特集1 Special Article

RPKIのAPNICとの連携開始! 海外からも国内経路が検証可能に

～ RPKIの最新動向とルート・リークの対策について ～

2017年7月の下旬にAPNICとJPNICとの間で、RPKIシステムの連携が始まりました。RPKI（リソースPKI）は、IPアドレスなどが記載された電子証明書を発行する認証基盤の技術です。電子証明書を応用することでBGPにおける経路情報をチェックし、不正な経路情報を検知する仕組みとして使うことができるもので、今回のAPNICとの連携によって、国内からだけでなく海外からも、日本の経路情報が検証できるようになりました。

本稿では、この連携の意義についてまとめるとともに、AS運用者が本来は広く公開する意図はなかったにもかかわらず、設定ミスなどによって優先度の高い経路情報が流れてしまうルート・リークについて取り上げ、その対策を考察します。

RPKIの証明書チェーンを本来の形に

リソースPKI（RPKI）は、IPアドレスやAS番号といった、番号資源の分配を証明する認証基盤です。RPKIで配布する電子証明書であるリソース証明書は、レジストリの木（ツリー）構造に合わせた形で発行されるのが本来の形です 図1 。しかし、RPKIは個々のRIRやNIRが独立して作り始めたため、これまではレジストリの木構造の途中からという形になっていました。

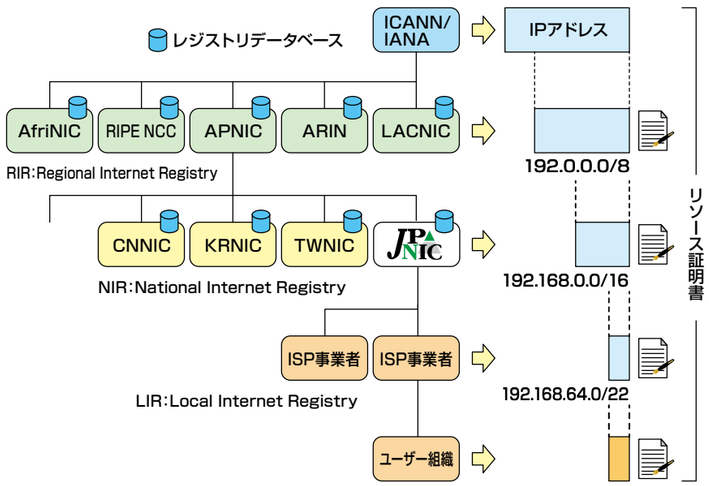
APNICとの連携に至るまで

RPKIを実現するシステムは、地域インターネットレジストリ（RIR）や国別インターネットレジストリ（NIR）といったレジストリがおのおの運用する認証局システムを連携させて、IPアドレスの分配について整合性を保ちながら稼働する仕組みになっています。RPKIシステムは、レジストリデータベースとのデータ連係とともに上位認証局との間で、リソース証明書に記載するIPアドレスについての整合性を保つ連携を行う必要があります。

JPNICでは、まずは試験提供として、2015年3月からRPKIサービスを開始しました。サービス開始当初は、APNICとの連携に先立って、JPNICが分配したIPアドレスのリソース証明書を利用できるようにするために、JPNICのレジストリデータベースに基づくリソース証明書を発行しました。そのため、JPNICから分配されたIPアドレスのリソース証明書は、JPNICのトラストアンカー※1を使って検証する形になっていました。

APNICのRPKIシステムとJPNICのRPKIシステムで、システム間の連携を実現するためには、いくつかの課題がありました。連携システムの開発作業中にもRPKIに関する技術の標準化が進んだことで、連携の形式などにも変更が発生し対応が必要になりました。また、APNICにおける証明書の発行方法が、他のRIRと比べて特殊な方式であったこと※2も、連携にあたって解決しなければいけない課題でした。これらの課題はすべて、実際にRPKIのシステムを運用しながら開発したものを、連携のためのシステムに組み込んでいくような技術課題でした。こういった課題の解決にあたってはAPNICとJPNICの双方で取り組み、APNICで複数の連携形式に対応してもらったり、JPNICでさまざまな証明書ツリーの形に対応できる改良を行ったりすることで、この度の連携が実現しました。

図1 RPKIのリソース証明書の構造



ROAを使った経路広告元の検証も可能に

RPKIを使う仕組みの一つに、ROA（Route Origination Authorization）を使ったBGP経路のオリジン検証（Origin Validation）があります。これまでは、JPNICが分配したIPアドレスを含むROAは、JPNICのRPKIの証明書ツリーを辿ることでしか署名検証を行うことができなかったため、JPNICのトラストアンカーを使わなければ、検証することができませんでした。

