



Bali, Indonesia

2007.2.26→3.2

第23回APNICオープンポリシーミーティングレポート

毎年この時期に開催されるAPNICミーティングは、APRICOTと併せて開催されるのが定例となりましたが、ここではそのミーティングの様子をお伝えしたいと思います。

第23回となるこのたびのAPNICミーティングは、インドネシア・バリで開催されました。APNICスタッフの何名かはテロの影響を懸念して参加を見送り、遠隔での参加という形をとっていましたが、会場は街の中心から離れたホテル地域で、程よくリラックスした雰囲気の中で会議が進められたように思います。

今回の議論の焦点は「IPv4アドレスの枯渇に向けたポリシー」と「APNICにおける料金体系の見直し」の2点であり、どちらも今後のアドレス管理やAPNICの運営に関わる重いテーマであったと言えます。

◆開催概要

【開催期間】2007年2月26日(月)～3月2日(金)

【開催地】インドネシア・バリ

【会場】Bali International Convention Center (BICC)

【参加者】132名

【プログラム】チュートリアル、各種BoF、APOPS (The Asia Pacific OperatorS Forum)、各種SIG、APNIC総会、懇親会
<http://www.apnic.net/meetings/23/program/>

■全体報告

◆提案事項の結果

今回は6点の提案がポリシーSIGに提出され、うち4点はIPv6に関するものでした。そして、「prop-046:IPv4アドレスの枯渇に向けたポリシー」の一部を除き、いずれの提案もコンセンサスは得られない結果となりました(提案事項と結果の一覧は末尾参照)。

IPv6に関する提案は全てJordi Palet氏というヨーロッパのIPv6 Task Forceのメンバーでもある方が提案されたものでしたが、IPv6の普及目的のみに着目しているとの懸念が強く、内容よりもこの点について参加者より随分強い口調で反対意見が表明されていました。

そして、提案事項のうち、最も大きな注目を集めたものはIPv4アドレスの枯渇に向けたポリシー提案です。これはJPNICのIPv4アドレス枯渇対応チームにより策定され

提出した提案ですので、当然、JPNICとしてもその結果は非常に気になる所でした。

議論の結果、提案された要素のうち、「世界的に調整のうえ取り組みを進める」「延命のためのルール変更は行わない」「分配済みアドレスの回収は別の議論とする」との考えについてはコンセンサスが得られましたが、「一定のIPv4アドレスを在庫として残すこと」および「割り振り終了日の周知」についてはコンセンサスが得られませんでした。この結果だけ見ても、参加者の総意としては「世界的に検討が必要な課題ではあるとは考えるが、枯渇時期に関する人為的な介入には反対」とのスタンスであることが見て取れます。

本件については、JPNICとしても国内での議論も踏まえたうえで、次回のAPNICミーティングでも議論を継続することになると考えています。

◆IPv4アドレスの枯渇に向けたポリシーに関する議論

参加者からの主な意見のうち、JPNICからの提案との最も大きな違いは、枯渇期を目処にISPが一斉に準備を開始する必要性を、必ずしも強く感じていないという点でした。

市場原理に従って物事を進めるのが望ましく、おそらく今後の流れとしてはIPv4アドレスの取り引きが行われたりISPによるNATの多用が進み、IPv4ベースでそういった運用を続けることが経済的にISPにとって合理的ではなくなった時点で、例えばIPv6といった他の運用を自然に選択していくことになるだろう、との意見が米国、豪州

等からの参加者の間では主流です。

また、APNICの事務局長も、今後何らかの形でアドレスの取り引きが行われることに備え、現在ポリシーで禁止しているアドレスの譲渡を認めることも検討項目に入れていることを表明しています。

こういった実際の運用状況と市場に委ねる姿勢を、どの程度JPNICの提案の中に盛り込んでいくかが今後の課題と言えそうです。

◆APNICにおける料金体系の見直し

APNICにおける料金体系の見直しは、“APNIC Feeセッション”として専用に時間をとり、提案ではなく、いくつかの料金体系モデルを基に議論を進める形式をとりました。



DNS operations SIGの様子

第23回APNICオープンポリシーミーティングレポート

これまではAPNIC事務局より提示されたモデルをベースに議論を進めており、これは課金額は異なるものの、基本的には現行通りアドレスサイズに応じて課金するモデルでした。

一方、アドレスが分配された時期、すなわち、実際のコストも考慮したモデルが紹介され、これは古い時期に分配されたアドレスは最近分配されたアドレスよりもレジストリ側のコストは低い、との前提に基づいたモデルです。これはレジストリ側のコストも考慮したモデルであることから特にFeeセッションのチェアは大いに検討の余地があると考えている様子で、今後このモデルをベースに料金体系に関する議論を継続することになりそうです。

また、JPNICのようなNIRに対する課金方法も議論に上り、NIRは収入のうち一定の割合をAPNICへ上納する仕組みや、APNIC、NIR管理下に関わらず、全てのLIRは一律同じ金額が課金されるべき等の意見も表明されました。JPNICの料金体系は基本的にAPNICをモデルにしていることから、こういった料金体系の見直しはJPNICおよび国内の事業者にも影響を及ぼすため、IPアドレス管理指定事業者と調整を進めながら今後も議論を進めていく予定です。

◆その他の議論

今回は提出期限に間に合わなかったことから提案ではありませんでしたが、既存のGLOPマルチキャストアドレス (RFC3180) の割り当てを拡張した「eGLOP (RFC3138)」

アドレス (233.144/14) を、IANAではなくRIR経由で分配するという提案です。同じ提案が他のRIRにも提出されており、アジア太平洋地域においても次回のAPNICミーティングで正式に提案として議論が行われる予定です。

prop-047: eGLOP multicast address assignments
<http://www.apnic.net/docs/policy/proposals/prop-047-v001.html>

RFC:3180 GLOP Addressing in 233/8
<http://www.ietf.org/rfc/rfc3180.txt>

RFC3138: Extended Assignments in 233/8
<http://www.ietf.org/rfc/rfc3138.txt>

◆まとめ

今回注目を集めたトピックスであった「IPv4アドレスの枯渇に向けたポリシー」と「APNICにおける料金体系の見直し」は、いずれも提示された実装論の根底に疑問を投げかける議論が展開され、結論には結びつきませんでした。

これはテーマの大きさを考えるとある程度予測できたことであり、単なる意見の発散ではなく、一つの視野に縛られずにより多角的な視野で今後の進め方を再検討できる状態になったという意味では建設的であったと考えています。

当日の議論は公式ページより動画やトランスクリプトでもご覧いただけますので興味のある方はAPNIC23のWebページよりご覧ください。

◆次回のAPNICミーティング

次回のAPNICミーティングは2007年8月末から9月にかけて、インド・ニューデリーでSANOG*と併せて開催されます。南アジアでの開催はAPNICミーティングとしてこれが初めてです。

◆提案事項と結果の一覧

コンセンサス	提案事項	URL
なし	prop-042:IPv6における初回割り振り基準の変更	http://www.apnic.net/docs/policy/proposals/prop-042-v001.html
	prop-043:IPv6ポリシー文書中の“暫定”の記述の削除	http://www.apnic.net/docs/policy/proposals/prop-043-v001.html
	prop-044:IPv6における/48を超える割り当てに対する審議の撤廃	http://www.apnic.net/docs/policy/proposals/prop-044-v001.html
	prop-045:IPv6割り振り対象者をエンドサイトへ拡張	http://www.apnic.net/docs/policy/proposals/prop-045-v001.html
	prop-037:電子メールによる申請の廃止 (前回より継続)	http://www.apnic.net/docs/policy/proposals/prop-037-v002.html
一部あり	prop-046:IPv4アドレスの枯渇に向けたポリシー	http://www.apnic.net/docs/policy/proposals/prop-046-v001.html

◆参考情報

APNIC23公式ページ

<http://www.apnic.net/meetings/23/>

提案事項一覧

<http://www.apnic.net/docs/policy/proposals/>

(JPNIC IP事業部 奥谷泉)

※ SANOG (South Asian Network Operators Group)
<http://www.sanog.org/future.htm>

2007.3.18→3.23

第68回IETF報告

2007年3月18日～23日の6日間にわたり、チェコのプラハにて、第68回IETFミーティングが開催されました。本稿では、全体概要とDNS関連WG、IPv6関連WG、セキュリティ関連WGについてのレポートと、番外編として全体概要レポートの筆者である廣海緑里氏からの貴重な経験談をご紹介します。

■全体会議報告

◆概要

毎日摂氏0度を行ったり来たり、寒風吹きすさび、3日目の夜にはみぞれも降るなど、暖冬の東京でぬくぬくすることを覚えた体にはちょっぴり厳しいプラハが開催地となったIETF68の「全体会議」についてレポートします。

