

## 第4章 IPアドレス認証の展開に関する 調査研究

### 内容

- 経路情報の登録機構のポイントとディスカッション
- 経路情報の登録機構の実験と改修
- 経路情報の登録機構の応用

ほか

## 4. IP アドレス認証の展開に関する調査研究

平成 14 年度から平成 16 年度にかけて、「IP アドレス認証局」と呼ばれる認証局に関する調査研究を行った<sup>1</sup>。「IP アドレス認証」という言葉は、この時に作られた言葉である。

JPNIC は日本国内で唯一、IP アドレスの登録管理業務を行うための組織「インターネットレジストリ」である。IP アドレスはインターネットにおけるホストの識別子であることから、認証技術と組み合わせることで様々なセキュアネットワークサービスが考えられる。IP アドレス認証の調査研究が開始した当時は、その様々なセキュアネットワークサービスのあり方を考える調査研究活動を行った。この中で軸として考えられていたのは、JPNIC において信頼点となる認証局、ルート認証局を立ち上げることである。この認証局の立ち上げについては、2002 年度から 2004 年度にかけて調査研究が行われた。

しかし、認証局を運用するということは、事業の方向性について検討を要するほどに影響のあることであった。認証局は「電子証明書」を発行する機関であるが、その電子証明書で「証明される」内容は、予め証明に足る情報であることが確認されていなければならない。証明に足らない情報を証明しても、単に情報伝達に電子証明書という仕組みを作るだけになってしまい、その仕組み作りが目的化しかねない。そこで、JPNIC という IP アドレスを管理する組織が、どのような情報の証明を行い、それがどのように使われていくべきかを考える必要がある。

ところで、先に述べた IP アドレスにはホストの識別子の他に、もう一つの役割がある。経路制御（ルーティング）の識別子である。ここではインターネットルーティングの詳細は述べないが、IP アドレスの登録管理業務は必然的にルーティングにも影響してしまう。例えば、あるネットワーク利用組織から IP アドレスの返却があるとき、そのネットワーク利用組織は、インターネットにおける経路情報を失わなければ、IP アドレスを使わない状態になったとは言えない。逆に、インターネットにおける経路情報さえあれば、IP アドレスの割り振りを受けていなくても IP ネットワークの到達性を得ることが技術的に可能である。

本調査研究の結果、「IP アドレス認証」は JPNIC における登録情報を不正な書き換えから守り、そして登録情報を正常なインターネットルーティングに役立てるような仕組みになった。JPNIC 認証局は、IP アドレスの割り振りを受け、その IP アドレスに関する情報を JPNIC に登録するユーザの認証と、JPNIC における IRR (JPIRR) に、経路情報を登録するユーザの認証と認可を実現するための電子証明書を発行することとなった。

2007 年度は、経路情報を登録するユーザの認証と認可を実現する「経路情報の登録機

<sup>1</sup> JPNIC 認証局 受託研究の報告書  
<http://www.nic.ad.jp/ja/research/ca/>

## 第4章 IP アドレス認証の展開に関する調査研究

構」の実験運用を開始し、国内外における発表と議論を重ねることとなった。実験システムである為、JPNIC において全面的な導入を図るなどの利用者増は望めなかったが、利用者からのフィードバックを得ることができた。また他の地域（アメリカやヨーロッパ、アジア太平洋地域など）のレジストリの取り組みを現地調査し、比較検討することで、インターネットレジストリにおける経路制御への関与が、どういう意味を持つかがわかった。

本章では、IP アドレス認証の展開に関する調査研究の一環として行った経路情報の登録機構の開発と、国内外でこれについて発表と議論を行ってきた結果について述べる。

### 4.1. 経路情報の登録機構の開発と調査研究

IP アドレス認証の展開に関する調査研究では、「経路情報の登録機構」を開発し、国内外での発表および議論と、実験運用を行った。経路情報の登録機構は、JPIRR( JPNIC で運用されている Internet Routing Registry ) の登録情報の正当性を維持するシステムである。

2008 年 3 月の段階でエンドユーザとしての利用実験に参加したのは 4 社で( この他に利用可能なユーザは 6 社以上 ) あった。

また APNIC や IEPG などの国際会議で発表や、JANOG 等での発表を通じて、本機構で向上する IRR の信頼性や課題点に関する議論を行うことができた。重要性の高い課題点については改修を行い対策を取った。

### 4.2. 経路情報の登録機構を使った実験の考え方

経路情報の登録機構を使った実験は、いくつかの段階に分けて行われるものとした。

## 実験の考え方

- 第一段階（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

図 4-1 実験の考え方

第一段階の実験は、登録者による利用実験である。本機構は IP アドレス管理業務を行っているものに利用されることが実験である。業務の中にうまく組み込むことが可能かどうかの検証を行う。それに先立って割り振られた IP アドレスが、他の組織によって経路情報として不正に登録されることを避けられることが理解される必要がある。

第二段階の実験は、データ分析である。本機構によって正当性の担保されたデータが蓄積されると、既存の IRR における不適切なオブジェクトが判別できるようになる。その原因や対策を検討する。

第三段階と第四段階は、実際に JPIRR に本機構を提供し、ルーティング業務において利用する実験である。

### 4.3. 経路情報の登録機構とは

経路情報の登録機構(以下、本機構と呼ぶ)は、インターネットにおける経路制御の安全性向上のため、JPIRR で提供される経路に関する情報(route オブジェクト)の正当性の向上と維持を図るシステムである。本機構を使うことで、自組織以外のネットワークによる route オブジェクトの不正登録(設定ミスを含む)を防ぎやすくなる。JPIRR における登録情報を使ったインターネット上の不正な経路情報を、より正確に検知できるようになり、経路ハイジャックの予防等に役立つと考えられる。

## 第4章 IP アドレス認証の展開に関する調査研究

本機構の三つのポイントを以下に示す。

- ポイント1 - 割り振られた IP アドレスが経路広告で使われる組織の指定
- ポイント2 - JPIRR のオブジェクト登録者に対するユーザ認証の強化
- ポイント3 - 認可登録に基づいた JPIRR への route オブジェクトの登録制限

これらの仕組みを実現するため、本機構は JPNIC で運用されている JPNIC 認証局、IP レジストリシステム、JPIRR の三つと連携する。本機構がどのようにこれらのシステムと連携動作するかを図 4-2 に示す。

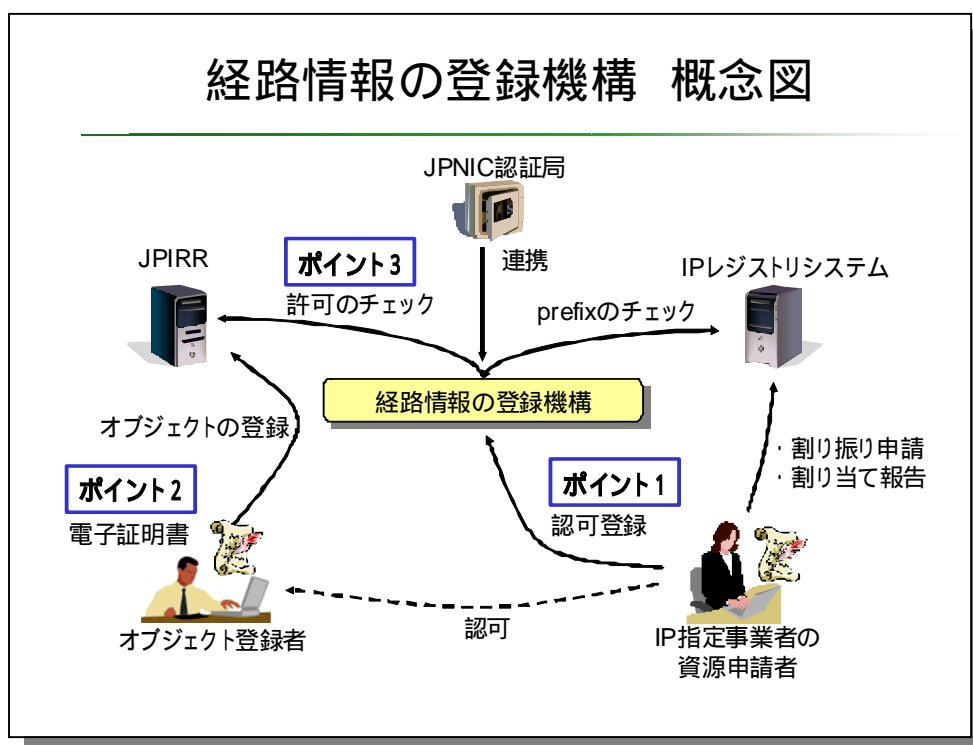


図 4-2 経路情報の登録機構 概念図

IP レジストリシステムは、IP アドレス管理指定事業者（以下、IP 指定事業者）による IP アドレスの割り振り申請や割り当て報告などのために使われているシステムである。「Web 申請システム」と呼ばれる申請用のシステムは、IP レジストリシステムによって提供されている。一方、JPIRR は AS 番号が割り振られている個人またはネッ

トワーク運用組織のオブジェクトの登録のために使われている。

本機構は、IP 指定事業者に割り振られている IP アドレスに関する情報を IP レジストリシステムから取得し、JPIRR に登録される route オブジェクトの IP アドレスが正当なものであるかどうかをチェックする。ここでいう正当性は、IP アドレスが IP 指定事業者に割り振られているか、ということに加え、割り振り先の IP 指定事業者から、JPIRR のオブジェクト登録者であるメンテナーに対して、その登録が認可されているかどうか、という意味である。この正当性の確認のため、本機構は許可リストと呼ばれるデータベースを持ち、IP 指定事業者に対して認可登録の Web インターフェースを提供する。

以下、各々の仕組みについて説明する。

#### ポイント 1

一つ目は、IP アドレスを割り振られた IP 指定事業者がその IP アドレスの利用をネットワーク運用組織に認可するための、「許可リスト」と呼ばれるデータベースである。

本機構は、IP 指定事業者が認可登録を行うデータベース「許可リスト」を提供する。許可リストは、IP アドレスがどのメンテナーに利用されるかを示すリストで、どのメンテナーがどの IP アドレスを含む route オブジェクトの登録ができるか、という情報を持つ。許可リストで認可登録のできる IP アドレスは、その認可を行おうとしている IP 指定事業者に割り振られた IP アドレスのみである。さらに認可登録の追加項目として、AS 番号を指定することもできる。これによりインターネットにおいて特定の AS から経路広告が行われるような認可登録ができる（図 4-3）。

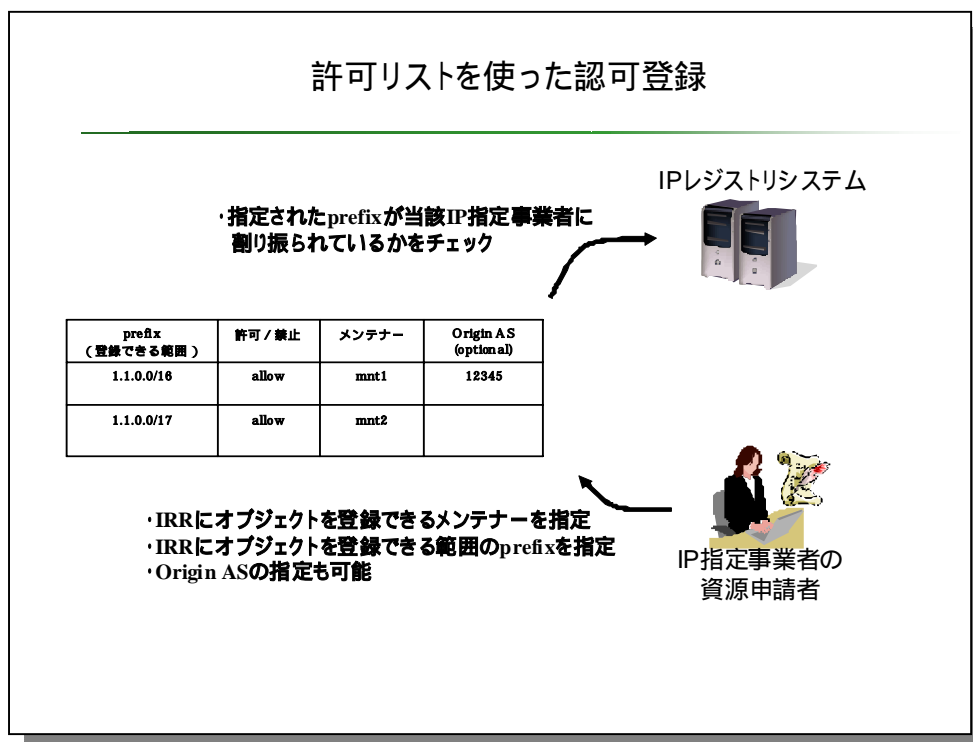


図 4-3 許可リストを使った認可登録

## ポイント 2

二つ目は JPIRR におけるオブジェクト登録者に対するユーザ認証に、電子証明書を使う点である。

本機構では、JPIRR における情報登録者を、「メンテナー管理者」と「オブジェクト登録者」という二種類のユーザとして認識する。メンテナー管理者は JPIRR のメンテナーオブジェクトで admin-c や tech-c として登録されているユーザで、次に述べるオブジェクト登録者の電子証明書を管理できる。オブジェクト登録者は、JPIRR に route オブジェクト等の登録ができるユーザである。どのユーザも本機構から発行されたユーザ向けの電子証明書 (クライアント証明書) を使ってアクセスする。本機構が提供するクライアント証明書を使うことで、これまでの認証方式であるパスワードや PGP に比べ、ユーザの管理を適切に行いやすくなる。本機構が持つ電子証明書の管理機能は、悪意のある第三者による成りすまし行為が起こった場合に、証明書を即時に失効させるなどの事後の対策を取りやすくしている (図 4-4)。

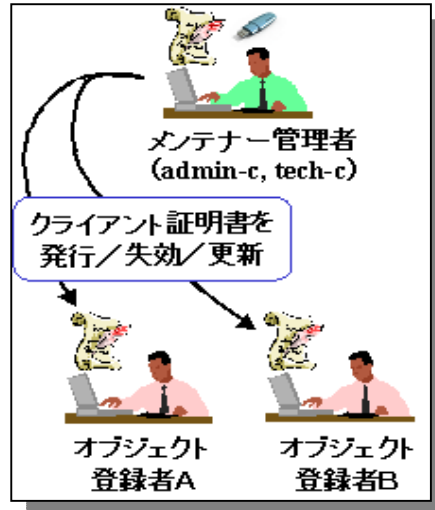


図 4-4 ユーザの違いと役割

メンテナー管理者は JPIRR のメンテナーオブジェクトを管理できるユーザで、メンテナーオブジェクトの内容を編集できる。またオブジェクト登録者のクライアント証明書を発行/失効/更新を行うことができる。オブジェクト登録者のクライアント証明書は認証トークンに入っており、この認証トークンを使って、これらの管理業務を行う(図 4-5)。

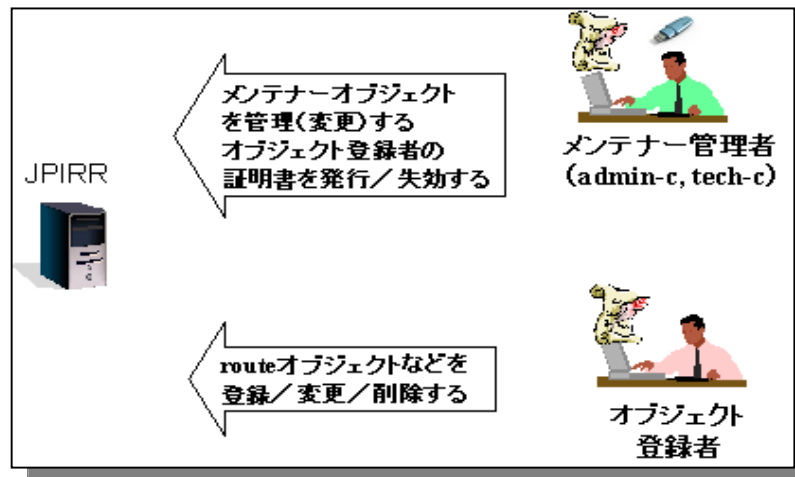


図 4-5 ユーザ毎の登録業務の違い

### ポイント3

三つ目は、許可リストを使った、JPIRR でのアクセス制御である。許可されたメンテナーだけが、特定の IP アドレスを含む route オブジェクトを JPIRR に登録できるようになることである。



## 第4章 IP アドレス認証の展開に関する調査研究

本機構は JPIRR に route オブジェクトが登録される際、申請データの内容を許可リストに基づいて検査し、JPIRR に登録するか登録を拒否するかの制御を行う。IP 指定事業者によってメンテナーが指定されていない IP アドレスなどが、JPIRR に登録されることを防ぐ(図 4-6)。

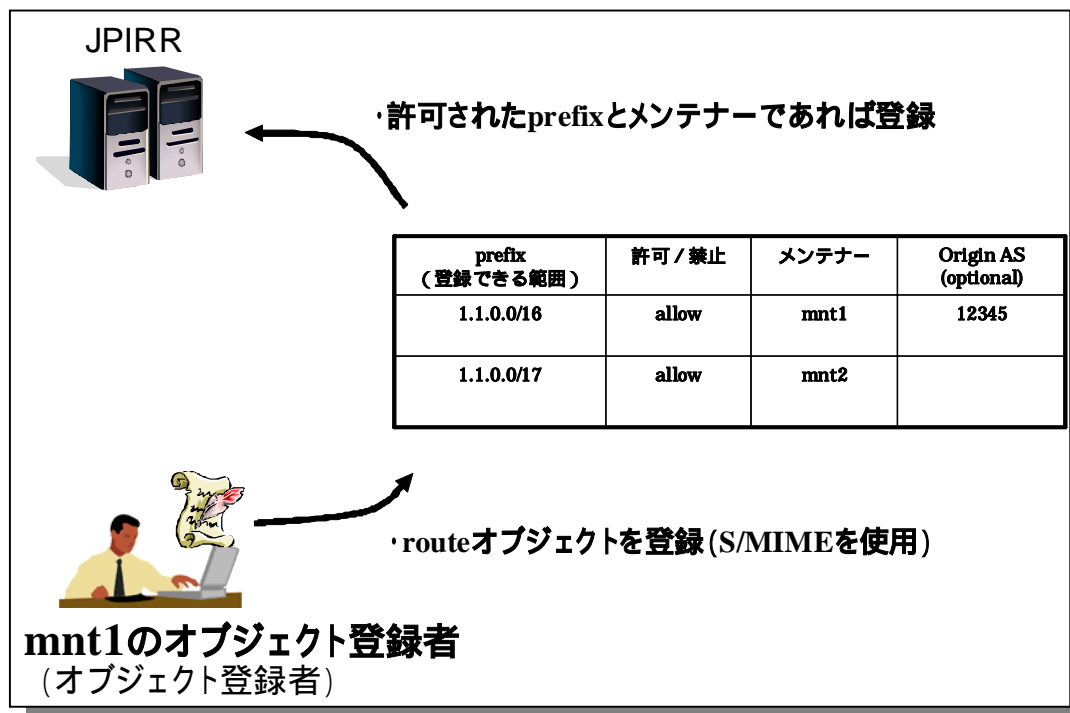


図 4-6 route オブジェクトに対するチェック

本機構を通じて route オブジェクトの正当性を維持することで、JPIRR に不正な route オブジェクトが登録されることを防ぐことが可能になる。この仕組みが適切に運用されれば、JPIRR が、経路ハイジャックの検知等に一層役立つと考えられる。

