あなたのDNS運用は
来るべきDNSSEC時代に
耐えられますか

民田雅人 <minmin@jprs.co.jp>
株式会社日本レジストリサービス
2009-07-09 JANOG 24@東京

はじめに

- 本セッションの構成
  - DNSSEC豆知識
  - DNSSEC化によるDNSデータの変化
  - ディスカッション
  - まとめ

本セッションでは
DNSSECの具体的な設定は扱いません

DNSSEC豆知識

DNSSECとは

- **DNS SEC**urity Extensions
  - 公開鍵暗号技術の応用
- ゾーン情報に秘密鍵で署名
  - DNSの応答パケットに署名情報を付加
- クライアントが公開鍵で署名を検証
  - ゾーン情報の第三者による改ざんや騙りを公開鍵を用いて検証

DNSSECとは(続き)

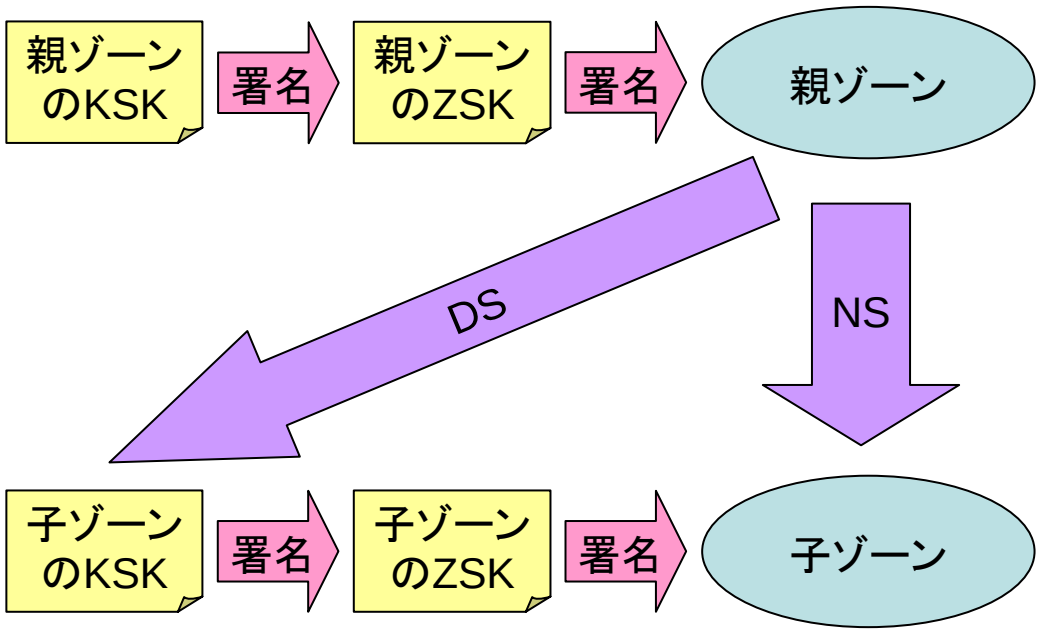
- 現時点で、DNSキャッシュへの毒入れ攻撃による被害を防ぐ唯一の現実解
  - 短いTTLのリスク(JANOG 19)
  - Kaminsky型の攻撃

  これらによる被害を**完全**に防ぐことができる
- よくある(?)誤解
  DNSSECは、DNSの通信を暗号化するものではない

DNSSECの信頼の連鎖(1/2)

- 親ゾーンに子ゾーンのDS RRを登録することで子ゾーンを認証
- KSK（秘密鍵）でZSK（公開鍵）を署名
- ZSK（秘密鍵）でゾーンを署名
  - 以下、ゾーン委任毎に繰り返す
- ルートのKSK（公開鍵）を、DNSSEC検証者(**バリデータ**)が持つ
  - 主にキャッシュDNSサーバ

DNSSECの信頼の連鎖(2/2)



- 公開鍵暗号による信頼の連鎖を形成
- キャッシュDNSサーバに、ルートゾーンのKSKの公開鍵(**トラストアンカー**)を登録して署名を検証

用語：バリデータ(Validator)

