

RPKIキャッシュサーバの課題と提案

-より信頼できるRPKIを目指して-

2026年7月16日 JANOG58 Meeting 松山

ビッグロース株式会社

山口 勝司

好きが、未来を変えていく。

会社紹介・自己紹介

- 会社紹介

- ・ ビッグロブ株式会社(AS2518)
- ・ 全国で固定系ブロードバンド、MVNO、IPTランジットなどのインターネット接続サービスを提供

- 自己紹介

- ・ 山口 勝司 (Katsushi Yamaguchi)
- ・ 2022年中途入社、AS2518のネットワーク戦略立案や設計、ピアリングコーディネーターなどの業務を主に担当
- ・ インターネットと通信技術が好きで技術コミュニティ活動や若手の育成にも積極的に関わる
- ・ インターネット運用は10年以上の経験

2025年11月にAS2518はROVを開始しました



ルーティングセキュリティへの取り組み

～より安心安全なインターネット環境の提供に向け、RPKIの導入とROAの正当性を評価する仕組みづくり～

プレスリリース

接続

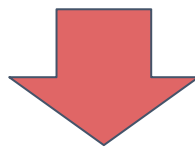
2025-10-03

ビッグロブ株式会社

ビッグロブ株式会社（本社：東京都品川区、代表取締役社長：山田 靖久、以下 BIGLOBE）は、2025年11月未までに自社ネットワーク内へRPKI（Resource Public-Key Infrastructure）の導入を完了します。これにより、お客さまにさらに安心・安全なインターネット環境を提供することが可能になります。

