2015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～

Internet Multifeed / JPNAP
Tomoya Yoshida
<yoshida@mfeed.ad.jp>

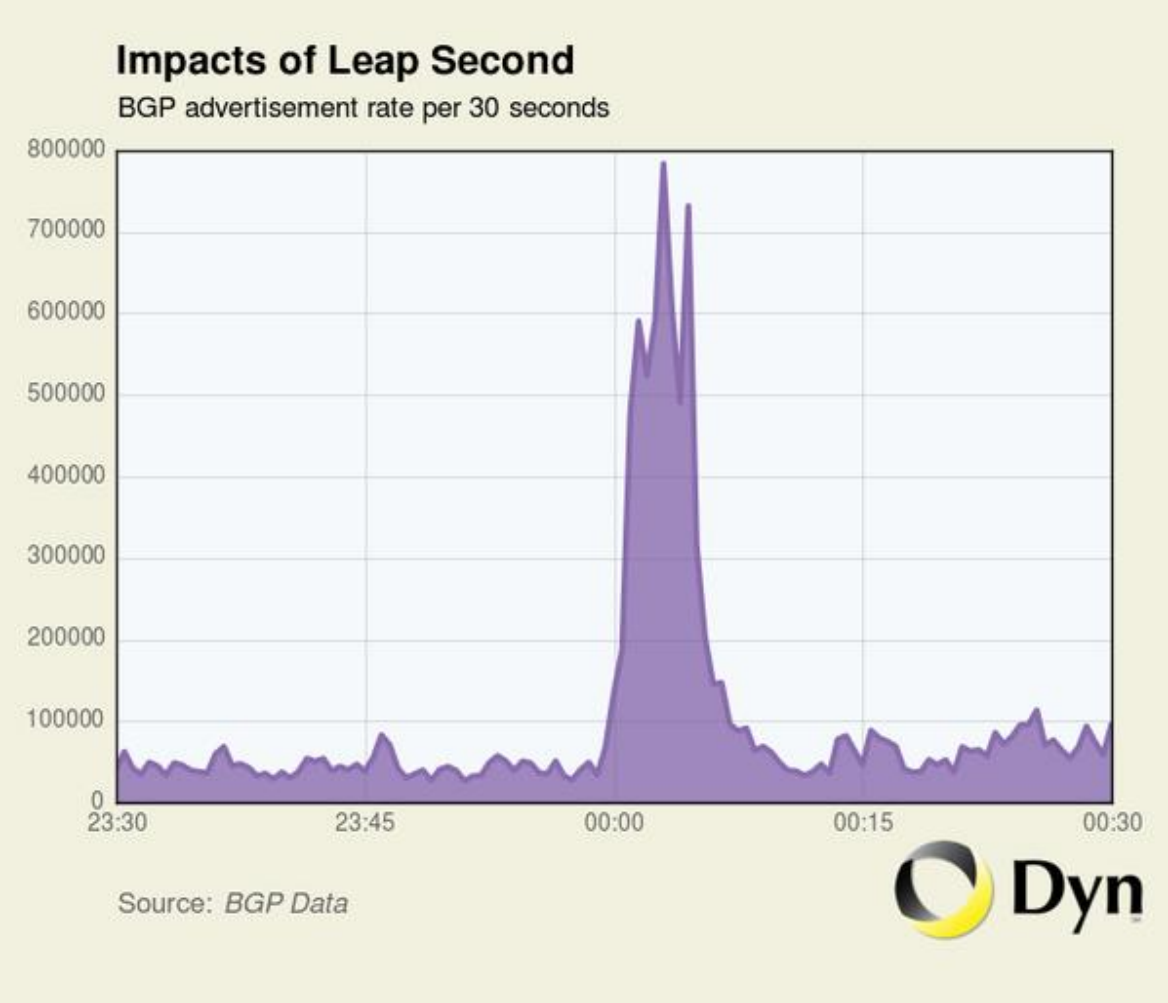
内容

- 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

2015年のうるう秒

- ７月１日、3年ぶりに「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、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、7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）
  - 3年前に比べると大きな被害はなかったが、未だに問題は起きている
    - 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
  - 11月に世界無線通信会議（WRC-15）で存続or廃止が検討される予定
    700年で30分のずれ。日本は廃止派
    - ただし仮に今回廃止になったとしても次回からうるう秒対応がすぐに無くなるかは不明
    - **【12月 アップデート追記】2023年のWRCまでに結論を得ることが決定**
- 一部のネットワークでも障害が発生し、不意な装置の再起動等によりBGP Updateの急増が観測された
  - 通常時の約10倍程度
  - アップデートが増加すると、BGPプロセスの処理に影響する

Leap second causes ~5 minutes of transient global routing instability



出展：https://twitter.com/dynresearch/status/616059353821487104

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

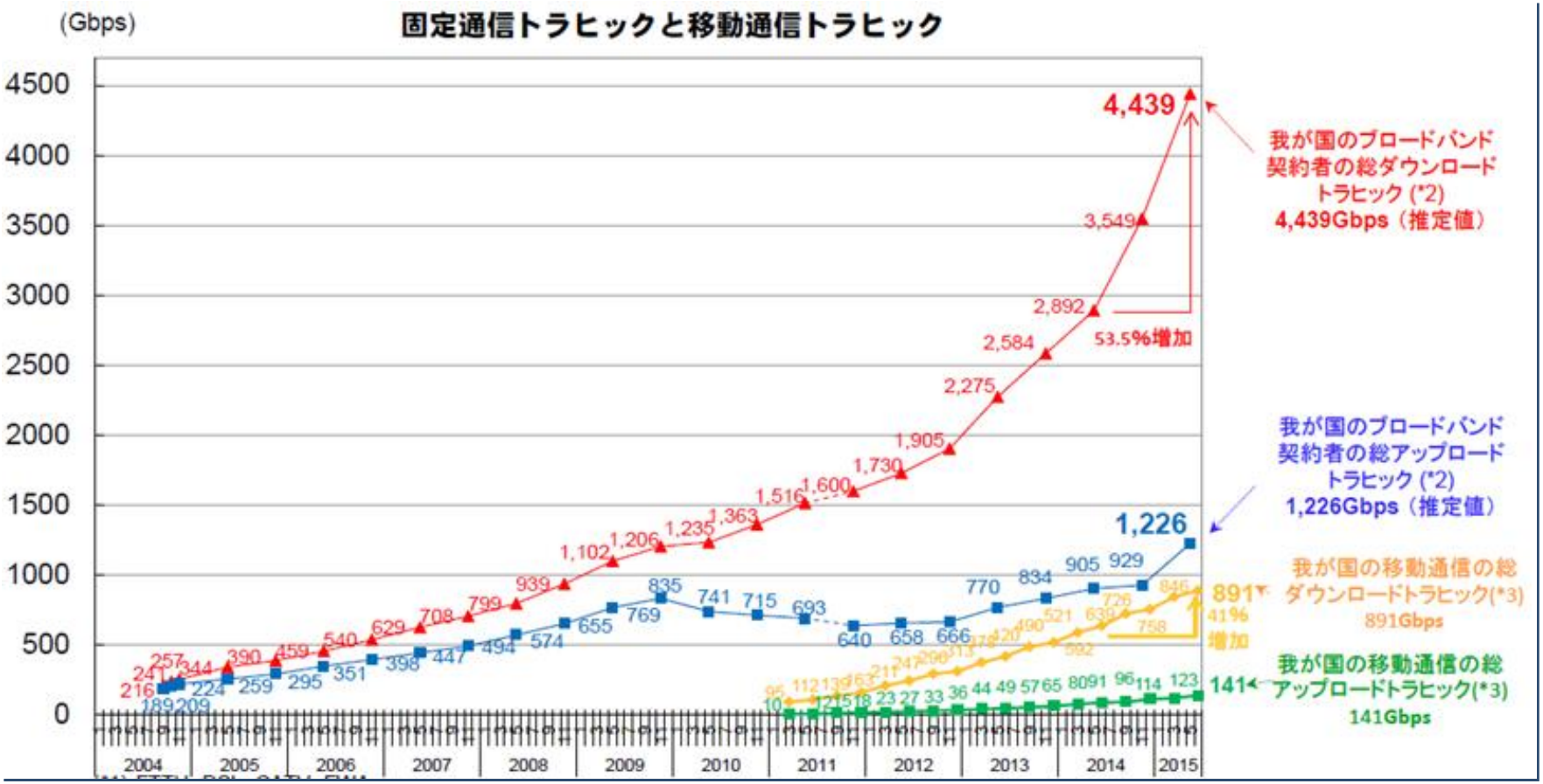
2015年 トラフィック動向

- ブロードバンドトラフィックの増加が著しい
  - ここ１年でダウンロードが53.5%増、2014年は27.1%
  - アクセス環境やコンテンツ自体の内容がリッチなり増加し続けている
  - 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の増加もここ最近多い傾向
  - ブロードバンドの増加には、実はwifiのオフロードが含まれている
- モバイルトラフィックも順調に増加
  - ここ1年で1.41倍、増加率は徐々にゆるやかになってきている
  - 帯域制限により月末にかけて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
  - スマートフォンやモバイル端末の普及により利用時間の幅が拡大
  - 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特に今年は急増
- IPv6トラフィックはゆるゆる増加
- HTTPからHTTPSへの動きが加速化
  - Google(youtube, Gmail etc..), facebook, twitter等がHTTPS化を推進
  - 一方考慮すべき課題なども出てきている
- イベント時のトラフィック変動

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

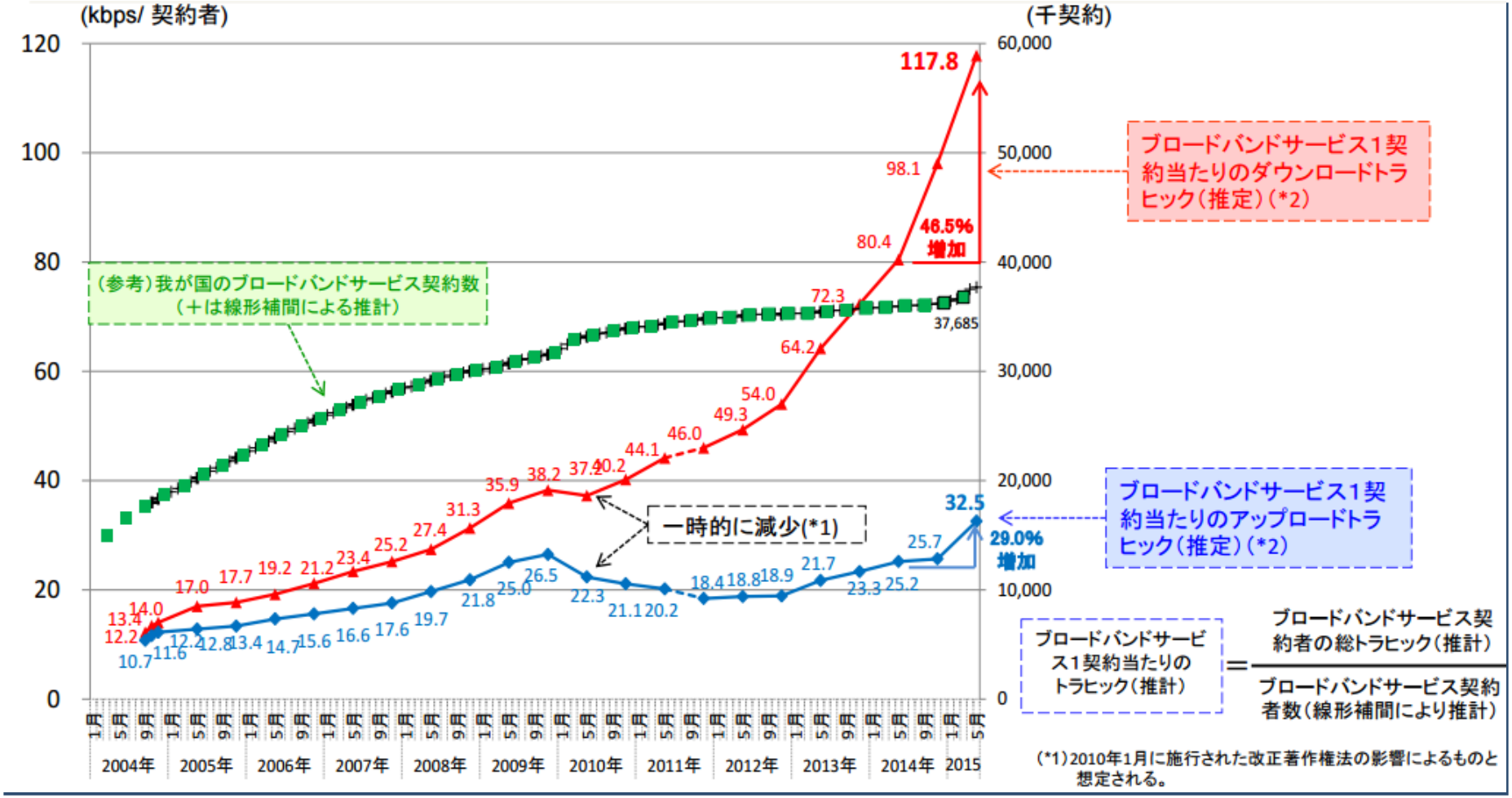
集計:2015年5月



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**」　2015年9月30日

日本国内のトラフィック推移

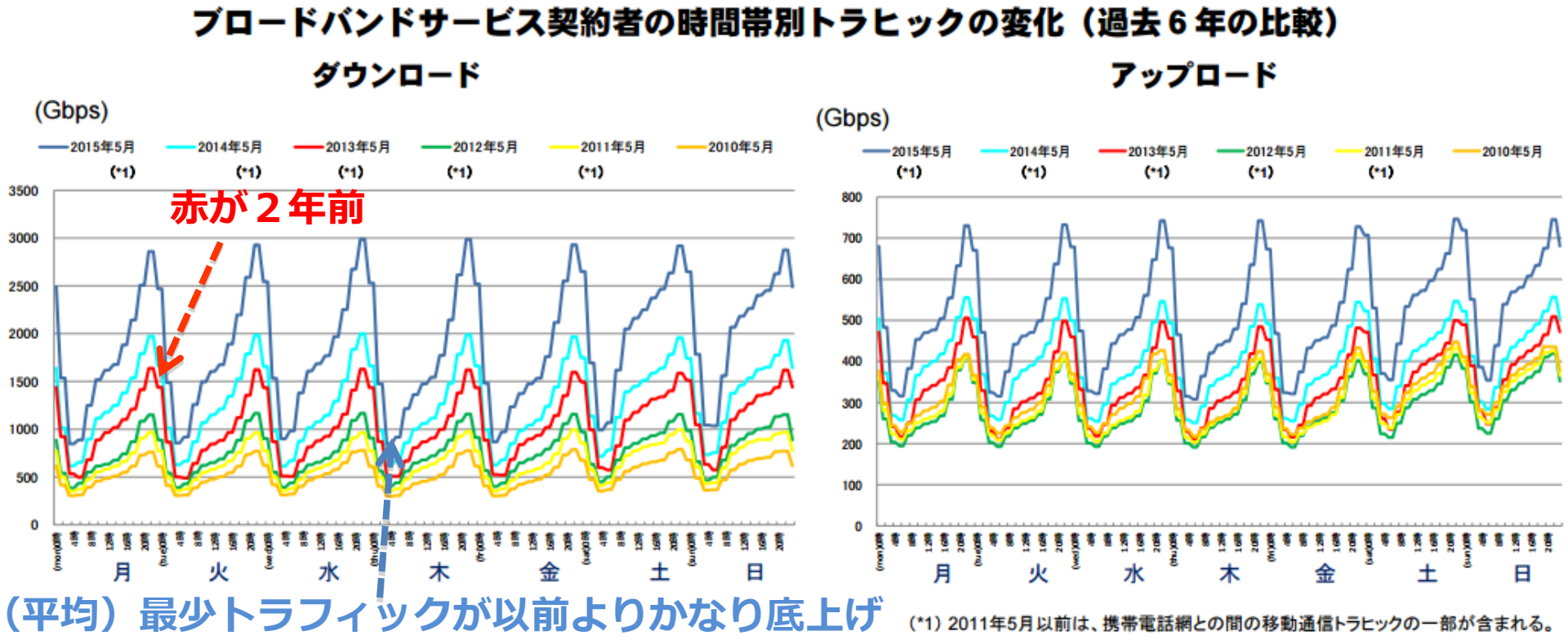
1契約者あたりのブロードバンドトラフィックの推移



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**」　2015年9月30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



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**」　2015年9月30日

「平成26年情報通信メディアの利用時間と情報行動に関する調査報告書」より

平成26年 自宅での無線LANによるインターネット接続（全年代・年代別・男女別あり）

（調査対象者全体のうちの割合）

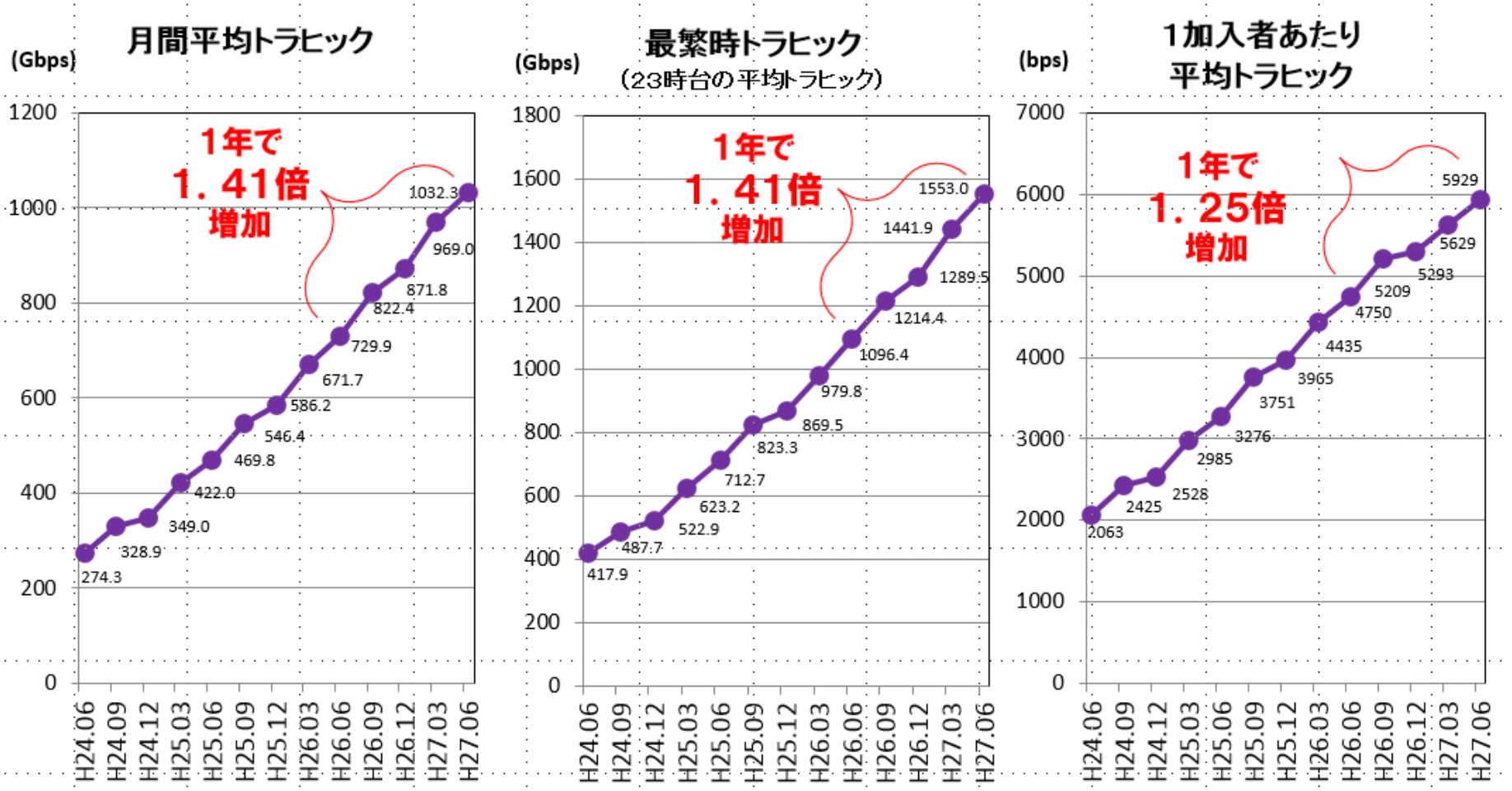
	自宅で無線LANを利用	自宅に無線LANはあるが自分は非利用
全年代（N=1500）	58.7%	9.9%
10代（N=140）	70.7%	7.9%
20代（N=221）	66.1%	4.5%
30代（N=281）	66.2%	4.6%
40代（N=303）	68.0%	7.3%
50代（N=255）	52.5%	16.9%
60代（N=300）	36.7%	16.3%
男性（N=755）	61.1%	9.0%
女性（N=745）	56.4%	10.7%
男性10代（N=72）	72.2%	5.6%
女性10代（N=68）	69.1%	10.3%
男性20代（N=113）	64.6%	7.1%
女性20代（N=108）	67.6%	1.9%
男性30代（N=143）	60.8%	4.9%
女性30代（N=138）	71.7%	4.3%
男性40代（N=153）	73.2%	5.2%
女性40代（N=150）	62.7%	9.3%
男性50代（N=128）	57.0%	12.5%
女性50代（N=127）	48.0%	21.3%
男性60代（N=146）	43.8%	17.1%
女性60代（N=154）	29.9%	15.6%

（スマートフォン利用者かつ自宅に固定インターネット接続回線がある者のうちの割合）

	①自宅で無線LANを利用	①のうち、パソコン等でもモバイルでも利用	①のうちパソコン等では利用、モバイルでは非利用	②自宅に無線LANはあるが自分は非利用	③自宅に無線LANはない
全年代（N=773）	80.5%	69.7%	10.7%	6.5%	12.4%
10代（N=88）	79.5%	75.0%	4.5%	5.7%	14.8%
20代（N=162）	80.2%	67.9%	12.3%	5.6%	13.6%
30代（N=180）	81.7%	73.3%	8.3%	2.8%	13.9%
40代（N=191）	84.3%	74.9%	9.4%	6.3%	9.4%
50代（N=104）	76.9%	64.4%	12.5%	10.6%	11.5%
60代（N=48）	70.8%	43.8%	27.1%	16.7%	12.5%
男性（N=405）	81.7%	69.9%	11.9%	5.9%	11.6%
女性（N=368）	79.1%	69.6%	9.5%	7.1%	13.3%
男性10代（N=46）	82.6%	80.4%	2.2%	2.2%	15.2%
女性10代（N=42）	76.2%	69.0%	7.1%	9.5%	14.3%
男性20代（N=81）	79.0%	64.2%	14.8%	8.6%	12.3%
女性20代（N=81）	81.5%	71.6%	9.9%	2.5%	14.8%
男性30代（N=86）	77.9%	72.1%	5.8%	2.3%	16.3%
女性30代（N=94）	85.1%	74.5%	10.6%	3.2%	11.7%
男性40代（N=103）	87.4%	77.7%	9.7%	3.9%	8.7%
女性40代（N=88）	80.7%	71.6%	9.1%	9.1%	10.2%
男性50代（N=54）	81.5%	64.8%	16.7%	7.4%	11.1%
女性50代（N=50）	72.0%	64.0%	8.0%	14.0%	12.0%
男性60代（N=35）	80.0%	48.6%	31.4%	17.1%	2.9%
女性60代（N=13）	46.2%	30.8%	15.4%	15.4%	38.5%

出典：総務省「**平成26年情報通信メディアの利用時間と情報行動に関する調査報告書**」　2015年5月19日

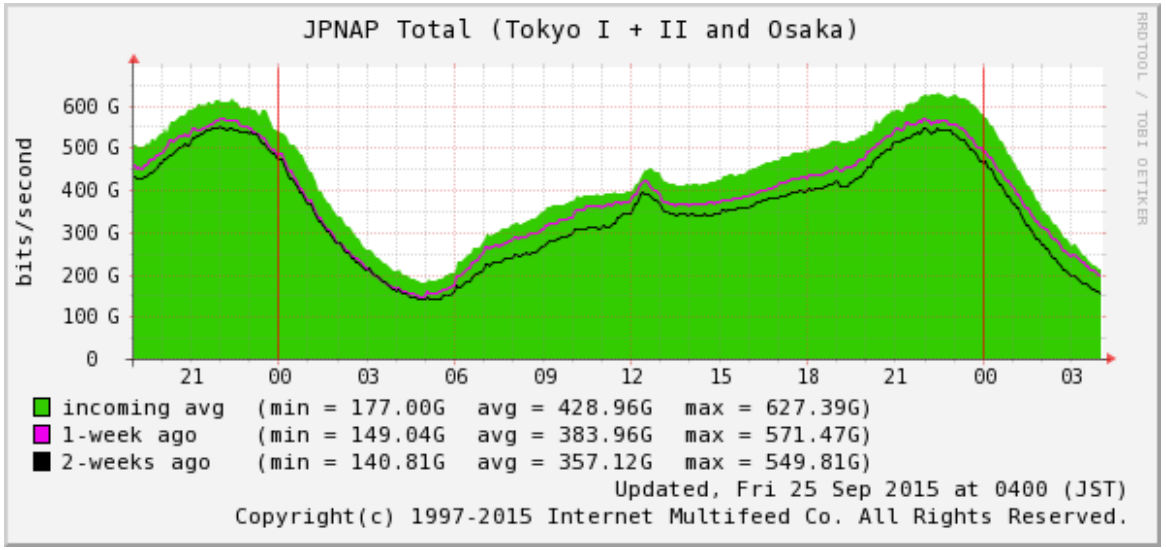
移動通信トラヒックの推移（過去３年間）



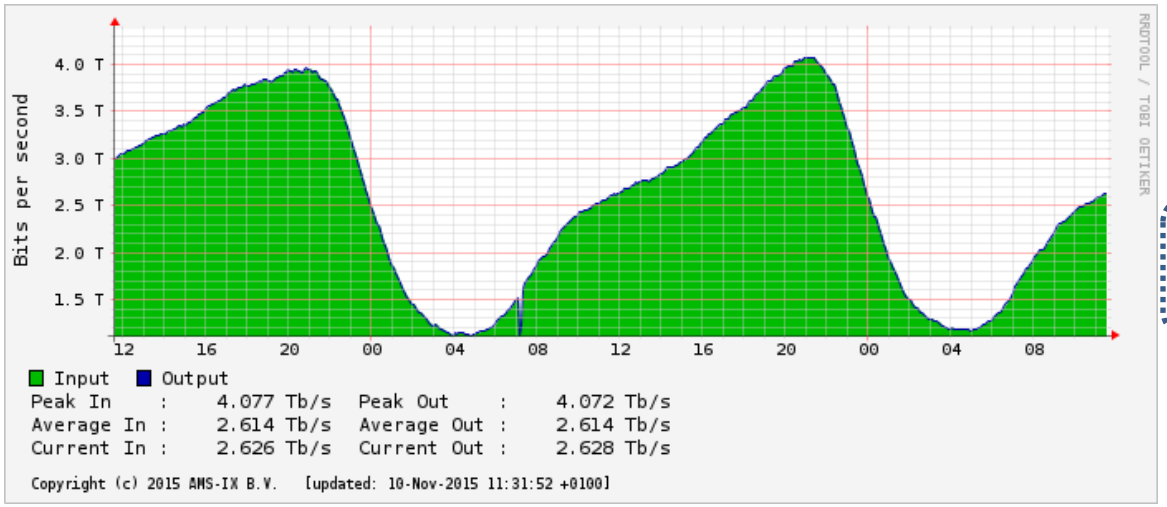
出典：総務省「**我が国の移動通信トラヒックの現状**」

1日のトラフィック傾向

ピークは夜の22時～23時の間の早い時間へとシフトしている傾向
日本のお昼のトラフィックは特徴的



JPNAP(Japan)の
1日のトラフィック推移

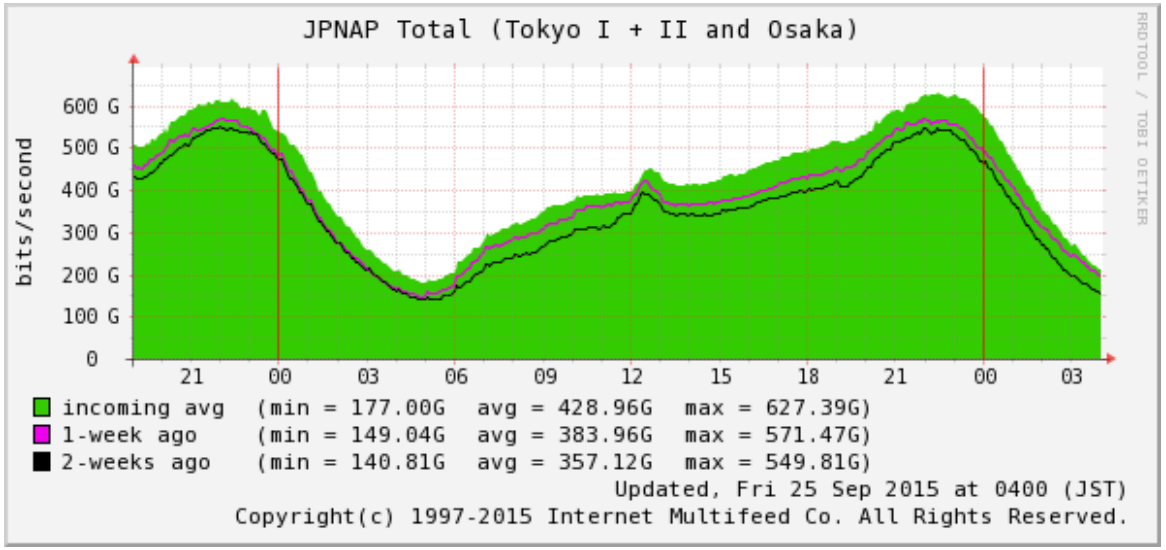


AMS-IX(Europe)の
1日のトラフィック推移

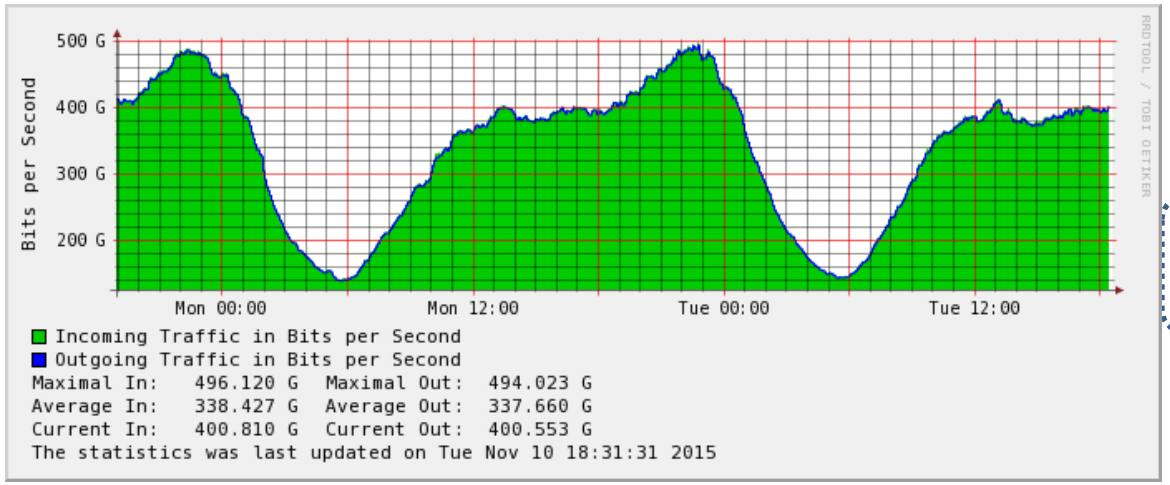
https://ams-ix.net/technical/statistics

1日のトラフィック傾向

ピークは夜の22時～23時の間の早い時間へとシフトしている傾向
日本のお昼のトラフィックは特徴的



JPNAP(Japan)の
1日のトラフィック推移



HKIX(香港)の
1日のトラフィック推移

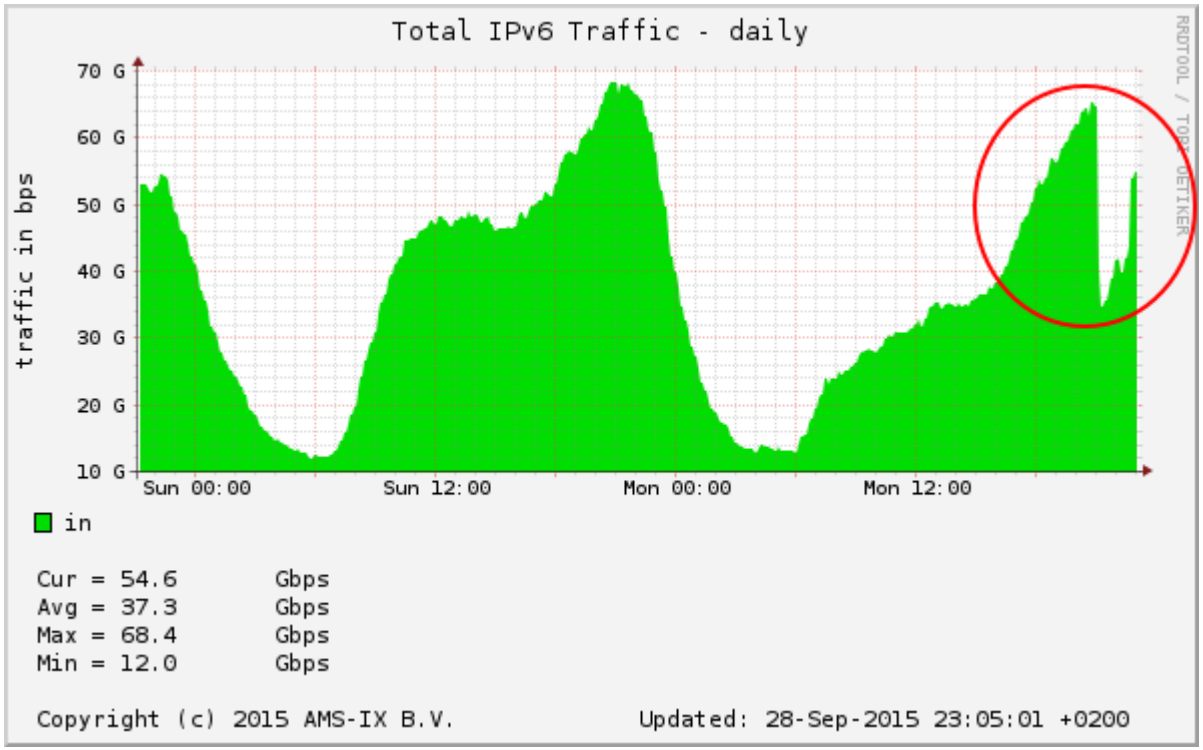
http://www.hkix.net/hkix/stat/aggt/hkix-aggregate.html

トラフィックの急激な変動

- 何が異常で何が正常か？
  - 全体の流量だけを見ていると分かりずらい
- 監視する
  - 接続先ごとに閾値での監視をする
  - でも結構難しいです
    - 意図してトラフィックを移しているだけかもしれない
  - 最近はApple iOSやMS windows update等のトラフィックがどこから流入してくるかわからない
    - コンテンツ事業者側が激しくコントロールをし、時として同じ状況にならないことも多く、通信事業者が最近困ってしまうケースもある
    - ただし、あいている帯域をうまく活用できる場合もあり、一概に良し悪しは言いにくいが、ユーザ側がコントローラブルではないことは確か。。

