

そこが知りたいDNSSEC

民田雅人 <minmin@jprs.co.jp>
株式会社日本レジストリサービス
2010-01-22 JANOG 25@新潟

今日の話

1. 世界のDNSSEC導入状況
2. DNSSECは「生もの」
3. DNSSEC導入までの長い(?)道のり
4. そこが知りたいDNSSEC

1. 世界のDNSSEC導入状況

導入済TLD (試験的導入を含む)

種別	TLD名	特記事項
ccTLD	SE (スウェーデン)	・2005年9月導入、世界で最初にDNSSEC対応したTLD ・これまでに多くのノウハウを外部に発信
	PR (プエルトリコ)	・2006年8月導入
	BG (ブルガリア)	・2007年1月導入
	BR (ブラジル)	・2007年6月導入、2009年1月に全属性で対応 ・最新方式(NSEC3)を採用した最初のTLD
	CZ (チェコ)	・2008年9月導入
	TH (タイ)	・2009年3月導入、アジアで最初にDNSSEC対応したccTLD
	TM (トルクメニスタン)	・2009年10月導入
	US (アメリカ)	・2009年12月導入
gTLD	MUSEUM	・2008年9月導入
	GOV (米国政府)	・2009年2月導入、2009年末に全組織が対応予定
	ORG	・2009年6月導入、2010年に本サービス化予定

導入予定TLD(1/2)

種別	TLD名	特記事項
ccTLD	AT (オーストリア)	
	CA (カナダ)	・2009年10月にテストベッドを開始
	CH (スイス)	・2009年9月に実地検証開始、2010年2月サービスイン予定
	CN (中国)	・2010年末までに導入予定
	DE (ドイツ)	・2009年5月にテストベッドを開始
	GR (ギリシャ)	
	JP (日本)	・2010年を目処に導入予定
	KR (韓国)	・2010年6月に導入し、2011年1月に全空間で対応予定
	LI (リヒテンシュタイン)	・2009年9月に実地検証開始、2010年2月サービスイン予定
	MY (マレーシア)	・2010年第四四半期に導入予定
	RU (ロシア)	
	UK (イギリス)	・プロトコル策定・IANAとの共同実験など積極的に活動

導入予定TLD(2/2)

種別	TLD名	特記事項
gTLD	BIZ	・2010年第三四半期に導入予定
	CAT	・2009年中に導入予定
	COM	・2011年の早い時期に導入予定
	EDU	・2010年3月末に署名予定
	INFO	
	NET	・2010年末までに導入予定

注意:

これらの表はDNSSEC導入の定義の違いにより、多少曖昧な面を含む

– 何をもってDNSSECの導入と呼ぶかの違い

rootゾーンの状況(1)

- 2008年10月
rootゾーンのDNSSEC対応声明
 - ICANNが、DoC(NTIA)、NIST、VeriSignと協調し、2009年中のroot署名を目指す旨の発表
- その後、いくつかの問題点などが指摘される
 - ICANN35(2009年6月)での会合
 - IETF75(2009年7月)での併設会議
- 2009年中の導入は厳しい(?)

rootゾーンの状況(2)

- 2009年10月 RIPE 59@リスボンにて
2010年7月から正式運用と発表
 - ICANN36@ソウル、OARC@北京、
IETF 76@広島等の会合でもアナウンス
- 2009年12月 実験的な署名を実施
 - 実験的 ⇒ 内部の署名作業のみ
- 2010年1月より各rootサーバに**徐々に適応**
- 2010年7月に正式運用

rootゾーンの状況(3)

<http://www.root-dnssec.org/>

- 「徐々に適応」⇒ 万が一に備える
 - rootゾーンはすべてのフルリゾルバがアクセスするにも関わらず、DNSSEC化によるDNSデータの変化に対するインパクトが不明確
 - 検証できないダミーの署名データを追加したrootゾーン(DURZ)を用意し、一部のrootサーバから順に適応
 - L ⇒ A ⇒ M, I ⇒ D, K, E ⇒ B, H, C, G, F ⇒ J
- 2010年7月の正式導入までに完了予定

「ほらDNSSECの足音が
そこまで...」

2. DNSSECは「生もの」

古くて新しいDNSSEC

RFC	発行年	概要	対応BIND
2065	1997年	DNSSEC最初のRFC	
2535	1999年	RFC 2065の改良版	9.2系まで
3658	2003年	DS RRの登場	9.3系から
4033 4034 4035	2005年	現行のDNSSEC方式の基本 (NSEC 方式)	9.3系から
5011	2007年	トラストアンカーの自動更新	9.7系から
5155	2008年	NSEC3 方式(NSEC方式の改良)	9.6系から
5702	2009年	DNSKEY,RRSIGの SHA-2 対応	9.7系から

