RPKI システム開発　提案依頼書（Request For Proposal）

概要

2014 年 6 月 2 日

一般社団法人日本ネットワークインフォメーションセンター

1.　概要

1.1. 本提案依頼書の目的

一般社団法人日本ネットワークインフォメーションセンター（以下、JPNIC と呼ぶ）では、リソース PKI（RPKI）の試験的な提供を計画しております。本提案依頼書は、これに必要なシステムの要件を提示し、提案を依頼するものです。

1.2. IP アドレス管理

（IP アドレス管理の基礎知識：https://www.nic.ad.jp/ja/ip/admin-basic.html より）

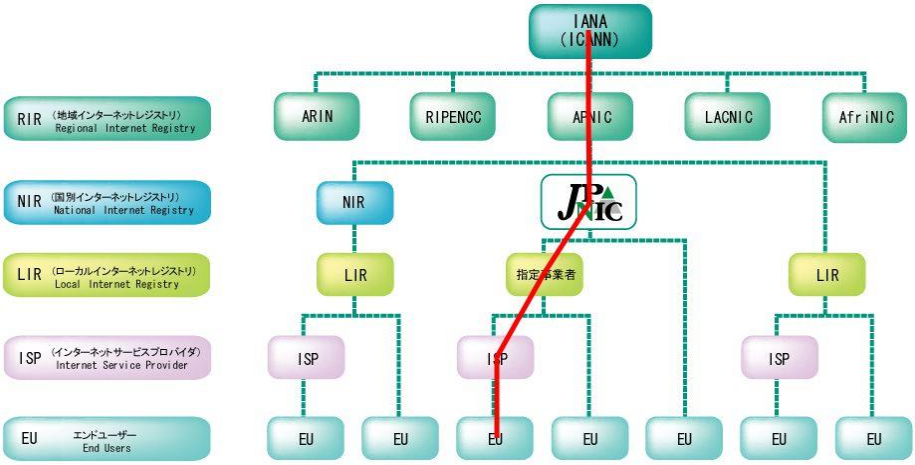
IP アドレスはインターネットユーザーが公平に共有する資源として、「アドレスポリシー」と呼ばれる管理方針に基づき世界的に管理が行われています。 アドレスポリシーとは IP アドレスの分配、 または利用にあたって従うことが求められる、IP アドレス管理の構造、 考え方、アドレス分配の基準等を定義したものであり、 RIR が管轄している地域単位で文書化し、公開しています。 JPNIC のように国別にアドレス管理を行う NIR が存在している場合は、NIR がポリシー文書を公開しているケースもあります。

JPNIC におけるアドレス空間管理ポリシー(IPv4) [1]
https://www.nic.ad.jp/doc/ip-addr-ipv4policy.html

JPNIC における IPv6 アドレス割り振りおよび割り当てポリシー
https://www.nic.ad.jp/doc/ip-addr-ipv6policy.html

[1] このポリシーに記載された「IP アドレス空間の移転」は、後述するリソース証明書の内容を変更し再発行する必要性につながる、特に関連する項目です。

IP アドレスの分配は「インターネットレジストリ」と呼ばれる組織により、 階層的な管理・分配が行われています。 JPNIC は、アジア太平洋地域におけるアドレス管理を行っている APNIC の管理下にある国別インターネットレジストリとして、 日本国内におけるアドレス管理を行っています。

