最近のルーティング動向
経路奉行Update

Telecom-ISAC Japan / KDDI
中野 達也

目次

1. 経路奉行って何？
2. 最近の経路奉行
3. ルーティング事象に関連した事例の紹介
4. その日が来た時のために

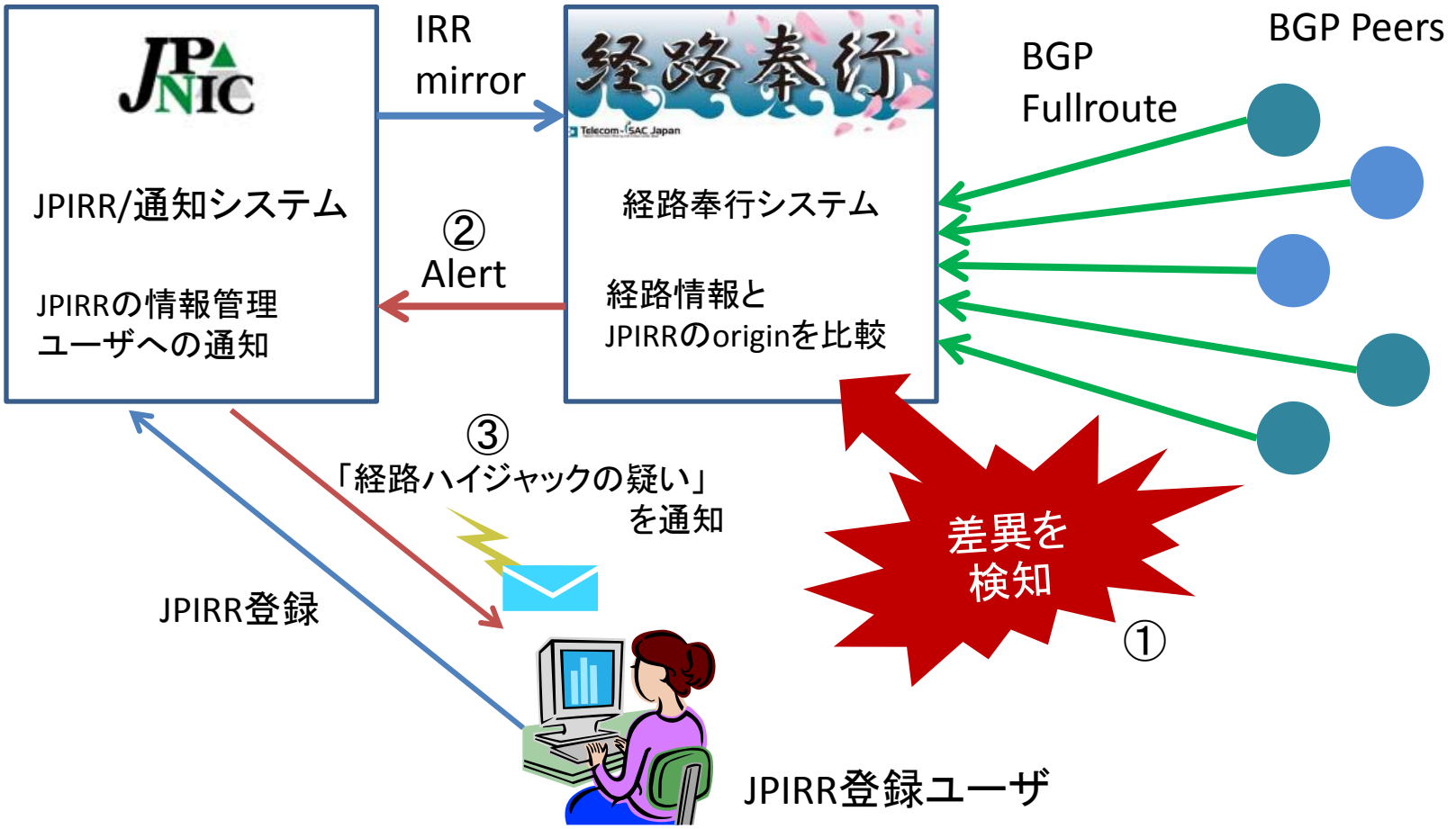
経路奉行って何?

経路奉行の仕事

- 経路情報(BGP Fullroute)を蓄積
- 経路情報をJPIRRの登録情報(origin AS)と比較する
  - 結果に差分があれば警告を出す

JPNICは警告を元に、JPIRR登録者(X-keiroに記載のアドレス)に「経路ハイジャックの疑い」があることを通知

経路奉行の仕事


JPNIC
JPIRR/通知システム
JPIRRの情報管理
ユーザへの通知
IRR
mirror
②
Alert
経路奉行
Telecom-ISAC Japan
経路奉行システム
経路情報と
JPIRRのoriginを比較
BGP Peers
BGP
Fullroute
差異を
検知
①
③
「経路ハイジャックの疑い」
を通知
JPIRR登録
JPIRR登録ユーザ

BGP Peersの内訳

- Telecom-ISAC BGP-WGメンバー(ASN順 14社18AS)
  - 株式会社インターネットイニシアティブ(AS2497)
  - 富士通株式会社(AS2510)
  - 株式会社エヌ・ティ・ティピー・シーコミュニケーションズ(AS2514)
  - KDDI株式会社(AS2516/AS4716)
  - NECビッグローブ株式会社(AS2518)
  - ソネットエンタテインメント株式会社(AS2527)
  - エヌ・ティ・ティ・コミュニケーションズ株式会社(AS2914/AS4713)
  - ヤフー株式会社(AS4694)
  - ソフトバンクテレコム株式会社(AS4725)
  - インターネットマルチフィード株式会社(AS7521)
  - 株式会社KDDI研究所(AS7667/AS131078)
  - エヌ・ティ・ティ・スマートコネクト株式会社(AS7671)
  - さくらインターネット株式会社(AS9370/AS9371)
  - ソフトバンクBB株式会社(AS17676)

なんで作った?