### 4.4. 経路情報の登録機構を使った IP アドレス関連の業務

経路情報の登録機構は、いわば IP アドレスの管理とインターネットルーティングの業務を連携させるシステムである。IP アドレスの管理という観点では、インターネットに接続するネットワークの管理業務において、IP アドレスに関わる業務は大きく分けて 3 つある(図 4-7)。

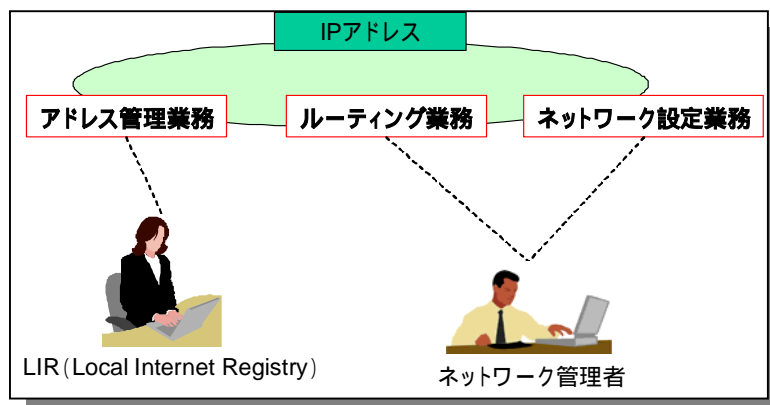


図 4-7 IP アドレスに関連する 3 つの業務

一つ目は IP アドレスの割り振りを受けそのアドレスを管理する業務(アドレス管理業務)である。LIR(主に IP 指定事業者)がその役割を担っている。二つ目は割り当てられた IP アドレスからインターネットルーティングのためのネットワークの設計を行う業務(ルーティング業務)である。これはネットワーク管理者が行っている。三つ目は到達性が確保された IP アドレスをネットワーク機器に設定し、ユーザの接続性を確保する業務(ネットワーク設定業務)である。ネットワーク設定業務もネットワーク管理者によって行われる。ここでネットワーク設定業務を二つに分けた理由は、ルーティング業務とネットワーク設定業務を行う会社や部署が異なるケースが多いためである。

本機構は、このうちアドレス管理業務とルーティング業務を結びつける役割を持っている。ネットワーク設計業務とルーティング業務は、IP アドレスの観点では密接に連携しており、ルーティングの設定が行われていない IP アドレスをネットワーク設定業務で使うことは、インターネットの接続性という観点では直接的には意味がない。

一方、アドレス管理業務とルーティング業務では、特に今日のように ISP の業務細分化が進んでいると、IP アドレスに関する業務の関連性が失われがちである。例えば、ある ISP が IP アドレスの割り振りを受け、ISP 事業で使う際、ルーティング業務を行っている ISP 事業者はそのアドレスの経路広告を委託することがある。この場合、一見割り振られた IP アドレスとインターネットルーティングが一貫性を持っているように見えるが、実はそうではない。他の ISP が IP アドレスの打ち間違いなどを起こしても、IP アドレスの割り振りを受けている事業者にはそのことがわからない。つまり IP アドレスの割り振り先と、ルーティング業務を行う事業者が一方向かつ疎な関係にあると言える。

アドレス管理業務を行っているものとルーティング業務を行っているものが、IP アドレスの利用において密な関係を持つにはどのようにすればよいのか。本調査研究では、許可リストと呼ばれる、ルーティングで IP アドレスを用いる組織を指定する仕組みを提供することにした。こうすることで、割り振りを受けている組織が、意図しない他の組

## 第4章 IP アドレス認証の展開に関する調査研究

織によって IP アドレスを利用されてしまったときに、それがわかるようになる。そして許可リストに則った経路の情報は、IRR に格納されるものとした。

ルーティング業務では、不適切な IP アドレスの利用、すなわち不適切なルーティングの情報は、経路フィルターと呼ばれる仕組みを使って防がれている。経路フィルターとは、予め不適切とわかっている IP アドレスの経路情報がルータに伝わってきたときに、それをフィルター（遮断）し、ルータの経路制御処理が適切に行われないようにする仕組みである。経路フィルターは特定の Web ページで公開されている、BOGON リストと呼ばれる「経路広告には不適切な IP アドレスのリスト」を使って実施されたり、IRR を使って実施されたりしている。すなわち、ルーティング業務においては、BOGON リストや IRR が、経路情報の正しさを示す指標として考えられている。

### 4.5. 許可リストを使った IP アドレス管理業務

許可リストを使った IP アドレス管理業務は、割り振り申請や割り当て報告を行った IP アドレスを許可リストに登録するという手順で行われる。許可リストは、IP アドレスが登録されるリストであり、次の節で述べる IRR への登録業務の中で使われる。

図 4-8 は、JPNIC で実験的に運用されている IP アドレス認証局と、経路情報の登録機構を使った、IP アドレス管理業務の手順を示したものである。

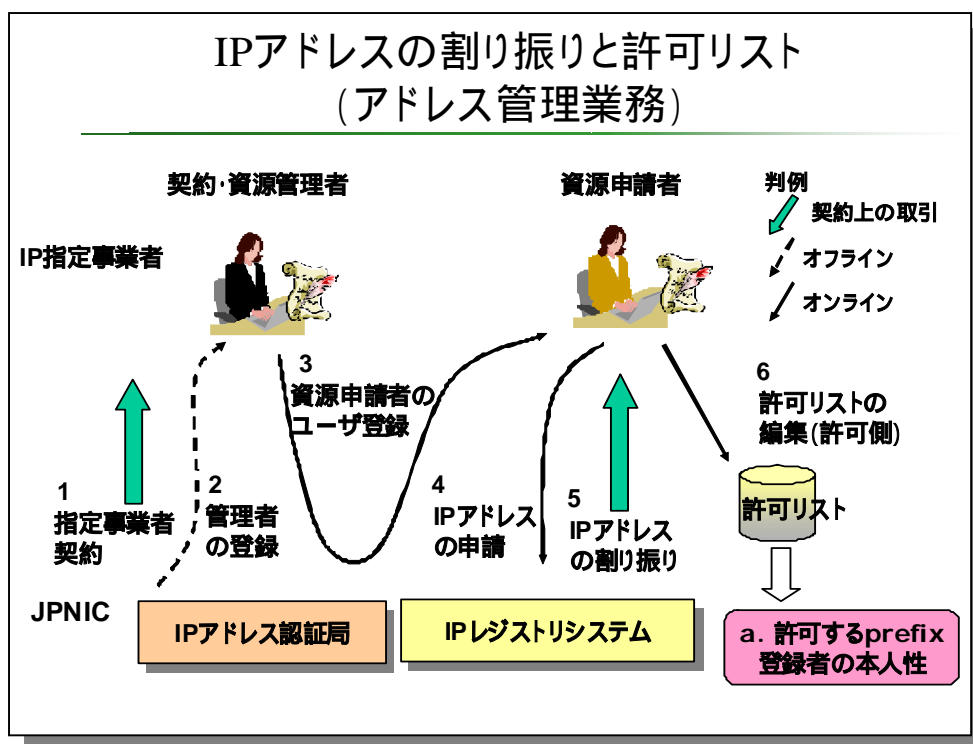


図 4-8 IP アドレスの割り振りと許可リスト

図 4-8 中の矢印は、業務が実施される順番である。はじめにレジストリから IP アドレスの割り振りを受け、IP アドレス管理業務を行うための「指定事業者契約」を結ぶ。これは一度行われてしまえば、その後の IP アドレスの各種申請において逐一行われるものではない。JPNIC 認証局 (IP アドレス認証局) は、この段階で IP 指定事業者の「契約・資源管理者」に電子証明書を発行する (1、2)。契約・資源管理者は、IP 指定事業者の契約情報や資源管理情報を登録・変更・削除できるユーザである。実際の IP アドレスに関する各種申請は「資源申請者」によって行われる。資源申請者は、契約・資源管理者によってユーザ登録される (3)。IP アドレスの申請は資源申請者が担当して実施される (4、5)。最後に割り振られた IP アドレスについて許可リストに登録する (6)。

許可リストへの登録の段階で重要なのは二点である。一つ目は prefix が資源申請者の属する IP 指定事業者に割り振り済みであり、二つ目は登録を行った資源申請者の本人性が確認されていることである。一点目は、許可リストへ登録される段階で、割り振り / 割り当て情報を持つ IP レジストリシステムと照合することで確認される。二点目は、IP アドレス認証局の電子証明書を使って本人性が担保される。

許可リストに登録された prefix は JPIRR への登録の段階で使われる。

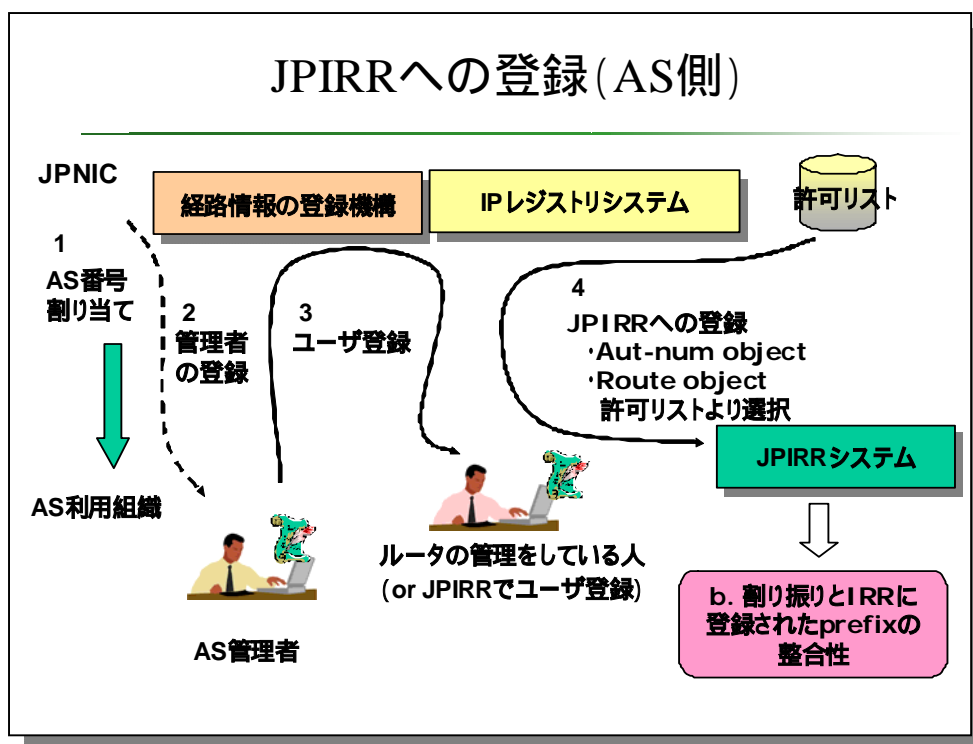


図 4-9 JPIRR への登録 (AS 側)

インターネットにおける BGP を用いたルーティング業務には、AS 番号が必要である。予め AS 番号の割り当てを受けておく必要がある (1)。経路情報の登録機構は、AS 番号の割り当て先の管理者「AS 管理者」に電子証明書を発行する。AS 管理者は資源申請者と同様に、JPIRR に登録業務を行うユーザに電子証明書を発行する (2、3)。このような仕組みは、JPIRR に情報登録を行うユーザが、業務管理を行う AS 管理者とは地理的に離れているケースがあり、またルーティング業務が会社のある場所と離れたデータセンターで行われることなどを考慮して設計された。最後に、JPIRR に情報登録を行う際、許可リストを使って登録データの確認が行われ、問題がなければ JPIRR システムに登録される (4)。ここでいう確認は、route オブジェクトと呼ばれる登録データに含まれる、AS 番号と prefix である。この AS 番号と prefix が、前節で述べた登録内容と齟齬がある場合、経路情報の登録機構は JPIRR への登録を行わせないようにする。これにより、IP アドレスの割り振り先が、その IP アドレスがインターネットルーティングの中でどのように使われるかを指定 / 制限することができる。具体的には意図しない AS から自組織に割り振られた prefix がインターネットで経路広告されたとき、JPIRR の登録情報と比較することで、それが不適切な経路情報であることがわかる。

#### 4.6. 経路情報の登録機構の利用実験

本節では 2007 年度に行った経路情報の登録機構の利用実験について述べる。

#### 4.6.1. 利用実験の考え方

2007 年度に行った利用実験は、図 4-1 に示した四つの段階を想定して行った。第一段階は、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ことである。これは LIR が、割り振られた IP アドレスのルーティングの上での制御ができるようになる、という概念を実際の操作を通じて体験してもらうという実験である。同時に 2006 年度に開発した本システムに関して利用上の不具合があれば挙げてもらうことも行った。

#### 4.6.2. 利用実験の手順

第一段階の利用実験については、Web ページにて手順書を公開した<sup>2</sup>。この手順書で示した手順を以下に示す。

- 1、LIR の IP アドレス関連の申請担当者は、自組織に割り振られた IP アドレスを確認する。(資源申請者の操作)
- 2、許可リストを操作し、割り振られた IP アドレスを特定のメンテナーに許可する登録を行う。(資源申請者の操作)
- 3、ルーティング業務を行っておりメンテナーの管理を行っているものは、IRR にオブジェクトを登録する担当者「オブジェクト登録者」の証明書を発行する。(IRR のメンテナー管理者の操作)
- 4、オブジェクト登録者は、許可リストの範囲に入っている IP アドレスと入っていない IP アドレスを、各々 route オブジェクトに登録する。(IRR のメンテナー管理者の操作)

最後に許可リストの設定を通じて、IRR への route オブジェクトの登録に関する制御を意図通りに行われたことを確認する。確認の結果は、手順書の最後にあるチェックシートに記録する。

#### 4.6.3. 利用実験の参加状況

利用実験には IP 指定事業者である 4 社が参加した。この 4 社は、資源申請者の証明書だけでなく、IRR のメンテナー管理者のトークンを取得した。利用者からのフィードバックは、主に電子メールを通じて得られた。

<sup>2</sup> 経路情報の登録認可機構 実験手順書

<http://www.nic.ad.jp/ja/research/ca/routerreg-outline/routerreg-testing-guide-05.pdf>

#### 4.6.4. 利用実験のフィードバック

利用者からは、意図通りの操作ができたことを示す報告があったが、経路情報の登録機構のインターフェースに関する意見はほとんどあがらなかった。

メンテナ管理者のトークンを利用するための技術的な問い合わせがほとんどであった。その中の代表的なものを以下に示す。

##### 利用者からの問い合わせ

「USB トークンを指したままオブジェクト登録者の証明書を取得すると、Web ブラウザではなく USB トークンの方にその証明書がインストールされてしまう。これは技術的な仕様であるか？」

「USB トークンのドライバのインストールはできたが、トークンを使うことができなかった。(以下、利用環境に関する問い合わせなど)」

その他に画面を見せるなどして複数の事業者と情報交換を行った。それらの事業者からは、以下のようなフィードバックがあった。

「許可リストの編集画面で、割り振り済みの IP アドレスを指定する必要があるが、自社は割り振り済み IP アドレスが多く、すべてを常時把握しているわけではない。割り振り済みの IP アドレスを表示するような補助機能が欲しい。」

「メンテナの管理者は、IRR における admin-c であるが、tech-c であることもある。tech-c として登録されている利用者もメンテナ管理者になれるようにして欲しい。」

「許可リストにある IP アドレスの検索機能を充実させて欲しい。検索の際に more specific や less specific といった指定ができるようにして欲しい。」

利用者からの USB トークンに関する問い合わせについては、個別に環境を聞いて対応策を調整するなどした。また上記のフィードバックのうち、経路情報の登録機構の改修が必要なものについては、一旦すべての要件をまとめ、2007 年度中に改修するものとした。

#### 4.7. 経路情報の登録機構の改修

2007年度の調査研究では、経路情報の登録機構の改良を行った。前節までに述べた経路情報の登録機構を使った業務の見直しを行ったが、基本的な業務フローは変更の必要がないことがわかった。一方で、許可リストを操作する画面がIPレジストリシステムのWeb申請システムとは別であることから、利便性が損なわれている状況であった。

2007年度の経路情報の登録機構の改良点を以下にまとめる。

##### 2007年度 経路情報の登録機構の改良点

###### 1. 本機構における割り振り済みアドレス空間の一覧表示

IP指定事業者は割り振られたIPアドレスの空間を把握しながら、本機構を操作する必要があるが、現行のシステムはその情報が表示されない。該当IP指定事業者に割り振られたIPアドレスを表示するように改善する。

###### 2. Windows Vista 対応

Windows Vista では電子証明書に関わるデフォルト機能の仕様に変更があり、本機構で提供している証明書発行機能が利用できない。Windows Vista は普及しつつあるOSであるため、これに対応する。

