

ROA 登録しようよ！

2022/9/29 @ IRS33

NTTコミュニケーションズ

渡辺英一郎

今回の発表内容

IRS32(2021/09/17)で「RPKI ROA登録のすすめ」ということでROAの登録状況などをご報告させていただきました。

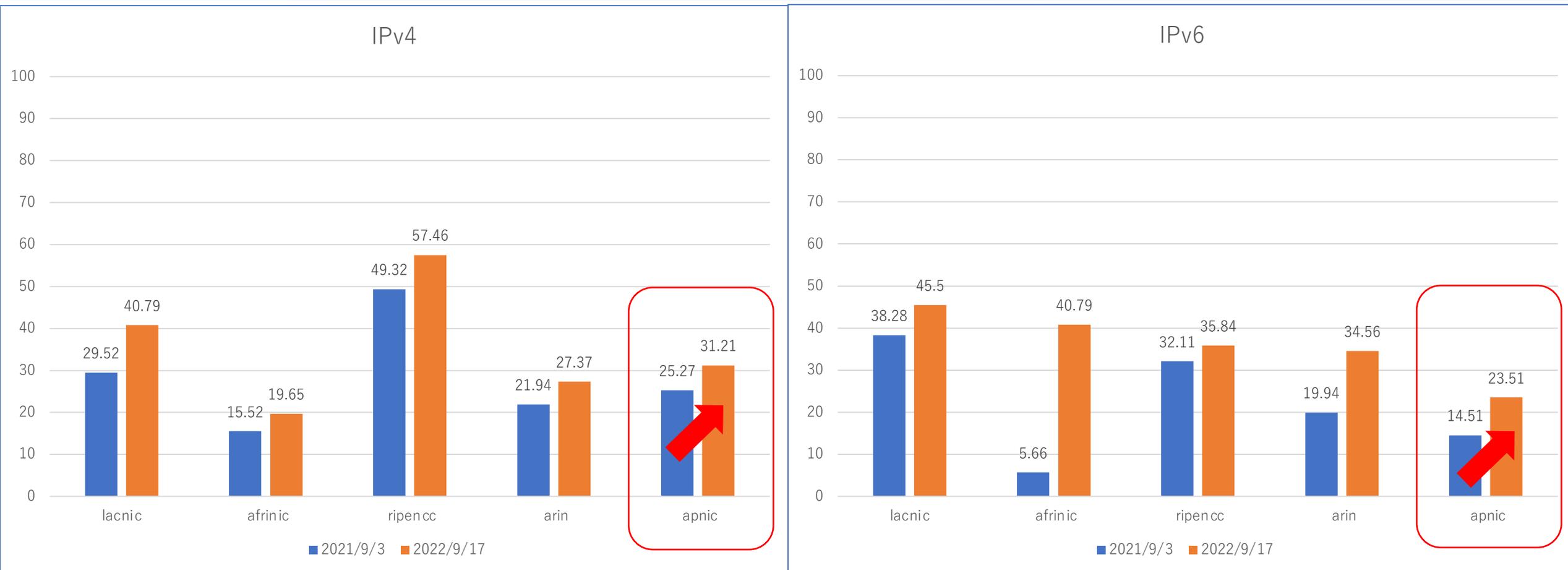
今回の発表では、

- あれから1年経過して、ROA登録状況にどのような変化があったのか？
 - OCN(AS4713)の状況
 - 経路異常発生時におけるROA登録効果？
- について話をいたします。

注) 調査に関してはNROの統計情報やJPNICのAS番号・JPIRR情報、ROAキャッシュサーバのROA情報、RIPE RISのBGPアーカイブなど、ほぼ公開されている情報の中で算出しました。報告している数値に関しては取得のタイミングなどで一部誤差があるかと思えます。ご了承のほどよろしくおねがいします。

