RPKIガイドラインとROVの効果検証
～RPKIのはじめの第一歩～

2025年2月28日(金) ENOG 85 Meeting

JPNIC 塩沢 啓

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

自己紹介

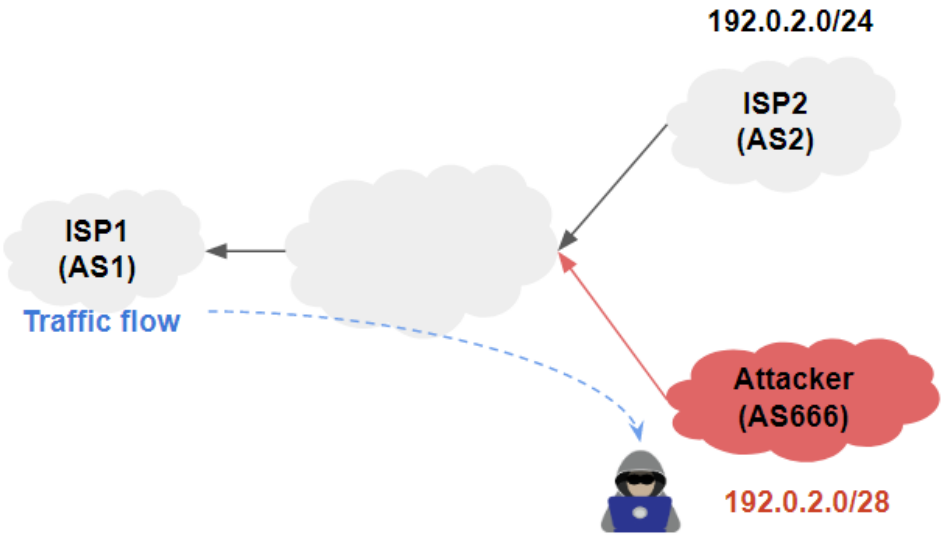
- 名前　塩沢　啓
- 所属　JPNIC インターネット推進部・技術部
- 出身　長野県
- コミュニティ　ChuNOG 運営メンバー

目次

- Why RPKI ？
  - ルーティングインシデント
  - RPKIとは？
  - RPKIの普及状況
- RPKIの導入に向けて…
  - RPKIガイドラインについて
  - ROVの効果検証について
    - ROV-CHECKのご紹介

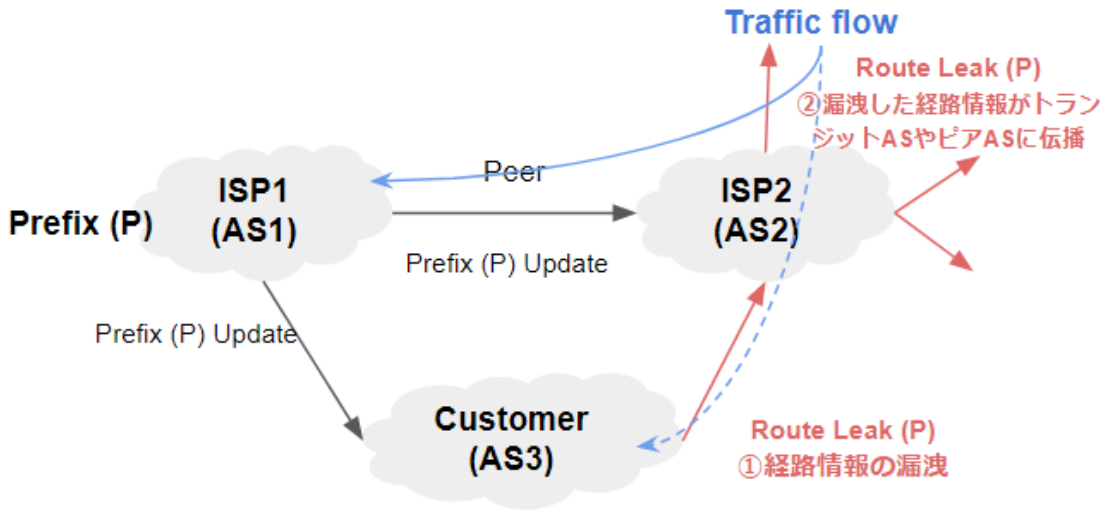
代表的なルーティングインシデント

・Mis-Origin



第三者が（時には設定ミスにより）不正な経路情報を広告することで、特定のネットワークへの通信を奪ってしまうこと

・ルートリーク



（多くの場合、設定ミスにより）インターネット上の意図しない範囲に広く経路情報が漏洩してしまうこと

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, 當間 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-lt-toma-1.pdf

