DNSSEC 2010 サマーフォーラム

DNSSEC運用技術SWG活動報告
-DNSSEC運用の困りどころ-

2010年07月21日

NRIセキュアテクノロジーズ株式会社
MSS事業本部
エンタープライズセキュリティサービス部

中島　智広

〒105-7113
東京都港区東新橋1-5-2 汐留シティセンター

目次

1. DNSSEC運用技術SWG活動紹介

2. DNSSEC運用の困りどころ

3. 運用負荷軽減のために

4. まとめ

1. DNSSEC運用技術SWG活動紹介

2. DNSSEC運用の困りどころ

3. 運用負荷軽減のために

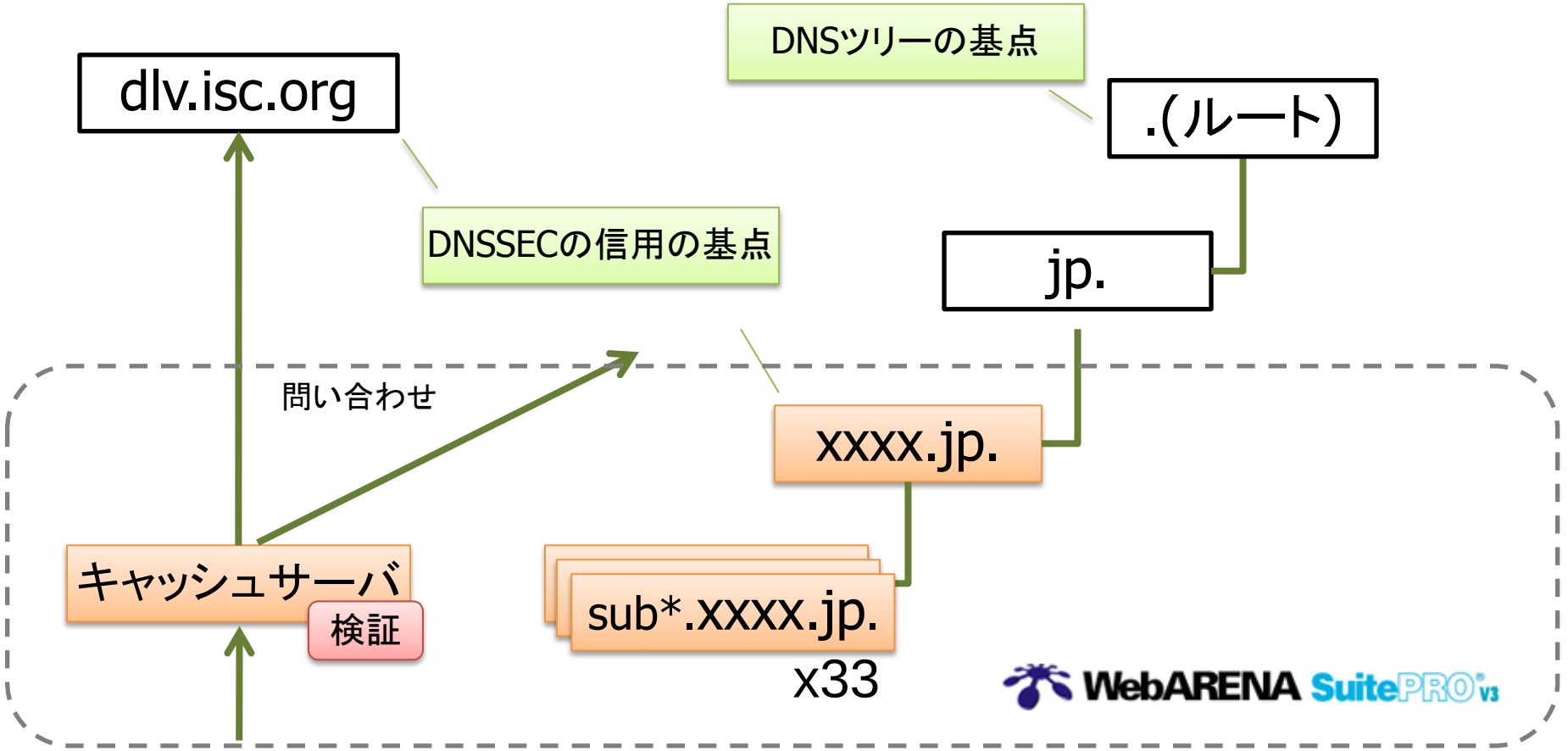
4. まとめ

DNSSEC運用技術SWGとは

- DNSSECの運用ノウハウ共有を目的としたサブワーキンググループ
- DNSSECジャパンメンバー企業を対象にワークショップを開催
  - 実施内容
  1. BINDを用いたDNSSEC導入
  2. BINDを用いた鍵と署名の交換
  3. OpenDNSSECを用いたDNSSEC運用