- 2005年ごろ、まずはBGP-WGメンバー向けのLookingGlassから始まった
- せっかく経路情報があるので活用したい
  → 経路の監視をしてみよう
- 名前を決めよう
  → 経路奉行にしよう

before JPIRR

- RADBを参照して(BGP-WGメンバー向け)試験
  → アラート大量発生 orz
  - 消し忘れ
  - 誤登録

使い物にならなかった ☹

after JPIRR

- JPIRRを参照して試験
  → なかなかいい感じ ☺
  - BGP-WGメンバーの経路 ＝ だいたいJPIRRにある
  - JPNICの努力により、精度も高め

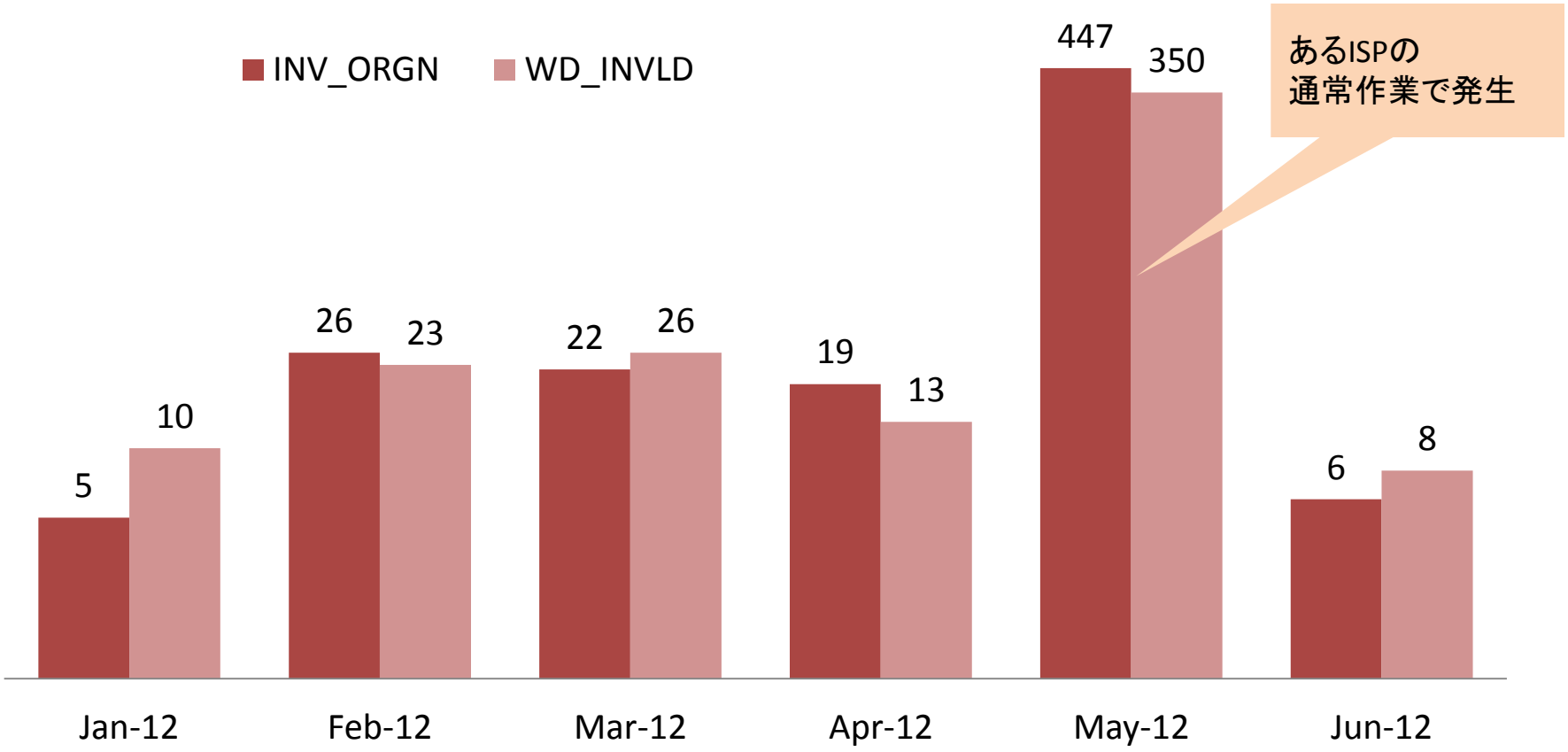
2008/5～ JPNICと協力して通知実験を行うことに
(そして現在に至る)

