第 2 章　RIR におけるアドレス資源の認可機構

内容

- RIPE NCC における認可機構
- ARIN における認可機構の議論
- APNIC におけるリソース証明書

ほか

2. RIR におけるアドレス資源の認可機構

2005 年度の調査研究を通じて、インターネットにおける大規模な不正利用排除にはアドレス資源の認可機構が重要であることが判明した。

RIR（Regional Internet Registry – 地域インターネットレジストリ）のうち、ヨーロッパ地域の RIPE NCC、北米地域の ARIN、アジア太平洋地域 APNIC は、JPNIC と同様に IP レジストリシステムと IRR（Internet Routing Registry）を持っているが、アドレス資源の認可に対する考え方が各々に異なっている。

これらの主要 RIR で現地調査を行い、アドレス資源の認可機構とアドレス資源情報のセキュリティ、およびリソース証明書の動向について調査した。リソース証明書はアドレス資源の利用認可を電子証明書を使って行うもので、主に APNIC が中心となって開発が進められている。

2.1. RIPE NCC

RIPE NCC はヨーロッパ地域の IP アドレスの管理を行っている地域インターネットレジストリである。RIPE NCC は 1 年に 3 回 RIPE ミーティングと呼ばれるミーティングを開いており、ここではデータベースのセキュリティや IP アドレス管理ポリシーなどについて議論されている。リソース証明書についての議論も開始している。そこで第 53 回 RIPE ミーティングに参加し、また現地のスタッフにヒアリングを行ってこれらについての動向を調査した。

2.1.1. 第 53 回 RIPE ミーティングを通じた調査

2006 年 10 月 2 日～6 日にオランダのアムステルダムで開かれた第 53 回 RIPE ミーティングに参加した。今回は、セキュリティに関する議論の動向を調べるとともに、RIPE NCC のスタッフに、RIPE データベースの仕組みや課題についてヒアリングを行った。

第 53 回 RIPE ミーティングでは、初日に主に LIR（Local Internet Registry）向けのチュートリアルが行われ、初日から 3 日目にかけて全体会議である Plenary が行われた。3 日目以降は WG のセッションが開かれた。ミーティングの参加登録者は 355 名で、ここ 1 年ではほぼ平均的な人数である。

セキュリティに関しては、全体会議である Plenary と NCC Services WG でリソース証明書に関する議論が、Database WG で IRT オブジェクトと CRYPT-PW を廃止する案についての議論が行われた。

□リソース証明書に関して

リソース証明書については、Plenaryをはじめ複数のWGで議論が行われていた。リソース証明書はIPアドレスやAS番号が入った電子証明書[1]で、WHOISの代わりにIPアドレスの割り振りや割り当てを証明するために使われる。IPアドレスの割り振り構造に従って発行され、そのツリー構造の末端部分ではIPアドレスとAS番号の両方が入った電子証明書が発行される。この電子証明書はBGPなどにおける経路制御を安全にするために使われることが想定されている[2]。リソース証明書の実装は、2006 年 4 月頃よりAPNICとRIPE NCCが中心となって進められてきた。

Plenary では、APNIC の Geoff Huston 氏によって、リソース証明書を使って IRR の登録情報に電子署名を行うデモが行われた。この電子署名は IRR の route-set オブジェクトに対して行われるもので、その route-set オブジェクトに含まれる route オブジェクトが authorize(認可)されたことを意味している。route オブジェクトには広告元(すなわちそのアドレスを持つノードの収容先)となる AS 番号が記載されているため、LIR がその AS に対してインターネットでその IP アドレスを使うことを認可した、という意味になる。この認可の概念は ROA(Route Origination Authorization)と呼ばれている。インターネットレジストリの割り振りを意味するリソース証明書は 2006 年 7 月の時点で既に実装されていたので、この ROA を示すリソース証明書の発行によって、ツリー構造の最上位から末端までのすべてのリソース証明書が発行できる状況になったことになる。

Plenary の会場では、このプログラムが無事に動作したことに対して拍手が送られる一方、リソース証明書の発行に使われるデータベースが信頼に足るかどうかという根本的な疑問が投げかけられた。リソース証明書自体が信頼できる仕組みであっても、証明書の元になるデータが間違っていたら意味がないからである。RIPE NCC では既にこの点に着目しており、リソース証明書の導入に関して、予測される効果やインパクトを評価する活動が提案されている。この活動は NCC Services WG で発表されていた。

2007 年度のRIPE NCCの活動計画によると[3]、RIPE NCCでは 2006 年度のAPNICの実装プロジェクトへの参加は継続され、リソース証明書に着目した活動が行われていくとされている。NCC Services WGでのRIPE NCCのAlex Pawlik氏の発表では、2007 年度の本格的な活動に先立って、Evaluation Task Force(評価タスクフォース)[4]の立ち上

[1] RFC3779
http://www.ietf.org/rfc/rfc3779.txt
[2] Secure Border Gateway Protocol(S-BGP)
--- RealWorldPerformanceandDeploymentIssues
http://www.ir.bbn.com/sbgp/NDSS00.S-BGP.ps
[3] Newor Significantly Developed Activitiesfor2007
http://www.ripe.net/ripe/draft-documents/gm-october2006/ap-2007.html#3
[4] RIPE Certification Task Force

げが提案されていた。この評価は必要となる業務の詳細やポリシーへの影響を明らかにすることが目標になっている。Evaluation Task Forceは現行の開発活動やトライアルに参加しつつ、まずリソース証明書が持つ目標とその目標に現行のアプローチが適するかどうかを調査して報告することになっている。最終的には 2007 年 5 月に予定されている第 55 回RIPEミーティングで、導入の方向性について決定が行われることとなる。

これは、これまで実装を行ってきたAPNICをはじめ、リソース証明書の効果に対して同様の疑問が投げかけられているARINコミュニティ、そして認証局に関する調査研究を行ってきた当センターにとっても注目すべき活動である。というのもRIPE NCCのデータベースは、アドレスの割り振り／割り当て情報を登録するデータベースと経路に関する情報が登録されるIRRが統一されている上に、インターネットで経路広告されているアドレスとIRRの登録情報を比較する調査プロジェクトが行われてきていることが背景にある[5]。これによって、RIPE NCCでは、登録されているにもかかわらず実際には使われていないアドレスを調べることが可能である。使われていないアドレスや登録情報と異なる経路広告の量がわかれば、リソース証明書が現状で何割程度のアドレスに対して発行できるのか、またそれらの管理が現実的なものなのかどうかが判明する可能性がある。

□RIPE データベースのセキュリティ機能に関して

RIPE データベースには、ユーザ認証やユーザが編集できる登録情報の範囲を限定するようなデータベースを保護する機能の他に、あるアドレスで起こったコンピューターインシデントに関する連絡先となる IRT(Incident Response Team)の情報を提供するという、コミュニティのセキュリティを考慮した機能がある。

ここでは RIPE ミーティングの 5 日目に行われた Database WG の議論の中から、ユーザ認証の機能である CRYPT-PW の廃止に関する提案と、IRT 情報を提供する IRT オブジェクトに関する議論を紹介する。

RIPEデータベースはLIRに対して 4 つの認証方式を提供しており、ユーザは好きなものを選んで使用できるようになっている。現在提供されている認証方式は、CRYPT-PW、MD5-PW、PGP-KEY、X509 で、CRYPT-PWとMD5-PWはいわゆるパスワード認証方式である（2007 年 3 月現在、CRYPT-PWを使った認証は廃止の方向で活動が進められている）。LIRがメールで申請業務を行う場合、送信するフォームの中であらかじめ登録されているパスワード文字列を記入する。パスワード文字列が正しければ、RIPEデータベースはユーザ本人によって送信されたと判断でき、申請内容のチェックに移ることができる。-PWの前についているCRYPTとMD5 は、パスワード文字列をRIPEデータベースの中で処理する方式の名前である。CRYPTは昔のUNIXでパスワード文字列を隠蔽す

http://www.ripe.net/ripe/tf/certification/index.html

[5] Routing Registry Consistency Check Project
https://www.ripe.net/projects/rrcc/index.html

