2008.8.25▶8.29

第26回APNICオープンポリシーミーティングレポート

第26回APNICミーティングは2008年8月25日（月）～29日（金）、ニュージーランドのクライストチャーチで開催されました。

東京は残暑の続いている時期でしたが、南半球ということで季節は冬、ミーティング期間中の最高気温は摂氏10度以下、最低気温が3～4度でした。そのため、街を見渡してみると、木々の葉は既に落ちてしまっていましたが、街の中心にはエイボン川も流れており、新緑の季節に訪れたらまた随分と印象が違うのではないかと思いました。

◆全体概要

今回のミーティングの参加者は237名と、単独開催においては過去最多であったと聞いています。このうち、約4割の103名が初めての参加者であり、地元ニュージーランドからの参加者は57名と、全体の4分の1を占めていました。

カンファレンスの構成としては、従来の各種SIG、APOPS（The Asia Pacific OperatorS Forum）、トレーニング、BoFに加え、新しい試みとして「インターネットガバナンス」、「IPv4アドレスの在庫枯渇」、「IPv6への準備」等、インターネットコミュニティにとって重要な動向にテーマを絞ったプレナリーセッションも開催されました。

また、参加者がノートPCをIPv6対応に設定し、実際にIPv6での環境を体験してもらうことを目的とした“IPv6 at your fingertips”というBoF等、実践を中心としたセッションも見受けられました。

APNIC26プログラムについては、次のURLでご確認いただけます。また各セッションへのリンクからは、発表資料とトランスクリプト（質疑/議論の生ログ）も参照できます。

http://www.apnic.net/meetings/26/

また余談ですが、参加者へ配られたグッズには、APNICロゴ入りのフリースのジャンパーと折り畳み傘（この時期は雨が多いためのようです）が入っており、参加者への配慮が感じられました。

◆ミーティングでの決定事項

○NRO（The Number Resource Organization）NC（Number Council）の選挙

現職NCのHyun-Joon Kwon氏の任期満了に伴い、アジア太平洋地域を代表するNRO NCの選挙が行われました。

NRO NCは各RIR地域から3名の代表（2名は投票による選出、1名はAPNIC ECより指名）が選出され、実質的にはICANN ASO（Address Supporting Organization）のAddress Councilとして、グローバルIPアドレスポリシーの施行にあたり、ICANN理事会に勧告を行う役割を担っています。

今回は候補者12名と候補者数の多い選挙でしたが、Naresh Ajwani氏が新NCに選出されました。

○ポリシー提案の結果：

今回は10点の提案事項のうち、6点がミーティング参加者によるコンセンサスが得られる結果となりました。

次に記述する通り、今回は2011年と予測されているIPv4アドレス在庫の枯渇と、2010年1月から2バイトと区別なく配布される、4バイトAS番号への移行に向けた議論が中心です。提案は公募されているため、主催者側が計画したものではないにも関わらず、IPアドレス、AS番号いずれにおいても現行のバージョンから次にどう進んでいくのか、というテーマが自然と取り扱われる結果となったように思います。

なお、prop-061およびprop-065については、AS番号の分配方法ではなく表記のあり方等を定義することから、APNICではなくIETFで定義すべきものとしてその後APNICスタッフからIETFへ提案を行い、RFC化されました。

その他コンセンサスの得られた提案については、2008年11月にAPNICでの施行が正式に決定し、APNIC、JPNICともに随時実装していく予定です。

※下記一覧において、IPv4アドレスの在庫枯渇に向けた提案は［IPv4］と、4バイト番号に関する提案は［4バイトAS］と記載してあります。

コンセンサスの得られた提案	
prop-055	IANAからRIRへの最後のIPv4アドレスの分配［IPv4］（Global policy for the allocation of the remaining IPv4 address space）
prop-061	文書記述用のAS番号の定義［4バイトAS］（Autonomous System Numbers（ASN）for documentation purposes）その後IETFへの提案を経て、RFC5398
prop-062	APNIC在庫の最後の/8の分配方法［IPv4］（Use of final /8）
prop-064	4バイトAS番号割り当てポリシーの変更［4バイトAS］（Change to assignment policy for AS numbers）［4バイトAS］
prop-065	4バイトAS番号の表記の変更（ASDOT※1→ASPLAIN※2）［4バイトAS］（Format for delegation and recording of 4-byte AS numbers）その後IETFへの提案を経て、RFC5396
prop-066	歴史的経緯を持つPIアドレスの効率的な利用［IPv4］（Ensuring efficient use of historical IPv4 resources）

※1 ASDOTとは、32ビットのAS番号を16ビットで区切って10進数で表し、区切りを「.」（DOT）で表現する表記方法のことです。

※2 ASPLAINとは、間に区切りを設けず、32ビットのAS番号をそのまま10進数に置き換えて表現する表記方法のことです。

継続議論となった提案	
prop-063	IPv4割り振り承認期間の12ヶ月から6ヶ月への短縮［IPv4］（Reducing timeframe of IPv4 allocations from twelve to six months）
prop-050	IPv4アドレスの移転［IPv4］（IPv4 resource transfers）
prop-060	新規NIR設立基準の変更（Change in the criteria for the recognition of NIRs in the APNIC region）
（提案者の意思により）取り下げとなった提案	
prop-059	IRRデータ正確性向上のためのRPKIの利用（Using the Resource Public Key Infrastructure to construct validated IRR data）

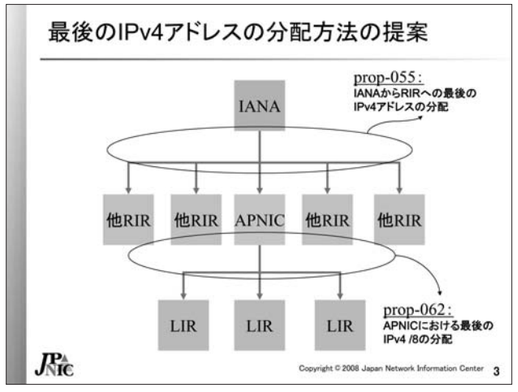
提案の原文と和訳は、次のURLからご覧いただくことが可能です。

http://venus.gr.jp/opf-jp/apnic/apnic26.html

◆今回の提案事項の主な結果について

今回の提案事項のうち、JPNICとして特に注目していたものは、prop-055、prop-062、そしてprop-050の3点です。

prop-055はIANAの、そしてprop-062はAPNICの、未割り振りIPv4アドレスを最後にどう分配するのか定義したものです。そしてprop-050は、「利用していないIPアドレスはレジストリへ返却する」というこれまでのIPアドレス管理のあり方から、LIR間でのIPv4アドレスの移転を認めようとする提案です。



■「最後のIPv4アドレスの分配方法の提案」－JPNIC IP事業部 奥谷泉の「APNIC26アップデート」資料より抜粋

prop-055: IANAからRIRへの最後のIPv4アドレスの分配

prop-055は、在庫枯渇期における混乱を避けるためにRIR間で最後のIPv4アドレスをどう分け合うのか、あらかじめ定義しておくことが重要であると考え、JPNICがLACNIC/AfriNIC地域の関係者と一緒に提案を行ってきているものです。過去3回のAPNICミーティングで提案を続け、今回コンセンサスに至りました。本提案は、自らの地域のRIRが分配を受けるアドレスサイズを定義することから、LIRをはじめとするISPにとって間接的な影響はありますが、直接的な影響はありません。

prop-062: APNIC在庫の最後の/8の分配方法

prop-062は、APNICがLIR、すなわち国内でいうところのIPアドレス管理指定事業者へ、最後の/8の在庫をどう分配するのか定義した提案です。事業者のみなさんにとっての直接的な影響が大きいことから、JPNICとしても注目していました。今回コンセンサスが得られたことにより、APNICにおける最後の/8の在庫から分配されるアドレスは、1組織（LIR）一律/22ということになりました。また、予期せぬ事態に備えて、当該/8空間から/16がリザーブされます。

prop-050: IPv4アドレスの移転

prop-050は、現在のアドレスポリシーで禁止されているIPv4アドレスの移転を、IPv4アドレス在庫枯渇後の状況に備えて認めるとする提案です。提案者であるAPNICのGeoff Huston氏は、IPv4アドレス在庫枯渇後、RIRから新たなIPv4アドレスの供給を受けられなくなったISPは、IPv4ベースのサービスの需要が継続すれば、それを埋めるために分配済みのIPv4アドレスを取り引きするようになると仮定しています。そして、そのような事態となった場合、データベース登録上の分配先と実際の利用者に乖離が生じ、APNICデータベースの信頼性低下、ひいてはアドレス管理に混乱をきたすことを避けるために、公式にAPNICで移転を認めることを目的としています。

また、提案の目的としてあげられてはいませんが、他の組織へアドレスを移転する経済的なインセンティブが提供されることにより、分配済みIPアドレスの流動化という効果もあると考えられます。

APNIC26では提案の趣旨に賛同し、一刻も早く本提案を施行するべきとの意見も表明された一方、移転条件の定義や規制に対するAPNICの関わり方を検討する必要があるとの意見も表明され、継続議論となりました。

その後、本提案について国内では、2008年11月に開催した第15回JPNICオープンポリシーミーティングにて、提案者のGeoff Huston氏も交えて議論を行いました。

