JPNIC認証局と経路情報の登録機構について

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
技術部／インターネット推進部
セキュリティ事業担当
木村 泰司

本発表の主旨

- これまでに進めてきたJPNIC認証局のプロジェクトを、JPIRRでの利用へ拡張することを検討しています。
  - そこで以下の二点についてのご意見を頂きたいと思います。
    - JPNIC認証局の本運用に向けた検討
    - JPIRRとの連携「経路情報の登録機構」

本発表の内容

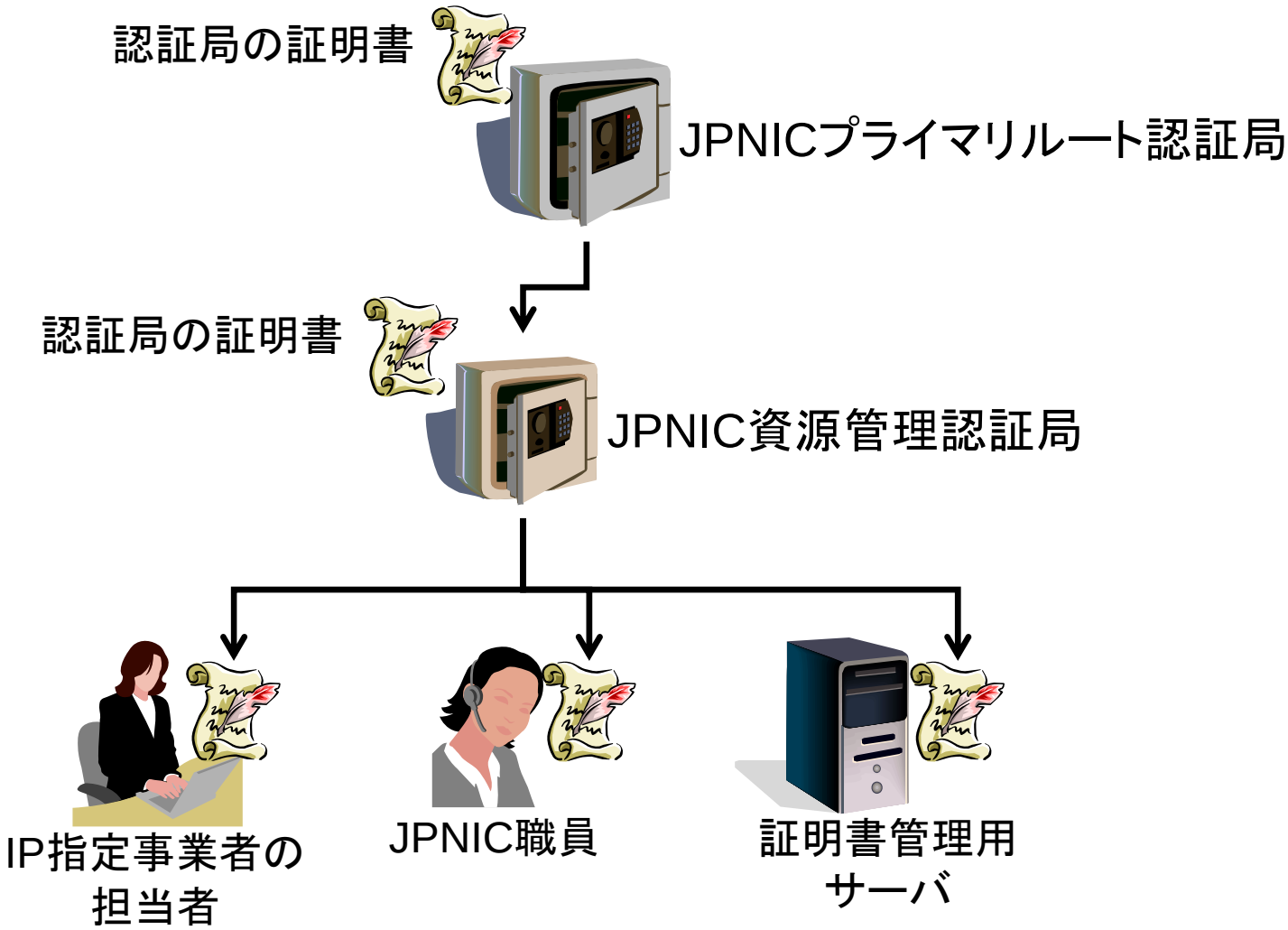
- JPNIC認証局の概要及び実験運用の状況と本運用に向けた検討について

- 電子証明書とJPNIC認証局を利用した経路情報の登録機構の概要

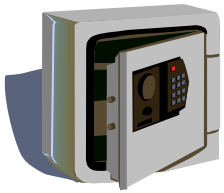
JPNIC認証局の概要及び実験運用の状況について

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認証局（1／3）


認証局の証明書
JPNICプライマリルート認証局
認証局の証明書
JPNIC資源管理認証局
IP指定事業者の
担当者
JPNIC職員
証明書管理用
サーバ

JPNIC認証局（2／3）

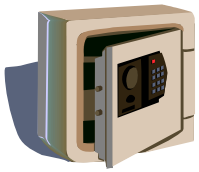


JPNICプライマリルート認証局

○JPNICにおける電子認証業務の「信頼点」の提供
- 「信頼された認証機関」として設定
- JPNICのすべての電子証明書の検証に使用

JPNIC認証局のツリー構造

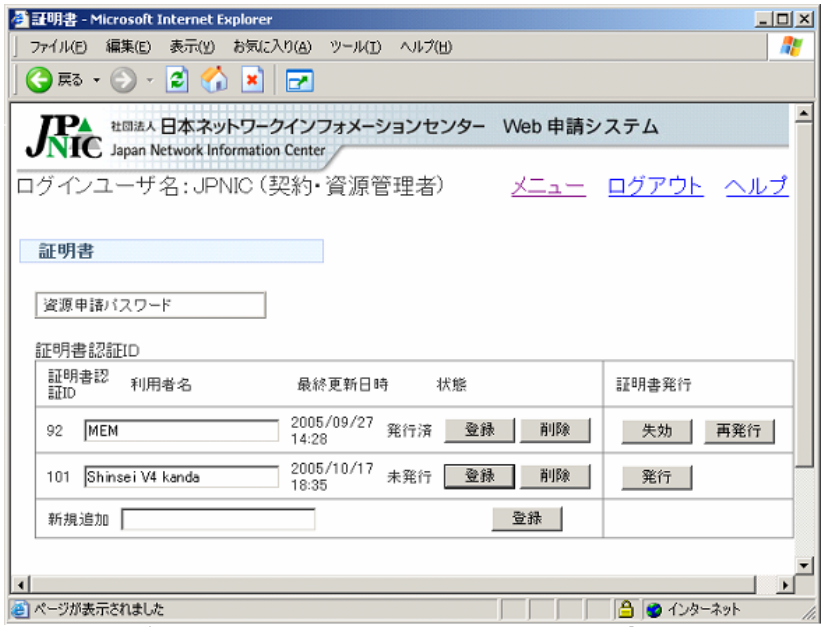
JPNIC認証局（3／3）



JPNIC資源管理認証局

○アドレス資源管理における電子認証の提供が目的
- IP指定事業者向けのクライアント証明書の発行
- 証明書管理用サーバの証明書の発行

資源管理カード
とICカードリーダ



JPNIC資源管理認証局の証明書管理画面

証明書を使った認証強化の利点

JPNIC資源管理認証局

証明書管理Web

1.資源申請者の証明書を発行

2.証明書の配布

