



おさえておきたい基本や、最新動向を解説するコーナーです。



No. 91号

10:00



RPKI (Resource Public Key Infrastructure) ※1 ※2は、IPアドレスやAS番号といった番号資源が分配された際にそれを証明する電子証明書を発行することで、ASパスや経路情報として使われるIPアドレスの正しさを検証できるようにする仕組みです。このRPKIについて、前号の90号より前後編の2回に分けて解説をしています。

※1 RFC4271: A Border Gateway Protocol 4 (BGP-4) <https://www.rfc-editor.org/rfc/rfc4271.html>

※2 インターネット10分講座:BGP <https://www.nic.ad.jp/ja/newsletter/No35/0800.html>

「RPKIとは」  
後編



後編となる本稿では、RPKIを利用した実際の検証手順や、周辺技術の紹介、鍵管理や設計、障害事例といった運用に関する情報、普及状況や課題などを取り上げます。以下の項目については前編で取り上げていますので、90号のバックナンバーをご覧ください。

01. 概要

02. BGPと経路情報の正しさ

03. RPKIと利用—全体像

04. ROA Manifest CRL

RPKI (Resource Public Key Infrastructure)とは  
<https://www.nic.ad.jp/ja/newsletter/No90/0800.html>

## 05

### Route Origin Validation (ROV) が完了するまでの一連の流れ

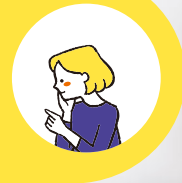
インターネット上でROVが機能するまでには、複数の技術とプロトコルがバトンをつなぐように役割を果たします。まず第一走者となるのは資源を保有するCA (Certification Authority) です。各CAは「このASがこのプリフィクスを広告してよい」という内容を暗号署名したROAを作成し、リポジトリへ配置します。配置時にはrsync用のディレクトリを生成するか、またはHTTPベースのRRDPエンドポイントを公開し、どちらの方式でも第三者が同一内容を取得できるようにします。

次にバトンを受け取るのがRelying Party (RP) ソフトウェアで、代表例としてRoutinatorなどが挙げられます。RPは数分から数十分ごとにrsyncあるいはRRDPを使って全リポジトリの最新ファイルをダウンロードし、前のものと比較することによって改ざんや欠落をチェックします。検証が通ったROA群からは、ルータで直接参照可能な形に整形したVRP (Validated ROA Payload) を生成します。VRPには「プリフィクス、最大長、Origin AS」という三つのパラメータが含まれ、これが経路の“通行許可証”として扱われます。

生成されたVRPは、RPKI-RTR (RFC 6810/8210) を介してルータへストリーム転送されます。RTRはTCP/SSH上で動作し、ルータはセッション確立後に「前回との差分だけ」をプッシュ形式で受け取るため、頻繁な更新でも帯域や無駄なリソースの負荷を抑えられます。こうして受け取ったVRPをルータはメモリ上にテーブルとして保持し、それをBGP更新メッセージと逐次突き合わせます。広告プリフィクスとOrigin ASがVRP内に完全一致すればValid、プリフィクスは含まれますがASが異なればInvalid、どのVRPにも合致しなければNot Foundと分類します。

最終的に、Validな経路は通常通りルーティングに採用され、Invalidはフィルタやlocal preferenceの変更で事実上排除され、Not Foundはポリシーに応じて通すか落とすかを決定します。こうしてROVのパイプラインが途切れなく回り続ける限り、設定ミスや悪意があるBGPハイジャックは、Data Planeに到達する前に高い確率で遮断される仕組みになっています。

## ▶▶▶ RPKI (Resource Public Key Infrastructure) とは



06

## 新技術ASPAについて

ASPAは、これまでROAだけでは防ぎ切れなかった経路リークやAS\_PATHの改ざんを暗号的に見つけ出すために設計された仕組みです。ROAが「そのプリフィクスのOrigin ASが正しいか」を保証する一方で、ASPAは「その経路は受け取っていいASから来ているか」を検証対象に据えます。やり方はきわめてシンプルで、顧客AS (Customer AS) が自分の上流 (Provider AS群) を署名付きオブジェクトに列挙し、これをRPKIリポジトリへ置くという仕組みになっています。PKIを使用した仕組みという点ではROAと同じ思想ですが、ASPAは「到着方向の妥当性」を判断できるため、発信者が正しくても途中の道のりが不自然というケースまで網羅できます。