これまでのアドレス管理方法からの大きな変更となることから、2009年2月に開催される次回のAPNICミーティングに向けて、ip-usersメーリングリストを含め、できるだけ多くの議論の場を引き続き設けた上で国内のポリシーフォーラム、そしてJPNICとしての姿勢を固めていく予定です。

◆APNIC26での結論に伴う影響

APNIC26でコンセンサスが得られた提案に伴い、JPNICへの申請者/ISP等が受ける主な影響は次の通りです。

prop-062：APNIC在庫の最後の/8の分配方法
APNIC在庫の最後の/8からIPアドレス管理指定事業者が分配を受けられるサイズは、ネットワークの規模に関わらず、1事業者につき一律/22（1,024ホストアドレス）となります。

prop-064：4バイトAS番号割り当てポリシーの変更
2009年7月～2010年1月の間にAS番号を申請し、2バイトのAS番号の割り当てを希望する場合は、4バイトAS番号では対応できない技術的な理由を提示することが求められます。

prop-065：4バイトAS番号の表記の変更（ASDOT→ASPLAIN）
資源管理においては、APNICも含めた全RIRおよびJPNICによる4バイトAS番号の表記は、ASPLAIN方式に統一されます。

prop-066：歴史的経緯を持つPIアドレスの効率的な利用
歴史的経緯を持つPIアドレスの割り当てを受けているIPアドレス管理指定事業者は、IPv4アドレスの追加割り振り申請時に、当該アドレスも含めて、管理下のIPv4アドレスを適切に利用していることを示すことが求められます。

また、「prop-061: 文書記述用のAS番号の定義」はIETFへの再提案を経てRFC化されたことにより、文書上、例として記述できるAS番号空間が次の通り定義されました。

2バイトAS：64496 - 64511
4バイトAS：65536 - 65551

◆次回のミーティング

次回のAPNICミーティングは、APRICOT2009カンファレンスの一部として、2009年2月にフィリピンのマニラで開催される予定です。

□APRICOT2009
http://www.apricot2009.net/

（JPNIC IP事業部　奥谷泉）

2008.10.26▶10.30

第57回RIPEミーティング報告

本稿では、アラブ首長国連邦（UAE）のドバイで開かれた、第57回RIPEミーティングの様子を報告します。

経済発展で知られるドバイは、インドの人をよく見かける国際的な都市です。道路工事やビルの建設が至るところで行われており、夜も電気がついている工事中のビルの間を、スピードを出したタクシーで走り抜けると、急成長するドバイ特有の、静かな熱気のようなものを感じます。

RIPEでは、割り振り済みのPAアドレスに対するリソース証明書のポリシーについての議論が始まりました。仮にIPアドレスの移転が行われるようになっても、正しいIPアドレスの情報をレジストリが担保することが、インターネットの運用に不可欠であるという考え方が背景にあります。この提案は、これまでに何度か活動を紹介した、RIPE NCC CA Task Force（CA-TF）によるものです。

■ 道路のバイパス工事が進むドバイ市内の様子

◆ミーティングの概要

第57回RIPEミーティングは、2008年10月26日（日）～30日（木）に行われました。ドバイでは金曜日と土曜日が週末であるため、1日繰り上げたスケジュールになっています。

参加登録者数は380名でした。最も多かったのがアラブ首長国連邦からで、55名（15%）でした。次いでドイツが39名（10%）、アメリカが37名（10%）で、日本からは9名（2%）でした。RIPE NCCでは、できるだけさまざまな地域でミーティングを開くようにしており、アムステルダムに来ることができない人でも、ミーティングに参加しやすいようにしているそうです。オランダのアムステルダムにはRIPE NCCのオフィスがあり、毎年5月のRIPEミーティングが開催されています。

Dubai, United Arab Emirates

開催地からの参加者は、通常よりも多い傾向があることから、RIPE NCCの配慮はある程度功を奏しているように思われます。ただし、2位以降は割合の構成が似ており、参加を検討する側には、“国内で開催されれば参加できるが、距離が離れていない隣の国であっても、国外だと参加できない”という状況がありそうです。

週の前半は参加者全員が集まるPlenaryで、火曜日を中心にAddress Policy WGが行われました。後半はEIXやDNS、DatabaseといったWGが、二つの会場で並行して開かれました。

□ミーティングプラン
http://www.ripe.net/ripe/meetings/ripe-57/meeting-plan.html

■ 第57回RIPEミーティング会場のJW Marriott Hotel

◆Plenary

Plenaryでは、ローカルホスト企業からのプレゼンテーションや、各RIRの最新状況についての紹介、IETF等でのIPアドレスやAS番号に関連した議論の紹介などが行われます。

今回のローカルホスト企業は、アラブ首長国連邦の通信会社であるEtisalat社で、タイやニューヨークにBGPのピアが張られているバックボーンの状況や、特定のSNSのトラフィックが1.5Gbpsを超えており、トラフィックシェイピングを検討していることなどが紹介されました。また、UAEで結成されているIPv6 Task Forceに参加し、政府や通信事業者と連携を図っていることなどについてプレゼンテーションが行われました。

興味深かったのは、最終日のPlenaryで行われた、Google社のLorenzo Colitti氏によるプレゼンテーションです。Googleの検索結果のページにIPv6のサーバにもアクセスする仕掛けを設け、クライアント側のIPv6の利用状況を調査しました。主な結果を以下に示します。

・全ユーザー中の0.238%にIPv6の到達性がある

・IPv6の利用方法としては、6to4が最も多く、全体の67.9%を占める

・アメリカとカナダでは95%が6to4を利用しており、逆にフランスでは95%がnative接続である

・IPv6の到達性がある中で、使われているOSはMacOSが最も多く、次にLinux、Windows Vista、Windows Server 2003の順である

クライアント側のIPv6の利用状況を具体的に調査した事例が少ないことから、会場ではこの調査と結果の公表に対して、拍手が送られていました。

また、日本からはインターネットマルチフィード株式会社の外山勝保氏が、日本におけるIPv6トラフィックの量について紹介しており、こちらも「日本におけるIPv6の現状を正確に伝えているプレゼンテーションである」として評価を受けていました。

◆リソース証明書に関するポリシーとデモ

リソース証明書については、Address Policy WGとNCC Services WGで議論が行われました。

Address Policy WGでは、リソース証明書の発行に関する初めてのポリシー提案があり、リソース証明書の失効が意味する「IPアドレスの返却」などについて議論されました。

□Initial Certification Policy for Provider Aggregatable Address Space Holders
http://www.ripe.net/ripe/policies/proposals/2008-08.html

提案は、PAアドレスに対するリソース証明書の発行です。RIPE NCCにおけるメンバーの契約に紐づく有効性を持っており、LIRの契約が切れると発行済みのリソース証明書が失効します。また、有効期限は18ヶ月とされており、更新されなければ無効になります。つまりIPアドレスに有効期限ができるということです。IPアドレスが自動的に返却されるような仕組みとして考えることができますが、この議論は分けた方がいい、という意見が出ていました。

一方、NCC Services WGは、RIPE NCCのサービスに関するWGです。RIPE NCCでは、リソース証明書とROA（Route Origination Authorization）の管理を体験できるデモプログラムを開発し、Webアプリケーションとして公開しています。NCC Services WGでは、このデモプログラムの紹介が行われました。

このデモプログラムは、RIPE NCCから割り振られているPAアドレスを含めたリソース証明書を発行することができます。RIPEのメンバーでないユーザーには、試験用のIPアドレスが用意されており、簡単な登録で利用できます。

さらにこのデモプログラムは、IPアドレスとOriginASの番号が入ったROAを生成することができ、それらを鍵ペアと連携させて管理する機能も持っています。例えば、鍵ペアを更新した後に、ROAを全て発行しなおすことができます。

□RIPE NCC Resource Certification
https://certtest.ripe.net/

RIPE NCCのTim Bruinzeels氏は、リソース証明書とROAのメリットとして、以下の二つを挙げていました。

・ISPが経路広告の要望を顧客から受けたときに、その顧客が正しくIPアドレスの割り当てを受けているかどうかを確認できる

・WHOISの登録情報はRIR毎に異なるが、リソース証明書はグローバルスタンダードである

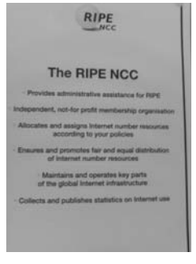
会場では、以下の三点について議論されていました。

・リソース証明書の失効
リソース証明書が失効すると、インターネット経路制御に即座に影響が出てしまうのかどうかの確認とその対策に関する議論

・国ごとの法律の違いによる問題
リソース証明書で使われる暗号アルゴリズムや、法制度の中での、証明書の有効性が国によって異なってしまうことの指摘

・Webアプリケーションであるために生じる鍵ペアの安全性
RIPE NCCが提供している利用実験は、Webサーバ上に生成された鍵などの一切が保存される。鍵の信頼性はこれで担保できるのか、という議論。RPKI（Resource PKI）は、技術的にユーザ側に鍵を持たせることができるが、現行の利用実験ではそれができない

リソース証明書の実験提供は始まったばかりですが、デモプログラムや、紹介ビデオによって参加者の関心が集まり、具体的に論点が挙がり始めたかたちとなりました。



■ RIPE NCCの事業内容を簡潔に説明したポスター
（RIPEコミュニティに対する、RIPE NCCの位置づけが、参加者に分かりやすいように、RIPEミーティングでは必ず掲示されています）

