リソースPKI（RPKI）の動向

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

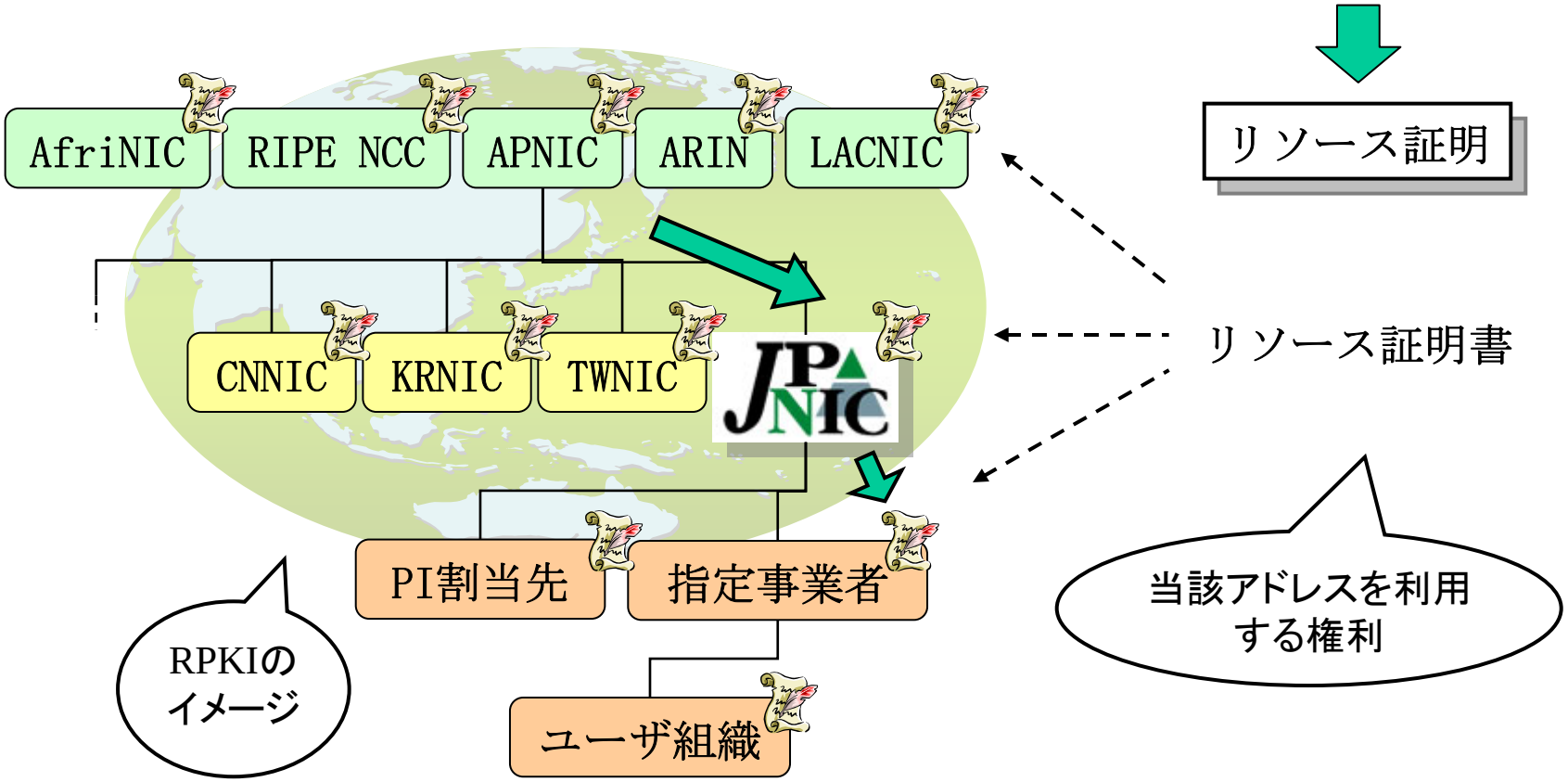
内容

- IETFやRIR（Regional Internet Registry）のリソースPKIの整備状況ほか
- 日本におけるRPKIについて
- RPKIとJPNICの活動の位置づけ

