ROA作成体験記

- ENOG87 Meeting -

ハロー！！
RPKIのマスコット
ケーロちゃんダヨ！

2025年8月22日

株式会社グローバルネットコア

金子 康行

GLOBAL NET CORE

https://www.global-netcore.jp/

今日お話しすること

- 2025年4月、弊社が管理するIPアドレス資源に対応するROA（Route Origin Authorization）を作成しました
- ROA作成自体はそう難しい作業ではありませんが、実際にやってみて、いろいろと思うところがありました…
- 本日はその「いろいろと思うところ」について、ざっくばらんにお話ししたいと思います

自己紹介

・金子康行 （かねこやすゆき）

- 株式会社グローバルネットコア　常務取締役
- 一般社団法人日本インターネットプロバイダー協会　監事
- 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　評議委員
- 越後ネットワーク・オペレーターズ・グループ　運営委員

- 歌舞伎や文楽など、日本の伝統芸全般が好き
- 美味しいお酒と美味しい食べ物が好き

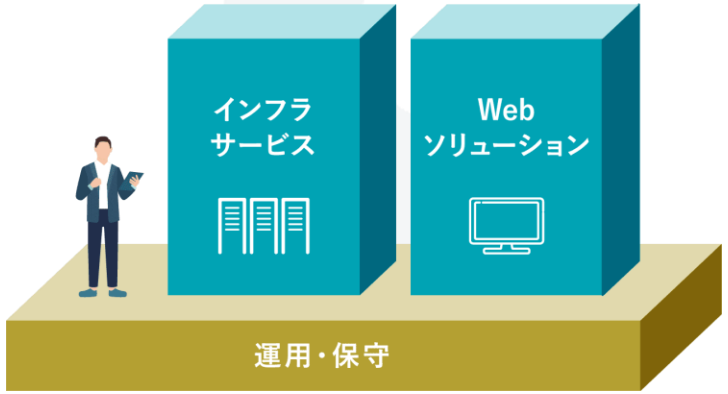
グローバルネットコアとは

インフラサービス

Webソリューション

運用・保守

セキュリティ



すべてを一気通貫で提供する ITソリューションカンパニー です。




新潟県内初のAWSサービスパートナー

新潟県初 !!

新潟県本社所在企業として初のパートナー認定取得

・クラウドインフラの設計・構築・運用支援
・サービスのリセール（請求代行）
・DirectAccess専用回線接続提供
・Webシステム設計・開発

aws PARTNER Select Tier Services

aws 50 CERTIFIED

AWS認定資格保有者が多数在籍（のべ67名）

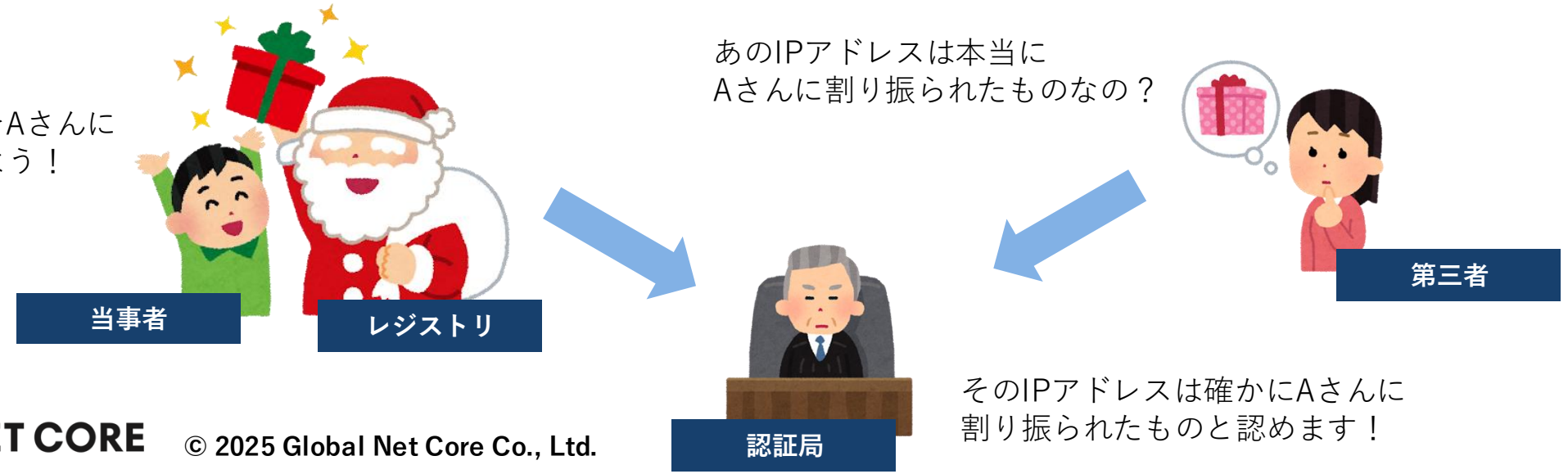
・Solutions Architect Professional
・DevOps Engineer Professional
・Advanced Networking Specialty
・Machine Learning Specialty
・Security Specialty　など

RPKIの概要

RPKIとは？

- **リソースPKI（RPKI）は、 アドレス資源の割り振りや割り当てを証明するためのPKI（Public-Key Infrastructure：公開鍵基盤）**である

- IPアドレスの割り振りや割り当てを証明する**リソース証明書（Resource Certificate）と呼ばれる電子証明書**は、RPKIを使って発行される



ROAとは？

- アドレス資源の割り振りや割り当てを受けた組織は、リソース証明書を利用することで、**IPアドレスとAS番号の正しい組み合わせを示すデータ、Route Origin Authorization（ROA）**を生成することができる

- AS運用者は、**BGPルーターで受信した経路情報が誤った内容（Mis-Origination）であるか否か**を、ROAを参照し比較することによって検証することができる

IPアドレス[X]の
Origin ASは[A]だよ
RPKIを使ってROAを作成するよ

AS A

BGPで経路
情報を送るよ

AS B

この[X]と[A]の組み合わせって
本当に正しいのかな？

ROA証明書
[X]:[A]