◆IRRにおける4バイトAS番号対応

Routing WGでは、元RIPE NCCで、現在はISCに所属するShane Kerr氏によって、IRRToolSetの近況が紹介されました。

4バイトAS番号については、パッチの存在は確認されているものの、本体への組み込みはまだされていないそうです。コミュニティを構成して開発しているため、作業してくださる方を募集している、とのことでした。

□IRRToolSet
http://irrtoolset.isc.org/

◇　　◇　　◇

ドバイの街中でインターネットカフェを何軒か見かけました。オランダのアムステルダムでインターネットカフェというと、電飾のついた暗めの電気屋さんといった雰囲気なのですが、ドバイで見たインターネットカフェは、立派で小さなオフィスのようでした。

革張りの椅子が並んでいて、店内の照明は落ち着いた暖色です。日本の少し高級なインターネットカフェに似たところがありますが、店内にポスター等は張られておらず、やや厳かな雰囲気です。これは宗教上の理由からかもしれません。街中のインターネット環境に、ドバイらしさを見つけた気がしました。

（JPNIC 技術部/インターネット推進部 木村泰司）

2008.11.3▶11.7

ICANNカイロ会議報告

［関連記事］ P.24「第23回ICANN報告会レポート」

エジプトのカイロにて、2008年11月3日から7日に開催された、ICANN会議に出席しました。

カイロ会議での議論に向けて、2008年10月23日には、ICANNより新gTLD導入に関するドラフト版RFPとなる「Draft Applicant Guidebook（以下、ドラフト版ガイドブック）※1」と、IDN ccTLD Fast Trackプロセスの実装計画案である「Draft Implementation Plan for IDN ccTLD Fast Track Process※2」が意見募集のために公開されており、今回の会議では、新gTLDの導入とIDN ccTLD Fast Trackに関する話題が議論の中心となりました。参加者が自由に質問や意見を述べることができる、パブリックフォーラムのオープンマイクでは、新gTLDに関するコメントが目立ちましたので、多くの人々が新gTLD導入に関心を寄せている様子がうかがえました。そこで、本稿では、新gTLD導入に関する現在の状況についてご報告します。

◇　　◇　　◇

◆ドラフト版ガイドブックが公開された経緯

2008年6月に開催された前回のパリ会議では、JPNIC News & Views vol.559※3の報告でお伝えした通り、GNSO※4評議会が作成した新gTLD導入に関する勧告※5が、ICANN理事会によって承認されました。これにより、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が終息し、ポリシー実装フェーズに突入しました。ICANNスタッフにより実装計画が策定され、その内容として公開されたのが、前述のドラフト版ガイドブックとなります。ドラフト版ガイドブックは、6部構成で97ページから成り、各部について説明する説明覚え書き（Explanatory Memoranda）も、ガイドブック本体とは別に7点公開されています。詳しくは、ICANNの新gTLDに関するWebページ※6でご確認ください。

◆カイロ会議での反応

カイロ会議では、新gTLDの導入に関する背景を説明するセッションと、ドラフト版ガイドブックおよび説明覚え書きに関する、説明と質疑応答のためのワークショップが開催さ

れ、ALAC、ccNSO、GAC、GNSOの合同セッションやパブリックフォーラムなど多くの場でも、新gTLD導入に関する議論が行われました。それらの場で耳にしたコメントは、立場によって異なる多様な内容ではありましたが、次の3項目については複数の方々が述べていたように記憶しています。

・スケジュールについて
- いつから申請受け付けが開始するのかといった詳細が分からず、スケジュールの全体像がつかめない。
- 新gTLD導入を心待ちにしているので、とにかくスケジュールを遅らせないで速やかに進めてほしい。

・手数料について
- 申請にあたって最初に払う手数料（gTLD Evaluation Fee）がUS$185,000、レジストリに選ばれた場合にICANNに支払う手数料が、四半期で少なくともUS$18,750であるなど、既存のTLDに関する手数料と比較して高い。これらの料金設定は、新gTLDの導入を促進しようとする動きとはかけ離れており、最終的には登録者の負担になるだけである。
- 手数料が高いのは、申請を希望する者を排除してしまうという悪影響よりも、むしろ真剣味の足りない申請を抑制する効果があるのではないか。
- 手数料算出にあたっての、明確な根拠の提示を求める。

・新gTLDとIDN ccTLDとの関係について
- 新gTLDとIDN ccTLDが導入される時期は、これまでの予定通り、ほぼ同時期と考えて良いのか。もしIDN ccTLDの方が先に導入されると、新gTLDよりも、市場での優位性を得てしまうのではないかと懸念する。

なお、まだ意見募集期間中であったということもあり、GACやGNSOといった、ICANN内の各組織からの正式なコメントは控えられていました。

◆今後の想定スケジュール

新gTLD導入のスケジュールについては、本原稿執筆時点（2008年12月）で確認できる2008年10月アップデート版でICANNが想定するスケジュール※7と、2008年6月のパリ会議の際に発表されたICANNの想定スケジュール※8を比較すると、ドラフト版ガイドブック（RFP）の公開時期および申請受け付け開始時期が、それぞれ1ヶ月半から2ヶ月ほど繰り下がっています。

しかしながら、最終日の理事会でICANNスタッフから説明された、今後のスケジュール案は下記のようになっており、2008年10月アップデート版のスケジュールよりも、さらに繰り下がることもあり得るようです。

2008年10月23日
　～12月 8日 ：ドラフト版ガイドブック（RFP）の意見募集
2009年2月15日頃：修正を反映したRFP第2版を公開
2009年3月中旬 ：RFP第2版の意見募集を終了（メキシコ会議直後）
2009年5月はじめ：最終版ガイドブックが完成し、2009年5月の理事会で審議
2009年5月終わり：最終版ガイドブックを公開
2009年9月30日 ：最終版ガイドブックを公開後、公示期間を4ヶ月設定した場合、2009年9月30日以降に申請受け付けが可能となる

ICANNスタッフとしては、最終版ガイドブックを公開する前に、パリ会議や意見募集期間に寄せられた意見を反映し、改めてドラフト版ガイドブックを公開する予定としているようです。スケジュールを早めるためには、改めてドラフト版ガイドブックを公開せずに、最終版を公開してしまうという考え方もあるものの、コミュニティの反応を考えると、ICANNスタッフとしては、次のドラフト版を出したほうが良いと考えているとのことでした。

GNSOの勧告に従い、最終版ガイドブックが公開されてから申請受け付け開始までには、内容を理解してもらうための期間として、4ヶ月の公示期間（Communications Period）を設定することが考えられます。ただし、修正されたドラフト版が最終形に近いと考えられる場合には、修正されたドラフト版が公開されるのと同時に、公示期間を開始することもできるかもしれない、との説明がありました。

いずれにしても、スケジュールについては引き続き検討され、追って報告があるようです。

◇　　◇　　◇

2008年12月11日（木）に開催した、第23回ICANN報告会（東京、虎ノ門パストラルホテル）でも、ICANNカイロ会議の詳細についてご報告いたしました。報告会の内容については、P.24からの「第23回ICANN報告会レポート」をご覧ください。

（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 New gTLD Program: Draft Applicant Guidebook（Draft RFP）
http://www.icann.org/en/topics/new-gtlds/draft-rfp-24oct08-en.pdf

※2 Draft Implementation Plan for IDN ccTLD Fast Track Process
http://www.icann.org/en/topics/idn/fast-track/idn-cctld-implementation-plan-23oct08-en.pdf

※3 JPNIC News & Views vol.559［特集］ICANNパリ会議報告
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2008/vol559.html

※4 GNSO（Generic Names Supporting Organization:分野別ドメイン名支持組織）
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。GNSOは、カテゴリー別の六つの部会（gTLDレジストリ、gTLDレジストラ、商用ユーザー、非商用ユーザー、知的財産権関係者、ISP）と、GNSO評議会によって構成されています。GNSOの運営を担うGNSO評議会のメンバー構成は、各部会からの代表計18名および指名委員会が選出する3名となっています。

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

※6 New gTLD Program
http://www.icann.org/en/topics/new-gtld-program.htm

※7 Anticipated Timeline（2008年10月時点）
http://www.icann.org/en/topics/new-gtlds/timeline-oct08-en.pdf

※8 Anticipated Timeline（2008年6月時点）
https://par.icann.org/files/paris/gTLDUpdateParis-23jun08.pdf

2008.11.16▶11.21

第73回IETF報告

■ 全体会議報告

◆はじめに

2008年は、IPv4アドレスの在庫枯渇や、DNSSECの導入、経路制御のセキュリティ、暗号アルゴリズムの移行など、インターネットの運用に関する話題に事欠かない年でした。

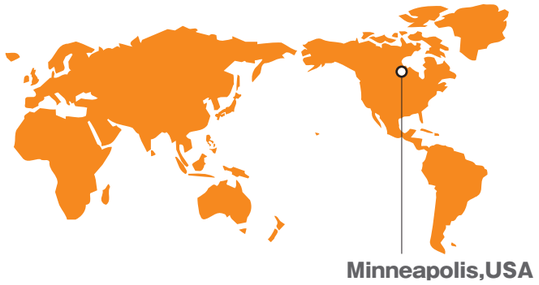
IETFの中の、これらの話題に関係するWGでは、インターネットのアーキテクチャを踏まえた上で、技術課題の解決に向けた議論が行われています。今回の第73回IETFでは、新たな経路制御アーキテクチャに関する議論とデザインを行うResearch Groupであるrrgと、NATの要件や挙動を明確化してIPv4とIPv6の相互の通信をサポートするBCPを策定するbehave WGに、各々三つの時間枠が取られていました。

