

InternetWeek2014

DNS DAY(D1)

DNSSEC Update

株式会社ブロードバンドタワー

大本 貴

• 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

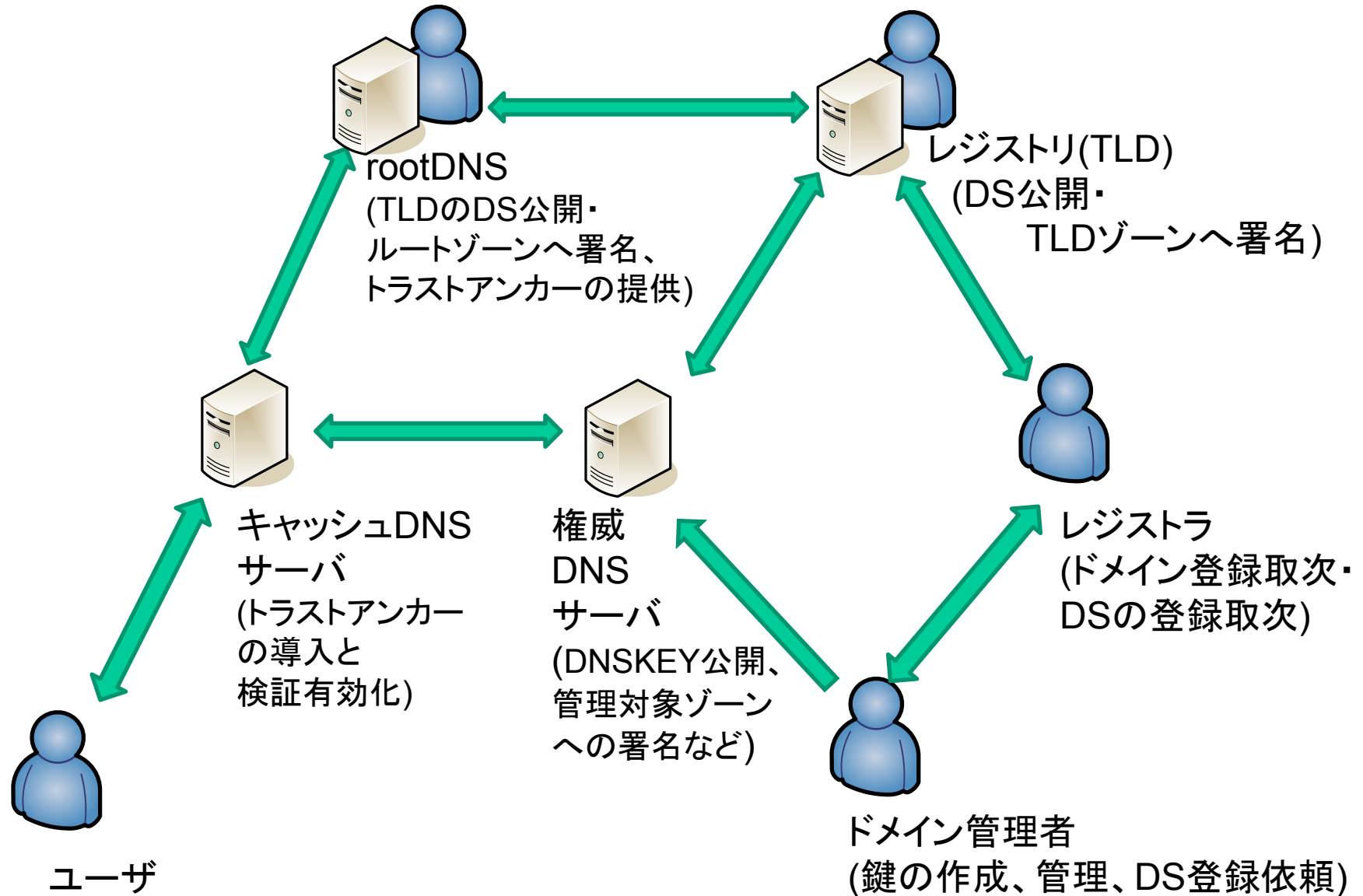


- この一年間でのDNSSEC関連のupdate情報についてまとめました。(2013年11月～2014年11月まで)
- これらの情報はccTLDのレジストリwebサイトやICANNの資料、DNSコミュニティ関連ML、JPRS社提供の情報等を確認してまとめたものです