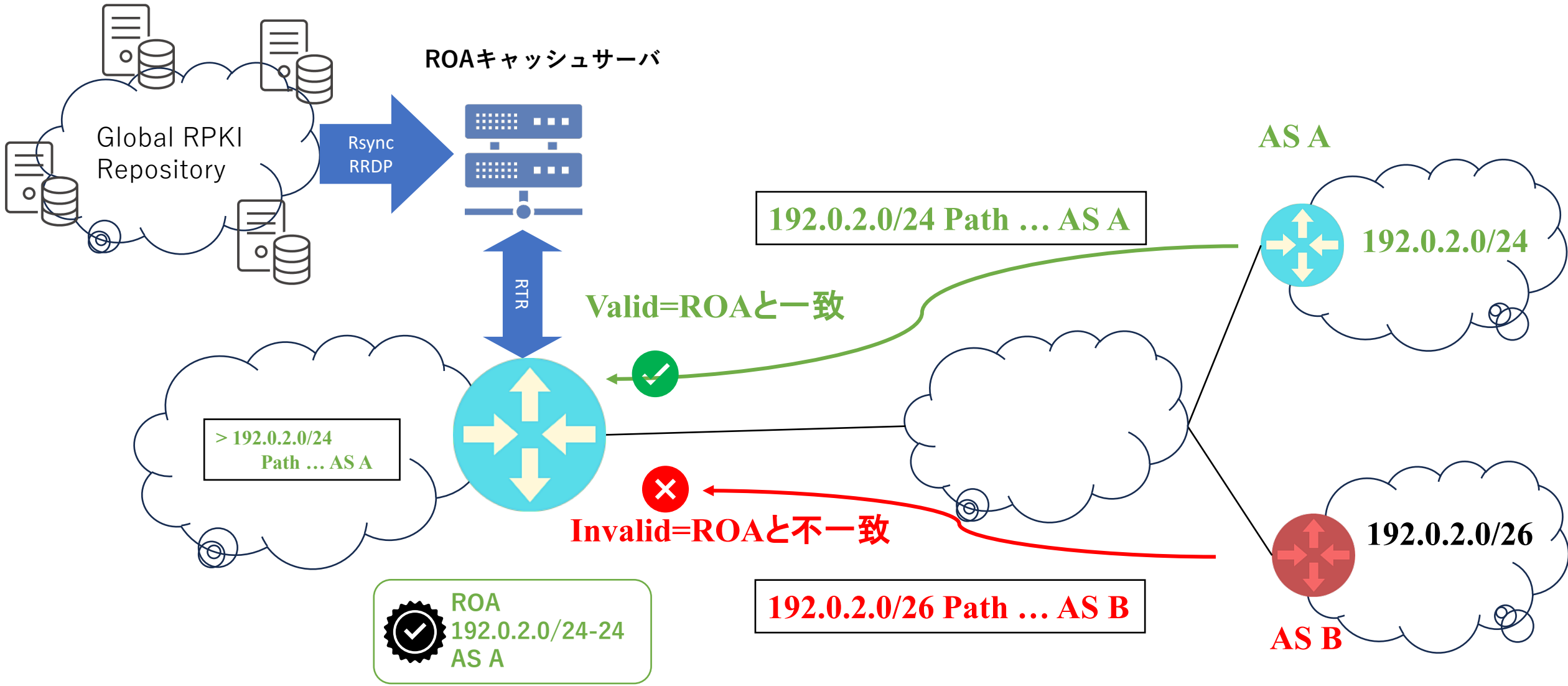
RPKI

- **RPKI (Resource Public Key Infrastructure)**
  - 番号資源（IPアドレスやAS番号）の割り当ての正当性を証明するための公開鍵基盤
  - ROAとROVによって、**Mis-Originな経路による不正な乗っ取り**を防ぐことができる

