特集

# 国際的に整備が進められるリソースPKI

2008年にリソース証明書を提供し始めたAPNICに加えて、RIPE NCCやARINでも同様の試験的な提供が始まりました。RIRでは、2011年頃と予測されているIPv4アドレスの在庫枯渇時期よりも前の2010年度に、リソース証明書のための「リソースPKI」を準備すると言われています。特集1では、このリソースPKIの国際動向をお送りします。

## リソース証明書とリソースPKI

2009年、新たにRIPE NCCやARINでリソース証明書の提供が開始されました。リソース証明書は、WHOISを使わなくても、IPアドレスやAS番号がインターネットレジストリを通じて割り振られたものかどうか、端的に言えば不正に使われているIPアドレスか否かを判別するための仕組みです。リソースとは、アドレス資源、すなわちIPアドレスやAS番号のことを指しています。

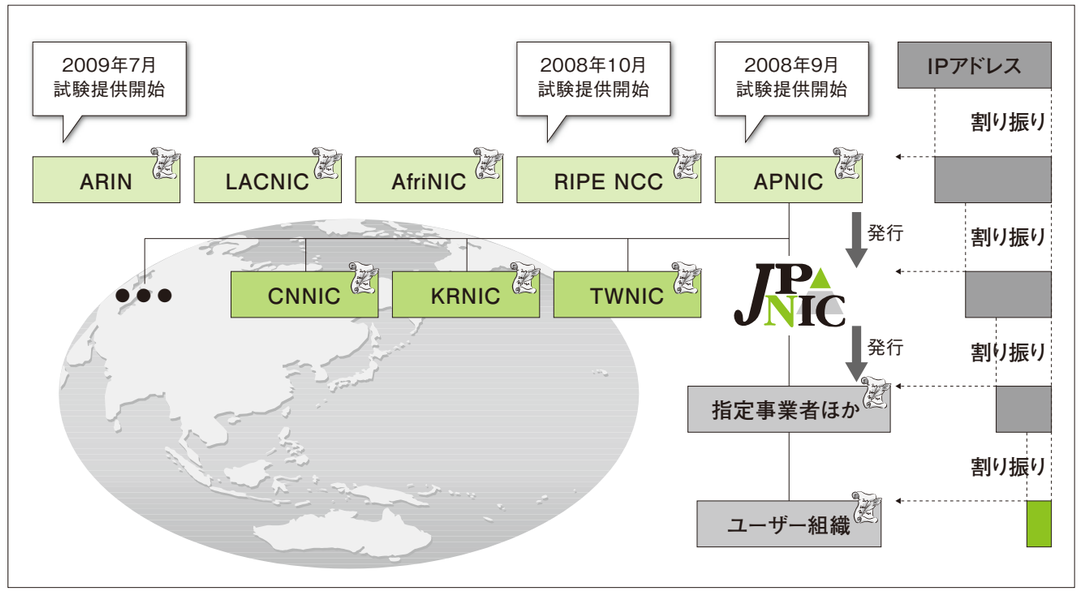
このリソース証明書を国際的に利用できるようにするため、RIRでは「リソースPKI」の整備が進んでいます。リソースPKIは、IPアドレスの割り振りや割り当ての構造に合わせてリソース認証局を設置することで、アドレス資源の利用者がリソース証明書の正しさを確認できるようにするものです。グローバルIPアドレスのリソースPKIは、図1のようにツリー構造になります。

図1の中でAPNICは2008年9月、RIPE NCCは2008年10月、ARINでは2009年7月に試験的に提供を開始しました。LACNICやAfriNICでも、リソース証明書に関する議論が行われています。

