# 2014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

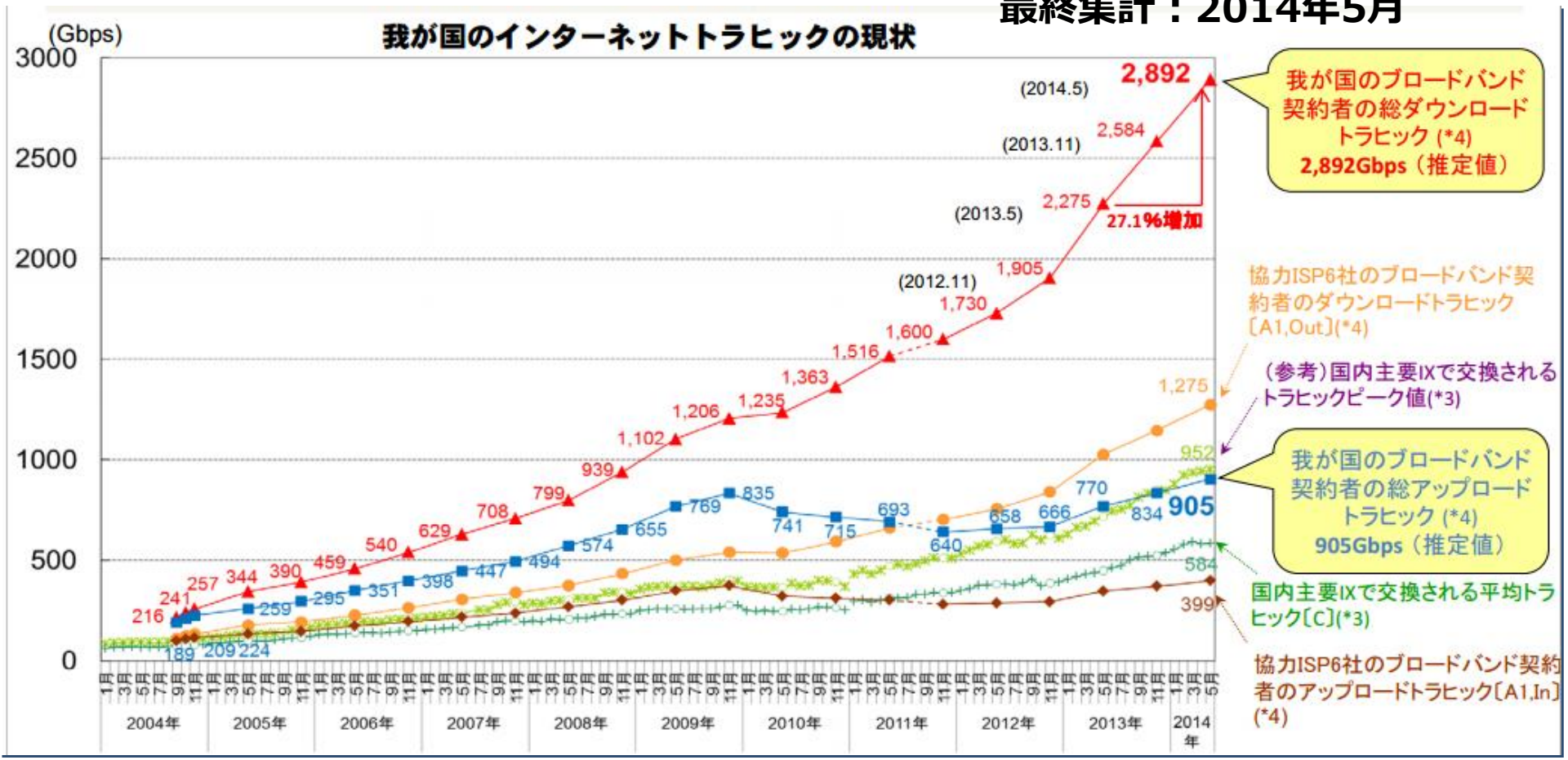
- トラフィック動向
- ルーティング動向
- DNS動向
- セキュリティ動向
- 日本や世界のIX動向
- まとめ

# 2014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3Tbps近くに
  - スマートフォンの普及によるモバイルトラフィック増　年1.5倍程度の伸びへ（伸び率微減）
  - 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）が加速している一方で、クラウドサービスの活用により、アップロードのトラフィックも増加してきた
  - モバイル：帯域制限により月末にかけて減少する傾向は継続
  - ショートパケットが増えており、利用している通信機器の制限等に注意が必要
- 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がさらに急増
  - Googleが検索結果にSSL化を反映したり、各種サービスをHTTPS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
  - Wcup2014、iOS8ダウンロード、各種update等で急激な増減が観測
- 給料日の金曜日2次会探し。。

# 日本国内のトラフィック推移

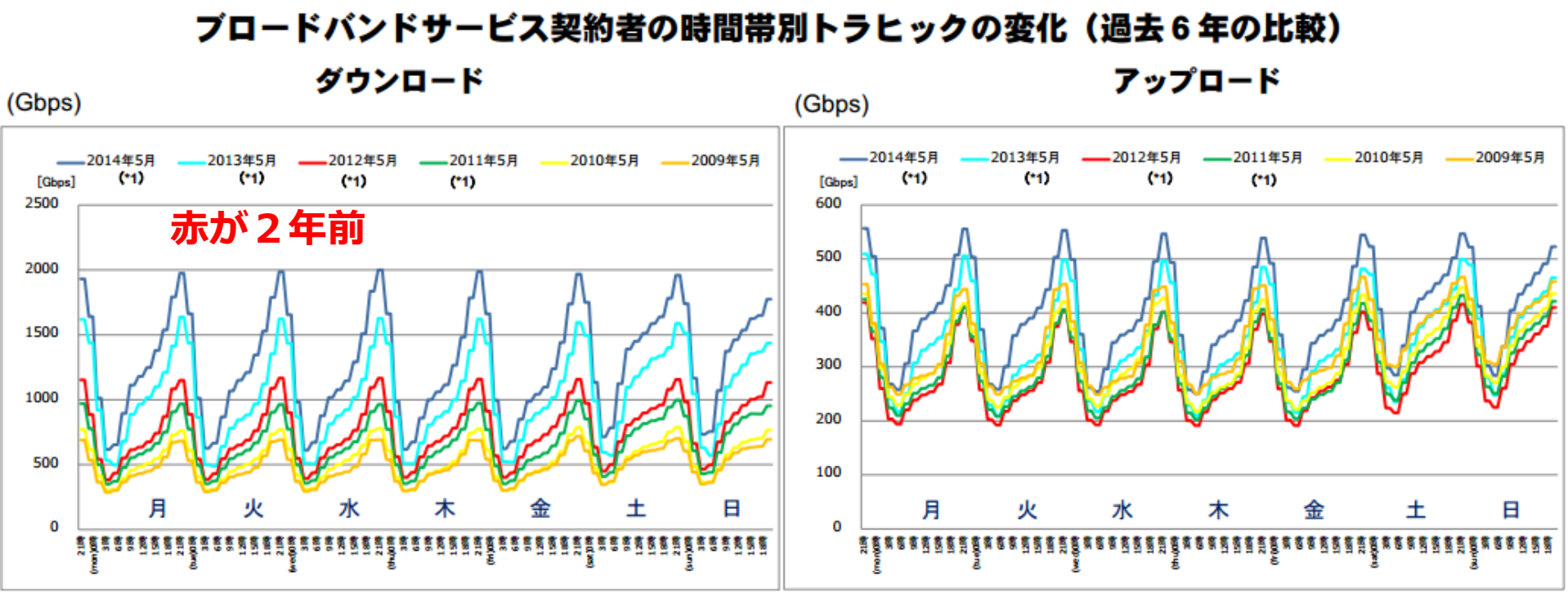
**最終集計：2014年5月**




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**」　2014年10月7日
http://www.soumu.go.jp/main_content/000316564.pdf

# 日本国内のトラフィック推移

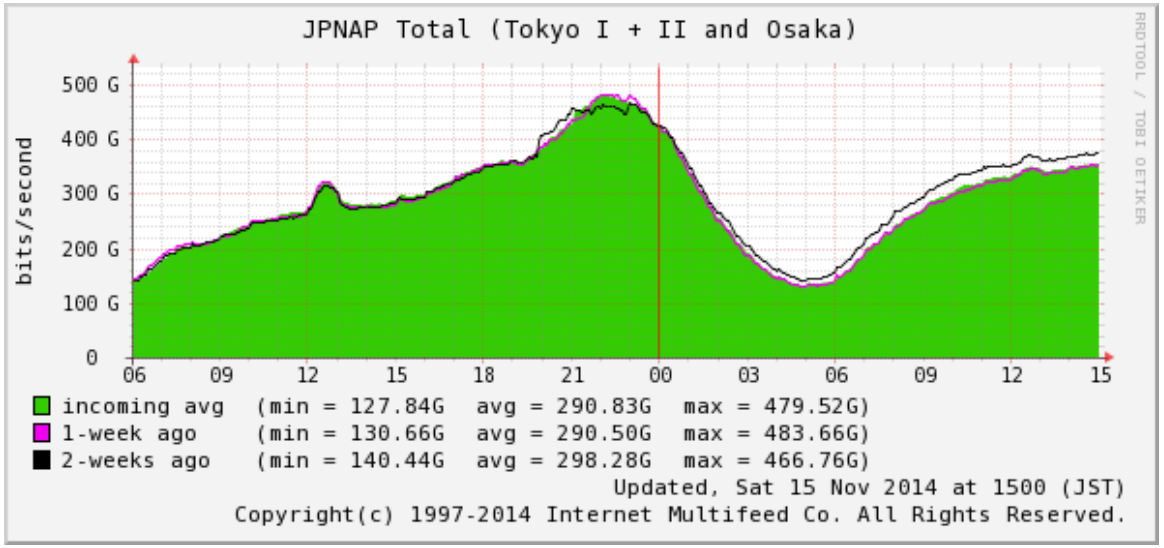
5分平均のピークトラフィックの推移



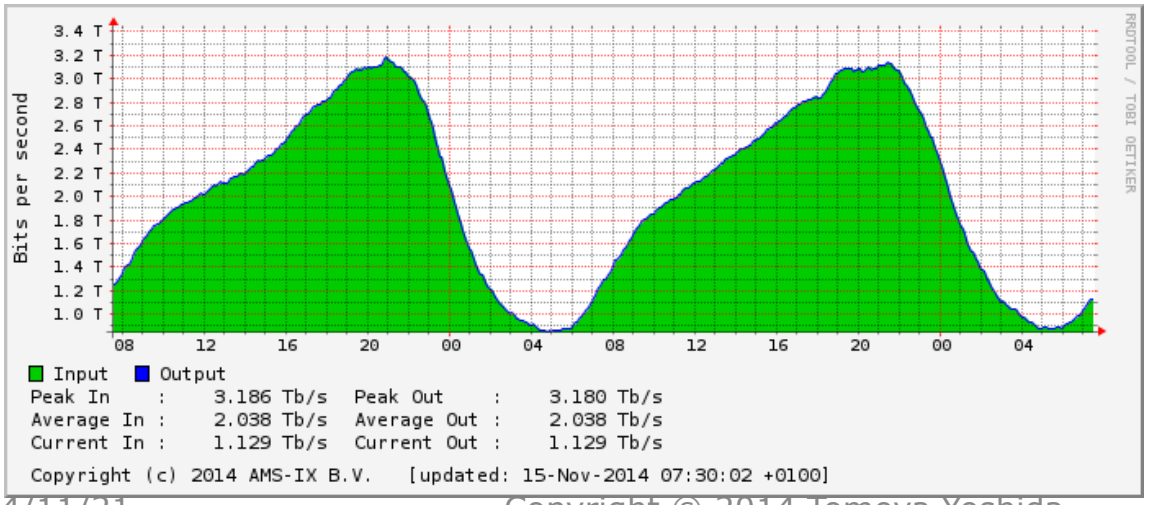

出典：総務省「**我が国のインターネットにおけるトラヒックの集計・試算**」　2014年10月7日
http://www.soumu.go.jp/main_content/000316564.pdf

# 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
日本のお昼のトラフィックは特徴的



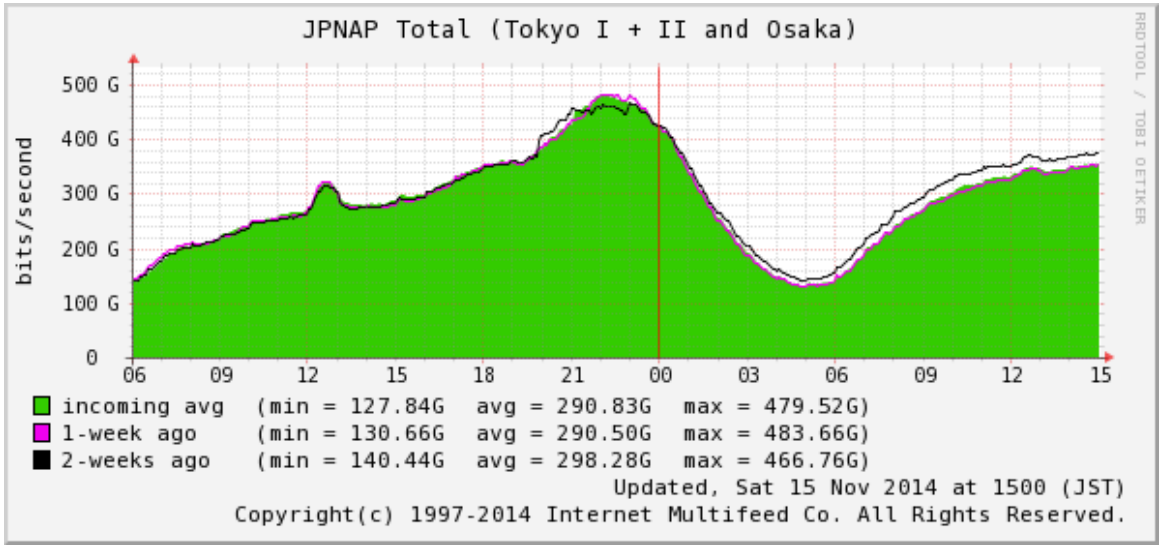

JPNAP(Japan)の
1日のトラフィック推移



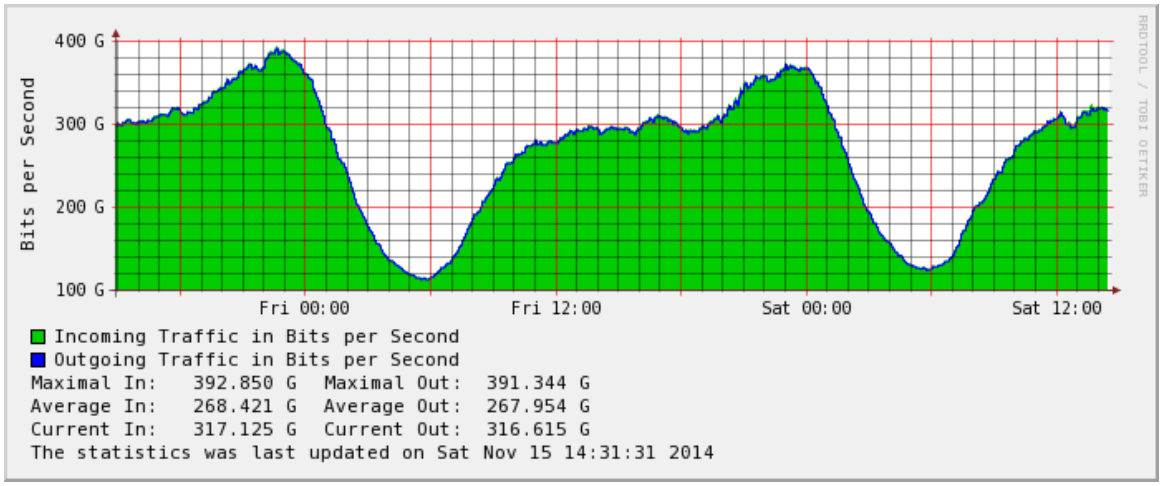

AMS-IX(Europe)の
1日のトラフィック推移

# 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



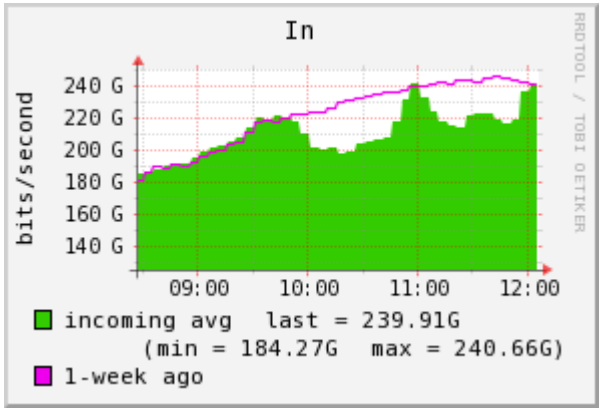

JPNAP(Japan)の
1日のトラフィック推移

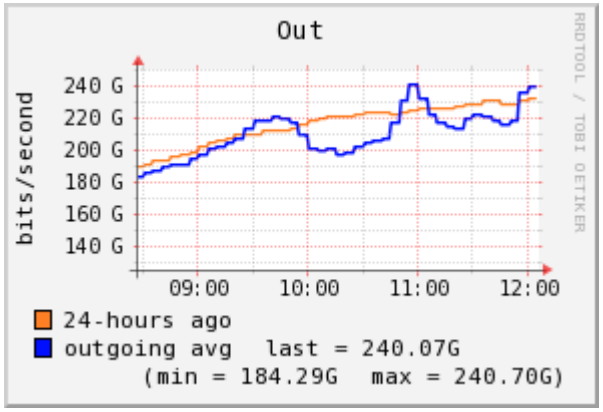


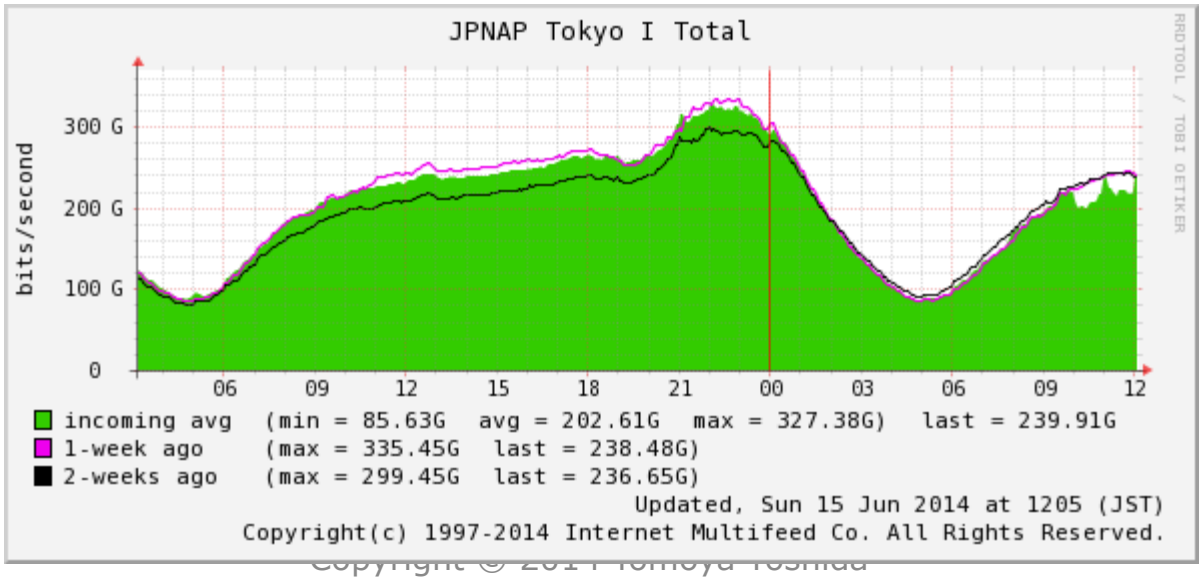

HKIX(香港)の
1日のトラフィック推移

# Worldcup2014 6/14(土) 日本vsコートジボワール

- ハーフタイムを境にトラフィックが減少
  - 最大15%(前半)の減少を観測

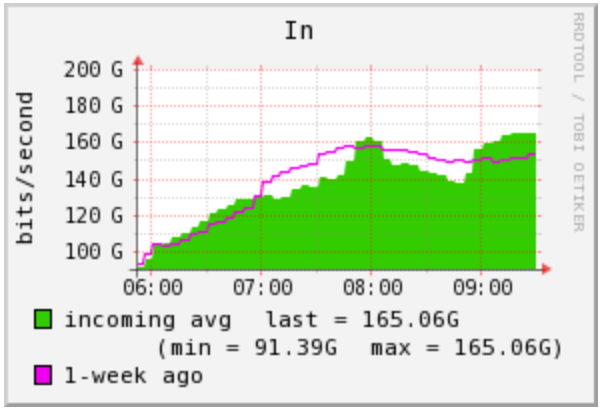


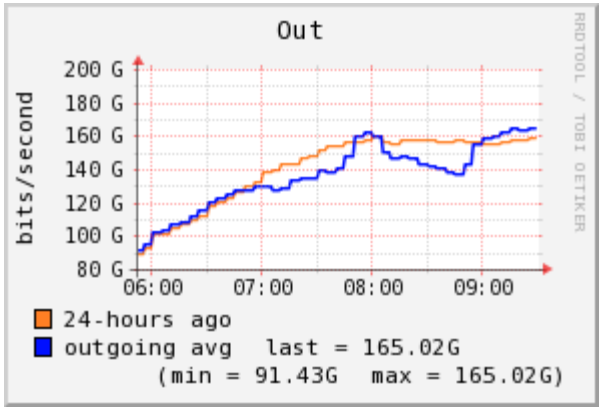



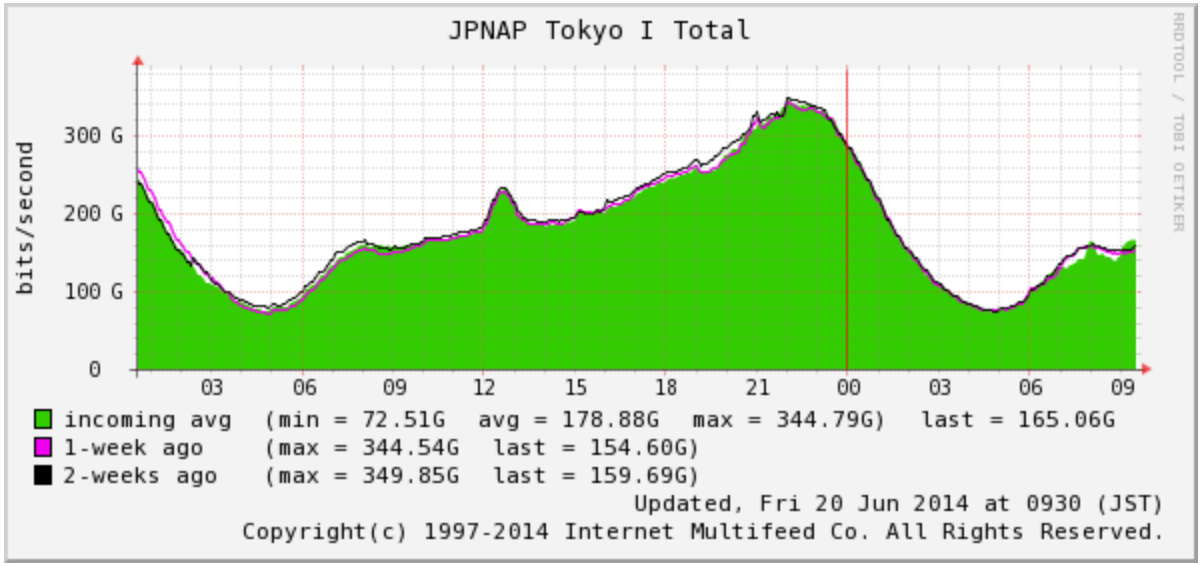



# Worldcup2014 6/20(金) 日本vsギリシャ

- ハーフタイムを境にトラフィックが減少
  - 最大10%(後半)の減少を観測

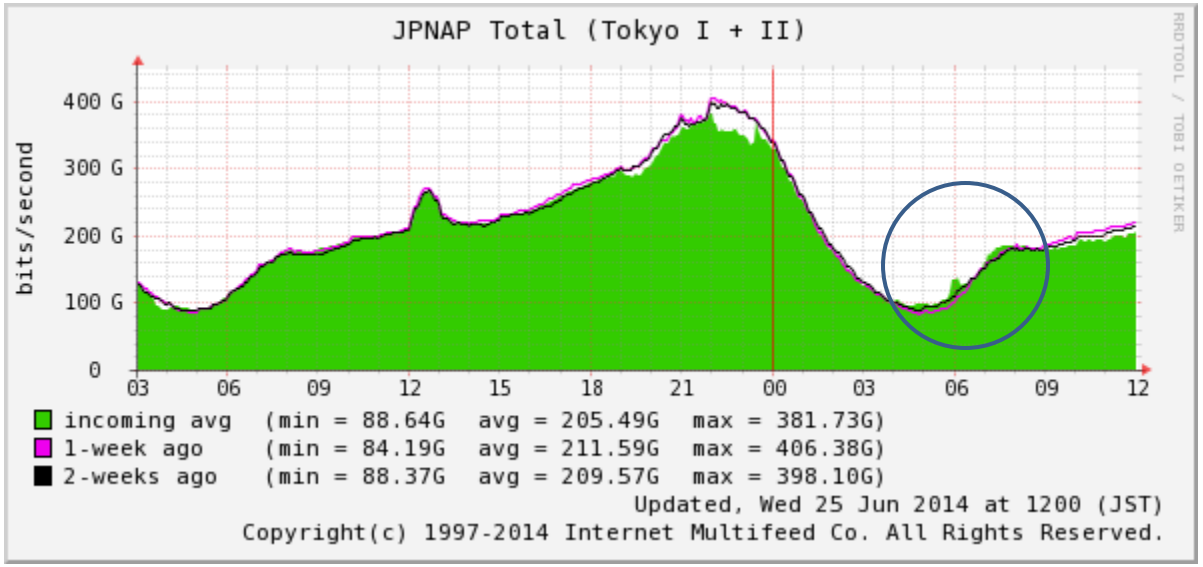


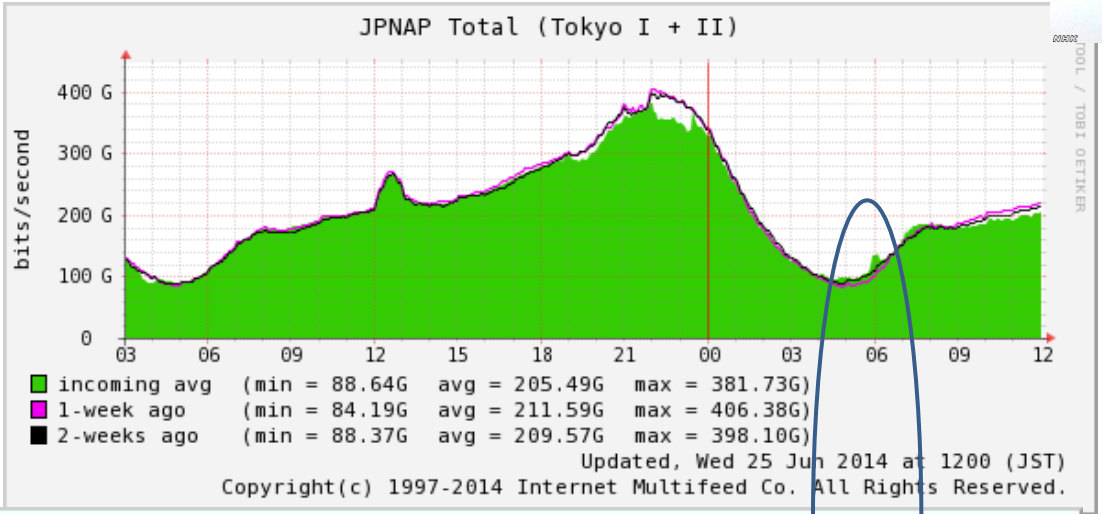
# Worldcup2014 6/25(水) 日本vsコロンビア

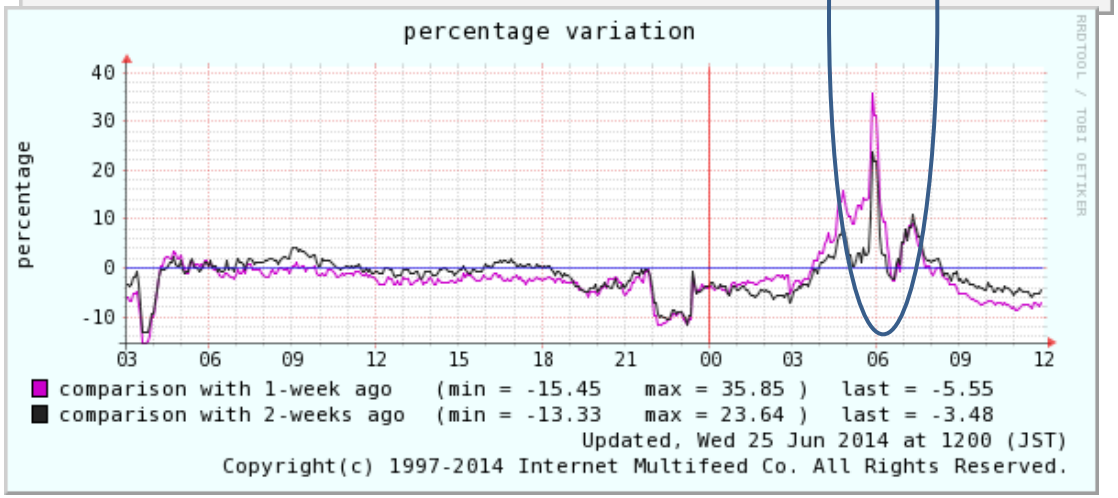
- 早朝時間帯により減少は見られず、むしろ増加
  - 普段寝ている人（インターネットは当然やっていない）人がテレビを見る



# Worldcup2014 6/25(水) 日本vsコロンビア

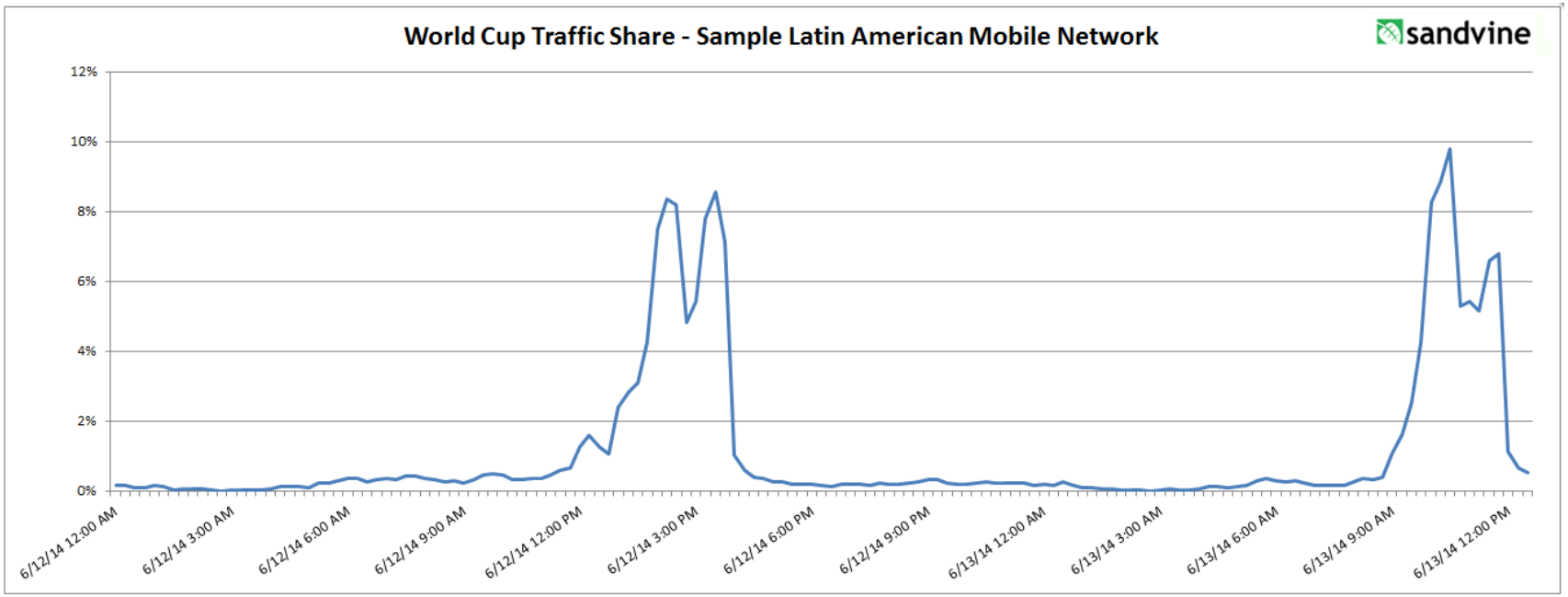
- なんと朝6時に36%増加（対１週間前）---岡崎効果
  - 試合開始前～終了後で合計４４４万ツイート
  - 携帯からコンテンツを参照したトラフィック等も増加

# Worldcup2014 ラテンアメリカの例

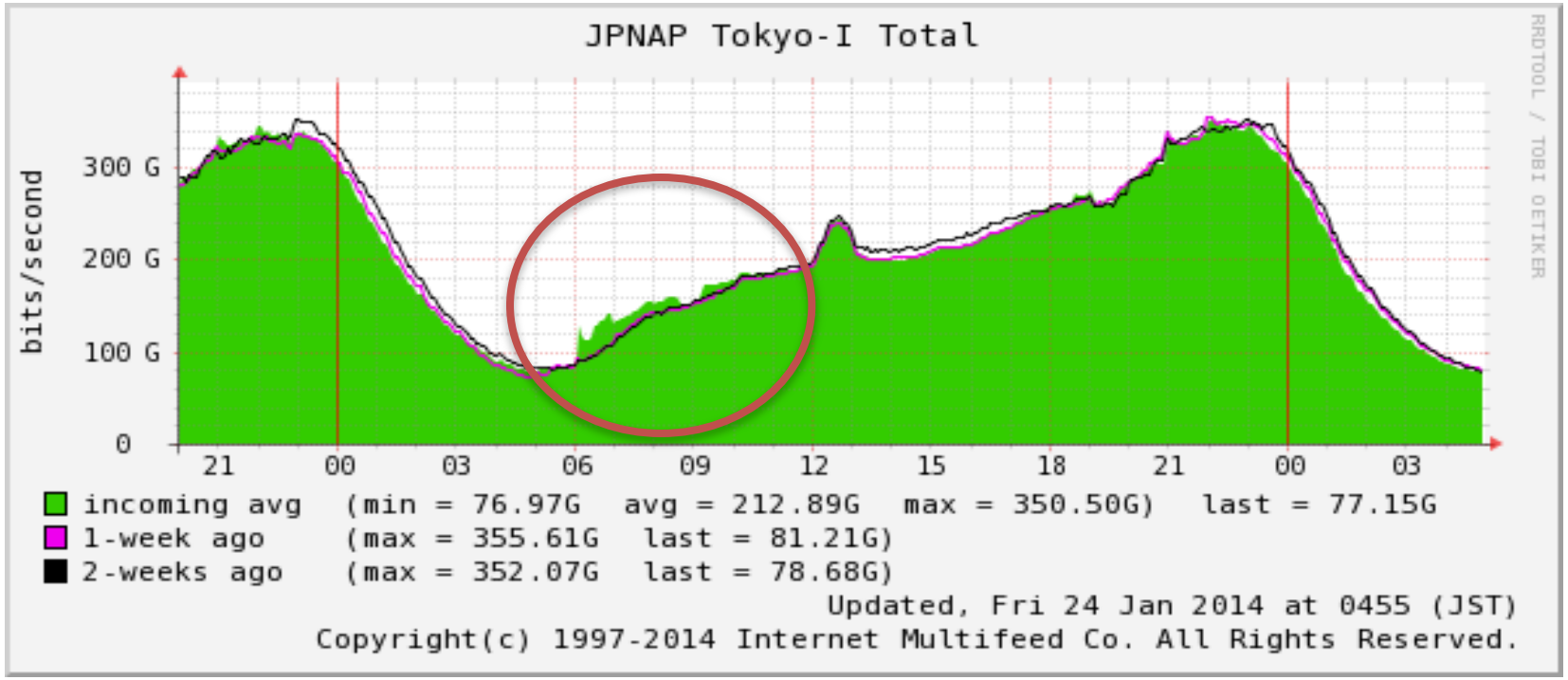
- ラテンアメリカのmobile networkでは、通常時と比べて10%程度伸びがあったとのレポートもある
- ハーフタイムはトラフィックが少なくなる




http://www.internetphenomena.com/2014/06/world-cup-week-one/

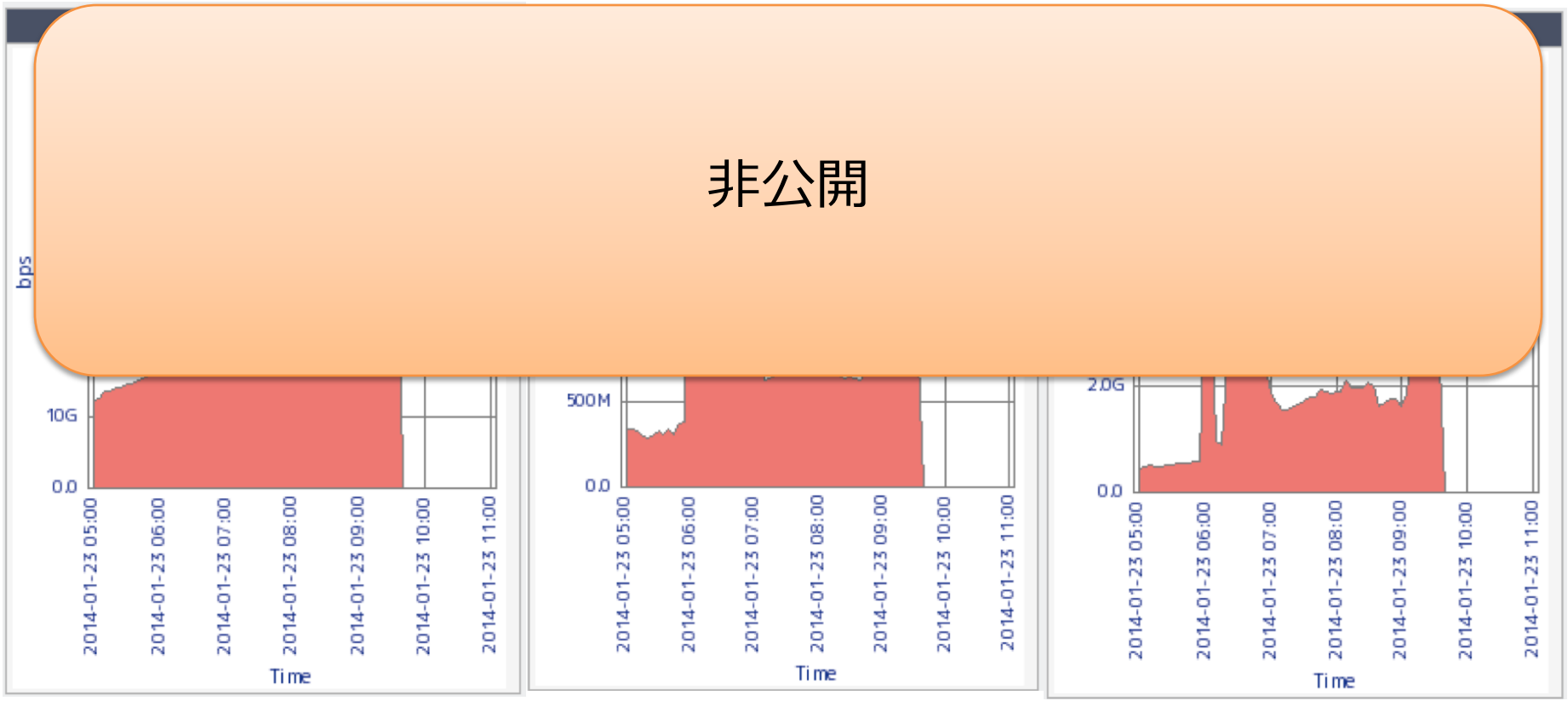
# 2014/1/23(木)

- 朝6時から急激なトラフィック増との連絡あり
  - ん、6時？？



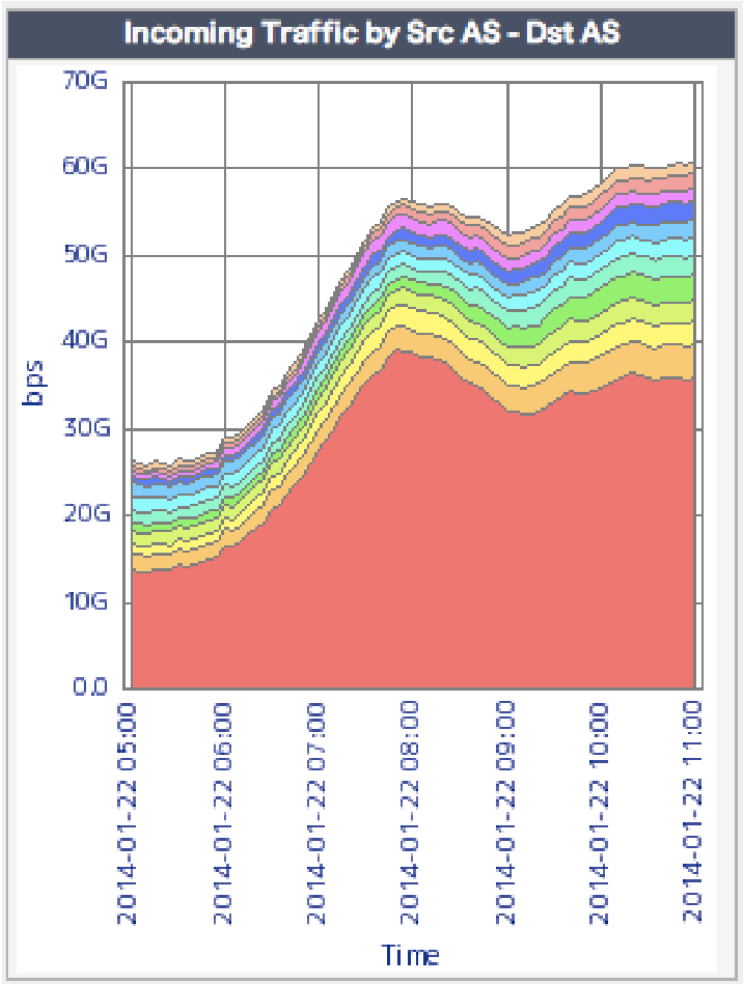
# 2014/1/23 (木)

- 某ASの方々の様子
  - なんだかあるところを中心にトラフィックが急変動している？

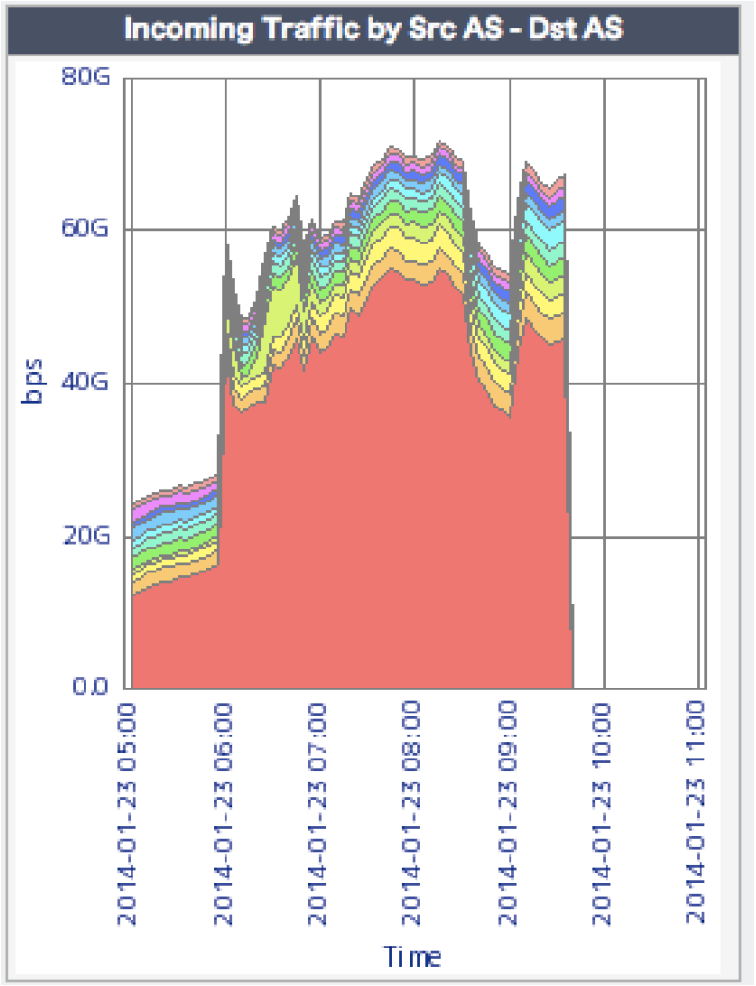


# 2014/1/23 (木)

通常時



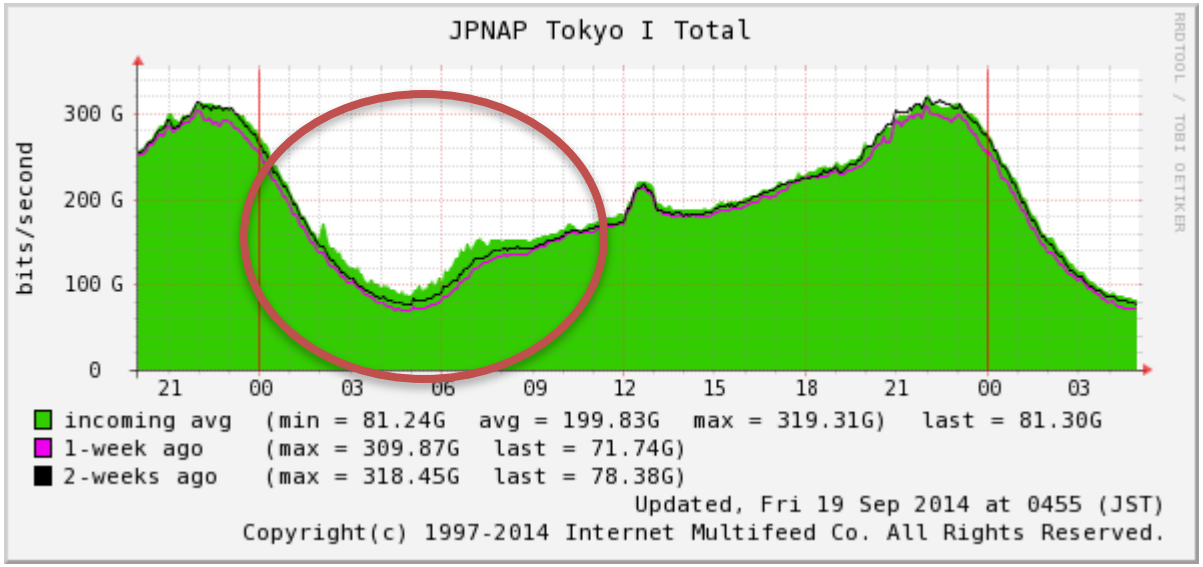

朝６時からダウンロード開始




パズドラのアップデートが開始（6時開始が多い）

# 9/18 iOS8 update

- 20Gが一瞬で埋まる (JPNAP)
- 夜中の2時開始、いい具合にトラフィックが乗ってくれた。。
  - 普段沢山流れていない時間帯だと幸せですね。

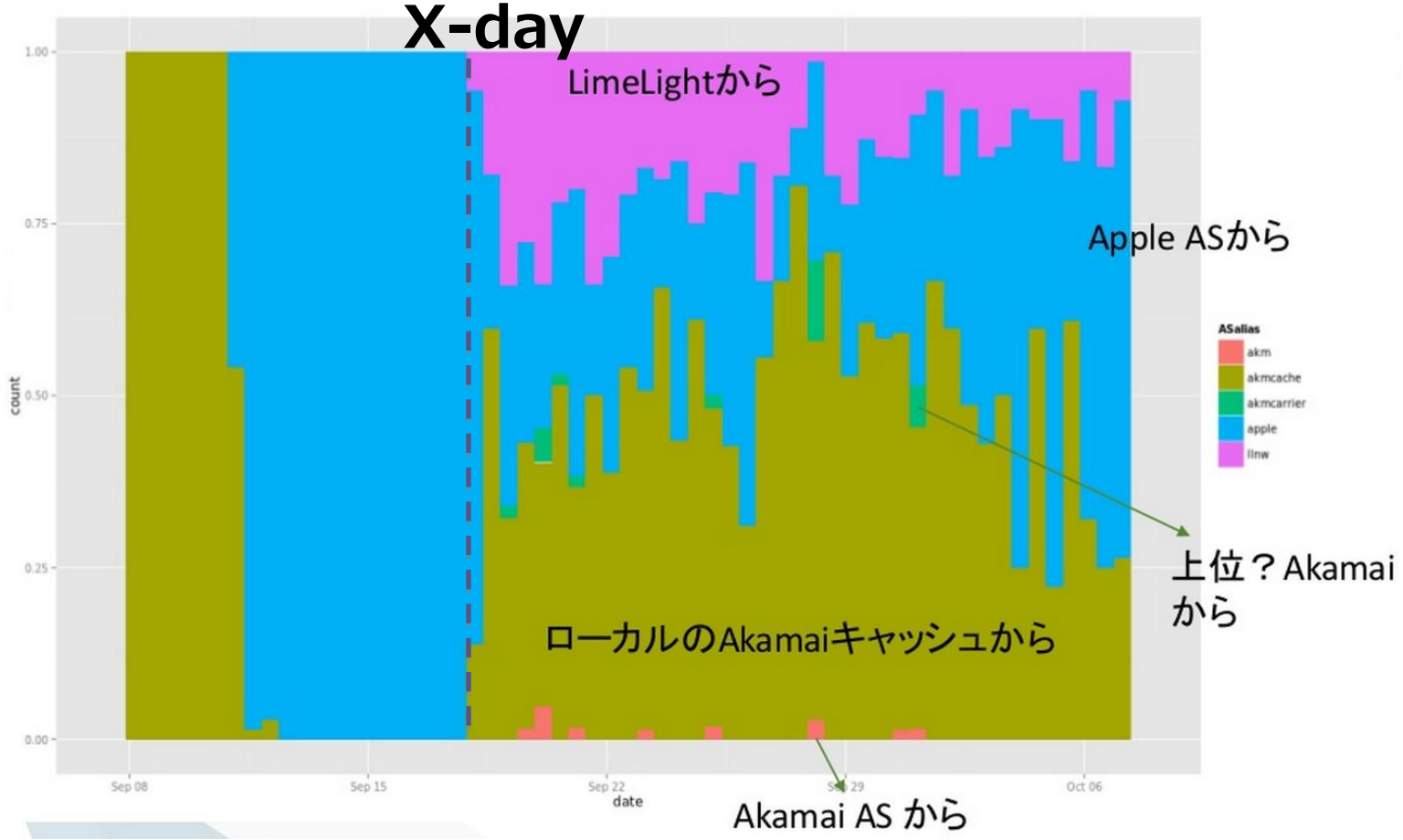



- Mobile端末はwifi経由のみでupdate可、だが何故かLTE等が増加？
  - 携帯端末ショップのwifiのアップリンクがLTEだった…
  - Pocket wifiを利用してupdateした…

