InternetWeek2013

DNS DAY(D2)

DNSSEC Update

株式会社ブロードバンドタワー
大本　貴

自己紹介

- 職歴
  - 2000年 インターネット総合研究所入社
  - 2001年 プロデュースオンデマンド(PoD)に出向
    - ストリーミング配信技術担当
  - 2007年 インターネット総合研究所に帰任
    - 主に社内システムのサーバ運用、コンサルなど
    - 2010年春からDNSSECジャパンの活動に参加
  - 2010年 ブロードバンドタワーに転籍
    - DNSSECジャパンの活動終了に伴いDNSOPS.jpの活動に合流

twitterでたまにDNSSEC関連のつぶやきをしています。

@taxiJPN

最初に

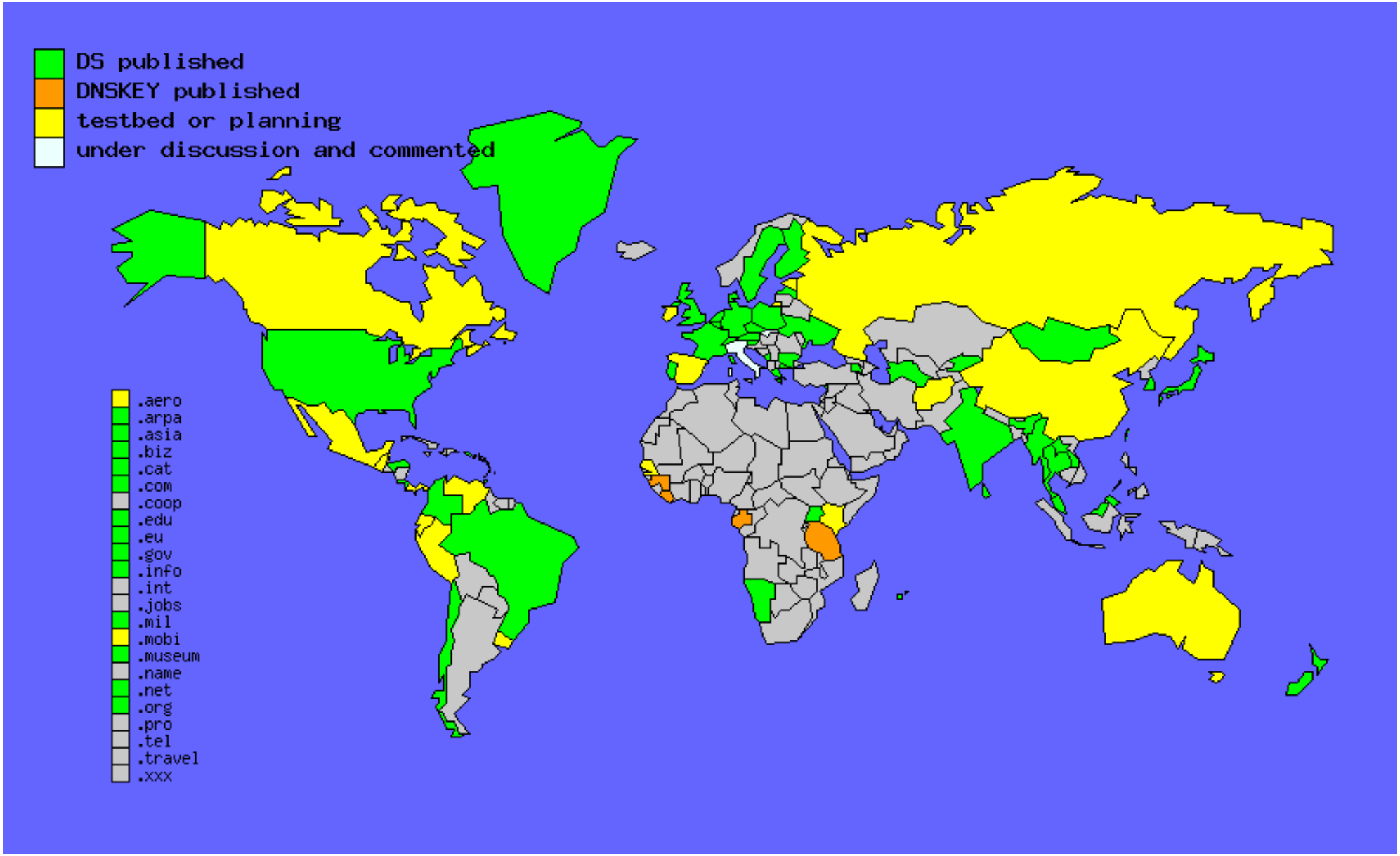
- この一年間でのDNSSEC関連のupdate情報についてまとめました。(2012年11月～2013年11月まで)

