

インターネット トピックス

第51回RIPEミーティング

2005年10月10日から14日まで、オランダ・アムステルダムにてRIPE51ミーティングが開催されました。当地は16日のアムステルダムマラソンを控え、街のあちこちに交通規制予告の張り紙が見られました。ミーティング期間中は最高気温が20℃前後で私には快適でしたが、マラソンには少し暑かったかもしれません。

以下に今回の会議の主要トピックを、アドレスポリシーを中心にご紹介いたします。

◆アドレスポリシー・ワーキンググループ(WG)

今回のアドレスポリシー WGでは、以下の提案が議論されました。

(1) IPv4アドレス (以下IPv4) 追加割り振り基準へのHD-ratio適用

IPv4の追加割り振り基準(現在は既割り振り空間の80%を使用していること)を変更する提案です



第51回RIPEミーティング総会の模様

が、賛成と反対に意見が分かれている状態で、引き続きメーリングリスト(ML)で議論するという結論になりました。

(2) ccTLD/gTLD DNSのエニーキャスト^{*1}用プロバイダ非依存アドレス

ccTLD及びgTLDのネームサーバのエニーキャスト用に、プロバイダ非依存のIPv4(/24)又はIPv6アドレス(以下IPv6)(/32)、もしくはその両方を割り当てることができるとする提案です。IPv6のプロバイダ非依存アドレスについてはIETFでも議論中であることなどから、MLで議論を継続することとなりました。

(3) IPv6初期割り振り要件の見直し

現行のIPv6初期割り振り要件の一つである「2年以内に最低でも200の/48の割り当てを行う計画がある」という要件を撤廃するという提案です。会場では、この要件を撤廃すると、LIRは全てIPv6の割り振りを受けられることになるがそれで本当に良いのかなどの意見が出され、本提案は一旦提案者に差し戻して、内容を再検討することとなりました。

(4) IPv6ポリシーにおけるエンドサイトの定義について

IPv6ポリシー中に出てくる「エンドサイト」の定義箇所を、よりわかりやすい説明に書き換えようという提案です。エンドサイトの定義上、ISPと「ビジネス上の関係にあること」という文言があるのですが、「大学と生徒は『ビジネス』上の関係にあると言えるの

か]などの意見が出て、引き続きMLで議論することとなりました。

(5) IPv6の割り当てと利用率要件の変更

現在、IPv6のエンドサイトへの割り当ては基本的には/48で、サブネットが一つと決まっている場合/64、接続機器が一つと決まっている場合/128とされています。本提案は、これらに追加して/56という割り当てサイズを定義したうえで、さらにHD-ratioの基準値を現在の0.8から0.94へ変更しようとするものです。割り当てサイズの変更、HD-ratioの変更共に節約方向での変更と言えます。

本提案とほぼ同様の提案は2005年9月のAPNICミーティングでも提出されています*2。APNICミーティングでは、割り当てサイズの変更については賛同が得られなかったものの、HD-ratioの変更についてはコンセンサスとなっています。RIPEミーティングに出された提案がAPNICへ提出されたものと違う点は、「割り当てサイズをどのプリフィクスにするかはLIRの判断に委ねる」とされた所です。APNICミーティングでの提案では、「サブネットが255超であれば/48、255以下であれば/56を割り当てる」とされていました。

今回のRIPEミーティングでは、割り当てサイズの変更とHD-ratioの変更は独立して議論すべきだとの意見が出た結果、これを別々の提案として分けたいと、それぞれを今後MLで継続して議論していく、

という結論になっています。

(6) IANAからRIRへのIPv6割り振りポリシー

本件は既にARIN、APNICでコンセンサスを得ている内容となります。RIPEでも今回特に反対意見が無かったため、ML上で最終コメント期間に入ることとなりました。ここでも特に反対なければ、コンセンサスとして扱われることとなります。

◆DNS WG

2005年9月のAPNICミーティングでもコンセンサスを得たip6.int廃止について議論されました。APNICミーティングでは廃止の時期を「2006年6月1日以降で調整」としていますが、RIPEでは「6bone*3の停止と同時期(2006年6月6日)くらい」として、コンセンサスとなっています。本提案は今後引き続き他地域でも議論され、廃止の日程が協議されることとなります。

◆その他の話題 - IPv4の寿命 -

APNICのGeoff Huston氏が「IPv4 Address Lifetime Expectancy Revisited」と題し、IPv4の寿

*1 エニーキャストアドレス(Anycast Address)
IPアドレスは、一般的に特定のインタフェースへ一意に割り当てますが(ユニキャストアドレス)、それに対して、エニーキャストアドレスは、複数のインタフェースに割り当てられたIPアドレスです。

*2 JPNIC News & Views vol.293
「IPv6アドレスポリシーの変更について
～第20回APNICオープンポリシーミーティングでの議論～」
<http://www.nic.ad.jp/ja/mailmagazine/backnumber/2005/vol293.html>

*3 6bone
<http://www.nic.ad.jp/ja/basics/terms/6bone.html>

命予測のアップデートを行いました※4。RIRの2005年の割り振り量等を考慮に入れ、従来の予測を更新したものです。これによると、IANAからRIRへの割り振りアドレスが底をつくのは2012年8月5日、RIRからLIRへの割り振りアドレスが底をつくのは2014年5月2日とされています。同氏が2003年に行った予測※5では、RIRからLIRへの割り振りアドレスが底をつくのが2022年としていましたから、それ

よりも予測枯渇時期が早まったことになります。

同氏はこれからIPv4の残りが少なくなってくるにつれ、駆け込み申請やアドレス売買の可能性など様々な問題が発生する可能性があり、RIRやコミュニティはこれらの問題にどう対処していくべきか考える必要があるのではないか、との問題提起を行いました。

ARIN XVI ミーティング

今回のARINミーティングは2005年10月25日(火)から10月28日(金)、ロサンゼルスユニバーサルシティで開催されました。

ユニバーサルスタジオから歩いて15分のヒルトンホテルが会場でしたが、場所がどこであってもTシャツにジーンズ姿の業界の方々がIPアドレス管理について議論を行うことに変わりはなく、華やかな雰囲気は漂っているということはありませんでした。



ポリシー SIGの様子

例年、秋のARINミーティングはNANOGとあわせての開催ということもあり、参加者約190名のうち、NANOG、ARIN両方の参加者は135名だそうです。管轄地域が主に北米のため、米国カラーが非常に強いことがARINミーティングの特徴です。どんな些細なことでもきちんと議論を行う土壌のせい、今回も話題は盛りだくさんでした。

特に注目すべきトピックスとして、IPv4アドレス(以下、IPv4)の寿命予測、IPv6アドレス(以下、IPv6)ポリシーの変更、IPv6におけるPIアドレス、そしてAS番号の4ビット化、についてご紹介したいと思います。

◆IPv4の寿命予測

ARINミーティングの議長でもあるJohn Curran氏がモデレーターを務め、Geoff Huston氏(APNIC)、Tony Hain氏(Cisco Systems)、Thomas Narten氏(所属の明記なし)とKC Claffy氏(CAIDA)がそれぞ

会場ではこの発表を受け、最大割り振りサイズを制限すべきではないかという意見や、今後WGを結成して、アドレス枯渇にかかる課題を検討していけばどうかという提案など、活発な発言がありました。枯渇に至るにはまだ時間があるとはいえ、今後も引き続きアドレスの消費状況、各RIRでの議論の動向等を注視する必要があるようです。IP

(JPNIC IP 事業部 穂坂俊之)

※4 ミーティング発表資料

<http://www.ripe.net/ripe/meetings/ripe-51/presentations/pdf/ripe51-ipv4-lifetime-rev.pdf>

※5 "IPv4 - How long have we got?" - The ISP Column

<http://www.potaroo.net/ispcolumn/2003-07-v4-address-lifetime/ale.html>

れの見解を発表し、パネルディスカッションを行いました。

IPv4の寿命予測について、Geoff Huston氏は8年、Tony Hain氏は5～7年としています。二人の予測に若干の差異が生じているのは、過去のどの時点の推移を参考に今後の伸びを予測しているかによって、消費カーブが異なることと、どの時点(IANAプールが尽きた時点か、RIRプールが尽きた時点)で「枯渇」と見なすのかということが理由です。

