2010.8.24▶8.27

APNIC30ミーティング報告

■ 全体報告

今回のAPNICミーティングは、日本人も多く訪れるオーストラリア最大の観光保養地、ゴールドコーストで開催されました。

・開催期間：2010年8月24日～8月27日
・開催地　：オーストラリア、ゴールドコースト
・会場　　：サーファースパラダイス・マリオットリゾートアンドスパ
・参加者　：オンサイト　183名
　　リモート会場　24名
　　リモート参加　165名

実は当初開催地としてバンコクが予定されていたのですが、反政府デモで政情が不安定なことから、開催の3ヶ月前に急遽APNICオフィスから1時間程度でアクセスできる、本開催地に変更したという経緯があります。当初の想定外ではありましたが、2000年のブリスベンでの開催以来、ちょうど10年ぶりにAPNICの地元での開催となりました。

アドレスポリシーについては、今回議論の対象となった5点のうち、提案者の意思により今回の提案としては取り下げられ次回持ち越しとなった1点を除き、残り4点の提案はすべて継続議論となり、APNICミーティング後、施行するポリシーがないという珍しい結果で終了しました。

◆プログラム

プログラム構成は従来同様、初日にトレーニング・チュートリアル、最終日にAPNIC総会を行い、APOPS、ポリシーSIGを主な軸として、その他の時間にPlenaryや各種BoF等が割り当てられていました。

今回、議論の行方が一番注目されていたセッションは、新たに設けられたプログラム"Member Petition BoF"です。これは、APNICのフォーラム運営会則の改定を求める提案が、インドのコミュニティメンバーからポリシーSIGに提出されたことに対応したものです。

提案では、APNIC EC（Executive Council）選出方法の変更等、APNICフォーラムの組織運営に関する改善を求めており、ポリシーSIGで取り扱うテーマではないとSIGチェアが判断したため、ECで協議の結果、専用のBoFを設けて議論を行う運びとなりました。

また、ミーティング最終日のAPNIC総会には、距離的に近いこともあって、普段はカンファレンスに参加しないバックオフィスのAPNICスタッフも顔を出しており、私自身も普段メールだけでやりとりを行っている担当者に直接会って話をすることができました。

◆Member Petition BoF

Member Petition BoFで議論されたAPNIC組織運営に関する改善については、前回のAPNIC29ミーティング以来、ECの選出方法の改定や政府関係者の関与の必要性を主張するインドのコミュニティメンバーと、その他メンバーとの間でメーリングリストでの議論が白熱していた経緯もあり、どのようなかたちで決着させるのかが注目されていました。また、アドレスポリシーと料金改定以外のテーマで、コミュニティメンバーから提案が行われたことはフォーラム上初めてのことでもあります。

組織運営上のルールはAPNICの定款で定められており、全会員票数の2/3以上の賛成をもってしか変更することができません。そのため、BoFでは冒頭で、定款変更などに必要な請願（petition）プロセスについて、説明が行われた後、ポリシーSIGに提出された三つの改定案が発表されました。

■ APNIC30はオーストラリア最大の観光地ゴールドコーストで開催されました

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

・EC選挙における投票権を1会員1票に限定する

・再選されたECの就任期間に上限を設ける

・政府機関の意見を取り入れられるGAC（Governmental Advisory Committee; 政府諮問委員会）の新設を求める

このうち、EC選挙における投票権を1会員1票に限定する提案と、政府機関の意見を取り入れられるGACの新設を求める提案の2点については、改定の必要性を検討していくことが合意され、ワーキンググループも設立されることになりました。

メーリングリストでの議論の流れからは、こうした合意に達することが難しいように見えましたが、共通の現状認識に基づいて今後議論を進める土台はできたと考えられます。今回のようにAPNICフォーラムにおいて、政府が議論できる場を設ける必要性について公式に議論されたことは初めてです。

◆アドレスポリシー提案の結果

＜次回持ち越しとなった提案＞

prop-083：IPv6追加割り振りにおける別要件の新設

＜継続議論となった提案＞

prop-084：定期的なWHOIS情報の更新要請

prop-085：APNIC最後の/8在庫からのクリティカルインフラへの割り当て

prop-086：IANA在庫枯渇後のIPv4割り振りに関するグローバルポリシー

prop-087：IPv6の実装実現のためのIPv6アドレスの割り振り

このうち、prop-086は、在庫枯渇後にRIRに返却されたアドレスの管理方法を定義したものです。現在の提案内容は、RIRからIANAへの返却が任意であるために実効性が薄く、必要性が理解できない等の理由から支持されませんでした。

ただし、現在はIANAからRIRへの最小分配単位が/8という大きなブロックであるため、在庫枯渇に向けて、より小さな単位での未割り振りアドレスも分配可能とする必要があるのではとのコメントはありました。

prop-087については、6rd（IPv6 rapid deployment）の実装に向けたIPv6アドレスポリシーを定義することを目的として、国内のアドレスポリシーフォーラムで議論を行い、そこでは支持の得られなかった提案を改めたものです。APNICフォーラムでは、提案の意図自体は支持できるとのコメントも表明されていた一方、運用を工夫することで必要とするアドレスサイズを小さくしながら、6rdの実装を実現できないのかとの確認が議論の焦点となり、継続議論となりました。

それぞれの提案概要については、下記URLよりご参照ください。

http://www.apnic.net/community/policy/proposals

◆選挙の結果

今回のミーティングでは、以下三つのポジションに対する選挙が行われました。

http://meetings.apnic.net/30/elections

・NRO NC[※1]
Naresh Ajwani氏（再選）

前回のEC選挙プロセスについて問題提起が行われたこともあり、これまでにないほど丁寧にプロセスの説明が行われていました。票カウントにあたっても細かい点まで状況が共有され、コミュニティへの確認が行われていたことも印象的でした。

・SIG Chair/Co-Chair[※2]
Policy SIG Chair:Gaurab Raj Upadhaya氏
（旧Chair:Randy Bush氏）
NIR SIG Co-Chair:Ji-Young Lee氏
（旧Co-Chair:Ching-Heng Ku氏）

◆その他:IPv4 Tomorrow?

このPlenaryセッションでは、APNICのIPv4アドレス在庫枯渇に向けたアドレス管理に関する3点の課題への対応について、APNIC事務局からコミュニティに問いかけが行われ、それぞれ以下の結論となりました。

・最後のIPv4 /8在庫空間の特定
どの/8プリフィクスから最後の/8ポリシー[※3]を適用するべきかは、運用上の課題としてAPNIC事務局の判断に一任

・在庫枯渇後に返却されたアドレスの管理
セッションでは明確な結論が出ずその後、APNICにおける在庫枯渇後に返却されたIPv4アドレスはすべて最後の/8の分配ポリシーを適用するよう、APNIC31に向けてコミュニティメンバーが提案[※4]を提出

・APNIC管理下のIPv4 /8における最小プリフィクスの変更
最小移転単位に合わせてAPNIC管理下の全/8における最小分配プリフィクスの表記を/24とし、文中に最小割り振り単位を記述

http://www.apnic.net/publications/research-and-insights/ip-address-trends/minimum-allocations

◆ミーティングを振り返って

ここ最近のミーティングの傾向としては、これまで中心に進めてきたネットワーク運用やアドレスポリシーに関する議論に加え、前回のミーティング[※5]ではITUにおけるIPv6アドレスの管理、今回はEC選挙のプロセス、および地域内の国や経済圏の意見をどうAPNICフォーラムに反映していくのかといった、ガバナンスの話にテーマが拡張しつつあることを感じました。

実際、今回もアドレスポリシー提案よりも、EC選挙プロセスをはじめとしたAPNICフォーラム運営方針の改定について、活発な議論が行われていたことが印象的でした。

アドレス管理面では、IPv4アドレス在庫枯渇に向けて必要となる大枠のポリシーは施行されているため、個々の未対応のケースはまだ提案されてはいるものの、ポリシー以外の現在フォーラムを取り巻く課題に関心がシフトしてきているのかもしれません。

