

2017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>

本題の前に本題

当日のみ

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

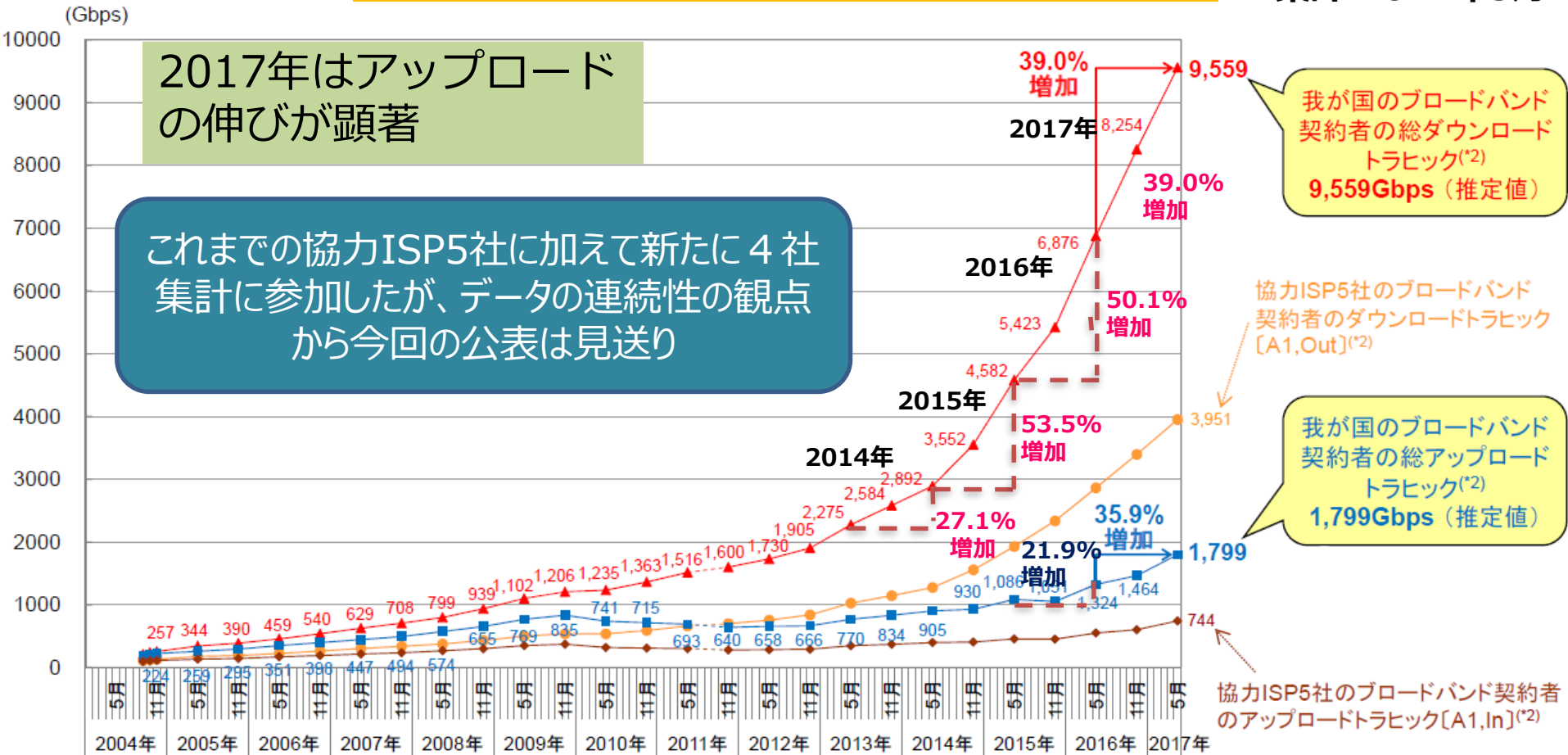
2017年 トラフィック動向

- ブロードバンドトラフィックは引き続き増加、特にアップロードが顕著に
 - ここ1年でダウンロードは**39.0%増**、昨年50.1%
 - ここ1年でアップロードは**35.9%増**、昨年21.9%
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がここ最近顕著に増加
 - 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）
 - **wifiのオフロードトラフィックも含め増加**
- モバイルトラフィックはここ最近1.3～1.4倍で安定的に増え続けている
 - ここ1年で**1.4倍**、昨年の1.35倍よりも増加率UP
 - 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トラフィックは比較的顕著に増加、対応ISPの導入増加による
- **HTTPからHTTPSへの動きが全世界で加速化しているが、2017年は特に日本国内のHTTPS化が加速化**
- イベント時のトラフィック変動も様々観測されている

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:2017年5月

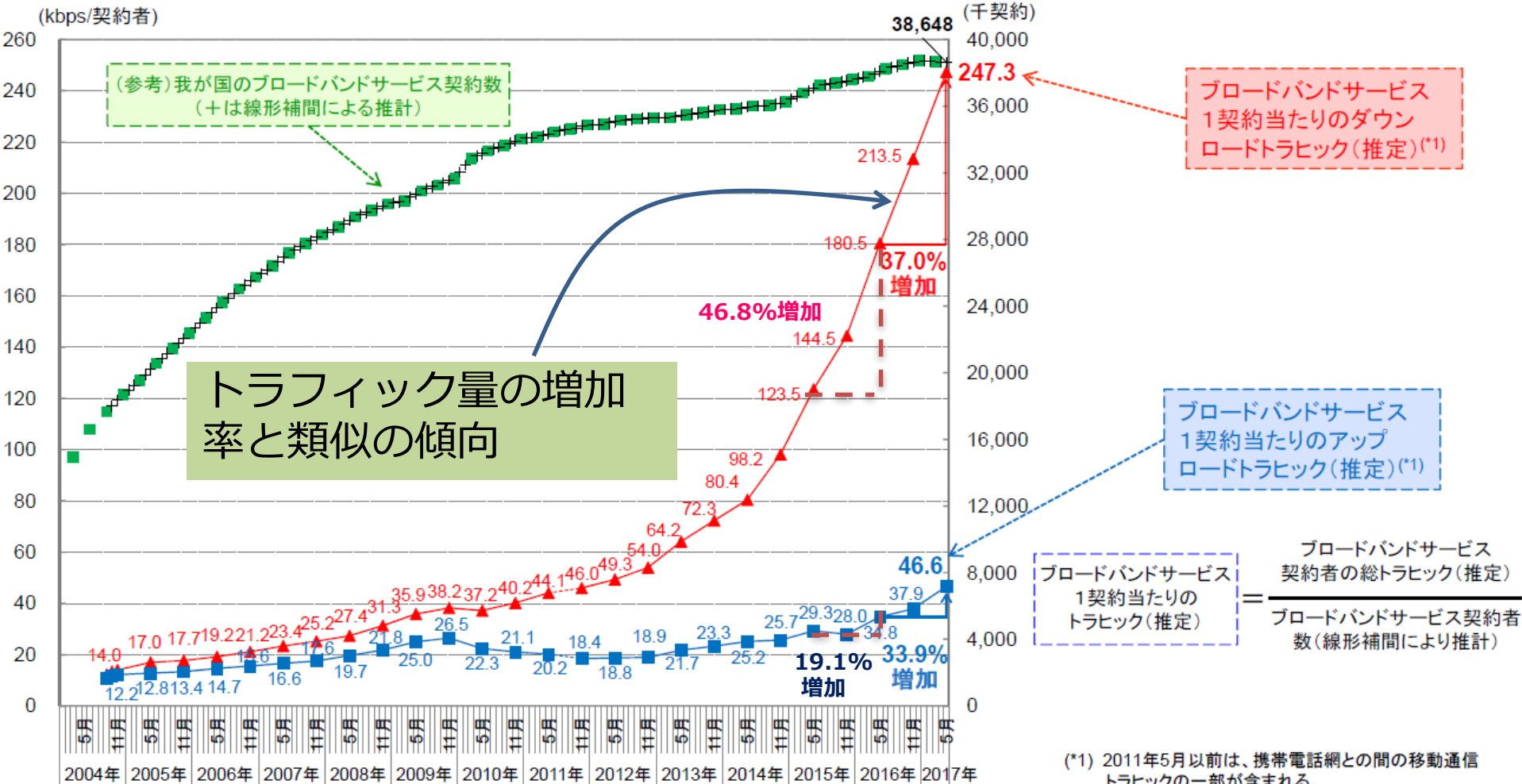


出典：総務省「我が国のインターネットにおけるトラフィックの集計・試算」 2017年8月15日

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:2017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フィックの集計・試算」

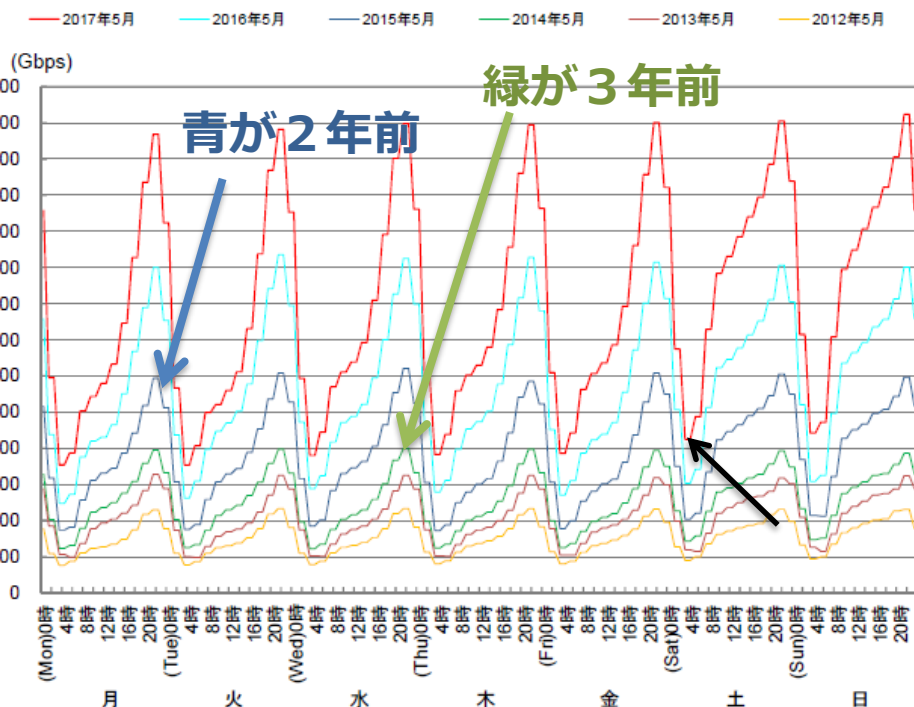
2017年8月15日

日本国内のトラフィック推移

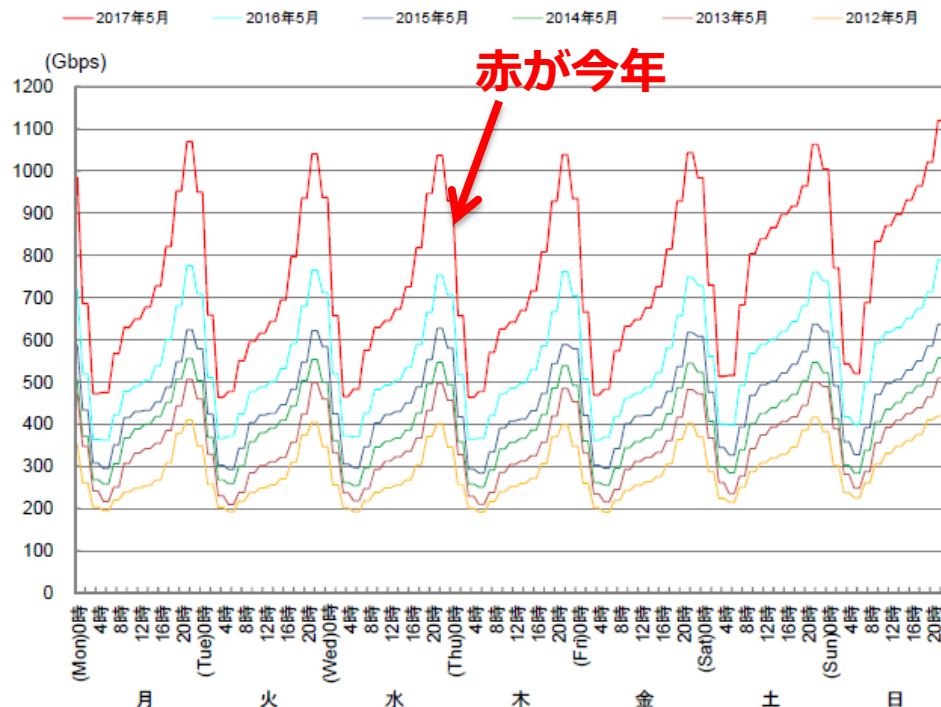
5分平均のピークトラフィックの推移

ブロードバンドサービス契約者の時間帯別トラフィックの変化(過去5年との比較)

ダウンロード



アップロード



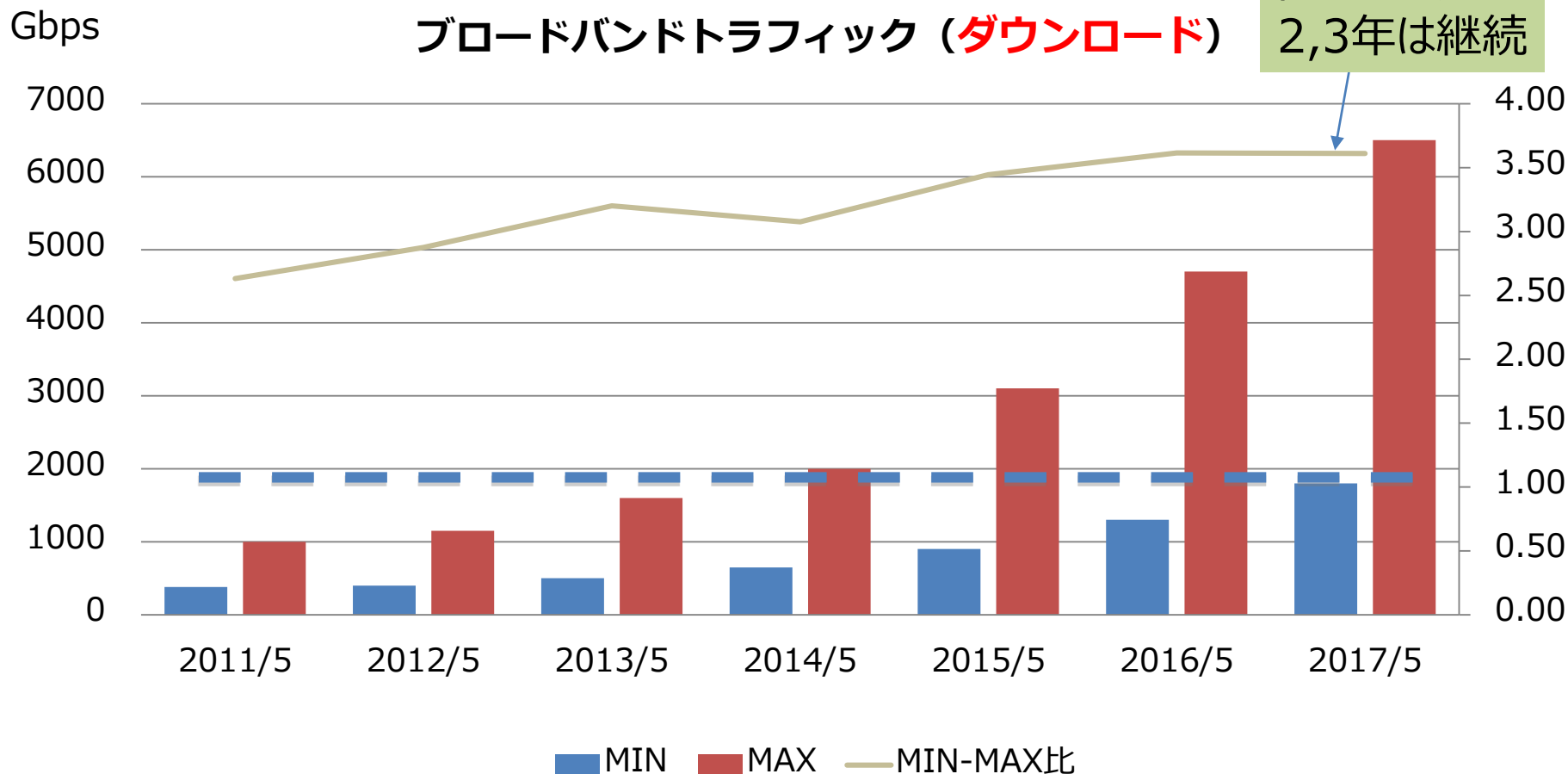
(平均) 最少トラフィックも年々底上げされている (3年前のピークと同等相当の量)

出典：総務省「我が国のインターネットにおけるトラフィックの集計・試算」 2017年8月15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

3.5倍以上の開きがありここ2,3年は継続



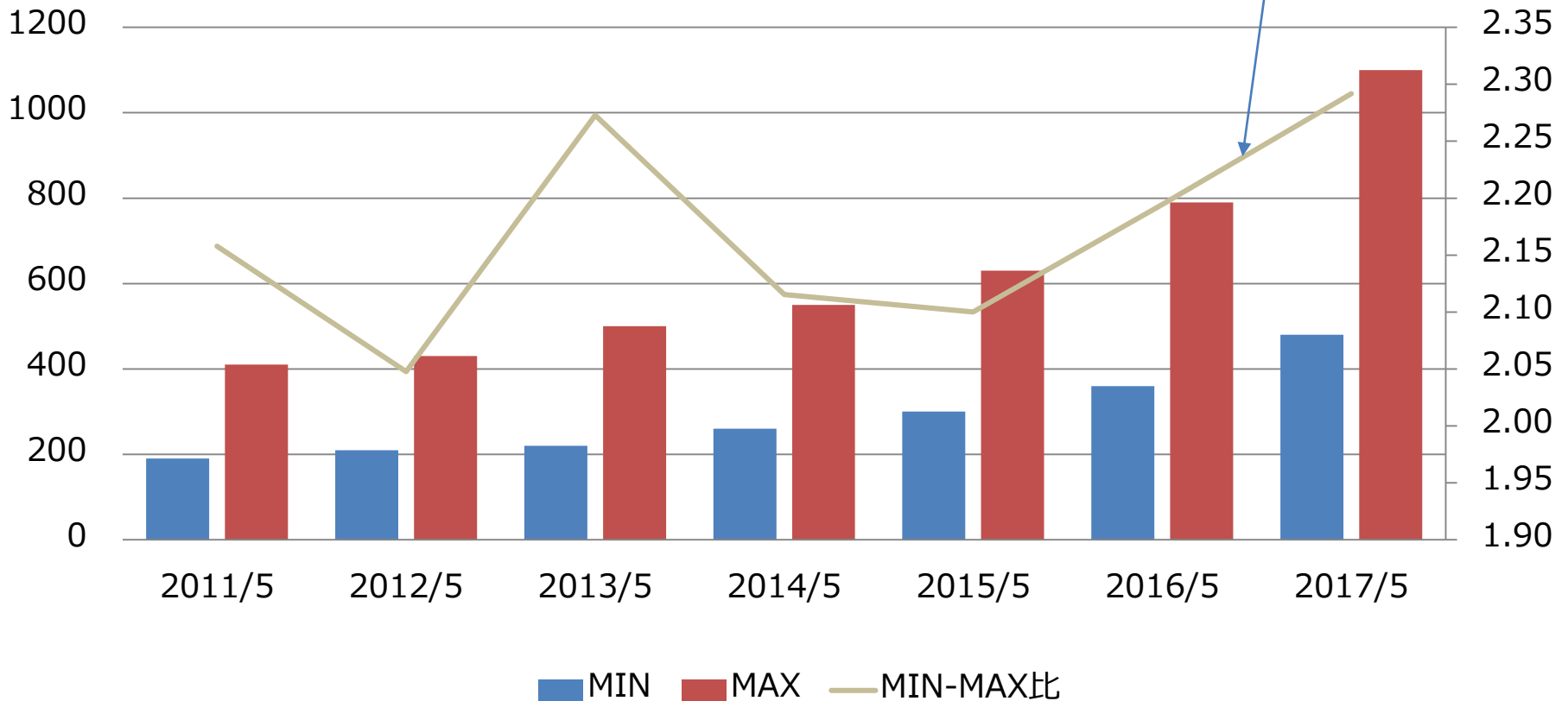
「我が国のインターネットにおけるトラフィックの集計・試算」のデータ (2011年~2017年) を集計

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

ここ2,3年アップロードの伸びが顕著

ブロードバンドトラフィック (アップロード)

