2014年のroutesec国際動向

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

内容

- routsec国際動向
- RPKI動向
- 軽く512K問題

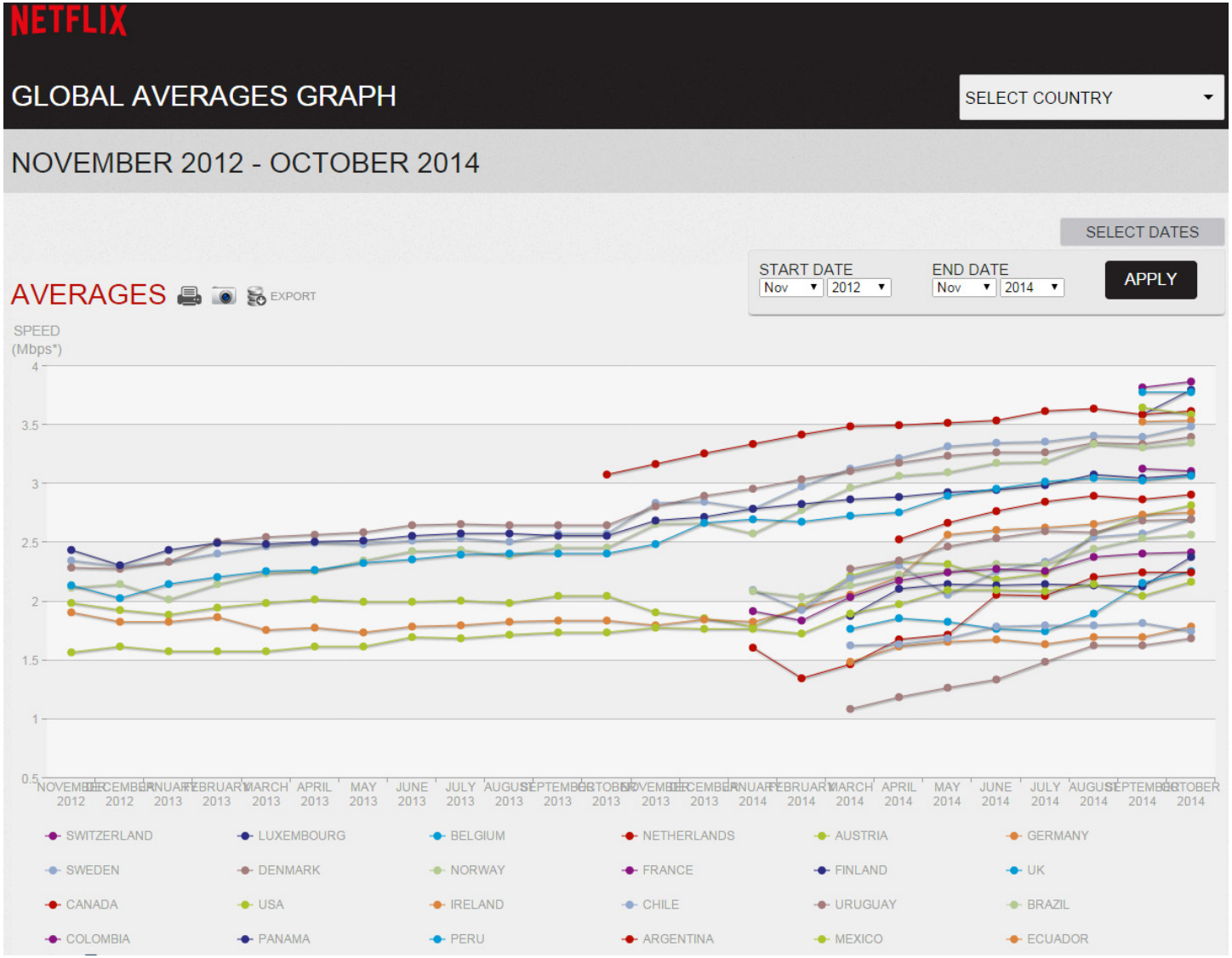
内容

- routsec国際動向
- RPKI動向
- 軽く512K問題

Video配信事業者によるISP格付け

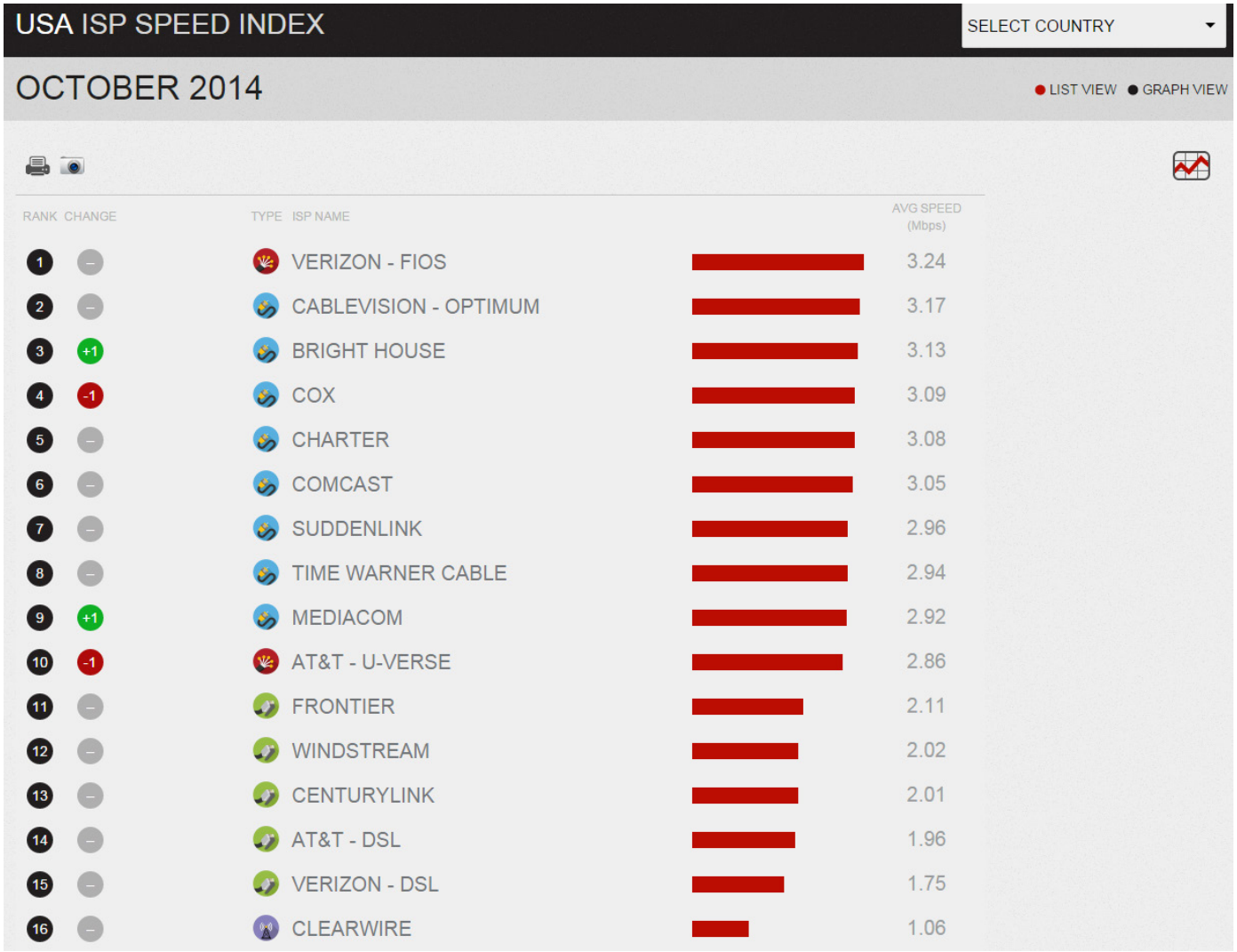
- Netflixの自社サイトでサービス提供国でのISP毎のVideo視聴品質を公開
- Googleによるyoutubeストリーミング品質の解析ツールをリリース（2014年5月）

NETFLIXによる ISP Speed Index



http://ispspeedindex.netflix.com/

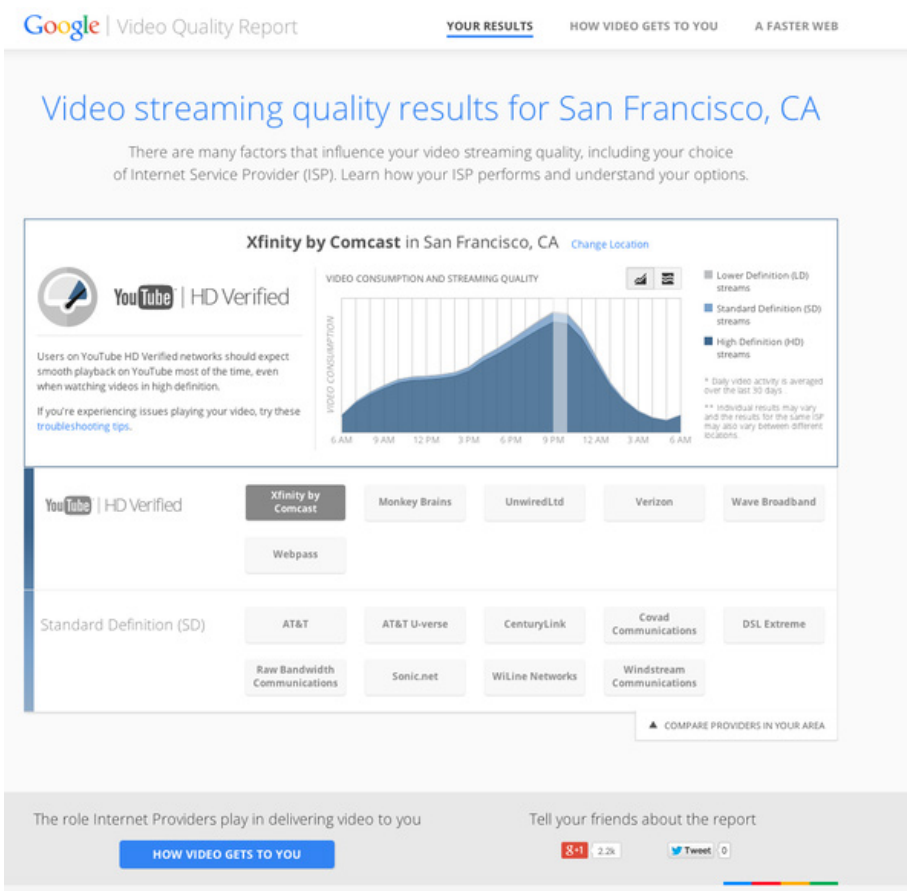
NETFLIX USA ISP Speed Index



http://ispspeedindex.netflix.com/

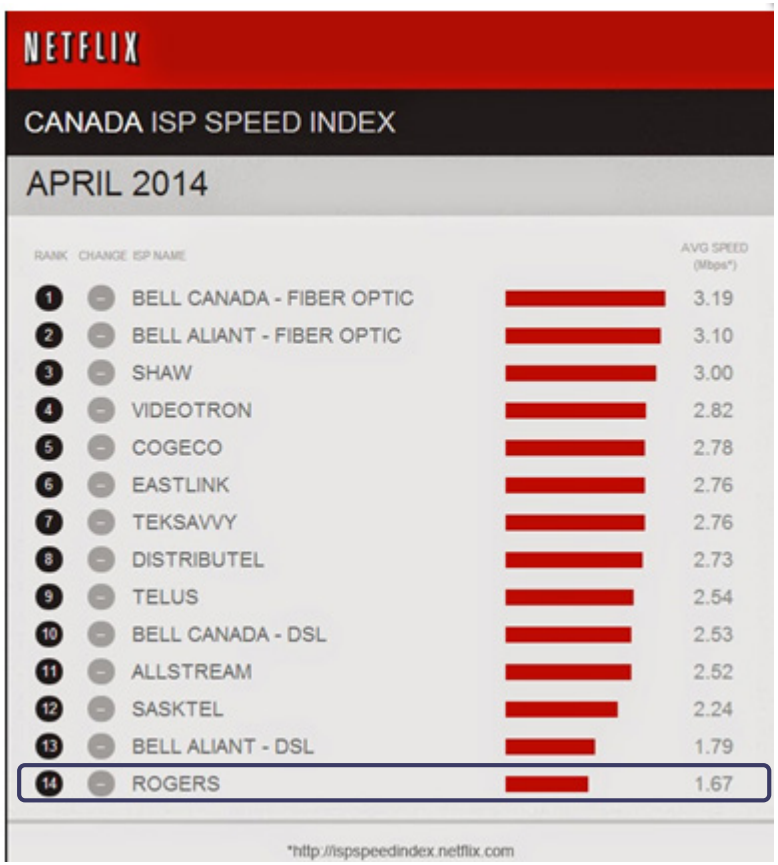
Google Video Quality Report

- 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

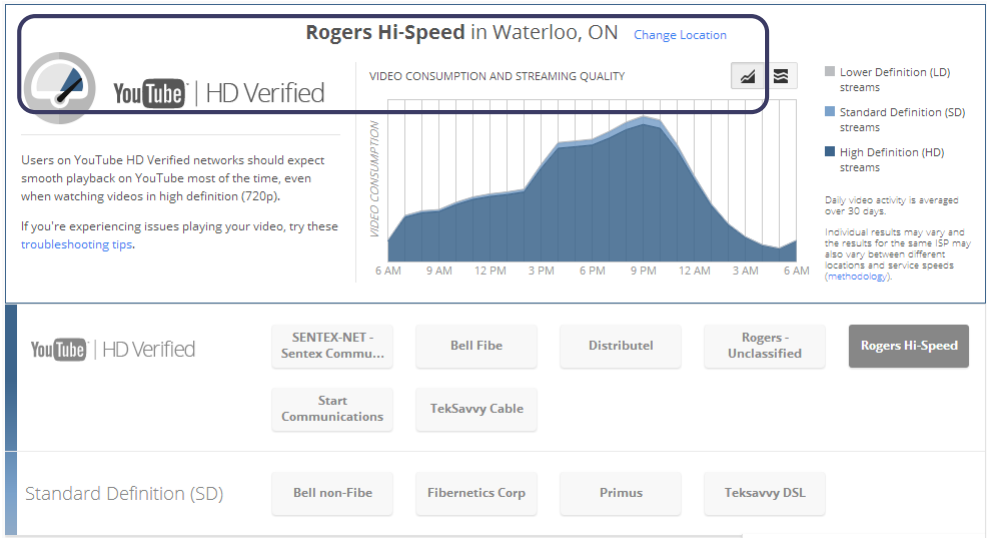


事業者毎の品質比較(CAの例)

