

# リソースPKI(RPKI)の動向

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

---

- 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

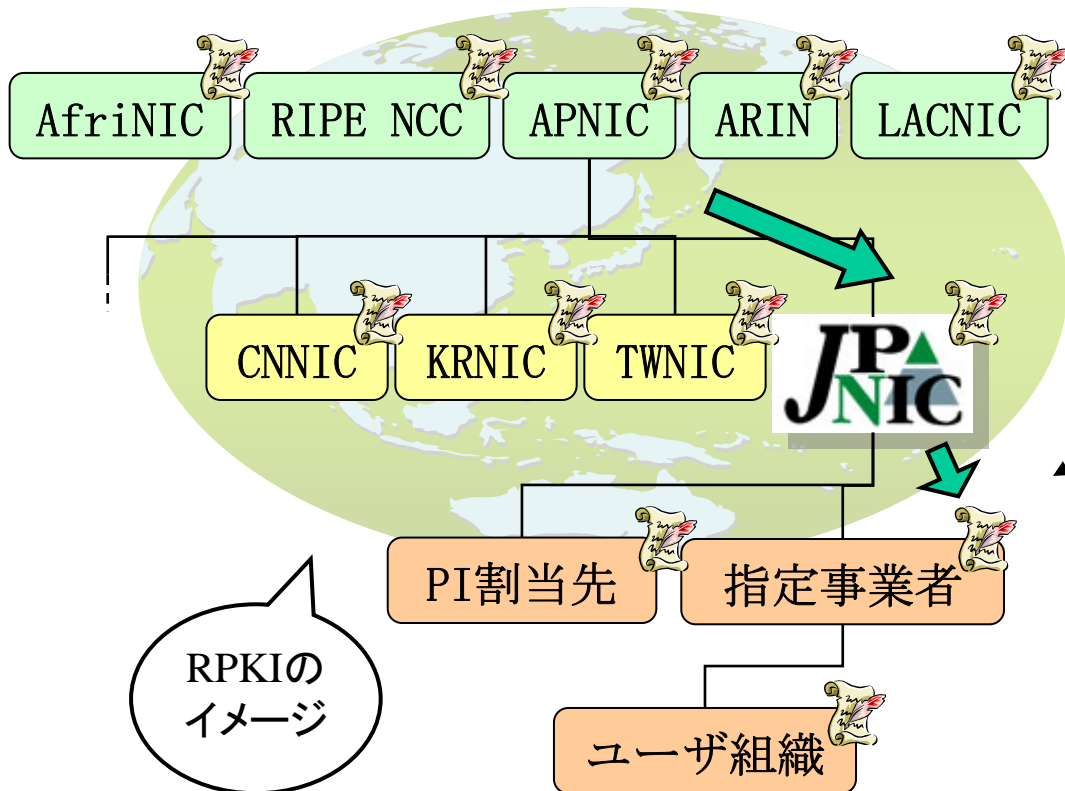
# RPKI

「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



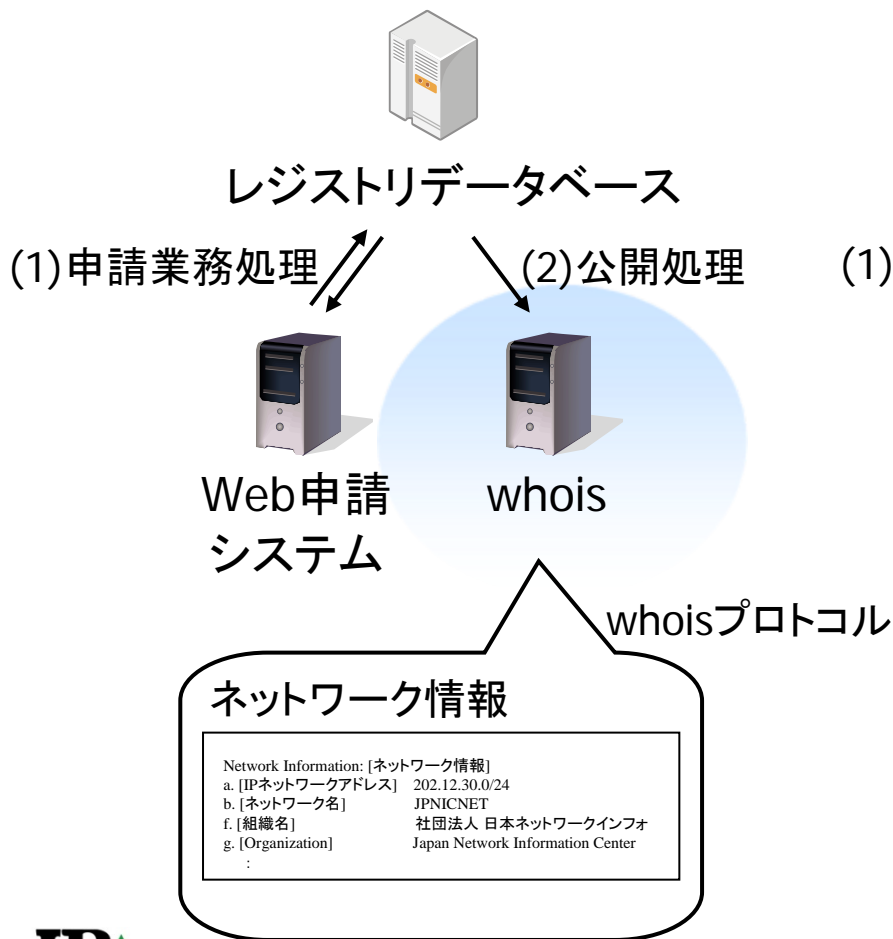
リソース証明書

当該アドレスを利用する権利

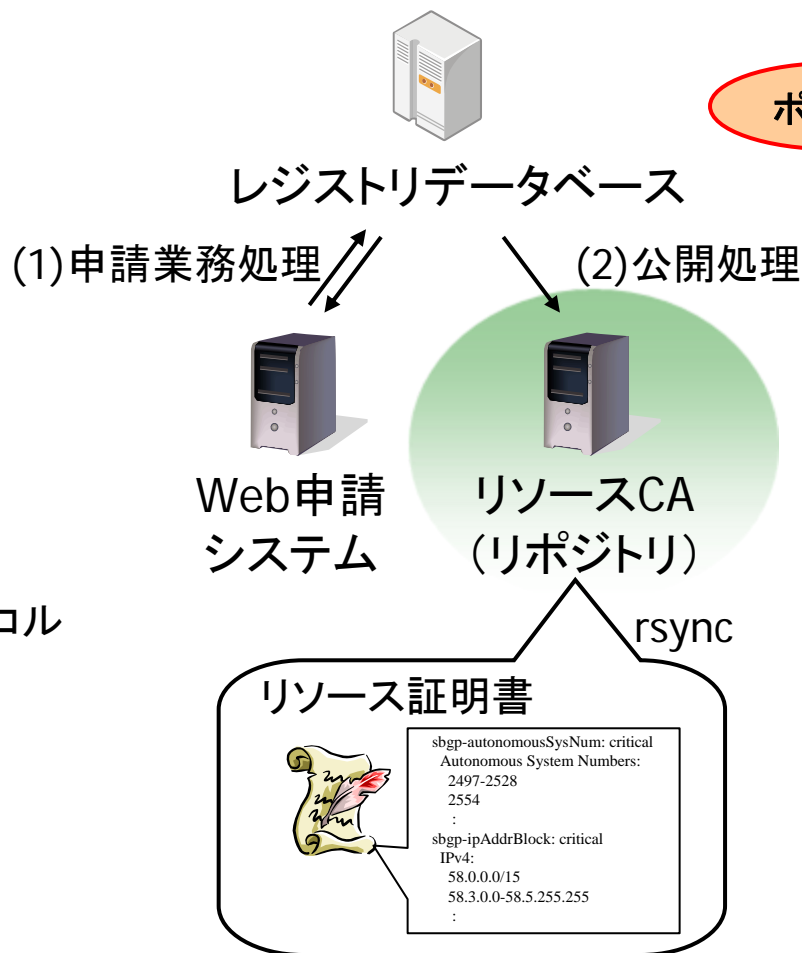
RPKIのイメージ

# 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

★2004<sup>th</sup> Jun RFC3779

	2006年度	2007年度	2008年度	2009年度
IETF	<ul style="list-style-type: none"> <li>★Mar 1<sup>st</sup> SIDR BoF</li> <li>★Apr SIDR WG結成</li> </ul>	<ul style="list-style-type: none"> <li>★Mar I-D “ROA”</li> <li>★Apr I-D “profile”</li> <li>★Jul I-D “architecture”</li> </ul>	<ul style="list-style-type: none"> <li>★Dec I-D “rpsl-sig”</li> </ul>	<ul style="list-style-type: none"> <li>★Feb I-D “trust anchor”</li> </ul>