最近の経路奉行

1. 最近の検知・通知状況
2. 最近の経路奉行について

注意

最近の検知状況



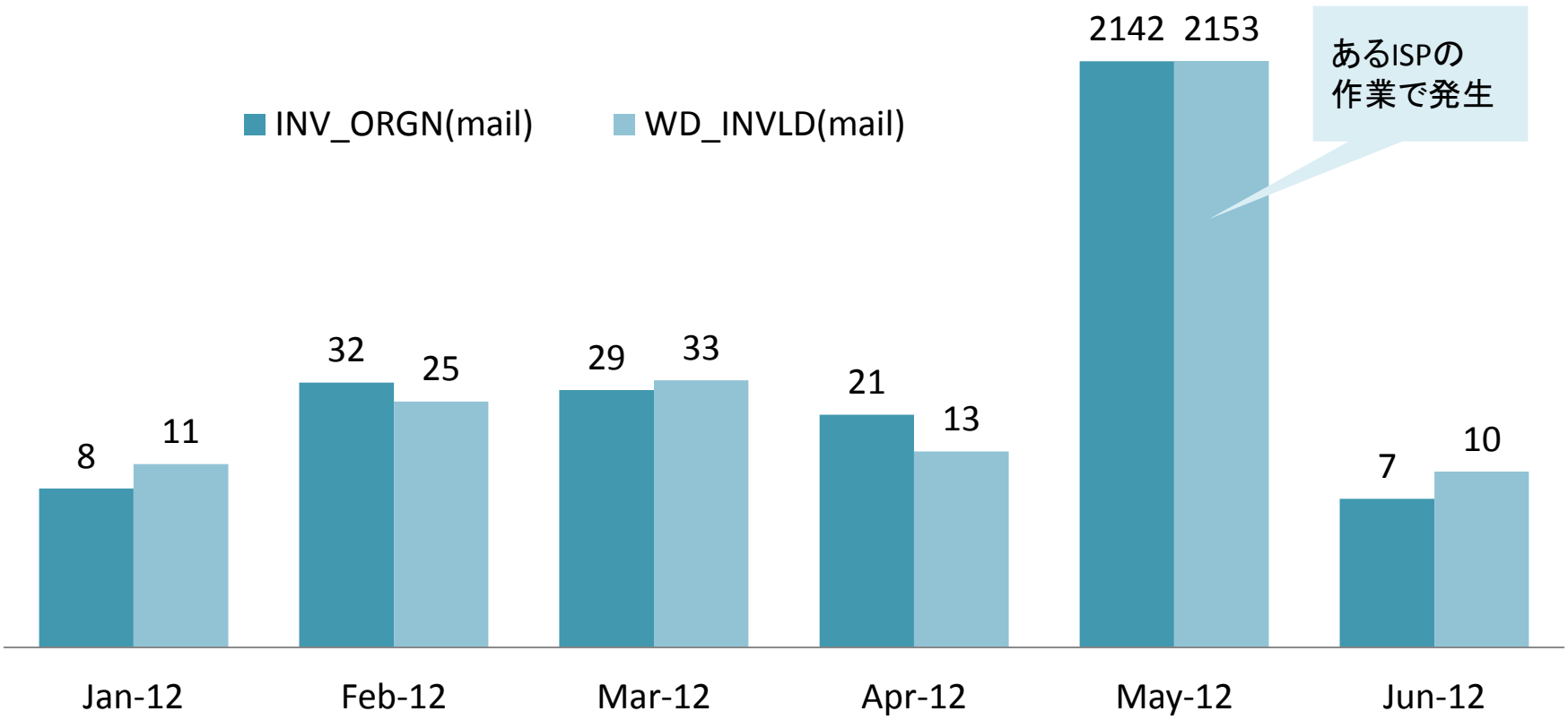
INV_ORGN : Invalid Origin / 経路情報に含まれるOriginとIRRに差異がある状態
WD_INVLD : Withdraw Invalid / INV_ORGNが解消された状態

考えられる検知原因

- 作業の過程で発生(not オペミス)
- ASをまたぐPrefixの移行(PI引っ越し等)
  - IRR更新前に移行すると、そうなる
- パンチングホール

- オペミスによる誤広報☹
- リアルな経路ハイジャック行為☹☹

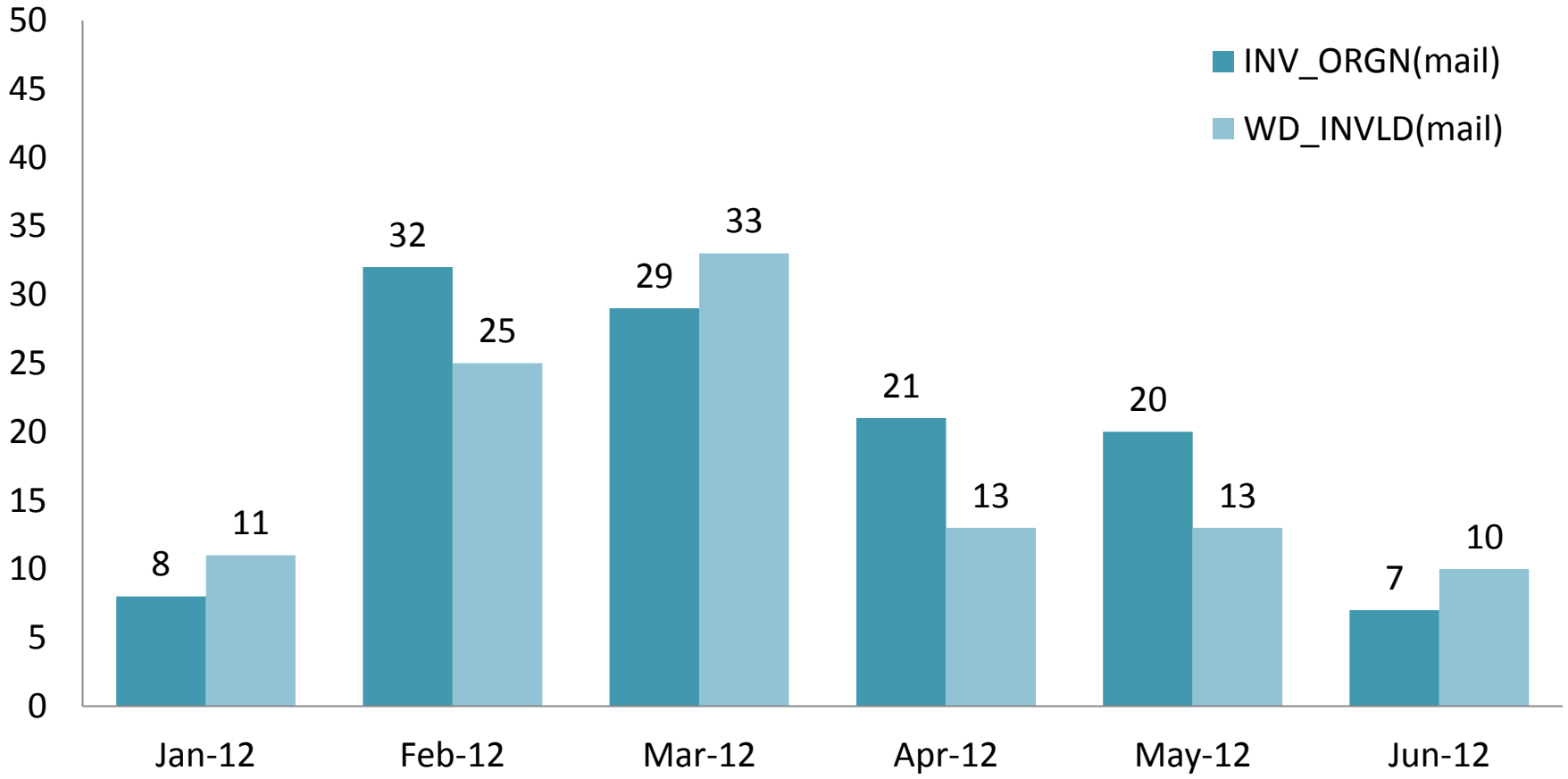
最近の通知状況
(メンバー向けmail送付数)



