第 5 章　経路制御のための電子認証技術に関する国際動向

内容

- IETF SIDR WG の動向
- リソース証明書の動向
- RIR の認証技術に関する動向

5. 経路制御のための電子認証技術に関する国際動向

本調査研究では、経路制御のための電子認証技術の国際動向を調査するため、国際会議に参加して情報共有を行った。参加した会議は、IETF ミーティング、RIPE ミーティング、ARIN ミーティング、APNIC ミーティングである。

本節では経路制御に関連する電子認証技術の国際動向について述べる。国際動向は、わかりやすさのため、一旦スライドにまとめ、それを解説する形で述べる。

5.1. 概要

インターネットにおける経路制御は、国際的なネットワークを通じて行われている。インターネットにおける代表的な経路制御プロトコルは、BGP4（Border Gateway Protocol）である。インターネットのようなインタードメインの経路制御では、BGP4 のような経路制御プロトコルを使って相互に経路情報を交換している。

インターネットにおける経路制御の安全性を考える場合、国際的に普及されている安全性向上の考え方を取り入れることは肝要である。インターネットは国際的なネットワークであるため、例えば日本だけがセキュアの高い経路制御の仕組みを取り入れることは、相互運用性の観点で難しい。

本調査研究では、国際的な経路制御の電子認証技術について調査を行うため、IETF と RIR のミーティングに参加した。IETF では、2003 年頃より新しいセキュアな経路制御プロトコルの策定が始まっているためである。また RIR では、各 RIR の取り組みに違いはあるものの、各々がセキュアな経路制御に資する仕組みを検討し実装しつつある。

本節では、本調査研究のメインテーマである IRR と電子認証技術に関連する、IETF および RIR（RIPE NCC、ARIN、APNIC）における動向について述べる。

今年度の調査の結果、RIPE NCC は ARIN や APNIC のリソース証明書の開発に参加しつつも、Certification Task Force や CertProto といった委員会活動を通じて、業務面の検討を進めていることがわかった。また ARIN と APNIC は XML ベースのプロトコルを用いた、リソース証明書のプロトタイプシステムの開発を行った。APNIC では 2008 年 3 月に LIR 向けのポータルサイトである MyAPNIC にリソース証明書の機能を実装した。APNIC におけるリソース証明書は、経路制御の安全性向上よりも先に、IP アドレスの使用権を示す署名付データとして捉えられている。

IETF SIDR WG では、APNIC と ARIN のプロトタイプで採用されているような XML ベースのプロトコルの策定とは方向性が異なり、ルータにおけるリソース証明書の検証に話題が絞られてきた。

RIPE NCC とは、大手 ISP のメンバーとオフィスを訪問し、IRR の技術的な信頼性向上策について情報交換を行った。RIPE NCC でも IRR の運用上の信頼性向上は取り組み課題となっており、相互の技術交流が可能であることを確認した。

このように、IP アドレスの管理の信頼性向上と IRR の運用上の信頼性向上を図る活動は、IETF および RIR において進みつつあると言える。本調査研究の一環として開発を行った経路情報の登録機構は、IRR とリソース証明書への発展を考慮したシステムである。国際的な動向に合わせて、JPIRR のユーザに経路制御の安全性向上策に必要な仕組みを提供できるようにして行きたい。

5.2. IETF SIDR WG の動向

IETF SIDR（Secure Inter-Domain Routing）WG は、新しいセキュアなインタードメインの経路制御アーキテクチャを策定することを目的とした WG[1]である。

2007 年度は、リソース証明書を用いたセキュアな経路制御の方式の検討が行われた。リソース証明書がルータにおいて機能する全体像としたときの、2007 年度の SIDR WG の状況を以下に示す。

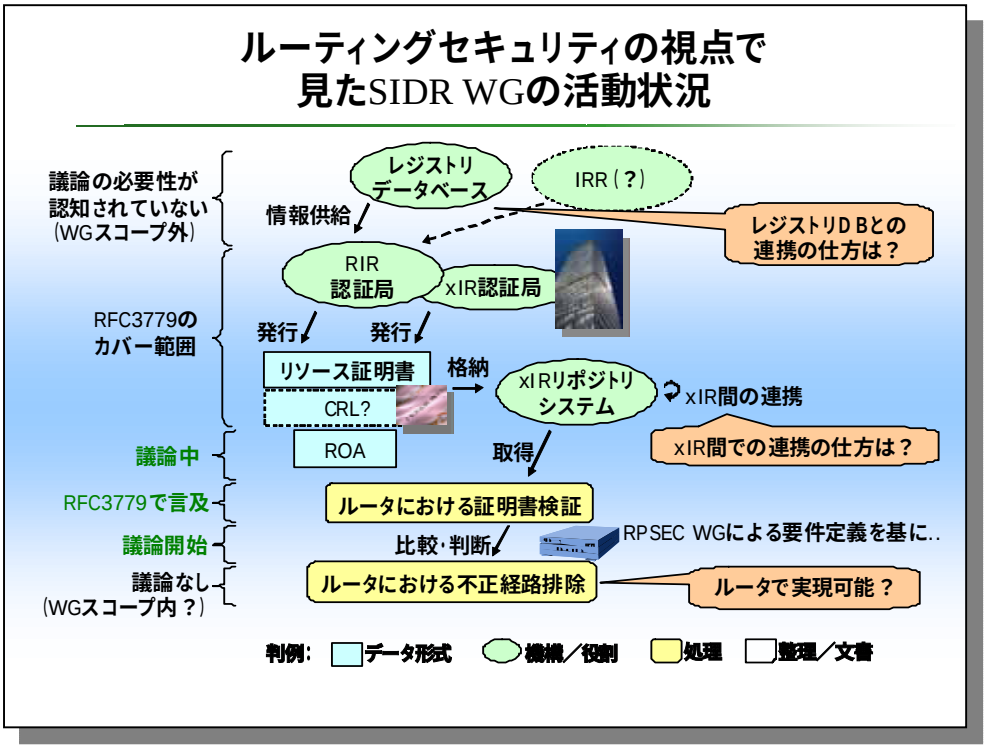

図 5-1　ルーティングセキュリティの視点で見た SIDR WG の活動状況

図 5-1 は、レジストリデータベースに基づいて発行されたリソース証明書が、ルータに取り込まれて検証され、インターネットにおける経路制御がセキュアに行われるまでの情報と処理の流れを示したものである。SIDR WG では、RFC3779[2]という書式に則った議論が行われているが、2007 年度は、主に ROA（Route Origination Authorization）のデータオブジェクトの要件に関する議論や、リソース証明書の検証方式に関する議論が行われた。

---

[1] Secure Inter-Domain Routing (sidr)
http://www.ietf.org./html.charters/sidr-charter.html

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

しかし、今の段階では大きな三つの課題があると考えられる。これまでの進捗状況から、これらがすぐに解決されるとは考えにくいが、ここでは今後の方向性として各々について述べる。

一つ目は、レジストリデータベースとの連携方法である。リソース証明書はレジストリの割り振りや割り当てと同じ内容を持つ電子証明書である。従って、証明書発行システムは IP レジストリシステムと連携している必要がある。ARIN や APNIC では、一部の連携の為の検討が始まっているが、それは技術的な連携方法に留まっている。例えば返却時の処理や、発行の時間的な粒度については、今後議論し、決定していく必要がある。

二つ目は、インターネットレジストリ間の連携方法である。IP アドレスの割り振り先で証明書発行が起こると、その証明書データを提供するリポジトリに発行された証明書が格納される必要がある。そのためインターネットレジストリ間、例えば APNIC と JPNIC の間で発行された電子証明書を交換する仕組みが必要になる。APNIC と ARIN で開発されているプロトタイプシステムでは XML ベースのプロトコルが使われることになっている。(実装状況は明らかになっていないが、相互運用が実験できる状態にはまだなっていない)

三つ目はルータにおけるリソース証明書の検証である。ルータにおけるリソース証明書の検証については議論が行われているが、有効性が確認された証明書を使って実際の経路制御のどのようなコントロールを行うかは定かになっていない。証明書の有効性が確認できなくなったときに、急にルータがその prefix を経路表から削除してしまうと、電子証明書に依存しすぎ、管理業務が高くなりすぎてしまう恐れがある。

次に、2007 年度に行われた各回の IETF SIDR WG の状況について述べる。

5.3. 第 69 回 IETF SIDR (Secure Inter-Domain Routing) WG

SIDR WG は 5 日目の朝、9 時から 10 時 45 分まで行われた。SIDR WG は、インターネットにおけるドメイン間(AS 間)の経路制御をセキュアに行う仕組みを検討している WG である。今回の WG では、主にドキュメントの更新に関する議論が行われた。

図 5-2　第 69 回 IETF における SIDR WG の概要

現在、SIDR WG で行われている議論は大きく分けて三つある。一つ目は RFC3779 を使ってセキュアなルーティングを実現するアーキテクチャをドキュメント化するための議論である。二つ目はリソース証明書を発行する認証局の CP(Certificate Policies)と CPS に関する議論で、Stephen Kent 氏を中心に議論が進められている。三つ目は ROA(Route Origination Authorization)の書式と取り扱いに関する議論である。

SIDR のアーキテクチャについては、継続して行われている議論がいくつもある。

図 5-3　SIDR WG における Action Item と議論
～アーキテクチャドキュメント～

まず、経路集約が可能な隣接する IP アドレスのリソース証明書をどのように扱うかという議論がある。単一の ISP に対してレジストリが複数の IP アドレスブロックを割り当てている場合、ISP は集約(route aggregation)された経路を広告することが考えられます。しかしリソース証明書は割り振りブロックを含んだ形で発行されるので、広告される経路情報とリソース証明書が一対一で対応しない。すると集約されたプリフィックスの正しさを検証できないことになってしまう。この件については会場ではあまり議論されず、ML で継続して議論が行われることになった。

他に、リソース証明書と CRL を示す URL で rsync をプロトコルとして使うことが提案されているが、書式上認められるか、という議論も進行中で、今は作業を担当する人を探している段階である。WG のマイルストーンによるとアーキテクチャは 2007 年 3 月には RFC 化が目指される予定であるが、大幅に遅れてしまっているようである。なお 4 バイト AS 番号については既に対応済みである。

□ An Infrastructure to Support Secure Internet Routing

draft-ietf-sidr-arch-01.txt

この他に、リソース PKI のための CPS と ROA に含まれる prefix の比較ルールなどについて議論が行われた。

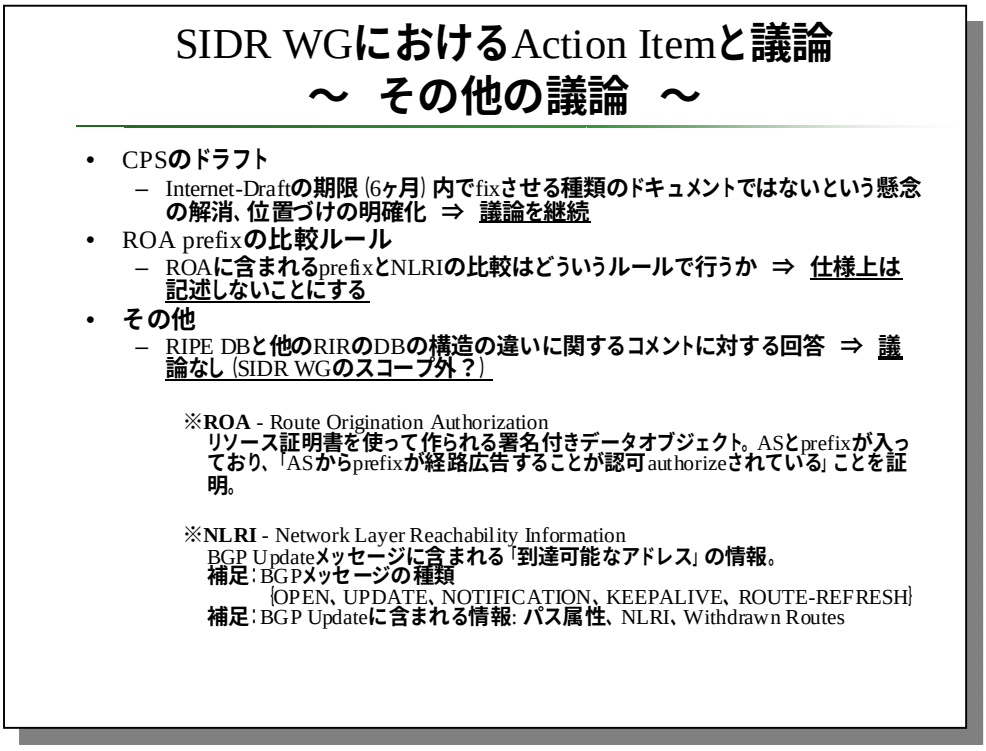

図 5-4　SIDR WG における Action Item と議論
～　その他の議論　～

CPS については、本ドキュメントの策定の時間的な制約に関する議論が行われた。提案者である Stephen Kent 氏によると、本ドキュメントは、リソース証明書を発行する認証局が構築され始める頃には必ず必要になるが、Internet-Draft の有効期限は 6 ヶ月であり、この期限内で有意義な議論が進めることができるか、という疑問が Stephen Kent 氏自身にもあるそうである。議論の結果、今後、ドキュメントの位置づけを明確化することが課題になった。

