つぶらな瞳で考える、DNSSECの普及に必要な何かは何か？JANOG45でやったやつのおさらい

JPCERT/CC 中井 尚子

IIJ 其田 学

QTnet 末松 慶文

JPNIC→長崎県立大 岡田 雅之

DNSSECの普及？

- DNSのSecurityなんだから当然広まるよね！
  - でもどうやらちょっと悲しい状況らしい
- 自分の住んでる場所と比較
  - BGPルーティングと比較して考える
- BGPルーティング：相互信頼でセキュリティは・・・・
- どちらも相互信頼、悪意にあがなうすべが厳しい技術
- BGPSec/RPKIを活用したルーティングは普及の兆しが見える
- DNSSECはどうなんだろう？

	RPKI/ROA wit Origin Validation	DNSSEC
元々の技術	BGP 牧歌的	DNS 牧歌的
かかわる人数	少なめ	たくさん
かかわる機械	少なめ	たくさん
運用する集団	集中が進行？	オンプレミスな運用が多？

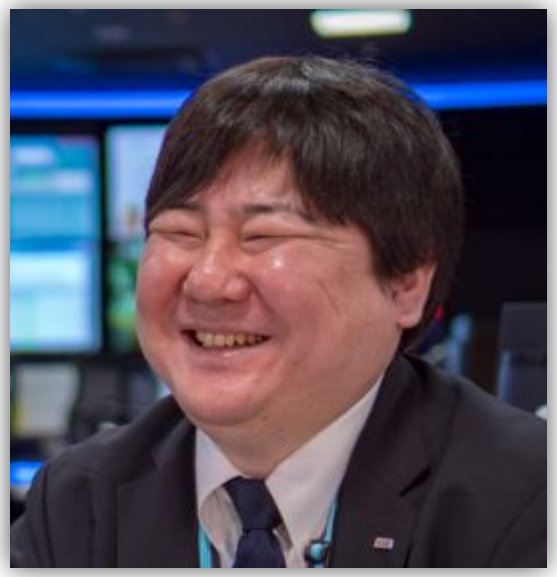
DNSSECに対する暖かい声

人類には早すぎる	ほげほげ
コミュニティへの無駄な負荷	ほげほげ
DNSのセキュリティをより悪化させる	もげもげ
難しい	うげうげ
インターネットの安定を損なう	にんにん
DNS自体が問題	うほうほ

普及を阻むものは何だろう？

JPCERT/CC 中井さん

IIJ其田さん



QTnet末松さん

議論のポイント・ログ

- 普及状況
  - 海外では進みつつある。日本は？
- 対応が進んでいる国
  - スウェーデン
  - アイスランド
  - サウジアラビア
- ソフトウェアの成熟
- 日本で普及が進まないのはなぜ？
  - 鶏卵を考えている場合じゃない？
- なぜ？
  - DNSSECに興味がない？顧客が要望しない。

議論のログ

- **100% 近く普及しないといけない がんばれ**
  - **→暖かいご声援･ご清聴ありがとうございます！**
  - 中途半端はだめ
  - 第一フラグメント攻撃を発表した人がいっている
    - 毒をいれやすくなる。対案も証明できてない
  - ゾーンがでかくないとかそれは関係ない
  - TLDから委任がされる、毒を入れる。
  - 隣のゾーンが大きいと危ない
    - グルーに隣のゾーンから毒をいれることができる。
  - みんなで署名してみんなで検証するしかない。
- Dosをどう対抗するかを考えておかないといけない

議論のログ

- JPドメイン名のOPT OUTをやめてすべての委任をまもってほしい
  - (オーディエンス)賛成！
- みんなが一斉にがんばらないといけない
  - Port Randmizationのときはみんなでがんばったけど、
  - 第一フラグメント攻撃でカミンスキーの前のID16びtにもどってる
  - 数分でドクドクいれられちゃう
  - ご近所さんの偽グルーでやられてしまう

議論のログ

- 経験から
  - 個人でとったJPドメインにDNSSEC署名をおくろうとおもったけど、レジストラで手数料とられたくないとおもうと選択k氏がすくない
  - 指定事業者たる義務があるべ→すぐできるんでおくってください、でできた
  - そのくらいライトのはずなのにレジストラがしない、一部のレジストラは高額な料金をとられると観測されている
  - 特にJPRSというよりは、dン祖psでも議論がつづいているけどレジストラの方の関心がすくない？後にくるオペレーションもあるけどなぜレジストラは外にDS登録のオプションをだしていないのかなぁ。と。
  - 署名が先か検証が先かとあるけど、かんがえられれば。
  - →本当は規約で取り次がないといけない、技術的なハードルはない

議論のログ

- 今回はDNSSECだけどほかのテクノロジーの話でもある
  - DKIMとかIpv6とか
- 事業者が有効にしても顧客が利用しない
  - Googleゆざーが顧客にDKIMどれだけ有効にしているか、しらべたが日本はすくなかった。
  - 日本の特性かもね
- 中井さんのコメント
  - EPPやられると本当は、、、
  - 多層防御でたすけられるはず
  - DNSSEC推奨：政府主導型、DNSSEC/TLS/DKIMセット割、企業推進型