RPKIはIPアドレスやAS番号情報が含まれた電子証明書(ROA)を使い、ルータが経路情報をチェック(ROV)するルーティングセキュリティの仕組み

RPKIキャッシュサーバで思わぬトラブルが起きるかもしれない？



トラブルの原因として考えられること、その解決方法、より**安全にRPKIキャッシュサーバを運用し、ROVするにはどうすべきか**議論したい

■ 以下の内容については今回は議論しないものとします

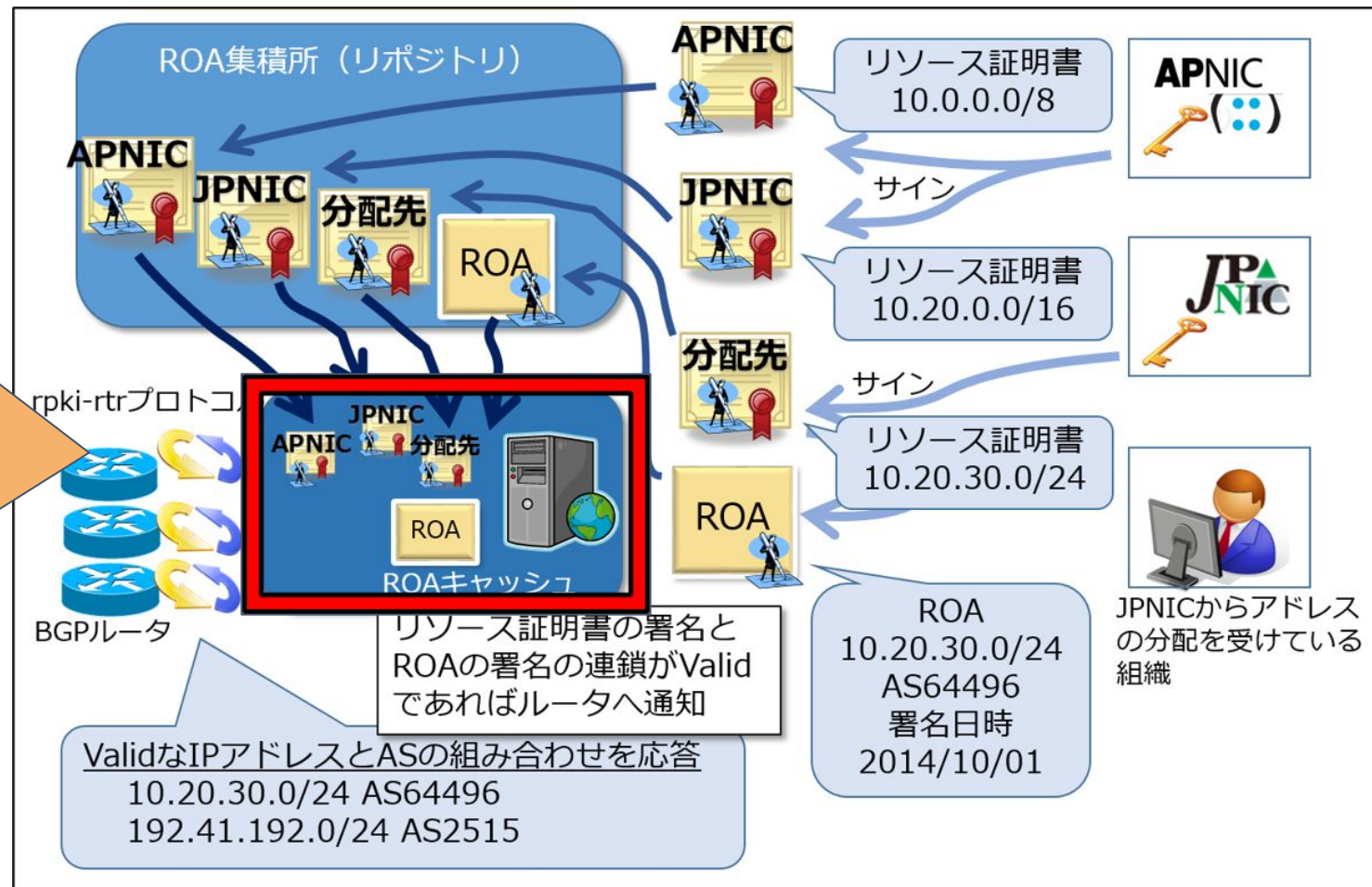
- ・ RPKIの仕組みそのもの、ROVで不正経路対策をすることの是非や有効性
- ・ BGPルーター側の実装やオペレーション、RPKIキャッシュサーバの個別のソフトウェアの実装

RPKIの仕組みとROAキャッシュサーバ

ルータとROA集積所の間を取り持つキャッシュサーバ

ROAを集めて
VRP(Validated ROA
Payload)にして
ルータに引き渡す

ROAキャッシュ =
RPKIキャッシュ



[リソースPKI (RPKI; Resource Public Key Infrastructure) - JPNIC] <https://www.nic.ad.jp/ja/rpki/>

RPKIキャッシュサーバの運用が抱える懸念事項

RPKIキャッシュサーバの 懸念事項	起こりうる事象
ROA集積所(リポジトリ)の運用	運用者のROAの公開トラブルやサーバ運用のトラブル → RPKIキャッシュサーバが取得する情報に影響
ROA集積所(リポジトリ)自体の到達性	リポジトリへの疎通性が消失・遅延大・経路上のパケットロス → RPKIキャッシュサーバが取得する情報に影響
RPKIキャッシュサーバの運用	RPKIキャッシュサーバ運用のトラブル → BGPルータがRPKIキャッシュサーバから取得する情報に影響
サーバソフトウェアの実装差異	ソフトウェアにより機能・データの取り扱いなどが異なる ソフトウェアの多様性を確保する際に同一運用が困難
サーバソフトウェアの保守運用	OSSソフトウェアの継続的な保守開発

本プログラムではリポジトリのトラブル、リポジトリとネットワークの問題に着目

RPKIキャッシュサーバが抱える懸念事項

リポジトリの運用トラブル(実例)