ROA については、ROA に含まれる prefix と検証の対象である BGP Update に含まれる NLRI との比較ルールについて議論が行われた。前回の SIDR WG では、ROA に内包される prefix が NLRI に含まれるのであればよい、という方向になっていたが、前述の経路集約の問題があり、ROA として比較ルールを定めることは難しいことがわかってきた。ひとまず ROA のドキュメントでは比較ルールを記述しないことになった。

□ A Profile for Route Origin Authorizations (ROAs)

draft-ietf-sidr-res-certs-08.txt

最後に、"Private AS space"というタイトルでチェアの Sandra Murphy 氏よりプレゼンテーションがあった。これは AS 内のプライベートな経路制御のためにユニークローカルアドレス(RFC4193)を使う場合、リソース証明書をどこが発行すればよいのか、という疑問の投げかけである。これはリソース証明書のトラストアンカー(trust anchor - 信頼点)の議論に密接に関係するため、トラストアンカーとして何を想定すべきか、という議論に発展した。IANA をトラストアンカーとして想定すると、RIR への追加割り振りがあった場合にユーザ環境のトラストアンカー証明書を入れ替える必要がなく、手続きは簡単である。また、本来、トラストアンカーは RP(Relying Party - 証明書検証者)によって選ばれることが望ましくもある。しかし現在の IANA にはトラストアンカー認証局を提供する役割がなく、RIR の認証局で対応せざるを得ないのが現状である。

5.4. 第 70 回 IETF SIDR WG

SIDR WG は第一日目の 2007 年 12 月 3 日(月)15 時 25 分から行われた。

図 5-5　第 70 回 IETF における SIDR WG の概要

SIDR WG では既存のドラフトドキュメントの更新に関する議論が三つ、新しいトピックに関する議論が二つあった。既存のドラフトドキュメントの更新に関する議論があった。

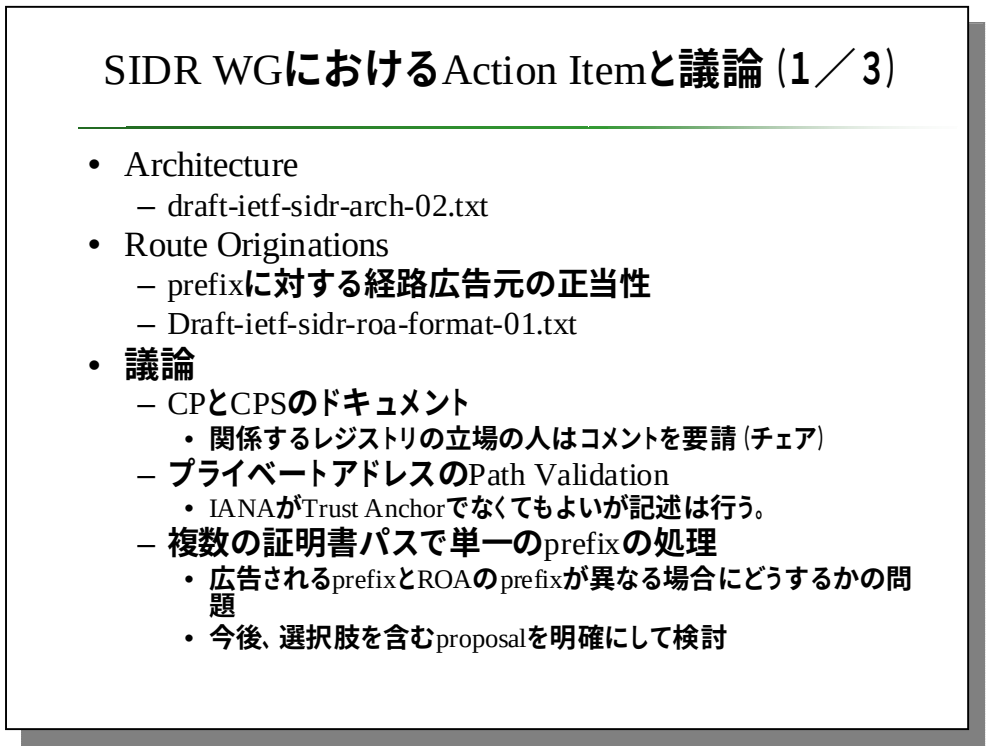

図 5-6　SIDR WG における Action Item と議論（1／3）

□CP/CPS update

特に内容が update されたわけではないが、インターネットレジストリなどの関係する組織の人はコメントをするように要請があった。

□Architecture と Route Originations

リソース証明書のツリーの末端に位置づけられる、ROA(Route Origination Authorizations)に関する議論である。

今回はプライベートアドレスを含む ROA の扱いについて議論された。プライベートアドレスについて、IANA をトラストアンカーとするリソース証明書を発行する必要がないのではないか、各機器がトラストアンカーを定められるような証明書ツリーを構築できるようにすべきでは、という議論である。結局、IANA をトラストアンカーにしなくてもよいが、ドキュメントでは IANA について言及することになった。

□複数の証明書パスで単一の prefix の処理

経路広告される prefix と ROA に含まれる prefix が異なる場合に、ルータはどのように処理すべきか、という議論である。例えば、複数の prefix について経路集約を行う場

合、インターネットレジストリの構造に合わせて発行されたリソース証明書と prefix が一致しないことが考えられる。正しく発行されたリソース証明書が実際の正しい経路広告をうまく扱えなければならない。

会場では更に、更に複数のインターネットレジストリ、例えば歴史的 PI の経路集約をどう扱うかといった議論になった。今後、方式の選択肢の提示を含め、提案内容を固めてから議論が進められることになった。

□リソース証明書に含まれる prefix の処理

現行のリソース証明書の仕様では、上位 CA が階層ごとに IP アドレスと AS 番号を内包していく構造になっている必要がある。従って、リソース証明書を検証する段階で、両方の包含関係が必ず両立する必要がある。

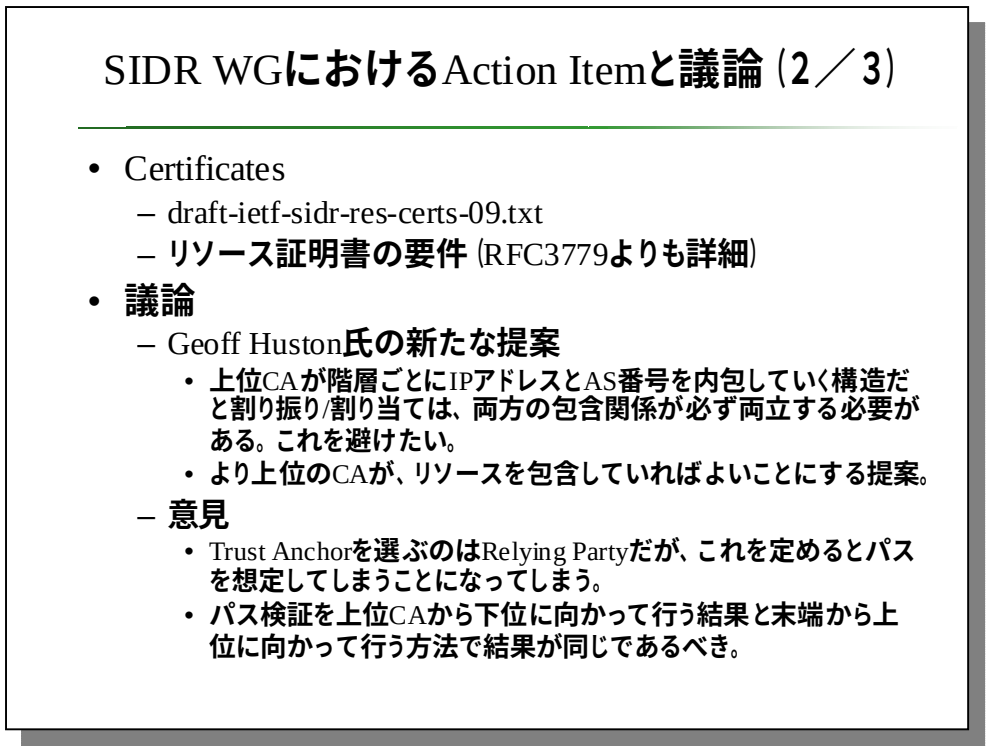

図 5-7　SIDR WG における Action Item と議論（2／3）

この仕様を緩め、より上位(すなわち上位の上位など)の CA のリソース証明書が、リソースを包含していればよいことにする提案が、APNIC の Geoff Huston 氏によって行われた。会場ではパス検証の結果が、ツリーの上から行う場合と下から行う場合とで変わってしまうのは良くない、などの議論が行われたが、ML で継続議論される模様である。

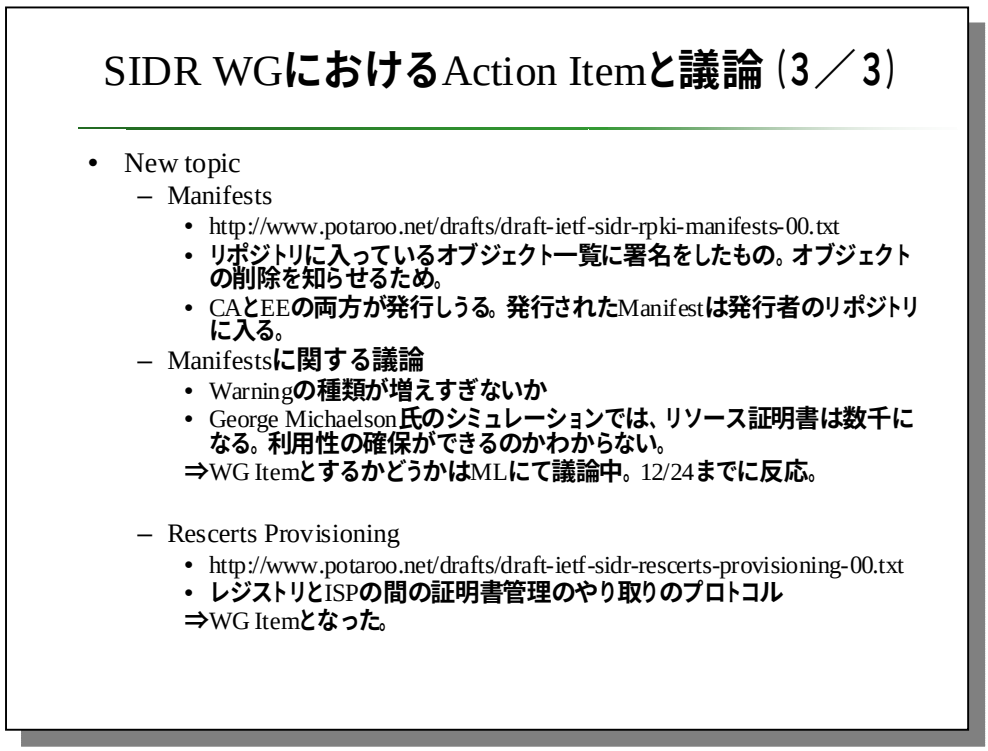

図 5-8　SIDR WG における Action Item と議論（3／3）

新しいトピックとしては、以下の二つがあった。各々について、WG の working item として採用するかどうかの問いかけ、WG チェアから行われたが、いずれも ML で意見収集を行うことになった。

