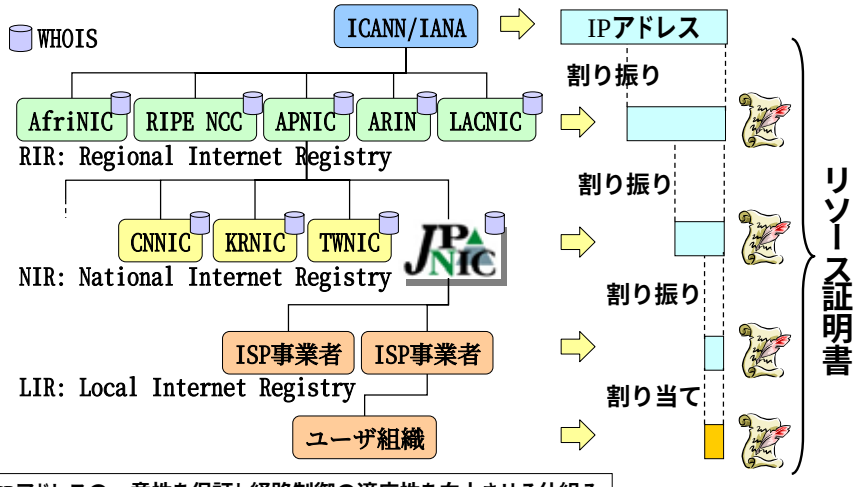
「リソース証明書」とは？

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

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

インターネットレジストリと リソース証明書



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

内容

- リソース証明書の背景
- リソース証明書とは
- 国際動向
- 電子証明書の相互運用性とは

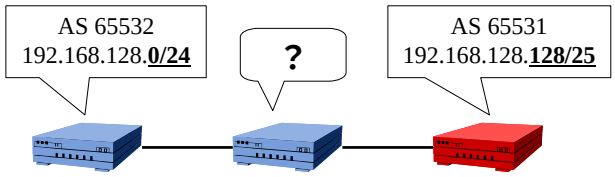
リソース証明書の背景

インターネットルーティングにおけるセキュリティと
アドレス資源の不正利用

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

リソース証明書の背景 (1)

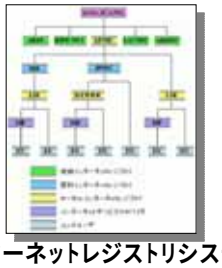
- インターネットルーティング (経路制御) におけるセキュリティ
  - **経路ハイジャック**
    - BGPでのIPアドレスやAS番号の不正利用
      (広義には不正なASパスも含む)



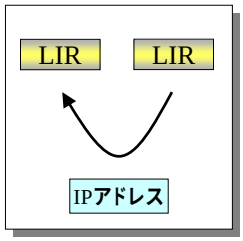
経路情報の発信元が正しいかどうかを検証することが必要

リソース証明書の背景 (2)

- IPv4アドレスの在庫枯渇期におけるセキュリティ
  - **アドレス資源の不正利用**
    - IPアドレスやAS番号の不正な利用や、利用権利の主張など