資源管理者

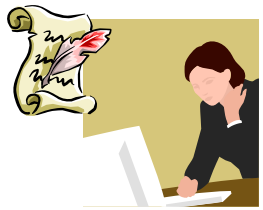
資源申請者の担当者が変わっても安心

資源申請者のユーザ管理ができて便利

第三者による不正な書き換えや不正な申請を防ぎやすく安全

IPレジストリシステム

3.証明書を使ってログイン
各種申請業務を行う



資源申請者

（IPアドレス関連の申請業務の手順は変わらない）

資源申請者

JPNIC認証局プロジェクトの状況（1／2）

	4月～6月	7月～9月	10月～12月	1月～3月
FY2004		認証局システム開発／規程（CPS）の更新 →	★JPOPM	
FY2005	★指定事業者連絡会	指定事業者向けの認証強化実験 → ★利用者説明会 ★JPOPM	★指定事業者連絡会	（★JANOG）
FY2006	指定事業者向けの認証強化実験（継続中） →	★利用者説明会	★JPOPM	

JPNIC認証局プロジェクトの状況（2／2）

- 実験運用の結果
  - 証明書発行数
    - 資源管理カード（ICカード）発行
      - 指定事業者13枚
      - JPNIC職員12枚
    - 資源申請者証明書の発行
      - 指定事業者9枚

    ⇒httpsのクライアント認証を使ってIP指定事業者の申請業務における認証強化を図ることはできた。

  - システムが止まる程の障害はなかった
    - 発行された証明書の利用上のトラブル対応はあった。

    ⇒利用上の不具合に関するノウハウが得られた。

利用状況とこれまでに頂いたご意見

- 証明書利用の状況
  ⇒ 利用者数はなかなか増えない。
    - 「難しすぎて使えない」という状況とも考えにくいが・・・。

- IP指定事業者複数社よりこれまでに頂いたご意見
  - 認証方式をよりセキュアなものにしていくことについては反対しない。
  - 電子証明書の利用に関する抵抗について ★
    - 「社内のPCの利用に関する社内規定がある。ICカード等を利用する為には、それなりの説明が必要。」

    ⇒ まず具体的な利用環境の情報が必要
  - 利用促進に関するご意見 ★
    - 「プロモーションの仕方が足りない」
    - 「国内のISPをコーディネートして早く形として状況を作ることが必要」