Facebook down

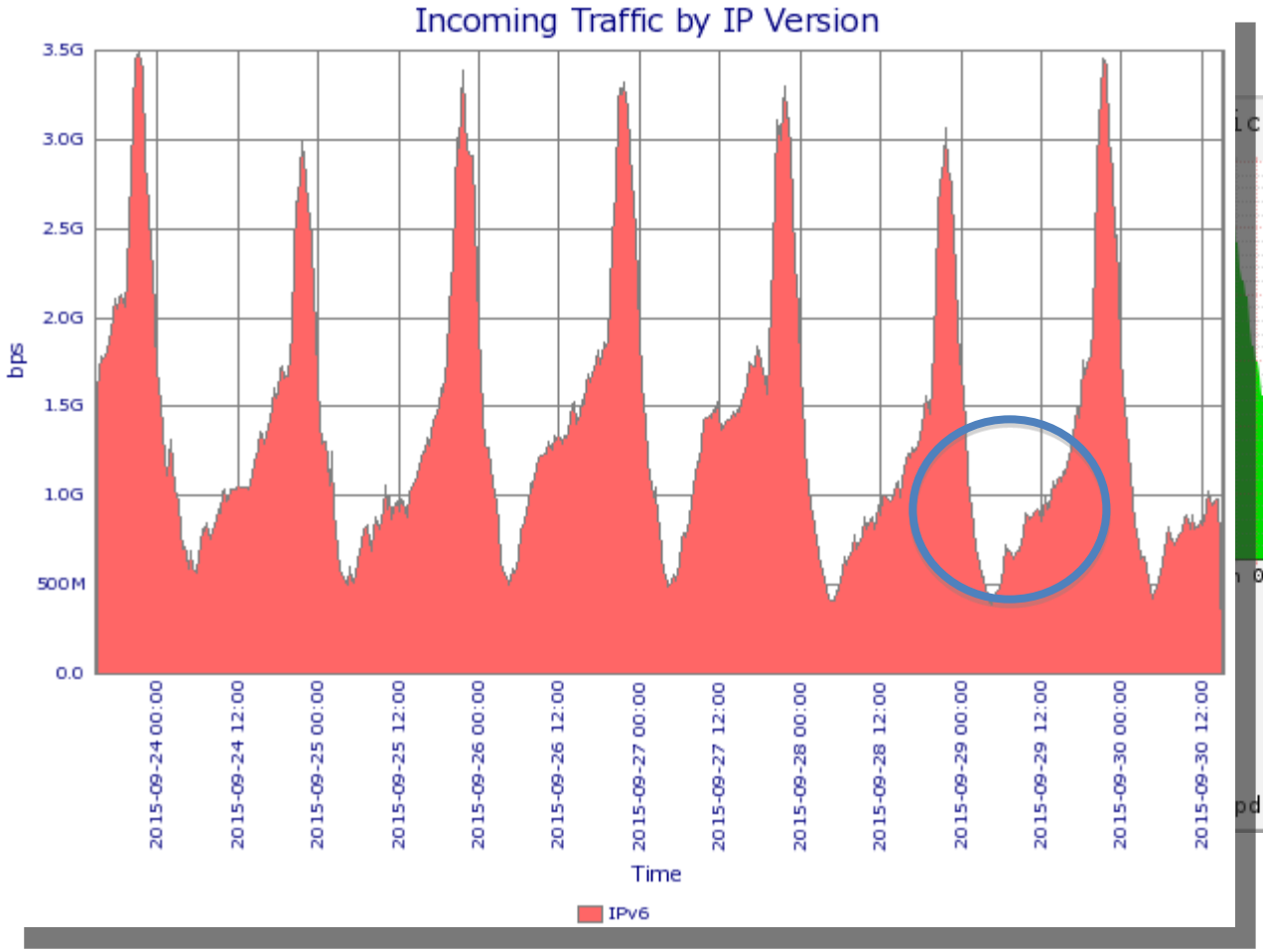
FacebookがダウンしたときのAMS-IXのIPv6のトラフィックグラフ



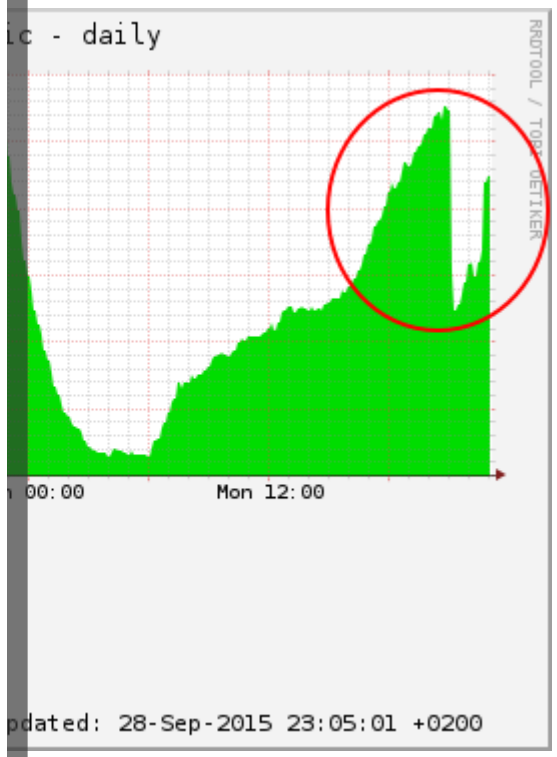
https://ams-ix.net/technical/statistics/sflow-stats/ipv6-traffic

Facebook down vs IPv6

JPNAP



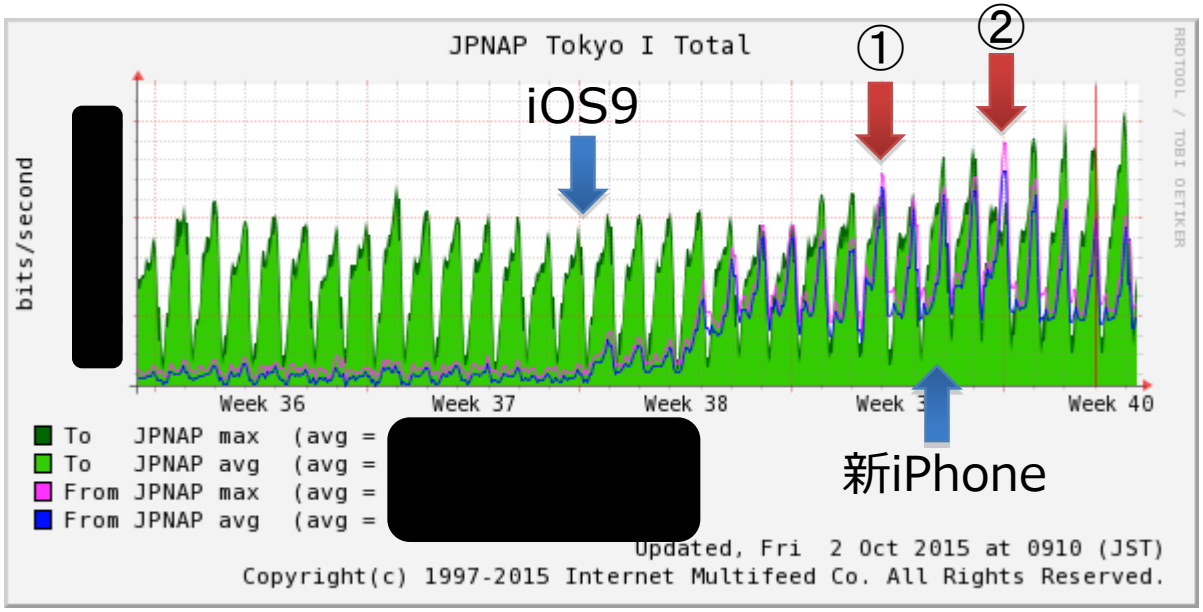
AMS-IX



殆ど変化見られず・・・

時間帯が明け方だったため、JPNAPでは全く影響が見られず。 (AMS-IXは+0200, 日本は+0900なので7時間差)　そもそもv6のトラフィック量が20倍近く違う。

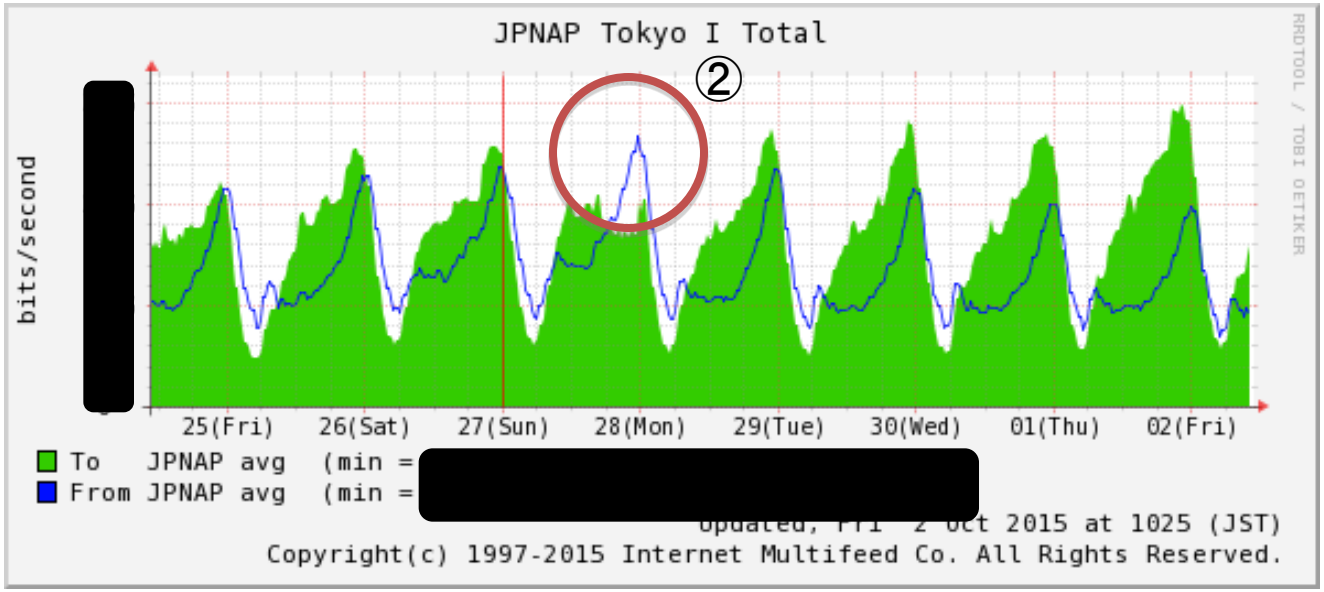
A*****のEyeball化現象



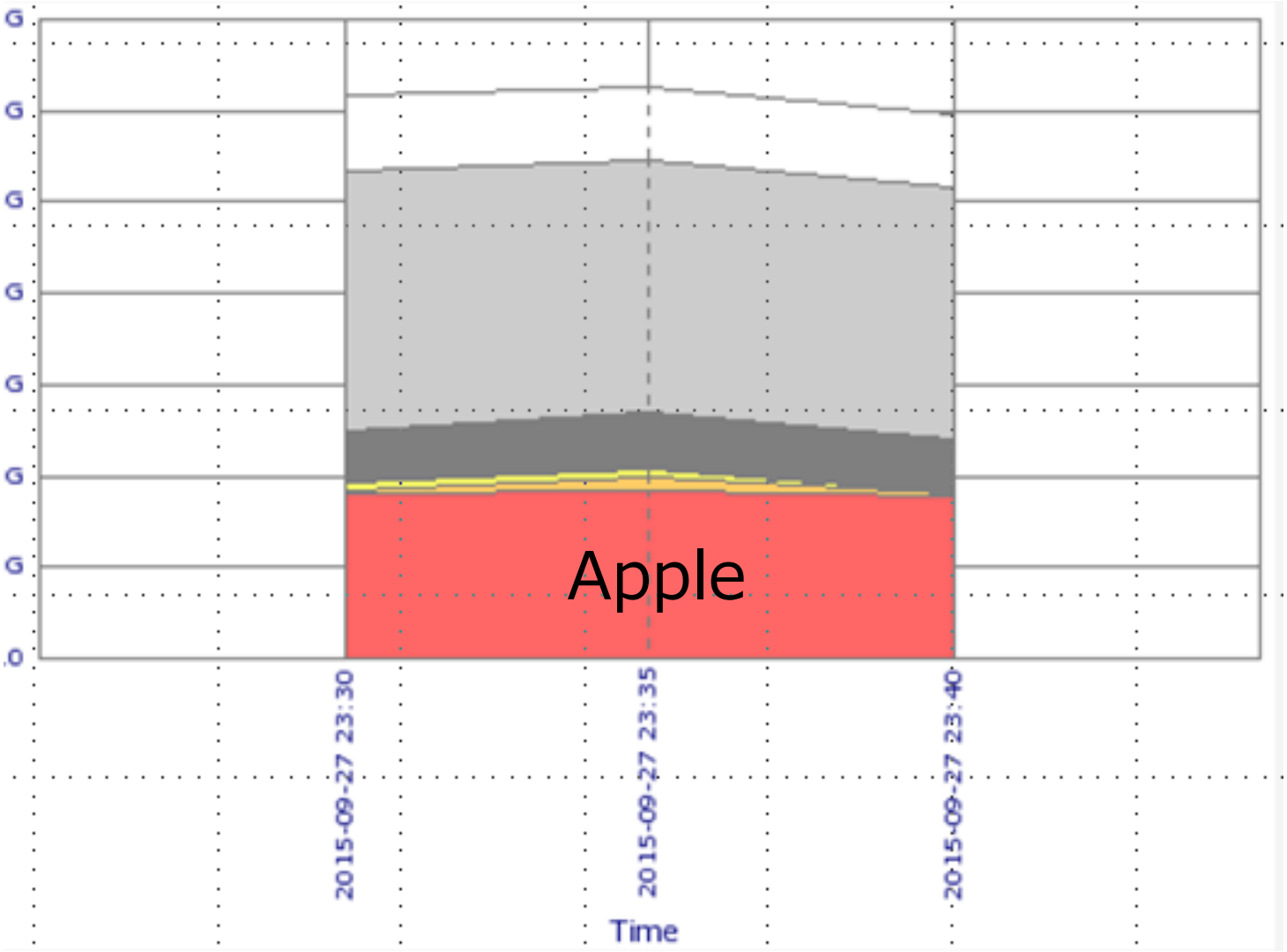
①連休最終日の水曜
②週明け直前の日曜日

に、逆転

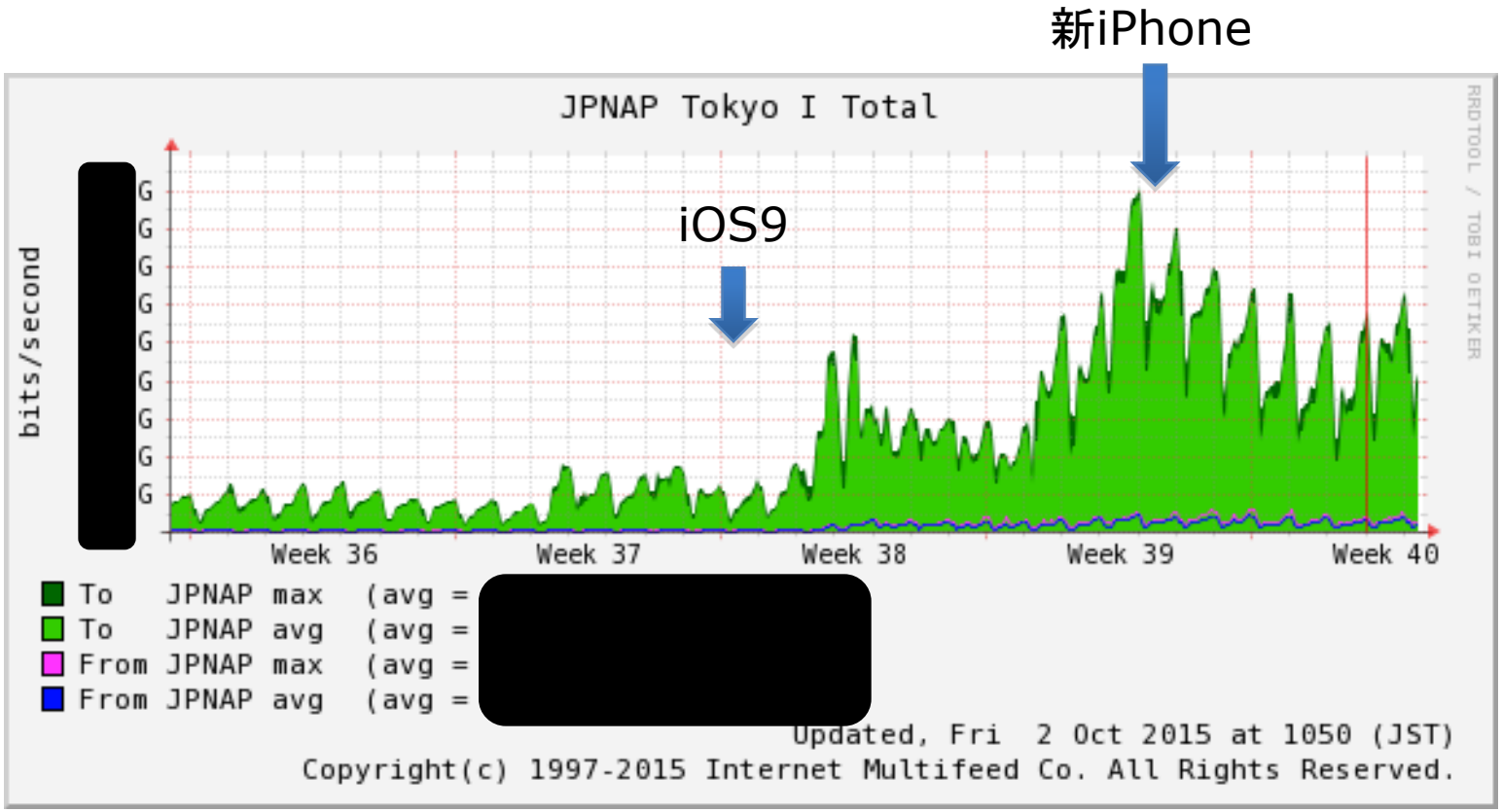
現在は徐々に収束中？



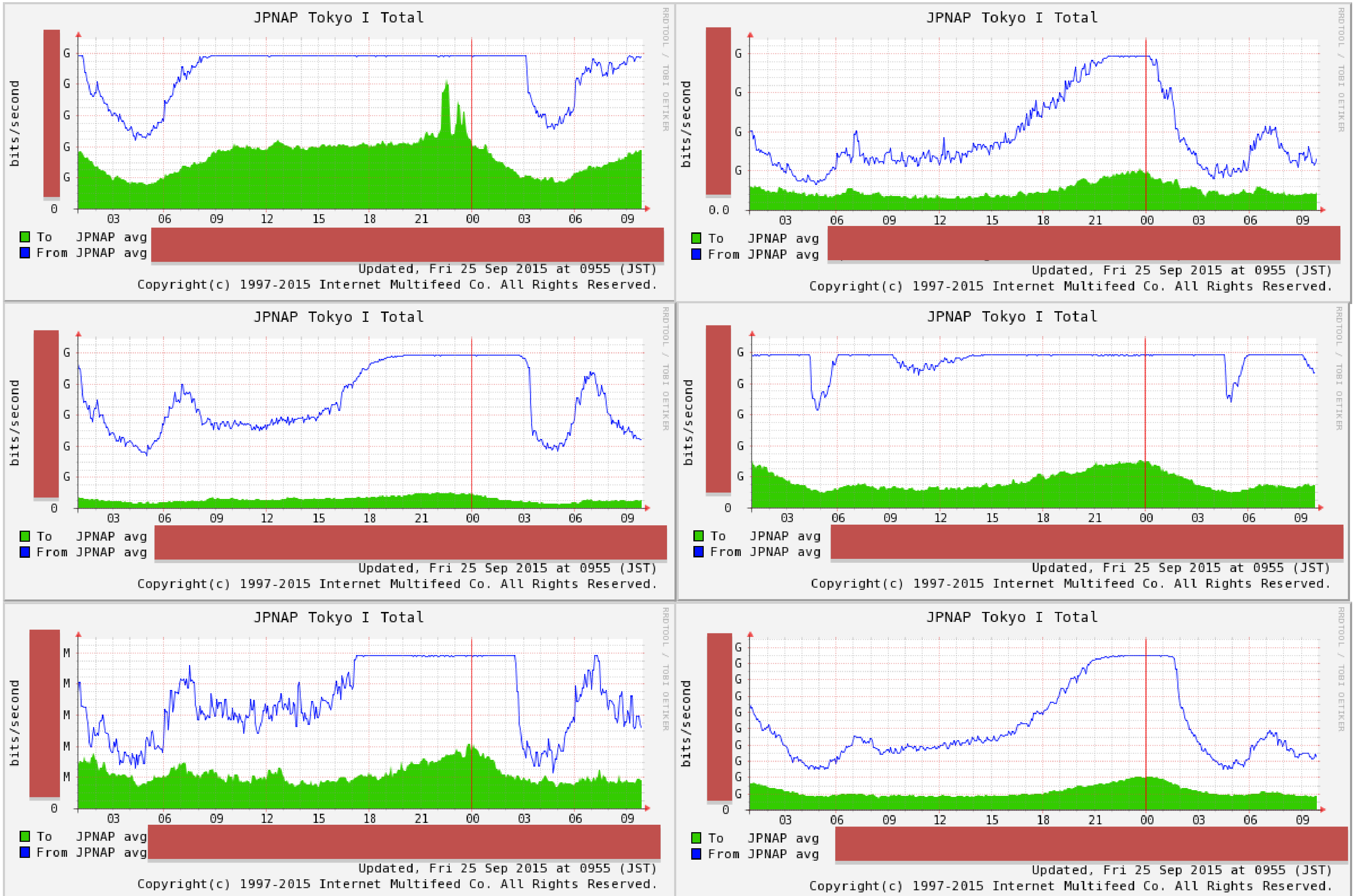
A*****のEyeball化現象



Impact of iOS9



Impact of iOS9



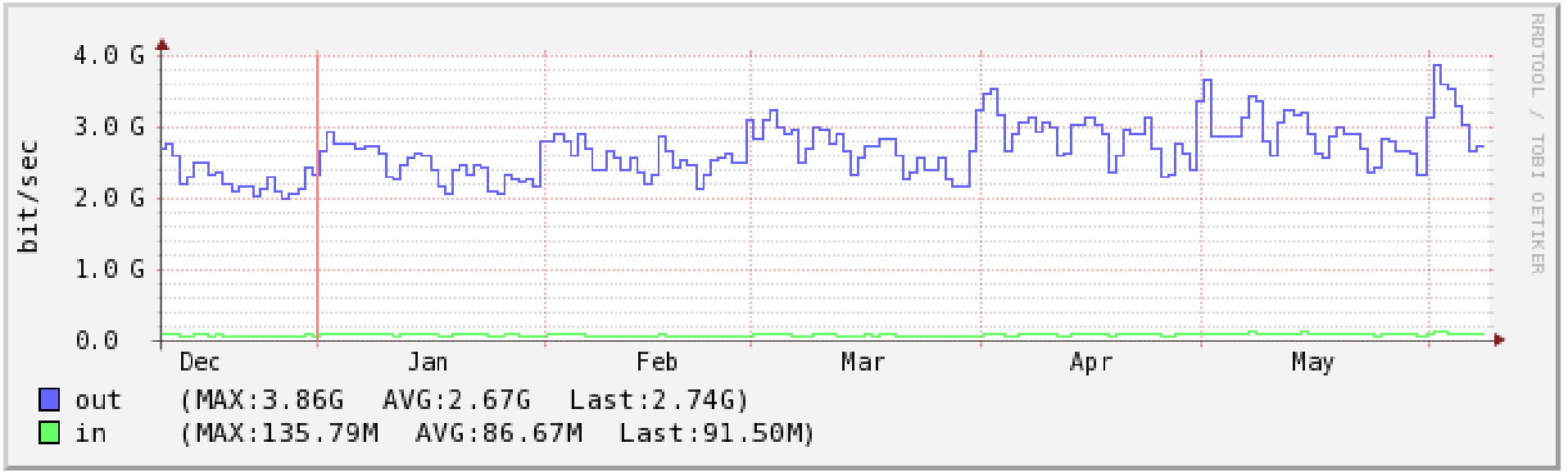
iOS9の各社向け配信状況

iOS8と比較するとAppleAS配信比率（緑）があがっている

情報提供：NTTコム亀井氏

月末に向けて減少するトラフィック

- 月初から月末にかけてトラフィックが落ち込んでいく



**** の 10月 の通信量の合計バイト数が7GBを超えましたのでお知らせします。当月の通信速度が送受信時最大128kbpsになります。

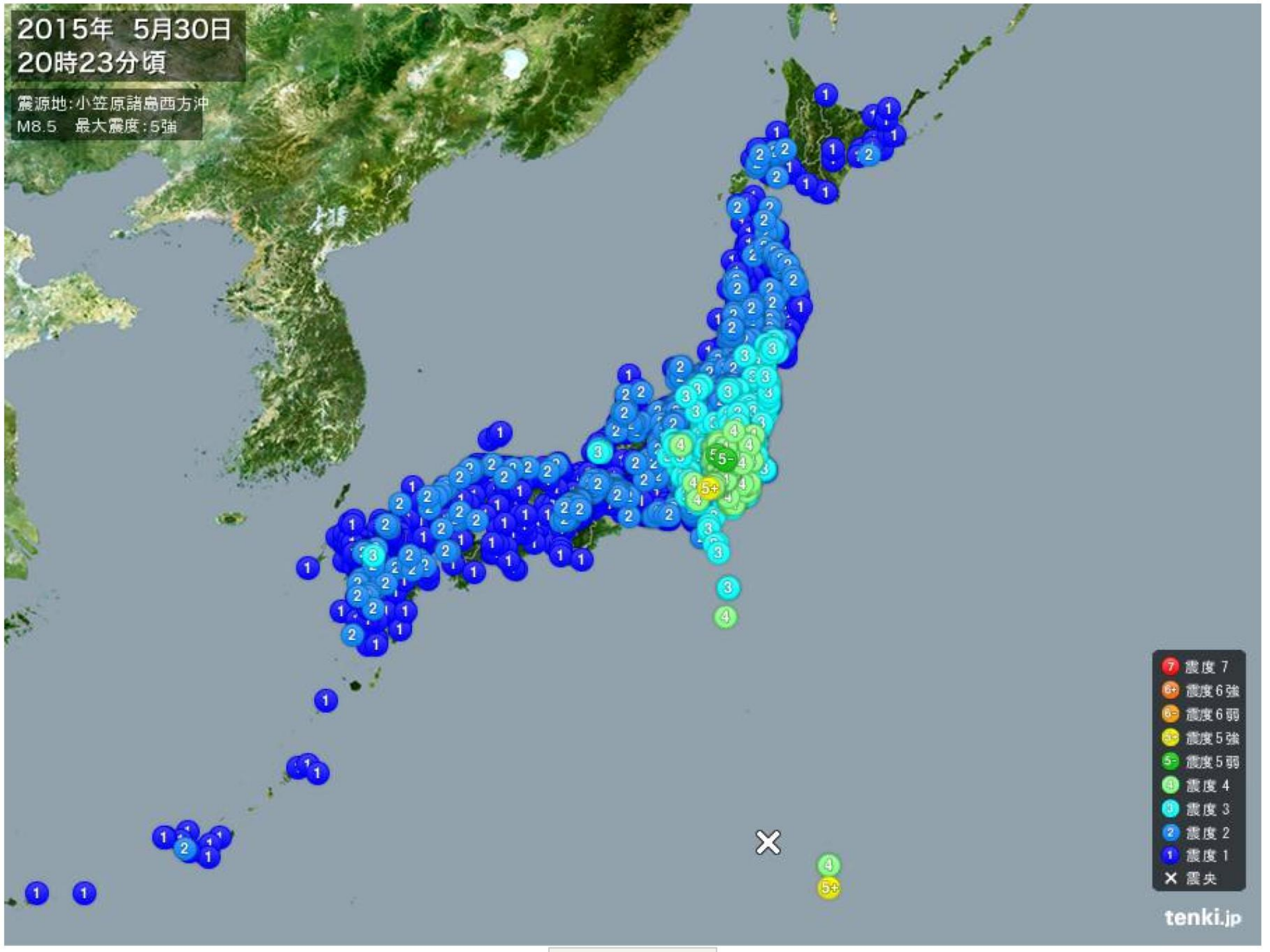
Fr:au/KDDI
Sub:7.00GBを超過したため通信速度が制限されます。容量追加→
https://cs.kddi.com/dc

Sub:通信量が　月　日に7.00GBを超えました。月末まで通信速度が制限されます

- 全体的にもう少し平準化してもよさそう
  - Softbankは、月初、10日、20日締め

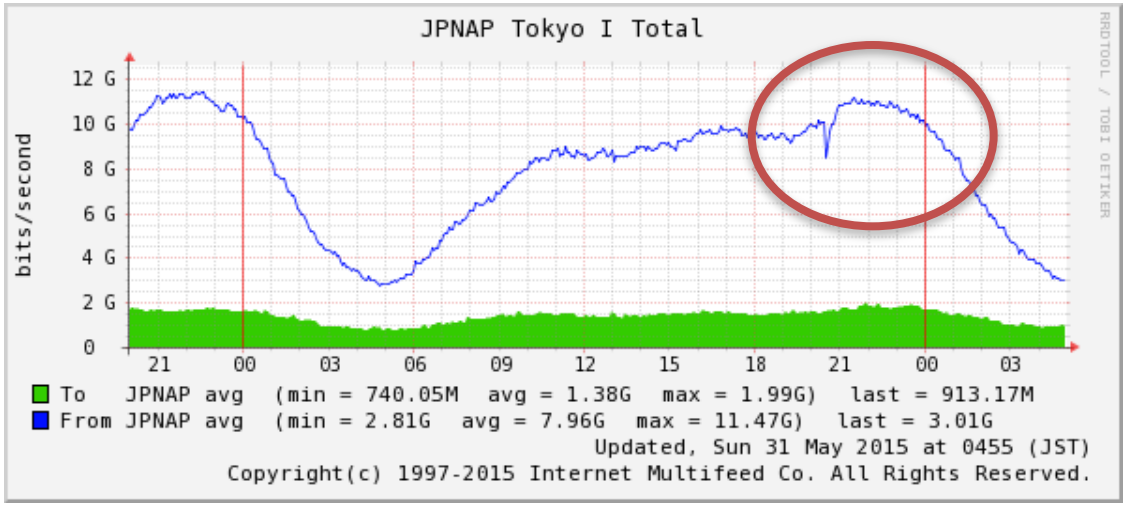
締め日	請求月
10日	前月11日～当月10日
20日	前月21日～当月20日
末日	当月1日～当月末日

  - トラフィックの変動が少なくなる
  - CS部門の問い合わせ対応も平準化されるはず

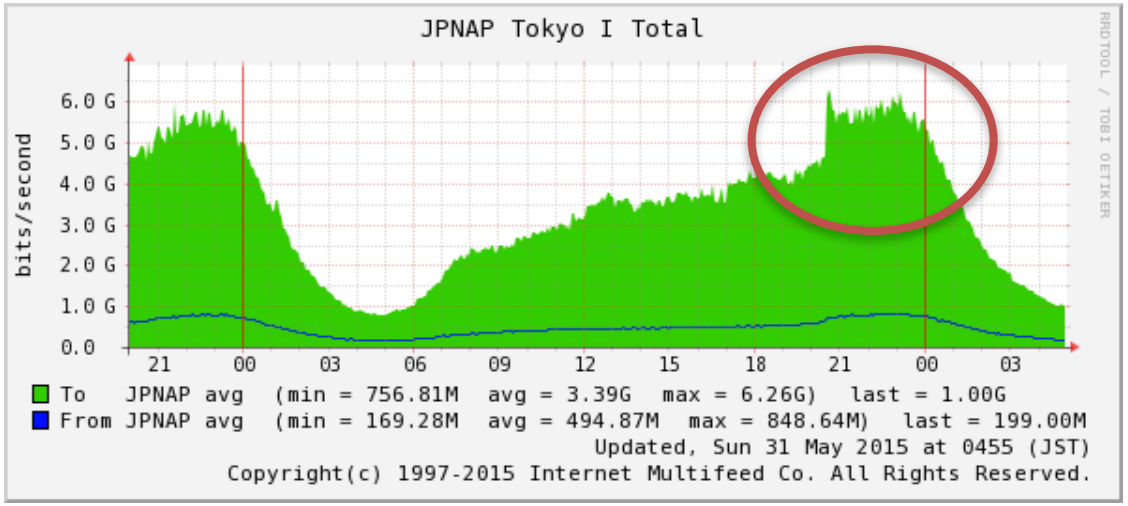

2015年　5月30日
20時23分頃
震源地:小笠原諸島西方沖
M8.5　最大震度:5強
震度 7
震度6強
震度6弱
震度5強
震度5弱
震度 4
震度 3
震度 2
震度 1
震央
tenki.jp

