

ROAキャン△旅のしおり ～RPKIの概要といま～

JPNIC 技術部 花井直樹

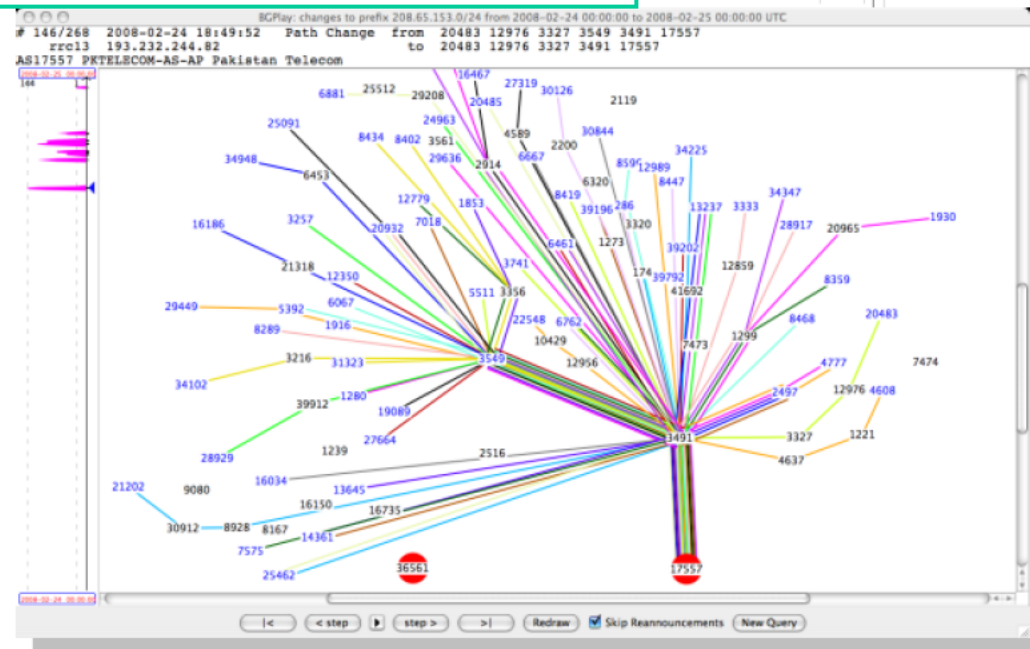
RPKIとは - RPKIでできること

RPKIでできること

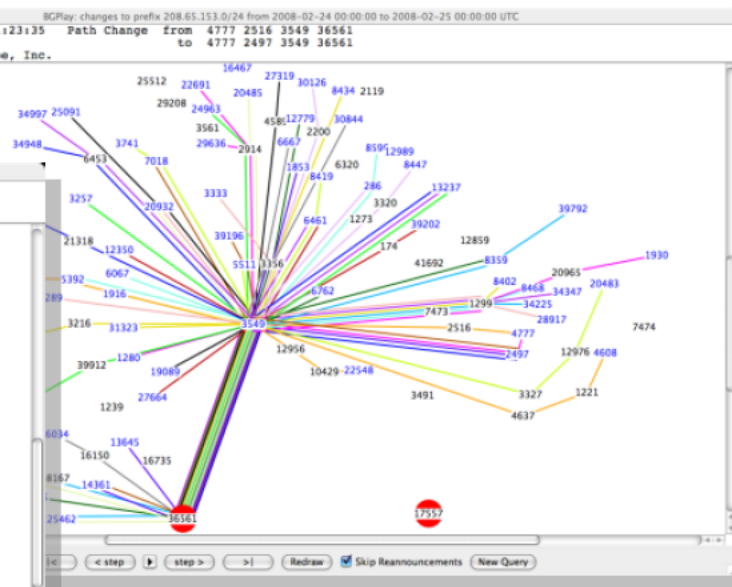
- **ROAを使ってインターネット上の不正なBGP経路を検知できる**
 - ここでいう「不正な」とは = オリジンASが異なること
 - 世界のどこかで発生した不正経路を検知できる！

2008年のYouTubeインシデント

インシデント発生時



平常時



YouTube Hijacking: A RIPE NCC RIS case study, 17 Mar 2008, RIPE NCC,
<http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>

**YouTubeの経路情報が別のASによって広告され、
約2時間半の間、アクセスできなくなった。**

8.8.8.0/24



BGPStream About Contact

Possible BGP hijack

Beginning at 2016-01-21 13:25:35 UTC, we detected a possible BGP hijack.