るために使われていた方式で、パスワードとして指定できる文字の長さは 8 文字である。一方、MD5 はメッセージダイジェスト関数のMD5 を用いた方式で、RIPEデータベースでは 65 文字のパスワードをつけることができる[6]。

今回の提案は、CRYPT-PW で利用できる文字列が短いために、ブルートフォース攻撃(総当たり攻撃)や辞書攻撃といった基本的な攻撃が通用してしまうため、今後この方式の利用を廃止しようというものである。既に第 52 回 RIPE ミーティングで基本的な方針についてはコンセンサスが得られており、今後はスケジュールについて検討したいとのことであった。しかし、約2300のメンテナーでCRYPT-PWが使われているそうで、完全な廃止にはやや時間がかかりそうである。また変更手続きが間に合わなかったユーザへの対応なども検討する必要があると考えられる。

一方、IRT オブジェクトに関する議論は潜在的な問題を抱えたままの提案となった。今回の提案は WHOIS を使って、ある IP アドレスを元に inetnum オブジェクトが検索された場合、検索時のオプションに-c が指定されていなくても WHOIS のサーバは関連する IRT オブジェクトを返すというものである。従って WHOIS で IP アドレスを調べるだけで IRT オブジェクトが自動的に表示されるようになる。このことはユーザの観点では便利になるという意味でとてもよいことである。また IRT オブジェクトは一度一つのメンテナーに対して定義しておけば、そのメンテナーによって管理されている割り振り／割り当て情報のすべてに対して適用されるという意味で、LIR にとっても利便性は高いと言える。そのため RIPE NCC では IRT オブジェクトの利用を推奨している。

IRT オブジェクトの普及に関する潜在的な問題は abuse-mailbox という類似した連絡先情報の存在である。abuse-mailbox は inetnum や inet6num といった個々の割り振り／割り当て情報に付加される情報で、そのアドレスブロックにおける abuse(不正や不具合に対する連絡)用のメールアドレスが記載されている。abuse-mailbox は 2004 年 1 月の第 47 回 RIPE ミーティングで採用されたもので、それ以降多くの inetnum/inet6num で登録されてきた。一方、IRT オブジェクトは 100 程度に留まっており、利用されているものは 60 程度に留まっている。しかし両者共に効果が見えにくいことなどから、議論の余地が大きく、RIPE のコミュニティの中でも扱いにくい話題になっているようである。

2.1.2. 認可機構の詳細

RIPE NCC では route object の authorization 機構に関するヒアリングを行った。その結果、RIPE データベースは IP アドレスの割り振り／割り当て情報と IRR が統合さ

[6] Crypted password generation
https://www.ripe.net/cgi-bin/crypt.cgi

れたシステムであるだけでなく、LIR が AS 管理者に対して経路情報(route オブジェクト)の登録認可する機構を備えていることがわかった。この機構によって、IP アドレスの割り振り先と AS の運用が別の組織によって行われていても、どの IP アドレスがどの AS から経路広告されるのかが、絞り込めるようになっている。

他の組織によって間違った経路広告をされてしまうことで、本来は自分のネットワークで使われるべき IP アドレスが使えなくなってしまうことは「経路ハイジャック」と呼ばれている。これを検出し防止するためには、RIPE データベースが持つ機構は有効である。この後の調査で、ARIN のコミュニティでも IP アドレスと AS 番号の組み合わせがわかる仕組みが提案されていることがわかった。

□ヒアリングの目的

JPNIC の「経路情報の登録機構」は route object の登録者を authorization(認可)する機構を通じて、IRR の提供する経路に関する情報の信頼性向上を図るものである。本機構は APNIC, RIPE NCC で検討が進んでいるリソース証明書の原本となると考えられるが、APNIC からは特に authorization に関する見解が見えない。認可機構を持つ RIPE NCC の仕組みを調査し、経路情報の登録機構を設計することの意義の正しさを確認する。また本機構の開発にあたって参考になる認可の仕組みのもつ課題や今後の展開についても調査を行うことを目的とした。

□ヒアリングの結果

ヒアリングの結果は 3 つのポイントにまとめられる。

a. RIPE データベースにおける認可機構

RIPE NCC のデータベースは認可機構を持っており、これまでも運用されていた。RIPE NCC のデータベースはメンテナーと呼ばれる認証情報を用いてユーザ認証と割り振り済み IP アドレスおよび割り当て済 AS 番号等の管理が行われている。認可は LIR のメンテナーと登録者のメンテナーにおける認証(例えば PGP を使った電子署名)の両方が行われなければ登録されない、というものである。登録される情報自体に認可情報が記載されていることになる

b. 運用上の課題

登録済の route オブジェクトのうち、管理者が不在になったものが削除されてこなかった。そのため本来は使われていない経路の情報が登録されたままとなり、これをインターネット上の経路情報と比較すると不整合または余計な登録情報となる可能性がある。

項目 a で述べた mnt-route 及び mnt-by は、別々のメンテナーである。どちらかの組織が ISP 事業をやめた場合、route オブジェクトは本来の意味では不適切な登録であり、削除する必要がある。しかしこの削除によって起こる影響、つまり IRR として参照された場合に重要な経路情報が伝達されなくなる状況を懸念して削除されることにはなっていない。

このことで不要な route オブジェクトが存在し続けている状況がある。aut-num オブジェクトの mnt-by に指定されたメンテナーの LIR が ISP 事業をやめた場合にその aut-num オブジェクトが削除されないことも指摘されていた。これは一度取得された AS 番号は基本的に再利用されず、消費し続けられることになる。

c. ポリシー実施の課題

LIR の解約の際などに割り振り済および認可済 route オブジェクト及び AS オブジェクトの削除が実施されてこなかった。登録上明らかに削除できるものは一括削除できるものの、これまでは特に行われてこなかった。これは AS 番号の枯渇の一因になっている。しかし 32bit 化の提案があることから、RIPE NCC IP アドレス管理部門では特に問題視されていない。技術部門のスタッフは不要な route オブジェクトが残存することに対して懸念を示しており、今後の課題だと結論付けていた。

○認証対象について

メンテナーには admin-c（運用責任者）tech-c（技術連絡担当者）の連絡先がそれぞれ複数登録可能である。登録される情報は nic-hdl と呼ばれ、これがユーザ一人に使われるか、複数のユーザによって使われるかは規定されない。

nic-hdl として person オブジェクトが指定された場合であっても、role オブジェクトという person オブジェクトを複数指定できるオブジェクトの場合でも、各々が複数のユーザによって使われるかどうかはケアしないという方針である。

認証する方式はメンテナーで指定される。使用される方式は CRYPT-PW, MD5-PW, PGP-KEY, X509 である。申請を送付しているユーザが前述した person であるかどうかはケアされず、純粋に認証方式に準じた確認が取れれば認証を完了する仕組みである。

○認可に使われるメンテナーの指定について

割り振り済 IP アドレスおよび再割り振り済の IP アドレスは inetnum オブジェクトとして登録され、また割り振り済 AS 番号は aut-num オブジェクトとして登録される。これらのオブジェクトには以下のフィールドを使って管理元(すなわち割り振り／割り当て先)が記載される。

mnt-by: <メンテナー名>

メンテナー名によって指定されたメンテナーの権限を使って内容の変更を行うことができる。メンテナー名は当該オブジェクトの登録時に RIPE NCC が記載する。

mnt-lower: <メンテナー名>

メンテナー名によって指定されたメンテナーの権限を使って内容の変更を行うことができる。mnt-lower は IP アドレスの再割り振りの際に使われ再割り振り先のメンテナー名が記載される。これは同オブジェクトの mnt-by で指定された LIR が記載する。

mnt-route: <メンテナー名>

メンテナー名によって指定されたメンテナーの権限を使って内容の変更を行うことができる。mnt-route は route オブジェクトの登録を認可する先のメンテナー名を指定するために使われる。これは同オブジェクトの mnt-by で指定された LIR が記載する。

