2016年の
インターネット運用動向

～トラフィック・ルーティング・DNS・Security～

NTT Communications
Tomoya Yoshida
<tomoya.yoshida@ntt.com>

内容

- トラフィック動向
- ルーティング動向
- DNS動向
- セキュリティ動向
- まとめ

内容

- トラフィック動向
- ルーティング動向
- DNS動向
- セキュリティ動向
- まとめ

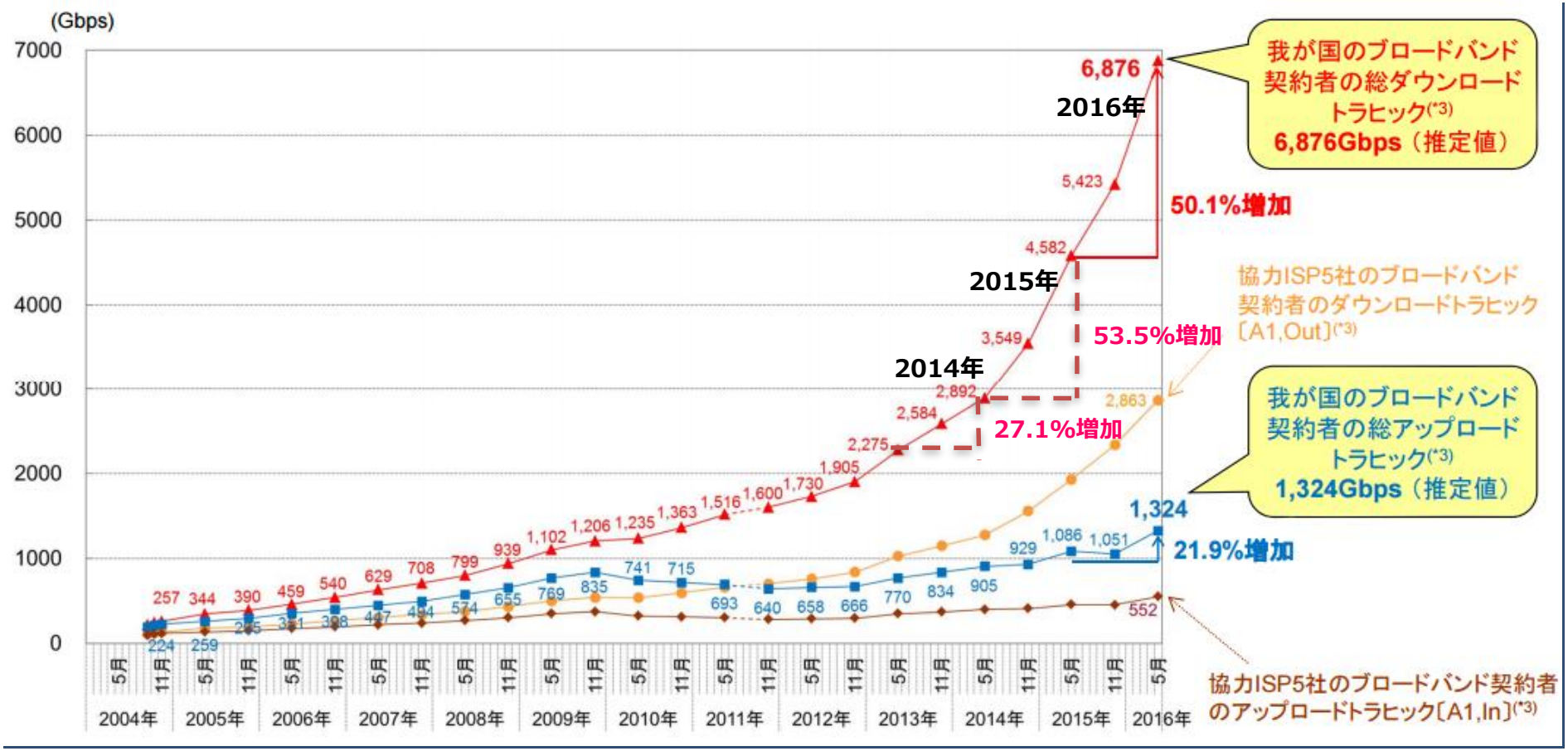
2016年 トラフィック動向

- ブロードバンドトラフィックは増加の一途を辿っている
  - ここ１年でダウンロードが**50.1%増**、2015年は53.5%
  - 1契約者あたりのブロードバンドトラフィックが伸びている（後述）
  - アクセス環境やコンテンツ自体がリッチになり増加を牽引
  - **wifiのオフロードトラフィック**の増加
  - クラウド型サービス等によりアップロードトラフィックも益々増加
- モバイルトラフィックも増加率は低迷するも増え続けている
  - ここ1年で**1.35倍**、増加率は徐々にゆるやかに
  - 帯域制限により月末にかけてトラフィックが減少する傾向は依然見受けられる
- 1日のトラフィック
  - お昼休みの12時台と夜の22時～23時前後にピークの傾向は変わらない
  - **１日のトラフィック変動幅がますます増加し、下限値の上がり幅が年々急増**
- IPv6トラフィックはゆるやかに増加、ISPの導入次第
- **HTTPからHTTPSへ**の動きが全世界で加速化しているが、日本は慎重
- イベント時のトラフィック変動も様々観測されている
  - 7月にリリースされたあのソフトの影響は大きかった。。

日本国内のトラフィック推移

日本全体のブロードバンドトラフィックの推移

集計:2016年5月

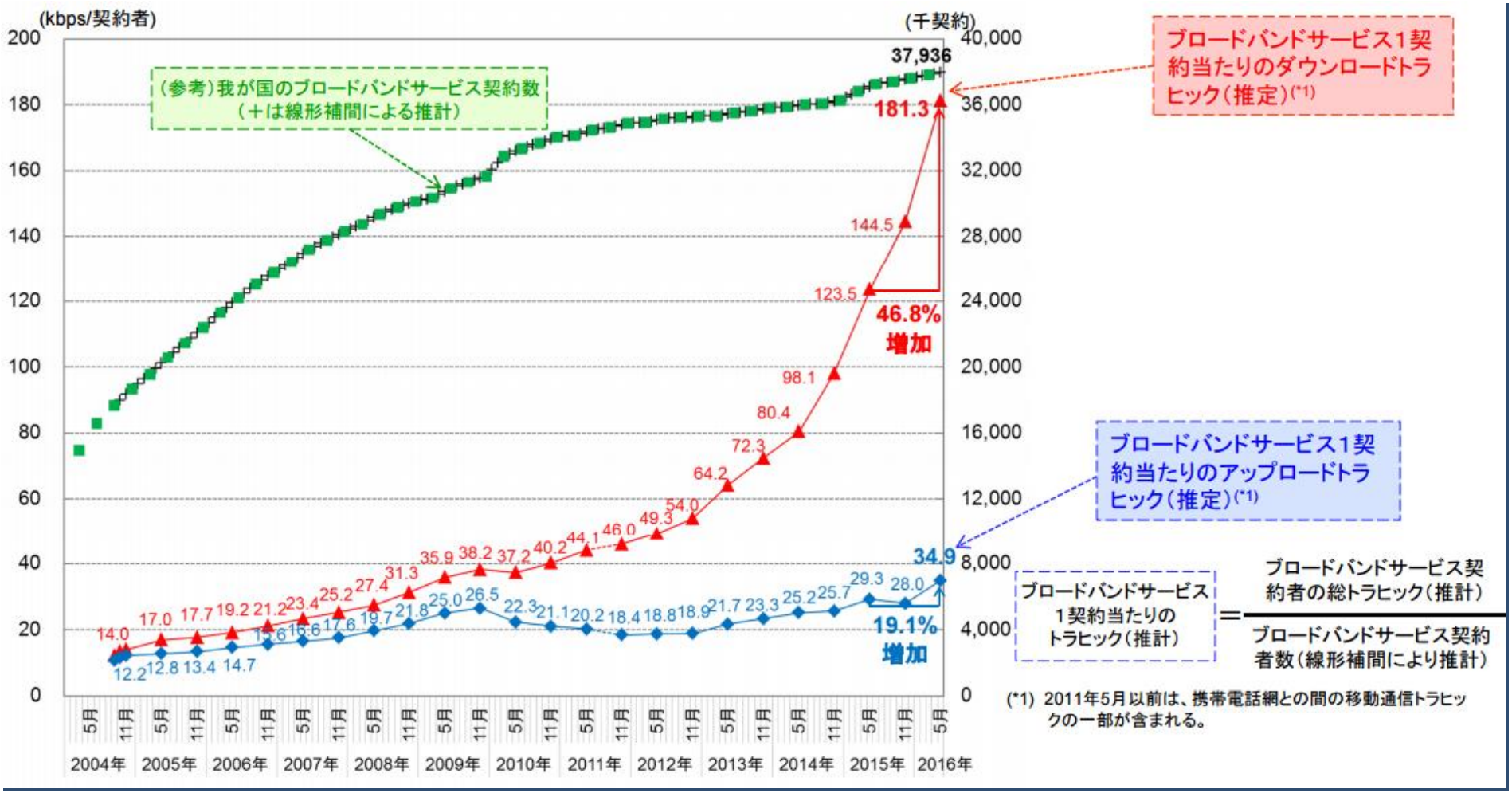


出典：総務省「**我が国のインターネットにおけるトラヒックの集計・試算**」　2016年7月22日

日本国内のトラフィック推移

1契約者あたりのブロードバンドトラフィックの推移

集計:2016年5月

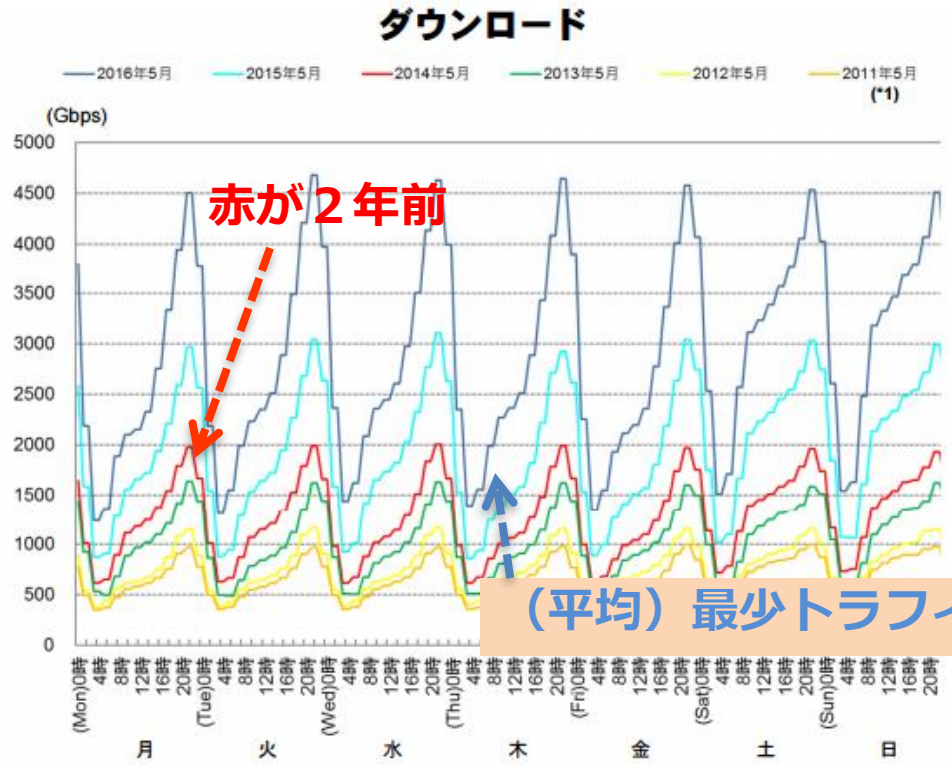


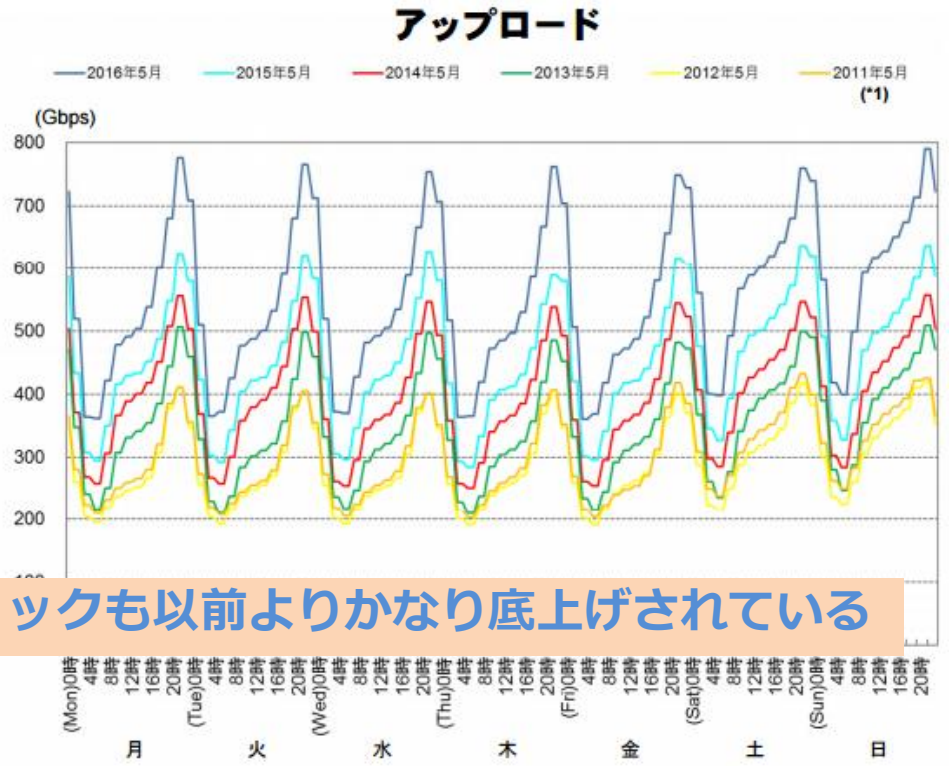
出典：総務省「**我が国のインターネットにおけるトラヒックの集計・試算**」　2016年7月22日

日本国内のトラフィック推移

5分平均のピークトラフィックの推移

ブロードバンドサービス契約者の時間帯別トラヒックの変化（過去６年の比較）





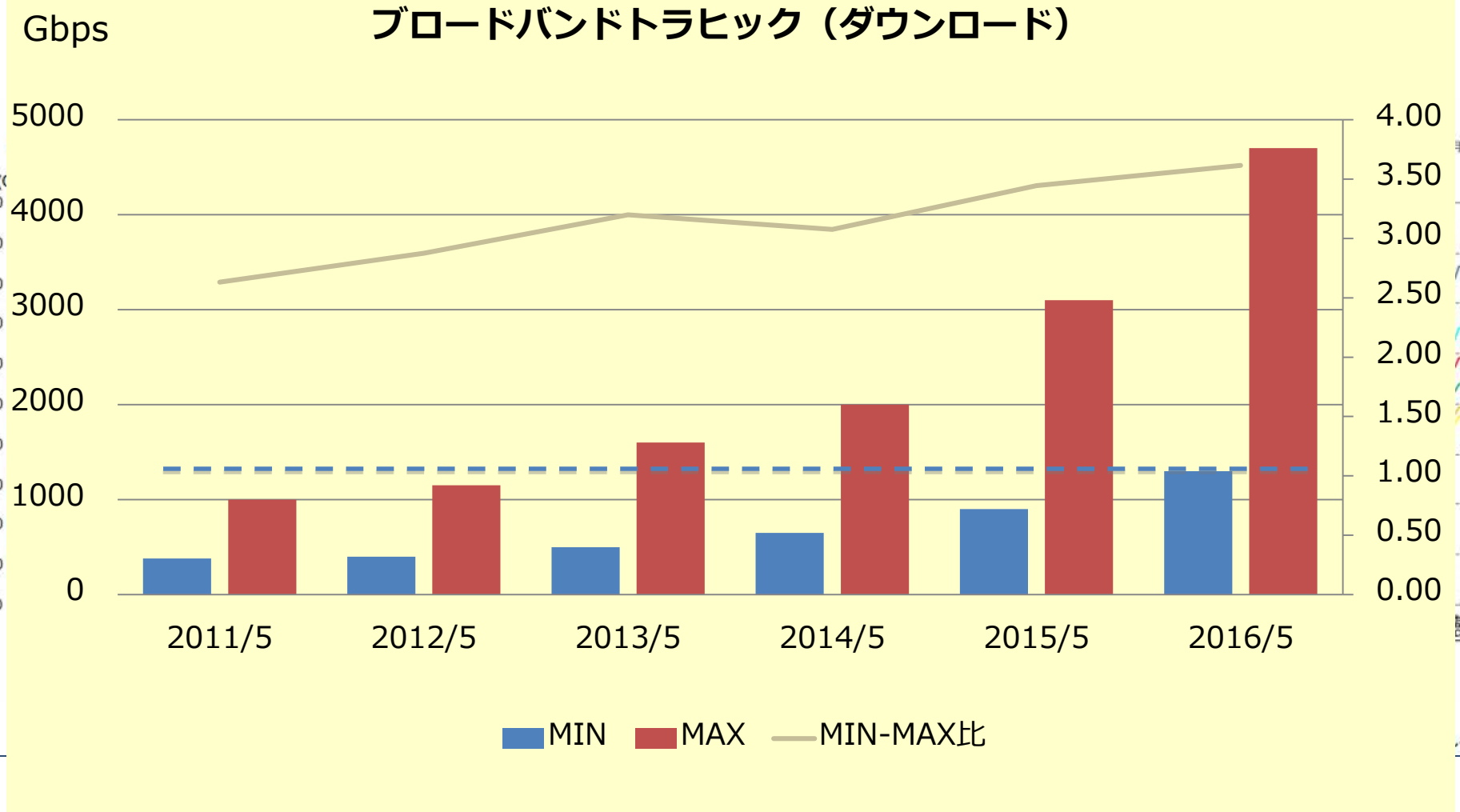
（平均）最少トラフィックも以前よりかなり底上げされている

(*1) 2011年5月以前は、携帯電話網との間の移動通信トラヒックの一部が含まれる。

出典：総務省「**我が国のインターネットにおけるトラヒックの集計・試算**」　2016年7月22日

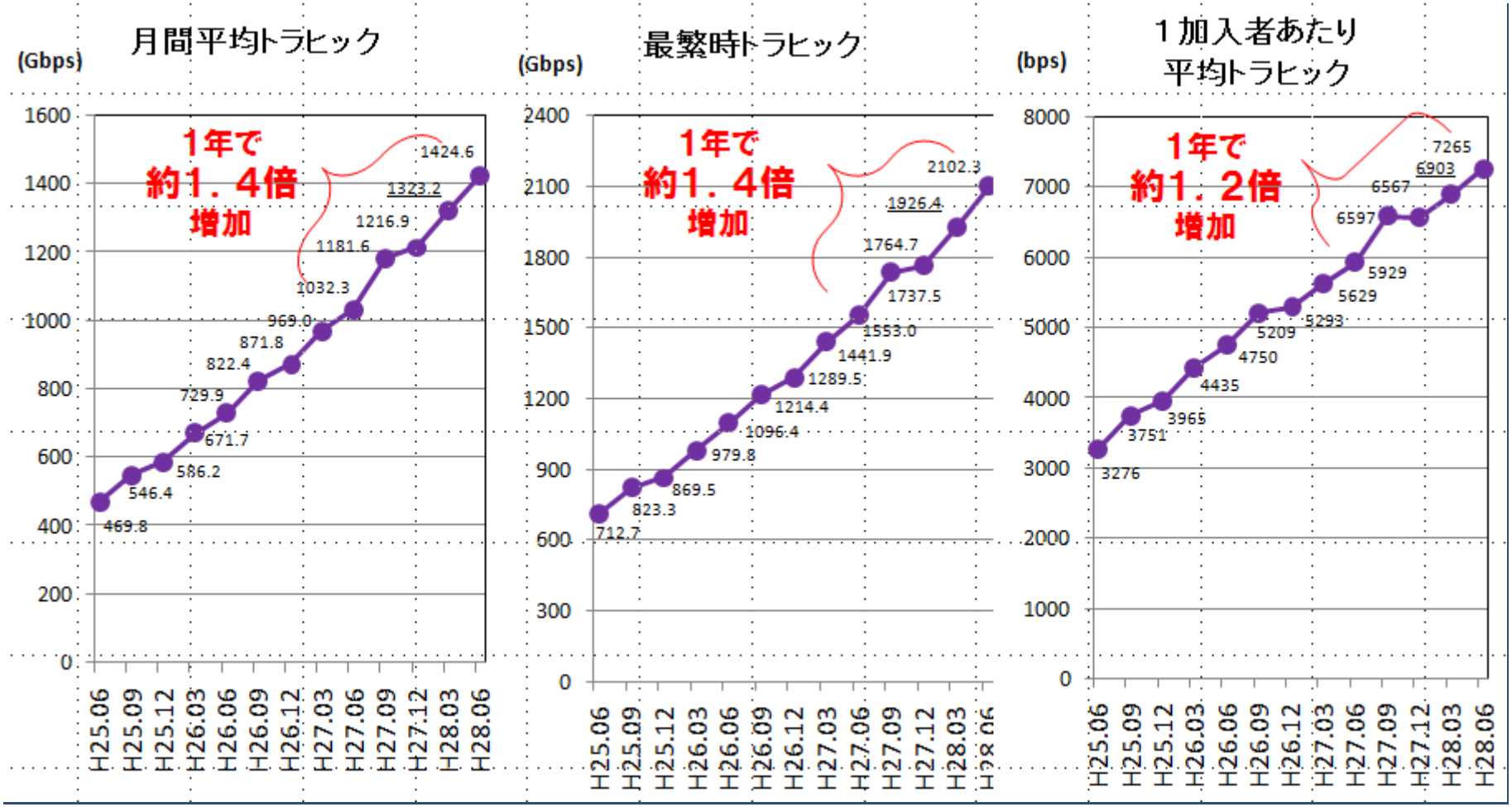
日本国内のトラフィック推移

5分平均のピークトラフィックの推移



移動通信トラヒックの推移（過去３年間）

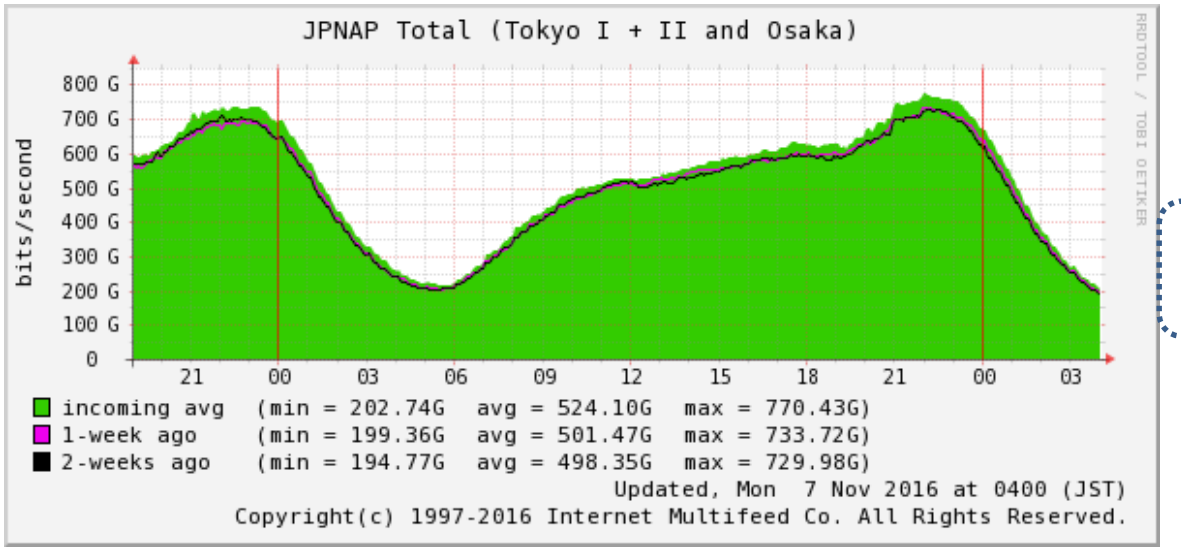
トラヒックの**伸び幅**は、ここ1年で　**固定通信(50%)＞移動通信(35%)**　徐々に減少傾向