また、Geoff Huston氏は予測されている寿命の正確性そのものよりも、実際に枯渇した場合の対策に目を向けています。具体的にはIPv4が枯渇した時点でIPv6への完全移行が完了していない可能性が高く、「その間のアドレッシングをどうすべきか」ということについて問題提起が行われていました。

また、そのようなことが起こった場合、IPv4が市

場に出回ることも予測され、RIRをはじめとするレジストリの役割についてもコミュニティに対して問いかけてきました。

これはJPNICでも大きな取り組みが必要な問題と考え、2005年12月より番号資源利用状況調査研究専門家チームを設立して調査を進めています。今後調査結果を発表し、みなさまと一緒に検討を進めていきたいと考えています。

◆IPv6ポリシーの変更

以下二つに分けて提案が行われました。

- ・追加割り振り利用率の変更(HD-ratio 0.8→0.94)
- ・/48以外の新たな割り当てサイズの追加

1点目の追加割り振り利用率の変更についてはAPNICで行われた提案と同じ内容で、ここでも参加

者からのコンセンサスが得られました。

新たな割り当てサイズを設けることについては今回のミーティングで結論は出ず、今後コミュニティの意見を反映させたいと改めて具体的な提案を行うことになりました。

こちらについて当初はAPNIC、RIPE同様、既存の/48に加えて/56の割り当てサイズを追加することが提案されましたが、参加者から「割り当ては可変的に行うべき(つまりビット単位で割り当てサイズが決定できるべき)」とのコメントがあり、他の参加者からも支持するコメントがいくつかありました。

その後、議長から「既存の/48よりもより小さな割り当てサイズを検討するべきか」と「割り当てサイズを固定ではなく、可変とするべきか」の2点について確認が行われた際、どちらも賛成者数が反対者数を大きく上回ったため、この点も考慮したうえで、次回のARINミーティングで提案が行われることになるかと思えます。

◆IPv6におけるPIアドレス

過去数回のミーティングから継続議論として提案されており、特に現在IPv4でマルチホームを行っている組織については強いニーズが確かにあることは共通認識として確立されているようです。

ただし、具体的な基準を定めることで難航しており、今回の提案では「100,000ホスト以上を持つネットワーク」ということが基準に含まれていたため、「割り振り基準よりも厳しいじゃないか」と不評を買っていました。

経路情報集約のため、あまりにも誰でも取得できるようにするべきではないとの考えもあり、基準を緩和しすぎず、かつ必要な人に取得してもらえる、バランスのよい基準というのはなかなか難しいようです。引き続き、ARINのメーリングリストで活発に議論が行われています。

スレッド名: "2005-1 or its logical successor"
<http://lists.arin.net/pipermail/ppml/>

また、IPv6におけるPIアドレスは国内においても前回のJPNICオープンポリシーミーティング※1でニーズが確認され、今後のAPNICミーティングでの提案に向けて、IPv6 PIアドレスWGで検討を進められています。

◆AS番号の4バイト化

正式な提案としてではなく、今後ポリシー提案を検討している参加者が自分の案を紹介して参加者の感触をさぐるPolicy BoFにてGeoff Hustonより紹介されたものです。現時点では以下のスケジュール案をもとに進めたいと考えているようです。

2007年1月 4バイトのASも申請可能とする
2009年1月 4バイトのASをデフォルト分配
2010年1月 2バイトASの分配停止

その後、アジア太平洋地域においても2月27日よりオーストラリア・パースで開催されるAPNICミーティング※2でGeoff Huston氏から提案が行われています。

◆NRO NCの選出

現職Lee Howard氏に代わり、Martin Hannigan氏が選出されました。

◆提案事項の結果一覧

2005-1: IPv6におけるPIアドレス
コンセンサスには至らなかったが、継続議論を行う。今後ACは提案者と調整しながら、コミュニティからの意見を反映した内容で再提案を行う。

2005-2: ARIN WHOISにおける情報の扱い
提案者が取り下げ

2005-4: AfriNIC設立に伴うポリシー変更
アフリカ地域をARINポリシー適用対象から省くことでコンセンサス

2005-5: IPv6 HD-ratioの変更
0.8⇒0.94への変更でコンセンサス

2005-6: エニーキャスト向けのアドレスの割り当て
却下

2005-7: マルチホームの定義の変更
現実に即した定義に変更することでコンセンサス

2005-8: IPv6割り当てサイズの変更
コンセンサスには至らなかったが、継続議論を行う。今後ACは提案者と調整しながら、コミュニティからの意見を反映した内容で再提案を行う。IIS

◆参考情報

ARIN XVIプレゼンテーション資料
http://www.arin.net/meetings/minutes/ARIN_XVII_ppm.html

(JPNIC IP 事業部 奥谷泉)

※1 第9回JPNICオープンポリシーミーティング
「プロバイダ非依存なIPv6アドレス割当に関する提案」
<http://venus.gr.jp/opf-jp/opm9/opm9-program.html>

※2 prop-032-v001: 4-byte AS number policy proposal
<http://www.apnic.net/docs/policy/discussions/prop-032-v001.txt>

WIPO Workshop “Advanced Domain Name Dispute Resolution” レポート

2005年10月20日および21日、スイス・ジュネーブにて、WIPO仲裁センター主催のWorkshop、“Advanced Domain Name Dispute Resolution”が開催されました。ジュネーブはヨーロッパ最大の淡水湖であるレマン湖に面し、国連の欧州本部をはじめとする多くの国際機関を抱える静かな落ち着いた街です。WIPO本部は国連欧州本部のすぐ隣にあり、Workshopは、このWIPO本部の1階会議室で行われました。今回、日本からはJPNIC丸山直昌理事および私が昨年引き続き参加し、また、今年はJPNICドメイン名検討委員会委員長の早川吉尚氏(立教大学教授)も参加しました。以下、Workshopの主なプログラムをかいつまんでご説明します。

WIPO仲裁センター(以下、センター)は、1999年12月以来、これまで8000件を超えるUDRP (Uniform Domain Name Dispute Resolution Policy : 統一ドメイン名紛争処理方針)*1に基づく申立を受け付け、裁定を下してきました。Workshopは、これらの裁定に関連して同センターに蓄積された情報を参加者に提供することを主な目的として開催されたもので、毎年CLE*2の対象にもなっています。Workshopでは、センタースタッフおよび著名なパネリスト*3経験者David Bernstein氏とパネリスト経験者のAnna Carabelli氏らが主な講師を務め、センターやUDRPの法的枠組みの解説、UDRP重要条文の解説、最近の重要裁定の紹介、UDRPに基づくドメイン名紛争で裁判にも至った事例の紹介等がありました。参加者にはドメイン名紛争の仮想事例(Case Scenario)が事前送付され、参加者は予め目を通し、考えをまとめておくことが求められます。

参加者の多くは今回が初めての参加であることを考慮して、Workshopでは、まずセンターやUDRPの法的枠組みの解説がセンタースタッフより行われました。

その後のBernstein氏およびCarabelli氏によるUDRPの条文についての解説は、特にUDRP第4節a.の(i)から(iii)を中心に行われました。第4節a.の(i)から(iii)は、申立人側が申立の中で立証しなければならない3項目を定めるものです。両パネリスト経験者による解説は、条文の一般的解説にとどまらず、実際の事例の中で上記3項目の立証の成否を左右し得るような具体的な状況例、例えば「商標権の成立のタイミングとドメイン名の登録」「批判サイト(の正当性)」等、微妙な典型的状況例が列挙され、さらに典型的な各状況例について、「Majority View (パネリスト間の多数意見)」「Consensus View (パネリスト間の統一的な意見)」が明確に表示された上で解説がなされました。

UDRPに基づくドメイン名紛争で裁判にも至った事例に関しては、センタースタッフEun-Joo Min氏より、スペインやアメリカ、韓国で裁判に至ったケースの紹介がありました。裁判に至った場合でもその情報がセンターに自動的に入ってくるわけではありません。そのため、センターは、今年のWorkshopでは、ほとんど裁判事例を把握していないと言っていました。その後かなり時間をかけて情報を収集したようでした。