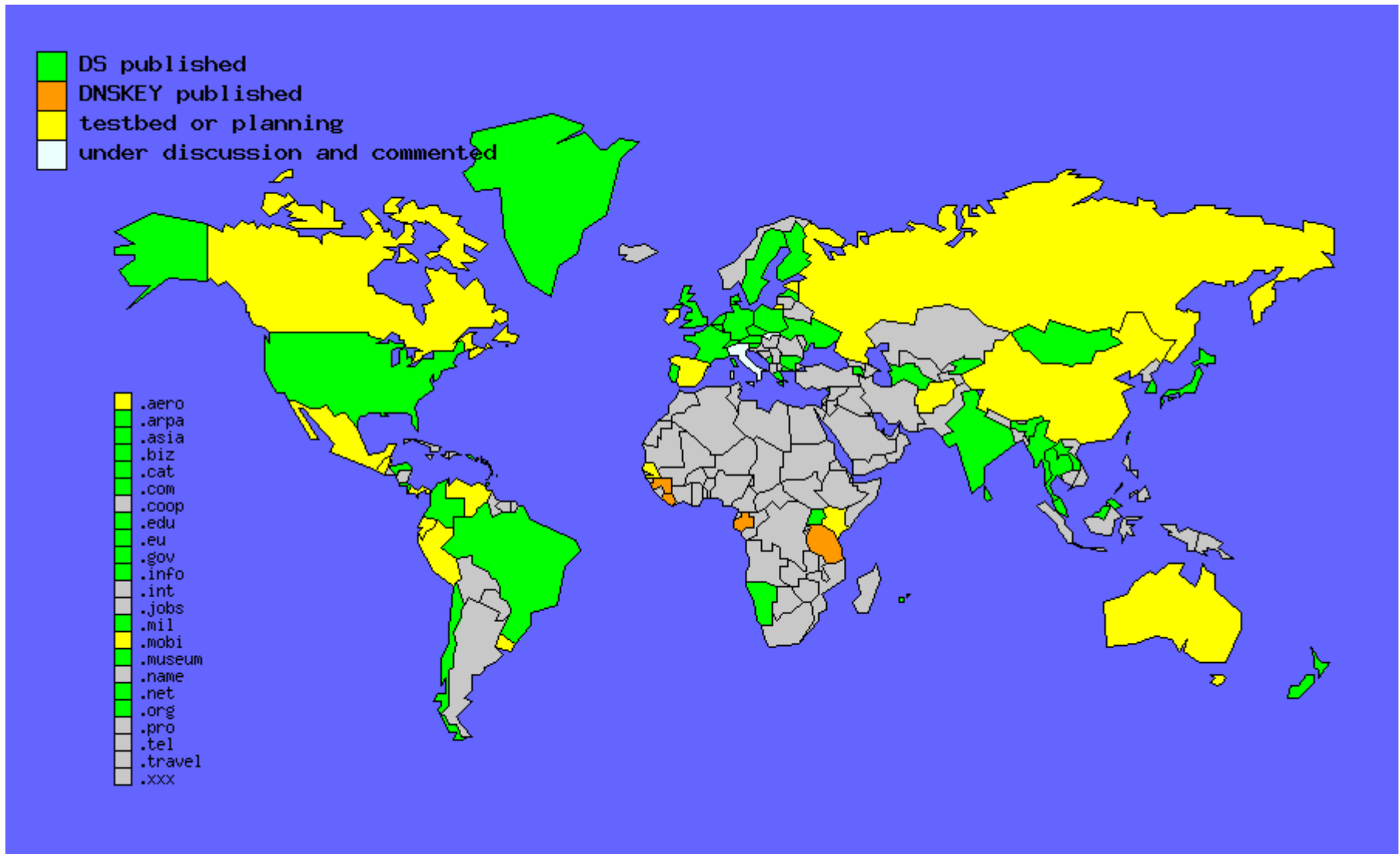
- Agenda
 - DNSSEC導入状況 update
 - DNSSEC関連RFC update
 - DNSSEC関連Topics & 動向 update

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

DNSSEC対応が必要な関係組織・システム

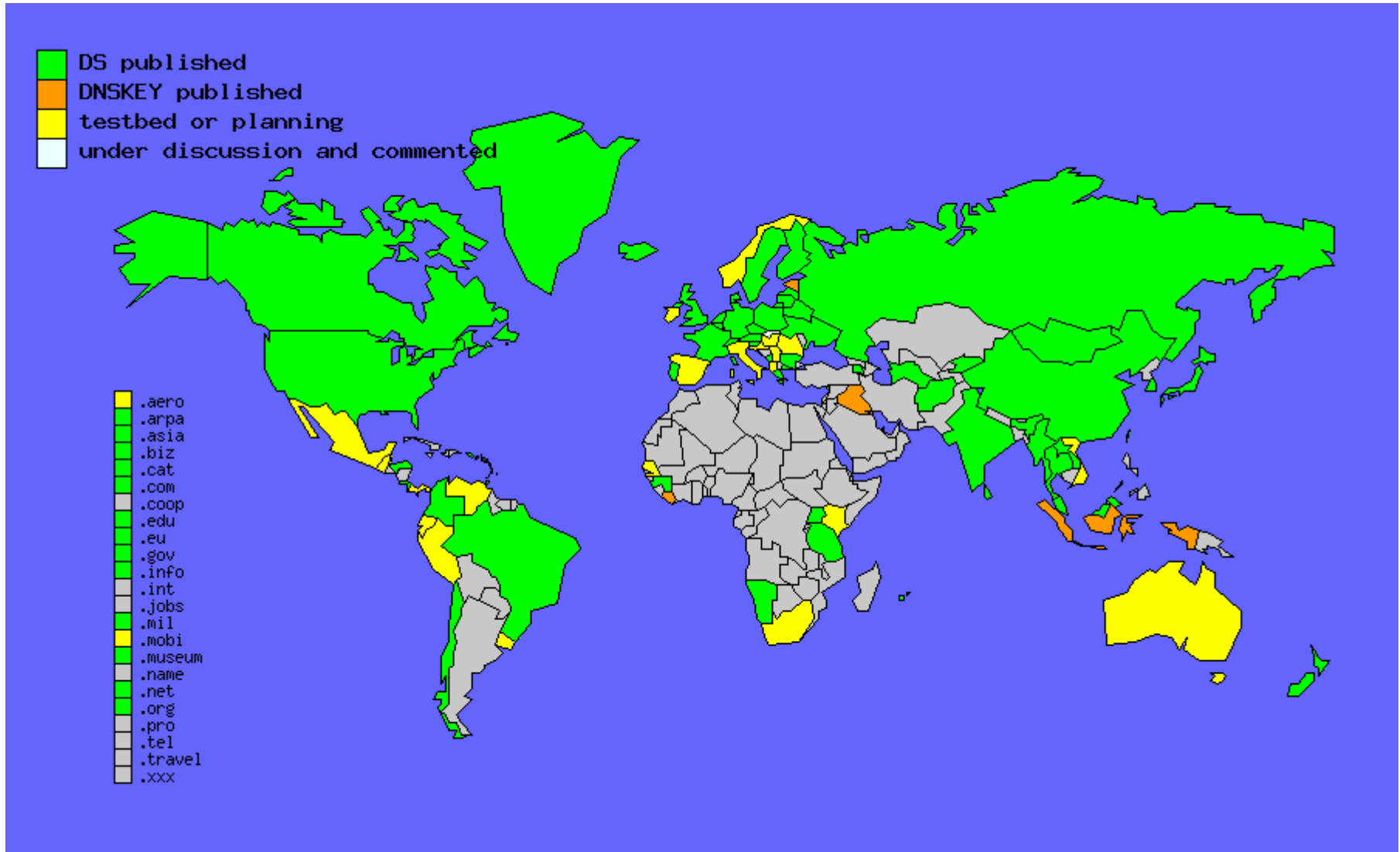


ccTLD & gTLD導入状況(2012/11/25)