Manifest とはリポジトリに入っているオブジェクト一覧に署名をしたもので、CRL より早く、証明書検証者に対してオブジェクトの削除を知らせることを目的としたデータである。

会場では、証明書検証に関わる Warning(警告)すべき状態が増えすぎないか、リソース証明書の数は多いために CRL を含めて、利用可能性について検証する必要がある、といった意見が出された。WG の working item とするかどうかについては、12 月 24 日までに ML で意見収集を行い決定していくことになった。

リソース証明書を発行するインターネットレジストリと証明書申請者の間で、証明書管理(発行や失効など)のために使われるプロトコルの提案である。これについては会場では議論は多くなく、WG の working item となった。

SIDR WG は、リソース証明書のルータにおける仕様に関して、これまでにあまり多くの議論がされてきていなかった。今回は、経路集約を踏まえたルータの挙動について議論されており、徐々にではあるが、実用化に向けた動きが見えてきた。しかし Manifest

などの、新しい処理を要するプロトコルが追加され、リソース証明書を扱うプログラムの全体像にたどり着くには、まだ時間がかかりそうである。

5.5. リソース証明書に関する RIR の相互運用実験

第 70 回 IETF では、APNIC、RIPE NCC、ARIN で、リソース証明書の相互運用実験が行われた。結果的に、APNIC と ARIN が開発を行っているプロトタイプシステムの動作検証が行われるに留まった。

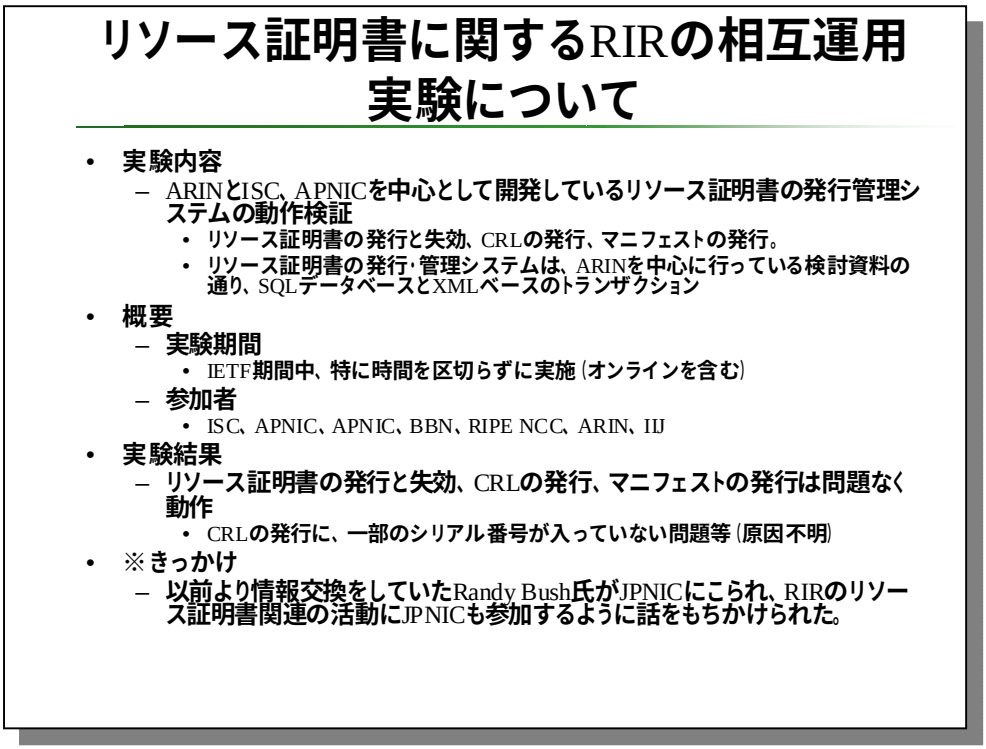

図 5-9　リソース証明書に関する RIR の相互運用実験について

CRL の発行に、一部問題があったものの、リソース証明書の発行および失効の操作については問題なく行うことができたという報告があった。

5.6. 国際会議 IEPG での発表

第 70 回 IETF の前日に行われた IEPG ミーティングで、経路情報の登録機構に関するプレゼンテーションを行った。

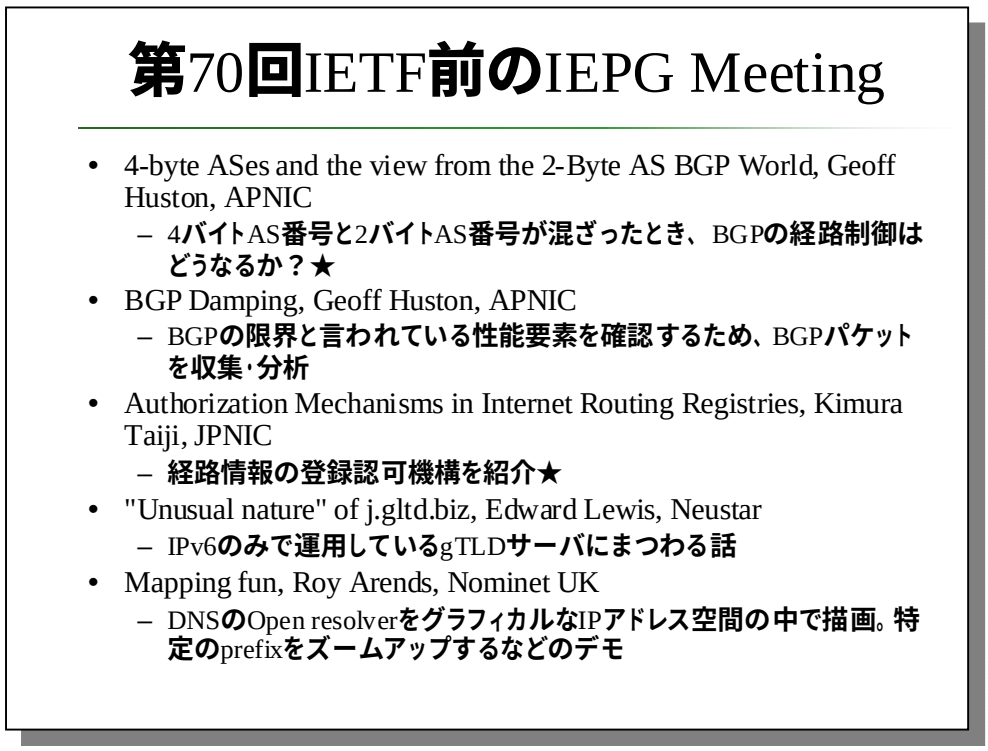

図 5-10　第 70 回 IETF 前の IEPG Meeting

今回の IEPG ミーティングでは、4 バイト AS や BGP の経路情報の解析など、インタードメインルーティングに関する発表が APNIC の Geoff Huston 氏によって行われた。経路情報の登録機構に関する発表は、その話題に引き続いて行われた。

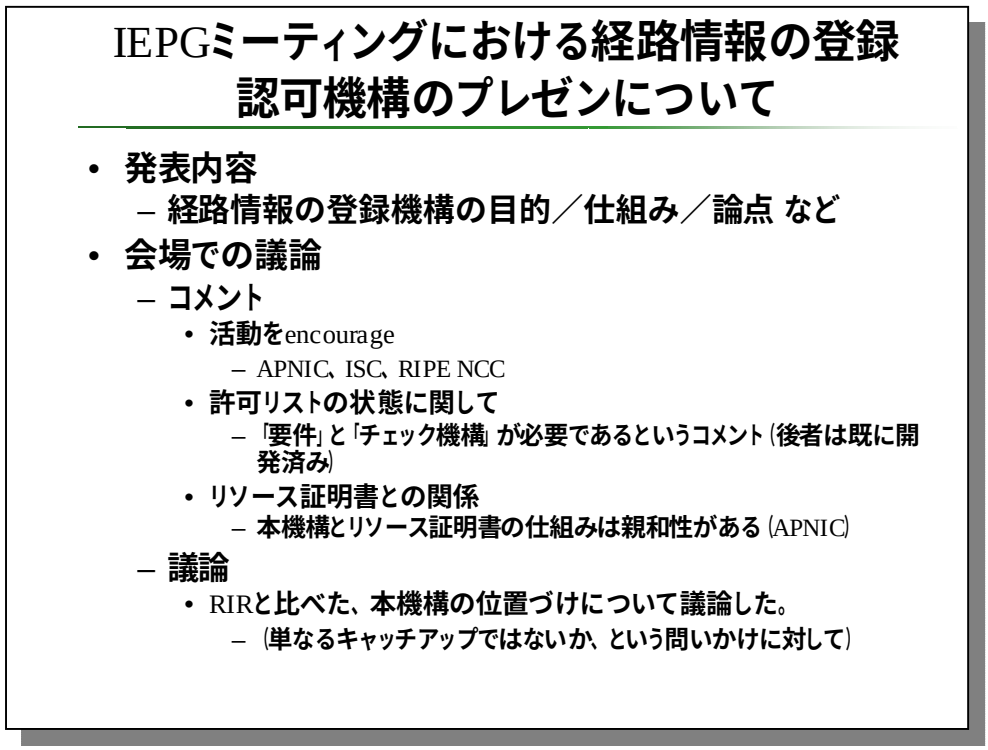

図 5-11　IEPG ミーティングにおける経路情報の登録
認可機構のプレゼンについて

IEPG ミーティングにおけるプレゼンテーションの結果、まず複数の参加者より本機構を使った実験に関する encourage するという意見を頂いた。この意見は、ISC（Internet Systems Consortium）、APNIC、RIPE NCC からの参加者から頂いた。プレゼンテーションについては、特に許可リストの正当性についてディスカッションが行われた。

5.7. RIPE NCC における動向

RIPE NCC における経路制御のセキュリティに関する動向調査のため、第 54 回 RIPE ミーティング及び第 55 回 RIPE ミーティングに参加した。

RIPE NCC では、mnt-route、mnt-lower といった IP アドレスの利用認可の機構が既に運用されており、IP アドレスの利用認可という意味では先進的な IP レジストリシステムを有している。またリソース証明書の開発プロジェクトにも参画しており、LIR を交えた検討を行っている。2007 年度は、特にリソース証明書の業務面での影響に着目し、二つのチームを作成して調査を行った。

一つは Certification Task Force（CA-TF）である。CA-TF は、RIPE 地域の LIR からリソース証明書に興味のある参加者を募り、RIPE 地域におけるリソース証明書の影

響や意義について検討を行うチームである。CA-TF は、2008 年 1 月にホワイトペーパーを作成した。ホワイトペーパーでは、リソース証明書の提供方法と、リソース証明書を使ったルーティング、IP アドレスの再割り振りの方法などについて、基本的な情報がまとめられている。

もう一つは CertProto である。CertProto は CA-TF をサポートし、RIPE NCC 内でリソース証明書を扱う業務の実現性を検討する目的で作られた。実際にリソース証明書を発行するプロトタイプの業務システムが作られ、RIPE NCC の各セクションのスタッフによって既存の業務との変更点や課題点が RIPE NCC 内部でまとめられた。今後、CertDeploy というチームが作られ、RIPE NCC 内でリソース証明書を扱うためのポリシー調整、料金などに関する検討が進められる。

次節以降では、各 RIPE ミーティングでの議論の詳細について述べる。

5.8. 第 54 回 RIPE ミーティング

第 54 回 RIPE ミーティングは、2007 年 5 月 7 日～5 月 11 日、エストニアのタリンで開催された。

図 5-12　第 54 回 RIPE ミーティング

今回の RIPE ミーティングは、規模は 300 名ほどと大きくないものの、参加国数は 40 カ国と多かった。RIPE 地域には多くの国が含まれていることからから、毎回参加国数は多いようである。

