AAAAフィルタとDNSSECは仲良くなれるのか

民田雅人 <minmin@jprs.co.jp>
株式会社日本レジストリサービス

2012-01-20 JANOG29@和歌山

AAAAフィルタ

- IPv6時代の、IPv6閉域網で新しいOSを利用しているユーザーへの必須(?)の対策
- BIND 9.7以降でサポート
- コンパイル時にオプションの指定が必要

```
./configure --enable-filter-aaaa
```

- ここではAAAAフィルタの是非は問わない

素朴な疑問: 誰がBIND 9に、AAAAフィルタ欲しいと思ったんだろう…

AAAAフィルタの設定

- BIND 9の設定ファイルでoptionsに設定

```
filter-aaaa-on-v4 <設定値>;
```

- 設定値は次の3種類

```
no | yes | break-dnssec
```

- yes と break-dnssec は何が違うの?

DNSSEC運用のドメイン名を アプリケーションが署名検証する場合

	filter-aaaa-on-v4の設定	
	yes	break-dnssec
AAAAのフィルタ	**効かない**	効く
AAAAの署名検証	出来る	**出来ない** ※
Aの署名検証	出来る	出来る

※DNSSECの署名を検証しようにも、DNSSEC運用ドメイン名と見なせない応答パケットとなる

- 署名検証はできずDNSSECとしてはエラーだが
  - その場合A(IPv4)へフォールバックするのか?
  - それ以前に署名検証しようとするのか?

filter-aaaa-on-v4 まとめ 1
AAAAフィルタとDNSSECの仲は?

- yes; AAAAがフィルタされない
  - 署名検証する相手にまでフィルタすべき?
- break-dnssec; 不具合が発生
  - Aにフォールバックすれば大丈夫か? (実装依存)

⇒ AAAAフィルタとDNSSECの仲はイマイチ

- 現状DNSSECの署名検証を、DNS経由で直接行うアプリは実験的用途を除き存在しない
  - 通信路(家庭用ルーター、ホテル内ネットワーク等)がDNSSEC的にクリアである必要がある

filter-aaaa-on-v4 まとめ 2
AAAAフィルタ設定時の注意

- AAAAフィルタを設定すると
  - 通常のDNS応答パケットと違い yes / break-dnssec とも、DNS応答の回答セクションにフィルタが影響し権威・追加セクションがそのまま残り、厳密なフォーマットチェックでエラーとなる

⇒ AAAAフィルタって、やっぱり汚い

- ブラウザ等の一般アプリケーションは、厳密なチェックは行わないので問題とはならない
  - キャッシュDNSサーバー等では問題になる

参考資料: 調査結果一覧

サイトにAAAAが ○：有る (両方) ×：無い (Aのみ)	サイトが DNSSEC ○：運用する ×：運用しない	アプリケーションが ○：署名検証する ×：署名検証しない	BIND 9での設定 filter-aaaaの値 yes / break-dnssec	結果 AAAAのフィルタ ○：効く ×：効かない △：関係無い	結果 A RRで 署名検証の不具合が ○：発生しない ×：発生する	結果 AAAA RRで 署名検証の不具合が ○：発生しない ×：発生する
×	×	×	yes	△	○	○
○	×	×	yes	○	○	○ (※)
×	○	×	yes	△	○	○
○	○	×	yes	○	○	○ (※)
×	×	○	yes	△	○	○
○	×	○	yes	○	○	○ (※)
×	○	○	yes	△	○	○
○	○	○	yes	×	○	○
×	×	×	break-dnssec	△	○	○
○	×	×	break-dnssec	○	○	○ (※)
×	○	×	break-dnssec	△	○	○
○	○	×	break-dnssec	○	○	○ (※)
×	×	○	break-dnssec	△	○	○
○	×	○	break-dnssec	○	○	○ (※)
×	○	○	break-dnssec	△	○	○
○	○	○	break-dnssec	○	○	× (※)

※ 権威セクションの内容がDNSパケットとして異常であるため、キャッシュDNSサーバー等で厳密にチェックする場合はフォーマットエラーとなる

jPRS
JAPAN REGISTRY SERVICES