特集 Special Article 2

RPKIシステムの試験的な提供開始について

2015年3月3日、JPNICではRPKI（リソースPKI）システムの試験的な提供を開始しました。RPKIはIPアドレスの記載された「リソース証明書」を発行する技術で、インターネットの経路の安全性を高める応用技術として注目されています。

本稿では、インターネットの経路制御におけるセキュリティと、RPKIを使ったOrigin validation、JPNICがRPKIの認証局を構築する意味、そしてRPKIシステムの使い方を紹介します。

インターネットの経路制御におけるセキュリティ

インターネットは、ISPや企業などで運用されるAS（Autonomous System）のネットワークが相互に接続することで構成されています。ASの間では、BGP（Border Gateway Protocol）を使ってIPパケットの到達性を得るための「経路情報」が交換されています。この仕組みによって、IPアドレスが使われている場所（具体的にはAS）が変わっても、インターネットから到達することができるようになっています（図1）。

図1：AS間ルーティングとBGP

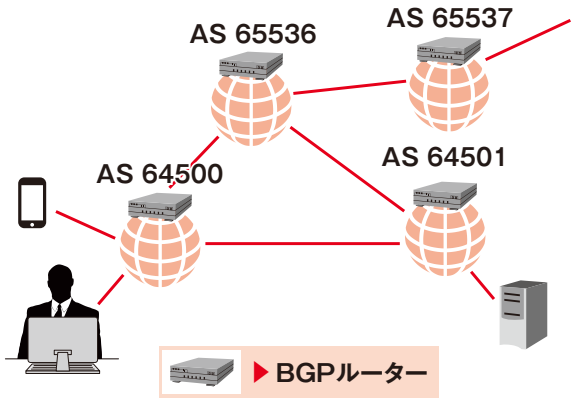


図1はAS間ルーティングとBGPの関係を示しています。ASには、割り当てられたAS番号と、収容しているIPアドレスの情報を交換する「BGPルーター」があります。近年、このBGPルーターが交換する情報である「経路情報」の中に、本来とは異なるAS番号が含まれた情報が見つかっています。これは mis-origination（IPアドレスを使っているASが本来とは異なること）と呼ばれ、本来IPアドレスを使っているべきASとは異なるASによって、IPアドレスが使われている状態を示しています。このIPアドレスが使われると、パケットの送信元を特定しにくいため、スパムメールや攻撃パケットの送信のために使われることがあります。そして同時に、WHOISに本来の割り当て先が登録されているため、本来のIPアドレスの割り当て先からスパムメールや攻撃パケットが送られたかのように見られてしまう恐れもあります。

インターネットへの接続のために使われるIPアドレスが増加するのに伴い、BGPの経路情報は処理のできないルーターが出てくると言われる50万エントリを超えるほどに増加してきました。数多くの経路情報から正しい経路情報と本来とは異なる経路情報を判別する手法の一つが、発信元のAS番号を確認する技術 Origin validationです。

Origin validationとRPKI

Origin validationは、ROA（Route Origination Authorization）という、IPアドレスとAS番号が記載されたBGPの経路情報とは独立したデータを使って、本来とは異なる経路情報を見つける技術です。Origin validationに対応したBGPルーターを使うと、受け取った経路情報の中で以下のような三つの区分けを行うことができます。

- ROAに合致する（Valid）
- ROAに合致しない（Invalid）
- 一致するIPアドレスが記載されたROAが見つからない（Not found）

BGPルーターにおいてInvalidに区分けされた経路情報の優先度を下げたり、ROAを使って経路情報を監視したりすることで、インターネットにおけるルーティングのセキュリティに役立つと考えられています。

ROAは、レジストリやIPアドレスの割り振り先の組織によって発行されるリソース証明書を使って確認されます。つまりROAの検証と同時に、正しく割り当てられたIPアドレスであることが確認されるようになります。リソース証明書の発行を行うのがRPKIです。2015年6月現在、すべての地域インターネットレジストリ（RIR; Regional Internet Registry）でRPKIの認証局が立ち上げられ、リソース証明書が提供されています。

国際的に、IPアドレス空間に対するROAのカバー率はまだまだ低いものの、特に主にヨーロッパのIPアドレスを管理しているRIPE NCCの地域で伸びてきています。Origin validationは、シスコシステムズ社やジュニパーネットワークス社、アルカテル・ルーセント社といった大手ルーターベンダーによってサポートされており、ルーティングのセキュリティにおいて注目されている技術の一つです。

・インターネット1分用語解説：リソースPKIとは
https://www.nic.ad.jp/ja/basics/terms/resource-pki.html

JPNICがRPKIの認証局を構築する意味

アジア太平洋地域では、IPアドレスを共有化されたプールから各国の国別インターネットレジストリ（NIR; National Internet Registry）が割り振りを行う「共有プール」化が行われました。共有プールからIPアドレスの分配を受けている場合には、直接APNICのリソース証明書の発行を受けられることになります。

一方、日本では、CIDR（Classless Inter-Domain Routing）へとIPアドレスの管理方法が変わる前から、IPアドレスが分配されてきました。分配の経緯とポリシーが異なったIPアドレスブロックが混在する中でRPKIを構成するには、それぞれのブロックの違いを吸収しつつ、IPアドレスの申請を行われている方が使いやすいような構造にしていく必要があります。そのためには、JPNICでRPKIの認証局を運用し、リソース証明書を発行する仕組みが必要です。