通常、WGセッションの時間枠は一つか二つですので、通常のWGよりもアジェンダが多いことがうかがわれます。後半で簡単にご紹介したいと思います。

◆概要

第73回のIETFミーティングは、2008年11月16日から21日にわたって、アメリカのミネソタ州・ミネアポリスで開催されました。昼間の外気温は、摂氏マイナス6度と寒い時期です。しかし、ミネアポリスでは過去に5回IETFミーティングが開かれており、古参の参加者にとっては、おなじみの場所であるようです。

■ 受付デスクでバッジなどを受け取った後の筆者



参加登録者数は962名で、前回に比べ221名減でした。国別の内訳は、第1位がアメリカ（50%）、2位が日本（10%）、3位はドイツ（5%）でした。初日はIEPGミーティングやチュートリアルが行われ、2日目以降にはWGのセッションが、4日目の水曜日にTechnical PlenaryとOperations and Administration Plenaryの二つのPlenaryが行われました。

ホスト企業はGoogle社で、Cisco社、Juniper社、Infoblox社の3社がスポンサー企業でした。

◆Technical Plenary

Technical Plenaryでは、ホスト企業であるGoogle社のプレゼンテーションとIABで議論が進められているドキュメント「Evolution of the IP Model」の紹介が行われました。

PlenaryのGoogle社のプレゼンテーションでは、Google社がIETFをサポートする理由として、オープンソースが真のオープンスタンダードにつながり、オープンスタンダードがインターネットの発展につながっていくのだ、という考え方が紹介されました。また4日目の昼休みに行われる、Google Open Source ProgramとAndroidに関する説明会のお知らせもありました。

□Google and Open Source
http://code.google.com/opensource/

「Evolution of the IP Model」は、さまざまなドキュメントで述べられていたIPのサービスモデルと、その発展についてまとめることを目的としたドキュメントです。

□Evolution of the IP Model
http://tools.ietf.org/id/draft-thaler-ip-model-evolution-01.txt

IPの基本的なモデルはRFC791に書かれており、例えば、送信前にあて先のホストとシグナリング処理を行わず、ただアドレスを指定して送信する、といったことや、パケットサイズが可変であるといったことが定義されています。また、IPで通信するホストの、トランスポートプロトコルに関する要件が書かれたRFC1122では、送信インタフェースの選択の仕方に応じて“Strong Host”や“Week Host”といった区別がされており、日頃意識はしていなくても、IPのサービスモデルに対して前提だと考えられている事が、いくつも存在していると言えます。

しかし、IPサービスモデルの発展に伴い、上位レイヤやアプリケーションがそのサービスモデルに期待してもいいこと、すなわち“前提”があいまいになってきており、場合によっては誤解されていると言われています。

この状況は、近年の新しいプロトコルを策定する場面で問題となっています。例えばStream Control Transmission Protocol（SCTP）※1のように優れたプロトコルでも、NATを超えられないという理由でインターネットで使えないことがあります。この問題は、NATを前提とするかどうかといった考え方の違いに直接的な原因があると言えますが、より広く捉えると、プロトコルの策定や実装の段階で、IPのサービスモデルに対して置かれている前提が、多くの人の間で共有できていないことに原因があると言えます。「Evolution of the IP Model」は、プロトコルの設計を行ったり、実装を行ったりする人が、同じ前提を持つことを目指して、上位レイヤやアプリケーションから見たIPサービスモデルの性質をまとめています。

◆Operations and Administration Plenary

Operations and Administration Plenaryでは、Postel Service Awardの発表とIETFチェアの活動報告などが行われました。

今回のPostel Service Awardは、10回目です。今年の受賞者はLa Fundacion Escuela Latinoamericana de Redes（EsLaRed）という非営利団体です。ラテンアメリカとカリブ海地域における情報通信技術の普及への貢献が称えられました。

□Coveted Jonathan B. Postel Service Award Granted to EsLaRed
http://www.isoc.org/awards/postel/eslared.shtml

IETFチェアのRuss Housley氏からは、IETFの概況が報告されました。現在115のWGがあり、第72回IETF以降、97のRFCが出ました。同じ期間に、新しいInternet-Draft（I-D）が389作成されました。この他の主な報告事項を以下にまとめます。

- RFCの修正がまとめられる、ErrataのWebページに「ドキュメント更新待ち」のステータスが追加された。

□RFC Errata
http://www.rfc-editor.org/errata.php

- IANAのリクエストの処理状況が公開されており、処理待ちは、常に15以下に抑えられている。

□IANA Statistics for IETF-related Requests
http://www.iana.org/about/performance/ietf-statistics

- IETFのドキュメントやWGの議事録などをさかのぼって閲覧できるDatatrackerのプログラムが、第73回IETFミーティングが始まる前日の2008年11月15日に開かれたイベント、“Code Sprint”を通じてバージョンアップした。

□datatracker（デフォルトでI-D Trackerが表示される）
http://datatracker.ietf.org/

■ 全体会議の様子

◆ホットな話題に関係するWG/RG

最後に、冒頭であげた話題に、IETFではどのようなWGが関係しているのかについて、筆者なりに紹介したいと思います。IETFのWGは多数あり、カバーできていない可能性がありますので、ご参考程度に留めてください。

○IPv4アドレスの在庫枯渇とIPv6
IEPGミーティング
http://www.iepg.org/
RIRの動向に加えて、4バイトAS番号の利用状況などを含めたインターネット経路制御やDNSSECについての議論も行われている。
behave WG
http://www.ietf.org/html.charters/behave-charter.html
NATの要件や挙動を明確化してIPv4とIPv6の相互の通信をサポートするBCPを策定するためのWGである。IPv6のためのNATやCarrier Grade NAT（CGN）も主にこのWGで議論されている。
v6ops WG
http://www.ietf.org/html.charters/v6ops-charter.html
IPv6の運用に関するWGで、IPv6の普及動向やトンネル技術、NAT技術等多岐にわたって議論されている。
6man WG
http://www.ietf.org/html.charters/6man-charter.html
IPv6プロトコルのメンテナンスを行うWG。実装の上で明らかになった課題にも取り組んでいる。

○経路制御のセキュリティ
sidr WG
http://www.ietf.org/html.charters/sidr-charter.html
経路制御プロトコルの新しいセキュリティ・アーキテクチャについて議論しているWG。主にリソース証明書について議論されている。経路制御プロトコルとの関係については、rpsec WGでまとめられたセキュリティ要件が引き合いに出されることがある。

○DNSSEC
dnsext WG
http://www.ietf.org/html.charters/dnsext-charter.html
DNSSECを含めたDNSの拡張について扱うWG。DNSSECに関するRFCが多数出されている。dnsop WGでも、関連するI-Dが作られている。

○暗号アルゴリズムの移行
pkix WG
http://www.ietf.org/html.charters/pkix-charter.html
PKI関連のドキュメントを扱うWG。電子証明書で使われる暗号アルゴリズムについて議論されている。
s/mime WG
http://www.ietf.org/html.charters/smime-charter.html
S/MIMEのメッセージ形式であるCMSで、扱うことのできる暗号アルゴリズムについて議論されている。最近の2回のIETFでミーティングは行われなかったが、MLでの議論は行われている。
tls WG
http://www.ietf.org/html.charters/tls-charter.html
TLSにおける暗号アルゴリズムについて議論されている。TLSにおける共通鍵暗号についても、I-Dが作成されている。

○新たな経路制御プロトコル
rrg
http://www.irtf.org/charter?gtype=rg&group=rrg
経路制御プロトコルの多岐にわたる問題解決や再検討を行うResearch Group（Internet Research Task Force（IRTF）のグループ）である。最近のミーティングでは、LISP（Locator/ID Separation Protocol）の実装に関する話題が多いようである。

◇　　◇　　◇

次回の第74回IETFミーティングは、2009年3月22日から27日に、アメリカのサンフランシスコで行われます。

なお、既にご存知の方はいらっしゃるかと思いますが、2009年11月の第76回IETFは、日本の広島で開催される予定です。ホストを務めるのはWIDEプロジェクトです。この機会を生かして、IETFのディスカッションに参加されてみてはいかがでしょうか。インターネットのアーキテクチャや、最新のプロトコルに関する本場の議論に、気軽に参加できるチャンスだと思います。

（JPNIC 技術部/インターネット推進部 木村泰司）

※1 Stream Control Transmission Protocol（SCTP）
SCTPは、通信相手と複数の論理的なパスを確立できる、コネクション型のトランスポートプロトコルです。一つのネットワークインタフェースが使えなくなるなど、TCPではコネクションが失われてしまうときにも、別のパスに切り替えることでコネクションを継続できる「パス管理」の機能を持っています。コネクションを維持したまま無線LANと有線LANを切り替えたり、別のネットワークに移ったりすることを実現する応用方法が研究・開発されています。

■ DNS関連WG報告

◆dnsext WG（DNS Extensions WG）報告

前回に引き続き、今回の第73回IETFにおいても、dnsext WGの会合が開催されました。まずいつも通りに、Internet-Draftの状態確認が行われました。draft-ietf-dnsext-forgery-resilienceやdraft-ietf-dnsext-dnssec-rsasha256といった文章は、前回のIETF会合の後に更新版が発行されました。その他の文書は特に更新は無く、進捗が無いことの確認が行われただけでした。

