2007.5.7→5.11

第54回RIPEミーティング報告

第54回RIPEミーティングは、2007年5月7日～11日、エストニアのタリンで行われました。エストニアは東欧の北部にあるバルト三国の一つで、人口が140万人程の小さな国です。バルト海のフィンランド湾を挟んだ反対側はフィンランドです。タリンはエストニアの首都で、タリンのすぐ近くにフィンランド湾に面した港があります。タリンには13世紀頃に建てられた歴史的な建造物が残る旧市街があり、今回RIPEミーティングが行われたSokos Viruホテルは、この旧市街のすぐそばにあります。

第54回RIPEミーティングは、1日目から3日目にかけてPlenary（全体会議）が、3日目から最終日の5日目にかけてWGのミーティングが行われました。Plenaryでは、“Colocation Workshop”と題して、IXを収容していて機器の集約が進みつつあるデータセンターに関して、パネルディスカッションが行われました。電力不足のネットワークへの影響や、設備、価格の動向などが話題になりました。

今回の参加登録者の数は288名で、前回の317名および前々回の315名に比べてやや少なかった模様です。最も多かったのはアメリカからの参加者で15%程、続いてドイツが11%、オランダが8%でした。日本からの参加者は7名で2%でした。

■全体会議報告

◆Plenaryミーティング

Plenaryミーティングでは、先に述べましたワークショップの他に、IPv6の普及の現状や移行に関するプレゼンテーションが行われました。特に関連するものを以下に挙げます。

□ IPv6 Routing Update
発表者：Gert Doring氏
IPv6におけるグローバルルーティングテーブルの傾向や、RIRの割り振りと経路広告の傾向などを紹介。

□ IPv6 deployment in reality - an update.
発表者：Fernando Garcia氏
国別のIPv6を使ったWebサーバ数紹介や、著名な組織のIPv6でのWebサービス提供状況などの紹介。

□ The Cost of Not Deploying IPv6
発表者：Jordi Palet氏
IPv6に移行せず、IPv4を使い続けた場合に考えられるコスト要素を、技術的な観点で紹介。

これらのプレゼンテーションの資料は、以下のWebページから入手できます。

□ RIPE 54 Presentations
http://www.ripe.net/ripe/meetings/ripe-54/presentations/tuesday.html

◆IPv4アドレスの在庫枯渇時期の予測に関する発表

IPv4アドレスの在庫枯渇時期について予測を行っているAPNICのGeoff Huston氏が、3日目のPlenaryミーティングで、最新の予測結果についてプレゼンテーションを行いました。

Huston氏は、これまでにも予測を行ってきており、その予測では2011年に枯渇すると言われていました。今回はIPv4アドレスの需要を予測する際、一次関数ではなく、より過去のデータに近似することができる二次関数を増加率の計算のために用いたそうです。その結果、最新の予測ではIPv4のIANAプールが2009年12月に枯渇するという結果になりました。

RIRをはじめ、多くの会議では2011年という予測を基に議論が行われてきましたが、今回発表された予測ではそれより2年も早まり、IPv4アドレスの在庫枯渇は、従来言われていた4年後ではなく、2年後に迫ったことになります。ただしHuston氏は、この予測が今後ポリシーの変更が無く、枯渇時期の混乱等が一切発生しない状況を前提としていることや、現実の割り振りや経路広告状況は刻一刻と変化していることなどから、予測時期は常に変化する可能性がある点を付け加えています。

最新の予測結果は以下のWebページで公開されています。

□ IPv4 Address Report
http://ipv4.potaroo.net/

◇　　◇　　◇

RIPEミーティングでは、ミーティングのテーマについて、ISPの技術とビジネスという両方の観点から、うまく取り上げられているように感じます。例えば今回は、Colocation Workshopの他に、ビデオストリーミングサービスの普及によるISPへの影響や、IPv6への移行を議論するにあたっての、論点の整理などについて取り上げられました。議論の方向性はオペレーターを対象とした技術的な話題や、アドレス資源管理のポリシーに関する話題とは異なるものの、ISPにとっては大変興味深い議論ではないかと思います。ヨーロッパやアメリカに比べて、ユーザに提供されるネットワーク帯域が抜きん出ている日本でも、ISPの技術とビジネスという、それぞれの観点から議論ができる場が増えることで、より興味深い話題が取り上げられるのではと思いました。

次回の第55回RIPEミーティングは、2007年10月22日から26日にかけて、オランダのアムステルダムで開催される予定です。

（JPNIC 技術部 木村泰司）

会場となったSokos Viru Hotelの外観

■IPアドレスポリシー関連報告

◆概要

RIPE54におけるアドレスポリシーの動向についてお伝えしたいと思います。4日半にわたって開催されたミーティングのうち、アドレスポリシーWGは5月9日（水）11時半から2時間半のセッションでした。

RIPEミーティングは、オペレーションに関わるテーマを中心に議論が進められるため、APNIC、ARINと比較すると、アドレスポリシーに関する議論が占める割合は低いと言えます。

RIPEでは、基本的にミーティングで結論を出すことを目的としておらず、ミーティングは、メーリングリストでの議論への補足的な位置付けで捉えられているようです。したがって、新規の提案に対しては、その内容紹介を中心として踏み込んだ議論や結論を求めることはせず、継続議論になっている提案に多くの議論の時間を費やす構成となっていました。

◆今回結論が出た提案

今回取り扱われた提案は合計12点あり、このうち施行が決定したものは次の2点です。

2006-06：IPv4 Maximum Allocation Period
http://www.ripe.net/ripe/policies/proposals/2006-06.html
現在、RIPE地域では最大2年分の需要を満たすIPv4アドレスの割り振り※1が認められているが、他の地域との公平性の観点からこれを1年に短縮する

2006-07 : First Raise in IPv4 Assignment Window Size
http://www.ripe.net/ripe/policies/proposals/2006-07.html
LIRのアサインメントウィンドウ※2を、当該事業者が初回割り振りを受けた6ヶ月後に、自動的に/21に更新する

一方、提案事項「2006-04:Contact e-mail Address Requirement」は、否決が決定しました。

受付デスク(Registration Desk)の様子

◆IPv4アドレスの在庫枯渇に向けたポリシー

今回、JPNICとしての主な参加目的は、JPNICのIPv4アドレス枯渇対応チームが策定した提案を行うことでした。内容は基本的にAPNIC23、ARINXIXで行ったものと同じく、以下の方針を定めることを提案しています。

- IPv4アドレスの在庫枯渇に対しては、世界的に調整の上取り組みを進める
- 延命のためのルール変更は行わない
- 分配済みアドレスの回収は別の議論とする
- 割り振り終了日を前もって決めた上で周知する

なお、提案では割り振り終了日を告知日の2年後と定義していますが、質疑応答ではこの日の午前中、Plenary Session中に行われたGeoff Huston氏の発表で在庫枯渇予測日が2009年に縮まったとの発表があったため、「今から2年半後には在庫が枯渇するため、提案が機能していない」「グローバルポリシーとして施行するには間に合わない」といった指摘がありました。

時間的な制約からそれ以上コメントを受け付けることができなかったため、ポリシーWGのチェアより啓発を中心に捉える等、アプローチを変えて提案してはどうか、とのコメントがあり、セッションは締めくくられました。

本提案については、ミーティング開催中に参加者とも個別に話をしたところ、在庫枯渇のテーマそのものには関心を持っているようでしたが、新規の提案ということもあってか、ポリシーとしての今後の取り組みについては、地域内の参加者からは積極的な反応はありませんでした。その他地域からの参加者も総合した、主な意見は以下の通りです。

