リソースPKI (RPKI) アップデート

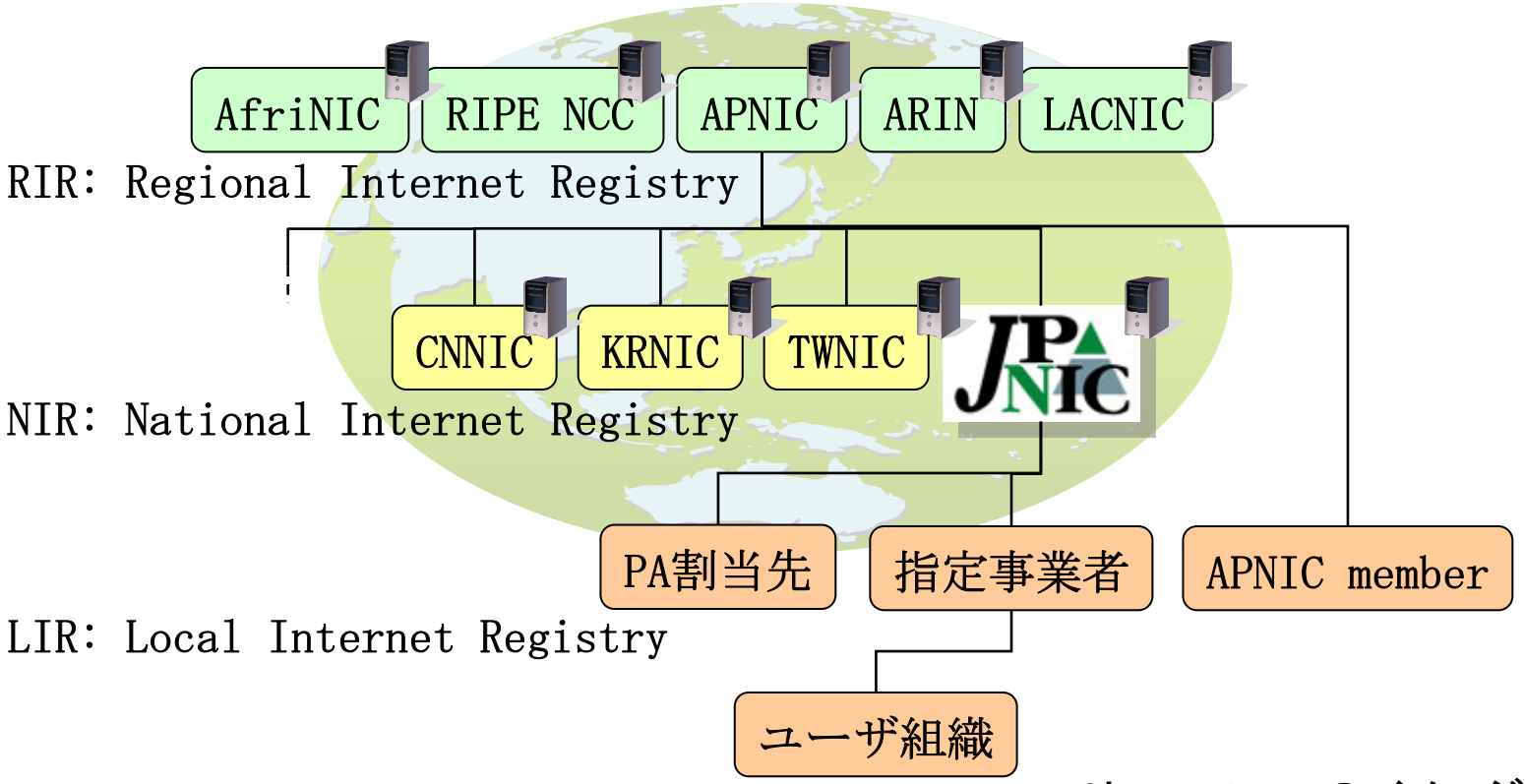
社団法人日本ネットワークインフォメーションセンター
木村泰司

内容

- リソースPKIとは
- RPKIの国際動向
- RPKI testbed
- プロトコル策定と実装の状況

リソースPKIとは

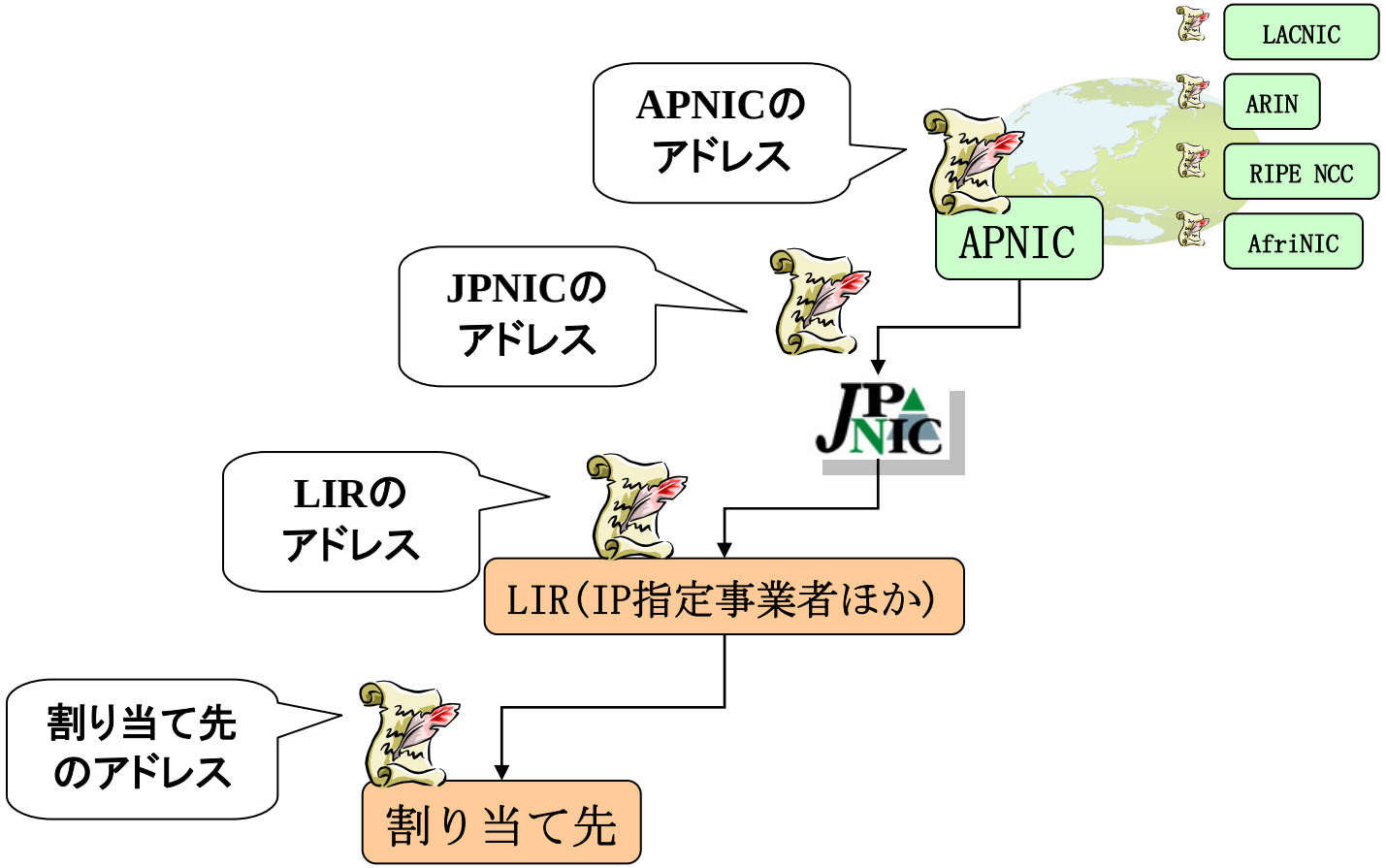
- RIRで準備が進められている、「リソース証明書」を提供する仕組み