また、上記解説の合間に何度かグループに分かれてディスカッションが行われました。ある状況例の解説の後、その状況例を反映したCase Scenarioについてディスカッションが行われ、参加者はディスカッションを通じて各状況例におけるポイントに対する自身の理解度を確認することができます。

ちなみに、今年のCase Scenarioは、センターへの過去の実際の申立を参考にして作成されたものなので、昨年のもものと比べて現実に参考になる事例だったと思います。

今年のプログラムの中には昨年とは全く違う趣旨のものが一つありました。それは、センターのパネリストを務めたことのない人(ドイツのBMW社、SeniorLegal CounselのAimee Gessner氏)がインストラクターを務めたプログラムです。

Gessner氏からは、BMW社の商標保護方針や同社のドメイン名紛争事例についての解説がありました。同社は過去にUDRPに基づく申立を800件以上も行ったということで、多くの事例紹介がありました。こうした話は、企業から派遣されていた人達にとっては現実的で参考になるものだったのではないかと思います。センターは来年以降のWorkshopにも同様の内容を含める予定だということでした。

Workshopには今年は19ヶ国から予定定員(50名)を超える参加者があり、Workshop初日の夜にはWIPOの最上階の部屋でカクテル・レセプションが行われました。同レセプションや2日間の昼食会等では他の参加者から各国のDRP制度やドメイン名紛争の現状について話を聞くことができました。参加者の多くは各国弁護士で、顧客の要望に応えるために知識を得たいという人が多いようでしたが、イタリアのGucci社やドイツのMerck社といった一般企業の法務部門から派遣されていた人もおり、パネリスト経験者も数名参加していました。

前述の早川氏は、レセプションや昼食会でセンタースタッフやパネリストと積極的に情報交換をしていましたが、Workshopの中でも挙手し、予め用意した資料を配布してUDRPとJP-DRPの比較について紹介する等して他の参加者の関心を集めていました。

WIPO仲裁センターは、UDRPに基づく申立を過去最も多く処理してきた紛争機関です。しかし、申

立の処理はセンターおよびセンター指名のパネリストにより処理され、当事者の審問や公開の審理等は行われません。また、センターの下す裁定は公表はされているものの、裁定の傾向の分析等に関する情報等はあまり蓄積されていないのが現状です。また、こうしたWorkshop等を開催している機関も他にはないため、センターのWorkshopはドメイン名紛争のトレンドや情報を得ることができる年1回の貴重な機会だと思います。

なお、同様のWorkshopは、来年も同時期に開催される予定になっています。 

(JPNIC インターネット政策部 小久保明日香)



WIPO Workshopの様子

- ※1 UDRP:
<http://www.nic.ad.jp/ja/dr/udrp.html>
<http://www.nic.ad.jp/ja/tech/glos-kz.html#03-udrp>
・UDRP紛争処理方針(翻訳文)
<http://www.nic.ad.jp/ja/translation/icann/icann-udrp-policy-j.html>
・UDRP手続規則(翻訳文)
<http://www.nic.ad.jp/ja/translation/icann/icann-udrp-rules-j.html>
- ※2 CLE:
Continuing Legal Education (研修受講義務) の略。日本の弁護士資格と異なり、海外特に米国の弁護士資格の中には資格取得後、CLEとして認定された講座の受講が義務付けられているものがあります。受講を怠ると資格の継続は認められません。
- ※3 パネリスト:
UDRPに基づくドメイン名紛争において、紛争機関(センター)からの指名により審理を行い、裁定を下す人

インターネットガバナンスに関する 最新動向

◆これまでのいきさつ

2003年に行われた世界情報社会サミット(W SIS)ジュネーブ会合に端を発したインターネットガバナンスの議論は、2004年に国連事務総長配下のワーキンググループ(WGIG)を作り、そのWGIGがインターネット資源管理を含むインターネットガバナンスの現状と問題点をまとめた文書を発表し、2005年7月に最終報告書を上程するという一連の作業を経て、2005年11月16日から18日までのWSISチュニス会合で一つの節目を迎えました。

2005年7月のWGIG最終報告書の中では、現在ICANNが行っているルートサーバ、ドメイン名、IPアドレスの管理の監視形態を今後どうしていくかについて複数の提案が行われ、この最終報告書を基にサミット前の準備会合を経て最終文書の内容に関する交渉が各国間で行われることになりました。

サミットの準備会合では、米国が現在の管理体制を支持する主張をし、これに対しEUは政府の責任・関与を現状より高めるべきという提案を行います。一方途上国側は米国一国がICANN監督機能を握っていることへの強い問題意識からこの「米国一国支配」状態を解消するよう求めるといふそれぞれの立場の違いから、意見の一致を見るのが非常に難しい状況となりました。

しかし本会合前夜の最後の2時間でなんとか各国が最終文書に合意し、無事文書を発表できることとなりました。インターネットガバナンスに関する事項は、「チュニスアジェンダ」と呼ばれる文書に集約して記述されています。

◆インターネットガバナンスフォーラム

この「チュニスアジェンダ」で設立されることが決まったのが、「インターネットガバナンスフォーラム

(IGF)」です。結局、WSISチュニス会合では現行のインターネットの管理体制に影響を及ぼす決定はなされず、議論はさらにこのIGFに持ち越されることとなりました。

チュニスアジェンダでは、第72-79段落にIGFの規定が見られます。以下に主な記述を抜粋します。(総務省参考訳: http://www.soumu.go.jp/s-news/2005/051119_1.htmlより)

72. 我々は、国連事務総長に対し、開かれた包括的なプロセスにより、2006年第二四半期までに、マルチステークホルダーの政策対話のための新しいフォーラムの会合を開催することを求める。これをインターネットガバナンスフォーラム(IGF)と呼ぶ。

73. インターネットガバナンスフォーラムは、その作業と機能において、多国間、マルチステークホルダー、民主的、及び透明であるべきである。

77. IGFは監督権限を持たず、既存の取り決め、仕組み、機関や組織を置き換えることは行わない。しかし、それぞれを包括し、その能力を活用するものである。IGFは中立で、重複することなく、拘束力のないプロセスに基づいて進められる。ここにはインターネットの日常的又は技術的運営は含まれない。

これらの記述を要約・解釈すると、以下のようになります。

- ・国際連合管轄でインターネットガバナンスフォーラム(IGF)を設立し、マルチステークホルダーアプローチで最低5年間維持する。
- ・IGFは既存の組織や取り決めなどを置き換え

るものではなく、対話のための場である。

- ・議論の対象となっていたICANNの体制は、米
国政府の関与を含めて当面現状のまま維持さ
れる。

実質は、WSISジュネーブ会合に引き続いて再度
先送りされたということができると言えるでしょう。ただ、米
国一国支配という批判に対しては、次の文を入れる
ことで合意したので、ある程度途上国側としても納
得できる結論になったということと言えると思いま
す。

63. ～各国は、他の国の国別ドメイン名 (ccTLD) に
関する意思決定に関与してはならない。～

69. 我々は、インターネットに関する国際的な公共
政策課題に関して、各政府が同等の立場でそれ
ぞれの役割や責任を果たすことを可能にするた
め、将来、拡張した協力の必要が生じることを認
識する。

◆マルチステークホルダー

3年越しで議論されているインターネットガバナ
ンスの問題ですが、WSIS/WGIGの一連のプロセス
において議論を行っていたのは政府関係者だけ
ではありません。議論の対象となった当のICANNも
WSIS/WGIGワークショップの開催を通じて参加者
と逐一議論の場を設け、情報の共有を行ってしま
したし、地域インターネットレジストリもそれぞれの地
域ミーティングでインターネットガバナンスに関する
セッションを設けたりしており、民間、市民社会の
参加者も活発に意見交換、主張、提言を行ってきま
した。

集中的に議論を行ったWGIGも、政府関係者、民
間、市民社会という複数の背景を持つメンバーがバ

ランス良く参加し、論点を整理し、報告をまとめ上
げることができた点で評価できると言えるでしょう。
IGFの規定の中にある「マルチステークホルダーであ
るべき」という記述は、その有用性、重要性を政府
関係者側も認めたということだと思えます。今後も
インターネットガバナンスに関する議論は、今まで
通りにこのマルチステークホルダーアプローチで行
われることになります。