NSEC RR

- NSEC RRは**不在**を**存在**を使って**表現**する
 - ns1.example.jpを問い合わせた場合の応答

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

権威セクションで応答し、ns0.example.jp の次のドメイン名はns2.example.jpでAとRRSIGとNSECのレコードがあることを示す
⇒ ns1.example.jpは存在しないと判断できる

- NSEC RRに署名を付加し**不在を証明**する

NSEC vs NSEC3

- NSEC RR
 - 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)
- NSEC3 RR
 - ドメイン名を一方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
 - 一方方向性ハッシュ関数(SHA1)であるため、元の
ドメイン名は推測困難
- NSEC3はBIND 9.6やUnboundで対応

RSASHA256

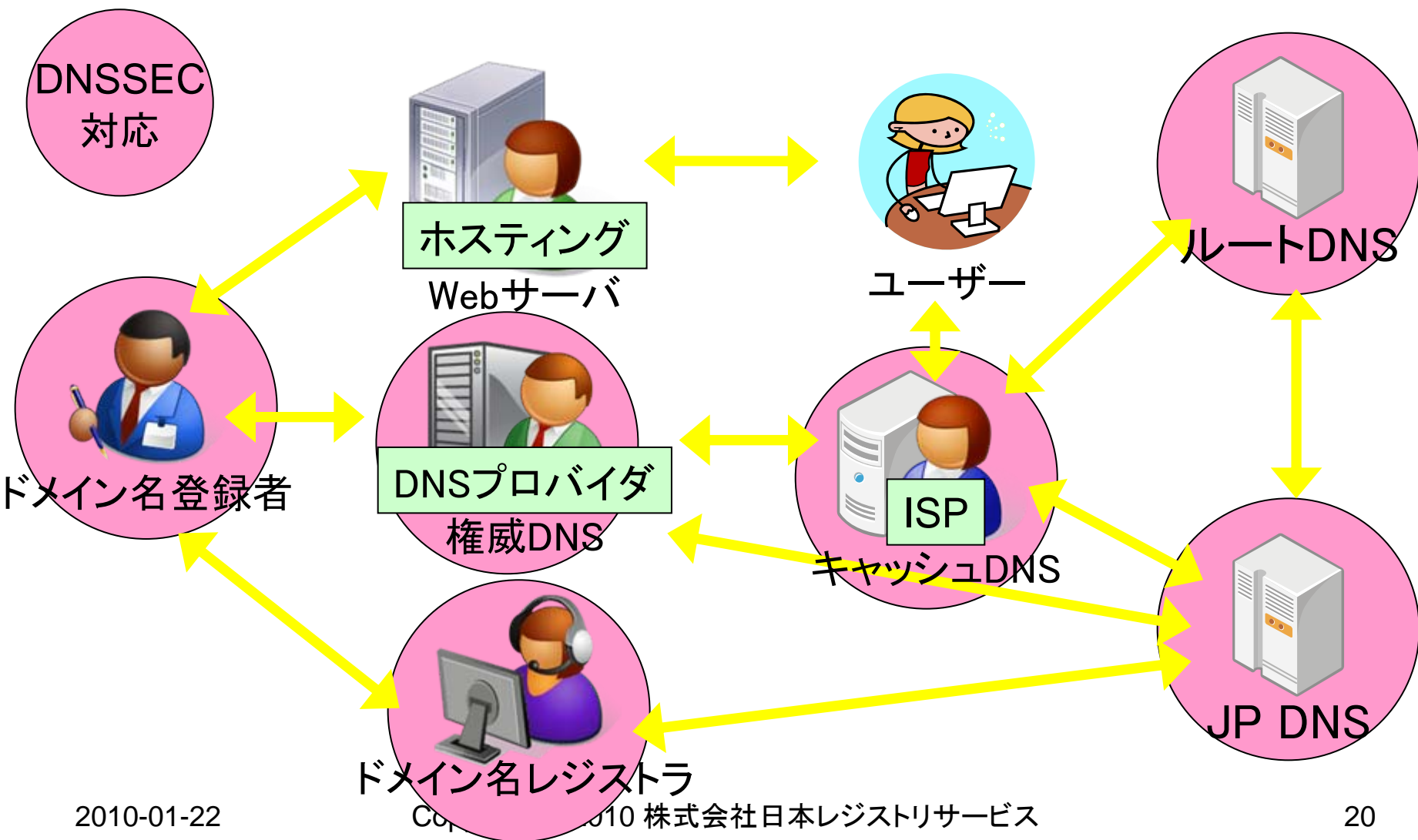
- rootで採用するDNSSECのアルゴリズム
 - 暗号化にRSA、ハッシュにSHA-256を採用
 - 以前はRSASHA1
 - RFC 5072(2009年10月)での標準化ホヤホヤ
- BIND 9.7系、Unboundは1.4系で対応
 - BIND 9.6.1では未対応
 - BIND 9.6.2で対応 (9.6.2rc1以降)

