RPKIとインターネット ルーティングセキュリティ

～ルーティングセキュリティの未来 ～

セキュリティ事業担当
木村泰司

JPNIC 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

内容

1. リソース証明書とRPKI
2. 国際的な動きと標準化動向
3. ディスカッションのポイント

1、リソース証明書とRPKI

JPNIC 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

リソース証明書とは
～アドレス資源の「正しさ」～

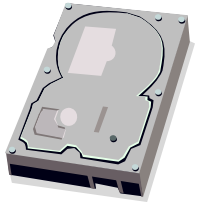
イ）

whois

$ whois –h whois.nic.ad.jp 192.0.2.0

これは正しいアドレスだ

ロ）

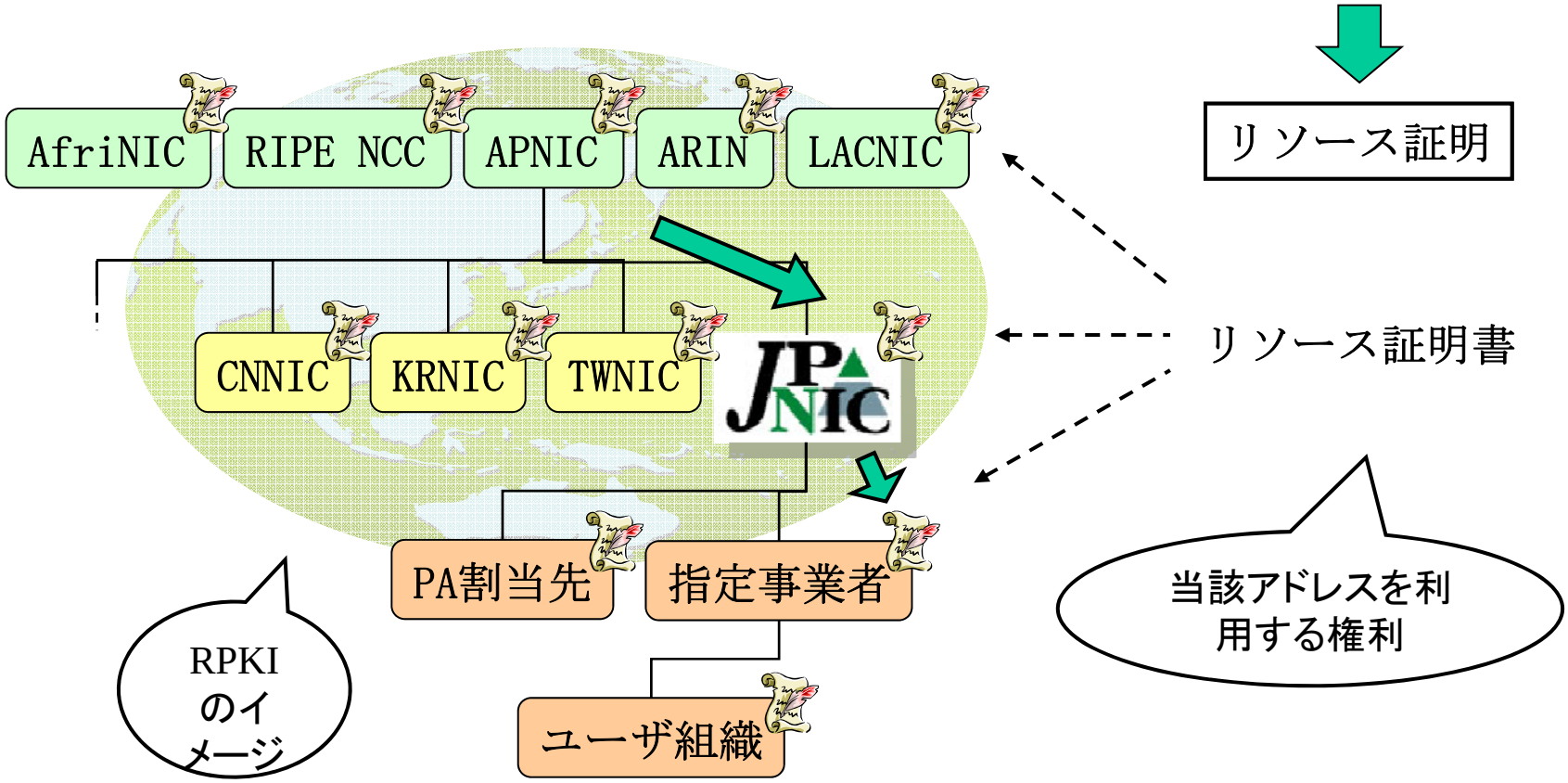


ハードディスク

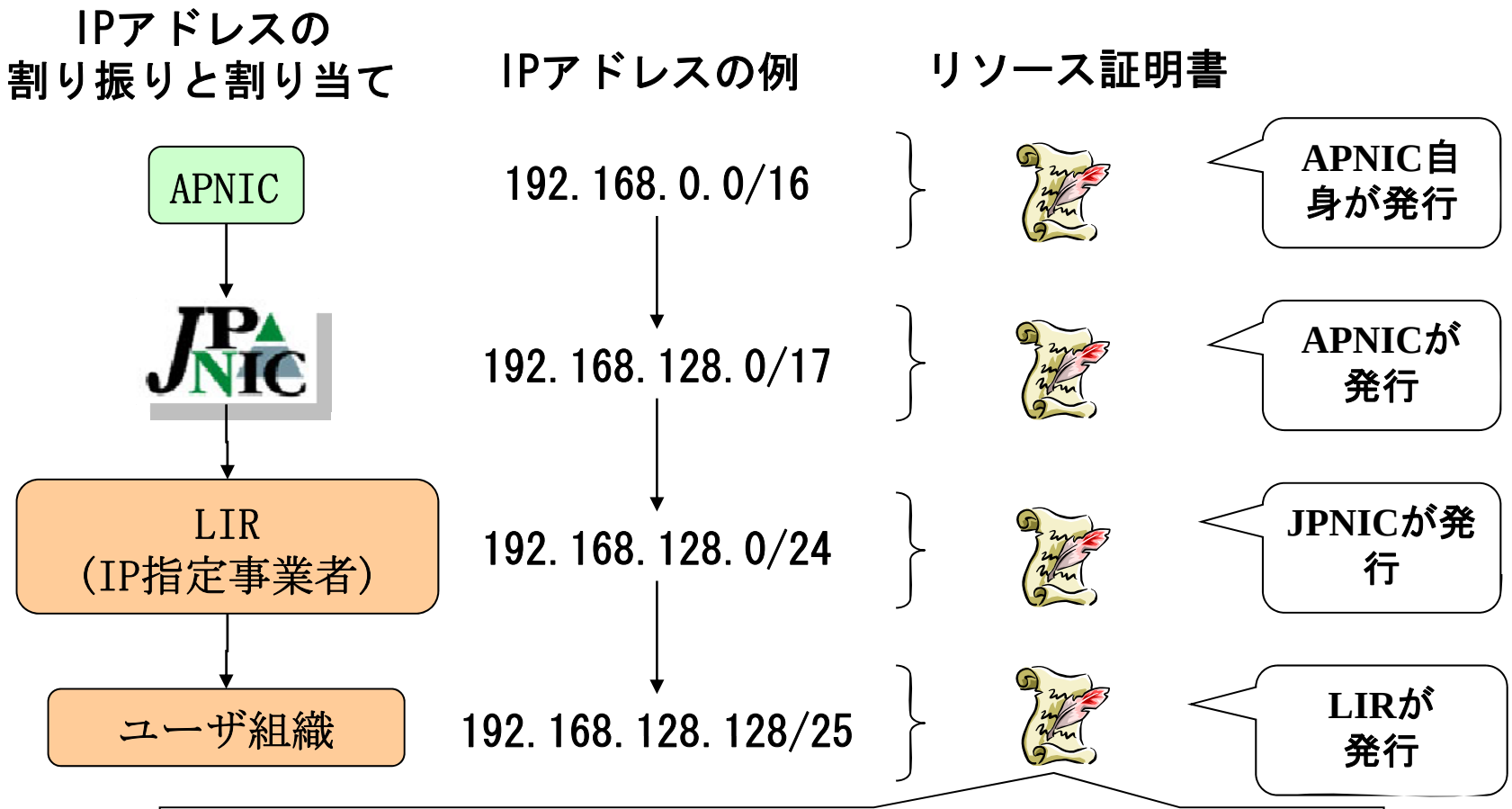
