資料更新：2015/11/19

既存リゾルバをDNSSEC対応に移行する方法

2015年11月19日

Internet Week 2015 今日から始めるDNSSECバリデーション

九州通信ネットワーク株式会社 (QTNet)

末松慶文 (yo_suematsu at qtnet.co.jp)

自己紹介

- 末松慶文(すえまつ よしぶみ)
  - DNSを含むサーバ関連の構築と運用/保守などを7-8年くらい。
- 九州通信ネットワーク(QTNet)
  - 児童ポルノブロッキングの自動化やってます
    - 実装と運用自動化について(QTNet 久米)
    http://dnsops.jp/event/20130718/20130718-kume-jipo-blocking-kume-1.pdf
  - キャッシュDNSのDNSSEC Validateやってます
  - DNSの耐障害性強化に向けてJPRSと共同研究を開始
    JPRS: JPRSが新gTLD「.jprs」でDNSの耐障害性強化に向けてISPとの共同研究を開始　http://jprs.co.jp/press/2015/150713.html
    QTNet: JPRSとの共同研究について　http://www.qtnet.co.jp/massmedia/2015/20150713_2.html

本発表の内容

- 前提条件
- 注意事項
  - 時刻同期について
  - BINDバージョンについて
  - OpenSSLバージョンについて
  - ネットワークの問題について
- 各種設定方法
  - ・トラストアンカーの入手と登録について
    - BINDに付属する、トラストアンカーを使用する場合
    - トラストアンカーを自動更新したい場合
    - マニュアルでトラストアンカーを設定したい場合
  - ・移行と導入について
- まとめ

DNSSECで実現すること

- DNSSECで実現すること
  - 出自と完全性の保証
    -> DNS応答が正しいことの検証

- DNSSECでは実現できないこと
  - 通信路の暗号化やDNS応答の暗号化は行いません。

ここで取り扱う

DNSSECバリデーションとは

- クライアントでのDNSSECバリデーション

- フルリゾルバでのDNSSECバリデーション

既存フルリゾルバをDNSSEC対応に移行する方法について説明

前提条件

- 前提条件

・すでにキャッシュDNSとして動作していること

-> パフォーマンスチューニングは扱いません。

-> フルリゾルバとしての基本設定は扱いません。

・特に指定のない場合、BIND9.9.7とします。

・Unboundの設定などについては扱いません

注意事項(1)

- DNSSECバリデーションを行う場合の時刻同期について
  - サーバの時刻が極端に異なると

    署名が正しくてもバリデーションに失敗する。

    expireを許容する設定もあるが・・・

    `dnssec-accept-expired`

  - 複数のタイムソースを利用すべき

    NTP,GPS,TELJJY,FM,etc..

正常に時刻同期が行われている確認/監視が重要

構成変更などによりNTP同期が外れていませんか

注意事項(2)

- バージョンの選択について　(BIND)

- BIND (9.7系以降で対応)

VERSION	STATUS	EOL DATE
9.10.3	Current-Stable	TBA
9.9.8	Current-Stable.ESV	Jun 2017
9.8.x	End-of-Life (EOL) as of Sep 2014	

引用: https://www.isc.org/downloads/software-support-policy/

機能的に問題がないのであればESVである9.9系がおすすめ

注意事項(2)

- バージョンの選択について　(OpenSSL)

DNS Security Algorithm Numbers 抜粋 (http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml)

Number	Description	Mnemonic	Zone Signing	Trans. Sec.	Reference
13	ECDSA Curve P-256 with SHA-256	ECDSAP256SHA256	Y	*	[RFC6605][standards track]
14	ECDSA Curve P-384 with SHA-384	ECDSAP384SHA384	Y	*	[RFC6605][standards track]

ECDSAでの署名も進むと考えられる

どのバージョンを選択するのが望ましいか

-> 複雑で一概には.. (ディストリビューション、パッチ、特許・・)

BINDだけでなく、OpenSSLバージョンについても考慮が必要

注意事項(3)

- ネットワークの問題について
  - ロードバランサ、ファイアウォール要確認
    - ・EDNS0への対応
    - ・TCPへの対応

DNSSECバリデーションの固有の問題ではないが注意が必要

注意事項(3.1)

- ネットワークの問題について

BIND 9.9.6-P1 Release Notes

Outstanding Issues

Refinements to EDNS fallback behavior in BIND 9.9.6 and 9.10.1 may prevent named (running as a recursive server) from attempting a f inal query using UDP without EDNS0 in some rare situations where prior queries using EDNS0 with both and TCP did not obtain usable answers.

