

JPRS技術セミナー —DNSSEC導入実践編—

使えます！ OpenDNSSEC

2010年7月

株式会社日本レジストリサービス(JPRS)

内容

1. 概要
2. 準備
3. インストール
4. ポリシー定義
5. 初期設定
6. 運用



凡例

- 各種設定
 - JPRS検証環境における設定は「~@JPRS」と略記する
- コマンド入力
 - 入力時に固定文字列のものは通常フォント、可変パラメータの具体例は斜体フォントで示す

コマンド名 パラメータ
 - 入力時に具体的な値に置き換える可変パラメータは[]で括る

コマンド名 [パラメータ]
- コマンド出力
 - タイプライタ体で表記する

logmessagelogmessagelogmessagelogmessag
- コマンド実行ユーザ
 - 一般ユーザでの実行は先頭行に%、ルートでの実行は先頭行に#を付けて表記する

% コマンド名
コマンド名
- 設定ファイル
 - 追加・変更した部分は **下線付き赤字** で表記する

<PIN>5678</PIN>
 - 削除した部分は標準字体(グレー)で表記する

<!-- 削除タグ -->

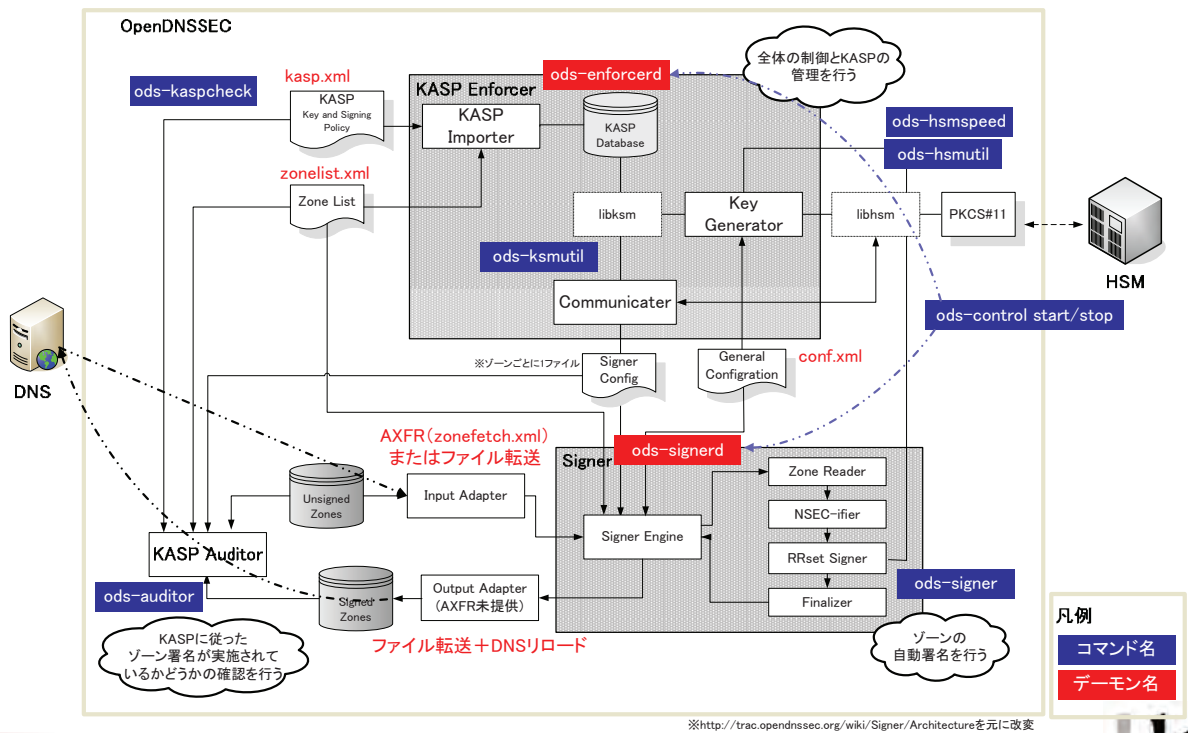


1. 概要

OpenDNSSECとは

- ゾーン署名プロセスを簡易化したBSDライセンスのオープンソースソフトウェア
 - <http://www.opendnssec.org/>
 - 開発者: .se、John A Dickinson、Kirei、NLnetLabs、Nominet、SIDN、SURFnet
- 主な特長
 - 秘密鍵管理のためHSMを使用(PKCS#11に対応)
 - 署名鍵の状態管理を自動化
 - 署名鍵のプールが可能(署名鍵生成コストを時間的に分散)
 - 複数ゾーンで署名鍵を共有可能
 - ゾーン再署名、署名鍵ロールオーバーを自動化
 - 既存署名の再利用(署名負荷を低減)
 - SOAシリアルの自動管理(指定値を使用することも可能)
 - ゾーン監査機能を実装
 - 少ないカスタマイズで実際的な運用パラメータ設定が可能
 - 別システムからの移行が容易(既存のゾーンファイルがそのまま使える、BIND署名鍵のインポートができる、etc.)
- OpenDNSSECの利用TLDなど
 - .uk (Nominet)、.se (IIS)、.dk (DK Hostmaster)、*.arpa (ICANN)

システム構成



主要コンポーネント

KASP Enforcer

- 予め設定された署名鍵管理ポリシーに従い運用を行う

Signer

- ゾーンの署名を行う

KASP Auditor

- ゾーン署名がKASPに従って適切に行われているか監視を行う

※KASP (Key and Signing Policy)

ゾーン署名の方法、鍵のサイズ・使用期間・アルゴリズム等のパラメータを記述したポリシー



入出力

入力

未署名ゾーンのOpenDNSSECへの転送

- A) ファイル転送
- B) AXFR

設定ファイル(conf.xml、zonefetch.xml)で設定

出力

署名済みゾーンのDNSサーバへの転送

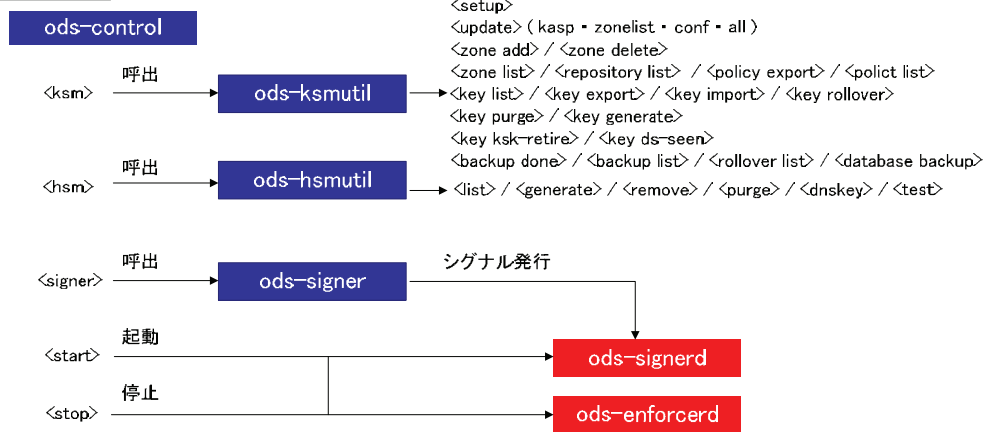
- A) ファイル転送+リロードコマンド
設定ファイル(conf.xml)で設定
- B) (AXFR)

今後実装予定



コマンド体系

主要コマンド



ユーティリティコマンド

- ods-auditor
- ods-hmspeed
- ods-kaspcheck

凡例	
ods-control	コマンド名
ods-signerd	デーモン名
<ksm>	<引数名>



コマンドの分類

主要コマンド

ods-control	ods-ksmutil、ods-hsmutil、ods-signerへのパイプコマンドとods-enforcerd、ods-signerdの起動・停止
ods-ksmutil	各種設定ファイルの更新(ods-ksmutil update)や署名鍵管理(ods-ksmutil backup doneなど)
ods-hsmutil	署名鍵の生成(ods-hsmutil generate)、削除(ods-hsmutil remove)
ods-signer	署名の実行(ods-signer sign)