2015年5月30日 20時23分頃

コンシューマの
一般的な通信量



SNS等のソーシャル
メディア通信量

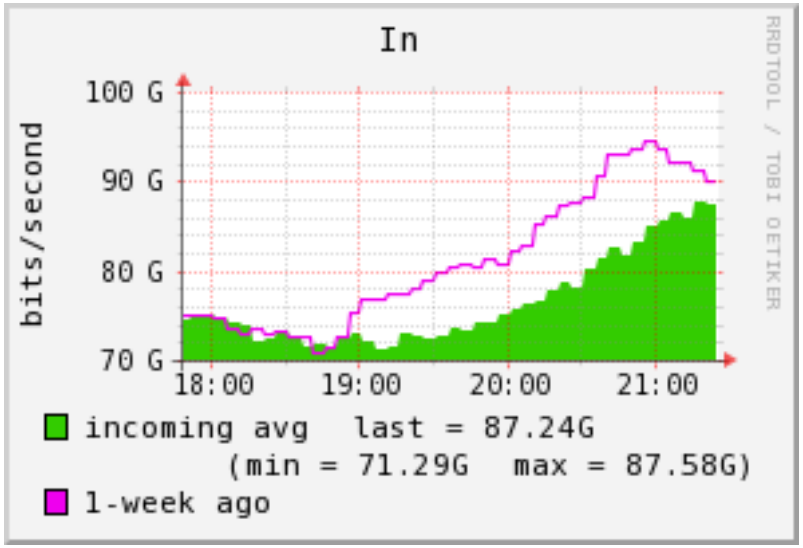


情報伝達手段にSNS等が非常に多く活用されてきている

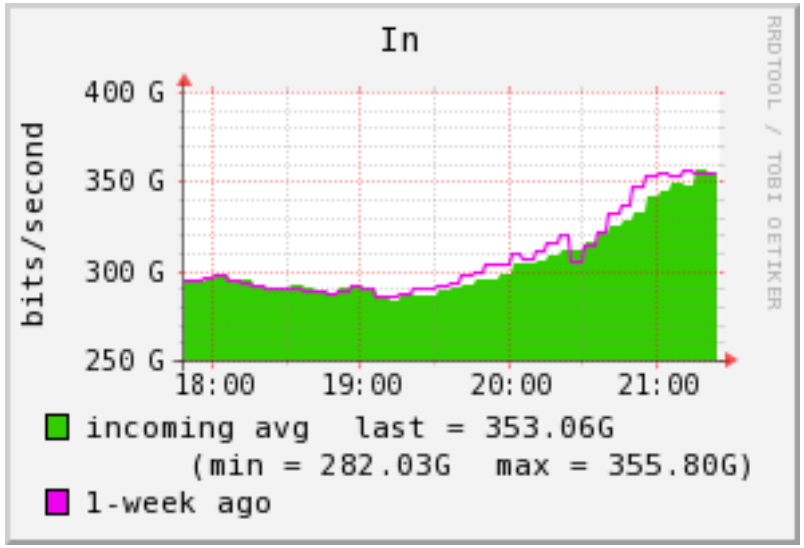
2015年6月6日

- 夜の時間帯にトラフィックの減少が観測された

関西



関東

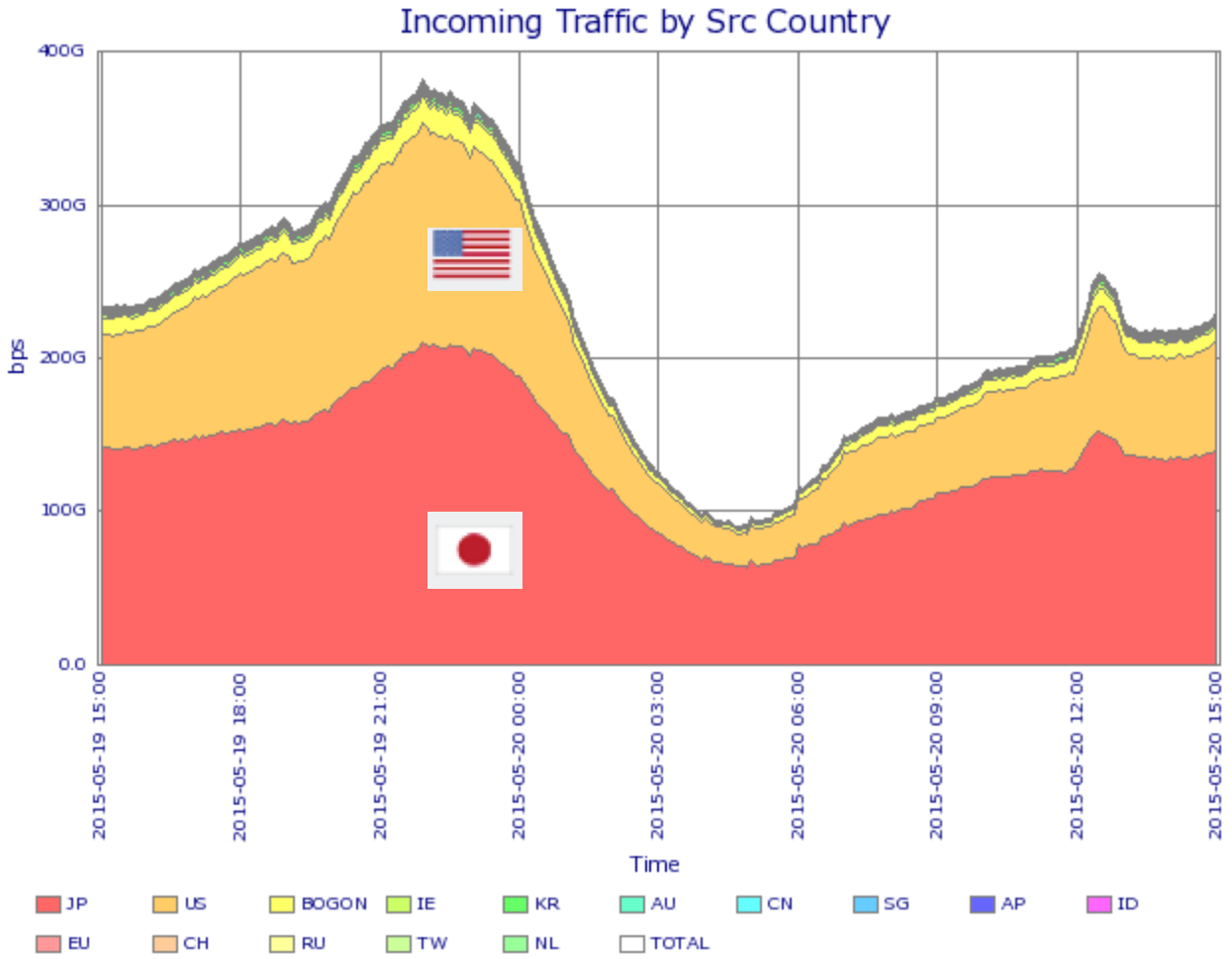


開票結果
Result

◆ 41stシングル 選抜メンバー ◆

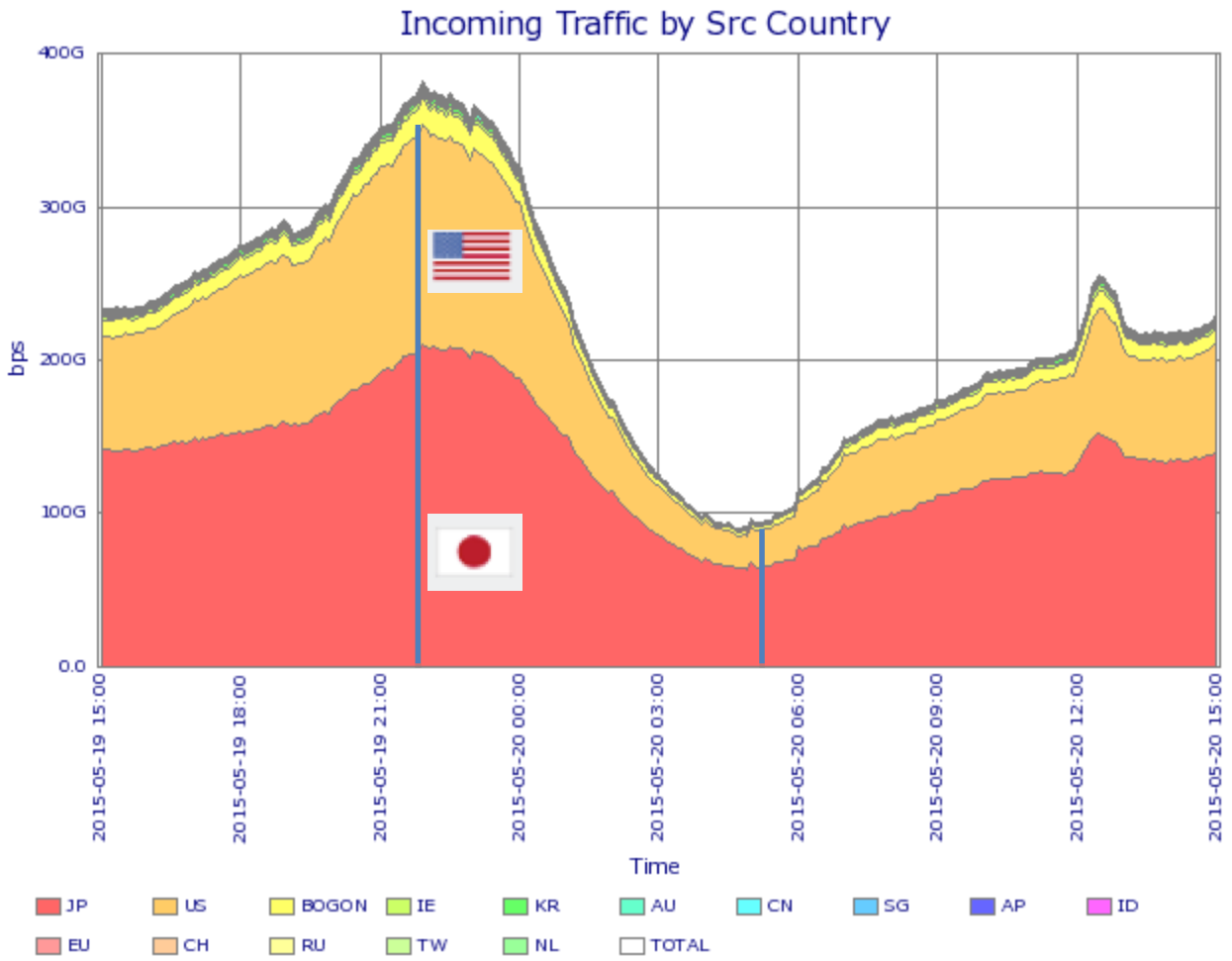
ある１日の国別トラフィック

- 国内を中心としたトラフィックが約半分、最近国内が若干増加傾向



ある１日の国別トラフィック

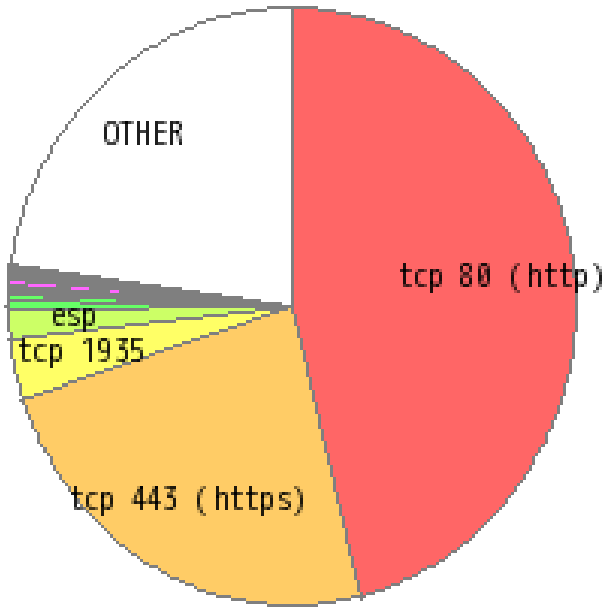
- 国内を中心としたトラフィックが約半分、最近国内が若干増加傾向
- ピーク時と明け方の国別比率が変化している（朝はUSが減少）



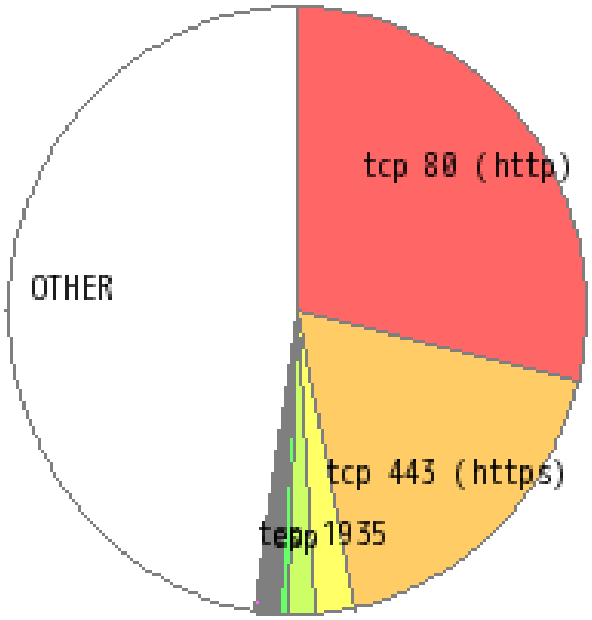
最近の利用ポート比率

- 約半分がtcp80(http)
- tcp80のパケットは大きい（ダウンロード型）ことがわかる。
- tcp443は様々なアプリケーションで利用されていると想定される

bps

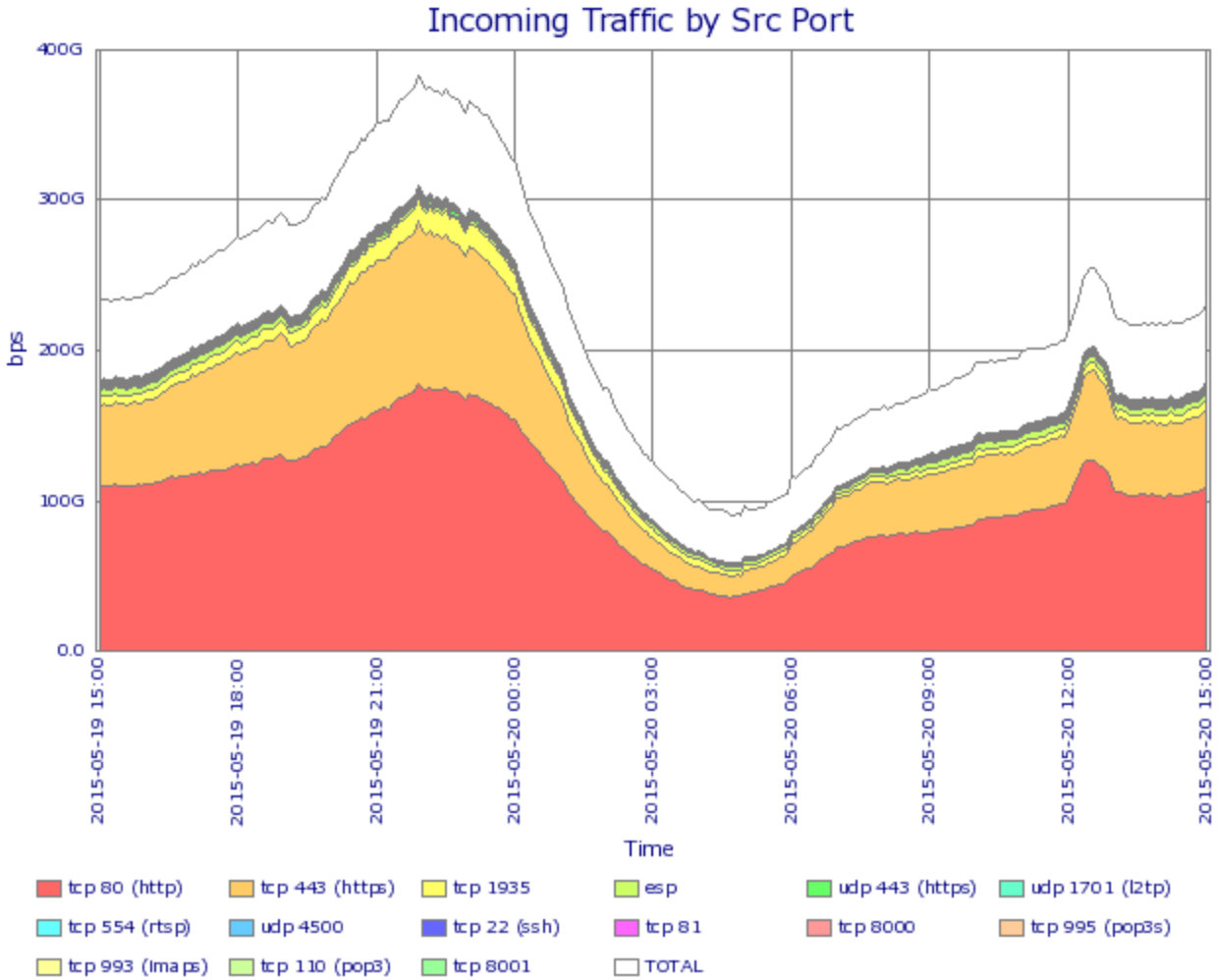


pps



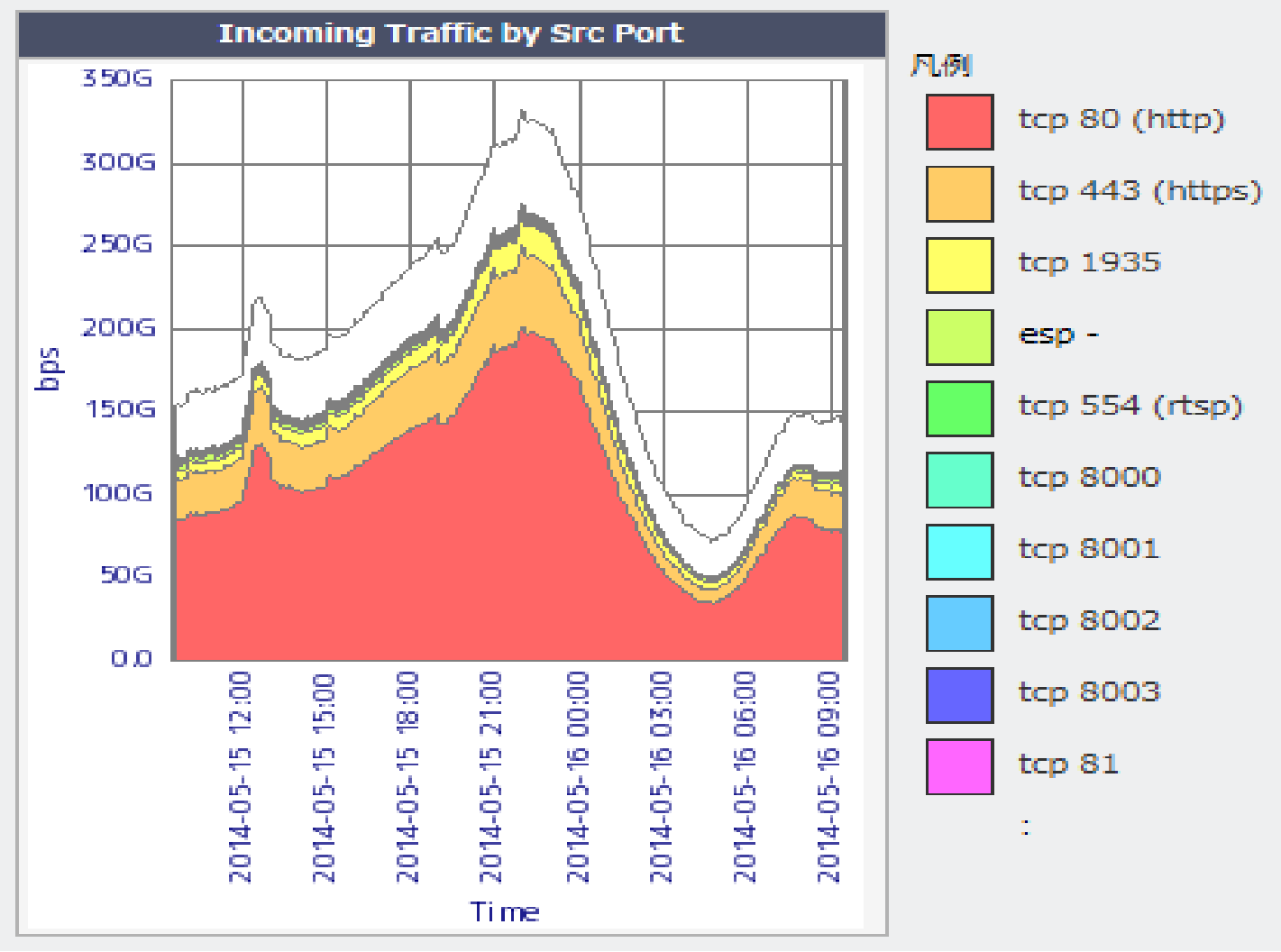
JPNAP全体での利用ポート比率

- tcp443の割合が深夜から早朝にかけて減少
- ただ過去と比べると割合が増加してきている



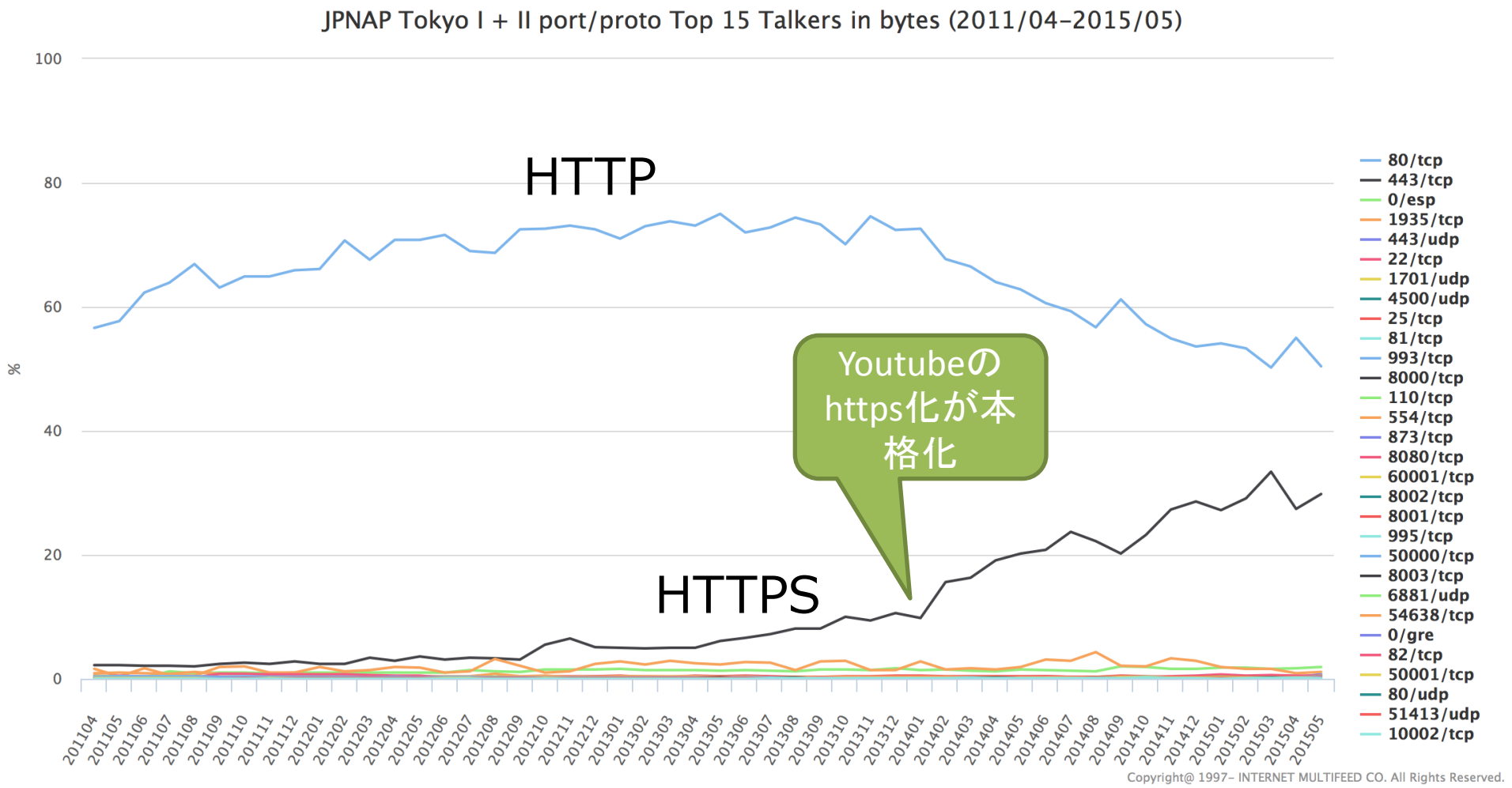
１年前

- TCP443の割合が着実に増加している



４年間の利用ポート比率

- TCP443の増加が著しい　2016年中にTCP80と逆転？



Copyright@ 1997- INTERNET MULTIFEED CO. All Rights Reserved.

既に多くのサービスがHTTPS化

Gmail

facebook

YAHOO

bing

YouTube

twitter

CIO.GOV

US政府の最高情報責任者 トニースコット氏（元Vmwareの幹部）の発表

https://cio.gov/https-everywhere-for-government/

HTTPS-Everywhere for Government

June 8th, 2015

CIO Council

Today, Federal CIO Tony Scott signed an OMB memorandum to enact the HTTPS-Only Standard for all Federal websites and web services.

OMB first proposed the standard in March and requested comment from the public. During the feedback period, the proposal received numerous comments and suggestions from Internet's standards bodies, popular web browsers, and concerned citizens [1]. To assist with the conversion to HTTPS, technical assistance and best-practices for migration are available at https://https.cio.gov – a site that is open to contribution from technical experts around the world. In addition, a public dashboard has been constructed to monitor implementation progress across the Federal web space.

Per the issuance of this Memorandum, all publicly accessible Federal websites must meet the HTTPS-Only Standard by December 31st of 2016.

NETFLIXもHTTPS化へ

Netflix to Use HTTPS to Secure Video Streams

April 20, 2015 K. Paul Mallasch Articles & News/ Security

Rate this (1 Vote)

House of Cards a Solid Foundation for Netflix

Prices for Netflix stock have been going up because the company is doing so well, especially with the coveted 18 to 34 year old demographic.

With original programming like House of Cards, Orange is the New Black and Daredevil, the streaming video service has become even more popular over the last year.

NETFLIX

Netflix HTTPS Coming Soon

https://info.ssl.com/

Useful Information

Recent Posts | Most Viewed | Recent Comments

Instagram Forgot to Renew its SSL Certificate

Upgrading a Certificate from SHA-1 to SHA-2

Logjam SSL/TLS Vulnerability: Time to FREAK Out Again?

SSL.com's Friday Security Roundup - June 5, 2015

NoCrack: Protect Passwords With Fake Ones?

Top Rated

Posts:

FAQ: Can I Use Wildcard Domain...

HTTPS化の加速

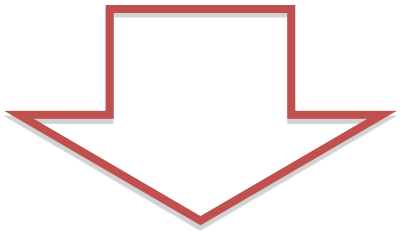
- 通信がセキュアになる
- Google
  - HTTPS をランキング シグナルに使用すると名言
- 従来できていたことが困難に
  - ログやデータ解析
  - リファラの取得
- SSLのオーバーヘッド

ところで

＋ YouTube w/IPv6

実はUDP443

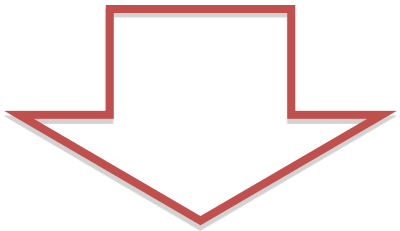
＋ YouTube w/IPv6



QUIC w/IPv6

Google: chromeユーザの半数はQUICによるリクエストになっている

+ YouTube w/IPv6



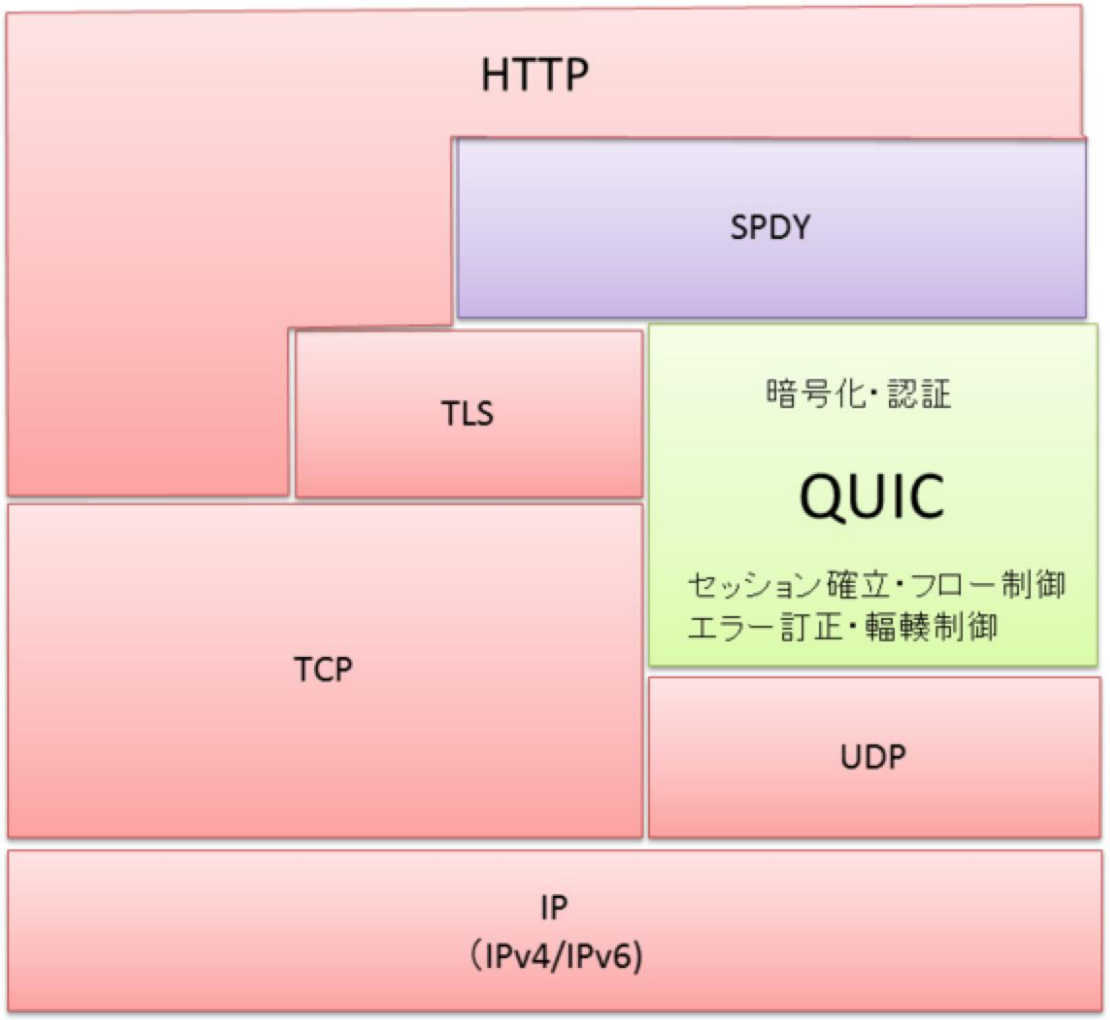
Jiri H 1 か月前 - Google Chrome (News)

Googleの実験的な輸送にQUIC更新

今日では、GoogleのサーバーへのChromeからのすべての要求の約半分は、QUIC上で提供しています、私たちは最終的には、Googleのクライアントからデフォルトのトランスポート作り、QUICトラフィックを増加し続けている - Googleサーバーに - Chromeとモバイルアプリの両方。

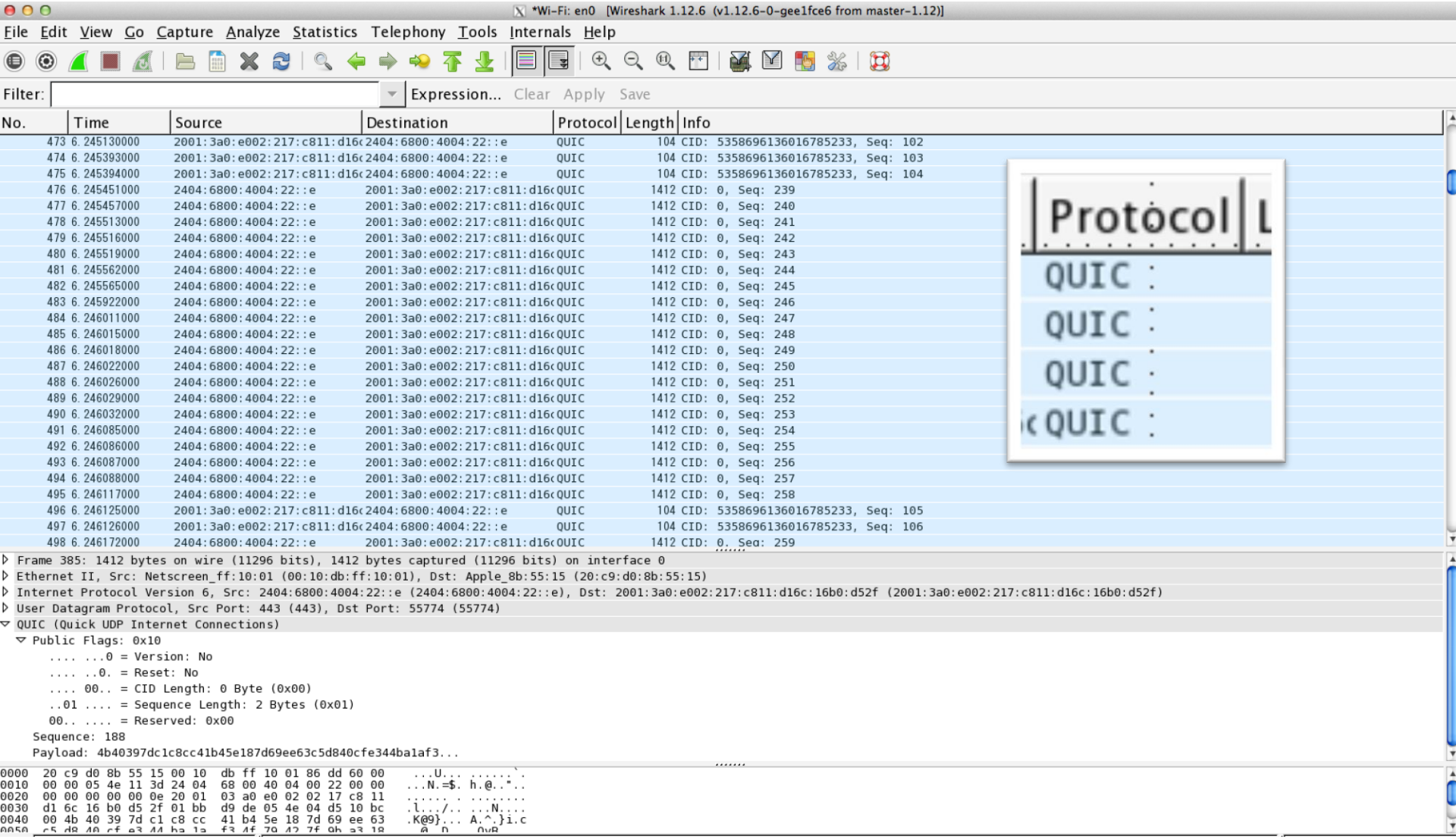
QUIC：Quick UDP Internet Connection

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

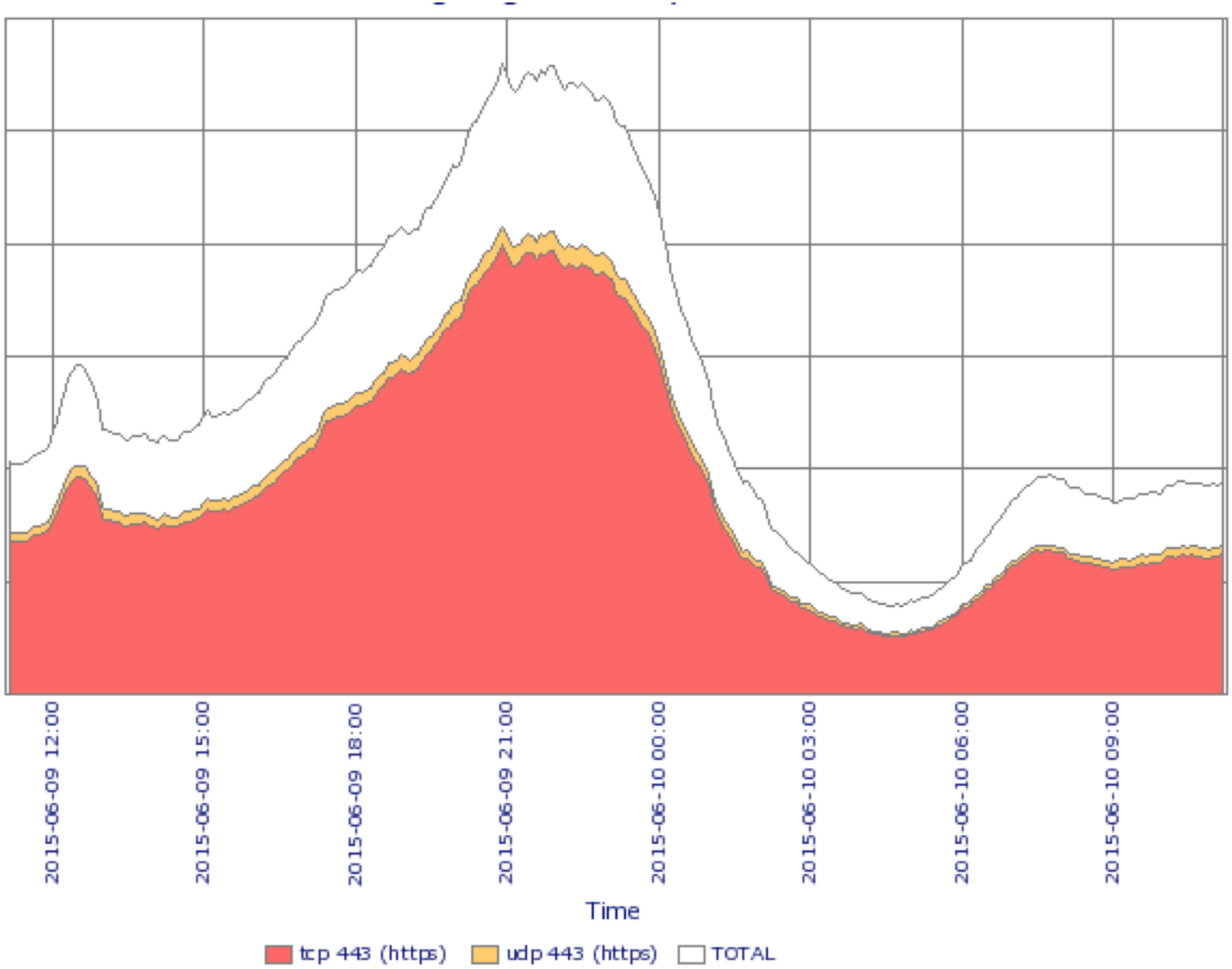


参照：http://d.hatena.ne.jp/jovi0608/20130227/1361975933

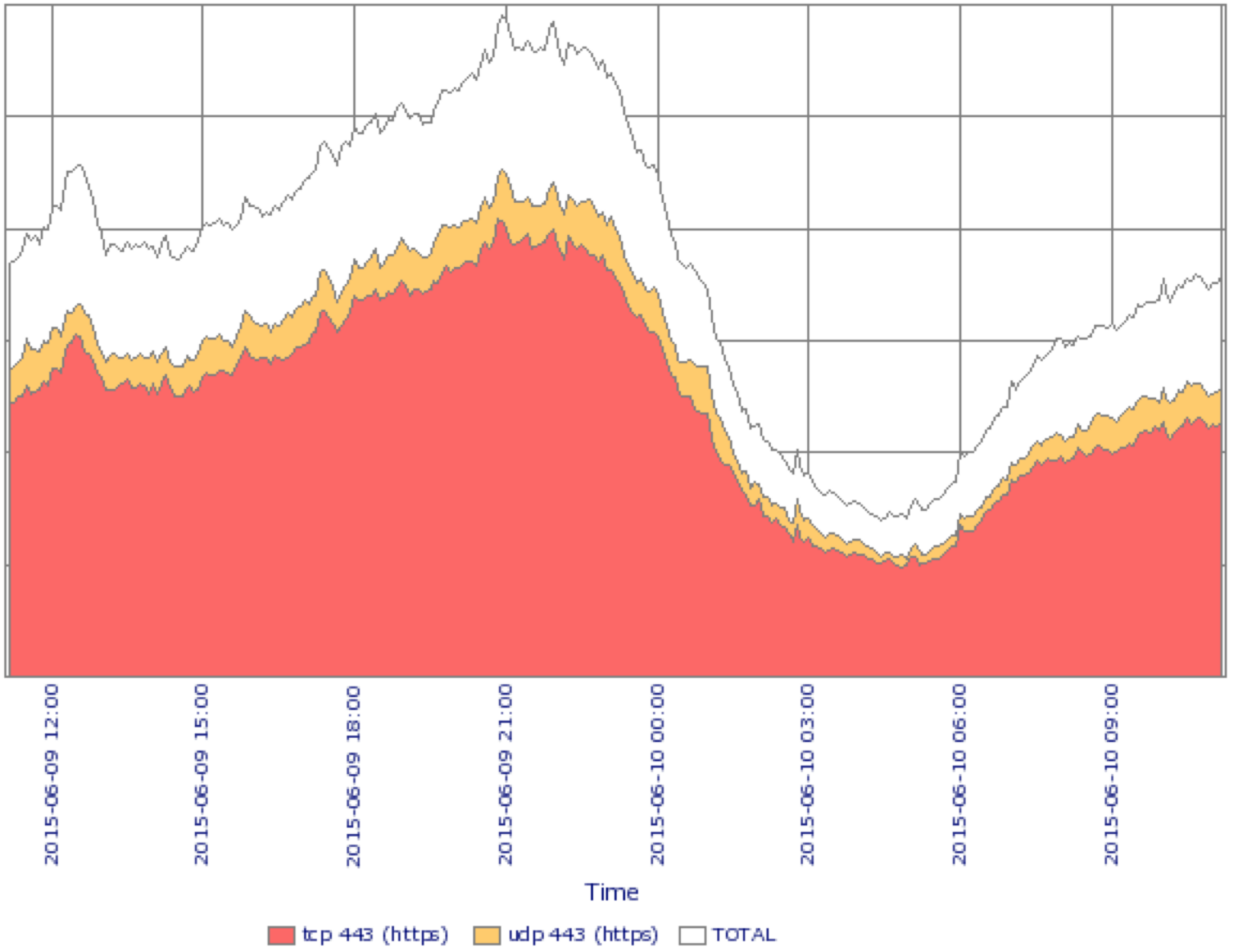
Youtubeを見ながら手元でwireshark



Server → Client へのrequest



Client → Server へのrequest



現状と今後の課題

- 増え続けるトラフィックへの対処
  - 通信事業者は容量を増加せざるを得ない
  - 一方で一時的な急激なトラフィック増加への対応
- 災害時やイベント時のトラフィック対策
  - 大規模災害、停電、公共機関の影響、イベント
- 流れるトラフィックの傾向の変化をとらえる
  - 定常的なトラフィック把握や分析が重要

