DNSSECの普及度 (+IPv6の普及度)

藤原和典
fujiwara@jprs.co.jp
株式会社日本レジストリサービス
http://jprs.co.jp/

自己紹介

- 氏名:　　藤原和典
- 勤務先:　株式会社日本レジストリサービス (JPRS)
- 業務内容:DNS関連の研究・開発、標準化(IETF)
  - RFC 5483 6116 (2004~2011):ENUMプロトコル
  - RFC 5504 5825 6856 6857(2005~2013):メールアドレスの国際化
  - RFC 8499: DNS Terminology (←RFC7719)
  - RFC 8198: DNSSECを用いた名前解決の性能向上
  - Internet Week プログラム委員 (2016~)
- 個人ページ: http://member.wide.ad.jp/~fujiwara/
- 略歴: 1991年からWIDEプロジェクト, 1992-1996早稲田大学情報科学研究教育センター助手, 1996-2001 TDI, 2002-JPRS, 博士(工学)

Copyright © 2019 Japan Registry Services Co., Ltd.

DNSSECの普及度の考え方

1. DSが設定されているドメイン名の数/割合
   - ゾーンファイルを入手, DSがあるドメイン名を数える
   - NSEC3 Zone WalkingでDSがあるNSEC3を数える
   - dnssec-tools.org が公開している評価結果
2. DNSSEC検証するフルサービスリゾルバの数/割合
   - DNSSEC検証する際に . DNSKEY, JP DNSKEY を問い合わせ
   - JPのNegative cache TTLが900のため、DSがないJPドメイン名のDSを最大900秒ごとにJP DNSへ問い合わせる

   → Root, JPでDNSKEY, DSクエリを送るIPアドレス数を数える
3. DNSSEC検証した結果を使えるクライアント数/割合
   - APNIC Labs での評価　https://labs.apnic.net/
   - https://stats.labs.apnic.net/dnssec
   - 2.を使っているクライアント数

Copyright © 2019 Japan Registry Services Co., Ltd.

1. DSが設定されたドメイン名の観測 (1)

- TLDのゾーンファイルの入手方法
  - .com: 使用目的を書いてVerisignに申請
  - その他のgTLD: ICANN CZDS で申請
  - ccTLD: .SE などは公開

  DSの行を取り出し、owner nameをsort | uniq | wc -l

- gTLDのゾーンファイルを入手してもいいし、
  いくつかは見られるところにあるが、別の方法で評価
  → 次ページ

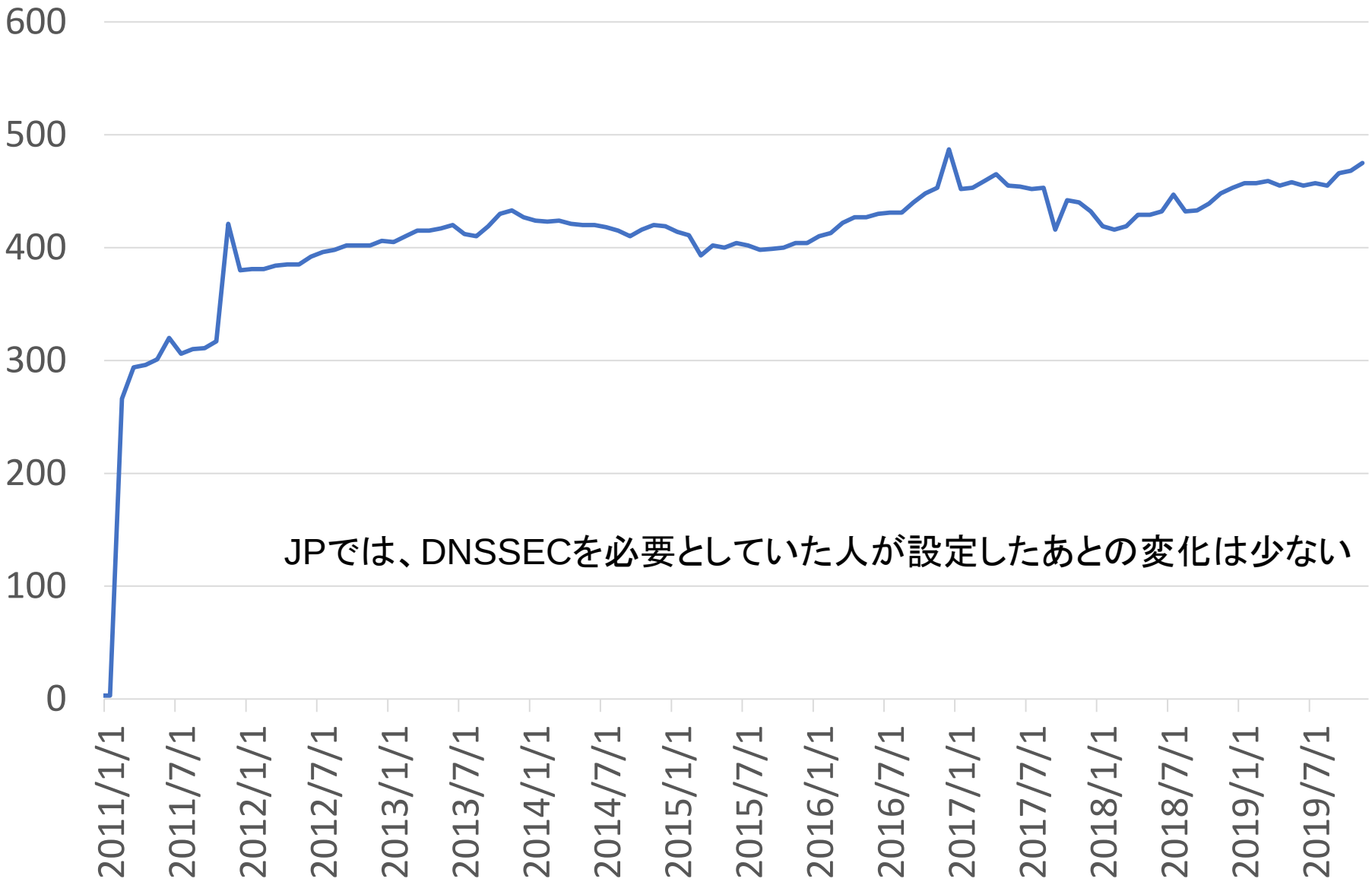
Copyright © 2019 Japan Registry Services Co., Ltd.

NSEC3 Zone walking

- 多くのTLDはNSEC3方式でDNSSEC署名、オプトアウトあり
- DSがある委任には対応するNSEC3が存在する
- そこで、“ランダムラベル.TLD” A の問い合わせを多数送ることで、多数のNSEC3を多数入手できる
- うまくすればすべてのNSEC3を入手でき、チェインにできる
- DSがあるNSEC3の数を数えればよい
- 最適化: NSEC3パラメータをもとにクエリ名からNSEC3を計算し、入手済のNSEC3の範囲に含まれたら問い合わせない
  - TLDの権威サーバの場合、DSの数程度のクエリを送ればNSEC3チェインを入手できる
- .com, .netなどの大規模ゾーンでは、チェインを収集し終わる前にゾーンの内容が変化するため、どこかであきらめる
- プログラム例: https://dnscurve.org/nsec3walker.html

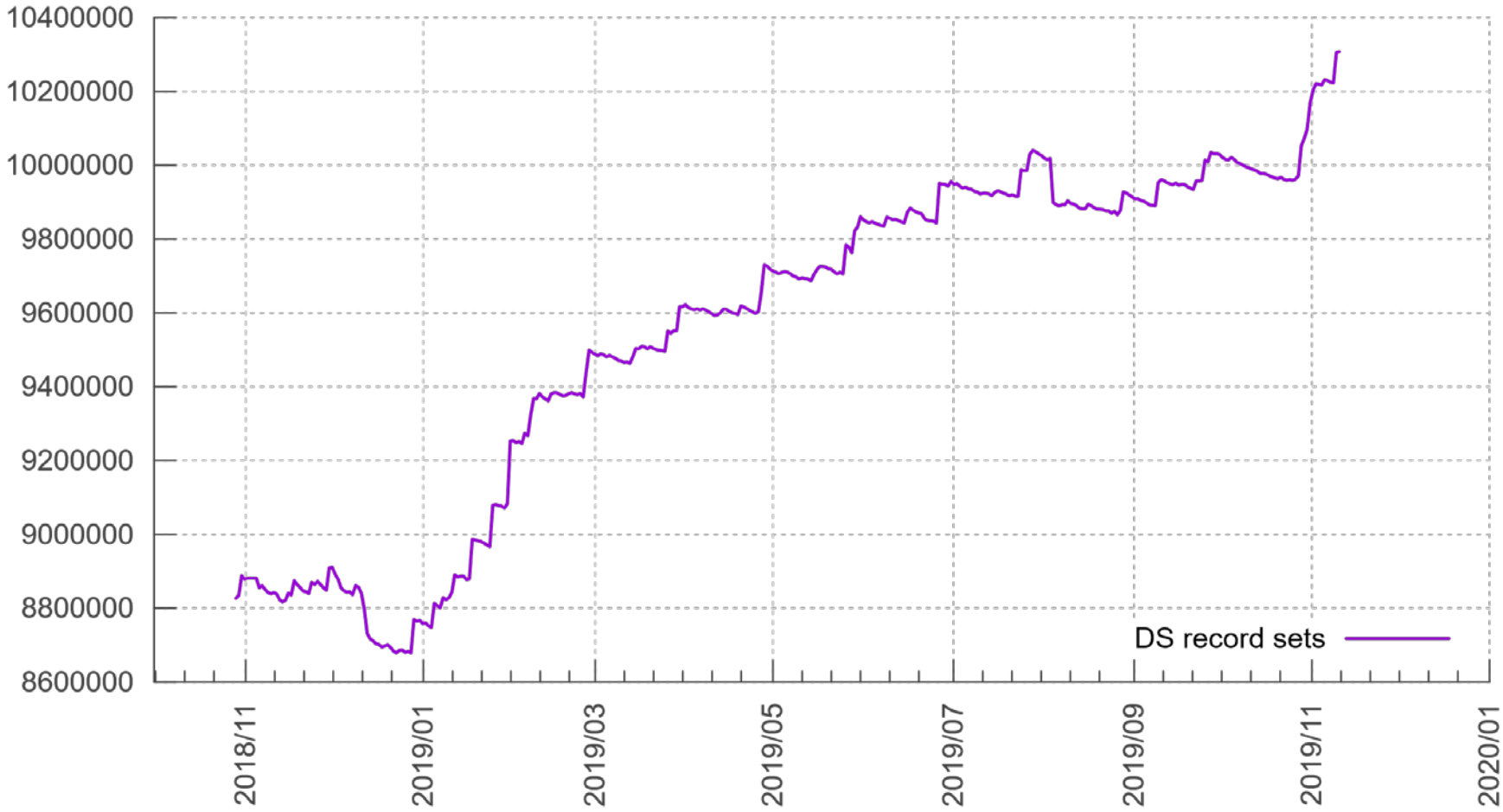
Copyright © 2019 Japan Registry Services Co., Ltd.