192.0.2.0 – 192.0.2.255

リソース証明書とRPKI

「正しい」リソースとは
レジストリに登録された通りに割り振りまたは割り当てが行われているリソースである。



リソース証明書の「検証」



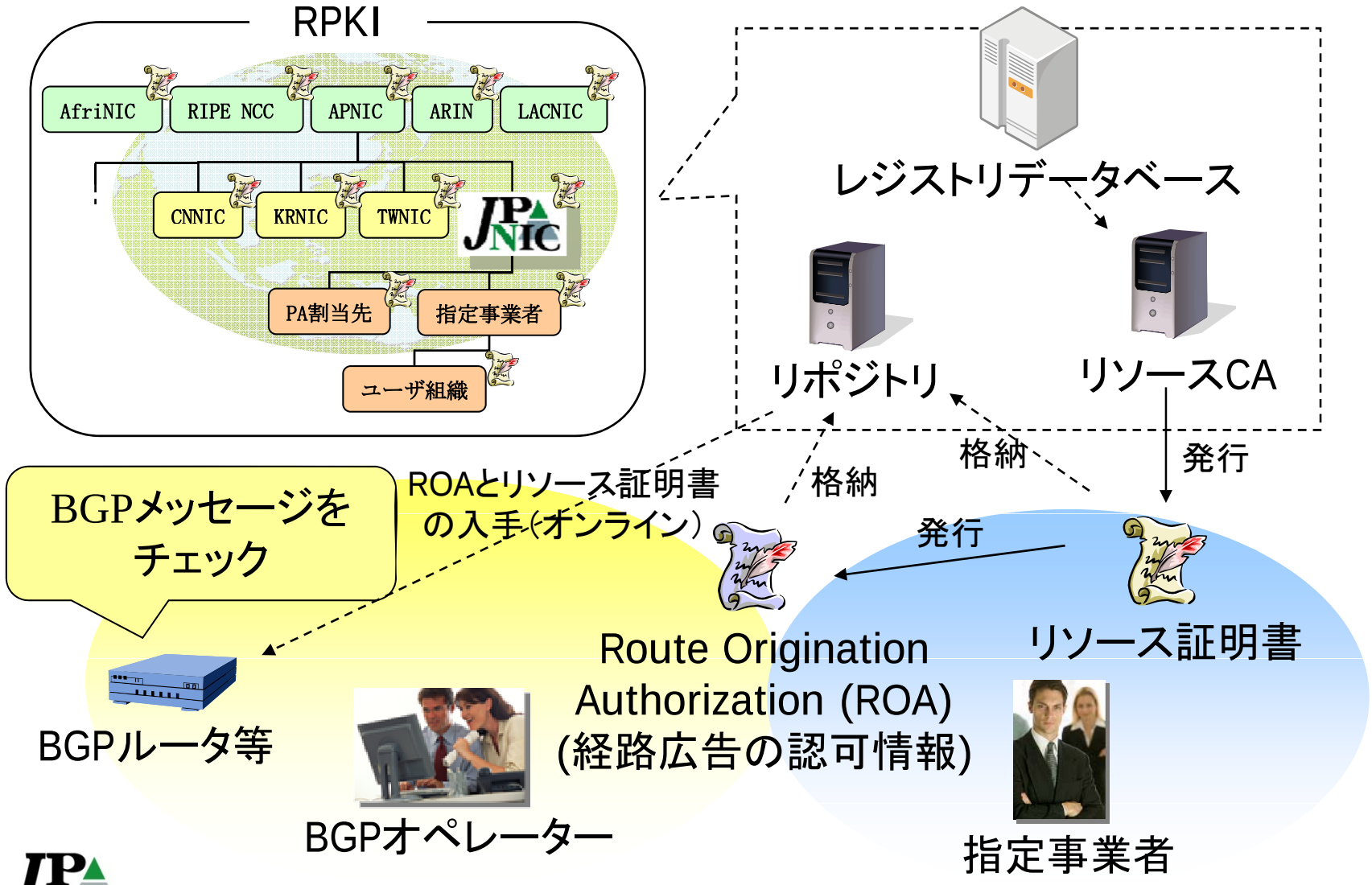
○チェックポイント
- IPアドレスが発行元のIPアドレスの範囲に入っていること。
- 元を辿っていくとレジストリの認証局にたどり着くこと。