リポジトリ

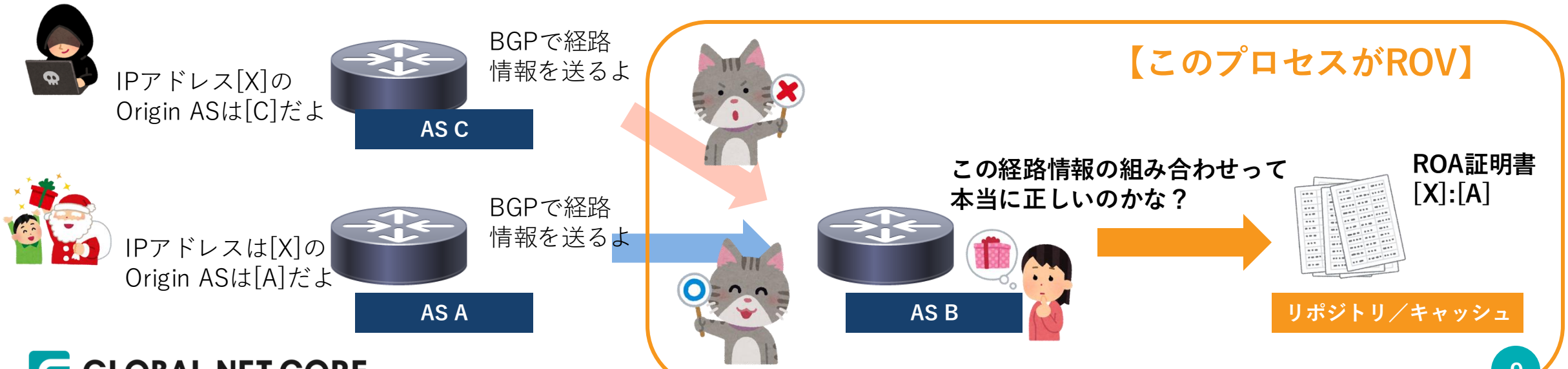
認証局

確かにXを割り振られたAさんからの申請なので署名するぞい

ROVとは？

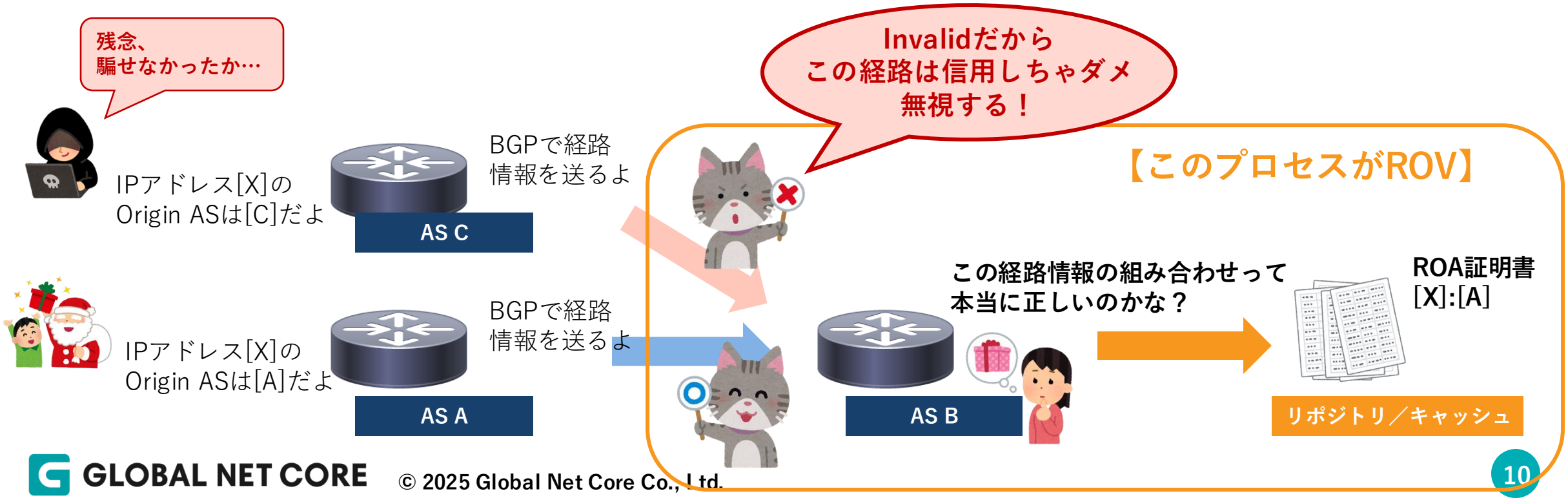
- BGPルータで**ROAと経路情報の比較・検証を行うことを、Route Origin Validation（ROV）**と呼ぶ

- ROVにより経路情報は、**Valid（ROAと整合）**、**Invalid（ROAと不整合）**、**Not Found（ROAが存在しない）**、の3種類に区分けされる



ROVに基づく経路情報処理

- ROVの結果を元に、**Valid経路の優先度を上げる**、**Invalid経路を無視する**、といった処理をルータで実施することにより、**誤った経路情報に起因する通信障害を防止する**ことができる

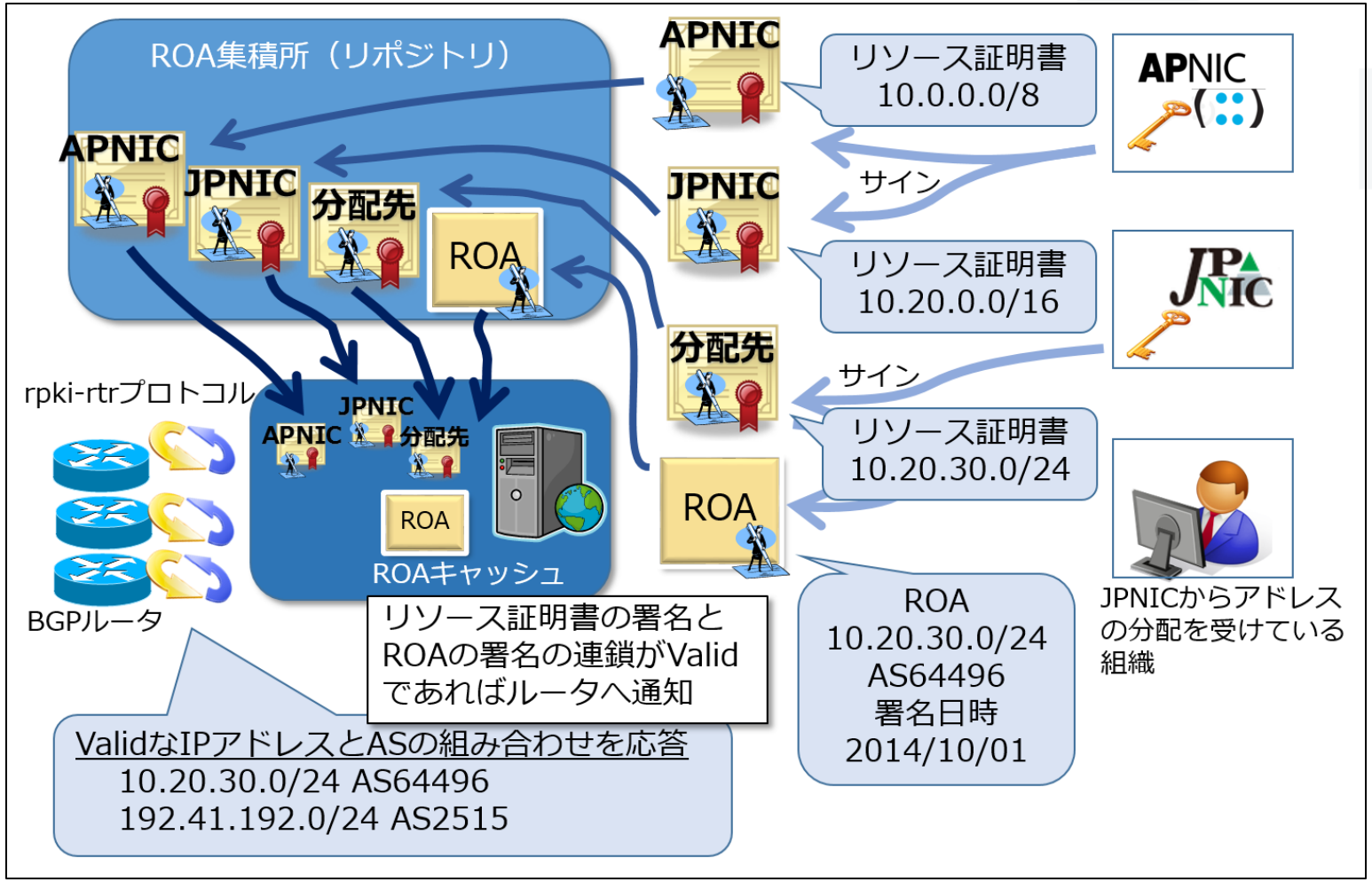


RPKIの全体像

ROAは各レジストリが管理するリポジトリに保管されます

各リポジトリの情報を収集し、ルータからの問い合わせに応答する役割を担うのはROAキャッシュです

ROAキャッシュは一般公開されているものもあれば、独自に構築運用することもできます



https://www.nic.ad.jp/ja/rpki/

過去のENOGでのRPKI関連発表

- **ENOG20（2013年4月、木村さん・岡田さん）**
  - RPKI チュートリアル & ハンズオン ～ ROA 発行からルータでの参照まで～
- **ENOG46（2017年8月、川端さん）**
  - 祝！RPKIがAPNICとつながりました！
- **ENOG66（2021年2月、木村さん）**
  - RPKIトピック 2020
- **ENOG81（2024年2月、木村さん）**
  - RPKI/DNSSEC/DMARCと越後
- **ENOG85（2025年2月、塩沢さん）**
  - RPKIガイドラインとROVの効果検証 ～RPKIのはじめの第一歩～

JPNICのみなさん、いつもありがとうございます！！

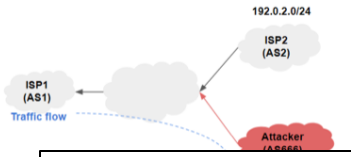
ENOG85、塩沢さんの発表

https://enog.jp/archives/3045

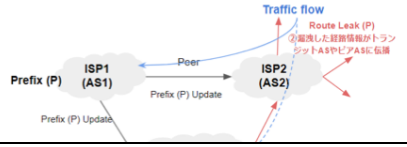
RPKIガイドラインとROVの効果検証 ～RPKIのはじめの第一歩～

代表的なルーティングインシデント

・Mis-Origin

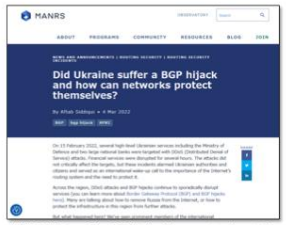


・ルートリーク



代表的なルーティングインシデント

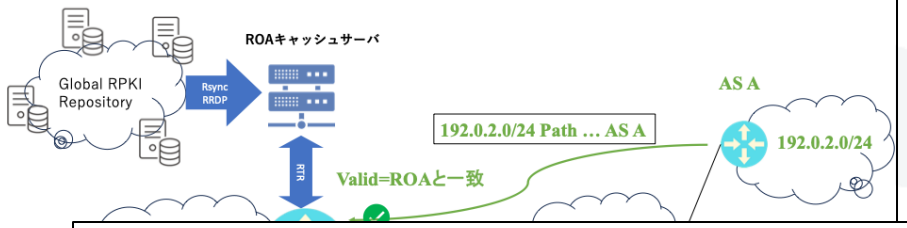
- 1997年 米国にあるISP事業者によるルートリーク発生。多数の不到達。
- 2008年 YouTubeへの到達性が一時的に失われる。
- 2013年 米国国内の経路が外国経由になっていたことが分かる。
- 2014年 ビットコイン・マイニングプールに対する不正経路/不正サーバ
- 2018年 クラウドサービスに対する不正経路発生。MyEtherWalletの偽サイトへ誘導される。
- 2022年 ロシアにあるASよりオリジンASの異なるBGP経路が観測される（ブログ記事）
- 2023年 不正経路の影響で、ミャンマーにおけるX/Twitterへのアクセスができなくなる。



(出典) Did Ukraine suffer a BGP hijack and how can networks protect themselves? - MANRS, https://manrs.org/2022/03/did-ukraine-suffer-a-bgp-hijack-and-how-can-networks-protect-themselves/