# iOS8 update の様子

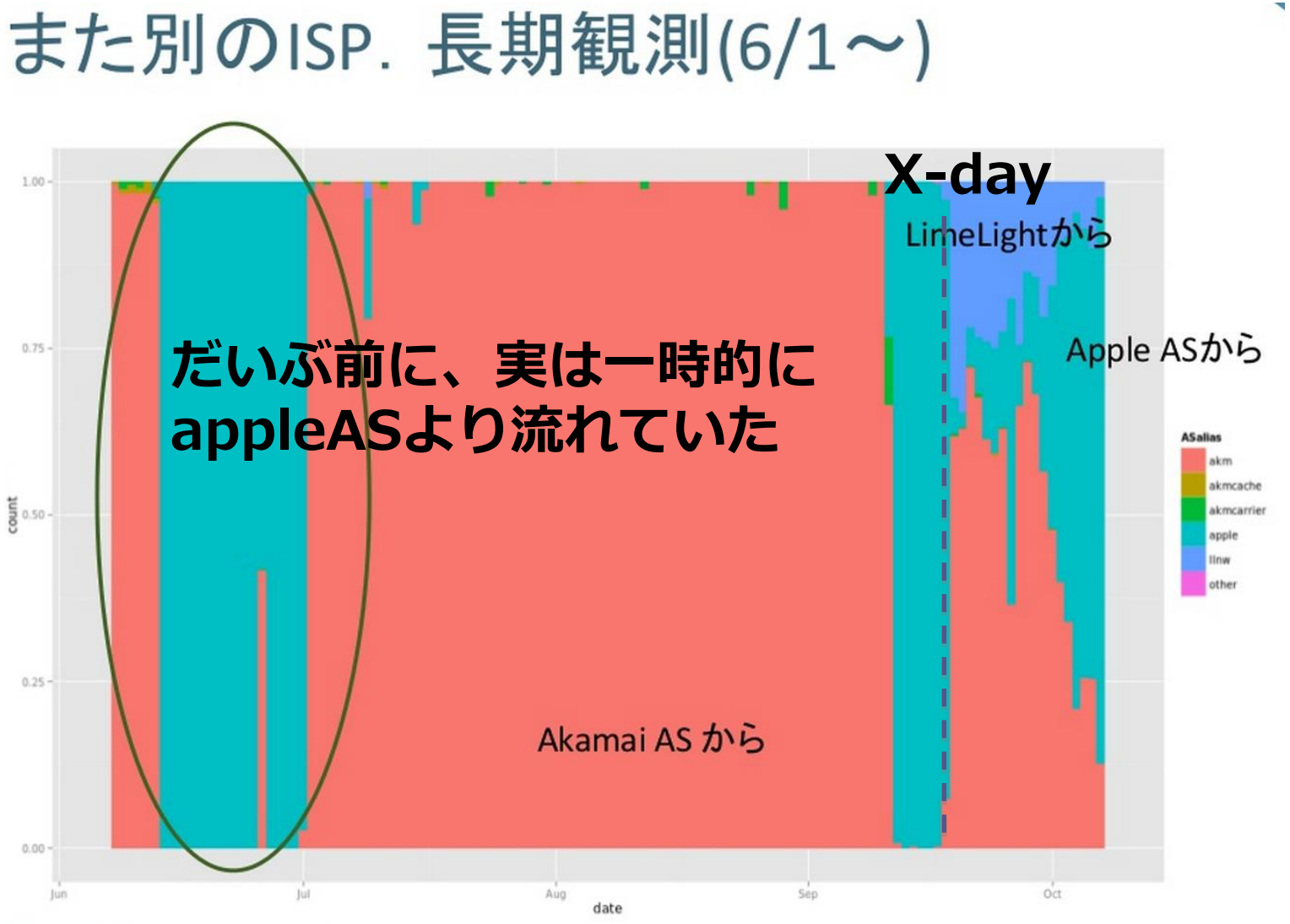
## あるISPのiOS配信前後の状況(12時間毎)

配信元FQDNを30分毎に名前解決し，データ取得元ASで分類したもの．
9/8～10/7まで．12時間毎の統計値(率)．




http://www.slideshare.net/kameisatoshi/20141006-jpnap

# iOS8 update の様子

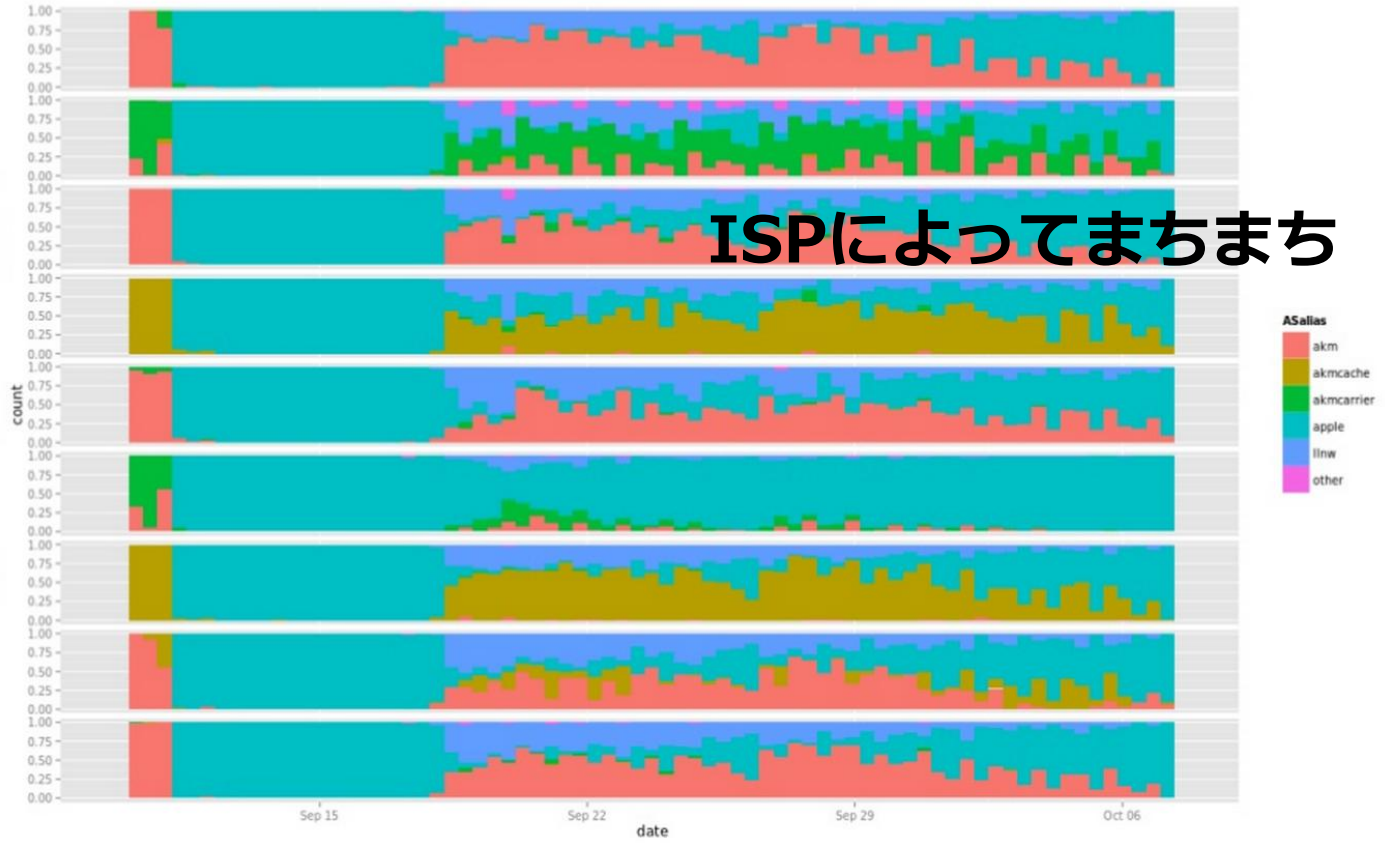



http://www.slideshare.net/kameisatoshi/20141006-jpnap

# iOS8 update の様子

## iOS8アップデートにおけるISP毎の配信元

基本的にAppleASから流し，一定キャパを越えた時点でLimeLight と Akamaiを
併用して流していると推測できそう.
キャッシュの有無はあまり関係ない模様(Akamai側マター？).

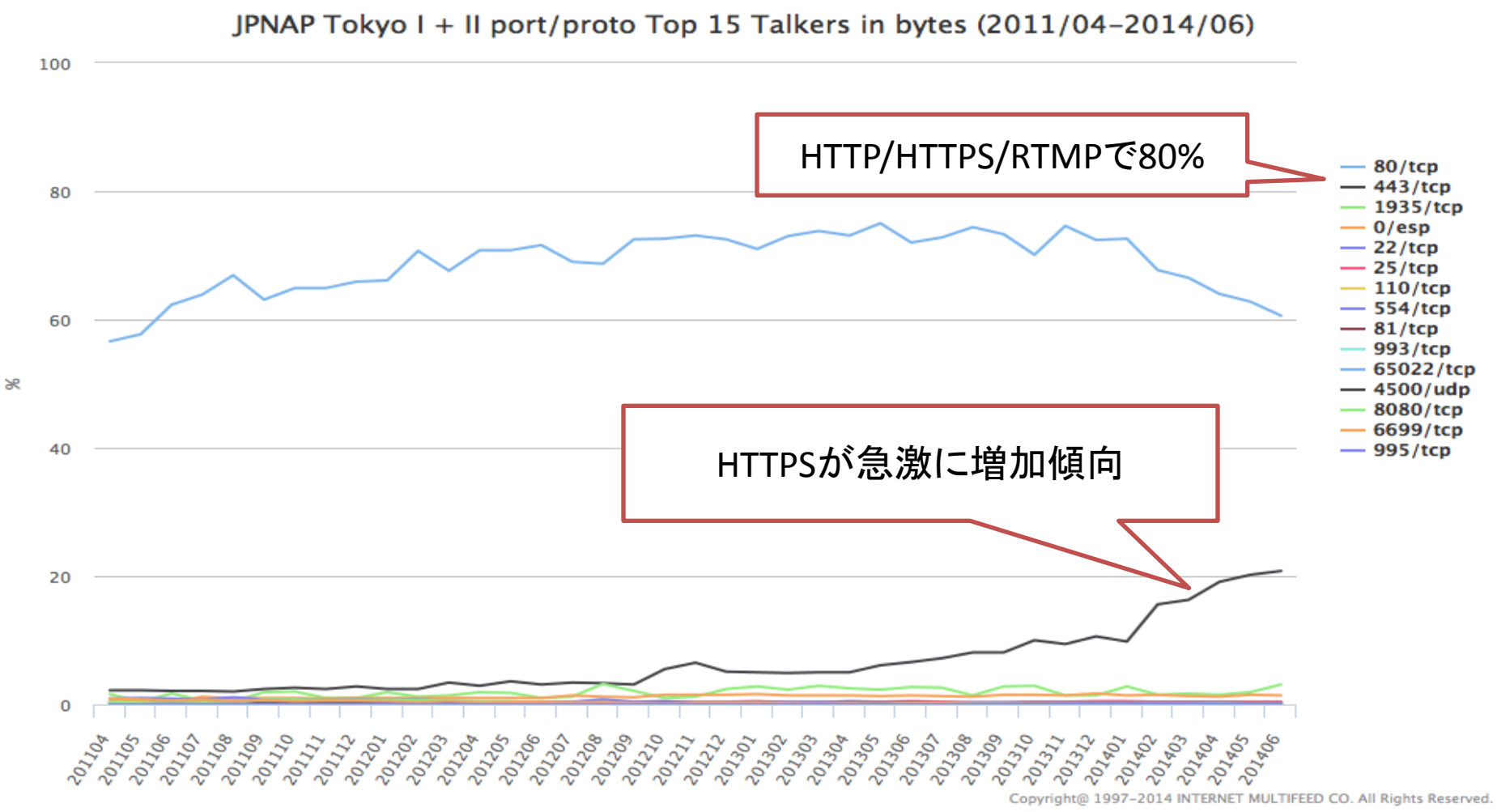



http://www.slideshare.net/kameisatoshi/20141006-jpnap

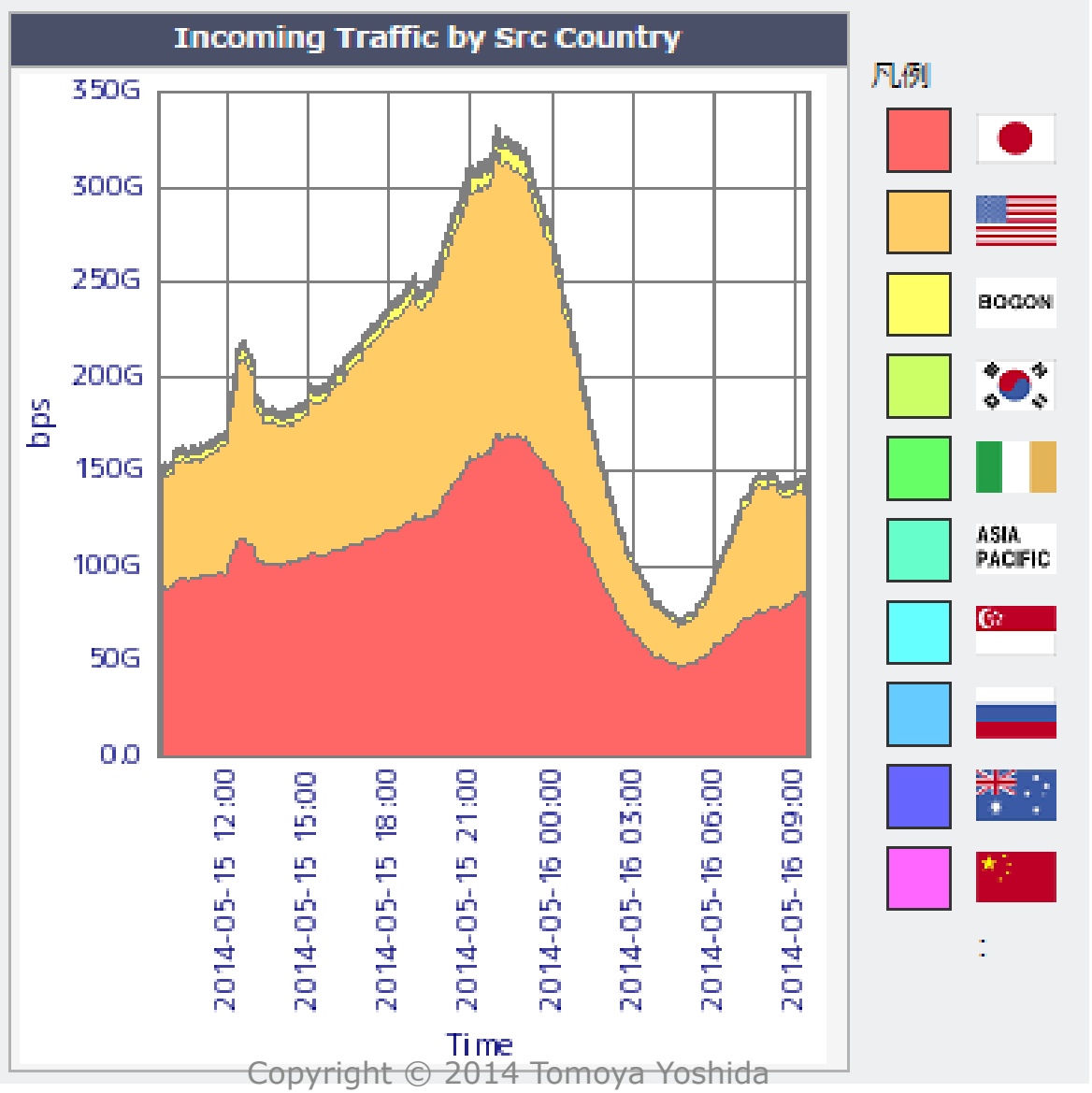
# トラフィックの急激な変動

- 何が異常で何が正常か？
- 監視しよう
  - 閾値での監視は出来ないことはないです
  - 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
    - やりすぎると痛い目にあうこともあります
      - 数年前windows update時の朝3時に日本全国からアラートの山が…
  - そもそも機械にまかせていない部分を、他の人間がその心を読み解いて機械化するのは難しい
  - 出来る範囲で気付きやすい仕組みを作ることが重要
- インターネット天気予報が真面目に必要かもしれない
  - それによって備えもできる

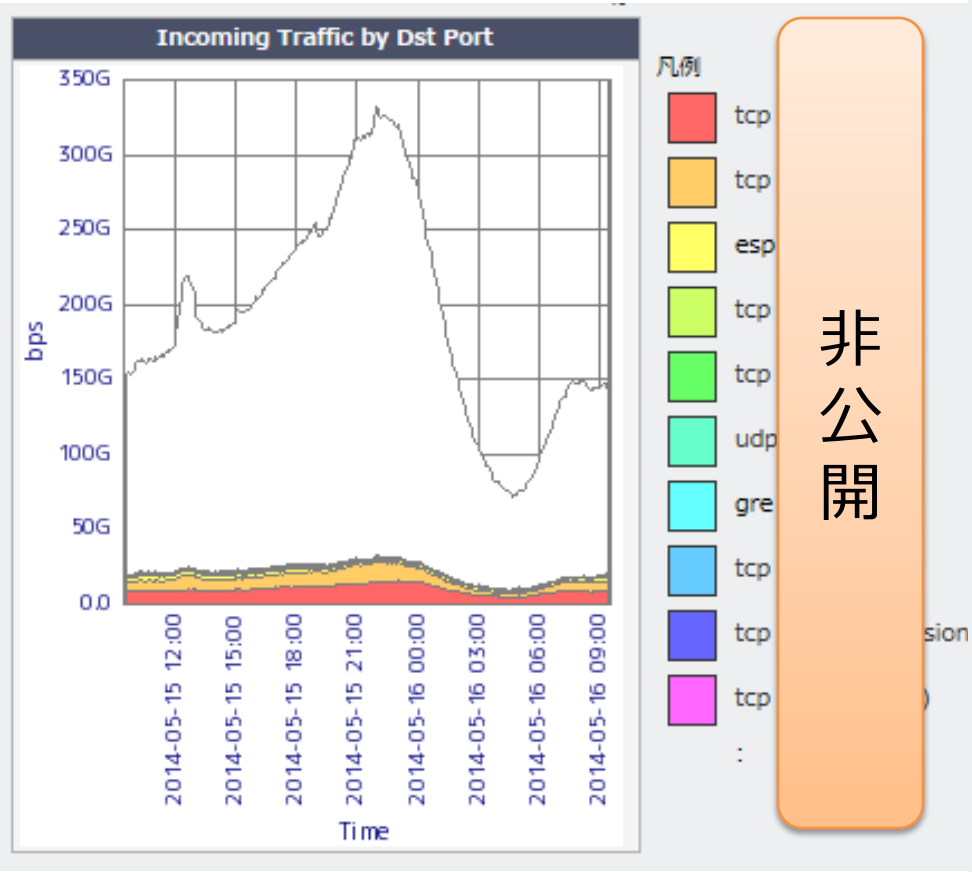
# ここ３年のJPNAP (byte)

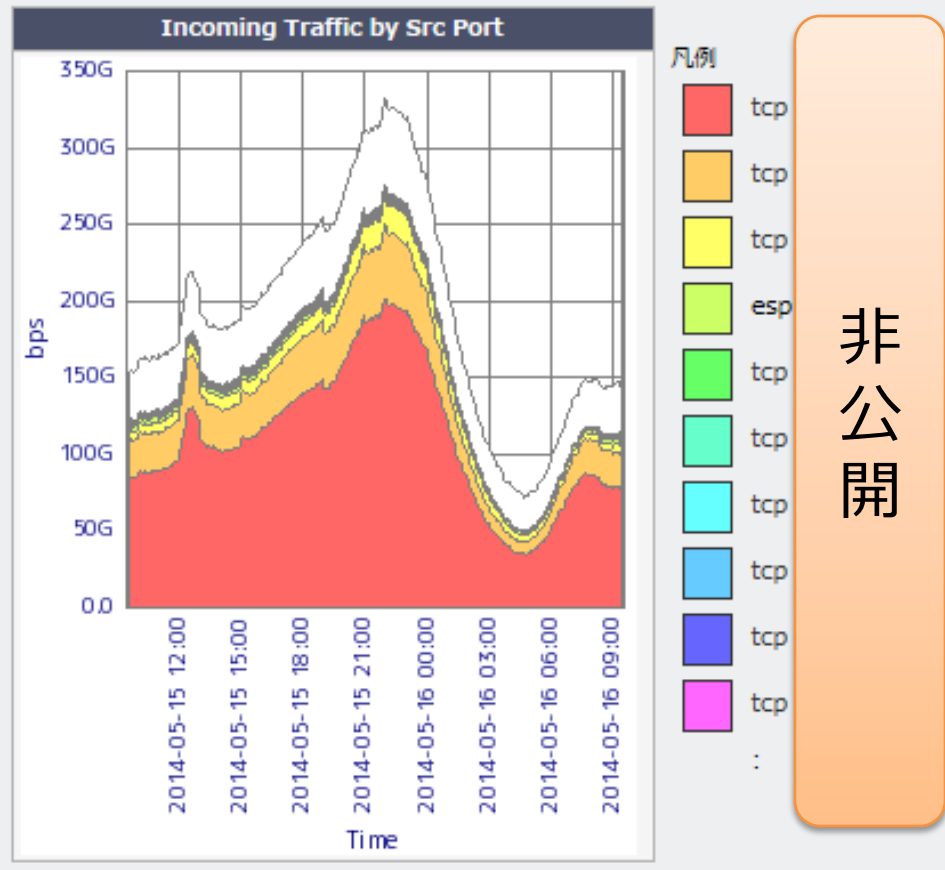


# 国別



# JPNAP TokyoI のトラフィック



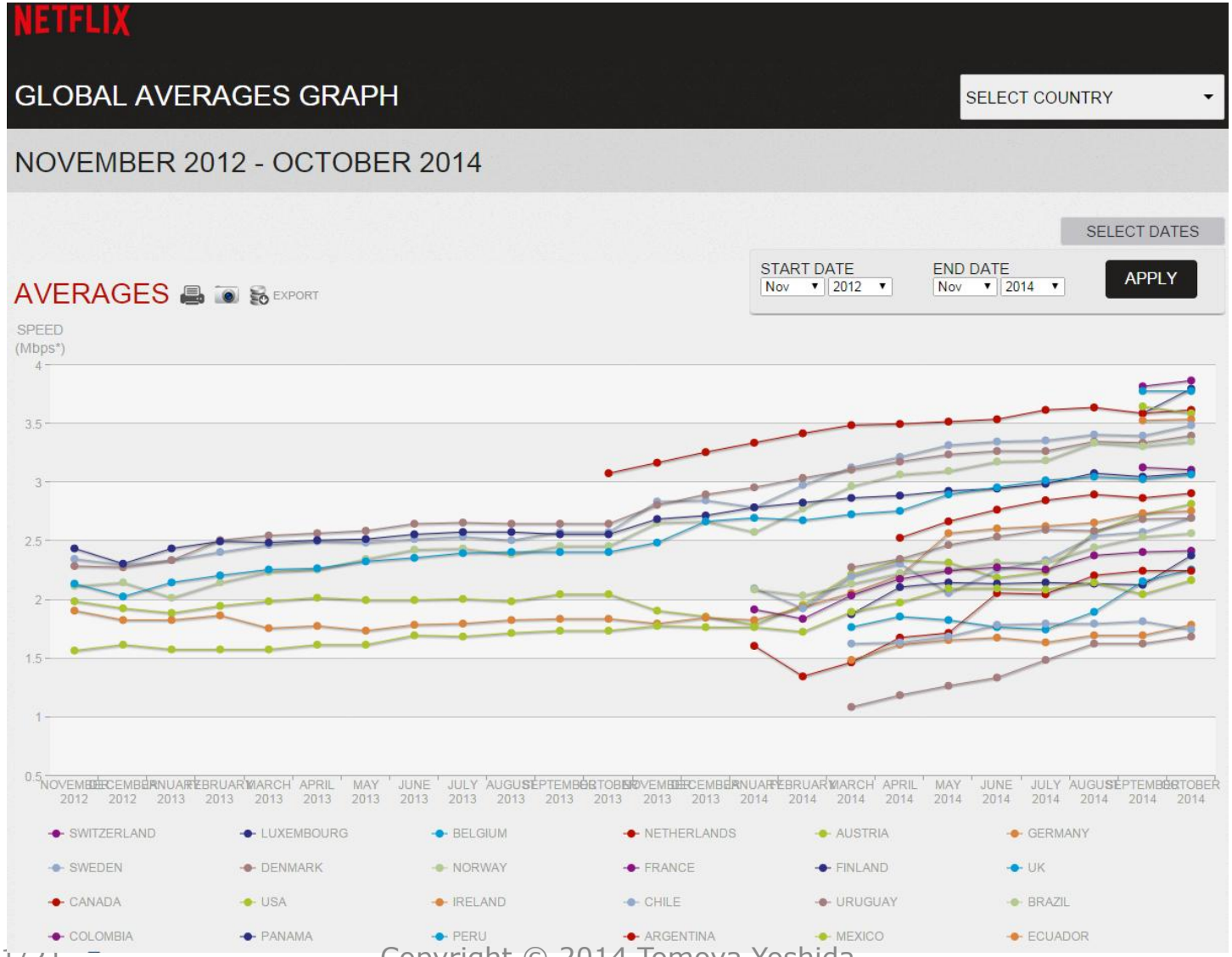



# Video配信事業者によるISP格付け

- Netflixの自社サイトでサービス提供国でのISP毎のVideo視聴品質を公開

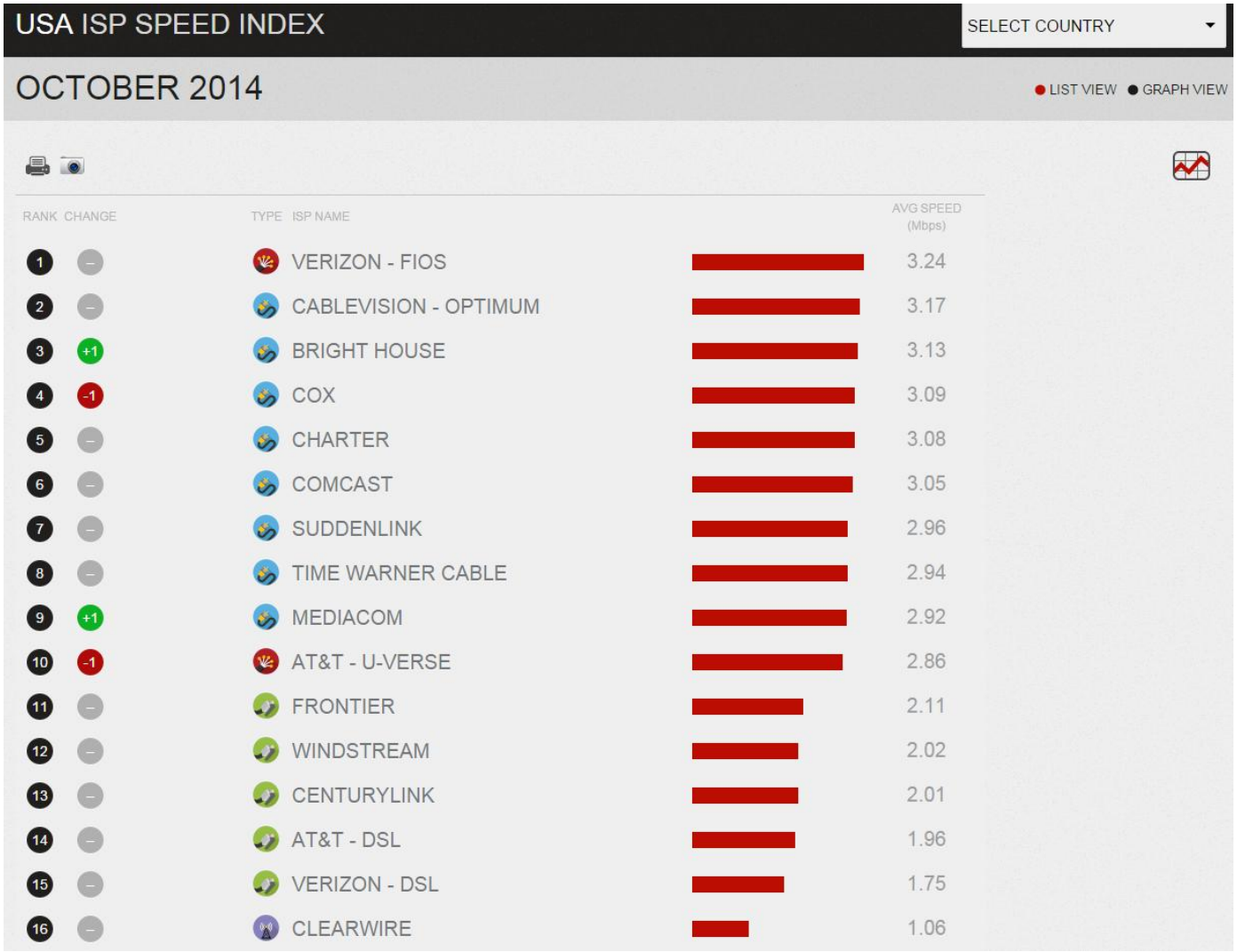
- Googleによるyoutubeストリーミング品質の解析ツールをリリース（2014年5月）

# NETFLIXによる ISP Speed Index




http://ispspeedindex.netflix.com/

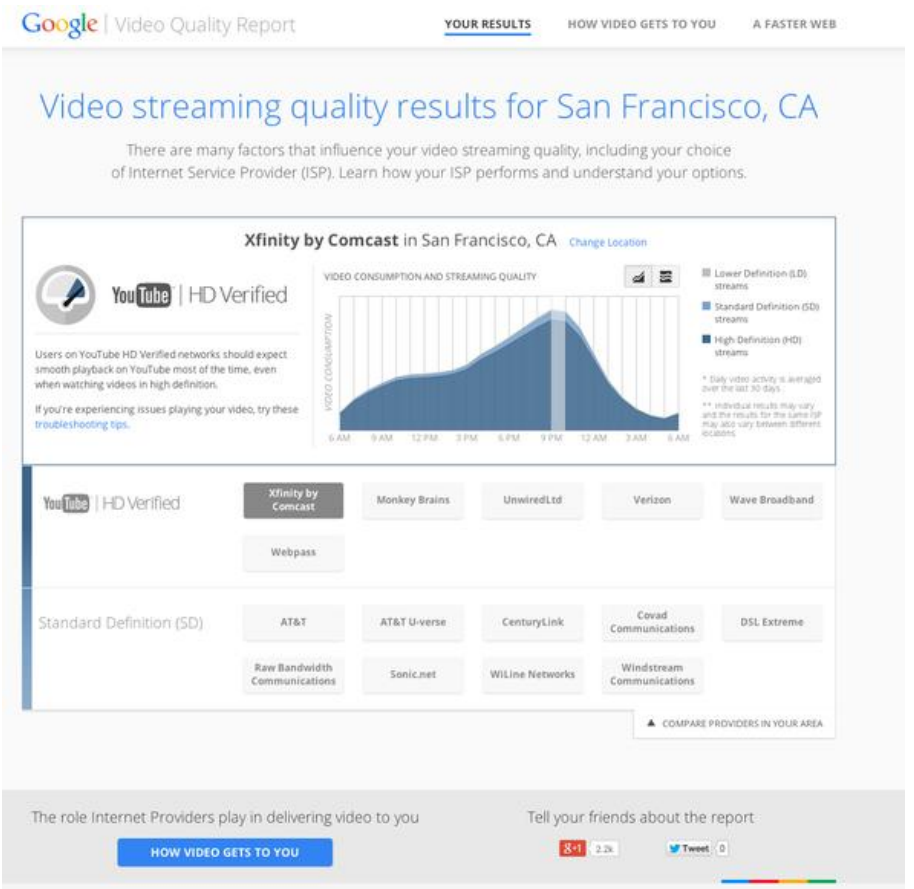
# NETFLIX USA ISP Speed Index




http://ispspeedindex.netflix.com/

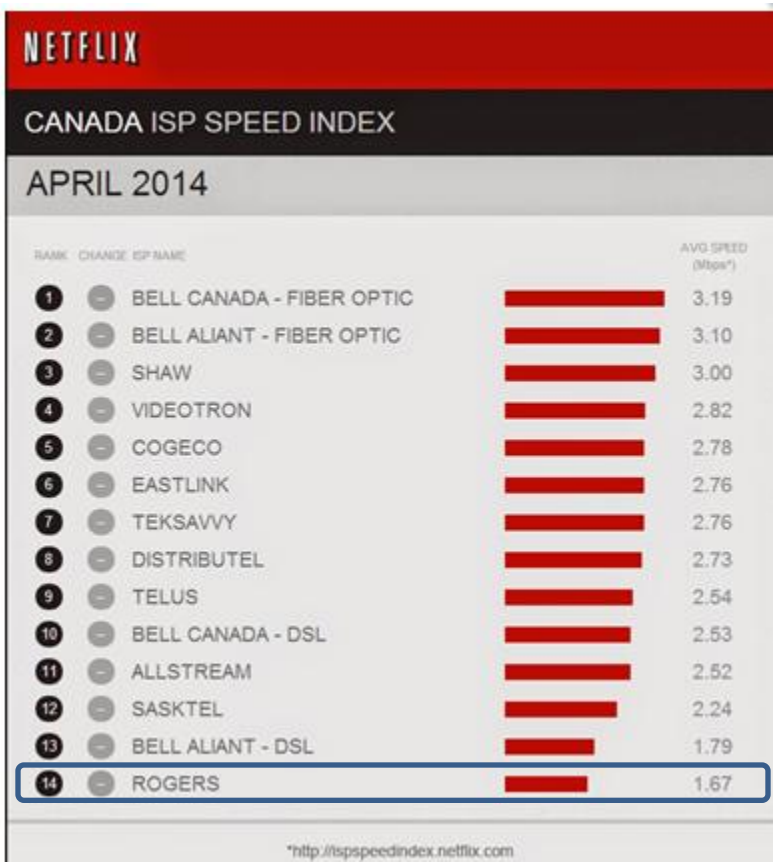
# Google Video Quality Report

- 3つの基準で比較
  - HD Verified(720p)
    - プロバイダーがHD動画を720p以上の解像度でバッファリングや中断なく一貫して提供できる状態
  - Standard Definition (360p)
    - 360pでの中断のない動画ストリーミング
  - Lower Definition
    - 360p未満で動画を再生し、中断がよくある状態

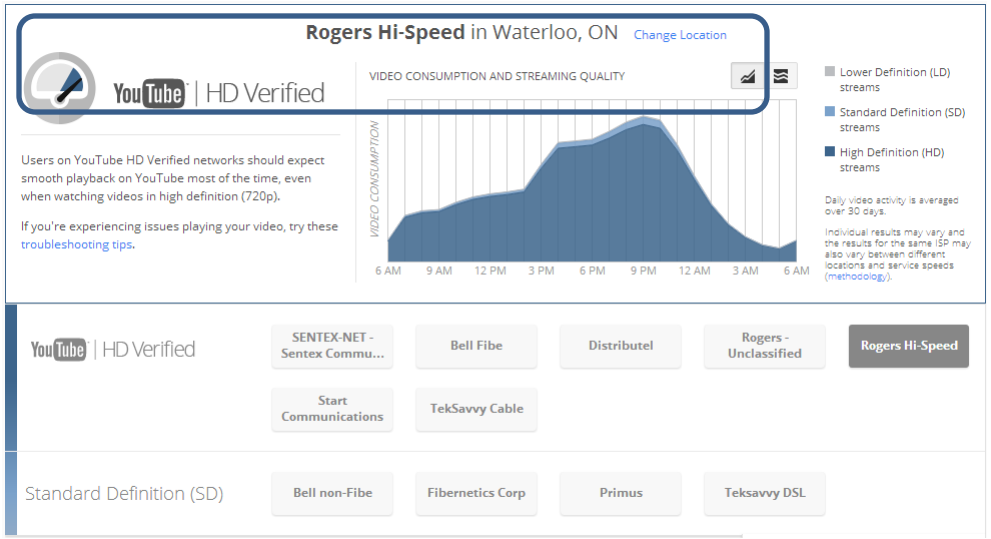


# 事業者毎の品質比較(CAの例)

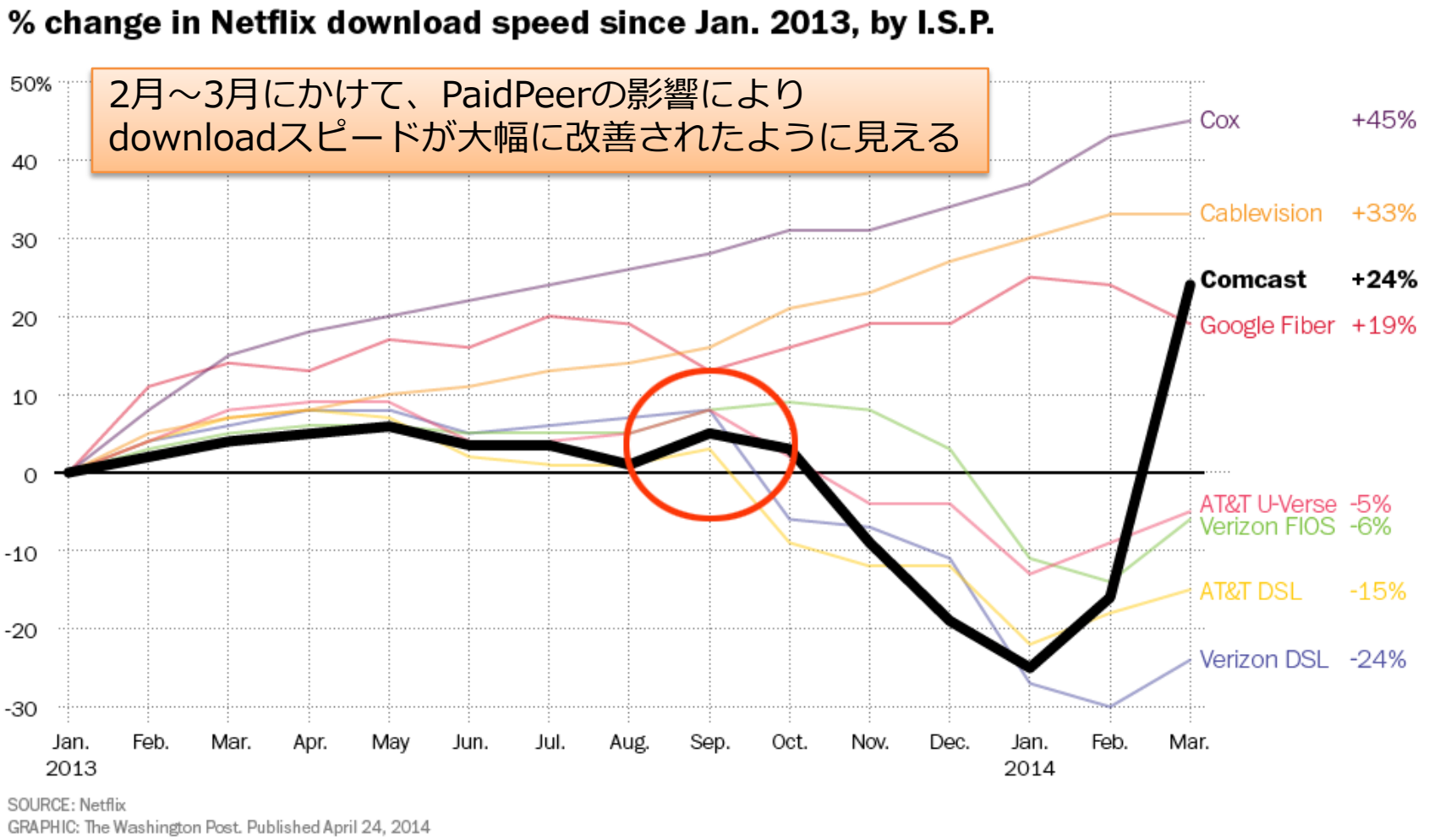
- NetflixとGoogleで結果がまったく違う。。。




2月　NetflixとComcast、PaidPeerを締結
4月　NetflixとVerizon、 PaidPeerを締結




http://www.internetphenomena.com/2014/06/conflicting-reports-canadian-isp-rankings/




http://blog.streamingmedia.com/2014/06/netflix-isp-newdata.html

# Measuring Broadband America - 2014

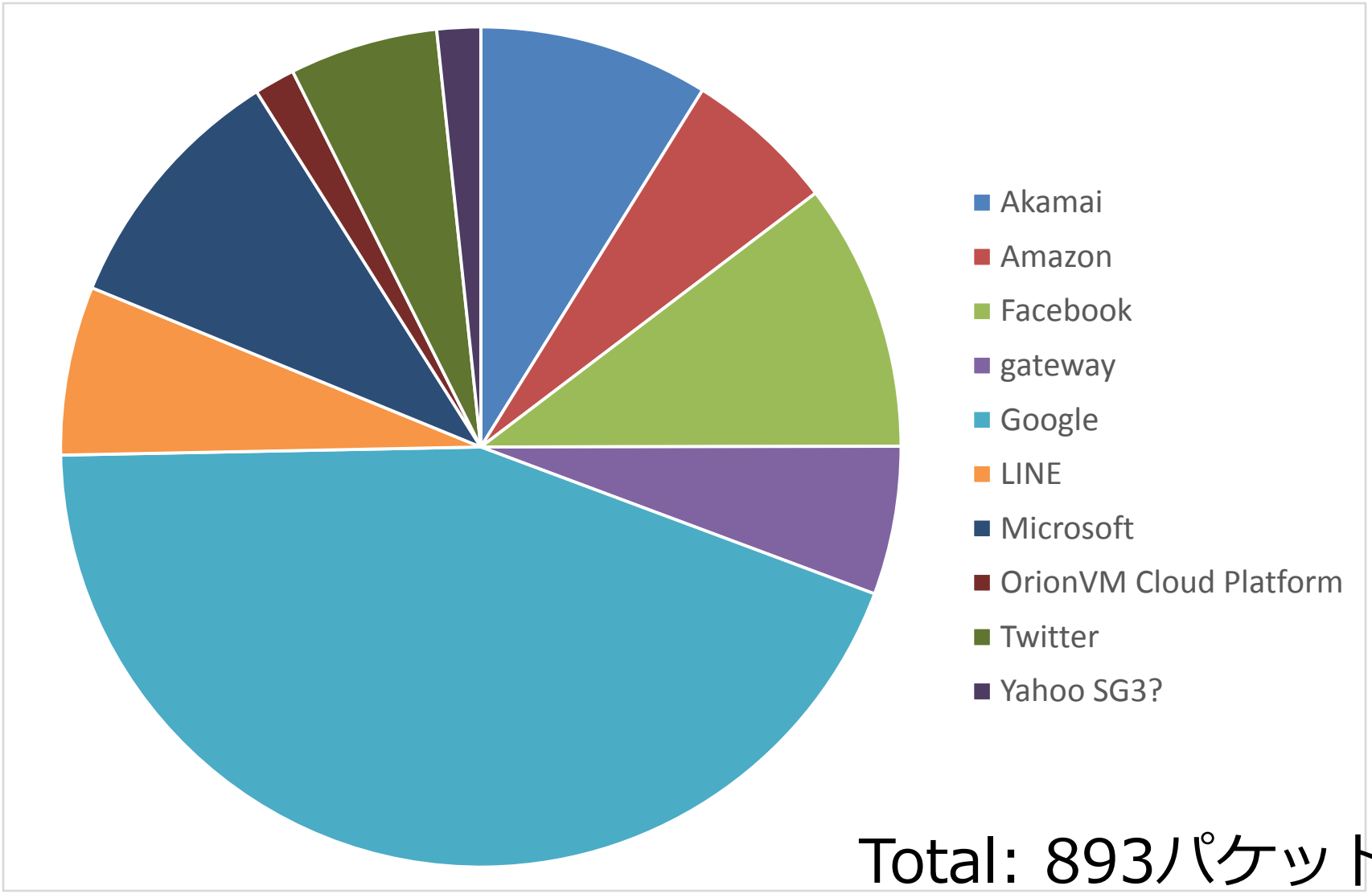
- FCCが広告表示速度を通信事業者ごとに比較
- 4事業者が平均90%を達成できず、とか…


http://www.fcc.gov/reports/measuring-broadband-america-2014

# モバイルトラフィック

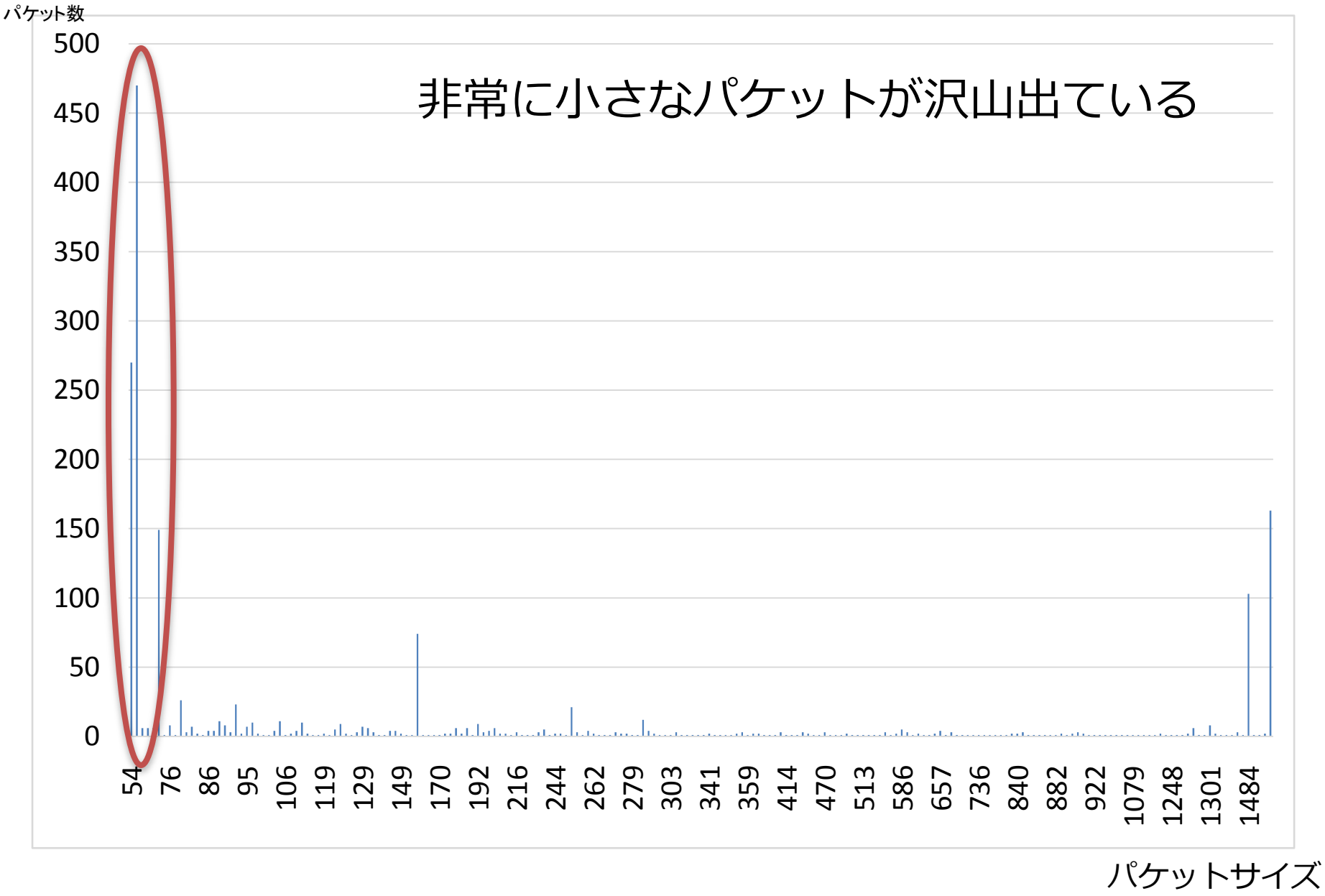
- 気にしなければいけないことが違う
- bpsよりpps
  - 1パケットのサイズが小さいものが多い
  - 帯域には余裕があるのにパケットをさばけないことも起きる
  - スマートフォンのショートパケットの多さはやはり異常な程
  - 常に電源が入っているため何かしらパケットを出している
  - アプリ怖いよ