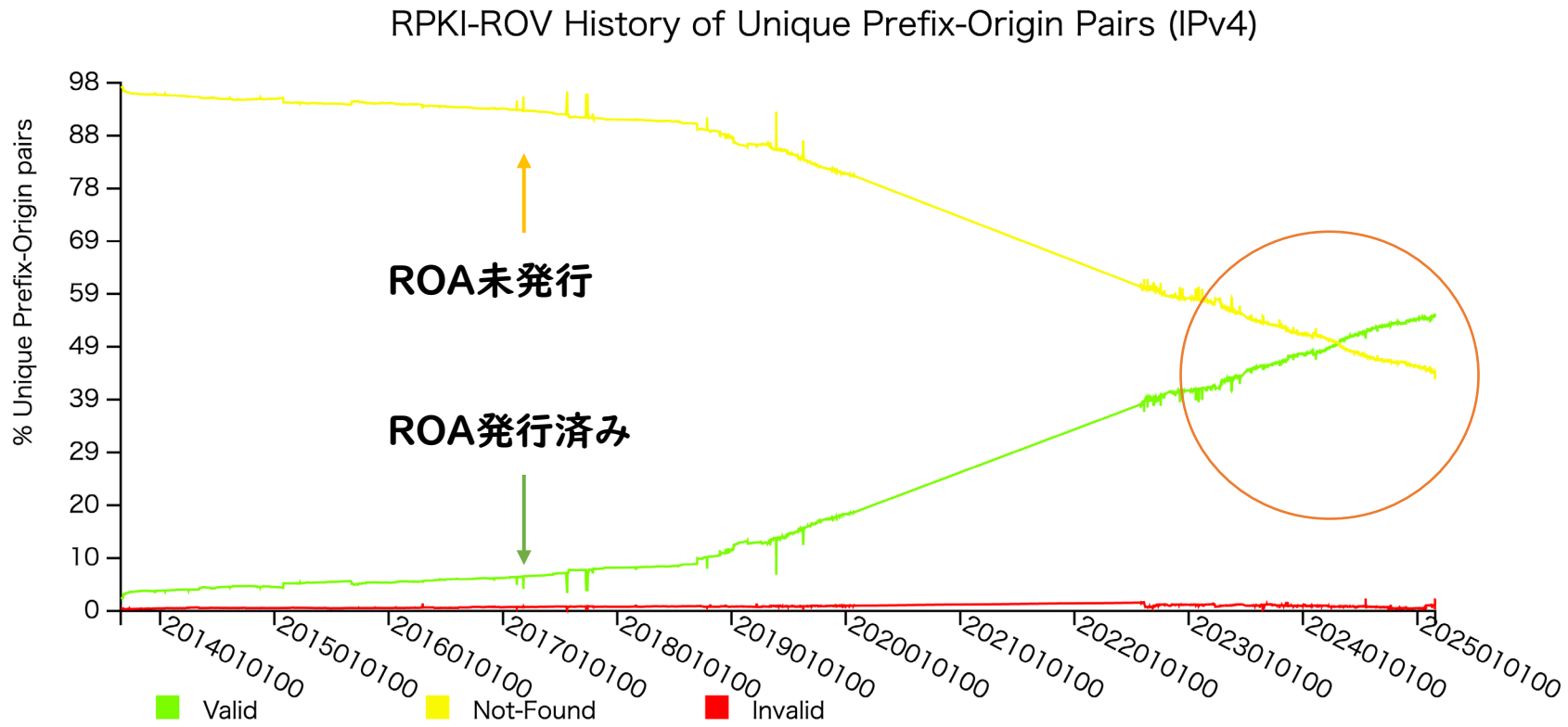
- **第一段階：ROA**
  - Route Origination Authorization
  - **IPアドレスとAS番号の組み合わせに対して、それが正しい組み合わせであることを示す電子署名が施されたデータ**
  - **リソースホルダーであれば自身のプレフィックスのROAを発行可能**