例：

inetnum: 10.10.0.0-10.10.255.0

mnt-by: MNT-A

10.10.0.0/16 は MNT-A に割り振られ、本 inetnum オブジェクトを MNT-A が変更できることを示す。例えば、再割り振りを行うために mnt-lower の追記や管理元を増やすための mnt-by の追記、特定の AS 管理者(AS 番号の管理を行っているメンテナー)による route オブジェクトの新規登録を認可するための mnt-route の追記を行うことなどができる。

inetnum: 10.10.0.0-10.10.255.0

mnt-by: MNT-A

mnt-lower: MNT-B

mnt-route: MNT-R

10.10.0.0/16 は MNT-A に割り振られ、本 inetnum オブジェクトを MNT-A が変更できることを示す。本アドレスブロックはそのまま MNT-B に再割り振りされ、MNT-B も同様に本 inetnum オブジェクトを変更できる。

mnt-route は本 inetnum に含まれる IP アドレスブロックの route オブジェクトを登録できるメンテナーの指定に使われる。この指定がない場合は mnt-by および mnt-lower で指定された MNT-A,MNT-B の両方が route オブジェクトの登録できる。しかし mnt-route がある場合、MNT-R のみが route オブジェクトを登録できるようになる。

経路情報の登録機構はいわば mnt-by, mnt-lower, mnt-route をリスト形式で格納するものであると考えられる。

2.2. ARIN

ARIN は北アメリカ地域を対象とする地域インターネットレジストリである。ARIN は年に 2 回ミーティングが開かれており、データベースのセキュリティや IP アドレスポリシーに関する議論が行われている。

北アメリカ地域には、RADB[7]と呼ばれる国際的に著名なIRRがある一方、ARINでは多くのネットワークオペレーターに利用されているIRRは運用されてきていなかった。しかしIPアドレスの申請業務の電子証明書をいち早く取り入れると共に、リソース証明書に関連する議論も行われつつある。そこで第 18 回ARINミーティングに参加すると共に、関連するポリシーの提案を行っている複数の人物にヒアリングを行って調査を行った。

2.2.1. 第 18 回 ARIN ミーティングにおける調査

本調査研究で取り組んでいる「経路情報の登録機構」と同様の目的をもつ仕組みに関して、ポリシーに関するセッションにおいて議論が行われた。

この議論はPolicy Proposal 2003-3 "Capturing Originations in Templates"[8]に基づくもので、ARINの割り振り・割り当ての申請書式に、そのアドレスを経路情報として広告しうるAS番号のリストを登録できるようにするものである。登録された情報は

OriginatingASList:

という属性の値として保存され、WHOIS 等で提供されるとされている。この情報によって WHOIS 利用者が、IP アドレスの prefix と AS 番号のマッピングを得ることができるようになり、経路制御の安全性向上に寄与すると考えられている。会場での挙手の結果は、賛成：60 程、反対：30 弱であった。

以下、提案とプレゼンテーションの詳細などについて述べる。

本提案は IETF SIDR WG の chair 及び RFC4272 の著者である Sandra Murphy 氏によって、2006 年 2 月頃に ML にて行われたもので、ミーティングでの議論は前回の ARIN ミーティングで初めて行われた。今回の氏のプレゼンテーションは 150 名程の参加者がいる中で行われた。プレゼンテーションで話された内容などは以下の通りである。

---

[7] RADB
http://www.nic.ad.jp/ja/tech/glos-kz.html#03-radb

[8] Policy Proposal 2006-3: Capturing Originations in Templates
http://www.arin.net/policy/proposals/2006_3.html

○提案のモティベーション
リソース PKI と同じモティベーションで認可リストを whois の返答に含める。
○ARIN における提供方法
・IRR
・bulk 転送
・ftp
○ARIN において提供されないもの
・データの検証
○テンプレートを使う理由
・オペレーターへの認可業務の啓発
・IRR のデータを正確に保つ
・リソース証明書に移行するためのデータ収集
○IRR との違い
・IRR は mnt-by を POC と同様に検証していない。
・IRR は mnt-by があるが、route オブジェクトを ARIN は検証せずに
登録している。
○必要になること
・POC と mnt-by の同期
・route オブジェクトの検証
○導入のインパクト
・実装に 3-6 か月かかると考えられる。
○ARIN がリストに責任を持てるかどうか
・これは rwhois と同じ。

議論された内容は以下の内容である。

・ARIN 以外から割り振られた情報について扱えない。現行の運用を変える
ことに対して、目標とすることと得られることの関係が見出せない(反対意見)
・認証対象(OrgID)と結び付ける案があるのでは。
弱い認証が行われた上で登録されうる。(反対意見)
・取り組みの重要性 x 2 (賛成意見)

□Policy Proposal 2006-3 の要約

参考のため、本提案の要約を以下にまとめる。

○提案の主旨

IPv4 アドレス及び IPv6 アドレスの割り振り、再割り振り、割り当て、再割り振り、再割り当て等の情報に、それらを広告する AS 番号を付加した情報を収集する。

この情報は少なくとも 1 日に 1 回生成され、IP アドレスとそれを広告することが許可された AS のマッピングの為に使われる。個々のアドレスと AS 番号の組み合わせや、検索サービス等で必要とされる形式のデータの、ARIN における生成に関しても本件の対象とする。

ARIN はコミュニティの要望に応じてバルク転送やその他の形式での提供ができるようにする。再配布に関する制限はなく、再構成(repackage)も許される。なおバルク転送で提供される WHOIS データは WHOIS データへのバルクアクセスに関する AUP（Acceptable Use Policy）に従うものとする。本ポリシーは NRPM（Number Resource Policy Manual） 3.4 節に結合されると考えられる。本ポリシーは承認後 60 日以内に実装されるものとする。

○提案の根拠

プリフィックスの広告元である AS(Origination of prefixes by ASes)がその広告元であることの authority を持たないことは、現在のルーティングシステムの根本的な問題となっている。認可されたプリフィックスの広告元のリストは、オペレーターの利益となる。

オペレーターの利益
- ・広告の偽装に対処するためのルーティングフィルターの生成
- ・プリフィックスの広告を必要とする顧客との連携
- ・経路制御の問題の原因究明

ARIN はアドレス資源を IRR に変換するメカニズムを持たず、またオペレーターは(IRR の)route オブジェクトをメンテナンスする程勤勉ではないという点を考慮し、アドレス資源を管理する ARIN においてプリフィックスの広告元に関する認可の情報収集における主な目的を以下の 2 点とする。

ARIN における認可情報収集の目的
- ・初期及びそれに続くトランザクションを、ARIN において精密に検証できることによる利点
- ・リソース要求等を生成するなどのオペレータの習熟を継承することによる利点

○申請の書式
既存の属性
NetRange:
NetType:
追加される属性
OriginatingASList:

OriginatingASList の値はプリフィックスの広告元となる AS 番号のリストである。

□登録情報のプライバシー保護に関する議論

登録情報のプライバシー保護については「2006-1: Residential Customer Privacy」[9]という提案に関して議論が行われた。

はじめに ARIN の Ray Plzak 氏によって概説があり、次に提案者の Samuel Weiler 氏によるプレゼン、続いて議論と挙手があった。

○Ray 氏の概説
コンセンサス：現行のものを見直して提案すること
PPML への投稿：46、16 名参加、2 名賛成、3 名反対

○Samuel 氏のプレゼン
モントリオールでのディスカッション
－より包括的なものが必要
－ARIN に対する情報提示の制限かどうかの確認
ARIN における影響
－部分的な郵便番号での実施の可否
極小地域での実施の難しさ
ARIN 地域内で司法権の及ばない地域での実施の難しさ
－匿名となるセットをより縮小し他のデータとの相関関係により個人が特定できるようにする