ワークショップ資料は近日一般公開予定

ワークショップ実施環境



35台のVPSを活用し一人一台ずつDNSSEC対応DNSを構築

1. DNSSEC運用技術SWG活動紹介

2. DNSSEC運用の困りどころ

3. 運用負荷軽減のために

4. まとめ

DNSSEC運用の困りどころ

1. ベンダ提供のパッケージが使えない
2. ミスオペレーションが致命的である
3. 作業ステップが多くコマンドも複雑
4. 鍵ファイルの数が多く管理が煩雑
5. 鍵交換時にはタイミングを考慮したオペレーションが必要

1.ベンダ提供のパッケージが使えない

■各OSで提供されているBINDのバージョン(情報源:distrowatch.com)

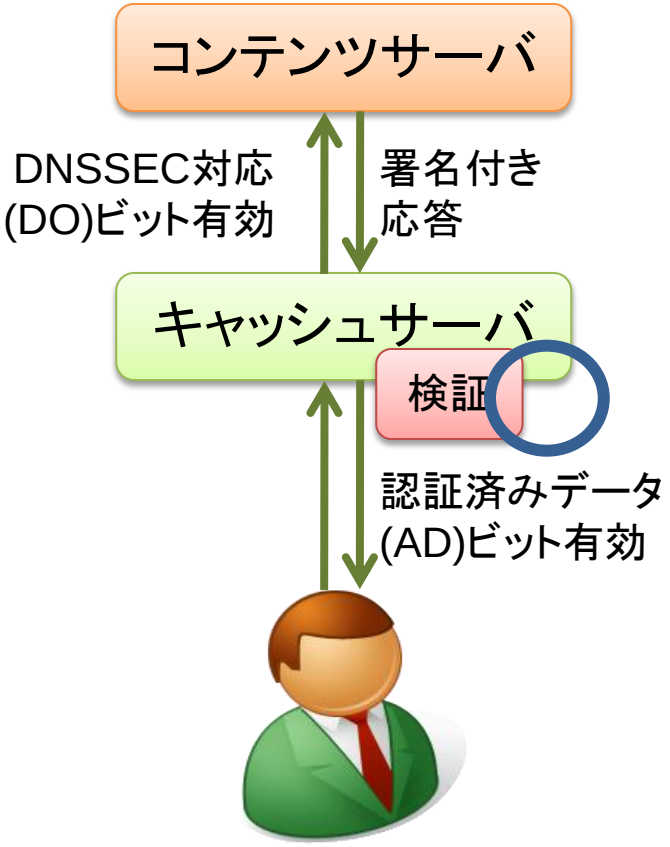
OS	OSバージョン	BINDバージョン
RHEL/CentOS	5.5	9.3.7-P2
	6.0-BETA2	9.7.0-P2
SUSE Linux Enterprise	11-SP1	9.5.0-P2
Solaris	10	9.2.4
openSUSE	11.3	9.7.1
Debian	5.0 lenny	9.5.1
Ubuntu	10.04 LTS lucid	9.7.0-P1
FreeBSD	8.0 RELEASE	9.6.1-P1