内容

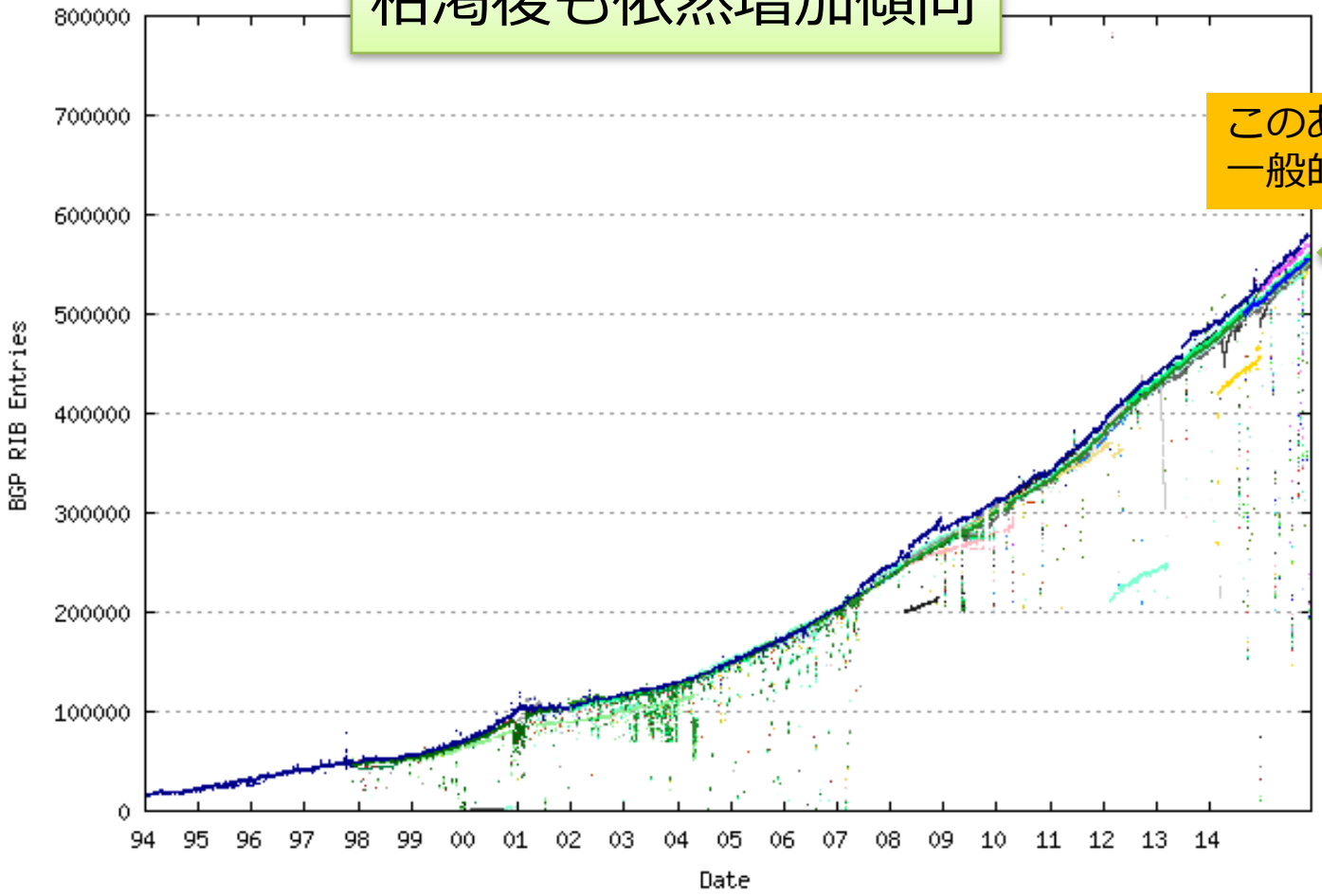
- トラフィック動向
- ルーティング動向
- DNS動向
- セキュリティ動向
- まとめ

ルーティング動向

- IPv4経路が56~57万に到達
  - 年増加率は変わらず約1.1倍で引き続き枯渇後も増加
  - /24は依然全体の半分超で、ここ最近ますます増加
  - ARIN地域も9月に枯渇
- IPv6経路は約2万5千経路に
  - 年間で約5000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
    - 64K等が上限の場合もある（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
    - 安全策をとるケースや、上位ISPが4byte未対応の影響

IPv4経路数の推移

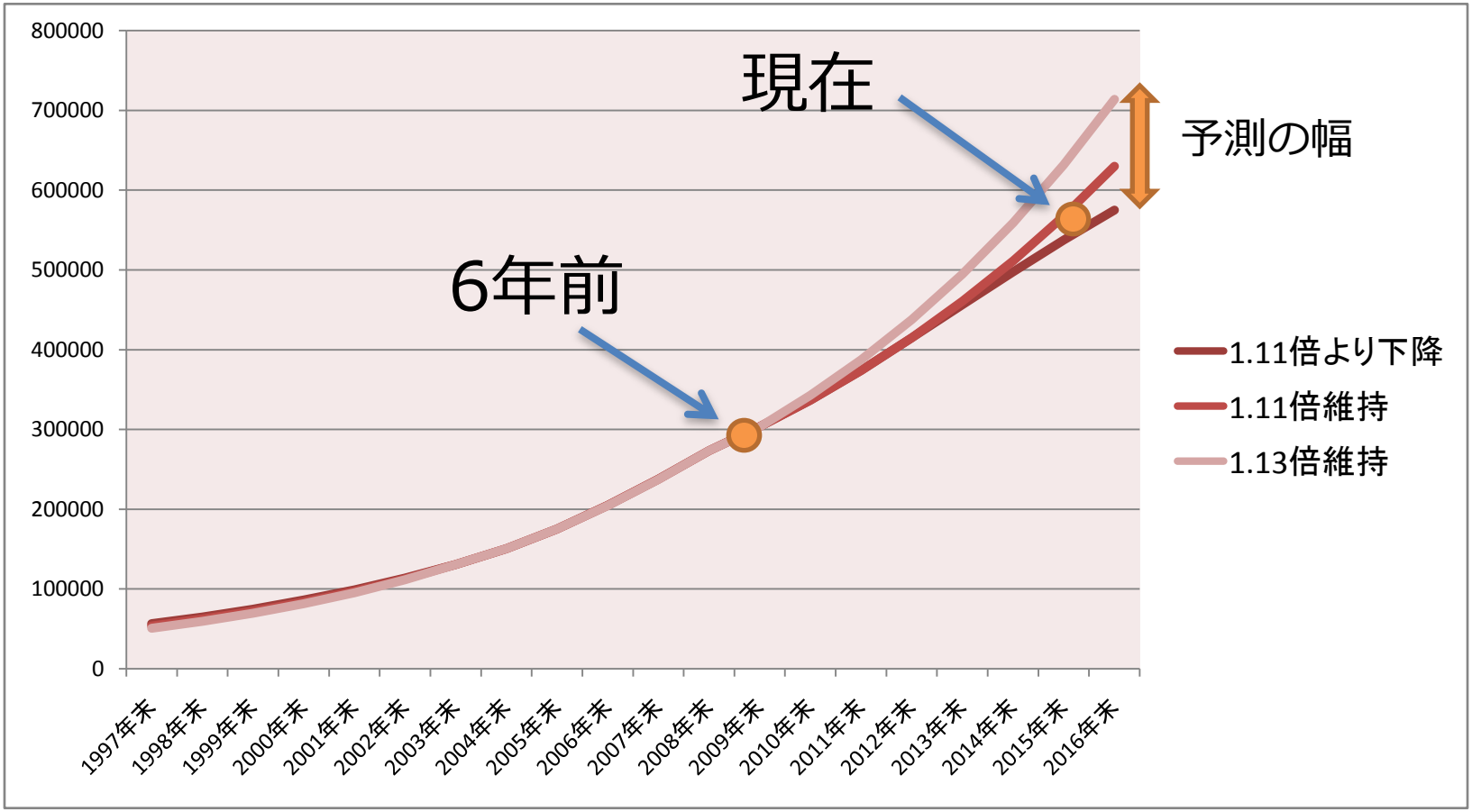
枯渇後も依然増加傾向



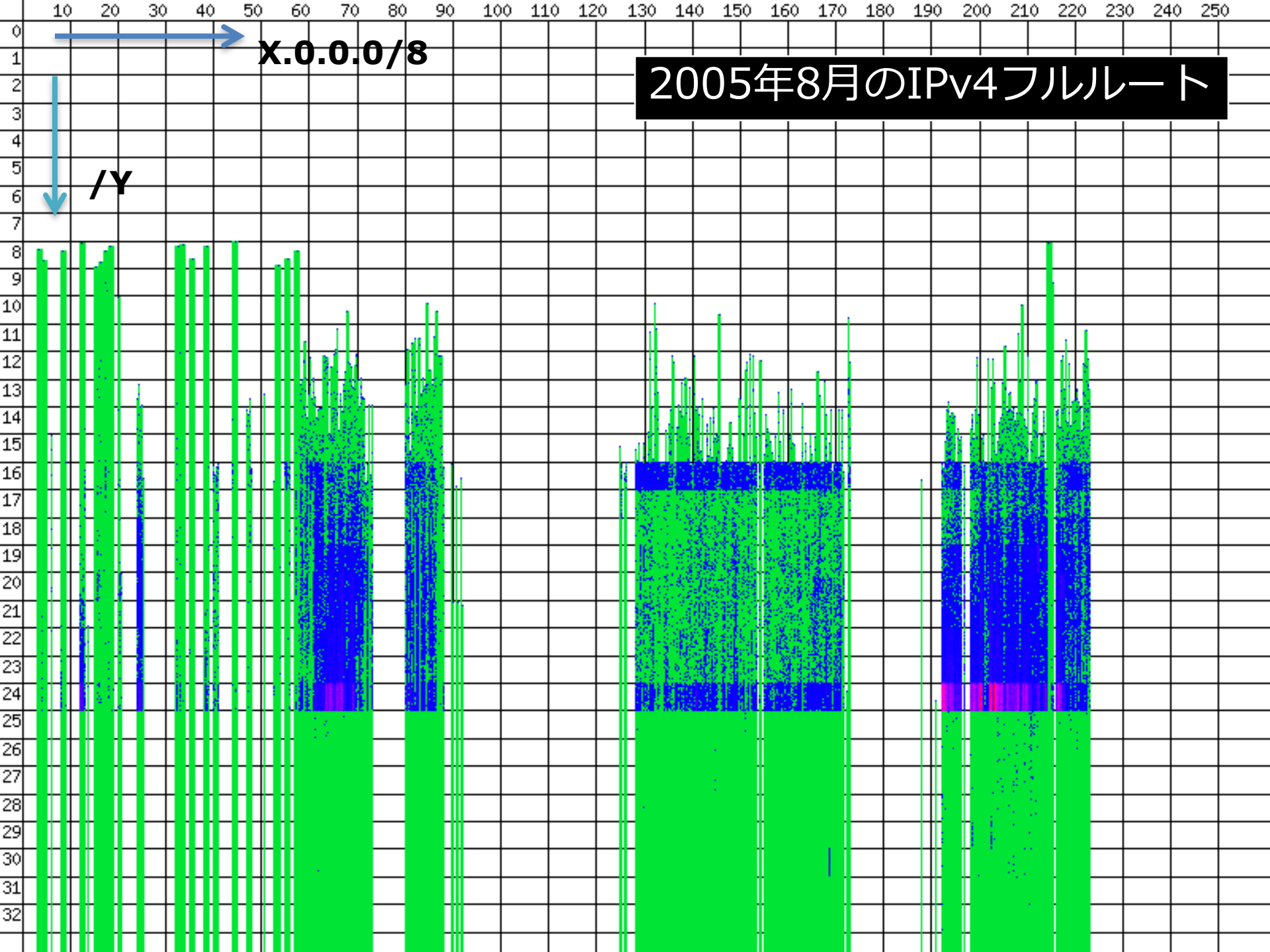
このあたりが
一般的な経路数

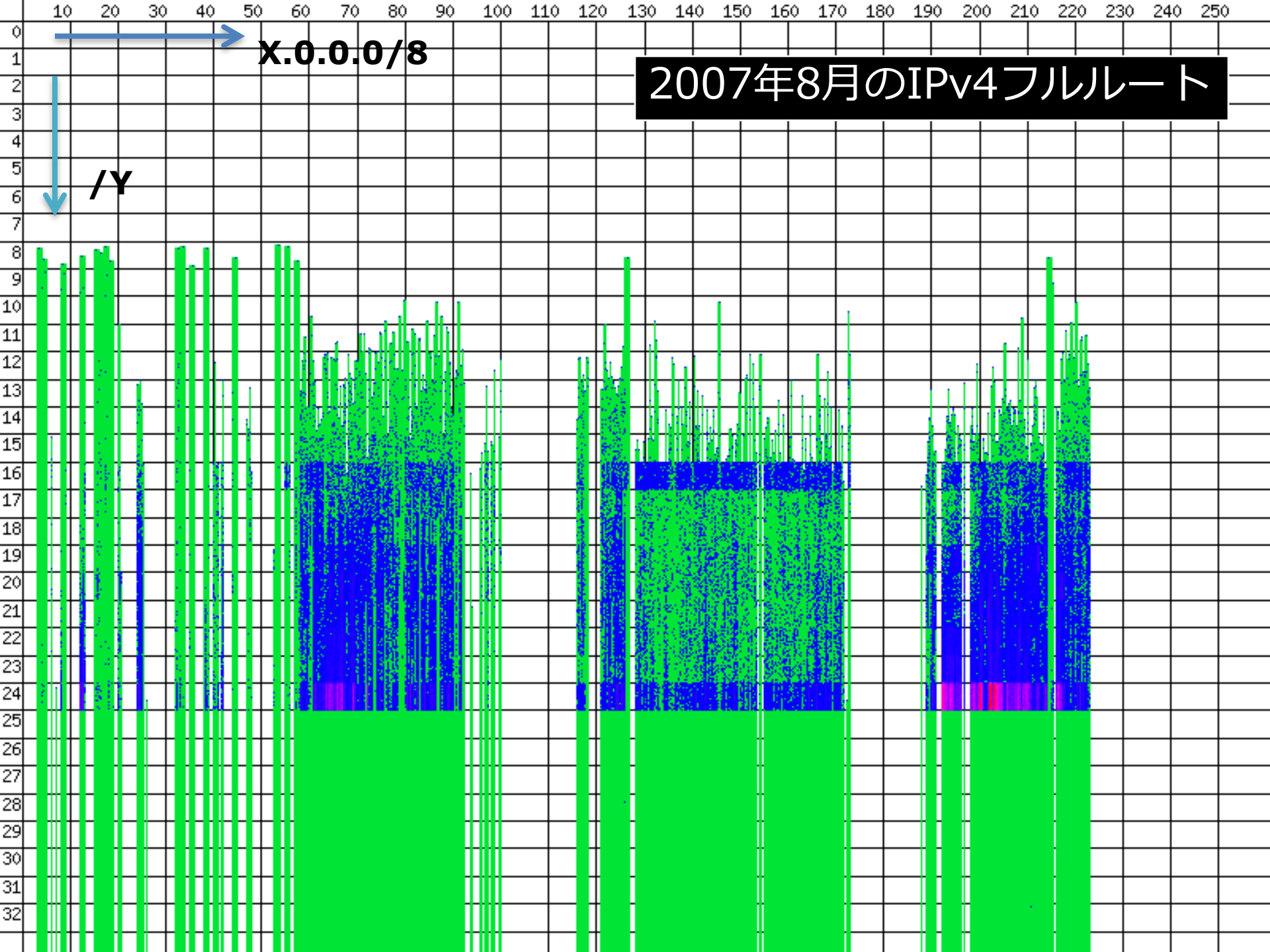
参照: http://bgp.potaroo.net/

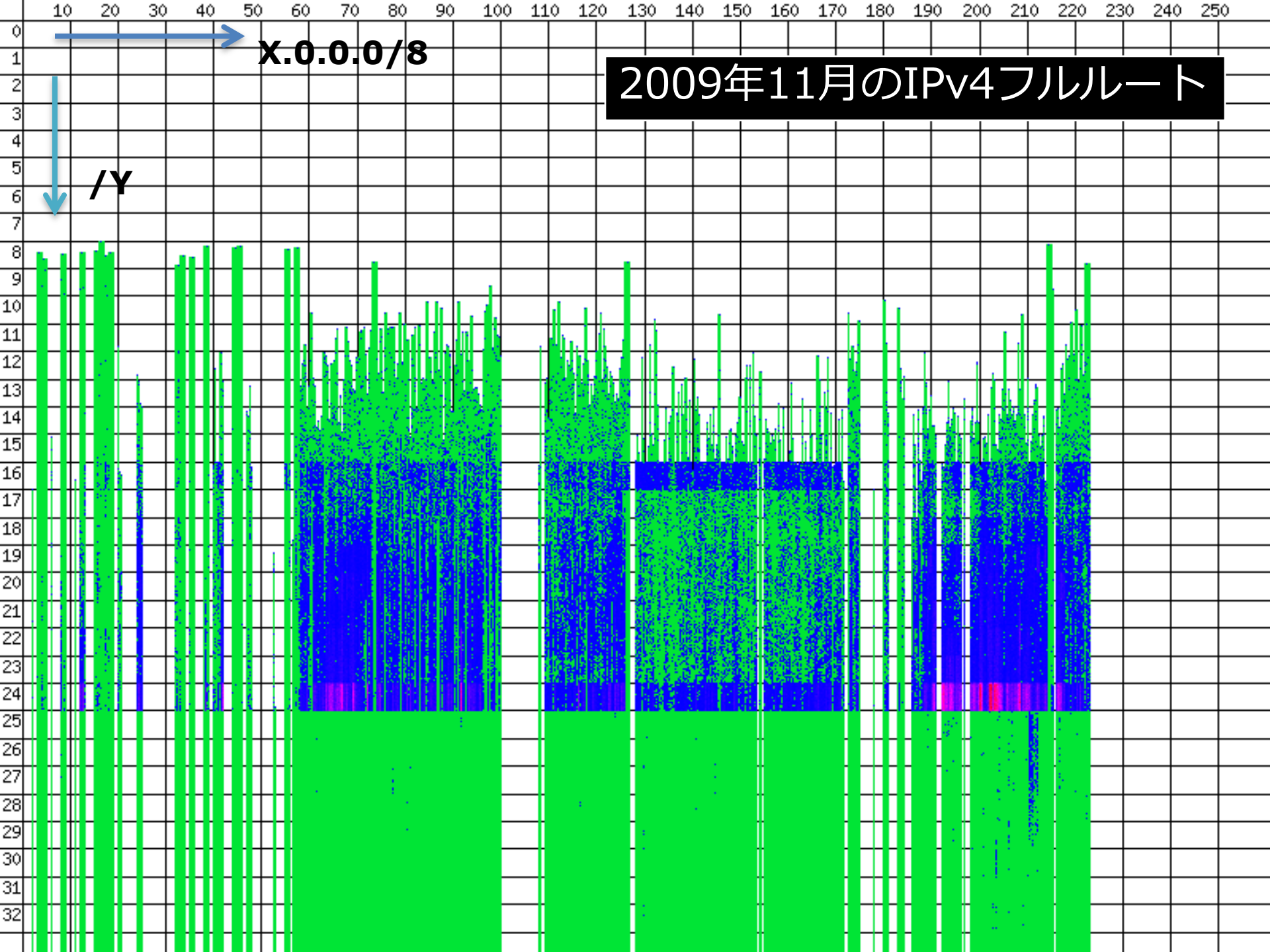
IPv4経路数推移予測
(6年前の2009年末予測)

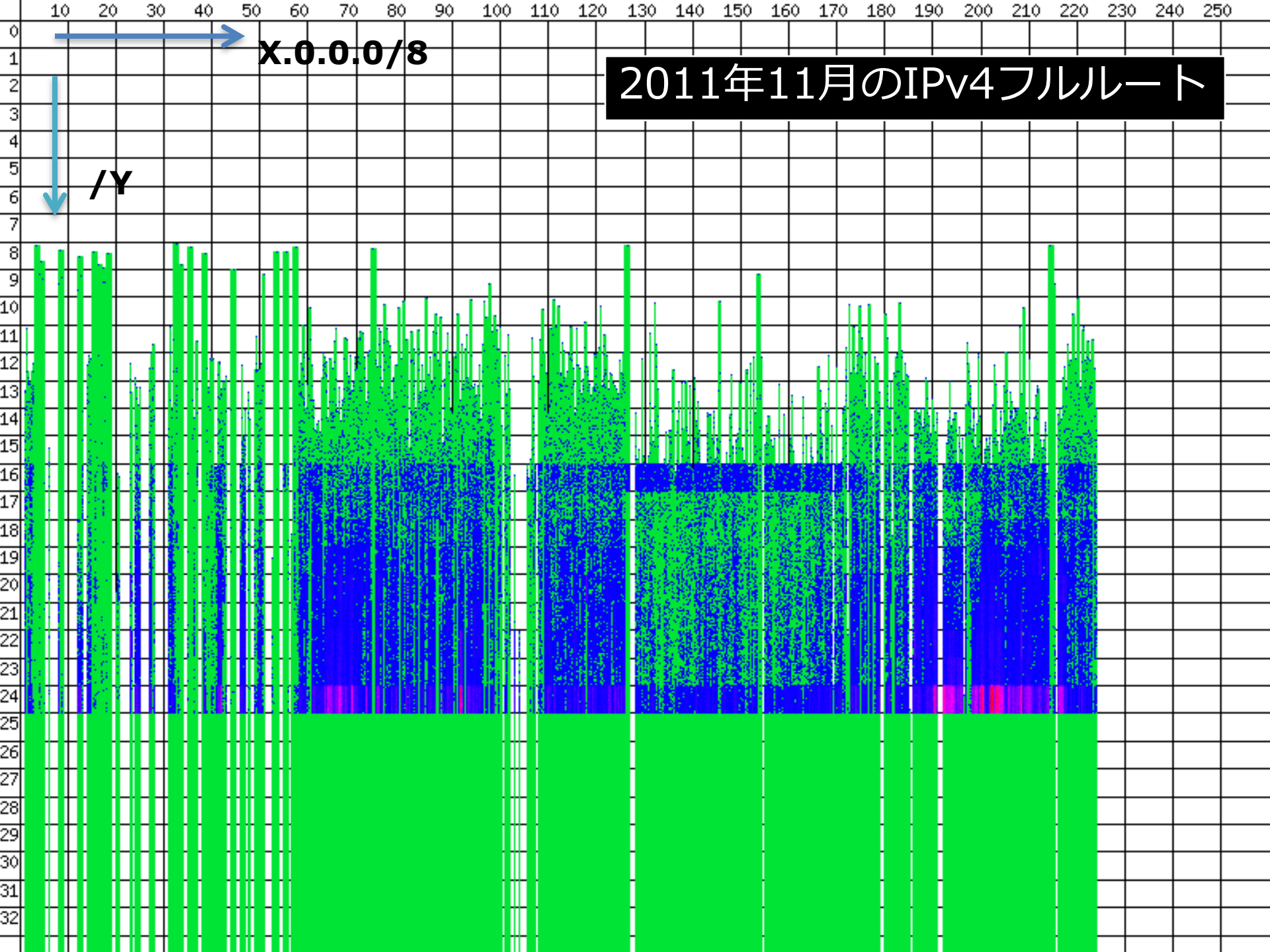


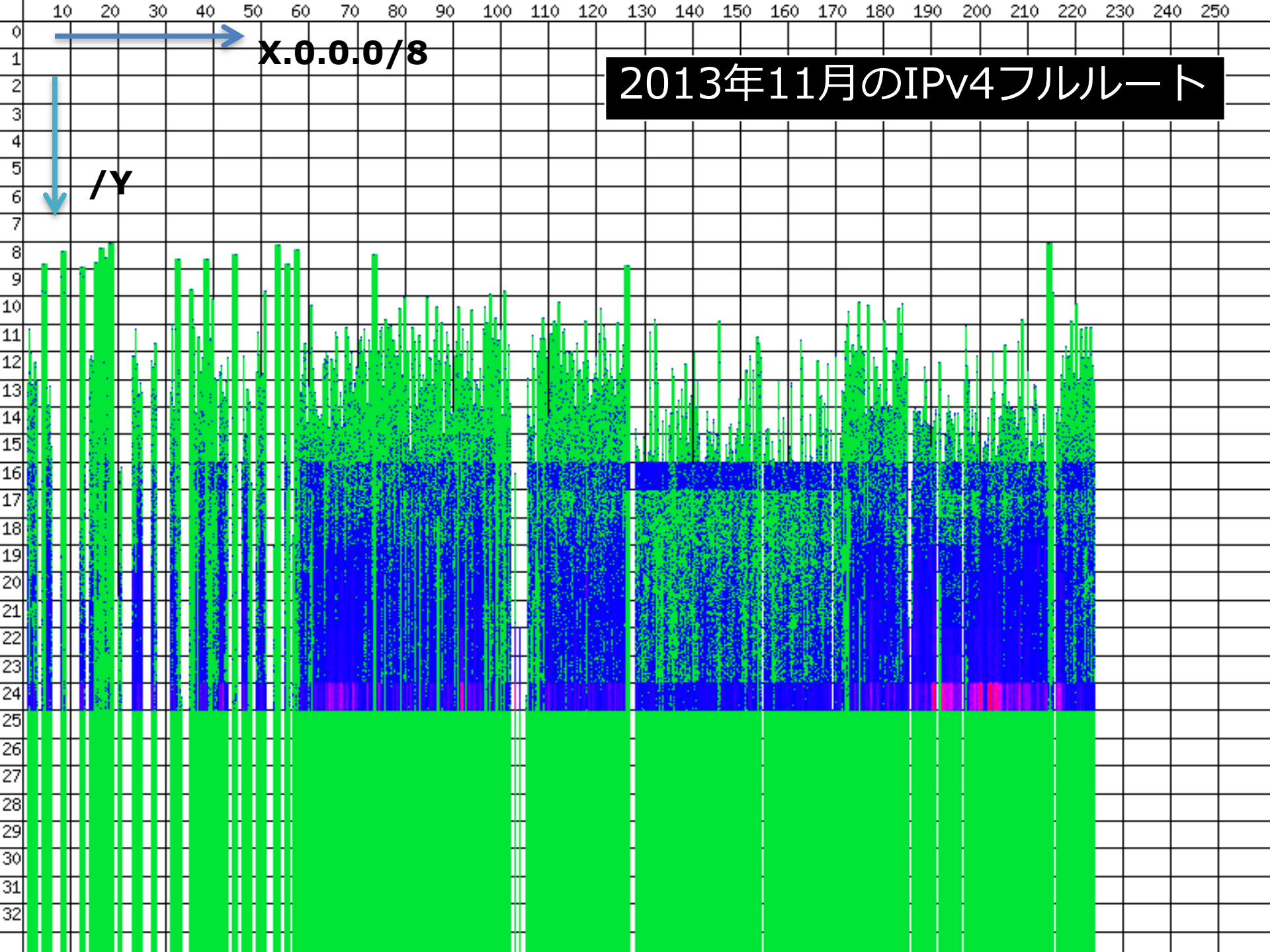
IPv4アドレスの枯渇後、緩やかに増加し続けている
依然IPv4アドレスの流通や細分化が進み経路数増加を牽引

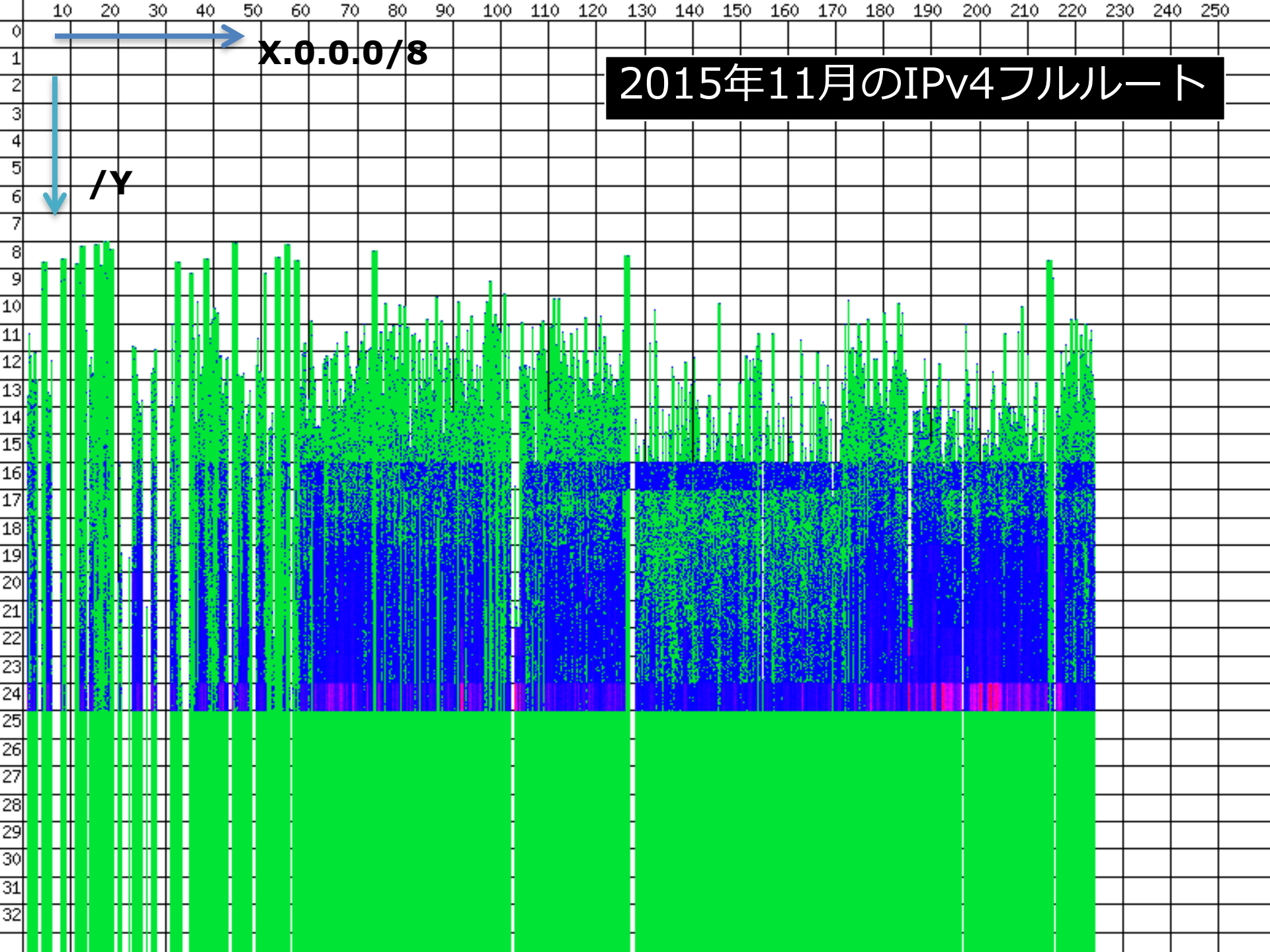

10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
x.0.0.0/8
/Y
2005年8月のIPv4フルルート


10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
x.0.0.0/8
/Y
2007年8月のIPv4フルルート


10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
x.0.0.0/8
/Y
2009年11月のIPv4フルルート

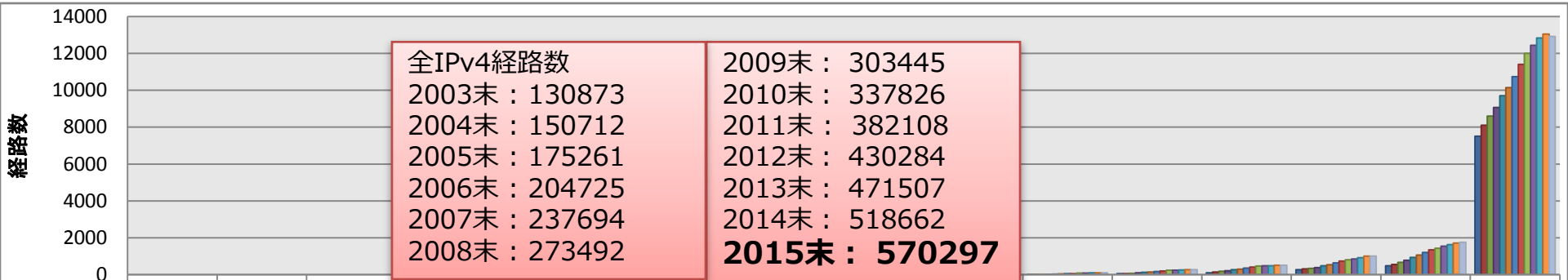

10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
x.0.0.0/8
/Y
2011年11月のIPv4フルルート


10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
x.0.0.0/8
/Y
2013年11月のIPv4フルルート


10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
x.0.0.0/8
/Y
2015年11月のIPv4フルルート

