BroadBand Tower, Inc.

DNSOPS.jp
DNS Operators Group, Japan

DNS Summer Days 2014
DNSSEC Update

株式会社ブロードバンドタワー
エキスパート
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
    - メインは社内情報システム担当。その他いろいろ。
    - 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

- 前回のSummerDays2013からこの約一年間でのDNSSEC関連のupdate情報についてまとめました。
(2013年06月～2014年06月まで)

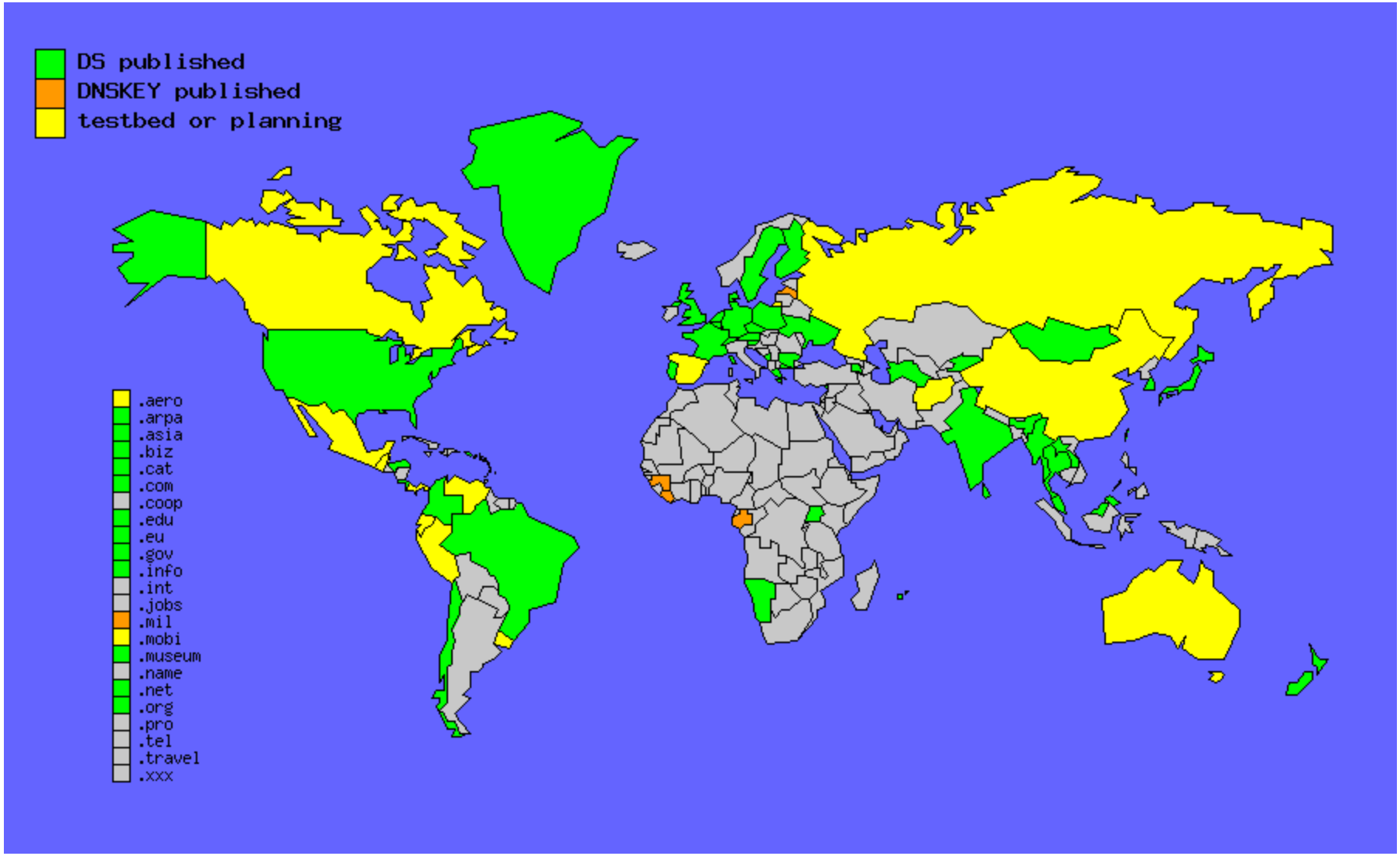
- これらの情報はccTLDのレジストリwebサイトやICANNの資料、DNSコミュニティ関連ML、JPRS社提供の情報等を確認してまとめたものです