1、RPKIの国際動向

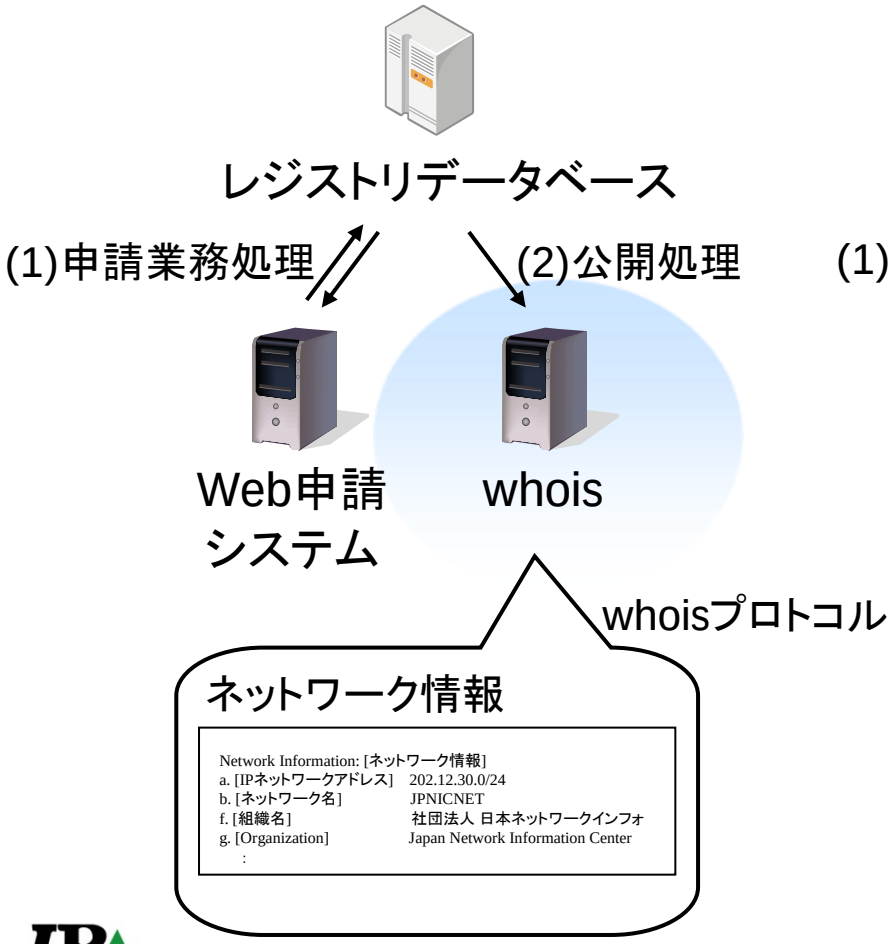
RPKI

「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。

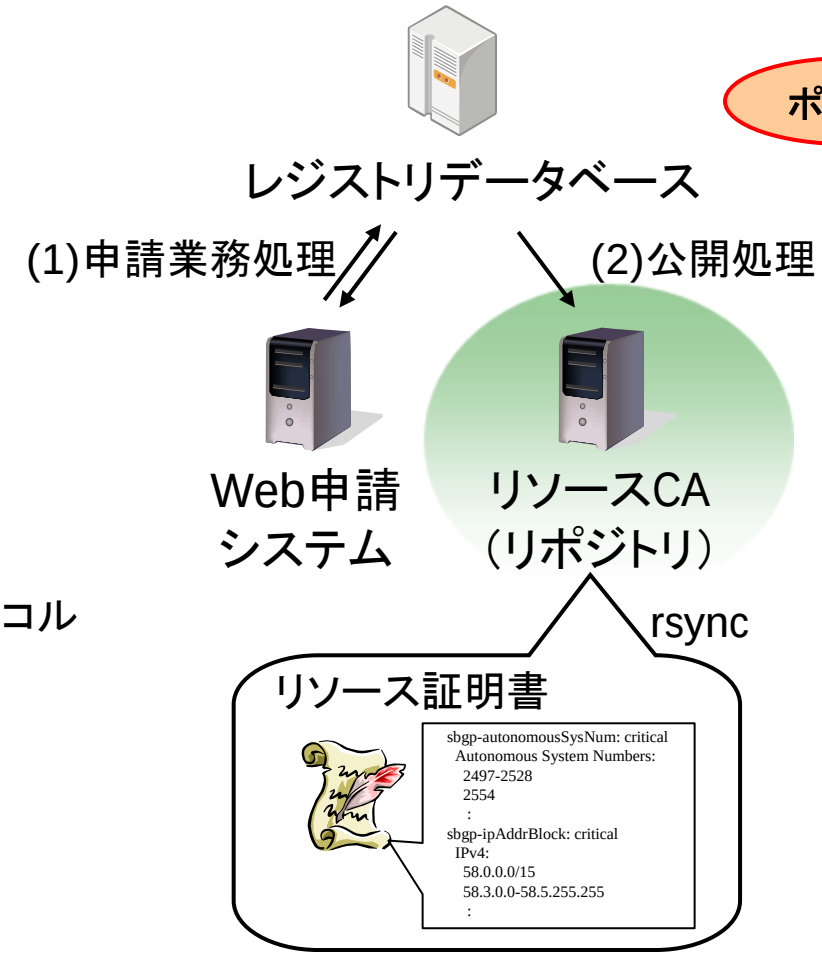


リソース証明書

■IPアドレス管理業務



■リソース証明書

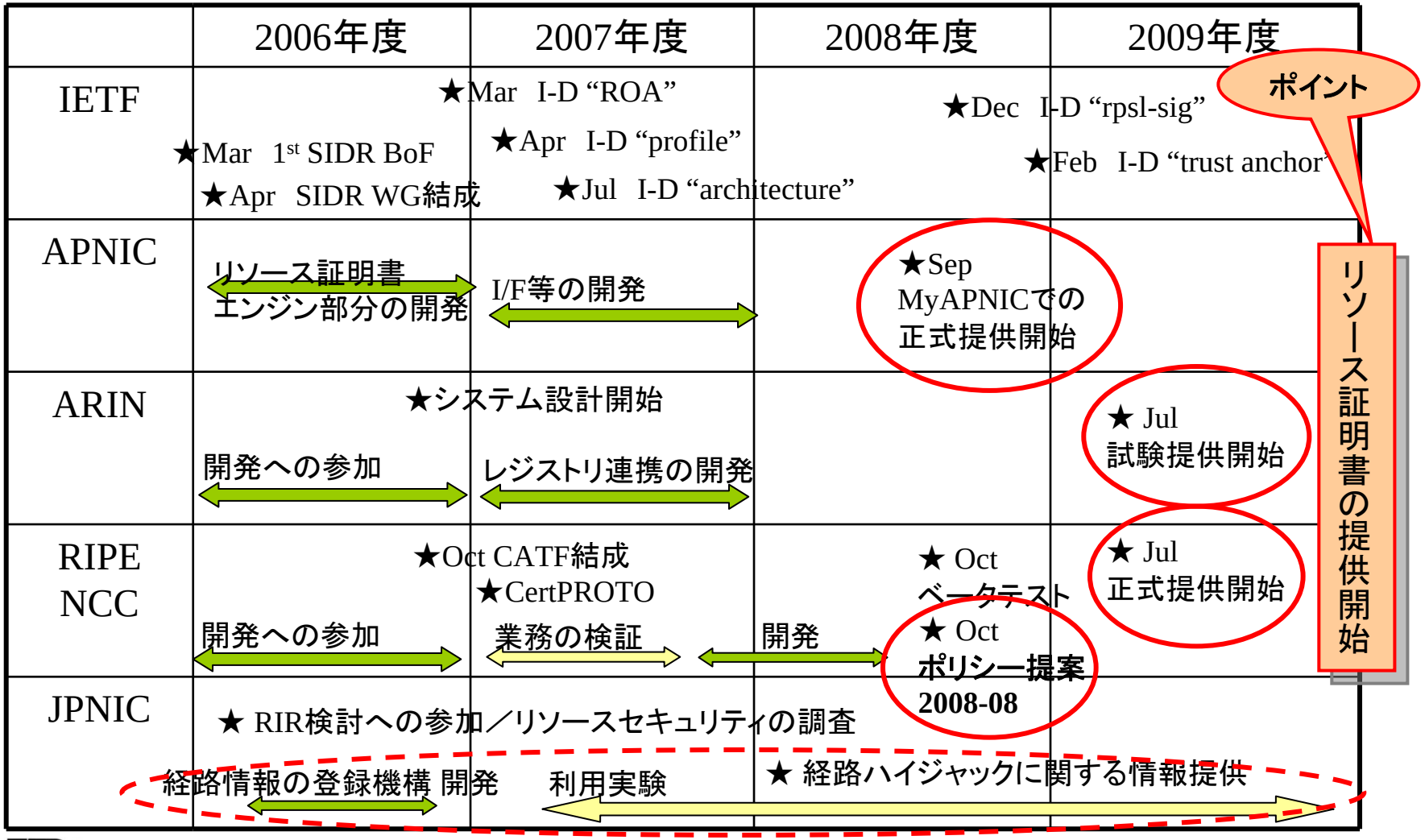


ポイント

