Internet Topics
インターネット・トピックス ～関連団体の動向～

2009.8.25▶8.28

APNIC28ミーティング報告

■ アドレスポリシー動向

［関連記事］P.28「第17回JPNICオープンポリシーミーティング報告」

今回北京で行われたAPNIC28ミーティングは、中国のNIRであるCNNICがローカルホストを務め、2009年8月25日（火）～28日（金）の4日間で開催されました。

会場となったホテル、Grand Hyatt Beijingは、天安門広場から徒歩15分ほどの街の中心にあり、会議に参加しながらも短い観光ができ、街の雰囲気を味わうことのできる環境となっていました。

参加者は51組織、272名（APNIC26では70組織、237名）と、昨年の単独開催（APRICOTとの併催型でなかったAPNIC26）と比較した場合、組織単位での参加者数が昨年よりも多かったことが特徴です。

数年前まではAPNICミーティングというと、アドレスポリシーの提案について議論を行うカンファレンスとのイメージが強くありましたが、現在はAPOPSやIPv4アドレスの在庫枯渇/IPv6の実装などをテーマにしたテクニカルセッションも主なプログラムとして組み込まれ、地域内でオペレーショナルな情報を共有/議論できる構成になっています。

□Program Highlights

トレーニング、APOPS、各種プレナリー、ポリシーSIG（およびNIR SIG）、APNIC総会、レセプション/懇親会
http://meetings.apnic.net/28/program/

今回はやはり地元である中国からの発表が普段よりも多く、オペレーション面では、4バイトAS番号の対応に向けた情報提供や、IPv6の実装について具体的な事例紹介、また、時事ネタとして2009年7月のDDoS攻撃の事例が紹介されていました。

本稿ではアドレスポリシー提案の結果を中心にお伝えします。オペレーション面での内容については、P.35の「APOPSにおけるオペレーター向けの話題」をご覧ください。

◆APNIC28でコンセンサスの得られたポリシー提案

前回までの流れから見ると、IPv4アドレス在庫枯渇に向けた対応、IPv6アドレスの取得における障壁に向けたポリシー面での対応は一段落したと考えていたので、あまり多くの提案が提出されないことが予測されていました。

しかし、結果としては今回のミーティングでは、ポリシーSIGにて7点の提案が提出されました。そのうち、コンセンサス※1の得られた提案は、次の4点です。

テーマとしてはIPv4アドレスの移転、IPv4保有者に対するIPv6の分配手続きの簡素化が注目され、残り2点のAS番号に関する提案も、現状の2バイトAS番号の利用状況を見据えて必要な施策として支持されました。

コンセンサスの得られた提案

prop-050：IPv4アドレスの移転
http://www.apnic.net/policy/proposals/prop-050
（＊）提案の背景については、JPNIC News & Views vol.623※2の特集記事内、「prop-050 IPv4アドレス移転の提案」を参照ください。

移転元、移転先、両者の合意があれば、以下の要件でAPNICから直接分配を受けているIPv4アドレスの移転（最小移転単位/24）を認める。
（1）移転元は、移転後12ヶ月はAPNICへ追加のアドレス申請を行うことができない。ただし正当な事情があることを証明すれば、当該期間内の申請も可能。
（2）APNICのIPv4アドレス在庫枯渇前は移転時に利用状況の審議を行う。枯渇後は、審議は行わない。

prop-073：現IPv4保有者を対象としたIPv6アドレス申請手続きの簡素化
http://www.apnic.net/policy/proposals/prop-073
（＊）旧題:IPv4アドレス保有者へのIPv6の自動的な割り振り/割り当て

IPv4アドレスの分配をAPNICから直接受けている組織は、IPv6においても同じく分配対象と想定されており、当該組織が分配を必要とする意思表明をすれば、それ以上の審査をすることなく、以下のIPv6の分配を行う。
（1）IPv4の割り振りを受けている場合:IPv6/32を割り振る。
（2）IPv4の割り当てを受けている場合（＊）:IPv6/48を割り当てる。
（＊）歴史的PIは対象外

prop-074：4バイトAS番号の分配に関するIANAからRIRへのAS番号割り振りポリシー
http://www.apnic.net/policy/proposals/prop-074

IANAからRIRへ2バイトから4バイトを区別してAS番号を割り振る期間を2009年12月31日→2010年12月31日に1年間延長する。
グローバルポリシーとして全RIRにて提案中。

prop-075：歴史的経緯を持つAS番号の有効利用
http://www.apnic.net/policy/proposals/prop-075

経路広告されておらず、利用意思の確認できない歴史的経緯を持つAS番号を回収する。歴史的PIアドレスの回収と基本的に同じ手続きとする。

◆ポリシー提案の結果について

今回のミーティングにあたって参加者が最も気にかけていたのは、2007年から議論を行っているIPv4アドレス移転の提案に対する結果でした。

また、「prop-073 現IPv4保有者を対象としたIPv6アドレス申請手続きの簡素化」提案も当初は懸念の方が強かったものの、コミュニティメンバーの意見を反映した形で提案内容が見直され、コンセンサスが得られる結果となりました。

移転提案については、前回のAPNIC27（マニラ）では、ミーティングのコンセンサスは得られたものの、その後のメーリングリストでの議論により、最終的な結論としては「継続議論」となり今回に持ち越されたため、提案者も、前回のミーティングで提案を支持していた参加者も、今回こそは正式な決定に至りたい、という気持ちがあったと思います。

事前に行われていたメーリングリスト上での議論の争点は、IPv4アドレス在庫枯渇前の、移転目的でのAPNIC在庫消費/再移転を目的とした移転アドレスの取得防止に向けた要件設定でした。意見の異なるコミュニティメンバーが自主的に調整し、合意できる要件を見つけられたため、ミーティング当日は大きな反論もなくスムーズに参加者のコンセンサスが得られる結果となりました。

国内での施行については、2009年11月26日（木）開催のJPNICオープンポリシーミーティングで議論をいたしました。議論の詳細については、P.28の「第17回JPNICオープンポリシーミーティング報告」をご覧ください。

また、prop-073に基づき、IPv6の割り振り申請手続きが簡素化されることにより、これまでよりも申請時の負荷が軽減されると考えられます。国内においては、具体的にIPv6の実装を予定している組織であれば、既存の要件でIPv6アドレスを取得済みであるケースが多いと考えられ、具体的な障壁となっているとの意見はありませんで

■ 会場となったGrand Hyatt Beijing

■ Opening PlenaryでスピーチをするAPNICのPaul Willson氏

した。しかしながら、まずはアドレスを取得しようと考えている組織にとっては、これまでよりも申請が行いやすくなるのかもしれません。

◆ミーティング後のプロセス

8週間のメーリングリストでのコメント期間中に、特筆すべき懸念が表明されなかったため、定義されたプロセス※3に従って、これらの提案はAPNICにおいて正式に承認されました。

◆次回のAPNICミーティング

次回はAPRICOTカンファレンスプログラムの一部として、2010年3月にマレーシアのクアラルンプールで行われる予定です。

□APNIC29 kuala Lumpur
http://meetings.apnic.net/29

◆参考情報

□APNIC28 -Beijing 2009
http://meetings.apnic.net/28

□その他APNIC28におけるポリシー提案

継続議論となった提案：

prop-076：IPv6追加割り振り申請時における経路集約の要件追加
http://www.apnic.net/policy/proposals/prop-076
JPOPM16でのコンセンサスに基づいた提案。

http://venus.gr.jp/opf-jp/opm16/jpopm16-p1-v1.pdf
IPv6追加割り振り申請時にも、初回申請時と同じく、ポリシー上、割り振りIPv6アドレスを単一の経路に集約することを求める。

提案者へ差し戻しとなった提案：

prop-077：歴史的経緯を持つPIアドレスにおける移転に関する移転要件の補完
http://www.apnic.net/policy/proposals/prop-077
APNICと契約/費用支払い関係にない歴史的PIは、LIR管理下に移転することが認められている。当該アドレスの移転要件もprop-050と統一することをめざしている。なお、JPNIC管理下の歴史的PIは、すべて合意書締結済みのため対象外。

prop-078：IPv6の実装を前提として分配するIPv4アドレスのための/10 IPv4アドレス空間の確保
http://www.apnic.net/policy/proposals/prop-078
IPv6の実装を前提としたIPv4アドレスの分配専用に、APNICの最後の/8在庫のうち、/10を別途リザーブする。

（JPNIC IP事業部 奥谷泉）


■ NIR SIGでは、chairに筆者（写真右端）が、co-chairにWei Zhao氏（写真中央）が選ばれました

※1 コンセンサス
JPNICやAPNICのポリシーフォーラムにおける「コンセンサス」とは、特定の提案事項に対するコミュニティの「総意」を意味します。そして、コンセンサスに至った提案はJPNICやAPNICのポリシー、またはIPアドレス登録管理業務に反映、施行されます。

※2 JPNIC News & Views vol.623
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2009/vol623.html

※3 APNIC地域におけるポリシー策定プロセス
http://www.apnic.net/community/policy/process

■ APOPSにおけるオペレーター向けの話題

本稿では、APNIC28ミーティングの中で開かれた、The Asia Pacific OperatorS Forum（APOPS）※1について報告します。APOPSは、AP地域のインターネット・オペレーターを対象とした技術的な話題を扱うフォーラムで、APNICミーティングで開催されるプログラムの一つとして開催されています。APNIC28ミーティングでは、2日目の2009年8月26日（水）午前11時から15時半にかけて開催され、約90名が参加しました。

今回のAPOPSは、特にテーマが限られておらず、NAT、IPv6、AS番号、DNSSEC、DDoSといったさまざまな話題のプレゼンテーションが行われました。日本からは、川村聖一氏（NECビッグローブ株式会社）、芦田宏之氏（イッツ・コミュニケーションズ株式会社）、外山勝保氏（インターネットマルチフィード株式会社）の3名が、プレゼンテーションをされていました。

APOPSの議題

（午前の部）

- “DNSSEC deployment in New Zealand”
  Andy Linton氏（Victoria University of Wellington）
- “IPv6 representation”
  川村聖一氏（NECビッグローブ株式会社）
- “Careful planning is needed for introducing NAT”
  芦田宏之氏（イッツ・コミュニケーションズ株式会社）
- “Challenges in Large IP network deployment”
  Echo Liu氏（WANDL社）
- “The strategic value of introducing IPv6”
  Cancan Huang氏（China Telecom社）

（午後の部）

- “APIX Update”
  外山勝保氏（インターネットマルチフィード株式会社）
- “AS number report”
  Geoff Huston氏（APNIC）
- “DITL”
  George Michaelson氏（APNIC）
- “7.7 DDoS cyber attack in Korea”
  Ji-Young Lee氏（KRNIC/KISA）
- “The Emperor's New Cloud: An Analysis of the July 2009 RoK/USA DDoS Attacks”
  Roland Dobbins氏（Arbor Networks社）

本稿では、これらのプレゼンテーションのうち、DNSに関するトピックを二つとセキュリティに関するトピックを一つ、合計三つについて報告します。

◆DNSSEC deployment in New Zealand

Andy Linton氏から、ニュージーランドのccTLDである、.nzにおけるDNSSECの取り組みについて紹介がありました。はじめに、.nzは2009年中もしくは2010年早々に、DNSSECのサービス開始をする予定であり、それに向けて準備をしている段階だという話がありました。続いて、DNSSECでサービスを開始するにはさまざまな課題があり、その解決が必須であることも紹介されました。DNSSECサービス開始のためにDNSソフトウェアの整備が必要であることや、DNSSECが加わったときのドメイン名登録手続きに関わる作業の変化、鍵の管理、レジストリやレジストラの責任など、多数の検討項目が挙げられました。

