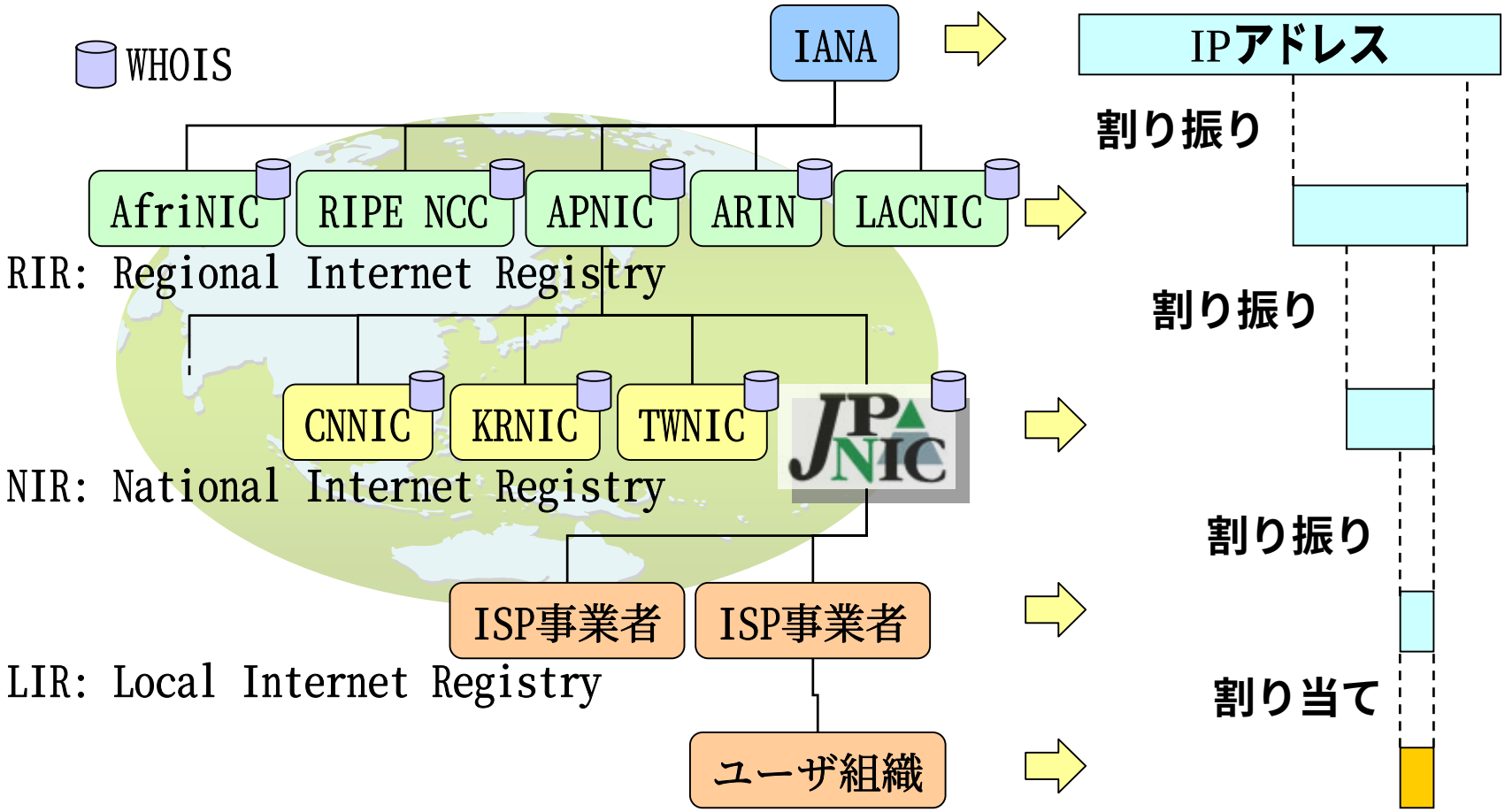
# IPアドレスの使用権を示すリソース証明書の動向

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
セキュリティ事業担当　木村泰司

# 概要

- IPアドレスの管理体系と枯渇問題
- リソース証明書とは
- リソース証明書の適用に関する取り組み状況
- 相互運用性の維持を目指す活動

# インターネットレジストリのツリー構造




IPアドレスの一意性を保証し経路制御の適応性を向上させる仕組み

# IPv4アドレスの枯渇と課題

- IPv4アドレスの枯渇予測状況
  - APNIC Geoff Huston氏による予測（6/13現在）
    - 2010年2月　IANAプールの枯渇
    - 2010年9月　RIRプールの枯渇
- 予測される現象
  - セカンド市場の登場
  - 登録されていないIPアドレスの利用が増加