- DNSSECにおいて、バリデータは、署名の検証を行うもの(プログラム、ライブラリ)を指す
- 通常、署名検証はキャッシュDNSサーバ
  - スタブリゾルバもバリデータとなりうる
- バリデータにトラストアンカーを登録

DNSSECの2組の署名鍵
KSK (Key Signing Key)

- **ZSK公開鍵を署名**するための鍵
- 暗号強度の高い鍵
  - RSAで2048bitや4096bitなど
- 署名コストは高い
  - 少数のZSKのみを署名対象とするため問題にならない(署名コストは鍵の長さに応じて増える)
- KSK公開鍵と暗号論的に等価な情報(DSレコード)を作成し、親ゾーンに登録する
  - 利用期間を長くできるため、鍵を更新する頻度(＝親に送る頻度)を低くできる

DNSSECの2組の署名鍵
ZSK (Zone Signing Key)

- **ゾーンを署名**するための鍵
- 比較的暗号強度の低い鍵
  - RSAで768bitや1024bitなど
- 署名コストが比較的低い
  - 大規模ゾーンでも運用しやすい
- 安全確保のため(ある程度)頻繁に鍵を更新する必要がある
  - ZSKそのものは、親ゾーンに関係なく独立に変更できる
    ⇒ KSKのようなDSの登録は不要

DNSSEC関係のRR

- DNSKEY　　KSK･ZSK公開鍵の情報
- RRSIG　　ZSKによる各RRへの署名
- DS　　KSK公開鍵のハッシュ値を含む情報（親ゾーンに登録）
- NSEC　　次のRRへのポインタと存在するレコード型の情報
- NSEC3　　NSECを改良したもの(後述)
- NSEC3PARAM　NSEC3に必要な情報

DS (Delegation Signer)

- KSK公開鍵と1対1対応するように圧縮したDNSレコード
  - 特定のハッシュアルゴリズム（SHA-1,SHA-256など）を用いて作成する
- DSからKSK公開鍵の復元は不可
- 親ゾーンにのみ存在する唯一のレコード

DNSソフトウェアの対応状況

- 権威DNSサーバ(権威サーバ)
  - BIND 9、NSD3など
- キャッシュDNSサーバ(キャッシュサーバ)
  - BIND 9、Unboundなど
- Windows環境
  - Windows 7とWindows Server 2008 R2で対応予定 (2009年10月頃?)

いくつかのTLDが DNSSEC対応済 or 対応を表明

- gTLD
  - .ORG　.GOV　.MUSEUM
- ccTLD (試験運用を含む)
  - .BG　.BR　.CZ　.PR　.SE　.TH
- VeriSign (.com .net等)も対応表明
- ROOTゾーンのDNSSEC対応も時間の問題
  - http://www.nist.gov/public_affairs/releases/dnssec_060309.html
  - http://www.icann.org/en/announcements/announcement-2-03jun09-en.htm
- 時間の問題でDNSSECはみなさんのお手元に

.JPのDNSSEC対応は？

本日(7/9)、JPRSはJPドメイン名をDNSSEC対応することを表明しました

JPドメイン名サービスへの
DNSSECの導入予定について

http://jprs.jp/info/notice/20090709-dnssec.html

▼ はじめに

JPRSでは、DNSのセキュリティ拡張方式であるDNSSECを、2010年中を目処にJPドメイン名サービスへ導入する予定で準備を進めています。

DNSSECに対応しますか？
対応します：キャッシュサーバ側

- 設定は比較的簡単
  - 対象ドメイン名のトラストアンカー(KSK公開鍵)を設定に追加する(設定ファイルに数行の追加)
- ルートゾーンがDNSSEC化されれば、トラストアンカーは”.”のみ設定
  - 現状は各TLD毎に必要。また、鍵更新された場合トラストアンカーも更新作業が必要

しかし…

署名検証による負荷の増大は想像に難くない

DNSSECに対応しますか？
対応します：権威サーバ側

- 鍵を作る
  - KSKとZSKの生成
- 署名する
  - 生成した鍵を使ってゾーンへの署名作業
- 親ゾーンへのDSの登録
- ゾーン情報の変更に伴う再署名

DNSSECに対応しますか？
対応します：権威サーバ側(続き)