今回のdnsext WGの会合にて最も時間をかけて議論されたのは、やはりforgery-resilienceでした。騙されにくくするためのテクニックとして、DNS ping、0x20 entropy、RTT Bandingといったものが紹介され、この中でも0x20 entropyの手法が一番害も無く、かつ騙されにくくできるのではという、これまでの議論のまとめがありました。また、キャッシュの上書きを禁止する条件や、CNAME、DNAMEの連鎖のさらなる検証、複数回の試行によるデータの検証といったテクニックも紹介されました。これらは今までの議論の中で出てきたものです。TCPでのDNS応答という提案もありましたが、できるだけ避けるべきと結論付けられました。

また、上記で紹介されたテクニックは、いずれも特効薬となるものではないのに、これらのテクニックを導入したら、ますますDNSSECの普及が阻害されるのではないかという意見も出されました。その一方で、何もしないのは現実的な解決策ではないといった意見も出され、結局まとまることはありませんでした。このInternet-Draft自体は、これらの選択肢をまとめた後に更新され、IETF Last Callが完了した段階となっています。

新たなInternet-Draftとしては、draft-bellis-dnsext-dnsproxyの紹介がありました。この文章は、ブロードバンドルータ等にDNS Proxyを実装するにあたっての注意事項や、セキュリティ上留意する点についてまとめられた文章です。会場内でWG draftとすることの合意がとられ、その後draft-ietf-dnsext-dnsproxyとして発行されました。

また、draft-bagnulo-behave-dns64に関する発表もありました。これは、IPv6/IPv4トランスレータ用DNSの挙動を定義した文章ですが、特に新しい着眼点があるわけでもなく、あまり建設的な意見が出ることなく途中で時間切れとなりました。なお、発表の続きは、dnsop WGの会合にて行われることとなりました。

◆dnsop WG（Domain Name System Operations WG）報告

dnsop WGの会合は、2時間の枠で開催されました。まずいつも通り、Internet-Draftの状態確認が行われました。前回のIETFからの進捗としては、draft-ietf-dnsop-reflectors-are-evilがRFC5358として発行されました。また、draft-ietf-dnsop-default-local-zonesやdraft-ietf-dnsop-reverse-mapping-considerations、draft-ietf-dnsop-name-server-management-reqsもWG Last Callの段階であることが確認されました。

draft-jabley-dnsop-missing-mnameについては、dynamic updateによってDNS管理者が困っている状況があるか、ということがRoot DNSオペレータに確認されました。その結果、あまり困っているわけではないという回答があったため、特にLast Callをかけること無く、一旦保留することが確認されました。その他、draft-ietf-dnsop-respsizeがWG Last Callされることが決まりました。

dnsop WG自体としては、今回は特に新しい話題はありませんでした。今までのInternet-Draftの確認が主な議題でした。一方、dnsop WG自体の議題ではありませんが、他のWGやその他関連draftとの協調に関する議題がありました。

その一つとして、draft-carpenter-renum-needs-workがあります。これは、リナンバリングの機構は必須ではないにせよ、やはり必要となる場面は多く存在するため、リナンバリングを行うにあたっての技術的な問題点をまとめた文章です。その中でDNSも取り上げられており、レコードのTTLに関する注意点に言及されています。この文章自体、これから先本当に発展していくのかわかりませんが、dnsop WGにもレビューの依頼が来ました。

その他には、draft-bagnulo-behave-dns64に関する議論もありました。これはdnsext WGでも議論が行われたものですが、dnsop WGでは、特にDNSSECの扱いについて議論されました。NAT64トランスレータを利用する場合、DNSの問い合わせクエリ中にあるDO（DNSSEC OK）flagとCD（Checking Disabled）flagをどう扱うかという議論がなされました。こ

れに関しては、behave WGでも引き続き議論が行われることとなりました。

また、DNSSECに関連して、RootゾーンをDNSSECにて署名する方向で動いているというIABの声明が報告されました。これはKaminsky Attack等でDNSプロトコル自体の脆弱性を指摘する声が高まったことに対応する動きで、NTIA（米国商務省電気通信情報局）が発表した、Rootゾーンへの署名にIABとして協力するという声明でした。NTIAの発表は、下記サイトにまとめられています。

□NTIA Seeks Public Comments Regarding the Deployment of DNSSEC
http://www.ntia.doc.gov/dns/dnssec.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

第73回のIETFは、2008年11月16日から21日まで、米国ミネアポリスにて開催されました。既にミネアポリスは最高気温がほぼ摂氏0度という気候で、日本に比べてかなり寒く、また、暖房のためか部屋が極端に乾燥しており、体調を崩していた日本の方が非常に多く見受けられました。

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。

■ 第73回IETFのミーティング会場近辺から見たミネアポリスの中心部

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

IEPGミーティングは、毎回、IETFミーティング開始前の日曜日の午前中に開催されています。IPv6に関連する発表としては、IEPGのチェアであるKurtis Lindqvist氏による、.se（スウェーデン）におけるIPv6利用状況に関する報告、および、Brian Carpenter氏のリナンバリングに関する検討がありました（Brian氏の代理でチェアが発表しました）。

IPv6の利用状況に関しては、このところNANOG等のオペレーターミーティングや、APNICのようなRIRミーティングでもしばしば報告されますが、その多くは現状、IPv6トラフィックはほとんどない、というものです。今回のKurtis氏の発表では、トラフィック量の具体的な値にはあまり触れられませんでしたが、IPv6対応したコンテンツサーバ（ニュースサイト）におけるアクセス状況の分析結果についての報告がありました。このサイトでは、2008年1月から9月までの間に、11,504のアドレスからのアクセスがあり、アクセス手段の内訳は、6to4が83%、ネイティブが10.5%、Teredoが2%となっていること、また、OS種別では、Mac OS Xが52%と多く、Windows Vistaが21%であったとのことです。

この他にも、別なサイトの短期間データも紹介されましたが、トラフィックの大部分はまだまだトンネルプロトコルであることが指摘されています。Kurtis氏は、この原因の一つとして、「xDSLやFTTx等のブロードバンドネットワークにおけるIPv6技術の標準化が十分でない」という意見がオペレーターより寄せられていることを紹介していました。

□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。今回は、月曜日の午後最初のコマにて、120名程度の参加者のもと、ミーティングが開催されました。

最初に、チェアから、アジェンダの確認と、WGで扱っている文書について、次の通り現状報告がありました（これらの項目が、IETF73開始時点における6man WGのオフィシャルな議論アイテムとなっています）。

・前回議論になった重複フラグメントに関するドラフトのWGアイテム化
・予約インタフェース識別子ドラフトをIESGにレビュー依頼
・IPv6サブネットモデルについては、問題点について議論継続
・アドレス選択問題解法ドラフトは、設計チームの結果が出るまで議論停止
・ノード要求文書については、今回議論

今回は、

1. フローラベルの利用方法の提案
2. IPv6複数アドレス選択に関する報告
3. ノードに対する要求仕様議論
4. ルータ広告を利用したDSL回線識別方法の提案
5. 短命IPv6アドレスの提案
6. IPv6アドレスのステート拡張
7. ドメイン名を利用したインタフェース選択

のそれぞれの項目について、議論が実施されました。次に、このうち重要な議論について説明します。

2.の「IPv6複数アドレス選択に関する報告」と3.の「ノードに対する要求仕様議論」は前述の通り、6man WGとしての正式な対応アイテムとなっています。2.のIPv6複数アドレス選択に関する議論報告は、前回のIETFでの6man WGミーティングにて設立が決まった、IPv6アドレス選択設計チームの議論報告です。ノードが複数のIPアドレスを持っている場合、通信をする際に使用するアドレスを選択することが必要になります。その際に使用する選択ポリシーを配布する機構について、どのようなタイミングでポリシー配布が必要か、また、どれくらいの頻度で配布することが必要かの検討結果として、多くの場合、頻度的にはそれほど多くなく、また、ネットワーク管理者がポリシー配布のトリガーとなることが多いという報告がありました。会場から、ポリシー配布のみでなく、ベースとなっているRFC3484のアドレス選択機構自体の検討も進めてほしいという意見がありました。今後、配布に使用するプロトコルの検討等、さらに議論を進めていくとのことです。

5.「短命IPv6アドレスの提案」は、IPv6の新たなアドレスとして、アプリケーションが短時間だけ利用する「短命IPv6アドレス」を定義しようという提案です。従来、匿名性等を担保するために、ランダムなアドレスを一定期間利用する、一時アドレス（RFC4941）が定義され、既にWindows Vista等で利用されています。今回提案された「短命IPv6アドレス」は、アドレスの有効期限をさらに短く、アプリケーションが通信する“セッション”毎とすることで、匿名性を向上させ、アドレスが外部に漏れることから発生するセキュリティ問題を防ごう、というものです。発表では、実装して試験をし、問題がないとのことでしたが、会場からは、短時間でアドレスを大量に使用する場合、ルータ等のNDキャッシュへの影響が大きいことや、セッション毎にアドレスが変わるとなると、現在、サーバ側は、同じノードは同じアドレスを使っているという前提で動いているものがあるため、通信のセマンティクスが変わってしまう、といった意見が出されました。

