RPKI in DNS DAY

木村泰司

2015年11月19日(木)

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

発表者

- **名前**
  - 木村泰司（きむらたいじ）
- **所属**
  - 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)
    - CA / RPKI / DNSSEC / セキュリティ情報：
      調査 (執筆)・セミナー・企画・開発・運用・ユーザサポート
- **業務分野**
  - 電子証明書 / RPKI / DNSSEC (DPS/鍵管理/HSM他)

Resource PKI（RPKI）の目的

- **アドレス資源（IPアドレスやAS番号）の真正性を確認するための認証基盤**
  - 利用例：ルーティングの情報を確認するため
  - 利用例：移転元のIPアドレスを確認するため(構想)

RPKIの利用イメージ(1/2)

リソースホルダー

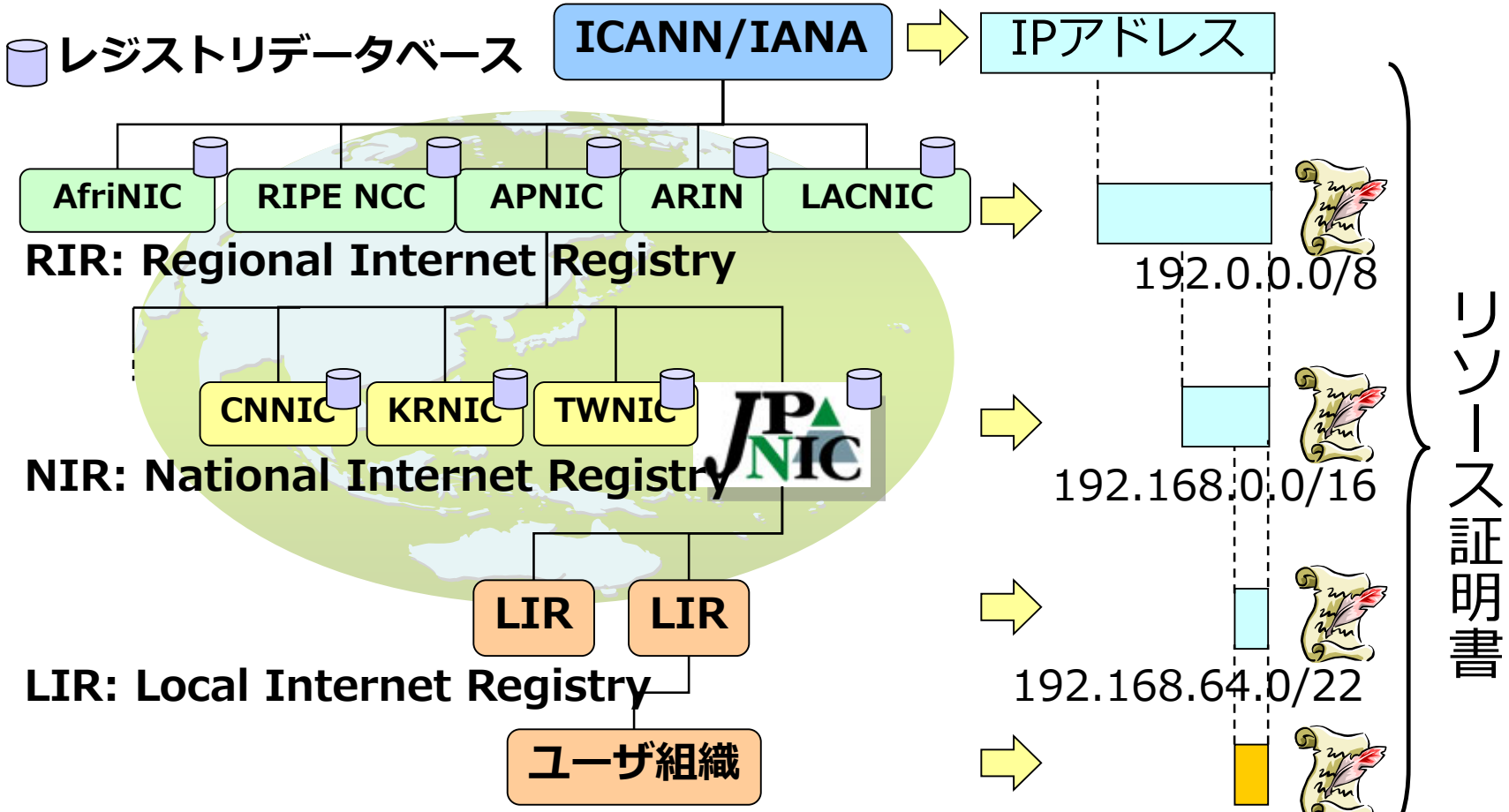
リソースホルダーが、発行されたリソース証明書の私有鍵を使ってROA（Prefixに対してBGPのOrigin ASを示した署名データ）に署名し、経路情報の正しい広告元Origin ASを確認できるようにしておく。