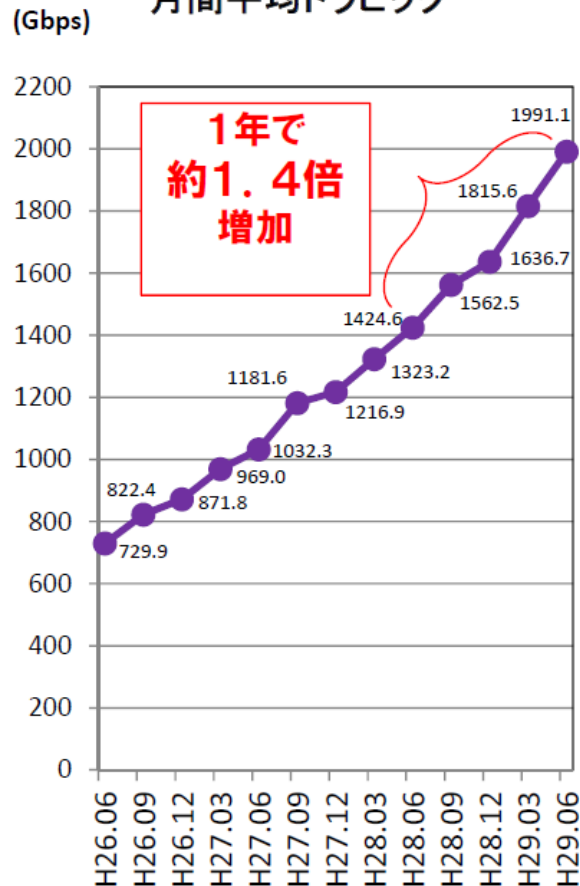


「我が国のインターネットにおけるトラフィックの集計・試算」のデータ (2011年~2017年) を集計

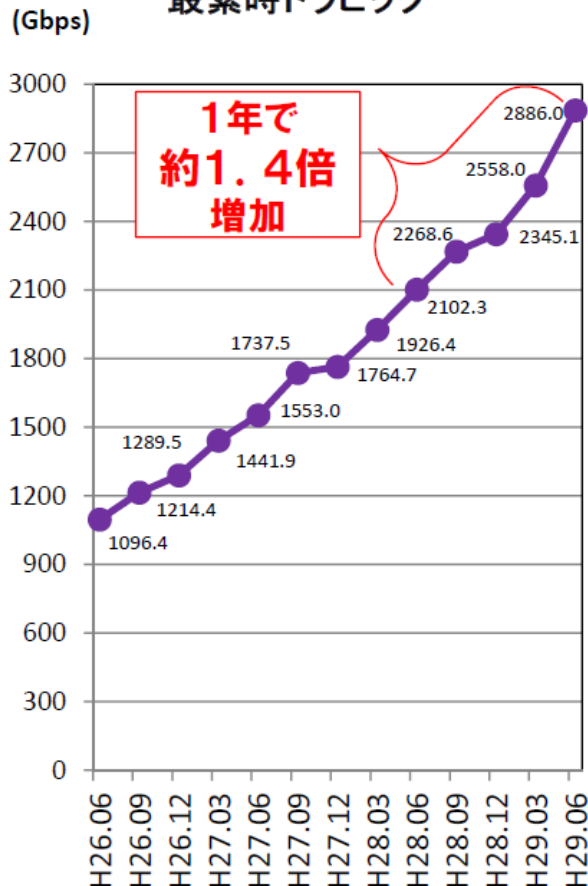
移動通信トラヒックの推移（過去3年間）

トラヒックの伸び幅は、ここ1年は **固定通信(40%) > 移動通信(35%)** であるものの、着実に増加しており、移動体通信のトラフィック増加は継続傾向

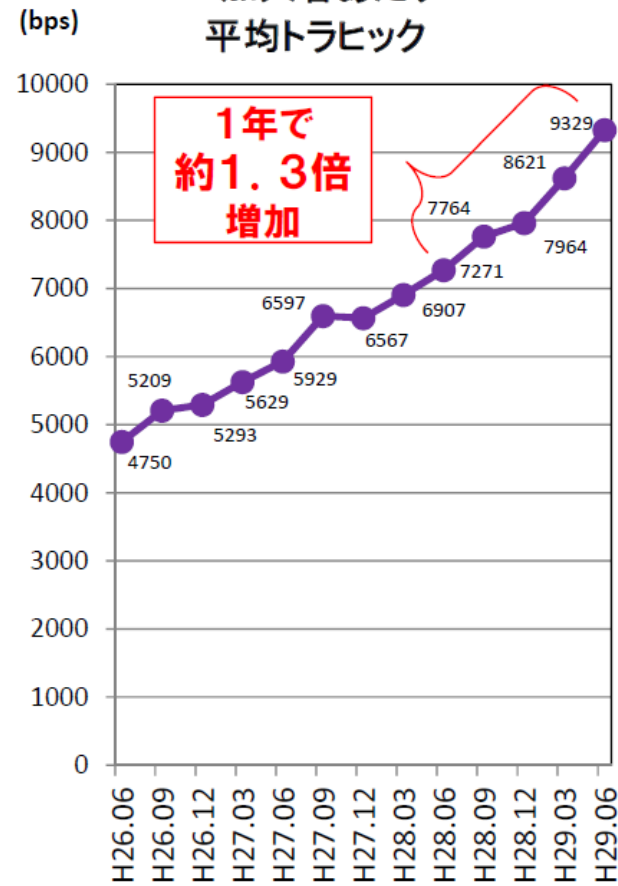
月間平均トラヒック



最繁時トラヒック

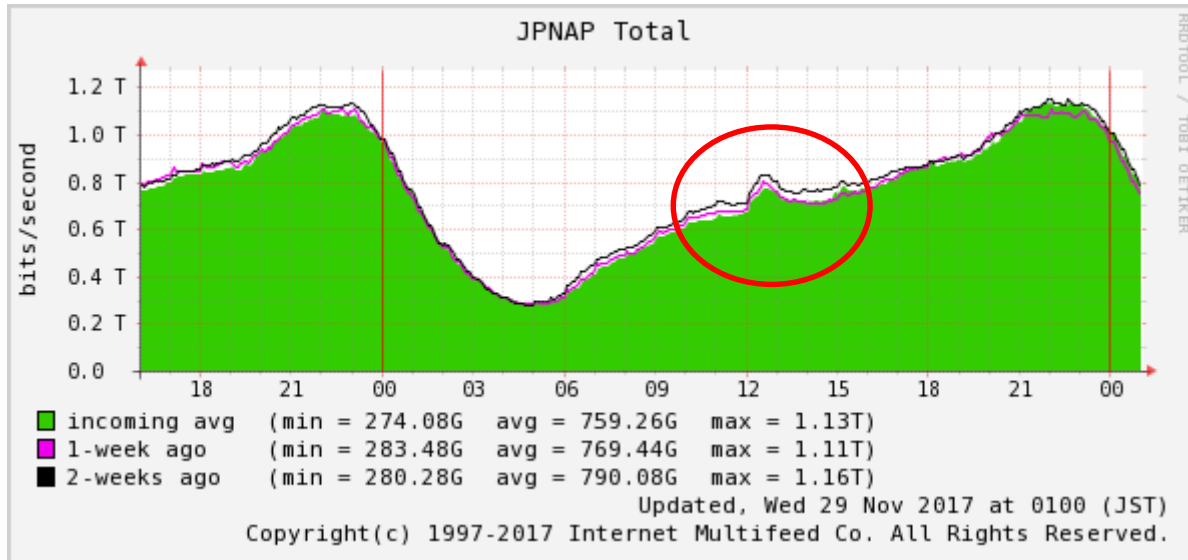


1加入者あたり平均トラヒック



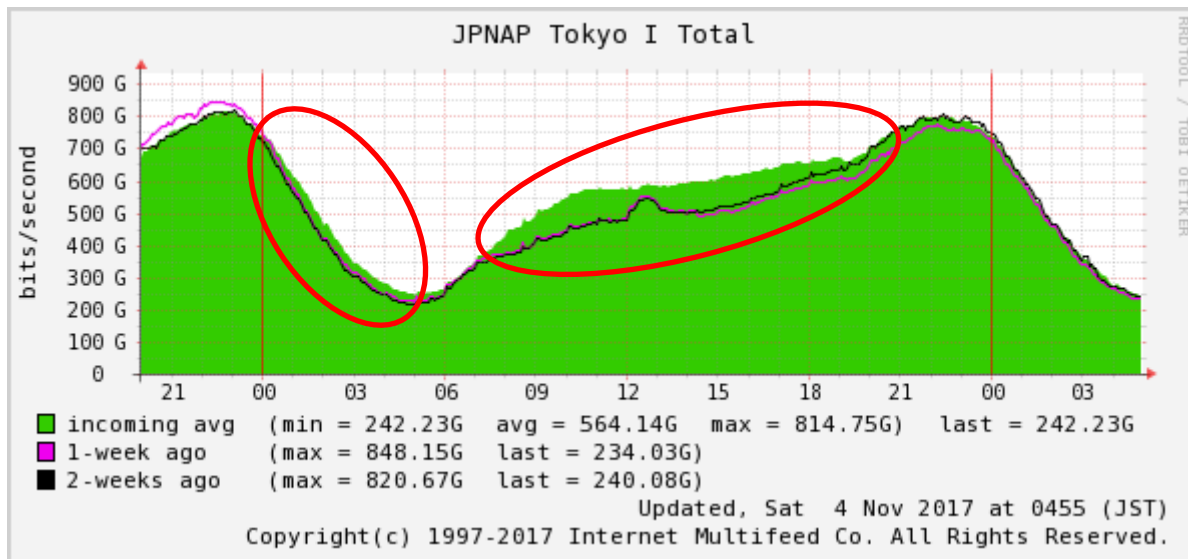
出典：総務省「我が国の移動通信トラヒックの現状（平成29年6月分）」

1日のトラフィック傾向



JPNAPのトラフィック推移 (平日)

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
MIN-MAXの比率は、3.5倍程度



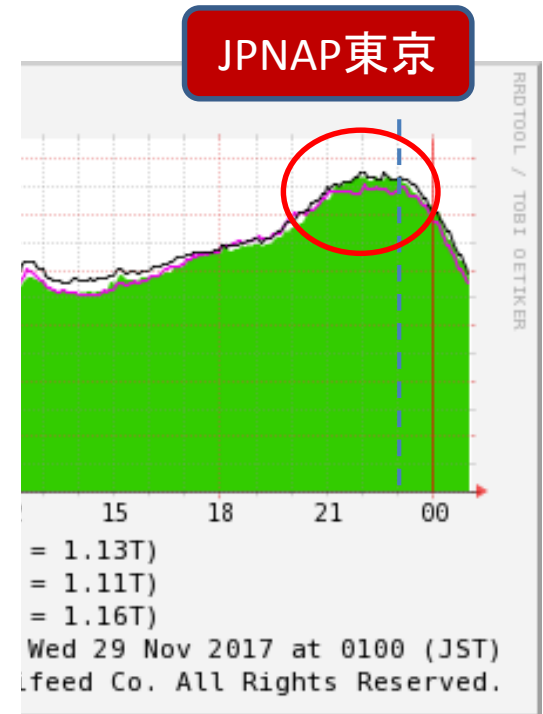
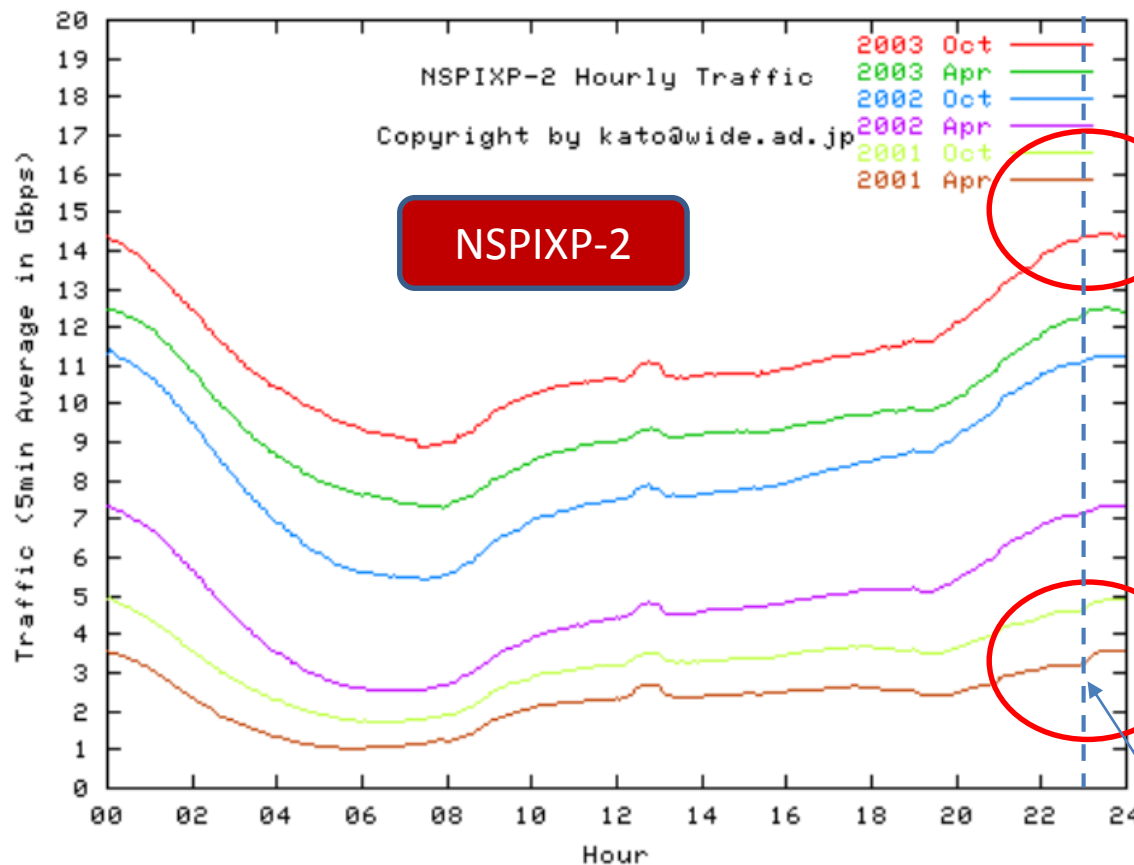
JPNAPのトラフィック推移 (2017年11月3日祝日)

祝日は明け方、日中共に
トラフィック量が多い(緑)
夜のピークはあまり変わらない
平均的な生活の人は寝る時間
一緒?

14年前と比較

1日のトラフィック推移

ピークは年々前倒しになってきている
昔は23時30分頃→22時30分頃

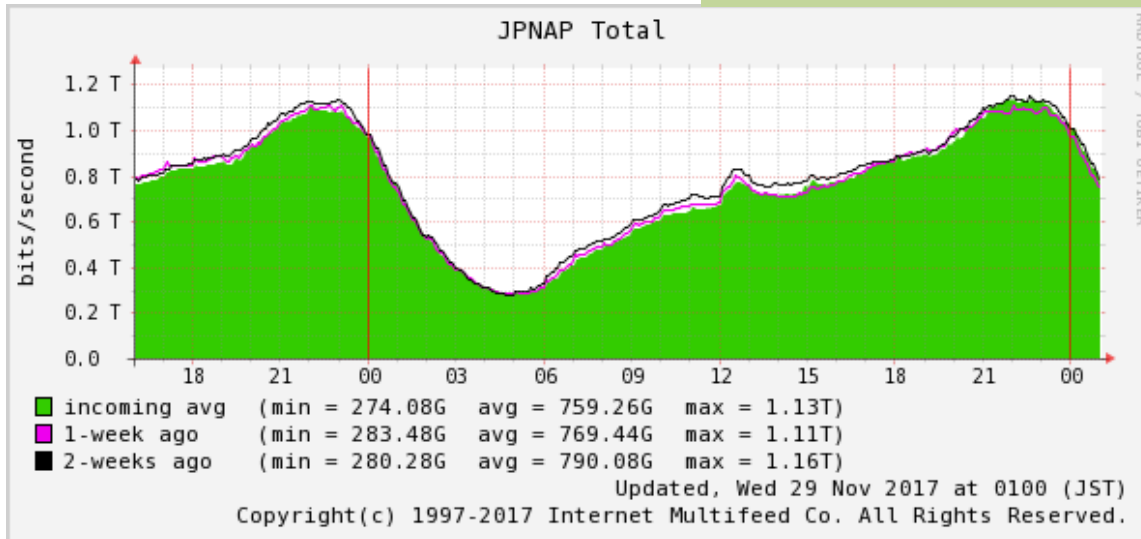


テレホーダイ？

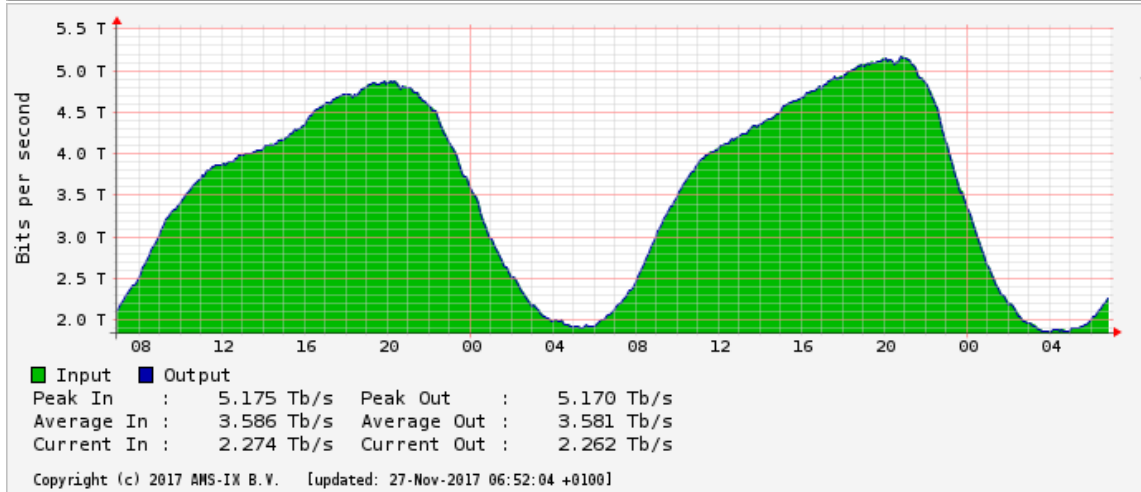
2003年のIPミーティングの資料より

EUとJPの比較

ピークが2時間ほど違う！寝る時間が日本は遅い？
お昼の時間帯にトラフィックの伸びは日本特有



JP NAP東京(日本)の
1日のトラフィック推移

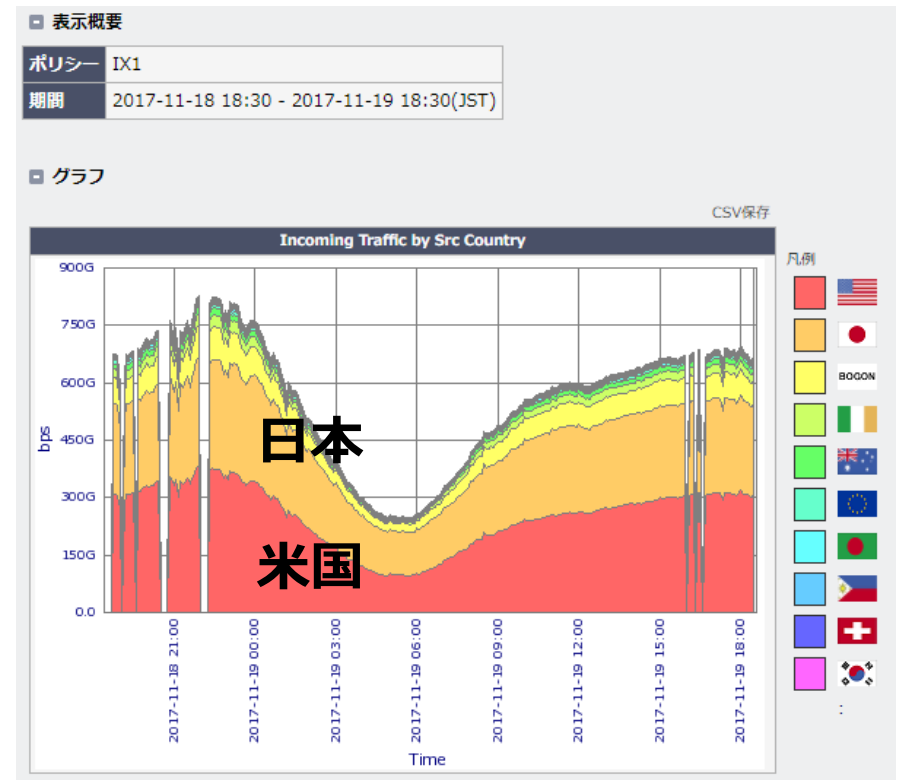
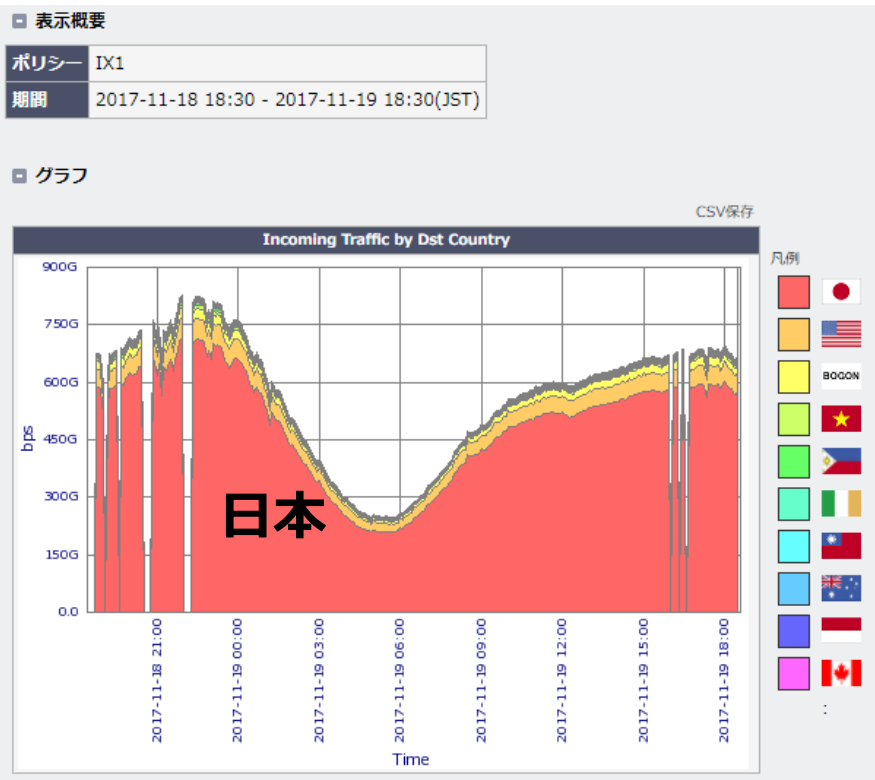