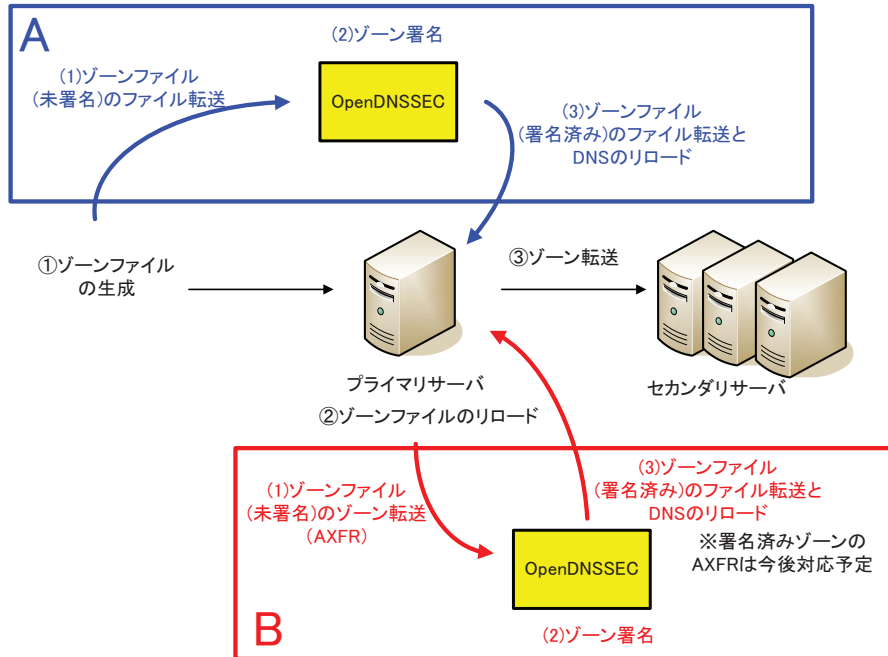
ユーティリティコマンド

ods-auditor	システムがポリシー(kasp.xml)に従っているか監査
ods-hsmspeed	HSMのパフォーマンステスト
ods-kaspcheck	設定ファイル(conf.xmlとkasp.xml)が正しく設定されているか確認

2. 準備

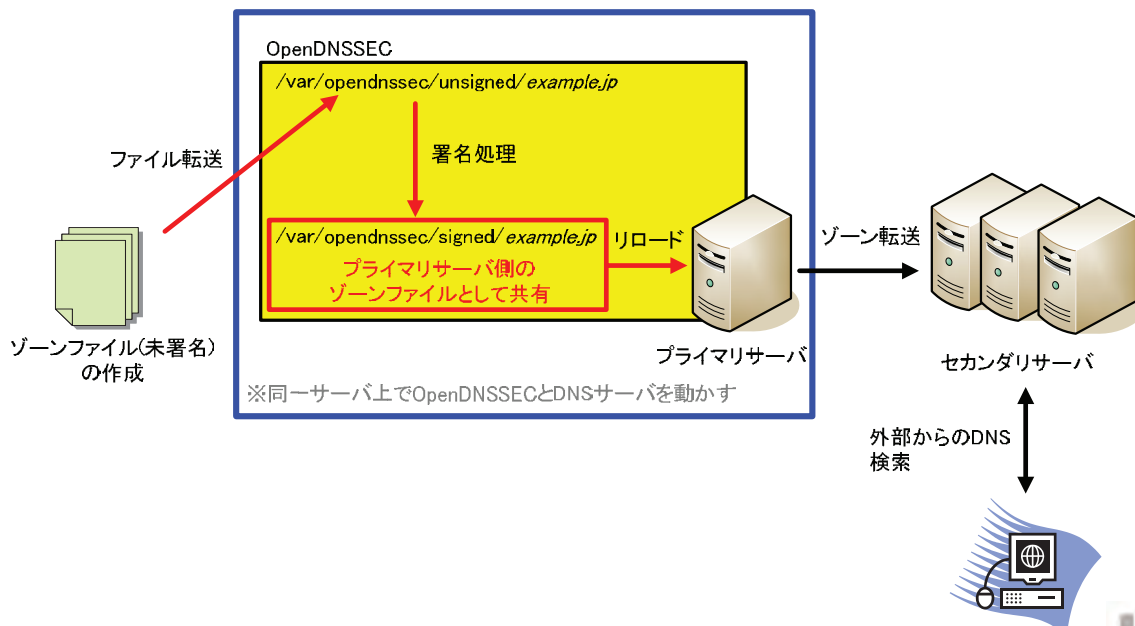
運用モードの選択

運用モードは下記の2種類から選択



運用モード@JPRS

運用モードAを選択



ハードウェアの選択

- OpenDNSSECでは複数ゾーンの運用時にはマルチスレッド処理になっているが、単一ゾーンの運用時にはマルチスレッドに対応していない
- そのため、単一の巨大なゾーンを運用する場合には大量のコアを搭載したCPUよりも速いCPUを選ぶことが重要
- OpenDNSSECはゾーンサイズの7倍近くのディスク容量を使用する
- H/W@JPRS
 - VMWare @ Dual Core AMD Opteron 2GHz CPU x 1
 - 1GB Memory
 - 16GB Disk Capacity

OSの選択

- OpenDNSSECがサポートするプラットフォーム
 - Debian 5.0
 - Mac OS X 10.5
 - OpenBSD 4.4
 - Red Hat Enterprise Linux 5
 - Solaris 10
 - Ubuntu 8.0.4
- FreeBSD、NetBSDでも利用可能
 - <http://pkgsrc.se/wip/opendnssec>
- OS@JPRS
 - 今回はサポート対象外のFedora12を選択

HSMの選択

- HSM(Hardware Security Module)とは
 - 秘密鍵などの秘密情報を管理するハードウェア機器
 - HSMとのやり取りはPKCS(Public Key Certification Standard)#11インタフェース(PKIの公開鍵処理系のAPI規格)を介して行う必要がある
- OpenDNSSECでは秘密鍵管理にHSMを使用する
 - OpenDNSSECパッケージにPKCS#11インタフェースが実装されている
- OpenDNSSEC開発プロジェクトの一部として、HSMをソフトウェアでエミュレートした「SoftHSM」がリリースされている
- HSM@JPRS
 - 今回はSoftHSMを利用

依存パッケージ

- Idns(ver1.0.0以上)
- libxml2、libxml2-dev、libxml2-utils(ver2.6.16以上)
- ruby、rubygems
- dnsruby(ver1.45以上)
- libopenssl-ruby
- sqlite3、libsqlite3、libsqlite3-dev(ver3.3.9以上)
 - またはmysql-client、libsqlclient15、libmysqlclient15-dev(ver5.0.3以上)
- python
- pythons-4suite-xml
- それぞれのモジュールのインストール方法については以下を参照
 - <http://trac.opendnssec.org/wiki/Signer/Using/Installation/Dependencies>

パッケージ導入@JPRS

- Fedora12の導入後、以下を追加インストール
 - ※libxml2、ruby、pythonはFedora12の導入時にインストール済み
 - rubygems(yumコマンド使用)
 - dnsruby(gemコマンド使用)
 - python-4suite-xml(yumコマンド使用)
 - 以下はソースからビルドした
 - Idnsを/usr/local/libにインストール
 - sqlite3を/usr/local/binにインストール

3. インストール

SoftHSM1.1.4のインストール(1/3)

- SoftHSMインストールに先立ち、下記パッケージがインストールされているか確認
 - SQLite3(ver3.4.2以上)
 - Botan(ver1.8.5以上)

※Fedora12ではソースからビルドする必要があった

```
% wget http://files.randombit.net/botan/v1.8/Botan-1.8.8.tgz
% tar xzvf Botan-1.8.8.tgz
% cd Botan-1.8.8
% ./configure.py
% make
% make check
# make install
```

SoftHSM1.1.4のインストール(2/3)

1. コンフィグレーション

```
% wget http://www.opendsnsec.org/files/source/softhsm-1.1.4.tar.gz
% tar xzvf softhsm-1.1.4.tar.gz
% cd softhsm-1.1.4
% ./configure
```

コンフィグオプション

```
--with-botan=PATH   Botanのパスのprefixを指定
--with-sqlite3=PATH  SQLite3のパスのprefixを設定
--enable-64bit       64bitでコンパイル
--with-loglevel=INT  ログレベルの設定 (0=ログ無し 1=エラー 2=警告
                    3=インフォ 4=デバック; デフォルトはINT=3)
--prefix=DIR         インストール先のディレクトリ(デフォルトはDIR=/usr/local)
```

SoftHSM1.1.4のインストール(3/3)