◆今後の展開

設立されることが決まったIGFは、2005年末の時
点では2006年6月を目処にギリシャのアテネで開か
れることがほぼ決まっていたと言われていました。
2006年1月時点ではようやくIGFのWebサイトが開
設※1され、2006年2月16日と17日の両日にスイスの
ジュネーブでIGF 開催のための準備会合を開くこと
がアナウンスされました。

その後、IGFのアジェンダをどうするか、費用は誰
がどう負担するべきか、会合の頻度と期間はどうす
べきか、などのアンケートがIGFのWebサイトに公開
され、回答を受け付けています。IGFの運営につい
てはまだほとんど何も決まっていないということが、
このことから伺えます。

JPNICとしてはこれからもIGFの準備状況を逐一
追いつつ、議論に何らかの形で関わっていきたく
と考えています。IP

(JPNIC インターネット政策部 穂坂俊之)

※1 The Internet Governance Forum (IGF)
<http://www.intgovforum.org/>

インターネット技術の標準化プロセス～RFCとは？

インターネット技術の標準化を推進する団体としてIETFがあります。IETF (Internet Engineering Task Force)では、新しい技術仕様についてオープンな議論が行われ、ここでの議論を経てインターネット技術の標準[RFC (Request For Comments)]が生まれます。

RFCとはインターネット利用者、運用担当者、開発者等に有益と判断された情報を公開するための文書シリーズで、インターネット技術の発展に伴い常に新しいRFCが発行され続けています。

以下では、RFCの種類とその標準化プロセスについてご紹介します。

◆ RFCの種類

RFCは、5種類のドキュメント種別が存在しており、情報の性質により区別されます。

(1) Standard Track RFC

IETFでは技術分野毎に組織されるワーキンググループという単位で議論、検討を行っています。Standard Track RFCとは、ワーキンググループでコンセンサスが得られた業界での国際標準とすべき仕様をまとめたドキュメントです。PS (Proposed Standard)、DS (Draft Standard)を経て、S (Standard)となります。PSは複数の組織での独立な実装テストと相互接続性の確認が条件、DSは実質的かつ広範囲での運用テストが条件とされています。S (Standard)の状態になると、STD番号が割り振られます。現在、STD番号を割り振られているドキュメントは非常に少数であり、実質的には、DSのRFCになると、国際標準とみなすことができます。なお、最近では、必ずしも、複数での独立な実装テストと相互接続性の確認が行われなくてもPSとして

RFC化される場合も見受けられるようになってきました。

(2) Informational RFC

Standard Trackには分類されませんが、業界にとって有用な情報を含むドキュメントです。例えば、各組織固有の仕様であっても、それが標準仕様の議論や策定に有効と認められる場合に、RFCとすることができます。企業が標準化を待たずに製品展開を行うような場合に、Informational RFCとしてその仕様を広く公開し、事実上のStandardの地位を確立するための手段としてもしばしば利用されます。

(3) Experimental RFC

標準化が目的ではなく、研究等の目的で検討される技術仕様に関するドキュメントです。純粋な研究目的の場合と、企業が企業固有の仕様を使ってそれを標準化しようとする場合などに用いられます。

(4) Historical RFC

標準化過程での議論の経過など、過去の記録として残すべき情報に関するドキュメントです。IPv6技術の検討経過などがHistorical RFCとなっています。

(5) Best Current Practice

直訳すると「現時点での最善の方法」となり、その時点で最善だと考えられるインターネット管理運用手法やIETFでの標準化プロセスなどを文書化する際に用いられます。

各組織は、各自のIETFにおける発言力とビジネ

ス戦略に基づいて、どのTrackを用いて技術仕様の標準化を進めるべきかを検討しています。Standard Trackでの活動は王道ですが、ドキュメントが作成されRFCとなるまでは、1年以上の月日を必要とするのが一般的で、Informational RFCやExperimental RFCを用いて、より迅速な仕様の公開と普及を図る組織も少なくありません。

◆ 標準化プロセス

IETFにおいては以下の技術標準化プロセスを経てRFCが発行されます。

(1) Internet-Draftの投稿

Internet-Draftとは、その時点でまだ標準化されていない下書き段階の仕様書のことです。各個人が自由に投稿することができ、6ヶ月間IETFのFTPサーバおよびWEBサーバに置かれます。Internet-Draftは、6ヶ月でArchiveから消えていくWork-in-Progressのドキュメントです。Internet-Draftには、ワーキンググループとして投稿・管理されるドキュメントと、個人として投稿されるドキュメントとがあります。

(2) Internet-Draftの成熟

Internet-Draftが、インターネット業界に有益な情報を含んでおり、将来的に標準化されるに相応しいと判断されるとIETFで継続的に議論、検討が行われます。その結果は逐次Internet-Draftに反映され、そのInternet-Draftはより成熟したものとなります。

(3) IESGの承認

IESG (Internet Engineering Steering Group) とは、IETFにおいて議論されるインターネット技術の標準化に関する責任を負い、IETFが作成するRFC

の取り扱い方法について決定をくださる組織です。Internet-DraftがRFCとして発行されるのに十分成熟したと判断されると、IESGに対してRFC発行の申請が行われます。申請が承認されると、そのInternet-DraftにはRFC番号が割り当てられ、IETFのFTPおよびWEBサーバを通じて公式に参照可能なドキュメントとなります。

◆ 今後の展望

1990年後半のインターネット産業の急成長に伴い、IETFへの参加者数の増加と関係するコミュニティの多様化が進展しました。その結果、IETFにおける技術検討やコンセンサスの形成に必要な時間が、長期化してしまう傾向が観測されるようになってきました。これに対応するためか、最近では、ワーキンググループでの技術検討において少人数のデザインチームを形成し、技術仕様確立の迅速化が行われるようになってきました。さらに、標準化速度の迅速化と実態に合ったStandard Trackの再検討、あるいは、知的財産権に関する対応方法など、インターネット標準(STANDARD)化プロセスの見直しに関する検討も始まっています。IE

(JPNIC 理事 / WIDE プロジェクトボードメンバー / 東京大学教授 江崎 浩)
(編集 : JPNIC 技術部)

第 64 回 IETF

1. 全体会議報告

◆概要

2005年11月6日(日)～11月11日(金)、カナダのバンクーバーにあるThe Westin Bayshore Resort and Marinaにて、第64回IETFが開かれました。今回のホストはNortel社で、スポンサーはBC.NET、Symantec社、Telus社の3組織です。Symantec社を除いて、すべてカナダを拠点にしているネットワーク関連の企業や任意団体です。

IETFチェアの発表によると今回のIETFの参加登録者数は1,291名でした。前回(第63回)の1,454名よりは少ないものの、1,100名から1,500名で推移しているここ2年間では、まずまずといったところです。この時期のIETFは毎年アメリカ国内で行われてきましたが、アメリカへの入国手続きが煩雑化している国に配慮してか、今回はカナダで開催されました。参加国は40ヶ国と多かったのはその影響かも知れません。

IETFミーティングは基本的に、初日から始まるチュートリアルと2日目以降に行われるWGやBoFのセッション、4日目や5日目に行われるPlenary (全体会議)で構成されています。またIETFには含まれていませんがグローバルなインターネットの運用に関する調整を目的としたIEPG (Internet Engineering and Planning Group)ミーティングが、おおむね毎回初日の午前に行われています。

今回のIETFでは124のWGやBoFが開かれ、このうちBoFは14セッションでした。BoFは、WGが結成される前に活動趣意(チャーター)を決めたり、WGの必要性についてのコンセンサスを確認したりする会議です。

Plenaryの一つ目である“IETF Operations and Administration Plenary”は11月9日(水)に、二つ目の“Technical Plenary”は11月10日(木)に開かれました。

◆IETF Operations and Administration Plenary

IETF Operations and Administration Plenaryは、IETFの活動全体の運営に関する報告と議論を扱う全体会議です。今回は、IETFチェアのBrian Carpenter氏によるチェア報告、ホストを務めるNortel社によるホスト報告とNOCの運用報告、IAD (IETF Administrative Director)からの報告、RFC Editor報告、IANA近況報告、PROTOチームの近況報告などが行われました。

