RPKIシステムの試験的な提供について ～利用開始と使い方～

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
木村泰司　岡田雅之

内容

- お知らせとご利用方法（ポイント）
- RPKIとOrigin Validation
- JPNICのRPKIシステム ～試験提供とは～
- RPKIシステムの使い方
- ROAキャッシュサーバの設置方法
- RPKIの技術課題

お知らせ

- **JPNICにおけるRPKI機能として、「ROA Web」「BPKI接続設定」の試験提供を開始しました。**
  - APNICとのBPKI接続は近日予定 (訳は後ほど)

http://rpki.nic.ad.jp/

ご利用方法（発行側）

a. 技術的な動作の検証をしたい
   ⇒ RPKI模擬環境　もしくは
   　ROAパブリックキャッシュサーバ

b. 国内で検証可能なROAを利用したい
   ⇒「ROA Web」

c. きちんとRPKIの分散運用を…
   ⇒「BPKI接続」

ご利用方法（検証側）

- **Origin Validationを行うには**
  - ROAキャッシュサーバに**JPNICのTALファイル**をダウンロードして指定／対応ルータを設定
    https://serv.nic.ad.jp/capub/rpki/jpnic-preliminary-ca-s1.tal (JPNICのTAL)
  - 対応ルータで**ROAパブリックキャッシュ**を指定
    https://www.nic.ad.jp/ja/rpki/howto-usepubcache.html (設定例)