- 半年前にInternetWeek2013で発表した内容と重複してしまうために一部Topicsは省略しますので
https://www.nic.ad.jp/ja/materials/iw/2013/proceedings/d2/d2-ohmoto.pdf
もご参照ください。

- Agenda
  - DNSSEC導入・普及状況 update
  - DNSSEC関連Topics ＆ 動向 update

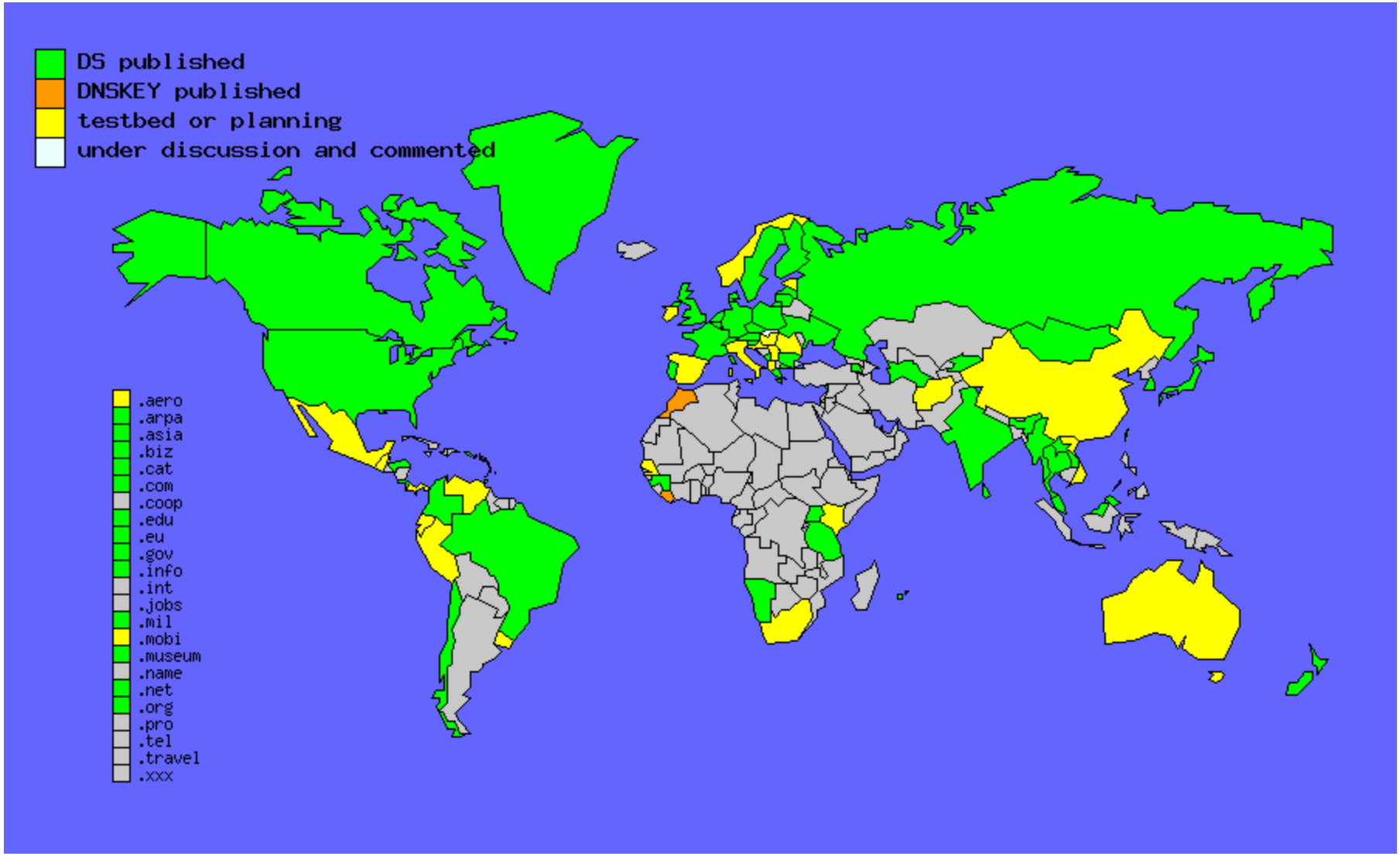
- Agenda
  - DNSSEC導入・普及状況 update
  - DNSSEC関連Topics ＆ 動向 update

