ROVデプロイ状況調査

2020/11/27 InternetWeek2020

C45 知って楽しむルーティングセキュリティ

渡辺　英一郎 / NTTコミュニケーションズ株式会社

背景

インターネットルーティングにおいて、経路ハイジャック事象などの経路異常の防御策としてRPKI (Resource Public Key Infrastructure)の導入が進んでいます。

特に、昨年くらいから、欧米中心に大規模ISPやIXにおいて、このRPKIを用いて、”invalid”と判定されたBGP経路を破棄(reject)するROV(Route Origin Validation)の実装報告がされ始めています。

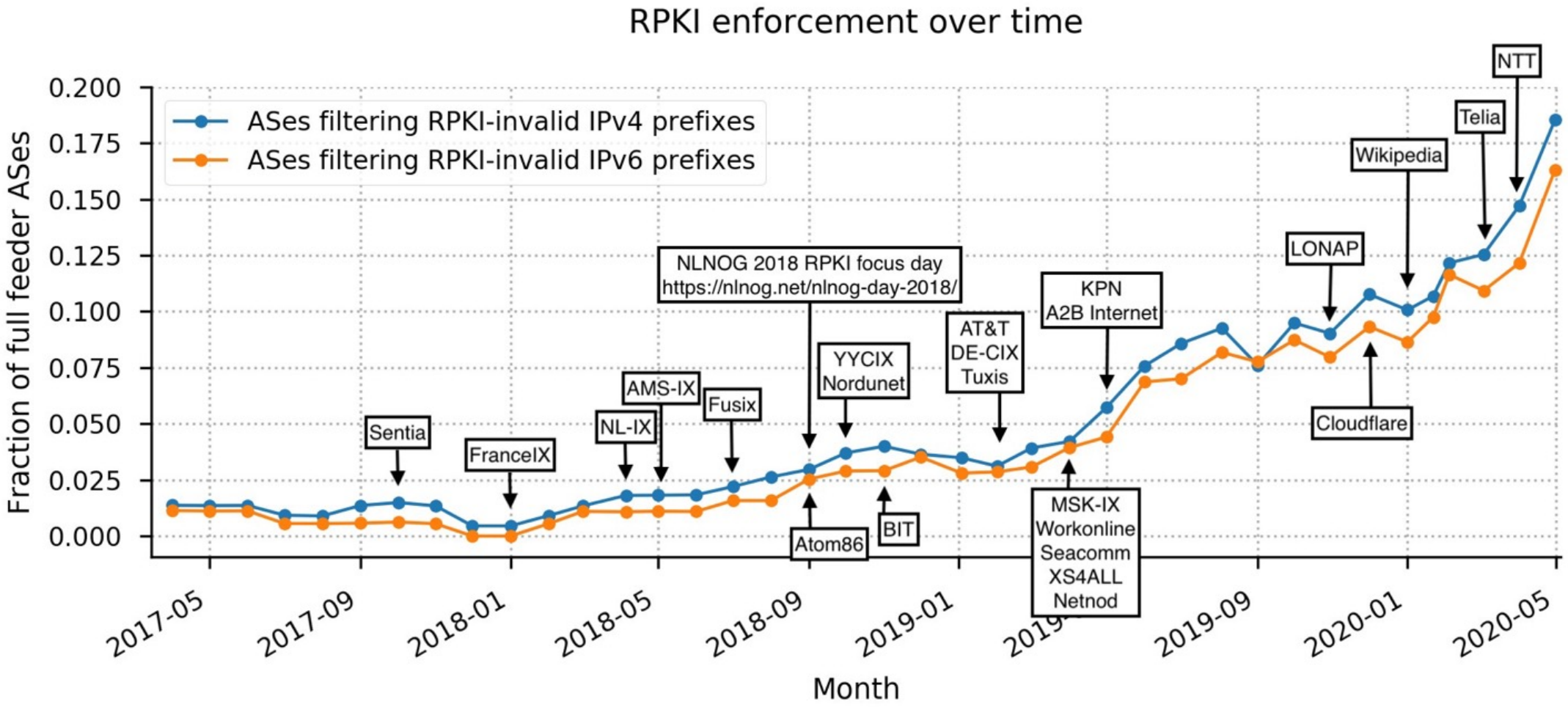
私の発表内容

私のパートでは、国内外でのROVの実装報告例と実験結果報告の紹介から
NW運用者として今後考慮すべきことをお話します。

- 海外におけるROV実装報告例の紹介
- 日本におけるROV実装報告例の紹介
- 本当にROVは実装されているのか？実験
- NW運用者として考慮すべきこと
- まとめ

海外におけるROV実装報告例の紹介

IXや大規模ISPによるROV実装報告が増えてきています



https://twitter.com/JobSnijders/status/1256326712347881473

ROV実装報告その１(AT&T/AS7018, by nanog ML)

AT&T/as7018 now drops invalid prefixes from peers

Jay Borkenhagen jayb at braeburn.org
Mon Feb 11 14:53:45 UTC 2019

- Previous message (by thread): BGP topological vs centralized route reflector
- Next message (by thread): AT&T/as7018 now drops invalid prefixes from peers
- **Messages sorted by:** [date] [thread] [subject] [author]

FYI:

The AT&T/as7018 network is now dropping all RPKI-invalid route announcements that we receive from our peers.

We continue to accept invalid route announcements from our customers, at least for now. We are communicating with our customers whose invalid announcements we are propagating, informing them that these routes will be accepted by fewer and fewer networks over time.

Thanks to those of you who are publishing ROAs in the RPKI. We would also like to encourage other networks to join us in taking this step to improve the quality of routing information in the Internet.

Thanks!

Jay B.