またその実現には、JPNICのレジストリデータベース（WHOISデータベース）と連携し、国内における最新の割り振りに基づいたリソース証明書が発行できること、日本語でわかりやすいユーザーインタフェースを持つこと、といったことが必要になってきます。日本のWHOISの情報に基づいたRPKIの構築のため、2014年度に開発を行い、2015年3月に試験提供を開始したのがJPNICのRPKIシステムです。

JPNICのRPKIシステムの使い方

JPNICのRPKIシステムは、RIRと同等の仕組みを国内でも提供できるように構築されました。RIPE NCCやAPNICと同様に、リソース証明書の発行やROAの作成を行うためには、「ROA Web」と「BPKI接続」の二つの利用方式があります。

（1）ROA Web（ROA発行代行機能）

Webインタフェースを使って、リソース証明書の自動発行やROA発行ができる仕組みです。ユーザーの認証には資源申請者証明書を使うため、IPアドレスに関する申請を行うことができる方は、リソース証明書の自動発行の開始や停止、ROAの作成や削除ができます。

ROA Webには、JPNICから発行されている「資源申請者証明書」を使って、次のページの「RPKIシステムへアクセス」をクリックしてアクセスします。

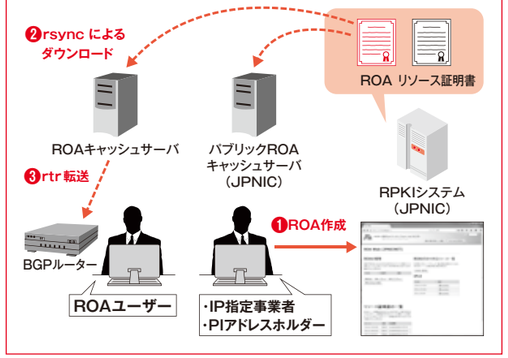
リソースPKI（RPKI）
http://rpki.nic.ad.jp/

資源申請者証明書は証明書の名称が LIR-HM, HPI-HM, SPI-HMで始まるユーザー向けの証明書です。あらかじめ資源管理者証明書（JPNICのIPアドレス管理指定事業者（IP指定事業者）の場合には資源管理カード）を使って、発行しておく必要があります。

図2：ROA Web（ROA発行代行機能）

ROA Web（図2）に初めてアクセスすると、ご利用条件のほか、二つの利用方式を選択する画面が表示されます。「ROA Webを開始」をクリックすると、リソース証明書の発行が開始されます。リソース証明書の発行が終わると、次にROAを作成できるようになります。リソース証明書は自動更新される仕組みになっています。ROAが作成されると、RPKIシステムからダウンロードできる状態になり、rsyncを使ってダウンロードすることができます。ダウンロードされたROAをROAキャッシュサーバで検証し、これをBGPルーターからRPKI-to-Routerプロトコルを使って参照することで、Origin validationの結果をBGPルーターで利用できます（図3）。

図3：ROA Webを使ったROAの利用までの流れ



作成されたROAやリソース証明書は、パブリックROAキャッシュサーバやUNIXサーバなどを使って立ち上げたROAキャッシュサーバを使ってダウンロードし、Origin validationのために使うことができます。詳しくは次のURLをご覧ください。

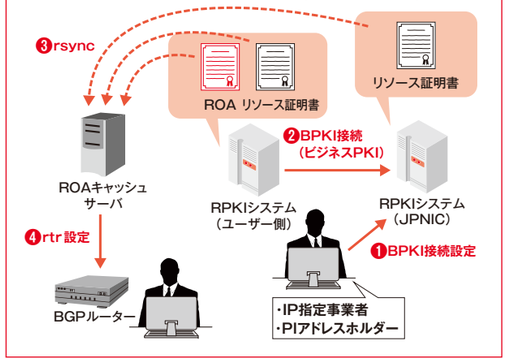
ROAキャッシュサーバの設置方法
https://www.nic.ad.jp/ja/rpki/howto-setuproacache.html

（2）BPKI接続

BPKI（Business PKI）とは、リソース証明書の発行に必要なIPアドレスの情報などを、RPKIシステムの間で交換するために使われる仕組みです。BPKIを使ってJPNICのRPKIシステムと接続するとRPKIのリポジトリサーバを、JPNICとは独立して運用することができ、リソース証明書やROAの有効性に関するリスクを1ヶ所に集中させないことが可能です（図4、図5）。

図4：BPKI（ビジネスPKI）の設定画面

図5：ROAご利用までの流れ（BPKI接続）



◇　◇　◇

（1）（2）のどちらかを選んで利用を開始すると、以後その方式でリソース証明書が発行されます。利用方式を変えるには一度RPKIの利用を停止して、方式を選択しなおす必要があります。「利用を停止」ボタンをクリックすると、発行済みのリソース証明書やROAがすべて失効されますので、ご注意ください。

ROAの登録とIPアドレスのセキュリティ

ROAを登録しておくと、インターネットのほかのASから、経路情報の正しさを確認できるようになります。IPアドレスが勝手に他のASによって使われてしまったような場合でも、他のASがこれを検知し、不正な経路情報を無視するといった連携を図ることが可能です。IPアドレスの割り振り／割り当てを受けている皆さまには、ROAの登録を行うことをおすすめします。

ROAの登録には、前述の資源申請者証明書が必要であるほか、IPアドレスの経路広告を行うAS番号がわかっている必要がありますので、この機会に一度ご確認いただければ幸いです。RPKIに関する情報は、リソースPKI（RPKI）のページで公開しています。

RPKIについてご不明な点などがありましたら、RPKI担当 <rpki-query@nic.ad.jp> までご連絡をお願いします。

（JPNIC 技術部／インターネット推進部 木村泰司）