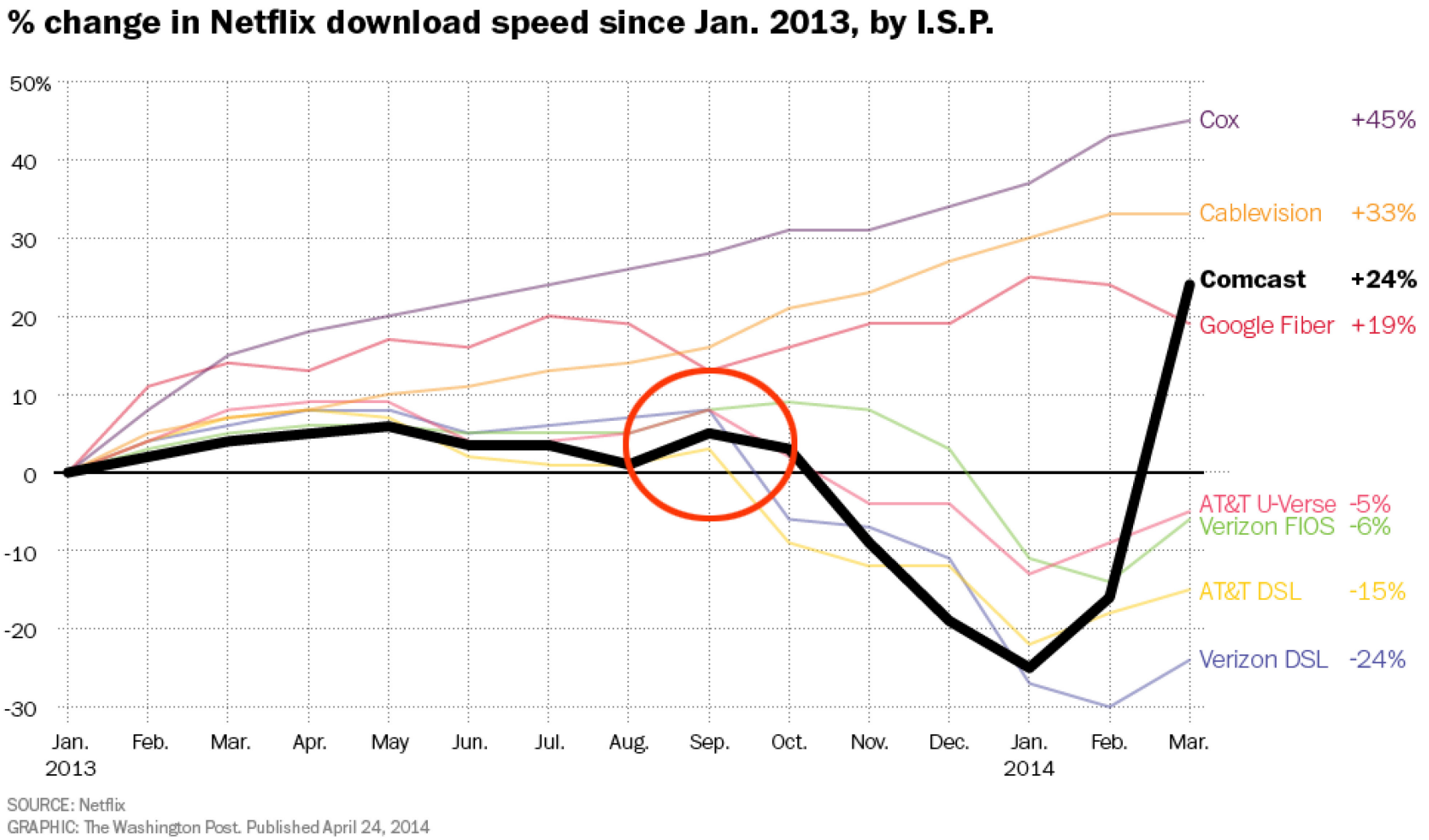
- NetflixとGoogleで結果がまったく違う。。。



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



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



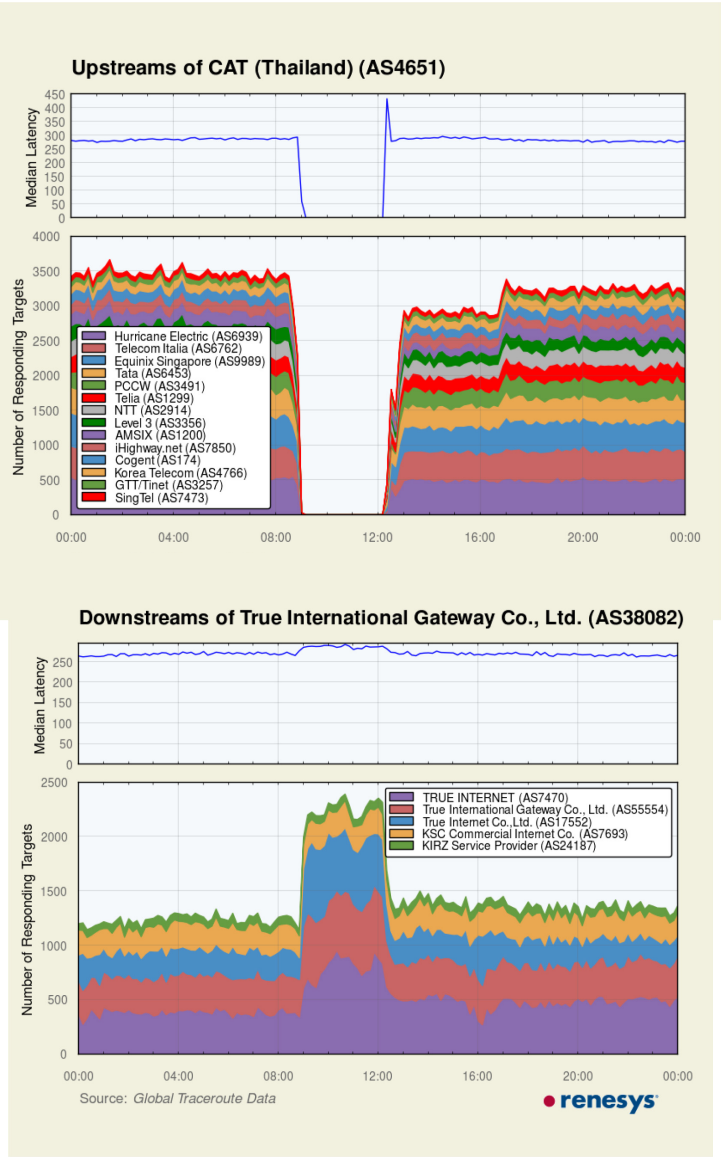
http://blog.streamingmedia.com/2014/06/netflix-isp-newdata.html

買収案件

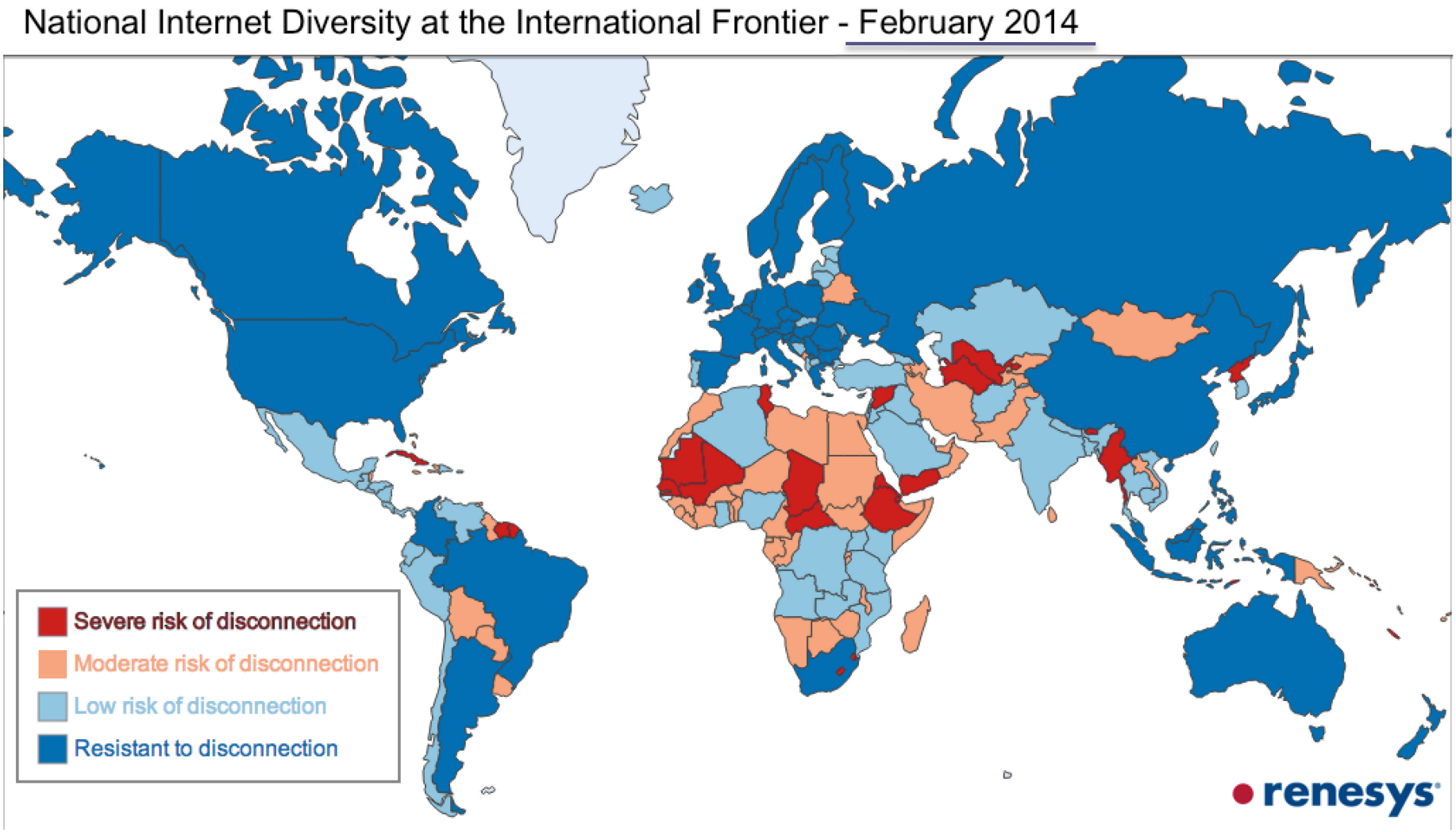
- Dyn、インターネットモニタリングのRenesysを買収
（2014年5月）
- Google、クラウドモニタリングの新興企業Stackdriverを買収
（2014年5月）
- Level3、tw telecomを57億ドルで買収へ
（2014年6月）

2013年12月: タイ政府への反政府デモに起因したOutage

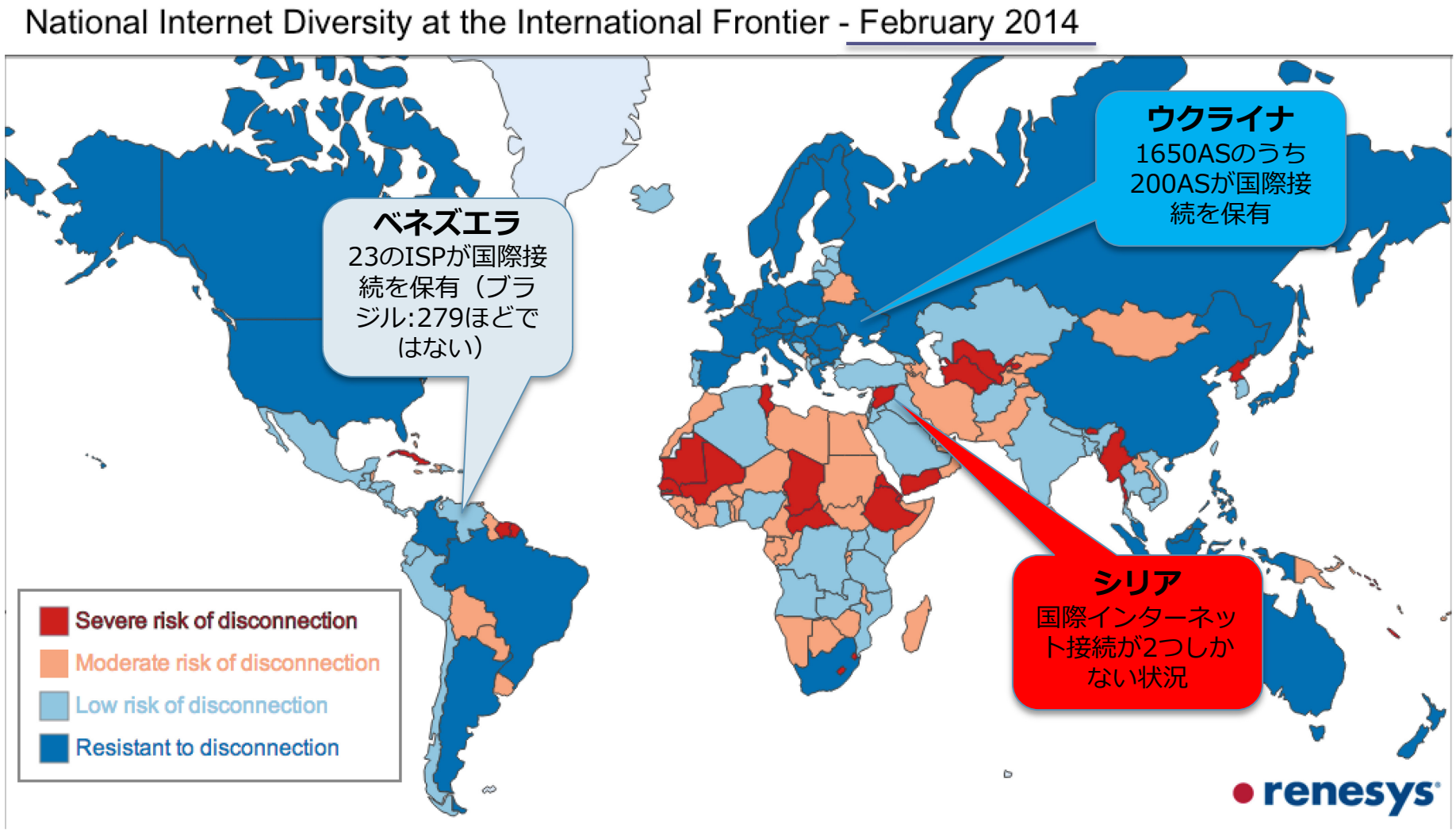
- タイ国営のThai telecomが運営するAS4651が約3時間程度に渡り通信不能
- しかし、マルチホームをしていたAS群はalternate pathにきちんとトラフィックがバックアップされる
- タイのインターネットは素晴らしい！という話！



