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

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

本発表の主旨

- これまでに進めてきたJPNIC認証局に関する「本運用化に向けた検討」と「経路情報の登録機構の実験サービス」についての最新状況をお知らせ致します。

  - 本運用化に向けた検討
  - JPIRRとの連携「経路情報の登録機構」

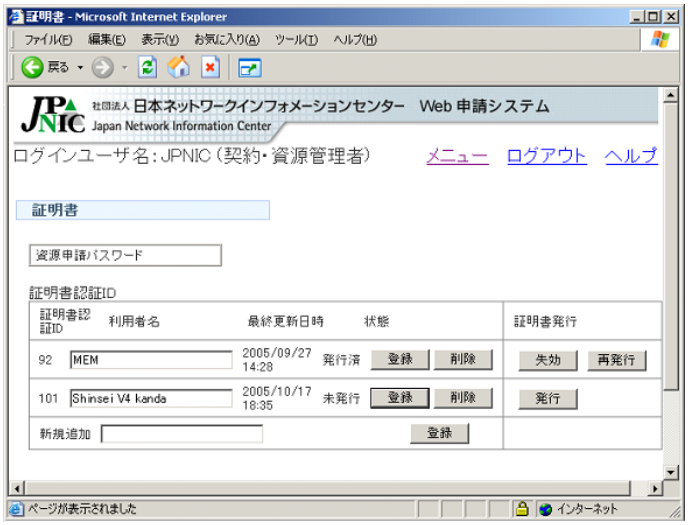
JPNIC認証局の本運用化に関する検討状況について

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認証局とは

- JPNIC認証局
  - JPNICプライマリルート認証局
  - JPNIC資源管理認証局
  - （JPIRR認証局）
- JPNIC資源管理認証局
  - Web申請システムのユーザ向け電子証明書を発行
  - 2005年9月より実験利用開始
  - 実験参加：11社（2007年11月現在）

Web申請システム



申請業務の担当者

申請業務の管理者

本運用化に関する検討

- IPアドレス管理の安全性向上のためには、認証強化は重要
  - 「電子証明書を使った認証強化実験」
    - 電子証明書の仕組みが業務に適合するか構築して利用実験
      ⇒　大きな問題はなく実施中
  - 今後の状況
    - アドレス在庫枯渇期に入りIPアドレスの不正利用の危険性が相対的に上がると考えられる。
    - 一部の希望者のみが*実験として*利用しているだけでは、認証局構築・導入の効果は得られにくい。

⇒　本運用化が必要

本運用化の考え方

- **積極的にすべてのユーザへ導入を図る。**
  - 指定事業者の認証方式を電子証明書に移行することを視野
  - 将来的にIP指定事業者以外でも利用することも考える。
- **サービスを継続的に実施できるようにする。**
  - IPレジストリシステムと同程度のサービスレベル
  - JPNICの事業としてサービスを維持

検討作業の内容

- ユーザ環境における導入に関して
  - ユーザにおける導入障壁をきちんと調査する必要
    - 電子証明書を使った認証方式への移行に関するアンケート調査
    - 電子証明書の導入障壁となっている事項に関するヒアリング調査

- 事業の一部としてのサービス実施に関して
  - 認証局の設備維持や運用費用の確保をJPNICの事業の中で行うための精査の作業
    - JPNICの事業における位置づけの整理など

ユーザ環境における導入に関する調査結果と考察

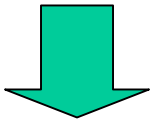
- 電子証明書を使った認証方式への移行可能性
  - 認証局の本運用化と認証強化に関する十分な情報提供により、デフォルトの認証方式をパスワードから電子証明書に移行することは可能であると考えられる。
- 導入障壁の低減に必要な事柄
  - メリットを含めた情報提供と「今後継続すること」の提示
  - 電子証明書のみになった場合の機能追加
    - Webトランザクションの高機能化
    - S/MIMEの導入

経路情報の登録機構について

背景

- IRR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。
  - 全く関係のない他のISPが経路広告すべきprefix
  - 未割り振りのprefixなど

