janog53.5

RPKIホットトピック

2024年05月31日

NTTコミュニケーションズ株式会社

© NTT Communications Corporation All Rights Reserved.

自己紹介

名前：　　渡辺　英一郎（わたなべ　えいいちろう）
所属：　　NTTコミュニケーションズ㈱　PS本部 C&N部開発オペレーション部門
主な業務内容：OCN(AS4713)のネットワーク設計/ピアリング担当

出身：　　栃木県宇都宮市🥟
年齢：　　５３歳


愛犬ゴン

社外活動：
・ICT-ISAC Japan BGP-WG主査
　経路ハイジャック検知システム「経路奉行」運用など
・総務省事業 RPKI有識者検討会メンバー
　RPKIガイドライン策定など

過去のjanog発表：
・2006/07 janog18 経路ハイジャックについて考える～prologue of 経路奉行～
・2012/01 janog29 IXで見えるユーザ動向とマルチラテラルピアリングの可能性

興味のある技術領域：
BGP　Google Cloud　terraform　kubernetes
AWS　vim　rust　python　go　Next.js

© NTT Communications Corporation All Rights Reserved.

Agenda

- RPKIに関するガイドライン案について
- ROA statistics
- ROV statistics
- その他のトピック

© NTT Communications Corporation All Rights Reserved.

「RPKIに関するガイドライン案」について

© NTT Communications Corporation All Rights Reserved.

RPKIに関するガイドライン案について

総務省「サイバーセキュリティタスクフォース政策分科会」
「ISPにおけるネットワークセキュリティ技術の導入及び普及促進に関する調査」
事業の中で**「RPKIに関するガイドライン案」**が公開されました。

総務省｜サイバーセキュリティタスクフォース｜ICTサイバーセキュリティ政策分科会（第5回）（soumu.go.jp）
https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00286.html
参考資料2・RPKIのROAを使ったインターネットにおける不正経路への対策ガイドライン案
https://www.soumu.go.jp/main_content/000941397.pdf

RPKI(ROA/ROV)導入に関するさまざまな点を考慮に入れて策定いたしました。
ぜひ、ご一読を。

© NTT Communications Corporation All Rights Reserved.

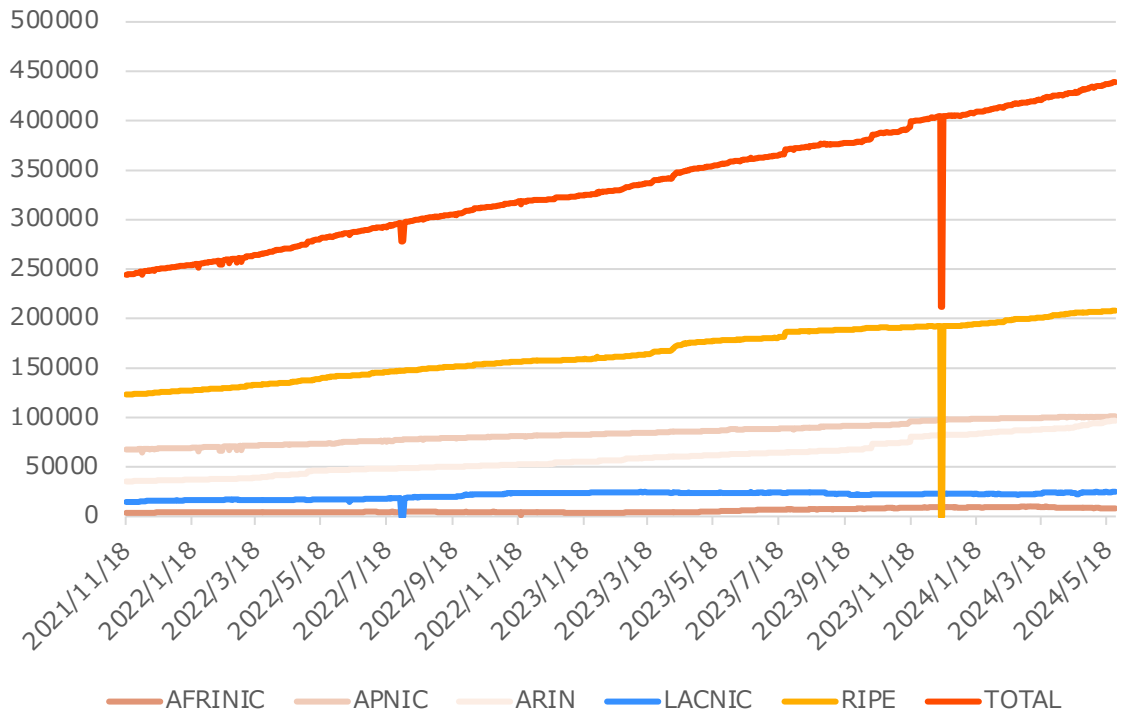
ROA statistics

© NTT Communications Corporation All Rights Reserved.