APNIC	<ul style="list-style-type: none"> <li>リソース証明書エンジン部分の開発</li> </ul>	<ul style="list-style-type: none"> <li>I/F等の開発</li> </ul>	<ul style="list-style-type: none"> <li>★Sep MyAPNICでの正式提供開始</li> </ul>	
ARIN	<ul style="list-style-type: none"> <li>開発への参加</li> </ul>	<ul style="list-style-type: none"> <li>★システム設計開始</li> <li>レジストリ連携の開発</li> </ul>		<ul style="list-style-type: none"> <li>★Jul 試験提供開始</li> </ul>
RIPE NCC	<ul style="list-style-type: none"> <li>開発への参加</li> </ul>	<ul style="list-style-type: none"> <li>★Oct CATF結成</li> <li>★CertPROTO</li> <li>業務の検証</li> </ul>	<ul style="list-style-type: none"> <li>★Oct ベータテスト</li> <li>★Oct ポリシー提案</li> </ul>	<ul style="list-style-type: none"> <li>★Jul 正式提供開始</li> </ul>
JPNIC	<ul style="list-style-type: none"> <li>★RIR検討への参加</li> </ul>	<ul style="list-style-type: none"> <li>リソースセキュリティの調査</li> </ul>	<ul style="list-style-type: none"> <li>★経路ハイジャックに関する情報提供</li> </ul>	