###### 3. ミドルウェアのアップデート

本機構のプログラムが利用するミドルウェアの不具合を避けるため、アップデートを行う。

###### 4. 証明書発行用アクセスキーのメール通知機能

本機構は、証明書発行の処理を行った後、画面に表示されるアクセスキーの全体を証明書発行対象者に伝達する必要があり、業務が行いにくい。アクセスキーがメールで送られるように改善する。

###### 5. 画面フローの改善および多国言語対応によるユーザビリティの向上

表示される画面の数を減らすと共に、Web ページ表示機能を改善し、ユーザビリティ向上を図る。また本機構は英語圏の技術者にも動向が注目されていることから、英語等での表示ができるようにし、わかりやすさの向上を図る。

###### 6. 許可リスト検索機能の改善

許可リストの検索の項目および表示を変更し、ユーザビリティ向上を図る。

###### 7. 本機構経由で登録されたオブジェクトの識別

本機構を経由して登録されたオブジェクトを識別する仕組みについて、概要設計を行う。

###### 8. 割り振り済みアドレス空間のリアルタイム反映

本機構の許可リストに、割り振り済みアドレス空間をリアルタイムで反映する仕組みについて、概要設計を行



## 第4章 IP アドレス認証の展開に関する調査研究

う。

### 9. ユーザの利用状況確認 Web インターフェース

ユーザの利用状況を確認する Web インターフェースの仕組みについて、概要設計を行う。

1の「本機構における割り振り済みアドレス空間の一覧表示」は、経路情報の登録機構の資源申請者がアクセスする Web ページの改良である。許可リストには自組織に割り振り済みの IP アドレスを登録しなければならないが、ユーザは許可リストの編集画面で割り振り済みアドレスを確認することができない。この点の指摘に対してシステムの改良を行う為、経路情報の登録機構が IP レジストリシステムから割り振り済みの IP アドレスの情報を取得し、一画面で割り振り済みアドレスと許可リストを確認しながら、編集ができるように改良した。

2の「Windows Vista 対応」は、新しい OS である Windows Vista への対応である。Windows Vista に付属する Internet Explorer バージョン 7 では、ユーザ側の鍵生成機能の仕様に変更があることが、2007 年度の後半に判明した。Windows Vista の普及状況を踏まえて今回の改良では、Windows Vista 以前の OS と Windows Vista の両方の Internet Explorer に対応することとした。これは Web サーバ側で通知を受けた、Web ブラウザのバージョン情報に基づいて表示する Web ページを切り替えるだけでよい。しかし Windows Vista は、これまでに使われていた Xenroll から ActiveX の Cenroll が使われるようになり、Cenroll では以前のバージョンで鍵生成を行うことができないことがわかった。

3の「ミドルウェアのアップデート」は Web サーバのソフトウェアを含むバージョンアップである。各種ソフトウェアのバージョンアップはセキュリティパッチの適用などを踏まえると定期的に行われるべきものである。今回のバージョンアップでは、IP レジストリシステムとの連携上の問題が起こらないかどうかの調査を並行して進めながら行った。

4の「証明書発行用アクセスキーのメール通知機能」は資源申請者の証明書発行インターフェースにならった改良である。経路情報の登録機構は JPIRR に情報登録を行うユーザ、オブジェクト登録者の証明書発行の際に、電子メールで「アクセスキー」を通知する機能がない。資源申請者の証明書の場合、契約・資源管理者が証明書発行操作を行うと、資源申請者に対して証明書取得用の URL とアクセスキーの一部がメールで送られる。アクセスキーの残りは契約・資源管理者の画面に表示され、その部分をオフライ

ンで資源申請者に伝えることとなっている。オフラインで伝えることで、契約・資源管理者は資源申請者の本人性確認を行うことができ、本人性確認が行われていない電子証明書発行を防ぐことが可能になる。

5 の「画面フローの改善および多国語言語対応によるユーザビリティの向上」は証明書の発行の際に表示される確認画面を減らすと共に、Web ページを英語表記することである。確認画面については、様々な内部処理を経るためにユーザには冗長と思われる Web ページの表示が行われていた。そこでユーザの観点で類似する確認画面を省き、利便性の向上を図った。

また Web ページに表示されるメッセージを英語でも表示できるようにした。これは、国際会議などでデモンストレーションを行ったり、画面を見せて説明を行ったりする際に、日本語の表示だけでは操作の意図が理解されなかったためである。IRR を使うようなルーティング業務は、日本人だけで行われているわけではなく、英語を母国語としていて日本の IRR に登録を行うユーザも想定される。今回の改修では RIR で議論されている IP アドレスの authorize 関連のディスカッションで使われていた用語を用いた。

6 の「許可リスト検索機能の改善」は許可リストの操作上の改良である。許可リストは IP アドレスの列挙である為、編集の際に目的とするエントリを探しにくい。特にルーティングで用いられている IP アドレスの指定方法が利用できなければ、IP アドレス管理業務に携わっているユーザには使いにくい。この検索機能の改良は、大手 ISP のルーティング業務を行っている業務担当者に指摘を受けたものである。具体的には、less specific となる IP アドレスと more specific となる IP アドレスを検索できるようにした。less specific と more specific はルーティング業務の中ではよく使われる概念である。なお less specific では、検索結果に入力した IP アドレスが含まれず、実際には less specific or equal (等しいかより少ない指定) という検索条件とした。more specific についても同様である。

7 の「本機構経由で登録されたオブジェクトの識別」は本機構を使って登録された登録情報 (route オブジェクト) が、JPIRR の中で他の route オブジェクトとは区別される仕組みの概要設計である。本機構を使って登録された route オブジェクトは、割り振りが確認されているなど、他の route オブジェクトとは位置づけが異なる。JPIRR を検索したものが本機構を通じて登録されたものとそうでないものを区別することで、例えば経路ハイジャックの判断の際に役立てることができる。巧妙な経路ハイジャックは、IRR に登録された情報から詐称し、あたかも正しい経路であるかのような状況を作ることができると考えられることから、この機能は重要である。しかし 7 の仕組みを実現するには IRR の書式確認機能に改良を加えたり、IRR の登録情報が伝播していくミラー先の IRR の機能確認を行っていったりする必要がある。これにはより長期的な取り組みが

## 第4章 IP アドレス認証の展開に関する調査研究

必要である為、今回は概要設計に留まった。

8の「割り振り済みアドレス空間のリアルタイム反映」は本機構のリアルタイム処理に関する機能向上である。2006年度に作られた本機構はIRRに対する情報登録の申請メールを逐次処理することができない。しかしIRRにオブジェクトを登録するものは、whois コマンドを使って逐次登録されたことを確認しながら業務を行っていることから逐次処理ができることは本機構の課題であった。ISPのルーティング業務担当者によって指摘された。しかし、逐次処理には大量の申請を処理できるような性能の設計が必要であるが、プロトタイプシステムではこれを避ける性能を確保することが難しいため、今回は概要設計に留まった。

9の「ユーザの利用状況確認 Web インターフェース」もルーティング業務の担当者より指摘された機能である。(なおIPアドレス認証局(認証)でも同様に機能が要望として上がっている)ルーティング業務の中で、JPIRRへの登録業務を誰が行ったのかを確認する業務がある。現在は申請に使われた電子メールを申請者側で確認することで業務の確認が行われていたが、オブジェクト登録者の管理がWebページを使って行われるようになることから、過去にどのユーザによって申請が行われたかについて、Webページで確認できるようにしてほしいという要望である。この機能改善についても、業務フローなどの検討を要するため、概要設計を行った。

### 4.8. 経路情報の登録機構の応用

経路情報の登録機構は、IRRにおける登録情報の正当性を保つために、独立して機能するシステムである。しかし本機構の仕様を検討する段階で、いくつかの応用が可能であることがわかった。本機構によって正当性が担保された情報を使って、インターネットにおけるIPアドレスの情報を照合し、不適切なIPアドレスの利用がないかどうかを確認するという応用である。ここでは、実現性が高く一部調整に入っている応用を二つ挙げる。

一つは、国内ISPにおける、経路ハイジャックの検知や予防である(図4-10)。

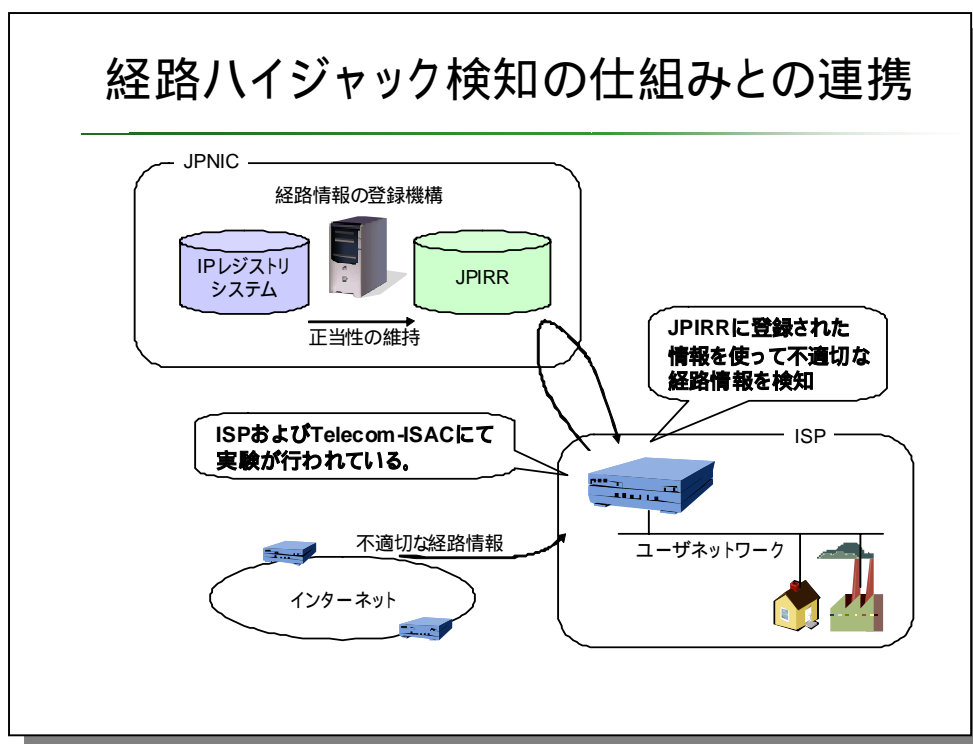


図 4-10 経路ハイジャック検知の仕組みとの連携

経路ハイジャックとはインターネットで交換されている経路情報に不適切な IP アドレスや AS 番号の情報を流すことである。これによって、特定の通信ホストへの成りすましや、盗聴、特定のネットワークに対する利用不能攻撃が可能になる。経路情報の登録機構によって登録された route オブジェクトは、本来使用されるべき、すなわち正しい IP アドレスと AS 番号の組み合わせの情報を IRR で一般に提供できるため、不適切な IP アドレスや AS 番号の利用を検知することが可能である。

もう一つの応用は、リソース証明書<sup>3</sup>の発行管理システムである。RFC3779 で提案されているリソース証明書は、LIR を含む IP アドレス割り振り先組織において専用の認証局システムが運用されることを想定している。しかしルーティング業務を行っている ISP にとって、認証局の運用業務は本来業務ではなく付帯業務である。しかし認証局の運用は継続性等を踏まえるとルーティング業務と同等かそれ以上の業務負荷を要し、容易に普及することは考えにくい。そこで考えられるのが、IP レジストリシステムもしくは IRR と一体化したリソース証明書管理インターフェースである (図 4-11)。

<sup>3</sup> リソース証明書 - IP アドレスや AS 番号の使用権を示す電子証明書。RFC3779 にプロファイル等が定められており、APNIC、ARIN、RIPE NCC で開発が進められている。

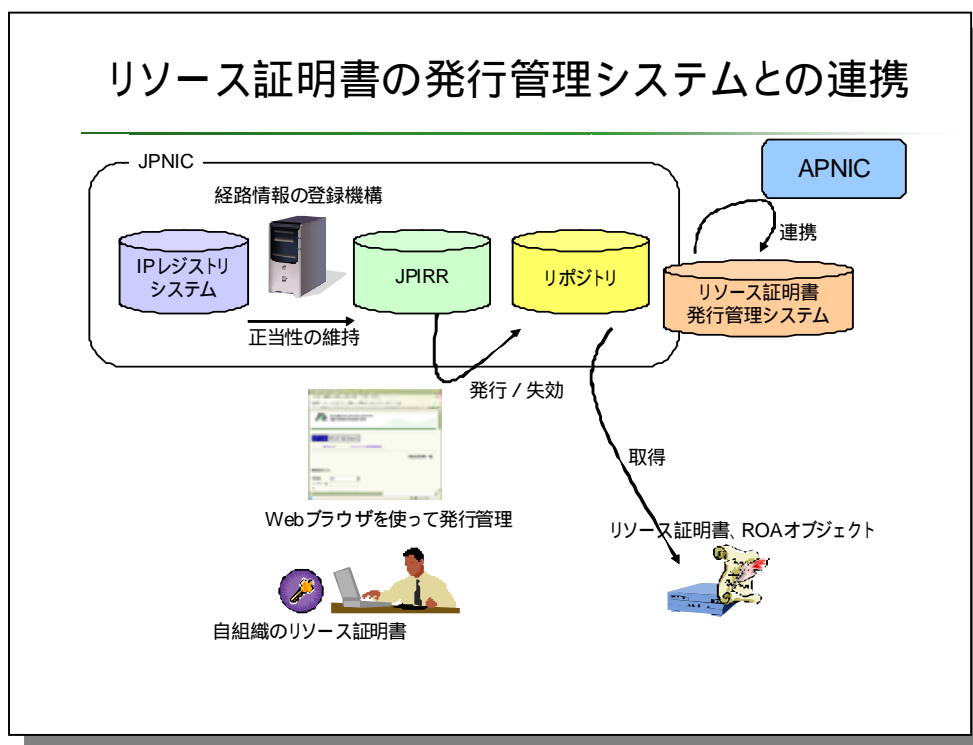


図 4-11 リソース証明書の発行管理システムとの連携

リソース証明書に関する業務の中で管理負荷が比較的高いのは、割り振られた IP アドレスに対するリソース証明書の発行業務や ROA オブジェクト<sup>4</sup>の発行、そしてリポジトリ運用業務であると考えられる。これらは、高い可用性が要されるか高い確実性が要される業務である。図 4-11 で示したシステムはこれらの負荷の高い業務の共通部分を集中化すると共に、リソース証明書システムの共通化を図っている。ISP は自組織のためのリソース証明書と私有鍵、およびリソース証明書発行管理システムにアクセスする Web ブラウザ等のみを持っていればよい。これにより、ルーティング業務に対する付帯業務の負荷を下げ、リソース証明書を扱うための業務負荷を下げる事が可能であると考えられる。

今後、これらの応用について ISP および APNIC との調整を継続していきたい。

#### 4.9. 経路情報の登録機構に関する国際会議での議論

経路情報の登録機構は、IP アドレス管理業務とルーティング業務を結びつける機構である。この根本的な概念は、本調査研究において独自に発想したものではない。ヨーロッパ地域におけるインターネットレジストリの RIPE NCC では、登録情報において

<sup>4</sup> Route Origination Authorization オブジェクト - IP アドレスがある AS によって経路広告されることを認可したことを示す、構造を持ったデータ。電子署名がついており、その検証にはリソース証明書が使われる。

mnt-route と呼ばれる記入欄を設けることで、同様の概念を実現している。また ARIN では、2006 年度から IP アドレスの割り振り・割り当ての申請書式に OriginatingASList という記入欄を設けることで、IP アドレス管理業務を行う組織が、ルーティング業務を行っている AS の番号を指定できる。これは本機構や RIPE NCC のルーティング業務を行うものを記載するよりも運用の柔軟性は欠けるが、経路ハイジャックのような不適切な IP アドレスの利用を検知できるような、正しいデータを維持するという意味で、同様の概念を実現していると言える。

このように RIR (Regional Internet Registry) では、IP アドレス管理業務とルーティング業務を結びつける機構が利用されている。一方、IETF では、SIDR WG のようにルーティングセキュリティの向上のために、IP アドレスの管理情報とルーティングの情報を電子証明書で結びつける仕組みの Protokol 策定が行われている。

そこで、本調査研究では、経路情報の登録機構について RIR や IETF の参加者が一同に集う会合で発表し、RIR および IETF において有意性などの確認を行った。RIR や IETF の参加者が一同に集う会合に、IEPG (Internet Engineering and Planning Group) がある。IEPG は IETF ミーティングの前日に毎回行われる会議で、IETF の参加者の中でインターネットの運用に興味のある技術者や運用者が参加している (図 4-12)。



図 4-12 IEPG Web ページ <http://www.iepg.org/>

本節では、2007 年 12 月 2 日、カナダのバンクーバーで行われた IEPG ミーティングにて行った、経路情報の登録機構に関するプレゼンテーションの内容と行われた議論について述べる。

RIR と IETF のセキュアルーティングにおける議論の中では、IP アドレス管理業務の中でルーティングへの IP アドレスの利用は、IP アドレスの利用認可 (authorization) という概念で捉えられている。経路情報の登録機構はこの利用認可を実現しているため、プレゼンテーションでは JPIRR における authorization の仕組みというタイトルとした (図 4-13)。

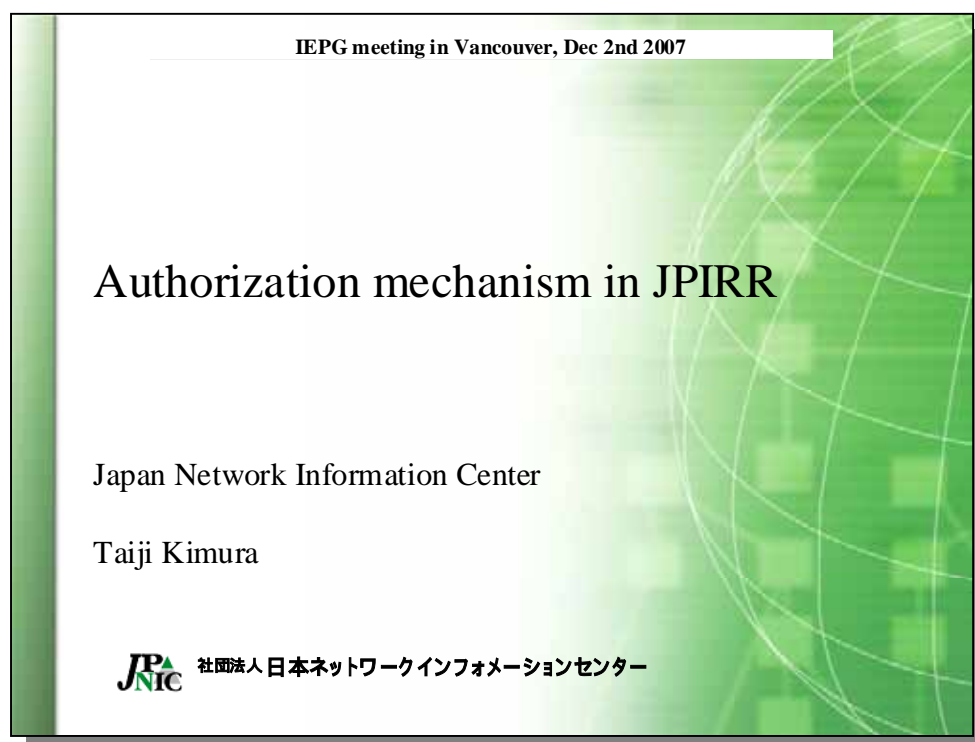


図 4-13 第 70 回 IETF の IEPG ミーティングで行ったプレゼンテーション

経路情報の登録機構に関する説明の前に、本機構の位置づけに関する説明を行った(図 4-13)。経路情報の登録機構は、JPIRR における実験的な実装であり、まだリリースされていないことや、本機構が「許可リスト」によって IP アドレスの利用認可を実現していることなど、概要を説明した。また論点がわかりやすくなるよう、本機構がルーティングセキュリティに効果を持つか、という疑問文を残しておいた。



## One topic about Internet Routing Registry

---

- An trial implementation of authorization mechanism for JPIRR
  - Will be released for LIRs in Japan this month
  - Has LIR's authorization list
    - Maintained by LIRs who have allocated prefixes from JPNIC
    - Allow/Deny mntners in JPIRR to put prefixes in route objects
      - AS numbers can be specified by LIRs.
- Does this works well for routing security?