条件によってはTCPフォールバックしない！？

BINDでのDNSSEC設定

- 既存リゾルバをDNSSEC署名検証有効にするには
設定追加と(場合によって)トラストアンカーの登録が必要

- DNSSECに関連するオプション

  dnssec-enable yes_or_no;

  dnssec-validation (yes_or_no | auto);

DNSSEC対応にするかどうか

DNSSEC署名検証を行うか

BIND 9.9.8では両方ともyesがdefault

設定例

```
options { ...
        dnssec-enable yes;
        dnssec-validation auto;
};
```

参考：ftp://ftp.isc.org/isc/bind9/9.9.8/doc/arm/Bv9ARM.pdf

BINDでのDNSSEC設定

- dnssec-validation (yes_or_no | auto);について
設定追加と(場合によって)トラストアンカーの登録が必要

BIND9.8以降では

・dnssec-validation yes;

- trusted-keysやanaged-keysを指定して**いる**場合、指定された物を使う
- trusted-keysやanaged-keysを指定して**いない**場合、BIND built-inを使う

・dnssec-validation auto;

- BIND built-inを使う

BIND9.8より前ではBIND built-inは使用できないので注意

BINDでのDNSSEC設定

- 既存リゾルバをDNSSEC署名検証有効にするには

- トラストアンカーの登録について

  ・BINDに付属する、トラストアンカーを使用する場合

  ・トラストアンカーを自動更新したい場合

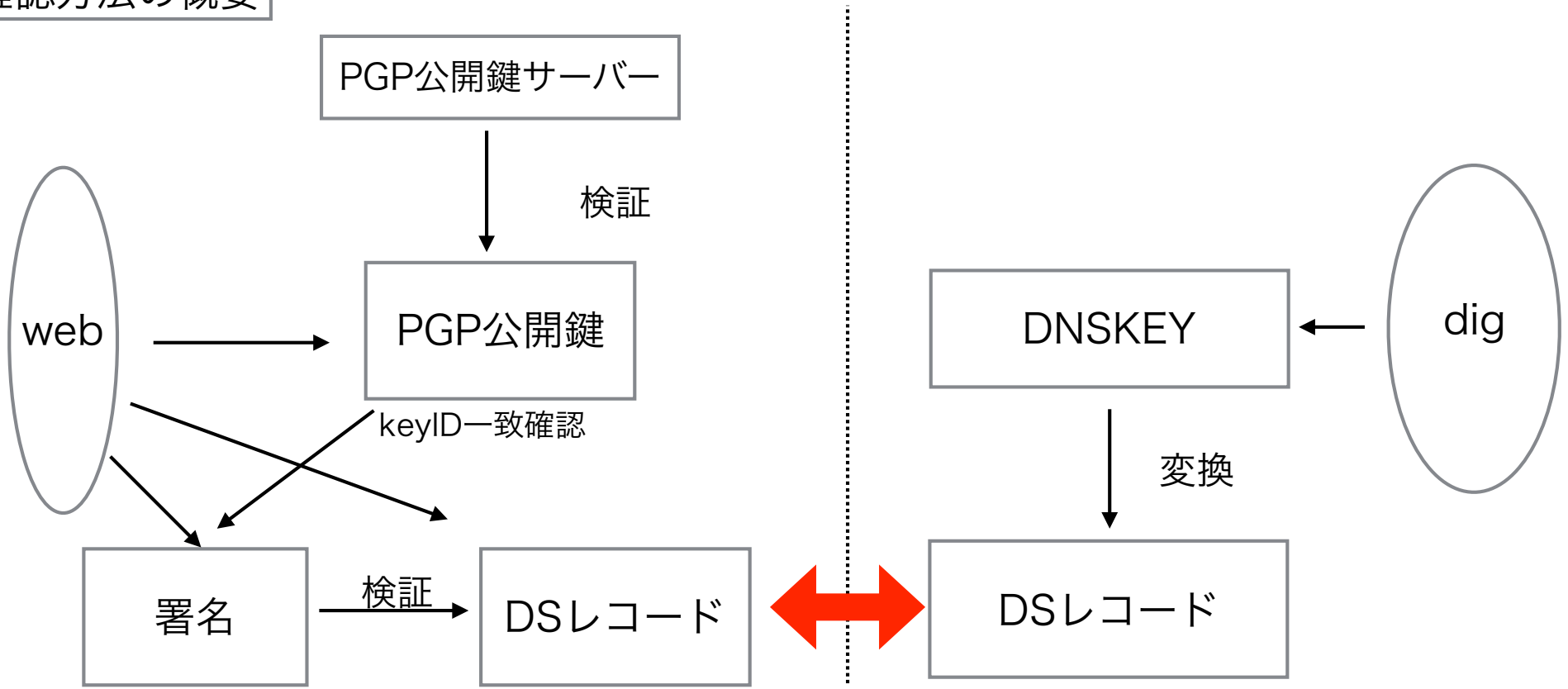
  ・マニュアルでトラストアンカーを設定したい場合

それぞれの設定方法とトラストアンカーの入手について解説します。

BINDでのDNSSEC設定

- ルートゾーンのトラストアンカーの入手と確認方法

確認方法の概要



配布元の正しさ、配布データと入手データの同一性の確認が重要

BINDでのDNSSEC設定

- ルートゾーンのトラストアンカーの入手と確認方法

入手方法

・digコマンドを用いてルートゾーンのDNSKEYレコードを取得する

```
$ dig . DNSKEY |grep -w DNSKEY |grep -w 257 > root-anchors.key
```

```
.                   124844      IN   DNSKEY     257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYI7OyQdXfZ57relS
Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