IPv4経路数の推移

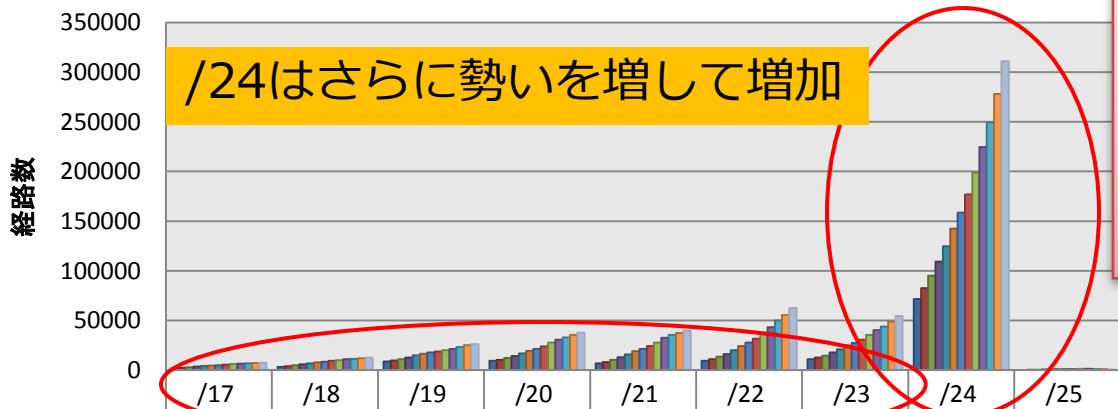
/14, /16が2003年の観測以降初の減少



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

	/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

IPv4経路数の推移

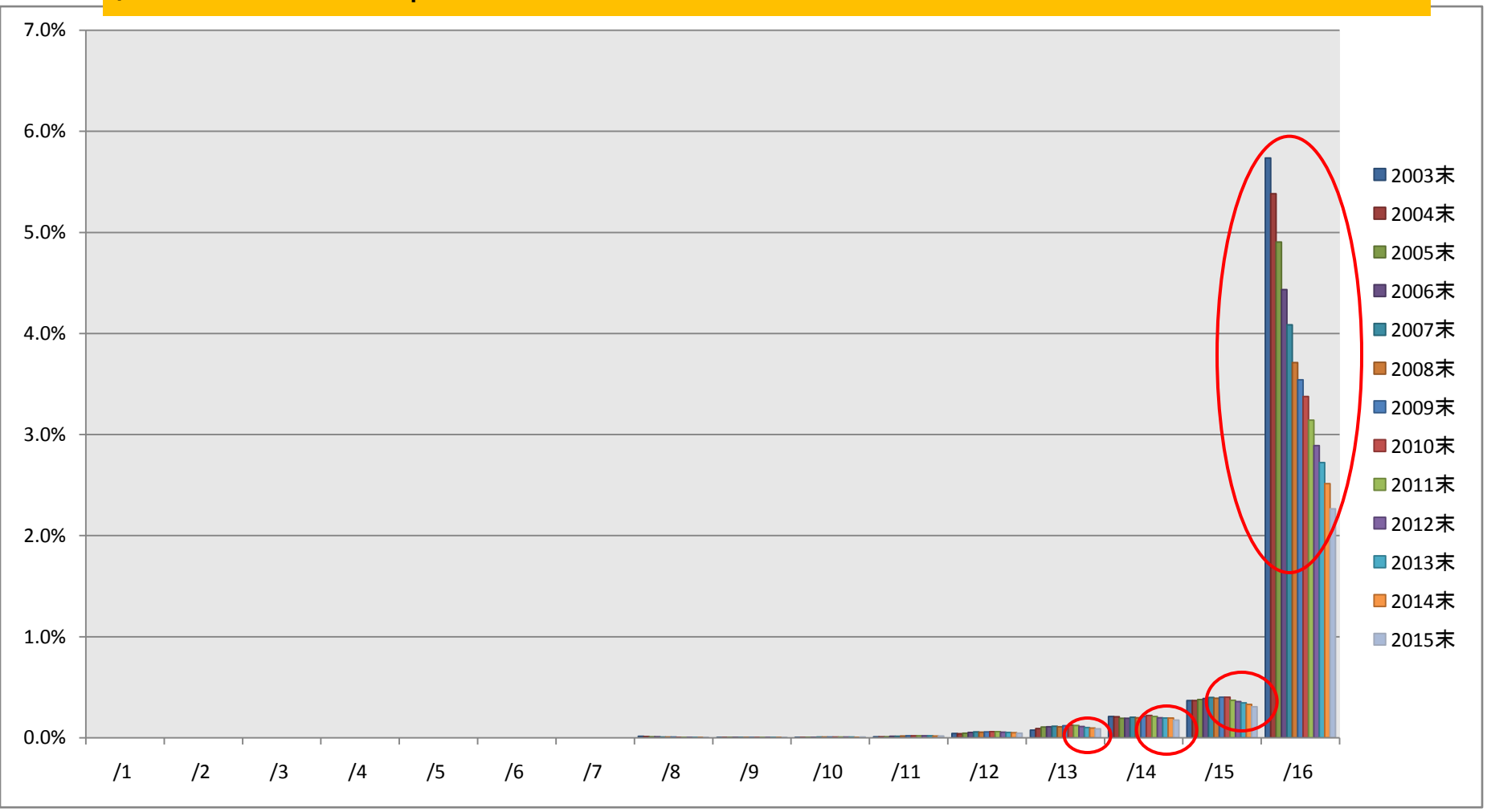


全IPv4経路数
2003末：130873
2004末：150712
2005末：175261
2006末：204725
2007末：237694
2008末：273492
2009末： 303445
2010末： 337826
2011末： 382108
2012末： 430284
2013末： 471507
2014末： 518662
2015末： 570297

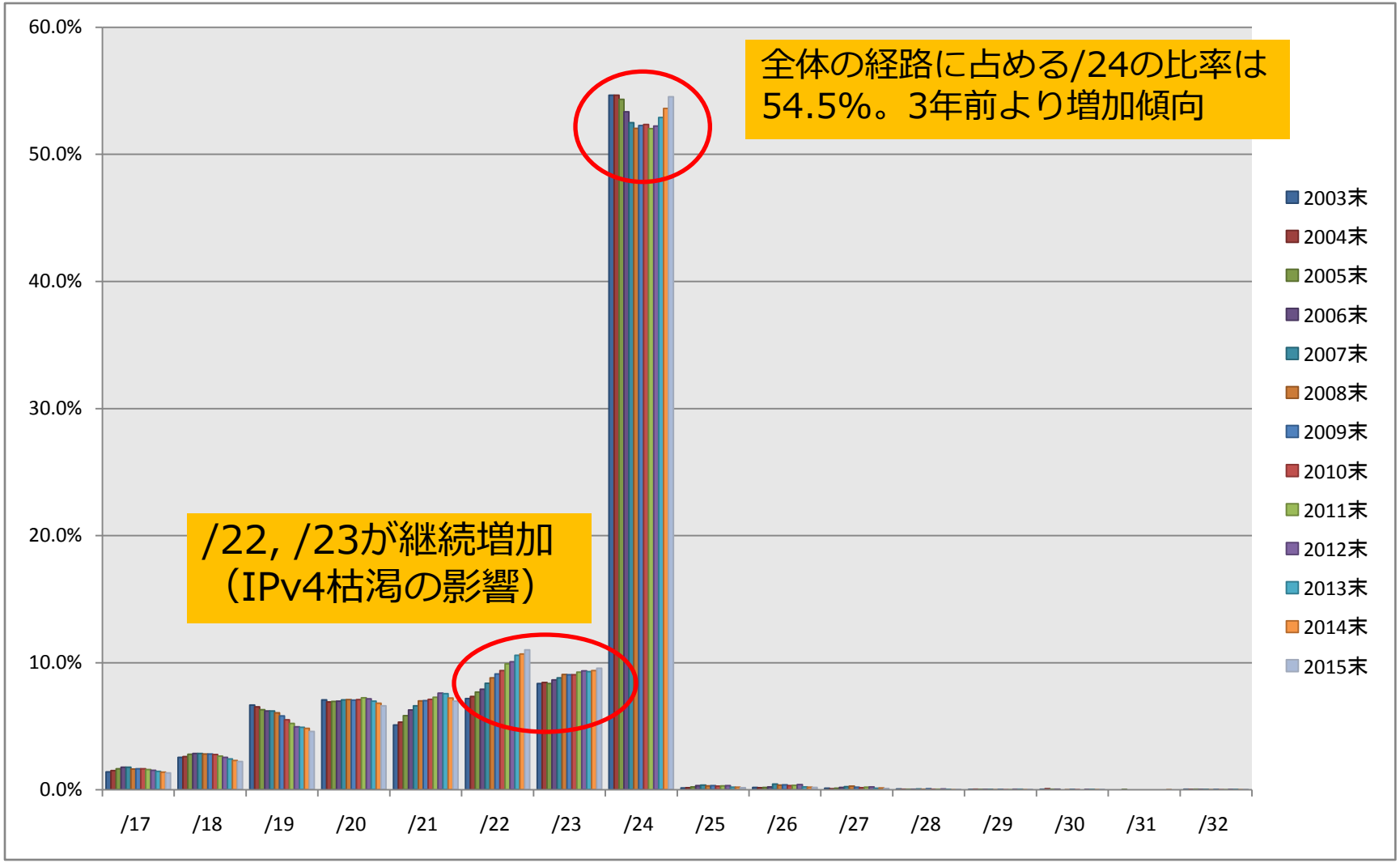
	/17	/18	/19	/20	/21	/22	/23	/24	/25	/26	/27	/28	/29	/30	/31	/32
2003末	1829	3334	8716	9249	6656	9386	10943	71541	182	233	156	70	21	50	0	41
2004末	2270	3933	9818	10402	8007	11066	12707	82382	252	239	130	69	54	120	0	40
2005末	2880	4871	11026	12142	10194	13440	14626	95225	345	292	194	26	12	36	3	30
2006末	3625	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

IPv4経路数の推移（割合）

/16等のshorter prefixの割合は減少傾向（枯渇前後で大きな変化はない）



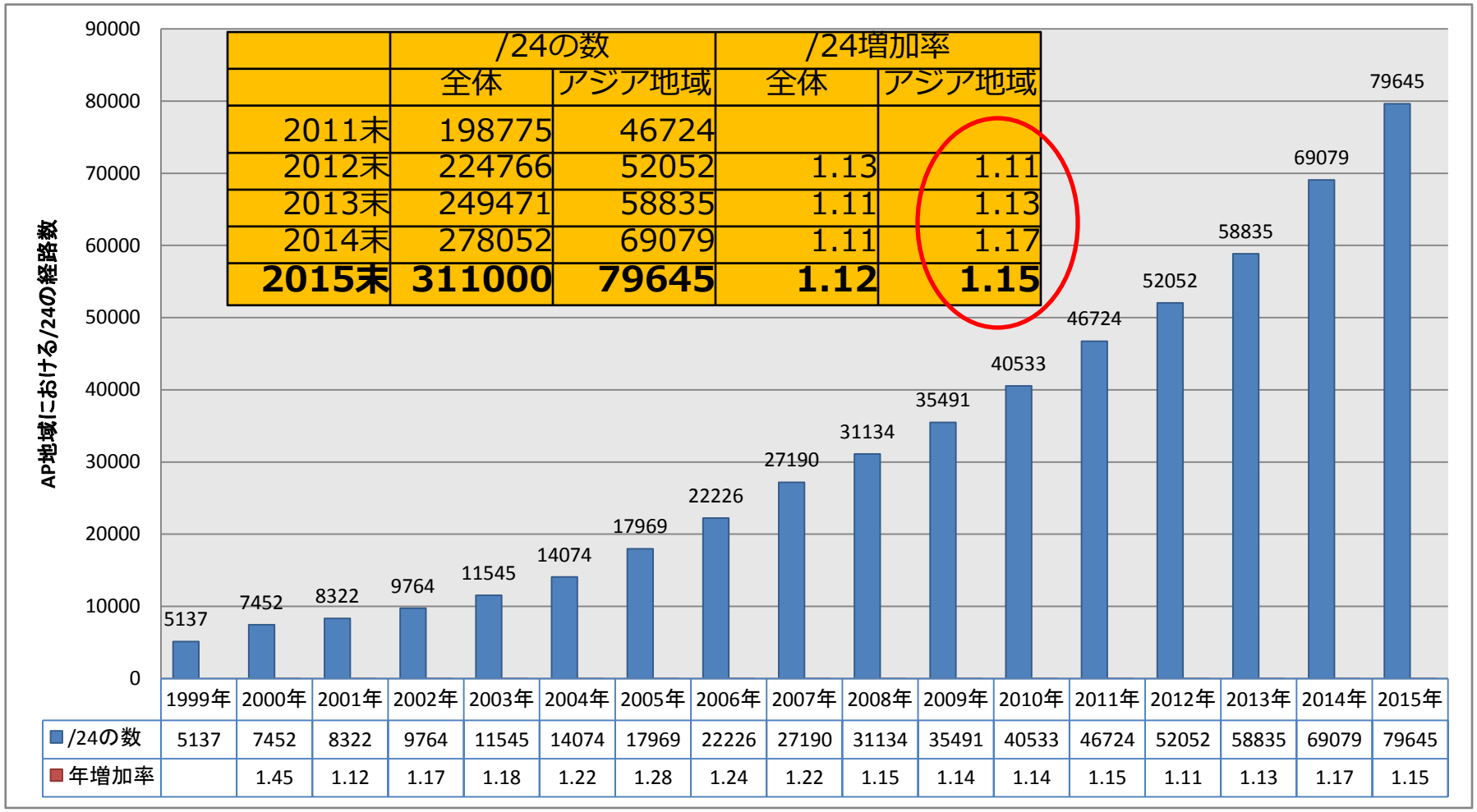
IPv4経路数の推移（割合）



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単位で今後とれない状況に）



	/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**

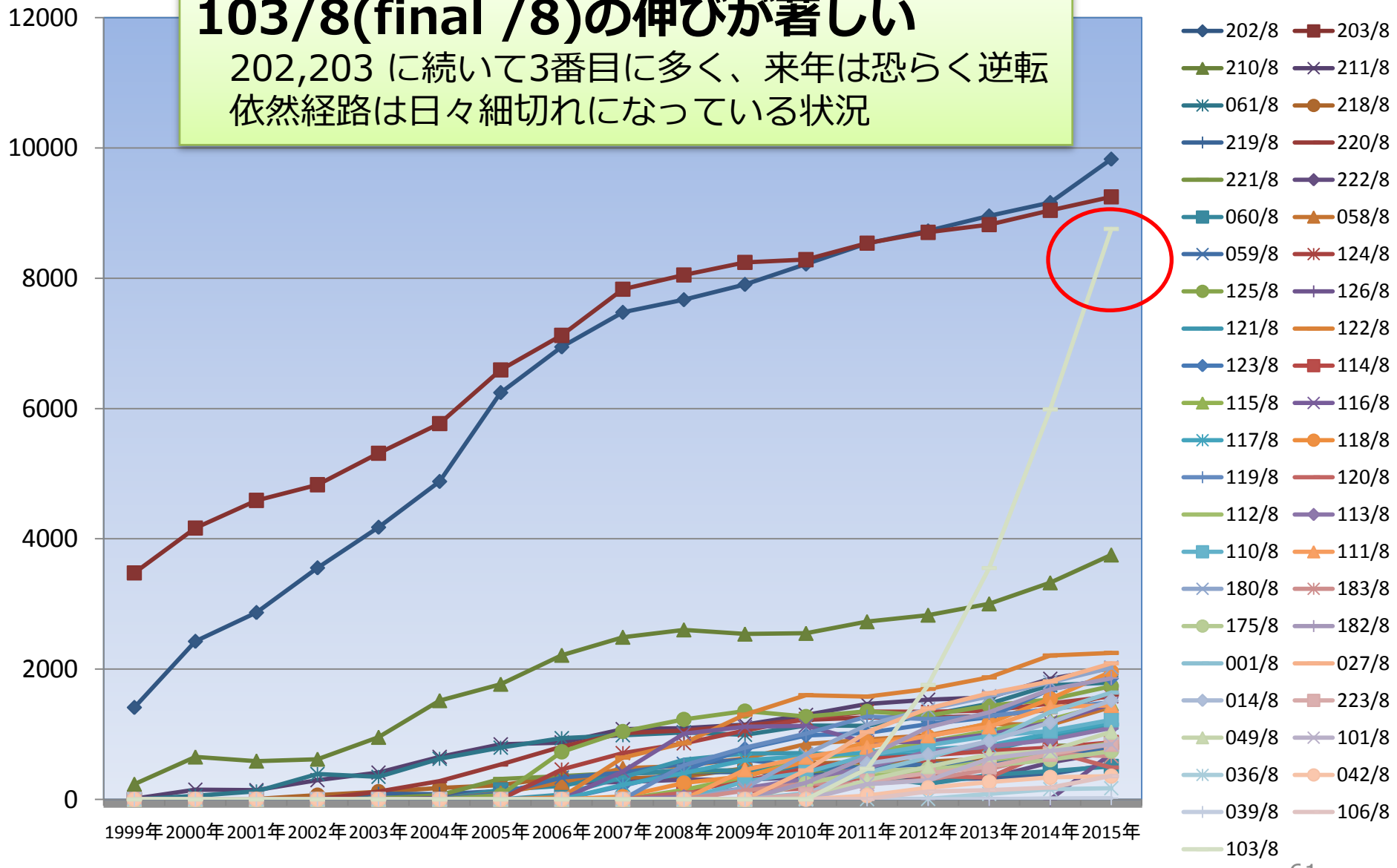
	1999年	2000年	2001年	2002年	2003年	2004年	2005年	2006年	2007年	2008年	2009年	2010年	2011年	2012年	2013年	2014年	2015年
/24の数	5137	7452	8322	9764	11545	14074	17969	22226	27190	31134	35491	40533	46724	52052	58835	69079	79645
年増加率		1.45	1.12	1.17	1.18	1.22	1.28	1.24	1.22	1.15	1.14	1.14	1.15	1.11	1.13	1.17	1.15

AP地域の/24の推移

103/8(final /8)の伸びが著しい

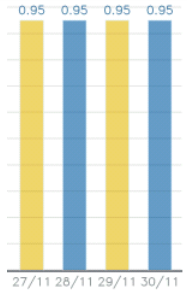
202,203 に続いて3番目に多く、来年は恐らく逆転

依然経路は日々細切れになっている状況

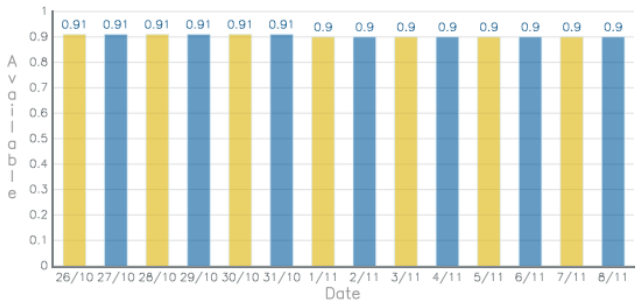


AP地域の最後の/8
103/8 (2011年～2015年)

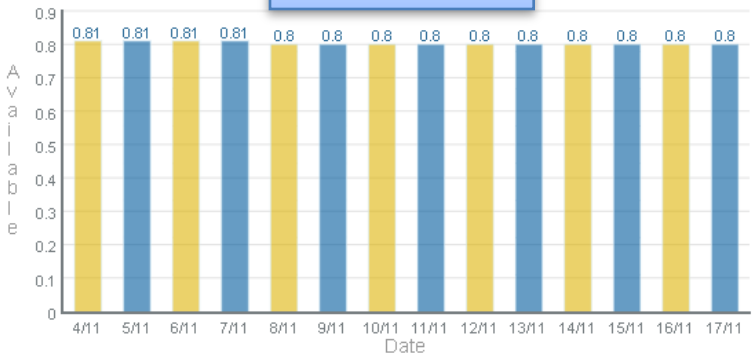
2011年



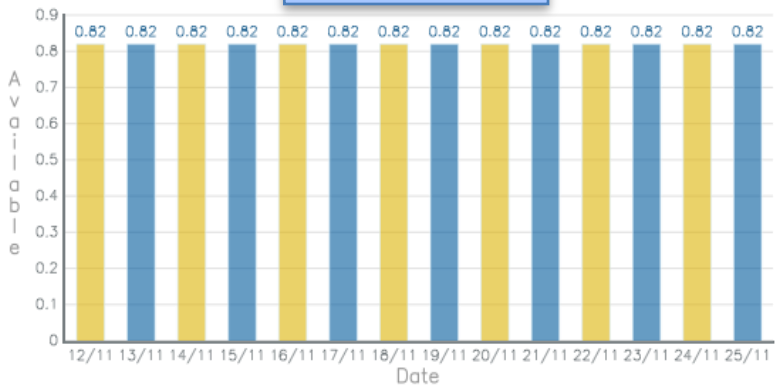
2012年



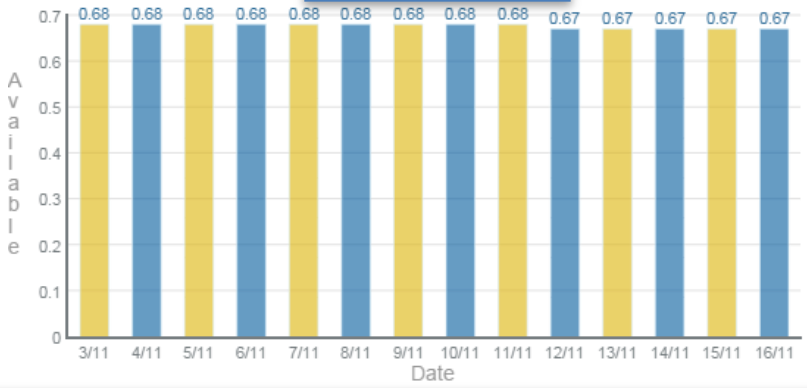
2014年



2013年



2015年



2015年中に急激に取得組織が増加。既に103/8も移転されている。。

APNIC公認？のブローカー

Registered IPv4 brokers

Like Share 0 Tweet 0

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	
Jelly Digital, LLC	US	Norman Jester	+1 323-345-6236	jellydigital

2013年に追加

2014年に追加

2015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

IPv4アドレスを買いたい人リスト。2015年11月時点の状況
IN(インド)からの大きな空間のIPv4アドレス申請が目立つ

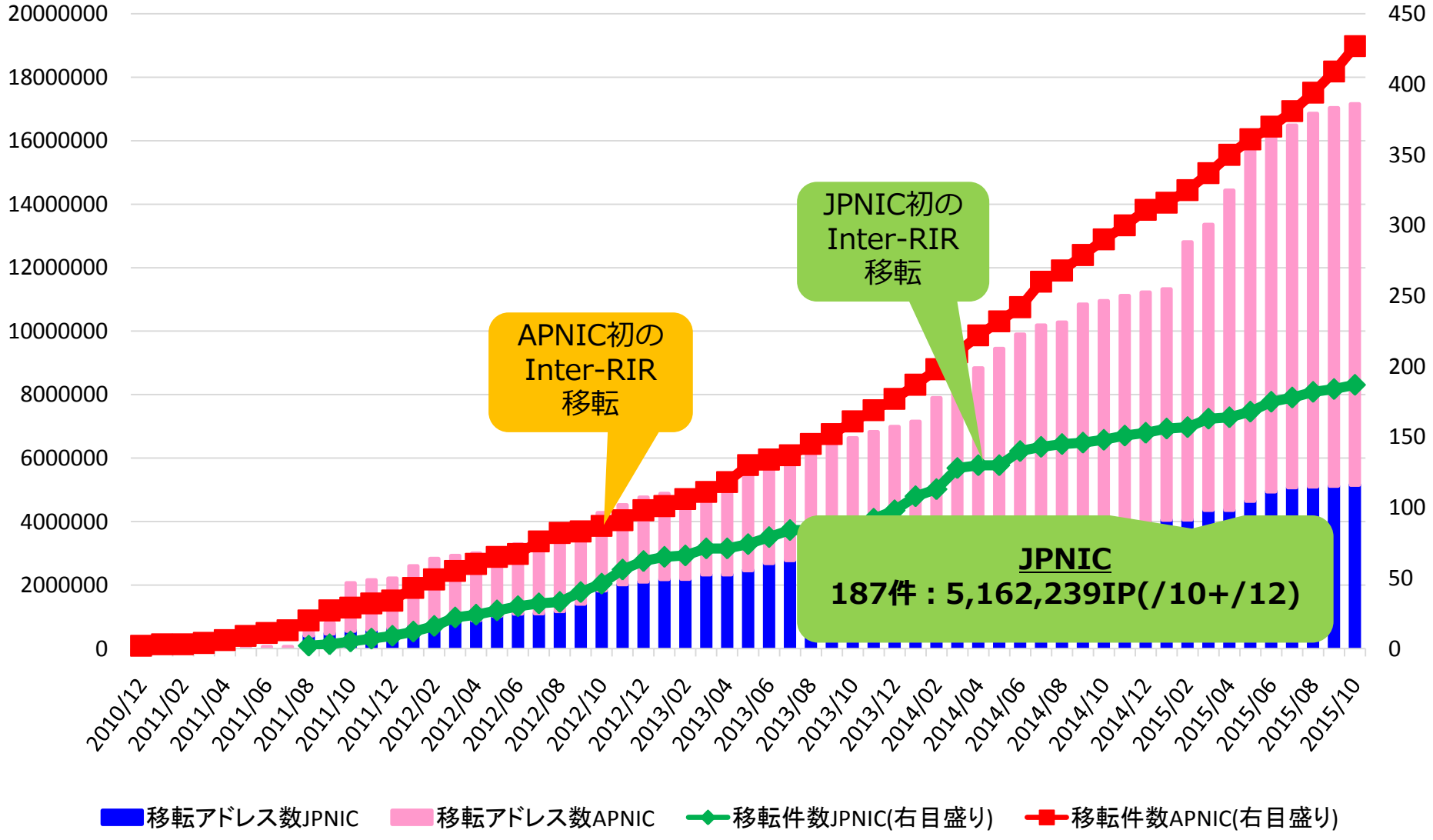
45	/17	KH	19 Nov 2015	Contact
51	/16 + /17	IN	20 Nov 2015	Contact
52	/19 + /20	AU	3 Dec 2015	Contact
53	/16	HK	5 Dec 2015	Contact
58	/20 + /21	PK	9 Jan 2016	Contact
60	/13	IN	25 Feb 2016	Contact
61	/21	PH	12 Mar 2016	Contact
62	/16	HK	21 Mar 2016	Contact
63	/19	IN	24 Apr 2016	Contact
64	/20	BD	2 Apr 2015	Contact
65	/18	MY	22 May 2016	Contact
67	/18 + /20	IN	10 Jun 2016	Contact
68	/15	TH	4 Jun 2016	Contact
69	/16	TH	18 Dec 2016	Contact
70	/20	NZ	13 Apr 2017	Contact
71	/19	KH	25 May 2017	Contact
72	/10	IN	20 Jul 2017	Contact
73	/20	KH	27 Jul 2017	Contact
74	/20 + /21	SG	10 Aug 2017	Contact
75	/20	IN	28 Aug 2017	Contact
76	/19 + /21	IN	10 Sep 2017	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

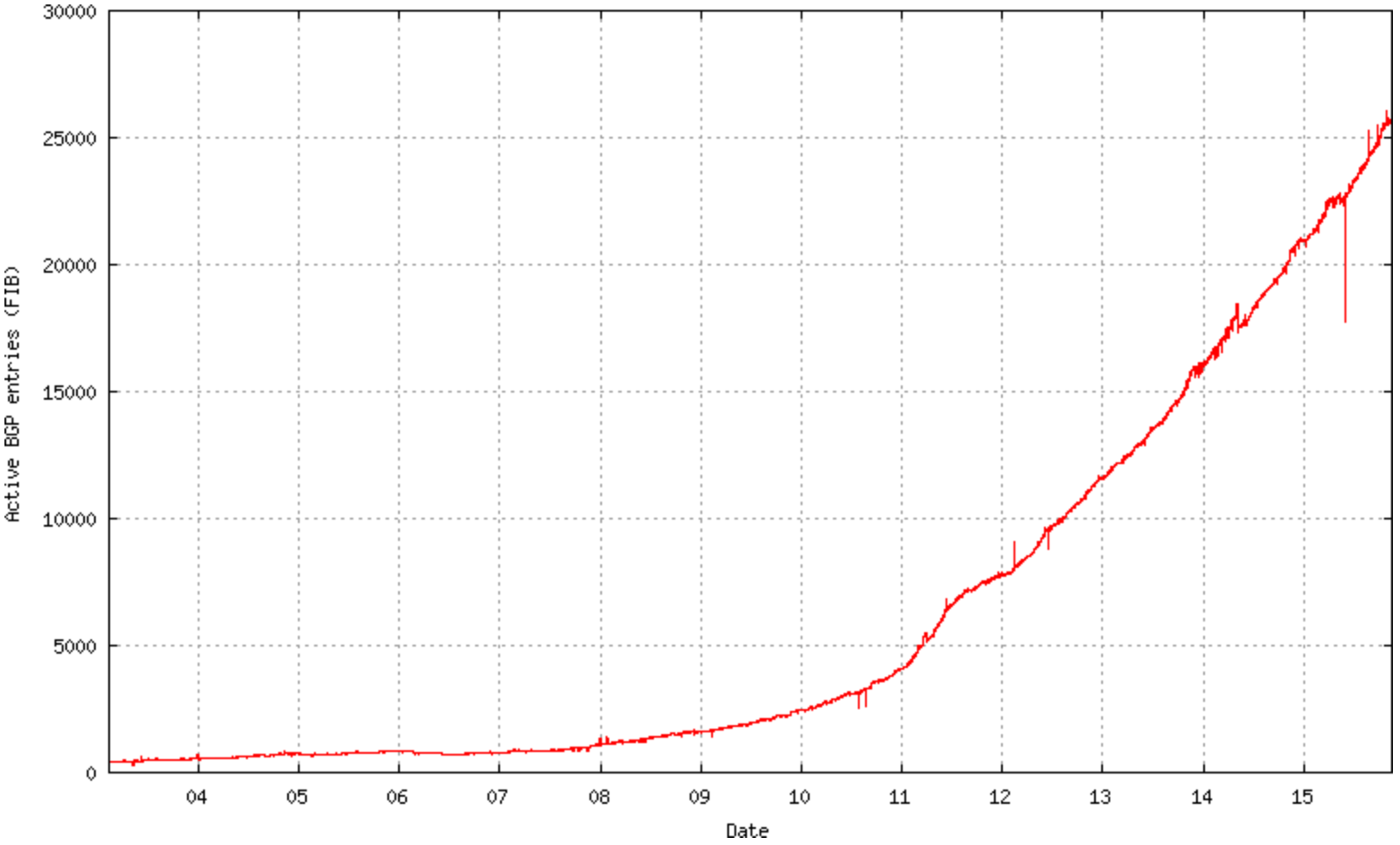
- 2015年11月現在187件（2011年８月より）
- 国際移転も10件以上に
- 移転の理由
  - 純粋にIPv4アドレスが不足しているケースが断然多い
  - 事業者間での整理
    - グループ企業間でやり取り
    - 上位ISPからの割り当てブロックをそのまま下位事業者へ移譲
- 移転履歴
  - https://www.nic.ad.jp/ja/ip/ipv4transfer-log.html
- JPNICによるlisting serviceが12月開始予定
  - **【1月 アップデート追記】**
    2015年12月21日　IPv4アドレス移転希望者リスト公開開始
- AS番号の移転も可能（日本では1件）

APNIC地域と日本の移転状況比較



出展：JPOPM 29thより

最近のIPv6経路増も要注意



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

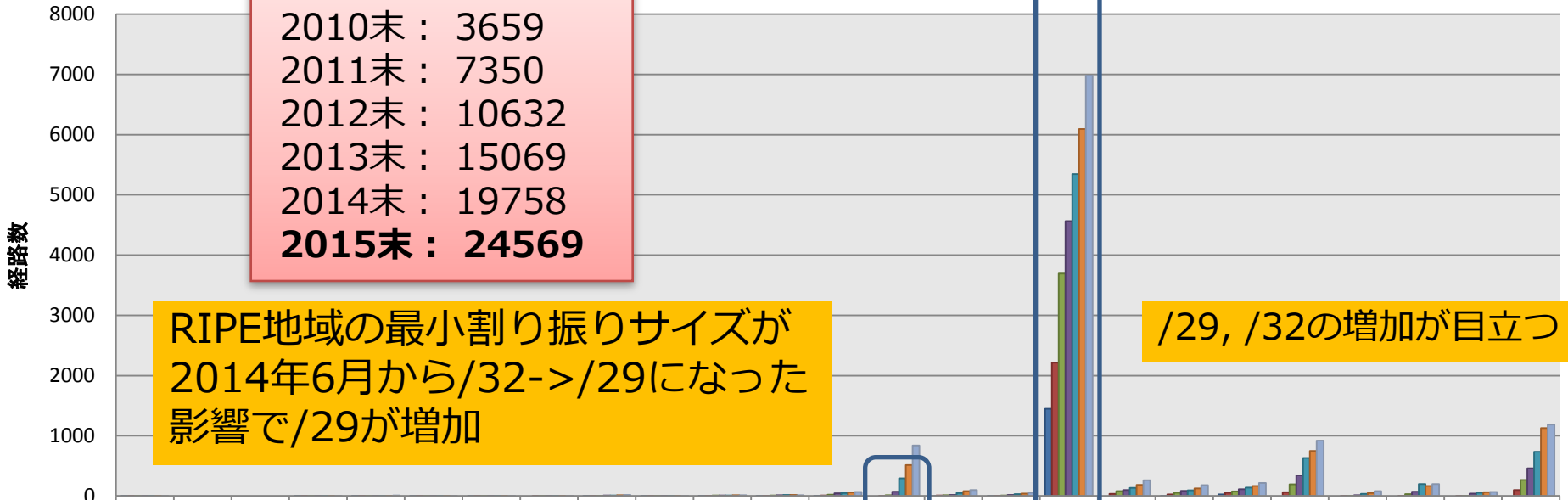
参照　http://bgp.potaroo.net/v6/as2.0/index.html

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

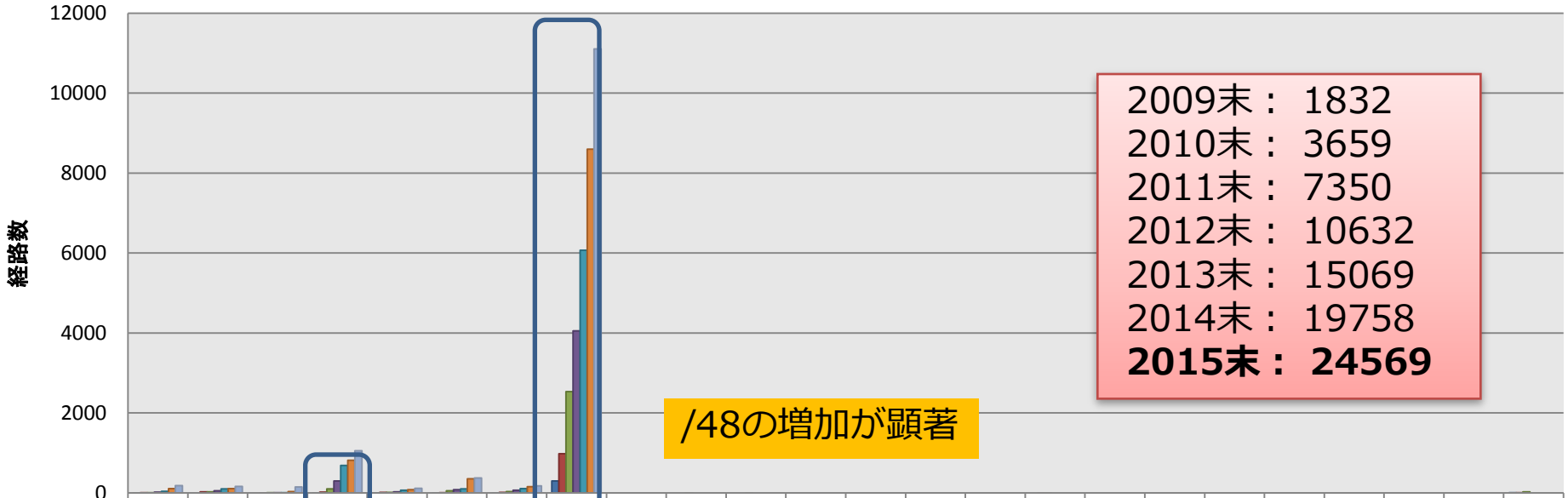
RIPE地域の最小割り振りサイズが2014年6月から/32->/29になった影響で/29が増加