ROA登録状況

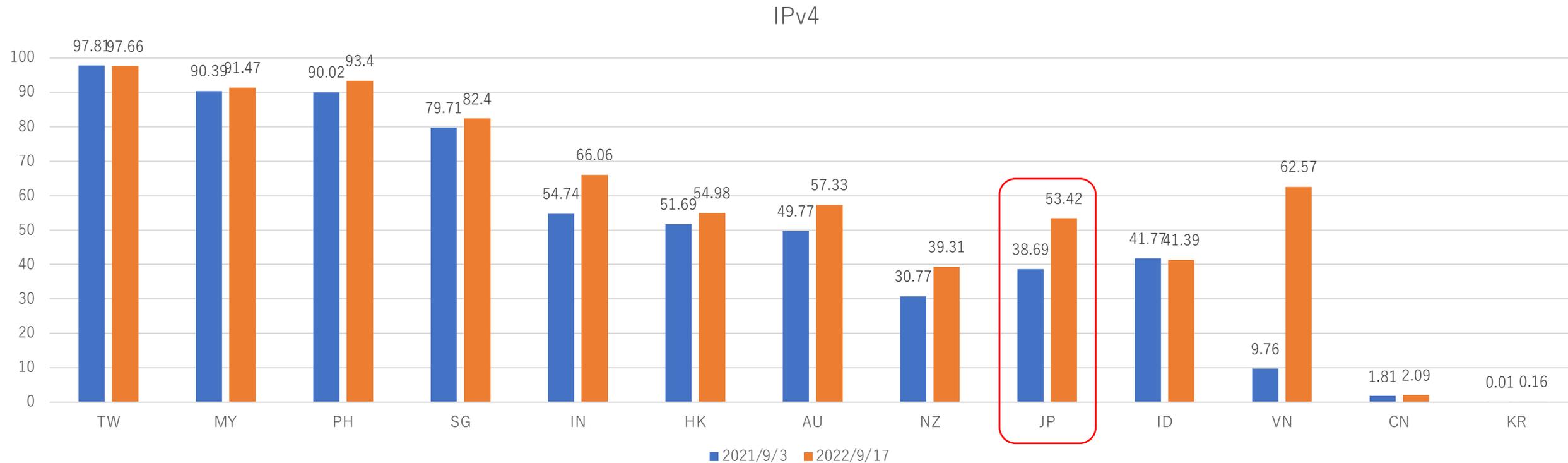
RIRごとのROA登録率



APNICのROA登録率はIPv4: 約6%、IPv6: 約9%増加

<https://www.nro.net/wp-content/uploads/rpki-uploads/rir-adoption.csv>

APNICリージョンの主要国(経済圏)ごとのROA登録率 (IPv4)