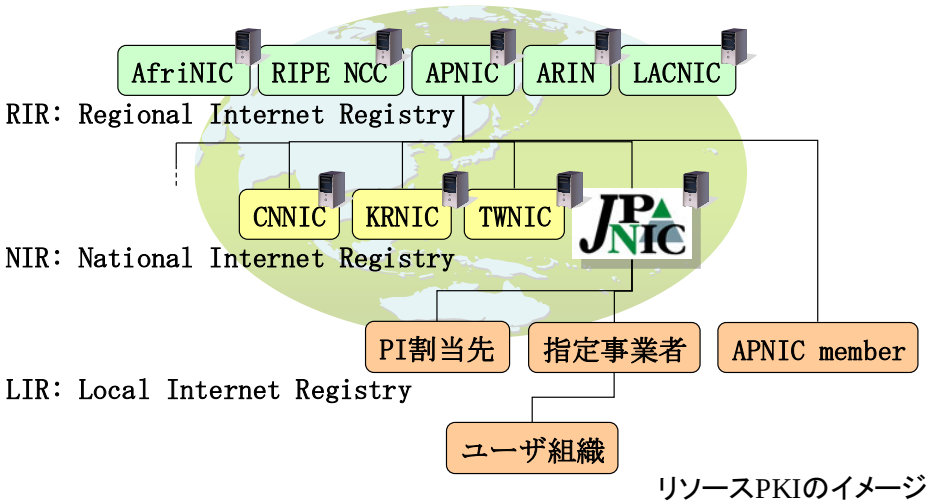


IP アドレスは、 原則として上で示した通りの流れで分配が行われていますが、 階層構造による管理が実装される以前は LIR (日本では IP アドレス管理指定事業者)を介さず、APNIC、 または JPNIC に該当するインターネットレジストリより直接ネットワークに分配が行われていた時代がありました。このような方式で分配された IP アドレスは 「歴史的経緯を持つ PI(Provider Independent)アドレス」 と呼ばれています。

1.3. リソース PKI

リソース PKI（以下、RPKI と呼ぶ）は、IP アドレスなどのアドレス資源の利用権利を示す電子証明書（以下、リソース証明書と呼ぶ）を発行する仕組みです。リソース証明書には IP アドレスや AS 番号が記載されており、正しく割り振られたアドレスであることを示しています。リソース証明書はインターネットにおける経路広告を始めるときに、その IP アドレスが登録と異なる不正なものではないことを示したり、ISP（インターネットサービスプロバイダー）などにおけるルーターで受信されたインターネットの経路情報が、本来の正しいものであることを確認したりするために使うことができます。

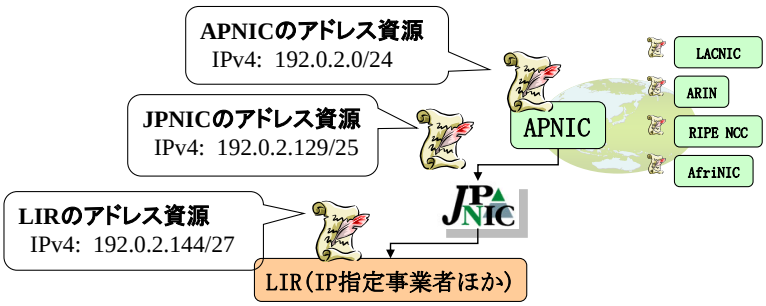
リソース PKI における認証局は、IP アドレスなどのアドレス資源の割り振り／割り当て構造に沿って構築されます。



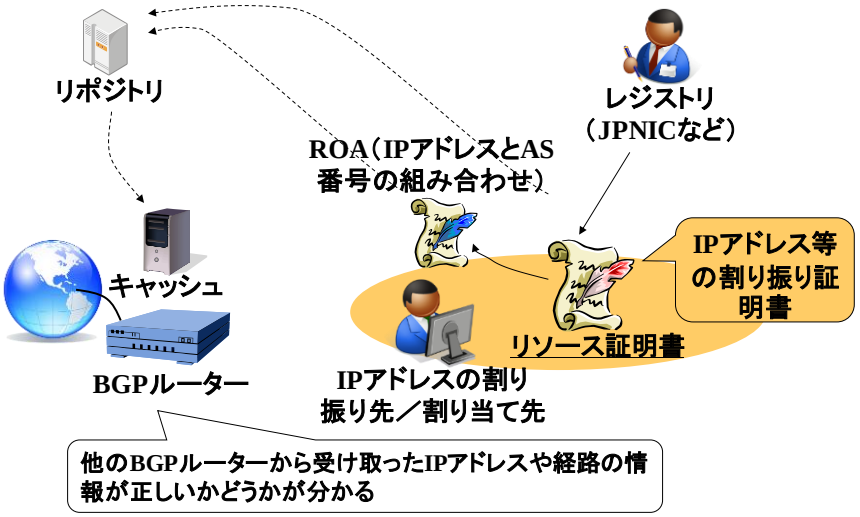
リソースPKIのイメージ

リソース証明書は、RFC3779 で示される X.509v3 拡張フィールドでアドレス資源が記載されます。

リソース証明書のイメージ



リソース証明書の発行を受けた IP アドレスの割り振り／割り当て先組織（LIR）は、IP アドレスと AS 番号が記載された Route Origin Authorization（ROA）と呼ばれる電子署名付きのデータを発行することができます。リソース証明書と発行された ROA は、リポジトリと呼ばれるサーバに蓄積されます。