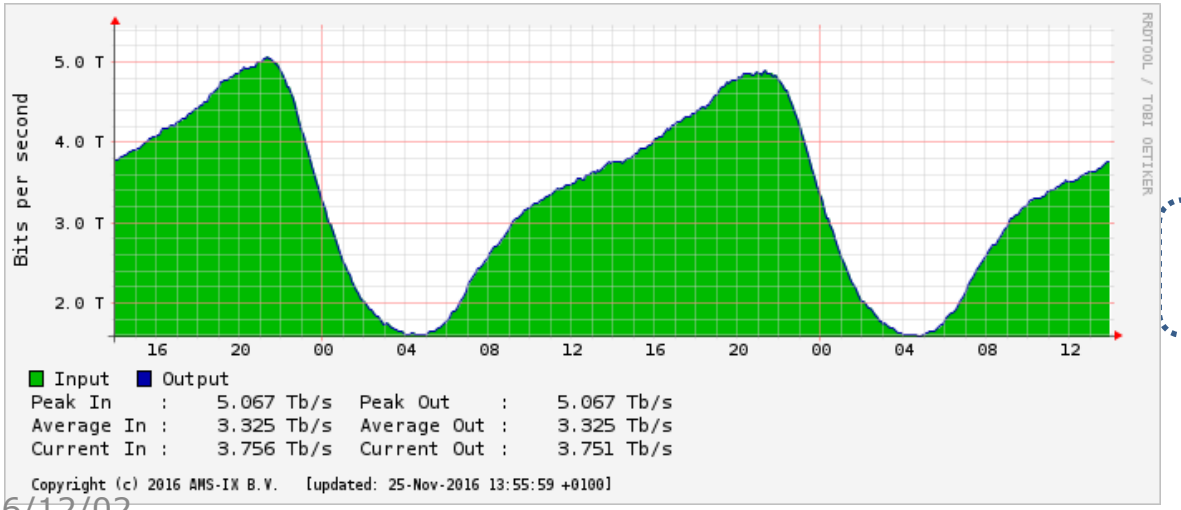
出典：総務省「**我が国の移動通信トラヒックの現状**（平成２８年６月分）」

1日のトラフィック傾向

JPNAPのグラフは休日の例（お昼のトラフィックの凸凹はない）
MIN-MAXの比率は、双方ともに概ね4倍程度



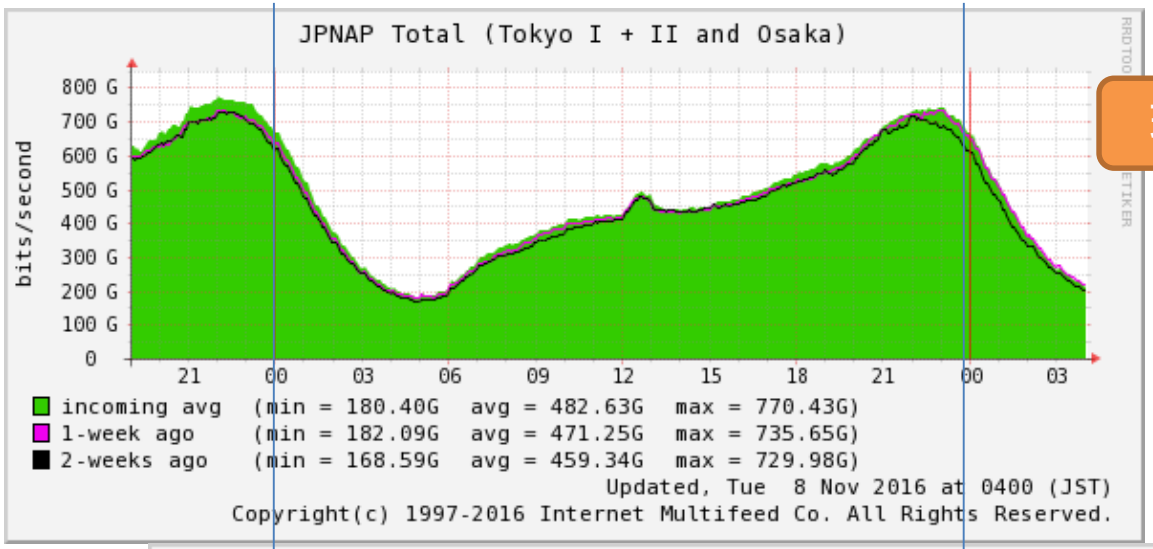
JPNAP(Japan)の
1日のトラフィック推移



AMS-IX(Europe)の
1日のトラフィック推移

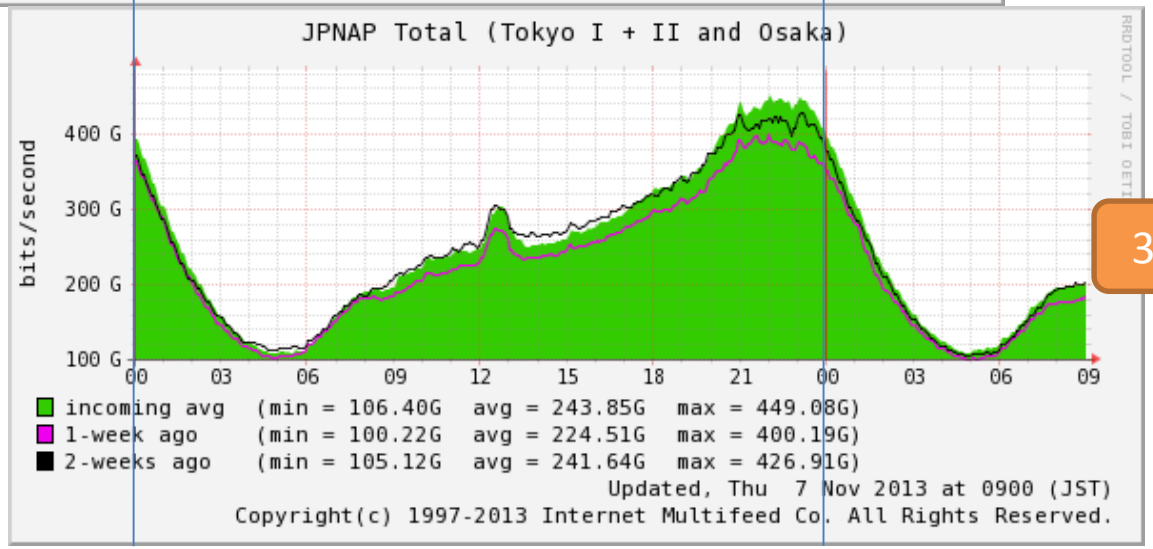
1日のトラフィック傾向（3年前比較）

ピークは夜の22時30分ぐらい。日本のお昼のトラフィックは特徴的
朝方のトラフィックも着実に増加している



現在

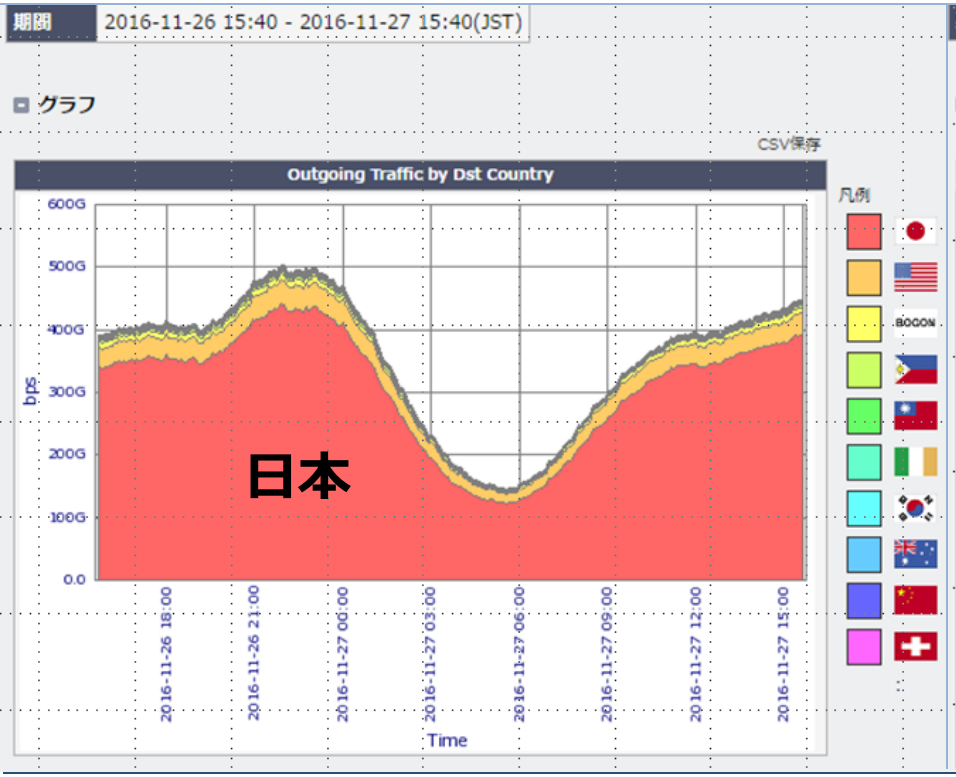
JPNAP(Japan)の
1日のトラフィック推移



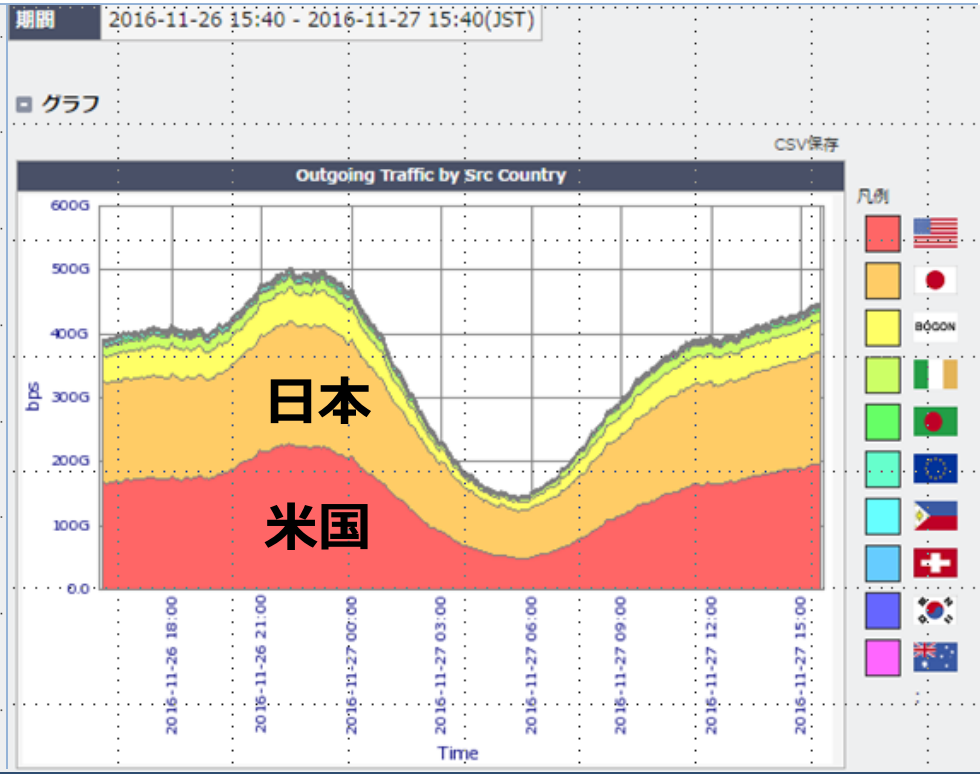
3年前

JPNAP通信の国別集計結果
2016/11/26～27

宛先IPの国別集計（宛先国）

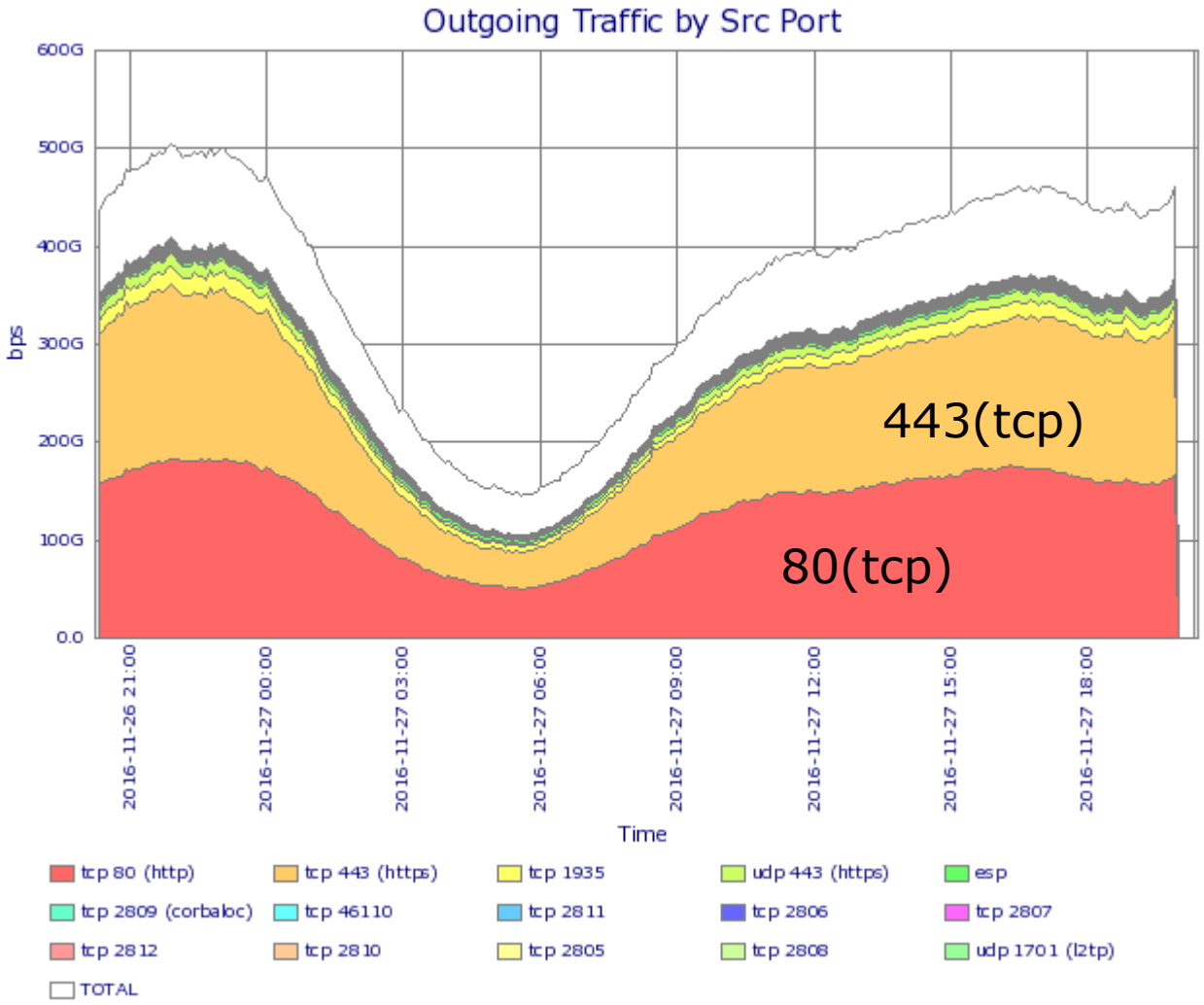


送信元IPの国別集計（発信国）



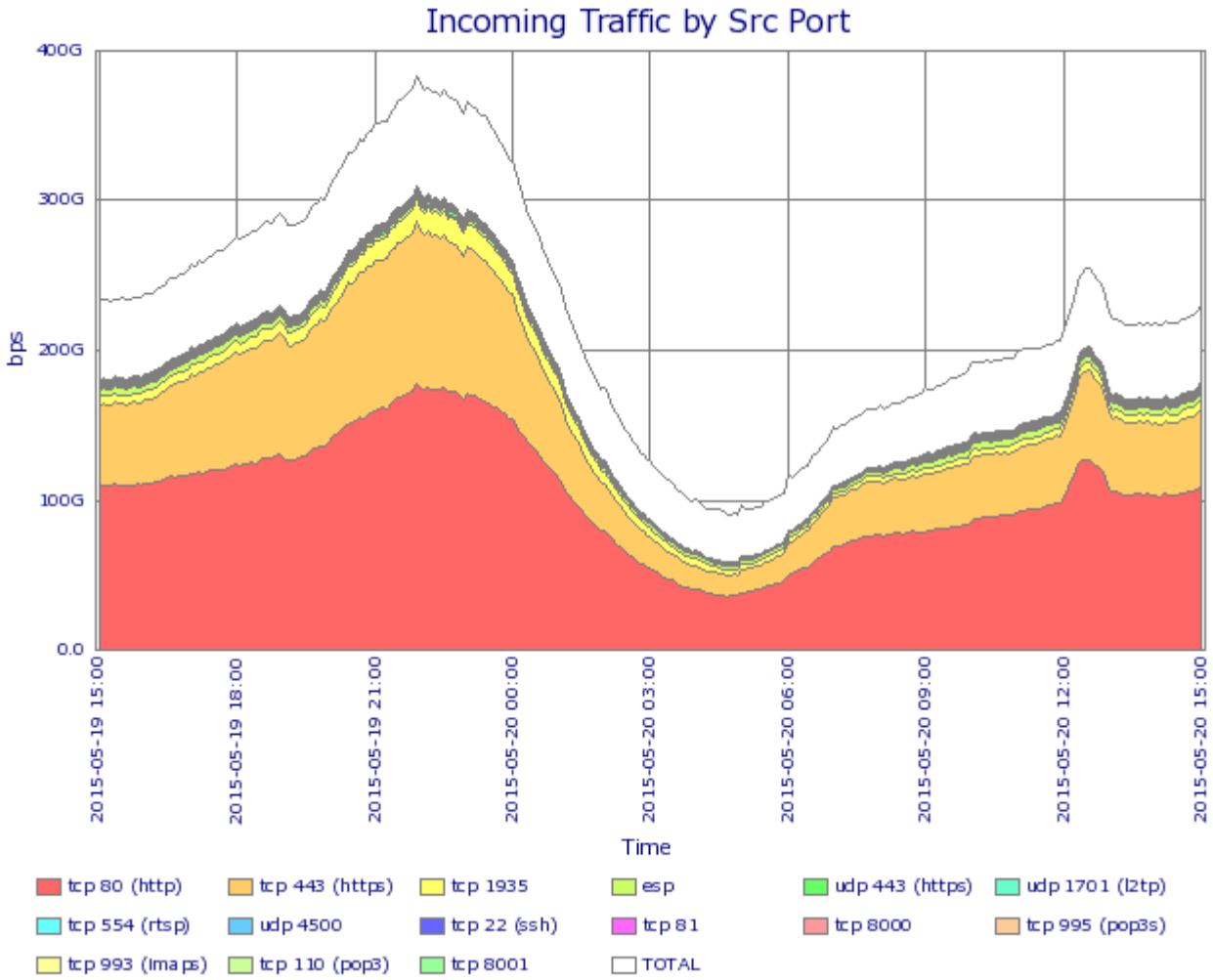
JPNAP全体での利用ポート比率

- tcp443の割合が増加してきている



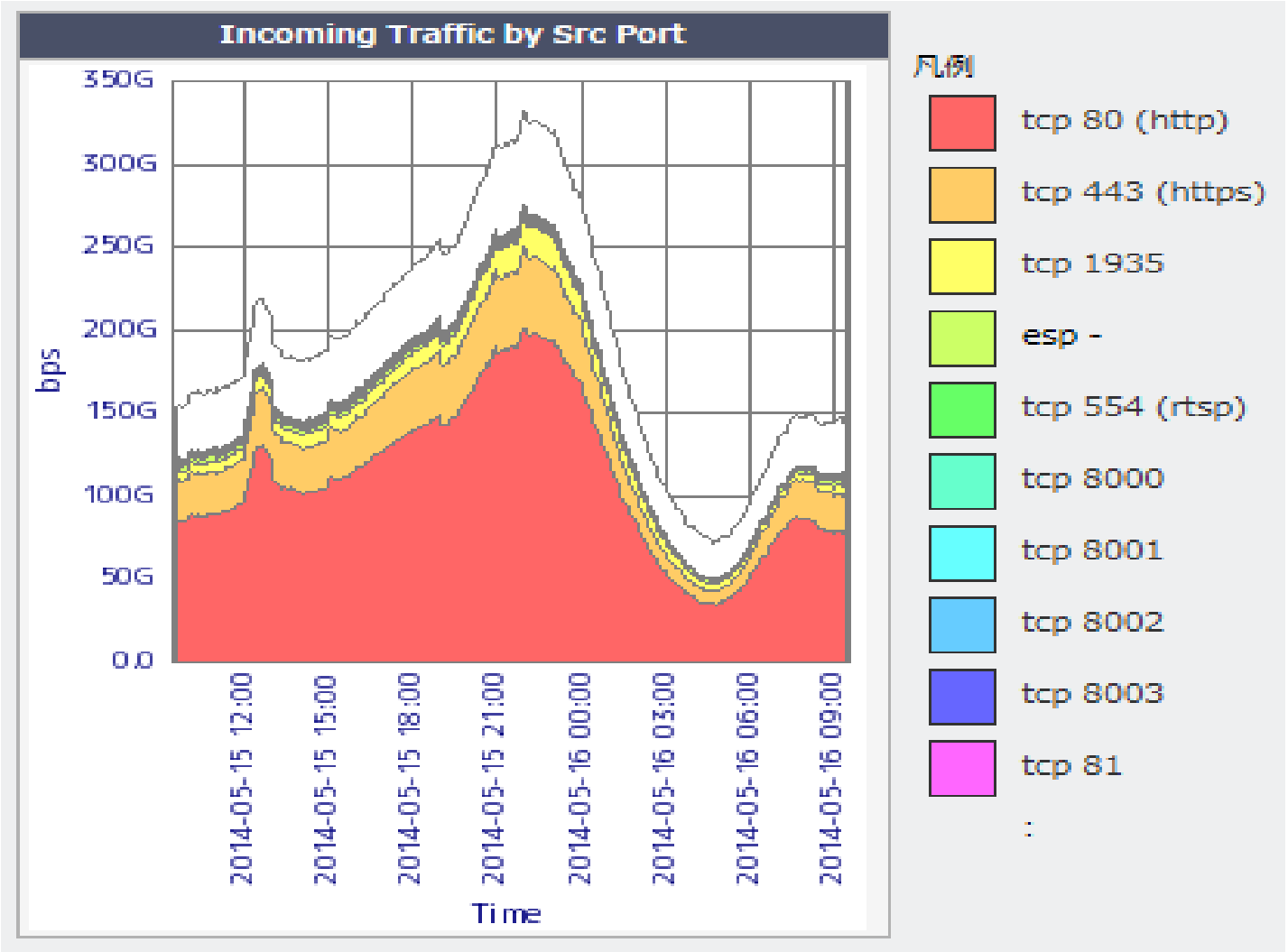
1年前

- TCP80の割合が多い
- 特に早朝帯の人が寝ている時間はTCP80の割合が増加

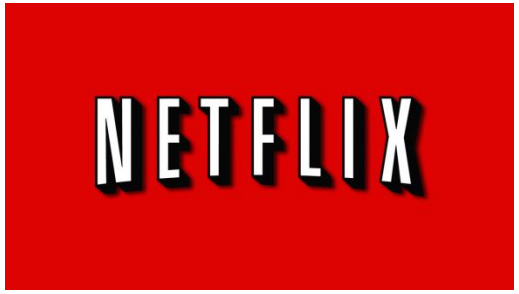


2年前

- かなりTCP80の割合が多い
- tcp80 => tcp443 は2014年～2015年の変化が顕著



既に多くのサービスがHTTPS化

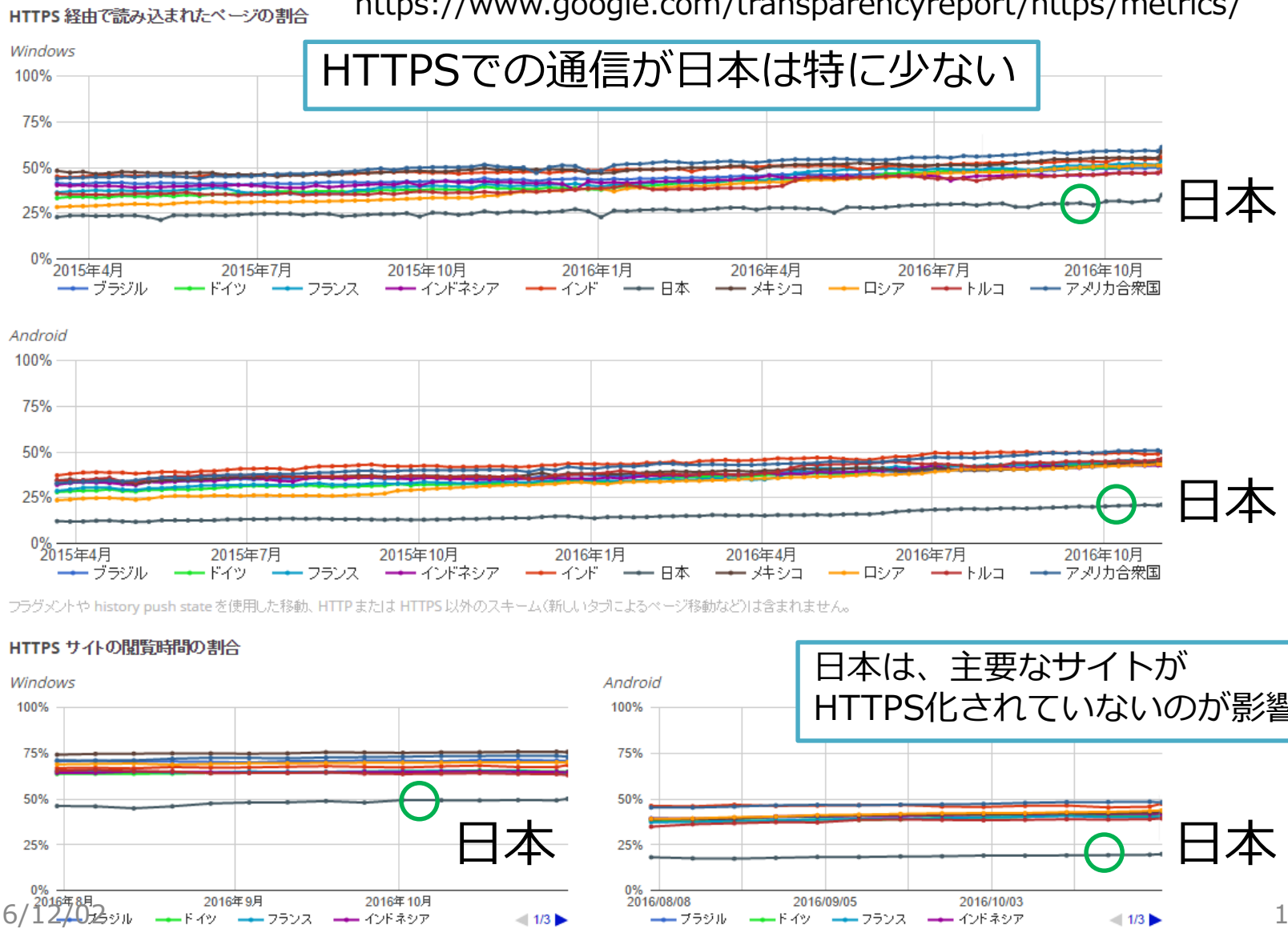


HTTPS化の加速

- 通信がセキュアになる
- Google
  - HTTPS 優先でランキング シグナルに反映
- 従来できていたことが困難に
  - ログやデータ解析
  - リファラの取得
- SSLのオーバーヘッド