RFC5155(NSEC3)は9.6.0以上でサポート
RFC5011(トラストアンカー自動更新)は9.7.0以上でサポート

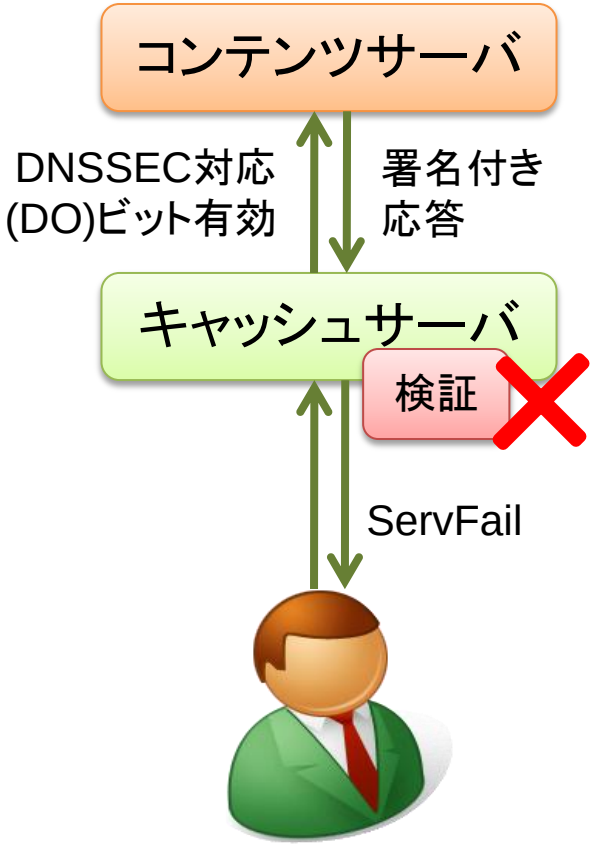
ソースコードからのインストールが必要(サポートは得られない)

2. ミスオペレーションが致命的である

■署名の検証成功時



■署名の検証失敗時



署名の検証失敗時には名前解決そのものが失敗する

3.作業ステップが多くコマンドも複雑

1. 鍵ファイルの生成

```
# dnssec-keygen -a RSASHA256 -b 1024 -q -r /dev/urandom example.jp
# dnssec-keygen -a RSASHA256 -b 2048 -f ksk -q -r /dev/urandom example.jp
```

2. ゾーンファイルへの鍵の登録

```
# cat Kexample.jp+xxxx.key >> example.jp
# cat Kexample.jp+yyyy.key >> example.jp
```

3. ゾーンファイルへの署名

```
# dnssec-signzone  -k Kexample.jp+xxxx -k Kexample.jp+zzzz  example.jp
```

鍵の取り違え等のミスオペレーションが発生する可能性あり

4.鍵ファイルの数が多く管理が煩雑

■DNSSEC導入後のゾーンファイルディレクトリ

```
# ls -1|grep example.jp
Kexample.jp.+008+09076.key
Kexample.jp.+008+09076.private
Kexample.jp.+008+12369.key
Kexample.jp.+008+12369.private
Kexample.jp.+008+22956.key
Kexample.jp.+008+22956.private
Kexample.jp.+008+50350.key
Kexample.jp.+008+50350.private
example.jp
example.jp.signed
```