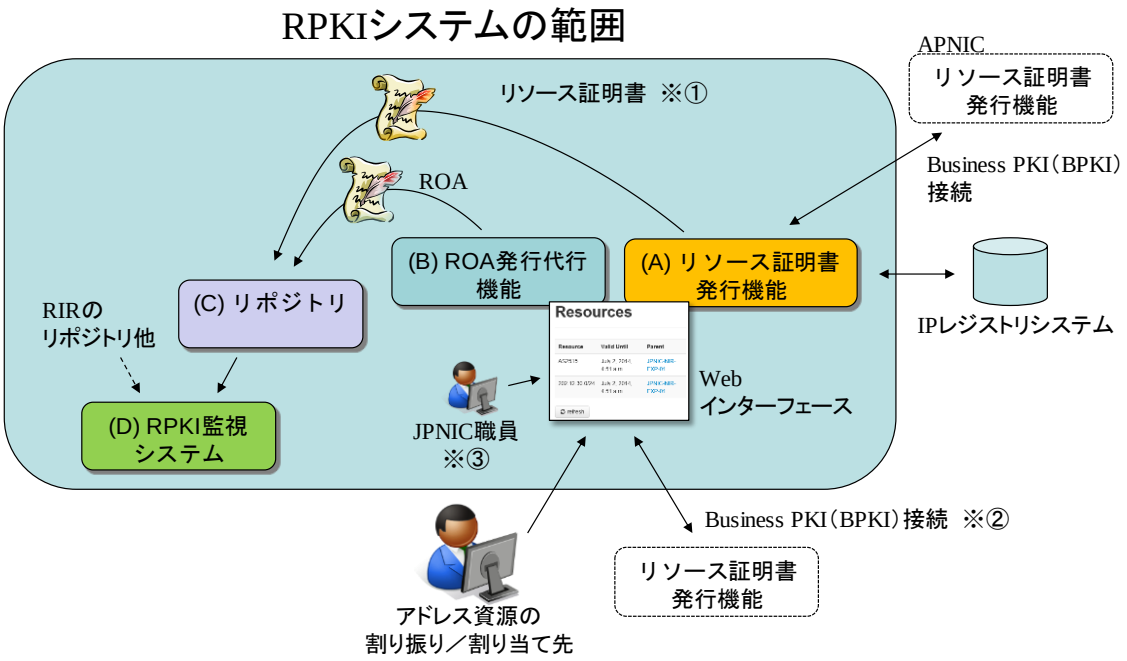


リポジトリに蓄積されて公開されているリソース証明書と ROA 他署名付きデータ（CRL、Manifest、Ghostbusters）は、国際的に分布している「キャッシュ」サーバによってダウンロードされ、署名検証が行われます。署名検証の結果は BGP ルーターに伝えられ、不正な経路情報を検知するといった使われ方をします。

2. RPKI システムの要件

2.1. RPKI システムの範囲と機能

RPKI システムは、JPNIC において、前節で述べたリソース証明書と ROA を実現します。RPKI システムの範囲と必要な機能を以下に示します。



(A) リソース証明書発行機能

APNIC のリソース証明書発行機能と接続し、JPNIC および JPNIC の管理下のリソース証明書の発行を行います。

- **認証連携**
  アドレス資源の割り振り／割り当て先を JPNIC が発行しているクライアント証明書（資源管理者証明書および資源申請者証明書）を使ってユーザ認証します。

- **データ連携**
  クライアント証明書に記載されている情報（ID）を元に JPNIC の IP レジストリシステムと連携し、アドレス資源の情報とリソース証明書の情報が一致するように連携します。

以下の 3 種類の Web インターフェースを提供します。

① アドレス資源の割り振り／割り当て先向け操作インターフェース
アドレス資源の割り振り／割り当て先が、「リソース証明書発行機能」に任せて Web インターフェースを操作し、後述する ROA 発行代行機能を使用する。「リソース証明書発行機能」では、アドレス資源の割り振り／割り当て先の鍵データを格納し運用する必要がある。

② アドレス資源の割り振り／割り当て先向け接続設定インターフェース
アドレス資源の割り振り／割り当て先が、RPKI としての接続設定（Business PKI – BPKI と呼ぶ）を行うためのインターフェース。リソース証明書（下位認証局証明書）の鍵データは、アドレス資源の割り振り／割り当て先の設備にある。