JPでのDSあり委任数の変化



Copyright © 2019 Japan Registry Services Co., Ltd.

DSあり委任数 (stats.dnssec-tools.org)



http://stats.dnssec-tools.org/　より引用
1000万を超えている
世界のドメイン名数は3.3億といわれているため、3%のドメイン名がDSあり
世界ではDNSSECが普及しつつある

TLDでのDSあり委任数 (NSEC3 zone walk)

- jpは非常に少なく500未満、co.jpなどへのTXTのほうが多い
- com net org info は多いが、登録ドメイン名数の1%未満
- nl, seが非常に多く、登録ドメイン名数の半分以上

TLD	日付	NSEC3数	途中停止	NSEC3未解決	DSあり委任	特記事項
jp	2019/10/15	3,744	No	0	473	RRSIG TXT 例co.jp
pro	2019/10/22	7,112	No	0	2,729	
name	2019/10/22	18,550	No	0	1,005	
info	2019/10/22	152,096	Yes	3	47,499	RRSIG A多数
net	2019/10/18	162,777	Yes	5	162,476	
com	2019/10/18	1,338,434	Yes	886	1,338,433	さらに886以上DSあり
org	2019/10/10	160,979	Yes	27	117,556	RRSIG A多数
edu	2019/10/17	163	No	0	162	
gov	2019/10/15	5,993	No	0	1,181	オプトアウトしていない
moe	2019/11/6	426	No	0	425	
se	2019/11/6		No		738,595	NSEC zone walk
no	2019/11/6	448,388	Yes	125	448,363	さらに125以上DSあり
nl	2019/10/10	2,779,850	Yes	376,171	2,779,845	さらに37万以上DSあり
de	2019/10/18	624,356	Yes	266	217,991	RRSIG A多数

Copyright © 2019 Japan Registry Services Co., Ltd.

TLDごとのDSあり委任数 (dnssec-tools.org)

TLD	DSあり委任数
nl	3,196,189
com	1,364,376
se	738,310
cz	676,335
br	579,881
eu	496,696
pl	477,790
fr	400,106
no	397,439
be	302,786
de	219,046
dk	215,672
net	163,502
hu	123,597
org	118,988
nu	103,983
ch	92,981
info	48,127
app	40,850
uk	38,561

- http://stats.dnssec-tools.org/ 公開の表よりTLDごとのDSあり委任数を引用
- NSEC3 zone walkの答え合わせ (自分でやる必要はなかった)
- nl se cz br eu pl fr no be de dk hu ch ukといったヨーロッパのccTLDでDNSSECが普及している
- com net org info は登録ドメイン名数が多いのでDSも多い

Copyright © 2019 Japan Registry Services Co., Ltd.

DNSSEC検証対応フルリゾルバの推定

- DNSSEC検証に対応しているフルリゾルバは、EDNS0に対応し、DNSSEC OKビットをセットして問い合わせる
- DNSSEC検証を行うフルリゾルバは、. (root) DNSKEY や jp DNSKEY、JP登録ドメイン名のDSを定期的に問い合わせる
- ルート、JPでのパケットキャプチャ、クエリログをもとに調査
- 大手のリゾルバサービス(Google, Quad9, Cloudflareなど)の対応は完了している

Copyright © 2019 Japan Registry Services Co., Ltd.

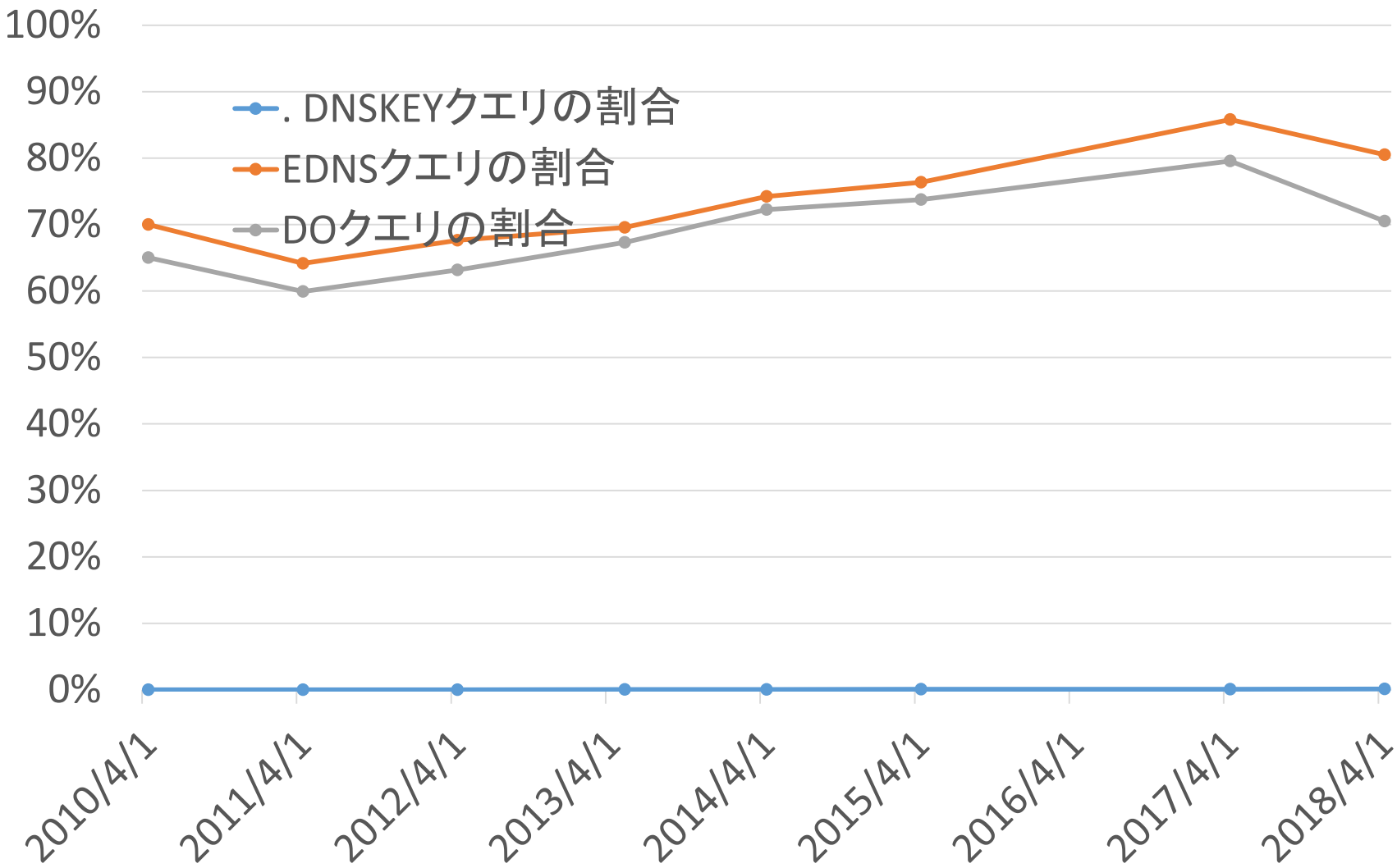
DNS-OARC's Root Datasets

- "A Day in the Life of the Internet" (DITL) is a large-scale data collection project undertaken by CAIDA and DNS-OARC every year since 2006
  - https://www.dns-oarc.net/ditl/2011/
  - 48 hours packet capture at root DNS servers

Year	Start(UTC)	End	Analyzed data from
2011	Apr 12 1200	Apr 14 1200	a c d e f h j k l m (10/13)
2012	Apr 17 1200	Apr 19 1200	a c e f h j k l m (9/13)
2013	May 28 1200	May 30 1200	a c d e f h j k l m (10/13)
2014	Apr 15 1200	Apr 17 1200	a c e f h j k m (8/13)
2015	Apr 13 1200	Apr 15 1200	a c f h j k l m (8/13)
2017	Apr 11 1200	Apr 7 1200	a c d e f h j k l m (10/13)
2018	Apr 10 1200	Apr 12 1200	a c d e f h j k l m (10/13)

Copyright © 2019 Japan Registry Services Co., Ltd.

