JP DNSで見た最近の変化

IPv6普及, DNSSEC検証, ポートランダマイゼーションなど

藤原 和典
<fujiwara@jprs.co.jp>
株式会社日本レジストリサービス (JPRS)

2015/11/19 dnsops.jp BoF

概要

- JPRSでは、A.DNS.JPのクエリログを11年分と、全JP DNSの50時間のパケットキャプチャを年に2度程度収集しています。

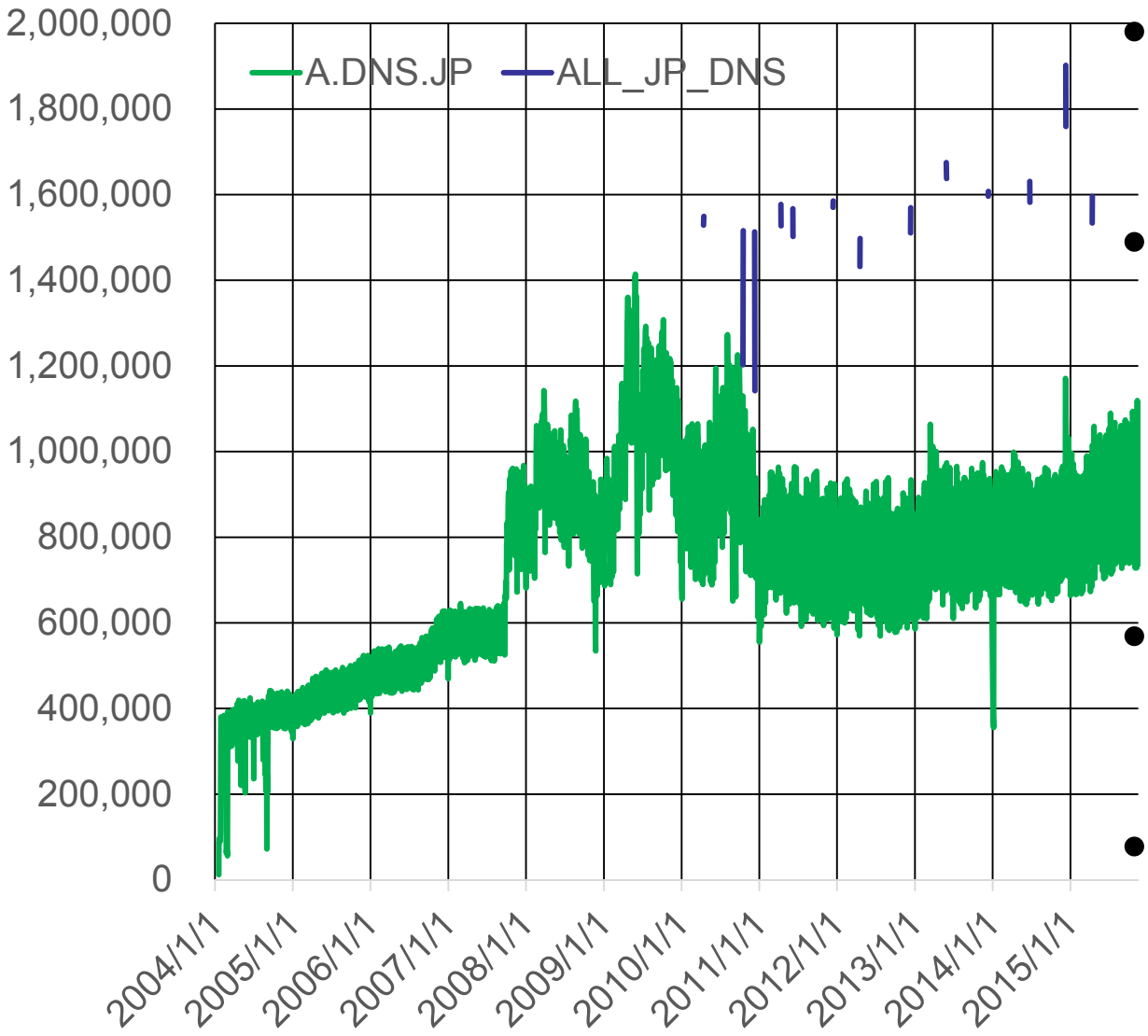
- 今回はIPv6関連のクエリ、DNSSEC検証、ポートランダマイゼーションの普及について見てみました。