AMS-IX(Europe)の
1日のトラフィック推移

JPNAP通信の国別集計結果 2017/11/18~19

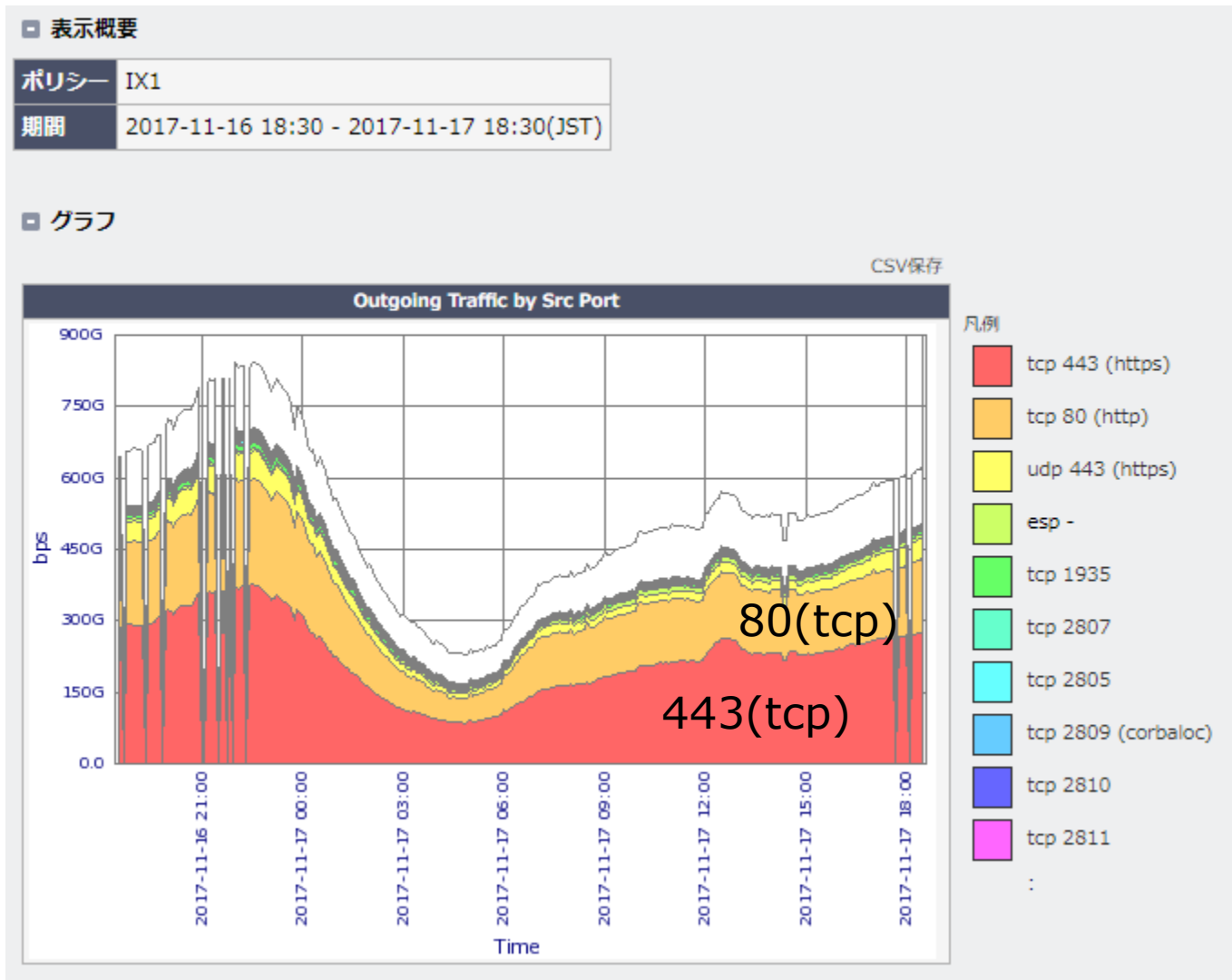
宛先IPの国別集計（宛先国）

送信元IPの国別集計（発信国）



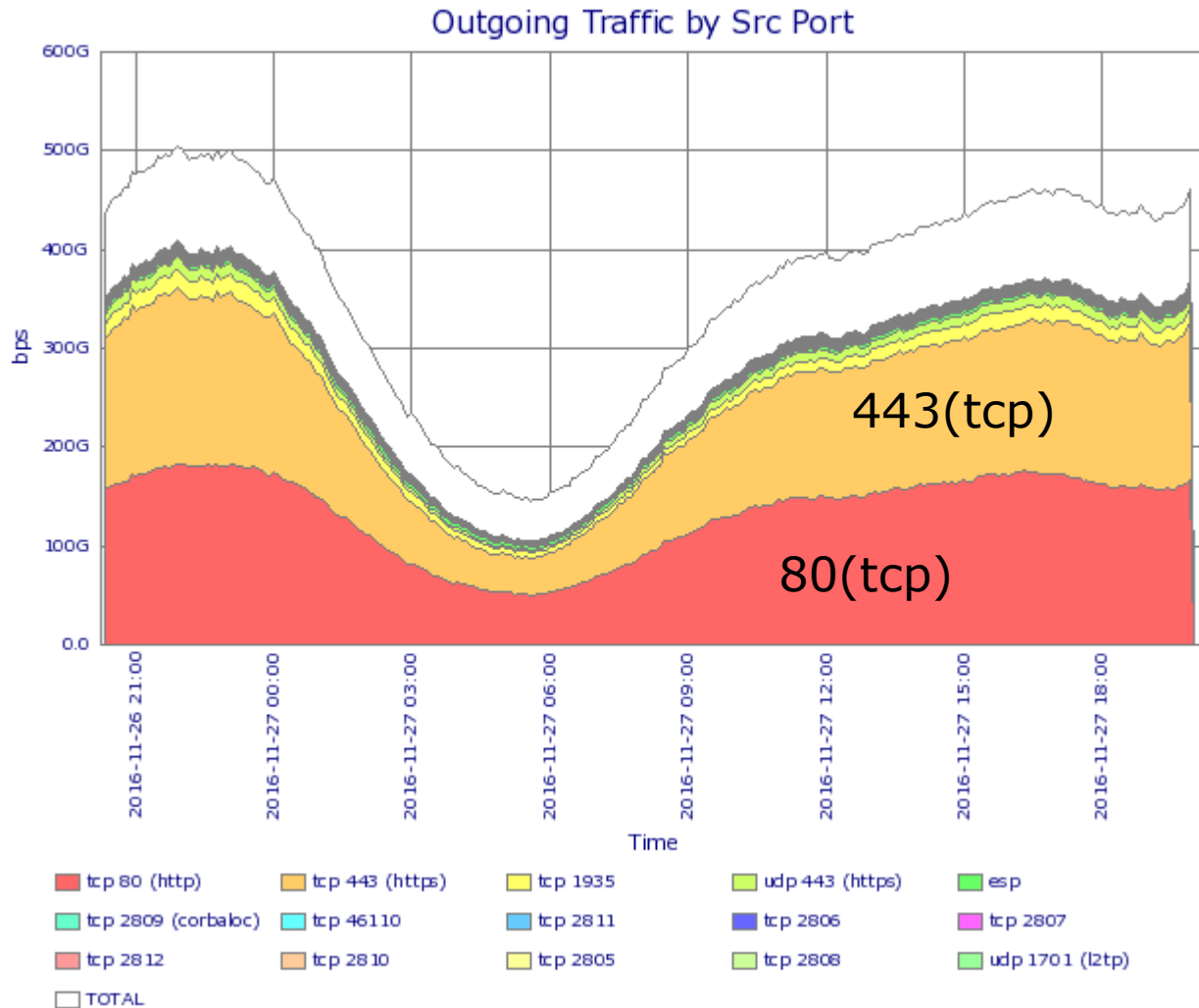
JPNAP全体での利用ポート比率

tcp443の割合がtcp80を完全に逆転



1年前

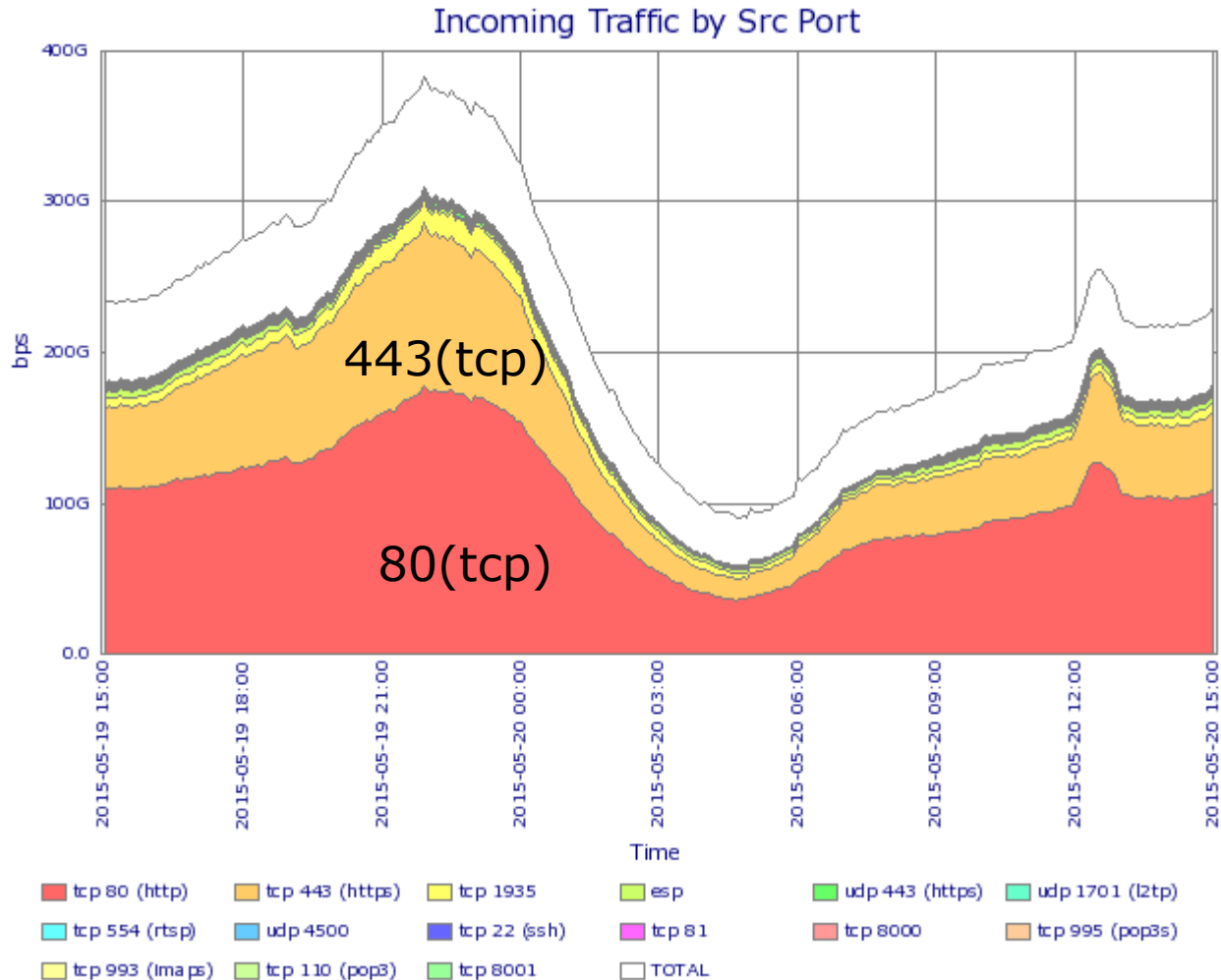
tcp443とtcp80の割合がほぼ一緒程度になってきた



2年前

TCP80の割合が多い

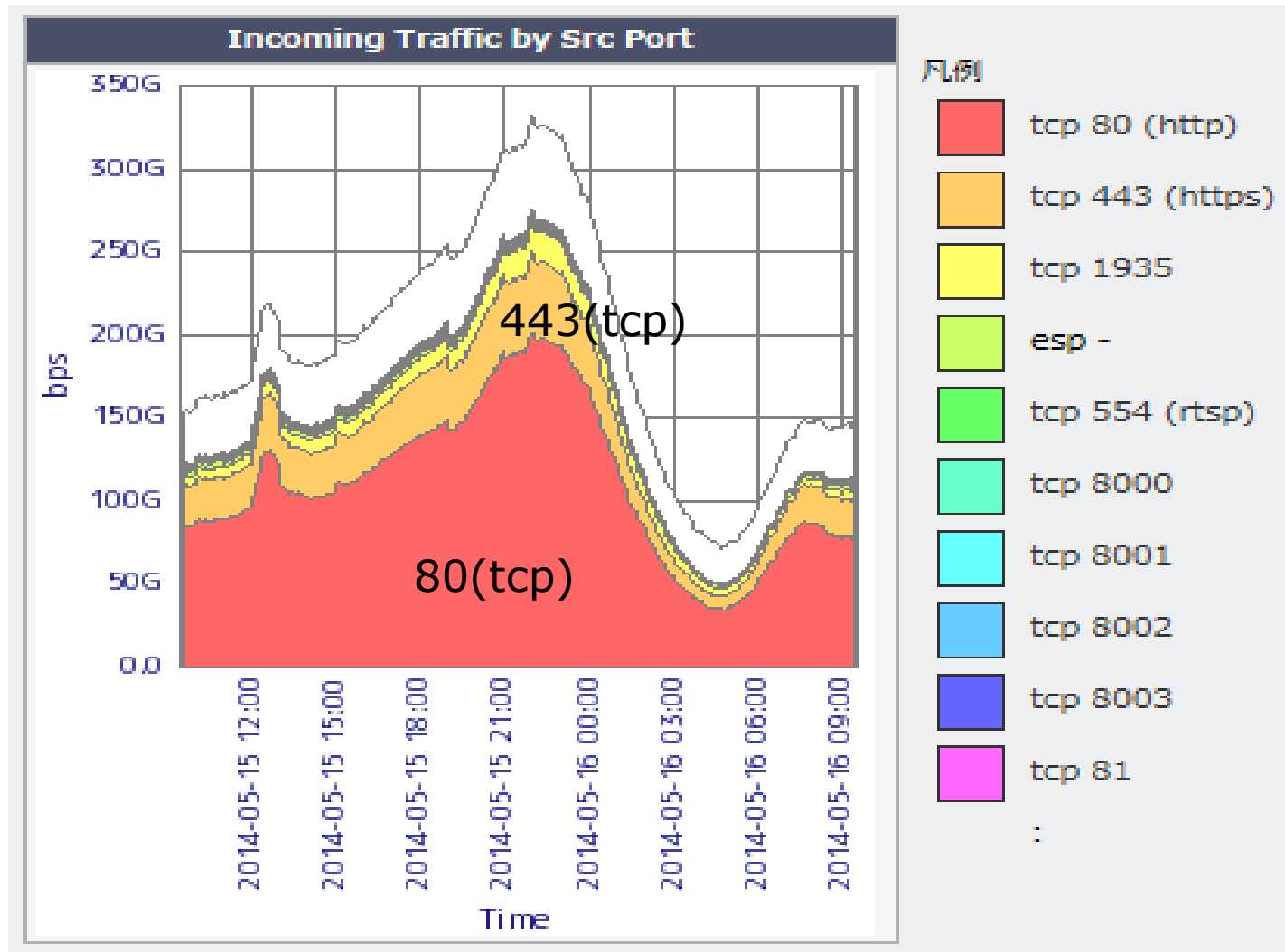
特に早朝帯の人が寝ている時間はTCP80の割合が増加



3年前

約8割はTCP80

2014年～2016年、80->443へのTransitionが顕著に



既に多くのサービスがHTTPS化(2016年以前より)



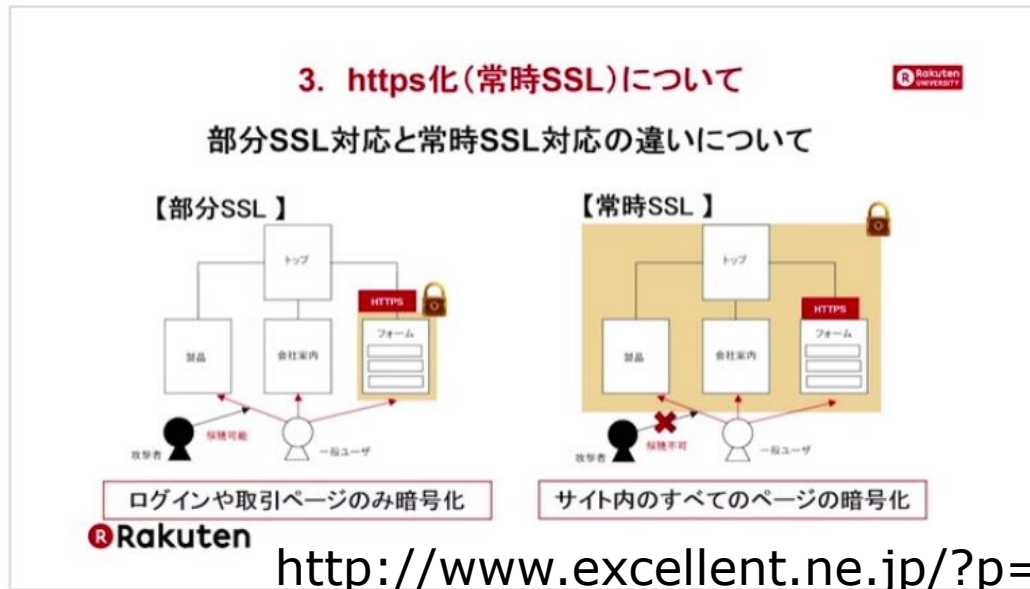
YAHOO!



NETFLIX



今年HTTPS化が本格化された代表的なサービス



これまでは

一部サービスのみ
HTTPS (SSL 暗号化通信) に対応

HTTPS (暗号化)	Yahoo! JAPAN ID 登録情報 メール ウォレット ショッピングカート
HTTP (非暗号化)	天気・災害 ニュース 路線情報 GYAO! 地図 不動産 Sportsnavi ファイナンス

お客様

▲ 覗き見リスク

これからは

すべてのサービスが
HTTPS (SSL 暗号化通信) に対応

HTTPS (暗号化)	Yahoo! JAPAN ID 登録情報 メール ウォレット ショッピングカート 天気・災害 ニュース 路線情報 GYAO! 地図 不動産 Sportsnavi ファイナンス
-------------	---

お客様

※上記のサービスは一例です

<https://about.yahoo.co.jp/info/aossil/>

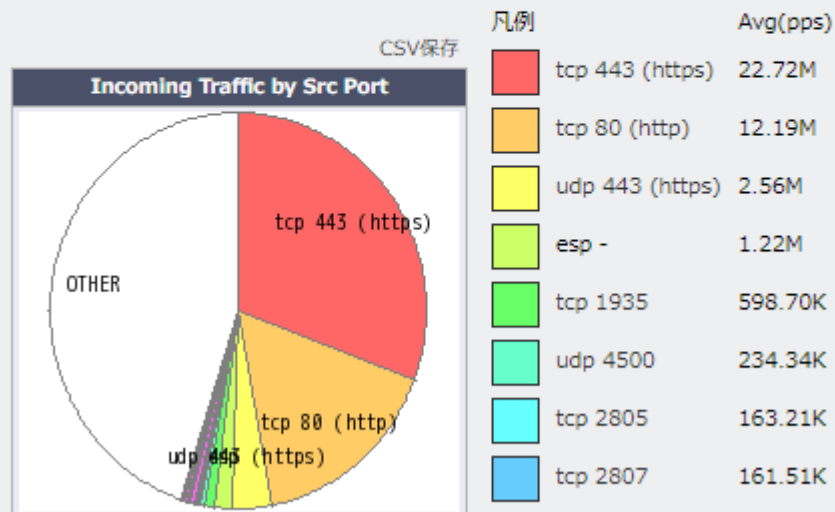
ポート番号推移

2017年、TCP/UDP 443を合算するとHTTPSが約50%

表示概要

ポリシー	IX1
期間	2017-11-16 18:30 - 2017-11-17 18:30(JST)

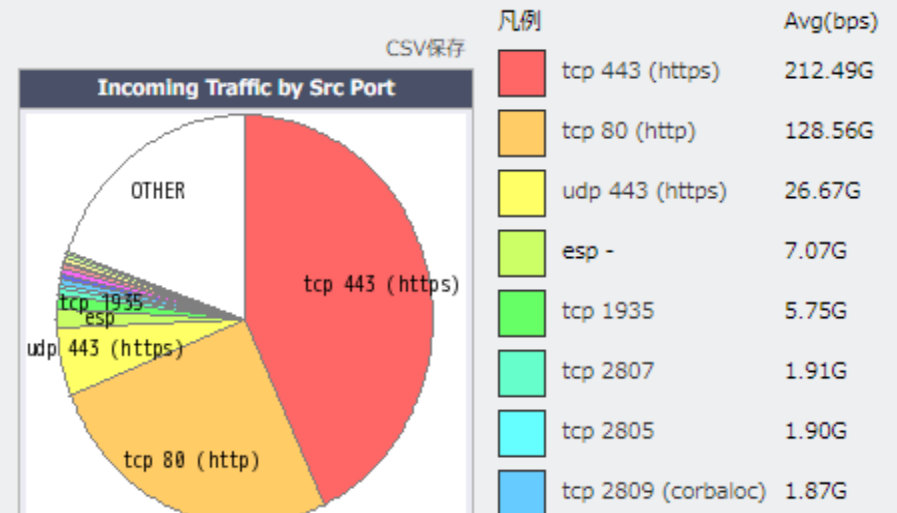
グラフ



表示概要

ポリシー	IX1
期間	2017-11-16 18:30 - 2017-11-17 18:30(JST)

グラフ



HTTPS化の加速

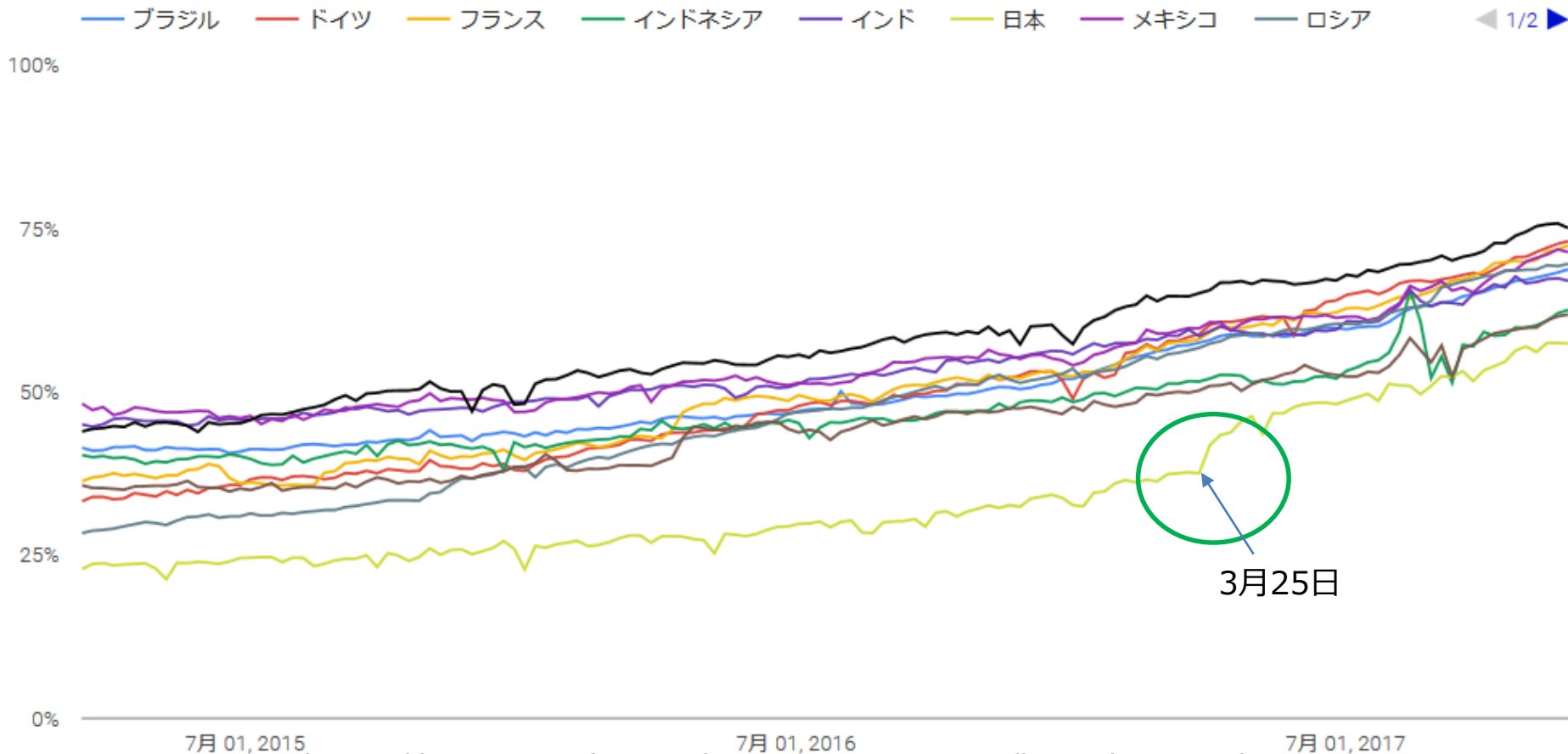
- 通信がセキュアになる
- Google
 - HTTPS 優先でランキング シグナルに反映
- 従来できていたことが困難に
 - ログやデータ解析
 - リファラの取得
- SSLのオーバーヘッド

Chromeユーザーのアクセス状況解析統計結果（透明性レポート）

HTTPSでの通信は日本はまだまだ少ないが、昨年から倍近くに（32%→57%）
特に今年3月より急激に増加（RAKUTEN、Yahooの影響と考えられる）

Chrome で HTTPS 経由で読み込まれたページの割合（国別）

Windows



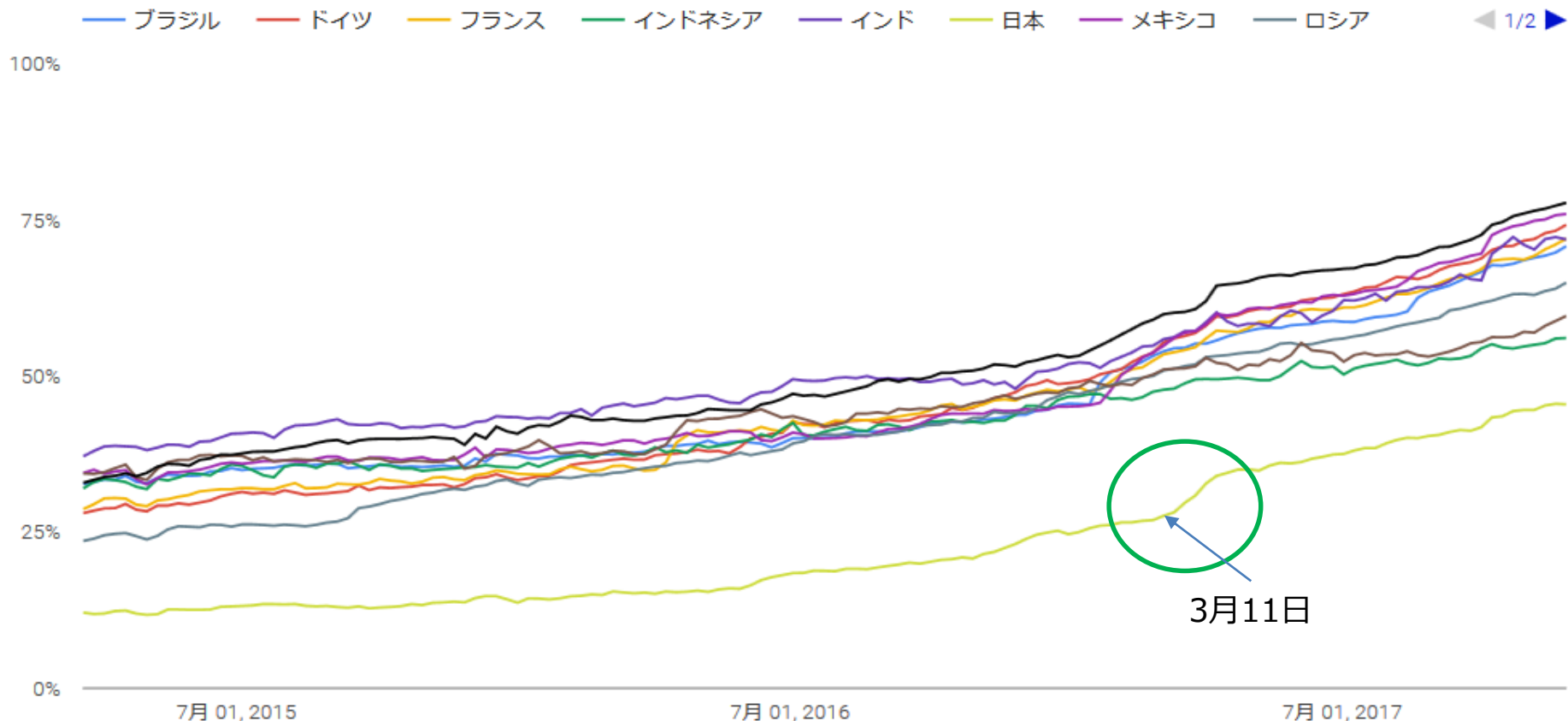
<https://www.google.com/transparencyreport/https/metrics/>

Chromeユーザーのアクセス状況解析統計結果（透明性レポート）

HTTPSでの通信は日本はまだまだ少ないが、昨年から倍に（23%→45%）
特に今年5月より急激に増加（RAKUTEN、Yahooの影響と考えられる）

Chrome で HTTPS 経由で読み込まれたページの割合（国別）

Android



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

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、日本固有のサイトが多い中、徐々に外資系サイトの勢いが大きく

Top10にランクインしている **Yahoo, Rakuten**が2017年に本格的にHTTPS対応を実施したため、日本のHTTPS化が加速化

他、Nicovideo, Kakaku.comは未対応。 **Ameblo, Naver**はHTTPS対応済み

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	昨	GLOBAL	昨
1	Google.co.jp	1	Google.com	1
2	Google.com	3	Youtube.com	2
3	Youtube.com	4	Facebook.com	3
4	Yahoo.co.jp	2	Baidu.com	4
5	Amazon.co.jp	5	Wikipedia.org	6
6	Facebook.com	7	Yahoo.com	5
7	Nicovideo.jp	9	Google.co.in	7
8	Twitter.com	8	Reddit.com	-
9	Rakuten.co.jp	10	Qq.com	8
10	Wikipedia.org	11	Taobao.com	9
11	Fc2.com	6	Amazon.com	10
12	T.co	13	Tmall.com	21
13	Baidu.com	17	Twitter.com	14
14	Kakaku.com	18	Vk.com	13
15	Livedoor.com		Live.com	12
16	Ameblo.jp	14	Google.co.jp	11
17	Amazon.com	-	Instagram.com	15
18	Qq.com	-	Sohu.com	17
19	Livedoor.jp	12	jd.com	-
20	Instagram.com	-	Sina.com.cn	18
21	Tmall.com	-	Weibo.com	22
22	Yahoo.com	-	360.cn	19
23	Taobao.com	-	Google.de	23
24	Naver.jp	15	Google.co.uk	24
25	Reddit.com	-	Google.com.br	-