7.の「ドメイン名を利用したインタフェース選択」では、複数のネットワークインタフェースを持ち、別々のネットワークに同時に接続しているノードが通信をする場合、通信先のネットワークを選ぶ際にドメイン名を利用することを提案しています。それぞれのネットワークがDNSサーバアドレスをノードに伝える際、ドメインサフィックスも同時に伝え、そのドメインサフィックスに該当する名前解決、通信は、該当するインタフェース向けに実施しようというものです（日本では、NTT東西の提供するアクセス網にて、同様の技術がアドホックに利用されています）。この提案に対しては、利用環境に関する質問や、既存の経路制御を利用することで実現可能であるといった議論が実施されました。

それぞれの新提案については、継続議論となっています。

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

□第73回IETF 6man WGのアジェンダ
http://www3.ietf.org/proceedings/08nov/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。今回は火曜日の午後最初のコマにて、ミーティングが実施されています。参加者は、150名程度に見受けられました。

前回ダブリンで開催されたIETFでは、IPv6/IPv4の共存技術であるIPv6トランスレータに関する議論が長時間にわたって実施されましたが、2008年10月1日と2日にカナダのモントリオールにて開催されたsoftwire、v6ops、behave、intareaの各WG合同のIPv4-IPv6共存中間ミーティングでの議論の結果を受け、実際のプロトコル策定議論は、behave WGとsoftwire WGにて実施されることになりました。

今回は、

1. 不正ルータ広告への対応に関する提案
2. CPEルータの仕様に関する提案
3. Teredoの拡張に関する提案
4. サイト境界ルータ発見プロトコルと経路制御に関する提案
5. スウェーデンにおけるIPv6利用の紹介
6. Google社におけるIPv6統計情報の紹介

の六つの項目の議論がありましたが、最後の2点は状況紹介であり、v6opsで扱う議論項目が急に少なくなってしまった感がありました。ここでも、このうち重要な議論について、ご説明します。

セッションは、チェアからのWG文書5点に関するステータス報告から始まりました。WG文書を含め、現在v6ops WGで扱っている内容は、セキュリティに関する話題が多くなっています（上記5点のWG文書のうち3点が、CPEルータ、ルータ広告、トンネル機構のそれぞれのセキュリティに関する検討となっています）。

1.の「不正ルータ広告への対応に関する提案」は、ここ数回議論が続いています。今回議論された対象は、要求条件ドラフトに関するもので、前回のIETFでWGアイテムとして認定された文書の改版です。この要求条件ドラフトと、解法の一つであるRA Guardの双方のドラフトについて、WGラストコールが実施されることになりました（執筆時（2008年12月時点）において、既にMLでのラストコール期間は終了しています）。

2.の「CPEルータの仕様に関する提案」に関しても、ここ数回継続的に議論されています。前回IETFのWGミーティングにおいて、この提案は重要であるとの合意は得られましたが、内容的に不足点が多く、WG文書化は見送られていました。今回の改版で、モデルや環境の追記、不必要と指摘された記述の削除、IPv4からの移行/共存に関する記述の追記等を実施し、WG文書として今後検討を継続することとなりました。3.の「Teredoの拡張提案」は、Teredoを改良し、より多くの種類のIPv4 NAT環境下で動作するようにしたことについて、非常に詳しい解説がありました。こちらは、v6opsで扱う内容を超えるものがあるため、intareaにて議論が継続されますが、v6opsでもWGラストコールがかかる予定です。

5.「スウェーデンにおけるIPv6利用の紹介」と6.「Google社におけるIPv6統計情報の紹介」は、IPv6のトラフィック状況などに関する報告です（5.は、IEPGで報告されたものと同じものです）。6.は、Google社のサービス向けのトラフィックからIPv6の普及度合いなどを測定したもので、測定手法の紹介、IPv6浸透の状況について多角的に報告がありました。これによると、IPv6の普及度合いが高いのはロシアやフランスで、日本はかなり下位となっています。私見ですが、日本の普及度合いが低く測定されている原因としては、計測トラフィックの60%程度が6to4であり、IPv6ネイティブアドレスがついている場合や、IPv4グローバルアドレスが端末に直接付与されない場合には6to4機構が利用されないことから、環境的な問題ではないかと思われます。Google社の報告の結論としては、IPv6の普及度は低いものの、増加傾向であること、現状では6to4がIPv6移行プロトコルの主流を占めることが述べられています。

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

□第73回IETF v6ops WG のアジェンダ
http://www.ietf.org/proceedings/08nov/agenda/v6ops.txt

■ 第73回IETFミーティングの会場であるHilton Minneapolis

◆behave WG（Behavior Engineering for Hindrance Avoidance）

behaveという名前からはちょっと想像が難しいですが、behaveはIPv4で広く普及しているNATの挙動を定義するワーキンググループです。標準仕様が定義されないままに広く普及してしまったNATにはさまざまな実装があり、NATトラバーサルの処理が複雑化しEnd-to-End通信を阻害してしまうことになるため、NATの実装をBCP（Best Current Practices）として文書化するというのが主な目的です。

今回の第73回IETFの会期中に、behaveのセッションは3回行われました。これまでのbehaveで扱っていたNATに関係する各種提案に加え、2008年10月にモントリオールで行われたIPv4-IPv6共存中間ミーティングで提案されたIPv4とIPv6の共存技術のうち、IPv4-IPv6トランスレーションに関する方式をbehaveで扱うことになったため、三つのスロットを取って議論が行われました。また、中間ミーティングで検討された技術のうち、トンネル方式をベースとしたものはsoftwireにて議論が行われました。

behaveで行われた、IPv6とIPv4の在庫枯渇対策に関係する議論としては以下のものがありました。

・IPv4-IPv6トランスレーションに関する提案
draft-baker-behave-v4v6-framework
draft-baker-behave-v4v6-translation
draft-bagnulo-behave-nat64
draft-bagnulo-behave-dns64
draft-vogt-durand-virtual-ip6-connectivity

・大規模NATに関する提案
draft-nishitani-cgn
draft-shirasaki-nat444-isp-shared-addr

・ユーザー毎に使用できるポートを制限する提案
draft-ymbk-aplusp
draft-bajko-v6ops-port-restricted-ipaddr-assign
draft-boucadair-port-range
draft-despres-sam
draft-boucadair-dhc-port-range

・IPv6 NATの提案
draft-mrw-behave-nat66

IPv4-IPv6トランスレータとしては最初に、Fred Baker氏から中間ミーティングでの議論の結論として、NAT64方式とIVI方式が統合されてトランスレーション方式のベースとなり、トランスレーションに関する機能毎にドキュメントを分割して検討していくという、トランスレーション方式の検討のフレームワークについて説明がありました。ドキュメントとして、全体のフレームワークについて記述したドラフト、パケットの変換ルールを規定したSIIT（RFC2765）の更新について記述したドラフト、ステートフルアドレス変換方式への拡張（今のところIPv6からIPv4への変換方式のみ）について記述したドラフト、DNS ALGでのアドレス合成について記述したドラフト、そしてその他の要素（FTP ALG等）について記述したドラフトという構成になっています。

アドレス変換方式に関する議論としては、対象とするトランスポートプロトコルがTCPやUDPだけになっているが、SCTP、DCCPやIPSecなどの新しいプロトコルは考慮しなくていいのかという質問がありましたが、SCTP、DCCPやIPSecなどのプロトコルは変換方式についての議論が尽くされておらず、別のドラフトとして進めるという意見が大勢を占めました。

大規模NATに関してはKDDI株式会社の中川あきら氏より発表があり、4-4NATや6-4NATなど各種のアドレス変換をISPや企業網で利用する場合に共通して必要となる機能を整理した提案と、4-4-4NATすなわち、IPv4 NATを2回行うモデルに関する提案がありました。また、この4-4-4モデルを利用する際の、ISPの空間で利用するアドレスについて、本提案ではISPで共有できるアドレスブロックの新設を提案しており、その議論はintareaのセッションにて別途行われました。

同じくIPv4アドレス在庫枯渇に関する技術として、ユーザーにIPv4グローバルアドレスを付与するが、利用できるポート範囲を制限するというA+Pと呼ばれる方式がRandy Bush氏より提案されました。本方式のメリットとしては、ユーザーがISPのNATの配下に収容されるのではなく、利用は制限されるものの、あくまでグローバルIPv4アドレスがユーザーに付与されるため、End-to-Endの透過性が保持されるというものです。しかし、ISP内でのルーティングや、ユーザーが使用しているルータや時には端末への変更が必要であり、実際に利用するにはクリアすべき障壁の多い方式になっています。

また、3回目のセッションではMargaret Wasserman氏とFred Baker氏より、NAT66、つまりIPv6からIPv6へのNATに関する発表がありました。IPv6の設計思想の一つとして、IPv4で現在広く使用されているNATを使わないようにする、というものがありましたが、本提案の趣旨としては、IPv6においてもなおNATを必要とするケースがあることから、IPv6 NATを実装し利用する人々が出てくることは不可避であり、そこでIETFとしてはIPv4 NATのような標準仕様のない混沌とした状況を生み出さないためには、IPv6 NATの標準仕様を策定する必要がある、という論調になっています。

