2013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 etc～

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
- 日本や世界のIX動向
- まとめ

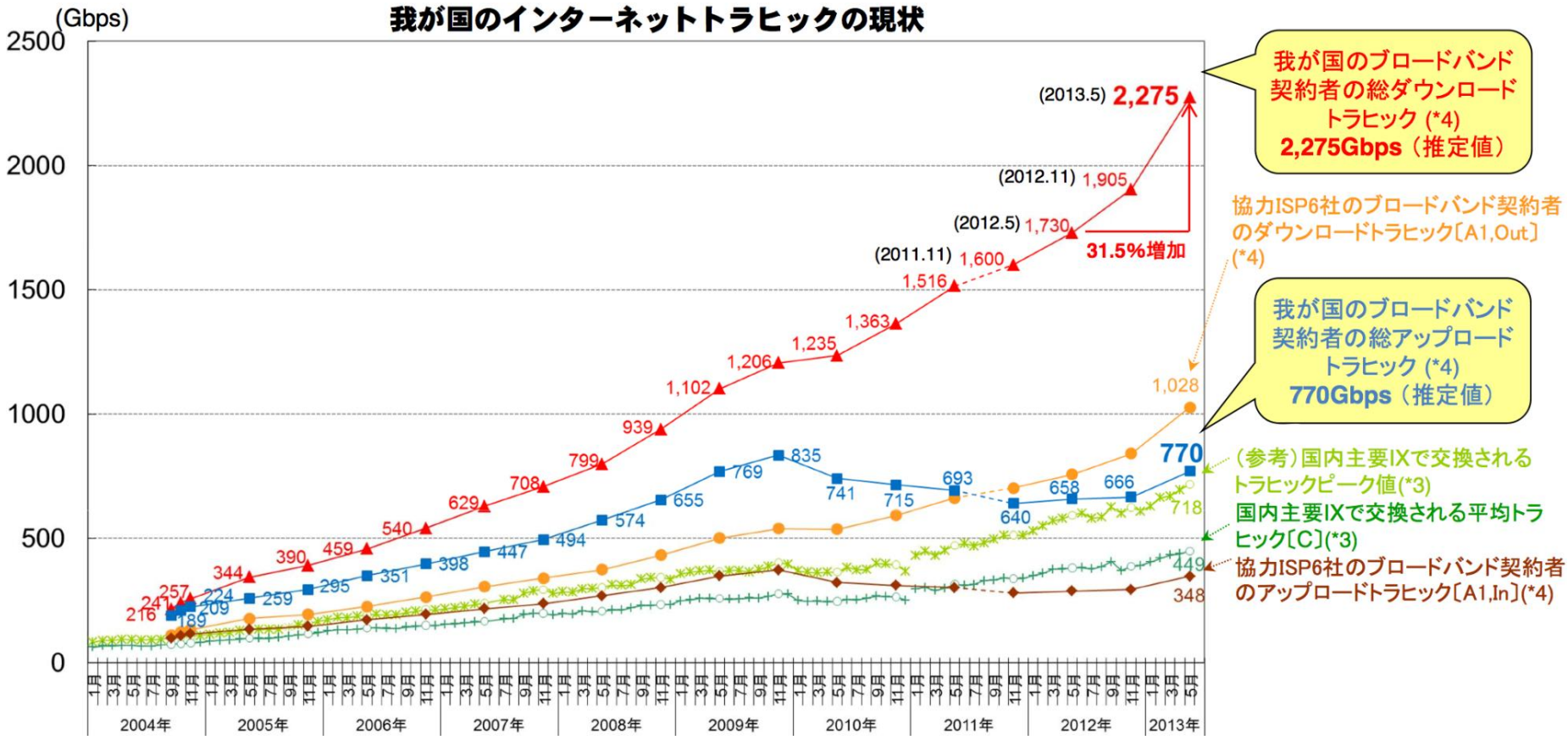
内容

- 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
- 日本や世界のIX動向
- まとめ

2013年 トラフィック動向

- ブロードバンド、モバイルトラフィックの継続増加
  - 日本のブロードバンドの平均トラフィックが2Tbpsを超える
  - スマートフォンの普及により著しいモバイルトラフィック増　年1.7倍程度の伸び
  - ダウンロード型のトラフィック増（特に国際トラフィック）が加速している
  - モバイル端末：帯域制限により月末にかけて減少する傾向が最近目立つ
  - ショートパケットが増えており、pps rateを気にしないといけない
- 1日のトラフィック
  - ピーク時間が徐々に前倒しになってきている（22:00-23:00の前半がピーク）
  - 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
- HTTPSが急増
  - Googleがログインユーザ以外にも検索結果を強制SSL化した影響
- IPv6トラフィックはゆるやかに増加
- イベント時のトラフィック変化
  - 半沢直樹、IOSダウンロード、プロ野球、台風等で急激な増減が観測

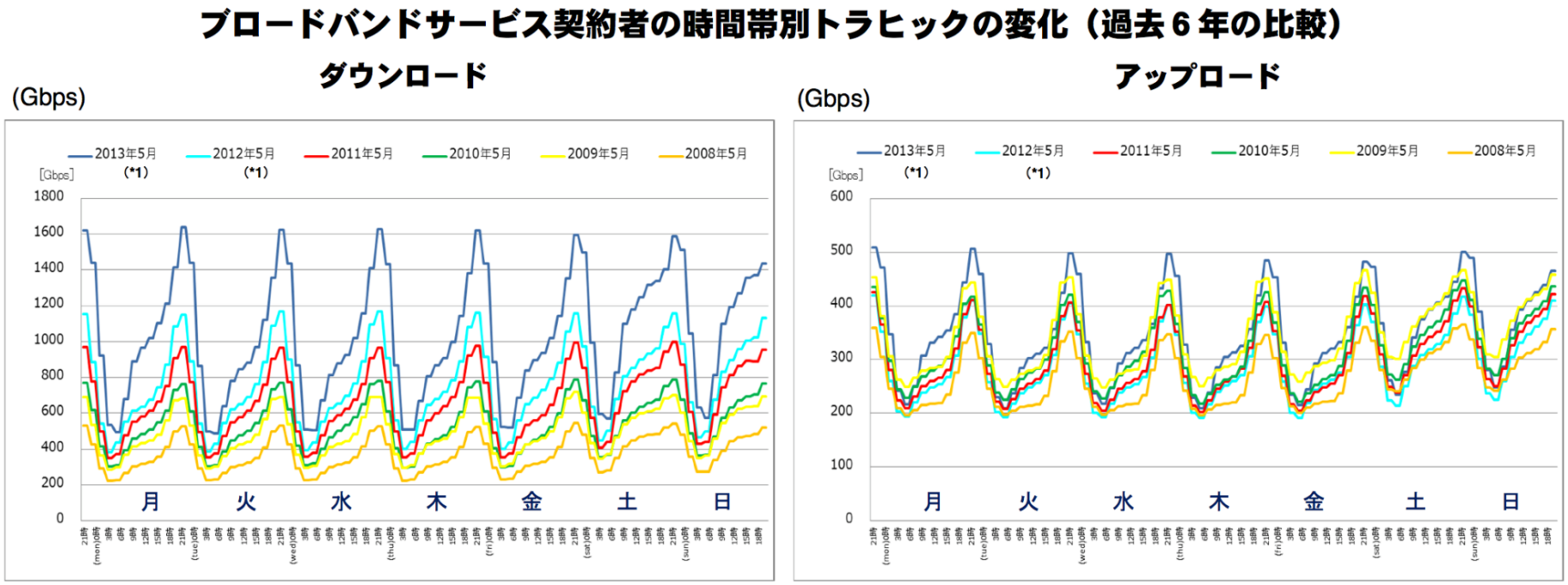
日本国内のトラフィック推移



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**」　2013年8月30日
http://www.soumu.go.jp/main_content/000244628.pdf

日本国内のトラフィック推移

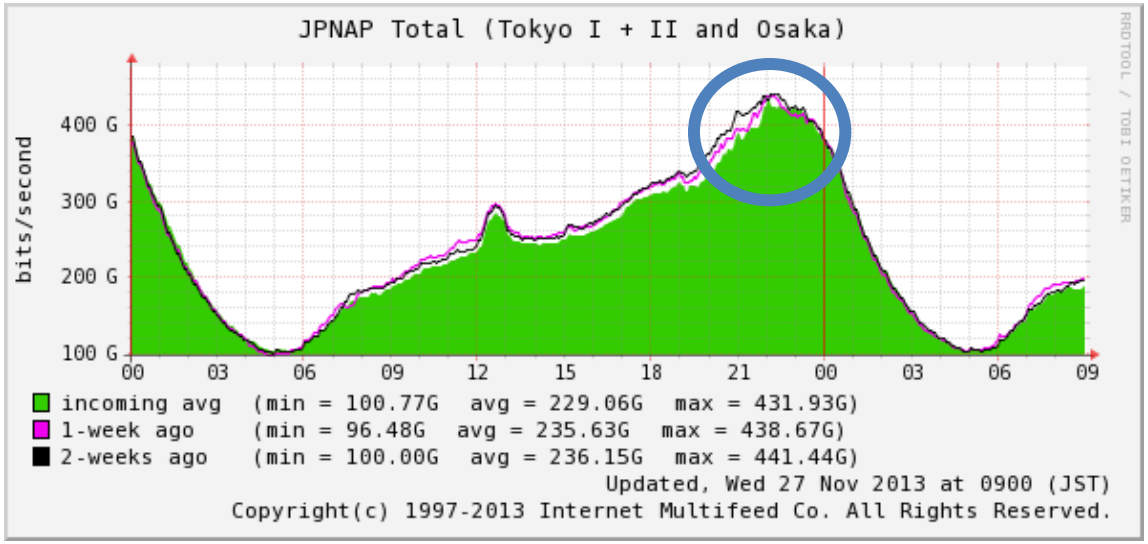
5分平均のピークトラフィックの推移



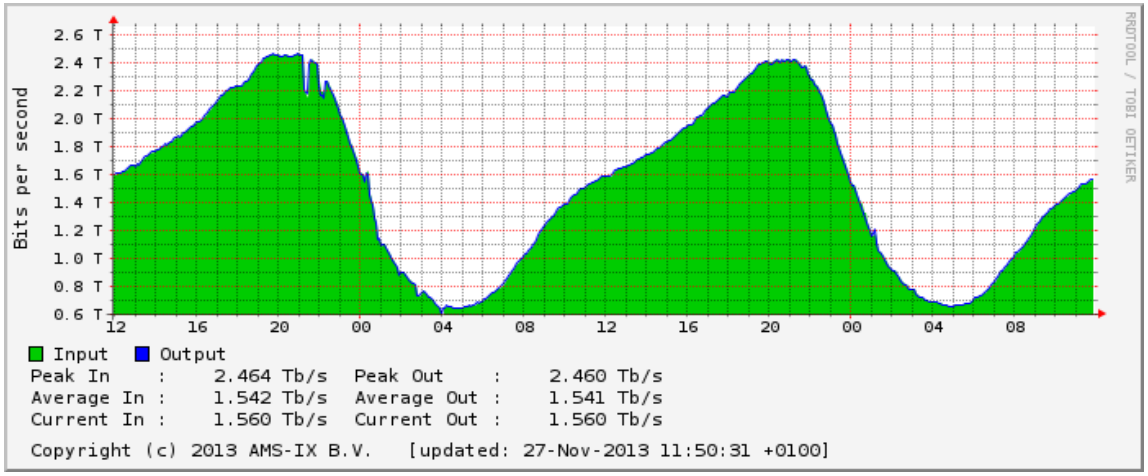
出典：総務省「**我が国のインターネットにおけるトラヒックの集計・試算**」　2013年8月30日
http://www.soumu.go.jp/main_content/000244628.pdf

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

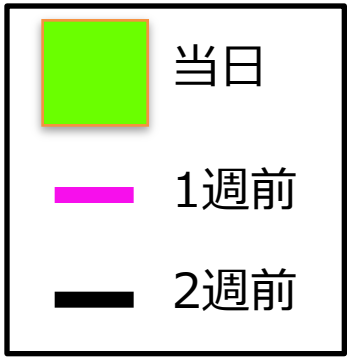


JPNAP(Japan)の
1日のトラフィック推移

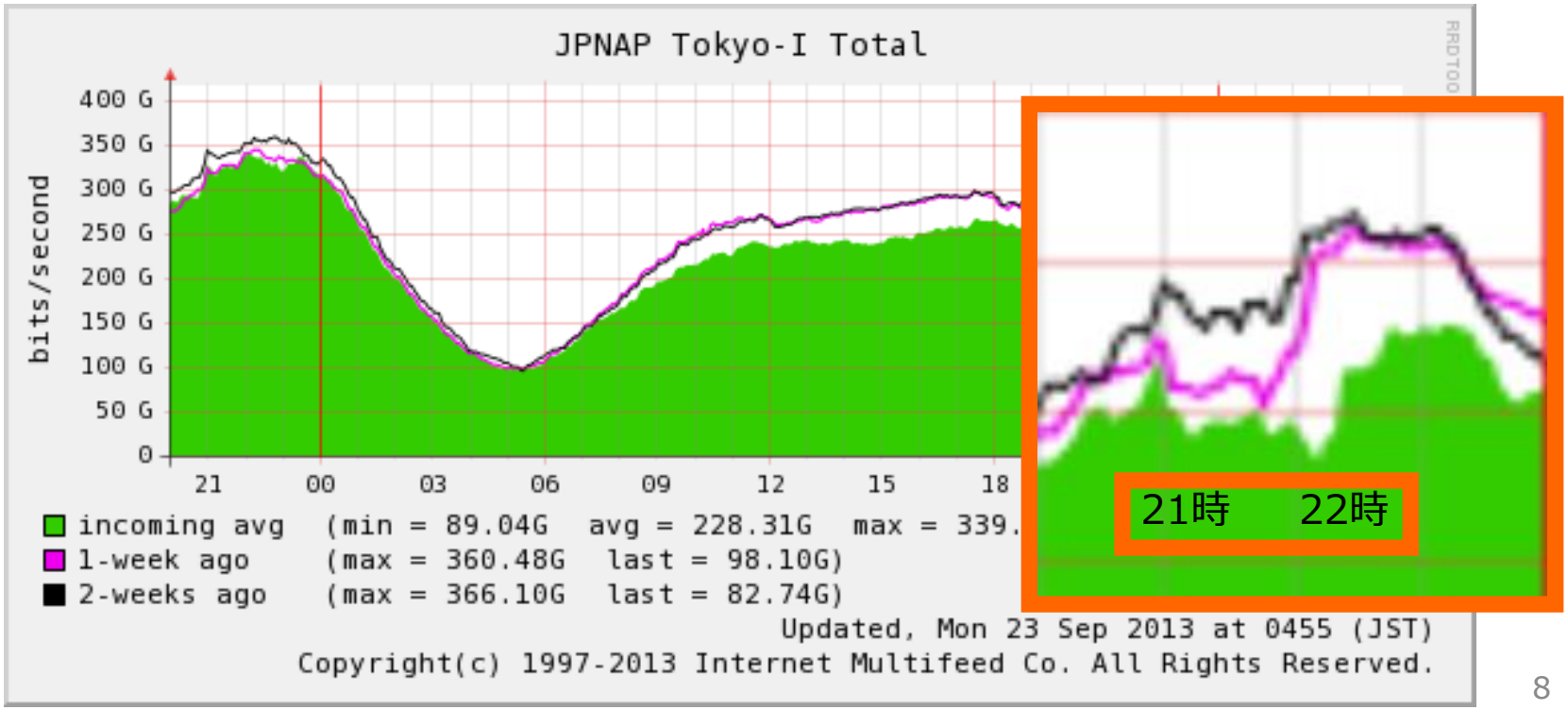


AMS-IX(Europe)の
1日のトラフィック推移

9/22 Sun. 21:00-22:19



- 放映時間：21:00 – 22:20 (通常は22:00まで)
- 倍返し効果？　によるトラフィック減少を観測
  - 毎週日曜夜のトラフィックが減少（最終回がMAX）



9/22 Sun. 21:00-22:19 の1週間後

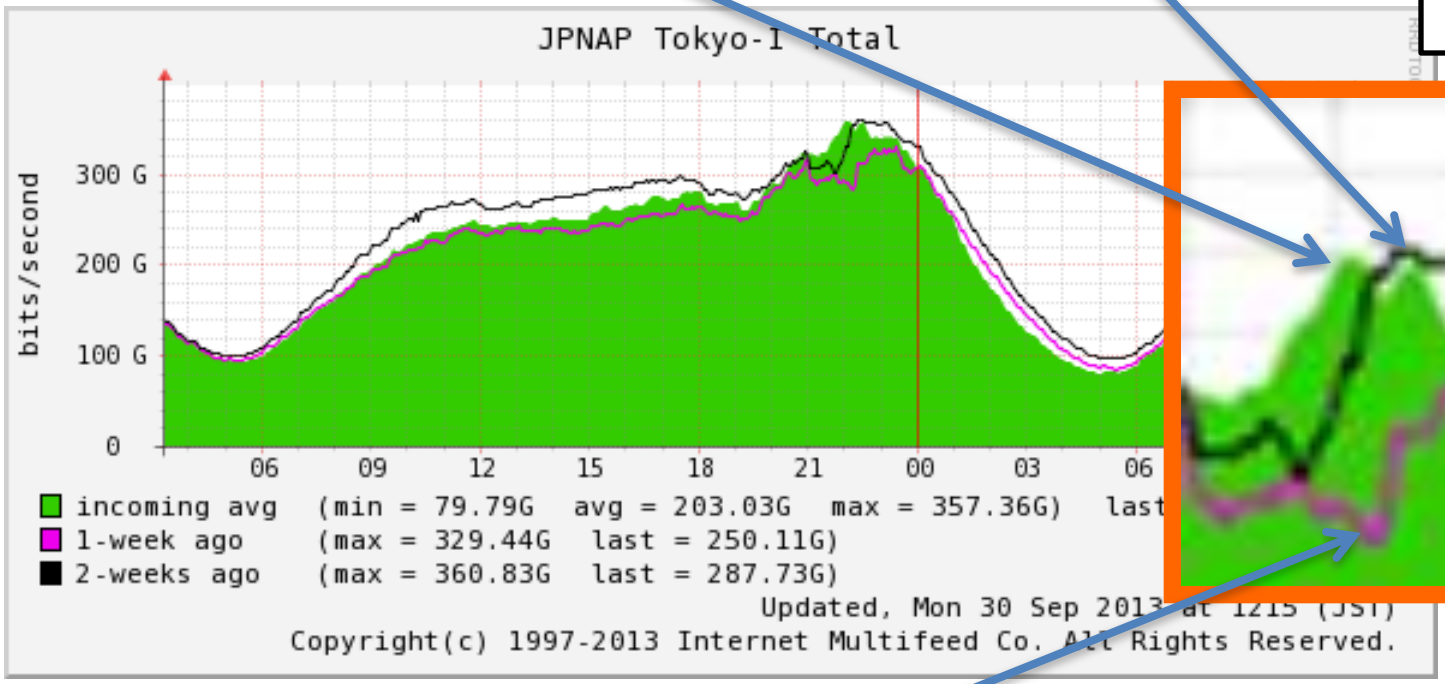
29日（22:00ごろピーク）

15日（22:30ごろピーク）

1週後

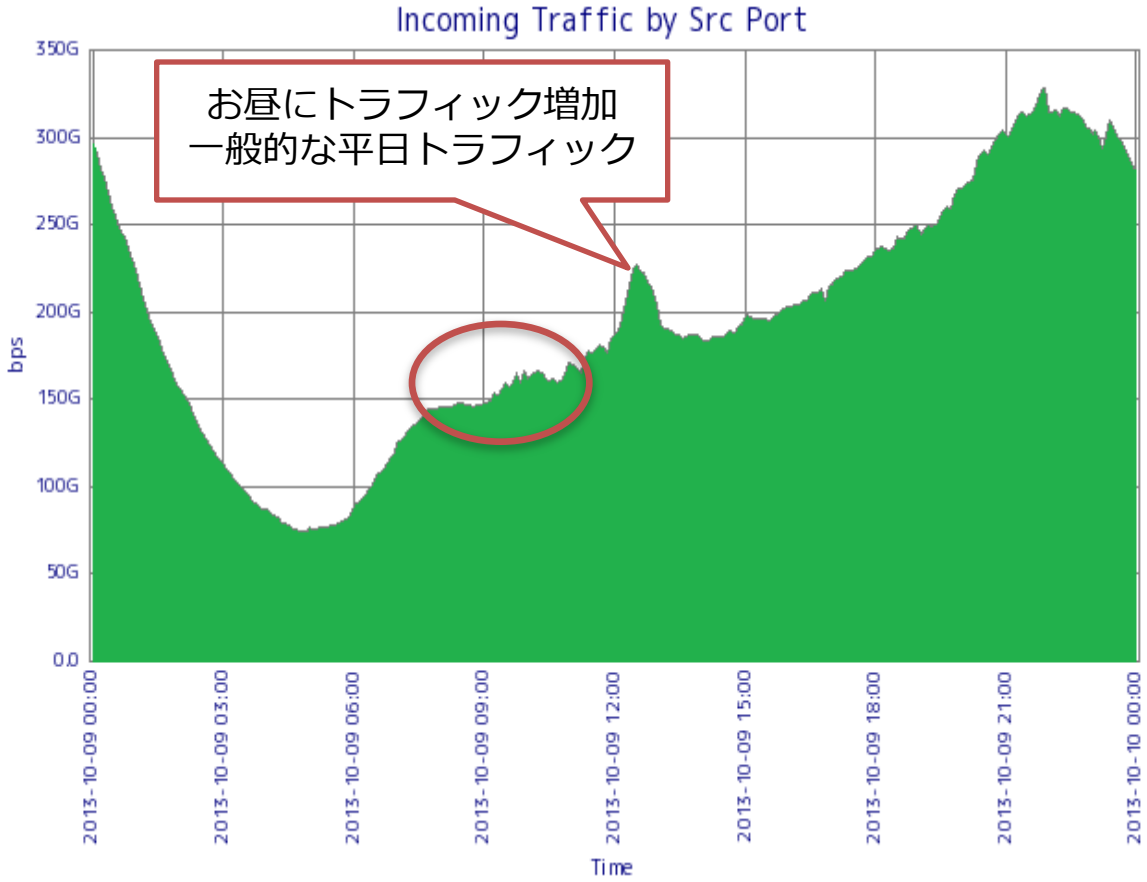
最終回

2週前



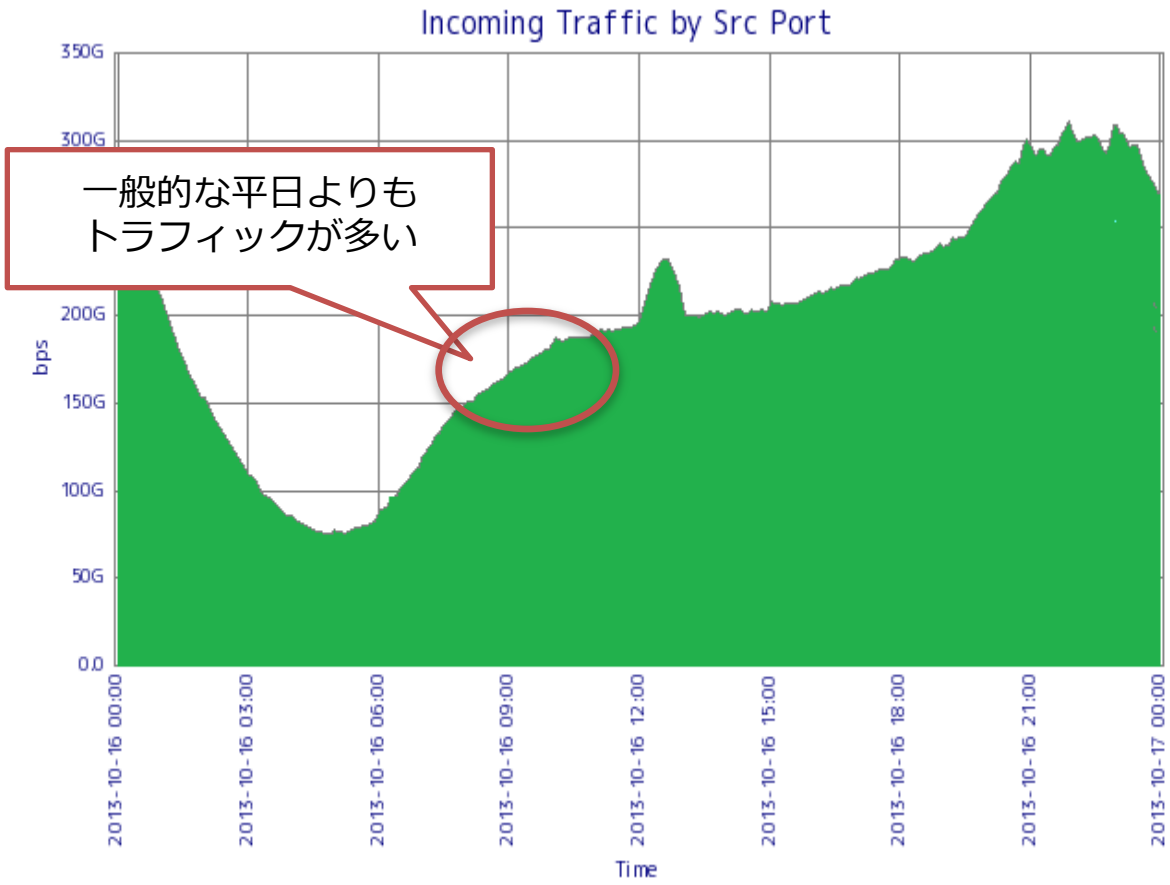
22日（22:20ごろ底）

10/9 Wed. 平日トラフィック(台風の1週間前)



