2008.5.5▶5.9

第56回RIPEミーティング報告

■ 全体会議報告

IPv4アドレスの在庫枯渇が徐々に近づいており、RIPEミーティングでも、IPv6アドレスの利用状況に関するディスカッションが増えてきました。また経路ハイジャックなどの話題も大きく取り上げられています。

第56回RIPEミーティングは、2008年5月5日（月）～9日（金）にかけて、ドイツのベルリンで行われました。ベルリンと言えば、ベルリンの壁を思い起こさせますが、今では道路や地下鉄が西側と東側にまたがっており、私が滞在中に見た限りでは、都市の西側が壁で囲まれていたという当時の様子はわかりませんでした。しかしヨーロッパ地域の人にとってのベルリンは、冷戦の悲劇を身近な出来事として思い出させる場所であるようです。ミーティング参加者と夕食を取った際、話が市内の様子に及ぶと、多くの人は真顔になり、チェックポイント・チャーリー※1などが話題に挙がりました。ベルリンの壁が崩壊したのは、1989年ですので、ミーティング参加者のほとんどが崩壊の顛末を実際に見たり聞いたりしているはずです。

今回の参加登録者の総数は、430名でした。ドイツからの参加者が最も多く、このうちの30%を占めていました。その次がアメリカ（12%）、続いてイギリス（7%）です。日本からの参加者は7名でした。

■ 会議では“scribe”（文字サービス）が提供されました

RIPEミーティングのセッションは、前半はPlenary（全体会議）、後半はWG（Working Group）ミーティングという構成になっています。WGにはAddress Policy WG、Database WG、Routing WG、Anti-spam WGなどがあり、後半は二つの会場で並行してWGミーティングが行われます。今回のPlenaryは、特にIPv6の利用と、インターネット経路制御の話題が多かったように思います。

◆Plenary

RIPE NCCには、インターネット経路制御の情報の蓄積と分析を行うRIS（Routing Information Service）と呼ばれるサービスがあります。今回のPlenaryでは、RISを使って行われた二つの分析に関する報告が行われていました。

一つ目は、2008年1月末にエジプト近辺で起こった海底ケーブルの障害です※2。この障害は、ケーブルの切断や損傷による通信障害で、障害発生から11日後の2月11日未明に修復されました。RIPE NCCでは、蓄積されているインターネット経路制御の情報を使って、インターネットのASパスなどの分析を行いました。その結果、11日間まったく経路情報が届いていなかったASがあったことがわかりました。経路情報が届いていないということは、接続性がまったくなくなっていた可能性が高いと言えます。その他、バングラデシュでは、障害の起こっている経路を使わないシンガポールや香港を経由する経路への変更が起こっていたことがわかりました。これらの様子はBGPlay※3というツールにより、アニメーションで見ることができました。

BGPlayは、二つ目の報告でも使われています。この報告は、2008年2月末にパキスタンで起こった経路ハイジャックの時、インターネットの経路に何が起こっていたのかをわかりやすく示したものです。経路ハイジャックの起こっていた2時間に、YouTube側でmore specific routeを流す対策を取った様子などがわかりました。最後に、経路ハイジャック問題への対策は、IRRとroute filteringを使うことであると締めくくられました。

□Mediterranean Fibre Cable Cut - a RIPE NCC Analysis
http://www.ripe.net/projects/reports/2008cable-cut/index.html

□YouTube Hijacking: A RIPE NCC RIS case study
http://www.ripe.net/news/study-youtube-hijacking.html

5月7日（水）のPlenaryでは、インターネットへの接続がIPv6だけで行われる“V4 switch off”という時間が設けられました。会場でIPv4を使えないようにすることで、どのような問題が起こるのかを調べることが目的です。会場での挙手の結果、初めてIPv6を利用した人は少なかったにもかかわらず、インターネットにうまく繋げなかった人は多い様子でした。会場からは、端末側でIPv4を無効にするとIPv6も使えなくなった、無線LANのアクセスポイントが不安定だった、といった意見が出されており、会場のネットワークにも改善の余地があったようです。ちなみに、日本ではIPv6を利用する上での不備を解消するため、v6fix※4と呼ばれる活動が、2005年頃にWIDEプロジェクトで行われていました。

■ インターネットへの接続がIPv6だけで行われる“V4 switch off”のお知らせ

この他に、IPv6とIPv4の経路表から見た傾向や、ルータのFIBエントリの数を減らす技術などに関するプレゼンテーションが行われていました。アジェンダは、以下のWebページで参照することができます。

□RIPE 56 Meeting （Agenda）
http://www.ripe.net/ripe/meetings/ripe-56/agendas/

◇　　◇　　◇

年に2回行われるRIPEミーティングのうち1回は、通常、オランダのアムステルダムのKrasnapolskyホテルで行われます。RIPE NCCのスタッフの話によると、今年はアムステルダムの同ホテルで内装工事が行われており、今年度は2回ともアムステルダム以外で開催されるようです。Krasnapolskyホテルは、RIPE NCCのオフィスのそばにあるので、ミーティングの開催にあたっては何かと便利だと思いますが、離れた場所では、限られた人数で行わなければならない中で、なかなか大変そうでした。

（JPNIC 技術部/インターネット推進部 木村泰司）

※1 チェックポイント・チャーリー
「チャーリー」はNATOのフォネティックコードで「C」を意味するコードで、ベルリンが分割統治されていた時代に、当時設置されていたA～Dまでの外国人が通行可能な四つの国境検問所のうちの一つです。この検問所はアメリカ合衆国統治地区とソビエト連邦統治地区の境界線上に設置されていて、冷戦時代はベルリンの壁と並んで東西分断の象徴的存在でした。

※2 JPNIC News & Views vol.531「第25回APNICオープンポリシーミーティングレポート ～APOPSレポート～」
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2008/vol531.html

※3 BGPlay - graphical visualisation of BGP updates
http://bgplay.routeviews.org/bgplay/

※4 IPv6 Fix
http://v6fix.net/docs/v6fix.html.ja

■ RIPE NCCにおけるセキュリティ動向

◆概要

第56回RIPEミーティングでは、RIPE NCCのリソース証明書※1に関して大きな動きがありました。RIPE NCCでリソース証明書に関わる検討を行ってきたCA-TF（Certification Task Force）から、1年後の第57回RIPEミーティングまでに、リソース証明書をproductionレベルのサービスとして提供できるように準備するという発表があったのです。

これまでRIPE NCCは、APNICやARINの開発プロジェクトに参加しつつ、リソース証明書の影響範囲などの検討をしてきましたが、いよいよリソース証明書を“発行するため”の検討に入りました。さらに、RIPEにおけるリソース証明書発行の考え方をまとめたポリシー提案も行われています。

本稿では、RIPE NCCにおけるリソース証明書の動向とともに、IRR関連の話題についても報告したいと思います。

◆RIPE NCCにおけるリソース証明書の意義

リソース証明書はIETFのPKIX WGとSIDR WGで提案され、APNICが中心となって開発が行われてきました。今回のPlenaryでは、このようにRIPE以外で提案や実装が行われてきたリソース証明書に対して、RIPE NCCとして取り組む意義が明確化されました。その内容から、RIPE NCCのメンバーに対するサービスの一環として位置づけられていることがわかります。Plenaryで紹介された、RIPE NCCとしての意義を、次に示します。

■ 会場に設置されたターミナルルームの様子

A. メンバーにとってのリソース証明書は、第三者に対する割り振りの証明である。
B. RIRの間でリソース移管を可能にする標準技術になりうる。
C. リソース証明書自体による資源の確認を可能にする。
D. 将来的に経路制御のセキュリティに役立つ。

Aに関する説明の中で、リソース証明書の使い方が示されました。RIPE NCCのLIRであるアドレスホルダー（アドレスの割り振りを受けたもの）が、そのアドレスの割り当て先を、インターネットに接続できるようにするときの使い方です。アドレスホルダーが経路制御を行うISPに対してリソース証明書を提示することで、IPアドレスの正しい割り振り先であることを示します。

Bは、APNICやARIN、AfriNICなど、複数のRIRでリソース証明書の検討が進んでいることから、RIR間のリソースの移管を行うための技術として、標準的な位置づけになるであろう、という考え方があるようです。

Cは、他のRIRであまり明文化されていないことですが、あるアドレスが本当にそのネットワークに割り振られているものであるかどうかを確認する手段としてリソース証明書を主として使う、というものです。IPアドレスの割り振り/割り当てに関する専門知識とRIRのWHOISを駆使しなくても、証明書が有効かどうかをチェックするだけで、任意のIPアドレスが正しい割り振りであるかどうかがわかる、ということです。WHOISの情報が最新かどうかわからないような場合、例えば再々割り振りが行われていても、証明書さえあれば正しいかどうかがわかることになります。

Dは、IETFのSIDR WG※2で提案されているROA（Route Origination Authorization）オブジェクトの生成に利用できるという点です。ROAは、アドレスホルダーが特定のASに対して「当該アドレスの経路制御を認可する」という意味を持っている、電子署名つきのデータです。リソース証明書を持つものだけが正しいROAを発行できるため、ルータがROAを検証できるようになると、不正なアドレスを経路広告するようなタイプの経路ハイジャックを、ルータで検知できることになります。