/29, /32の増加が目立つ



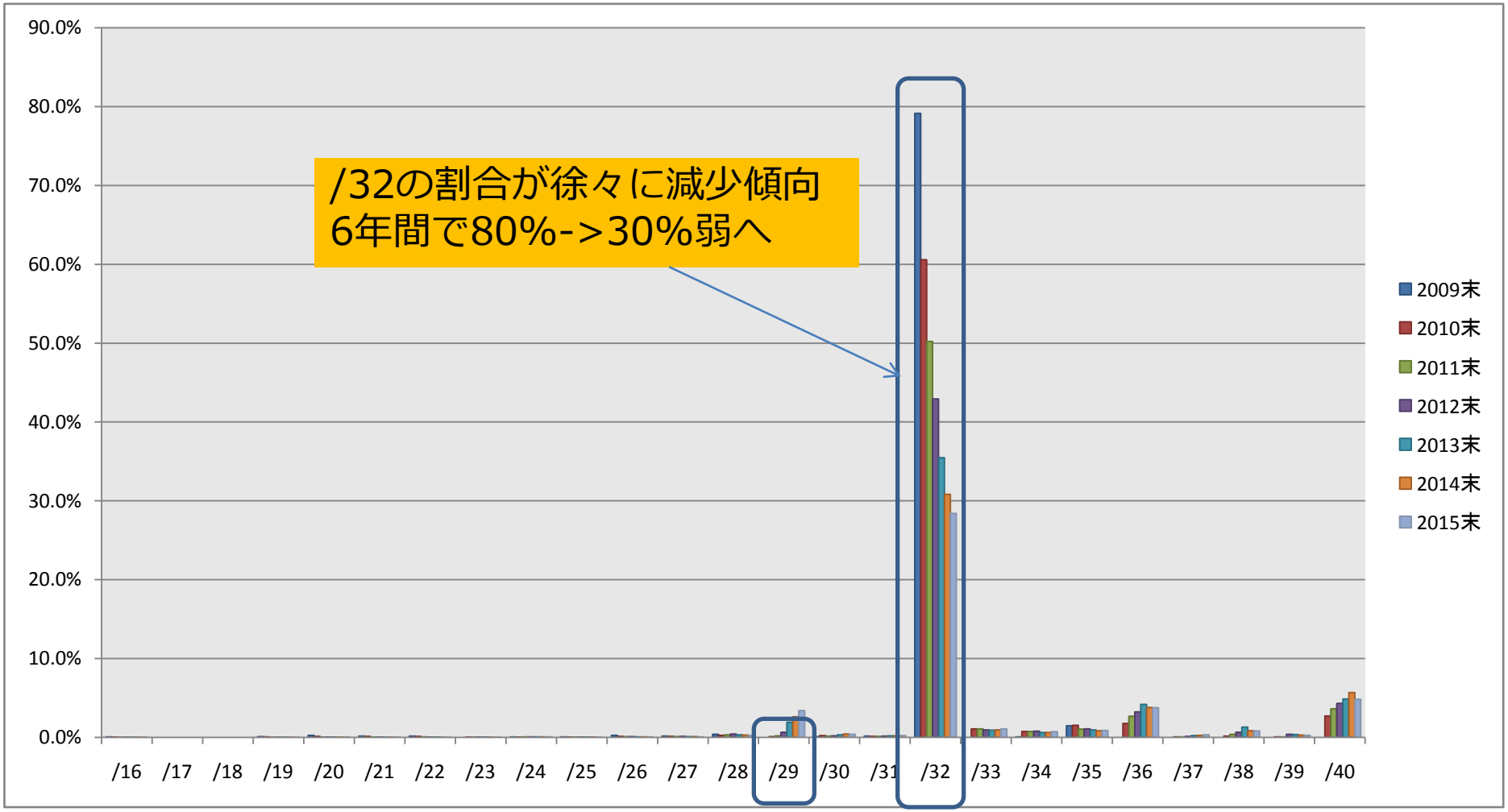
	/16	/17	/18	/19	/20	/21	/22	/23	/24	/25	/26	/27	/28	/29	/30	/31	/32	/33	/34	/35	/36	/37	/38	/39	/40
2009末	1	0	0	2	5	3	3	0	1	1	5	3	7	0	2	3	1450	0	1	27	0	0	0	0	0
2010末	1	0	0	2	5	4	4	1	1	1	5	5	9	3	8	4	2217	39	27	56	64	2	6	2	99
2011末	1	0	0	2	4	3	5	4	7	4	9	9	24	16	14	10	3692	80	57	79	197	7	31	7	268
2012末	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

IPv6経路数の推移

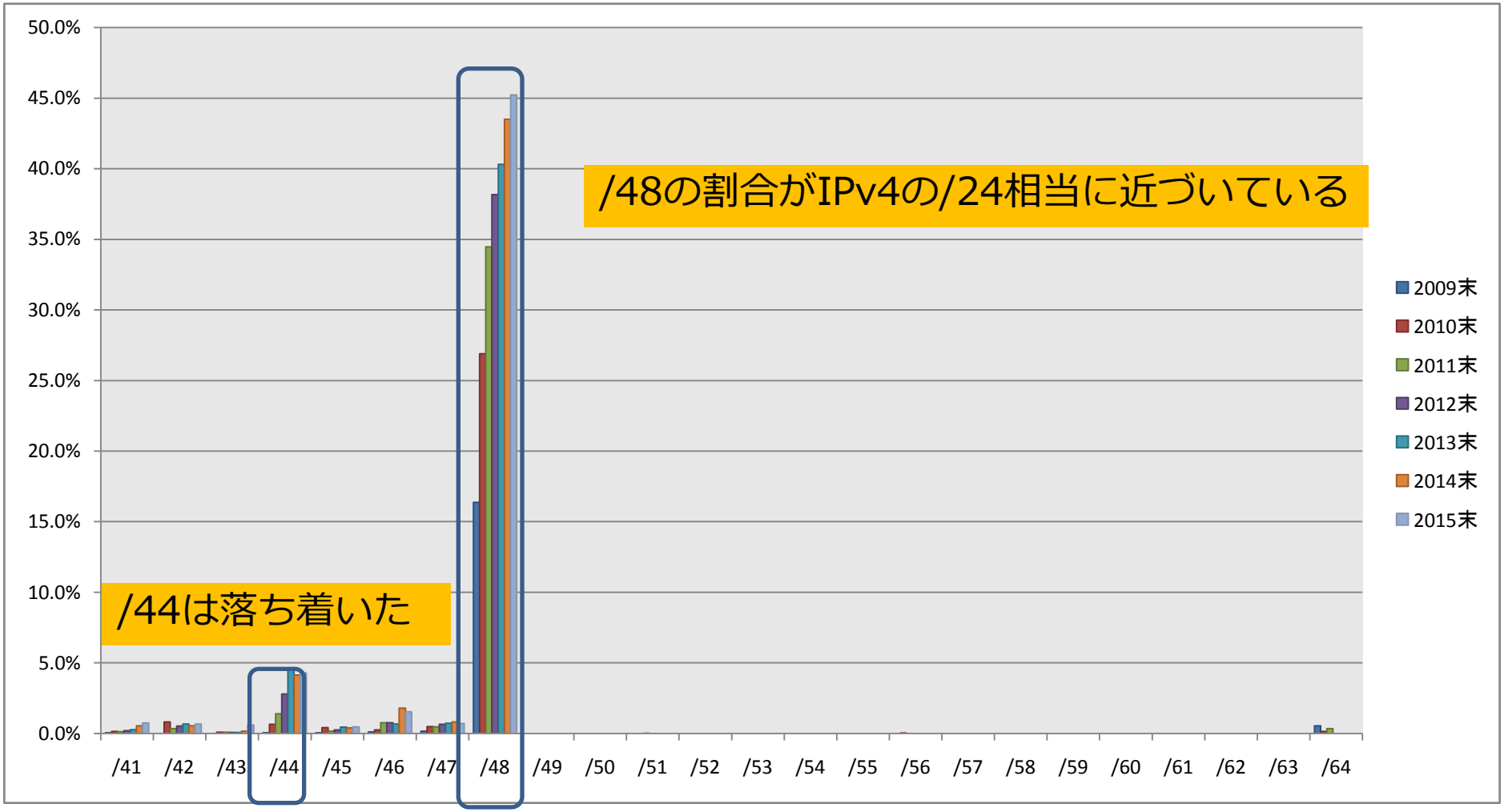


	/41	/42	/43	/44	/45	/46	/47	/48	/49	/50	/51	/52	/53	/54	/55	/56	/57	/58	/59	/60	/61	/62	/63	/64
2009末	1	0	0	1	1	2	3	300	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10
2010末	5	30	3	24	15	9	18	984	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	5
2011末	10	27	8	104	13	57	36	2534	0	1	3	0	0	0	0	1	0	0	0	0	0	0	0	26
2012末	21	55	8	298	27	81	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	1111	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

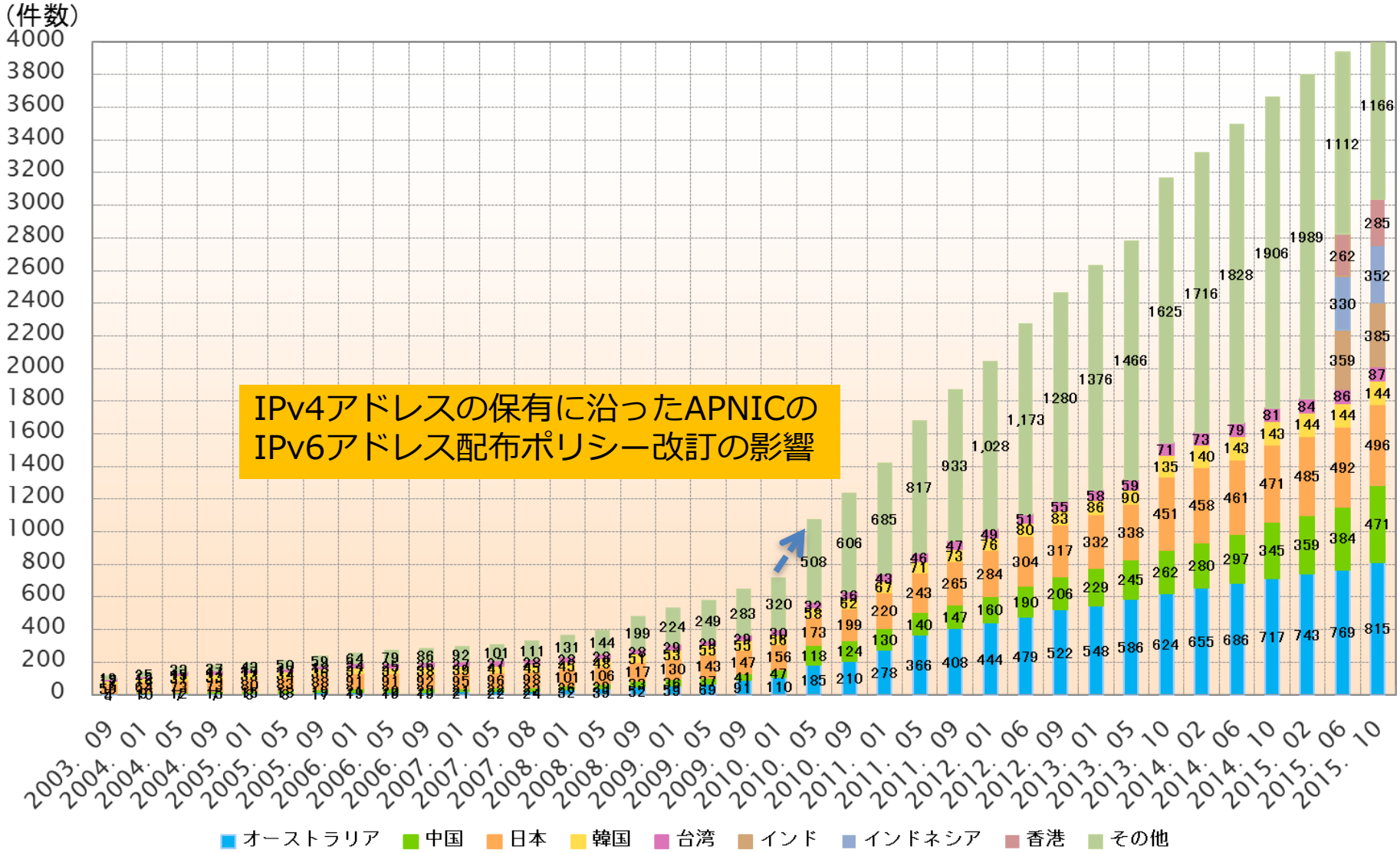
IPv6経路数の推移（割合）



IPv6経路数の推移（割合）

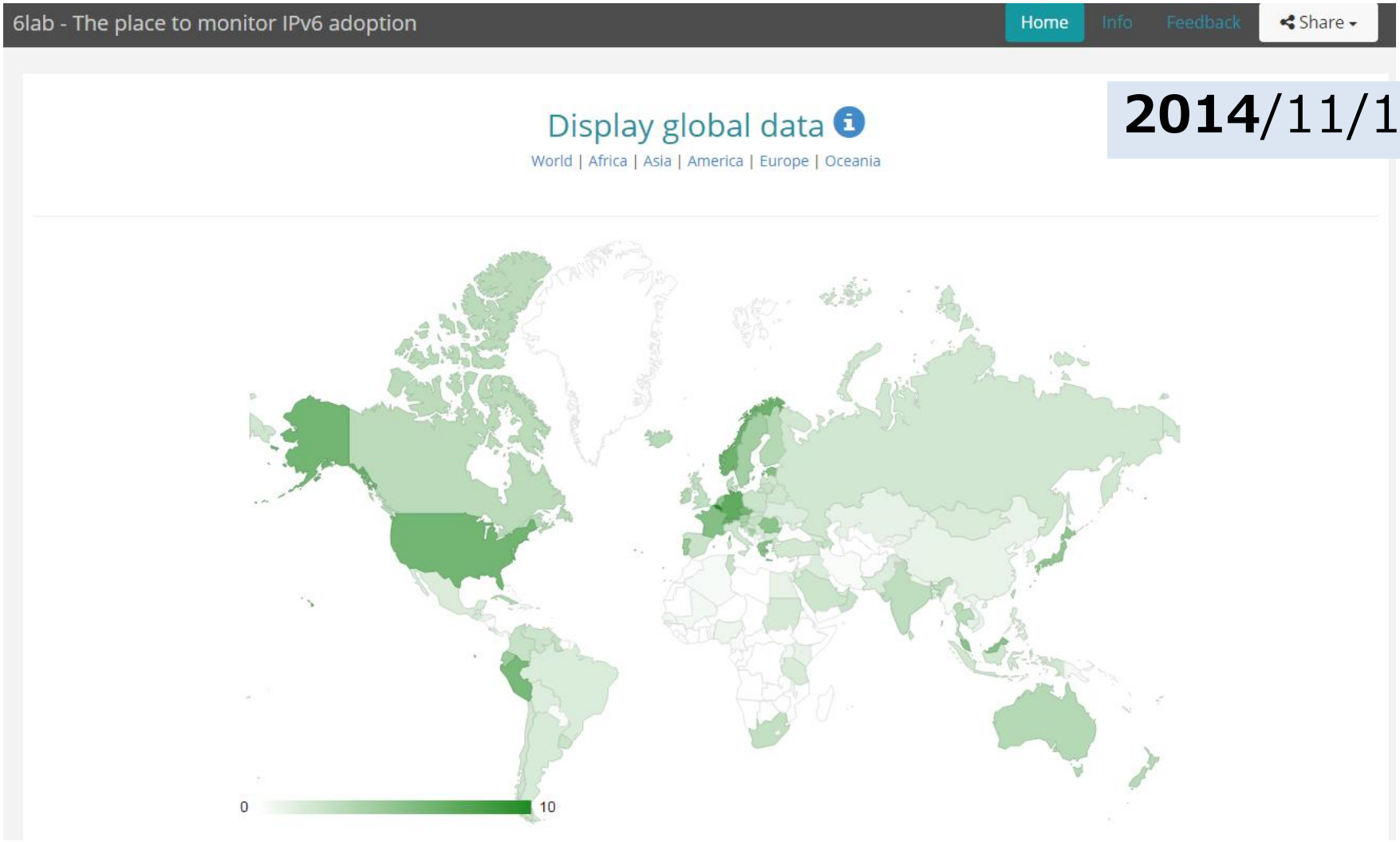


AP地域の国別IPv6アドレス配分状況

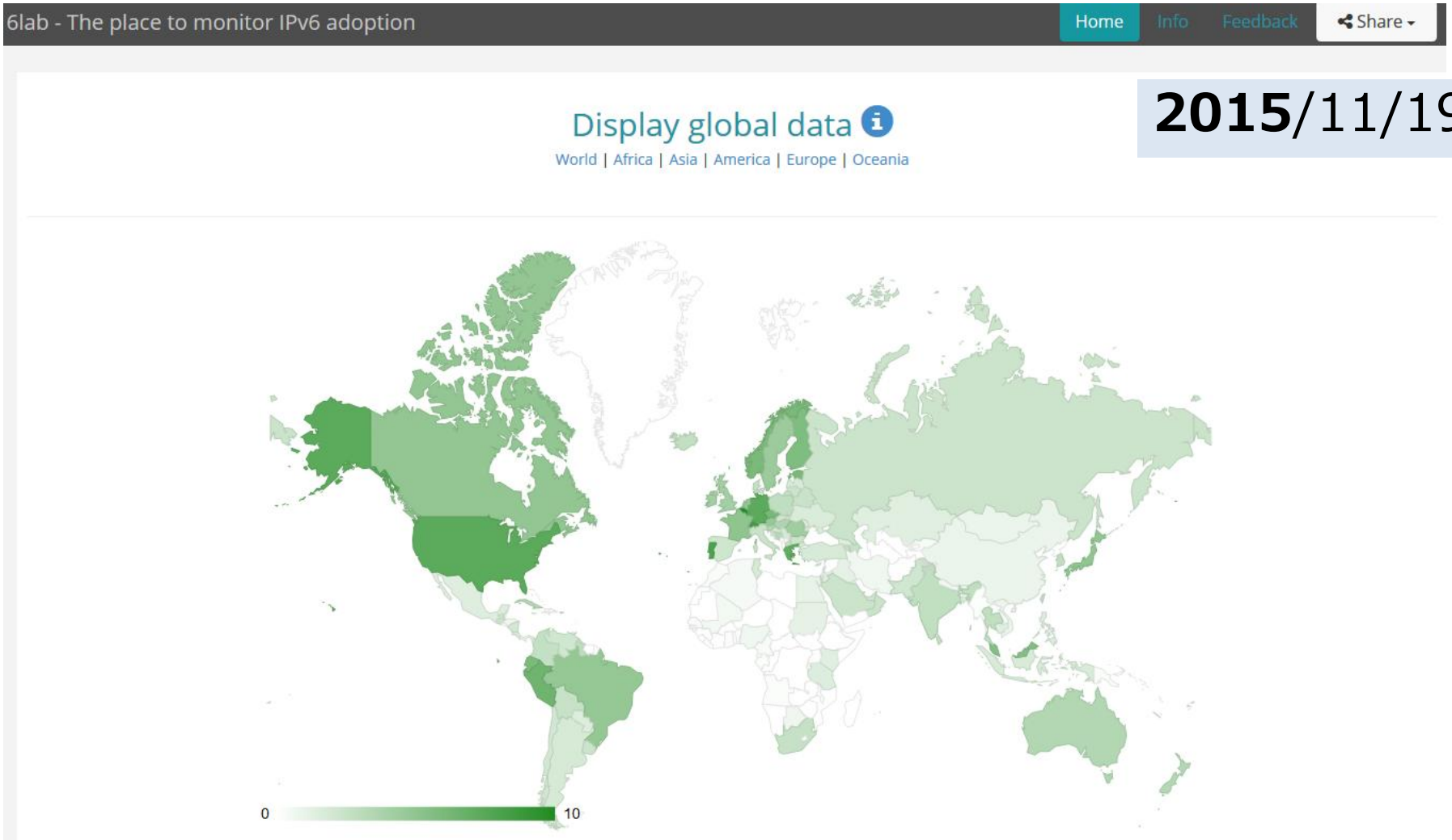


出典： http://www.nic.ad.jp/ja/stat/ip/asia-pacific.html

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



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

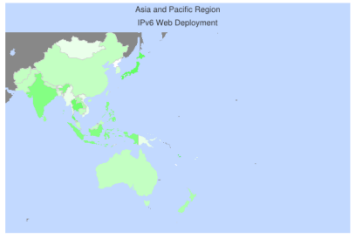


主要な日本のサイトのIPv6対応状況

2014/11/20

IPv6 Deployment Status

For country: Japan For type: All categories Filter



Japan is scanned since 2010-06-17 and the last information is dated 2014-11-20. Return to Aggregated Results. Jump to the IPv6 allocated prefixes.
Leave the cursor over a green/orange box to have more information (MSS, MTU). Hoover the mouse over a red box to display the AS of the web site (this is usually a good indication of the web hoster).
Click on any graphs or maps to zoom on it.
You can add a widget on your own web site with your country IPv6 status or get more geographical maps, click here to see how ;-)

: this site participated at the World IPv6 Day in 2011.

: this site has removed the IPv6 access after the World IPv6 Day (fear?).

Name	Alexa	Web	Mail	DNS
Search Yahoo whois	1/18	FAILED	FAILED	FAILED
Search Google whois	2/32	www.google.co.jp 2a00:1450:4009:808::1017 2011-06-08	aspmx.l.google.com 2a00:1450:400c:c00::1b 2012-07-26	FAILED
B2C Amazon whois	3/49	FAILED	FAILED	pdns6.ultradns.co.uk ns1.p31.dynect.net pdns1.ultradns.net ns3.p31.dynect.net pdns3.ultradns.org pdns2.ultradns.net pdns5.ultrad 2001:502:4612::1 8/10 2010-12-11
fc2.com whois	4/59	FAILED	FAILED	FAILED
rakuten.co.jp whois	5/87	FAILED	FAILED	ns01c.rakuten.co.jp ns04.rakuten.co.jp ns03.rakuten.co.jp ns05c.rakuten.co.jp 2403:400:300:1::5 4/4 2012-11-28
ameblo.jp whois	6/129	FAILED	FAILED	FAILED
livedoor.com whois	7/177	FAILED	FAILED	ns6.livedoor.com ns5.livedoor.com 2407:3000:6c::53 2/6 2010-12-11

https://www.vyncke.org/ipv6status/detailed.php?country=jp

主要な日本のサイトのIPv6対応状況

IPv6 Deployment Status

2015/11/19

For country: Japan For type: All categories Filter

Japan is scanned since 2010-06-17 and the last information is dated 2015-11-19. Return to Aggregated Results. Jump to the IPv6 allocated prefixes.
Leave the cursor over a green/orange box to have more information (MSS, MTU). Hoover the mouse over a red box to display the AS of the web site (this is usually a good indication of the web hoster).
Click on any graphs or maps to zoom on it.
You can add a widget on your own web site with your country IPv6 status or get more geographical maps, click here to see how ;-)

: this site participated at the World IPv6 Day in 2011.

: this site has removed the IPv6 access after the World IPv6 Day (fear?).

Name	Alexa	Web	Mail	DNS
Search Yahoo whois	1/15	FAILED	FAILED	FAILED
Search Google whois	2/18	www.google.co.jp 2a00:1450:4016:802::1017 2011-06-08	alt1.aspmx.l.google.com 2a00:1450:4010:c04::1b 2012-07-26	FAILED
B2C Amazon whois	3/27	FAILED	FAILED	ns3.p31.dynect.net pdns2.ultradns.net pdns4.ultradns.org pdns6.ultradns.co.uk ns1.p31.dynect.net pdns1.ultradns.net pdns3.ultrad 2610:a1:1016::1 8/10 2010-12-11
fc2.com whois	4/53	FAILED	FAILED	FAILED
rakuten.co.jp whois	5/67	FAILED ***CDN***	FAILED	ns04.rakuten.co.jp ns01c.rakuten.co.jp ns03.rakuten.co.jp ns05c.rakuten.co.jp 2403:400:300:1::5 4/4 2012-11-28
nicovideo.jp whois	6/79	FAILED	FAILED	FAILED
livedoor.jp whois	7/109	FAILED	FAILED	FAILED

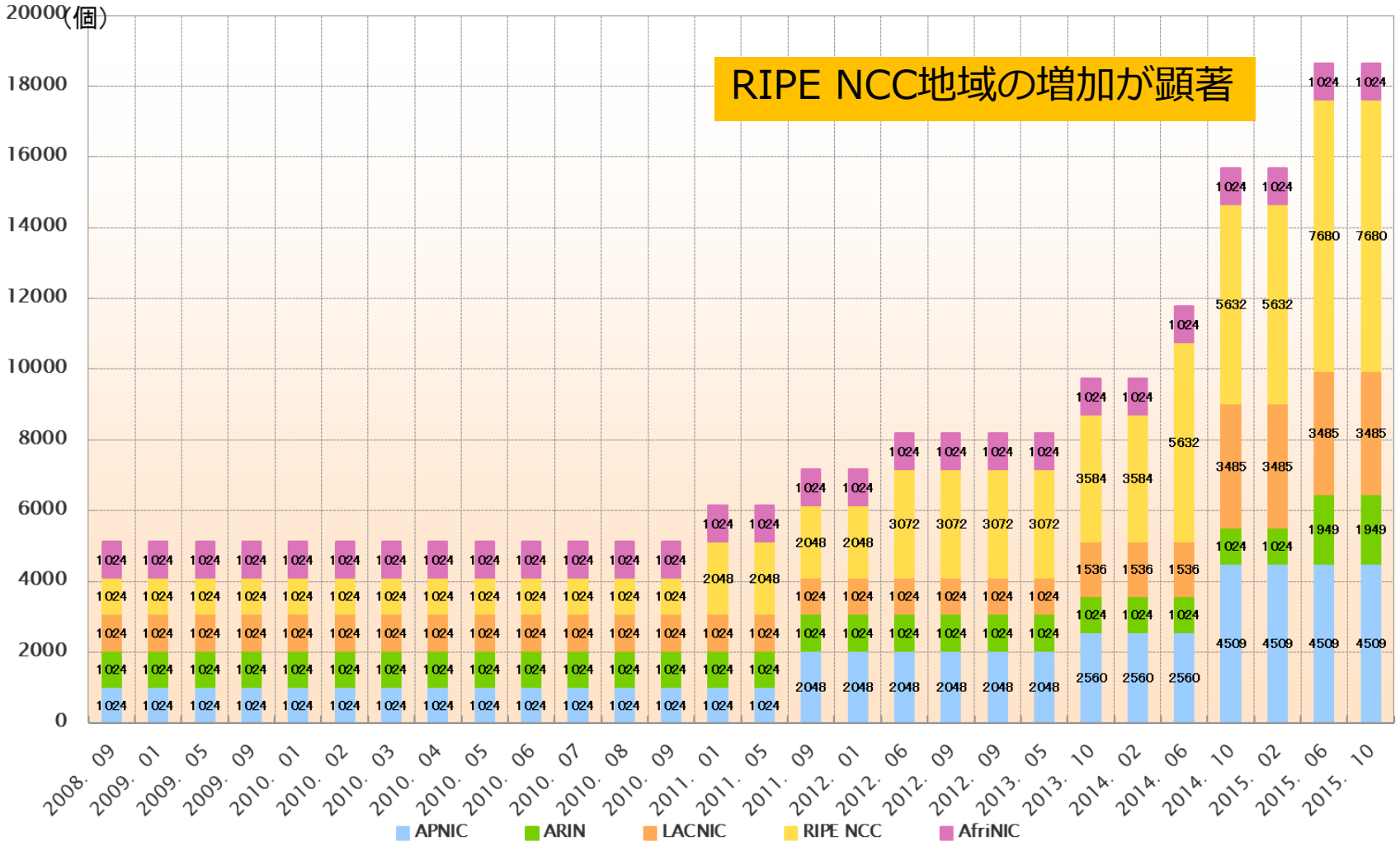
https://www.vyncke.org/ipv6status/detailed.php?country=jp

AS番号 (2byte/4byte)

- 2byte AS
  - 現在残り約200AS
  - 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
  - 日本は促進せず。。
    - 上流ISPが未だ4byteAS未対応、及び心配な人が多い
    - AS取得者のうち、約1割-2割程度の人が4byteASを取得するにとどまる

4byteASのRIRへの配分状況



参照　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

2015年 DNSトピック（セキュリティ関連）

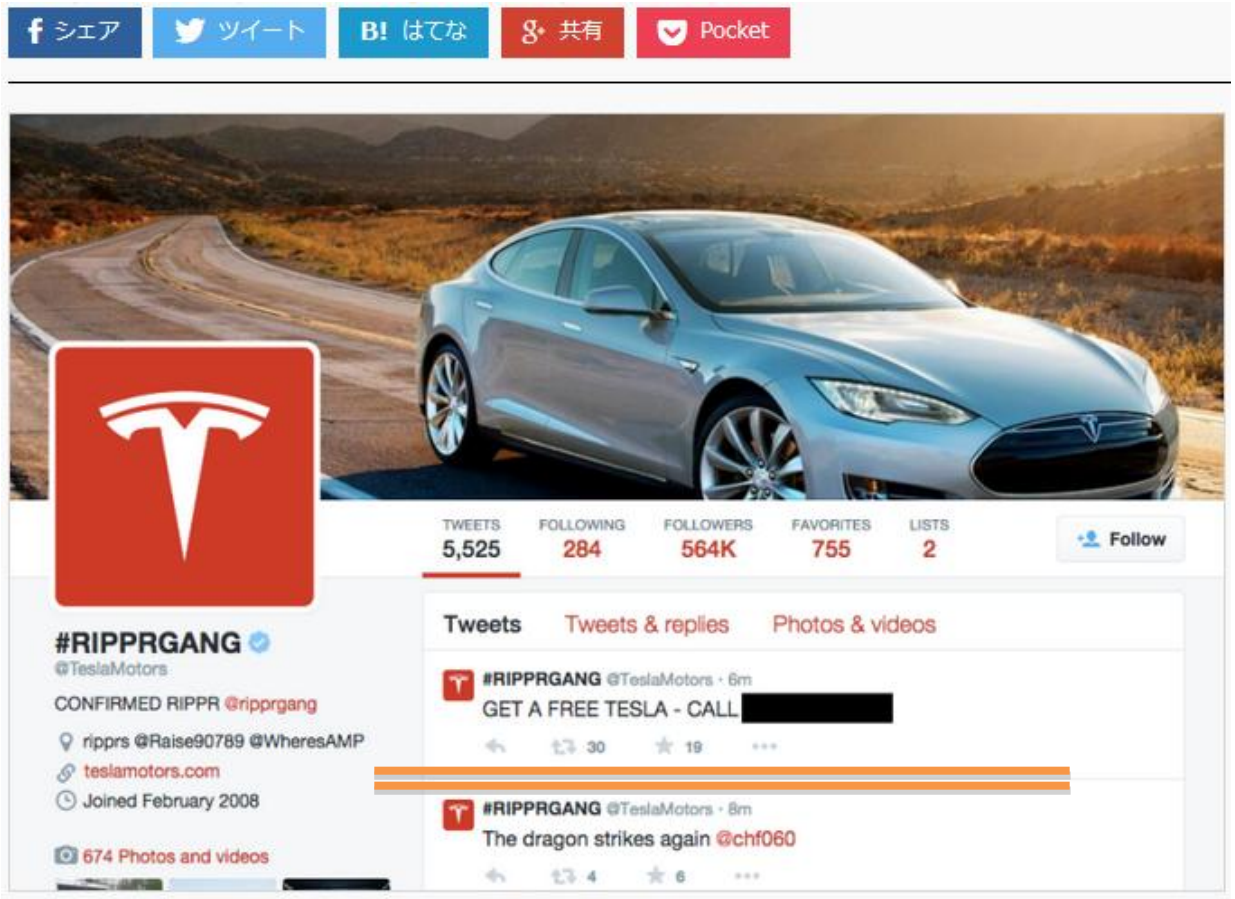
- 相変わらず続くDNS水責め攻撃
  - 関係者の努力と対策により、影響（被害）は2014年に比べ軽減
  - 実施された主な対策
    - ISPにおける攻撃検知・対応、顧客向けアクセス網へのIP53Bの適用
    - 負荷分散、サーバー・ネットワークインフラの強化
    - 攻撃の踏み台となるオープンリゾルバーを減らすための地道な努力
- 今年もあったBINDコロリ。魔の7月は健在
- 大規模化・巧妙化する攻撃　ホームルーターのDNS機能が標的に
  - 問い合わせ先キャッシュサーバを書き換えられて、google-analytics.comを攻撃者が準備した別のサーバに誘導し、不適切な広告が挿入される事例
  - ホームルーターが「オープンDNSフォワーダー」となり、DDoSの踏み台として悪用
- レジストリ・レジストラが被害に遭うドメイン名ハイジャック事例が多発
  - lenovo.comなど（2015年2月）
  - google.com.my、yahoo.com.myなど（2015年4月）
  - teslamotors.com（2015年4月）twitter公式アカウントの乗っ取りにも成功
    - 電子メール経由でのパスワードリセット機能を悪用
  - google.{ma,co.ma}、microsoft.ma、kaspersky.maなど（2015年7月）
  - google.co.pnなど（2015年7月）

2年おきに発生するBINDコロリ

- 2008年：カミンスキー型攻撃手法の発表
- 2009年：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：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：パケット一発で死ぬ脆弱性（再び「**BINDコロリII**」）
- 2012年：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：パケット一発で死ぬ脆弱性（再び「**BINDコロリIII**」）
- 2014年： BIND 9.10.xの脆弱性（DNSサービスの停止）

- （緊急）BIND 9.xの脆弱性（DNSサービスの停止）について **BINDコロリIV**
  （2015年7月31日更新）
  - フルリゾルバー（キャッシュDNSサーバー）／権威DNSサーバーの双方が対象
  -バージョンアップを強く推奨
  - http://jprs.jp/tech/security/2015-07-29-bind9-vuln-tkey.html

TKEY RRの取り扱いの不具合。パケット一発でnamedを落とせる
複数の国内ISPで被害報告あり。



記事：http://jp.techcrunch.com/2015/04/27/20150425teslas-site-and-twitter-account-hacked/

シェア ツイート B! はてな 共有 Pocket

テスラ車「乗っ取り」も　サイバー攻撃、対応済み

Tweet G+1 0 スゴいっ! 0

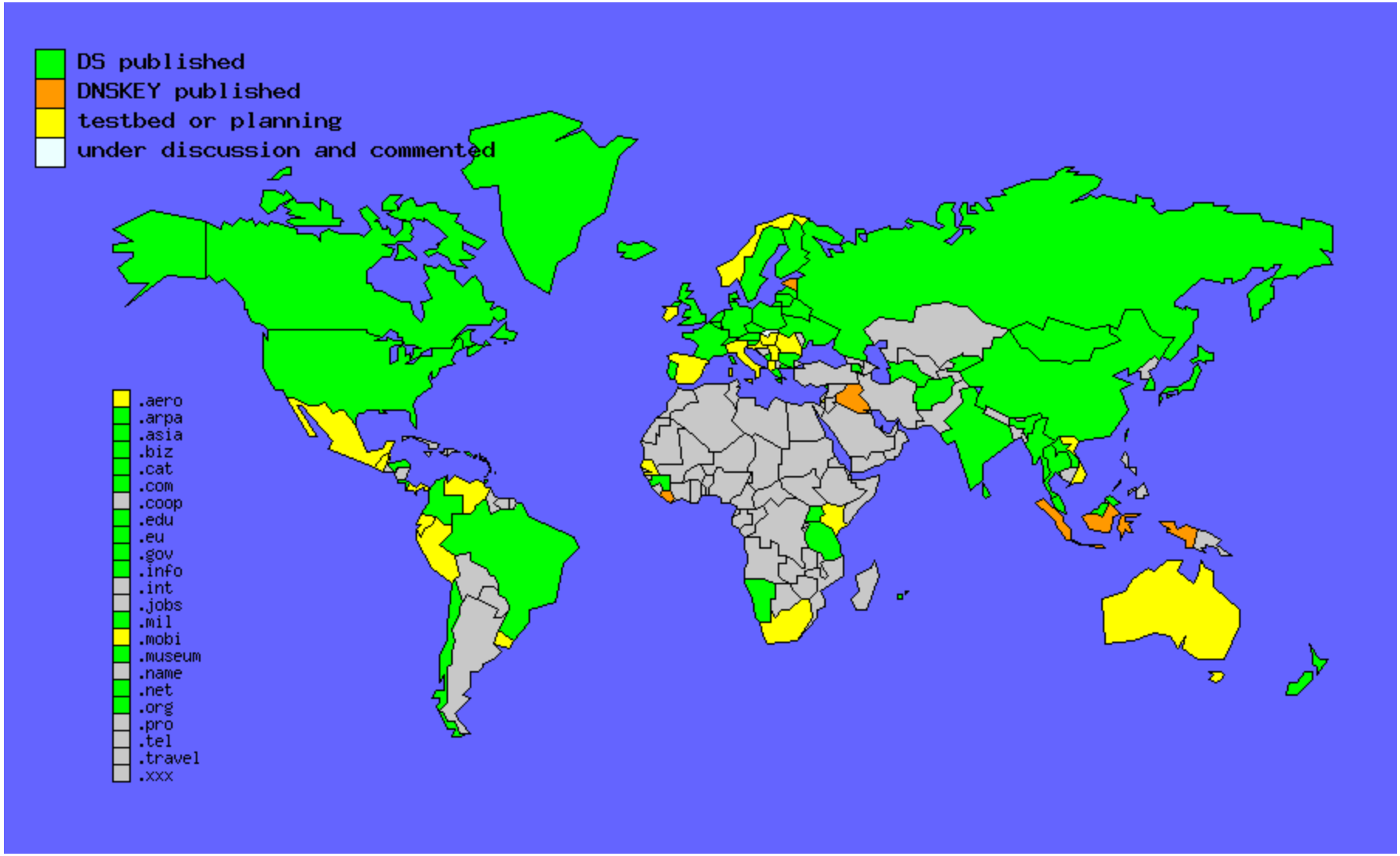
米テスラ・モーターズの電気自動車「モデルＳ」に対し、専門家が車内で細工をした上でサイバー攻撃を仕掛ける実験をしたところ、低速走行中の車を外部からの操作で停止させる「乗っ取り」が可能だったことが６日、分かった。欧米メディアが同日報じた。

記事：http://jp.techcrunch.com/2015/04/27/20150425teslas-site-and-twitter-account-hacked/

