リソース証明書は何を「証明」しようとしているのか

セキュリティ事業担当

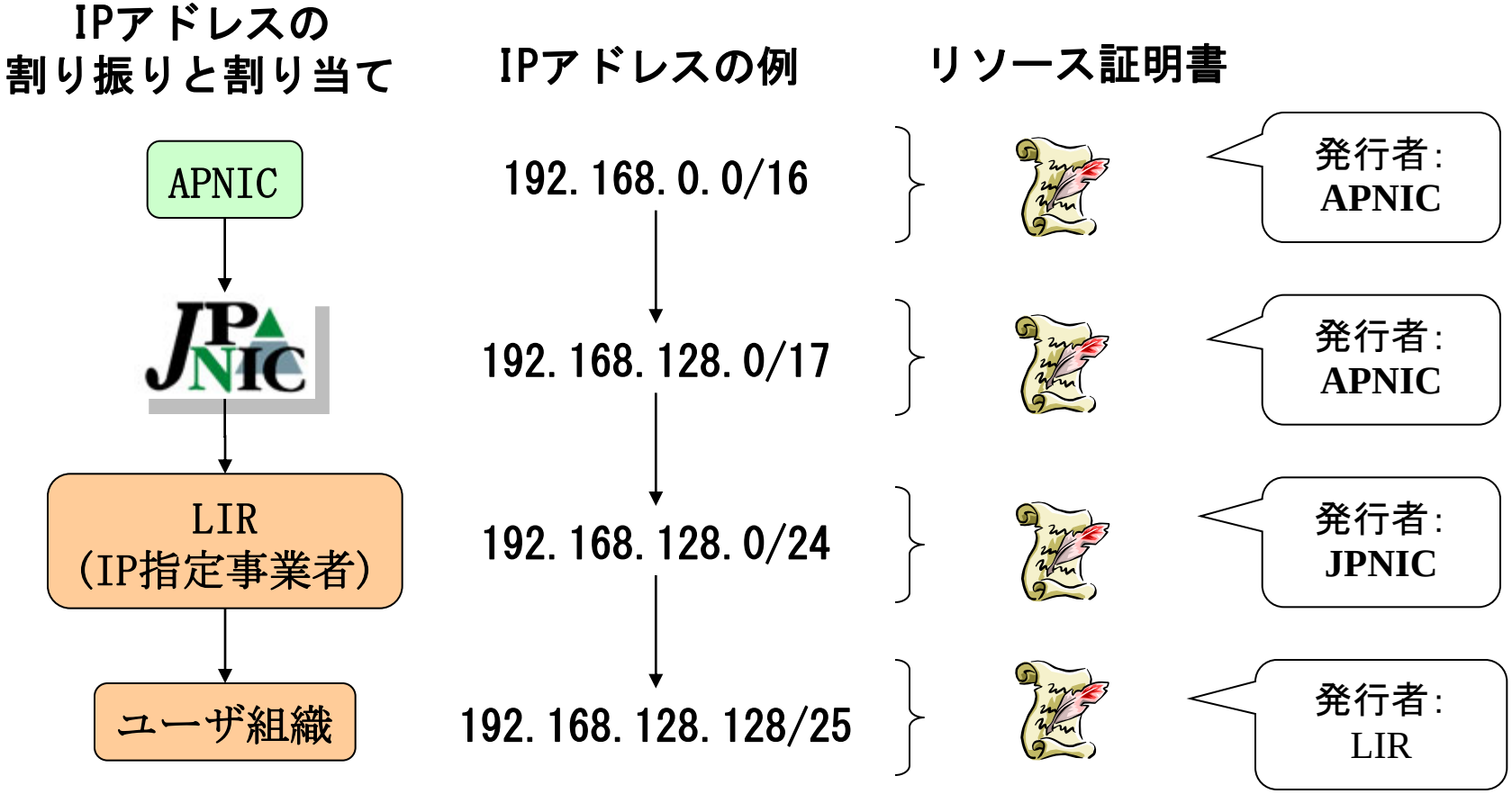
木村泰司

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

- リソース証明書とは何か
- 他のレジストリの状況
- ディスカッションのポイント

リソース証明書とは何か(1/2)