◆RIPE NCCにおけるリソース証明書の現状と今後

リソース証明書を実際に発行してみることができる、テストプログラムの提供が2008年5月から開始されています。これは、RIPE NCCにおけるWebベースの申請システムである、“LIR Portal”の中で使えるものです。発表資料によると、リソース証明書の他に、ROAを発行する機能も持っています。

このテストプログラムは、今後、希望者に対して2008年9月まで提供され、毎月操作を行ってもらいつつ、フィードバックを反映していくような活動が行われる模様です。

また3日目のAddress Policy WGでは、“Initial Certification Policy Proposal”と題してCA-TFから発表があり、申請を行ったLIRや、PAに対してリソース証明書が発行されること、一つのLIRには複数のプリフィクスが入った一つのリソース証明書が発行されることなどが提案されていました。会場では、証明書の有効期限が切れるとBGPで経路情報が伝達されなくなってしまうのかといった、ISPにおけるリソース証明書への依存度合いに関する議論が行われていました。今後、PIホルダー（プロバイダ非依存アドレスの割り当て先）に関する追記などを行い、正式なポリシー提案が行われる模様です。

◆RIPE NCCにおけるIRRの関連動向

Plenaryの最初に、リソース証明書とIRRを結びつける、興味深いポリシー提案がありました。これはPolicy Proposal 2008-04※3で、ROAに基づいたrouteオブジェクトが登録される、新しいIRRを立ち上げる提案です。

Policy Proposal 2008-04では、IRRの更新業務におけるセキュリティが確保されておらず、登録される情報の信頼性が低いという問題が指摘されています。そこで新たに別のIRRを構築し、リソース証明書の業務スキームを用いて、発行されたROAをrouteオブジェクトとして登録し、既存のIRRと同様のツールで使えるようにすることが提案されています。今回は会場での議論はほとんどなく、今後は、Routing WGで議論が継続されます。発案者のRuediger Volk氏によると、この新たなIRRに、リソース証明書に基づいたinetnumオブジェクトやinet6numオブジェクトを登録することは、今のところ考えていないようです。あくまで正しいrouteオブジェクトを、既存のツールが使えるIRRで提供することを考えている、とのことでした。

この他に4日目のDatabase WGで、エヌ・ティ・ティ・コミュニケーションズ株式会社の白崎泰弘氏によって、RIPE NCCのDatabaseソフトウェア（RIPE Database Server※4）の信頼性を向上させる改良に関する発表が行われていました。発表資料によると、同社では、RIPE Database Serverを用いて、IRRデータベースを複数拠点に分散化するシステムの開発が行われています。複数のデータベースクラスターで同期を取るためのモジュールを開発したり、ダウンタイムの最小化やSQL文の最適化などを行ったりした結果が報告されました。今後、このプログラムコード（パッチ）は、RIPE NCCに提供されるそうです。

◇　　◇　　◇

RIS※5のページが面白くなっています。インターネットの経路情報に関する可視化ツールが増えてきました。経路広告の統計情報を一つのページで見せるAS dashboardは、まだテスト段階のようですが、自分のASや気になるASの歴史を簡単に知ることができます。P.22の全体会議報告で紹介したBGPlayやMyASNは、RISのToolsにリンクがあります。

MyASNといえば、JPNICでも経路ハイジャック情報通知※6の実験が始まりました。AS番号をお持ちの方は両方試されてみてはいかがでしょうか。

次回の第57回RIPEミーティングは、2008年10月26日～30日にかけて、アラブ首長国連邦のドバイで行われる予定です。

（JPNIC 技術部/インターネット推進部 木村泰司）

※1 リソース証明書
IPアドレスとAS番号の利用権利を示す電子証明書で、2004年6月に発行されたRFC3779でその構造が提案されています。
RFC3779 “X.509 Extensions for IP Addresses and AS Identifiers”
http://www.ietf.org/rfc/rfc3779.txt

※2 IETF SIDR WG
http://www.ietf.org/html.charters/sidr-charter.html

※3 RIPE Policy Proposal 2008-04
http://www.ripe.net/ripe/policies/proposals/2008-04.html

※4 RIPE Database Server
http://www.ripe.net/db/cvs-bugzilla.html

※5 Routing Information Service（RIS）
http://www.ripe.net/projects/ris/

※6 Telecom-ISAC Japan 経路奉行とJPIRR間の連携実験について
http://www.nic.ad.jp/ja/ip/irr/jpirr_exp.html

2008.6.23▶6.26

ICANNパリ会議報告

［関連記事］　P.18「第22回ICANN報告会レポート」

フランスのパリにて、2008年6月23日から26日に開催されたICANN会議に出席しました。

本稿では、今回の会議における主要トピックのうち、ポリシー策定プロセス（PDP）※1からポリシー実装のフェーズに移った新gTLDの導入およびドメイン名テイスティングの件と、2008年度運営計画案・予算案の承認についてご報告します。

◇　　◇　　◇

◆新gTLD導入に関するPDP

GNSO※2評議会が作成した、新gTLD導入に際しての原則、ポリシー勧告、実装に関するガイドライン等を含む、新gTLD導入に関する最終報告書※3は、2007年9月6日のGNSO評議会にて3分の2以上の賛成を要する特別多数で採択され、その後理事会に提出されていました。しかしながら、2007年11月のロサンゼルス会議でも、2008年2月のニューデリー会議でも、理事会は勧告の内容を実装するにあたっての課題や方策等を検討するようICANNスタッフに要請するのみに留まり、勧告の採択は見送られていました。

GNSOの勧告には、ICANNのミッションである技術的な内容のみならず、倫理的、政治的な判断を要する内容等も含まれていたため、ICANNスタッフの検討にも理事会の判断にも時間を要したことが、理事会により採択が見送られてきた理由であるように推察されます。

ICANNスタッフによる検討の結果、GNSOの勧告は実装可能であると判断され、今回のパリ会議において、理事会により勧告が承認されるに至りました。2005年12月に開始された新gTLD導入に関するポリシー策定プロセスは、理事会の勧告承認をもって終息しました。確かに、理事会がGNSOの勧告を採択したことは、新gTLD導入において一歩前進と言えますが、ポリシー実装に向けて詳細を詰め、具体的な実装計画に落とし込んでいくのはこれからです。これらの背景や今後の展開等については、P.28「TLD新設についての誤解」で

取り上げていますので、あわせてご覧ください。

今回の会議でICANNスタッフより説明があった“New gTLD Implementation Model”※4によれば、パリ会議の時点でICANNが想定している新gTLD実装のスケジュールは次のようになっています。

2008年第4四半期：ドラフトRFPの公開
（3～4ヶ月間）：意見募集期間やドラフトRFP修正期間を経て、理事会が最終RFPを承認
2009年第1四半期：最終RFPの公開
この後、新gTLD導入プロセスに関する公示期間を少なくとも4ヶ月設ける
2009年第2四半期頃：申請受け付け開始

このスケジュールは、2008年2月のニューデリー会議で説明されたスケジュールよりも、全体的に3～4ヶ月程度繰り下げられています。今後ICANNスタッフにより実装計画が策定されるわけですが、その実装計画は新gTLD導入プロセスの開始前に、コミュニティからの意見募集に付され、理事会により承認される必要があります。ICANNスタッフによる実装計画の策定はもとより、理事会承認を得るまでの過程でも時間を要することが予想され、今後もスケジュールが変更される可能性は大いにあると考えられます。

◆ドメイン名テイスティングへの対応に関するPDP

ドメイン名テイスティング※5は、登録猶予期間（AGP：Add-Grace Period）※6の仕組みを利用して行われることから、AGPの運用方法について議論が行われてきていました。2008年4月25日に、GNSO評議会がICANN理事会に提出したドメイン名テイスティングに関する勧告でも、AGPについて提案を行いました。内容は、「AGPを実装しているgTLDレジストリは、AGPの期間に削除されるドメイン名が、新規の月間ドメイン名登録総数の10%もしくは50ドメイン名のどちらか多い方を超えた場合、超えた分についてレジストラに返金を行わないようにする。ただし、特殊な状況については、それが証明できれば例外も認められる。」というものです。

時期が前後しますが、NeuStar社（.biz）とAfilias社（.info）からも、レジストリ契約のAGPに関する条項の修正提案が2008年2月5日にICANNに提出され、2月下旬から3月下旬までの意見募集期間を経て、2008年3月27日の理事会で承認されています。GNSO評議会では、両社の提案を参考に検討を進めていたこともあり、AGP期間中に削除されるドメイン名のうち、課金が猶予されるドメイン名数の上限は上記GNSOの勧告と同様です。

いずれの提案も、タイプミスの修正といった本来の目的にAdd-Grace Periodが利用されることを考慮し、一定割合の削除件数を許容する内容となっています。

パリ会議最終日の理事会では、GNSOの勧告が採択され、今後はポリシー実装のフェーズに入ります。AGPへの制限には、反対を唱えるレジストリ、レジストラもあったようですが、2007年11月のロサンゼルス会議でPDPが開始されてから1年足らずで、ポリシー策定が完了したことになります。

◆2008年-2009年度運営計画案・予算案の承認

2008年-2009年度の予算案が、最終日の理事会で承認されました※7。収入は、ドメイン名テイスティングに関する前項でお伝えしたように、AGPに制限を設けることを前提として試算されています。また、支出面では、新gTLDおよびIDN関連予算として862万7,000ドル（前年度比485万4,000ドル増）を見積もっており、今までにも増して精力的に活動を行っていこうとする意向がうかがえる内容です。収入は6,067万4,000ドル（前年度比20.5%増）、支出は5,712万9,000ドル（前年度比34%増）を見込んでおり、収支ともに引き続き増加傾向にあります。