ROAの公開ミス - 2025/3/27

JPNICのRRDPデータサイズに起因するミス

RRDPを通じて提供する**ROAとその有効性に関わるファイルが古いもの**となっており、有効性を失っていた

<https://www.nic.ad.jp/ja/topics/2025/20250327-01.html>

サーバ運用のトラブル - 2025/6/26

APNIC RPKIリポジトリサーバのダウン

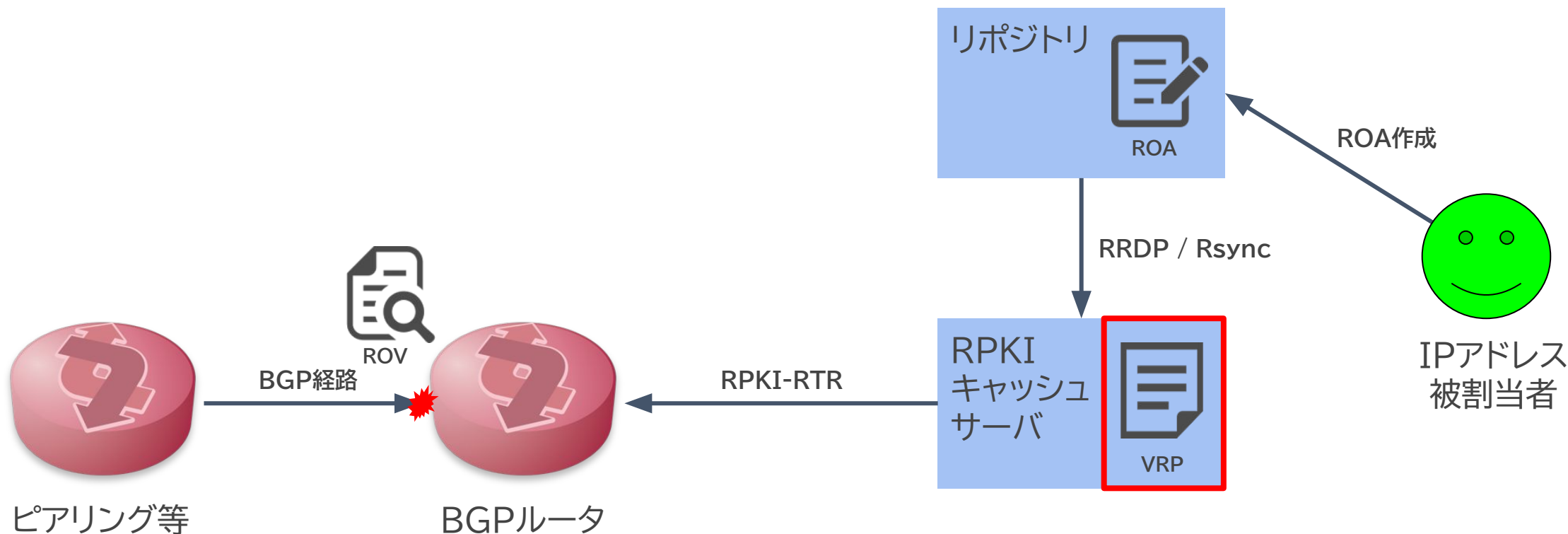
インシデント期間中サーバがダウンしており、対象期間中本リポジトリサーバ配下が公開する**ROAが取得できなかった**と推測できる

<https://apnic.site24x7statusiq.com/>

- 上記の実例以外にも2023年～2024年にかけてはLACNICとAFRINICで、2022年にはRIPE NCCでもトラブルによりROAが取得できなくなるトラブルが発生している。2026年現在ではリポジトリまたはリポジトリとRPKIキャッシュサーバ間のネットワークの問題などによってROAが利用できなくなることは十分に発生しうるリスクである。

不完全なVRP

- 生成した**VRPが不完全**になるリスクが存在
 - リポジトリ側の問題により一部のROAが欠損
 - リポジトリとキャッシュサーバ間のネットワークの問題により一部のROAが欠損
- ROA作成者が誤ったROAを作成した場合もその情報が直ぐにルータに反映される



ルータに反映されるVRPの検証とは？

検証により、経路には何れかのステータスが付与される

- **VALID**（全経路の約68%）
 - ルータの経路が対応するROAの内容と**完全一致**する状態
- **NOTFOUND**（全経路の約30%）
 - ルータの経路に対するROAが**存在しない**状態
- **INVALID**（全経路の約1%）
 - ルータの経路が対応するROAの内容と**矛盾**する状態