- 在庫枯渇日の予測は変動するため、具体的な日付を人為的に定めることは意味を持たない
- 分配済みのアドレス管理をより確実にするPKIによる認証導入の検討が必要
- 現在利用されていないIPv4アドレスの有効活用も検討するべき

現時点では、最後となる割り振りブロックの扱いをどのようにRIR間で分け合うかについて、ポリシー策定の意識が高い人は一定の関心があるようですが、時期を合わせる必要性については、まだ一致した見解はないようです。

本提案については、この結果をチームに報告の上、今後の対応を検討してまいります。

※1 インターネット用語1分解説
「割り振り（Allocation）、割り当て（Assignment）とは」
http://www.nic.ad.jp/ja/basics/terms/allocation-assignment.html

※2 アサインメントウィンドウ
IPアドレス管理指定事業者が、接続組織にJPNIC審議を受けることなく、自主的に割り当てることができる最大のアドレス空間の大きさを示すものです。

Internet Topics インターネット・トピックス

◆その他の議論

アドレスポリシーWGセッション全体としては、IPv6に関する提案に対して最も多く議論の時間が割かれていました。このうち、既にAPNICでは適用している追加割り振り基準の変更については、おそらく次回、施行が決定すると予測されます。

2005-08：Proposal to Amend the IPv6 Assignment and Utilisation Requirement Policy
http://www.ripe.net/ripe/policies/proposals/2005-08.html
追加割り振り申請時において、利用率を算出する基準となるHD-ratioの値を0.8から0.94へ変更する提案。この施行により、申請者はより高い利用率での追加申請が求められ、IPv6アドレスのより効率的な利用につながると考えられる。APNICでは今年3月より施行済み。

また、前回のAPNIC23でも提案され、「実際ニーズがあるとの声を聞かない」とのことから継続議論になった、初期割り振り基準についても議論が行われました。

2006-02：IPv6 Address Allocation and Assignment Policy
http://www.ripe.net/ripe/meetings/ripe-54/presentations/Policy_Proposal_2006-2.pdf
現在のIPv6アドレス割り振り要件が、具体的な割り当て数を要件として設けることにより、IPv6アドレスの申請にあたって障壁になっていることから、要件を以下のように変更する提案。

（変更前）
2年以内に200の/48の割り当てを行う計画があること
（変更後）
2年以内に他組織に対してIPv6アドレスの分配を行う計画があること

ここではAPNIC地域で指摘された、障壁となっている具体的なケースの欠如については問題にならず、すぐに対応するべきとの支持が表明されました。一方、今回の提案における変更対象には含まれていなかった、現在のポリシーで割り振り要件の一部として定義されている割り振り空間を/32に集約して経路広告を行うことを求めている点に対しては、経路広告の方法についてはオペレーターの判断に委ねるべきとの理由から、いくつか反対意見が表明されました。これはオペレーターの参加が多い、RIPE地域の特色が現れた結果かもしれません。その後、メーリングリストでの議論を経て、2007年7月に本提案に基づいたポリシーはRIPE地域でも施行されました。

その他の提案については、ミーティング後も大きな動きはありませんでした。今回行われた提案の一覧については、以下のページをご覧ください。

RIPE54 Meeting“Address Policy Working Group Draft Agenda”
http://www.ripe.net/ripe/meetings/ripe-54/agendas/address_policy.html

（JPNIC IP事業部 奥谷泉）

■RIRにおける電子証明書の動向

◆概要

JPNICでは、インターネットレジストリにおける電子証明書のあり方と動向について調査研究を行っています。電子証明書は、通信相手の認証や電子署名のために使われている技術で、SSLを使ったWebサーバの認証や、SSLを使ってWebサーバにアクセスしているユーザの認証、電子メールや公的認証の電子証明書に使われるなどしています。

RIPE NCCをはじめARINやAPNICでは、LIRのユーザ認証に電子証明書を導入することに加えて、リソース証明書と呼ばれる電子証明書についての検討が進められています。リソース証明書は、IPアドレスの割り振りやAS番号の割り当てを証明し、ひいてはルーティング情報のorigination（発信元）を電子的に証明する仕組みです。RIPE NCC、ARIN、APNICの三つのRIRでは、リソース証明書を発行するプログラムを開発するプロジェクトが立ち上げられ、技術的な評価が行われてきました。

本稿では、第54回RIPEミーティングの参加を通じて見えてきた、RIPE NCCにおける電子証明書の動向について、第19回ARINミーティングの動向を交えながら報告したいと思います。

◆RIPE NCCにおける認証と電子証明書の動向

RIPE NCCでは、電子証明書を使ったユーザ認証の方式（通称“X509”）が導入されています。これは、RIPE NCCの各種申請用Webページである LIRPortalへのアクセスの際に、各LIRに対して発行された電子証明書が使われる方式です。RIPE NCCにおけるユーザの認証方式には、他にMD5（長いパスワードが使えるもの）とPGP（PGPの電子署名を使ったもの）があります。なおCRYPT-PW（短いパスワードしか設定できないもの）は、以下のプロジェクトを通じて廃止されました。

□ CRYPT-PW Deprecation Project
http://www.ripe.net/db/support/security/crypt-pw_deprecation/

WGの様子

RIPE NCCにおけるリソース証明書関連の活動は、これまではAPNICのプロジェクトに参加する形で進められてきました。しかし第54回RIPEミーティングでの二つの発表によると、現在は「Certification Task Force」と「CertProto」が中心的な活動になりつつあるようです。以下では、この二つの活動について紹介します。

Certification Task Force（以下、CA-TF）は第53回RIPEミーティングにおいて結成されたもので、RIPEコミュニティの中から立候補した6名※1で構成されています。

□ RIPE Certification Task Force
http://www.ripe.net/ripe/tf/certification/

設立当初の趣意書によると、以下について評価することが期待されています。

Certification Task Forceに期待されている報告の内容：
・リソース証明書の利便性
・LIRに対する業務面での影響
・リソース証明書サービスの要件
・ポリシーへの影響
・LIRに要求される事項

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ました。この発表は、Nigel Titley氏によって3日目のNCC Services WGで行われました。発表によると、CA-TFでは下記五つのエリアにわけて調査と議論が行われています。

CA-TFにおける五つの調査・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※2やRIR間の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※3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が行われることになっています。

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ました。

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ます。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ます。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ます。

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す。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ます。これまでのAPNICやARINの活動状況を見る限り、このような活動はRIPE NCCでしか行われていません。

今後このプロジェクトでは、費用面の検討等が行われた後、9月に調査結果が公開されることになっています。

◆ARINにおける認証と電子証明書の動向

RIPE NCCと同様に、ARINでもLIRの認証に電子証明書が使われています。一方、ARINにおけるリソース証明書の検討は、現在はクローズドなミーティングで進められています。6月頃までに利用技術等を定めたシステムデザインを進め、その後に本格的な開発が行われていく模様です。

LIRの認証については、ARINにおける認証方式に関する章を、NRPM※4に新たに設ける提案について、第19回ARINミーティングで議論されていました。以下の三つが関連する提案です。

□ Policy Proposal 2007-1: Reinstatement of PGP Authentication Method
ARINではmail-fromとX.509の2種類の認証方式しか選べないが、これにPGPを使って署名するcrypt-authを加える提案（InterNIC時代にはPGPを使うことができた）。以下の2007-2と2007-3の内容と一緒に、NRPMへの追加を行う。

