経路情報の登録認可機構
～JPIRRのrouteオブジェクトをきれいにするぞ～

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
インターネット推進部　セキュリティ事業担当　木村泰司

2008年1月21日（月）　IRS15、東京ミッドタウン

「経路情報の登録認可機構」

- 概要
  - IRRのrouteオブジェクトって…
    - 割り振られていないIPアドレスや好きなOrigin ASを書ける…
  - 割り振られているアドレスなのかどうかは
    - JPNICがJPIRRをやってるなら確認すればいいのでは？
    - 一括で確認して一定期間したら削除するのではなく、登録するときに「そのアドレス間違ってまっせ」という方がよい
  - 作ってみました。
    - routeオブジェクトを登録する前にチェックします。チェック済みのrouteオブジェクトだけが登録されます。
  - 利用実験をやっています。
    - 詳しくはWebページをご覧下さい。
      - http://www.nic.ad.jp/ja/research/ca/routereg-outline.html
      - トップページ → JPNIC認証局 → 経路情報の登録認可機構とは

背景　JPIRRの登録情報キレイ化の仕組み（1）

- IRRオブジェクト　ガーベージコレクター
  - 更新期間を過ぎても更新されないオブジェクトを参照不可にするバッチ処理
    - mntnerのdescr: expire=6（更新期間は6ヶ月）
      - 1ヶ月以上24ヶ月未満を指定可能
    - 詳しい説明
      - https://jpirr.nic.ad.jp/gc/doc/
- ポリシーチェッカー
  - aut-numオブジェクトに書かれたimport/exportに不整合がないかチェックするWebツール
    - 隣接asやas-setは登録されている？import文とexport文は合っている？
    - 詳しい説明
      - https://jpirr.nic.ad.jp/PolicyCheck/document.html

背景　JPIRRの登録情報キレイ化の仕組み (2)

- IRRオブジェクト　ガーベージコレクター
- ポリシーチェッカー

＋

- 経路情報の登録認可機構

経路情報の登録認可機構のチェック

- どういうタイミングで？
  - routeオブジェクトを登録しようとするとき
- どういうチェックをするの？
  - routeオブジェクトに書かれているIPアドレスが、割り振り先によって「routeオブジェクトとして登録してよいよー」と言われているかどうか
    - 「許可リスト」に載っているかどうか