Prefix 8.8.8.0/24, is normally announced by AS15169 Google Inc..

But beginning at 2016-01-21 13:25:35, the same prefix (8.8.8.0/24) was also announced by ASN 34329.

This was detected by 3 BGPMon peers.

Expected

Start time: 2016-01-21 13:25:35 UTC

Expected prefix: 8.8.8.0/24

Expected ASN: 15169 (Google Inc.)

Event Details

Detected advertisement: 8.8.8.0/24

Detected Origin ASN 34329 (OMZ-IT LLC)

Detected AS Path 20632 34329

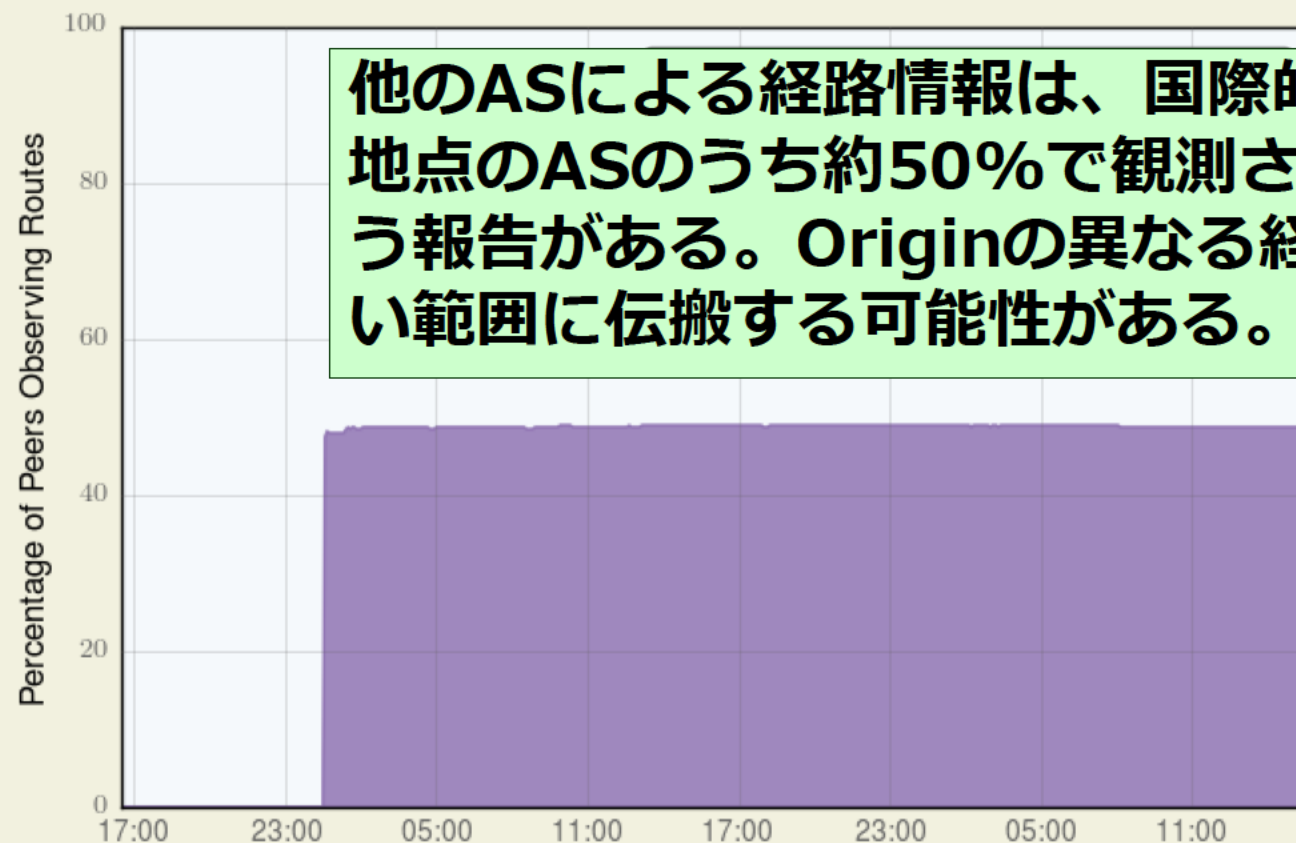
Detected by number of BGPMon peers: 3

**Googleパブリックキャッシュサーバ
のアドレスを別のASが広告していた
という報告**

BGPStream Event #17605
<https://bgpstream.com/event/17605>

Origination of 46.244.81.0/24 (Mada Network)