リソースPKIのイメージ

リソース証明書とは

- IPアドレスやAS番号の利用権利を証明する電子証明書

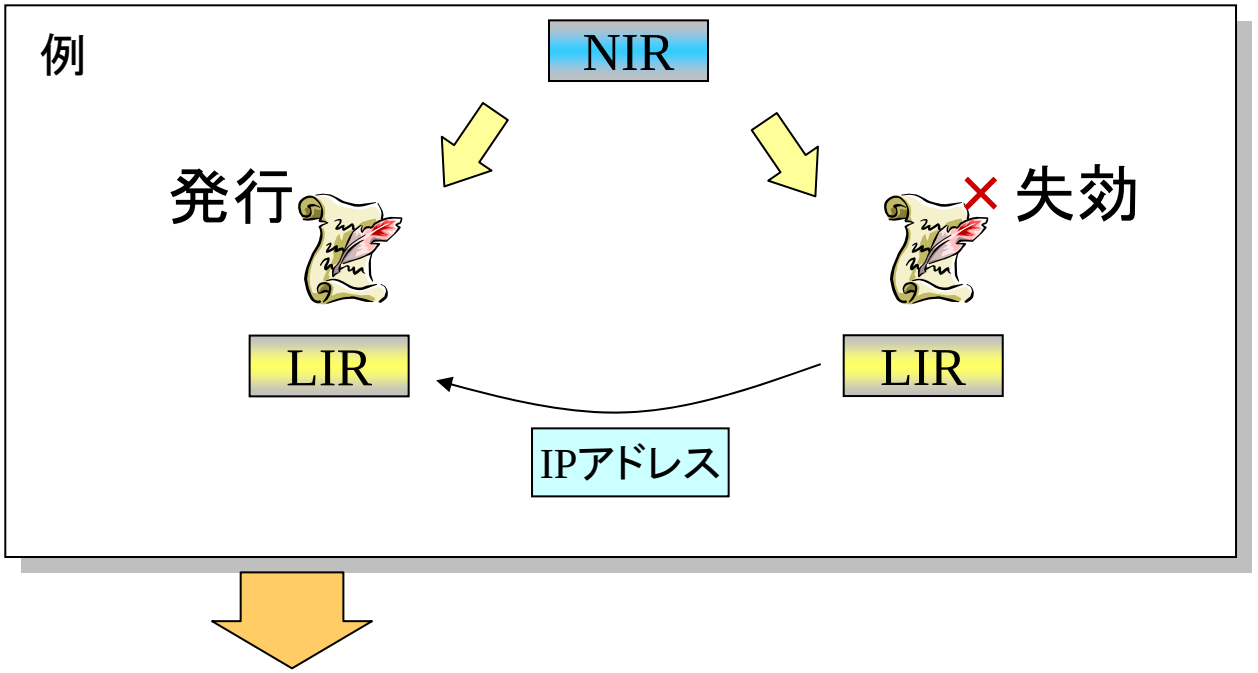


リソース証明書の用途

- アドレス資源の利用権利を証明する仕組み
- ルーティングセキュリティ

JPNIC

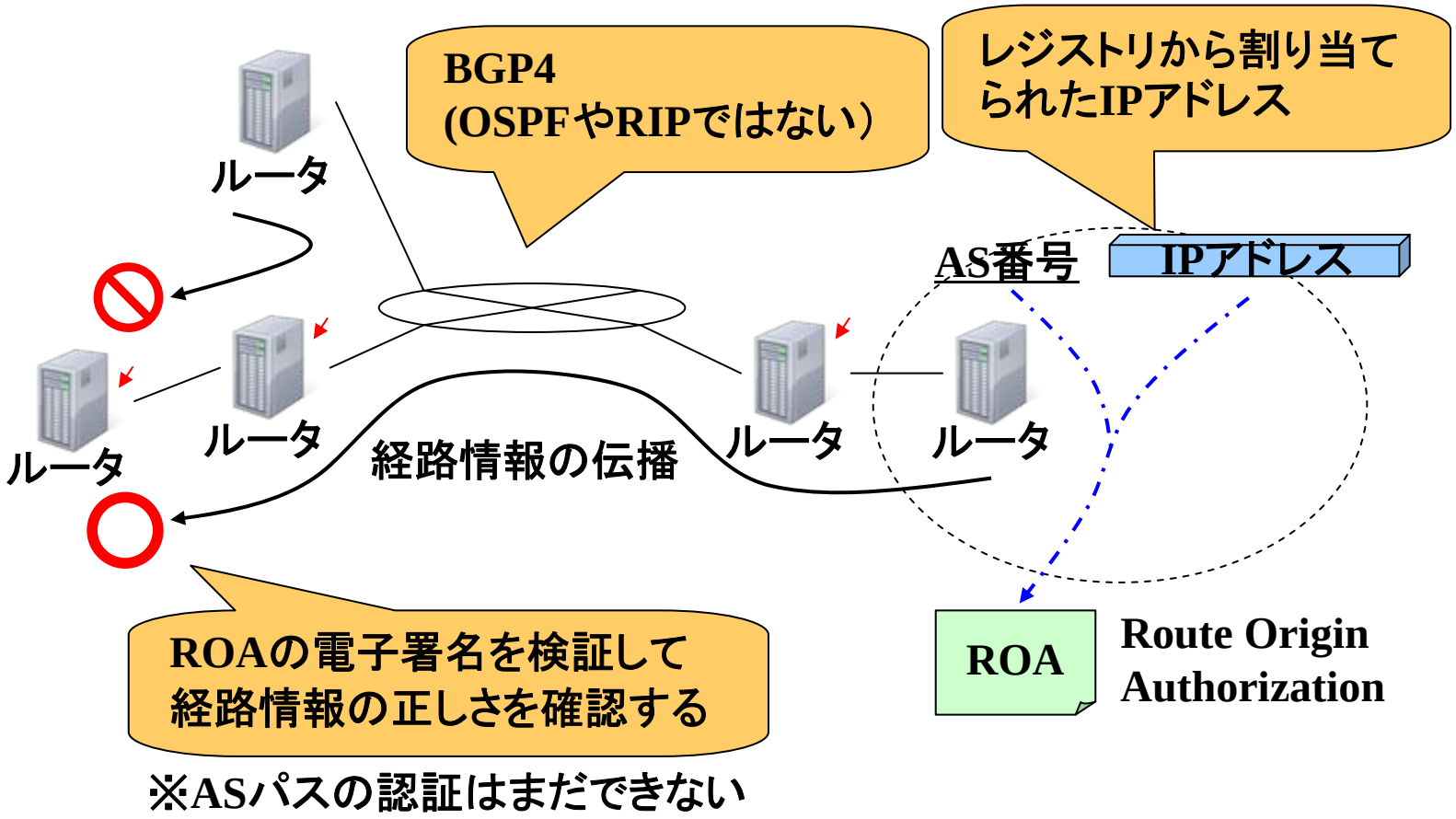
アドレス資源の利用権利の証明



Whoisを使うのと同じように、IPアドレスの利用権利を確認できる

※あるIPアドレスが正しく割り振られたものであるかどうかを電子署名を使って検証できる

ルーティングセキュリティ



アップデート

RPKIの国際動向

- RIRにおける実装と提供状況

	APNIC	RIPE NCC	ARIN	LACNIC	AfriNIC
RPKI実装	○あり	○あり	○あり (RIPE NCC コード?)	○あり	△準備中 (APNIC)
提供状況	メンバーに実験提供中 2008年9月	メンバーに実験提供中 2008年9月	メンバーに実験提供中 2009年7月	メンバーに実験提供中 2010年5月	2011年1月に実験提供の見込み

- 実装
  - APNIC
  - ISC RPKI tool
  - BBN Technologies
  - RIPE NCC Validator
- IETF SIDR WGの最近の話題
  - RPKI/Router protocol
  - CA Keyrollover
  - Ghost Busters