- これらの情報はccTLDのレジストリwebサイトやICANNの資料、DNSコミュニティ関連ML、JPRS社提供の情報等を確認してまとめたものです

- Agenda
  - DNSSEC導入状況 update
  - DNSSEC関連RFC update
  - DNSSEC関連Topics ＆ 動向 update

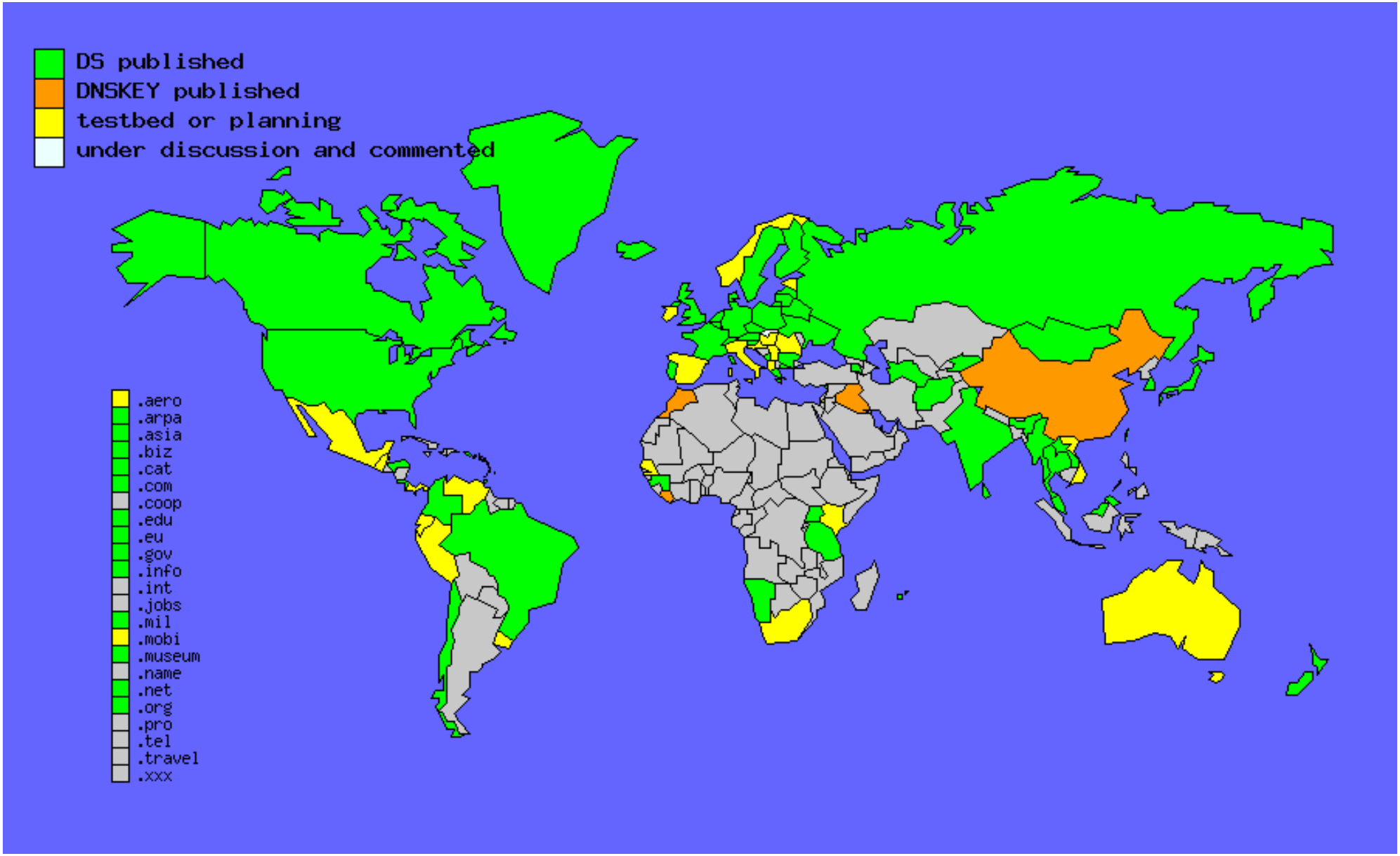
- Agenda
  - DNSSEC導入状況 update
  - DNSSEC関連RFC update
  - DNSSEC関連Topics ＆ 動向 update