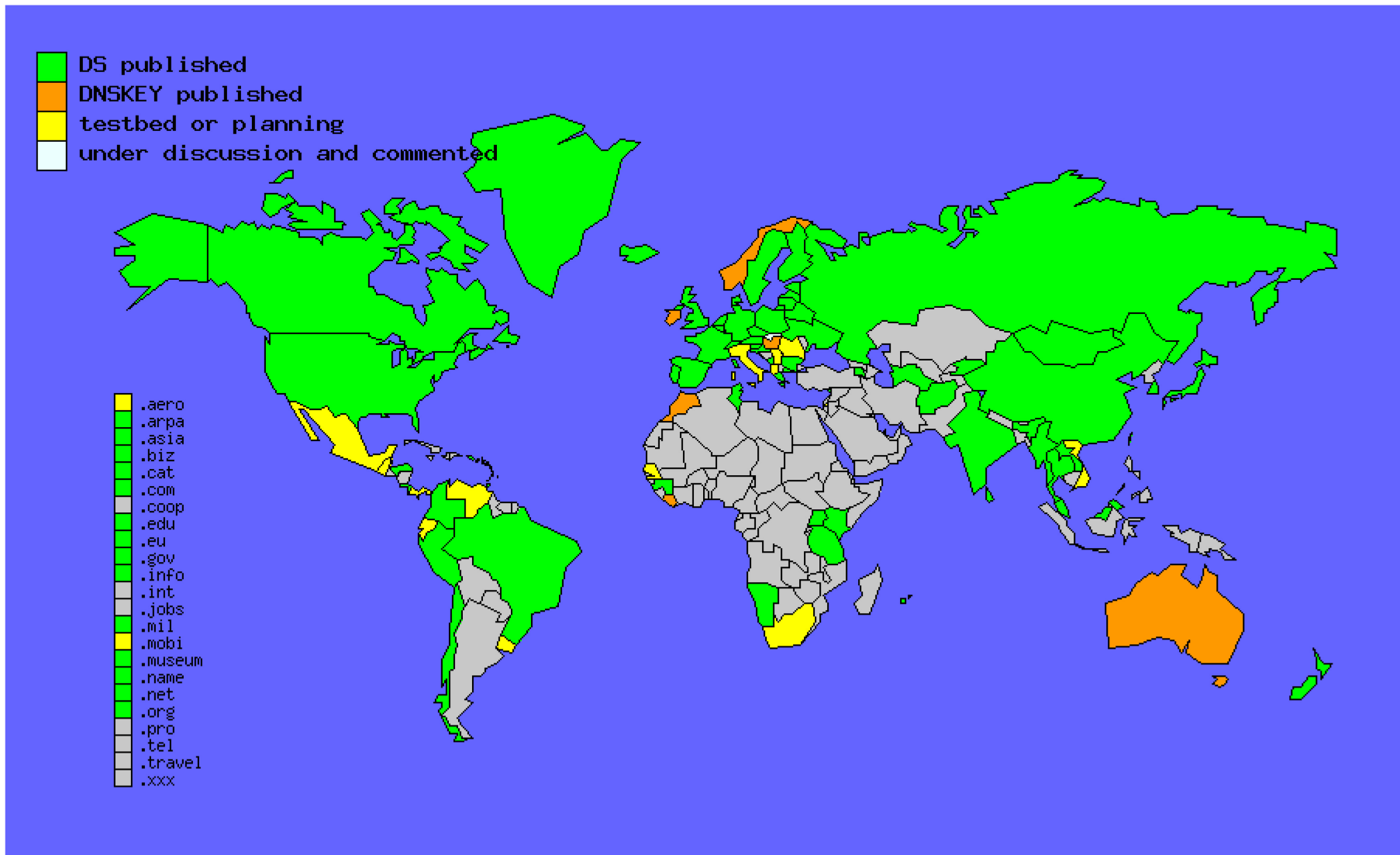
- <http://www.ohmo.to/dnssec/maps/>

ccTLD & gTLD導入状況(2013/11/26)



- <http://www.ohmo.to/dnssec/maps/>

ccTLD & gTLD導入状況(2014/11/04)



- <http://www.ohmo.to/dnssec/maps/>

ccTLD & gTLD導入状況

この1年でステータス変化のあったTLD (new-gTLDに属するTLDは除く)

DNSSECを導入したTLD	Rootゾーン導入日
.ee (エストニア)	2013/12/26
.pe (ペルー)	2014/01/20
.name	2014/01/25
.ke (ケニア)	2014/03/21
.aw (アルバ)	2014/03/29
.ad (アンドラ)	2014/05/15
.sj (スバルバル諸島・ヤンマイエン島)	2014/05/16
.es(スペイン)	2014/07/16
.hr (クロアチア)	2014/07/16
.tn (チュニジア)	2014/09/26

DNSKEYを公開したTLD	DNSKEY公開日
.id (インドネシア)	2013/12/09～ 2014/03/05
.ma (モロッコ)	2014/02/21
.au (オーストラリア)	2014/04/24
.hu (ハンガリー)	2014/04/24
.no(ノルウェー)	2014/10/30
.ie(アイルランド)	2014/11/04