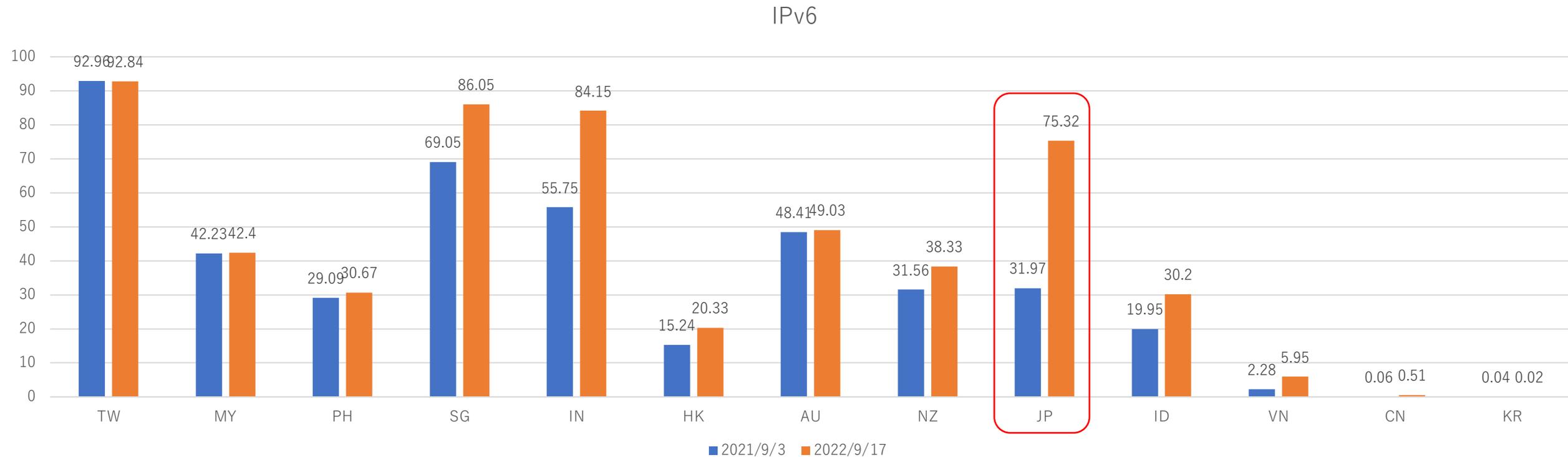


日本(JP)は53.42%(+15%)

APNICリージョン諸国も概ね増加傾向だが、台湾(TW)、インド(ID)は微減。

特にベトナム(VN)は大きく増加している。

APNICリージョンの主要国(経済圏)ごとのROA登録率 (IPv6)



日本(JP)は75.32%(+43.35%)

APNICリージョン諸国も概ね増加傾向だが、台湾(TW)、韓国(KR)は微減。

JPNIC割り当てASの状況

	2021/09/03時点	2022/09/17時点	差分
アサインされているAS数(総数)	735	755	+20
1つでもROAが登録されているAS数	87	124	+37
ROA登録がなく、かつ経路広報していないAS数	156	178	+22
経路広報しておりROA登録がないAS数	492	453	-39

約1年で39ASのROA登録が増えた！

Cable/DSL/ISP事業者さんの登録が増えているように見えます👏

残り453のASにも、ぜひ、ROA登録のご検討お願いいたします！

JPNIC割り当てASの状況 (ROAカバー率100%)

広報している経路がROAで100%カバーされているAS数

	2021/09/03時点	2022/09/17時点	差分
IPv4	42	69	+27
IPv6	30	51	+21

IPv4/v6ともにカバー率100%のASは38AS! すばらしい!

コンテンツ、NSPの登録が多かったが、Cable/DSL/ISPも増えてきています。
今年登録してくれたASの方々かな?



JPNIC下の広報経路Top10 ASのROAカバー率

IPv4

Rank	ASN	# of adv routes (/24units)	ROA adoption rate for advertised routes(*)	2021/9/3との増減
1	AS17676	170,893	96.21%	+27.12%
2	AS4713	112,871	97.51%	-0.01%
3	AS2516	71,465	66.90%	+66.90%
4	AS2907	34,501	0.25%	
5	AS17506	21,024	0.00%	
6	AS2527	14,852	100.00%	+2.19%
7	AS2497	14,638	57.91%	+12.64%
8	AS2518	14,336	100.00%	+17.86%
9	AS17511	12,001	0.00%	
10	AS2510	10,761	0.00%	

IPv6

Rank	ASN	# of adv routes (/64units)	ROA adoption rate for advertised routes(*)	2021/9/3との増減
1	AS17676	18,695,992,639,488	100.00%	
2	AS9595	4,410,931,412,992	0.00%	
3	AS4713	4,406,636,511,232	99.90%	
4	AS2516	2,757,369,069,568	0.00%	
5	AS2527	141,733,920,768	100.00%	
6	AS2519	103,079,215,104	0.00%	
7	AS55391	73,014,444,032	100.00%	
8	AS55392	73,014,444,032	100.00%	
9	AS9370	68,719,476,736	100.00%	
10	AS63784	68,719,476,736	100.00%	+100.00%

※ROA adoption rate for advertised routes:
9/17時点の広報経路に対するROA適用率（持ち込みIPも含む）

IPv4：大手ISPのROA登録率向上してきています。

IPv6：AS63784(デジ庁?)が100%の登録率に。これで安心 ;-)

参考) ハイパージャイアントたちのROA登録状況

IPv4

IPv6

※ROA adoption rate for advertised routes:
9/17時点の広報経路に対するROA適用率 (持ち込みIPも含む)