# IPv4アドレスの枯渇と課題

- 起こりうる問題
  - IPアドレスのハイジャックの増加
    - IPv4アドレスの相対的な価値向上
  - 追跡が困難な不正アクセスの増加
    - 透過性のない接続の増加 (トランスレータ、NAT等)
  - ルータにおける接続性の低下
    - ルーティングテーブルの増大
- 重要性の高まり
  - アドレス割り振りの証拠
  - ルーティングの安全性向上、性能維持

# RIRとJPNICの取り組み

| | APNIC | ARIN | RIPE NCC | JPNIC |
|---|---|---|---|---|
| 認証局の構築 | 運用中 | 運用中 | 運用中 | (実験)<br>運用中 |
| “X.509”認証の導入 | ○ | ○ | ○<br>(登録も可能) | (導入実験)<br>○ |
| リソース証明書の取り組み | 2006年度に開発プロジェクト | APNICの開発に参加、2007年度に内部プロトタイプ開発 | APNICの開発に参加、業務検討開始 | ROAに向けたデータベースの準備 (システム開発) |

- 認証局の構築と認証強化 (認証方式の変更)
  - crypto-pw、mail-from等から“X.509”認証への移行
  - リソース証明書 (利用権限を証明する証明書) の開発プロジェクト

# リソース証明書の概要

IPアドレス・AS番号の利用権を示す電子証明書

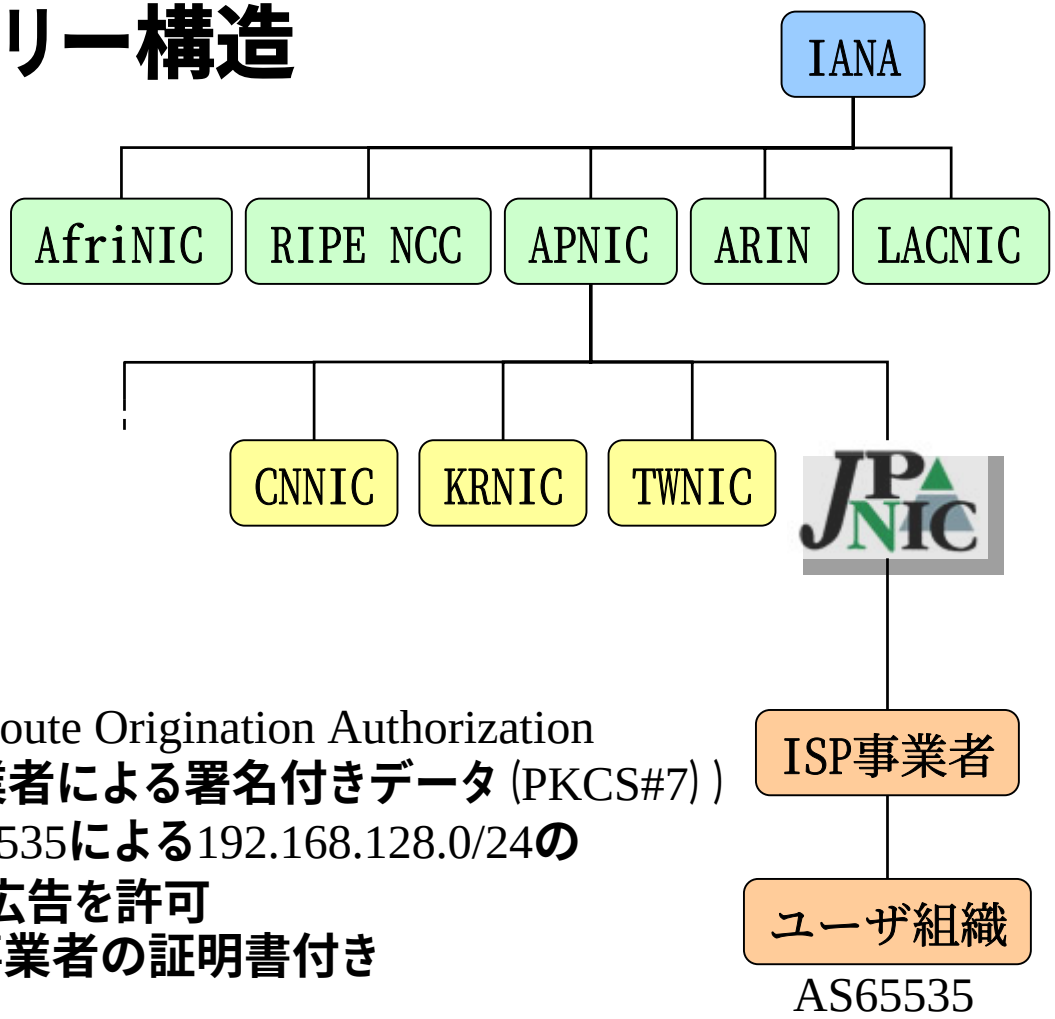
JPNIC 社団法人 日本ネットワークインフォメーションセンター

# リソース証明書とは（1）

- PKIX（Public-Key Infrastructure – X.509）WG
  - RFC3779
    - X.509 Extensions for IP Addresses and AS Identifiers