許可リスト

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	

許可リストを使った認可登録

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

許可のチェック

JPIRR

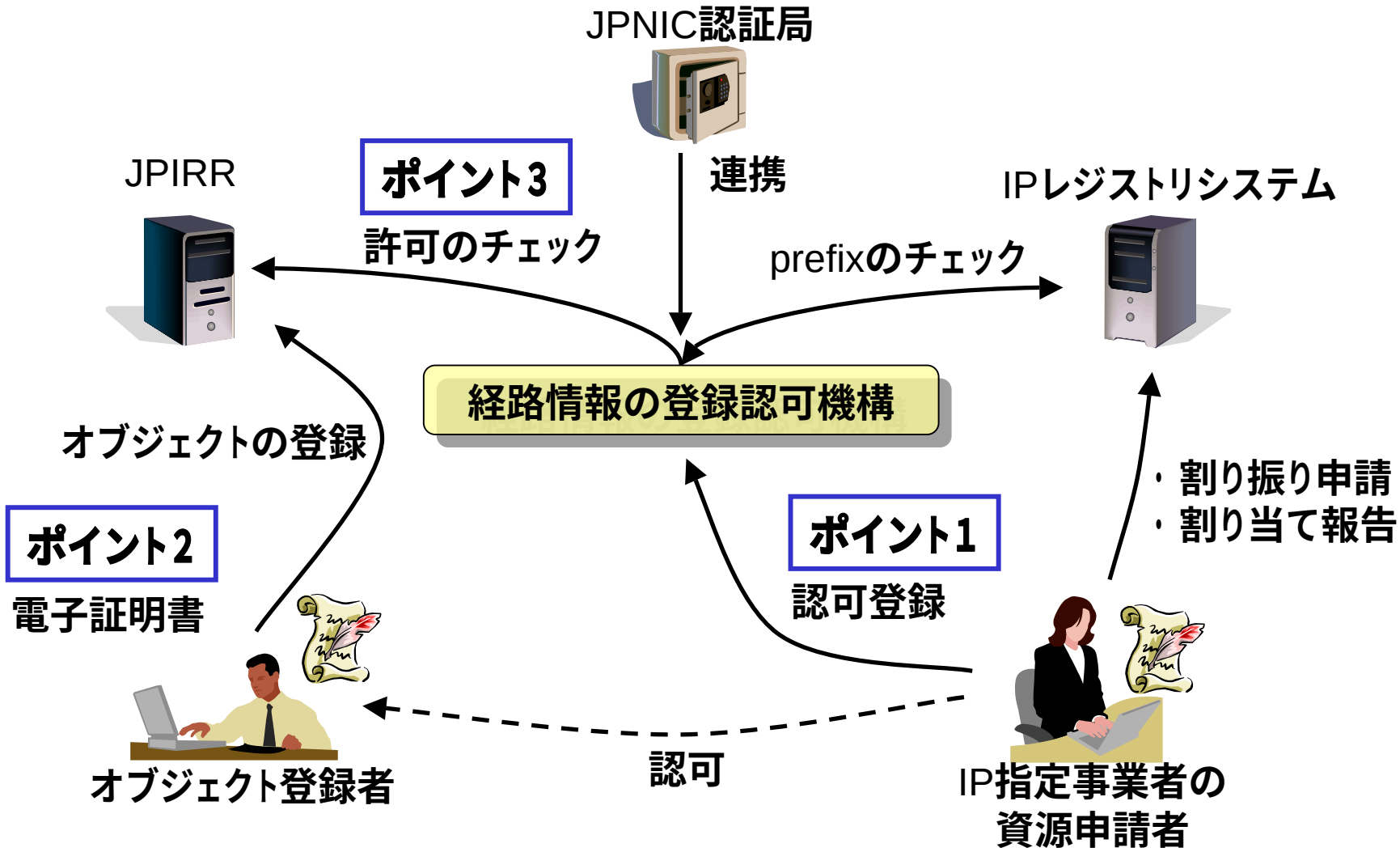
・許可されたprefixとメンテナーであれば登録

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）

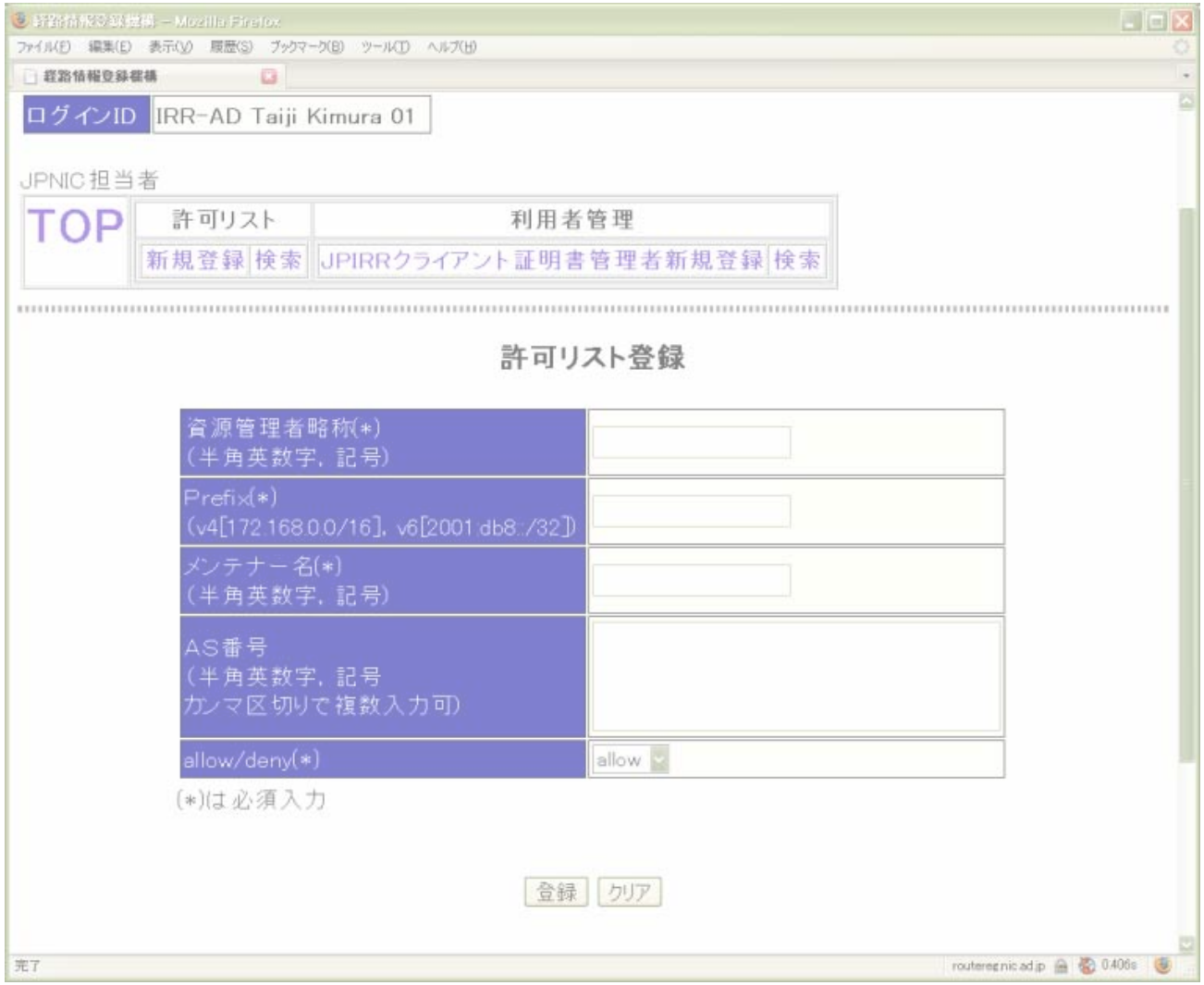
mnt1のオブジェクト登録者
（オブジェクト登録者）

概念図

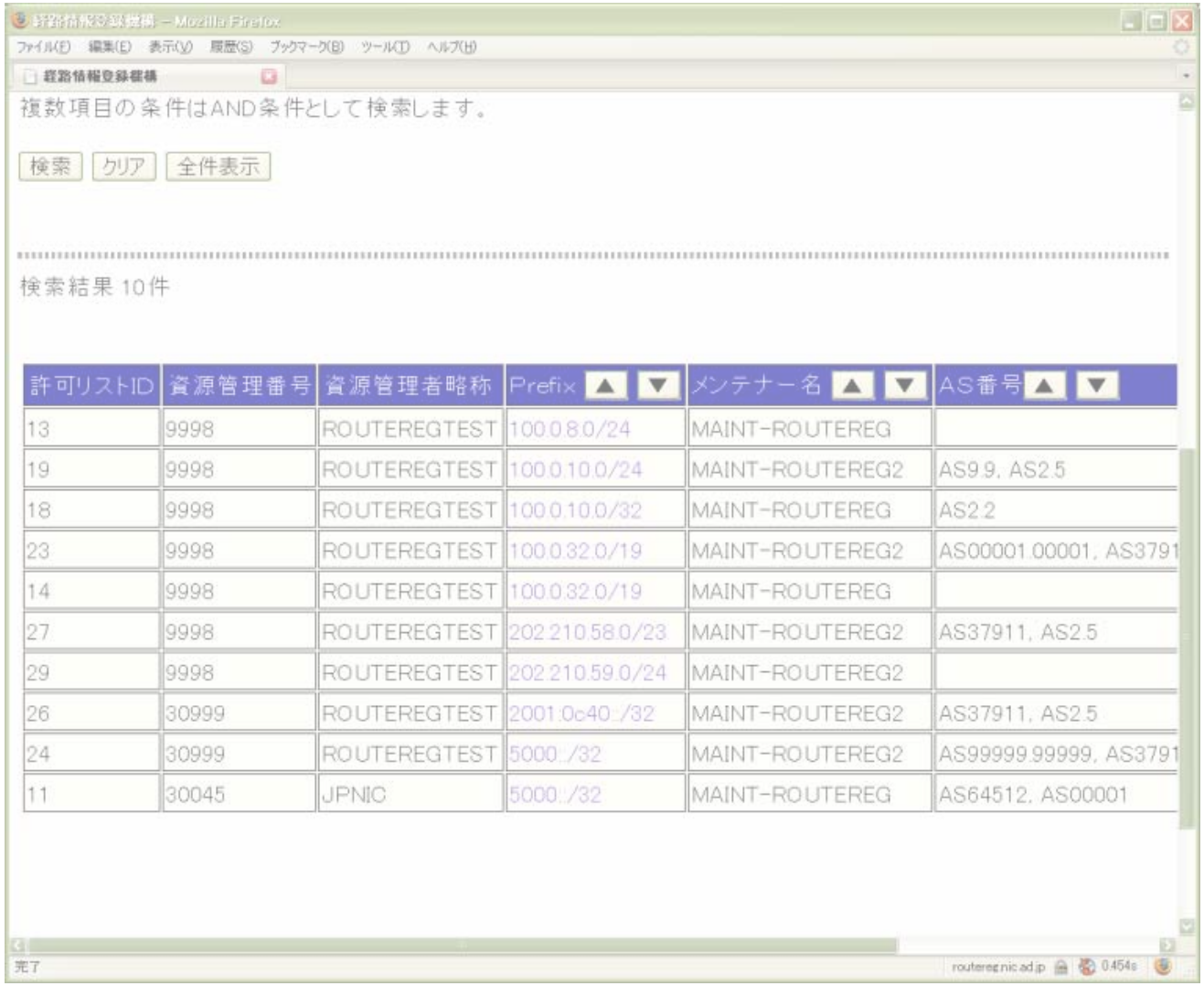

JPNIC認証局
連携
JPIRR
ポイント3
許可のチェック
IPレジストリシステム
prefixのチェック
経路情報の登録認可機構
オブジェクトの登録
ポイント2
電子証明書
ポイント1
認可登録
・割り振り申請
・割り当て報告
認可
