経路情報の登録認可機構について

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

はじめに

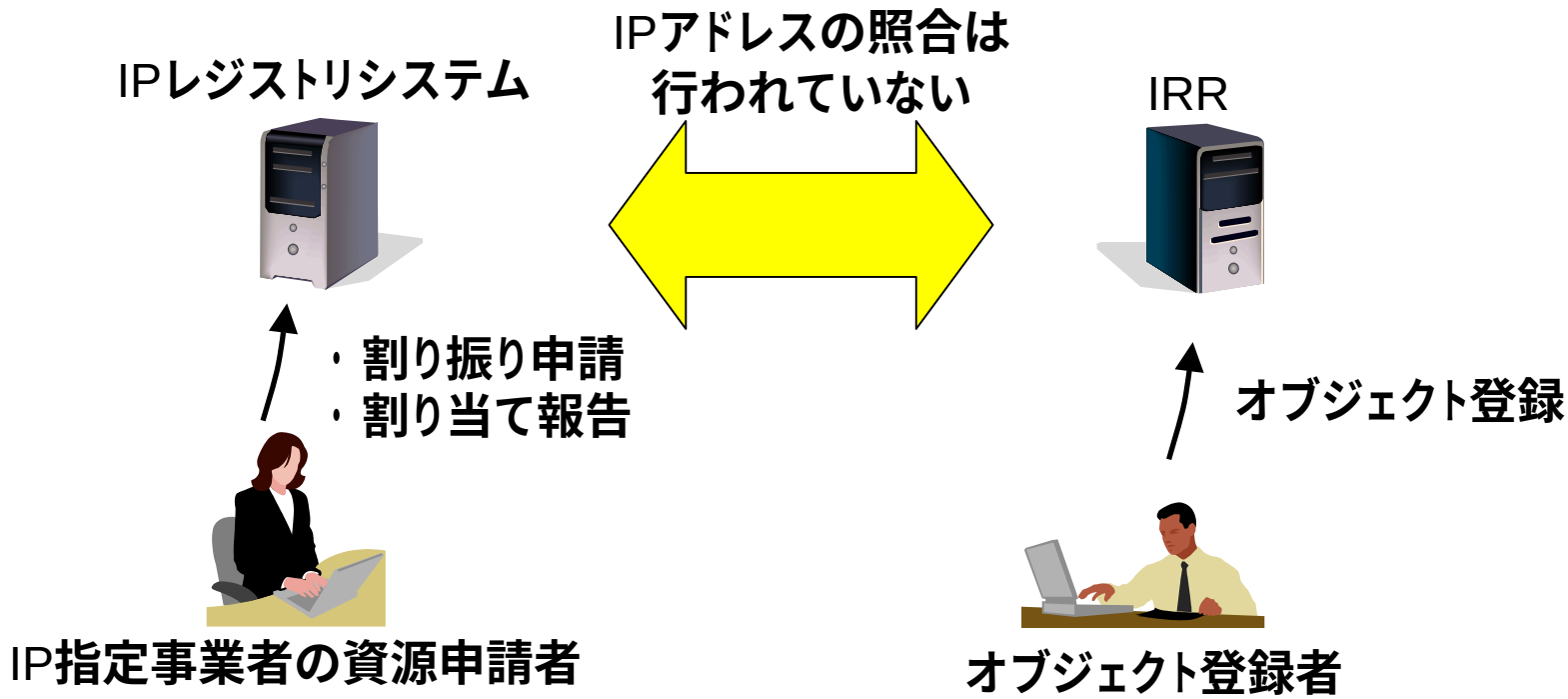
- 現在利用実験を行っている「経路情報の登録認可機構」についてご紹介致します。
  - 実施中の利用実験について
  - 「経路情報の登録認可機構」のご紹介
    - 目的と機能、背景
  - 利用実験の参加方法

実施中の利用実験について

- 2007年12月以降、指定事業者の皆様を対象にした利用実験を行っています。
  - 実験の目的
    - 本機構を使った業務の実行可能性を検証
  - 実験期間
    - 2007年12月以降～2009年3月末
    - 実験結果を受けて継続運用を検討
  - 実験の対象
    - 参加を希望されるIP指定事業者、及びJPIRRの登録者
    - 電子証明書を用いた指定事業者認証強化サービスを利用
  - 参加費用
    - 無料　（USBトークンを無償で貸し出し）

