

祝？APNICとRPKIで つながりました！ (WHOISの話題も少し…)

川端宏生(JPNIC)

今日のお知らせ

- APNICとRPKIつながりました
- WHOIS関連の動向

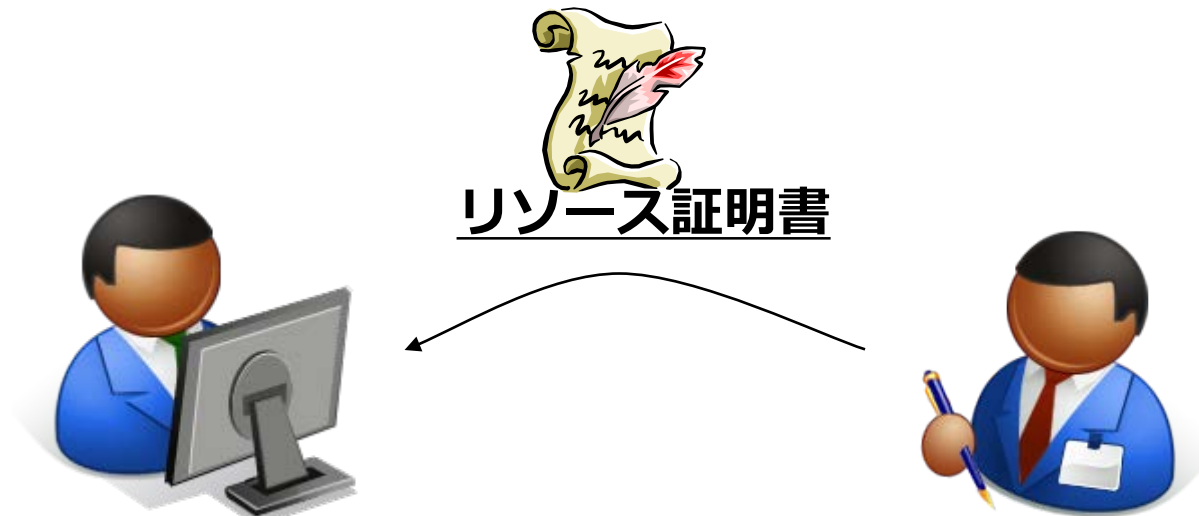
RPKI



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

Copyright © 2017 Japan Network Information Center

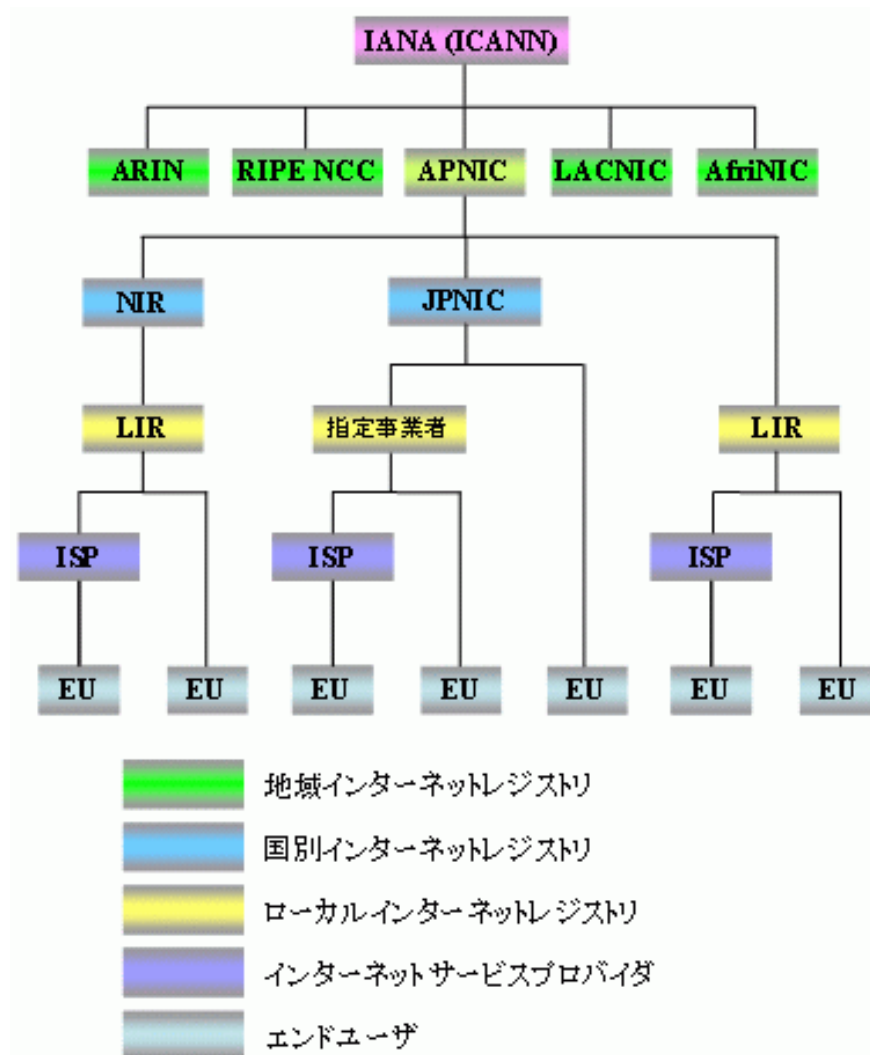