DNSSECは「生もの」

- DNSSEC運用を行う場合、最新のソフトウェアを使う必要がある
 - BIND 9 9.6.2以降 まもなく(?) 9.6.2rc1
 9.7系以降 現在 9.7.0rc1
 - Unbound 1.4.0以降 現在 1.4.1
 - NSD 3.1.0以降 現在 3.2.4
- rootゾーンがDNSSEC化されることで、そろそろ落ち着つく(か?)
 - 今後もアルゴリズムが増える可能性はある

3. DNSSEC導入までの 長い(?)道のり

DNSSEC対応が必要な関係者



DNSSEC対応作業の概要

- ドメイン名登録者
 - DNSSEC導入の決定
 - 秘密鍵・公開鍵の生成
⇒ 実運用者が担当
- ドメイン名レジストラ
 - 鍵の上位への取次ぎ
- JP DNS、ルートDNS
 - 権威DNSサーバのDNSSEC対応化
 - ゾーンへの署名
- DNSプロバイダ
 - 権威DNSサーバのDNSSEC対応化
 - 登録者の鍵を使ってゾーンに署名
- ISP
 - キャッシュDNSサーバのDNSSEC対応化
 - (キャッシュDNSサーバでの)署名の検証

JPでのDNSSECテストベッド

- DNSSEC導入時の対応をスムーズにするため、JPではDNSSEC化した仮想のDNSツリーを用意し、技術検証等を実施中
 - 一部のISP、ベンダーにも参加頂いております
 - ⇒ ご協力ありがとうございます
- 本日、簡易なベンチマーク結果をお届けする予定でしたが、間に合いませんでした orz
 - 結果は別途公開！

他TLDに聞いてみました 技術検証やっていますか？ (1)

- 関係者と技術検証やりましたか？
 - 署名システムとDS受付インターフェース用の開発時に内部テストを実施した
⇒「お、がんばってるじゃん」
 - やって見たけど、みんなの興味が無くて失敗した
⇒「いいのか、それで」
 - そのような技術検証はやってません
⇒「はひ～！」

他TLDに聞いてみました 技術検証やっていますか？ (2)

- 情報公開しました？
 - 導入までのプロセスは文書化していないが、
重大な課題は見受けられなかった
⇒「まあ、いいでしょう」
 - 公開するようなものは無かった
⇒「ほんとに？ 技術検証やったの？」

日本人って、やっぱりまじめ 😊

4. そこが知りたいDNSSEC

署名の検証に失敗すると どうなるのですか？

- 現状、DNSの応答でSERVFAILとなる
⇒ 目的の名前解決ができなくなる
「インターネットが繋がりません～」
- DNSSECは嘘を見破る技術
 - 正しい答えを見つける技術では無い

RSASHA256をサポートしていないサーバが運用されてますが、RSASHA1からの移行はどのように行われるのでしょうか

- 気にしなくてよい
 - rootではRSASHA256を採用し、RSASHA1の運用期間がない
 - DNSSECを運用する場合rootの署名検証ができないのでは意味が無い
- DNSSEC運用する場合RSASHA256をサポートした最新のソフトウェアを利用することになる

今すぐ新規ドメイン名でDLVを使わずに
DNSSEC実運用を試したいのですが、手
段はありますか

- .SEをどうぞ

- .SEにはローカルプレゼンスが無い
⇒ 日本からでも登録可能

- 質問者は、国内で.SEのレジストラを見つけられ
なかったとのこと ⇒ 私も知りません

- .SE内のレジストラで直接登録すればokなはず

- DLV運用については以下を参照

- 「今すぐDNSSECで遊ぶには」

- <http://dnsops.jp/bof/20090904/dnsops-20090904.pdf>

- (第7回 DNSOPS.JP BoF)

