

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



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す」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ページをご覧ください。
 - <http://www.nic.ad.jp/ja/research/ca/routerreg-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

- 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チェック

IPレジストリシステム



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	

- 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



IP指定事業者の
資源申請者

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

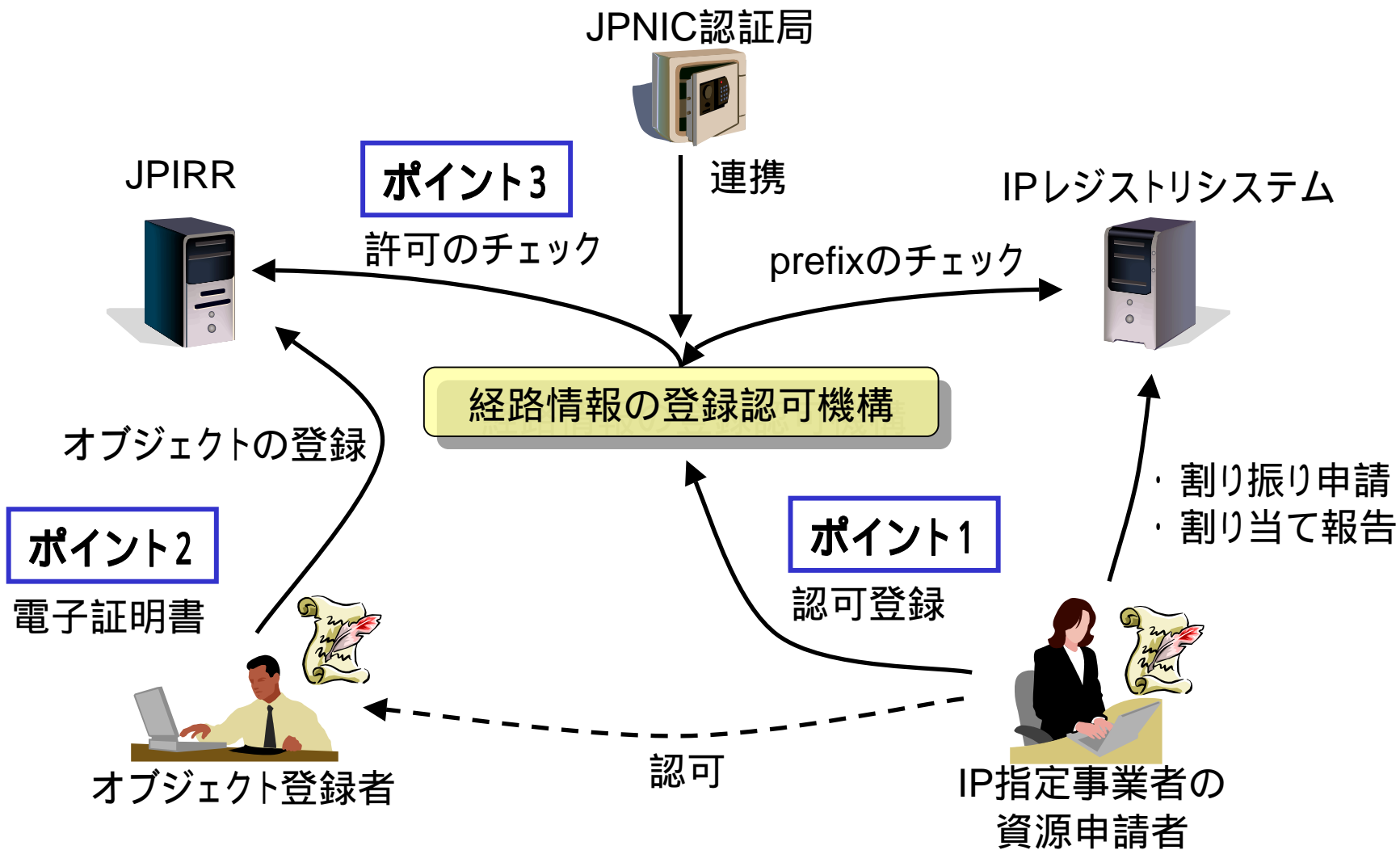
prefix (登録できる範囲)	許可 / 禁止	メンテナー	Origin AS (optional)
1.1.0.0/16	allow	mnt1	12345
1.1.0.0/17	allow	mnt2	



・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



経路情報の登録認可機構の画面(1)

The screenshot shows a web browser window titled "経路情報の登録認可機構 - Mozilla Firefox". The address bar contains "経路情報登録機構". The page header features the JPNIC logo and the text "日本ネットワークインフォメーションセンター Japan Network Information Center".

The main content area includes a login field with the text "ログインID" and the value "IRR-AD Taiji Kimura 01". Below this, it says "JPNIC 担当者".

A navigation menu contains the following items:

- TOP
- 許可リスト
- 利用者管理
- 新規登録 検索
- JPIRRクライアント証明書管理者新規登録 検索

The main section is titled "許可リスト一覧". Underneath, there is a "検索条件入力" (Search Condition Input) section with the following fields:

- 許可リストID:
- 資源管理番号:
- 資源管理者略称:
- IPバージョン:
- Prefix:
- メンテナー名:
- AS番号:
- allow/deny:
- 登録者種別:

Below the search fields, it states: "複数項目の条件はAND条件として検索します。"

At the bottom of the search section, there are three buttons: "検索" (Search), "クリア" (Clear), and "全件表示" (Show All).