リソース証明書



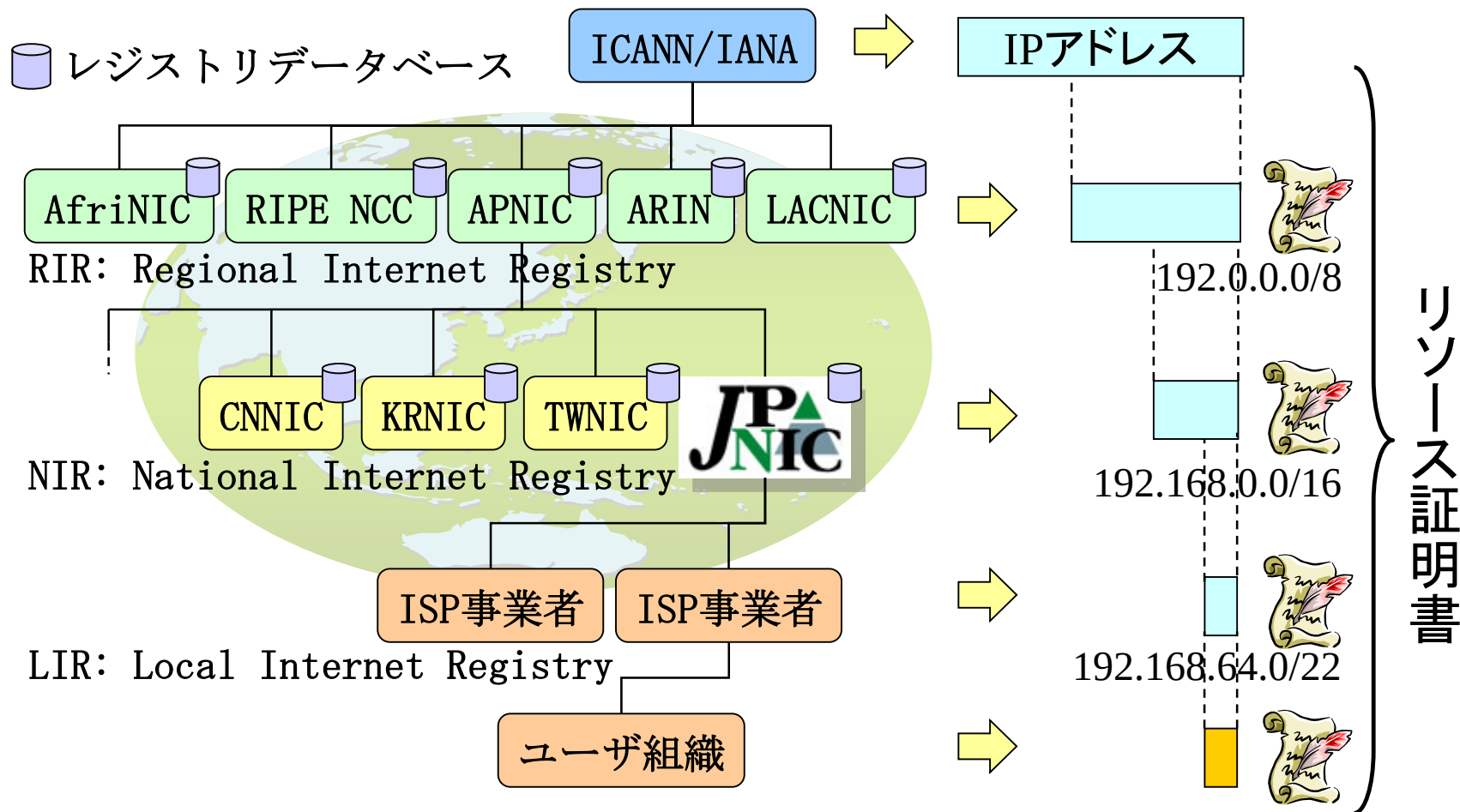
IPアドレスの割り振り先／割り当て先 レジストリ（JPNICなど）

リソース証明書 = IPアドレスやAS番号が書かれている電子証明書

IPアドレスの管理

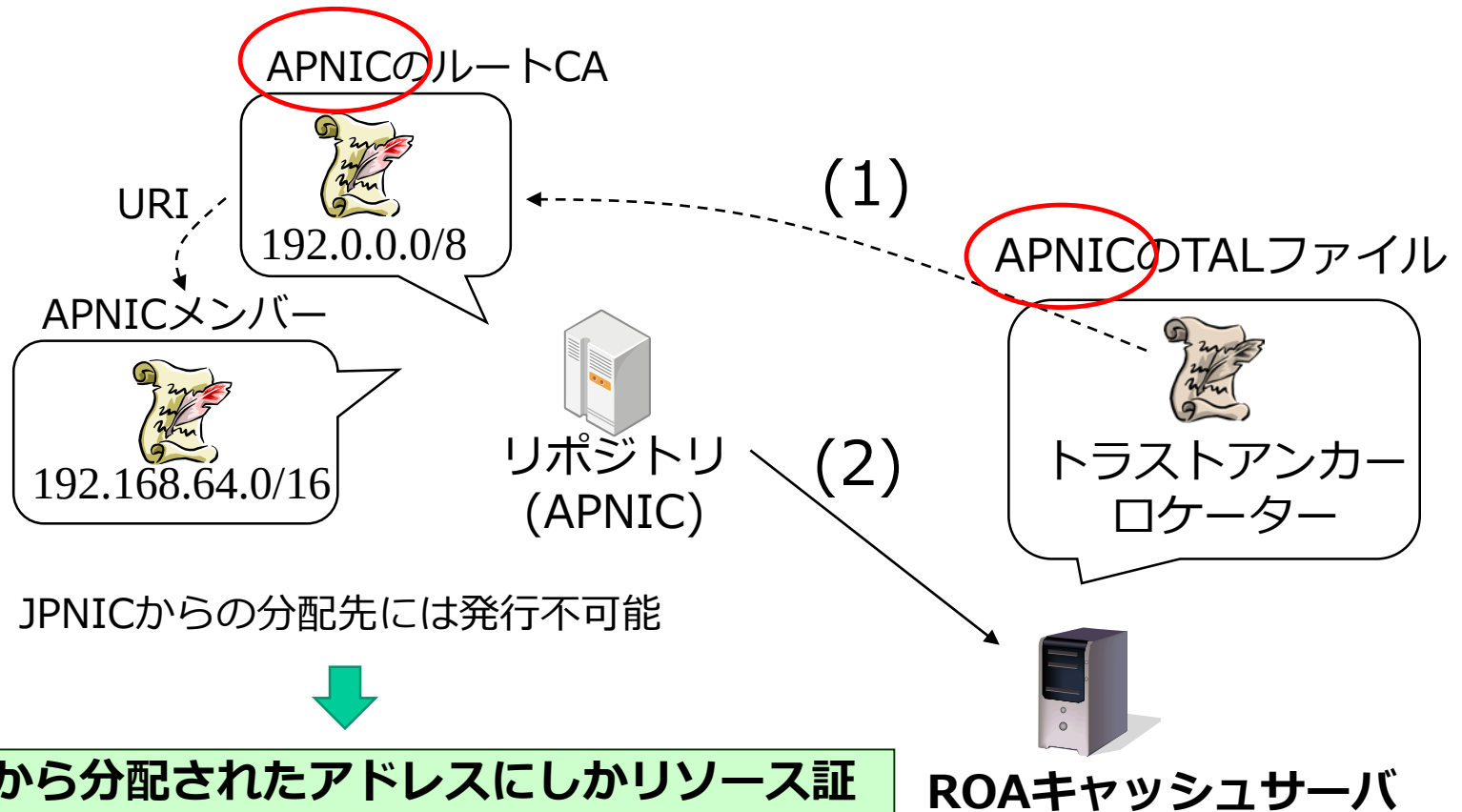


リソース証明書 + IPアドレスの管理



リソース証明書は、下に行くほど小さなprefixが記載される。

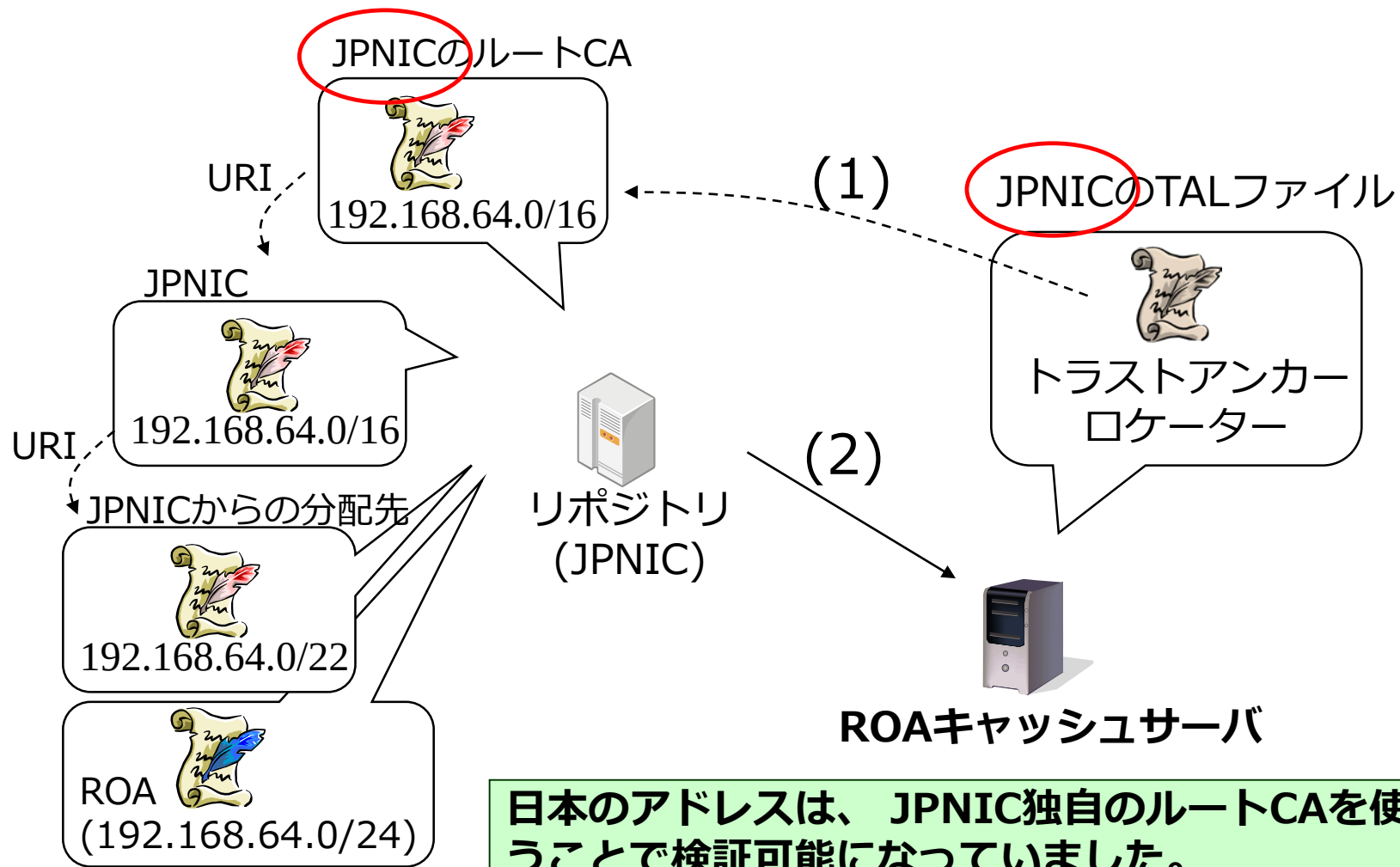