(出典) ロシアISPによる Twitter経路ハイジャックの影響調査, 岩間 拓矢, JANOG 51 LT, NTT コミュニケーションズ https://www.janog.gr.jp/meeting/janog51/wp-content/uploads/2023/01/janog51-it-toma-1.pdf

ROV Filtering



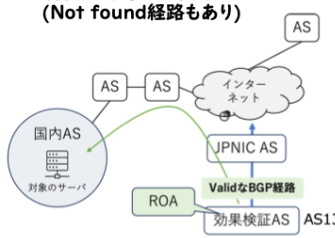
RPKIのガイドラインを発行しました！

- 「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」
  - RPKIの導入・運用を円滑に進めるための手順と指針を包括的にまとめている
  - 総務省の調査研究や実証実験(*)の結果や有識者の意見、JANOGなどのインターネット運用コミュニティからのフィードバックを反映
  - 経営者から技術者まで幅広く活用できる実践的な内容
- 2024年11月、JPNICのWebサイトで公開
  - *https://www.nic.ad.jp/ja/rpki/guideline/*

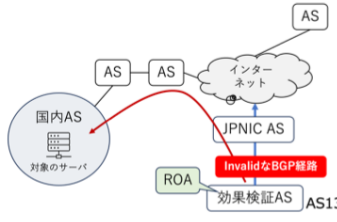
RPKI効果検証

- ValidとなるROAと、あえてROVの結果Invalidとなるようなオリジンが異なる検証用ROAを作成
- 効果検証用AS（AS131971）からValidとなるBGP経路、InvalidとなるBGP経路、NotFoundとなる経路を広告し、ROVによる到達生の違いを確認

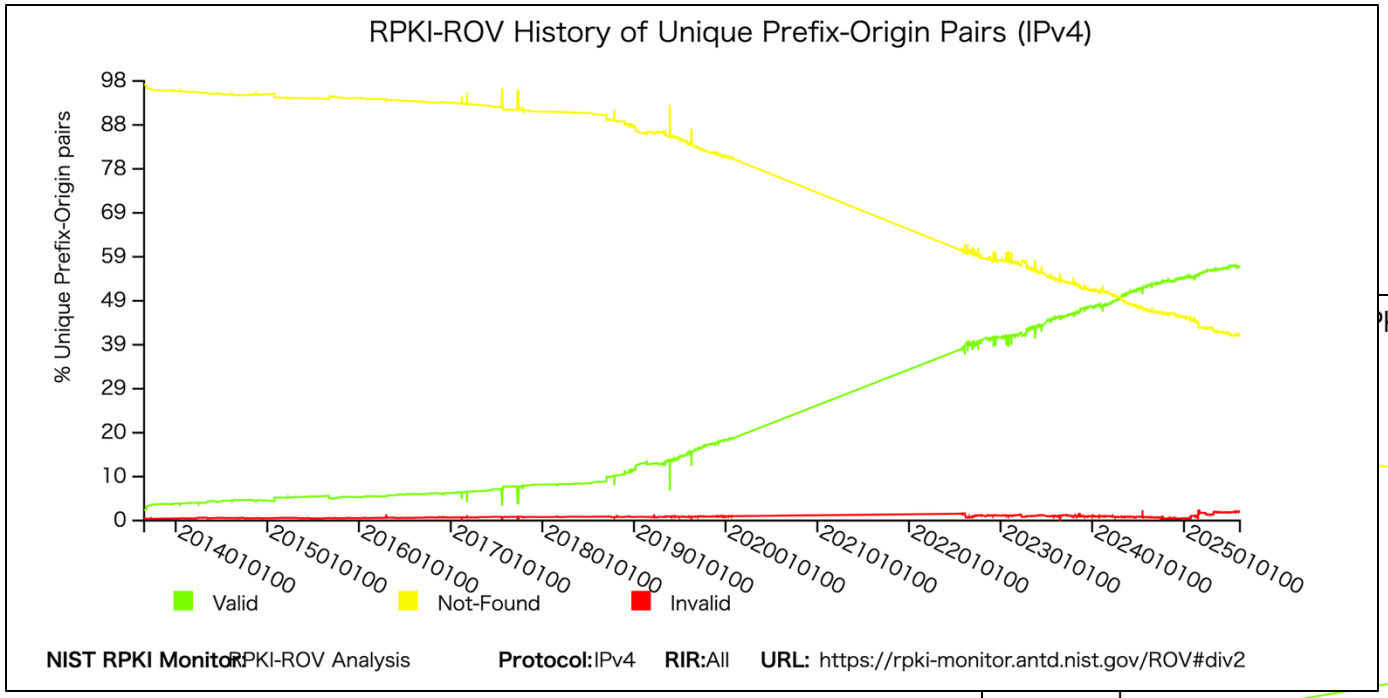
Step 1 - Valid経路で到達性を確認
⇒ 現状の到達性を確認
(Not found経路もあり)



Step 2 - Invalid経路で到達性を確認
⇒ 到達できなければOK (ROVで守られている)
⇒ 到達できるとNG (不正経路の影響を受けている)