（JPNIC インターネット推進部 高山由香利）

■ 最終日に開かれた理事会の様子

※1 ポリシー策定プロセス（PDP:Policy Development Process）
ICANNの役割の一つに、インターネットの各種資源の調整業務に関連するポリシー策定があり、このポリシー策定のための一連の流れをポリシー策定プロセス（PDP）と呼んでいます。ICANN改革を受けて改定された新付属定款には、プロセスの詳細が明確に規定されています。

※2 分野別ドメイン名支持組織（GNSO:Generic Names Supporting Organization）
ICANNの基本構造となる三つの支持組織（Supporting Organization：SO）の一つであり、分野別トップレベルドメイン（generic Top Level Domain：gTLD）に関するポリシーを策定し、ICANN理事会への勧告を行う役割を負っています。

※3 “Final Report Introduction of New Generic Top-Level Domains” 8 August 2007
http://gnso.icann.org/issues/new-gtlds/pdp-dec05-fr-parta-08aug07.htm

※4 “New gTLD Implementation Model”
https://par.icann.org/files/paris/gTLDUpdateParis-23jun08.pdf

※5 ドメイン名テイスティング
Webサイト上に設置したオンライン広告などからより多くの収入を得ることなどを目的として、よりトラフィックの多いドメイン名を選別するために、ドメイン名を一度に大量に登録し、ある程度のアクセス数を持つ少数のドメイン名を残してあとは全て登録猶予期間内に登録を取り消す行為です。

※6 Add Grace Period（登録猶予期間）
登録者がドメイン名を登録してからすぐ（5日以内）にその登録を取り消して手続きを行えば、登録料が不要となる仕組みで、ユーザーの勘違いや手続き上のミスなどが原因で意図しないドメイン名が登録され、そのドメイン名に課金されることで、ユーザーが不利益を被ることを避けるために導入されています。

※7 Fiscal Year 2008-2009 Operating Plan and Budget
http://www.icann.org/en/financials/proposed-opplan-budget-v3-fy09-25jun08-en.pdf

TLD新設についての誤解

2008年6月下旬、トップレベルドメイン（TLD）新設の話題が、いくつかのニュース媒体でかなりセンセーショナルに取り上げられました。中には「.ibm」とか「.love」、あるいは「.berlin」、果ては「.maruyama」のような個人名を付けたTLDまで、誰でも申請できて好きなドメイン名を登録できる、というような書きぶりのニュースまで見られました。発端はICANNパリ会議（2008年6月23日～26日開催）における議論と、それに関するICANN側の報道発表（6月26日）[※1]にあると思われますが、多くの報道にはかなりの誤解があると言わざるを得ません。どのような誤解があるのか、本稿で述べてみたいと思います。

ご存知の方も多いと思いますが、ICANNの設立（1998年10月）には、1996年頃から高まったTLDの新設を要求する声に応える必要があった、という事情が深く関係しています。そのため、TLDの新設は、設立以来ずっとICANNの最重要課題でした。これまで2000年開始の第一ラウンド、2003年開始の第二ラウンドで合計13個のTLDが新設されました。ここで言うTLDはgTLD（Generic Top Level Domain：次頁「gTLDの訳語について」参照）と呼ばれるものですが、2回のラウンドとも、新しいgTLDの登録事業（レジストリ）の運用を希望する組織が、申請書をICANNに提出して審査が行われ、適切と認められれば申請した文字列のTLDが新設されて申請者に運用が許可される、というプロセスでした。そして今、これまでの経験を踏まえて、第三ラウンド以後に適用される申請プロセス、具体的には申請の仕方とか申請書類の審査方法の検討が行われています。

誤解の第一は、多くの報道がICANNがTLD新設のための規則改正を「承認した」と言っている部分です。事実は申請プロセスの検討が一歩進んだ、というに過ぎません。申請の仕方とか書類審査の判断基準は、言わばgTLD新設のルールですから、これまでとは違う申請プロセスがもし決定されれば、それを「gTLD新設の規則を改正」と呼ぶことは言葉として適切ですが、事実はまだ検討中であって決定してはいません。

では、この点についてICANNパリ会議最終日の理事会決定はどのようなものだったのでしょうか。申請プロセスの検討は、2007年9月7日付で出されたGNSO評議会から理事会へのポリシー勧告に基づいて、ICANNスタッフ（事務局）が行ってきました。理事会決議ではまずこの勧告に関して、

> 決議［2008.06.26.02］
> 新gTLDコミュニティの支持と、新gTLDの追加は実現可能であるとするスタッフの助言に基づき、理事会はGNSO評議会のポリシー勧告を受け入れる。

とし、さらに

> 決議［2008.06.26.03］
> 理事会はICANNスタッフに対して、申請プロセスの詳細実現計画の策定作業を継続・完成し、作業に関してコミュニティとの対話を継続しつつ、gTLD新設プロセス開始に向けて、実現計画の最終版を理事会とコミュニティに対して提示することを命ずる。

となっています。かなりもってまわった言い方ですが、要するに後の方の決議で言うところの「実現計画の最終版」はまだできておらず、できたとしてもその承認はおそらく次回（2008年11月）のICANN会議以降になると思われます。紛らわしいのは初めの決議にある「ポリシー勧告を受け入れる」の部分で、この部分だけ取って「承認した」という言い方が一人歩きしているようにも思えます。

誤解の第二は、「誰でも好きなTLDが取れて好きなドメイン名を登録できる」の部分にあります。これのどこが誤解なのかを理解していただくために、現在のgTLDで採用されている「レジストリ－レジストラ モデル」という仕組みをまず説明します。

レジストリ－レジストラ モデルは、元々アメリカの独占禁止法に対する対策として考えられた仕組みで、gTLDの登録機関（レジストリ）は一般顧客から直接ドメイン名登録の申請を受けることができず、必ずICANN認定のレジストラを通さなくてはいけない、という制度です。レジストラ経由で来た申請を拒絶することも許されず、また特定のレジストラを他のレジストラに対して優遇することも許されていません。今話題となっている「gTLDの新設」は、新しいレジストリの募集であり、確かにこれまでの2回のラウンドに比べて大幅に審査基準が緩和されることが期待されていますが、レジストリ－レジストラ モデルは厳格に堅持されることが予想されています。このため、例えばIBMが「.ibm」というTLDを申請することはできますが、それが承認されたとしても、IBMが「xxxx.ibm」というタイプのドメイン名を自分の好き勝手に登録できるわけではありません。レジストラ経由で「anti.ibm」というドメイン名登録申請が来ても拒否できないのです。次回ラウンドの応募者はあくまでも、レジストリとしての事業展開のために自由にTLD文字列を選べる、という話であって、応募者が自社用に使うTLDを申請できるという話ではありません。また一般の登録者が好きなドメイン名を登録できるか、という問題とも次元が違う話です。

さて、以上が今回の報道に見られる主要な誤解ですが、どうもこれらの誤解が、必ずしも報道機関の怠惰によって起こったとは言い切れない面があるような気がしてなりません。6月26日のICANN理事会決議は、上記のように注意深く書かれており、誤解の余地はありませんが、同日付のICANN報道発表は、理事会で決まったことを正確に説明しようというよりは、むしろICANNにおいてこの件について大きな前進があったということを世間に示すためのプロパガンダの色合いを強く感じます。このように感じるのは私だけでしょうか？

さらに踏み込んで言いますと、今回のICANNパリ会議でこの件について大きな前進があったのかと言えば、それにも多くの疑問の声が上がっています。実際、GNSOのポリシー勧告の実現には多くの困難があることが既に前回2008年2月のICANNニューデリー会議で指摘されており、これらの困難な点が克服されたという明確な根拠は、私の理解する限りでは、今回のパリ会議で示されていません。理事会決議［2008.06.26.03］で、実現計画最終版の提示期限が明示されていないのも非常に奇異です。多くのパリ会議参加者の感想は「今回の理事会決議には新鮮味がない」というものであり、理事の多くが困難克服にいまだに疑問を持っていることが、6月26日の理事会での討論からうかがえます。この理事会の速記録は既に公開されていますので[※2]、興味がある方はご覧ください。

今後の本件の展開には、まだ多くの紆余曲折があるものと思われます。

gTLD(Generic Top Level Domain)の訳語について

良い機会ですので、少し話題を変えて、gTLDの訳語についても話をしたいと思います。

JPNICは長い間、「Generic Top Level Domain」の訳語として「分野別トップレベルドメイン」を使ってきました。しかし、1997年頃までは「一般トップレベルドメイン」という訳語を使っていました。当時gTLDの代表格であった「.com」「.org」「.net」では既に登録者に対する審査は無く、実質上誰でも、いくつでも登録できたので、“generic”に当初何の疑問も感じずに「一般」の訳語を当てたわけです。実際、“generic”は“general”の派生語でもあるので、自然な訳語にも思えました。

ところがある日突然、この場合の“generic”は“genre”（ジャンル、種類）の形容詞形として使われているのではないのか？という考えが頭に浮かびました。例えば、インターネットの父と言われるJon Postel氏が1994年に書いたRFC1591を見てみますと、

Each of the generic TLDs was created for a general category of organizations.