07 Jan 2015 - 09 Jan 2015 (Times in UTC)



他のASによる経路情報は、国際的な観測地点のASのうち約50%で観測されたという報告がある。Originの異なる経路も広い範囲に伝搬する可能性がある。

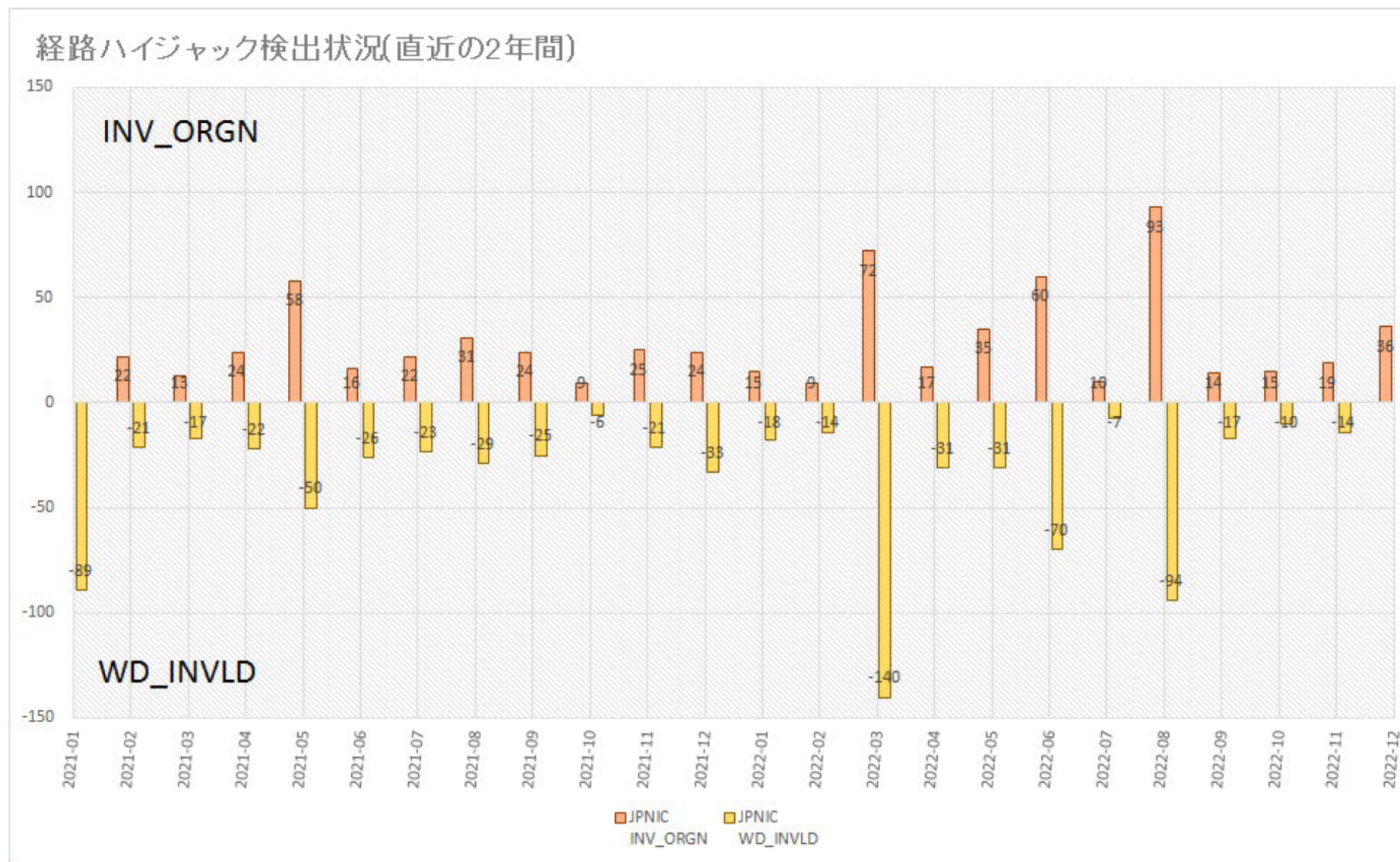
Source: BGP Data



On-going BGP Hijack Targets Palestinian ISP, Apr 10, 2015, Dyn Research
<http://research.dyn.com/2015/01/going-bgp-attack-targets-palestinian-isp/#!prettyPhoto>

国内における観測

AS番号が本来とは異なる疑いのある経路情報が観測されている
(JPIRRの登録情報との比較)



なぜHijackingが起こるのか

- **prefix違い**
 - origin ASとprefixの組み合わせが、正しいのかどうか分からない。従ってルーターでその経路情報を無視すべきかどうか分からず、伝播していつてしまう。
- **AS番号違い**
 - ある経路情報のorigin ASが本当にそのAS番号を使ってよいASなのかどうか分からない。（同上）
- **AS_PATH違い**
 - ある経路情報のAS_PATHがオペレーターが正しいと思っているトポロジーと一致しているのかどうか分からない。（よく見ると怪しさを感じることも）

RPKI

- **Resource Public-Key Infrastructure**
 - IPアドレスやAS番号といった番号資源（Number Resource）の割り振り／割り当てを証明するPKI