DNSSEC対応状況(2012/07/16)



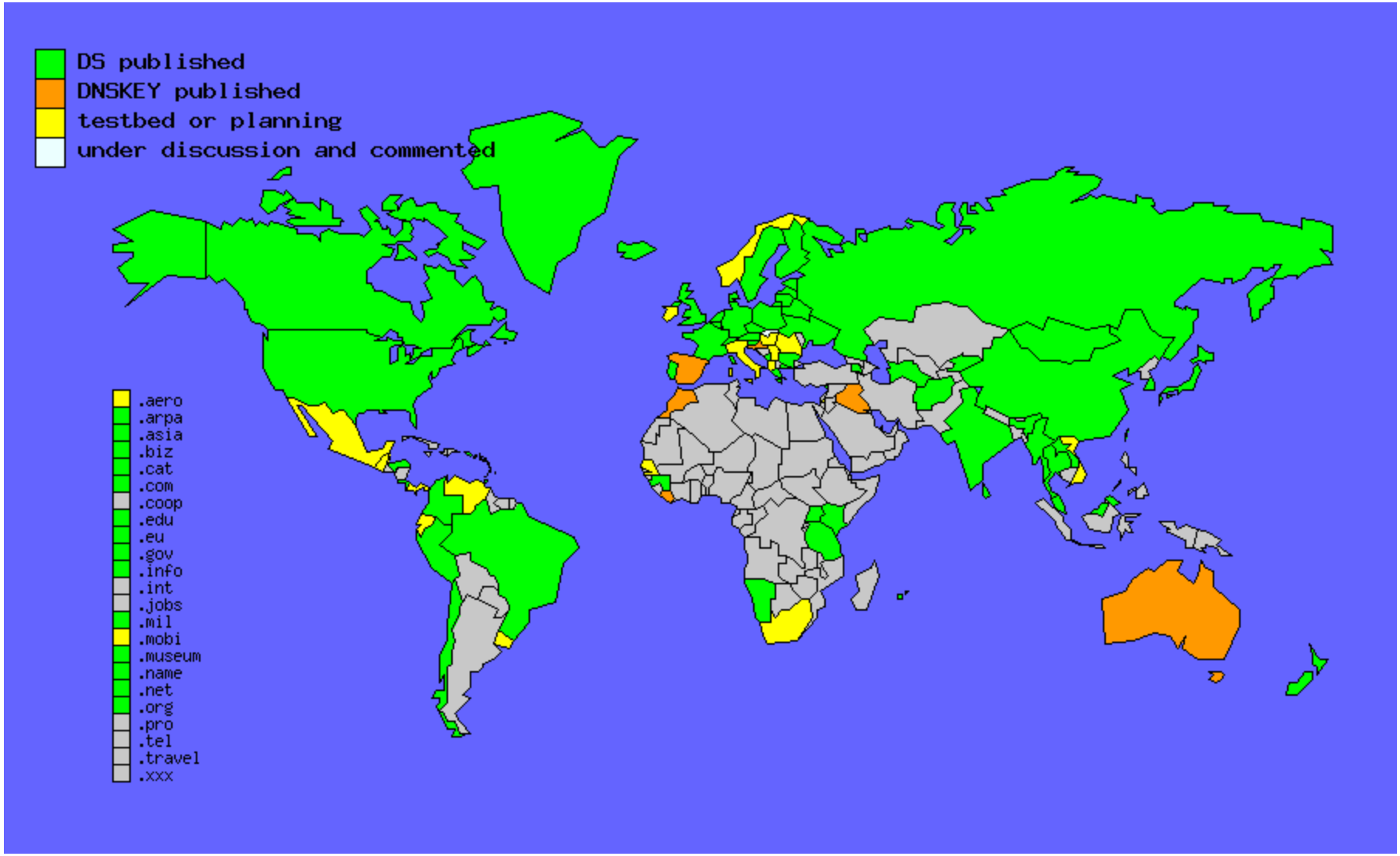
- **http://www.ohmo.to/dnssec/maps/**

DNSSEC対応状況(2013/07/26)



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

DNSSEC対応状況(2014/06/23)



- **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)

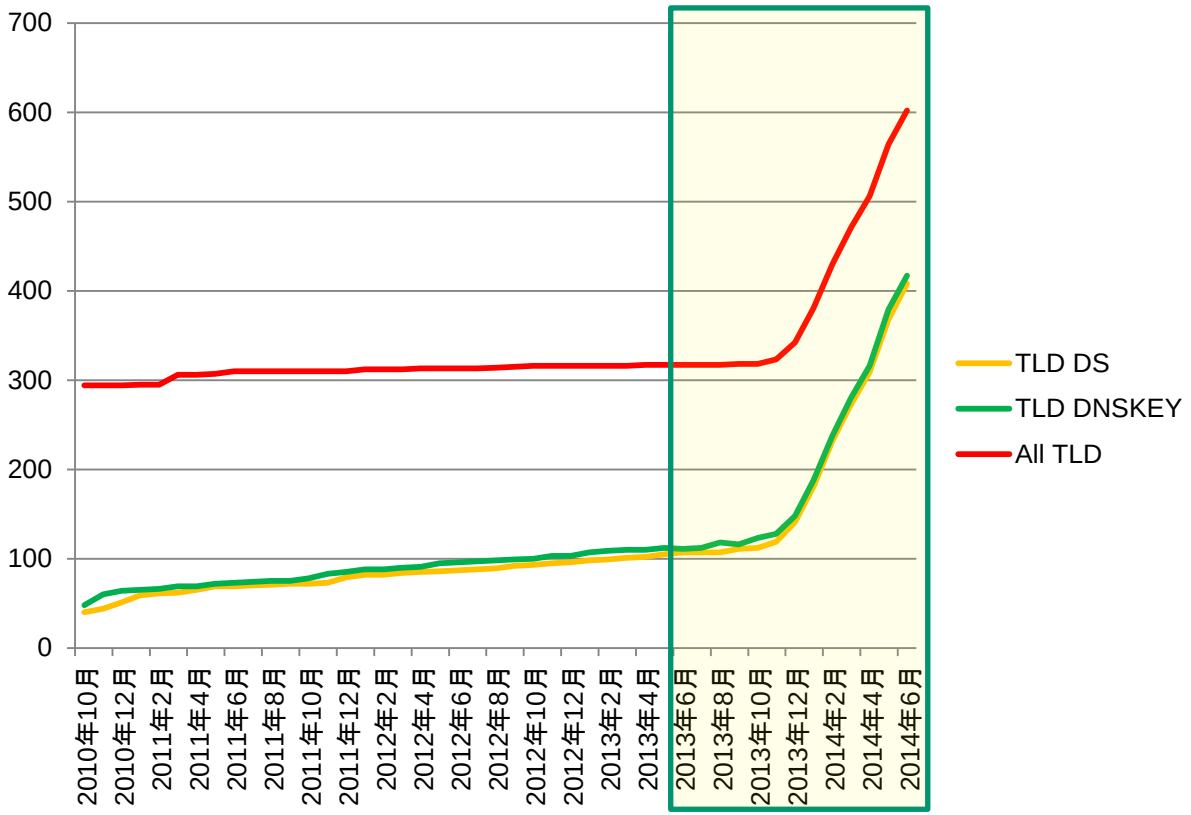
DNSSECを導入したTLD	Rootゾーン導入日
.tl（東ティモール）	2013/08/02
.gs(サウスジョージア島・サウスサンドイッチ島)	2013/08/04
.sb（ソロモン諸島）	2013/08/31
.af（アフガニスタン）	2013/09/29
.is（アイスランド）	2013/10/06
.ki（キリバス）	2013/10/16
.by（ベラルーシ）	2013/10/24
.cn（中国）	2013/11/13
.ee（エストニア）	2013/12/26
.pe（ペルー）	2014/01/20
.name	2014/01/25
.ke（ケニア）	2014/03/21
.aw（アルバ）	2014/03/29
.ad（アンドラ）	2014/05/15
.sj（スバールバル諸島・ヤンマイエン島）	2014/05/16