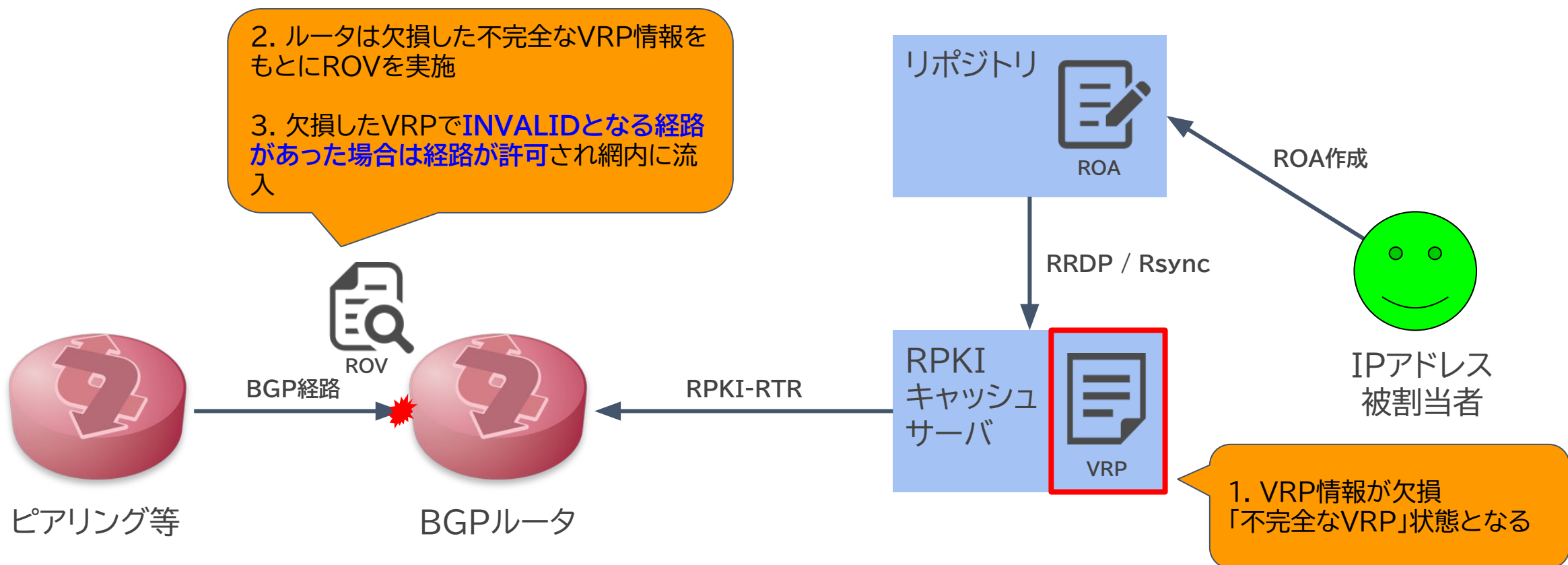
ステータスによって経路をどのように取り扱うかはルータ運用者が決める
現在、「**INVALID**」は破棄、「**NOTFOUND**」は許可する運用が一般的である

各経路の比率のデータはNIST RPKI MonitorのIPv4アドレスのデータに基づく <https://rpki-monitor.antd.nist.gov/>