- **第二段階：ROV**
  - Route Origin Validation
  - ROAの情報と、BGPで受信した経路情報を照合して、正しいASから広報されているか検証する仕組み
  - ルータ等でROVを行うためには、ROAに付与された電子署名を事前に検証するROAキャッシュサーバを用意する必要がある

ROV Filtering



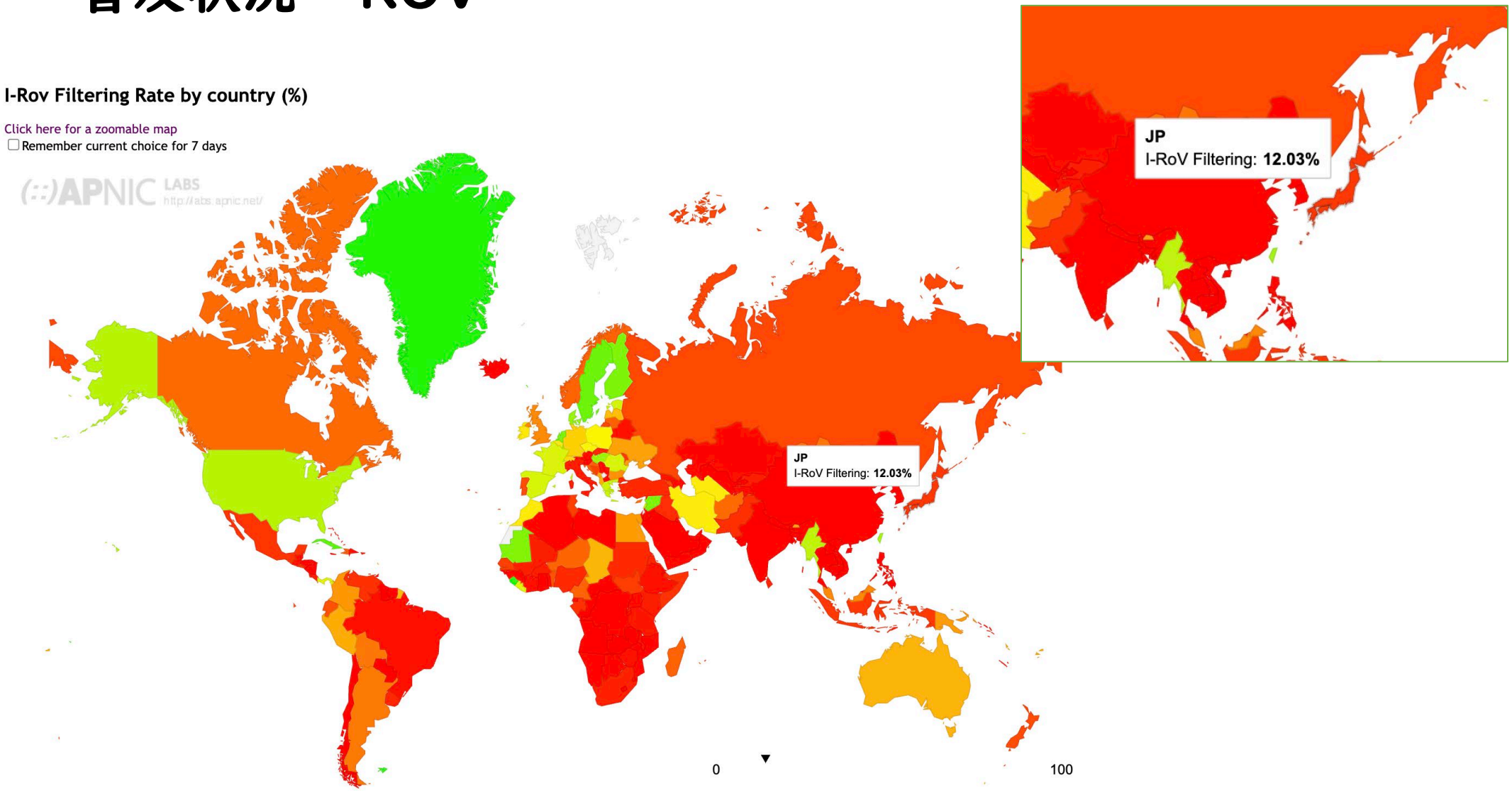
普及状況 - ROA



2024年5月頃にROA発行済みのプレフィックスが50%を超える

NIST RPKI Monitor
https://rpki-monitor.antd.nist.gov/

普及状況 - ROV



APNIC Lab – RPKI I-ROV Filtering World Map
https://stats.labs.apnic.net/rpki

目次

- Why RPKI ？
  - ルーティングインシデント
  - RPKIとは？
  - RPKIの普及状況
- RPKIの導入に向けて…
  - RPKIガイドラインについて
  - ROVの効果検証について
    - ROV-CHECKのご紹介