リソース証明書に記載されたIPアドレスなどが
レジストリによって分配されたものなのかが確認できる。

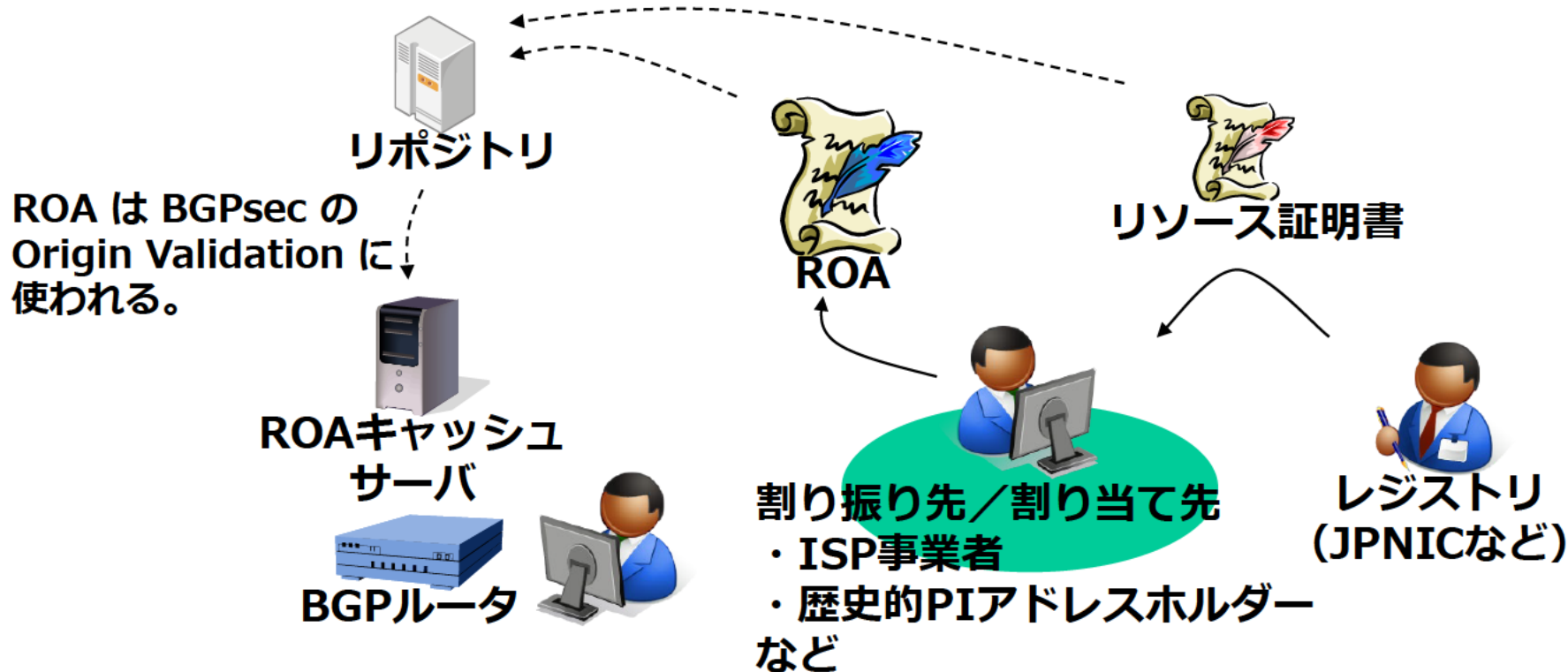


ROAが“正しい”分配先によって発行されたものかどうかの
確認ができる。

ROA

- **Route Origination Authorization**