□ Policy Proposal 2007-2: Documentation of the Mail-

※1 2007年8月現在で7名になっています。

※2 ERX（Early Registration Transfer project）
過去にInterNICにより割り当てられ、その後ARINが管理を引き継いだIPアドレスやAS番号のうち、現在、他のRIRs地域への割り当て分について、管理元を現在の適切なRIRへ移管するプロジェクトです。

※3 RPSL（Routing Policy Specification Language）
RFC2280で定義されるルーティングポリシーを記述するための言語で、ネットワークオペレータはこの記述を用いることにより、さまざまな階層においてポリシーを定義することができます。

RFC2280 “Routing Policy Specification Language （RPSL）”
http://www.ietf.org/rfc/rfc2280.txt

※4 NRPM（Number Resource Policy Manual）
ARINにおけるポリシーを一つの文書としてまとめたもので、ポリシーに関する議論は主にこの文案を基にして行われ、ポリシー変更の際もこの文書を変更する形で変更が行われます。

Internet Topics
インターネット・トピックス

From Authentication Method
NRPMに12章を追加し、現行の認証方式にmail-from、X.509の方式があることを明文化する提案。記述中でmail-fromは推奨されない点が補足される。

□ Policy Proposal 2007-3: Documentation of the X.509 Authentication Method
NRPMに追加される12章に、X.509の方式が選べることを記述する提案。

いずれもPaul Vixie氏、Mark Kosters氏ら5名による提案です。会場での挙手の結果、賛成意見の方が40名以上いて、反対意見の方はいませんでした。現在はBoard of Trusteesによる議論が行われている段階にあります。※5

「2007-3 “Documentation of the X.509 Authentication Method”」の提案については、会場で興味深い議論がありました。X.509の認証方式で、他のRIRの電子証明書を使えるようにすべきかどうかという議論です。提案の趣旨からは外れますが、もしこれが実現すると、RIPE NCCにおけるLIRの電子証明書やAPNICにおけるメンバーの電子証明書を、ARINにおける各種申請業務で使えることになります。複数にわたるRIRからIPアドレスの割り振りを受けていたり、他地域のASでIPアドレスが使われていたりするLIRの利便性が上がるかもしれません。

◇　◇　◇

RFC3779によると、リソース証明書はSecure BGP等のルーティングプロトコルで使われることが想定されています。しかし、これを実現するには、各RIRで発行されるリソース証明書の相互運用性が必要です。IETFのSIDR WGでは、リソース証明書を発行する認証局の証明書発行条件等を明確化するためのCPS（Certification Practice Statement）のテンプレート作りが行われており、電子証明書の相互運用性に向けた足がかりが探られつつあります。

IPv4の在庫枯渇期には、自分の組織に割り振られたIPアドレスが、他のASによって経路広告されてしまい、インターネットとの接続性が第三者に奪われてしまったり、不正なIPアドレスの使用を通じて、不正アクセスの温床が作られたりしてしまう危険性が増すかもしれません。RIPE NCCやARIN、APNICで検討されているリソース証明書は、このような不正行為の影響を避けることが可能になる技術ですが、実現性や効果はまだ明らかになっていません。効果や業務面の検討を進め、実効性のある対策が取れる状況を作ることが、RIRにとって重要になってくると考えられます。

（JPNIC 技術部 木村泰司）

※5 議論の結果、これらの三つの提案はポリシーとはなりませんでしたが、ARINにおいて、各々の認証機能について実装とマニュアル類の整備が行われることになりました。特にPGPの実装が急がれるとされています。

2007.5.21→5.25 第10回LACNICミーティング報告

第10回LACNICミーティングが、2007年5月21日から25日まで、ベネズエラのマルガリータ島で、25ヶ国から約300人の参加を得て行われました。LACNICは世界に五つあるRIRの一つで、ラテンアメリカおよびカリブ海地域を管轄するRIRです。会場のホテルは町中から隔絶され、隣の建物まで数km離れているという、実に会議に集中できる環境でした。

LACNICミーティングにJPNICの職員が出席するのは、今回が初めてということになります。また、全参加者の中でも日本人は私1人でした。プレゼンテーションはほとんどスペイン語で行われますが、ミーティング全体でスペイン語・英語・ポルトガル語の三言語相互同時通訳がつきますので、英語での質疑応答が可能でした。

LACNICにおいても、提案は事前にメーリングリスト（ML）に提出され、MLおよび実際の会議での議論を経て、コンセンサスを得るという大きな流れは、他のRIRにおけるIPアドレスポリシー策定プロセスと同じです。

今回の会議では、IPアドレスポリシーを議論する場として、1時間半のセッションが4日間にわたり、合計5セッション設けられました。そこで行われた議論の内容を、以下に報告いたします。

◆IPv4アドレス消費に関するパネルディスカッション

最近注目を浴びているIPv4アドレス在庫枯渇問題ですが、LACNICミーティングでも、この問題と議論の内容を紹介するパネルディスカッションが行われました。私もパネリストの一人として招かれ、最新のIPv4アドレス在庫枯渇予想や、この問題に対応するためのアドレスポリシーが、各地域で議論されていることなどを紹介しました。

パネリストと会場のいずれからも「IPv4アドレス在庫枯渇に対する長期的かつ根本的な解は、IPv6の利用である」というコメントが聞かれ、IPv6の普及に向けて、レジストリやコミュニティがやるべきことを早急に検討する必要がある、ということが確認されました。

◆ポリシー提案

今回のミーティングで議論された、IPアドレスポリシー提案の概要と結果を、以下にご紹介いたします。

●IPv4アドレス関連

(1) IPv4アドレスの在庫枯渇に向けたポリシー

前回のAPNICミーティング（APNIC23）、ARINミーティング（ARIN XIX）、RIPEミーティング（RIPE 54）で提案されたものと同じ内容で、以下の四つの要素からなるものです。

・IPv4アドレスの在庫枯渇に対しては世界的に調整の上、取り組みを進める
・延命のためのルール変更は行わない
・分配済みアドレスの回収は別の議論とする
・割り振り終了日を前もって決めた上で周知する

会場では、「割り振り終了日を決めてしまうと駆け込み申請が起きてしまうのではないか」「RIRに未割り振りア

ドレスがある限りは割り振りを続けるべき」などのコメントが出て、コンセンサスには至らずMLで継続議論することとなりました。

(2) IANAからRIRへのIPv4アドレスの最終割り振りに関するポリシー

IANAにおける/8の在庫が25個になった時点で、その25個を5個ずつ、五つのRIRへ割り振ってIANAからRIRへのIPv4割り振りを終了するという提案です。IANAからRIRへの割り振りポリシーは「グローバルポリシー」と呼ばれ、全RIRのミーティングでコンセンサスを得た後、さらにICANN理事会の承認を得る必要があります。

会場では、「25個もの/8を一度に割り振り切ってしまうのは乱暴ではないか」「一律に5個ずつではなく、人口比で分けてはどうか」等のコメントが出ましたが、細かい数値は他RIRの議論を反映して修正し、再度ミーティングでコンセンサスを得るものとする条件付きでコンセンサスとなり、45日間の最終コメント期間（Last Call）に付されることとなりました。その後、最終的にLACNICの理事会で承認されています。

メンバーミーティングの様子

(3) マルチキャストアドレスのRIRからの割り当て

現在、IANAで行っているマルチキャストアドレスの割り当てを、RIRから行うように変更するという提案です。賛否両論ありましたが、提案者が自ら、今後さらに議論することを望んだため、MLで継続議論されることとなりました。