◆DITL

APNICのGeorge Michaelson氏により、DNSの状況を調査するDITL（Day In The Life）というプロジェクトについて紹介がありました。DITLは毎年ある期間、世界中のDNSサーバにおけるクエリ状況を調査するもので、2009年も3月29日から4月2日まで行われました。37組織190ノードのDNSサーバが対象となってデータが収集され、そのデータの総計は4TBにもなったそうです。


■ 会場内のロビーの様子

APNICのDNSサーバもそのうちの一つであり、この発表ではAPNICが管理するサーバの統計が紹介されました。問い合わせ元のIPアドレスについて、2008年のものと2009年のものを比較すると1/3が一致せず、流動的なアドレスが比較的多数を占めること、ごく少数のホストが大量に問い合わせを行っていること、2008年と比較してIPv6トランスポートでの問い合わせが増えていること、毎日午前4時頃に日本から大量の問い合わせがくることなど、APNIC DNSの挙動について興味深い紹介がありました。

◆7.7 DDoS cyber attack in Korea

KRNICのJi-Young Lee氏からは、2009年7月7日頃に韓国および米国で起こったDDoS（Distributed Denial of Services）事件について報告されました。DDoS攻撃は、最初のうちは米国のホワイトハウスを対象としていましたが、時間の経過とともに、韓国内のポータルサイトや新聞社のWebサーバへの攻撃に変わっていったことがわかっています。zombie PC※2となったホスト数を集計した結果、韓国内ではその台数が77,875台にのぼりました。

KRNICでは、ISPとしての対策が取れるように、DDoSに利用されたzombie PCのIPアドレスを該当するISPに通知したり、主要なポータルサイトにワクチンを載せるための連携を図ったりしました。それらの活動を通じて、WHOISの情報を正確に保つことの重要性をあらためて学んだ、とのことです。会場からは、DDoSが起こった時間的経緯に関する質問がありましたが、技術的な経緯のわかる詳細な情報は、KRNICには来ていなかったようです。他には、DDoS攻撃のあった時間帯にBGPのupdateメッセージが多くなったという情報が寄せられました。

■ 会場のそばの王府井大街

当日のプレゼンテーション資料などは、以下のWebページに載せられています。

□APNIC28 / Program / APOPS
http://meetings.apnic.net/28/program/apops

◇　　◇　　◇

APOPSでは、日本からの参加者も活躍していました。チェアを務める吉田友哉氏（NTTコミュニケーションズ株式会社）の活躍をはじめ、日本の事業者の方々が内容の濃い発表をされていることが印象的でした。

今回のAPOPSは、APNICミーティング全体に比べると参加人数が少なく、また会場での質疑応答は多くありませんでしたが、各発表の内容の良さがより多くの人に知られることで、今後この状況は変わっていくかもしれません。

今後も特筆すべき事項がありましたら、本稿のような形で報告していきたいと思います。

（JPNIC 技術部 小山祐司／木村泰司）


■ 手前の東長安街通りの先には天安門広場があります

※1 The Asia Pacific OperatorS Forum
http://www.apops.net/

※2 zombie PC
DDoS攻撃のパケットを送出するために利用されたホスト

2009.10.5▶10.9

第59回RIPEミーティング報告

■ 全体会議報告

ポルトガルの首都リスボンは、ゴツゴツとした石畳と明るいクリーム色の建物が印象的な歴史ある街です。夕食のために旧市街に出かけると、情緒あるケーブルカーが急な斜面を登っていくのを目にしました。

◆RIPE59ミーティングの概要

第59回RIPEミーティングは、リスボンにあるCorinthia Hotelで行われました。

開催期間：2009年10月5日（月）～9日（金）
参加者数：300名（登録者数355名） ※2009年10月9日時点
参加国数：36ヶ国
参加者の多い国：イギリス（36名）、オランダ（34名）、ドイツ（34名）、米国（33名）、ポルトガル（28名）（日本からの参加者は9名）

初日と2日目は全体会議であるPlenaryが行われ、後半は各WGのミーティングが行われました。2009年10月現在、活動していないWGを除くと、RIPEには11のWGがあります。

□RIPE Working Groups
http://www.ripe.net/ripe/wg/

◆Plenary

全体会議であるPlenaryは、以下のような内容で行われました。

Plenary 1 - 4バイトAS番号やMPLS、CPE（Customer Premises Equipment: カスタマー構内設備）等

Plenary 2 - IPv6のディプロイメント

Plenary 3 - RIR/NRO等関連団体の活動報告

Plenary 4 - RIPE NCCのトピック

Plenary 5 - 主にDNSSEC関連のトピック

Plenaryのアジェンダと資料は、次のURLから見ることができます。


Lisbon, Portuguese Republic

□“Agendas RIPE 59 Lisbon, 5-9 October 2009”
http://www.ripe.net/ripe/meetings/ripe-59/agendas.php?wg=plenaries

以降、主にPlenaryでの議論を中心に報告いたします。

◆IPv6関連

IPv6のディプロイメントについては、2日目のPlenary 2で四つのプレゼンテーションがありました。簡単に内容を紹介します。


■ Plenaryの様子

- France Telecom's IPv6 Strategy

フランスの大手通信会社であるフランステレコム社の、インターネット接続サービスにおけるIPv6導入の中間発表です。CPEとNATを併用する方式や、IPv6でIPv4のプライベートアドレスをカプセル化する、Dual-Stack Lite方式などのいくつかの収容方法が検討されています。フランステレコム社では、2010年末までにグループ会社全体でIPv6が使えるように整備が進められています。

- A Strategic Approach to IPv6

HEARNET社では既にIPv6の導入が済んでいますが、今後IPv6のみのサービスネットワークを提供するという課題に直面しています。IPv4アドレスの在庫枯渇時期と予測されている、2011年に向けたマイルストーンが示されています。

- IPv6 in Real Life

DNSを使ったIPv6導入に関する国別統計を、2、3年前と比較しています。100ヶ国程度を調査した結果、AAAAが返ってくるドメイン名は3～4倍に増えていますが、中にはリンクローカルのアドレスが返ってくるなど、設定が適切ではないところがあったようです。

- IPv6 in the Citizens with Special Needs' Network

ポルトガルの学術関連ネットワークにおけるIPv6導入状況の紹介です。IPv6の通信を行っているノードは約120見つかっているそうです。

◆RIPE Labs

RIPE NCCでは、正式サービスになる前の実験サービスや開発途中のプログラムを公開し、RIPEコミュニティにおける議論の活性化を目的とした「RIPE Labs」と呼ばれる活動が始められました。これは、RIPE NCCのRobert Kisteleki氏の考案によるものです。会場では、IPv4アドレスの/8の割り振りを自動車レースになぞらえたアニメーションが紹介されていました。この他に以下のようなアプリケーションやデータベースが開発されています。

- REX - the Resource Explainer

割り振り済みIPアドレスの利用状況を、経路情報やDNS･ブラックリストに載っているIPアドレスといった複数の観点で見られるWebのツールです。ISPやRIPE NCCのIPアドレス担当者がIPアドレスの利用状況を確認できるほか、IPアドレスの移転が行われる場合にもIPアドレスの情報を確認できるようになっています。

- The Internet Number Resource Database（INRDB）

RIPE NCCのRISやIANA、他RIRの情報を集約したデータベースで、RIPE Labsの各アプリケーションやコマンドラインプログラムで使えるような出力インタフェースを持っています。

- RIPE 59 Meeting Plan for Google Calendar

これは厳密には「開発」とは呼べませんが、Google CalendarでRIPE59ミーティングの予定が見られるようにメンテナンスされているようです。

- 16-bit ASN Exhaustion - some data

2バイトAS番号の在庫枯渇状況をわかりやすく見えるようにするツールで、会場では在庫枯渇のグラフが紹介されていました。

- NetSense - next generation Information Services

1990年にIPアドレスが割り当てられたホスト数の統計を求める「hostcount」がRIPEコミュニティで始まって以降、RIPE NCCではRIS（Routing Information Service）、TTM（Test Traffic Measurements）、DNSMON（DNS Monitoring Services）といった統計データを取り、それを視覚化するさまざまなツールが開発されました。

NetSenseは、これらを簡単に見られるようにするためのWebアプリケーションで、詳しい情報を表示しつつも全体概要を捉えやすいようなツールになるように設計されています。

RIPE Labsのこれらのツールは、同Webサイトで紹介されつつ、リンクも張られています。

□RIPE Labs
http://labs.ripe.net/

◆DNSSEC

2日目のPlenary 5では、DNSSECについて三つのプレゼンテーションがありました。

- DNSSEC in .pt

ポルトガル国内で行われたDNSSECの必要性に関するアンケート結果などについての報告です。

- Scaling the Root

ICANN理事会の要請により行われている調査活動で、DNSSECや国際化TLD、新gTLDを視野に入れた、ルートゾーンのサイズと変更頻度の増加に関する調査の途中経過です。今後、ソウルで開催されるICANN会議やパブリックコメントの募集が行われるようです。

- DNSSEC for the Root Zone

ICANNとVeriSign社による、ルートゾーンへのDNSSECの導入に関する発表です。Transparency（業務の透明性）、Audited（ISO/IEC 27002:2005認定）、High Security（NIST SP800-53相当）といったキーワードを使って取り組みが紹介されていました。PKIでいうCPS（Certification Practice Statement）と似た構成のDPS（DNSSEC Policy & Practice Statement）を作成するなど、堅牢性に留意したシステムが検討されています。

このうち3番目のプレゼンテーションで、今後のルートゾーンへの署名スケジュールが発表されました。

December 1, 2009
　ルートゾーンへの署名
　ICANNとVeriSign社によるKSR（Key Signing Request）の処理

January - July 2010
　署名付きルートゾーンの提供

July 1, 2010
　トラストアンカー提供とKSK運用
　署名付きルートの提供完了

会場では、KSK（Key Signing Key）の鍵長が1,024bitでは短かすぎるのではないか、provisioning systemの準備が遅れているのではないか、実際にKSKがITAR（Interim Trust Anchor Repository）などに置かれるのはいつなのかが重要である、といったコメントが挙がりましたが、スケジュールを公開しながら進めることに関する評判はよかったようです。

これを受けてRIPEのDNS WGでは、ICANNによるルートゾーンへのDNSSEC導入の発表を歓迎するとともに、今後も計画を公開しながら進めるよう要請する声明を出すことになりました。

◆RPKI関連

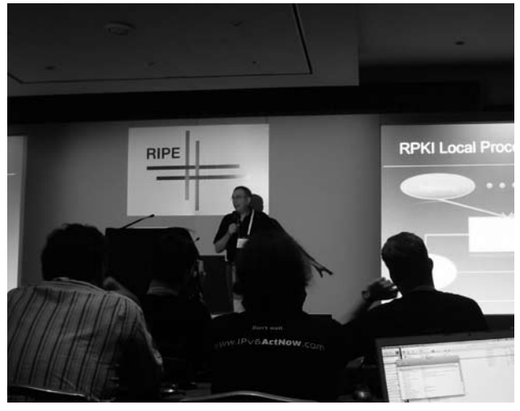
RPKI（Resource PKI）証明書については、Address Policy WGで議論が行われました。NCC Service WGでもプレゼンテーションが行われました。RIPE NCCでは、リソース証明書を発行し利用していくまでに、大きく分けて四つの課題があると考えられています。