INV_ORGN : Invalid Origin / 経路情報に含まれるOriginとIRRに差異がある状態

WD_INVLD : Withdraw Invalid / INV_ORGNが解消された状態

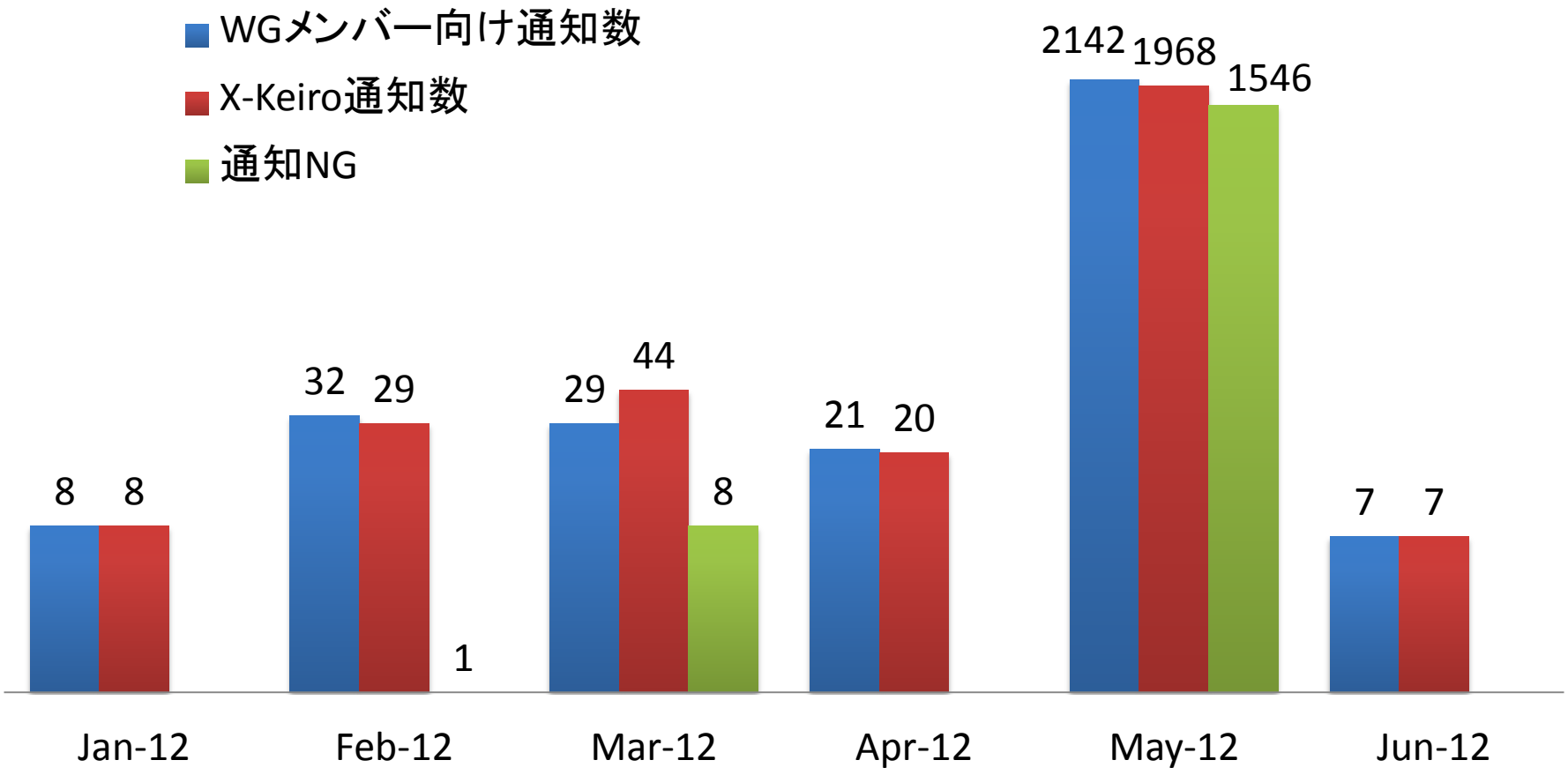
最近の通知状況
(メンバー向けmail送付数 – 作業分除く)