お問い合わせ先

JPNIC RPKI担当　rpki-query@nic.ad.jp

RPKIとOrigin Validation

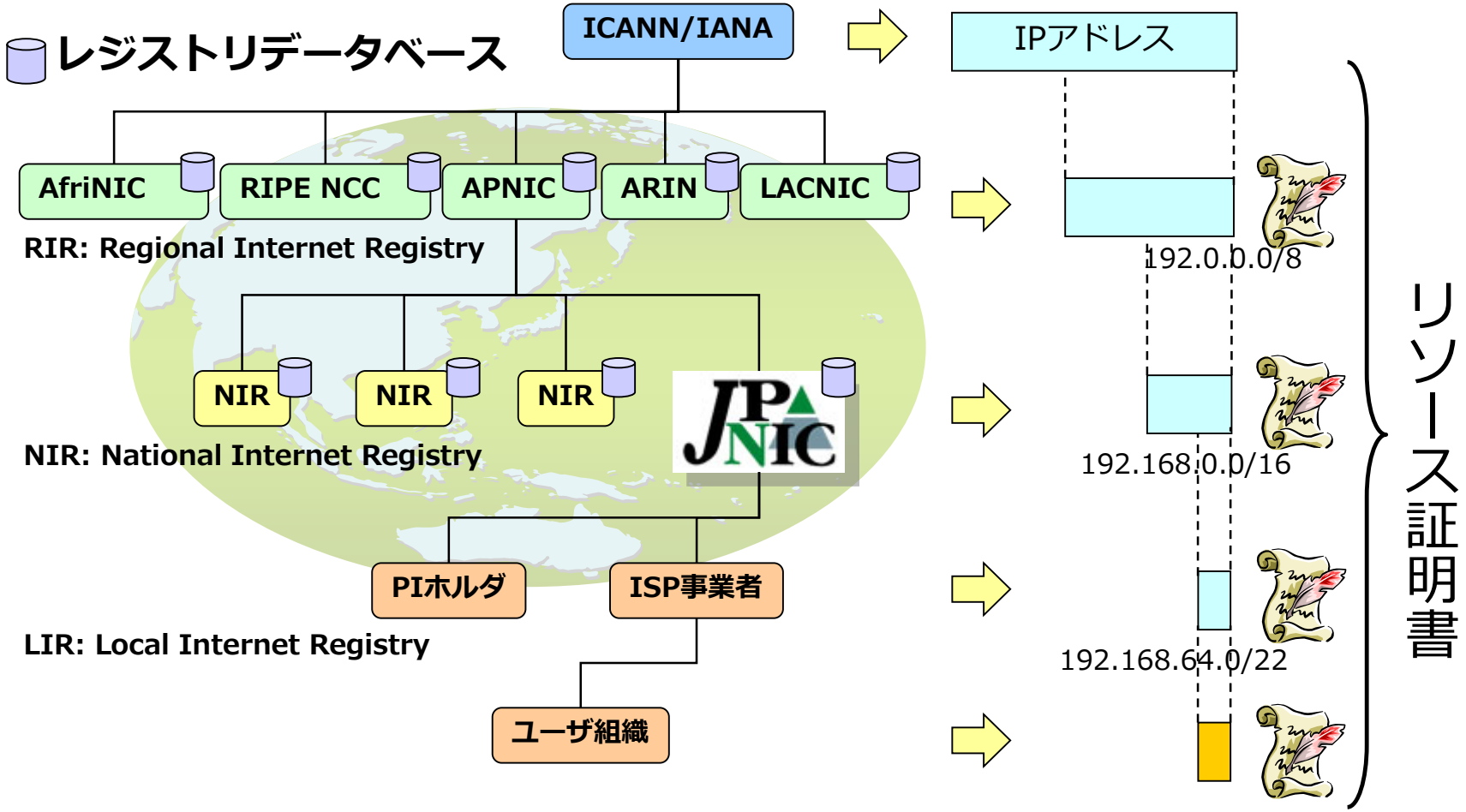
RPKI

- **Resource Public-Key Infrastructure**
  - IPアドレスやAS番号といった番号資源（Number Resource）の割り振り／割り当てを証明するPKI