ポイント

リソース証明書の提供開始

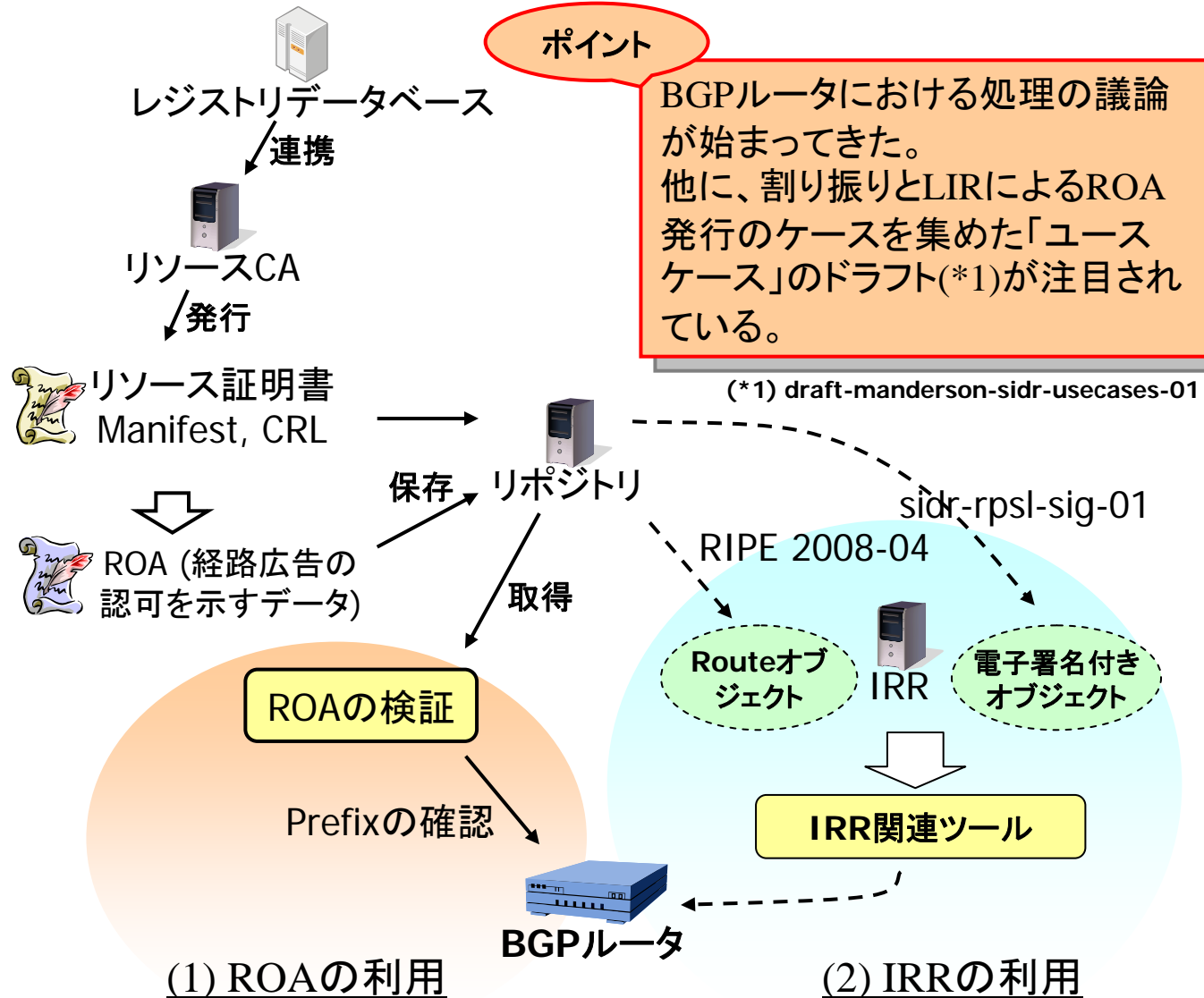
# IETF等における標準化動向

## SIDR WGのドラフト ドキュメント

sidr-arch-09  
sidr-res-cert-17  
sidr-repos-struct-03  
sidr-  
rescerts-provisioning-05  