中世の町並みを残す旧市街や新市街からも外れ、ビジネス街を抜けた静かな区域に位置するヒルトン・プラハを会場に、1,000名以上の研究者やオペレーターが参加して熱い議論が交わされました。

会 期：2007年3月18日～23日

会 場：Hilton Prague (Czech Republic)

参加費：600USD (Early Bird Registration)
750USD (Regular Registration)

セッション数：112

(Tutorial, Training, Plenary sessionを除くWGやBoFセッション数)

ホスト：NeuStar社

参加登録者数：1,129人(前回より135人減)

参加国数：45(前回より9カ国増。US、JPが2強は変わらず)

相変わらず、来る日も来る日もたくさんのセッションがあり、当然ながら全ての議事進行は英語なので、時差ほけと戦いながらの議論参加となります。しかし、最先端の技術動向がわかること、そして、それに参加できることは、非常に喜ばしいことです。

今回、Operation and Management Area Open Meetingでは、通常WGになる前のBoFのさらに前段階の状況を含む、mini-BoFがいくつか開催され、データモデルの提示やそれに基づくオペレーションやマネージメント手法への展開論などが議論されました。また、“Harnessing IP for Critical Communications Using Precedence (HICCUP)”というタイトルで、Ad-HOC meetingの呼びかけなどもされていました。

このような公式、非公式な意見交換から、新しい技術が生まれるのを実感できることも参加する意義の一つと言えます。

◆IETF Operations and Administration Plenary

いつも通り、Operations and Administration Plenaryは、4日目の夜(3月21日、17:00-19:30)に行われました。

会期中は、IPv4/IPv6のコネクティビティの他、jabber、wiki、参加者用メーリングリスト、tools-webといった付帯サービスも提供されます。毎回その運用に携わる人達が新しく組織されますが、今回はホストをNeuStar社、協

力組織CZ.nic & CESNET、スポンサーDial Telecom社、NOC-NW運営VeriLAN社、会議運営NeuStar Secretariat Servicesという体制で実施されました。

参加者への接続は、無線LAN(802.11a/b/g+802.1X)で提供され、運用状況の詳細はNOCレポートとして、プレナリセッションで報告されます。1フロアでも広大な会場を4フロアで利用できるように多数のアクセスポイントを設置し、初日はトラブルシュートなども大変だったようです。

ホストを務めたNeuStar社からは、HOST Presentationがあり、会議運営で利用されたNeuStar Secretariat Servicesのサービスが紹介されましたが、今やインターネットへのコネクティビティだけではなく、会議運営のためのファシリタサービスへのIP技術の利用も当たり前になっているのだということをあらためて認識しました。

今回のIETFでは、NomCom (Nomination Committee)の選出結果の発表がありました。IETFチェアは、Braian Carpenter氏から、Russ Housley氏に交代となりました。また、IABチェアも、Leslie Daigle氏からOlaf Kolkman氏に交代となります。Russ Housley氏からの所信表明は、先代チェアの功績を時にジョークを交えながら讃え、見習いながらリーダーシップを発揮するというもので、これからの活躍に期待が持てます。

Olaf Kolkman氏は「Bertを連れている人*」というとおなじみかもしれません。

前回のIETF67からの活動として、新設されたWGが3、終わったWGが6で、現在合計120ものWGが活動中である



Praque, Czeh Reublic

ことが報告されました。また、441もの新しいドラフトが提出されており、更新も1,020もあったそうです。そのうち、IETF LastCallにあるものが119、スタンダード/BCPトラックとして認められたものが67とのことでした。RFCとなったものは、95文書あり、キューもわずかに減ってきているそうです。2006年の1年間で459の文書がRFCになっています。

IANAの活動報告では、IETF関係では1,160のリクエスト(796のprivate enterprise number申請、81のport申請、16のMIME type申請)処理があったことや、300を超える文書のレビューがあったこと、並行してIAOC/IETF trust actionに従った契約が完了したことが報告されました。

定常業務発表の後は、前回発表のあった「Routing and Addressing」についての状況報告と議論がありました。

まず、問題意識の共有として、現在までの技術の発展、展開の末、scaling/transparency/multihoming/renumbering/provider independence/traffic engineering/IPv6 impactについて対処する必要性が説明されました。これは、前回のIETF67でも発表されていた事柄ですが、その後もIABでは、オペレーターグループやレジストリの会合に参加してワークショップを開き、議論するなど活動を続けており、これらの活動成果についてのレポートも作成されています。結果として、新しいアーキテクチャの検討を開始することになり、メーリングリスト(ram@iab.org)では活発な議論が繰り返されています。

* Bert meets the Stars
<http://bert.secret-wg.org/Stars/>

Internet Topics
インターネット・トピックス

プレナリでの結論として、IABから、RoutingとAddressing問題について、

- (1) IETFの役目として、ベンダー、ユーザー、オペレーターを巻き込んだ問題分析のオープンな議論の場を提供し、解決策を見つけ、対策すること。
- (2) 技術的には、短期的にはBGPなどのプロトコルに手を入れることのサポートと、長期的な視点でアーキテクチャの再考を行うこと。
- (3) 付帯する事項に対する継続的な議論の継続を行っていくこと。

が提示されました。

会場の参加者からは、「セキュリティも考慮したアーキテクチャを議論した方がよい」、「市場や製造など経済的な事情は考慮しない点についての異論」や、「新しいビジネスの可能性もある程度考慮すべし」、「IDとロケータを分離しない方がいいのでは」といったさまざまな意見が出ていました。

IABからの提案を受けて、今回のIETFでは、プレナリセッションでの全体発表の他、Internet AreaでのROuting & Addressing Problem discussion (ROAP)、Routing AreaでのBGP tableの増大対策に焦点をあてた議論、Routing Research Groupでの議論といったように個別の議論も行われました。

- ・ IAB Report
<http://www.ietf.org/internet-drafts/draft-iab-raws-report-01.txt>
- ・ RAM mailing list
<https://www1.ietf.org/mailman/listinfo/ram>
- ・ IETF Agenda&Materials
https://datatracker.ietf.org/public/meeting_materials.cgi?meeting_num=68

◆IETF Technical Plenary

最後にTechnical Plenaryですが、これも通例の5日目の夜(2007年3月22日、17:00-19:30)に行われました。

「IAB update」では、新しいチェアであるOlaf Kolkman氏の紹介がありました。IABから提出されている文書について、前述のRouting&Addressing Workshopのレポートの他、前回のIETFで発表があった“ネットの透過性”や“Unwanted Traffic”に関するレポートが発行間近であることの紹介がありました。発行されたものとしては、RFC作成に関してのガイドなどの他に、マルチリンク・サブネットに関するものがあります。

- ・ Transparency (draft-iab-net-transparent-04.txt)
- ・ Unwanted Traffic (draft-iab-iwout-report-03.txt)
- ・ Multilink Subnet Issues (draft-iab-multilink-subnet-issues-03.txt)

「IRTF Report」は、IRTFチェアのAaron Falk氏から、各リサーチグループの最新動向の発表がありました。特記事項としては、Anti-Spam-RGでDNSをベースにしたブラックリストやspamの管理といったトピックスで活発な議論が見られることや、Internet-Measurement-RGで、10月4日にワークショップを計画中であることなどがありました。

続いて、Network-Management-RGのAiko Pras氏から、2006年10月に行われたワークショップの報告がありました。ワークショップでは、あらためて、現状行われているマネージメントモデルの理解や、分散環境でのマネージメントなど難しい点の確認がなされたそうです。こうしたワークショップで得られた見解は、文書化され、広

く共有すべく現在準備中だそうです。

「Technical Discussion」では、“Internationalization Technical Discussion”と銘打って、国際化についてのパネルディスカッション形式で実施され、IABチェアのLeslie Daigle氏をモデレータに、Ted Hardie氏、John Klensin氏、Xiaodong Lee氏、Patrik Faltstrom氏、Pete Resnick氏といった英語を母国語としない人がパネラーとなって、議論が進められました。

議論に先だって、ASCIIからUnicodeの登場、そしてUnicodeの拡張にいたる多言語化の過程の説明があり、そうした多言語化の努力の一方で、プロトコルのデータ形式は依然としてASCIIとなっているものが少なくないことなどの問題点の指摘がありました。例えば、「Latin Small Letter A with Diaeresis (ISO-646-SEの“0x7B”)」(aの上に点がついたもの)というキャラクターについて、ASCII/ISO-646-SE/Unicode/UTF-8/UTF-16/UTF-32/XHTMLなどでの表現形式はどうなっているのかを例にした解説と、たくさんの表現形式が生み出す混乱についての説明がありました。