ASN	AS名	# of adv routes (/24units)	ROA adoption rate for advertised routes(*)	ASN	AS名	# of adv routes (/64units)	ROA adoption rate for advertised routes(*)
714	Apple	70,294	0.00%	714	Apple	17,179,934,720	0.00%
8075	Microsoft	187,655	98.89%	8075	Microsoft	558,615,101,440	100.00%
15169	Google	55,531	99.94%	15169	Google	94,506,123,264	100.00%
16509	Amazon	167,949	99.89%	16509	Amazon	364,638,306,304	98.82%
20940	Akamai	53,764	0.02%	20940	Akamai	1,138,167,119,872	0.02%
32934	Facebook	562	16.01%	32934	Facebook	4,311,744,512	99.61%

各社のメインASのみ調査しています。

ROA登録に関しては対応方針がわかれているようです。

Google, Amazon, Facebookは過去の影響を受けた経験がありますからね....

OCN(AS4713)のRPKI進捗状況

OCN(AS4713)のRPKI進捗状況

• ROA登録

- AS4713 OriginのPA(Provider Aggregatable)経路についてはすべて登録完了。
- PAについては広報経路、IRR登録、ROA登録の内容を約1年かけて一致させた。
 - 以前は、MaxlenをIPv4:/24, IPv6:/48としていたがexact matchに。
 - OriginAS詐称対策。
 - 可能なかぎり広報経路・IRR登録を集約させた上でROAを登録しなおし。
 - 管理しやすくするために。
 - less specificな経路ハイジャック対策。それほど効果は無いけどね。広報されたら気持ちわるいので。
 - Punching Holeしていた（されていた）経路をアドレス移管処理を経てクリーンに。
- PIについてどうするかが課題
 - このプレゼンをみたOCNのPIのお客様、ROA登録して～！ハイジャックされても知らんよ～w

• ROV導入

- Peerに対して絶賛導入中。年内 or 年度内には導入完了予定。
- Customerに対しては未検討。

経路異常時のROA登録効果？

8/10のAS4775のMisoriginの例

8/10 05:34~06:35(JST)にかけて、AS4775(フィリピン/Globe Telecom)が数千のIPv6経路を広報しました。

https://twitter.com/Qrator_Radar/status/1557125324638494723

 **Radar by Qrator** @Qrator_Radar
August 10, 2022 – AS4775, GLOBE-TELECOM-AS [PH]
– hijacked 329 prefixes creating 3625 conflicts for 3113 prefixes and 278 ASNs in 19 countries. Maximum propagation: 52%. Duration: 10 minutes. <https://t.co/DyGXwbeaM0>

私がRIPE RISで調べた限りでは、
広報されるべきではない経路：4,612（うち61経路がJPNIC割当て）
観測されたRIPE rrcピア数：最大385ピア
ありました。
みなさんどうでしたでしょうか？