という記述があり、また、各TLDについて記述した部分では、「COM/EDU/NET/ORG/INT」に続いて、

United States Only Generic Domains:

として、「GOV/MIL」について説明が行われています。「.gov」や「.mil」は「一般向け」のTLDではなく、一部の特別な種類の組織を登録対象にしていますので、ここの“generic”を「一般」と訳すのは変で、むしろ「種類別」の方が意味としては合っています。そう考え直してみると、RFC1591の全文を通してJon Postel氏が“generic Top Level Domain”の“generic”を“genre”の形容詞形の意味で使っていたことは間違いないように思えてきました。

1997年頃、JPNICはIAHC（International AdHoc Committee）の最終報告書や、gTLD MoUの日本語訳を手掛けましたが、“genre”に気が付いたのは翻訳が一段落した後で、あらためてこれらの文書の原文を読み直してみると、著者達がこの場合の“generic”を“genre”の形容詞形として使っているという思いを一層強く持ちました。実際これら著者達の多くはJon Postel氏と親交があったので、共通の語感はごく自然なことだったと思います。そのようなわけで、この頃からJPNICは、それまでの翻訳文書で「一般トップレベルドメイン」を使ったのは誤訳であったとの立場を取り、「分野別トップレベルドメイン」という用語に切り替えました。ただし、過去の文書の訂正までは徹底し切れず、また一度世の中に広がった「一般トップレベルドメイン」という用語も、無くなりませんでした。

その後 ICANNができて、gTLD新設の2回のラウンドがありましたが、その時も新gTLDのレジストリ事業申請者は当該TLDの運用方針を説明した文書（Description of TLD Policies）を申請書に添付することになっており、それが審査の対象にされましたから、これまでに作られたgTLDについてはそれぞれ特定の利用目的が、少なくとも概念的にはある、というのがICANNの建前であったと思います。その意味で、JPNICがここ10年ほど「分野別トップレベルドメイン」という言葉を訳語として使ってきたことは、妥当であったと考えます（ただし、ICANNの建前と、それぞれのTLDにおいて第二レベルドメイン名登録者に対する資格審査があるかないか、という話は、現状ではあまり関連付けられていません）。

しかし、言葉は生き物です。全ての人が一つの言葉を同じ気持ちで使っているとは限りません。時代とともに、また使用する状況により、違った使われ方をされる場合があります。最近の傾向として、「誰でも審査無しで登録できるからgeneric」という感覚でgeneric Top Level Domainという言葉を使っている人達が多くなっていることも、また事実と思われます。それどころかICANNにおいてすら、この用語の使い方に不統一が見られるように思います。通常のICANN会議の議論では「.com」「.biz」「.info」はいずれもgTLDですが、IANAのRoot Zone Database※3を見ると、「.com」と「.info」は“Generic top-level domain”と“Purpose”の欄に書かれているのに対して、「.biz」は“Restricted for Business”と書かれていて、明らかに不統一が見られます。さらに言えば、現在検討されている次回ラウンドのgTLD新設では、“Description of TLD Policies”という添付書類も廃止される可能性もあり、「誰でも自由に登録できる」TLDが名実ともにgTLDの主流になることが予想されます。そうなった時は、JPNICは再び訳語を変更し、「一般トップレベルドメイン」を使うべき時かもしれません。

（JPNIC インターネットガバナンス・DRP分野担当理事 丸山直昌）

※1 “Biggest Expansion in gTLDs Approved for Implementation”
http://www.icann.org/en/announcements/announcement-4-26jun08-en.htm（原文）
http://www.nic.ad.jp/ja/translation/icann/2008/20080626.html（日本語訳）

※2 Meeting of the ICANN Board
http://par.icann.org/en/node/64

※3 IANA Root Zone Database
http://www.iana.org/domains/root/db/

2008.7.27▶8.1

第72回IETF報告

■ 全体会議報告

Dublin, The Republic of Ireland

◆概要

年に3回開催されるIETFでは、1回以上を北米以外で実施することになっています。今回は、その“北米以外”にあたっており、アイルランドで開催されました。アイルランドといえば、子供の頃に聞いた丸山薫作詞の「汽車に乗って」の一節、「日が照りながら雨のふる/あいるらんどのやうな田舎へ行かう」を思い出しますが、そのような天候ではなく、朝方雨が降っても昼間は太陽が輝き、隣接するゴルフ場の芝生を美しく照らす素敵なところでした。緯度が高いため、日が暮れるのも20時半過ぎで、朝から晩まで続く会議で1日がやたらと長く感じるIETFですが、最後のセッションを聞いた後もまだ日が出ているため、ちょっといつもとは違う感覚を味わうことができました。

会場は、ダブリン市内からバスで30分ほどの田園地帯にあり、普段はゴルフのための宿泊客が多いようで、ヘリコプターで来るゲストのためにヘリポートが備わっており、会期中も頻繁にヘリコプターが行き来していました。隔離された環境に、世界中から研究者や技術者が集まって、議論に没頭する1週間となりました。

- 会　　期：2008年7月27日～8月1日
- 会　　場：CityWest Hotel（Dublin, Ireland）
- 参 加 費：635USD（early registrationの場合）
- セッション数：118（tutorial、training、plenary sessionを除くWGやBoFセッション数）
- ホ　ス　ト：Alcatel-Lucent社（通信機器ベンダー）
- 参加登録者数：1,183人（前回比50人増、1,000人強で常態化しているようです）
- 参 加 国 数：48ヶ国（国別の分類などもUS、JP、DEなど変わらず。参加国数も常態化）

今回の会場は、ゴルフ場の中にあり、宿泊施設とメイン会議場の他にも数棟の建物内の会議場がありました。鮮やかなグリーンやよく手入れのされた草花を見ながらの移動は気分転換にもなり、また、途中のテラスやバルコニーにもイスやテーブルがあり、そこかしこで議論をしている人でにぎわっていました。

会期の始まる直前に、ComputerWorld※1のWebサイトに、IETFチェアのRuss Housley氏による「IETFでは、現在VoIP、MPLS、P2PとならんでIPv4/IPv6プロトコル変換機がホットトピックである」というインタビュー記事が公開されました。しかし、IETFではプレナリをはじめ、この話に触れる発言もなく、特にどのプロトコルに力を入れているということもなく、どの標準化作業についてもタフな議論がされていたように思います。

◆IETF Technical Plenary

今回は、Technical Plenaryが4日目（2008年7月30日、17:00～19:30）にあり、Operations and Administration Plenaryが5日目に行われました。

Welcomeスピーチの後、ホストのAlcatel-Lucent社（アイルランド支社のKevin O'Callaghan氏）のホスト・プレゼンテーション、IRTFとIABからのレポートに続き、「IPv6 Deployment Forum」のタイトルでテクニカルセッション、オープンマイクという流れでした。

ホスト・プレゼンテーションでは、通信機器ベンダーらしく、通信環境の変遷についてどのようなことを課題として取り組んできたか、最近のトレンドは何か、という発表がありました。エコロジー（エネルギー問題）についての取り組みの紹介では、いくつか実例紹介があり、その中でも、富士通社がspamを低減することで消費エネルギー（電力）を削減したというエピソードは、海外で聞く日本の評判という点からも興味深いものがありました。

「IRTF Report」では、IRTFチェアのAaron Falk氏から、DTNRG※2で開発した参照コード“DTN2”※3がSource Forgeに

も掲載され取得できるようになったことの報告がありました。最近の各リサーチグループの動きの中では、ICCRG※4内に、リサーチペーパー作成のためのデザイン&ドラフティングチームが形成されていることの紹介がありました。また、SIPのアプリケーションやIPv6についてのリサーチについてもトピックとしてあがっているとのことでした。

続くOlaf Kolkman氏による「IAB update」では、通常のドキュメント更新状況や多組織との協調活動報告のほかに、「RFC Editor Model」というタイトルで、RFCの執筆から発行までの整理と提言がされました。この提案では、RFCの生産工程における担当者とその役割が提示されるとともに、具体的には、“stream producers”、“stream approvers”、“production house”、“publisher”、という大きな枠組みがあり、その中における“RFC Editor”の“production house”と“publisher”に対する関与の仕方を整理しています。詳細は、IABのWebページ※5で閲覧可能で、コメントも受け付け中です。

また、IABとして現在まとめている文書のうち、前回紹介された、「よいプロトコルの条件」（What makes For successful protocol?, draft-iab-protocol-success-02.txt）は、RFC5218として発行されたという報告がありました。

これにより、現在進行中のIAB文書は、「ヘッダと常用文」が追加されて、次の三つになります。

- 「Internet上の端末設定の原則」（Principles of Internet Host Configuration, draft-iab-ip-config-04.txt）
- 「DNS拡張を行う際のデザインの選択性について」（Design choices when expanding DNS, draft-iab-dns-choices-06.txt）
- 「ヘッダと常用文」（Headers and Boilerplates, draft-iab-streams-headers-boilerplates-00.txt）

IAB主導で進められているアーキテクチャに関する活動としては、2008年4月25～26日にストックホルムで開催した会合があり、この結果は、「IPモデルの進化（The evolution of the IP model, draft-thaler-ip-model-evolution-01.txt）」「ピアツーピアのアーキテクチャ（Peer to Peer Architecture, draft-camarillo-iab-p2p-archs-00.txt）」としてまとめられたほか、今回のテクニカルプレナリの企画につながったそうです。