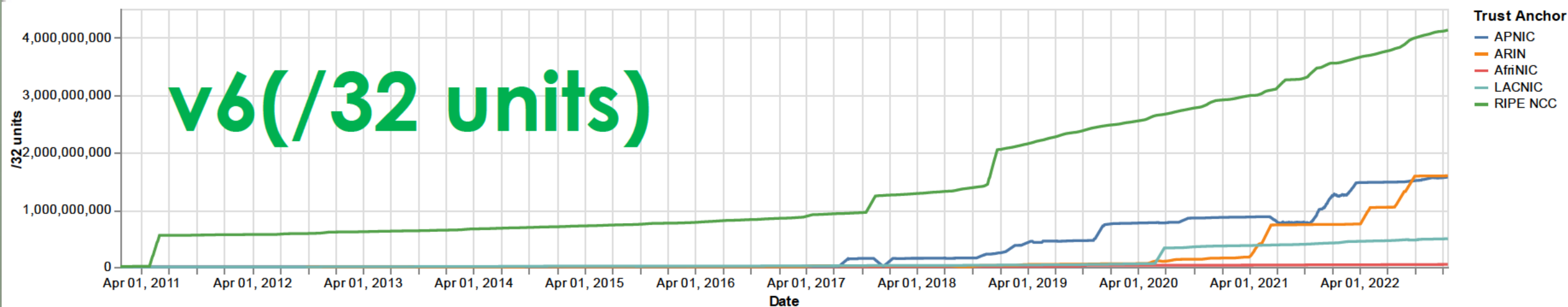
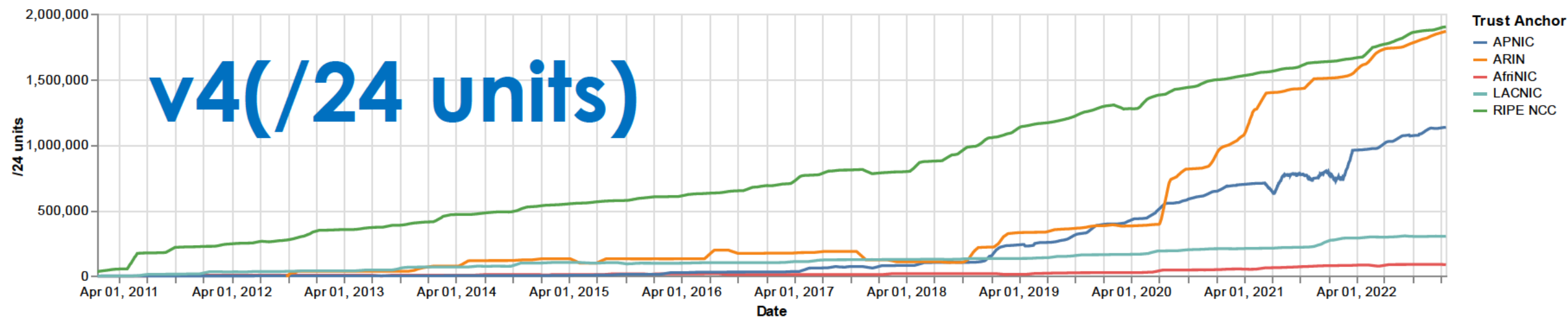
- IPアドレスのホルダーによる署名付きデータで、割り当てられたIPアドレスの経路広告を特定のASから経路広告することを認可したことを示す