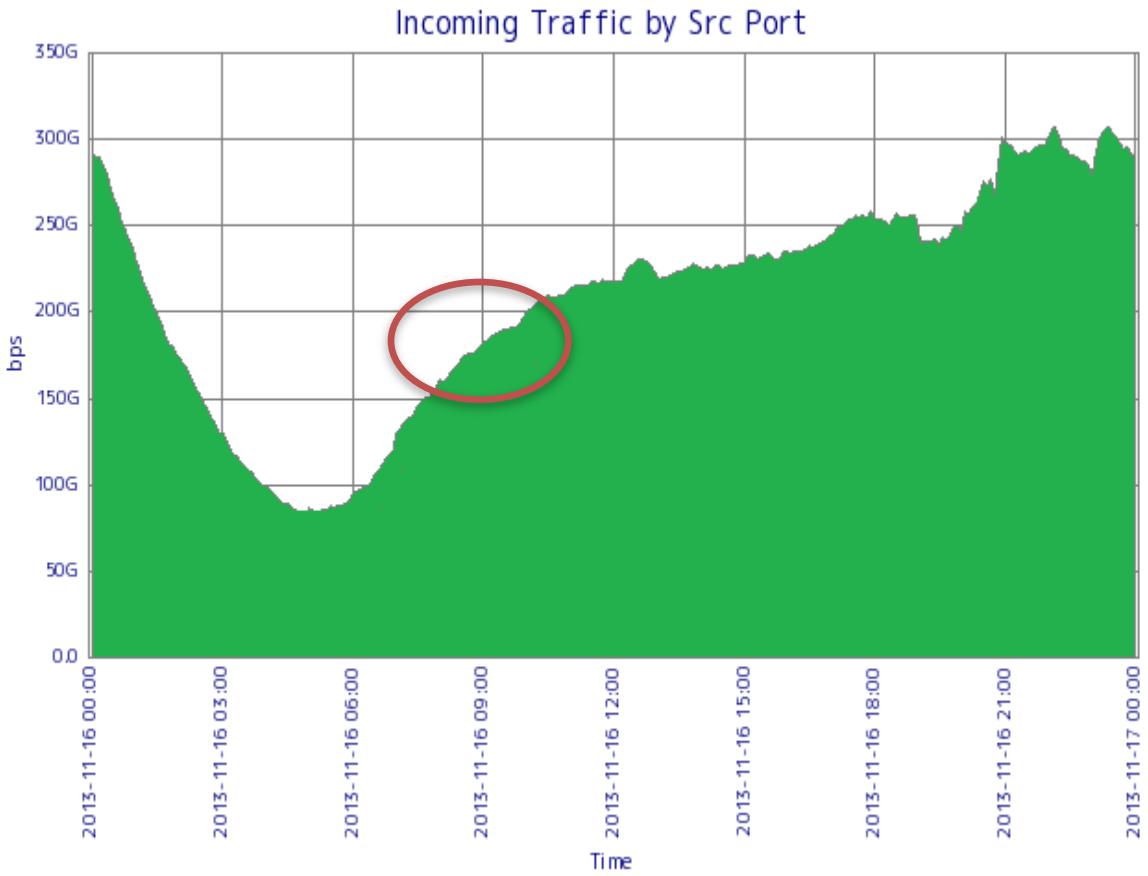
JPNAPのトラフィック

10/16 Wed. 台風当日



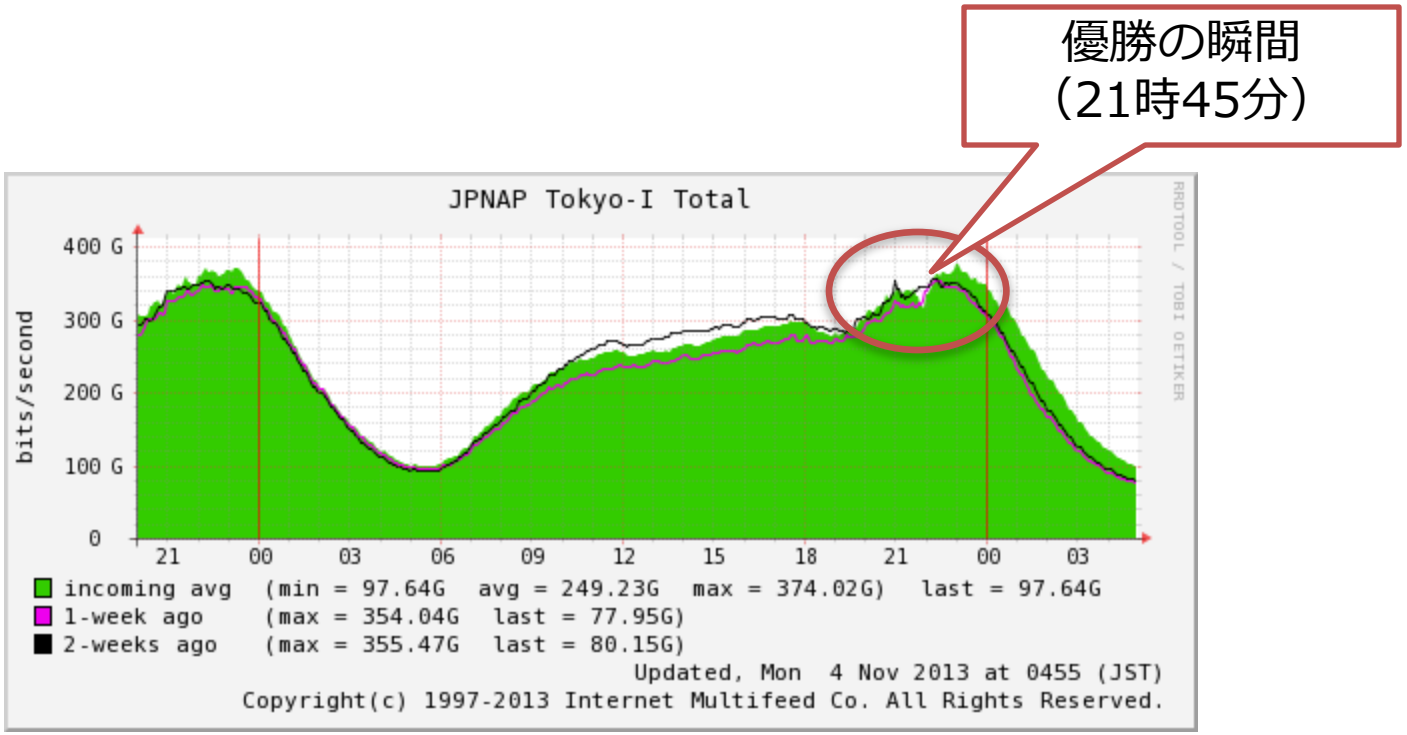
JPNAPのトラフィック

11/16 Sat. 休日トラフィック



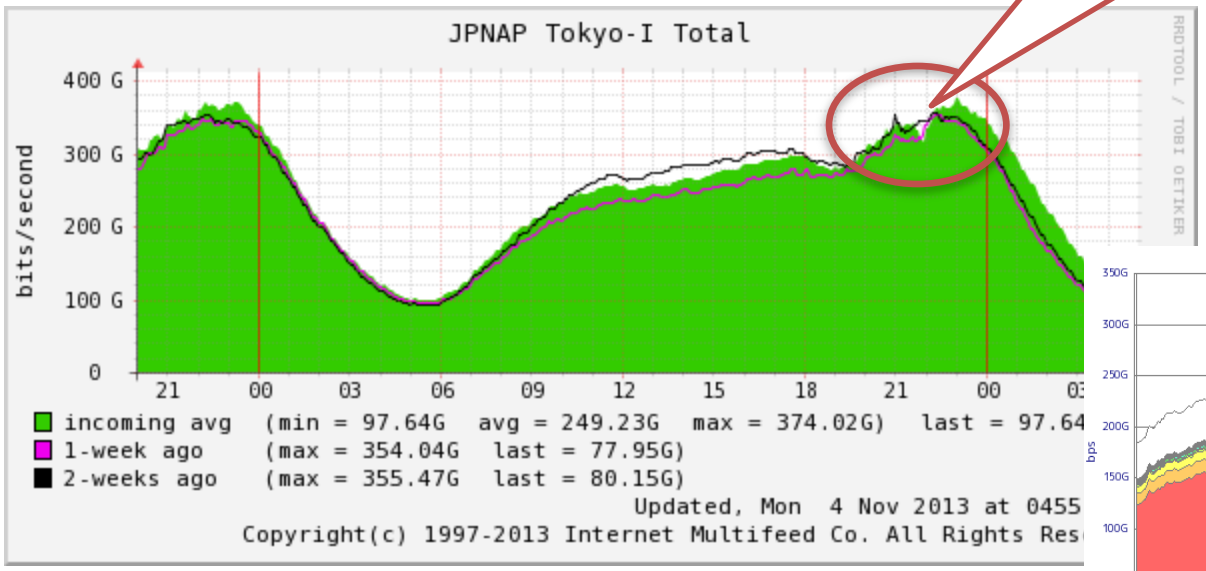
JPNAPのトラフィック

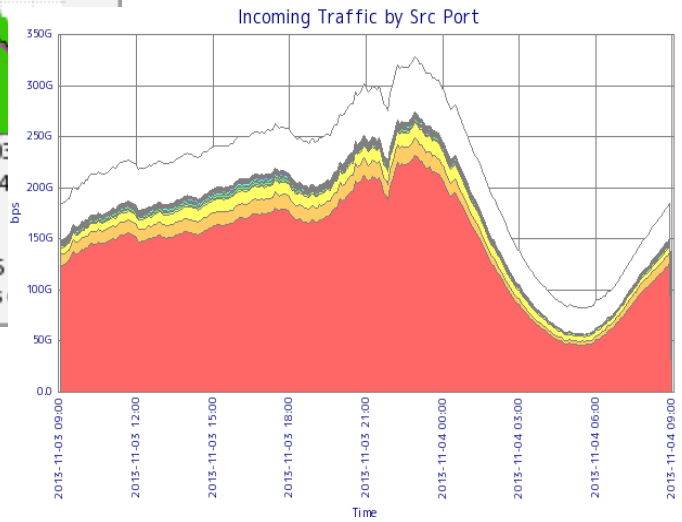
11/3 Sun. 21:45 勝敗決定の瞬間



11/3 Sun. 21:45 勝敗決定の瞬間

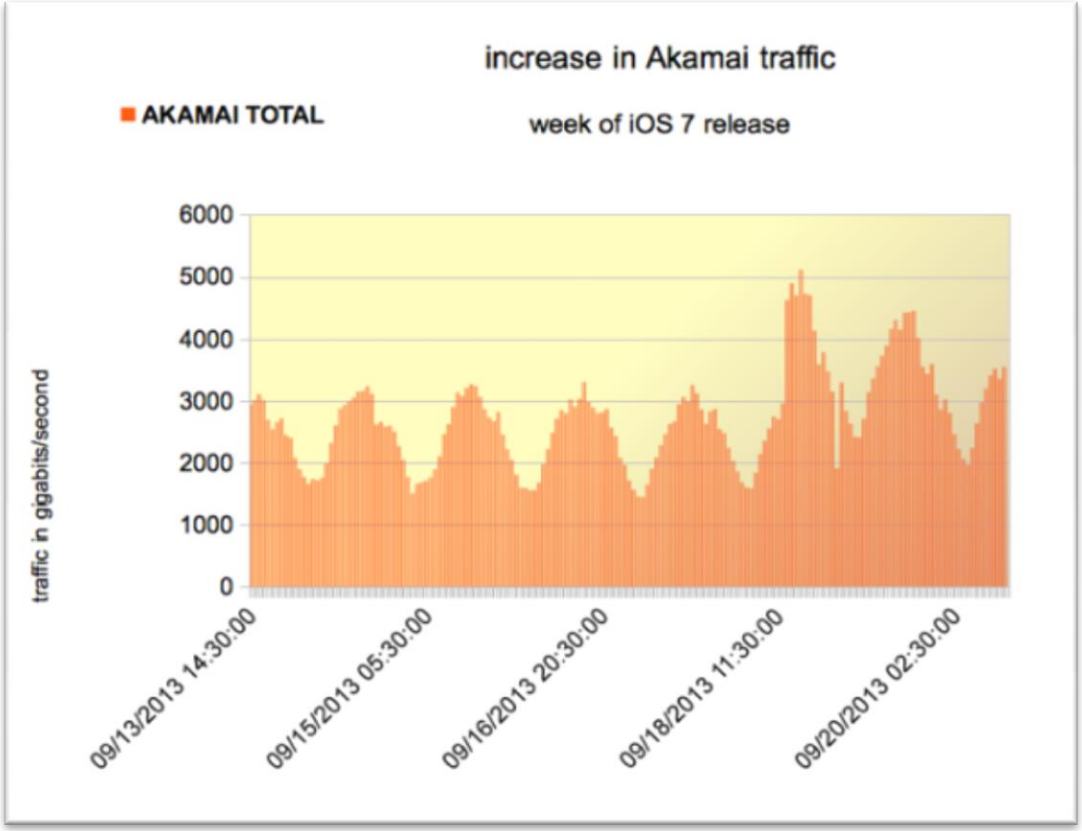
優勝の瞬間
（21時45分）





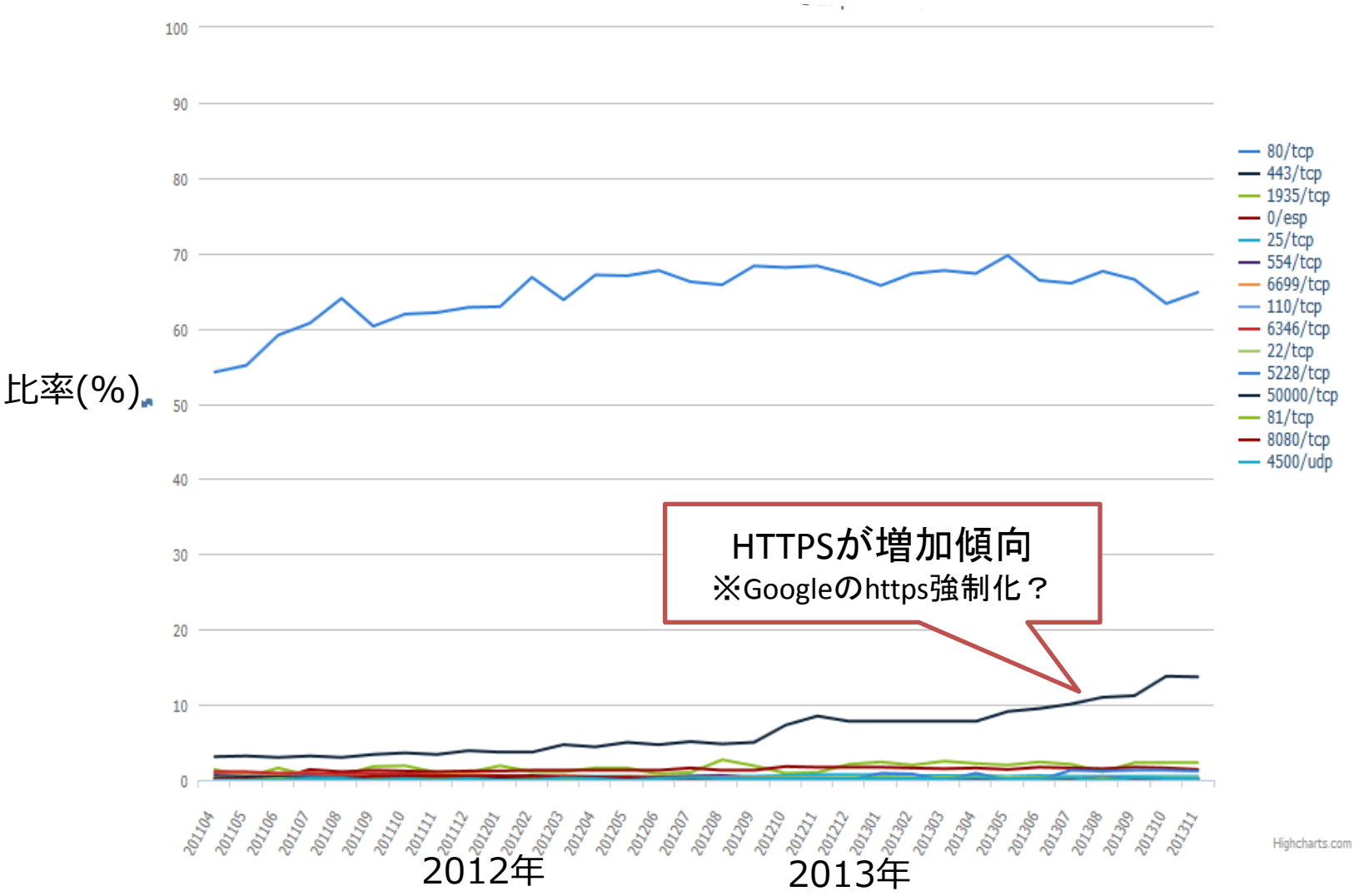
9/18 Wed. IOS7 download

- 日本時間の9/18早朝より急激なトラフィック変化
  - Akamaiのトラフィックは5Tbpsへ

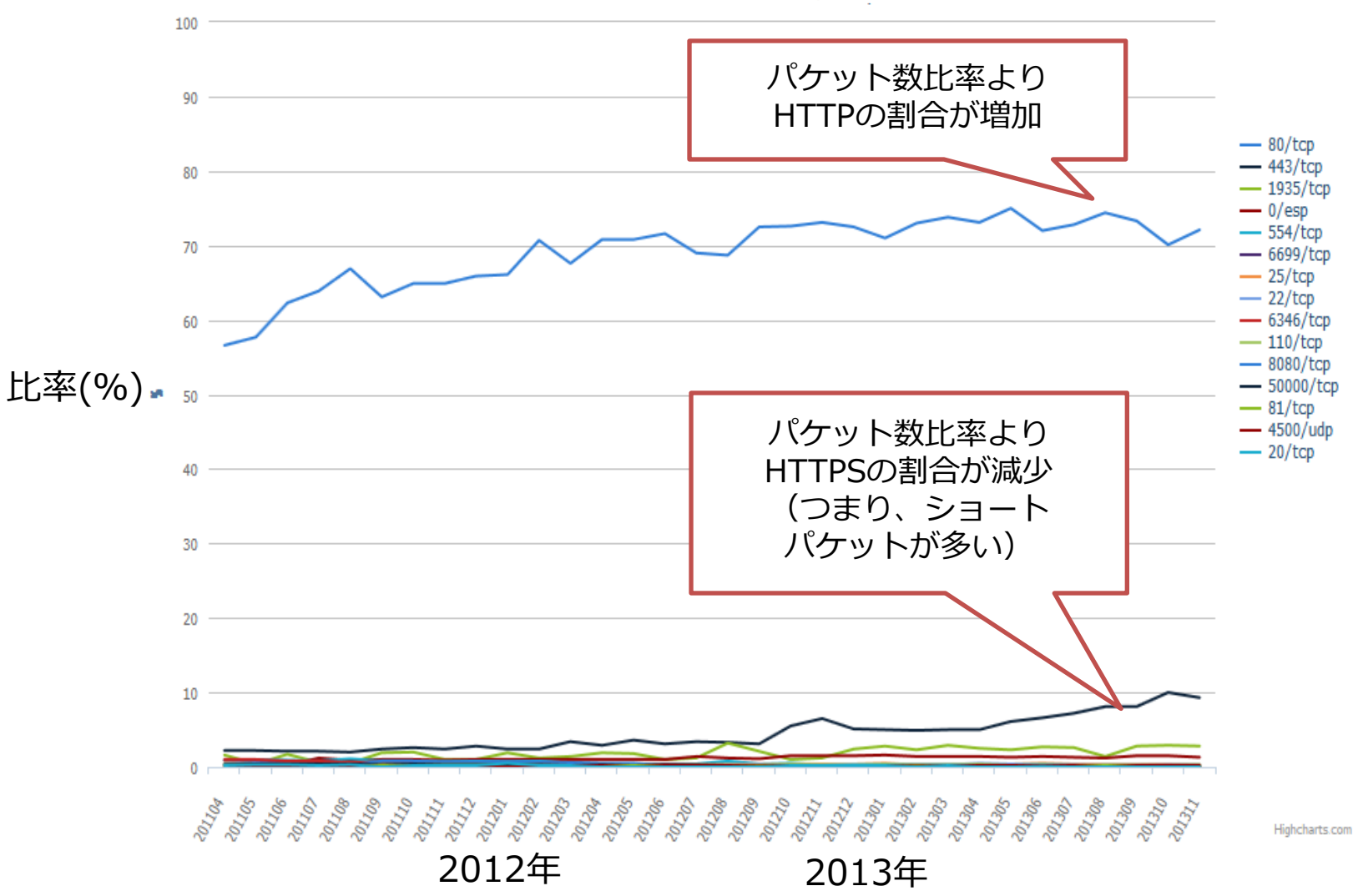


http://www.arbornetworks.com/asert/2013/09/the-apple-wow-effect/

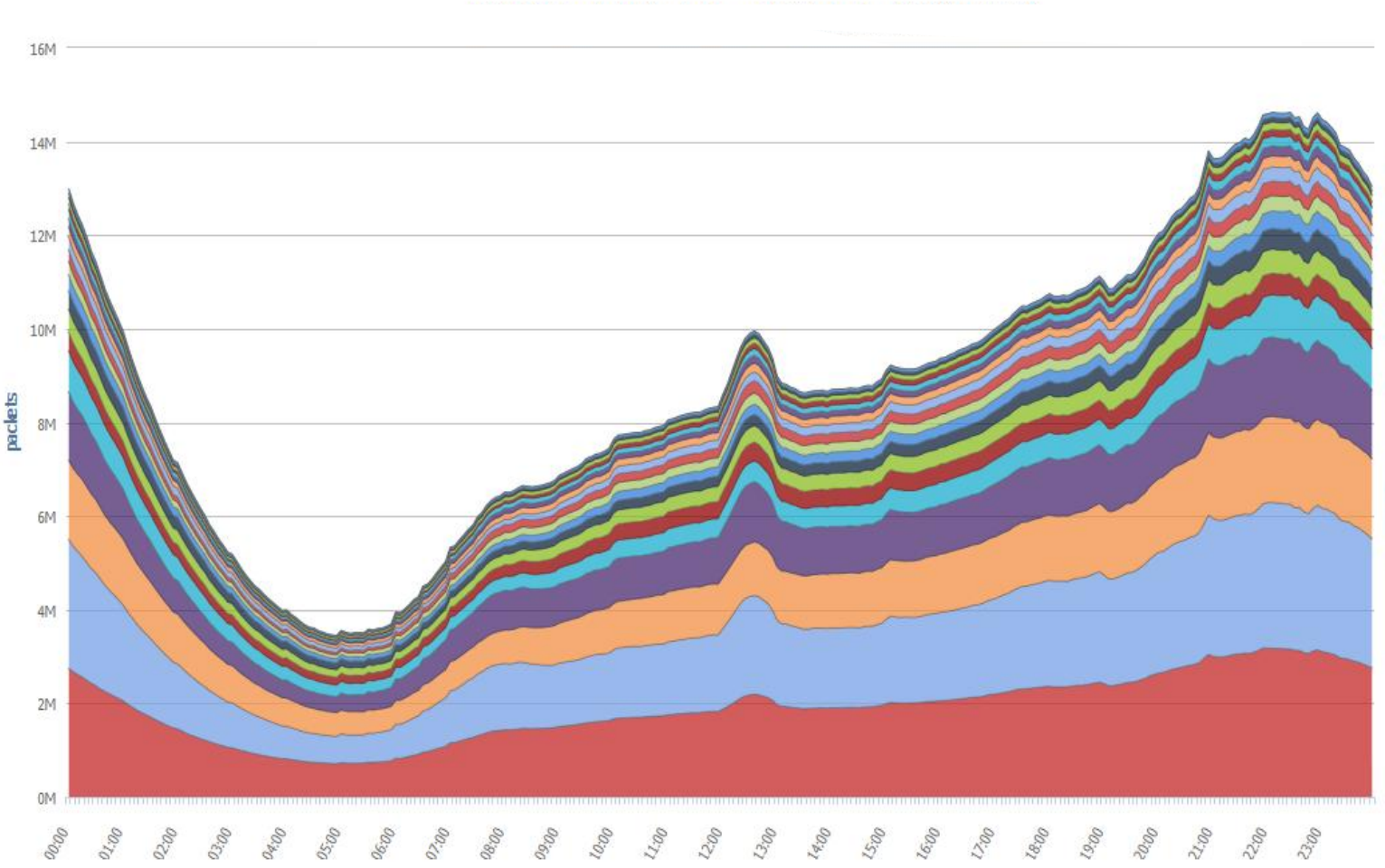
プロトコル比率の推移（パケット数比率）



プロトコル比率の推移（バイト数比率）



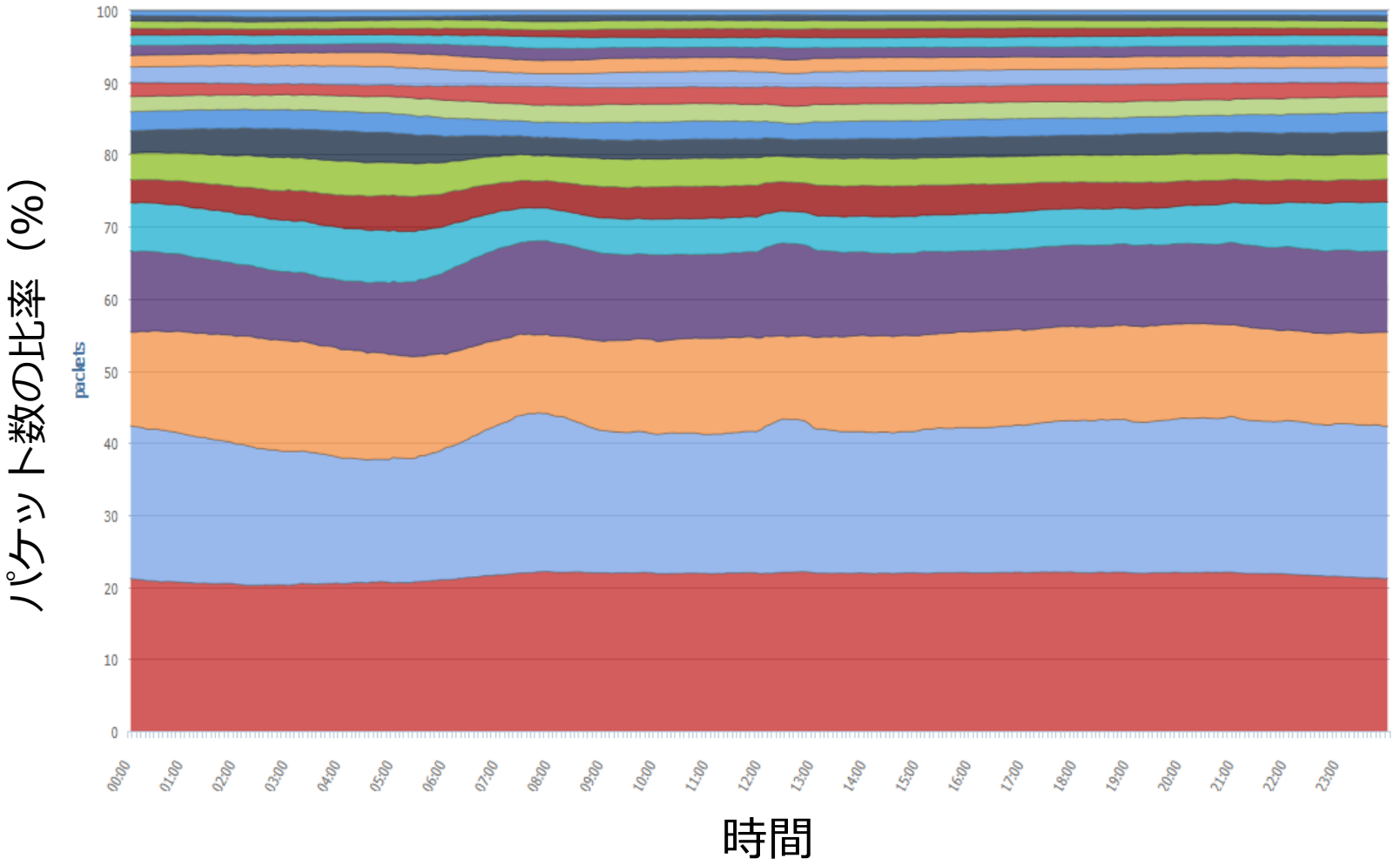
パケットサイズの分布（一週間平均）



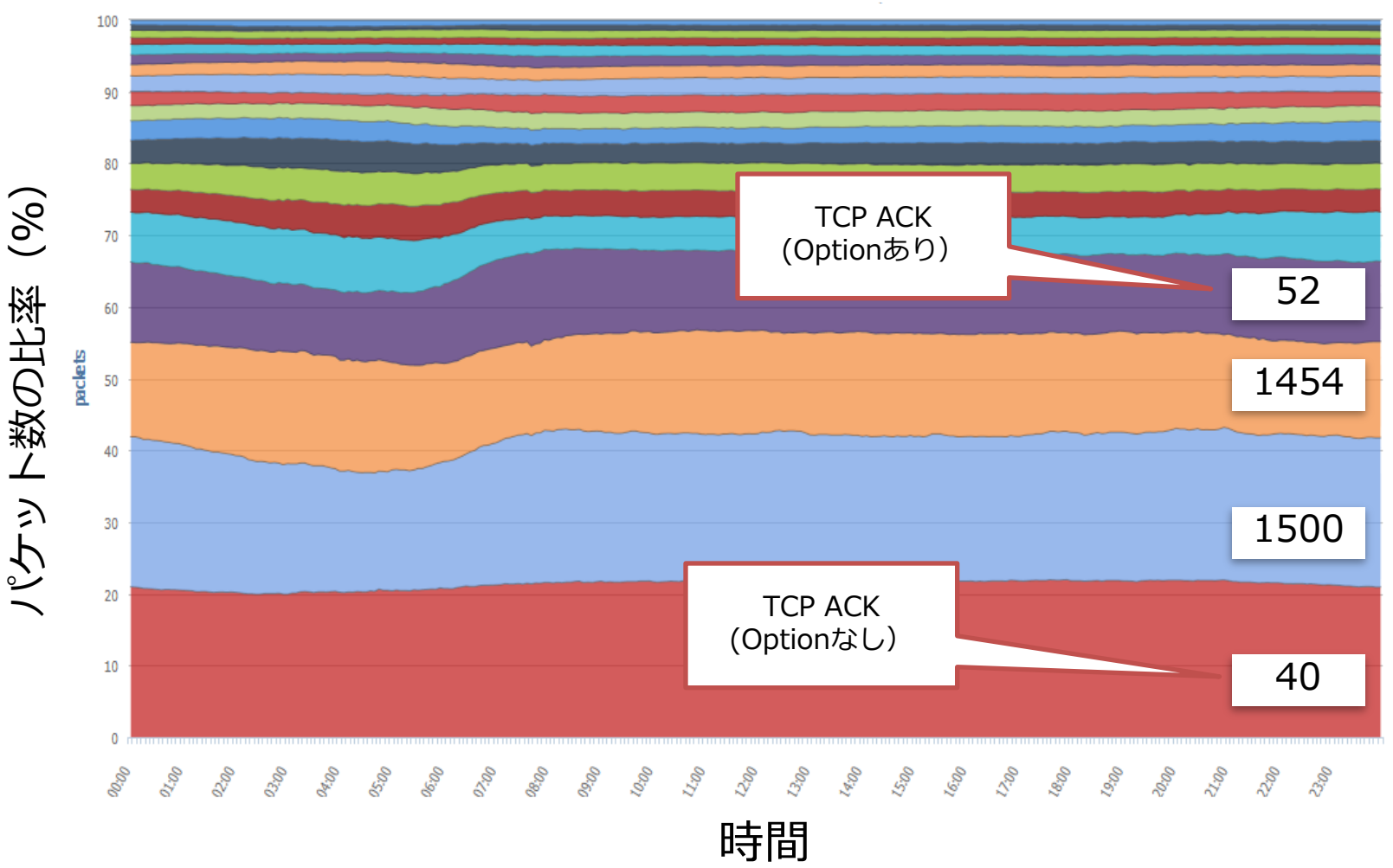
パケット数

時間

パケットサイズの分布（一週間平均）

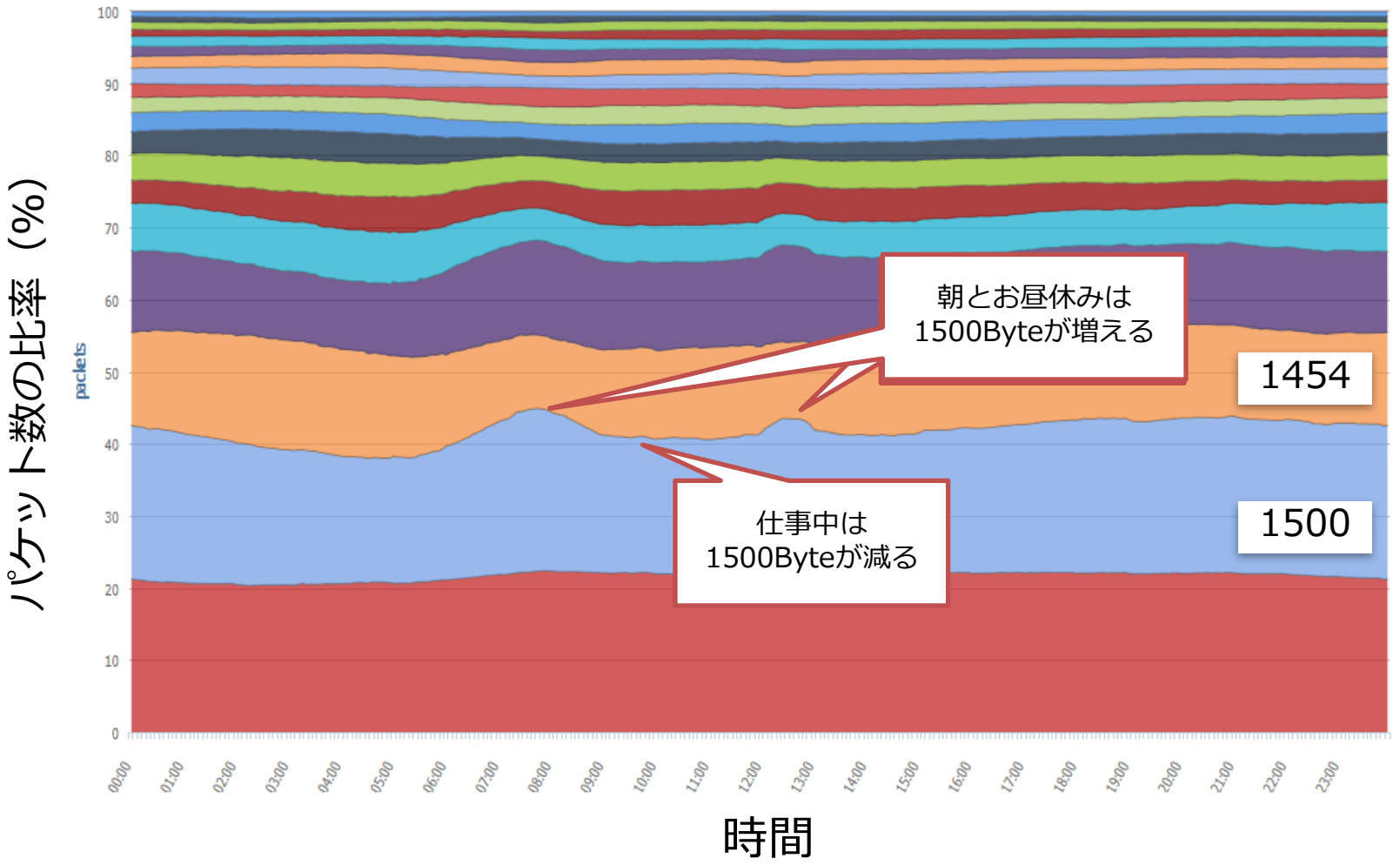


パケットサイズの分布（休日）



パケットサイズの分布（平日）

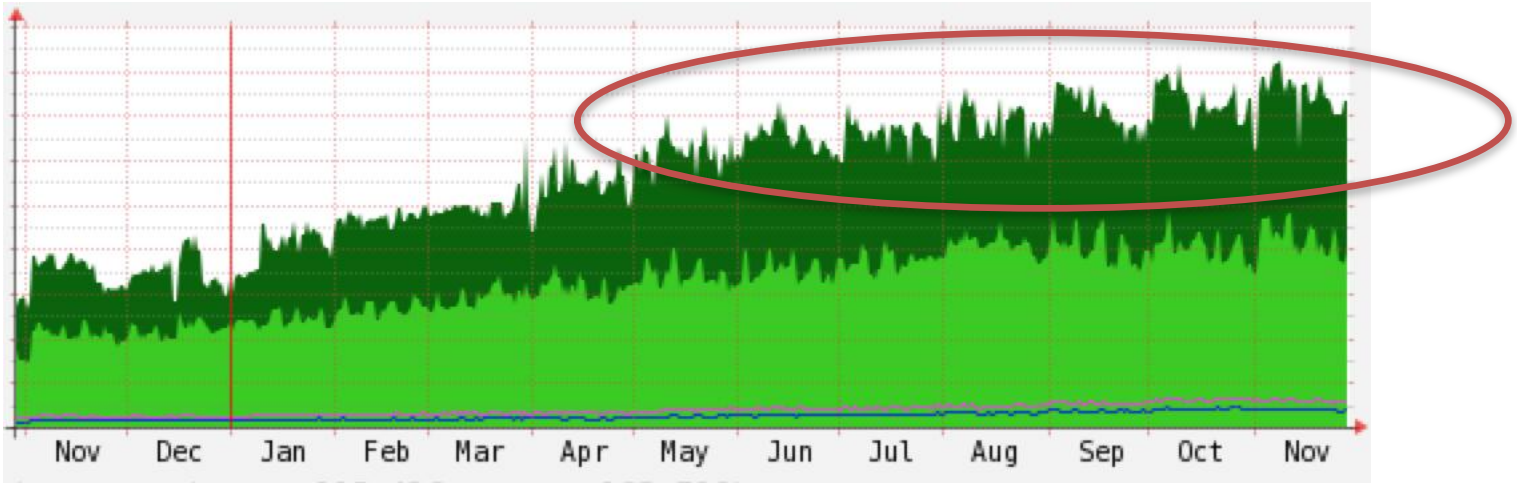
モバイルからの1500byteのトラフィックが影響している



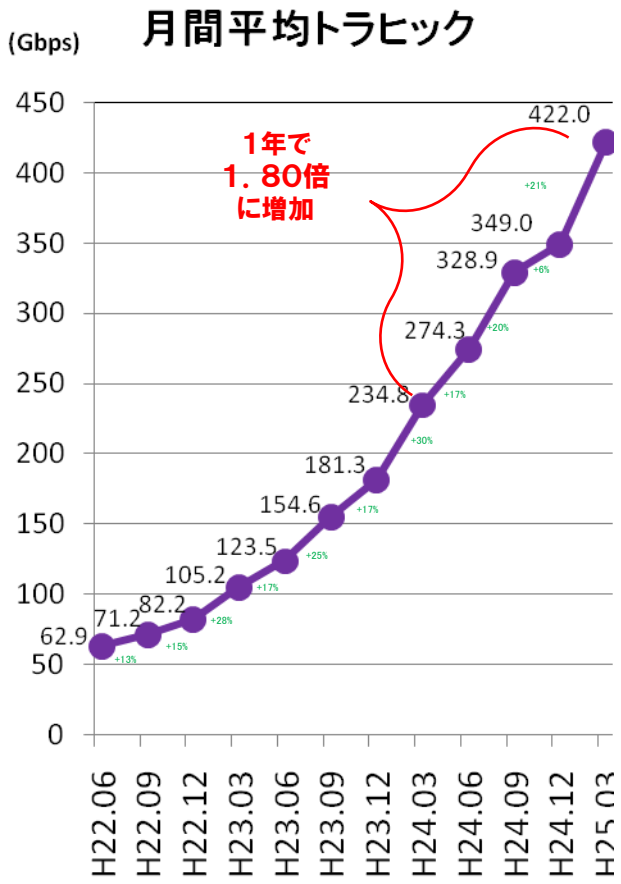
その他トラフィック傾向

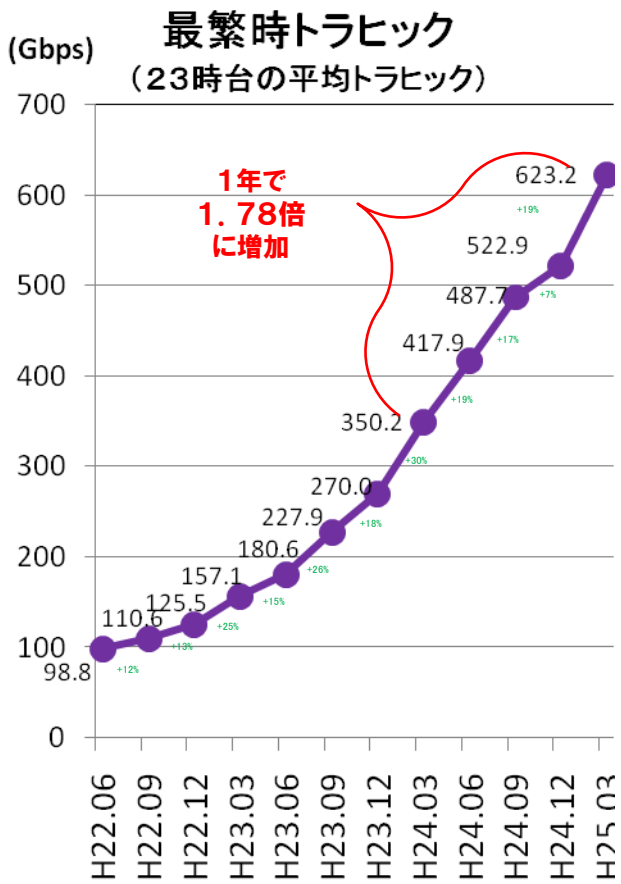
- アクセス回線は高速化しているが、それに比例してトラフィックがのびているわけでもない。
- 将来各家庭のトラフィックが急激に増加する可能性あり
  - 2020年東京オリンピックに向けた仕掛けとか
- 国内と国際のトラフィックの把握が難しい
- 1つのIPv4アドレスに占めるトラフィックが増加傾向
  - 単純に /userのトラフィック増
  - アドレス共有
    - 位置の特定が困難

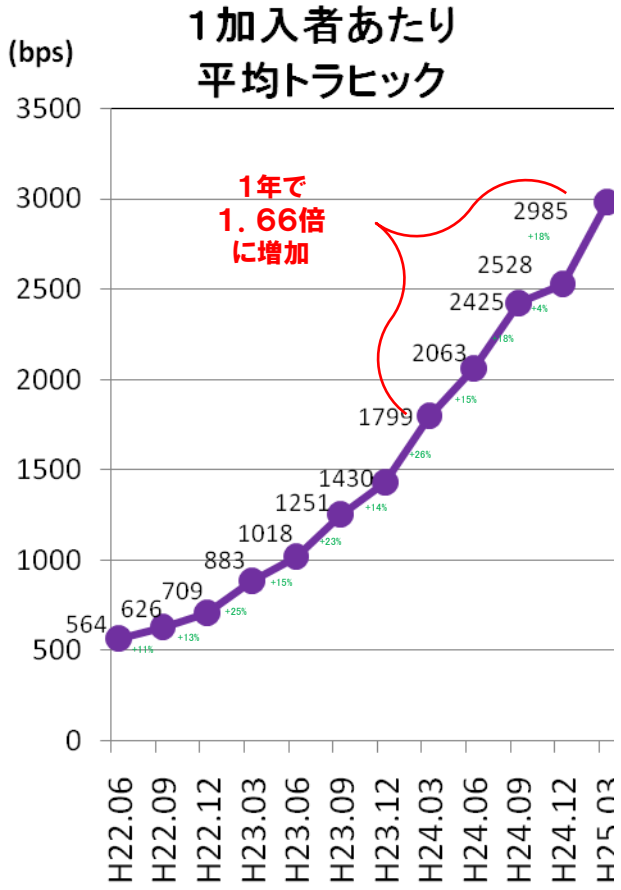
JPNAPのとあるバックボーン回線