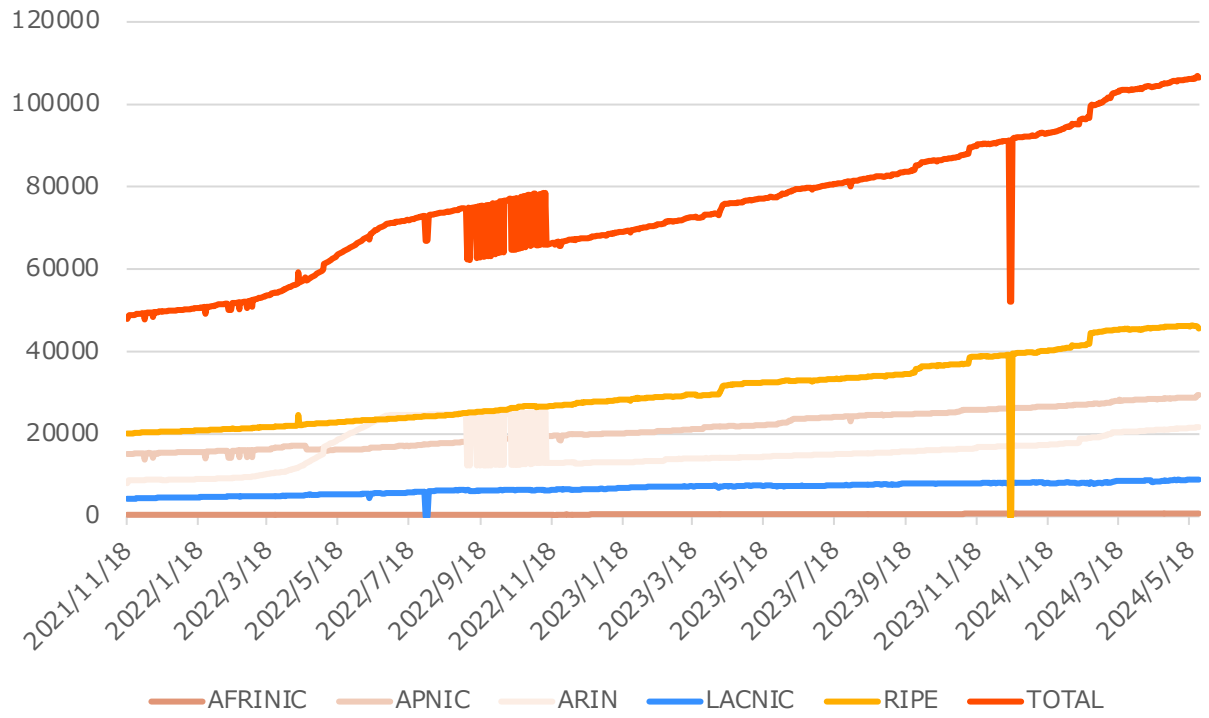
VRP数推移

RIRごとのROAに含まれるVRP(Validated ROA Payload)数の推移

IPv4



IPv6



IPv4/IPv6ともに増加傾向

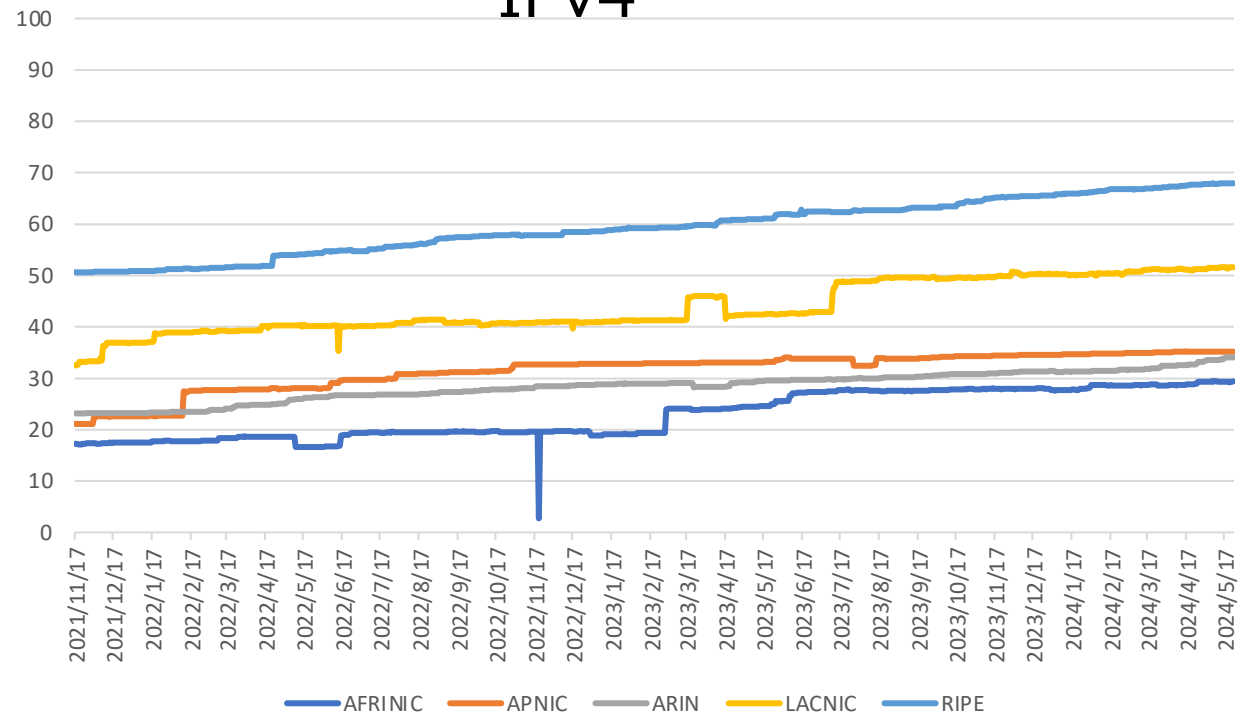
© NTT Communications Corporation All Rights Reserved.