具体的な適用先としては、企業ネットワークなどが挙げられ、特にネットワーク間を接続する際にトポロジーの隠蔽が必要であり、双方向のNATが必要である、などの提言がありました。NATを利用しないためにIPv6を標準化し、普及を推進してきたIETFとしては、非常に重要なトピックであり、さまざまな議論が交わされました。否定派の意見としては、IETFでNAT66がRFCになることで、NAT66の普及を促進してしまうのではないか、IPv6でのセキュリティ実現方法について記述したLNP（RFC4864）でカバーできているのではないか、といった意見がありました。その場でのディスカッションでは、肯定否定というのではなく慎重派が多いように見受けられましたが、結論としては本提案内容をベースとして議論を継続することになりました。

□v4v6interim
http://trac.tools.ietf.org/area/int/trac/wiki/v4v6interim

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

□第73回IETF behave WGのアジェンダ
http://www.ietf.org/proceedings/08nov/agenda/behave.html

◆intarea（Internet Area Open Meeting）

先にbehaveの項でも触れましたが、ISP等でNATを行う場合にNAT配下で利用するアドレスとして、ISP共有アドレス（ISP Shared Address）の新設に関する提案がKDDI株式会社の中川氏よりありました。NAT配下で利用するアドレスとしては、RFC1918で定義されるプライベートアドレスを利用することが一般的ですが、ISPでこのアドレス空間を使った場合に、ユーザーが設置するNAT装置配下で利用するアドレス空間とバッティングする可能性があり、通信障害が発生するため別のアドレスブロックが必要であること、またISP共有アドレスとしてどの程度の大きさのアドレスブロックが必要か、などの説明がありました。この提案に関する議論としては、現在利用されていないクラスE（240/4）の空間を利用してはどうか、ISPによっては際限なく大きなアドレス空間を要求するのではないか、ISP共有アドレスを利用している複数のISPにマルチホームしている場合にはやはり通信障害が発生するのではないか、といったものがありました。その場の結論としては、メーリングリストで継続して議論を行うということになりました。

また、これらのIPv4アドレス在庫枯渇、IPv6への移行といった一連のトピックに関して、今回の第73回IETFと次回のIETFとの間に、マルタ島にて中間ミーティングを開催して集中議論を行うことが計画され、参加者数の調査などが行われていたのですが、3回目のセッションにおいて、マルタ島での中間ミーティングはキャンセルになったことが発表されました。中止の理由としては十分な参加者数が期待できないことが主だと思われますが、場所を移して中間ミーティングが行われるかもしれないとのことでした。

□第73回IETF intareaのアジェンダ
http://www.ietf.org/proceedings/08nov/agenda/intarea.txt

第73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（議事録も今後掲載される予定です）。

□全体プログラム、WGアジェンダ、発表資料
https://datatracker.ietf.org/meeting/73/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）
（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

本稿では、インターネット経路制御のセキュリティ・アーキテクチャ策定に取り組んでいるSIDR WG（Secure Inter-Domain Routing WG）と、認証基盤技術であるX.509を使って、インターネットで使われるPKI技術の策定に取り組んでいるPKIX WG（Public-Key Infrastructure（X.509））について報告いたします。

◆SIDR WG（Secure Inter-Domain Routing WG）

SIDR WGは、インターネットにおけるドメイン間（AS間）の経路制御に関して、セキュリティ・アーキテクチャの検討を行っているWGです。第73回IETFでは、2日目（11/17）の13:10から2時間ほどミーティングが開かれ、約50名の方が参加しました。

SIDR WGはまだRFCを出しておらず、Internet-Draft（以下、I-D）が10あります。今回、さらに二つのI-Dが出されました。

□BGP Prefix Origin Validation
http://tools.ietf.org/html/draft-pmohapat-sidr-pfx-validate-00

RPKI（Resource PKI）を背景に、BGP UPDATEメッセージの検証における有効性を提案しているドキュメントです。大手ベンダーであるCisco社やJuniper社に加え、日本のISPであるNTT Communications社やIIJ社からの参加者が議論に参加しています。

□Securing RPSL Objects with RPKI Signatures
http://tools.ietf.org/html/draft-kisteleki-sidr-rpsl-sig-00

WHOISデータベースの記述言語であるRPSL（Routing Policy Specification Language）に、電子署名を加える提案です。電子署名のためにリソース証明書が使われます。RPSLを策定しているRIPE NCCの、スタッフによって提案されています。

ミーティングでは、アジェンダに従って、三つのWGドキュメントについて議論されました。

□Secure Inter-Domain Routing WG（sidr）（アジェンダ）
http://www.ietf.org/proceedings/08nov/agenda/sidr.html

SIDR WGにおける議論を私なりに分類すると、以下の三つに分けられます。この分類を使って、今回のSIDR WGで議論が行われた三つのI-Dを紹介したいと思います。

a. RPKIのアーキテクチャ

全体的なアーキテクチャで、このPKIの目的や信頼の構造に関する議論です。

b. RPKIの認証局

リソース証明書を発行する認証局に関する議論で、IPアドレスの管理業務との関係や、レジストリ同士の連携も関連します。

c. ROA（Route Origination Authorization）を使ったprefixの検証

リソース証明書に基づいて発行されるROAと、経路情報の関係を明確化し、目的とするセキュリティを担保するための議論です。

最初のアジェンダである“RPKI Architecture”は、aに分類されます。WGでは、経路フィルタやトラストアンカーについて、ドキュメントにどう記述するかが議論されました。最終的にどちらも具体化せずに、一般化した記述にすることになりました。五つのRIRがトラストアンカーになることを前提とするような記述は、避けられることになりました。

□RPKI Architecture
http://tools.ietf.org/html/draft-ietf-sidr-arch-04

二つ目の“ROA Format”は、cに分けられます。BGP UPDATEのprefixを検査する段階で、ROA（Route Origination Authorization）とのオーバーラップをどのように扱うかについて議論されました。その結果、現行の記述は変更しないことになりました。

□ROA Format
http://tools.ietf.org/html/draft-ietf-sidr-roa-format-04

三つ目の“Certificate Policy”は、bに関連したドキュメントです。リソース証明書を発行するRPKIのCertificate Policyについて提案しています。主にRIRにコメントが求められていますが、IETFの場であることに加えて、ドキュメントの内容がビジネス判断を伴うものであったりする理由で、なかなか十分なコメントを得られていません。

□Certificate Policy
http://tools.ietf.org/html/draft-ietf-sidr-cp-04

WGのメーリングリストでは、bogon prefix※1を示すROAに関する議論などが行われています。

3年前から始まったSIDR WGですが、目標としているアーキテクチャに対して、徐々にドキュメントが揃ってきた印象があります。これも2007年度にAPNIC、ARIN、RIPE NCCの三つのRIRでプロトタイプシステムが作られ、上記のbが、現実味を帯びてきたからかもしれません。

ただし、ROAとリソース証明書をBGPスピーカーがどのように経路制御に反映するのか、という大きな課題が残っています。ベンダーやISPを交えた議論が、今後も必要とされていくと思われます。

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

PKIX WGは、X.509を使ってインターネットで使われる、PKI技術の策定に取り組んでいるWGです。PKIX WGは新たなドキュメントを扱わず、近々クローズすると宣言されたことが4年程前にありましたが、暗号アルゴリズムの移行や、TAM（Trust Anchor Management）など、WGの活動項目が減る様子はありません。ミーティングは11/21（金）の15:20から2時間行われました。50名程の参加者がありました。

前回の第71回IETF以降、RFCになったドキュメントは無く、二つのドキュメントがIESGのレビューを受けている状態です。ECC Subject Public Key Informationは、2008年11月24日にレビュー状態からAD（Area Director）の最終判断を待つ状態になりました。

- ECC Subject Public Key Information
  http://tools.ietf.org/html/draft-ietf-pkix-ecc-subpubkeyinfo-10

  証明書にECC（Elliptic Curve Cryptography - 楕円暗号）の鍵を入れるためのパラメーターを定義しています。

- RFC4055 update
  http://tools.ietf.org/html/draft-ietf-pkix-rfc4055-update-01

  証明書でRSAES-OAEP（RSA Encryption Scheme - Optimal Asymmetric Encryption Padding）を使うため、暗号アルゴリズムを定義しているRFC4055を更新するための変更点を述べています。

PKIX WGには、WGで議論することになっているI-Dが11あります。このうち9のI-Dについて議論が行われました。その他に“関連する仕様やリエゾンのプレゼンテーション”として、二つのプレゼンテーションがありました。主だったドキュメントの動向を報告します。

- Other-certs extension
  http://tools.ietf.org/html/draft-ietf-pkix-other-certs-01

  単一のEE（End Entity - 証明書の発行対象）に発行された、複数の証明書の、証明書同士を関連付ける証明書拡張です。若干の修正の後、WG Last Callにかけられることになりました。

- PKI resource Query Protocol
  http://tools.ietf.org/html/draft-ietf-pkix-prqp-01※2

  認証局証明書とリソースID（OCSP、LDAP、CRLなど）を使って、アクセスするためのURIを問い合わせるプロトコルです。問い合わせる先のRQA（Resource Query Authority）のアドレスをクライアントにどう伝えるのか、といった議論がありました。PRQPを実装しているプロジェクトがあります。

□OpenCA Research Labs - LibPRQP Project
http://www.openca.org/projects/prqpd

- Attribute Certificate Profile Update
  http://tools.ietf.org/html/draft-ietf-pkix-3281update-01