2. インストール

```
% make
# make install
```

3. /etc/softhsm.confへスロットを追加

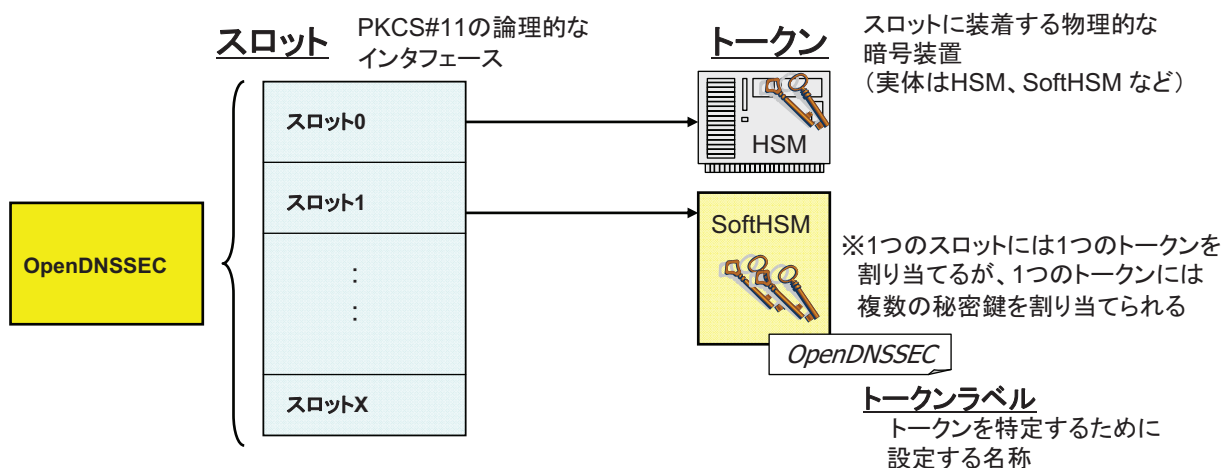
```
% vi /etc/softhsm.conf
0: /var/softhsm/slot0.db
```

4. softhsmツールを使ってトークンを初期化

```
% softhsm --init-token --slot 0 --label "OpenDNSSEC"

Type in SO PIN and user PIN.
```

補足:用語について



種別	個数	主な用途
SO(Security Officer)PIN	トークン毎に1個	ユーザを作成するためのPIN (運用時には使わない)
ユーザPIN	トークン毎に1個	秘密鍵へのアクセス

OpenDNSSEC1.1.0のインストール(1/2)

- ソースコードの取得

```
% wget http://www.opendnssec.org/files/source/opendnssec-1.1.0.tar.gz
```

- コンフィグレーションとインストール

```
% tar xzvf opendnssec-1.1.0.tar.gz  
% cd opendnssec-1.1.0  
% ./configure  
% make  
# make install
```

OpenDNSSEC1.1.0のインストール(2/2)

- コンフィグオプション

--disable-auditor	※KASP Auditorのビルドを無効化(デフォルトは有効)
--enable-epclient	※EPPクライアントのビルドを有効化(デフォルトは無効、実験的)
--with-database-backend	※DBのバックエンドの選択(SQLite3またはMySQL、デフォルトはSQLite)

- インストール後
 - Linuxユーザはダイナミックリンクをリビルドする

```
# ldconfig [library-path [library-path ...]]
```

4. ポリシー定義

ポリシー定義 (1/3)

- 署名鍵／署名ポリシーを定義する

No	パラメータ	タグ名	値
1	署名のパラメータ	<Signatures>	-
1.1	署名実施間隔	<Resign>	PT2H
1.2	署名リフレッシュ期間	<Refresh>	P3D
1.3	署名有効期間	<Validity>	P7D
1.4	署名有効期間のゆらぎ	<Jitter>	PT12H
1.5	署名有効期間の開始オフセット	<InceptionOffset>	PT3600S
2	不在証明のパラメータ	<NSEC>または<NSEC3>	<NSEC3>
2.1	NSEC3 ソルトの再生成間隔	<Resalt>	P100D
2.2	NSEC3 アルゴリズム	<Algorithm>	1
2.3	NSEC3 繰り返し回数	<Iterations>	5
2.4	NSEC3 ソルトの長さ	<Salt>	8

ポリシー定義 (2/3)

No	パラメータ	タグ名	値
3	署名鍵のパラメータ	<Keys>	-
3.1	TTL	<TTL>	PT3600S
3.2	使用停止猶予期間	<RetireSafety>	PT3600S
3.3	使用開始猶予期間	<PublishSafety>	PT3600S
3.4	削除猶予期間	<Purge>	P14D
3.5	KSKのパラメータ	<KSK>	-
3.5.1	アルゴリズム/鍵長	<Algorithm>	8 (7)/2048ビット
3.5.2	使用期間	<Lifetime>	P1Y
3.5.3	リポジトリ	<Repository>	SoftHSM
3.5.4	スタンバイさせる署名鍵数	<Standby>	1
3.6	ZSKのパラメータ	<ZSK>	-
3.6.1	アルゴリズム/鍵長	<Algorithm>	8 (7)/1024ビット
3.6.2	使用期間	<Lifetime>	P30D
3.6.3	リポジトリ	<Repository>	SoftHSM
3.6.4	スタンバイさせる署名鍵数	<Standby>	1

※下線付き赤字: 今回変更した値 (): デフォルト値

ポリシー定義 (3/3)

No	パラメータ	タグ名	値
4	ゾーンのパラメータ	<Zone>	-
4.1	セカンダリの同期遅延見込み	<PropagationDelay>	PT43200S
4.2	SOAのパラメータ	<SOA>	-
4.2.1	TTL	<TTL>	PT3600S
4.2.2	ネガティブキャッシュ	<Minimum>	PT900S (PT3600S)
4.2.3	SOAシリアル形式	<Serial>	unixtime
5	親ゾーンのパラメータ	<Parent>	-
5.1	親ゾーンの反映遅延見込み	<PropagationDelay>	PT1200S (PT9999S)
5.2	DSのパラメータ	<DS>	-
5.2.1	TTL	<TTL>	PT86400S (PT3600S)
5.3	SOAのパラメータ	<SOA>	-
5.3.1	TTL	<TTL>	PT86400S (PT172800S)
5.3.2	ネガティブキャッシュ	<Minimum>	PT900S (PT10800S)
6	ゾーン監査の有無	<Audit>	-

※下線付き赤字: 今回変更した値 (): デフォルト値

5. 初期設定

- 5-1. 設定ファイルの編集
- 5-2. ゾーンファイルの設定
- 5-3. OpenDNSSECの初期化

5-1. 設定ファイルの編集

設定ファイル

ポリシーを/etc/opendnssec/に配置される4種類の設定ファイルに反映する

conf.xml

- OpenDNSSEC全体の設定
- 署名鍵リポジトリ、ログレベル、システムパス、実行ユーザ、システムデータベース、DNS同期方式の設定

kasp.xml

- 署名鍵・署名ポリシー (Key and Signing Policy: KASP) の設定
- 署名パラメータ、タイミングパラメータなど

zonelist.xml

- ゾーン名、ゾーンに適用する署名ポリシー、ゾーンデータ入出力の設定

zonefetch.xml (オプション)

- ゾーン転送の設定

日付・時間の表記

- ISO8601形式を使用
(ex) “P3Y6M4DT12H30M5S” → 3年6ヶ月4日12時間30分5秒の期間
P...期間を示す
Y...年
M...月
D...日
T...時間を示す
H...時
M...分
S...秒
- OpenDNSSECでは以下の定義となる
 - 1ヶ月 = 31日
 - 1年 = 365日

conf.xmlの編集(その1)

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- $Id: conf.xml.in 3192 2010-04-14 20:51:42Z rb $ -->