（1）RIPE NCCにおける契約との関連性

（2）政府による要望や命令に従って証明書を失効すべきかどうか

（3）紛争の対象となっているアドレスの扱い

（4）業務ミスやプログラムエラーへの対応



■ RPKIに関するプレゼンテーションを行うStephen Kent氏

この中で特に議論されたのは、(2)のリソース証明書の失効についてです。失効とは、有効期限内に電子証明書を無効化することで、リソース証明書を発行しているRIPE NCCは、技術的には証明書保持者の意図に反してリソース証明書を失効させることができます。例えば、RIPE NCCの事務局があるオランダの政府当局によって、特定のネットワークのIPアドレスを無効化させるような要請や命令があった場合に、どのような対処をし、問題の整理を行えばよいのか、といったことが議論されました。

会場では、ISPで経路制御のためにリソース証明書を使い、自動的に制御されるような状況をすぐに実現させるべきではないといった意見や、レジストリはインターネット経路制御に関与しないという背景を受けて、リソース証明書の失効は割り振り情報の削除と同様に、インターネット経路制御に影響しないようにすべきといった意見が挙げられました。

今後、Certification Task Forceが中心となって、Address Policy WGでリソース証明書のためのCPSの作成が行われることになりました。RIPE NCCでは、全てのRIRで正式サービス化されると言われている2011年1月1日までに正式サービス化する、としています。

◇　　◇　　◇

次回の第60回RIPEミーティングは、2010年5月3日～7日にチェコのプラハ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）

■ RIPE地域におけるアドレス分配ポリシーの動向

2009年10月5日から9日に行われた第59回RIPEミーティングのうち、本稿では、アドレス分配ポリシーの動向をお伝えします。

今回のミーティングでのアドレス分配ポリシーにおいて特筆すべきトピックは、やはりIPv4アドレス在庫枯渇後の対応です。

これに関わる提案としては、「RIPE NCCでのIPv4在庫の分配方法」や「返却されたアドレスの世界的な管理・再分配方法」が挙げられます。そして、在庫枯渇後は重要性が増すと考えられている、アドレス資源の利用権利を担保する仕組みとしてのRPKI（Resource PKI）の提供について、RIPE NCCでの検討状況も紹介されていました。

また、ドイツ国防省による省内のネットワークにおける他に類を見ないアドレス利用の事例紹介も行われ、そのような情報提供を公式のミーティングで堂々と発表していることも含めて新鮮でした。

RPKIの検討については前号でご紹介しましたので、ここではIPv4アドレスの在庫枯渇に向けたポリシー提案について、どのような議論が行われていたのかを簡単にご報告します。

◆IPv4アドレスの在庫枯渇に向けたポリシー提案

今回議論された主な提案の目的は、以下の二つに整理することができます。

1.RIPE NCCの最後のIPv4アドレス在庫をどう分配していくかを定義したもの:2008-06、2009-04、2009-03

■ 会場のCorinthia Hotel

2.返却されたIPv4アドレスを、世界的にどう管理・再分配していくかを定義したもの:2009-01

個々の提案の概要は、以下の通りです。

◎RIPE地域における最後の/8の分配方法について

［提案］2008-06：Use of Final/8
2009-04：IPv4 Allocation and Assignments to Facilitate IPv6 Deployment

2008-06
- RIPE NCCの最後の/8在庫は1組織につき/22（1,024アドレス）の分配に限定し、同じ/8空間の中から/16を予期せぬ用途のために確保することを提案しています。
- 内容、提案者ともに、2009年2月からAPNICで施行したポリシーと同じです。

2009-04
- 2008-06の代案として同じ/8の空間を、IPv6の実装を前提としたネットワークに分配先を限定することにより、IPv6移行へのインセンティブとするものです。ARIN地域では、これと同じ趣旨の提案が施行されています。

どちらの提案もIPv4在庫枯渇後の状況に備えて、RIPE NCCにおける最後の/8アドレス在庫を別途リザーブし、この空間からのアドレスの分配はこれまでの基準と分けて定義していることが共通しています。

Policy WGセッションでの議論では、IPv4アドレス在庫枯渇まで時間的な制約もあることから、多くの要素は盛り込まず、最低限必要な対応と考えられる2008-06をベースに、継続議論を行うことになりました。この提案が施行された場合は、新規・既存の事業者ともに、/22の分配を必ず受けることができるため、一定数のIPv4アドレスの分配が最後に保障されることを前提として、在庫枯渇後の状況に備えることが可能となります。

◎在庫枯渇時期に応じた“公平”なIPv4アドレスの分配について

［提案］2009-03：Run Out Fairly

これは前項で紹介した提案と若干アプローチが異なり、より多くの申請者に機会を与えるために、枯渇時期が近づくにつれ、段階的に分配量を縮小していく（例:2010年7月:9ヶ月分の需要を分配→2011年1月:6ヶ月分の需要を分配等）というものです。大きなISPが一度に大量のアドレス申請を行うことにより、その後に申請を行ったISPが分配を受けられなくなる事態を避けることが、提案者の目的です。

会場では分配量を調整するタイミングの定義について、参加者の一人からは懸念が表明されましたが、基本的には好意的に受け止められました。現行の提案を施行する方向で、継続議論を行うことになっています。

◎IPv4在庫枯渇に向けたIANAからRIRへのIPv4割り振りに関するグローバルポリシー

［提案］2009-01：Global Policy for the allocation of IPv4 blocks to RIRs

現在、RIRへ返却されたIPv4アドレスは各RIR単位で在庫管理・再分配が行われています。しかし、アドレスの返却が特定のRIRに集中し、IANA在庫枯渇後に再分配できるアドレスが、RIR地域によって偏ることも想定されます。

そこで、この提案では返却されたアドレスを、IANAが世界共通の在庫として管理・再分配を行うことを定義しています。施行にあたっては、全RIRフォーラムにおけるコンセンサス（提案への賛同）とICANN理事による承認が必要となり、現在はAfriNIC、APNIC、LACNICの3 RIRフォーラムにてコンセンサスが得られています。

Policy WGセッションでは、ARIN地域ではIANAへの返却を必須ではなく「任意」に変更して提案されており、本提案の有効性が薄れること、また、全RIRに対して共通に適用されるグローバルポリシーとして機能しないことが問題提起されていました。

結論としては、参加者からARINの対応について懸念が表明されていたものの、基本的には他のRIRにおける対応であるため、RIPEのアドレスフォーラムとしてはARINでの結論を待った上で、議論を再開することになりました。

■ RIPE NCCの新サービスNetSenceを紹介するパンフレット

◆その他の特筆すべき提案

アジア太平洋地域のAPNICフォーラムとも共通するテーマを取り扱った提案としては、以下2点がありました。

2009-06 Routing Requirements

・本提案により、RIPE地域においては、IPv6初回割り振り申請時に割り振りを受けたアドレスに対する、経路集約を求める要件が撤廃され※1、ミーティング期間中の10月8日に施行されました。

・ポリシーの要件とはしないものの、経路集約は促進するため、IPv6における経路広告に関するガイドラインをどう文書化していくかについて、ルーティングWGにて別途議論が行われました。

・APNIC28（2009年8月25日～28日）ではこれと逆行し、初回に加え、追加割り振り申請時にも経路集約を求める提案が行われましたが、支持されませんでした（詳しくはP.32からの「APNIC28ミーティング報告」をご覧ください）。今後は、RIPEと同じ対応を行う方向で検討する可能性が濃厚です。

2008-07:Ensuring Efficient Use of Historical IPv4 Resources

・追加割り振り申請時に、申請者が分配を受けている歴史的PIアドレスも含めて、分配済みアドレスの効率的な利用の確認を行うとする提案です。

・RIPEでは一部要件見直しの上、継続議論となりました。APNICでは2009年2月より施行されています。

■ 会場周辺のリスボン市街の様子

※1 IPv6アドレスポリシーではIPv6アドレス初回申請時の要件の一つとして、割り振りを受けたIPv6アドレスの経路広告は単一に集成して行うことを求めています（例：/32の割り振りを受けた場合は/32で経路広告を行い、複数の/36等に分割しない）。RIPE地域では、アドレスポリシーで経路広告を定義することは適切ではないとして撤廃されました。

◆今後の議論の動向を知りたい方は

RIPEのポリシーフォーラムでは、IETFに比較的近いポリシー決定プロセスが採用されており、提案に対してミーティングで議論は行いますが、決議はとらず、メーリングリストでの議論も踏まえて、WGのチェアが施行の判断を行います。

今後のRIPE地域におけるポリシー提案の動向が気になる方は、“address-policy-wg@ripe.net”に下記URLよりご登録ください。提案の議論や施行の発表を追うことができます。

□address-policy-wg MLへの登録サイト
http://www.ripe.net/mailman/listinfo/address-policy-wg#subscribers

◆参考

第59回RIPEミーティング　アジェンダ・発表資料
http://www.ripe.net/ripe/meetings/ripe-59/agendas.php?wg=address-policy

第59回RIPEミーティング　トランスクリプト・映像（Policy WGは「Wednesday」および「Thursday」に開催）
http://www.ripe.net/ripe/meetings/ripe-59/archives.php

RIPE地域にて議論中のポリシー提案一覧
http://www.ripe.net/ripe/policies/proposals/

（JPNIC IP事業部 奥谷泉）

2009.9.11▶9.12

ICANNと米国政府との新しい関係

■ ～「責務の確認（AoC）」の締結～

2009年6月15日発行のJPNIC News & Views vol.646※1にて、インターネットの資源管理の頂点に立つICANNと米国政府の関係について述べ、両者が締結し終了を間近に控えたJPA（Joint Project Agreement「共同プロジェクト合意」の意）※2について解説しました。その際、「JPA満了後の枠組みや、ICANNと米国政府の関係がどのようになるのか興味深い」と記しましたが、2009年10月1日に、JPAに代わる「責務の確認（Affirmation of Commitments; AoC）」と呼ばれる新しい文書が発効しました。本稿では、このAoCの解説と、これまでの背景についてお伝えします。

◆背景

今回、AoCの締結に至った背景は、AoCの前身であるJPA、さらにその前身となるMoU（Memorandum of Understanding）※3の締結にまで遡れます。ICANNと米国商務省（Department of Commerce; DoC）との間でのMoUの締結は、「ドメイン名の一元的管理を含むDNSの管理権限は米国政府が持っている」とする米国政府の主張に基づいて、1998年11月に行われました。この主張はいわゆるホワイトペーパー※4の中で主張されたものですが、同文書は「DNSの管理は民間主導で行われることが望ましい」とも述べ、ICANNが設立された際にMoUを結び、DNSの管理をICANNに委託することになりました。MoUはその後何回か改訂された後、3年の期限付きであるJPAとなりました。

JPA終了が近づいた2009年5月、NTIAはJPAに関して意見募集を行いました。また、同時期に米国議会もこの問題に興味を示し、公聴会を開いてICANNおよびNTIAより参考人を招致しました。これらの動きを背景に、NTIAとICANNとの間でJPA終了後の取り決めについて交渉がなされたと思われます。

ICANNがWebページで公開している内容によりますと、2009年9月11日から12日にかけて理事合宿を行っています。正式な理事会ではないため議事録は公開されていませんが、主な議題を列挙している中にAoCが含まれています。そして、AoCがICANN理事会で正式に承認されたのは、JPA終了期限ぎりぎりの2009年9月30日となっています。