RIRごとのRPKI適用率

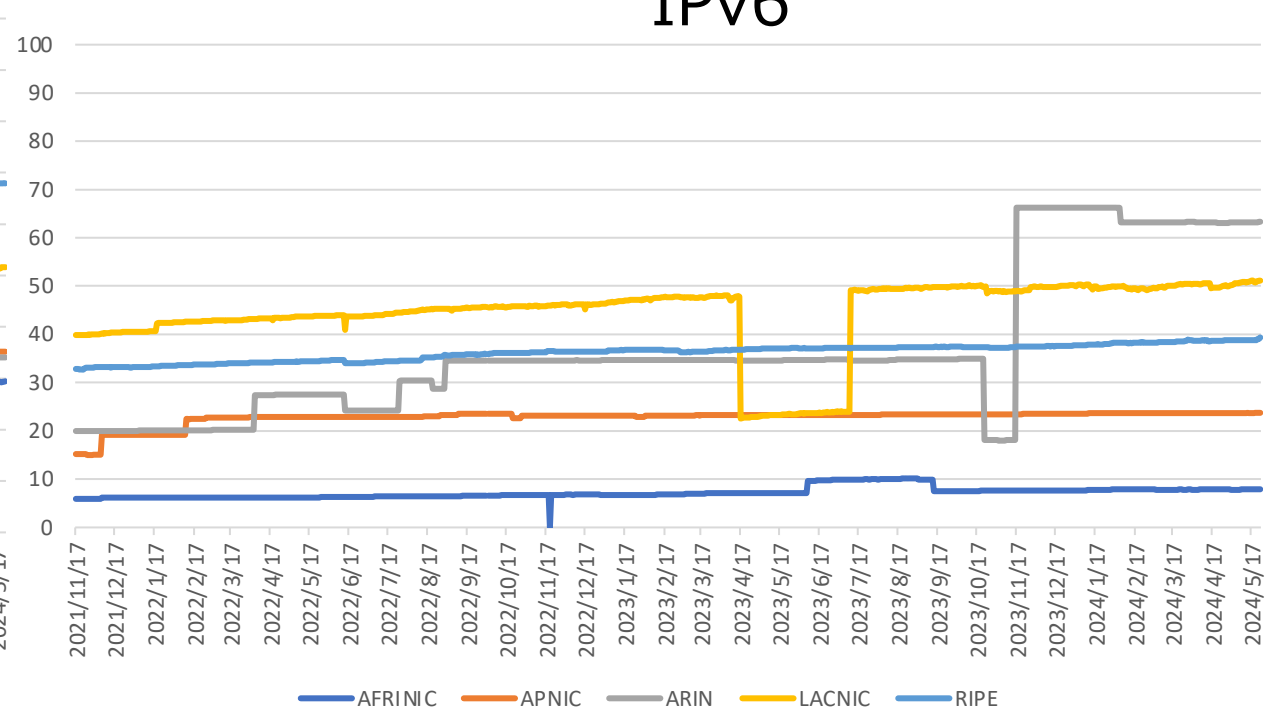
NRO(Number Resource Organization)が公開している情報を元にグラフを作成

情報元）https://www.nro.net/wp-content/uploads/rpki-uploads/rir-adoption.csv

IPv4



IPv6



IPv4/IPv6ともに増加傾向

APNICリージョン：IPv4 35.23%, IPv6 23.74%(2024/05/24現在)