      - Jun 2004, C. Lynn, S. Kent, K. Seo
- SIDR（Secure Inter-Domain Routing）WG
  - draft-ietf-sidr-res-certs-06.txt
    - A Profile for X.509 PKIX Resource Certificates
  - draft-ietf-sidr-cp-01.txt
    - Certificate Policy (CP) for the Internet IP Address and AS Number (PKI)
  - draft-ietf-sidr-roa-format-00.txt
    - A Profile for Route Origin Authorizations (ROA)
  - draft-ietf-sidr-arch-00.txt
    - An Infrastructure to Support Secure Internet Routing
  - **他、CPSのテンプレートなど**

# リソース証明書とは（2）

- **ツリー構造**




**発行元**：APNIC
**対象**：JPNIC
**アドレスブロック**：
192.168.0.0/16

**発行元**：JPNIC
**対象**：ISP事業者
**アドレスブロック**：
192.168.128.0/24

**発行元**：ISP事業者
**対象**：**ユーザ組織**
**アドレスブロック**：
192.168.128.0/24

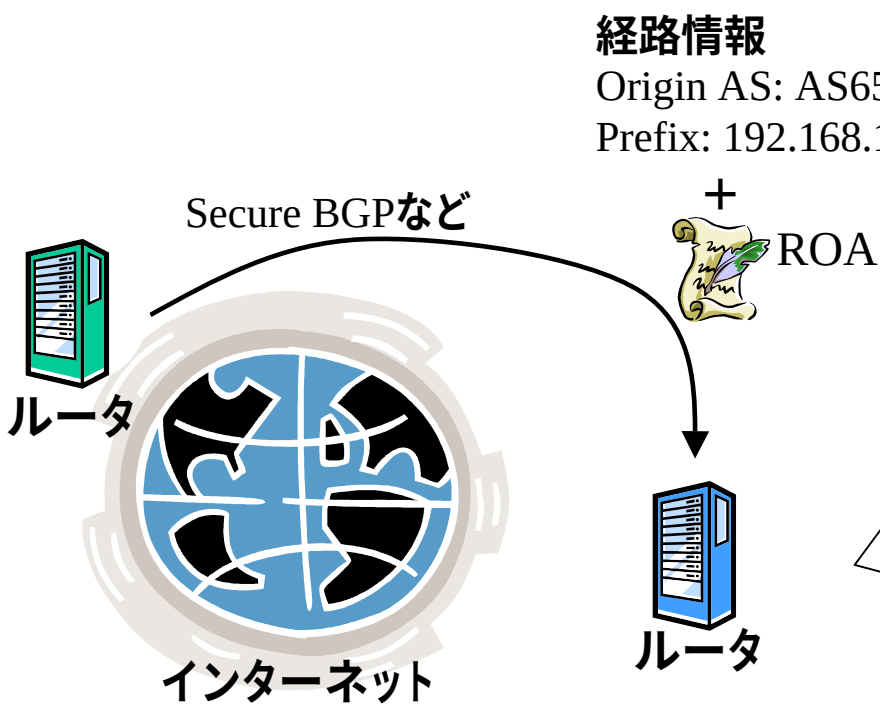
ROA – Route Origination Authorization
（**ISP事業者による署名付きデータ**（PKCS#7））