◆AoCとは

AoCとは、DoCとICANNとが、それぞれが果たすべき責務を記載した文書です。その前身であるJPAが2009年9月30日に終了したのに伴い、同日DoCの一機関である米国商務省電気通信情報局（National Telecommunications and Information Administration; NTIA）およびICANNがそれぞれ公開し、翌10月1日より発効しました。

AoCに書かれている責務は多岐にわたりますが、ICANNに関する主なものは次の通りです。

a）公益のための、DNSのグローバルな技術的調整
b）DNSのセキュリティ、安定性、回復性の維持
c）競争、消費者の信頼、DNS市場での消費者による選択の自由の促進
d）DNSの技術的調整における国際的な参画の促進

これに対し、DoCの責務としては主に次のものを挙げています。

e）グローバルなインターネットユーザーのメリットを代表するDNSの技術的調整において、マルチステークホルダー、民間セクターが率いる、かつボトムアップなポリシー策定モデルへの関与

前身であるJPAとAoCを比べた場合の主な違いは、以下の4点となります。

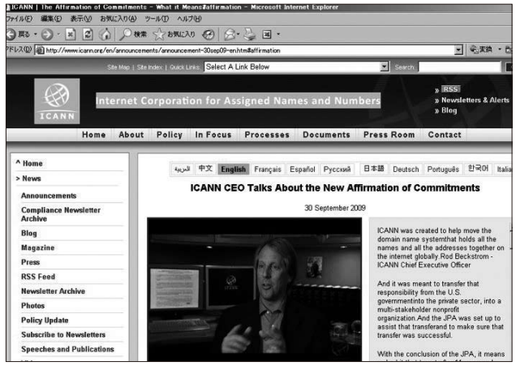
1）期限が定められていない
2）これまで定期的にICANNからDoCに報告書を提出して評価を受けていた仕組みから、ICANNの自主性を尊重した評価の仕組み※5に移行する
3）米国政府のICANNに対する関与は、米国以外の各国政府同様にGAC（Governmental Advisory Committee:政府諮問委員会）※6を通じて行う
4）AoCは、米国政府もしくはICANNのどちらか一方の当事者が、意思を表明することにより、いつでも終了となる

これに対し、JPAの頃から一貫して変わらない点は、ICANNが米国に本拠地を置く一民間非営利団体として運営されることです。

◆AoCが示すもの

では、JPAからAoCになったことで、DNSの管理運営が民間主導となったと言えるのでしょうか。これについては、前述したAoCとJPAの相違点の4番目である「AoCは、米国政府もしくはICANNのどちらか一方の当事者が意思を表明することにより、いつでも終了となる」という条項により、必ずしもそうとは言えないと解釈することが可能です。つまり、AoCが終了すればICANNはDNSの管理権限を持たなくなるため、DoCはICANNに対してAoCの終了通告を行うことで、引き続きいざというときの関与を可能としているということです。ただし、通常時における米国政府の関与は、他国の政府と等しいGAC経由の関与とされているため、この点だけが注目されて、ICANNが米国政府の管理下より独立したという見方がされているようです。

AoCの締結後に、ICANNに寄せられたコメントは公開されており、米国の連邦議員からのものも含め、歓迎する内容のものばかりです。米国政府が前述の「相違点4）」という担保を残している点では、JPAとそれほど変わらないのでは、という見方も可能なAoCですが、ICANNが米国政府の管理から独立することを望んでいたと思われる国々も歓迎している理由は、上記、相違点4）が発動されない限りにおいて、全ての政府はGACを通じてICANNに関与することになっており、同等の権利を有するからです。今後、ICANNの評価委員会がスムーズに立ち上がり、ICANNの評価内容が肯定的なものとなれば、AoCおよびそれに付随した体制が成功したということになるのかもしれません。



■「ICANNのCEOが語る新しい『責務の確認』」が掲載されているICANNのWebサイト

■ ICANNと米国商務省間のDNS管理に関する「責務の確認」契約締結に対するJPNICのコメント

◆参考

Affirmation of Commitments（原文）
http://www.icann.org/en/announcements/announcement-30sep09-en.htm#affirmation

（JPNIC インターネット推進部 山崎信）

※1 JPNIC News & Views vol.646
ICANNと米国政府の関係 ～JPA終了に向けて～
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2009/vol646.html

※2 JPA（Joint Project Agreement:共同プロジェクト合意）
米国商務省（DoC, Department of Commerce）とICANNの間で、2006年9月に結ばれた覚書のことを指します。1998年11月にICANNと米国商務省との間の覚書（ICANN/DoC MoU）として締結されて以来、明確にJPAと称されるようになった2006年9月に至るまで6回更新され、2009年9月30日に期限満了を迎えました。

※3 ICANN/DoC MoU（Memorandum of Understanding）
ICANNと米国商務省（DoC）が、DNSの技術的管理の権限を米国政府から民間セクター（ICANN）へ移行させるために、その方法や手順を両者が共同で策定することを目的として、1998年11月に締結した覚書です。1998年11月25日に締結され、2006年9月30日まで延長された後、JPAへと引き継がれました。

※4 ホワイトペーパー
1998年6月5日に発表された、インターネットの管理体系に関する提案が記述されている、米国政府による文書の通称です。1998年1月30日のグリーンペーパーに対するコメントの一部を反映してまとめられました。ドメイン名やIPアドレスの管理の調整のために非営利法人を設立するとしています。グリーンペーパー、ホワイトペーパーという流れを受けて、ICANNという新しい組織が設立されました。

※5 AoCでのICANN評価の仕組み
AoCでは、GAC議長、ICANN理事長または事務総長、DoC情報通信担当次官補、ICANNの各諮問委員会（Advisory Committee; AC）および各支持組織（Supporting Organization; SO）の代表、および独立した専門家からなる評価委員会を設置する、としています。

※6 GAC（Governmental Advisory Committee:政府諮問委員会）
ICANNの諮問委員会の一つで、各国政府の代表などで構成されています。各国政府の立場からICANNの理事会に対して助言を行っています。

2009.10.25▶10.30

ICANNソウル会議報告

2009年10月25日（日）から30日（金）まで、韓国のソウルで第36回ICANN会議が開催されました。今回の会議で最も大きく取り上げられたのはIDN ccTLDですが、新gTLDに関する議論も盛りだくさんでした。

◆IDN ccTLD導入に関する進捗

前回シドニー会議では、2009年5月31日に公開された“Draft Implementation Plan for the IDN ccTLD Fast Track Process（IDN ccTLD ファスト・トラック プロセス実装計画案）”の第3版※1に従って議論されましたが、これを反映した“Proposed Final Implementation Plan for the IDN ccTLD Fast Track Process（IDN ccTLD ファスト・トラック プロセス最終実装計画案）（以下Prop Final）”※2が9月30日に公開され、これが理事会審議に掛かることになりました。2日目の10月26日（月）に行われたIDN ccTLD Fast Track Workshopでは、このProp Finalの説明がなされました。バリアント（異体字）やコミュニティサポートなどに関する質問が出ましたが、Prop Finalの大枠を左右する議論はありませんでした。

同日夕刻のレセプションは“IDN Reception”と名付けられ、TLDにおけるIDNの導入という大きな節目に際して、関係者の労をねぎらうような趣向で、TLDに限らずIDNの標準化、サービス開始に関与した関係者が壇上で挨拶しました。

Prop Finalは、最終日の10月30日（金）に開かれた理事会の議案に上がり、無事承認されました。この承認によって、Prop Finalでの記述通りに、2009年11月16日からFast Trackの申請受け付けが開始されることが正式に決定しました。この議決は、歴史的なものであるとして、理事会の聴衆からスタンディングオベーションによって迎え入れられ、また、事務総長Rod Beckstrom氏は壇上からリアルタイムで、この議決をTwitterでも全世界に向けて伝えていました。その後、11月16日から予定通りIDN ccTLDの登録受け付けが開始され、中国などいくつかの国から申請が行われています。

◆新gTLD導入に関する進捗

新gTLDに関しては、ICANN会議以外にもコンサルテーションセッションを開催しながら検討が進められた結果、ソウル会議の直前である10月2日に、“Draft Applicant Guidebook（ドラフト版申請ガイドブック）”の第3版（以下DAGv3）※3が発表されました。ソウル会議では、新gTLDに関する総括的セッションである“New gTLD Program Overview”以外に、商標保護やレジストリ・レジストラ分割など、関連するテーマ毎に分けられたセッションが複数開催されました。

商標保護に関するセッション“Trademark Protection and new gTLDs”においては、商標保護に関するメカニズム - トレードマーク・クリアリングハウス（IPクリアリングハウスから改称）、URS（Uniform Rapid Suspension）、PDDRP（PostDelegation Dispute Resolution Process）に関して、DAGv3において変更された点と、議論中のポイントが提示されました。

「レジストリ・レジストラ分離」のセッションでは、理事会議長であるPeter Dengate Thresh氏のモデレーションの下、分離支持派と分離反対派の計2名のパネリストが壇上で発表する形で、ディスカッションが展開されました。セッションの最後には参加者の発声によって、双方に対する支持が測られ、若干ながら分離支持に対する賛

■ 会場となったロッテホテル

成が多かったものの、際立った違いはありませんでした。

また、理事会の席上、AOB（Any Other Business：「その他」）の部で「新gTLDに対する関心表明（Expression of Interest）を行った場合に起こり得る影響を調査し、理事会における検討計画案を、リスク分析を伴う実施オプションとともに12月の理事会で提示することを、ICANN事務局に指示する」という決議が承認されました。

新gTLDに関してこのような関心表明が議論となったのはこれが初めてですが、関心表明のプロセスが新gTLD追加のプログラムに付け加えられる見通しであることが、この決議で明らかになりました。また、ここで挙げた商標保護、レジストリ・レジストラ分離を含む六つのポイントなどが、継続議論のアイテムとして残されており、これらの準備が整って新gTLDが募集されるまでには、今しばらく時間が掛かるという印象を持ちました。

◆その他

前号の「ICANNシドニー会議報告※4」でも報告した、GNSOの組織改正はそのプロセスを終え、今回のソウル会議では、二院制の組織構造になってから初めての評議会が開催されました。これに加え、新たな事務総長Rod Beckstrom氏が2009年7月に就任して以降初のICANN会議でもあり、ICANNと米国商務省の間の覚書、JPA（Joint Project Agreement:共同プロジェクト合意）※5が満了し、AoC（Affirmation of Commitments: 責務の確認）※6が発効してからも初のICANN会議と、IDN ccTLD以外にも「初めて」尽くしのICANN会議となりました。

（JPNIC インターネット推進部 前村昌紀）

■ GNSO評議会の様子

■ 理事会でIDN ccTLD Fast Track Processの最終実装計画案が承認されると、会場ではスタンディングオベーションが起こりました

※1 “IDN ccTLD Fast Track Process（IDN ccTLD ファスト・トラック プロセス実装計画案 第3版）”
http://www.icann.org/en/announcements/announcement-31may09-en.htm（英語）

※2 “Proposed Final Implementation Plan for the IDN ccTLD Fast Track Process（IDN ccTLD ファスト・トラック プロセス最終実装計画案）”
http://www.icann.org/en/announcements/announcement-2-30sep09-en.htm（英語）
http://www.icann.org/ja/announcements/announcement-2-30sep09-ja.htm（日本語）

※3 “Draft Applicant Guidebook（ドラフト版申請ガイドブック）”
http://www.icann.org/en/topics/new-gtlds/dag-en.htm

※4 JPNIC News & Views vol.654
ICANNシドニー会議報告
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2009/vol654.html