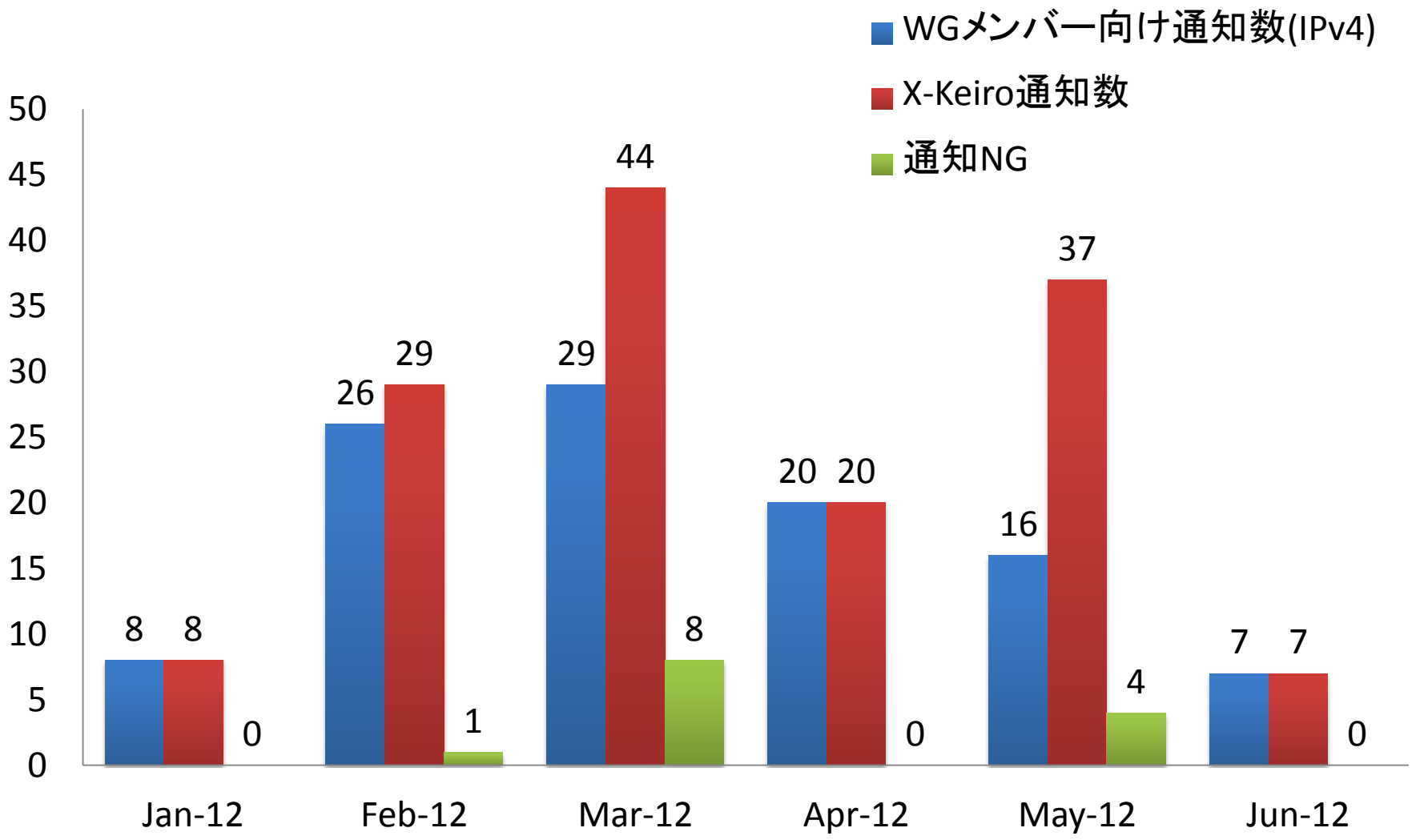
INV_ORGN : Invalid Origin / 経路情報に含まれるOriginとIRRに差異がある状態

WD_INVLD : Withdraw Invalid / INV_ORGNが解消された状態

最近の通知状況
(X-Keiro宛送付数)