    ⇒ 説明機会をより多く設ける必要

- 認証強化実験と証明書が使われない要因について、これら以外にありましたらご意見を頂けますようお願い致します。

JPNIC認証局の本運用に向けた検討について

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認証局の本運用に向けた検討

- 検討を開始した理由
  - これまでに頂いたご意見から、IPアドレスの管理業務におけるセキュリティ強化のニーズはあると考えられる。
  - APNIC、RIPE NCC、ARINでは、IPアドレスの管理業務で電子証明書を利用した認証強化を、既に実施している。

  - セキュリティの抜本的な向上には認証局は中期的に不可欠だと考える。その為には着実に本運用に向けて歩みを進める必要がある。

⇒ 本運用に向けた検討へ

  - 必要十分かつ継続できるような運用レベルを明らかにする為の調査

本運用に向けた検討

- 検討の目標
  - 認証局サービスの運用レベルを明らかにする
    - 利用者と合意できるようなサービスレベル
- 検討事項（案）
  a. 認証業務の内容と体制
  b. 本運用に必要な設備
  c. サービスの範囲や効果（利用価値）
  d. 改善を図る為の追加開発等の有無
- 検討を開始した事項
  - JPNIC認証局の本運用にかかる費用
    - a、b に対して、実験結果から想定

- 本検討について、またJPNIC認証局の本運用に関するご意見をお願い致します。

電子証明書とJPNIC認証局を利用した経路情報の登録機構の概要

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

経路情報の登録機構とは

- 概要
  - 割り振り情報／割り当て情報との整合性を持たない、不正なオブジェクトをJPIRRに登録できないようにする仕組み
    - JPIRRの登録情報と割り振り／割り当て情報との整合性を確認してから登録

背景

- JPIRRには割り振り／割り当てに関わらず、任意のアドレスprefixが入ったrouteオブジェクトを登録できてしまう。
  - 他のISPが経路広告すべきprefix
  - 割り振られていないprefixなど