  - 1997年頃、Stephen Kent氏 (BBN Technologies) によって提案され、現在は IETF (Internet Engineering Task Force) の SIDR WGで仕様策定が行われている。

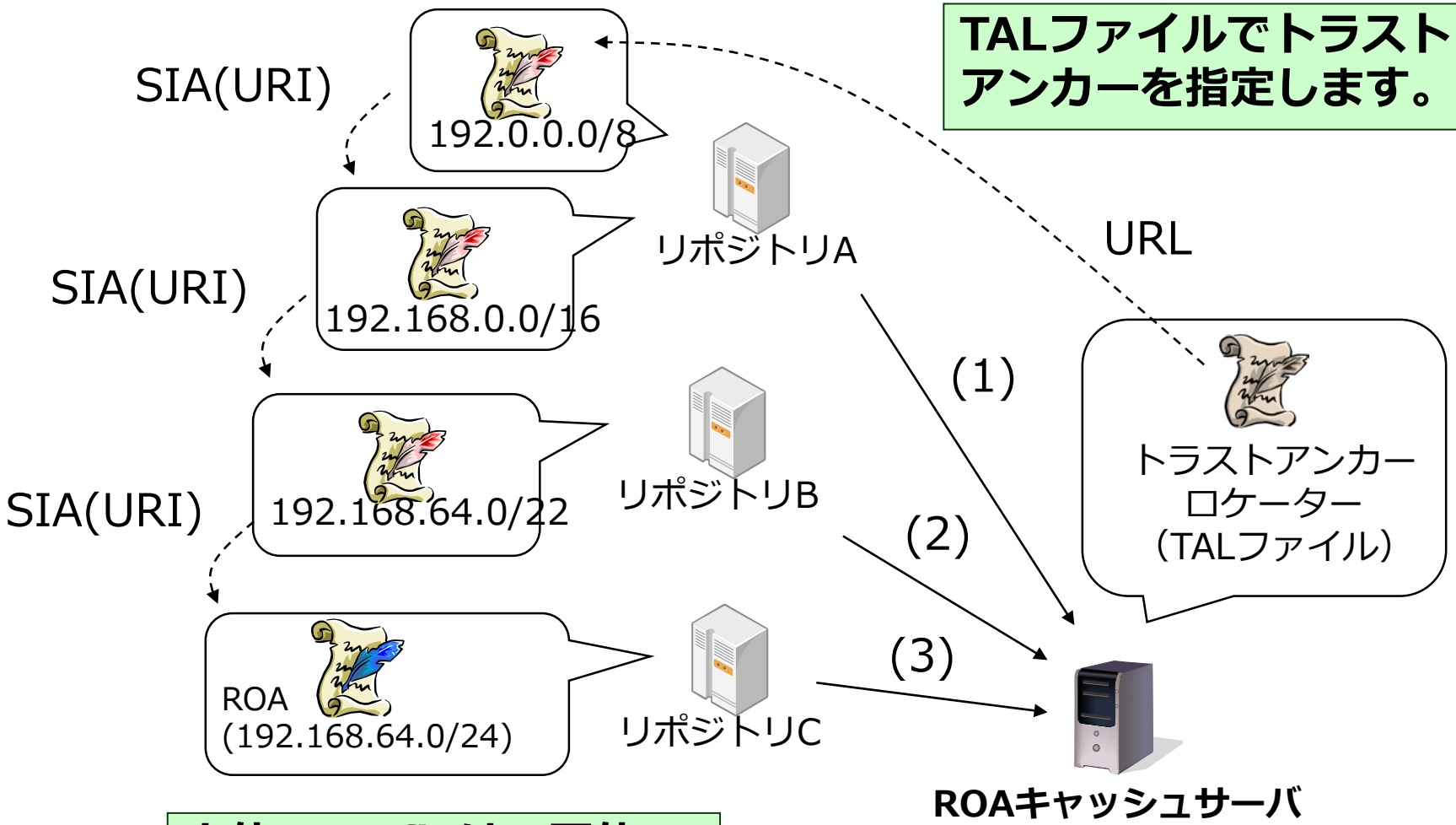
IPアドレスの割り振り／割り当てを証明する「リソース証明書」のためのPKIです。