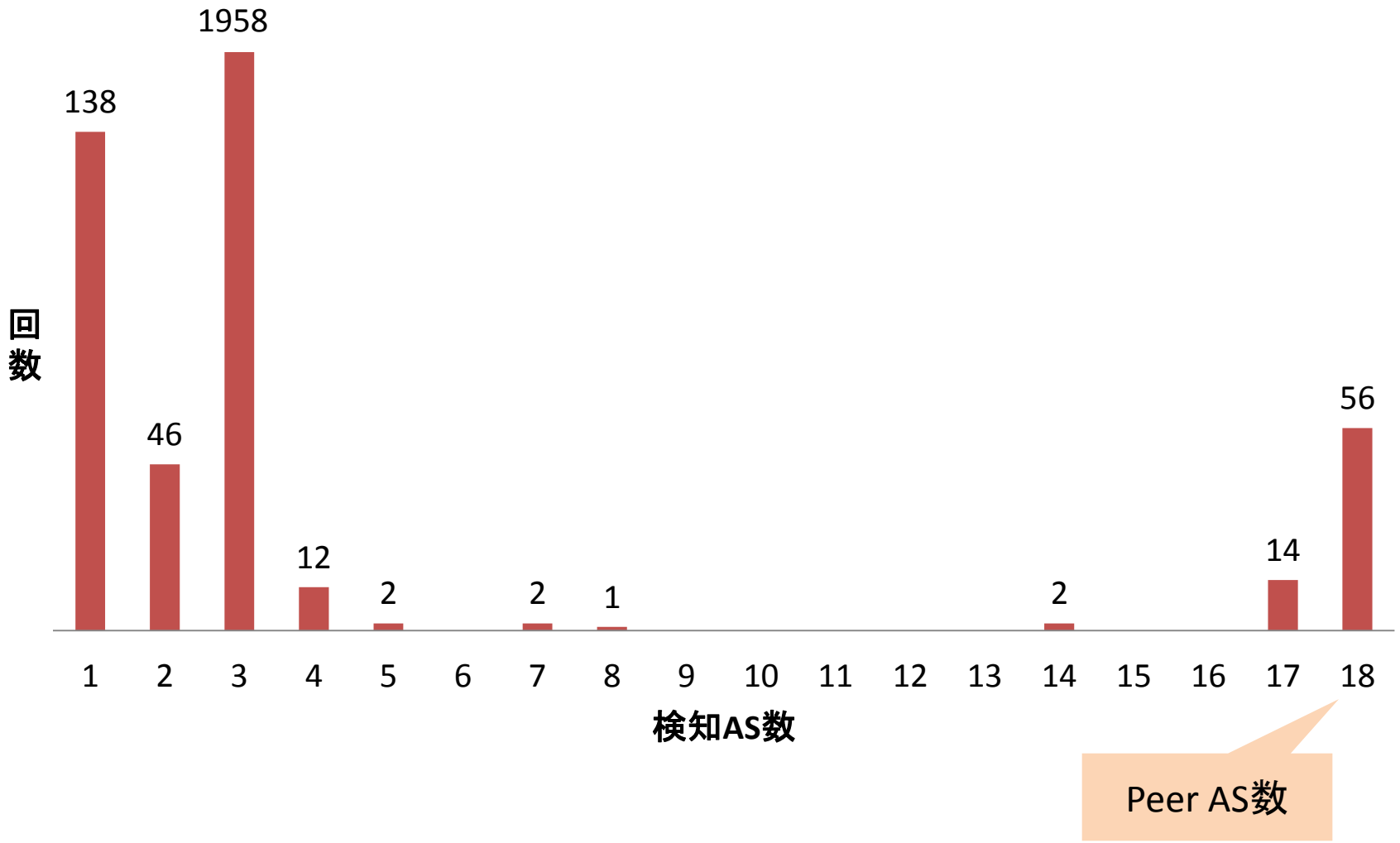


最近の通知状況
(X-Keiro宛送付数 – 作業分除く)



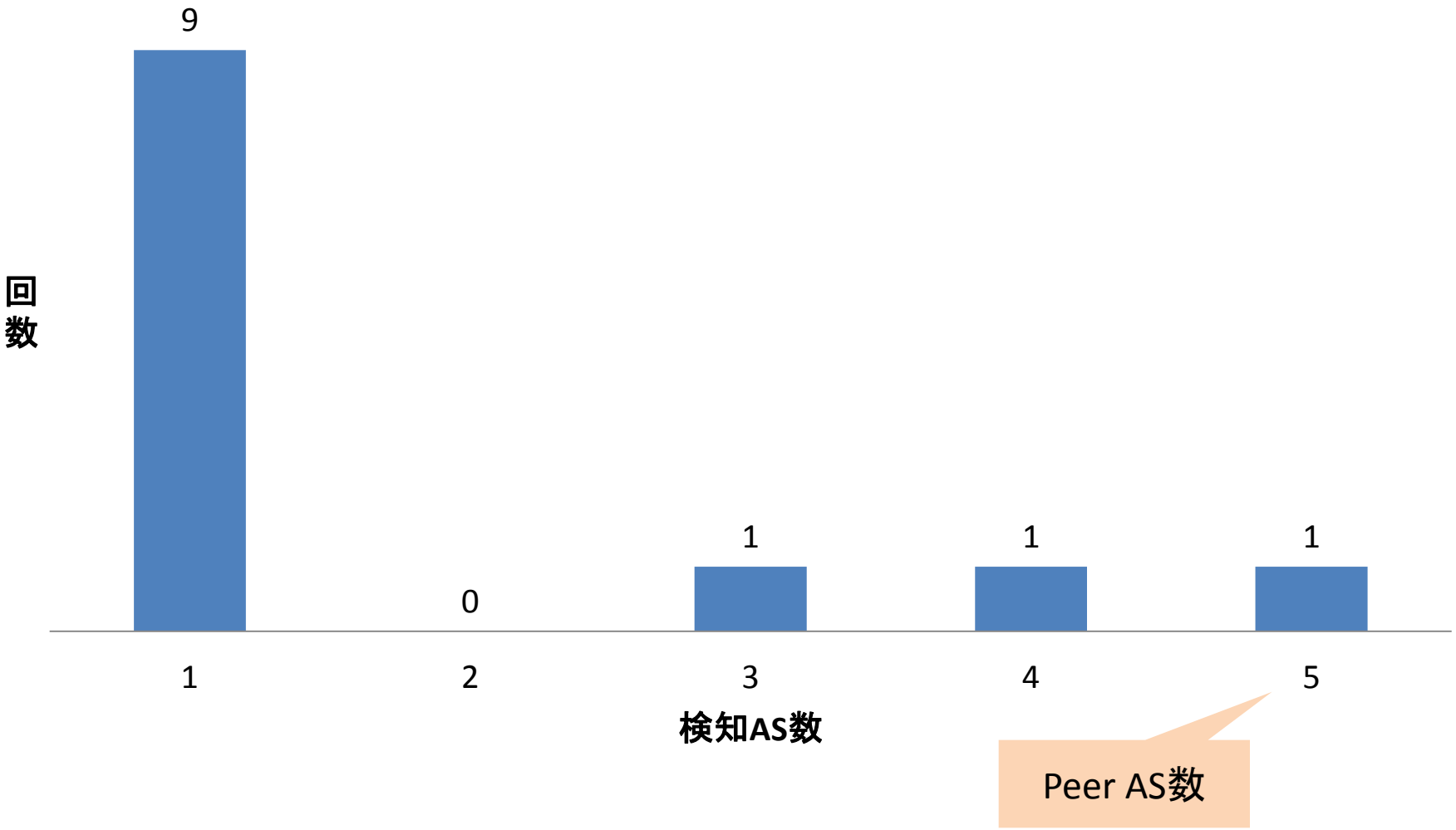
検知AS数の分布

(2012/01-06 IPv4)