Relying Partyは、リポジトリに置かれたASPAを定期的に取り込み、検証が済んだものをVAP (Validated ASPA Payload) という内部形式に変換します。ルータはRPKI-RTRセッションでVAPを受け取り、BGP UPDATEに含まれるAS\_PATHを左から右へ走査しながら、隣接ペアがVAPに登録された上下関係と一致するか照合します。たとえば、ある区間にあるtransit関係が実際には破綻しておりルートリークが起こっていたり、valley-freeの原則を無視してpeer間を抜け道にしていたりした場合、ルータは即座にInvalidとして経路を捨てます。こうして、ROAでは検出できなかった「正しいOriginだが経由ASが怪しい」という経路も表面化前に遮断できます。

標準化の状況を2025年6月時点の最新情報で整理すると、ASPAの構文を定めるdraft-ietf-sidrops-asma-profile-19が2025年2月に更新されたのち大きな技術変更はなく、ASN16/32の併用方法やCMSラッピングの細部がブラッシュアップされている段階です<sup>※3</sup>。一方、検証手順を規定するdraft-ietf-sidrops-asma-verification-22は3月末に発行され、SIDROPS WGのLast Callを通過後、IESGのAD Evaluationに進んでいます<sup>※4</sup>。議論は落ち着いており、2025年内にRFC番号が付く見込みが高まりました。関連技術としては、ASPAで扱えないneighborやcustomerの検証を補完するASRA (Autonomous System Relationship Authorization) が2025年5月に初版を公開し、今後の拡張先として注目されています。

実装面でも動きが速く、Relying PartyではRoutinatorがversion 0.15から--enable-asmaオプションで実運用テストを支援しており<sup>※5</sup>、OpenBSD由来のrpki-clientもversion 8でVAP出力を標準化しました。rpki-clientから生成されるBIRD用コンフィグは既にASPA セットを含む構造になっており、BIRD 2.16以降とはそのまま連携できます<sup>※6</sup>。ルーティングソフトウェアではOpenBGPD 8.5とBIRD 2.1.11がvalidationを実装済みで、部分導入でも効果は顕著で、たとえば自ASと直上流がASPAを発行し、自ASがVAPを参照するだけで、自ASから外部へ漏れる不正経路は封じ込められます。RFC 9234で定義されたBGP Rolesだけでは「お作法に反するルートリーク」を禁止できても、鍵を使った真正性検証までは踏み込めませんでした。ASPAを併用することでそのギャップが埋まります。

もっとも、運用上の課題も残っています。Unknown、つまりVAPに情報が存在しない経路をどう扱うかは事業者のポリシーに委ねられており、部分導入フェーズでは事業者ごとに異なる判断が混在します。また、大規模ASほど上流の数が多く、ASPAをメンテナンスする作業量が跳ね上がるため、自動化を検討するなどの手段を取る必要がある可能性があります。さらに、誤ったASPAオブジェクトを公開すると、それを経由する全経路が一斉にInvalid扱いになるという“広範囲の巻き添えリスク”があり、導入をためらう声もあります。それでも、「Originは正しいのにroute leakの可能性がある」というこれまでの死角を塞げる意義は大きく、ROAとASPAを併用することで、諸攻撃に対しての防御が可能になるでしょう。

※3 A Profile for Autonomous System Provider Authorization  
draft-ietf-sidrops-asma-profile-20  
<https://datatracker.ietf.org/doc/draft-ietf-sidrops-asma-profile/>

※4 BGP AS\_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects  
draft-ietf-sidrops-asma-verification-23  
<https://datatracker.ietf.org/doc/draft-ietf-sidrops-asma-verification/>

※5 ROUTINATOR - Advanced Features  
<https://routinator.docs.nlnetlabs.nl/en/stable/advanced-features.html>

※6 rpki-client 9.6  
<https://github.com/rpki-client/rpki-client-portable/releases>



運用フェーズになると、RPKIは「鍵を安全に保管し署名オブジェクトを確実に公開し続ける」というフローになります。小さな手抜きでもVRPが欠落し、最悪の場合は正当な経路が世界から見えなくなります。ここでは典型的な4種類のトラブルと、その背景にある設計上のポイント、さらに実際に北米で起こった鍵失効事故をまとめておきます。