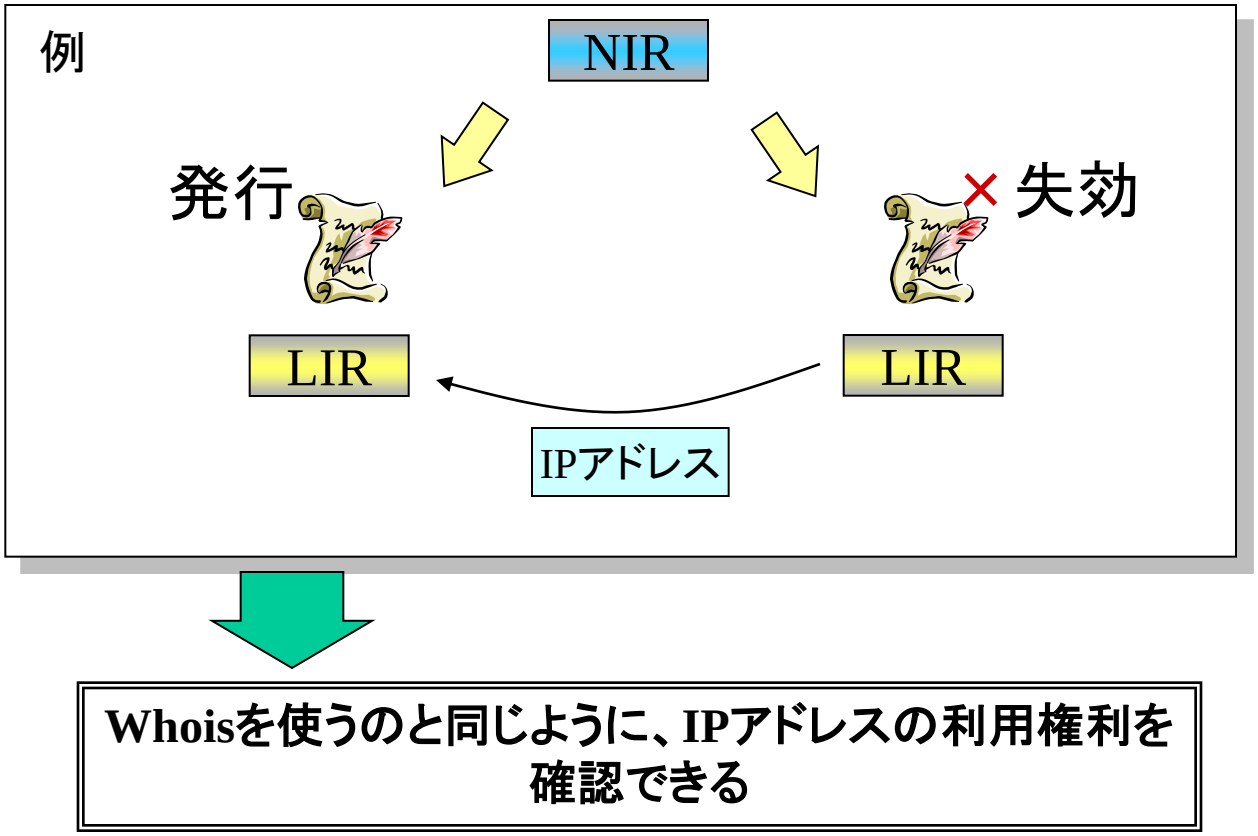


リソース証明書とは何か(2/2)

