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、本号より前後編の2回に分けて解説をします。

※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

01 概要

インターネットは、AS（Autonomous System）と呼ばれるネットワーク同士がつながって形作られています。Autonomous System（自律システム）は、元来、ルーティング（経路制御）に関わる考え方の範囲の意味で、おのおののネットワークで独立してルータの設定が行われ、世界規模のルーティングを成立させています。このルーティングは動的ルーティングと呼ばれ、BGPというプロトコルが多く使われています。BGPで相互に伝搬される経路情報（経路制御に関する情報）においては、何が正しいのかを示すことは難しく、真正性を保証する仕組みがありません。IPv4アドレスの在庫枯渇時期が予測されていた2000年代、不正なIPアドレスの利用すなわち不正な経路情報に対する懸念が地域インターネットレジストリ（RIR）等のコミュニティで挙げられていた中で登場したのがRPKIです。RPKIはPKI（公開鍵暗号基盤の仕組み）を用いて「どのIPアドレスがレジストリによって正しく分配されたものか」を証明するもので、あるIPプリフィクスに対するOrigin ASを示す、ROA（Route Origination Authorization）の署名検証をするためなどに使われます。RPKIやROAを使うことで、BGPルータにおける設定ミスや不正な設定を通じた攻撃行為（意図的に不正経路情報を伝搬させることで経路を不正に操作などする行為）への対策となります。

02 BGPと経路情報の正しさ

AS と BGP

ホスト同士がIPを使った通信を行うためには、相手のIPアドレスを指定したIPパケットをルータ同士が適切な経路で転送していく必要があります。この転送先を定める情報の集まりは経路表と呼ばれ、経路表に新たに加えられたり削除されたりする情報をルータ同士がやり取りしています。その通信プロトコルの一つがBGPです。

BGPはどのASを通って宛先に到達するのかを伝えるパス・

［ テーマ ］

▶▶▶ RPKI（Resource Public Key Infrastructure）とは

ベクタ型プロトコルと呼ばれる方式を採用し、BGPメッセージを通じてIPアドレスの情報やASパス（経由するASの情報）が伝えられます。不正経路と関係のあるBGPメッセージを示したのが次の表1です。

表1 BGP経路情報に含まれる属性と不正経路の選択との関係

属性名	通常の使われ方	不正経路との関係やリスク
AS PATH	BGPメッセージで伝えられる通過したASのリスト。近い経路を選択するために使われる。	不正なBGP経路においてAS_PATHを偽装して短い=より近傍かのように伝搬させることで本来の経路よりも優先される。
ORIGIN	経路情報の広告元のAS番号を示す。	AS番号を詐称した不正なBGP経路においては本来のAS番号と同一になるが、BGPにおいてはAS間のピアの設定が必要であるため偽装可能な協力者が必要になる。 AS番号を偽装しなくてもORIGINが本来とは異なる経路情報の広報は可能である。これにより、特定の宛先IPアドレスへの経路を不正に変えることが可能。

AS間の通信にはeBGP、同一AS内の通信にはiBGPが使われます。本稿ではAS同士でやり取りされる経路情報のセキュリティについて述べるため、BGPと呼ぶ際にはeBGPを意味するものとします。

BGPでは、あるIPプリフィクスへの到達性について「この経路を自分のASで扱える」と広告し（advertisement=アドバタイズメント）、その際に経路属性などの情報を添えて伝えます。

BGPにおける属性値は、BGPを扱うルータの設定値に従ってBGPメッセージに入れられて伝えられます。つまり、オペレーターが設定をミスしたり、場合によってはあえて不正な値が伝わるようにしたりすることで、間違った経路情報が伝

えられることになります。その場合、BGPのパス・ベクター方式では、経路情報は基本的に全体のASに伝えられるため、多くのASが影響を受ける可能性があります。

数多くのASが存在するインターネットにおいて、正しい経路情報をBGPで扱うためにはどうすればよいのでしょうか。歴史的には、IRR（Internet Routing Registry）と呼ばれる登録／検索システムが使われてきました。ASが扱う経路情報や連絡先の情報を登録し、場合によってはプログラムを使って、BGPでやり取りされる情報から、IRRの登録情報と齟齬がないものを取り入れるといった具合に使われてきました。しかしIRRに登録される情報は、必ずしも正しいものとは限らず、またメンテナンスされにくい側面があったため、いわゆる決定打となる情報がない状態が続いてきました。

03 RPKIと利用 ── 全体像

BGPのような情報の正しさを確認できないプロトコルにおいて、IPアドレスやAS番号といった、登録管理されている情報に基づいて正しさを確認できるようにする、さらには、国際的に流通する経路情報のような情報を、分散的に、かつプログラムで処理できるようにする仕組みがRPKI（リソースPKI）です。