⇒ JPIRRを使っていても、BGPルータのオペレーターが経路広告を始める前に、そのprefixに関する各種のチェックを行う必要がある

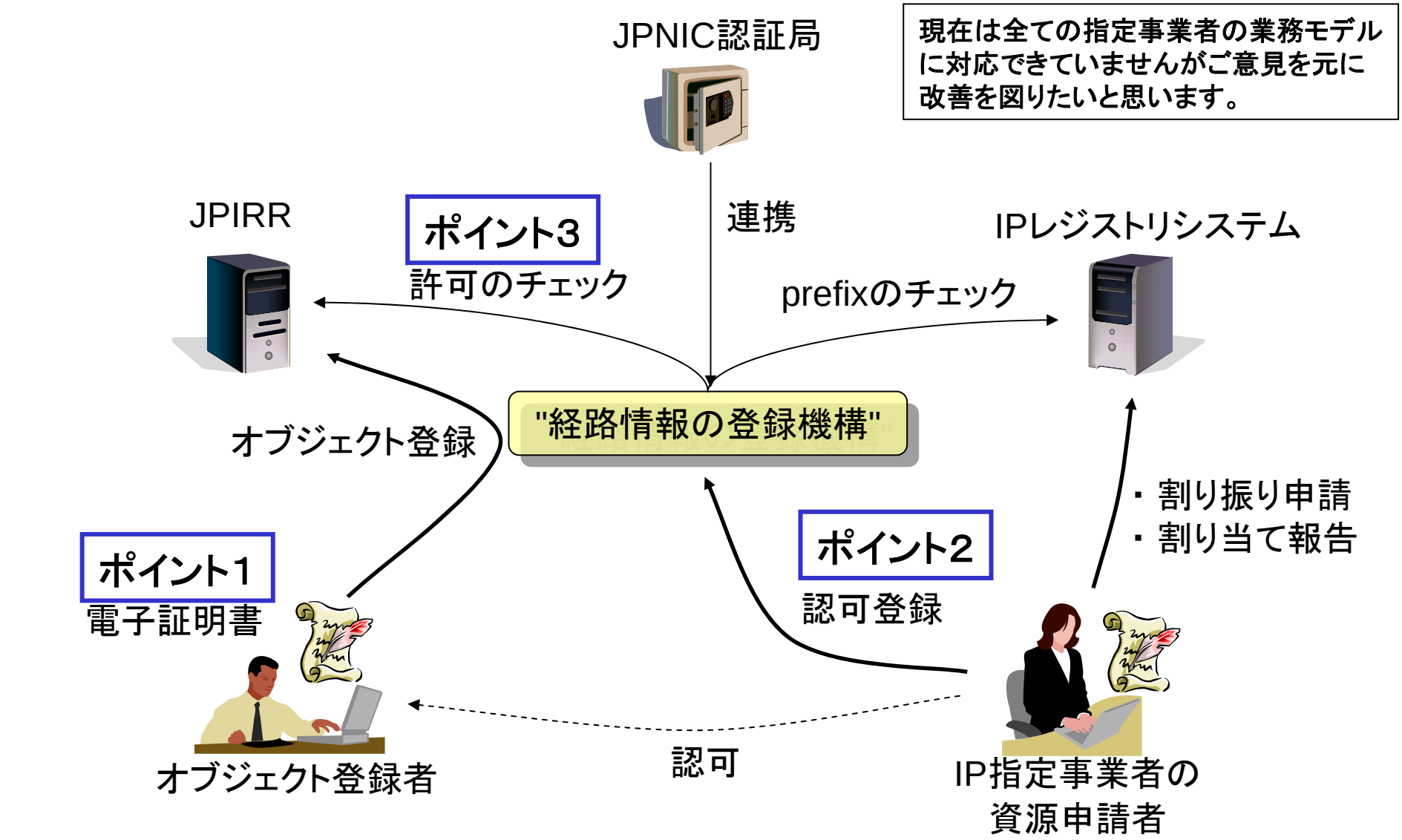
- インターネットに流れる経路情報と比較すればよい?
  - No ⇒ これでは"IPアドレスは使ったもの勝ち"