Chromeユーザのアクセス状況解析統計結果（透明性レポート）

https://www.google.com/transparencyreport/https/metrics/



HTTPSでの通信が日本は特に少ない

日本

日本

日本は、主要なサイトが
HTTPS化されていないのが影響？

日本

Alexa Top site on the web

Alexa社が提供している、世界中のWeb siteへのアクセス Top ranking結果より

日本からのアクセスは、日本固有のサイトへのアクセスが多い中、徐々に外資系サイトの勢いが大きくなってきている

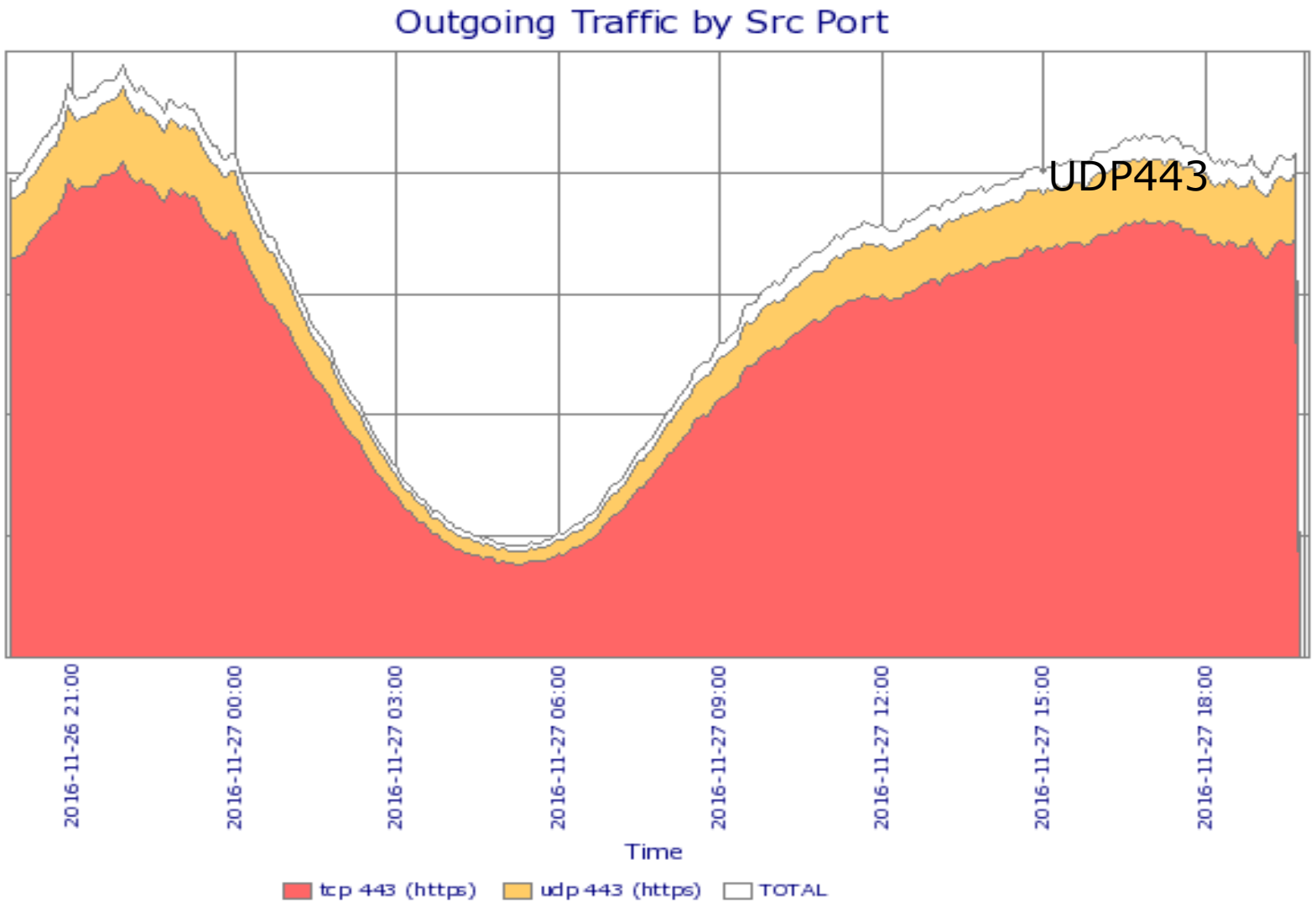
この中で、yahoo, rakuten, livedoor, ameblo, naver, などのトップRANKサイトがHTTPS対応を行っていないため、日本のHTTPS比率は低い水準になっている模様

直接関係はないが、、
Captive Portal等では、HTTPSでアクセスするとproxyされない問題もあり、今後要対応？？

http://www.alexa.com/topsites

RANK	JP	GLOBAL
1	Google.co.jp	Google.com
2	Yahoo.co.jp	Youtube.com
3	Google.com	Facebook.com
4	Youtube.com	Baidu.com
5	Amazon.co.jp	Yahoo.com
6	Fc2.com	Wikipedia.org
7	Facebook.com	Google.co.in
8	Twitter.com	Qq.com
9	Nicovideo.jp	Taobao.com
10	Rakuten.co.jp	Amazon.com
11	Wikipedia.org	Google.co.jp
12	Livedoor.jp	Live.com
13	T.co	Vk.com
14	Ameblo.jp	Twitter.com
15	Naver.jp	Instagram.com
16	Goo.ne.jp	Hao123.com
17	Baidu.com	Sohu.com
18	Kakaku.com	Sina.com.cn
19	Dmm.co.jp	360.cn
20	Hatenablog.com	Linkedin.com
21	Hatena.ne.jp	Tmall.com
22	Blog.jp	Weibo.com
23	2ch.net	Google.de
24	Qiita.com	Google.co.uk
25	Blogspot.jp	Google.fr

TCP443だけではない
UDP443も増加している



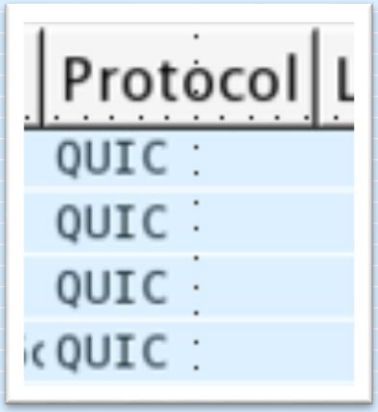
Youtubeを見ながら手元でwireshark

*Wi-Fi: en0 [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
473	6.245130000	2001:3a0:e002:217:c811:d16c	2404:6800:4004:22::e	QUIC	104	CID: 5358696136016785233, Seq: 102
474	6.245393000	2001:3a0:e002:217:c811:d16c	2404:6800:4004:22::e	QUIC	104	CID: 5358696136016785233, Seq: 103
475	6.245394000	2001:3a0:e002:217:c811:d16c	2404:6800:4004:22::e	QUIC	104	CID: 5358696136016785233, Seq: 104
476	6.245451000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 239
477	6.245457000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 240
478	6.245513000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 241
479	6.245516000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 242
480	6.245519000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 243
481	6.245562000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 244
482	6.245565000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 245
483	6.245922000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 246
484	6.246011000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 247
485	6.246015000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 248
486	6.246018000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 249
487	6.246022000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 250
488	6.246026000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 251
489	6.246029000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 252
490	6.246032000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 253
491	6.246085000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 254
492	6.246086000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 255
493	6.246087000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 256
494	6.246088000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 257
495	6.246117000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 258
496	6.246125000	2001:3a0:e002:217:c811:d16c	2404:6800:4004:22::e	QUIC	104	CID: 5358696136016785233, Seq: 105
497	6.246126000	2001:3a0:e002:217:c811:d16c	2404:6800:4004:22::e	QUIC	104	CID: 5358696136016785233, Seq: 106
498	6.246172000	2404:6800:4004:22::e	2001:3a0:e002:217:c811:d16c	QUIC	1412	CID: 0, Seq: 259



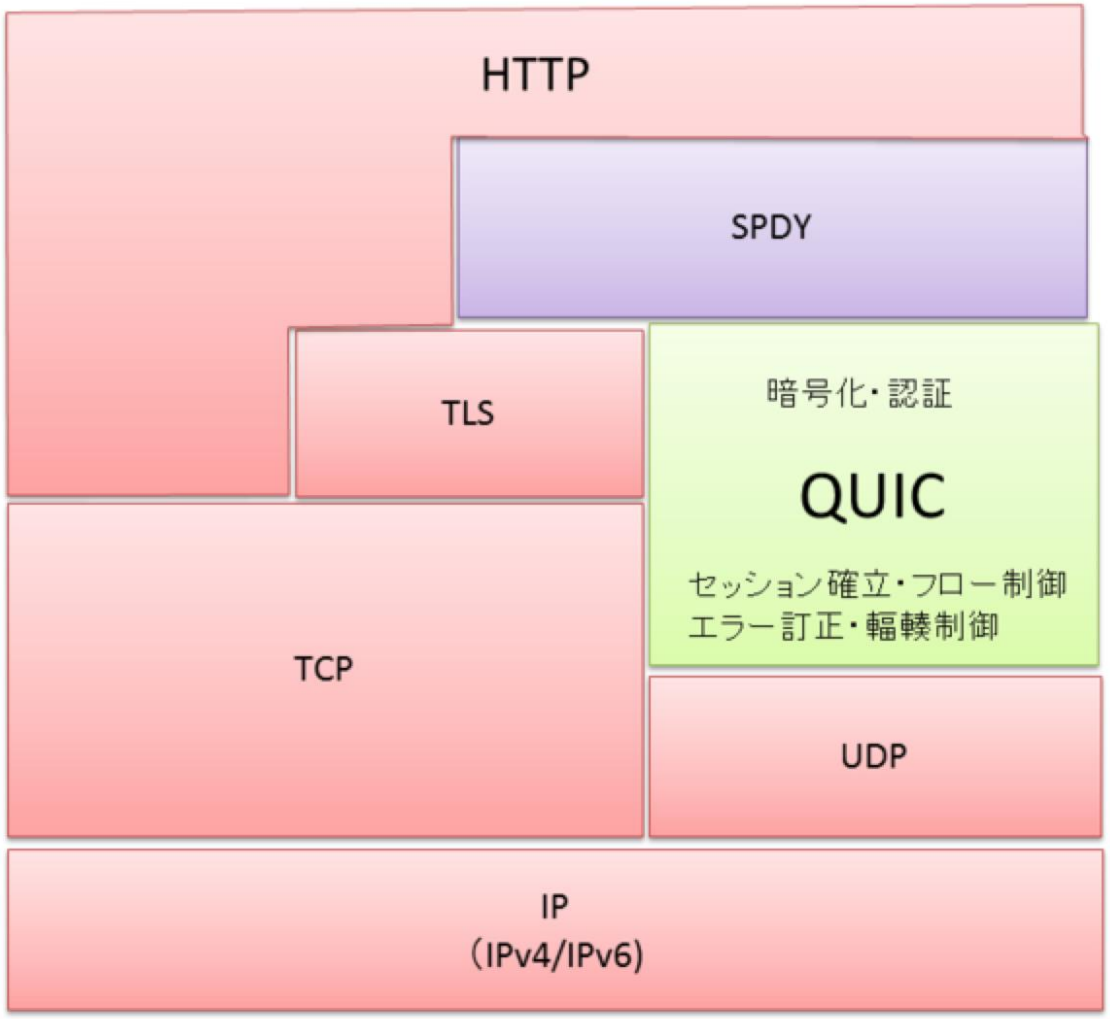

```
▷ Frame 385: 1412 bytes on wire (11296 bits), 1412 bytes captured (11296 bits) on interface 0
▷ Ethernet II, Src: Netscreen_ff:10:01 (00:10:db:ff:10:01), Dst: Apple_8b:55:15 (20:c9:d0:8b:55:15)
▷ Internet Protocol Version 6, Src: 2404:6800:4004:22::e (2404:6800:4004:22::e), Dst: 2001:3a0:e002:217:c811:d16c:16b0:d52f (2001:3a0:e002:217:c811:d16c:16b0:d52f)
▷ User Datagram Protocol, Src Port: 443 (443), Dst Port: 55774 (55774)
▽ QUIC (Quick UDP Internet Connections)
  ▽ Public Flags: 0x10
      .... ...0 = Version: No
      .... ..0. = Reset: No
      .... 00.. = CID Length: 0 Byte (0x00)
      ..01 .... = Sequence Length: 2 Bytes (0x01)
      00.. .... = Reserved: 0x00
    Sequence: 188
    Payload: 4b40397dc1c8cc41b45e187d69ee63c5d840cfe344ba1af3...
```

```
0000  20 c9 d0 8b 55 15 00 10  db ff 10 01 86 dd 60 00    ...U... ......`.
0010  00 00 05 4e 11 3d 24 04  68 00 40 04 00 22 00 00    ...N.=$. h.@.."..
0020  00 00 00 00 00 0e 20 01  03 a0 e0 02 02 17 c8 11    ...... . ........
0030  d1 6c 16 b0 d5 2f 01 bb  d9 de 05 4e 04 d5 10 bc    .l.../.. ...N....
0040  00 4b 40 39 7d c1 c8 cc  41 b4 5e 18 7d 69 ee 63    .K@9}... A.^.}i.c
0050  c5 d8 40 cf e3 44 ba 1a  f3 4f 79 42 7f 9b a3 18    ..@..D.. .OyB....
```

QUIC(UDP443)かつIPv6

QUIC：Quick UDP Internet Connection

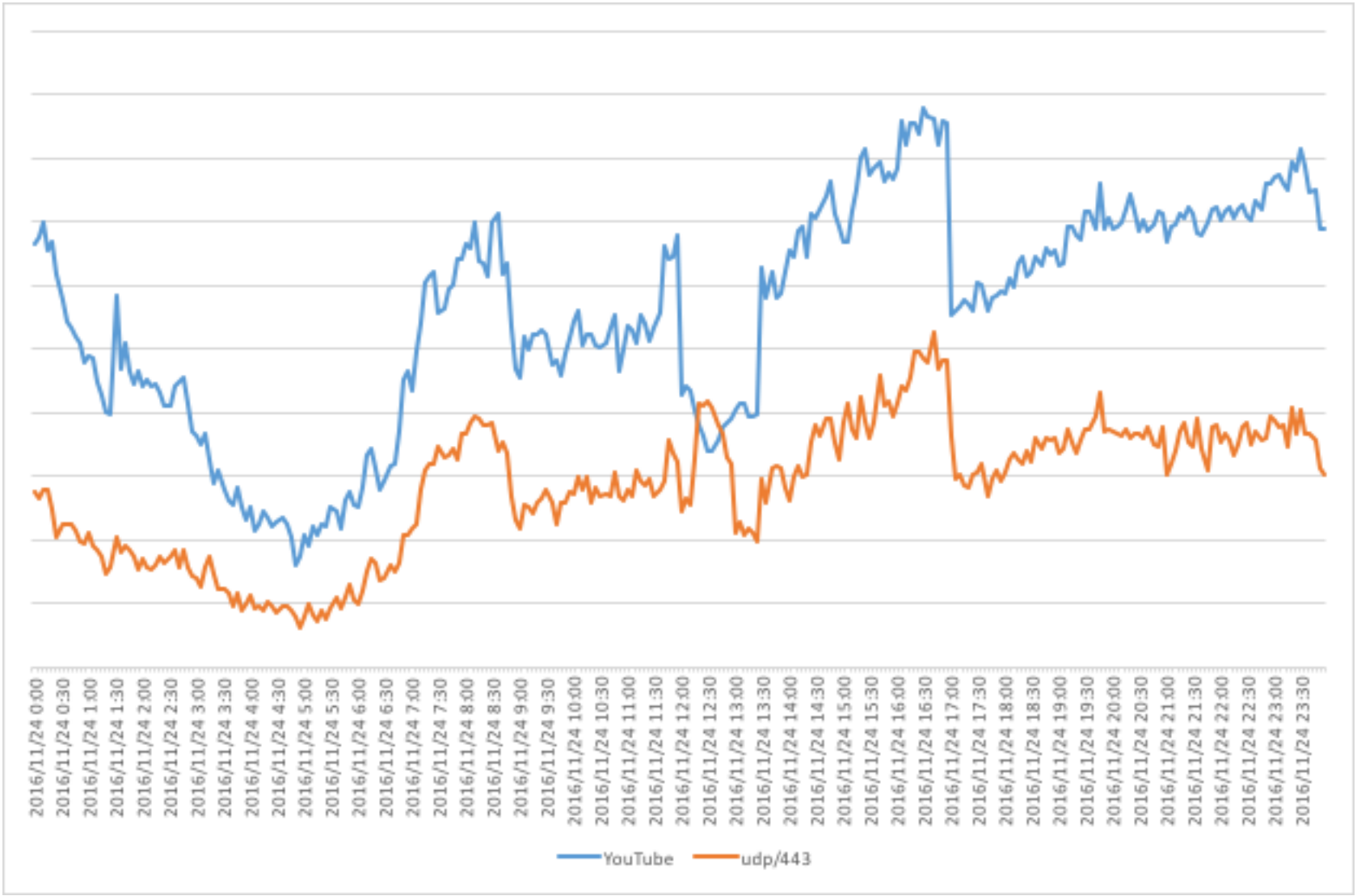
TCPのオーバーヘッドから解放され、UDPを用いて低遅延を実現



http://d.hatena.ne.jp/jovi0608/20130227/1361975933

某ISPでのトラフィック

- YouTubeの半分がQUICに

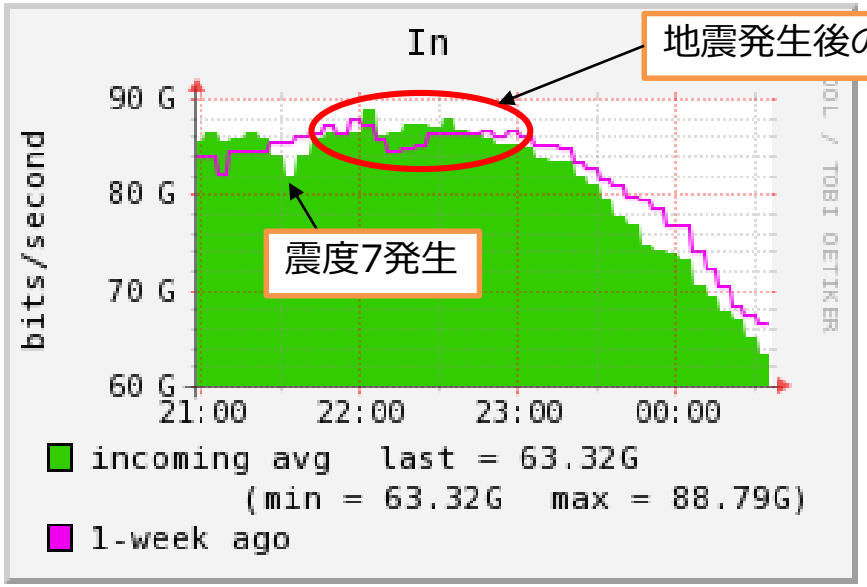


トラフィックの変化要因とトレンド

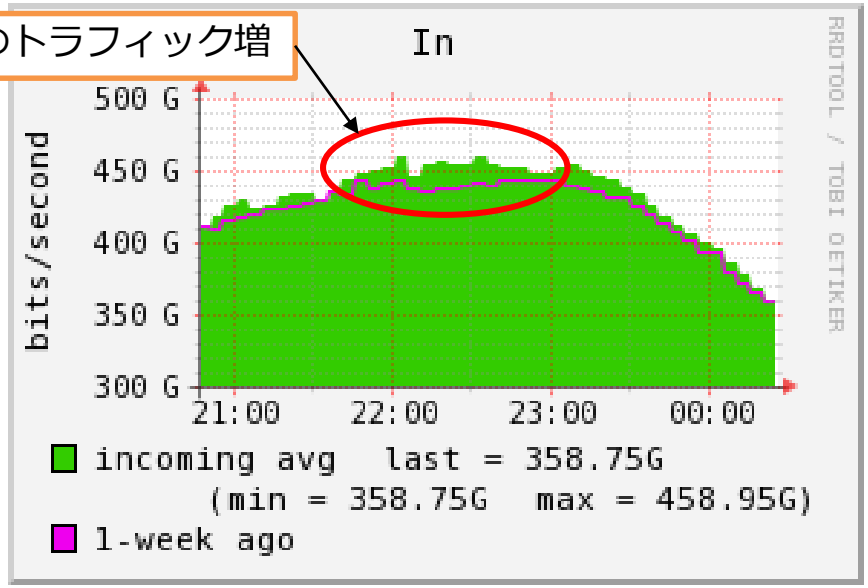
- イベントトラフィックによる変動
  - 自然災害
    - 福岡地震
  - ライブや中継・ネット配信
  - ソフトウェアアップデートやゲーム配信
    - IOS Windows update
    - 今年はPokémon GOが第一位？
- CDNやコンテンツ事業者からの流入トラフィック制御
  - 複数の対外接続からきまぐれに流入してくる問題
  - 最近自ASでのコントロールが非常に困難に
- 何が異常で何が正常かの見分けが困難に
  - 気にしない時代が到来？
  - 制御も含めてAIに任せる時代？

熊本地震発生時のトラフィック状況

- 2016年4月14日(木) 21時26分および
  2016年4月16日(土) 1時25分　に震度7の地震発生
  - 一部お客様に対して地震発生時のトラフィックに落ち込みが見られた反面、SNS等の利用に連動して該当時間にはトラフィックの増加も見られた



JPNAP大阪



JPNAP東京I

災害時の様々な施策

- LINEのline-out無料開放
  - http://bylines.news.yahoo.co.jp/ishinojunya/20160415-00056640/
  - 輻輳を助長しかねない、
    という意見もある
- 公衆Wi-Fi無料スポットの解放
  - 野良 “00000JAPAN”問題…

Rioオリンピック

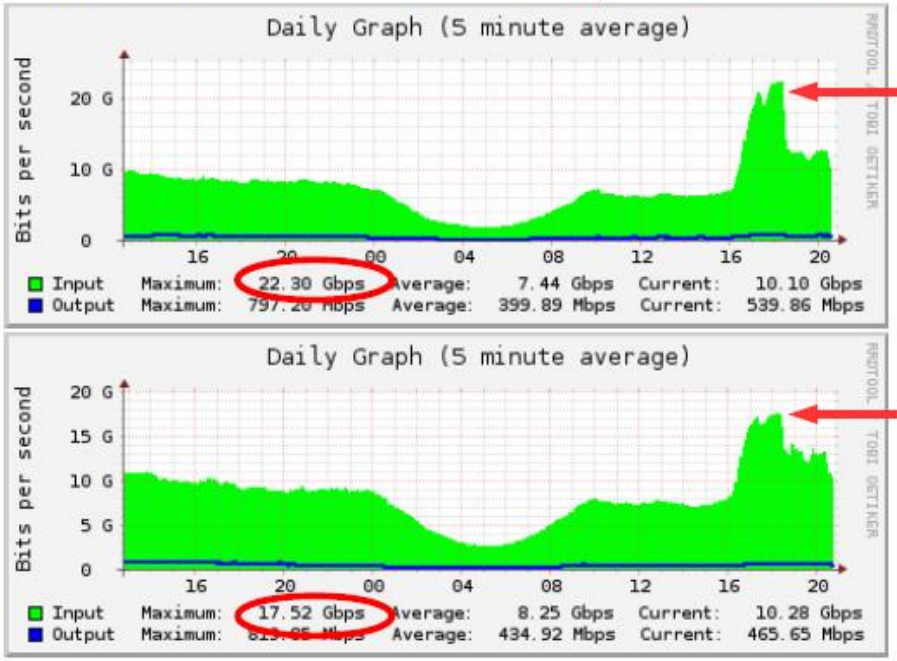
- Internetでの配信は成功裏に
  - 2014 FIFA Wcupの知見などを生かすなど
- ビジネスアワーにトラフィック増が観測
- 帰宅後は基本テレビ観戦
- Globo.com(AS28604)がブラジル内限定で配信

http://www.rcrwireless.com/20160729/americas/rio-olympics-technical-operations-center-tag5

国際親善試合

IX.br – Preview traffic - 2016 Olympic Games

Traffic of AS28604 in IX.br São Paulo and IX.br Rio de Janeiro - July 30th, 2016



22,30Gbps

17,52Gbps

AMISTOSOS AMISTOSO

BRASIL
Marquinhos, Gabriel

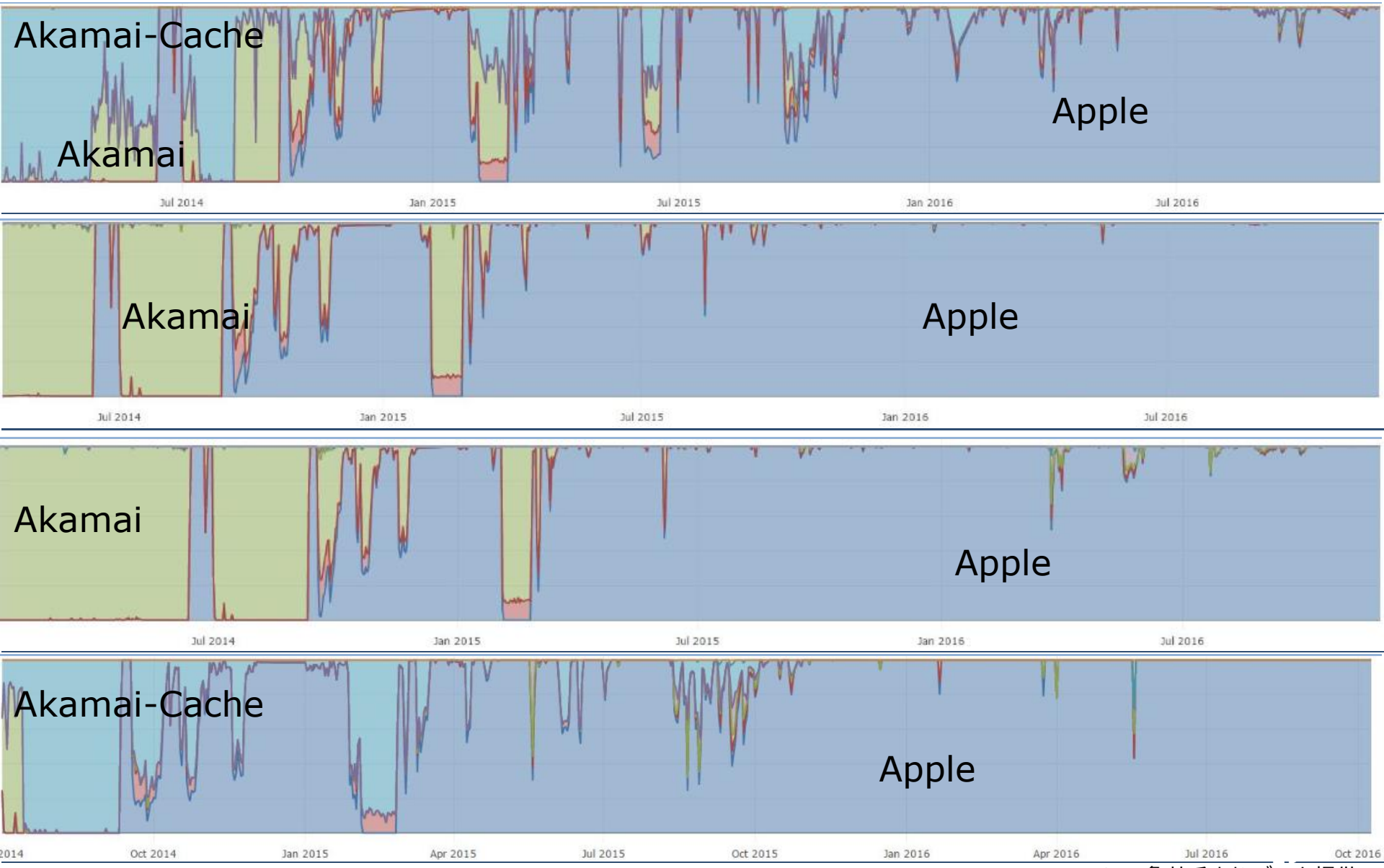
2 × 0

JAPÃO

出典：2016 LACNOG資料より

iOS{8,9,10}の各社向け配信状況

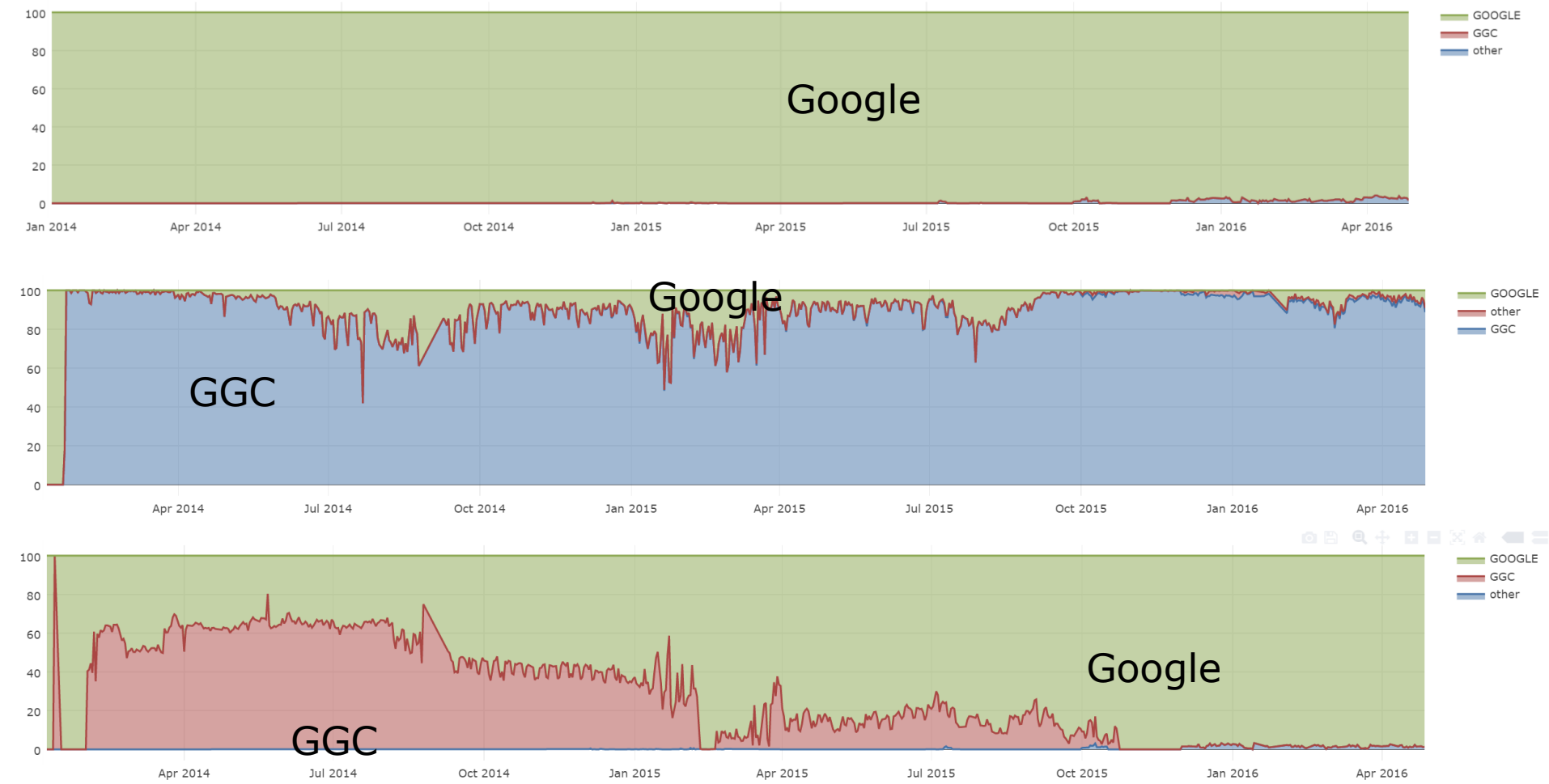
iOSのアップデート前後で大きくCDNに依存していたのが，ほぼAppleだけで配信可能