QxA+Uk1ihz0=
```

※256はZSK 257はKSK

BINDでのDNSSEC設定

- ルートゾーンのトラストアンカーの入手と確認方法

確認方法

PGP公開鍵の入手

```
$ curl https://data.iana.org/root-anchors/icann.pgp > icann.pgp
```

PGP公開鍵のインポート

```
$ gpg --import icann.pgp
gpg: key 0F6C91D2: public key "DNSSEC Manager <dnssec@iana.org>" imported
gpg: Total number processed: 1
gpg:               imported: 1
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   2  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: next trustdb check due at 2018-08-19
```

PGP公開鍵のidとfingerprintの確認

```
$ gpg --fingerprint dnssec@iana.org
pub   1024D/0F6C91D2 2007-12-01
      Key fingerprint = 2FBB 91BC AAEE 0ABE 1F80  31C7 D1AF BCE0 0F6C 91D2
uid       [ unknown] DNSSEC Manager <dnssec@iana.org>
sub   2048g/1975679E 2007-12-01
```

BINDでのDNSSEC設定

- ルートゾーンのトラストアンカーの入手と確認方法

確認方法

PGP公開鍵の検索

```
$ gpg --search-keys --interactive --keyserver pgp.nic.ad.jp 0x0F6C91D2
gpg: searching for "0x0F6C91D2" from hkp server pgp.nic.ad.jp
(1)  DNSSEC Manager <dnssec@iana.org>
     1024 bit DSA key 0F6C91D2, created: 2007-12-01
Enter number(s), N)ext, or Q)uit > 1
gpg: requesting key 0F6C91D2 from hkp server pgp.nic.ad.jp

pub  1024D/0F6C91D2  created: 2007-12-01  expires: 2011-11-25
      Key fingerprint = 2FBB 91BC AAEE 0ABE 1F80  31C7 D1AF BCE0 0F6C 91D2

     DNSSEC Manager <dnssec@iana.org>
```