チェア報告ではドキュメント策定状況の報告の他にPESCI (Process Evolution Committee of the IETF)が紹介されました。PESCIはIETFにおけるドキュメント策定プロセスの見直しを図るため、改善を図るべき範囲を特定し、議論を進めるためのチームです。今回のIETFで初めてのBoFが開かれ、策定プロセスを変更するにあたっての考え方を明確にする(明確化されたものはPrinciplesと呼ばれる)議論が行われました。この策定プロセスの見直しについては[1]にまとめられています。

[1] Goals and Principles for IETF Process Evolution
draft-davies-pesci-initial-considerations-00.txt

また続いて、TCP/IPの開発やIETFの創設といった貢献で有名なVinton G. Cerf氏とRobert E. Kahn氏がPresidential Medal of Freedomを受賞したことのお知らせがありました。Presidential Medal of Freedomは米国の市民栄誉賞にあたるようです。

The Presidential Medal of Freedom
<http://www.medaloffreedom.com/>

IAD (IETF Administrative Director)からの報告では、IETFミーティング参加費用の値上げのお知らせがありました。ISOCからの補助額は毎年増加しており、2005年度には100万ドルを超える見込みがあるものの、RFC Editorの業務増強のための支出増加が見込まれ、参加費用の値上げに踏み切った模様です。2006年度以降に行われるIETFのミーティング参加費用は550ドルになるとのことです。

RFC Editor報告では、昨年に比べてRFC化の業務速度が向上しており、一月あたりの公開ドキュメント数が投稿される数(30程度)に近づいているとのことです。RFC Editorの編集待ちリストは以下のURLで見ることができます。

RFC Editor Queue
<http://www.rfc-editor.org/queue.html>

◆Technical Plenary

Technical PlenaryはIETFの活動のなかで技術的な議論を扱う全体会議です。IRTF (Internet Research Task Force) の報告、IRTFのCFRG (Crypto Forum Research Group)のハッシュ関数の問題に関するプレゼンテーション、IABのチェア報告などが行われました。

IRTFの報告では新設されたりサーチ・グループの紹介とサーチ・グループの状況報告が行われました。新設されたりサーチ・グループは、Transport Modeling Research GroupとInternet Congestion Control Research Groupの二つです。

続いてIRTF CFRGのチェアであるDavid McGrew氏から、SHA-1やMD5といった、多くのプロトコルで使われている一方方向性ハッシュ関数が脆弱になっている状況と、IETFにおける対策についての説明が

ありました。対策としてSHA-1やMD5の利用をやめ、SHA-256を利用する等の方法が挙げられました。

最後のIABのチェア報告では、IABの役割に照らし合わせた活動報告がありました。IABにはIESGやRFC Editorのメンバーの補填のための候補選^{ほてん}びやIETFにおける策定プロセス遂行状況の監視といった役割があります。

Charter of the Internet Architecture Board (IAB)
<http://www.ietf.org/rfc/rfc2850.txt>

今回のIETFではIABの主導により、TechSpec (Technical Specification) BoFが開かれました。これはドキュメント化の要求事項を見直す活動について議論を行うためのBoFです。IETFのWGにおける議論では、しばしばドキュメント化される技術に対するrequirement (要求事項)の整理とレビューが行われます。このプロセスを促進する意味で、現行のドキュメント策定プロセスを見直す必要性が指摘されています。BoFでは特に、draft-mankin-pub-req-01 [2]を元に、IETFの現行のドキュメント策定プロセスの中で、編集のタイミングを見直すことについて議論が行われました。

[2] Requirements for IETF Technical Publication
Service

<http://www.ietf.org/internet-drafts/draft-mankin-pub-req-01.txt>

Technical Plenaryの最後のオープン・マイクロホン(参加者が自由に発言できる時間)では、JPNIC IRR企画策定専門家チームのメンバーである長橋賢吾氏によってIRR (Internet Routing Registry)のあり方に関する議論が行われていました。世界各地のIPレジストリはICANN/IANAを頂点とするIPアドレスの割り振り構造に従って木構造の関係を持ってお

り、各IPレジストリにある登録情報の整合性を保ちやすい構造になっています。一方、IRRはIPレジストリのような構造を持たずに運用されており、登録情報の正しさを実質的に担保できるような仕組みはありません。

以前より、IRRをIPレジストリで運用し、IPレジストリの割り振り／割り当て情報と照らし合わせて、正しさを確認できるようにするという考え方があります。しかし、ある程度の数のルータ管理者に利用されているIRRと、IPレジストリの両方が一つの組織によって運用されているJPNICのようなケースは少なく、その効果や実現性が理解されにくい状況があるようです。

Technical Plenaryでは、木構造にするのは危険である、IRRはRIRよりも多く必要であり、例えばヨーロッパ地域ではNIRのあるアジア地域のようにうまくいかない、といった意見が挙っていました。またオープン・マイクロホンの場ではありませんが、IETFの Protokol 策定の場合だけでなく、ルーティングのコミュニティでの議論が必要だという意見が挙っていました。

今後、IRRの登録情報に関連したプロトコルの策定と、IRRにおける登録情報の正当性に着目した議論が活発に行われていくと考えられます。

(JPNIC 技術部 木村泰司)

2. DNS関連WG報告

◆dnsex WG (DNS Extensions WG)

今回のdnsex WGミーティングでは、NSEC3とTrust Anchor Managementに関する議論が中心となりました。NSEC3にしか対応していないリゾルバとの互換性問題や、DoS攻撃への根本的な対処法

はあるのか、等話し合われました。Issue Tracker (<http://dnssec.nominet.org.uk/nsec3>)が立ち上げられ、残る問題を解決していこうと確認されました。DNSSECが普及する前にDNSSECBisの仕様が議論されていることもあり、古い実装との互換性をどこまで考えるのか、また運用的に実用に耐えるためにはopt-inの仕様を盛り込まなければならない等、まだ多くの問題が残されています。

次に、Trust Anchor Managementに関しては、Trust Anchorの更新を自動的に行う方法について議論が行われました。Trust Anchorとは、DNSSEC検証の起源となる委譲点のことであり、DNSツリー全体で検証を行う場合には、ルートDNSサーバがTrust Anchorとなります。しかし、すべての検証をルートDNSから行うのは現実的ではなく、Trust Anchorを複数設けることによって、DNSSECにおけるデータの検証に対して規模性を持たせることが可能となります。このTrust Anchorリストの自動更新をするために、いくつかのプロポーザルが出されました。まだ議論は始まったばかりで、これからさらなる議論が行われていくと思われます。

dnsex WG

<http://www.ietf.org/html.charters/dnsex-charter.html>

第64回IETF dnsex WGミーティングのアジェンダ

<http://www3.ietf.org/proceedings/05nov/agenda/dnsex.html>

◆dnsop WG

(Domain Name System Operations WG)

今回のdnsop WGミーティングでは、ドラフトの確認が中心の議題となり、特に新しい議論はなされませんでした。DNS Server ID (draft-ietf-dnsop-serverid) に関するドラフトはWGラストコールがか

かることとなり、ようやく標準化されそうです。エニーキャストを用いたDNSサーバの負荷分散が一般的になりつつある現状で、DNS Server IDは、運用管理のために必要な機能であると考えられます。他には、draft-ietf-dnsop-inaddr-requiredやdraft-huston-6to4-reverse-dnsといったドラフトも、早くWGラストコールしようと確認されました。最後に、dnsop WGのこれからの方向に関して議論が行われました。その結果、

- (1) IPv4/IPv6 DNS co-existence issue
- (2) DNSSEC operation
- (3) General DNS operation
- (4) DNS resolver

といった項目が挙げられました。やはりIPv4/IPv6の共存環境における運用上の問題点の解決、DNSSECの運用、ならびにDNSプロトコル自体に起因するDNS 運用上の問題点の解決が、WGの目的となっていくと思われれます。これは最近のdnsop WGの議論と合致する方向性であり、これからのdnsop WGの方向性が確認された形となりました。

dnsop WG

<http://www.ietf.org/html.charters/dnsop-charter.html>

第64回IETF dnsop WGミーティングのアジェンダ

<http://www3.ietf.org/proceedings/05nov/agenda/dnsop.txt>

(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)