なお、今回議論されたアドレスポリシー提案は、基本的にすべて継続議論となったため、次回香港で開催されるAPNIC31ミーティングで再度議論が行われます。

◆次回のミーティング

次回のAPNICミーティングはAPRICOT 2011と併せて、2011年2月に香港で開催される予定で、この号が発行される頃にはミーティングの結果を以下のURLからご覧いただけるようになっているかと思います。

□APNIC31
http://meetings.apnic.net/31

（JPNIC IP事業部 奥谷泉）

※1 NC（Number Council）
各RIRの地域ポリシーフォーラムから選出された2名と、各RIRの理事会から指名された1名の計15名からなる組織で、グローバルポリシーに関する判断などを行っています。

※2 SIG Chair/Co-Chair
SIG（Special Interest Group）セッションの議長を務め、提案事項があった場合はコンセンサスの判断を行います。

※3 最後の/8ポリシー
APNICにおける通常在庫枯渇後は、別途リザーブしている当該/8空間からの分配に切り替えます。この空間からの分配は1組織一律/22（1,024ホスト）に限定されます。

※4 prop-088: Distribution of IPv4 addresses once the final /8 period starts
http://www.apnic.net/policy/proposals/prop-088

※5 JPNIC News&Views vol.731「APNIC29ミーティング報告 [第1弾] 全体報告」
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2010/vol731.html

APOPSレポート

APNIC30ミーティング内の1セッションとして開催された、APOPS（The Asia Pacific OperatorS Forum）についてご報告します。APOPSは、アジア太平洋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す。APNIC30では、2010年8月25日（水）10時から15時30分にかけて、九つのプレゼンテーションが発表されました。

本稿では、紹介されたプレゼンテーションのうち、ネットワークの調査・計測に関する三つのアジェンダについてご報告します。

◆Measuring traffic in 1/8, 14/8, and 223/8

APNICのGeorge Michaelson氏から、1/8、14/8、223/8といった各アドレスブロックにおけるトラフィック量の調査について紹介がありました。1/8、14/8、223/8は、今年になって新規にAPNICへ割り振られたアドレスブロックで、それぞれのブロックには以下のような特徴があります。

- 1/8 “1”で始まる特徴的な数字を持ったアドレスブロック
- 14/8 X.25との接続のために使用されていたアドレスブロック
- 223/8 プライベートや実験目的のアドレスとして使用されやすいアドレスブロック

2010年1月に、RIPE NCCが1/8のうち一部のアドレスブロックを経路広告したところ、10Mbpsのトラフィックが流れたことや、また、Merit Network社が1/8のアドレスブロックを経路広告したところ、1週間で7.9TBのパケットが捕捉でき、瞬間的には860Mbpsのトラフィックを観

測したことなどが紹介されました。

14/8や223/8のアドレスブロックと比較して、1/8では数倍のトラフィックが流れていること、1.1.1.0/24のアドレスを持つパケットが全体の44.5%を占めることも紹介されました。また、宛先ポート番号も調査され、TCP445番ポート宛のパケットが多数を占めていることから、ウイルスやワームによるトラフィックも無視できないほど存在することが述べられました。

◆Route Filtering: Handle with Care

APNICのFrank Salanitri氏、NTTコミュニケーションズ株式会社の吉田友哉氏の両氏から、経路情報のフィルタリングについて紹介がありました。

初めに、Salanitri氏から、古くなったブラックリスト、Bogon※1リストによる通信障害が発生しているため、フィルタに使用する各種のリストは、最新の状態に保つことが重要であることが紹介されました。また、APNICでも、広報活動やトレーニングを行って啓発に努めていることが紹介されました。

続いて、吉田氏から、debogon projectについて紹介がありました。新しい/8のアドレスブロックからその一部を顧客に割り当てたところ、Webサイトを見ることができないという苦情があり、その原因を調べてみると、古いBogonリストがWebサイトに到達するまでの途中経路で使われていた、というエピソードが紹介されました。

また、27/8、14/8、223/8のネットワーク到達性の調査について報告があり、割り振られた直後では、20～30%のネットワークに対して到達性が無いことが報告されました。

◆A second look at measuring IPv6

APNICのGeorge Michaelson氏から、IPv6に関する調査結果が紹介されました。

まず初めに、IPv6の普及状況として、www.apnic.netへのIPv6によるアクセスがどれくらいあるのかが述べられました。2008年の中頃までは、割合として1%にも満たない程度だったのが、それ以降は1～2%程度になったことが紹介されました。

また、IPv4およびIPv6プロトコルスタックが、クライアントにどのように実装されているかについての調査発表がありました。プロトコルスタックの実装としては、

・IPv4のみ
・IPv6のみ
・IPv4/IPv6デュアルスタック（IPv6優先）
・IPv4/IPv6デュアルスタック（IPv4優先）

と分類されますが、これらがどの程度使用されているか調査されたそうです。方法としては、APNICのWebサイトに、IPv4/IPv6アドレスそれぞれでアクセスできる画像ファイルを置き、どのくらいアクセスがあったのかを調べたとのことです。その結果、デュアルスタックのクライアントはIPv4優先のクライアントが多く、IPv6のみのクライアントは1%以下だったことが分かったそうです。

■ 会議の様子

◇　　◇　　◇

今回のAPNICミーティングでは、アドレス割り振り時のネットワーク到達性について、また、IPv6の実装や普及状況についてのプレゼンテーションが多かったように思います。これには、IPv4アドレス在庫枯渇も目前に迫ってきており、それに対する備えを喚起する意味があったようにも感じられました。

（JPNIC 技術部 小山祐司）

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

□Program / Agenda - APNIC 30
http://meetings.apnic.net/30/program/

※1 Bogon
インターネットの経路制御において、広告可能アドレスとして登録されていないアドレスブロックやAS番号を指します。

■ リソースPKI関連報告

本稿では、APNICにおけるリソースPKI（以下、RPKI）の動向や、RIRにおけるデータベースの動向について報告します。

前回のAPNIC29ミーティングで行われたRPKI BoFに続き、今回はRPKIセミナーと呼ばれるセッションが行われました。RPKIに関する話題は、3日目（2010年8月26日）に行われたライトニングトークやRIRの活動報告、APNICのメンバーミーティングでも挙がりました。

◆RPKIセミナーで行われたプレゼンテーションの内容

RPKIセミナーでは、RPKIツールの開発状況やRIRの取り組み状況が報告され、ディスカッションが行われました。セミナーという名前ではありますが、チュートリアルではなく活動紹介を集めたようなセッションでした。おのおのが興味深いプレゼンテーションでしたので、内容を紹介します。

(1) BBN's RPKI Relying Party Software

RPKIの証明書検証プログラムの設計と開発を行っているBBNテクノロジーズ社のStephen Kent氏によるツールの紹介です。IETF SIDR（Secure Inter-Domain Routing）WGで新たに提案されたRPKI/Router Protocol※1を実装しています。このプロトコルは、RPKIサーバと呼ばれるリソース証明書を処理するサーバとルータの間で使われるプロトコルで、キャッシュと呼ばれる、リソース証明書の検証結果を含んだデータをBGPルータに送ることができます。今後ソースコードが公開される予定です。

(2) RPKI Tools from Soup to Nuts

ISC（Internet Systems Consortium）で、RPKIのツール開発を行っているRob Austein氏による開発状況の報告です。ISCのRPKIツールは、IPアドレスのリストからリソース証明書を発行したり、リソース証明書が格納された複数のリポジトリの間で、リソース証明書の交換を行ったりする機能を持っています。