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

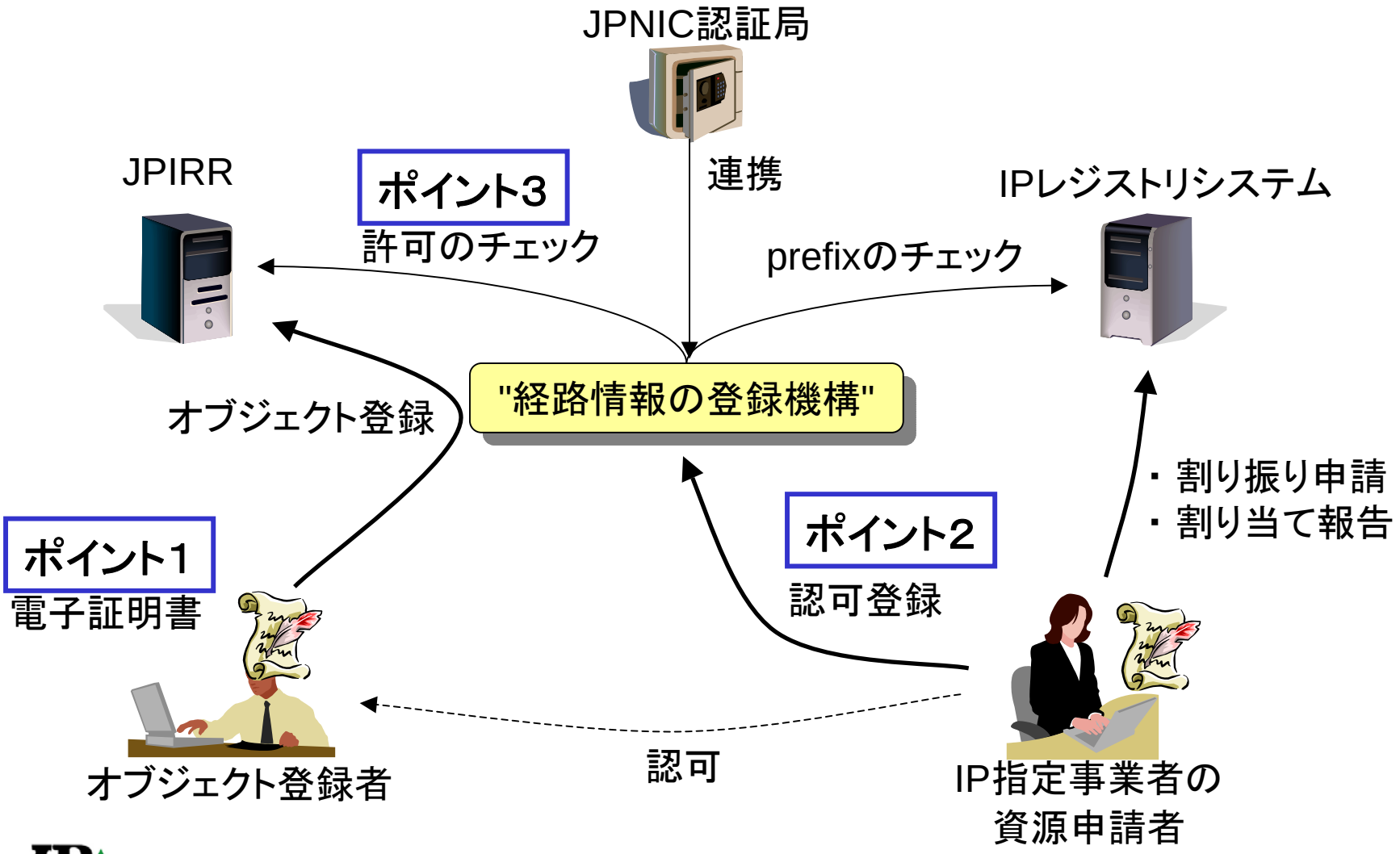


- JPIRRに登録されている情報が予めチェック（＝IPアドレス登録情報との照合）されていれば、機械的に経路ハイジャックを検知できる可能性がある。

経路情報の登録機構とは

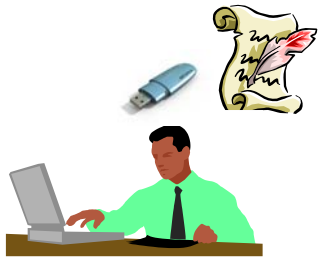
- 割り振り情報／割り当て情報との整合性を持たない、不正なオブジェクトをJPIRRに登録できないようにする仕組み
  - JPNICのIPアドレスに関する登録情報（割り振り情報、割り当て情報）との整合性を確認してから登録