○議論で出た意見
－賛成意見　　3 ないし 4
・現行のポリシーでは顧客のプライバシー保護に不十分
・データベースの信頼性を維持できる。ただ登録されるすべてのデータは同じデータを持っていないといけない

[9] Policy Proposal 2006-1: Residential Customer Privacy
http://www.arin.net/policy/proposals/2006_1.html

SWIP の場合部分的に登録できるのか　他

－反対意見 5～7 (Randy Bush 氏含む) 以下その理由
・既存の住所のデータとマスクされた公開データの違い
・政府による利用
・ARIN が既存のデータを保持していること
・WHOIS の本来の目的に沿うべき

○挙手の結果
賛成：8 反対：52

□Policy Proposal 2006-1: Residential Customer Privacy の要約

参考のため、JPNIC で作成した要約を以下に載せる。

○提案者：Samuel 氏

○概要

2006 年 2 月 PPML にて提案。ARIN17 での議論に引き続き 2 回目。NRPM 4.2.3.7.6 と 6.5.5.1 節に関連。(3.2 も)居住地利用を想定したユーザへのダウンストリームを行う組織は顧客名の代わりに組織名を使うことができる。"Private customer - XYZ Network"ユーザのすべてのアドレスは"Private Residence"と置き換えることができる。各ダウンストリームはアップストリームの abuse と Technical POC（Point of Contact）を WHOIS に正確に持たなければならない。

○根拠

本ポリシーは顧客の住所を秘匿することができるようにする。多くの場合、郵便番号や市町名だけで個人を特定することができる。特に IP アドレスの割り振りと合わせるとポリシー提案 2003-3 の意図が覆されてしまう。

2.3. APNIC

APNIC はアジア太平洋地域の地域インターネットレジストリで、リソース証明書に関する開発プロジェクトを推進しているレジストリである。

APNIC では年に 2 回ミーティングが開かれており、IP アドレスに関するポリシーの議論や、NIR のシステムに関する議論が行われている。リソース証明書の開発プロジェクトが進められているため、APNIC ミーティングにおけるリソース証明書に関連するセッションでは詳しい内容のプレゼンテーションが行われるなどしている。

そこで第 22 回 APNIC ミーティングに参加し、動向の調査を行った。

2.3.1. 第 22 回 APNIC ミーティングでの議論

APNIC ではリソース証明書と呼ばれる電子証明書を発行する仕組みを作るプロジェクトが進んでいる。このプロジェクトは 2006 年 4 月頃から始まった 1 年間のプロジェクトで、2007 年 4 月以降、APNIC 会員に対する試験的なサービスを始めることを目標に進められている。

本章では、リソース証明書の概要を紹介するとともに、第 22 回 APNIC ミーティングの参加を通じてわかってきた、プロジェクトの考え方と状況について述べる。

□APNIC と IETF におけるリソース証明書

リソース証明書は、IPアドレスとAS番号の利用権利を示す電子証明書である。2004年 6 月に発行されたRFC3779[10]でその構造が提案された、インターネットレジストリのIPアドレスの割り振り構造と同じツリー構造でPKI(Public-Key Infrastructure)の認証局を構築することで、利用されているIPアドレスとAS番号の正当性を保証するための仕組みである。リソース証明書はアドレスの割り振り先に対して発行される。証明書の発行元はCA(Certification Authority)と呼ばれている。割り振り先がさらに割り振りを行うとそこでもリソース証明書が発行されるので、割り振り先にはCAとしての証明書が発行されることになる。IANA（Internet Assigned Numbers Authority）CAの部分は現在の提案内容としては存在せず、RIRが頂点になる案が有力である。

証明書の書式には基本的に X.509v3 の形式が使われ、IPAddr(IP アドレス)やASIdentifier(AS 番号)の値は X.509v3 拡張フィールドと呼ばれる拡張のひとつとして証明書の中に記載される。発行元のリソース証明書は、発行先のリソース証明書に記載さ

[10] X.509 Extensions for IP Addresses and AS Identifiers
http://www.ietf.org/rfc/rfc3779.txt

れるアドレスブロックを内包するようなアドレスブロックが記載される。

この証明書は、ルーティングのセキュリティとアドレス資源管理のセキュリティに役立つと考えられている。ルーティング・セキュリティのための応用として代表的なのがS-BGP[11]である。S-BGPはBBNテクノロジー社のStephen Kent氏によって提案されたプロトコルで、ルーティングプロトコルのBGPを拡張し、ルータ間で交換される経路情報の正当性を電子的に確認できるようにするものである。

□APNIC におけるリソース証明書プロジェクトの進捗状況

APNIC ではリソース証明書について以下のスケジュールが立てられている。

フェーズ 1 (2006/5/1-20066/30)
・認証局の実装
・リポジトリの実装
・IETF SIDR WG への提案

フェーズ 2 (7/1-8/31)
・電子署名付き経路要求の作成
・電子署名付き IRR オブジェクトの取り組み
・CP/CPS 完了

フェーズ 3 (9/1-12/1)
・LIR toolkit (の整備)
・RIR Portal web サービスツール (の整備)

フェーズ 1 は 7 月上旬に行われた第 66 回 IETF に向けた活動、フェーズ 2 は 9 月上旬に行われた第 22 回 APNIC ミーティングに向けた活動であることが読み取れる。認証局の実装は RIPE NCC と共同で開発が進められており、既にフェーズ 1 の認証局の実装とリポジトリの実装が完了していることは、第 66 回 IETF の会期中に行った JPNIC と APNIC の打ち合わせの際に確認されている。

第 22 回 APNIC ミーティングでは、オペレーター向けのセッションである APOPS（Asia Pacific OperatorS Forum）で、APNIC の Geoff Huston 氏によって進捗状況が報告された。今回新しく発表があったのは以下の 4 点である。

[11] Secure BGP Project (S-BGP)
http://www.ir.bbn.com/projects/sbgp/

a. APNIC の Web ポータルで証明書発行サービスを提供すること

b. LIR が証明書管理に利用できるツールの提供

c. IRR の route オブジェクトに対する電子署名

d. Web インターフェースを持つ電子署名ツール

a は、AP 地域のコミュニティに対して情報提供することでフェーズ 3 で取り組む Portal web での実装に関する意見集約を開始したものと考えられる。b、c、d については実際の画面イメージが提示され、フェーズ 2 の実装が完了に近いことが示された。ただし署名ツールの利用者を LIR の中のどの立場にするのか、その電子署名をどのように検証するのか、といった利用面での検討はまだ進んでいないようである。

□リソース証明書にかかわる課題

リソース証明書の実装は、RIPE NCC と APNIC を中心に順調に進められているように見える。しかしその背景には、証明書の発行だけでは解決できない大きな課題がある。筆者はその課題について第 22 回 APNIC の APOPS のセッションで発表した。

一つはリソース証明書に入るアドレスブロックが運用に適するように調節できない問題である。リソース証明書に入るアドレスブロックはアドレスの割り振り元によって決められる。しかし ISP では、割り振られたアドレスをさらに分割し、ネットワークの接続先に応じて伝達される経路情報を切り替えるような運用がしばしば行われる。従って ISP がリソース証明書に記載されるアドレスブロックをあらかじめ選択できるようにしておく必要がある。そうでないと、追加割り振りがあったような場合に、ルータに既に設定された多くの証明書を一斉に入れ替える必要が出てきてしまう。また逆に接続先に対して不必要な経路の情報を、リソース証明書を通じて伝えてしまうことにもなりかねない。

もう一つは ISP におけるリソース証明書の管理の煩雑さである。リソース証明書が使われるようになると、ISP ではルータと経路の管理の他に CA の管理を行う必要が出てくる。CA は CA 自身の暗号鍵の管理や証明書の失効処理といった複雑な業務を必要とする。その上、アドレスの割り振りや返却といった処理はインターネットレジストリによって行われるため、ISP でその情報を基にした証明書管理を行うことは、一部を自動化したとしても煩雑なものになると考えられる。