●IPv6アドレス関連

(4) IPv6プロバイダ非依存（PI）アドレスの割り当て

IPv4のPIアドレス割り当て要件を満たしていれば、IPv6のPIアドレス（/48）についても、割り当てを受けることができるとする提案です。ARINやAPNICでは、既にPIアドレスの割り当てを認めるポリシーが施行されていますが、割り当ての要件をもう少し明確に記述する必要がある等のコメントが出てコンセンサスに至らず、MLでさらに議論することとなりました。

(5) IPv6アドレスにおける2回目の割り振り（初回の追加割り振り）を受ける要件の変更

IPv6アドレスの初期割り振りを受けた組織が、初めての追加割り振りを受けるとき、初期割り振りで受けたアドレスを6ヶ月以内に返却する場合に限り、追加割り振り要件ではなく、初期割り振りの要件を適用して、割り振りアドレスのサイズを決定する、という提案です。

現在のポリシーでは、それまでに受けた総アドレス量と同じだけのサイズが、追加割り振りとして割り振られますが、この提案では、より多くのアドレスの割り振りを受けることが可能となります。

この提案はコンセンサスに至り、その後LACNIC理事会で承認がなされています。

(6) 同一サイトへ複数の/48を割り当てる際の審議不要化

現在のポリシーでは、同一サイトへ複数の/48を割り当てる際には、RIR/NIRに対し審議申請を行うことを求めていますが、これを不要とする提案です。APNIC、ARINでは却下となった提案ですが、ミーティングでは特に反対は無くコンセンサスに至り、この提案もLACNIC理事会で承認されました。

(7) IPv6アドレスポリシー文書からの「暫定的」という言葉の削除

現在のポリシーでは「このポリシーは暫定的（Interim）であるものとしてみなされ、将来IPv6の運用に関するより幅広い経験に従って見直される」という記述がありますが、既にIPv6の運用の経験は十分蓄積されたとの理由で、この部分を削除するという提案です。先のARINミーティングではコンセンサスとなった提案ですが、今回のLACNICミーティングでもコンセンサスとなり、その後LACNIC理事会で承認されました。

(8) IPv6アドレス広報に関するポリシー変更

現在のポリシーでは、割り振りを受けたIPv6アドレスは、集成して一つのブロックとして広報することという記述がありますが、トラフィックコントロールのためにいくつかのブロックに分けて広報するニーズがあることから、この要件を削除しようとする提案です。

ミーティングでは、この要件の削除に関して否定的なコメントが複数なされたこともあり、MLで継続議論することとなりました。

(9) IPv6アドレス初期割り振り要件の変更

現在のポリシーではエンドサイトへの割り振りを認めていませんが、エンドサイト内で/48を割り当てる計画があれば、割り振りを認めるという提案です。

ミーティングでは特に反対も無くコンセンサスに至り、LACNIC理事会で承認されました。

(10) IPv6ユニークローカルアドレス割り当てに関する提案

現在、IETFでも議論されているIPv6ユニークローカルアドレスの割り当てを、RIRで行うという提案です。現時点では、このアドレスに関するRFC自体が成立していないこともあり、今後も継続して議論するという結論になっています。

●その他のポリシー

（11）IANAからRIRへのAS番号割り振りポリシー

このポリシーも「グローバルポリシー」として提案されているもので、IANAからRIRへは、1,024個単位でAS番号を割り振ることを定めるポリシーです。提案者からは、現在取られている割り振り方法を明文化するものだという説明があり、IANAの担当者からも同様のコメントがありました。

この提案に関しては特に反対のコメントは無く、コンセンサスとしてLast Callに付され、その後LACNIC理事会で承認されました。

LACNICミーティングは年一回開催のため、次回は2008年5月の開催（場所は未定）となります。

（JPNIC IP事業部 穂坂俊之）

2007.6.23→6.29 ICANNサンファン会議報告

［関連記事］ P.27 第19回ICANN報告会レポート

2007年6月23日から29日まで、サンファン（プエルトリコ）にて開催されたICANN会議に出席しました。

◇ ◇ ◇

◆ドメイン名登録者保護に関する議論

リスボン会議報告※1でお伝えしたように、米国のRegisterFly社がRAA（Registrar Accreditation Agreement:レジストラ認定契約）を解約された一件を受けて、コミュニティからは登録者保護に向けて契約の見直しをすべきとのコメントが多く寄せられました。そのため、ICANNではRAAの内容見直しやレジストラが所有するデータのエスクロー（第三者への預託）強化などについて議論されるようになりました。

本会期中には、登録者保護に関するワークショップが開催され、ICANNにおける登録者保護の取り組み状況が報告されるとともに、参加者からはフィードバックが寄せられました。

ICANNでは、既にエスクローエージェントの募集を行っており、7組織の応募があったこと、また7月初旬に選考を行うことが報告されました。登録者のデータを第三者に預託することについては、WHOISと同様にプライバシーの問題を指摘する人もいましたが、レジストラが機能しなくなった場合にタイムリーに登録者を救済する必要があるといった現実的な問題を考慮すると、現時点においてはエスクローが最も有効な方策と言えるのではないか、といったコメントがありました。

ICANNは引き続きコミュニティからのフィードバックを検討しつつ、レジストラ部会と協調してRAA改正案を作成し、パブリックコメントに付すこととなります。

◆ドメイン名テイスティング

ドメイン名テイスティングに関する課題レポート※2がICANNスタッフより提出され、本会議で議論されました。

GNSO内の課題解決にあたっては、多くの場合PDP（Policy Development Process:ポリシー策定プロセス）が実施されますが、本課題レポートではドメイン名テイスティングに関して、以下のような提案がなされています。

・PDPを開始する前には、さらなる事実調査を行うこと

・PDPがICANNやGNSOのスコープ内であるかどうかを確認すること

・PDP以外にも解決方法がないか検討すること

GNSO評議会では、GNSOメンバーとICANNスタッフでアドホックグループを結成して、ドメイン名テイスティングについてさらなる情報収集を行うこととし、その結果によってPDPを開始すべきかを判断することになりました。

※1 JPNIC News & Views vol.445 「ICANNリスボン会議報告」
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2007/vol445.html

※2 GNSO Issues Report on Domain Tasting - English
http://gnso.icann.org/issues/domain-tasting/gnso-domain-tasting-report-14jun07.pdf

Internet Topics インターネット・トピックス

ICANNサンファン会議報告

◆IPv6の実装に向けて

ASO（Address Supporting Organization:アドレス支持組織）より、最新のIPv4アドレスの割り振り予測が報告され、インターネットを継続して安定的に運営し、また今後も発展させていくためには、IPv6の実装を促進していく必要があるとの見解が述べられました。今後は、IPv4だけではなくIPv6でも到達できるシステムを構築する必要があると考えており、RIRは注意を喚起するとともに実装も促進していく意向にあることが伝えられました。

ASOはIPv6実装の必要性について啓発するようICANNに対して要請し、ICANNはRIRと協力してIPv6に関する教育活動やアウトリーチ活動を行っていくことを決議しました。

最終日に行われた理事会の様子

◆ICANN 2007年-2008年度予算案を承認

2007年-2008年度の予算案が、最終日の理事会で承認されました※3。翻訳費用を27万ドルから47万ドルに増額するなど、コミュニティからのフィードバックも反映された内容となっています。収入は4,937万3,000ドルを見込んでおり、昨年度に引き続き前年度比で45%増となります。

（JPNIC インターネット推進部 高山由香利）

※3 ICANN Posts Approved Version of the Proposed Fiscal Year 2008 Budget
http://www.icann.org/financials/adopted-budget-29jun07.pdf

Chicago, U.S.A.