AT&T/AS7018はPeerからの(RPKI的に)”invalid”な経路広告をdropすることを始めたよ。

まだ顧客からの”invalid”経路は受信して配信しちゃうけど今後、顧客と相談しながらなくして行く方向だよ。

インターネットルーティングの品質向上のために、みんなもがんばろう。

nanog ML:
https://mailman.nanog.org/pipermail/nanog/2019-February/099501.html

ROV実装報告その２(NTT/AS2914, by official HP)

NTT GIN(AS2914)は3/25からすべてのEBGPセッションにおいて”invalid”な経路広告をrejectします。

RPKI based BGP Origin Validation

On March 25th, 2020, NTT GIN will deploy BGP routing policies which reject **RPKI Invalid** BGP route announcements on all AS 2914 EBGP sessions. This change will positively impact the Internet routing system.

NTT GIN is committed to excellence in operating our global network and as such on March 25, 2020 – NTT GIN will perform RPKI based BGP Origin Validation with *invalid is reject* EBGP routing policies.

NTT Global IP Network公式HPより抜粋

https://www.gin.ntt.net/support-center/policies-procedures/routing-registry/

ROV実装報告その3(Telia/AS1299, by Peering DB)

メモ	
	IPv4 + IPv6 Prefixes above would be actuals, not proposed max- prefix values. AS1299 is matching RPKI validation state and reject invalid prefixes from peers and customers. Our looking-glass marks validation state for all prefixes. Please review your registered ROAs to reduce number of invalid prefixes. All trouble ticke[illegible]uests or support related emails should be sent to carrier-[illegible]liacompany.com.

AS1299のPeeringDBから抜粋

https://www.peeringdb.com/net/10

AS1299はRPKI検証を実施し、peerとcustomerからの”invalid” prefixをrejectします。”invalid” prefixを減らすためにあなたが登録しているROAの再確認をお願いします。

ROV実装報告その４(isbgpsafeyet.com)

RPKIのデプロイ状況を報告する公開サイト(https://isbgpsafeyet.com/)
ROVをデプロイしたASのアップデートや状況が確認できる。

Latest updates

- September 14, 2020 - HOPUS (AS44530) is now filtering all eBGP sessions using RPKI ROV. (source)
- September 2, 2020 - Netflix has deployed RPKI globally and is dropping invalids prefixes. (source)
- September 1, 2020 - Swisscom is fully dropping RPKI invalids since end of July. (source)
- August 26, 2020 - Google is currently deploying RPKI. The network operator signed more than 90% of its prefixes.
- August 7, 2020 - HKIX, an Internet Exchange in Hong Kong deployed RPKI validation on all its member sessions and is now dropping RPKI invalids on their route servers. (source)
- July 24, 2020 - Telstra AS1221, Australia's leading telecommunications and technology company, now filters RPKI invalids. (source)
- July 13, 2020 - Chilean Government Network (Red de Conectividad del Estado) at AS17147 succesfully deployed RPKI filtering and drops invalid prefixes. (source)
- July 6, 2020 – GR-IX, the Greek Internet Exchange, is now dropping RPKI invalids on their route servers (source)
- June 16, 2020 – Hurricane Electric AS6939, a major transit provider deployed RPKI filters (source)

Status

Displaying 29 major operators　+ Show all　− Hide ASN column

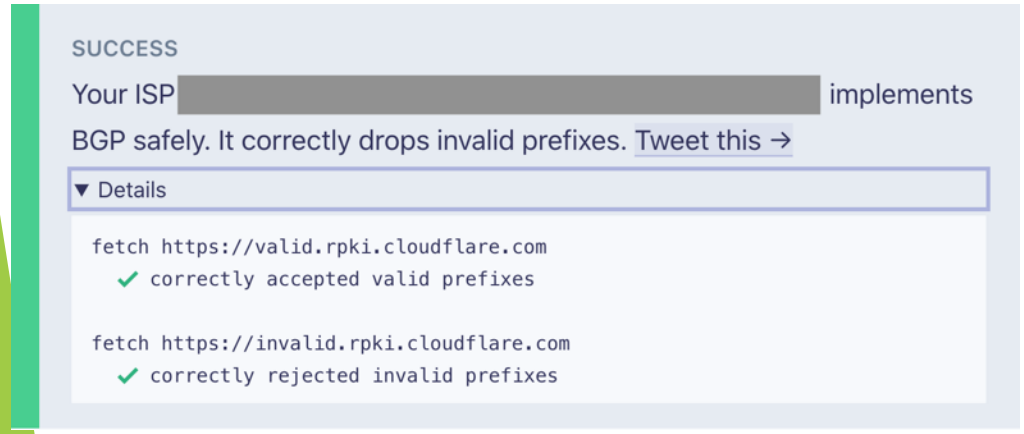
NAME	TYPE	DETAILS	STATUS ▲	ASN ?
Telia	transit	signed + filtering	safe	1299
Cogent	transit	signed + filtering	safe	174
GTT	transit	signed + filtering	safe	3257
NTT	transit	signed + filtering	safe	2914
Hurricane Electric	transit	signed + filtering	safe	6939
Cloudflare	cloud	signed + filtering	safe	13335
Netflix	cloud	signed + filtering	safe	2906
Wikimedia Foundation	cloud	signed + filtering	safe	14907
Scaleway	cloud	signed + filtering	safe	12876
TATA	transit	filtering peers only	partially safe	6453
PCCW	transit	filtering peers only	partially safe	3491
Telstra International	transit	signed	partially safe	4637
AT&T	ISP	signed + filtering peers only	partially safe	7018
Google	cloud	signed	partially safe	15169
Amazon	cloud	signed	partially safe	16509