3. IPv6関連WG報告

本稿では、第64回IETFでのIPv6に関連したトピックスとして、IPv6、v6ops、softwireの各WGの動向についてレポートします。

◆IPv6 WG (IP version 6 WG)

IPv6基本スペックや、プロトコル自身の挙動にかかわる標準を扱ってきたIPv6 WGですが、今回でface-to-faceのミーティングは最後になります。理由として、IPv6に関する標準化は、既にIPv6 WGのみでなく、IETF全般にわたって実施されていること、IPv6 WGが取り扱っている内容に、現状特に大きな問題はないこと、などが挙げられています。

さて、最後のミーティングですが、11月8日(火)の午前中、9:00~10:30に一コマ実施されました(IETFの時間割ですが、前回のパリで実施された、遅くても20:00前にはすべてのWGミーティング、プレナリが終了するという変更の評判が良かったようで、終了時間に関しては前回と同じような形になっています)。参加者もそこそこ多く、大きめの部屋がほぼ満席になっていました。

今回の主なトピックスは、

- ・ルータ広告のM/Oフラグの扱いについて
- ・IAB IPv6 Ad-Hoc groupの活動状況報告
- ・IPv6コア仕様の標準化

などとなっています。

まず、従来通り、チェアよりIPv6 WGで取り扱っているドラフトの状況について報告がありました。前回までは、チェアが独自に報告用のWebページを用意していましたが、IETFにおいても各種ツールの整備が進んでおり、公式のドラフト等ドキュメント状況管理ページが用意されました。IPv6 WGに関する情報は、<http://tools.ietf.org/wg/ipv6>にあります。他のWGのドキュメント状況に関しても、<http://tools.ietf.org/wg>からたどることができます。各IETF WGの状況をつかむのに非常に便利です。是非ご

利用ください。

さて、「ルータ広告のM/Oフラグの扱いについて」の議題は、かなり前から議論されているものです。RFC2461 Neighbor Discovery for IP Version 6の改版の際に、両フラグの利用方法があいまいであるとの指摘から議論が始まり、別ドラフトにして議論をしてきました。今回、MフラグはアドレスをDHCPv6で取得することを示すこと、OフラグはStateless DHCPv6で情報を取得することを示すこととし、RFC2461の新版に反映することとなっています。

IAB IPv6 Ad-Hoc groupでは、下記のような、今まで実施してきた活動の紹介がありました。

- ・ IABからIPv6に関する各種諮問を受け、意見を返すというグループのミッション
- ・ IANAがRIRに対するIPv6アドレス割り振りの際に、割り振りサイズについての意見照会をIABにしたことに端を発する、という設立経緯
- ・ RFC4147として発行されたIANAのIPv6アドレス空間利用規約の整備
- ・ RFC4159のip6.int廃止

IPv6 WGのIETFでのミーティングは今回で終了ですが、引き続き現在取り組んでいる関連RFCの改版は実施していくことになっています。また、IPv6に関連する話題を扱うために、メーリングリストは継続運用されることになっています。

IPv6 WG

<http://www.ietf.org/html.charters/ipv6-charter.html>

<http://playground.sun.com/publipng/html/ipng-main.html>

第64回 IETF IPv6 WG ミーティングのアジェンダ

<http://www.ietf.org/proceedings/05nov/agenda/ipv6.txt>

第64回 IETF IPv6 WG ミーティングのプレゼンテーション資料

https://datatracker.ietf.org/public/meeting_materials.cgi?meeting_num=64

◆v6ops WG (IPv6 Operations WG)

IPv6のデプロイメントに関する話題を扱うv6ops WGのミーティングは、11月7日(月)の午後、13:00～15:00の2時間枠で開催されました。今回、v6ops WGのミーティングマネジメントがうまくいっていないようで、直前までアジェンダが発表されず、発表されたアジェンダもMLに流れたのみでした(通常はWebにも掲載されます)。

今回の主なトピックスは、

- ・ 企業でのIPv6利用に関するドラフトについての議論
draft-ietf-v6ops-ent-analysis-03.txt
- ・ ルーティングガイドラインドラフトについての議論
draft-blanchet-v6ops-routing-guidelines-00.txt
- ・ IPv6のポートスキャンに関するドラフトについての議論
draft-chown-v6ops-port-scanning-implications-02.txt

などです。

企業でのIPv6利用に関するドラフトも、かなり長い間議論が続いています。今回、このドラフトがExperimentalステータスであるDSTMPプロトコルや、標準でないプロトコルを推奨していることが問題になりました。この推奨部分について、修正文案を作成し、その後にラストコールをかけることになりました。

ルーティングガイドラインのドキュメントでは、

内容が昔の6boneのルーティングガイドラインに似通っているが、6boneはIETFが実施した実験だったため、ガイドラインに従うように要求できたが、一般のISPオペレーター等にはガイドラインは強制力を持たない、つまりルーティングガイドラインはIETFで実施する内容ではなく、レジストリコミュニティやオペレーターコミュニティで実施する内容だ、という意見が出されました。一方で、このようなガイドラインは提示することは必要である、という意見もあり、メーリングリストで継続議論となっています。

ポートスキャンに関するドラフトでは、IPv6はアドレス空間が広い分、IPv4よりもポートスキャンを受けにくいとされていますが、アドレスの付け方によってはその利点が生かせないことになる、としています。ポートスキャンを受けにくいアドレスの付け方やネットワークの構築方法について述べています。このドラフトは、WGドラフトとして議論をしていくことになりました。

v6ops WG

<http://www.ietf.org/html.charters/v6ops-charter.html>

<http://www.6bone.net/v6ops/>

第64回IETF v6ops WGのアジェンダは2006年2月1日現在、IETFのWebページに未掲載

<http://ops.ietf.org/lists/v6ops/v6ops.2005/msg00667.html>

(MLのアーカイブ)

◆Softwire BoF (softwire WG)

v6ops WGから分離し、第62回IETFでのTunneling Configuration BoF、前回のLightweight Reachability softWires BoFに引き続き開催された Softwire BoFですが、ミーティング開催直前にWGとして承認され、第一回のWGミーティングを兼

ねることになりました。

このWGでは、主に以下の2つの問題を取り扱うこととしています。

- ・トンネル技術を利用したユーザーアクセス部分の提供方法
「Hubs & Spokes」と呼んでいます。
- ・コアネットワークのトンネル技術を用いた実現
「Mesh」と呼んでいます。

今回は、問題提起、WGのスコープに関する議論を実施することに時間を使いました。一点目については、一般ユーザーにIPv6サービスを提供するためには現状、ユーザーアクセス機器の対応状況などからIPv6をネイティブで提供することが困難であり、トンネルを使用する方が効率がよいことから、ユーザーに自動的にトンネルサービスを提供する方法を検討していく、というものです。二点目は、コアネットワークをトンネルベースで自動構成する技術に関してですが、例として挙げられていたネットワークがIPv6ピュアネットワークで、その上でトンネルを用いてIPv4サービスを提供する、というものであったため、一般的でなく議論をする意味があるのか、という質問がされていました。

今後、WGのチャーターをMLで詳細検討することになっています。

softwire WG

<http://www.ietf.org/html.charters/softwire-charter.html>

第64回 IETF softwire BoF ミーティングのアジェンダ

<http://www3.ietf.org/proceedings/05nov/agenda/softwire.txt>

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

4.ENUM/CRISP関連WG報告

本稿では、第64回IETFでのCRISPおよびENUMの各WGの動向についてレポートします。

◆CRISP (Cross Registry Information Service Protocol) WG

レジストリデータの検索照会のためのCRISP WGでは、まずインターネットドラフト(以下、I-D)の状況について確認を行いました。いずれも大きな問題はなく小変更を加えた上でIESGに送付されることになりました。

次に、ドメイン名用のIRIS DREG (RFC 3982)発表後に提起された新たな(マイナーな)要求を盛り込むべくDREG2が提案されました。現時点ではまだI-Dとしては提出されていませんが、次回IETFまでには今回のIETFでの議論を反映しドラフトとなる予定です。議論された内容は新たな要素の追加、検索時の部分一致の導入、DNSSECに関する項目およびIDNに関する項目です。