2007.7.22→7.27

第69回IETF報告

■全体会議報告

2007年7月下旬に第69回IETFが開催されました。本稿では、全体概要とDNS関連WG、IPv6関連WG、セキュリティ関連WGについてのレポートをご紹介します。

◆はじめに

11時間半のフライトを経て、航空機はやや揺れながらシカゴ・オヘア空港に着陸しました。シカゴはミシガン湖から吹く風のため「Windy City（風の街）」と呼ばれているそうですが、そのためか湿度が高く、この時期の気候は東京の気候に近いように感じます。しかし、ループと呼ばれるダウンタウンの中心部には、ビルがひしめくように建っており、ビルの間を高架の電車が行き交う様子はシカゴ特有の情景と言えます。世界第三の高さを誇るシアーズタワーはシカゴのループ内にあります。

◆概要

第69回IETFは、2007年7月22日（日）から27日（金）にかけて、シカゴのPalmer House Hiltonというホテルで開催されました。このホテルのビルは歴史のある建物で、テラス付きのホールがあるなど内装が素晴らしい会場です。

今回のIETFの参加登録者数は1,146名で、前回より37名ほど増えました。前回と同様に約40ヶ国からの参加があり、内訳は第一位がアメリカ（45%）、第二位は日本（10%）、第三位はドイツ（4%）でした。その後はフランス（4%）、イギリス（3%）、韓国（3%）と続きます。今回も日曜日のチュートリアルから始まり、月曜日から金曜日までWGやBoFのミーティングがありました。水曜日と木曜日に、それぞれIETF Operations and Administration PlenaryとTechnical Plenaryが開かれました。Plenaryは参加者全員を対象とした全体会議です。

◆IETF Operations and Administration Plenary

IETF Operations and Administration Plenaryは、こちらも前回と同様、4日目の水曜日に行われました。このPlenaryは、IETFの活動全体や各ミーティングの運営に関する報告などが行われるミーティングです。

会場となったホテル、Palmer House Hiltonの外観

Internet Topics インターネット・トピックス

今回は、Russ Housley氏がIETFチェアに就任してから初めて行われるPlenaryです。アジェンダの構成には特に変更がなく、NOCのレポート、ホスト企業のプレゼンテーション、第69回IETFミーティングの概要、IESGのオープンマイク（会場から意見を挙げてもらって議論を行う時間）がありました。

NOCのレポートによると、今回のIETFミーティングでは、合計87台のアクセスポイントが使われて、参加者が行き来する1階、2階から6階までで無線LANが使えるようになっていました。会期中の同時利用ノード数は最大で748ありました。これは参加登録者数の65%にあたります。参加者の半数以上が同時に無線LANに接続しているカンファレンスは、他にはあまり例を見ないのではと思われます。近年のIETFでは、会議の資料をWebで閲覧できるようになっていることが関係しているかもしれません。

Administration Plenaryの様子

□ IETF 69 Preliminary & Interim Materials
https://datatracker.ietf.org/meeting/69/materials.html

ホストを行ったMotorola社からは、インターネットの昔と今を比べたプレゼンテーションが行われました。10年前は世界の携帯電話台数が約32万台であったのが、今や30億台に達しているそうです。ユーザーの接続部分である“エッジ”を提供しているMotorola社らしく、IETF参加者に向けて「Don't forget the Edge.」というメッセージが伝えられていました。

続いてRuss Housley氏からIETF活動状況の報告がありました。現在、約120のWGが活動しており、新たに436のドラフトが作成されました。またRFCは103発行されました。ここ1年のドキュメント数を比較してみましたが、WG数や新規ドラフト数には大きな変化はないようです。

	WG数	前回以降の新規ドラフト	前回以降の新規RFC
第69回IETF	120	436	103
第68回IETF	120	441	95
第67回IETF	120	440	104

他に、IAOC（IETF Administrative Oversight Committee）Webページの公開や、IETF ToolsのWebページにパスワード認証機能が付加されたことについてお知らせがありました。

□ IETF Administrative Support Activity （IASA）
http://iaoc.ietf.org/

□ IETF Tools
http://tools.ietf.org/
パスワード入手のためのページは、左側の「Get Password」というリンクから辿ることができます。

IESGオープンマイクは、参加者がIESGメンバーとIETFの運営等に関する議論を行う時間です。会場からは、IPv6 WGの活動が見られない、IPv6におけるNATの位置付けなどIPv6への移行について包括的に整理した文書が必要である、IETFの策定プロセスを改善する議論を継続する必要がある、といった意見が出されていました。

◆Technical Plenary

Technical Plenaryは5日目の木曜日に行われました。今回はOlaf Kolkman氏がIABチェアに就任してから初めてのTechnical Plenaryです。

今回は、IRTF活動報告とIAB活動報告の後に、恒例のテクニカルプレゼンテーションはなく、そのままオープンマイクの時間になりました。

IRTFの活動報告とIABの活動報告は比較的手短に終わりました。IRTFではここ3ヶ月の間にRFC4838を作成し、新たなドラフトの作成も行っているそうです。この報告では他に大きなトピックはありませんでした。

IABからは、ITUから送られてきた“Consultation on ITU Resolution 102”という活動のアンケートに対して回答したという報告がありました。これはIPアドレスやドメイン名などの管理に付随する、国際的かつパブリックなポリシーの策定に関するアンケート（問い合わせ）で、ITUメンバーの活動方針を検討するために使われるようです。IETFの活動を概説した回答がなされていました。

□ Response on “Consultation on Resolution 102”
http://www.iab.org/documents/correspondence/2007-05-21-itu-resolution-102.html

オープンマイクでは、まず今回のTechnical Plenaryで技術的なプレゼンテーションがなく、技術的な議題が明らかになっていないことに対する指摘から議論が始まり

ました。これに対しては、今回適切なスピーカーが見つからなかったというKolkman氏からの回答に留まりました。

この他には、IPv6におけるNATの位置付けを発端とする、End to Endの原則に関する議論が行われました。会場の参加者による呼びかけで挙手が行われ、自宅においてグローバルIPアドレスを使ってインターネットに接続しているユーザーは、NATもしくはNAPTを使って接続しているユーザーよりも少ないことがわかりました。この結果から、IPのレイヤーでは、End to Endの原則が成り立っていないのではという問いかけがありました。

これに対し、IABメンバーからは、IETFにおけるEnd to Endの原則は、技術の複雑化を避け、ネットワークの堅牢性を維持するために重要である、デザインゴールとしての原則であるといった反論がありました。続いて、ユーザーのPCにおいてファイアウォールをデフォルトで設定せざるを得ない状況や、IPv6アドレスが必要とされる場所についての意見交換等に繋がっていきました。ただし、議題の中心的なトピックが提示されなかったためか深い議論にはならず、ほぼ定刻通りにPlenaryが終了しました。

IABによるRouting & Addressing workshopやその報告を受けて、今の段階で必要とされる議論は多いと考えられます。次回以降のTechnical Plenaryでは、より活発な議論が行われることが望まれていると思われます。