Rootで観測したEDNS/ DNSSEC OK/ DNSKEYクエリの割合



70%ほどのクエリはDNSSEC対応したソフトウェアから送られている

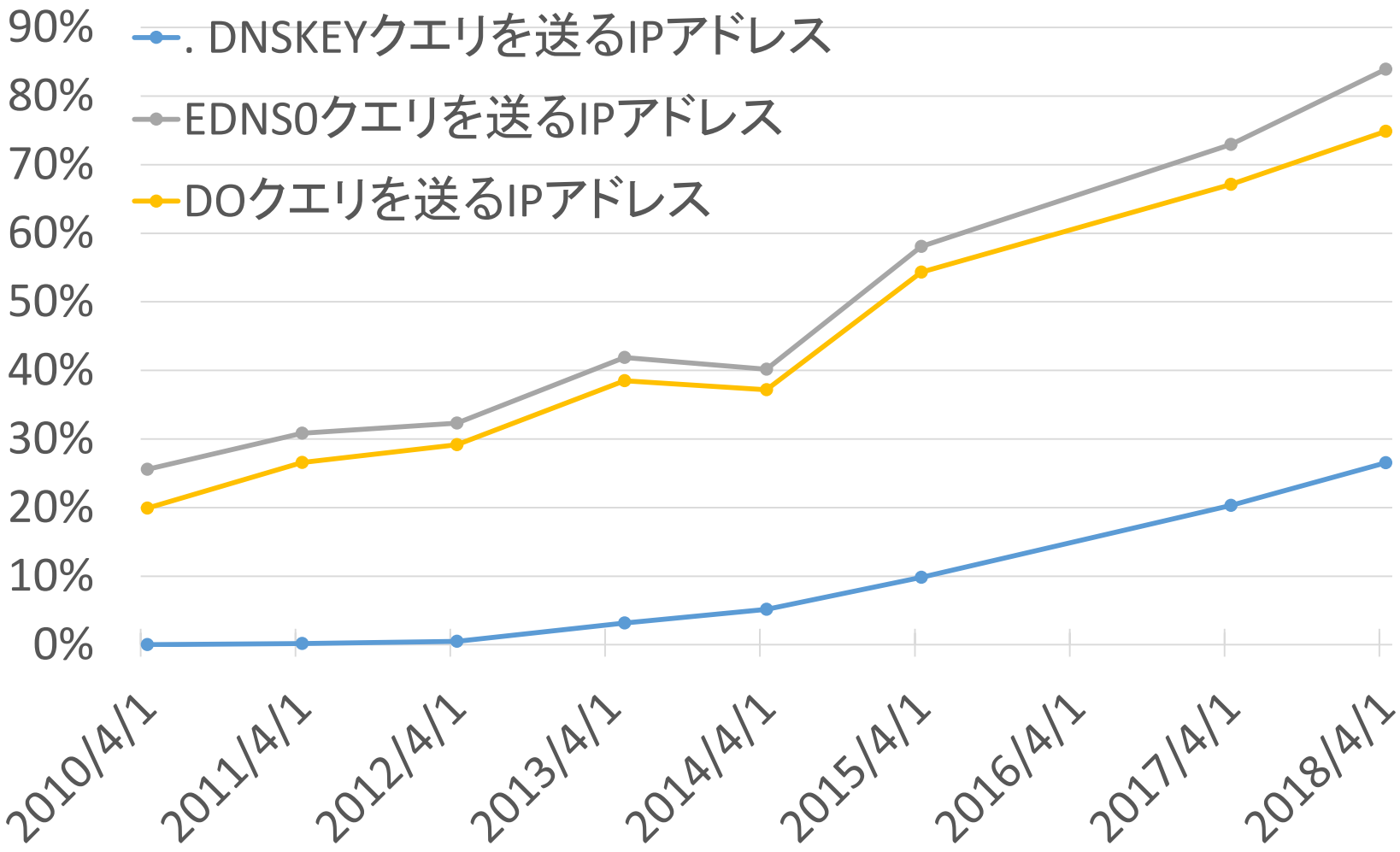
Copyright © 2019 Japan Registry Services Co., Ltd.

Rootで観測した root DNSKEYクエリの割合

root DNSKEYは制御情報のため比率が少ないが、順調に増加

Copyright © 2019 Japan Registry Services Co., Ltd.

Rootで観測したEDNS/ DNSSEC OK/ DNSKEYクエリを送るIPアドレスの割合



DNSSEC対応したソフトウェアを使用しているIPアドレスが75%以上
DNSSEC検証に対応していると考えられるIPアドレスが27%程度

Copyright © 2019 Japan Registry Services Co., Ltd.

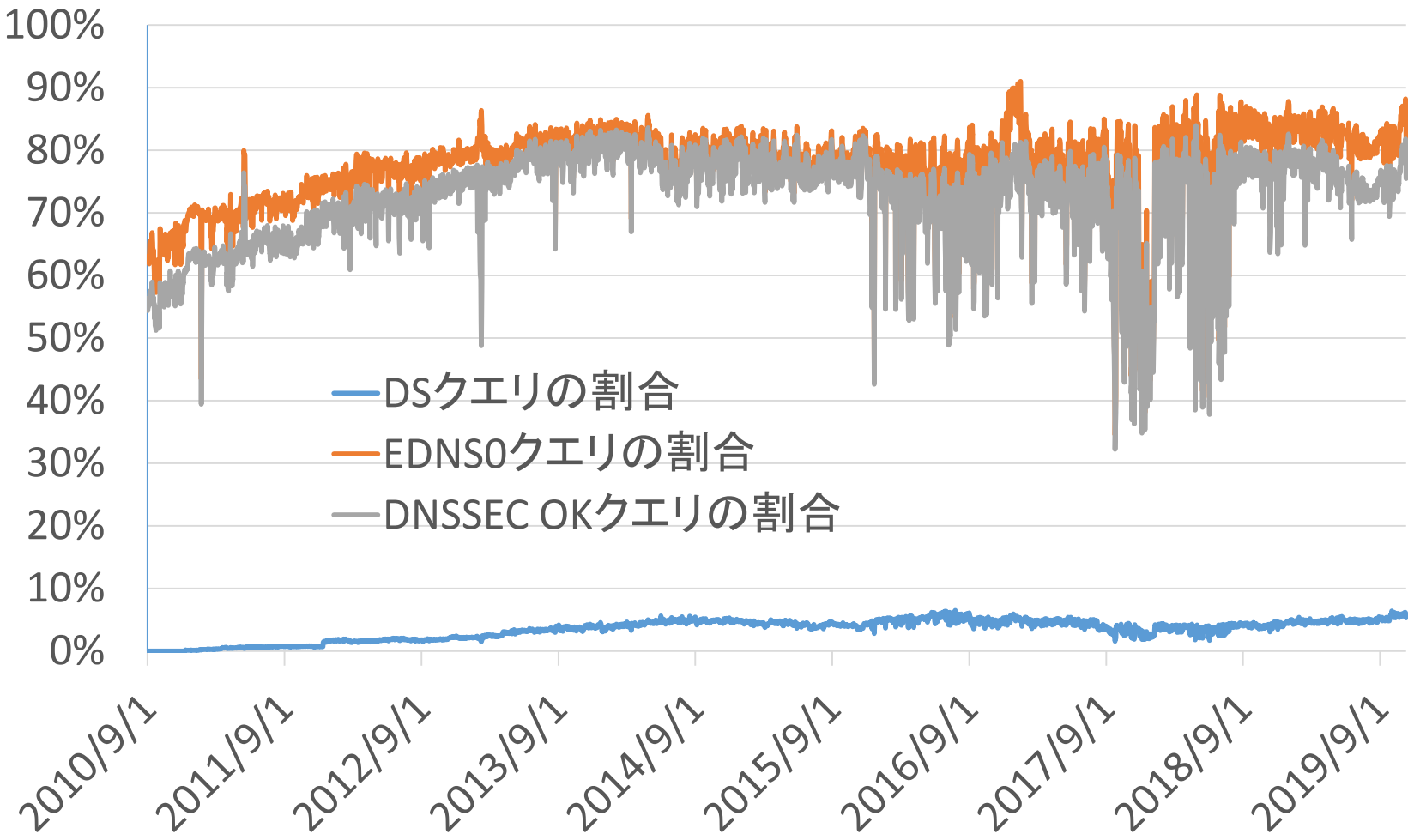
JP datasets

- 2006年4月からA.DNS.JPとG.DNS.JPのクエリログをすべて保存
  - G.DNS.JPは2008年10月に追加されたため、それ以降
- 2009年から、Root DITLデータ収集と同時期などに全JP DNSのパケットキャプチャデータを収集

- そのうちクエリログを用いて日々の JPドメイン名へのDSクエリ数を送るIPアドレス数の変化を示す
  - JPドメイン名のDSがない委任では、ネガティブキャッシュのTTL値が900秒のため、DSが存在しないという情報は900秒しかキャッシュされない
  - 委任のNSは1日キャッシュされる
    - キャッシュにあるNS RRSetをみてDNSSEC検証しようとしてもDSが存在しないという情報がない可能性あり → DSだけ問い合わせ
  - DNSSEC検証サーバはDS設定していないJPドメイン名のDSクエリを頻繁に送ることが想定される
    - 最大 通常クエリの 86400 / 900 = 96倍

Copyright © 2019 Japan Registry Services Co., Ltd.