リソース証明書に関しては、まず CA-TF の活動紹介が行われた。

図 5-13　RIPE NCC における Certification Task Force

Certification Task Force は、第 53 回 RIPE ミーティングのときに結成されたもので、LIR の中の希望者によって構成されている。RIPE 地域の ISP のオペレーターにリソース証明書に関する周知を図ったり、RIPE NCC に対して、リソース証明書の影響などに関するアドバイスを行ったりするとされている。

第 54 回 RIPE ミーティングでは、CA-TF の 1 回目となる報告が行われた。発表によると、下記五つのエリアにわけて調査と議論が行われている。

CA-TF で活動中の五つの調査・検討エリア：

○ビジネスエリア（ポリシーを含む）

認証と業務上の関連性(エンドユーザや PI アドレスの割り当て先)、ERX や RIR 間におけるアドレス資源の移転に関する事項を扱う。

○サービスエリア

公開用の証明書データベースとしての証明書リポジトリやリソース証明書の検証サービスに関する事項を扱う。

◯テクニカルエリア

証明書リポジトリのアーキテクチャや性能の影響に関する事項を扱う。

◯RIR エリア

信頼点（trust anchors）や導入プランに関する事項を扱う。

◯アプリケーションエリア

ルーティングにおける IP アドレスの認可（authorization）や RPSL との互換性、準備の自動化などに関する事項を扱う。

今回は評価の結果や内容については報告されておらず、第 55 回 RIPE ミーティングで結果報告のドキュメントが公開されることになっている。結果として、2008 年 1 月にホワイトペーパーが出され、更に RIPE NCC における適用に関する議論も行われた。

また今回、CertProto チームについても紹介された。CertProto プロジェクトは、リソース証明書のシステム評価を行う RIPE NCC 内部のプロジェクトで、CA-TF と同じ 3 日目の NCC Services WG において、RIPE NCC の Henk Uljterwaal 氏によって活動内容が紹介された。CertProto プロジェクトは 2007 年 1 月頃に始められたもので、CA-TF の活動促進と RIPE NCC 内部でのリソース証明書についての理解を深めることを目的としている。

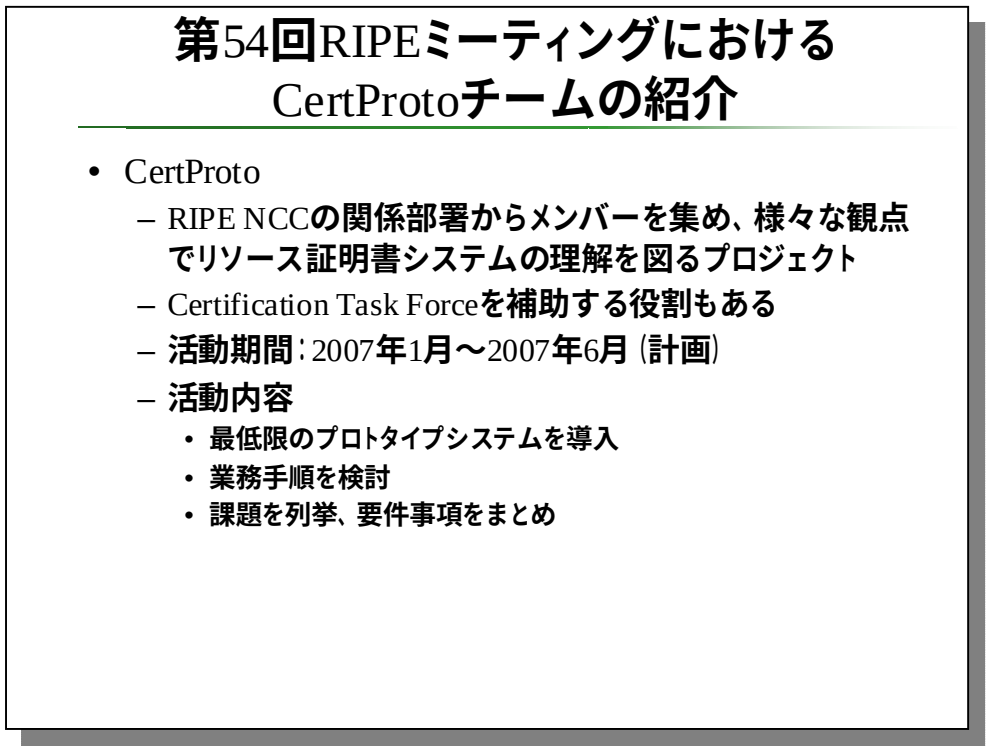

図 5-14　第 54 回 RIPE ミーティングにおける CertProto チームの紹介

活動の一環として、プロトタイプシステムの構築や、業務プロセスの仮構築が行われている。プロジェクトメンバーは、RIPE NCC の各部から選ばれたスタッフで構成されている。

CertProto プロジェクトの注目すべきところは、本番用のシステム開発を行う前に試験利用のためのシステムを開発し、このシステムを使うことでスタッフがリソース証明書の業務プロセスを理解する工程が入っている点である。これによって、RIPE NCC でリソース証明書のサービスを行う場合に、業務を変更するための課題やシナリオを具体化しやすくなると考えられる。これまでの APNIC や ARIN の活動状況をみる限り、このような活動は RIPE NCC でしか行われていない。

RIPE ミーティングでは、IPv4 アドレスの枯渇の問題や IPv6 関連の話題もあった。

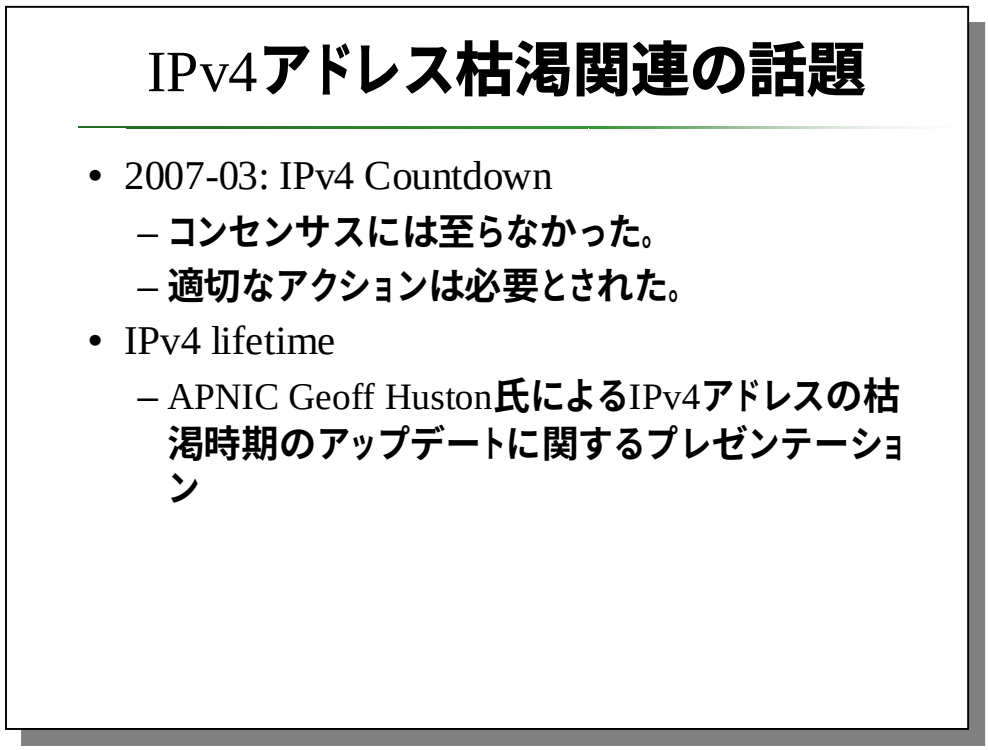

図 5-15　IPv4 アドレス枯渇関連の話題

IPv4 アドレスの枯渇については、JPNIC を中心として提案された IPv4 Countdown ポリシーである。これは IANA から RIR への最後のブロックの割り振り方に関するポリシーである。コンセンサスには至らなかったが、このポリシーで取り組もうとしている割り振りの課題について、適切なアクションを取ることが必要であるという認識を広める結果になった。

また APNIC の Geoff Huston 氏より「IPv4 lifetime（IPv4 アドレスの寿命）」と題してプレゼンテーションが行われた。IPv4 アドレスの枯渇時期の予測にあたって、より現状に近くなるような式を当てはめた結果、枯渇時期が前倒しになったというプレゼンテーションである。いずれにしても予測される時期は 2011 年頃である。

IPv6 については三つほどのプレゼンテーションがあった。

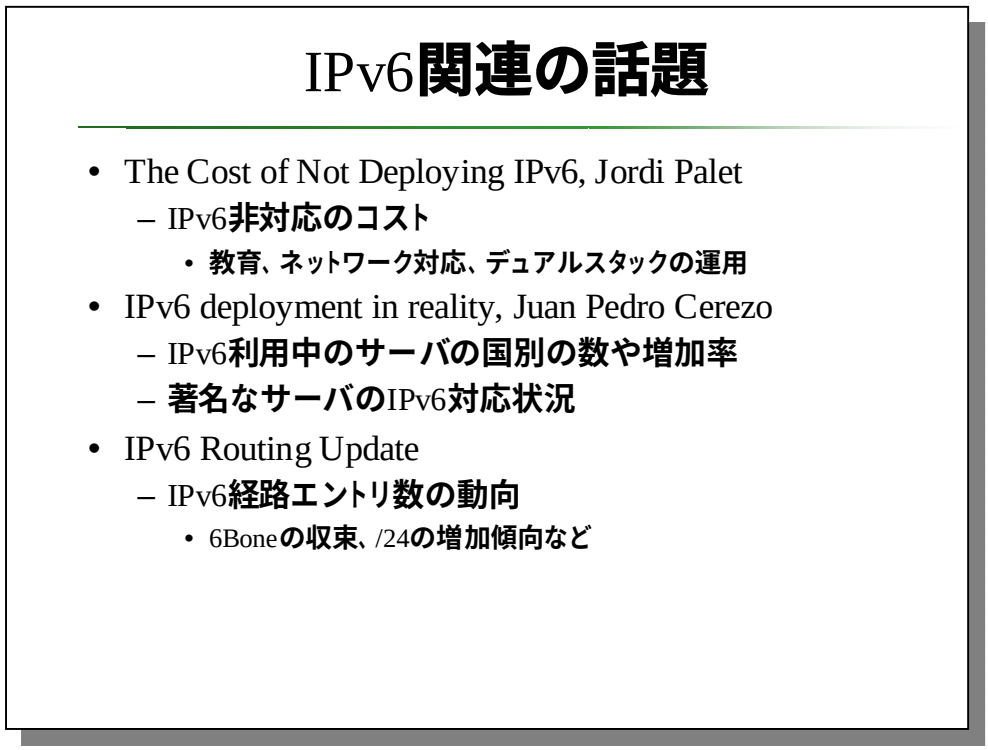

図 5-16　IPv6 関連の話題

「The Cost of Not Deploying IPv6」は、IPv6 を利用しない場合には、IPv4 のみのネットワークを維持し続けるよりもコストがかかる、というプレゼンテーションである。発表者の Jordi Palet 氏は、IPv6 の普及の為にこのようなプレゼンテーションを各 RIR で行っており、またチュートリアルにも力を入れている人物である。

「IPv6 deployment in reality」は、IPv6 の利用状況を簡単な統計データを元に紹介したものである。増加傾向はあるものの、国に依存する様子が伺われた。またインターネットレジストリや著名な検索エンジンの Web サーバで、IPv6 が使われていないような意外な事実も紹介された。

「IPv6 Routing Update」は、IPv6 の経路表の統計データなどについて述べたものである。6bone のプロジェクトが終わったことの影響が経路表から見て取れたり、/24 の経路情報の増加傾向がわかるような説明が行われた。