RPKI testbed

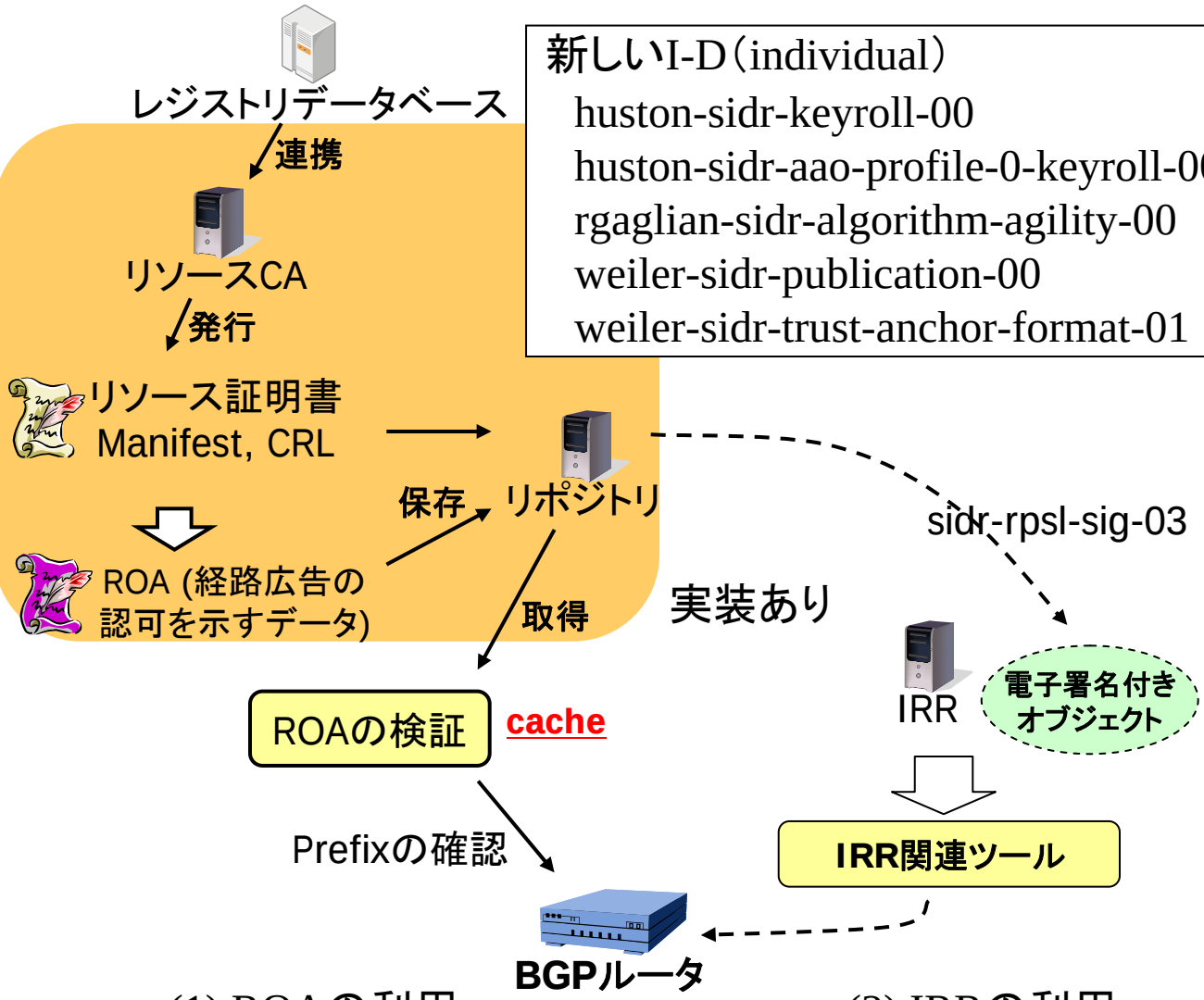
- 第79回IETF会場（北京）で行われた接続実験
  - 日時：2010年11月6日（土） 10時～会期中
  - 場所：ターミナルルーム
  - 参加：APNIC, ISC, BBN Technologies, RIPE NCC, JPNIC, IIJ 他
  - 実施内容：
    - 実験用のRIRのリソースCA稼動
    - リポジトリからのリソース証明書等の収集／検証
    - JPNICのリソースCA稼動／国内LIRのCA稼動
  - 状況
    - JPNICの実験ではISC RPKI toolを使用
    - ISC RPKI toolは開発が進行中でドキュメントよりもコード読み

プロトコル策定と実装の状況

SIDR WG関連の
ドキュメント

- sidr-arch-11
- sidr-res-cert-20
- sidr-cp-15
- sidr-ta-06
- sidr-repos-struct-06
- sidr-rescerts-provisioning-09
- sidr-rpki-manifest-09
- sidr-rpki-rtr-03
- sidr-roa-format-09
- sidr-roa-validation-10
- sidr-pfx-validate-00
- sidr-usecases-00

新しいI-D（individual）
- huston-sidr-keyroll-00
- huston-sidr-aao-profile-0-keyroll-00
- rgaglian-sidr-algorithm-agility-00
- weiler-sidr-publication-00
- weiler-sidr-trust-anchor-format-01



まとめ

- RIRにおけるリソースPKIの整備状況
  - 2011年1月には5つのRIRが実験提供の見込み
- リソースPKIに関連する実装の動向
  - RIPE NCC、APNICの他にBBN TechnologiesやISCの実装が出てきた
- プロトコルの策定動向
  - BGPルータにおけるリソースPKIの利用技術策定が進んでいる

参考文献

- “APNIC - Resource Public Key Infrastructure”, APNIC, http://www.apnic.net/services/services-apnic-provides/resource-certification/RPKI
- “RIPE NCC Resource Certification”, RIPE NCC, http://www.ripe.net/certification/
- “ARIN RPKI”, ARIN, https://www.arin.net/resources/rpki.html
- “Resolucion Inversa / DNS – Services de Registro – LACNIC”, LACNIC, http://lacnic.net/sp/rpki/
- “Secure Inter-Domain Routing (sidr)”, IETF, http://datatracker.ietf.org/wg/sidr/