sidr-rpki-manifest-05

sidr-roa-format-06  
sidr-roa-validation-03

Pmohapat-sidr-pfx-  
validate-03



## 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)

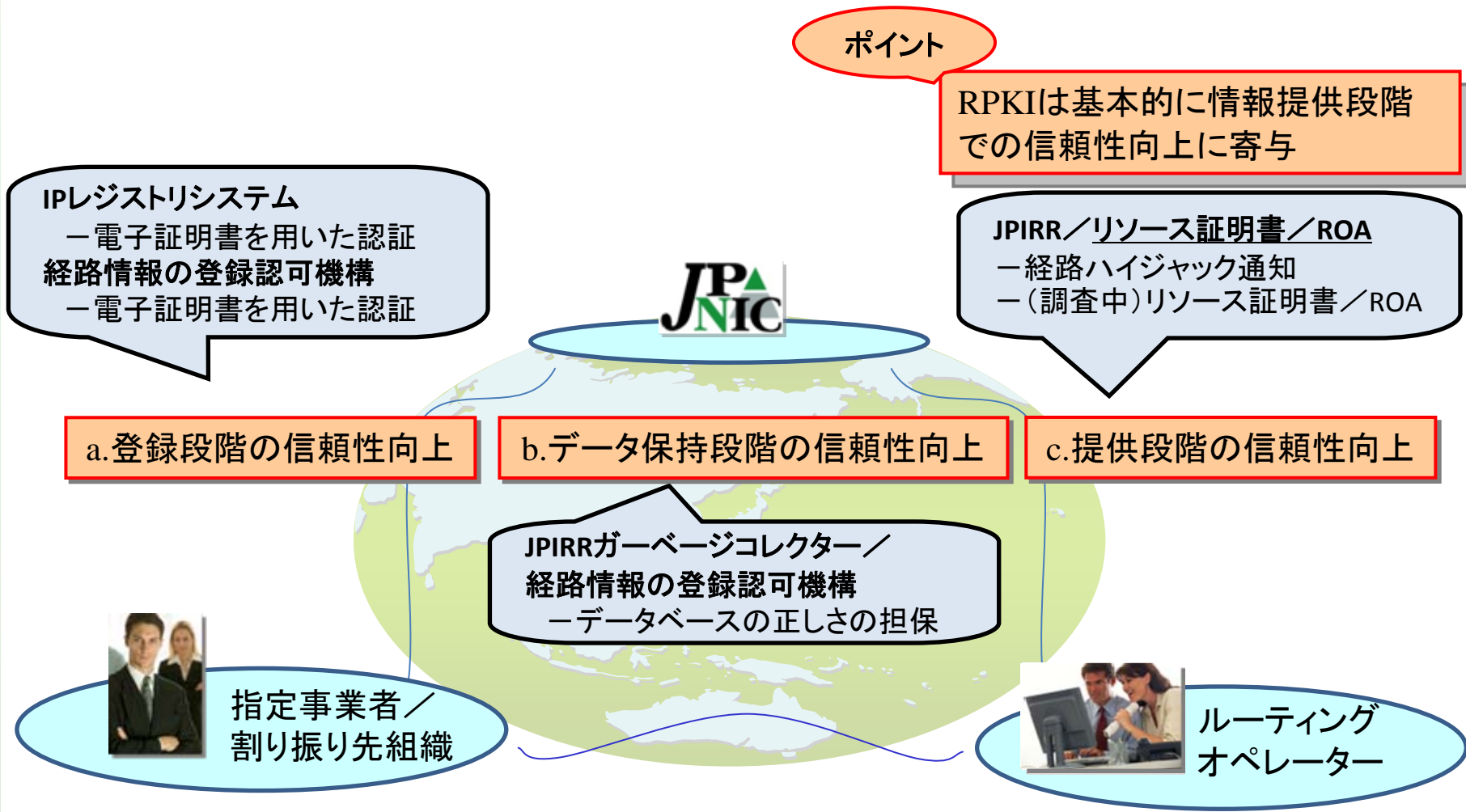
# 質問(2/2)