# とあるAndroid の 60分




Total: 893パケット

# パケットサイズの分布


パケット数
500
450
400
350
300
250
200
150
100
50
0
非常に小さなパケットが沢山出ている
54
76
86
95
106
119
129
149
170
192
216
244
262
279
303
341
359
414
470
513
586
657
736
840
882
922
1079
1248
1301
1484
パケットサイズ

# 最近のゲームを
# 軽く覗いてみる

# パズドラ

# ちょっとダンジョンに入ってパケットキャプチャ

観測されたTCPストリームは合計13本

- パズドラ起動
  - ダンジョン→スペシャル→水曜ダンジョン
    →仮面の間 上級
  - フレンド選択
  - 挑戦
  - (プレイ 約2分間)
  - クリア→クリア報酬確認→友情ポイント清算
    →OK

# ちょっとダンジョンに入ってみる

- 0. 17.173.66.102
  - p11-buy.itunes.apple.com
  - 443 / HTTPS
  - 起動直後～1秒以内で終了
  - 30秒後にFIN
  - クライアント側から割りと大きめのデータを送っているようにも見える
- 1, 2: 17.173.254.14
  - service.gc.apple.com
  - 443 / HTTPS
  - 起動直後～2秒以内で終了
  - 30秒後にFIN
  - 1, 2ともにホスト名から想像するにGameCenter関連？
- 3, 4, 5
  - 80 / HTTP
  - 起動後のタイトル画面下部に出てくるバナーの取得をしている
  - 3.がバナーのHTMLだが、この中でGoogle Analyticsへのリンクがあるため4.のGoogle Analyticsへの通信が発生する
  - 5.も上記の一環？JSONだけが返ってきている

# バナー取得

Filter: tcp.stream eq 3 Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 84 | 7.042119 | 192.168.3.2 | 103.246.150.250 | TCP | 78 | 62190 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 T |
| 85 | 7.049348 | 103.246.150.250 | 192.168.3.2 | TCP | 66 | http > 62190 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=14 |
| 86 | 7.051649 | 192.168.3.2 | 103.246.150.250 | TCP | 54 | 62190 > http [ACK] Seq=1 Ack=1 Win=262144 Len=0 |
| 87 | 7.056792 | 192.168.3.2 | 103.246.150.250 | HTTP | 536 | GET /banner.html HTTP/1.1 |
| 88 | 7.071646 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 89 | 7.071697 | 103.246.150.250 | 192.168.3.2 | HTTP | 1019 | HTTP/1.1 200 OK (text/html) |
| 90 | 7.074080 | 192.168.3.2 | 103.246.150.250 | TCP | 54 | 62190 > http [ACK] Seq=483 Ack=2426 Win=261168 Len=0 |
| 92 | 7.132605 | 192.168.3.2 | 103.246.150.250 | HTTP | 538 | GET /img/pad_140613_zeusv.jpg HTTP/1.1 |
| 93 | 7.140246 | 103.246.150.250 | 192.168.3.2 | TCP | 54 | http > 62190 [ACK] Seq=2426 Ack=967 Win=8128 Len=0 |
| 94 | 7.161144 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 95 | 7.161203 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 96 | 7.161349 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 97 | 7.161399 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 98 | 7.161493 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 99 | 7.161621 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 100 | 7.161660 | 103.246.150.250 | 192.168.3.2 | TCP | 294 | [TCP segment of a reassembled PDU] |
| 101 | 7.161757 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 102 | 7.161871 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 103 | 7.164624 | 192.168.3.2 | 103.246.150.250 | TCP | 54 | 62190 > http [ACK] Seq=967 Ack=5346 Win=260672 Len=0 |
| 104 | 7.166421 | 192.168.3.2 | 103.246.150.250 | TCP | 54 | 62190 > http [ACK] Seq=967 Ack=8266 Win=259216 Len=0 |
| 105 | 7.166660 | 192.168.3.2 | 103.246.150.250 | TCP | 54 | 62190 > http [ACK] Seq=967 Ack=11186 Win=256304 Len=0 |
| 106 | 7.167053 | 192.168.3.2 | 103.246.150.250 | TCP | 54 | 62190 > http [ACK] Seq=967 Ack=11426 Win=256064 Len=0 |
| 107 | 7.167562 | 192.168.3.2 | 103.246.150.250 | TCP | 54 | 62190 > http [ACK] Seq=967 Ack=14346 Win=253136 Len=0 |
| 108 | 7.167850 | 192.168.3.2 | 103.246.150.250 | TCP | 54 | [TCP Window Update] 62190 > http [ACK] Seq=967 Ack=14346 |
| 109 | 7.172112 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 110 | 7.172230 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 111 | 7.172344 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 112 | 7.173871 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 113 | 7.174003 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 114 | 7.174117 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 115 | 7.174232 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 116 | 7.174349 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 117 | 7.174490 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 118 | 7.174595 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 119 | 7.174845 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 120 | 7.174941 | 103.246.150.250 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |

# 続き

- 6 ~ 12:
    - api-pad.gungho.jp.
    - 全て 443 / HTTPS
    - これが実際のゲームの通信に相当すると思われる
        - ダンジョン選択かクリアして元の画面に戻ってくるまでの通信
        - 6. ノーマルダンジョン一覧表示 | -> スペシャル選択
        - 7. スペシャルダンジョン一覧表示 | -> 水曜ダンジョン選択
        - 8. 水曜ダンジョンフロア一覧表示 | -> フロア選択
        - 9. 助っ人一覧表示 | -> 助っ人選択
        - 10. 潜入確認画面 | -> 挑戦する
        - 11. ダンジョン潜入
        - プレイ中通信なし
        - 12. クリア時通信
    - 時間を見ると、11の通信終了から12の通信開始まで130秒程度の空きがある
        - つまりプレイ中はまったく通信していない
    - あまり大きめのパケットはない模様
        - たまにある1514のパケットはHTTPSのサーバー証明書が多い印象

    DNSのレコードから察するに、AWSで運用している

# ノーマルダンジョン一覧表示 -> スペシャル選択

Filter: tcp.stream eq 6 Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 193 | 8.871620 | 192.168.3.2 | 54.248.241.83 | TCP | 78 | 62193 > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=76780024 |
| 194 | 8.877000 | 54.248.241.83 | 192.168.3.2 | TCP | 74 | https > 62193 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM= |
| 195 | 8.879450 | 192.168.3.2 | 54.248.241.83 | TCP | 66 | 62193 > https [ACK] Seq=1 Ack=1 Win=131760 Len=0 TSval=767800250 TSecr=1 |
| 196 | 8.885587 | 192.168.3.2 | 54.248.241.83 | TLSv1 | 250 | Client Hello |
| 197 | 8.890712 | 54.248.241.83 | 192.168.3.2 | TCP | 66 | https > 62193 [ACK] Seq=1 Ack=185 Win=15616 Len=0 TSval=1984046164 TSecr |
| 198 | 8.891514 | 54.248.241.83 | 192.168.3.2 | TLSv1 | 1514 | Server Hello |
| 199 | 8.891563 | 54.248.241.83 | 192.168.3.2 | TLSv1 | 1408 | Certificate, Server Hello Done |
| 200 | 8.893992 | 192.168.3.2 | 54.248.241.83 | TCP | 66 | 62193 > https [ACK] Seq=185 Ack=2791 Win=129728 Len=0 TSval=767800262 TS |
| 201 | 8.902417 | 192.168.3.2 | 54.248.241.83 | TLSv1 | 333 | Client Key Exchange |
| 202 | 8.902732 | 192.168.3.2 | 54.248.241.83 | TLSv1 | 72 | Change Cipher Spec |
| 203 | 8.902822 | 192.168.3.2 | 54.248.241.83 | TLSv1 | 119 | Encrypted Handshake Message |
| 204 | 8.910154 | 54.248.241.83 | 192.168.3.2 | TCP | 66 | https > 62193 [ACK] Seq=2791 Ack=511 Win=16640 Len=0 TSval=1984046169 TS |
| 205 | 8.910202 | 54.248.241.83 | 192.168.3.2 | TLSv1 | 125 | Change Cipher Spec, Encrypted Handshake Message |
| 206 | 8.912303 | 192.168.3.2 | 54.248.241.83 | TCP | 66 | 62193 > https [ACK] Seq=511 Ack=2850 Win=131008 Len=0 TSval=767800279 TS |
| 207 | 8.915041 | 192.168.3.2 | 54.248.241.83 | TLSv1 | 407 | Application Data |
| 208 | 8.958975 | 54.248.241.83 | 192.168.3.2 | TLSv1 | 471 | Application Data |
| 209 | 8.959003 | 54.248.241.83 | 192.168.3.2 | TLSv1 | 103 | Encrypted Alert |
| 210 | 8.974370 | 192.168.3.2 | 54.248.241.83 | TCP | 66 | 62193 > https [ACK] Seq=852 Ack=3255 Win=130656 Len=0 TSval=767800327 TS |
| 211 | 8.974509 | 192.168.3.2 | 54.248.241.83 | TCP | 66 | 62193 > https [ACK] Seq=852 Ack=3292 Win=131024 Len=0 TSval=767800329 TS |
| 212 | 8.974561 | 192.168.3.2 | 54.248.241.83 | TLSv1 | 103 | Encrypted Alert |
| 213 | 8.974606 | 192.168.3.2 | 54.248.241.83 | TCP | 66 | 62193 > https [FIN, ACK] Seq=889 Ack=3292 Win=131072 Len=0 TSval=767800 |
| 214 | 8.981273 | 54.248.241.83 | 192.168.3.2 | TCP | 66 | https > 62193 [FIN, ACK] Seq=3292 Ack=890 Win=17920 Len=0 TSval=19840461 |
| 215 | 8.983243 | 192.168.3.2 | 54.248.241.83 | TCP | 66 | 62193 > https [ACK] Seq=890 Ack=3293 Win=131072 Len=0 TSval=767800348 TS |

# スペシャルダンジョン一覧表示 -> 水曜ダンジョン選択

Filter: tcp.stream eq 7 Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 216 | 10.049306 | 192.168.3.2 | 176.34.29.171 | TCP | 78 | 62194 > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=767801386 TSecr=0 SACK_PE |
| 217 | 10.055072 | 176.34.29.171 | 192.168.3.2 | TCP | 74 | https > 62194 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=19840479 |
| 218 | 10.057574 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62194 > https [ACK] Seq=1 Ack=1 Win=131760 Len=0 TSval=767801420 TSecr=1984047971 |
| 219 | 10.062760 | 192.168.3.2 | 176.34.29.171 | TLSv1 | 250 | Client Hello |
| 220 | 10.067891 | 176.34.29.171 | 192.168.3.2 | TCP | 66 | https > 62194 [ACK] Seq=1 Ack=185 Win=15616 Len=0 TSval=1984047974 TSecr=767801425 |
| 221 | 10.070418 | 176.34.29.171 | 192.168.3.2 | TLSv1 | 1514 | Server Hello |
| 222 | 10.070537 | 176.34.29.171 | 192.168.3.2 | TLSv1 | 1408 | Certificate, Server Hello Done |
| 223 | 10.073582 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62194 > https [ACK] Seq=185 Ack=2791 Win=129728 Len=0 TSval=767801433 TSecr=1984047974 |
| 224 | 10.083582 | 192.168.3.2 | 176.34.29.171 | TLSv1 | 333 | Client Key Exchange |
| 225 | 10.083677 | 192.168.3.2 | 176.34.29.171 | TLSv1 | 72 | Change Cipher Spec |
| 226 | 10.083957 | 192.168.3.2 | 176.34.29.171 | TLSv1 | 119 | Encrypted Handshake Message |
| 227 | 10.093238 | 176.34.29.171 | 192.168.3.2 | TCP | 66 | https > 62194 [ACK] Seq=2791 Ack=511 Win=16640 Len=0 TSval=1984047980 TSecr=767801443 |
| 228 | 10.093291 | 176.34.29.171 | 192.168.3.2 | TLSv1 | 125 | Change Cipher Spec, Encrypted Handshake Message |
| 229 | 10.100077 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62194 > https [ACK] Seq=511 Ack=2850 Win=131008 Len=0 TSval=767801458 TSecr=1984047980 |
| 230 | 10.101853 | 192.168.3.2 | 176.34.29.171 | TLSv1 | 407 | Application Data |
| 231 | 10.146998 | 176.34.29.171 | 192.168.3.2 | TCP | 66 | https > 62194 [ACK] Seq=2850 Ack=852 Win=17920 Len=0 TSval=1984047994 TSecr=767801459 |
| 232 | 10.267091 | 176.34.29.171 | 192.168.3.2 | TLSv1 | 1511 | Application Data |
| 233 | 10.267178 | 176.34.29.171 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 234 | 10.267236 | 176.34.29.171 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 235 | 10.267397 | 176.34.29.171 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 236 | 10.267462 | 176.34.29.171 | 192.168.3.2 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 237 | 10.267495 | 176.34.29.171 | 192.168.3.2 | TLSv1 | 1239 | Application Data |
| 238 | 10.267527 | 176.34.29.171 | 192.168.3.2 | TLSv1 | 103 | Application Data |
| 239 | 10.267563 | 176.34.29.171 | 192.168.3.2 | TLSv1 | 103 | Encrypted Alert |
| 240 | 10.314925 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62194 > https [ACK] Seq=852 Ack=4295 Win=129616 Len=0 TSval=767801650 TSecr=1984048023 |
| 241 | 10.315069 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62194 > https [ACK] Seq=852 Ack=7191 Win=126720 Len=0 TSval=767801650 TSecr=1984048023 |
| 242 | 10.315120 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62194 > https [ACK] Seq=852 Ack=10087 Win=123824 Len=0 TSval=767801650 TSecr=1984048023 |
| 243 | 10.315164 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62194 > https [ACK] Seq=852 Ack=11260 Win=122656 Len=0 TSval=767801650 TSecr=1984048023 |
| 244 | 10.315209 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62194 > https [ACK] Seq=852 Ack=11297 Win=122624 Len=0 TSval=767801650 TSecr=1984048023 |
| 245 | 10.315251 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62194 > https [ACK] Seq=852 Ack=11334 Win=122576 Len=0 TSval=767801650 TSecr=1984048023 |
| 246 | 10.315298 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | [TCP Window Update] 62194 > https [ACK] Seq=852 Ack=11334 Win=131072 Len=0 TSval=7678016 |
| 247 | 10.315346 | 192.168.3.2 | 176.34.29.171 | TLSv1 | 103 | Encrypted Alert |
| 248 | 10.315398 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62194 > https [FIN, ACK] Seq=889 Ack=11334 Win=131072 Len=0 TSval=767801654 TSecr=198404 |
| 249 | 10.320480 | 176.34.29.171 | 192.168.3.2 | TCP | 66 | https > 62194 [ACK] Seq=11334 Ack=889 Win=17920 Len=0 TSval=1984048037 TSecr=767801651 |
| 250 | 10.320612 | 176.34.29.171 | 192.168.3.2 | TCP | 66 | https > 62194 [FIN, ACK] Seq=11334 Ack=890 Win=17920 Len=0 TSval=1984048037 TSecr=767801 |
| 251 | 10.321813 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62194 > https [FIN, ACK] Seq=889 Ack=11334 Win=131072 Len=0 TSval=767801677 TSecr=198404 |
| 252 | 10.322146 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62194 > https [ACK] Seq=890 Ack=11335 Win=131072 Len=0 TSval=767801677 TSecr=1984048037 |
| 253 | 10.326967 | 176.34.29.171 | 192.168.3.2 | TCP | 78 | [TCP Dup ACK 250#1] https > 62194 [ACK] Seq=11335 Ack=890 Win=17920 Len=0 TSval=19840480 |

# 水曜ダンジョンフロアー覧表示 -> フロア選択

Filter: tcp.stream eq 8 Expression... Clear Apply

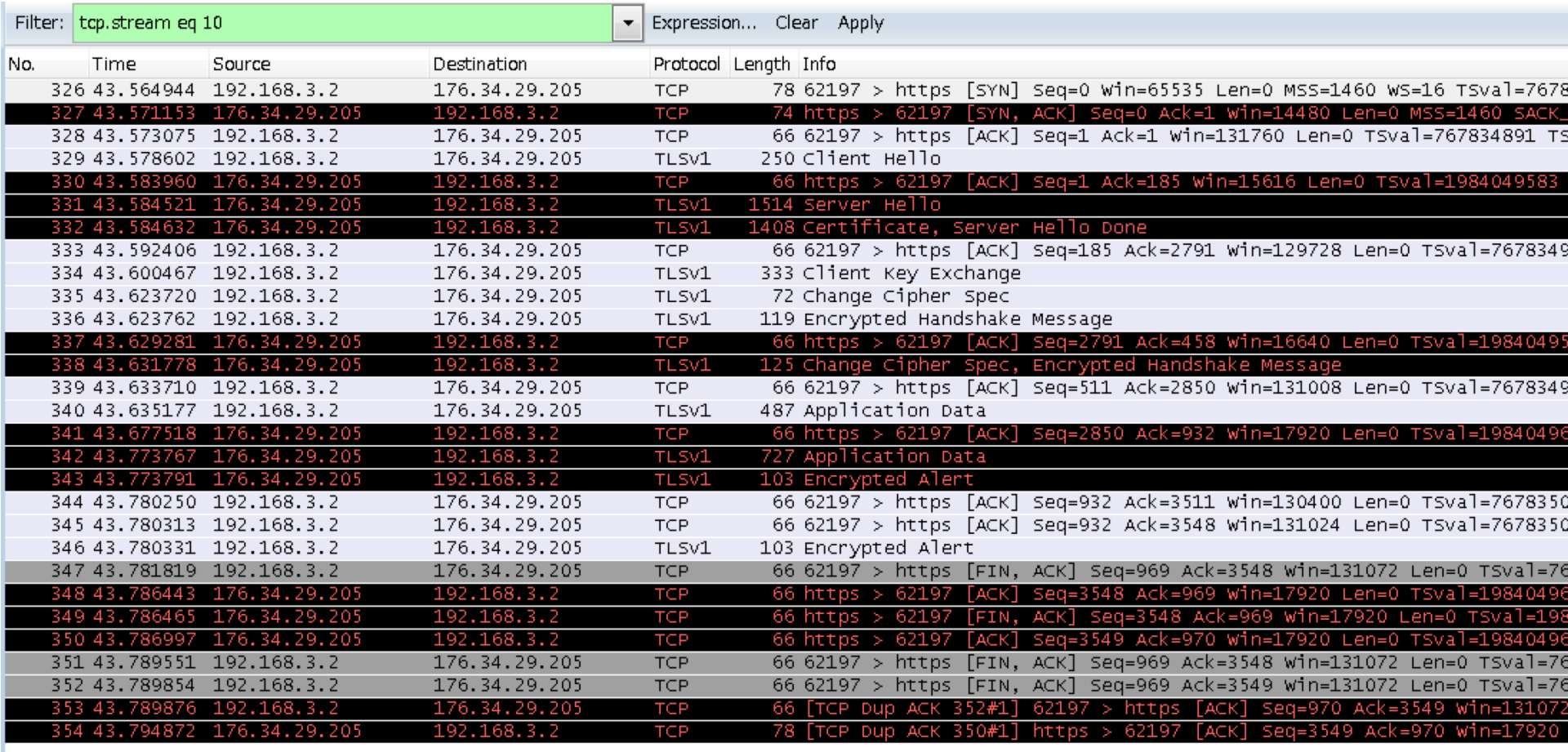
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 254 | 10.577017 | 192.168.3.2 | 176.34.29.171 | TCP | 78 | 62195 > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=7678018 |
| 255 | 10.585602 | 176.34.29.171 | 192.168.3.2 | TCP | 74 | https > 62195 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PER |
| 256 | 10.587745 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62195 > https [ACK] Seq=1 Ack=1 Win=131760 Len=0 TSval=767801940 TSecr |
| 257 | 10.593450 | 192.168.3.2 | 176.34.29.171 | TLSv1 | 282 | Client Hello |
| 258 | 10.599413 | 176.34.29.171 | 192.168.3.2 | TCP | 66 | https > 62195 [ACK] Seq=1 Ack=217 Win=15616 Len=0 TSval=1984048107 TSe |
| 259 | 10.599463 | 176.34.29.171 | 192.168.3.2 | TLSv1 | 211 | Server Hello, Change Cipher Spec, Encrypted Handshake Message |
| 260 | 10.602762 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62195 > https [ACK] Seq=217 Ack=146 Win=131616 Len=0 TSval=767801953 T |
| 261 | 10.603887 | 192.168.3.2 | 176.34.29.171 | TLSv1 | 72 | Change Cipher Spec |
| 262 | 10.604288 | 192.168.3.2 | 176.34.29.171 | TLSv1 | 119 | Encrypted Handshake Message |
| 263 | 10.604948 | 192.168.3.2 | 176.34.29.171 | TLSv1 | 407 | Application Data |
| 264 | 10.609825 | 176.34.29.171 | 192.168.3.2 | TCP | 66 | https > 62195 [ACK] Seq=146 Ack=276 Win=15616 Len=0 TSval=1984048109 T |
| 265 | 10.633101 | 176.34.29.171 | 192.168.3.2 | TLSv1 | 567 | Application Data |
| 266 | 10.633146 | 176.34.29.171 | 192.168.3.2 | TLSv1 | 103 | Encrypted Alert |
| 267 | 10.699495 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62195 > https [ACK] Seq=617 Ack=647 Win=131120 Len=0 TSval=767802048 T |
| 268 | 10.699777 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62195 > https [ACK] Seq=617 Ack=684 Win=131072 Len=0 TSval=767802048 T |
| 269 | 10.700868 | 192.168.3.2 | 176.34.29.171 | TLSv1 | 103 | Encrypted Alert |
| 270 | 10.704968 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62195 > https [FIN, ACK] Seq=654 Ack=684 Win=131072 Len=0 TSval=767802 |
| 271 | 10.706279 | 176.34.29.171 | 192.168.3.2 | TCP | 66 | https > 62195 [FIN, ACK] Seq=684 Ack=654 Win=16640 Len=0 TSval=1984048 |
| 272 | 10.710622 | 176.34.29.171 | 192.168.3.2 | TCP | 66 | https > 62195 [ACK] Seq=685 Ack=655 Win=16640 Len=0 TSval=1984048134 T |
| 273 | 10.712201 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | 62195 > https [FIN, ACK] Seq=654 Ack=685 Win=131072 Len=0 TSval=767802 |
| 274 | 10.713460 | 192.168.3.2 | 176.34.29.171 | TCP | 66 | [TCP Dup ACK 273#1] 62195 > https [ACK] Seq=655 Ack=685 Win=131072 Len |

# 助っ人一覧表示 -> 助っ人選択

Filter: tcp.stream eq 9 Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 275 | 20.614915 | 192.168.3.2 | 54.249.233.223 | TCP | 78 | 62196 > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=767 |
| 276 | 20.623064 | 54.249.233.223 | 192.168.3.2 | TCP | 74 | https > 62196 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK |
| 277 | 20.624932 | 192.168.3.2 | 54.249.233.223 | TCP | 66 | 62196 > https [ACK] Seq=1 Ack=1 Win=131760 Len=0 TSval=767811968 T |
| 278 | 20.630879 | 192.168.3.2 | 54.249.233.223 | TLSv1 | 250 | Client Hello |
| 279 | 20.636044 | 54.249.233.223 | 192.168.3.2 | TCP | 66 | https > 62196 [ACK] Seq=1 Ack=185 Win=15616 Len=0 TSval=1984041283 |
| 280 | 20.636252 | 54.249.233.223 | 192.168.3.2 | TLSv1 | 1514 | Server Hello |
| 281 | 20.636883 | 54.249.233.223 | 192.168.3.2 | TLSv1 | 1408 | Certificate, Server Hello Done |
| 282 | 20.641081 | 192.168.3.2 | 54.249.233.223 | TCP | 66 | 62196 > https [ACK] Seq=185 Ack=2791 Win=129728 Len=0 TSval=767811 |
| 283 | 20.648708 | 192.168.3.2 | 54.249.233.223 | TLSv1 | 333 | Client Key Exchange |
| 284 | 20.649016 | 192.168.3.2 | 54.249.233.223 | TLSv1 | 72 | Change Cipher Spec |
| 285 | 20.649069 | 192.168.3.2 | 54.249.233.223 | TLSv1 | 119 | Encrypted Handshake Message |
| 286 | 20.656331 | 54.249.233.223 | 192.168.3.2 | TCP | 66 | https > 62196 [ACK] Seq=2791 Ack=511 Win=16640 Len=0 TSval=1984041 |
| 287 | 20.656383 | 54.249.233.223 | 192.168.3.2 | TLSv1 | 125 | Change Cipher Spec, Encrypted Handshake Message |
| 288 | 20.661885 | 192.168.3.2 | 54.249.233.223 | TCP | 66 | 62196 > https [ACK] Seq=511 Ack=2850 Win=131008 Len=0 TSval=767812 |
| 289 | 20.663001 | 192.168.3.2 | 54.249.233.223 | TLSv1 | 407 | Application Data |
| 290 | 20.675971 | 54.249.233.223 | 192.168.3.2 | TLSv1 | 871 | Application Data |
| 291 | 20.676032 | 54.249.233.223 | 192.168.3.2 | TLSv1 | 103 | Encrypted Alert |
| 292 | 20.677865 | 192.168.3.2 | 54.249.233.223 | TCP | 66 | 62196 > https [ACK] Seq=852 Ack=3655 Win=130256 Len=0 TSval=767812 |
| 293 | 20.678219 | 192.168.3.2 | 54.249.233.223 | TCP | 66 | 62196 > https [ACK] Seq=852 Ack=3692 Win=130224 Len=0 TSval=767812 |
| 294 | 20.678800 | 192.168.3.2 | 54.249.233.223 | TLSv1 | 103 | Encrypted Alert |
| 295 | 20.681680 | 192.168.3.2 | 54.249.233.223 | TCP | 66 | 62196 > https [FIN, ACK] Seq=889 Ack=3692 Win=131072 Len=0 TSval=7 |
| 296 | 20.683708 | 54.249.233.223 | 192.168.3.2 | TCP | 66 | https > 62196 [FIN, ACK] Seq=3692 Ack=889 Win=17920 Len=0 TSval=19 |
| 297 | 20.685368 | 192.168.3.2 | 54.249.233.223 | TCP | 66 | 62196 > https [FIN, ACK] Seq=889 Ack=3693 Win=131072 Len=0 TSval=7 |
| 298 | 20.686288 | 54.249.233.223 | 192.168.3.2 | TCP | 66 | https > 62196 [ACK] Seq=3693 Ack=890 Win=17920 Len=0 TSval=1984041 |
| 299 | 20.687555 | 192.168.3.2 | 54.249.233.223 | TCP | 66 | [TCP Dup ACK 297#1] 62196 > https [ACK] Seq=890 Ack=3693 Win=13107 |

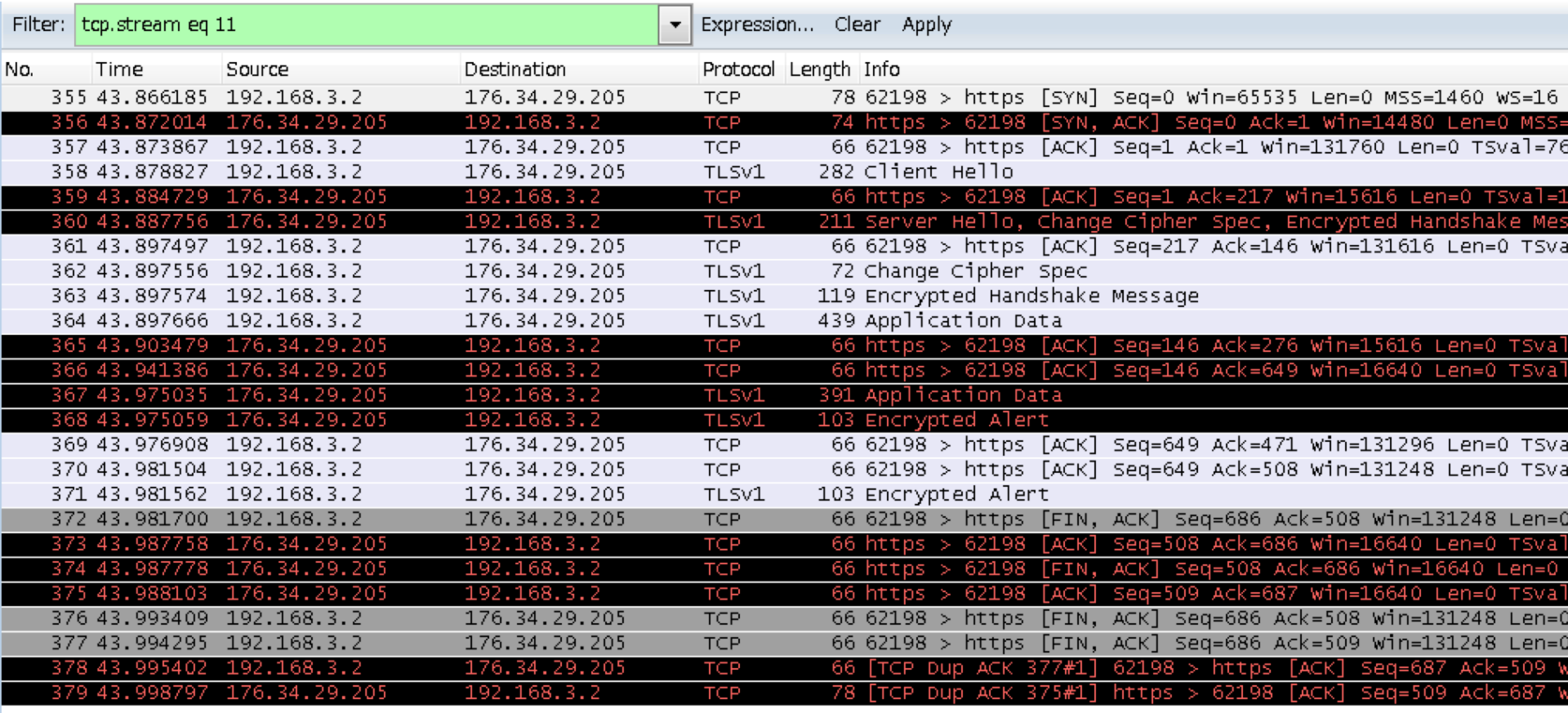
# 潜入確認画面 -> 挑戦する



Filter: tcp.stream eq 10 Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 326 | 43.564944 | 192.168.3.2 | 176.34.29.205 | TCP | 78 | 62197 > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=7678 |
| 327 | 43.571153 | 176.34.29.205 | 192.168.3.2 | TCP | 74 | https > 62197 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_ |
| 328 | 43.573075 | 192.168.3.2 | 176.34.29.205 | TCP | 66 | 62197 > https [ACK] Seq=1 Ack=1 Win=131760 Len=0 TSval=767834891 TS |
| 329 | 43.578602 | 192.168.3.2 | 176.34.29.205 | TLSv1 | 250 | Client Hello |
| 330 | 43.583960 | 176.34.29.205 | 192.168.3.2 | TCP | 66 | https > 62197 [ACK] Seq=1 Ack=185 Win=15616 Len=0 TSval=1984049583 |
| 331 | 43.584521 | 176.34.29.205 | 192.168.3.2 | TLSv1 | 1514 | Server Hello |
| 332 | 43.584632 | 176.34.29.205 | 192.168.3.2 | TLSv1 | 1408 | Certificate, Server Hello Done |
| 333 | 43.592406 | 192.168.3.2 | 176.34.29.205 | TCP | 66 | 62197 > https [ACK] Seq=185 Ack=2791 Win=129728 Len=0 TSval=7678349 |
| 334 | 43.600467 | 192.168.3.2 | 176.34.29.205 | TLSv1 | 333 | Client Key Exchange |
| 335 | 43.623720 | 192.168.3.2 | 176.34.29.205 | TLSv1 | 72 | Change Cipher Spec |
| 336 | 43.623762 | 192.168.3.2 | 176.34.29.205 | TLSv1 | 119 | Encrypted Handshake Message |
| 337 | 43.629281 | 176.34.29.205 | 192.168.3.2 | TCP | 66 | https > 62197 [ACK] Seq=2791 Ack=458 Win=16640 Len=0 TSval=19840495 |
| 338 | 43.631778 | 176.34.29.205 | 192.168.3.2 | TLSv1 | 125 | Change Cipher Spec, Encrypted Handshake Message |
| 339 | 43.633710 | 192.168.3.2 | 176.34.29.205 | TCP | 66 | 62197 > https [ACK] Seq=511 Ack=2850 Win=131008 Len=0 TSval=7678349 |
| 340 | 43.635177 | 192.168.3.2 | 176.34.29.205 | TLSv1 | 487 | Application Data |
| 341 | 43.677518 | 176.34.29.205 | 192.168.3.2 | TCP | 66 | https > 62197 [ACK] Seq=2850 Ack=932 Win=17920 Len=0 TSval=19840496 |
| 342 | 43.773767 | 176.34.29.205 | 192.168.3.2 | TLSv1 | 727 | Application Data |
| 343 | 43.773791 | 176.34.29.205 | 192.168.3.2 | TLSv1 | 103 | Encrypted Alert |
| 344 | 43.780250 | 192.168.3.2 | 176.34.29.205 | TCP | 66 | 62197 > https [ACK] Seq=932 Ack=3511 Win=130400 Len=0 TSval=767835C |
| 345 | 43.780313 | 192.168.3.2 | 176.34.29.205 | TCP | 66 | 62197 > https [ACK] Seq=932 Ack=3548 Win=131024 Len=0 TSval=767835C |
| 346 | 43.780331 | 192.168.3.2 | 176.34.29.205 | TLSv1 | 103 | Encrypted Alert |
| 347 | 43.781819 | 192.168.3.2 | 176.34.29.205 | TCP | 66 | 62197 > https [FIN, ACK] Seq=969 Ack=3548 Win=131072 Len=0 TSval=76 |
| 348 | 43.786443 | 176.34.29.205 | 192.168.3.2 | TCP | 66 | https > 62197 [ACK] Seq=3548 Ack=969 Win=17920 Len=0 TSval=19840496 |
| 349 | 43.786465 | 176.34.29.205 | 192.168.3.2 | TCP | 66 | https > 62197 [FIN, ACK] Seq=3548 Ack=969 Win=17920 Len=0 TSval=198 |
| 350 | 43.786997 | 176.34.29.205 | 192.168.3.2 | TCP | 66 | https > 62197 [ACK] Seq=3549 Ack=970 Win=17920 Len=0 TSval=19840496 |
| 351 | 43.789551 | 192.168.3.2 | 176.34.29.205 | TCP | 66 | 62197 > https [FIN, ACK] Seq=969 Ack=3548 Win=131072 Len=0 TSval=76 |
| 352 | 43.789854 | 192.168.3.2 | 176.34.29.205 | TCP | 66 | 62197 > https [FIN, ACK] Seq=969 Ack=3549 Win=131072 Len=0 TSval=76 |
| 353 | 43.789876 | 192.168.3.2 | 176.34.29.205 | TCP | 66 | [TCP Dup ACK 352#1] 62197 > https [ACK] Seq=970 Ack=3549 Win=131072 |
| 354 | 43.794872 | 176.34.29.205 | 192.168.3.2 | TCP | 78 | [TCP Dup ACK 350#1] https > 62197 [ACK] Seq=3549 Ack=970 Win=17920 |

# ダンジョン潜入



Filter: tcp.stream eq 11 Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 355 | 43.866185 | 192.168.3.2 | 176.34.29.205 | TCP | 78 | 62198 > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 |
| 356 | 43.872014 | 176.34.29.205 | 192.168.3.2 | TCP | 74 | https > 62198 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS= |
| 357 | 43.873867 | 192.168.3.2 | 176.34.29.205 | TCP | 66 | 62198 > https [ACK] Seq=1 Ack=1 Win=131760 Len=0 TSval=76 |
| 358 | 43.878827 | 192.168.3.2 | 176.34.29.205 | TLSv1 | 282 | Client Hello |
| 359 | 43.884729 | 176.34.29.205 | 192.168.3.2 | TCP | 66 | https > 62198 [ACK] Seq=1 Ack=217 Win=15616 Len=0 TSval=1 |
| 360 | 43.887756 | 176.34.29.205 | 192.168.3.2 | TLSv1 | 211 | Server Hello, Change Cipher Spec, Encrypted Handshake Mes |
| 361 | 43.897497 | 192.168.3.2 | 176.34.29.205 | TCP | 66 | 62198 > https [ACK] Seq=217 Ack=146 Win=131616 Len=0 TSva |
| 362 | 43.897556 | 192.168.3.2 | 176.34.29.205 | TLSv1 | 72 | Change Cipher Spec |
| 363 | 43.897574 | 192.168.3.2 | 176.34.29.205 | TLSv1 | 119 | Encrypted Handshake Message |
| 364 | 43.897666 | 192.168.3.2 | 176.34.29.205 | TLSv1 | 439 | Application Data |
| 365 | 43.903479 | 176.34.29.205 | 192.168.3.2 | TCP | 66 | https > 62198 [ACK] Seq=146 Ack=276 Win=15616 Len=0 TSval |
| 366 | 43.941386 | 176.34.29.205 | 192.168.3.2 | TCP | 66 | https > 62198 [ACK] Seq=146 Ack=649 Win=16640 Len=0 TSval |
| 367 | 43.975035 | 176.34.29.205 | 192.168.3.2 | TLSv1 | 391 | Application Data |
| 368 | 43.975059 | 176.34.29.205 | 192.168.3.2 | TLSv1 | 103 | Encrypted Alert |
| 369 | 43.976908 | 192.168.3.2 | 176.34.29.205 | TCP | 66 | 62198 > https [ACK] Seq=649 Ack=471 Win=131296 Len=0 TSva |
| 370 | 43.981504 | 192.168.3.2 | 176.34.29.205 | TCP | 66 | 62198 > https [ACK] Seq=649 Ack=508 Win=131248 Len=0 TSva |
| 371 | 43.981562 | 192.168.3.2 | 176.34.29.205 | TLSv1 | 103 | Encrypted Alert |
| 372 | 43.981700 | 192.168.3.2 | 176.34.29.205 | TCP | 66 | 62198 > https [FIN, ACK] Seq=686 Ack=508 Win=131248 Len=0 |
| 373 | 43.987758 | 176.34.29.205 | 192.168.3.2 | TCP | 66 | https > 62198 [ACK] Seq=508 Ack=686 Win=16640 Len=0 TSval |
| 374 | 43.987778 | 176.34.29.205 | 192.168.3.2 | TCP | 66 | https > 62198 [FIN, ACK] Seq=508 Ack=686 Win=16640 Len=0 |
| 375 | 43.988103 | 176.34.29.205 | 192.168.3.2 | TCP | 66 | https > 62198 [ACK] Seq=509 Ack=687 Win=16640 Len=0 TSval |
| 376 | 43.993409 | 192.168.3.2 | 176.34.29.205 | TCP | 66 | 62198 > https [FIN, ACK] Seq=686 Ack=508 Win=131248 Len=0 |
| 377 | 43.994295 | 192.168.3.2 | 176.34.29.205 | TCP | 66 | 62198 > https [FIN, ACK] Seq=686 Ack=509 Win=131248 Len=0 |
| 378 | 43.995402 | 192.168.3.2 | 176.34.29.205 | TCP | 66 | [TCP Dup ACK 377#1] 62198 > https [ACK] Seq=687 Ack=509 W |
| 379 | 43.998797 | 176.34.29.205 | 192.168.3.2 | TCP | 78 | [TCP Dup ACK 375#1] https > 62198 [ACK] Seq=509 Ack=687 W |

# クリア時通信

Filter: tcp.stream eq 12 Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 386 | 175.923484 | 192.168.3.2 | 176.34.44.136 | TCP | 78 | 62199 > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=7679 |
| 387 | 175.928854 | 176.34.44.136 | 192.168.3.2 | TCP | 74 | https > 62199 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_ |
| 388 | 175.932953 | 192.168.3.2 | 176.34.44.136 | TCP | 66 | 62199 > https [ACK] Seq=1 Ack=1 Win=131760 Len=0 TSval=767967224 TS |
| 389 | 175.940908 | 192.168.3.2 | 176.34.44.136 | TLSv1 | 250 | Client Hello |
| 390 | 175.945717 | 176.34.44.136 | 192.168.3.2 | TCP | 66 | https > 62199 [ACK] Seq=1 Ack=185 Win=15616 Len=0 TSval=1984086711 |
| 391 | 175.946405 | 176.34.44.136 | 192.168.3.2 | TLSv1 | 1514 | Server Hello |
| 392 | 175.946438 | 176.34.44.136 | 192.168.3.2 | TLSv1 | 1408 | Certificate, Server Hello Done |
| 393 | 175.966633 | 192.168.3.2 | 176.34.44.136 | TCP | 66 | 62199 > https [ACK] Seq=185 Ack=2791 Win=128976 Len=0 TSval=767967 |
| 394 | 175.976823 | 192.168.3.2 | 176.34.44.136 | TLSv1 | 333 | Client Key Exchange |
| 395 | 175.977126 | 192.168.3.2 | 176.34.44.136 | TLSv1 | 72 | Change Cipher Spec |
| 396 | 175.977185 | 192.168.3.2 | 176.34.44.136 | TLSv1 | 119 | Encrypted Handshake Message |
| 397 | 175.983921 | 176.34.44.136 | 192.168.3.2 | TCP | 66 | https > 62199 [ACK] Seq=2791 Ack=511 Win=16640 Len=0 TSval=19840867 |
| 398 | 175.984146 | 176.34.44.136 | 192.168.3.2 | TLSv1 | 125 | Change Cipher Spec, Encrypted Handshake Message |
| 399 | 175.991718 | 192.168.3.2 | 176.34.44.136 | TCP | 66 | 62199 > https [ACK] Seq=511 Ack=2850 Win=131008 Len=0 TSval=767967 |
| 400 | 175.993001 | 192.168.3.2 | 176.34.44.136 | TLSv1 | 487 | Application Data |
| 401 | 176.037928 | 176.34.44.136 | 192.168.3.2 | TCP | 66 | https > 62199 [ACK] Seq=2850 Ack=932 Win=17920 Len=0 TSval=19840867 |
| 402 | 176.133139 | 176.34.44.136 | 192.168.3.2 | TLSv1 | 487 | Application Data |
| 403 | 176.133199 | 176.34.44.136 | 192.168.3.2 | TLSv1 | 103 | Encrypted Alert |
| 404 | 176.135093 | 192.168.3.2 | 176.34.44.136 | TCP | 66 | 62199 > https [ACK] Seq=932 Ack=3271 Win=130640 Len=0 TSval=7679674 |
| 405 | 176.135440 | 192.168.3.2 | 176.34.44.136 | TCP | 66 | 62199 > https [ACK] Seq=932 Ack=3308 Win=130608 Len=0 TSval=7679674 |
| 406 | 176.137335 | 192.168.3.2 | 176.34.44.136 | TLSv1 | 103 | Encrypted Alert |
| 407 | 176.138826 | 192.168.3.2 | 176.34.44.136 | TCP | 66 | 62199 > https [FIN, ACK] Seq=969 Ack=3308 Win=131072 Len=0 TSval=76 |
| 408 | 176.142254 | 176.34.44.136 | 192.168.3.2 | TCP | 66 | https > 62199 [ACK] Seq=3308 Ack=969 Win=17920 Len=0 TSval=19840867 |
| 409 | 176.142290 | 176.34.44.136 | 192.168.3.2 | TCP | 66 | https > 62199 [FIN, ACK] Seq=3308 Ack=969 Win=17920 Len=0 TSval=198 |
| 410 | 176.143685 | 176.34.44.136 | 192.168.3.2 | TCP | 66 | https > 62199 [ACK] Seq=3309 Ack=970 Win=17920 Len=0 TSval=19840867 |
| 411 | 176.144282 | 192.168.3.2 | 176.34.44.136 | TCP | 66 | 62199 > https [FIN, ACK] Seq=969 Ack=3308 Win=131072 Len=0 TSval=76 |
| 412 | 176.145489 | 192.168.3.2 | 176.34.44.136 | TCP | 66 | 62199 > https [FIN, ACK] Seq=969 Ack=3309 Win=131072 Len=0 TSval=76 |
| 413 | 176.147548 | 192.168.3.2 | 176.34.44.136 | TCP | 66 | [TCP Dup ACK 412#1] 62199 > https [ACK] Seq=970 Ack=3309 Win=131072 |
| 414 | 176.148974 | 176.34.44.136 | 192.168.3.2 | TCP | 78 | [TCP Dup ACK 410#1] https > 62199 [ACK] Seq=3309 Ack=970 Win=17920 |

# ダンジョン中は通信しない

| | | | | | |
|---|---|---|---|---|---|
| 376 | 43.993409 | 192.168.3.2 | 176.34.29.205 | TCP | 66 62198 > https [FIN, ACK] Seq=686 Ack=508 Win=1 |
| 377 | 43.994295 | 192.168.3.2 | 176.34.29.205 | TCP | 66 62198 > https [FIN, ACK] Seq=686 Ack=509 Win=1 |
| 378 | 43.995402 | 192.168.3.2 | 176.34.29.205 | TCP | 66 [TCP Dup ACK 377#1] 62198 > https [ACK] Seq=68 |
| 379 | 43.996797 | 176.34.29.205 | 192.168.3.2 | TCP | 78 [TCP Dup ACK 375#1] https > 62198 [ACK] Seq=50 |
| 380 | 69.371119 | c8:6f:1d:1c:e6:11 | 46:2a:60:2f:5b:64 | ARP | 42 Who has 192.168.3.1? Tell 192.168.3.2 |
| 381 | 69.371140 | 46:2a:60:2f:5b:64 | c8:6f:1d:1c:e6:11 | ARP | 42 192.168.3.1 is at 46:2a:60:2f:5b:64 |
| 382 | 159.342840 | c8:6f:1d:1c:e6:11 | 46:2a:60:2f:5b:64 | ARP | 42 Who has 192.168.3.1? Tell 192.168.3.2 |
| 383 | 159.342879 | 46:2a:60:2f:5b:64 | c8:6f:1d:1c:e6:11 | ARP | 42 192.168.3.1 is at 46:2a:60:2f:5b:64 |
| 384 | 175.907175 | 192.168.3.2 | 192.168.3.1 | DNS | 120 Standard query A PAD-production-LB-608318448.a |
| 385 | 175.918023 | 192.168.3.1 | 192.168.3.2 | DNS | 248 Standard query response A 176.34.44.136 A 175. |
| 386 | 175.927484 | 192.168.3.2 | 176.34.44.136 | TCP | 78 62199 > https [SYN] Seq=0 Win=65535 Len=0 MSS= |
| 387 | 175.928854 | 176.34.44.136 | 192.168.3.2 | TCP | 74 https > 62199 [SYN, ACK] Seq=0 Ack=1 Win=1448 |
| 388 | 175.932953 | 192.168.3.2 | 176.34.44.136 | TCP | 66 62199 > https [ACK] Seq=1 Ack=1 Win=131760 Len |
| 389 | 175.940908 | 192.168.3.2 | 176.34.44.136 | TLSv1 | 250 Client Hello |
| 390 | 175.945717 | 176.34.44.136 | 192.168.3.2 | TCP | 66 https > 62199 [ACK] Seq=1 Ack=185 Win=15616 Le |
| 391 | 175.946405 | 176.34.44.136 | 192.168.3.2 | TLSv1 | 1514 Server Hello |
| 392 | 175.946438 | 176.34.44.136 | 192.168.3.2 | TLSv1 | 1408 Certificate, Server Hello Done |

# pazdoraのパケットまとめ

- プロトコル
  - HTTPSで基本的には通信
  - Bannerを取得する部分はHTTP
- パケットサイズ
  - SSL通信は大きいものも含む
  - ゲームのパケットは基本的にショートパケット
- 基本的にゲーム中は通信しない
- 都度セッションを張りにいく

# 黒猫のウィズ

# 黒猫のウィズ

- 観測されたTCPストリームは合計９本

- 起動→お知らせ画面表示
- ガチャを一回引く
- ダンジョン潜入
- クリア
- 元の画面に戻る

# 起動、ガチャを引く、ダンジョン潜入

- 0.
  - 54.249.246.3:80 HTTP
    - quiz.colopl.jp
    - ec2-54-249-246-3.ap-northeast-1.compute.amazonaws.com.
      - Amazon EC2
  - HTTPでのやり取り。データはバイナリなので中身はよくわからないがリクエストを見るとなんとなく何をしているか想像できる
    - POST /notification/register HTTP/1.1
    - POST /register/checkregister HTTP/1.1
    - POST /dataresponse?rt=8 HTTP/1.1
    - POST /dataresponse?rt=9 HTTP/1.1
    - POST /stamp/stamp HTTP/1.1
    - POST /dataresponse?rt=5 HTTP/1.1
    - POST /dataresponse?rt=8 HTTP/1.1
    - POST /stamp/stamp HTTP/1.1
    - POST /loginquiz/get HTTP/1.1
    - POST /gacha/list HTTP/1.1
    - POST /gacha/exe HTTP/1.1
    - POST /dataresponse?rt=5 HTTP/1.1

# 起動、ガチャを引く、ダンジョン潜入

- POST /dataresponse?rt=8 HTTP/1.1
- POST /stamp/stamp HTTP/1.1
- POST /loginquiz/get HTTP/1.1
- POST /dataresponse?rt=6 HTTP/1.1
- POST /dataresponse?rt=8 HTTP/1.1
- POST /dataresponse/dungeonlist HTTP/1.1
- POST /dungeon/list?evid=5102&reqhelplist=1 HTTP/1.1
- POST /dungeon/getstepdeck HTTP/1.1

- 起動、ガチャを引く、ダンジョン潜入までの流れとほぼ一致、時間も一致

- ひとつのTCP Connectionで起動からダンジョン潜入までを行っている

# その他の通信

- 1.
  - 54.249.246.3:80 HTTP
    - 0.と同じ
  - time: 5, 35(FIN)
  - GET /news/show/?osType=ios&ver=1.5.4&i=MTg3OTAyMzU= HTTP/1.1
    - HTTPだが中身はバイナリデータでよく分からない
  - 起動後、スタートボタンを押した後の「お知らせ画面」のデータを取得するものと思われる