図 4-14 One topic about Internet Routing Registry

本機構に関する説明のはじめに、本機構が適用される JPIRR と本機構の必要性について述べた(図 4-14)。これは、RIR や IETF では、IRR というと米国 Merit 社の RADB で有名であり、JPIRR の紹介が必要な為である(図 4-15)。

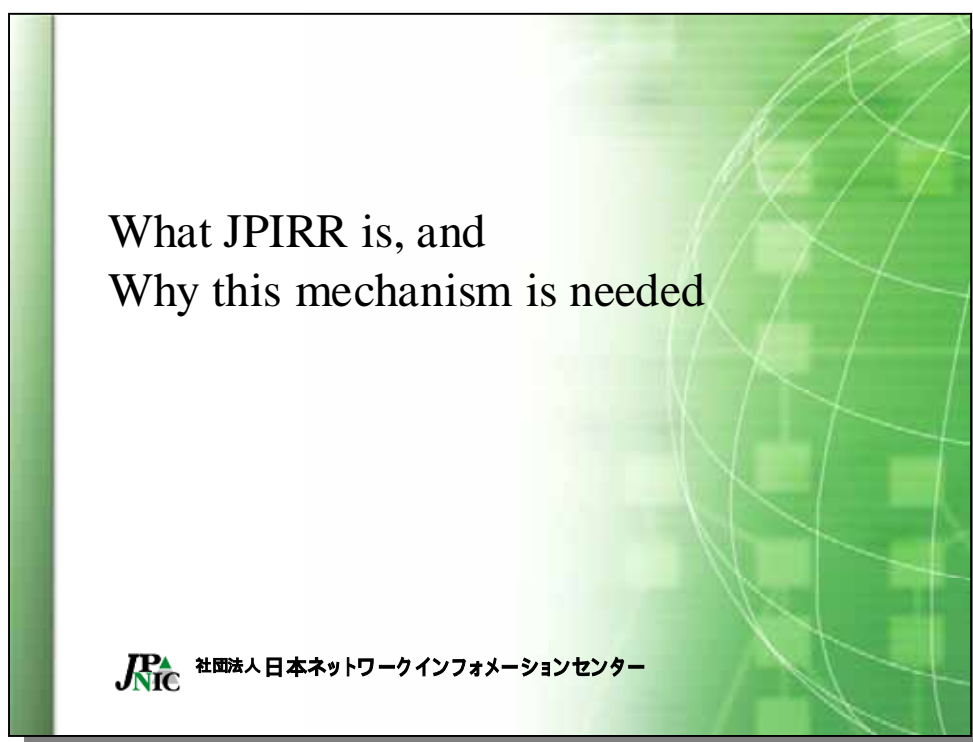


図 4-15 What JPIRR is, and Why this mechanism is needed

JPIRR に関する説明では、そのデータベースの規模と IP レジストリシステムとの連携状況について述べた。JPIRR はメンテナ数が 122 (2007 年 12 月現在) で RADB の約 20 分の一の数の管理者情報が登録されている。一方、経路に関する登録情報は RADB の 10 分の一以上あり、一件辺りの管理者情報に対する経路の情報は、RADB よりも多く登録されていることになる (図 4-16)。

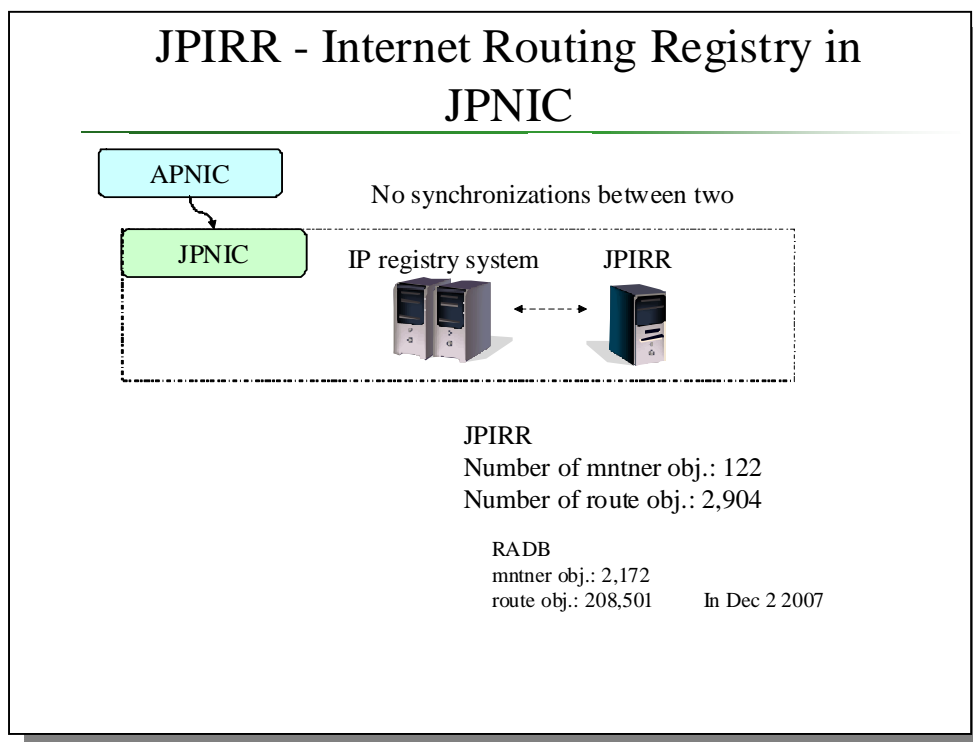


図 4-16 JPIRR - Internet Routing Registry in JPNIC

JPIRR は、JPNIC の IP レジストリシステムとは独立したシステムである( 図 4-16 )。RIPE NCC の IRR は RIPE NCC における IP レジストリシステムと一体であり、IP アドレスの割り振り / 割り当て情報と、経路の情報は連動している。ARIN や APNIC の IRR は各々の IP レジストリシステムとは分離しており、むしろ分離している方が主流であるといえる。Merit 社の RADB は当然の事ながら IP レジストリシステムと連動していない。

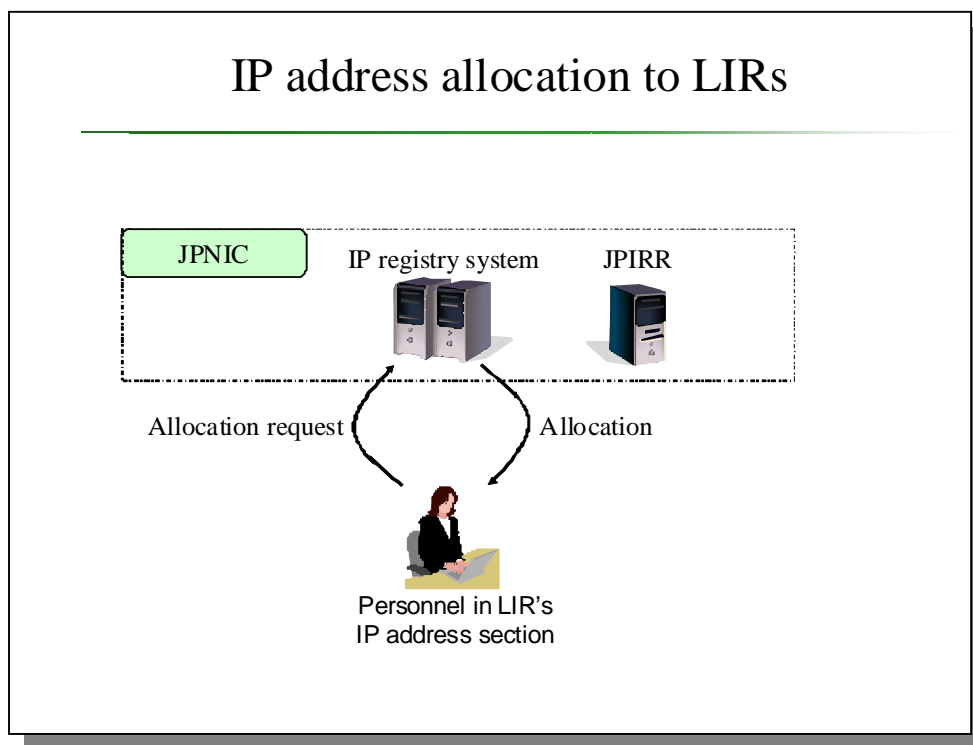


図 4-17 IP address allocation to LIRs

JPIRRの説明の後、JPNICにおけるIPアドレスの割り振り業務について述べた(図4-17)。日本国内のIP指定事業者は、国際的にはLIRと捉えることができるため、簡単のためLIRへの割り振り業務、という説明とした。JPNICからIPアドレスの割り振りを受けても、JPIRRに自動的に登録は行われない。

一方、JPIRRではIPレジストリシステムと独立した登録業務が行われている(図4-18)。JPIRRに登録業務を行うのはISPでルーティング業務を行っているもので、JPIRRにおけるユーザの登録情報もIPレジストリシステムのユーザとは異なっている。

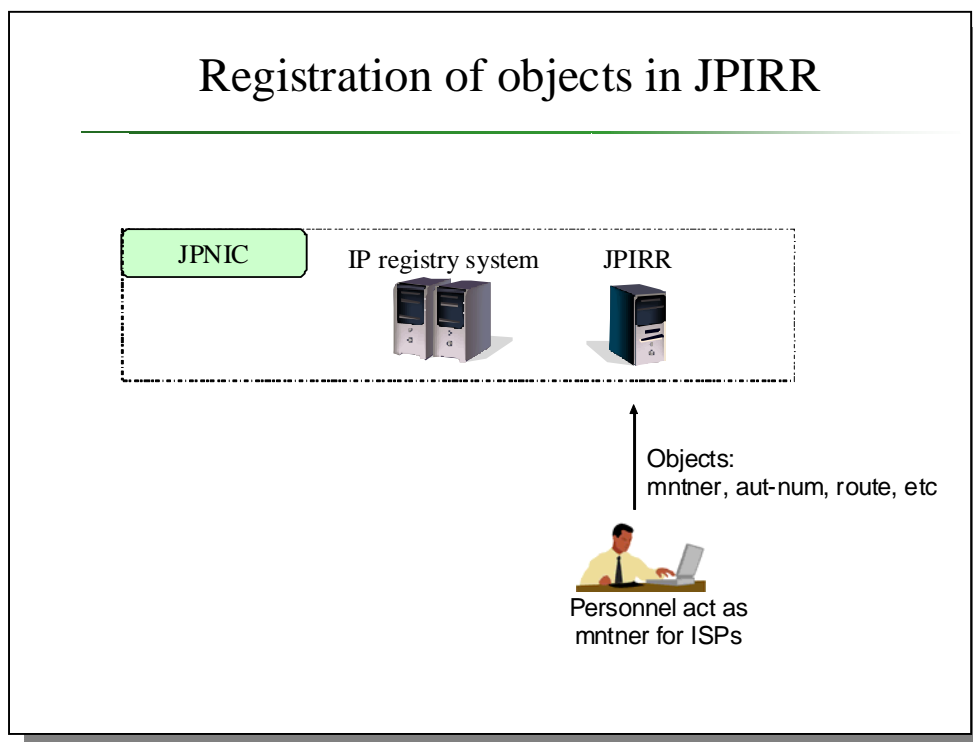


図 4-18 Registration of objects in JPIRR

JPNIC や他の RIR における IRR は、IP レジストリシステムと独立したシステムであるが、ここで二つの疑問を提示した（図 4-19）。

## Why this mechanism is needed

- There are no relationship between IP address allocated to LIRs and prefixes in route objects in JPIRR.

Two big questions:

- Does anyone can put any prefixes in route objects? - - Yes he/she can.
- Is there any correctness of prefix-based filtering for BGP routers along with JPIRR? - - Well, yes if all mntner does correctly.
- How should we handle it?
  - At least, LIRs are need to be aware of use of prefixes in global routing operations.

図 4-19 Why this mechanism is needed

一つは「IRR にはあらゆる IP アドレスの登録が可能か？」ということである。現行の IRR では、割り振りが行われていない IP アドレスであっても IRR に登録することが可能である。もう一つは、「BGP ルータで JPIRR の登録情報に従って prefix フィルター（IP アドレスベースのフィルタリング方式）を利用した場合に、それは正しいと言えるか？」ということである。これに対しては「もしもすべての登録者が正しい情報を登録していれば」という逆説的な答えをあえて提示した。つまり、IRR の登録情報を利用して正しい prefix フィルターを利用することが難しいのである。

更に LIR における prefix の利用が、グローバルなルーティング業務で重要な位置づけにあることを述べた。後述する、本機構の狙いの一つに LIR における prefix の正しい利用に関する注意喚起があることに繋げている。

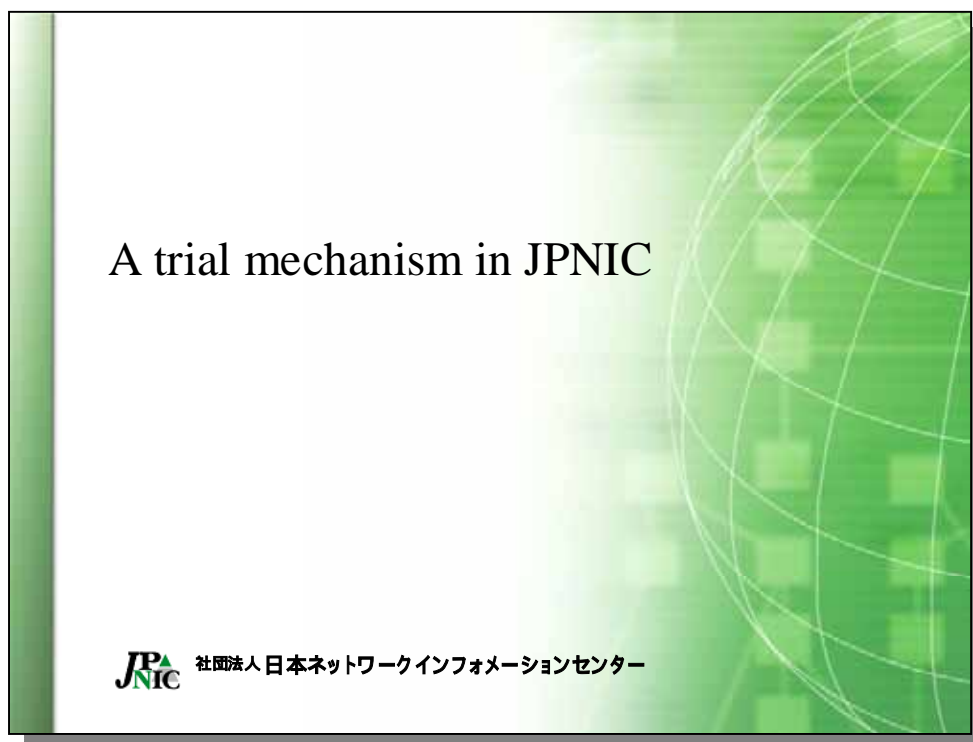


図 4-20 A trial mechanism in JPNIC

本機構の開発は、経済産業省からの受託事業の一環であるため、あくまでトライアルであるという位置づけとした(図 4-20)。JPNIC では IP アドレスの割り振り / 割り当て業務と IRR の運用の両方を行っているため、このトライアルは JPNIC ならではのものであると言える。

はじめに、利用認可の基本概念を説明する。経路情報の登録機構は、LIR に割り振られていない IP アドレスを含む route オブジェクトが JPIRR に登録されることを防ぐシステムである。同時に、IP レジストリシステムと JPIRR における登録業務はこれまでと大きく変わらないように工夫されている。