NTTCom亀井氏よりデータ提供

Google cache (GGC) の状況

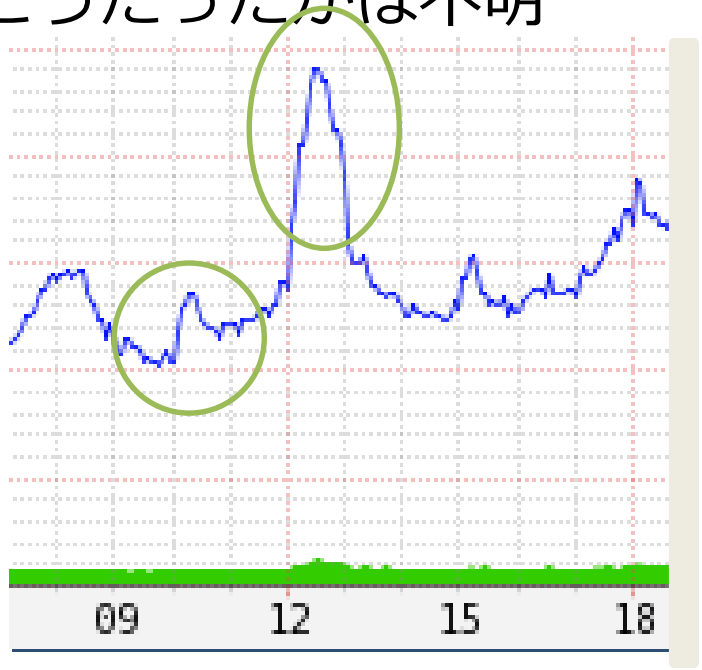
増大するトラフィックをさばくために、コスト削減のためGGCを導入するISPも多い
トラフィック制御権がGoogleに移るため、自身でのコントロールが効かず、外したISP



NTTCom亀井氏よりデータ提供

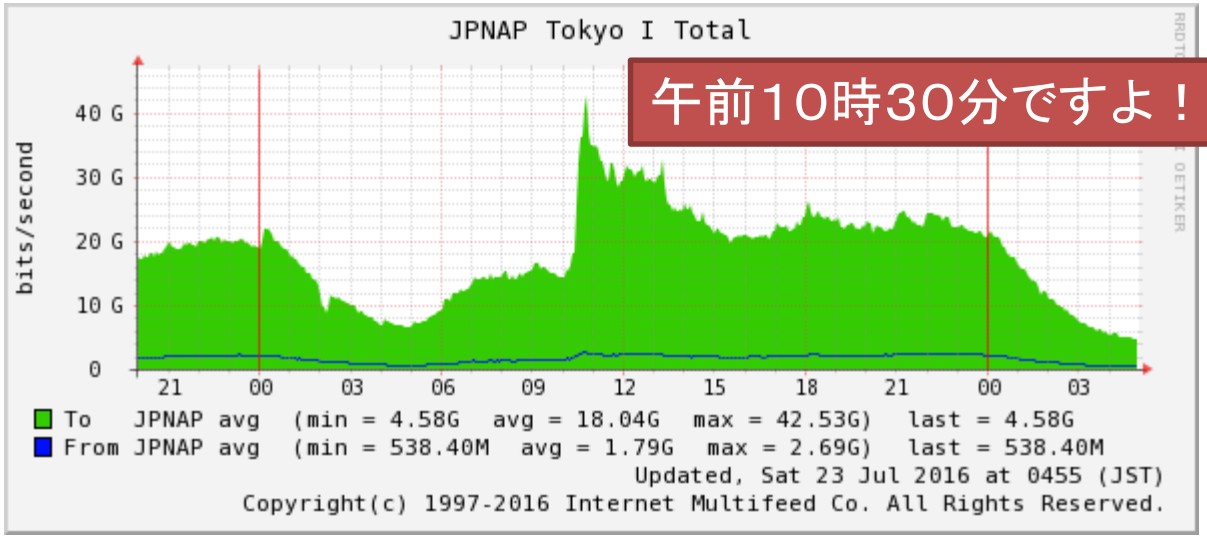
Pokémon GO リリース当日 7/22(金)

- スマホの通信量が昼時ピークに！
  - 過去にここまでの伸びは見たことがない
    - 夜の時間帯で一番大きな変化は、テレビドラマ「半沢直樹」
  - 日本全体がこうだったかは不明

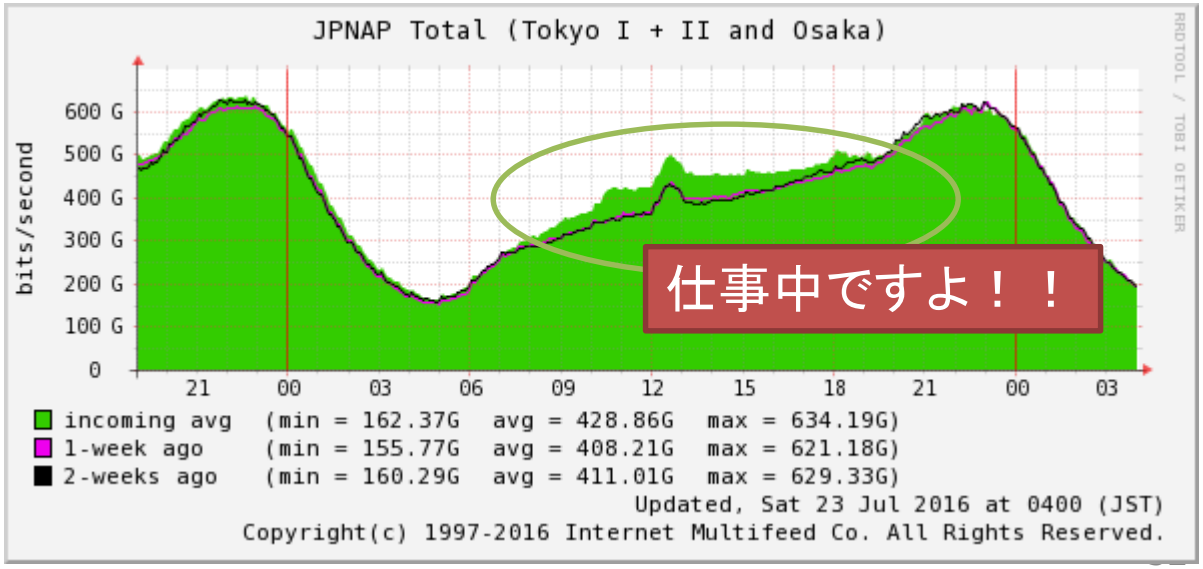


7/22(金)のインターネットトラフィック（一部）

アプリの
ダウンロード
トラフィック



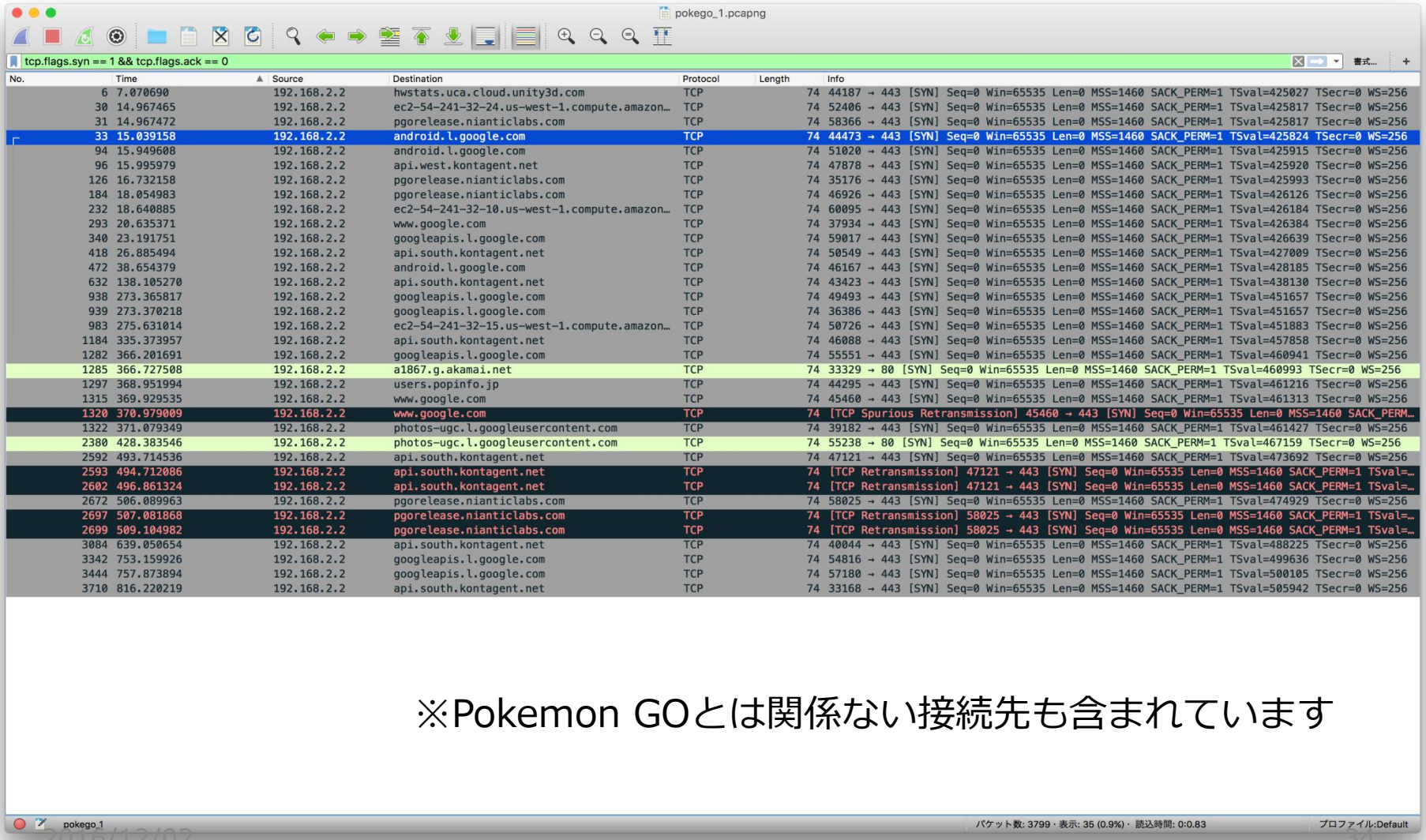
JPNAP全体の
トラフィック動向



Pokémon GO パケット解析

- 通信内容のサマリ
  - 全ての通信が443/SSL
  - セッションは貼り直さず、常時2~3セッションを使いまわしている
  - 定常通信は30秒ごとに実施
  - SSLのセッション確率とACKを除けばショートパケットは少なく、基本1514byteで通信
  - 1時間何もしないで、3MBぐらい

Pokémon GO パケット解析
syn==1 && ack ==0（約1時間）



※Pokemon GOとは関係ない接続先も含まれています

アプリケーションとNWの関係

- 特定のアプリケーションが通信や人の生活を大きく変える
- アプリケーションの作り次第でネットワークの使われ方やトラフィック傾向が簡単かつドラスティックに変わる
  - 通信量が多いアプリや、ダウンロードトラフィックの影響など
  - 震災時に娯楽サービスが重要通信に影響を与えることも起きえる？
- ここ最近アプリケーションがネットワークに与える影響が徐々に増してきている
  - アプリがネットワークを本気で使おうとしている

- アプリとネットワークの歩み寄りが必要な時期にきている
  - トラフィックコントロールはHyper Giantが中心
  - トラフィックの変動が激しく、NW側でのコントロールが出来ない状態
    - ISP側が意図したトラフィックコントロールができなくなってきている

内容

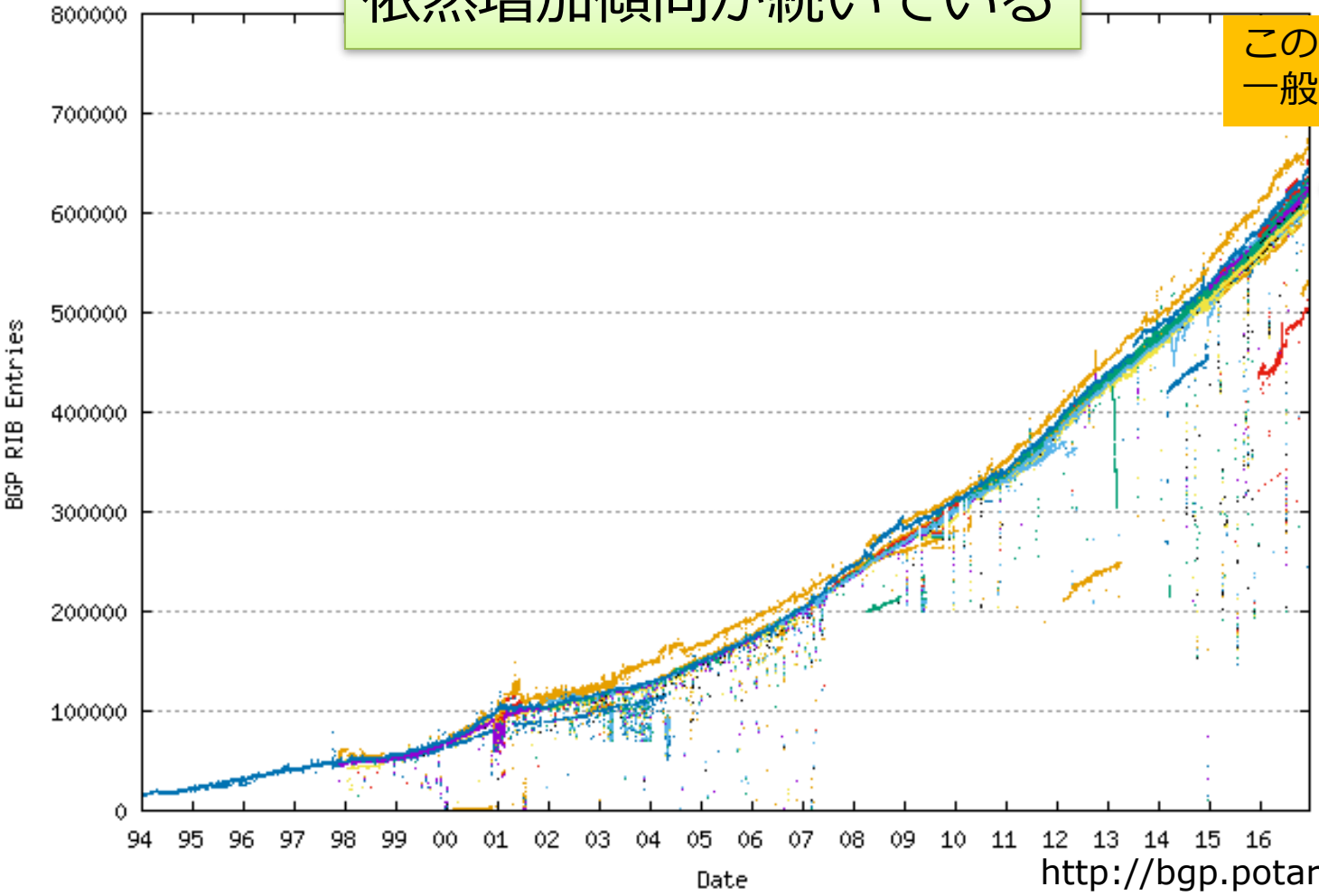
- トラフィック動向
- ルーティング動向
- DNS動向
- セキュリティ動向
- まとめ

ルーティング動向

- IPv4経路が**62~63万**に到達
  - 年増加率は**変わらず約1.1倍**で引き続き枯渇後も増加
    - 追加IPv4経路の申請と移転により継続的に増加している
  - **/24は依然全体の半分超**で、ここ最近ますます増加
  - **残るはLACNIC**地域の在庫枯渇が**2018年予想**
- IPv6経路は約3万2千経路に
  - **年間で約6000-7000経路の増加**
  - 急激な経路増によるルータのFIB容量等の制限に注意
    - **不慮の細かい経路のルートリーク**
    - /64までの経路を受信するポリシーだと影響を受けやすい
    - 64K等が上限がそろそろ気になる時期（IPv4は昨年512Kの壁）
- AS番号の枯渇対応 ⇒ 4byteASへの移行が促進
  - 世界的には普及しているが、日本での普及が低迷
    - ただ2015年と比較すると徐々に増加

IPv4経路数の推移

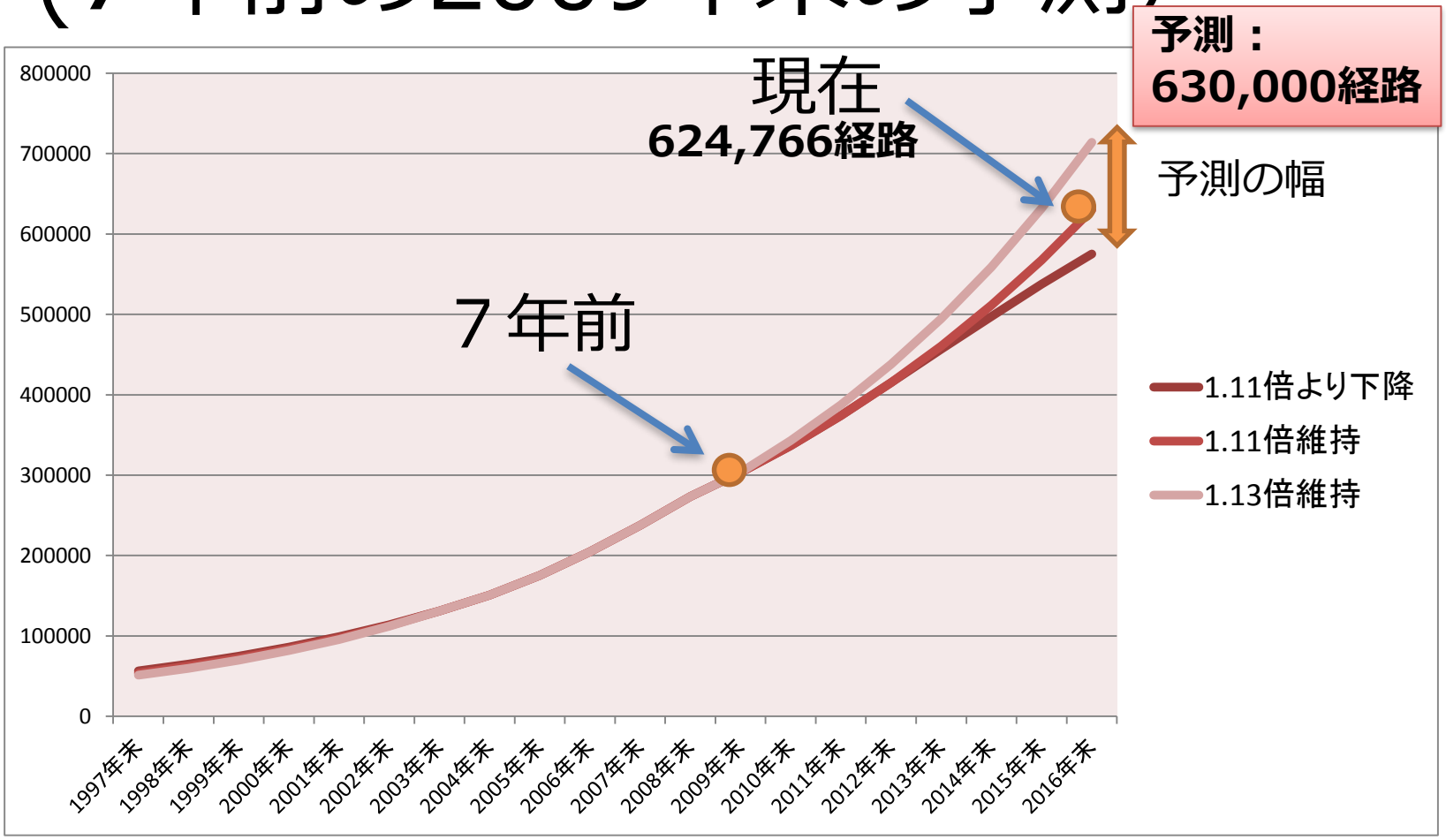
依然増加傾向が続いている



このあたりが
一般的な経路数

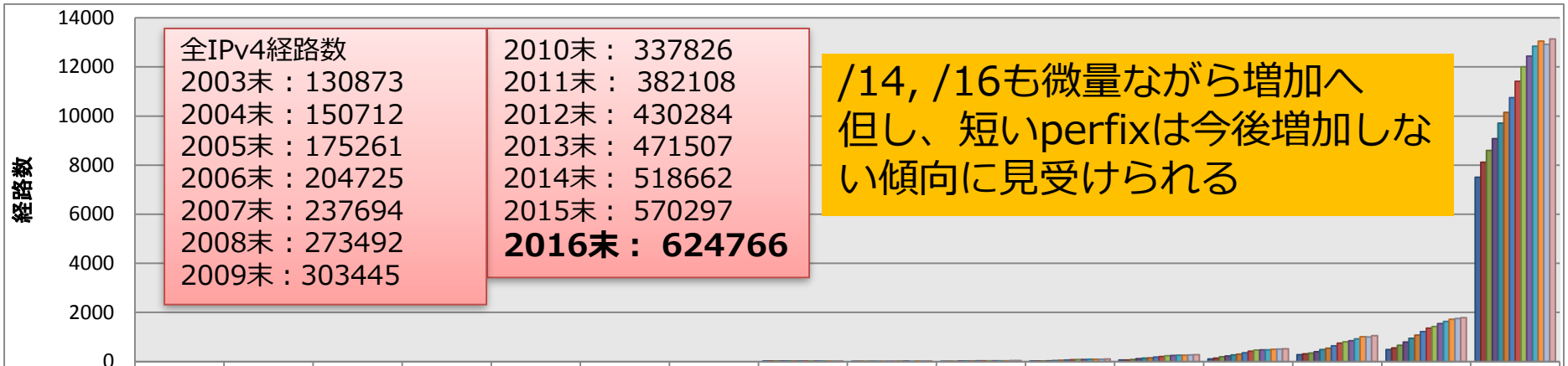
http://bgp.potaroo.net/

IPv4経路数推移予測1.0
(7年前の2009年末の予測)



IPv4アドレスの枯渇後も、依然IPv4アドレスの流通や細分化が進み経路数増加を牽引

IPv4経路数の推移



全IPv4経路数
2003末：130873
2004末：150712
2005末：175261
2006末：204725
2007末：237694
2008末：273492
2009末：303445