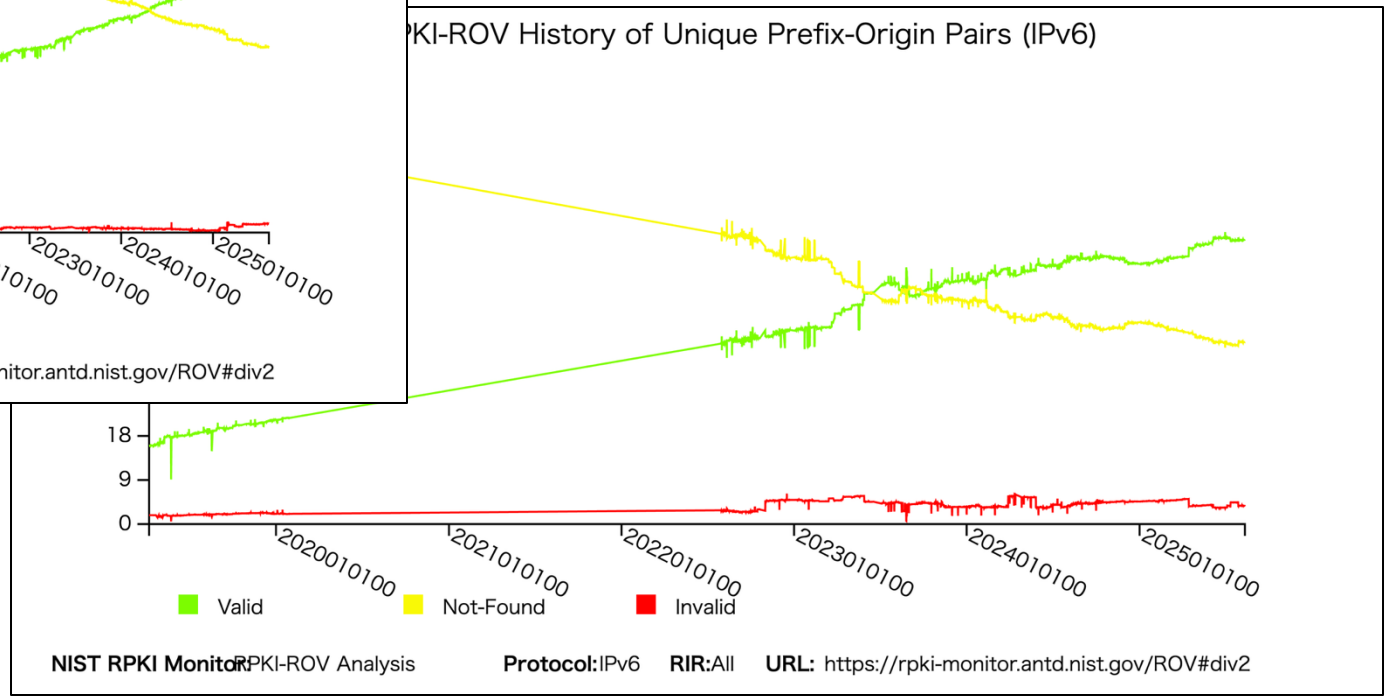


RPKIの普及率（ROA発行、推移）



Global

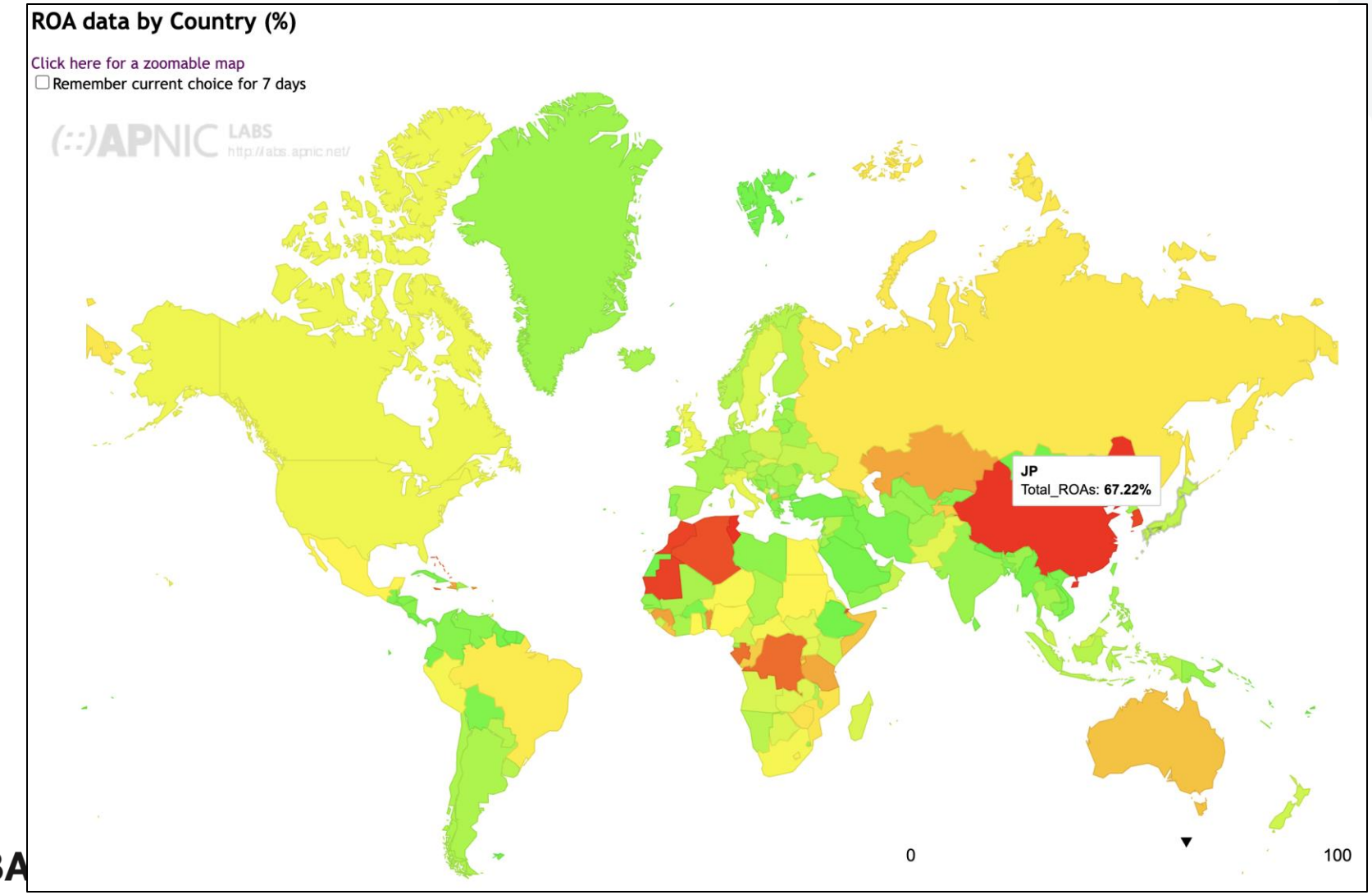
IPv4	56.5%
IPv6	58.6%



https://rpki-monitor.antd.nist.gov/

RPKIの普及率（ROA発行、国別）

https://stats.labs.apnic.net/roas

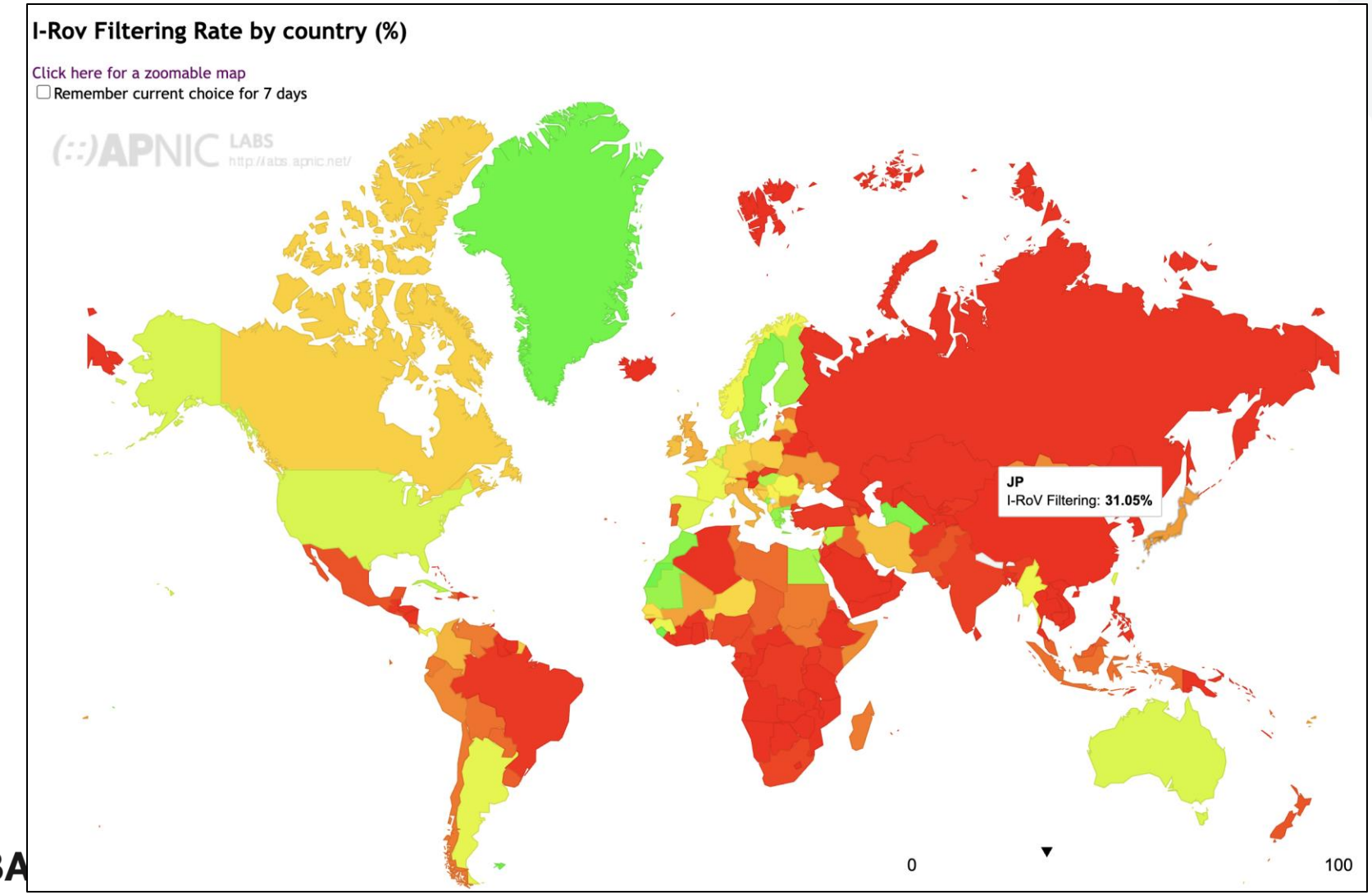


Japan

IPv4	58.06%
IPv6	76.37%

RPKIの普及率（ROV実施、国別）

https://stats.labs.apnic.net/roas

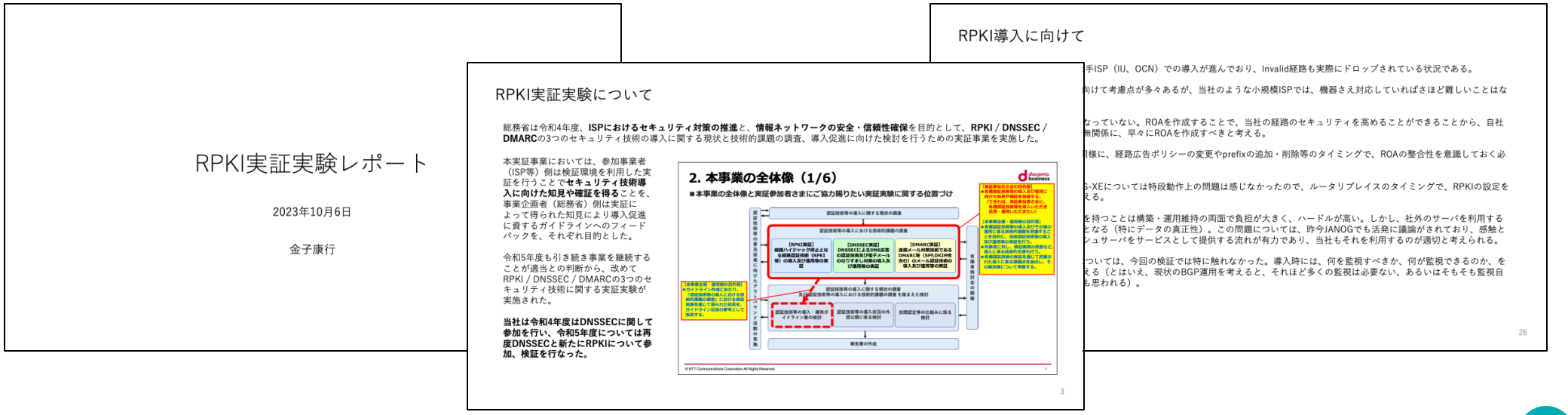


Japan
31.05%

ROA作成作業の実際（フムフム編）

2023年10月、RPKI検証を実施

- 2023年に、**総務省セキュリティ技術導入実証実験**に参加
  - 検証環境を利用し、RPKIの設定や動作について検証作業を実施
  - RPKIへの理解を深めるとともに、技術的な課題についても確認
  - **ROA作成については、早々に実施すべきとの結論を出す**
  - ROV導入については、ルータの更新時期に改めて判断することに