- 2.
  - 173.194.126.211:443 HTTPS
    - PTR: nrt04s08-in-f19.1e100.net
  - time: 155
    - ダンジョン中の通信
  - GoogleへのhttpsアクセスO。関係なし？
    - Server Certificateを見るとcnがwww.google.com

# 黒猫のウィズのパケットのまとめ

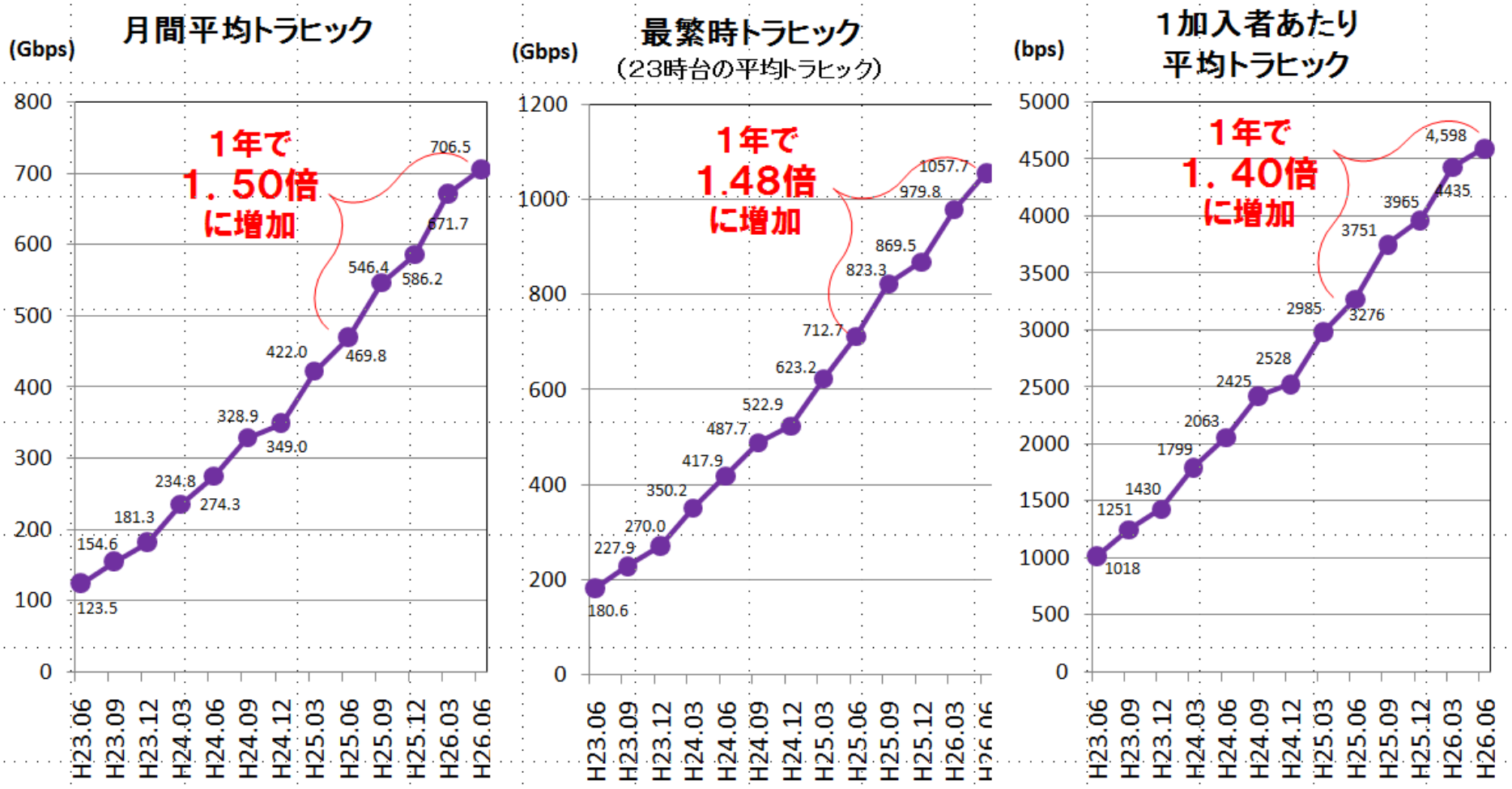
- プロトコル
  - HTTPで基本的には通信
  - GoogleへのHTTPSアクセスが途中途中発生
- パケットサイズ
  - SSL通信は大きいものも含む
  - ゲームのパケットは基本的にショートパケット
- Googleへのhttpsアクセスを除けば、ゲーム中は特にゲーム自体の通信は基本なし
- セッションは最初に張ったものを利用し続ける

# 何を気にしないといけない？

- ppsのrateが上昇している
  - 個々のトラフィック量はそれほど多くないが、多くのパケットをさばいている状態が発生している
    - Packetサイズが1/3 --> pps rateが３倍！
  - 装置によっては、short packetの処理に影響しパフォーマンスが落ちる可能性があるので要注意！
- アプリケーションの作りに影響する
  - とくにスマホのトラフィック影響が大きい

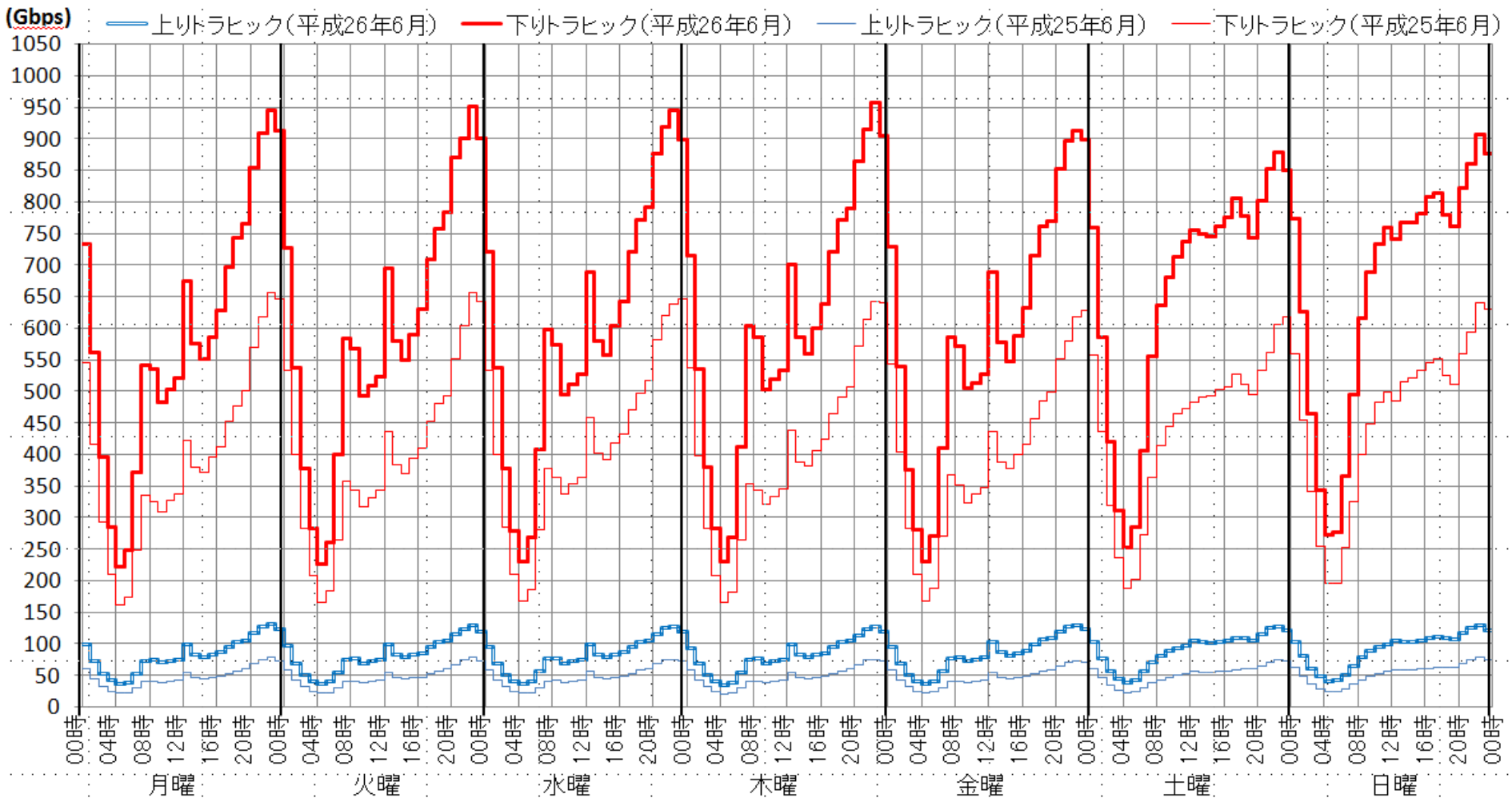
- 少し違った観点でネットワーク屋さんが通信状況やトラフィックの流量を見ていく必要がある

# 移動通信トラフィックの推移




出典：総務省 我か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

# 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
    - 位置の特定は出来る範囲で
- カンファレンス会場でIPv4アドレスが枯渇？
  - 最近ネットに接続する端末が一人２つ以上になっている
  - IPv6でアクセスして、途中のリンクがIPv4のため通信できない
  - 利用者がIPv4/IPv6プロトコルを意識しないところは良いが、何故つながらないかがわかりにくい状況が起きている

# 現状と今後の課題

- トラフィックの変動が多様化
  - 状況を定期的に把握
- 正しい情報を利用者に提供する
- 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
- HyperGiantとEyeBall間のトラフィック変動
  - 最適化のすり合わせが今後重要

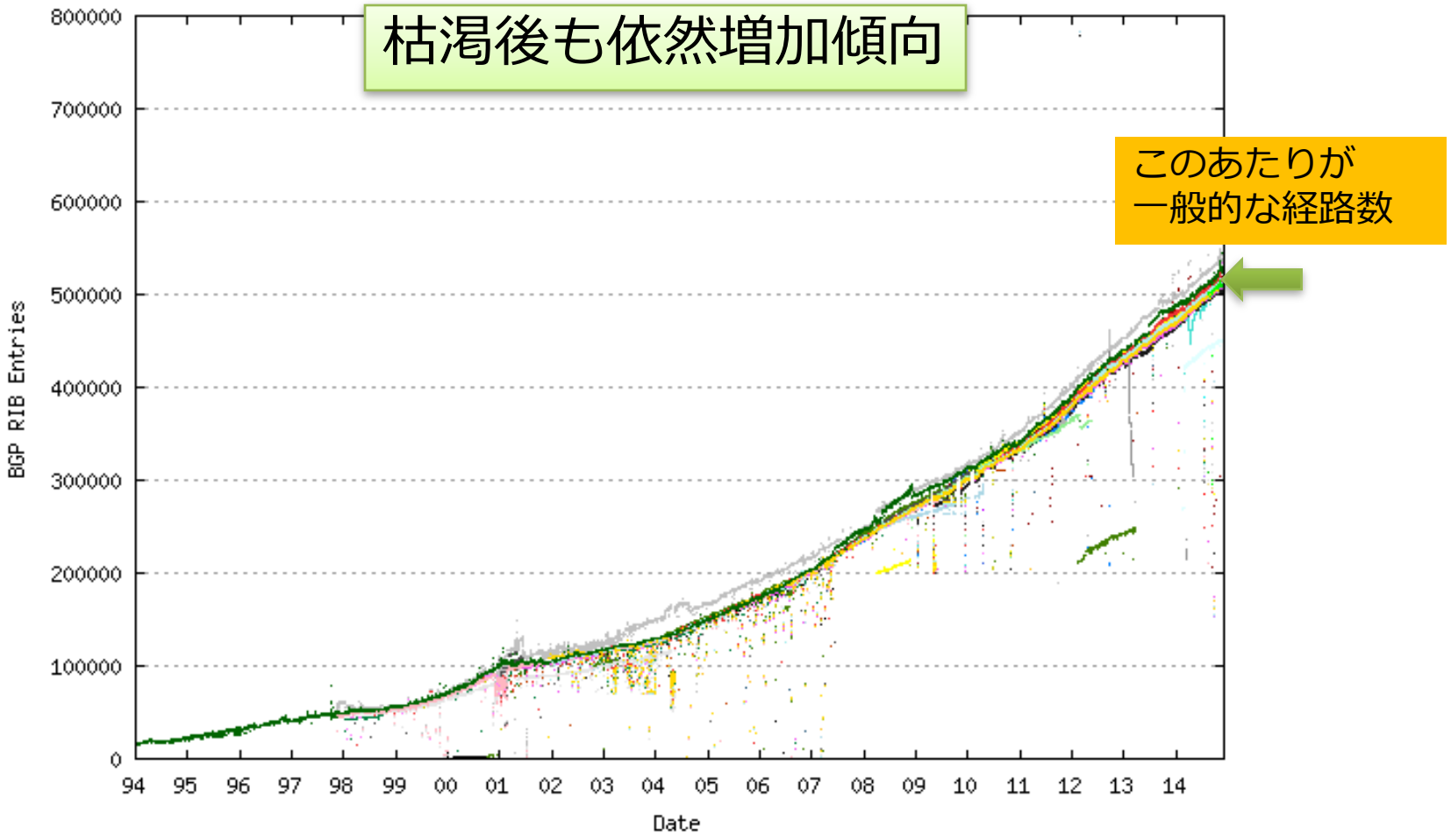
# 内容

- 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
- 日本や世界のIX動向
- まとめ

# ルーティング動向

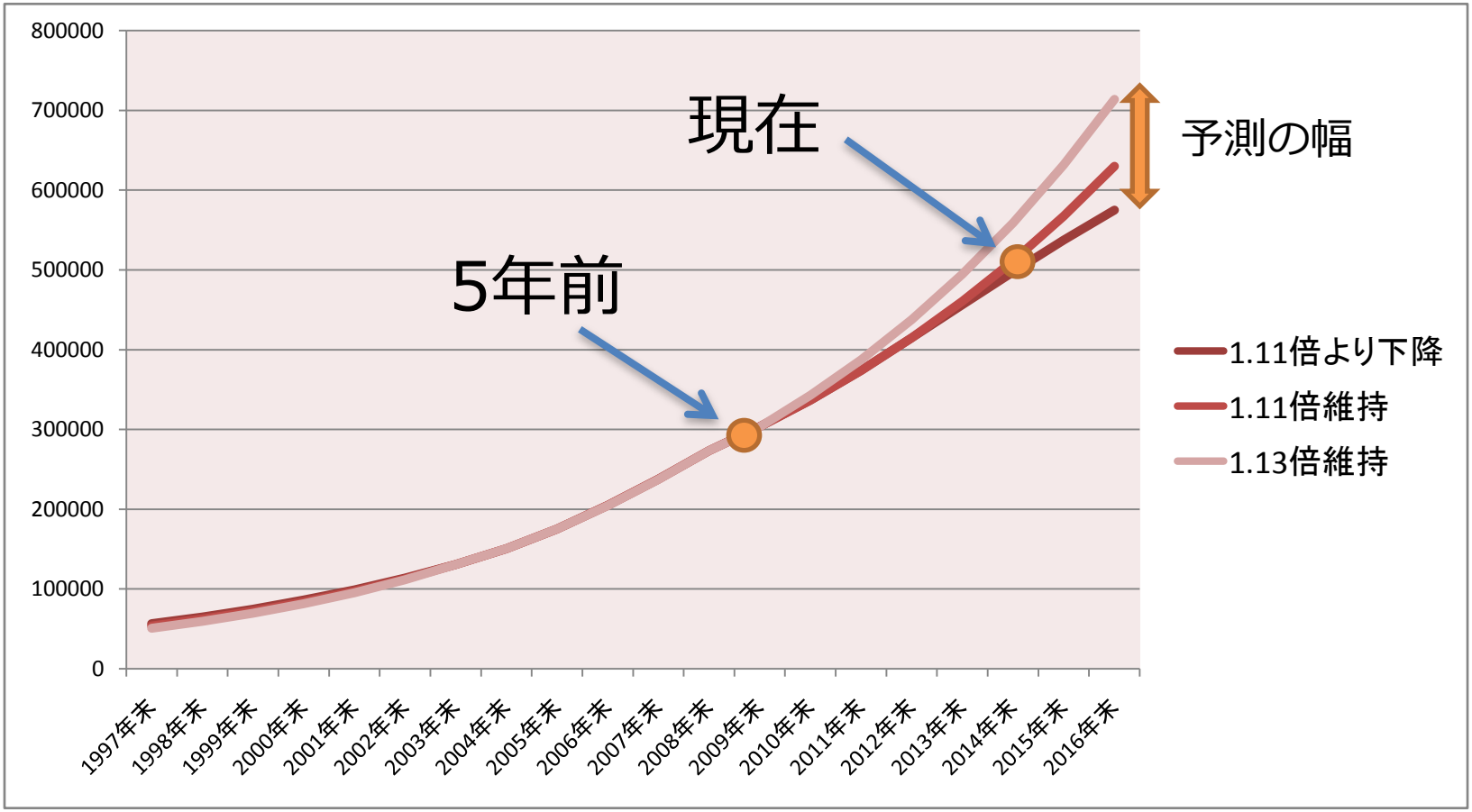
- IPv4経路が51万経路に到達
  （2セッション張ると100万超）
  - 年増加率は変わらず約1.1倍で引き続き枯渇後も増加
  - /24は依然全体の半分超
- IPv6経路は約2万経路に
  - 年間で約5000経路の増加
  - 本格的な利用者と様子見と二分している状況
- AS番号の枯渇対応 ⇒ 4byteASへの移行が促進
  - ここ最近は大きな問題は発生していない
  - 上位ISPが4byteに未対応のところが依然存在
    ⇒日本国内にも複数ある

# IPv4経路数の推移




http://bgp.potaroo.net/

# IPv4経路数推移予測
# (5年前の2009年末予測)

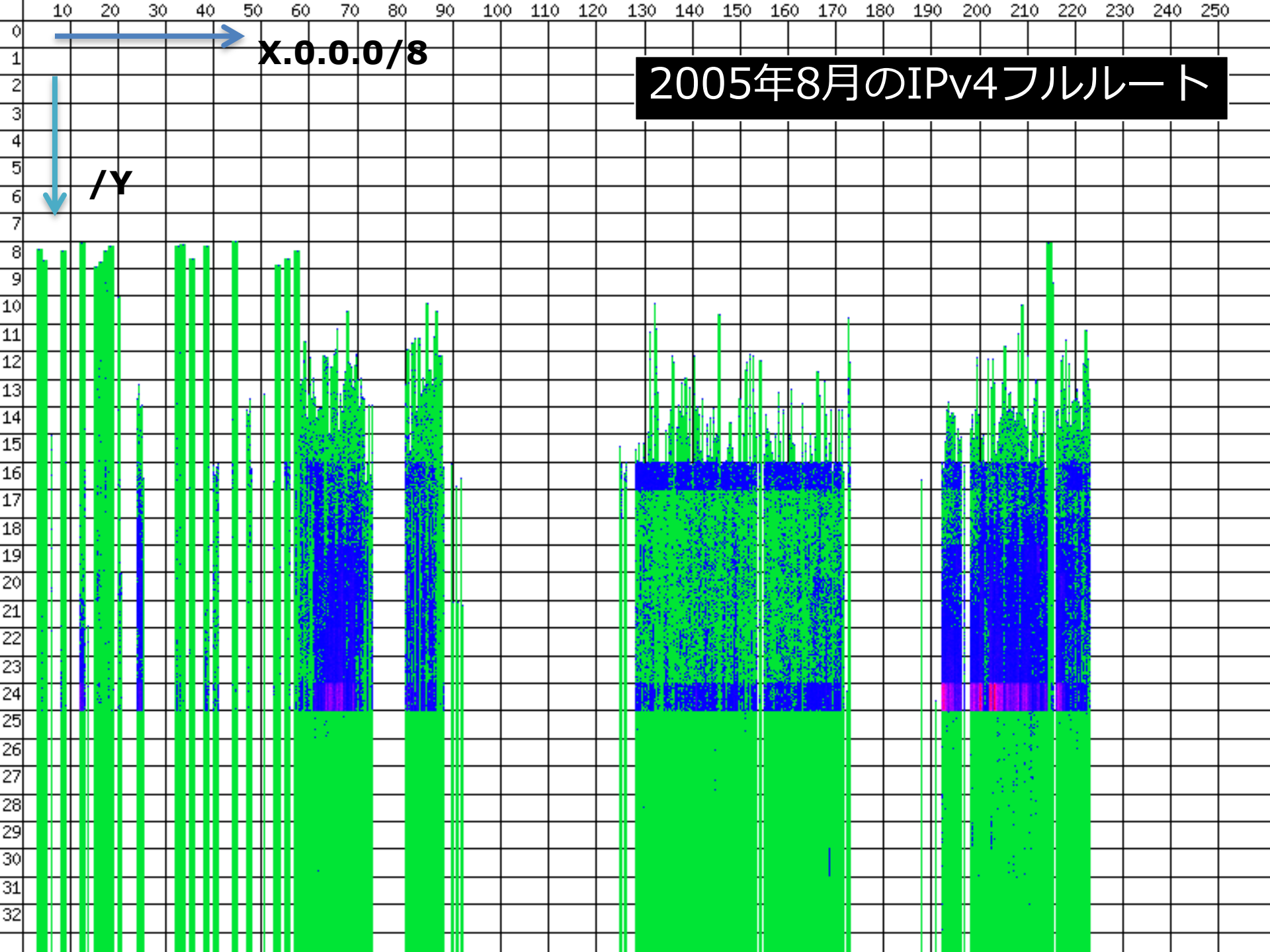


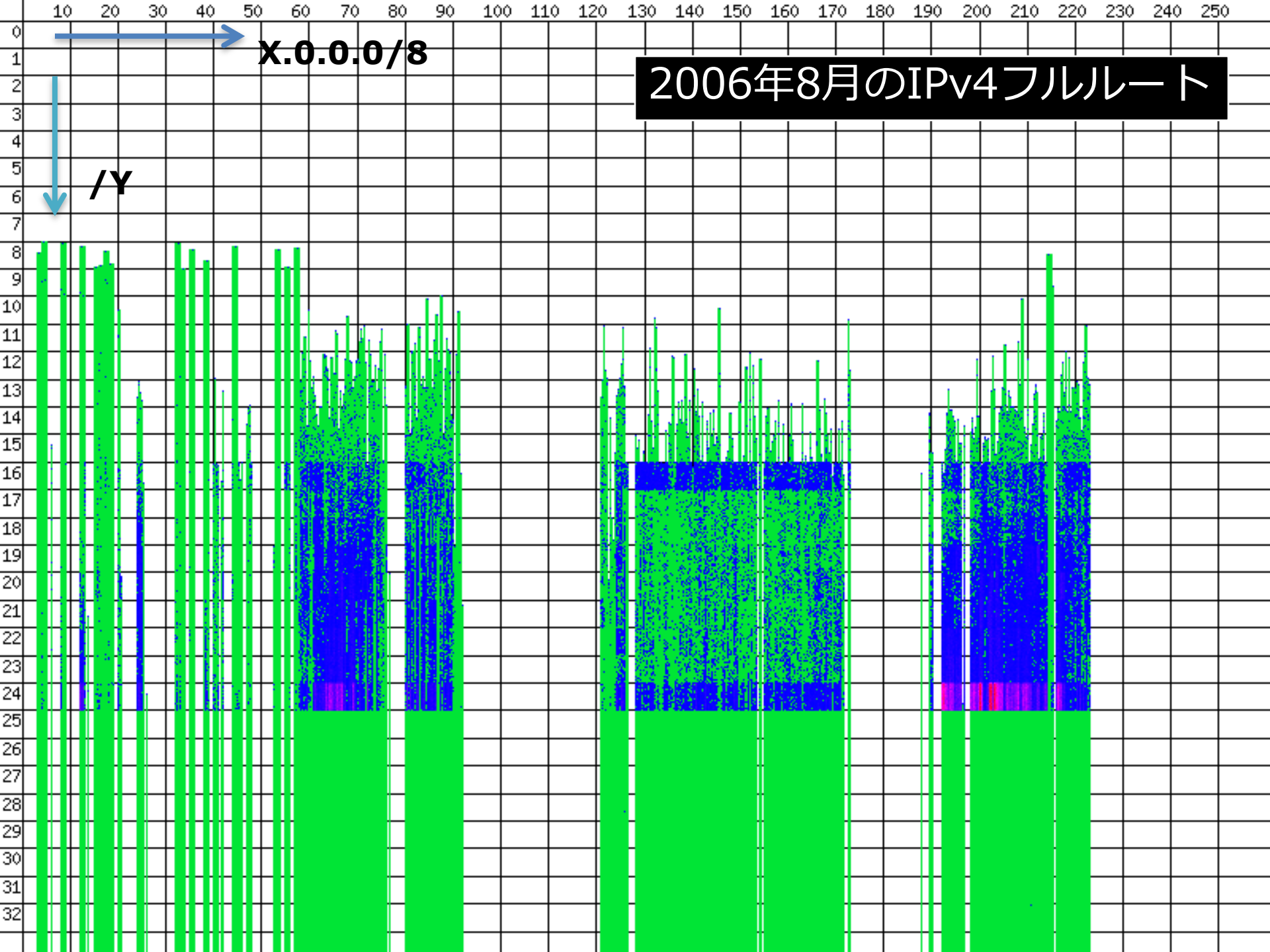

IPv4アドレスの枯渇後、緩やかに増加し続けている
依然IPv4アドレスの流通や細分化が進み経路数増加を牽引

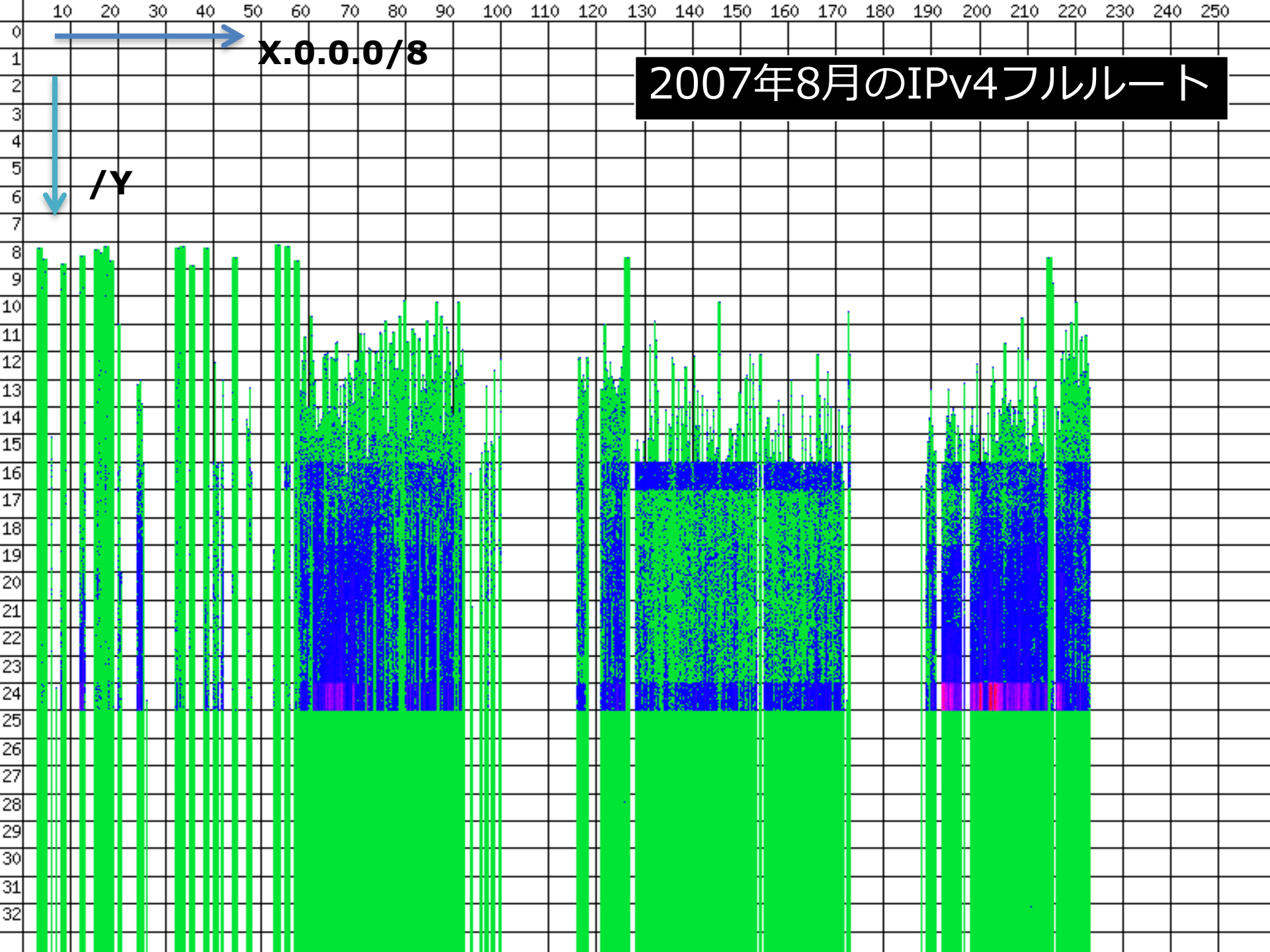
# IPv4フルルート512Kの壁

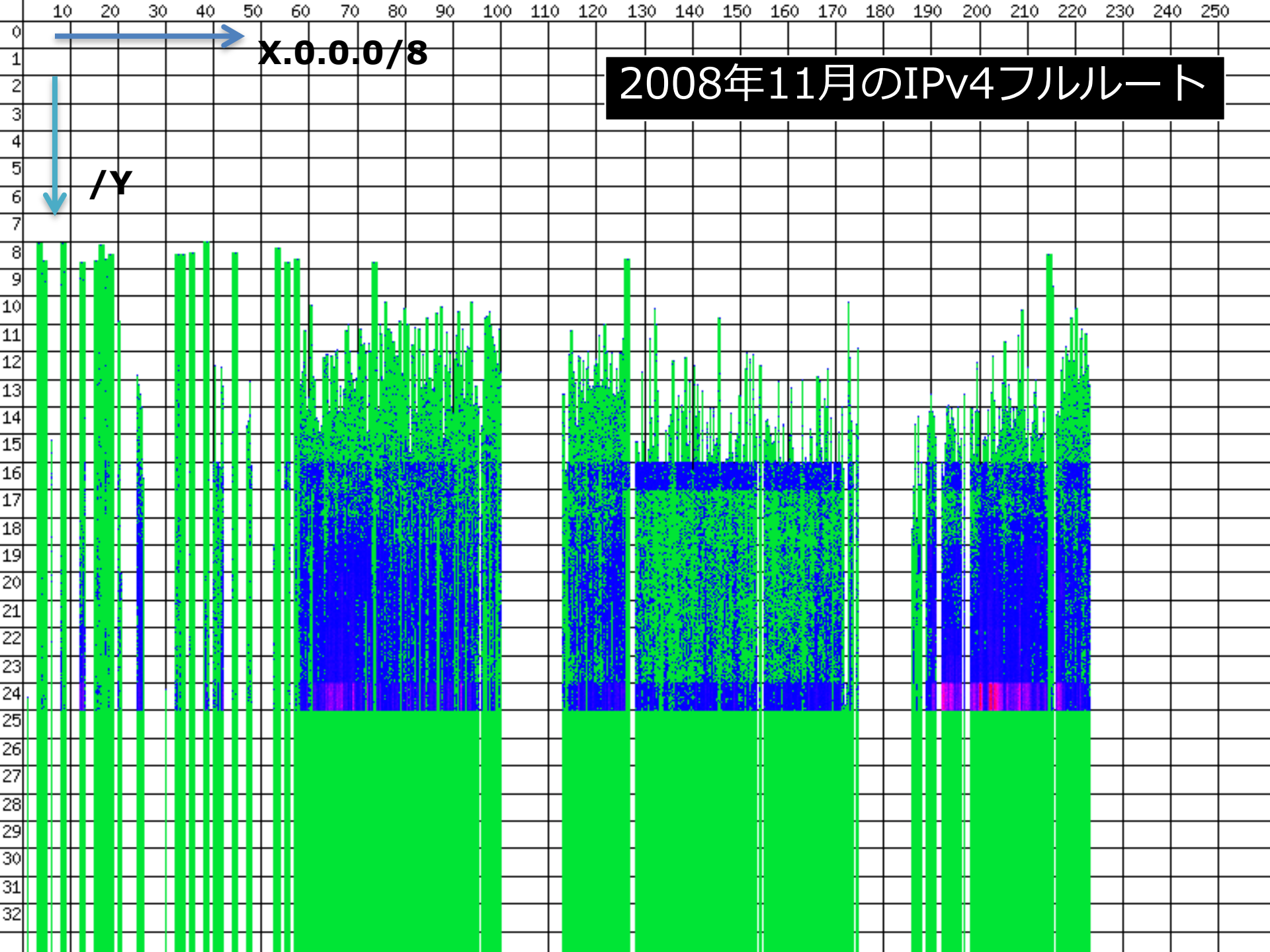
- JANOG等でも春先から注意喚起がされていた
- が、ばたばた512Kの壁にやられた人が散見
  - JPNAPでも複数の緊急メンテナンスを実施されているISPさんがいた
  - 192K, 224K等昔の頃よりは少なかった？
  - 内部BGP経路が大量に存在するISPでは600K前後

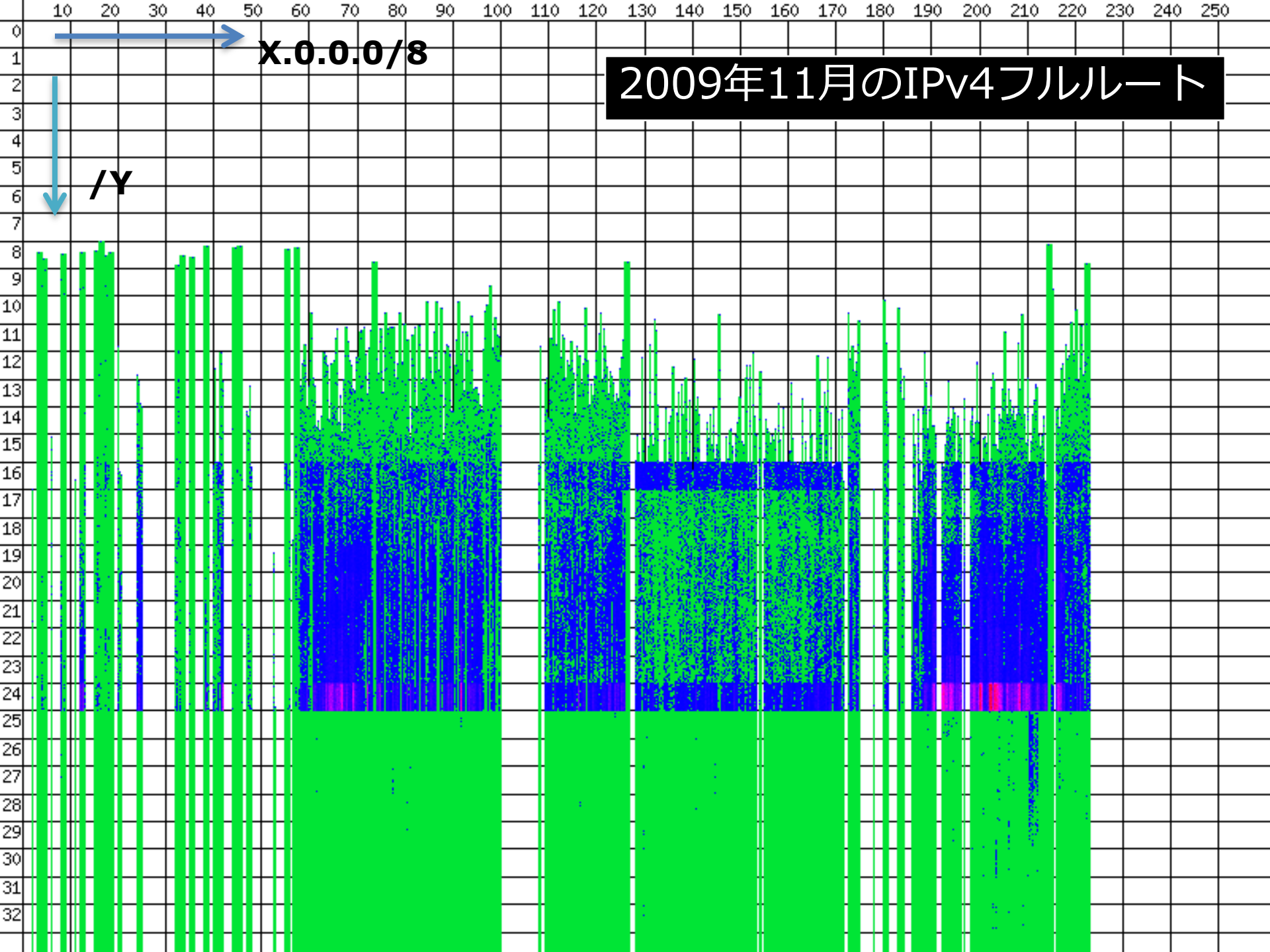
- フルルートが悪だといった風潮は間違い
- 適切にフルルートを活用し、インターネットのルーティングを行う必要がある

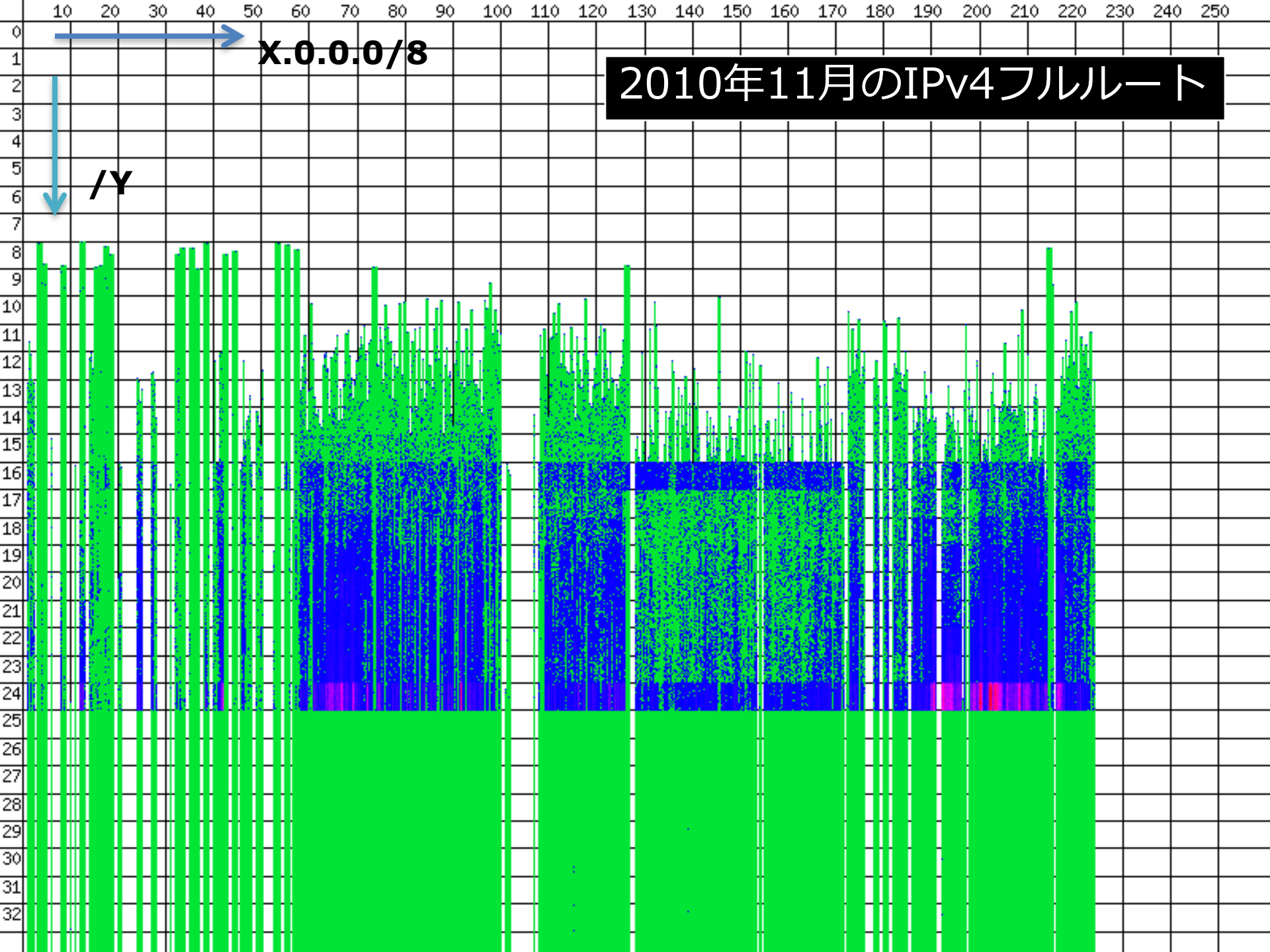

10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
x.0.0.0/8
/Y
2005年8月のIPv4フルルート

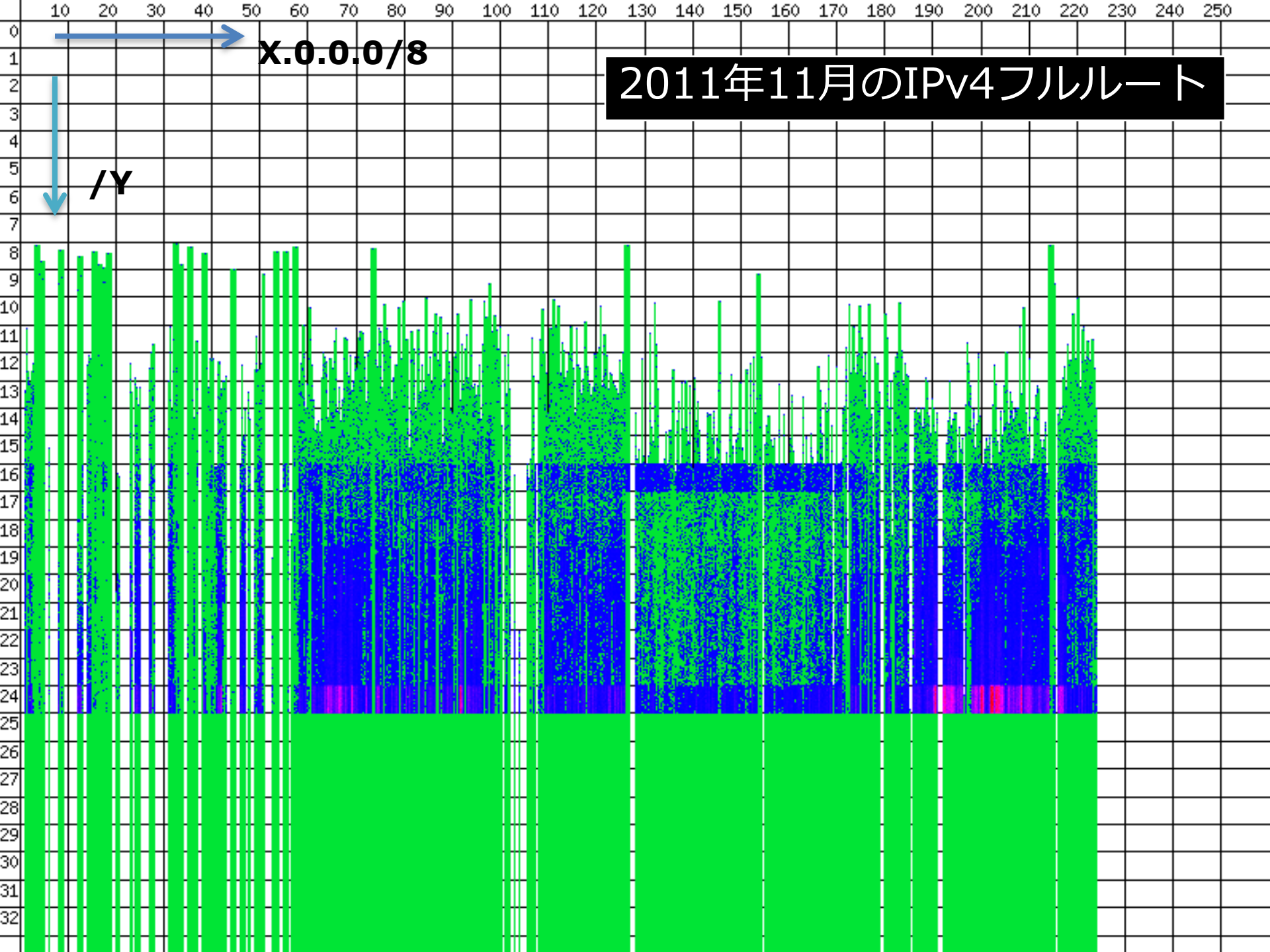

10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
x.0.0.0/8
/Y
2006年8月のIPv4フルルート

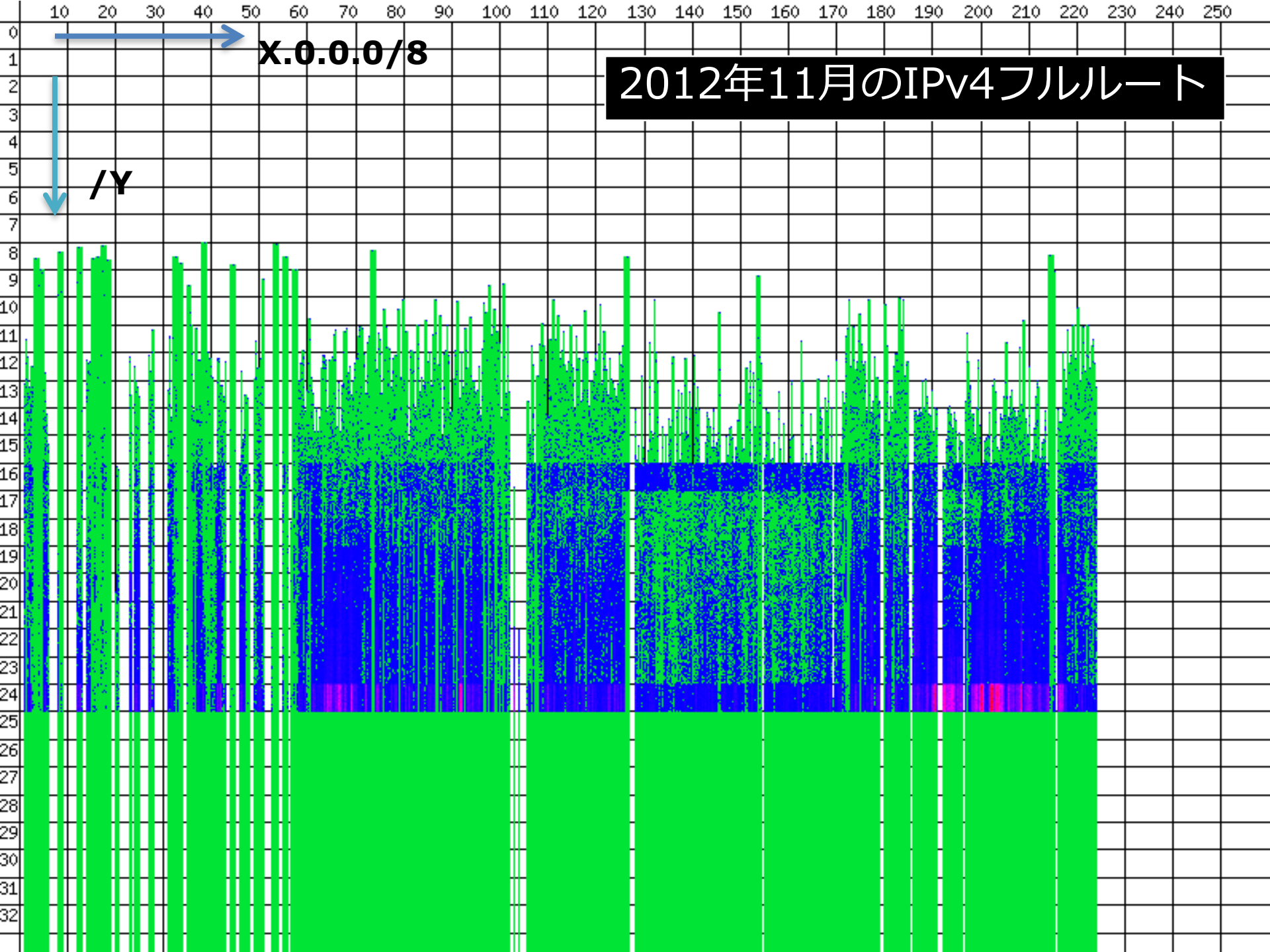

10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
x.0.0.0/8
/Y
2007年8月のIPv4フルルート