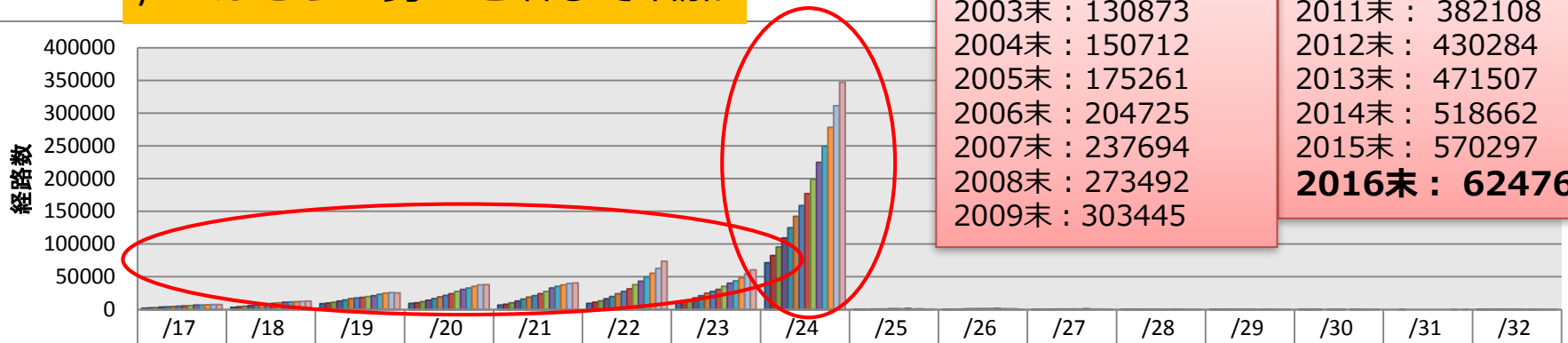
2010末： 337826
2011末： 382108
2012末： 430284
2013末： 471507
2014末： 518662
2015末： 570297
2016末： 624766

/14, /16も微量ながら増加へ
但し、短いperfixは今後増加しない傾向に見受けられる

	/1	/2	/3	/4	/5	/6	/7	/8	/9	/10	/11	/12	/13	/14	/15	/16
2003末	0	0	0	0	0	0	0	19	4	6	14	57	100	277	483	7506
2004末	0	0	0	0	0	0	0	19	3	7	15	61	138	314	553	8113
2005末	0	0	0	0	0	0	0	18	5	8	17	81	187	340	666	8597
2006末	0	0	0	0	0	0	0	19	10	13	30	111	222	397	794	9077
2007末	0	0	0	0	0	0	0	18	9	16	39	136	271	485	948	9715
2008末	0	0	0	0	0	0	0	18	9	18	46	152	301	541	1072	10153
2009末	0	0	0	0	0	0	0	20	10	25	65	177	361	641	1220	10747
2010末	0	0	0	0	0	0	0	19	10	25	69	207	423	748	1355	11409
2011末	0	0	0	0	0	0	0	19	12	27	81	236	465	808	1423	12008
2012末	0	0	0	0	0	0	0	18	14	29	88	243	478	850	1547	12442
2013末	0	0	0	0	0	0	0	16	11	31	92	254	474	923	1628	12842
2014末	0	0	0	0	0	0	0	16	12	31	90	262	501	1011	1715	13046
2015末	0	0	0	0	0	0	0	17	13	36	97	263	506	1002	1755	12925
2016末	0	0	0	0	0	0	0	16	13	36	102	274	521	1050	1784	13142

IPv4経路数の推移

/24はさらに勢いを増して増加

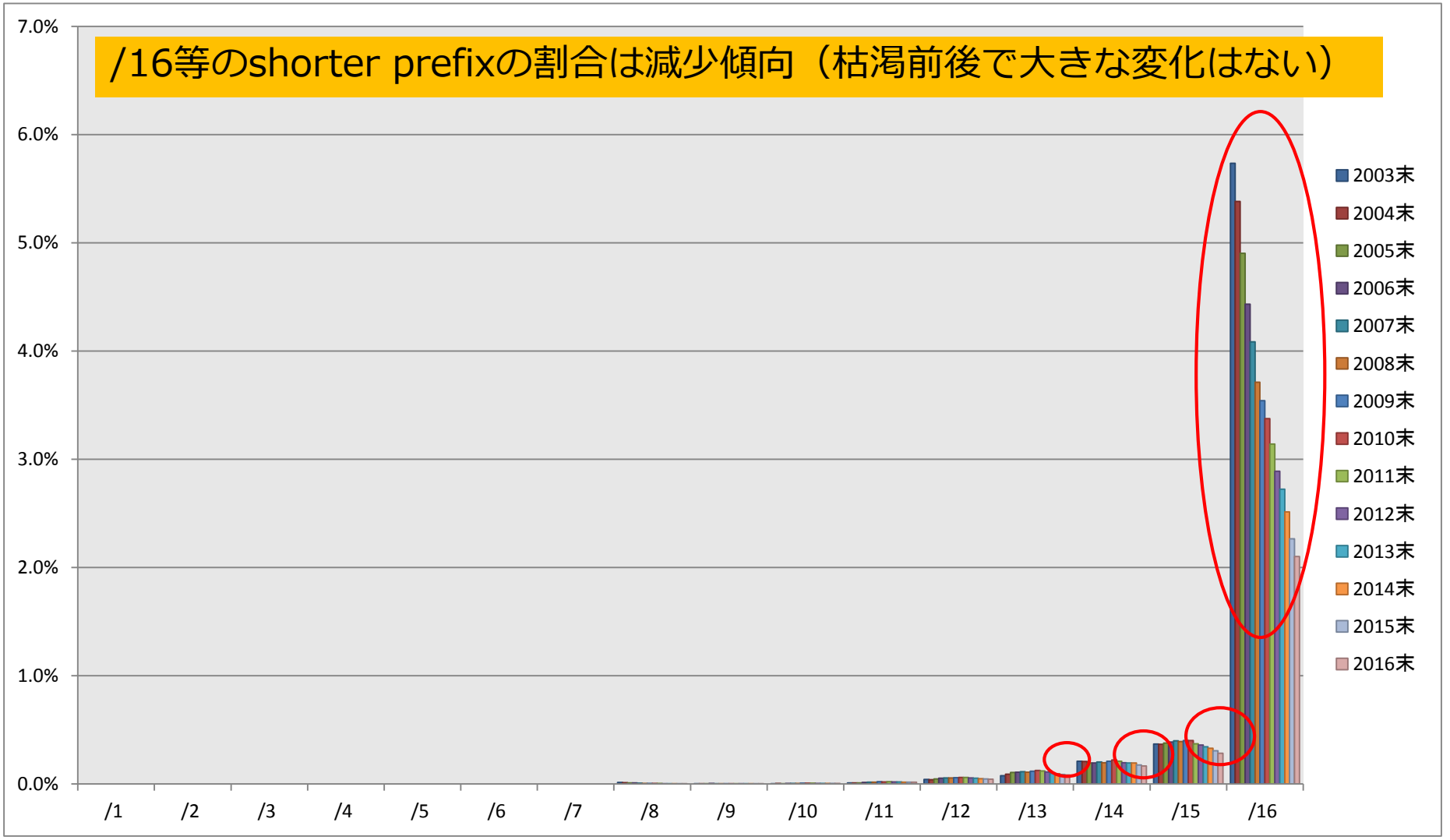


全IPv4経路数
2003末：130873
2004末：150712
2005末：175261
2006末：204725
2007末：237694
2008末：273492
2009末：303445

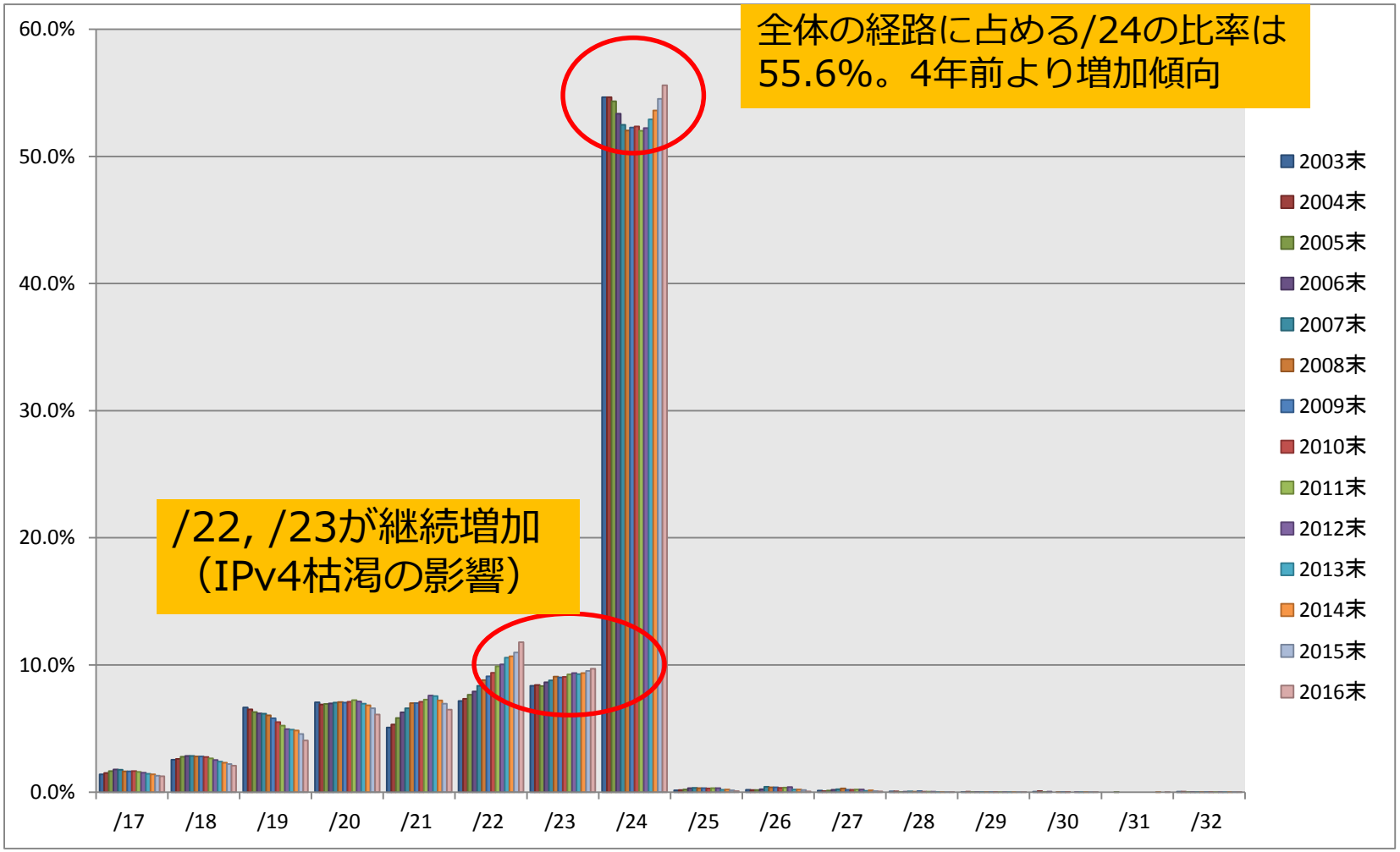
2010末： 337826
2011末： 382108
2012末： 430284
2013末： 471507
2014末： 518662
2015末： 570297
2016末： 624766

	/17	/18	/19	/20	/21	/22	/23	/24	/25	/26	/27	/28	/29	/30	/31	/32
2003末	1829	3334	8716	9249	6656	9386	10943	71541	182	233	156	70	21	50	0	41
2004末	2270	3933	9818	10402	8007	11066	12707	82382	252	239	130	69	54	120	0	40
2005末	2880	4871	11026	12142	10194	13440	14626	95225	345	292	194	26	12	36	3	30
2006末	3625	5826	12664	14281	12838	16203	17682	109219	658	468	364	69	44	80	0	31
2007末	4192	6767	14670	16753	15656	19873	20885	124763	814	1013	544	114	5	0	0	8
2008末	4444	7678	16540	19394	19123	24098	24829	142338	831	1000	798	92	9	1	0	7
2009末	4977	8507	17591	21348	21260	27614	27395	158588	955	1128	565	224	11	8	0	8
2010末	5584	9343	18618	23987	24029	31706	30591	176852	992	1102	585	151	12	2	0	7
2011末	6065	10115	19979	27645	27788	37839	35374	198775	1148	1364	762	166	4	0	0	5
2012末	6533	10880	21269	30693	32699	43237	40249	224766	1356	1689	903	181	79	17	0	24
2013末	6761	11348	23134	32798	35561	49863	43778	249471	880	1002	477	50	79	20	0	14
2014末	7209	11942	25102	35370	37390	55368	48597	278052	1107	1065	717	15	19	11	1	13
2015末	7409	12558	26070	37594	39698	62668	54398	311000	805	937	485	16	15	9	0	21
2016末	7812	13008	25385	38165	40565	73601	60659	347337	466	373	311	62	39	12	1	32

IPv4経路数の推移（割合）



IPv4経路数の推移（割合）

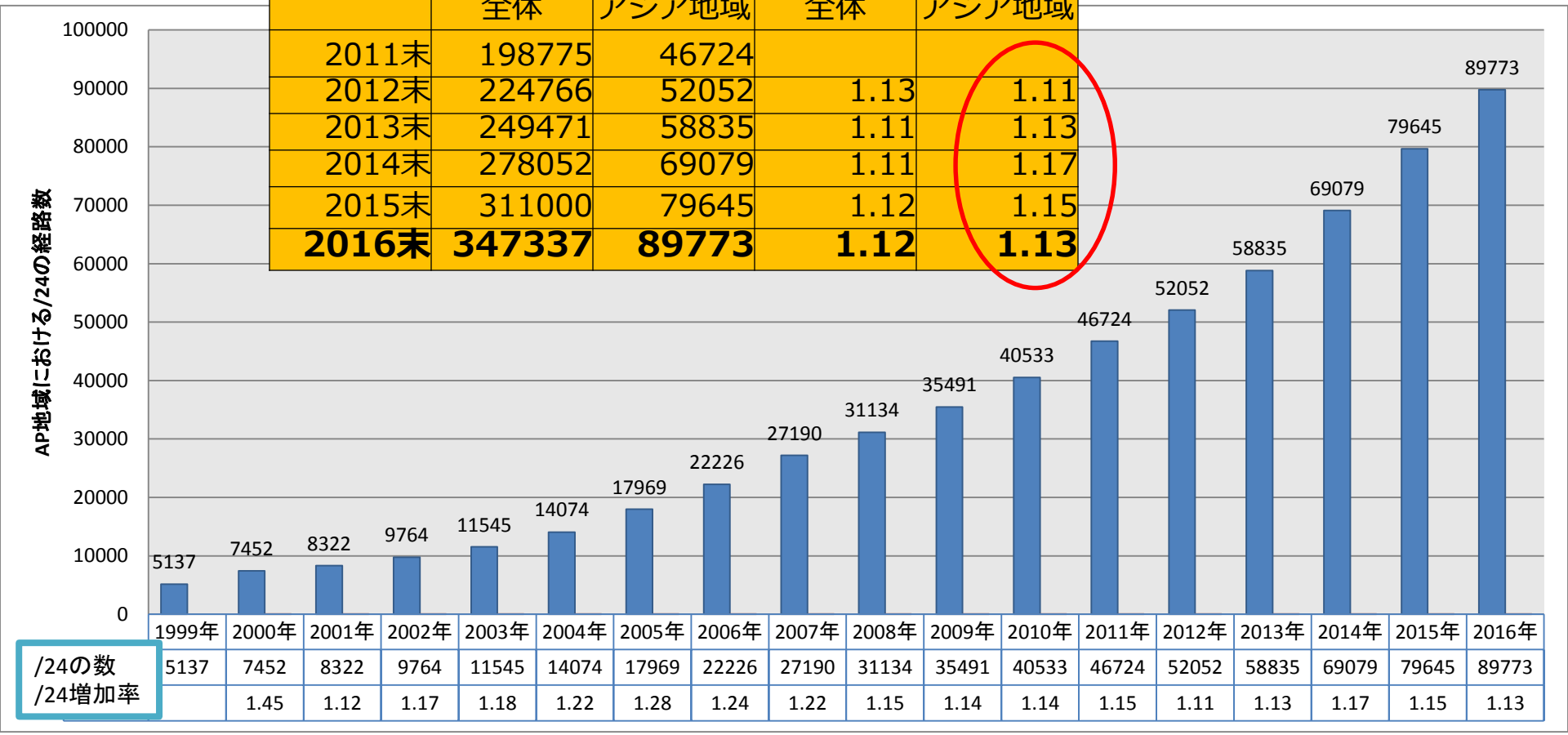


AP地域の/24の推移

AP地域の/24増加率が世界全体に比べて多い

注：移転も含まれるため誤差あり　（統計情報が/8単位では取得できない）

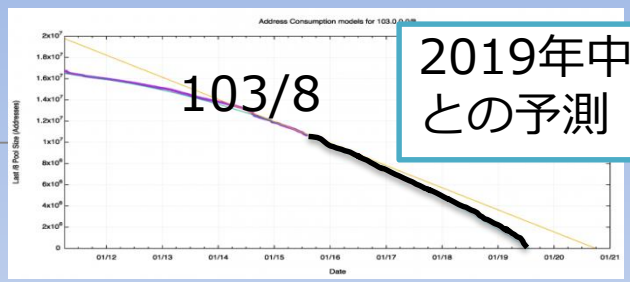
	/24の数		/24増加率	
	全体	アジア地域	全体	アジア地域
2011末	198775	46724		
2012末	224766	52052	1.13	1.11
2013末	249471	58835	1.11	1.13
2014末	278052	69079	1.11	1.17
2015末	311000	79645	1.12	1.15
2016末	**347337**	**89773**	**1.12**	**1.13**



	1999年	2000年	2001年	2002年	2003年	2004年	2005年	2006年	2007年	2008年	2009年	2010年	2011年	2012年	2013年	2014年	2015年	2016年
/24の数	5137	7452	8322	9764	11545	14074	17969	22226	27190	31134	35491	40533	46724	52052	58835	69079	79645	89773
/24増加率		1.45	1.12	1.17	1.18	1.22	1.28	1.24	1.22	1.15	1.14	1.14	1.15	1.11	1.13	1.17	1.15	1.13

AP地域の/24の推移

103/8(final /8)の伸びが著しい
202,203 を余裕で追い越す。全般的に
依然経路は日々細切れになっている状況



2019年中には枯渇しそう
との予測（APNIC: Geoff Huston）

14000
12000
10000
8000
6000
4000
2000
0

1999年 2000年 2001年 2002年 2003年 2004年 2005年 2006年 2007年 2008年 2009年 2010年 2011年 2012年 2013年 2014年 2015年 2016年

202/8 203/8
210/8 211/8
061/8 218/8
219/8 220/8
221/8 222/8
060/8 058/8
059/8 124/8
125/8 126/8
121/8 122/8
123/8 114/8
115/8 116/8
117/8 118/8
119/8 120/8
112/8 113/8
110/8 111/8
180/8 183/8
175/8 182/8
001/8 027/8
014/8 223/8
049/8 101/8
036/8 042/8
039/8 106/8
103/8

APNIC公認？のブローカー

Registered IPv4 brokers

Like Share 0 Tweet 0

昔に登録されたブローカーは事業を継続

Organization	Economy	Contact	Phone	Skype
IPTrading.com	US	Michael Burns	+1 855-478-7233	
IPv4 Market Group LLC	US	Sandra Brown	+1 855-880-5906	
The Kalorama Group	US	Louis Sterchi	+1 202-425-2118	louissterchi
Hilco Streambank	US	Jack Hazan	+1 212-610-5663	
V4ESCROW, LLC	US	Elvis Daniel Velea	+1 702-475-5914	elvisvelea
v4Now	AU	Skeeve Stevens	+61-2-8014-7398	
IPv4 Xchange, LLC	US	Mickey Mullins	+1-718-764-6775	
Avenue4 LLC	US	Marc Lindsey	+1-202-741-9521	
Maxtel Holdings, LLC	US	M Feras Bakkour	+1-323-870-4858	

2013年に追加

2014年に追加

2015年に追加
→削除

2016年に追加

https://www.apnic.net/manage-ip/manage-resources/transfer-resources/transfer-facilitators

APNIC事前承認済みのrequest（抜粋）

IPv4アドレスを買いたい人リスト。2016年11月時点の状況
　特に香港、シンガポール、パキスタンから多量のIPv4アドレス申請

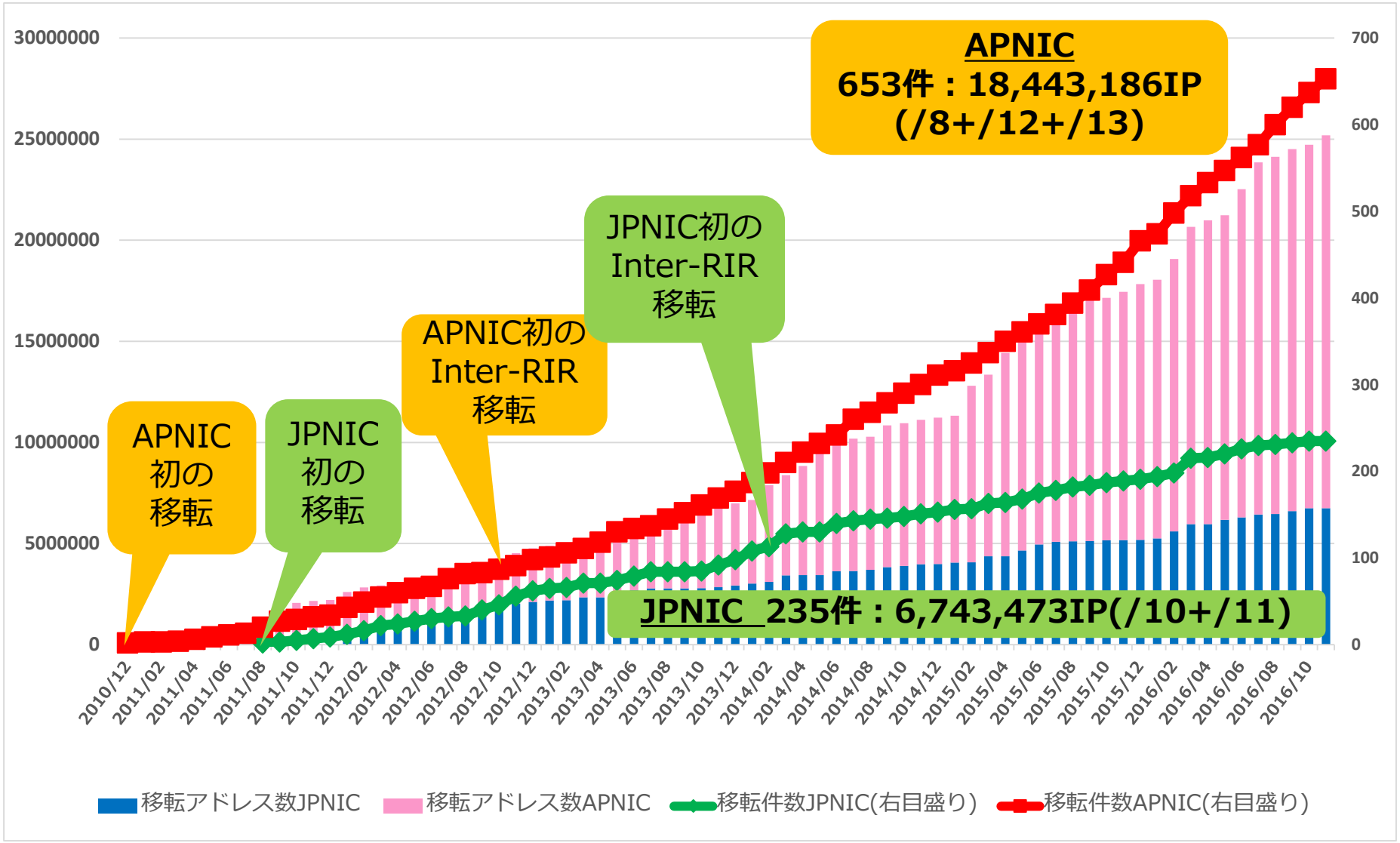
72	/11+/12+/14	SG	15 Dec 2017	Contact
78	/14	SG	8 Jan 2018	Contact
94	/14	HK	12 Aug 2018	Contact
95	/16	HK	16 Aug 2018	Contact
96	/14	PK	6 Sep 2018	Contact
99	/15	PK	27 Oct 2018	Contact

https://www.apnic.net/services/become-a-member/manage-your-membership/pre-approval/listing

日本のIPv4アドレス移転状況

- 2016年11月現在235件(去年+38)
  - 申請件数の伸びは鈍化しているが、大きなサイズは国際移転で
- 国際移転も33件（去年+20）
  - 他レジストリ→JPNIC：28件
  - JPNIC→他レジストリ：5件
- 移転の理由
  - 純粋にIPv4アドレスが不足しているケースが断然多い
  - 事業者間での整理
    - グループ企業間でやり取り
    - 上位ISPからの割り当てブロックをそのまま下位事業者へ移譲
- 移転履歴
  - https://www.nic.ad.jp/ja/ip/ipv4transfer-log.html
- JPNICによるlisting serviceが2015年12月開始
  - 現在4件中3件掲載
  - https://www.nic.ad.jp/ja/ip/transfer/wishlist.html
- AS番号の移転4件（去年+3）