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

*「ISPにおけるネットワークセキュリティ技術の導入および普及促進に関する調査」事業（令和4～5年度）

RPKIの導入に向けたガイドラインの活用例

- 活用のポイント


目次

- **第一章：企業がRPKIを導入する意義やレピュテーションリスク等について記載**
  - 不正な経路情報のリスクや損失や、その対策技術としてのRPKI、ROA、ROVについて解説
  - 経営者向けの内容

- **第二章：対象となる技術者向けに、実例を含めて記載**
  - IPアドレスの分配を受けた組織が実施すべきこと
    … 2.1節 ROA
  - AS運用者が実施すべきこと…2.2節 ROV
  - また、各種ベンダーの具体的なROVの設定例も別紙に記載

RPKIの導入に向けたガイドラインの活用例

- 導入/運用の役割や担当に分けて
  - 対策をしなければいけない項目(必須)
  - 対策をすることが望ましい項目(推奨)
    もわかりやすく整理

- ROA…IPアドレスの分配を受けている組織
  - 必須：2項目
    - ROAの作成
    - ROAと経路情報が一致するように保つ
- ROV…ASを運用している組織
  - 推奨：1項目
    - ROVを行う等の処置

1.5 実施事項

■JPNICやAPNICからIPアドレスの分配を受けているすべての組織や個人

○ROAを作成します(必須事項)。

管理下にあるIPアドレスに関するROAを必ず作成してください。 これを行わないとそのIPアドレスに関するROVを行うことができず、 インターネットにおいて不正な経路情報への対策を取ることができません。

⇒ 「2.1. ROA/IPアドレスの分配を受けた者の実施事項」を参照してください。

○ROAが実際の経路情報と一致するように保ちます(必須事項)。

作成したROAと経路情報が一致するように保ってください。 これを行わないと正常な経路情報であるにもかかわらず、 ROVを行っているルータにおいて不正な経路情報と判定されてしまうことがあります。

⇒ 「2.1. ROA/IPアドレスの分配を受けた者の実施事項」を参照してください。

“RPKI効果検証”という企画について

- RPKI効果検証 ??
  - RPKI/ROVの実証実験・ガイドライン公開の次なる取り組み
  - ROVの普及によって、日本のインターネットは本当に不正な経路から守られているのかを確認したい！

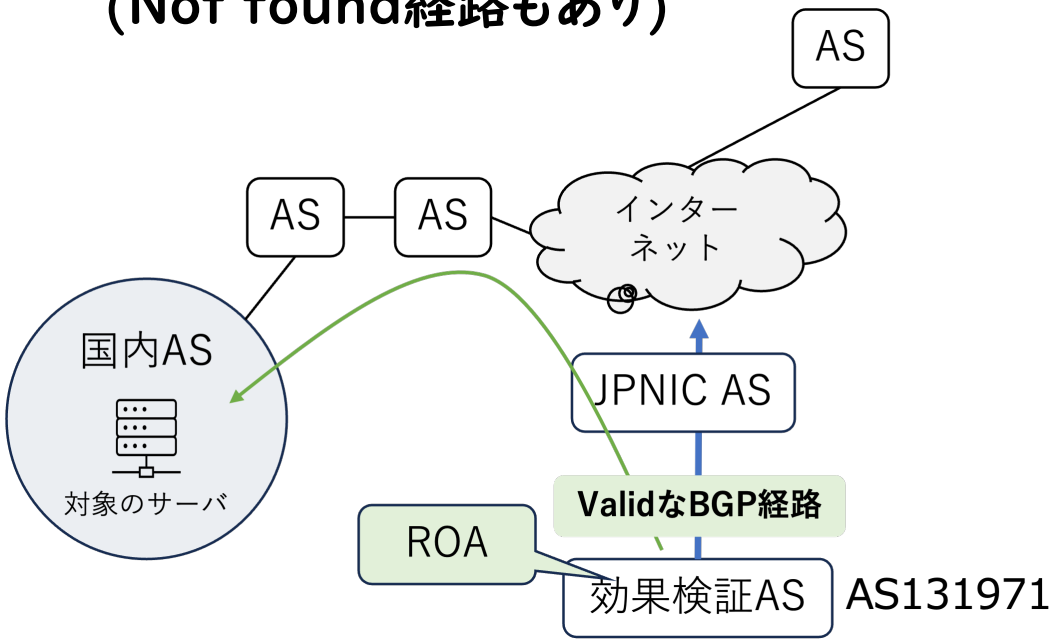
- 主な取り組み
  - “国民生活を支える”サーバやネットワークは不正なBGP経路の影響を受けないのか
    ⇒ ROV Invalidなネットワークから到達性はあるのか
    ⇒ そのネットワークは不正経路から守られているのか