移動通信トラフィックの推移



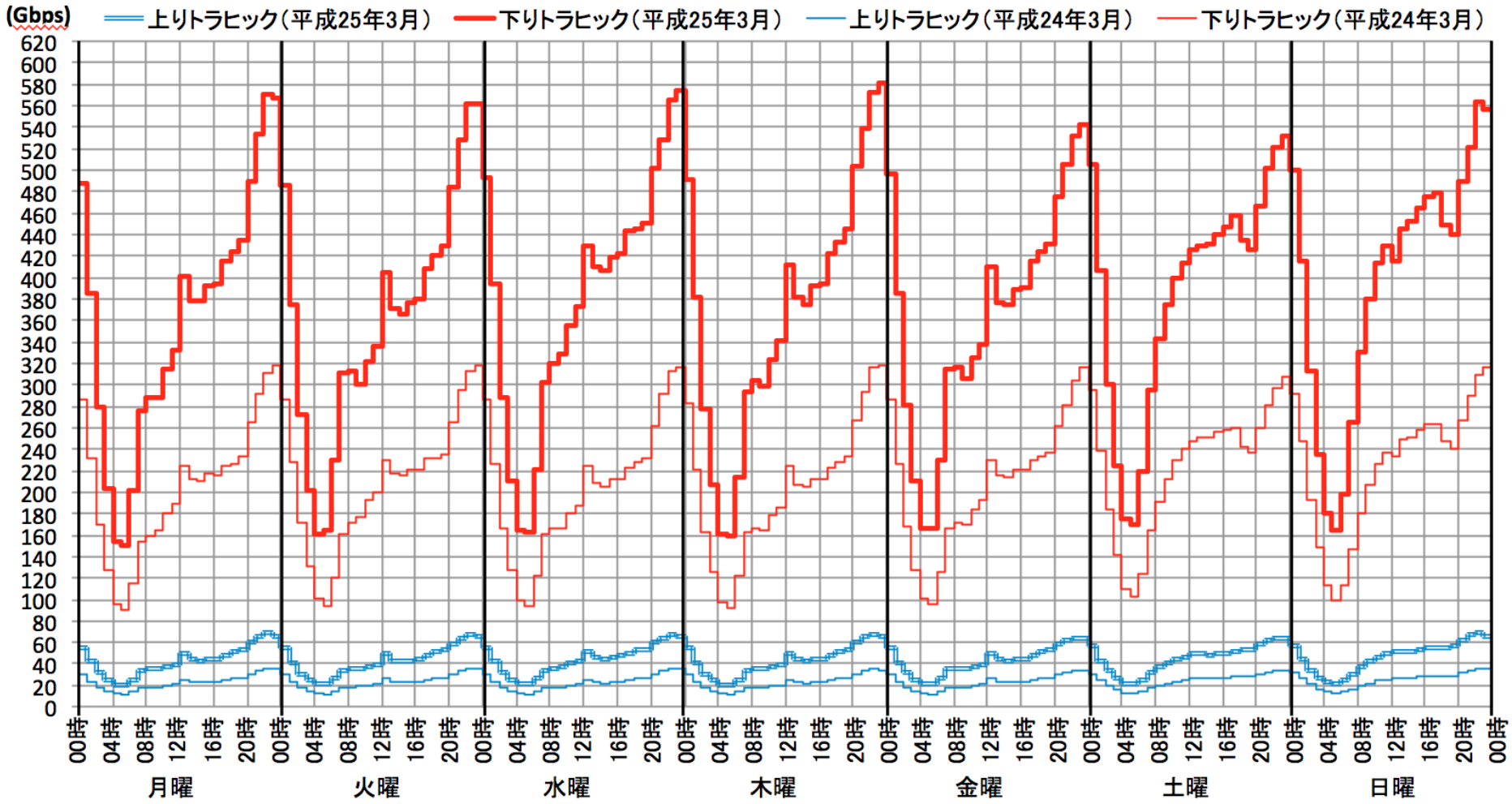




〇直近四半期で伸びが鈍くなったものの、年間約2倍のペースで移動通信トラヒックは増加している。
（各社のスマートフォン利用者数の増加や、動画等の大容量コンテンツの利用増加等が主要因と推測される。）

出典：総務省 我が国の移動通信トラヒックの現状

移動通信トラフィックの推移



出典：総務省 我が国の移動通信トラヒックの現状

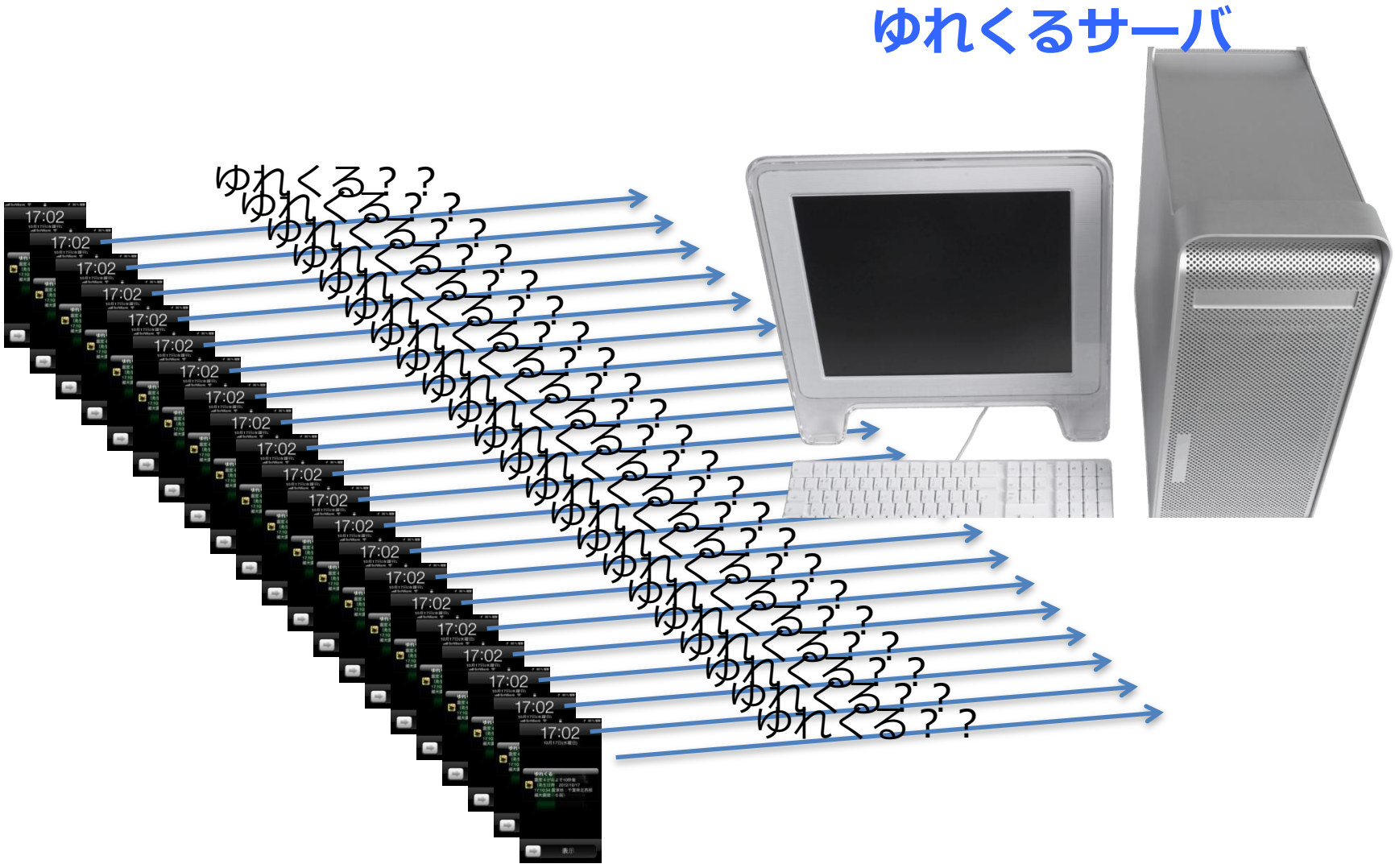
モバイルトラフィック

- これまでと気にしなければいけない所が違う
- bpsよりpps
  - 1パケットのサイズが小さいものが多い
    - Keepalive packetのようなもの等
  - 帯域には余裕があるのにパケットをさばけないことも起きる
  - スマートフォンのショートパケットの多さはやはり異常な程
  - 常に電源が入っているため何かしらパケットを出している
  - アプリ怖い

ゆれくるアプリ

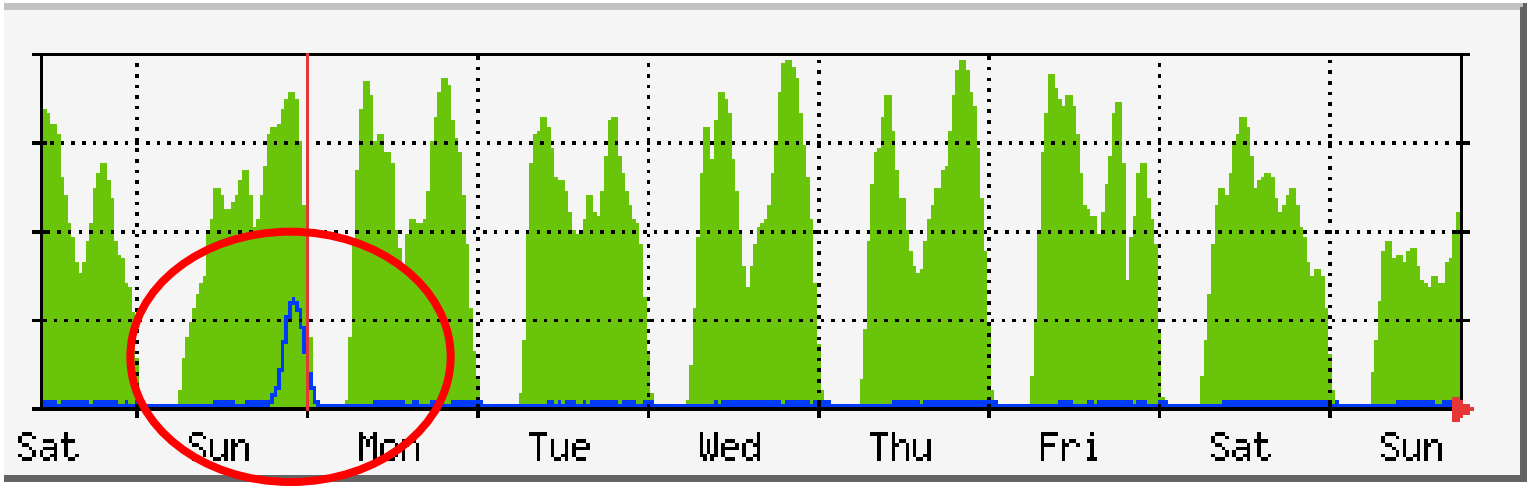

SoftBank
36 %
17:02
10月17日(水曜日)
ゆれくる
震度４がおよそ10秒後
（発生日時：2012/10/17
17:10:34 震源地：千葉県北西部
最大震度：６弱）
表示

ゆれくるアプリ



某高速鉄道のモバイル

- 電車が遅れたり、公共交通機関に何か起きると、バースト的にアクセスユーザ数とトラフィックが増加する



現状と今後の課題

- とにかく増強
  - モバイルキャリアやISPの涙ぐましい努力は続いています
- 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
  - 従来トラフィックが減っていたタイミングでトラフィックが急増する可能性が高い
  - うまくコントロールできる仕組みや東西分散などを模索中

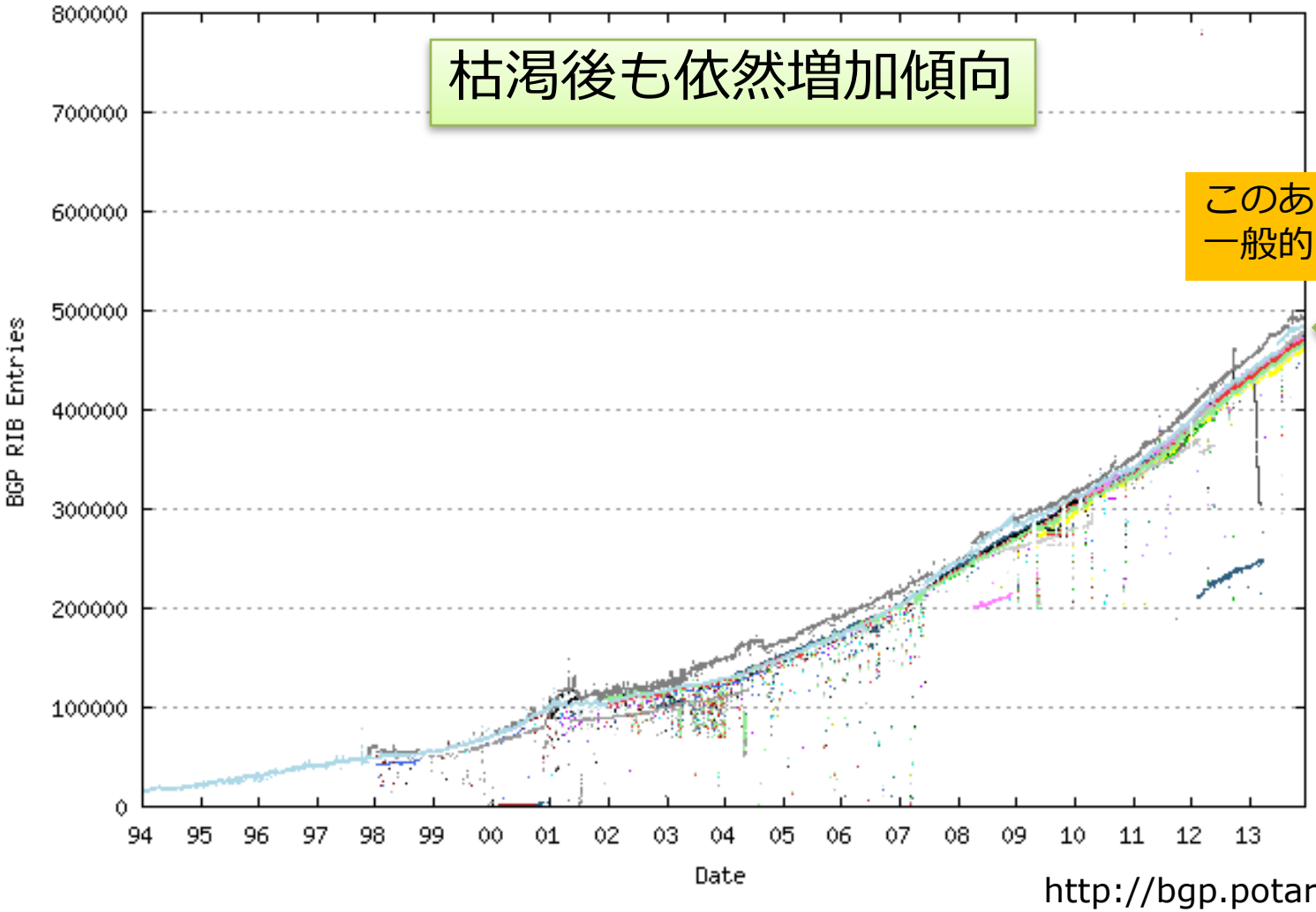
内容

- 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
- 日本や世界のIX動向
- まとめ

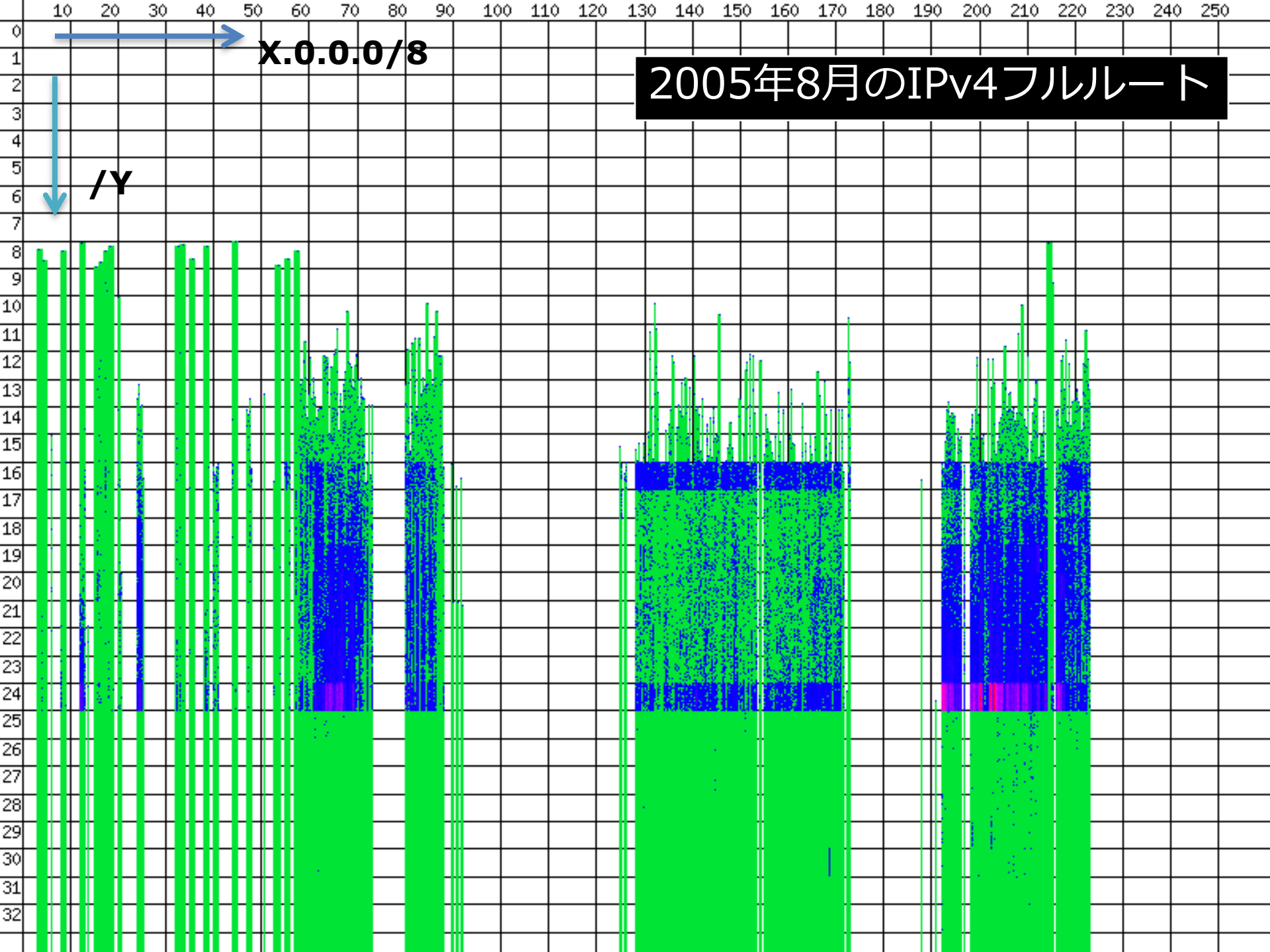
ルーティング動向

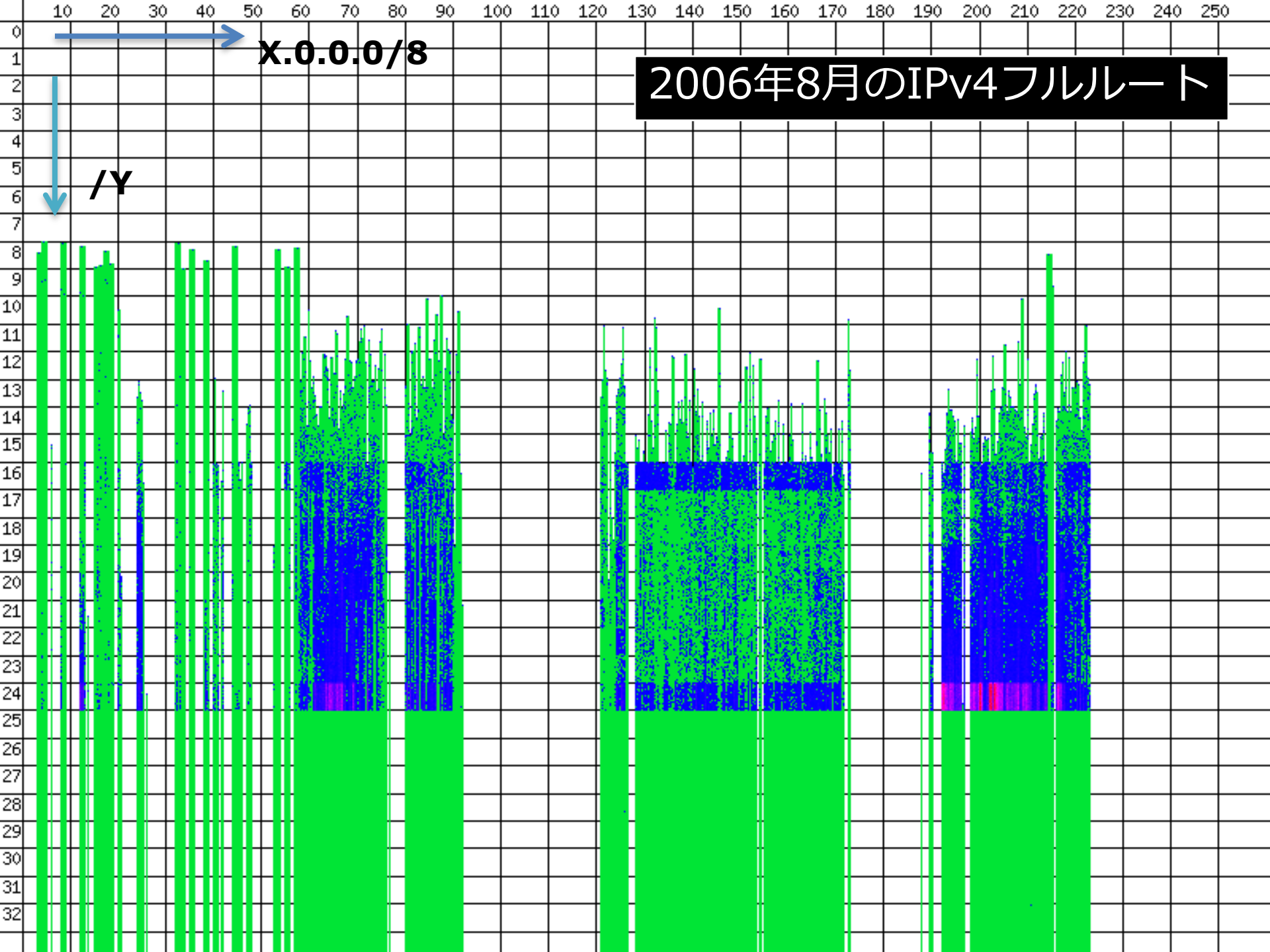
- IPv4経路が47万～48万に到達
  - 年増加率は約1.1倍で引き続き枯渇後も増加
  - /24は依然全体の約半分、最後の/8で急増傾向
- IPv6経路の増加・本格的なルーティングが開始
  - 1万経路の大台を突破し1.5万経路
- AS番号の枯渇対応 ⇒ 4byteASへ移行
  - ここ最近は大きな問題は発生していない
  - 上位ISPが4byteに未対応のところが依然存在
⇒日本国内にも複数ある