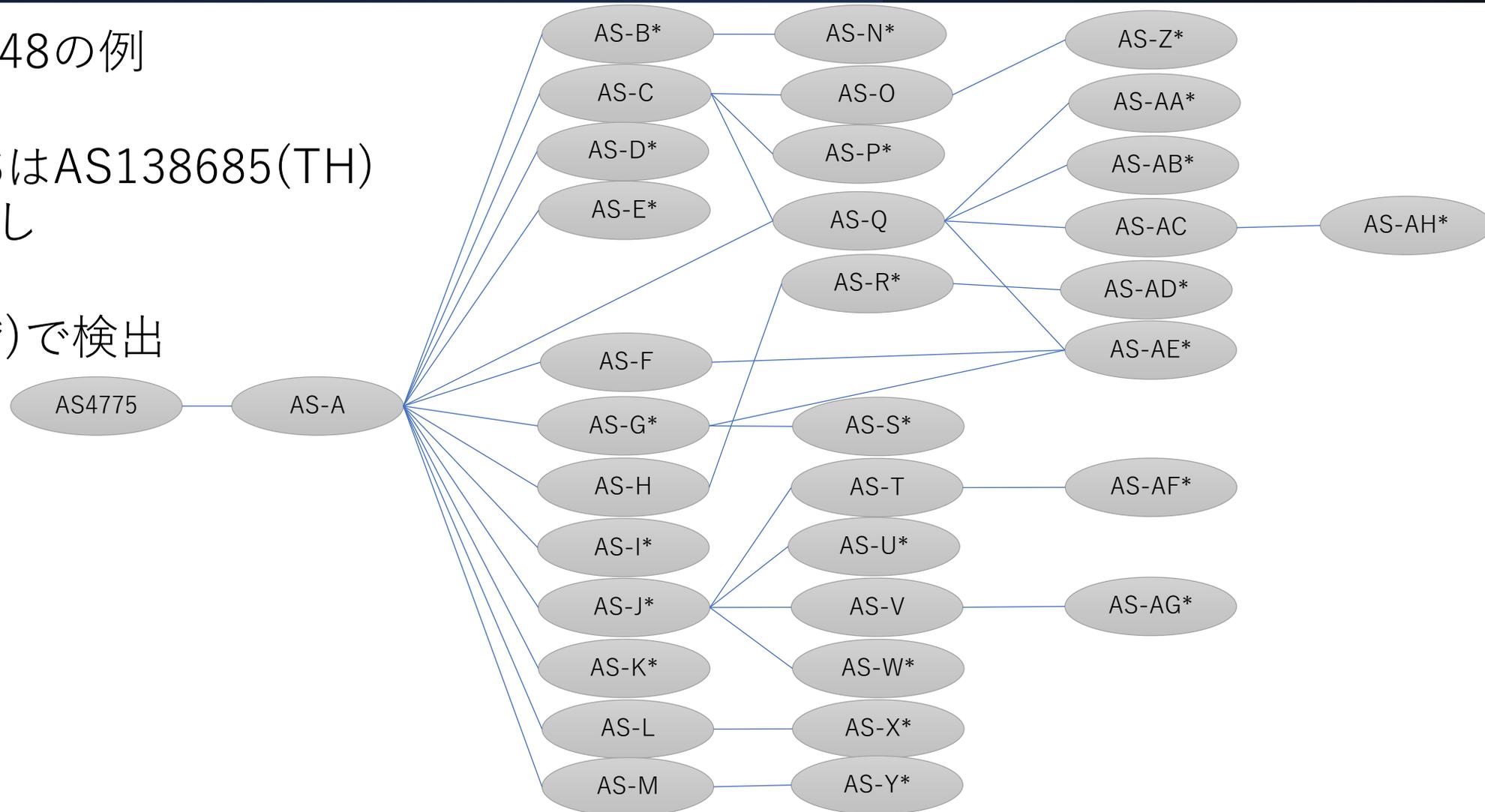
OCNは影響を受けましたが、トラフィック変化・お客様申告ともにありませんでした。