まずは鍵やROAの有効期限切れです。証明書チェーンの中で最も短い残存期間がVRPの「実効期限」になるため、Relying Partyは数時間単位で期限を再評価し、切れた瞬間に該当VRPを丸ごと破棄します。その結果、該当プリフィクスはNot Foundとなり、厳格なROVポリシーを採るルータからは即座に経路が撤去されます。2023年には北米のローカルインターネットレジストリ(LIR)が鍵更新を失念し、/17プリフィクスが約40分間Not Foundとなり通信が途絶えた例が報告されました。これを機に、ARINは2023年5月以降のROAを自動更新対象に切り替え、管理者の介入なしで有効期限をロールオーバーする仕組みを導入しています<sup>※7</sup>。

Manifestの不整合も見逃ごせない問題です。Manifestは「リポジトリに存在すべきファイル名とハッシュ」を署名した状態で挙げますが、アップロードが途中で途切れて新旧ファイルが混在すると、Relying PartyはManifest検証に失敗し、そのCAが発行したすべての証明書を無視します。実態としては、有効なROAまで一斉に消える“巻き添え”が発生します。公開時はまず新しいファイル群を別ディレクトリに配置し、最後にManifestを置いてからシンボリックリンクを切り替える、といった原始的な公開手順が推奨されます。また、地理的に離れたCDNノードに複製して冗長化しておくのも、Relying Party側のタイムアウトを防ぐ上で効果的とされています<sup>※8</sup>。

次にrsyncサーバの停止やネットワーク分断です。rsyncは長距離TCPセッションを張りっぱなしにするため、片方向のパケットロスでも同期が止まります。Relying Partyが数回リトライしても接続できなければ、最後に取得した古いROAを更新しないまま使用して動作せざるを得ません。これを回避するには、HTTP/HTTPSベースで差分取得できるRRDPを併用し、Anycastで複数のパブリケーションポイントにトラフィックを散らす設計が多用されています<sup>※8</sup><sup>※9</sup>。

一方、単純にROAの発行の段階でミスが発生する可能性もゼロではありません。典型例は、顧客の/24に対しMaxLengthを/24のままにすべきところを/16まで広げてしまい、本来通すべき/23や/22がInvalid扱いになるケース、あるいは古いAS番号を残してOrigin ASを間違えるケースです。誤設定は即座に経路断につながるため、多くの事業者が申請と承認を別担当者が行う「フォーアイ・レビュー」を導入し、加えてCI/CDでlintチェックを走らせる運用に移行しています<sup>※10</sup>。

最後に、前述の北米での実例をもう少し詳しく振り返ります。2023年夏、複数のローカルISPが保有する鍵ペアの失効期日が深夜に到来しましたが、担当者は業務時間外で更新作業を忘れていました。失効直後にRelying Partyが新しいCRLを取得し、該当ROAを破棄。/17プリフィクスはBGP上でNot Foundと見なされ、下位の/20~/24も消失してしまいました。影響はCDNのキャッシュミスと相まってパケットロスとRTTの急上昇という形で表面化し、エンドユーザーからは「突然Webが遅い、つながらない」と報告が相次ぎました。およそ40分後に鍵が再発行され、ROAが再公開されると経路は自動的に復旧しましたが、この事故は「有効期限を確認し、必要に応じて更新をしなければ、RPKIが逆にSingle Point of failureになり得る」ことを示しました。その後、ARINはRESTful API経由で作成されたROAを自動更新対象に設定し、失効直前のロールオーバーをリポジトリ側で肩代わりするよう改修しています<sup>※7</sup>。

これらすべてをスケールさせることで、RPKIの強みは初めて定着します。経路を守る仕組み自体が新たな障害点にならないよう、運用部門とネットワーク部門が連携し、監視と手順の整備を継続していくことが肝要です。

※7 ARIN Bits: December 2023  
<https://www.arin.net/blog/2023/12/20/arin-bits-december-2023/>

※8 Stalloris: RPKI Downgrade Attack <https://arxiv.org/abs/2205.06064>

※9 rpkiller: Threat Analysis of the BGP Resource Public Key Infrastructure  
<https://dl.acm.org/doi/full/10.1145/3617182>

※10 BGP Origin Validation  
<https://nsrc.org/workshops/2021/riso-pern-apan51/networking/routing-security/en/presentations/BGP-Origin-Validation.pdf>