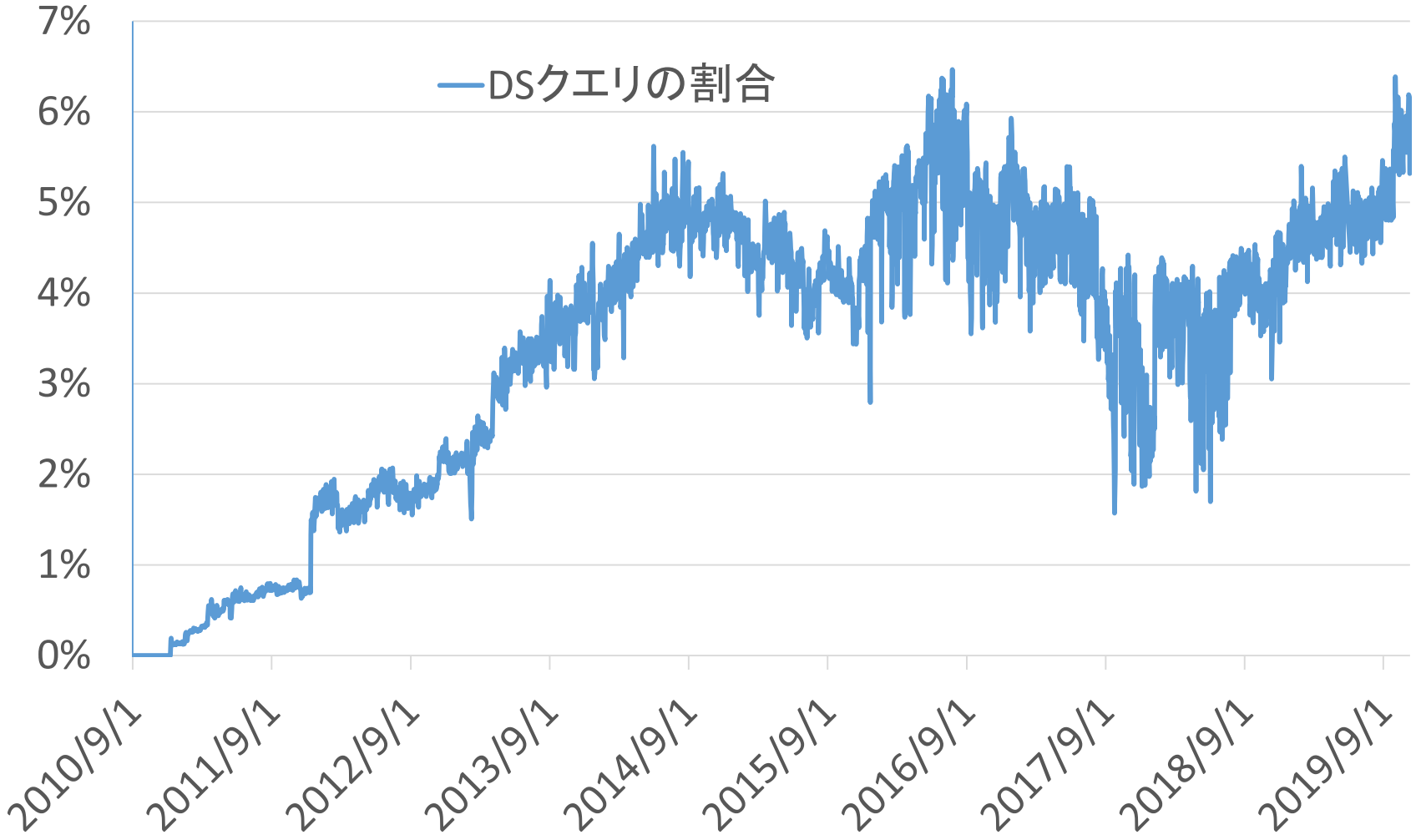
JP DNSでのEDNS0, DO, DSクエリ



- EDNS0,DNSSEC OKはソフトウェアのDNSSEC対応を示す
- 80%ほどのクエリはDNSSEC対応ソフトウェアからくる

Copyright © 2019 Japan Registry Services Co., Ltd.

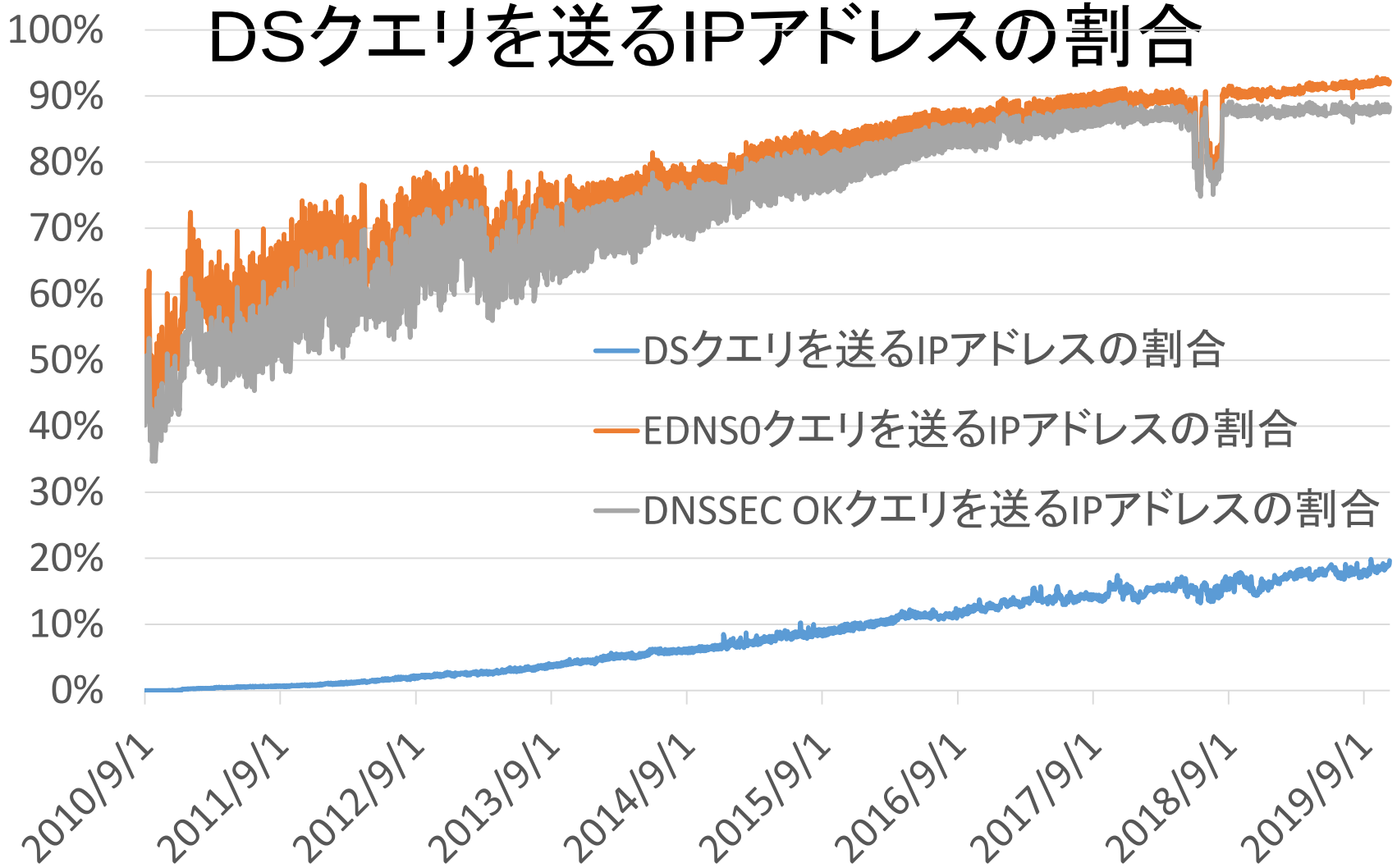
JP DNSでのJPドメイン名DSクエリ



JPドメイン名に関心を持つDNSSEC Validatorは増えていない
DNSSEC Validatorが増えて、JPでのDS登録が増えない場合、ほとんどのクエリがDSとなるみこみ（うれしい悲鳴？）

Copyright © 2019 Japan Registry Services Co., Ltd.