- 鍵を管理する ⇒ 定期的な鍵更新
  - 同じ鍵を長期間使い続けるのは鍵解析のリスクとなる
- ZSKの更新(例えば1ヶ月に1回とか)
  - 新たなZSKを作り、ゾーンを再署名
- KSKの更新(例えば1年に1回とか)
  - 親ゾーンへのDSの登録情報の更新
  - ZSKへの再署名 ⇒ ゾーン情報の更新 ⇒ ゾーン情報の再署名

やることいっぱい！

DNSSECに対応しますか？
対応します：時刻の同期

- DNSSEC運用に欠かせない時刻の正確性
  - 署名には有効期間があり期間外では無効
- DNSサーバの時刻を正確に保つ
  - ゾーン管理者は署名の有効期限に余裕をもって再署名
    ⇒ 実用上5分程度のずれなら問題ない(はず)
  - NTPなどを設定して確実に合わせる

素朴な疑問
DNSSEC非対応プログラムは？

- DNS Security *Extensions*
  - 名前が示す通り、DNSSECはDNSの拡張機能
- DNSSEC対応でも設定を行わない場合、あるいはDNSSEC非対応でも、従来の名前解決には影響が無い
  - もちろん毒入れの脆弱性の対策にはならない

よってDNSSEC非対応は望ましくない

でも…

DNSSEC化による
DNSデータの変化

DNSSEC有無による www.nic.seの検索

- DNSSEC無し

```
$ dig +norec @ns.nic.se www.nic.se a | grep SIZE
;; MSG SIZE  rcvd: 173
```

- DNSSEC有り

```
$ dig +norec +dnssec @ns.nic.se www.nic.se a | grep SIZE
;; MSG SIZE  rcvd: 1180
```

DO(**D**NSSEC **O**K)ビット

- dig の +dnssec オプション
  - 問合せでEDNS0を使いDOビットをONにする
  - DNSSECでは**EDNS0のサポートは必須**
- DOビット
  - DNSSEC OK ⇒ DNSSECの応答を受ける
    ⇒ DNSSECを要求する
  - 権威サーバは、問合せのDOビットがONであれば、DNSSECの情報を含んだ応答を返す

権威サーバへのdigの結果(1/2)

- +dnssec無しのdigの応答

```
; <<>> DiG 9.6.1 <<>> +norec @ns.nic.se www.nic.se a
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14346
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4

;; QUESTION SECTION:
;www.nic.se.                    IN              A

;; ANSWER SECTION:
www.nic.se.     60              IN              A               212.247.7.218

;; AUTHORITY SECTION:
nic.se.         3600            IN              NS              ns3.nic.se.
nic.se.         3600            IN              NS              ns2.nic.se.
nic.se.         3600            IN              NS              ns.nic.se.

;; ADDITIONAL SECTION:
ns.nic.se.      3600            IN              A               212.247.7.228
ns.nic.se.      3600            IN              AAAA            2a00:801:f0:53::53
ns2.nic.se.     3600            IN              A               194.17.45.54
ns3.nic.se.     60              IN              A               212.247.3.83

;; Query time: 328 msec
;; SERVER: 212.247.7.228#53(212.247.7.228)
;; WHEN: Tue Jul  7 23:39:18 2009
;; MSG SIZE  rcvd: 173
```

権威サーバへのdigの結果(2/2)