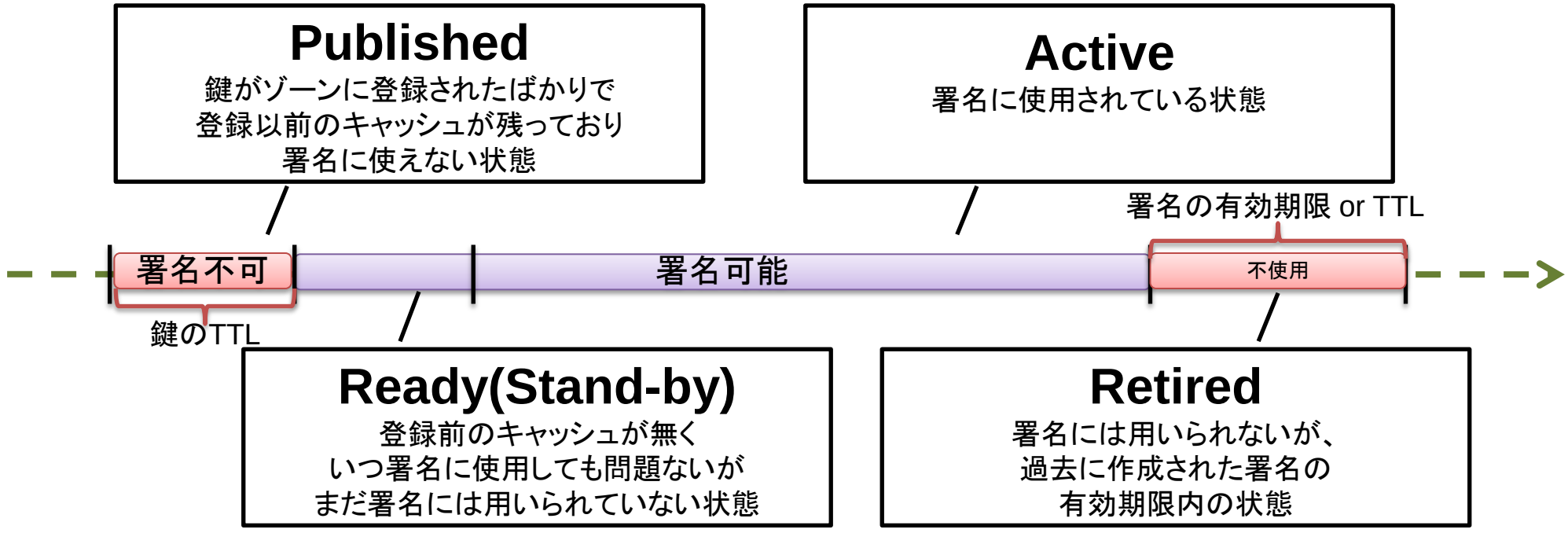
```
# cat Kexample.jp.+008+09076.key
; This is a zone-signing key, keyid 09076,
for example.jp.
; Created: Sun Jul 18 20:01:11 2010
; Publish: Sun Jul 25 20:01:11 2010
; Activate: Sun Jul 25 20:01:11 2010
; Inactive: Sun Aug  1 20:01:11 2010
; Delete: Sun Aug 20 22:25:11 2010
example.jp. IN DNSKEY 257 3 8 (略)
```

※BIND-9.7.xの場合

鍵交換を考慮すると1ゾーンあたり8つの鍵ファイルが必要
さらにファイルの中身を確認しなければ役割がわからない

5.鍵交換時にはタイミングを考慮したオペレーションが必要

■DNSのレコードはキャッシュされるため、
新しい鍵で署名する際にはTTLや署名の有効期限の考慮が必要



[参考]draft-morris-dnsop-dnssec-key-timing-01.txt

タイミングを誤ると検証に失敗し名前解決できない可能性有り

1. DNSSEC運用技術SWG活動紹介

2. DNSSEC運用の困りどころ

3. 運用負荷軽減のために

4. まとめ

運用負担軽減のために

1. SmartSigning
   - BIND-9.7で実装されたDNSSEC運用支援機能

2. OpenDNSSEC+SoftHSM
   - DNSSEC運用の全課程を自動化することを目的として作られた運用支援ツール

ご参考までに二つの方法例をご紹介します

1.SmartSigning

- 鍵ファイル作成時に時間情報を付加し、
  これに基づいて自動的に鍵と署名の登録を行う仕組み

1. 鍵の生成

```
# dnssec-keygen  -a RSASHA256 -b 1024 -q -r /dev/urandom ¥
-P +3600 -A +86400 -I +864000 -D +867600  example.jp
```