発行元: (RIPE NCC)
対象: (JPNIC)
アドレスブロック:
10.0.56.0/21

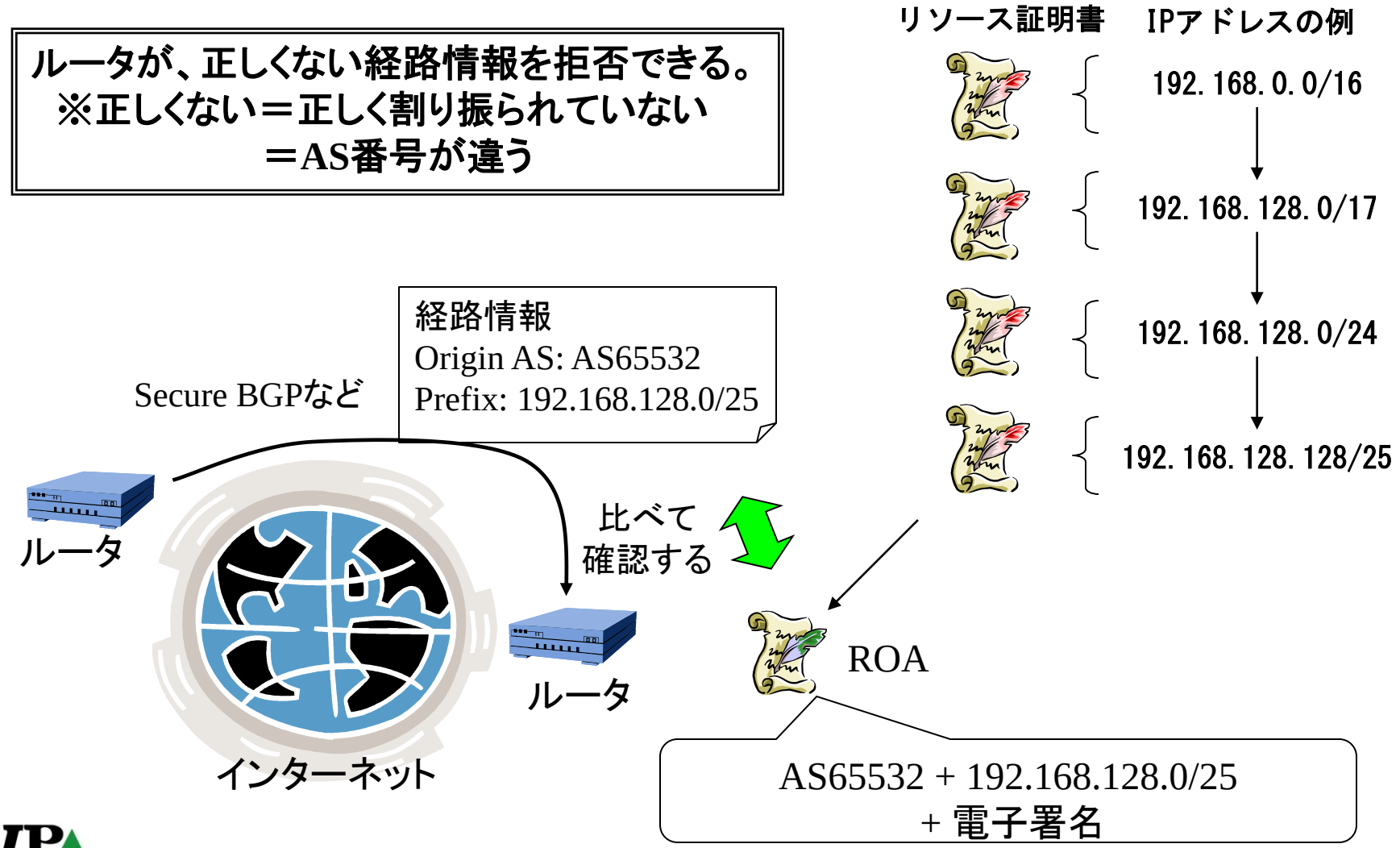
Version: 3
Serial: 3fc2
Issuer: CN=0NzrOpdx0k5_wB44AhMeNzEc0Mk
Not Before: 2008年10月30日 15:52:32
Bot After: 2009年7月1日 9:00:00
Subject: CN=0a8f65ba-d8e2-4759-b73c-8913ffc731f2
Subject Key Identifier: 22d85f282bdf913326cf29d2149a26d82ac37fe4
Authority Key Identifier: d0dceb3a9771d24e7fc01e3802131e37311cd0c9
Authority Info Access: CA Issuers:
URI: rsync://certtest.ripe.net/certrepo/4e/2df8f5-18be-4542
-b991-d2dde6d19ebb/1/0NzrOpdx0k5_wB44AhMeNzEc0Mk.cer
Subject Info Access: caRepository -
URI: URI:rsync://certtest.ripe.net/certrepo/16/135b01-8cde-4286
-aa68-5d517f5e2c1b/1/IthfKCvfkTMmzynSFJom2CrDf-Q.roa
CRL Distribution Points:
URI:rsync://certtest.ripe.net/certrepo/16/135b01-8cde-4286-aa68
-5d517f5e2c1b/1/0NzrOpdx0k5_wB44AhMeNzEc0Mk.crl
Certificate Policies: critical 1.3.6.1.5.5.7.14.2
sbgp-ipAddrBlock: IPv4: 10.0.56.0/21