IPv6になればIPSecで安全に通信できるのでDNSSECは不要ではないですか？

- IPv6になればというより、IPSecが**全ての**通信に利用されるようになれば、そうかも
 - データの信頼性と通信の信頼性は別とは言え、サーバに侵入された場合とかはDNSSEC、IPSecとも差はなさそう
- IPSecってDNSSECより普及するんですか？
 - 現状はDNSSECの普及が早い

ゾーン外のNSを用いている場合の 弊害があれば教えてください

- キャッシュDNSサーバはDNSSECで守られていない委任情報を辿る可能性がある
 - キャッシュへの毒入れ攻撃があると、最終的なDNSSECの委任先へ辿りつけない
 - ⇒ 目的の名前解決ができない
- ゾーン外のNSはDNS的には...
 - 運用面で止むを得ない場合があるのは確か
 - 出来る範囲でゾーン内のNSでお願いしたい ☺

キャッシュの内容が実際の委譲関係とずれが生じた場合に問題は発生しませんか？

質問者の意図

自分が管理する内部でNSを変更する場合の話
例) ns1.example.jp ⇒ ns2.example.jp

- NSの変更時はDNSSECだからと言って特に変わることはなく、既存のNSの変更作業と同様です

DNSやDNSSECを理解していない人でも 設定できて運用し続けることはできますか？

- できるかもしれないけど...
DNSSEC運用はより高いスキルが必要
 - トラブルシューティングはきっと大変
- 権威DNSサーバ側
 - エンドユーザにはお勧めしない
 - DNS運用はISP等に任せるべき
- キャッシュDNSサーバ側
 - それほど難しい設定は要らないので(トラストアンカーの設定と**更新**)、なんとかなるのかも

秘密鍵をなくした時には どうすれば良いですか？

- その鍵についてはあきらめるしかない
 - 署名済みゾーンデータは**まだ**有効なはず
- KSKとZSKでリスクは大きく異なるけど...
 - 新たな秘密鍵を生成
 - ⇒ KSKだとDSの再登録(上位とのやりとり)
 - 署名のやり直し
 - 以上を署名済みデータの有効期限までに対処
- 秘密鍵の管理は確実に

DNSサーバの引越し(特に運用主体の異なるケース)はどのような手順でおこなうのが良いですか？

- 技術的にはDNSSEC運用のまま可能
 - ただし、前運用主体と新運用主体で秘密鍵の情報を引き継ぐ必要があり、実現は難しい
- 現実的には、一時的にDNSSECを解除するしか手が無いのではないかとされている

ホモグラフィック攻撃は防げるのですか

- 防げません
 - DNSSECの有無とホモグラフィック攻撃は独立
- ちなみに、ホモグラフィック攻撃とは
一見同じドメイン名ですが...
 - <http://日本レジストリサービス.jp/>
 - <http://日本レジストリサービス.jp/>
 - 上は「一」(長音) 下は「一」(漢数字)

DNS AmpによるDDoSのリスクが高まることは無視していいのでしょうか？

- 無視して良いわけではないが、DNSを守るという観点からDNSSECは必須
 - 応答データが大きくなり、権威サーバを踏み台にした攻撃が行いやすくなるのは事実
 - = 「DDoSのリスクが高まる」なの？
- DNS Ampへの対処方法として...
 - DNSサーバは、同じソースアドレスからの問い合わせにはレートコントロールを行うべき
 - ISPは是非Ingress Filterの実装を

「署名の検証」vs「ハッシュ計算」

- あるサーバの openssl speed の結果より

type	16 bytes	64 bytes	256 bytes		
sha1	32703.07k	95698.03k	210731.95k		
sha256	24535.69k	59389.97k	108704.00k		
		sign	verify	sign/s	verify/s
rsa 1024 bits	0.000554s	0.000030s	1803.6	32874.3	
rsa 2048 bits	0.003439s	0.000103s	290.8	9690.5	

(Xeon 5540 2.53GHz CentOSにて計測)

DNSSECはキャッシュDNSサーバに厳しい ☹

Q. 追加セクションの扱い

- DNSキャッシュへの毒入れ攻撃は、追加 (Additional)セクションの情報を信用せず、上位から取り直す実装にすればリスクは相当低くなると考えていますが、実際にそのようなパッチをBIND 9に実装するとDNSSECで困るといふのをbind-users MLでみかけました
- DNSSECでは追加セクションの扱いは何か変わるのですか

A. 追加セクションの扱い

- 追加セクションのデータの扱いは、元々「権威のある回答」と「権威の無い回答」である程度の差異がある
- DNSSECにおいては、データの出所が権威ある回答からもらったものであれば、追加セクションのデータにも署名が付加される
 - 署名検証ができれば信頼できるデータと判断可

Q and A