Syria, Venezuela, Ukraine ネット情勢



Syria, Venezuela, Ukraine ネット情勢



2011年 中東地域の経路消失

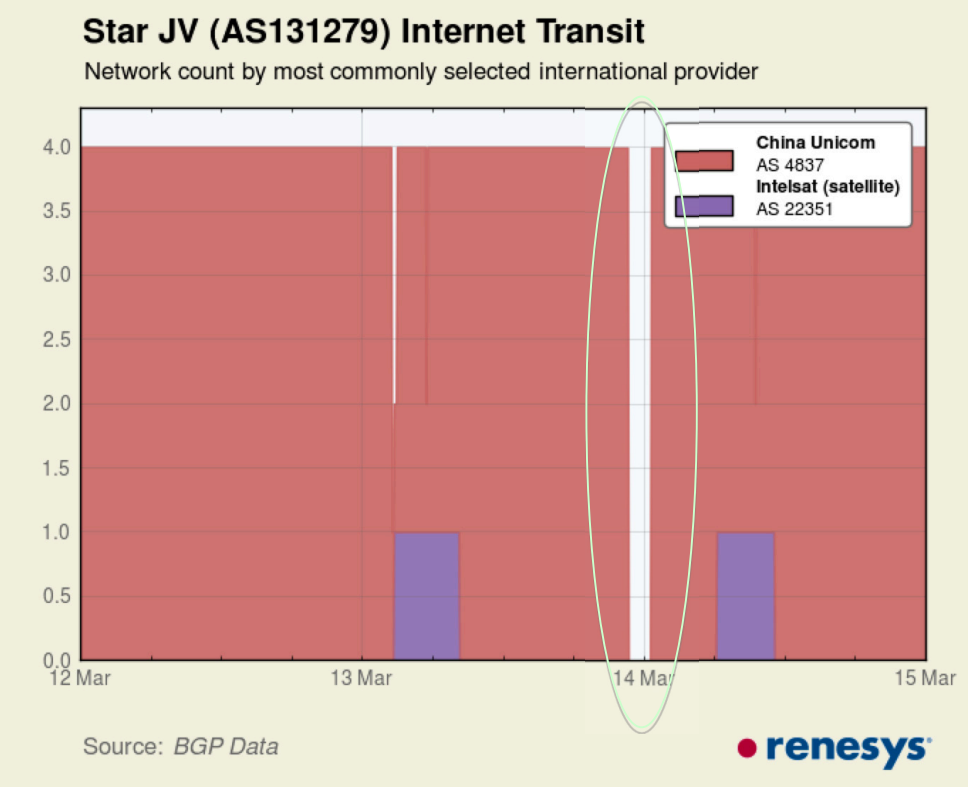
	エジプト	リビア	シリア	パキスタン
事象	約2900程度のエジプト国内のprefixが320経路程度に減少し、通信が遮断された	ほぼ全てのISPの経路が消失	全域の2/3程度の経路が消失した模様	ほぼ全てのISPの経路が消失
発生時期	2011年1月	2011年2月	2011年6月	2011年10月
要因	反政府デモを当局が防ぐため、デモ情報の伝達手段として利用されるFacebook、Twitter、Blackberryなどインターネットや SMSを遮断した	カダフィ大佐による独裁体制が続くリビアでも、反体制デモが続発していたことから、エジプト同様にネットを遮断	アサド政権に対する反政府デモが続いており、その断圧を目的としてシリアの2/3程度がインターネットから遮断	
対処方法	なし	なし	なし	なし

2013年の経路消失事件

- ３月：北朝鮮
- ８月：ミャンマー
- ９月：スーダン

- 反政府運動を阻止するためにネットを遮断する動きが目立っている

北朝鮮： 4Prefixが2時間程度Withdrawn状態に

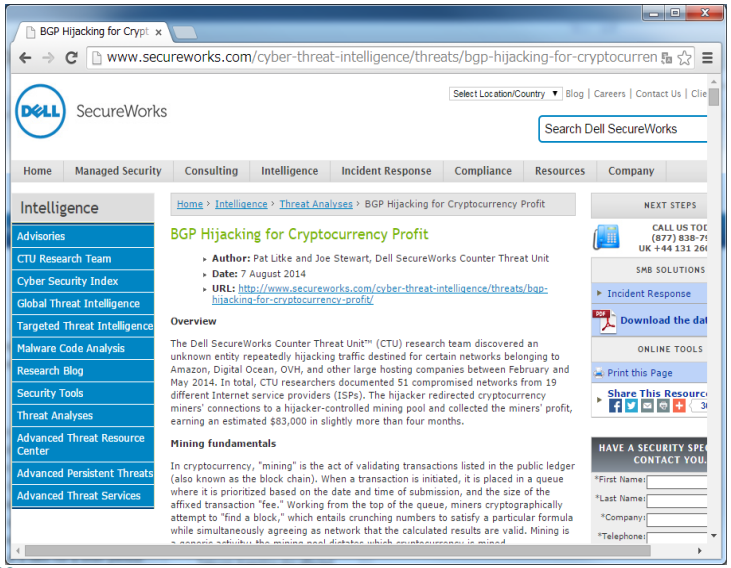


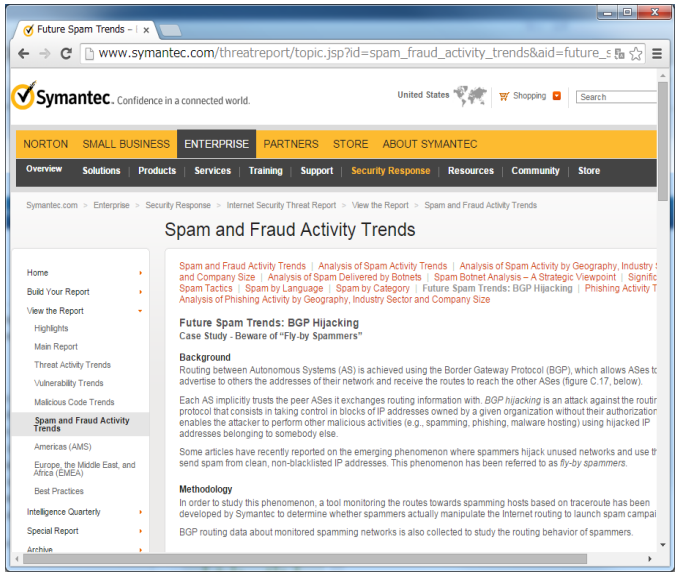
2014年の経路ハイジャック事情

- 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 --

spamcop.net

Report Spam | Filtered Email | Blocking List | Statistics | Login

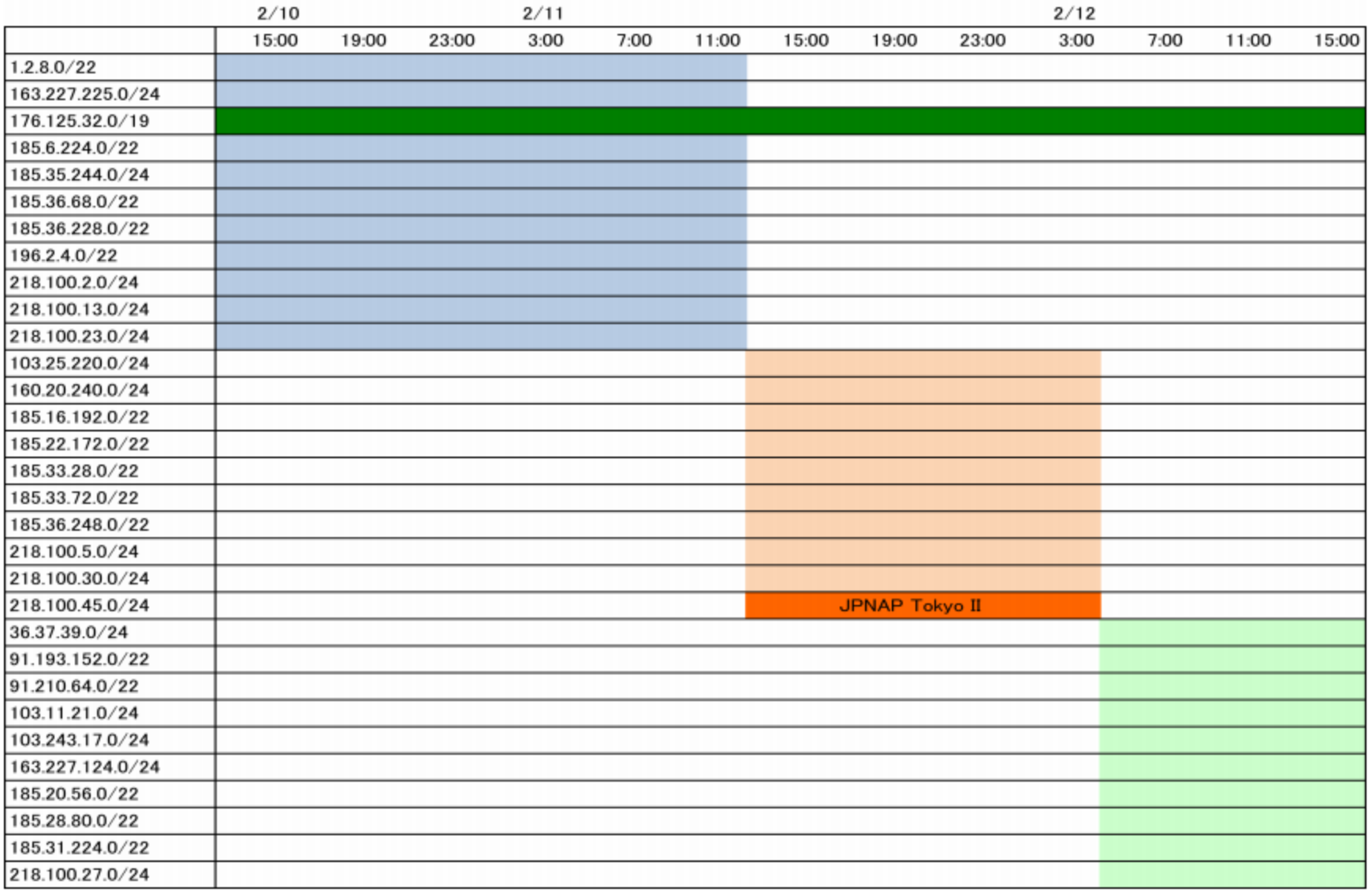
SpamCop v 4.8.1.007 © 2014 Cisco Systems, Inc. All rights reserved.
Here is your TRACKING URL - it may be saved for future reference:
http://www.spamcop.net/sc?id=z5729621514zf033f7ded6df91c29bf9908db8e0d513z
Skip to Reports

```
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 hvbsaalhvj41 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.
X-Originating-IP: [218.100.45.34]
Message-id: <0N0V________TI20@vms172083.mailsrvcs.net>
```

218.100.45.34 is not an MX for vms172083.mailsrvcs.net
218.100.45.34 is not an MX for vms172083.mailsrvcs.net

Tracking message source: 218.100.45.34:

Routing details for 218.100.45.34
[refresh/show] Cached whois for 218.100.45.34 : tech-c@mfeed.ad.jp
Using last resort contacts tech-c@mfeed.ad.jp
Sorry, this email is too old to file a spam report. You must report spam within 2 days of receipt. This mail was received on Tue, 11 Feb 2014 22:27:49 -0600


2/10
2/11
2/12
15:00
19:00
23:00
3:00
7:00
11:00
15:00
19:00
23:00
3:00
7:00
11:00
15:00
1.2.8.0/22
163.227.225.0/24
176.125.32.0/19
185.6.224.0/22
185.35.244.0/24
185.36.68.0/22
185.36.228.0/22
196.2.4.0/22
218.100.2.0/24
218.100.13.0/24
218.100.23.0/24
103.25.220.0/24
160.20.240.0/24
185.16.192.0/22
185.22.172.0/22
185.33.28.0/22
185.33.72.0/22
185.36.248.0/22
218.100.5.0/24
218.100.30.0/24
218.100.45.0/24
JPNAP Tokyo II
36.37.39.0/24
91.193.152.0/22
91.210.64.0/22
103.11.21.0/24
103.243.17.0/24
163.227.124.0/24
185.20.56.0/22
185.28.80.0/22
185.31.224.0/22
218.100.27.0/24

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

その他hijack関連事案

- INDOSAT hijacking various prefixes
  - 2014年1月、Googleの8.8.8.8やAkamai, Amazonなどを含む2800程度のPrefixを38分間hijack
- Google DNS hijacking from Venezera
  - 2014年3月、8.8.8.8/32がAS7908より23分間広告
    - ブラジルやフロリダの大学等に一部影響が出たが、/32だったので広範囲の被害には至らず
- HIJACKS: Detecting and Characterizing Internet Traffic Interception based on BGP Hijacking（2014年７月）
  - ハイジャック監視システムを開発、すでに世界中の３６カ国、８３箇所にモニタリングシステムを設置