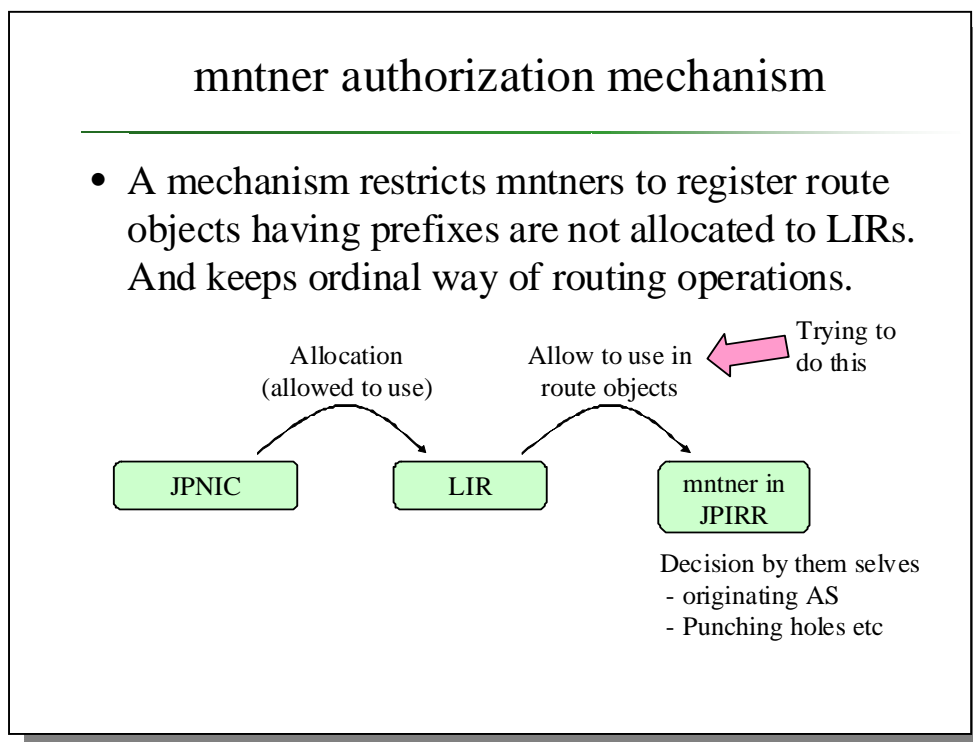


図 4-21 mntner authorization mechanism

図 4-21 は、IP アドレスに対する LIR の概念的な業務内容を示したものである。JPNIC（上位のインターネットレジストリ）は LIR に対して割り振りを行うが、これは IP アドレス利用を認めていることでもある。これと似た形で、LIR は JPIRR におけるメンテナに対して、IP アドレスのルーティングにおける利用を認可する。JPIRR におけるメンテナはルーティング業務を行っているもの識別子を持たせて顕在化させるための方法である。ルーティング業務を行うもの、すなわちメンテナはどの AS を広告元としてルーティング業務を行うか、またどの IP アドレス空間を経路広告せずに下位のネットワークに使わせるか、等のルーティング業務上の判断を行う。

経路情報の登録機構は、LIR が JPIRR におけるメンテナに対して、route オブジェクトを登録することを認可する、という業務を実現する。



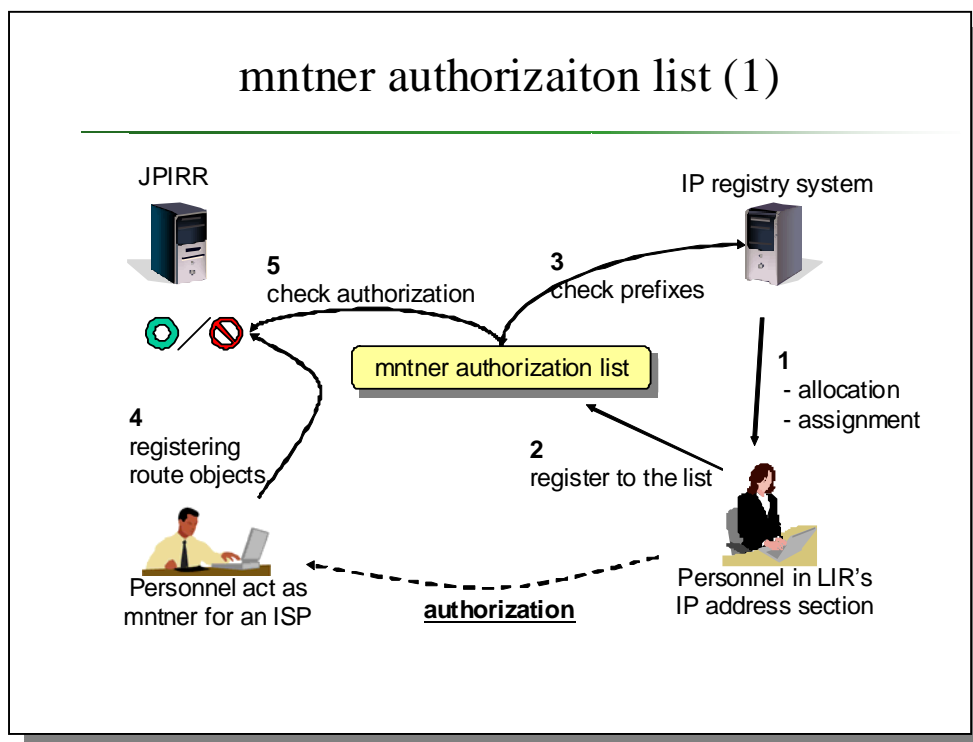


図 4-22 mntner authorizaiton list (1)

経路情報の登録機構における IP アドレスの利用認可登録は、LIR の IP アドレス申請担当者によって行われる。図 4-22 は LIR に IP アドレスを割り振られてから、利用認可の確認された route オブジェクトが登録されるまでの業務流れを示したものである。

はじめに LIR に IP アドレスの割り振り / 割り当てが行われる (1)。これは LIR の IP アドレスの申請業務担当者によって、IP レジストリシステムを通じて行われる。次に、IP アドレスの申請業務担当者は割り振られたアドレスを許可リスト (mntner authorization list) に登録する (2)。この時、登録された IP アドレスがその LIR に割り振り済みであるかどうかを確認される (3)。IP アドレスの申請業務担当者はこの操作を必要数だけ行い、自組織に割り振られた IP アドレスを可能であればすべて、特定の mntner に対して利用認可を行う。

JPIRR にオブジェクトを登録するオブジェクト登録者 (Personal act as mntner for an ISP) は、通常の IRR へのオブジェクト登録の書式を使ってオブジェクト登録を行う (4)。この時、登録されようとしている route オブジェクトの検査が行われ、IP アドレスの利用認可がされているかどうかを確認される (5)。

mntner authorization list (2)

---

Prefix (inclusive)	allow / deny	mntner	Origin AS (optional)
1.1.0.0/16	allow	MAINT-JPNIC	12345
1.1.0.0/17	deny	MAINT-AS2515	

図 4-23 mntner authorization list (2)

図 4-23 は、許可リストの内容を説明したものである。ここでは多様な IP アドレスの管理方法に対応できることを説明するため、詳細に説明を行った。

許可リスト (mntner authorization list) は、基本的に 4 つの値を持つ表である。最初は prefix で、IP アドレスの範囲である。二番目の allow/deny は、その IP アドレスに対する認めないし認めないことを示す値である。三番目の mntner は IP アドレスの利用を認可する対象のメンテナー名である。図では、MAINT-JPNIC や MAINT-AS2515 は 1.1.0.0/16 の範囲にある route オブジェクトを登録できる。四番目の Origin AS は登録される route オブジェクトの Origin AS の欄に記入される AS 番号の制限である。図の場合には、1.1.0.0/16 は Origin AS を 12345 に指定した route オブジェクトしか登録することができない。Origin AS の指定は Optional (追加事項) であり指定を行わなくてもよい。

許可リストは、次に述べるような使い方ができる。ある IP 指定事業者が、自社の ISP 事業でのみ IP アドレスを使う場合、自社に割り振られたすべての IP アドレスを自社のメンテナーに許可すればよい。自社に複数の AS 番号が割り当てられており、ルーティング業務の中で随時変更できるようにしておくには、Origin AS の欄には何も記入しないでおく。また IRR への登録業務を自社のメンテナー以外で行う場合には、mntner の欄にそのメンテナー名を併記しておく。これにより、自社に割り振られた IP アドレスが、他の AS によって経路広告されたとき、IRR の登録情報と差異が生じる。すべての割り振り済み IP アドレスを登録しておけば、自社に割り振られた IP アドレスが一部でも他

## 第4章 IP アドレス認証の展開に関する調査研究

の AS に使われたときに、IRR と比較して異常を発見できる。

自社に割り振られた IP アドレスのルーティング業務を他社に委託する場合には、その他社のメンテナー名を mntner 欄に記入するだけでよい。そのルーティング業務を行う他社は、自社の AS 番号を用いてルーティング業務を行うことができ、また AS 番号が変わる場合やマルチプル Origin (複数の Origin AS の同一 prefix の経路情報) を広告することも可能である。

mntner authorization list (3)



ID	Org	Org Name	Prefix	Org Name	AS Number
13	9999	ROUTEREGTEST	100.0.0.0/24	MAINT-ROUTEREG	
19	9999	ROUTEREGTEST	100.0.10.0/24	MAINT-ROUTEREG	AS999, AS25
19	9999	ROUTEREGTEST	100.0.10.0/22	MAINT-ROUTEREG	AS2
23	9999	ROUTEREGTEST	100.0.32.0/19	MAINT-ROUTEREG	AS00001, AS0001, AS3791
14	9999	ROUTEREGTEST	100.0.22.0/19	MAINT-ROUTEREG	
27	9999	ROUTEREGTEST	200.210.99.0/22	MAINT-ROUTEREG	AS37911, AS25
29	9999	ROUTEREGTEST	200.210.99.0/24	MAINT-ROUTEREG	
28	30999	ROUTEREGTEST	200.0.40.0/22	MAINT-ROUTEREG	AS37911, AS25
24	30999	ROUTEREGTEST	200.0/32	MAINT-ROUTEREG	AS99999, AS9999, AS3791
11	30045	IPRDC	2030/22	MAINT-ROUTEREG	AS64512, AS00001

図 4-24 mntner authorization list (3)

図 4-24 は、経路情報の登録機構で許可リストを表示した画面である。許可リストは Web インターフェースで編集することができる。ソートや編集、削除などを行うことができる。

なお、テストのために入力された IP アドレスを表示している。メンテナー名もテスト用のものであり、実際には JPIRR に登録されたメンテナー名が表示される。

図 4-25 と図 4-26 はシステムがどのように動作するかを説明したものである。

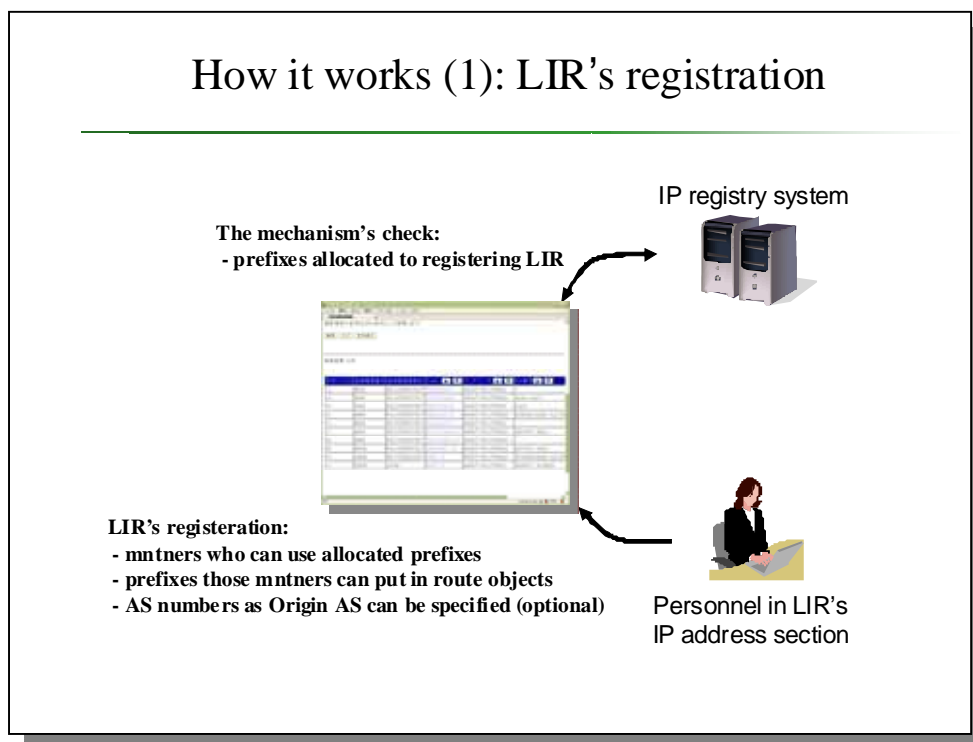


図 4-25 How it works (1): LIR's registration

はじめはLIRによる許可リストへの登録がどのように行われるかを説明した図である。LIRのIPアドレスの申請業務担当者は、自社の認証用の電子証明書を用いて経路情報の登録機構にアクセスする。自社の認証用の電子証明書は、IPアドレス認証局（認証）（サービス名：資源管理認証局）から発行されたクライアント証明書である。

LIRの担当者は、はじめにIPアドレスの利用者であるメンテナー名を登録する。そのメンテナー名はJPIRRにrouteオブジェクトを登録できるメンテナーである。更に必要があればAS番号の指定を行う。経路情報の登録機構がクライアント認証に用いる認証用の電子証明書は、IPレジストリシステムのものと同様であるため、IPレジストリシステムが許可リストに登録を行おうとしているユーザがどのLIRのユーザであるかを認識することができる。許可リストへの登録の差異に、そのLIRに割り振られたIPアドレスが登録されるかどうかの確認を行う（図4-25）。

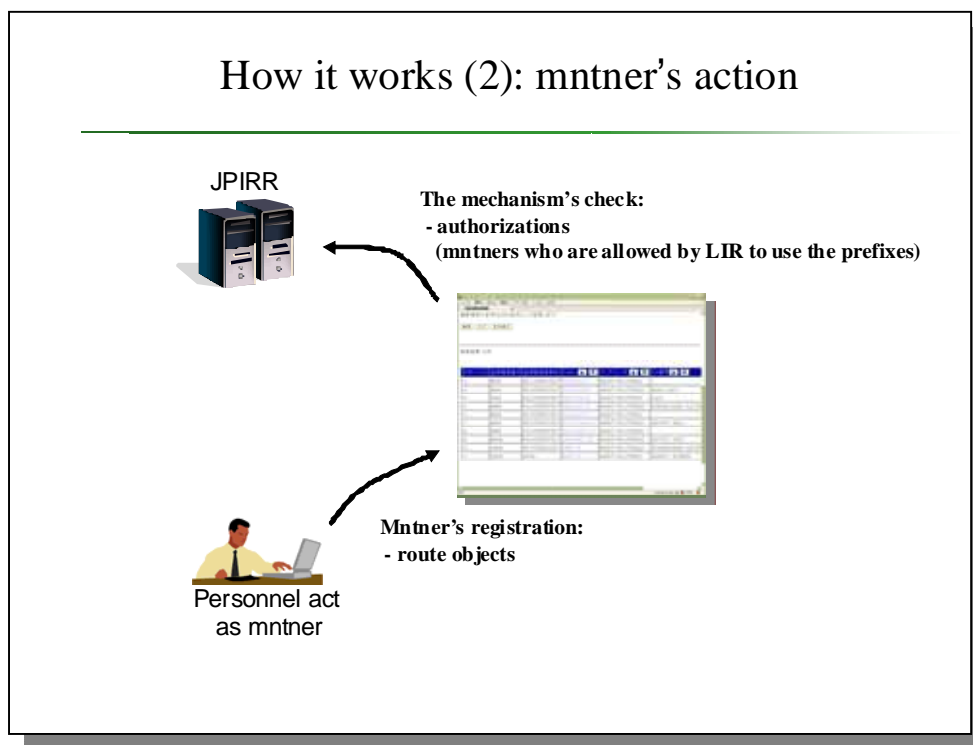


図 4-26 How it works (2): mntner's action

図 4-26 に示したスライドはメンテナによる route オブジェクトの登録について説明している。メンテナの権限で route オブジェクトを登録する際、経路情報の登録機構は route オブジェクトに含まれる IP アドレスが許可リストに載っているものであるかどうかの確認を行う。更に登録しようとしているユーザ（メンテナの権限を使おうとしているユーザ）が、認可の対象になっているかどうかを確認する。

## Expected results

---

- All new registered route objects will have allocated prefixes. And they are registered by appropriate mntners.

This situation can keep:

- Avoiding
  - Use of un-allocated prefixes in route objects
  - Miss-matches from registry's allocations
- Providing
  - Selecting originating AS by mntners according to operational reasons
  - Nothing new if LIR and mntner are the same

図 4-27 Expected results

このスライドは、以上の手続きを踏まれて登録されることでどのような効果が期待できるかを説明したものである。以上の業務手続により、JPIRR に登録されるすべての route オブジェクトは、割り振り済みで、かつ利用認可されたメンテナーによって登録されることが担保されるようになる。

このことで、まず route オブジェクトに少なくとも割り振られていない IP アドレスが入ることがなくなる。またインターネットレジストリによる割り振りとなる IP アドレスも入ることがなくなる。

また業務上の自由度を二つの意味で確保している。一つ目はメンテナーによって Origin AS を選択できることである。ルーティング業務においては、ネットワークの構成に自由度を持たせたり、障害時にネットワークの構成を変更できることは重要である。またもし LIR とメンテナーが同一の担当者や担当部署である場合、これまでの業務とほとんど変わらない。すなわち経路情報の登録機構を使うことで業務負荷が大きく変わることはない。

## Operator's expect on use of JPIRR in Japan

- irrzebra
  - Checks BGP updates with IRR
  - Shows flags as “checked” when displaying routing table
- Keiro-bugyo
  - (Keiro is 'route')
  - (Bugyo is organized decision makers for local society in Samurai era)
  - Checks received BGP updates with local configurations
    - (Local configurations are checked by using IRR)
  - Notify if a miss-use is detected by e-mail

They will have more accuracy of 'checks' if the authorization mechanism works well.