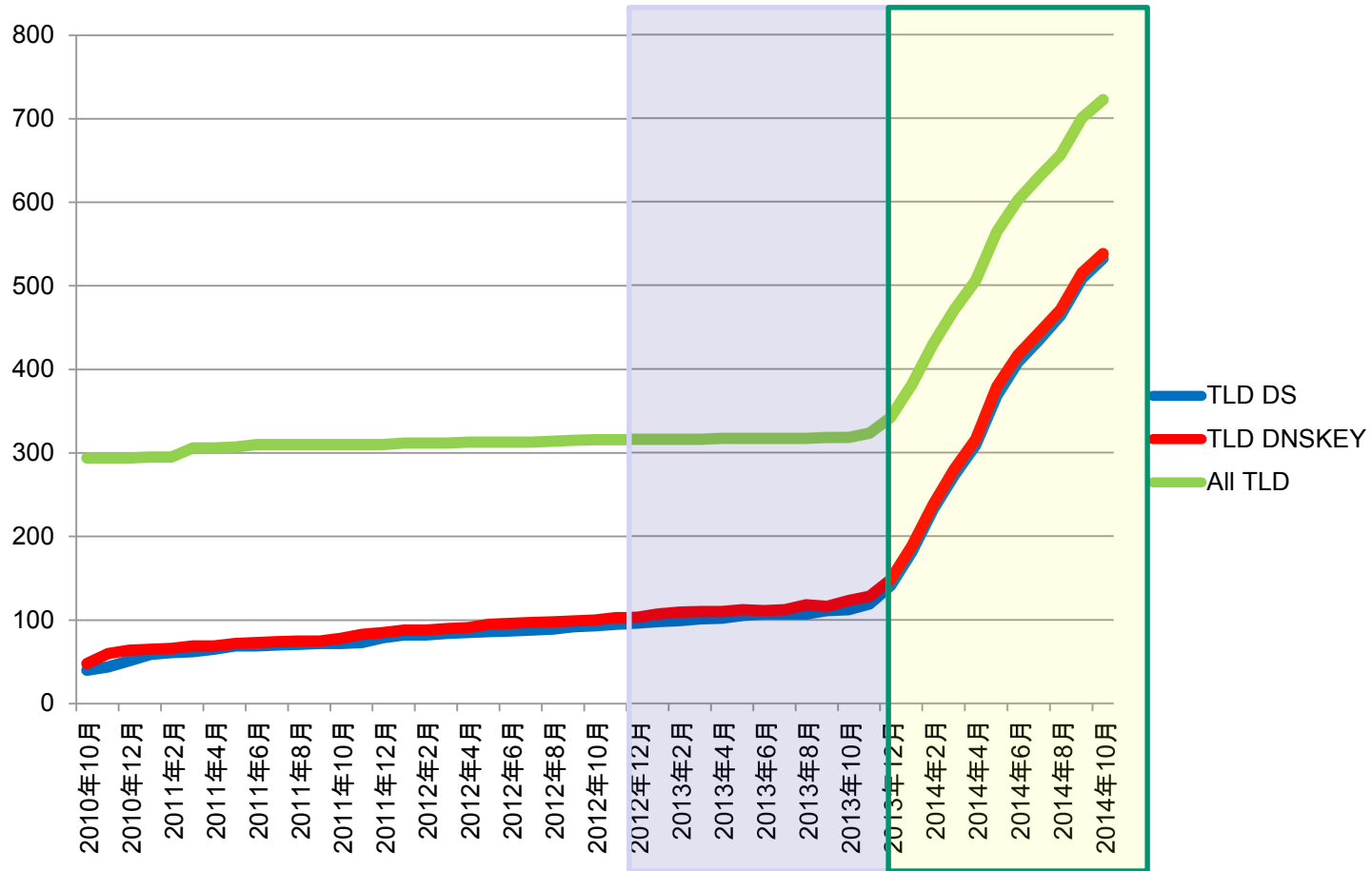
1年でRootにDSを署名されたTLDは10TLD、

(→資料提出後. ieと.noもDS署名済みになり12TLD)

DNSKEYを公開したTLDは上記10TLDに加え6TLD。(→12TLDに加え、4TLD)

(ただしidは公開終了している。→今月中旬に再度公開されました。)

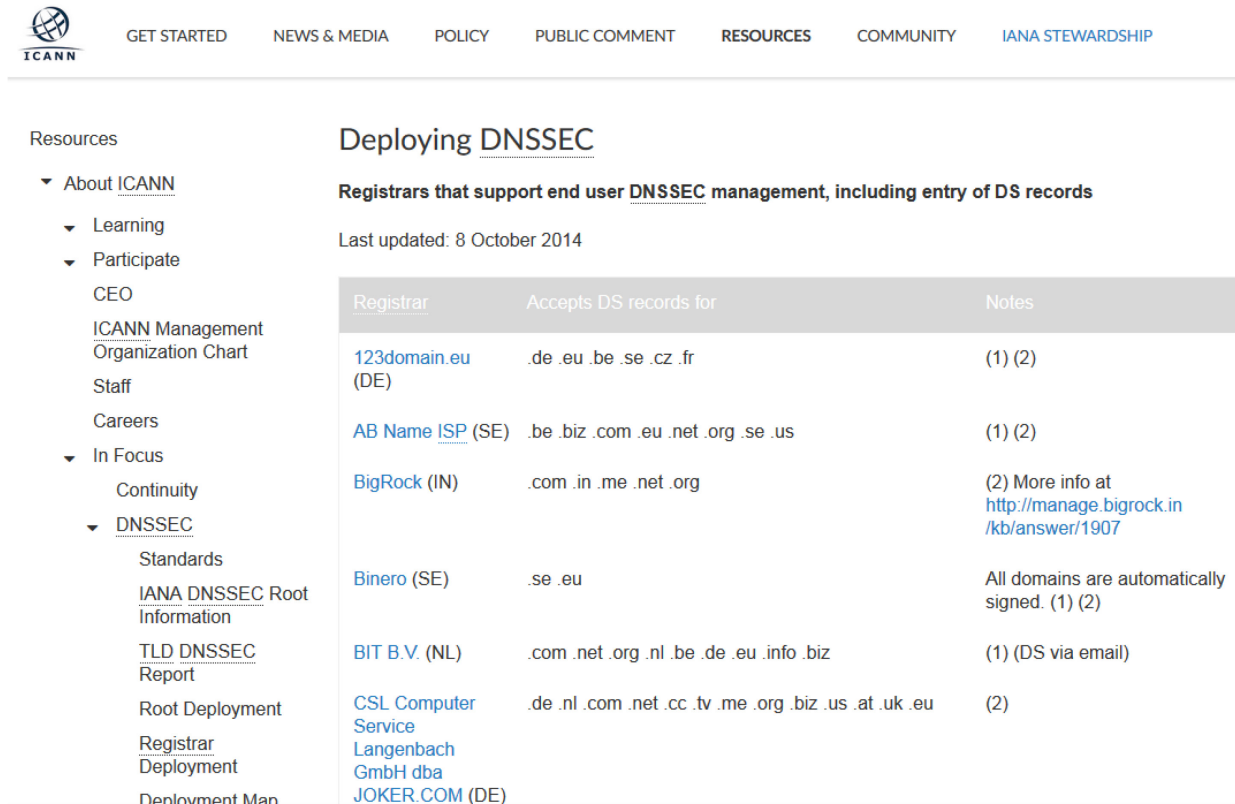
TLD導入推移状況



- 2013年11月末 TLD全体の41%(139/340TLD)が導入済み。
- 2014年10月末現在 74%(532/722TLD)が導入済み。
新gTLDの運用開始により、TLDの分母が倍以上になった影響。