例)1時間後にゾーンに登録、24時間後に署名に利用開始
10日後に署名に用いられなくなり、その1時間後にゾーンから削除される鍵

2. ゾーンファイルへの鍵の登録と署名

```
# dnssec-signzone -S example.jp
```

鍵ファイルの生成が正しく行われていれば、
運用担当者は鍵ファイルや鍵交換のタイミングの考慮が不要

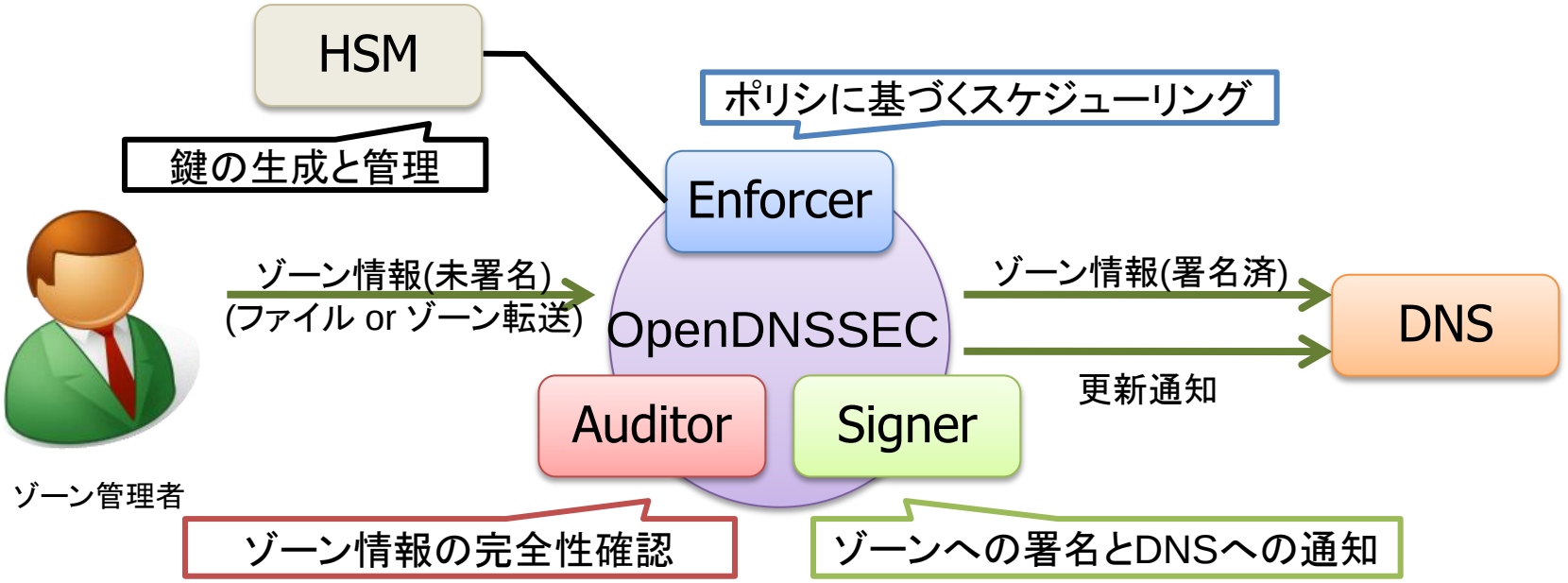
SmartSigning実行例

```
# dnssec-keygen  -a RSASHA256 -b 1024 -q -f ksk -r /dev/urandom ¥
-P +0 -A +0 -I +864000 -D +867600  example.jp          ←KSK鍵ペア作成
# dnssec-keygen  -a RSASHA256 -b 1024 -q -r /dev/urandom ¥
-P +0 -A +0 -I +864000 -D +867600  example.jp          ←ZSK鍵ペア作成
# dnssec-keygen  -a RSASHA256 -b 1024 -q -r /dev/urandom ¥
-P +0 -A +300 -I +864000 -D +867600  example.jp        ←ZSK鍵ペア作成
# dnssec-signzone -S example.jp                        ←SmartSigning
Fetching KSK 30169/RSASHA256 from key repository.
Fetching ZSK 46638/RSASHA256 from key repository.
Key example.jp/RSASHA256/46638: Delaying activation to match the DNSKEY TTL.

Fetching ZSK 9429/RSASHA256 from key repository.
Verifying the zone using the following algorithms: RSASHA256.
Zone signing complete:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 1 stand-by, 0 revoked
example.jp.signed
```

2.OpenDNSSEC + SoftHSM

- DNSSEC運用の全課程を自動化することを目的として作られた運用支援ツール
- 鍵の管理、ゾーンの再署名、鍵のロールオーバーをスケジューリングして自動実行
- PKCS#11に準拠したHSMの利用を前提とし、代替となるSoftHSMも併せて提供
- 必要とするライブラリ類が新しく旧環境への導入は敷居が高い



ゾーン管理者はDNSSECを意識することなくゾーン管理が可能

1. DNSSEC運用技術SWG活動紹介

2. DNSSEC運用の困りどころ

3. 運用負荷軽減のために

4. まとめ

まとめ

- DNSSEC導入にあたってはミスオペレーションを防ぐため
  人間の手によるオペレーションを減らす工夫が必要
- スクリプトによる自動化や運用支援ツールの導入を推奨