DNSSEC対応状況(2012/11/25)



- **http://www.ohmo.to/dnssec/maps/**

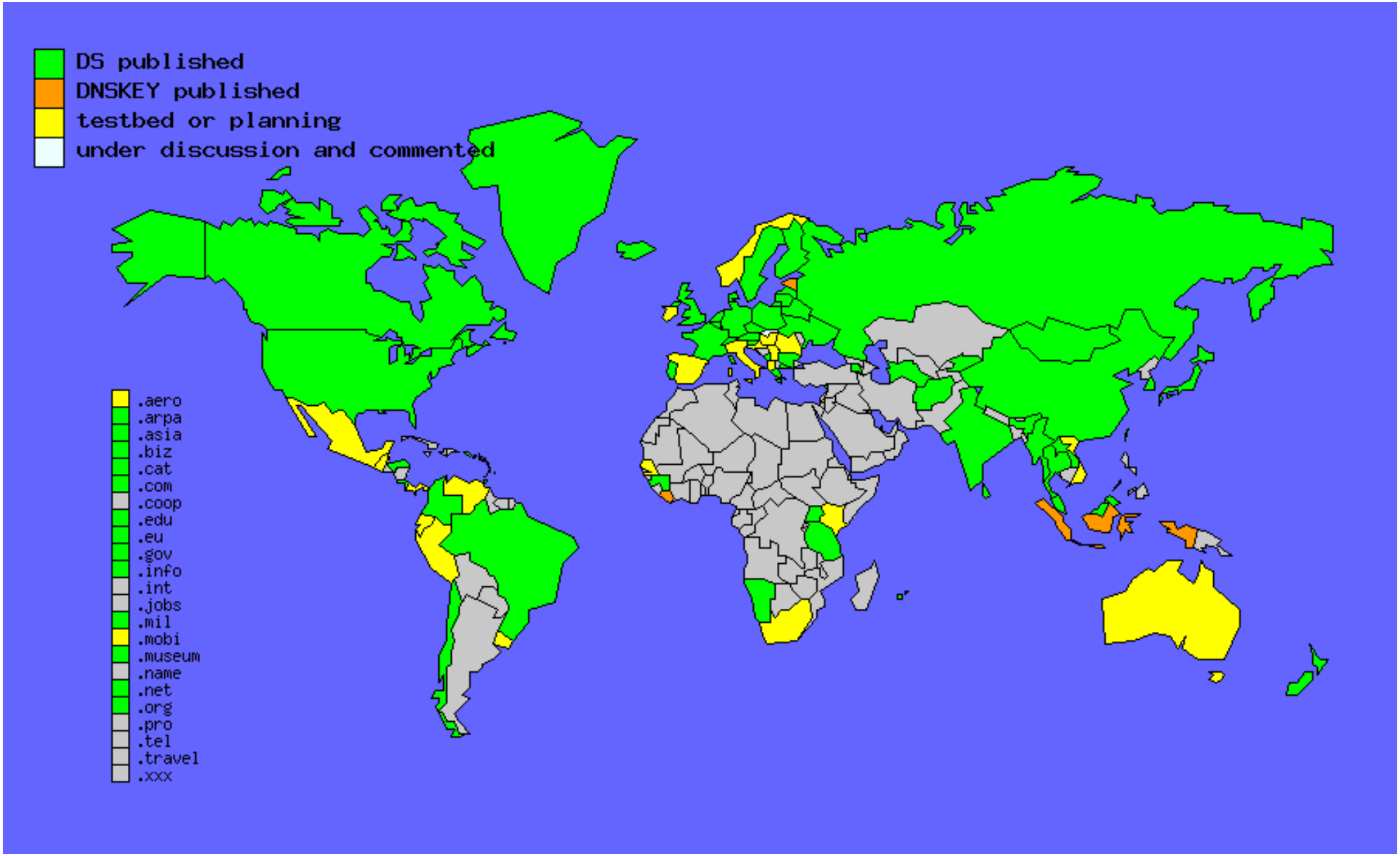
DNSSEC対応状況(2013/11/01)