  属性証明書を策定したRFC3281の、Errata（修正）対応です。数年来のErrataを反映し、新たなRFCとして更新しようとしています。

- Traceable Anonymous Certificates
  http://tools.ietf.org/html/draft-ietf-pkix-tac-01

  名称（CN）にハッシュ値を記述し、匿名性を担保しつつ、後でEEと証明書の関係を追跡できるようにした証明書です。韓国のKISA（Korea Information Security Agency:韓国情報保護振興院）の方々による提案です。

“関連する仕様やリエゾンのプレゼンテーション”として、OCSPにおけるハッシュアルゴリズムの移行に関する状況と、タイムスタンププロトコルに関するRFCの更新について議論が行われました。

- OCSP Algorithm Agility
  http://tools.ietf.org/html/draft-hallambaker-ocspagility-02

  オンラインで証明書の有効性を問い合わせるOCSP（Online Certificate Status Protocol）の、レスポンスの中で使われるアルゴリズムの移行に関する議論です。

  返答する側（レスポンダー）が、問い合わせた側（リクエスター）のサポートしていない署名アルゴリズムを使ってしまうことを避けるため、アルゴリズムを選ぶ方法について議論が行われました。WGの活動項目としてMLで意見が求められることになりましたが、この議論は1年程前にも行われたことがあり、進んでいない様子がうかがわれます。

- Time-Stamp Protocol update - 3161bis

  ETSIのTC ESI（Technical Committee Electronic Signature & Infrastructure）の要望を受けて、更新するための活動が行われています。WGの活動項目に入れるかどうかの議論が行われ、ドキュメントに含まれる八つの特許についての記述を、削除することの賛否が問われました。その結果、削除するべきであるという方向になりました。

◇　　◇　　◇

先日行われたInternet Week 2008でも、「次世代暗号アルゴリズムへの移行～暗号の2010年問題にどう対応すべきか～」というセッションがありました※3。利用する暗号アルゴリズムを切り替えるには、プロトコルとして切り替えが可能になっていなければなりません。また、並行して、認証局や認証システムの対応も必要になってきます。これらの状況を踏まえ、安全性を維持しつつスムーズに移行できるよう、2009年も引き続き議論を進められればと思います。

（JPNIC 技術部/インターネット推進部　木村泰司）

※1 bogon prefix
割り振られていないIPアドレスなど、本来はインターネットの経路表に載るはずの無いprefixのこと。

※2 PKI Resource Query Protocol（PRQP）
2008年12月8日に修正版の“-02”になりました。
http://tools.ietf.org/html/draft-ietf-pkix-prqp-02

※3 次世代暗号アルゴリズムへの移行
～暗号の2010年問題にどう対応すべきか～
https://internetweek.smartseminar.jp/public/session/view/40

2008.12.3▶12.6

IGFハイデラバード会合報告

今年で第3回となるインターネットガバナンスフォーラム（IGF）が、2008年12月3日（水）から12月6日（土）まで、インドのハイデラバードで開催されました。

IGF自体がどういうものであるか、現在までの流れに関しては、第1回アテネ会合、第2回リオデジャネイロ会合に関する、メールマガジンの記事※1をご覧ください。

今回のハイデラバード会合は、会期直前の11月26日にムンバイで発生した同時多発テロの影響で、波乱含みでした。オープニングセッションはテロ被害者への黙祷で始まり、全てのスピーチは被害者に対するお悔やみから始まりました。

日本では多くの企業が社員のインドへの渡航を禁止したため、日本からの参加予定者の半数以上が出席を取りやめました。欧米からの出席取りやめも少なくなく、セッション主催者が直前に登壇者の再調整を行っている姿も目立ちましたが、全体としてみますと、公式発表による参加者数は94ヶ国から1,280名と例年並みの水準でした。会場となったHICC - Hyderabad International Convention Centreは街中の雑踏が嘘のようで、最新の施設に国連主催会議独特の厳重な警戒で、テロの危険を感じることはありませんでした。

会議は、一つのメインセッションと複数のワークショップが同時に進行する形式で進みました。これは過去のIGFと同様です。一方で、メインセッションの形式は大きく変わりました。

■ セッションの様子

第1回、第2回は、主要テーマ（第2回では五つ。開放性、セキュリティ、多様性、アクセス、重要インターネット資源）ごとに1セッションで完結するように構成されていましたが、今回は、午前中をパネルディスカッションとして、パネリストによる発表とパネルの中での議論を中心としたセッションを配置し、午後はオープンダイアログと称して、午前中のパネルディスカッションで得た共通認識を前提に、フロアからの意見を数多く集める形式を取りました。

□2008 IGF Hyderabad Programme
http://www.intgovforum.org/cms/index.php/hyderabadprogramme

第1回会合では、パネリスト、聴衆ともに短く簡潔な意見を多数取り上げるように、モデレータによって注意深くコントロールされている感じがありましたが、今回はもう少しラフな、インターネット系の会合で見慣れた感じとなりました。


IGF meet tomorrow

Special Correspondent

HYDERABAD: Internet Governance Forum (IGF), with about 1,500 participants from 100 countries, will begin its brainstorming on several critical issues like reaching out to the next billion, promoting cyber security, and managing critical Internet resources, will begin here on Wednesday.

Addressing a press conference here on Monday, Under Secretary-General of United Nations, Marcus Koomer, the chief nodal agency for the conduct of IGF, said that the Hyderabad edition was the third in series after Athens in 2006 and Rio De Janeiro in 2007.

"Internet for all" was the main theme, as providing access to all was the main ob-

10,000 institutions of higher learning in the country to be networked as part of National Knowledge Network

would have to be moved from IP version 4 to IP version 6 to accommodate much more, including route servers, technical standards, and telecom infrastructure.

e-readiness

The IGF might not come up with any declaration, but it would make efforts to ensure e-readiness of the world, particularly the developing world.

The forum would provide a

Water

Situation to co

Staff Reporter

HYDERABAD: There is no option but to bear with the slow down in traffic movemen from NFCL rotary to Punj gutta graveyard, at least f one more month.

Digging of the road at t points on this small stretch lay drinking water pipel has resulted traffic su during peak hours. As per original plan, width of road was supposed to b creased by taking space the graveyard.

The graveyard's old pound wall was demo and new road was laid widening the road to modate nearly dou present volume of tra

Just when the wor completion and c began to feel that t

■ IGFの開催を伝える新聞記事

ワークショップは数が多く、同時に8セッションが並行して開催されるため、一人で全体像をつかむことは不可能です。私は、重要インターネット資源（Critical Internet Resource）に関するセッションを選んで見ていくことにしました。重要インターネット資源というテーマの下には、IPアドレス、特にIPv6とIPv4アドレス在庫枯渇の問題、ドメイン名管理、ICANN体制自体といった内容のセッションが並んでいます。

「IPv4からIPv6への移行 Transition from IPv4 to IPv6 」と題されたメインセッションには、総務省データ通信課の柳島智企画官が登壇され、総務省研究会※2や、IPv4アドレス枯渇対応タスクフォースなどの取り組みの紹介がありました。今までこういうセッションでは、IPv6対応において進んでいる組織がその対応状況を自慢げに語るか、逆にIPv6対応の難しさを嘆くかの両極端の論調ばかりが目立っていた感じがありますが、スウェーデンのIXであるNetnod社（http://www.netnod.se/）のKurtis Lindqvist氏、Nokia Siemens社のJonne Soininen氏などヨーロッパからの登壇者は、IPv4アドレス在庫枯渇を現実問題として捉え、どう解決するべきなのかという観点から、IPv6を真剣に考えていることがうかがえました。

ICANN体制自体に関しては、ICANNと米国商務省との間のJoint Project Agreement（JPA）に関するワークショップが開催されました。ここがまさに、WSIS（世界情報サミット）で大論争となったテーマ※3であるわけですが、米国政府の関与に反対意見を示す人はいるものの、紛糾には至らず淡々とセッションが進んでいきました。


■ 会場入り口では厳重なセキュリティ対策が取られていました

最後に、全体を通して印象に残ったことを述べます。

IGFに関して、いくつかの地域ではリージョナルなIGFを組織する動きがあるようです。活発な例が英国のUK IGF（http://www.ukigf.org.uk/）で、国会議員までこれに関与し、今回数名の国会議員がハイデラバード会合に参加するとともに、フロアから積極的に意見を述べていました。

サイバーセキュリティやグリーンITなど、新たなテーマを付け加えつつも、大枠としては3年間同じような議論が繰り返されている感じもします。ワークショップは背景説明に終始しているものもあり、IGFが設定した壮大なテーマに対する進捗の難しさを感じます。

一方で、チュニスアジェンダによって設定されたIGFの活動期間は5年間であり、3年目となる今回は折り返し地点となるため、依然試行錯誤は続いているものの、2年後の着地点を意識するような発言も複数見受けられました。これからの2年間は、ICANNのJPA満了と合わせて、注視が必要です。

（JPNIC IP事業部 前村昌紀）


■ 会場に設置された国連旗

※1 JPNIC News & Viewsバックナンバー
vol.408 IGFアテネ会合報告
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2006/vol408.html
vol.421 IGFを振り返る
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2006/vol421.html
vol.500 IGFリオデジャネイロ会合報告
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2007/vol500.html

※2 インターネットの円滑なIPv6移行に関する調査研究会
http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/ipv6/

※3 JPNIC News & Views vol.316［特集］世界情報社会サミット（WSIS）報告
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2005/vol316.html