Ted Hardie氏のIETFにおける国際化のプレゼンテーションでは、人間の理解の仕方という観点からの解説になっており、認識や検索といった目的に対するキャラクターの果たす役割は興味深い話でした。

最後に、現在の多言語化における問題意識を埋めるものとして、IDNAとして新しい体系を作る活動が紹介されました。

- ・ General mailing list (discuss@apps.ietf.org)
- ・ IDNAbis mailing list (idna-update@alvestrand.no)

◆おまけ

Social Eventは、slavonic island に建つ、「The Zofin Palace」という新ルネサンス様式の建物を貸し切って、伝統的ボヘミア料理がふるまわれたそうで、かなり盛況のうちにお開きとなったようです。その後の、参加者メーリングリストでは、「素晴らしかった」というメールが多数飛び交っていました。

以前に開催してから既に10年以上経っている上、急速に国内情勢も変わりつつある見知らぬ東欧圏のプラハという事情からか、IETF68参加者メーリングリストは、プラハの現地情報や現地における生活の知恵などの情報交換で大活躍していました。電子メールによるコミュニケーションは、依然重要なのだなあと認識させられました。

5日目の夜には、セッション(と各々食事)の後に、有志で、標準化の苦労話や各国での技術展開への希望などを分かち合う集まりが恒例で行われています。飲み物や食べ物を持ち寄って、深夜まで旧交が温められていました。IETFでは、大真面目な議論ばかりではなく、このようなくだけた雰囲気「extended BoF」も開催されます。

次回のIETF69は、2007年7月22日から27日まで、米国イリノイ州シカゴで、モトローラ社がメインホストで開催される予定です。

(JPNIC IPアドレス検討委員会メンバー 廣海緑里)

■DNS関連WG報告

会期中に議論された、DNSに関連したトピックスをいくつか紹介します。

◆dnsop WG (Domain Name System Operations WG)

dnsop WGでは、まずdraftの状態確認がなされました。draft-ietf-dnsop-serverid-08は既にWG Last Callが終了し、RFC Editorの手に渡っているという報告がなされました。その他には、draft-ietf-dnsop-default-local-zone がWG Last Callを終了し、draft-ietf-dnsop-reflectors-are-evil-03がWG Last Callの最中となっていることが確認されました。また、draft-ietf-dnsop-respsize-07も会場からレビューする人が選出され、WG Last Callが合意されました。

次に、dnsop WGの2007年のチャーターが確認されました。主にAS112に関する事項やRRのTTLに関する問題について活動していくことが確認されました。AS112に関しては、IPv6トランスポートによるサービスの提供もサポートするか、また現在の IPv4プライベートアドレス空間以外のゾーンもサービスとして提供するかどうかについて、話し合われました。どちらも提供する方向で進めるよう大まかな合意は取れたのですが、これらをきちんと進めるためにはドキュメントが必要であるという意見が出され、WGとしてdraftが必要であるという合意がなされました。

新たな話題としては、draft-regnauld-ns-communicationに関する発表がありました。これは、DNSサーバ間で同期する情報に関して、ゾーンデータだけではなく、DNSサーバ自身の設定も同期するためのプロトコルを決めたらどうか、という提案でした。会場からはいくつかの賛同ならびに反対意見が出されました。WGとしてボランティアを募り、検討を進めていくことが確認されました。

DNSSEC関連では、draft-larson-dnsop-trust-anchor-01にてDNSSEC認証の始点となるTA (Trust Anchor) の管理方法に関する発表があり、draft-koch-dnsop-resolver-priming-00において、一部のDNSサーバ実装で起動時に行うPrimingにてDNSSECを適用する場合の問題等が検討されました。

◆dnsexp WG (DNS Extensions WG)

dnsexp WGでは、今回をもって定期的なミーティングを終了することが確認されました。会場からは、まだいくつかのDNSSEC関連draftがRFCになっておらず、定期ミーティング終了は早いのではないかと、いった意見も出されました。しかし、draftの多くは既に何回か議論されているものであり、あとはMLでの議論で十分であるという点や、DNSSECの普及はdnsexp WGのチャーターではないという観点から、新たに議論すべき事項が発生するまでdnsexp WGのミーティングは一時休止する、という確認がなされました。

また、前回のミーティングにて発表のあったDNSSEC SO (Signature Only) ですが、MLでの議論の結果、WGとし

ては取り扱わないということが合意されました。これは、NSEC3がWG Last Callを目指している最中ということもあり、提案された時期が悪かったという意見も見られました。

draft-ietf-dnsexp-rfc2672bis-dname-01の発表では、残された問題としてCNAMEとDNAMEの混在や、DNAME自身のTTL設定についての議論がなされました。これらの問題点を解決して、早くWG Last Callを行うべきという合意がなされました。

DNSSEC関連では、DNSSECの普及に関して、“DNSSEC Deployment Initiative Roadmap Version 2.0” という発表がなされました。これはDNSSEC普及のために、プロトコルで決まったことと実際の運用との間にある問題を解決していく活動です。詳しくは<http://www.dnssec-deployment.org/>を参照してください。

その他のdraftに関しては、LLMNR (Link Local Multicast Name Resolution) がRFC4795として発行され、draft-ietf-dnsexp-dnssec-opt-in-09がRFC Editorの手に渡っており、draft-ietf-dnsexp-nsec3-10もAD (Area Director) レビューの段階にあることが確認されました。

今回のIETF69では、dnsexp WGのミーティングは開催されないと思われるため、今後はMLでの議論が中心となります。

(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

会期中に議論された、IPv6に関連したトピックスをいくつか紹介します。

◆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、初日、一コマ目である3月19日(月)の午前9時~11時半枠で開催されました。

今回はまず、v6ops WGの属するOperations and Management AreaのArea Director (AD) が変わったことの紹介がありました。今までは、RIPEのIPv6 WGでもチェアをしているDavid Kessens氏がADをつとめていましたが、今回からRonald Bonica氏に変わります。David、長い間、お疲れ様でした！

さて、今回のv6opsミーティングですが、大きく分けて、前回ミーティング終了後にワーキンググループラストコール(WGLC)がかかったWGドラフトの状況確認、オープンWGアイテムの議論およびIPv6ファイアウォールなどの運用紹介の3部構成でした。

まずは、WGLCがかかった以下のドラフトに関して、それぞれの著者より状況の報告がありました。

- (1) IPv6におけるポートスキャン
(draft-ietf-v6ops-scanning-implications)

- (2) IPv6ユニキャストアドレス割り当て (draft-ietf-v6ops-addcon)
- (3) 802.16ネットワーク (WiMAXなど) におけるIPv6 デプロイメントシナリオ (draft-ietf-v6ops-802-16-deployment-scenarios)
- (4) キャンパスネットワークにおけるIPv6移行シナリオ (draft-ietf-v6ops-campus-transition)

(2) については、MLでも議論がありましたが、会場でも、IPv6 PIアドレスについての記述を追加すべき、アドレスプリフィックス「/126」はRFC違反であることを明記すべき、RFC3306で定義されているUnicast-Prefix-based IPv6Multicastアドレス使用法について記述すべき、などの意見が出されました。

(1)、(3) については、MLでも、会場でもあまり意見がなく、今後ステータスを進めることに対する懸念も表明されましたが、(1)、(2)、(3) のドラフト全てにつきまして、コメント反映版の改版ドラフトに、再びWGLCをかけることになりました((1)、(2)、(3) については、2007年4月に、WGLC期間が終了しています)。 (4) については、コメントが少ないこと、また、有用であるがIETFのRFCとして記述すべきものかどうかという意見も表明され、今後の方向性についてMLで議論することになりました。

オープンWGアイテムの議論では、JANOGでも話題になりました、ルーティングフィルタ記述のガイドライン (draft-ietf-v6ops-routing-guidelines) と、IPv6におけるア

ドレス選択の問題提起 (draft-ietf-v6ops-addr-select-ps)、要求仕様 (draft-ietf-v6ops-addr-select-req) に関する議論が実施されました。

ルーティングフィルタのガイドラインに関する議論では、ルーティングフィルタと言いながら、IPv6の特殊用途アドレスの記述が主であり、フィルタの例に関しても、「ガイドラインと言うには情報が少なすぎる」「これはレジストリやオペレーションコミュニティで実施すべきであり、既にフィルタの例が存在する」「フィルタは将来に亘ってメンテナンスが必要であるためRFCに適さない」といった意見が出されました。結論として、IPv6の特殊用途アドレスを文書化し、RFC3330 (Special-Use IPv4 Addresses) と同等の文書を作成することになりました。