## リソースPKI開発の経緯

リソースPKIのアイデアは、1997年頃、BBNテクノロジー社のStephen Kent氏、Charles Lynn氏らによって考案されました。当時研究が進められていたSecure BGP※1がそれで、IPアドレスやAS番号の正しさを担保するための仕組みです。伝搬してきたIPアドレスやAS番号を記載した情報（以下、「経路情報」と呼ぶ）のIPアドレスが正しいかどうかを確認し、不正な操作が行われている経路情報はルータで受け入れを拒否することができるメカニズムです。

図1：国際的な整備が進められるリソースPKI




BGPでは、インターネットでのIPパケットの到達性を確保するため、BGPルータ間で経路情報を交換しています。しかし、経路情報はいくつものBGPルータを経由して伝わっていくため、途中で変更が加えられていても、それを受信したBGPルータには変更が加えられたことはわかりません。また、経路情報の発信元であるBGPルータが、自組織に割り当てられていないような不正なIPアドレスを経路情報に記載していても、それが正しいかどうかを自動的に判別することは容易にはできません。

偽の経路情報を流すことができると、IPパケットの通る経路を、不正に操作することができる可能性があります。例えば、他の組織に割り当てられたIPアドレスを不正に使ったり、特定の組織のパケットを横取りして盗聴したり、目的のネットワークをインターネットに到達できないようにしたりすることが可能です※2。近年ではYouTubeのWebページが、ISPの意図的な経路広告によって閲覧できなくなった事件が有名です※3。

## リソースPKIの目的

前節で述べたように、リソースPKIはもともとインターネットにおけるルーティングのセキュリティのために考案されました。リソースPKIに関連するプロトコルの策定が行われているIETFのSIDR（Secure Inter-Domain Routing）WGも、ルーティングのセキュリティ・フレームワークを作ることを目的としています※4。

しかし、リソースPKIの構築が進み始めた2007年には、別の目的についても議論されるようになりました。それが、リソースPKIを使った、アドレスリソースの利用権利の担保です。2007年7月、APNICのGeoff Huston氏により、レジストリのデータベースの正確性を保つために、IPv4アドレスの移転を認める提案が行われました※5。この頃より、リソースPKIは、移転されるようなIPアドレスの正確性を確認するための技術としても考えられ始めました。

リソース証明書が考案される以前は、IPアドレスの利用権利を表したり、保存したり、それが正しいのかどうかを電子的に検証したりできるようなデータ形式はありませんでした。IPアドレスがどこに割り振られているかという情報は、WHOISサーバにしかないため、WHOISサーバが攻撃されたり、トラフィックが不正に操作されたりすると、IPアドレスの正しさを調べられなくなってしまいます。一方、リソース証明書は電子証明書の形式であるため、記載されたIPアドレスが正しいかどうかを、WHOISサーバにアクセスせずに確認できます。

## リソースPKIの普及状況

執筆時の2010年1月時点において、いくつかのRIRではリソースPKIの整備が一旦完了しており、リソース証明書の提供が始まっています。一方、WHOISサーバに対するWHOISクライアントのように、リソースPKIを利用してリソース証明書を確認するようなプログラムは、まだほとんど普及していない状況です。

以下に、RIRの動向をまとめます。

- APNIC

2008年9月、APNICのIPアドレス申請業務を行うためのポータルサイト"My APNIC"で、リソース証明書の提供が実験的に始まりました。

APNICはRIRの中でもリソースPKI関連の開発において、先導的な立場を取っているRIRです。2006年頃、他のRIRに呼びかけて、RPKIエンジンと呼ばれる主要部分の開発を行い、2007年にはユーザーインタフェースやレジストリデータベースとの連携部分の開発を行ってきました。APNICのGeoff Huston氏は、設立当初よりIETF SIDR WGのチェアを務めてきました。

- RIPE NCC

2009年2月、RIPE NCCの申請業務を行うためのポータルサイト"LIR Portal"で、リソース証明書の提供が始まりました。

RIPE NCCでは2008年10月以前から"Certtest"と呼ばれる、誰でもリソース証明書を取得できるWebページを提供しており、実際に入手してもらったり、管理Webインタフェースを使ってもらうことで、リソース証明書に関する議論を活性化する活動を行ってきました。