「不完全なVRP」の影響と懸念

現在（**INVALID経路のみを拒否**している）

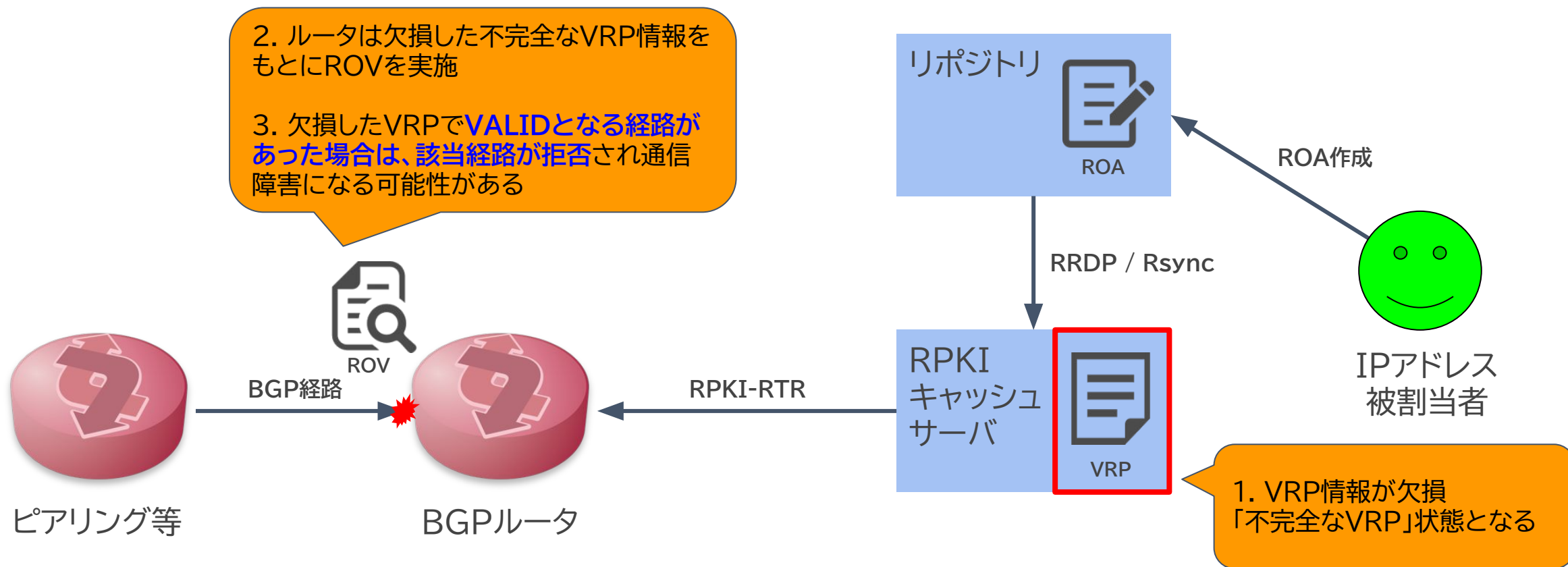
- 本来はINVALIDとなる経路のVRP情報が存在せず不正経路の流入を許す可能性がある
- これは事実上のセキュリティレベルの低下となる可能性がある



「不完全なVRP」の影響と懸念

未来（INVALID経路 & NOTFOUND経路 を拒否している）

- INVALID & VALID経路となるVRP情報が取得できず、NOTFOUND経路としてルータで処理される
- 正常な経路がフィルタされ通信障害となる可能性がある



「不完全なVRP」の影響と懸念

「NOTFOUND」経路を拒否する未来では不完全なVRPは大きな通信影響を与える

	現在 (INVALID拒否)	未来 (INVALID&NOTFOUND拒否)
発生する事象	INVALIDとなるROAが取得不可 ⇒ 結果、NOTFOUNDとしてルータで処理される	VALIDとなるROAが取得不可 ⇒ 結果、NOTFOUNDとしてルータで処理される
影響	AS内に不正経路の流入を許す ⇒ ルーティングセキュリティが低下	多くの経路が拒否される ⇒ ルーティングへの影響が発生

「不完全なVRP」の影響と懸念

NOTFOUND経路を拒否する未来に関して

現在の一般的な運用

■ NOTFOUND経路は拒否しない

- ・現状のインターネットにおいては、NOTFOUND経路を拒否しない運用が一般的

■ RFC7115 (BCP185)

- ・INVALID経路は「使うべきではない(SHOULD NOT)」と明記されている一方、NOTFOUND経路については使うべきではないとは定められていない。

BGP Communities for Security Policy Intent (IETFドラフト)