最近のSIDR WGではPath Validationの実装とRSYNCに代わる差分転送プロトコルの話題

リソース証明書



トラストアンカーと署名検証



TALファイル – trust anchor locator

TALファイルの例

rsync://rpki-repository.nic.ad.jp/ta/jpnic-preliminary-ca-s1.cer

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnjfovjOzuZP5zOT5iHtB
3z35k9uarx3ltKHrh4eq1xO4f7i0Dt/VEsqLJxuBfuRPUwskaH/96ewzqeeL9iPv
vGHL479kJ6YrhN7StkNXLVePxw4uHe7DWuw0CSsRCLEu+SssWTiXyEp3olkgutUV
mwZrNZ1aCfi8tvibz44v1iYvOYcTXRXgvwneJbxepqt+2xchHwMrjBIWsexdqVK7
1/iMHXChEr6wCzZyFW2rJjeFEAF6nFnu1DDhb1bSVe+PEd4PmrQ5vNeYkcffC3dL
Y8ZrjCU51LFD441EA8ae0gDRBnnD7+O3J0rjUi+Y34xLu5XSw8nDordErnX31sqV
XwIDAQAB

署名検証するためには、入手済みのTALファイルを読み込んでトラストアンカーの証明書をダウンロードします。

ROA – Route Origination Authorization

ROAの内容例

```
$ cd /var/rcynic/data/authenticated/rpki-repository.nic.ad.jp/
$ print_roa 1003/6gaLktvYFfRfkbwTJnYU-STtxYI.roa
ROA Version:    0
SigningTime:    2015-03-20T11:12:21Z
asID:           2515
 addressFamily: 1
    IPAddress: 192.41.192.0/24

$ print_roa publication/1003/HKEK_75JQYmCWP26zFDz2IcXSIg.roa
ROA Version:    0
SigningTime:    2015-03-20T11:12:21Z
asID:           2515
 addressFamily: 1
    IPAddress: 202.11.240.0/21
$
```

ROAには署名日時とAS番号、IPアドレスの範囲が記載されています。

Origin Validationの仕組み

- **ROAキャッシュサーバ**
  - リソース証明書の署名検証を通じて、IPアドレスが正式に割り当てられたものであることを確認
  - ROAの署名検証を通じて、経路広告元のAS番号が正式なIPアドレスの割り当て先によって指定されたものであることを確認
- **BGPルータ**
  - BGP Updateメッセージとして伝播してきたIPアドレスprefixと経路広告元のAS番号を確認