※5 JPA（Joint Project Agreement:共同プロジェクト合意）
米国商務省（DoC, Department of Commerce）とICANNの間で、2006年9月に結ばれた覚書のことを指します。1998年11月にICANNと米国商務省との間の覚書（ICANN/DoC MoU）として締結されて以来、明確にJPAと称されるようになった2006年9月に至るまで6回更新され、2009年9月30日に期限満了を迎えました。

※6 AoC（Affirmation of Commitments: 責務の確認）
インターネットの資源管理に関して米国商務省とICANN、それぞれが果たすべき責務について記載した文書です。前身の文書であるJPAが2009年9月30日に失効したことに伴い、同日公開され、翌10月1日より発効しました。詳しくはP.43「ICANNと米国政府との新しい関係 ～「責務の確認（AoC）」の締結～」をご覧ください。

2009.11.8▶11.13

第76回IETF報告

■ 全体会議報告

◆概要

山陽新幹線の改札口を出ると、正面に立っている看板「Welcome -76th IETF Meeting Hiroshima」の文字が目に入ってきました。ホテルに向かう途中のアーケードには、IETFミーティング開催の横断幕がかかっています。市内のこのような掲示は、私が参加したことのあるIETFミーティングでは見たことがありませんでした。IETFが日本の広島で開催されるという実感とともに、ホストであるWIDEプロジェクトの力の入れように驚き始めた開催前夜でした。

第76回IETFミーティングの開催概要は以下の通りです。

開催期間：2009年11月8日（日）～13日（金）
会　　場：ANAクラウンプラザホテル広島
参加登録者数：1,155名
参加国数：44ヶ国
参 加 費：635USD（早期割引料金）、785USD（通常料金）、200USD（一日料金）
ホ ス ト：WIDEプロジェクト


■ Plenaryの様子

全体会議（Plenary）での発表によると、日本からの参加人数は363名と最も多く、全体の34%を占めていました。米国は304名で27%、中国は99名で9%、続いてフランス4%、韓国4%という内訳でした（2009年11月10日時点）。

初日の11月8日（日）はチュートリアルとレセプションが開かれ、2日目から最終日にかけて、各WGのミーティングとBoFが開かれました。

◆Operations and Administration Plenary概要

Operations and Administration Plenaryは、IETFの運営などに関する全体会議です。4日目の11月11日（水）16:30から3時間程行われました。ホストであるWIDEプロジェクトのプレゼンテーションと、新設されたItojun Service Awardの発表、NOCレポート、IETFチェアの活動報告などが行われました。

○WIDEプロジェクトのホストプレゼンテーション

WIDEプロジェクトのプレゼンテーションでは、WIDEプロジェクト代表で、JPNICの理事でもある村井純氏によって広島市内の広告や、第76回IETFのロゴやTシャツのデザイン、RFID（Radio Frequency Identification）の利用実験などについて説明が行われました。

会場のホテルが面している平和大通りでは、数多くのイルミネーションが飾られるイベント「ひろしまドリミネーション」が毎年行われていますが、今回はIETFの開催期間に合わせ、イベントの開始が例年よりも早められたとのことでした。また、ロゴとIETFで恒例となっているTシャツは、広島市立大学の及川久男教授によってデザインされたそうです。

RFIDは、以下の二つの実験で使われました。

- 発言者の情報表示システム

マイクの前に立って発言する際、マイクスタンドにかかっているRFIDリーダーにタグをかざすと、発言者の氏名などがスクリーンに表示されます。タグは、首から下げる名札入れに入っているため、人によってはマイクに近づくだけでタグが認識されます。議論中に発言者の名前を確認できる他、Jabberや議事メモの作成に役立っていました。

- E-bluesheet

ブルーシート（Bluesheet）とは、WGなどで参加者自身が記入する形式の参加者リストです。今回のIETFでは、ブルーシートに加えてRFIDリーダーが座席にまわってきました。タグをRFIDリーダーにかざすだけでよいため、紙に氏名やメールアドレスを記入するよりも楽になっています。

RFIDタグは、1,121名中、889名によって使用されました（2009年11月10日時点）。RFIDの利用実験で印象的だったのは、その運用とサポートです。RFIDタグは、ユーザーが登録しなければ有効にならないオプトインの形で配布され、また意図せずに他人に読み取られるのを防ぐ、“スキミングプロテクション”カードも一緒に配布されていました。会場にはヘルプデスクが設けられ、常時スタッフが対応できるようになっていました。

この他に、ソーシャルイベントの参加者向けに、「PASPY」と呼ばれるFelicaカードが配布されていました。PASPYは広島市内の交通機関で使えるだけでなく、平和記念資料館の入場などにも使うことができます。

■ 発言者のRFIDを読み取るためにマイクスタンドに設置されたRFIDリーダー

○Itojun Service Award

Itojun Service Awardは、KAMEの実装などで知られる萩野純一郎氏の功績をたたえ、萩野氏の家族と有志の寄付を基にして設置された賞です。この賞は、インターネットに関わる開発や運用などの技術的貢献を行った人に贈られます。

第1回のItojun Service Awardは、Google社のLorenzo Colitti氏とErik Kline氏に贈られました。両氏は、GoogleのWebサービスを、IPv6を使って利用できるように尽力したことが認められ、受賞に至りました。

□The KAME project
http://www.kame.net/

□Internet Society（ISOC）- Itojun Service Award
http://www.isoc.org/itojun/

○NOCレポート

NOCレポートは、IETFのために設置されたネットワークに関する、ネットワークオペレーションチームからの報告です。WIDEプロジェクトのメンバーでもある東京大学の加藤朗氏によって行われました。概要は以下の通りです。

- ネットワークのデザイン

“Simple but robust”という原則の下、どのネットワークでもIPv4とIPv6が使えるようになっていました。


■ 萩野氏のご家族と、Itojun Service Awardの最初の受賞者になったGoogle社のLorenzo Colitti氏とErik Kline氏（右端の二人）

会場のみならず、会場以外の五つのホテルでもIETFのネットワークが提供されました。一般の宿泊客も使えるようになっており、ボトルネックになると考えられるNATが介在しない、高速なネットワークが提供されました。

- ネットワーク回線

会場のANAクラウンプラザホテル広島は1Gbps、他のホテルは100MbpsでNTT西日本の回線に接続され、その先はSINET、JGN2+、NSPIXP3、JPNAPに各々1Gbpsで接続されました。主にAlaxala社とCisco社の機器が使われました。NSPIXP3とJPNAPから先では、NTTコミュニケーションズ、KDDI、IIJの3社によって接続サービスが提供されました。

- 無線LAN

これまでのIETFと同様に複数の規格で提供されました。クライアント数を以下に示します（2009年11月11日時点）。最大で854クライアントが接続しました。

802.11g: 324　802.11n: 255
802.11a: 149　802.11b: 10

会場1階のレストランでは、ガラス張りのワインセラーの中に基地局が設置され、カバー範囲を広げるとともに、NOCチームのユーモアが現れていました。

- IPv6

総トラフィックのうち約7%がIPv6でした。これにはGoogleのDNSサーバで、WebサーバのAAAAレコードが返されるような設定変更が会期中に行われたことが影響したようです。

今回のネットワークは、特に障害が発生せず大変安定していたことから、IETF参加者のメーリングリストでNOCチームに感謝する旨のメールが数多く飛び交っていました。

○IETFチェア報告など

IETFチェアのRuss Housley氏からは、RFCの公開状況などについて報告がありました。

- RFCの作成状況

前回（IETF-75）以降、RFCは104公開されました。合計で約3,077ページあるそうです。

- Code Sprint

ミーティングの前日に、IETFのWebページなどのプログラミングを行うセッション“Code Sprint”が今回も行われました。今回は、IETFのコンテンツ管理に使われている、Djangoの1.1へのバージョンアップが行われました。

IAOC（IETF Administrative Oversight Committee）とIAD（IETF Administrative Director）のレポートは、Bob Hinden氏とRay Pelletir氏によって行われました。

- 2009年度のIETF運営状況

今のところ参加者数は計画の範囲内ではあるものの、当初予算に比べて収入が減りました。一方、会議費における飲料費の低減化を図るなどし、支出も減りました。ISOCからの追加補助は不要である見込みです。

- 2010年度の予算

2010年度の予算が承認されました。IETFミーティングの参加費は635ドルに据え置かれる予定です。


■ ReceptionでスピーチをするWIDEプロジェクト代表の村井純氏

◆Technical Plenary概要

Technical Plenaryは、ミーティング参加者全体で技術的な議論を行う全体会議（Plenary）です。11月12日（木）の16:30から3時間ほど行われました。

- IRTF（Internet Research Task Force） Chair's report

二つのResearch Group（RG）の紹介が行われました。Anti-Spam Research Group（ASRG）は、スパム対策のRGで、現在はブラックリスト管理に関するドラフトの作成が行われています。Scalable, Adaptive Multicast Research Group（SAMRG）は、複数の方式のマルチキャストに関するRGで、“ハイブリッドマルチキャスト”と呼ばれる複数の方式が組み合わされたマルチキャストの、テストベッドの構築が行われています。

- IAB（Internet Architecture Board） Chair's report

逆引きに使われるTLDである「.ARPA」における署名レコードの提供が計画されています。2009年第4四半期に一時的なセットアップが行われ、2010年第2四半期にルートゾーンを管理するためのアーキテクチャへの組み込みが行われるスケジュールとなっています。

○ドメイン名や識別子の国際化に関する議論

今回のTechnical Plenaryにおける議論のテーマは、ドメイン名や識別子の国際化（Internationalization in Names and Other Identifiers）です。はじめに、アルファベット以外の文字列がドメイン名やパス名で使われるケースを紹介し、文字列同士の比較やマッピングなどの処理が持つ複雑さが説明されました。

IABでは、ドメイン名と文字列のエンコーディングに関する考察の結果をドキュメントにまとめる作業が行われています。

会場では、複数のコード体系がある中でbackward compatibility（後方互換性）を保つにはどうすればいいのかといった疑問が投げかけられたり、誤認しやすいURLを使ったフィッシングを防ぐためにどうすればいいのか、といった議論が行われました。

□IAB Thoughts on Encodings for Internationalized Domain Names
http://tools.ietf.org/html/draft-iab-idn-encoding-01

◆IETFミーティングに合わせて行われたイベント

今回のIETFでは、会期中以下のイベントがありました。いずれもランチの時間を使ったセッションで、会場のホテルで行われました。

- ISOC Briefing Panel: “Internet Bandwidth Growth: Dealing with Reality” - 11月10日（火）

近年のさらなる広帯域化の影響と広帯域アプリケーションの影響などについて、トラフィックの統計を取っている研究者などによるパネルディスカッションが行われました。

- Challenges to the Future in WIDE Project - 11月12日（木）

ホストであるWIDEプロジェクトによる最新動向の紹介が行われました。同プロジェクトの村井純氏、江崎浩氏に加え、パナソニック電工株式会社と日本放送協会のスピーカーによる、さまざまなIPの適用場面について発表が行われました。

◆今回のIETFについて

■「Chanllenges to the Future in WIDE Project（2009年11月12日）」の案内板

今回、ミーティング参加者用のMLのやりとりが、とても活発でした。通常は“本MLは稼動していますか?”といった質問が投げられることがあるほど静かなMLですが、今回は、広島への行き方に始まり、市内のサッカー/フットサル場や、空手道場がどこにあるかといった質問、さらに広島という地名の由来、RFIDの活用法など、さまざまな情報交換に使われました。質問には、WIDEプロジェクトのメンバーが、一つ一つに丁寧に対応していたのが印象的でした。