<Configuration>

  ①<RepositoryList>
    ②<Repository name="SoftHSM">
      ③<Module>/usr/local/lib/libsofthsm.so</Module>
      ④<TokenLabel>OpenDNSSEC</TokenLabel>
      ⑤<PIN>5678</PIN>
    </Repository>
  <!--
    ②<Repository name="sca6000">
      ③<Module>/usr/lib/libpkcs11.so</Module>
      ④<TokenLabel>Sun Metaslot</TokenLabel>
      ⑤<PIN>test:1234</PIN>
      ⑥<Capacity>1000</Capacity>
      ⑦<RequireBackup/>
    </Repository>
  -->
</RepositoryList>

```

個々のリポジトリに関する設定

conf.xmlの編集(その1)

- ① <RepositoryList>
 - リポジトリを列挙(複数リポジトリを設定可能)
- ② <Repository>
 - リポジトリ名を定義
- ③ <TokenLabel>
 - HSM(トークン)を特定するトークンラベルを指定
- ④ <Module>
 - リポジトリを管理するダイナミックリンクライブラリを指定
- ⑤ <PIN>
 - トークンに設定したパスワード(ユーザPIN)を指定
- ⑥ <Capacity>(オプション)
 - トークンに保管する署名鍵の最大数を設定
- ⑦ <RequireBackup/>(オプション)
 - バックアップしていない署名鍵を使わせない

conf.xmlの編集(その2)

<pre> <Common> <Logging> ①<Syslog><Facility>local0</Facility></Syslog> </Logging> ②<PolicyFile>/etc/opensnsec/kasp.xml</PolicyFile> ③<ZoneListFile>/etc/opensnsec/zonelist.xml</ZoneListFile> ④<!-- <ZoneFetchFile>/etc/opensnsec/zonefetch.xml</ZoneFetchFile> --> </Common> </pre>	システム設定ファイル等の指定
<pre> <Enforcer> <!-- ⑤<Privileges> <User>opensnsec</User> <Group>opensnsec</Group> </Privileges> --> ⑥<Datastore><SQLite>/var/opensnsec/kasp.db</SQLite></Datastore> ⑦<Interval>PT3600S</Interval> <!-- <ManualKeyGeneration/> --> <!-- the <DelegationSignerSubmitCommand> will get all current DNSKEYs (as a RRset) on standard input --> <!-- <DelegationSignerSubmitCommand>/usr/local/sbin/epclient </DelegationSignerSubmitCommand> --> </Enforcer> </pre>	KASP Enforcerの動作に関する設定

conf.xmlの編集(その2)

- ① <Syslog>
 - <Facility>でログレベル(local0からlocal7まで)を設定
- ② <PolicyFile>
 - kasp.xmlのパスを設定
- ③ <ZoneListFile>
 - zonelist.xmlのパスを設定
- ④ <ZoneFetchFile>(オプション)
 - zonefetch.xmlのパスを設定
- ⑤ <Privileges>(オプション)
 - Enforcerの実行ユーザ(<User>)・グループ(<Group>)を設定
- ⑥ <Datastore>
 - KASP Enforcerデータを持つデータベース(<SQLite>または<MySQL>)を指定する
 - ただしMySQLは実験レベル
- ⑦ <Interval>
 - 署名鍵の状態遷移を行う頻度を設定
 - 署名鍵の使用期間が月単位であれば、1日から1週間の<Interval>指定でよい

conf.xmlの編集(その3)

```

<Signer>
<!-- ①<Privileges>
      <User>opendssec</User> <Group>opendssec</Group>
      </Privileges> -->
②<WorkingDirectory>/var/opendssec/tmp</WorkingDirectory>
③<WorkerThreads>8</WorkerThreads>
-->
<!-- the <NotifyCommand> will expand the following variables:
      %zone    the name of the zone that was signed
      %zonefile the filename of the signed zone -->
<!--
      <NotifyCommand>/usr/local/bin/my_nameserver_reload_command</NotifyCommand>
-->
④<NotifyCommand>/usr/sbin/rndc reload %zone</NotifyCommand>
-->
</Signer>
<Auditor>
<!-- ①<Privileges>
      <User>opendssec</User> <Group>opendssec</Group>
      </Privileges> -->
②<WorkingDirectory>/var/opendssec/tmp</WorkingDirectory>
</Auditor>
</Configuration>

```

Signerの動作に関する設定

プライマリサーバに対して発行するコマンドの指定

KASP Auditorの動作に関する設定

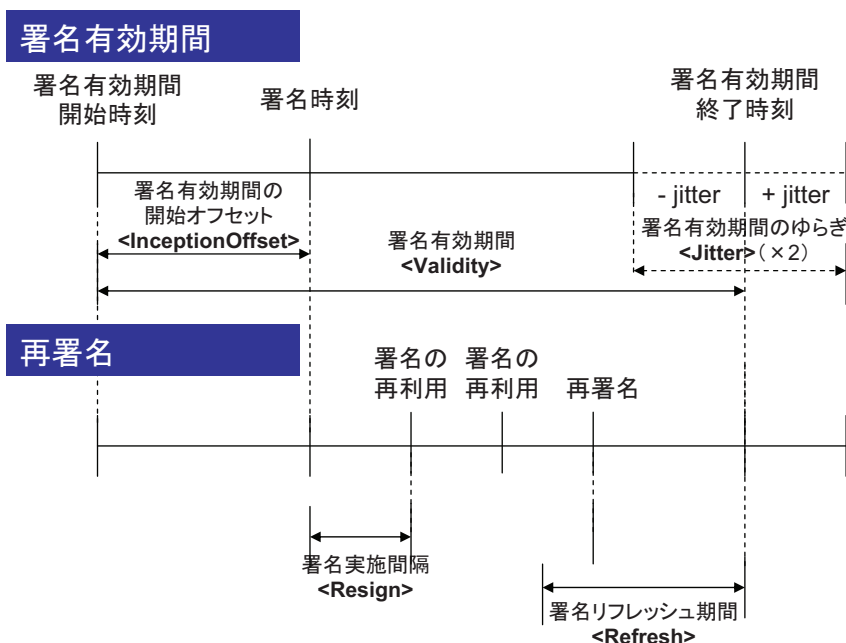
conf.xmlの編集(その3)

- ① <Privileges>(オプション)
 - Signer、Auditorの実行ユーザ(<User>)・グループ(<Group>)を設定
- ② <WorkingDirectory>
 - Signer、Auditorが作成する一時ファイルのパスを指定
- ③ <WorkerThreads>
 - 起動するsignerプロセスの上限数を指定
 - 1つのsignerプロセスは一度に1つのゾーンを扱うことができる
- ④ <NotifyCommand>(オプション)
 - DNSの同期を行う際にSignerが呼び出すコマンドを設定
 - 下記変数が実行時に展開される
 - %zone・・・署名したゾーンの名前
 - %zonefile・・・署名したゾーンファイル名

一般ユーザでのOpenDNSSEC運用

- 今回は一般ユーザでOpenDNSSECを運用することにした
 - この際、conf.xmlの<Privileges>のコメントを外すほか、下記フォルダのオーナーを当該ユーザに変更する必要があった
 - /var/opendssec
 - /var/softsm
 - /etc/opendssec

署名関連のタイミングパラメータ



kasp.xmlの編集(その1)

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- $Id: kasp.xml.in 3192 2010-04-14 20:51:42Z rb $ -->
<KASP>
  ①<Policy name="default">
    <Description>A default policy that will amaze you and your friends</Description>
    <Signatures>
      ②<Resign>PT2H</Resign>
      ③<Refresh>P3D</Refresh>
      ④<Validity>
        <Default>P7D</Default>
        <Denial>P7D</Denial>
      </Validity>
      ⑤<Jitter>PT12H</Jitter>
      ⑥<InceptionOffset>PT3600S</InceptionOffset>
    </Signatures>
    ⑦<Denial>
      ⑧<NSEC3>
        <!-- <OptOut> -->
        <Resalt>P100D</Resalt>
        <Hash>
          <Algorithm>1</Algorithm>
          <Iterations>5</Iterations>
          <Salt length="8"/>
        </Hash>
      </NSEC3>
    </Denial>
  </Policy>
</KASP>
  
```

署名に関する設定

不在証明の設定

kasp.xmlの編集(その1)

- ① <Policy>
 - name属性でポリシー名を指定
- ② <Resign>
 - 署名実施間隔を設定
- ③ <Refresh>
 - 署名のリフレッシュ期間を指定
 - リフレッシュ期間に入ったら署名の再利用をやめて再署名する
- ④ <Validity>
 - <Default>にはNSEC、NSEC3レコード以外に対する署名有効期間を設定
 - <Denial>にはNSEC、NSEC3レコードに対する署名有効期間を設定
- ⑤ <Jitter>
 - 全ての署名が同時に有効期限切れにならないよう、署名有効時間に加減算する値を設定
 - 加減算される値は-<Jitter> ~ +<Jitter>の乱数値
- ⑥ <InceptionOffset>
 - 署名有効期間の開始時刻として署名時刻から遡る時間を設定
- ⑦ <Denial>
 - 不在証明方式としてNSEC3またはNSECを指定
 - NSECを用いる場合は<NSEC></NSEC>と記述(値なし)
- ⑧ <NSEC3>
 - <OptOut/>(オプション)・・・Optoutを有効化
 - <Resalt>・・・ハッシュ生成のためのソルト値を再生成する間隔を設定する
 - <Algorithm><Iteration><Salt>・・・ハッシュアルゴリズムのパラメータを設定する

kasp.xmlの編集(その2)

```

<Keys>
  <!-- Parameters for both KSK and ZSK -->
  ①<TTL>PT3600S</TTL>
  ②<RetireSafety>PT3600S</RetireSafety>
  ②<PublishSafety>PT3600S</PublishSafety>
  ③<!-- <ShareKeys/> -->
  ④<Purge>P14D</Purge>

  <!-- Parameters for KSK only -->
  <KSK>
  ⑤<Algorithm length="2048">8</Algorithm>
  ⑥<Lifetime>P1Y</Lifetime>
  ⑦<Repository>SoftHSM</Repository>
  ⑧<Standby>1</Standby>
  </KSK>

  <!-- Parameters for ZSK only -->
  <ZSK>
  ⑤<Algorithm length="1024">8</Algorithm>
  ⑥<Lifetime>P30D</Lifetime>
  ⑦<Repository>SoftHSM</Repository>
  ⑧<Standby>1</Standby>
  ⑨<!-- <ManualRollover/> -->
  </ZSK>
</Keys>
  