RPKIの普及状況

RPKI 普及状況 (RIRごと／アドレス空間)

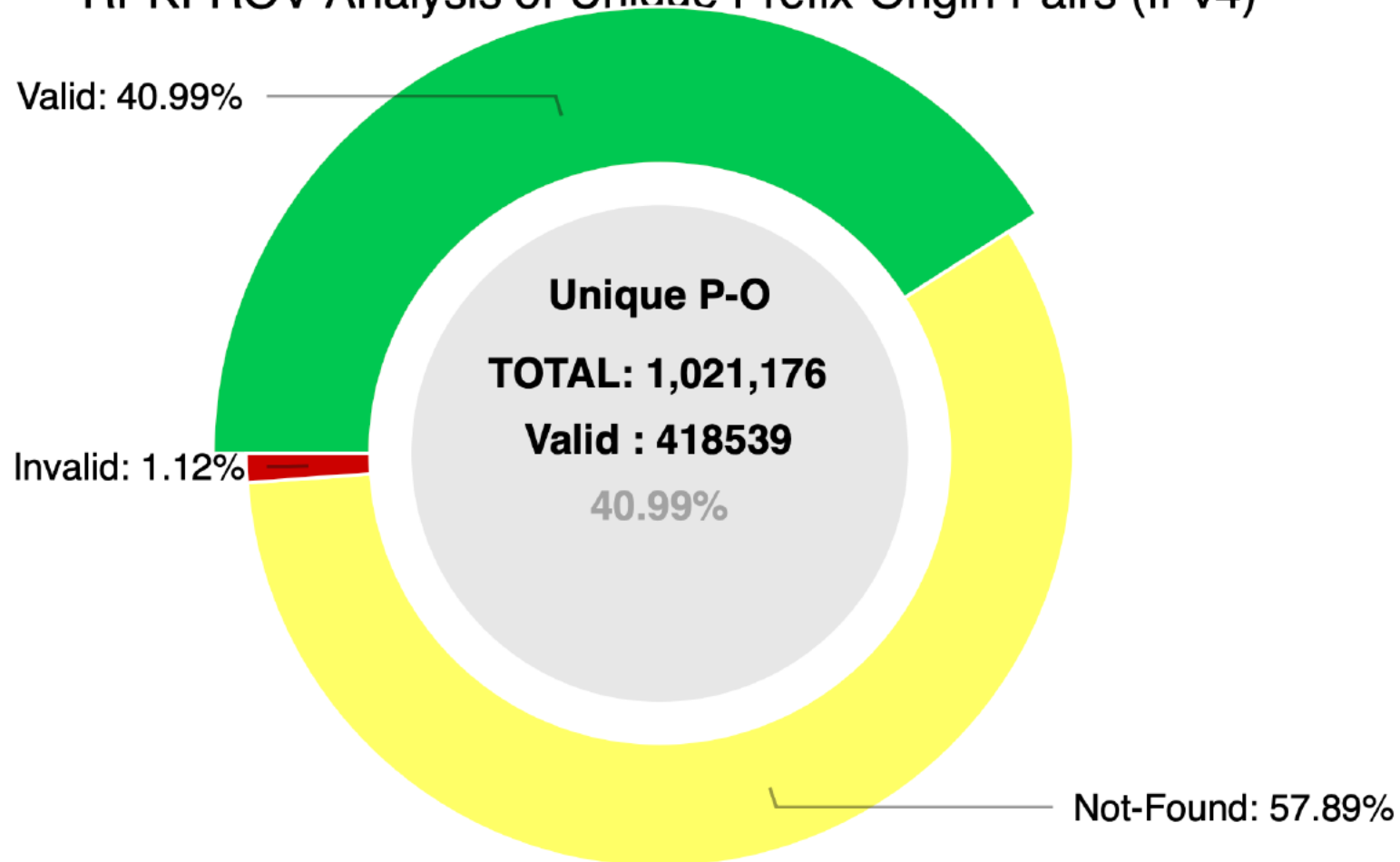
<https://certification-stats.ripe.net/>



観測状況 (全RIR/IPv4)