2009年11月に広島で開催された第76回IETFの時には、既に一連の動作をするまでに開発されていましたが、その後、RPKIサーバとルータの間の通信や、リソース証明書の検証結果をBGPルータで使うための設定、IRRのようなWHOISサービスなどが実装されました。このプログラムは、以下のURLから入手可能です。

Resource PKI Software: http://www.rpki.net/

(3) RIPE NCC Certification Software

RIPE NCCのレジストリシステムであるLIR Portalの、リソース証明書関連のユーザーインタフェースの紹介です。LIR Portalは、JPNICのWeb申請システムにあたります。Webインタフェースでリソース証明書やROA（Route Origin Authorizations）の生成や管理を行うことができます。2年程前にご紹介したことのある※2certtestというプロトタイプシステムと基本的な機能は変わっていませんが、当時RIPE NCCのメンバーでなくても試すことができたものが、今は実際の割り振り/割り当ての通りに提供されるようになり、RIPE NCCのメンバーのみが利用できるようになっています。

またRIPE NCCでは、RIPE NCC Validatorと呼ばれるリソース証明書の検証ツールがJavaを使って開発されました。このプログラムも、RPKI/Routerプロトコルを実装しています。

http://labs.ripe.net/Members/agowland/ripe-ncc-validator-for-resource-certification

(4) Using RPKI tools in MyAPNIC

APNICのMyAPNICにおける、RPKIの実装に関する紹介です。新たに、ROAをグループ単位で管理できるインタフェースが加わりました。これにより、数多く発行されることが予測されるROAを、一度にグループ全体で更新することなどができるようになりました。また、リソース証明書の検証を行うための公開用Webページの準備が進められているようです。

質疑応答の時間には、RIRで提供されているRPKIのツールにおける、秘密鍵の管理方法について議論されました。LIR PortalとMyAPNICは、ユーザーの秘密鍵がWebサーバ側で保管されています。Webサーバ側で保管されていることについて、ARINのチェアであるJohn Karren氏は、多くのユーザーの秘密鍵が同時に漏洩してしまう構造である点を指摘しました。これに対して、現在はWebサーバ側

であるが、将来はユーザー側で管理することが考えられるという意見が挙がったり、それには鍵の生成と安全な切り替えを行う必要があるといったりした議論が行われました。

■ 会場となったSurfers Paradise Marriott Resort & Spa

◆ライトニングトークにおけるRPKIの話題

APNICミーティングの3日目に行われたライトニングトークでは、RPKIを導入することの経路ハイジャックに対する効果について、RIPE NCCのMark Dranse氏が紹介していました。2008年2月に起こったYouTubeの経路ハイジャック事件のように、Origin ASが本来とは異なり、かつASパス長が短くなるような経路情報が流されるタイプの経路ハイジャックに対して、RPKIがどの程度有効なのかをRIS[※3]のデータを使って試算しています。

経路ハイジャックが成功しうる経路情報の組み合わせは、今回対象とした80程度のASにおける経路数の34.2%あります。しかしRPKIを導入すると、これを13.6%に下げることができるとのことです。当然のことながら、この数値はASによって違いがあり、7%～22%と幅があります。またこれは、Origin ASの確認が100%行われ、必ずASパス長が最も短い経路が優先される、といったシンプルかつ有利に働く条件で試算されています。

◆RIRにおけるRPKIの取り組み

APNICメンバーミーティング（AMM）での報告によると、APNICではAfriNICでのRPKIの導入に協力し、現在のテスト段階からAfriNICメンバーへの提供ができる段階まで引き上げていく活動を行っているようです。

APNICとRIPE NCCでは既にメンバーにリソース証明書を提供しており、ARINでも試験的に、メンバーのうち希望者に対しては提供されています。今後AfriNICで提供されると、四つの地域でリソース証明書が使えることになります。

しかし、NIRからアドレスの割り振りを受けている事業者は、リソース証明書を技術的に試すこともできません。今後、アジア太平洋地域でどのように取り組んでいくべきなのかを考える段階に入っていくと考えられます。

◇　　◇　　◇

AMMの活動報告に関するプレゼンテーションの中で、DNSSEC対応が完了し、MyAPNICでDSレコードが登録できるようになったことが報告されました。ある技術がどの程度役に立つのかを議論し、綿密に検証していくことは大事なことではありますが、RIPELabsやAPNICのDNSSECに対する取り組みのように、短期間で実装し、試験利用を通じて効果や利便性を考えていくというアプローチには興味深いものがあります。

（JPNIC 技術部／インターネット推進部 木村泰司）

※1 “The RPKI/Router Protocol”, Randy Bush, Rob Austin
http://tools.ietf.org/id/draft-ietf-sidr-rpki-rtr-02.txt

※2 JPNIC News & Views vol.592「第57回RIPEミーティング報告」
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2008/vol592.html

※3 Information Services（RIPE NCC）
http://is-portal.ripe.net/

■ “10minutes talks”の様子

2010.11.7▶11.12

第79回IETF報告

■ 全体会議報告

◆概要

第79回IETFミーティングは、中国の北京で行われました。会場となったホテルは、北京の中心部から少し外れていますが、付近に大型の商店やカフェがあり、参加者にとって快適な会場であったようです。

第79回IETFミーティングの開催概要:
開催期間：2010年11月7日(日)～12日(金)
会場：Shangri-La Hotel Beijing
参加者数：1,177名
参加国数：52ヶ国
ホスト：清華大学(Tsinghua University)

IETFチェアの発表によると、国別の内訳は、第1位が中国（33%）、第2位が米国（29%）、第3位が日本（8%）、第4位がフランス（4%）でした。

初日の11月7日(日)に、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、IETFの全体会議である二つのプレナリ、各ワーキンググループ(WG)のミーティング、BoFが開かれました。本号では、二つのプレナリの模様を中心に報告します。

◆Operations and Administration Plenary

本プレナリはIETFの運営等に関する全体会議で、11月10日（水）16:30から行われました。初めに清華大学のホストプレゼンテーションがあり、次にISOCのItojun Service Award受賞者の発表、IETFチェアの活動報告が行われました。

今回のホストは中国の国立大学である清華大学です。中国の大学間ネットワークであるCERNET（China Education and Research Network）は、清華大学が中心となり構築と運用が行われています。1988年当初は、X.25をバックボーンに使った小規模なものでしたが、CERNETはいまや中国の主要な大学間を10Gbpsのリンクで結ぶまでに発展しています。後述するIADの活動報告で、Bob Hinden氏が、1991年にビデオ会議システムのCUSeeMeで“Hello from Beijing”という文字列を見てから、ちょうど20年経ったと述べています。ネットワークの相互接続のみならずIETFのホストを

行うまでに発展したことは意義深いと思われます。

2回目となるItojun Service Awardは、FreeBSDにおけるIPv6の実装に貢献したBjoern A. Zeeb氏に贈られました。Itojun Service Awardは、萩野純一郎氏にちなんで2009年に設立された賞で、IPv6の開発や運用などについて技術的貢献を行った人に贈られます。受賞者のZeeb氏は、FreeBSDにおけるIPv6、IPsec、IPv6のFirewallやSeND（Secure Neighbor Discovery）などの実装において貢献しました。

IETFチェアのRuss Housley氏からは、第78回IETFミーティング以降の全体の活動状況が報告されました。現在WGは124あり、108のRFCが作成されました。IETFチェアの報告内容は以下のWebページで公開されています。

□Plenary report（IASA）
http://iaoc.ietf.org/plenary_reports.html

オープンマイクロホンでは、IETFの資料を載せるWebページに資料があまりアップロードされていない状況を改善してほしいという要望が挙げられたり、IETFチェアのHousley氏が検討しているBoF枠の割り当ての考え方について、参加人数を考慮してほしいといった要望が挙げられたりしていました。