レジストラのDS取次状況

- 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>



Resources

- ▼ About ICANN
 - ▼ Learning
 - ▼ Participate
 - CEO
 - ICANN Management Organization Chart
 - Staff
 - Careers
 - ▼ In Focus
 - Continuity
 - ▼ DNSSEC
 - Standards
 - IANA DNSSEC Root Information
 - TLD DNSSEC Report
 - Root Deployment
 - Registrar Deployment
 - Deployment Map

Deploying DNSSEC

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

Last updated: 8 October 2014

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)
BigRock (IN)	.com .in .me .net .org	(2) More info at http://manage.bigrock.in/kb/answer/1907
Biner (SE)	.se .eu	All domains are automatically signed. (1) (2)
BIT B.V. (NL)	.com .net .org .nl .be .de .eu .info .biz	(1) (DS via email)
CSL Computer Service Langenbach GmbH dba JOKER.COM (DE)	.de .nl .com .net .cc .tv .me .org .biz .us .at .uk .eu	(2)

2013年11月時点でレジストラ側では40TLD
→2014年10月8日時点で 63TLDのDNSSEC対応

- 昨年のDNS SummerDays 2013にて発表された、NTTネットワーク基盤技術研究所 佐藤 一道さんの計測手法を踏襲して、比較した。
 - <http://dnsops.jp/event/20130718/20130718-dnssec-sato-1.pdf>
 - データソースも同じくAlexa Top100万ドメインのリストを利用
 - <http://s3.amazonaws.com/alexa-static/top-1m.csv.zip>
 - 2014/10/28日のリストデータを取得した

検証環境 validator

bind9.8 (Scientific Linux6.1)

```
$dig +dnssec @localhost
```

```
$dig +dnssec @localhost DS
```

```
$dig +dnssec @localhost DNSKEY
```

等を利用し、フラグの立ち方、ステータス、対象リソースレコードおよびRRSIGレコードの有無等を確認した。

権威DNSサーバ普及度調査結果の比較

Alexa人気ランク順100万ドメイン中のステータス内訳

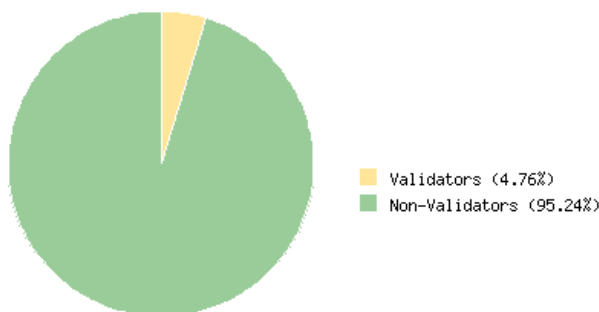
	2013/05/19	2014/06/13	2014/10/28
NoError	959,252	978,834	983,126
NXDomain	18,113	15,964	12,896
ServFail	1,361	1,743	1,669
その他・不明	18,602	3,459	2,309
合計	1,000,000	1,000,000	1,000,000

NoErrorステータス中のDNSSECステータス内訳

	2013/05/19	2014/06/13	2014/10/28
NoError	959,252	978,834	983,126
署名済みドメイン数	7,636 (0.80%)	9,766(0.997%)	10769(1.10%)
Secure	5,827 (0.61%)	7,868 (0.80%)	8570 (0.87%)
Insecure+bogus	1,809 (0.19%)	1,898(0.19%)	2199 (0.22%)
署名済みドメイン中の Insecureドメインの割合	23.7%	19.4%	20.4%

- Verisignlabsの調査データ
- <http://validator-search.verisignlabs.com/>
 - ブラウジングでPrefetchされたデータを元に検証が有効になっているサーバの普及率を調査。
 - 公開された2012年9月時点では3.66%