RPKIは、IPアドレスやAS番号をリソースと呼び、リソースが正しく分配されたことをX.509形式の電子証明書で表現するものとして考案されたものです。具体的にはX.509v3拡張フィールドに、証明書発行対象に分配されているIPアドレスやAS番号が記載されます。IPアドレスの分配構造と同様に、分配を受けた者は、その範囲内でさらに分配、すなわち電子証明書を発行することができ、RPKIの証明書ツリーはリソースの分配構造に沿って構成されることになります。

従来のBGPでは、どのASがどのプリフィクスを広告してよいかの情報はIRRのように登録に基づく情報しか存在せず、正しさを検証する方法は限られていました。RPKIは、アドレス資源の分配を行うRIR（Regional Internet Registry）などのレジストリが、アドレス資源の分配構造に従って証明書を使って、あるIPアドレスやAS番号がレジストリを経由して正しく分配されたものかどうかを確認できるようにしたのです。このアーキテクチャを定義したものが、2012年に策定されたRFC 6480です。

RPKIの証明書は、公開鍵とともに「この AS／この IPブロックをいつまで、どの範囲まで使ってよい」という情報をX.509v3拡張フィールドに格納します。また他の拡張フィールドには、そのCA（Certification Authority、信頼できる証明書の発行元組織）が提供するリポジトリのURI（subjectInfoAccess）が入ります。リポジトリでは、rsyncと軽量 HTTP ベースのRRDP（RPKI Repository Delta Protocol）というプロトコルの二系統でファイルが配布されます。

全体像は次のように動作します:

1.CAが新たなリソースを委譲するときはCA証明書とROA（Route Origin Authorization）を生成し、それらをManifestという目録に記載して署名します。また、CRL（Certificate Revocation List：証明書失効リスト）を公開します。

2.検証を行う者はManifestを照合して「リポジトリから欠落しているファイルはないか」「ハッシュ値が改ざんされていないか」を確認し、差分をダウンロードします。

3.検証する側では、RPKIを通じて作成されたROA等のファイル全体の整合性が保たれた状態になります。

注目されるのは、これらの処理結果がBGPルータに伝えられて処理される点です。ルータはRPKI-RTRという軽量プロトコルで「このプリフィクスとASの組み合わせはValid／

Invalid／Not Foundのどれか」を伝えてもらい、経路選択ロジックの最上位でフィルタリングを行います。結果として、誤設定や悪意ある経路情報が悪影響を及ぼす前に遮断することができるというわけです。

04 ROA・Manifest・CRL

本節では、RPKIにおけるデータとおのおのの役割について述べます。

4.1 ROA

ROA（Route Origin Authorization）は、「どのASが、どのプリフィクスを、どこまで分割して良いか」を示す署名付きオブジェクトです。作成時にはまず対象となるプリフィクスを決め、正当な広告者であるオリジンASを一つだけ指定し、最後にそのプリフィクスをどこまで分割してもよいかを示す最大プリフィクス長（MaxLength）を指定します。たとえば、203.0.113.0／24に対してMaxLengthを／24に固定すれば、／25や／26など細かい経路の広告は自動的に「Invalid」と判定されます。生成されたROAはリソース証明書の公開鍵に対応する鍵で署名され、リポジトリに置かれます。ROAの利用者は RPKIの証明書チェーンを検証することで、経路広告されているプリフィクスとオリジンASの組み合わせが、あらかじめ指定されたものであることを判定できます。この判定結果は、ROA等の署名検証を行う“RPKIキャッシュサーバ”に保持されます。BGPルータでは、RPKI-RTRプロトコルを通じてValid／Invalid／Not Foundといった判定結果をRPKIキャッシュサーバから受け取り、これをBGP経路表に入れるかどうかの判断に利用します。

4.2 Manifest と CRL

Manifestは、リソース証明書やROAといった、CAが発行した“存在すべきファイル”とそれぞれのハッシュ値を署名付きで格納したデータです。RPKIキャッシュサーバはManifestとダウンロードしたファイルとを照合します。欠落や改ざんを検知した場合には、その時点でその一式を利用しないように機能します。これにより、意図せぬファイル削除や中間者攻撃による置換を防ぐことができます。

CRL（Certificate Revocation List）は、失効済みのリソース証明書を列挙した署名付きリストで、資源が返却されて証明書が不要になった場合などに利用されます。RPKIキャッシュサーバは、CRLのタイムスタンプと署名を確認し、リストに含まれる証明書を無効なものとして扱います。Manifestが「あるべきものを保証する」仕組みだとすれば、CRLは「無効にすべきものを示す」位置づけです。両者が相補的に機能することで、RPKIリポジトリ全体の完全性と最新性が担保されるような仕組みになっています。

（慶應義塾大学 島田怜奈）

後編となる次号では、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。