◇　　◇　　◇

次回の第70回IETFミーティングは、2007年12月2日から7日にかけて、カナダのバンクーバーで開催される予定です。Plenaryで発表されたIASAの予算計画によると、ホスト企業が現れない場合、参加費の大幅な値上げが見込まれるようです。

（JPNIC 技術部 木村泰司）

■ DNS関連WG報告

◆dnsop WG（Domain Name System Operations WG）報告

今回のdnsop WGミーティングは、3時間枠にて行われました。まずはじめに、前回draftだったドキュメントの確認が行われました。draft-ietf-dnsop-serveridがRFC4892として発行されたことが報告されました。これによって、DNSサーバ個体のサーバIDを確認する手法が標準化されました。また、draft-huston-6to4-reverse-dnsがIESGレビューの段階にあり、draft-ietf-dnsop-reflectors-are-evilならびにdraft-ietf-dnsop-default-local-zonesが、WG Last Callにてコメントを受けた後の更新待ち状態であることが報告されました。

次に、draft-ietf-dnsop-as112-opsについての議論が行われました。前回のプラハでのミーティングならびにそれ以後の議論で、AS112が現在提供しているゾーン以外におけるゾーンのサービス提供や、IPv6トランスポートでのサービス提供についての意見が出されました。そこで、それらを文章に入れるかどうかの議論がなされました。結論としては、新たなものを盛り込むより、現在の運用を早くRFCとして発行するほうがいいだろう、という流れになりました。

さらに、draft-ietf-dnsop-respsizeに関しても、同様にEDNS0を文章に入れるかどうか議論がなされました。これも同様に、EDNS0まで話を広げずに、現状を早めにRFCとして発行し、EDNS0を含めたメッセージサイズの議論は別の文章にしたほうがいい、という意見が出されました。

今回一番議論が多くなされたのは、draft-ietf-dnsop-resolver-primingでした。これは、一部のDNS実装が行っているprimingという挙動を標準化する文章です。このprimingに関しての議論では、（1）ルートDNS サーバにIPv6トランスポートが提供され、AAAAレコードがhintファイルに追加された場合のprimingの挙動、（2）ルートゾーンにDNSSECが導入された場合のprimingの挙動、という2点について議論が行われました。特に（2）に関しては活発に議論が行われ、結論としてはpriming時にDNSSECのvalidationが行われても害は無いであろう、という方向になりました。

□ Domain Name System Operations（dnsop）Charter
http://www.ietf.org/html.charters/dnsop-charter.html

◆dnsext WG（DNS Extensions WG）に関連する動向

前回のプラハでのミーティングにて宣言された通り、dnsext WGのミーティングは行われませんでした。次回も行われる予定は無いようです。前回のミーティングからメーリングリストで行われた議論としては、主に次のものが挙げられます。

(1) DNAME update : DNSSECにてvalidationをする場合の挙動
(2) 2929bis update : Resource Records仕様の更新
(3) DNSSEC key rollover : DNSSEC鍵更新に関する問題点
(4) dnsext WGチャーター更新

なお、DNSSEC ExperimentsがRFC4955として、DNSSEC Opt-InがRFC4956として発行されました。DNSSECに関する文章はまだdraftのまま残っているものがあるため、引き続きメーリングリストにて議論されると思われます。

□ DNS Extensions（dnsext）Charter
http://www.ietf.org/html.charters/dnsext-charter.html

（JPNIC DNS運用健全化タスクフォースメンバー/東京大学 情報基盤センター 関谷勇司）

■ IPv6関連WG報告

本稿では、会期中に議論された、IPv6に関連したトピックスをいくつか紹介します。

◆dhc WG （Dynamic Host Configuration WG）

DHCP/DHCPv6の機構および新規オプションの定義に関する話題を扱う、dhc WGのミーティングは、月曜日朝一番目のコマで開催されました。今回のミーティングで大きな議論になったのは、"Extensions to DHCPv6 for prefix and default router information"というタイトルで報告された、DHCPv6の拡張に関する話題です。IPv6では、ネットワーク上に接続されているルータのIPアドレスを通知するために、ルータ広告（RA, Router Advertisement）メッセージを用いますが、設定ミスなどによりこのメッセージを不正に出してしまうノードが存在すると、IPv6通信が阻害されてしまいます。実際に、イベント会場などでこの問題はよく発生しています。また、故意にRAを送信し、他人のパケットを不正中継するなどといったことが可能になってしまうという問題もあります。この問題に対して、IPv4と同じく、ルータの情報をDHCPv6にて配布することで解決してはどうかという提案です。この提案に対しては、IPv6の基本仕様にまで影響することや、仮にDHCPv6を利用してルータ情報を配布したとしても、問題の完全な解決にはならないこと（DHCPサーバの認証が必要になる）、他にも取り得る方法（RAをセキュアにするプロトコルを使用するなど）が存在することから、DHCPv6でルータ情報を配布することに関しては、見送りとなりました。同じ話題が、v6ops WGでも議論されています。

□dhc WG
http://www.ietf.org/html.charters/dhc-charter.html

□第69回 IETF dhc WGのアジェンダ
http://www3.ietf.org/proceedings/07jul/agenda/dhc.html

◆v6ops WG（IPv6 Operations WG）

IPv6とIPv4の共存技術、IPv6のデプロイメントに関する話題を扱うv6ops WGのミーティングは、初日、午後一番目のコマにて開催されました。今回は、チェアより簡単に現在のWGドキュメントステータス（「RFCエディタに提示中」「AD預かり」「ワーキンググループラストコール（WGLC）終了」）の説明がありました。

その後、本題として主に、

(1) 始点アドレス選択
(2) CPE セキュリティに関する話題
(3) Teredo に関する話題
(4) DHCP に関する話題

の4項目について議論されました。

(1) については、問題提起に関するドラフト（draft-ietf-v6ops-addr-select-ps）と、解法に関する要求条件ドラフト（draft-ietf-v6ops-addr-select-req）が前回WGLCとなっており、筆者から、メーリングリストで受けたコメントの紹介、ドラフト改版案が提示されました。この2ドラフトについては特にコメントが無く、次のステップに進むことになりました。その後、始点アドレス選択問題の解法として、draft-arifumi-v6ops-addr-select-solドラフトについて、説明および議論が実施されました。解法については、「デプロイメントまで考えると、どの解法も実施困難である」「そもそもマルチプリフィクスは無用」「一つの解では全ての場合をカバーできないので場合に応じた解法が必要」といった意見が出されました。この解法ドラフトに関しては、WGアイテムとして取り上げるコンセンサスは得られず、継続議論となっています。

受付デスク(Registration Desk)の様子

（2）は、小規模オフィスやホームネットワーク環境での、CPEデバイスのあり方に関する議論です（draft-ietf-v6ops-cpe-simple-security）。IPv4のNATによるセキュリティの担保や、CPEへの穴あけプロトコル（UPnPなど）が、IPv6環境ではどのようにあるべきかについて、議論されました。ファイアウォールは必要無い、その理由として、「ファイアウォールの存在はIPv6にもNATを持ち込むことになってしまいかねない」「ホストがガードすべき」といった意見や、「実際にそのような環境で日々過ごしており、問題無い」といった意見が表明されました。議論は収束せず、ML上で継続議論を実施することになりました。

（3）は、Teredoのセキュリティに関する問題提起です。（draft-hoagland-v6ops-teredosecconcerns-01）Teredoは、NATを超えてIPv6 over IPv4トンネルを実現するプロトコルであり、Windows Vista等に標準で実装されています。Teredoを使うと、意図せずFirewall/NAT等をバイパスされてしまう可能性があることから、これがセキュリティリスクになり得ることを指摘しており、管理者は、「Teredoの使用を禁止する」「Teredoパケット（UDP）をフィルタする」等の方策を取ることを推奨しています。このドラフトは、WGアイテムとして議論されることになっています。