RPKIの利用イメージ(2/2)

```
bgpd# show ip bgp

BGP table version is 0, local router ID is 192.168.10.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, R Removed

Validation:    v - valid, n - notfound, i - invalid, ? - undefined
SRx Status:    I - route ignored, D - SRx evaluation deactivated
SRxVal Format: validation result (origin validation, path validation)
Origin codes: i - IGP, e - EGP, ? - incomplete

   Ident     SRxVal SRxLP Status Network          Next Hop         Metric  LocPrf Weight Path
*> DE83681E v(v,-) + 200,       192.168.1.0      172.16.10.1                200s      0 65001 64496
*> FBF4BE57 n(n,-) + 100,       192.168.2.0      172.16.10.2                100s      0 65001 64497

bgpd#
```

対応ルータは、経路表でOrigin ASが正しいかどうかを判別でき、IPアドレスを不正に利用した経路情報を無視できる＝経路ハイジャックの影響を受けないようにできる。

リソース証明書の役割



レジストリから正しく分配されたリソースであることを証明する

リソース証明書の例

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: CN=D5BBADA3
    Validity
      Not Before: Apr 15 10:24:39 2014 GMT
      Not After : Apr 14 10:24:39 2019 GMT
    Subject: CN=D5BBADA3
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)

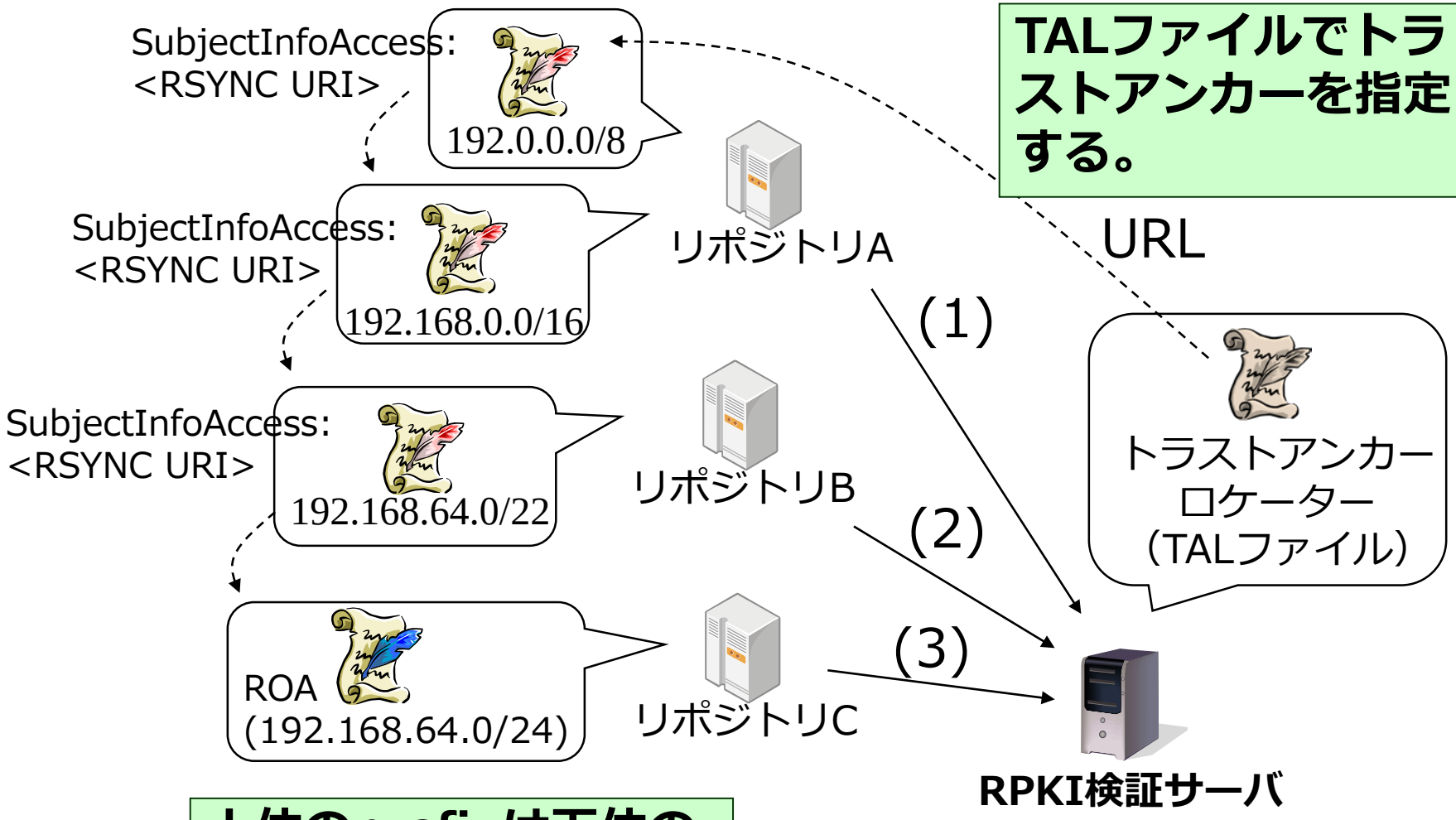
    X509v3 extensions:
      X509v3 Basic Constraints: critical
        CA:TRUE
      X509v3 Subject Key Identifier:
        18:CE:ED:52:F0:99:02:8A:58:3C:F1:7B:53:71:0E:1F:5D:37:4F:8D
      X509v3 Key Usage: critical
        Certificate Sign, CRL Sign
      Subject Information Access:
        CA Repository - URI:rsync://rpki01.nic.ad.jp/repository/
        1.3.6.1.5.5.7.48.10 - URI:rsync://rpki01.nic.ad.jp/repository/jpnic-ta-03.mft