この他に、RIPE NCCの事務局内でリソース証明書の発行業務が可能かどうかを検証する"CertPROTO"プロジェクトや、RIPE地域のLIRが参加し、RIPEにおけるリソース証明書のあり方を議論する"Certification Task Force"が編成され

る等しました。

RIPE地域ではポリシーの提案も行われています。

2008年8月には、PAアドレスのリソース証明書に関するポリシー"2008-08: Initial Certification Policy for Provider Aggregatable Address Space Holders"が提案されました。

- ARIN

ARINでは、2009年7月にパイロットプロジェクトという位置付けでリソース証明書の提供を開始しました※6。このパイロットプロジェクトのWebページは、RIPE NCCが行っていた"Certtest"のWebページと似ており、RIPE NCCと同様にリソース証明書を試験する目的で設置されています※7。

- LACNIC

LACNICは、IETF SIDR WGにWG設立当初より積極的に参加しており、2006年以降継続して検討が行われているようです。LACNICミーティングでプレゼンテーションが行われたり、説明ビデオが製作されたりしており※8、コミュニティにおける議論の活性化が図られている模様です。

- AfriNIC

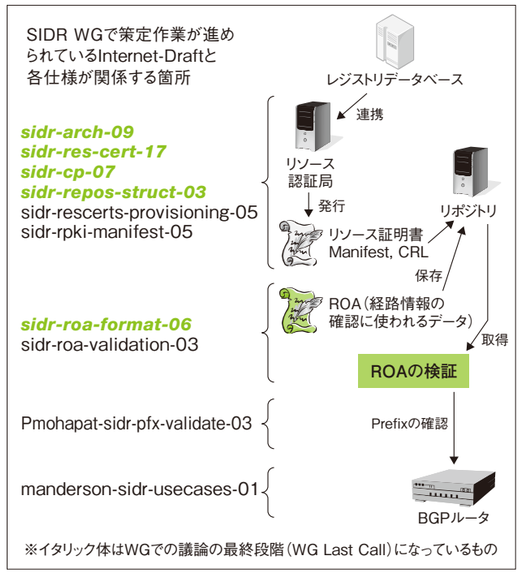
AfriNICでは、2006年頃前述のStephen Kent氏によるワークショップが開かれたり、AfriNICミーティングにおいてRandy Bush氏のプレゼンテーションが行われる等しており、情報収集の段階であるようです。しかし、AfriNICのレジストリシステムは、RIPE NCCのレジストリシステムをカスタマイズしたものであり、RIPE NCCと同様のシステムでリソース証明書を提供することは容易であると想像できます。

- IETF

IETFでは、SIDR WGにおいてリソースPKIに関わるRFCの策定が行われています。2009年11月、広島で行われたIETF-76では、WGでの議論が収束し、最終的なコメントを募集する"WG Last Call"がかけられたドキュメントが増えてきました。ドキュメントの策定状況を図2にまとめます。

**図2：IETF SIDR WGにおけるドキュメント策定状況**

IETF SIDR WGでは、RFC化は行われていないものの、"WG Last Call"が呼びかけられて、仕様がほぼ固まったドキュメントが増えてきた。




※イタリック体はWGでの議論の最終段階（WG Last Call）になっているもの

## リソース証明書

リソース証明書の内容を図3に示します。

**図3：APNICから発行されているJPNICのリソース証明書**

```
Serial Number:  70092                                  ← シリアル番号
Signature Algorithm: sha256WithRSAEncryption           ← 署名アルゴリズム
Issuer:CN=APNIC Production-CVPQSgUkLy7p0XdNeVWGvnFX_0s ← 発行者
Validity                                               ← 有効期限
    Not Before:  Jan  8 17:46:11 2010 GMT              ← 開始
    Not After:  Sep 30 00:00:00 2010 GMT               ← 終了
Subject:CN=A91A7381                                    ← 発行先
X509v3 Basic Constraints: critical                     ← 認証局フラグ
    CA:TRUE
sbgp-autonomousSysNum: critical
    Autonomous System Numbers:                         ← AS番号
      2497-2528
      2554
          :
sbgp-ipAddrBlock:critical
    IPv4:                                              ← IPv4アドレス
      58.0.0.0/15
      58.3.0.0-58.5.255.255
          :
    IPv6                                               ← IPv6アドレス
      2001:240::/32
      2001:258::/32
          :
```