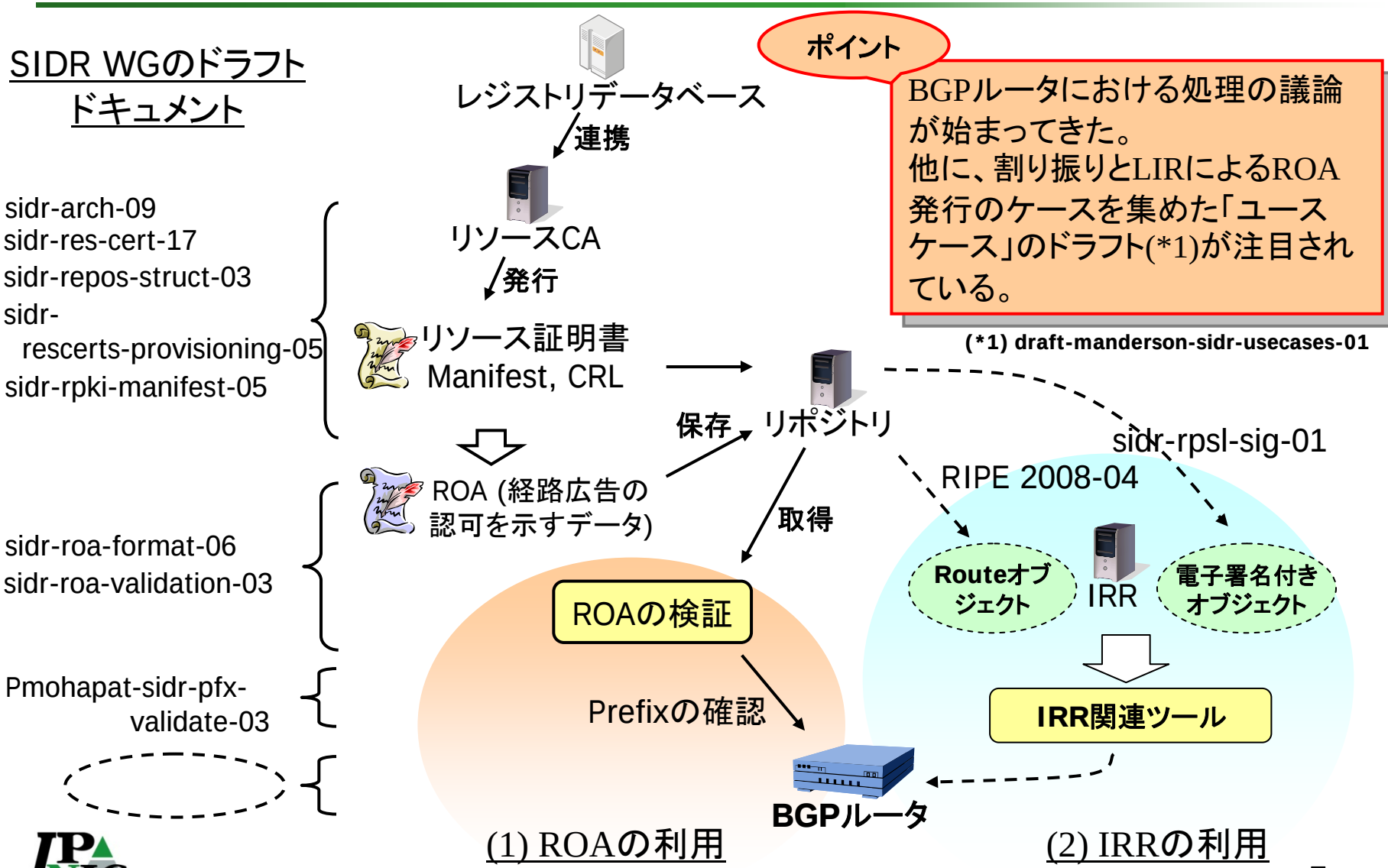
リソース証明書が割振られたIPアドレスであることを示す

時系列

★2004th Jun RFC3779



IETF等における標準化動向



2、日本におけるRPKIについて

質問(1/2)

- JPNICもリソース証明書を提供すべき？

  もし提供されるならば…

  - 実験であっても、実際の割り振り情報に基づいたリソース証明書を提供すべき？
  - リソース証明書関連のツールや情報も提供すべき？