前回報告のあった、ITU-TとIETFによるMPLSの拡張に関するジョイント・ワーキング・チームについては、draft-bryant-mpls-tp-jwt-report-00.txtとして成果がまとめられたそうです。そのほかにも、OECDとも、世界経済におけるインターネットのもたらす経済と将来性についての議論が始まったそうです。

Olaf氏からは最後に、IABのロゴマークが紹介されました。ロゴデザインは、Dow Street氏によるものだそうです。

パネルディスカッション形式で行われた、「IPv6 Deployment Forum」では、開催に先立って、このディスカッションのモデレーターであるIABのGregory Lebovitz氏から参加者に、概要や参考情報などが提示されました。※6

IPv6の普及については、“ニワトリと卵の問題”と揶揄される状況も見受けられますが、そのような状況でもIPv6によるサービスを開始している事業者も出始めています。こうした先例を知ることによって、IPv4の在庫枯渇問題（RIRからの新規割り当てアドレス売り切れ）やIPv6を取り入れていくことにどう立ち向かうのかヒントを得るとともに、IETFがどのようにサポートしていくべきであるのかを見極めたいというのが、今回のパネルディスカッションの狙いでした。

セッションは、Lebovitz氏から、あらためて主旨説明がされた後、IETFが手掛けたIPv6の移行作業の一つとして、NAT-PT（Network Address Translation-Protocol Translation）の話がありました。NAT-PTは、2000年の2月に、RFC2766として発行されましたが、2007年7月にRFC4966により“Historic Status”となっています。しかし、1年たって状況をみてみると、NAT-PTであげられている利用例は現存しており、NAT-PTの必要性は残っているという説明がありました。実際に、IETF72でも、三つのWGと二つのエリアミーティング、一つのBoFで取り上げられていたそうです。

ということで、「現場の苦労を語る」ために選ばれた、5人のパネリストの紹介がありました。

- ARINのMark Kosters氏
- Comcast社のAlain Durand氏
- NTTコミュニケーションズ社のShin Miyakawa氏
- Google社のLorenzo Colitti氏
- Apple社のStuart Cheshire氏

ARINのKosters氏からは、IPv4とIPv6のアドレススペースの動向について、わかりやすい統計資料を用いた説明がありました。IPv4の5大RIRへの割り振りでは、ARIN/RIPE/APNICでそれぞれ30%ずつを分け合っており、これはLIRやISPへの割り当てとほぼ合致するため、実際の利用状況もそのようになっていると言えます。一方で、IPv6の割り振りは、各RIR に/12ずつ均等に分配されているため、その/12内のLIRやISPへの割り当て状況が報告されていました。RIR内の割り当て件数で推移をみると、およそ50%がRIPEで、APNICが30%、ARINが18%、LACNICとAfriNICが2%といった状況であるという報告がされました。また、ポリシー提案状況について、IPv4では枯渇や割り振りサイズであるのに対して、IPv6では、プロモーションをはじめとして割り当てと割り振りそのものについてとなっていて、プロトコルバージョンの普及度合いによって議論の内容に違いがあるという興味深い報告もされていました。

続いて、Comcast社のAlain Durand氏からは、全米一の巨大CATV網におけるIPv6の導入について話がありました。Comcast社では、インフラ（CATVバックボーン）のIPv6対応、その次に家庭への接続計画とラボテストという2段階のアプローチで取り組んできたそうです。CATV業界では、DOCSISというケーブルモデムの仕様があり、これのバージョン3.0で、IPv6対応となっているという事情もあるようですが、それでもベンダーから対応ソフトがなかなか入手できないなどの苦労があったそうです。また、数100万世帯分のIPv4アドレスを苦労して調達・管理し続けるより、IPv6の大きなスペースをまとめて入手し、それを使ったケーブルモデムの管理ネットワークを設計構築してしまう方が安上がりという考えも当初あったようです。

ところが、現実の問題として、ケーブルモデムから先の家庭内の事情として、家庭内の機器はやはりIPv4ベースのものが多く、また、その家庭内の機器の通信先であるコンテンツサーバもIPv4ベースであるという事情から、CATVバックボーンがIPv6に対応しても、IPv4パケットを受け取り、IPv6対応バックボーンを通過して、IPv4網に流す仕組みは必要である、という結論に達したそうです。さらに、IANAからRIRへのIPv4グローバルアドレスの新規割り振りができなくなった際には、これまでのISPからホームゲートウェイにIPv4グローバルアドレスを割り当てられることもなくなります。そのため、現在、同社ではこれまでの、「やがてくるIPv6対応のためのネットワーク計画」に、「IPv4だけの機能しか持たない機器」の救命策の導入を行っているそうです。Durand氏からは、三つのプランが提示されました。

プランA：デュアルスタック対応のホームゲートウェイを提供するが、IPv4のみの接続性は提供しないという案
プランB：IPv4プライベートアドレス対応のホームゲートウェイを提供し、ISPのIPv4プライベート網に接続するダブルNAT案
プランC：デュアルスタック対応のホームゲートウェイを提供し、IPv4のみの機器にはIPv4overIPv6トンネルを提供してIPv4の接続性をもたせるデュアルスタック・ライト案
（全てのプランは、新規加入者が対象です。既存顧客にはこれまでと同じ環境が提供されます）

それぞれのプランのメリット・デメリットを踏まえ、プランCが既存顧客にとっても、デュアルスタックの環境を持つユーザー、将来増えると目されるIPv6顧客のいずれにとってもよいと結論づけていました。そして、プランCを遂行するには、ISPのバックボーン内にIPv4ネットワークをつなぐためのキャリアグレードNAT(Network Address, protocol translator)を導入する必要性を訴えていました。

一方、Google社のIPv6対応はとてもシンプルな要求によるものです。それは、「IPv6だけの環境を持つユーザーが出てきた時にコンテンツを提供できるようになっていること」だそうです。そして、もしもIPv6でコンテンツを提供することが、もっとよいユーザーサービスにつながるのであれば、推進していくというゴモットモな動機が表明されていました。Google社がIPv6を用いることで検証したいのは、具体的には、

・IPv6によって、遅延やパケットロスが低減するかどうか
・NATレスによるAjaxアプリケーションの挙動の向上（多数コネクション接続時のNAPTによるポート消費解消）
・NATトラバーサル対応からの解放（開発時間をもっと別のことに使えるようにしたい）

といったあたりです。また、IPv4の在庫枯渇問題に対するGoogle社の答えも非常にシンプルで、RIRのアドレスプールがなくなった時の根本的な解決策はIPv6を使うということであり、アドレスプールは2011年末になくなることがわかっているのだから、「なぜIPv6なのか」と言っている場合ではなくて、「いつやるべきか」ということが問題であり、

・やるなら早いうちに対応しておく方が良い（サービス品

質が求められる前に）
・すぐやる方が後からせっぱつまって対策するより、コスト削減につながる
・IPv6対応は、高等理論いっぱいの難しいことではないが、時間はかかりそうだという考えの着地点が、「今」だった

という説明がありました。とはいえ、Google社におけるIPv6対応も、いわゆる「20%プロジェクト」として開始され、試験環境を整え、社内会合のネットワークで試し、ネットワークが立ち上がることによってアプリケーション側の対応が始まり、という具合に進んできたそうです。その後、規模を大きくし、精度を高める、というステップを踏んできたそうです。そうした体験から、「IPv6はIPv4ほどすんなりとは進まないから、オペレーターは注意深く、ゆっくり、確実に取り組んだ方がいい」という助言がありました。ただし、「高等な理論は必要なく、時間がかかるだけ」というフォローもありました。

ここまでのところ、Google社はIPv6にすごく好意的であるという印象を受けますが、機器・相互運用性についての現状評価は厳しく、期待に反して、実装されていない機能や信頼性がない事象の紹介がされるとともに、「インターネット（相互に接続し合って成り立つネットワーク網）ではない」という嘆きも表明されていました。しかし、解決策の見えている問題ばかりとして捕らえているようであり、その上で、Google品質を保つにはどうすべきか?という課題解決に向けて取り組んでいるようです。また、キャリアグレードNATについての考えは、できるだけクライアントはIPv6に移行すべきと考えているようで、そうした中でもIPv4コンテンツにアクセスすることができるように、「IPv6-Only Networks with NAT-PT」を提案していました。ここでも、IPv4 NATより、こちらの構成の方がまだまし、というアンチNATの発言が強調されていたように思います。最後に、IETFへの要望として、以下の4点が伝えられました。

・IPv6-onlyのネットワークへの最低限のNAT-PT機能（RFC2766の部分的復活）
・point-to-pointリンクへの/127接続（RFC4291の該当部分の改訂）
・IPv6のVRRPの策定
・/48を使ったマルチホーム

最後のパネリストである、Apple社のCheshire氏からは、OS、Apple TVといった機器、iTunesなどのアプリケーション、.Macのようなサービス機能の提供者というあらゆる側面から話がありました。前述のように、Apple社が世に出す製品は沢山あるのですが、どれもIPネットワークを利用するものばかりで、IPv6をサポートした際にも、TCP/IPの基本的な挙動上でのIPv4とIPv6双方の共存面に苦労したようです。Apple社では、そうした困難に遭遇した際には、純粋にOSとして、またアプリケーションとして、それを扱うISPというそれぞれの立場に立って、「これはイケル」と思えるものとそうではないものに整理して対処にあたってきたそうです。