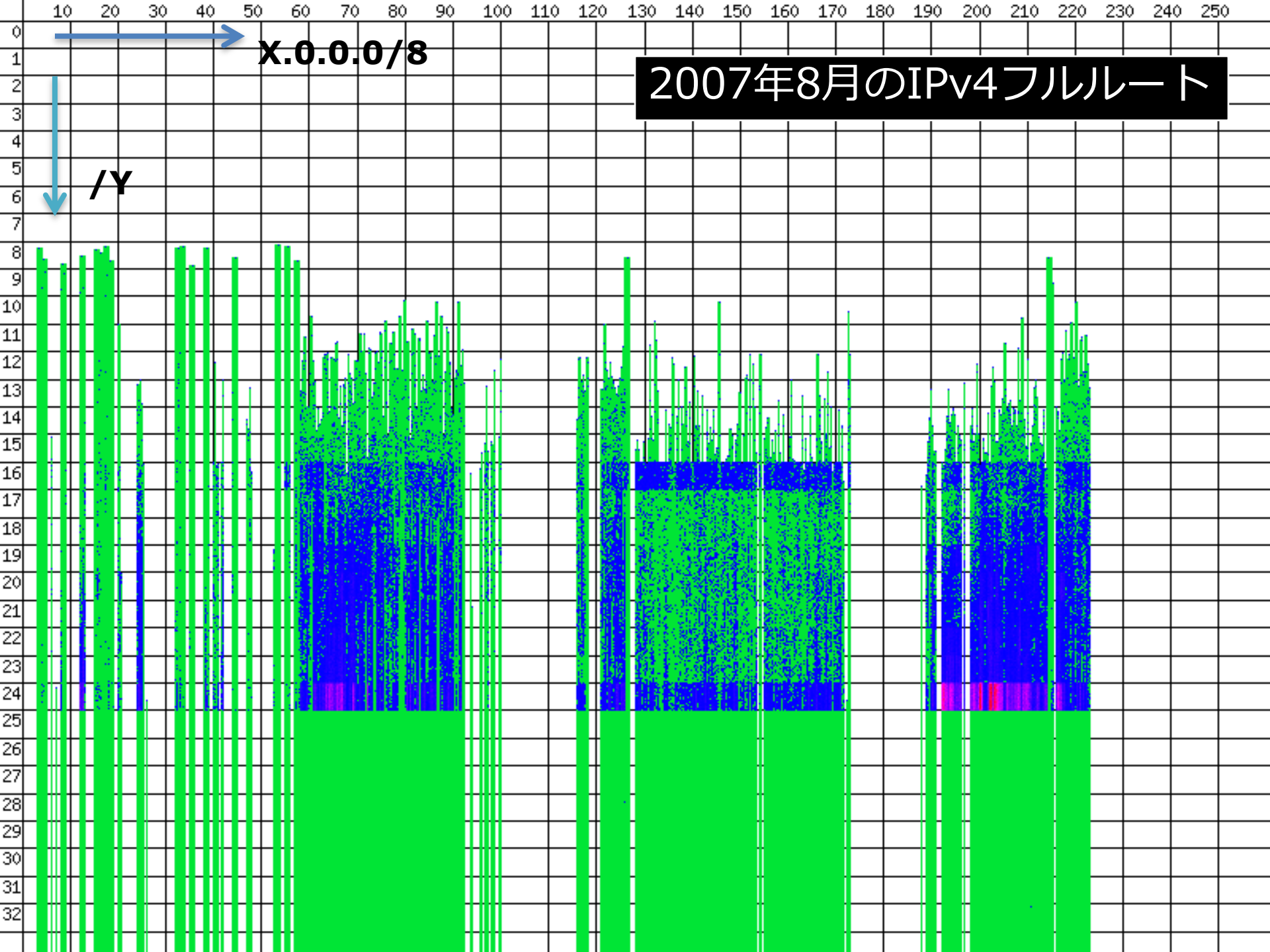
IPv4経路数の推移

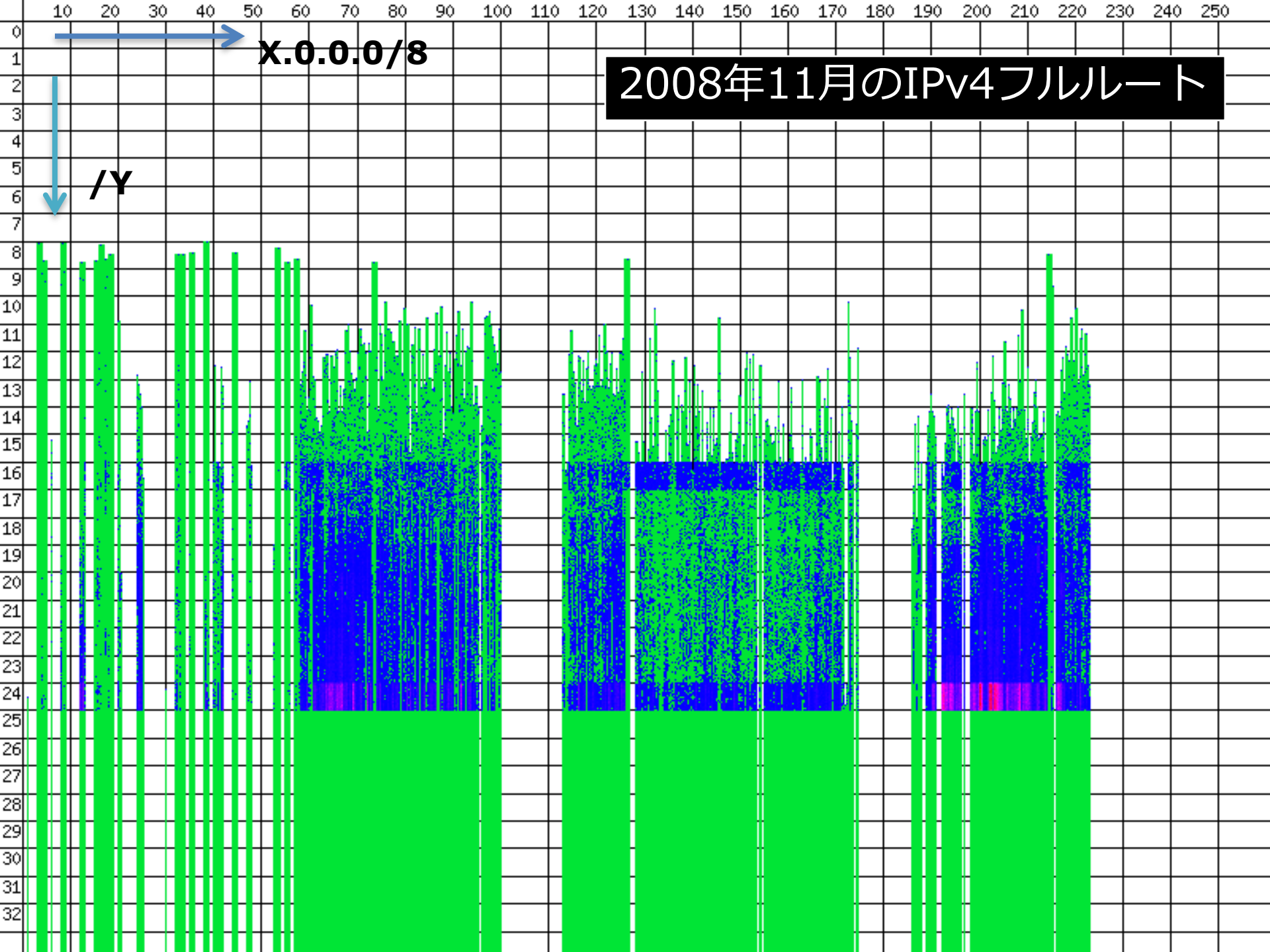


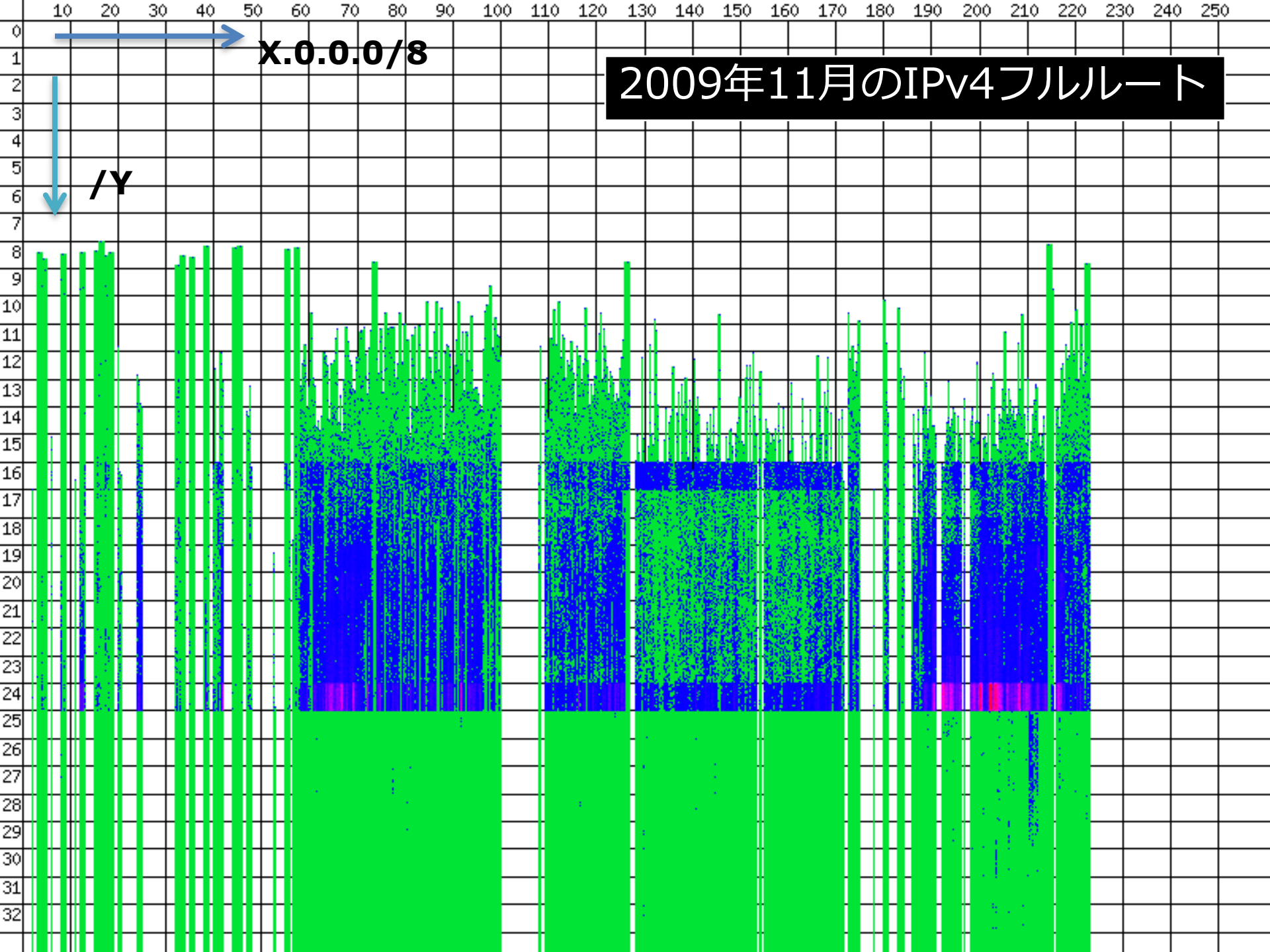
http://bgp.potaroo.net/

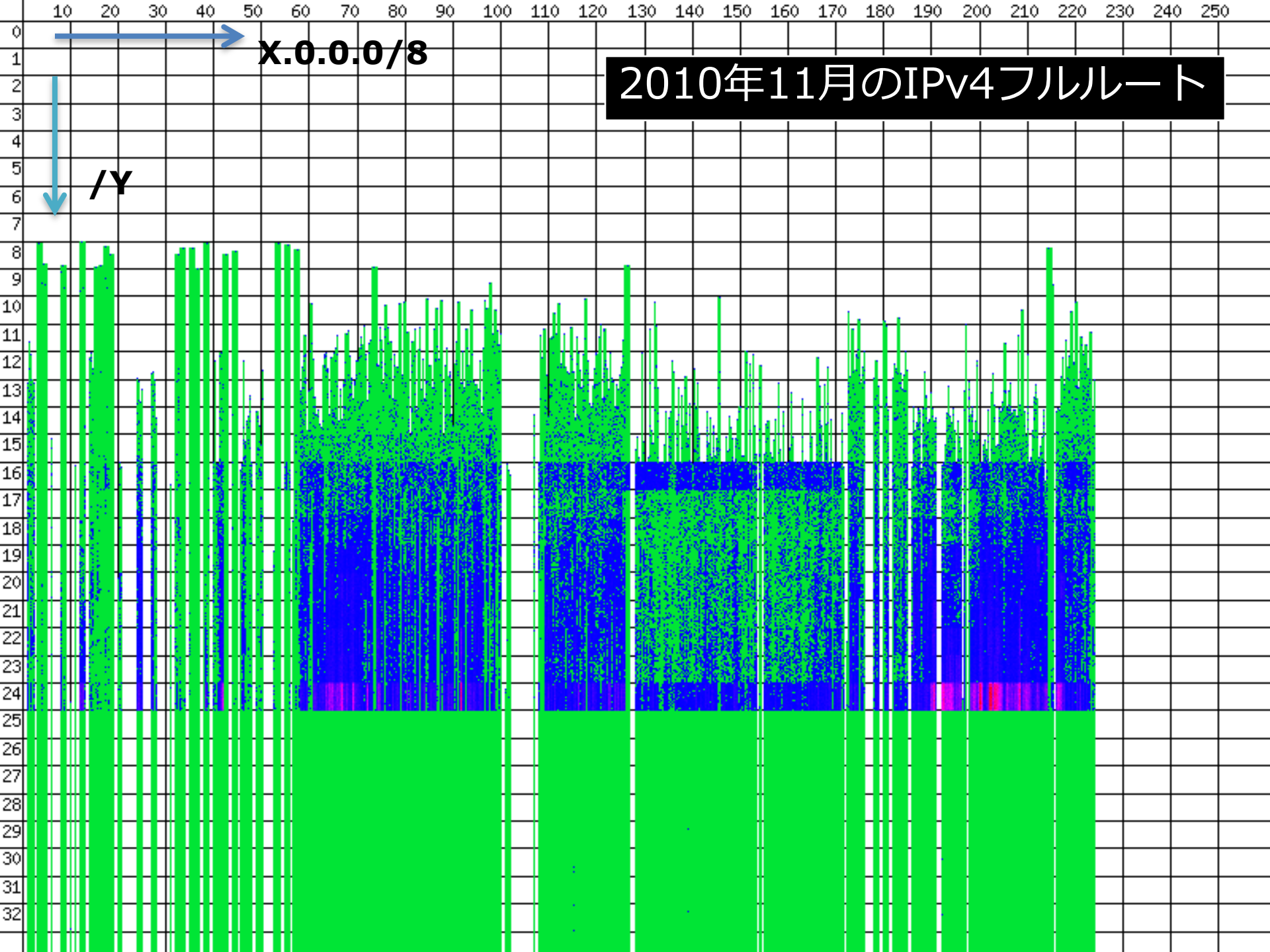

10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
x.0.0.0/8
/Y
2005年8月のIPv4フルルート

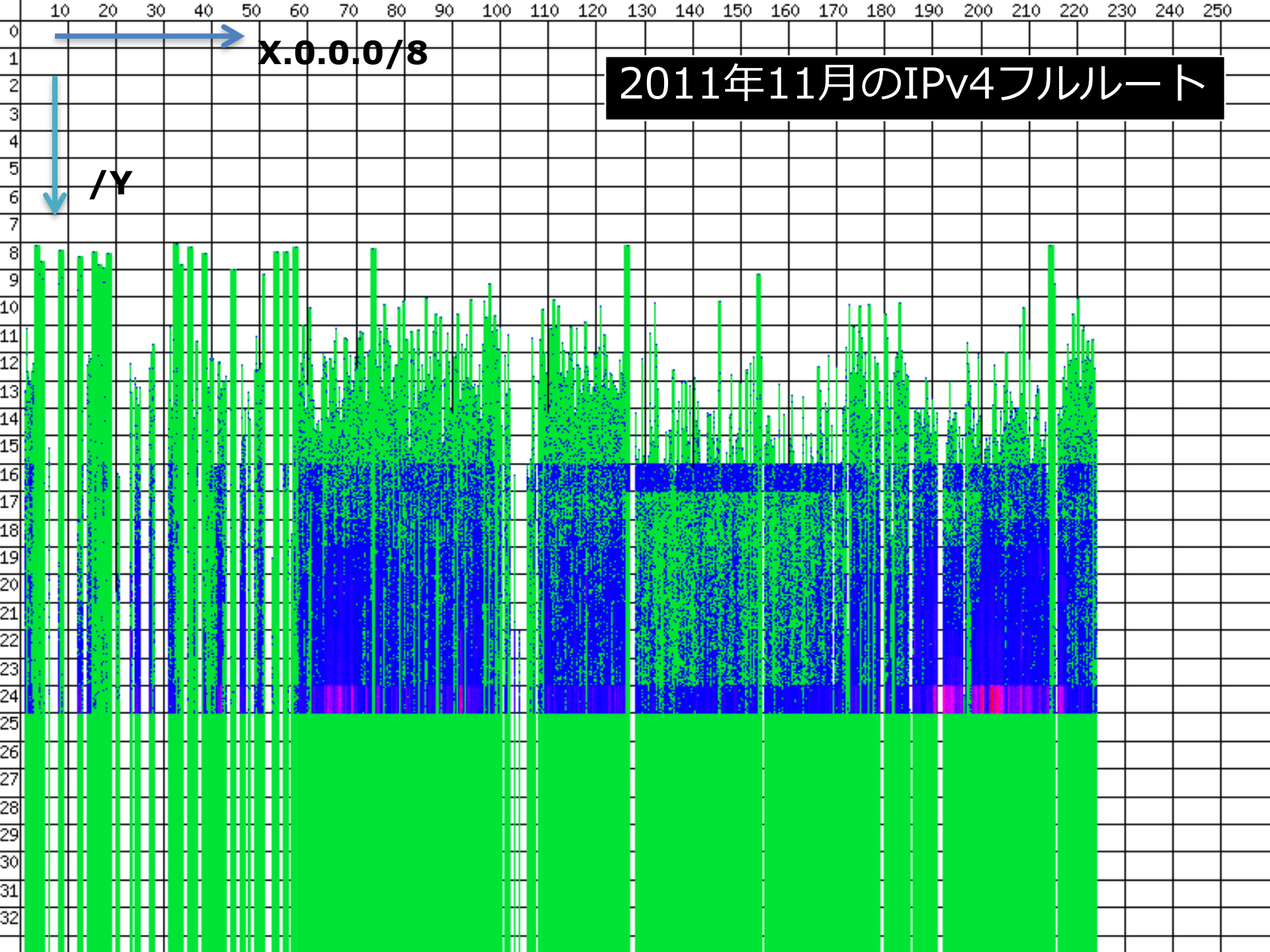

10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
x.0.0.0/8
/Y
2006年8月のIPv4フルルート

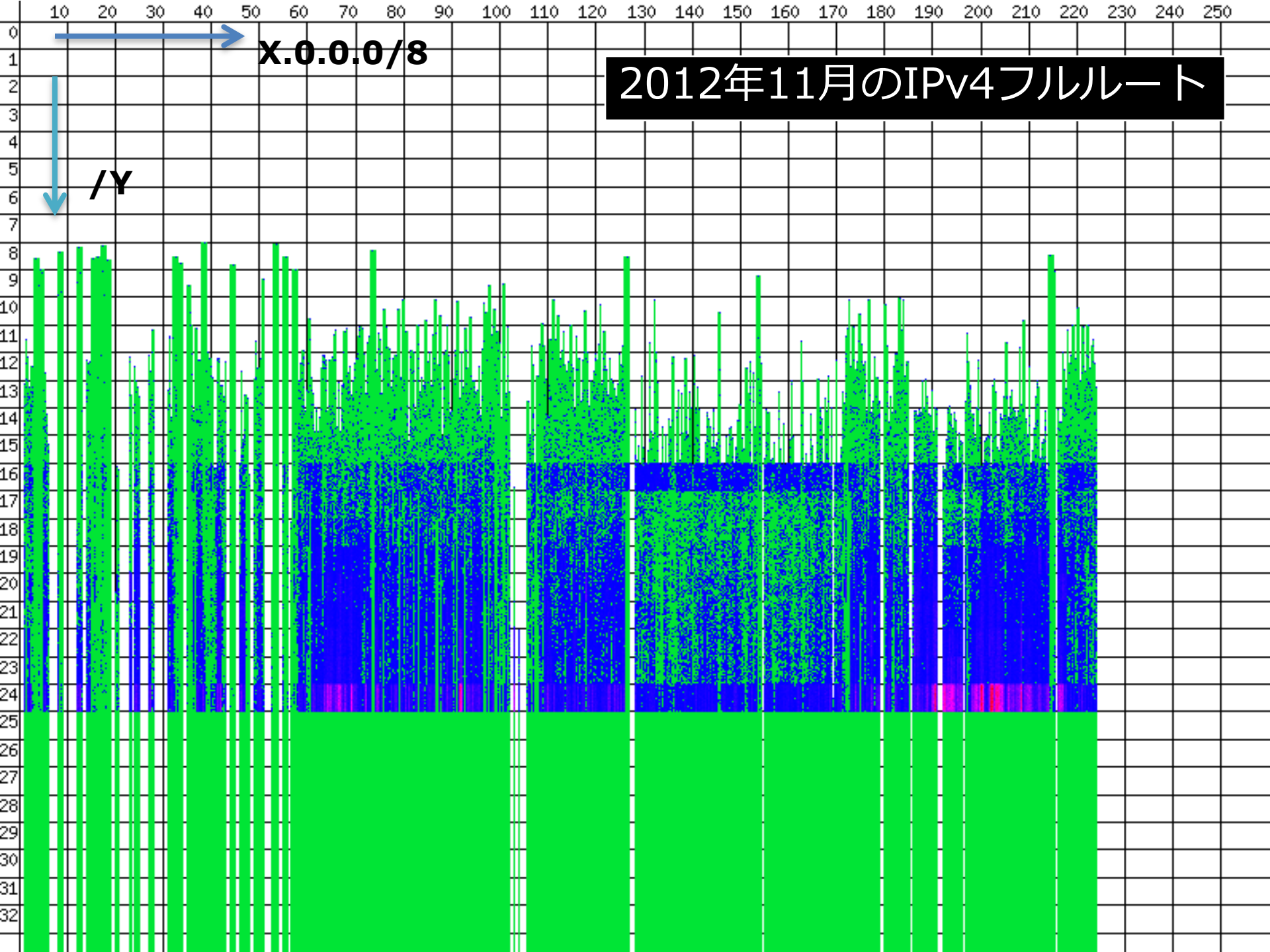

10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
x.0.0.0/8
/Y
2007年8月のIPv4フルルート

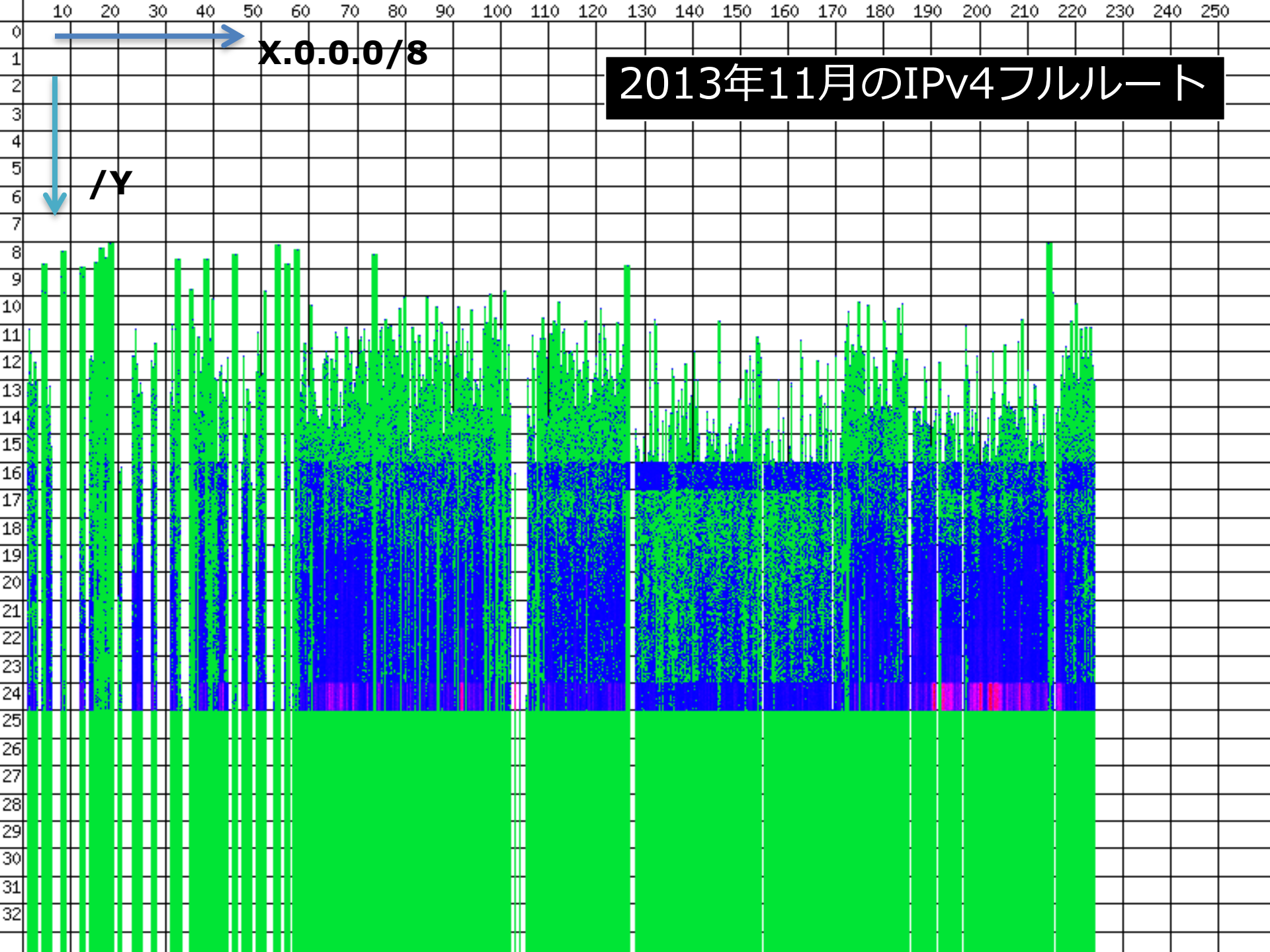

10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
x.0.0.0/8
/Y
2008年11月のIPv4フルルート


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
2009年11月のIPv4フルルート

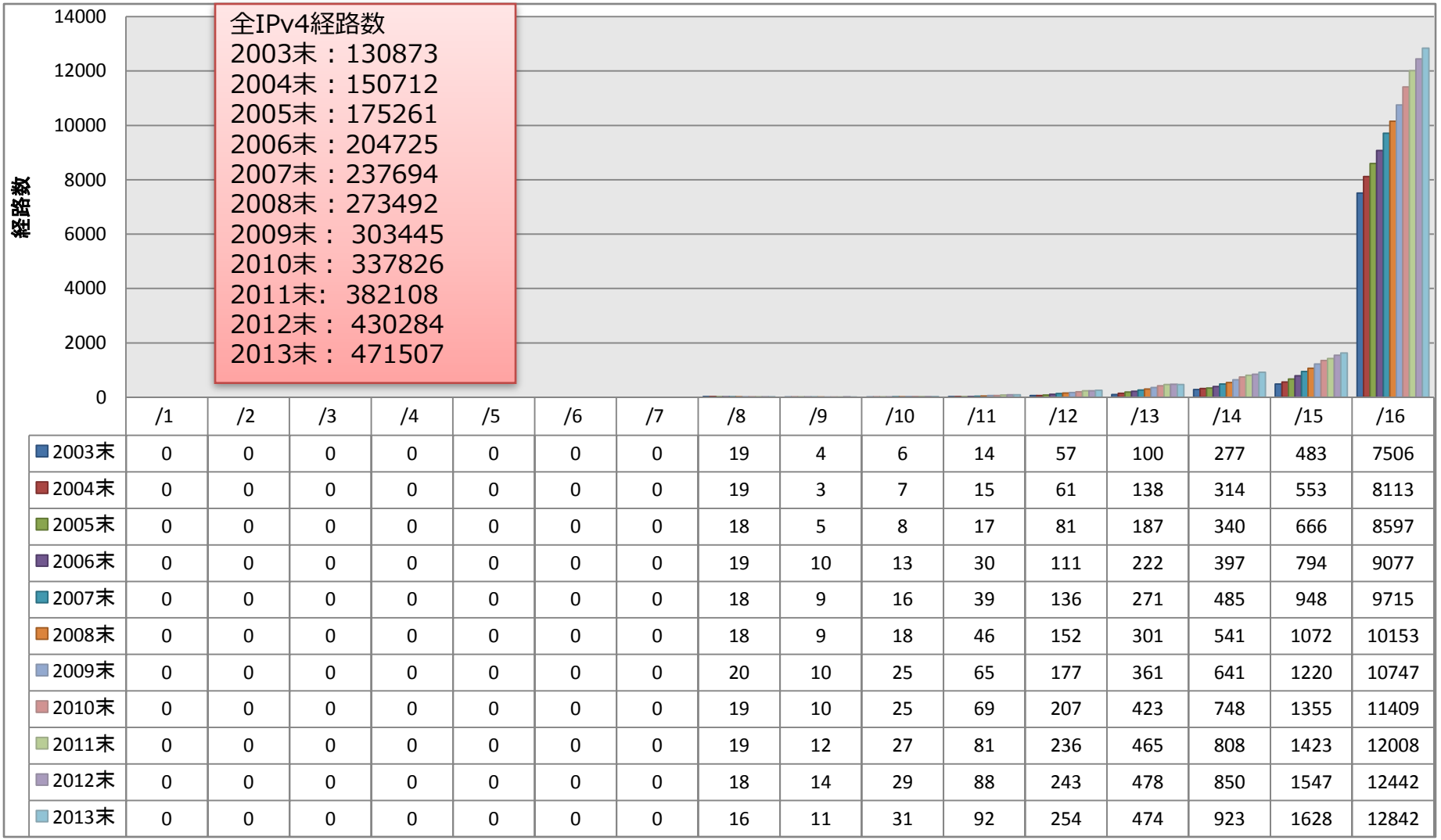

10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
x.0.0.0/8
/Y
2010年11月のIPv4フルルート