DNSKEYを公開したTLD	DNSKEY公開日
.iq（イラク）	2013/8/27
.id（インドネシア）	2013/12/9～ 2014/3/5
.hr（クロアチア）	2014/4/22
.au（オーストラリア）	2014/4/24
.es（スペイン）	2014/4/24

1年でRootにDSを申請したTLDは15、DNSKEYを公開したTLDは上記15TLDに加え5TLD。
(ただしidは公開終了している。)

.auは本年8月に導入予定

TLD導入推移状況



- 2013年5月 TLD全体の33%(105/317TLD)が導入済み。
- 2014年10月からnew-gTLDのrootへの導入が開始
- 2014年6月1日現在 68%(408/602TLD)が導入済みに。←new

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

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月の時点でレジストラ側では40TLDのDNSSEC対応。
2014年5月に久々に更新され、レジストラ側では63TLDがDNSSEC対応となった。

DNSSEC 普及度調査

- 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
    - 2014/6/13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。

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年5月19日	2014年6月13日
NoError	959,252	978,834
NXDomain	18,113	15,964
ServFail	1,361	1,743
その他・不明	18,602	3,459
合計	1,000,000	1,000,000

NoErrorステータス中のDNSSECステータス内訳

	2013年5月19日	2014年6月13日
NoError	959,252	978,834
署名済みドメイン数	7,636 (0.80%)	9,766(0.997%)
Secure	5,827 (0.61%)	7,868 (0.80%)
Insecure+bogus	1,809 (0.19%)	1,898(0.19%)
署名済みドメイン中のInsecureドメインの割合	23.7%	19.4%

Alexaの人気ランク(ドメイン&TLD)

ランク順位	ドメイン名
1	google.com
2	facebook.com
3	youtube.com
4	yahoo.com
5	baidu.com
6	wikipedia.org
7	qq.com
8	taobao.com
9	live.com
10	twitter.com
11	amazon.com
12	linkedin.com
13	google.co.in
14	sina.com.cn
15	hao123.com
16	blogspot.com
17	weibo.com
18	tmall.com
19	sohu.com
20	yahoo.co.jp

TLD	Alexaリスト出現数
com	524927
net	50855
ru	39121
org	38276
de	34041
jp	19326
uk	19148
br	17137
pl	13604
fr	13421
it	12555
in	12204
info	10464
cn	9209
au	8168
nl	8061
es	7693
ir	7327
eu	5010
ca	4842

AlexaベースのTLDごとの普及状況

- Alexa100万件レコードのTLDごと解析。
- 昨年よりも署名率、Secure率共に増加傾向。
  - be、de、eduに関してはSecure割合が減少
    (署名付きドメイン数、Secure数も増加しているがそれ以上にInsecure数が増えている)