ROA登録なしの場合の影響範囲

2001:3c8:343::/48の例

本来のOrigin ASはAS138685(TH)
ROAの登録はなし

RIPE rrc 22AS(*)で検出



ROA登録ありの場合の影響範囲

2001:df1:6c00::/48の例

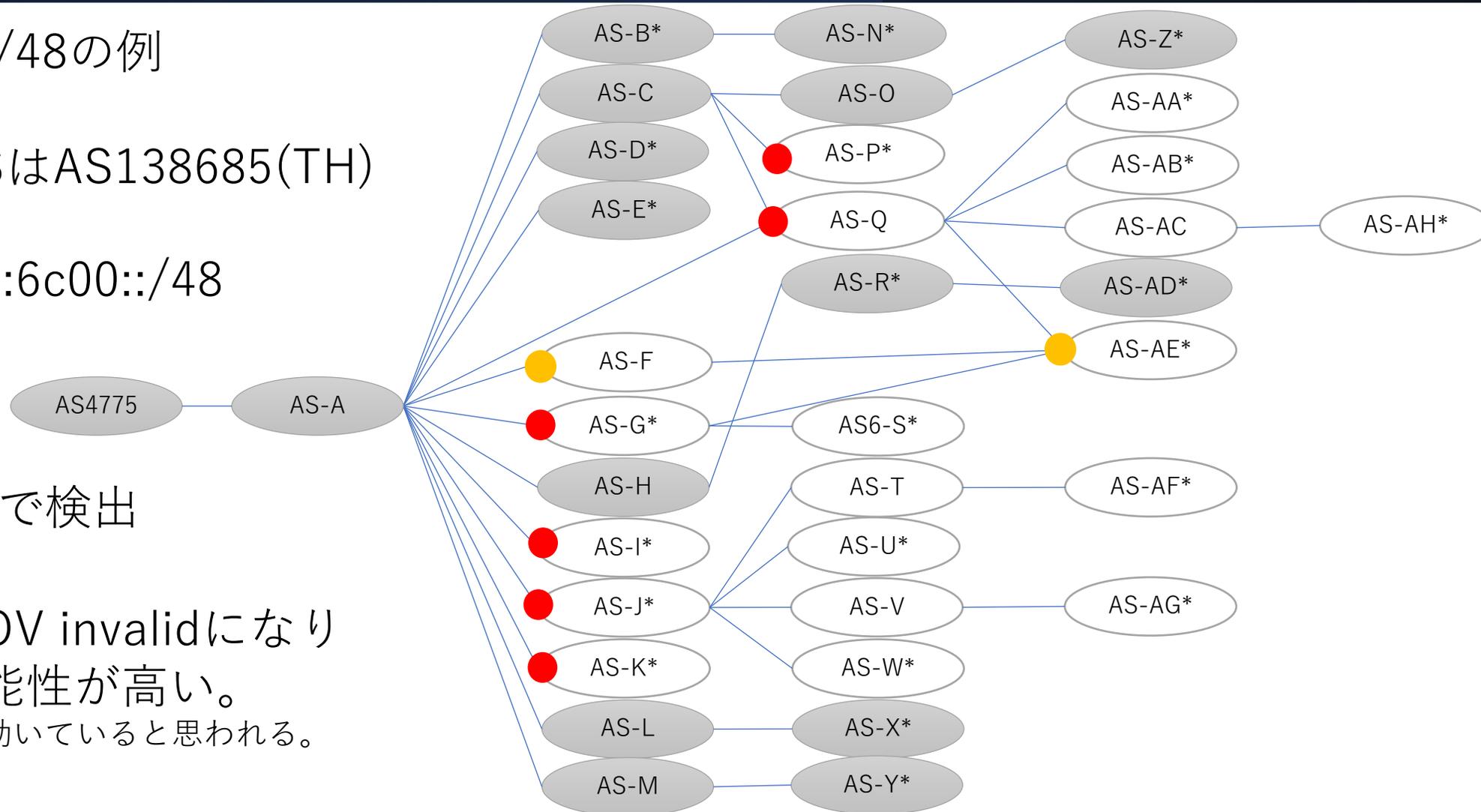
本来のOrigin ASはAS138685(TH)