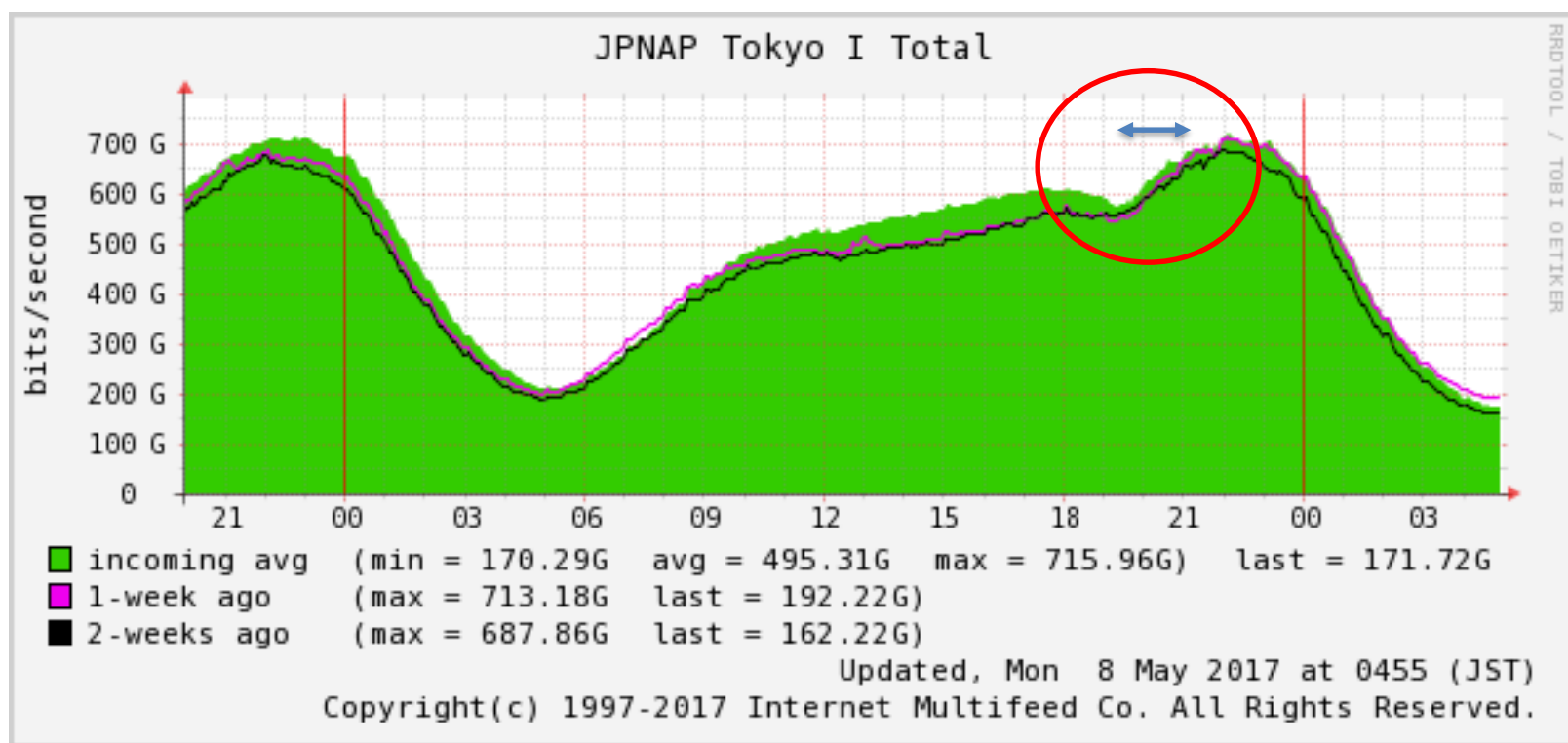
トラフィックの変化要因とトレンド

- イベントトラフィックによる変動
 - 自然災害
 - 2017年は大きな地震発生はなかったので主だった変動は見られなかった
 - 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
 - APPLE IOS update
 - Microsoft Windows update
- 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があったが、ここ最近ではCDNを自前化する傾向があり多少改善（後述）
- 何が異常で何が正常かの見分けが困難に
 - 昔ほど気にしない時代になってきた？
 - 制御も含めてAIに任せる時代？

亀田興毅に勝ったら1000万円 (5/8日)

AbemaTV史上、視聴数歴代最高記録 (延べ1420万回)

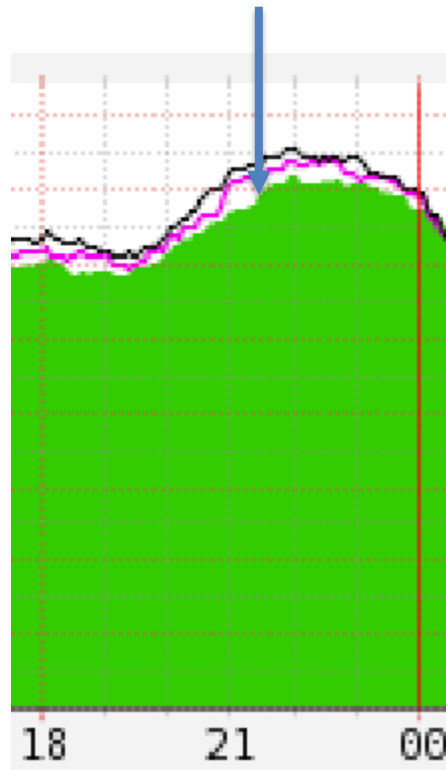
第一試合開始の19時40分頃～第2試合終了の21時頃まで一時サーバがダウン



提供：JPNAP東京のトラフィックグラフより

AKB総選挙(6/17土)

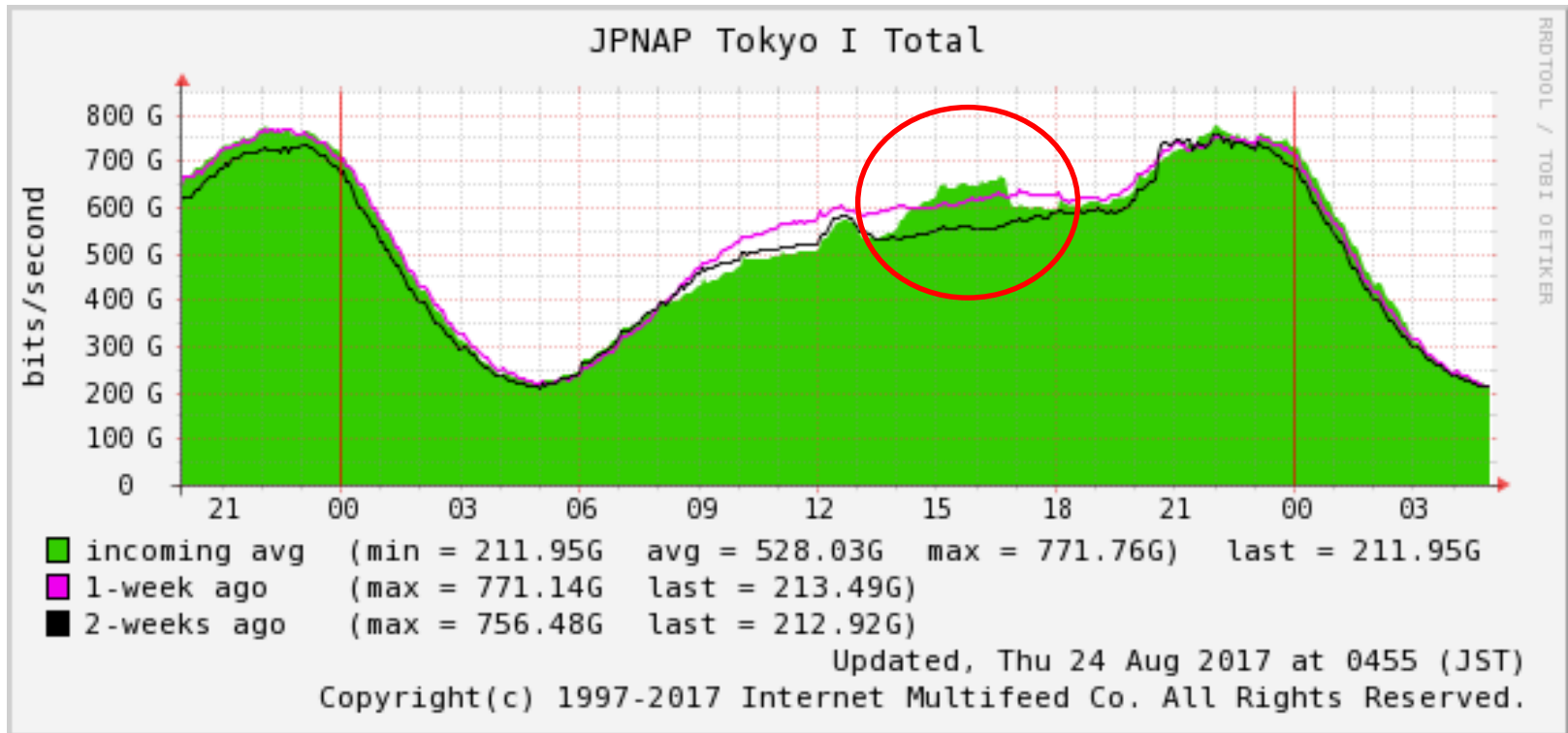
21時24分放送終了後から少し伸びているようにも見える



提供：JPNAP東京のトラフィックグラフより

甲子園決勝(8/23水)

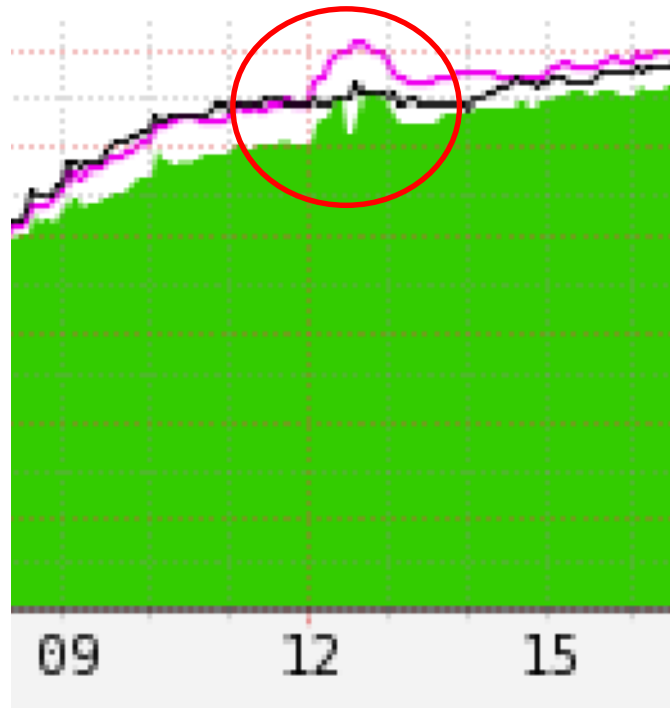
14時試合開始、16時55分より閉会式 皆さん仕事してましたか？



広陵 (広島) 4 - 14 花咲徳栄 (埼玉)

提供：JP NAP東京のトラフィックグラフより

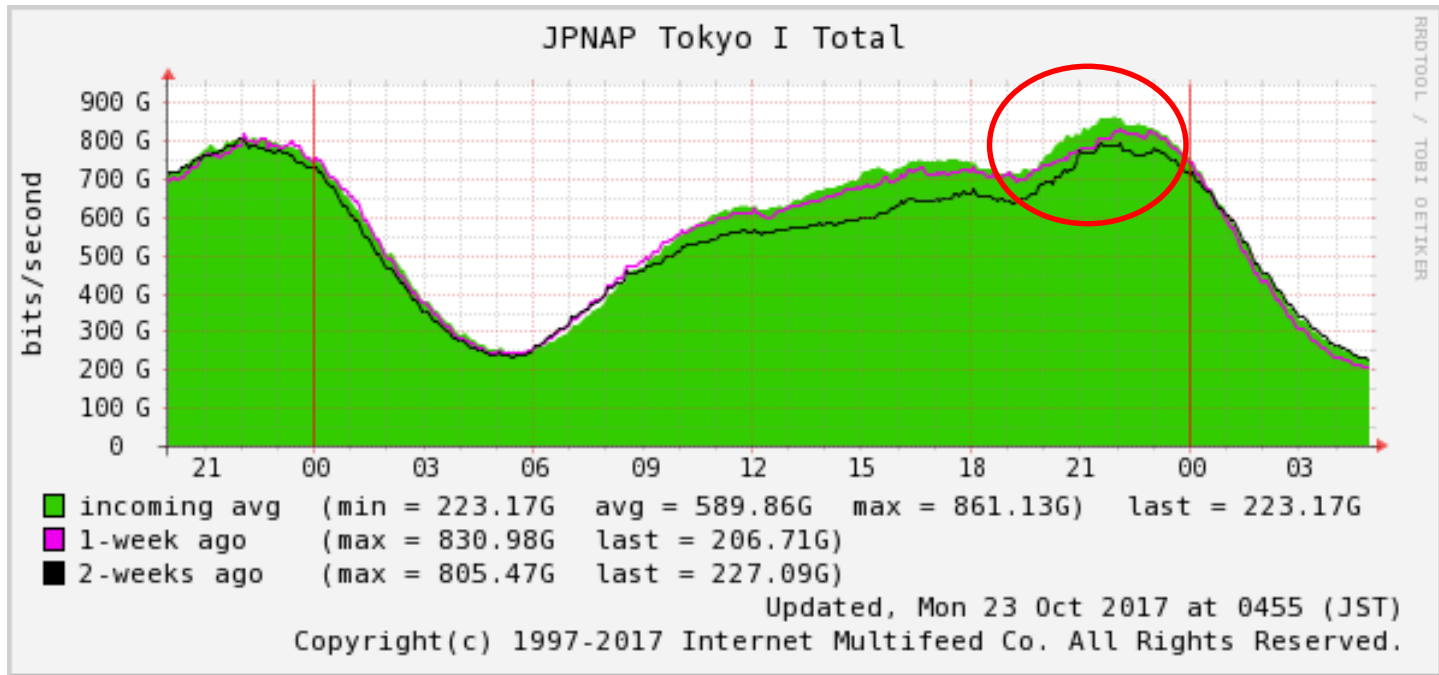
Google障害(8/25金)



提供：JPNAP東京のトラフィックグラフより

衆議院選挙(10/22日)

20時の開票開始前後よりネットトラフィックが22時頃まで増加



提供：JPNAP東京のトラフィックグラフより

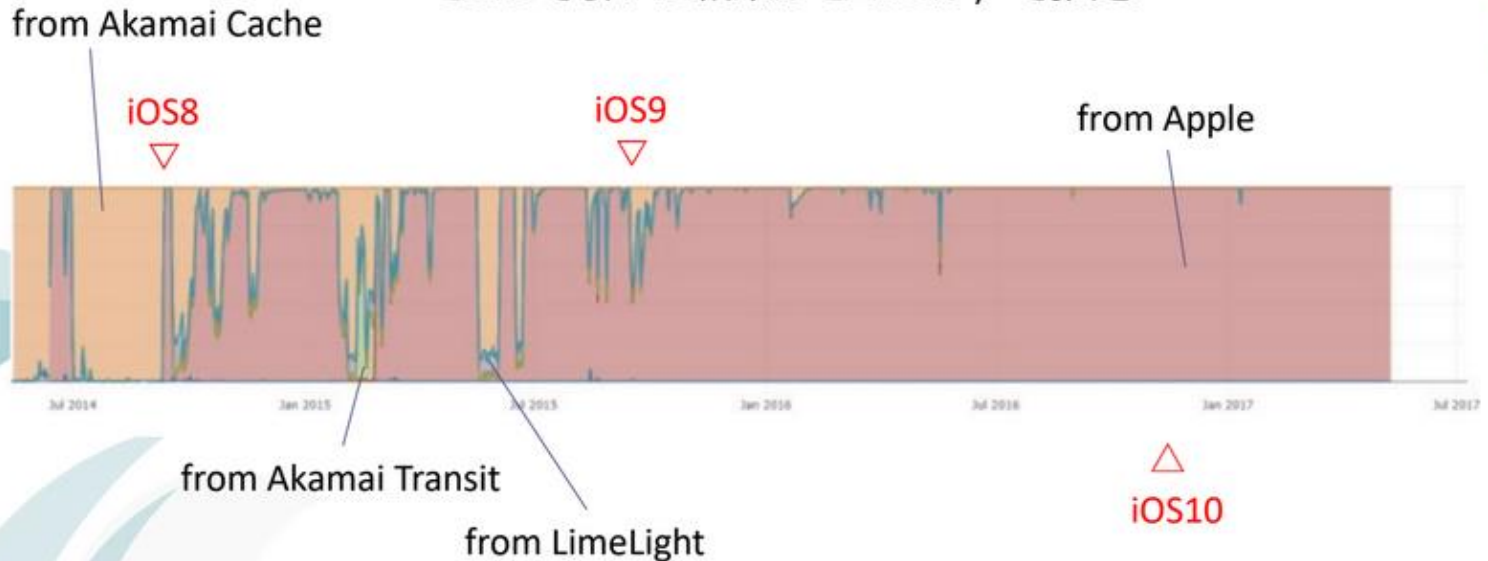
iOS{8,9,10}の各社向け配信状況

過去はCDN配信に大きく依存していたのが、IOS10ほぼAppleだけで配信可能に

15

Apple(iOS配信)でのCDN利用状況

あるISPからiOSのアップデートが載ってるFQDNをDNSで引いた結果がどのASか、で推定。



普段は自前ASから配信し、混雑時(iOS配信時等)はCDNを併用。

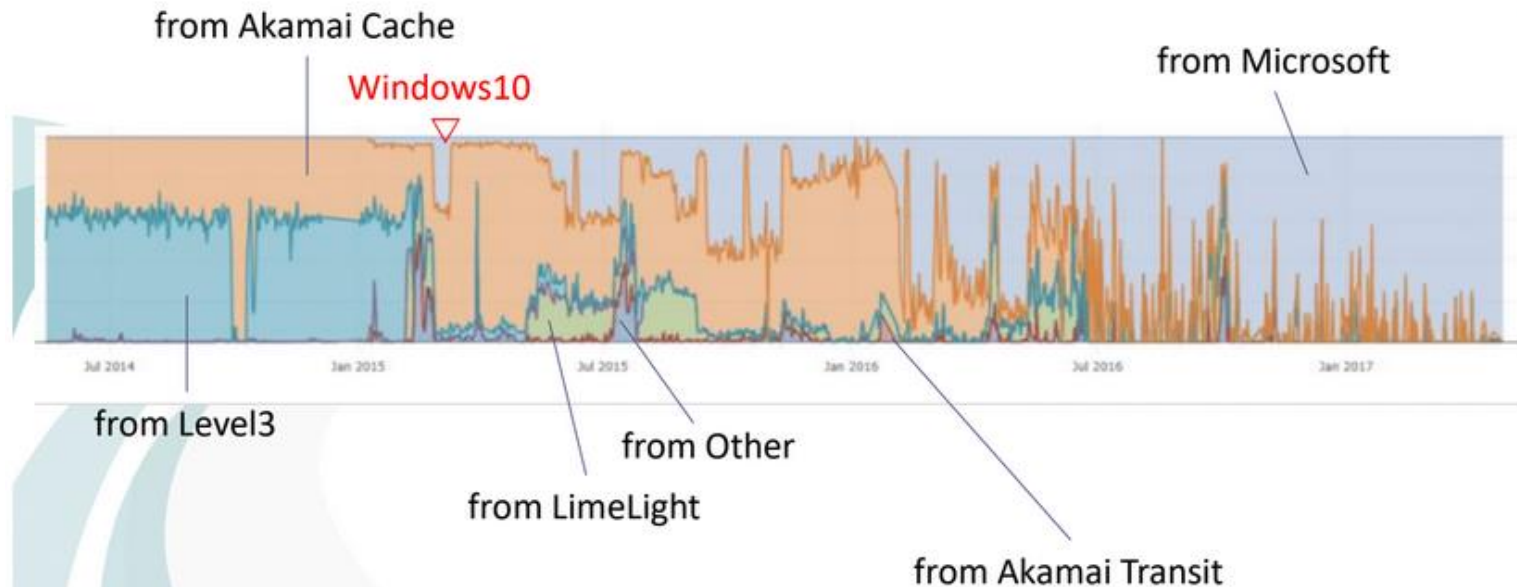
Windows Update の状況

AppleのIOS10ほどでは無いが、自前のCDNからの配信傾向がより顕著になってきた

16

Windows Update での CDN 利用状況

マルチCDNから自前化？



アプリケーションとNWの関係

- **特定のアプリケーション（サービス）が通信や人の生活を変える**
- **アプリケーションの作り次第でネットワークの使い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
- **ネットワークデバイスの増加と多様化によりここ、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気にせず本気で使いたおしていく時代へ
- **アプリ（サービス）とネットワークの相互理解が重要**
 - 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にならないよう配慮が重要
 - 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らないように

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

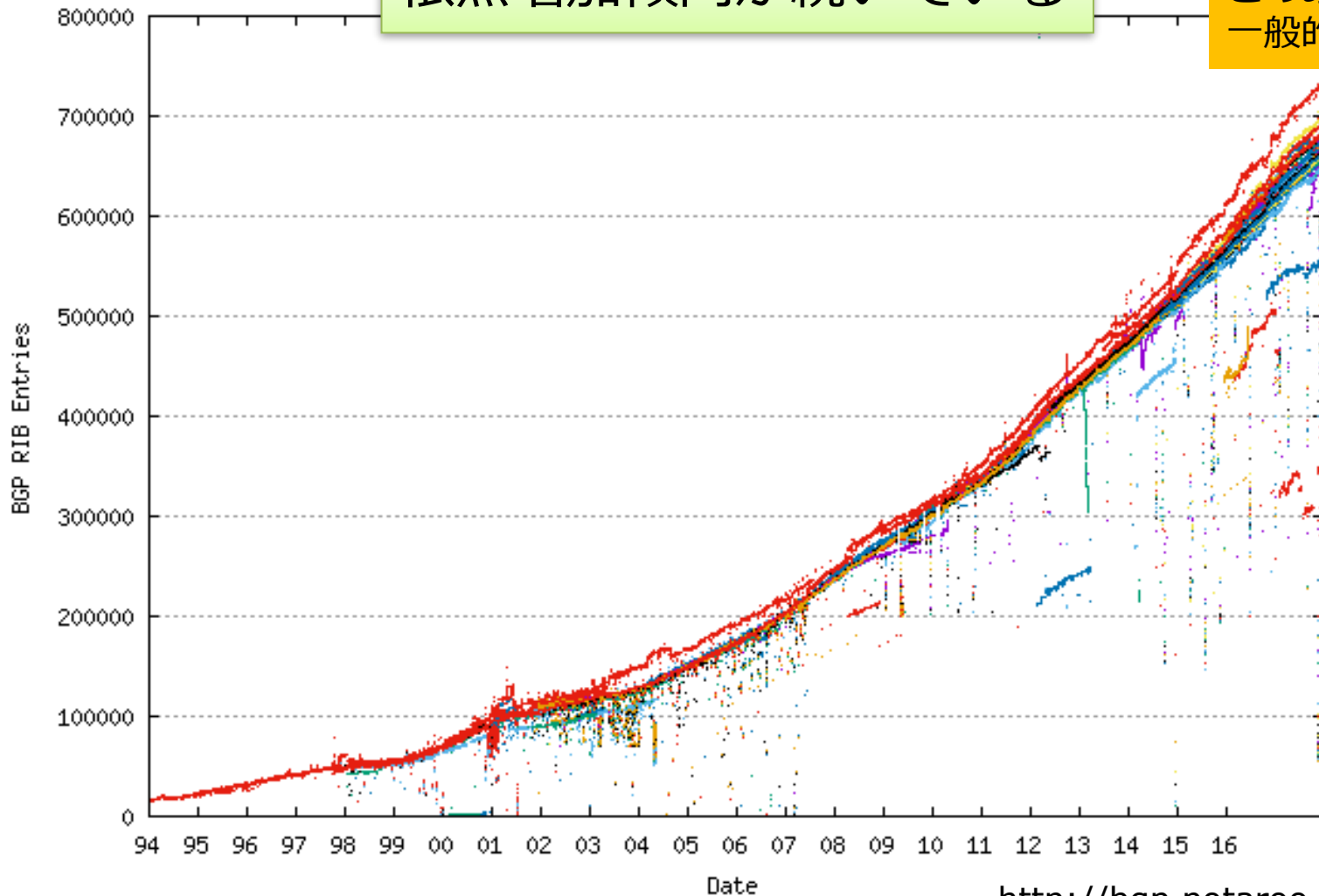
ルーティング動向

- IPv4経路が**67万～68万**に到達
 - 年増加率は**約1.08倍**で伸び率は減少へ
 - 返却済みアドレスの追加割振が2016年比で90%大幅減の影響大か？
 - **/24は依然全体の半分超**で、継続的に増加し続けている
 - **残るはLACNIC地域の在庫枯渇が2018年1月の予想**
- IPv6経路は約4万3千経路に
 - **年間で約9,000-10,000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に注意が必要**
 - /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+IPv6 FIBとして要考慮）
- 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、日本での普及はまだ低迷
 - 但し2015年～2016年と比較すると徐々に増加（約半分は4byte割り当て）