その他に、インターネットに関わるいくつかの話題についてもプレゼンテーションが行われた。

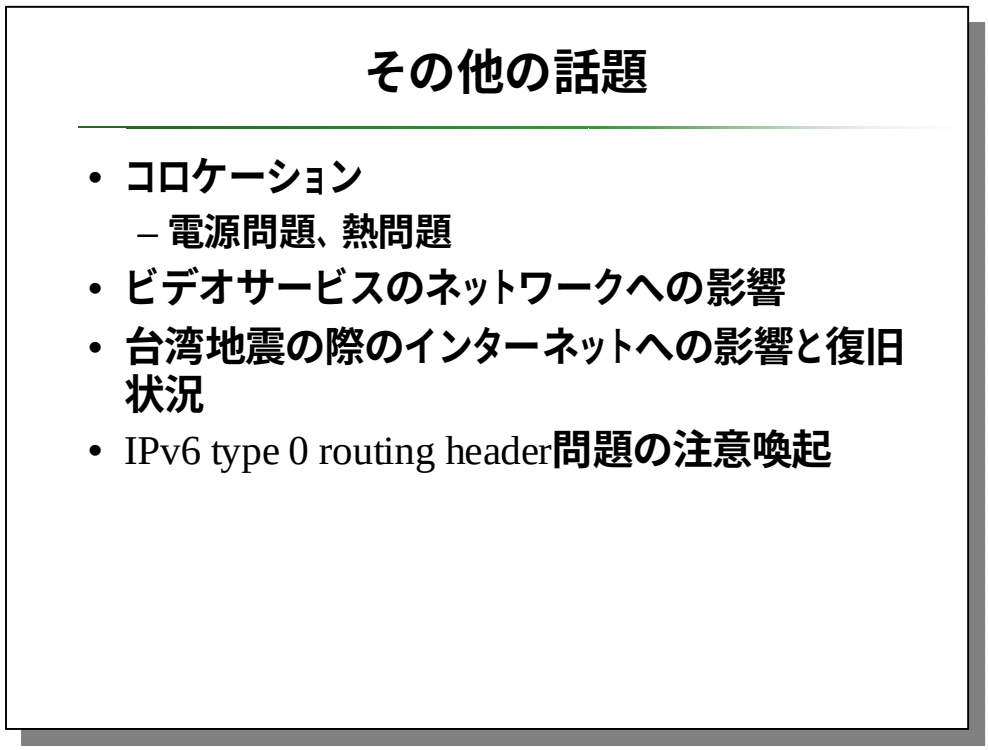

図 5-17　その他の話題

RIPE ミーティングの参加者には LIR が多く、従ってサーバ設備を持つ ISP であることも多い。最初の「コロケーション」では米国にある巨大なデータセンターにおいて取り組まれている電源問題や熱問題について紹介された。

RIPE 地域では、各種ビデオストリーミングサービスのサービス形態が日本とは大きく異なっている。ヨーロッパ地域全体という視点では、日本のように ISP に共通のネットワーク基盤が存在するわけではないので、各 ISP がネットワーク帯域等を考慮したコンテンツデリバリーネットワークを検討し、構築する必要がある。ネットワーク帯域とユーザ数を考慮して、いくつかのコスト対収容可能顧客数のモデルが示されていた。コンテンツ提供側との接続をよくすると維持費がかかるが、より高品質なビデオサービスを提供できることになり、顧客獲得に繋がりやすい。

この他に、他に台湾でおきた地震の影響でインターネット経路制御が変化した様子を統計データを元に示したプレゼンテーションなどが行われた。

5.9. 第 55 回 RIPE ミーティング

第 55 回 RIPE ミーティングは、2007 年 10 月 22 日～10 月 26 日、オランダのアムステルダムで行われた。会場は RIPE NCC のオフィスに歩いて行ける距離にある

Krasnapolsky ホテルである。

図 5-18　第 55 回 RIPE ミーティング

第 55 回 RIPE ミーティングでは、リソース証明書の動向の調査などと共に、IRR の信頼性向上に関する研究を行っている NTT コミュニケーションズ社と RIPE NCC を訪問し情報交換を行った。

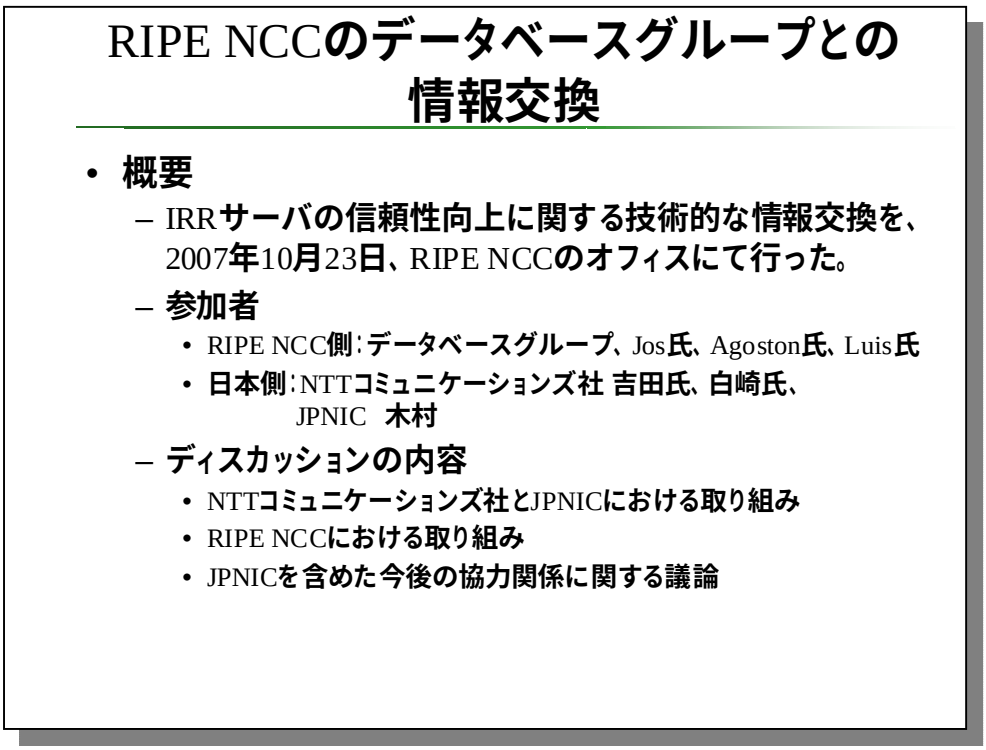

図 5-19　RIPE NCC のデータベースグループとの情報交換

本調査研究の経路情報の登録機構を使って登録情報の正当性の維持を図ると共に、NTT コミュニケーションズ社が開発中の IRR サーバシステムを用いると運用の冗長性を確保するというアイディアがある。

ディスカッションの結果、RIPE NCC でも IRR システムの信頼性向上を課題としており、可能であれば技術的に協力関係を築きたいという意向であることがわかった。

5.10. RIPE Certification Task Force

第 55 回 RIPE ミーティングの初日に、RIPE Certification Task Force に関するミーティングが行われた。このミーティングはインフォーマルに行われたが、議事についての情報は RIPE ミーティング期間中に得ることができた。以下、概要を示す。

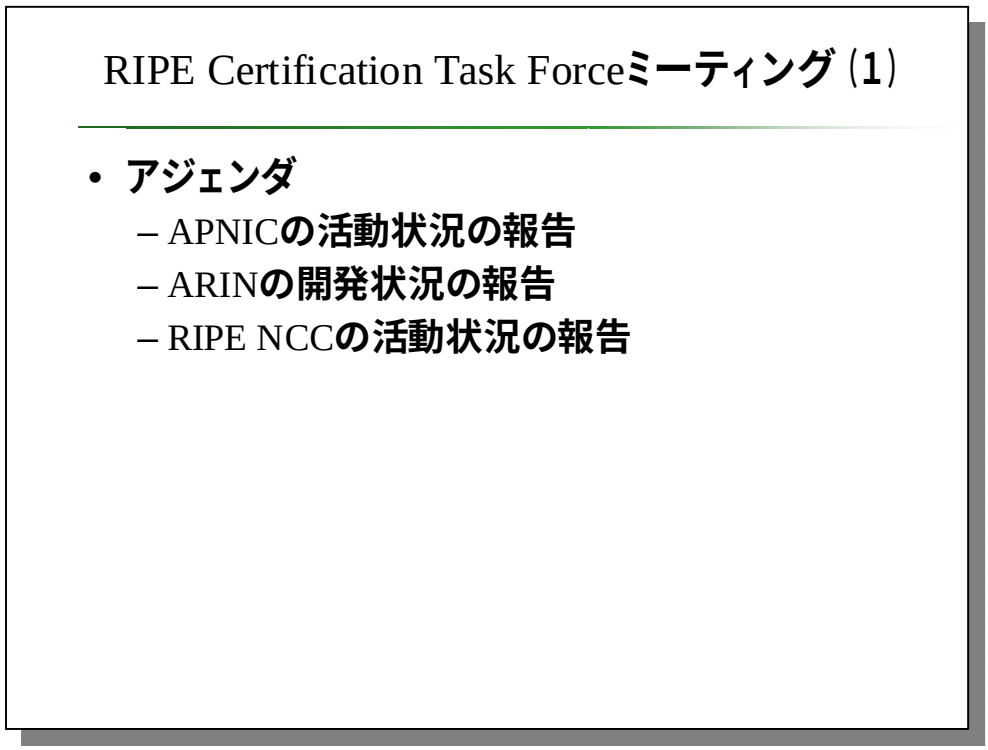

図 5-20　RIPE Certification Task Force ミーティング（1）

今回のミーティングは、リソース証明書について活動を行っている各 RIR の活動状況を報告することが主な議題であった。はじめに APNIC が活動状況を報告し、その次には ARIN が、最後に RIPE NCC が活動報告を行った。

APNIC の報告の概要を以下に示す。

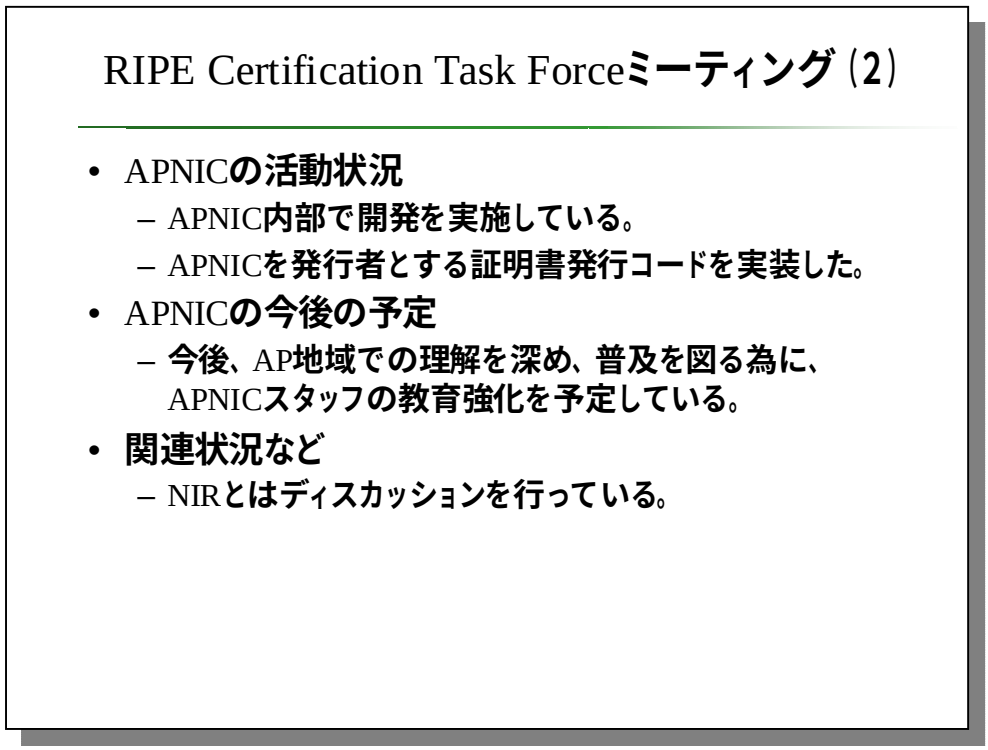

図 5-21　RIPE Certification Task Force ミーティング（2）

APNIC は APNIC 内部でプログラム開発を行っており、リソース証明書に関する中心的なシステムである証明書エンジンの開発が終わっている。ただし、AP 地域においてリソース証明書の理解は進んでおらず、普及の目処が立っていない。APNIC の LIR 向けのポータルサイト「MyAPNIC」では 2008 年 3 月に実装される予定になっている。