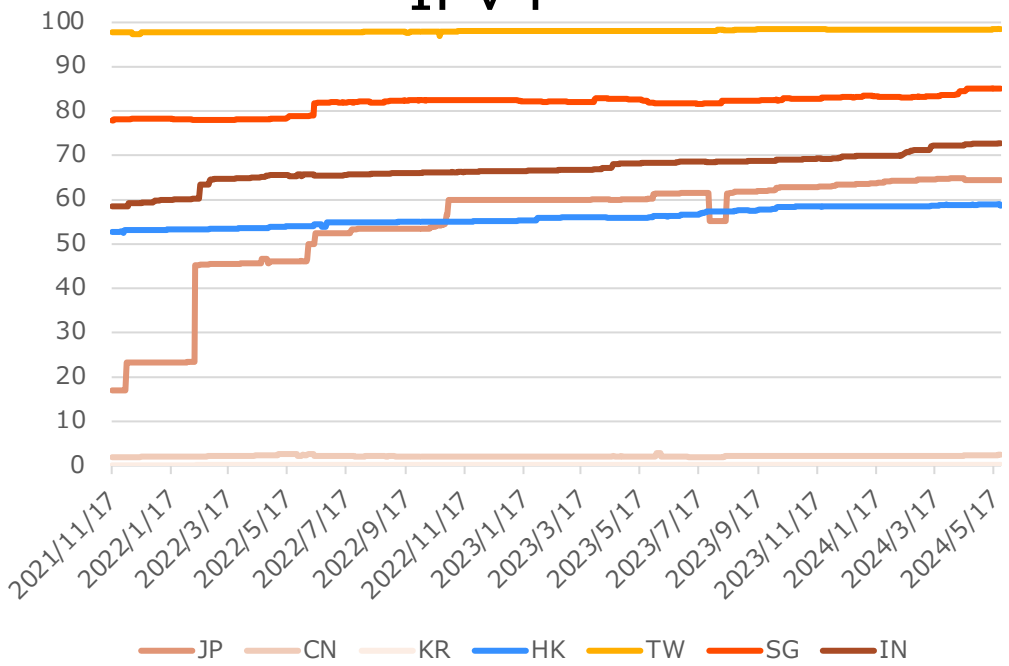
© NTT Communications Corporation All Rights Reserved.

APNICリージョンでの主要な経済圏ごとのRPKI適用率

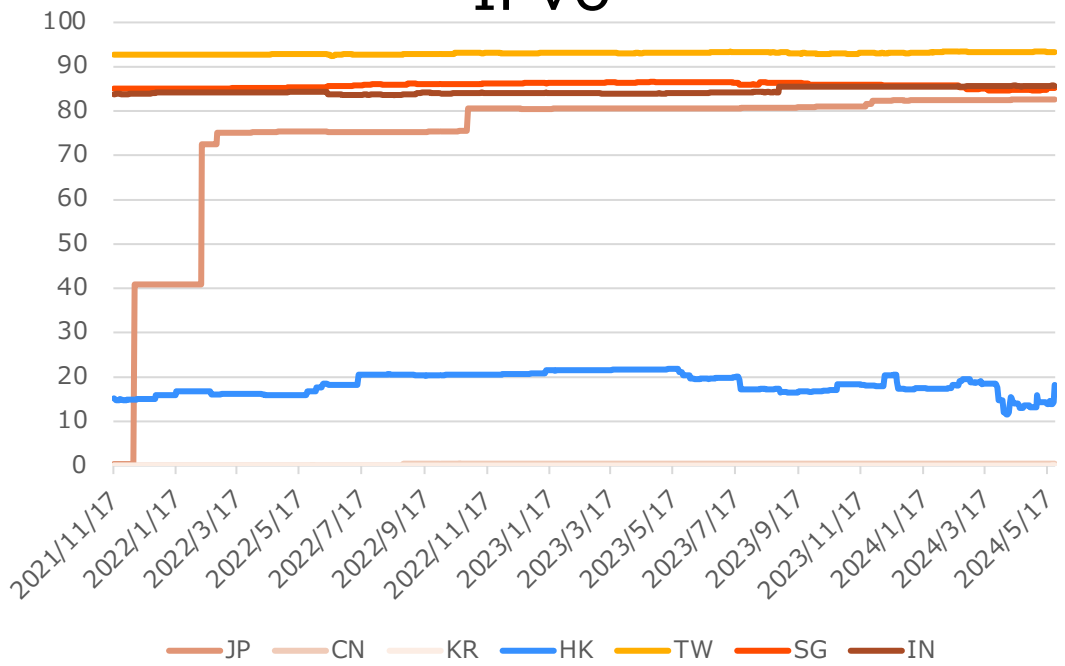
NRO(Number Resource Organization)が公開している情報を元にグラフを作成

情報元）https://www.nro.net/wp-content/uploads/rpki-uploads/economy-adoption.csv

IPv4



IPv6



TW, SGの適用率は高い。逆にCN, KRはほとんど登録がない。

JP：IPv4 64.49%, IPv6 82.62%(2024/05/24現在)

© NTT Communications Corporation All Rights Reserved.