概念図

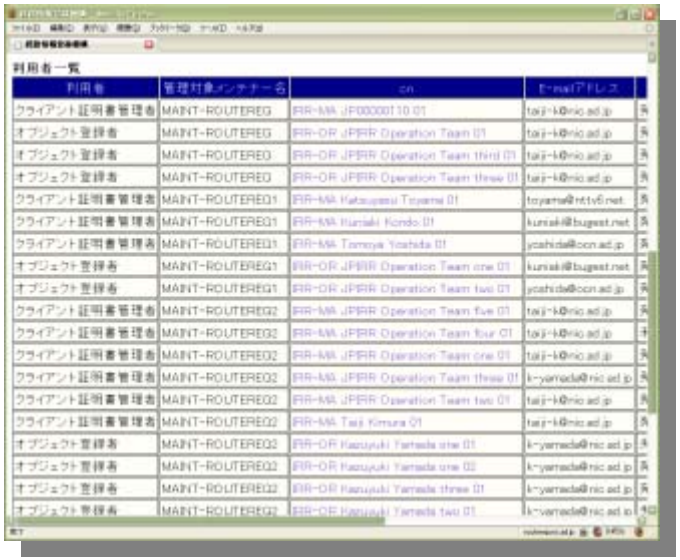

JPNIC認証局
連携
JPIRR
ポイント3
許可のチェック
IPレジストリシステム
prefixのチェック
"経路情報の登録機構"
オブジェクト登録
・割り振り申請
・割り当て報告
ポイント1
電子証明書
ポイント2
認可登録
認可
オブジェクト登録者
IP指定事業者の
資源申請者

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, tech-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（任意登録）
  - S/MIMEの電子署名を使ってIRRのオブジェクトを登録



admin-c, tech-c



オブジェクト登録者

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

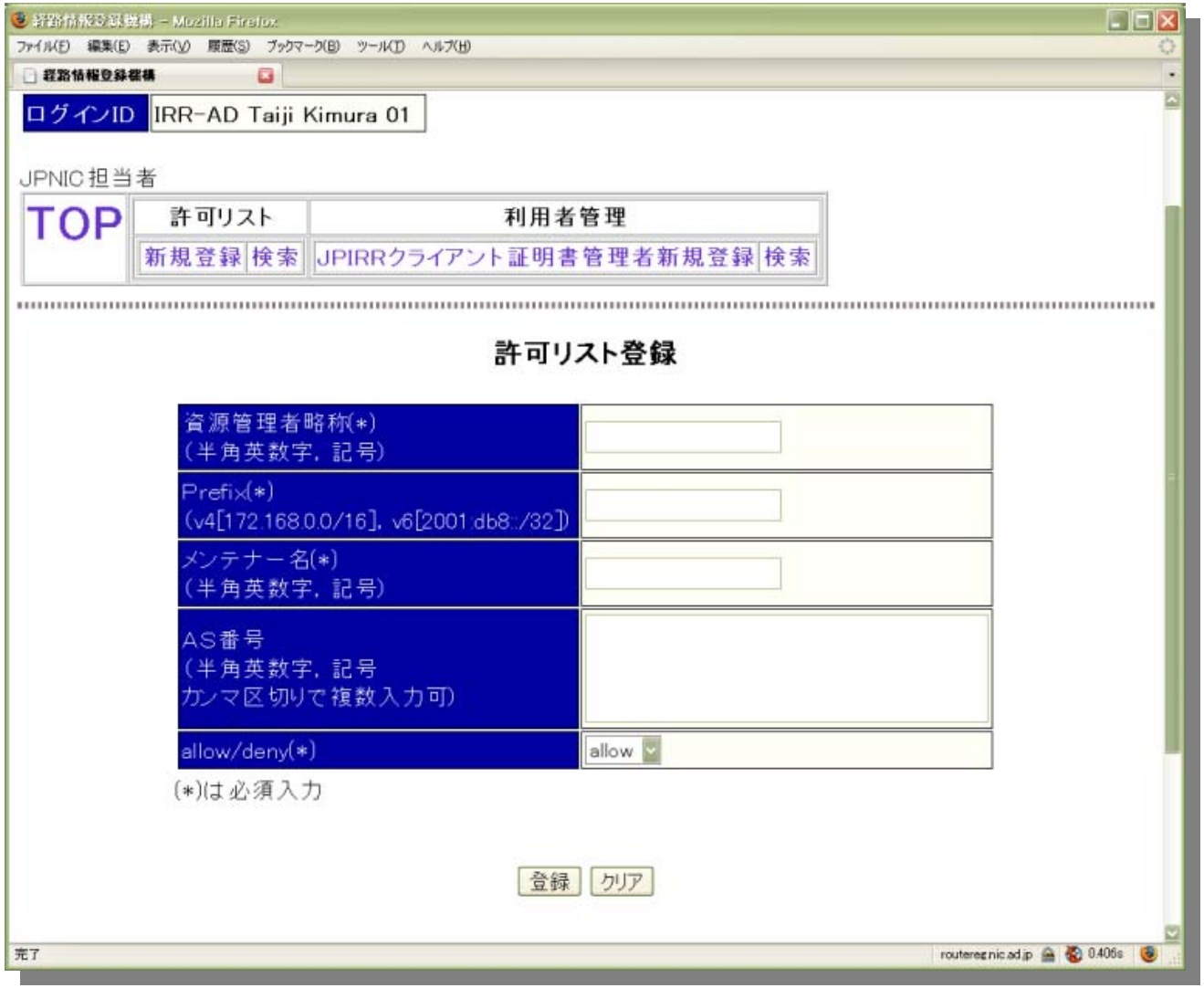
prefix （登録できる範囲）	許可／禁止	メンテナー	Origin AS (optional)
1.1.0.0/16	allow	mnt1	12345
1.1.0.0/17	allow	mnt2	