◇　　◇　　◇

次回の第77回IETFは、2010年3月21日～26日、米国のアナハイムで開催される予定です。

（JPNIC 技術部/インターネット推進部 木村泰司）

■ DNS関連WG報告

◆dnsext WG

今回のdnsext WG会合では、TCPによるDNS問い合わせに関する話題が多くとりあげられました。これは、DNSSECの導入によりクエリサイズが大きくなることを解決する方法としての、TCPクエリの利用を想定した議論となっています。

draft-ietf-dnsext-dns-tcp-requirementsの発表では、RFC1123においてTCPによるDNSクエリ応答のサポートがSHOULDと明記されており、それをMUSTに変える必要があるのではないかと提案がありました。またEDNS0といった提案もあり、いまだUDPによるDNSクエリが一般的ではあるが、DNS実装としてはTCPを必須項目にするべきだ、と提案がなされました。しかしこの提案に対して、CPEといった小型の機器に内蔵されるDNS Proxy等はTCPをサポートしていないものが多く、EDNS0とTCPどちらもまだ、必ず機能するというものではないため、対策が必要であるとの認識がなされました。

次に、“TCP for DNS security consideration”という発表が行われました。これは、TCPに発見されているセキュリティ問題（draft-ietf-tcpm-tcp-security）に対して、DNSとしてどう対応すべきかという提案です。HTTP Keep Aliveと同じように、永続的にDNSサーバ間でTCPコネクションを保つような仕組みが必要になるかもしれないので、DNSクライアントは積極的にTCP active closeを行うべきだという提案がなされました。DNSクエリにTCPが本格導入されるにあたっての注意点を提起する発表となりました。


■ 会場の様子

また、APNICのGeoff Huston氏から、“An Experiment in Implementing a Stateless TCP DNS Server”という発表が行われました。これはDNSクエリ応答のために簡略化されたTCPを用いるという提案です。もっとも、本人はこの提案を“Really a Bad Idea!”と言っており、本気で提案したわけではないのですが、思いついて実験してみたらできてしまったので紹介した、というもののようです。ユーザーランドでTCPによるDNSクエリを受け取って、DNSサーバに仲介するというDNS Proxyモデルです。

以上のような、TCPによるDNSクエリに関する話題が会合の中心となりました。DNSSECの導入をにらんだ、現実的な提案が行われていたように思われます。

◆dnsop WG

dnsop WG会合では、DNSSEC鍵更新に関する話題、ならびにDNSSECのトラストアンカーに関する話題に多くの時間が割かれました。

まずdraft-morris-dnsop-dnssec-key-timingについての発表が行われ、DNSSECのZSK、KSKの鍵更新を行うタイミングに関して提案がなされました。発表後の質疑応答では、署名アルゴリズムの導入や削除に関する記述がもっと必要との提案がありました。ゾーンの署名サービスを提供しているOpenDNSSECも、この提案に基づいて鍵更新を行っているそうです。引き続き議論が行われます。

また、draft-ljunggren-dps-frameworkに関する発表も行われました。これは、ドメイン名レジストリに対して.seにおけるDNSSEC署名の経験を踏まえた提案を行っている文章です。署名されたゾーンの生成や更新、鍵の更新時における処理等を提案した文章となっています。

他には、CNNICの方がIDN TLDに関する発表を行いました。日本よりも漢字のバラエティが多い中国では、“bank.中国”と“bank.中國”の扱いをどうするのか、等大きな議論になっているようです。

◆Root DNSSEC Presentation with Q&A

IETF76において、公式なBoFではないのですが、オープンな会合として“Root DNSSEC Presentation with Q&A”という会合が開催されました。これは、Root DNSオペレーターやレジストリ、ICANNの有志からなるRoot DNSSECデザインチームによる、Rootゾーンの署名計画の報告と質疑応答が行われた会合です。まずRootゾーンの署名時期や、鍵管理の仕組みについて報告がありました。そして鍵の所有者を明確に定義し、VeriSign社が行う

ゾーン署名のシステム説明とその流れが報告されました。その後の質疑応答では、鍵が盗まれた際の緊急処理やゾーンの緊急再署名に関する話題を中心として、活発な議論が行われました。

署名されたRootゾーンの提供は、2010年7月までに行われる予定となっており、DNSSECの導入が急速に始まろうとしている感がうかがえました。

（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）

■ IPv6関連WG報告

本稿では、第76回IETFミーティングの会期中に議論されたIPv6に関連したトピックスのうち、IPv6に特化した内容を議論するWGでの話題を中心に紹介します。

◆6man WG（IPv6 Maintenance WG）

6manワーキンググループは、IPv6プロトコルのマイナーなメンテナンスを実施しているWGです。今回のミーティングは、11月10日（火）の午前最初のコマにて、開催されました。

会議は、前回と同様、チェアよりのミーティングの議題確認および、WGで取り組み中である文書のステータスについての報告から始まりました。現在、6man WGにて正式に取り組み中の文書（WG document）は、

・フラグメント重複問題（IESG※1 review中）
・ノード要求仕様（メーリングリストで議論中、アジェンダからは落ちました）
・アドレス選択（今回、議論されました）
・IPv6推奨アドレス表記（今回、議論されました）
・IPv6サブネットモデル（ワーキンググループラストコール中:ラストコールは最終合意のこと。以下、Working Group Last Callを略してWGLCと表記。）※2009年11月14日に終了
・経路制御ヘッダ（WGドラフト化）

の六つとなっています。

今回のミーティングの議題は、

・IPv6アドレスのテキスト表記方法（draft-ietf-6man-text-addr-representation）
・6LoWPANでの近隣探索（draft-ietf-6lowpan-nd）
・アドレス選択に関する次へのステップ
  - アドレス選択ポリシー間の矛盾解決（draft-arifumi-6man-addr-select-conflict）
  - アドレス選択デザインチーム議論報告（draft-ietf-6man-addr-select-considerations）
・近隣探索キャッシュの更新について（draft-kitamura-ipv6-neighbor-cache-update）
・P2Pリンクでの/127プリフィクス長の利用（draft-kohno-ipv6-prefixlen-p2p）
・ノード要求仕様文書に関する議論（draft-ietf-6man-node-req-bis）
・IPv6のUDPチェックサムついて（draft-fairhurst-tsvwg-6man-udpzero）

となっています（上記の通り、ノード要求仕様については簡単なコメントのみで議論されませんでした）。このうち、いくつかについて簡単に紹介します。

・IPv6アドレスのテキスト表記方法

前回のミーティング、およびその後のメーリングリスト（ML）での議論で、6man WGとして取り組んでいくことに合意し、今回のミーティングの前にWGLCが終わっていました。ミーティングでは、IETF75からの変更点について簡単に解説がありました。会場からのコメントも、文章表現についての簡単なもので、RFC化に向けて進めることになっています。

・アドレス選択問題について（アドレス選択ポリシー間の矛盾解決）

今回も引き続き、IPv6サイト/ホストがアドレスプリフィクスを複数持った場合の、アドレス選択のあり方の検討状況報告がありました。前回は、複数の上流から矛盾するアドレス選択ポリシーが配布された場合の、コンフリクトの解消（ポリシーのマージ）についての提案・議論がありましたが、今回は、主にポリシーを配布するプロトコルについての議論がありました。プロトコルとして、ルータ広告、DHCPv6、もしくは経路制御プロトコルのオプションを利用する場合の利点、欠点の検討紹介について、どれか一つに決めるべきである、DHCPv6でも情報をアップデートは可能、といったコメントがありました（その後、MLでも手法についての議論が延々と続いています）。提案文書について、より多くのコメントが欲しい、とのことです。

・P2Pリンクでの/127プリフィクス長の利用

現在、アドレスのプリフィクス長に/127を利用することはIPv6の仕様的に問題があるとされており、/127のプリフィクスを使用することの問題点を記述した文書（RFC3627）も出版されています。これに対して、特にオペレーションの観点から、P2Pリンクにて/127より短いプリフィクスを利用することの問題点を提示し、P2Pリンクでの/127の利用を明示的に可能とすることについての提案です。リンクローカルアドレスに関する問題等仕様上の注意点が指摘はされましたが、賛成も多く、今後WGとして継続して議論することになると思われます。

・IPv6のUDPチェックサムついて

ここしばらくIETFで議論されている、UDPにおけるチェックサム計算をしなくてもよいことにする提案に関する議論です。IPv6では、IPv6ヘッダにチェックサムがないため、IPv4と違ってUDPにおけるチェックサムの計算を必須としています。しかしながら、UDPを利用したトンネルの際に、トンネルの中を通るパケットレベルで相当のチェックをしている場合には、外側のUDPでのチェックサム計算が必要ない、途中のルータでトンネルリンクにパケットをフォワードする際に、UDPチェックサムを計算するコストが高くなってしまう、などが問題とされていました。今回は、計算コストに関する議論、チェックサムを廃止した場合の影響が検討され、ミーティング中の議論では、UDPのチェックサム処理への変更は実施しない方向となっています。

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

□第76回 IETF 6man WGのアジェンダ
http://www.ietf.org/proceedings/76/agenda/6man.html

◆v6ops WG（IPv6 Operations WG）

v6opsはIPv6に関するオペレーション技術や、移行技術に関する議論を実施するWGです。今回は、11月10日（火）、11月12日（木）午後最初の、合計2コマにて議論が実施されています。今回も、数々の新提案があり、内容も多岐にわたっていました。

議論内容は以下の通りです。

11月10日（火）
・家庭向けIPv6インターネットサービス提供用CPEにおける簡易セキュリティ推奨機能（draft-ietf-v6ops-cpe-simple-security）（アジェンダから消されました）
・IPv6 CPEに関する高機能セキュリティ（draft-vyncke-advanced-ipv6-security）
・BitTorrentネットワークでのIPv6トラフィック測定（draft-defeche-ipv6-traffic-in-p2p-networks）
・IPv6 CPEルータ推奨機能（draft-ietf-v6ops-ipv6-cpe-router）
・IPv6 CPEルータ拡張推奨機能（draft-wbeebee-v6ops-ipv6-cpe-router-bis）
・IPv4/IPv6共存フレームワーク（PET）（draft-cui-softwire-pet）
・PETでのIPv6からIPv4への通信（draft-cui-softwire-pet64）
・Internet Exchange（IXP）でのIPv6ディプロイメント（draft-ietf-v6ops-v6inixp）

11月12日（木）
・ICPに対するISPのIPv6移行サービスのプロビジョンに関する推奨（draft-qin-v6ops-icp-transition）
・IPv6ディプロイメントに関する新サービスプロバイダシナリオ（draft-carpenter-v6ops-isp-scenarios）
・IPv6移行のための段階的キャリアグレードNAT（CGN）導入（draft-jiang-v6ops-incremental-cgn）
・ISATAPと6to4における経路ループ ： 問題提起と解決案（draft-nakibly-v6ops-tunnel-loops）
・Teredoの拡張（draft-thaler-v6ops-teredo-extensions）
・IPv4サーバにアクセスするIPv6アプリケーションの構築（draft-wing-v6ops-v6app-v4server）