JP DNSでのEDNS0,DNSSEC OK, DSクエリを送るIPアドレスの割合



- 80%のIPアドレスはDNSSECに対応したソフトウェア
- 20%のIPアドレスはDNSSEC検証している可能性あり

Copyright © 2019 Japan Registry Services Co., Ltd.

クライアントからみたDNSSEC検証

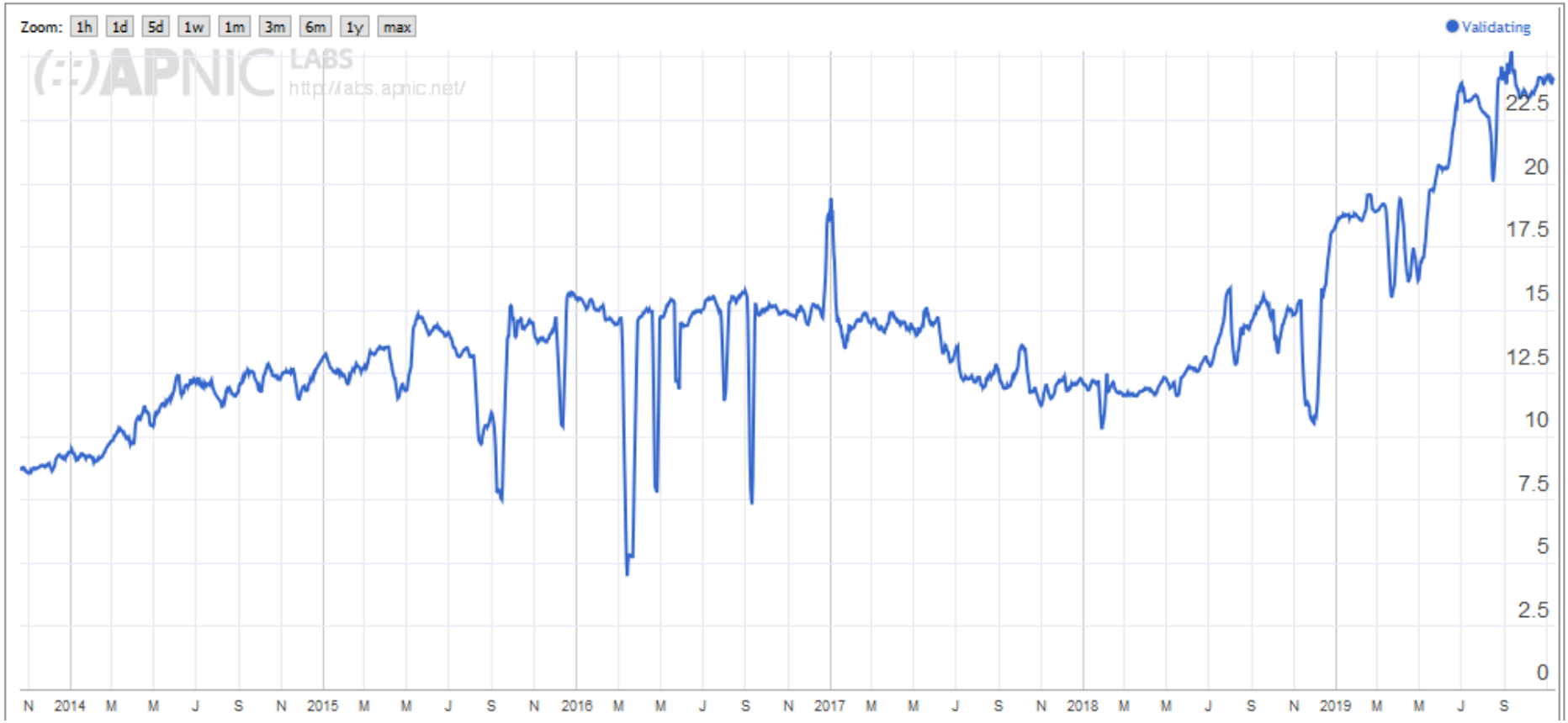
- APNIC Labs での評価　https://labs.apnic.net/
  - Google広告を使い、ブラウザでHTML5を実行させ、指定したドメイン名の名前解決を行い、結果をAPNICのサーバに収集
  - 権威サーバ側のデータと組み合わせて判定
  - 調査結果: https://stats.labs.apnic.net/dnssec

Copyright © 2019 Japan Registry Services Co., Ltd.

クライアントからみたDNSSEC検証の普及率

https://stats.labs.apnic.net/dnssec/XA?hc=XA&hx=0&hv=1&hp=1&hr=1&w=7&p=0

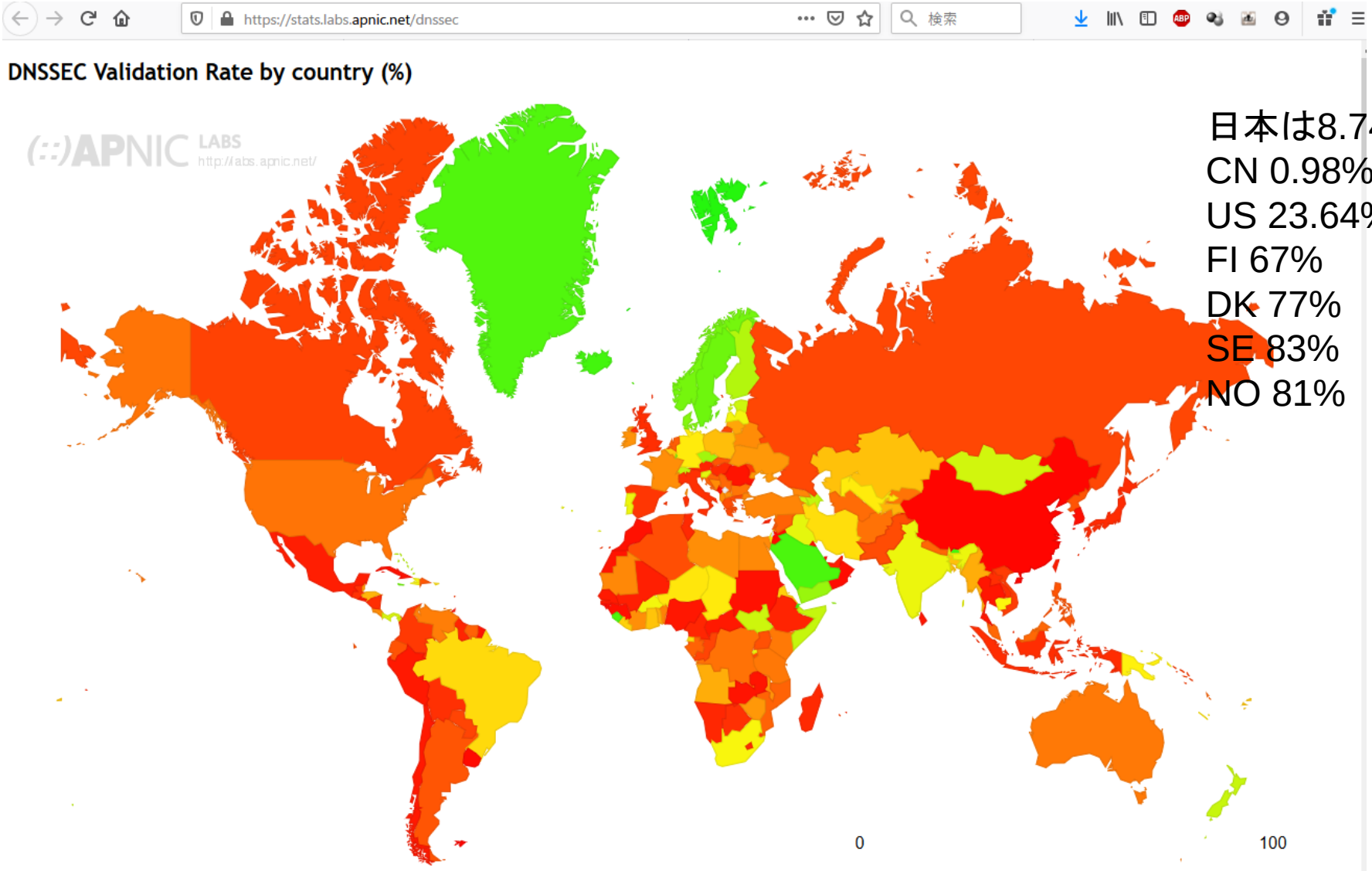
Use of DNSSEC Validation for World (XA)



- https://stats.labs.apnic.net/dnssec
- 2013年11月から2019年11月のグラフ
- 2019年11月には24%のクライアントがDNSSEC検証

クライアントからみたDNSSEC検証:国別

https://stats.labs.apnic.net/dnssec



日本は8.74%
CN 0.98%
US 23.64%
FI 67%
DK 77%
SE 83%
NO 81%

DNSSEC検証率とリゾルバの種類

CC	DNSSEC検証率	同じAS内リゾルバ	google pdns
JP	8.73%	61.71%	2.99%
CN	0.92%	56.41%	3.14%
US	25.22%	36.50%	6.74%
DE	51.24%	45.02%	10.95%
FI	68.05%	57.40%	6.49%
DK	80.03%	82.30%	6.30%
SE	82.68%	75.89%	5.33%
NO	82.09%	73.22%	7.67%
NL	19.73%	49.18%	11.00%
CZ	69.94%	69.96%	12.92%
MO	5.43%	80.86%	7.88%
IN	52.56%	19.81%	8.05%
SA	95.00%	47.86%	2.99%
AI	61.73%	25.66%	66.42%