Preliminary Results



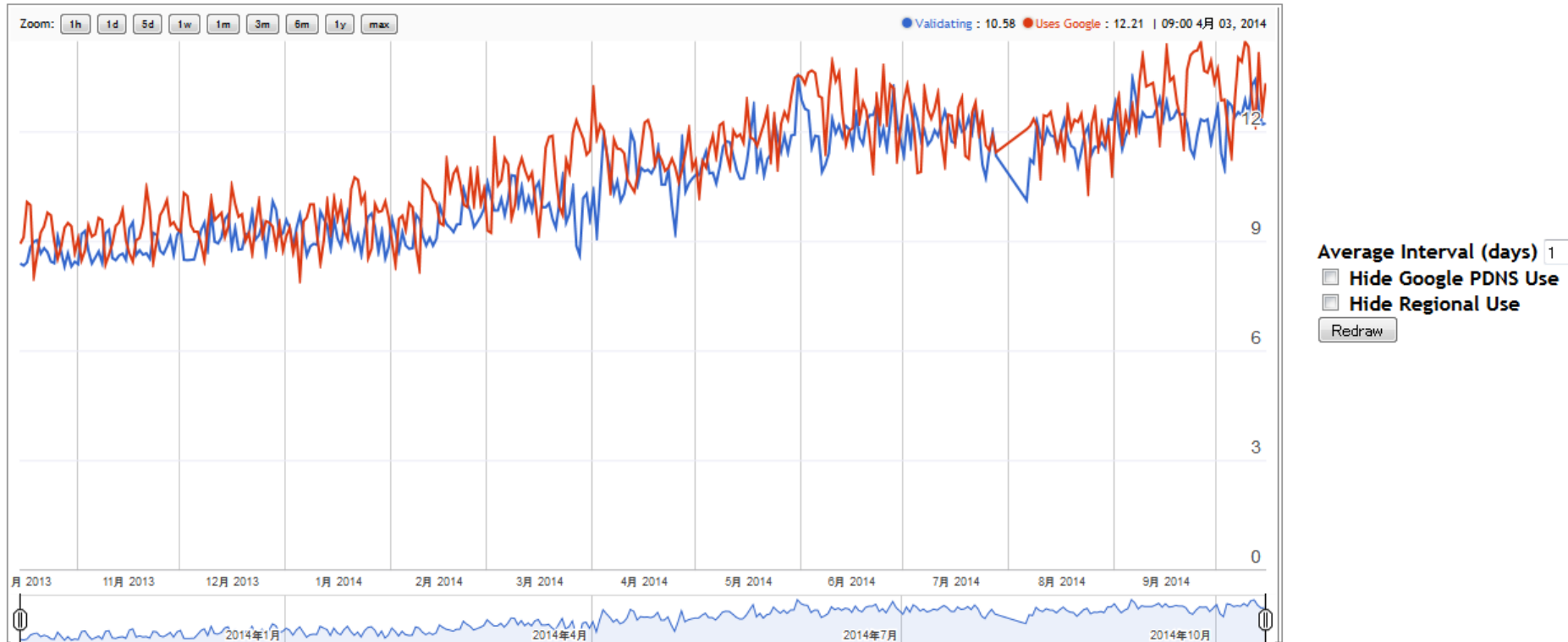
Validators/Non-Validators: 14996/299830

Percentage of resolvers doing DNSSEC validation

- 2014年6月現在4.56%、11月現在は4.76%とやや微増している。

クライアント側のDNSSEC対応状況

Use of DNSSEC Validation for World (XA)



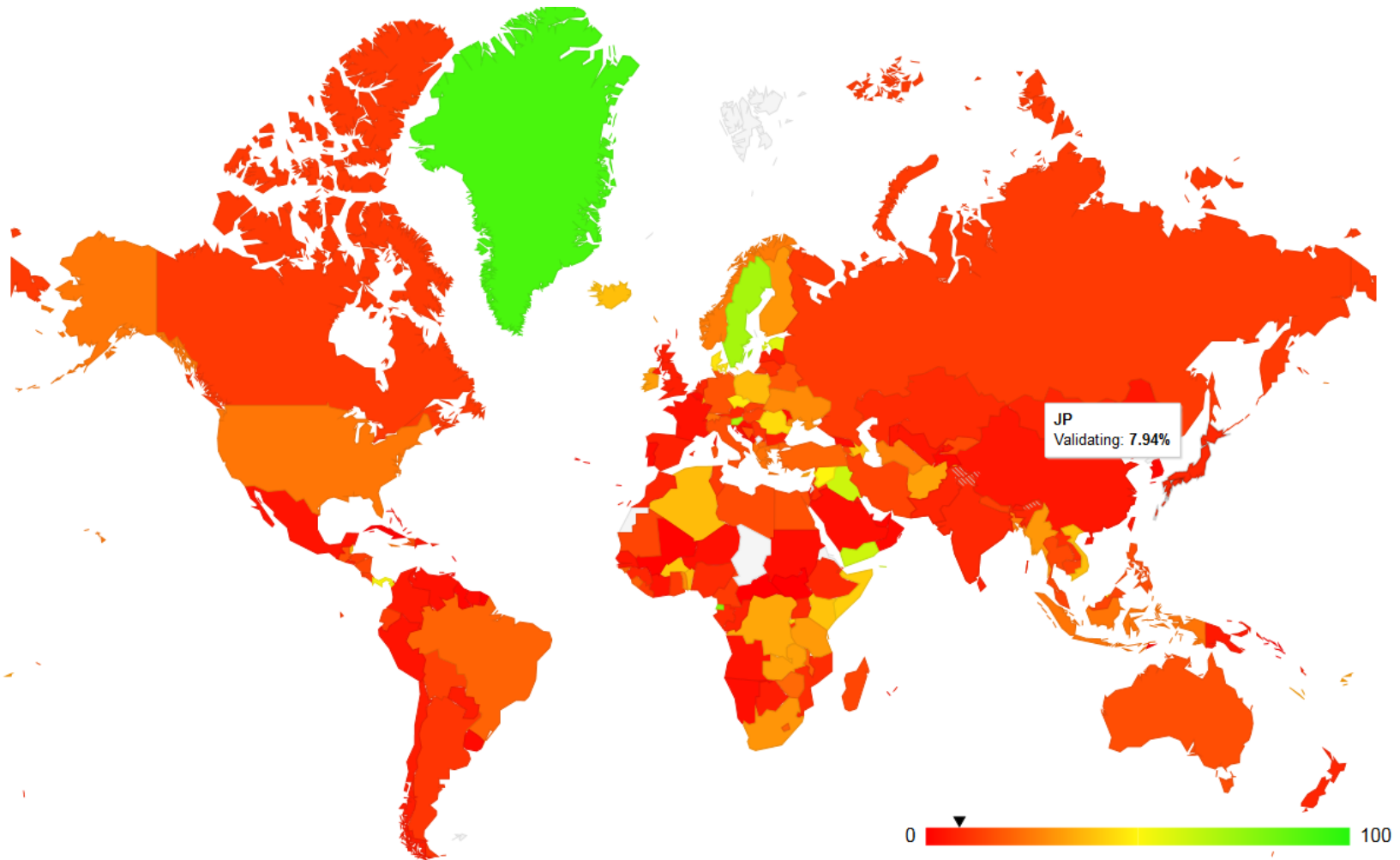
<http://gronggrong.rand.apnic.net/cgi-bin/ccpage?c=XA&x=1&g=0&r=1&w=1&g=1>

by Geoff Huston (APNIC)