- AS65535**による**192.168.128.0/24**の経路広告を許可**
- ISP**事業者の証明書付き**

# リソース証明書とは（3）

Version: 3
Serial: 111111
Issuer: CN=JPNIC
Not Before: Mon Jan 1 00:00:00 2007 GMT
Bot After: Tue Jan 1 00:00:00 2008 GMT
Subject: CN=ISP, E=resourcecerts@isp.jp
Subject Key Identifier: SSS-SSS
Subject Info Access: caRepository -
rsync://repository.nic.ad.jp/jpnic-isp/AAA-AAA/SSS-SSS
Key Usage: DigitalSignature, nonRepudiation
CRL Distribution Points:
rsync://repository.nic.ad.jp/jpnic-isp/AAA-AAA.crl
Authority Info Access: caIssuers -
rsync://repository.nic.ad.jp/jpnic-isp/AAA-AAA.cer
Authority Key Identifier:
Key Identifier: AAA-AAA
Certificate Policies: 1.2.392.200175.1.4.1
IPv4: 192.168.128.0-192.168.128.255

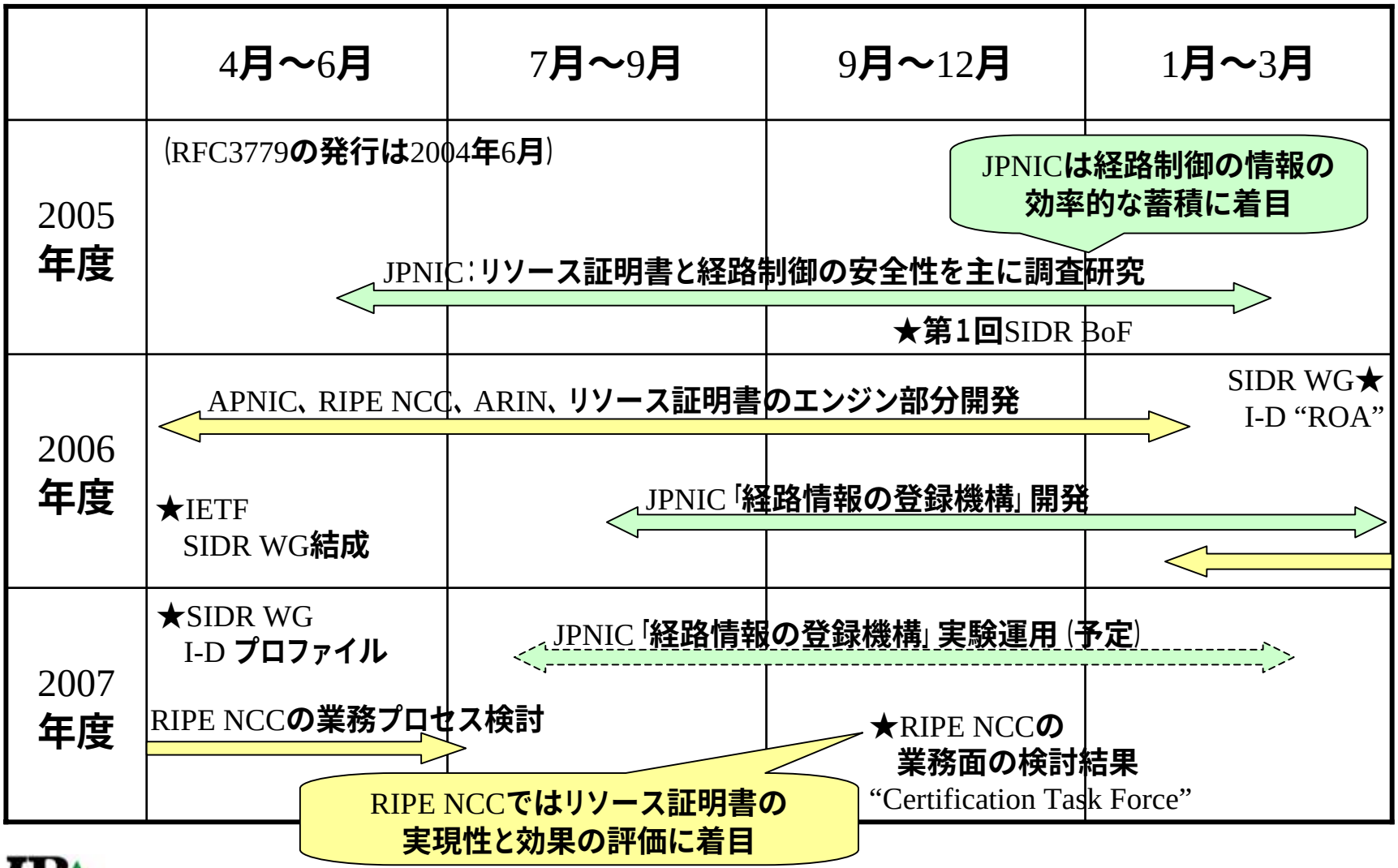
# リソース証明書とは（4）




**ROAとリソース証明書の検証**

a. ROAの署名検証
b. リソース証明書の検証
- パス構築
- パス検証
  - IPアドレスの範囲
    - 192.168.128.0/24
    - 192.168.128.0/24
    - 192.168.0.0/16
    - …