RPKIの用途

a. アドレス資源の管理
   - Whoisに代わる「正しい」アドレス資源を証明する基盤

b. 応用
   - セキュアルーティング
     - セキュアなインターネット経路制御の自動化 ★
     - IXにおけるアドレス確認業務の補強

RPKIを使ったセキュアな インターネット経路制御



2、国際的な動きと標準化動向

JPNIC 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

RIRにおけるリソース証明書

	APNIC	ARIN	RIPE NCC	LACNIC	AfriNIC	JPNIC
リソース証明書	提供中	試験提供中	提供中	検討中「Resource Certification project」	検討中	調査と検討

- APNIC、RIPE NCCではリソース証明書を既に提供中。ARINは試験提供。

時系列

★2004th Jun　RFC3779

	2006年度	2007年度	2008年度	2009年度
IETF	★Mar　1st SIDR BoF ★Apr　SIDR WG結成	★Mar　I-D “ROA” ★Apr　I-D “profile” ★Jul　I-D “architecture”	★Dec　I-D “rpsl-sig”	★Feb　I-D “trust anchor”
APNIC	リソース証明書 エンジン部分の開発	I/F等の開発	★Sep MyAPNICでの 正式提供開始	
ARIN	★システム設計開始 開発への参加	レジストリ連携の開発		★ Jul 試験提供開始
RIPE NCC	★Oct CATF結成 開発への参加	★CertPROTO 業務の検証	開発 ★ Oct ベータテスト ★ Oct ポリシー提案 2008-08	★ Jul 正式提供開始
JPNIC	★ RIR検討への参加／リソースセキュリティの調査 経路情報の登録機構 開発	利用実験	★ 経路ハイジャックに関する情報提供	

IETFにおける標準化動向

- RFC
  - X.509 Extensions for IP Addresses and AS Identifiers (RFC3779)
    - X.509証明書にIPアドレスとAS番号を入れられるようにする拡張
- Internet-Draft
  - An Infrastructure to Support Secure Internet Routing (draft-ietf-sidr-arch-09.txt)
    - リソース証明書やROAの説明。RPKIの構造やレジストリにおけるCAの役割など。
  - A Profile for Route Origin Authorizations (ROAs) (draft-ietf-sidr-roa-format-06.txt)
    - IPアドレスのholderがASに経路広告を認可するというROAを定義。
  - A Profile for X.509 PKIX Resource Certificates (draft-ietf-sidr-res-certs-17.txt)
    - リソース証明書の意味「right-to-use」やリソース証明書の記載内容（プロファイル）を定義。

RPKIの主要オブジェクト

- Resource Certificate（リソース証明書）
  - IPアドレスやAS番号の利用権利（right-of-use）を示す電子証明書
- Route Origination Authorizations（ROA）
  - IPアドレスの割り振り先（または割り当て先）が、ASに対してIPアドレスの経路広告を認可（authorization）したことを示す電子署名付きのデータ
- Manifest
  - RPKIにおける認証局が発行したリソース証明書・ROA・CRLのリストに電子署名を付けたデータ
  - リソース証明書・ROA・CRLなどの、一部を消して再配布するような、不正行為対策のデータ

3、ディスカッションのポイント

JPNIC 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

ディスカッションのポイント

① リソース証明書の内容は正しいのか
- レジストリデータベースと変わらない

② RPKIを使ってみるには何がいるのか
- レジストリから発行されたリソース証明書（もしくは。。）
- リソース証明書やROAを発行するプログラム
- リソース証明書やROAを検証するプログラム（OpenSSL-0.9.8e頃より表示が可能になっている）