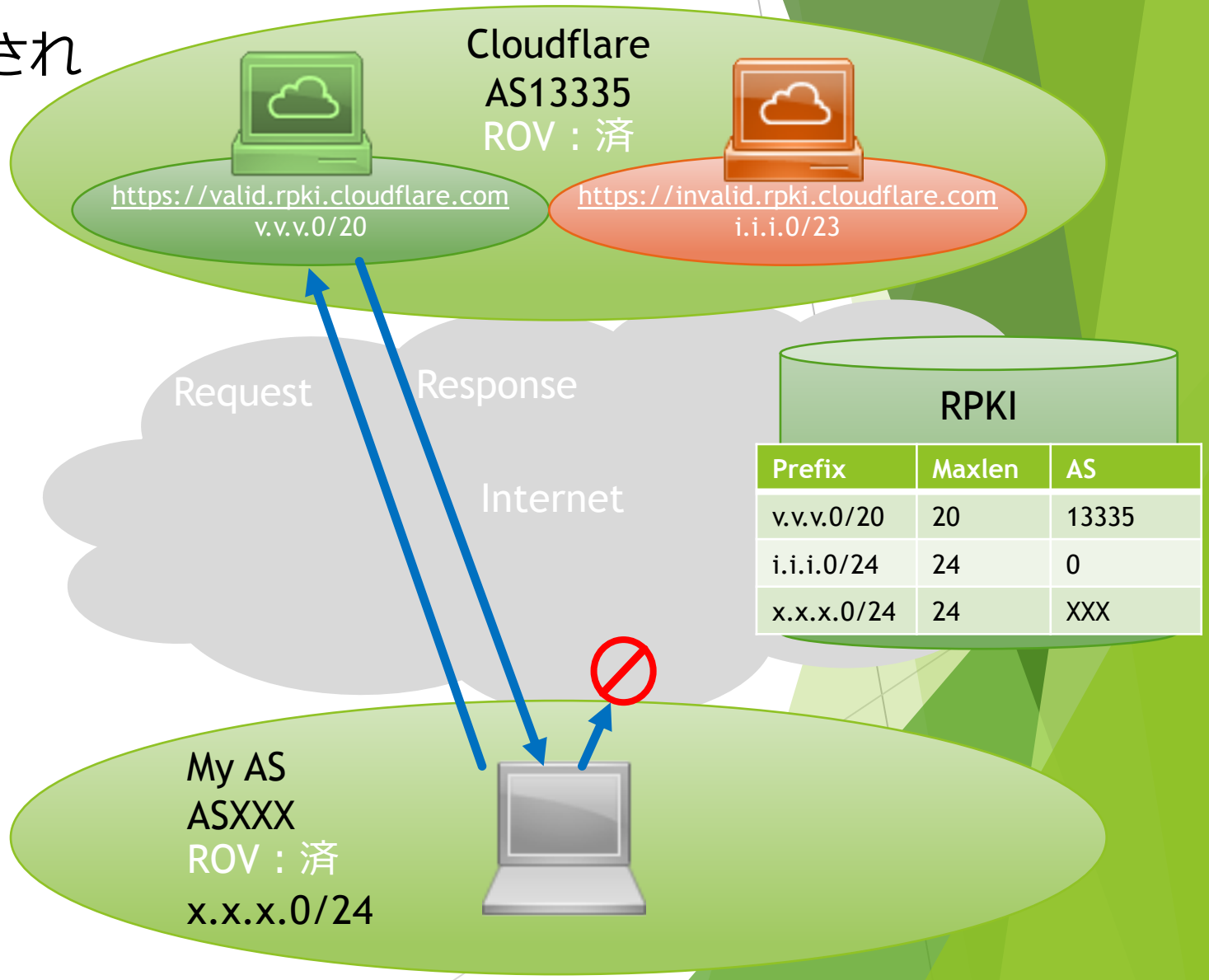
情報精度については賛否両論あるがわかりやすいし参考情報としては使えそう。

isbgpsafeyet.comの判定方法①（推定）

- 自AS(My AS)においてROVが実装されている場合
  - validホストへの接続: OK
  - invalidホストへの接続: NG

あなたのASは”safe”と判定

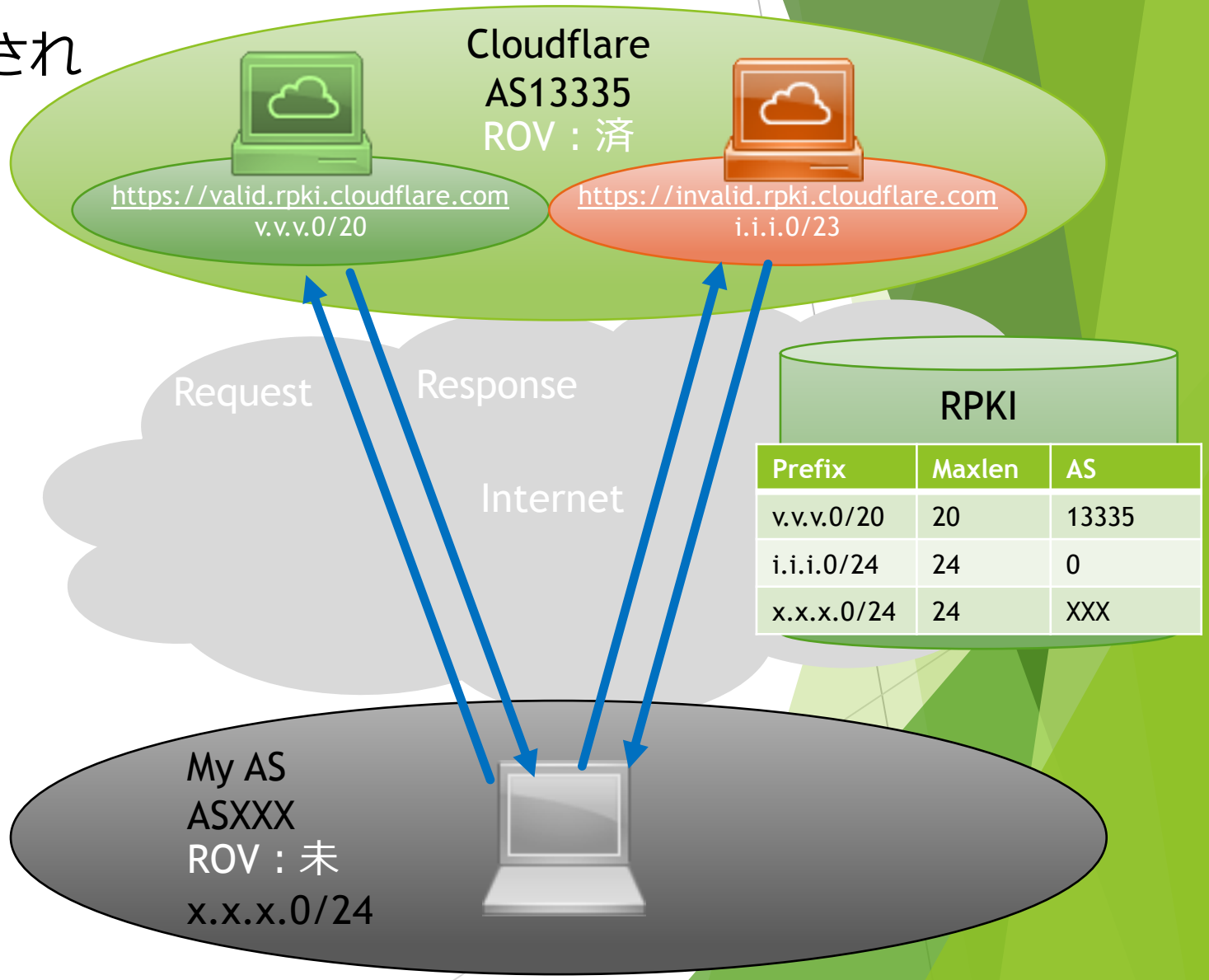




isbgpsafeyet.comの判定方法②（推定）

- 自AS(My AS)においてROVが実装されていない場合
  - validホストへの接続: OK
  - invalidホストへの接続: OK