◆IAB Technical Plenary

こちらのプレナリは技術的な議論を行う全体会議で、11月8日（月）に行われました。IRTF（Internet Research Task Force）の活動報告とIABの活動報告が行われた後に“IPv6 Operations Transitional Issues”と題してパネルディスカッションが行われました。

IRTFチェアのAaron Falk氏によると、IRTFでは“Machine Learning & Communication Systems”と“Internet of Things”という二つの新しいリサーチトピックを扱おうとしているそうです。特に前者は、irtf-discuss@irtf.org メーリングリスト（ML）で議論が行われることになっています。なお、Falk氏は2011年3月に引退し、次のIETFで次期IRTFチェアが決まることになっています。

■ IAB Technical Plenaryでパネルとして登壇する株式会社インターネットイニシアティブ（IIJ）の松崎吉伸氏

IABでは、これまでにプレナリで議論されてきた話題をドキュメント化する作業を進める一方で、ワークショップを開催しています。

□IESG/IAB workshop “Architectural Oversight Forwarding Plane OAM”（2010年10月12日～14日開催）
http://trac.tools.ietf.org/area/ops/trac/wiki/oamJDS

□How can Technology help to Improve Privacy on the Internet（2010年12月8日～9日開催）
http://www.iab.org/about/workshops/privacy/

最後に、第2部としてRFC Series Editorモデルについて議論が行われました。2年前の組織構造の見直しで、RFC5620: RFC Editor Model（Version 1）が作成されましたが、このモデルに合うRFC Series Editorを雇うことに失敗、再度モデルの見直しを行うことになっています。そのためのVersion 2のたたき台についての議論です。しかし、会場からはVersion 2の案がこれまでの議論を反映しておらず、意味がないという指摘が挙がりました。結局、コメントを再度集めてディスカッションをし直すことになりました。

◆IETFミーティングに合わせて行われたイベント

- IEPGミーティング
IEPG（Internet Engineering and Planning Group）は、IETF参加者に加えてRIRやISPにおける技術者などが集まり、ルーティングやDNSなど、インターネットの運用や研究に関連した話題が議論される会議です。参加は無料で、毎回IETFの直前の日曜日（今回は初日の11月7日）に行われます。今回は、IPv4とIPv6のトランスレーターの性能比較や、DNSとDNSSECの性能比較に関する発表が行われました。

□IEPG
http://www.iepg.org/

- ISOCパネル
第76回IETFミーティング以降、ランチの時間に行われているISOC主催のパネルディスカッション“ISOC Panel”は、3日目の11月9日に行われました。今回のテーマは“Mobility”、ワイヤレスのモバイル機器に広がってきたインターネットについてディスカッションが行われました。モデレーターであるLeslie Daigle氏の資料や会場の録音データは、以下のページで入手できます。

□Internet Society Mobility Panel @ IETF 79
http://www.isoc.org/isoc/conferences/mobility/

- CNNICツアー
CNNICは中国のNIR（National Internet Registry）で、IPアドレスやAS番号の他にドメイン名のレジストリでもあります。IETF期間中の11月7日と9日にCNNICの見学ツアーが行われました。CNNICではDNSSECの実験の他に、DNSトラフィックデータに基づいてDNSルートサーバ等に関する研究が行われており、技術的にこだわりのあるIETF参加者からも注目されて、好評を得ていました。

■ 中国開催ということでCNNICの見学ツアーが行われました

□CNNIC
http://www.cnnic.net.cn/en/index/index.htm

第80回IETFミーティングは、2011年3月27日～4月1日、チェコのプラハで行われる予定です。

■ IPv6関連WG報告

本稿では、会期中における、IPv6に特化した内容を議論するワーキンググループ（WG）での議論内容を中心に紹介します。

◆6man WG（IPv6 Maintenance WG）

6man 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、11月9日（火）の午後最初に1コマにて開催されました。

セッション開始後、チェアより6man WGで取り組み中である、以下の文書についてステータス報告がありました。

・IPv6推奨アドレス表記（RFC5952として発行済み）
・DNS RAオプション（IESG承認、RFCエディタ発行準備中）
※2010年11月末に、RFC 6106（Standard Track）として発行

・ルータ要請メッセージでの回線識別（draft-krishnan-6man-rs-mark-08）：WGドラフトとして登録

最後の回線識別ドラフトに関しては、「技術的問題が多く、WGドラフトとする合意に達していないのでは」という指摘がありましたが、「まずはWGドラフトにしてから技術的課題を検討するのであって、RFCとして発行することとは別」というフォローがありました（WGドラフト化は、IETF79前に、WGドラフトとするかどうかの合意確認がMLで実施された結果です）。

今回、以下のテーマが議論されています。時間の割には議題が非常に多いという印象でした。

・IPv6拡張ヘッダの統一フォーマット
draft-ietf-6man-exthdr

・UDPゼロチェックサムの検討
draft-ietf-6man-udpzero、draft-eubanks-chimento-6man

・RFC3848 IPv6デフォルトアドレス選択の更新
draft-ietf-6man-RFC3484-revise

・P2Pリンク上におけるIPv6プリフィクス長 /127の利用
draft-ietf-6man-prefixlen-p2p

・重複アドレス選択プロキシ
draft-costa-6man-dad-proxy

・アドレス登録に関する要求条件
draft-jiang-6man-addr-registration-req

・IPv6フローラベル仕様の更新
draft-carpenter-6man-flow-update、draft-carpenter-flow-ecmp

・IPv6フローラベルに関するセキュリティ評価
draft-gont-6man-flowlabel-security

・Teredo ループ攻撃の緩和
draft-gont-6man-teredo-loops
（・エンドポイント識別子（EID）オプションの廃止 draft-gont-6man-obsolete-eid-option）→ 時間切れで議論できず。

これらのアジェンダの中から、いくつかのトピックについてご紹介します。

・IPv6拡張ヘッダの統一フォーマット
draft-ietf-6man-exthdr

IPv6拡張ヘッダの標準フォーマットを決めよう、という提案です。現在定義されている拡張ヘッダでは、フォーマットに統一性はありません。今後新たに拡張ヘッダを追加定義する際、新しい拡張ヘッダを認識できない古い機器がそのヘッダ部分をスキップすることができるよう、ヘッダの長さ情報等のフィールドを規定するなど、フォーマットに統一性を持たせることを提議しています。会場から、中間ノードが知らない拡張ヘッダに遭遇した場合に取るアクション（そのまま通過させる/パケットを落とす）を定めるビットを設けるべき、という意見があり、このビット追加を反映後、WGラストコールを実施することとなりました。

・UDPゼロチェックサムの検討
draft-ietf-6man-udpzero、draft-eubanks-chimento-6man

IPv6では必須となっているUDPでのチェックサムについて、IPv4と同様に、計算の省略を可能にしようという、ここ数回議論が続いている提案です。計算しない場合に関する考察である文書（draft-

ietf-6man-udpzero）は、WGラストコールを実施することになり、実際の適用手法に関する提案（draft-eubanks-chimento-6man）が議論となりました。適用を特定の場合のみに限定することについてはおおむね賛同を得ましたが、IPv6の基本文書であるRFC2460の改変が必要という意見も挙がっています。後者の文書についても、WGドラフトとして引き続き検討をすることに反対はありませんでした。

・RFC3484 IPv6デフォルトアドレス選択の更新
draft-ietf-6man-RFC3484-revise

IPv6ノードおよび通信相手が複数のアドレスを持つ場合に、通信に使うアドレスペアを選択する必要があります。この選択方法については、RFC3484に記載されていますが、デフォルトのルールに最新のアドレス情報（ULA; Unique Local IPv6 Unicast Addresses（RFC4193）等）が記載されていない問題等があるため、RFC3484を改版しようという提案です。本提案には、アドレスペアを選択する際の優先度に関して、ULA空間の優先度を引き下げるという提案が含まれていましたが、これに対して「自分が使っているULA空間は優先すべき」等の意見があり、検討を継続することになりました。関連して、デフォルトルールをDHCPv6で配布し、変更できるようにするという提案（draft-fujisaki-6man-addr-select-opt）について、WGドラフトとして扱うことに対するコンセンサス確認が実施され、WGドラフトとして議論することになりました。