# RIRとJPNICの取り組み状況

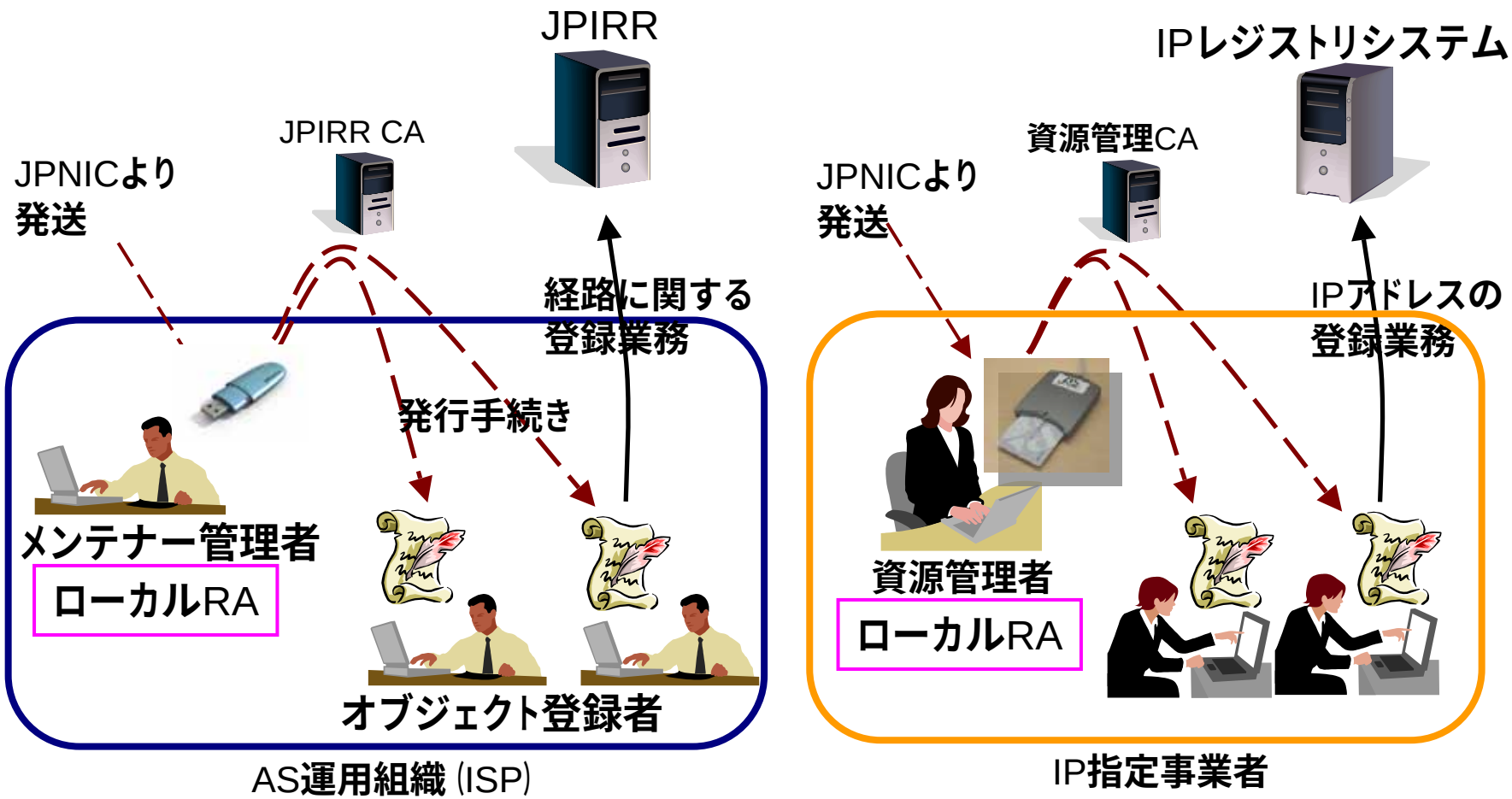


# RIPE NCCにおける業務面の検討

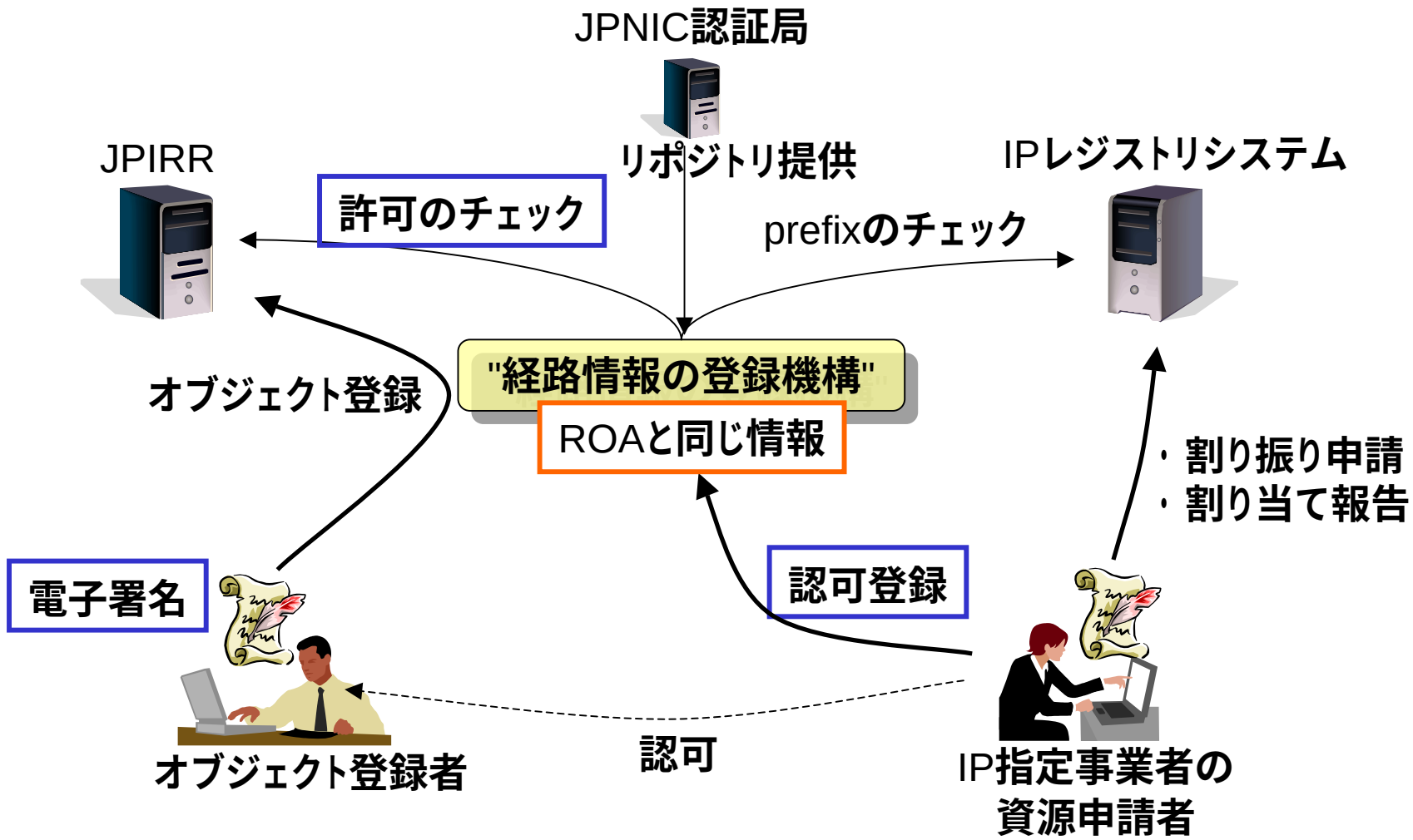
- RIPE NCC Certification Task Force
  - 第５３回RIPEミーティングのときに結成（LIRより6名）
    - 第５４回および第５５回RIPEミーティングで成果を報告。
  - 目的
    - 開発状況に応じて（LIRの）オペレーターへの周知を図る
    - 影響に関するアドバイスを行う
      - 運用手順、サービス機能
      - 認証モデルの最適化
      - ポリシーの検討
      - LIRとRIPE NCCの関係検討
    - 本開発を行う際に要件の提供を行う
- CertProto
  - RIPE NCCの関係部署からメンバーを集め、様々な観点でリソース証明書システムの理解を図るプロジェクト。Task Forceを補助する役割も持つ。
  - 活動期間：2007年1月～2007年6月（このときに継続の判断を行う）
  - 活動内容
    - 最低限のプロトタイプシステムを導入
    - 業務手順を検討
    - 課題を列挙、要件事項をまとめ