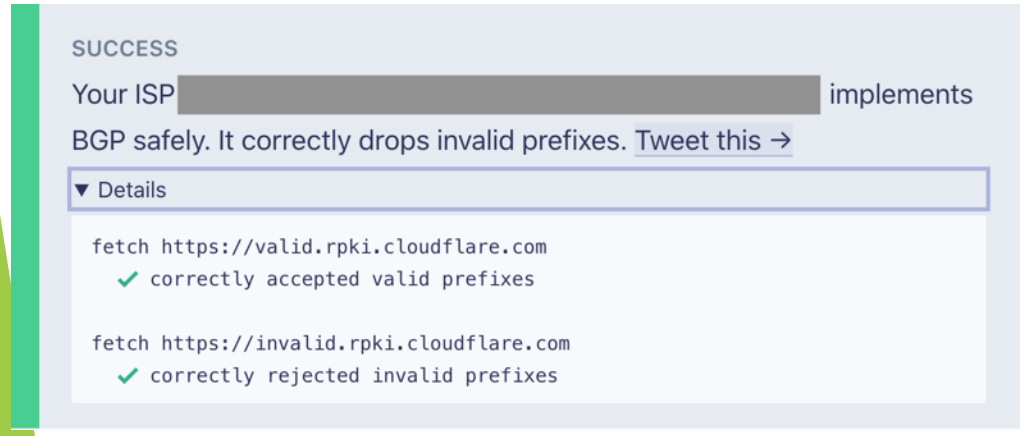
あなたのASは”unsafe”と判定

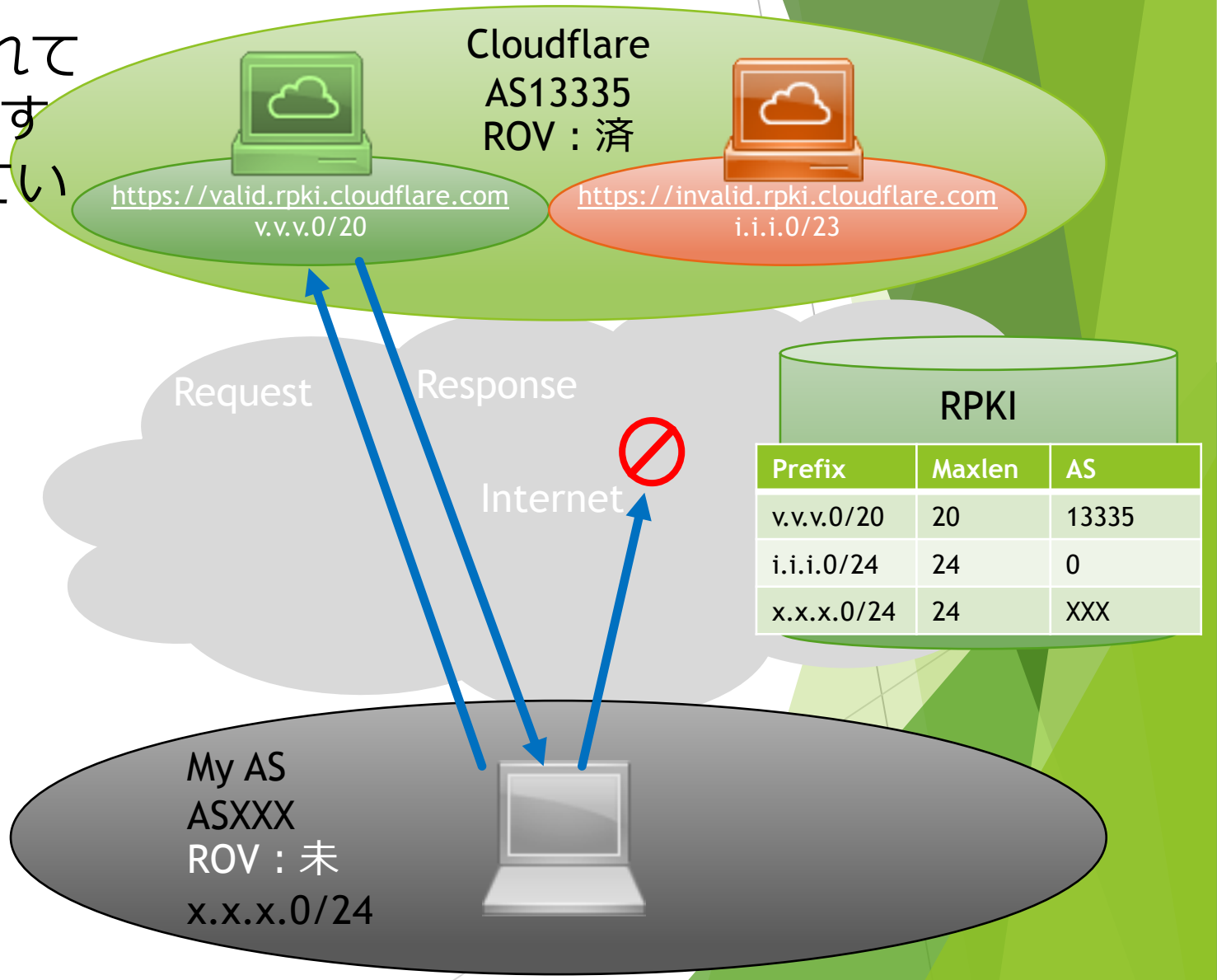


isbgpsafeyet.comの判定方法③（推定）

- 自AS(My AS)においてROV実装されていないが、cloudflareまでに経由するASのどこかでROVが実装されている場合
  - validホストへの接続: OK
  - invalidホストへの接続: NG

あなたのASは”safe”と判定

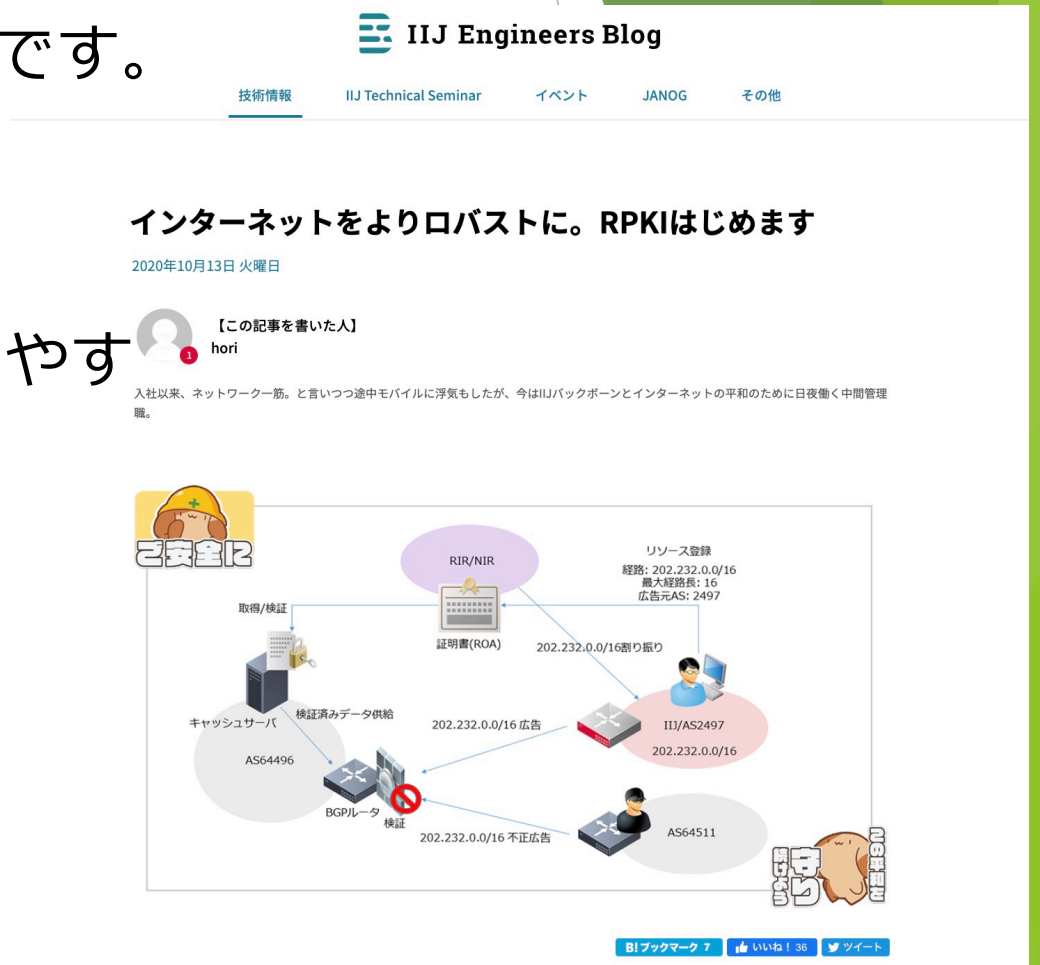




日本におけるROV実装報告例の紹介

日本初！実装報告

- IIJ(AS2497)さんがROVの実装を開始されたようです。
- 商用ISPとしては国内初ではないでしょうか。
- ブログでは、背景や具体的な例をもとにわかりやすく紹介されているので、ぜひご一読を。



https://eng-blog.iij.ad.jp/archives/6861

本当にROVは実装されているのか？実験

ROVは本当に実装されているのか実験してみる。

前述の通り、ROVの実装報告がされ始めているが、実際のところどうなのか
JPNAPの検証環境をお借りして実験してみることにしました。

実験方法：
isbgpsafeyet.comと同様の手法で、国内から広告している経路を意図的に
invalidになるようROAを登録し、Tier1 ISPのPublicなlooking glassを用いて
経路状態がどうなるのか確認してみる。