・P2Pリンク上におけるIPv6プリフィクス長 /127の利用
draft-ietf-6man-prefixlen-p2p

前回WGドラフトとなった、ルータ間のリンクに付与するアドレスとして、127ビットのプリフィクスを用いることを可能としよう、という提案についての議論です。この文書中に挙げられている問題の一部は、より広い範囲でも検討する必要があるのでは、といった意見が出されました。ミーティング後に、WGラストコールを実施し、より広い意見を集めることになりました（2010年12月6日までの期限でラストコールが実施されていました）。

今回の議論で、上記以外に、

・重複アドレス選択プロキシ
draft-costa-6man-dad-proxy

・IPv6フローラベル仕様の更新
draft-carpenter-6man-flow-update、
draft-carpenter-flow-ecmp

がWGドラフトとして採用の方向、

・Teredoループ攻撃の緩和
draft-gont-6man-teredo-loops

が適切なWGにて議論を継続、となっています。

□6man WG
https://datatracker.ietf.org/wg/6man/

□第79回 IETF 6man WGのアジェンダ
http://www.ietf.org/proceedings/79/agenda/6man.html

◆v6ops WG（IPv6 Operations WG）

v6opsは、IPv6に関するオペレーション技術および共存・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（水）と12日（金）の2コマにて議論が実施されました。

IPv6の導入加速の世相を反映してか、今回も数多くの新提案がありました。チェアの方でも、議論時間を極力短縮するため、おのおのの発表では合意の確認を実施せず、インターネット上に用意したサイトにて、賛同、不賛同を後ほど入力するような形式を取ることにする、という周知が事前にありました。

ここでも、いくつかのトピックについて、簡単に紹介します。

・Happy Eyeballs: デュアルスタックホストにおいて通信を成功させるために
draft-wing-v6ops-happy-eyeballs-ipv6

・複雑な環境でのTCPセッションの開始
draft-baker-v6ops-session-start-time

IPv6/IPv4デュアルスタック環境では、通信相手がIPv4/IPv6両方のアドレスを持っている場合、ノードは、最初に選んだ通信プロトコルでの通信に支障が発生した場合に、もう一方の通信プロトコルに切り替えるという、いわゆるフォールバック、と呼ばれる動作をすることが一般的です。昨今の多くのデュアルスタック実装では、IPv6がIPv4よりも優先されるため、IPv6通信に支障があった場合にIPv4で再度試す、という動作をしますが、この切り替えに時間がかかり、ユーザーの利便性が損なわれる、という問題が発生しています。このようにデュアルスタック環境で発生する問題を、ユーザーの観点からいかに解決するかについて提案があり、議論が行われました。複数のTCPセッションを同時にスタートし、最初に通信できたセッションを利用する、といった解が提案されています。SCTPでの実装例や、アプリケーションとの関連に関するコメントが出されました。提案名が漠然とし過ぎていてすぐに提案内容を想像できないため、もっとわかりやすいものに変更すべき、という意見もありました。

ミーティング後に公表された投票の結果、それぞれ78.8%、63.2%がWGドラフトとして扱うべき、ということになり、特にHappy Eyeballsについては、出版ステータスの確認（InformationalかBCP（Best Current Practice）か）が、ML上で実施されています。

・IPv6カスタマーエッジルータの高度要求仕様
draft-wbeebee-v6ops-ipv6-cpe-router-bis

・IPv6普及におけるCPEに関する考察
draft-herbst-v6ops-cpeenhancements

間もなくRFCとなる予定の、IPv6カスタマーエッジルータ基本仕様文書（draft-ietf-v6ops-ipv6-cpe-router）に対する、追加仕様の提案です。従来、基本仕様と同時に議論されていたものを、分離して別文書として検討しています。また今回は同時に、スマートメーター等で利用される省電力無線デバイス（IEEE802.15.4（Zigbee）等を利用したデバイス）と家庭用ルータの接続に関する提案も実施されています。CPE追加仕様については、6rd、DS-liteといった移行プロトコルの記述追加、家庭でのCPEのトポロジーに関する考察（多段ルータ環境を考慮するか）、ULAの利用方法などについて言及され、後者ではIEEE802.15.4の接続方法、ULAでの通信の必要性等が例として挙げられました。議論としては、マルチキャストDNSの利用の是非、まずはトポロジーは単一ルータ環境に限定すべきである、といった点が挙げられています。今後、継続して議論していくこととなりました。

投票の結果では、前者は65.2%、後者は36.8%が、WGドラフトとして議論をすべきという意見でした。

・IPv6 AAAA DNSホワイトリスティングの影響
draft-livingood-dns-whitelisting-implications

キャッシュサーバからのクエリパケットのアドレスに基づき、DNS権威サーバにて、AAAAレコードを応答するかどうかを制御する、DNSホワイトリスティングに関する提案です。上記Happy Eyeballsのドラフトにも関連しますが、この仕組みにより、クライアント（正確には、クライアントの利用するキャッシュサーバ）のIPv6アドレスごとに、自サイトにIPv6を利用してアクセスするかどうかを制御できます。Googleでは実際にこの仕組みを使い、IPv6の接続性が良い相手からのみ、IPv6接続を利用可能とするような制御を実施しています。DNSの名前空間を分断することになり問題だ、DNS関連WGでも情報共有し議論をしてほしい、という意見が出されました。

投票の結果では、67.9%が、WGドラフトとして議論をすべきという意見でした。

アジェンダにはありませんでしたが、ミーティングの最後に、opsareaミーティングで話題に上がった、IPv4プライベートアドレス（RFC1918）の拡張に関する議論がありました（draft-weil-shared-transition-space-request）。こちらは、ISP共有アドレス空間として、2段NATの中間に使うための空間として利用したい、というものです。この用途として、IPv4の/10程度をリザーブしたい、という提案でしたが、賛成・反対共に多数の非常に激しい議論となりました。結果として、IETFではコンセンサスに至りませんでしたが、IPv4アドレス空間のIANA在庫が枯渇直前となり、このような空間を用意することは既に困難な状況になっていると思われます。

その他、前回のレポートでご紹介した、

・NATを用いないIPv6マルチホーミング方式
draft-troan-multihoming-without-nat66

について、ステータスレポートが実施されました。こちらについては、76%がWGドラフトとして議論をすべきという結果になっています。

□v6ops WG
http://datatracker.ietf.org/wg/v6ops/charter/

□第79回 IETF v6ops WGのアジェンダ
http://www.ietf.org/proceedings/79/agenda/v6ops.html

◆softwire WG（Softwires WG）

softwire WGは、トンネルを用いたIPv4 over IPv6、またはIPv6 over IPv4通信の実現方式を検討するWGです。昨今、さまざまなISPで導入が検討されている、DS-lite（Dual Stack Lite）や6rd（IPv6 Rapid Deployment）といった、新しいIPv4とIPv6の共存環境を構築する方式も併せて検討されています。今回は、開始早々の月曜朝一のコマにも関わらず、100名を超える参加者を集めて開催されました。

10件以上の新規提案があるなど議論アイテムも非常に多く、新規

アイテムの提案については、「技術の説明で1スライド、問題点や必要性等で1スライド程度で説明することを話者に連絡済み」「なるべく時間を短く」とチェアより念押しがありました。このためか、ほとんどの新規アイテムで議論も質問もありませんでした。