■ 会場となったANAクラウンプラザホテル広島

いくつかの内容について、簡単に紹介します。

・IPv6 CPEに関する高機能セキュリティ

IPv6 CPEに関する高機能セキュリティは、現在議論中である「簡易セキュリティ推奨機能」（当初、議題には挙がっていましたが、議論はされませんでした）に対する、より高度なセキュリティモデルとしての提案です。IPv6ネットワークは、IPv4グローバルアドレスを内部にも使っている企業ネットワークと同等であり、セキュリティポリシーを考える際に、企業で利用しているポリシーが参考にできると考えて、七つのホームネットワーク用セキュリティポリシーを提案しています。特に、CPEデバイスを外部から動的にアップデートすることで、より強固なセキュリティを担保できるようにすることの必要性を強調していました。提案に対する賛成意見もありましたが、一方で、これはIPv6に特化したものであるのか、また、動的アップデートには標準等は必要ないため、IETFでなく、ブロードバンドフォーラム等で議論すべき内容ではないかとの反対意見もあり、提案に対する賛成、反対も含め、MLで継続議論となりました（火曜日のセッション終了後、継続議論されています）。

・IPv6 CPEルータ推奨機能、IPv6 CPEルータ拡張推奨機能

ここ数回のIETFで議論を続けている、IPv6対応のCPEルータが持つべき機能に関する提案です。今回から、検討事項が多い部分を拡張機能として別ドラフト（フェーズ2ドラフト）に切り出し、WANとLANの設定や、基本的なルータ機能、セキュリティ機能のみを基本部分として分離しています。基本部分のドラフトについては、MLにて意見を集め、それを反映後にWGLCを実施することとなりました。フェーズ2ドラフトの議論項目としては、マルチキャスト、DNS、プレフィックスの再委譲、IPv6移行機能、パケットフィルタ、QoS等が挙げられており、議論を継続していくこととなりました。

・Internet Exchange（IXP）でのIPv6ディプロイメント

IXPにおけるIPv6導入モデルは、3度目の発表となります。今回は、AMS-IXで導入されている、余計なARPトラフィックを減少させるための仕組みであるARPスポンジと同等の機能を、IPv6で実装する方法についての検討報告がありました。ARPスポンジは、多くのIXPで導入されているそうです。IPv6では、近隣探索プロトコルへの対応となりますが、アドレス長の違い、利用されていないアドレスが広大なことによる必要資源の増加等が問題となるようです。会場からは、この問題はIXPに特有でなく一般的な問題である、利用されていないアドレス対策が必要なら、/64より長いプリフィクスを使ったらどうか、といった質問がありました。コメントを反映して改版後、WGLCに進むことになりました。

・ICPに対するISPのIPv6移行サービスのプロビジョンに関する推奨

ICPをどのようにIPv6対応にしていくべきかをまとめようとしている提案です。利用できる移行機構（デュアルスタック、NAT64、IVI）を列挙し、利用できるツール等をまとめることを目的としています。会場からは、重要な観点であり、利用可能な技術を集めて情報共有をすることは意味がある、という意見や、重要ではあるが、多くのプロトコルは現状、標準化中であったり、どれがよい、と選べるものではなかったりと、まとめ方には注意が必要だ、といった意見がありました。今後デザインチームを作って、各機構、ツールの利点、欠点、ユースケース等を議論することになっています。

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

□第76回 IETF v6ops のアジェンダ
http://www.ietf.org/proceedings/76/agenda/v6ops

◆softwire WG（Softwires WG）

softwire WGは、トンネルを用いてIPv4 over IPv6、またはIPv6 over IPv4通信を実現する方式を検討するWGです。現在扱っている方式は三つあります。一つはWGタイトルそのままのsoftwireと呼ばれる、IPv4 over IPv6またはIPv6over IPv4の汎用的なトンネル方式です。他にはDS-Lite（Dual Stack Lite）と呼ばれる、softwireのIPv4 over IPv6方式にCGN（Carrier Grade NAT）の機能を加味することで、IPv4アドレス在庫枯渇対策も含めたもの、そして6rd（IPv6 Rapid Deployment）と呼ばれる、IPv6アドレスの自動割り当ても含むIPv6 over IPv4トンネル方式があります。

これら三つの方式はいずれもまだ標準化が完了していませんが、それぞれが競合しているわけではなく、適用領域が異なっているとして、並行して標準化が進められています。

今回のセッションでは6rd、DS-Liteそれぞれについての標準化の進捗が報告され、いくつかの子細な部分に関する議論が行われました。6rdに関する議論では、Dave Thaler氏より6to4プロトコルで得られたNUD（Neighbor Unreachability Detection）の扱いや、routing loop問題への対策などの知見を盛り込むこと、また複数のBR（Border Router）を扱えるようにしてはどうか、といった提案がなされました。

DS-Lite方式の進捗に関しては、用語の変更などがあり、これまでCGNと呼ばれていたNAT装置を、AFTR（Address Family Translation Router）と呼ぶとの説明がありました。DS-Liteでも6rdと同様に、トンネル終端装置であるAFTR を二重化する話が議論され、6rdと違ってDS-LiteではAFTRがクライアント装置毎にstateを持つ必要があるため、より実現が困難であり、引き続き検討が必要であるということになりました。

その他、6rd over UDPといった、6rdに対する拡張の提案などがありましたが、根本的な仕様変更を伴う提案であったため、まずはベースとなる6rdの標準化が完了してから検討すべきであるとの結論に至りました。

6rdは今回の議論を反映した改訂版を作成し、すぐにでもWGLCに進む予定になっています。DS-Liteに関しては、AFTRの二重化に関する議論が終わればWGLCに進むものと思われます。

□第76回 IETF softwire WGのアジェンダ
http://www.ietf.org/proceedings/09nov/agenda/softwire.txt

□softwire WG
http://www.ietf.org/dyn/wg/charter/softwire-charter.html

◆aplusp BoF

IETFではIPv4アドレス在庫枯渇の対策として、ISP内でNAT装置（CGN）を用いる方法と、ユーザーにグローバルIPv4アドレスを割り当てつつ、利用できるポート番号の範囲を限定する、というA+P方式の二つが主に議論されてきました。今回のBoF（WG設立前のミーティング）では、このA+P方式全般というよりはさらにフォーカスをしぼって、DS-Liteのトンネル上でこのA+Pを行うという方式についての議論が行われました。

A+P方式の利点としては、ポート範囲が限定されてはいるものの、ユーザーに直接グローバルIPv4アドレスを配布できるため、NATに阻害されずに通信が可能であるということが挙げられます。欠点としては、ホストやルータに対する影響が大きいことなどが挙げられます。このDS-Liteのトンネル上でA+Pを行うことで、トンネル終端装置以外の装置（中継ルータなど）への影響を最小限に留める、といった狙いがあると思われます。

今回のBoFのゴールは、IETFがこの方式を扱うかどうかを決定すること、ということで、新たなWGを設立するか、既存のWGのアイテムとなるかといった選択肢が示されました。

セッションでは、まずA+Pの概要説明後、モバイル環境への適用についての提案、そしてA+Pに関する懸念事項、そしてフリーディスカッションの後に、今後の方針について決定する、という流れで検討が行われました。

フリーディスカッションでは多くの意見が交わされましたが、結局Dave Thaler氏によるA+P方式のTCP/IPプロトコルスタックへの微小な修正が、多大な影響をもたらすものであり、またそれはNATの導入とは質の異なる根本的な変化であるとの指摘に同意する人が多かったのか、WGの設立はおろか、本提案についてIETFで取り組むべきではないと感じる聴衆が大半を占めるに至りました。これらの意見はIESGにインプットされ、A+P提案が他のWGで扱われるか、などの決定がなされることになっています。

□第76回 IETF aplups BoFのアジェンダ
http://www.ietf.org/proceedings/09nov/agenda/aplusp.html

◆behave WG（Behavior Engineering for Hindrance Avoidance WG）

behaveは主にNATの挙動に関して扱うWGですが、その技術的な関連性の高さからIPv6-IPv4変換についての議論も行われています。今回も、そのIPv6-IPv4変換の議論や、その他のNATに関する議論など、多数のトピックがありました。

まず、チェアからWGの状況についての報告があり、IPv6-IPv4変換に関する提案については、Interim Meeting（IETFミーティング期間以外での中間ミーティング）を経て、当初最重要であるとした問題ケースを解決する提案として、ほぼ仕様策定が完了したとの報告がありました。次の五つの提案について、2009年12月にはWGLCを行うとし、5人のレビュアーが必要であるということで、ボランティアを募りました。

- Address Format
  draft-ietf-behave-address-format-01
- Framework for IPv4/IPv6 Translation
  draft-ietf-behave-v6v4-framework-03
- IPv6/IPv4 Translation

draft-ietf-behave-v6v4-xlate-03
- Stateful IPv6/IPv4 Translation
draft-ietf-behave-v6v4-xlate-stateful-02
- DNS64
draft-ietf-behave-dns64-02

その後、これらのそれぞれの提案について、変更点の報告などが行われました。Address Formatの提案では、Well Known Prefixのフォーマットについての議論や、またTranslationの提案では、パケットのフラグメントの扱いに関する詳細議論が行われましたが、特に大きな変更が必要となるような意見は出ず、今後もInterim Meetingを行いながら迅速に標準化を進めていくということになりました。

また、これらの提案以外に、ホスト自身でIPv6-IPv4変換を行うといった提案や、A+Pの考え方をIPv4からIPv6への変換方式に組み込むことで、IPv6ホストにIPv4グローバルアドレスを付与するといった提案など、さまざまなIPv6-IPv4変換に関する変更や拡張の提案がなされました。しかしながら、これらの提案は、現在注力している上記の方式の標準化が終わってから着手するべきであるとか、また他のWGで進められている技術と同一目的であるのでそこで議論するべきである、という意見が多数となっていました。

IPv6-IPv4変換だけでなく、IPv4-IPv4変換の議論も行われ、CGN装置の信頼性向上のための冗長化の議論、また複数のユーザーで同一のIPv4アドレスを共有するという観点から問題点、対策をまとめた文書などの発表がありました。これらの議論も継続して進めることになっています。

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

□第76回 IETF behave WGのアジェンダ
http://www.ietf.org/proceedings/09nov/agenda/behave.html

（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）

※1 Internet Engineering Steering Group（IESG）
IETFの活動と標準化プロセスの、技術的な側面についての責任を担っているグループです。IESGのメンバーは、IETFの複数のWGで文書のレビューを行ったり、WGの方向性について助言を行っているArea Directorで構成されています。IESGはInternet-Draftの標準化プロセスを進めるかどうかを決定し、IESGによって承認されるとRFC番号が割り振られ、RFCとしてIETFのサーバで公開されます。

■ セキュリティ関連WG報告

第76回IETFは、日本の広島にて、2009年11月8日から13日まで開催されました。2002年横浜以来の7年ぶりとなる日本での開催であることから、全参加者1,155名中363名と、日本人が一番多い結果となりました。また、会場のあちこちで積極的に議論に参加しているNew Comer（初参加者）を多く見ることができました。

毎回IETFでは、セキュリティに関連したWG（今回は13セッション）が開催され、世界中からいろいろな背景を持った参加者によって議論されています。幅広い領域において、WGが開催されているため、全てのセッションの内容を把握することが困難な状況です。そこで本稿では、会期中に議論されたセキュリティに関連したセッションのうち、認証や通信に特化した内容を議論するWGでの話題を中心に紹介します。

◆krb WG（Kerberos WG）

krb WGは、認証方式の一つであるマサチューセッツ工科大学（MIT）が開発したKerberos※1について、新規仕様の検討や実装のための検討を行うWGです。このミーティングは、11月11日（水）に開催され、参加者は20名程度でした。最初にチェアから、WG文書のステータスおよび今回のミーティングのアジェンダについて説明が行われました。