これらの課題に対して、JPNIC から、IRR と外部 RA(Registration Authority)の 2 つを使う解決案のプレゼンテーションを行った。IRR は ISP のルーティング・オペレーターによって登録情報の管理が行われている。IRR に登録されている route オブジェクトを使ってリソース証明書の発行が行うことができれば、経路制御のために都合のよい証

明書の発行ができると考えられる。また外部 RA と呼ばれている"証明書管理を行うユーザ"を設けることで、ISP 自身が自分に発行される証明書の申請管理を行うことができ、また同時に ISP で CA のシステムを持たなくて済む。

これらの課題と解決策は証明書管理に限定されたものであるが、S-BGP の利用にはさらに大きな課題がある。それはルータにおけるリソース証明書の扱いである。経路情報を交換するたびに電子証明書を検証していたのでは経路を確定するまでに時間がかかり過ぎてしまう。またリソース証明書が完全に検証できなかったからといって接続を切ってしまと、接続が切れやすいネットワークができてしまう可能性がある。リソース証明書の検証のタイミングや検証結果を経路情報にどのように反映すべきか、といった検討が必要である。

□リソース証明書の今後

第 22 回 APNIC ミーティングの発表を見る限り、APNIC におけるプロジェクトは順調に進んでいる。このまま進んでいけばフェーズ 3 も無事終了し、2007 年 4 月には APNIC の Web ポータルである MyAPNIC で試験的に利用できるようになる可能性がある。

一方、前述した課題をクリアするためには、インターネットレジストリと IRR の関係作りが重要になってくると考えられる。これまでは IP アドレスの割り振り構造であるインターネットレジストリとルーティング・オペレーターの信頼構造の根拠となる IRR は分離しており、またそれが望ましいと考えられてきた。インターネットレジストリが経路制御に関与しないという歴史的な状況が守られてきた反面、ルータの設定における簡単なアドレスの打ち間違いが他のネットワークの接続性を失わせてしまうことがあったり、本来割り振られていないアドレスが IRR に登録されてしまったりして、アドレスが不正利用されてしまう状況がある。

多くのルーティング・オペレーターに使われている RADB は、ARIN と運営組織が異なるだけでなく、インターネットレジストリと連動する仕組みを持っていない。

一方、RIPE NCC で運用されている RPSL ベースのレジストリシステムは IRR とインターネットレジストリが連携する仕組みを持っているようである。RIPE NCC のレジストリシステムは、IRR を兼ねているだけでなく、LIR が route オブジェクトを登録できるユーザを限定する機能を持っている。詳細については、今後調査を進めていく予定であるが、リソース証明書の管理にこの仕組みが使われると前述の課題は解決し、ルーティング・オペレーターにとって使いやすいリソース証明書ができることになる。RIPE NCC の 2007 年度の活動計画にある電子証明書がどのような形で実装されていくのか、RIR の中で注目されると思われる。

2.4. APNIC ミーティングでの ROA と IRR に関する発表

第 22 回 APNIC ミーティングでは、JPNIC から ROA とリソース証明書の取り扱いについて発表した。その発表の内容はリソース証明書の運用を現実的なものにするためのモデルであり、IP アドレス認証の展開には大きな意味を持つ。この発表の考え方について以下にまとめる。

図 2-1　２つのポイント（第 22 回 APNIC ミーティングにて）

この発表では 2 つのポイントに絞って発表を行った（図 2-1）。

一つ目の「Use of IIR for handy and legitimate information for certificates」は IRR をリソース証明書を発行するための、利便性が高くかつ正当性が確保されたデータベースとして利用する考え方である。

二つ目の「External RA for simple deployment」はリソース証明書をシンプルな構成で展開・利用促進するために、「外部 RA」（もしくはローカル RA）と呼ばれる手法を用いる考え方である。

これらについて以降のスライドで述べている。

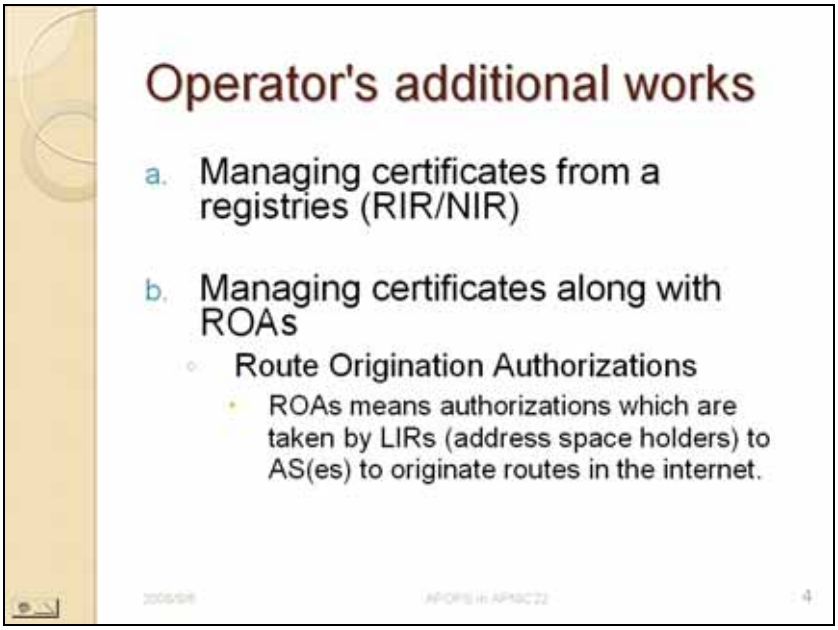

図 2-2　リソース証明書によってオペレータの付加される業務

図 2-2 では、背景としてネットワークオペレーターに付加される業務を挙げている。リソース証明書の導入により、リソース証明書自体を管理する必要が出てくるからである。

「a. Managing certificates from a registries (RIR/NIR)」は、RIR や NIR から発行された証明書を管理する必要がある点である。「b. Managing certificates along with ROAs」は、ROA（Route Origination Authorization）によって発行されるリソース証明書の管理する必要がある点である。

ROA は、アドレス資源が割り振られた LIR によって AS に対して行われるもので、対象の AS が LIR に割り振られている IP アドレスの origin（経路情報の発信源）になることの認可を意味する。ルーティングの安全性向上には、origin の他に AS パスの検証などの手法が考えられるが、リソース証明書は origination（発信源の正しさ）に着目しているためここでは ROA の証明書に注目している。

これらの業務負荷を下げることがリソース証明書を適切に deployment（展開）するための要件であると言える。

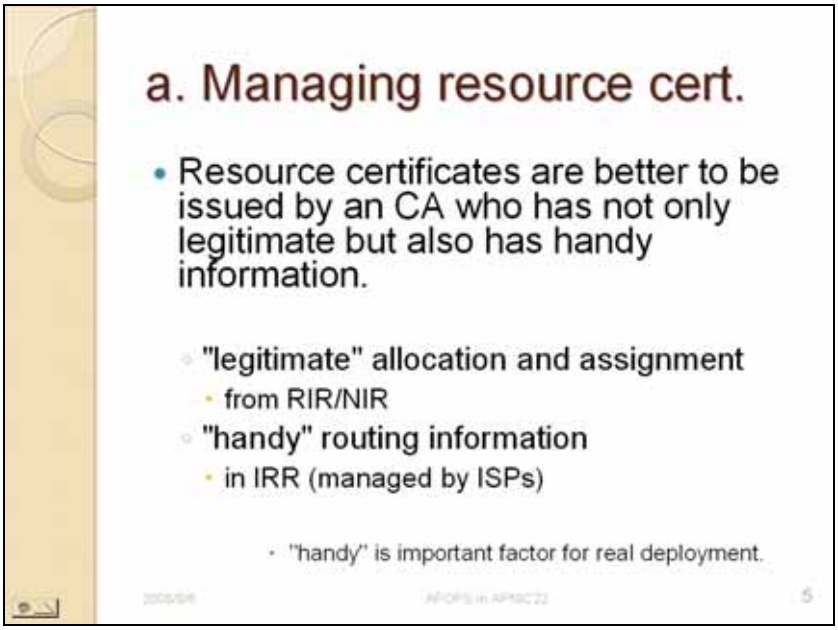

図 2-3　リソース証明書の管理

「Resource certificates are better to be issued by and CA who has not only legitimate but also has handy information」は、「リソース証明書は、正当性のある情報に基づいて発行されるべきであるだけでなく、利便性が高い情報に基づいて発行される必要がある」ということ意味している。