経路情報の登録認可機構の紹介

開発の背景



IPアドレスの割り振り／割り当てに関わらず、IRRには不適切なprefixが登録される可能性がある。

不適切なprefix： 他のISPのprefix、未割り振りのprefix

⇒ **これではIPアドレスが、使ったもの勝ちの状態**

経路情報の登録認可機構の目的

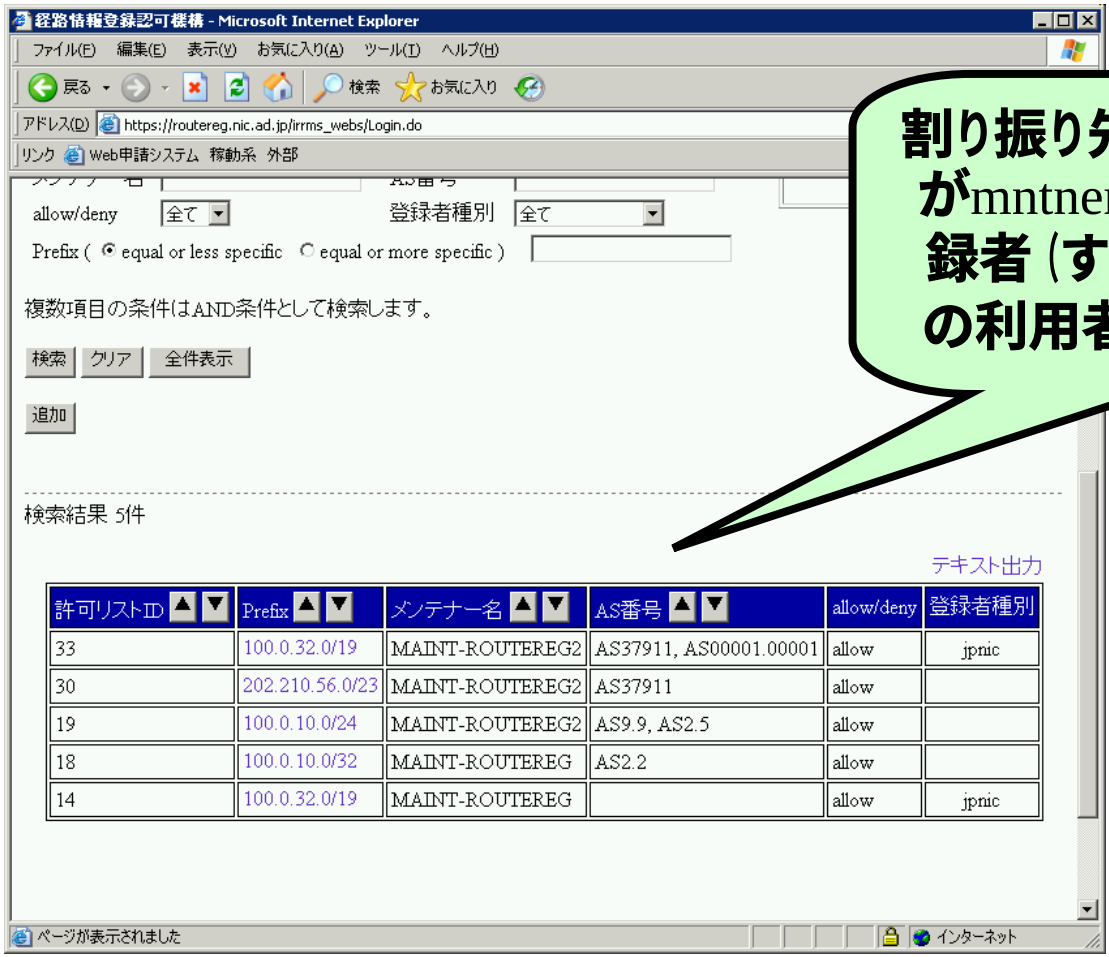
JPIRRに情報が登録される前に、WHOISの情報と照合し、JPIRRに不正な情報が登録されるのを防ぐ。

経路情報の登録認可機構の機能

割り振り先組織によって指定されたメンテナー（JPIRRのmnter）だけが、割り振り済みIPアドレスが入ったオブジェクトをJPIRRに登録できるように制限する。

資源申請者によるmntnerの指定

- 許可リスト



割り振り先の「資源申請者」がmntnerを指定し、IRR登録者（すなわちIPアドレスの利用者）を制限できる。

JPIRRにおける登録制限

- JPIRRの登録者認証と
  アクセス制御

指定されたmntnerだけが、routeオブジェクトを登録できる。S/MIMEでなりすましを防ぐことが可能。

利用実験の参加方法

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
    - 認証強化サービスで使われているもの
  - 経路広告されるメンテナー名を把握
- JPIRRユーザ
  - S/MIME対応メールソフト
    - Thunderbirdなど
  - USBトークン
    - JPNICより無償で貸し出し

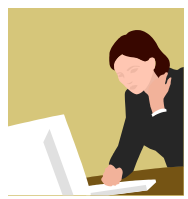
ご利用までの流れ（IP指定事業者の電子証明書）

1. 認証強化実験の参加申し込み（申込書の郵送）

2. 管理者用証明書（資源管理カード）を取得

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
   経路情報の登録認可機構を利用開始



ご利用までの流れ（JPIRRのメンテナー）

1. mntnerオブジェクトを登録 ＋実験の参加申込

2. 管理者用証明書を取得

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. オブジェクト登録者がS/MIMEを使ってJPIRRに
オブジェクトを登録

情報源

- 経路情報の登録認可機構
  - 経路情報の登録認可機構
    http://www.nic.ad.jp/ja/research/ca/routereg-outline/

- 指定事業者の認証強化サービス
  - 資源管理証明書
    http://www.nic.ad.jp/ja/research/ca/lir-certificate/

是非、利用実験にご参加下さい。
ご意見、ご希望などをお寄せ頂ければ
幸いです。

JPNIC**電子証明書担当窓口**
ca-query@nic.ad.jp

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

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）