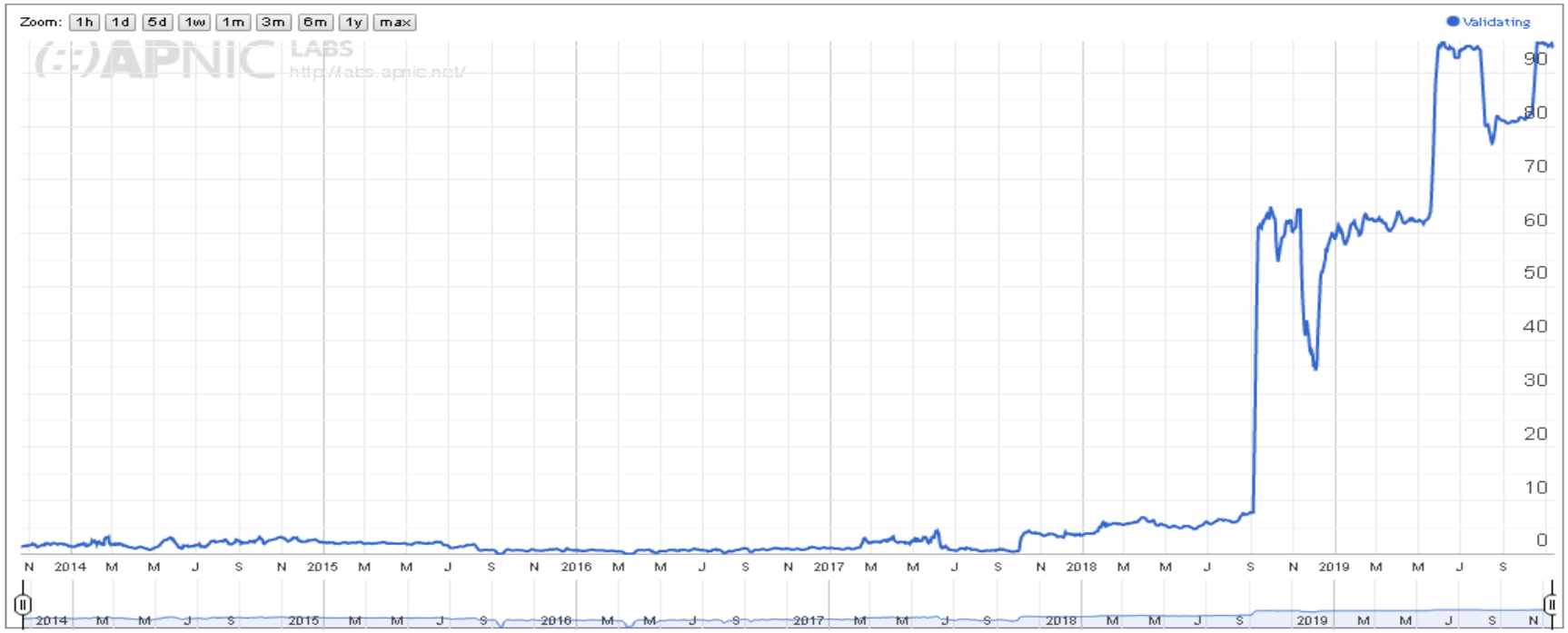
- https://stats.labs.apnic.net/rvrs/XA 各国のリゾルバの分類と、https://stats.labs.apnic.net/dnssec/ 各国のDNSSEC検証率の表をマージ
- DE FI DK SE NO CZなど、ヨーロッパ諸国でDNSSEC検証率が高く、同じAS内のリゾルバがDNSSEC対応
- SAの検証率が高く、大手のISPがDNSSEC対応 (詳細は次ページ)
- AI (Anguilla, カリブ海) など小さな国ではGoogle Public DNS利用率が高いためにDNSSEC検証率が高い
  - ISPがGoogle Public DNSを使わせている可能性あり
- JP, CN, MOは同じASのリゾルバを使う割合が高いが、DNSSEC検証率が低め

Copyright © 2019 Japan Registry Services Co., Ltd.

SAでのDNSSEC検証率とAS

https://stats.labs.apnic.net/dnssec/SA?hc=SA&hx=0&hv=1&hp=0&hr=0&w=7

Use of DNSSEC Validation for Saudi Arabia (SA)



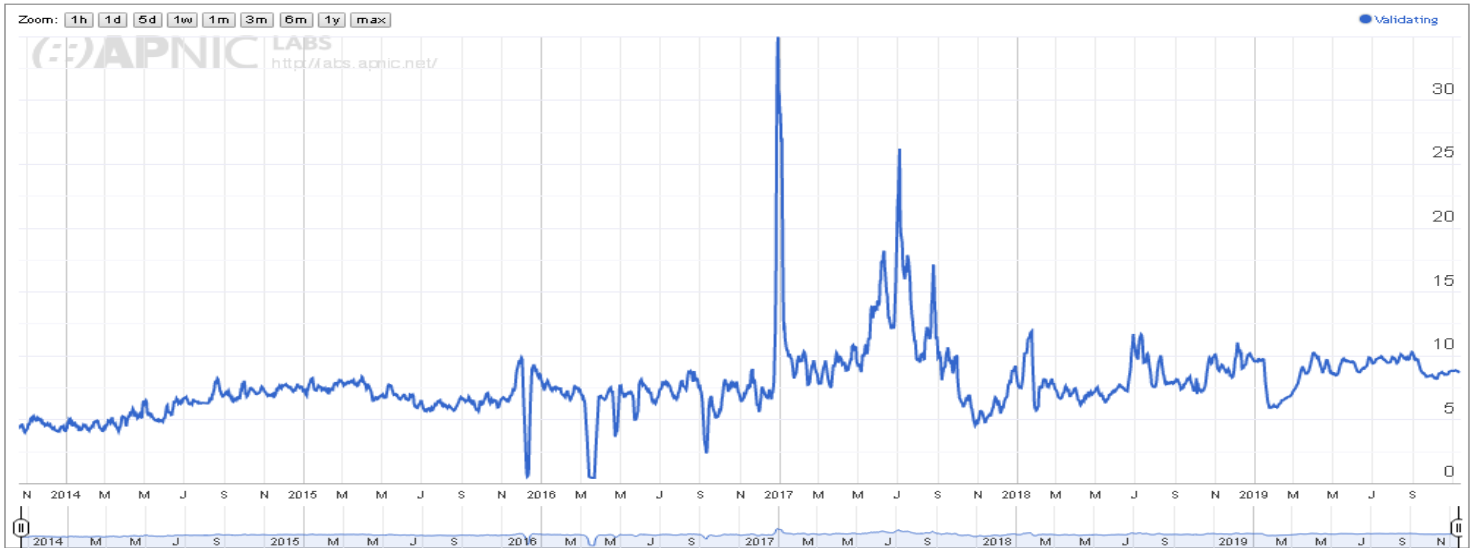
ASN	AS Name	DNSSEC Validates	Samples
AS39891	ALJAWWALSTC-AS	97.65%	102,313
AS25019	SAUDINETSTC-AS	93.78%	88,919
AS35819	MOBILY-AS Etihad Etisalat Company (Mobily)	95.59%	67,821
AS43766	MTC-KSA-AS	97.80%	40,536
AS35753	ITC ITC AS number	88.47%	4,866
AS48695	ATHEEB-AS	96.05%	2,050

2018年9月から60%以上に　　大規模なISPがDNSSEC検証対応

JPでのDNSSEC検証率とAS

https://stats.labs.apnic.net/dnssec/JP?hc=JP&hx=0&hv=1&hp=0&hr=0&w=7

Use of DNSSEC Validation for Japan (JP)



ASN	AS Name	DNSSEC Validates
AS4686	BEKKOAME BEKKOAME INTERNET INC.	99.20%
AS27471	SYMN - Symantec Corporation	98.59%
AS10001	MICSNET Mics Network Corporation	98.30%
AS17956	WASEDA WASEDA University	98.16%
AS131933	TTV-NET TAMA Television Co., Ltd	98.11%
AS59126	NCT NCT CO.,LTD.	97.38%
AS18283	CCV Fureai Channel Inc.	97.29%
AS131937	JCV Joetsu Cable Vision	97.21%
AS46562	TOTAL-SERVER-SOLUTIONS - Total Server Solutions L.L.C.	97.21%
AS9622	KCT Kurashiki Cable TV	96.86%
AS17958	KCV Kasaoka Cable Vision Co,LTD.	96.67%

DNSSEC検証率10%程度　　検証率が高いASあり

DNSSEC普及についてのまとめ

- DNSSECでのドメイン名運用
  - ほとんどのgTLD, 多くのccTLDがDNSSECに対応している
  - ドメイン名登録者は2011年からDNSSECを使える(jp, 多くのgTLD)
  - JPドメイン名でのDS設定は461程度と少ない
- DNSSEC検証について
  - ルートやJPでみて、20%以上のIPアドレスはDNSSEC Validatorだと推定される
  - 北欧、ドイツ、チェコ、サウジアラビアなどではISPが対応しているようにみえる
  - USではComcastが対応
  - 特にサウジアラビアでは2018年9月からDNSSEC検証が普及
  - JP CN MOなどではDNSSEC検証率が低め
  - 日本でもDNSSEC検証率が高いASがある

Copyright © 2019 Japan Registry Services Co., Ltd.