用途(1/2)
アドレス資源の利用権利を証明する

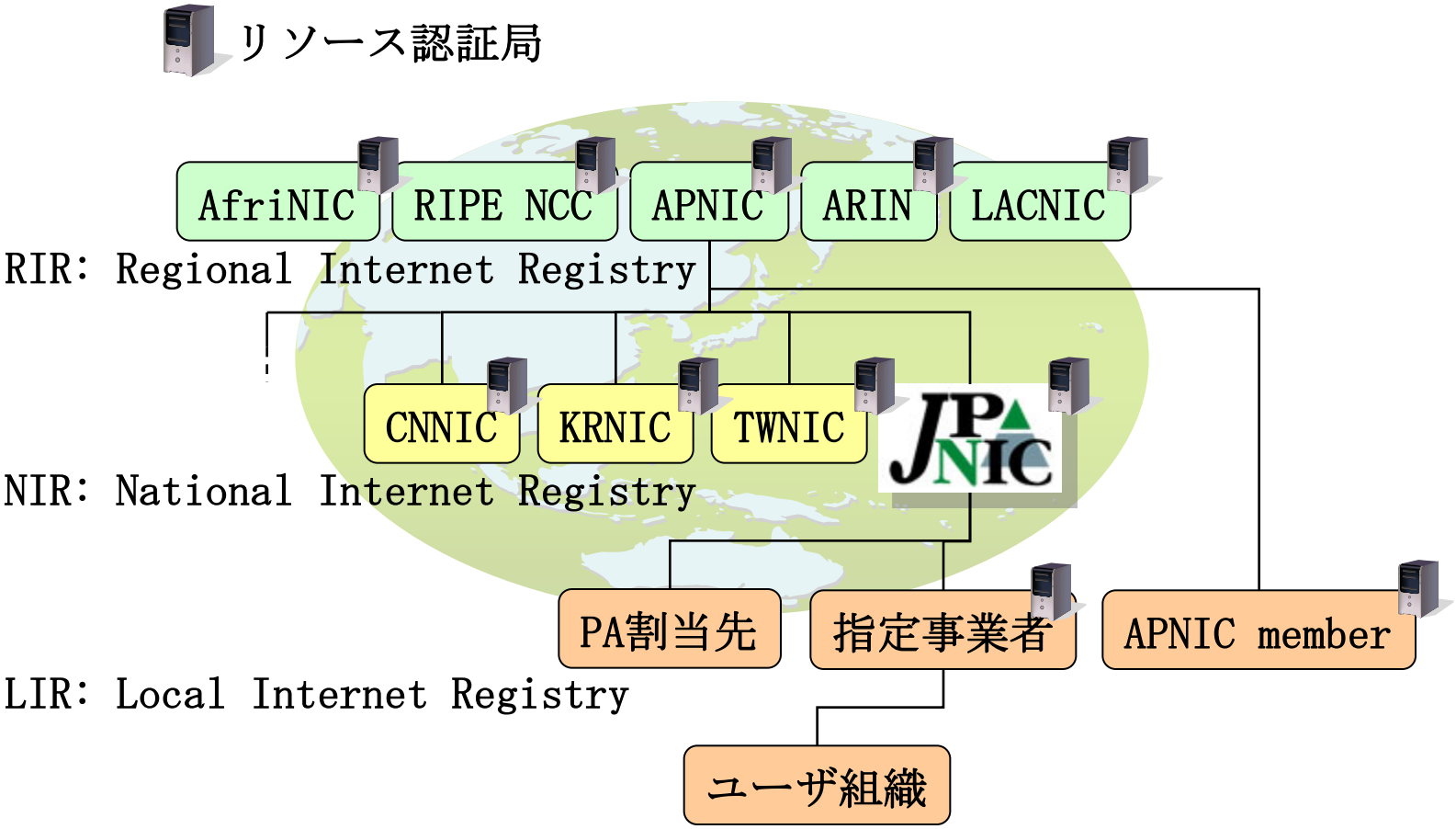


用途(2/2)
ルーティングセキュリティで使う