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
2012年11月のIPv4フルルート

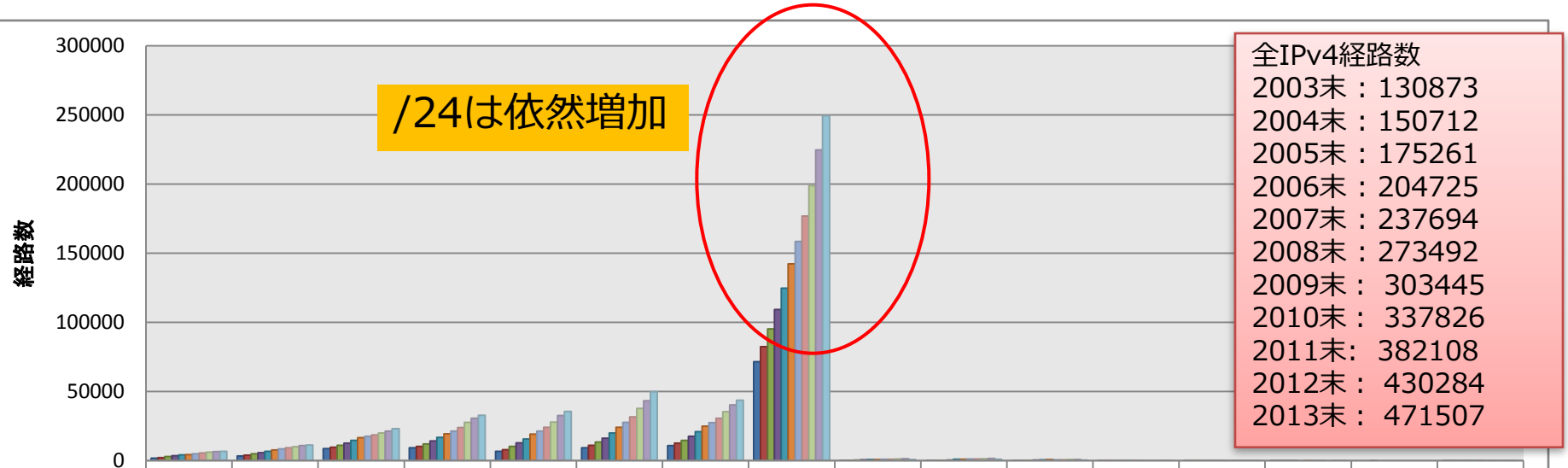

10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
x.0.0.0/8
/Y
2013年11月のIPv4フルルート

IPv4経路数の推移



	/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

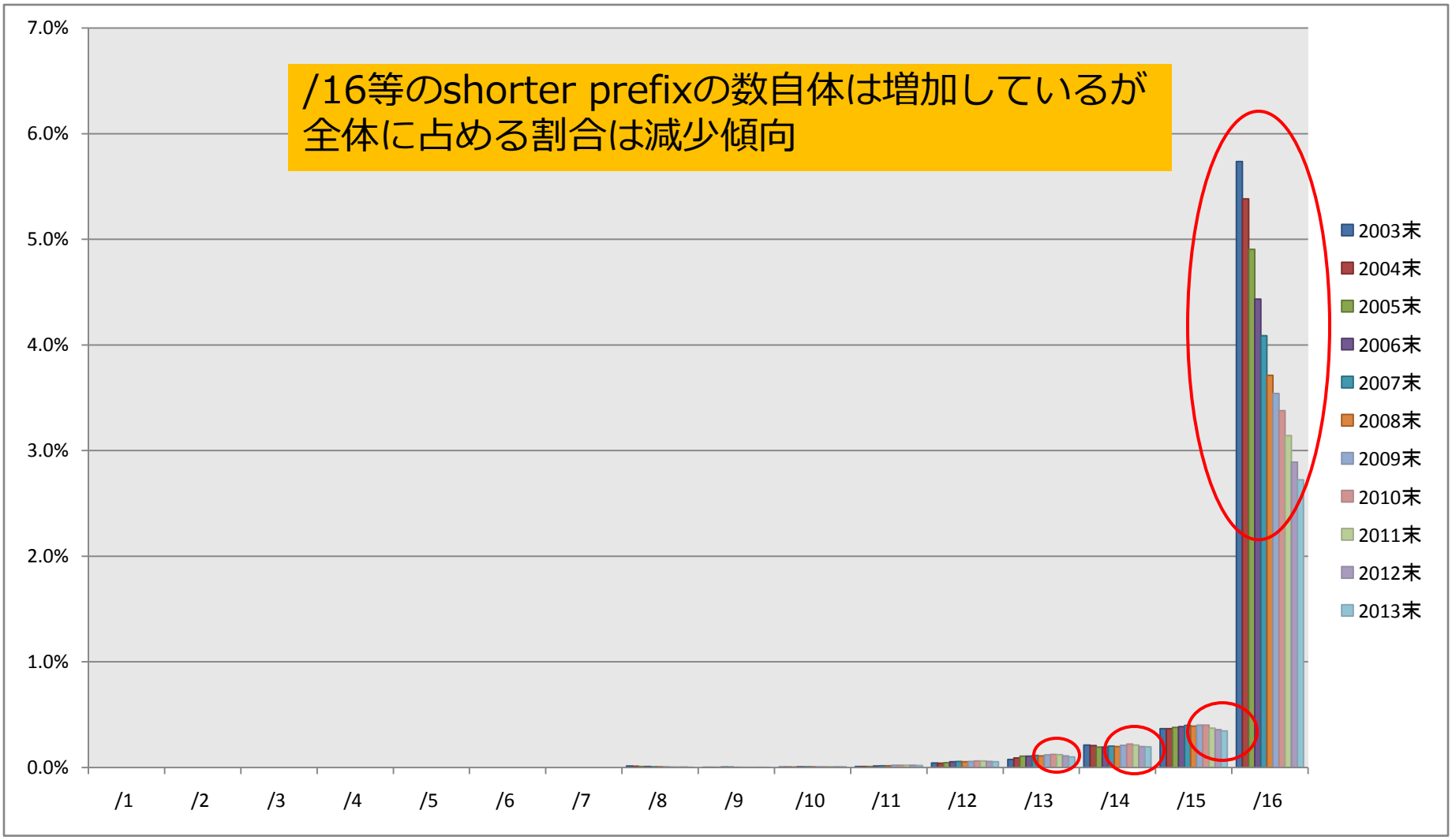
IPv4経路数の推移



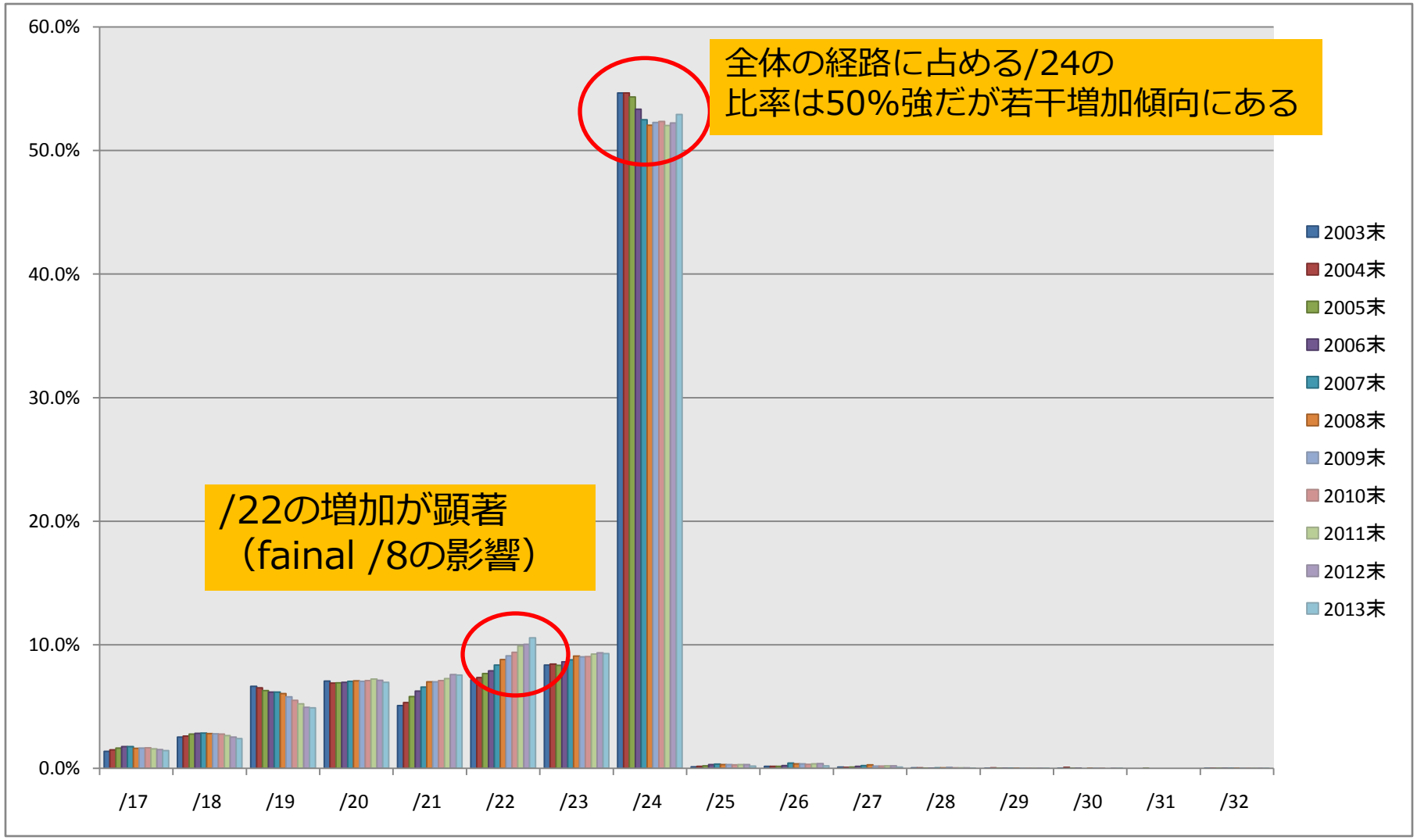
全IPv4経路数
2003末：130873
2004末：150712
2005末：175261
2006末：204725
2007末：237694
2008末：273492
2009末： 303445
2010末： 337826
2011末: 382108
2012末： 430284
2013末： 471507

	/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

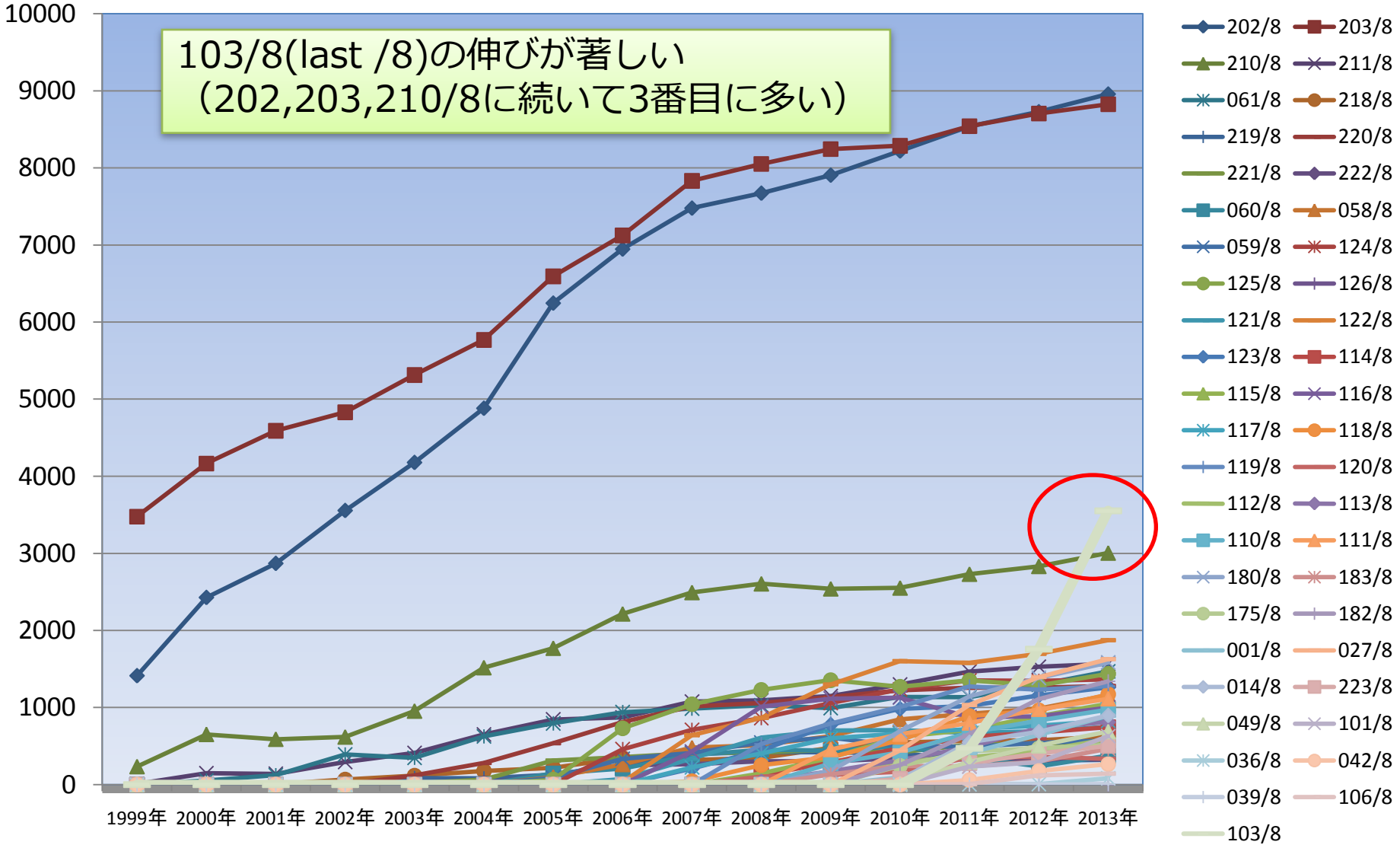
IPv4経路数の推移（割合）



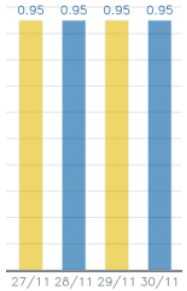
IPv4経路数の推移（割合）



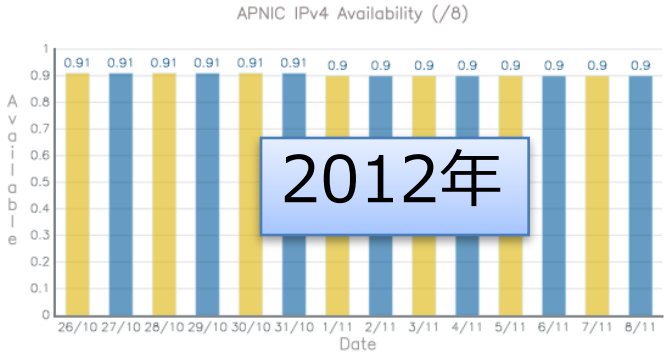
AP地域の/24の推移


103/8(last /8)の伸びが著しい
（202,203,210/8に続いて3番目に多い）
10000
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
1999年
2000年
2001年
2002年
2003年
2004年
2005年
2006年
2007年
2008年
2009年
2010年
2011年
2012年
2013年
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

AP地域の最後の/8
103/8 (2011年～2013年)

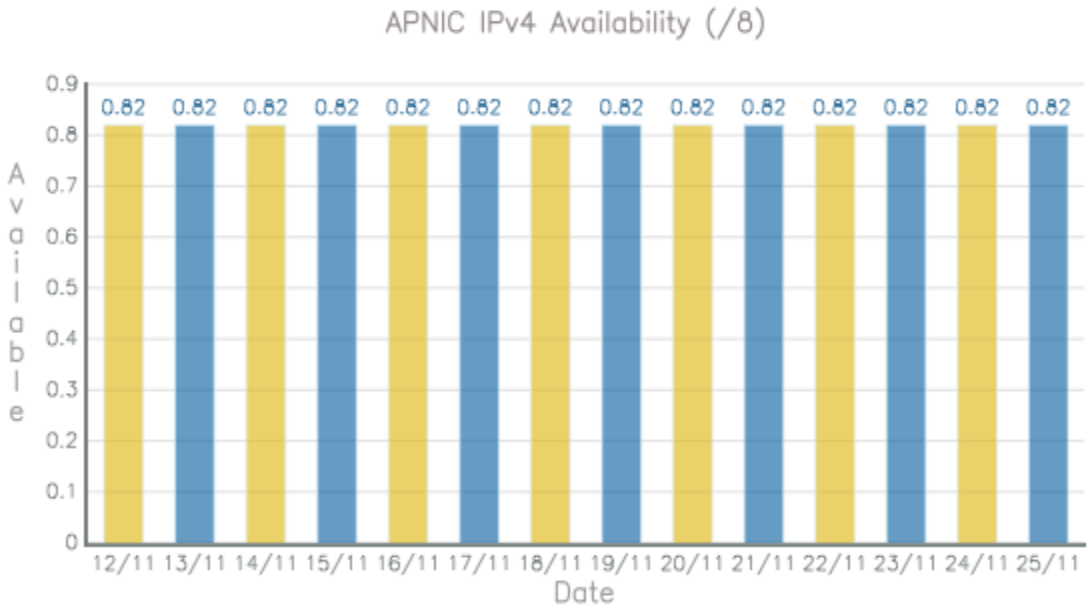


2011年



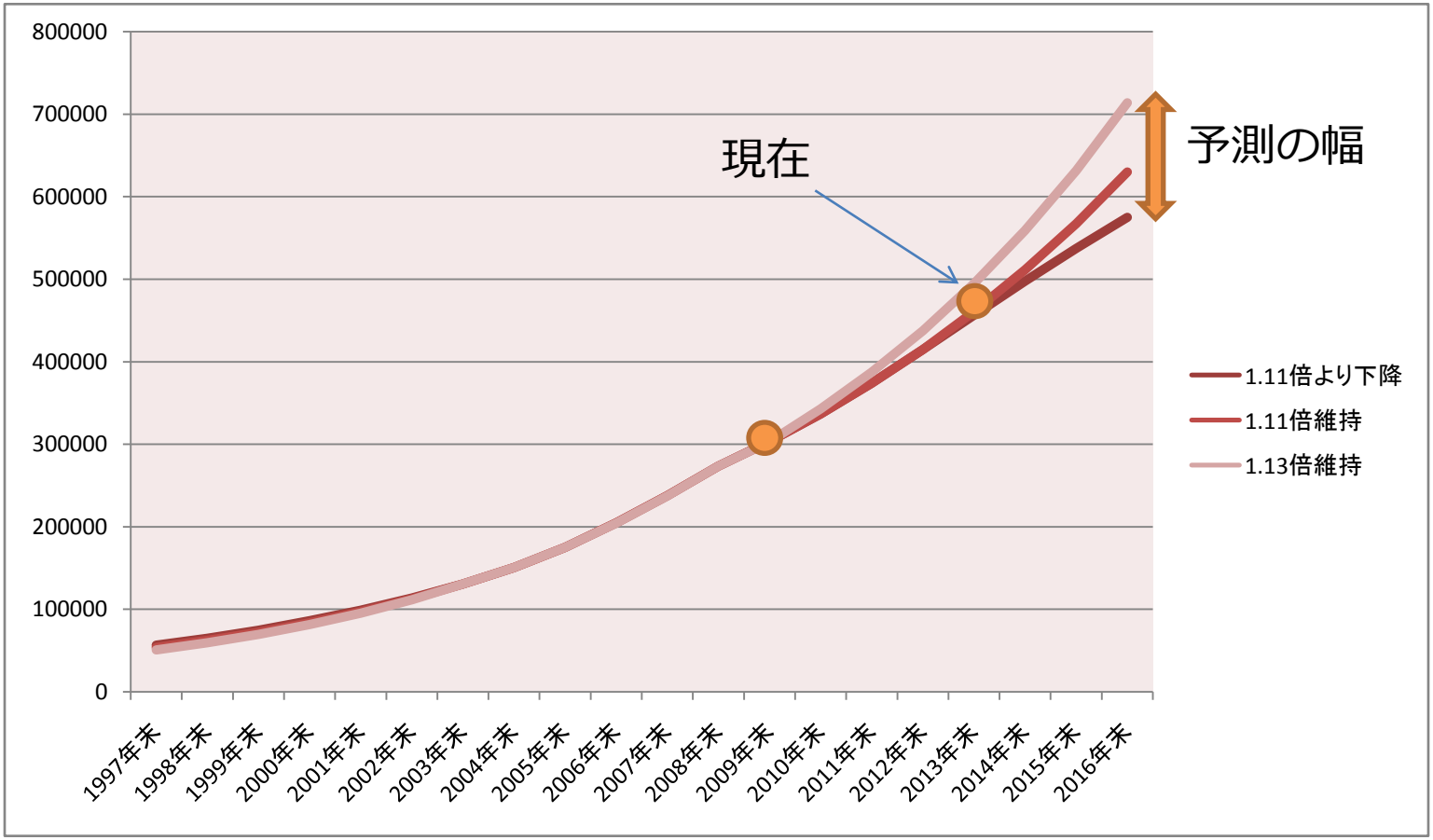
2012年

2013年



徐々に減少。本気でIPv4が必要な人は移転等で対応している状況

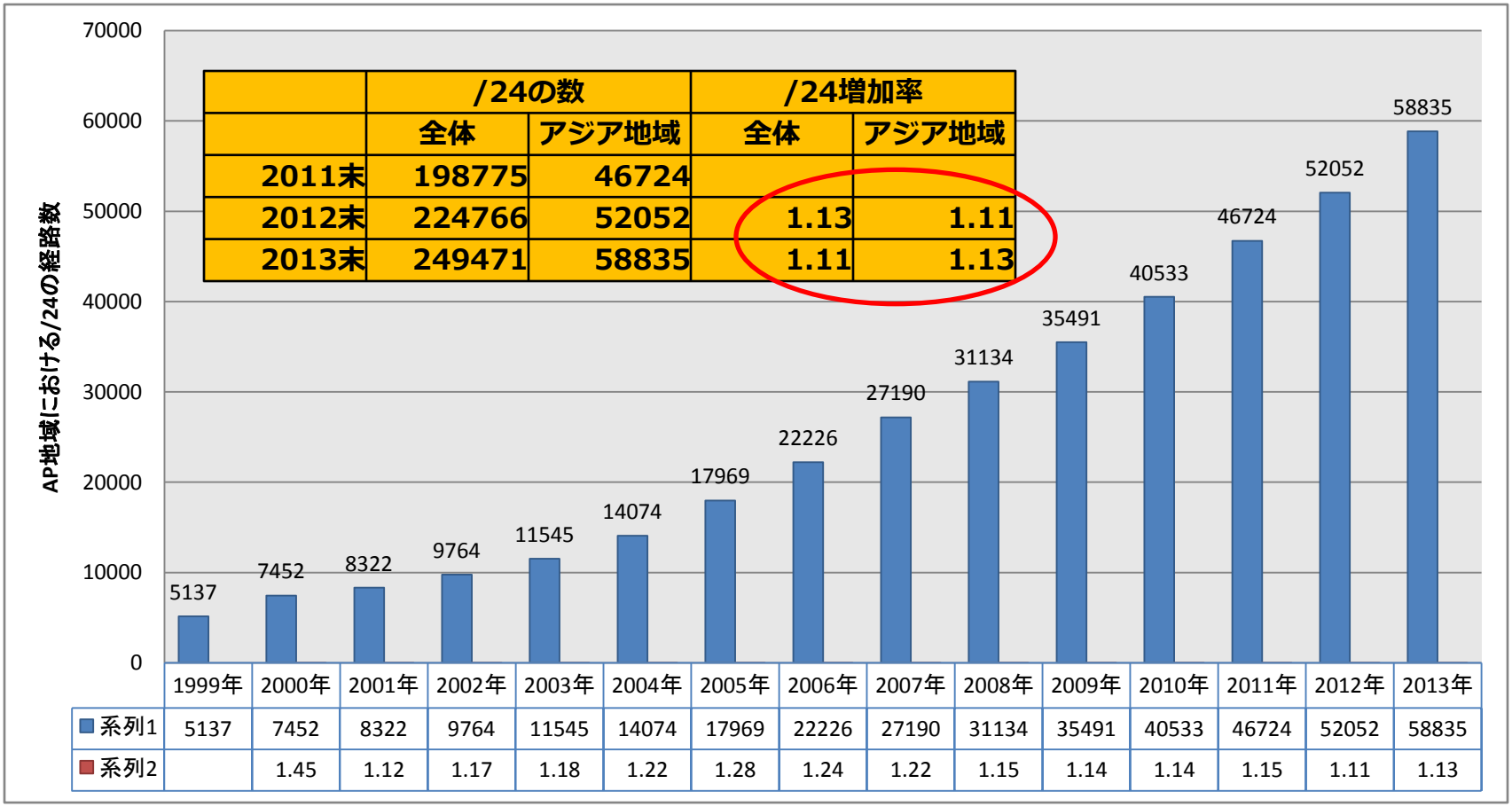
IPv4経路数推移予測
(4年前の2009年末予測)



2011年、2012年は枯渇後もほぼ従来相当の増加傾向
枯渇要因は来年あたりから顕著に見られる可能性があり

AP地域の/24の推移

AP地域の/24増加率は年々低い値となってきているが、最近再度
全体の/24増加率（1.11倍）よりも高い（1.13倍）値となってきている



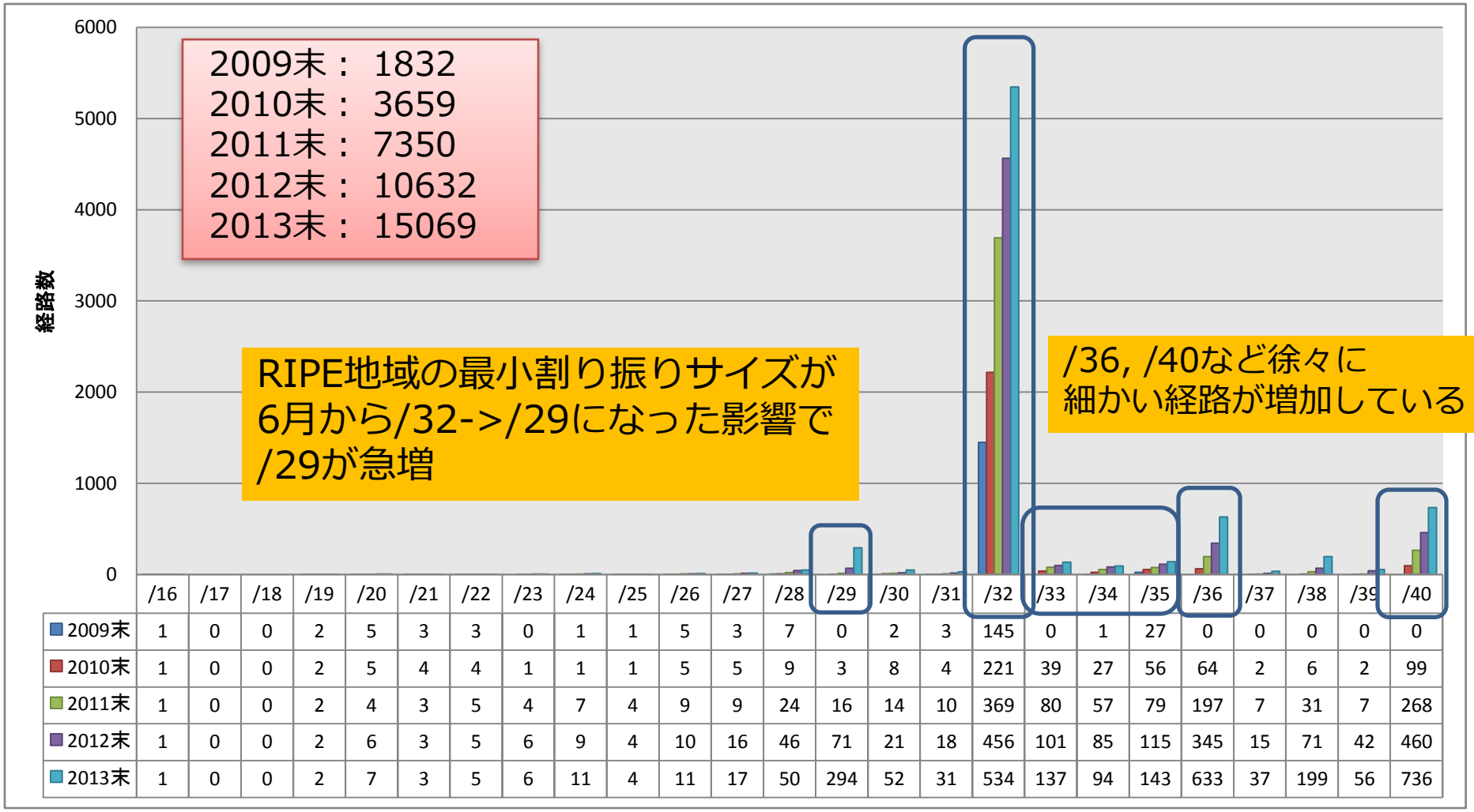
	/24の数		/24増加率	
	全体	アジア地域	全体	アジア地域
2011末	198775	46724		
2012末	224766	52052	1.13	1.11
2013末	249471	58835	1.11	1.13