- +dnssec有り 各RRにRRSIG RRを加えたものが返る

```
; <<>> DiG 9.6.1 <<>> +norec +dnssec @ns.nic.se www.nic.se a
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5979
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.nic.se.                            IN          A

;; ANSWER SECTION:
www.nic.se.     60          IN          A           212.247.7.218
www.nic.se.     60          IN          RRSIG       A 5 3 60 20090714132001 20090704132001 58670 nic.se. izdsOhTB1XThccw2Wv4TZjl

;; AUTHORITY SECTION:
nic.se.         3600        IN          NS          ns2.nic.se.
nic.se.         3600        IN          NS          ns.nic.se.
nic.se.         3600        IN          NS          ns3.nic.se.
nic.se.         3600        IN          RRSIG       NS 5 2 3600 20090714132001 20090704132001 58670 nic.se. pKDbUYXLQpPnhlU9NAZh

;; ADDITIONAL SECTION:
ns.nic.se.      3600        IN          A           212.247.7.228
ns.nic.se.      3600        IN          AAAA        2a00:801:f0:53::53
ns2.nic.se.     3600        IN          A           194.17.45.54
ns3.nic.se.     60          IN          A           212.247.3.83
ns.nic.se.      3600        IN          RRSIG       A 5 3 3600 20090714132001 20090704132001 58670 nic.se. GzLodvUOd0oB4qfhhbp8H
ns.nic.se.      3600        IN          RRSIG       AAAA 5 3 3600 20090714132001 20090704132001 58670 nic.se. 0tvno8Vz7Ihm27AZ+H
ns2.nic.se.     3600        IN          RRSIG       A 5 3 3600 20090714132001 20090704132001 58670 nic.se. UcEcYGX59H8bAVGwhfwko
ns3.nic.se.     60          IN          RRSIG       A 5 3 60 20090714132001 20090704132001 58670 nic.se. NRoFeFzAm0hoyKa2ObxjCfB

;; Query time: 382 msec
;; SERVER: 212.247.7.228#53(212.247.7.228)
;; WHEN: Tue Jul  7 23:39:24 2009
;; MSG SIZE  rcvd: 1180
```

注意：RRSIGは行の途中まで、残り省略

DNSSEC有無による存在しないドメイン名の検索

- DNSSEC無し (arimasen.org)

```
$ dig +norec @a0 arimasen.org a | grep SIZE
;; MSG SIZE  rcvd: 93
```

- DNSSEC有り (arimasen.org)

```
$ dig +norec +dnssec @a0 arimasen.org a | grep SIZE
;; MSG SIZE  rcvd: 1006
```

注) arimasen.orgは現時点では存在しないドメイン名
「a0」は「a0.org.afilias-nst.info」を省略して表記
(.ORGのネームサーバの一つ)

DNSSECにおける不在証明

- DNSSECではドメイン名が存在しない場合、**存在しないことを証明**する必要がある
  - 存在しないドメイン名が偽造されるのを防ぐ
- 存在するレコードは、署名(RRSIG RR)を付加し、署名を検証することで存在を証明する
- 存在しないレコードには?
  - 存在しないものは署名不能

ハンバーガーのパティの有無

- パティ(肉)が有る
  - パティの存在を判断できる
- パティが無く、バンズ(パン)も無い
  - パティが無いかどうか判断不能
    ⇒ 単純に配膳が遅れているだけ?
- パティが無く、クラウン(バンズ上部)とヒール(バンズ下部)がある
  - クラウンとヒールの存在が判断できる
    ⇒ パティが存在しないことを確実に判断できる

NSEC RR

- NSECは存在しないものを証明するためのレコード
  - 存在するレコードすべてを整列し、次のレコードへのリスト構造を生成することで、存在しないものを証明する

  例)
```
ns0.example.jp.  IN NSEC
        ns2.example.jp. A RRSIG NSEC
```

  - ns0.example.jp の次のドメイン名は ns2.example.jpでAとRRSIGとNSECのレコードを持つ
    ⇒ ns1.example.jp は存在しないことが分かる
- もちろんNSEC RRにもRRSIGを付加し、署名の検証を行う

NSEC3 RR

- NSEC RRの欠点
  - NSEC RRを辿ることで、芋づる式にゾーン情報を入手できる(DNSSEC Walker)
    ⇒ セキュリティ面で問題となる
- NSEC3
  - ドメイン名を一方向性ハッシュ関数でハッシュ化しそれをBase32でエンコードしたものを並べる
  - 一方向性ハッシュ関数であるため元のドメイン名は推測不可能

ここまでのまとめ
DNSSEC対応になると

- 署名の付加によりゾーンデータが大きくなる
  - 5～10倍程度(鍵のbit長に依存)
  - プライマリが署名すると、セカンダリにもインパクトがある
- DNS応答パケットのサイズが大きくなる
  - DNSトラフィックが増える
  - キャッシュサーバのキャッシュ効率が落ちる
  - 特に存在しない名前の検索では顕著

DNSSEC対応しますか?
(まだ)対応しません

- 権威サーバ側
  - 今は何もしません
- キャッシュサーバ側
  - すぐにやらないけど、そのうち対応します
    ⇒ だから、今は対応しません
  - 事情により今はできないので、次の機器更新時に対応します
    ⇒ だから、今は対応しません

キャッシュサーバ側
今はDNSSEC対応しません

- DNSSEC化で署名が追加
  - DNSパケットサイズは増加
  - DNSトラフィックの増加
- うちのキャッシュサーバ、まだDNSSEC対応の設定をしてないから影響無い(はず)

本当?