インターネットレジストリシステム
⇒ whois？



IPアドレスの売買
⇒ ？？？

IPアドレスの利用権利を示すデータが必要

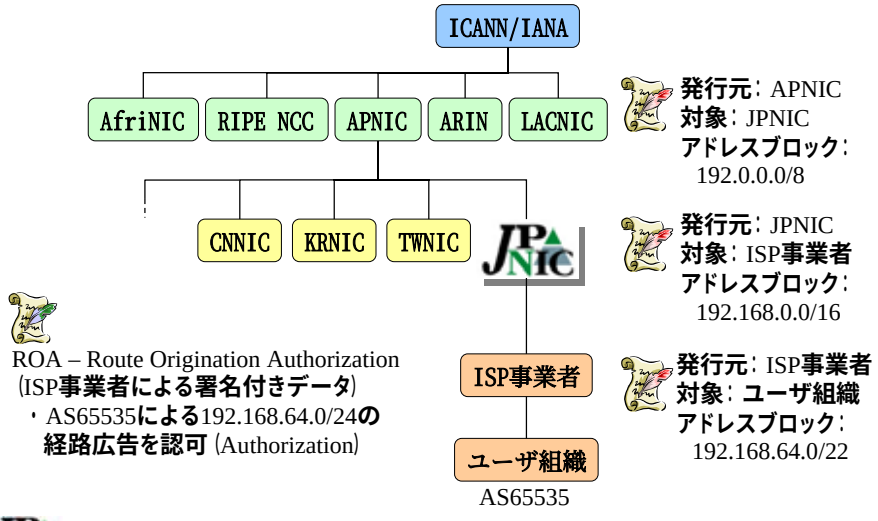
リソース証明書とは

IPアドレスとAS番号の利用権を示す電子証明書

内容：ツリー構造／プロファイル／
トラストアンカー／PKIドメイン／利用法

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

ツリー構造



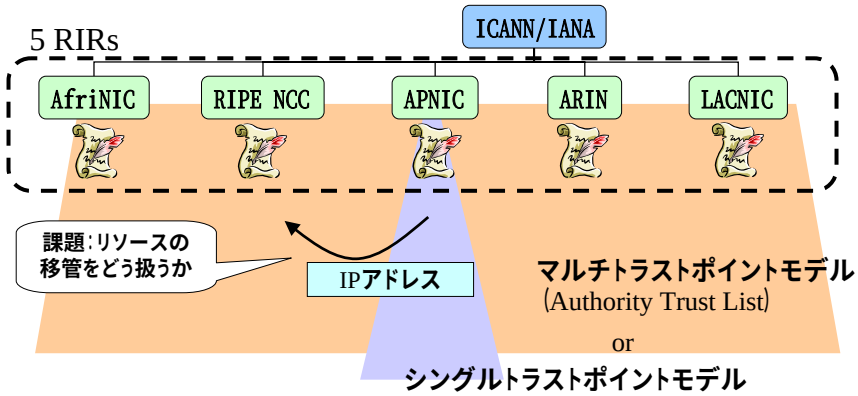
ROA – Route Origination Authorization
（ISP事業者による署名付きデータ）
・AS65535による192.168.64.0/24の
経路広告を認可（Authorization）

リソース証明書のプロファイル

発行元：JPNIC
対象：ISP事業者
アドレスブロック：
192.168.0.0/16

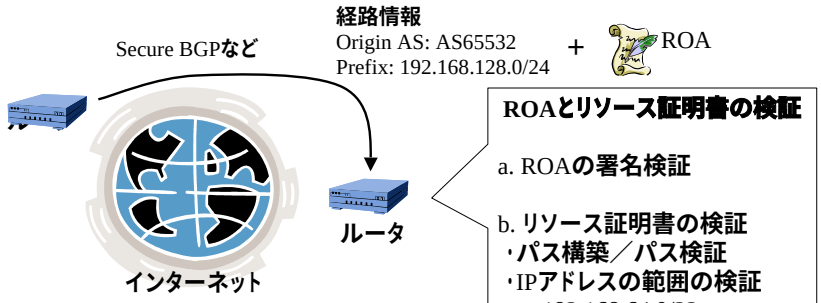
Version: 3
Serial: 111111
Issuer: CN=JPNIC
Not Before: Mon Jan 1 00:00:00 2007 GMT
Bot After: Tue Jan 1 00:00:00 2008 GMT
Subject: CN=ISP, E=resourcecerts@isp.jp
Subject Key Identifier: SSS-SSS
Subject Info Access: caRepository -
rsync://repository.nic.ad.jp/jpnic-isp/AAA-AAA/SSS-SSS
Key Usage: DigitalSignature, 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: 192.168.0.0-192.168.255.255

トラストアンカーとPKIドメイン



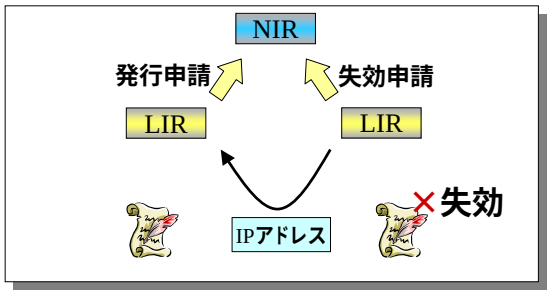
島岡 政基, マルチドメインPKIと相互運用性のBest Current Practice, PKI Day PKI技術最新情報, JNSAセキュリティセミナー, NPO 日本ネットワークセキュリティ協会, http://www.jnsa.org/seminar/2005/seminar_20051028/2shimaoka.pdf,2006年10月