APNIC では、普及の目処が立っていない原因を AP 地域の NIR の理解不足である為だと考えており、普及を図る為の APNIC スタッフ向けの教育コースを検討している。

APNIC、ARIN、RIPE NCC の中では NIR があるのは APNIC だけであり、リソース証明書の NIR の認証局の構築には、NIR の協力が不可欠となる。しかし次の ARIN の報告にもあるように、RIR 自身が NIR のリソース証明書機能を持つ方法も考えられる。

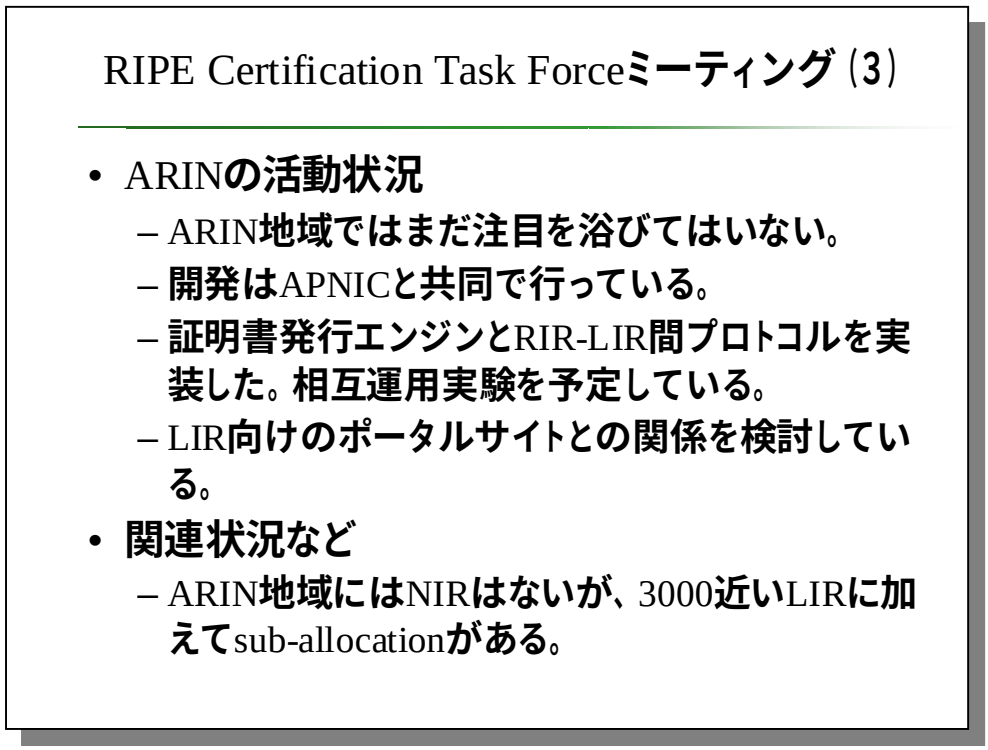

図 5-22　RIPE Certification Task Force ミーティング（3）

ARIN では、APNIC と共同でリソース証明書の開発を進めている。証明書エンジンをはじめ、認証局システムが行う 3 種類の通信プロトコルの実装を進めている。一つは認証局とレジストリシステムであり、もう一つは RIR-LIR 間のプロトコルである。三つ目は、証明書の公開機能（証明書リポジトリにあたる）であるが、この開発は未着手である。

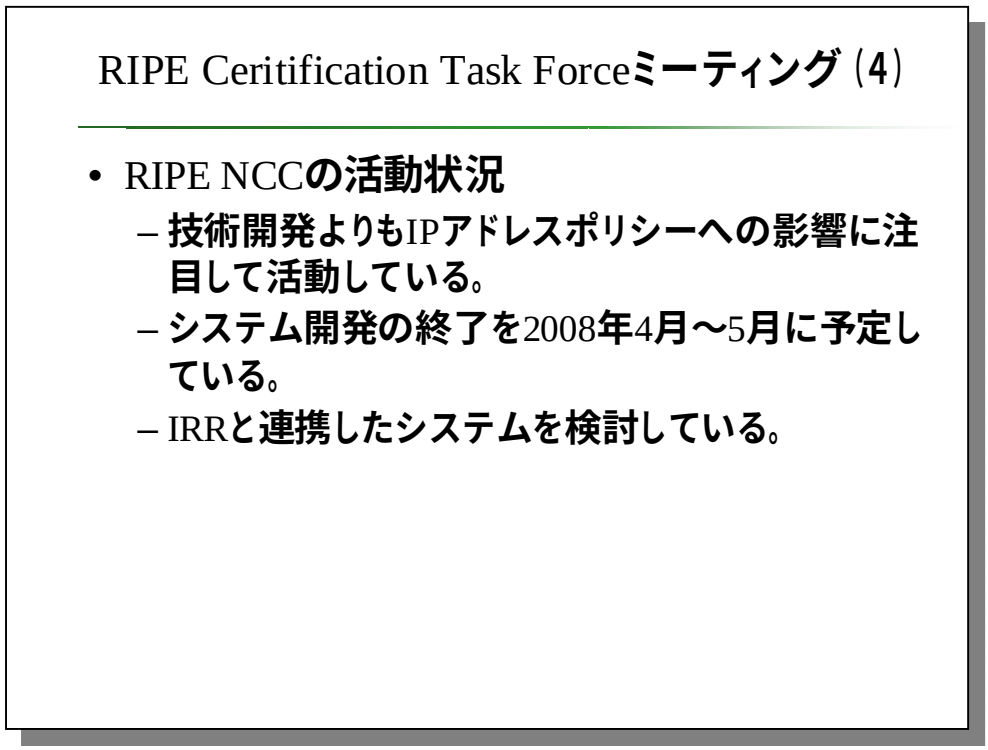

図 5-23　RIPE Certification Task Force ミーティング（4）

RIPE NCC では、ARIN や APNIC のようにプログラム開発よりも、リソース証明書の IP アドレスポリシーへの影響について注目した活動を行っている。Certification Task Force では IP アドレスポリシーや RIPE NCC での IP アドレスに関するビジネスへの影響を調査することになっており、活動中である。すでに業務検討のためのプロトタイプシステムは開発済みであるが、今後業務で利用可能なシステムの開発を予定している。この開発は 2008 年度の初頭に完成するとされている。なお RIPE NCC ではリソース証明書システムと IRR の連携を含めてシステムを検討しているとの事であった。

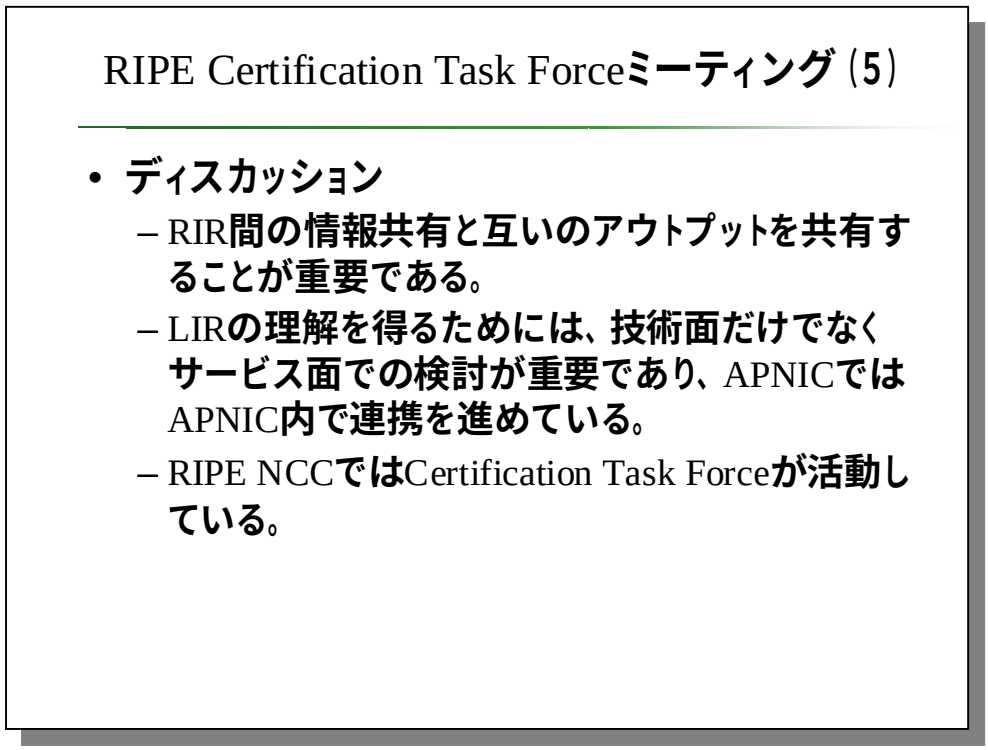

図 5-24　RIPE Certification Task Force ミーティング（5）

RIPE Certification Task Force ミーティングでは、問題点と今後の課題についてもディスカッションが行われた（図 5-24）。

問題点は普及に向けた LIR の理解が得にくいことである。これは主に APNIC が指摘している。ミーティングでは、APNIC や ARIN が、RIPE NCC の開発や実験に対するより多くの協力を行うように求めている側面があるように思われたが、RIPE NCC としては、ビジネス面および IP アドレスポリシーへの影響など、必要不可欠な検討を行っているという回答であり、RIR 同士の連携が、今後の課題であるという確認が行われた。

「RIPE Certification Task Force ミーティング」であったが、ARIN や APNIC が主に発言し、RIPE との協力関係を模索するようなミーティングとなった。

5.11. ARIN における動向

ARIN における電子認証とリソース証明書の動向を調査するため、第 19 回 ARIN ミーティングと第 20 回 ARIN ミーティングに参加した。本節では、ARIN ミーティングを通じてわかってきた ARIN における取り組みについて述べる。

図 5-25　第 19 回 ARIN ミーティング

ARIN ミーティングは、RIPE NCC のミーティングに比べると参加人数は少なく、併設されることの多い NANOG（North American Network Operator's Group）[3]のミーティングよりも少ない（図 5-25）。ARIN 地域では、アメリカの LIR が多いため、参加者の多くはアメリカの人である。また各 RIR からの参加者は多い。

[3] The North American Network Operators' Group
http://www.nanog.org/

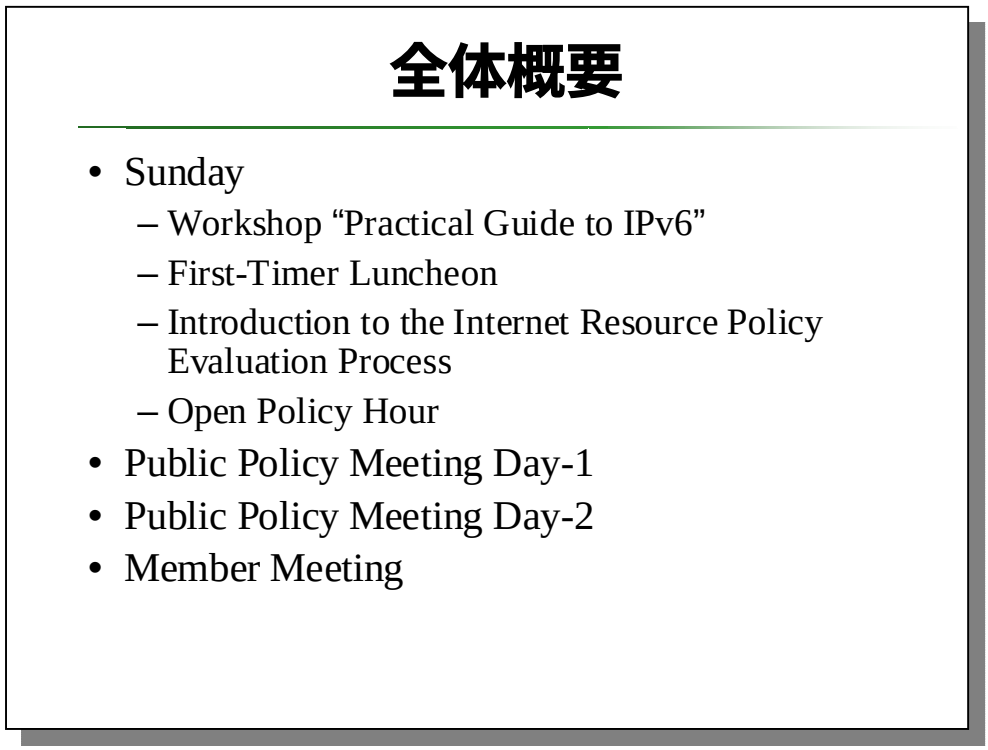

図 5-26　全体概要

第 19 回 ARIN ミーティングは、プエルトリコのサンファンで行われた（図 5-26）。ARIN ミーティングは初日の日曜日にチュートリアルやワークショップが行われ、二日目から三日目に IP アドレスポリシーに関する議論が行われた。最終日は ARIN の Member Meeting（JPNIC でいうところの総会）である。