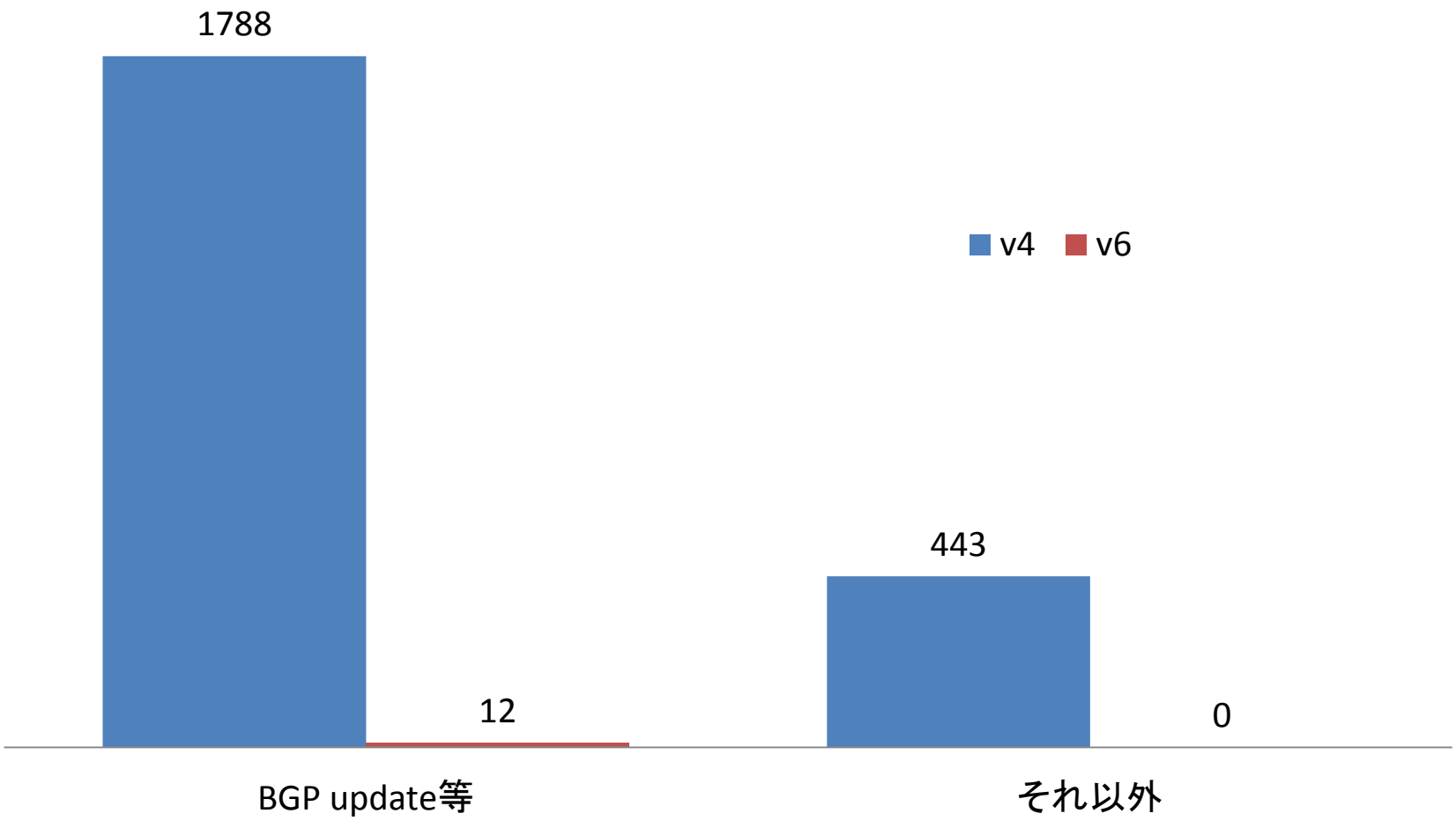


検知AS数の分布

(2012/01-06 IPv6)



回復要因別グラフ
(2012/01-06)



検知・通知状況についてのまとめ

- 作業等で大量にAlertが発生してしまうがある程度は仕方ない
  - 誤広報が検出できないよりはよい
- 正しい検知のためには正しいIRRが不可欠
  - X-Keiroの情報もあるとJPIRRに登録した方にも通知ができます

最近の経路奉行

1. 最近の検知・通知状況
2. 最近の経路奉行について

最近の経路奉行

今の経路奉行における問題

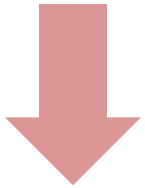
- 全ての機能が1台に集約
  → これが壊れると。。。
- bgpdがシングルスレッド
  → そろそろFullrouteが受けきれない

改善策を検討中(機能分散化等)

経路奉行を取り巻く事情

それぞれの思惑

- BGP-WGは分散化や実験的なことを行いたい
  → 当然、不安定になる可能性
- JPNIC(JPIRR)利用者は確実な通知を望んでいる
  → 求められるのは安定したシステム