TLD	Alexaリスト出現数(A)	署名付きドメイン数(B)	Secure数(C)	署名率(B÷A)	去年の署名率	各TLD中のserure率(C÷A)	去年の各TLD中のserure率	署名付きドメイン中のSecure割合(C÷B)	去年の署名付きドメイン中のSecure割合
com	524927	2203	1573	0.42%	0.33%	0.30%	0.20%	71.40%	59.95%
nl	8061	1719	1620	21.32%	17.03%	20.10%	16.50%	94.24%	96.90%
cz	4631	1506	1441	32.52%	31.28%	31.12%	29.75%	95.68%	95.10%
br	17137	962	951	5.61%	3.55%	5.55%	3.52%	98.86%	99.36%
se	3460	923	417	26.68%	23.88%	12.05%	8.91%	45.18%	37.32%
fr	13421	372	351	2.77%	1.10%	2.62%	1.01%	94.35%	91.92%
gov	858	355	349	41.38%	39.85%	40.68%	37.70%	98.31%	94.62%
net	50855	260	188	0.51%	0.38%	0.37%	0.25%	72.31%	66.51%
org	38276	259	170	0.68%	0.42%	0.44%	0.26%	65.64%	63.03%
eu	5010	167	139	3.33%	2.71%	2.77%	2.10%	83.23%	77.27%
pl	13604	125	117	0.92%	-	0.86%	-	93.60%	-
be	2984	90	70	3.02%	2.50%	2.35%	2.12%	77.78%	85.00%
de	34041	87	69	0.26%	0.22%	0.20%	0.18%	79.31%	82.00%
edu	2342	73	58	3.12%	1.99%	2.48%	1.74%	79.45%	87.50%
nu	359	62	9	17.27%	11.63%	2.51%	0.00%	14.52%	0.00%

DNSSEC対応済みドメインの状況

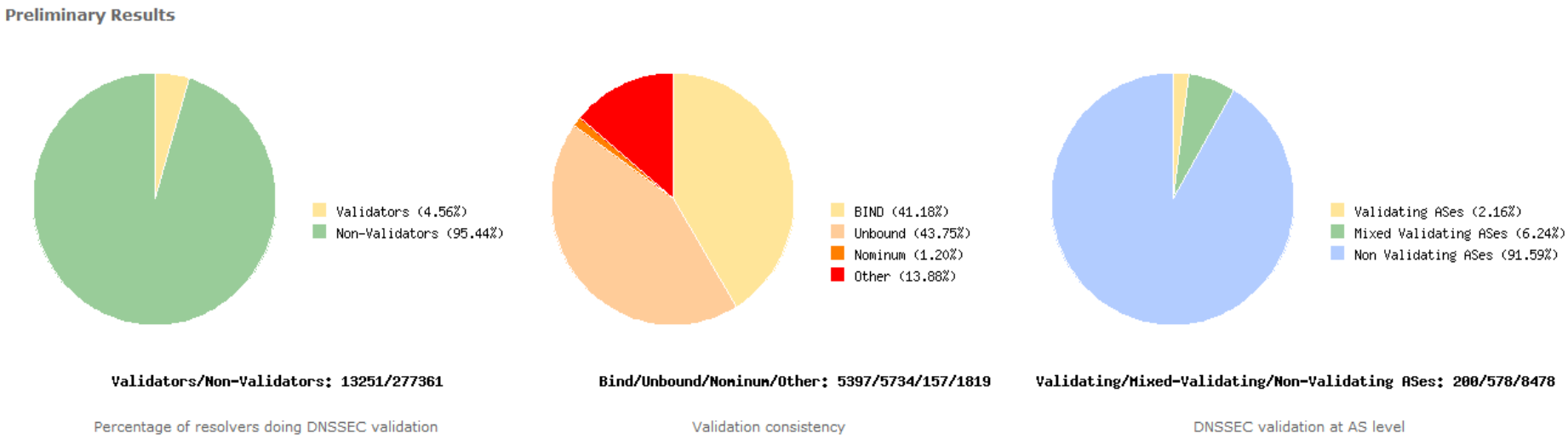
- 最もランクの高いドメイン名は去年に引き続きpaypal.com
- Alexaランク上位の署名付ドメイン名の中には有名サービスは多く含まれていない。
- DNSSECの権威DNSサーバ側の対応状況はあまり進んでいないように思われる。