もうちょっと日本の状況について調べてみる

広報経路に対するROA登録率を以下の方法で算出

① JPNICが割り当てているAS番号を日本のASとして定義(797AS)
https://www.nic.ad.jp/ja/ip/as-numbers.txt

② ①のASがOrigin ASとなっている経路をRIPE RIS Archive(rrc06/AS4777)から抽出し、これを広報経路として定義
https://data.ris.ripe.net/rrc06/2024.05/bview.20240524.0000.gz

③ ①のASそれぞれに対して、ROA(*)が広報経路のIPアドレス範囲を包含しているか計算し、IPアドレス数で割合を求め、これを**ROAカバー率**とする

例：
AS65000の広報経路：192.168.0.0/23, 192.168.2.0/24
AS65000のROA： 192.168.2.0/24-24-65000
だった場合、ROAカバー率は約33.33%となる

(*)ROAはROAキャッシュサーバ(routinator)を動作させ、routinator vrpsコマンドで抽出
https://github.com/NLnetLabs/routinator

© NTT Communications Corporation All Rights Reserved.

日本のROAカバー率(2024/05/24時点)

IP version	前述) NRO RPKI適用率	ROAカバー率	参考) JPIRRカバー率
IPv4	64.49%	**71.23%**	93.87%
IPv6	82.62%	**83.76%**	99.02%

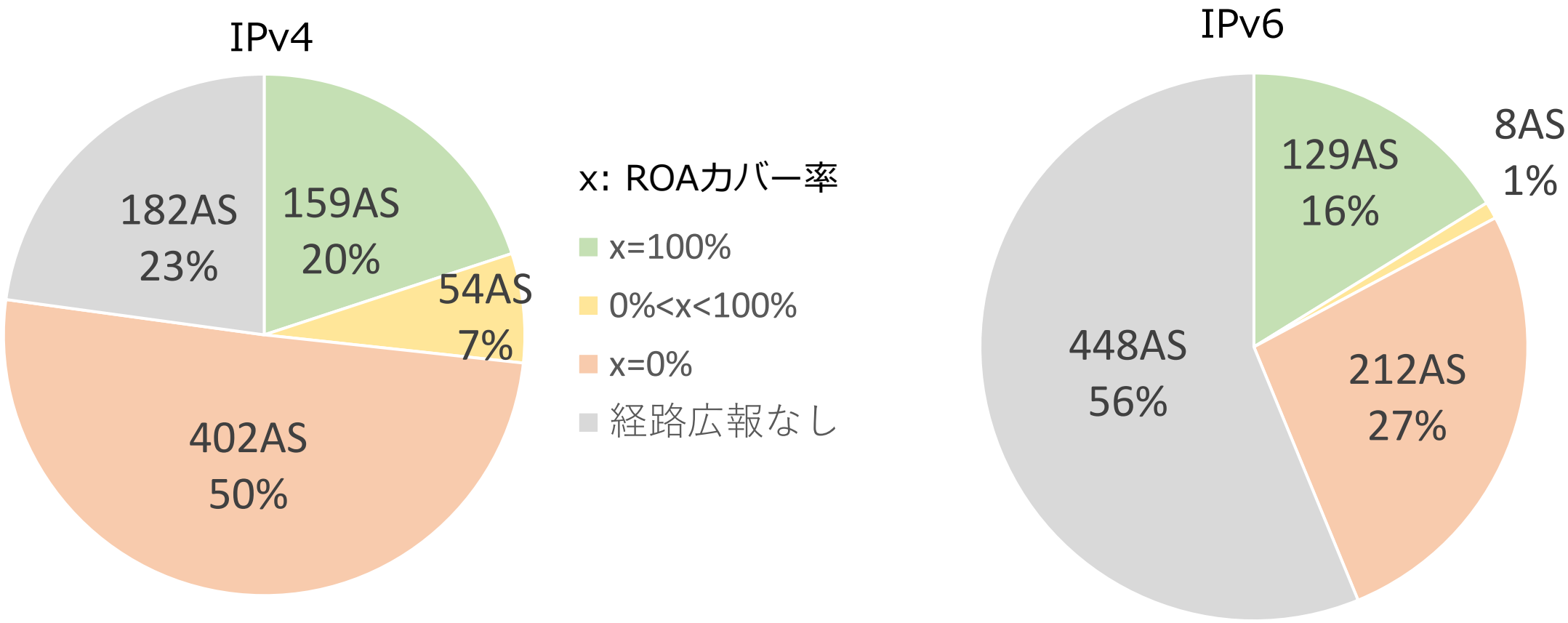
前述のNROのRPKI適用率と若干異なる。
NROのデータは割当アドレス(未広報アドレス含)で計算されていると思われるため割合的には低くなっていると推定。

route/route6 objectを利用して同様の計算方法で算出。
JPIRRのカバー率に比べるとまだ低い。

できれば、JPIRRくらいのカバー率を目指したいです！がんばりましょう！

© NTT Communications Corporation All Rights Reserved.

ASごとのROAカバー率分布



1つでもROAを登録しているASは、IPv4:213AS(27%), IPv6:137AS(17%)
ROAを登録していない経路を広報しているASはまだまだ多い。

© NTT Communications Corporation All Rights Reserved.