sbgp-autonomousSysNum: critical
  Autonomous System Numbers:
    0-4294967295

sbgp-ipAddrBlock: critical
  IPv4:
    0.0.0.0/0
  IPv6:
    ::/0

トラストアンカーと信頼モデル

トラストアンカーと署名検証



TALファイル – trust anchor locator

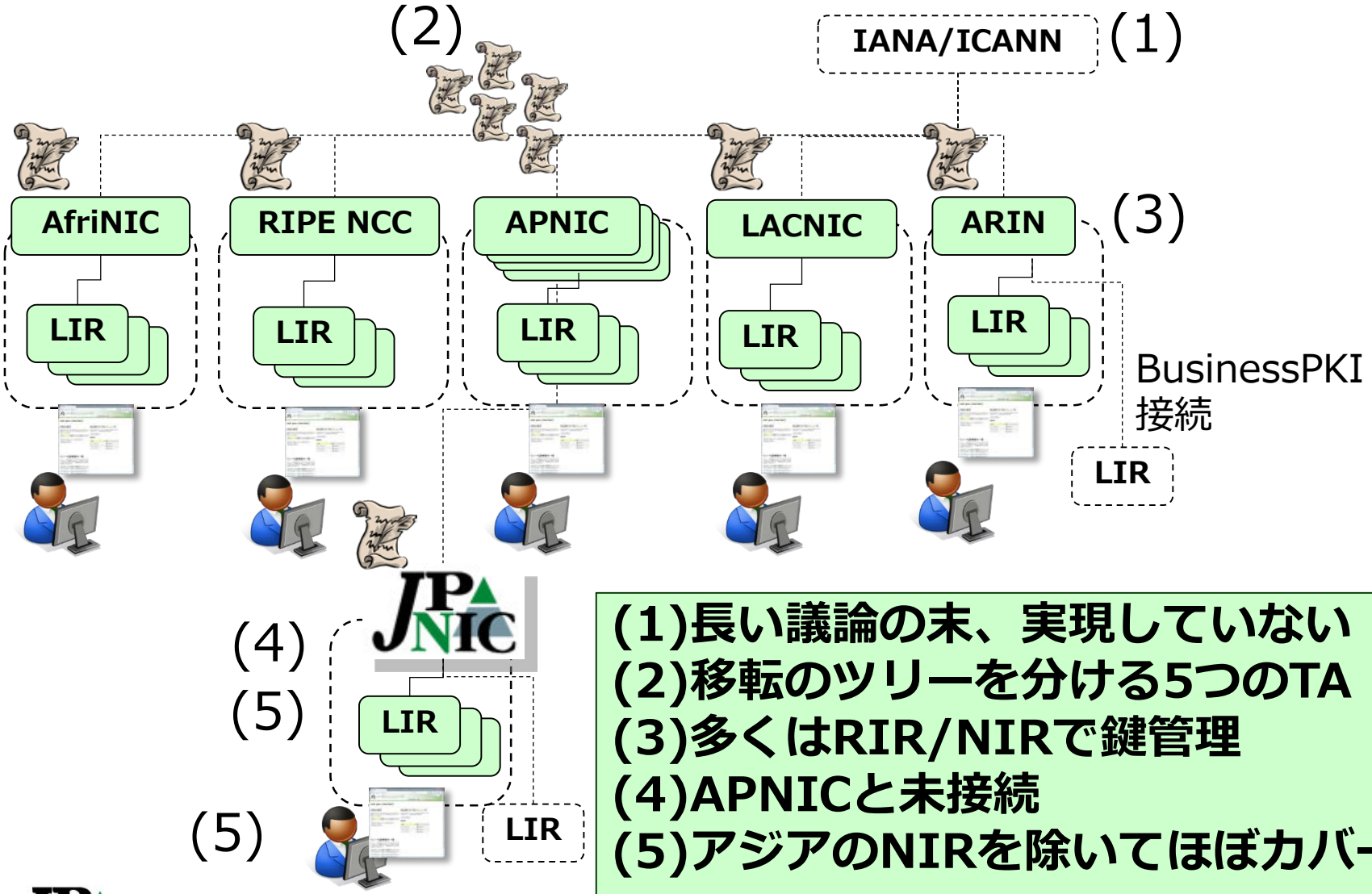
TALファイルの例

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

署名検証する前に入手済みの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する。

ツリー構造の実際



(1)長い議論の末、実現していない
(2)移転のツリーを分ける5つのTA
(3)多くはRIR/NIRで鍵管理
(4)APNICと未接続
(5)アジアのNIRを除いてほぼカバー

トラストアンカーの指定

あるキャッシュサーバにおけるトラストアンカーの設定

```
% ls /var/rcynic/conf/trust-anchors
afrinic.tal                          apnic-rpki-root-ripe-
origin.tal
apnic-rpki-root-afrinic-origin.tal   apnic-testbed.tal
apnic-rpki-root-arin-origin.tal      jpnic-preliminary-ca-s1.tal
apnic-rpki-root-iana-origin.tal      lacnic.tal