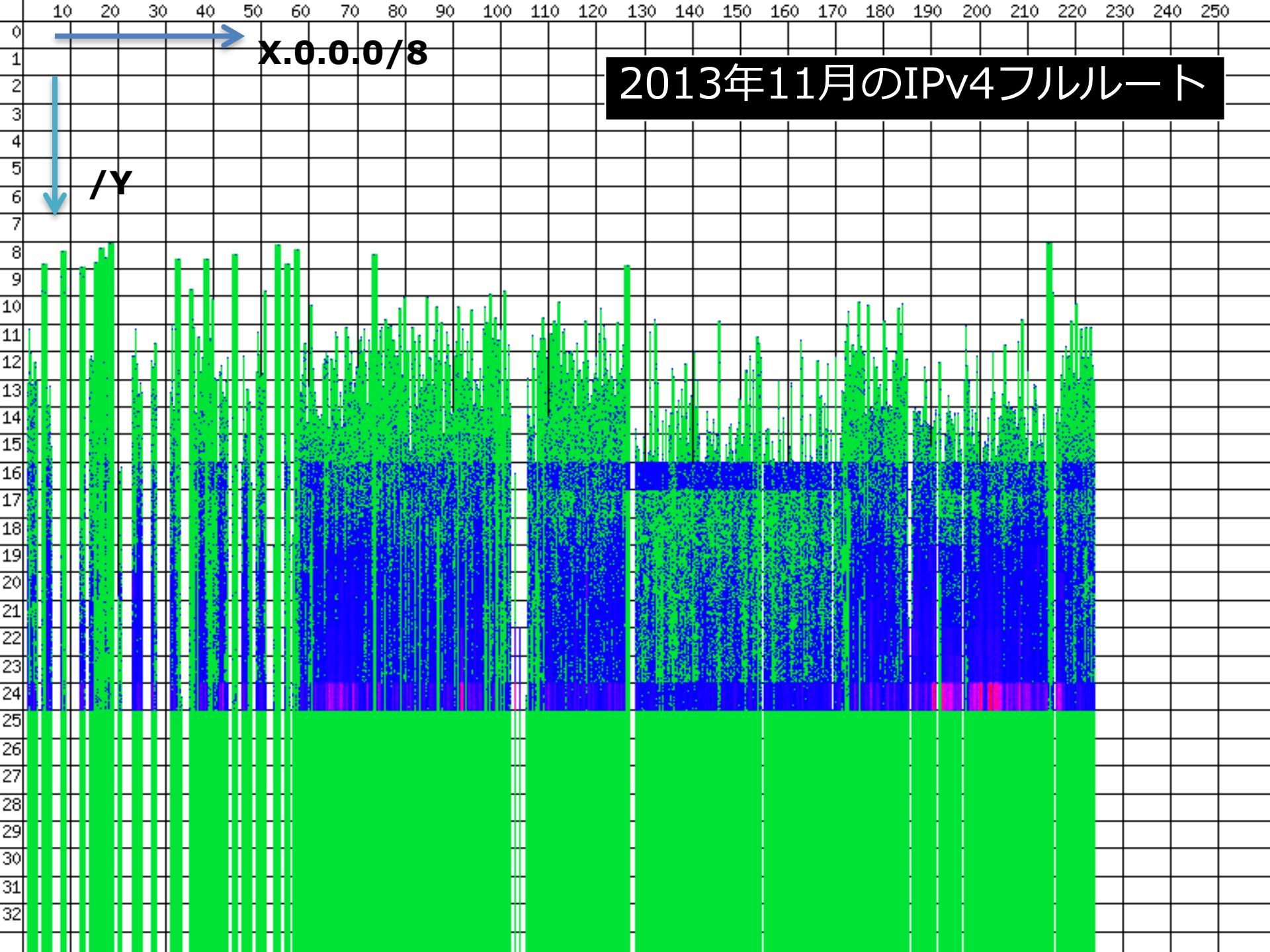

10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
x.0.0.0/8
/Y
2008年11月のIPv4フルルート

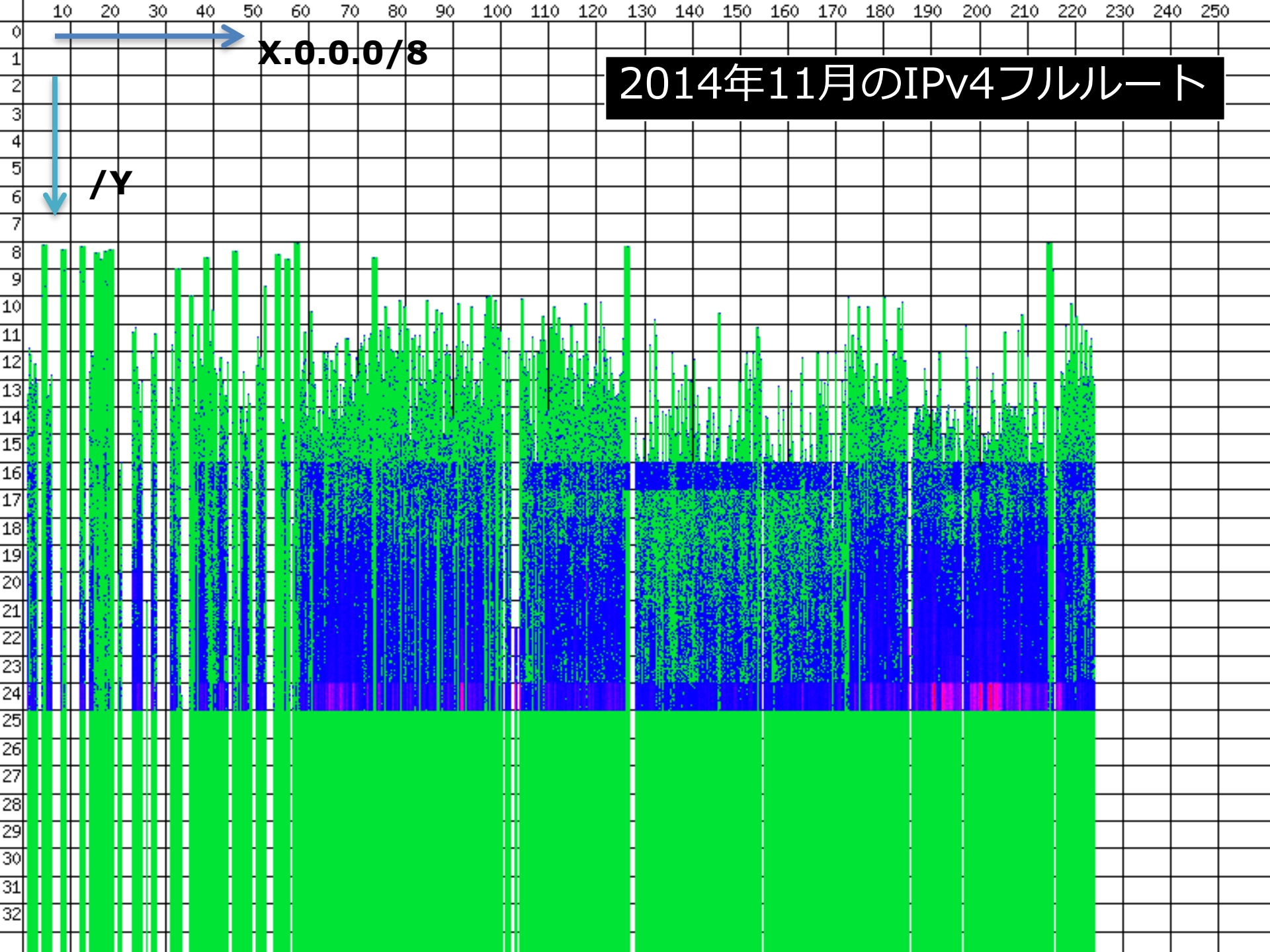

10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
x.0.0.0/8
/Y
2009年11月のIPv4フルルート


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

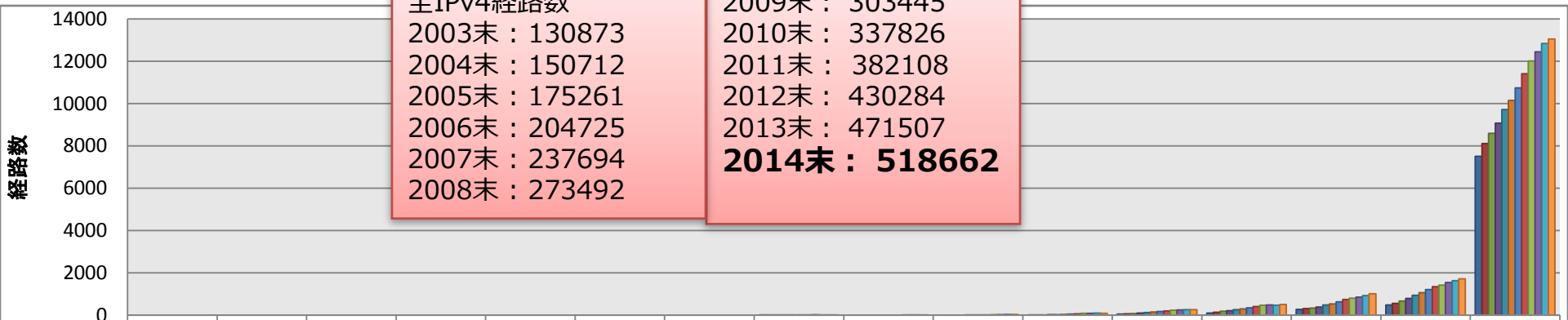

x.0.0.0/8
/Y
2013年11月のIPv4フルルート


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
2014年11月のIPv4フルルート

# IPv4経路数の推移

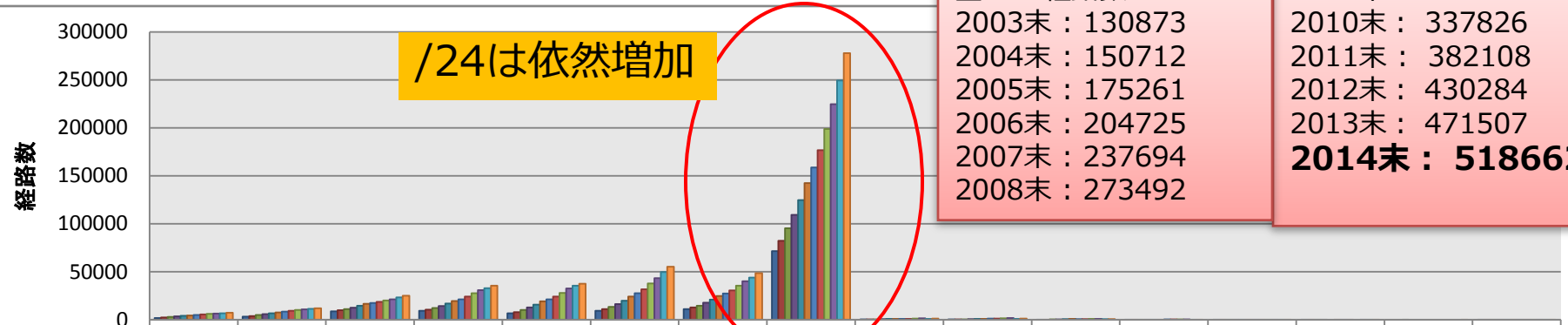
全IPv4経路数
2003末：130873
2004末：150712
2005末：175261
2006末：204725
2007末：237694
2008末：273492

2009末： 303445
2010末： 337826
2011末： 382108
2012末： 430284
2013末： 471507
**2014末： 518662**




| | /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 |

# IPv4経路数の推移



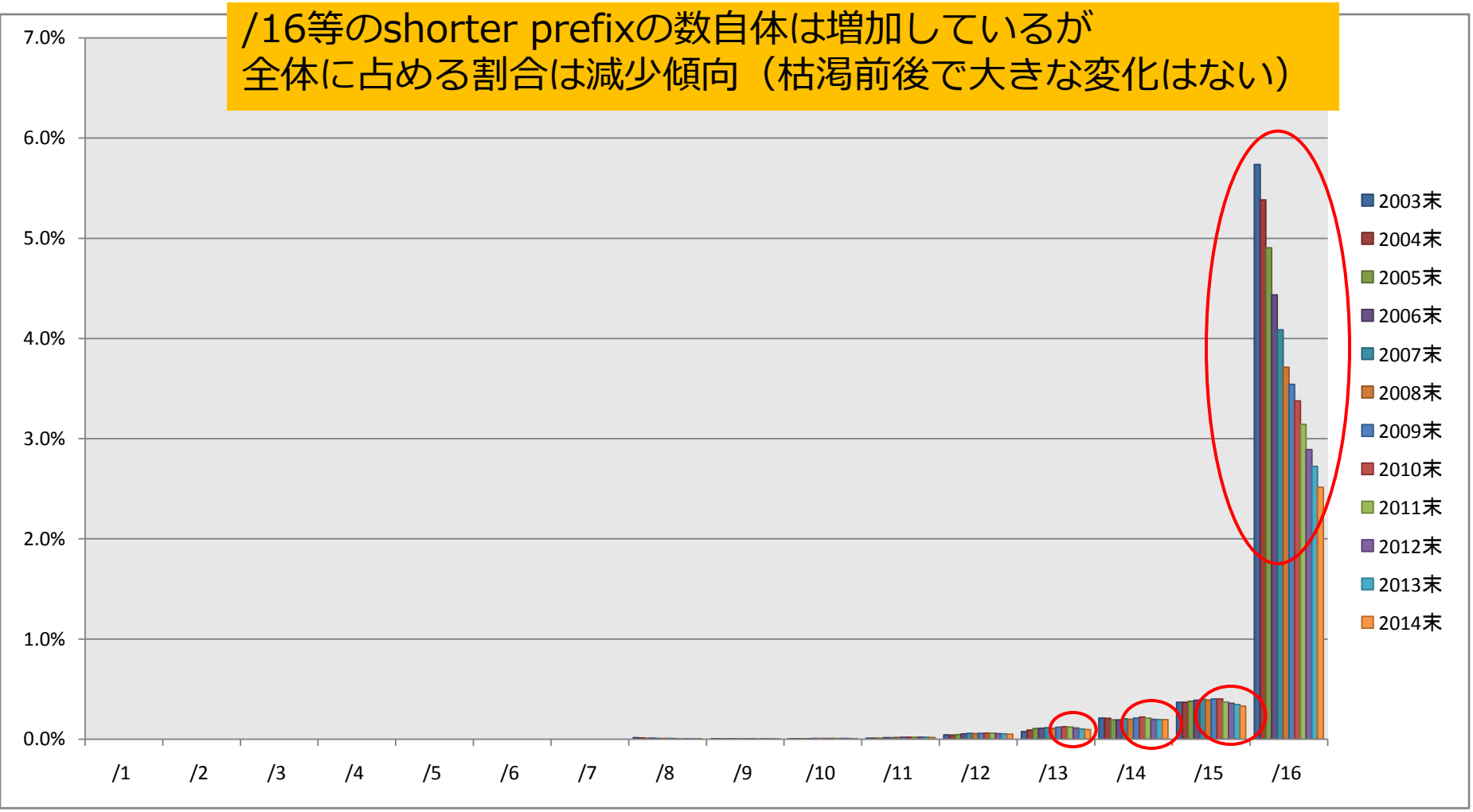

全IPv4経路数
2003末：130873
2004末：150712
2005末：175261
2006末：204725
2007末：237694
2008末：273492

2009末： 303445
2010末： 337826
2011末： 382108
2012末： 430284
2013末： 471507
**2014末： 518662**

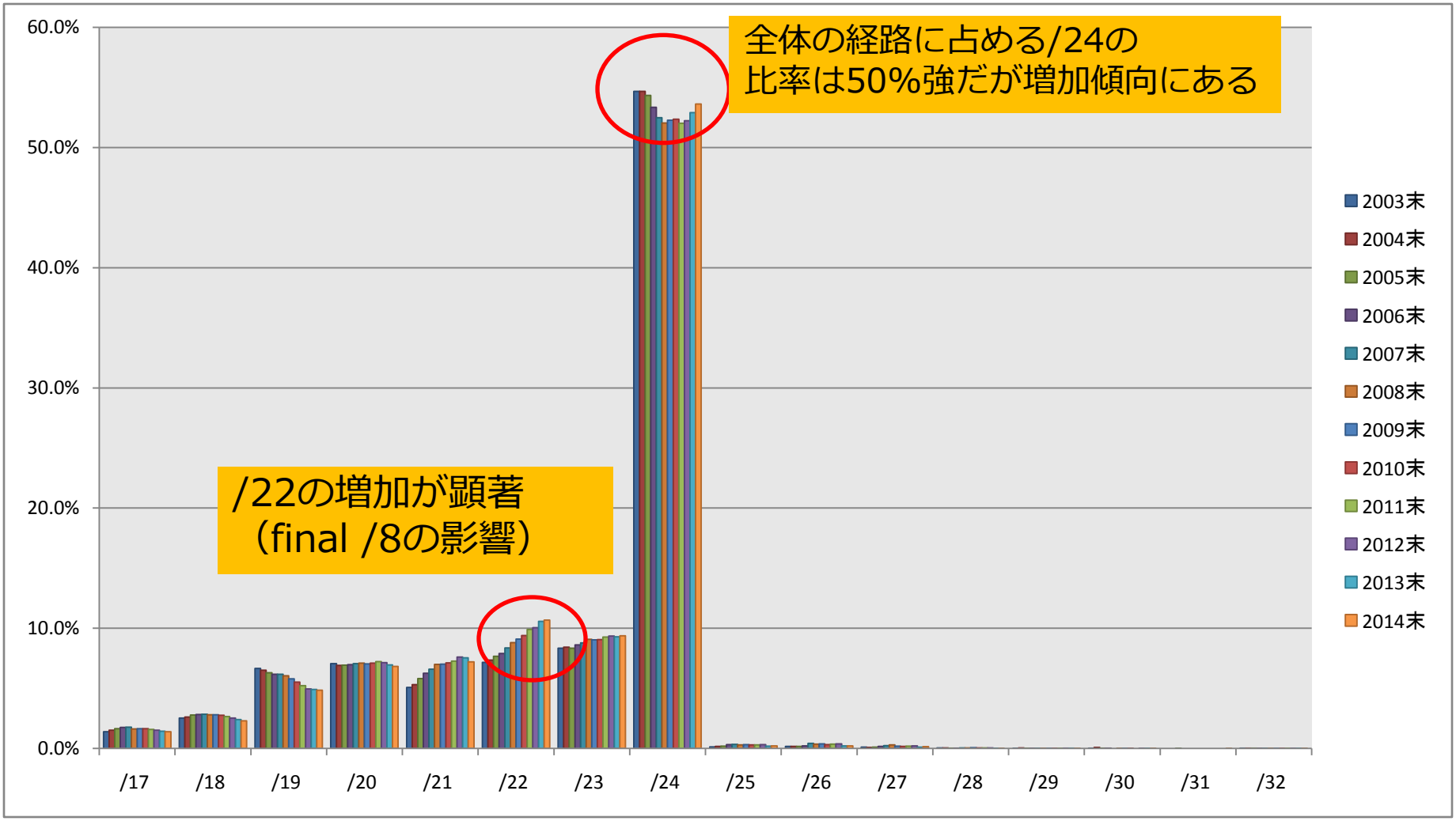
| | /17 | /18 | /19 | /20 | /21 | /22 | /23 | /24 | /25 | /26 | /27 | /28 | /29 | /30 | /31 | /32 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2003末 | 1829 | 3334 | 8716 | 9249 | 6656 | 9386 | 10943 | 71541 | 182 | 233 | 156 | 70 | 21 | 50 | 0 | 41 |
| 2004末 | 2270 | 3933 | 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 |

# IPv4経路数の推移（割合）

/16等のshorter prefixの数自体は増加しているが
全体に占める割合は減少傾向（枯渇前後で大きな変化はない）



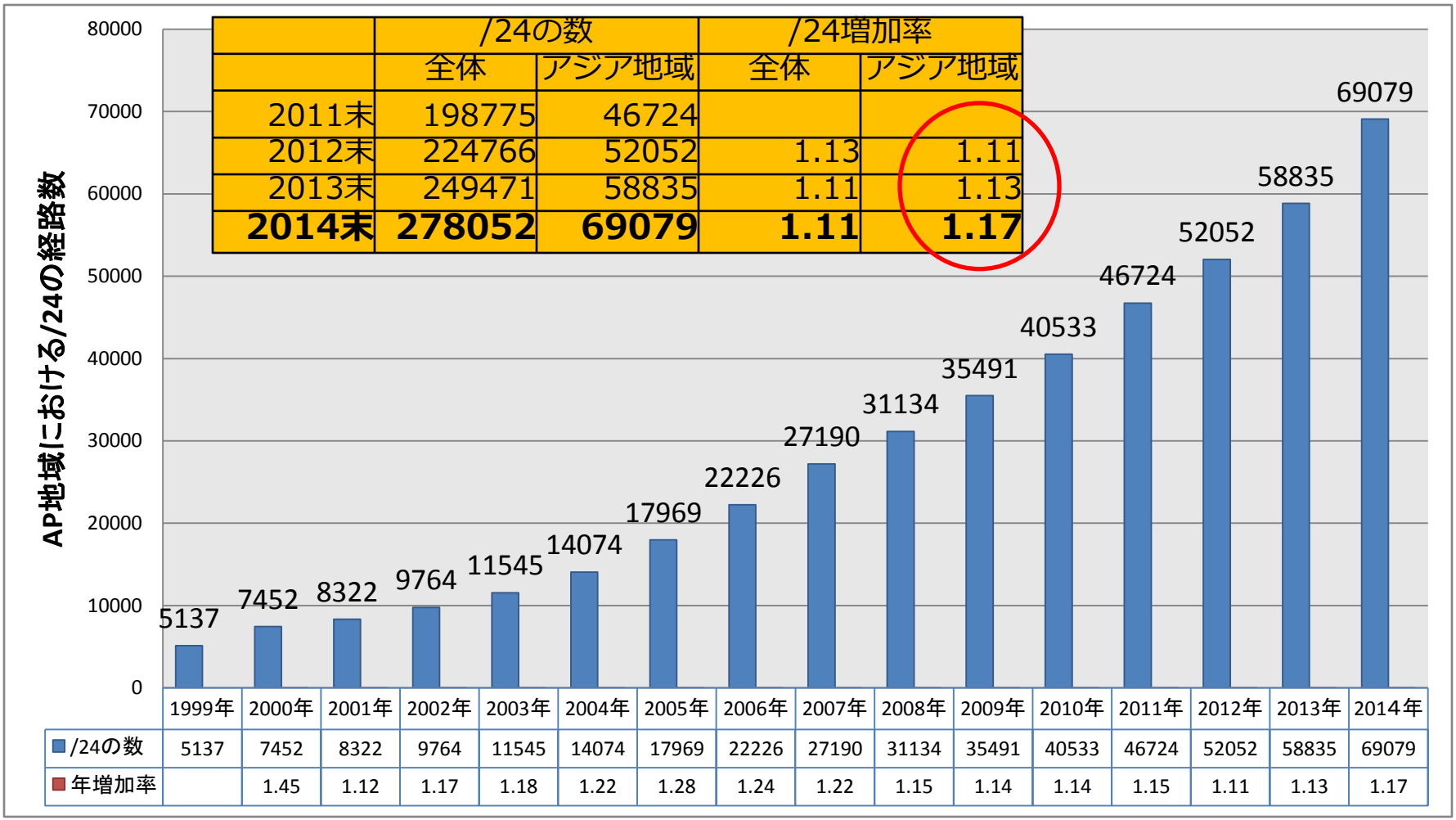
# IPv4経路数の推移（割合）



# AP地域の/24の推移

## AP地域の/24増加率が1.17倍に（世界全体では1.11）

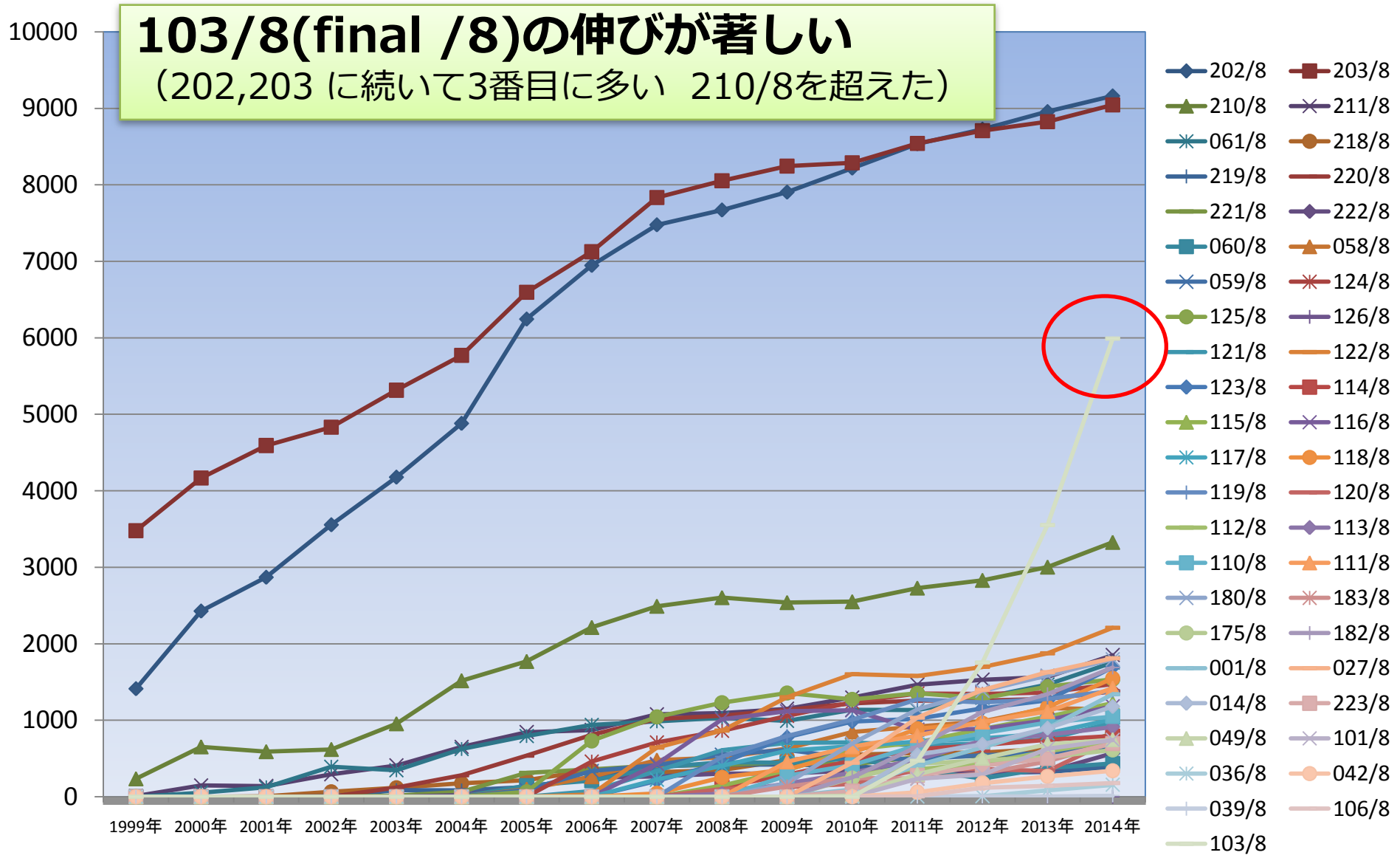
注：移転も含まれるため誤差あり



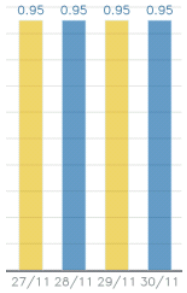

| | /24の数 | | /24増加率 | |
|---|---|---|---|---|
| | 全体 | アジア地域 | 全体 | アジア地域 |
| 2011末 | 198775 | 46724 | | |
| 2012末 | 224766 | 52052 | 1.13 | 1.11 |
| 2013末 | 249471 | 58835 | 1.11 | 1.13 |
| **2014末** | **278052** | **69079** | **1.11** | **1.17** |

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| /24の数 | 5137 | 7452 | 8322 | 9764 | 11545 | 14074 | 17969 | 22226 | 27190 | 31134 | 35491 | 40533 | 46724 | 52052 | 58835 | 69079 |
| 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 |

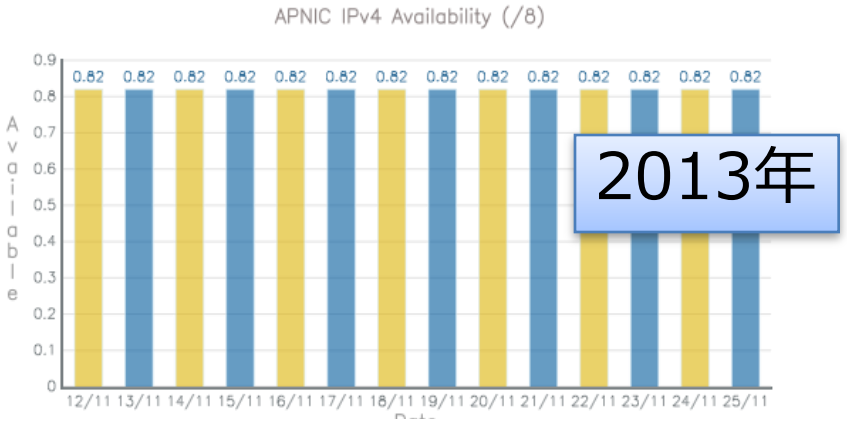
# AP地域の/24の推移



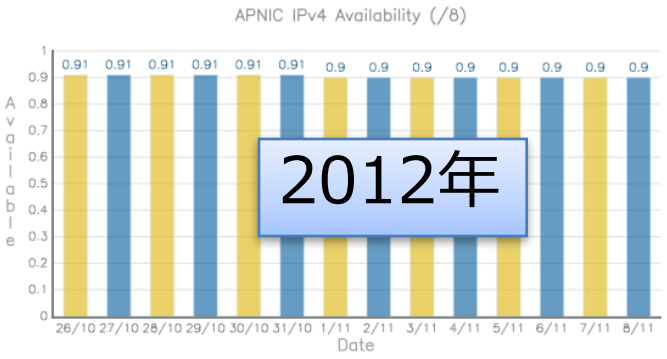
# AP地域の最後の/8
# 103/8 (2011年～2014年)



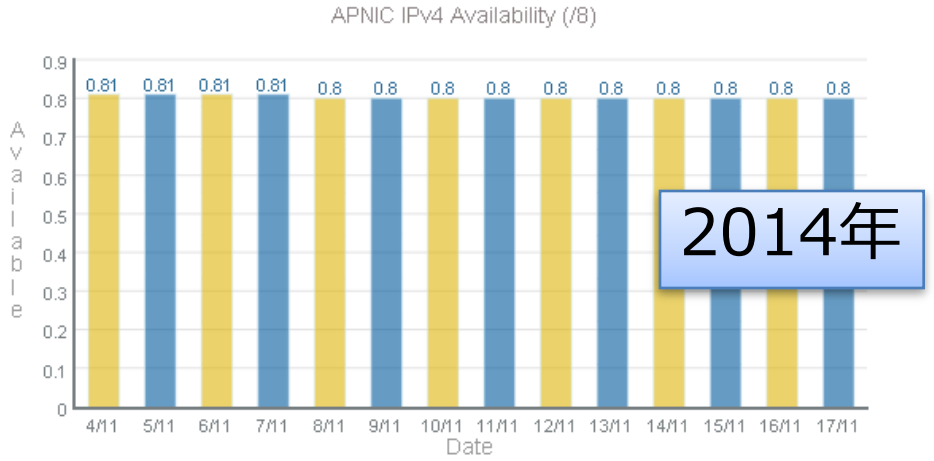

2011年




2013年




2012年




2014年

若干減少。本気でIPv4が必要な人は移転等で対応している状況

# APNIC公認？のブローカー

## Registered IPv4 brokers

Like Share 9 Tweet 7

| Organization | Economy | Contact | Phone |
|---|---|---|---|
| IPTrading.com | US | Michael Burns | +1 855-478-7233 |
| IPv4 Market Group LLC | US | Jeff Mehlenbacher | +1 855-880-5906 |
| The Kalorama Group | US | Louis Sterchi | +1 202-425-2118 |
| Hilco Streambank | US | Jack Hazan | +1 212-610-5663 |
| V4ESCROW, LLC | US | Elvis Daniel Velea | +1 702-475-5914 |
| v4Now | AU | Skeeve Stevens | +61-2-8014-7398 |
| IPv4 Xchange, LLC | US | Zack Myers | +1 646-863-8229 |
| Levine, Blaszak, Block & Boothby, LLP | US | Marc Lindsey | +1 202-857-2564 |

2013年に追加

2014年に追加

http://www.apnic.net/services/become-a-member/manage-your-membership/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。移転したい人は直接Contact

## IPv4 Transfers Listing Service

Like Share 3 Tweet 3

APNIC provides a listing service to help a source account of IPv4 addresses to make contact via APNIC to other accounts that requires more IPv4 address space but can not fulfill their IPv4 needs under the current IPv4 policy.

The table below contains the accounts that have had their IPv4 needs evaluated and and approved by APNIC using a process called "pre-approval". These accounts have given APNIC permission to make their needs for IPv4 public.

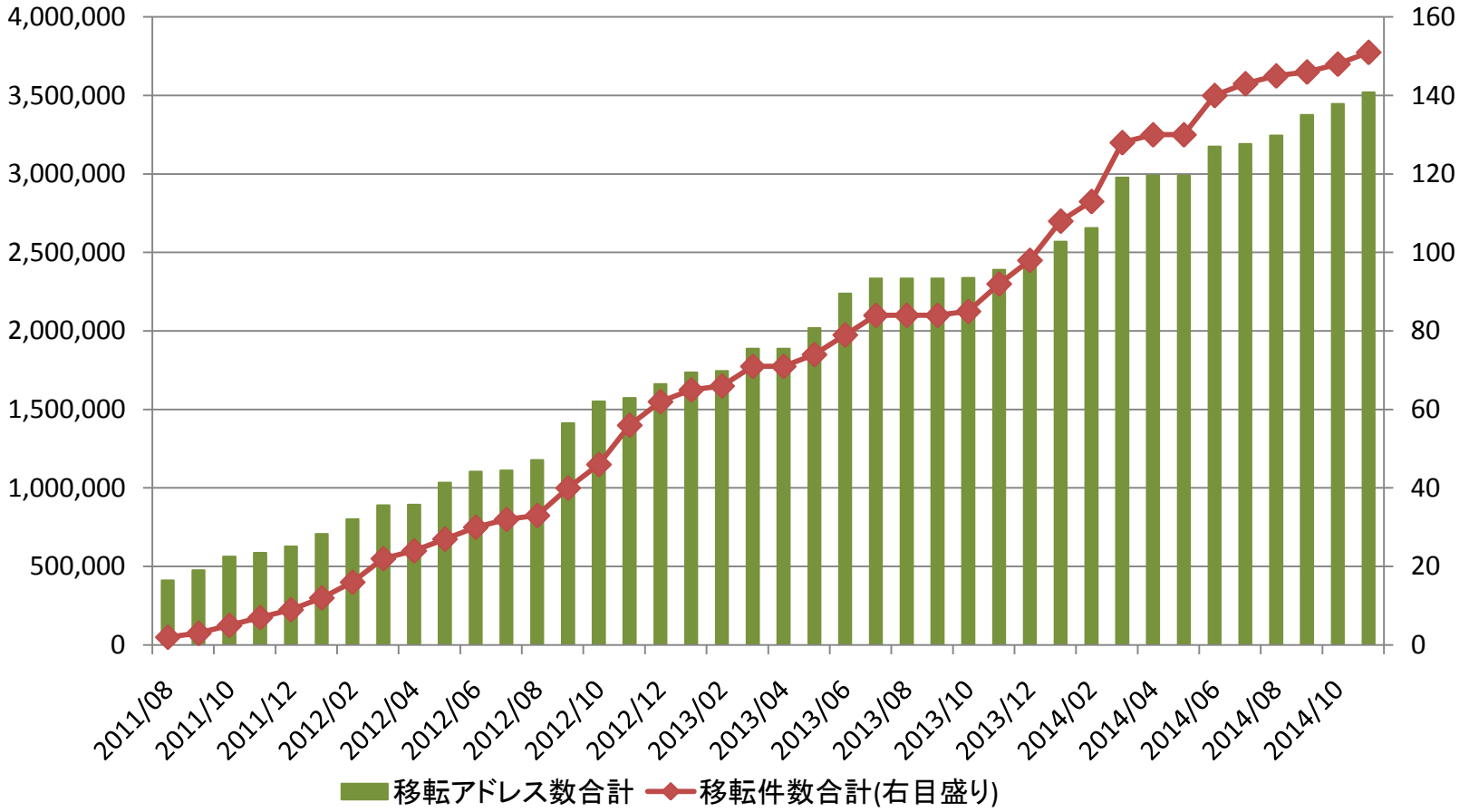
If you would like to transfer IPv4 addresses to any of the following accounts, you may make contact by clicking on the "Contact" link.

| Pre-approval ID | Pre-approved Size | Economy | Expire Date | Contact |
|---|---|---|---|---|
| 25 | /20 | HK | 26 Feb 2015 | Contact |
| 27 | /16 | MY | 12 Mar 2015 | Contact |
| 28 | /19 | BD | 25 Mar 2015 | Contact |
| 32 | /18 | AP | 24 Apr 2015 | Contact |
| 33 | /18 | SG | 29 Apr 2015 | Contact |
| 35 | /20 | IN | 20 Jun 2015 | Contact |
| 36 | /15 + /17 | MY | 1 Jun 2015 | Contact |
| 37 | /19 | BD | 31 Jul 2015 | Contact |
| 38 | /22 | AU | 29 Jul 2015 | Contact |

# 日本のIPv4アドレス移転状況

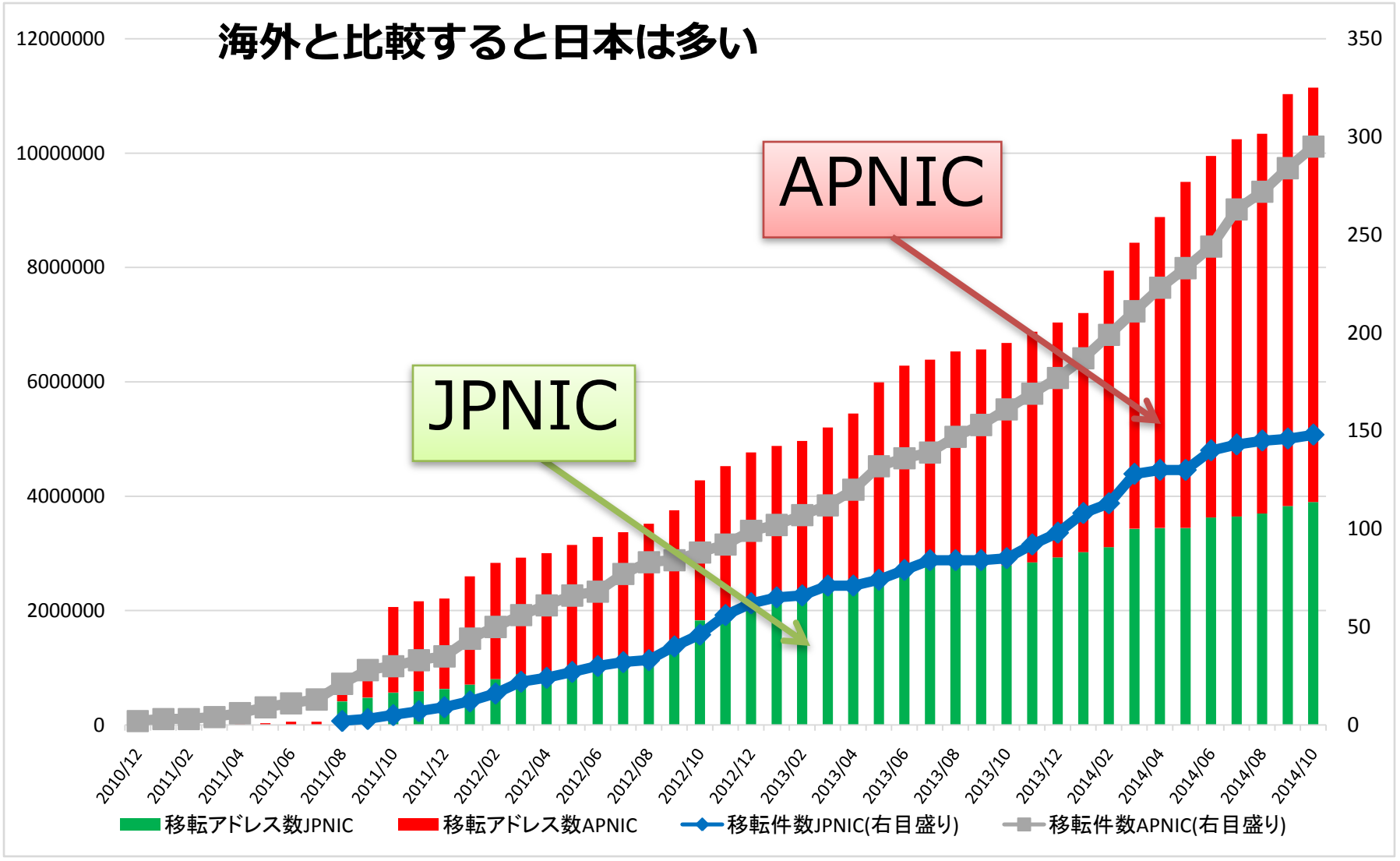
- 2014年11月17日現在150件（2011年８月より）
- ついに国際移転が4件(ARIN:2, APNIC:2)
- 移転の理由
  - 純粋にIPv4アドレスが既存の枠組みでは不足
  - 事業者間での整理
    - グループ企業間でやり取り
    - 上位ISPからの割り当てブロックをそのまま下位事業者へ移譲
- 移転履歴
  - https://www.nic.ad.jp/ja/ip/ipv4transfer-log.html
- 今後日本でもlisting serviceをJPNICで検討

# 日本のIPv4移転状況




出展：JPNICの川端さんより

# APNIC地域と日本の移転状況比較





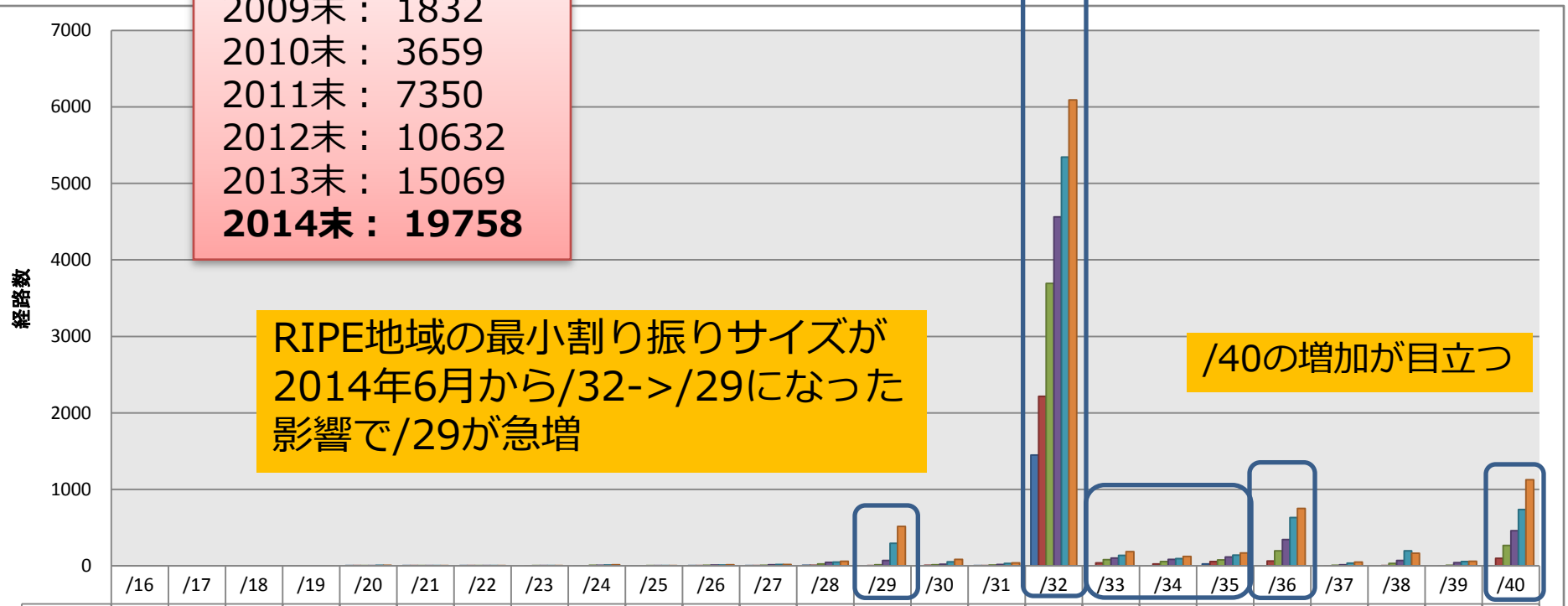

出展：JPNICの川端さんより

# 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**

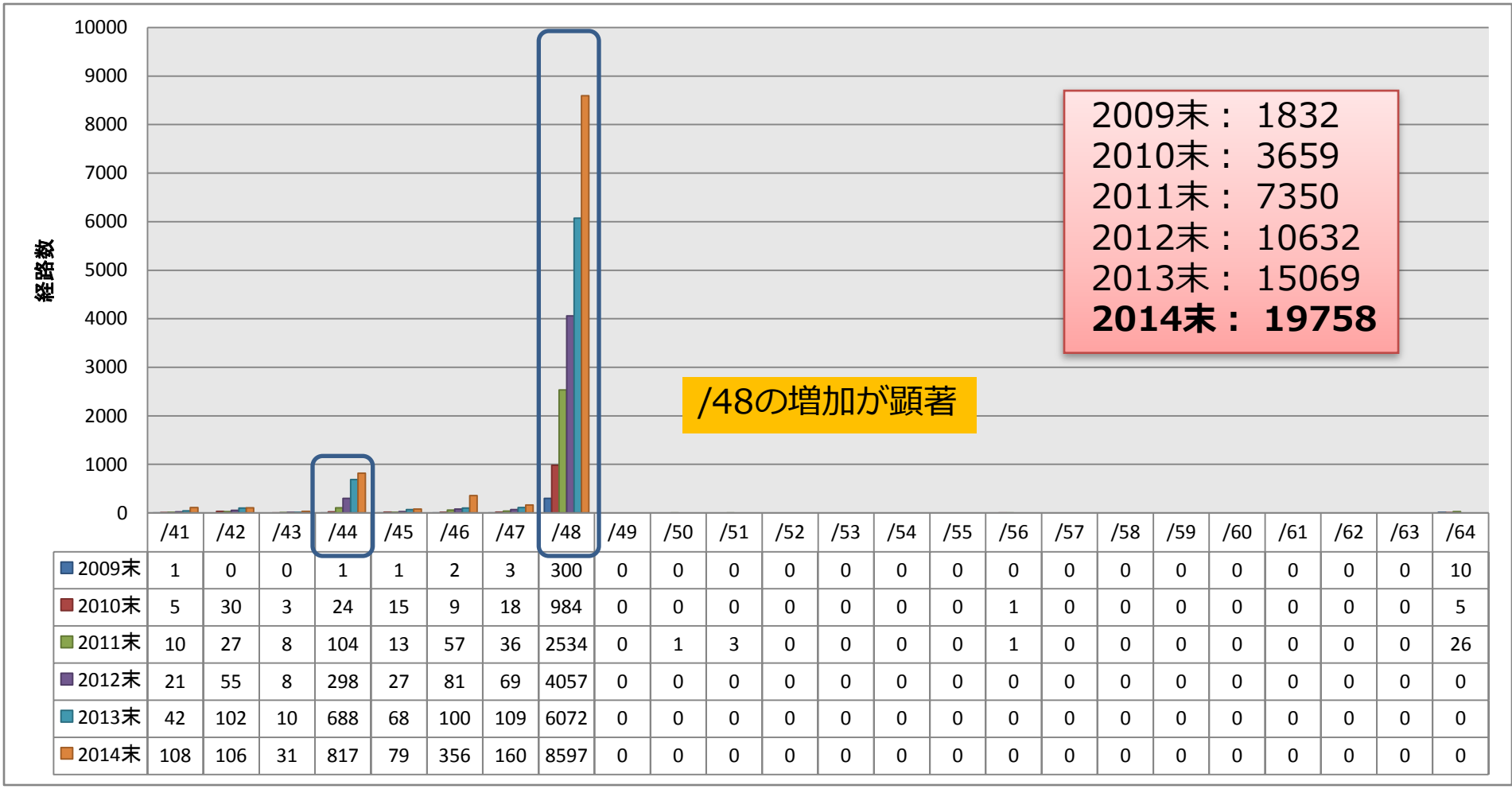
RIPE地域の最小割り振りサイズが2014年6月から/32->/29になった影響で/29が急増

/40の増加が目立つ



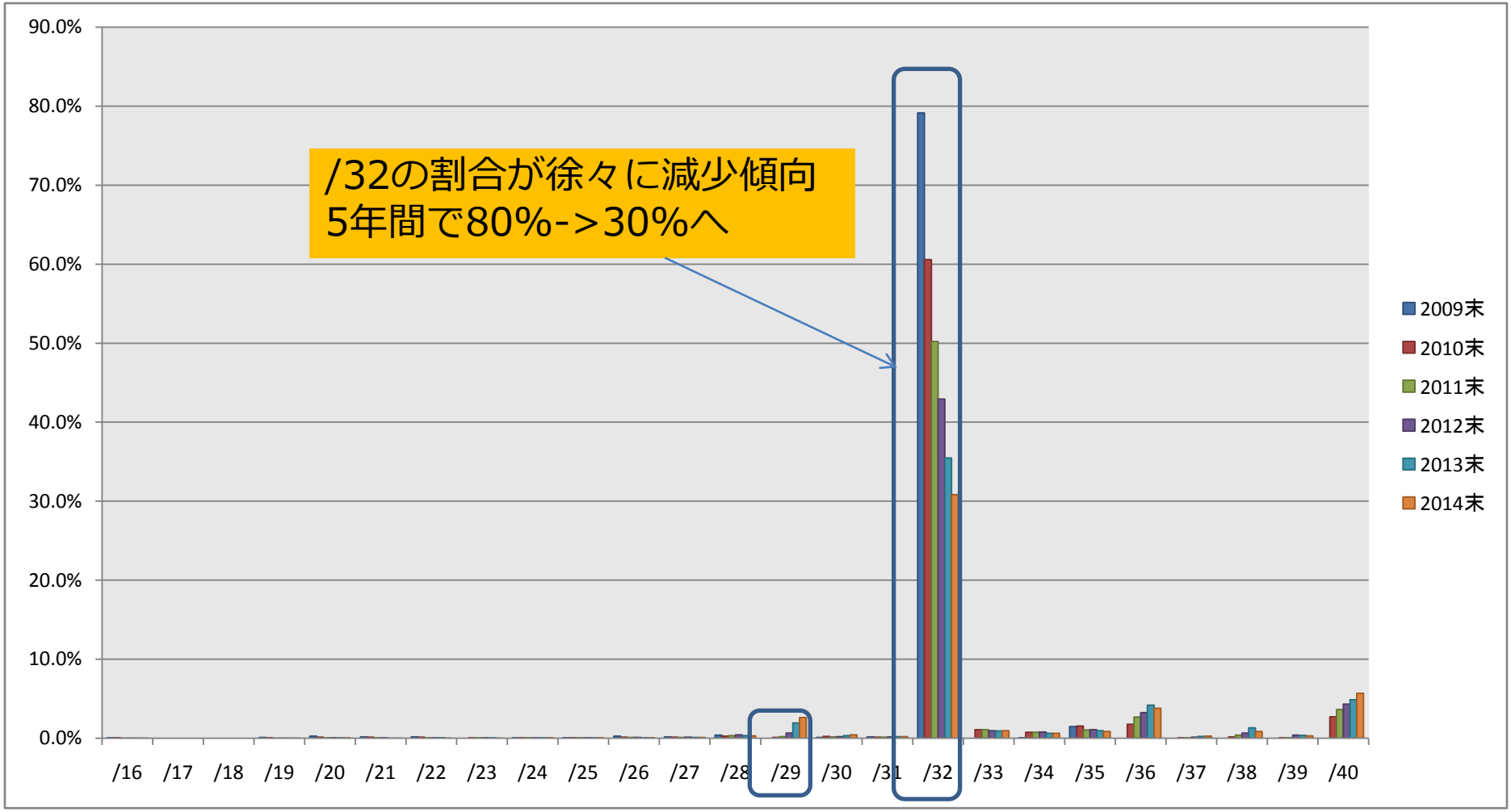

| | /16 | /17 | /18 | /19 | /20 | /21 | /22 | /23 | /24 | /25 | /26 | /27 | /28 | /29 | /30 | /31 | /32 | /33 | /34 | /35 | /36 | /37 | /38 | /39 | /40 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2009末 | 1 | 0 | 0 | 2 | 5 | 3 | 3 | 0 | 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 |