- **http://www.ohmo.to/dnssec/maps/**

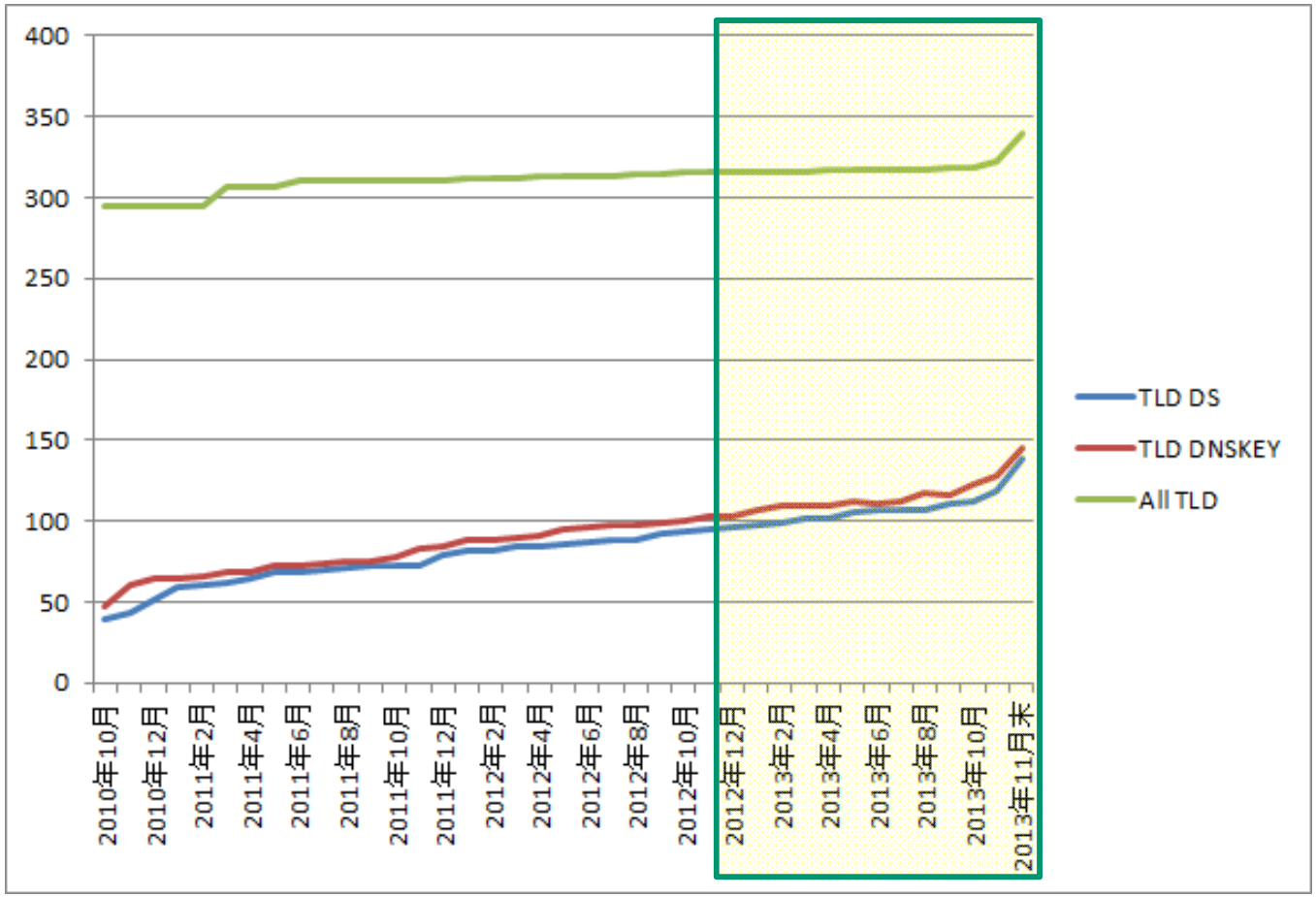
DNSSEC対応状況(2013/11/26)

BroadBand Tower, Inc.



- **http://www.ohmo.to/dnssec/maps/**

TLD導入推移状況



- 2013年5月 TLD全体の33%(105/317TLD)が導入済み。
- 2013年10月末現在 37%(119/323TLD)が導入済み。
  (2013年11月26日現在 41%(139/340TLD)が導入済みに)←new

レジストラのDS取次状況

BroadBand Tower, Inc.