（4）は、同日午前中のdhc WGで議論されたものと同一のプレゼンテーションが実施されました。v6ops WGでは、解決策として、DHCPv6サーバの認証やSEND（RAをセキュア化するプロトコル）の利用をすべきであり、DHCPv6でルータ情報を配布することは問題を悪化させるだけである、という意見が主流を占めました。

□v6ops WG
http://www.ietf.org/html.charters/v6ops-charter.html
http://www.6bone.net/v6ops/

□第69回 IETF v6ops WG のアジェンダ
http://www3.ietf.org/proceedings/07jul/agenda/v6ops.txt

◆その他

全体会議報告で紹介した、IETF Operations and Administration Plenaryのレポートでも触れられていましたが、オンサイトミーティングを実施せず、既存IPv6仕様の標準化等のみを進めていくことになっていたIPv6 WG について、IPv6 WGとして活動が必要な話題が最近出てきていることもあり、次回のバンクーバーミーティングにて、新IPv6 WGのミーティングが実施されることになっています。現在のIPv6 WGはクローズし、新たにIPv6のメンテナンスのみを目的としたWGが設立される予定です。（既にミーティング中に、新たなWGが提案され、（IPv6 Maintenance Working Group（6man））取り組み内容について、議論が始まっています）

◆ram（rrg）

前回の第68回IETFミーティングでは、intareaセッションでID/Loc Separation BoFが開催され、デフォルトフリーゾーンにおけるルーティングスケーラビリティ問題について検討が行われたことは、前回報告した通りです。その後もram（Routing and Addressing）やrrg（Routing Research Group）といったメーリングリストで、ID/Loc分割に基づくさまざまな提案について議論が行われました。今回のIETFミーティングでは、最終日の金曜日に丸一日rrgのセッションを使って、主にramのメーリングリストで行われている提案について、発表や議論が行われました。

このルーティングスケーラビリティの問題は、IPv6のみに関係するものではなく、IPv4では既に問題が顕在化し始めています。IPv6ではIPv4に比べてさらに状況が悪化することも予想されており、現在そして今後のインターネットを占う重要なトピックであるといえます。

まずrrgのチェアであるTony Li氏から、設計目標についてのドラフトのアップデート状況について発表があった後、Lixia Zhang氏から解決アプローチの分類学について発表があり、IDとLocatorのマッピングの管理方法、通信障害の検出・使用方法について、各種方式の分析が行われました。

また、rrgということでリサーチグループよろしく、研究論文の紹介も2件ほど行われました。一つはケンタッキー大学からの発表で、階層化されたルーティングとフォワーディング方式により、スケーラビリティを高めるといった研究が提案されました。また、ベルギーのルーバンカトリック大学からは、ID/Loc分離を実際に行った場合の、IDとLocatorのマッピングキャッシュサイズや、マッピング解決に必要なトラフィック等のコストに関する研究が発表されました。コスト見積もりには、LISPと呼ばれるID/Loc 分離プロトコルを例に取り、大学ネットワークで観測されたユーザートラフィックとBGP経路表が用いられ、キャッシュのタイムアウト時間にも依存するものの、既存のDNSのような枠組みでマッピングシステムが実現可能であることなどが示されました。

本セッションのメインである、ID/Loc分離方式に関する議論では、大きく分けてLISPとSIX/Oneと呼ばれる方式が発表されました。LISPとは、Locator Identifier Separation Protocolの略で、通信を行うホストが位置するサイトのゲートウェイルータ（トンネルルータ）同士で、パケットのカプセル化/デカプセル化を行うことにより、ホストには一切変更を加えずにマルチホームを実現するというものです。サイト内で使うアドレスがIdentifier、トンネルルータに付与されパケットのカプセル化に用いられるアドレスがLocatorとして機能することになります。SIX/One方式は、これまでIETFのshim6ワーキンググループで検討されてきた、ホストによって実現されるマルチホーム方式であるshim6プロトコルをベースとし、途中のルータでパケットのアドレスフィールドを変更することを許容するというものです。これにより、shim6の弱点とされていた、ISPなどにおけるサイト管理者のポリシーを反映したマルチホームを行うことが可能となりますが、ホストのプロトコルスタックに変更を加えなければならないという点は変わりありません。これら以外にも、LISPの変更・拡張方式である、APT、LISP-CONS、

LISP-NERDなどの発表が行われ、活発な議論が行われました。

特に、LISP方式はramのメーリングリストでも最も注目を集めており、また実装も既に開始されるなど、IETFとしては非常に短いタイムスケールで実用化に向けた活動が行われているように思われます。今後、オペレーターコミュニティなどで意見を吸い上げ、いかに効果的で実用可能な方式を策定できるかが、成功のポイントになることでしょう。

□ 第69回IETF rrgのアジェンダ
http://www3.ietf.org/proceedings/07jul/agenda/RRG.html

□ 第69回IETF rrgの発表資料
https://datatracker.ietf.org/meeting/69/materials.html

第69回IETFミーティングの各種情報は、以下のURLより参照可能です。

□ 全体プログラム、WGアジェンダ、発表資料
https://datatracker.ietf.org/meeting/69/materials.html

□ 録音
http://videolab.uoregon.edu/events/ietf/

（JPNIC IPアドレス検討委員会メンバー/NTT情報流通プラットフォーム研究所 藤崎智宏）
（NTT情報流通プラットフォーム研究所 松本存史）

■ セキュリティ関連WG報告

第69回IETFでは、セキュリティエリアのセッションが18開かれました。そのうちの一つはBoFでした。本稿では、PKI（Public-Key Infrastructure）と、リソース証明書に関連するWG、並びにTAM（Trust Anchor Management）BoFについて、お送りいたします。

◆PKIX WG（Public-Key Infrastructure（X.509））

PKIX WGのミーティングは、5日目の2007年7月26日（木）に行われました。PKIX WGは、電子的な認証基盤の規格であるITU-TのX.509をインターネットに適用して、新たな規格作りを行っているWGです。アジェンダが多くなりがちなPKIX WGにしては1時間と短く、最後に行われたWebDAVを使ったデモは、unofficial PKIX WGという位置付けで、休憩時間を割いて行われました。

最初はドキュメント策定状況の確認です。メッセージの簡略化等を図ったLightweight OCSPと、subjectAltName拡張フィールドにホスト名やプロトコル名等を入れる仕様のService Name SANは、IESGよりRFC化の承認を得ました。現在、RFC Editorの処理待ちです。オンラインの証明書検証プロトコルであるSCVP（Server-based Certificate Validation Protocol）と、RFC3280の改良版（RFC3280bis）、それからCMC（Certificate Management over CMS）に関わる三つのドキュメント（下記）は、IESGのレビューを受けている最中です。

□ Certificate Management Messages over CMS
draft-ietf-pkix-2797-bis-04.txt

□ Certificate Management over CMS（CMC） Transport Protocols
draft-ietf-pkix-cmc-trans-05.txt

□ CMC Complience Document
draft-ietf-pkix-cmc-compl-03.txt

いよいよRFC3280bisがIESGのレビューに入りました。Certification PathBuilding（RFC4158）やAuthority Information Access Certificate Revocation List Extension（RFC4325）など、ドキュメントは別々になっていますが、各々のRFC化が済んでおり、証明書とCRL（Certificate Revocation List）の処理に関する基本的な仕様が、ある程度固まる時期が来つつあるのかも知れません。