	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
系列1	5137	7452	8322	9764	11545	14074	17969	22226	27190	31134	35491	40533	46724	52052	58835
系列2		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

APNIC公認？のブローカー

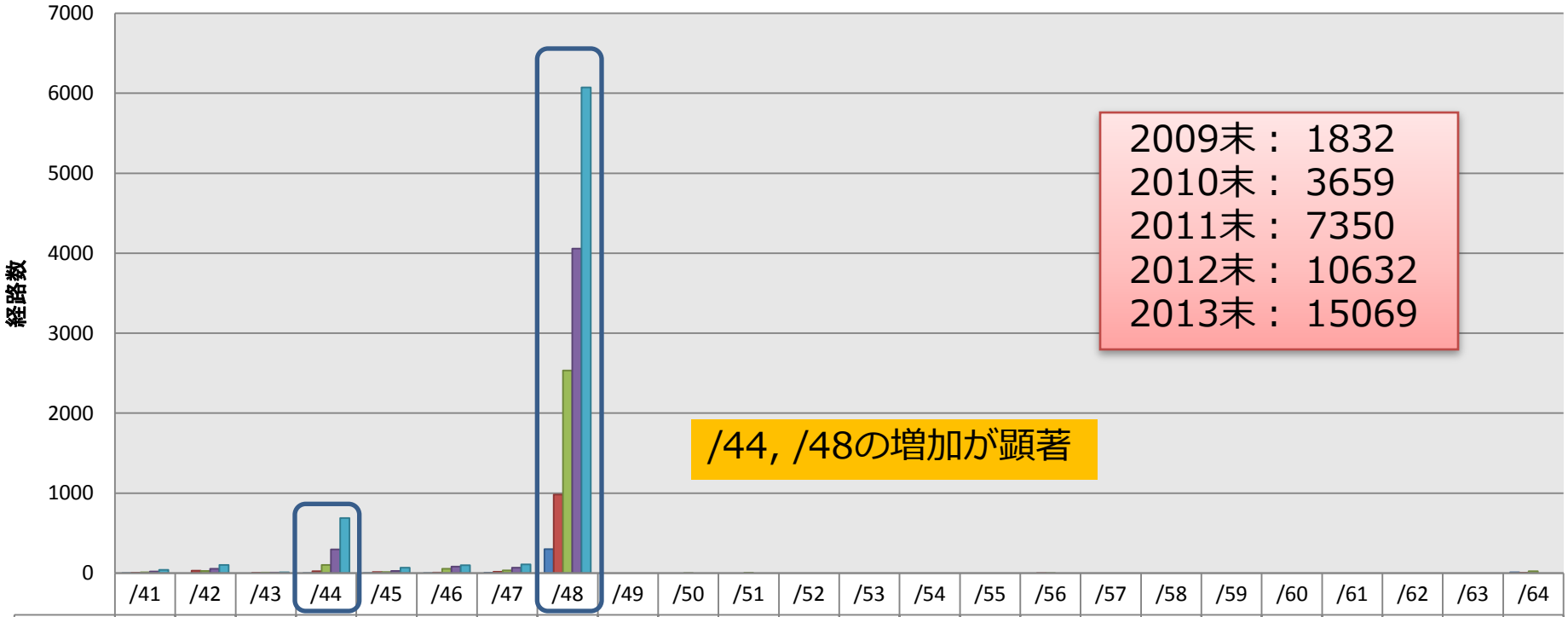
http://www.apnic.net/services/become-a-member/manage-your-membership/transfer-resources/transfer-facilitators

IPv6経路数の推移



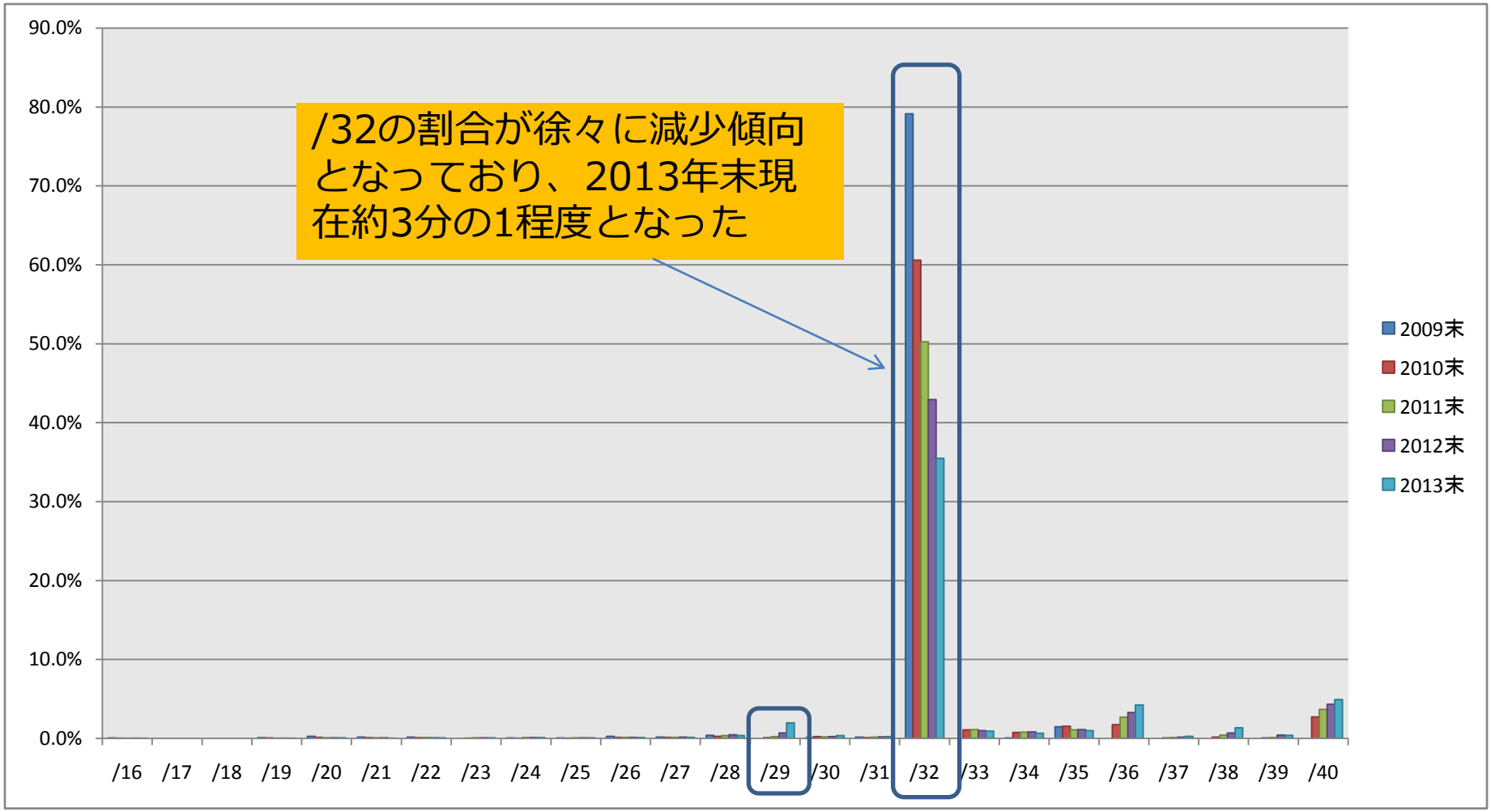
	/16	/17	/18	/19	/20	/21	/22	/23	/24	/25	/26	/27	/28	/29	/30	/31	/32	/33	/34	/35	/36	/37	/38	/39	/40
2009末	1	0	0	2	5	3	3	0	1	1	5	3	7	0	2	3	145	0	1	27	0	0	0	0	0
2010末	1	0	0	2	5	4	4	1	1	1	5	5	9	3	8	4	221	39	27	56	64	2	6	2	99
2011末	1	0	0	2	4	3	5	4	7	4	9	9	24	16	14	10	369	80	57	79	197	7	31	7	268
2012末	1	0	0	2	6	3	5	6	9	4	10	16	46	71	21	18	456	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	534	137	94	143	633	37	199	56	736

IPv6経路数の推移

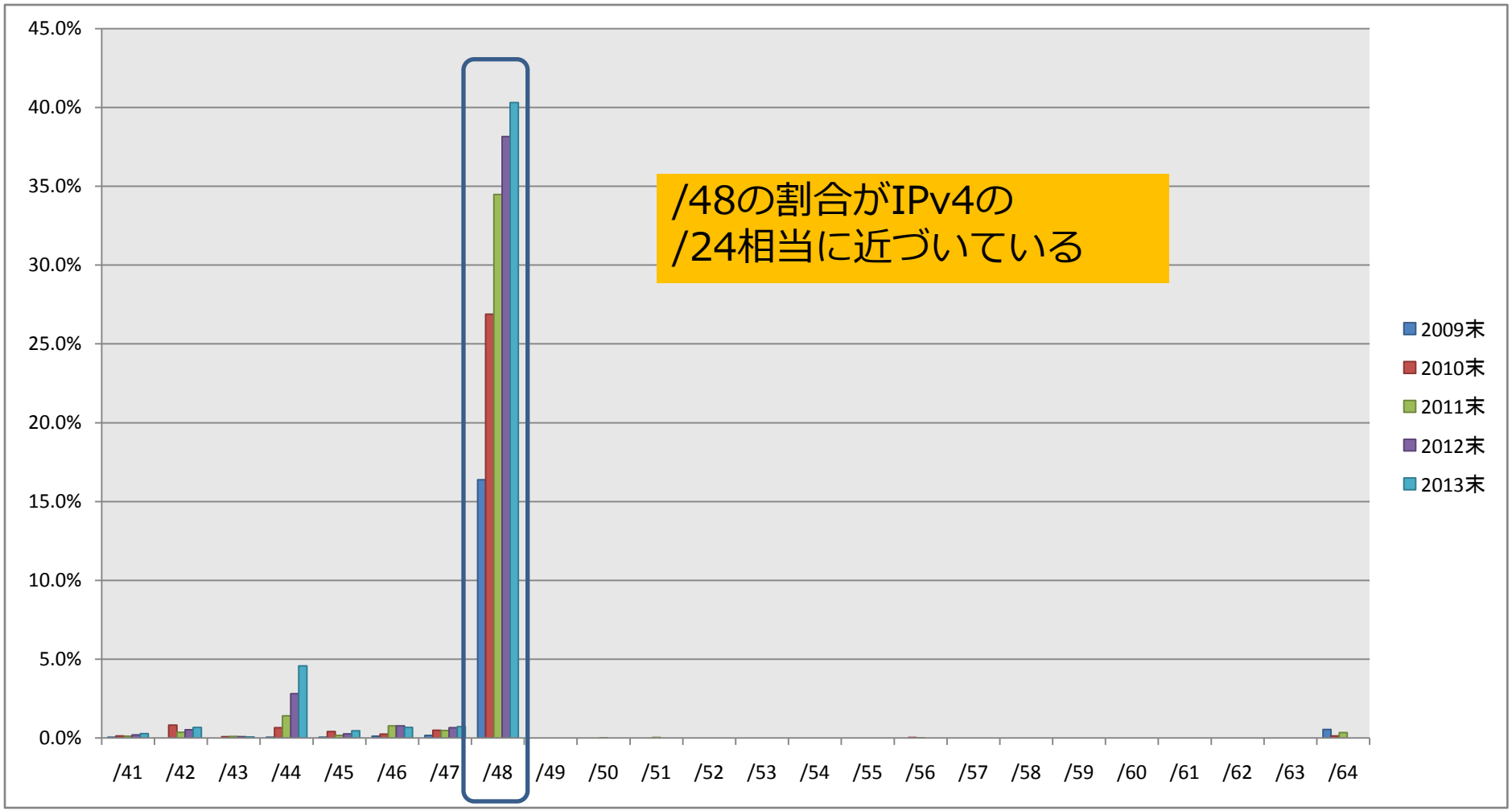


	/41	/42	/43	/44	/45	/46	/47	/48	/49	/50	/51	/52	/53	/54	/55	/56	/57	/58	/59	/60	/61	/62	/63	/64
2009末	1	0	0	1	1	2	3	300	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10
2010末	5	30	3	24	15	9	18	984	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	5
2011末	10	27	8	104	13	57	36	2534	0	1	3	0	0	0	0	1	0	0	0	0	0	0	0	26
2012末	21	55	8	298	27	81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

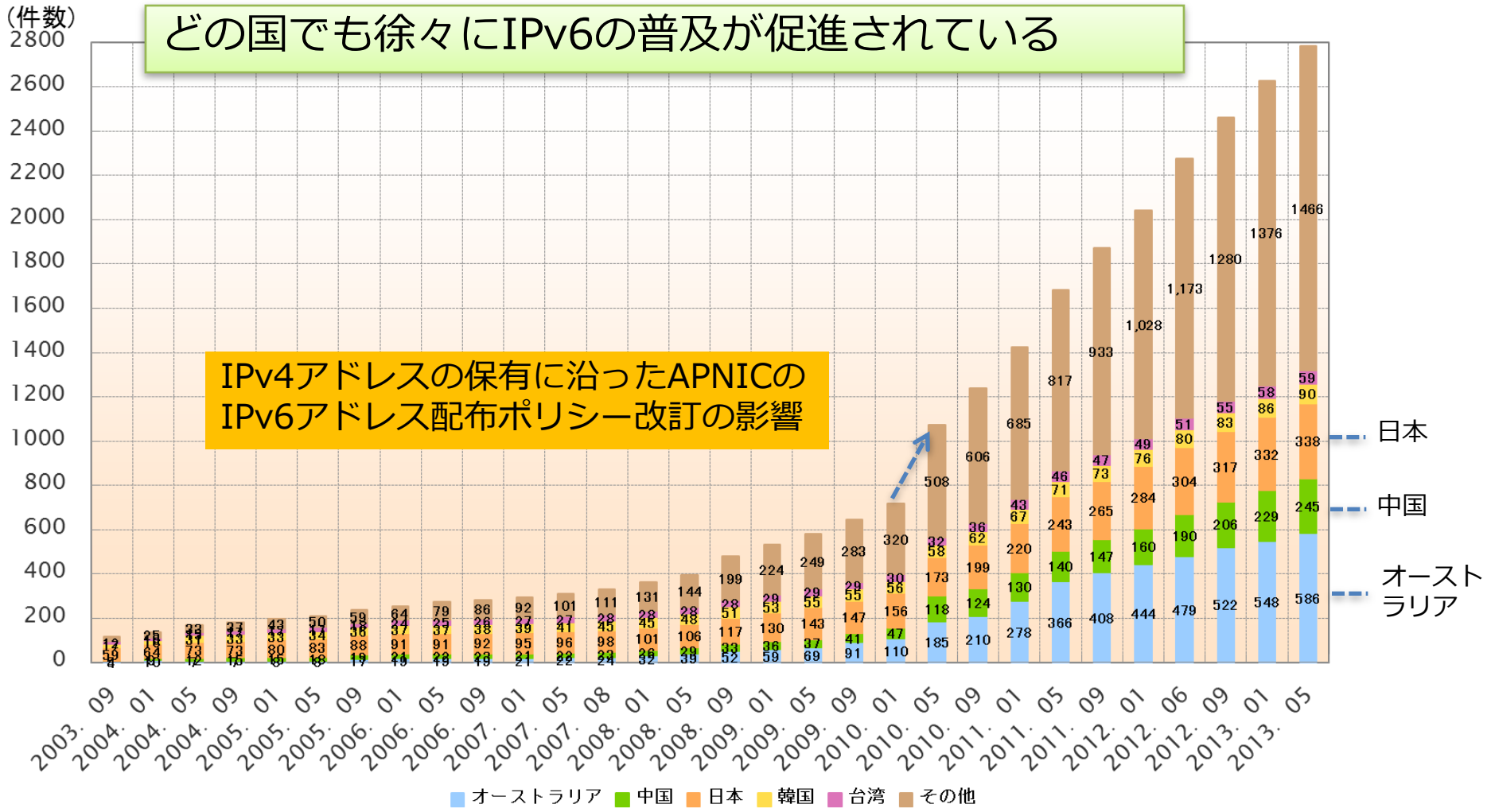
IPv6経路数の推移（割合）



IPv6経路数の推移（割合）



AP地域の国別IPv6アドレス配分状況



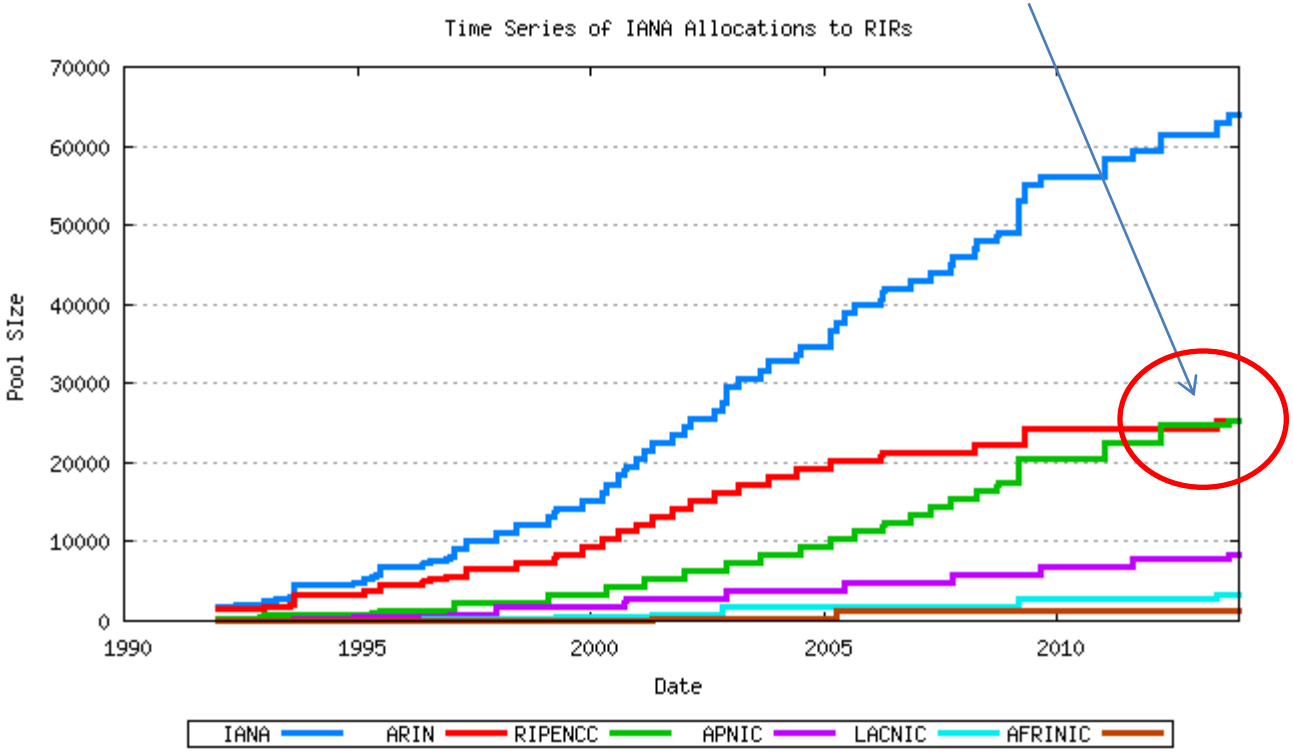
http://www.nic.ad.jp/ja/stat/ip/asia-pacific.html

AS番号 (2byte/4byte)

- 2byte AS
  - 現在残り約500AS（昨年は残り約3000AS）
  - 2014年にIANApoolは枯渇されると予測
  - 特にRIPE地域が継続的に増加
- 4byte AS
  - RIPE NCC地域では積極的に払い出しが実施
    - 依然状況によりRIR毎に運用対処し2byteを払い出す
    - 4byteASのbogon経路も観測されている
    - 日本はほとんど取得が無い。。2013年は1個のみ。。
    - ルータベンダの実装は一通り落ち着いたが依然ISP側で未対応あり

AS Allocation

RIPEと ARINがほぼ同数となった



http://www.potaroo.net/tools/asn16/

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
- 日本や世界のIX動向
- まとめ

2013年 DNS関連トピック

- 大規模化・巧妙化するDNSリフレクター攻撃
  - 大規模な攻撃が複数回発生
  - オープンリゾルバー以外に権威DNSサーバーも踏み台に
  - 洗練される攻撃手法
  - ホームルーターが「オープンDNSフォワーダー」に
  - 技術的な取り組み、対応策
- 多発するレジストリ・レジストラへの攻撃
  - 2012年10月の.ieの事件以降頻発、「月刊TLD」といった様相
  - 複数のccTLDに加え、大手gTLDレジストラも攻撃対象に
- IPフラグメンテーションを利用した「古くて新しい」攻撃手法
  - 第一フラグメント便乗攻撃（1st-fragment piggybacking attacks）
  - ICMPの偽造と組合わせることでパワーアップ
- DNSSECは徐々に増加、設定ミス等で引けないzoneも増加
- おまけ：今年も来なかった平穏無事な7月
  - しかも、「ゼロデイ攻撃」状態での緊急公開（日本時間の土曜日）

大規模化・巧妙化する DNSリフレクター攻撃

- 大規模な攻撃が複数回発生
  - Spamhaus/CloudFlareが攻撃目標に：3月の事件（300Gbps超）
  - Prolexicが預かっている金融プラットフォームが攻撃対象に：5月の事件（167Gbps）
- オープンリゾルバー以外に権威DNSサーバーも踏み台に
  - IPアドレスベースのフィルタ対処は困難のため、DNSRRLやAny-to-TCPなどが今後の対策としては検討されている
- 洗練される攻撃手法
  1. 適当なドメイン名にたくさんAを登録して
  2. 大きな応答を作っておき
  3. それをオープンリゾルバーにキャッシュさせ、攻撃する
- ホームルーターが「オープンDNSフォワーダー」に
  - 特定の箱　＝　特定の国　で多い（韓国、イタリア）
- 技術的な取り組み、対応策
  - BCP38、とにかくつぶす、DNSRRL、Any-to-TCP

dig hizbullah.me

A 204.46.43.90
A 204.46.43.148
A 204.46.43.211
A 204.46.43.15
A 204.46.43.115
A 204.46.43.153
A 204.46.43.60
A 204.46.43.127
A 204.46.43.225
A 204.46.43.192
A 204.46.43.69
A 204.46.43.214
A 204.46.43.234
A 204.46.43.164
A 204.46.43.184
A 204.46.43.140
A 204.46.43.25
A 204.46.43.201
A 204.46.43.197
A 204.46.43.23
A 204.46.43.204
A 204.46.43.200
A 204.46.43.57
A 204.46.43.173
A 204.46.43.96
A 204.46.43.61
A 204.46.43.111
A 204.46.43.139
A 204.46.43.74
A 204.46.43.59
A 204.46.43.17
A 204.46.43.72
A 204.46.43.199
A 204.46.43.158
A 204.46.43.169
A 204.46.43.210
A 204.46.43.117
A 204.46.43.108
A 204.46.43.30
A 204.46.43.31
A 204.46.43.100
A 204.46.43.172
A 204.46.43.135
A 204.46.43.207
A 204.46.43.161
A 204.46.43.50
A 204.46.43.94
A 204.46.43.53
A 204.46.43.36
A 204.46.43.13
A 204.46.43.233
A 204.46.43.206
A 204.46.43.114
A 204.46.43.145
A 204.46.43.219
A 204.46.43.218
A 204.46.43.125
A 204.46.43.170
A 204.46.43.136
A 204.46.43.146
A 204.46.43.1
A 204.46.43.142
A 204.46.43.101
A 204.46.43.41
A 204.46.43.11
A 204.46.43.45
A 204.46.43.52
A 204.46.43.203
A 204.46.43.51
A 204.46.43.194
A 204.46.43.226
A 204.46.43.123
A 204.46.43.81
A 204.46.43.224
A 204.46.43.209
A 204.46.43.35
A 204.46.43.95
A 204.46.43.44
A 204.46.43.22
A 204.46.43.8
A 204.46.43.130
A 204.46.43.144
A 204.46.43.38
A 204.46.43.167
A 204.46.43.97
A 204.46.43.83
A 204.46.43.63
A 204.46.43.28
A 204.46.43.191
A 204.46.43.196
A 204.46.43.188
A 204.46.43.119
A 204.46.43.166
A 204.46.43.223
A 204.46.43.217
A 204.46.43.138
A 204.46.43.186
A 204.46.43.232
A 204.46.43.75
A 204.46.43.77
A 204.46.43.26
A 204.46.43.29
A 204.46.43.16
A 204.46.43.122
A 204.46.43.168
A 204.46.43.128
A 204.46.43.47
A 204.46.43.149
A 204.46.43.34
A 204.46.43.113
A 204.46.43.27
A 204.46.43.109
A 204.46.43.202
A 204.46.43.79
A 204.46.43.58
A 204.46.43.110
A 204.46.43.104
A 204.46.43.7
A 204.46.43.241
A 204.46.43.189
A 204.46.43.21
A 204.46.43.12
A 204.46.43.215
A 204.46.43.9
A 204.46.43.238
A 204.46.43.208
A 204.46.43.49
A 204.46.43.190
A 204.46.43.235
A 204.46.43.133
A 204.46.43.134
A 204.46.43.5
A 204.46.43.231
A 204.46.43.124
A 204.46.43.141
A 204.46.43.66
A 204.46.43.175
A 204.46.43.102
A 204.46.43.71
A 204.46.43.183
A 204.46.43.240
A 204.46.43.20
A 204.46.43.222
A 204.46.43.178
A 204.46.43.121
A 204.46.43.55
A 204.46.43.198
A 204.46.43.73
A 204.46.43.64
A 204.46.43.54
A 204.46.43.216
A 204.46.43.32
A 204.46.43.155
A 204.46.43.157
A 204.46.43.85
A 204.46.43.230
A 204.46.43.107
A 204.46.43.68
A 204.46.43.131
A 204.46.43.65
A 204.46.43.227
A 204.46.43.39
A 204.46.43.176
A 204.46.43.10
A 204.46.43.116
A 204.46.43.86
A 204.46.43.4
A 204.46.43.162
A 204.46.43.147
A 204.46.43.212
A 204.46.43.120
A 204.46.43.106
A 204.46.43.182
A 204.46.43.177
A 204.46.43.24
A 204.46.43.46
A 204.46.43.152
A 204.46.43.37
A 204.46.43.14
A 204.46.43.185
A 204.46.43.180
A 204.46.43.42
A 204.46.43.105
A 204.46.43.40
A 204.46.43.179
A 204.46.43.151
A 204.46.43.70
A 204.46.43.98
A 204.46.43.126
A 204.46.43.18
A 204.46.43.150
A 204.46.43.33
A 204.46.43.156
A 204.46.43.193
A 204.46.43.93
A 204.46.43.159
A 204.46.43.220
A 204.46.43.91
A 204.46.43.242
A 204.46.43.187
A 204.46.43.92
A 204.46.43.62
A 204.46.43.3
A 204.46.43.229
A 204.46.43.84
A 204.46.43.82
A 204.46.43.48
A 204.46.43.165
A 204.46.43.80
A 204.46.43.221
A 204.46.43.89
A 204.46.43.160
A 204.46.43.143
A 204.46.43.19
A 204.46.43.6
A 204.46.43.78
A 204.46.43.103
A 204.46.43.118
A 204.46.43.129
A 204.46.43.228
A 204.46.43.132
A 204.46.43.171
A 204.46.43.154
A 204.46.43.163
A 204.46.43.137
A 204.46.43.205
A 204.46.43.99
A 204.46.43.2
A 204.46.43.237
A 204.46.43.88
A 204.46.43.236
A 204.46.43.181
A 204.46.43.56
A 204.46.43.213
A 204.46.43.67
A 204.46.43.174
A 204.46.43.239
A 204.46.43.76
A 204.46.43.195
A 204.46.43.43
A 204.46.43.112
A 204.46.43.87

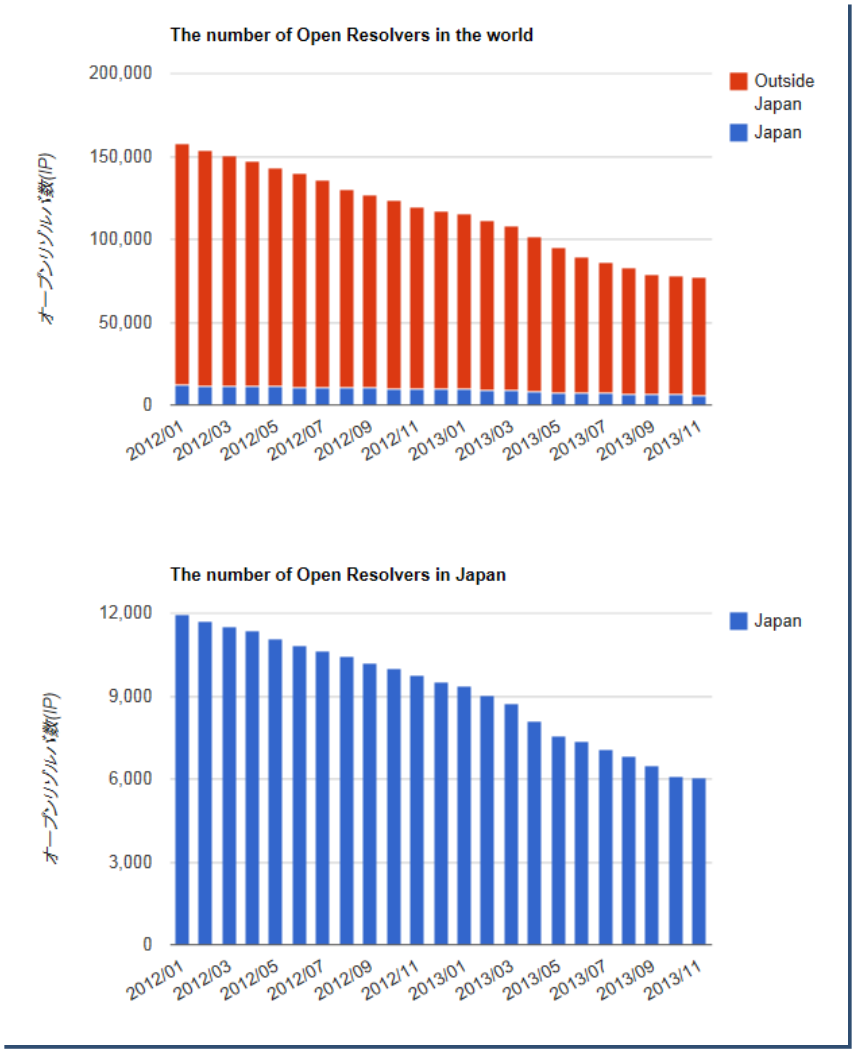
大規模化・巧妙化するDNSリフレクター攻撃

- 大規模な攻撃が複数回発生
  - Spamhaus/CloudFlareが攻撃目標に：3月の事件（300Gbps超）
  - Prolexicが預かっている金融プラットフォームが攻撃対象に：5月の事件（167Gbps）
- オープンリゾルバー以外に権威DNSサーバーも踏み台に
  - IPアドレスベースのフィルタ対処は困難のため、DNSRRLやAny-to-TCPなどが今後の対策としては検討されている
- 洗練される攻撃手法
  1. 適当なドメイン名にたくさんAを登録して
  2. 大きな応答を作っておき
  3. それをオープンリゾルバーにキャッシュさせ、攻撃する
- ホームルーターが「オープンDNSフォワーダー」に
  - 特定の箱　＝　特定の国　で多い（韓国、イタリア）
- 技術的な取り組み、対応策
  - BCP38、とにかくつぶす、DNSRRL、Any-to-TCP