```

署名鍵の共通情報の設定

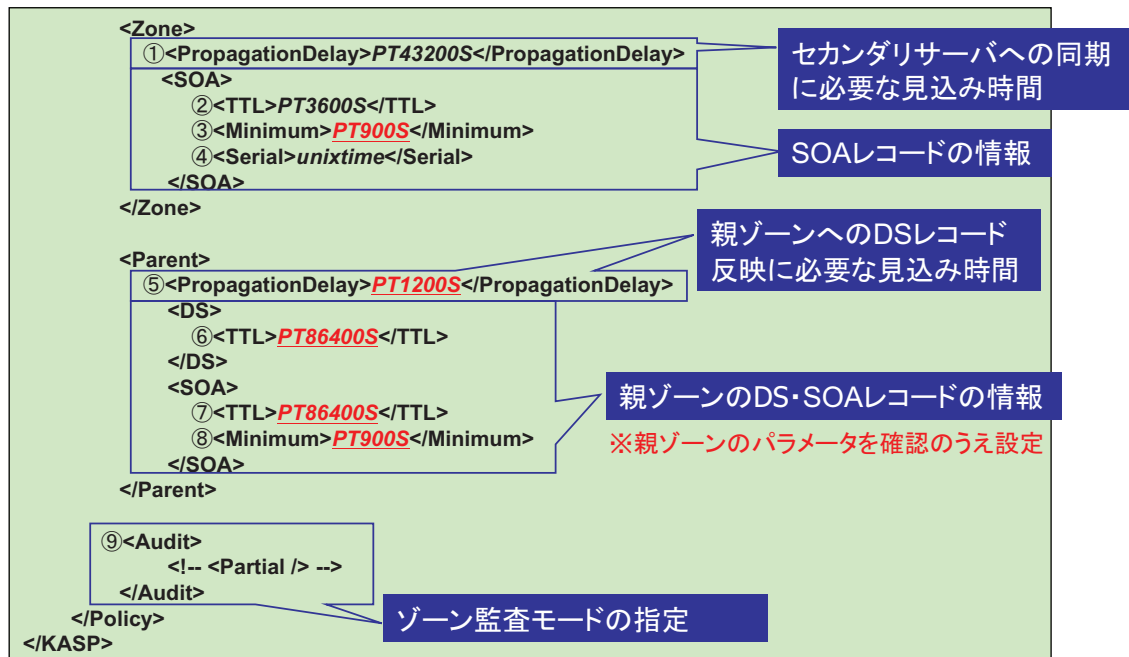
KSKパラメータの指定

ZSKパラメータの指定

kasp.xmlの編集(その2)

- ① <TTL>
 - 署名鍵(DNSKEY RR)のTTLを設定
- ② <PublishSafety><RetireSafety>
 - まだ有効でない・すでに無効な署名鍵で署名しないための使用猶予期間を設定
- ③ <ShareKeys/>(オプション)
 - 複数ゾーンで署名鍵を共有する場合に設定
- ④ <Purge>
 - 使用停止した署名鍵をデータベースから自動削除する期間を指定
- ⑤ <Algorithm>
 - 署名鍵のアルゴリズムを設定
- ⑥ <Lifetime>
 - 署名鍵の使用期間を設定
- ⑦ <Repository>
 - 使用するリポジトリを設定
- ⑧ <Standby>
 - スタンバイさせる署名鍵数を設定
 - ・ 署名鍵の危殆化が疑われる場合にその署名鍵を速やかに削除できるようにするための機能
- ⑨ <ManualRollover/>(オプション)
 - 手動ロールオーバーを指定

kasp.xmlの編集(その3)



kasp.xmlの編集(その3)

- ① <PropagationDelay>
 - セカンダリサーバへの同期に必要な見込み時間を設定
- ② <TTL>
 - 署名済みゾーンのSOAレコードのTTLを設定
- ③ <Minimum>
 - 署名済みゾーンのネガティブキャッシュ値を設定
- ④ <Serial>
 - 署名済みゾーンのシリアル番号の形式を設定
 - counter、datecounter、unixtime、keep
- ⑤ <PropagationDelay>
 - 親ゾーンへのDSレコードの反映遅延見込み時間を設定
- ⑥ <TTL>
 - 親ゾーンのDSレコードのTTLを設定
- ⑦ <TTL>
 - 親ゾーンのSOAレコードのTTLを設定
- ⑧ <Minimum>
 - 親ゾーンのネガティブキャッシュ値を設定
- ⑨ <Audit>
 - ゾーン監査モードを指定
 - <Partial/>(オプション)でゾーンの部分監査指定が可能となる(大規模ゾーンなどで有用)

zonelist.xmlの編集

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- $Id: zonelist.xml.in 2890 2010-02-24 23:00:11Z jakob $ -->
<ZoneList>
  <!--
    ①<Zone name="example.jp">
      ②<Policy>default</Policy>
      ③<SignerConfiguration>/var/opendnssec/signconf/example.jp.xml</SignerConfiguration>
      ④<Adapters>
        <Input>
          <File>/var/opendnssec/unsigned/example.jp</File>
        </Input>
        <Output>
          <File>/var/opendnssec/signed/example.jp</File>
        </Output>
      </Adapters>
    </Zone>
  -->
</ZoneList>
  
```

ゾーン署名に使用するポリシー (kasp.xmlで定義)

SignerConfigファイル (自動生成) のパス

ゾーンデータの
入出力パス

zonelist.xmlの編集

- ① <Zone>
 - name属性でゾーン名を指定
- ② <Policy>
 - ゾーン署名に使用するポリシー (kasp.xmlで定義) を指定
- ③ <SignerConfiguration>
 - EnforcerからSignerへ渡す自動生成ファイル (SignerConfig) のパスを設定
 - このファイルはOpenDNSSECのコンポーネント間での一時ファイルで、ユーザが編集することはない
- ④ <Adapters>
 - <Input><File>
 - 入力ゾーンデータ (未署名ゾーン) のファイルパスを設定
 - <Output><File>
 - 出力ゾーンデータ (署名済みゾーン) のファイルパスを設定

zonefetch.xmlの編集

※運用モードBのみ

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- $Id: zonefetch.xml.in 2735 2010-01-28 14:11:27Z matthijs $ -->

<ZoneFetch>
  <!-- where to listen for notifies -->
  <!-- DEFAULT: do not listen to notify on specific address -->
  ①<NotifyListen><Port>53</Port></NotifyListen>

  <!-- default inbound AXFR settings
  (per zone setting not yet implemented) -->
  <Default>
    <!-- TSIG secret for inbound AXFR -->
    <!-- DEFAULT: don't use TSIG -->
    ②<!-- <TSIG>
      <Name>secret.example.jp.</Name>
      <!-- http://www.iana.org/assignments/tsig-algorithm-names -->
      <Algorithm>hmac-sha256</Algorithm>

      <!-- base64 encoded secret -->
      <Secret>sw0nMPCswVbes1tmQTm1pcMmpNRK+oGMYN+qKNR/BwQ=</Secret>
    </TSIG-->

    <!-- address of host to request AXFR from -->
    <!-- incoming NOTIFY has to match this address as well -->
    <!-- DEFAULT: none -->
    ③<RequestTransfer>
      <IPv4>192.0.2.2</IPv4><Port>53</Port>
    </RequestTransfer>
  </Default>
</ZoneFetch>
  
```

Notifyを待つポート番号を設定

プライマリサーバ(未署名)のTSIG共有鍵を設定

プライマリサーバ(未署名)のアドレスとポート番号を設定



zonefetch.xmlの編集

- ① <NotifyListen>
 - NOTIFYメッセージを待つインターフェースのアドレスとポートを指定
- ② <TSIG>
 - TSIG共有鍵のゾーン名、アルゴリズム、鍵情報を設定
- ③ <RequestTransfer>
 - プライマリサーバ(未署名)のアドレス、ポートを設定
 - 複数のIPv4/IPv6アドレスを設定可能