Alexaランク	ドメイン名
43	paypal.com
141	mozilla.org
284	comcast.net
324	nih.gov
649	ca.gov
865	comcast.com
978	irs.gov
1103	weather.gov
1150	state.gov
1170	noaa.gov

Alexaランク	ドメイン名
1227	usaa.com
1342	nasa.gov
1388	stanford.edu
2027	yandex.com
2109	walmart.com.br
2110	psychologytoday.com
2135	ed.gov
2217	cdc.gov
2266	berkeley.edu
2391	vmware.com

validator(検証)側の普及状況

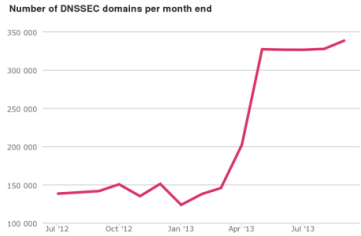
- Verisignlabsの調査データ
- http://validator-search.verisignlabs.com/
  - ブラウジングでPrefetchされたデータを元にvalidatorの普及率を調査
  - 公開された2012年9月時点では3.66%



  - 2014年6月現在4.56%とやや微増している。

- Agenda
  - DNSSEC導入・普及状況 update
  - DNSSEC関連Topics ＆ 動向 update

DNSSEC関連Topics(2013年後期)



- **.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

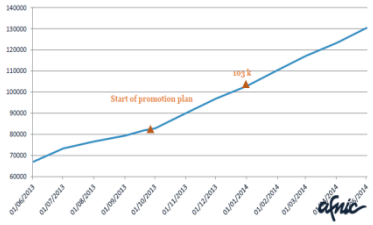
- **ICANN50 DNSSEC WorkShopの発表**
  - **Afnic(.frなどのレジストリ)では9月末よりDNSSEC適用キャンペーンを開始。**
    http://www.afnic.fr/en/about-afnic/news/operations-news/7355/showOperational/dnssec-promotional-campaign-check-it-out-1.html
  - Financial Incentive あり

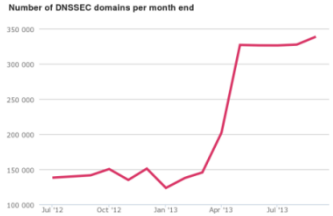
    →このキャンペーンの結果が6/25(水)のICANN50でAfnicから報告が出ました！

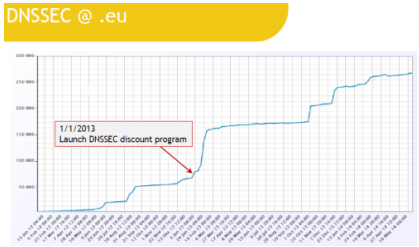
    http://london50.icann.org/en/schedule/wed-dnssec/presentation-dnssec-afnic-25jun14-en.pdf

    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
    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。

DNSSEC関連Topics(技術寄り)

- 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

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TLDレベルでは導入率が倍増した。(分母もだけど。)
  - 各レジストラでのDS取次サービスでも対応TLDが増加してきている。
  - TLDによっては対応レジストラおよびドメイン登録数が急増しているTLDも。
    - .frや.se、.euのようなレジストリの施策による急増。
- ただし、真の普及は権威DNSサーバ側、validator側でもまだまだこれから。google public DNS(8.8.8.8)でvalidationが有効になっている中、人気サイトの権威DNSサーバ側対応が待たれる。
- 一方でDNSSECのパケットがアタックの標的になる可能性が報告されており、今後も動向の注視が必要。
- 新gTLDや.govでもキーロールオーバーfail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
- 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
- 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
- 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。