(DNSからみた)
IPv6の普及状況

Copyright © 2019 Japan Registry Services Co., Ltd.

JPドメイン名でのIPv6設定状況

- JPRSでは、2006年からゾーンファイルなどを保存している
  - (それ以前のものもあるはずだが、取り出しにくいので)
- JPゾーンファイルのホスト情報(JPドメイン名)にIPv6アドレスを設定しているものは数えられる
  → IPv6アドレスを持つホスト情報を参照するドメイン名数
- ただし、JPゾーンファイルからわかるものは一部だけ
  - JP以外のネームサーバ名のものは、過去の情報がわからない
  - JPでも、JPゾーンにないネームサーバ名はわからない
- 現在の情報は、別途名前解決を行って集計可能

Copyright © 2019 Japan Registry Services Co., Ltd.

JPゾーンファイル例 (一部)

jp. IN SOA z.dns.jp. root.dns.jp. 1560495602 3600 900 1814400 900

jp. IN NS a.dns.jp.

dnslab.jp. IN NS ns.dnslab.jp.

ns.dnslab.jp. IN AAAA 2001:200:132:7::3

ns.dnslab.jp. IN A 203.178.129.35

wide.jp. IN NS ns-wide.wide.ad.jp.

ns-wide.wide.ad.jp. IN AAAA 2001:200:0:1::f

ns-wide.wide.ad.jp. IN A 203.178.136.59

jpdirect.jp. IN NS dns-b.iij.ad.jp.

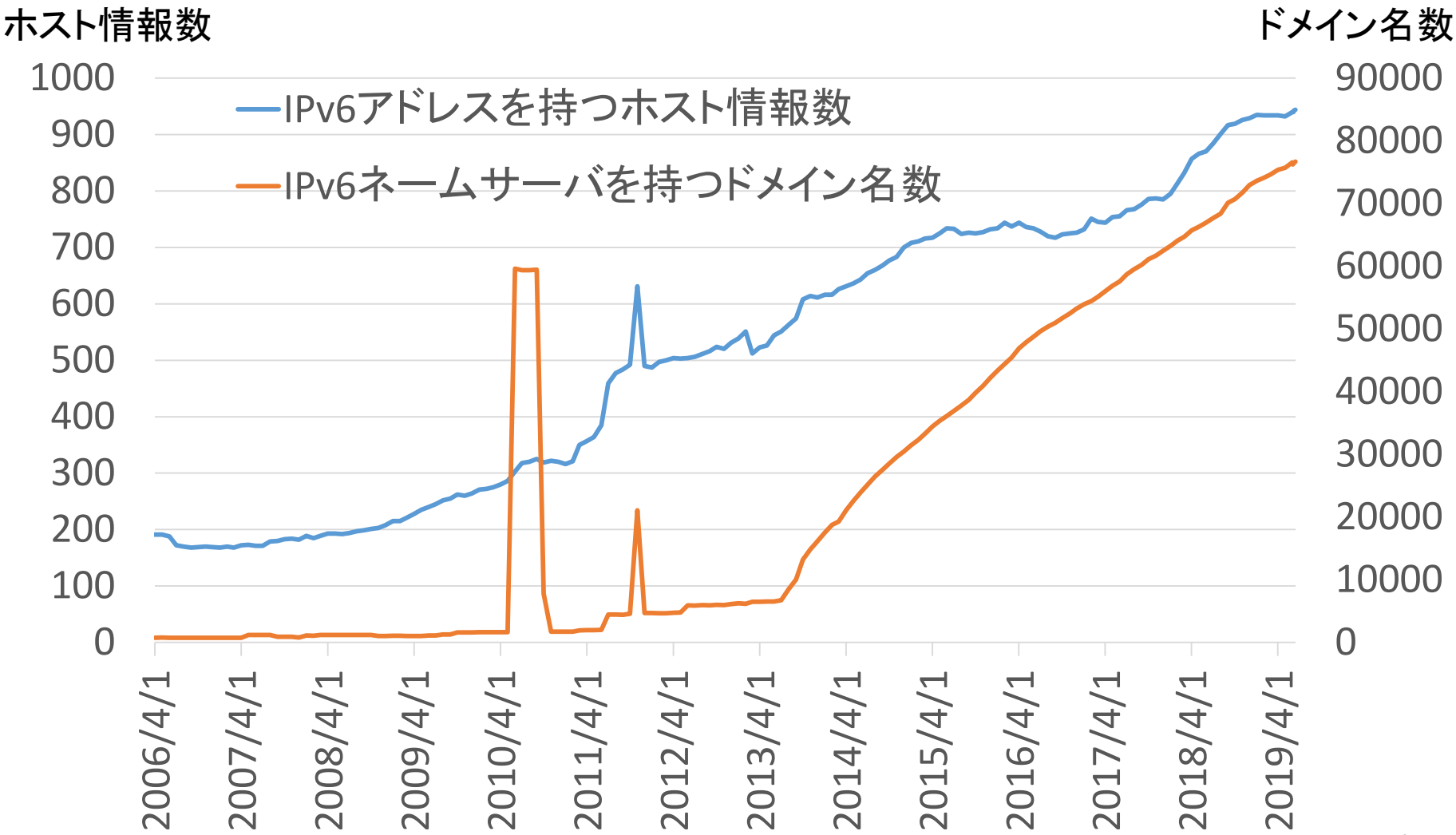
jpdirect.jp. IN NS dns-c.iij.ad.jp.

JPゾーンファイルだけでIPv6ネームサーバがあることがわかる
(過去の評価も可能)

ゾーンファイルだけではIPv6ネームサーバがあるかわからない
別途、ネームサーバ名の名前解決を行い、AAAAリソースレコードがあるか判定する必要あり
(過去に遡れない)

Copyright © 2019 Japan Registry Services Co., Ltd.

JPゾーンファイルから見たIPv6対応の変化



各月の1日の情報をプロット

Copyright © 2019 Japan Registry Services Co., Ltd.

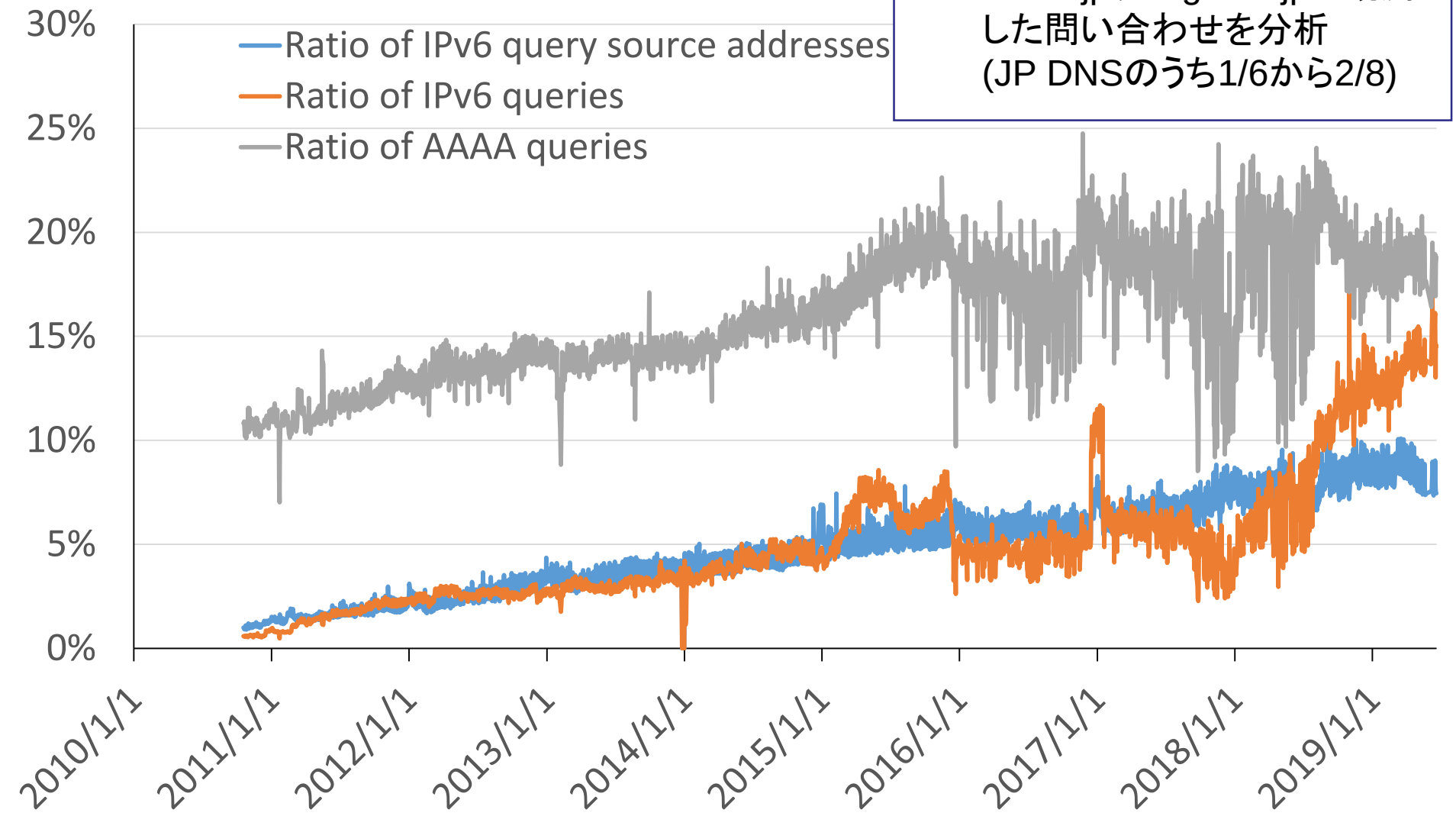
JPドメイン名の状況 (2019/6/21)