<https://rpki-monitor.antd.nist.gov/ROV>

RPKI-ROV Analysis of Unique Prefix-Origin Pairs (IPv4)



Valid:418,539

Not-Found:591,184

Invalid:11,453

2023/1/17 取得

国内RPKI利用者数とカバー率

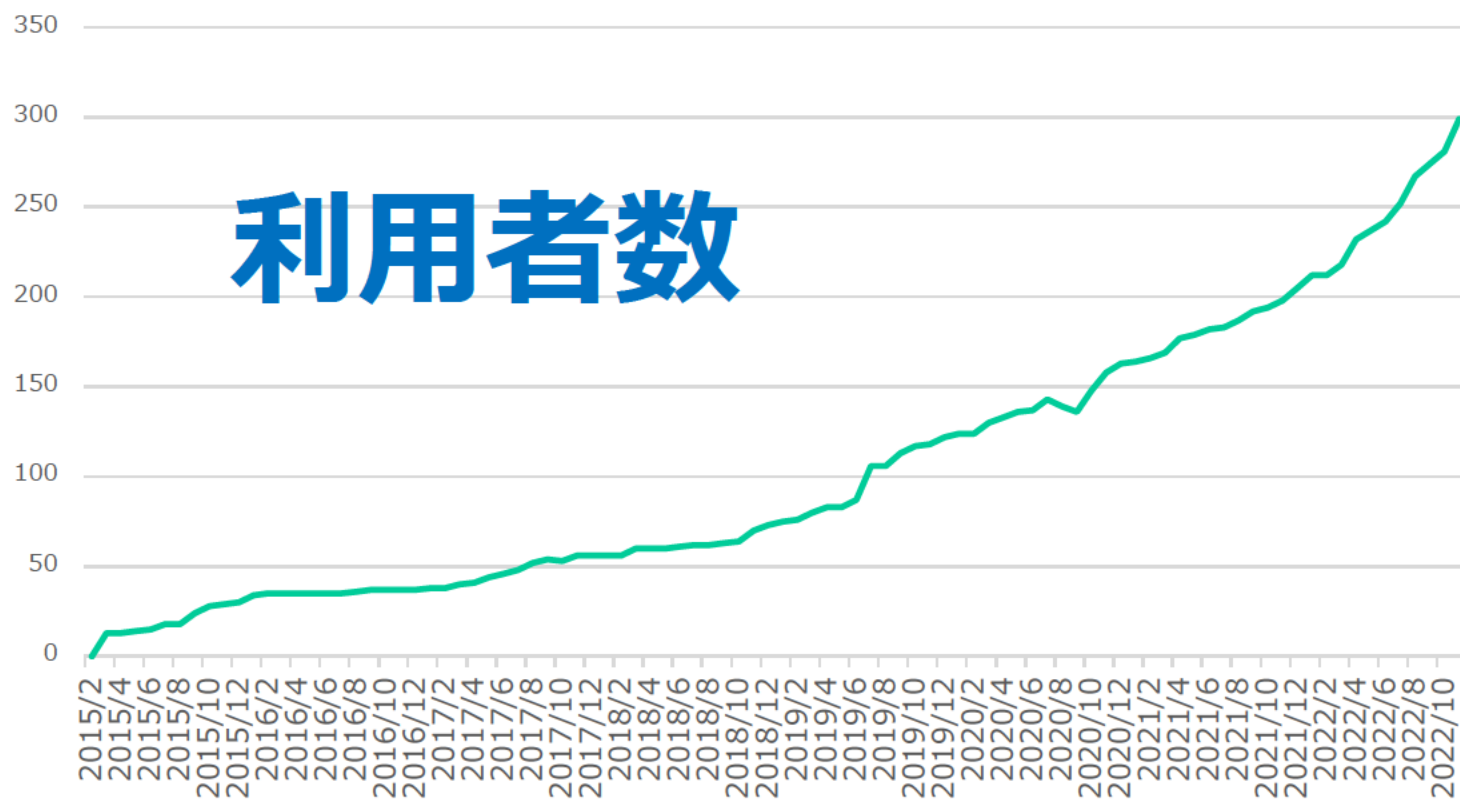
- **利用者数（資源管理情報数 - IPv4とIPv6等別にカウント）**

- 299

- **ROAのカバー率**

- IPv4(アドレス数) 74.4%

- IPv6(/48数) 71.7%



RPKI 近年の状況

Microsoft が最近ROVを開始。

国際的な通信事業者でROVの導入が進む

- Microsoft (AS8075): ROVの展開を全てのピアに対し開始 (2022 年 10 月)

<https://corporate.comcast.com/stories/improved-bgp-routing-security-adds-another-layer-of-protection-to-network>

- NOS Comunicações (AS2860) : ROAを発行し、invalidな経路をドロップ (2021年7月)

<https://isbgpsafeyet.com>

- AWS(AS16509) : ROAを発行し、RPKI ROVを展開 (2021 年 1 月 14 日)

<https://aws.amazon.com/jp/blogs/networking-and-content-delivery/how-aws-is-helping-to-secure-internet-routing/>

Is BGP **safe** yet? *No.*

<https://isbgpsafeyet.com/>

Status

Displaying 31 major operators

+ Show all

+ Show ASN column

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
PCCW	transit	signed + filtering	safe
RETN	transit	partially signed + filtering	safe
Orange	transit	signed + filtering	safe
Comcast	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
Telstra International	transit	signed	partially safe
AT&T	ISP	signed + filtering peers only	partially safe
Google	cloud	signed	partially safe

Invalid な経路の扱いは……？

Please to say Vocus AS4826 is now dropping all invalid ROAs as of this morning. Another step towards routing security. #rpki #apnic