なお、この新ドキュメントは、draft-ietf-v6ops-rfc3330-for-ipv6として記述され、2007年5月頭にWGLCがかかっています。

IPv6アドレス選択に関する議論では、MLでの意見を要求条件ドラフトに反映したことの報告および今後予定している解法についての議論が実施されました。問題提起ドラフトについては、WGLCをかけることになり、また、アドレス選択の解法については多くの意見が出され、それを反映したドラフトを記述することになっています。

IPv6ファイアウォールなどの運用紹介では、ファイアウォールや、IDSを実際に運用している状況について報告がありました。IPv6ネットワークに対してもアタックが増え始めていること、ツール群はそろい始めているが、IPv4

用の焼き直しであり、IPv6に特化した攻撃への対処はできないこと、などについてレポートされています。

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

- 第68回IETF v6ops WG のアジェンダ
<http://www3.ietf.org/proceedings/07mar/agenda/v6ops.txt>

◆SAVA BoF (Source Address Validation Architecture BoF)

SAVAは清華大学やChina Mobile社、China Telecom社、Juniper Networks社らが提案する、送信元アドレスの詐称を防ぐ新しいアーキテクチャです。前回のIETFミーティングでは、Internet Area Open Meetingにおいて、問題提起といくつかの解決策の提案がなされ、今回はBoFという形で2時間の枠を取ってセッションが実施されました。また、APRICOT2007のIPv6トラックでも、SAVAアーキテクチャについての発表が実施されており、提案者のSAVAの普及・標準化に対する意気込みが感じられます。

今回のセッションでは、新しいWGの設立に向けて、問題提起とフレームワークの定義、要求条件の整理、そしてCERNET2と呼ばれる中国のIPv6ネットワークをテストベッドとして行われた実験についての発表がありました。

セッションでは、SAVAの適用先はどのようなネットワークのどの部分なのか、また既存手法であるBCP38ではなぜ不十分なのか、について議論が実施されました。同様

の議論は、前回のIETFや、APRICOTでも質問としてあがっていました。セッションの最後に採決が実施され、結論として、問題は重要であるが、新しい技術を導入するのか、それとも運用的対処が可能なのか、解決の方針が決まらない段階であり、IETFで取り組むべき問題であるかどうかはまだ判断できないということとなり、何をすべきかを具体化するために、問題提起および要求条件について再度検討し、次回以降のIETFにて再提案することになっています。

- 第68回IETF SAVA BoFのアジェンダ
<http://www3.ietf.org/proceedings/07mar/agenda/sava.txt>

◆intarea meeting (Internet Area Open Meeting)
/Identifier-Locator Separation BoF/ROAP
(Routing And Addressing Problem BoF)

昨今さまざまなところで取り上げられている、デフォルトフリーゾーンにおけるルーティングのスケラビリティ問題の解決方針を考えるBoFが開かれました。このBoFでは、ルーティングプロトコルの拡張や修正による解決策を検討するのではなく、ID/Loc分割と呼ばれるIPアドレスの個体識別子 (ID) と位置識別子 (Loc) の二つの役割を分けることによって、マルチホームによる経路表の増大を防ぐことが検討されました。これは、IPv4のみならず、IPv6においても、PIアドレスの配布開始などの情勢を受けたものです。

これまでにIETFで検討してきたID/Loc分割に基づく方式としては、Shim6やHIPなどがありますが、これらはトラフィックエンジニアリングなどにおいてオペレータからの要求を満たすことができず、普及が困難であると見込まれています。そこで、今回のセッションでは普及コストとメリットを第一に考え、これまでの議論を最初からやり直すことが目標として掲げた上で、新しいWG設立に向けたアーキテクチャ設計に関する議論が行われました。

今回のセッションでは、解決方式に求められる要求条件を列挙し、どのような方式が考えられるかというデザインスペースに関する議論、そしてこれまで検討された方式がどのようなデザインであり、どの要求条件を満たしていたかについての確認が行われました。個別の解決方式につい

での議論は今回は行われませんでした。現在メーリングリスト上で既にいくつかの新しい方式が提案されています。それらの方式を見てみると、ホストの手前にMiddleboxと呼ばれる装置を設置し、ホストに変更を加えずMiddlebox間でのやり取りによって、ID/Loc分割を実現する方式が多数提案されています。

また、このルーティングスケラビリティに関する議論は、今回のIETFミーティングのスペシャルプレナリヤ、ルーティングエリアのセッションにおいても実施されています。

□第68回IETF intareaミーティング (ROAP BoF) のアジェンダ

<http://www3.ietf.org/proceedings/07mar/agenda/intarea.txt>

第68回IETFミーティングの各種情報は、以下のURLより参照可能です。

□全体プログラム、WGアジェンダ、発表資料

https://datatracker.ietf.org/public/meeting_materials.cgi?meeting_num=68

□録音

<http://videolab.uoregon.edu/events/ietf/>

(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)
(NTT情報流通プラットフォーム研究所 松本存史)

■セキュリティ関連WG報告

セキュリティに関連したトピックスを報告します。

◆Secure Inter-Domain Routing (SIDR) WG
(3/19 13:00~17:00、参加人数：約120名)

SIDR WGでは、ドメイン間ルーティングの安全性を高めるために、AS番号の正当性を検証するメカニズムの検討を行っています。

まず、Resource CertificateプロファイルのI-Dの修正点が報告されました。そして、今後の暗号アルゴリズム拡張への対応が考慮され、SHA-256がMUSTと記述されていた部分が、Minimumに変更されました。また、CA証明書更新のためにAIA属性を利用することが記載されました。

次に、PKIXのチェアであるStephen Kent氏 (BBN) からは、CP/CPSに関する三つのI-Dが提案されました。三つの内訳は、IPアドレス・AS番号に対する証明書ポリシー、インターネットレジストリ向けのCPSテンプレート、ISP向けのCPSテンプレートです。

さらに、Stephen Kent氏からアーキテクチャドキュメントが提案されました。このドキュメントでは、インターネットナンバーリソースに対するPKIの位置付け、ROA (Route Origination Authorizations)、リポジトリについて規定されています。

最後に、再度Stephen Kent氏からROA (Route Origin Attestation) プロファイルの説明が行われました。Route Origin Attestationは、バージョン番号、AS番号、IPアドレスブロックで構成され、CMSのSigned Dataを利用しています。CMSを採用した理由として、XMLよりデータサイズが小さく、CMSはOSS (例えばOpenSSL) を活用できることが挙げられています。

◆RTP Secure Keying (RTPSEC) BoF
(3/19 15:20~17:20、参加人数：約200名)

RTPSEC BoFは、RTP (Real-time Transport Protocol) のセキュアなプロトコルを検討するBoFです。セキュアRTPとしていくつかの鍵交換メカニズムや、RTPの下位レベルにあたるセキュリティが提案されており、基本的な要件を確認しプロトコルの策定を目指しています。

今回のBoFでは、IABメンバーでもありTLS WGのチェアであるEric Rescorla氏によるDTLS-SRTP、Lakshminath Dondeti氏によるMIKEY v2、PGPの作成者であるPhil Zimmermann氏 (MIT) によるZRTPの三つの鍵交換メカニズムについて議論が行われました。議論の最後にハミング投票*が行われ、今後、DTLS-STRPをベースに検討が進められることとなりました。

* ハミング投票
参加者がハミングを行い、その音量によってコンセンサスの成否を判断する方式。

◆Transport Layer Security (TLS) WG

(3/20 9:00~11:30、参加人数：約120名)

TLS-WGは、TLS (Transport Layer Security) の標準化を行うWGです。既にTLS1.0/1.1の標準化を終え、現在はTLS1.2の標準化を行っています。本WGでは、以下のよう

□RFCとして出版されたもの

- ・ TLS1.1 (RFC4346 (PS))
- ・ TLS1.1 Extensions (revised) (RFC4346 (PS))
- ・ Datagram Transport Layer Security (RFC4347 (PS))
- ・ ECC Cipher Suites (RFC4492 (PS))
- ・ Transport Layer Security (TLS) Session Resumption without Server-Side State (RFC4505 (PS))
- ・ TLS User Mapping Extension (RFC4681)
- ・ TLS Handshake Message for Supplemental Data (RFC4680)
- ・ Pre-Shared Key Cipher Suites with NULL Encryption for Transport Layer Security (TLS) (RFC4785)

□Last Call中

- ・ Transport Layer Security (TLS) Authorization Extensions (draft-housley-tls-authz-extns-07)

□RFC Editorの処理待ち

- ・ Using OpenPGP keys for TLS authentication (draft-ietf-tls-openpgp-keys-11)

□RFC Editorが作業中

- ・ Using SRP for TLS Authentication (draft-ietf-tls-srp-13)