# IPv6経路数の推移

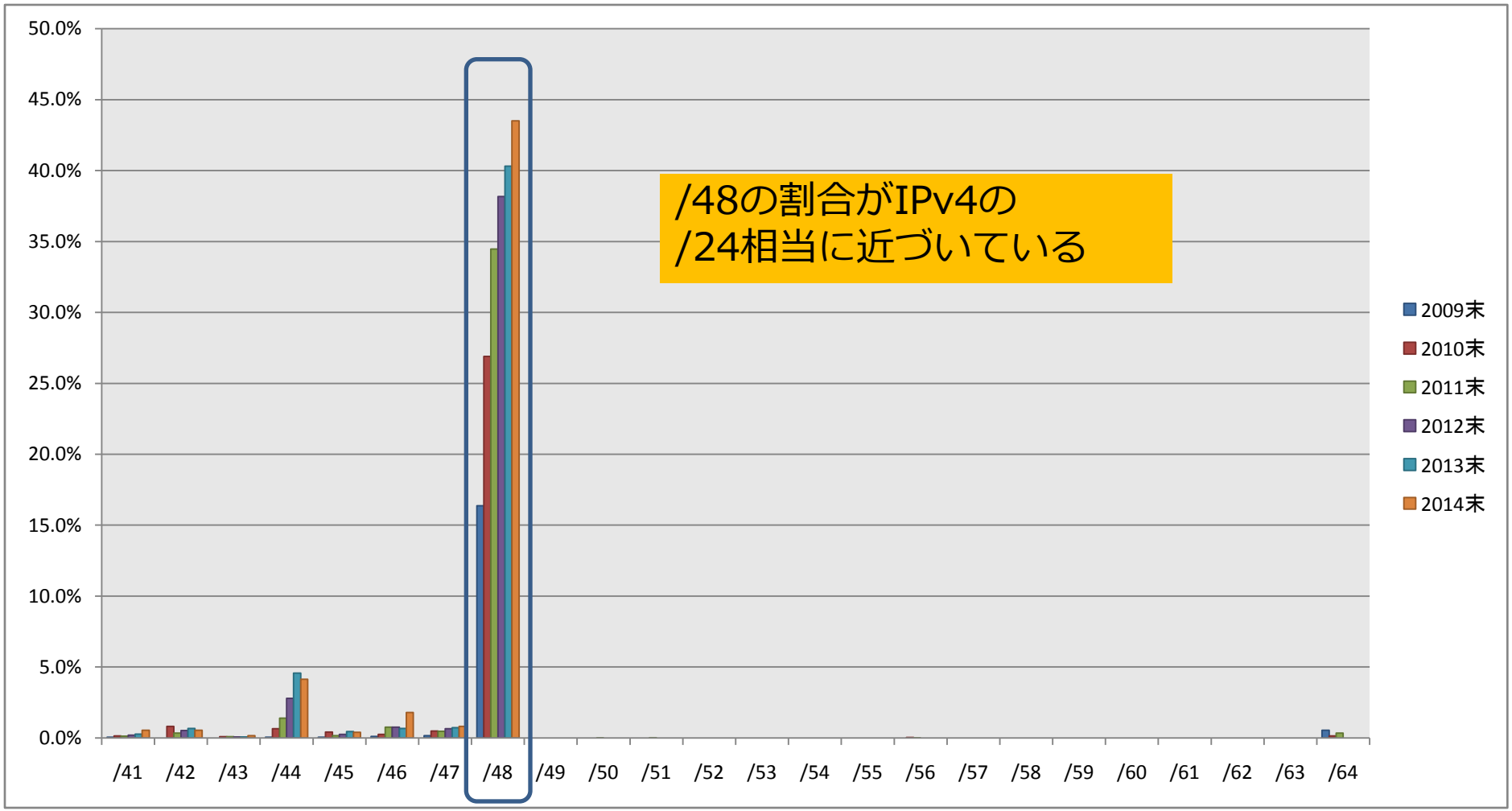



| | /41 | /42 | /43 | /44 | /45 | /46 | /47 | /48 | /49 | /50 | /51 | /52 | /53 | /54 | /55 | /56 | /57 | /58 | /59 | /60 | /61 | /62 | /63 | /64 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2009末 | 1 | 0 | 0 | 1 | 1 | 2 | 3 | 300 | 0 | 0 | 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 |

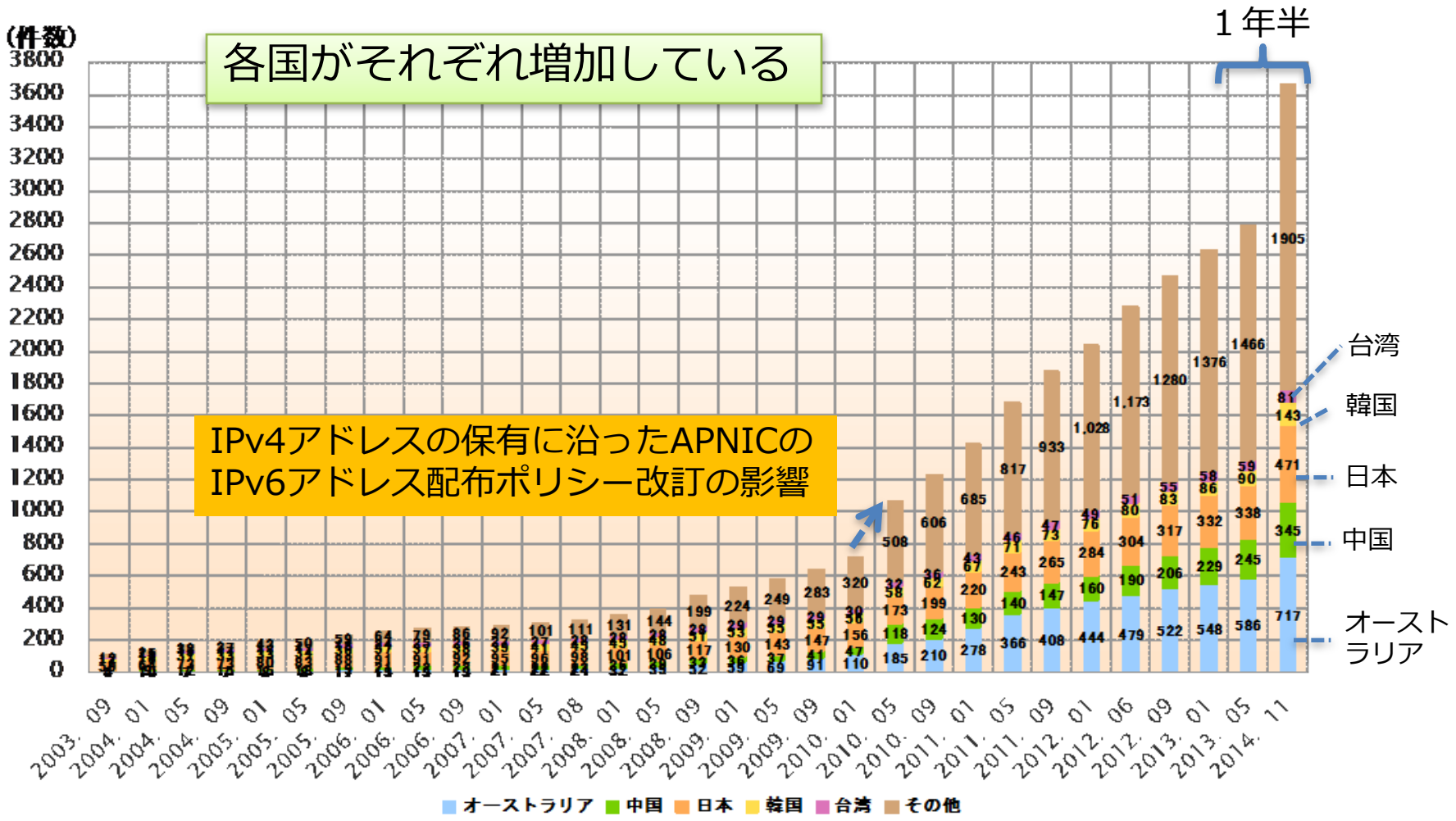
# IPv6経路数の推移（割合）



# IPv6経路数の推移（割合）

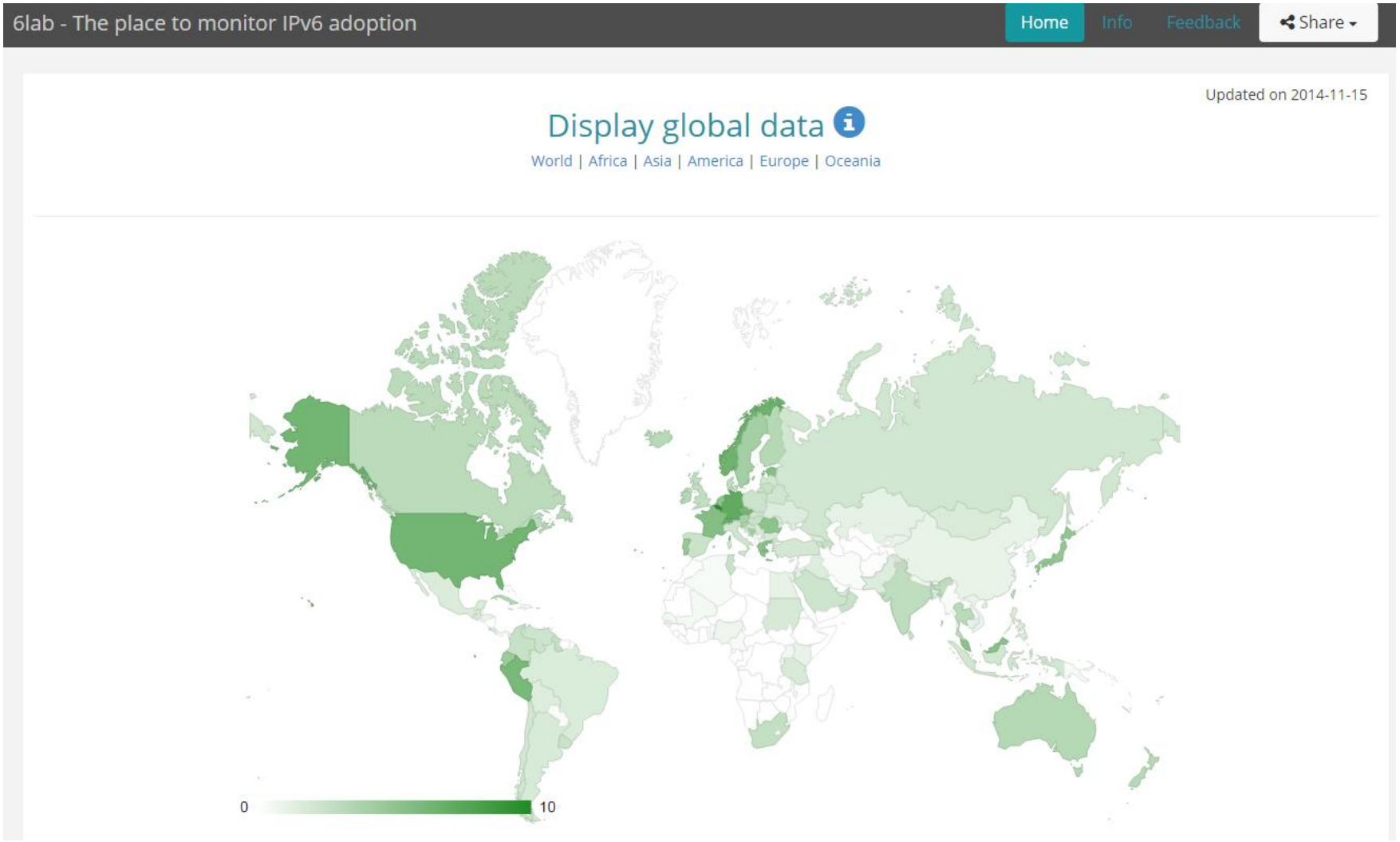


# AP地域の国別IPv6アドレス配分状況




出典：http://www.nic.ad.jp/ja/stat/ip/asia-pacific.html + JPNICの川端さん

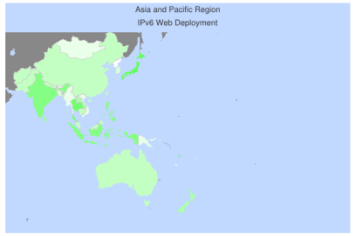
# http://6lab.cisco.com/stats/



# 主要な日本のサイトのIPv6対応状況

## 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<br>2a00:1450:4009:808::1017<br>2011-06-08 | aspmx.l.google.com<br>2a00:1450:400c:c00::1b<br>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<br>2001:502:4612::1<br>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<br>2403:400:300:1::5<br>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<br>2407:3000:6c::53<br>2/6 2010-12-11 |

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

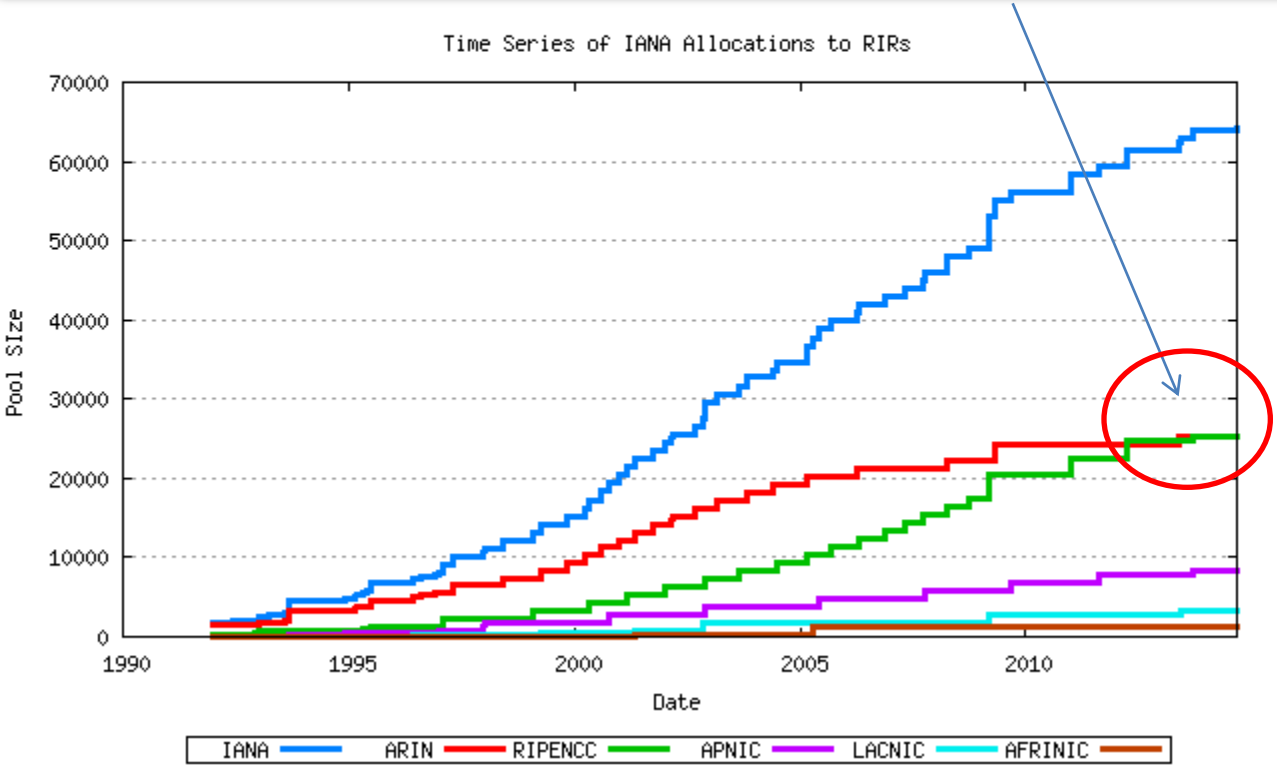
# AS番号 (2byte/4byte)

- 2byte AS
  - 現在残り約300AS
  - 2014年に枯渇すると予測されていたが、4byteASの払い出しや2byteASの移転により予測より枯渇が伸びている
    AS番号の移転： APNICで2014年4月~, JPNICで7月~開始

- 4byte AS
  - RIPE、APNIC、LACNIC地域が継続的に増加
    - 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

# AS Allocation

2014年にRIPEがARINを超えた（RIR poolで200AS程度）




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

# 2014年 DNS関連トピック

- 大規模化する攻撃　ホームルーターのDNS機能が攻撃の標的に
  - 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
  - 従来からのDNSリフレクター攻撃に加え、DNS水責めと呼ばれる攻撃が多く発生
- ドメイン名ハイジャックが日本国内でも発生
  - サイトに加え、閲覧者も攻撃のその標的に（例: java-se.comへ誘導）
  - 攻撃の隠蔽を図っており、より悪質な攻撃と言える（NSの一部のみを書き換える、数日で書き換えたNSを元に戻すなど）
- BIND以外の選択肢も充実
  - non-BIND solutionの最右翼：NSD/Unbound
  - レジストリが開発した「軽くて速い」権威DNSサーバー　Knot DNS, Yadifa
- そんな中、BIND 10が開発終了しBundyに改名
- DNSSECは徐々に増加、設定ミス等で引けないzoneも増大
- IANA機能の移行（来年9月？）
  - ルートゾーン管理も米国政府の管理下から独立
- 複数のルートサーバ（B,C）でIPアドレス変更やIPv6追加等
- gTLD新設と名前衝突問題、かの有名なドメインも？
- 数年ぶりに平穏な7月が遂に到来？

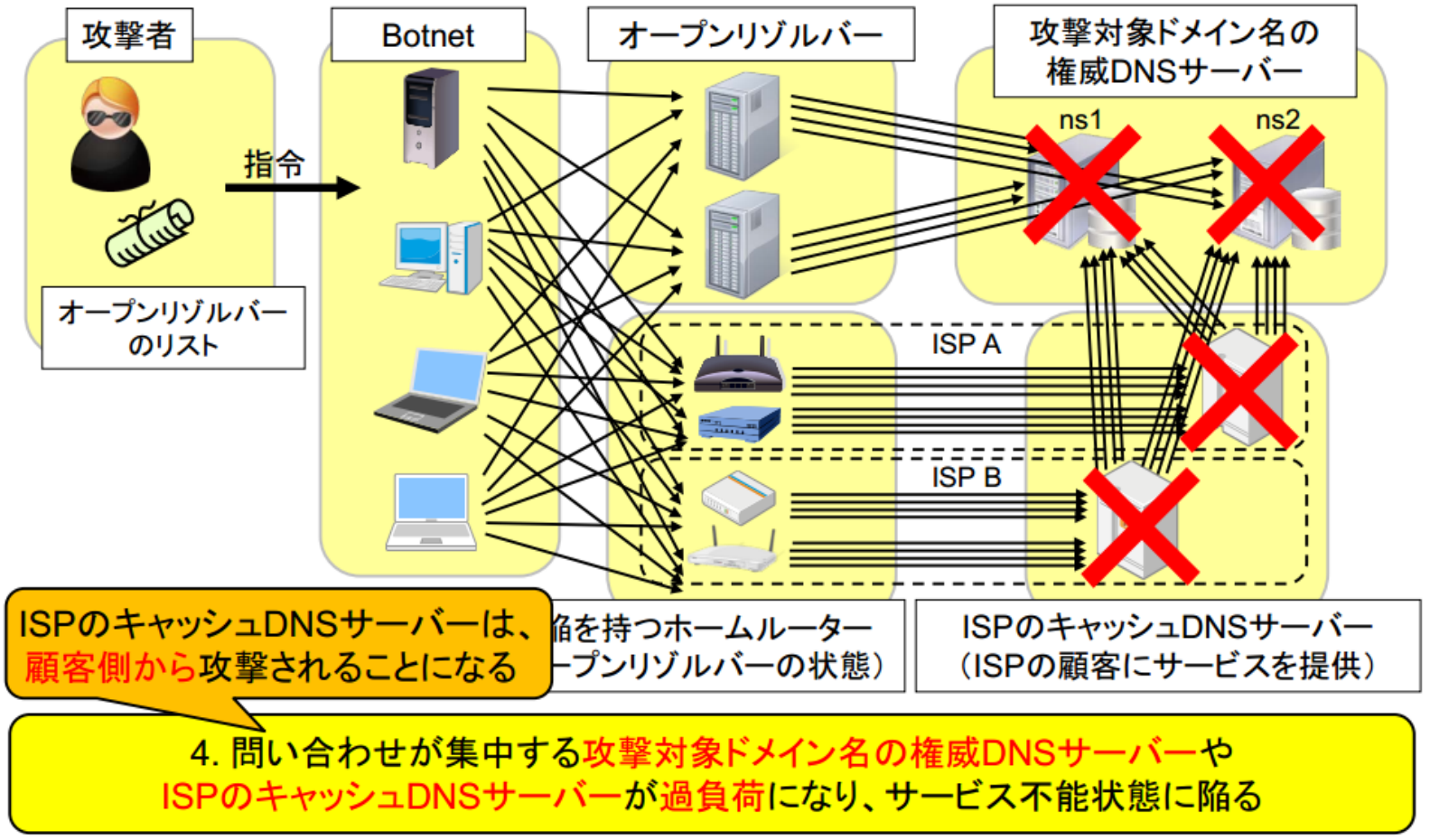
# オープンDNSフォワーダー問題

- ホームルーターが「オープンDNSフォワーダー」となり、ISPのキャッシュDNSを経由して不要なqueryが大量におくりつけられたり、権威DNSサーバへの大量のqueryが発生する「DNS水責め」と呼ばれる攻撃が多数発生した

- 従来からのDNSリフレクター攻撃と異なり、DNS問い合わせ自体を攻撃に直接使用する新しい手法

- 一時的に8.8.8.8に書き換えて、8.8.8.8の通信異常時に通信できなくなって、下のISPキャッシュDNSへ戻したというケースも報告されている

# 攻撃のシナリオ(4/4)







出展：JPRS森下さん　http://2014.seccon.jp/dns/dns_water_torture.pdf

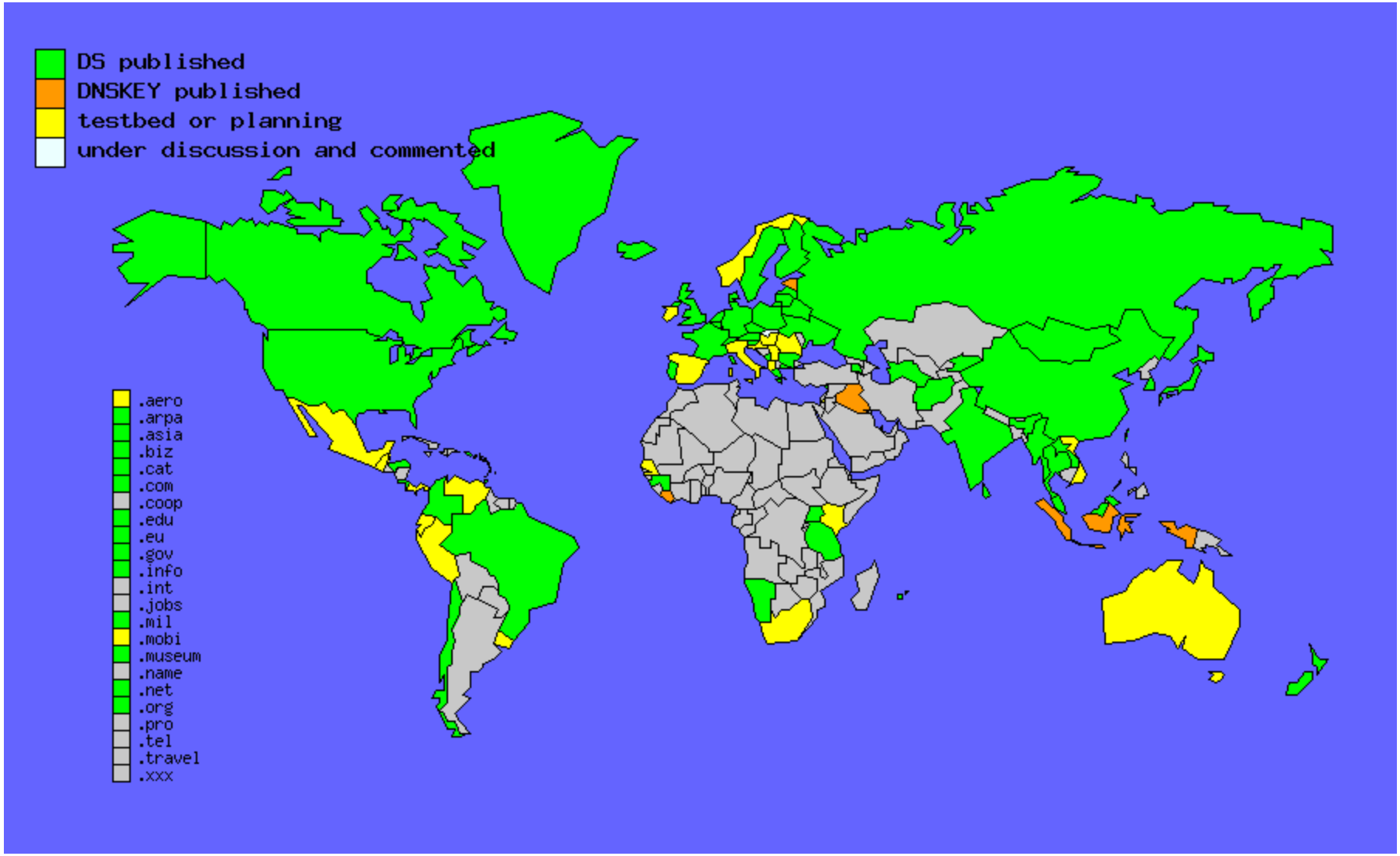
# ドメイン名ハイジャック問題

- 9月～10月にかけ、国内の複数の.comドメイン名を標的としたドメイン名ハイジャックが発生（以下対象サイトの例）
  - 日経新聞（nikkei.com）
  - はてな（st-hatena.com）
  - オークファン（aucfan.com）
- 攻撃がそのサイトだけではなく、そのサイトの利用者も対象
  --> java-se.comへ誘導
- 攻撃の隠蔽を図っており、より悪質な攻撃と言える（NSの一部のみを書き換える、数日で書き換えたNSを元に戻すなど）
- JPでは被害は発生していないが攻撃のしくみは同様であり、JPCERT/CC、JPRSが緊急の注意喚起を発表

# blogspot.jp

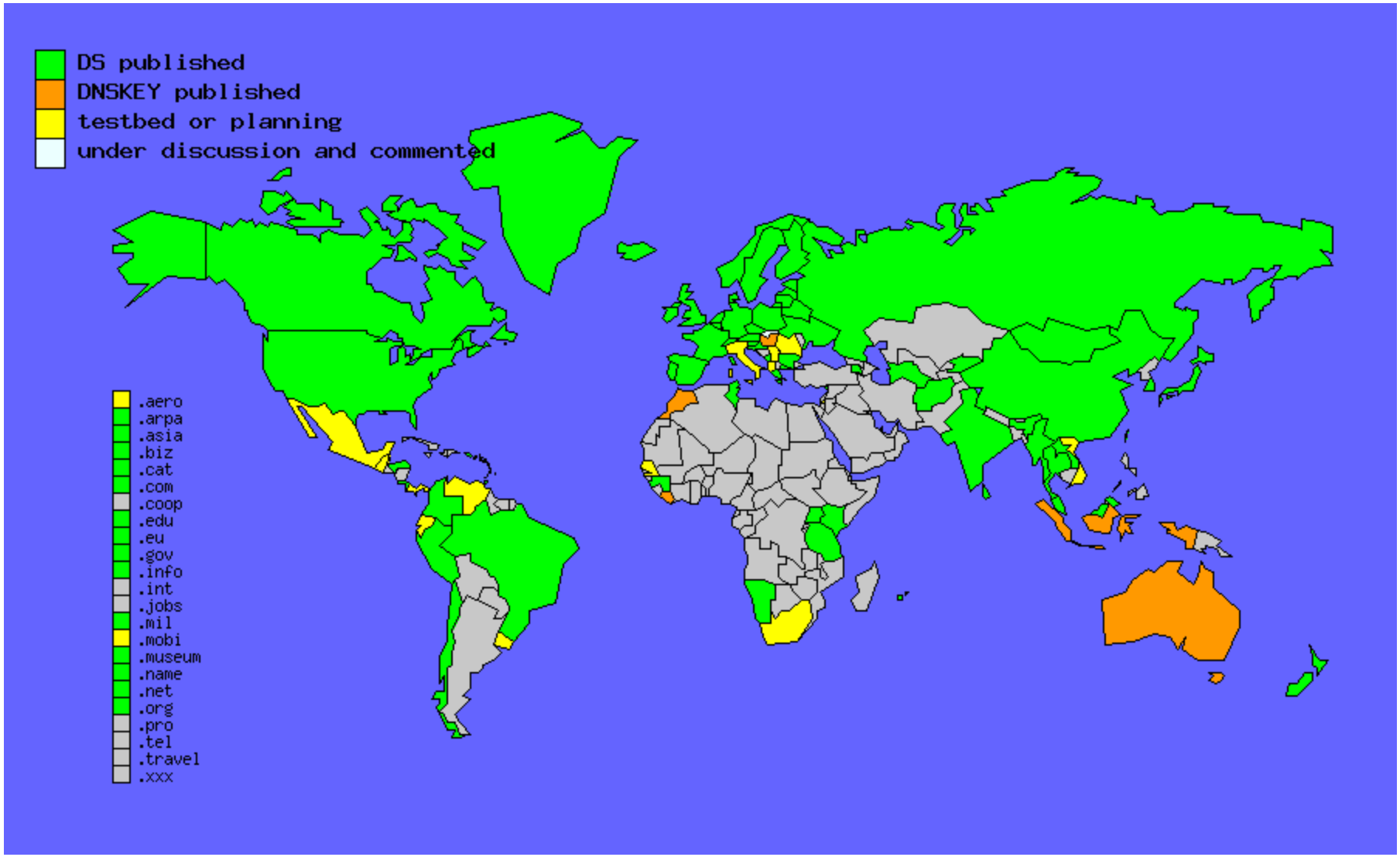
- NSが書き換えられた
- 経緯は不明
- 指定事業者／Googleいずれからも説明なし
- 現在は復旧

# TLDのDNSSEC普及状況(2013)




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

# TLDのDNSSEC普及状況(2014)




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

# DNSSECのvalidation失敗事案が相変わらず

## dcma.mil is failing DNSSEC validation

**Posted by Comcast on January 14, 2014 in DNSSEC News**

dcma.mil is attempting to send a payload that exceeds their path MTU (between 1130 and 540 bytes). DNS resolvers may not be able to properly receive the DNSKEY RRset with its covering RRSIGs.

Tags: DNSSEC

## gov Failing DNSSEC Validation

**Posted by Comcast on August 14, 2013 in DNSSEC News**

The domain .gov is currently failing DNSSEC validation This is because the chain of trust within the gov domain is broken. 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/gsa.gov/UguNUw/dnssec/

Tags: DNSSEC

## GoDaddy Domain Resolution Issues on June 2, 2013

**Posted by Comcast on June 05, 2013 in DNS News**

Customers in our northern California and Utah markets reported sporadic DNS failures when looking up domain names hosted by GoDaddy. Working with GoDaddy we learned that queries from these parts of our network routed to a GoDaddy Anycast node that was experiencing technical issues that caused our queries to timeout, while queries from other parts of our network were answered normally. GoDaddy made some Anycast changes and DNS resolution for our customers returned to normal.

Tags: DNS News

## flyinggiants.com Failing DNSSEC Validation

**Posted by Comcast on May 29, 2013 in DNSSEC News**

The domain flyinggiants.com is currently failing DNSSEC validation. This is because RRSIG records in the domain 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/flyinggiants.com/UaYVFQ/dnssec/.

Tags: DNSSEC

http://dns.comcast.net/

# t●m●cha.moe

どうやら過去利用していた形跡があったため（何らかのqueryが出ていた模様）
SLD(Second Level Domain)ブロックリストに登録され、自分が取得したい
.moe ドメインが取得できなかった、という話題

***2004年05月19日(水)*** *[曇り/雨]*

**＊ [Comp] BIND8/BIND9**

bsd.gyojya のサーバは BIND8 を ports で入れていた。
後に、IPv6 絡みで、BIND9 にすることにし、 ports で BIND9にしていた。

で、そんなところに罠があり、BIND8 と BIND9 が入っている。^
これが不幸を招いたらしく、BIND9 にしたとき、rc.conf を書き換え忘れていたらしい…。
つーわけで、 FreeBSD-SA-04:04.tcpを適用し、再起動したとき、BIND8 が起動してまずーでした(T_T

view を使わず、BIND8/9 互換のあるconf 書いていて、エラーが出なかったらしい。

つーことで、これを期に、named.conf の書き直し(整理とも言う)、
moeTLD ＊1 のゾーンも書き、tomocha.moe 等でもアクセス可能になりました(^^
ついでに、monyoさまの だめだめ日記が http://damedame.moe/ でアクセスが可能になりました(ぇ？

# 6年連続　祭りの魔の7月は終了

- 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**」）

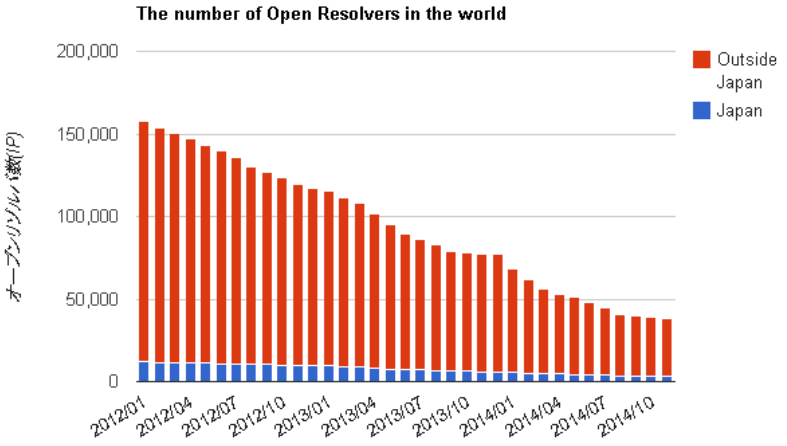
- （緊急）BIND 9.10.xの脆弱性（DNSサービスの停止）について
  （2014年6月12日公開）
  - キャッシュ／権威DNSサーバーの双方が対象、バージョンアップを強く推奨

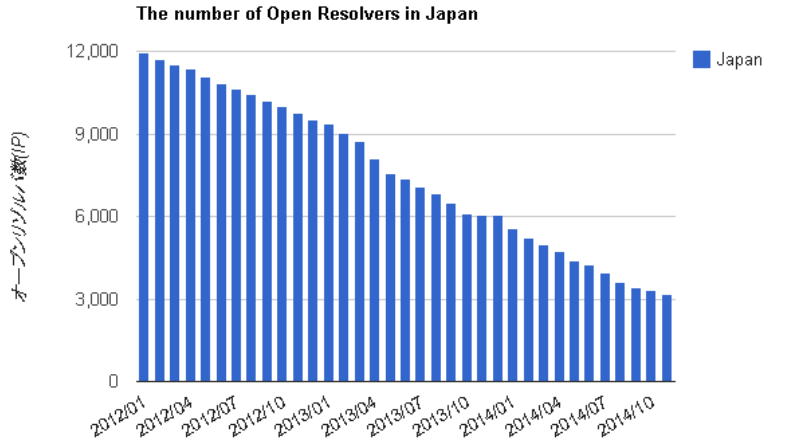
  株式会社日本レジストリサービス（JPRS）初版作成 2014/06/12（Thu）

# 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
- 着実に減少してきている


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



# 内容

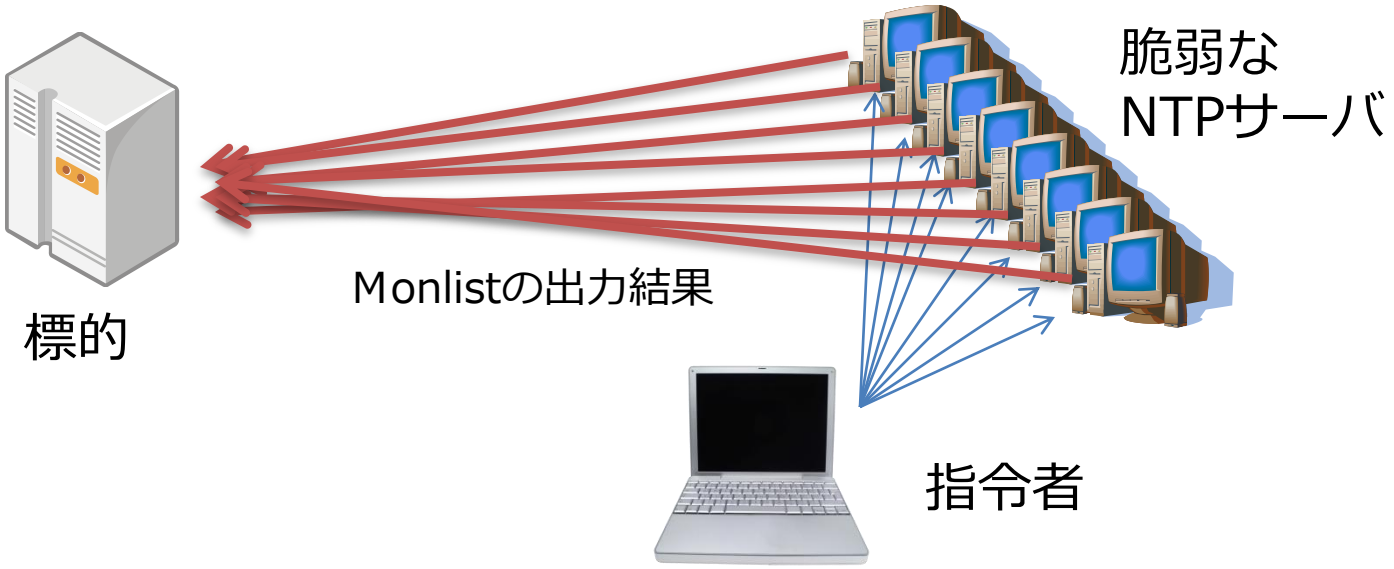
- トラフィック動向
- ルーティング動向
- DNS動向
- セキュリティ動向
- 日本や世界のIX動向
- まとめ

# 2014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）
- NTPのmonlist攻撃
- フィッシング攻撃
  - 相変わらず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
- 経路消失、のっとり事件
  - 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
- openSSL Hearbleed, bash etc…
- Web改ざん月平均400件　softwareのバージョンが古い脆弱性
- 官民連携のマルウェア対策支援プロジェクト「ACTIVE」

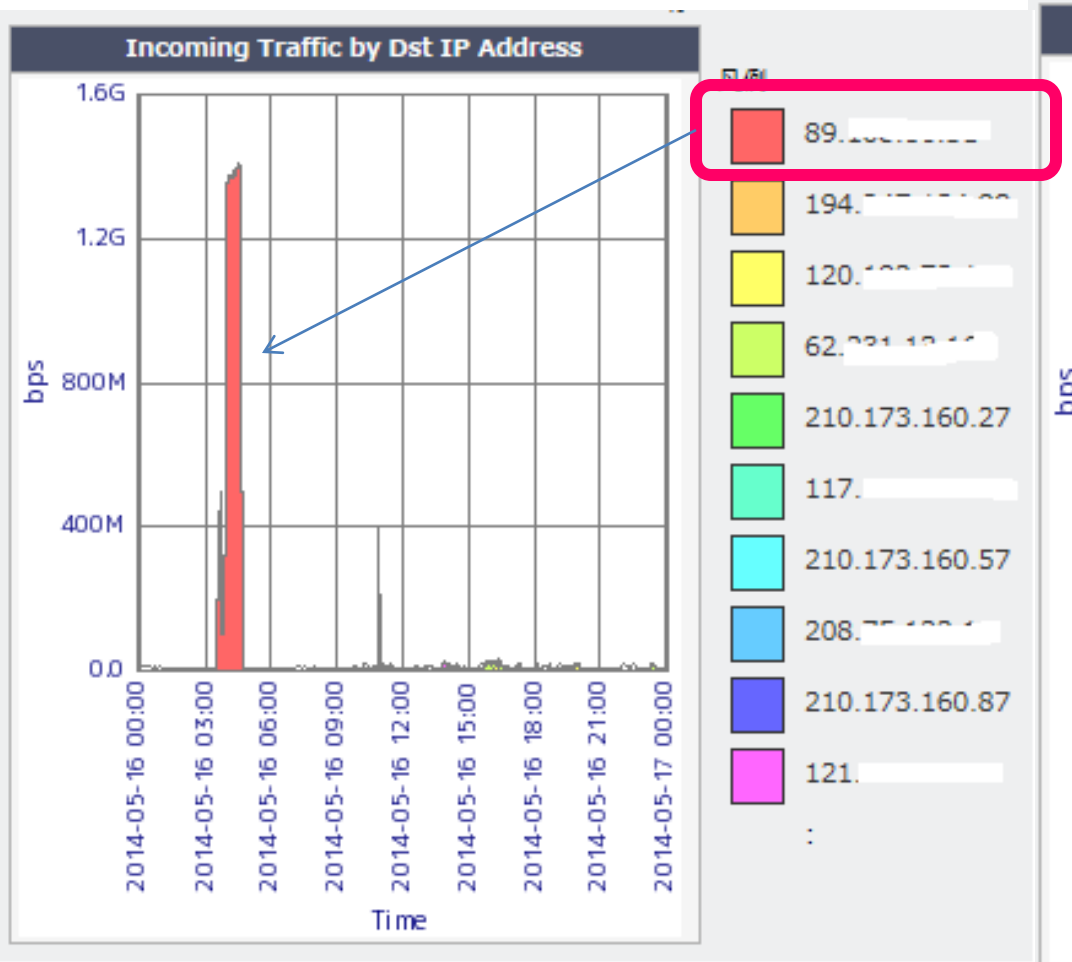
# NTPのmonlist攻撃

- NTPのmonlist攻撃がはやってます
  - Monlistという、NTP clientの接続情報などを取得するコマンド（600行の出力が最大で返る）
- 攻撃手法は非常に昔ながらの手法です
- NTPサーバのアドレスを送信元IPにしてスプーフし、踏み台を利用して攻撃対象に大量のデータを送りつける

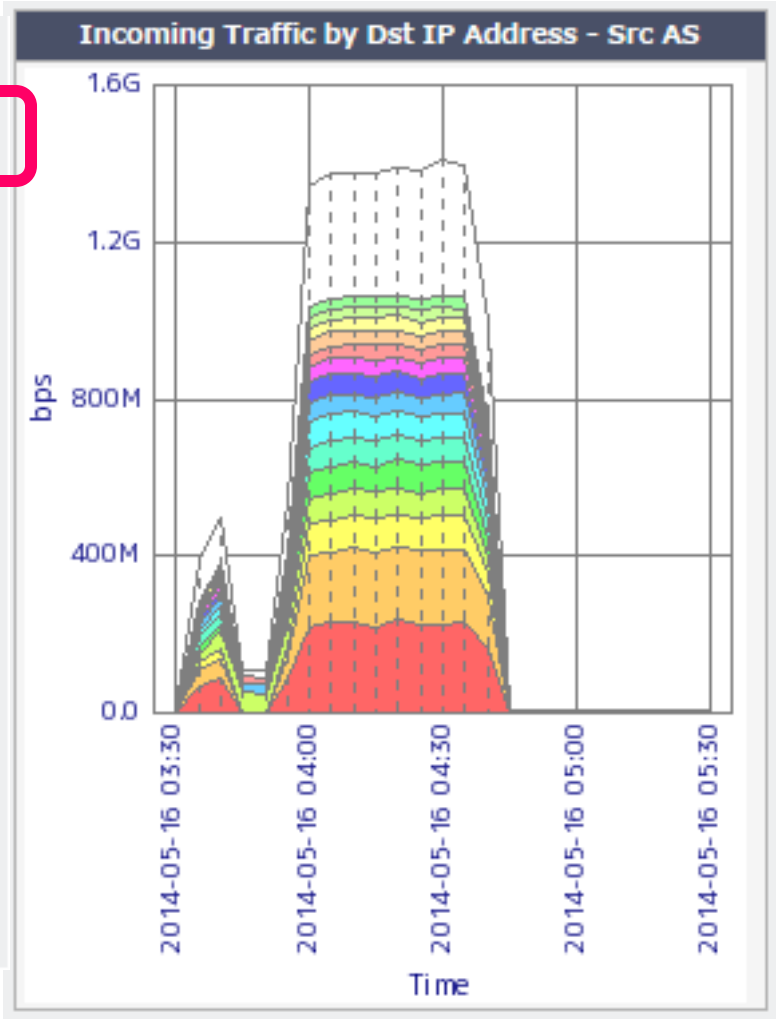


# UDP123 (ntp)

**攻撃を受けているDstIP**




**送信元AS（まばらに分布）**

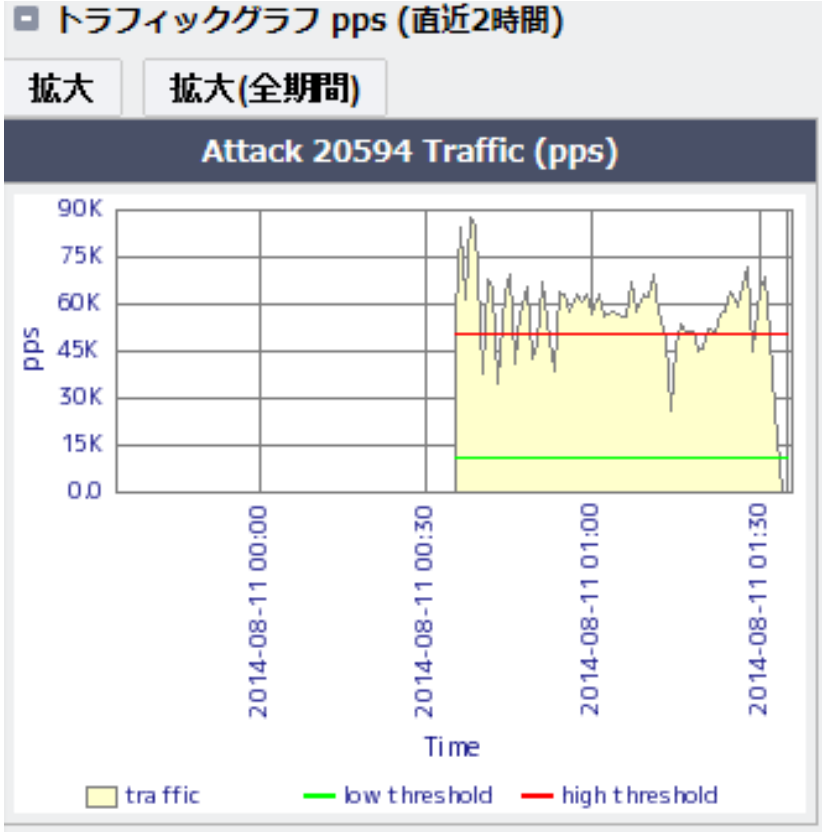


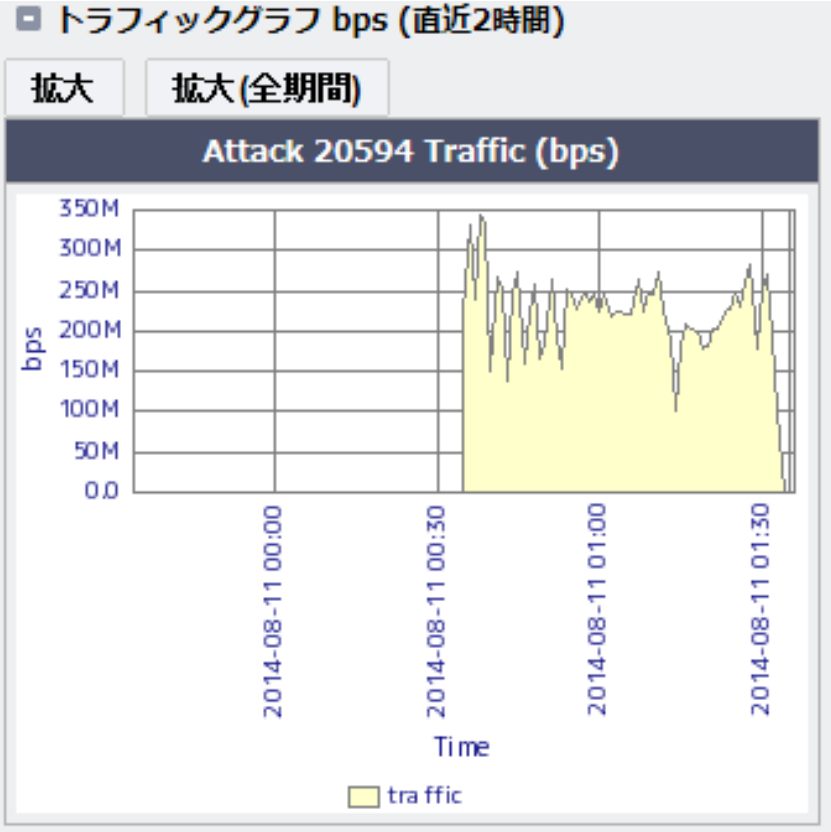
# 攻撃を受けているDstIPリスト（数百Kppsなどはざらにある）

| 重要度 | bps/pps | タイプ | IP Address | 継続時間 | 開始時刻 |
|---|---|---|---|---|---|
| HIGH | 126.02K pps | NTP | 非公開 | 00:09:00 | 2014-08-15 09:59:00+9.0 |
| HIGH | 155.51K pps | NTP | | 04:30:00 | 2014-08-14 17:54:00+9.0 |
| HIGH | 62.53K pps | NTP | | 00:06:00 | 2014-08-14 07:52:00+9.0 |
| HIGH | 115.78K pps | NTP | | 00:58:00 | 2014-08-14 02:49:00+9.0 |
| HIGH | 103.22K pps | NTP | | 00:06:00 | 2014-08-11 02:17:00+9.0 |
| HIGH | 87.79K pps | NTP | | 00:59:00 | 2014-08-11 00:35:00+9.0 |
| HIGH | 70.86K pps | NTP | | 00:10:00 | 2014-08-10 23:25:00+9.0 |
| HIGH | 77.55K pps | NTP | | 00:04:00 | 2014-08-10 21:46:00+9.0 |
| HIGH | 109.50K pps | NTP | | 00:34:00 | 2014-08-10 12:39:00+9.0 |
| HIGH | 87.24K pps | NTP | | 00:04:00 | 2014-08-10 02:30:00+9.0 |
| HIGH | 84.51K pps | NTP | | 00:07:00 | 2014-08-09 23:45:00+9.0 |
| HIGH | 223.78K pps | NTP | | 01:07:00 | 2014-08-09 18:15:00+9.0 |
| HIGH | 79.73K pps | NTP | | 01:32:00 | 2014-08-09 14:09:00+9.0 |
| HIGH | 183.50K pps | NTP | | 01:02:00 | 2014-08-09 11:30:00+9.0 |
| HIGH | 77.14K pps | NTP | | 00:07:00 | 2014-08-09 10:47:00+9.0 |
| HIGH | 102.67K pps | NTP | | 01:00:00 | 2014-08-09 04:55:00+9.0 |
| HIGH | 157.56K pps | NTP | | 00:31:00 | 2014-08-08 19:48:00+9.0 |
| HIGH | 254.50K pps | NTP | | 00:31:00 | 2014-08-08 19:47:00+9.0 |
| HIGH | 114.82K pps | NTP | | 00:06:00 | 2014-08-08 19:32:00+9.0 |
| HIGH | 107.86K pps | NTP | | 00:32:00 | 2014-08-08 18:00:00+9.0 |
| HIGH | 126.98K pps | NTP | | 00:30:00 | 2014-08-08 18:00:00+9.0 |
| HIGH | 314.71K pps | NTP | | 00:30:00 | 2014-08-07 21:23:00+9.0 |
| HIGH | 185.55K pps | NTP | | 00:54:00 | 2014-08-07 16:10:00+9.0 |
| HIGH | 86.97K pps | NTP | | 00:06:00 | 2014-08-07 00:40:00+9.0 |
| HIGH | 121.11K pps | NTP | | 00:32:00 | 2014-08-06 18:45:00+9.0 |
| HIGH | 122.47K pps | NTP | | 00:34:00 | 2014-08-06 18:43:00+9.0 |
| HIGH | 66.22K pps | NTP | | 02:48:00 | 2014-08-06 05:41:00+9.0 |
| HIGH | 153.60K pps | NTP | | 00:44:00 | 2014-08-05 02:39:00+9.0 |
| HIGH | 227.19K pps | NTP | | 00:10:00 | 2014-08-04 08:12:00+9.0 |
| HIGH | 161.38K pps | NTP | | 01:36:00 | 2014-08-04 06:33:00+9.0 |
| HIGH | 155.10K pps | NTP | | 01:37:00 | 2014-08-04 00:27:00+9.0 |
| HIGH | 311.43K pps | NTP | | 00:07:00 | 2014-08-04 00:20:00+9.0 |
| HIGH | 79.33K pps | NTP | | 00:14:00 | 2014-08-01 16:09:00+9.0 |
| HIGH | 79.46K pps | NTP | | 00:11:00 | 2014-08-01 15:56:00+9.0 |
| HIGH | 229.38K pps | NTP | | 00:11:00 | 2014-07-29 03:29:00+9.0 |
| HIGH | 132.71K pps | NTP | | 00:08:00 | 2014-07-28 23:48:00+9.0 |
| HIGH | 96.80K pps | NTP | | 00:08:00 | 2014-07-28 21:49:00+9.0 |