内容

- routsec国際動向
- RPKI動向
- 軽く512K問題

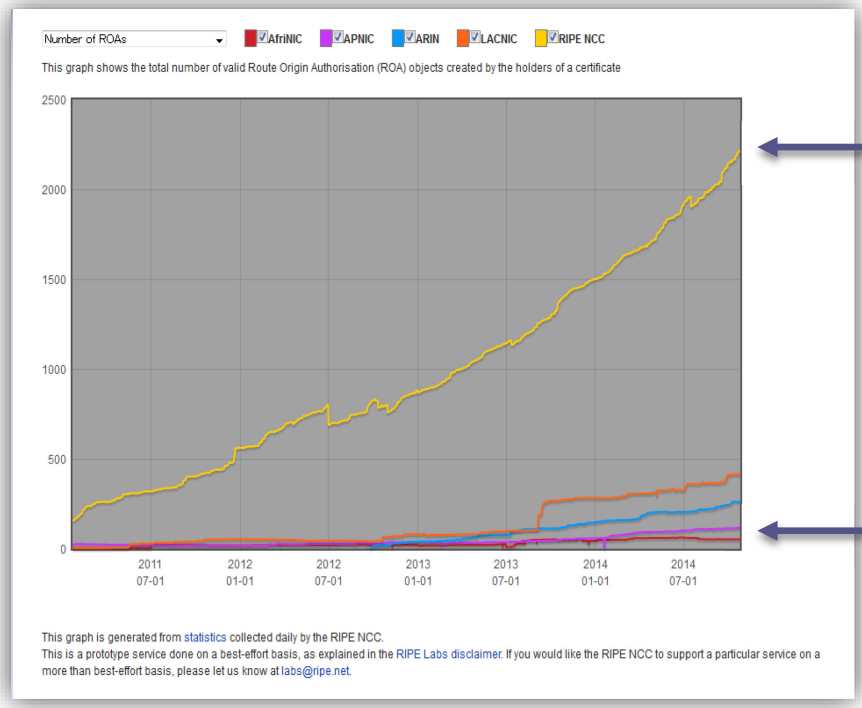
2014年はRPKI元年

- 2014/10/1
  - 日本国内初「RPKI ROAパブリックキャッシュ情報配信」の試験提供をIMFとJPNICで開始
    - 全世界のROA情報（正しいPrefixとOriginAS情報）を気軽に取得することができ、AS内のBGP経路制御に活用
    - BGPルータが動作するインターネット環境からアクセス可能
  - RPKIに関するポータルサイト
    - IMF -> http://www.mfeed.ad.jp/rpki/
    - JPNIC -> https://www.nic.ad.jp/ja/rpki/

ROA: Route Origin Authentication

RPKIの普及状況

- 日本を含むアジア太平洋地域では、RPKIの普及がヨーロッパ地域等に比べて乏しい状況



RIPE

APNIC

登録されているROA数の推移
http://certification-stats.ripe.net

- 日本やアジア地域での普及促進が必要

IMF RPKI Project Page

MF RPKI Project　English

- ROAキャッシュ
- 技術情報
- 統計情報
- その他
- RPKIとは
- メンテナンス・障害情報
- 関連リンク
- 免責事項
- お問い合わせ

MF RPKIプロジェクト

インターネットにおけるBGP経路情報の交換では、AS運用者の設定ミスや悪意のある不正な経路広告によって、正しい宛先ネットワークに到達出来なくなる可能性があります。2008年に発生した、YouTubeが世界中から参照できなくなった事例のように、不正な経路情報がインターネット全体に蔓延し、世界中の通信に悪影響が及ぼされる事例も多く発生しています。

このような状況の中、インターネットマルチフィード社(MF)では、これまでJPNICや大手ルータベンダ各社等と連携し、インターネットの経路制御の信頼性向上を目指し、将来ISPの皆様が利用されるRPKI技術に関して、2012年よりROAキャッシュサーバの構築およびそれを参照するルータの動作検証を実施し、業界へフィードバックして参りました。

2014年10月1日より、日本のISPの皆様が今後RPKIの運用を本格化することを念頭に、ROAキャッシュサーバの運用を開始し、本格的にRPKI運用技術の習得およびインターネット全体の信頼性向上を目指し、より安心・安全なネットワーク環境を提供できるよう、インターネットの発展に貢献して参ります。

トピックス

2014/10/27 NEW!!

英語版ページをリリースしました。
Alcatelのルータ設定例を追加しました。

2014/10/01

MF RPKIプロジェクトページ(本サイト)を開設しました。
ROAキャッシュサーバの試験提供を開始しました。

いいね！ シェア 66　+1 2
ツイート 2

ツイート　フォローする

rpki_project @rpki_project　10月27日
English page has been released!
mfeed.ad.jp/rpki/en/index....
And added sample config for alcatel.

rpki_project @rpki_project　10月1日
インターネットルーティングにおけるRPKIの普及を目的として、ROAキャッシュサーバの提供を開始しました！
mfeed.ad.jp/rpki/index.html
開く

rpki_project @rpki_project　10月1日
URLは
mfeed.ad.jp/rpki/
です。

rpki_project @rpki_project　10月1日
インターネットルーティングにおけるRPKIの普及を目的として、ROAキャッシュサーバの提供を開始しました！
開く

さらに読み込む

@rpki_projectさん宛にツイートする

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)

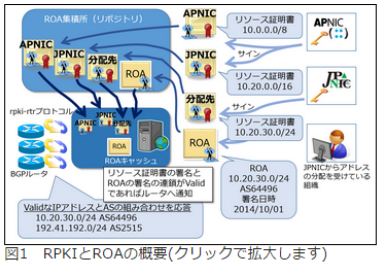


図1　RPKIとROAの概要(クリックで拡大します)

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。

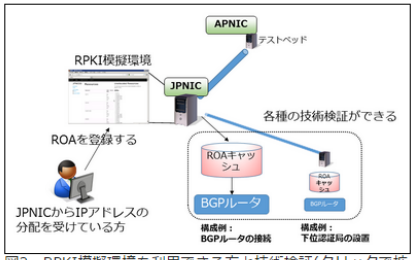


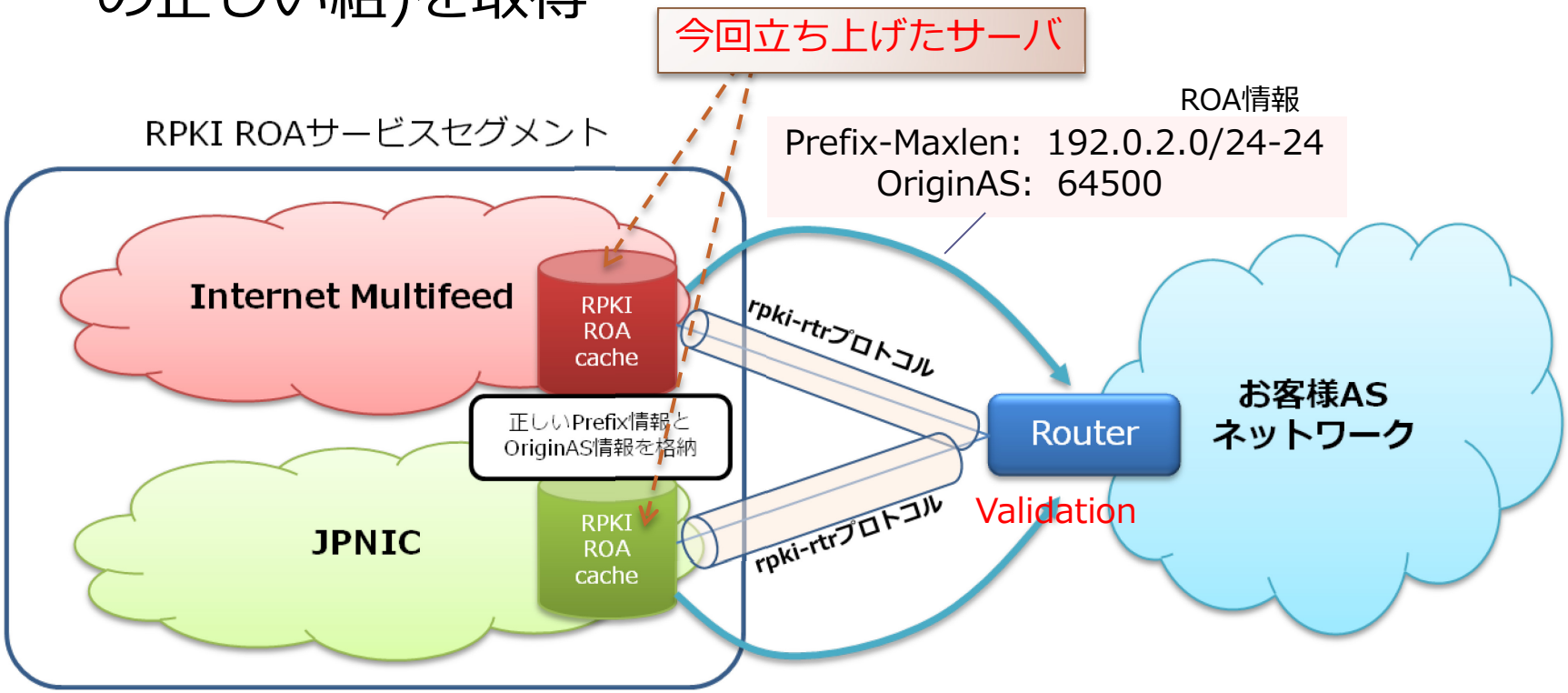
図2　RPKI模擬環境を利用できる方と技術検証(クリックで拡大します)

- JPNICとは
- IPアドレス
- インターネットの基礎
- ドメイン名
- インターネットガバナンス
- 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
- インターネットの歴史・統計
- ライブラリ
- JPNICトピックス一覧
- Web更新履歴一覧
- Q&A
- イベントカレンダー
- WHOIS