5-2. ゾーンファイルの設定

ゾーンファイルの準備

- ゾーンファイルの置場所
 - /var/opendnssec/unsigned/(zonelist.xmlに指定)にゾーンファイルを置く
- フォーマット
 - 未署名のゾーンファイル
 - DNSKEYレコードは設定不要
 - マルチライン、コメントの記述が可能
 - ゾーンファイルに空行を含めない
- ディレクティブ
 - \$ORIGIN、\$TTL、\$INCLUDEをサポート
- サポートするレコードの種類
 - 下記以外全てのIANAで指定されたレコードタイプをサポート

未対応なもの	ATMA、APL、EID、NIMILOC、HIP、SINK、NINFO、RKEY、TA
Obsoleteなもの	MD、MF、WKS、GPOS、SIG、KEY、NXT、A6、NSAP-PTR
ゾーンレコードでないもの	NULL、OPT、TKEY、TSIG、IXFR、AXFR、MAILB、MAILA、*

- Unknownレコード(RFC3597)の運用も可能

example.jp.	IN	TYPE1	¥# 4 0A000001
-------------	----	-------	---------------

ゾーンファイルの例

```

$ORIGIN .
$TTL 3600          ; 1 hour
example.jp        IN SOA      ns.example.jp. example.jp. (
                    2010070800 ; serial
                    43200      ; refresh (12 hours)
                    3600       ; retry (1 hour)
                    1814400    ; expire (3 weeks)
                    900        ; minimum (15 minutes)
                    )
example.jp        NS       ns.example.jp
$ORIGIN example.jp.
ns                A       192.168.0.50
www               A       192.168.0.51
smtp              A       192.168.0.52
pop3              A       192.168.0.53
ftp               A       192.168.0.54
    
```

5-3. OpenDNSSECの初期化

データベースの初期化

- KASP Enforcerデータベース (/var/opendnssec/kasp.db) を作成する
 - 下記コマンドはデータベースを上書きしてしまうため、初期化を行う場合のみ使用する

```
% ods-ksmutil setup
*WARNING* This will erase all data in the database; are you sure? [y/N] y
SQLite database set to: /var/opendnssec/kasp.db
fixing permissions on file /var/opendnssec/kasp.db
zonelist filename set to /etc/opendnssec/zonelist.xml.
kasp filename set to /etc/opendnssec/kasp.xml.
Repository SoftHSM found
No Maximum Capacity set.
RequireBackup NOT set; please make sure that you know the potential problems of using
keys which are not recoverable
Policy default found
Zone example.jp found
Policy set to default.
Added zone example.jp to database
```

署名鍵の初期生成

```
% ods-ksmutil key generate --policy default --interval 1
SQLite database set to: /var/opendnssec/kasp.db
Key sharing is Off
HSM opened successfully.
Created KSK size: 2048, alg: 8 with id: dbc18471f3952b2d10f2e62e4bfe0c3b in repository:
SoftHSM and database.
Created KSK size: 2048, alg: 8 with id: 98726a4744dd7b544ef51454e430dafd in repository:
SoftHSM and database.
Created ZSK size: 1024, alg: 8 with id: f6aa77739ae2c81a211f4596fbbb55e0 in repository:
SoftHSM and database.
Created ZSK size: 1024, alg: 8 with id: b2e1a51d854296f959c64cb33c7b6567 in repository:
SoftHSM and database.
all done! hsm_close result: 0
```

- policyオプションにはkasp.xmlで定義したポリシー名を指定
- intervalオプションには事前生成する鍵の世代を指定
 - 安全性の高い署名鍵の生成には時間がかかるため、予め生成しプールしておくことで緊急事態に備える
- 初回起動の際、KSK状態遷移を手動で行う必要がある(後述)

6. 運用

主な運用シーン

- 起動と停止
- ログの確認
- ポリシーの変更
- ゾーンデータの変更
- ゾーンの追加・削除
- 署名鍵のバックアップ
- 署名鍵の状態確認
- 署名鍵の状態遷移
- 署名鍵のロールオーバー操作
- 署名鍵の日付指定ロールオーバー
- ゾーンの監査

起動と停止

起動

Signer(/usr/local/sbin/ods-signerd)

Enforcer(/usr/local/sbin/ods-enforcerd)

```
% ods-control start
Starting signer engine...
connecting to /var/run/opendnssec/engine.sock
OpenDNSSEC signer engine version 1.1.0
Zone list updated: 0 removed, 1 added, 0 updated
running as pid 21167
Starting enforcer...
OpenDNSSEC ods-enforcerd started (version 1.1.0), pid 21169
```

停止

```
% ods-control stop
Stopping enforcer...
Stopping signer engine..
connecting to /var/run/opendnssec/engine.sock
Sent stop command to engine
```

ログの確認

- OpenDNSSECのログはsyslogで管理される
 - その他の手段は今後提供される予定

(ログメッセージ例)

```
ods-enforcerd: ERROR: Trying to make non-backed up ZSK active
when RequireBackup flag is set
```

→状況:<RequireBackup/>指定があるのにバックアップが行われていないためZSKのロールオーバーに失敗した

→対処法:ZSKのバックアップを実施する

```
ods-enforcerd: Error getting db lock
```

→状況:SQLiteのDBロックを取得できずDB操作が失敗した

→対処法:データベースのあるフォルダの権限を確認する

ポリシーの変更

```
% vi /etc/opendnssec/kasp.xml (パラメータ設定値の変更など)
% ods-kaspcheck
```

```
% ods-control stop
```

```
% ods-ksmutil update all
```

```
SQLite database set to: /var/opendnssec/kasp.db
zonelist filename set to /etc/opendnssec/zonelist.xml.
kasp filename set to /etc/opendnssec/kasp.xml.
Repository SoftHSM found
No Maximum Capacity set.
RequireBackup set.
Policy default found
Zone example.jp found
Policy set to default.
```

```
% ods-control start
```

ゾーンデータの変更 (1/2)

- ゾーンデータ変更後に署名コマンドを実行する

```
% ods-signer sign example.jp
connecting to /var/run/opendnssec/engine.sock
Zone scheduled for immediate resign
```

syslog出力

```
Jul 08 13:29:30 ts ods-signerd: Received command: 'sign example.jp'
Jul 08 13:29:30 ts ods-signerd: Scheduling task to sign zone example.jp,
zone in progress, scheduling as soon as possible
```

出力ファイル

デフォルト設定であれば/var/opendnssec/signed/example.jp、
/var/opendnssec/signconf/example.jp.xmlが更新される

DNSリロード

conf.xmlで<NotifyCommand>が指定されていればDNSのリロードが
行われる

ゾーンデータの変更 (2/2)

- 署名済みゾーン (/var/opendnssec/signed/example.jp)

```
; Signed on 2010-07-08 03:48:59
example.jp. 3600 IN SOA ns.example.jp. postmaster.example.jp. (
1278528539 43200 3600 1814400 900 )
ns.example.jp. 3600 IN A 192.168.0.50
ns.example.jp. 3600 IN RRSIG A 8 3 3600 20100708120007 20100707182424 38338 example.jp (
umBlKjCeJTC51oNZoSvCDTHbiSUT8GG20Ea44tulN3fMltItyXFKJ9ad4FgdsU0yXCSFfaXm1uaGDkoyWgKy+ku
+oymzUHNNeo4nByBIXSWld0KONGzC/kJpANDy71RoDUSW+dyQ/KDSFz4niNajxBe07oHq5pQg+g0e9Vux+E= ) ;id = 38338)
03trplebrkja52ncrgfab2ao88ikbah4.example.jp. 900 IN NSEC3 1 0 5 38d7dd5ba2450e04 (
9uq2orau44skvqh9k0onvf50cve4fqgm A RRSIG )
03trplebrkja52ncrgfab2ao88ikbah4.example.jp. 900 IN RRSIG NSEC3 8 3 900 20100708110510 (
20100707182424 38338 example.jp. I+Mq2xYongQpNSvpYXUpN5NbAaPHHIEDTGGohG3EqodXOGdLDXLdJPM
F3brAIHQ+TpxQcBg19b0d0TkaHbrEh2fpNKqBLBbU0Hl cgnYmhE2pvTgMF81JTaSbq/KkJH6h60gV6/3GRhySvGr
Fu2D5knpB2Rmd7K87s6cFEReq4Q= ) ;id = 38338)
smtp.example.jp. 3600 IN A 192.168.0.52
smtp.example.jp. 3600 IN RRSIG A 8 3 3600 20100708105921 20100707182424 38338 (
example.jp. oiqkMe16eJRCTSIHQ5mfQReuKh74bsosorshDj5K7fI+5MQKcNqoM591sH4DHobCO9IDw5MPHbq8
MSFVdO6kwm+fyTranj+kXk9mF6fKFyz2RKApxTb6RRHXaljfjwOMkeJQkyUv5terjh+PYvXbgl1nm2N4xULG71yj
BBI4gkk= ) ;id = 38338)
9uq2orau44skvqh9k0onvf50cve4fqgm.example.jp. 900 IN NSEC3 1 0 5 38d7dd5ba2450e04 (
i6i7ik6umbq2nqosjc0hvd338kj821oh A RRSIG )
9uq2orau44skvqh9k0onvf50cve4fqgm.example.jp. 900 IN RRSIG NSEC3 8 3 900 20100708105619 (
20100707182424 38338 example.jp. 4gkrz4v9+kK7gJXL8edrExEawLuK9RbXVDLzYqMmKaSMEE8e65ysktC
o+nRQ6HRiIQ2GtBxz6oSU4QJRyJ8Dk5oPABDYuTxR70NDz2tVtYaPaFvU7EYfi7a2hayIA8cyM0Y3E+av4yQ1Drr
Tb0fnXGFBjtwwQgVXTLE48SUNU3g= ) ;id = 38338)
pop3.example.jp. 3600 IN A 192.168.0.53
~~以下省略~~
```