BGPルータにおいて、IPアドレスの割り当て先組織の意図と異なる経路情報を検出できます。

JPNICのRPKIシステム

～試験提供とは～

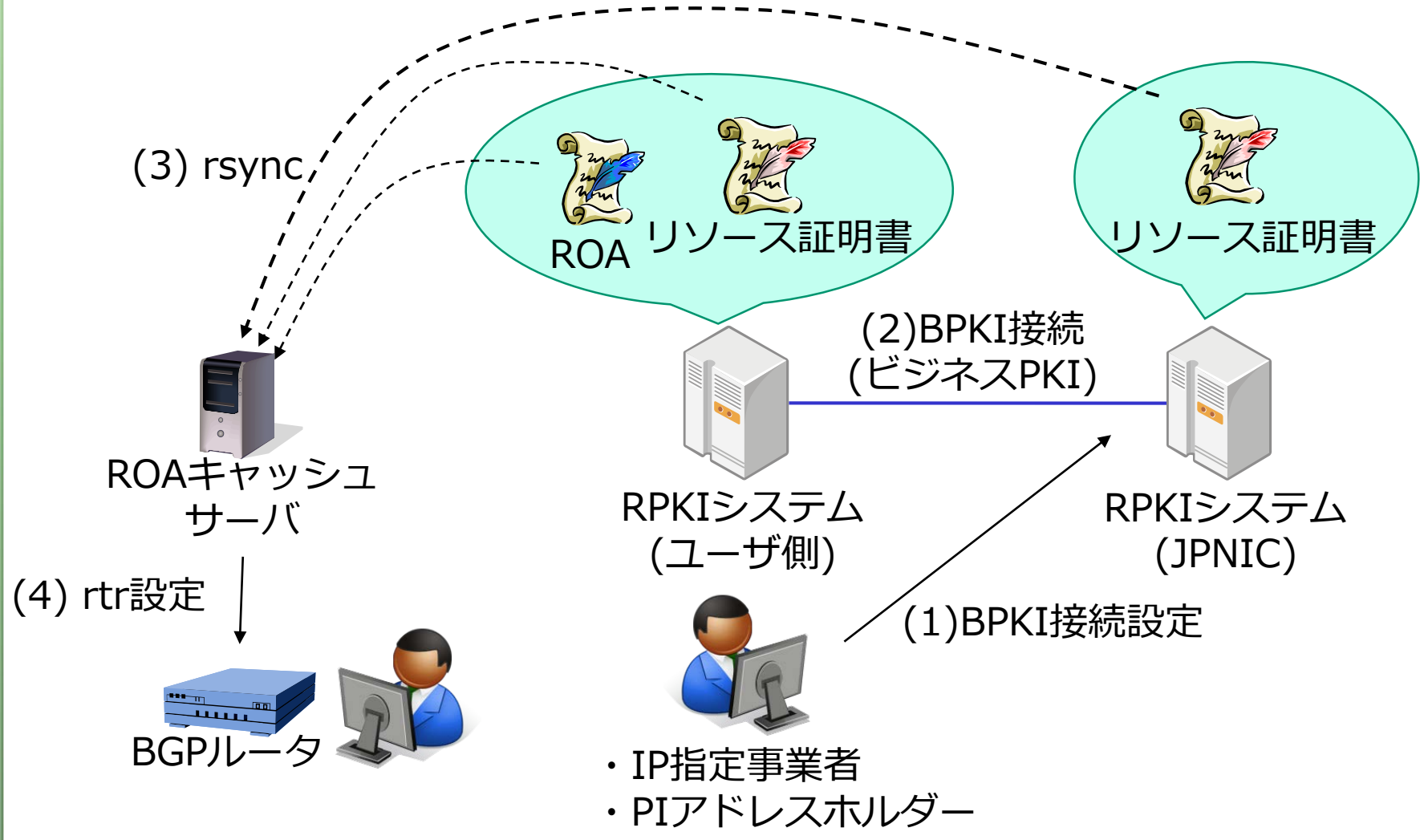
一般社団法人 日本ネットワークインフォメーションセンター

JPNICのRPKIシステムの試験提供

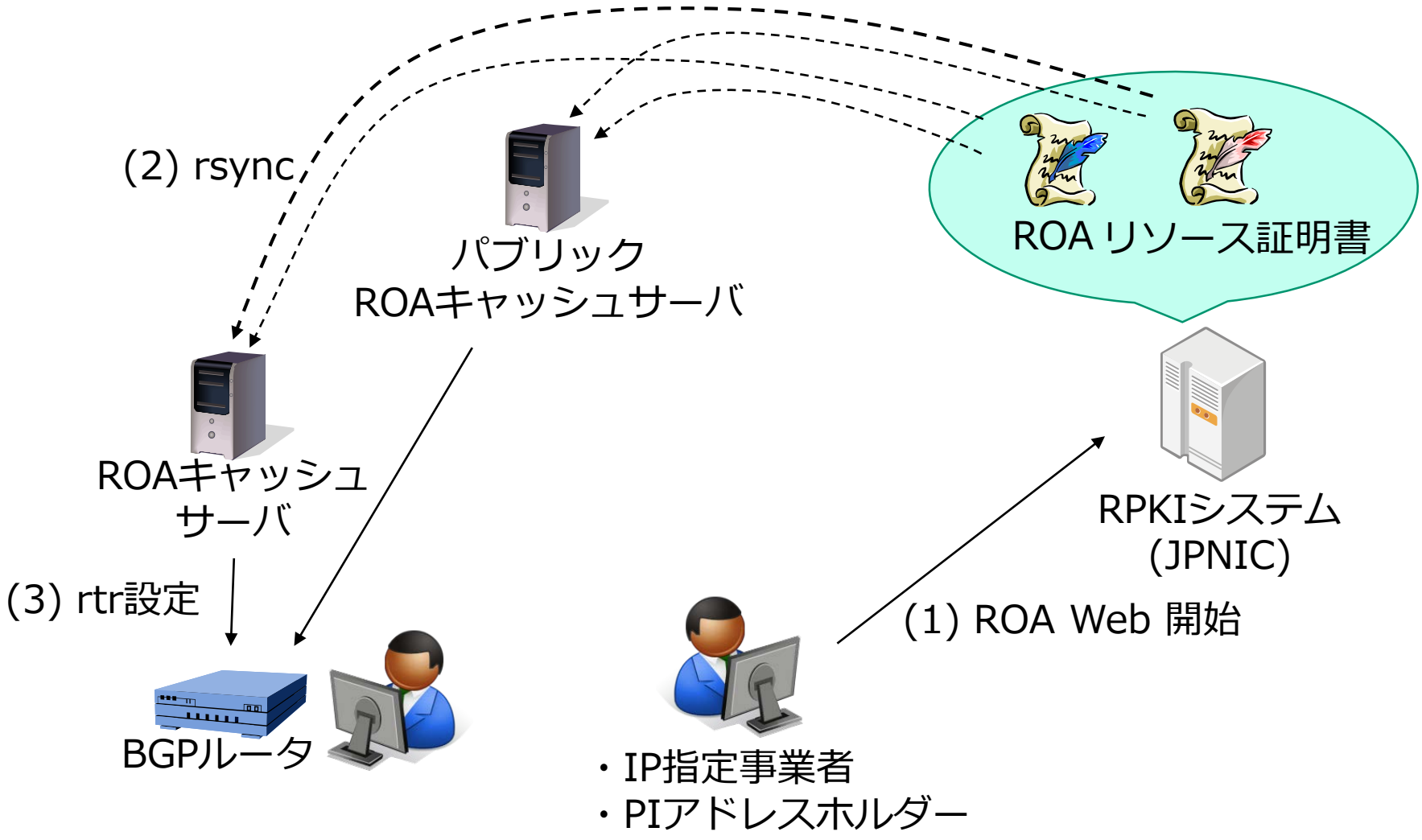
- **分配済みIPアドレスが入ったリソース証明書**
  - RPKIシステムはWHOISデータベースと連携しています。
- **資源申請者証明書を使ってログイン**
  - 「Web申請システム」と認証連携をしています。
- **日本語化対応**
  - 模擬環境では英語でしたが日本語メッセージにしています。（多国語言語対応）