2025年4月、ROA作成作業を実施

- **目的と概要（作業計画書に記載）**
  - インターネット上での不正経路対策として、当社がJPNICより分配を受け、経路広告しているIPアドレスのプレフィックスに対して、ROA（Resource Origin Authorization）を作成する。
  - **ROAを作成することで、当社が広告する経路が真正であることが検証可能となり、ROV（Resource Origin Validation）を実施しているネットワークにおいては、不正経路流入による被害を防止することができるようになる。**
  - 今回、当社はROAを作成するのみであり、当社ルータにおけるROVは実施しない。ROVの実施については、ルータのハードウェアおよびソフトウェアが対応し、運用の準備が十分にできてから改めて検討するものとする。

実際に作成したROA

- IPv4
  - 103.215.84.0/22　18070
  - 117.102.168.0/21　18070
  - 117.102.168.0/24　55895
  - 210.158.160.0/20　18070
  - 218.223.32.0/20　18070
  - 221.120.168.0/21　18070
- IPv6
  - 2400:e000::/32　18070
  - 2400:e000:105::/48　55895

IPv4/IPv6とも、以下の条件でROAを作成

- 当社が割り振りを受けている全てのIPアドレスをカバー
- 実際にBGPで広告している経路と完全一致

※Echigo-IXに割り当てたprefixはAS55895をoriginとして経路広告している

ROA作成手順

- **作業前状態確認**
  - ping、traceroute
  - Looking Glass、RPKI Validator
- **ROA作成**
  - JPNIC RPKIシステム
- **作業後状態確認**
  - ping、traceroute
  - Looking Glass、RPKI Validator