IPv4経路数の推移

依然増加傾向が続いている

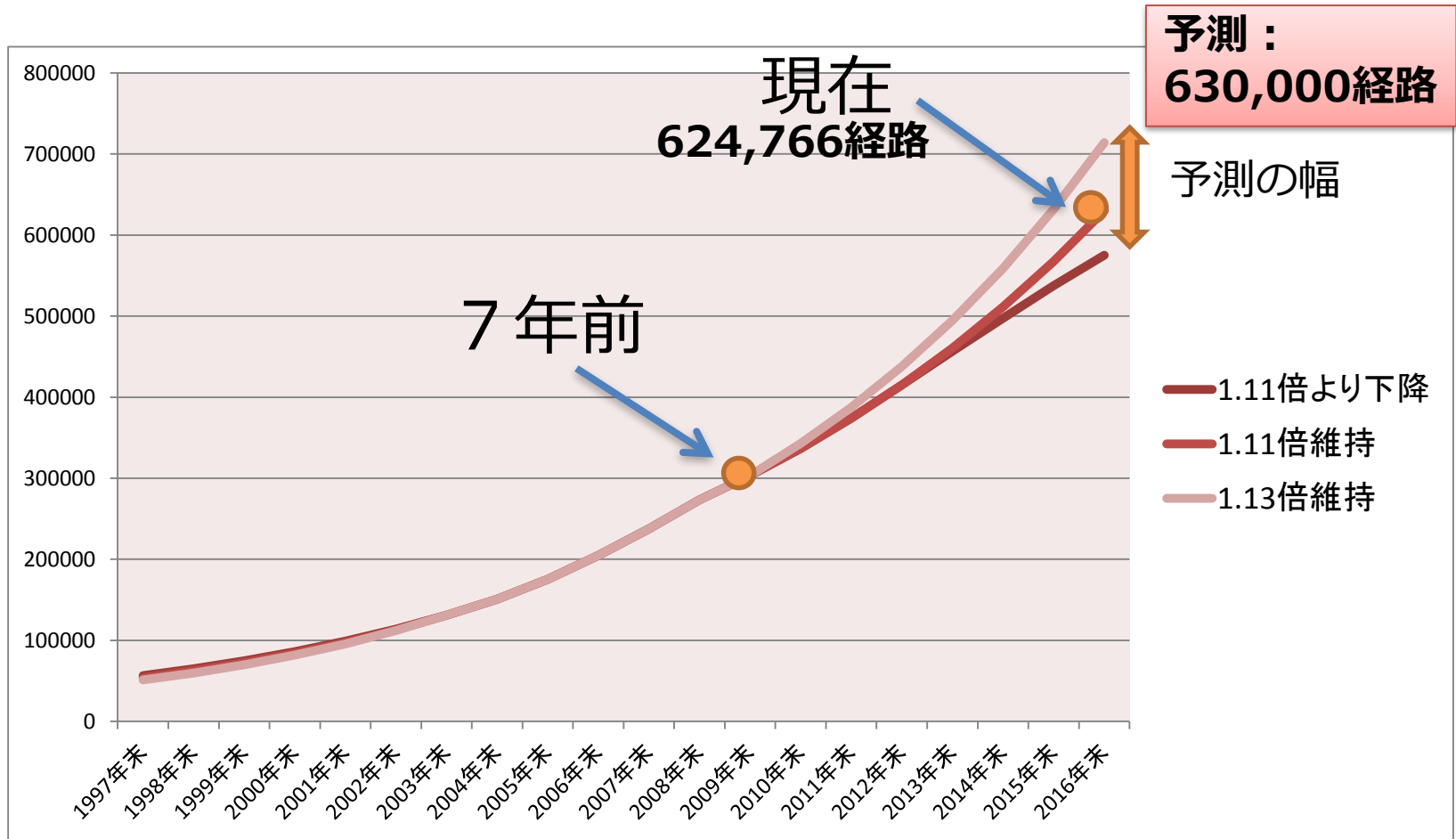
このあたりが
一般的な経路数



<http://bgp.potaroo.net/>

IPv4経路数推移予測1.0

(8年前の2009年時点での2016年末予測)



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

16000

14000

12000

10000

8000

6000

4000

2000

0

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

2017末 : 671033

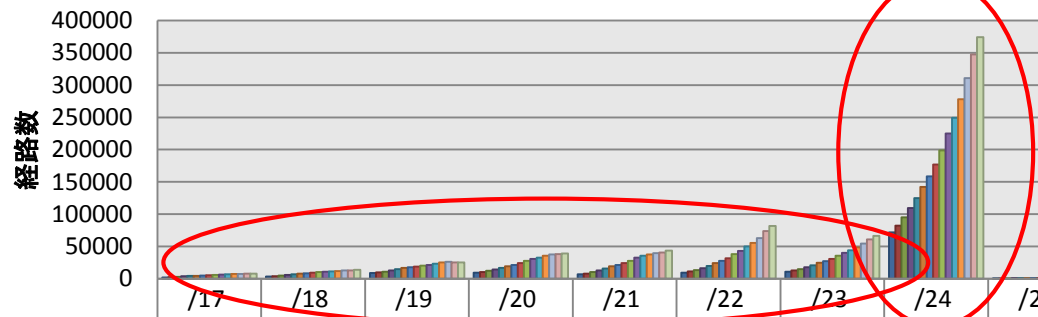
/11~/16も微量ながら増加だが、
短いprefixは今後顕著には増加し
ない傾向に見える

	/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
■ 2017末	0	0	0	0	0	0	0	15	13	36	106	285	550	1060	1856	13336

IPv4経路数の推移

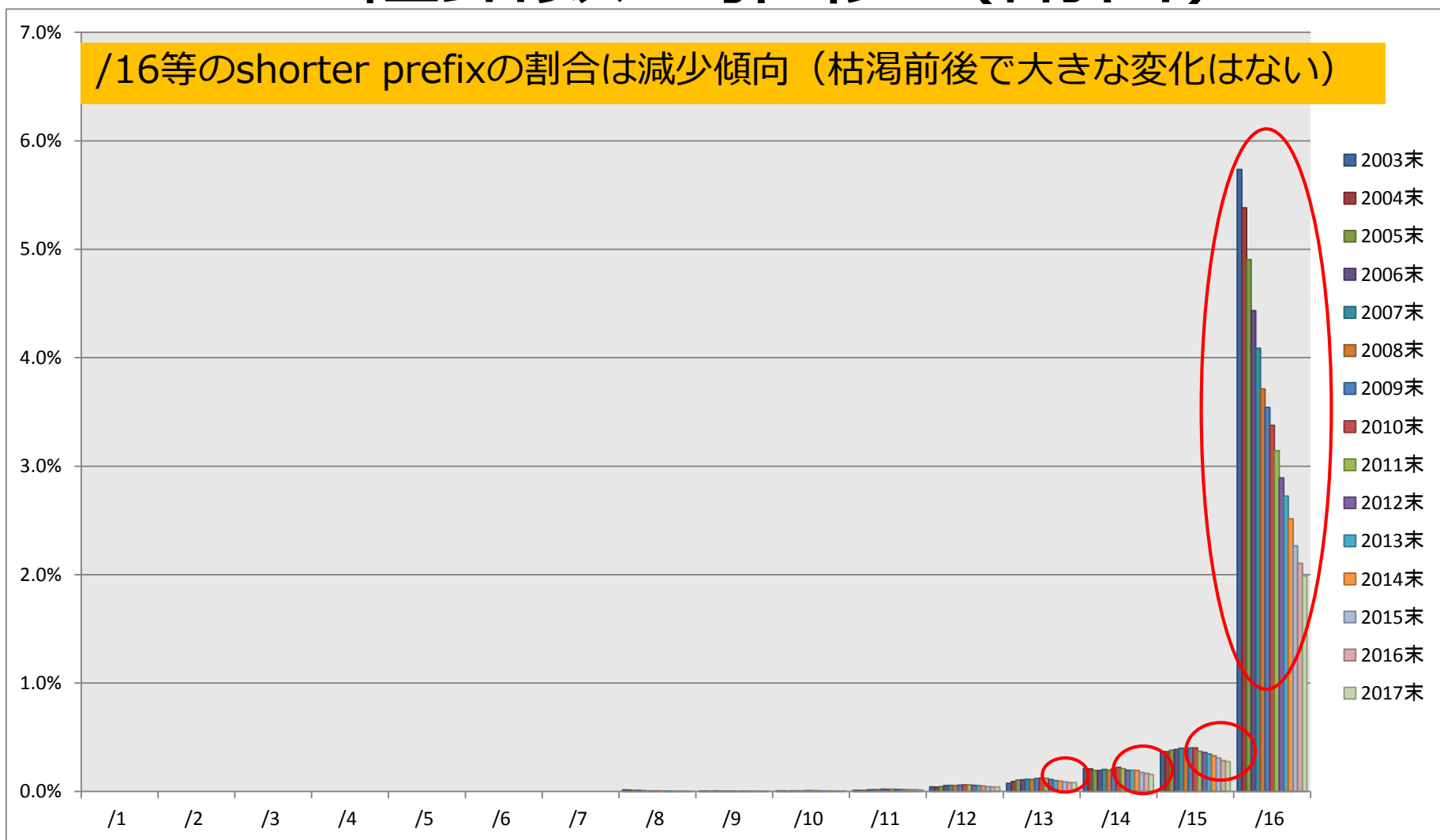
/24は依然増加するも2016年より少し緩やかに増加

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
2017末：671033

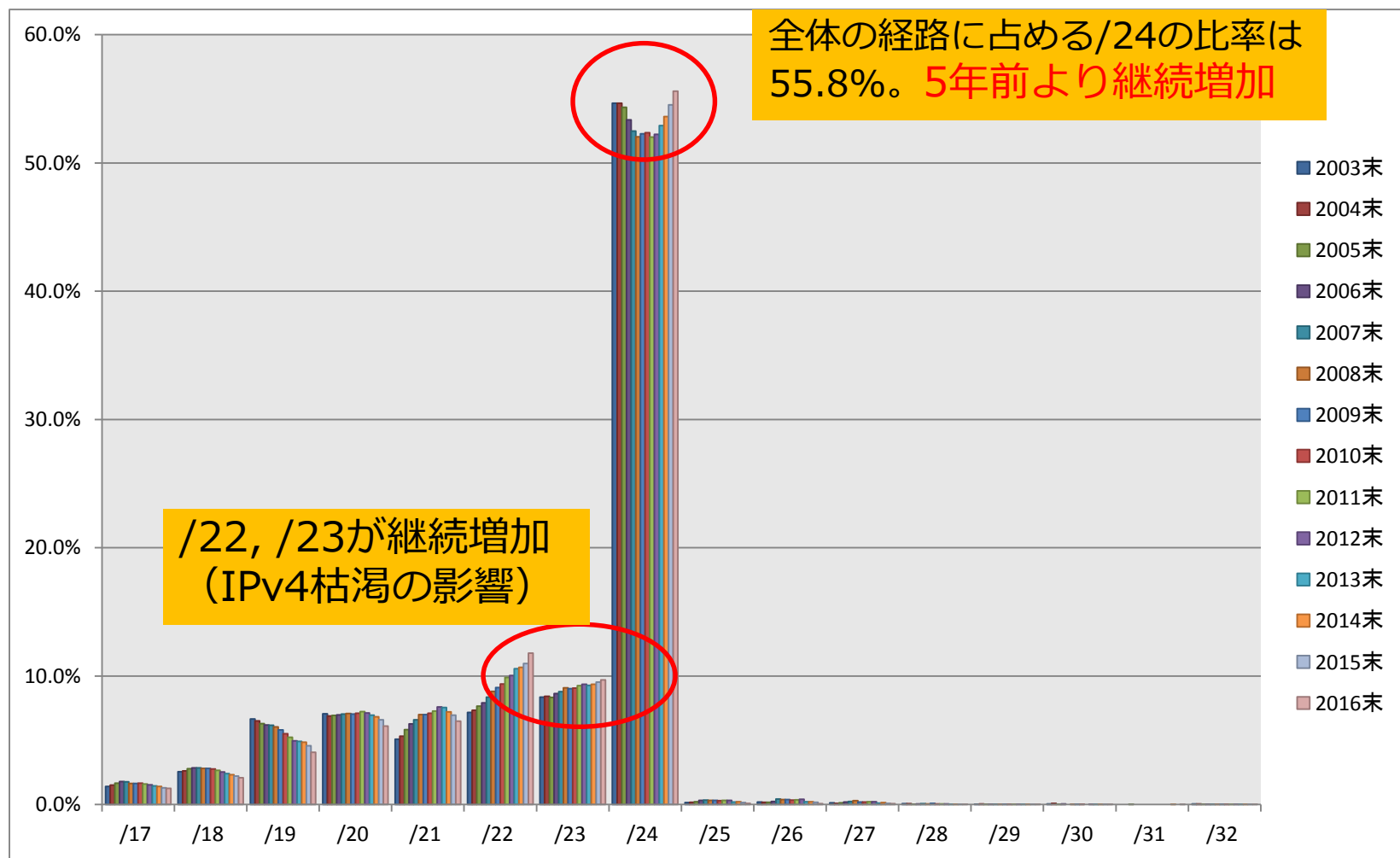


	/17	/18	/19	/20	/21	/22	/23	/24	/25	/26	/27	/28	/29	/30	/31	/32
■ 2003末	1829	3334	8716	9249	6656	9386	10943	71541	182	233	156	70	21	50	0	41
■ 2004末	2270	3933	9818	10402	8007	11066	12707	82382	252	239	130	69	54	120	0	40
■ 2005末	2880	4871	11026	12142	10194	13440	14626	95225	345	292	194	26	12	36	3	30
■ 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
■ 2017末	7754	13617	25184	38959	43744	81587	66378	374339	840	622	652	35	21	15	2	27

IPv4経路数の推移（割合）



IPv4経路数の推移 (割合)

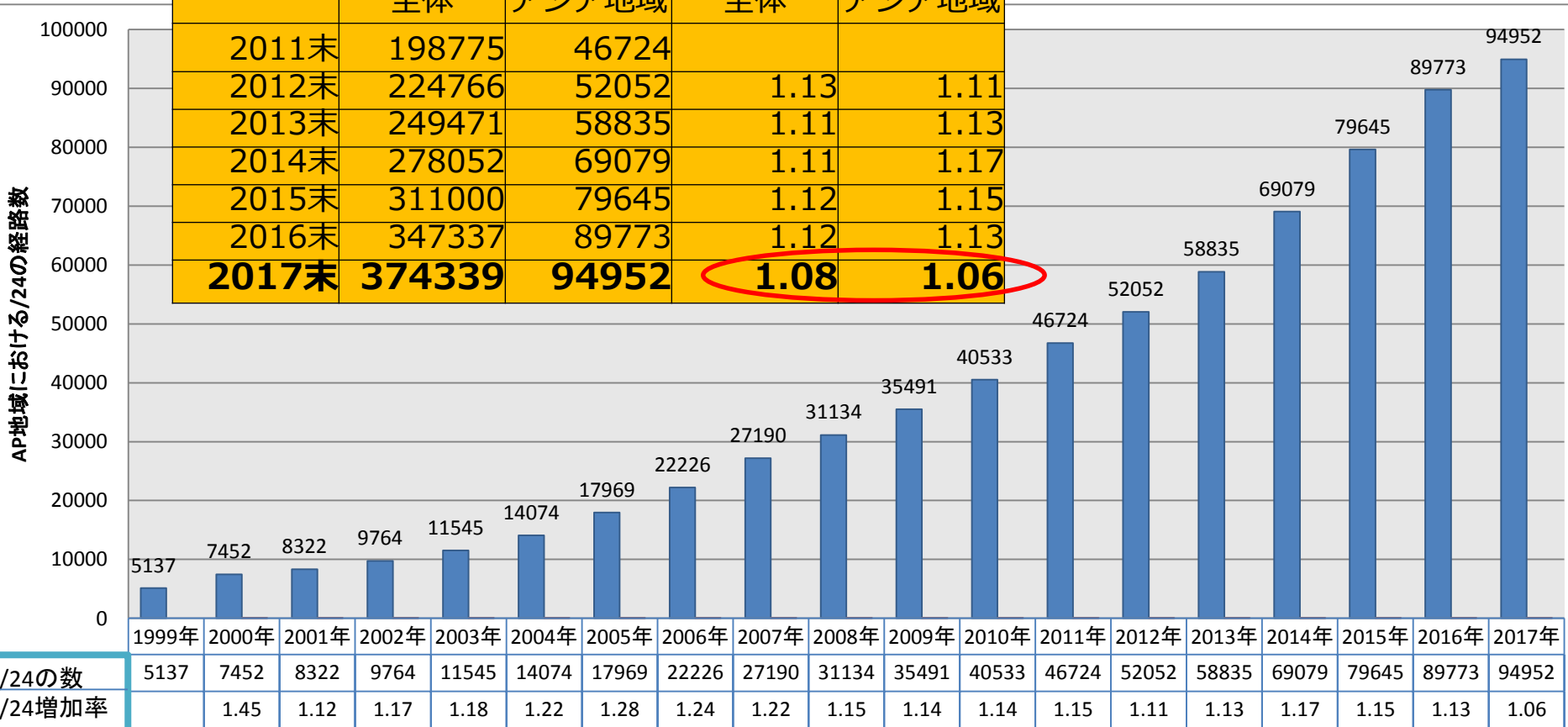


AP地域の/24の推移

AP地域の/24増加率が約20年の統計上で初めて1.10倍率を下回る

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
2017末	374339	94952	1.08	1.06

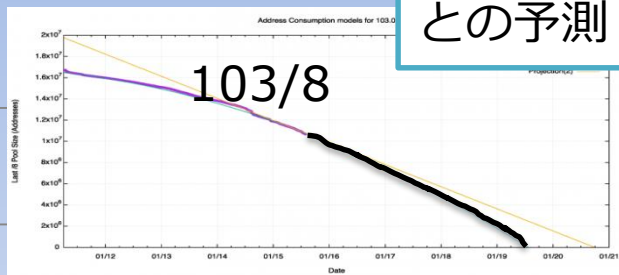


AP地域の/24の推移

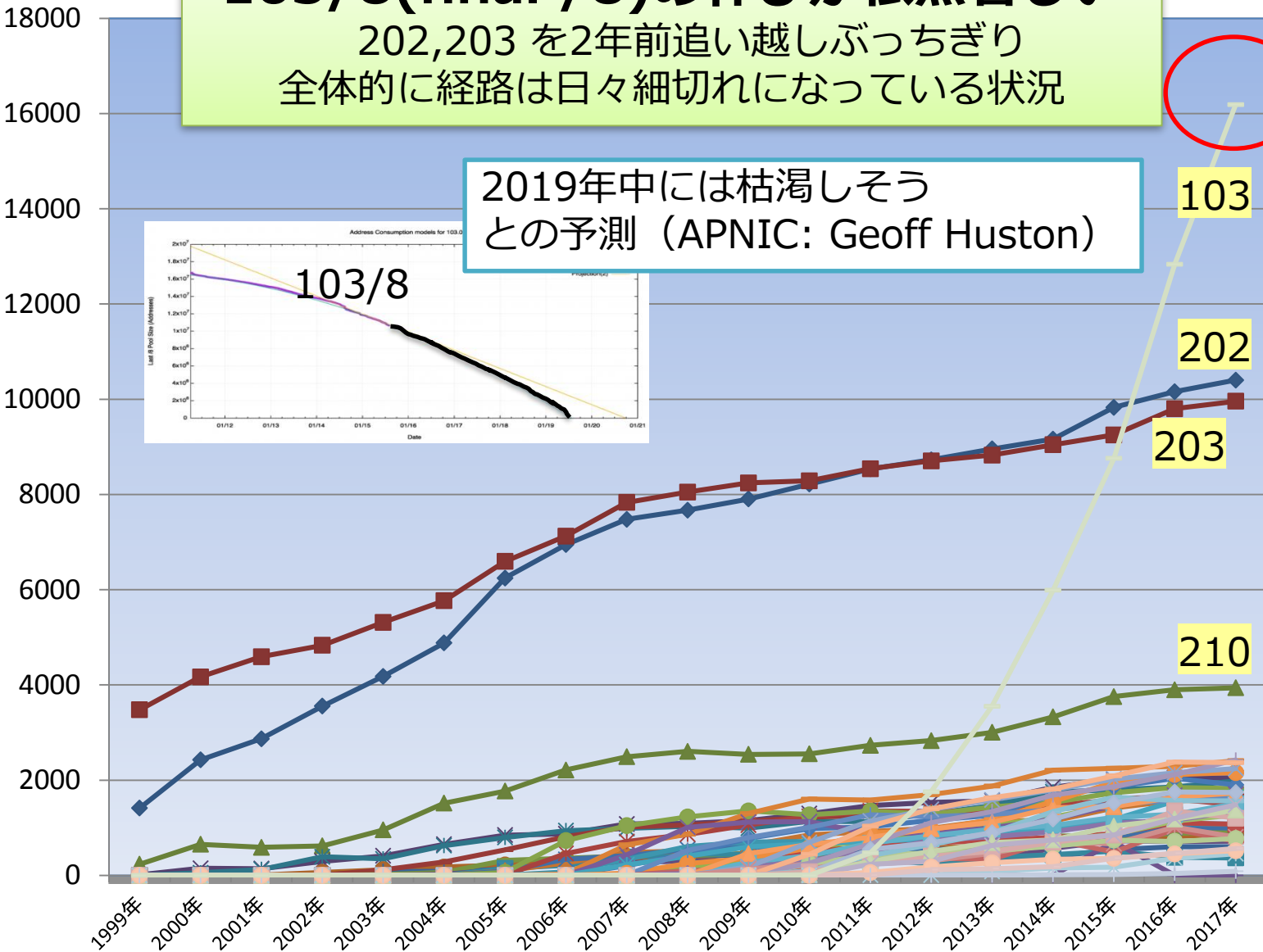
103/8(final /8)の伸びが依然著しい

202,203 を2年前追い越しぶっちぎり
全体的に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)



- ◆ 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掲載のブローカーリスト

Registered IPv4 brokers

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	michaelandrewburns
IPv4 Market Group LLC	US	Sandra Brown	+1 855-880-5906	
The Kalorama Group	US	Josh Bourne	+1 202-499-4422	
Hilco Streambank	US	Jack Hazan	+1 212-610-5663	2013年に追加
V4ESCROW, LLC	US	Elvis Daniel Velea	+1 702-475-5914	elvisvelea
v4Now	AU	Skeeve Stevens	+61-2-8014-7398	2014年に追加
IPv4 Xchange, LLC	US	Mickey Mullins	+1-718-764-6775	IPv4Xchange
Avenue4 LLC	US	Marc Lindsey	+1-202-741-9521	
Maxtel Holdings, LLC	US	M Feras Bakkour	+1-323-870-4858	Feras2 2016年に追加
PT. ARSEN KUSUMA INDONESIA	ID	Bayu B Megananda	+62-21-7918-4484	
Guangzhou data union Mdt InfoTech Ltd	CN	Wang Yu Feng	+86-138227771183	2017年に追加
Silicon Desert International (dba IPv4 Depot)	US	Marcus Mamolen	+1-602-456-4831	IPv4 Depot

<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。2017年11月時点の状況 (新規追加分より抜粋)
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

104	/16 + /17	PK	8 Feb 2019	Contact	IPv4アドレスを 提供可能な人は 直接コンタクトが可
107	/16	HK	22 Feb 2019	Contact	
117	/16	HK	22 Sep 2019	Contact	
119	/16	MV	11 Oct 2019	Contact	
122	/16	SG	10 Nov 2019	Contact	

<https://www.apnic.net/manage-ip/manage-resources/transfer-resources/listing/> URLが2017年に変更

APNIC事前承認済みのrequest（2016年抜粋）

IPv4アドレスを買いたい人リスト。2016年11月時点の状況
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
→1年以上経過したが、いまだにリストに掲載されている。。