この度の連携によりこういった制約が解消され、APNICのトラストアンカーを使って、JPNICのRPKIシステムを使って発行されたROAが検証できるようになりました。RPKI ToolsやRPKI Validatorといった、デフォルトでRIRのトラストアンカーしか持たないオープンソースソフトウェアで、JPNICの分配アドレスを含むROAを検証できます。

BGP経路モニタリングへの応用

BGP経路のモニタリングを行うサービスの一つに、BGPMONがあります※3。BGPMONでは、RIRのトラストアンカーを使ったROAの検証が行われていました。この度の連携によって、JPNICから分配されたIPアドレスについても、BGPMONでROAの検証結果が見られるようになりました 図2 。

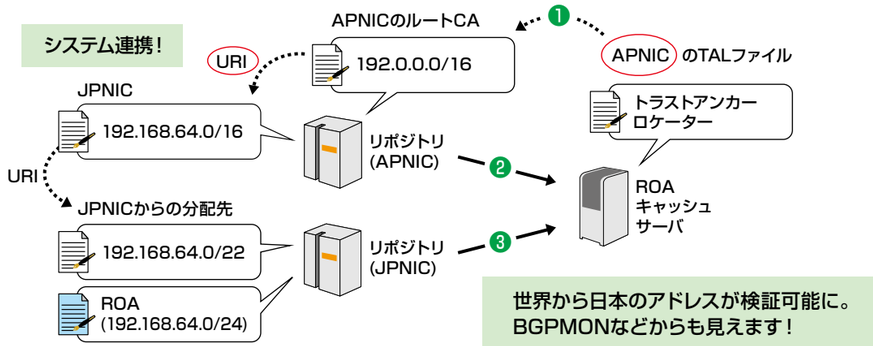
APNICとNIRの連携に役立つ仕組みに

APNICが担当するアジア太平洋地域は、五つのRIRの中でNIRがもっとも多く存在している地域です。各国のNIRから分配された番号資源のRPKIを構築していくにあたっては、それぞれのNIR単位で、自身のリソース証明書を発行する形が考えられます。その際に、各NIRとAPNICとの間でJPNICと同様の連携を行おうとする場合には、この度APNICとJPNICで得られた知識や仕組みが役立つと思われます。JPNICでは、2017年6月にRPKIサービスを開始しAPNICとの接続に向けた作業が進められているCNNICと技術的な情報交換を行っており、双方で技術ノウハウが蓄積されつつあります。

ルート・リークとBGPsec

ルート・リークとは、本来は特定のASや特定のASの間だけで使われている細かい経路情報が、他のASに伝わってしまうことを言います。意図的に細かい経路を扱うことで、ネットワーク的に近い経路を作るといった制御のために使われています。通常は他のASに伝わってしまわないような設定がなされていますが、設定変更のタイミングなどで自AS外に流れてしまうことが起こり得るため、可能な場合には経路情報を受け取るASでフィルタリングするといった対策が採られています。ここで言う細かい経路とは、IPアドレスにおけるネットワーク部を示す、ビット長の長い経路情報のことで、長いほど少ない数のノードを収容したネットワークを示します。例えば、「172.16.0.0/22」よりも「172.16.0.0/24」の方が長い（細かい）経路となり、BGPを使った経路制御においては短いものよりも優先されます。2017年8月25日に起きた通信障害は、このルート・リークが原因とされており、その検知と各ASで利用できる対策技術が、BGPオペレーターの間で話題となっています※4。

図2 APNICのトラストアンカーを使って JPNICから分配されたIPアドレスを含むROAが検証できる



※1 JPNICのトラストアンカー
リソース証明書は、トラストアンカーからツリー状に発行された証明書を収集して検証されます。JPNICのトラストアンカーを使うための設定ファイルであるTAL（Trust Anchor Locator）を下記で公開しています。
https://serv.nic.ad.jp/capub/rpki/jpnic-preliminary-ca-s1.tal

※2 APNICの証明書発行方式
APNICでは、他のRIRから移転されたIPアドレスを別々の認証局で扱うために、トラストアンカーを五つ設けています。2017年10月現在、2018年1月の作業完了をめどに、トラストアンカーを一つに統一する計画が進められています。