オブジェクト登録者
IP指定事業者の
資源申請者

経路情報の登録認可機構の画面（1）

経路情報の登録認可機構の画面（2）



経路情報の登録認可機構の画面（3）



今後の実験の考え方

- **第一段階　(2008年1月めど、参加者による実施)**
  - **許可リストを利用してIRRのオブジェクトを管理できることを確認する**
    - **実験用IRR利用**
    - **不正なrouteオブジェクトの登録ができないことを確認**
    - **「正しい」routeオブジェクトを試験的に蓄積**
- **第二段階　(主にJPNICによる実施)**
  - **JPIRRに登録されたオブジェクトとの比較、分析**
    - **実験用IRRとJPIRRの両方を利用**
    - **不適切なオブジェクト(JPIRR)または不適切な認可(経路情報の登録認可機構)を分析、対策手順を検討**
- **第三段階**
  - **JPIRRへの適用**
    - **JPIRRを利用**
    - **適切なrouteオブジェクトを蓄積**
- **第四段階**
  - **JPIRRを用いた経路ハイジャックの検知　など**

実験利用に必要なもの

- JPIRRにオブジェクトを登録する方（オブジェクト登録者）
  - メンテナー名
    - JPIRRにメンテナーを登録している必要があります。
  - 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ています。
- IPアドレスの割り振りを受けている方（IP指定事業者）
  - 資源管理証明書（クライアント証明書）
    - 認証強化実験に参加している必要があります。
  - 業務上、IPアドレスに対して経路広告されるメンテナー名を把握しておく必要があります。

お問い合わせ先など

- **経路情報の登録認可機構**
  - **経路情報の登録認可機構とは**
    http://www.nic.ad.jp/ja/research/ca/routereg-outline.html
  - **ご利用の流れなど**
    http://www.nic.ad.jp/ja/research/ca/jpirr/
  - **お問合せ先**
    ca-query at nic.ad.jp