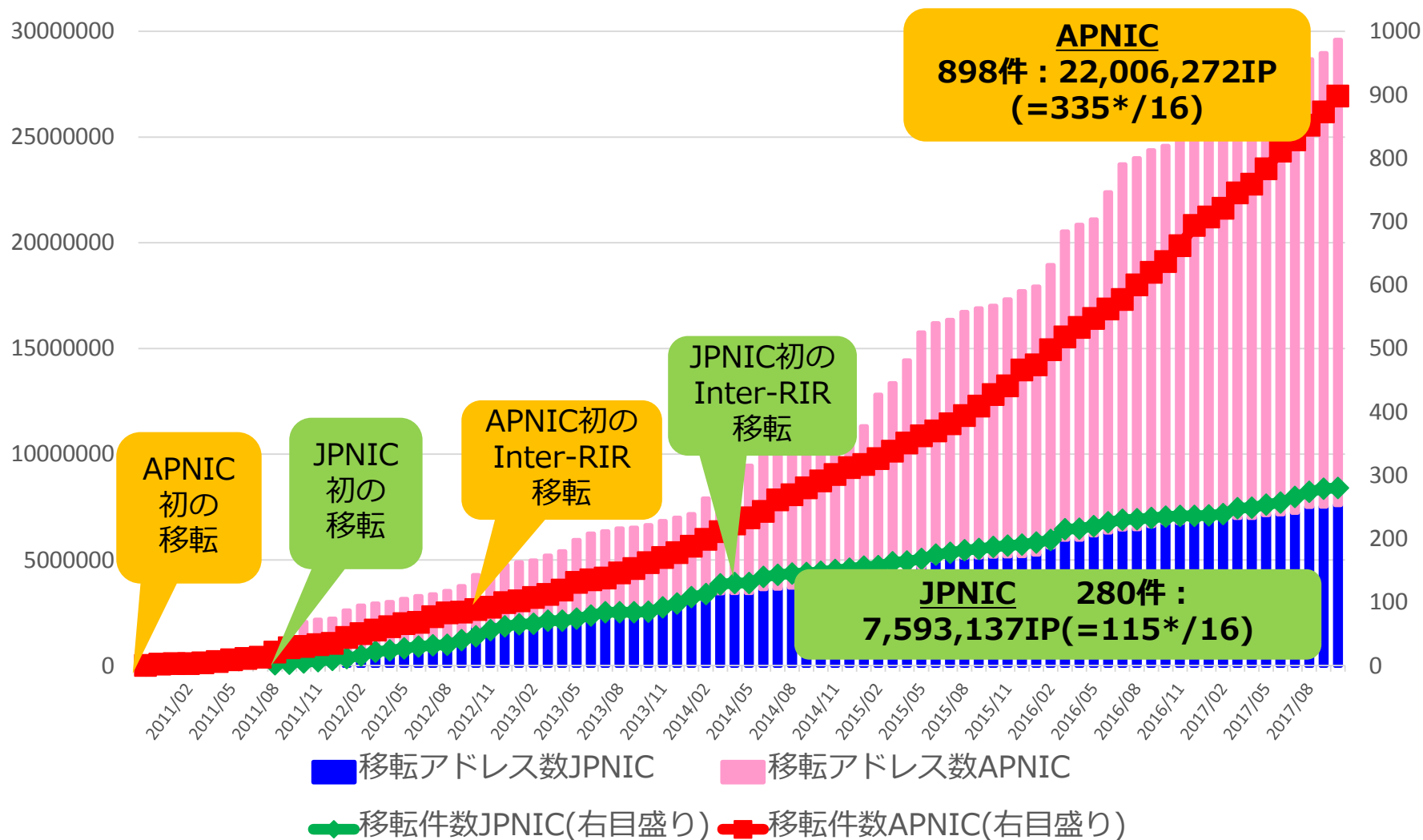
72	/11+/12+/14	SG	15 Dec 2017	Contact
78	/14	SG	8 Jan 2018	Contact
94	/14	HK	12 Aug 2018	Contact
95	/16	HK	16 Aug 2018	Contact
96	/14	PK	6 Sep 2018	Contact
99	/15	PK	27 Oct 2018	Contact

<https://www.apnic.net/manage-ip/manage-resources/transfer-resources/listing/> URLが2017年に変更

日本のIPv4アドレス移転状況

- 2017年11月現在282件(去年+47 2年前+38)
 - 申請件数は微増ながら増加傾向、大きなサイズは国際移転が中心
- 国際移転も50件 (去年+17)
 - 他レジストリ→JPNIC : 44件
 - JPNIC→他レジストリ : 6件
- 移転の理由
 - 純粹にIPv4アドレス不足のケースが断然多い(特にCATV事業者)
 - 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/transfer/ipv4-log.html>
- JPNICによるlisting serviceが2015年12月開始
 - 現在1件掲載 (昨年2016年は3件掲載)
 - <https://www.nic.ad.jp/ja/ip/transfer/wishlist.html>
- AS番号の移転5件 (去年+1)

APNIC地域と日本の移転状況比較

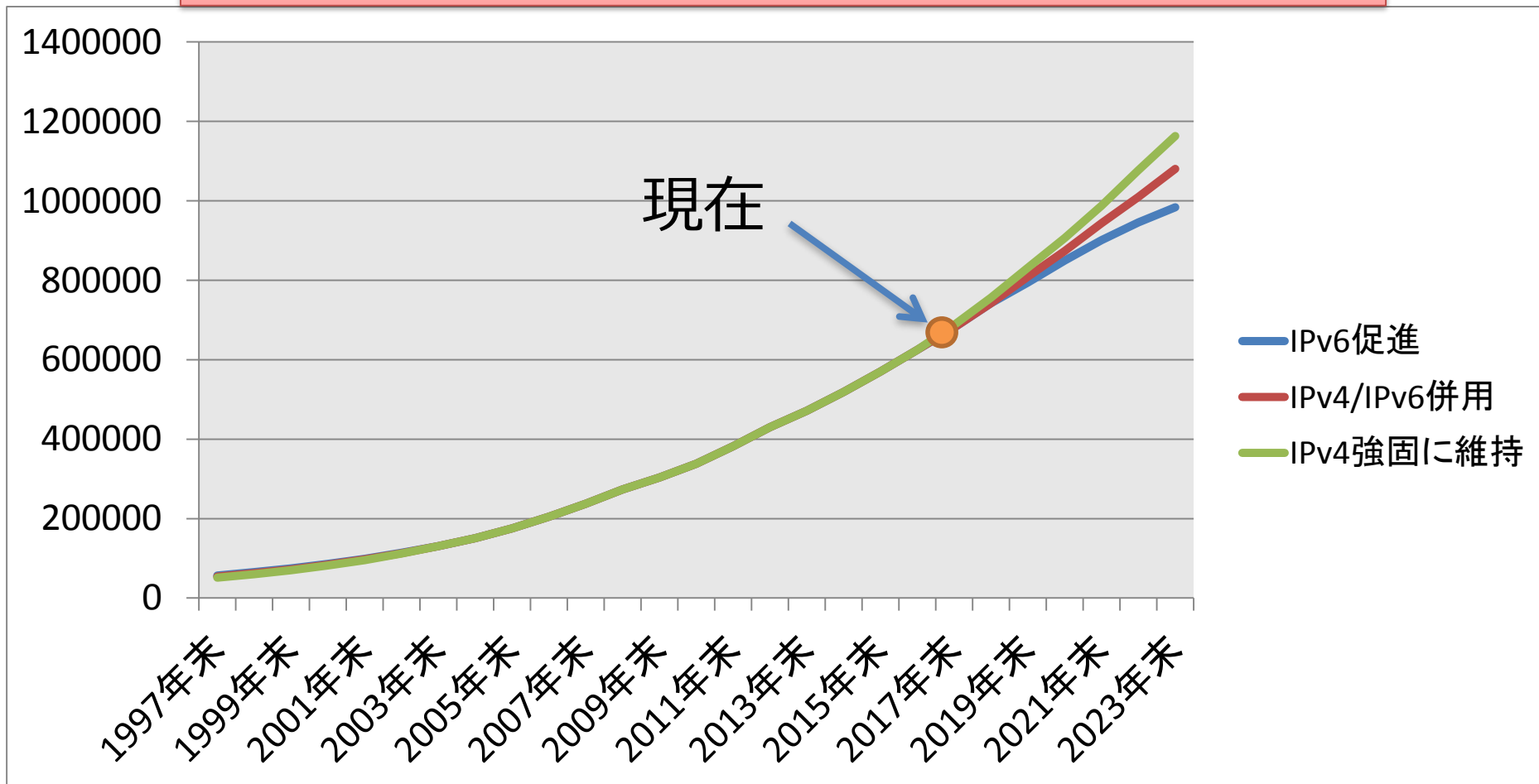


ftp://ftp.apnic.net/public/transfers/apnic/
<https://www.nic.ad.jp/ja/ip/transfer/ipv4-log.html> より作成

出典：JPNIC川端氏より

IPv4経路数推移予測2.0(2016年予測)

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



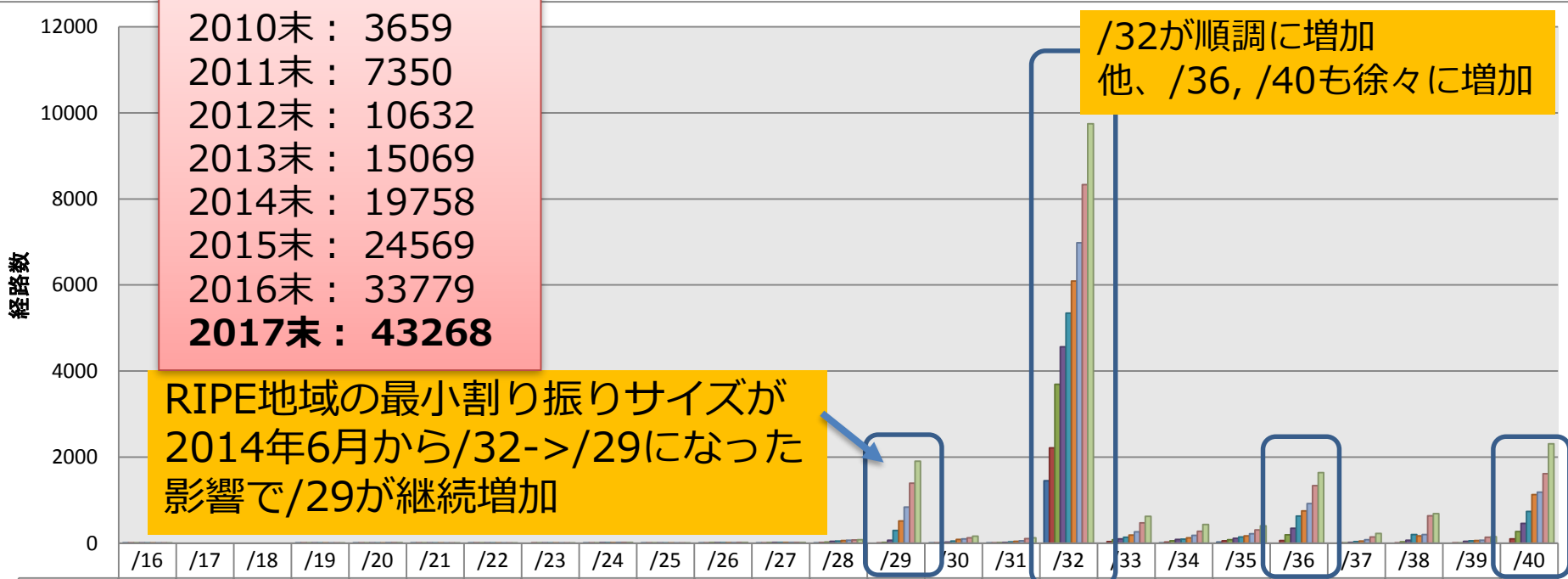
誤った経路広告による一時的な経路増大等への対処にも注意下さい

IPv6経路数の推移

2009末 : 1832
 2010末 : 3659
 2011末 : 7350
 2012末 : 10632
 2013末 : 15069
 2014末 : 19758
 2015末 : 24569
 2016末 : 33779
2017末 : 43268

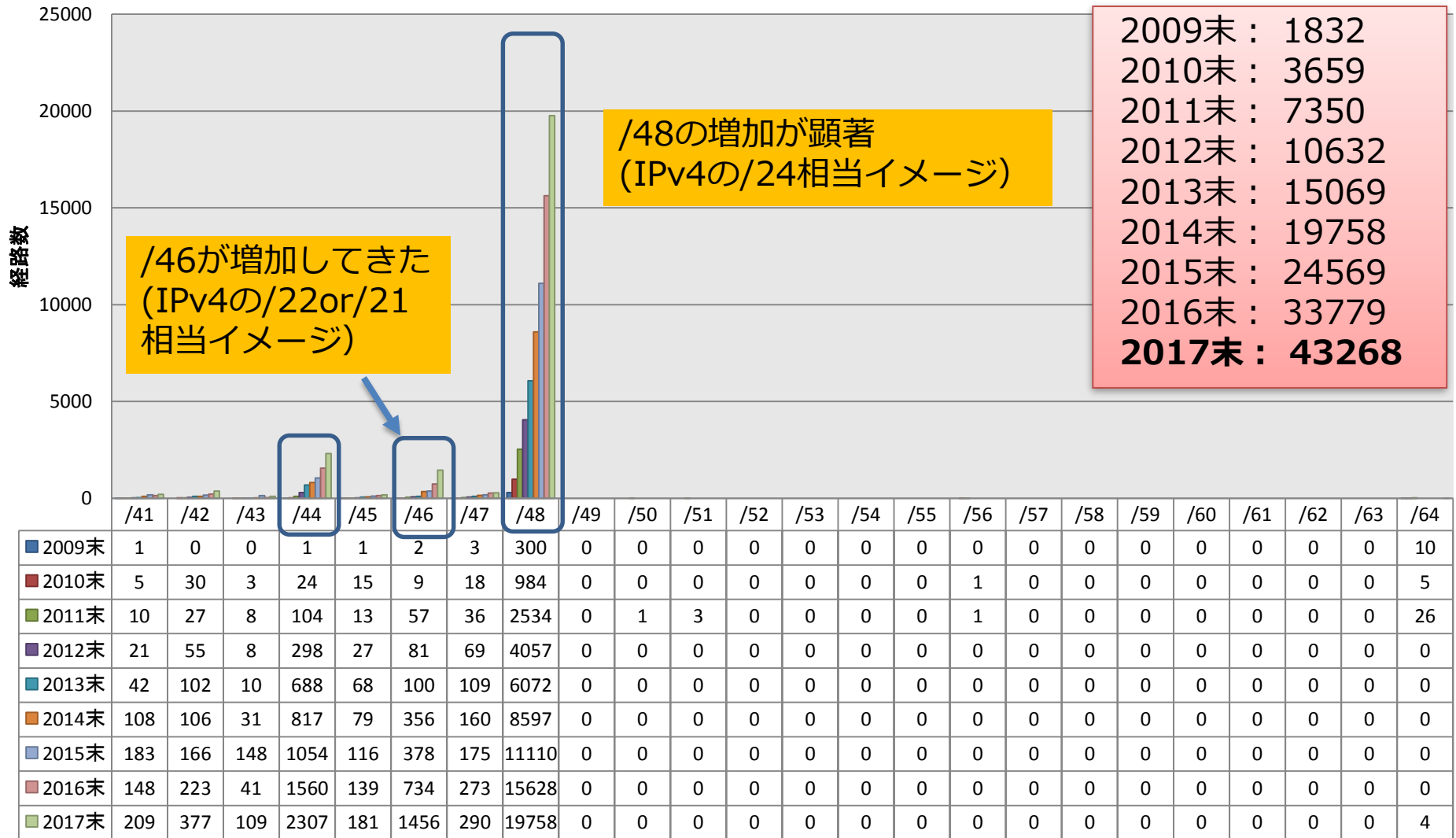
/32が順調に増加
 他、/36、/40も徐々に増加

RIPE地域の最小割り振りサイズが
 2014年6月から/32->/29になった
 影響で/29が継続増加

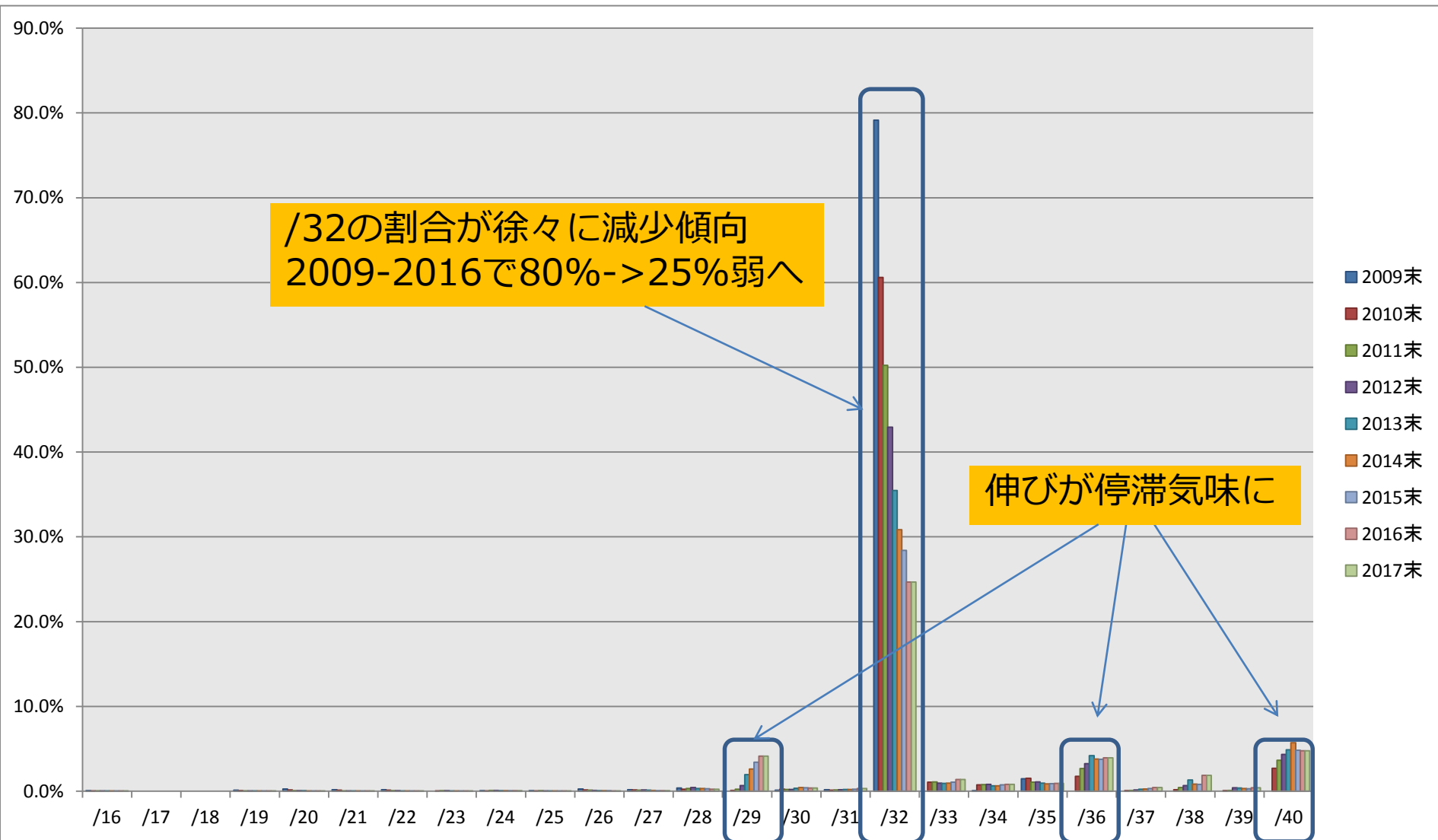


	/16	/17	/18	/19	/20	/21	/22	/23	/24	/25	/26	/27	/28	/29	/30	/31	/32	/33	/34	/35	/36	/37	/38	/39	/40
■ 2009末	1	0	0	2	5	3	3	0	1	1	5	3	7	0	2	3	1450	0	1	27	0	0	0	0	0
■ 2010末	1	0	0	2	5	4	4	1	1	1	5	5	9	3	8	4	2217	39	27	56	64	2	6	2	99
■ 2011末	1	0	0	2	4	3	5	4	7	4	9	9	24	16	14	10	3692	80	57	79	197	7	31	7	268
■ 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
■ 2017末	1	0	0	2	9	3	4	4	19	6	15	17	79	1904	161	125	9750	626	437	401	1640	229	688	150	2307

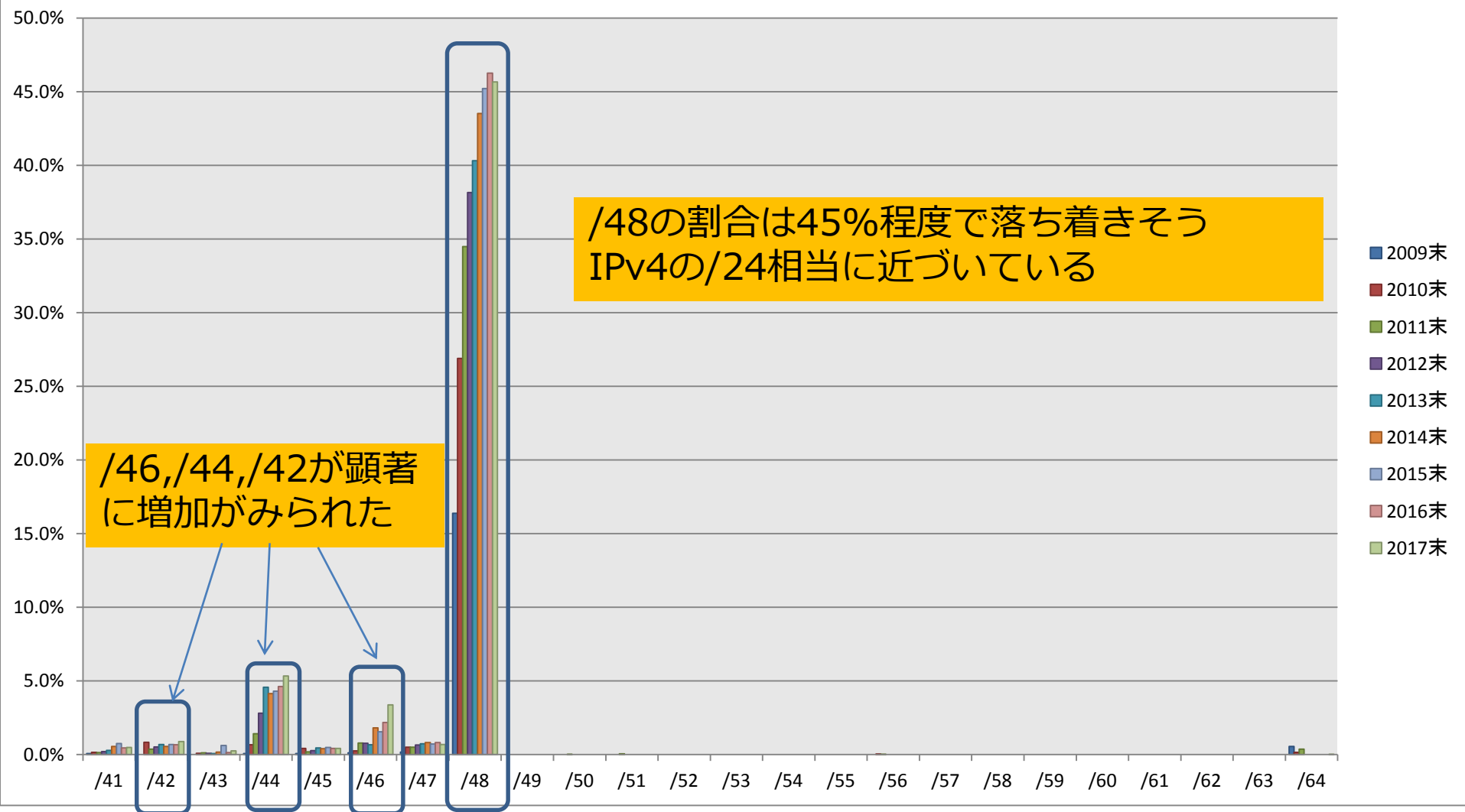
IPv6経路数の推移



IPv6経路数の推移 (割合)