全世界のユーザの約12%+約12%(GooglePublicDNS)=約24%が
Validation利用可能な環境になっている。

講演後訂正

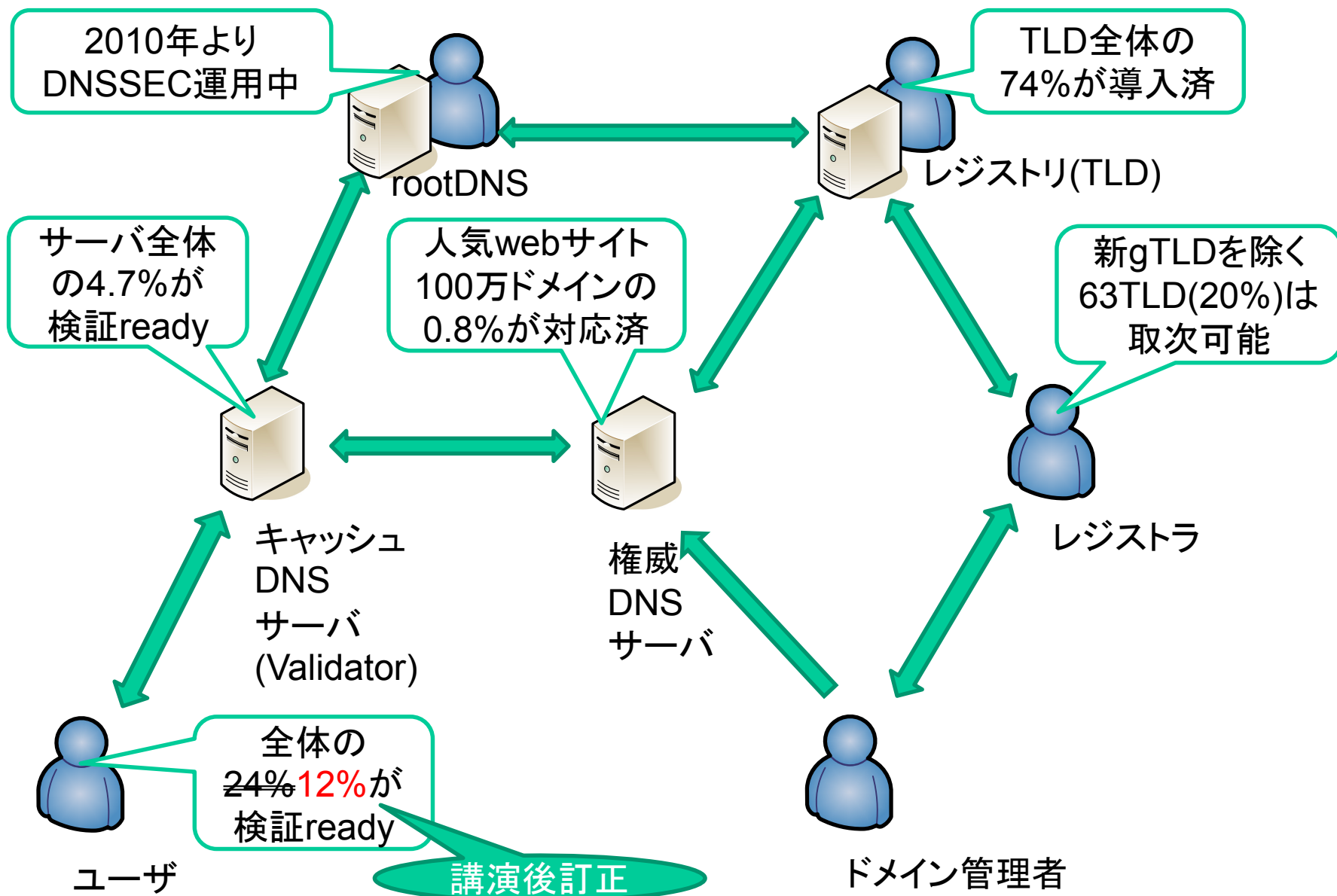
クライアント側のDNSSEC対応状況



<http://gronggrong.rand.apnic.net/cgi-bin/worldmap>

by Geoff Huston (APNIC)

DNSSEC対応状況まとめ



- Agenda

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

- **RFC 7144 Automating DNSSEC Delegation Trust Maintenance. (Informational)**
 - 親子ゾーン間のDSレコードのアップロードと署名・更新処理は、現在のDNSSECの運用における課題の一つ。
(レジストラ、レジストリとも自動化出来ていない)
 - CDS(ChildDS)、CDNSKEY(ChildDNSKEY)というレコードを新たに定義。
 - bind9.10.1/9.9.6/9.9.8でTYPE定義は実装。NSDは4.1.1でTYPE定義を実装予定。
 - PowerDNS, knotDNS, unbound は、まだ対応情報なし。
 - 新規CDSレコードが公開されたことを親ゾーンのソフトが受信すると、CDSレコードをDSレコードとして自動的に更新する仕組み。

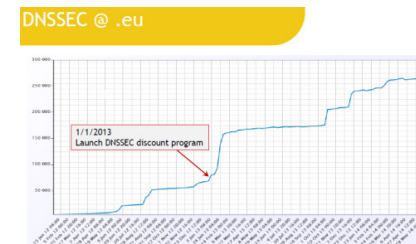
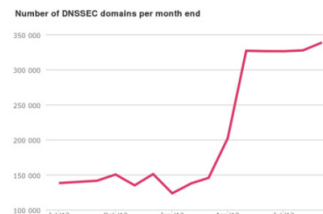
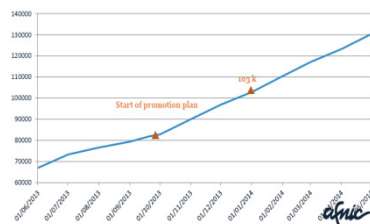
※2014年10月現在、このメカニズムを実現しているソフトウェアはまだない。

- Agenda

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

● ICANN50 DNSSEC WorkShopの発表

- 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 (※去年のInternetWeek2013で報告したTopics)
→このキャンペーンの結果が6/25(水)のICANN50でAfnicから報告された。
<http://london50.icann.org/en/schedule/wed-dnssec/presentation-dnssec-afnic-25jun14-en.pdf>
2か月間、DNSSEC対応の新規/更新ドメインに対して10%のディスカウントキャンペーンプロモーション期間だけで1.25倍登録増加。
→2013年全体でDSレコード登録数1.5倍、1ドメイン以上署名した対応レジストラ数倍増、10ドメイン以上署名しているレジストラは1.8倍に。
更に来年はレジストラを対象とした20%ディスカウント期間を実施する計画を公表。
- .frだけではなく、.se、.eu、でそれぞれレジストラ向けキャンペーンでDNSSEC対応ドメイン数が急増したことがICANN50で報告された。