利用法 (1) セキュアルーティング



経路情報の発信元 (Origination) が正しいことを確認できる

利用法 (2) アドレス資源の利用権利

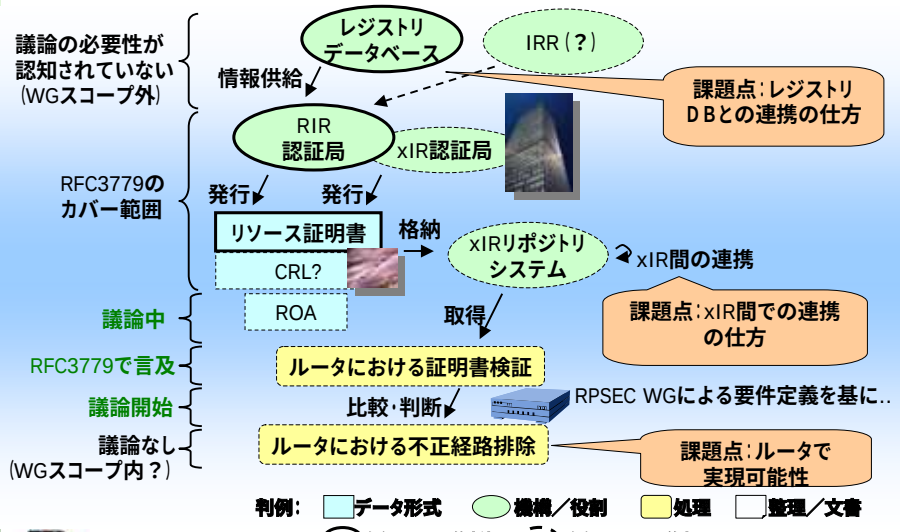


一意となるIPアドレスの利用権利を確認できる

リソース証明書関連のドキュメント

- 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-08.txt
    - A Profile for X.509 PKIX Resource Certificates
  - draft-ietf-sidr-cp-02.txt
    - Certificate Policy (CP) for the Internet IP Address and AS Number (PKI)
  - draft-ietf-sidr-roa-format-01.txt
    - A Profile for Route Origin Authorizations (ROA)
  - draft-ietf-sidr-arch-01.txt
    - An Infrastructure to Support Secure Internet Routing
  - **他、CPSのテンプレートなど**

セキュアルーティングに向けた課題



利用権利の基盤構築に向けた課題

- 証明書データの正当性維持
  - 再割り振りやパンチングホールの扱い
  - 証明書データの元になるレジストリデータベースの正当性
    など
- アドレス資源の扱い
  - 移管： RIR-RIR間、RIR-NIR間
  - 返却： リソース証明書の失効タイミング
    - ルーティングへの影響

国際動向

RIRにおける検討と開発の状況

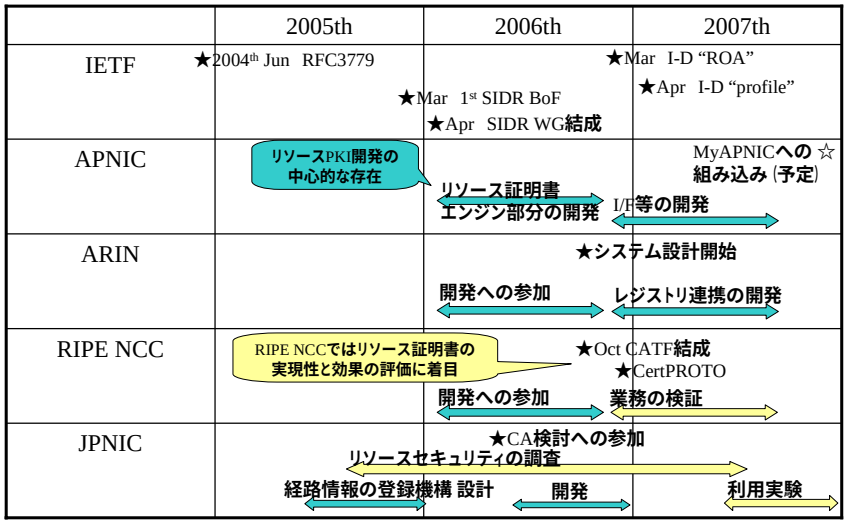
JPNIC 社団法人 日本ネットワークインフォメーションセンター

RIRにおける認証局と リソース証明書に向けた取り組み

	APNIC	ARIN	RIPE NCC	JPNIC
認証局の構築	運用中	運用中	運用中	(実験) 運用中
"X.509"認証の導入	○	○	○ (個別証明書の登録も可能)	(導入実験) ○
リソース証明書に向けた取り組み	2006年度以降開発プロジェクト	APNICの開発に参加、2007年度に内部システム開発	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整合性維持 (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

取り組み状況 (時系列)



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（2006年10月）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する予定であったが第56回に延期
  - 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（若干継続した模様）
  - 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