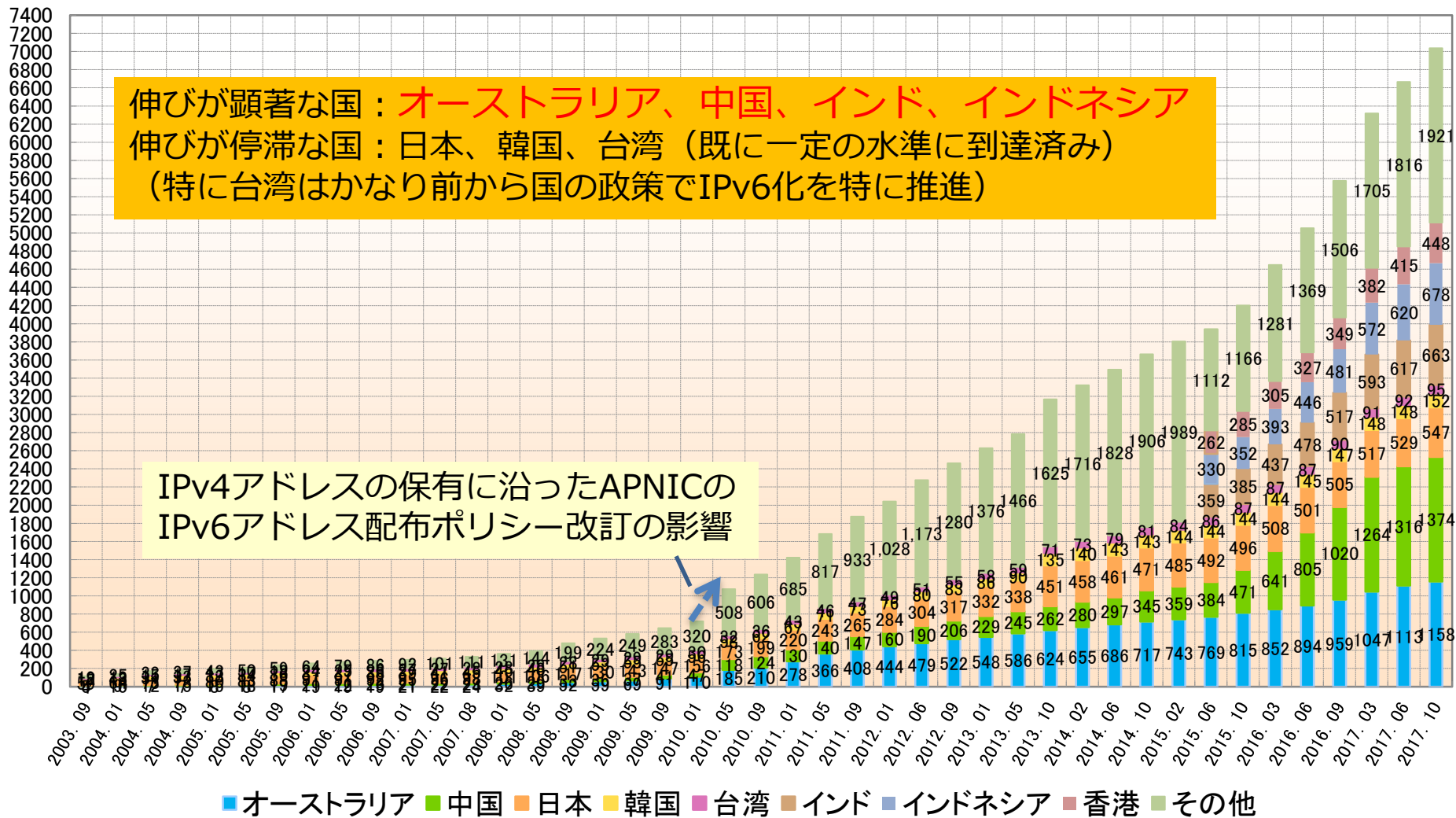


IPv6経路数の推移（割合）



AP地域の国別IPv6アドレス配分状況

(件数)

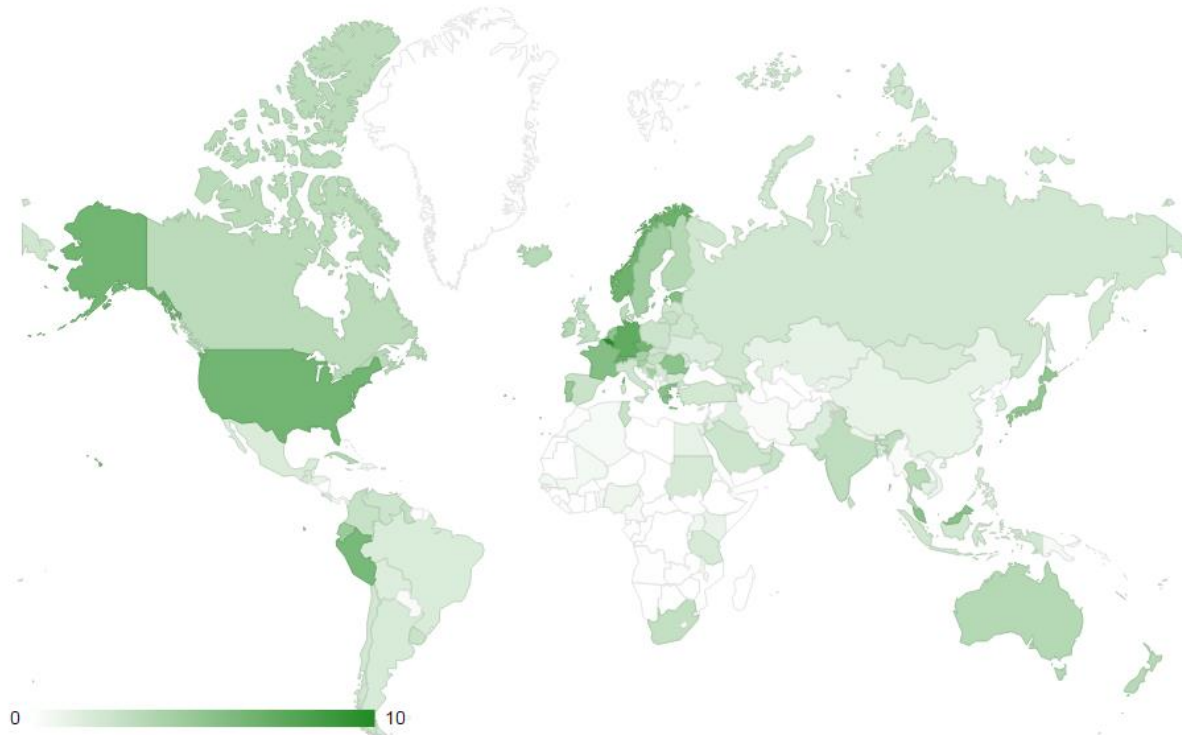


http://6lab.cisco.com/stats/

2014/11/15

Display global data ⓘ

World | Africa | Asia | America | Europe | Oceania

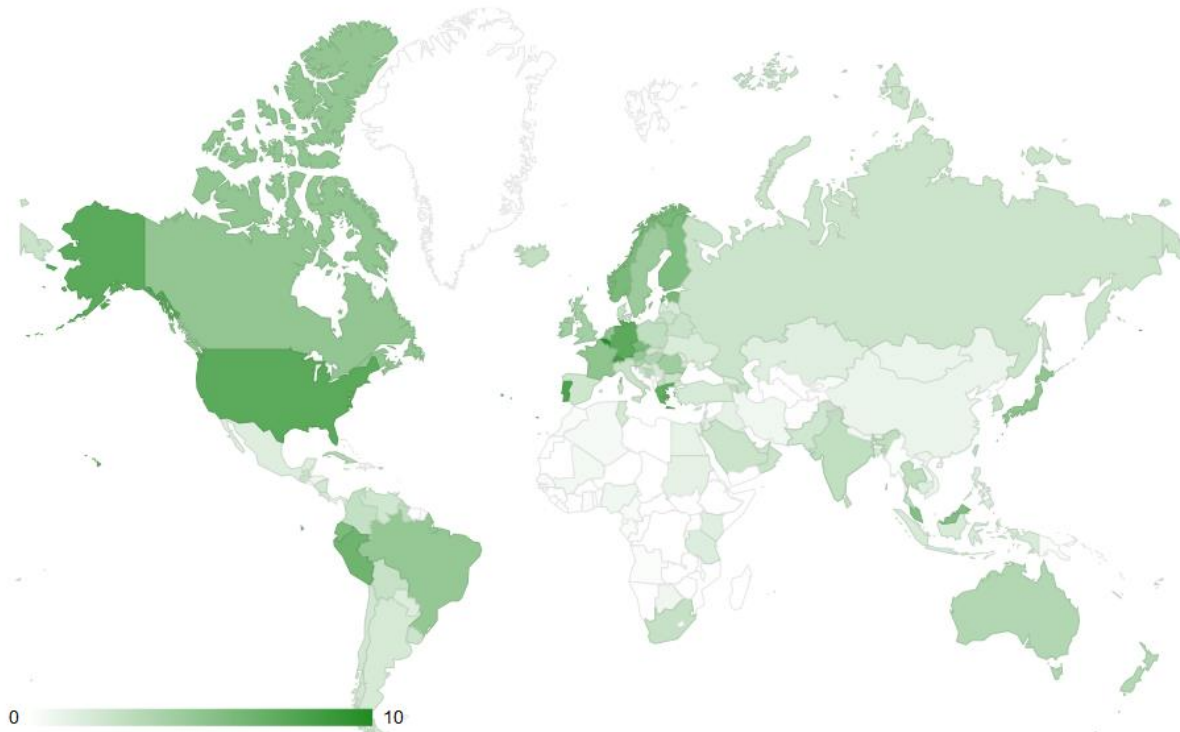


http://6lab.cisco.com/stats/

2015/11/19

Display global data 

World | Africa | Asia | America | Europe | Oceania



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

6lab - The place to monitor IPv6 adoption

Home

Info

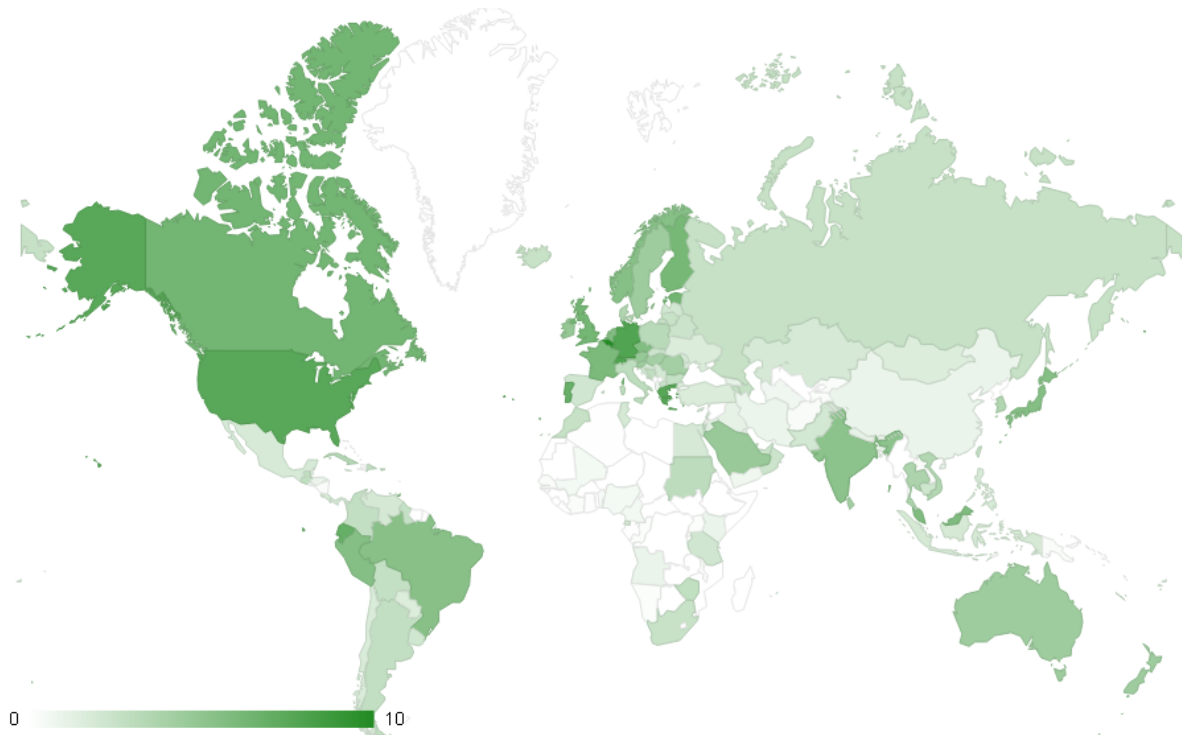
Feedback

Share ▾

2016/11/20

Display global data ⓘ

[World](#) | [Africa](#) | [Asia](#) | [America](#) | [Europe](#) | [Oceania](#)



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

6lab - The place to monitor IPv6 adoption

Home

Info

Feedback

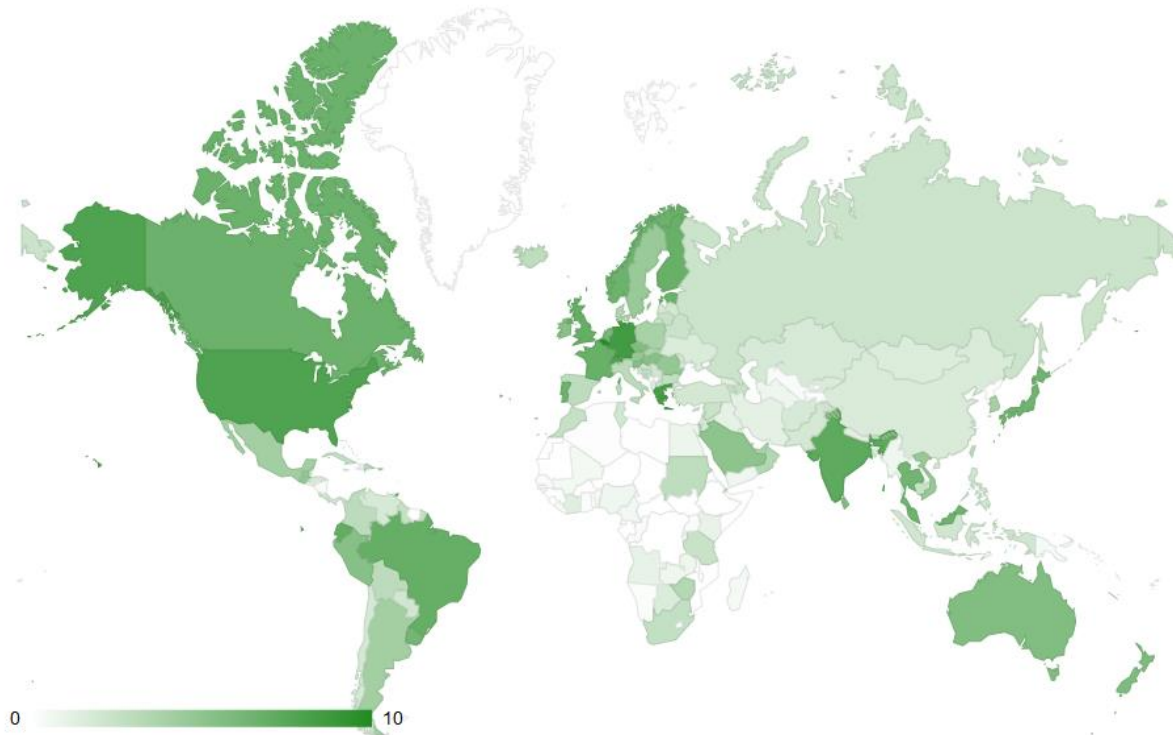
Share

2017/11/26

Display global data 

World | Africa | Asia | America | Europe | Oceania

着実にIPv6化は進んでいる



AS番号 (2byte/4byte)

- 2byteAS

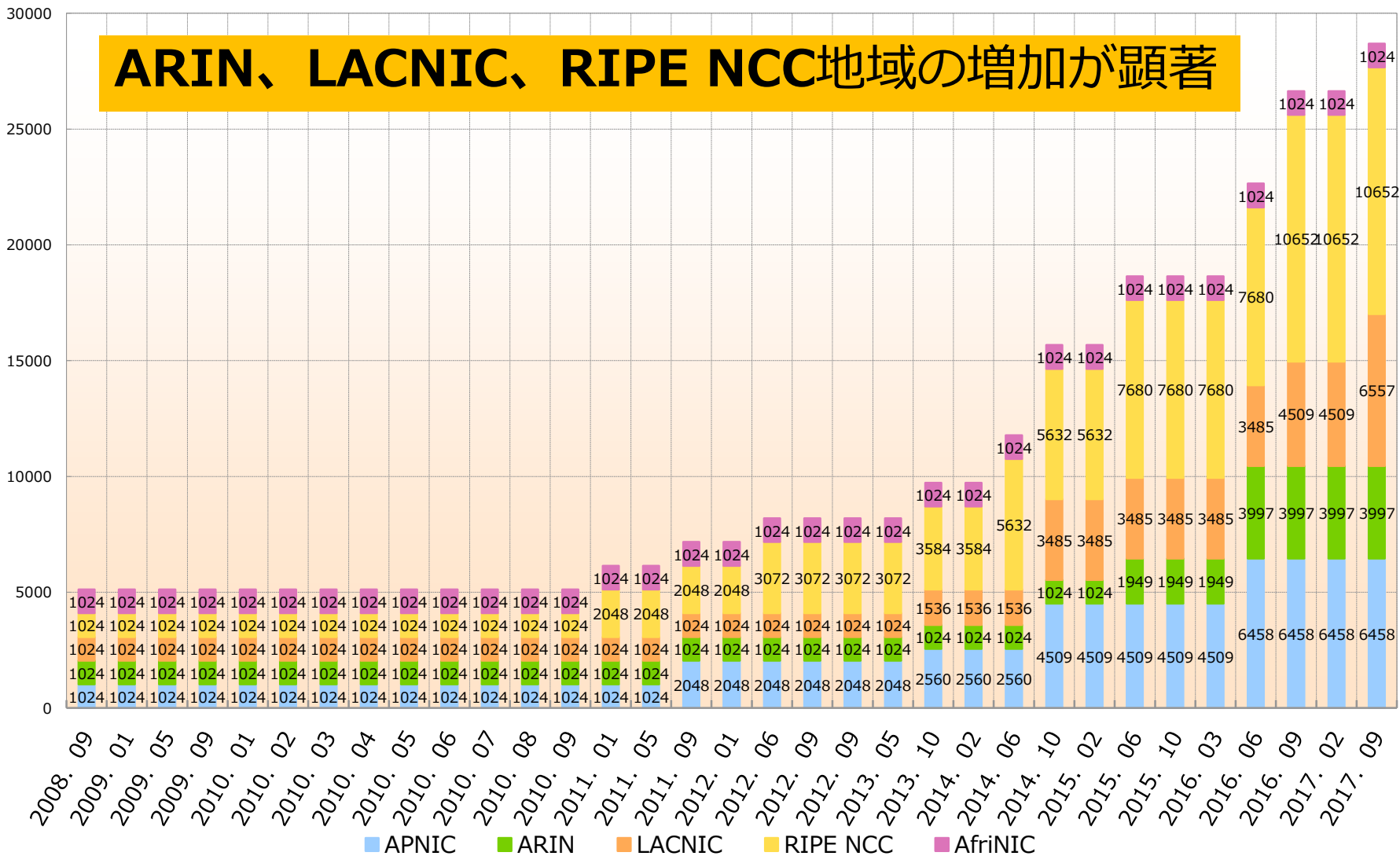
- IANA在庫は**昨年枯渇** (2016-07-29 RIPEが最後)
- RIRに若干の在庫があり4byteでの対応が困難な事業者向けには2byteを配布中
- AS番号の移転も2014年より開始

- 4byteAS

- 全世界的には4byteがほぼ主流、APNICも**97%**4byte
- 日本は大分浸透してきたものの**半分はまだ2byte頼り**
 - 上流ISPや自ASが4byteAS非対応のケースが依然ある模様
 - 2015年 : 2byte : 4byte = **5:1**
 - 2016年 : 2byte : 4byte = **2:1**
 - 2017年 : 2byte : 4byte = **1:1** (半分は2byte)

4byteASのRIRへの配分状況

(個)



<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

2017年 DNSトピック

- ルートゾーンKSKロールオーバーが延期（2017年9月27日）
 - DNSSECのトラストアンカー、KSK(Key Signing Key)の初の更新
 - ルートゾーンのDNSKEY RRの署名鍵切り替え(KSK-2010 → KSK-2017)が、2017年10月11日に行われる予定だった
 - 理由：KSK-2010しか保持していないリゾルバが無視できない数存在していることが、新たに判明したため
 - トラストアンカー情報をルートサーバに送ってきたリゾルバの約5%
 - リトライ：未定（最速で2018Q1、状況次第で再延期も十分あり得る）
- 10月24日、B-RootサーバのIPv4アドレスが更新
 - 今のところ大きな問題は報告されていない。旧IPアドレスでも運用中
- M-Rootは2017年8月、運用開始から20年
 - 日本に置かれた初のルートサーバ、Mは村井のM？
- .com、.net、.jobsのThin→Thickモデル移行の延期
 - レジストラからレジストリ（Verisign）への登録者情報の登録が必要になる
 - .comを1億件分、.netを1000万件分以上登録する必要あり
- 新gTLDが約1300に。申請/委任は収束へ。徐々に本格活用へ

2017年 DNSセキュリティ動向

- ドメイン名ハイジャック

- Google Bangladesh (google.com.bd) (2016年12月) 2011年にも発生
- Google Brazil (google.com.br) (2017年1月)
パキスタンのハッカーによるといわれている12月のBangladeshの件の後に発生

- .io TLDのセキュリティインシデント (2017年6月)

- ネームサーバーホスト名そのもののドメイン名が登録可能な状態で、TLD全体がドメイン名ハイジャックされうる状態になっていた
- 原因は.ioのレジストリシステムのバグ
- .ioは過去にも各種問題を起こしている

```
;; AUTHORITY SECTION:
```

```
io.      172800 IN NS ns-a1.io.  
io.      172800 IN NS ns-a2.io.  
io.      172800 IN NS ns-a3.io.  
io.      172800 IN NS ns-a4.io.  
io.      172800 IN NS a0.nic.io.  
io.      172800 IN NS b0.nic.io.  
io.      172800 IN NS c0.nic.io.
```

- 今年もBIND祭りは健在、年12件で過去最高の脆弱性報告数

- うち緊急が6件。しかし今年はいつもと傾向が違う。。

2年おきに発生するBINDコロリが無かった

- 2008年7月：カミンスキー型攻撃手法の発表
- 2009年7月：パケット一発で死ぬ脆弱性（通称「**BINDコロリ**」）
発見者が公開ML上に「こうやるとBINDが落ちちゃうんですけど、どうして？」 →大祭りに
- 2010年7月：ルートゾーンがDNSSEC対応したその日に、DNSSEC対応したゾーンの権威DNSサーバーに全力でDoSするキャッシュDNSサーバーの脆弱性が発表
- 2011年7月：パケット一発で死ぬ脆弱性（再び「**BINDコロリII**」）
- 2012年7月：割と安定しているNSDに脆弱性2件、BIND 9の脆弱性2件、全世界に3億台ぐらいあるAndroid端末のDNSリゾルバにキャッシュポイズニング可能な脆弱性が発覚
- 2013年7月：パケット一発で死ぬ脆弱性（再び「**BINDコロリIII**」）
- 2014年 : 7月のBIND祭りはなかったが、キャッシュポイズニング攻撃の手法が改めて話題に
- 2015年7月：TKEY RRの取り扱い不具合。パケット一発で死ぬ脆弱性（再び「**BINDコロリIV**」）
- 2016年**9月**：パケット一発で死ぬ脆弱性、**国内でも被害が発生**（CVE-2016-2776）
- **2017年：魔の7月「BINDコロリV」はやってこなかった。。**
 - 2017年7月以降、BINDの脆弱性そのものが公開されていない。。

JPRSが公開した脆弱性情報 (1/2)

公開・更新日	タイトル
2017年1月12日	(緊急) BIND 9.xの脆弱性(DNSサービスの停止)について (CVE-2016-9131)
2017年1月12日	(緊急) BIND 9.xの脆弱性(DNSサービスの停止)について (CVE-2016-9147)
2017年1月12日	(緊急) BIND 9.xの脆弱性(DNSサービスの停止)について (CVE-2016-9444)
2017年1月12日	BIND 9.xの脆弱性(DNSサービスの停止)について (CVE-2016-9778)
2017年1月17日	PowerDNS Authoritative Server及びPowerDNS Recursorの脆弱性について (CVE-2016-7068、CVE-2016-7072、CVE-2016-7073、CVE-2016-7074、CVE-2016-2120)
2017年2月9日	BIND 9.xの脆弱性(DNSサービスの停止)について (CVE-2017-3135)
2017年4月13日	BIND 9.xの脆弱性(DNSサービスの停止)について (CVE-2017-3136)

「提供: JPRS」

JPRSが公開した脆弱性情報 (2/2)