The browser status bar at the bottom shows "完了" (Completed) and the URL "router.nic.ad.jp".

経路情報の登録認可機構の画面(2)

経路情報登録機構 - Mozilla Firefox

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

経路情報登録機構

ログインID IRR-AD Taiji Kimura 01

JPNIC担当者

TOP 許可リスト 利用者管理

新規登録 検索 JPIRRクライアント証明書管理者新規登録 検索

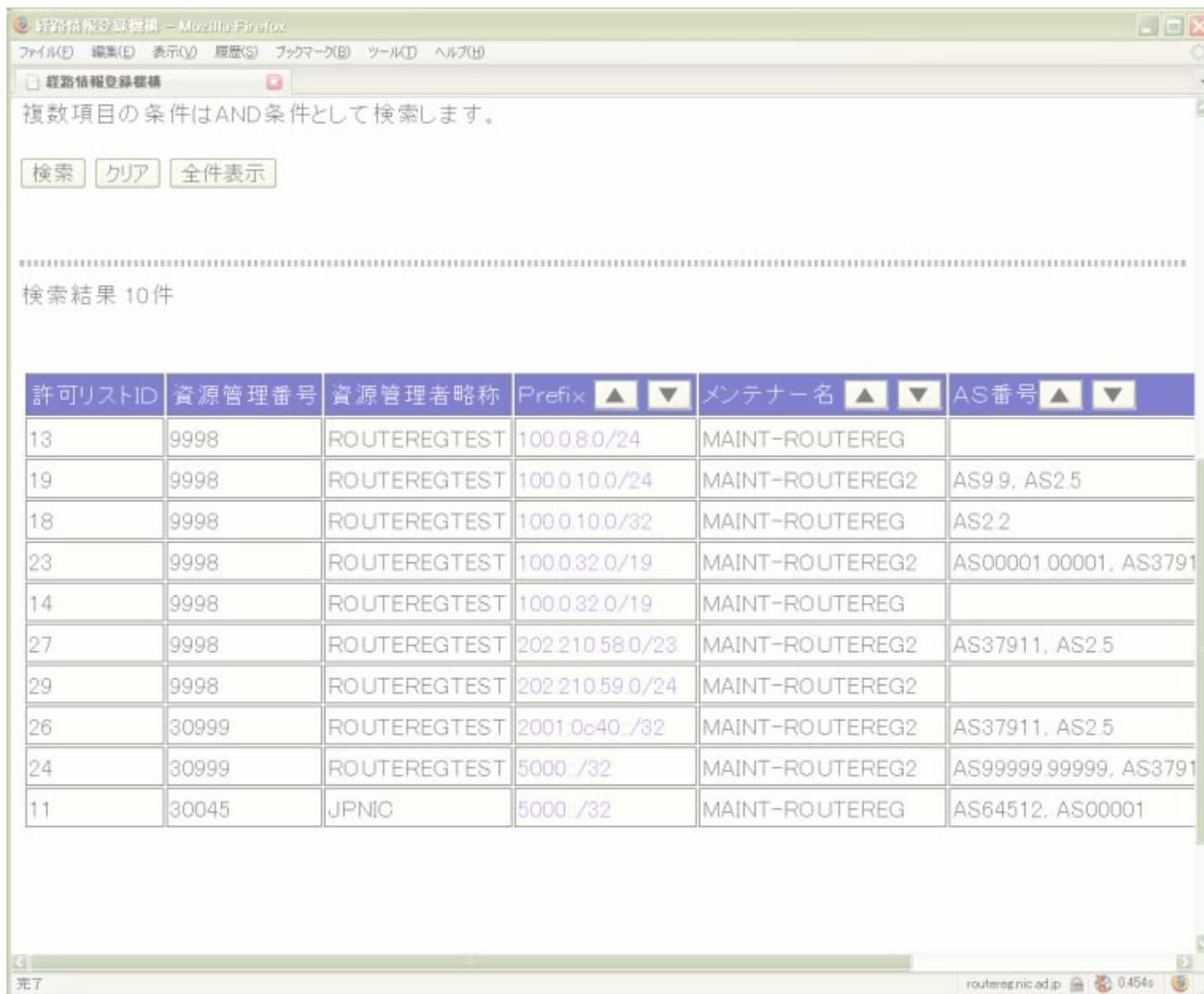
許可リスト登録

資源管理者略称(*) (半角英数字, 記号)	<input type="text"/>
Prefix(*) (v4[172.168.0.0/16], v6[2001:db8::/32])	<input type="text"/>
メンテナー名(*) (半角英数字, 記号)	<input type="text"/>
AS番号 (半角英数字, 記号 カンマ区切りで複数入力可)	<input type="text"/>
allow/deny(*)	allow <input type="button" value="v"/>

(*)は必須入力

完了 routereg.nic.ad.jp 0.406s

経路情報の登録認可機構の画面(3)



経路情報の登録認可機構 - Mozilla Firefox

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

経路情報登録機構

複数項目の条件はAND条件として検索します。

検索 クリア 全件表示

検索結果 10件

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, AS37911
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, AS37911
11	30045	JPNIC	5000./32	MAINT-ROUTEREG	AS64512, AS00001

完了 routerreg.nic.ad.jp 0.454s

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/>
 - お問い合わせ先
ca-query at nic.ad.jp