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

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



JPRS公開のDNS関連セキュリティ情報(2013年)

セキュリティ情報

- BIND 9.xの脆弱性（サービス提供者が意図しないアクセスの許可）について（2013年11月7日公開）
- （緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（2013年7月27日公開）
- （緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（2013年6月5日公開）
- （緊急）BIND 9.xの致命的な脆弱性（過度のメモリ消費）について（2013年3月27日公開）
- BIND 9.8.x/9.9.xにおけるDNS64/RPZの実装上のバグによるnamedのサービス停止について（2013年1月25日公開）

注意喚起

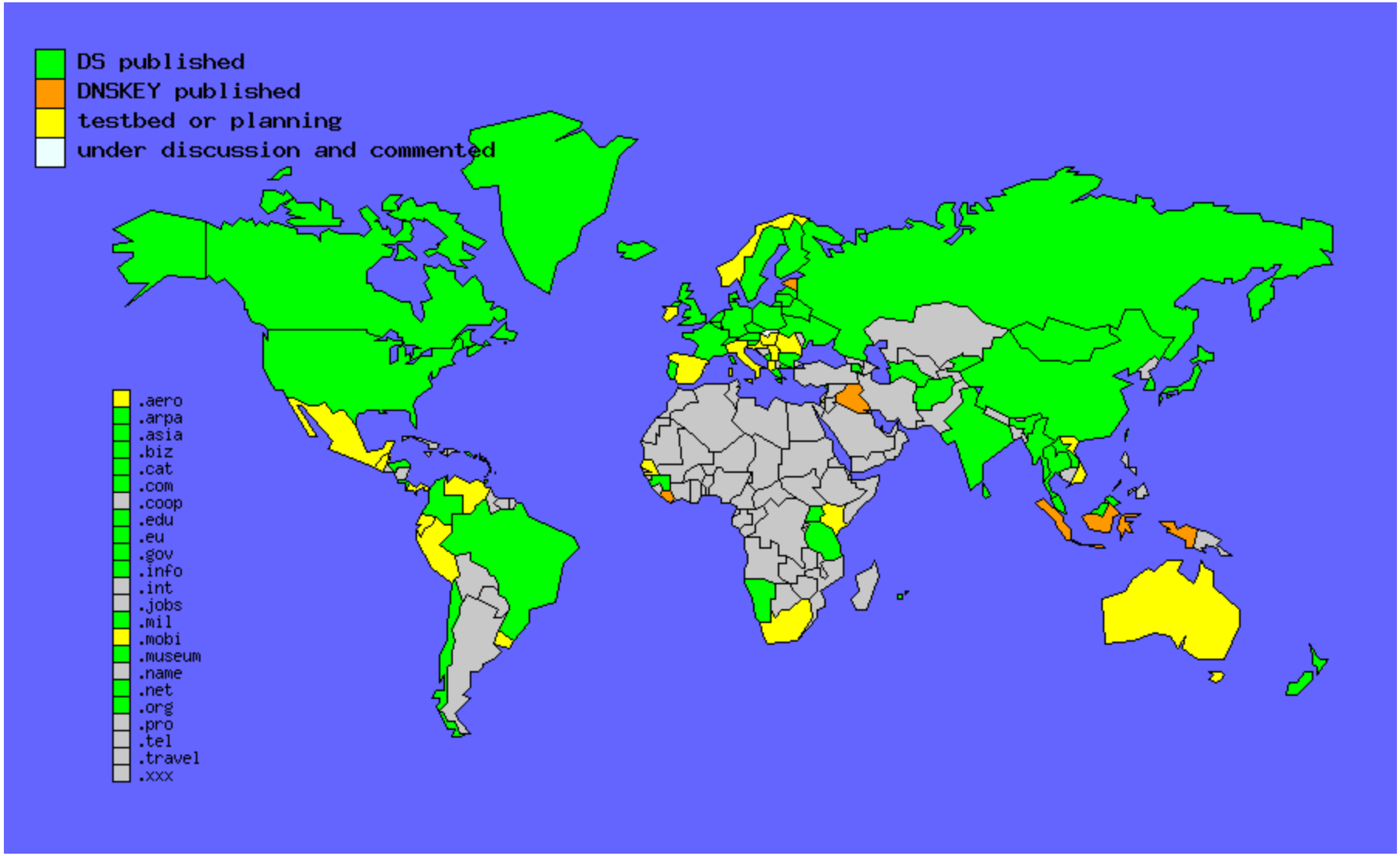
- 2013-04-18 技術解説：「DNS Reflector Attacks（DNSリフレクター攻撃）」について
- 2013-04-18 設定ガイド：オープンリゾルバー機能を停止するには【BIND編】

6年連続　祭りの魔の7月

- 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**」）
  JPRS: （緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（2013年7月27日公開）
  - 1パケットで確実にnamedを落とせる
  - キャッシュDNSサーバ、権威DNSサーバ双方に対して有効
  - namedのアクセスコントロールでは防げない

TLDのDNSSEC普及状況



http://www.ohmo.to/dnssec/maps/

www.bncr.fi.cr Failing DNSSEC Validation

Posted by Super User on April 30, 2013 in DNSSEC News

The domain bncr.fi.cr is currently failing DNSSEC validation. This is because several RRSIG records in the domain are invalid, including www.bncr.fi.cr. The domain owners have been contacted and made aware of the issue. The DNSViz report of this failure can be found at http://dnsviz.net/d/www.bncr.fi.cr/UX_OqQ/dnssec/.

Tags: DNSSEC

vsp.virginia.gov Failing DNSSEC Validation

Posted by Comcast on April 11, 2013 in DNSSEC News

The domain vsp.virginia.gov is currently failing DNSSEC validation. This is because DNSKEYs are expired. The domain owners have been contacted and made aware of the issue. The DNSViz report of this failure can be found at http://dnsviz.net/d/vsp.virginia.gov/UWb1Yg/dnssec/.

Tags: DNSSEC

energystar.gov Failing DNSSEC Validation

Posted by Super User on April 11, 2013 in DNSSEC News

The domain energystar.gov is currently failing DNSSEC validation. This is because the domain has a published DS record that does not match any DNSKEY record. The domain owners have been contacted and made aware of the issue. The DNSViz report of this failure can be found at http://dnsviz.net/d/energystar.gov/UWbUKg/dnssec/.

Tags: DNSSEC

bncr.fi.cr Failing DNSSEC Validation

Posted by Comcast on April 11, 2013 in DNSSEC News

The domain bncr.fi.cr is currently failing DNSSEC validation. This is because the RRSIG and DNSKEY do not validate records in the domain. The domain owners have been contacted and made aware of the issue. The DNSViz report of this failure can be found at http://dnsviz.net/d/bncr.fi.cr/UWbGQA/dnssec/.

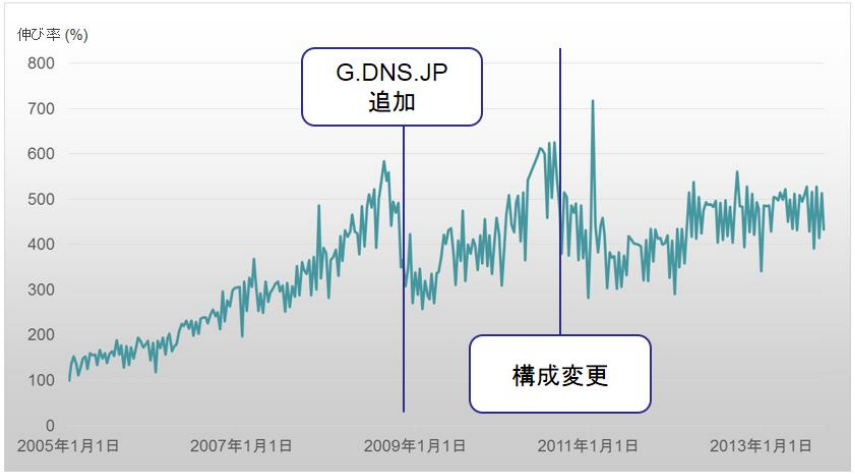
Tags: DNSSEC

http://dns.comcast.net/

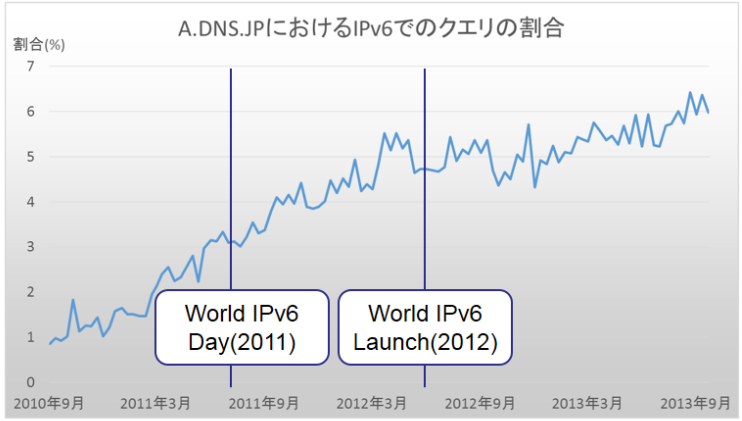
DNSクエリ数の推移

統計情報 A.DNS.JP のクエリ数

A.DNS.JPへのクエリ数の推移（2005年1月1日を100%とする）



統計情報 IPv6でのクエリの割合



- 2010年の後半から、IPv6でのクエリの割合が増加
- 2013年11月現在、IPv6でのクエリの割合は6%前後
  - 前年比1%程度増加

Internet Week 2013 「JP DNS Update」資料より引用

（例）www.nikkei.com

１つのサイトだけでもこれだけのqueryが出る。
ブラウザを立ち上げ時はものすごい量。
（DNSプリフェッチの影響はすごい）

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
- 日本や世界のIX動向
- まとめ

2013年セキュリティ動向

- オープンリゾルバを利用した大規模なサイバー攻撃：3月
  - Spamhaus/CloudFlareが攻撃目標に（300Gbps超）
  - 欧州の主要IX（AMS-IX, DE-CIX, LINX）も通信品質劣化などの影響を受けた
  - 以降、様々なサイトに対して同様の手法により攻撃が多数観測
- サイバー攻撃予告／予兆：9月
  - 満州事変を背景とするサイバー攻撃が毎年何らか発生しているが大規模な被害はなかった模様
- フィッシング攻撃
  - 大手銀行や大手通信事業者を狙ったフィッシングサイトが相変わらず多い
- 経路消失、のっとり事件
  - 中東情勢の影響で中東各国の経路が消失、北朝鮮の経路も一時消失
  - 故意に経路ハイジャックが不定期に行われている
- MITM攻撃の脅威が顕在化
- 官民連携のマルウェア対策支援プロジェクト「ACTIVE」が開始

2013年のフィッシング事情

- 銀行、通信事業者のポータルサイト、ゲームサイトなど、アカウント情報を管理している様々な企業を狙うケースが多発

フィッシング対策協議会より：　https://www.antiphishing.jp/

2013年11月19日　コミュファ光 Webメールをかたるフィッシング(2013/11/19)
2013年11月18日　三菱東京UFJ銀行をかたるフィッシング(2013/11/18)
2013年11月15日　[11/15更新] eoWEBメールをかたるフィッシング(2013/10/01)
2013年10月10日　スクウェア・エニックスをかたるフィッシング(2013/10/10)
2013年10月10日　UCカード(アットユーネット)をかたるフィッシング(2013/10/10)
2013年10月03日　ODNをかたるフィッシング(2013/10/03)
2013年10月01日　ポータルサイトgooをかたるフィッシング(2013/10/01)
2013年08月07日　ハンゲームをかたるフィッシング(2013/08/07)
2013年06月07日　NCSOFTをかたるフィッシング(2013/06/07)
2013年05月29日　新生銀行をかたるフィッシング(2013/05/29)
2013年05月15日　Nexyz.BB Web.Mailをかたるフィッシング(2013/05/15)
2013年04月05日　@niftyをかたるフィッシング(2013/04/05)
2013年03月26日　Yahoo!メールをかたるフィッシング(2013/03/26)
2013年02月20日　ODNをかたるフィッシング(2013/02/20)
2013年02月15日　eoWEBメールをかたるフィッシング(2013/2/15)
2013年02月14日　MasterCardをかたるフィッシング(2013/2/14)
2013年01月10日　PayPalをかたるフィッシング(2013/1/10)
2013年01月08日　三菱東京UFJ銀行をかたるフィッシング(2013/1/8)

最近の事例（2013/11/18）：東京三菱UFJ銀行を騙るフィッシング

こんにちは！

これは三菱東京ＵＦＪ銀行によって行っているユーザ番号の調査です。
あなたのユーザ番号は使用停止になっているかどうかをチェックしています。
あなたのユーザ番号は合法的であることが保障できるために、下記のリンクを
クリックしてください。

https://entry11.bk.mufg.jp/ibg/dfw/APLIN/loginib/login?_TRANID=AA000_001
<http://www.●●●●.net/images/index.htm>

あなたのユーザ番号の承認が完成された後、三菱東京ＵＦＪ銀行よりあなたの
ユーザ番号をチェックしていただきます。

フィッシング対策協議会より: https://www.antiphishing.jp/

最近の事例：
東京三菱UJFを騙るフィッシング

本物

偽物

フィッシング対策協議会より：　https://www.antiphishing.jp/

待ち受け型ハニーポットの観測状況

非公開

サンドボックス解析によるマルウェアの通信先

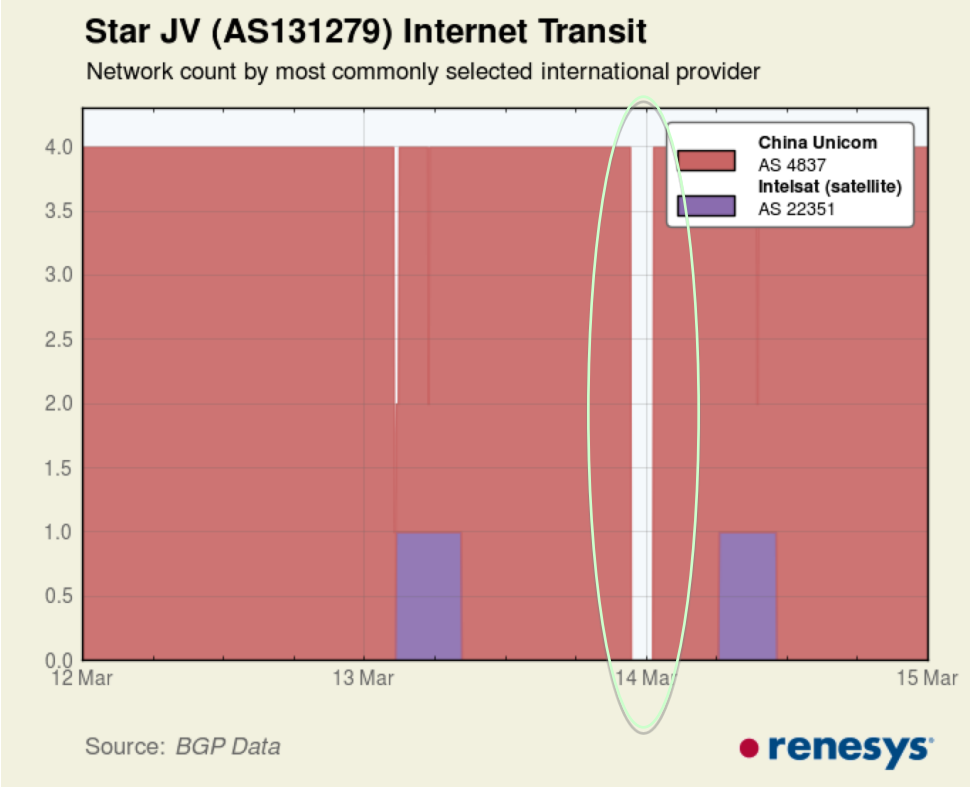
非公開

経路消失事件

- ３月：北朝鮮
- ８月：ミャンマー
- ９月：スーダン

- 反政府運動を阻止するためにネットを遮断する動きが目立っている

北朝鮮： 4Prefixが2時間程度Withdrawn状態に



Source: http://www.renesys.com/

主な不正経路広報、のっとり事案

- 2013/01：Dream Host問題
- 2013/03：Spamhouse Route Hijack
- 2013/06：米国の複数銀行サイトが狙われた
- 2013/08：中国CNNIC運営のDNScacheサーバが停止

- 日々のっとりや不正経路広報が行われているのが実情

MITM from nenesys report

- 2013年、60日程度MITM攻撃状態があった
- 少なくとも一人(IP/Prefix)以上が影響を受けた都市が150に上る
- 一見問題なさそうに見えるところが問題

Source: http://www.renesys.com/

Ex1: Belarusian Traffic Diversion 2013/02

- 2,3分のものから数時間のものまでいろいろ
- 金融機関、政府機関、ISPなどが狙われている
- US、韓国、ドイツ、チェコ、リトアニア、リビア、イラン

Source: http://www.renesys.com/

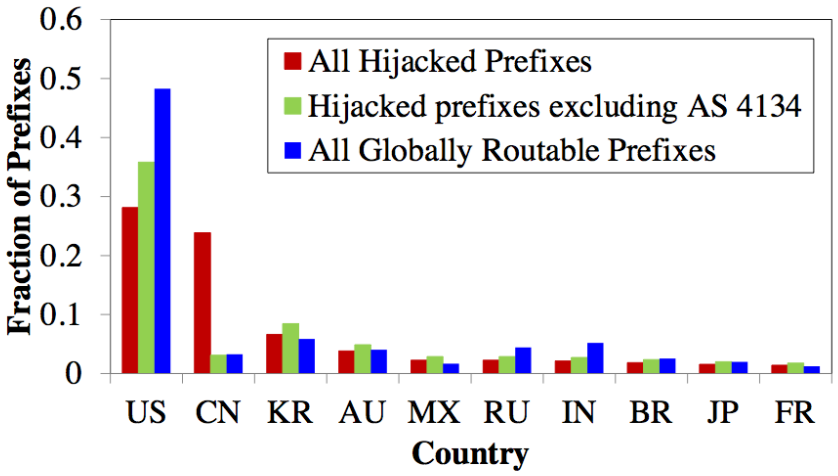
Ex2: Icelandic Traffic Diversion 2013/07

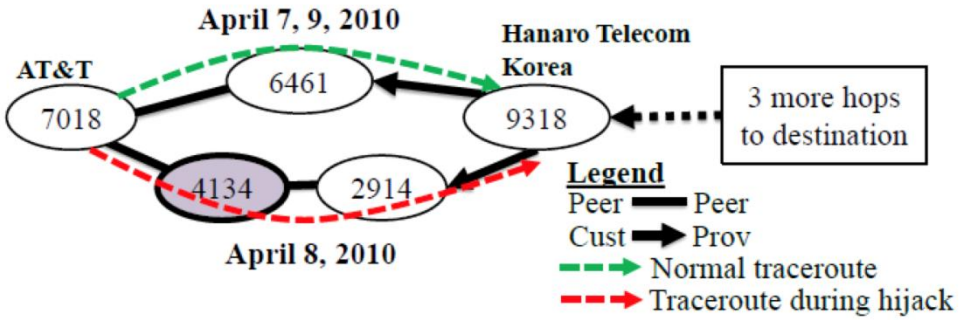
- ベラルーシの事件が２ヶ月何もなくおとなしくなっていた後に発生
- USのVoiceトラフィックが影響をうけた模様

Source: http://www.renesys.com/

2012/12

- 2010年の中国による米国経路乗っ取りに関する詳細レポートがpublish
  - 50000程度のPrefixが影響を受けていた
  - 約15分程度の短い時間
  - USの重要機関等が標的になった模様





RPKIによるOrigin Validation

- DFZ上での不正経路を排除
- Cisco, Juniperでも順次正式にコードがリリース
- 徐々に普及が進んでいるが、まだまだ課題は多い
  - ROA情報の登録者（アドレスホルダー?）
  - ルーティングシステム全体への影響
    - 意図せずinvalidになってしまうケースが発生しうる
  - トラストアンカーの構造（5RIR?）
- JPNICを中心とした実証環境も本格展開の予定
- コンフィグ、コマンド等の参考例
  - http://www.janog.gr.jp/meeting/janog30/program/rpk.html
- RPKI Dashboardによる普及状況の観測（http://rpki.surfnet.nl/）

RPKI Dashboard

Breakdown per RIR

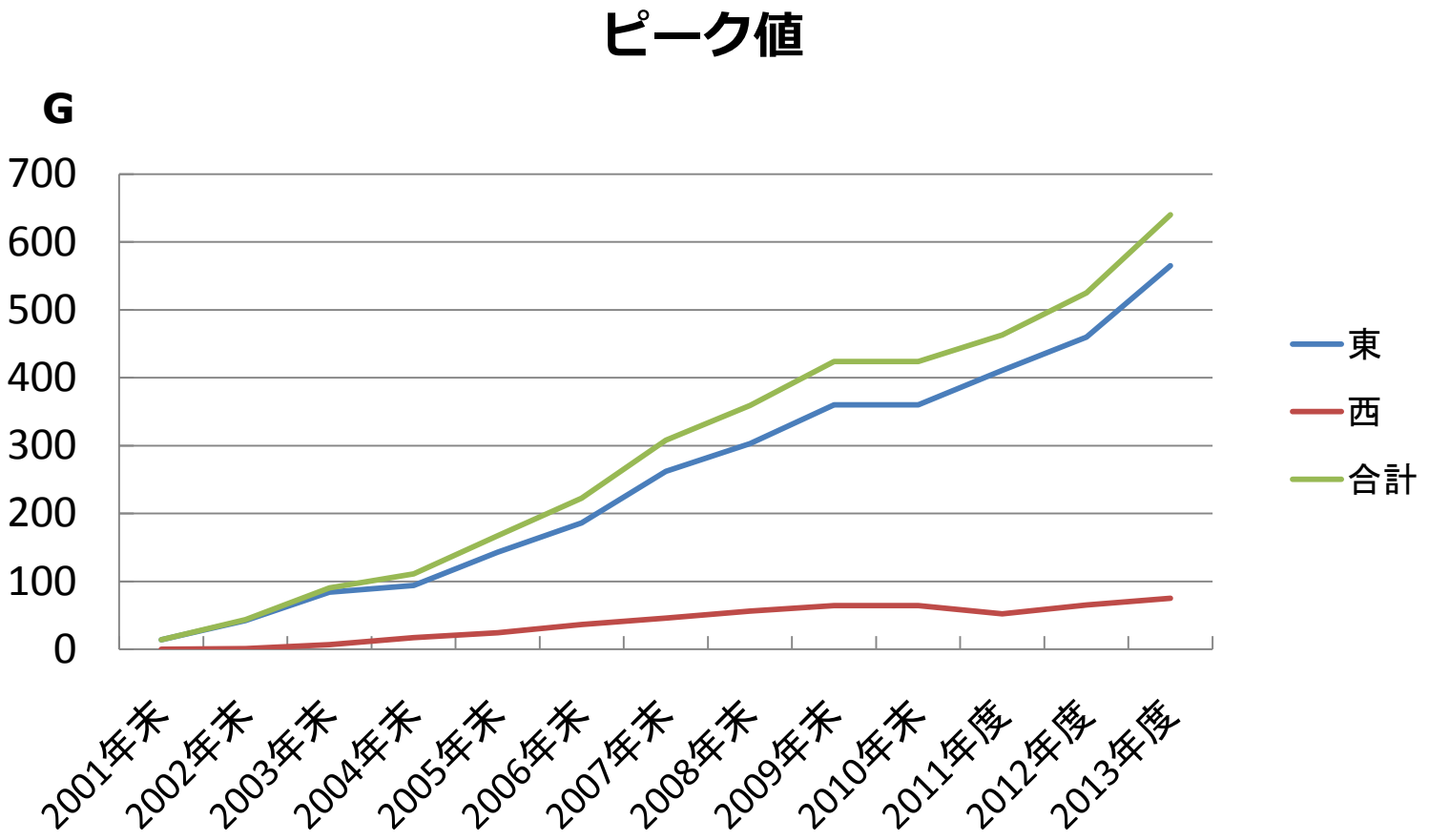
RIR	Total	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
RIPE NCC	131810 (100%)	7714 (5.85%)	1204 (0.91%)	122892 (93.23%)	86.5%	6.77%
LACNIC	62406 (100%)	11316 (18.13%)	1151 (1.84%)	49939 (80.02%)	90.77%	19.98%
ARIN	187396 (100%)	674 (0.36%)	103 (0.05%)	186619 (99.59%)	86.74%	0.41%
APNIC	119596 (100%)	168 (0.14%)	240 (0.2%)	119188 (99.66%)	41.18%	0.34%
AFRINIC	11462 (100%)	43 (0.38%)	44 (0.38%)	11375 (99.24%)	49.43%	0.76%