  - 任意のネットワークからROV Invalidなネットワークにあるサーバに到達性はあるのか
    ⇒ そのネットワークはROVによって不正経路から守られているのか

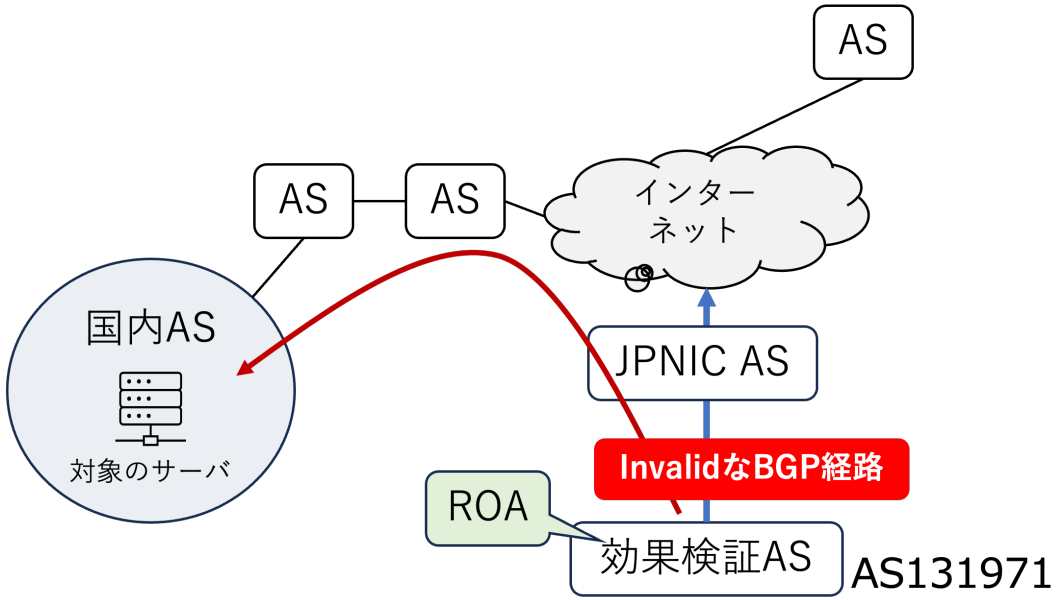
RPKI効果検証

- 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)



rov-check サイト

- RPKI効果検証の取り組みの一環で開発。先ほどの効果検証用ASを利用
- 自身が使っているネットワークがROVによって保護されているかどうか、簡単に確認することができる。

  https://rov-check.nic.ad.jp/

まとめ

- RPKIの導入に向けて、、

- RPKIガイドラインの発行
  - RPKI導入に向けた社内での検討材料・指針としてぜひご活用ください
  - まずは、ROAの発行から！

- ROVの効果検証について
  - rov-check サイト
  - ご自身のネットワークがROVで守られているか確認できるサイト
  - ROVによる効果について引き続き調査していきます！