IP アドレスポリシーの中で、ARIN における電子認証に関連するポリシー提案があった。電子認証に関連するポリシー提案は三つあった。三つのポリシー提案は、ARIN におけるポリシー文書である NRPM（ARIN Number Resource Policy Manual）に電子認証に関する章を設けることに各々が関連しており、いわば電子認証方式に関する包括的な提案である。

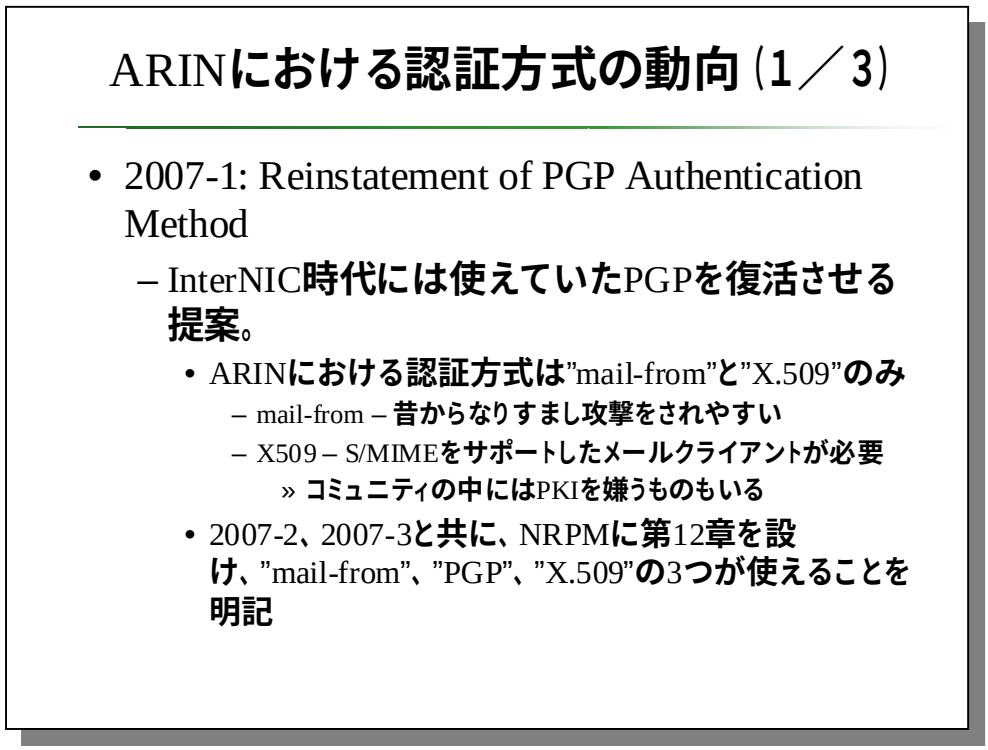

図 5-27　ARIN における認証方式の動向（1／3）

一つ目は、歴史的に古い IP アドレスの割り振り先組織に対する電子認証の方式に、PGP を使った方式を加える提案である（図 5-27）。ARIN では mail-from と X.509（PKI の電子証明書を使う方式）が使われることになっているが、すでにユーザがなじんでいる PGP を使えるようにするポリシー提案である。

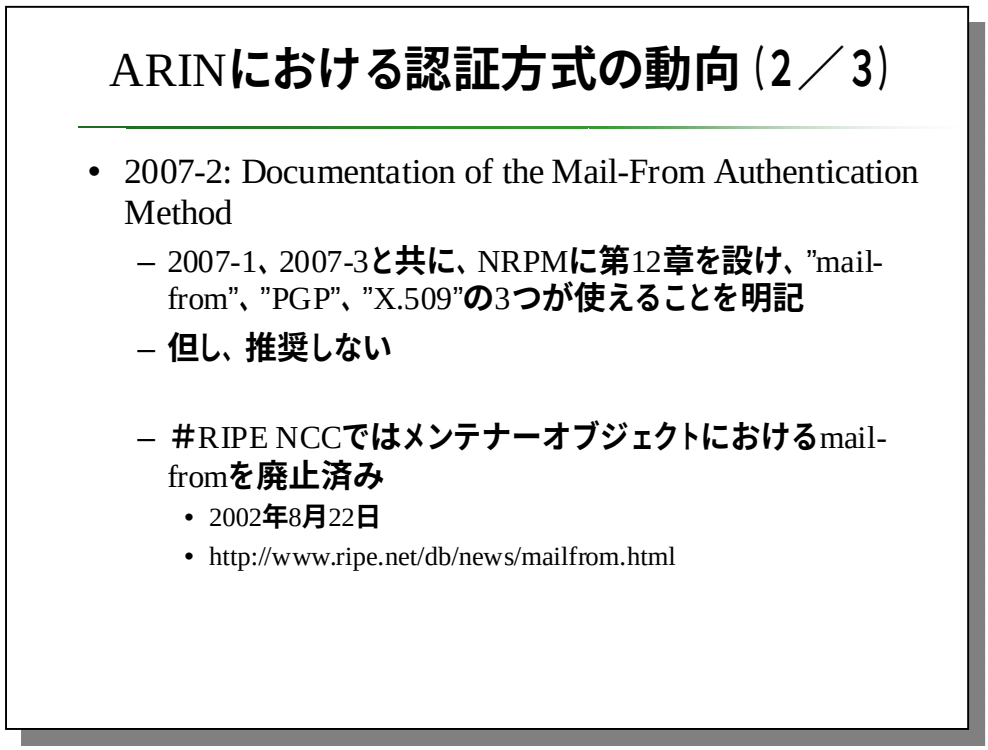

図 5-28　ARIN における認証方式の動向（2／3）

二つ目は、新たに設ける第 12 章で mail-from についても方式の一つとして明文化するという提案である（図 5-28）。ただし、この方式は推奨しないことを明記することとなっている。

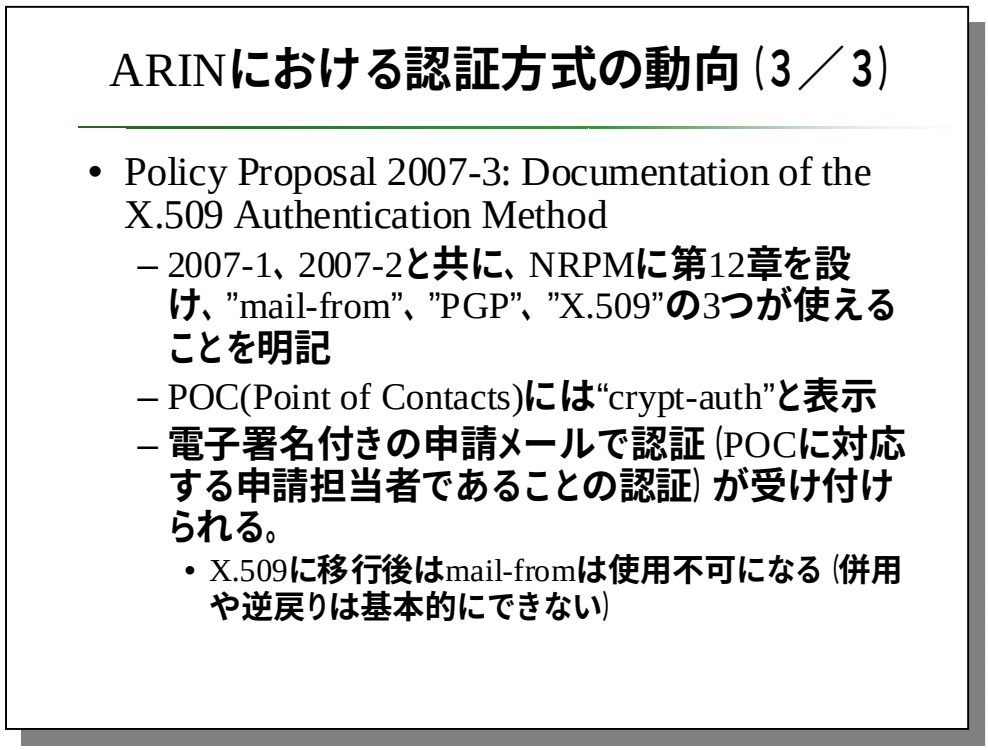

図 5-29　ARIN における認証方式の動向（3／3）

三つ目は、X.509 形式の電子証明書を用いた認証方式である。ARIN ではすでに S/MIME の電子署名を用いた申請業務を開始している（図 5-29）。電子証明書の発行対象は、ARIN における LIR の連絡先情報である POC（Point of Contact）に対応する申請業務担当者とされている。また一旦電子証明書を用いた方式に移行すると、基本的に mail-from の方式に戻ることはできない。

リソース証明書については、プログラム開発の動向を中心に発表があった（図 5-30）。

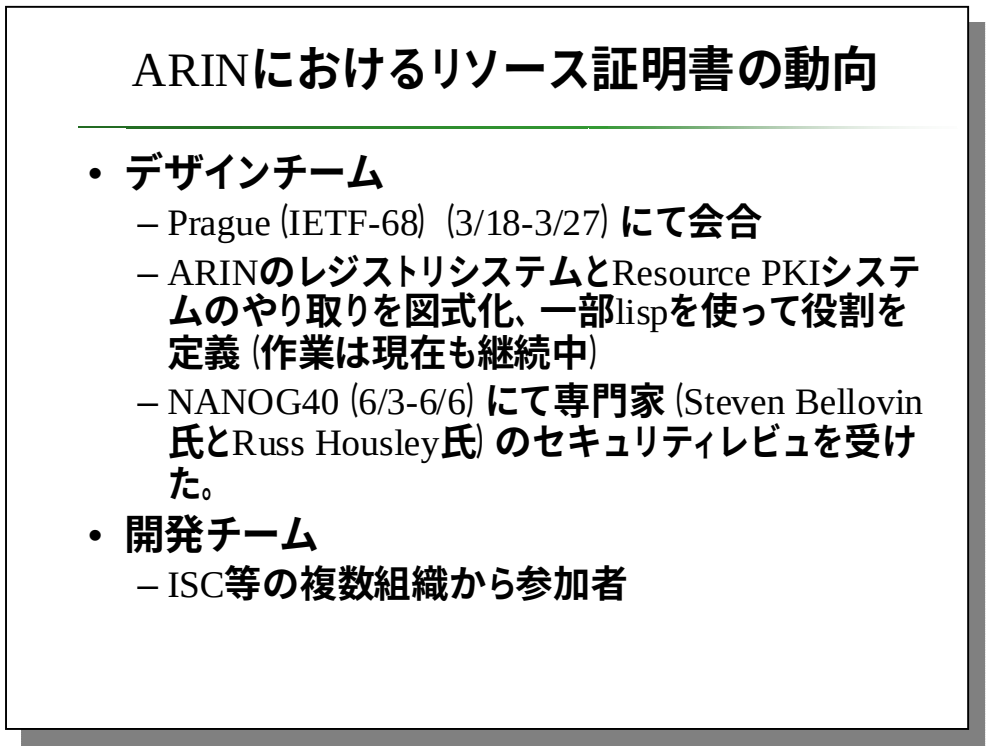

図 5-30　ARIN におけるリソース証明書の動向

プログラム開発は、ISC や APNIC と共同のチームで行われている。開発の際には、デザインチーム（概要設計を行う専門家グループ）が作られ、概要設計の段階で、セキュリティレビューを受けたとの報告があった。本格的な開発はこのあとに行うとされていたが、2007 年 7 月下旬に行われた第 69 回 IETF で相互運用試験が予定されていることから、詳細設計と開発が同時に行われていることが伺われる。