□WGで作業中

- ・ AES Counter Mode Cipher Suites for TLS and DTLS (draft-ietf-tls-ctr-01.txt)
- ・ The TLS Protocol Version 1.2 (draft-ietf-tls-rfc4346-bis-03.txt)

この報告の後に、TLS1.2の状況が報告されました。前回からの差分としては、公開鍵指数が3の場合、容易に電子署名を偽造できる問題 (e=3問題もしくはBleichenbacher Attack) への対策と、Timing Attackへの対策が求められていること、NISTのSuite Bへの対策が引き続き行われていることなどについて修正したことが報告されました。

また、未解決な部分として、PKCS#1においてNULLパラメータを指定した際にエンコードを行うべきか否かや、電子署名時のHash Agilityの問題 (DSAではSHA-1しか使えない、自分の証明書で使われているHashしか事実上使えないなど) が指摘されました。さらに、Alert Packetの扱いについての議論が前回に引き続き行われました。これらの問題については、MLで継続して議論することになっています。

NSAのSuite Bへの対応については、2010年までの猶予はあるものの、Hash Agilityを考慮すると、Hash Algorithmの選択についてどう自由度を上げ、相手側とネゴシエーションするかが鍵となりそうです。

新しいWG Draftの提案として、EAPを使ってTLSの認証を行うTEEが提案されましたが、TLS WGの範疇ではないという意見が多く、また現在、前提としているEAPの

モデルとの齟齬があり、EAPのコミュニティとの協力が必要であるという指摘がありました。

さらに、前回のIETFに引き続き、Microsoft社のStefan Santesson氏より、GSS-APIをTLSの認証および鍵生成に使うことが提案されていました。実質的なプレゼンテーションは行われませんでした。興味は持たれたようです。しかしながら、形になるにはまだ時間がかかりそうです。

◆Network Endpoint Assessment (NEA) WG

(3/20 13:00~15:00、参加人数：約100名)

NEA WGでは、Windows Vistaで導入されたNAP (Network Access Protection) のように、ネットワークに接続している物 (Endpoint) が、ネットワークに接続する要件を満たしているかどうかをクライアントから報告するとともに、サーバ側で要件を満たしているかについても監査をし、その結果により接続の許可もしくは切り離し (もしくは限定的な接続) をするための、標準としてのプロトコルを策定しようとしています。

WGのステータス報告として、まずプロトコルデザインを行うデザインチームの選任 (Symantec社のPaul Sangster氏、Intel社のHormuzd Khosravi氏、Avaya社のMahalingam Mani氏、Cisco社のKaushik Narayan氏とNevis networks社のJoseph Tardo氏) 報告がありました。

また、デザインチームにより、要求仕様のI-D (第0版が2007年1月10日公開、第1版が2007年3月5日公開) が公開されたことの報告がありました (4月に第2版が無事公開され

たようです)。なお、この報告の際、会合に参加しているメンバーに当該I-Dを読んでいるかどうかについての確認があり、30%程度のメンバーが読んでいることがわかりました。最近はこの手のI-Dが読まれることはそれほど多くなく、関心の高さがうかがえました。

この報告の後、以下に記したWGの活動におけるマイルストーンが確認され、承認されました。

- 2007年3月 要求仕様I-Dの未解決部分の解決
- 2007年4月 第2版NEA要求仕様I-Dの提案
- 2007年5月 要求仕様についての議論
- 2007年6月 第3版NEA要求仕様I-Dの提案
NEA要求仕様I-DのWG Last Call実施
- 2007年7月 第69回IETFにてWG Last Callで判明した未解決部分の解決
- 2007年8月 第4版NEA要求仕様I-Dの提案
NEA要求仕様I-Dの提案をInformational RFCとするためにIESG Last Call実施

この後、NEA要求仕様I-Dの議論が行われました。

はじめに、NEA要求仕様I-Dの簡単な説明と、前回 (第67回IETF) で合意されたNEAのReference Modelの確認の後、実際にPA (Posture Attribute) プロトコルで交換すべきAttribute値のタイプとストラクチャが紹介されました。この際に、クライアント/サーバ間における情報交換のユースケース紹介と、それに従ったデータのやり取りが紹介されました (この部分は、問題無く軽く流されました)。

また、未解決の問題点として、以下の4点が挙げられました。

- (1) Virtualization
- (2) Non EndpointにおけるNEA
- (3) Securityを全てのLayerで行うか否か
- (4) クライアント/サーバ間で交換すべき情報の最小化を行うべきか否か

種々の観点で議論がなされましたが、いずれもMLにおいて議論を継続するという結果となりました。

特に、(1) および (2) については、NEAの適応範囲を決めるものとなり、意見、コメントが多く寄せられました。(1) に関しては、原則としてVirtualizationを含むという意見が大勢を占めました。その一方でVLAN/VPNにおける扱いはどうするのかという意見が出ました。(2) に関しては、IDSのようなものは積極的にパケットを出さないし、また存在を教えたくないがその点についてどう考えるかという意見が出ました。

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

(3/20 17:40~18:40、参加人数：約50名)

まず、ドキュメントステータスレビューが行われました。前回のミーティングから新しいRFCは発行されておらず、SCVP、Lightweight OCSP、SAN for Service NamesがLast Callとなっていること、RFC3280bisはWGチェアによるレビュー待ちであること、CMCドキュメントはIESGからの指摘事項への対応を行っていることが報告されまし

た。また、ECCアルゴリズムI-Dは進捗が無く、Russ Housley氏（セキュリティエリアディレクタ）からの指摘事項に対応中であること、ECDSAとDSA with SHA-2ドラフトは期限切れとなったが、FIPS 186-3として発行されることも報告されました。

続いて、Jim Schaad氏（Soaring Hawk Consulting社）より、Certificate Management Messages over CMS (CMC) の説明が行われました。三つのドキュメントがIESGによるレビューを受け、いくつかの修正要求があったことが報告されました。その指摘事項の一つは、PKCS#10をMUSTとすることを止め、CRMFをMUSTとすることですが、Microsoft社はPKCS#10を利用しているため課題が残ります。なお、Windows VistaからはCRMFも利用可能です。その他の指摘事項としては、Proof of possessionで利用されるShared Secretサイズをガイダンスとして提供すべきということです。SP 800-56A (NIST document) の最近の修正では、暗号化用途のRSA鍵をProof of possessionへの署名に利用することを許していますが、破棄リクエストへの署名に対しては使うことを許していないという矛盾を抱えています。

Tim Polk氏（NIST）からは、ECCデザインチームの報告がありました。前回のミーティングからecc-pkalg-03の進捗は無く、デザインチームの再構築を行うことになりました。

Stefan Santesson氏（Microsoft社、PKIXチェア）からは、Subject Alternative Name for Expression of Service

Nameについて、IESGからの指摘事項と、国際化の問題に関する説明があり、この問題については修正することになりました。修正後、新たなWG Last Callにかけられる予定です。また、同氏からは、国際化電子メールの説明がありました。EAI WGでは、電子メールアドレスのローカルパートに対する国際化を行っています。これらの名前をどのように証明書で扱うかが課題となっています。

Stephen Kent氏（BBN社、PKIXチェア）からは、Stefan Santesson氏（Microsoft社）が提案した“santesson-pkix-vcrl”をWGアイテムとして受け入れるかどうかについて説明がありました。ML上で投票を行い、その結果、賛成11票、反対22票であったため、WGアイテムからは除外されることとなりました。反対意見のいくつかは、扱っている問題を探ることには賛成だが、そのアプローチには反対という意見でした。

Denis Pinkas氏（Bull社）からのFramework on Key Compromise, Key Loss & Key Rolloverの提案については、代理でStephen Kent氏（BBN社）が行いました。CA、AA、TSAなどの計画的あるいは予定外の鍵交換に対するガイダンス (Informational RFC) を作るべきであるという提案です。より詳細に記載するとドキュメントのサイズはどんどん大きくなるとか、ETSIドキュメントとして既に存在しているのではといった質問がありました。WGアイテムとするかどうかは、MLで投票を行うことになりました。

そして、Scott Lawrence氏（Pingtel社）から、Domain

Certificates in the Session Initiation Protocol (SIP) の課題報告がありました。Lawrence氏からは、TLSコネクション確立における、SIPプロキシの証明書プロファイル作成に対する協力依頼がありました。ExtendKeyUsageを利用すれば良いとか、ある目的に発行された証明書を他のアプリケーションで不適切に使うべきでないといった議論があり、これはMLで引き続き議論することになりました。

◆Long-Term Archive and Notary Services (LTANS) WG (3/20 18:50~19:50、参加人数：約20名)