2015年 DNSトピック（その他）

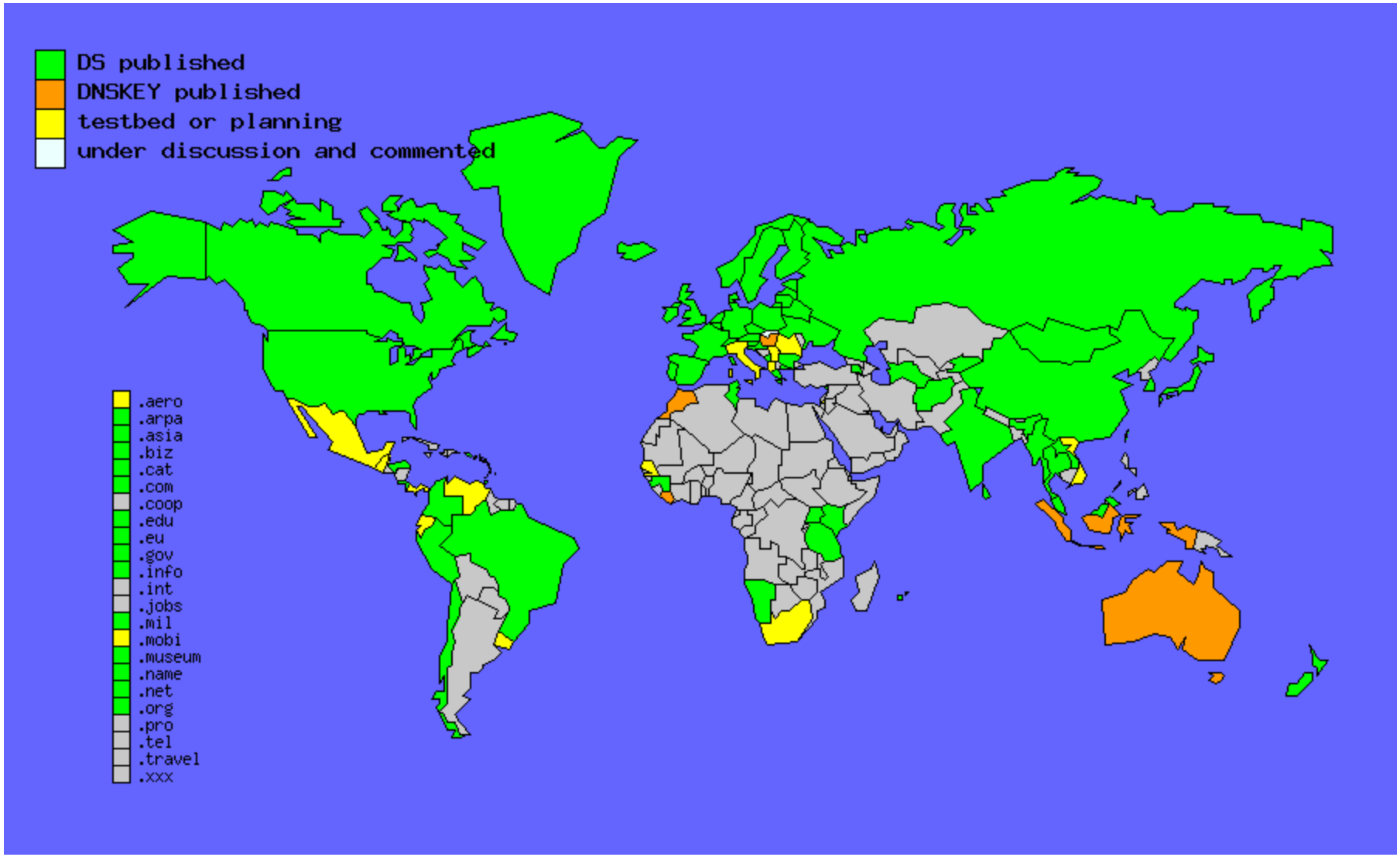
- BIND以外のDNSソフトウェアも充実
  - 権威DNS: NSD, PowerDNS, Knot DNS, Yadida, etc
  - キャッシュDNS: Unbound, PowerDNS Recursor, Knot DNS Resolver, etc
- Public DNSサービスの増加
  - Google Public DNS（8.8.8.8/8.8.4.4）
  - OpenDNS (208.67.222.222/208.67.220.220)
  - NortonDNS (199.85.126.10/199.85.127.10 etc; 参照できるコンテンツが異なるサービスを3段階で提供
  - Baidu（180.76.76.76/114.114.114.114)
  - 114DNS (14.114.114.114/114.114.115.115)
  - Verisign（64.6.64.6/64.6.65.6）
- h.root-servers.net のIPv4/IPv6が12月1日に変更予定
  - 要ヒントファイルの書き換え対応
- .onionが特殊用途ドメインに予約（2015年9月）
  - Torネットワーク用で内部利用可能なドメインとして定義
  - RFC7686：The ".onion" Special-Use Domain Name

TLDのDNSSEC普及状況(**2013**)



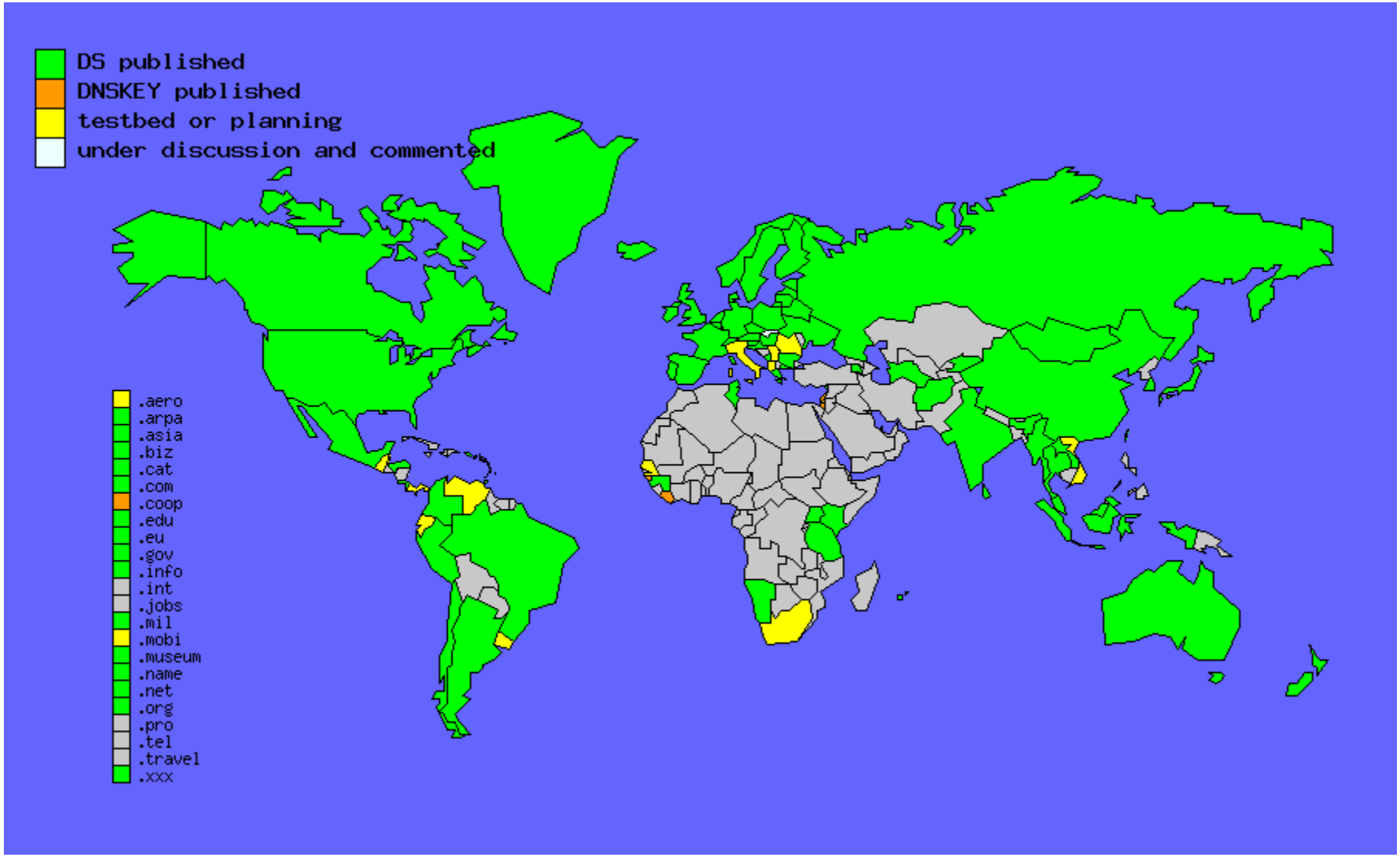
参照　http://www.ohmo.to/dnssec/maps/

TLDのDNSSEC普及状況(**2014**)



参照　http://www.ohmo.to/dnssec/maps/

TLDのDNSSEC普及状況(**2015**)



参照　http://www.ohmo.to/dnssec/maps/

http://dnssec-debugger.verisignlabs.com/

Domain Name: jprs.jp

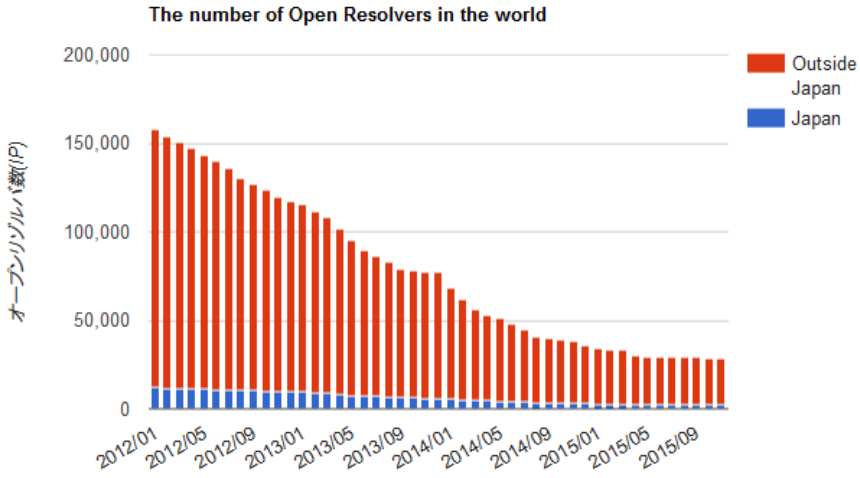
Analyzing DNSSEC problems for jprs.jp

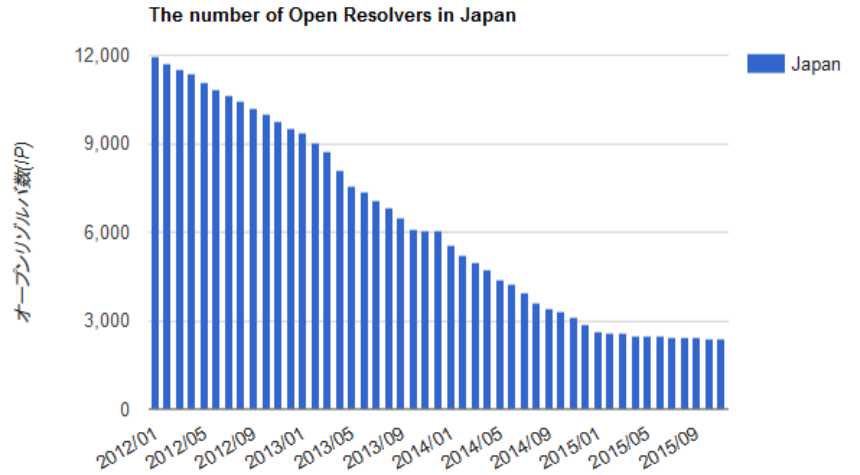
.	Found 2 DNSKEY records for . DS=19036/SHA-1 verifies DNSKEY=19036/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
jp	Found 2 DS records for jp in the . zone Found 1 RRSIGs over DS RRset RRSIG=62530 and DNSKEY=62530 verifies the DS RRset Found 3 DNSKEY records for jp DS=53899/SHA-1 verifies DNSKEY=53899/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=53899 and DNSKEY=53899/SEP verifies the DNSKEY RRset
jprs.jp	Found 2 DS records for jprs.jp in the jp zone Found 1 RRSIGs over DS RRset RRSIG=46491 and DNSKEY=46491 verifies the DS RRset Found 3 DNSKEY records for jprs.jp DS=1942/SHA-256 verifies DNSKEY=1942/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=1942 and DNSKEY=1942/SEP verifies the DNSKEY RRset jprs.jp A RR has value 117.104.133.167 Found 2 RRSIGs over A RRset RRSIG=25161 and DNSKEY=25161 verifies the A RRset

http://www.openresolver.jp/

- オープンリゾルバ確認サイト
  - 接続元 IP アドレスとPC に設定されている DNS サーバ の IP アドレスに対して確認。問題なければグリーンで結果が表示される
- 日本や世界の状況をアップデートしたり注意喚起の実施
- ここ最近数が同程度で推移

http://www.openresolver.jp/ powerd by JPCERT/CC





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

2015年セキュリティ動向

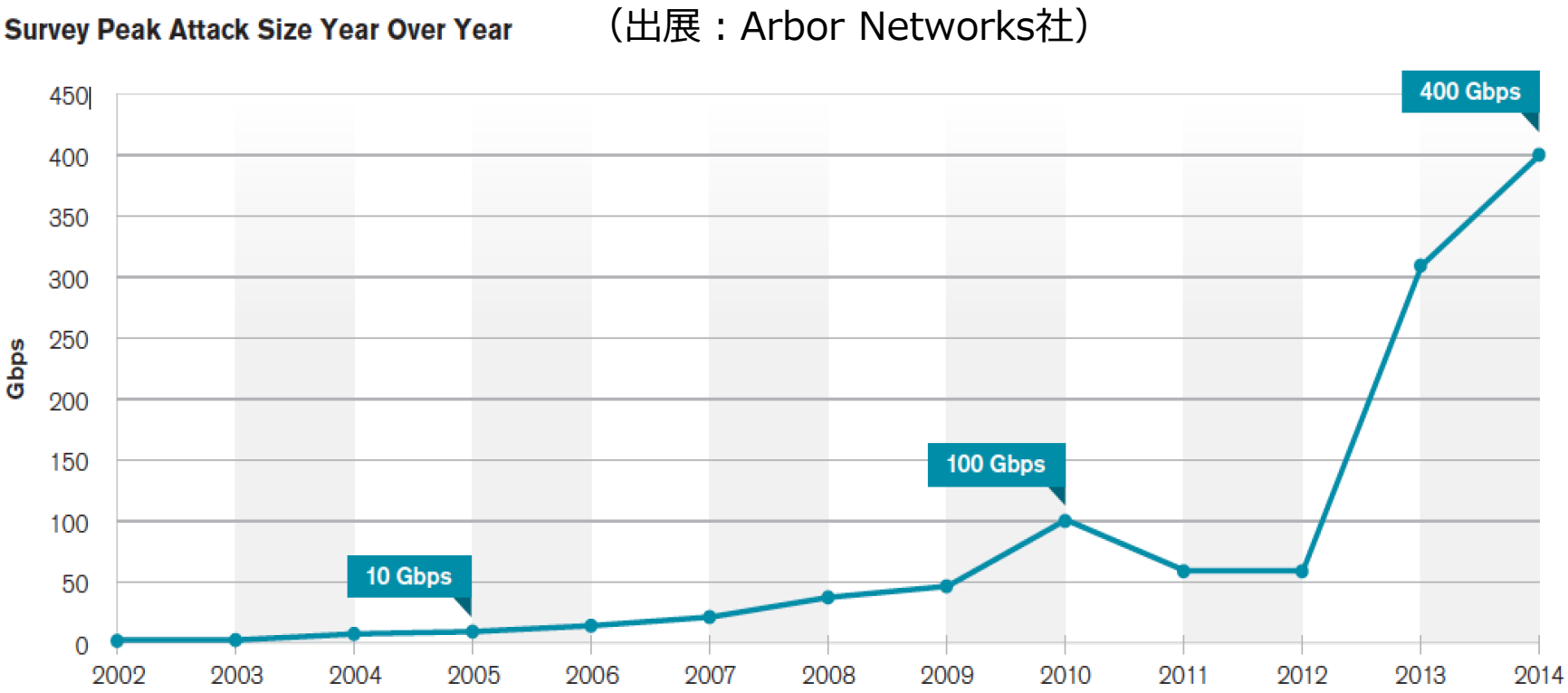
- 大規模するDDoS攻撃
  - Spamhaus/CloudFlareが攻撃目標に（2013年：300Gbps超）
  - Akamai社: 2014年度第三四半期のみで100Gbps以上が17件（最大321Gbps）
- UDPを利用した攻撃の増加（NTP、SSDP、DNS等）
- フィッシング攻撃
  - 特に2015年はネットバンキングを狙った不正サイトへの誘導やウイルス
- PWD漏えい問題が多発
  - 他のサイトで利用されているPWDリストを元に攻撃されるパターン
- 経路のっとり、消失
  - 他人の使っていないアドレスを勝手に利用し故意に経路ハイジャック
  - 国際情勢の影響で経路が一時消失

大規模DDoS攻撃の事例

日時	継続時間	攻撃対象	影響内容
2014年5～6月	14日間	K-optcom社 eo光　DNSサーバー	Web閲覧、メール送受信などに時間がかかる、または表示不可
2014年7月	5日間以上	K-optcom社 eo光　DNSサーバー	Web閲覧、メール送受信などに時間がかかる、または表示不可
2014年6～7月	28日間	セガ「ファンタシー スターオンライン2」	当該期間は、サービス停止 6月27日から、一次サービスを再開
2014年6月	数時間	Evernote	400Gbps以上のDDoS攻撃を受け、サービスに支障が出た 金銭要求
2014年6月	半日	Feedly	Evernoteとほぼ同時にDDoS攻撃を受け、サービス停止 金銭要求。米国ISPなどの協力により、サービス復旧
2014年8月	数時間	PlayStation Network	ネットワークに接続障害。サービス利用停止
2014年12月	不明	北朝鮮（STAR-KP）	9時間半にわたり北朝鮮がインターネットから孤立
2015年3月	6日間以上	Greatfire.org	2.6B/h（通常の2500倍）の接続要求が発生。サービス停止。
2015年3月	4日以上	Github	改竄された第三者Webサイトから2秒毎にGithubへ大量アクセスが発生。攻撃が繰り返され、都度対策を実施。
2015年5月	1時間	FXプライム by GMO	ネットバンキングに接続しつらい状況。金銭要求。
2015年6月	約2時間	セブン銀行	ネットバンキングに接続しつらい状況。金銭要求。
2015年8月	約3時間	ゲーム「Dota2」の世界大会	賞金総額1800万ドルの世界大会「The International 2015」二日目にDDoS攻撃が発生。約3時間試合中止

攻撃の規模が大規模化(数百Gbps)
国内でも金銭要求を目的とした攻撃が顕在化

DDoS攻撃の傾向

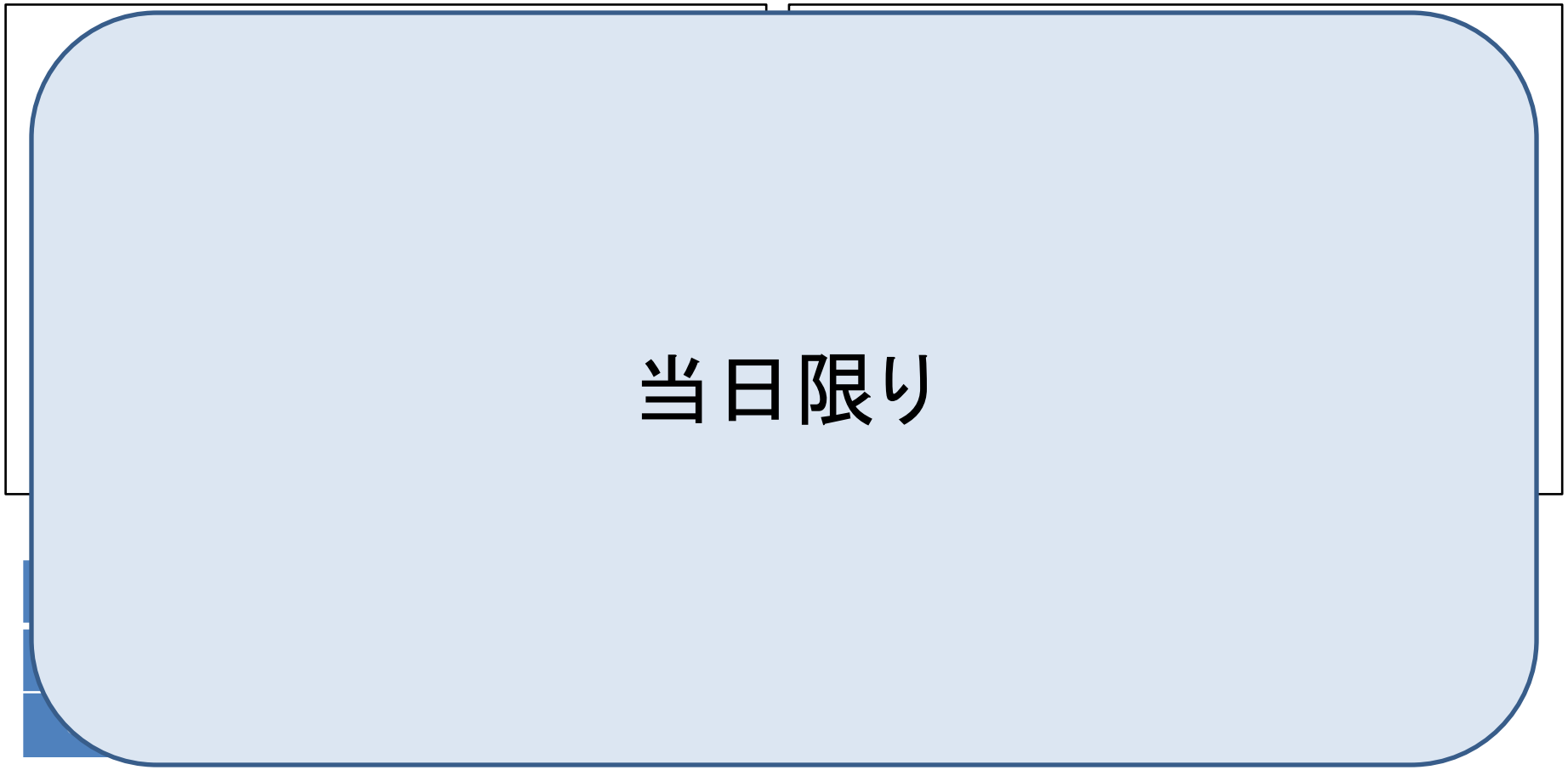


10Gbpsから400Gbpsへ規模が拡大
社会インフラや国家を標的にした攻撃も増大

2015 ATLAS : Attack traffic sizes JP

- Average attack size increases between Q1 2015 and Q2 2015

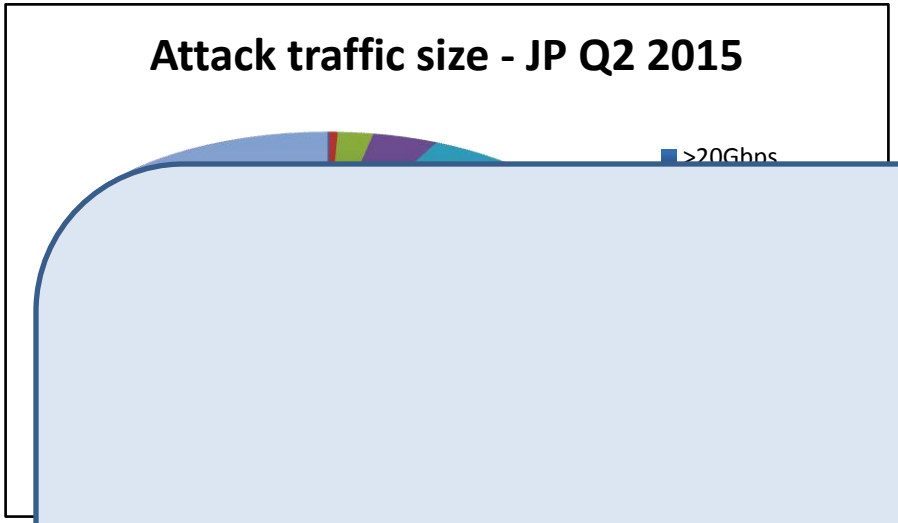
平均するとJPでは数百Mbpsのアタックが発生

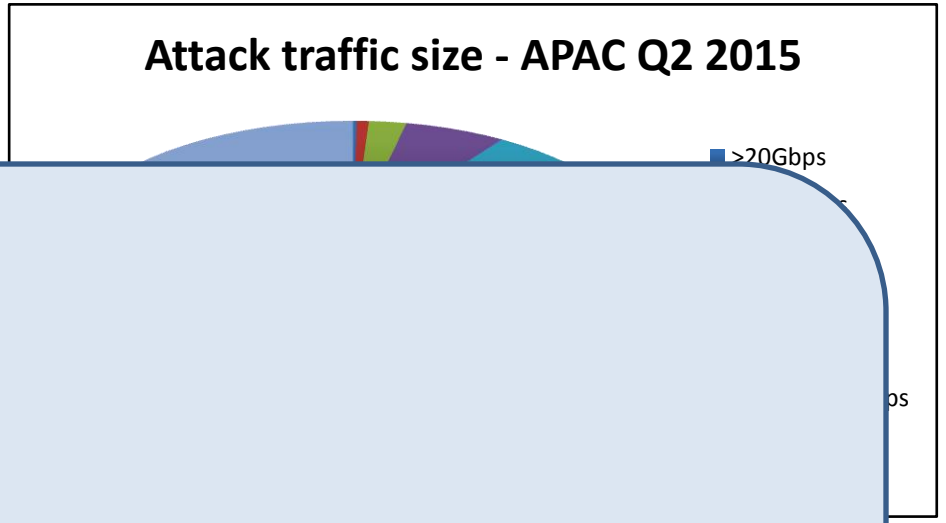


Reference: Arbor Networks, Inc "ATLAS Q2 2015 Update - Japan"

2015 ATLAS : Attack traffic sizes JP

数十Gクラスのアタックが JP/APで発生





当日限り

Reference: Arbor Networks, Inc "ATLAS Q2 2015 Update - Japan"

2015 ATLAS : Reflection attacks JP

Reflection Attacks Analysis

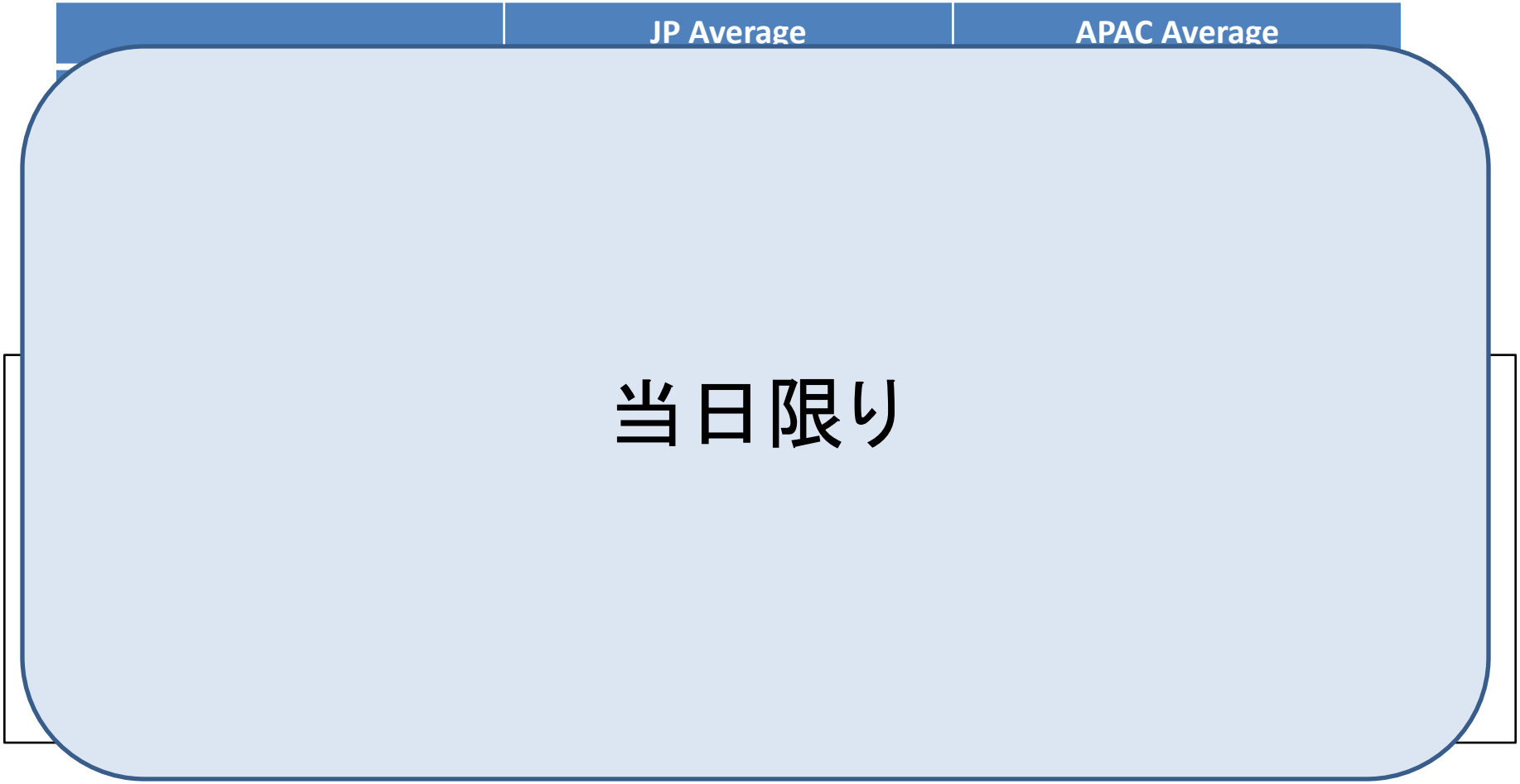
- 90% of the Reflection attacks in Q2 2015 are NTP & SSDP attacks.

当日限り

Reference: Arbor Networks, Inc "ATLAS Q2 2015 Update - Japan"

2015 ATLAS : Attacks duration JP

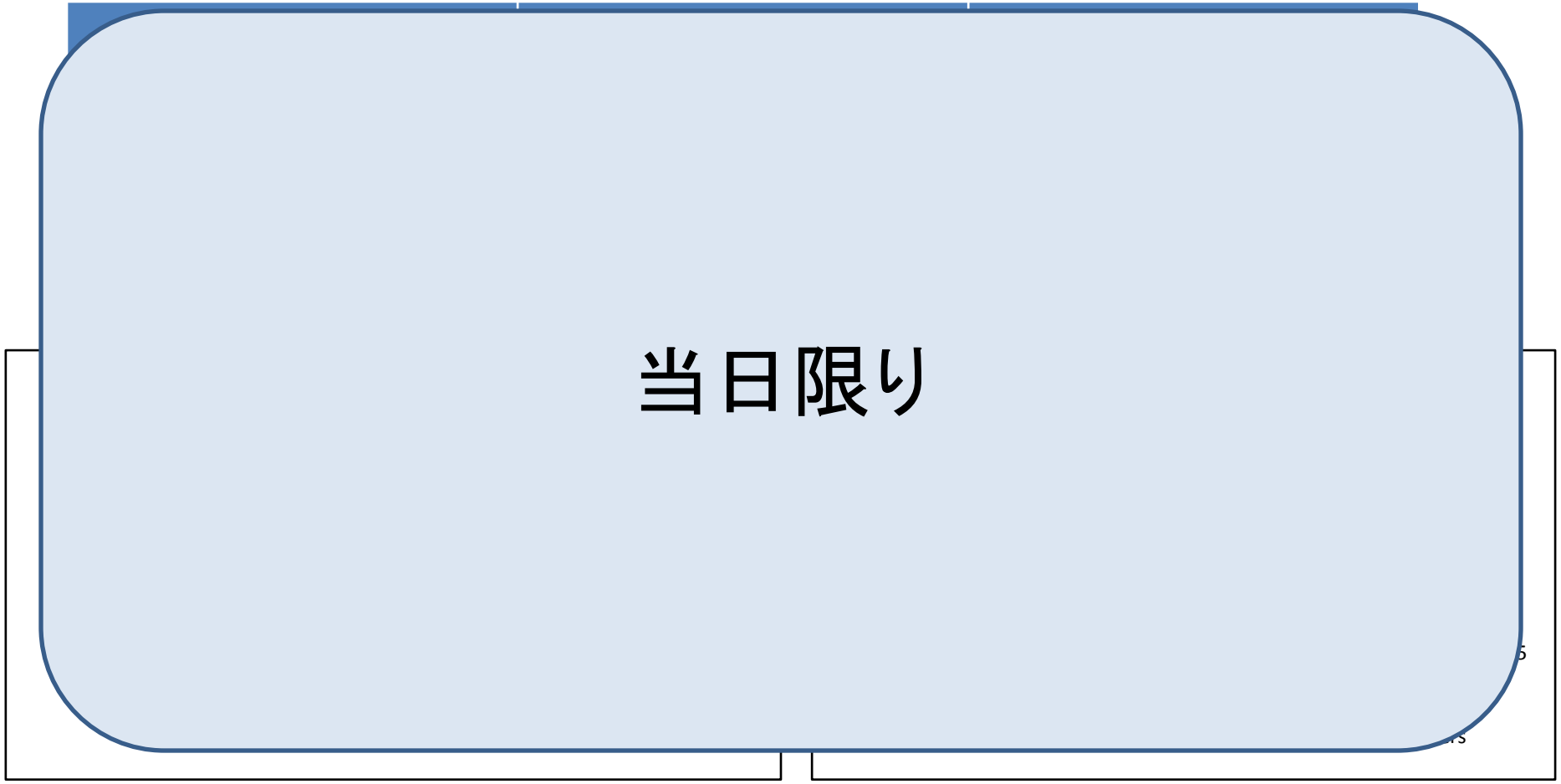
Duration Break-Out (Q2 2015)



Reference: Arbor Networks, Inc "ATLAS Q2 2015 Update - Japan"

2015 ATLAS : Attack destination ports JP

Dest Port Break-Out (Q2 2015)



Reference: Arbor Networks, Inc "ATLAS Q2 2015 Update - Japan"

2015 ATLAS : Attack source countries JP

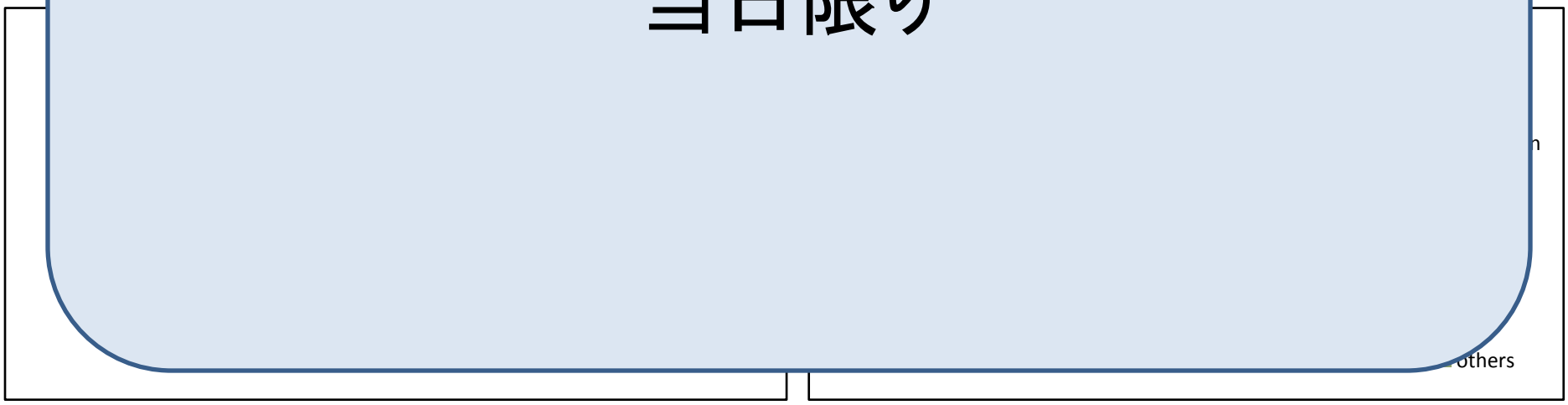
Event Source Break-Out, Q1 2015

- 27% of monitored events cannot be attributed due to data anonymisation / distrib
- C
s

Event Source Break-Out, Q2 2015

- 18% of monitored events cannot be attributed due to data anonymisation /

当日限り



Reference: Arbor Networks, Inc "ATLAS Q2 2015 Update - Japan"