# とある攻撃の例

**0:35頃～1:40頃に攻撃の形跡あり**



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 |
| | | | | 0M | 21.57K | 84.56M | 0.00 | 0.00 |
| | | | | 6M | 9.56K | 37.46M | 0.00 | 0.00 |
| | | | | 2M | 9.28K | 36.39M | 0.00 | 0.00 |
| | | | | 0M | 9.15K | 35.86M | 0.00 | 0.00 |
| | | | | 7M | 7.65K | 29.97M | 0.00 | 0.00 |
| | | | | 2M | 7.78K | 30.51M | 0.00 | 0.00 |
| | | | | 3M | 7.92K | 31.04M | 0.00 | 0.00 |
| | | | | 3M | 6.42K | 25.15M | 0.00 | 0.00 |
| | | | | 6M | 6.83K | 26.76M | 0.00 | 0.00 |
| | | | | 7M | 5.73K | 22.48M | 0.00 | 0.00 |
| | | | | 1M | 6.96K | 27.30M | 0.00 | 0.00 |
| | | | | 0M | 3.96K | 15.52M | 0.00 | 0.00 |
| | | | | 4K | 3.69K | 14.45M | 0.00 | 0.00 |
| | | | | 2K | 4.51K | 17.66M | 0.00 | 0.00 |
| | | | | 5K | 3.69K | 14.45M | 0.00 | 0.00 |
| | | | | 9K | 9.15K | 35.63M | 0.00 | 0.00 |
| | | | | 7K | 2.18K | 8.52M | 0.00 | 0.00 |
| | | | | 3K | 409.60 | 176.95K | 0.00 | 0.00 |
| | | | | 1K | 136.53 | 63.35K | 0.00 | 0.00 |
| | | | | 2K | 955.73 | 3.75M | 0.00 | 0.00 |
| | | | | 1K | 682.67 | 2.68M | 0.00 | 0.00 |
| | | | | 4K | 546.13 | 2.14M | 0.00 | 0.00 |
| | | | | 3K | 409.60 | 1.59M | 0.00 | 0.00 |
| | | | | 3K | 273.07 | 1.06M | 0.00 | 0.00 |
| | | | | 0K | 409.60 | 1.61M | 0.00 | 0.00 |
| | | | | 6K | 273.07 | 1.07M | 0.00 | 0.00 |
| | | | | 4K | 273.07 | 1.06M | 0.00 | 0.00 |
| | | | | 7K | 273.07 | 126.70K | 0.00 | 0.00 |
| | | | | 9K | 273.07 | 1.07M | 0.00 | 0.00 |
| | | | | 4K | 136.53 | 530.84K | 0.00 | 0.00 |
| | | | | 4K | 136.53 | 535.21K | 0.00 | 0.00 |
| | | | | 4K | 136.53 | 535.21K | 0.00 | 0.00 |
| | | | | 4K | 136.53 | 535.21K | 0.00 | 0.00 |
| | | | | 5K | 136.53 | 530.84K | 0.00 | 0.00 |
| | | | | 5K | 136.53 | 530.84K | 0.00 | 0.00 |
| | | | | 2K | 136.53 | 535.21K | 0.00 | 0.00 |
| | | | | 2K | 136.53 | 535.21K | 0.00 | 0.00 |
| | | | | 5K | 136.53 | 530.84K | 0.00 | 0.00 |
| | | | | 5K | 136.53 | 530.84K | 0.00 | 0.00 |

非公開

## 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 |
| [redacted] | 97.42G | 199.15M | 55.32K | 216.49M | 87.79K | 343.19M | 0.00 | 0.00 |

## プロトコル

| プロトコル | 通信量 | | Avg | | Max | | Cur | |
|---|---|---|---|---|---|---|---|---|
| | bytes | packets | pps | bps | pps | bps | pps | bps |
| udp | 97.42G | 199.15M | 55.32K | 216.49M | 87.79K | 343.19M | 0.00 | 0.00 |

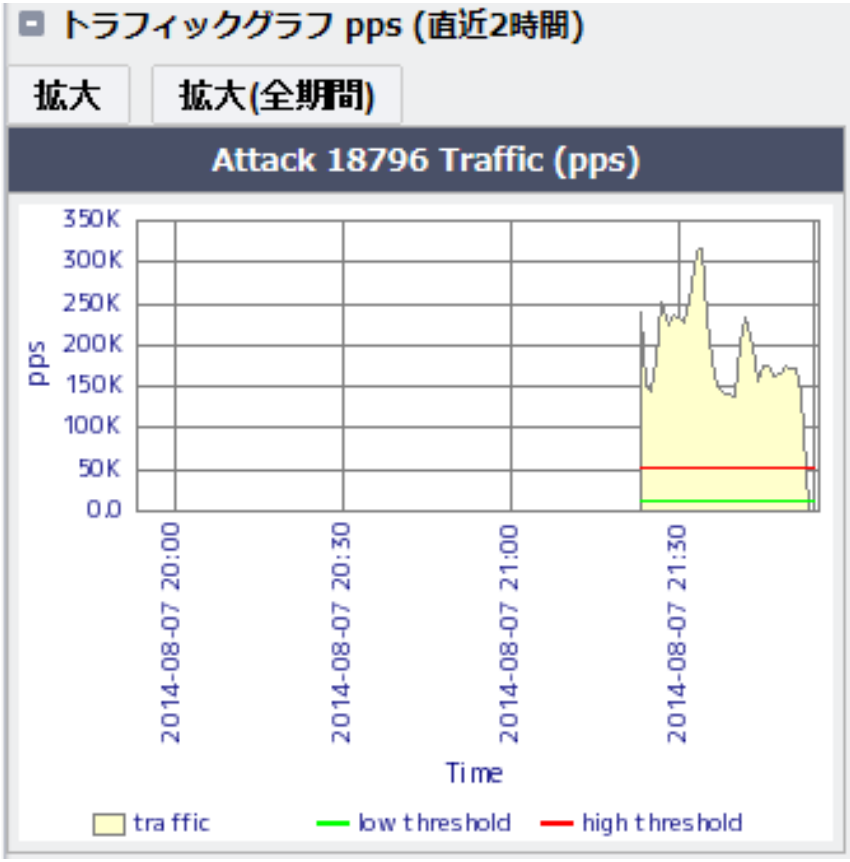
## TCPフラグ

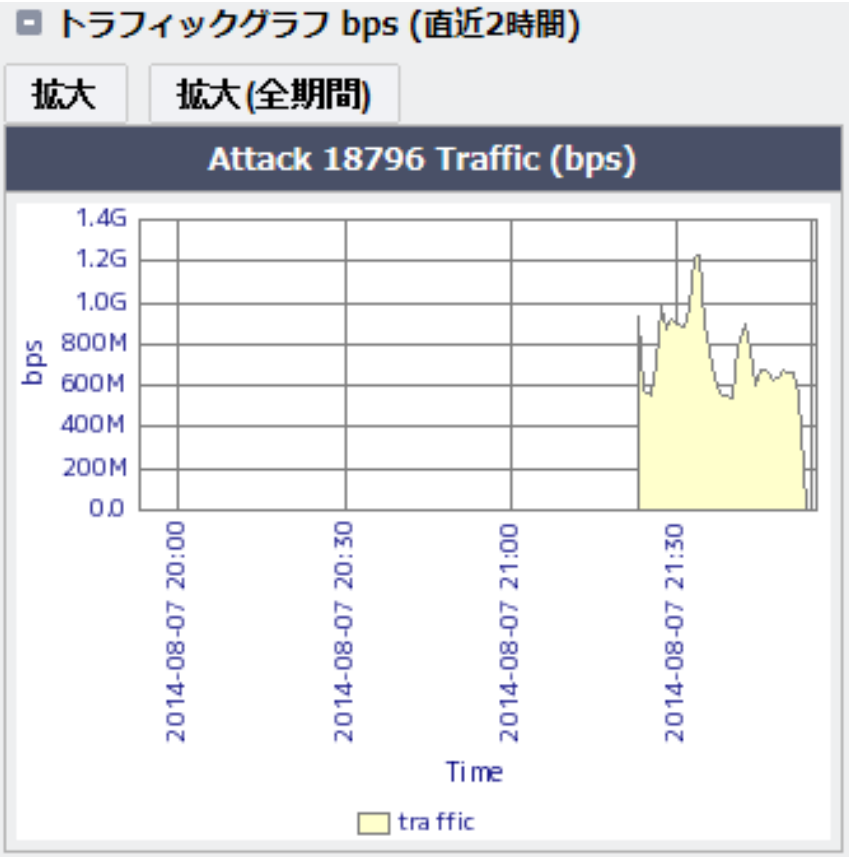
## 送信元ポート

| プロトコル | ポート番号 | 通信量 | | Avg | | Max | | Cur | |
|---|---|---|---|---|---|---|---|---|---|
| | | bytes | packets | pps | bps | pps | bps | pps | bps |
| udp | 123(ntp) | 97.42G | 199.15M | 55.32K | 216.49M | 87.79K | 343.19M | 0.00 | 0.00 |

## 宛先ポート

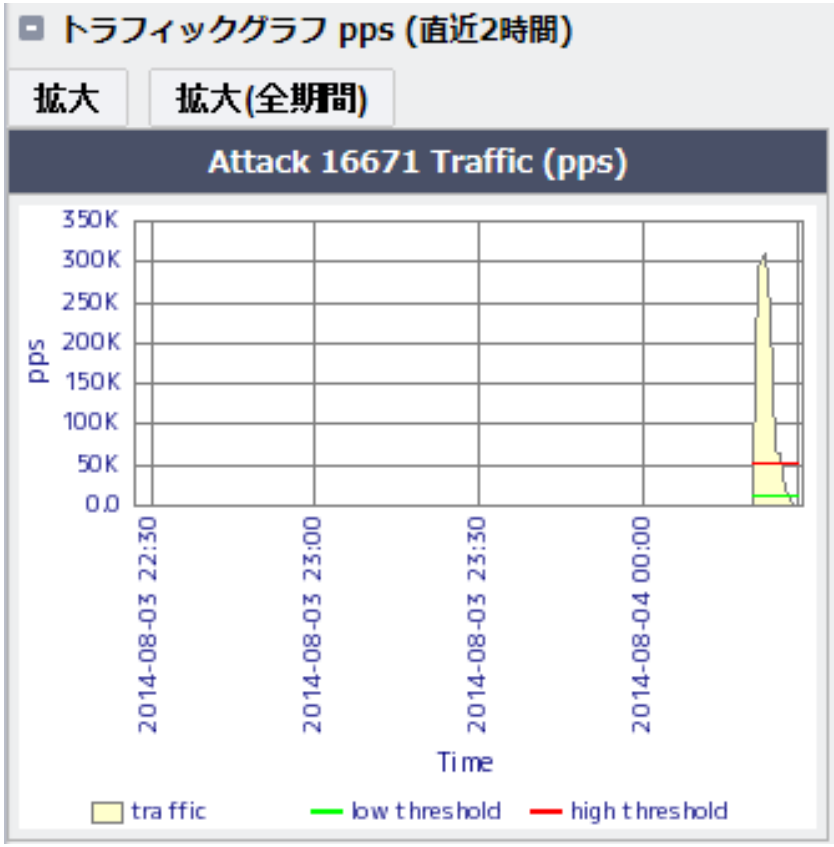
| プロトコル | ポート番号 | 通信量 | | Avg | | Max | | Cur | |
|---|---|---|---|---|---|---|---|---|---|
| | | bytes | packets | pps | bps | pps | bps | pps | bps |
| udp | 80(http) | 97.42G | 199.15M | 55.32K | 216.49M | 87.79K | 343.19M | 0.00 | 0.00 |

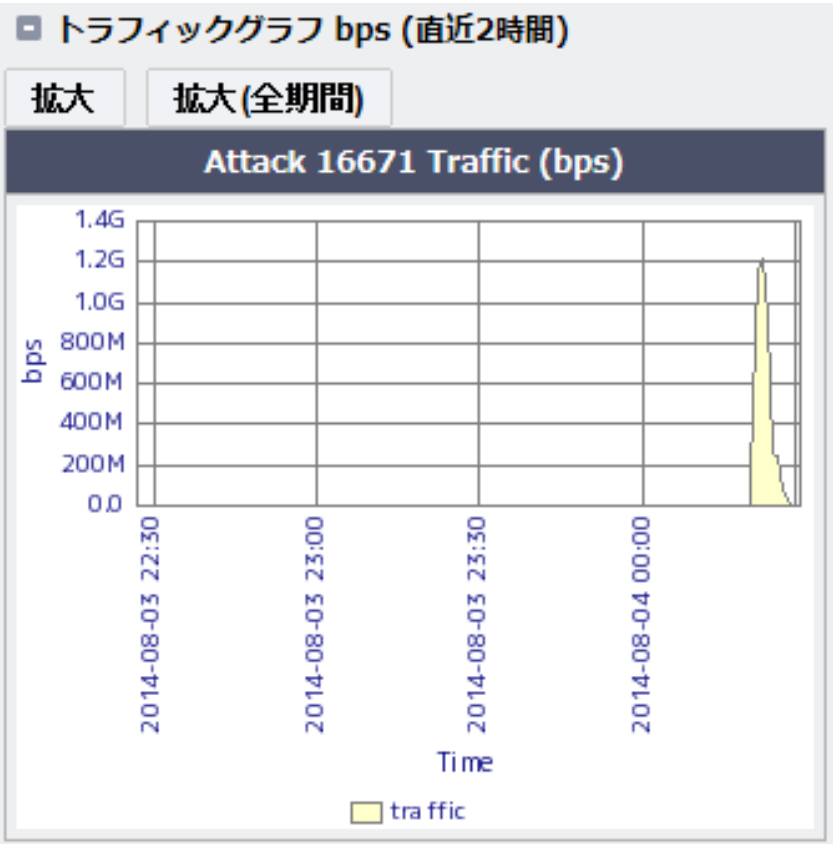


```
Tomoya-no-MacBook-Pro:~ yoshida$ ntpdc -c monlist [redacted]
remote address          port local address      count m ver rstr avgint  lstint
===============================================================================
s                      33980 0.0.0.0                1 7 2      0      0       0
c                         53 0.0.0.0            17194 7 2      0      0       0
2                       2038 0.0.0.0           197384 7 2      0     24       0
d                      27015 0.0.0.0            96276 7 2      0     21       1
2                       2038 0.0.0.0           105217 7 2      0    102      14
d                      27015 0.0.0.0            49349 7 2      0     25      17
d                      27015 0.0.0.0            62869 7 2      0     43      18
c                      27015 0.0.0.0            68176 7 2      0     25      20
d                      27015 0.0.0.0            96051 7 2      0     25      21
c                      27015 0.0.0.0            45840 7 2      0     38      39
d                      27015 0.0.0.0            44850 7 2      0     67      43
c                      27015 0.0.0.0            65985 7 2      0     32      48
s                      27015 0.0.0.0              302 7 2      0      0   53774
2                      45374 0.0.0.0             1125 7 2      0      0   53985
1                         80 0.0.0.0             4491 7 2      0      0   54823
1                       5135 0.0.0.0             2693 7 2      0      0   55347
g                         53 0.0.0.0              109 7 2      0      0   55389
8                       4444 0.0.0.0             2216 7 2      0      0   56206
n                      27031 0.0.0.0              317 7 2      0      0   56309
1                      18930 0.0.0.0              240 7 2      0      0   56537
2                         80 0.0.0.0             5218 7 2      0      0   57524
8                         80 0.0.0.0              973 7 2      0      1   57524
t                         80 0.0.0.0             6045 7 2      0      0   58580
m                         80 0.0.0.0             3698 7 2      0      0   58935
m                         80 0.0.0.0            11983 7 2      0      0   59578
1                         80 0.0.0.0             4340 7 2      0      0   59832
6                         80 0.0.0.0              624 7 2      0      0   61196
1                         80 0.0.0.0               67 7 2      0      0   61296
c                         53 0.0.0.0            47531 7 2      0      0   61344
l                         22 0.0.0.0              230 7 2      0      0   61779
1                         80 0.0.0.0             1109 7 2      0      0   62167
1                         80 0.0.0.0              722 7 2      0      0   62550
1                         80 0.0.0.0              244 7 2      0      0   62575
1                         80 0.0.0.0              142 7 2      0      0   63072
n                      13337 0.0.0.0              210 7 2      0      0   64200
1                         80 0.0.0.0           112077 7 2      0      0   64579
a                         80 0.0.0.0            36199 7 2      0      0   65046
u                      25565 0.0.0.0             8907 7 2      0      0   65064
p                      51569 0.0.0.0             6335 7 2      0      0   65230
b                       3306 0.0.0.0              330 7 2      0      0   65622
s                      27035 0.0.0.0             8411 7 2      0      0   65715
1                         80 0.0.0.0             3418 7 2      0      0   65761
                        3306 0.0.0.0             1350 7 2      0      0   65959
1                         80 0.0.0.0             3729 7 2      0      0   66233
c                         53 0.0.0.0            19862 7 2      0      0   66279
9                         53 0.0.0.0             4689 7 2      0      0   66427
v                         80 0.0.0.0            20498 7 2      0      0   66796
p                        179 0.0.0.0             5464 7 2      0      0   66982
                          80 0.0.0.0             1620 7 2      0      0   67284
1                      28050 0.0.0.0              328 7 2      0      0   67471
i                         53 0.0.0.0             4333 7 2      0      0   67941
8                         80 0.0.0.0              172 7 2      0      0   68465
1                         80 0.0.0.0             3114 7 2      0      0   68480
1                         53 0.0.0.0             9104 7 2      0      0   68487
i                         80 0.0.0.0             2275 7 2      0      0   68679
1                       6667 0.0.0.0             5473 7 2      0      0   69569
d                         80 0.0.0.0            24580 7 2      0      0   69661
1                      27005 0.0.0.0              486 7 2      0      0   70179
i                        720 0.0.0.0             1689 7 2      0      0   70447
7                         80 0.0.0.0             7390 7 2      0      0   71118
1                         80 0.0.0.0            31744 7 2      0      0   71329
a                         53 0.0.0.0            10972 7 2      0      0   71333
5                         80 0.0.0.0              513 7 2      0      0   71355
c                         80 0.0.0.0             6206 7 2      0      0   71647
m                         80 0.0.0.0             1701 7 2      0      0   72127
d                         53 0.0.0.0             3873 7 2      0      0   72486
```

非公開



# Monlist攻撃の対策

- NTPサーバ側
  - Monlistを無効化
    - #Disable monitor
- Client側（ISP側）
  - BCP38
    - 送信元アドレスがspoofされているパケットを排除

# Akamaiよりセキュリティレポート

Press Releases

2014年10月24日

アカマイ、PLXsertの2014年第3四半期
「インターネットの現状」セキュリティレポートを発表

- DDoS攻撃が急増：DDoS攻撃の規模と容量が4倍に増加
- 勢いに乗る犯罪業界、インターネット機器を悪用、使いやすいツールを拡散

※2014年10月23日に米国 Akamai Technologies, Inc. より発表されたプレスリリースの抄訳です。

オンラインコンテンツとビジネス・アプリケーションの配信、最適化、および保護を実現するクラウドサービスの代表的プロバイダーであるアカマイ・テクノロジーズ・インク（NASDAQ：AKAM、以下アカマイ）は本日、2014年第3四半期「インターネットの現状」セキュリティレポートを発表しました。アカマイのプロレクシック・セキュリティ・エンジニアリング＆リサーチチーム（PLXsert）は、分散型サービス妨害（DDoS）保護サービスおよび戦略の第一人者として定評があります。今四半期のレポートは、DDoS攻撃を含むグローバルな攻撃の脅威の状況に関する分析と洞察を提供しており、<http://www.stateoftheinternet.com/security-report>からダウンロードできます。

「今年はDDoS攻撃の規模と容量が急増しました」と、アカマイのセキュリティビジネス部門バイスプレジデントであるジョン・サマーズ（John Summers）は語っています。「第3四半期だけで、アカマイは17件の100Gbps（ギガビット/秒）以上の攻撃（最大のものは321Gbps）を緩和しました。興味深いことに、前年同期にはこの規模の攻撃は1件も観測されておらず、前四半期は6件だけでした。これらの大規模攻撃は、それぞれ複数のDDoSベクトルを使用しており、大きな帯域幅を消費するパケットを非常に高速で配信しています。」

2013年第3四半期との比較

- DDoS攻撃の総数は22パーセント増加
- 平均攻撃帯域幅は389パーセント増加
- 平均ピークパケット/秒は366パーセント増加
- アプリケーション層への攻撃は44パーセント増加
- インフラ層への攻撃は43パーセント増加
- 平均攻撃時間は5パーセント増加
- マルチベクトル攻撃は9パーセント増加

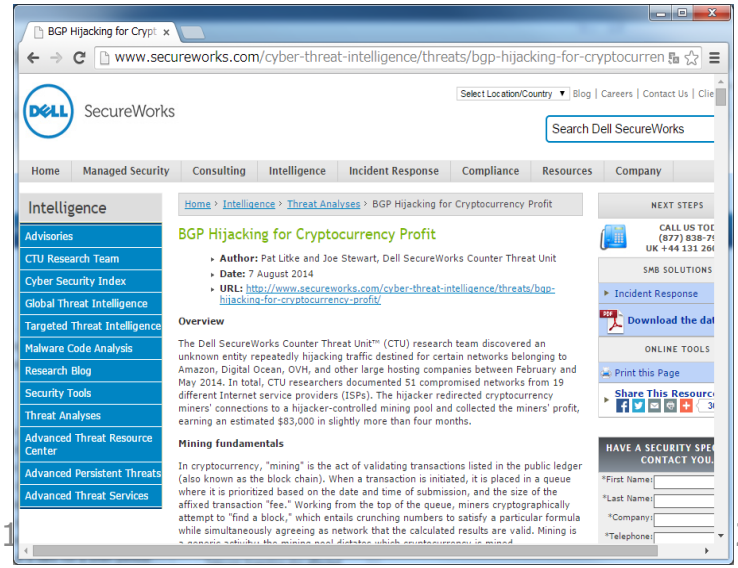
2014年第2四半期との比較

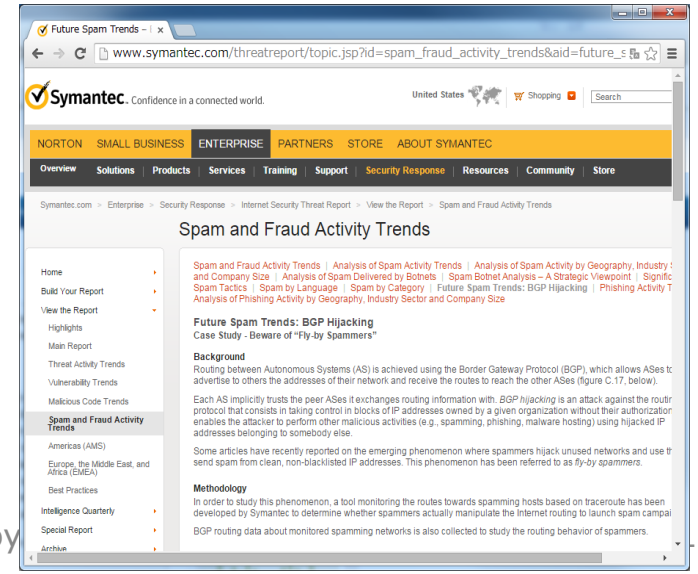
- DDoS攻撃の総数は2パーセント増加
- 平均攻撃帯域幅は80パーセント増加
- 平均ピークパケット/秒は10パーセント増加
- アプリケーション層への攻撃は2パーセント増加
- インフラ層への攻撃は2パーセント増加
- 平均攻撃時間は29パーセント増加
- マルチベクトル攻撃は11パーセント増加
- 広帯域幅（100Gbps以上）の攻撃は、6件から17件へ、183パーセント増加

http://www.akamai.co.jp/enja/html/about/press/releases/2014/press_jp.html?pr=102414

# 2014年の経路ハイジャック事情

- 以前の愉快犯的な状況ではない。金銭目的の意図的なものも多い
  - BGP経路ハイジャックでBitcoin(8万ドル)を稼ぐ
    http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/
    http://www.bgpmon.net/the-canadian-bitcoin-hijack/
  - BGP経路ハイジャックを使ったSPAM
    http://www.symantec.com/threatreport/topic.jsp?id=spam_fraud_activity_trends&aid=future_spam_trends
    https://www.usenix.org/conference/lisa-07/homeless-vikings-bgp-prefix-hijacking-and-spam-wars



# Bitcoinの事例

2014/08/07にDell Secure Worksから、
”BGP Hijacking for Cryptocurrency Profit"
という報告あり"(URLは前述)

カナダのあるASが、AmazonなどのASをOriginASに偽装してBitcoinマイナーとBitcoinプールの間の通信を4ヶ月に渡って盗みとられたようです。見積では約8万ドルが盗まれた模様。

**BGP Origin 詐称が利用された模様。。**

AS Originが詐称されているため、BGP Path validationを動作させないと検出できない

# SPAMの事例(1)

SANOG(South Asian Network Operators Group)のML:

"Prefix hijacking, how to prevent and fix currently"
https://lists.sanog.org/pipermail/sanog/2014-August/thread.html

RIPEリージョンのASにいくつかのPrefixが経路ハイジャックされ、SPAMに利用されていた模様。spamcopから大量の存在しないホストが記載されたアラームが来た模様。。

# SPAMの事例(2)

2014年2月、 弊社JPNAPののセグメント(/24)で“経路ハイジャックを使ったSPAM”を、ロ●アのASにやられました

**時系列(JST)**

2/11 23:47 経路奉行で経路ハイジャック発生検知
(218.100.45.0/24)

2/12 13:22 SPAM送信
(218.100.45.34, JPNAP未割当IP)

2/12 13:27 spamcopがSPAM検出

2/12 14:40 経路奉行で経路ハイジャック回復検知

2/12 PM spamcopからのメールに気づき対応
=> SPAMメールヘッダのMXレコードはすでに存在せず。

未利用IPを勝手に使う
組織的な犯罪との見方が強い

**spamcopからのアラートメール**

[SpamCop (218.100.45.34) id:6074690948]A sweet deal! Moto X. No contract. No down payment..

---

[ SpamCop V4.8.1.007 ]

This message is brief for your comfort. Please use links below for details.

Email from 218.100.45.34 / Tue, 11 Feb 2014 22:27:49 -0600

**http://www.spamcop.net/w3m?i=z6074690948z4d537a65b10c84041666fb2664f998cez**

[ Offending message ]

Return-path: <Motorola@wappextil.com>

**Received: from wappextil.com ([unknown] [218.100.45.34])**
**by vms172083.mailsrvcs.net**
(Sun Java(tm) System Messaging Server 7u2-7.02 32bit (built Apr 16 2009))
with ESMTP id <0N0V004K08E3TI20@vms172083.mailsrvcs.net> for
x; Tue, 11 Feb 2014 22:27:49 -0600 (CST)

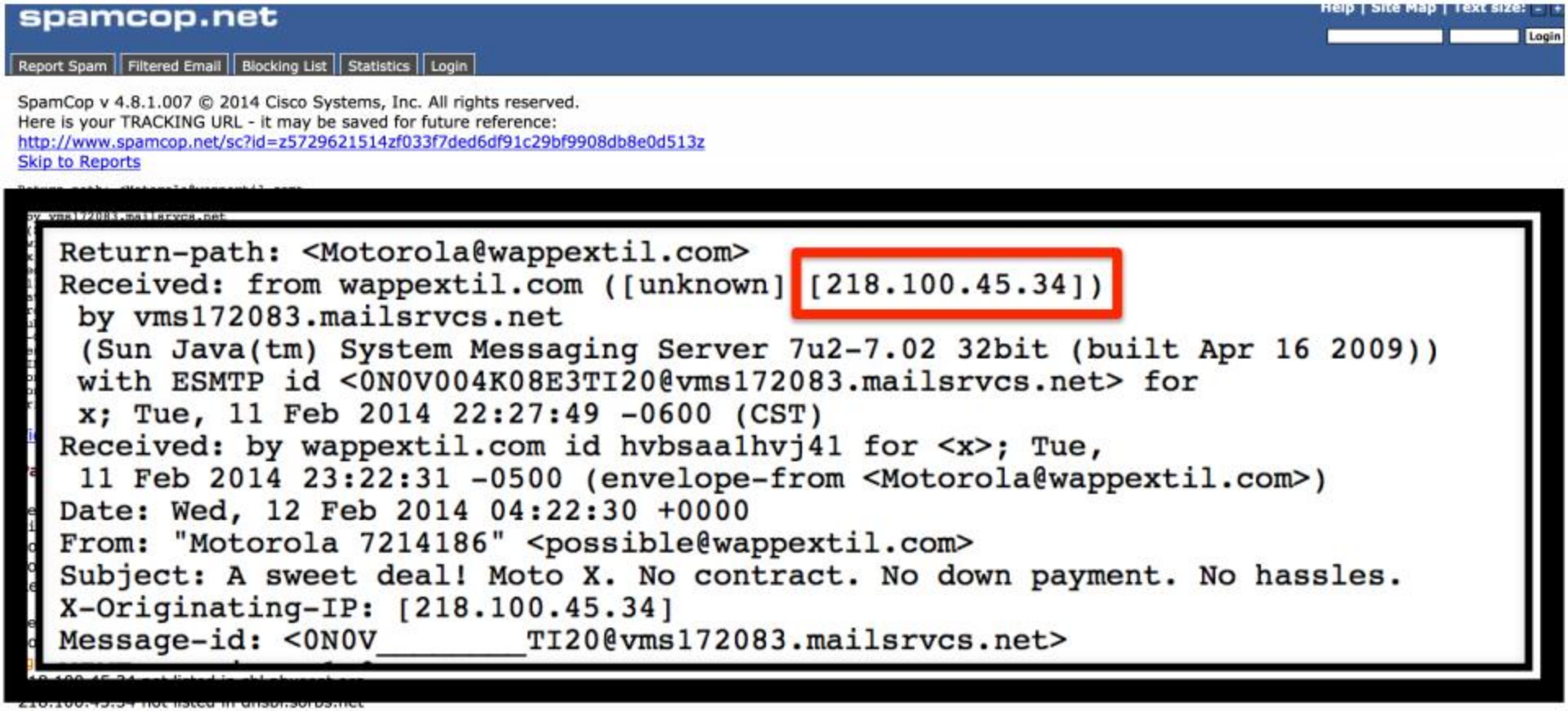
Received: by wappextil.com id hvbsaa1hvj41 for <x>; Tue,
11 Feb 2014 23:22:31 -0500 (envelope-from <Motorola@wappextil.com>)

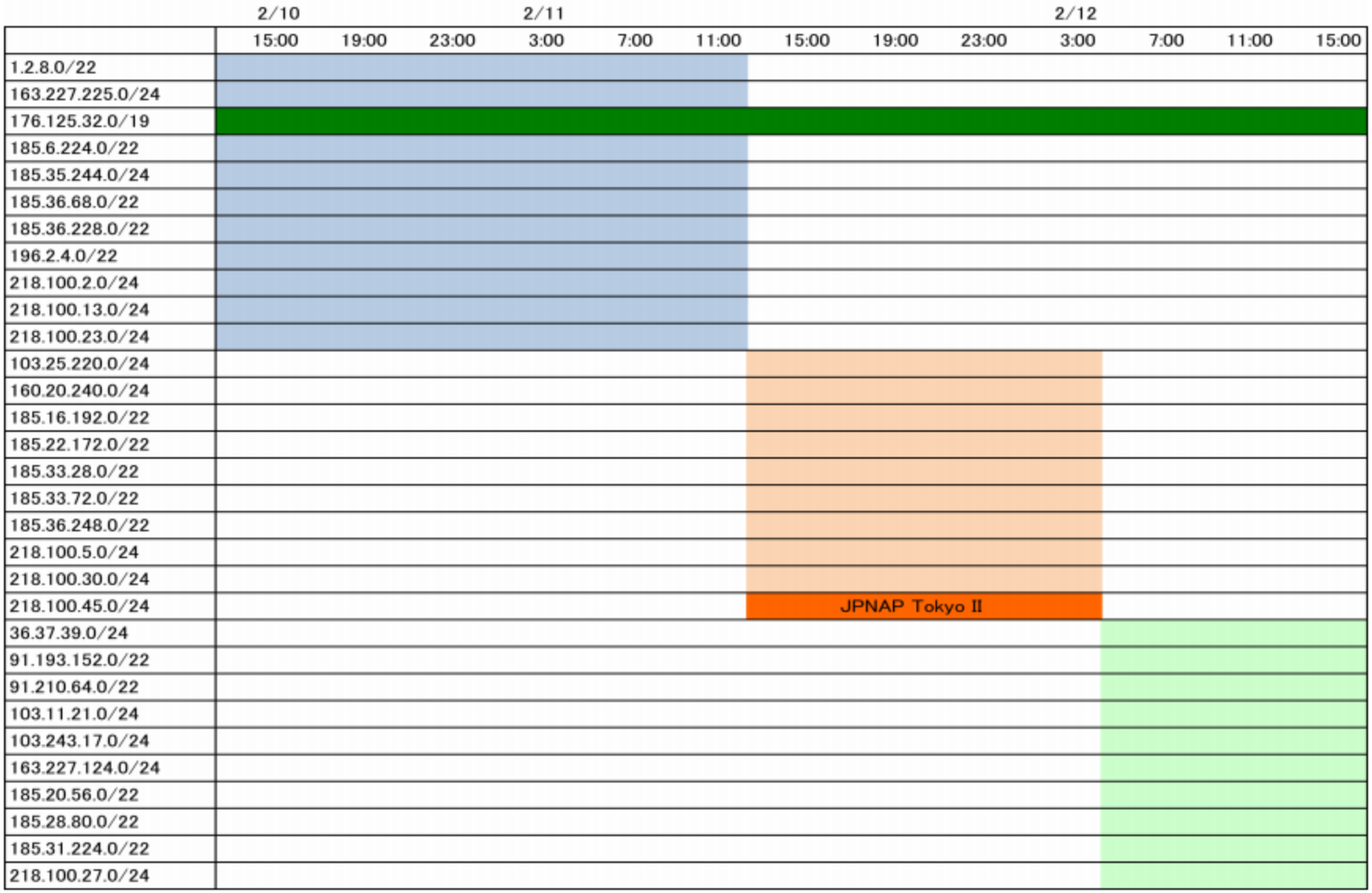
Date: Wed, 12 Feb 2014 04:22:30 +0000

From: "Motorola 7214186" <possible@wappextil.com>

Subject: A sweet deal! Moto X. No contract. No down payment. No hassles.

-- 以下、spamメールの内容添付 --

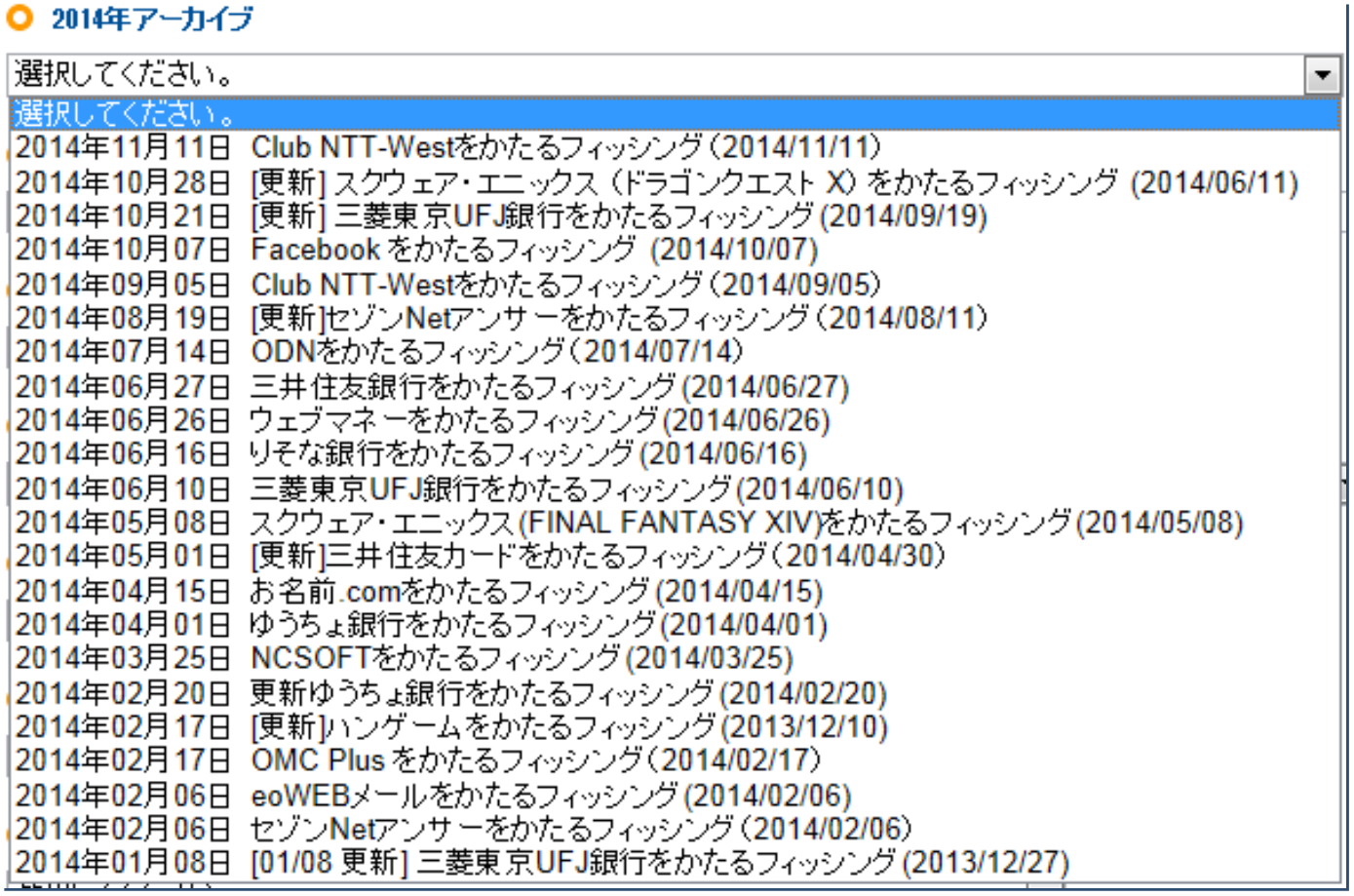




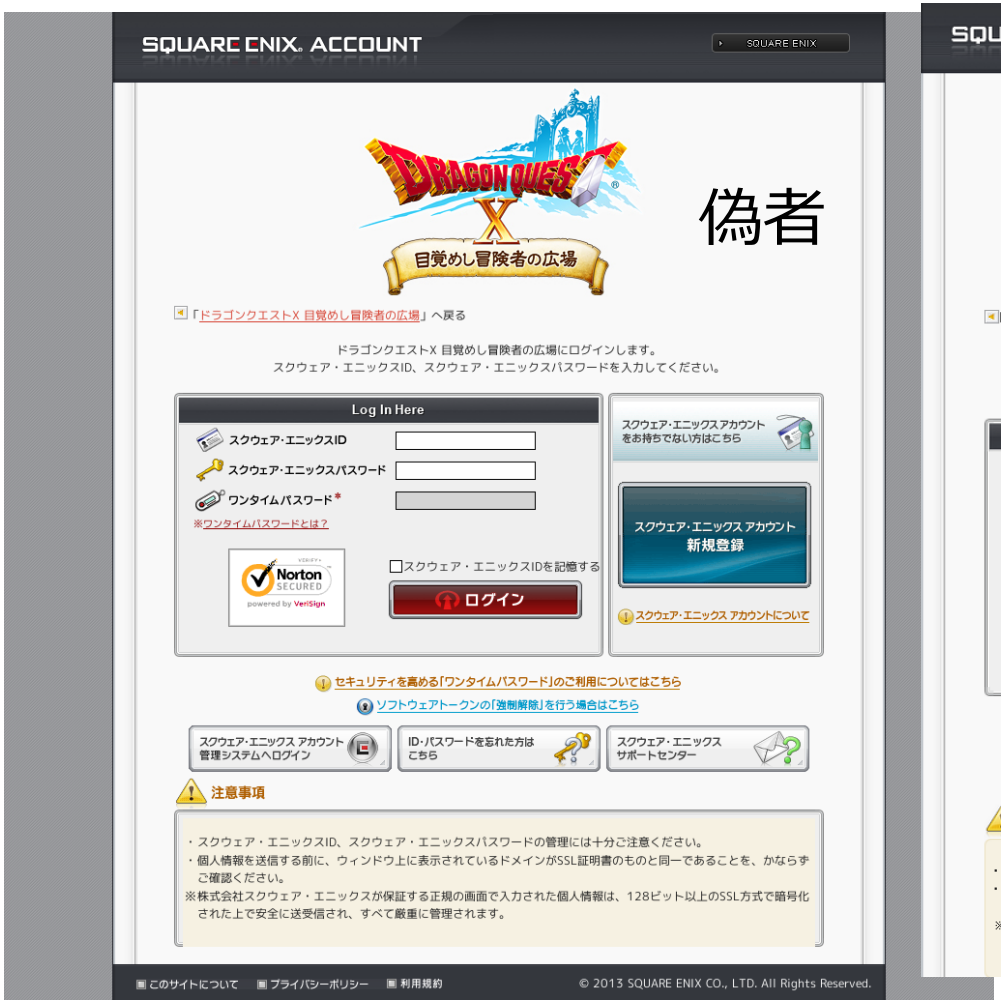
| Prefix | Desc |
| --- | --- |
| 218.100.2.0/24 | Sydney IX Lan |
| 218.100.5.0/24 | OBIS-IX,Internet Exchange Point,Okayama,Japan |
| 218.100.13.0/24 | Melbourne IX Lan |
| 218.100.23.0/24 | Dunedin Peering Exchange |
| 218.100.27.0/24 | OpenIXP, Internet Exchange Point, Indonesia |
| 218.100.30.0/24 | APJII Indonesia Internet eXchange |
| 218.100.45.0/24 | JPNAP Tokyo II IX |

# 2014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後を絶たない



# SQUARE ENIXをかたるフィッシング





https://www.antiphishing.jp/news/alert/square_enix20140611.html

# ODNをかたるフィッシング

画像1

各位加入者、
==========

ウイルスの通知

DGTFXウイルスは、電子メールのフォルダに検出されました。メールアカウントは、当社のWebメールログに、すべての重要なファイルのダメージを防ぐために、我々の新担保DGTFXアンチウイルス2014バージョンにアップグレードする必要があります。お返事]タブをクリックし、以下の列を記入し、私たちに返信したり、メールアカウントは、ウイルスの拡散を避けるために終了します。

Eメール：
ユーザー名：
パスワード：
パスワードを再確認する。

あなたのパスワードは、パスワードの安全性のための1024ビットのRSA鍵で暗号化されることに注意してください。

すべての電子メールユーザーが返信すべき！
これを行わないと、すぐにWebベースのメールアドレスは、当社のデータベースから非アクティブにレンダリングされます。
ご協力いただきありがとうございます。

ワーニングコード：ID67565434メールアカウントのサポート。
著作権?・2014

これは、2 GB のデータ計画の制限に近づいていることを通知させることです。あなたの電子メール アカウントから送信メールと受信メール アカウントは 48 時間以内にで検証されていない場合ブロックされます。

送信または電子メール クォータをアップグレードするまで、新しいメールを受信することができるされません。あなたは私たち下検証ポータルと、変更が有効に再ログインを訪問するお勧めします。

( ここで確認 )