Overview of JP

- .JP has 1,404,572 registered domain names (Nov. 1, 2015)
- JP DNS servers serve 1.6 billion queries per day
- Collecting packet captures and query logs

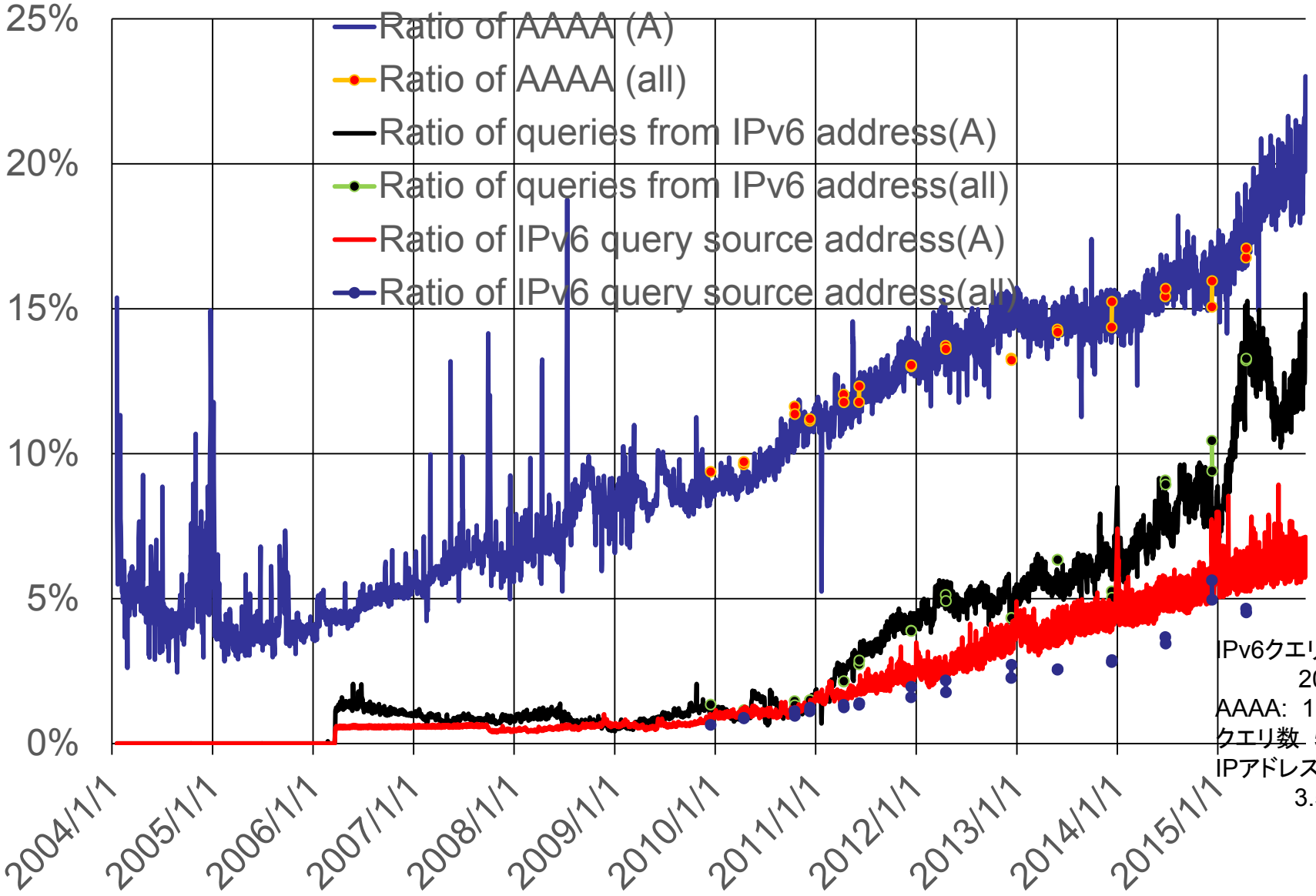
Name	Operator	Location	Address (IPv4:7, IPv6:6, total 13)	Capture
A.DNS.JP	JPRS	JP*2	203.119.1.1, 2001:dc4::1	Pcap/Log
B.DNS.JP	JPNIC	JP*1	202.12.30.131, 2001:dc2::1	Pcap
C.DNS.JP	JPRS	Worldwide	156.154.100.5, 2001:502:ad09::5	Pcap
D.DNS.JP	IIJ	JP*2, US*2	210.138.175.244, 2001:240::53	Pcap
E.DNS.JP	WIDE	JP*1,US*1, FR*1	192.50.43.53, 2001:200:c000::35	Pcap
F.DNS.JP	NII	JP*1	150.100.6.8, 2001:2f8:0:100::153	Pcap
G.DNS.JP	JPRS	JP*1	203.119.40.1	Pcap/Log