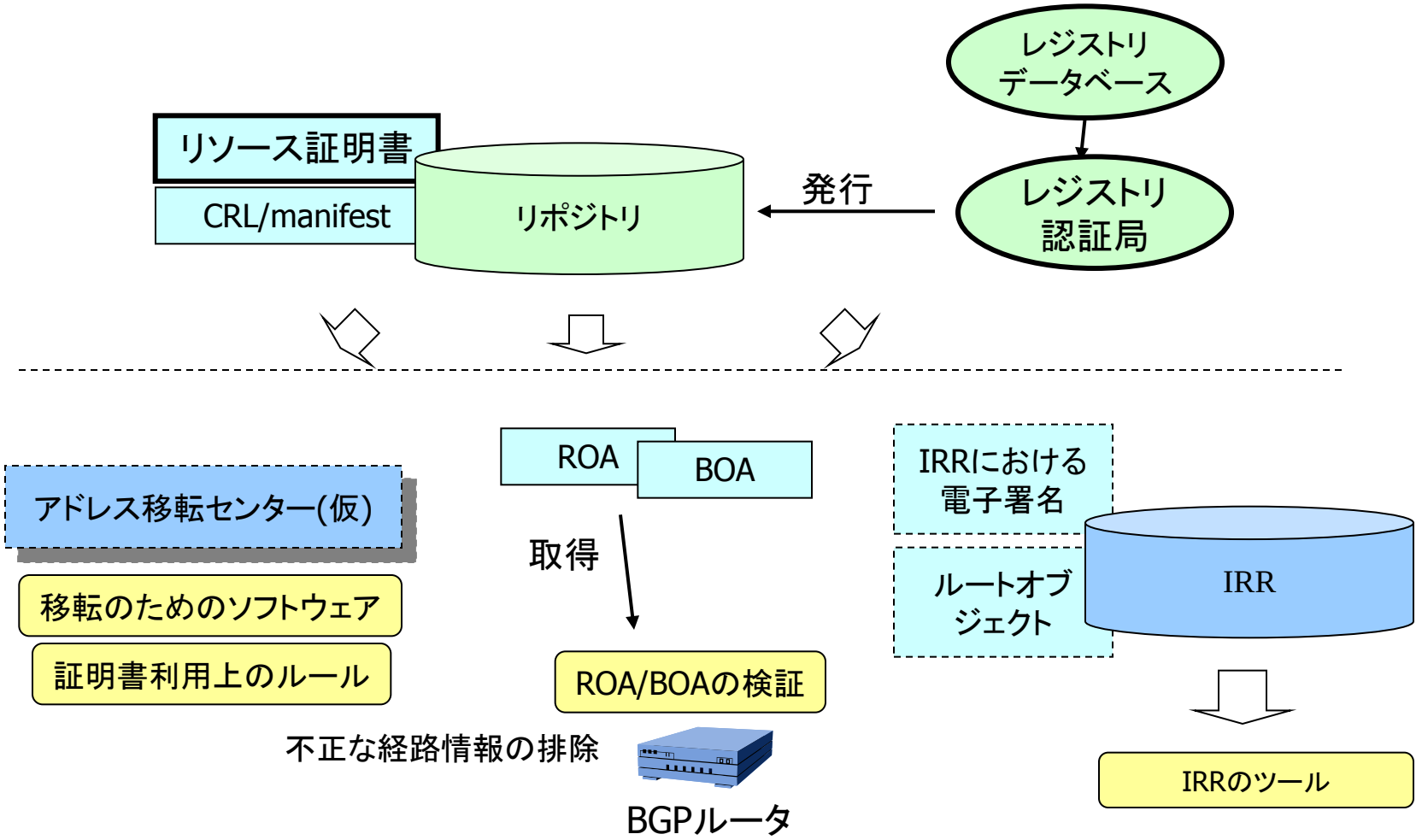
ルータが、正しくない経路情報を拒否できる。
※正しくない＝正しく割り振られていない
＝AS番号が違う