これまで(APNIC) - 世界から見ると



APNICから分配されたアドレスにしかリソース証明書が発行されていなかった。

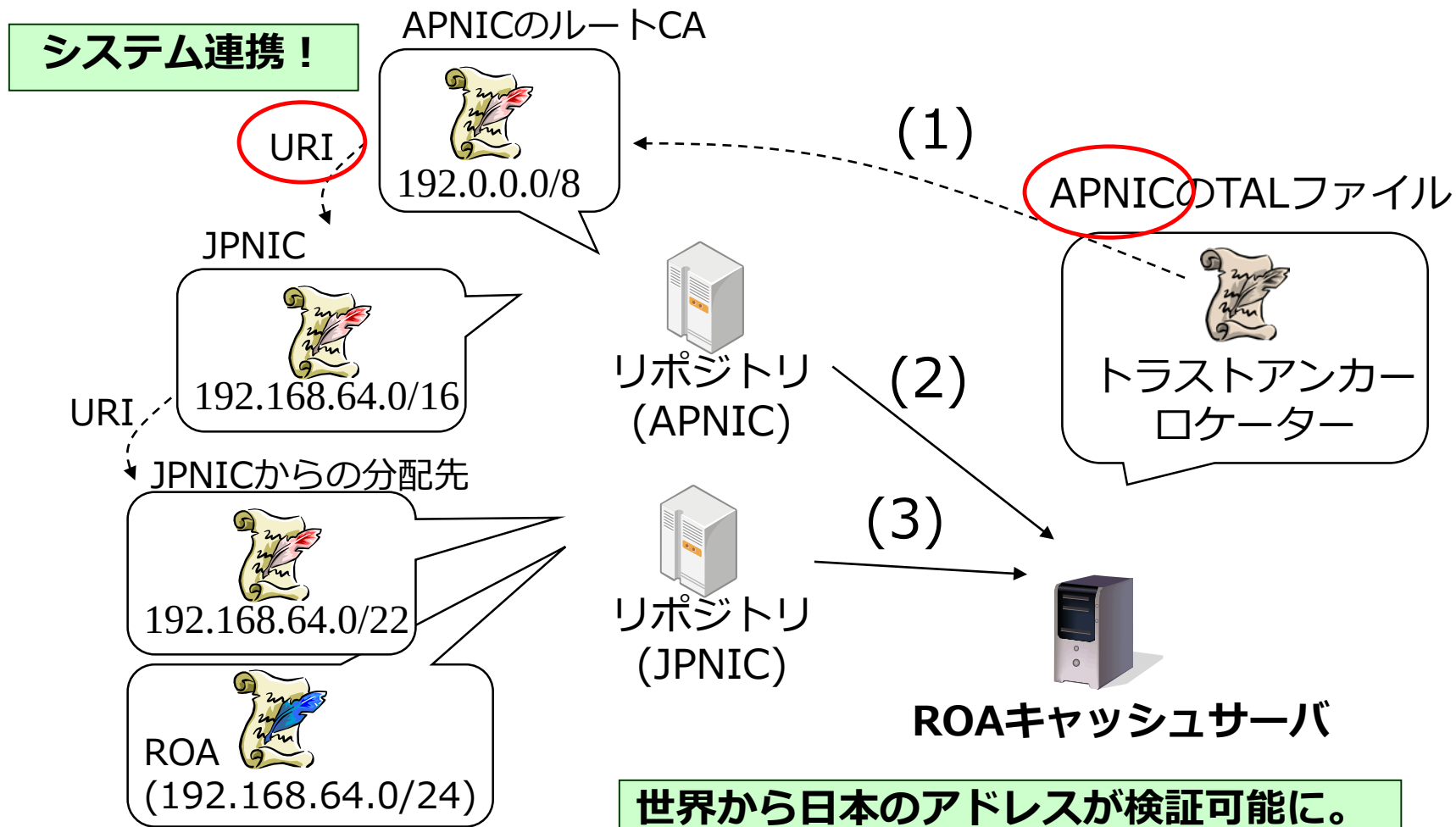
⇒ 世界からは日本のアドレスは検証できない。

これまで(JPNIC)



日本のアドレスは、JPNIC独自のルートCAを使うことで検証可能になっていました。

今回の連携により



世界から日本のアドレスが検証可能に。
BGPMONなどからも見えます！

祝！BGPMOMでもみえました

- 8/7の検索結果

```
$ whois -h whois.bgpmon.net " --roa 2515 202.12.30.0/24"  
[Querying whois.bgpmon.net]  
[whois.bgpmon.net]  
1 - Not Found
```

- 8/18の検索結果

```
$ whois -h whois.bgpmon.net " --roa 2515 202.12.30.0/24"  
[Querying whois.bgpmon.net]  
[whois.bgpmon.net]  
0 - Valid  
-----  
ROA Details  
-----  
Origin ASN:      AS2515  
Not valid Before: 2017-07-18 15:27:08  
Not valid After:  2018-07-17 08:58:07 Expires in 333d1h16m31s  
Trust Anchor:     rpki-repository.nic.ad.jp  
Prefixes:         202.12.30.0/24 (max length /32)
```