「legitimate allocation and assingment」とは RIR や NIR による割り振りや割り当てが行われているという意味である。

また「handy routing information」は、ISP 自身によって管理されている、IRR に登録された情報を意味している。IRR は ISP 自身が情報を登録するため、ISP のネットワーク事業に添った情報が登録されることになる。ISP が非公開とする情報があれば、それは IRR に登録されないため、公開されている情報は公開情報であることを前提にした解釈を行うことができる。

ここで課題になるのは、”handy”である IRR の情報が以下に正当な情報を担保するかという点である。

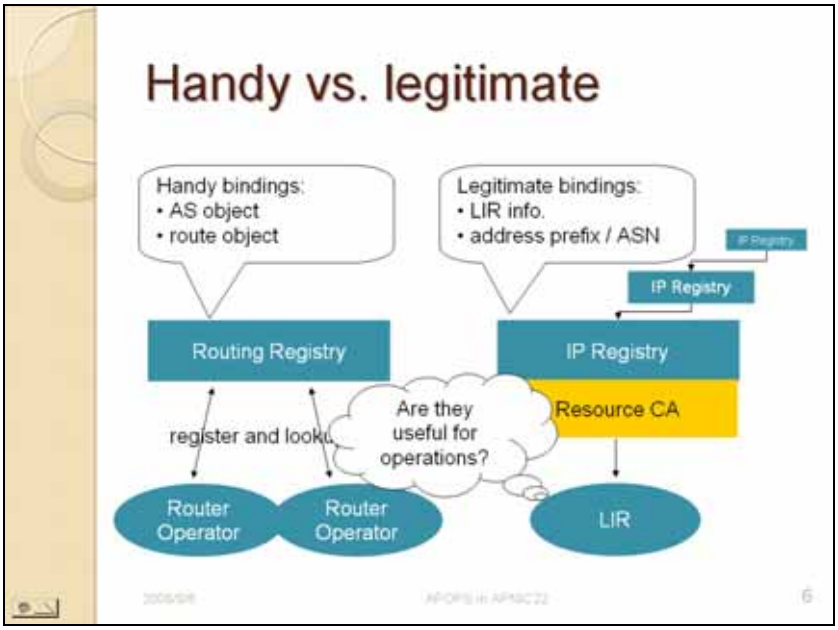

図 2-4　利便性と正当性の違い

「Handy vs. legitimate」は利便性を一義的に考えるか、正当性を一義的に考えるかという比較を提起している。「Routing Registry」に登録される情報は「Router Operator」すなわちルーティングのオペレーター自身が情報を登録する。ここでいう情報は「AS object」すなわち AS 情報や、「route object」すなわち経路情報である。ルーティングレジストリにおける AS 情報と経路情報の組み合わせが登録されることで、ある AS から間違った経路が広告されたときに、ルーティングレジストリの参照を行っているものは、それを検出できるようになる。ルーティングレジストリではオペレーター自身が登録するため、運用のための情報交換のために必要最低限のものが登録／公開され、また prefix のサイズも運用の事由に一致した「handy」なものとなる。

一方「IP Registry」すなわちインターネットレジストリも、LIR（日本国内の IP 指定事業者など IP アドレスの割り振りを受けている組織）と「address prefix」すなわち IP アドレスブロック、そして「ASN」すなわち AS 番号の情報を持っている。これら情報はインターネットレジストリが、自ら割り振り／割り当てを行った結果であるため正当「legitimate」な情報であると言える。しかしネットワークの運用上の都合で分割された IP アドレスの情報や、その一部が非公開である場合であってもそれが逐次反映されているわけではない。ルーティングレジストリは常にルーティングのオペレーターに参照されていると考えられるが、インターネットレジストリの割り振り／割り当て情報は、LIR に対する割り振り／割り当ての情報でしかないため、ネットワークの状況を反映しなくてもルーティングには影響が少ないためである。

インターネットレジストリに登録されている情報は正当「letigimate」であるが、ネットワークオペレーターにとって利便性が低い意味で、「Resource CA」リソース証明書

の発行の為にどの情報を利用すべきかについて、検討する必要がある。

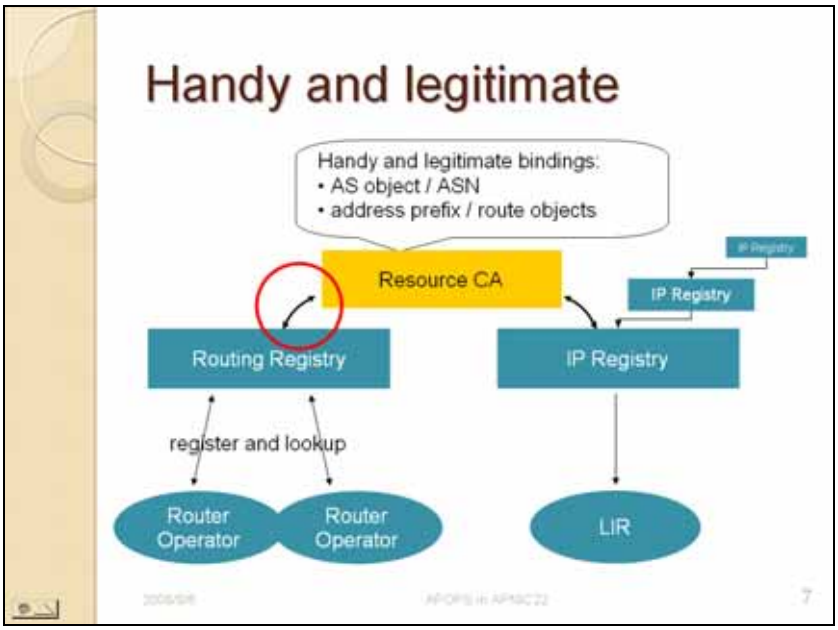

図 2-5　リソース証明書の為の利便性が高くかつ正当な情報源

「Handy and legitimate」すなわち利便性が高くかつ正当な情報源を確保するには、「Routing Registry」（ルーティングレジストリ）と「IP Registry」（インターネットレジストリ）の情報の両方の参照が必要であると考えられる。図 2-5 はリソース証明書の発行を行う「Resource CA」がルーティングレジストリとインターネットレジストリの両方の情報を参照し、「AS object / ASN」（AS 情報）と「address prefix / route objects」（アドレスブロックと経路情報）の両面から「bindings」（組み合わせ）を抽出することを示している。

APNIC で進められているリソース証明書プロジェクトでは、インターネットレジストリの割り振り情報／割り当て情報を一元的な情報源とするため、図 2-5 のマルで示された連携を行うことができない。

なお後に判明したことであるが、2006 年 11 月に ARIN のミーティングや IETF で行われた、APNIC Geoff 氏のプレゼンテーションによると、IRR に登録される情報である as-set オブジェクトが使用されており、上記の考え方に沿っていることがわかる。