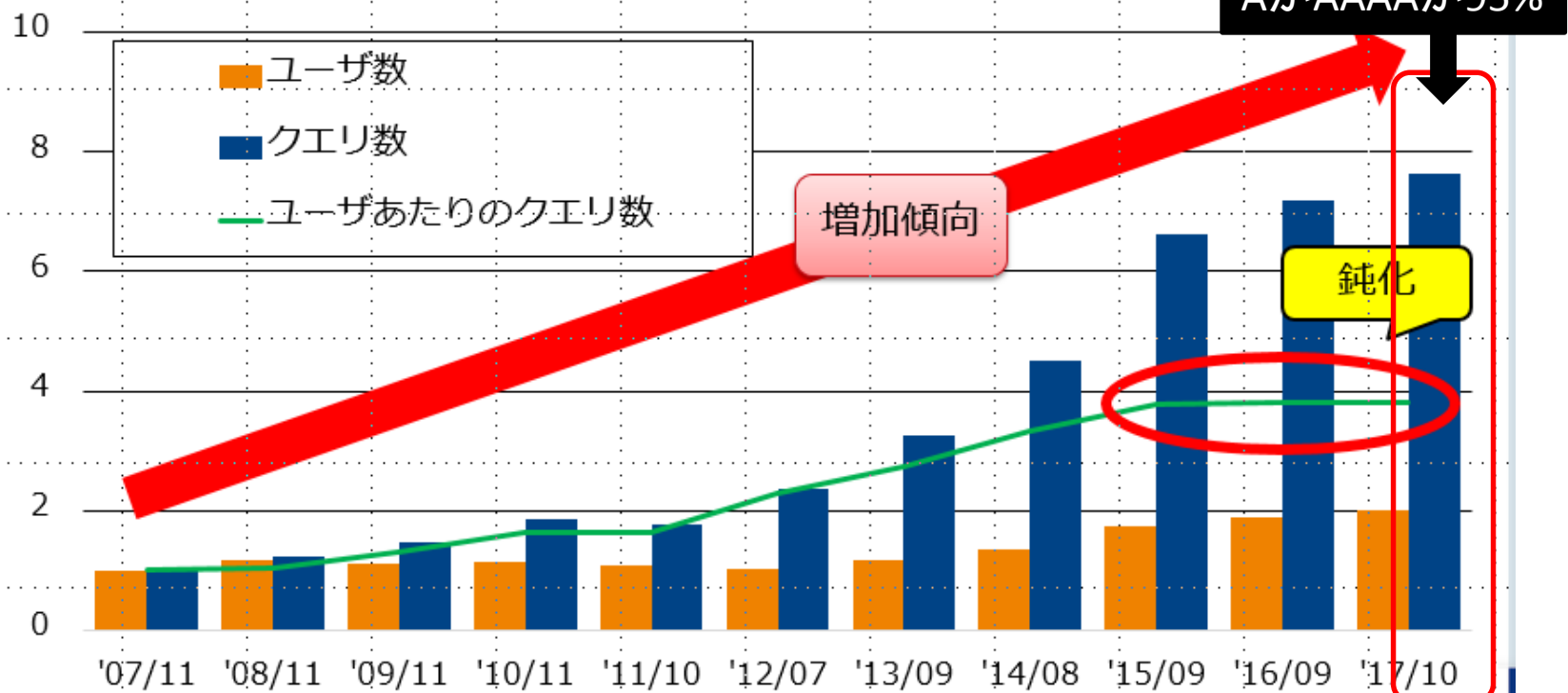
公開・更新日	タイトル
2017年4月13日	(緊急) BIND 9.x の脆弱性(DNSサービスの停止)について (CVE-2017-3137)
2017年4月13日	BIND 9.x の脆弱性(DNSサービスの停止)について (CVE-2017-3138)
2017年5月16日	Windows DNS Serverの脆弱性(サービス拒否)について (CVE-2017-0171)
2017年6月15日	BIND 9.x の脆弱性(サービス性能の劣化及びパケットの連続送信)について(CVE-2017-3140)
2017年6月15日	(緊急) BIND 9.x の脆弱性(権限の昇格)について (CVE-2017-3141)
2017年6月30日	BIND 9.x の脆弱性(TSIG認証の迂回によるゾーンデータの流出)について(CVE-2017-3142)
2017年6月30日 2017年7月13日	(緊急) BIND 9.x の脆弱性(TSIG認証の迂回によるゾーンデータの操作)について(CVE-2017-3143)

「提供: JPRS」

OCNのキャッシュDNS動向

ユーザからのクエリ数とユーザ数

- 10年前(2007年)と比べるとクエリ数は約7.5倍
- 直近の2年間ではユーザあたりのクエリ数の伸びは鈍化傾向
 - ✓ これまでは1ユーザが出すクエリ数も年々増加していた
 - ✓ 宅内の端末(スマホ、タブレット機器)数が飽和してきた?



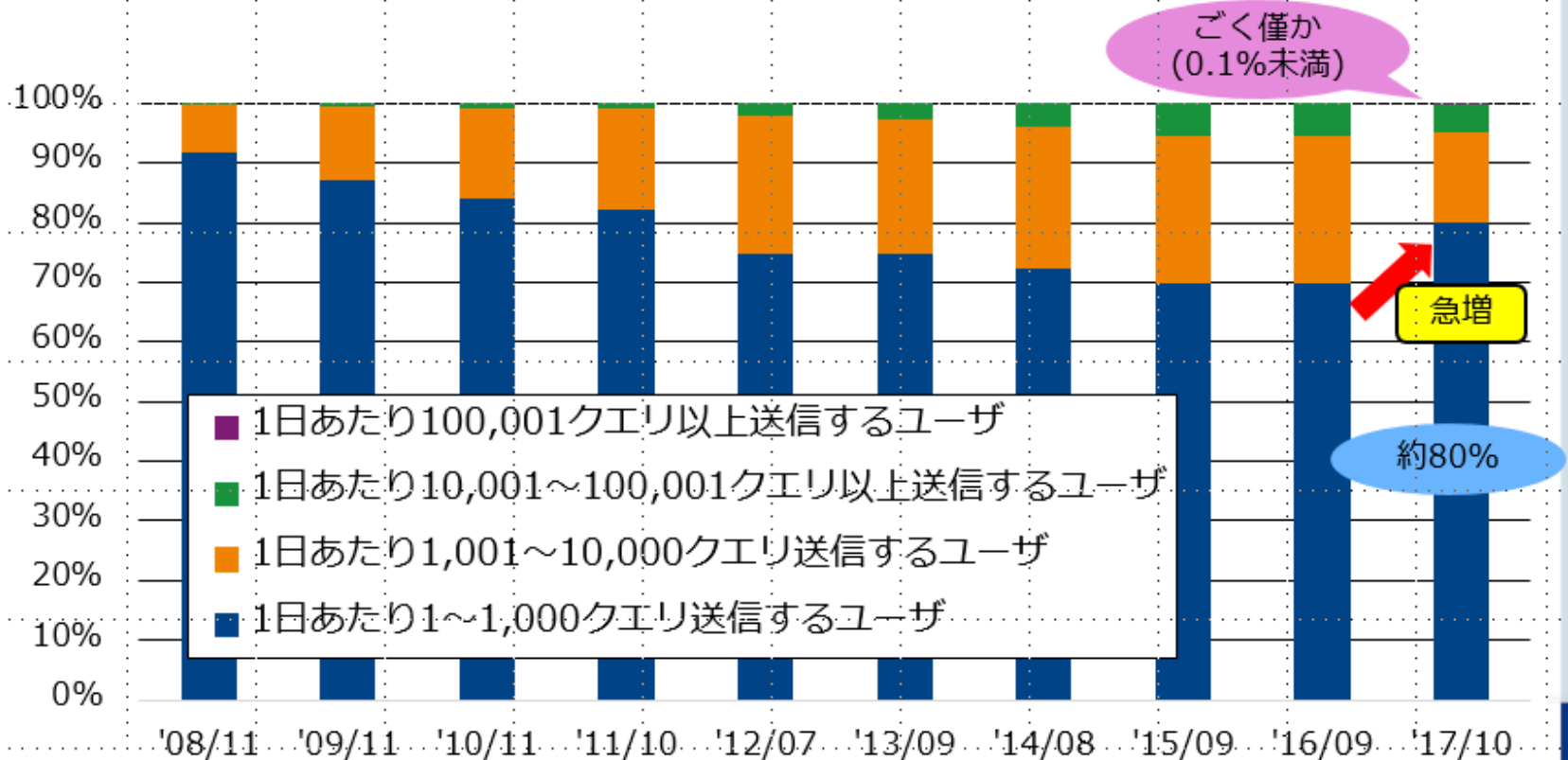
※縦軸は'07/11の値を1とする

11/30 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

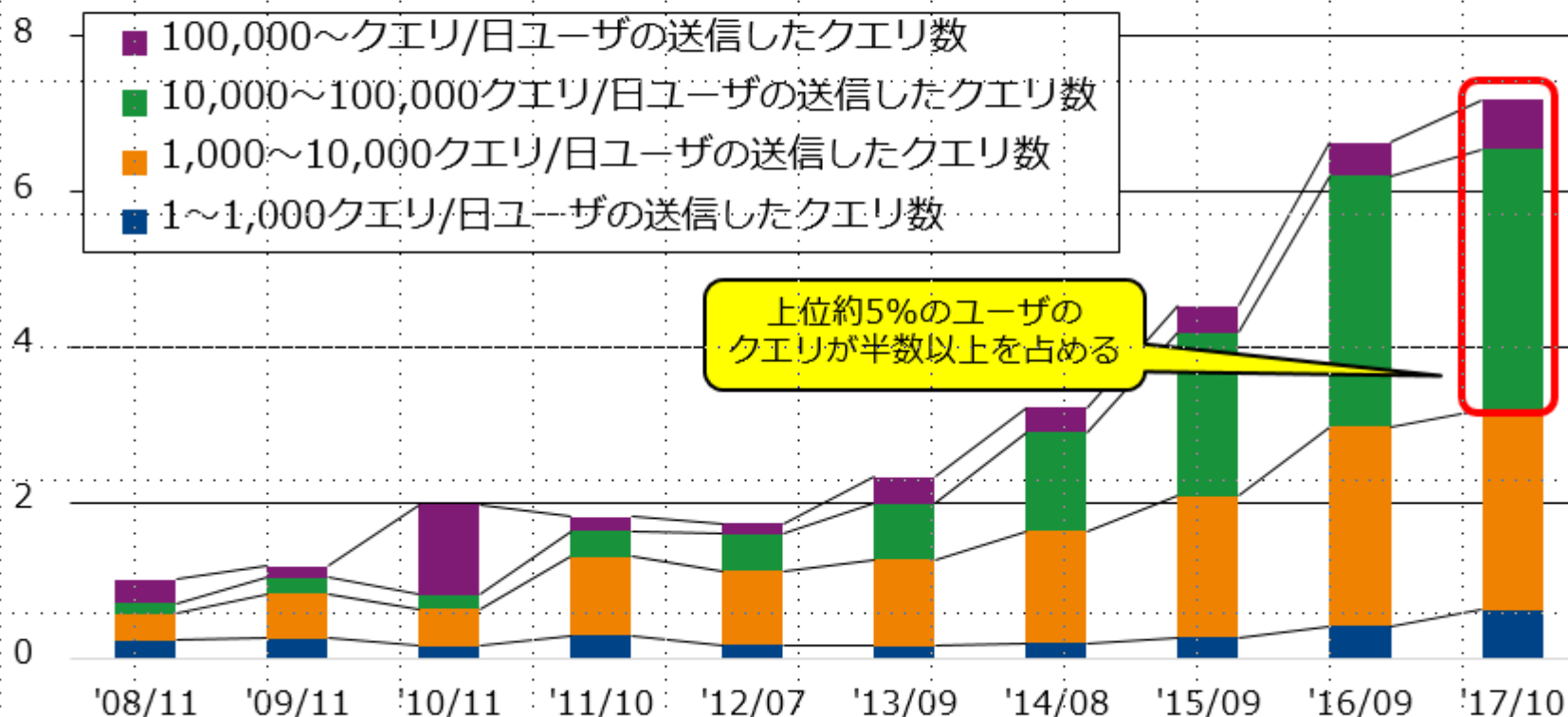
- 1日1~1,000クエリ送信するユーザの割合が急増
 - ✓ ユーザ層：宅内ルータは電源onだけどPCやスマホを使っていない状態？
 - ✓ 弊社の網外(海外含む)からのIPが多く検出された？
- 1日10万クエリ以上送信するユーザはごく僅か(0.1%未満)



11/30 DNS DAY NTTCom小坂氏発表資料より

総クエリに対するユーザ層ごとのクエリの割合

- 総クエリの半数以上はヘビーユーザ(≒1日1万クエリ以上送信)のクエリ
 - ✓ 1日1万クエリ以上送信するユーザは上位約5%(前ページより)
- 1~1,000クエリ/日送信するユーザは人数は多いがクエリ数自体は少数



※縦軸は'07/11の値を1とする
(p5参照、'08/11以降を再掲載)

8

11/30 DNS DAY NTTCom小坂氏発表資料より

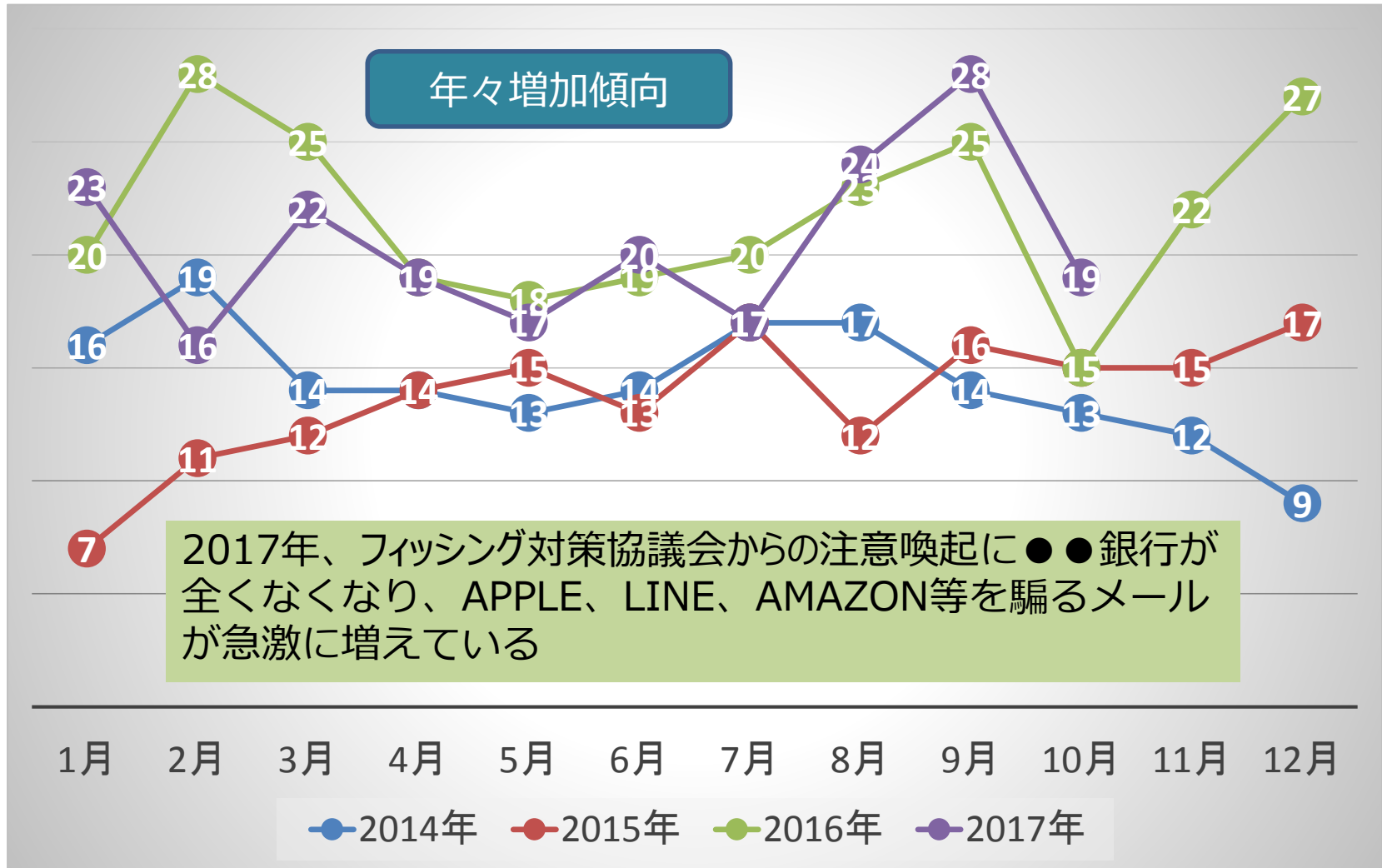
内容

- 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

2017年セキュリティ動向

- DDoS攻撃は今年は例年に比べて少々落ち着いた傾向
 - 落ち着いたとは言え600G前後のDDoS攻撃は今年も複数回観測されている
 - 超短時間の攻撃により検出が難しい攻撃がしばし観測されている
 - Botが簡単に買える時代に
- ランサムウェア「WannaCry」攻撃が5月に再び猛威を振るう
 - 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
 - 比較的安価に売られている事もあり、簡単にあらゆる企業がターゲットに
- フィッシング攻撃も相変わらず止まない
 - ネットバンキング等を狙った不正サイトへの誘導やウイルスの傾向から、Apple、LINE、Amazon等を騙る誘導メールが急増（2016年後半からの傾向）
 - フィッシング協議会の緊急情報通知一覧の掲載数は過去最大に（46件）
- UDPを利用した水攻め攻撃は依然継続（DNS、NTP、SSDP等）
 - IoT機器等からの大量なクエリーなどによる攻撃も観測されている
- 経路ハイジャック、意図的な経路操作や意図しないもの双方あり
 - 特定のターゲットのみへ不正経路広報しSPAMを配信する
 - 意図的に国策？で実施したが国外にリークし被害が及ぶケースも

フィッシングに悪用されたブランド件数



「フィッシング対策協議会」の公開データより集計

Appleをかたるフィッシングメール

安全のため、このApple IDはすでにロックされました。

あなたのApple IDはwindows PCのiCloudにログインしたりダウンロードしたりする操作があったとAppleゲームのセキュリティチームは発見しました。

日付と時間：2017/11/05

iCloudバージョン：6.2.2.35

IP：●●●●● (岐阜)

あなたのアカウントの安全性を守るために、セキュリティ質問を再設定して頂くことが必要です。再設定された後、たとえあなたのApple IDとパスワード及び元のセキュリティ情報を知っているとしても、それを使用することができません。

この問題を解決するにはこちら <<http://help-id-●●●●●.online/>>

このリンクとあなたのApple IDのセキュリティ質問とは、2017年10月21日から失効になります。詳細情報について、「よくある質問」をご利用いただけます。

以上

Apple IDサポートセンター

「更新」 Apple かかたるフィッシング (2017/11/07)

相変わらず日本語変です

「フィッシング対策協議会」サイトより

イランISPによるCensoring目的のハイジャック

- Iranian state telecom TICによるポルノサイトのハイジャックが発生 (99.192.226.0/24) ; 本来は99.192.128.0/17
- 意図としては、イラン国内にのみ該当経路を配信するものだったが、ルートリークしてしまった模様
 - 2008年のパキスタンテレコムによるyoutubeのハイジャックに類似
- 本来の広告元ASが同一経路を広告し、一部可能な範囲で奪還し、のちにTICによる経路広報の停止により収束
- しかしイラン国内向けには経路は広報され続けていた模様



Iranian Research and Academic Network



IPM/IRANET Looking Glass

- show ip bgp 99.192.226.0/24

Router: IPM/IRANET (AS6736)
Command: show ip bgp 99.192.226.0/24

```
BGP routing table entry for 99.192.226.0/24, version 2788026
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Multipath: eBGP iBGP
Not advertised to any peer
12880 65050, (received & used)
195.146.63.104 (metric 2560002560) from 194.225.150.110 (194.225.150.110)
Origin IGP, metric 0, localpref 70, valid, internal, best
```

Disclaimer: All commands will be logged for possible later analysis and statistics. If you don't like this policy, please disconnect now!

Please email questions or comments to contact@iranet.ir.

Dynのサイトより <https://dyn.com/blog/iran-leaks-censorship-via-bgp-hijacks/>

http://lg.iranet.ir/

現在はLG上では経路は見えない



Iranian Research and Academic NETwork



IPM/IRANET Looking Glass

- show ip bgp 99.192.226.0

Router: IPM/IRANET (AS6736)

Command: show ip bgp 99.192.226.0

```
BGP routing table entry for 0.0.0.0/0, version 157733
Paths: (1 available, best #1, table Default-IP-Routing-Table, RIB-failure(17) - next-hop mismatch)
Multipath: eBGP iBGP
  Not advertised to any peer
  29049, (received & used)
  194.225.151.13 (metric 156416) from 194.225.150.110 (194.225.150.110)
  Origin IGP, metric 0, localpref 185, valid, internal, best
  Originator: 194.225.151.49, Cluster list: 194.225.150.110, 194.225.150.120
```

Disclaimer: All commands will be logged for possible later analysis and statistics. If you don't like this policy, please disconnect now!

Please email questions or comments to contact@iranet.ir.

(参考) <https://www.tic.ir/>

色々リアルタイムで通信状況等を計測するなど非常に頑張ってる感じがあります

کیفیت سرویس صادره از شبکه ثابت



کیفیت سرویس کشورهای مختلف



هر دو پارامتر کیفی بالاتر از حد شاخص هستند ■ یکی از پارامترهای کیفی پایین تر از حد شاخص است ■ هر دو پارامتر کیفی پایین تر از حد شاخص هستند ■

جدول پارامترهای کیفی ترافیک صادره بین الملل از اپراتورهای سيار

Name ↑	ACT Sec(s)	ASR %
IRANCELL	111.46	42.34
MCI_ALBORZ	120.38	41.25
MCI_ARDABIL	62.84	65.6
MCI_BUSHEHR	128.35	99.73
MCI_CHAHAR MAHAL AND BAKHTIARI	112.04	57.17
MCI_EAST AZERBAIJAN	85.3	58.68
MCI_FARS	126.19	57.94

ロシア政府管理下のISPによる 金融サービス機関等のハイジャック

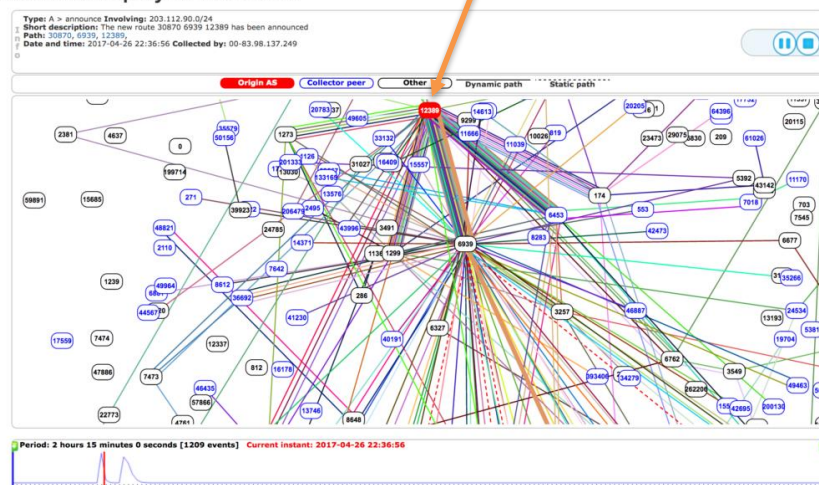
- 2017/4/16、ロシア政府管轄下にある通信事業者「Rostelecom」による約7分程度のハイジャックが発生
- 50Prefix、37ASの経路がRostelecomにreidirect（以下抜粋）

AS2559	Visa International
AS12257	EMC Corporation
AS25410	Bank Zachodni WBK S.A.
AS26380	MasterCard Technologies LLC
AS28827	Fortis Bank N.V.
AS30060	VeriSign Infrastructure & Operations

BGP.monより：
AS12389へ各所から
トラフィックがdivert

- 金融サービス機関を狙った
一時的かつ意図的な通信トラフィック
の傍受との見方が有力

Watch the replay of this event



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

2017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は引き続き増加、特にアップロードが顕著に
 - モバイルトラフィックはここ最近1.3~1.4倍で安定的に増え続けている
 - HTTPSがHTTPを逆転。日本国内でのHTTPS化が促進した年に
- **ルーティング動向**
 - IPv4は多少伸びが落ち着き、IPv6経路は9千~1万経路の過去最高の伸びに
 - IPv4/IPv6問わず急激な経路増大にはご注意を（FIB容量の制限など）
- **DNS動向**
 - BINDの脆弱性は12件で過去最高だが、今年は後半異常に静か…
 - 権威DNSへの攻撃やドメインハイジャック、インシデントは依然継続している
 - キャッシュDNSの総クエリ数の増加は多少鈍化したが、スマホやIoTデバイス等の増加により今後の動向を把握していく必要がある
- **セキュリティ動向**
 - DDoS攻撃は多少落ち着いたが依然数百Gクラスの被害は発生している
 - WannaCryを代表とするランサムウェア、フィッシング等の被害も多かった
 - 意図的な経路ハイジャックも依然として発生、通信事業者での根本対策も重要