図 4-28 Operator's expect on use of JPIRR in Japan

このスライドは、経路情報の登録機構の応用に関する日本国内での動向を簡単に紹介したものである。JPIRR は irrzebra<sup>5</sup>や経路奉行<sup>6</sup>と呼ばれる ISP によって開発されたシステムによっても利用されている。irrzebra は BGP の Update メッセージに含まれる prefix に対して IRR を使った検査ができるルーティングデーモンである。ルーティングテーブルに検査の結果を表示することができ、ルーティング業務を行うものは、異常を発見しやすい。

経路奉行は irrzebra と同様に BGP の Update メッセージの検査を行うシステムである。経路奉行は一度に大量の検査が行えるように、一旦ローカルの設定ファイルに IRR の事前調査事項を保存しておく仕組みを持っている。また経路奉行は、検査の結果を電子メールで通知する機能を持っている。

これらの仕組みと IRR および経路情報の登録機構が連携することで、実際のルーティング業務において IP アドレスの利用認可がなされていない IP アドレスを検知できる。

<sup>5</sup> irrzebra は「インターネット中枢機能のセキュリティ強化に関する研究開発」(委託研究)に掲載されている。

[http://www2.nict.go.jp/q/q265/s802/seika/h18/seika/81/81\\_ntt-com.pdf](http://www2.nict.go.jp/q/q265/s802/seika/h18/seika/81/81_ntt-com.pdf)

<sup>6</sup> 経路奉行は「Telecom-ISAC Japan の 最近の取組について」に詳しく述べられている。

<http://www.ipa.go.jp/security/event/2006/infra-sem/pdf/Telecom-ISAC.pdf>

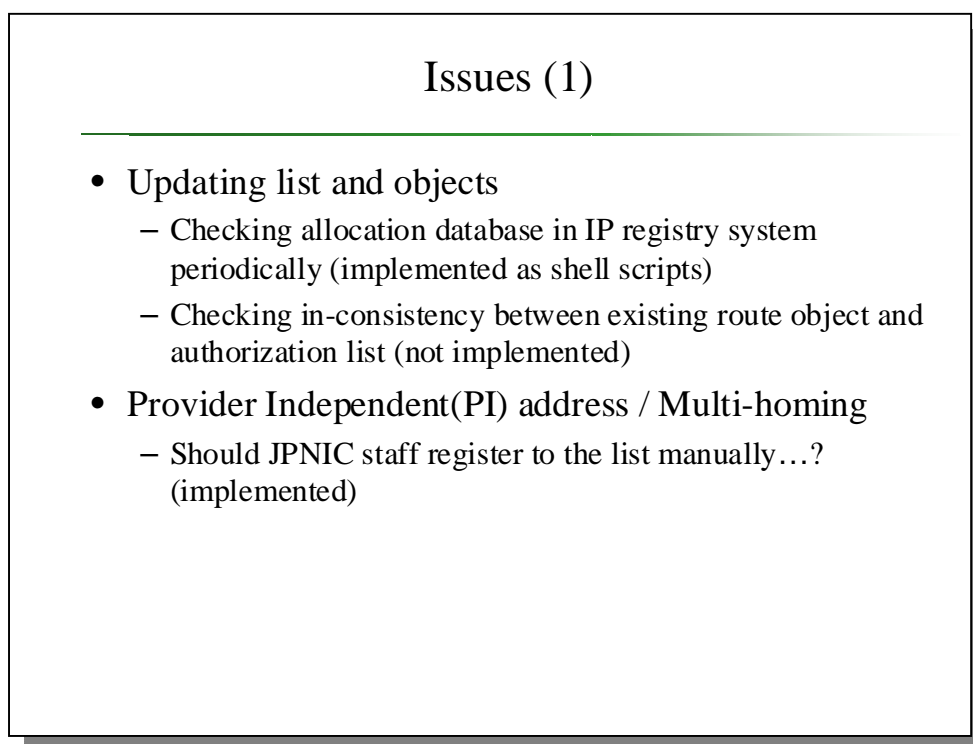


図 4-29 Issues (1)

Issues は、経路情報の登録機構に関する論点を整理したスライドである（図 4-29）。

RIR に同様の仕組みが導入されていることがわかっているため、それらの運用の中で問題点となっていることを中心にまとめた。

経路情報の登録機構の許可リストは、長期間運用されていると古いデータが残る可能性がある。RIPE NCC では割り振り情報と齟齬が生じた状態の、古いデータが残ってしまう問題が起こっている。経路情報の登録機構では、IP レジストリシステムと許可リストを定期的に比較し、齟齬が生じている場合には登録者に通知する機能を実装した。一方で、許可リストと IRR に登録済みの route オブジェクトの比較については、いまのところ行っていない。許可リストは IRR の登録と IP レジストリシステムの割り振り / 割り当てとの間に許可リストというクッションを設けることで、IP アドレスの返却等によって、即座に IRR の登録情報が異常だと検知されるような状況を避けている。しかし逆に許可リストが正しい情報を保持しているか（IP レジストリシステムのデータベースとの比較）、現状とあっているか（IRR の登録情報との比較）を行う必要がある。

PI アドレスとマルチホームに関しては、現在のところ JPNIC の職員が許可リストに登録するものとしている。これは一部の業務上の理由による。PI アドレスの割り当て先は、JPNIC の IP 指定事業者でないケースがあり、また割り当て先組織の本人性確認手順が IP 指定事業者とは異なる。IP 指定事業者に対する電子証明書の発行は実験的に開始しているが、PI アドレスの割り当て先組織には、まだ電子証明書を発行できていない



状況である。

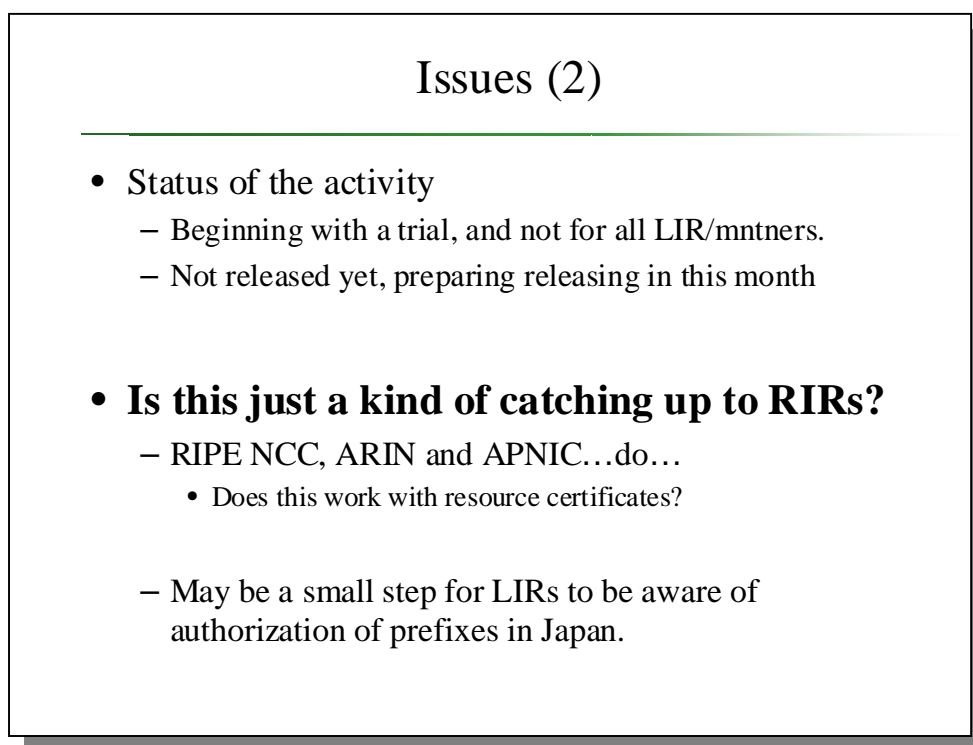


図 4-30 Issues (2)

前述の運用上の論点だけではなく、実験としての論点もある。経路情報の登録機構は、実験を開始したばかりであり、まだすべての LIR やメンテナーが利用できるわけではない。

本機構は RIR (RIPE NCC と ARIN) に対してキャッチアップする位置づけのシステムであると言う事もできる。また主に APNIC で取り組まれているリソース証明書との親和性を検討することも課題である。もしリソース証明書が日本を含むアジア太平洋地域で利用されるようになると、この prefix の利用認可の概念は必ず必要になるものである。

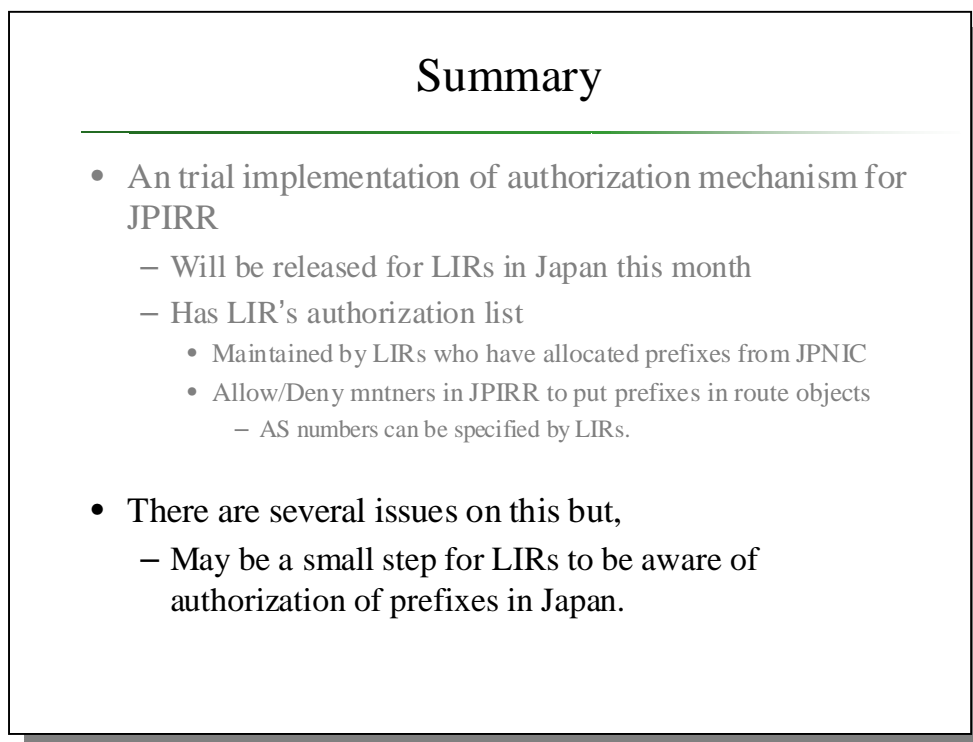


図 4-31 Summary

最後に、プレゼンテーションのサマリを行った（図 4-31）。

経路情報の登録機構が実験的な運用であることは先に述べた通りであるが、この実験によって prefix の安全な利用に関する認識が高まることが重要であると述べた。

以上が IEPG ミーティングにおけるプレゼンテーションである。この後、15 分以上、本件に関する意見交換が行われた。

## IEPGミーティング会場でのディスカッション

- コメント
  - 活動をencourage
    - George Michaelson氏(APNIC), Shane Kerr氏(ISC,元RIPE NCC), Andrew de la Have氏(RIPE NCC)
  - 許可リストの状態に関して
    - 「要件」と「チェック機構」が必要であるというコメント(後者は既に開発済み)
  - リソース証明書との関係
    - 本機構とリソース証明書の仕組みは親和性がある(George Michaelson氏)
- 議論
  - その他にRIRと比べた、本機構の位置づけについて議論された。
    - RIPE NCCにおけるRPSS:登録情報の安全性確保手法、等

図 4-32 IEPG ミーティング会場でのディスカッション

図 4-32 は、IEPG ミーティングで行われた意見交換をまとめたものである。まず、この活動を高く評価する意見が多数挙げられた。その後の意見交換の中では大きく分けて二つの点について議論が行われた。

一つは、許可リストの「正しい」状態を保つことに関する議論である。まず「正しい」という状態の要件の定義が必要ではないか、という意見が挙げられた。これは例えば LIR による登録が常にルーティング業務に合ったものであるかどうか分からないという点である。またプレゼンテーション中でも述べた、チェック機構が必要であるという意見である。チェック機構は一部実装されているものではあるが、RIPE NCC のように IRR と IP レジストリシステムが同一であれば、チェック機構はよりシンプルなものになると考えられる。RIPE 地域の発言者は、許可リストによって二重のチェックが必要になっているのでは、という疑問が投げられた。許可リストは確かに二重のチェックを要するものであるが、各々のチェック内容と間違っている場合の通知先が異なる。また同一のシステムの場合、チェック後に IRR の route オブジェクトを消してしまい、ルーティングに障害を起こしてしまいかねない。許可リストのようにクッションを設けるべきか、同一のデータベースで管理されるべきであるかは、実験運用を行ってみてどのような問題が起こるのかを観察することで初めて解決が図られると考えられる。

他に、本機構とリソース証明書の親和性については、APNIC のリソース証明書の開発担当者から発言があった。それは、本機構はリソース証明書と親和性があるというシンプルな発言であった。

これらの議論の他に、RIPE NCC におけるセキュリティの仕組みと比較して本機構がどのような仕組みであるのかを確認したいといった意見交換が行われた。

#### 4.10. 経路情報の登録機構に関する国内会議での議論

経路情報の登録機構に関する国内での議論は、主に JANOG (Japan Network Operator's Group) ミーティングで行った。本節では、第 21 回 JANOG において「IRR を使ったセキュアなインタードメイン・ルーティングを考える会」という時間に行った議論について述べる。

### 経路制御の問題解決とIRR

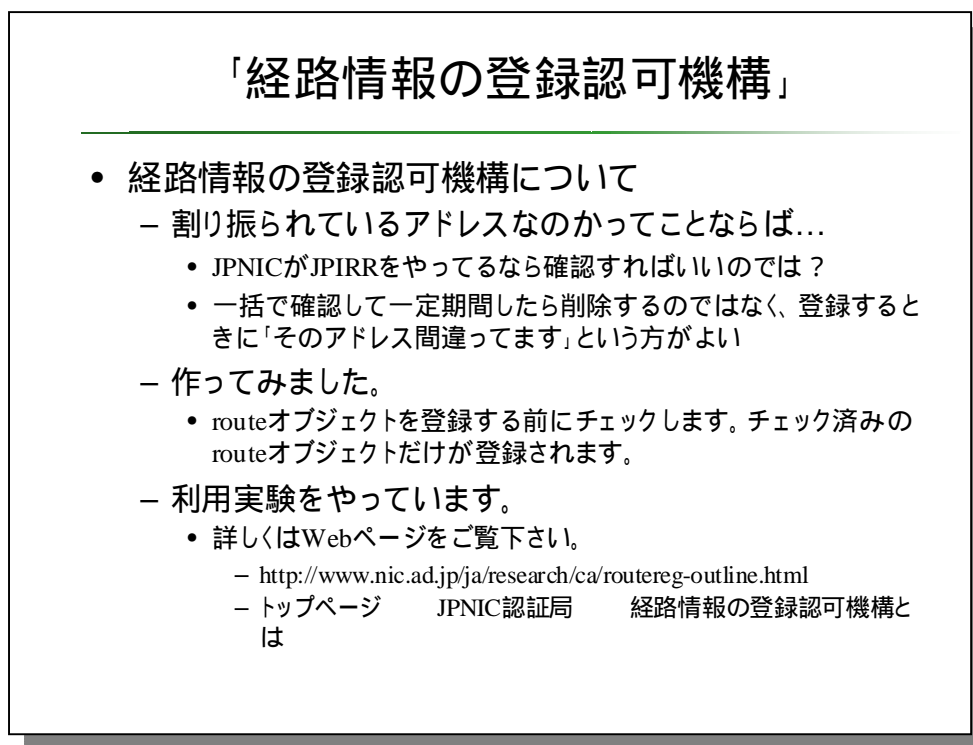
- 経路の問題と解決策
  - Inter-Domainの経路制御で、問題解決に人的ネットワークに頼らなくていい部分があるはず...というか、IPv4アドレスプールが枯渇する時期に、いまのままで大丈夫？
- 例えば経路ハイジャックを防ぐとして
  - その情報源は？
- IRRにちゃんとrouteオブジェクトがたまれば大丈夫？
  - routeオブジェクトの割り振り情報との違い
    - IRRには割り振り/割り当てに関わらず、任意のアドレスprefixが入ったrouteオブジェクトを登録できる。
    - 全く関係のない他のISPが経路広告すべきprefix
    - 未割り振りのprefix など

図 4-33 経路制御の問題解決と IRR

これまで、経路制御における問題解決の多くは、人的ネットワークに頼っており、また経路情報の正当性の確認はオペレーターの地道な作業で行われている。しかし IPv4 アドレスの割り振りプールの枯渇時期に入り、他の ISP が経路広告して使うはずの IP アドレスが勝手に使われてしまう事態が今後起こりやすくなり、問題解決をある程度自動化する必要があると考えられる。

経路情報の登録機構は、IRR における登録上の問題を機械的に解決とも言える。既存の IRR には任意の prefix が入った route オブジェクトを登録できるため、他の ISP が経路広告すべき prefix を登録したり、未割り振りの prefix を登録できる。IRR はルー

タにおける経路情報の正しさの確認のために利用されているため、IRR に誤った情報が登録されているとその確認が行えなくなる。経路情報の登録機構は、他の ISP が経路広告すべき prefix を登録できないようにしたり、未割り振りの prefix を登録できないようにできる。



**「経路情報の登録認可機構」**

- 経路情報の登録認可機構について
  - 割り振られているアドレスなのかってことならば...
    - 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/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

図 4-34 「経路情報の登録認可機構」(JANOG21)

図 4-34 は経路情報の登録機構を紹介したスライドである。サービス名が「経路情報の登録認可機構」であるため、スライドでは経路情報の登録機構と表記している。経路情報の登録機構は、JPIRR に登録されている情報を一括して検査するようなバッチ形システムではなく、ユーザが登録する段階で、その登録内容のチェックを行うシステムである。これは一定期間後に削除する形では、オペレーターにとって突然経路制御に障害が起こるような事態を引き起こしかねないからである。