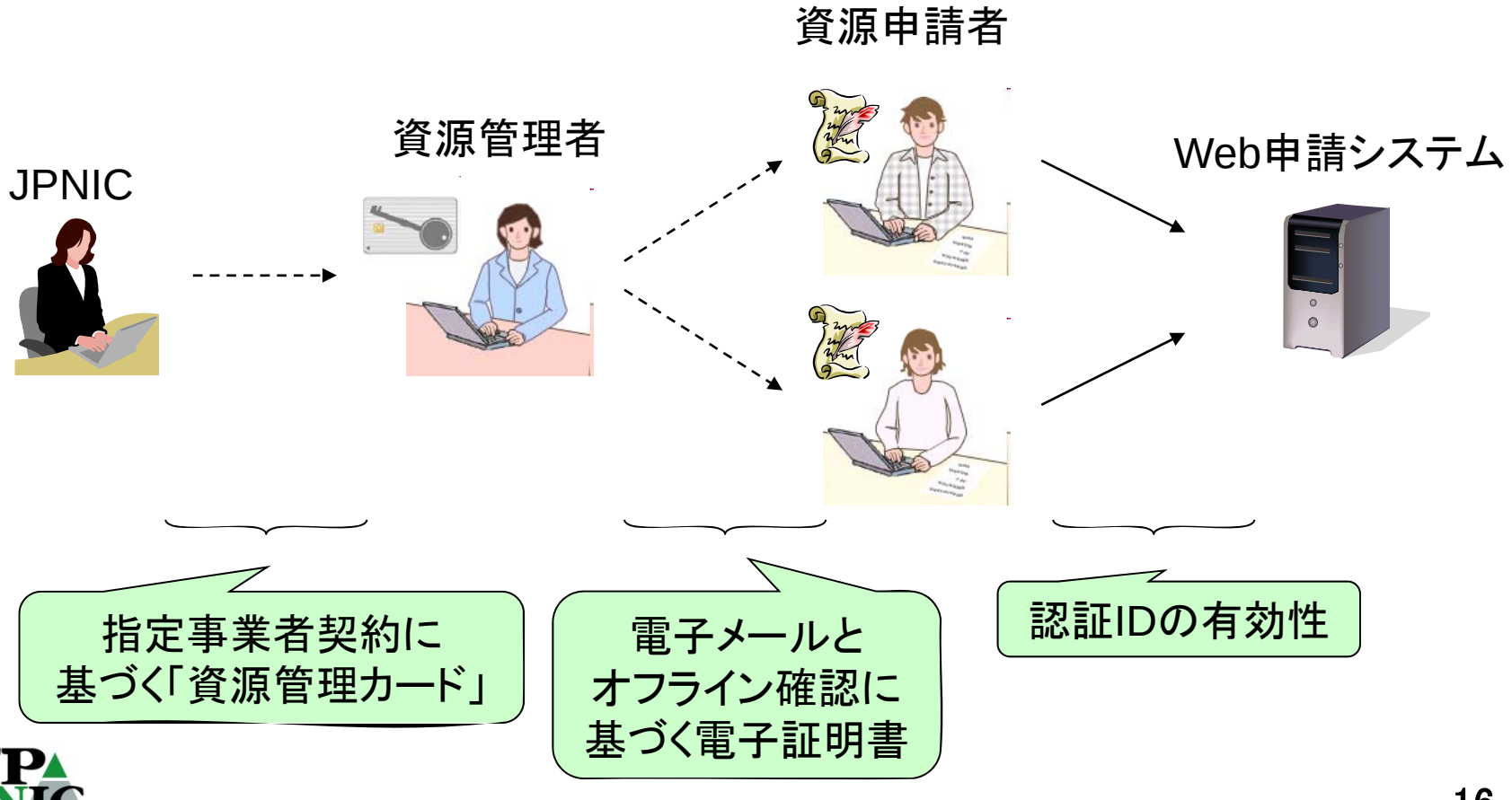
③ Route Origination Authorization
- アドレスの利用権利を持つものが経路制御を決める