ROAの登録あり

Prefix: 2001:df1:6c00::/48

Maxlength: /48

AS: 138685

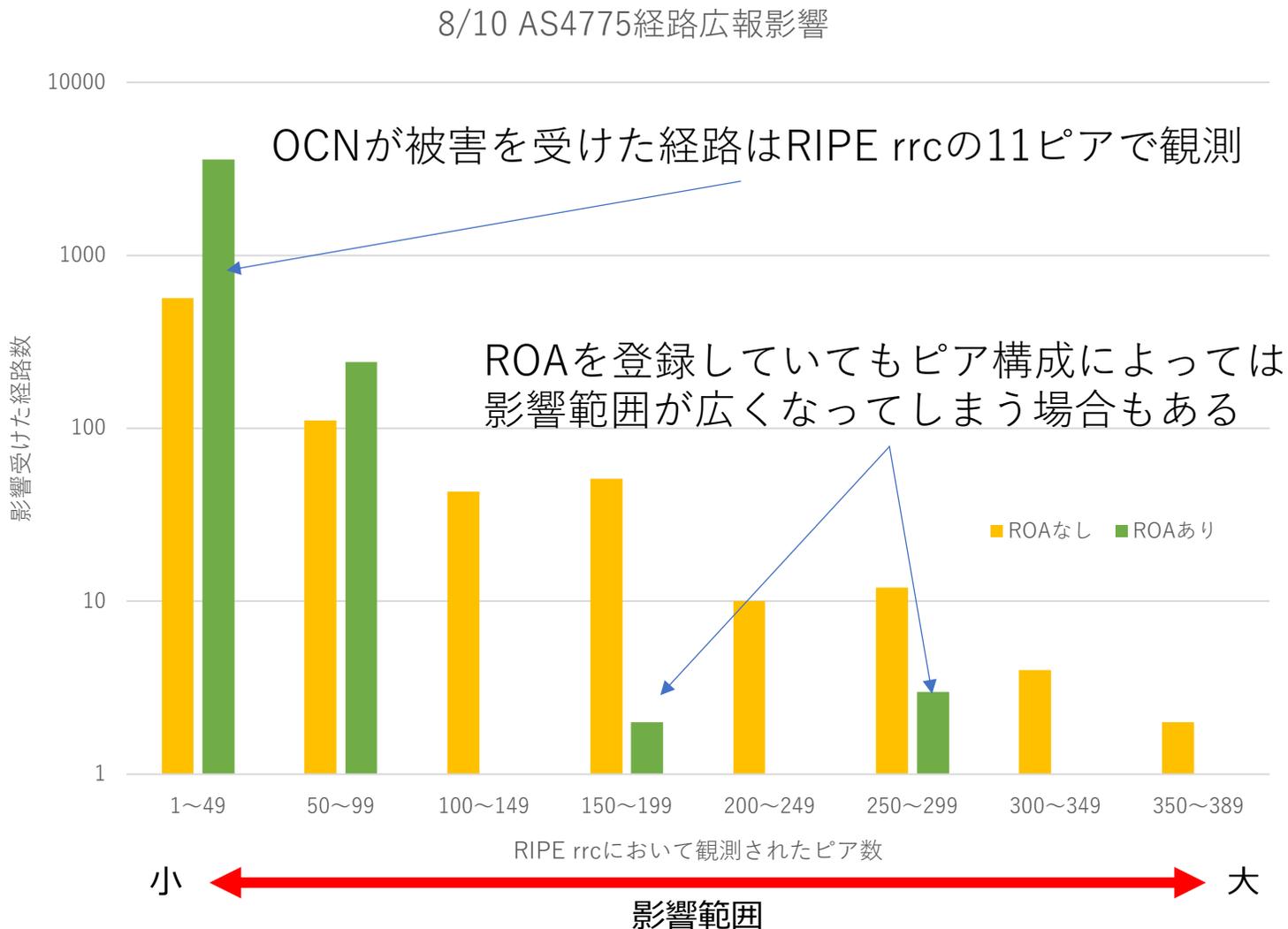


RIPE rrc 9AS(*)で検出

●ポイントでROV invalidになり
rejectされた可能性が高い。

●はどちらかでROVが効いていると思われる。

ROA登録あり/なしでの影響範囲の違い



ROAを登録していない経路（黄色）はまんべんなく観測されているのに対し、ROAを登録している経路（緑色）は観測されたピア数が少ない範囲に偏っている。

100%要因ではないと思うが、前述のとおり、ROVを導入しているASが増えてきていることによるとと思われる。

つまり、ROAを登録しておけば、影響を軽減できる。

今後、ROV導入が進んでいけばより効果が高くなる。

ROA登録しようよ！

現状、RPKIの導入に関して、NW管理者がやるべきことは大きく2つあります。

「ROAの登録」と「ROV導入」です。

「ROV導入」については、ROAキャッシュサーバの構築やルータへの実装など比較的ハードルが高いですが、「ROAの登録」は比較的簡単ですし、Tier1 ISPやIX router-serverなどがROVを導入し始めているので、ROAを登録するだけでも経路異常対策としての恩恵（影響の軽減）を受けられます。

ROA登録は一度間違えずに登録しさえすれば、それほど問題にはならないはず。
（仮にJPNICのCAが全滅しても、今の状態に戻るだけ。）

ROA未登録なみなさま、ぜひ、ご検討を！