Looking Glass - Telia

https://lg.telia.net/

ROVの結果がわかりやすく表示されて便利！！
（この例ではNot Found）

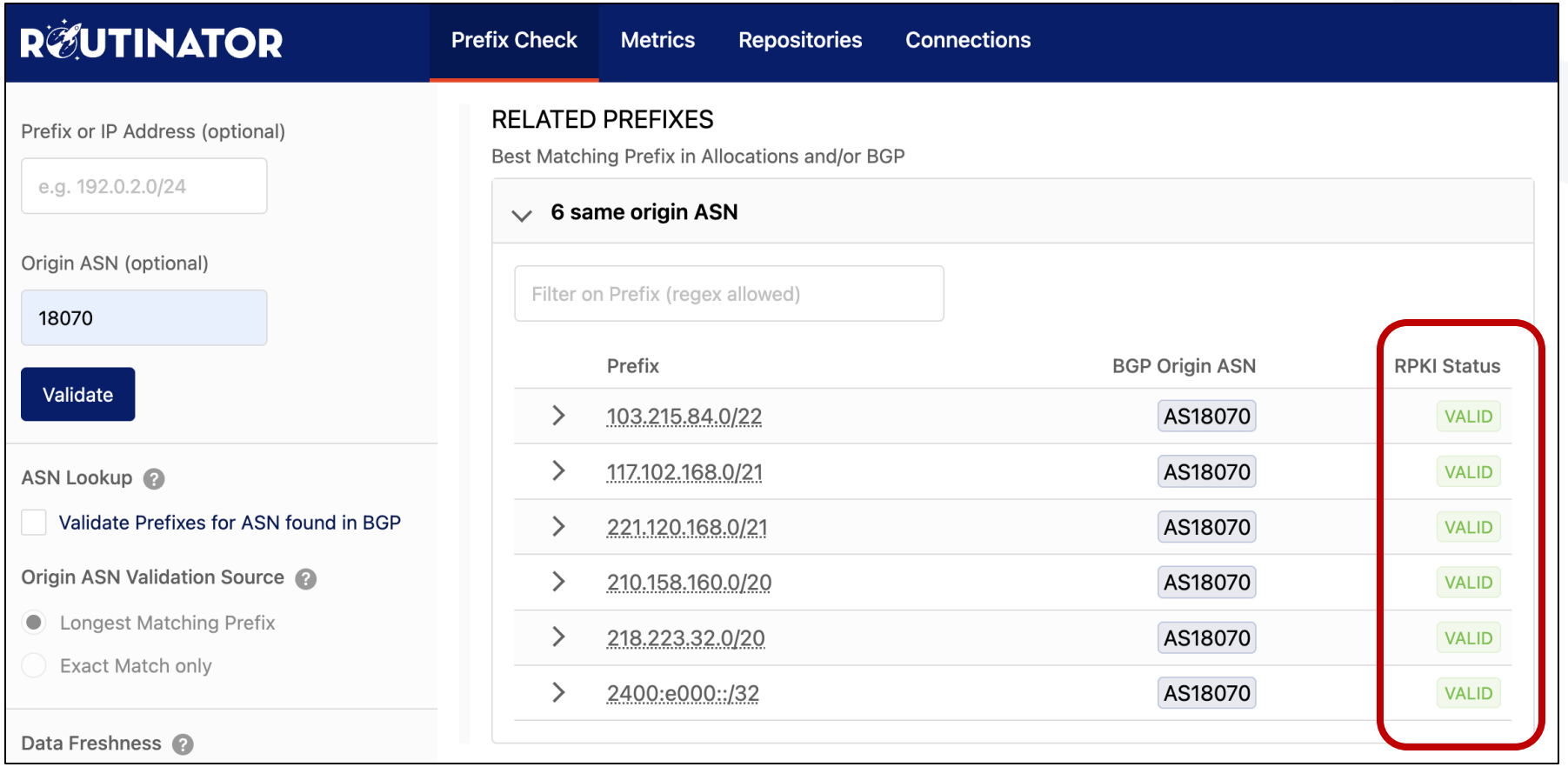
Looking Glass - Telia

https://lg.telia.net/

ROVの結果がわかりやすく表示されて便利！！
（この例ではValid）

RPKI Validator - RIPE NCC

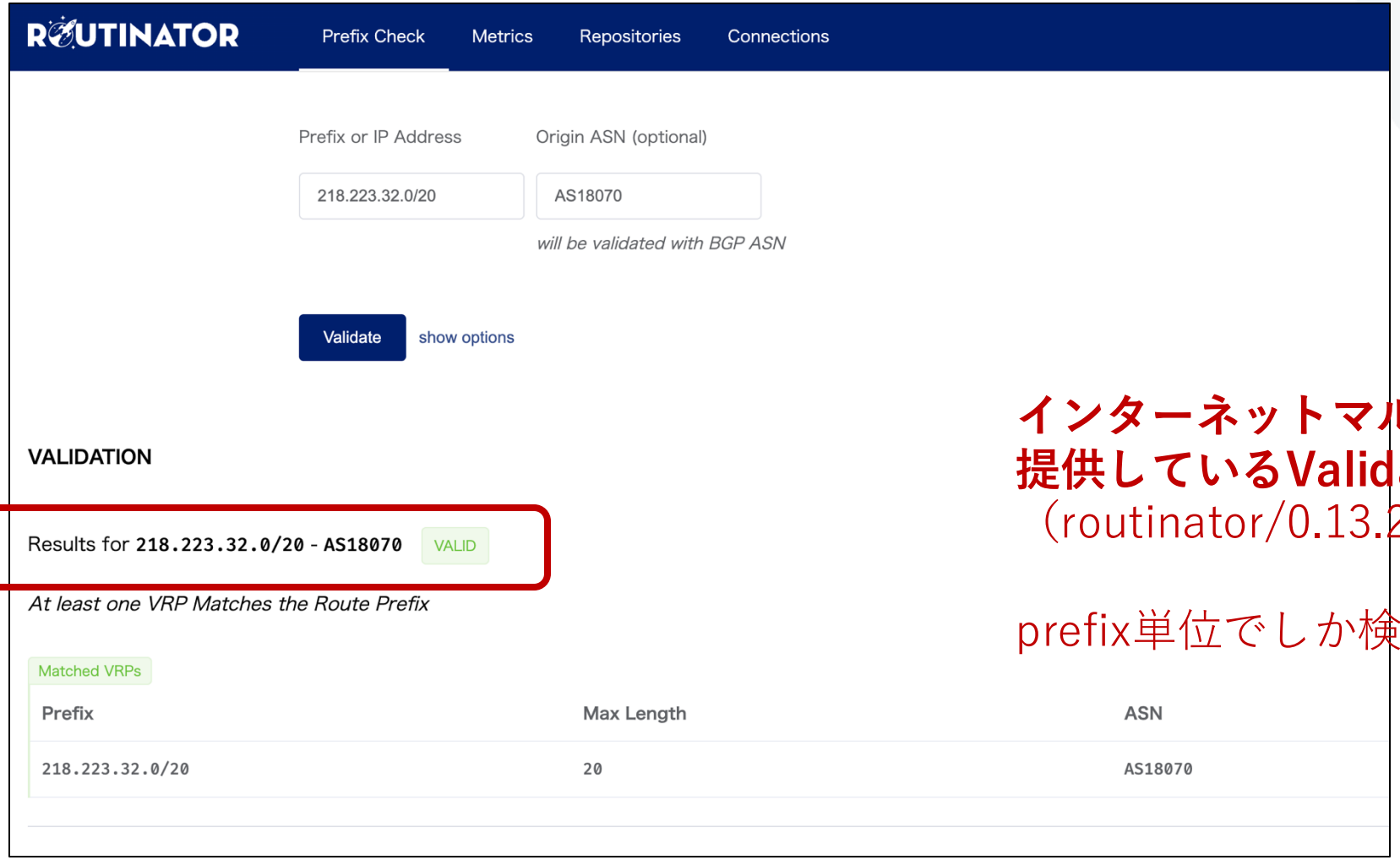
https://rpki-validator.ripe.net/ui/



RIPE NCCが提供しているValidator
（routinator/0.14.2 - ui/0.4.5）

RPKI Validator - INTERNET MULTIFEED

https://public-roa1.mfeed.ad.jp/ui/

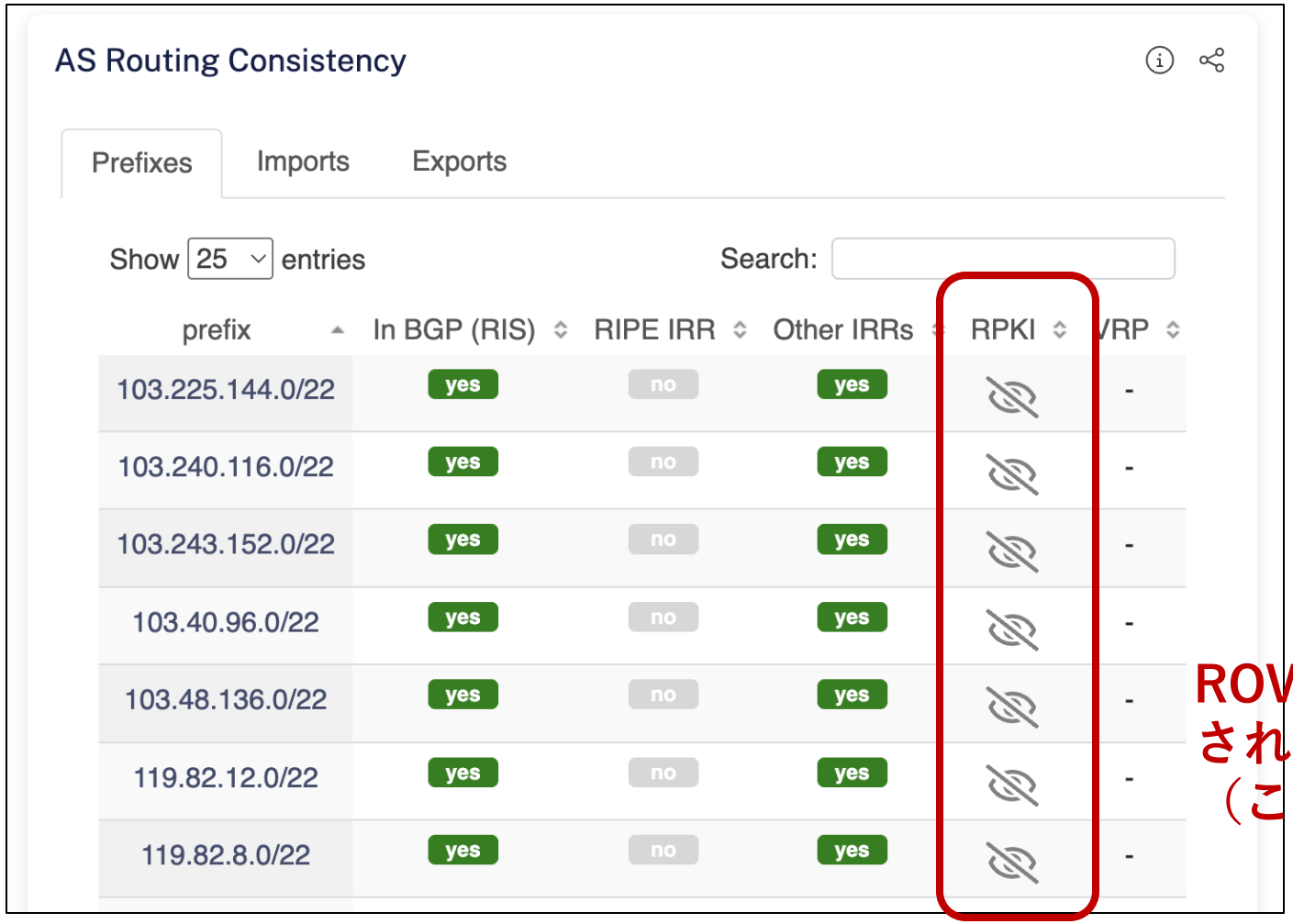


インターネットマルチフィードが提供しているValidator
（routinator/0.13.2 - ui/0.3.4）

prefix単位でしか検索できない…

RIPE Stat

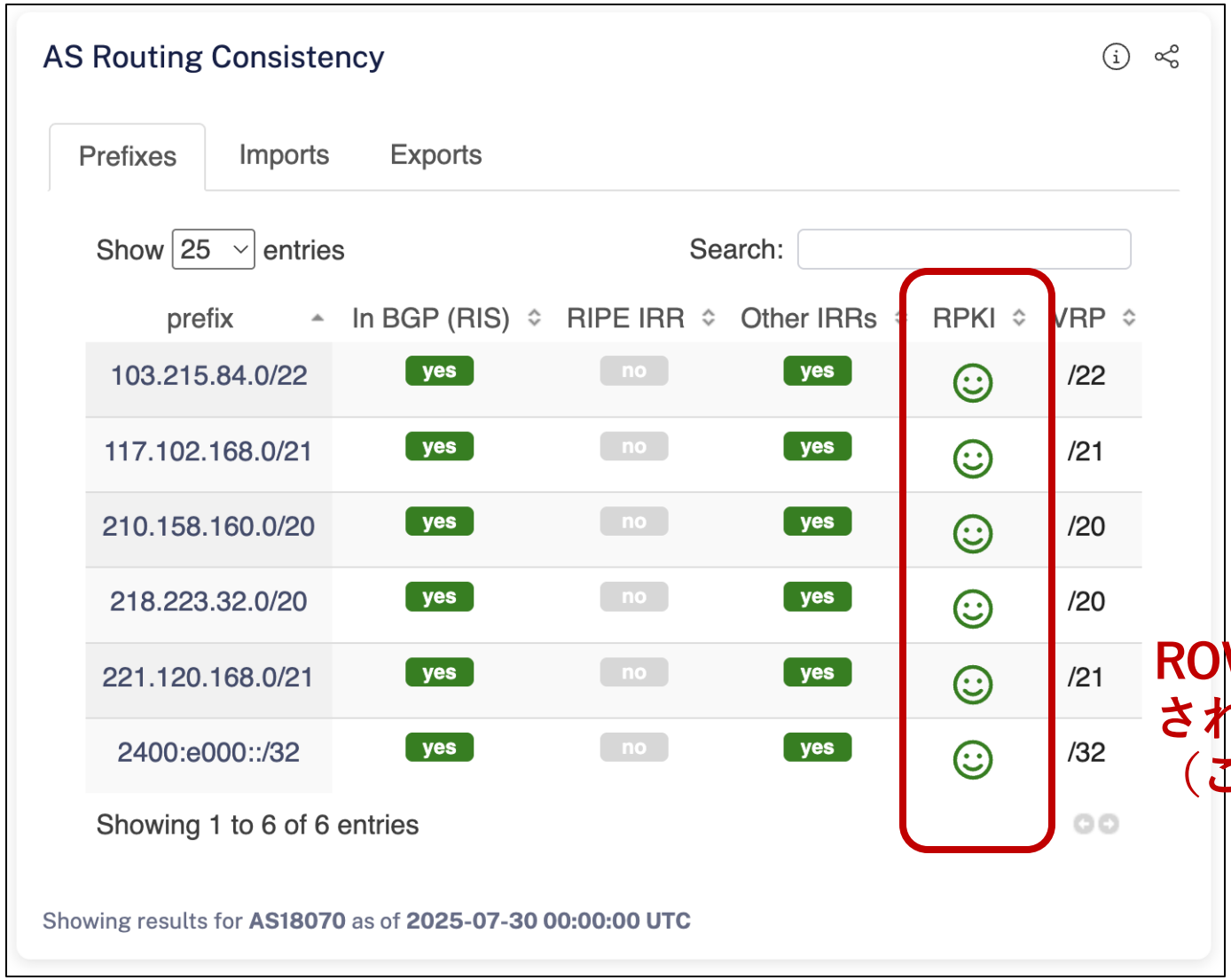
https://stat.ripe.net/



ROVの結果がわかりやすく表示されて便利！！
（この例ではNot Found）

RIPE Stat

https://stat.ripe.net/



AS Routing Consistency

Prefixes | Imports | Exports

Show 25 entries Search:

prefix	In BGP (RIS)	RIPE IRR	Other IRRs	RPKI	VRP
103.215.84.0/22	yes	no	yes	☺	/22
117.102.168.0/21	yes	no	yes	☺	/21
210.158.160.0/20	yes	no	yes	☺	/20
218.223.32.0/20	yes	no	yes	☺	/20
221.120.168.0/21	yes	no	yes	☺	/21
2400:e000::/32	yes	no	yes	☺	/32