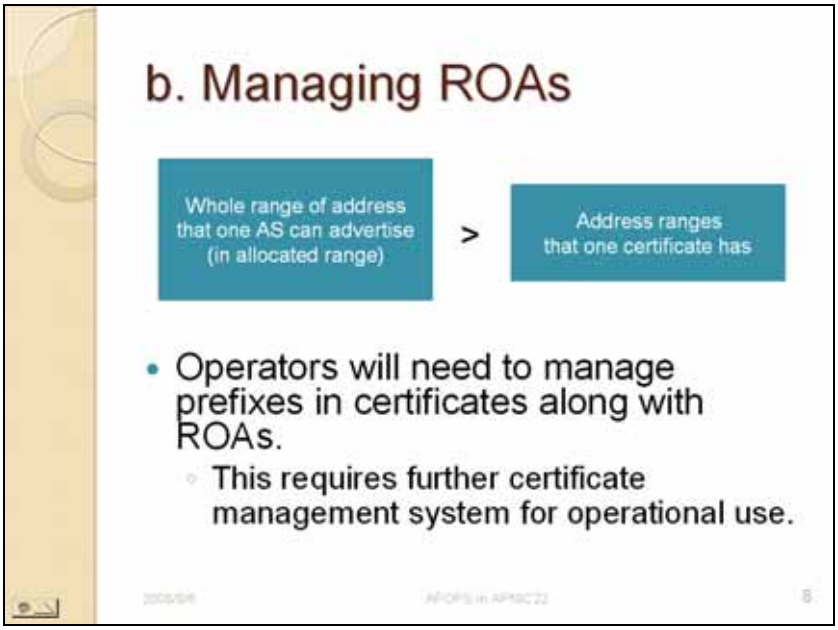

図 2-6　ROA の管理

「b. Managing ROAs」すなわち ROA（Route Origination Authorization）の管理は、ネットワークの prefix の管理と平行して行われる業務になると考えられる。そのためリソース証明書の管理は、アドレス prefix の分割などが業務上簡単に行えるような状況でなければ実現が難しい。

まず、ある LIR が割り振られた IP アドレスをそのままある AS が経路広告に使用することは少なく、分割された IP アドレスのブロックがネットワークのトポロジー（接続状況）に応じて配置されることが一般的である。

そして「Whole range of address that one AS can advertise (in allocated range)」すなわち、割り振り済みの IP アドレスの中である AS が広告できるアドレスの範囲は、「Address ranges that one certificate has」すなわち一つのリソース証明書が持つアドレスの範囲よりも大きいことが容易に考えられる。

この 2 点から、ある AS は経路広告の認可を示す ROA のリソース証明書を受け取った後、ネットワークのトポロジーに応じて prefix を分割し、その分割状況に合わせてリソース証明書を発行しなおす必要があることが考えられる。これが「Operators will need to manage prefixes in certificates along with ROAs」の意味である。これにより「This requires further certificate management system for operational use.」すなわち既存のリソース証明書発行システムよりも高度な、オペレーションに合った証明書管理システムが必要になることがわかる。

この問題が如実に表れるのは末端の LIR である。

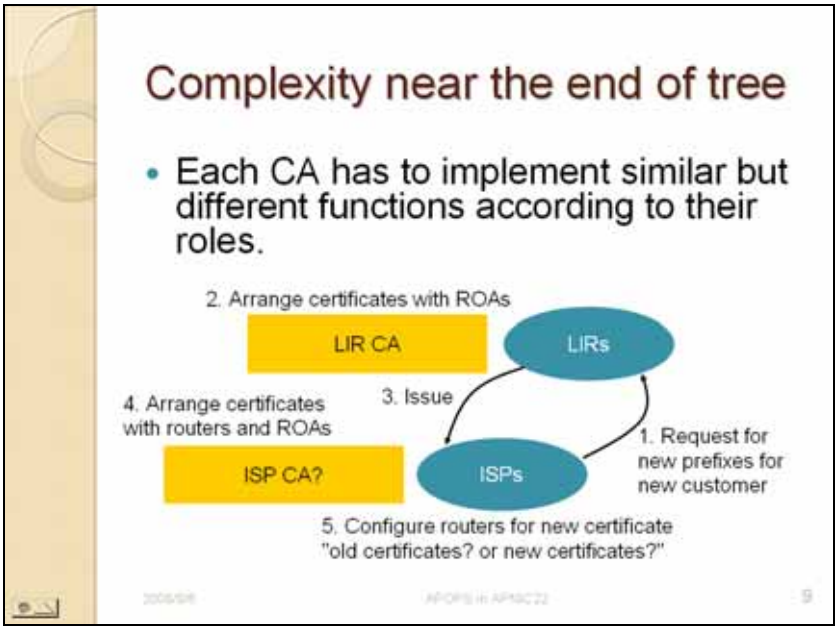

図 2-7　末端部分でのリソース証明書の複雑さ

「Complexity near the end of tree」広義のインターネットレジストリのツリー構造に則って考えた LIR では、AS のオペレーションを行っている ISP に対する IP アドレスの割り当て業務が行われている。この割り当ては JPNIC のようなインターネットレジストリに「割り当て報告」されていないケースもある。

リソース証明書は広義のインターネットレジストリのツリー構造に沿って発行されるものであるが、そのためには「Each CA has to implement similar but different functions according to their roles.」各々の CA が似て非なる機能を役割（NIR や LIR など）に応じて持っている必要がある。

「1. Request for new prefixes for new customer」は新規の顧客に対する新たな prefix の要求を ISP から LIR に対して出すことを示している。「2. Arrange certificates with ROAs」は LIR がその必要な prefix に応じた ROA を設定し「3. Issue」で LIR の CA がリソース証明書として発行する。「4. Arrange certificates with routers and ROAs」は ISP でリソース証明書の管理のために運用されている CA が存在する場合にはそこで証明書の組み込みが行われること示している。「5. Configure routers for new certificate “old certificates? or new certificates?”」はルータを新たなリソース証明書の為に設定することを示しているが、経路制御への影響を考慮して、古い証明書を使うべきなのか新しい証明書を使うべきなのかの判断は、この段階で必要になる。

これらの複雑さを解決するための提案が次のスライドである。

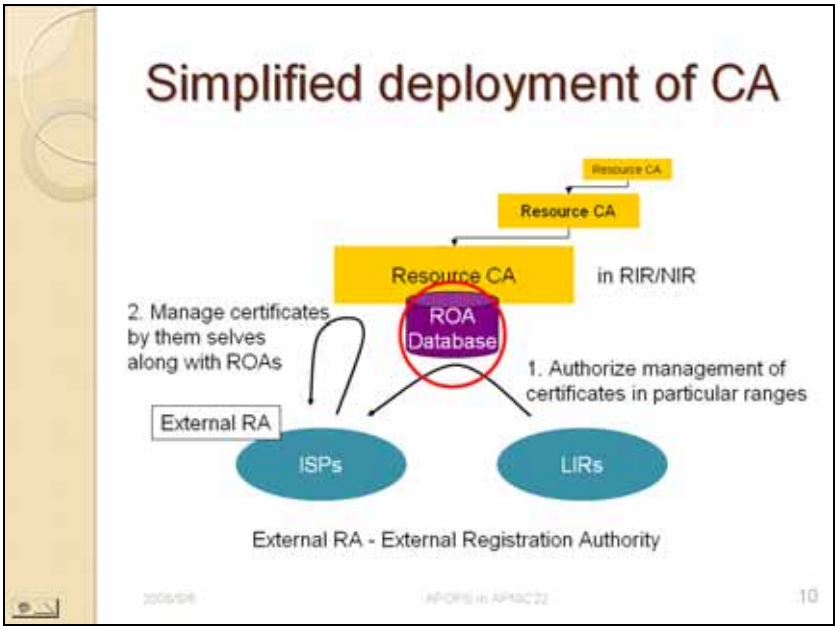

図 2-8　シンプルなリソース証明書用 CA の展開

リソース証明書の為の CA のシンプルな展開「Simplified deployment of CA」の為に、図 2-8 に示すようなモデルが考えられる。

RIR や NIR における「Resource CA」リソース証明書は従来通りであるが、新たに「ROA Database」を設置している。ROA Database は LIR における ISP への ROA を集めたもので、これらの ROA を LIR 自身が CA を構築して管理するのではなく、そのオリジナルデータを RIR や NIR が持つという考え方である。

元来 IRR は ISP 自身が持つべき情報のうち、共有すべき情報を集約したものである。IRR と同様にインターネットレジストリに自由に登録／参照なデータベースを設ければ、LIR や ISP 同士の登録／参照の為には自組織で認証局を構築管理するよりも利便性が高い。また登録される情報を RIR/NIR における割り振り情報／割り当て情報と比較すれば、登録情報の内容の正当性を維持することもできる。利用手順は以下のようになる。