その結果、TCP確立時のIPv6-IPv4フォールバック問題（接続に時間がかかったり、タイムアウトしたりする問題）には、getaddrinfo（）関数をカスタマイズして、IPv6の接続性を確認した上でIPv6のコネクションを張るように改良をしたり、“connect-by-name”と呼ばれるAPIを使って、TCPの名前解決をせずにアプリケーションをオープンするような仕組みを取り入れるといった工夫を随所に施した上での製品提供となっている、という説明がありました。Cheshire氏自身は言及していませんでしたが、説明にあったようなIPv4とIPv6を同時に動かした上で共存状況での挙動について、早くから取り組んできたことによって得た知見が活かされ、対処できているよい例だと思われました。

パネリストの発表が一通り終わった後に、モデレーターと会場からのQ&Aがありましたが、

・DHCPv6を使った設定やDHCPv6 Proxyなどの利用はうまくいくか。問題点はないか
・キャリアグレードNATなどの議論はなぜBEHAVE WGで行われているのか
・softwireはどうなのか
・proxy（Application Level Gateway）はどうなのか
・Googleでv6クライアントのダイレクト・コネクションについて気にするのはなぜなのか
・キャリアグレードNATなどのような中間機器を新しく開発するのは本当に必要なのか
・v4だけでしか通信できない機器は本当にそんなにあるのか。どういう想定なのか。どれぐらい見越す必要があるのか

といった幅広い領域に対する質問が飛び交っていました。キャリアグレードNATなどについては、BEHAVE-WGを中心に議論が継続中です。

◆IETF Operations and Administration Plenary

Operations and Administration Plenaryでは、今回はホスト・プレゼンテーションも前日のテクニカル・プレナリで行われ、淡々とIETFの運営（NOC、IETFチェア、IETF trustチェア、IAOCチェア、IAD、NomCom、EDUチーム）に関する報告がされました。

標準化作業について、前回のミーティング後からのRFC発行数（88）、I-D投稿数（107）、そのうちIANAに依頼したレビュー数などの報告がありました。

今後のミーティング予定の発表では、次回IETF73のミネアポリスから、IETF76まで来年1年分の発表がありました。次が、2009年の開催予定です。

・IETF74 2009年3月22日～27日 サンフランシスコ（アメリカ）
ホストはJuniper Networks社
・IETF75 2009年7月26日～31日 ストックホルム（スウェーデン）
ホストはi.SE
・IETF76 2009年11月8日～13日 広島（日本）
ホストはWIDEプロジェクト

その後のIAOC Q&Aの時間に、IAOCから、2010年の開催予定地であるアナハイムとアトランタ（いずれもUSA）に関心のある人は、ホストを探していますのでぜひともよろしく、というアナウンスがありました。

IESG Q&Aでは、IESGの標準化プロセスへの介入方法や、権限について苦情に近い質問が出ていました。これに対して、かなり長時間、IESG内でどういうプロセスを持っているか、議論はどの程度行われているか、著者へのコンタクトやADへの協力体制はどうなっているか、といった説明が丁寧になされていました。途中、ダブリンの醸造所で誕生したギネスビールがIESGに振る舞われるという場面がありましたが、その後も継続して、この質問については、trackerというツールにより著者以外にも全ての人に対してどのようなコメントがされ著者の反応はどうか、といった状況は公開されていること、絶えずADやWGに対して満足されるような支援であるか考えながら進めているといった回答がされていました。

IAB Q&Aは、前もって、Olaf氏よりメーリングリストで事前に質問事項を送って、時間短縮をしようという提案がされていましたが、結局ポストされたのは1件で、内容も、「プレナリの時間は延長可能ですか」というものだったという哀しい発表がされていました。実際の会場からの質問は、nomcom processに関するもの、NATやトンネルプロトコルと協調動作する新しいインターネットプロトコルを作成すべきなのではないかというもの、NATやトンネルプロトコルに関係してUDPのカプセル化についての議論、Unicodeの普及に関しての援助依頼、といった事項があがっていました。いずれも継続した議論となりそうです。

◆余談

テクニカル・プレナリの「IPv6普及パネル」で、Google社発表の決め台詞として、「IPv6 is Not Rocket Science」という言葉が使われていましたが、発表スライドには、右肩に「TM」とありました。本当に、商標登録しているのか気になるところです（この言葉、初出典は、DNSの設定について述べたBill Manning氏のようです）。

IETF71に引き続き、無線のアクセスポイントとロケーション情報を使った、GEOPRIVとECRIT wgの実験がされていましたが、呼びかけがattendee listで行われる程度で、プレナリでの報告も特段されないのが残念でしたが、今回の実験については、Webサイト※7が開設されていました。実験結果は、それぞれのWGでの活動として実を結んでいるようです。

次回のIETF73は、2008年11月16日から11月21日まで、北米に戻って、ミネアポリスにて、Google社のメインホストで開催されます。すでに、会議の参加登録、ホテルの受け付けなどがスタートしたというアナウンスがありました。

（株式会社インテック・ネットコア 廣海緑里）

※1 Computerworld.jp“「IPv6にもNATは必要」――IETF会長が明言”
http://www.computerworld.jp/topics/nb/116249.html

※2 Delay Tolerant Networking Research Group（DTNRG）
http://www.dtnrg.org/wiki

※3 DTN2
https://sourceforge.net/project/showfiles.php?group_id=101657

※4 Internet Congestion Control Research Group（ICCRG）
http://trac.tools.ietf.org/group/irtf/trac/wiki/ICCRG

※5 Proposed RFC Editor Structure
http://www.iab.org/documents/resources/RFC-Editor-Model.html

※6 IAB's Introduction to the Wed Technical Plenary
http://www.ietf.org/mail-archive/web/ietf/current/msg52686.html

※7 Location Services @IETF72
http://geopriv.googlepages.com/

■ DNS関連WG報告

◆dnsext WG（DNS Extensions WG）報告

IETF開催前に、DNSキャッシュ汚染（ポイズニング）に関する脆弱性がCERTからアナウンス※1されました。そのため、キャッシュ汚染に関する話題がメーリングリストでも展開され、DNSプロトコル自体を拡張して、キャッシュ汚染が発生する可能性を低くするための方式がいくつか提案されました。しかし、この話題自体は以前からdraft-ietf-dnsext-forgery-resilienceとして存在していたため、大きな混乱もなく議論は進行しました。

WGの会合は、いつも通りドラフトの確認から始まりました。前回の会合からは新たなドラフトは提出されておらず、前回から存在したドラフトの状態を確認しました。draft-ietf-dnsext-forgery-resilienceはWGラストコールが行われ、そこで指摘された事項を改訂した新たな版が提出されました。draft-ietf-dnsext-rfc2672bis-dnameは、WGラストコールの準備が整ったことが確認されました。他のWGのInternet-Draftも状態が確認され、進捗が確認できました。しかし、draft-ietf-dnsext-dns-protocol-profileに関しては、一切の進捗がなく期限切れとなっているため、9月中に何も進捗がなければ削除することが確認されました。

会合の後半では、DNSのキャッシュ汚染問題に対する提案が話し合われました。ポート番号をなるべく無作為に選択するだけではなく、DNSクエリのトランザクションIDを拡張する手法として、WGでは以前から、draft-vixie-dnsext-dns0x20が提案されていました。これは、DNSの名前が大文字と小文字を区別しないという仕様を利用して、問い合わせる名前に大文字と小文字をまぜあわせ、それをトランザクションIDの一部として使用するという手法です。この手法に関しては、問題もなく従来のDNS実装に導入することができるという意見が出されました。一方で、短い名前の場合には、トランザクションIDの範囲がそれほど増えるわけではないので、やはりキャッシュ汚染されやすいのでは、という意見も出されました。

その他にも良い提案があればぜひWGに出して欲しい、と呼びかけがありました。この問題に関しては、継続してdnsext WGにて議論を行っていくことが確認されました。おそらく次のIETFでもWGの会合が持たれると思われます。

◆dnsop WG（Domain Name System Operations WG）報告

dnsop WGの会合では、いくつかの新たなドラフトが取り上げられたものの、ほぼ現在のドラフト確認に終始しました。

draft-ietf-dnsop-reflectors-are-evilはADレビューの段階にあり、draft-ietf-dnsop-default-local-zonesとdraft-ietf-dnsop-reverse-mapping-considerationsは、WGラストコールからの更新待ちであることが確認されました。また、draft-ietf-dnsop-respsize、draft-ietf-dnsop-as112-ops、draft-ietf-dnsop-as112-under-attack-help-helpも、WGラストコール待ちであることが確認されました。

会合の後半では、draft-hardaker-dnsops-name-server-management-reqsに関して議論が行われました。デザインチームから、アーキテクチャや制御、モニタリングやセキュリティに関する要求がまとめられ、ドラフトは完成した形となりました。会場からの意見では、いくつかの細かな修正が提案されましたが、ほぼ完成したとみなされ、デザインチームはこれで解散して、次の段階である具体的なプロトコルの提案に進もうという合意がなされました。

新たなドラフトとしては、draft-jabley-dnsop-missing-mnameとdraft-kerr-dnsop-edns0-penetrationが取り上げられました。前者は、DNSのDynamic Updateによって、SOAのMNAMEフィールドを変更することを禁止しようという提案でした。会場からは、大きな問題ではないという意見や、MNAMEの意味そのものを考え直す方がいいのではといった意見が出ましたが、引き続きWGの議論では取り上げていく方向になりました。後者のドラフトは、authoritative DNSサーバがどのくらいEDNS0に対応しているのかを調査した結果の報告です。それによると、90%以上のauthoritative DNSサーバがEDNS0をサポートしているということでした。中には、UDPに応えずTCPにのみ応えるDNSサーバも少数ながら存在することも報告されました。会場からは、思ったよりもEDNS0対応率が高いという意見が出され、興味深い結果と認識されました。次はresolver DNSサーバに関しても行って欲しい、という意見も出されました。