最近流行している経路ハイジャック

- 局所的なハイジャック
  - グローバルインターネット全体へ経路広報するのではなく、BGPのno-export community等を付与するなどして、一部の（狙い撃ちの）ピア先にのみ不正な経路を流し、必要な情報を盗み見る、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

- 未利用アドレスのハイジャック
  - 後述

JPIRRによるハイジャック検出

```
route:      202.12.30.0/24
descr:      JPNICNET
            Japan Network Information Center
            Kokusai Kogyo Kanda Bldg. 6F
            2-3-4 Uchi-Kanda
            Chiyoda-ku, Tokyo 101-0047
            JAPAN
            X-Keiro: okadams@nic.ad.jp
            X-Keiro: okadams-noc@nic.ad.jp
origin:     AS2515
admin-c:    SN3603JP
tech-c:     YK11438JP
tech-c:     MO5920JP
notify:     system@nic.ad.jp
mnt-by:     MAINT-AS2515
changed:    apnic-ftp@nic.ad.jp 20080116
source:     JPIRR
```

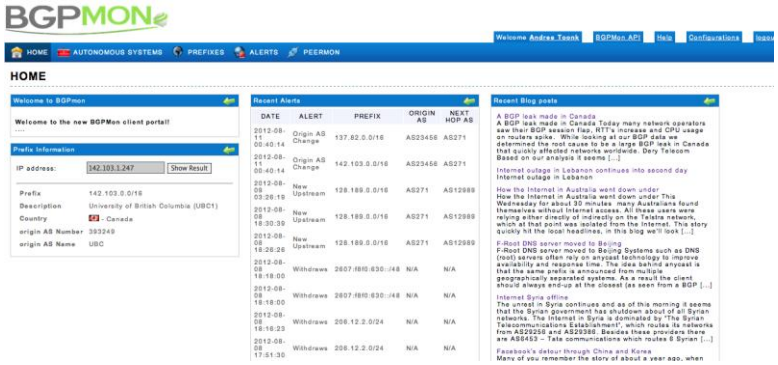
登録されたorigin情報とは異なるoriginASから経路広報が(経路奉行で)検出された場合に、「X-Keiro:」に記載のあて先にメール通知する

<--追加記述

<--複数あて先に通知する場合記述

世界の主な経路検出システム

- BGPmon
  - 5経路まで無料
  - それ以上は1経路あたり月13$
- JPIRR
- Dyn(renesys)
- thousandeyes



http://www.bgpmon.net/

未利用アドレスのハイジャック

- インターネット上に広告されていないIP Prefixが勝手に経路広告されて、SPAM配信等に利用される被害が増大
  - 内部でグローバルアドレスを利用しているケース
  - 保有はしているけど実際には未使用 or 利用開始前
- 2015年の被害例
  - 複数のNTT-NGNアドレスが勝手に使われていた。。
    - ブルガリアや中国から別ドメインと組み合わせて利用
    - RIPE DBにも登録情報があり、追跡するとかなり怪しい。
  - IIJで、アドレス移転に伴い取得したIPアドレスが、利用前に勝手に使われていた（janogレポート@松崎さん)。。
    - 証明書まで偽造されていて、こちらも怪しい。
  - そのIIJのアドレスの真後ろのIPを保有している人も、類似被害にあっていた。。
  - その他にも沢山の報告があがっている

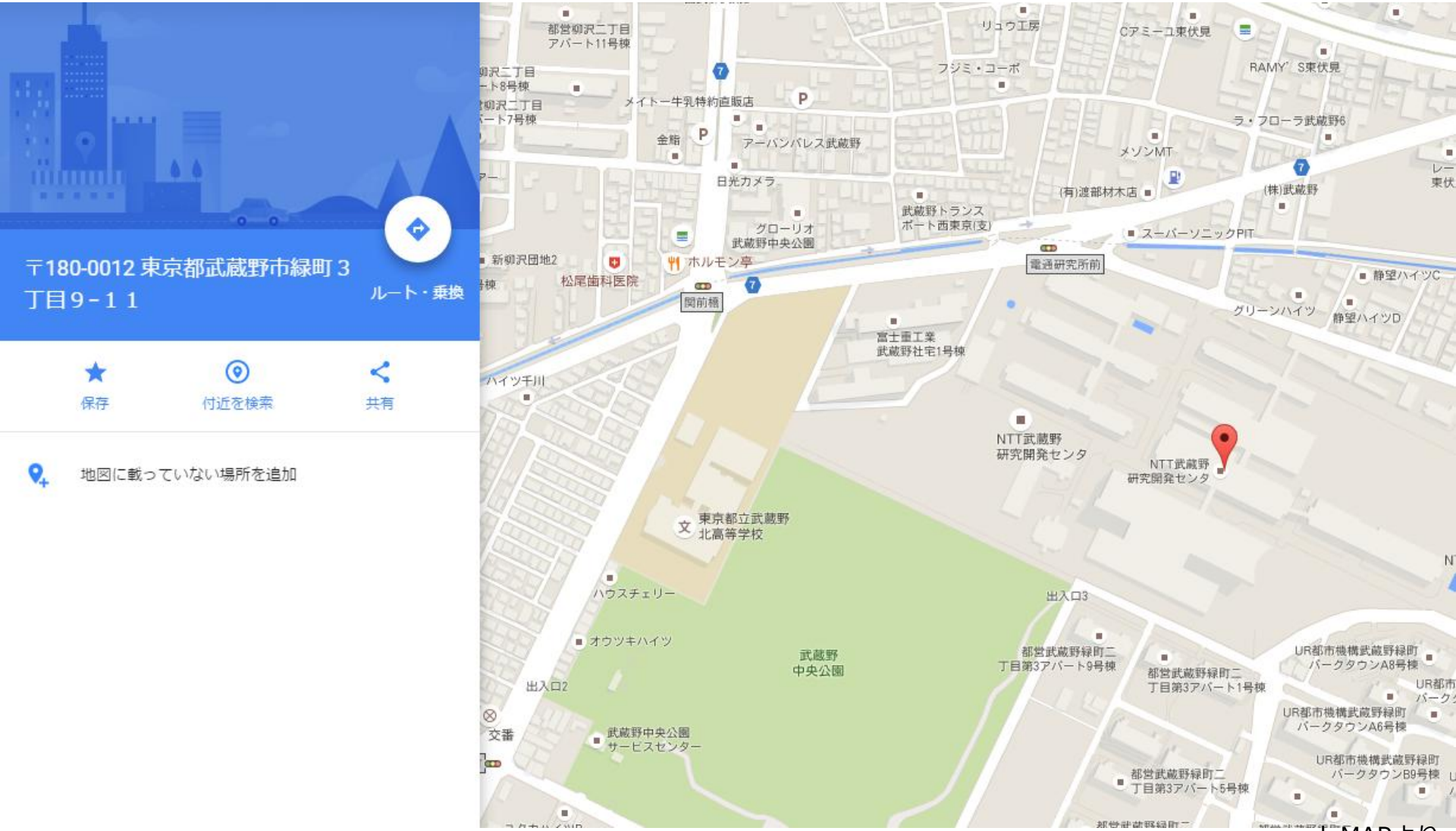
NTT-NGNの被害例

route: 124.245.0.0/16
descr: nipponroute
origin: AS7688
mnt-by: nipponmish-mnt
mnt-by: RIPE-NCC-RPSL-MNT
created: 2013-12-18T19:33:12Z
last-modified: 2013-12-18T19:33:12Z
source: RIPE # Filtered

mntner: nipponmish-mnt
descr: Maintainer
admin-c: HZ1260-RIPE
upd-to: hui.zao@nippontelecom.com
auth: MD5-PW # Filtered
mnt-by: nipponmish-mnt
notify: hui.zao@nippontelecom.com
changed: hui.zao@nippontelecom.com 20131218
remarks: Accepted the RIPE Database Terms and Conditions
created: 2013-12-18T19:19:48Z
last-modified: 2013-12-18T19:19:48Z
source: RIPE # Filtered

person: Hui Zao
address: 3-9-11 Midori-cho, Musashino-shi
phone: +81-422-59-7351
e-mail: hui.zao@nippontelecom.com
nic-hdl: HZ1260-RIPE
mnt-by: nipponmish-mnt
changed: hui.zao@nippontelecom.com 20131218
created: 2013-12-18T19:19:48Z
last-modified: 2013-12-18T19:19:48Z
source: RIPE

怪しい情報が何故か
RIPE DBに登録されていた。。



googleMAPより

よしださん,

研究所の社内名簿検索しましたが，やはり Zao さんは
いないですね.

ＮＴＴ ＮＴ研　　藤崎 智宏 (ＣｏＣｏじゃなくてもはねだ・えりか)
Tel: 04xx-xx-xxxx Fax: 04xx-xx-xxxx

RIPE-NCC-RPSL-MNTの存在

You will be able to delete the object by using then public password of the mntner RIPE-NCC-RPSL-MNT.

This maintainer is used to let people add a route object which address space and/or AS number are outside the RIPE region.

The password is mentioned in the remarks of the object itself:
mntner: RIPE-NCC-RPSL-MNT
descr: This maintainer may be used to create objects to represent
descr: routing policy in the RIPE Database for number resources not
descr: allocated or assigned from the RIPE NCC.
admin-c: RD132-RIPE
auth: MD5-PW # Filtered
remarks: **********
remarks: * The password for this object is 'RPSL', without the *
remarks: * quotes. Do NOT use this maintainer as 'mnt-by'. *
remarks: **********
mnt-by: RIPE-DBM-MNT
referral-by: RIPE-DBM-MNT
source: RIPE # Filtered

実は、自由度の高い「RIPE-NCC-RPSL-MNT」というメンテナーが存在し、それを利用して登録されていた。。

ということで、JPNICで簡単に削除できました

SBL Advisory

DROP Advisory Null List

Ref: SBL265093

124.245.0.0/16 is listed on the Spamhaus Block List - SBL

124.245.0.0/16 is listed on the Don't Route or Peer List - DROP

2015-09-19 13:17:28 GMT | ntt.net

NIPPON TELEGRAPH AND TELEFHONE WEST CORPORATION (AS1273)

Based on research, analysis of network records, our own intelligence sources and our experience, Spamhaus believes that this IP address range is being used or is about to be used for the purpose of high volume spam emission.

As a precaution we are listing this range in an SBL Advisory until we are able to determine with certainty exactly who is operating these domains/hosts/servers and also verify the opt-in permission status and origin of whatever lists are used for those mailings.

Network Information:
[Network Number] 124.245.0.0/16
[Network Name]
[Organization] NIPPON TELEGRAPH AND TELEFHONE WEST CORPORATION
[Administrative Contact] KU1605JP
[Technical Contact] KU1605JP
[Abuse] jpnic-tec@ml.hq.west.ntt.co.jp
[Allocated Date] 2007/10/04
[Last Update] 2007/10/04 18:51:38(JST)

https://www.spamhaus.org/

Domain Name: nunnativ.net
Registry Domain ID: D400353347
Registrar WHOIS Server: Whois.domainerschoice.com
Updated date: 2015-04-06T03:13:09Z
Creation date: 2015-03-28T06:10:14Z

2015/9/7 janogML by peter@ixp.jp より

JPNIC? http://www.spamhaus.org/sbl/query/SBL268451
RICOH http://www.spamhaus.org/sbl/query/SBL268217
KAWASAKI HEAVY INDUSTRIES http://www.spamhaus.org/sbl/query/SBL268212
TOKYO KOUGAKUIN http://www.spamhaus.org/sbl/query/SBL268203

NIDEC SANYO http://www.spamhaus.org/sbl/query/SBL267366
NTT WEST http://www.spamhaus.org/sbl/query/SBL265093
NTT EAST http://www.spamhaus.org/sbl/query/SBL262422
CAC (zombie?) http://www.spamhaus.org/sbl/query/SBL253946

TOKYU CONSTRUCTION http://www.spamhaus.org/sbl/query/SBL249300
MURATA http://www.spamhaus.org/sbl/query/SBL247800 (those dancing robots are so cute!)
LEILIAN http://www.spamhaus.org/sbl/query/SBL247797
FUJITSU http://www.spamhaus.org/sbl/query/SBL233285

有益な情報提供！

KYOWA HAKKO http://www.spamhaus.org/sbl/query/SBL229889
TOYOTECH http://www.spamhaus.org/sbl/query/SBL222568
CORPOVEN (dead company?) http://www.spamhaus.org/sbl/query/SBL222563

dig X.X.X.X.zen.spamhous.org

$ dig 0.0.245.124.zen.spamhaus.org

```
; <<>> DiG 9.8.3-P1 <<>> 0.0.245.124.zen.spamhaus.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42660
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 21, ADDITIONAL: 4

;; QUESTION SECTION:
;0.0.245.124.zen.spamhaus.org.          IN          A

;; ANSWER SECTION:
0.0.245.124.zen.spamhaus.org. 60 IN   A
```

127.0.0.2

Digすると、該当のprefixがどういう状態にあるのかがAレコードの値で判別できる。

ZEN Return Codes

Querying zen.spamhaus.org returns the following result codes for listed entries (see the FAQs for a more complete return code table):

Return Codes	Data Source	Contains
127.0.0.2	SBL Advisory	Direct UBE sources, spam operations & spam services
127.0.0.3	CSS SBL ADVISORY COMPONENT	Direct snowshoe spam sources detected via automation
127.0.0.4-7	XBL Advisory	CBL (3rd party exploits such as proxies, trojans, etc.)
127.0.0.10-11	PBL Advisory	End-user Non-MTA IP addresses set by ISP outbound mail policy

http://www.spamhaus.org/zen/

アタック傾向2015 in JPNAP

送信元IPアドレス (Src IP Address)

IPアドレス	通信量		Avg		Max		Cur	
	bytes	packets	pps	bps	pps	bps	pps	bps
61[redacted]2	65.02G	132.69M	40.21K	157.61M	55.43K	217.30M	0.00	0.00
22[redacted]32	15.28G	31.43M	9.53K	37.03M	12.29K	47.78M	0.00	0.00
21[redacted]/32	11.72G	24.16M	7.32K	28.41M	14.34K	55.50M	0.00	0.00
61[redacted]	7.23G	14.93M	4.53K	17.52M	7.24K	28.13M	0.00	0.00
20[redacted]32	6.73G	13.85M	4.20K	16.32M	7.37K	28.67M	0.00	0.00
11[redacted]32	6.29G	12.94M	3.92K	15.25M	7.78K	30.26M	0.00	0.00
21[redacted]32	5.25G	11.58M	3.51K	12.72M	6.42K	23.03M	0.00	0.00
11[redacted]32	4.64G	9.46M	2.87K	11.24M	8.47K	33.18M	0.00	0.00
12[redacted]32	4.52G	9.23M	2.80K	10.97M	7.78K	30.51M	0.00	0.00
18[redacted]/32	4.15G	8.46M	2.56K	10.05M	6.69K	26.33M	0.00	0.00
11[redacted]2	3[redacted]						0.00	0.00
10[redacted]/32 BOGON	2[redacted]						0.00	0.00
72[redacted]	1.94G	3.99M	1.21K	4.70M	6.14K	23.89M	0.00	0.00
21[redacted]2	1.92G	3.95M	1.20K	4.65M	3.96K	15.39M	0.00	0.00
21[redacted]	1.01G	2.29M	692.60	2.45M	1.64K	5.43M	0.00	0.00
20[redacted]/32	614.15M	1.37M	414.56	1.49M	1.64K	6.13M	0.00	0.00
11[redacted]2	518.13M	1.25M	377.33	1.26M	1.23K	4.19M	0.00	0.00
61[redacted]	407.42M	1.22M	369.88	987.69K	955.73	2.79M	0.00	0.00
21[redacted]/32	545.91M	1.11M	337.61	1.32M	1.23K	4.82M	0.00	0.00
21[redacted]32	172.61M	352.26K	106.74	418.44K	546.13	2.14M	0.00	0.00
21[redacted]32	159.99M	352.26K	106.74	387.85K	546.13	2.12M	0.00	0.00
49[redacted]2	144.51M	294.91K	89.37	350.32K	409.60	1.61M	0.00	0.00
22[redacted]2	144.51M	294.91K	89.37	350.32K	682.67	2.68M	0.00	0.00
21[redacted]32	23.89M	49.15K	14.89	57.91K	273.07	1.06M	0.00	0.00
27[redacted]32	5.67M	16.38K	4.96	13.74K	273.07	755.85K	0.00	0.00

ターゲットが国外

宛先IPアドレス (Dst IP Address)

IPアドレス	通信量		Avg		Max		Cur	
	bytes	packets	pps	bps	pps	bps	pps	bps
195[redacted]/32	144.69G	298.20M	90.36K	350.77M	126.43K	491.16M	0.00	0.00

送信元IPアドレス (Src IP Address)

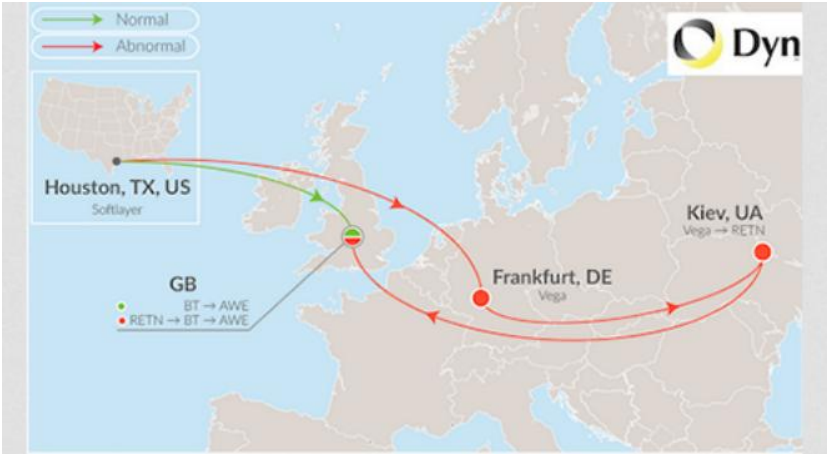
IPアドレス	通信量		Avg		Max		Cur	
	bytes	packets	pps	bps	pps	bps	pps	bps
41[redacted]	325.14M	663.55K	1.23K	4.82M	3.41K	13.38M	0.00	0.00
17[redacted]2	321.13M	655.36K	1.21K	4.76M	3.28K	12.85M	0.00	0.00
76[redacted]	297.04M	606.21K	1.12K	4.40M	2.87K	11.24M	0.00	0.00
20[redacted]	280.99M	573.44K	1.06K	4.16M	3.00K	11.77M	0.00	0.00
95[redacted]	268.94M	548.86K	1.02K	3.98M	3.82K	14.99M	0.00	0.00
78[redacted]	268.94M	548.86K	1.02K	3.98M	3.55K	13.92M	0.00	0.00
38[redacted]	264.93M	540.67K	1.00K	3.92M	3.28K	12.85M	0.00	0.00
70[redacted]	256.90M	524.29K	970.90	3.81M	3.14K	12.31M	0.00	0.00
21[redacted]2	243.68M	499.71K	925.39	3.61M	3.14K	12.31M	0.00	0.00
91[redacted]	244.86M	499.71K	925.39	3.63M	3.14K	12.31M	0.00	0.00
66[redacted]	236.83[redacted]							0.00
21[redacted]	232.82[redacted]							0.00
62[redacted]	222.95[redacted]							0.00
12[redacted]	216.76M	442.37K	819.20	3.21M	2.87K	11.24M	0.00	0.00
20[redacted]	216.76M	442.37K	819.20	3.21M	2.73K	10.70M	0.00	0.00
41[redacted]	208.73M	425.98K	788.86	3.09M	2.87K	11.24M	0.00	0.00
91[redacted] BOGON	188.66M	385.02K	713.01	2.79M	3.69K	14.45M	0.00	0.00
19[redacted]	188.66M	385.02K	713.01	2.79M	2.46K	9.63M	0.00	0.00
21[redacted]	172.61M	352.26K	652.33	2.56M	3.41K	13.38M	0.00	0.00
20[redacted]2	171.20M	352.26K	652.33	2.54M	3.00K	11.68M	0.00	0.00
37[redacted]	156.55M	319.49K	591.64	2.32M	2.73K	10.70M	0.00	0.00
89[redacted]	152.54M	311.30K	576.47	2.26M	2.73K	10.70M	0.00	0.00
76[redacted]	152.54M	311.30K	576.47	2.26M	3.28K	12.85M	0.00	0.00
89[redacted]	151.29M	311.30K	576.47	2.24M	2.59K	10.09M	0.00	0.00
20[redacted]	147.31M	303.10K	561.30	2.18M	2.59K	10.09M	0.00	0.00
46[redacted]	144.51M	294.91K	546.13	2.14M	2.59K	10.17M	0.00	0.00
16[redacted]2 BOGON	98.58M	204.80K	379.26	1.46M	1.23K	4.82M	1.09K	4.05M
64[redacted]	96.34M	196.61K	364.09	1.43M	3.28K	12.85M	0.00	0.00

ターゲットが国内

宛先が国外→国内の踏み台のTrafficを集める
宛先が国内→国外の踏み台のTrafficを集める

Hijack, RouteLeak関連事案

- 2014/12 シリアで（恐らく）アサド政権によるhijack
  - シリアテレコムから1400経路程度のルートが数分間広告
  - Note worthy networks that were affected include US DOD, Chicago Public Schools , Level3, Savis, Telstra, UPC Liberty Global, Comcast, Time Warner Cable, Tiscali UK, China Enterprise Communications, Internet2, Province of New Brunswick, Yandex, Rogers Communications, Uganda Telecom, Dell, Sanford Airport Authority, Kabel Deutschland, Red Hat, YOUTUBE, Iran Post Company, Etihad Atheeb Telecom Company, Akamai, Telefonica Germany and many more.
- 2015/3　イギリスへのトラフィックがウクライナ経由に
- 2015/3　INDOSAT hijack
  - More specific routeが検出
  - 2014年1月には、Googleの8.8.8.8やAkamai, Amazonなどを含む2800程度のPrefixを38分間hijack



http://research.dyn.com/2015/03/uk-traffic-diverted-ukraine/

Hijack, RouteLeak関連事案

- 2015/6 マレーシアTelecomのルートLeakで環太平洋地域の広範囲に遅延等の影響
- 2015/7 AWS(Boston)が約40分程度 RouteLeakにより停止
- 2015/9 インド/イランからK-rootへの到達不能
- 2015/10 iTELがRullRouteをoriginate
- 2015/11 インドからハイジャック

- Google's extensive peering likely insulated it from some of the effects of having its routes leaked. However, it didn't escape the incident completely unscathed. Here is an example of a normal traceroute to Google's data center in Council Bluffs, Iowa from Prague, which goes via Frankfurt and London before crossing the Atlantic Ocean.
- trace from Prague to Google, Council Bluffs, IA at 02:45 Jun 11, 2015

```
1  *
2  212.162.8.253    ge-6-14.car2.Prague1.Level3.net     16.583
3  4.69.154.135     ae-3-80.edge3.Frankfurt1.Level3.net 22.934
4  4.68.70.186      Level 3 (Frankfurt, DE)             23.101
5  209.85.241.110   Google (Frankfurt, DE)              23.796
6  209.85.250.143   Google (Frankfurt, DE)              24.086
7  72.14.235.17     Google (London, GB)                 32.709
8  209.85.247.145   Google (New York City)              103.091
9  216.239.46.217   Google (Council Bluffs)             133.098
10 209.85.250.4     Google (Council Bluffs)             133.245
11 216.239.43.217   Google (Council Bluffs)             133.536
12 *
13 74.125.142.192   Google (Council Bluffs)             132.643
```

2015/6
マレーシアのLeakで環太平洋地域の広範囲に遅延等影響

- During the routing leak, traces were redirected to Hong Kong (where Telekom Malaysia gets Level 3 transit) and across the Pacific Ocean for a performance hit of almost 400ms.
-

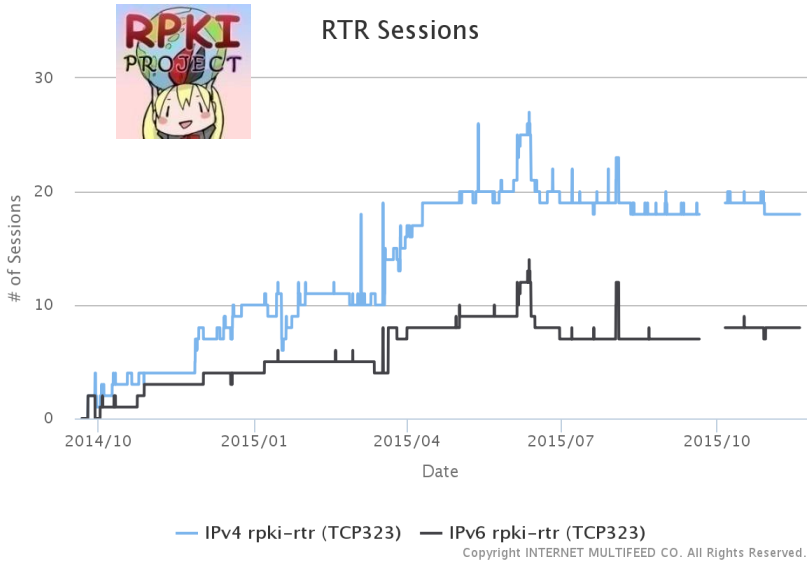
trace from Prague to Google, Council Bluffs, IA at 09:04 Jun 12, 2015

```
1  *
2  212.162.8.253    ge-6-14.car2.Prague1.Level3.net                  41.213
3  *
4  67.17.134.242    telekom-malaysia-berhad.xe-0-2-0.ar2.clk1.gblx.net 451.264
5  *
6  209.85.242.242   Google (Mountain View)                           509.481
7  66.249.94.140    Google (Mountain View)                           482.303
8  64.233.174.176   Google (Mountain View)                           459.441
9  216.239.41.139   Google (Council Bluffs)                          457.846
10 72.14.239.48     Google (Council Bluffs)                          468.626
11 216.239.43.219   Google (Council Bluffs)                          456.841
12 *
13 74.125.142.192   Google (Council Bluffs)                          509.298
```


http://research.dyn.com/2015/06/global-collateral-damage-of-tmnet-leak/

RPKIの普及

- 国際的にも徐々に普及が進んでいる
  - 特にLACNIC, RIPE地域
- 日本国内でも、ちらほら登録方法や、誰が登録したらよいの？等の質問が増えてきた。
  - IRRはAS holder, RPKIはAddress holder



10 records per page Search:

RIR	Total	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
AFRINIC	13721 (100%)	230 (1.68%)	14 (0.1%)	13477 (98.22%)	94.26%	1.78%
APNIC	153861 (100%)	3038 (1.97%)	1115 (0.72%)	149708 (97.3%)	73.15%	2.7%
ARIN	216330 (100%)	1698 (0.78%)	335 (0.15%)	214297 (99.06%)	83.52%	0.94%
LACNIC	76766 (100%)	14981 (19.52%)	689 (0.9%)	61096 (79.59%)	95.6%	20.41%
RIPE NCC	155033 (100%)	16280 (10.5%)	1205 (0.78%)	137548 (88.72%)	93.11%	11.28%

http://rpki.surfnet.nl/perrir.html

内容

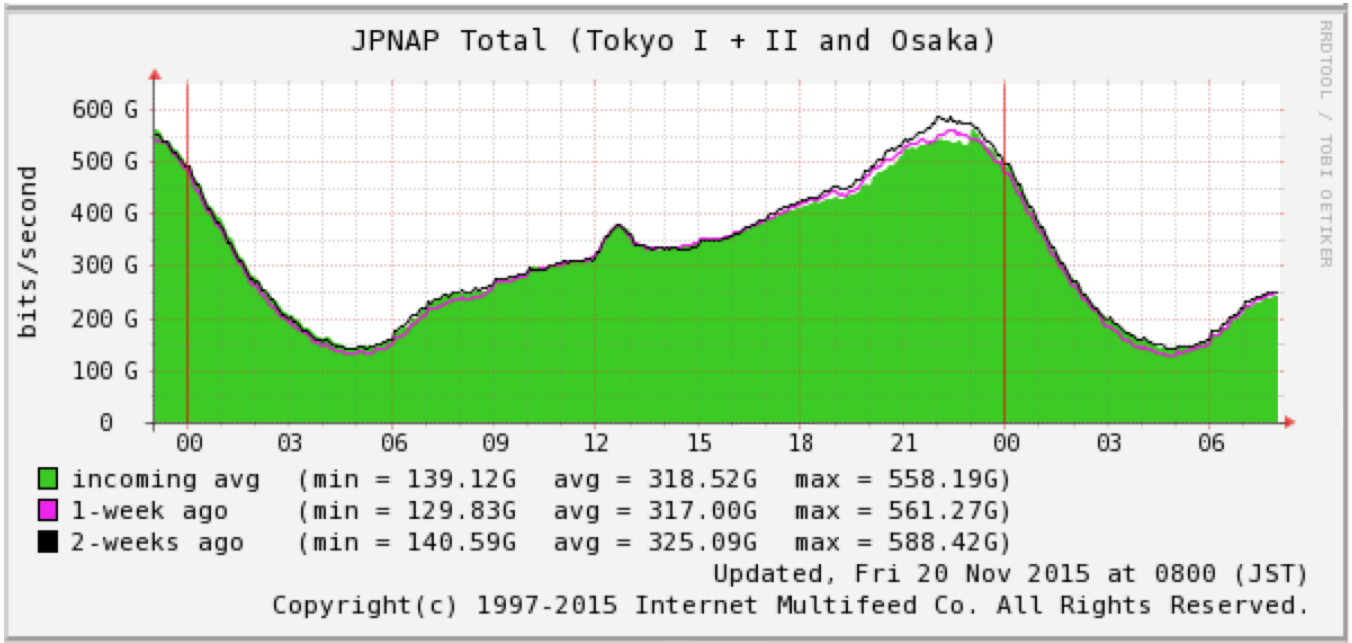
- トラフィック動向
- ルーティング動向
- DNS動向
- セキュリティ動向
- まとめ

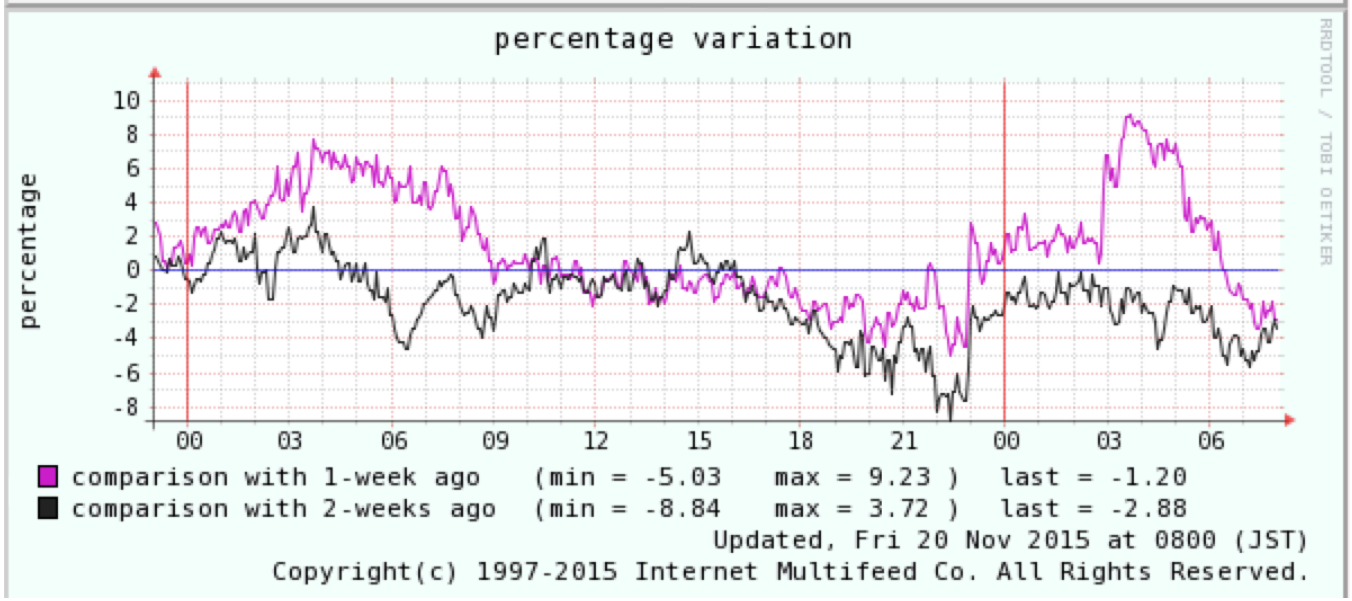
2015年のまとめ

- 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
  - クラウド型サービスの増加によりアップロードも増加
  - イベント時のトラフィック急増も顕著に
- ルーティング動向
  - 枯渇後もIPv4は依然増加、さらに細かくなる可能性あり
  - IPv6の急増にも注意が必要
- DNS動向
  - 水責め攻撃やドメインハイジャックも多数発生、継続して対策が必要
  - BINDの被害も相変わらず多く、日々の運用対処が必要
- セキュリティ動向
  - 大規模する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

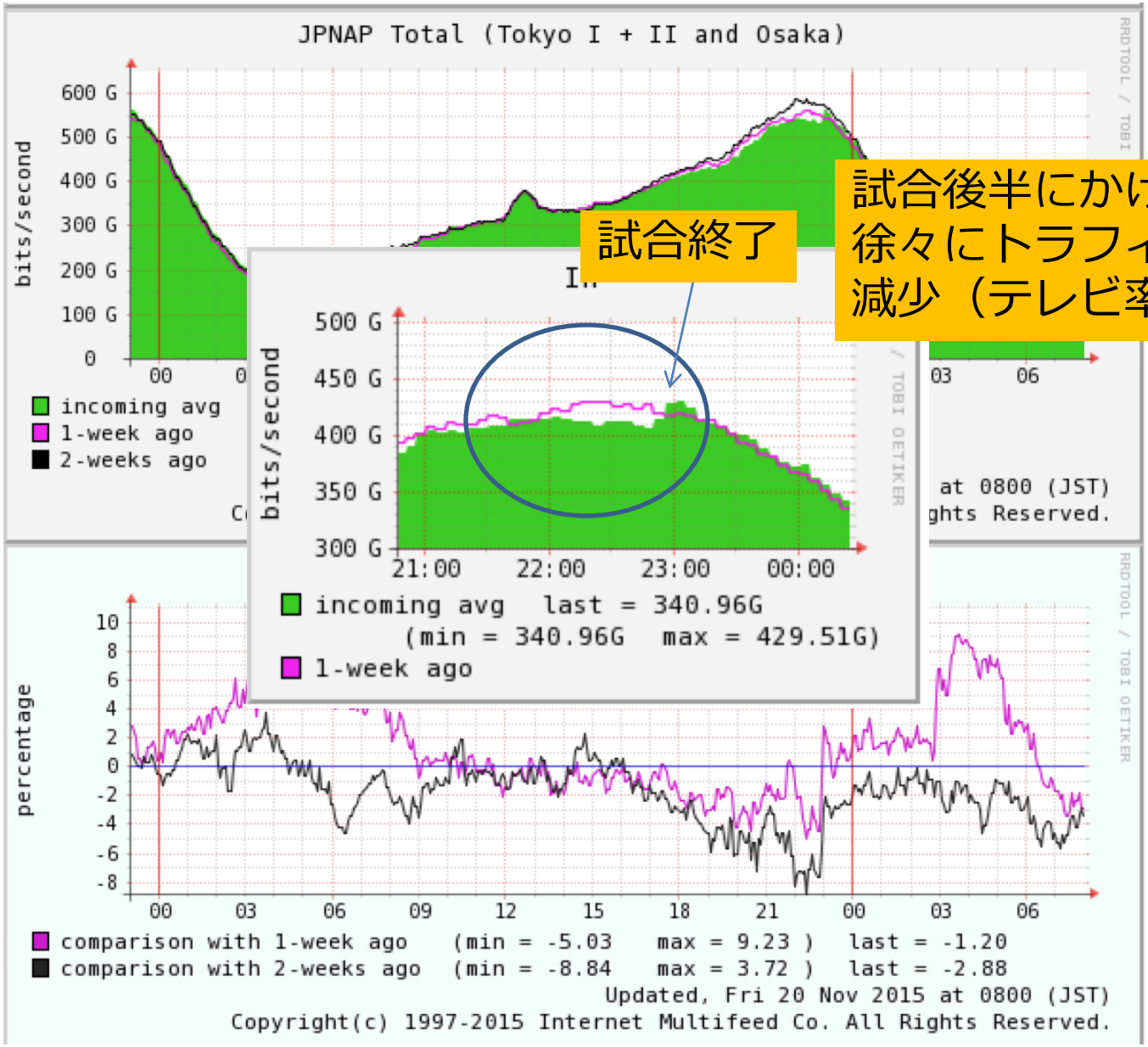
質疑応答スライド

前日11/19の世界野球準決勝（日韓戦）





前日11/19の世界野球準決勝（日韓戦）



夏の甲子園決勝（2015年8月20日）