④ RPKIを使わないといけなくなるのか
- ARIN、RIPE NCC、ARINは提供開始。使わないといけないわけではない。

⑤ 日本はどうするのか？
- JPNIC
  - リソース証明書について継続的に調査中
  - セキュアな経路制御の為に、経路情報の登録認可機構を含めて検討中

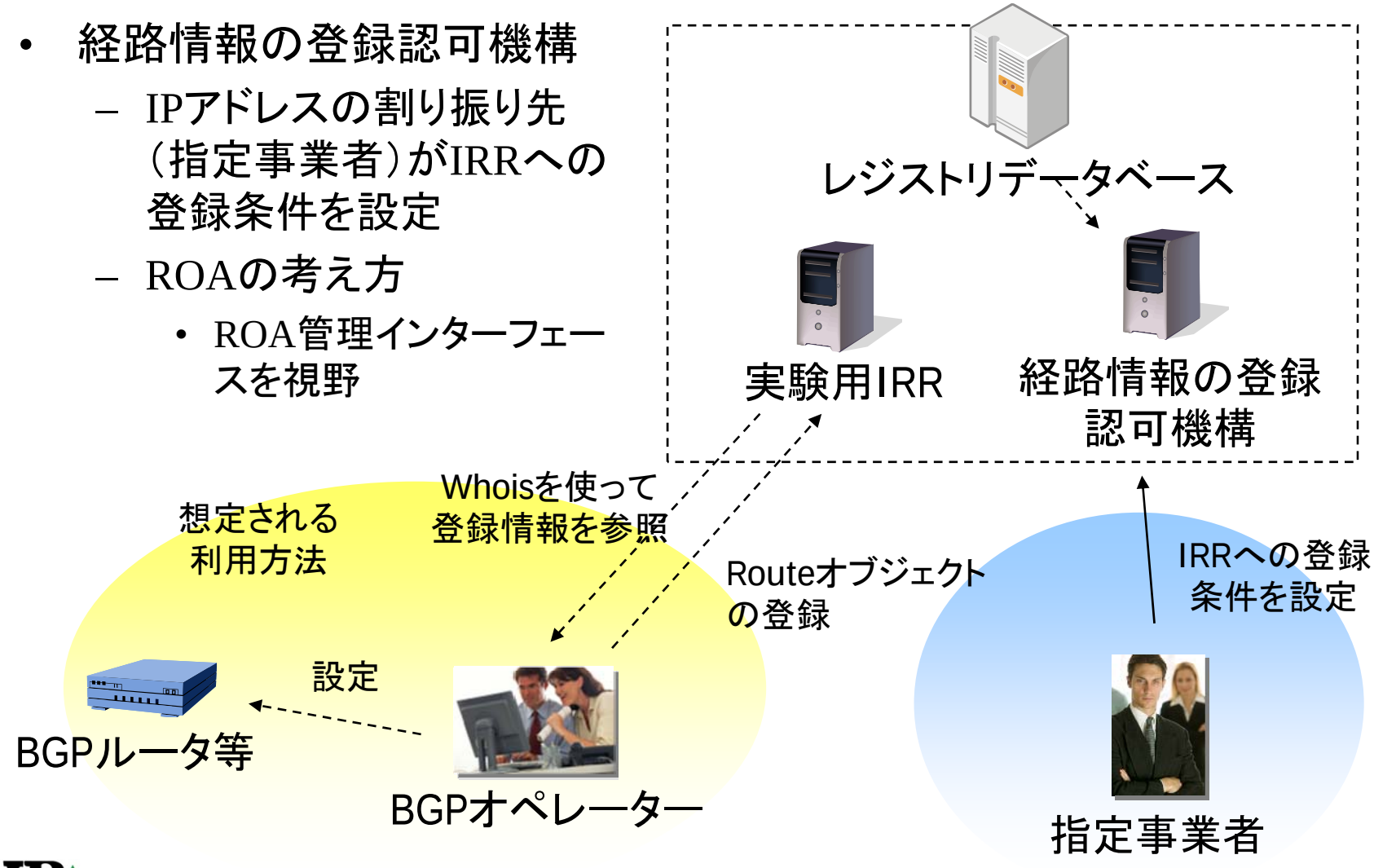
RPKIとJPNICの活動（1）

- JPNICの「電子証明書を用いた認証」
  - <u>ユーザ認証</u>です。



RPKIとJPNICの活動（2）

- 経路情報の登録認可機構
  - IPアドレスの割り振り先（指定事業者）がIRRへの登録条件を設定
  - ROAの考え方
    - ROA管理インターフェースを視野



情報源

- IETF Secure Inter-Domain Routing (sidr)
  - http://www.ietf.org/dyn/wg/charter/sidr-charter.html
- APNIC – Resource Certification
  - http://www.apnic.net/services/services-apnic-provides/resource-certification
- Resource Certification (RIPE NCC)
  - https://certtest.ripe.net/
- Resource Certification (ARIN)
  - http://rpki-pilot.arin.net/

JPNIC

おわり

JPNIC 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