（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）

※1 JPCERT/CCからのアナウンス
「複数の DNS サーバ製品におけるキャッシュポイズニングの脆弱性」
http://www.jpcert.or.jp/at/2008/at080013.txt

■ IPv6関連WG報告

2008年7月27日（日）から8月1日（金）まで、アイルランドのダブリンにて、2008年夏のIETFが開催されました。ダブリンは日本に比べ、かなり涼しく過ごしやすかったのですが、会場および投宿ホテルがダブリン郊外のゴルフリゾートであり、食事等でダウンタウンまで出るのにバスで30分ほどかかるため、場所的には少々不便を感じました。

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。

◆IEPGミーティング（Internet Engineering and Planning Group）

IETFミーティングは、正式には日曜日の正午から始まります。IEPGミーティングは毎回その直前、日曜日の午前中に開催されています。

今回は、IPv6に直接関係のあるトピックスとしては、APNICのGeorge Michaelson氏が発表した6to4のDNS逆引きサーバの登録状況紹介のみでした。6to4は、IPv4からIPv6への移行プロトコルとしてIETFで標準化され、Windows XP以降やApple社のAirMac Extremeに実装されています。このプロトコルを用いることで、IPv6 over IPv4トンネルを利用し、IPv4のみの環境からIPv6インターネットにアクセスすることができます。この発表では、6to4のDNS逆引き登録状況について紹介があり、2005年初頭に始まったこの試行サービスの登録数は線形に増加しており、現在は900以上の登録があること、米国、欧州が大部分を占めていることが述べられました。6to4は、IPv4からIPv6への過渡期に利用される移行プロトコルの一つではありますが、Windows OSに実装されたこともあり、実際の利用者は多いと思われます。

その他、IPv6には直接関係はありませんが、Randy Bush氏より、ISP網に導入される可能性のあるキャリアグレードNAT（CGN）について、否定的な見解が述べられました。CGNは、IPv4アドレスの在庫枯渇に対する一つの対応方法として検討が進められており、今回のIETFでも実装方法の提案や、導入に関するプレゼンテーションが実施されています。

□IEPGのWebページ
http://www.iepg.org/

◆6man WG（IPv6 Maintenance WG）

6manワーキンググループ（WG）は、IPv6のプロトコル自体のメンテナンスを実施するWGです。チャーターには、「IPv6プロトコルに対するマイナーな変更のみ扱う」、と明記されています。今回は、水曜日の午前中にミーティングが開催されましたが、6man WGのチェアでIPv6プロトコルの提案者の一人として有名なRobert Hinden氏は、所用により欠席で、もう一人のチェアである Brian Haberman氏が全て取り仕切るミーティングとなりました。

今回の議題は、

- PMIP6 向けのルータ広告改訂
  （PMIP6 Indication and Discovery）
  draft-damic-netlmm-pmip6-ind-discover
- IPv6 複数アドレス選択およびRFC3484の改訂
  draft-arifumi-6man-rfc3484-revise
  draft-6man-addr-select-sol
- ルータ広告のMフラグとOフラグの扱い
  draft-cha-ipv6-ra-mo
- 断片化ヘッダの問題（Overlapping Fragments）
  draft-krishnan-6man-overlap-fragment
- 拡張ヘッダの標準フォーマット
  draft-krishnan-ipv6-exthdr

の5点、となっています。

「PMIP6向けのルータ広告改訂」は、現在netlmm WGで標準化の進んでいるPMIP6（Proxy Mobile IPv6）に関連し、ネットワークがPMIP6をサポートしているかどうかを判断するために、IPv6のルータ要請/広告に手を入れたい、という提案です。これに対して、今後提案される可能性のある、いろいろなプロトコルについてアドレス割り当てレベルで機能を導入するようなことは困難であるという指摘等がありました。この提案は、6man WGのミーティング時点ではnetlmm WGでもまだ議論中ということであり、そちらでの議論が終わり、本提案の内容にnetlmm WGとして合意が得られた時点で再度検討することになりました。

「IPv6複数アドレス選択およびRFC3484の改訂」では、アップリンクから割り当てられた複数のIPv6アドレスを持つノードにおいて、通信の際に通信相手に応じた適切なIPv6アドレ

スを始点アドレスとして選択する機構に関する議論および、現在標準化されているアドレス選択に関する標準であるRFC3484の改訂に関する議論が実施されました。これは、RFC3484には、ノードが複数IPv6アドレスを保有する場合や、通信相手が複数のアドレスを持つ場合に、どのアドレスを利用するかの選択アルゴリズムが記述されていますが、標準化当初にデフォルトとして定義された条件が、その後追加定義されたULA等の新たな特殊用途アドレスに対応していない、等の問題点が指摘され、現在の状況に合わせて改訂しようというものです。また、あらゆる環境をカバーするような条件を作ることは不可能なため、デフォルトを変更するためのアドレス選択ポリシーを配布しよう、という提案に関しても議論されました。その結果、アドレス選択条件を動的に変更できるようにすることが必要だ、という合意が得られ、今後、アドレス選択ポリシーの配布をどのように実施するかを検討するチームを作り、議論を実施することになっています。

「ルータ広告のMフラグとOフラグの扱い」は、ルータ広告メッセージ中の、アドレス割り当て方式を制御するビットの扱いに対する改訂の提案です。MフラグとOフラグの扱いについては、6man WGの前身であるIPv6 WGでもかなり長い間議論され、現在の仕様に落ち着いた、という経緯があります。議論の中で、提案者が述べている問題が、本当に一般的な問題で多くの人が困る事象なのか、どこまでが仕様で、どこからが実装に依存するものであるのかの線引きの問題ではないか等の意見が出されました。この両フラグについて、問題を明確にするために、メーリングリストで議論を継続することとなりました。

「断片化ヘッダの問題」は、IPv6の拡張ヘッダの一つである断片化ヘッダに、IPv4の断片化でも問題になった、“重複断片の扱い（Overlapping fragments）”に関するセキュリティ的問題があるため、この対処が必要というものです。IPv4におけるこの問題は、RFC1858に述べられています。同様の問題がIPv6でも起こることはRFC4962に書かれていますが、現状、対処がなされておらず、また、IPv4で起こりうる問題よりも、IPv6の方がより深刻であるということが指摘されました。この問題に早急に取り組むことになり、提案ドラフトをWGアイテムとすること、および早急にRFC2460の改訂を図る方向で進めることになりました。

「拡張ヘッダの標準フォーマット」は、IPv6拡張ヘッダは、基本フォーマットが定義されておらず、新規に定義された場合には、既存実装では拡張ヘッダのサイズがわからない可能性があるという問題についてです。これを防ぐため、標準的な、TSVフォーマット（Type/Size/Value）を導入しようというものです。前回のIETFに引き続き議論されました。メーリングリストでも多くの意見があり、それらに対応してドラフトがアップデートされましたが、標準フォーマットを決めることの意義や、ヘッダ設計の概念的な部分に踏み込んでしまう可能性、また、決めたとしても、それをどのように周知していくのか等の指摘がなされました。ミーティングでは、賛同が多く、メーリングリストで意見を募集し、WGとして引き続き検討していく方向となっています。

□6man WG
http://www.ietf.org/html.charters/6man-charter.html

□第72回 IETF 6man WGのアジェンダ
http://www3.ietf.org/proceedings/08jul/agenda/6man.html

◆v6ops WG（IPv6 Operations WG）

v6opsは、IPv6とIPv4の共存技術、IPv6のディプロイメントに関する話題を扱うWGです。今回は一コマのミーティングを予定していましたが、直前に一コマ追加となり、月曜日の午前中と、木曜日の午後一番の2スロットで議論が開催されました。

一コマ目のミーティングでは、NAT-PTに代わるIPv6の移行技術に関する話題、IPv6のCPEルータに対する要求条件の話が実施されました。前回と同様、NAT-PTに代わる技術は多くの人がIPv6の導入に必要だと考えているためか、参加者が非常に多く、用意された席数では足りず、立ち見が出てしまうほど盛況なセッションでした。前回のミーティングにて、v6ops WGでは移行プロトコルに対する要求条件を中心に扱う方向になっており、今回のミーティングでも要求条件の議論に多くの時間を費やしました。IPv4/IPv6のプロトコル変換機構が持つべき必須の基本機能、推奨機能に関する提案として、既存ノードへの変更許容の是非、ネイティブ接続の優先、DNSとの連携時におけるDNSのセマンティクス変更不可、サポートする上位層プロトコル、NATの標準化を実施する、behave WGの定義した要求条件への準拠の必要性などについて議論されましたが、意見が百出し、議論時間が足りず、メーリングリストで引き続き議論を実施することとなりました。

この他にIPv6を利用したIPv4 NATを実施するプロトコルとして、

・draft-despres-v6ops-apbp（GAPプロトコル）
・draft-durand-dual-stack-lite（464変換）

について、概略の説明が実施されました。それぞれ、プロトコル自体は別WGで議論をすることになります（behave WGにて、IPv4/IPv6変換プロトコルについての提案が実施され、議論されています）。