コンピューティング サービス ヘルプ デスク サービスについての詳細。
記号。

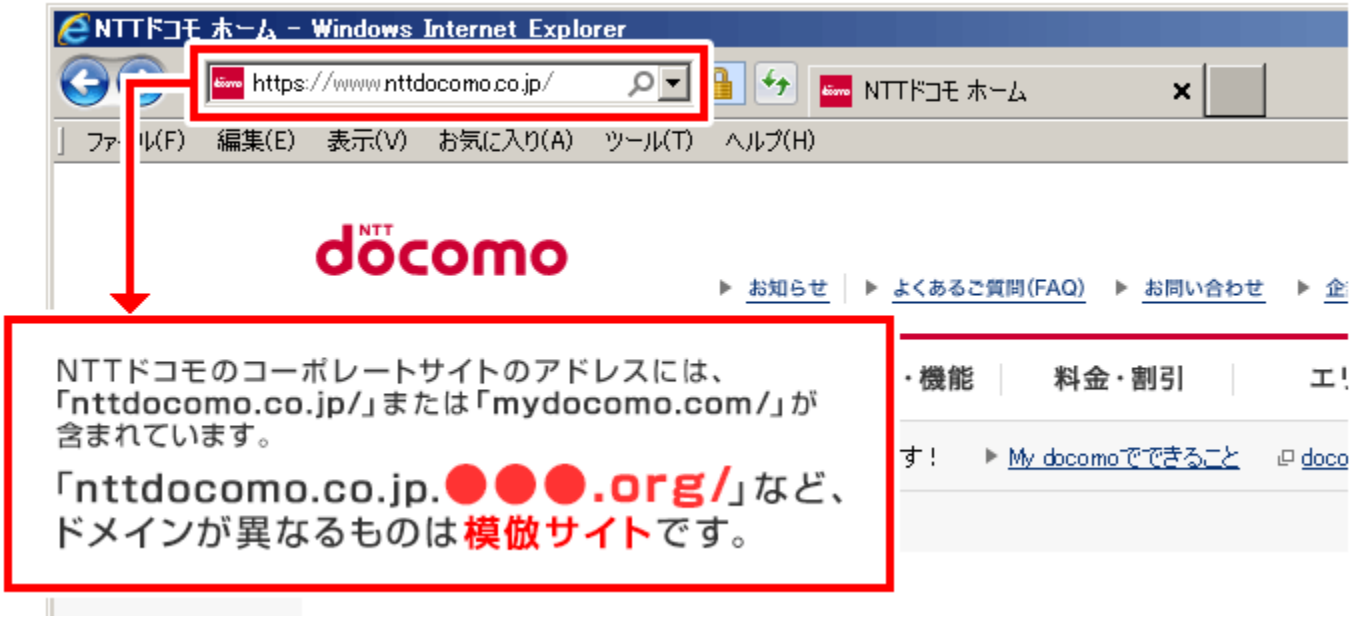
ヘルプデスク著作権 © 2014年ウェブメール管理者 （株）

画像2

https://www.antiphishing.jp/news/alert/odn0714.html

# docomoをかたるフィッシング

正規のドメインに後ろに任意のドメインをつけるパターンが多い
（一般の人が見分けにくい）




https://www.nttdocomo.co.jp/info/notice/pages/140725_00.html

# フィッシング対策ガイドラインの改訂

下記の項目が2014年6月より追加になっている。

**実施すべき**

【要件14】 ◎：利用者にパソコンを安全に保つよう、注意を促すこと

不正なポップアップが表示されインターネット・バンキングの情報を盗み取ろうとするフィッシング手口では、利用者のパソコンがマルウェアなどに感染することによって発生している。サービス事業者は利用者にパソコンやスマートフォンを安全に保つよう、注意を促す必要がある。

注意項目としては次にあげる内容を含める必要がある。

- 「Windows などの OS やウェブブラウザ、アプリケーションソフトは、最新の状態に保つこと」
- 「Flash や Java などのプラグインソフトをアップデートし、常に最新の状態を保つこと」
- 「セキュリティ対策ソフトをインストールし、機能を有効にして最新状態に保つこと」
- 「フィッシング対策に有効なツールを活用すること」
- 「発行元不明のソフトウエアはインストールしないこと」

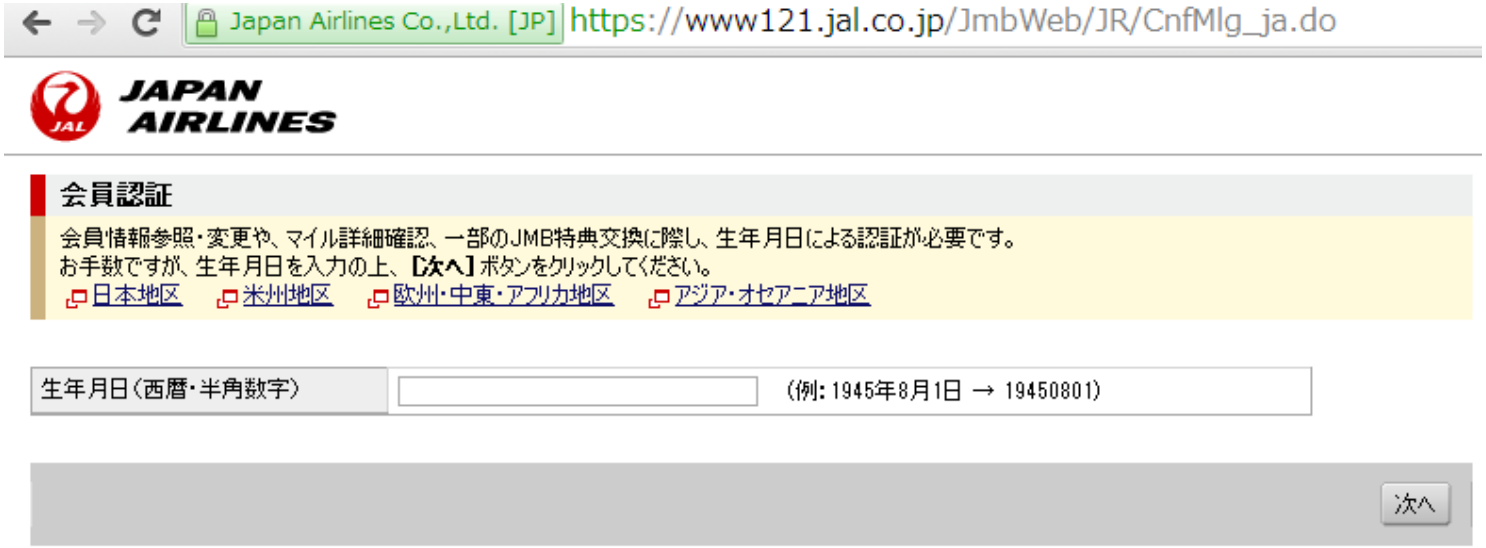
**実施推奨**

【要件15】 ○：資産の移動を実行する前に、複数要素認証を要求すること

フィッシャーによる利用者資産の窃盗被害を抑制するため、資金の移動機能（他金融機関への振込み、商品の購入等）を提供している場合には、資金の移動操作実行時に、乱数表やワンタイムパスワードなどの第二認証を求めるようにすること。

# 生年月日が追加されているサイトが増加

ログイン時に聞かれるケースや、金銭関係の取引を実施する前に改めて聞かれるケースなど

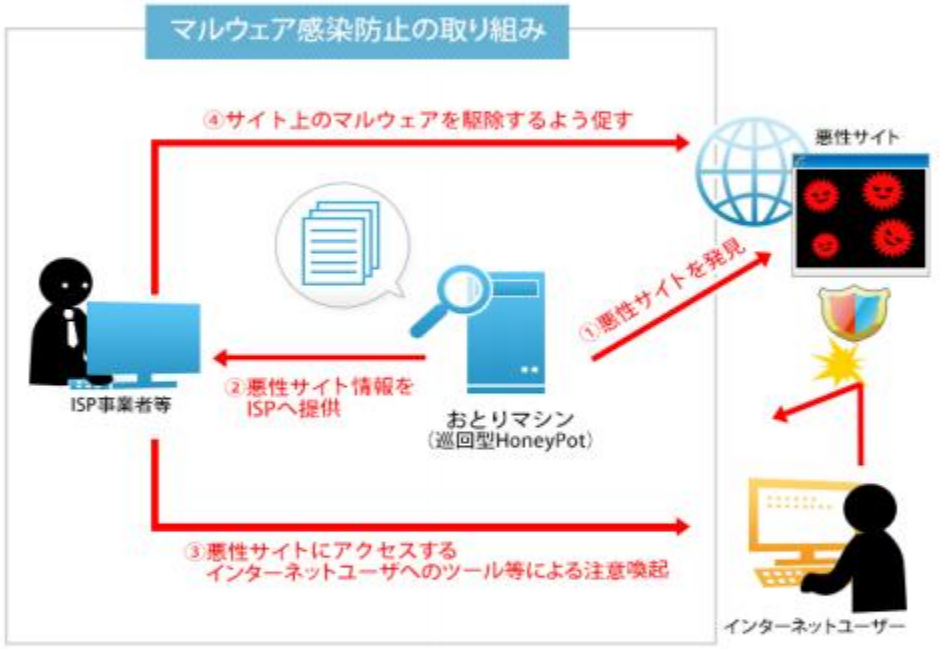



# 2014年10月 マルウェア感染防止の取り組み実績

**②悪性サイト情報（URL数）**

当月：14,173

悪性サイト情報をISP事業者へ提供した数




**★注意喚起URL数（重複したURLを除く）**

当月：833

累計：3,453

重複したURLを除く注意喚起のURL数

**③注意喚起総数**

当月：1,561回

累計：17,752回

各ISP事業者側で注意喚起（ツールのポップアップなど）をした回数

https://www.active.go.jp/pdf/jp/1410monthly.pdf

# 2014年10月 マルウェア駆除活動実績

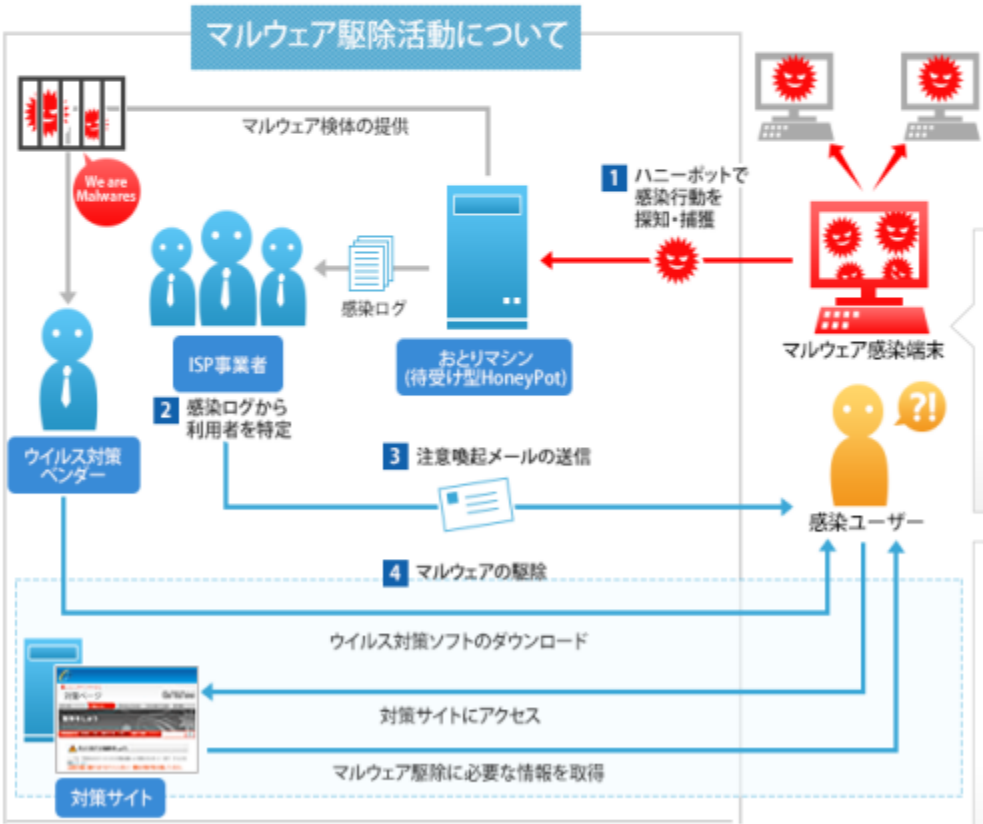
**★同定検体数 （同一検体を除く検体数）**
当月： 2,035体
累計：14,356体
収集検体総数のうち、同一検体を除く検体数

**1 収集検体総数**
当月： 39,261体
累計：947,940体
おとりマシンで検体を収集した総数

**2 利用者特定依頼数（ISP事業者合計）**
当月： 286件
累計：7,394件
各ISPへ感染ユーザーの特定を依頼した数

**★ウイルス対策ベンダー未知検体数**
当月： 174体
累計：6,723体
各ウイルス対策ベンダーにて未知判定された検体数

## マルウェア駆除活動について




**3 注意喚起ユーザー数（ISP事業者合計）**
当月： 24人
累計：996人
注意喚起を実施したユーザー数

**★ 注意喚起対象数（ISP事業者合計）**
当月： 279回
累計：4,682回
各ISPから注意喚起をした総数（同一ユーザーを含む）

https://www.active.go.jp/pdf/jp/1410monthly.pdf

# RPKIによるOrigin Validation

- IMFとJPNICでPublic ROAキャッシュをリリース（2014年10月）
  - ポータルサイトでRPKIに関する一般的な内容や技術情報を掲載
- Cisco, Juniperに続き、Alcatelでも正式にコードがリリース（2014年7月）
- 徐々に普及が進んでいるが、まだまだ課題は多い
  - 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
  - 交換されるデータ自体の暗号化がなされていない
  - ROA情報の登録者が不慣れ（アドレスホルダーが登録する前提）
  - トラストアンカーの構造が最終的にどうなるか
  - メリットが見いだせない…
- RPKI Dashboardによる普及状況の観測（http://rpki.surfnet.nl/）
  - LACNIC: 24%, RIPE: 9.4%, APNIC 0.92%

# IMF RPKI Project Page





http://www.mfeed.ad.jp/rpki/

# IMF RPKI Project Page

MF RPKI Project

## ルータ設定例

下記の例では、AS65000のBGPルータがROAキャッシュサーバ(210.173.170.254)にRPKI-RTRプロトコルで接続するための基本的な設定例とコマンド例です。 対応するVersionやその他のオプションについては各ルータベンダにお問い合わせください。

### Cisco IOS-XE

RPKI-RTR基本設定例

```
!
router bgp 65000
  bgp rpki server tcp 210.173.170.254 port 323 refresh 60
!
```

※ 上記設定では'RPKI State'が'valid'または'not found'のBGP経路のみ がルーティングテーブルにインストールされます。 invalidのBGP経路も追加したい場合は下記を参考にしてください。

BGP Origin Validation設定例('invalid'と判定された経路もルーティングテーブルにインストールする場合)

```
!
router bgp 65000
  address-family ipv4
    bgp bestpath prefix-validate allow-invalid
  exit-address-family
  !
  address-family ipv6
    bgp bestpath prefix-validate allow-invalid
  exit-address-family
!
```

※ その他のアクションを行いたい場合はroute-mapを書く必要があります。

RPKI-RTRセッション確認コマンド

```
Cisco> show ip bgp rpki servers
```

# JPNIC RPKI Project Page

JPNICはインターネットの円滑な運営を支えるための組織です

Top Q&A サイトマップ 文字サイズ：小 中 大

一般社団法人 日本ネットワークインフォメーションセンター
Japan Network Information Center

English(英語) RSS

サイト内検索 検索

トップページ > インターネットの技術

プリント用ページの表示 ツイート いいね！ 34

## リソースPKI(RPKI)

### リソースPKI(RPKI)とは

リソースPKI(RPKI)は、 アドレス資源の割り振りや割り当てを証明するためのPKI(Public-Key Infrastructure: 公開鍵基盤)で、 IPアドレスが正しく割り振られたものであるかどうかを確認できるほか、 BGPルータにおける誤ったインターネットの経路情報(Mis-Origination)を見つけるために使えます。 IPアドレスの割り振りや割り当てを証明するリソース証明書(Resource Certificate)と呼ばれる電子証明書はRPKIを使って発行されます。

BGPを使ったインターネットの経路制御では、 「IPアドレス」と「インターネット上のネットワークを識別する番号(Autonomous System Number: AS番号)」が情報交換されます。 リソース証明書は、 IPアドレスとAS番号の正しい組み合わせを示すデータ「Route Origin Authorization(ROA)」を生成するために使えます。

- リソースPKIとは(インターネット用語1分解説)
- ROAとは(インターネット用語1分解説)
- BGPルータにおける誤ったインターネットの経路情報(Mis-Origination)

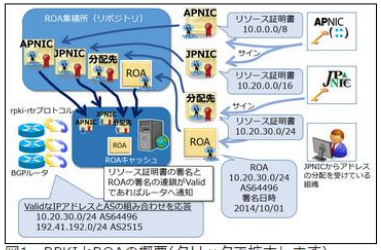


図1 RPKIとROAの概要(クリックで拡大します)

### JPNICが提供するRPKI関連の仕組み

#### RPKI模擬環境

JPNICではRPKIを簡単に試す環境として、 RPKI模擬環境を提供しています。 模擬環境は、RPKIの使い方を体験できるシステムで、 APNICのRPKIテスト環境(APNICテストベッド)と連携しています。

RPKIを本格的に利用してゆくには、 リソース証明書に記載されるIPアドレスがIPレジストリシステムのデータベースに基づいたものである必要があると考えられます。 模擬環境では、RPKIの体験や技術検証のための環境であるため、 JPNICのRPKI担当者が、 模擬環境利用者の希望や状況に応じてIPアドレスの分配情報を入力しています。 利用者はROAの発行をWebから実行できます。 模擬環境で発行したROAは、 ROAパブリックキャッシュサーバ等へいくつかの処理を経た上で転送され、 BGPルータで検証が可能となっています。

RPKI模擬環境は、 IPアドレスの分配を受けている方がWebインタフェースを利用してROAを発行したり、利用者側で立ち上げられたROAキャッシュでそれを処理したり、 といった技術的な操作を確認するために使えます。

またRPKIのリソース証明書を自組織で発行できるRPKIのプログラム(例：RPKI Tools)の設定をして、JPNICの模擬環境と接続し、 動作検証をすることも可能です。

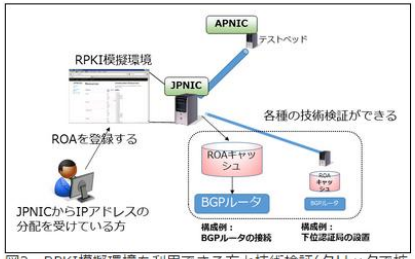


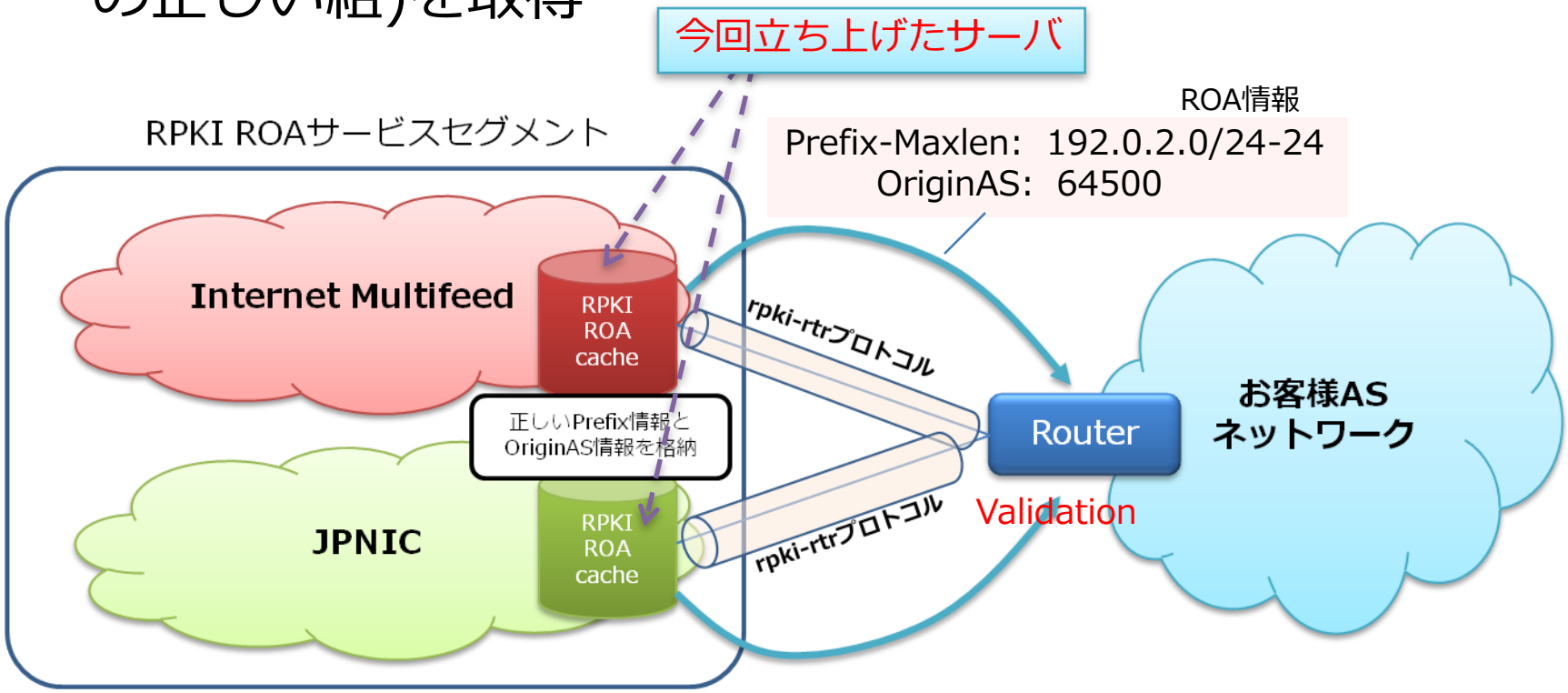
図2 RPKI模擬環境を利用できる方と技術検証(クリックで拡大します)

- インターネットの技術
  - IETFとRFC
  - IRR
  - DNS
  - RPKI
  - ENUM
  - ドメイン名の国際化

https://www.nic.ad.jp/ja/rpki/

# サービス提供概念図

- お客様ASネットワーク上にあるBGPルータが、「rpki-rtrプロトコル」を使ってRPKI ROA cache情報(IP/ASの正しい組)を取得



# 内容

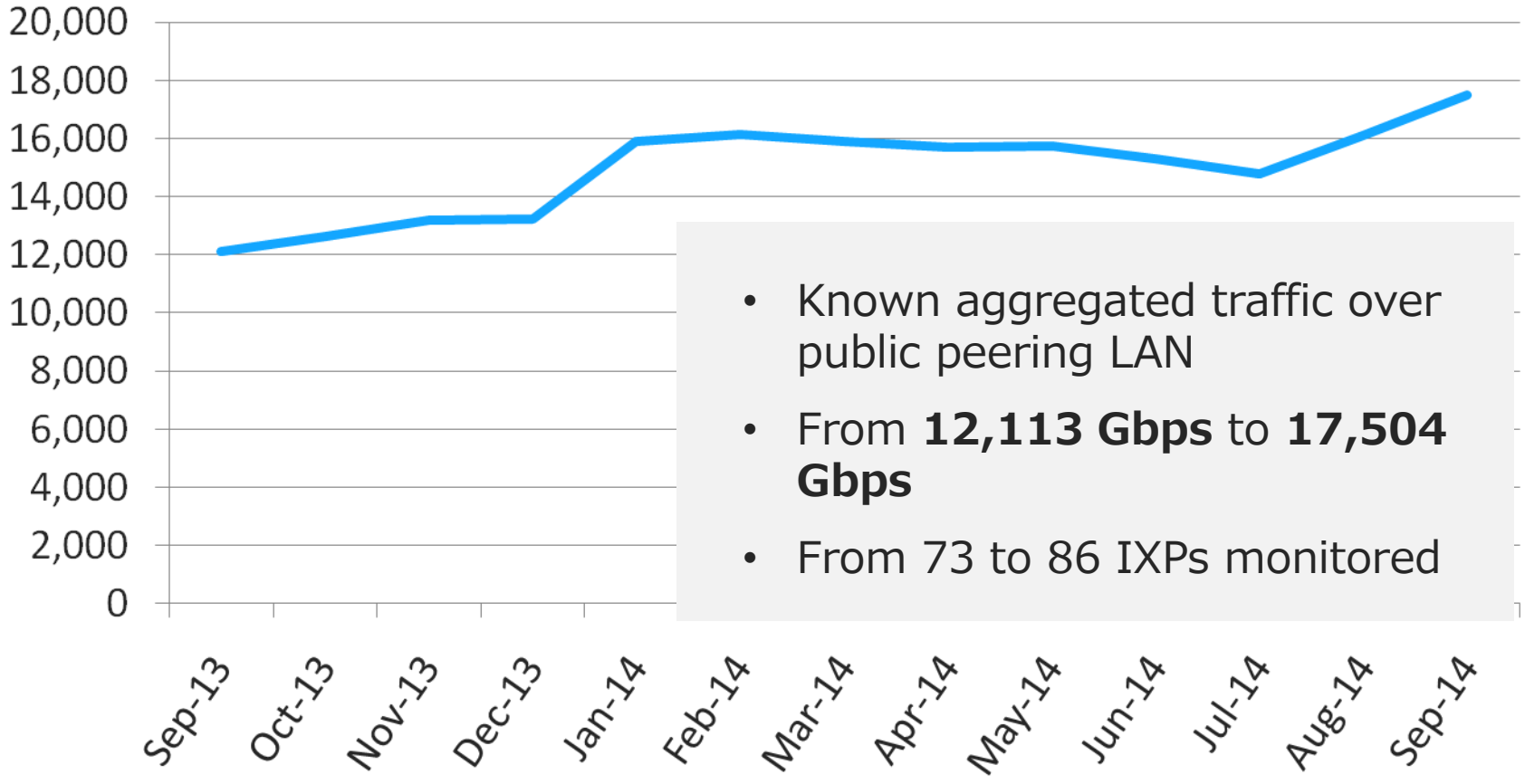
- トラフィック動向
- ルーティング動向
- DNS動向
- セキュリティ動向
- 日本や世界のIX動向
- まとめ

# 日本や世界のIX動向

- Open-IX
  - 加盟組織によって運営され、北米で中立的なIXの拡大を促進
  - Open-IXの暫定ボードメンバーには、Google、Akamai、Netflix、Comcast等に所属する個人が参画
  - 2013年末～2014年にかけて、欧州の主要IX(AMS-IX, LINX, De-CIX)が北米に進出しIX事業を展開

- SDN-IX
  - SDN技術を活用し、様々なネットワークをIX上で相互接続。既存のBGPにとらわれない接続方式など柔軟性が高い

# Traffic Growth in Euro-IX Region

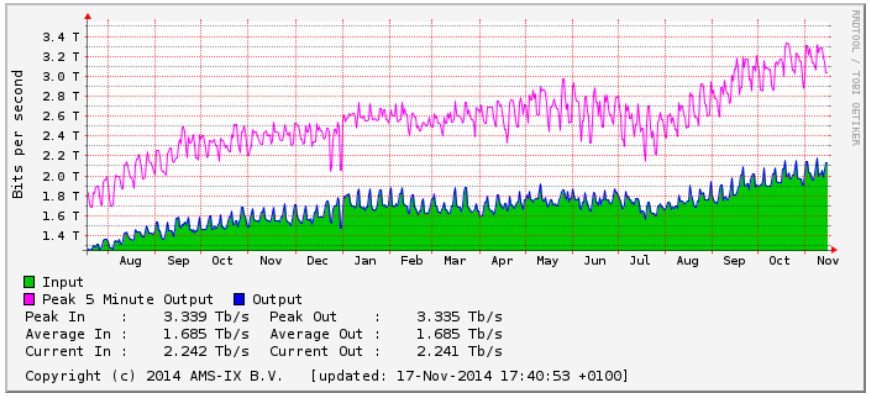



- Known aggregated traffic over public peering LAN
- From **12,113 Gbps** to **17,504 Gbps**
- From 73 to 86 IXPs monitored

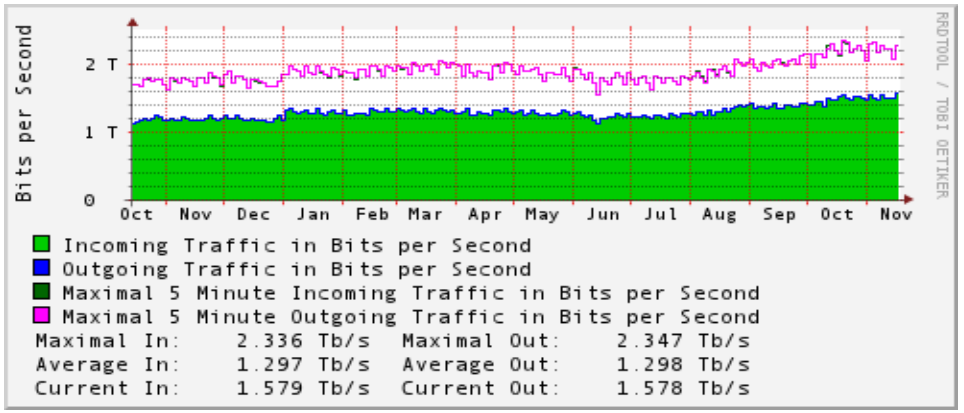
Euro-ix reportより（2014）

# 4 Major IXs

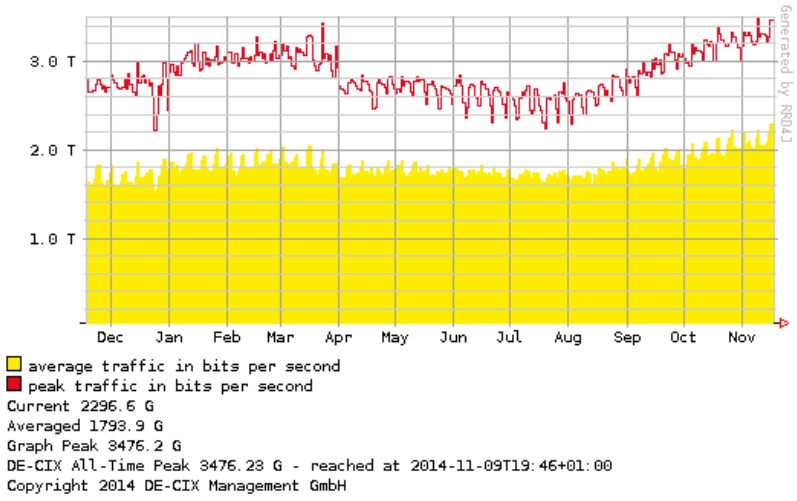
AMS-IX



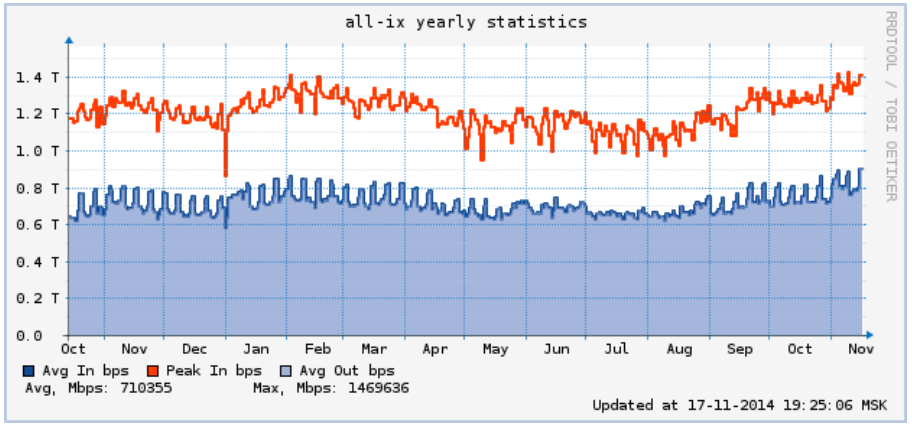

LINX




DE-CIX

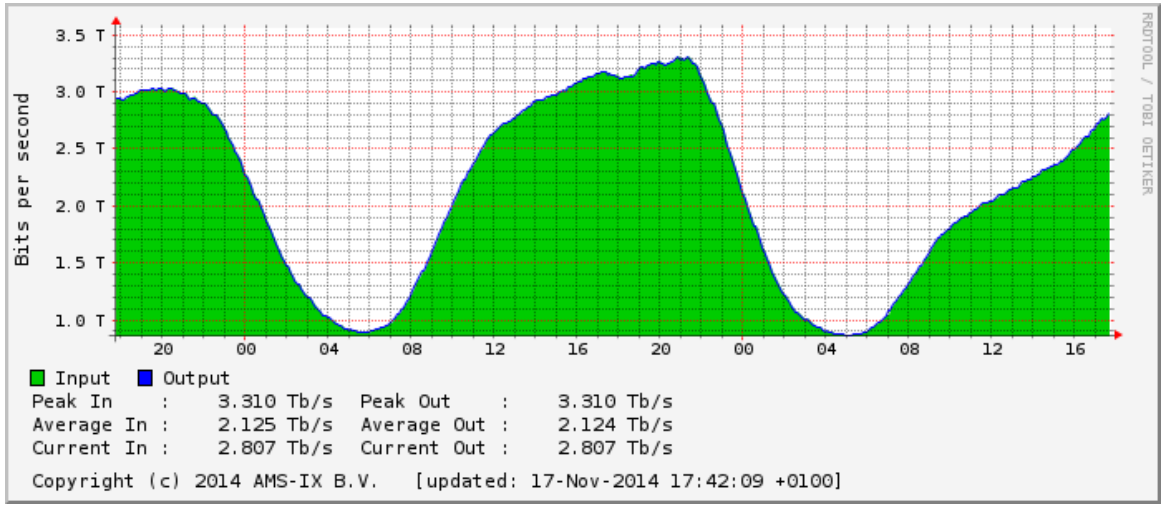



MSK-IX

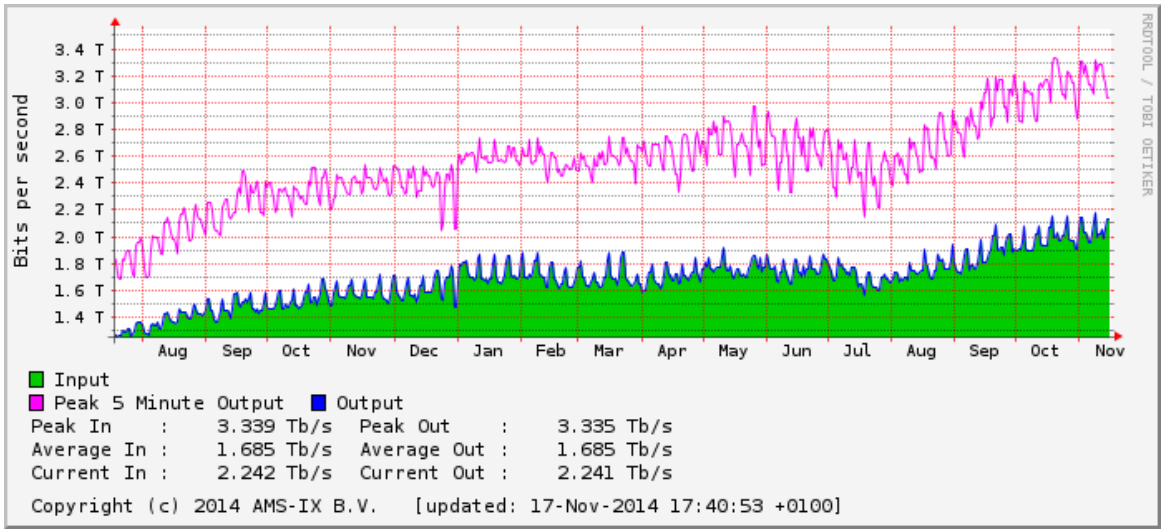


# AMS-IX

IXのアドレスを
/21から/20へ拡張




ピークは
20時～21時頃

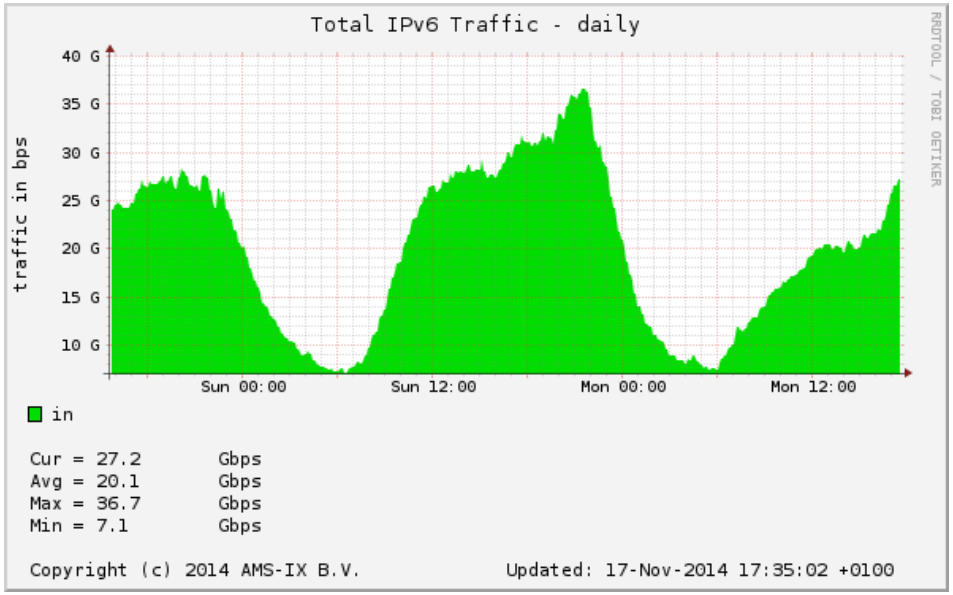


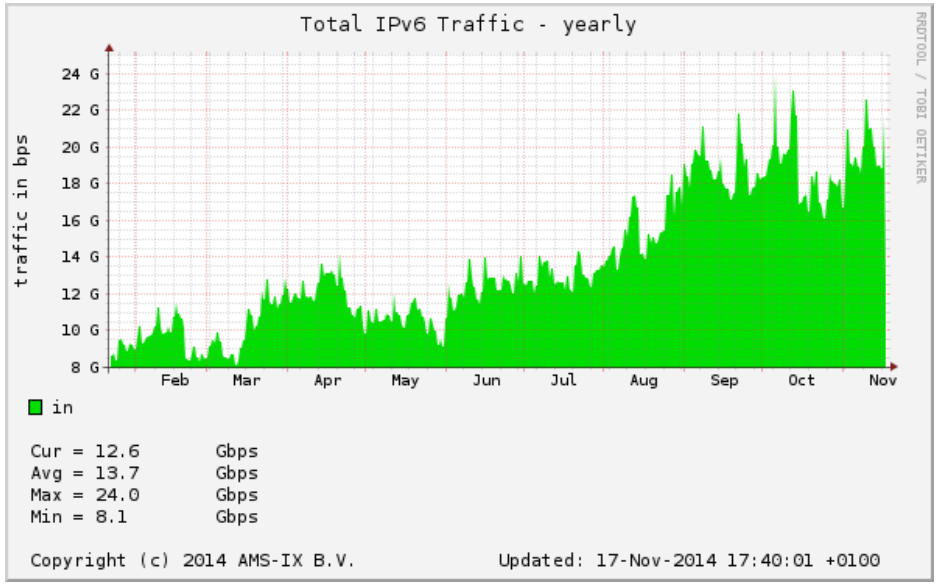

夏以降増加
（例年同様）

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

# AMS-IX：IPv6

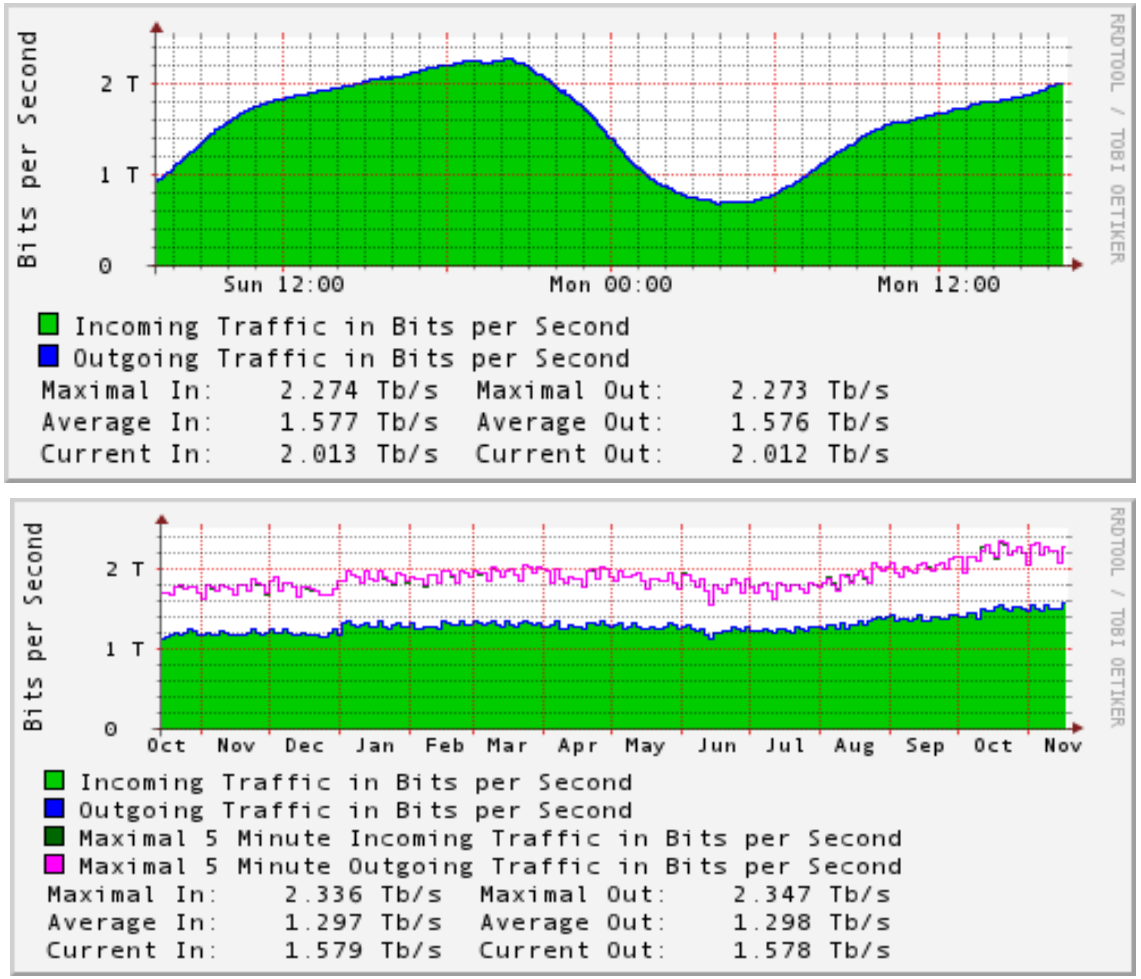
昨年より2倍程度増加
6月以降増加しているように見える




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

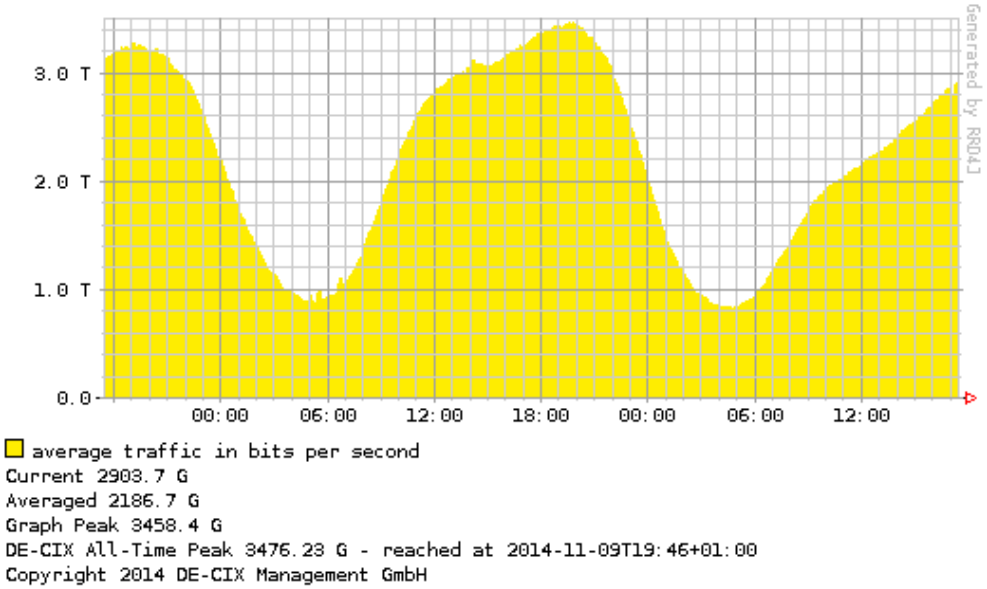
# LINX

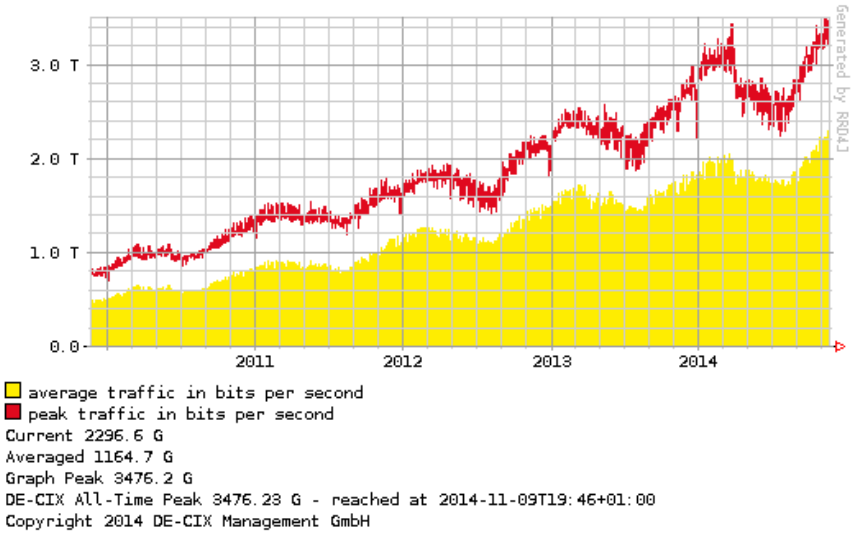



https://stats.linx.net/cgi-pub/exchange?log=combined.bits

# DE-CIX

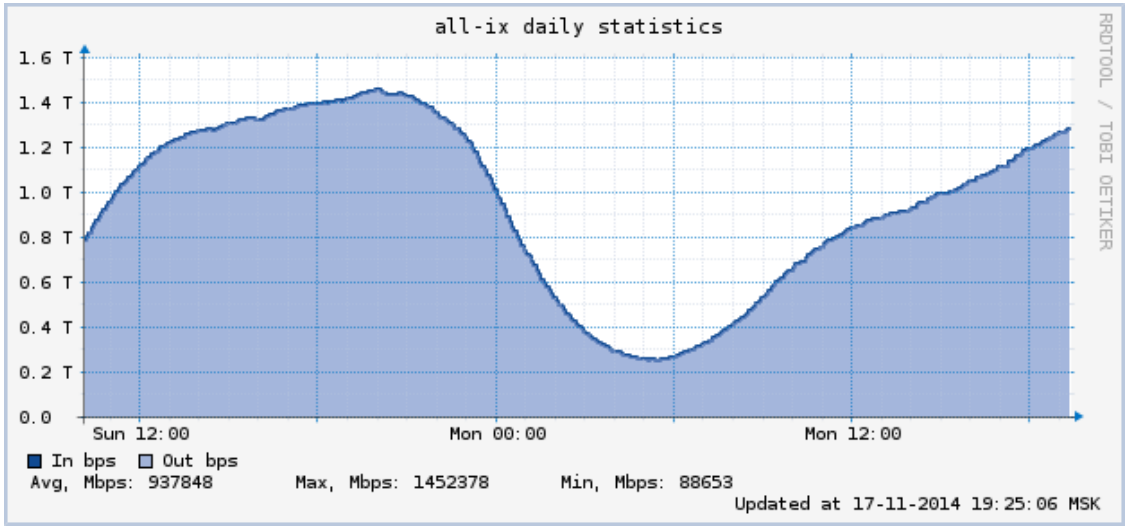
15 seconds average で sFLOWデータを元に描画

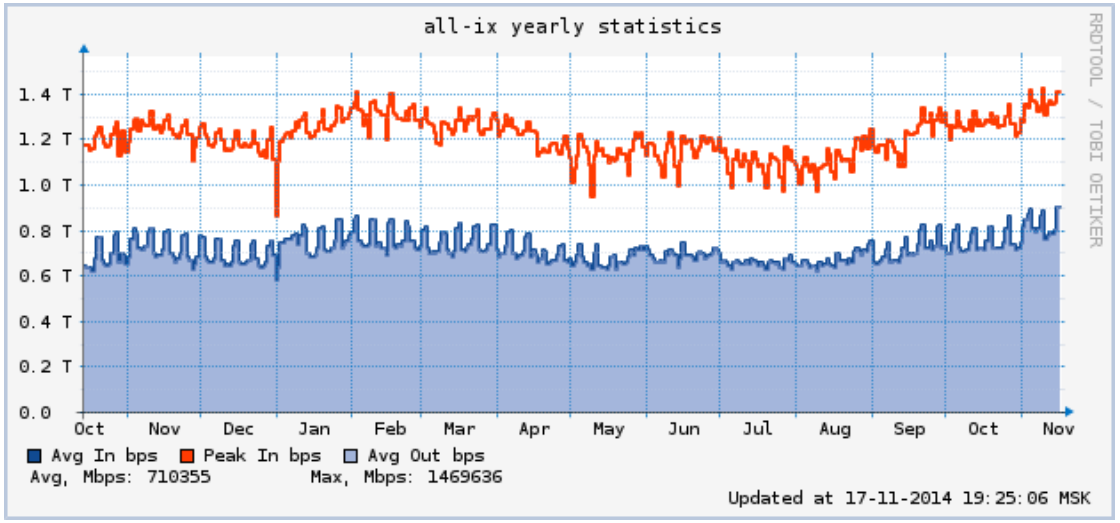



http://www.de-cix.net/content/network.html

# MSK-IX




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

# 2014年のまとめ

- トラフィック動向
  - 継続増加。スマホ等のモバイルトラフィックが牽引（年1.5倍）
  - 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やコントロールが必要な状況が増加
- ルーティング動向
  - 枯渇後もIPv4は依然増加、IPv6も単調増加、IPv4フルルートが50万を超える
  - 2byteAS番号は残り300AS、IANAプールもじきに枯渇
- DNS動向
  - オープンDNSフォワーダーによる攻撃やドメインハイジャックも多数発生
  - TLDドメインが本格化する中、名前衝突などに注意が必要
- セキュリティ動向
  - 大規模するDDoS攻撃、インターネット全体での協調した取り組みが必要
  - 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倍程度で拡大
  - 欧州型のIXモデルが北米へ(Open-IX)