Long-Term Archive Service RequirementsがRFC4810として公開されました。ERSはIESGレビュー中です。WGではLTAP、ERSおよびLTAPのXML化を行っており、ERS/SCVPとPKI Retentionが4月にWG Last Callとなる予定です。San Diegoで策定したマイルストーンより少々遅れていますが、2007年12月にはこのWGをクローズする予定となっています。また、draft-ietf-ltans-ltap-04が提出され、次のltap-05ではXMLに対応する予定です。ASN.1モジュールやXMLスキーマについても議論が行われ、ASN.1モジュールとして88-ASN.1の代わりに1997/2002-ASN.1モジュールを利用すべきかどうかという議論がありました。1997/2002-ASN.1に対応するフリーのコンパイラには、いくつか不具合もあるという報告が行われました。

続いて、draft-ietf-ltans-validate-01が提案されました。これは検証データの扱いについて規定している文書です。LTAサービスが、署名やタイムスタンプを無限に検証することが可能となるようにするためのメカニズムを提案して

います。

また、XMLERSの紹介が簡単に行われましたが、議論はML上で引き続き行うことになりました。

Michael Herfert氏（Fraunhofer社）からは、ERSの実装について紹介がありました。Herkert氏からOpen Textとの互換性テストも完了しているとの報告があった一方で、会場からはLTAPは利用できないのかといった質問がありました。

なお、RFC3161（TimeStamp）を利用しないERSについては、議論が行われる予定でしたが、これについてはMLで議論を行うことになりました。

◆IPsec FAllover and REdundancy (IFARE) BoF

(3/21 9:00~11:30、参加人数：約60名)

IFARE BoFは、モバイルIPのためのIPsecフェイルオーバーについて検討することを目的としたBoFです。

どの程度の規模を対象としているのか、単にプロビジョニングの問題なのか、どこが課題なのかといった白熱した議論が行われ、これらの点について継続した議論をMLで行うことを確認して終了しました。

また、三つのドキュメントがIESGによるレビューを受けたものの、IESGからいくつかの修正要求を受けたことが報告されました。その指摘事項の一つは、PKIX WGのところでも述べた通り、PKCS#10のサポートをMUSTではなくし、その代わりにCRMFをMUSTとすることです。しかし、Microsoft社はCRMFではなくPKCS#10を利用しており、こ

の提案は解決になっていません。

その他の指摘事項としては、POPで利用されるShared Secretのサイズをガイダンスとして提供すべきということでした。Jim Schaad氏は、これに対する公開されたスタンダードがないため、いくつかの数を揃える（make up some numbers）ことになると考えられます。

また、SP 800-56A（NIST document）の最近の修正では、暗号化用途のRSAをPOPのメッセージ署名のためだけに利用することを許しています。しかし、このドキュメントは、破棄リクエストへの署名に対しては鍵を使うことを許していません。これもまたミスマッチとなっています。

◆IETF Operations and Administration Plenary

(3/21 17:00~19:30、参加人数：多数)

第68回IETFの参加状況、収支報告、スポンサー紹介などが行われました。その中で、新たなIETFチェアとしてセキュリティエリアディレクターであるRuss Housley氏（Vigil Security社）の就任が報告されました。

Russ Housley氏は米国空軍のデータセンター勤務後、RSA laboratoriesでPKI関連の研究開発に従事し、現在ではVigil Security社を運営しています。彼は、IETFにおいてセキュリティエリアで主に活動し、複数のRFC/I-Dを書き、種々のプロトコルのセキュリティ設計を行ってきた人物です。特にPEM（Privacy Enhanced Mail、S/MIMEの前身）の開発と、PEMからS/MIMEへの移行に関して多くの貢献をしました。ここ数年はセキュリティエリアディレク

タとしてセキュリティエリアにおける複数のWGについて方向性を定め、インターネットプロトコルの安全性を高める活動を行ってきました。

また、新たなセキュリティエリアディレクターとして、元PKIX WGチェアのTim Polk氏（NIST）の就任が報告されました。Tim Polk氏はNISTにおけるPKI活動の中心人物の一人であり、米国政府におけるPKIの推進役でもあります。FPMI/PIVなどの活動に関する負荷が高くなり、一度、PKIX WGのチェアを退きましたが、Russ Housley氏のIETF Chairへの就任に伴い、セキュリティエリアディレクターとして活動を行うことになりました。

彼ら二人の昇格は、ともにインターネットプロトコルに対するセキュリティ分野での彼らの貢献と、今後さらに広くセキュリティ（特にPKIなどの公開鍵暗号系の認証技術）を広めることを期待されていると見るべきでしょう。

◆Provisioning of Symmetric Keys (KEYPROV) WG

(3/22 13:00~15:00、参加人数：約50名)

前回のSan Diego会議ではBoFとしての開催でしたが、今回はWGとして開催されました。SecureIDのようなワンタイムパスワード機能は、携帯電話にも搭載される見通しですが、このWGではこれらの共通鍵暗号の共有鍵を前もってシェアする方法、プロトコルの策定を目指しています。

今回のWGでは、パーソナルドラフトとして提案されている、Extensions to CT-KIP to support one- and two-pass key initialization、Cryptographic Token Key Initialization

Protocol (CT-KIP) Web Service、Dynamic Symmetric Key Provisioning Protocol、Portable Symmetric Key Containerについての説明があり、その方向性について議論が行われました。

◆S/MIME Mail Security (SMIME) WG

(3/22 15:10~16:10、参加人数：約20名)

ドキュメントステータスレビューの後、Russ Housley氏（Vigil Security社）から、CMS Authenticated-Enveloped-Data Content Typeの説明がありました。認証された暗号化を達成するための提案で、内容としては、Enveloped DataとAuthenticated Dataを足して2で割ったものです。

SMIMEチェアのSean Turner氏（IECA）からは、Multiple Signature Attributeの説明がありました。HashやSignatureアルゴリズムへの攻撃へ対処するために、複数の署名を埋め込めるようにしています。

(富士ゼロックス株式会社 稲田龍)

■IETF68でのv6fix的問題経験記

今回のIETF参加を通じて経験した、IPv6に関連したトラブルとその解決に向けた一連の経験を紹介します。

◆v6fixとは

IPv6によるネットワークやサーバ運用が始まって久しいとはいうものの、導入初期にありがちで、知らず知らずにかけている問題というものが、世の中には存在します。

「v6fix」は、そうした仕様・実装・運用上の問題を洗い出し、対策を検討し、改善することを目的としたプロジェクトです。

特に私達が問題視した典型的な悪い例は、急速に展開していたホテルのインターネットサービスを利用して、IPv6が有効になったPCをつなぐと、「どうも調子が悪い」というものでした。調査を進めると、仕様・実装・運用全てに問題があり、それらの複合産物として「どうも調子が悪い」状況を作っていることがわかりました。

結果として、On-link Assumption (RFC2461の5.2節)は仕様から外され、DNSの運用上における問題についてはRFC4074としてまとめ、IPv6からIPv4へフォールバックする際の問題については、UNIX系の実装 (KAME、USAGIなど)で改善のための工夫を施すと同時に、改善提案をするといった活動をしてきました。

□v6fix Project Webサイト

<http://www.v6fix.net/docs/v6fix.htmlja>

◆IETF68での問題と解決

そのような関係で、出張などに行くと何か問題がないか確認するのですが、最近では問題のある構成で運用しているホテルのインターネットサービスが減ってきており、「問題は随分改善された」という実感を持っておりました。

ところが、今回のIETF68で開催されたBoFの中で案内されたサーバへのアクセスにおいて、典型例ともいえる出来事がありましたので簡単にレポートします。

【状況】

1日目

- (1) BoFにおいて告知されたメーリングリスト登録用サイトにアクセスするがNG
“destination administratively prohibited” エラーになる
15 * 2001:x::x 3161.85 ms !A 3160.93 ms !A
- (2) Webサイトから登録後、IPv6 MXを持つサブスクライバへの通知がされない
- (3) IPv6 MXへの“host Unreachable” エラーになる
14 2001:x::x 3001.476 ms !H 3162.331 ms !H *
- (4) Webサーバへのアクセスは、IPv6からIPv4フォールバックすればできるため、問題に気がつきにくい
telnet www.foo.bar 80
Trying 2001:x::x...
telnet: connect to address 2001:x::x: Host is down

Trying 166.x.x.x...

Connected to www.foo.bar.

Escape character is '^['.