  - 試験サービスであれば秘密鍵はJPNICのシステムに保存されていてもよい？（RIRの試験サービスのように）

質問(2/2)

- リソース証明書の使い道は？
  - 正しく割り振られたIPアドレスであることを証明するために使う(「移転」のためには必須？)
  - BGPの接続業務の際に正しいIPアドレスであることを確認するために使う(RIPE NCCのアイディア)
  - BGPルータ等で利用し、セキュアなルーティングに役立てるために使う(RPKIアーキテクチャ)

３、RPKIとJPNICの活動の位置づけ

RPKIとJPNICの活動の位置づけ

ポイント

RPKIは基本的に情報提供段階での信頼性向上に寄与

IPレジストリシステム
－電子証明書を用いた認証
経路情報の登録認可機構
－電子証明書を用いた認証

JPIRR／リソース証明書／ROA
－経路ハイジャック通知
－（調査中）リソース証明書／ROA

a.登録段階の信頼性向上

b.データ保持段階の信頼性向上

c.提供段階の信頼性向上

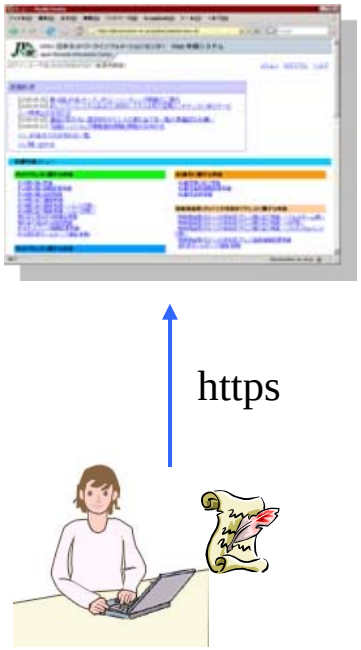
JPIRRガーベージコレクター／
経路情報の登録認可機構
－データベースの正しさの担保

