパスワード(再入力)  
更新する

Copyright (C) 2000-2004 Japan Registry Service

ENUM登録システム: リソースレコードの編集: 番号利用者用

管理者ID/番号利用者ID: 899003  
管理者名/番号利用者名: DNS花子

実験用番号: 81008998

NSリソースレコード

削除 ネームサーバ

KSK情報 (+)

```

899003
9.9.9.9.0.0.1.8.+184.jp 99488 IN KEY 258 258 (
ADPZ8hd2e3gor0bdGFhZ83a+40v6E1T9y+8Z
LY0Y/TSSY+rGofFGZw62s+rM4Y0vqvD1+88r
8TRVq890959e1Z8D196Z2evZfzshG1h/+
SeB15e2F92hbn9z8z84/M8e30L8w448or88
bG1e8P8J9TC16+U0Z33+4651d1C9eC8e81EE
8P+8P83[zuT88BokJ11F75o+711Yv88x1T8
Jk37Jw8#1ubaoct184L47+898a255V7+18a
w188/a8008gprvADev8jN8up1d8e0cat87
b188d5Ak+y88u18dY81f8n284Y8g8V2J7F
4vu71881c8p1F/T7rpt.c810Fq8C8fqt.c8C8
r81+88+1d/Y8k1F+c8Y1JapocT8u2717n78P
Re21y88e8P8e8z8Y88985C1g1S2o/Y8M1z8
Hv628Y811c8PP8z88+Z88F8w88e8c8e
8e88E88+88w1je87882/8e18Z18d18u47e8
33u88e810J18d8c8J8w88u8J8J838848E1
st218ep881U8E8u8P418838818A8388r8w8
y/vLJ88w8Z18d8v1d8e888ev8P18d8k18
ee/+78e8488e88Z81r878Yr8388e8z878e8d8
1r8e8F8f1888A814788w885188e8k8A8N88e
88r8
1 : key id = 17881)
    
```

- 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