【処置】

2日目

管理者から「直った」と連絡があり、確認すると無事にアクセスできるようになりました。管理者からの報告によると、前日ルータの設定変更の際に、static routeの設定ミスがあったとのことでした。

これまで私達が見てきたトラブル事例は、ホテルのインターネットサービスに代表されるような、接続時に課金システムに対するDNSのリダイレクトがあったり、そもそも端末がIPv6であることを意識せずに運用しているケースでした。

しかし、今回の事例は、IPv6の研究ネットワークとして、IPv6の protocols を利用することも前提となっていたはずですが、ホテルのような事例は減ってきていますが、今後、このようなよくあるネットワークトラブルが増えていくことが予想されます。

◆健全なIPv4&IPv6ネットワークの運用に向けて

今回トラブルが発生したサーバのあるネットワークは、IPv6の研究ネットワークとして以前から運用されているもので、これから導入する組織よりも運用経験はあったはずですが、それでも、このような些細なミスは起きます。

IPv4でも今回のようなケースはあるのですが、検知、修復までにそれほど時間がかからなくなって、リカバリ体制がきちんとできていると思われます。IPv6でもIPv4と同じレベルの運用ができることが望ましいのですが、考えてみれば、IPv4の運用も既に10年以上の年月が経っています。経験しながら技術が成熟するのを待つ方法もあるのかもしれませんが、私としては、機が熟すのを待つのではなく、積極的にこれまで蓄積してきたIPv4運用の実績や秘訣をIPv6運用に投入できれば、と考えています。

現在は、UNIX系OSやMacOS Xに加えて、Windows Vistaの登場で、さらにIPv6クライアントが増えてきています。前述のような、IPv6ネットワークの運営に長けている組織でも、トラブルシューティングに時間がかかることがあります。これから運用経験を積まれる組織も沢山あると思いますが、IPv4の運用に加えて、IPv6でのサービス設計や、サーバ/ルータ設定にも気をつけてみてください。

そして、相互に健全な共存期となるよう、ご協力いただければと思います。

(JPNIC IPアドレス検討委員会メンバー 廣海緑里)

2007.3.24→3.30

ICANNリスボン会議報告

[関連記事] P.24 第17回ICANN報告会レポート
P.31 第18回ICANN報告会レポート

2007年3月24日から30日まで、リスボン（ポルトガル）にて開催されたICANN会議に出席しました。

以下に、今回の会議の主要トピックをいくつかご紹介します。



◆ICM Registry,Inc.による.xxx (sTLD) の申請を却下

新sTLD^{*1}導入の一環として、ICM Registry,Inc.（以下、ICM）より申請されていた.xxxの契約案についてICANN理事会で審議され、賛成5票、反対9票、棄権1票で申請は却下されました。

本申請は、2004年3月のICMによる申請以降、3年に亘りICANNで審議が続けられ、契約案の修正等を経てICANNとの間で契約交渉がなされてきましたが、今回の却下により、本sTLDが新設されることは無くなったということになります。

ICMは、.xxxが新ドメイン名として導入されれば、インターネット上のアダルトコンテンツとそれ以外のコンテンツとの明確な棲み分けを可能にし、アダルトコンテンツを容易にフィルタリングできることや、多くの事前登録を受け付けており十分なニーズを感じていることなどの理由から、.xxxが有用なドメイン名であることを主張していました。

しかしながら、アダルトコンテンツは各国の法律により捉え方が異なることから、.xxx導入に懸念を示すGACの公式声明が発表され、またこれまでに無いほど多数のパブリックコメントが寄せられていました。

ICANNが.xxxを承認するということは、.xxxへの掲載に適するか否かといった、コンテンツに関する判断を伴うことにもなり、ICANNが負っている技術的な役割を超えることから、ICANN理事会は.xxxに関する契約案および申請を却下すべきとの判断に至りました。

◆RAAレビューに関する議論

これは、2007年3月16日にICANNから通知された^{*2}、米国のレジストラであるRegisterFly社とのRAA（Registrar Accreditation Agreement:レジストラ認定契約）解約を受けて、理事会の場で議論されたものです。

RegisterFly社では、経営上の問題に加え、それが引き金となりドメイン名の登録期限を更新できなかった登録者から数々の苦情が寄せられるなど、オペレーション上の問題をも抱えていました。

ICANNでは、状況を改善すべくRegisterFly社との交渉を再三試みたようですが、RegisterFly社の経営上の問題は訴訟へと発展したため、ICANNは実地調査のために職員を2名送り込み、最終的にはRAAを解約する決断を下しました。^{*3}

この一件を教訓として、登録者保護に向けたRAAの内容の見直しや、レジストラが所有するデータのエクスクローを強化することなどが課題点として浮上し、サンファン会合でも議論されることになりました。

◆WHOISに関するPDPの進捗

WHOISタスクフォースは、WHOISサービスに関する最

終報告書^{*4}をGNSOに提出するとともにその役目を終え、WHOISのPDP（Policy Development Process:ポリシー策定プロセス）は一つの節目を迎えたとも言えます。

ただ、報告書ではOPoC（Operational Point of Contact）とSpecial Circumstancesという二つの異なる提案が含まれ、かつそれらの役割は明確さを欠いており、タスクフォース内でも辛うじて過半数を獲得した内容となっています。WHOISについては、登録者の情報公開を巡って「情報公開派」と「プライバシー擁護派」の対極的な議論がこれまでに繰り返されており、コンセンサスを確立することの難しさが窺えます。

GNSO評議会では、活動期間を120日間に限定して、影響を受ける利害関係者（GNSOのメンバーや法執行機関の関係者など）からなるワーキンググループを結成し、OPoCの役割や責任などを明確にしたり、報告書内で提起された課題解決に取り組むことになりました。

◆新gTLD導入に関するPDPの進捗

新gTLD導入については、2007年3月16日に提出された最終報告書のドラフト版^{*5}をベースに議論が行われ、並行して活動している予約語および他者の権利保護に関するワーキンググループの活動進捗報告もありました。新gTLD導入にあたっては、IDNに関する検討も必要となることから、GACやccTLDメンバーとの会合を持った他、GNSO内のIDNワーキンググループからも会期中に報告書が提出されました。

5月までには勧告の内容を固め最終報告書とし、6月初旬



Lisboa, Republica Portuguesa

には理事会レポートとしてICANN理事会に提出され、サンファン会議の理事会にて審議されることが、4月以降の予定として確認されました。

（JPNIC インターネット推進部 高山由香利）



最終日に行われた理事会の様子。
GACチェアを退任するSharil Tarmizi氏に謝辞を述べるVint Cerf氏。

- ※1 sponsored Top-Level Domain（スポンサー付きトップレベルドメイン）
- ※2 Termination of RegisterFly.com Registrar Accreditation Agreement
<http://www.icann.org/announcements/announcement-2-16mar07.htm>
- ※3 Factsheet
<http://www.icann.org/announcements/factsheet-registerfly-registrars-26mar07.pdf>
- ※4 FINAL TASK FORCE REPORT ON WHOIS SERVICES
<http://gns0.icann.org/issues/whois-privacy/whois-services-final-tf-report-12mar07.htm>
- ※5 GNSO new TLDs Committee Draft Final Report
Introduction of New Generic Top-Level Domains
<http://gns0.icann.org/drafts/pdp-dec05-draft-fr.htm>

2007.4.22→4.25

ARIN XIXミーティングレポート

2007年4月22日～25日にかけて、プエルトリコのサンファンで開催された、第19回ARINミーティングの全体概要をご紹介します。

ARINは北米地域のインターネットレジストリで、一般に公開されたミーティング（有料）を年に2回開催しています。プエルトリコはカリブ海にあるアメリカ領の島です。ミーティング会場周辺はカジノ付きのホテルがあるなど、アメリカのリゾート地の雰囲気がありますが、島自体はダイビングやカリブ海沿岸特有の自然の森を楽しむような場所であるようです。

ARINミーティングは、JPOPMや他のRIRのミーティングと同様に、アドレス資源管理ポリシー策定プロセスの一環であるPublic Policyミーティング（PPMと呼ばれています）や、IPアドレス管理のあり方やARINに関する自由な議論が行われるカンファレンスです。

1日目はPre-meeting activity（事前活動）と呼ばれ、ワークショップやオープンポリシーアワー（アドレスポリシー自体に関する会議）が開かれます。今回は、「Practical Guide to IPv6」というテーマでワークショップが開かれました。2日目と3日目はPublic Policyミーティングが開かれ、4日目はARINメンバーミーティングと呼ばれる、ARINの運営に関するARINメンバーのための、いわば総会です。

今回のミーティングにおける特徴は、まずポリシー提案が13もあったことが挙げられます。この中には、JPNICを中心として各RIRでポリシー提案を行っている「IPv4アドレスの枯渇に向けたポリシー」が入っています。

各ポリシーの議論に当てられる時間が20分と短いため不満の意見が上がりましたが、迅速な進行によって全ての議論が期間中に行われました。

今回のミーティングの参加者は全体で144名でした。そのうちアメリカからが113名、カナダからが3名、カリブ海近辺と北大西洋近辺からが3名でした。各RIRからは3、4名ずつ参加者がいたようです。