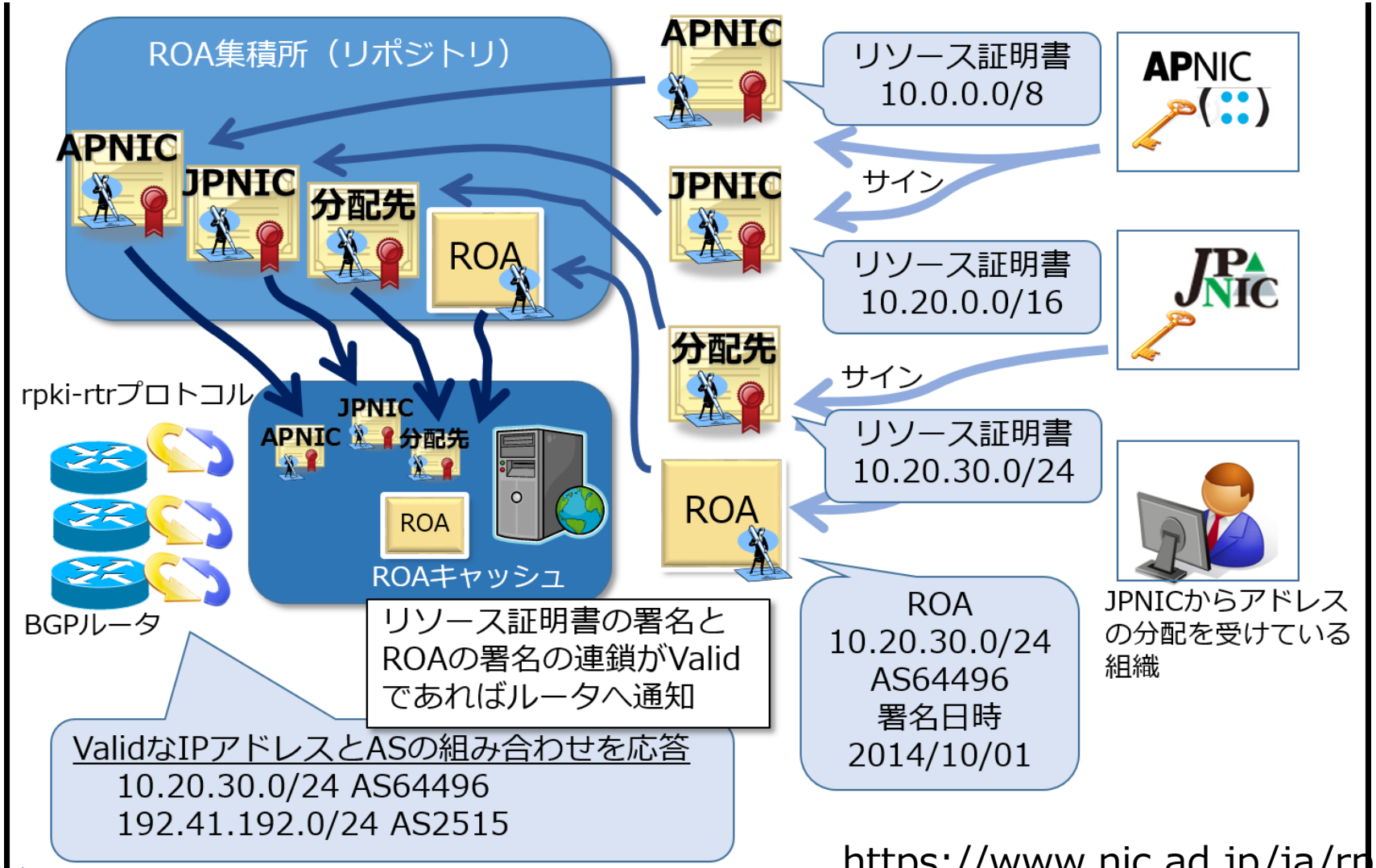
https://www.nic.ad.jp/ja/rpki/

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



RPKIとROAの概要



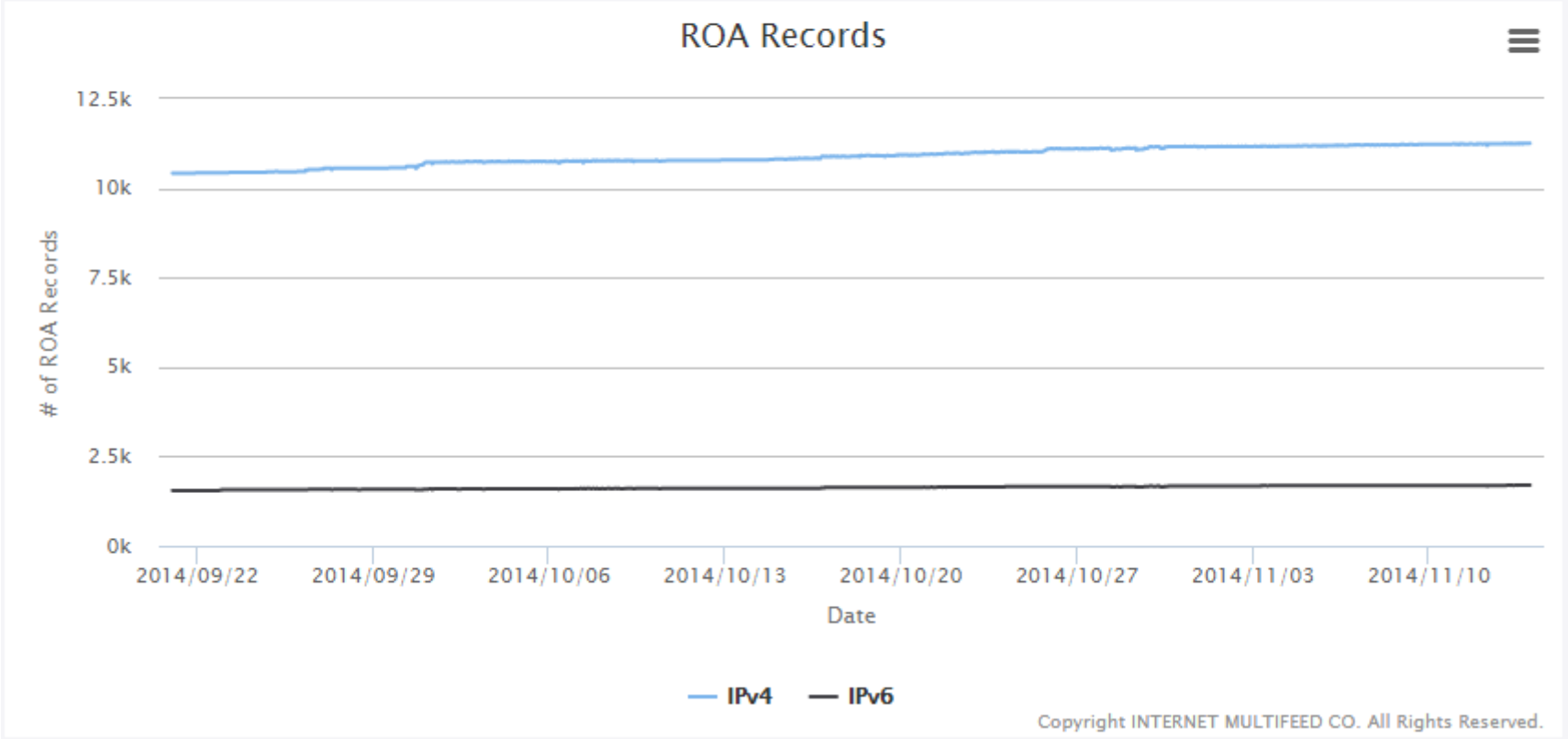
https://www.nic.ad.jp/ja/rpki/

ROAレコード数

RIPE地域、LACNIC地域の増加が牽引

ROAレコード数

ROAに登録されているレコード（Prefix, maxlenおよびAS番号の組み合わせ）数の推移です。（BGP sovc recordなどとも呼ばれます。）

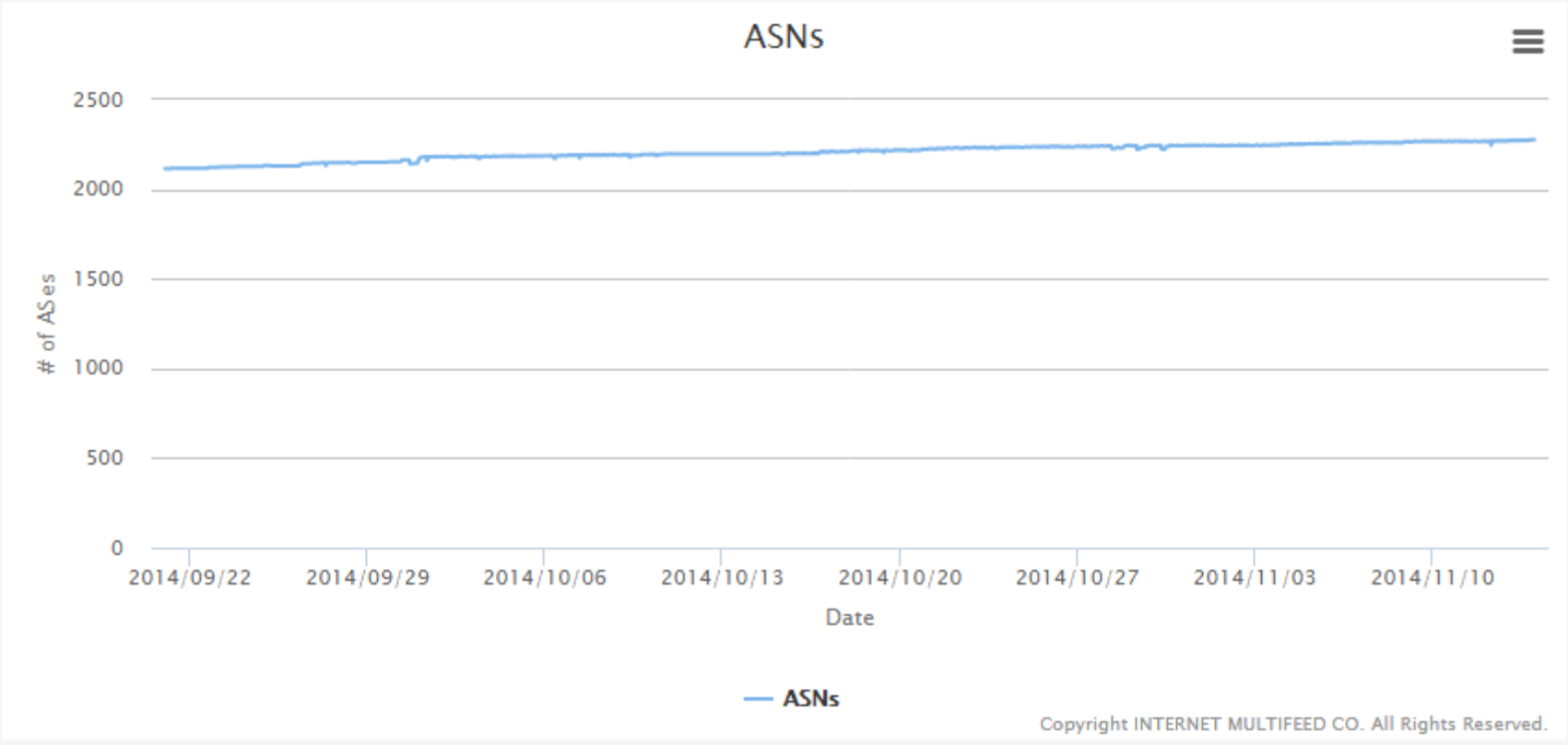


AS数

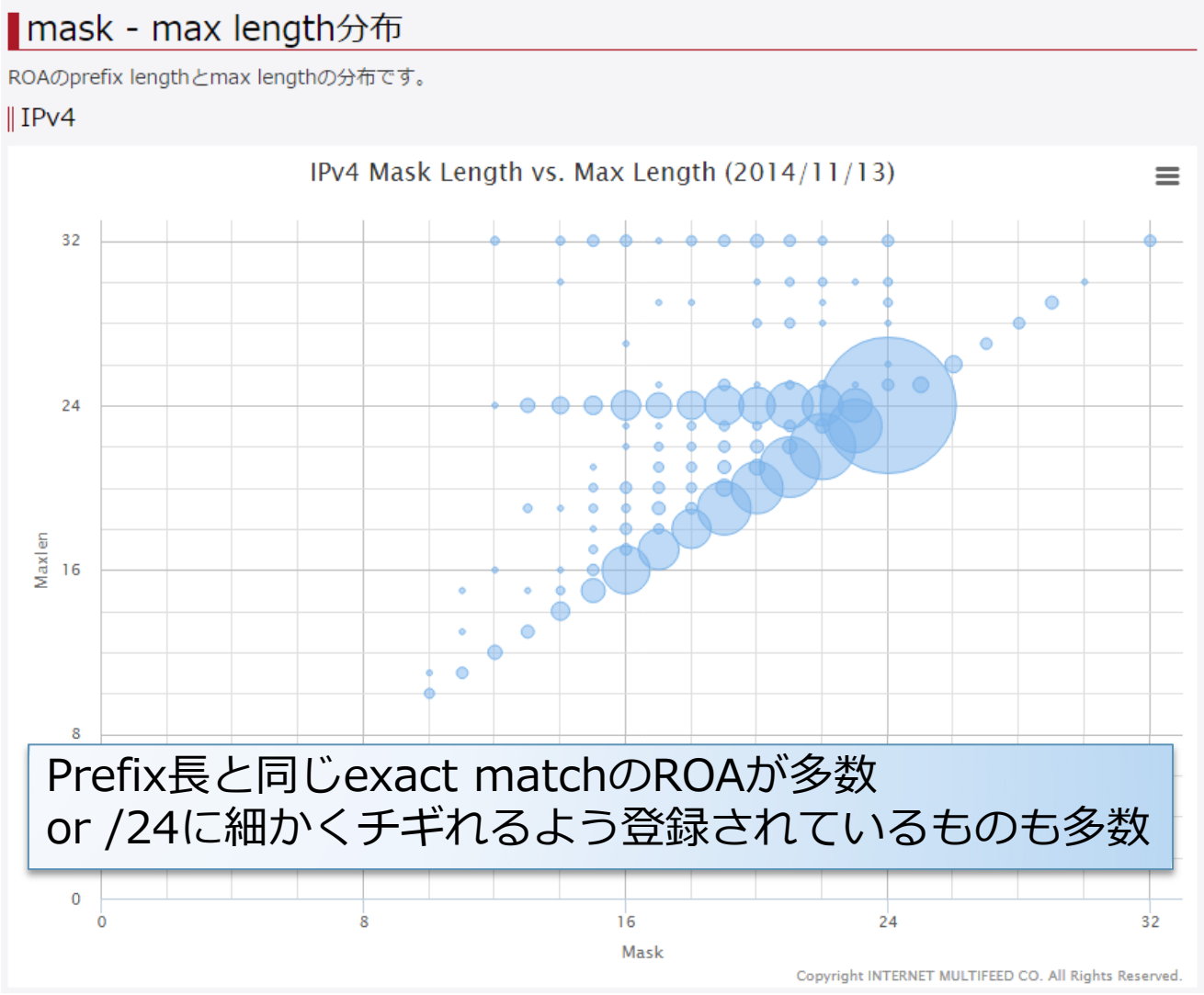
こちらもRIPE地域、LACNIC地域の増加が牽引

AS数

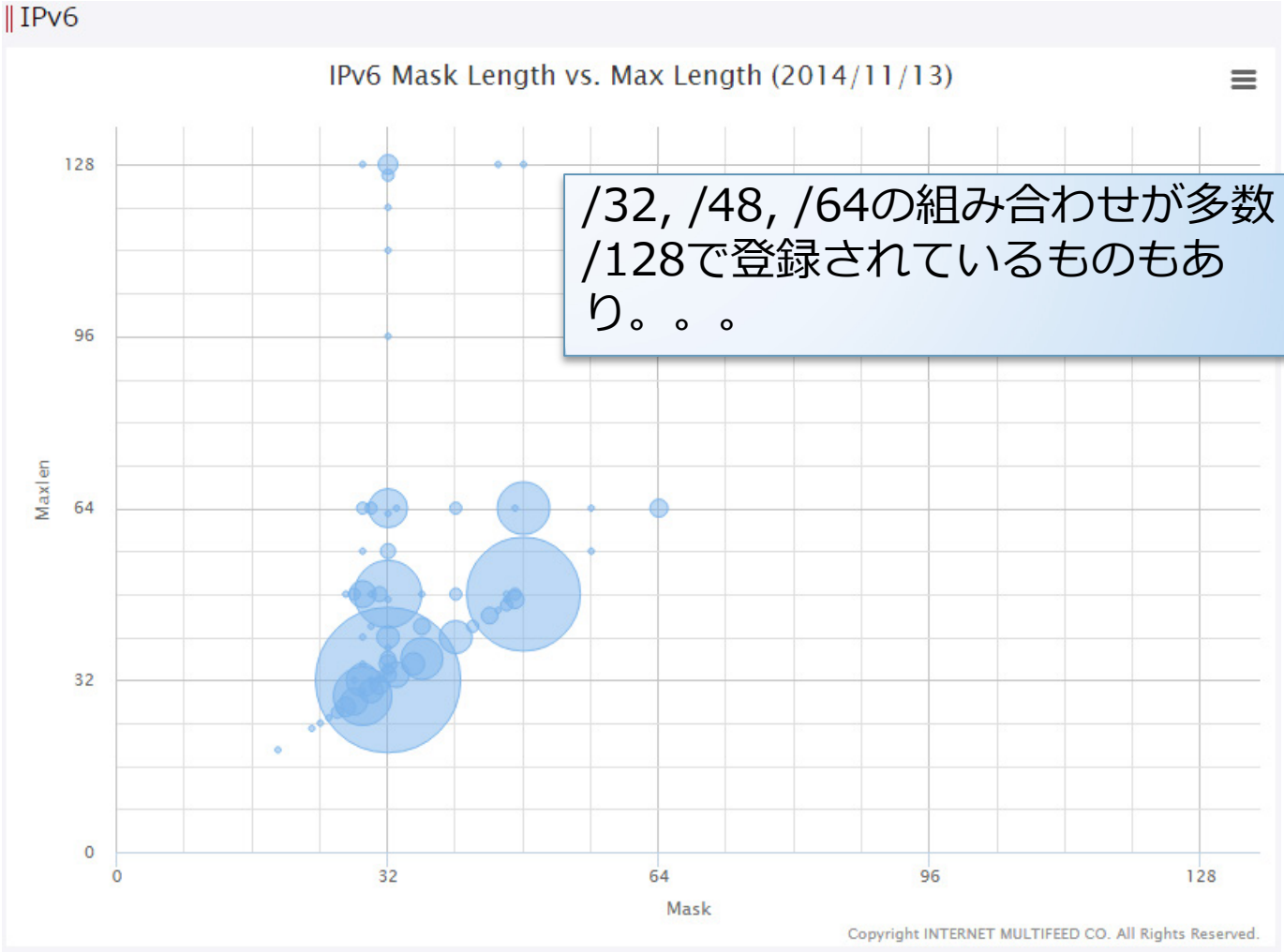
ROAに登録されているAS数の推移です。



IPv4 Prefixの maskとmax length 分布



IPv6 Prefixの maskとmax length 分布



RPKI普及に向けた課題

- ROAの情報がまだまだ不足
  - RPKIを活用して経路制御できるレベルではない
- ISPでのROAキャッシュ運用のハードルが高い
  - X509等の証明書関連技術知識が必要
  - 提供ツールがまだ発展途上の段階
- RPKIの重要性は理解できるが、社内で導入するにあたり、メリットを上司に説明できない。。
  - 世界中の人が登録しないと意味がない？？

- 最近はJPNICやIX事業者でのセミナーが幾つか開催

RPKIの課題(1)

- ARINのROA情報の取得／提供
  - ARINは、RPA(Relying Party Agreement)によって第三者への情報提供を禁止している
- RPKI-RTR(tcp:323) プロトコルのTLS encryptionがサポートされていない
  - ROAのような重要な情報に関するデータ転送には必須
  - CiscoやJuniperなどの大手ルータベンダも未サポート