③ JPNIC 職員向け管理インターフェース提供
JPNIC 職員がこの Web インターフェースを使って、アドレス資源の割り振り／割り当て先のリソース証明書の管理業務を行う。

■注意事項
アドレス資源の移転（国際移転を含む）への対応が必要です。移転の手順に合わせて、JPNIC とアドレス資源の割り振り／割り当て先が証明書発行／失効を行います。

(B) ROA 発行代行機能

ROA は、本来アドレス資源の割り振り／割り当て先が、自身の鍵を使って発行

するものですが、これをJPNICが代行するための機能です。
「リソース証明書発行機能」において格納されている鍵を使うことで、アドレス資源の割り振り／割り当て先は、Web インターフェースを操作するだけでROAの発行ができます。

(C) リポジトリ

JPNICのリソース証明書、「リソース証明書発行機能」および「ROA発行代行機能」によって発行されたリソース証明書と、ROAほか署名付きデータ（CRL、Manifest、Ghostbustersなど）を格納し、公開します。リポジトリは不特定多数のユーザによってアクセスされます。

(D) RPKI監視システム

リポジトリで公開されている署名付きデータの電子署名が有効であるのか、リソース証明書の内容に間違いがないのかを確認します。そのため、必要があればリソース証明書発行機能もしくはIPレジストリシステムと連携します。
JPNICのリソース証明書を監視するため、必要があればJPNICのRPKIシステムのみならずRIRのリポジトリにもアクセスします。

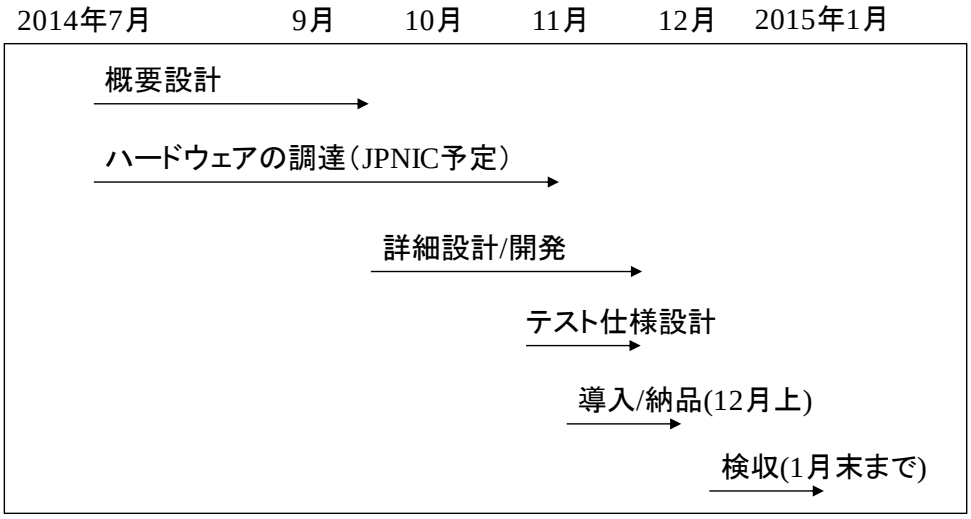
ご提案の範囲は、RPKIシステム全体です。IPレジストリシステム、JPNIC資源管理認証局、およびAPNICのリソース証明書発行機能、キャッシュやルーターは含まれません。

3. 提案手続きについて

JPNIC の公募に応募した業者から選定し、契約締結がおこなれ、開発が行われる予定です。提案依頼書は問い合わせのあった業者に、NDA を締結ののちにお送りします。その後希望する業者には個別の説明を二回まで行います。

3.1. 構築スケジュール

本開発の構築スケジュールを以下に示します。



3.1.1. 提案依頼スケジュール

2014 年 6 月 3 日（火）～6 月 19 日（木）　個別説明期間
2014 年 6 月 24 日（火）　提案書提出期限
2014 年 7 月 14 日（月）　業者選定結果内示
以降、契約締結までに打ち合わせをお願いすることがあります。

3.2. 参加資格条件

同規模のシステム開発経験を持ち、電子認証およびネットワークに通じたシステム開発に関する実績を持つベンダが望まれます。

以上