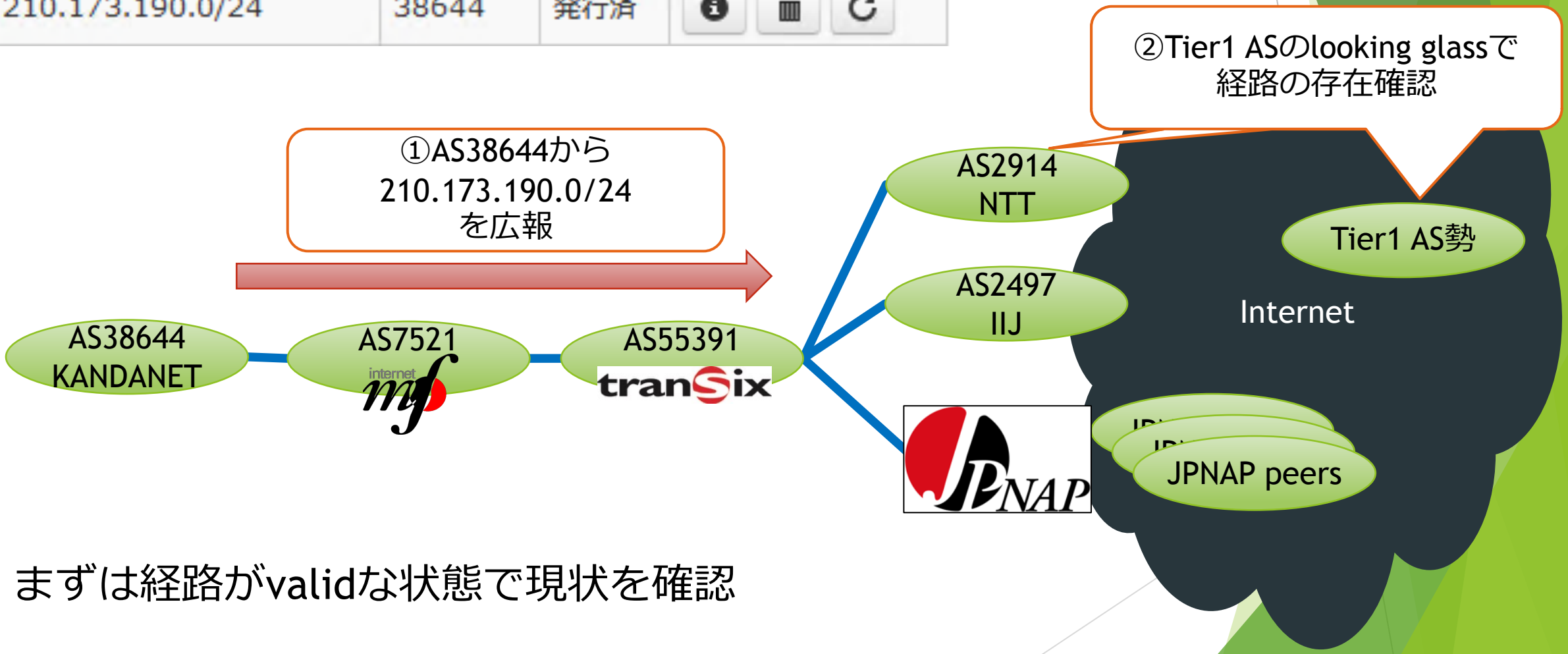
https://en.wikipedia.org/wiki/Tier_1_networkからTier-1 ISPを抽出

仮定：
ROAを変更後、確認したASのlooking glassで経路が見えない状況になってい
る場合、そのASは”ROVを導入している”可能性が高いのではないか？

というわけで、できたのがこれ。

ROA　JPNIC ROAWeb経由でAS38644でROA登録されている状態

210.173.190.0/24	38644	発行済	



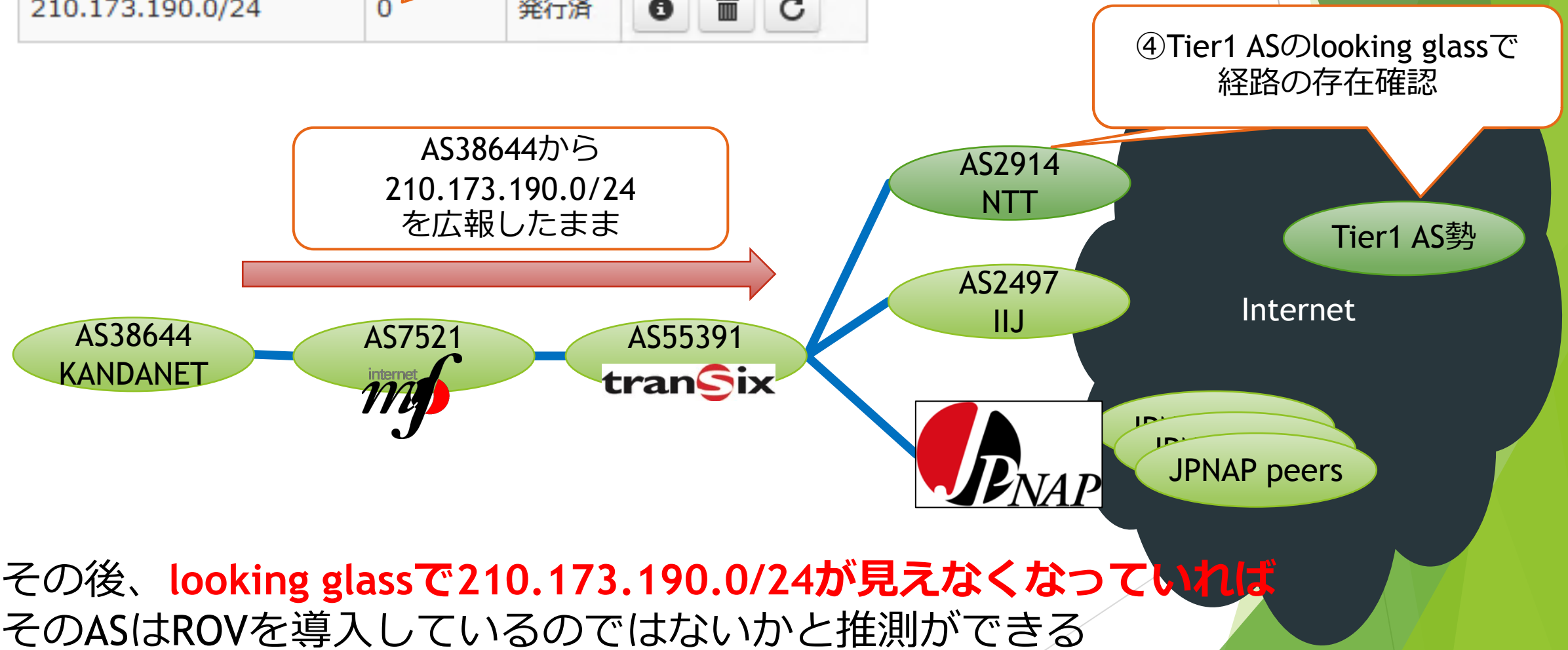
まずは経路がvalidな状態で現状を確認

というわけで、できたのがこれ。(つづき)