RPKIの課題(2)

- Juniperルータの挙動
  - JUNOSでRPKI validation設定を有効にすると、tcp port:2222 が自動的にlistenされる
    - JUNOS内部で利用しているポートらしい…
      - SoftwareのversionやOSに依存する可能性あり
    - 外部から攻撃を受ける可能性があるので、FW等できちんとフィルタを適応する必要がある

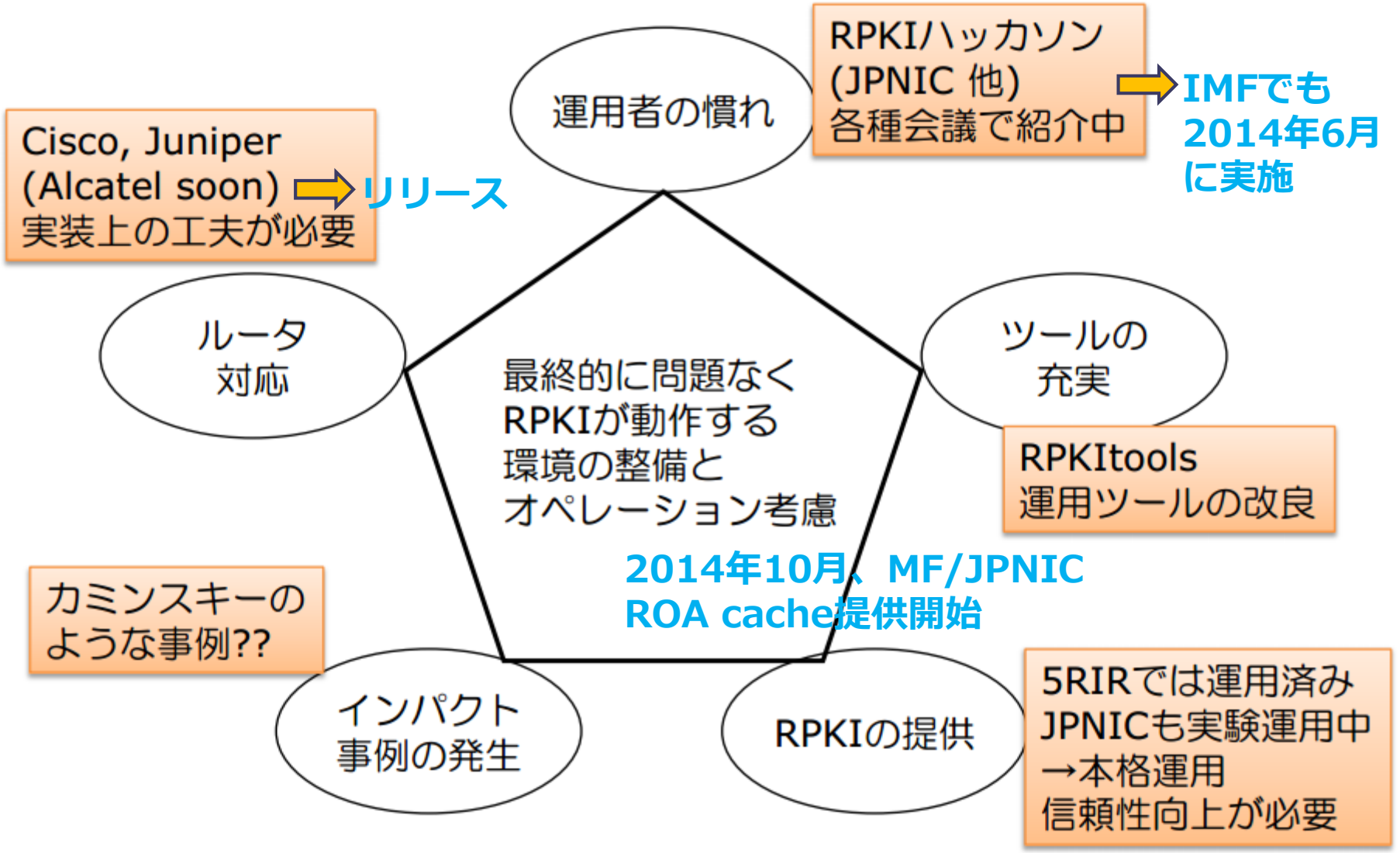
RPKIの課題(3)

- Cisco CSRの挙動
  - Show ip bgp/show ip bgp ipv6 unicast コマンドの結果が、何故か以下の条件の時に Validとなる（正しくは Not Found）
    1. 1つ以上のBGP経路を保有している
    2. 最初にはじめてRPKIをenableにする
    3. ROA cacheサーバより1つもROA情報を受信していない
  - 何らかのROAを受信すると正常に表示されるようになる
  - Cisco CSR/IOS-XE version 03.12.00Sで上記動作を確認
  - WA: ルータのreloadか、BGP resetか、RPKI設定前にBGPをshutdownしておく

RPKIの課題(4)

- 経路制御にどう適応するの？
  - まずはmarkingするところからはじめる
    - ROA cacheから情報を取得し自身のルータのBGP経路をvalidationし、判定結果をmarking
  - 不正な経路を叩き落すことが最終ゴールだが、経路制御への反映は慎重に
    - Invalidの経路はpriorityを低くするなど。ただしlonger-prefixを優先してしまうので悩ましい…

RPKI普及に関する要素と現状



http://www.ieice.org/~ia/archives/20130906-BGP-yoshida.pdf

Source: JPNIC岡田氏の講演資料を元に作成

内容

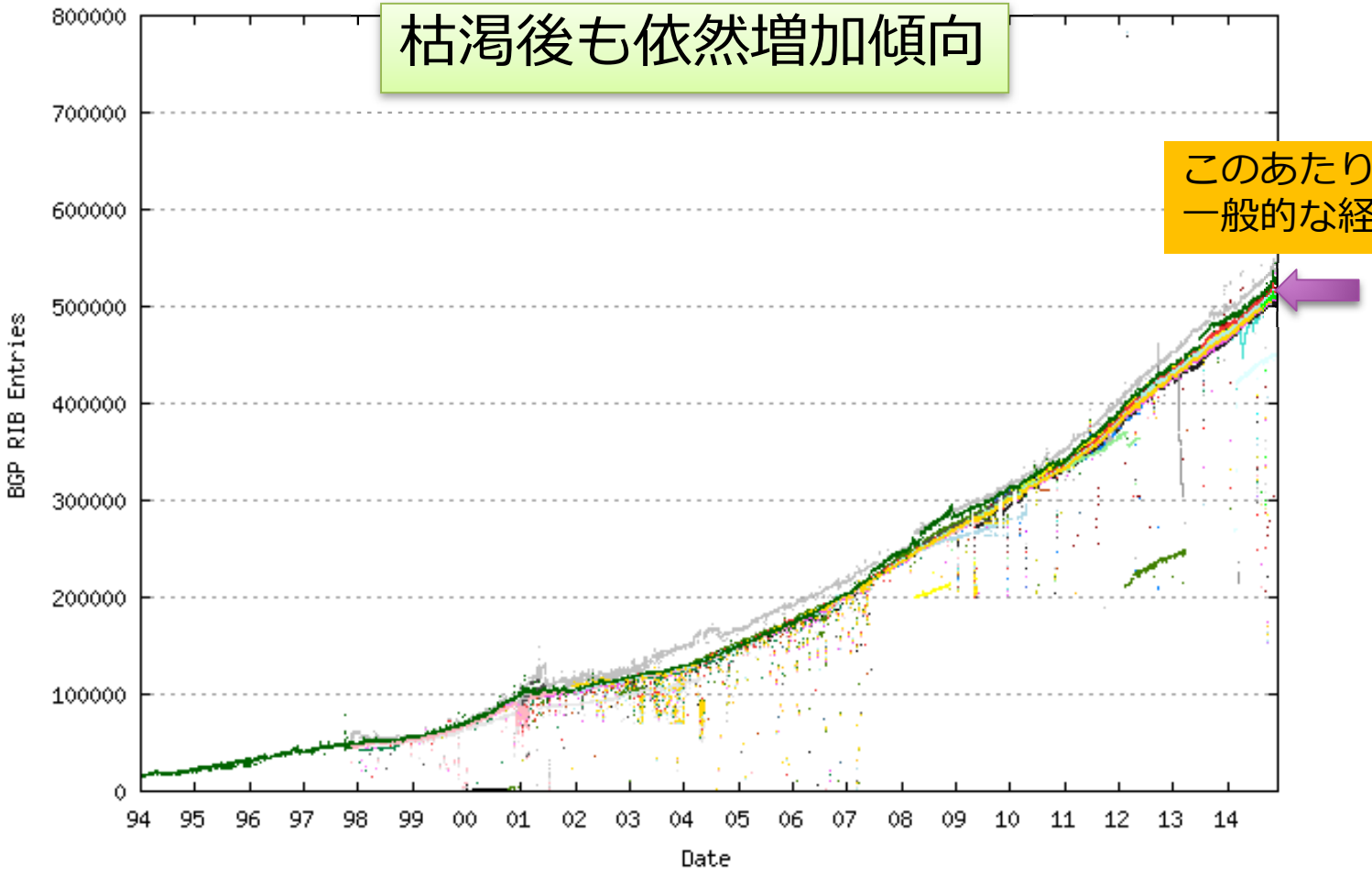
- routsec国際動向
- RPKI動向
- 軽く512K問題

IPv4フルルート512Kの壁

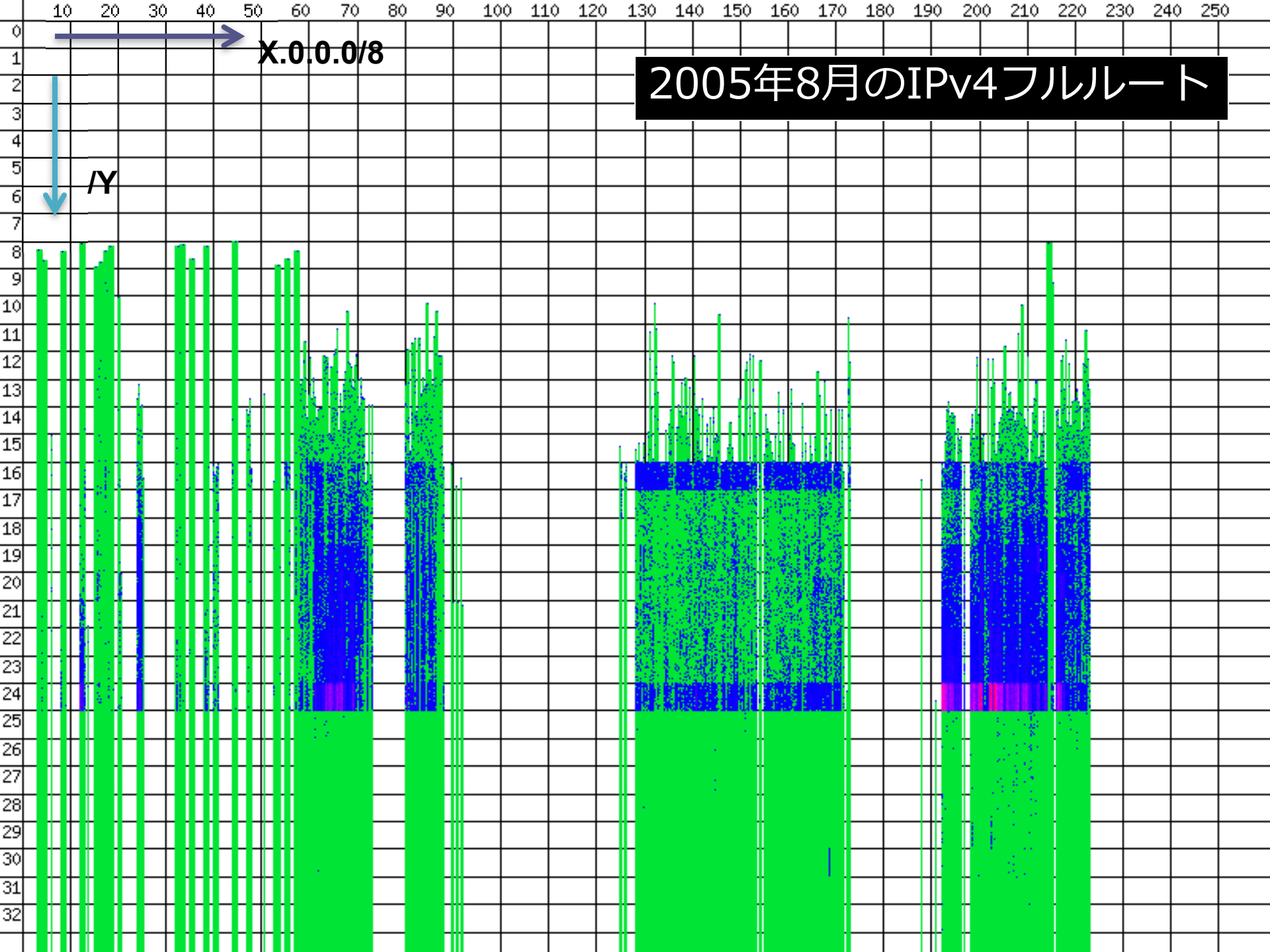
- JANOG等でも春先から注意喚起がされていた
- が、ばたばた512Kの壁にやられた人が散見
  - JPNAPでも複数の緊急メンテナンスを実施されているISPさんがいた
  - 192K, 224K等昔の頃よりは少なかった？
  - 内部BGP経路が大量に存在するISPでは600K前後