この後、チェアからDS-liteのステータスに関する説明がありました。DS-liteは、本体プロトコルと、必要なパラメータをDHCPで配布するDHCPオプション定義の二つの文書に分けられ、それぞれ個別に標準化が進められています。本体となるDS-lite（draft-ietf-softwire-dual-stack-lite）ですが、AD（Area Director）のレビューは終了し、そのコメント対応中となっています。DHCPオプションのドラフト（draft-ietf-softwire-ds-lite-tunnel-option）では、IESGレビューでコメントが付き、トンネル終点の指定に、FQDN（Fully Qualified Domain Name; 完全に限定されたドメイン名）とIPアドレスの両方ではなく、どちらか片方のみ指定することが議論され、その結果、最終的にはFQDNのみを指定するよう変更することになりました。こちらはドラフト修正後、WGラストコール、IESGにレビューを再依頼の予定となっています。

その他、以下のようなポイントが議論されています。

・今回のIETFよりWG化されたPCP（Port Control Protocol）WGより、PCPのプロトコルトランスポートとしてIPv6とIPv4のどちらを利用すべきか、という問いかけがありました。特にDS-liteでの利用の場合を想定しているとのことです。チェアからの双方ともに得失があるとの説明通り、その後の議論でも意見が分かれました。

・draft-ietf-softwire-dslite-radius-ext
draft-guo-softwire-6rd-radius-attrib

softwireのチャーター内のアイテムとして6rdやDS-liteのradius属性定義の提案がありました。それぞれ、WGドラフトとして議論していくことになっています。ISPでこれらのプロトコルを使用するには必須な部分であり、実導入に向けて検討が進んでいることがうかがえます。

□softwire WG
http://datatracker.ietf.org/wg/softwire/charter/

□第79回 IETF softwire WGのアジェンダ
http://www.ietf.org/proceedings/79/agenda/softwire.txt

IETFミーティングのすべての資料、Jabberログ、オーディオ録音等は、次のページより参照可能です。
http://tools.ietf.org/agenda/79/

（NTT情報流通プラットフォーム研究所 藤崎智宏）

■ DNS関連WG報告

本稿では、DNSに関連した内容を議論するワーキンググループ（WG）で議論された概要をご紹介します。

◆dnsext WG（DNS Extensions WG）

dnsext WGでは、会合のまず初めに、dnsext WGのメーリングリスト（ML）が、今までのnamedroppers@ops.ietf.orgからdnsext@ietf.orgへと変更になるとアナウンスがありました。現在登録されている人はそのまま新しいMLに引き継がれます。

今回の会合での主な議題は、draft-yao-dnsext-identical-resolutionとdraft-vixie-dnsext-resimproveでした。どちらもWG draftではありませんが、前者はIETF77から話題になっている、Zone Aliasing※に関するドラフトです。後者は、上位ゾーンと下位ゾーンのNSセットが同期していない場合の、リゾルバサーバの挙動に関する改善を提案しています。

前者のdraft-yao-dnsext-identical-resolutionは、Zone Aliasingに関しての目的と提案されている方式、問題点をまとめたドラフトです。Zone Aliasingの方式として、BNAMEとCNAME+DNAMEという二つの提案が出ていましたが、IETF78の後、特に進展はありませんでした。そのため、期限を区切って本ドラフトを更新することが提案され、Suzanne Woolf氏を中心として作業が行われることとなりました。

後者のdraft-vixie-dnsext-resimproveに関しては、NS RRのTTLに応じて、ゾーンの委譲を再検証し、検証においてNXDOMAINが返ってきた場合には、そのゾーンに関してそれ以降の検索を止める、という提案です。リゾルバDNSサーバの挙動を変えるものであるため、いくつか否定的な意見が出ました。発表の後、WG draftにするかの挙手による意思確認が行われましたが、ほとんど手は上がらず、議論はMLに引き継がれました。

その他には、DNSのリソースレコードとしてURI RRを追加する提案である、draft-faltstrom-uriや、AAAAレコードとAレコードを同時に問い合わせる手法を提案した、draft-kitamura-ipv6-simple-dns-queryに関する発表がありました。最後に、DNSSEC History Projectに関する発表がありました。この発表はdnsop WGでも行われたため、以下のdnsop WG報告にて説明します。

◆dnsop WG（Domain Name System Operations WG）

dnsop WGの会合では、まずWG draftの確認がありました。draft-ietf-dnsop-name-server-management-reqsがIETF Last Callを通過したため、Informational RFCとして発行される予定であることが報告されました。また、draft-ietf-dnsop-default-local-zones、draft-ietf-dnsop-as112-ops、draft-ietf-dnsop-as112-under-attack-help-helpの三つのdraftは、早めにAD（Area Director）レビューに回すことが確認されました。また、draft-ietf-dnsop-resolver-primingならびにdraft-ietf-dnsop-respsizeはExpireしているのですが、著者が更新に向けて作業をしているとの報告がありました。

次に、DNSSEC History Projectに関する発表がありました。これはDNSSECが実運用段階に入ったこと、ならびにDNSSEC提案から20周年であることを記念して、DNSSEC標準化と実運用までの記録を残すというプロジェクトです。https://wiki.tools.isoc.org/DNSSEC_History_Project に情報が集められています。

他には、draft-ietf-dnsop-dnssec-key-timingに関する報告がありました。現状では、Algorithm RolloverやCSK Rolloverといった項目に関して述べていないが、これらを盛り込んでからWG Last Callを行うべきか、これらの追加の項目に関しては別ドラフトとして発行すべきか、という議論がなされました。結論としては、別ドラフトとして執筆し、現状のドラフトはWG LastCallに向けて更新を行うことが確認されました。

WG draft以外では、draft-livingood-dns-whitelisting-implicationsに関する発表がありました。これは、DNSクエリの送信元IPアドレスによって、応答にAAAAを返すかどうかを決定するという仕組みです。これによって、IPv6接続性が無い組織のDNSサーバからDNS問い合わせが来た場合に、不要なAAAAを返さないことによって、IPv6接続タイムアウトの発生を回避することができるという提案です。これに関しては、いくつかの質問とコメントが出されましたが、dnsop WGとしては好ましくない手法であるとの意見が大勢を占めました。

最後に、Name Server Control Protocolに関する議論が行われました。これは、DNSサーバを制御するための共通のプロトコルを定めようという試みです。Nameserver Management Requirementsに関するドラフトがIETF Last Callを通過したため、次にそのプロトコルに関して定義しようというものです。具体的には、draft-kong-dns-conf-auto-sync、draft-dickinson-dnsop-nameserver-controlといったドラフトが提案されています。主にNETCONFの枠組みを利用して、DNSサーバの設定や制御を行うという提案です。会場での活発な議論が行われ、引き続きMLで議論を行うことが確認されました。

（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）

※ 参考:第78回IETF報告［第2弾］DNS関連WG報告
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2010/vol774.html

■ セキュリティ関連WG報告

IETFにはセキュリティ関連WGが14存在しており、今回は11WGによる13のセッションに加えて、BoFが二つ（KIDNS（Keys in the DNS）とSCAP（Security Content Automation Protocol））で、合計15のセッションが開催されました。

セキュリティ関連のWGに関するこれらのミーティングは、領域および範囲が広いため、すべてのミーティング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関連セッションの中から、認証やセキュア通信に特化した内容を議論する二つのWGの動向について報告します。

◆IPSECME WG（IP Security Maintenance and Extensions WG）

IPSEC WGの後継として、2005年に同WGがクローズした後、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。今回このミーティングは、2010年11月10日の午後1時から2時間程度開催されました。参加者は、40名程度でした。

IPSECME WGにおいて、前回のマーストリヒトでのIETFから今回までにRFCとして発行されたドキュメントや、RFCとして発行される直前のドキュメントを示します。