鍵の検索結果と入手したPGP公開鍵の情報が一致することを確認

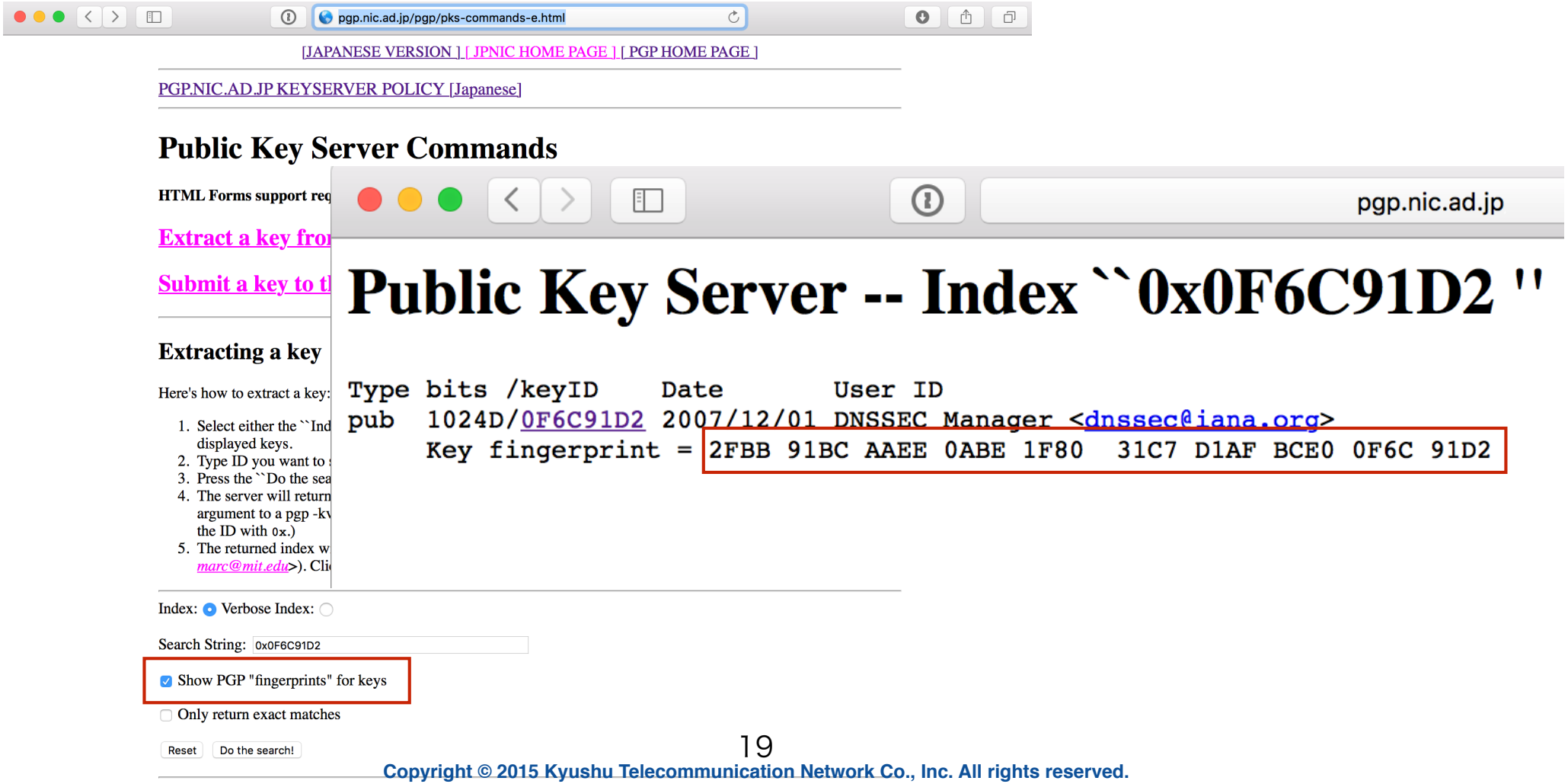
```
$ gpg --fingerprint dnssec@iana.org
pub   1024D/0F6C91D2 2007-12-01
      Key fingerprint = 2FBB 91BC AAEE 0ABE 1F80  31C7 D1AF BCE0 0F6C 91D2
uid       [ unknown] DNSSEC Manager <dnssec@iana.org>
sub   2048g/1975679E 2007-12-01
```

複数の鍵検索サーバで確認することが望ましい

BINDでのDNSSEC設定

- ルートゾーンのトラストアンカーの入手と確認方法

確認方法 PGP公開鍵の検索(Web)



BINDでのDNSSEC設定

- ルートゾーンのトラストアンカーの入手と確認方法

確認方法

ルートゾーンのトラストアンカーのDSレコードと署名を入手する

```
$ curl https://data.iana.org/root-anchors/root-anchors.xml > root-anchors.xml
$ curl https://data.iana.org/root-anchors/root-anchors.asc > root-anchors.asc
```