※3 BGPMON
https://bgpmon.net/

※4 IRS27 - Inter-Domain Routing Security
http://irs.ietf.to/wiki.cgi?page=IRS27

ルート・リークは、これまでにも国際的に起きているもので、リークそのものをなくすよりも、他のASで影響を受けないようにするにはどうすればいいのか、といった議論が行われてきました。前述の通り、RPKIの連携によって、国際的に日本国内のIPアドレスを検証できるようになりましたので、ここではRPKIを使った経路情報の検査技術であるBGPsecを使って、どのような対策を採ることができるのかについて、考察してみたいと思います。

BGPsecは、BGPの経路情報に対して、オリジン検証(Origin Validation)とパス検証(AS Path Validation)の、2種類の検査を行うことができる技術です。パス検証はまだ実装が進んでいませんが、オリジン検証のオープンソースソフトウェアや、その結果を扱うことのできるルータは増えてきています。

まずはじめに、今後の普及を見越してパス検証の利用について考えてみます。現在の仕様では、ルート・リークが起きた時にも、その経路情報を受け取ったASが正常な署名を付けてしまうことが考えられます。そうすると、ルート・リークの経路が有効なパスとなってしまいます。

受け取ったパスを自動的にASパスに対する署名データであるBGPSEC_PATHに加えるのではなく、指定したASが含まれるパスのみに署名をつけることによってこれを回避し、異常を発見するために使うことができるかもしれません。ただし、まだこのような仕様についての議論はなされていない状況です。この他に、パス検証を行う側で、X.509証明書の証明書チェーンに深さ制限を設けられるように、検証するパス(BGPSEC_PATH)の長さに制限を設けることも考えられます。

また実装にあたっては、RPKIの導入効果について研究しているボストン大学のSharon Goldberg氏が指摘しているように※5、環境によっては受け取ったパスの検証結果がinvalidであっても、使わざるを得ないことも考えられます。パス検証はまだ実験できる状態になっていないため、ルータにおける実装の要件を見つけていくために、各種の想定実験が必要と考えられます。

次に、オリジン検証で検知できることについても考えてみます。ROAには最大プリフィクス長を制限するパラメーターがあり、リーク時の細かい経路が、異常である旨の検知ができる可能性があります。ただし、検知後のアクションに制約があり、優先度を下げた程度では、BGPにおける細かい経路情報を優先する原則が優先されてしまうため、せっかく無効と判定できた経路情報であっても、その判断を経路変更の判断に利用できないという指摘があります。

ここまでで述べたように、RPKIの利用環境は整備されつつありますが、各種のルーティングにおけるインシデントを検知し、もしくは予防する技術に至るまでには、まだ課題があります。実用化のためには、さらなる実験や、ツールの開発を行っていく必要がありそうです。

(JPNIC 技術部／インターネット推進部 木村泰司)

※5 BGP Security in Partial Deployment, Robert Lychev, Sharon Goldberg, Michael Schapira, SIGCOMM'13, August 2013
http://www.cs.bu.edu/~goldbe/papers/partialSec.pdf

JPNICの後藤滋樹理事長がISOCインターネットの殿堂入り

2017年9月18日17時半(PDT、JSTでは9月19日9時半)、Internet Society (ISOC)が、2017年選出の「インターネットの殿堂(Internet Hall of Fame)」入りメンバー 14名を発表しました。その中で、JPNICの理事長を務める後藤滋樹(早稲田大学 理工学術院 基幹理工学部 情報理工学科 教授)が、「インターネットのグローバルな成長と利用に著しい貢献をした個人」として「グローバルコネクター部門」にて殿堂入りを果たしました。

・Visionaries Who Helped Shape the Internet Take Their Place in the Internet Hall of Fame
https://www.internetsociety.org/news/press-releases/2017/visionaries-helped-shape-internet-take-place-internet-hall-fame/

今回の殿堂入りにあたって後藤本人からのコメント

今回の殿堂入りの理由となっている複数の業績は、いずれも私1人が成し遂げたものではありません。多数の友人が実践してくれたものです。先輩の理解と指導も不可欠でした。本来はグループとして顕彰されるべきものです。たまたま私が職場の仲間の年長であったり、大学人は中立であるという想定で、私が名前だけの代表のようになった経緯があります。ただ、私が個人的に遠慮をすると、多くの友人の業績が埋もれてしまうかもしれないと考えて、仲間を代表する気持ちで受けることにしました。関係各位に厚く御礼申し上げます。

・Interview: 2017 Internet Hall of Fame Inductee Shigeki Goto
https://youtu.be/n-ds-qBwQXY

・2017年 インターネット殿堂入りメンバー一覧
https://www.internethalloffame.org/inductees

理事長の後藤をはじめ、JPNICは今後もより一層、国内外のインターネットの発展へ貢献してまいります。