IPv6のCPEルータに対する要求条件は、ケーブルTVネットワークにおけるケーブルモデム/ホームルータの標準である、eRouter仕様に対応するようなIPv6 CPEルータの仕様を記述することを目的とした提案です。CPEルータの持つべき機能として、ISPとの接続機能、ファイアウォール機能、宅内機器へのアドレス付与機能等があげられています。ミーティングにおいて、このようなドキュメントの必要性についてはコンセンサスを得られましたが、ドラフト自体にはまだ不足点も多く、引き続きメーリングリストで議論を実施することになりました。

二コマ目のセッションでは、一コマ目に予定されていましたが時間切れで先送りされたルータ広告に関するセキュリティの議論、アドレス割り振りのガイドライン（RFC3177）に関する議論、トンネルプロトコルのセキュリティに関する議論、および、ブロードバンドネットワークにおけるIPv6実装に関する議論が実施されました。

不正なルータ広告の扱いに関する議論は、ここ数回継続して実施されています。今回は、不正なルータ広告の扱いに関する要求条件ドラフトと、それに対する解としてのRA Guardについてのプレゼンテーションが実施されました。要求条件ドラフトに対しては、過去にあった不正なDHCPサーバや、不正な無線アクセスポイントに関する議論を参照するとよい、といったコメントがありました。不正なルータ広告に関するドラフトは、今後v6opsのWGアイテムとして議論されることになり、RA Guardに関してはRFC化に向けてWGラストコールをかけることになりました。この他、アドレス割り振りのガイドラインについては、前回議論が再開され、今回v6opsのWGアイテムとして検討を実施することとなりました。また、トンネルプロトコルのセキュリティについては、前回までTeredoのセキュリティ、として提案されていたものをトンネル一般の話として書き直したため、IPv6に特化した内容でなくなりました。そのため、今後v6opsでなくintareaにて議論を継続することになりました。最後に、ブロードバンドフォーラムとのリエゾンとして、ブロードバンドネットワークにおけるIPv6実装についてのプレゼンテーションがあり、この内容についてはメーリングリストでコメントを募集することとなりました。

今回のv6ops WGは議論の内容が多岐にわたり、それぞれ非常に活発に議論され、多くがメーリングリストでの継続議論となっています。IPv4アドレス在庫枯渇に関連して、IPv6への注目が高まっていることがうかがえました。

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

□第72回 IETF v6ops WG のアジェンダ
http://www3.ietf.org/proceedings/08jul/agenda/v6ops.html

この他に、IPv6への移行に関し、全体セッションでもパネル討論が実施されています。

第72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/72/materials.html

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

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

■ セキュリティ関連WG報告

◆IPSECME WG（IP Security Maintenance and Extensions）
（2008年7月28日の9:00～11:30に開催、参加人数:80名程度）

IPSECMEは、2005年にクローズしたIPsec WGの代わりに、IPsecの保守（主にIKEv2）と拡張（IPsecのロードマップの作成とIPv6のサポート、拡張仕様の策定）を目的としたWGとして7月に承認された、できたてのWGです。チェアはVPN ConsortiumのPaul Hoffman氏と、Checkpoint Software社のYaron Sheffer氏です。今回は、WGになって初めてのミーティングであり、WGの目的の説明と、現在のIPsecで問題となっているものに関する紹介と説明が行われました。説明が行われたものは、IKEv2bis status、Roadmap document、IKEv2 IPv6 config、IKE session resumption、IKE redirect、ESP-null visibility、Out-of-scope-for-the-WG documentsの7点でした。

□IPSECME WG Webサイト
http://www.ietf.org/html.charters/ipsecme-charter.html

◆DKIM WG（Domain Keys Identified Mail）
（2008年7月28日の11:30～15:00に開催、参加人数:60名程度）

このWGでは、デジタル署名を用いるタイプの送信ドメイン認証である、Domain Keys Identified Mail（DKIM）について検討をしています。初めに、今回の目的であるADSP（Author Domain Signing Practices）と、Overview（Domain Keys Identified Mail（DKIM）Service Overview）についてのLast Call確認と、WGでのドキュメントのステータス確認が行われました。ADSPのドラフトに対して、DNSワイルドカードを考慮するべきではないかという指摘から議論になり、ドラフトを更新することになりました。ドラフト確認後、二つのドラフトに対してWG Last Callを行う予定です。また、いくつかの新しい提案が行われましたが、WGの方針としてLast Callを予定している二つのドラフトを、次のステップであるIESGレビューへ移行するまでは取り掛からないという意見が、チェアから述べられていました。

□DKIM WG Webサイト
http://www.ietf.org/html.charters/dkim-charter.html

◆PKIX WG（Public-Key Infrastructure（X.509））
（2008年7月30日の13:00～15:00に開催、参加人数:100名弱程度）

通常通り、Documentのステータスについて報告があり、四つがRFC（CMC関連、RFC 5272、5273、5274、Certificate and CRL Profile RFC 5280）となり、八つのI-DがWGで議論中（四つがStandard Track、残りがInformational/Experimental）ということが報告されました。全部で八つの報告がありましたが、主要なものとして以下の五つを説明します。

1. RFC 3279/4055 update for ECC -- Sean Turner氏（IECA）
証明書に関して、ECCの適用状況について説明が行われました。現在IESGで検討中です。報告の中で、2002 ASN.1へ対応するべきかという問いがなされましたが、Tim Polk氏より、古いスタイルのASN.1で記述すべきとのコメントがありました。

2. Trust Anchor Management Requirements -- Carl Wallace氏（Orion）
現状のPKIXのプロトコルと、TAMPは共存できるという報告がありました。Stefan Sanntosson氏より、TA（Trust Anchor）のフォーマットをTAMPのI-Dから分離して、二つのI-Dにすべきとの意見が出ました。Tim Polk氏より、次回のMinneapolis前に変更するかどうかを投票で決めるようにとコメントがありました。Steve Kent氏からは、SIDR WGでもTAに関しての議論がなされているので協調すべきという意見が出ました。

3. Traceable Anonymous Certificates Protocol -- Sang Hwan Park氏（KISA）
追跡可能な匿名証明書に関しての韓国情報保護振興院（KISA）からの提案であり、新たにExperimental RFCとして検討を行うこととなりました。

4. Other Certificates Extension -- Stephen Farrell氏（University of Dublin, Trinity College）
証明書の連続性を記述するために、証明書の中に過去に発行された証明書へのポインタを入れることを提案したものであり、新たにExperimental RFCとして検討を行うことになりました。

5. OCSP Algorithm Agility -- Phillip Hallam-Baker氏（Verisign）
OCSPをアルゴリズム独立にするための調査に関する発表がありました。RFCによると、OCSPではRequest/Reply/チェックする証明書のいずれの署名アルゴリズムに対しても制限はなく、OCSP Verifier（サーバ）、Relying Partyが異なった署名アルゴリズムを使うことに、問題はないことがわかったことが報告されました。WGの検討事項にするかどうかは、メーリングリストでの投票を行うこととなりました。

□PKIX WG Webサイト
http://www.ietf.org/html.charters/pkix-charter.html

◆HOKEY WG（Handover Keying）
（2008年7月29日の9:00～11:30に開催、参加人数:40名程度）

HOKEY WGでは、無線モバイルネットワークにおける、ハンドオーバー時の認証情報を交換する仕組みについて検討を行っています。今回の議論の中心になったのは、東芝アメリカ研究所の大場義洋氏による鍵管理に関する提案でした。概要は、大場氏とAlan DeKok氏との間でWGのメーリングリスト上で議論されていた、鍵配布時のfraud対策として新たに技術的な解決策を導入すべきか、それとも従来通りの技術による対応で十分かどうかというものでした。議論の結果、従来通りの対応で十分であるというコンセンサスが得られ、その議論の結果を踏まえてドラフトに反映させてほしいとTim Polk氏が要求していました。

□HOKEY WG Webサイト
http://www.ietf.org/html.charters/hokey-charter.html

◆KEYPROV WG（Provisioning of Symmetric Keys）
（2008年7月30日の15:10～16:10に開催、参加人数:50名程度）

KEYPROV WGでは、ワンタイムパスワード技術について検討を行っています。まず初めにドキュメントのステータス報告が行われ、その後、以下のドラフトについての報告が行われました。

- The Dynamic Symmetric Key Provisioning Protocol
David Mitton氏によって、5版で加えられた修正について報告が行われました。スキーマ部分の修正点について矛盾がないことを確認した後、Last Callが行われることになりそうです。

- Symmetric Key Package Content Type
Sean Turner氏によって、3版で加えられた変更点として、PSKCでのユースケースの追加およびドキュメントとモジュールでのASN.1の整合性を得るための更新について報告されました。その報告を受けて、属性条件についても整合性を考慮する必要があるとコメントがなされました。

- Portable Symmetric Key Container
Hannes Tschofenig氏によって、5版で加えられた修正について報告が行われました。変更内容は、名前の変更と新しいNamespaceの追加とのことでした。議論の内容としては、UsageTypeとDeviceInfoTypeに関するものに集中していました。

□KEYPROV Webサイト
http://www.ietf.org/html.charters/keyprov-charter.html

（富士ゼロックス株式会社 稲田龍/NTTソフトウェア株式会社 菅野哲）

■ 都会から隔離され議論に没頭できる、落ち着いた雰囲気の会場です

■ アイルランドといえば“ギネス”で有名です