- ICANNのページにて情報公開してます。(申告制)
- http://www.icann.org/en/news/in-focus/dnssec/deployment

Deploying DNSSEC

Share

Registrars that support end user DNSSEC management, including entry of DS records

Last updated: 17 Jan 2013

Registrar	Accepts DS records for	Notes
123domain.eu (DE)	.de, .eu, .be, .se, .cz, .fr	(1) (2)
AB Name ISP (SE)	.be .biz .com .eu .net .org .se .us	(1) (2)
Binero (SE)	.se, .eu	All domains are automatically signed. (1) (2)
DK-Hostmaster (DK)		A list of DNSSEC DS supported domains could not be located on the site.
Domaininfo AB (SE)	.se .eu .us .biz .com .net	Also supports DS record entries for domains you may host elsewhere. (1)(2)
DYN (US)	.org, .se	(1) (2)

2013年1月から更新停止しているが、この時点でレジストラ側では40TLDのDNSSEC対応

- Agenda
  - DNSSEC導入状況 update
  - DNSSEC関連RFC update
  - DNSSEC関連Topics ＆ 動向 update

DNSSECに関連するRFCのupdate

- **RFC 6781**　DNSSEC Operational Practice v2　(Informational)
  - RFC 4641の更新版。2012年現在の運用ノウハウをまとめたもの。
  - 鍵サイズ　1024bit推奨　→　2048bit推奨、レジストラ移転について言及追加など。

- **RFC 6840**　DNSSECの仕様明確化と実装ノート (Standards)
  - DNSSECを実装するにあたり、これまでのRFCでは明確にされていなかった箇所を明記。
  - NSEC3、SHA256、BADキャッシュの実装や、ADビット、CDビットの取り扱いなど。

- **RFC 6841**　DNSSEC運用ステートメントのフレームワーク　(Informational)
  - DPS (DNSSEC Practice Statements)　の記述書式・項目などを定義したもの。
    DNSSECを適用するドメインの運用管理ポリシーを定義

- **RFC 6944**　DNSSEC DNSKEY Algorithm Status　(proposed standard)
  - 実装すべき暗号アルゴリズムについてRFC4041のA.1をupdate。
  - RSA/MD5は推奨しない→使用禁止に。RSA/SHA256などを実装推奨として追加など。

- **RFC 6975**　Signaling Cryptographic Algorithm Understanding in DNS Security Extensions (DNSSEC)　(proposed standard)
  - バリデータが解釈できる署名/ハッシュアルゴリズムをEDNS0のオプションでサーバに通知する仕組みについて定義。
  - RFC 6891によりEDNS0に新しく定義されたPseudo-RR(meta-RR) を利用する3つのアルゴリズムを定義。DAU(DNSSEC　Algorithm Understood) 、DHU(DS Hash Understood)、　N3U(NSEC3 Hash understood)

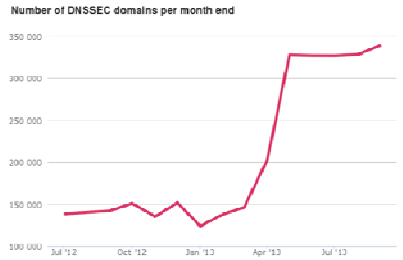
BroadBand Tower, Inc.

- Agenda
  - DNSSEC導入状況 update
  - DNSSEC関連RFC update
  - DNSSEC関連Topics ＆ 動向 update

DNSSEC関連Topics

BroadBand Tower, Inc.

- **Google public DNS (8.8.8.8)のDNSSEC対応(3月)**



- **.seで導入済みドメイン数急増**
  116万ドメイン中、14万ドメイン 12%前後 2013年4月
  121万ドメイン中、33万ドメイン 27%前後 2013年10月
  https://www.iis.se/english/domains/domain-statistics/growth/?chart=per-type
  - スウェーデンの最大手レジストラの一つが全ての顧客のドメインをDNSSEC署名したとのこと。

- **Afnic(.frなどのレジストリ)では9月末よりDNSSEC適用キャンペーンを開始。**
  http://www.afnic.fr/en/about-afnic/news/operations-news/7355/showOperational/dnssec-promotional-campaign-check-it-out-1.html
  - Financial Incentive あり