---

- 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



# 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。

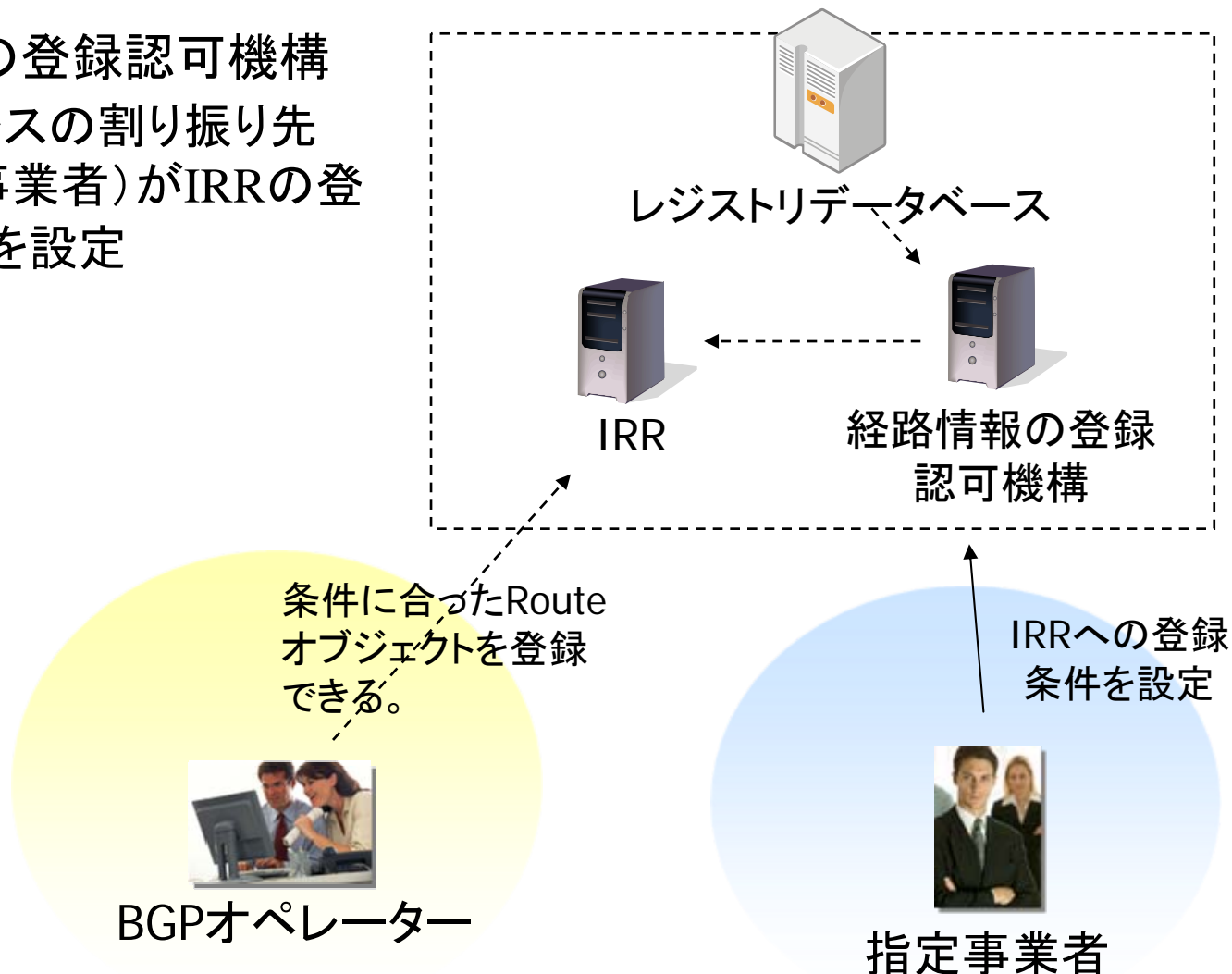