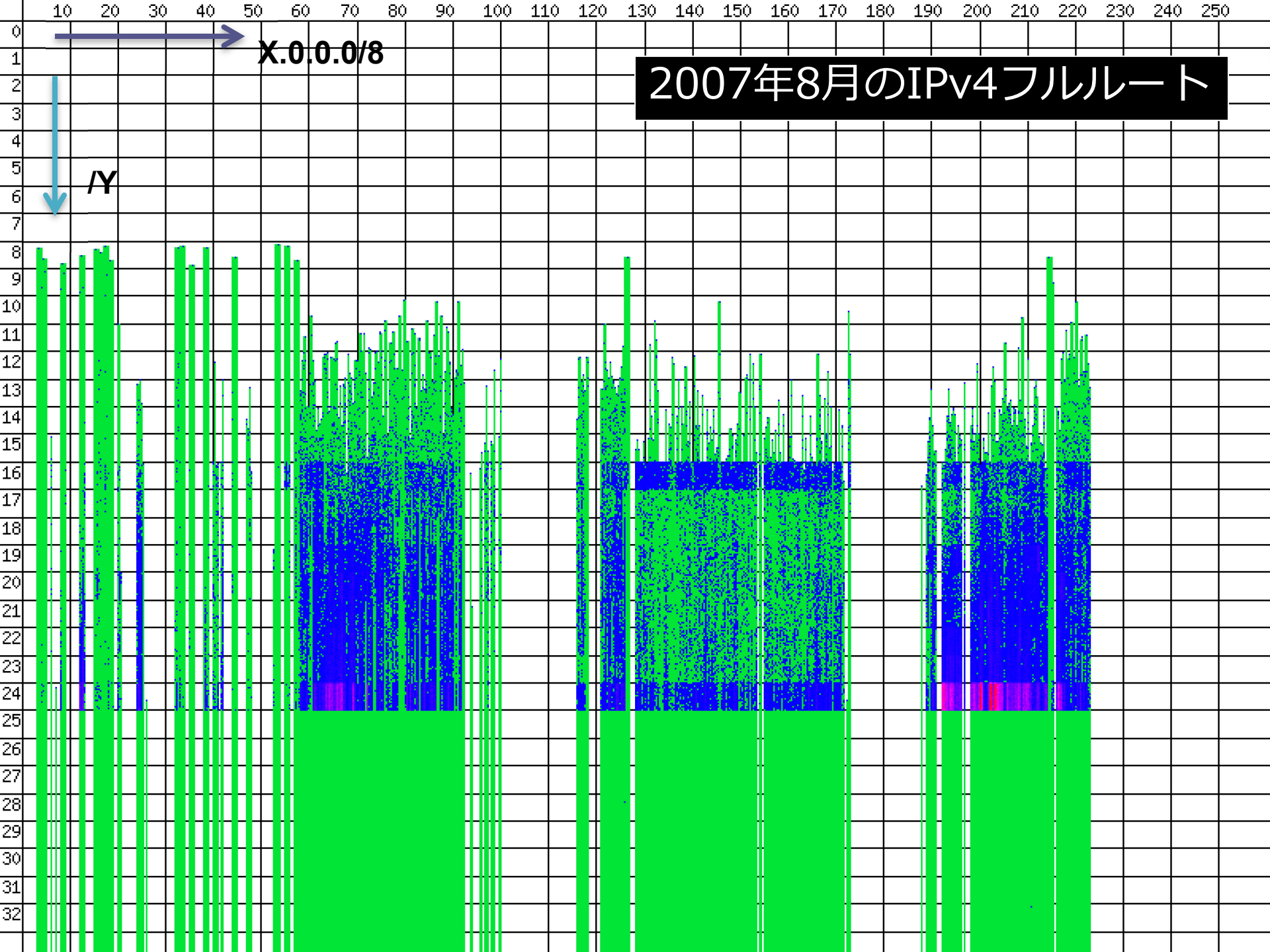
- フルルートが悪だといった風潮は間違い
- 適切にフルルートを活用し、インターネットのルーティングを行う必要がある