このAS番号を管理されている人いますか～？

2515	7672	10019	23778	37900	55391	63786	131921	146980
2518	7684	17530	23779	37904	55392	63791	131923	146981
2527	9371	17682	23805	37908	55898	63795	131925	146984
2915	9374	17683	23816	38631	55900	63797	131929	150359
4685	9607	17931	23831	38639	59105	63799	131934	150369
4721	9617	17948	24229	38644	59125	63800	131964	151371
7511	9621	18144	24259	38648	59127	63801	131965	151381
7521	9622	18259	24271	38651	59128	63806	131976	
7527	9997	18278	24277	45677	63771	131079	131984	
7530	10002	23618	24289	45680	63774	131160	131988	
7660	10011	23775	37892	55385	63776	131161	146974	

IPv4/IPv6ともにROAのカバー率100%を達成しているASです！ 👏

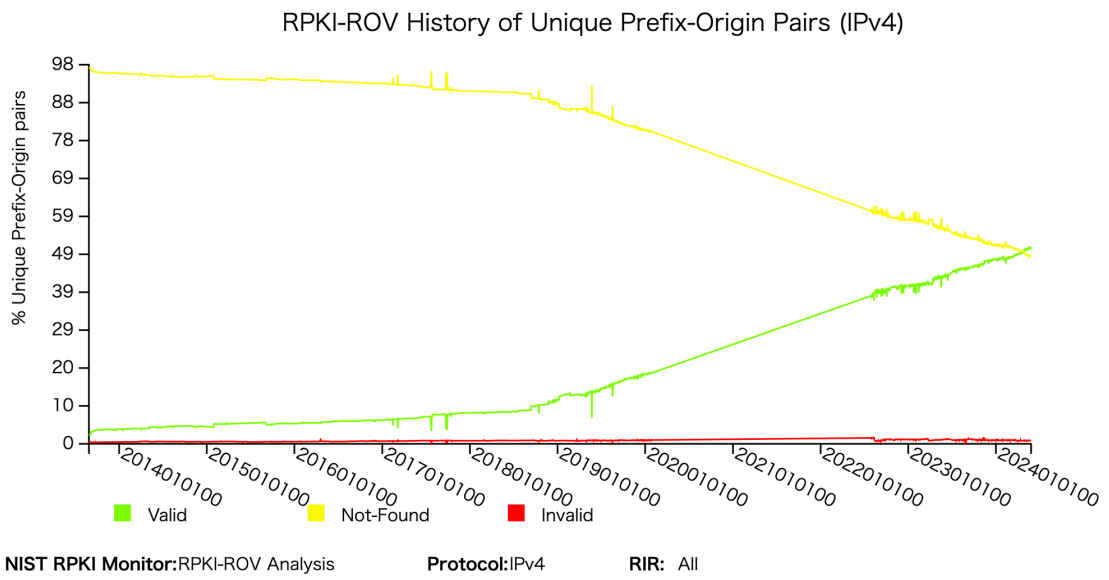
© NTT Communications Corporation All Rights Reserved.

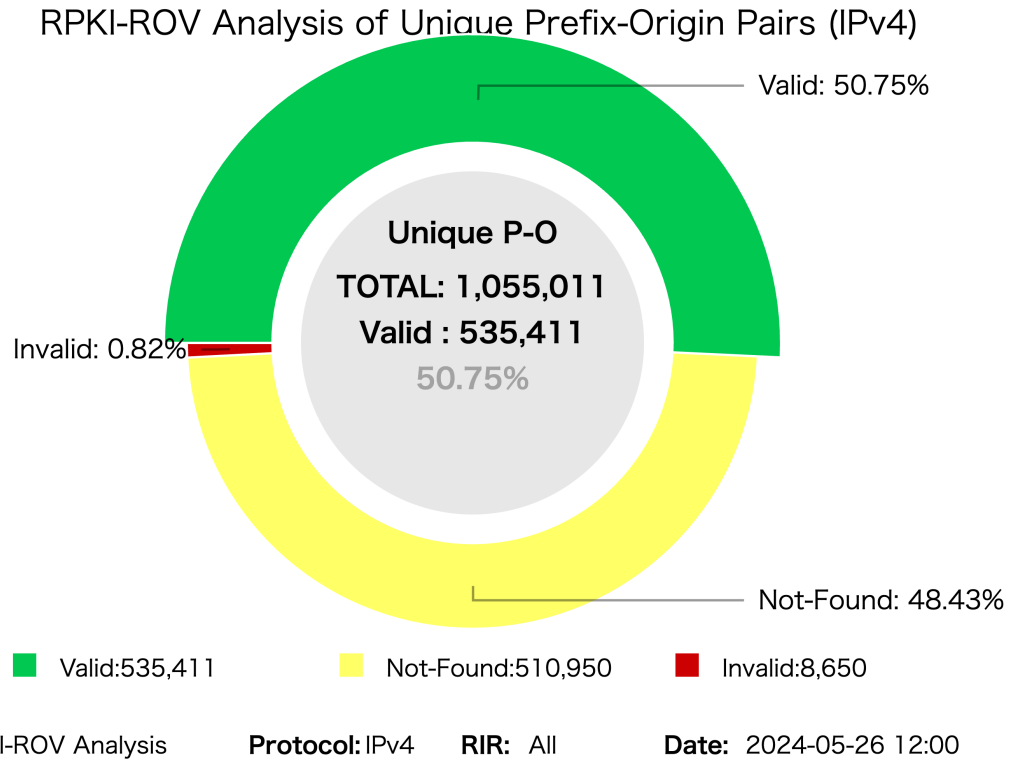
ROV statistics

© NTT Communications Corporation All Rights Reserved.