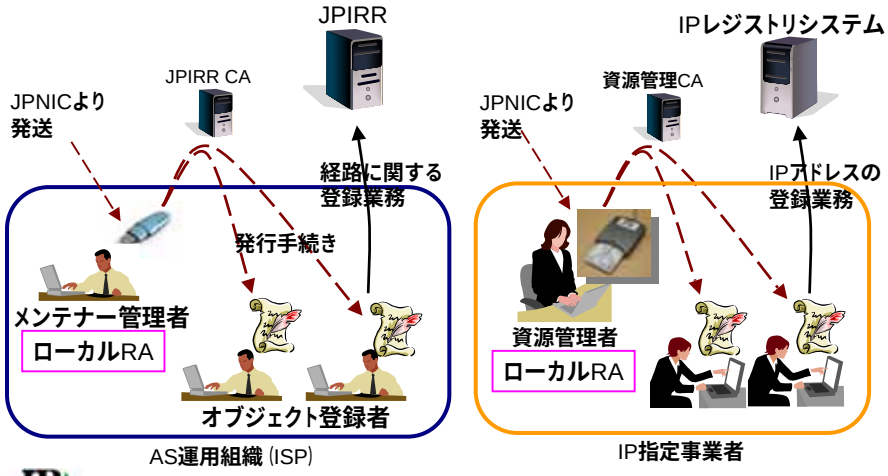
JPNICにおける取り組み

認証強化と経路情報の登録機構
～IPアドレスとAS番号の情報の正当性維持～

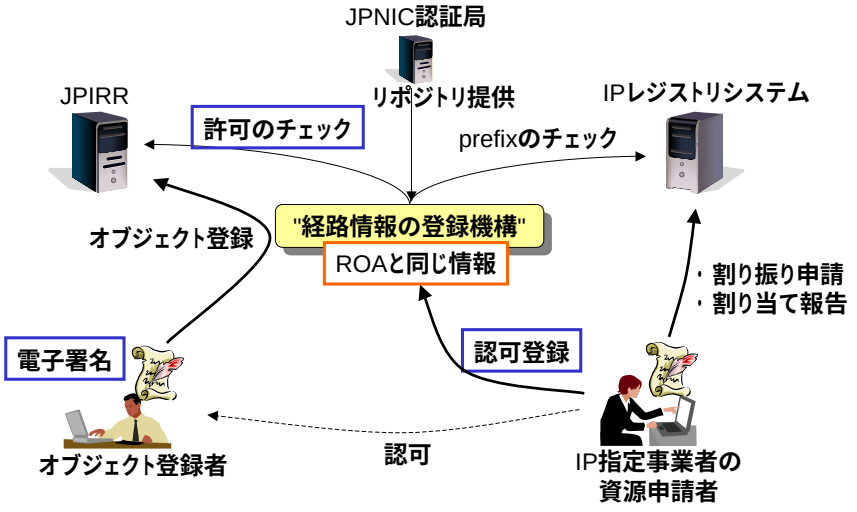
社団法人 日本ネットワークインフォメーションセンター

JPNICにおける業務面での取り組み（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）



リソース証明書の相互運用性

電子証明書の相互運用性とは

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
  - セキュアな経路制御
    - 国際的なピア (AS同士のつながり) が当然存在
    - 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。マルチホームの構成もある。
  - IPアドレスの利用権利
    - 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状況を作ることは必要条件

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)
    - フィールドの種類や意味／クリティカリティ

    ⇒ RPやCAの違いによって異なる挙動が起こることは避けたい ⇒ profileの定め方
  - リポジトリ (CRLDPや等) の運用状況
    - リソース証明書におけるauthorityInfoAccessやsubjectInfoAccess
    - RPに要求されるサービスレベルを維持

    ⇒サービスの継続性がなくなる状況は避けたい

    ⇒RPの挙動による

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（ルータの挙動）
    - 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
    - マルチドメインかシングルドメインか
    - リソースの移管が起こったときにパスはどうなるか
  - 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（1）

- JPNICで行っている実験的な活動
  - 電子認証プラクティスフォーラム
    - 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
      - PKIを含め、電子認証に関するBCP（Best Current Practice）をコンセンサスベースで文書化／公開することを目指す
      - リソース証明書に限定しない
    - MLとオフライン・フォーラム
      - http://eapf.nic.ad.jp/

相互運用性向上に向けた活動（2）

- BCPドキュメント例
  - CA証明書のロールオーバー方法
  - 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
  - アドレス資源の利用権利を示す電子証明書
  - 用途
    - セキュアルーティング
    - IPアドレスの利用権利
  - 課題
    - 証明書を利用したアプリケーション仕様
    - リソース証明書に含まれる情報の正しさ
- 相互運用性
  - 書式上の相互運用性
  - 意味的な相互運用性