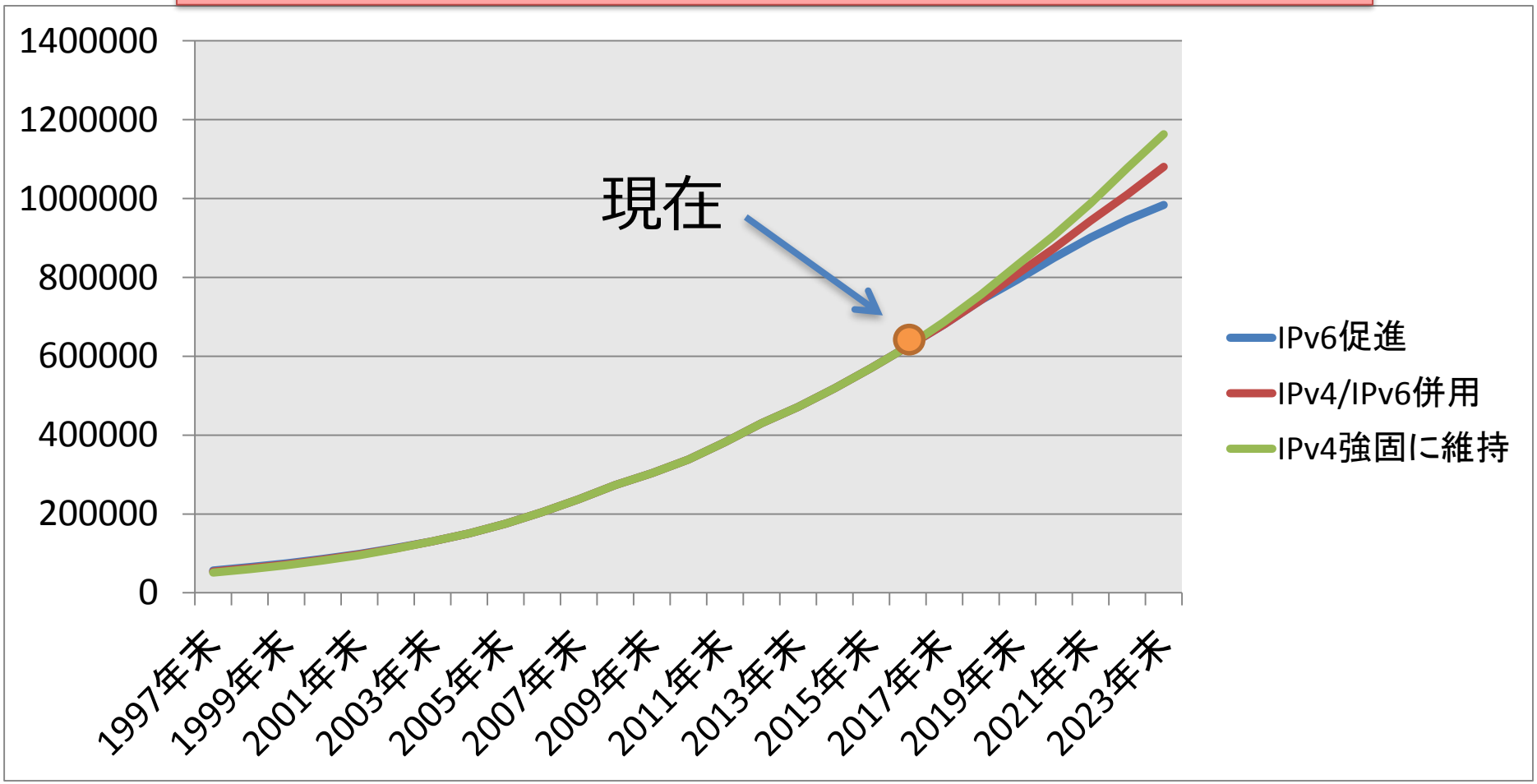
APNIC地域と日本の移転状況比較



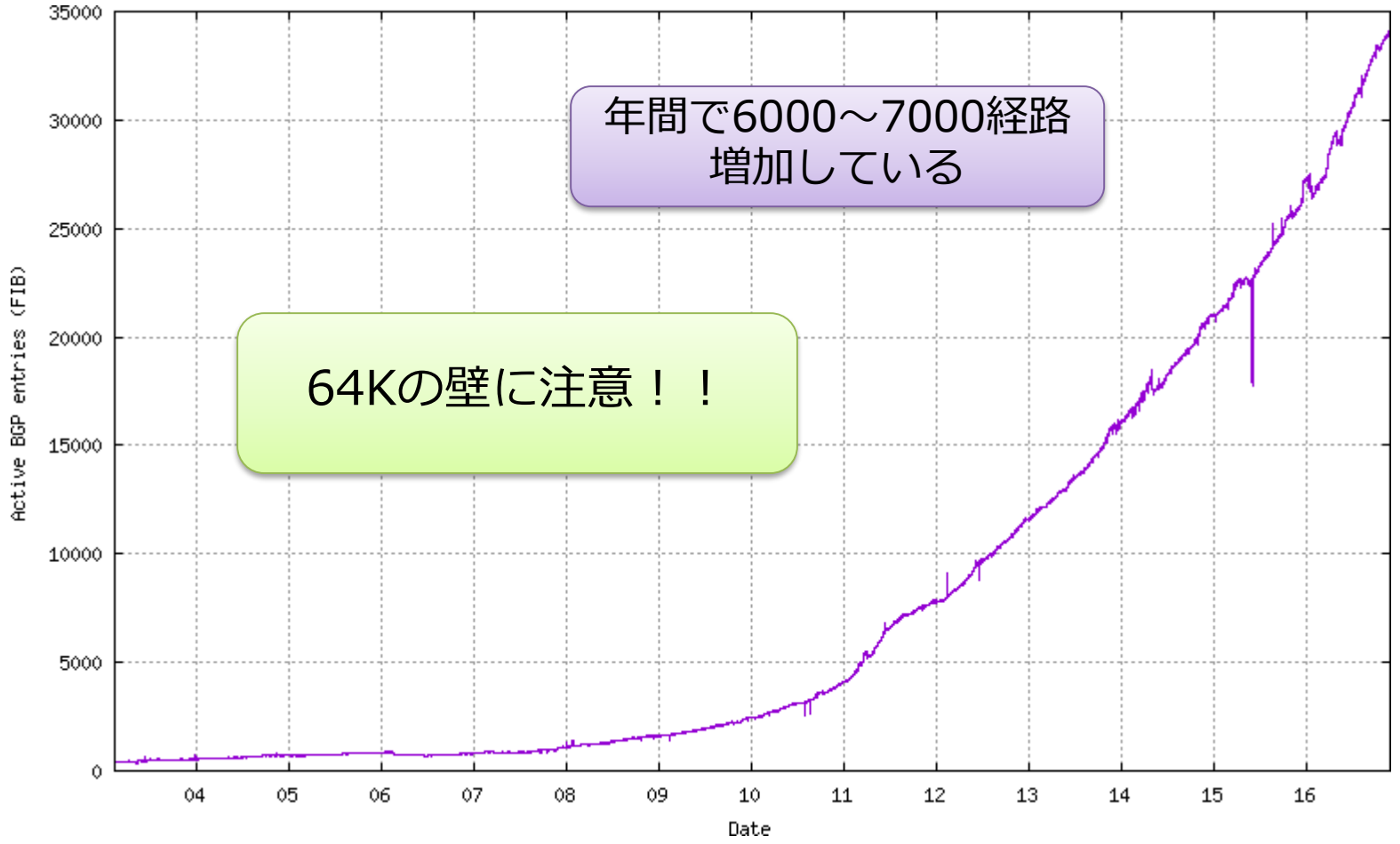
出典：JPNIC川端氏作

IPv4経路数推移予測2.0

コミュニティやTier1等での何らかのポリシー変更が無い限り、何れかの段階で100万経路(RIB)には到達する予測

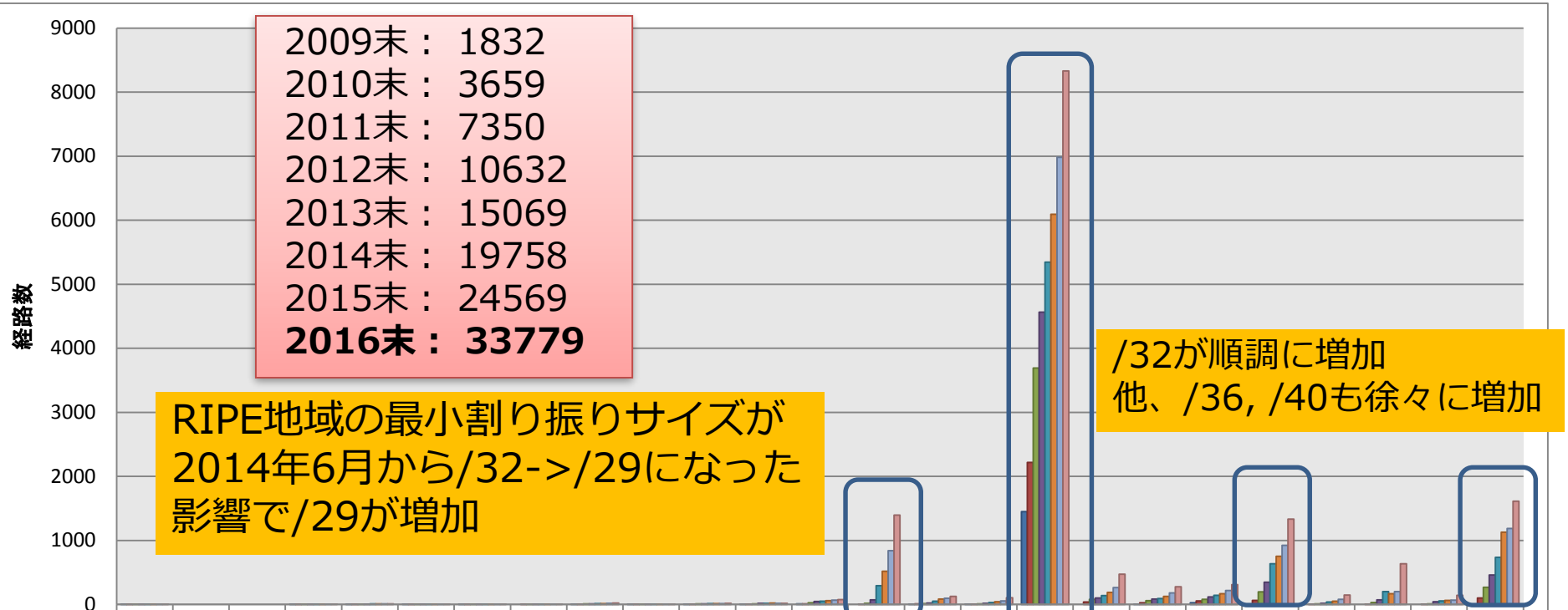


最近のIPv6経路増には要注意



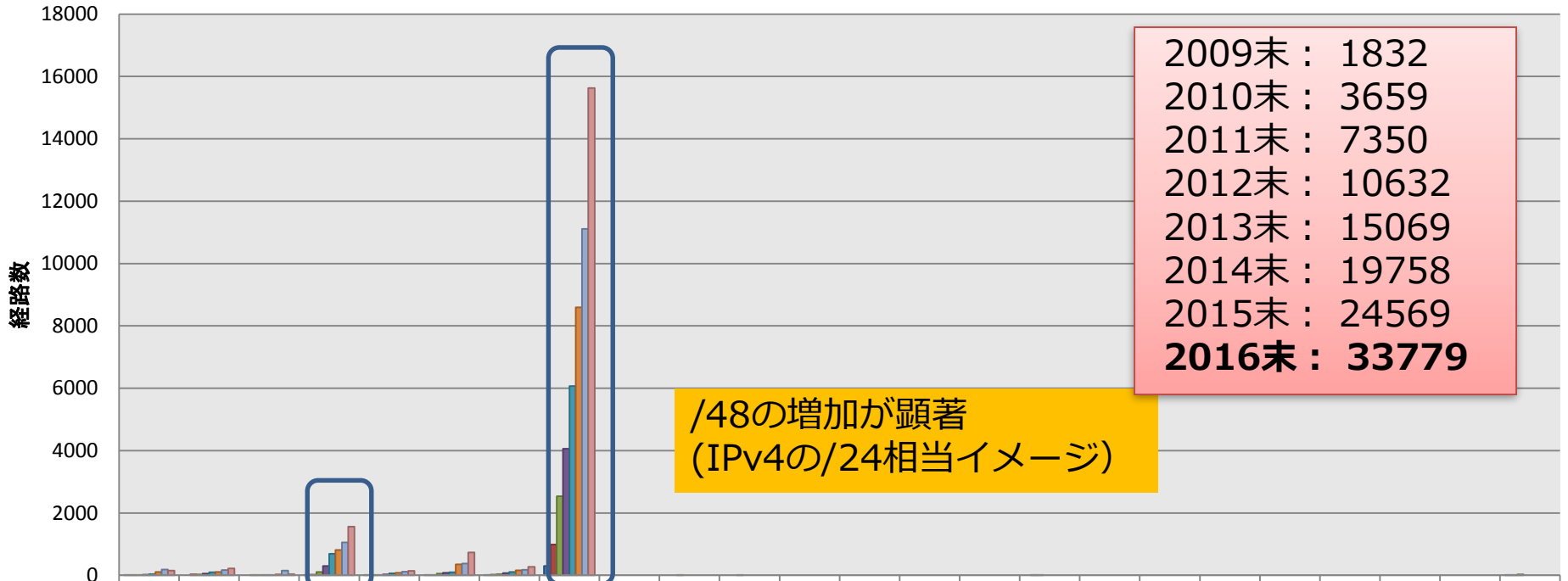
異常状態（例えば、細かい経路が急増したとか）への対処も重要

IPv6経路数の推移



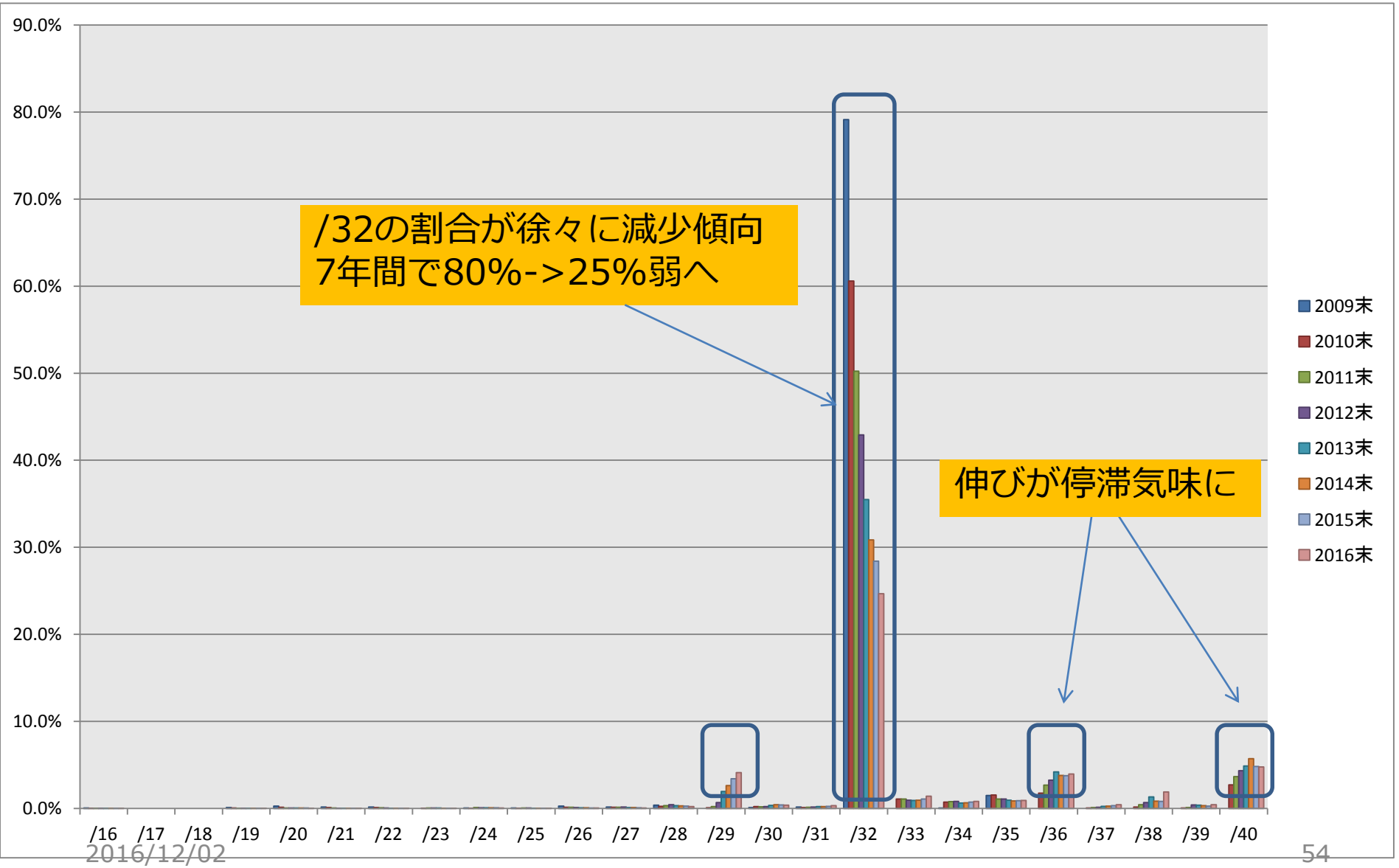
	/16	/17	/18	/19	/20	/21	/22	/23	/24	/25	/26	/27	/28	/29	/30	/31	/32	/33	/34	/35	/36	/37	/38	/39	/40
2009末	1	0	0	2	5	3	3	0	1	1	5	3	7	0	2	3	1450	0	1	27	0	0	0	0	0
2010末	1	0	0	2	5	4	4	1	1	1	5	5	9	3	8	4	2217	39	27	56	64	2	6	2	99
2011末	1	0	0	2	4	3	5	4	7	4	9	9	24	16	14	10	3692	80	57	79	197	7	31	7	268
2012末	1	0	0	2	6	3	5	6	9	4	10	16	46	71	21	18	4564	101	85	115	345	15	71	42	460
2013末	1	0	0	2	7	3	5	6	11	4	11	17	50	294	52	31	5345	137	94	143	633	37	199	56	736
2014末	1	0	0	2	7	3	4	4	14	5	14	20	60	516	84	41	6093	186	125	168	751	51	166	62	1127
2015末	1	0	0	2	9	3	4	4	18	5	14	16	68	840	98	56	6981	263	181	217	923	80	201	68	1187
2016末	1	0	0	2	9	3	4	4	19	5	15	16	75	1394	124	105	8330	471	276	311	1334	146	636	140	1613

IPv6経路数の推移

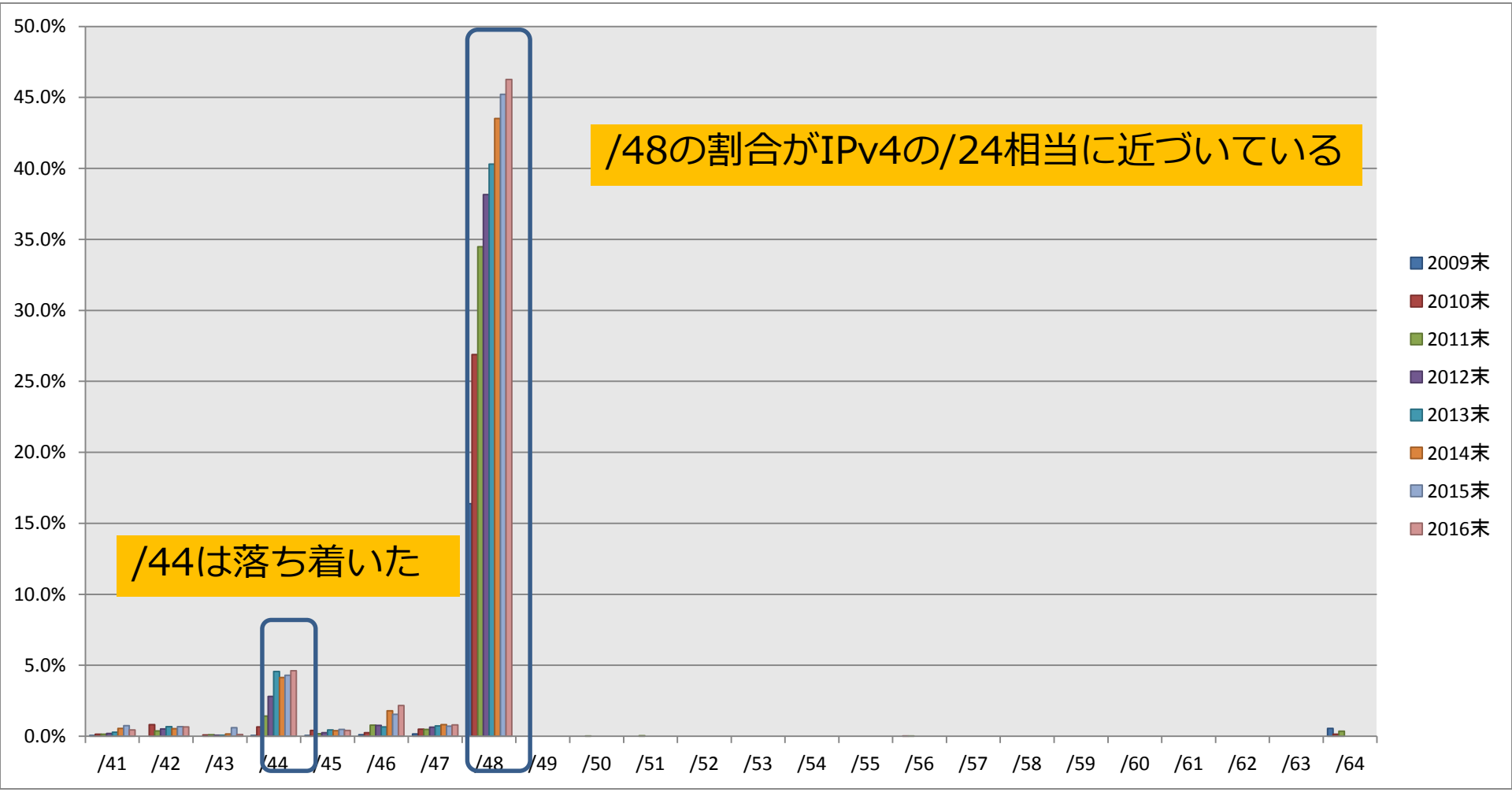


	/41	/42	/43	/44	/45	/46	/47	/48	/49	/50	/51	/52	/53	/54	/55	/56	/57	/58	/59	/60	/61	/62	/63	/64
2009末	1	0	0	1	1	2	3	300	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10
2010末	5	30	3	24	15	9	18	984	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	5
2011末	10	27	8	104	13	57	36	2534	0	1	3	0	0	0	0	1	0	0	0	0	0	0	0	26
2012末	21	55	8	298	27	81	69	4057	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2013末	42	102	10	688	68	100	109	6072	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2014末	108	106	31	817	79	356	160	8597	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2015末	183	166	148	1054	116	378	175	11110	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2016末	148	223	41	1560	139	734	273	15628	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