日本国内で実際のIPアドレスを使ってOrigin Validationのできる状況にすべく開発し提供開始

ROAご利用までの流れ（BPKI接続）

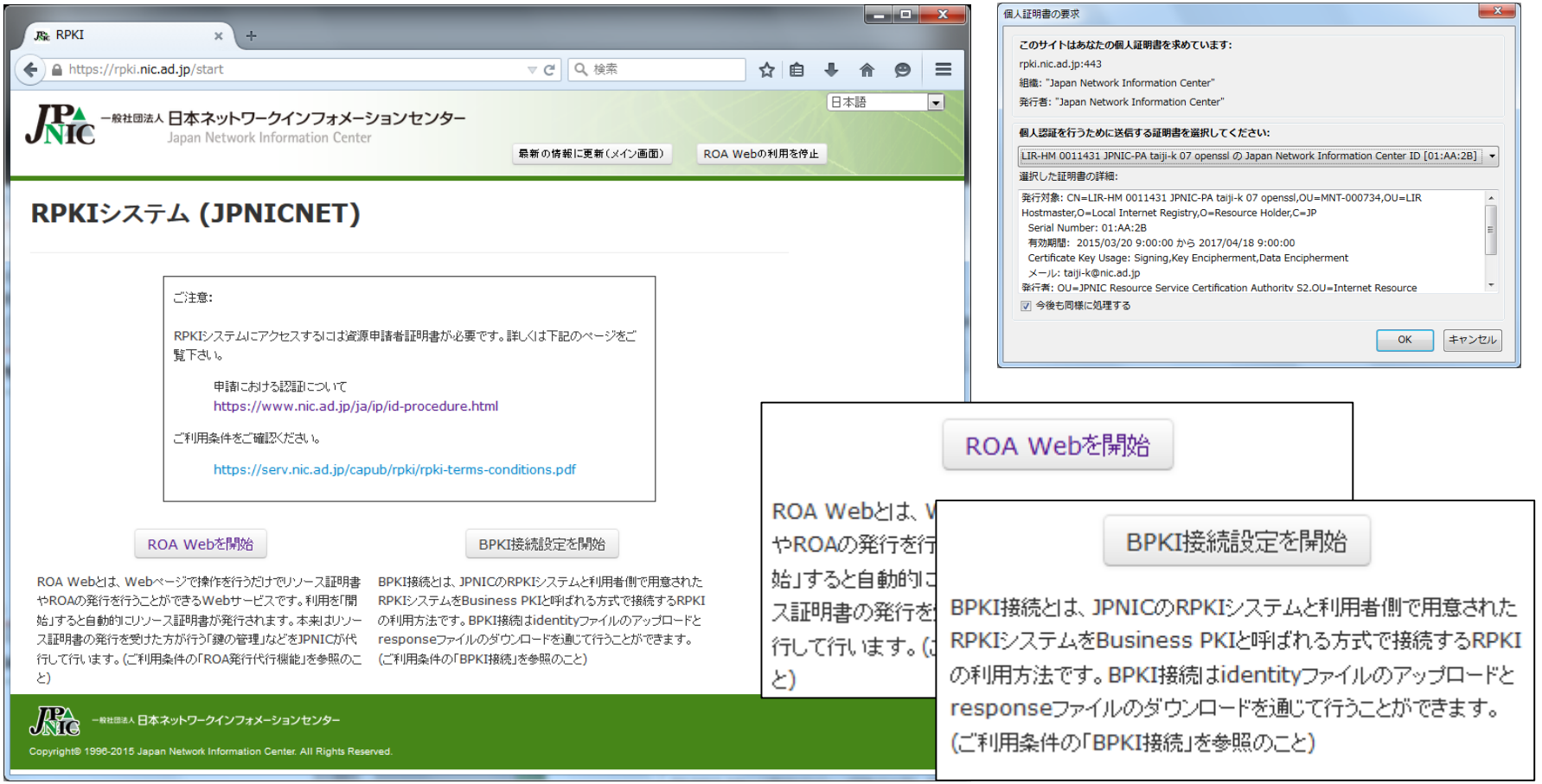


ROAご利用までの流れ（ROA Web）



RPKIシステムの使い方

利用開始画面



資源申請者証明書を使ってユーザ認証します。
「ROA Web」と「BPKI接続設定」を選べます。

BPKI(ビジネスPKI)接続設定

XMLファイルをアップロードすると
リソース証明書の発行を開始します。

ROA Web (ROA発行代行機能)