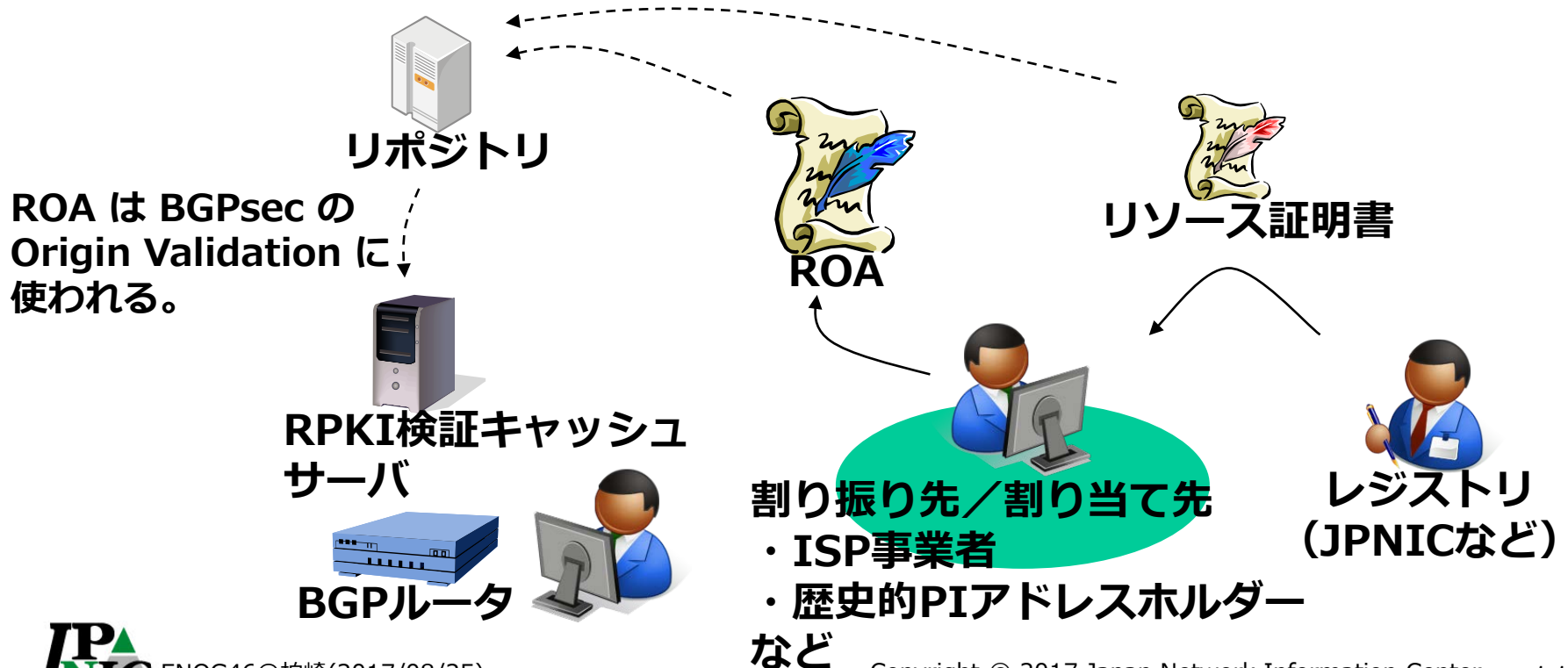
Tips

- **JPNICのTALは消さないで併用**
 - APNICから辿れなくなったときにもROAが検証できます
 - RPKIに起きている問題の原因究明に役立ちます

リソース証明書とROA

- **Route Origination Authorization**

- IPアドレスのホルダーによる署名付きデータで、割り当てられたIPアドレスの経路広告を特定のASから経路広告することを認可したことを示す。



参考情報

- **JPNIC Webページ**

- リソースPKI(RPKI)

- <https://www.nic.ad.jp/ja/rpki/>

- ROAの作成と管理の方法

- <https://www.nic.ad.jp/ja/rpki/howto-create-roa.html>

- **JPNIC技術セミナー**

- 【ハンズオン】 **無料** RPKI入門～BGPSECと最新動向、ROA管理まで～

- <https://www.nic.ad.jp/ja/tech/seminar/rpki-basic.html>

WHOIS



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

Copyright © 2017 Japan Network Information Center

WHOISからRDAPへ

- **Registration Data Access Protocol**
 - RFC7480-7485(2015年)
- **特徴**
 - HTTP(s)
 - RESTful
 - `http://[rdap-server]/ip/192.0.2.0/24`
 - `http://[rdap-server]/autnum/64496`
 - `http://[rdap-server]/domain/domain.example`
 - JSON
 - bootstrap

RDAP(Cont.)