指定事業者／
割り振り先組織

ルーティング
オペレーター

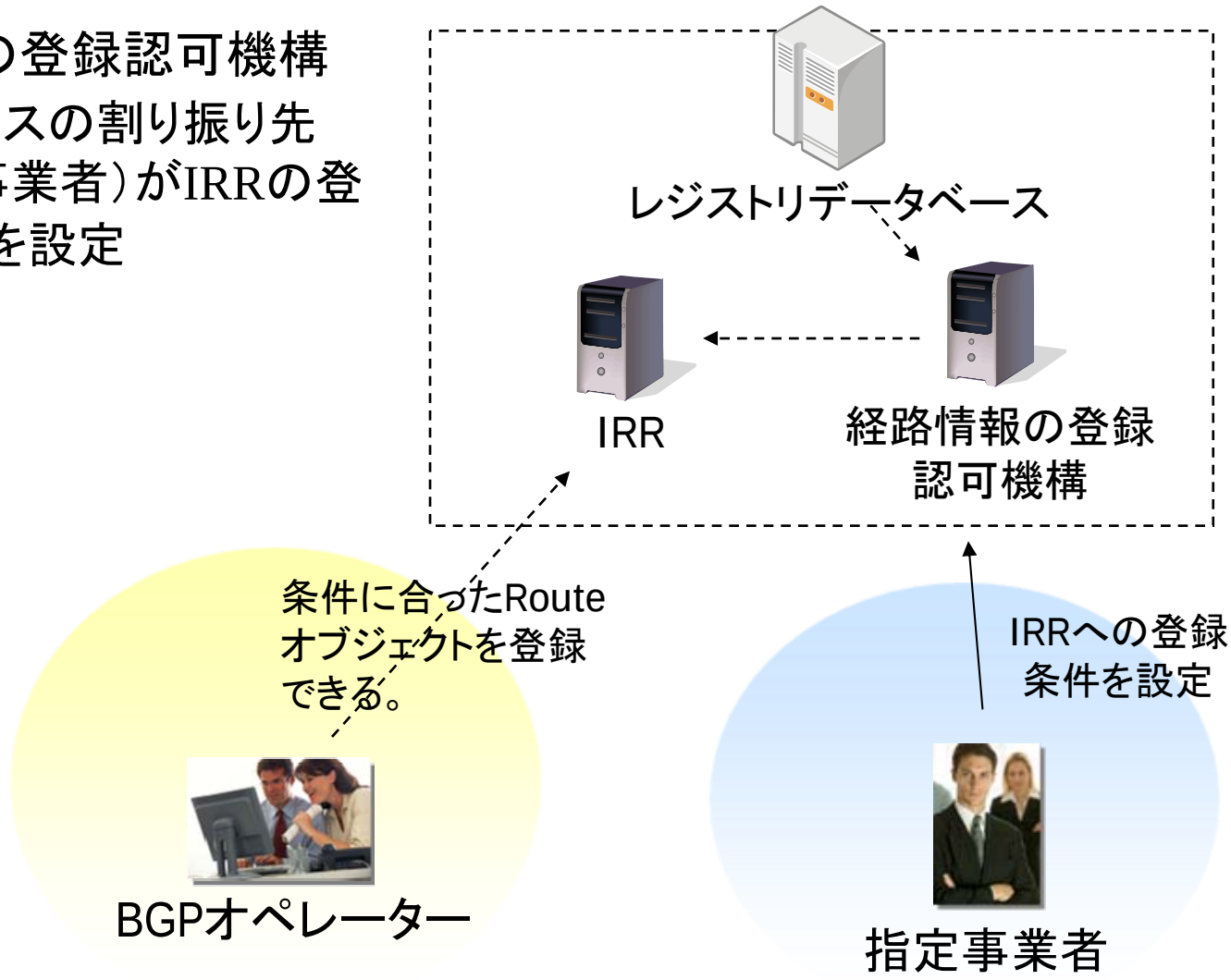
JPNICの活動の位置づけ(1)