デプロイメントの考え方(1/3)
リソースPKI



デプロイメントの考え方(2/3)
提供のされ方



デプロイメントの考え方(3/3)
必要なもの

- もの
  - リソース認証局
    - レジストリで運用される。
    - LIRも構築可能。
  - ROA発行システム
    - LIR(レジストリがASP？)
  - 証明書クライアント
    - OpenSSL
    - (RIPE NCCのPC用ツール)
    - (APNICのPC用ツール)
    - (ルータ)
- きまり
  - ポリシー
    IPアドレスの利用権利を定義
  - リソース証明書利用者同意書(レジストリユーザ間)
  - リソース証明書検証者同意書(ユーザ間)
- 運用
  - レジストリデータを実際の割り振り状況と一致するように保つ

他のレジストリの状況

RIRにおける認証局とリソース証明書

	APNIC	ARIN	RIPE NCC	LACNIC	AfriNIC	JPNIC
認証局の構築	○	○	○	×	ー	○
電子証明書を用いた指定事業者認証サービス	○	○	○	ー	ー	○
リソース証明書	試験利用サービスを実施中 (MyAPNIC)	実験やサービスを行うかどうかは不明 (システム開発は行っていた)	試験利用サービスを実施中 (LIRPortalへの組み込みは2009年に予定)	検討中 「Resource Certification project」	検討中	調査と検討

- ユーザ認証の為の認証局は整備が進んでいる
- APNIC、RIPE NCCではリソース証明書の試験利用サービスが始まっている

ディスカッションのポイント

ポイント（1/3）

- リソース証明書が証明することは何か
  - IPアドレスが割り振り済であるか、割り当て済であること
    - 誰に割り振られているのかはわからない
  - 私有鍵の持ち主がIPアドレスの利用権利を持っていること

⇒　リソース証明書を利用できるようにすれば、アドレスの移転が実現するというわけではない

JPNIC

ポイント（2/3）

- WHOISの代替機能かどうか
  - 当初、WHOISに代わって正当なアドレス割り振りを示す情報源になると言われたが・・
  - リソース証明書で提供できない情報がある
    - point of contact
    - name server

⇒ WHOISの代替機能ではない

ポイント（3/3）

- 運用課題
  - 実験してみなければわからない面もある
    - 実際にどういう場面で使われるのか
    - リージョンをまたいだ移転は実現するのか
    - リソース証明書の有効性が確認できない場合の対処方法

⇒ RIPE NCCの試験利用サービス開始の背景

- RIPE NCCのcerttest、APNICのMyAPNIC
- 第73回IETF SIDR WGでも議論される予定

まとめ

- リソース証明書が「証明」しようとしていること
  - IPアドレスが割り振り済であるか、割り当て済であること
    - 誰に割り振られているのかは証明書だけではわからない
  - 私有鍵の持ち主がIPアドレスの利用権利を持っていること

- 用途
  - セキュアルーティング
  - IPアドレスの利用権利

- ディスカッションのポイント
  - アドレス移転に対してリソース証明書がどのように役立つのか、できることとできないことを理解して議論していく必要がある。
  - 利用実験を通じた検討も重要だと考えられる。

おわり