apnic-rpki-root-lacnic-origin.tal    ripe-ncc-root.tal
%
```

トラストアンカーと信頼モデル

- **トラストアンカーは5つのRIR**
  - とJPNIC
- **トラストアンカーはTALファイルで指定**
  - RPKIの署名検証ソフトウェアに付属
  - 正しいTALファイルであることの確認方法…
- **第三者による認証業務のチェックはない**
  - RPKIのCertificate Policy(CP)はある(RFC6484)
  - どの位セキュアな運用を行うか(ex. CPS)の指標はない

RPKIにおける鍵管理

生成	RPKI Webサービスでは、RIR/NIRのシステム内で鍵生成される。BPKI(Business PKI)接続の場合はLIR側。規定なし。
公開	リポジトリ(rsyncサーバ)への公開。
配送/導入	予め入手したTALで確認。
更新	RPKI Webサービスの場合は自動的にシステム内で行われることが多い。BPKI接続の場合はBPKIを使って更新。
失効	リポジトリにCRLが置かれる。OCSPなどはない。抜け防止のためにManifest。
期限/廃棄	2年ほど。鍵更新を伴わない証明書更新はない。

RPKIのDNSとのかかわり

- **署名つきオブジェクトの配送**
  - TALファイルに記述されたURI
  - AuthorityInfoAccessに記述されたURI

  ⇒ 証明書やROA一式の正しさは署名検証で確認
- **DNSのRPKIへの応用**
  - DNSを使ったRPKIへの機能連携は...特になし
  - 逆引きDNS(DNSSECは必須)を使って経路情報を確認する提案(RLOCK RR)がIETFで行われているが標準化は進んでいない。

おわり