＜RFCとして発行されたドキュメント＞

・RFC5996 Internet Key Exchange Protocol Version 2（IKEv2）

IKEv2について記述するドキュメントです。このI-D（Internet-Draft）がRFC化されたことで、以前発行されたRFC4306（Internet Key Exchange（IKEv2） Protocol）とRFC4718（IKEv2 Clarifications and Implementation Guidelines）を廃止（Obsoletes）しました。なお、このRFCは、インターネット標準化過程（Standards Track）として発行されました。

URL:http://tools.ietf.org/html/rfc5996

・RFC5998 An Extension for EAP-Only Authentication in IKEv2

IKEv2において、拡張可能な応答者認証を提供するための相互認証（mutual authentication）や鍵合意（key agreement）を提供するEAP（Extensible Authentication Protocol）を仕様化するドキュメントです。なお、このRFCは、Standards Trackのドキュメントとして発行され、RFC5996を更新（Updates）しています。

URL:http://tools.ietf.org/html/rfc5998

・RFC6027 IPsec Cluster Problem Statement

クラスタ上でのIKEやIPsecを実装するための要求条件や問題の提示、および専門用語について定義しているドキュメントです。また、異なるクラスタ間の相互運用を可能にするピアを許可するための、仕様と実装のギャップも記述しています。なお、このRFCは、情報（Informational）に分類されるドキュメントとして発行されました。

URL:http://tools.ietf.org/html/rfc6027

＜RFCとして発行される直前のドキュメント＞

・IP Security（IPsec） and Internet Key Exchange（IKE） Document Roadmap（draft-ietf-ipsecme-roadmap-10）

IPsecやIKEに関係するRFCが多く発行され、それぞれの関係などが複雑化しており、そのドキュメントの背景や要約を記述することでそれらの関係を整理することを目的としたドキュメントです。なお、I-Dのステータスは、RFC Editorの 編集待ちリストに掲載されている状態（RFC Ed Queue）です。本I-Dは、Informationalのドキュメントとして発行される予定です。

このI-DがRFC化されると、以前発行されたRFC2411（IP Security Document Roadmap）は廃止されます。

また、今回議論された検討項目は、以下の通りです。

・A Quick Crash Detection Method for IKE
draft-ietf-ipsecme-failure-detection-02

・Protocol Support for High Availability of IKEv2/IPsec
draft-ietf-ipsecme-ipsecha-protocol-02

このミーティングでは、主に“A Quick Crash Detection Method for IKE”と“Protocol Support for High Availability of IKEv2/IPsec”に関する議論に時間を費やしました。

上記以外のトピックとして、以下の三つの話題が会議で取り上げられ議論されました。この中から二つに注目して、議論内容のポイントを報告します。

・IKEv2 Re-authentication

IKEv2bisとして議論され、RFC5996として発行された仕様において、Re-authenticationにいくつかの問題が存在しているという指摘がありました。それらの問題に対して、いくつかの解決策はあるが、現在思いつくような解決策ではなく、異なる方法による解決が必要であるという議論になりました。今後のIPSECMEでの議論に注目する必要があると考えます。

・IKEv2--（IKEv2 “minus minus”）

「デバイスによる高い制約を受ける状況などでIKEv2を実装する人などに向けて、最小構成のIKEv2を規定する必要はあるのではないか?」という議論が行われました。IKEv2という仕様は複雑であり比較的大きなものなので、IKEv2を利用するIPSECME WG以外の人に対して、最小構成仕様の必要性は高いと考えられます。この議論の結果としては、最小実装として満たさなければならない仕様は、RFC5996で規定されている仕様となりました。

・IKEv2 with CGA（CGA: Cryptographically Generated Addresses［RFC3972］）

なお、IPSECME WGの詳細情報および今回のアジェンダについては、次のURLをご参照ください。

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

□第79回IETF IPSECME WGのアジェンダ
http://www.ietf.org/proceedings/79/agenda/ipsecme.txt

■ 今回のIETFには中国国内から多くの技術者が参加しました

◆KRB WG（Kerberos WG）

KRB WGは、マサチューセッツ工科大学（MIT）が考案した、認証方式の一つであるKerberosプロトコルに関する新規仕様や機能拡張について、検討を行うWGです。このミーティングは、最終日である2010年11月12日の午後1時から2時間半程度開催されました。なお、参加者は、20名程度でした。

ミーティングの構成として、以下のような議題で進行されました。

・ドキュメントステータスおよび議論

・技術的な議論
- KerberosにおけるCamelliaに関する議論
- IANAに関する議論
- PAC（Privilege Attribute Certificate）に関する議論

・Mesh wireless network through Kerberosに関する提案
（draft-moustafa-krb-wg-mesh-nw）

このミーティングについて、ドキュメントステータス、技術的な議論および今回の3提案の中から、いくつかのトピックスに関して報告します。

＜ドキュメントステータスおよび議論＞

・Deprecate DES support for Kerberos
（draft-lha-des-die-die-die）

危殆（きたい）化した暗号アルゴリズムであるDESに関してKerberosでのサポート停止をアナウンスするためのDraftです。このドキュメントのステータスとしては、WG Last Callは完了しており、著者によるIESGへの対応待ちの状況です。この仕様は、暗号の危殆化（暗号の世代交代）の観点から重要なものであると考えられています。

・Kerberos Options for DHCPv6
（draft-sakane-dhc-dhcpv6-kdc-option）

Dynamic Host Configuration Protocol for IPv6（DHCPv6）において、Kerberosプロトコルに関係する設定情報を利用するために、四つのオプションを定義する仕様です。このドキュメントのステータスは、修正版の投稿待ちでしたが、ミーティング中に、著者から更新版が投稿されました。

＜技術的な議論＞

・KerberosにおけるCamelliaに関する議論

現在、KRB WGのスコープに暗号アルゴリズムの追加は含まれていないため、WGとして議論するトピックとしてコンセンサスを取るための議題でした。議論の概要としては、技術的な議論が主な目的だったため、Camellia-CCMを利用した際のKerberosに対する影響などについて活発な議論が行われました。

議論を行う際に、KRB WGのチェアから送られたメールを参照しました。そのメールの詳細については、以下のURLをご覧ください。

https://lists.anl.gov/pipermail/ietf-krb-wg/2010-November/008770.html

なお、KRB WGの詳細情報および今回のアジェンダについては、以下のURLをご参照ください。

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

□第79回IETF KRB WGのアジェンダ
http://www.ietf.org/proceedings/79/agenda/krb-wg.txt

（NTTソフトウェア株式会社 菅野哲）

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

■ICANN関連トピックス

ICANNが検討しているコミュニティベース新gTLD向けの紛争解決手続き

レジストリ制限事項に関する紛争解決手続き（Registry Restriction Dispute Resolution Procedure; RRDRP）について

◆本稿執筆の背景

RRDRP（レジストリ制限事項に関する紛争解決手続き）については、ICANN報告会などにおいても、今まで明示には取り上げてきませんでした。というのもこの仕組みが「コミュニティベースgTLD」を対象としたもので、影響の範囲も比較的限定的されていると考えられたためです。しかしながら、取り上げずにいれば、今後も本手続きに関する情報が十分提供されないままとなってしまうため、今回、テーマとして取り上げることとしました。

◆RRDRPとは

次のgTLD募集ラウンドで募集されることになる、いわゆる新gTLDの申請受け付け開始が、スケジュールは確定していないものの、近づいてきていると見られています。

RRDRPとは、新gTLDのうちコミュニティベースgTLDを対象としたサービス開始後の紛争解決メカニズムです。コミュニティベースgTLDとは、特定のコミュニティにおいて利用されることを前提とするgTLDのことで、既存のTLD では、.museum、.aero、.proなどのスポンサ※1付きgTLD（sTLD）※2が、これに類似したものと言えます。