世界全体で見ると、RPKIの普及はようやく半数を超えました。MANRSが2025年1月に公表した年次レビューによれば、2024年

末時点でIPv4とIPv6のプリフィクスのおよそ54%がROAによって保護されており、Kentikのフローデータ分析でもインターネット

上を流れるトラフィックの74%がRPKI-validな経路宛てに到達していると報告されています<sup>※11</sup>。

APNICが2025年1月にまとめた“RPKI’s 2024 year in review”では、有効と判定されたIPv4アドレス空間が前年からさらに10%増え、 $1.66 \times 10^9$ アドレスに達したと示されました。RPKIのキャッシュに登録されたユニークOrigin ASも4万台後半まで伸びており、地理的にも組織的にも裾野が広がりつつあることが分かります<sup>※12</sup>。

ところが、経路を「宣言する側」と「受け入れる側」の両方が機能しなければ安全性とは言えません。Pallas Digitalが2024年末にまとめた業界動向レポートによると、ROVを実際に有効化しているネットワークは世界の約5%にとどまり、大手クラウド・CDN事業者とTier-1事業者が牽引する一方、中小ISPや企業ネットワークでは導入が著しく遅れていると指摘されています。

地域差も依然として大きい状況です。ARINが2025年4月の総会資料で示した数字によれば、北米 (ARINスコープ) のIPv4資源のうちRPKI-validと判定されるものは45%程度にすぎません。契約に基づきARINが管理するアドレスに限れば60%を超えますが、Legacy実装のまま残るアドレスが全体の歩みを押しとめていきます<sup>※13</sup>。

国内でも同じ課題を抱えつつ、対策が始まりました。JPNICは

2024年11月に中小事業者を対象とした運用ガイドラインを公開し、Portal APIを使ったワンクリックROA発行手順や、機器側の設定例、ROVの際のACL設定例を示しています。ガイドラインでは「2026年度末までに国内プリフィクスの70%をRPKI-valid化する」という数値目標を掲げ、導入支援ウェビナーや啓発セミナーを順次展開する予定です。

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」公開のお知らせ

<https://www.nic.ad.jp/ja/topics/2024/20241113-01.html>

※11

Year to Year Growth of the distributed RPKI database  
<https://manrs.org/2025/01/rpki-growth-2024/>

※12

The Evolving Landscape of BGP: Past Five Years, Present State, and Future Directions  
<https://pall.as/the-evolving-landscape-of-bgp/>

※13

Routing Security Update  
[https://www.arin.net/participate/meetings/ARIN55/materials/arin55\\_routingsecurity.pdf](https://www.arin.net/participate/meetings/ARIN55/materials/arin55_routingsecurity.pdf)

## 09

### 結論と今後の課題

RPKIは、これまで相互の信頼と慣習に頼ってきたBGPの経路制御に、公開鍵暗号を利用することで、インターネットの表札管理を自動化し、高い信頼性を与える枠組みです。リソース証明書とROAが発信者の正統性を担保し、そこに ASPAによるAS PATHの検証が加わることで、経路リークやハイジャックといった従来の脅威に二重の防御壁を築けるようになりました。2024年末にROAカバー率が50%を超えたという事実は、RPKIが世界に浸透しつつあることを示しています。とはいえ、RPKIは「証明書を出す側」と「それを検証して経路を落とす側」の両方が揃って初めて最大化されます。ROVはいまだ一桁台にとどまり、中小ISPやエンタープライズの取り組みは後れを取っていますが、主要クラウドやIXが相次いで“Invalid経路を拒否する”方針を打ち出したことで、未対応ネットワークに対する外圧は日に日に強まっています。

運用現場では、鍵の有効期限切れやManifestの不整合といった事柄が、正当な経路をNot foundやInvalidへ転落させることを

防ぎます。自動更新ジョブやフォーアイ・レビューの導入、RRDPとrsyncの二重化、Anycastなど、些細に見える運用の手当てがRPKIの鍵になります。特に鍵管理とリポジトリ配信の自動化は、導入規模が大きくなるほど必須の整備項目です。

BGPハイジャックは、経路を誤誘導だけでなく、通信の遅延や遮断、最悪の場合はトラフィックの盗聴につながる深刻な問題です。RPKIを採用することで、こうした事故を抑止し、問題が起きた際にも「どこが正しかったか」を機械的に切り分けられるようになります。今後、ASPAがRFCとして確定し、その他のルーティングセキュリティに関わる技術を活用することが当たり前になれば、より安全にインターネットを利用できるようになるでしょう。早い段階で鍵運用を自動化し、自ASのプリフィクスと上流関係を公開鍵で証明しておくことこそが、健全で信頼される経路広告への第一歩となります。

(慶應義塾大学 島田怜奈)