・routeオブジェクトを登録（S/MIMEを使用）

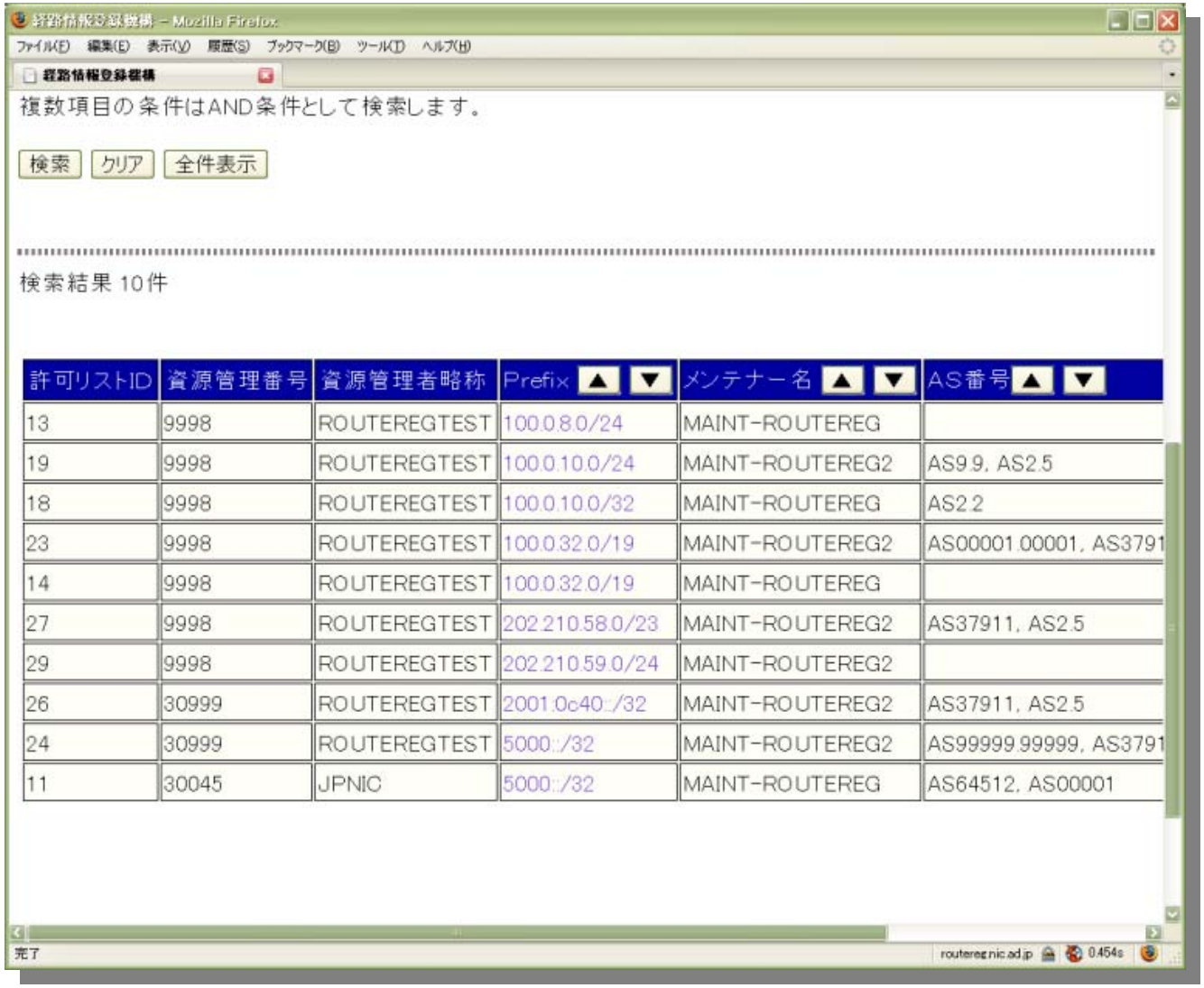
mnt1のtech-c
（オブジェクト登録者）

経路情報の登録機構の画面（1）

経路情報の登録機構の画面（2）



経路情報の登録機構の画面（3）



許可リストID	資源管理番号	資源管理者略称	Prefix	メンテナー名	AS番号
13	9998	ROUTEREGTEST	100.0.8.0/24	MAINT-ROUTEREG	
19	9998	ROUTEREGTEST	100.0.10.0/24	MAINT-ROUTEREG2	AS9.9, AS2.5
18	9998	ROUTEREGTEST	100.0.10.0/32	MAINT-ROUTEREG	AS2.2
23	9998	ROUTEREGTEST	100.0.32.0/19	MAINT-ROUTEREG2	AS00001.00001, AS3791
14	9998	ROUTEREGTEST	100.0.32.0/19	MAINT-ROUTEREG	
27	9998	ROUTEREGTEST	202.210.58.0/23	MAINT-ROUTEREG2	AS37911, AS2.5
29	9998	ROUTEREGTEST	202.210.59.0/24	MAINT-ROUTEREG2	
26	30999	ROUTEREGTEST	2001:0c40::/32	MAINT-ROUTEREG2	AS37911, AS2.5
24	30999	ROUTEREGTEST	5000::/32	MAINT-ROUTEREG2	AS99999.99999, AS3791
11	30045	JPNIC	5000::/32	MAINT-ROUTEREG	AS64512, AS00001

得られる効果

1. IRRに情報登録するユーザの正しさ
   - クライアント証明書の利用により、ユーザの正当性を担保できる。（確認事項が明確になる）

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。

実験利用に必要なもの

- IP指定事業者
  - IP指定事業者の電子証明書
    - 認証強化実験で使われているもの
  - 経路広告されるメンテナー名の把握
- JPIRRユーザ
  - S/MIME対応メールソフト
    - Thunderbirdなど
  - USBトークン
    - JPNICより無償でお貸しします。