RRDRPは、コミュニティベースgTLDにおけるドメイン名割り当てプロセスにおいて、「申請者の要件合致についての判断に関する事後紛争解決手段が必要」という考えに基づき導入されるものです。

コミュニティベースgTLDは、誰でも自由に登録できる通常のgTLDとは違い、レジストリ制限事項（Registry Restriction）と呼ばれる、レジストリによってドメイン名登録希望者に要求される、登録要件などの制限事項が存在します。コミュニティベースgTLDのレジストリがサービスを開始した後に、この制限事項が適切に遵守されていない場合に、RRDRPを利用して登録者などから異議申し立てを行うことが可能となります。

RRDRPは、新gTLD申請者ガイドブック案（本稿執筆時は第4版）がICANN理事会により正式に承認された段階で確定することになります。RRDRPでは他のDRPと同様、独立した外部の専門家に紛争処理の判断を任せることが想定されます。その理由は、ICANNが登録者レベルでのドメイン名の内容について判断することは、“技術的なことの委任”を受けるという、ICANNの使命を逸脱するためとされています。※3

◆RRDRPの想定例

RRDRPの想定利用例として、次のようなものが考えられます。

ペット（動物）愛好家団体が.petというgTLDを申請し、ドメイン名の登録要件にペット愛好家団体であることを定めてICANNの審査・評価を通過しサービスを開始した後、ペットボトル製造業界団体がbottle.petというドメイン名を申請して登録が認められた場合に、正しく要件を満たして申請・登録している、その他のペット（動物）愛好家団体が不服を申し立てるケース等です。

◆RRDRPにおける手続きの流れ

当該TLDレジストリへのTLD委任開始後、個人もしくは組織が申し立てを行います。ICANNは紛争の当事者になれないので、ICANN自身による申し立てはできません。申し立ての際には、WHOISの苦情申し立てフォームに類似したオンラインフォームが用意されるので、それを利用します。申し立てにあたって利用する言語は英語となり、RRDRP紛争処理機関（以下、紛争処理機関）とのやり取りはメールなどにより電子的に行います。申し立て時には、紛争処理機関が定める登録費用を申し立てから10日以内に、紛争処理機関に対して支払う必要があります。

申し立て後5営業日以内に、裁定を行う主体である紛争処理機関が指名するパネリストにより事前審査が行われた後、紛争処理機関からレジストリに対して申し立てがあったことと、申し立て内容について通知されます。

申し立て後30日以内に、レジストリは申し立てに対する答弁書を紛争処理機関に提出します。紛争処理機関は申し立て者に対し、答弁書を送付します。紛争処理機関が答弁書を受領してから10日以内に、レジストリは紛争処理機関に対し申請費用を支払います。

紛争処理機関は、1名の専門家パネルを、答弁書受領より21日以内に選定および指名します。申し立て者もしくはレジストリからの要望があったときは、3名パネルとなることもあります。その後、紛争処理機関は手続きに要する費用を見積もった上で、申し立て者およびレジストリの両方に費用の全額を請求します。これら費用については、紛争に勝った方が支払った分については後で返却されます。迅速に紛争処理を行うため、および費用を抑えるため、申し立て書および答弁書の内容に基づいた書類による審理のみで、通常は証拠開示や聴聞は行われません。

RRDRPを定めた文書において、裁定の期限については、裁定書が専門家パネルの指名から45日以内に提出されるよう努力すること、および正当な理由なしに60日を越えないようにすることとなっています。また、専門家パネルはレジストリに対して、当該gTLDでの新規ドメイン名登録の停止、レジストリ契約への改善措置の追加、レジストリ契約の終了などを勧告することができます。

◆まとめ

コミュニティベースgTLDは、gTLDの文字列がコミュニティのアイデンティティを示すことから、そのドメイン名をインターネット上で利用する登録者が、そのコミュニティを構成する者としての要件を満たしていることが担保されることは重要です。

既にサービスが開始されているsTLDでも、いくつか類似の紛争解決手続きが用意されていますが、今回新たなgTLD募集ラウンドの施行にあたり、統一した手続きがRRDRPとしてまとめられ実装されることは、コミュニティベースgTLDの価値を高める観点で、意義深いものだと考えられます。

［参考］導入検討の経緯

2009年2月18日に発行された（新gTLD）申請者ガイドブック案第2版（DAGv2）※4と、同日付公開のレジストリ契約書案※5では、RRDRPという名称こそ使われませんでしたが、初めて「コミュニティベースTLD運営者の義務」という条項が追加され、登録ポリシー遵守についての紛争解決手段の制定も、レジストリが守るべき義務の一つとなっています。続いて2009年5月30日には、ICANNがRRDRP導入の背景と詳細について記載された、単独の説明文書※6を公開しました。

2009年10月2日には、申請者ガイドブック案第3版（DAGv3）※7が発行され、その中の「Module 5: 委任への移行」という項目には、レジストリ契約書案※8およびRRDRP手続き文書案※9が付属しました。2010年2月15日にはICANNが手続き文書案を公開し、4月1日まで意見募集を行った後、コメントのまとめと分析※10が5月31日に公開されました。

ICANNナイロビ会議会期中の2010年3月12日には、ICANN理事会にて、RRDRP最終案を申請者ガイドブック案第4版（DAGv4）で公開するよう求めた決議※11がなされました。これを受け、2010年5月31日にはRRDRP最終案を含める形で、DAGv4※12が発行されました。DAGv4に含まれるRRDRP最終案※3は、2月15日から4月1日までの間に寄せられたコメントを受けて変更されていますが、変更はそれほど大規模なものではありません。

（JPNIC インターネット推進部 山崎信）

※1 スポンサ組織
トップレベルドメイン（TLD）の登録・運用ポリシーを策定する組織。

※2 JsTLD（sponsored Top-Level Domain; スポンサ付きトップレベルドメイン）
特定の業界・分野内に運用が制限されたTLDで、当該業界を代表する組織がスポンサ組織として登録ポリシー等を決定します。

※3 REGISTRY RESTRICTIONS DISPUTE RESOLUTION PROCEDURE（RRDRP）REVISED - MAY 2010
http://www.icann.org/en/topics/new-gtlds/rrdrp-clean-28may10-en.pdf

※4 New gTLD Draft Applicant Guidebook（DAGv2）
http://www.icann.org/en/topics/new-gtlds/draft-rfp-clean-18feb09-

※5 New gTLD Agreement Proposed Draft（v2）
http://www.icann.org/en/topics/new-gtlds/draft-agreement-clean-18feb09-en.pdf

※6 Proposed ICANN Registry Restrictions Dispute Resolution Procedure（RRDRP）
http://www.icann.org/en/topics/new-gtlds/rrdrp-30may09-en.pdf

※7 Draft Applicant Guidebook, version 3（DAGv3）
http://www.icann.org/en/topics/new-gtlds/draft-rfp-clean-04oct09-en.pdf

※8 New gTLD Agreement Proposed Draft（v.3）
http://www.icann.org/en/topics/new-gtlds/draft-agreement-specs-clean-04oct09-en.pdf

※9 REGISTRY RESTRICTIONS DISPUTE RESOLUTION PROCEDURE（RRDRP）
http://www.icann.org/en/topics/new-gtlds/draft-rrdrp-04oct09-en.pdf

※10 NEW gTLD DRAFT APPLICANT GUIDEBOOK VERSION 3 PUBLIC COMMENTS SUMMARY AND ANALYSIS
http://www.icann.org/en/topics/new-gtlds/summary-analysis-agv3-15feb10-en.pdf

※11 Adopted Board Resolutions ¦ Nairobi - 12 March 2010
http://www.icann.org/en/minutes/resolutions-12mar10-en.htm#8

※12 Draft Applicant Guidebook, version 4（DAGv4）
http://www.icann.org/en/topics/new-gtlds/draft-rfp-clean-28may10-en.pdf