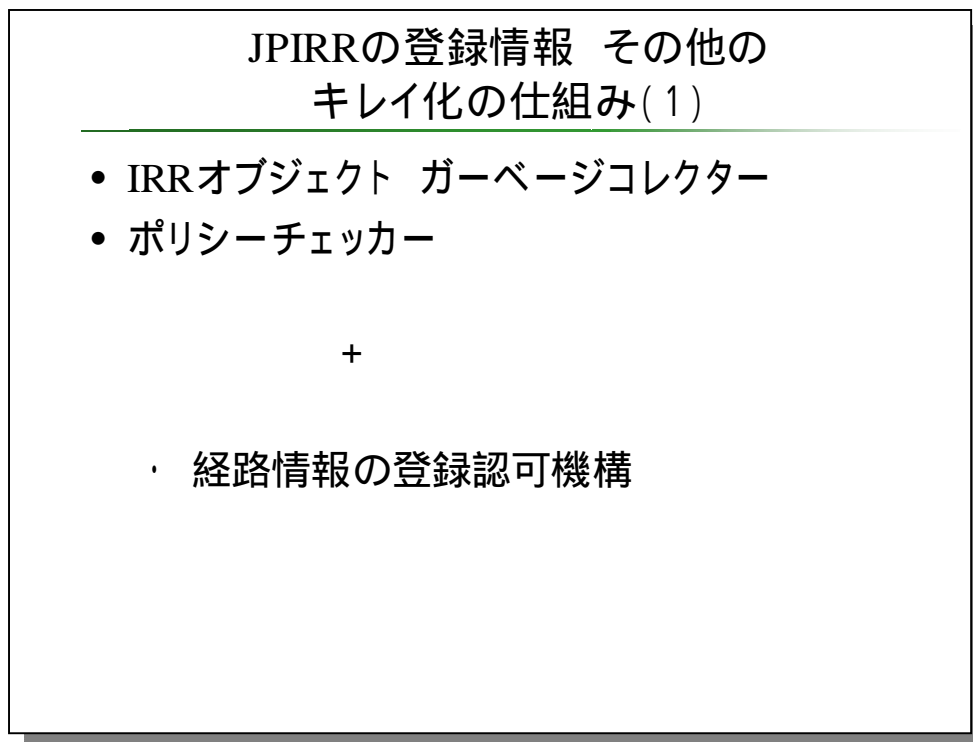


図 4-35 JPIRR の登録情報 その他のキレイ化の仕組み(1)

JPIRR には登録情報の正当性を保つための機能がこれまでに二つ実装されている。一つは「ガーベージコレクター」でもう一つは「ポリシーチェッカー」である。経路情報の登録機構は、この二つに加えて同時に使うことのできる仕組みである。

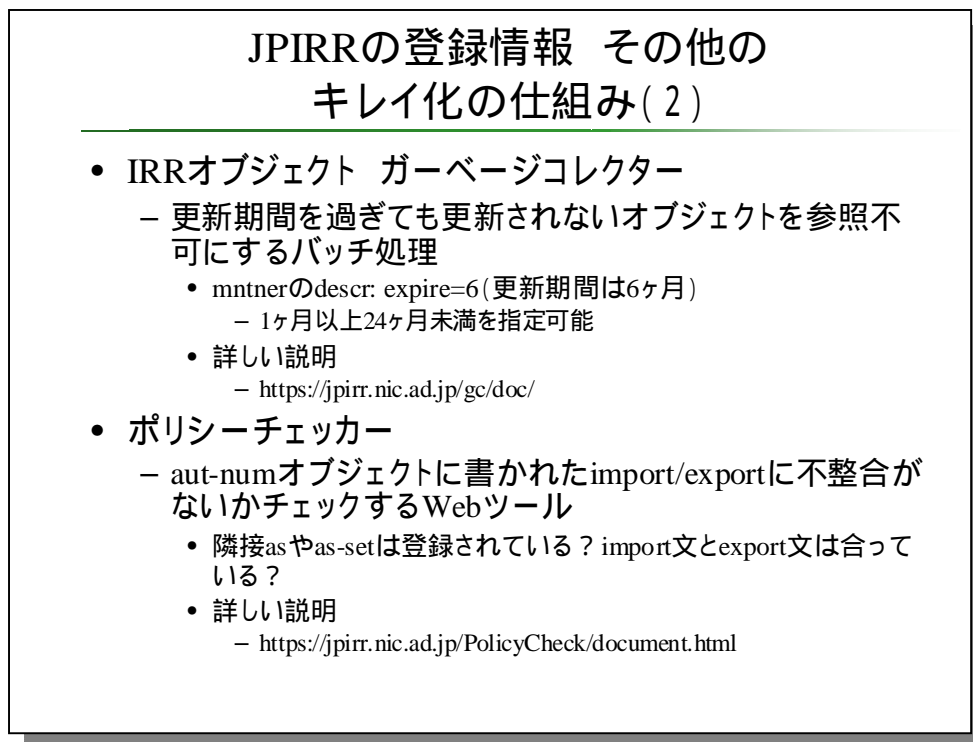


図 4-36 JPIRR の登録情報 その他のキレイ化の仕組み(2)

ガーベージコレクターは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機能である。mntner オブジェクトに予め更新期限を記述しておく、事前・事後の通知のあと最終的に参照できないようにする。このことで、オブジェクトが最新に保たれるようにするバッチ形のツールである。

ポリシーチェッカーは JPIRR に登録される情報の中で、import 文や export 文で不整合が生じていないかどうかを確認することができるツールである。ユーザは Web インターフェースを使ってポリシーの確認を行うことができる。

### 経路情報の登録認可機構のチェック

- チェックのタイミング
  - routeオブジェクトを登録しようとするとき
- チェック内容
  - 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」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

図 4-37 経路情報の登録機構のチェック

経路情報の登録機構は route オブジェクトの登録に関するチェックを行う。このチェックは一定期間毎のバッチ的な処理ではなく、ルーティング業務を行うものが JPIRR にオブジェクトを登録する電子メールを送ったときに行う。



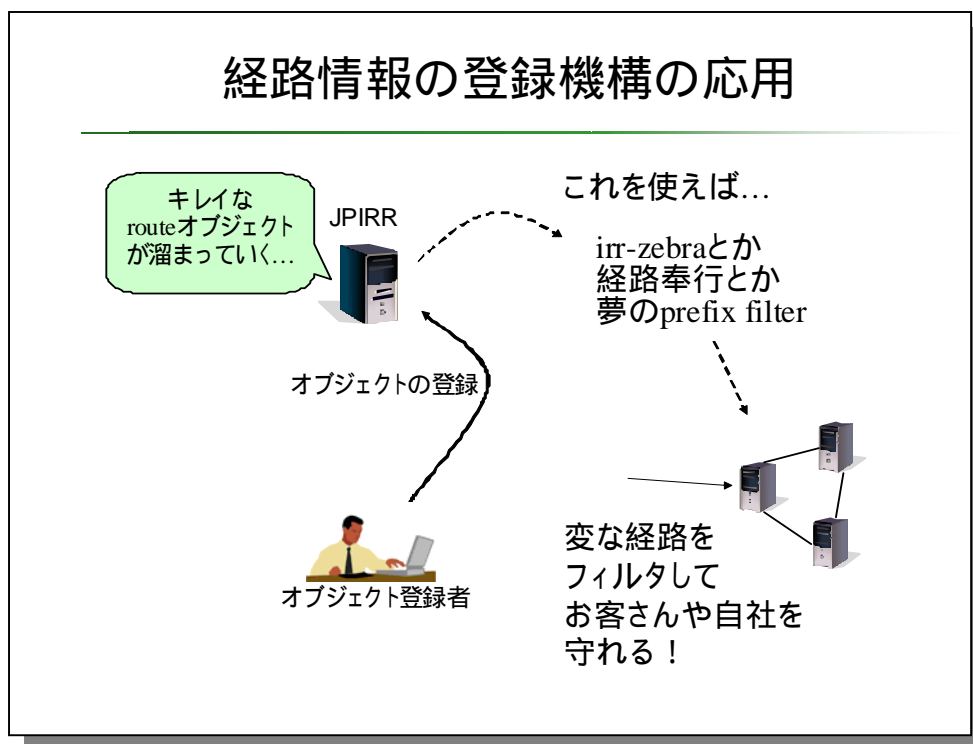


図 4-38 経路情報の登録機構の応用

JANOG では、自組織のネットワークを不正な経路制御から守る、という観点で議論を行った。irrzebra や経路奉行を用いると、不正な経路制御のメッセージを検知することができ、隣接する AS に対する経路制御も正しい状態を保つことができる。図では顧客や自社のネットワークを守ると記述しているが、実際には隣接する AS 同士が不正な経路情報のフィルターを行うことで、経路ハイジャックの影響を広域的に防ぐことができると考えられる。

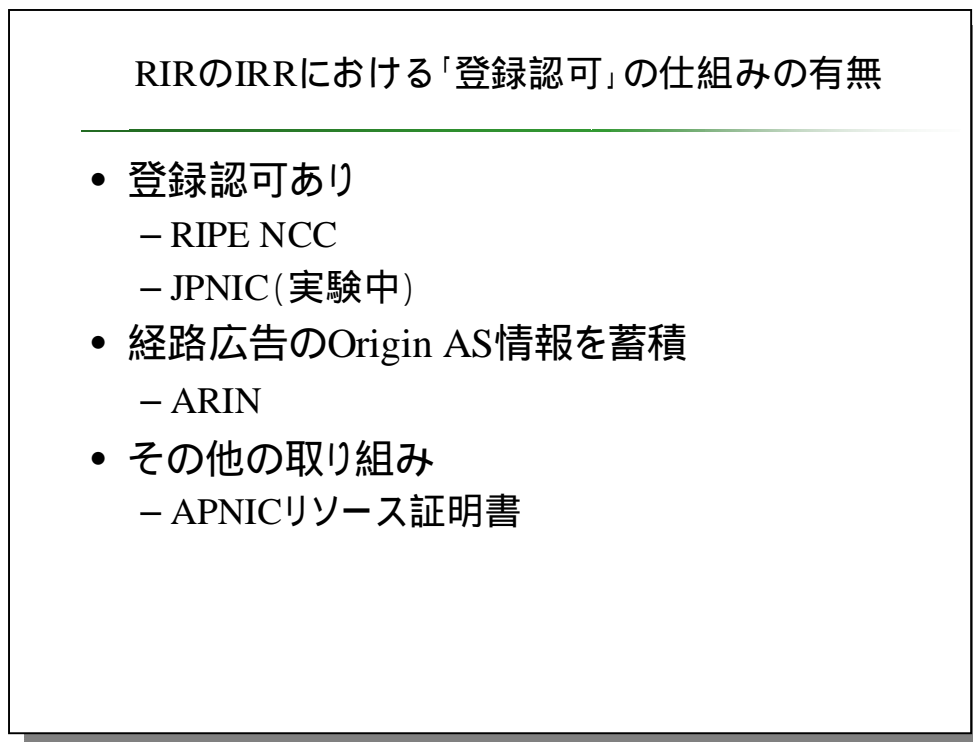


図 4-39 RIR の IRR における「登録認可」の仕組みの有無

JANOG21 では、RIR での取り組みと JPNIC の取り組みをまとめて紹介した（図 4-39）。

IP アドレスの利用認可の登録（図では登録認可）は、RIPE NCC と JPNIC で実施中である。ARIN では Origin AS の情報を蓄積できる申請テンプレート（書式）を 2006 年度より使っている。その他に APNIC のリソース証明書の取り組みがある。

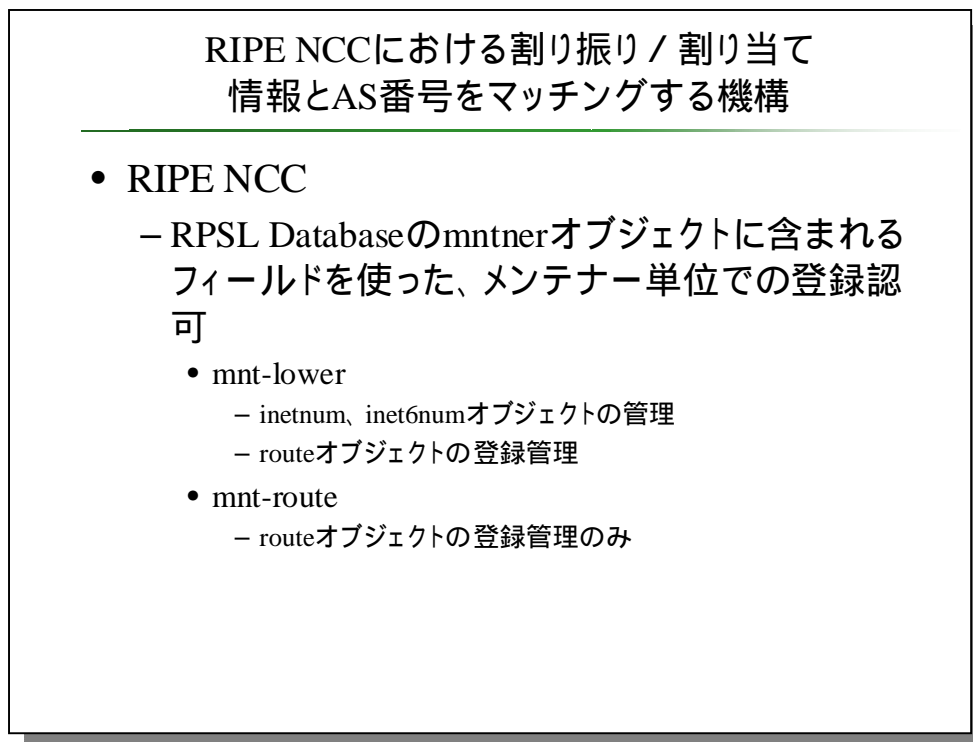


図 4-40 RIPE NCC における割り振り / 割り当て情報と AS 番号を  
マッチングする機構

RIPE NCC は mnt-lower と mnt-route を使った登録認可を実現している。mnt-lower は IP アドレスの割り振りが行われているケースで有効であり、mnt-route はルーティング業務を他社に委託している場合に有効である。

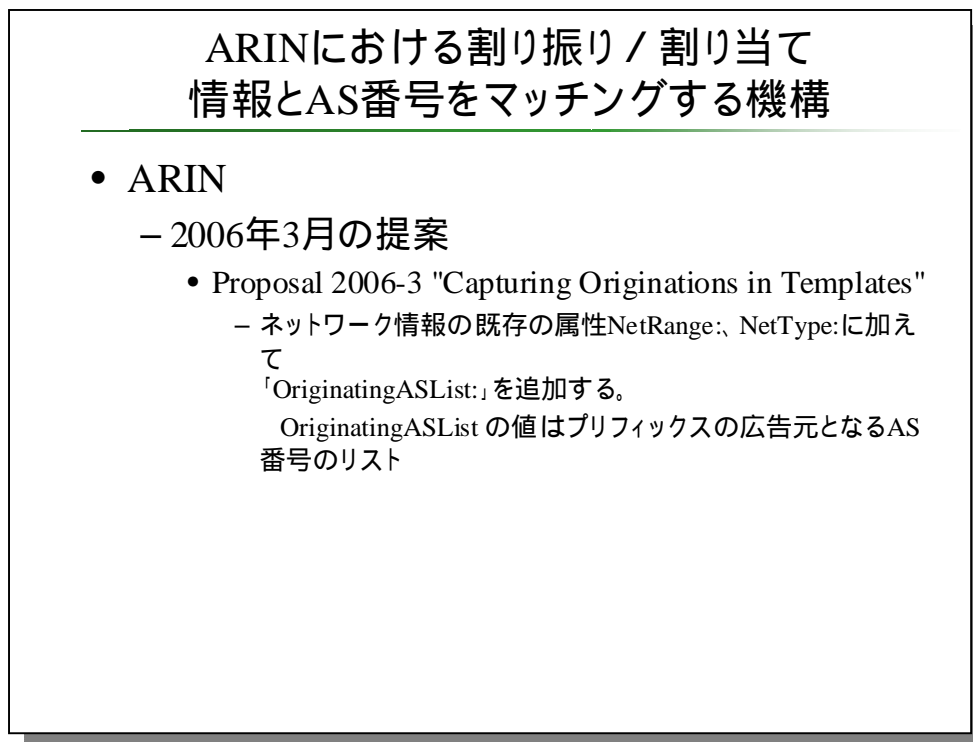


図 4-41 ARIN における割り振り / 割り当て情報と AS 番号を  
マッチングする機構

ARIN では、Proposal 2006-03 と呼ばれるポリシー提案で、Origin AS の情報を収集するテンプレートの採用が提案された。すでにこの提案は実装済みであり、ARIN XX での報告によると実際に Origin AS の情報が集まりつつある。

APNIC では、IP アドレスの認可登録の業務の観点よりも、新しい IP アドレスの使用権を示す電子証明書、リソース証明書の開発と標準化に力が入れている。

経路情報の登録機構の利用実験は、Web ページやメーリングリストでのアナウンスに加えて、JANOG でもアナウンスを行った。

## 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。

図 4-42 利用実験に必要なもの

実験利用には、JPIRR へのメンテナーの登録と、S/MIME 対応のメールソフト、登録機構を使うための USB トークンが必要である。USB トークンは申し込み後に JPNIC から発送しているため、実質的には JPIRR へのメンテナーの登録が必要になる(図 4-42)。

また IP 指定事業者が、認証用の電子証明書を取得している必要がある。

## 会場でのディスカッション(1)

- 経路ハイジャック(オペミス含む)の対処法
  - ハイジャックされた経路にたいしてmore specificな経路を流す。
  - 経路広告元のASに連絡する。ASに連絡が取れなければ、その国のコミュニティとか上流ISPとかに連絡してみる。
  - オペミスも多い。経路ハイジャック7件。
- 経路情報の登録認可機構に関する意見
  - IRRではオブジェクトがミラーリングされているので、複数のIRRにオブジェクトを登録する必要はないと思う。割り振り元のレジストリにあるIRR (RIPE NCC)には登録しているが、登録された信頼性の高いデータを他のIRRでも見えるようにしたほうが良いのではないか。ASのネットワークのオペレーターがIRRを引いてわかるようなVisibilityが大事。
- IRRを使っているかの挙手結果
  - RADB:10名ほど
  - JPIRR:10名よりは少ない
- IRRの利用に関する意見
  - RADBはインターネット全体に広く知らしめるため
  - JPIRR信頼性の高いデータを蓄積するため、という理由で両方に登録している。