⇒ JPIRRに登録されている情報が予めチェックされていれば、そのチェックの手間を軽減できる。JPIRRを使うことで機械的に経路ハイジャックを検知できる可能性が上がる。

登録される情報に対するチェックの考え方

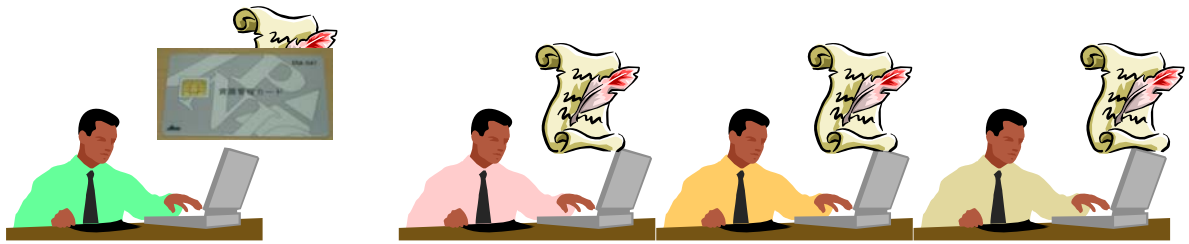
- レジストリにおけるIRRの登録情報の正しさ
  1. IRRに情報登録するユーザの正しさ
     - IRRに登録するユーザは認証されている
  2. routeオブジェクトの登録に関する正しい認可
     - IPアドレスを割り振られたIP指定事業者による、ASオブジェクトやrouteオブジェクトの情報登録者（メンテナー）に対する認可がある
  3. 登録情報のIPレジストリシステムとの整合性
     - AS番号やIPアドレスは、インターネットレジストリによって割り振り／割り当てられている

概念図


JPNIC認証局
現在は全ての指定事業者の業務モデルに対応できていませんがご意見を元に改善を図りたいと思います。
JPIRR
ポイント3
許可のチェック
連携
IPレジストリシステム
prefixのチェック
オブジェクト登録
"経路情報の登録機構"
・割り振り申請
・割り当て報告
ポイント1
電子証明書
ポイント2
認可登録
認可
オブジェクト登録者
IP指定事業者の
資源申請者

ポイント1：JPIRRユーザ向け電子証明書

- JPIRR証明書管理者（admin-c）
  - オブジェクト登録者の証明書を発行／失効
- オブジェクト登録者（tech-c）
  - S/MIMEの電子署名を使ってIRRのオブジェクトを登録



※mntnerオブジェクトのadmin-c、tech-c

ポイント2：許可リストを使った認可登録（1／2）

許可リスト

prefix （登録できる範囲）	許可／禁止	メンテナー	Origin AS (optional)
1.1.0.0/16	allow	mnt1	12345
1.1.0.0/17	allow	mnt2	

ポイント2：許可リストを使った認可登録（2／2）

IPレジストリシステム

・指定されたprefixが当該IP指定事業者に
割り振られているかをチェック

prefix （登録できる範囲）	許可／禁止	メンテナー	Origin AS (optional)
1.1.0.0/16	allow	mnt1	12345
1.1.0.0/17	allow	mnt2	

IP指定事業者の
資源申請者

・IRRにオブジェクトを登録できるメンテナーを指定
・IRRにオブジェクトを登録できる範囲のprefixを指定
・Origin ASの指定も可能

ポイント3：許可のチェック

JPIRR

・許可されたprefixとメンテナーであれば登録

prefix （登録できる範囲）	許可／禁止	メンテナー	Origin AS (optional)
1.1.0.0/16	allow	mnt1	12345
1.1.0.0/17	allow	mnt2	

・routeオブジェクトを登録（S/MIMEを使用）

mnt1のtech-c
（オブジェクト登録者）

得られる効果

1. IRRに情報登録するユーザの正しさ
   - 電子証明書の業務でユーザの認証を担保できる。

2. routeオブジェクトの登録に関する正しい認可
   - 許可リストに載ったメンテナーだけが、IP指定事業者が指定したprefixの範囲で登録できるようになる。