[ツイートを翻訳](#)

午前11:02 · 2021年3月16日

AS4826

<https://twitter.com/pmawson/status/1371642968512237569>

We are dropping RPKI invalids in 100% of our Internet Edge Border, in over 400+ global PoPs since December 2020.

AS16509 AWS

https://storage.googleapis.com/site-media-prod/meetings/NANOG86/4602/20221017_Robachevsky_Internet_Routing_And_v1.pdf

RPKI

T-Mobile filters all RPKI Invalid routes from settlement-free peers and customers.

最新トピック

RPKIを利用したASパス検証の有効性を示す

2023年1月16日

各位

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

RPKIを利用したASパス検証の有効性の高さに関する論文がIEEE論文誌に採録

情報通信分野の国際会議IEEE^{*1}による「Open Journal of the Communications Society^{*2}」は、電気通信システムとネットワークの最先端技術の進歩に関する論文を掲載するジャーナルです。そのジャーナルに、当センター職員が共著した論文が採録されましたので、お知らせします。この論文は、RPKIを利用したBGPのセキュリティ技術である「ASパス検証(ASPA^{*3})」について、不正経路対策としての効果の高さを示したものです。

*1 <https://www.ieee.org/> 

*2 <https://www.comsoc.org/publications/journals/ieee-ojcoms> 

*3 ASPAはASの並び(隣接するAS)の正しさを示し、ルートルークなどを引き起こす正しくないBGP経路が広がるのを止めることができる技術。

<https://www.nic.ad.jp/ja/topics/2023/20230116-01.html>

- ASPAはRPKIを使ったBGPのセキュリティ技術
- ASPAを使った経路の検証技術が部分的にしか導入されていない状態でも、効果を発揮できることをシミュレーションを通じて実証

RPKI有識者検討会資料1

事業概要

実施計画説明資料(概要版)

令和4年度 ISPにおけるネットワークセキュリティ技術の導入に関する調査の請負

2023年1月17日

NTTコミュニケーションズ株式会社
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
株式会社三菱総合研究所

実証実験プロジェクト

(令和4年度 ISPにおけるネットワークセキュリティ技術の導入に関する調査の請負 事業概要より)

2. 調査概要 (4/12) (②認証技術等の導入における技術的課題の調査)



■ [1] 経路ハイジャック抑止となる経路認証技術 (RPKI等) の実証環境全体イメージ