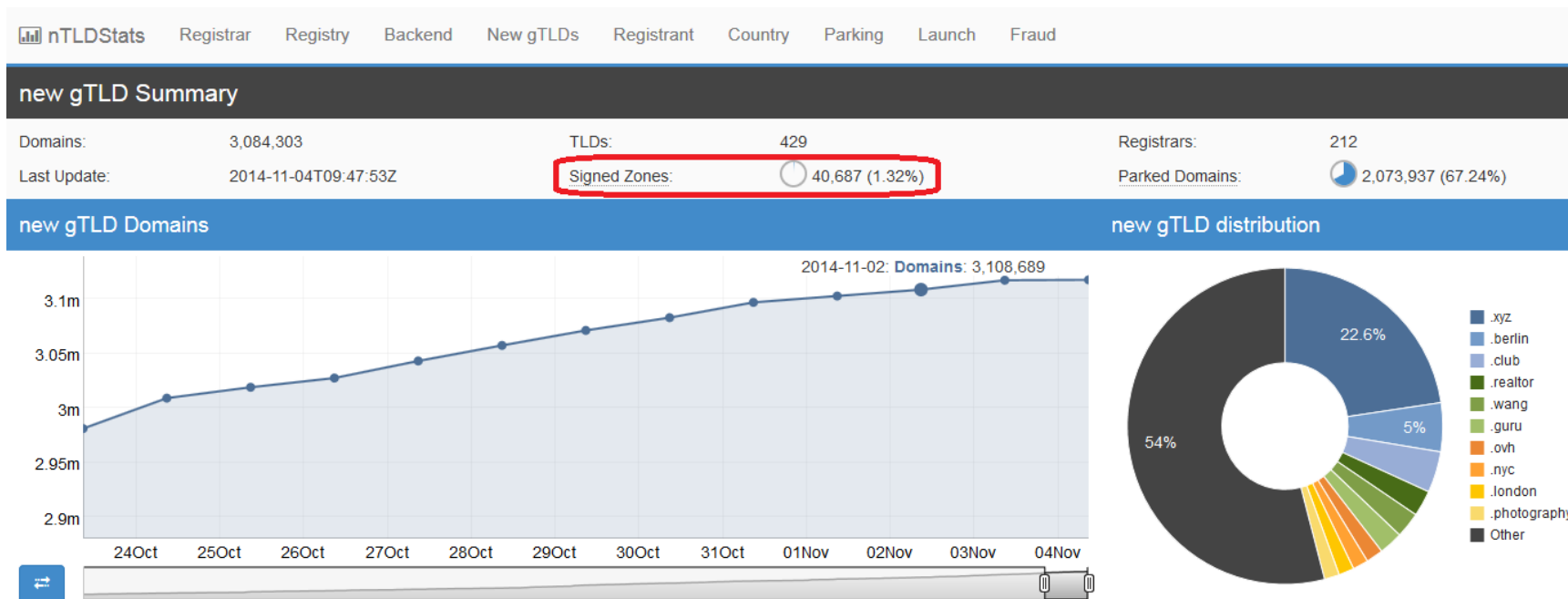


● Windows2012サーバでのDNSSEC導入資料の公開

- nslookupではDNSSEC未対応だが、Windows8 & 2012 ではResolve-DnsNameコマンドでDNSSEC対応実装。
- トラストアンカーの自動更新機能(RFC5011)も実装済

新gTLDドメインのDNSSEC対応

- 新gTLD登録ドメイン全体の1.32%のドメインがDNSSEC対応済
 - 新gTLDレジストリはDNSSEC必須のため、最初からDSレコードのやり取りを前提にシステム構築している?



- <http://ntldstats.com/>

- DNSSECの普及とDANE

(DNS-Based Authentication of Named Entities)

- tsla.infoでのテスト結果の蓄積データによると、2014/11/04 現在、334ドメインでDANE/TLSA対応済みになっている。<https://tsla.info/>

TLD別	TLSA対応数
.de	133
.net	49
.org	33
.com	31
.eu	14

- 2014/05/12 First ISP implements DANE TLSA support for SMTP (posteo.deのMX `_25._tcp.mx02.posteo.de`)
<http://www.ietf.org/mail-archive/web/dane/current/msg06696.html>
- mail.ietf.orgのSMTPもTLSAレコードが適用され(`_25._tcp.mail.ietf.org`) DANE運用開始。

- 各DNSSEC関係者の対応は順調に進んでいる。
 - 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まだ増加する見込み
 - 各レジストラでのDS取次サービスでも対応TLDが増加。
 - TLDによってはキャンペーンでドメイン登録数が急増しているTLDもある。
 - ただし、真の普及である権威DNSサーバ側、キャッシュDNSサーバ側の導入は、まだまだこれから。
特に人気サイトの権威DNSサーバ側対応が待たれる。
- 当初から課題となっているDSの取次ぎに関して、課題解決に向けてのアイデアがRFC化されてきた。
- DANEの実運用を開始した事業者も出てきた。

- 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
- ICANN50 DNSSEC Workshop資料 (2014/6/23-25開催)
 - <http://london50.icann.org/en/schedule/wed-dnssec>
- Windows 2012 R2 Resolve-DnsName 資料
 - <http://technet.microsoft.com/en-us/library/jj590781.aspx>
- DNS SummerDays2014 DNSSEC update資料 (2014/06/27開催)
 - <http://dnsops.jp/event/20140627/SummerDays2014ohmoto.pdf>
- 発表者のサイト
 - www.ohmo.to
 - <http://www.ohmo.to/dnssec/maps/>
今回の資料に関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で今回の資料に関する情報ソースのつぶやきを確認できます。

ご清聴ありがとうございました。