今回の会議は、FAST Negotiationに関する問題と、KDC（Key Distribution Center）のデータモデルにおけるEncryption typeについて技術的な議論を行うことを目的としており、それらについて会議の参加者たちが活発に発言していました。

前回の会議では、危殆化対策（暗号技術の世代交代）や新規アルゴリズムに関する議論が行われたので、今回の会議でも引き続き議論されることを期待していたのですが、それらについて議論されなかったので残念でした。

■ New comer's orientationで日本語のチュートリアルを行う江崎浩氏

□krb WG
http://www.ietf.org/dyn/wg/charter/krb-wg-charter.html

□第76回 IETF krb WGのアジェンダ
http://www.ietf.org/proceedings/09nov/agenda/krb-wg.txt

◆tls WG（Transport Layer Security WG）

tls WGは、インターネット上で情報を暗号化して送受信するためのプロトコルであるTLS（Transport Layer Security）について、仕様の拡張や新規Cipher suiteの検討を行うWGです。今回のミーティングは、11月12日（木）に開催され、参加者は100名程度でした。

最初にチェアから、WG文書のステータスおよび今回のミーティングのアジェンダについて報告がありました。今回のミーティングで議論の対象となった提案は、以下の通りです。

・TLS Cached Info
・Additional PRF Input
・TLS Renegotiation Vulnerability

今回のミーティングでは、ミーティング時間の大半を使って、2009年11月に発見されたTLS Renegotiationにおける脆弱性に関する議論が中心に行われました。この脆弱性について詳細を知りたい場合には、本ミーティングの発表資料やInternet-Draftをご参照ください。

◇TLS Renegotiation Vulnerability

・発表資料
http://tools.ietf.org/agenda/76/slides/tls-7.pdf
・Internet-Draft:Transport Layer Security（TLS）Renegotiation Indication Extension
http://tools.ietf.org/html/draft-rescorla-tls-renegotiation-00

また、今回発見された脆弱性は、他のプロトコル（例えば、IMAP、LDAP、XMPP、SIP、SMTPなど）も同様に起こり得るかもしれないとの指摘がされていました。

ミーティングで議論された内容として、技術的な内容の他にTLSプロトコル実装者への影響などを考慮して、今後のマイルストーンや進め方について、入念に議論が行われていました。

□tls WG
http://www.ietf.org/dyn/wg/charter/tls-charter.html

□第76回 IETF tls WGのアジェンダ
http://www.ietf.org/proceedings/09nov/agenda/tls.txt

◆ipsecme WG（IP Security Maintenance and Extensions WG）

ipsecme WGは、2005年にクローズされたIPsec WGの後継WGであり、IPsec WGがクローズされてから必要になった拡張や、既存ドキュメントの明確化などの議論を行うためのWGです。このミーティングは、11月12日（木）に開催され、参加者は40名程度でした。会場となった部屋が比較的に狭かったため、立ち見が出るような状況でした。

ミーティングの流れとしては、今回のアジェンダについて説明が行われ、参加者からコメントがなかったため予定通り会議が開始されました。

ipsecme WGとしての初めてのRFC（RFC 5685 IKEv2 Redirect）が発行されたことが周知され、多くの参加者から拍手が送られました。また、TAHI Projectから、The 10th TAHI Test Eventが2010年1月25日～29日に千葉で開催されることが周知されました。

今回、発表された議題は以下の通りです。

・A Childless Initiation of the IKE SA
・Labeled IPsec
・EAP-Only Authentication in IKEv2
・Secure Pre-Shared Key Authentication for IKE
・A Quick Crash Discovery Method for IKEv2
・WESP Extensions
・IPsec High Availability

今回、実験的な試みとして、Labeled IPsecでは、発表者がリモートから音声によるプレゼンテーションを行いました。実際に参加した感想としては、音声もクリアで聞き取りやすく成功だったのではないかと思いました。このような仕組みが本格化することで、今まで参加できなかったような人たちにも、IETFで発表するチャンスを与えられるのではないかと考えました。

□ipsecme WG
http://www.ietf.org/dyn/wg/charter/ipsecme-charter.html

□第76回 IETF ipsecme WGのアジェンダ
http://www.ietf.org/proceedings/09nov/agenda/ipsecme.txt

（NTTソフトウェア株式会社 菅野哲）
（NTTソフトウェア株式会社 小林千夏）

◆SIDR WG（Secure Inter-Domain Routing WG）

SIDR WGは、インターネットにおける経路制御のセキュリティ・アーキテクチャについて検討を行っているWGです。WG Last Call（WGLC）となるInternet-Draft（I-D）が出揃ってきました。WGLCとは、WG内でドキュメントを変更する必要性がないかどうか、一定の期間を取り最終確認をすることです。第76回IETFでは、SIDR WGのミーティングが2日目（11月9日）の午前9時から1時間半程行われました。参加者は80名程でした。

SIDR WGでWGLCの状態になっているI-Dを、以下に示します。

- An Infrastructure to Support Secure Internet Routing
  draft-ietf-sidr-arch-09
  RPKIの全体構造や概念を述べたドキュメントです。

- Certificate Policy（CP）for the Resource PKI（RPKI）
  draft-ietf-sidr-cp-07
  リソース証明書の発行条件を定義したドキュメントです。RIPE NCCのAndrei氏のコメントを受けた修正が終わりました。

- A Profile for Route Origin Authorizations（ROAs）
  draft-ietf-sidr-roa-format-06
  ROAの書式を定義したドキュメントです。

- A Profile for Resource Certificate Repository Structure
  draft-ietf-sidr-repos-struct-03
  リソース証明書などの格納や公開の仕方を定義したドキュメントです。公開サーバと登録オブジェクトの命名方法に関する提案がなされています。

- A Profile for X.509 PKIX Resource Certificates
  draft-ietf-sidr-res-certs-17
  リソース証明書の各フィールドの内容を定義したドキュメントです。

これらは、ほぼ議論が終わっており、大きな変更はない見込みです。ただ、RPKIで使われる暗号アルゴリズムの記述をまとめた次のドキュメントが新たに作成されたため、これらのドキュメントでは、各々記述を持つのではなく、これを参照する形に変更されました。

- A Profile for Algorithms and Key Sizes for use in the Resource Public Key Infrastructure
  draft-ietf-sidr-rpki-algs-00
  RPKIで使われる暗号アルゴリズム、ハッシュアルゴリズム、鍵長などについてまとめたドキュメントです。デフォルトではSHA-256と2,048bitのRSAが使われることになっています。

SIDR WGのアジェンダの最後で、2009年9月にISOC主催で行われた会議「RPKI Operators Roundtable Report and Discussion」の報告がありました。この会議は、RPKIに関するルーティング・オペレーターのニーズを確認するために開かれたもので、米国、日本、ヨーロッパのISPでルーティングに携わっている技術者を中心に、参加者が構成されました。SIDR WGでドキュメント策定に関わっている主要なメンバーは招待されなかった模様です。

下記のレポートには、以下のようなポイントがまとめられています。

- 参加者の間で確認された、RPKIに対するニーズ
  - ・RPKIにおいてはIPv4とIPv6のサポートが必要である。
  - ・IPアドレスの一意性の担保は必要である。
  - ・IPv6のデータ（登録情報）をきれいにする必要がある。（IPv4は難しいので後にする）
  - ・リソースホルダーの認証（レジストリごとの対応）が必要である。
- 参加者間における認識の違い
  - ・IRR（RADB）とWHOISとでどちらがクリーンか。
  - ・単一のルート（例えばIANAやNRO）は必要か。
  - ・BGP（プロトコル）を変えずにpath validationはできるか。
  - ・リージョンごとにIPアドレスやルーティングの正しさに関する認識や状況は異なる。
- 参加者が共通に認識している課題。
  - ・RPKIに関する共通のツール開発が必要である。
  - ・Origin Validationの仕組み（draft-ymbk-rpki-rtrprotocol）。

□"Securing Routing Information - Findings from an Internet Society Roundtable", September 2009
http://www.isoc.org/educpillar/resources/docs/routingroundtable_200909.pdf

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

PKIX WGは、インターネットのための、PKI技術の策定に取り組んでいるWGです。ミーティングは、3日目の11月10日（火）午後1時から2時間程、行われました。参加者は30名程でした。

新たに以下のドキュメントがRFC化されました。

- Elliptic Curve Cryptography Subject Public Key Information（RFC 5480）
  電子証明書発行先の公開鍵暗号として、楕円暗号のアルゴリズムを使うためのアルゴリズムIDと構造を定義したドキュメントです。以下のアルゴリズムを使うことができます。

  - Elliptic Curve Digital Signature Algorithm（ECDSA）
  - Elliptic Curve Diffie-Hellman（ECDH）family schemes
  - Elliptic Curve Menezes-Qu-Vanstone（ECMQV）family schemes

WGで作業中となっている主なドキュメントの状況を、以下にまとめます。

- Trust Anchor Management（TAM）関連
  PC以外の機器を含むPKIアプリケーションで、トラストアンカーのデータを管理するためのプロトコルなどのドキュメントです。Trust Anchor Formatに関するドキュメントdraft-ietf-pkix-ta-format-04はIESGのレビューが行われている状態で、プロトコルを定義したdraft-ietf-pkix-tamp-04は今後WGLCがかけられる見込みです。

- OCSP Algorithm Agility
  OCSPで使われる暗号アルゴリズムを、複数候補から選べるようにする仕組みの提案です。議論は特になく、今後WGLCがかけられる見込みです。

- Certificate image
  証明書の証明内容や発行元、発行先のイメージデータを入れる提案です。PDF（Portable Document Format）とSVG（Scalable Vector Graphic image）が入れられるようになっています。議論は特になく、今後WGLCがかけられる見込みです。

PKIの仕様に関係して行われた、主なプレゼンテーションを次にまとめます。

- RFC 5280 Implementation Report, 発表者 Tim Polk氏
  RFC 5657に基づく実装の調査報告です。実装が存在することを提示することで、RFC5280をProposed Standard（PS）からDraft Standard（DS）にする（格上げする）活動として行われています。

  PKIX WGのMLに投げられたS/MIMEメッセージを収集し、米国NISTのPublic Key Interoperability Test Suite（PKITS）を使って検証が行われました。国際化対応については、確認が行われませんでした。

  今後、RFC5280にはErrataの修正を行った上で、調査報告書を添えてDraft Standardをめざすようです。

- Certificate information expression, 発表者 Stefan Santesson氏
  電子証明書のフィールドに、EUで進められているSTORKプロジェクト※2で使われる「マッピングの情報」を含める提案です。STORKプロジェクトで課題となっている、EU内の各国間で、発行されている証明書を対応付けるマッピングの必要性についてプレゼンテーションが行われていました。

この他に、ホスティングサーバの間で行われるXMPP連携で使われる属性証明書の必要性や、Digital Right Management（DRM）のためのProxyアーキテクチャの提案、TLSでサービスごとに異なる識別子に関する共通ルールの提案などが行われました。

◇　　◇　　◇

日本での開催とあって、会場では多くの日本人を見かけましたが、SIDR WGやPKIX WGの議論でアクティブなのは相変わらずの常連メンバーでした。この二つのWGは、他のWGでも活躍しているIETFの常連メンバーによって成り立っている側面があり仕方がないことではあるのですが、日本からも抽象度の高いハイレベルな議論に参加していきたいとあらためて感じました。

（JPNIC 技術部 木村泰司）

※1 Kerberos認証
共通鍵暗号を用いるネットワーク認証方式の一つです。

※2 STORK（Secure idenTity acrOss boRders linKed）プロジェクト
http://www.eid-stork.eu/