最後に、長橋賢吾氏(JPIRR企画策定専門家チームメンバー)よりCRISP for IRR (RREG)について発表がありました。現在階層構造になっていないIRRをCRISPで扱うことが議論となり、このWGから分離独立して別途BoFを開催することとなりました。

CRISP WG

<http://www.ietf.org/html.charters/crisp-charter.html>

第64回IETF CRISP WGミーティングのアジェンダ

<http://www3.ietf.org/proceedings/05nov/agenda/crisp.txt>

インターネット10分講座 CRISP & EPP

<http://www.nic.ad.jp/ja/newsletter/No25/080.html>

◆ENUM (Telephone Number Mapping) WG

DNSを用いてインターネット電話で使用される電話番号とインターネットリソースの対応付けを行うための方式であるENUMを扱う本WGでは、議題が多く2コマ続けての議論となりました。

まずチャーターの変更についての議論が行われ、キャリアENUM^{※1}の実装の可能性について調査することが盛り込まれました。ENUMの中核となるRFC3761は現在Proposed Standardとして標準化されていますが、相互接続での実装のための必要性から、このRFCをDraft Standardにすることも盛り込まれました。

その後、各I-Dについてレビューが行われました。キャリアENUMへの関心を反映してか、キャリアENUM関連のI-Dが2点、前回(パリでのIETF 63)より引き続き議論されました。一つはキャリアENUMについての要件について、もう一つはキャリアENUMとユーザENUMを同一のDNSツリーに収めても問題ないように、e164.arpaの下にcarrierサブドメインを入れてサブツリーを作成することを提案するものです。前者ではキャリアENUMと呼ぶ代わりに、インフラストラクチャENUMと名称を変えることが合意されました。

その他に、DNSの拡張であるEDNS0をENUMに使う提案、ENUM ServiceへvCardを登録する提案、主に番号ポータビリティに使うことを想定してEnumserviceに電話網のデータのための識別子「pstr:」を登録するための提案などが議論されました。

ENUM WG

<http://www.ietf.org/html.charters/enum-charter.html>

※1 キャリアENUM:

ISPや電話事業者が事業者内または事業者相互間の経路制御のために用いるENUMの形態。

第64回IETF ENUM WGミーティングのアジェンダ
<http://www3.ietf.org/proceedings/05nov/agenda/enum.txt>

JPNICのENUMに関するWebページ

<http://www.nic.ad.jp/ja/enum/>

インターネット10分講座●ENUM

<http://www.nic.ad.jp/ja/newsletter/No21/080.html>

(JPNIC 技術部 山崎信)

5.セキュリティ関連WG報告

第64回IETFでは、セキュリティエリアのセッションが合計で18行われました。このうちBoFはDKIM BoF※2とEMU BoF※3の二つでした。DKIM BoFによって、2004年秋のMARID WGのクローズ以降、迷惑メール対策になる技術に関するIETF活動が再度始まったと言えます。またセキュリティエリアではありませんが、セキュリティに関連してSIDR BoFが開かれていました。

本稿では、SIDR BoFとPKIX WG、IEPGでのAS番号の枯渇と電子証明書に関する話題などについて報告致します。

◆SIDR BoF (Secure Inter-Domain Routing BoF)

これまでRPSEC WGにおいて、インターネットに

※2 DKIM BoF (Domain Keys Identified Mail BoF) :

迷惑メールなどの中でしばしば行われている発信元メールアドレスのドメイン部分を偽装する行為(スプーフィング)を、電子署名を使って検出できるようにする仕組みについてのBoFです。DKIM WGのチャーターでは、現在のスパムをなくすこと自体を目的とするのではなく、安全上の脅威(threats)や要求事項(requirements)をまとめ、またDKIMを使う場合と使わない場合の違いについて分析を行うといったアプローチを取っています。

※3 EMU BoF (EAP Method Update BoF) :

PPPや802.11等で使われている認証の枠組みであるEAP (Extensible Authentication Protocol) 方式のドキュメント整備に関するBoFです。EAP方式を使った認証プロトコルは数多く提案されていますが、RFCになっているものは少なくI-Dを元にした実装の相互運用性が確保されていない可能性があります。そこでEAP-TLS (RFC2716) のProposed Standard化を進めると共に、パスワードなどの方式についてもドキュメント化を進めていくとされています。

おけるルーティングの仕組みについて安全上の要件をまとめる作業が行われてきました。

・ "Generic Threats to Routing Protocols"
draft-ietf-rpsec-routing-threats-07.txt
ルーティング・プロトコルに対する脅威を、原因・可能性・脅威となる挙動・その結果といった形でまとめたもの。

・ "BGP Security Requirements"
draft-ietf-rpsec-bgpsecrec-03.txt
ルーティング情報の交換プロトコルであるBGP (Border Gateway Protocol) を安全にするための要件 (requirements) についてまとめたもの。ピア関係やBGPスピーカー同士、交換される経路情報の認証など複数のポイントについてまとめてある。

これらのドキュメントを通じてルーティングの安全性に関する認識が共有できるようになってきたことから、このBoFは論点を先に移して、ドメイン間ルーティングのセキュリティ・アーキテクチャについて議論し、さらにBGPの安全性の機能を定義する、といった活動を行うために開かれました。

このBoFでは、まずこの議論とドキュメント化活動がSIDRという新たなWGを設立して行われることの妥当性について議論されました。既にRPSEC WGやIDR WGといったWGで、ドメイン間ルーティングのセキュリティについての議論が行われてきたためです。議論の結果、これらのWGでは安全上の要件や短期的な解決方法のドキュメント化が行われてきたのに対し、SIDRはドメイン間ルーティングのインフラストラクチャやプロトコルに着目し、経路情報の認証を行う仕組みを検討するという点で独自の趣意を持っていることが確認されました。

次にsoBGP、S-BGP、psBGPという三つのプロトコルのデザインについて紹介されました。これらは経路情報を交換するためのプロトコルであるBGPを

拡張し、情報源の認証やASパスの検証といった手続きを通じて、ルーティングの安全性向上が図られたプロトコルです。

soBGPに関するI-D

- draft-white-sobgp-architecture-01.txt
- draft-ng-sobgp-bgp-extensions-01.txt
- draft-weis-sobgp-certificates-01.txt

S-BGPの情報源

- <http://www.net-tech.bbn.com/sbgp/sbgp-index.html>

psBGPに関するテクニカルレポート

- http://www.scs.carleton.ca/research/tech_reports/2005/download/TR-05-08.pdf

いずれもIPアドレスとAS番号の偽装を防ぐために電子証明書が使われており、soBGPとS-BGPでは、その電子証明書がIPレジストリで運用される認証局によって発行されることが想定されています。IPアドレスの割り振りをIPレジストリの認証局が証明する(certificate)という意味があります。IPレジストリの認証局が発行した証明書を使うことで、経路情報に含まれているIPアドレスが正当に割り振られたものなのかどうかを判断できるようになるというわけです。

BoFでは、この証明の基盤に基づく経路情報の認証についての議論を進めることに協力するメンバーがいることが確認されました。SIDR WGが設立されると、経路情報の証明データに関するドキュメント活動が行われていくと考えられます。

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

PKIX WGのセッションは11月7日(月)の9時から行

われました。約45名の参加で前回の約60名よりは減少しました。

前回の第63回IETF (2005年8月開催)から今回までの期間に、RFCになったドキュメントが三つ※4、RFC Editorの編集待ちのドキュメントが三つ※5という状況です。

RFC3280※6の後継(通称RFC3280bis)の議論は、ドキュメント改定が進んでいるSCVP (Simple Certificate Validation Protocol)への影響を避けるために一旦停止しています。PKIX WGのセッションの後に新たなドラフトの準備が行われるようです。

SCVPのI-Dは21版になりました。SCVPは電子証明書の検証を他のサーバに任せて行うためのプロト

※4 第63回IETFでRFCとなったドキュメント:

- RFC4158 - Certification Path Building
<http://www.ietf.org/rfc/rfc4158.txt>
証明書のパス(CAの繋がり方)を見つけ、全ての証明書の有効性を確認するための方法や条件など。
- RFC4210 - Certificate Management Protocol (CMP)
<http://www.ietf.org/rfc/rfc4210.txt>
CAと証明書を利用するクライアントプログラムの間などで証明書発行や失効のやり取りをするためのプロトコル。
- RFC4211 - Certificate Request Message Format (CRMF)
<http://www.ietf.org/rfc/rfc4211.txt>
登録局 (RA) から発行局としてのCAに証明書の発行要求をするための形式。