↑  
https



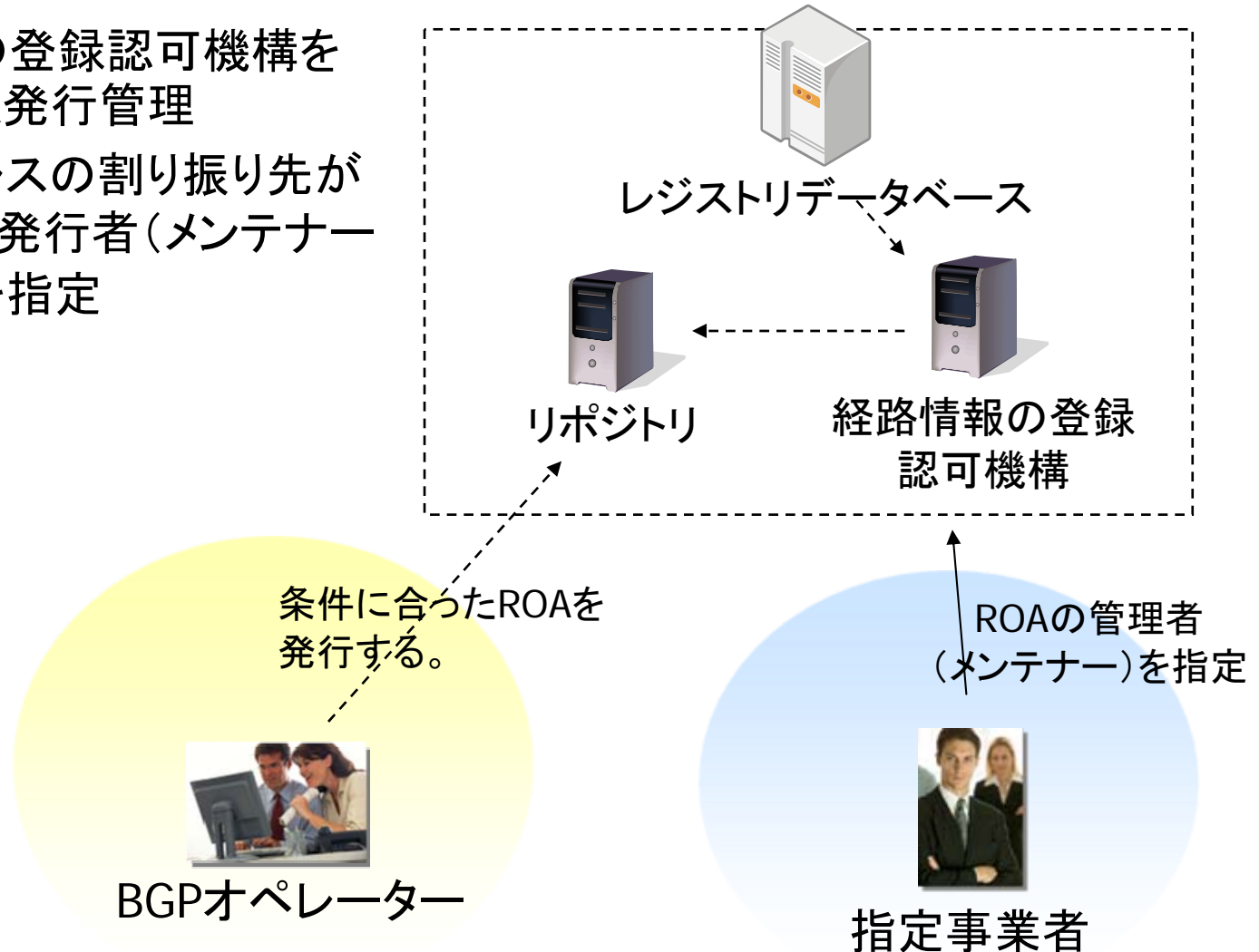
# JPNICの活動の位置づけ(2)

- 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