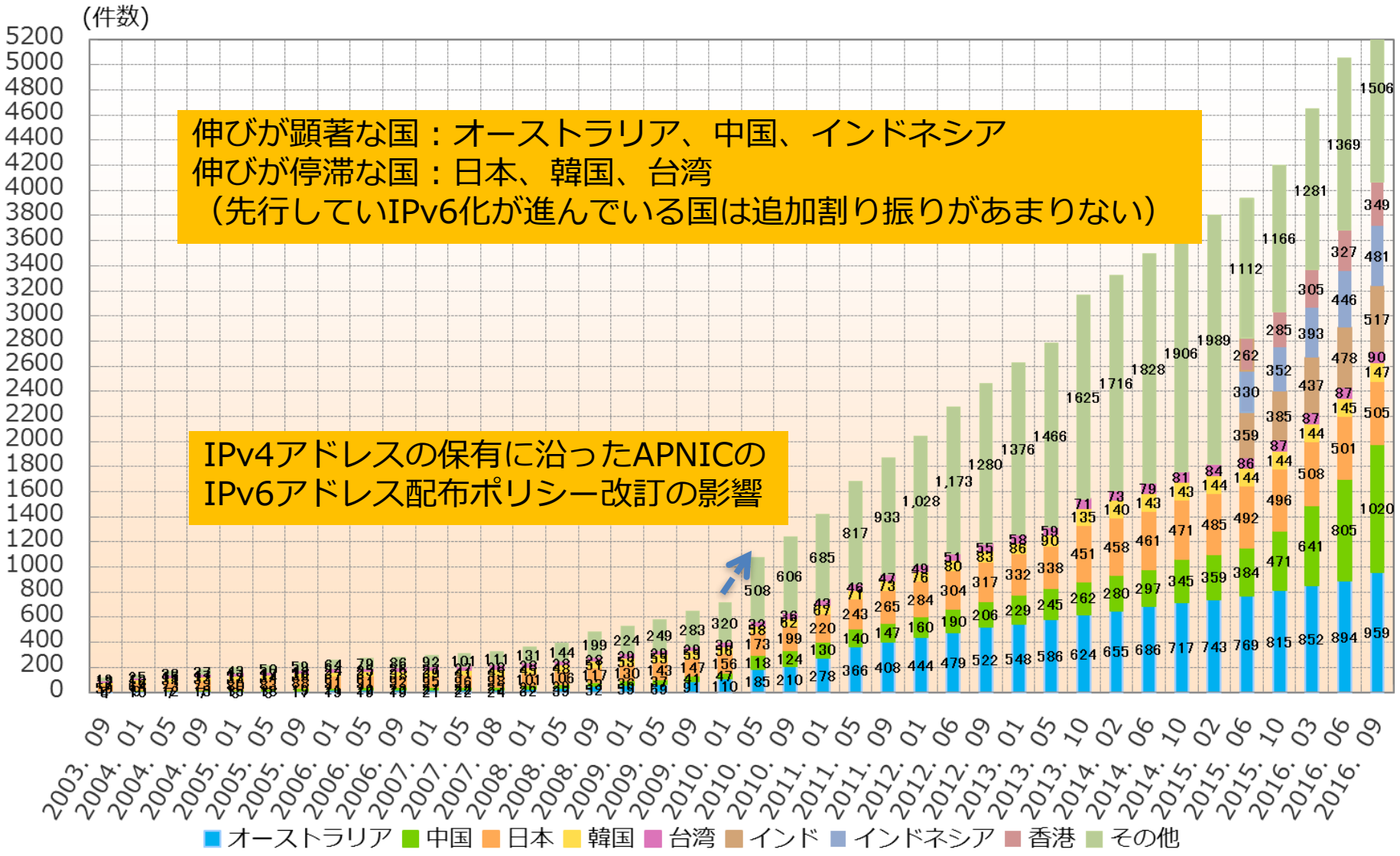
IPv6経路数の推移（割合）



IPv6経路数の推移（割合）

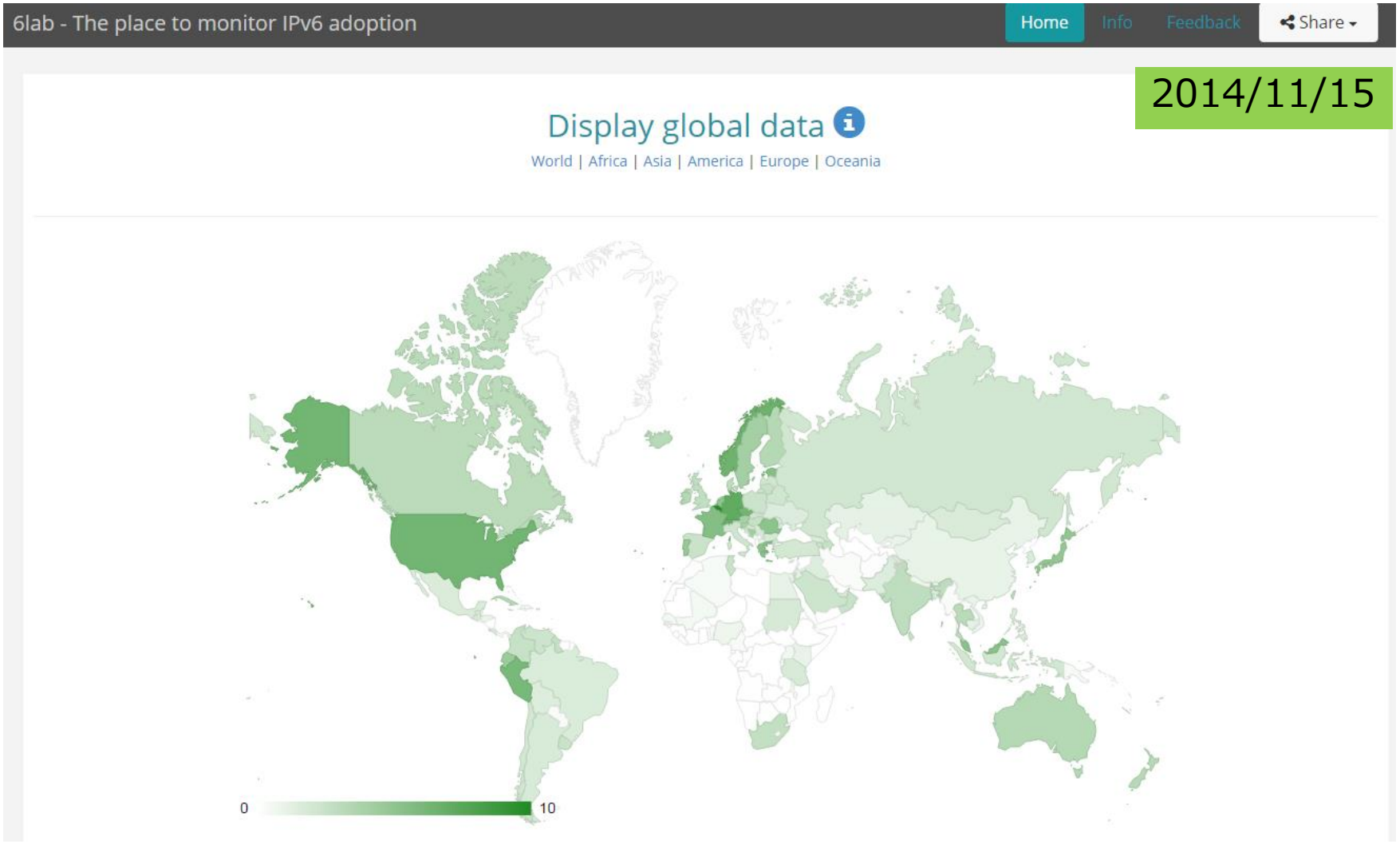


AP地域の国別IPv6アドレス配分状況

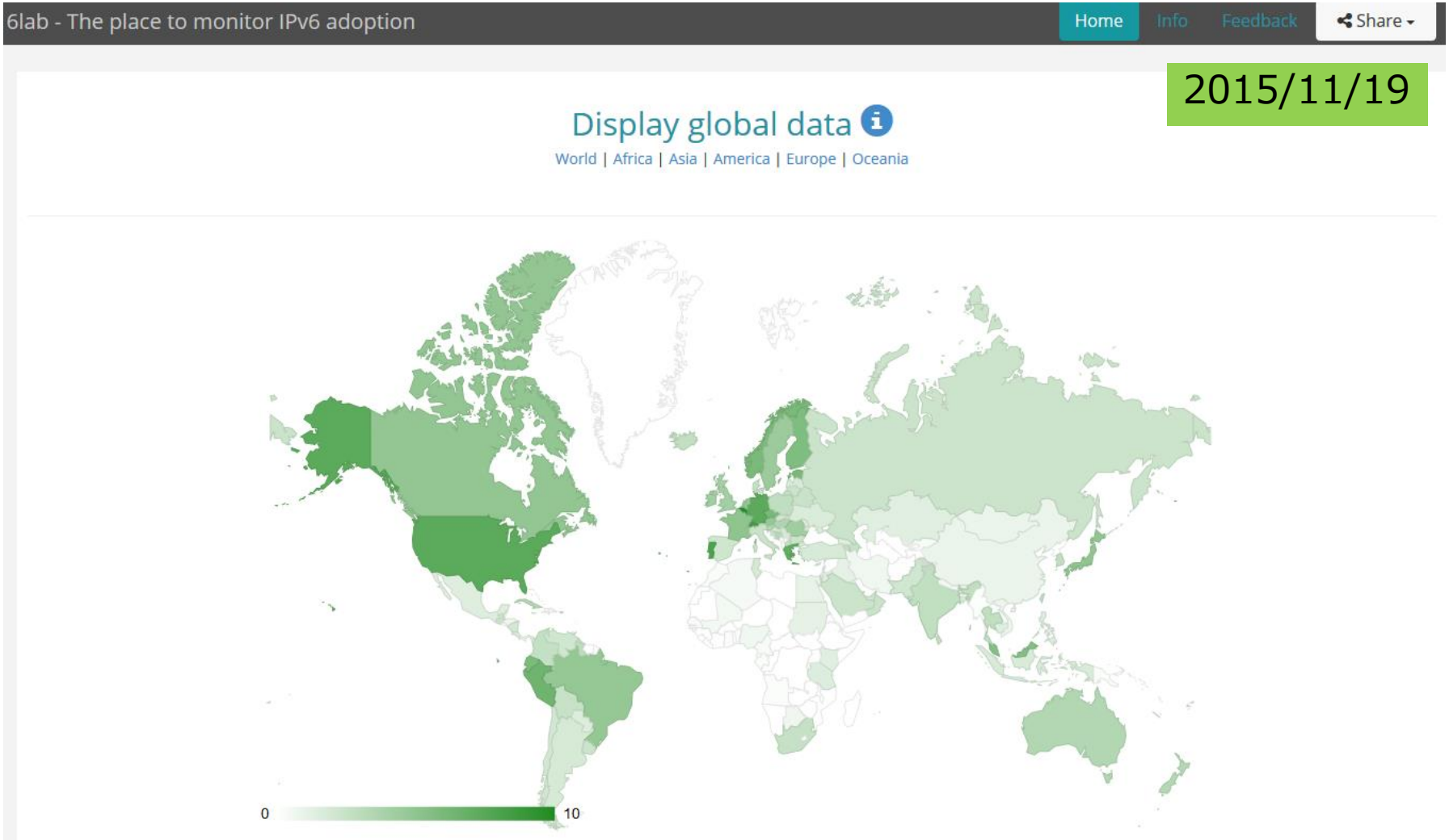


出典： http://www.nic.ad.jp/ja/stat/ip/asia-pacific.html

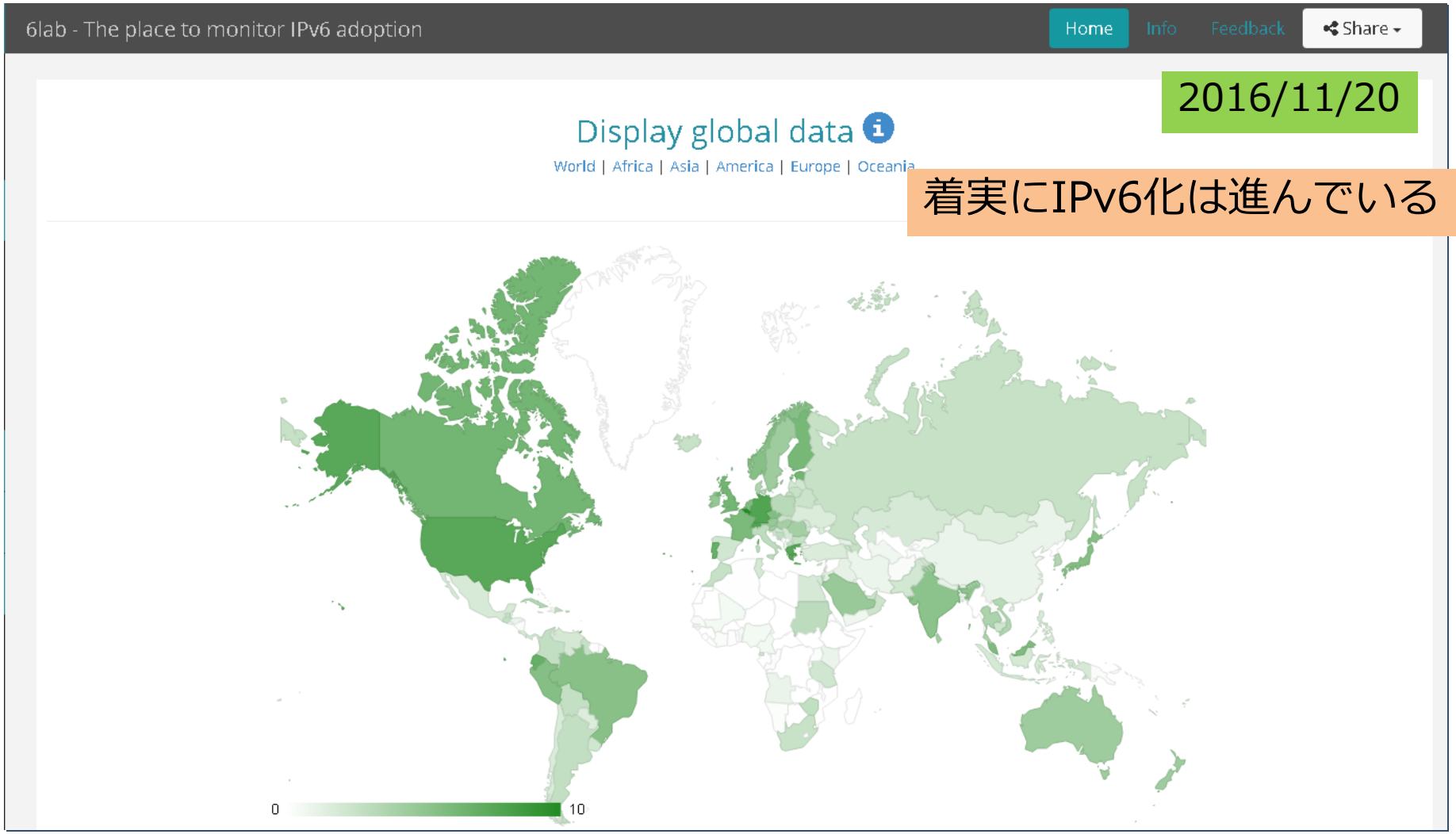
http://6lab.cisco.com/stats/



http://6lab.cisco.com/stats/



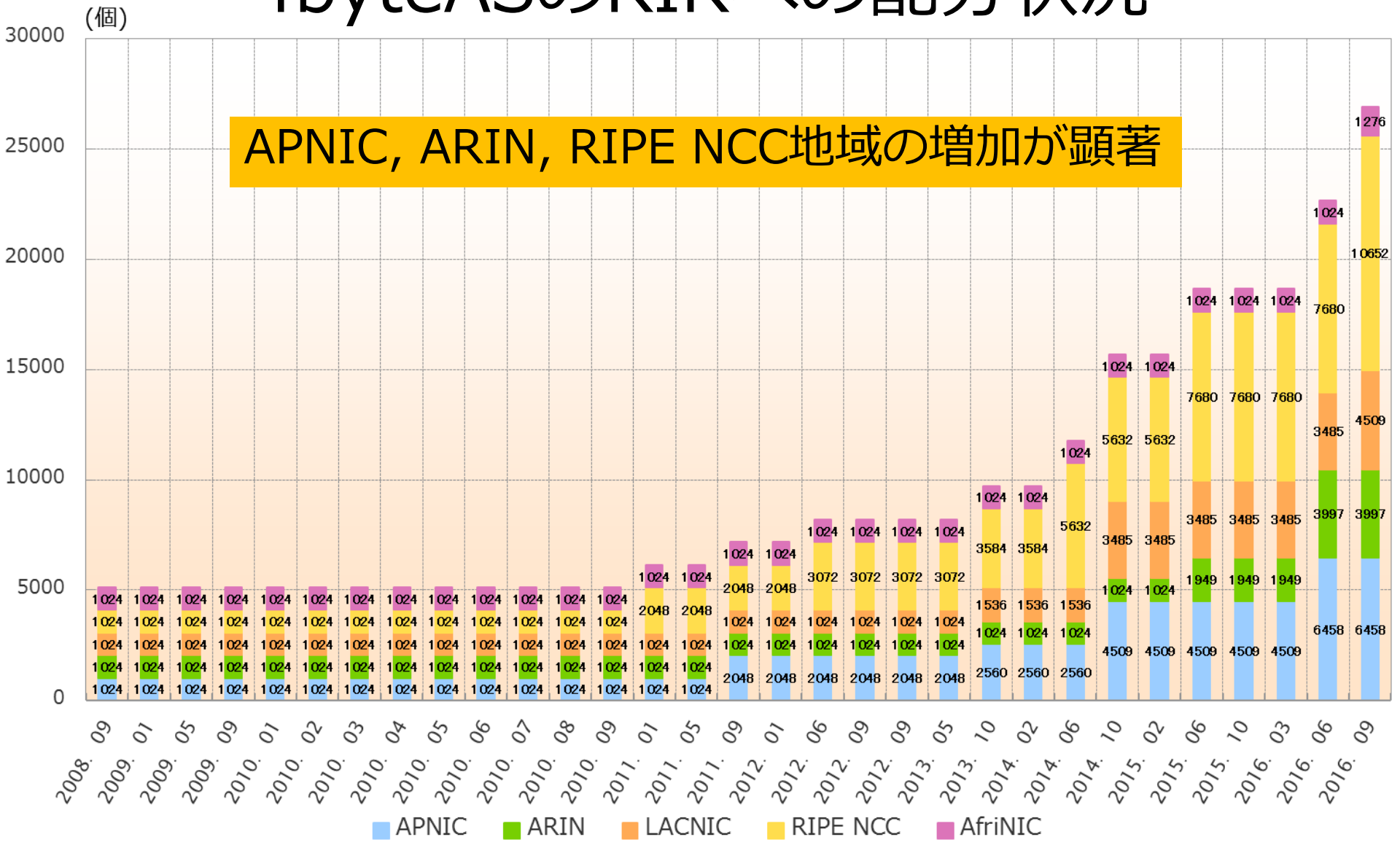
http://6lab.cisco.com/stats/



AS番号 (2byte/4byte)

- 2byte AS
  - IANA在庫はついに枯渇（2016-07-29 RIPEへ）
  - 2014年に枯渇すると予測されていたが、4byteASの払い出しや2byteASの移転により枯渇が伸びている
  - AS番号の移転も2014年より開始
- 4byte AS
  - RIPE、APNIC、LACNIC地域が継続的に増加
  - 日本は徐々に促進してきたが、依然2byte頼り。。
    - 上流ISPが未だ4byteAS未対応や、必要性を証明できる場合
    - 払い出し数として、2byte：4byte = 2:1 程度にはなってきた
      - これまでは、5:1 程度だった

4byteASのRIRへの配分状況



https://www.nic.ad.jp/ja/stat/ip/world.html

内容

- トラフィック動向
- ルーティング動向
- DNS動向
- セキュリティ動向
- まとめ

2016年 DNSトピック

- 全ルートサーバがIPv4/IPv6 dual stack対応
  - 最後はG-rootが今年2016年10月20日にIPv6対応完了
- .jp 30周年記念
  - 1986年8月5日、jon Postelから村井さんに委任されて30年
- 標準化動向
  - TCPで最初に問い合わせてもOKに（RFC7766: DNS Transport over TCP - Implementation Requirements）
- 新gTLDが1000を超える
  - 2016年6月に1000を超え、各サービスで利用されつつある
  - 内部で勝手に本格的に利用しているドメインがある場合には、きちんと取得・登録を行う等が必要

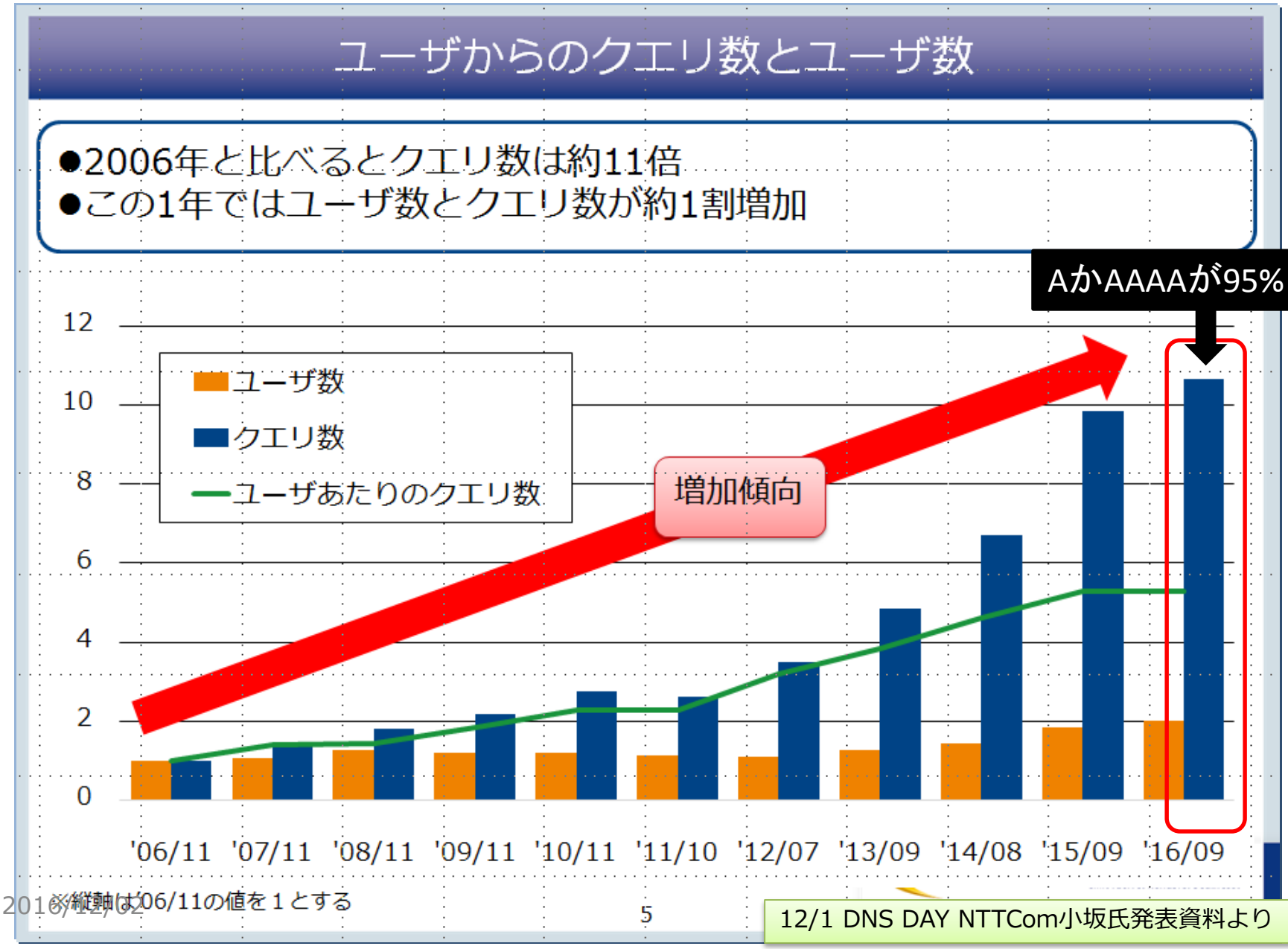
2016年 DNSセキュリティ動向

- 権威DNSサーバへのDDoS攻撃
  - RIPE NCCのccTLD用セカンダリサーバ（1月）
  - ルートサーバ（6月）
  - 日本国内のサービス（8月～9月）
    - ヨドバシドットコム、さくらインターネットのサーバ
    - 関係者の努力と対策により、影響（被害）は2014年に比べ軽減
  - Dynがやられて大騒ぎ（10月）
    - Twitter, Amazon, Netflix, Gidhub etc 多数のサービスに影響
    - NANOG68でDynの人が、botnetの悪意をもった通信を遮断する方法に関する発表を行った直後に攻撃が開始されたため、報復攻撃であった可能性も高い
    - Krebs on Security（セキュリティ情報提供サイト）が、イスラエルの二人がbotnetによる攻撃で荒稼ぎをしている記事を掲載し、二人が逮捕された後にブログサイトに620Gbpsを超える攻撃が発生
- ドメイン名ハイジャック
  - Bitcoin取り扱い大手に関わるblockchain.info（10月）
  - 2015年は日本国内でレジストラが被害に遭う事例が多発したが、落ち着いた模様
- 期限切れドメイン名の跡地を狙った攻撃：ドロップキャッチ
  - 新居浜韓国（niihamakanko.com）の本物そっくりの偽サイトを立ち上げ
  - 期限切れのため乗っ取りではないが、悪意を持って立ち上げていた
- 今年もBIND祭りは顕在、今年は9件で過去最高の脆弱性報告数

https://jprs.jp/tech/

2016-11-02 （緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2016-8864）
2016-10-21 （緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2016-2848）
2016-09-28 （緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2016-2776）
2016-07-19 BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2016-2775）
2016-03-10 （緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2016-1285）
2016-03-10 （緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2016-1286）
2016-03-10 BIND 9.10.xの脆弱性（DNSサービスの停止）について（CVE-2016-2088）
2016-01-20 （緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2015-8704）
2016-01-20 BIND 9.10.xの脆弱性（DNSサービスの停止）について（CVE-2015-8705）

OCNのキャッシュDNS動向

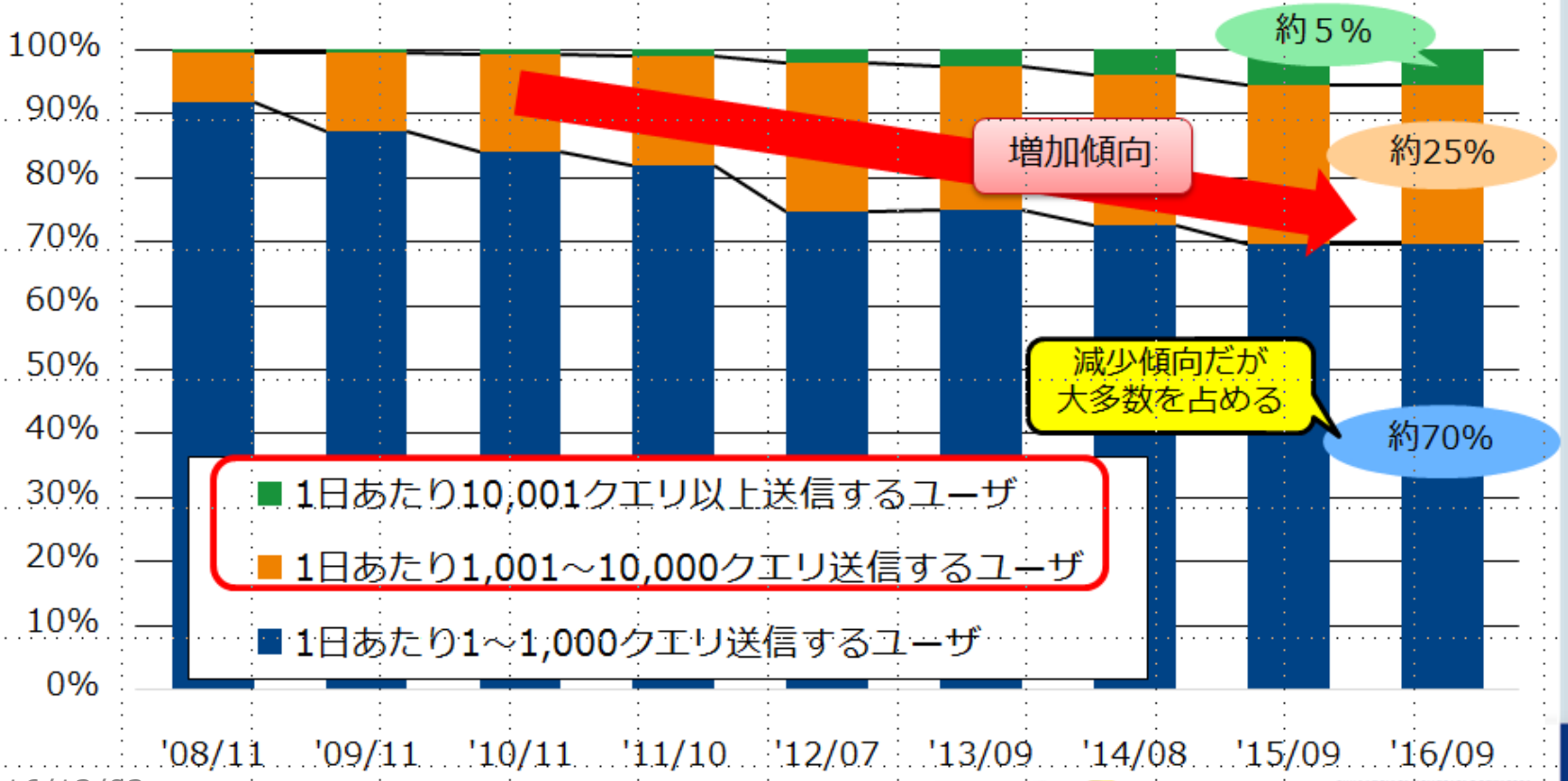


12/1 DNS DAY NTTCom小坂氏発表資料より

OCNのキャッシュDNS動向

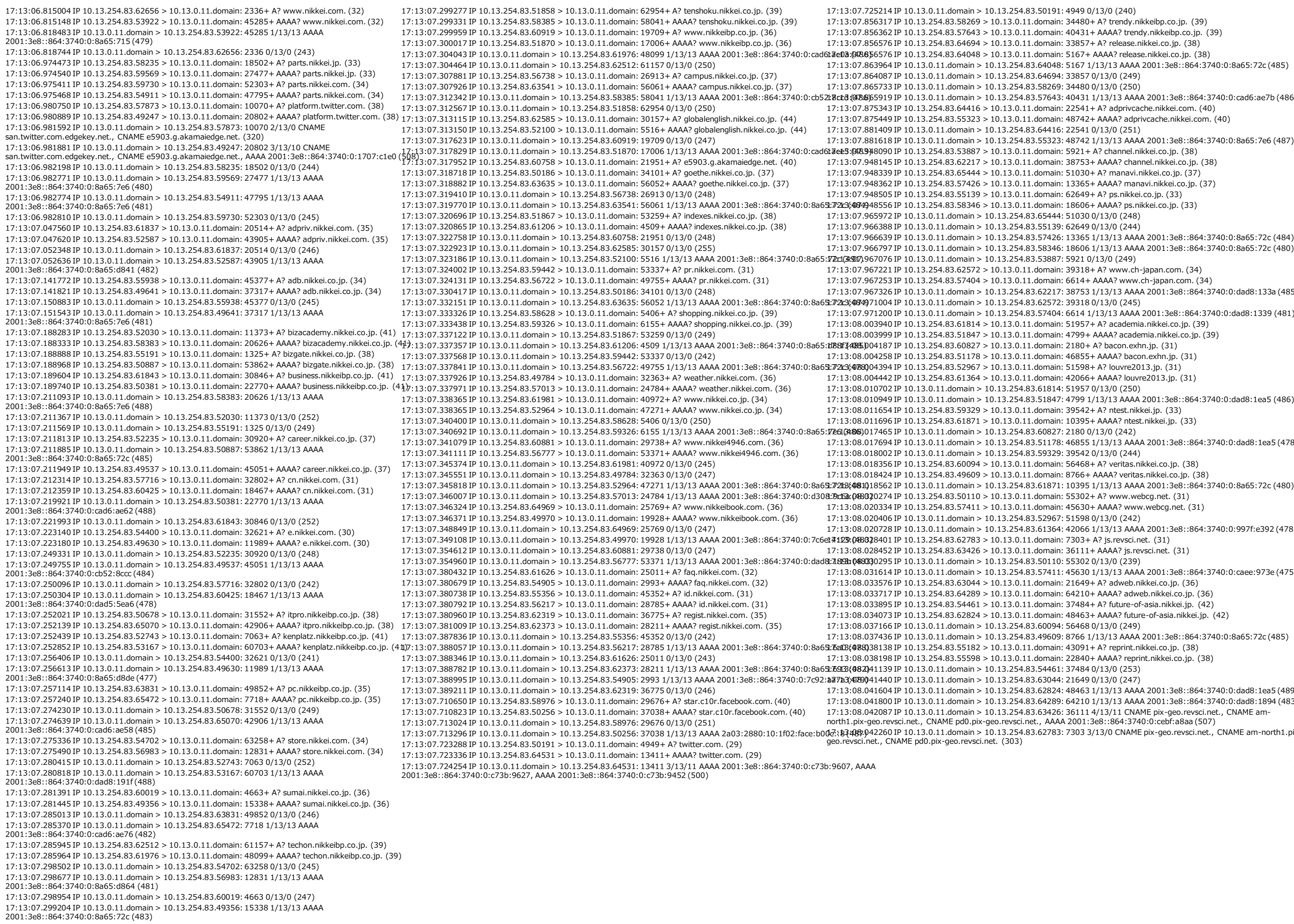
１日あたりに送信するクエリ数別ユーザ割合

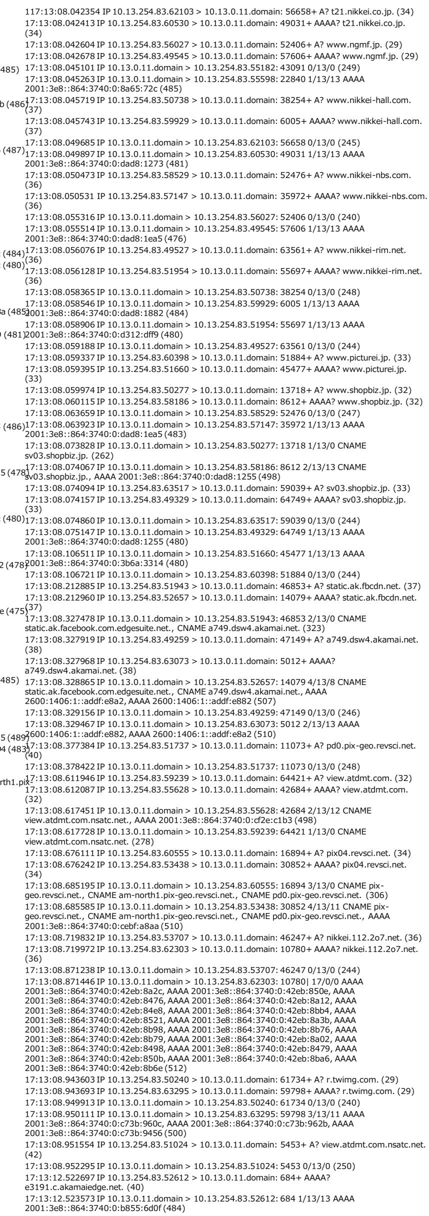
●1日1,000クエリ以上送信するユーザの割合は増加傾向
- ✓ WEBサイトの複雑化、ブラウザのプリフェッチ機能
- ✓ 家庭内端末(スマホ)の増加とWi-Fiオフロードが影響している？