※5 RFC Editorの編集待ちのドキュメント:

- RFC4158 - Certification Path Building
Operational Protocols: Certificate Store Access via HTTP
draft-ietf-pkix-certstore-http-09.txt
- RFC4158 - Certification Path Building
Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)
draft-ietf-pkix-rfc3770bis-03.txt
- RFC4158 - Certification Path Building
Authority Information Access CRL Extension
draft-ietf-pkix-crlaia-03.txt

※6 RFC3280:

- "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
<http://www.ietf.org/rfc/rfc3280.txt>
インターネットで使われることを想定したX.509v3形式の電子証明書とX.509v2形式のCRLの、書式と意味をまとめたドキュメント。RFC2457の後継で、証明書に含めた文字列の国際化や解釈方式などに関する記述を改訂する予定になっています。

コルです。新たにSCVPのサーバが別のサーバからの返答をリレーできるようにするための拡張が行われたりしています。またSHA1等の一方向ハッシュアルゴリズムの脆弱化を受け、新たなハッシュアルゴリズムに対応できるような書式が盛り込まれることになりました。

10月に米国のNIST(National Institute of Standards and Technology : 米国標準技術研究所)で行われたハッシュ・ワークショップでの議論の結果を受け、OCSP(Online Certificate Status Protocol)における新たなハッシュアルゴリズムへの対応手法について議論が行われました。OCSPはオンラインで失効状況を問い合わせるためのプロトコルで、応答の中で電子署名が使われています。ハッシュアルゴリズムの移行時期には複数の種類のハッシュアルゴリズムが使われることが考えられるため、問い合わせ側(requestor)は応答側(responder)が、どのハッシュアルゴリズムを使うのかを知っている必要があります。今のところ問い合わせ側が応答側に対し、事前に指定する方法が挙げられていますが、詳細の検討は今後行われる見込みです。

PKIX WGでは、OCSP以外のプロトコルでも新たなハッシュアルゴリズムに対応する必要があることがわかっています。なおNISTのワークショップでは、当面2010年を目処にSHA-256というハッシュアルゴリズムへの移行が提案されており、業界全体としての移行プランの検討が始まっているようです。またSHA-256の次のハッシュアルゴリズムに関する検討も始まっているようです。

前回のIETFでプレゼンテーションが行われたdraft-ietf-pkix-srvsanはDNSのSRVレコードにあまり依存しない仕様になるようです。このドキュメントは"_ldap._tcp.domain.com"といったドメイン名のSRV

レコードを使って証明書データをやり取りする手法を提案したものです。以前は、得られた証明書の中でsubjectAltNameとして指定された文字列と証明書の入手のために使われたドメイン名とが比較されることになっていました。新しい版では、問い合わせ側は予め対象のサーバのドメイン名とサービス名を知っているという前提に立ち、DNSのドメイン名ではなく、問い合わせ側でわかっている文字列(ユーザーに指定されたものなど)と比較をすることになりました。ただしこの用法の安全性は再検証される必要があると指摘されていました。

◆IEPGにおけるAS番号の枯渇と電子証明書に関する話題

IEPG (Internet Engineering and Planning Group)は主にインターネットのオペレーションに関して意見交換を行い、調整を行うためにIETFの直前に開かれている会合です。

The IEPG
<http://www.iepg.org/>

第64回IETFの直前に開かれたIEPGミーティングの中で、RIPE NCCのHenk氏がAS番号に関する電子証明書について紹介する場面がありましたので紹介します。

RIPE NCCのRIS^{※7}を使った調査によると、2005年8月1日現在、33681のAS番号が割り当てられていることがわかっています。AS番号として使える番号の総数は64511で、まだ残りがあるものの、ひと月に160前後の伸びがあるため、2013年から2024年の間に枯渇するという予測が立てられるとのこと

※7 RIS: Routing Information Service :
<http://www.ripe.net/ripenc/rip-services/np/ris-index.html>

枯渇を避ける方法として、AS番号のビット長を現行の16ビットから32ビットにする方法と、利用されていないAS番号を回収する方法の二つが考えられています。前者は、根本的な解決方法でありながらもまだ実装がなく、移行プランも立っていません。一方後者は回収したAS番号が再び使われ始めるとAS番号の一意性が失われてしまうという問題があります。

Henk氏は後者の問題の対策として、電子証明書を使ってAS番号の利用の証明(certification)を利用する手段について紹介していました。電子証明書を利用すると有効期限を設定したり、有効期限内に失効させたりできるためです。前の利用者の電子証明書が有効かどうかを確認することでAS番号を再利用してよいかどうかの判断ができると考えられます。

1月25日より 「日本ENUMトライアル」用 番号登録を開始

JPNICでは、2006年1月25日より「日本ENUMトライアル」用の番号登録を開始しました。

ENUMとは、E.164番号(電話番号)による名前空間を用いて、インターネット上の複数の通信サービスへの統一的なアクセスを可能にする仕組みです。ENUMを利用すると、IPネットワーク上の電話やメール、FAXなどのアプリケーションのURIを、自分の電話番号に対応するものとして登録することにより、異なる通信サービスを「一つの電話番号」で利用することができるようになります。

ENUMは、

- (1)電話番号は世界中に重複がない
- (2)電話番号は各国の言語に依存しない
- (3)国際接続を視野に入れた際、既に自律分散型で運用されているDNS(Domain Name System)を利用すれば効率的である

という理由からグローバルコミュニケーションの

基礎として高い潜在能力を持ちます。

日本では、総務省が2005年8月に公表した「IP時代における電気通信番号の在り方に関する研究会」の第一次報告書に記載の通り、総務省を中心にENUMトライアル枠組みの準備が進められてきました。具体的には、総務省が日本でのENUMトライアル用に、国コード「81」の番号空間の割当委任(1.8.e164.arpa delegation)を国際電気通信連合(ITU)に申請しました。そして、これは2005年11月15日に正式に承認されました。

総務省への割当委任の終了後、JPNICはENUMトライアル用DNSサーバの運用管理に関わる業務を総務省より受託し、トライアル環境の構築を進め、2006年1月25日に「日本ENUMトライアル」用番号の登録受付を開始する運びとなりました。

JPNICは、2002年9月に日本の実情に即したENUMの管理運用方式や技術標準を民間主導で

このAS番号の電子証明書はRIPE NCCの2006年活動計画の中に入っているそうです。なお第20回APNICミーティングRouting SIGでも"resource certificate" という考え方が紹介されていました。今後、RIRで電子証明書を使ったIPアドレスやAS番号の証明(certification)がさらに検討されていくと考えられます。  (JPNIC 技術部 木村泰司)

提案する「ENUM研究グループ」を設立し、また、2003年9月には、ENUMとその利用に関する実際の技術実験を行うトライアルグループ「ENUM Trial JAPAN (ETJP)」をJPRS、WIDEプロジェクトと立ち上げ、日本におけるENUMトライアルの推進を行ってきました。この蓄積した技術、経験を生かし、「日本ENUMトライアル」においても安定した1.8.e164.arpaのENUM DNS管理と運用を行い、日本国内でのENUMトライアルを行っていきたいと思います。

なお余談ですが、つい先日にはアメリカ政府が国コード「1」を利用する地域のENUMトライアル推進のため、国コード「1」の委任についてITUに申請を行いました。それを受け、カナダとジャマイカ政府からもその申請の承認を要請するレターが出されました。国コード「1」の委任は、2月中旬には承認され、このENUMトライアルは3月早々にはスタートするだろうと予想されており、現在、トライアルへの参加メンバーの募集が始まっています。

日本ENUMトライアル参加等の詳細につきましては、以下URLをご参照下さい。 

(JPNIC インターネット基盤企画部 根津智子)

◆参考URL

「日本ENUMトライアル」

<http://www.nic.ad.jp/jalenum-trial/>

JPNICのENUM紹介ページ

<http://www.nic.ad.jp/jalenum/>