JPで24時間に観測したIPアドレス数



- JP DNS全体で一日160万
- A.DNS.JPで80～100万
  - Aだけだと全体の6割程度
- 2010年から変化なし/微増
- (Root:48時間で約1000万, JPは200万)

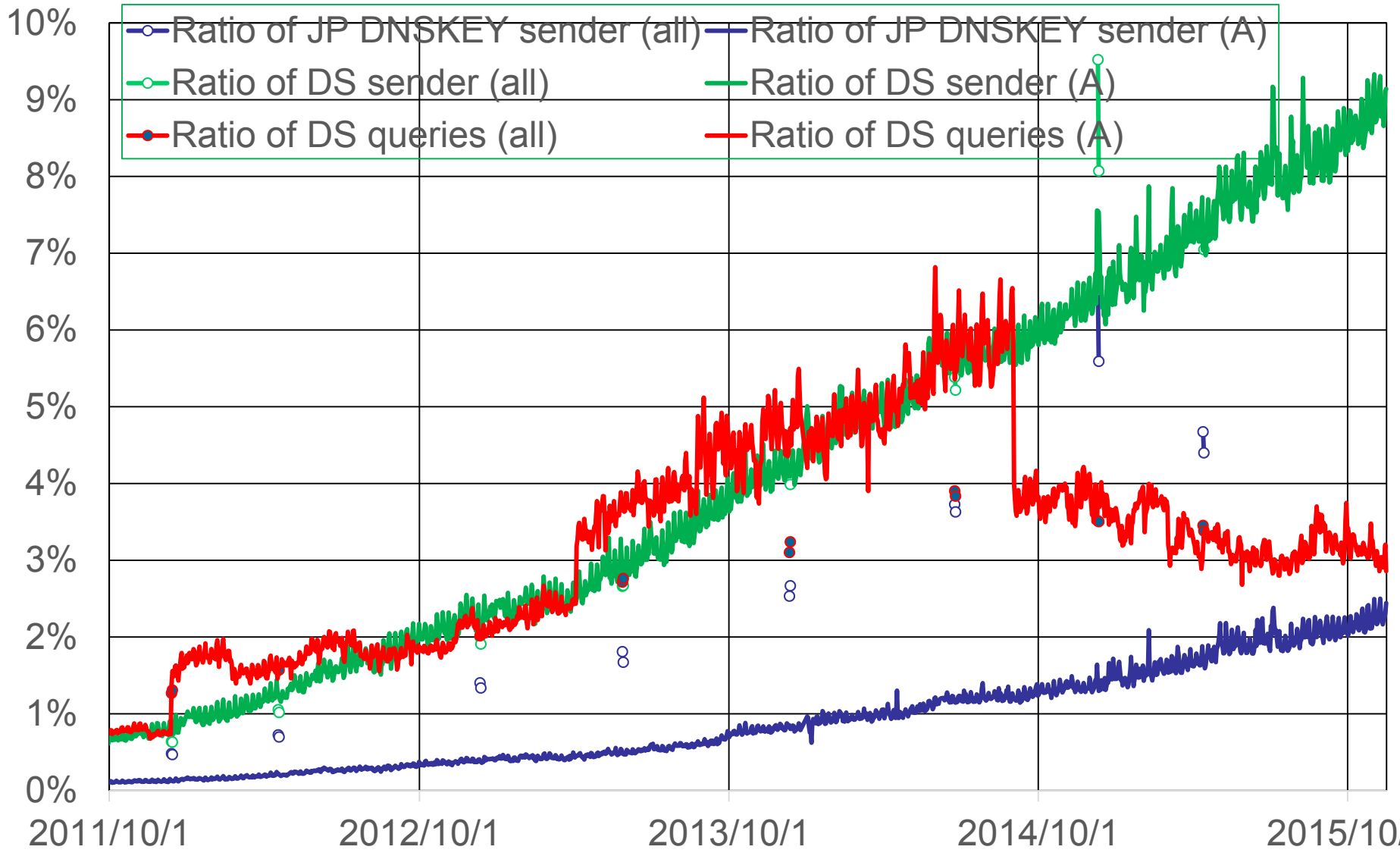
IPv6関連クエリの割合の変化



IPv6クエリは増加

	2012	2015
AAAA:	15%	20%
クエリ数	5%	14%
IPアドレス数:	3.5%	6%

DNSSECへの関心度



DNSSECへの関心度 (解説)

- JP DNSKEY, DSクエリをJP DNSに送るIPアドレスをValidatorだと仮定
  - ただし、Security-Aware Stub Resolverからのクエリを受けるフルリゾルバはDNSKEY, DSクエリを送るがValidatorではない
  - 例: local_unbound=“YES”と設定したFreeBSD 10
- Validatorの可能性があるアドレスは順調に増え、現在約9% (DS)
  - JP DNSKEYを送るアドレスだと4.5%
- DSクエリの割合は、2011年12月と2013年4月に増加し、2014年8月に激減した
  - 大規模ISPのon/offの可能性あり