- **機械可読**

- 例 : <https://rdap.apnic.net/ip/202.12.30.0/24>
の応答

```
{  
  "handle" : "202.12.30.0 - 202.12.30.255",  
  "startAddress" : "202.12.30.0",  
  "endAddress" : "202.12.30.255",  
  "ipVersion" : "v4",  
  "name" : "JPNIC-NET-JP",  
  "type" : "ASSIGNED PORTABLE",  
  "country" : "JP",  
  "objectClassName" : "ip network",  
  "entities" : [ {  
(以下略)
```


RDAP(Cont.)

- **Authoritativeであるリソースの参照場所を示す**

- 例 : <http://data.iana.org/rdap/ipv4.json>

```
{
  "description": "RDAP bootstrap file for IPv4 address
allocations",
  "publication": "2015-08-11T00:09:31Z",
  "services": [
    (略)
    "202.0.0.0/8",
    (略)
  ],
  [
    "https://rdap.apnic.net/"
  ]
}
```

仮にARINのRDAPサーバー(*)に問い合わせてもAPNICにリダイレクトされて応答

*<https://rdap.arin.net/registry/ip/202.12.30.0/24>

RDAP(Cont.)

- **RIR(地域レジストリ)はサービス提供中**
 - <https://rdap.apnic.net/>
 - <https://rdap.arin.net/>
 - <https://rdap.db.ripe.net/>
 - <https://rdap.lacnic.net/rdap/>
 - <https://rdap.afrinic.net/rdap/>
- **APNIC地域のNIR(国別レジストリ)は対応検討中**

WHOWAS

- **WHOIS登録情報の過去データを閲覧**
- **RIR**
 - ARIN : 所定の申請手続を経て閲覧する
 - <https://www.arin.net/resources/whowas/>
 - RIPE NCC : 公開
 - WHOISコマンドで所定のオプションを付ける
 - APNIC : RDAPを応用したサービスとして開発・試験公開中

WHOWAS(Cont.)

- APNIC WHOWASのWeb UI
 - <https://www.apnic.net/static/whowas-ui/#202.12.30.0/24>

The screenshot displays the APNIC WHOWAS web interface. The browser address bar shows the URL <https://www.apnic.net/static/whowas-ui/#202.12.30.0/24>. The page title is "Whowas" and the search input field contains "202.12.30.0/24".

On the left, a list of IP ranges is shown, with "202.12.30.0 - 202.12.30.255" selected. The main content area displays details for the network "JPNIC-NET-JP" (202.12.30.0 - 202.12.30.255), including its country (JP), type (ASSIGNED PORTABLE), and remarks (Email address for spam or abuse complaints: hostmaster@nic.ad.jp). The description mentions the Japan Network Information Center, Kokusai-Kogyo-Kanda bldg. 6F, 2-3-4 Uchi-Kanda, Chiyoda-ku, Tokyo 101-0047, Japan.

Below the network details, there are three sections for contacts:

- JI13-AP** (JPNIC IP Department): An individual contact with address Kokusai-Kogyo-Kanda bldg. 6F, 2-3-4 Uchi-Kanda, Chiyoda-ku, Tokyo 101-0047 JAPAN, voice +81-3-5297-2311, fax +81-3-5297-2312, and email hostmaster@nic.ad.jp.
- IRT-JPNIC-JP** (IRT-JPNIC-JP): A group contact with address Kokusai-Kogyo-Kanda Bldg 6F, 2-3-4 Uchi-Kanda, Chiyoda-ku, Tokyo 101-0047, Japan, email abuse@apnic.net.
- JE53-AP** (JPNIC Engineering Group): An individual contact with address Kokusai-Kogyo-Kanda bldg. 6F, 2-3-4 Uchi-Kanda, Chiyoda-ku, Tokyo 101-0047 JAPAN, voice +81-3-5297-2311, fax +81-3-5297-2312, and email hostmaster@nic.ad.jp.