http://rpki.surfnet.nl/

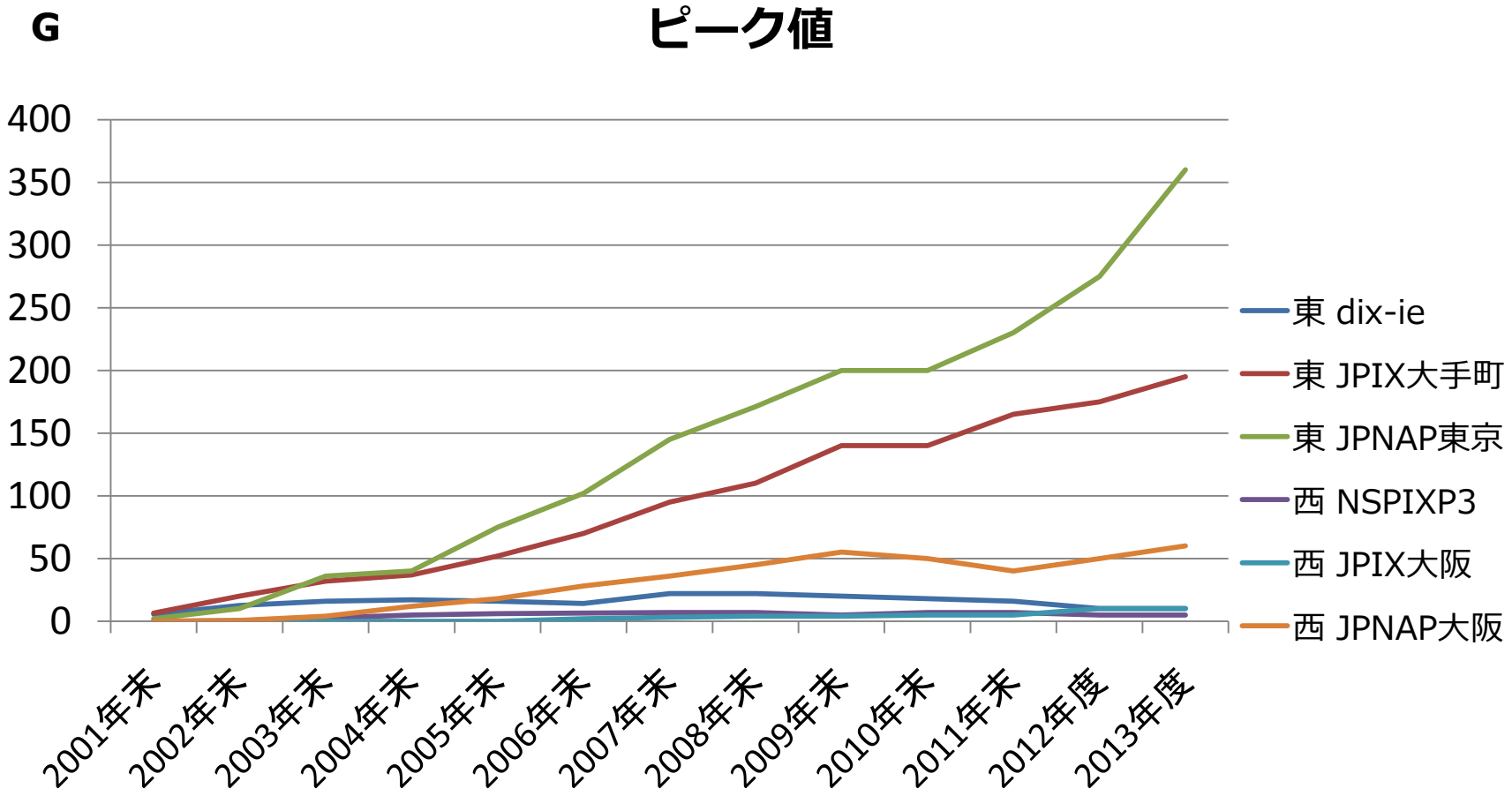
内容

- 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
- 日本や世界のIX動向
- まとめ

日本のIX トラフィックの推移（東西）



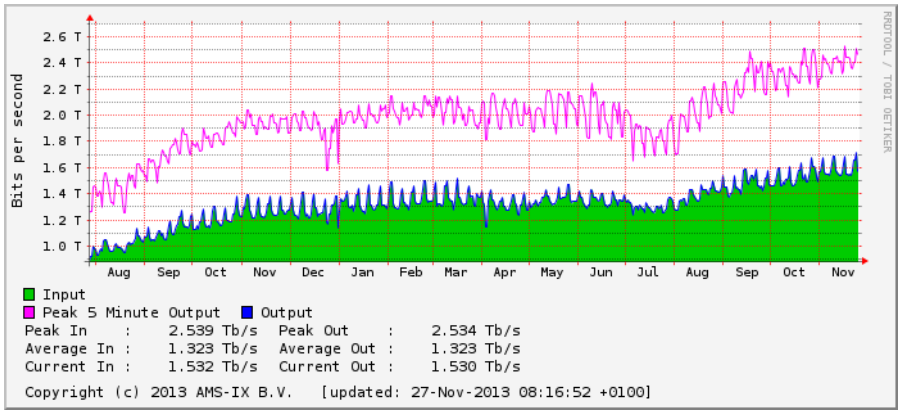
日本のIX トラフィックの推移



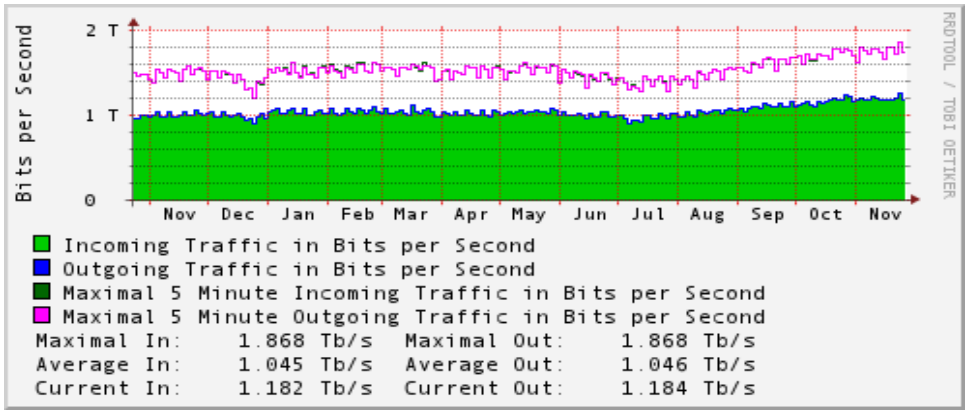
※dix-ie, NSPIXP3, JPIX大阪は推定値

4 Major IXs

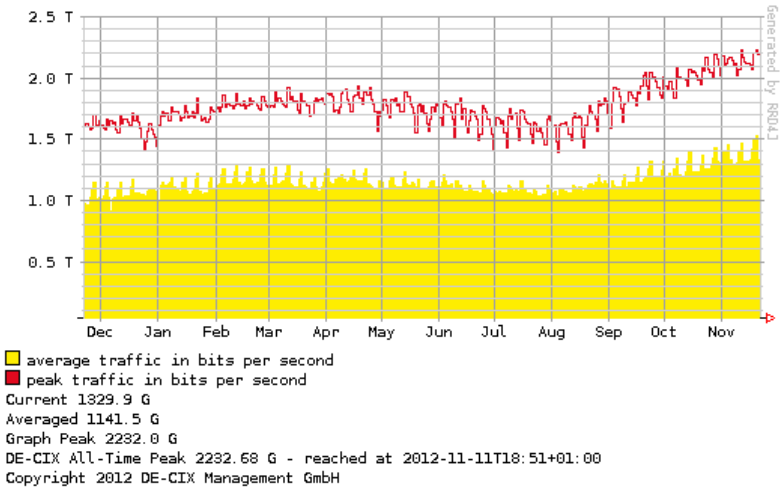
AMS-IX



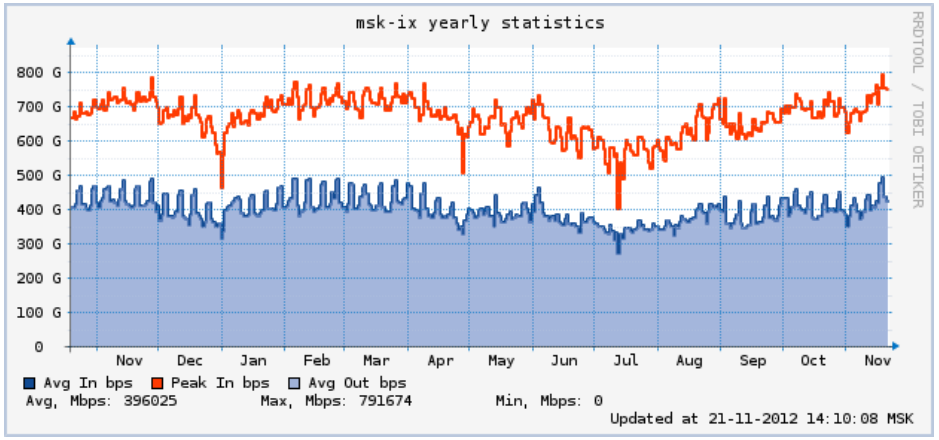
LINX



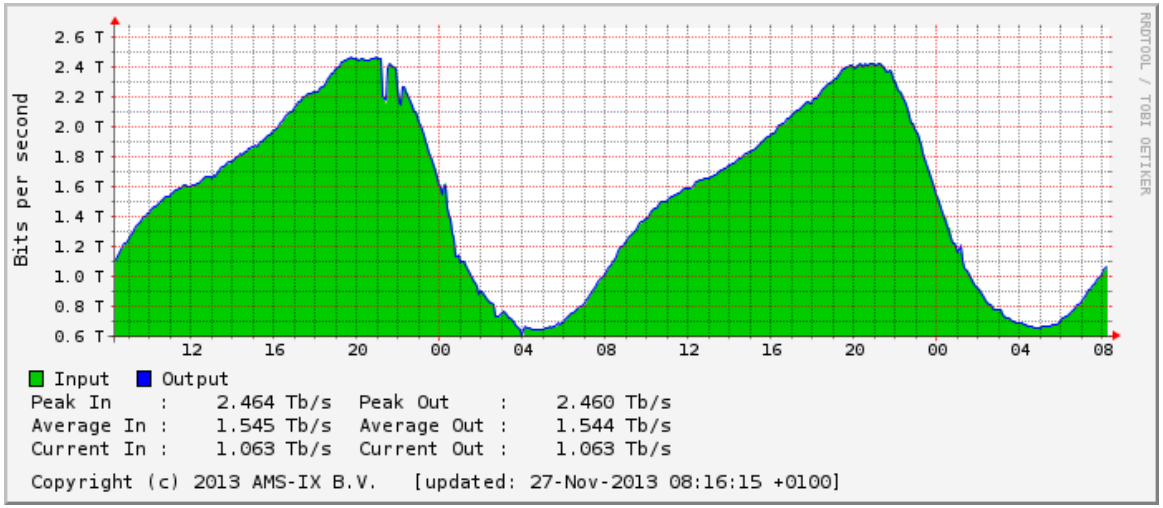
DE-CIX

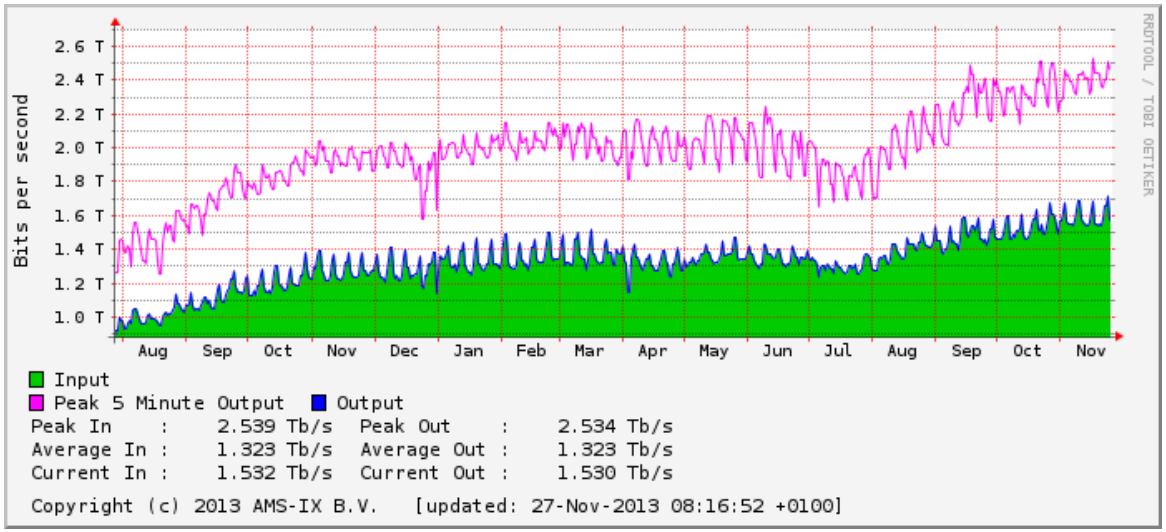


MSK-IX



AMS-IX





http://www.ams-ix.net/statistics/

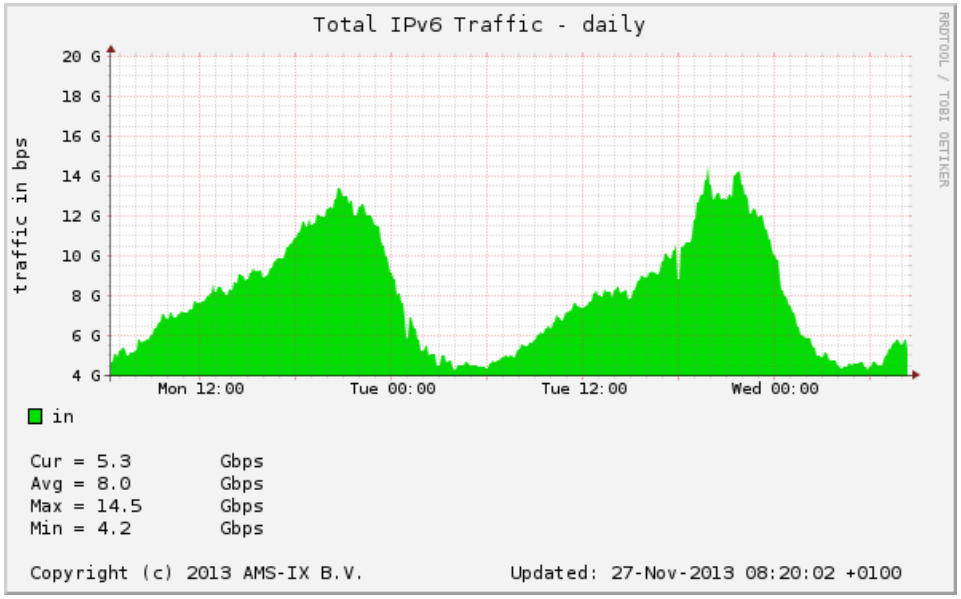
IXのアドレスを
/21から/20へ検討中

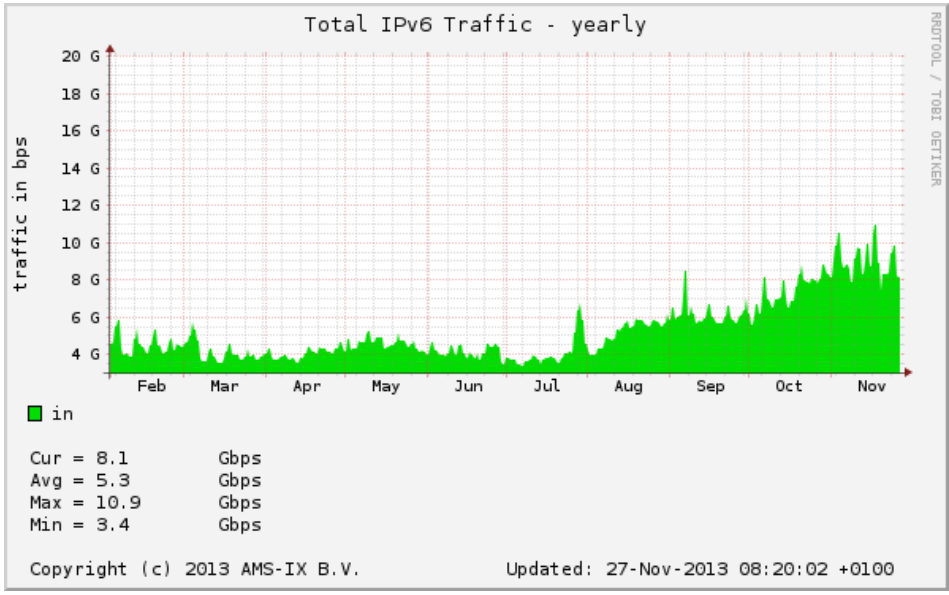
ピークは
20時～21時頃

夏以降増加
（例年同様）

AMS-IX：IPv6

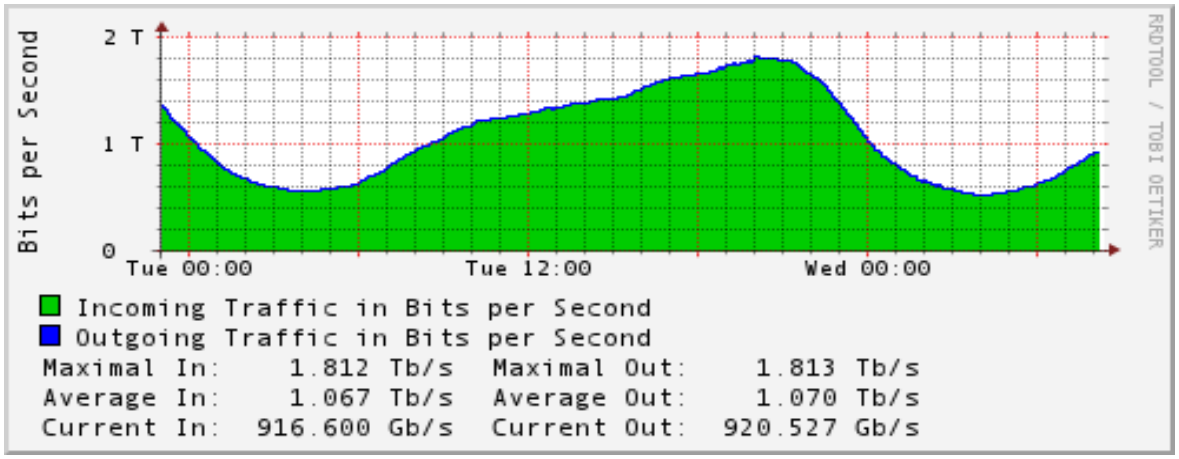
昨年より2～3倍程度増加
6月以降増加しているように見える

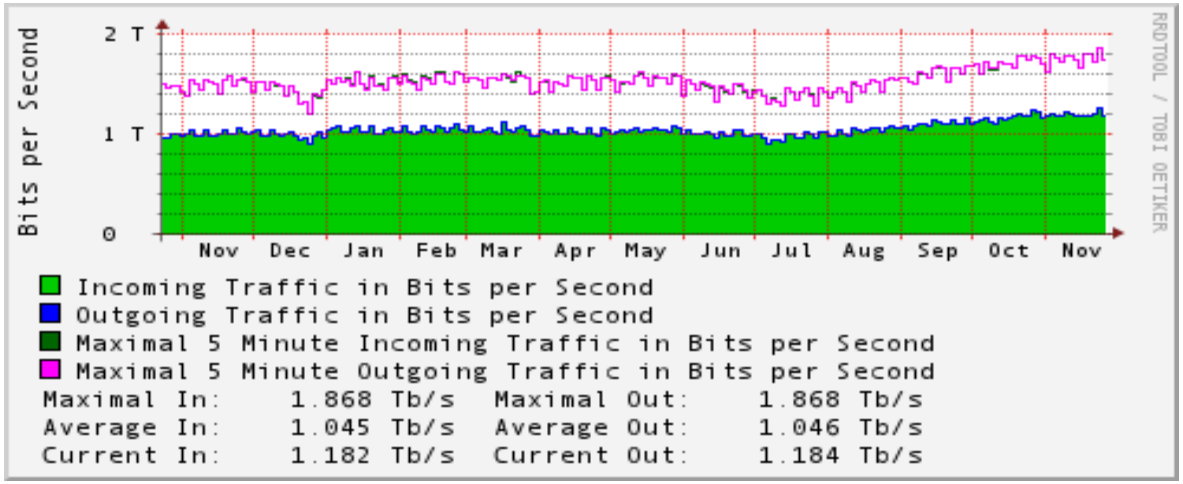




https://www.ams-ix.net/technical/statistics/sflow-stats/ipv6-traffic

LINX

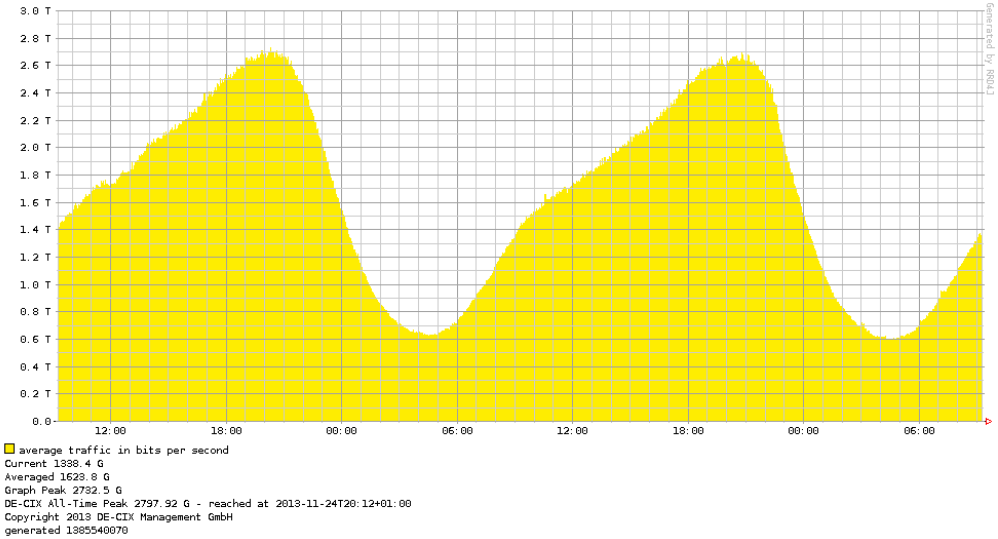


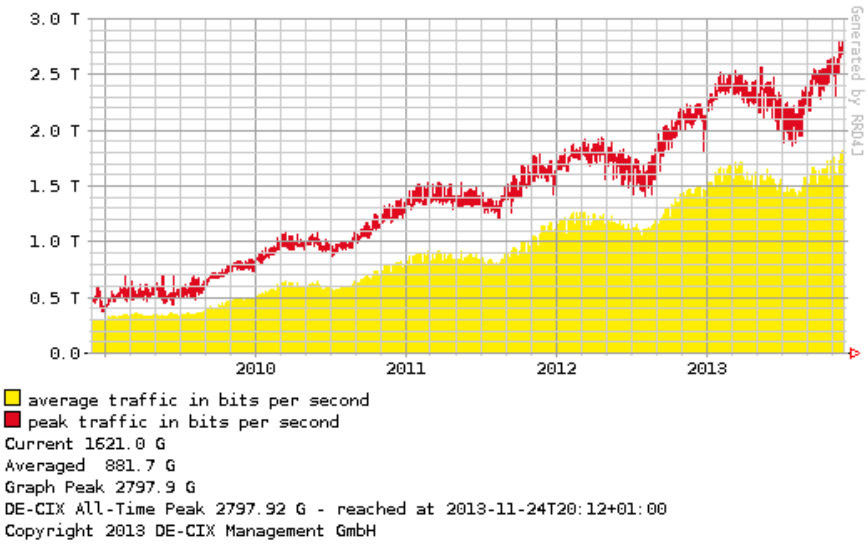


https://stats.linx.net/cgi-pub/exchange?log=combined.bits

DE-CIX

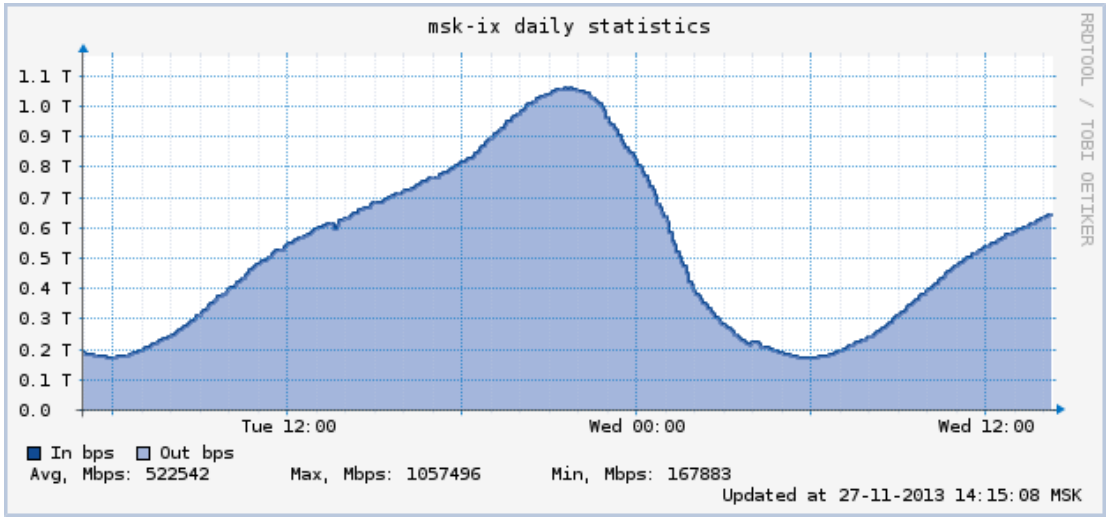
15 seconds average で sFLOWデータを元に描画

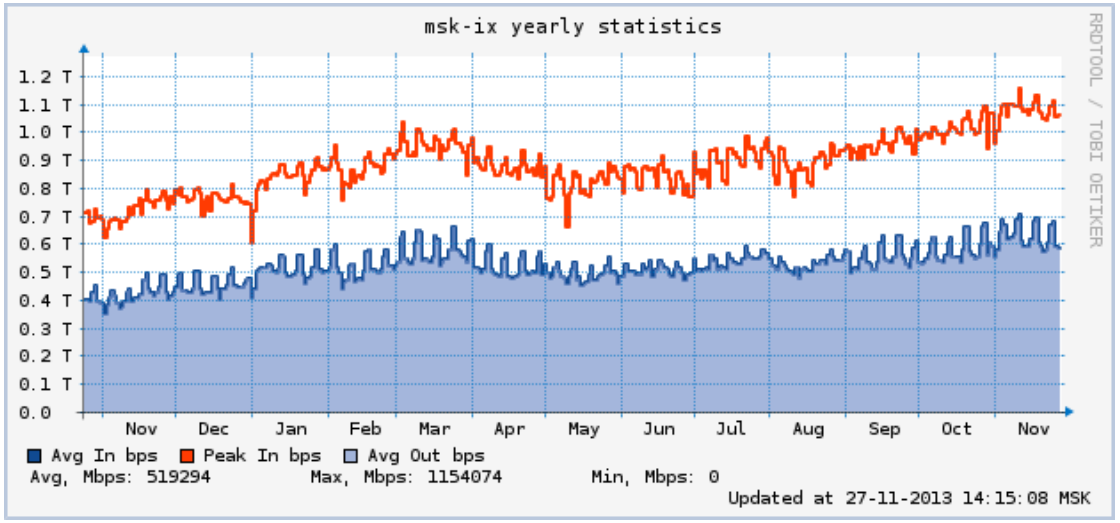




http://www.de-cix.net/content/network.html

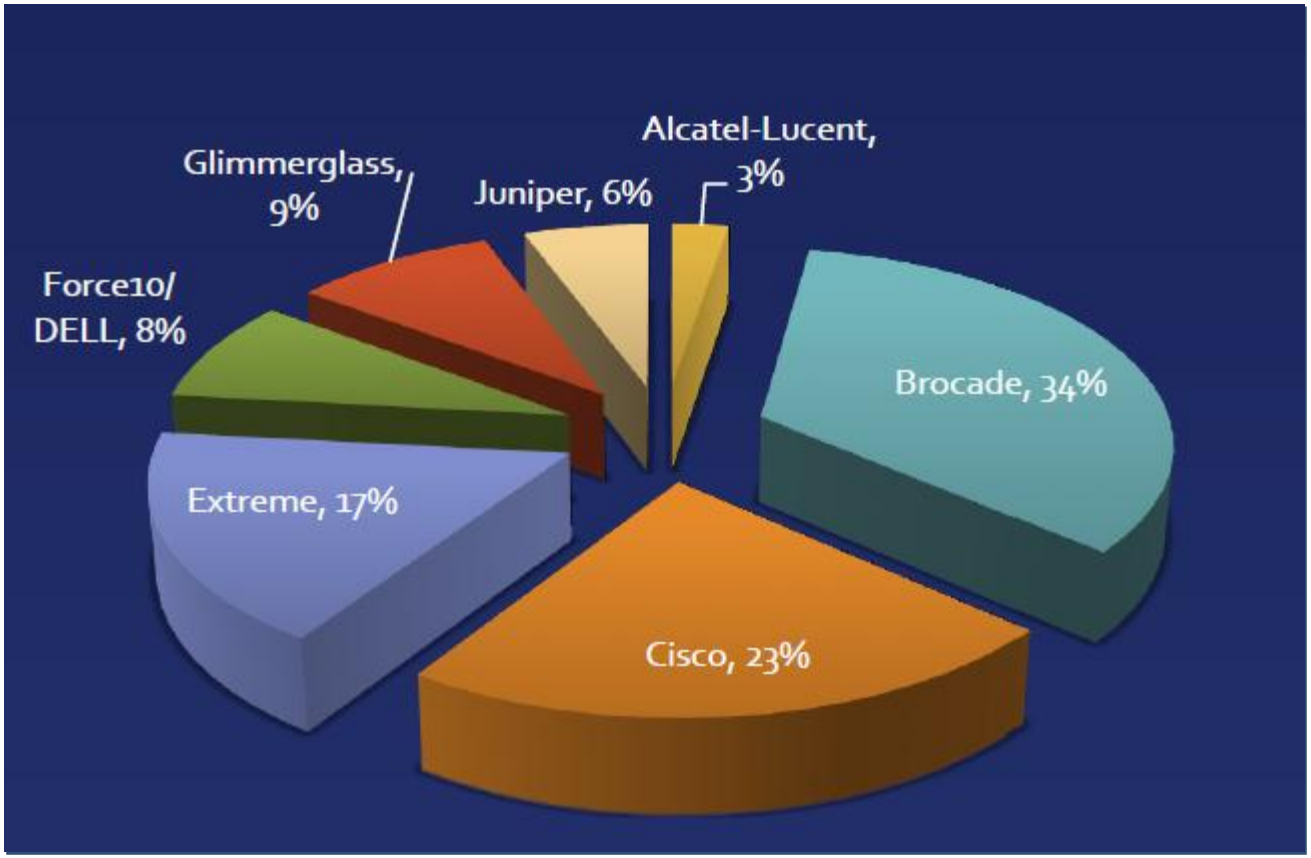
MSK-IX





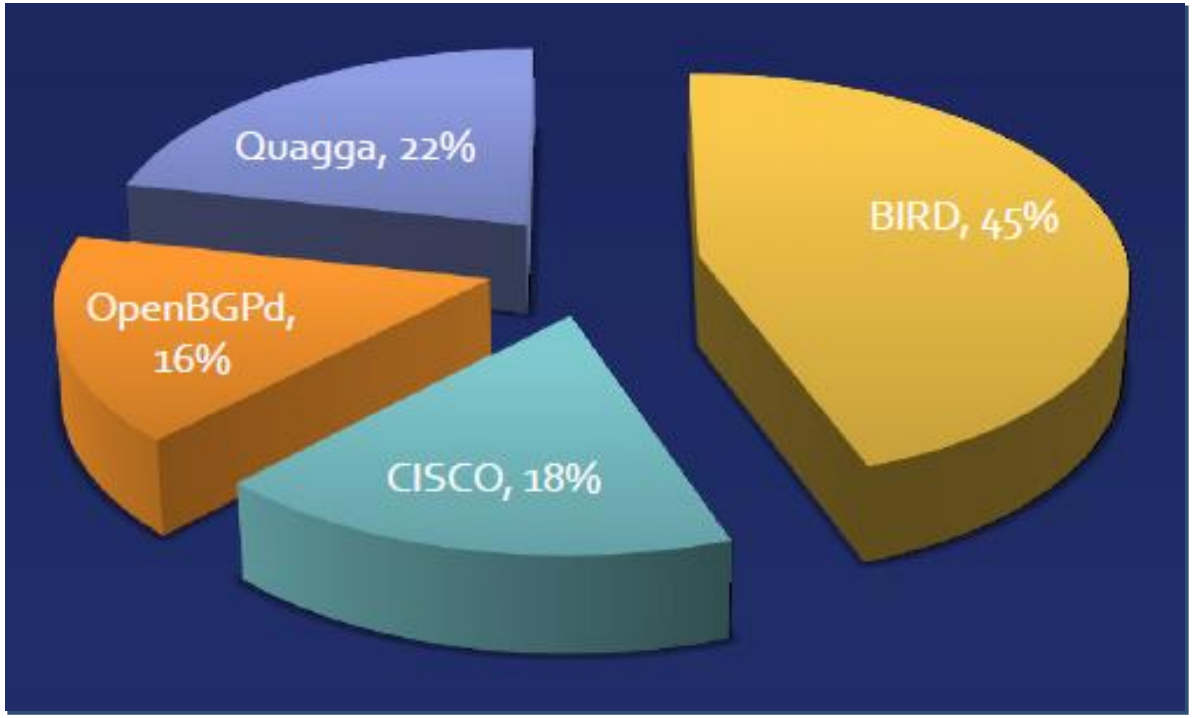
http://www.msk-ix.ru/network/traffic.html

Market share of vendors among EU IXPs within the Euro-IX Membership (%)



http://www.enog.org/presentations/enog-6/182-ENOG6_Kiev_FINAL.pdf

Route server daemons in use within the Euro-IX Membership (%)



http://www.enog.org/presentations/enog-6/182-ENOG6_Kiev_FINAL.pdf

2013年のまとめ

- トラフィック動向
  - 顕著に増加。スマホ等のモバイルトラフィックが継続的に増加（年1.7倍）
  - 急激なトラフィックの増減も観測、モバイルトラフィックは注意点も異なる
- ルーティング動向
  - 枯渇後もIPv4は依然増加、IPv6も単調増加
  - 2byteAS番号は残り500AS、2014年にIANAプールの枯渇が予想される
- DNS動向
  - オープンリゾルバ問題と共に解決に向けた取り組みが積極的に
  - Bind祭り等のセキュリティアップデートが相変わらず発生
- セキュリティ動向
  - 国際情勢に関わるサイバー攻撃は今年も確認された
  - フィッシングサイト等には引き続き注意が必要
- 日本や世界のIX動向
  - 増加率はそれほど大きな差はないが規模は世界のIXが約５倍程度
  - IPv6通信量はまだ1%未満。これからの動向に注目