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



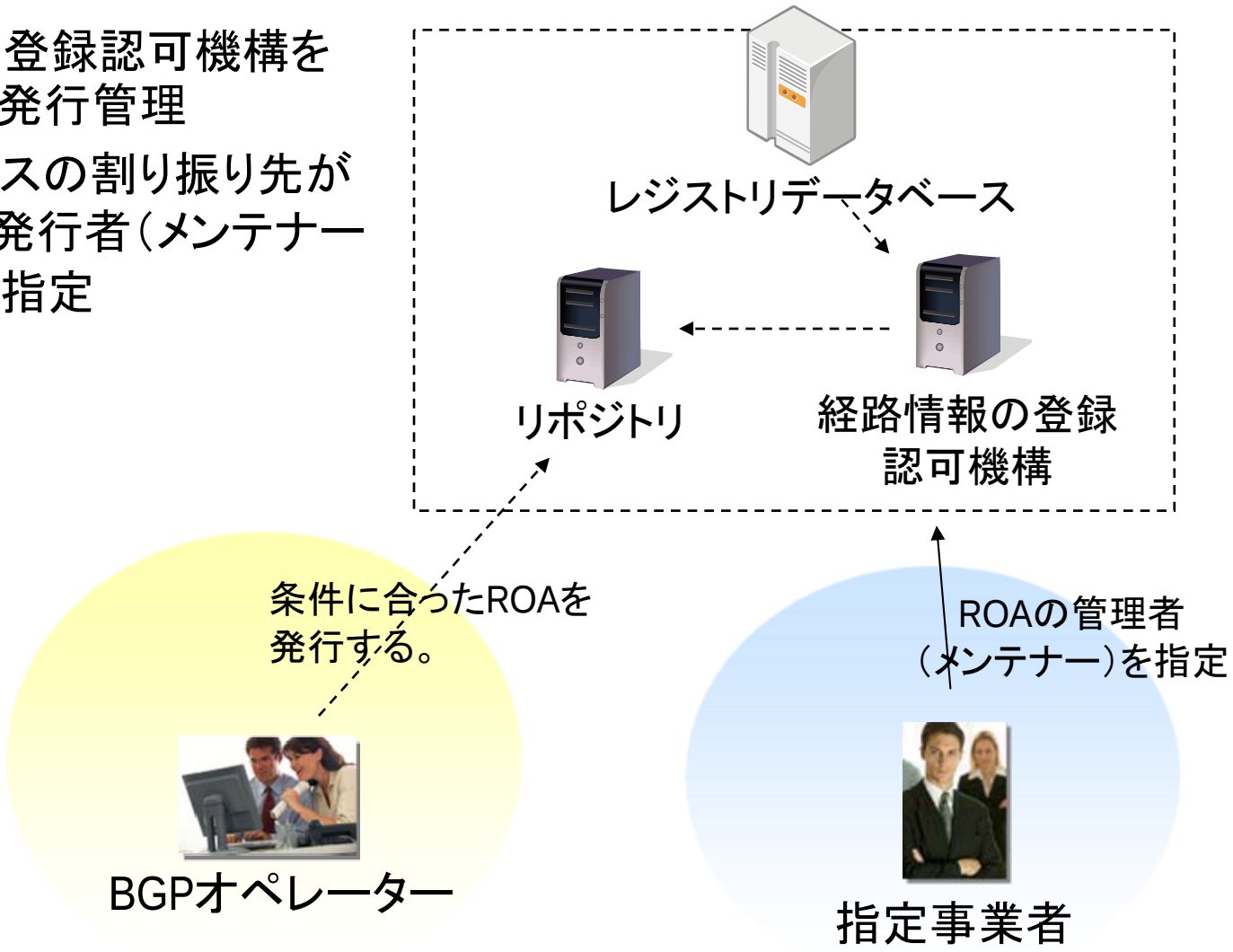
JPNICの活動の位置づけ(2)

- 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の登録条件を設定



おまけ：ROA管理システムの一案

- 経路情報の登録認可機構を使ったROA発行管理
  - IPアドレスの割り振り先がROAの発行者（メンテナー名等）を指定



まとめ

- 国際的なリソースPKIの整備状況
  - RIRでは提供が開始（試験を含む）
  - IETFではルータでの利用の議論が始まる
- 日本におけるRPKIについて
  - JPNICでもリソース証明書を提供すべきか
- JPNICの活動の位置づけ
  - 信頼性向上
    - 登録段階／データ保持段階／提供段階
    - 登録段階におけるユーザ認証のための資源管理カード

おわり