WHOIS登録情報の正確性向上

- **法執行機関の問題意識**

- WHOISは、公安事案・犯罪捜査の際に利用
 - データが不正確（特に二次割り当て）
 - データが不足（例：ポート番号がない）

→2016年秋頃から、EUROPOL/FBIなどの警察関係者が各RIR/NIRコミュニティで議論喚起

- 議論＋提案：ARIN
- 議論：RIPE NCC/APNIC/JPNIC

WHOIS登録情報の正確性向上(Cont.)

- **ARIN39(2017/04)**
- **ルール**
 - 年に一度全POCに電子メールを送信し、登録情報の正確性確認を実施
 - 反応がない情報は、その旨WHOISで表記
 - 90日以上反応がない場合、逆引きの委任停止(今回の提案)
- **議論**
 - 趣旨に大筋賛成で好意的
 - 登録情報の削除は効果が薄いうえに問題を悪化させるとして反対意見多数

参考情報

- **JPNIC Blog**
 - RDAP ～次世代WHOISプロトコル～ の紹介
 - <https://blog.nic.ad.jp/blog/rdap-intro/>

**ご清聴
ありがとうございました**

付録

RPKIのはじめ方

資源管理者証明書を準備（資源管理カード／ブラウザ内）

申請における認証について

<https://www.nic.ad.jp/ja/ip/id-procedure.html>



資源申請者証明書を担当者に発行（ブラウザ内）

資源申請者証明書発行マニュアル

<https://www.nic.ad.jp/doc/issue-manual-02.pdf>



リソース証明書とROAの発行開始

<https://rpki.nic.ad.jp/>



発行完了！

お問合せ窓口： ip-service@nir.nic.ad.jp
（または rpki-query@nic.ad.jp）

ROAの登録と管理の方法 (ガイド)

JPNICはインターネットの円滑な運営を支えるための組織です [Top](#)

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
Japan Network Information Center

あなたは IPv4 でアクセスしています。

IPアドレス検索(WHOIS)

WHOISとは? [JPNIC WHOIS Gateway](#)

JPNIC Blog 新着記事

2017/03/16

IPv4割り振り申請の手続きを解説します! ついて

RPKI ケーロちゃんからのお願い
RPKI を使って、IP ネットワークを守ってケーロ!

システムの試験提供開始

[インターネット](#) [Internet Week 2016 最前線から!](#) [JPNIC Blog](#) [RPKI](#)

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
Japan Network Information Center

Web申請システム

移転関連情報

RPKI IP アドレスの不正利用対策
ROA の登録
をお願いします

[ページトップへ](#)

本方針 | [Q&A](#) | [サイトマップ](#)

[RSS](#)

ログインユーザ名: JPNICNET (契約・資源管理者)

お知らせ

- [【2017.02.22】 ROAの登録をお願いします \[RPKIシステムへアクセス\(資源申請者\)\] \[登録方法\] \[ROA/RPKIとは\]](#)
- [【2017.02.21】 初心者向け「インターネット入門」～新入社員・異動社員の研修としてお役立てください～](#)
- [【2017.02.21】 Internet Week 2016 プレゼンテーション資料公開のお知らせ](#)
- [【2017.02.09】 BIND 9における脆弱性について\(2017年2月\)](#)
- [【2017.02.01】 IPレジストリシステムおよびJPIRRシステム2月のメンテナンスに伴うサービス一時停止のお知らせ](#)
- [>>> JPNICからのお知らせ一覧](#)
- [>>> 問い合わせ](#)

ROAの登録と管理の方法 (ガイド)

JPNICはインターネットの円滑な運営を支えるための組織です
カテゴリ別メニュー

Top Q&A サイトマップ 文字サイズ: 小 中 大

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
Japan Network Information Center

English(英語) RSS

サイト内検索... 検索

正常にアクセスできると初期の画面が表示されます。



The screenshot shows the 'ROA Web (JPNICNET)' interface. It has a header with the JPNIC logo and navigation links. The main content area is divided into sections: 'ROAの管理' (ROA Management) with buttons for 'Prefix', 'Import', and 'Export'; 'ROA発行のできるリソース一覧' (List of resources that can be issued as ROA) with a table of IPv4 prefixes; and 'リソース証明書の一覧' (List of resource certificates) with a table of certificates. The table for IPv4 prefixes shows three entries: 193.41.193.0/24, 202.112.240.0/21, and 202.112.240.0/24, each with a corresponding 'ROA' link. The table for certificates shows three entries with columns for 'リソース' (Resource), '状態' (Status), and '有効期限' (Valid Period).

ROA Webの初期画面

画面の右側にROAの発行対象となるIPアドレスが表示されます。「ROAを作成」をクリックします。

おわり