③JPNIC ROAWeb経由でROAのASを0に変更

ROA

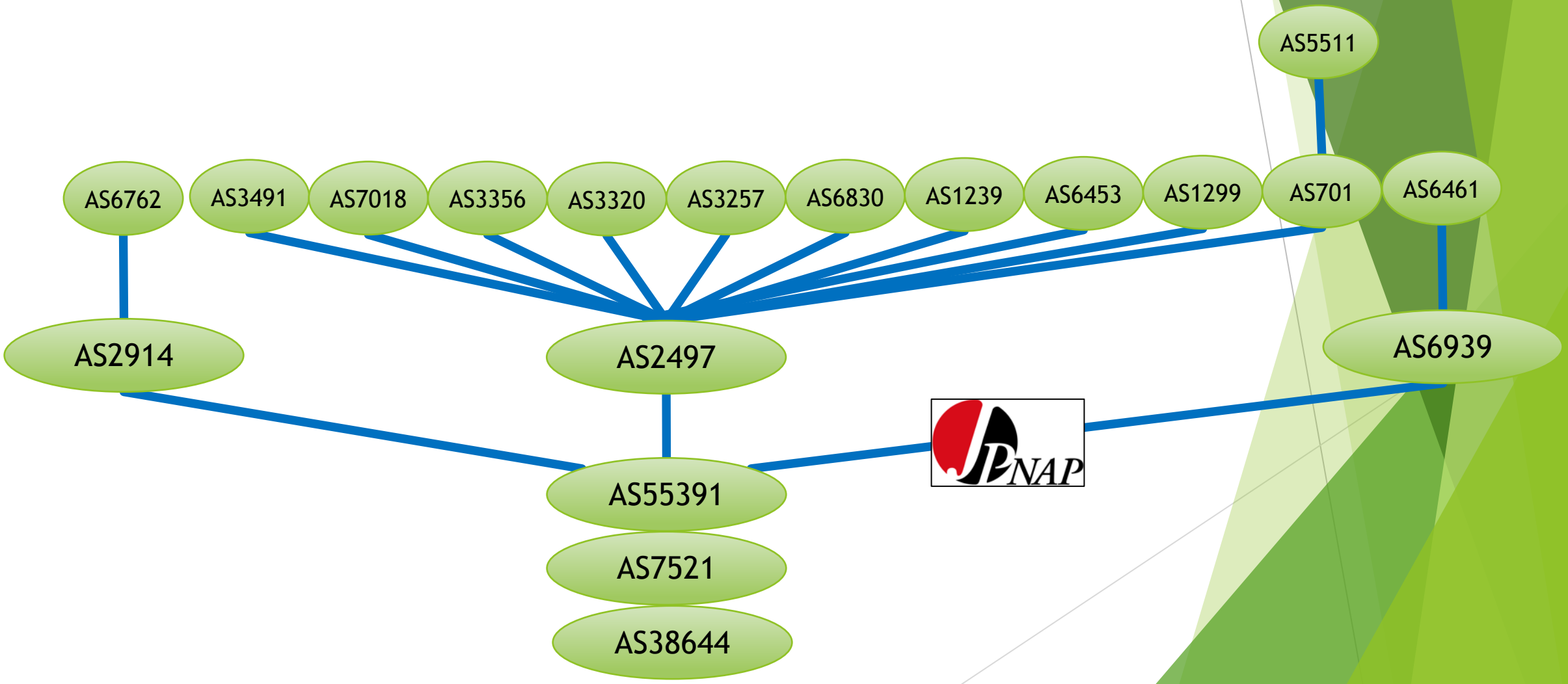
210.173.190.0/24	0	発行済	



その後、**looking glassで210.173.190.0/24が見えなくなっていれば**
そのASはROVを導入しているのではないかと推測ができる

実験結果(経路がvalidなときのAS隣接関係)