Showing 1 to 6 of 6 entries

Showing results for **AS18070** as of **2025-07-30 00:00:00 UTC**

ROVの結果がわかりやすく表示されて便利！！（この例ではValid）

ROA作成作業の実際（モヤモヤ編）

JPNIC RPKIシステム - マニュアルでは

https://www.nic.ad.jp/ja/rpki/howto-create-roa.html

JPNIC RPKIシステム - マニュアルでは

https://www.nic.ad.jp/ja/rpki/howto-create-roa.html

作成済みROAが確認できる

JPNIC RPKIシステム - マニュアルでは

https://www.nic.ad.jp/ja/rpki/howto-create-roa.html

ROAを作成した後、JPNICが提供する
RPKI Validator 日本語版で状態を確認する

JPNIC RPKIシステム - 実際は（Day1 IPv6編）

ROAWeb (NDAC)

作成されたROAはすぐに公開され、国際的に参照可能な状態になります。ご注意ください。

ROAの管理

ROAを新規作成

Prefix (- 最大prefix長)	AS番号	状態(*1)	操作	観測されているBGP経路 (Prefixと経路広告元のAS)

(*1) 発行処理には2分程度かかることがあります。「発行済」の状態はそのROAがRPKIのリポジトリで公開されていることを示しています。
(*2) Routing Information Servie (RIS) のBGPデータを元に、本サイトにおけるオリジン検証(ROV)の結果を表示しています。一部のBGP経路が表示されないことがあります。

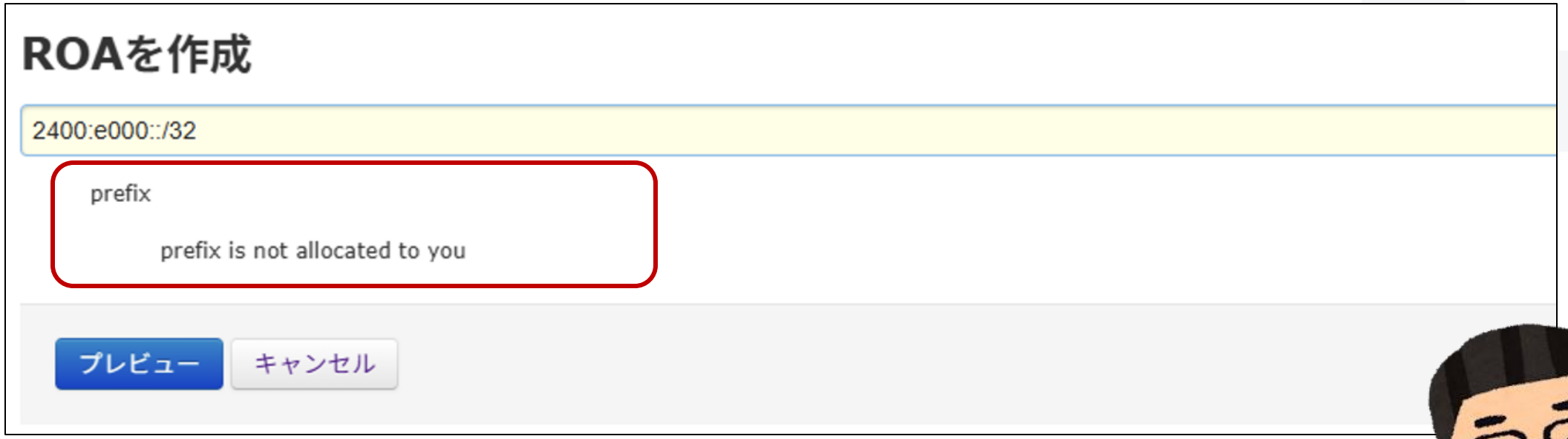
リソース証明書の一覧

リソース証明書が「発行済」になるとROAを作成できます。リソース証明書が「発行済」になるまでに2分程度かかることがあります。

	割り振られているが証明書に存在しない
IPv4	
IPv6	2400:e000::/32
AS	

割り振られているが証明書に存在しない？
「ROAを作成」ボタンがない？
とりあえず右上のボタンから先に進める…

JPNIC RPKIシステム - 実際は（Day1 IPv6編）



prefix is not allocated to you？？
なんか怖いので一旦キャンセル…

JPNIC RPKIシステム - 実際は（Day1 IPv6編）

ROAWeb (NDAC)

作成されたROAはすぐに公開され、国際的に参照可能な状態になります。ご注意ください。

ROAの管理

Prefix (- 最大prefix長)	AS番号	状態(*1)	操作	観測されているBGP経路 (Prefixと経路広告元のAS)

(*1) 発行処理には2分程度かかることがあります。「発行済」の状態はそのROAがRPKIのリポジトリで公開されていることを示しています。
(*2) Routing Information Servie (RIS) のBGPデータを元に、本サイトにおけるオリジン検証(ROV)の結果を表示しています。一部のBGP経路が表示されないことがあります。

ROA発行のできるリソース一覧

prefix表記のための正規化が行われているため、WHOISデータとは表記が異なる場合があります。

IPv6

Prefix	操作	観測されているBGP経路 (Prefixと経路広告元のAS)
2400:e000::/32	ROAを作成	

リソース証明書の一覧

リソース証明書が「発行済」になるとROAを作成できます。リソース証明書が「発行済」になるまでの処理にはしばらくかかることがあります。

ファイル名	B6SxrnWhC06C_oid9KG5ZdYKetw.cer
状態	発行済
有効期限 - 自動更新	2026年4月22日10:29:23 (日本時間/UTC+9)
IPv6	2400:e000::/32

よくわからんが出現した！！！
裏側の処理に時間がかかるとかなのかな…
とりあえず「ROAを作成」ボタンを押す

JPNIC RPKIシステム - 実際は（Day1 IPv6編）

作成されるROAの内容

ご注意： AS番号と最大prefix長が意図通りであることをご確認ください。作成されたROAはすぐに公開され、国際的に参照可能な状態になります。

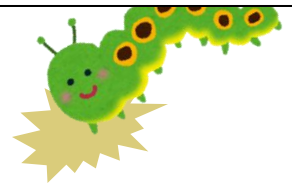
プレビュー

Prefix	最大prefix長	AS番号
2400:e000::/32	32	18070

RouteViewで観測されている経路情報

Prefix	経路広告元のAS	期待される経路の検証結果

作成 キャンセル



RouteViewで経路が観測されていない？
期待される検証結果もわからない？？
でもまあ、とりあえず作成してしまおう

JPNIC RPKIシステム - 実際は（Day1 IPv6編）

ROAWeb (NDAC)

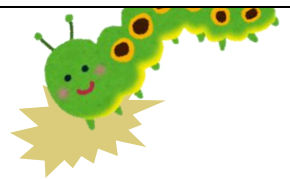
標準

作成されたROAはすぐに公開され、国際的に参照可能な状態になります。ご注意ください。

ROAの管理

Prefix (- 最大prefix長)	AS番号	状態(*1)	操作	観測されているBGP経路 (Prefixと経路広告元のAS)
2400:e000::/32	18070	発行済		

(*1) 発行処理には2分程度かかることがあります。「発行済」の状態はそのROAがRPKIのリポジトリで公開されていることを示しています。
(*2) Routing Information Servie (RIS) のBGPデータを元に、本サイトにおけるオリジン検証(ROV)の結果を表示しています。一部のBGP経路が表示されないことがあります。



とりあえず発行はできました
経路観測の情報はないけど…

JPNIC RPKIシステム - 実際は（Day2 IPv4編）

作成されるROAの内容

ご注意： AS番号と最大prefix長が意図通りであることをご確認ください。作成されたROAはすぐに公開され、国際的に参照可能な状態になります。

プレビュー

Prefix	最大prefix長	AS番号
210.158.160.0/20	20	18070

RouteViewで観測されている経路情報

Prefix	経路広告元のAS	期待される経路の検証結果
210.158.160.0/20	18070	valid

作成 キャンセル

翌日、IPv4の作業を実施
こっちはちゃんと想定通りの動きと表示…

重要

「期待される検証結果」が出ているだけで
安心感が全然違う

JPNIC RPKIシステム - 実際は（Day2 IPv4編）

作成されるROAの内容

ご注意： AS番号と最大prefix長が意図通りであることをご確認ください。作成されたROAはすぐに公開され、国際的に参照可能な状態になります。

プレビュー

Prefix	最大prefix長	AS番号
117.102.168.0/21	21	18070

RouteViewで観測されている経路情報

Prefix	経路広告元のAS	期待される経路の検証結果
117.102.168.0/21	18070	valid
117.102.169.0/24	55895	invalid