NIST RPKI Monitor (IPv4)

IPv4のNIST RPKI MonitorでのROV判定率推移と現状
https://rpki-monitor.antd.nist.gov/ROV/



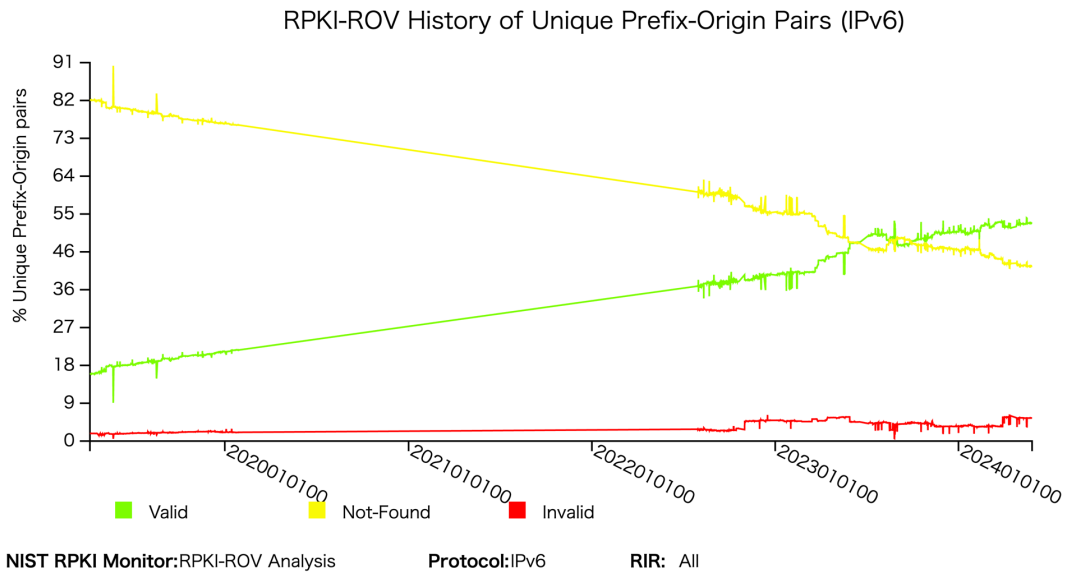


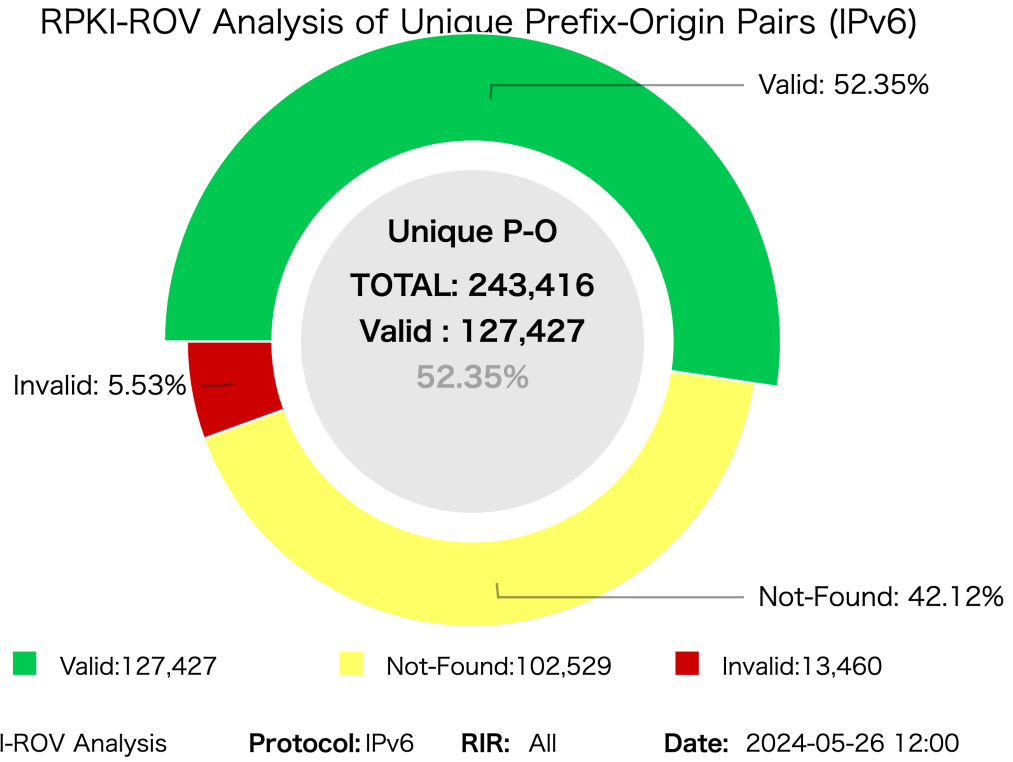
2024/04ごろからIPv4経路がnot-foundよりもvalidの割合が多くなっている。
現在のvalid率は約51%

© NTT Communications Corporation All Rights Reserved.