SCEP（Simple Certificate Enrollment Protocol）については、会場で若干議論がありました。SCEPは、いくつもの商用のソフトウェア等で利用されている、証明書の申請等のメッセージをやり取りするためのプロトコルですが、これまではWGにおけるRFC化が積極的に進められていませんでした。これはCMCという機能的に似ていながら、異なるデザインのプロトコルがあったためだと考えられますが、SCEPを使ったプログラムが普及しつつあることはRFC化の大きな推進理由となります。結局Informational RFCを目指して進められることになりました。

今回の新たな話題として、PKI Disaster Recovery and Key Rolloverと、WebDAV for certificate publication and revocationの二つをご紹介します。これらはWG後半、Related Specificationsの時間に、プレゼンテーションが行われました。

PKI Disaster Recovery and Key Rolloverは、実は今回新しく提案されたものではなく、2001年の7月に一度作られたことのあるドキュメントです。その時のタイトルは、“PKI Disaster Planning and Recovery”だったそうです。今回Joel Kazin氏によって再編集されたこのドキュメントは、プライベート鍵の危殆化や喪失といった、例外的な状況から正常な運用に復旧する方法が書かれています。主にCPS（Certificate Practice Statement）を記述したり、PKIに関するディザスターリカバリープランを立てるために役立つ、Informational RFCにすることが目指されています。記述されているディザスターリカバリーの対象は、エンドエンティティ、認証局、Revocation Authority、Attribute Authority、タイムスタンプ局（Time-stamp Authority）です。プライベート鍵の危殆化や喪失の他には、CRLのリポジトリに対するDoS（Denial of Services）攻撃や、認証局のキーロールオーバー（鍵の更新）についても言及されています。

クイックに復旧するという言葉から想像されるような、特殊な手法が提案されているわけではありませんが、復旧手段が網羅的にまとめられています。認証局の運用や設計をされる方には、とても参考になるドキュメントに

なっていくと思われます。

□ PKI Disaster Recovery and Key Rollover
draft-pinkas-pkix-pki-dr-kr-00.txt

WebDAV for certificate publication and revocationは、証明書やCRLのリポジトリへのアクセスに、WebDAVを使う手法の提案です。リポジトリにアクセスするためのプロトコルにはLDAP（Lightweight Directory Access Protocol）がありますが、LDAPはファイアウォールで遮断されがちであったり、証明書やCRLの内容を使った、証明書データやCRLデータの検索ができなかったりします。この提案は、HTTPやURIのデザインに影響しているREST（Representational State Transfer）の考え方を取り入れ、WebDAVを使った証明書データやCRLデータの取得や格納、さらに発行や失効手続きとの関連する処理等について提案しています。

□ Representational State Transfer （REST）
「Architectural Styles and the Design of Network-based Software Architectures」の第5章
http://roy.gbiv.com/pubs/dissertation/rest_arch_style.htm

この手法を用いると、証明書やCRLのURLは以下のように示されます。

https://dns.name/c=jp/o=NIR%20in%20Japan/cn=Taiji%20Kimura/
サーバdns.nameにあるC=jp, O=NIR in Japan, CN=Taiji KimuraというCNが入った証明書データ

https://dns.name/c=jp/o=NIR%20in%20Japan/cn=CRLs/
サーバdns.nameにあるC=jp, O=NIR in JapanによるCRLの全て（シリアル番号が一つ一つ入った形のCRLが使われる）

会場では、リソース証明書にも適用できるように、名前を示す文字列として鍵のハッシュ値が扱えるようにして欲しい、といった意見交換が行われていました。

今回ご紹介した二つのドキュメントの他にも、PRDP（PKI Resource Discovery Protocol）などの新しい作業項目が加わりました。まだまだPKIX WGの活動は続きそうです。

◆SIDR WG（Secure Inter-Domain Routing WG）

SIDR WGは5日目の朝、9時から10時45分まで行われました。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です。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ました。

現在、SIDR WGで行われている議論は大きく分けて三つあります。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す。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ます。三つ目は、ROA（Route Origination Authorization）の書式と取り扱いに関する議論です。

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ります。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ります。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に対応しません。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います。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りました。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、書式上認められるのか」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す。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したが、大幅に遅れてしまっているようです。ちなみに、4バイトAS番号については既に対応済みです。

□ An Infrastructure to Support Secure Internet Routing
draft-ietf-sidr-arch-01.txt

CPとCPSについては、本ドキュメントの策定における、時間的な制約に関する議論が行われました。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りますが、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を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す。議論の結果、今後、ドキュメントの位置付けを明確化することが課題になりました。

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ました。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ましたが、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ました。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りました。

□ 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りました。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す。これは、リソース証明書のトラストアンカー（trust anchor - 信頼点）として何を想定すべきか、という議論に発展しました。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、ユーザー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、手続きは簡単です。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ります。しかし、現在のIANAが

果たすとされている機能の中に、認証局が定義されておらず、RIRの認証局で対応せざるを得ないのが現状であるようです。

◆TAM BoF（Trust Anchor Management BoF）

電子証明書がVPNの機器等で使われるようになるにつれ、証明書検証で使われるトラストアンカーとなる認証局証明書を管理することの重要性は、一層増してきています。TAMは、Webブラウザや電子証明書の技術を使うVPN機器等にある、トラストアンカー証明書を格納する領域をモデル化して「トラストアンカーストア」と呼び、トラストアンカーの取り扱いが標準化されていない状況を改善する目的で開かれました。TAMは第69回IETFの最終日である7月27日（金）の午前に行われたにも関わらず、70名以上の参加者がありました。

はじめに、トラストアンカーに関する課題点をまとめたCarl Wallace氏から、課題点と解決策のあり方に関するプレゼンテーションが行われました。

目標

- トラストアンカーストアを管理するプロトコルを標準化する（トラストアンカー証明書の追加／削除／検索）
- out-of-bandの信頼メカニズムへの依存を減らす機能要件
- トランスポート（伝送路）との独立
- トラストアンカーをユーザーが意識しない、または意識させないデバイスなどをサポート

など

Carl Wallace氏がまとめたドキュメントを以下に示します。

□ Trust Anchor Management Problem Statement
draft-wallace-ta-mgmt-problem-statement-01

会場では、Webブラウザをこの議論に含めるべきかどうかについて、意見交換が行われました。また、リソース証明書における、この議論の重要性に関する指摘もありました。しかし、このBoFをWGにするかどうかは決まらず、MLを通じてこの議論の目的と意義を議論することになりました。その後、状況に応じて趣意書を作ることになりそうです。

◇　　◇　　◇

IETFチェアにRuss Housley氏が、そしてセキュリティエリアのエリアディレクターにTim Polk氏が就任し、PKIX WGでお会いしていた方々が、IETF全体で活躍されるようになりました。また、IABチェアには、RIPEミーティングでいつもユーモラスなプレゼンテーションをされていた、Olaf Kolkman氏が就任されました。

私にはIETFが少し身近に感じられる一方、彼らが発言の度に慎重に言葉を選び、そしてミーティング中も忙しそうにされている様子が、少し気の毒に思えます。今の私には、体調を崩されないよう応援する以外にできることが少なそうです。

（JPNIC 技術部 木村泰司）

会議の初日には恒例のレセプションが行われました。