- ゾーンファイルではよくわからないので、JP登録ドメイン名の名前解決で調査 (接続まではしていないことに注意)
  - ドメイン名$dom {SOA,NS,A,AAAA}, www.$dom {A,AAAA}, ネームサーバ名 $ns {A,AAAA}を問い合わせ
  - 2019/6/21朝のJPゾーンにあるドメイン名に6/21中に問い合わせ
- ネームサーバ設定されているもの　1,540,542
  これを100%として以下を集計
- ドメイン名 SOAの名前解決できたもの　1,452,053 (94.3%)
  - そのうち、IPv6ネームサーバをもつもの　315,621 (20.5%)
  - IPv6サーバのみ　17
- ドメイン名頂点またはwww. にAが指定　1,350,642 (87.7%)
- ドメイン名頂点またはwww. にAのみ(IPv4のみ) 1289008 (83.7%)
- ドメイン名頂点またはwww. にAAAAのみ(IPv6のみ) 17
- ドメイン名頂点またはwww. にAAAAとA　61634 (4%)
- ドメイン名頂点またはwww. にAAAA　61651 (4%)
  - ネームサーバがIPv6アドレスを持つ　54074 (3.5%)　IPv6対応
  - ネームサーバがIPv4アドレスのみ　7577 (0.5%)　IPv4に依存

Copyright © 2019 Japan Registry Services Co., Ltd.

JP DNSへの問い合わせの変化

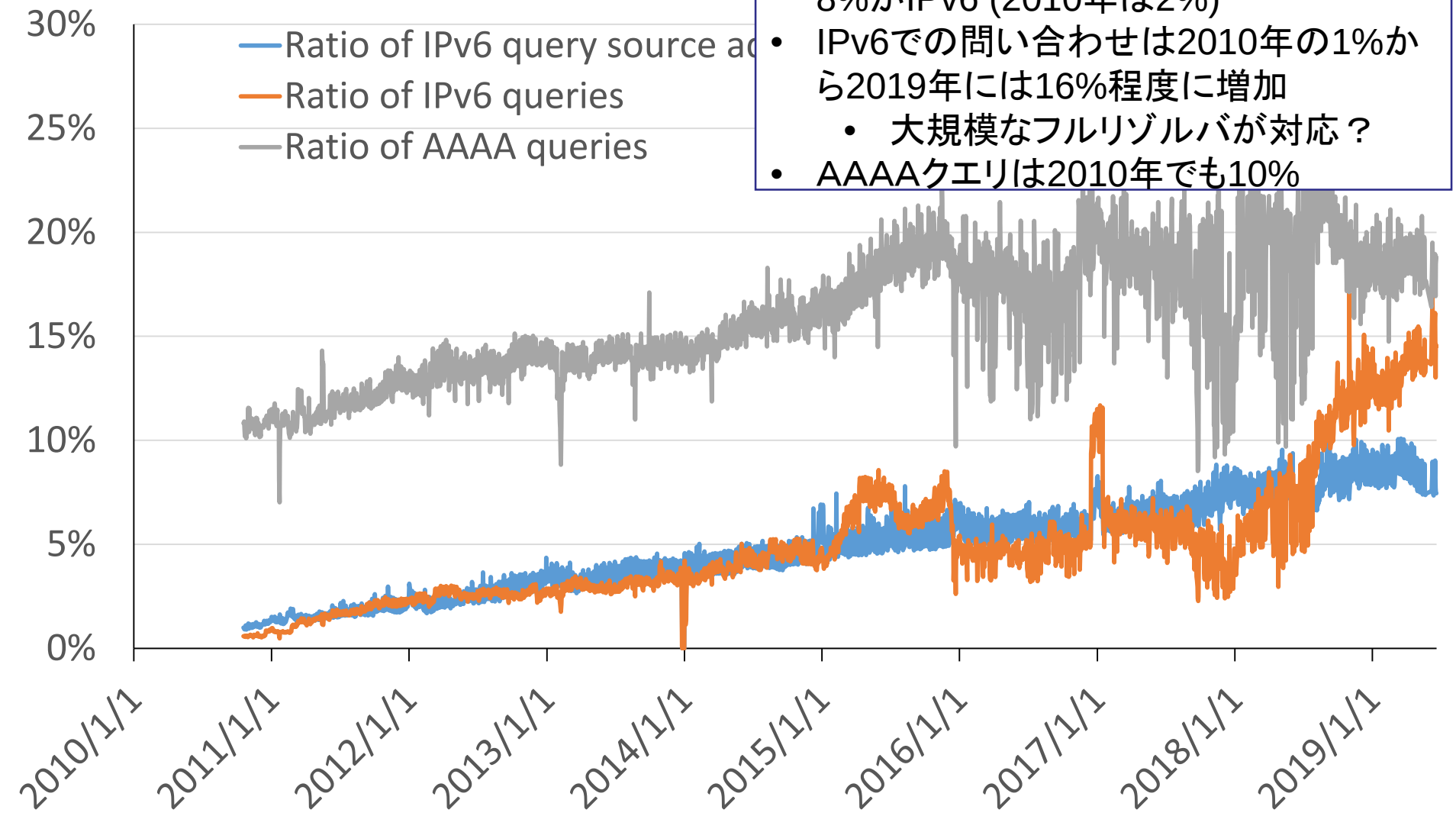
a.dns.jp及びg.dns.jpで観測した問い合わせを分析
(JP DNSのうち1/6から2/8)



Copyright © 2019 Japan Registry Services Co., Ltd.

JP DNSへの問い合わせの変化

- JP DNSに問い合わせを送るアドレスの8%がIPv6 (2010年は2%)
- IPv6での問い合わせは2010年の1%から2019年には16%程度に増加
  - 大規模なフルリゾルバが対応？
- AAAAクエリは2010年でも10%



Copyright © 2019 Japan Registry Services Co., Ltd.

人気あるドメイン名の対応状況

- リスト: http://s3-us-west-1.amazonaws.com/umbrella-static/top-1m.csv.zip
  - 登録ドメイン名に整形, 重複削除 → 約23万　そのうち10万調査
  - ドメイン名$dom {SOA,A,AAAA}, www.$dom {A,AAAA}
  - unboundに問い合わせ (IPv4-onlyとIPv6-onlyを用意)

		応答なし	SOA応答あり	Aあり	AAAAあり	両方なし	両方あり
IPv4 only	1 - 1000	6	994	791	167	203	167
IPv6 only	1 - 1000	168	831	653	134	179	134
IPv4 only	1 - 10000	90	9,894	8,490	1,654	1,420	1,654
IPv6 only	1 - 10000	2,321	7,653	6,450	1,397	1,229	1,397
IPv4 only	1 - 100000	8,633	90,883	84,078	17,611	7,280	17,602
IPv6 only	1 - 100000	36,434	63,136	57,615	15,391	5,942	15,382

  - IPv6のみで名前解決できたドメイン名が 63136(63%)　(SOA応答)
    - DNSサーバのIPv6対応は進んでいる (DNSプロバイダが対応か？)
  - そのうちゾーン頂点またはwwwにAAAAあるものが 15391 (15%)
    - WebサーバのIPv6対応は遅れているが JPの3.5%よりは多い
  - 名前解決できないものや、SOA応答がないものが10%
    - 存在しないもの (lan, local, home) や非終端ドメイン名 (com.fj)　掃除不足

Copyright © 2019 Japan Registry Services Co., Ltd.

IPv6普及状況のまとめ

- IPv6対応ドメイン名は増加傾向にあり、JPの3.5%
- 大規模ISPはIPv6に対応し、JPでのIPv6での問い合わせは2010年の1%から2019年には16%に増加

Copyright © 2019 Japan Registry Services Co., Ltd.

Acknowledgements

- DNS-OARC as the data source of Root dataset

- Referred APNIC Labs data and graphs
  - https://stats.labs.apnic.net/dnssec
  - https://stats.labs.apnic.net/rvrs/

- Referred stats.dnssec-tools.org data and graphs
  - http://stats.dnssec-tools.org/

Copyright © 2019 Japan Registry Services Co., Ltd.