ゾーンの追加・削除 (1/2)

- ステップ1:ゾーンファイルを準備する
例: /var/opendnssec/unsigned/example2.jp を作成(または削除)
- ステップ2:ゾーンをシステムに組み込む
→以下の2通りの方法が存在

① zonelist.xmlを手編集する

```
% vi /etc/opendnssec/zonelist.xml (該当ゾーンの記述を追加または削除)
% ods-control stop
% ods-ksmutil update all
% ods-control start
```

ゾーンの追加・削除 (2/2)

② ods-ksmutilコマンドを実行する

追加

```
% ods-ksmutil zone add --zone example2.jp --policy default --signerconf
/var/opendnssec/signconf/example2.jp.xml --input
/var/opendnssec/unsigned --output /var/opendnssec/signed
zonelist filename set to /etc/opendnssec/zonelist.xml.
SQLite database set to: /var/opendnssec/kasp.db
Imported zone: example2.jp
% ods-control stop
% ods-ksmutil update all
% ods-control start
```

削除

```
% ods-ksmutil zone delete --zone example2.jp
SQLite database set to: /var/opendnssec/kasp.dbzonelist filename set to
/etc/opendnssec/zonelist.xml.
connecting to /var/run/opendnssec/engine.sock
Zone list updated: 1 removed, 0 added, 0 updated
Configurations updated: 1 config errors: 0
% ods-control stop
% ods-ksmutil update all
% ods-control start
```

署名鍵のバックアップ

```
% ods-control stop
% ods-ksmutil backup done
SQLite database set to: /var/opendnssec/kasp.db
Marked all repositories as backed up at 2010-07-09 10:09:19
% ods-control start
```

- 署名鍵の確実なバックアップのためシステムを停止する
- conf.xmlに<RequireBackup/>を設定した場合、バックアップされていない署名鍵を署名に使用できないことに注意

署名鍵の状態確認

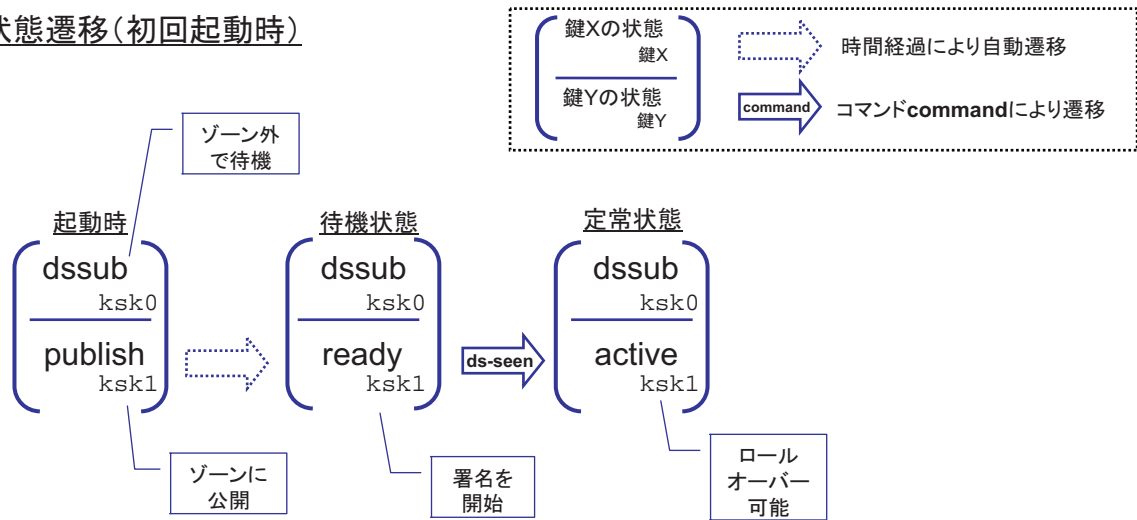
```
% ods-ksmutil key list -verbose
SQLite database set to: /var/opendnssec/kasp.db
Keys:
Zone:      Keytype:   State:      Date of next transition:  CKA_ID:      Repository:   Keytag:
example.jp KSK        active      2010-07-09 16:33:01      8ff0b9e9a**** SoftHSM       42329
example.jp KSK        dsready     When required           763400491**** SoftHSM       65101
example.jp ZSK        retire      2010-07-09 07:22:53      354906284**** SoftHSM       21303
example.jp ZSK        active      2010-07-09 13:16:53      3a345d9aa**** SoftHSM       42961
example.jp ZSK        publish     2010-07-09 15:48:21      d66ee4e2e**** SoftHSM       29031
```

署名鍵の状態

状態	DNSKEY	署名 (KSK)	署名 (ZSK)	意味
publish	○	×	×	ゾーンに公開した直後
ready	○	○	×	ゾーンに公開後、十分時間が経過した
active	○	○	○	ゾーン署名に使用されている
retire	○	×	×	署名生成を終了したが、十分時間が経過していない
dssub (KSKのみ)	×	×	—	スタンバイKSKのDSが上位ゾーンで未公開
dspublish (KSKのみ)	×	×	—	スタンバイKSKのDSを上位ゾーンに公開した直後
dsready (KSKのみ)	×	×	—	スタンバイKSKのDSを上位ゾーンに公開後、十分時間が経過した
keypublish (KSKのみ)	×	○	—	スタンバイKSKの使用を開始する

署名鍵の状態遷移(1/4)

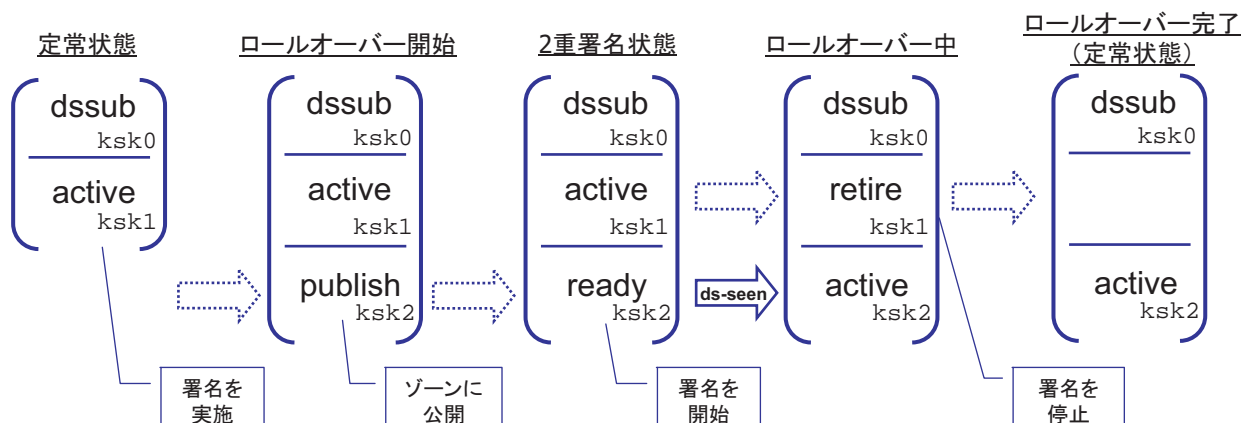
KSK状態遷移(初回起動時)



- ・待機状態時にexportコマンド(後述)を用いて、上位ゾーンへDSLレコード登録(+ksk1)を行う
- ・待機状態時に手動でds-seenコマンド(後述)を発行することで定常状態に移行させておく