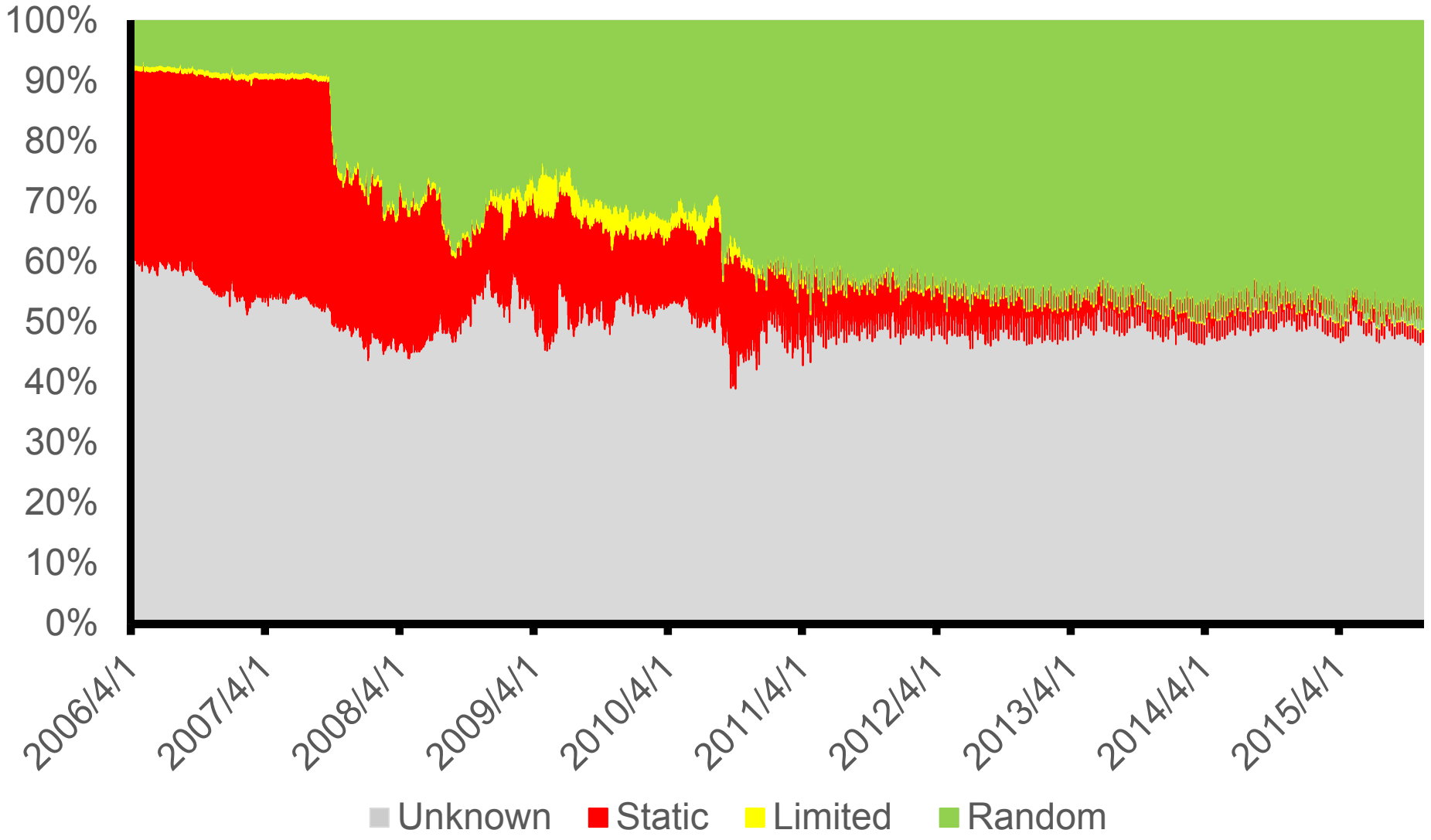
DSクエリが増える理由

- DNSSEC運用していないドメイン名、たとえばwide.ad.jpにはDSがない。
  - wide.ad.jp DSのTTLはJP NCACHE TTLの900
- Validatorは、wide.ad.jpの名前解決時に、wide.ad.jp DSが存在することを確認する
  - 最悪の場合、900秒ごとにDSクエリをJP DNSに送る
- 今後はJP DNSにDSクエリが殺到する懸念
  - draft-fujiwara-dnsop-ds-query-increase (2013/6)
  - DNS/DNSSECプロトコルとパラメータの問題
  - ただし、DSクエリが減ったので放置 (expired)
  - みなさん、DNSSEC検証を商用サービスにいれて、ぜひ大量のDSクエリを送ってください
  - それでクエリが増えたら、うれしい悲鳴ということで

ソースポートランダマイゼーション(SPR)の普及度

- 仮定
  - あるIPアドレスのフルリゾルバは常に同じ
  - SPRしているとJP DNSには毎回違うポート番号でクエリ
- 判定のアイデア
  - IPアドレスごとに、一日ごとのポート番号使用数を見る
  - 単調増加、単調減少もありうる
- 実装
  - IPアドレスごとに、65536ビットのビットマップは重いので上位下位8ビットつづの512ビットのビットマップ
  - ポート番号の大小や変化数もみたが、あまりグラフに変化がないため、単調な変動を無視
  - A,Gのクエリログをもとに集計
- 以下の4種に分類 → これは私見であり、他者の分類とは異なる
  - Unknown: 一日10クエリ未満を判定不能
  - Static: 上位3ビット以下 and 下位3ビット以下の使用を固定
  - Limited: 上位3ビット以下 or 下位3ビット以下の使用を限定
  - Random: 上位4ビット以上 and 下位4ビット以上をランダム

ソースポートランダマイゼーションの普及 (IPアドレスの割合)



ソースポートランダマイゼーションの普及 (IPアドレスの割合)