- **GoDADDYのICANN47での発表**
  - 6000ユーザがGoDaddyの準備したDNSSEC toolを利用中、3500ユーザがDSを登録申請している。と発表。(なおGoDaddy全体は850万ユーザ以上)

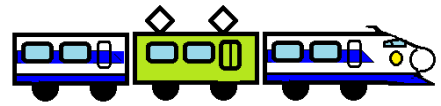
- **.govが、去年に引き続き、また・・・。(8月)**
  - 新しいKSK鍵のDSがrootに登録されてないのにKSKを切替
  - その一方で.govの80%がDNSSEC適用済みに。

- **そして10月に開始した新gTLDでも・・・。**
  - 2つの新gTLDでいきなり署名期限切れトラブル(11月2日)
  - Онлайн(ロシア語でOnline) http://dnsviz.net/d/xn--80asehdb/UnVEfA/dnssec/
  - Сайт(ロシア語でWeb site) http://dnsviz.net/d/xn--80aswg/UnYZQg/dnssec/

DNSSEC関連Topics(技術寄り)

BroadBand Tower, Inc.

- First-Fragment piggybacking attacks問題



  - http://www.ietf.org/proceedings/87/slides/slides-87-saag-3.pdf
  - UDPパケットの分割された2番目以降のパケットの代替として偽装パケットを割り込ませることで不正な処理を引き起こせる。
  - DNSSECはUDPペイロードサイズとしては4000バイトが推奨サイズ(SHOULD ※RFC4035より)であるため、UDPパケットが分割処理されるケースが想定される。このため、攻撃の影響を受ける対象として懸念されている。
  - 攻撃の影響として検証でのbogusや、それを利用したDoS Attackの可能性

- JP DNSサーバーに設定されるDS RRのTTL値の変更
  - http://jprs.jp/tech/notice/2013-11-06-jpdns-ds-ttl-change.html
  - TTL値1日→2時間へ変更(2013/11/17より)
  - KSKのキーロールオーバー処理等で発生した不整合に対する対策(復旧時間の短縮)
  - KSKロールオーバーに必要な総作業時間の短縮も期待できる対策

DNSSEC動向その他

BroadBand Tower, Inc.

- DNSSECの普及とDANE
  (DNS-Based Authentication of Named Entities)
  - そもそもDANEって何ぞや?

    SSL(TLS)+DNSSECで、通信の信頼性をより高める仕組み。

    →Dan YorkさんのICANN47でのWorkshop資料が
    概要としてわかりやすく入門におすすめ。

    http://durban47.icann.org/meetings/durban2013/presentation-dnssec-dane-intro-17jul13-en.pdf