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

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

以降は、補足のための資料です

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 2006-3 "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検討していた（2006年10月頃）

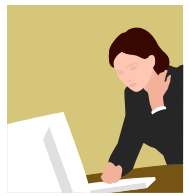
利用手順（IP指定事業者）

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
   許可リスト管理画面を利用



利用手順（JPIRRの登録者）

1. Maintainerオブジェクトを登録 ＋ USBトークン申請
   参照：http://www.nic.ad.jp/doc/jpnic-01048.html

2. 管理者用証明書を受け取る
   （業務手順については検討中）

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併用可能
   ただしprefixのチェックは登録機構を利用したときのみ）

ヒアリングとアンケートの結果

導入障壁の調査

a. 通常業務で利用可能かどうか
   - 対象：認証強化実験に参加している事業者
   - 実施状況：10社に電子メールで実施。8社が回答（80%）

b. 電子証明書への移行は可能か
   - 対象：過去2年間で申請量の多い15社
   - 実施状況：訪問してヒアリングを実施
     - 導入していない理由
     - 移行のために必要とされるもの

ほか

a.　通常業務で利用可能かどうか

- 電子証明書（認証局、及び資源管理カード）が通常業務に利用可能だと答えた事業者は 8社中7社
- 認証強化実験の業務／システムは通常業務に支障なく使用されている。

b.　電子証明書への移行は可能か

- 電子証明書を利用していないが、移行することになれば利用すると答えた事業者は半数以上。
- 利用していない理由
  - メリットを含めた情報が届いていない
  - 今後継続するかどうかが示されていない
- 移行の為に必要とされるもの
  - 主に申請を自動化しているところ、もしくは今後自動化したいところを中心に、パスワードから電子証明書への移行にはWebトランザクションが必要という回答が多かった。