NIST RPKI Monitor (IPv6)

IPv6のNIST RPKI MonitorでのROV判定率推移と現状
https://rpki-monitor.antd.nist.gov/ROV/





現在のvalid率は約52%

© NTT Communications Corporation All Rights Reserved.

ROV実装状況

cloudflareが提供するサイト
https://isbgpsafeyet.com/
でROVを実装しているASが自己申告制で公開。

- safe
  - Tier1勢(Lumen/Arelion/NTT/Verizon/TATAなど)
  - Microsoft
  - Amazon
  - Netflix

- partially safe
  - Google
  - IIJ
  - OCN

NAME	TYPE	DETAILS	STATUS
Lumen	transit	signed + filtering	safe
Arelion (formerly Telia)	transit	signed + filtering	safe
Cogent	transit	signed + filtering	safe
NTT	transit	signed + filtering	safe
Hurricane Electric	transit	signed + filtering	safe
GTT	transit	signed + filtering	safe
TATA	transit	signed + filtering	safe
Zayo	transit	signed + filtering	safe
PCCW	transit	signed + filtering	safe
RETN	transit	partially signed + filtering	safe
Orange	transit	signed + filtering	safe
Telefonica/Telxius	transit	signed + filtering	safe
Comcast	ISP	signed + filtering	safe
Verizon	ISP	signed + filtering	safe
Liberty Global	transit	signed + filtering	safe
Cloudflare	cloud	signed + filtering	safe
Microsoft	cloud	signed + filtering	safe
Amazon	cloud	signed + filtering	safe
Netflix	cloud	signed + filtering	safe
Wikimedia Foundation	cloud	signed + filtering	safe
Scaleway	cloud	signed + filtering	safe

ROV実装されている方はPull Request出してみては？

© NTT Communications Corporation All Rights Reserved.

その他のトピック

© NTT Communications Corporation All Rights Reserved.

その他のトピック(1/2)

- **RIPEアカウントを乗っ取られ、不正なROAが登録され経路ハイジャックされる(2024/01)**
  https://www.bleepingcomputer.com/news/security/hacker-hijacks-orange-spain-ripe-account-to-cause-bgp-havoc/
  → 安易なID/PW利用。2FAなし。クライアント端末のマルウェア感染によって情報流出。
  JPNICは、クライアント証明書(2年に1度更新)認証。
  とはいえ、端末のセキュリティについてもご注意ください。
  FYI) 上記とは無関係ですが、zscaler(ZIA)経由でのJPNIC ROAWebへの接続不可っぽいのでごにょごにょ必要。

- **JPNIC CA障害(2024/04)**
  https://www.nic.ad.jp/ja/topics/2024/20240416-01.html
  →JPNICのCA(rpki-repository.nic.ad.jp)がダウンし、ROAキャッシュサーバからのアクセスが不可になり、証明書/ROAのダウンロードができなくなった。
  JPNICさん、がんばって！

© NTT Communications Corporation All Rights Reserved.

その他のトピック(2/2)

- **LACNIC CAリプレース(2024/04)**
  https://www.lacnic.net/7148/2/lacnic/migration-to-lacnics-new-rpki-system
  →LACNICのCAがリプレースされました。
  versionの古いROAキャッシュサーバを使っていると、LACNICからのROAを検証できたりできなかったりする事象を確認。
  ROAキャッシュサーバのversionが古いまま運用されている場合はご確認を。

- **米国でのBGPセキュリティ規制化？(2024/05)**
  https://docs.fcc.gov/public/attachments/FCC-24-52A1.pdf
  https://docs.fcc.gov/public/attachments/DOC-402579A1.pdf
  →昨今の米国での経路ハイジャックによるセキュリティインシデントの対策として、米FCCが、
  ・すべてのBIAS(Broadband Internet Access Service)事業者に対し、RPKIの導入計画や進捗を記述した「BGP Routing Security Risk Management Plans(BGP Plans)」を作成すること
  ・上位9社のサービスプロバイダーに対し、四半期ごとに公開データを提出すること
  を求める。
  日本はどうなるんでしょう？ドキドキですね…。

© NTT Communications Corporation All Rights Reserved.

ご清聴ありがとうございました

© NTT Communications Corporation All Rights Reserved.