    →さらに突っ込んだ話はDNSSEC2012スプリングフォーラムでの
    セコム(株)IS研究所の島岡さんの資料がおすすめです。

    http://dnssec.jp/wp-content/uploads/2012/04/20120425-panel_tls-shimaoka.pdf

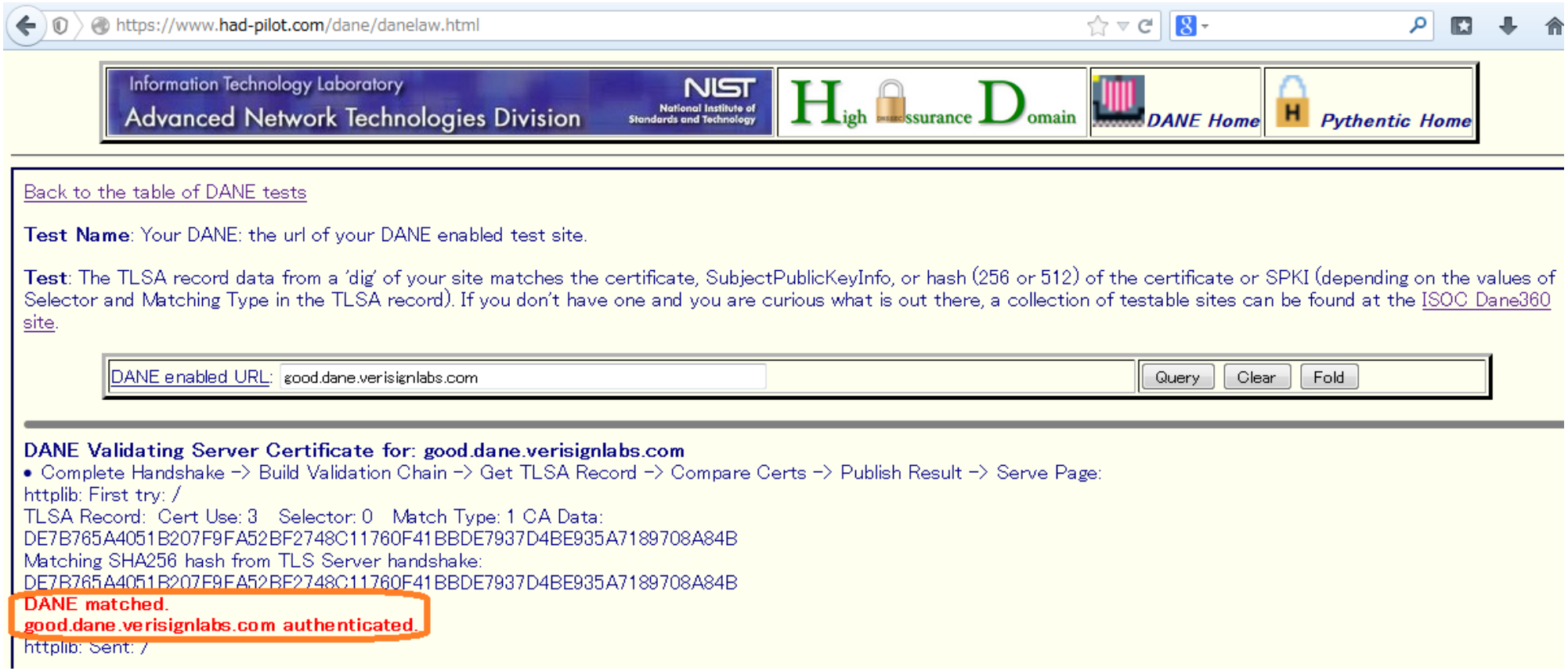
近年はDNSSECの普及におけるキーポイントと見なされているようで、海外の
DNSSEC関連プレゼン資料などでもよく見かけるキーワードとなってきた。

DANE

BroadBand Tower, Inc.

DANE対応済みサイトか確認できるwebツール(米NIST.gov公開)

https://www.had-pilot.com/dane/danelaw.html



まとめ

- 各TLD・レジストリのDNSSEC対応は順調に進んできている。
  - 既存TLDでの順調な導入傾向に加え、新gTLDでは運用開始時にDNSSECは必須事項のため今後も導入数は増加する見込み
  - 各レジストラでのDS取次サービスでも対応TLDが増加。
  - TLDによってはドメイン登録数が急増しているTLDも。
  - ただし、ドメイン登録数およびDNSSEC対応ドメイン数は非公開のTLDが多く実際の普及度は判断しにくい。

- 実運用経験が蓄積された結果、RFCも当初不足していた内容を補完するように更新されたものが出てきている。

- DANEがやや脚光を浴び始めたのに伴い、DNSSECの導入促進について期待と議論がある一方、DoS攻撃への脆弱性なども指摘されている。

- .govのfailedのような失敗もあるが、JPRSのTTL短縮の試みなど、失敗した時のリスク低減をするような試みも始まっている。

参考情報

- IANA TLD DNSSEC Report
  - http://stats.research.icann.org/dns/tld_report/
- Registry Services Evaluation Process (gTLD)
  - http://www.icann.org/en/registries/rsep/
- 各TLDレジストリwebサイト
  - http://www.iana.org/domains/root/db/ からリンク

- ICANN46 DNSSEC Workshop資料 (2013/4/7-11開催)
  - http://beijing46.icann.org/beijing46/documents
- ICANN47 DNSSEC Workshop資料 (2013/7/14-18開催)
  - http://durban47.icann.org/documents
- ICANN48 DNSSEC Workshop資料 (2013/11/17-21開催)
  - http://buenosaires48.icann.org/en/schedule/wed-dnssec
- 発表者のサイト
  - www.ohmo.to
    - http://www.ohmo.to/dnssec/maps/
      今回の資料に関係する情報ソースを一部リンクしています。
- 発表者のつぶやき
  - twilog.org/taxiJPN (twilogおよび製作者の@roprossさんありがとうございます)
    - http://twilog.org/tweets.cgi?id=TaxiJPN&word=dnssec
      上記URLで今回の資料に関係する情報ソースのつぶやきが確認できます。

ご清聴ありがとうございました。