# JPNICにおける業務面の取り組み (1)

- **ローカルRA (External RA) モデルを使った認証強化**



# JPNICにおける業務面の取り組み（2）



# 電子証明書の相互運用性のポイント

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

# リソース証明書の相互運用性

- Relying Party（RP）はルータやIPアドレス利用者
  - 国際的なpeer（AS同士のつながり）は当然存在
    - ルーターが他の地域のアドレスを使うように設定変更される可能性もある。
  - IPアドレスは、RIR間、RIR-NIR間で移管が起こりうる。

**◯リソース証明書の相互運用性を確保できるようにすることは必要条件**

# 電子証明書の相互運用性

- 書式上の相互運用性
- 意味的な相互運用性

# 書式上の相互運用性

- 書式上の相互運用性に関係する要素
  - Certificate Policy (の一部)
    - フィールド
      - 拡張フィールドの種類
      - CNに入っている値の意味
        など
    - クリティカリティ
  - リポジトリの運用状況
    - RPのアプリケーション／プロトコルの種類に応じたサービスレベル
      - リソース証明書の場合はネットワークが切れるかどうかにつながる(？)

# 意味的な相互運用性

- 保証レベル
  - 証明書における保証内容のレベル分け
    - 登録／発行の要件、秘密鍵の管理、鍵長、失効検証の内容
    - RPーCA間、CAーCA間ともに合意されたものが必要
- RPの検証手順と結果のアプリケーションに対する適用
  - 有効期限切れと失効の扱い
    - 即座に無効化／猶予期間を設ける／一部の適用
- 想定されるパス
  - トラストアンカー
    - RPが決めるものだが、セキュアなアプリケーションの普及を考えると選ばれる範囲の想定が必要
  - 中間認証局
    - 中間認証局証明書の有効性の判断材料

# 相互運用性向上に向けた活動

- JPNICで準備･検討している実験的な活動
  - 電子認証プラクティスフォーラム（仮）
    - 相互運用性向上の為にノウハウを明文化し、更新可能な状態で共有することが目的
    - MLとオフライン･フォーラム
    - PKIを含め、電子認証に関するBCPをコンセンサスベースで文書化／公開することを目指す

# 相互運用性向上に向けた活動

- BCPドキュメント例
  - ドキュメント化プロセス（フォーラム自体の運用）
  - CA証明書のロールオーバー
  - CAの標準的な構成の選択肢
  - 利用者同意内容のテンプレート
  - ある業界における標準プロファイルと保証レベル
    - 三文判PKIのような位置づけの電子証明書
  - など…

# まとめ

- リソース証明書
  - 取り組み開始時期、アドレスプリフィックスが入った証明書、ルーティングなどに利用
- 相互運用性
  - 書式上の相互運用性
  - 意味的な相互運用性

※BCPの蓄積：電子認証プラクティスフォーラム