Webの操作のみでROAの作成ができます。

ROA Webを使ったROA作成

AS番号を指定してROAを作成します。

ROA WebのROA管理画面

発行されたROAとリソース証明書はrsyncを使ってリポジトリからダウンロードできるようになります。

ROA Webの使い方詳細

- **二つのOrigin ASを並行運用したい**

  ⇒ 再利用ボタンを使うとOrigin ASの異なる二つのROAを追加できます。

- **一部のアドレスを除いてROAを一括作成したい**

  ⇒ 一部のアドレスのROAを仮に作成してから、残りのアドレスのROAを一括作成。一部を削除します。

- **表を項目ごとにソートをしたい**

  ⇒ 項目の行をクリックするとその項目でソートされます。

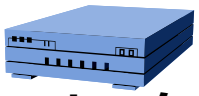
- **ROAの発行一覧をバックアップしたい**

  ⇒ 「エクスポート」でCSV形式でダウンロードできます。リストアは「インポート」です。

- **AS0を指定したい。(経路広告されないアドレス)**

  ⇒ Origin ASに0を指定します。

タイムスケール



BGPルーター

ROA
キャッシュ

RPKIシステム

経路情報の
チェック

署名検証

ROA作成
（数分程度）

割り振り／
返却手続き

数分　　数分～一日　　一日

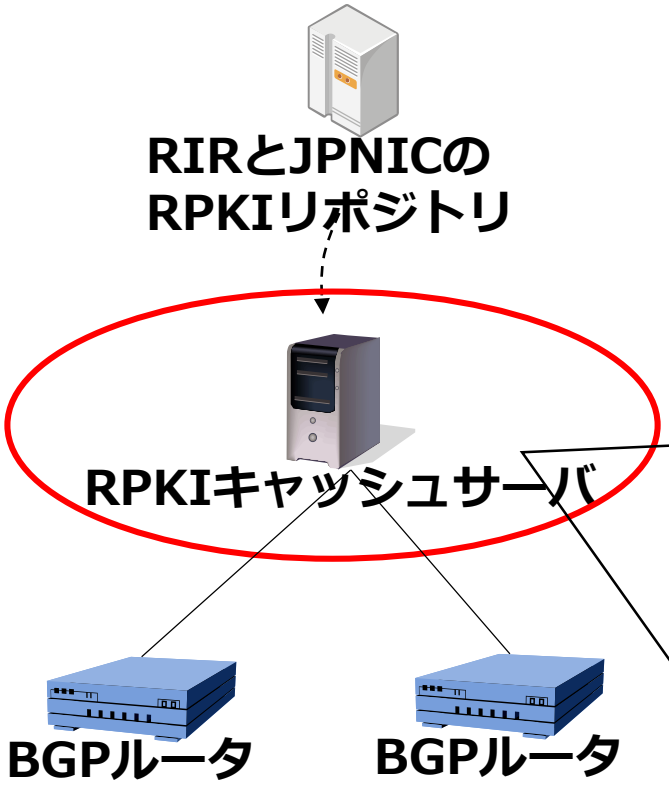
（ROAキャッシュの設定次第）

アドレスの種別とRPKI

- **APNICから割り振られたIPアドレス**
  - MyAPNICの「Resource certification」メニューからアクセス
- **JPNICから割り振られたIPアドレス**
  - RPKIシステムの「ROA Web」もしくは「BPKI接続設定」

ROAキャッシュサーバの設置方法

ROAキャッシュサーバの導入方法



RPKI Toolsインストール例 (Ubuntu)

$ wget -q -O -
http://download.rpki.net/APT/apt-gpg-key.asc | sudo apt-key add –
$ sudo wget -q -O
/etc/apt/sources.list.d/rpki.list
http://download.rpki.net/APT/rpki.precise.list
$ sudo apt-get update
$ sudo apt-get install rpki-rp
$ vi /usr/local/etc/rpki.conf

(詳細 http://rpki.net/)

ROAとリソース証明書の検証を行うことができる。

ROAキャッシュサーバを使う設定例

[Cisco IOS設定例]

```
router bgp <AS number>
bgp rpki server tcp <RPKI cache server>
port 42420 refresh 60
```

[JunOS設定例]

```
routing-options {
    validation {
        group rpki {
            session <RPKI cache server> {
                refresh-time 60;
                port 42420;
                }
```

RPKIキャッシュサーバのIPアドレスとリフレッシュタイムなどを設定する

RPKIを使ったOrigin Validation

BGPルータ

[Cisco IOS example]
>show ip bgp 10.0.1.0/24
BGP routing table entry for 10.0.15.0/24, version 64
:
192.168.0.15 from 192.168.0.253 (192.168.0.253)
Origin IGP, metric 0, localpref 100, valid, external, best
path 7F53CAD85C08 **RPKI State valid**
>