署名鍵の状態遷移(2/4)

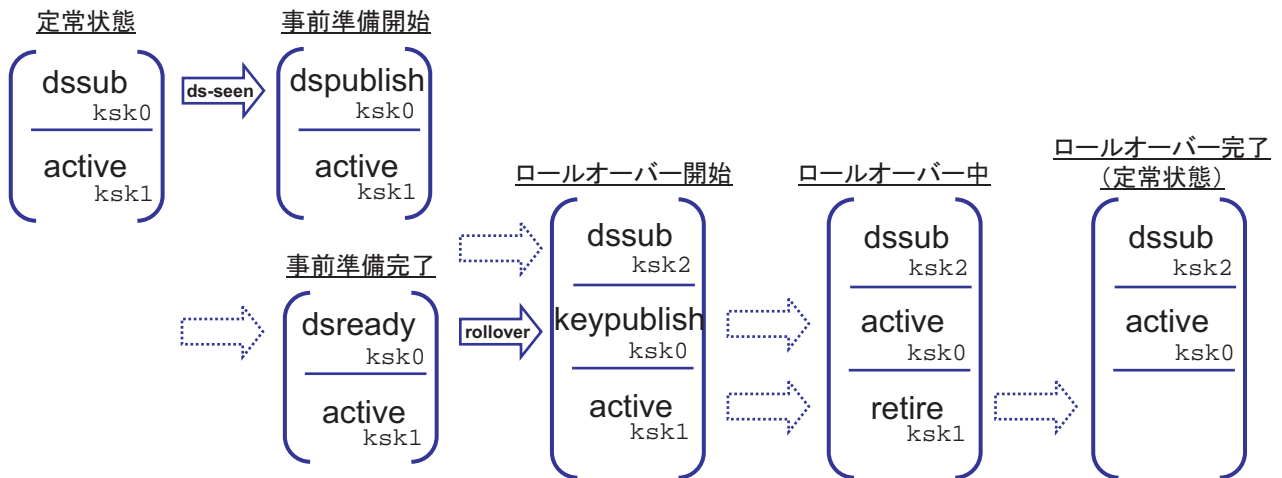
KSK状態遷移(通常ロールオーバー)



- ・通常ロールオーバーではスタンバイKSK(ksk0)は使用しない
- ・2重署名状態まではスケジュールに従い自動的に遷移する
- ・2重署名状態時にexportコマンド(後述)を用いて上位ゾーンのDSLレコードを更新する(ksk1→ksk2)
- ・2重署名状態時にds-seenコマンド(後述)を発行することでロールオーバーを完了する

署名鍵の状態遷移(3/4)

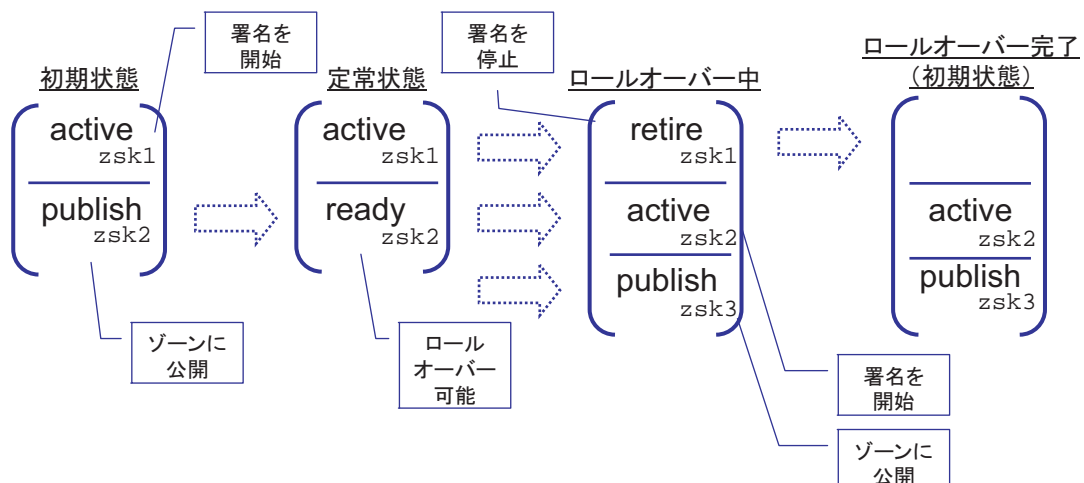
KSK状態遷移(緊急ロールオーバー)



- ・定常状態時にexportコマンド(後述)を用いて、上位ゾーンへDSレコード追加を行う(+ksk0)
- ・定常状態時にds-seenコマンド(後述)を発行することで事前準備を完了する
- ・事前準備完了後、rolloverコマンド(後述)を発行することで緊急ロールオーバーを開始できる
- ※事前準備完了までは緊急ロールオーバー実施前の任意の時点に行っておく

署名鍵の状態遷移(4/4)

ZSK状態遷移



- ・すべての状態遷移が自動で行われる
- ・rolloverコマンド(後述)を用いて緊急ロールオーバーを開始することも可能

署名鍵のロールオーバー操作 (1/2)

署名鍵のロールオーバーには手動操作を伴うものがある

① KSKの通常ロールオーバー

exportコマンド: 上位ゾーンに登録するDSレコードを出力する

```
% ods-ksmutil key export --zone example.jp --keystate active --ds
SQLite database set to: /var/opendnssec/kasp.db

;active KSK DS record (SHA1):
example.jp.      3600      IN          DS          28745 8 1
86d3c2083bd5e391971460b52b9658e651b3d93a ; xocit-fybib-mivut-homan-cihec-
gumer-hupin-kukev-kugyr-fikof-paxex

;active KSK DS record (SHA256):
example.jp.      3600      IN          DS          28745 8 2
2680e3382ef25ca4fc2a2d4629c854b957b0cb5ed73e438000c5d901ff4e70ee ; xenim-
bamof-muriz-dolep-gyzod-purag-kopos-myhor-nihar-bedyh-vihuf-vobom-bebys-
hekyb-cezog-vasev-voxyx
```

署名鍵のロールオーバー操作 (2/2)

ds-seenコマンド: 通常ロールオーバー時に特定状態への遷移を行う

```
% ods-ksmutil key ds-seen --zone example.jp --keytag 5462
SQLite database set to: /var/opendnssec/kasp.db
Found key with CKA_ID 8207bbd41fc1bb0c36f52e6864329f8c
Key 8207bbd41fc1bb0c36f52e6864329f8c made into standby
```

② 緊急ロールオーバー

rolloverコマンド: KSK・ZSKの緊急ロールオーバーを行う

```
% ods-ksmutil key rollover --zone example.jp --keytype KSK
SQLite database set to: /var/opendnssec/kasp.db
INFO: 0 ksks available in 'generate' state (need 1) - unable to promote
until more keys generated
WARNING: key rollover not completed as there are no keys in the 'ready'
state; ods-enforcerd will try again when it runs next
```

※ZSKの場合は -keytype ZSKを指定

署名鍵の日付指定ロールオーバー

ex.) 毎月1日に署名鍵のロールオーバーを実施する

- kasp.xmlにおいて手動ロールオーバーを指定
 - <ManualRollover/>タグを追加
- rolloverコマンドをcron jobに登録

```
% crontab -l  
0 0 1 * * ods-ksmutil key rollover --zone example.jp --keytype ZSK
```

ゾーンの監査

- Signerがポリシーに従って動いているか確認する(自動)
 - ゾーンの再署名が行われる際などに実施される
 - ods-auditorが検知したエラーはsyslogに出力
- ゾーンを監査する(手動)

```
% ods-auditor -z example.jp  
Auditor started  
Auditor starting on example.jp  
6: SOA differs : from 2010070801 to 1278529909  
6: Auditing example.jp zone : NSEC3 SIGNED  
3: Key (38338) has gone straight to active use without a prepublished phase  
3: Key (46541) has gone straight to active use without a prepublished phase  
6: Finished auditing example.jp zone  
Auditor found errors - check log for details
```

参考資料

■ OpenDNSSEC関連Webサイト

OpenDNSSECホームページ:

<http://www.opendnssec.org/>

マニュアル:

<http://www.opendnssec.org/documentation/>

バグレポート:

<http://trac.opendnssec.org/newticket>

■ OpenDNSSEC関連メーリングリスト

一般的な質問:

opendnssec-user@lists.opendnssec.org

リリース情報:

opendnssec-announce@lists.opendnssec.org

■ 署名鍵の状態に関する文書

“DNSSEC Key Timing Considerations”

<http://tools.ietf.org/id/draft-morris-dnsop-dnssec-key-timing-02.txt>

Q and A