作成 キャンセル

別originでmore specific経路を流しているケース

検証結果は確かにこうなるよねー！
（ROAを作成する順番が悩ましい…）

RPKI Validatorの不具合？

JPNICが提供しているValidator
（RIPE NCC RPKI Validator 2.17）

http://roa2.nic.ad.jp:8080/

RPKI Validator

ホーム　トラストアンカー　ROA　除外フィルター　ホワイトリスト　BGPプレビュー　エクスポートとAPI　ルータセッション

BGP経路広告に関わるルータで得られる検証結果の**プレビュー**を表示しています。このプレビューは下記にもとづいています。

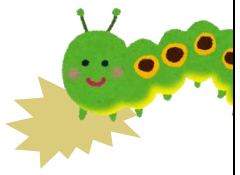
- 5 hours and 1 minute 前に更新されたRIPE NCC Route Collectorからの情報
- 5より多くのピア先で観測されたBGP経路広告
- RFC 6483に記述された検証ルール
- フィルターやホワイトリストが適用された後のRPKI Validatorで検証されたROA

BGPルータで観測できるBGP経路広告と下記にリストされているものとは異なることがあります。

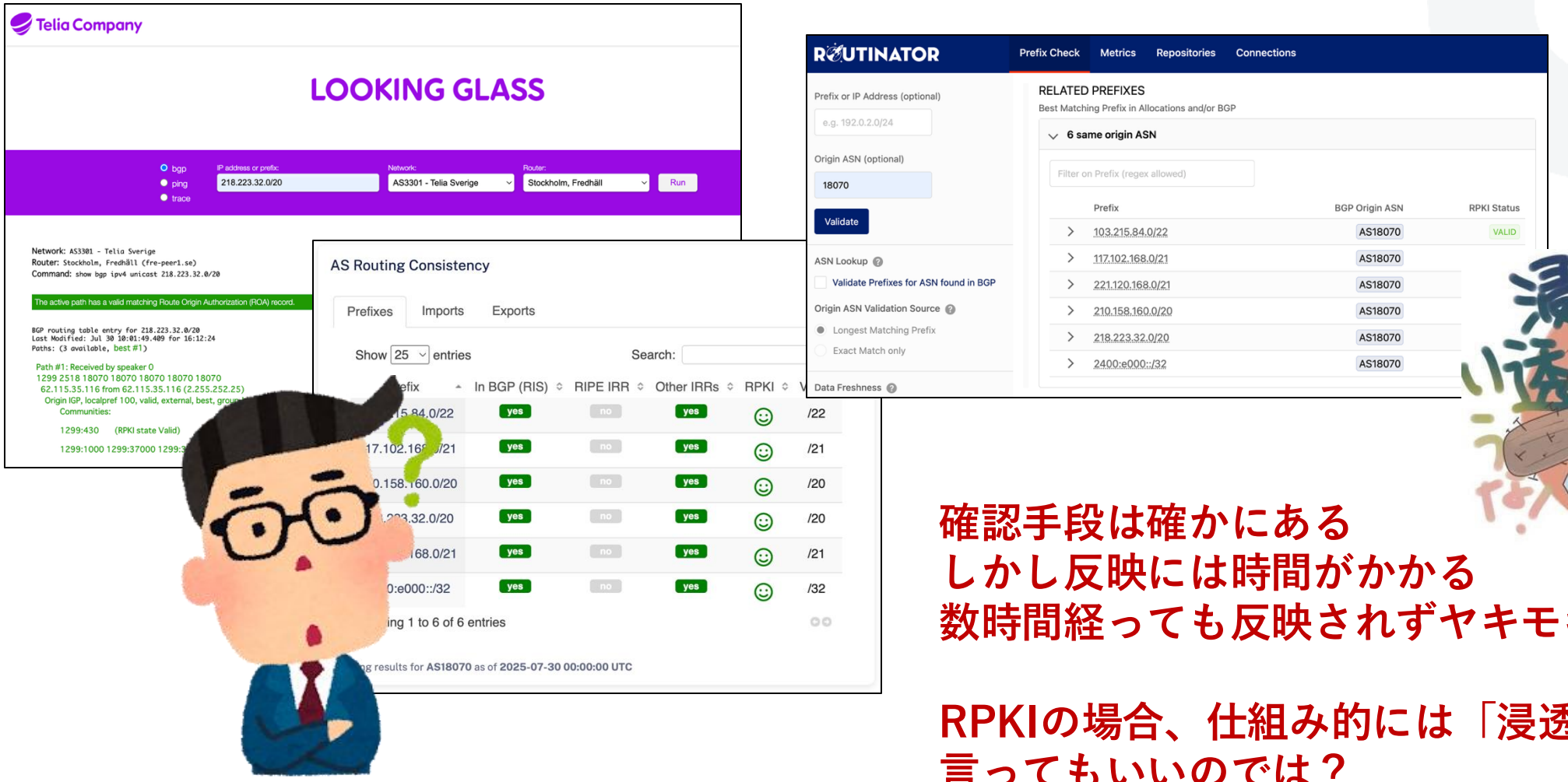
Show 10 entries　　Search: 18070

AS番号	プリフィックス	状態
18070	103.215.84.0/22	UNKNOWN
18070	117.102.168.0/21	UNKNOWN
18070	210.158.160.0/20	UNKNOWN
18070	218.223.32.0/20	UNKNOWN
18070	221.120.168.0/21	UNKNOWN
18070	2400:e000::/32	UNKNOWN

JPNICのROAWebで発行しているのに
JPNICのValidatorでなぜ見えない…？



なかなか確認できない…



確認手段は確かにある
しかし反映には時間がかかる
数時間経っても反映されずヤキモキ…

RPKIの場合、仕組み的には「浸透」って
言ってもいいのでは？

直近の事故案件…

2025年7月30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

障害復旧報告：JPNICにおいて発行されているROAの有効性の復旧について

本日(2025年7月30日)、 午前9時よりJPNIC管理下のIPアドレスに対するROAが有効性を失っていた状態が、 16時49分に復旧いたしましたことをお知らせいたします。 ご利用の皆様に、ご不便、ご心配をおかけいたしましたことをお詫び申し上げます。

記

■ 障害の原因

JPNICのRPKI CAにおいて作成されるManifestファイルの、 内部データにおいて本来更新されるべき有効期限が更新されておらず、 7月30日9時に有効期限が切れ、JPNICで発行されるROA等の有効性がなくなりました。 通常、この期限は、JPNICのRPKIシステムとAPNICのRPKIシステムが適切な時期に連携して更新されるものですが、 一時的に連携が取れずに更新できていませんでした。

■ 影響

JPNIC管理下のIPアドレスについて、 BGPルータにおけるオリジン検証の結果が「Not found」になっていたと考えられます。

■ 再発防止策について

原因となったManifestファイルの内部データは、 Manifest自身の有効期間とは異なるため通常のRPKIのクライアント(Relying Partyソフトウェア)で予見することはできませんが、 内部データの有効期限を確認する技術的な方法を使って監視を行い、 期限が切れる前に対処する方法を検討しております。

https://www.nic.ad.jp/ja/topics/2025/20250730-02.html

直近の事故案件…

Historical RPKI ROA Search:

Prefix to search for: 192.0.2.0/24

(Optional) Filter by ASN: 18070

Search

Date (UTC)		AS	CIDR	Max Length
2025-07-30 07:55	+	AS18070	2400:e000::/32	/32
2025-07-30 07:55	+	AS18070	221.120.168.0/21	/21
2025-07-30 07:55	+	AS18070	218.223.32.0/20	/20
2025-07-30 07:55	+	AS18070	210.158.160.0/20	/20
2025-07-30 07:55	+	AS18070	117.102.168.0/21	/21
2025-07-30 07:55	+	AS18070	103.215.84.0/22	/22
2025-07-30 00:08	−	AS18070	2400:e000::/32	/32
2025-07-30 00:08	−	AS18070	221.120.168.0/21	/21
2025-07-30 00:08	−	AS18070	218.223.32.0/20	/20
2025-07-30 00:08	−	AS18070	210.158.160.0/20	/20
2025-07-30 00:08	−	AS18070	117.102.168.0/21	/21
2025-07-30 00:08	−	AS18070	103.215.84.0/22	/22

下記の時間中、ROVの結果がNot Foundになっていたと思われる

（当社だけでなく、JPNIC管理下のIPアドレス全て）

2025-07-30 07:55 UTC
ROA再出現

2025-07-30 00:08 UTC
ROA消失

https://bgp.tools/rpki-history

まとめ：いろいろと思うところ

- 失敗影響が大きいため作業するのが恐ろしい…
  - 最悪の場合はインターネット全断、大丈夫だとわかっていてもドキドキ
- 作業後の確認が極めて困難…
  - 即時確認の手段がほぼない、いつどこでどう情報が反映されるかが不明
  - 確認に時間がかかる＝切り戻しに時間がかかる
- JPNICのシステムがまだ不安定…
  - RPKIシステムの挙動が怪しかった
  - JPNICのRPKI Validatorにはバグがある
  - ROAの有効性に関する重大事故の発生（RPKIの信頼性問題）

まとめ：いろいろと思うけどね

- **RPKIはかなり普及が進みましたよ！**
  - ROA作成はもちろん、ROVの実施も一般的になってきています
- **ROA作成していない人、早く作成しようぜ！**
  - ドキドキする作業は早く終わらせるに限る
- **ROAの次は、ROV！**
  - いろいろと考慮することはありますが・・・
    流れとしてはやる方向だよね

ケーロちゃん、カワイイ♡

確かな未来を、確かな力で。

GLOBAL NET CORE