5.12. 第 20 回 ARIN ミーティング

第 20 回 ARIN ミーティングは、アメリカ合衆国のアルバカーキで行われた。第 20 回 ARIN ミーティングに先立ち、第 41 回 NANOG ミーティングが行われた。NANOG は北米地域のネットワークオペレーターの会合で、ネットワークオペレーションに関わる技術的な議論が行われる。参加者は ARIN ミーティングよりも NANOG の方が多い傾向がある。

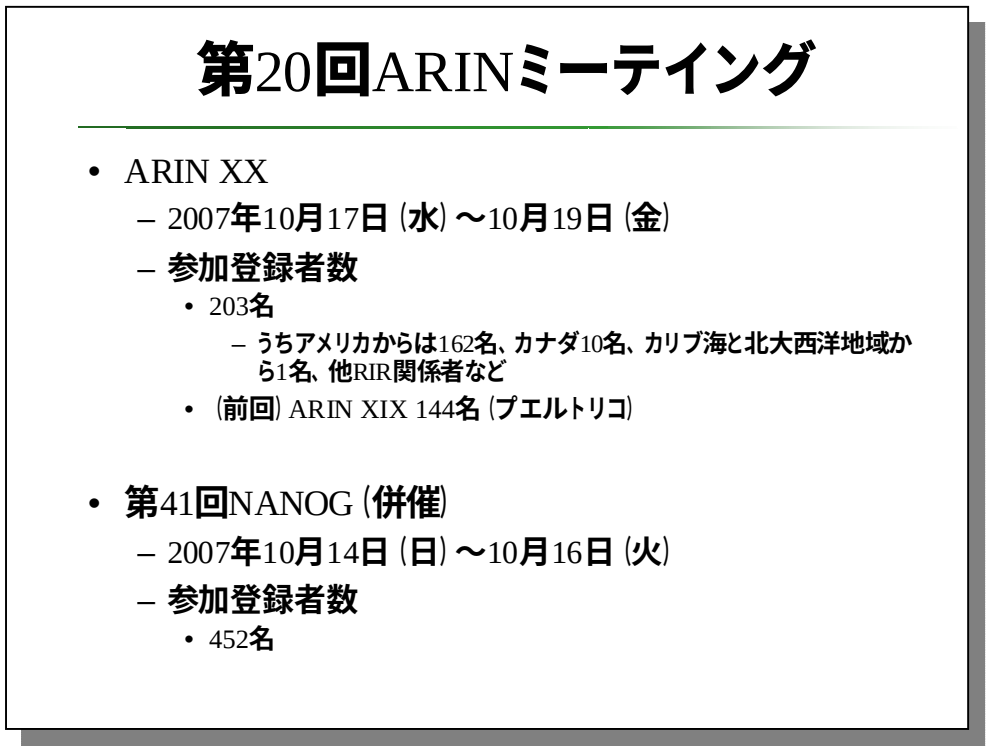

図 5-31　第 20 回 ARIN ミーティング

ARIN のメンバーミーティングで取り上げられた、電子認証に関わる話題を示す。

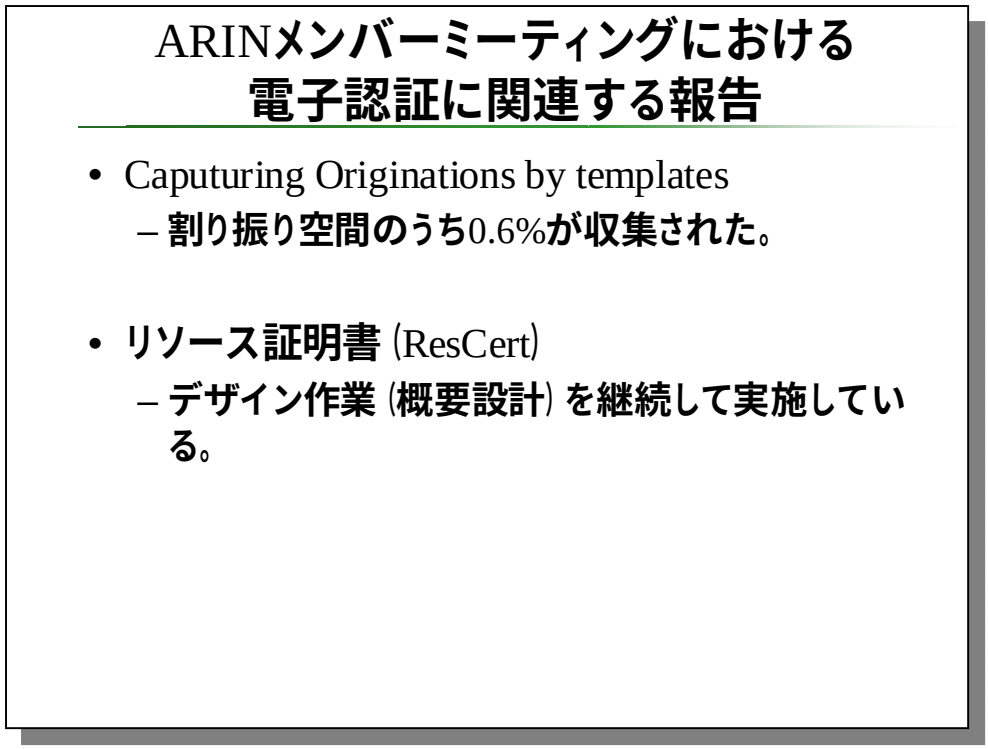

図 5-32　ARIN メンバーミーティングにおける電子認証に関連する報告

ARIN の技術部門から報告によると、Proposal 2006-3 で提案された割り振り／割り当てテンプレートを使った Origin AS の情報は、割り振り／割り当て情報のうち 0.6%が収集されたとのことである（図 5-32）。発表者は、これはペースが遅いという考えを持っていたようだが、提案が採用されて一年程で、ARIN の割り振り／割り当て情報の中の 0.6%という数字は決して少なくはない。

リソース証明書については、情報が少ないながら、ARIN としても公にして活動を始めた。前回の第 69 回 IETF での様子から、このときは既にプロトタイプシステムができており、動作試験ができているが、メンバーサービスとしてはまだ実装途中であると言える。

5.13. APNIC における動向

APNIC における電子認証とリソース証明書の動向について調査するため、第 24 回 APNIC ミーティングに参加した。

第 24 回 APNIC ミーティングは、インドのニューデリーで行われた。この APNIC ミーティングでは、NIR hostmaster workshop（NIR の IP アドレス申請業務担当者向けのワークショップ）として、リソース証明書に関するディスカッションが行われた。

APNIC では、2006 年度の初め頃からリソース証明書の開発に取り組んでいる。今回のワークショップは、リソース証明書のサービス化に先立って、リソース証明書の提供方法に関する意見を NIR から集めるという趣旨であった。

AP 地域には NIR が多く存在しているため、リソース証明書を提供する形態が、他の RIR よりも複雑になる。少なくとも、二種類の方式が考えられる。一つは APNIC が集中的に証明書を管理する方式で、もう一つは各 NIR が証明書の管理を行う方式である。リソース証明書の技術には、他に利用可能性等の課題があるが、こちらについてはアジェンダになく、議論されなかった。

今回の Workshop でわかってきたことは、まず APNIC ではリソース証明書の 2007 年度末のサービス化を、変更する余地のない計画だと考えている点である。IPv4 アドレスプールの枯渇期において、IP アドレスの不正利用対策としては、リソース証明書が唯一の手段であるように捉えられているようで、サービス開始を急ぎたい様子である。ただし、APNIC におけるリソース証明書の提供には次に述べるような利用可能性等に関する課題がある。

■サービス化に先立って存在する利用可能性の課題

APNIC 側が考えるリソース証明書の用途は二つあるとされている。一つは IP アドレスの割り振りを通じた正当な利用権利を示すデータである。もう一つは IETF SIDR WG で議論されている、セキュアなドメイン間ルーティングである。

リソースに対する電子証明書がいくら発行されても、それが本来の目的を達せなければ意味がない。ここでいう本来の目的とは、リソースの不正利用を排除したり、レジストリの登録情報に基づいてルーティングの安全性向上が図れるか、といったことである。つまり、サービス化の前に、以下に挙げる課題をクリアしている必要があると言える。

○サービス化に先立つ、リソース証明書の利用可能性の課題

a.リソースの不正利用があったときに、それを回避する／拒否する
　手法を確立すること

b.IETF SIDR WG で提案されているように、S-BGP 等で利用し、ルー
　ティングの安全性への利用ができること

前述の通り、今回のワークショップではこれらの課題に関する議論はできず、単に APNIC がサービス化する意思を NIR に伝える場になっていた。

■リソース証明書に関する NIR の動向

ワークショップの終了後、ワークショップに参加していた NIR の各担当者の方々がほぼ全員残る形で、リソース証明書に関する情報交換が行われた。KRNIC や TWNIC は、そもそもリソース証明書に関する技術的な情報が足りていない状況があり、懸念点がわからない様子であった。

今回のワークショップについては、以下のような意見が挙げられた。

〇KRNIC や TWNIC の意見

a.リソース証明書の技術的な必要性が理解できていない。

費用がかかる大きなプロジェクトだがその理由付けが少なすぎる。

b.実験的な利用開始はよいが、サービス化は改めて検討が必要。

－ルーティングの安全性向上は LIR に求められていることではある。

－投資の検討は必要だと考えられる。

今回の Workshop は、APNIC からの情報伝達に近いものがあったが、今後アジア太平洋地域での適切な普及を図るには、まず NIR の理解を図ることから始める必要があると考えられる。

これは、RIPE NCC における Certification Task Force ミーティングにおける発言にあった APNIC の認識と近いものがあるが、技術面に傾倒しており、AP 地域での普及にはコストとベネフィットを踏まえた、LIR へ提供することの妥当性の議論が必要であると考えられる。

5.14. まとめ

RIR と主に IETF SIDR WG では、リソース証明書を使った経路制御の安全性向上策について議論が行われている。

リソース証明書については、APNIC が中心的に推進しており、開発は APNIC と ARIN が主に行っている。RIPE NCC は開発に参加しつつも、IP アドレスに関するポリシーの関連の仕方など、総合的な捉え方をしている。2007 年度末には APNIC にて実装がリリースされることから、ARIN 地域や RIPE 地域に比べて AP 地域におけるリソース証明書の提供は早い。一方で、APNIC では技術開発に力が入れられており、LIR へのサービスとしてのリソース証明書、すなわちビジネス面の検討はまだ進んでいない状況である。

ARIN および RIPE NCC では、LIR の認証に関する取り組みが行われている。両 RIR

共に電子証明書を使った LIR の認証は採用済であり、認証方式の明文化や mail-from などの弱い認証方式（認証を行っていないとも言える）の削除の動きがある。

IETF SIDR WG では、ルータにおけるリソース証明書の検証にまで議論が進みつつあるが、インターネット経路情報に対してどのようにフィルタ等を適用すべきかについて、いまだ議論が進んでいない状況である。

本章で述べた RIR および IETF における電子認証に関わる動向調査は、ほとんどすべてについて現地調査を通じて行った。これにより、ここでは報告しきれないほどの情報を逐次得ることができ、また関係者と直接ディスカッションができる基盤ができた。

第 5 章　経路制御のための電子認証技術に関する国際動向