入手ファイルの署名検証

公開鍵IDと一致することも確認

```
$ gpg --verify root-anchors.asc root-anchors.xml
gpg: Signature made 水  7/ 7 07:49:10 2010 JST using DSA key ID 0F6C91D2
gpg: Good signature from "DNSSEC Manager <dnssec@iana.org>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 2FBB 91BC AAEE 0ABE 1F80  31C7 D1AF BCE0 0F6C 91D2
```

root-anchors.xmlが正しいものであることを確認する。

BINDでのDNSSEC設定

- ルートゾーンのトラストアンカーの入手と確認方法

確認方法

入手したDNSKEYからDSレコード方式への変換

```
$ dnssec-dsfromkey -a SHA-256 -f root-anchors.key .
. IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5
```

DSレコードとroot-anchors.xmlの署名検証

```
$ cat root-anchors.xml
<?xml version="1.0" encoding="UTF-8"?>
<TrustAnchor id="AD42165F-3B1A-4778-8F42-D34A1D41FD93" source="http://data.iana.org/root-anchors/
root-anchors.xml">
<Zone>.</Zone>
<KeyDigest id="Kjqmt7v" validFrom="2010-07-15T00:00:00+00:00">
<KeyTag>19036</KeyTag>
<Algorithm>8</Algorithm>
<DigestType>2</DigestType>
<Digest>49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5</Digest>
</KeyDigest>
</TrustAnchor>
```

配布元の正しさ、配布データと入手データの同一性の確認ができた

BINDでのDNSSEC設定

- マニュアルでルートゾーンのトラストアンカーを設定したい場合

設定方法

```
options {
        dnssec-enable       yes;
        dnssec-validation   yes;
};
trusted-keys {
    . 257 3 8 "AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
    FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
    bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
    X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
    W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
    Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
    QxA+Uk1ihz0=";
};
```

yesの場合
trusted-keys or managed-keysが必須

トラストアンカーが更新された場合、手動での更新が必要

BINDでのDNSSEC設定

- BINDに付属する、トラストアンカーを使用する場合
  - 配布物が真正であることを確認すること
  - 手動でトラストアンカーを設定する必要がない

設定方法

```
options {
    dnssec-enable          yes;
    dnssec-validation      auto;
};
```

BIND DNSSEC GuideによるとRecommend設定

※手動でトラストアンカーを設定する必要のない限り

参考：http://users.isc.org/~jreed/dnssec-guide/dnssec-guide.html

BINDでのDNSSEC設定

- 自動でルートゾーンのトラストアンカーを更新したい場合

設定方法

```
options {
        dnssec-enable       yes;
        dnssec-validation   yes;
};
managed-keys {
   . initial-key 257 3 8 "AwEAAagAIKlVZrpC6Ia7gEzahOR
+9W29euxhJhVVLOyQbSEW0O8gcCjF
   FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
   bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
   X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
   W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYI7OyQdXfZ57relS
   Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
   QxA+Uk1ihz0=";
};
```

BINDでのDNSSEC設定

- 自動でルートゾーンのトラストアンカーを更新したい場合

注意点

- Working directoryに2ファイルが作成される
  managed-keys.bind,managed-keys.bind.jnl
- namedの実行権限で読み書きできることを確認

- ディレクトリを指定することも可能

設定例

```
options { ...
        managed-keys-directory path_name;
};
```

移行や導入に関して

- 準備段階

  導入前のリソース(CPU,MEM,NW)やBIND統計状況を把握する

  導入した際のリソースなどについて、試算を行う。

- 一部適用

  導入準備に問題なければ、一部リゾルバへ設定を適用する

  導入前後のリソースとBIND統計状況を比較する。

- 全体適用

  一部適用に問題なければ、徐々に全体への適用を進める。

- 導入後段階

  導入前後のリソースとBIND統計状況を比較する。

まとめ

- 注意事項について
  - 時刻同期の重要性について
  - BIND,OpenSSLのバージョンの選択について
  - ネットワークの問題について
- BINDでのDNSSECについて
  - トラストアンカーの入手と確認方法について
  - トラストアンカーの設定について
    - ・マニュアル設定
    - ・トラストアンカー自動更新設定
    - ・BIND付属のトラストアンカーの使用方法