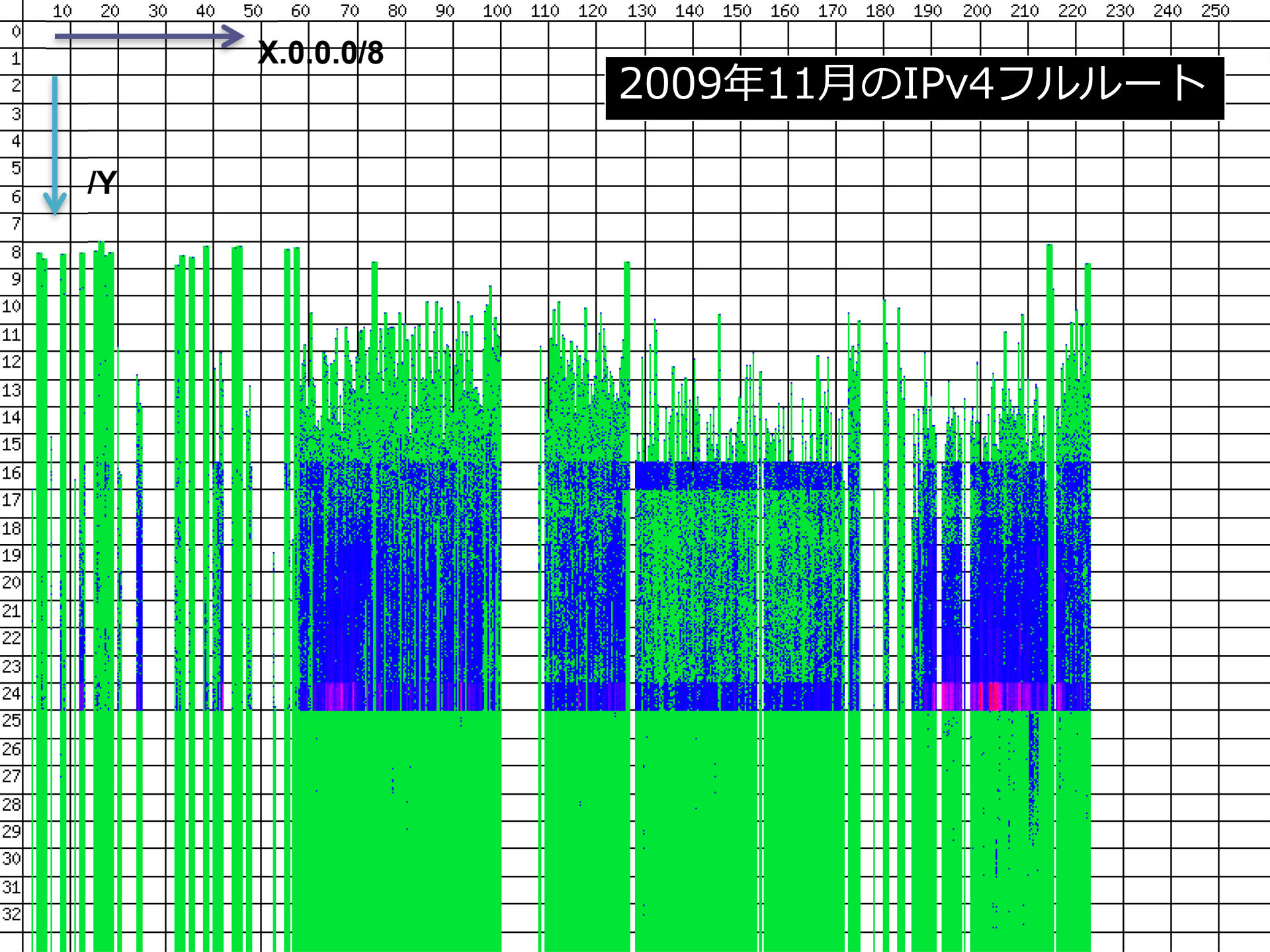
IPv4経路数の推移

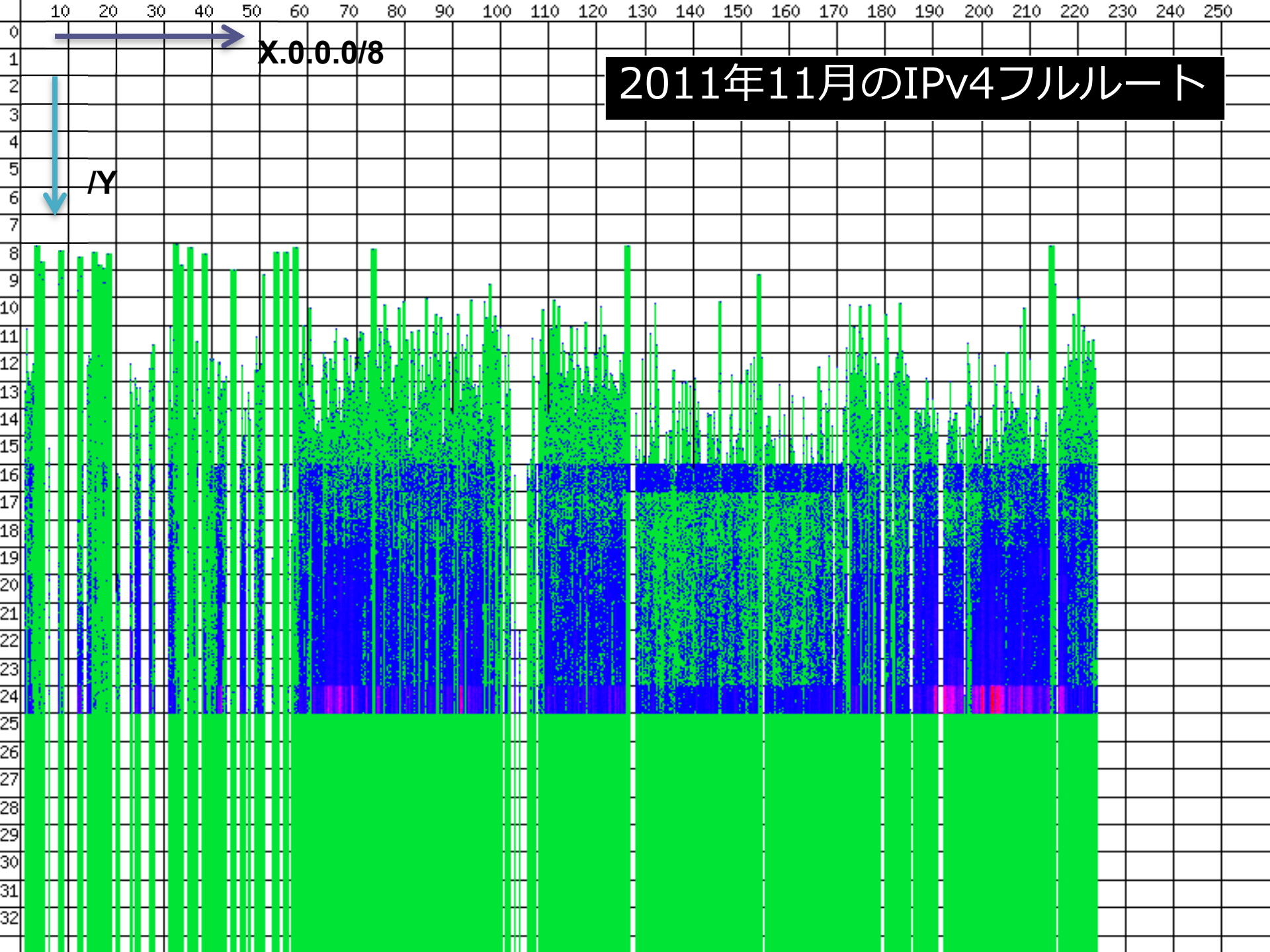


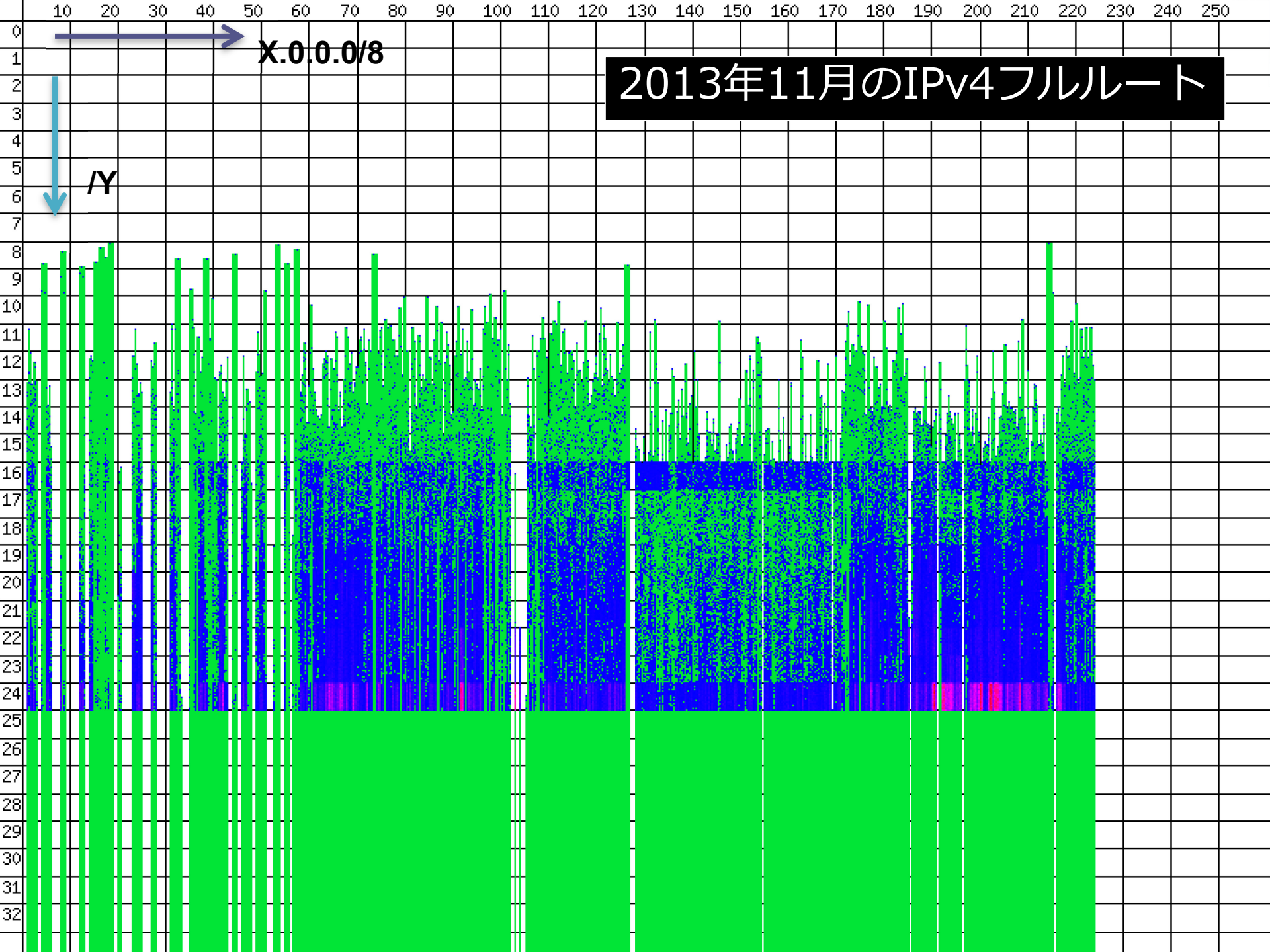
http://bgp.potaroo.net/

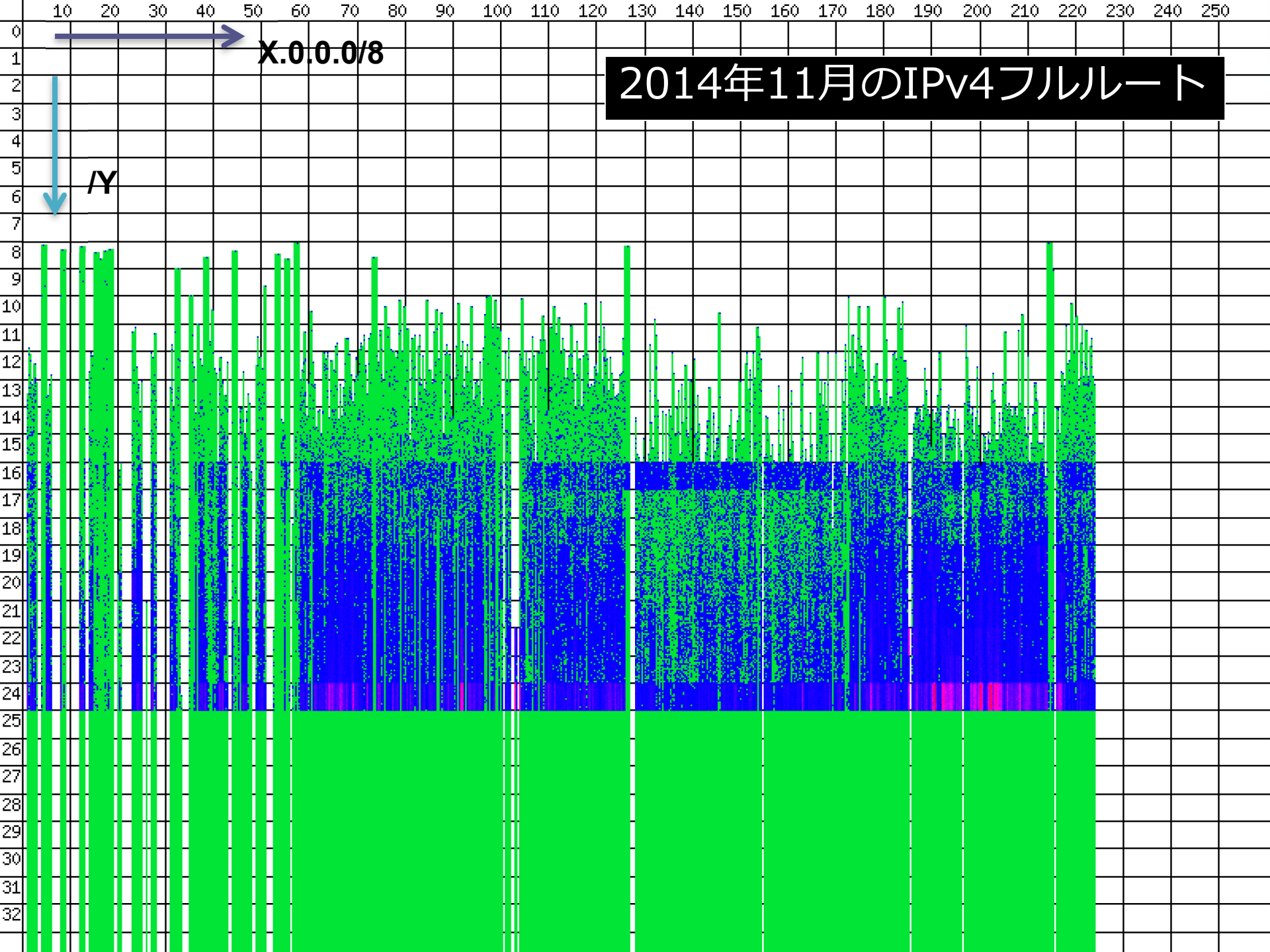

10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
X.0.0.0/8
/Y
2005年8月のIPv4フルルート


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

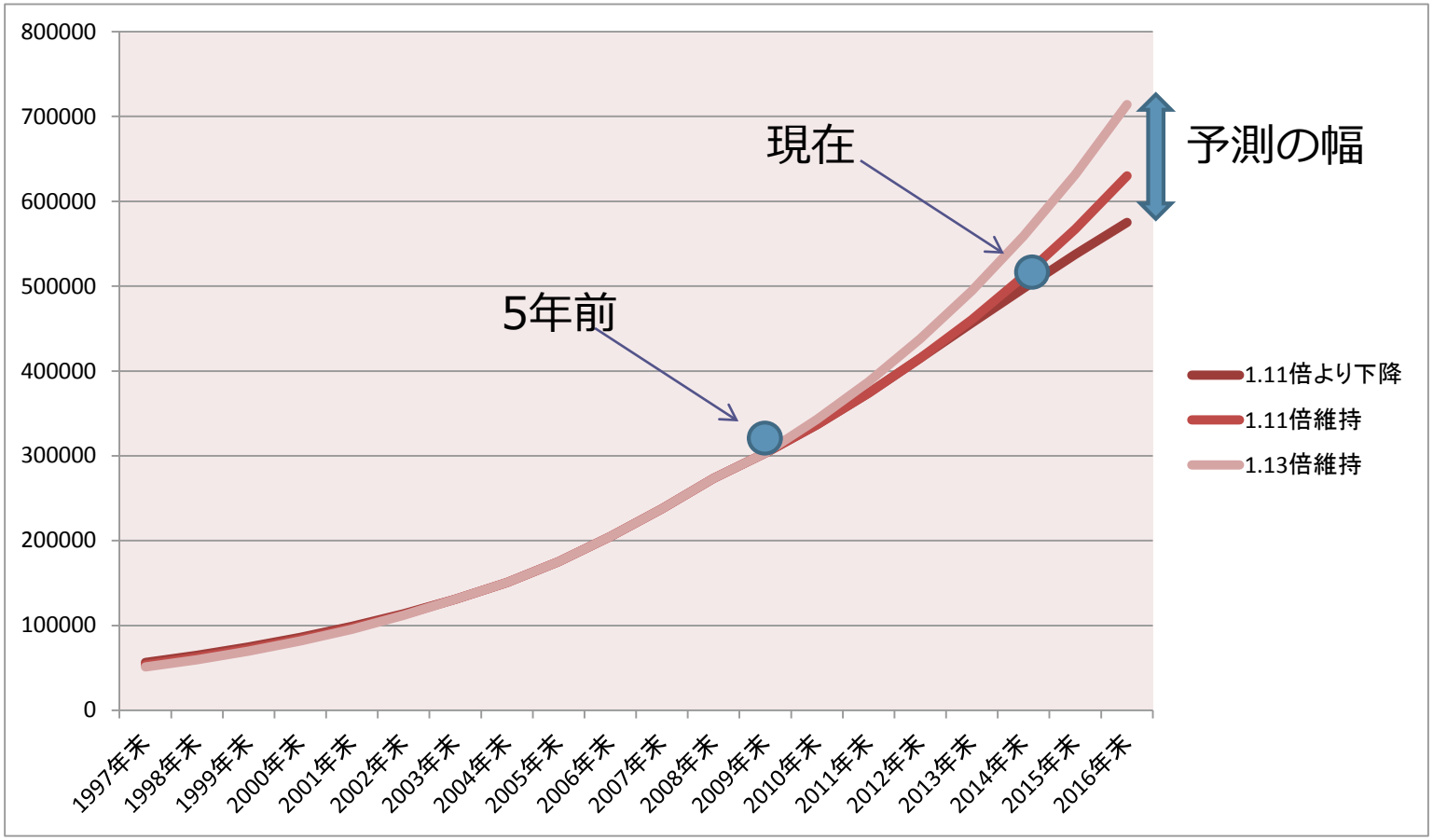

10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
X.0.0.0/8
/Y
2009年11月のIPv4フルルート


X.0.0.0/8
/Y
2011年11月のIPv4フルルート


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


10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
X.0.0.0/8
/Y
2014年11月のIPv4フルルート

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

今後の見通しと対応策

- 2,3年は現在の傾向に沿って増加し続けると推察される
- 対応策
  - 機器等の更改
  - フルルートが不要なドメインは経路削減を実施
    - ルーティングループが発生しないように注意が必要
- 利用しているルータ機器等の特性を把握しておく
- コミュニティの情報をきちんと得る
- IPv6の○○Kにも要注意

Brocade製品例

CAMプロファイル
–Xモジュール

X2モジュールではIPv4/IPv6共に概ね問題ない

Profile	IPv4	ipv6	MAC/ VPLS MAC	IPv4 VPN	Ipv4/L2 Inbound ACL	IPv6 Inbound ACL	Ipv4/L2 Outbound ACL	IPv6 Outbound ACL
Default Profile	512K	64K	128K	128K	48K	4K	48K	4K
IPv4 Profile	1M	0	32K	0	112K	0	64K	0
IPv6 Profile	64K	240K	32K	0	16K	24K	16K	12K
l2-metro Profile	256K	0	512K	0	64K	0	64K	0
mpls-l3vpn Profile	256K	0	32K	480K	64K	0	64K	0
mpls-vpls Profile	256K	0	512K	0	64K	0	64K	0
multi-service Profile	256K	32K	192K	256K	32K	8K	32K	8K
multi-service-2 Profile	384K	96K	128K	128K	48K	4K	48K	4K
mpls-vpn-vpls Profile	128K	0	224K	384K	48K	0	64K	0
ipv4-vpn Profile	320K	0	32K	448K	64K	0	64K	0
l2- metro-2 Profile	64K	0	608K	0	64K	0	64K	0
mpls-l3vpn-2 Profile	128K	0	32K	544K	64K	0	64K	0
mpls-vpls-2 Profile	128K	0	576K	0	64K	0	64K	0
ipv4-ipv6 Profile	320K	160K	32K	0	48K	20K	32K	8K
ipv4-ipv6-2 Profile	768K	64K	64K	0	64K	8K	48K	4K
ipv4-vpls Profile	320K	0	480K	0	64K	0	64K	0

ipv4-ipv6-2 Profile なら対処可。ただしIPv6の64Kの壁あり

Brocade製品例

CERシリーズは最大IPv4 150万経路までサポート可能

Feature	NetIron CES	NetIron CER	NetIron CER – RT	MLXe
IPv4 RIB	256K	10M	10M	10M
IPv4 FIB	32K	512K	1.5M	1M
IPv6 FIB	8K	128K	256K	240K
BGPピア	64	256	256	2000
VRF	16	128	128	2K
VLL	512	1536	1536	48K
VPLS	128	1K	1K	16K

Alaxala製品例

- AX8600R
  - Defaultの設定で対応済み

表3-8 router-1の経路系テーブルエントリ数(1/2)

パターン名	IPv4ユニキャスト経路	IPv4マルチキャスト経路	IPv6ユニキャスト経路	IPv6マルチキャスト経路
default	1015808	8000	425984	8000
ipv4-uni	1998848	0	0	0
ipv6-uni	32768	0	983040	0
ipv4-ipv6-uni	884736	0	557056	0

http://www.alaxala.com/jp/techinfo/archive/manual/AX8600R/HTML/12_4/CFGUIDE/0019.HTM#ID00066

- AX7800R, AX7700R
  - router-b2で対応は可（ただしIPv4に特化）

表3-12 PRU-B2, PRU-B2B, PRU-C2, PRU-D2およびPRU-D2Bのテーブルエントリの配分パターン

想定する利用形態		パターン名			
		router-b1	router-b2	router-b3	vpnrouter-d1
		ルータ IPv4を主に使用	ルータ IPv4特化	ルータ IPv6を主に使用	ルータ MPLSを使用
IPv4	ユニキャスト経路※	393,216 (384k)	1,048,576 (1024k)	262,144 (256k)	131,072 (128k)
	VPNユニキャスト経路※	−	−	−	262,144 (256k)
	マルチキャスト経路	8,192 (8k)	−	8,192 (8k)	−
	ARP	131,072 (128k)	131,072 (128k)	65,536 (64k)	32,768 (32k)
IPv6	ユニキャスト経路※	65,536 (64k)	−	131,072 (128k)	65,536 (64k)
	VPNユニキャスト経路※	−	−	−	−
	マルチキャスト経路	8,192 (8k)	−	8,192 (8k)	−
	NDP	32,768 (32k)	−	32,768 (32k)	32,768 (32k)

http://www.alaxala.com/jp/techinfo/archive/manual/AX7800R/HTML/10_10_/APGUIDE/0031.HTM

日立製品例

- GR4000
  - router-b2で対応は可（ただしIPv4に特化）

表 3-7　PRU-B，PRU-B2，PRU-B2B，PRU-C2，PRU-D2 および PRU-D2B のテーブルエントリの配分パターン

想定する利用形態		パターン名			
		router-b1	router-b2	router-b3	vpnrouter-d1
		ルータ IPv4 を主に使用	ルータ IPv4 特化	ルータ IPv6 を主に使用	ルータ MPLS を使用
IPv4	ユニキャスト 経路※	393,216 (384k)	1,048,576 (1024k)	262,144 (256k)	131,072 (128k)
	VPN ユニキャスト 経路※	−	−	−	262,144 (256k)
	マルチキャスト 経路	8,192 (8k)	−	8,192 (8k)	−
	ARP	131,072 (128k)	131,072 (128k)	65,536 (64k)	32,768 (32k)
IPv6	ユニキャスト 経路※	65,536 (64k)	−	131,072 (128k)	65,536 (64k)

http://www.hitachi.co.jp/Prod/comp/network/manual/router/gr4k/1010r1/PDF/APGUIDE/APGUIDE.PDF

他

- Cisco
  - http://blogs.cisco.com/sp/global-internet-routing-table-reaches-512k-milestone/
- Juniper（例）
  - Routing Engine: RE-850-1536-S
  - CFEB: FEB-M10i-M7i-S
    - RIB IPv4 capacity = 6M
    - FIB IPv4 capacity = 550K
    - RIB IPv6: 3M
    - FIB IPv6: 375K

まとめ

- 国際的にも様々なoutageが発生している
  - 近年のハイジャックは愉快犯ではなく、金銭目的で手法も巧妙で検出が難しい
- RPKIの普及
  - 日本で初のROA cacheサーバの提供
  - 本格展開
- IPv4経路増：512K問題
  - 対応が必要だった人もそこそこいた状況
  - 今後もしばらく経路増加が見込まれるため、継続的に個々のネットワークに応じた対応が必要