12/1 DNS DAY NTTCom小坂氏発表資料より

一昔前のwww.nikkei.com





１つのサイトだけでもこれだけのqueryが出る。
ブラウザを立ち上げ時（タブの読み込み）はすごい量に

ひたすらキャッシュサーバの増強で頑張る…

内容

- トラフィック動向
- ルーティング動向
- DNS動向
- セキュリティ動向
- まとめ

2016年セキュリティ動向

- 大規模するDDoS攻撃
  - Kerbs on Security（セキュリティ情報提供サイト）に620Gbpsの攻撃（9月）
  - DYNへのDDoS攻撃が広範囲にわたり影響（10月）
    - Twitter, Amazon, Netflix, Gidhub etc 多数のサービスに影響
    - NANOG68でDynの人が、botnetの悪意をもった通信を遮断する方法に関する発表を行った直後に攻撃が開始されたため、報復攻撃であった可能性も高い
  - Botが簡単に買える時代に
- フィッシング攻撃
  - ネットバンキングや特定の企業を狙った不正サイトへの誘導やウイルス
- ランサムウェアの攻撃が再び増加
  - マルウェアの一種で身代金要求型不正プログラム（ランサムウェア）によりファイルの暗号化等がしかけられ、解くのにお金を支払うケースが多発
- UDPを利用した攻撃は依然健在（NTP、SSDP、DNS等）
- 経路ハイジャックも巧妙化
  - 特定のターゲットのみへ不正経路広報しSPAMを配信する

三井住友銀行をかたるフィッシングメール

■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
ご登録パスワードの変更完了のお知らせ
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■

このメールは登録パスワードを変更された方へのメールです。

===
確認のためにメールを送信しています。
お客さまご自身で変更した場合は、このメールを無視しても問題ありません。

お客さまご自身で変更していない場合は盗用の可能性がございます。
至急以下のURLをクリックしてください。
（PC?スマートフォンからご利用ください。）

http://www.smbc.co.jp/idinforeset/changelink.nhn?
prm=R2f4thQReL91Td_CUaqNb7bismXy3rNoEqVinBRmwJ-QHg6pn9FIz4OPROjimL_WecGS--
F9n5sQAKY6yS_bs8fbsGa5gzWNZzIsh-UnRv8
<http://www.ssmbc.●●●●.net/>

※このメールアドレスに返信頂きましても、ご返答はできませんので、
お問い合わせは三井住友銀行ヘルプのサポートフォームよりお願い申し上げます。
URL : http://www.smbc.co.jp/supportformselect.nhn
<http://www.ssmbc.●●●●.net/>

今後とも三井住友銀行をよろしくお願いいたします。

三井住友银行サイトのご利用にあたって
URL : http://www.smbc.co.jp/
<http://www.ssmbc.●●●●.net/>

フィッシング対策協議会サイトより

Appleをかたるフィッシングメール

拝啓、

私たちは、あなたのアカウント情報の一部が誤っていることをお知らせしたいと思います。私たちは、あなたのアカウントを維持するためにお使いのApple ID情報を確認する必要があります。 下のリンクをクリックしてアカウント情報を確認してください。:

マイアカウント確認 >

私たちは24時間以内にあなたからの応答を受信しない場合は、アカウントがロックされます。

Appleチーム

My Apple ID | サポート | プライバシーポリシー

Copyright c 2016 Apple Inc. 全著作権所有。

日本語版

Your Apple ID has been disabled for security reasons.
What should i do ?

If your Apple ID was locked, you can use two-step verification for apple ID, once you have confirmed your account informations will start as normal again.

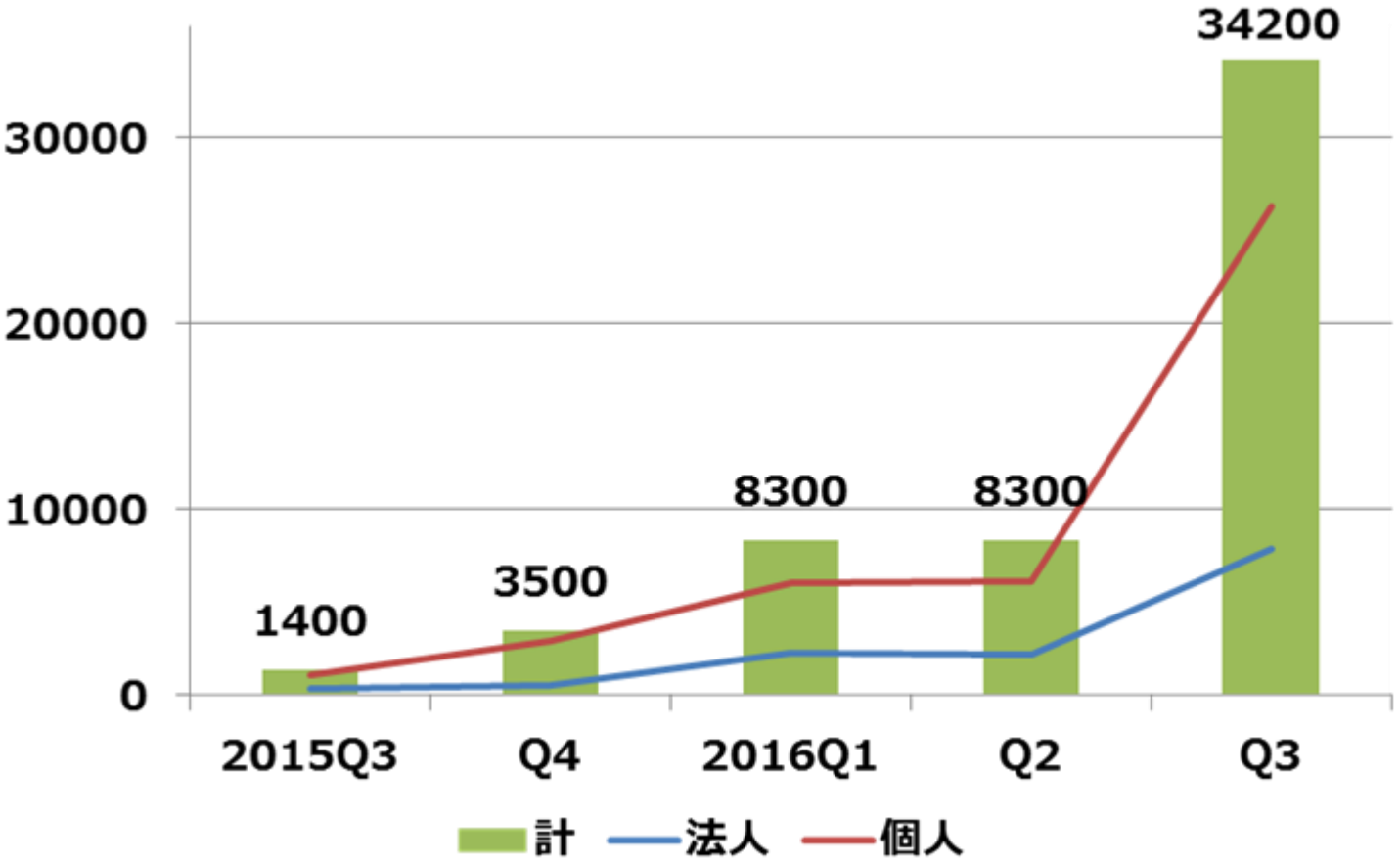
If you don't confirm your account within 24 hours, your account will be permanently frozen.

Start verification your Apple ID.

英語版

フィッシング対策協議会サイトより

ランサムウェアの数



トレンドマイクロ社の発表資料より　http://blog.trendmicro.co.jp/

最近の経路ハイジャック

1. 局所的かつ意図的な悪意を持ったハイジャック
   - 一部のピア先にのみ不正な経路を流し情報を盗むなど
     - 例）ビットコインのやり取りを盗む
   - Longer-prefixを再広告することで奪回可能だが、そもそも検出が難しいという問題がある
   - ASを持ちこんで接続性を確立しハイジャックを実施する実例も
2. 未利用アドレスのハイジャック
   - 勝手に使って無さそうなブロックを探して経路広報し悪用
   - ロシア方面のASから不定期に日本の経路も広告利用されている
   - **広報していない経路は、きちんと広報することが慣用**
   - **JPIRRに登録して経路奉行で検出・通知する機構を活用する**
3. Route Optimizerによる不慮の事故が発生
   - 経路を分割して内部に広報していた経路が誤って外に漏れる
   - Google, Amazon, Twitter, Apple, Akamai等が含まれており影響大
4. Defensive Hijacking 悪いことしてないよ？ってやつ

1. Invisible hijack（RIPE72）

- DE-CIXの顧客ASより、非常に悪質な局所的なハイジャックが発生
- 当時の状況（被害者：OutsideHeavenさん）
  - 1月21日より、日に２，３通のペースでSPAMCOPより/13のアドレス空間に対するレポートが頻繁にあがってくるようになった
  - 全てyahoo向けSPAM mailに関するレポート
  - 自ASでMailポートをブロックしたり、他から経路広報するも改善されず
    - 当然自社とは関係ないところで起きている出来事なので、無効
  - Yahooに問合わせ
    - なぜか/18が別ASからYahooに広告されていることが判明。。。
  - なんと、DE-CIXに接続している中国系AS番号から直ピアで広報
  - しかも、当初接続されていたASから途中でAS番号を変更している！
  - Reseller（仲介事業者のNW）を経由してDE-CIXのIX接続を購入
- あるASを利用してIXPの顧客になり、途中でIX接続のAS番号を変更したののち、yahooとpeering接続し、適当なprefixを広報しspam送り放題

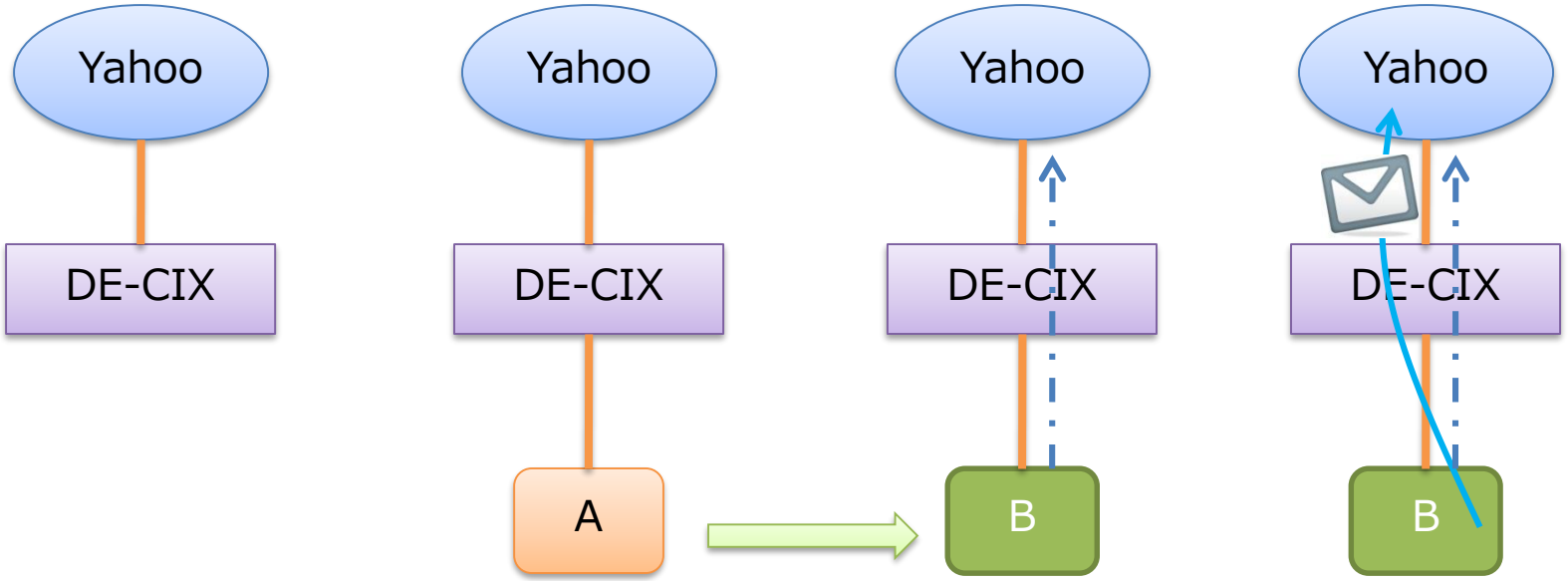
1. Invisible hijack（RIPE72）

Yahooは元から
お客さん

Aさんが
新規接続

AS番号をBに
変更し他人の
経路を勝手に
広告

YahooとピアしてIPを利用して該当経路のSPAM配信

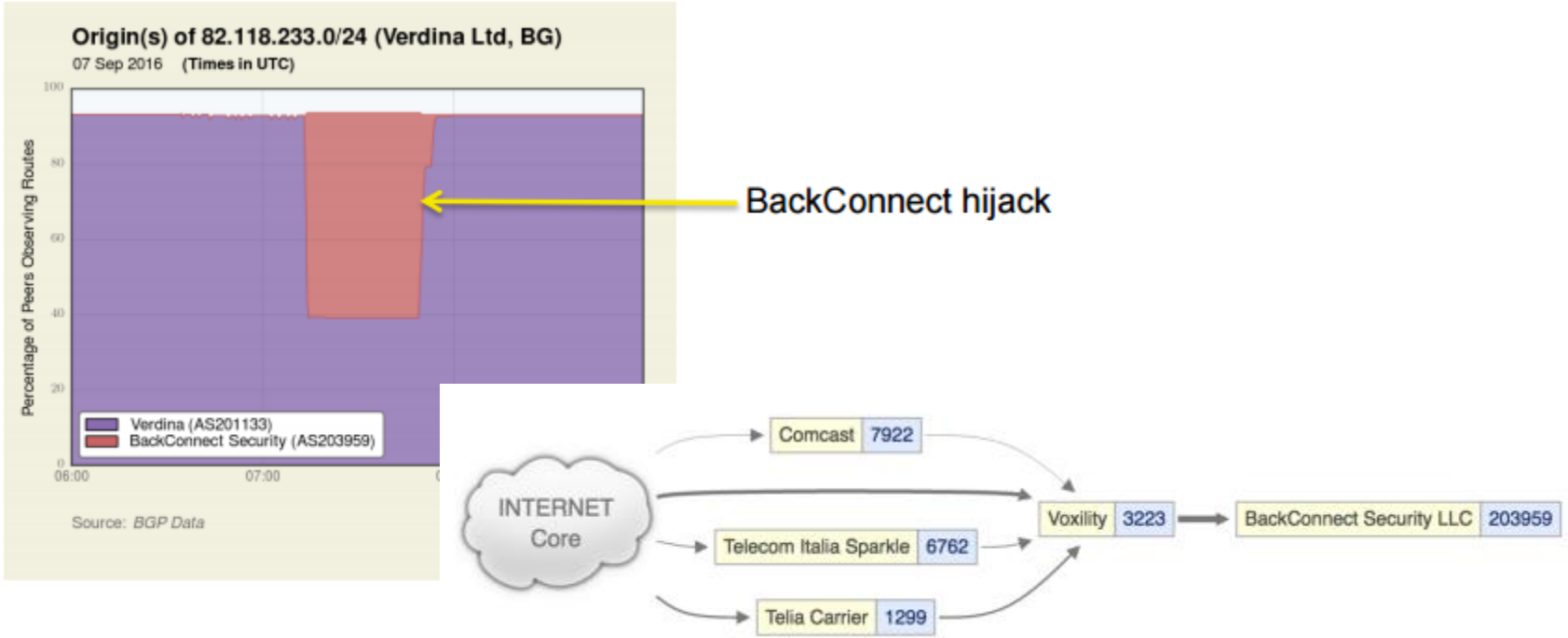


今後の対策は現在DE-CIX及び顧客、コミュニティで議論中
（by Arnold@CTO）

DE-CIX: ドイツの大手IX

4. BackConnect社によるhijack

- 2016年9月、Israeli Online Attack Service “vDOS”の経路情報を、BackConnect社が約40分程度経路広報



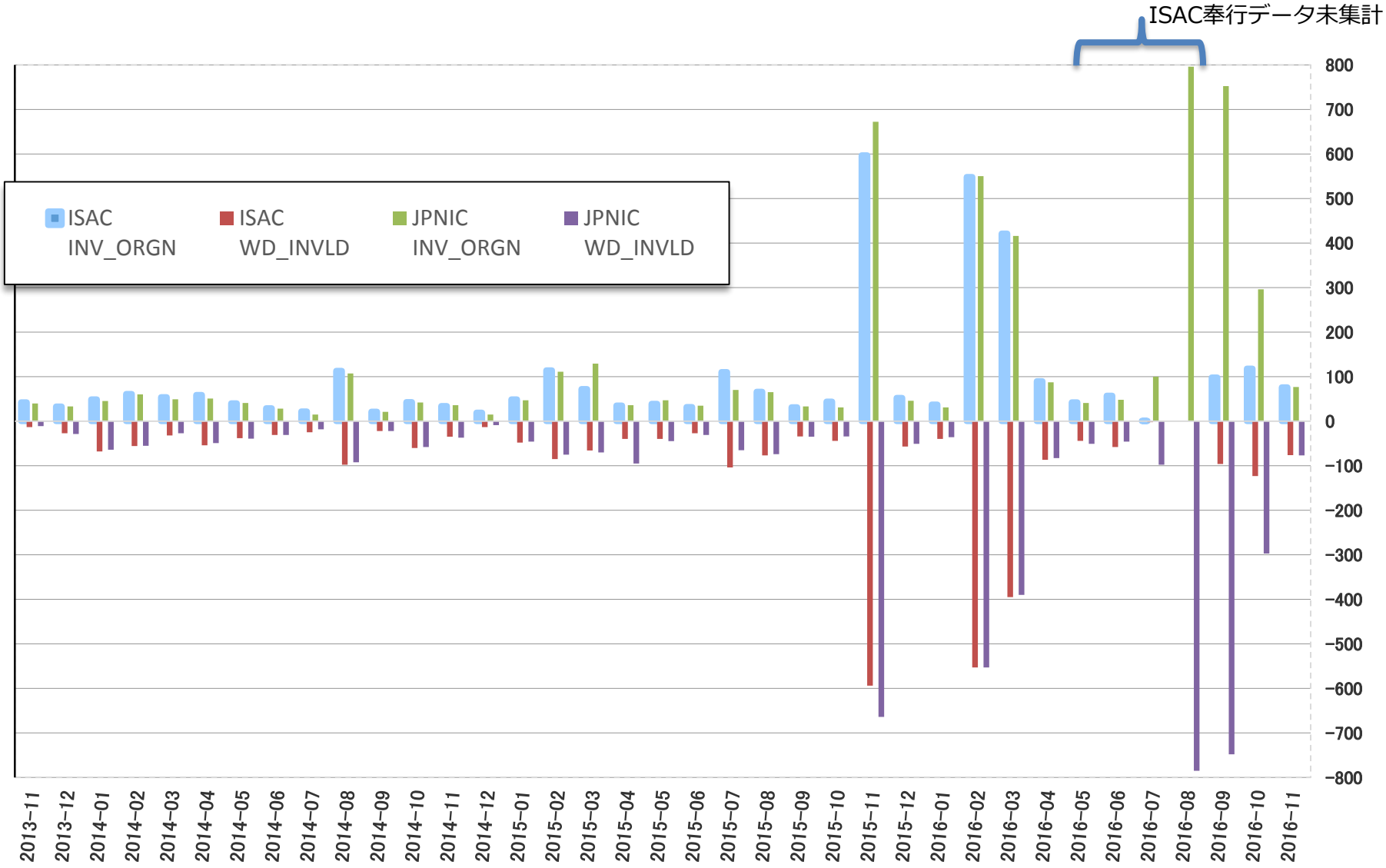
https://dyn.com/blog

4. BackConnect社によるhijack

- BackConnect社って何者？
  - BGP経路広報を伴い、不正なトラフィックをinterceptするセキュリティ会社
  - この件に限らず以前からやっている（by CEO）
  - Botnetの不正通信から守る
- つまり、DDoS mitigation service会社

- 今後多くの事業者が類似のサービスや事例を行った場合、何が正しいのかが判別しにくくなるかもしれない
  - ROAの登録が必須になってくる

ハイジャック経路検出状況@経路奉行



Telecom-ISAC JAPAN にて運用中の経路奉行の統計データより

内容

- トラフィック動向
- ルーティング動向
- DNS動向
- セキュリティ動向
- まとめ

2016年のまとめ

- トラフィック動向
  - ブロードバンドトラフィックが顕著に増加。Wifiオフロードも牽引
  - HTTTからHTTPSへ、日本の今後の動向にも注目
  - イベント時のトラフィック変動やコンテンツ配信の変化なども見受けられた
- ルーティング動向
  - 枯渇後もIPv4は依然増加、追加割り振りや移転等により継続的に伸びていく
  - IPv6の経路急増に要注意
- DNS動向
  - gTLDが1000を超え増加中
  - 権威DNSへの攻撃やドメインハイジャック、ドロップキャッチ等の被害が観測
  - BINDの被害も相変わらず多く、日々の運用対処が必要
  - スマホやIoTデバイス等の増加によりクエリ数がますます増加、増強が必要
- セキュリティ動向
  - 大規模化するDDoS攻撃、引き続き注意が必要
  - 経路ハイジャックも巧妙化かつ知らずに被害にあうケースが増加
- 全体
  - DNS、ルーティング含めセキュリティ事案が多いため、様々な分野におけるセキュリティ対策や日々の運用対策をしっかりとって行くことが重要

2017年1月1日にうるう秒

- 2017年 “元日に”「うるう秒」挿入。8時59分60秒。
  - 時刻同期の方法は大きく2通り
    - LIbitが挿入されたNTPサーバを参照し、調整日当日に1秒挿入する方法（stepモード）
    - 特定の時刻より継続的に徐々に時刻を微修正し、１月1日9時に向けて調整する方法（slewモード、アジャスト機能）
  - 2015年7月1日は、比較的被害は多くなかったが、未だに問題は発生
    - 特定メーカーの機器がLIbitを参照するとカーネルパニックが発生
    - カーネル不具合でCPU使用率が高騰しwatchdogで再起動など
    - 世界中で約2000のネットワークで9時0分～5分程度の間ダウンが観測された
  - ITU 2015世界無線通信会議(WRC-15)にて、2023年のWRCまでに結論をだすことが決定。700年で30分のずれ。日本は廃止派。もうやめる？
- LIbit挿入は前日の12月31日9時00分00秒予定
  - トラブルを未然に防ぐために
    - LIbitを参照しないように、ntpdを一時的に停止し、間をおいて再度ntpdを起動
    - バグ対策がされたOS（カーネル）にバージョンを挙げて対策をうっておく
  - 元日なので、予期せぬ事態を招かぬよう準備を整えて対応しましょう

2015年再掲

平素は当社サービスをご利用いただきありがとうございます。

7月1日(水)、お客様にご利用いただいております[redacted]/VPSの
一部におきまして、カーネルパニックが発生したため
7月1日午前9時0分から9時7分にホスト機を再起動いたしました。
インスタンスは順次起動いたしております。
全インスタンスの起動が完了いたしましたら改めてご連絡いたします。

お客様にはご迷惑をお掛けし、申し訳ございません。

■ 障害詳細
1.障害発生時間：7月1日(水)午前9時0分 ～
2.発生原因：原因につきましてはわかりかねました。
3.影響範囲：[redacted]
4.影響内容：インスタンスへ接続できない状態が発生しております。