確認可能な全てのTier1 ASで経路の存在を確認

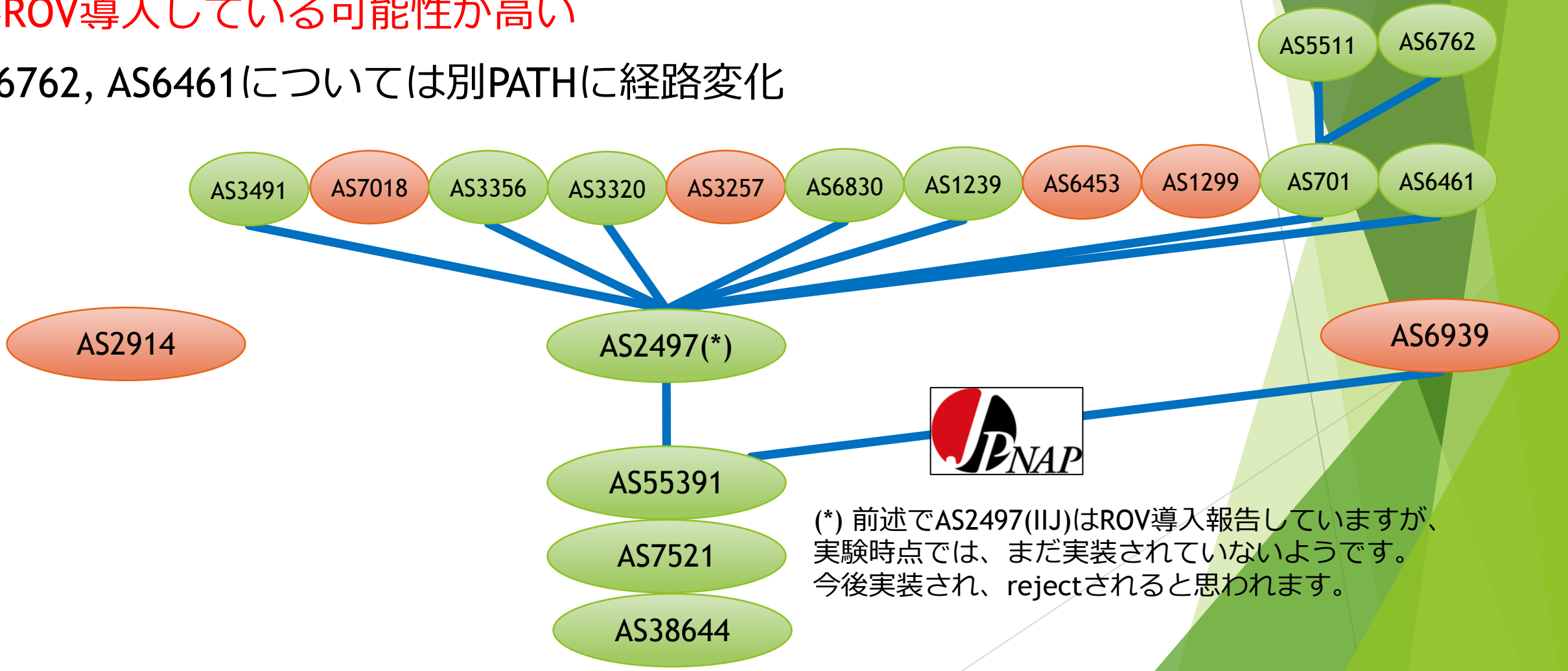


実験結果(経路がinvalidなときのAS隣接関係)

AS2914, AS7018, AS3257, AS6453, AS1299で”Not in Table”

→ROV導入している可能性が高い

AS6762, AS6461については別PATHに経路変化



(*) 前述でAS2497(IIJ)はROV導入報告していますが、
実験時点では、まだ実装されていないようです。
今後実装され、rejectされると思われます。

Tier-1 ISPのlooking glassと実験結果

Name	ASN	looking glass site	isbgpsafeyet.com status (2020/11/10時点)	ROV実験結果
Telia	1299	https://lg.telia.net/	safe (signed+filtering)	✓
NTT	2914	https://www.gin.ntt.net/looking-glass/	safe (signed+filtering)	✓
GTT	3257	telnet://route-server.ip.tiscali.net	safe (signed+filtering)	✓
TATA	6453	http://lg.as6453.net/bin/lg.cgi	partially safe (filtering peers only)	✓
AT&T	7018	telnet://route-server.ip.att.net	partially safe (signed+filtering peers only)	✓
Liberty Global	6830	telnet://route-views.linx.routeviews.org	partially safe (signed)	
PCCW	3491	https://lookingglass.pccwglobal.com/	partially safe (filtering peers only)	
Deutsche Telekom	3320	https://lookingglass.telekom.com/	unsafe (started)	
Orange	5511	telnet://route-server.opentransit.net/	unsafe (started)	
Sparkle	6762	https://gambadilegno.noc.seabone.net/lg/	unsafe (started)	
Level3/CenturyLink	3356	http://lg.level3.net/	unsafe (started)	
Sprint	1239	https://www.sprint.net/lg/	unsafe	
Telefonica/Telxius	12956	http://telxius.lg.ginernet.com/ ※BGP経路確認機能がないため割愛	unsafe	-
Verizon	701	https://enterprise.verizon.com/en-nl/why-verizon/looking-glass/	unsafe	
Zayo	6461	http://lg.zayo.com/lg.cgi	unsafe	

isbgpsafeyet.comと今回の実験ではほぼ同じ結果が得られた。

NW運用者として考慮すべきこと

経路に関わるトラブルシューティング時にROVの可能性も考慮しましょう

- トラブルシューティング対象の経路がROAに登録されているかどうか？登録されている場合は”invalid”になりうる経路かどうか確認しましょう。

  ROAのリスト(ROAキャッシュサーバを持たない人向け)
  https://rpki-validator.ripe.net/roas

- 現時点で、全てのASがROVを導入しているわけではないので、“invalid”な経路が流れこんでくる可能性もあります。upstreamやpeerなど近隣のASの導入状況を知っておくとよいでしょう。

- ROVはOrigin ASがROAと異なる場合だけでなく、（正しいOrigin ASであったとしても）Prefix Lengthが範囲内(Prefix Length～Max Prefix Length)に含まれない場合、”invalid”となるので注意しましょう。

自身が管理するアドレスのROAを登録しましょう！

- 経路ハイジャックをされた場合、ROV導入ASにおいてrejectされることにより、影響範囲を低減させることができます。

- ROAを登録できるのは、アドレスホルダです！
  IRRは経路を広報するASホルダが登録することが多いですが、ROAはASホルダが登録することはできません。PI（Provider Independent/持ち込み）アドレスを所有するNW管理者はご自身で登録しなければなりません。

- ROAの登録は慎重に！
  - 広報するASは他に存在しないか？(Punching Holeの可能性はないか？)
  - Max Prefix Lengthは適正か？（トラフィック制御目的や経路ハイジャック奪還の可能性を考慮した設定）
  - ROA登録は維持されているか？（定期的にROAが正しく登録されているかどうか確認する）

まとめ

- 昨年くらいから、Tier1 ASやIX route serverにおいてROV導入が活発化している。

- ROV導入報告はtwitterやpeeringdb, 公式HPなどで報告されている。
  さらに最近になってROV導入状況を報告するサイトなどもでてきているので参考にすると良い。

- 宛先までに経由するASでROVが導入され、人知れず守られるメリットがありますが、一方でそれが原因でトラブルが発生する可能性もあります。
  特にupstreamの導入状況は確認しておいたほうが良い。

謝辞：実験環境の利用についてはJPNAP様のご協力をいただきました。
この場をお借りしてお礼申し上げます。