「1. Authorize management of certificates in particular ranges」は、初めに特定のアドレスブロックに対する証明書の管理を ISP に対して「認可する」。このことで ISP はそのブロックに含まれるアドレスが入ったリソース証明書を管理できることになる。「2. Manage certificates by them selves along with ROAs」は ISP 自身が ROA に則って証明書の管理を行うことを示す。このとき ISP は「External Registration Authority」というモデルに則って証明書の管理を行う。

External Registration Authority は「外部登録局」と呼ばれ、証明書発行業務を行う役割を CA に対して外部（すなわち ISP 自身）に持たせたモデルである。このモデルにすることで、ISP 自身では認証局ソフトウェアを管理運用する必要はなく、RIR/NIR に

ある証明書管理システムに Web ブラウザ等でアクセスして、証明書の発行業務を行えばよいことになる。

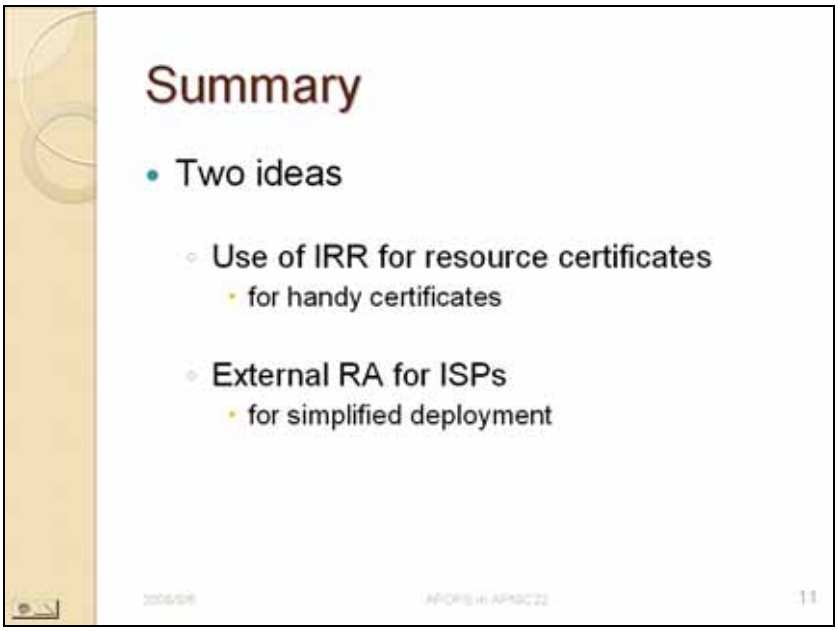

図 2-9　発表のまとめ

この提案では二つのアイディアを提示した。

「Use of IRR for resource certificates」はリソース証明書の管理の為に IRR を利用するという意味である。これによって ISP 自身の運用状況にあった「handy」便利なリソース証明書の発行を行うことができる。

「External RA for ISPs」はリソース証明書の管理の為に、外部登録局のモデルを利用し、ISP 自身が証明書の管理を行うことができるようにするということを意味する。ISP 自身が認証局ソフトウェアを運用する必要がないため、「simplified deployment」簡単化された利用・展開を目指すことが可能になる。

なお、発表の最後には RIR と IRR の運用ケースの違いについて補足した（図 2-10）。

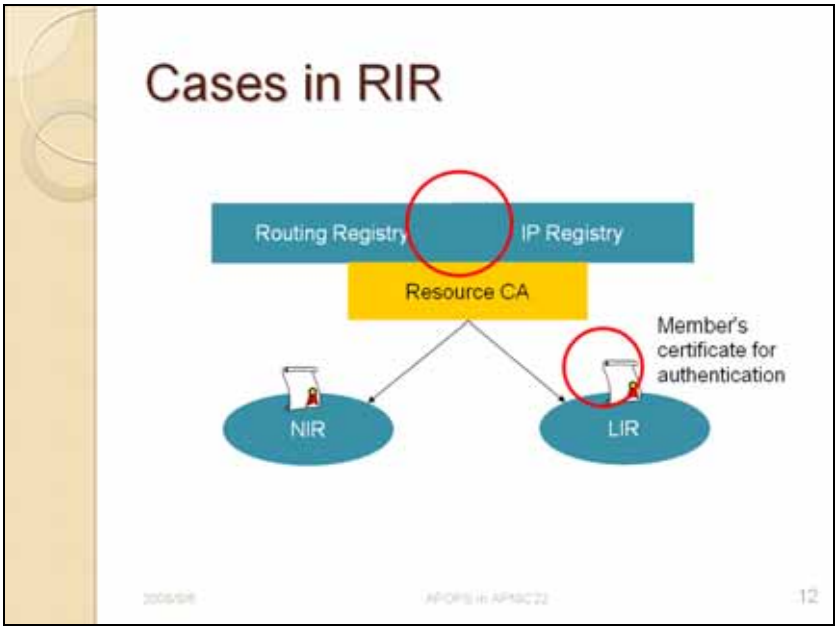

図 2-10　RIR における運用ケースの違い

RIR では、IRR を運用していないケースがあり、場合によってリソース証明書管理システムとの連携の仕方が異なってくる。

APNIC の場合には、IP アドレスの管理を行う IP レジストリシステムと IRR のシステムが同一であり、図 2-10 のようにリソース証明書のための認証局が直接連携して証明書の管理を行うことが可能である。また APNIC から IP アドレスの割り振りを受けている「メンバー」の認証用の証明書（図中では Member's certificate for authentication）が存在するため、ISP に対する authorization（認可）を業務上実現するためにこれを利用することができる。

このモデルは RIPE NCC の場合でも同様であるが、RIPE NCC の場合には IP レジストリシステム及び IRR の中に既に認可機構が組み込まれている。そのためリソース証明書の発行を行う認証局はこの認可情報を利用することが可能である。この意味で、RIPE NCC におけるリソース証明書の実現性は高いと考えられる。

ARIN の場合には、ARIN において IRR が本格運用されておらず、北アメリカ地域における大手の IRR の RADB を利用することが考えられる。（2007 年初めに IRR の運用開始のアナウンスがあった。しかしそのオリジナルデータはまだ少ない。）IP レジストリシステムと IRR が別である場合、JPNIC のモデルと似たシステム構成となる。

従って本調査研究の一環で設計／開発されている「経路情報の登録機構」は ARIN においても適用可能な仕組みであるといえる。

2.5. まとめ

本章では主に RIR における IP アドレスの認可機構の調査について述べた。IP アドレスの認可機構は IP アドレス認証の展開の最も肝要な機構であると共に、RIR でもその機構が見直され、リソース証明書管理システムの一部として検討が開始されている。

RIR の動向調査では、RIPE NCC、ARIN、APNIC のミーティングに参加し、また現地のスタッフにヒアリングを行った。調査の結果 RIPE NCC における認可機構を除いて未だ IP アドレスと AS 番号の組み合わせを確認する機構の開発は行われていないものの、リソース証明書の技術開発が進められていることがわかった。

一方、RIPE NCC のデータベースにおいて課題になっているように、時間が経って正当性がなくなったデータを消去する仕組みや、新たに LIR から ISP に認可する仕組みの構築はすべての RIR においてあまり取り組まれていないことがわかった。この結果を受け、JPNIC で IP アドレス認証の展開として取り組んでいる「経路情報の登録機構」では正当性がなくなったデータの整理の機能などが盛り込まれることになった。

第 22 回 APNIC ミーティングでは、JPNIC から、リソース証明書のより現実的な deployment（利用と展開）のために必要になるいくつかのポイントについて発表した。これらのポイントは「経路情報の登録機構」の設計に基づくものであり、今後本機構がリソース証明書の管理機能を持つことで、機能性・利便性の高いリソース証明書システムができると考えられる。