論よりRun！

ということで実演

DNSSECをサポートできるキャッシュサーバの挙動

- キャッシュサーバは、権威サーバへ問い合わせる際DOビットを**必ずON**にする
  - RFC 3225 Indicating Resolver Support of DNSSEC Section 3より抜粋
    A recursive DNSSEC-aware server MUST set the DO bit on recursive requests, regardless of the status of the DO bit on the initiating resolver request.
- よって、権威サーバはゾーン情報がDNSSECで署名されていれば、必ずRRSIG付で応答

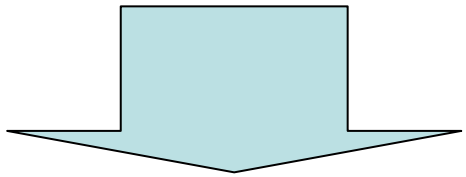
何故？

DNSSECをサポートできるキャッシュサーバの挙動(続き)

- キャッシュサーバとバリデータは独立
  - キャッシュサーバ(バリデータ)が別のキャッシュサーバをフォワーダーとして利用する場合
  - スタブリゾルバが署名検証を行うような場合
- 署名済みならば、レコードに付随するRRSIGがキャッシュされていないと、バリデータは署名の検証ができなくなる
  - RRSIGは存在するレコードに**付随する**レコード
  - 通常RRSIGだけを単独で問合せることは無い

DNSSECをサポートできる キャッシュサーバ

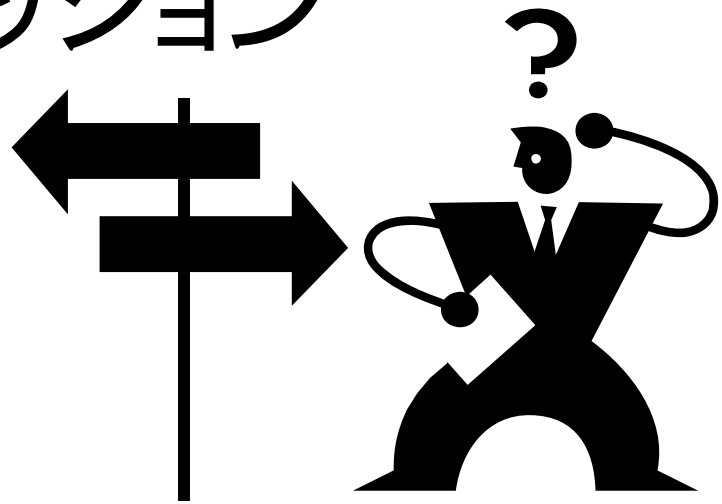
- DOビットをONにするキャッシュサーバ
  - BINDの場合9.3系以降すべて dnssec-enable の yes/no は無関係
  - もちろんUnboundも同様



DNSSECで署名されると そのドメインのDNSトラフィックは 自動的に増加する

ディスカッション

JAPAN REGISTRY SERVICES



- DNSSECでは**大きな**DNSパケット(UDP)が増える
  - DNSトラフィックが増えても大丈夫?
  - DNSサーバの負荷にもインパクトがあるよね?
  - キャッシュの効率が下がるのは痛いよね?
- 署名検証の負荷については今回は議論の対象外
  - 署名検証の負荷は機会を改めて考えたいかも ☺

まとめ

- 「うちはヤバいかも！」と思った人
  - Root　.JP　.COM　.NET等がDNSSEC化で揃うのは、もうしばらく先(のはず)

    ⇒ 対応する時間はまだある(はず)
- DNSSEC化されたDNSの世界では、

  より愛を持ってDNS運用に接して下さい
  - 現状よりは、多少なりとも手間をかける必要がありそうです