図 4-43 会場でのディスカッション(1)

はじめに、経路ハイジャックが起こったときの対処法について議論が行われた(図4-43)。対処法は経路情報の受け手となる自ASにおける対処法と、経路ハイジャックの発信元と考えられるASに近いネットワークにおける対処法の二つが挙げられた。ハイジャックされた経路に対して、more specificな経路を流すと、各ルータの経路表でハイジャック経路よりもその経路情報が優先されるため、本来のネットワークの接続性を維持できる、実効性の高い方法であるが、ネットワークオペレーターの中にはspecificな経路情報をフィルターしてしまうケースがあり、どの程度の範囲で、どの程度の有効性があるかは定かではない。経路広告元のASに連絡する方法は、より根本的な解決策である。経路の広告元がハイジャックをやめれば被害も止められる。しかし悪質な経路ハイジャックであったり、連絡のつかないようなASであったりすると効力はない。経路ハイジャックの中にはオペレーションミスによるものが多いという意見があげられたが、この後の議論の中で、故意によるものを実際にやられたという情報も寄せられた。

経路情報の登録機構については、IEPGミーティングで出た意見ほど前向きな意見は得られなかった。というのも、JPIRRを利用している理由が、信頼性の高いデータの蓄積という、必須であるとは言えない理由であった。RADb<sup>7</sup>に登録する方がJPIRRよりも実効的であるといったニュアンスが感じられた。特にIRR、特にRADbに対する信頼の置き方がIEPGミーティングでの反応とは異なるようである。

<sup>7</sup> RADb  
<http://www.radb.net/>

## 会場でのディスカッション(2)

- IRRのメンテナーやAS番号を意識したIPアドレスの管理に関する意見(登録認可機構がワークするか)
  - IPアドレス担当者とIRR担当者は二ホップ以上離れているし、担当者が代わったりするので、人を把握することは難しいと思う。  
メンテナー名が必要で、人を覚える必要はない。
  - IPアドレス管理指定事業者とAS番号割り当て先組織は現状バインドしていない。
  - IPアドレスを持っているところがASと経路広告をしているところを渡り歩いているのを見ている。
  - IPアドレス管理指定事業者の担当者にはこの仕組みは複雑すぎて説明してもわからないのではないか。
  - 証明書の仕組みが入るとさらに複雑になるのではないか  
いまはPAアドレスという最小限のセットでやっているの  
で、要望などを挙げて欲しい。

図 4-44 会場でのディスカッション(2)

次に、経路情報の登録機構が実際に使えるものかどうか、という観点の意見交換を行った(図 4-44)。

挙げた意見は、IP アドレス担当者と IRR 担当者の関係がなくなっているので難しいという意見を始め、IP アドレスの管理業務を行っているものと AS 番号の管理を行っているものが互いを知らずに業務を行っているという意見が多かった。

これは経路情報の登録機構を使った業務が難しいという意見であると同時に、経路ハイジャックに対して、そして IRR に登録していた route オブジェクトが間違っていたような状況に対して、人的ネットワークを通じた連絡以上の対策が、検討・開発されていないように受け取れた。

今後、ルーティング業務において悪意のあるオペレーターの存在を考える必要があるとすると、RIPE NCC や ARIN、そして APNIC で導入されつつあるような IP アドレスの利用認可の概念を日本国内で普及 / 啓発していく必要があると考えられる。

### 4.11. 経路情報の登録機構と JPNIC 認証局の連携

経路情報の登録機構は、これまでに述べた IP アドレスの利用認可という役割の他に、

IRR におけるユーザ認証で使える電子証明書を提供するという役割もある。経路情報の登録機構は内部に認証局機能を持っており、ユーザ管理機能の一環として電子証明書の発行や失効ができる。この認証局機能は 2002 年度以降に構築が行われてきた JPNIC 認証局と連携して行われている。

これは、JPNIC の IP アドレス管理業務における信頼構造に則って各種の業務が行われるような、信頼構造を作る意味を持っている。ユーザ認証に対する信頼性や、登録される情報に対する信頼性は、外部の利用者にとって、広義の JPNIC コミュニティに対する信頼に依存している。JPNIC は業務の信頼性構築の為に、認証基盤を構築し、この基盤に則って業務を行う者に適切な義務を課すことで、業務の信頼性向上が図ることが可能となる。

本節では、JPNIC 認証局が IP アドレス管理業務の中で、経路情報の登録機構とどのように連携しているかについて述べる。

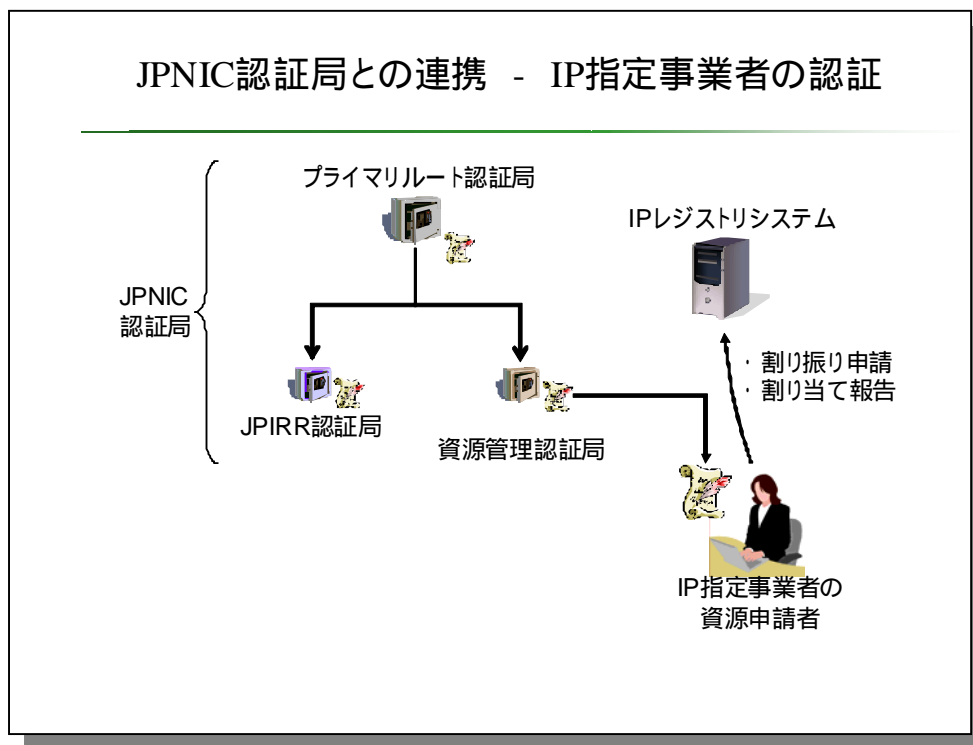


図 4-45 JPNIC 認証局との連携 - IP 指定事業者の認証

まず、許可リストの確認の基盤となる情報は、IP レジストリシステムに登録された IP アドレスの割り振り情報である。従って、IP アドレスの割り振り情報の信頼性確保が重要である。そのために登録者の認証を行い、かつ適切な割り振り業務を行うことが必要になる。



IP レジストリシステムに割り振り申請や割り当て報告を行うのは、IP 指定事業者の資源申請者である。JPNIC 認証局は資源管理認証局を使って資源申請者の電子証明書を発行している。資源申請者の認証は、JPNIC 認証局の信頼点であるプライマリルート認証局を信用することで、オンラインでの認証が可能になる。

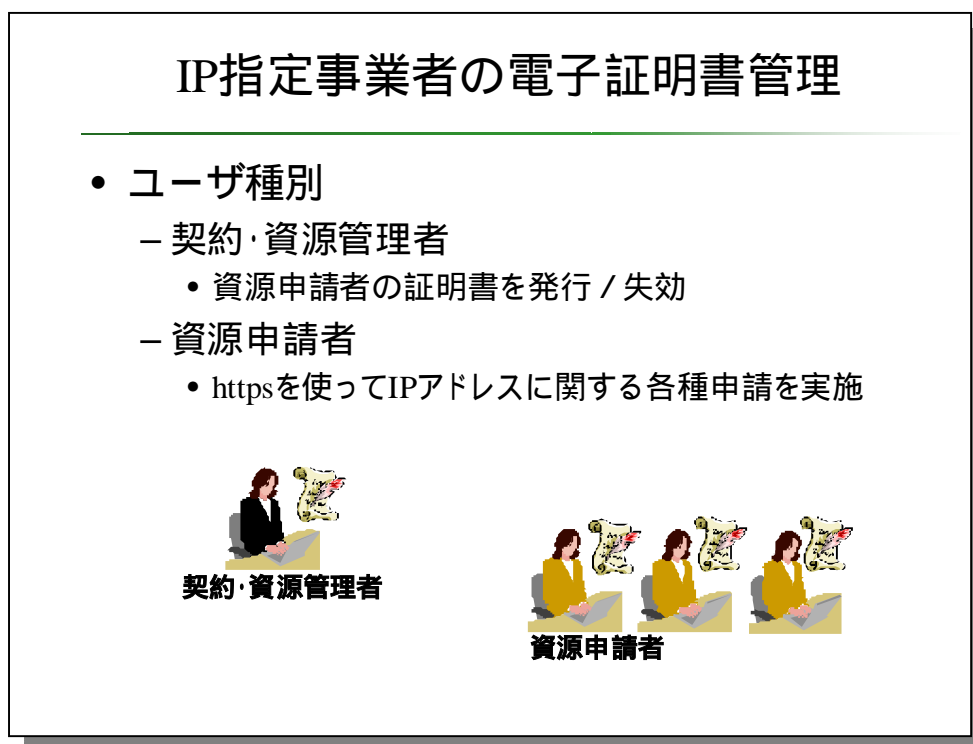


図 4-46 IP 指定事業者の電子証明書管理

資源申請者の証明書は、各 IP 指定事業者に設けられた「契約・資源管理者」によって管理される。これは、資源申請を行う者の本人性確認は、IP 指定事業者内で行われているためである。また JPNIC の申請業務に必要なクレデンシャル（認証に使われるデータ）も同様に IP 指定事業者内の業務管理者によって行われている。資源管理認証局（IP アドレス認証局（認証））は、契約・資源管理者に証明書管理の Web インターフェースを提供している。その Web インターフェースでは、資源申請者の本人性確認を行ってから証明書の発行が行われる。

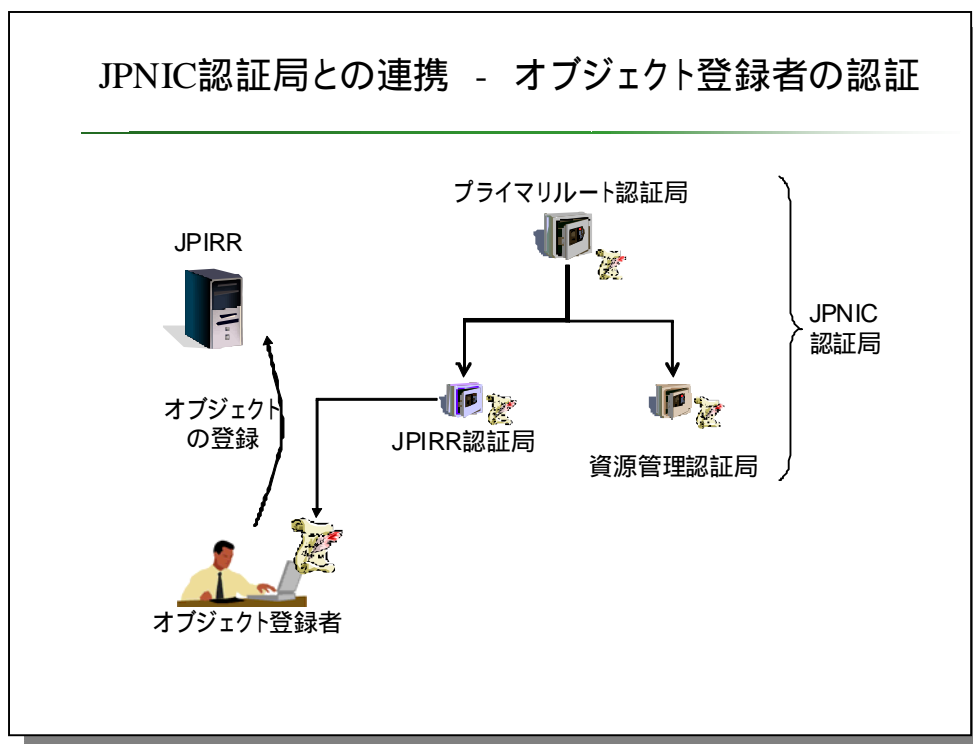


図 4-47 JPNIC 認証局との連携 - オブジェクト登録者の認証

JPIRR における登録者の認証も IP 指定事業者と同様である。JPIRR にオブジェクトを登録するもの「オブジェクト登録者」は、JPIRR 認証局（経路情報の登録機構の一部）の認証業務に則って証明書の発行を受ける。この電子証明書もプライマリルート認証局を信用することでオンラインでの検証が可能になる。

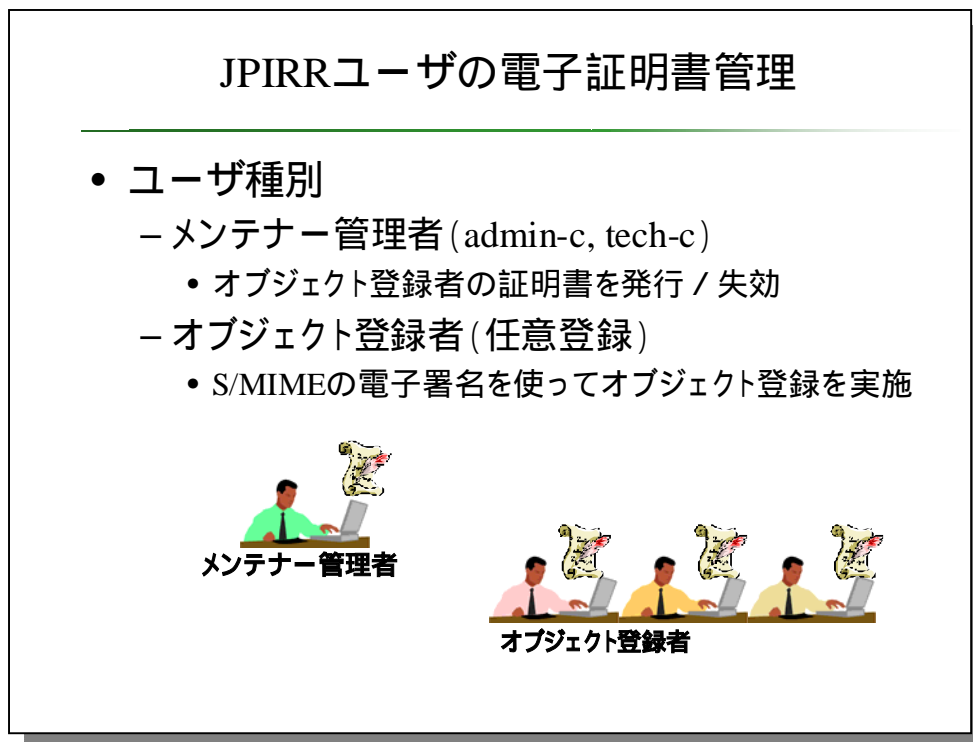


図 4-48 JPIRR ユーザの電子証明書管理

JPIRR のオブジェクト登録者の証明書は、各メンテナーで設けられた「メンテナー管理者」によって行われる。これは IP 指定事業者の場合と同じように、JPIRR にオブジェクト登録を行うユーザの本人性確認は、メンテナーの管理を行っている者によって行われているためである。JPIRR の登録業務に必要なクレデンシャル、パスワードや PGP の鍵の登録なども同様にメンテナーの管理者によって行われている。JPIRR 認証局は、メンテナー管理者に証明書管理の Web インターフェースを提供している。その Web インターフェースでは、オブジェクト登録者の本人性確認を行ってから証明書の発行が行われる。

#### 4.12. 認証業務規程 (CPS) について

JPNIC 認証局の運用にあたり、CPS を策定し、更に業務フローを規定して認証業務を行っている。業務フローは詳細である為ここでは割愛するが、2007 年度にも CPS の見直しを行ったので、紹介する。

認証局は、先に述べた認証基盤を構成する要であり、この運用のレベルによって認証基盤の信頼性が変わる。JPNIC 認証局はプライベートな PKI ドメインを構築しており、業務に合ったレベルの運用を行っている。

レジストリにおける認証局の運用は、RIR コミュニティでも注目されつつあり、IETF

で CPS を閲覧したいという要望があった。IETF の SIDR WG では、リソース証明書のためのレジストリの CPS テンプレートがドキュメント化されており、今後 JPNIC 認証局の CPS との調整も必要になると考えられる。そこで JPIRR 認証局とプライマリルート認証局の CPS の英語訳を作成した。JPIRR 認証局の認証業務規程とその英語訳を Appendix として載せた。

### 4.13. まとめ

本調査研究のもう一つの柱である「IP アドレス認証の展開」については、JPNIC における認証局を応用した経路情報の登録機構に関する調査研究を行った。経路情報の登録機構は、インターネット経路制御においてルーティング業務担当者に使われている IRR の登録情報を正しく保つ仕組みである。

本調査研究では、本機構の実験運用を行い、フィードバックを通じて明らかになった課題点に対応するための改修を行った。また本機構に関するプレゼンテーションを海外では IEPG で行い、国内では JANOG で行った。そこでのディスカッションの結果、IEPG では高い評価を受ける一方、国内では仕組みが難しそうだという声があがるなどした。

2007 年度、実験運用を開始したわけだが、本機構を本格的に IP アドレス管理業務に組み込むには更に利用者を増やし、利用実験を行う必要があると思われる。今後も実験を継続し、インターネット経路制御に資するような仕組みの確立を目指したい。

#### 第4章 IP アドレス認証の展開に関する調査研究