リソース証明書は、X.509形式［RFC5280］の電子証明書でバイナリデータです。以下のような特徴があります。

- 発行先の名称が記載されていない。
- IPアドレスやAS番号が記載されている。
- 認証局証明書として利用でき、リソース証明書の所有者は、記載されたIPアドレスの範囲内のIPアドレスが記載されたリソース証明書を発行できる。

リソース証明書には、WHOISに登録されているような連絡先情報等は記載されておらず、これだけでWHOISの代わりになるわけではありません。一方、記載されたIPアドレスがレジストリ経由で正しく割り振られたものであるかどうかは、リソース証明書を電子的に検証することで確認できるようになっています。

先に述べたルーティングセキュリティのためには、ROA（Route Origination Authorization）というデータが使われます。ROAには、経路情報として伝えられるOrigin AS番号とIPアドレスの情報が記載されています。リソース証明書を使って電子署名が行われているため、正しい経路情報であるのかどうかの確認に利用できます。ROAは、BGPのpeer（経路情報を交換するための接続）を行う前に、相手が使用しようとしているIPアドレスが正しいものであるかどうかを確認する手段としても考えられています※9。

## リソースPKIとインターネットレジストリの今後

IPアドレスの管理には五つの原則（一意性・登録・経路の集約・アドレスの節約・公平性）があります。これらの原則は、インターネットの接続性とIPアドレスの持続を重要視したものと言えます。一方、リソースPKIはアドレス資源が正しいものであるかどうかを重要視するものです。これを厳密に捉えると、"正しいIPアドレスを使わなければ、インターネットにつなげられない"という考え方にもなります。今後もIPアドレス管理の原則は変わらないとは思いますが、IPv6アドレスの普及に伴って、量よりも正しさ、そしてその確認手段が重要な意味を持つようになるかもしれません。

一方、インターネットレジストリは、IPアドレスのユーザーにとって、なるべく負担が少なくなる仕組みで、IPアドレスを提供すべき組織です。IPアドレスの正しさを担保するために、ユーザーの負担が大きくなることはできるだけ避けなければなりません。

今後もRIRとIETF等における技術動向を日本のコミュニティの皆さんと共有し、インターネットレジストリのあり方について、皆さんと一緒に考えていきたいと思います。

（JPNIC インターネット推進部/技術部 木村泰司）

※1 BGP Countermeasures（Secure-BGP）
http://www.ir.bbn.com/sbgp/IETF42.ppt

※2 Revealed: The Internet's Biggest Security Hole
http://www.wired.com/threatlevel/2008/08/revealed-the-in/

※3 YouTube Hijacking: A RIPE NCC RIS case study
http://www.ripe.net/news/study-youtube-hijacking.html

※4 Secure Inter-Domain Routing（sidr）
http://www.ietf.org/dyn/wg/charter/sidr-charter.html

※5 IPv4 address transfers
http://www.apnic.net/policy/proposals/prop-050

※6 ARIN RPKI
https://www.arin.net/resources/rpki.html

※7 ARIN Resource Certification
https://rpki-pilot.arin.net/

※8 LACNIC Resource Certification
http://www.youtube.com/watch?v=wzdM_wHMXV8

※9 Certification Update（RIPE NCC）
http://www.ripe.net/ripe/meetings/ripe-59/presentations/band-certification.pdf