■ 概要

- ・経路の送信元(Origin AS)が、BGP Large Communityを使い「優先度の扱いに関する意思(Intent)」を明示的に宣言する仕組み。

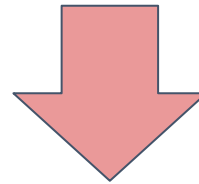
■ 厳格な扱いを求めることができる

- ・「ROA-Strict」Communityが付与された経路は、より厳格な扱いを求める意思を他ASへ伝達可能。
- ・「厳格」とは破棄を求めるものではないが、これを受けて、実際に破棄や優先度を下げる判断を行うASが将来的に現れる可能性がある

現在はNOTFOUNDの受け入れが一般的だが、将来的には変わっていく可能性もある

「不完全なVRP」の影響と懸念

- **INVALID経路が流入**することを許してしまうことへの懸念
 - 事実上のセキュリティレベルの低下となってしまう
 - ROVを始める前の状態に一時的に戻るだけという説明で済まされる？
- **不完全なROVにより正常な経路への通信影響を発生させることへの懸念**
 - ROVにより正常な経路への通信影響を発生させることはできるだけ避けたい
 - 正常な経路への通信影響はROV開始前と比較してデグレードかもしれない
 - 万一ROVにより通信影響が発生した場合、顧客に説明できる？



不完全なVRPがルーティングに影響を及ぼすリスクはできるだけ小さくしたい

「不完全なVRP」対策の検討

- 長崎県立大学 後藤さんから -

ビッググローブでの「不完全なVRP」対策と今後の検討

- 以下の項目についてはROV開始時から監視しており異常があった場合はアラートが上がる

監視項目	詳細	アラート閾値
同期成功リポジトリ数	同期に成功したリポジトリの数	1以上であること
同期失敗リポジトリ数	同期に失敗したリポジトリの割合	20%以上失敗していないこと
VRP数	キャッシュサーバが持つVRPの総数	0ではないこと
ROA収集時間	ROA収集完了までの時間	1時間以下であること

不必要なアラートによる運用負荷を避ける目的でかなり控え目な設定でスタート
異常が発生した場合は運用者の判断の下でROVを一時停止することも検討



長崎県立大学との共同研究の成果を元にした「VRPブレーカー」のような仕組みの導入を検討中

まとめ

01

「不完全なVRP」の問題

- リポジトリやリポジトリとキャッシュサーバの間のネットワークの問題により「**不完全なVRP**」が発生する可能性がある
- 「不完全なVRP」が発生することで**INVALID経路が流入**し、**セキュリティレベル低下**が懸念される

02

NOTFOUND経路を拒否する未来

- 「**NOTFOUND**」を拒否する**未来**では多くの正常な経路も拒否することになり、**通信障害となる可能性**がある
- 現状「NOTFOUND」は拒否しないことが推奨であるが、未来では変わる可能性もある

03

共同研究と今後の計画

- 長崎県立大学との共同研究で一つのアイデアとして「VRPブレーカー」の研究開発を行った
- ビッグローブのRPKIシステムに何らかの形で「**不完全なVRP**」対策の実装を検討中

ROVの課題やリポジトリを含めた信頼性向上について議論を深めたい

皆様と議論したいこと

ROVのリスクに関してどのように考えていますか？

- ・ 不完全なVRPによりINVALID経路がFIBにのる可能性
- ・ 正常な経路がROVにより破棄されて通信障害となるリスク
- ・ 「NOTFOUND」の経路を破棄(または優先度を下げる)する未来は来るでしょうか？

リポジトリの信頼性について

- ・ リポジトリの信頼性を高めるにはどうすれば良いでしょうか？
運用者、利用者の双方の立場から議論できればと思います

「不完全なVRP」への対策について

- ・ 「不完全なVRP」への対策は必要だと考えますか？
- ・ 「不完全なVRP」と判断するための要素として必要なものは何だと考えますか？
- ・ VRPブレーカーの仕組みに対してご意見があればご共有ください

好きが、未来を変えていく。



BIGLOBE