双方が幸せになれる方法を検討中

経路奉行のまとめ

- 経路奉行は今日も安定して動いています
- 経路情報とJPIRRのupdateがあれば
  (きっと)今後も動き続けます
- さまざまな問題を抱えているのは事実なので
  改善をしていきます
- BGPSecが当たり前な世の中になるまでは活
  躍し続けます

ルーティング事象に関連した事例の紹介

1. typoでPrefixがハイジャックされた例
2. 狙われそうなPrefixがハイジャックされた例

typoでPrefixがハイジャックされた例　～時系列～

ある休日の昼下がり。。。

13:19　事象発生。Alertメール受領
調査開始

13:30　使用中のアドレスであることを確認
細かい経路広報の準備開始

13:45　誤広報元のASに停止をメールにて依頼

14:05　細かい経路を広報し、取り返す

15:14　誤広報が停止

typoでPrefixがハイジャックされた例 ～時系列～

16:09　誤広報元ASより対処した旨連絡

16:25　先方に了解したことと原因について問い合わせ

16:49　先方より回答。ベンダーが誤設定した

17:00　了解の旨返答

(誤広報の)発生から終了まで：1時間55分
被害を受けた時間：46分

本件で感じたこと

- typoが原因とはいえ、実際に被害は受けてしまう
  そしてそれは他人事ではない
  - 加害者にならないよう気をつけないと
- 先方は非常に真摯に対応してくれた
  - ここはお国柄がよくあらわれる印象
- 対応手順の確立が早期解消につながると感じた

ルーティング事象に関連した事例の紹介

1. とあるPrefixがハイジャックされた例
2. 狙われそうなPrefixがハイジャックされた例

狙われやすそうなアドレス (XXX.XXX.XXX.0/24)がやられた例

飲み会を夜に控えた夕方のこと。。。

16:38　事象発生。Alertメール来ない(経路奉行。。。)
BGPMONからメールが来てた
(BGPMONは担当者のみ受信していた)

18時頃　担当者がBGPMONのメールに気づき慌てる
幸か不幸か、アドレスはまだ使われていなかった

BGP mon

19:15　誤広報元ASにメールで問い合わせ
→ 複数宛先に送ったが、大半がunknownで返ってきた

19:44　誤広報元の「上位AS」にメールで問い合わせ

20時頃　誤広報が停止

狙われやすそうなアドレス (XXX.XXX.XXX.0/24)がやられた例

HURRICANE ELECTRIC
INTERNET SERVICES

Looking Glass

Welcome to Hurricane Electric's Network Looking Glass. The information provided by and the support of this service are on a best effort basis. These are some of our routers at core locations within our network. We also operate a public route server accessible via telnet at route-server.he.net.

Show options

core1.fmt1.he.net> show ip bgp routes detail 1[redacted].0/24

Matching Routes	3
Status Codes	**A** - Aggregate **B** - Best **b** - Not Install Best **C** - Confederation eBGP **D** - Damped **E** - eBGP **H** - History **I** - iBGP **L** - Local **M** - Multipath **m** - Not Installed Multipath **S** - Suppressed **F** - Filtered **s** - Stale

Status	Network	Next Hop	Metric	LocPrf	Weight	Path	Origin
BI	[redacted].0/24	195.66.224.212	1486	100	0	2[redacted]8	IGP
I	[redacted].0/24	195.69.146.177	1575	100	0	2[redacted]8	IGP
I	[redacted].0/24	80.81.194.117	1585	100	0	2[redacted]8	IGP
Last Update	2h57m47s ago (1 path installed)						

Entry cached for another 59 seconds.

狙われやすそうなアドレス (XXX.XXX.XXX.0/24)がやられた例

- Alertメールが飛ばなかった理由
  - 経路奉行のシステムトラブル
- 気づいた点、感じたこと
  - 実は、メールがトリガーとなって対応してくれたかはわからない
  - 経路奉行の信頼性が上がると幸せ
  - けど、経路奉行だけに頼らない体制の構築も

事例を踏まえ、実際にやったこと

- 手順の策定及び文書化
  - 文書化といってもWikiですが…
  - メールテンプレートの作成も
- 支援ツールの作成
  (簡単なスクリプト。以下を一度に実行)
  - JPIRR/RADBへのwhois
  - 複数のホスト(含むLookingGlass)で traceroute/show ip bgp

その日が来た時のために

備えておきましょう(1)

- 検知できる/してもらえる体制づくり
  - 何かあった時にわかるように
    - IRR(JPIRR/RADB)の登録
    - X-Keiroをメンテナー/Routeオブジェクトに
  - 経路奉行以外のシステムへの登録も
    - BGPMON
    - ISAlarm

備えておきましょう(2)

- 注意してもらえる体制づくり
  - やってしまった時に教えてもらえるように
    - whois情報のアップデート
    - PeeringDBの登録・更新
- 調べるためのノウハウ作りも
  - LookingGlassやtraceroute.org
    - 自社網からshow ip bgpしても正しい答えは出ないかも
    - 第三者的視点としてLookingGlassも使ってみましょう

備えておきましょう(3)

- 簡単でもいいので対応手順をまとめる
  - やられた時のことを考える
  - やってしまった時のことも考える

でも、何より重要なのは
これらのことを継続して行うこと！

参考URL

- 「経路ハイジャック情報通知実験」開始のお知らせ
  http://www.nic.ad.jp/ja/topics/2008/20080521-02.html
- 「経路ハイジャックが疑われる状態発生時の対応について」
  http://www.nic.ad.jp/ja/ip/irr/counter-hi-jack.html
- BGPMON
  https://bgpmon.net/
- RIPE ISAlarm
  https://www.ripe.net/is/account/login
- PeeringDB
  https://www.peeringdb.com/

ご清聴ありがとうございました