3. 登録情報のIPレジストリシステムとの整合性
   - 割り振られていないような不正なprefixが登録されなくなる。

利用実験までのスケジュール

	4月～6月	7月～9月	10月～12月	1月～3月
FY2005		システムモデルと要件の調査 →		★JANOG
FY2006		システム開発 →		（★JANOG）
FY2007	利用実験 →			
	（★利用者説明会）		★JPOPM	
	（★指定事業者連絡会）			

実験利用に必要なもの

- IP指定事業者
  - 「資源管理カード」
  - JPNICより割り振られたIPアドレス
  - 経路広告を行うASのメンテナー名（JPIRRに登録されているもの）
- JPIRRユーザ
  - S/MIME対応メールソフト
    - Thunderbirdなど
  - USBトークン（予定）
    - JPNICより無償でお貸しする予定です。

実験利用は2007年度初頭に開始する予定です。
ご意見、ご希望などをお寄せ頂ければ幸いです。

お問い合わせ :
ca-query@nic.ad.jp

まとめ

- JPNIC認証局の運用状況と本運用に向けた検討
  - 大きな障害はなく、ノウハウは得られつつある。
  - 認証強化実験に反対する意見は頂いていないが、利用者が増えていない。
  - JPNIC認証局の本運用に関する検討を行っている。
- JPNICの経路情報の登録機構
  - JPIRRで登録時のチェックを行って、信頼性向上を図る。
  - 2007年度に実験利用開始を予定している。

RIRにおける認証局利用状況

	JPNIC	APNIC	ARIN	RIPE NCC	AfriNIC	LACNIC
認証局の運用	△	○	○	○	×	×
Webシステムの運用	△	○	×	○	×	×
申請業務での証明書の利用	△	○	○	○	×	×

○：本運用　△：実験運用　×：運用されていない

RIPE NCCにおける割り振り／割り当て情報とAS番号をマッチングする機構

- RIPE NCC
  - RPSL Databaseのmntnerオブジェクトに含まれるフィールドを使った、メンテナー単位での登録認可
    - mnt-lower
      - inetnum、inet6numオブジェクトの管理
      - routeオブジェクトの登録管理
    - mnt-route
      - routeオブジェクトの登録管理のみ

ARINにおける割り振り／割り当て情報とAS番号をマッチングする機構

- ARIN
  - 2006年3月の提案
    - Proposal 2003-3 "Capturing Originations in Templates"
      - ネットワーク情報の既存の属性NetRange:、NetType:に加えて「OriginatingASList:」を追加する。

      ⇒　OriginatingASList の値はプリフィックスの広告元となるAS番号のリスト

APNICにおける割り振り／割り当て情報とAS番号をマッチングする機構

- APNIC
  - 現段階でなし
  - リソース証明書プロジェクトで、route-setオブジェクトに対する電子署名によって認可を示す機構を開発中。

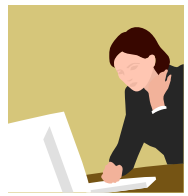
利用手順（IPレジストリシステムの認証強化）

1. 認証強化実験の参加申し込み
   申し込み先：ca-query@nic.ad.jp

2. 管理者用証明書（資源管理カード）の申請
   （業務手順については検討中）

3. 管理者が申請者用証明書を発行
   （資源管理カードを使って管理用Webにアクセス）

4. 申請者用証明書を使ってWeb申請システムと
   許可リスト管理システム（仮）を利用



利用手順イメージ（JPIRRの登録者認証）

1. Maintainerオブジェクトを登録 ＋ USBトークン申請
（業務手順については検討中）

2. 管理者用証明書を受け取る

3. 管理者がオブジェクト登録者の証明書を発行
（USBトークンを使って管理用Webにアクセス）

4. S/MIMEを使ってJPIRRにオブジェクトを登録
（CRYPT-PWやPGPキーも登録されていれば利用可能）

パスワード認証との違い

- 各々の申請者が別々の電子証明書を利用