[JUNOS example]
> show route protocol bgp all
:
10.0.1.0/24 *[BGP/170] 17:11:58, MED 0, localpref 100, from 192.168.0.253
AS path: 65001 I, **validation-state: valid**
> to 192.168.0.1 via ge-1/0/0.0
>

経路情報のprefix毎の確認結果が表示されるようになる。

RPKIの技術課題

～これから導入を検討される皆様へ～

JPNIC 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

トラストアンカーから検証するPKI

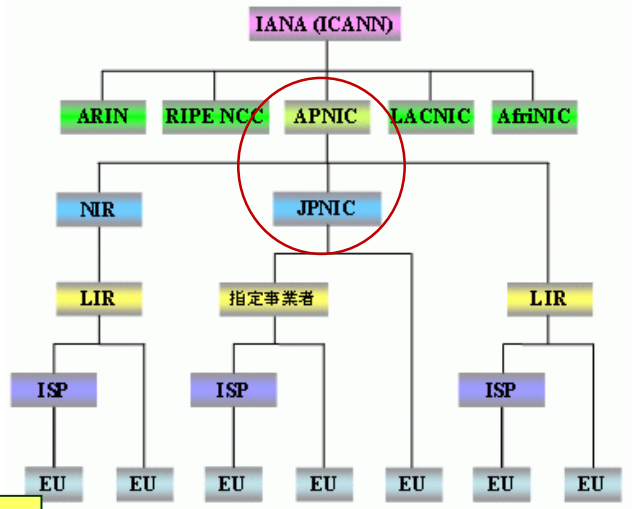
- **署名検証の結果としては「有効なIPアドレスとAS番号の組み合わせリスト」が得られる**
  - その中から特定の経路情報の有効性を確認するのはROAキャッシュサーバが担う

⇒ Origin Validationを行う上では、一つのROAの有効性ではなく、有効なROAの塊がトラブルシュートの対象になります。

一つのエラーが多数の検証結果に一度に現れてしまう仕組みです。BPKIが原因で検証に成功しないリソース証明書やROAができてしまうことがあります。

RPKIの信頼構造

- **5つのRIRがトラストアンカーロケーターを提供**
  - ひとつのCA証明書の有効性がNIR全域の有効性に影響する
    - NIRもトラストアンカーに指定できる (予備)
    - RP側に別の仕組みを設ける？
      draft-ietf-sidr-ltamgmt
      draft-dseomn-sidr-slurm
      draft-kent-sidr-suspenders
  - service agreement (ARIN)
  - LIRはWeb上の提供
    （鍵はRIR/NIRサーバ上）



予備＋HSMを使ったリスク回避策の後、
APNICとのBPKI接続を目指します。

ROAキャッシュサーバ

- **パブリックキャッシュサーバ**
  - ROAの検証結果を返すサーバ
  - 対応するBGPルータの設定を行うだけでROAとRPKIの検証結果が利用できる。
  - 今後も設置箇所が増えていく可能性あり。
- **RPKI RPのあるべき姿は？**
  - 署名検証は手元で行うべき？

    ⇒ 署名検証サーバを立ち上げないと利用できない仕組みになってしまう。
  - パブリックキャッシュサーバを併用？

    ⇒ 単一障害点を避けるために。

運用上の課題

- **自律分散への影響**
  - 単一障害点ができないようにするにはどうすればよいのか
    - レジストリのRPKI認証局
    - リポジトリ
    - ROAキャッシュサーバ
- **システムの信頼性**
  - 暗号アルゴリズムはRSA2,048/SHA-256のみ
  - TALやSIAではドメイン名で指定 → DNSに依存

BGPを使ったルーティングの自律分散という特徴を崩さずにセキュリティ技術を導入するにはどうすべきなのか

まとめ

- RPKIシステムの試験提供開始しました。
  - ROA Web　⇒　Web上でROAを作成できる。
  - BPKI接続設定　⇒　RPKIシステムを接続できる。

- Origin Validationできるようにするにはを作成しておきます。
  - ROAキャッシュサーバを使って検証できます。
    (有効なアドレスとASの組み合わせを取り出せる)
  - 対応するBGPルータでパブリックROAキャッシュサーバを指定する方法もあります。

- 引き続き技術課題があります。
  - 試験提供の段階でご利用頂くことで、RPKIを御社の到達性を守るのに役立つツールにしていきませんか！

おわり

JPNIC 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