◆Pre-meeting activity

Pre-meeting activityでは、前述の通り「Practical Guide to IPv6」というテーマのワークショップが行われました。ワークショップといっても内容はチュートリアルに近いもので、IPv6の基礎や各種OSやルータでの設定方法、6to4やトンネリングについての説明でした。参加者は10名～15名ほどでした。

ARIN XIXのPre-meeting activityの資料等
http://www.arin.net/meetings/minutes/ARIN_XIX/premeeting.html

オープンポリシーアワーでは、ARINコミュニティにおけるポリシー策定プロセスであるIRPEP（Internet Resource Policy Evaluation Process）の歴史の紹介や、今回のPPMで議論されるポリシーに関して、ステータスの確認が行われました。

ARINにおけるポリシーはNRPM（Number Resource Policy Manual）と呼ばれ、一つの文書にまとめられています。ポリシー変更はこの文書への変更を通じて行われるため、ポリシーに関する議論は主にその文案を元に行われます。

- IRPEP - Internet Resource Policy Evaluation Process
<http://www.arin.net/policy/irpep.html>
- NRPM - Number Resource Policy Manual
<http://www.arin.net/policy/nrmp.html>

◆Public Policyミーティング

Public PolicyミーティングはIRPEPの一環として行われるミーティングで、コミュニティの中の提案者によってPPML（Public Policy Mailing List）に投稿された提案のうち、ARIN AC（Advisory Council）によって受理され、再度PPMLに正式なポリシー提案として投稿されたものについて、意見交換を行うために行われます。

今回は先に述べたように13もの提案があり、ARINミーティングで時々見られるような意義についての討論は、参加者の間でも避けられたような印象がありました。

◆遠隔参加について

RIPEミーティングやAPNICミーティングと同様に、ARINミーティングでもオンラインでの遠隔参加（remote participation）ができるようなサービスが整いつつあります。ARINミーティングでは、RealVideoとWindows Mediaによるストリーミングが行われていました。しかしRIPE NCCやAPNICとは異なり、質疑応答に参加できるのは、remote participationの事前登録を行っているユーザーに限られていました。AUP（Acceptable Use Policy）が用意されているなど、ARINらしいサービス提供だと感じられました。



San Juan, Puerto Rico

- ARIN XIX Remote Participation Acceptable Use Policy (AUP)
http://www.arin.net/ARIN-XIX/remote_aup.html



ミーティング会場で、ポリシー策定プロセスを説明したflashアニメーションが展示されていました。このflashアニメーションはオンラインでも閲覧できます。

- The ARIN Policy Process: From Ideas To Actions
<http://www.arin.net/education/cbt/IRPEP/IRPEP.html>

次回のARINミーティングは、2007年10月17日～19日にかけて、米国ニューメキシコ州のアルバカーキで開催されます。

(JPNIC 技術部/インターネット推進部 木村泰司)



会議の様子
RIR updateの中でRIPE NCCについて報告するAxel Pawlik氏

Internet Topics
インターネット・トピックス

■IPアドレスポリシー関連報告

IPアドレスポリシー関連のトピックスをご紹介します。

今回のARINミーティングでは実に13ものポリシー提案が提出されました。以下に提案の概要と結果をお知らせしたいと思います。

◆IPv4アドレス関連

(1) プロバイダ非依存 (PI) アドレスの最小割り当てサイズ変更

現在ARINでは、マルチホームネットワーク向けにプロバイダ非依存アドレスの割り当てを行っていますが、その最小サイズは/22となっています。これを/24へ変更しようという提案です。

APNICでは特に最小割り当てサイズの規定はなく、/24の割り当ても行われていますが、ARINでは/24にすると対象を広げすぎることになるという懸念が示され、出席者の賛同を得られず却下となりました。

(2) プロバイダ非依存 (PI) アドレスの追加割り当て要件の新設

ARINでは、マルチホームするか否かに関わらず、割り当て直後に/22、1年後に/21を使うことを正当化できれば、/20の割り当てをARINから直接受けることができます。しかし、この割り当てにおいて追加の需要が発生した時の割

り当て判断基準が無いため、ここでは「過去に割り当てを受けたアドレスの80%以上を利用していること」という要件が提案されました。

この提案に関しては特に反対はなく、コンセンサスとして最終コメント期間 (Last Call) に付されることになりました。

(3) IPv4アドレスの在庫枯渇に向けたポリシー

前回のAPNICミーティング (APNIC23) で提案されたものと同じ内容で、JPNICのIPv4アドレス枯渇対応チームが策定し提出したものです。^{*1}

この提案は、「IPv4アドレスの在庫枯渇に対しては世界的に調整のうえ取り組みを進める」「延命のためのルール変更は行わない」「分配済みアドレスの回収は別の議論とする」「割り振り終了日を前もって決めた上で周知する」という四つの要素からなるものですが、割り振り停止日を前もって決めるとIANAやRIRで割り振られずに残るアドレスができる可能性があり、そうした状況でなお割り振りを行わないということは疑問である等のコメントが聞かれました。

結論としては、十分なサポートが得られていないという理由で提案は却下されましたが、同時にARINの諮問委員会 (AC: Advisory Council) から、IPv4アドレスの在庫枯渇に関しては引き続きポリシー提案の検討が必要であるとのコメントが付いた形となっています。

◆IPv6アドレス関連

(4) IPv6アドレスポリシー文書からの「暫定的」という言葉の削除

現在のIPv6アドレスポリシー文書では「このポリシーは暫定的 (Interim) であるものとしてみなされ、将来IPv6の運用に関するより幅広い経験に従って見直される」という記述がありますが、既にIPv6の運用の経験は十分蓄積されたとの理由でこの部分を削除するという提案です。

現在のポリシーに「暫定的」という言葉が入った経緯を確認する質問が出たものの、強く反対する意見は聞かれず、Last Callに付されることとなりました。

(5) IPv6初期割り振り要件の変更

1年以内に割り振られたIPv6アドレスを広報する予定があることを示すことができれば、/32の割り振りを受けられるようにするという提案です。

これについては、割り振りを受けられる対象を広げすぎであるという意見が大勢を占め、提案を修正したうえでメーリングリスト (ML) で議論し直すということとなりました。

(6) 同一サイトへ複数の/48を割り当てる際の審議不要化

現在のポリシーでは、同一サイトへ複数の/48を割り当てる際にはRIR/NIRに対し審議申請を行うことを求めています。これを不要とする提案です。

会場では、割り当ての正当化さえできればサイズに関わらずその割り当ては認められるべきではあるものの、今の

段階で全て審議不要とするのは時期尚早ではないかとの意見があり、本提案は却下されました。

◆パネルディスカッション

今回のARINミーティングでは、過去RIRができる以前にIANA等から直接割り当てを受けたアドレスの今後の扱い、およびIPv4アドレスの在庫枯渇に今後どう対処していくべきかに関するパネルディスカッションが行われました。

IANA等から直接割り当てを受けた、いわゆる歴史的経緯をもつアドレスについては、WHOISの更新、料金、返却のプロセスなど今後検討すべき課題の指摘がパネリスト、会場の参加者双方から聞かれました。

IPv4アドレスの在庫枯渇に関しては、IPv6へ移行させるインセンティブをどう考えればよいか、IPv4アドレスの市場取り引きを認めるべきか、認めたとしてARINはどういう役割を果たすべきか等の問題提起がなされましたが、統一された見解に至るということはありませんでした。また、現在利用されていない、いわゆるクラスE空間 (240.0.0.0-255.255.255.255) を、プライベートアドレスとして利用することを検討してはどうか、などの提案も聞かれました。

パネルディスカッションでもポリシー提案の議論中も「NATを用いればIPv4アドレスは十分延命できる」という意見はほとんど聞かれず、全体としてIPv4アドレスの在庫枯渇が今そこにある問題として認識されている雰囲気を感じました。

◆ARINミーティング後の動き

前述した一連のIPv4アドレス在庫枯渇に関する議論に触発されてか、今回のARINミーティング以降、IPv4アドレス在庫枯渇に関する別のポリシー提案が複数提出されています。以下、簡単に内容をご紹介します。

(1) IANAからRIRへのIPv4割り振りポリシー提案

<http://mail.lacnic.net/pipermail/politicas/2007-April/012082.html>

LACNICに提出されたポリシー提案です。IANAの/8の在庫が25個になった時点で、その25個を5個ずつ、五つのRIRへ割り振るという提案です。詳しい内容は上記リンクから参照ください。前半はスペイン語ですが、後半に英語で内容が記述されています。

(2) IPv4ソフトランディングポリシー

<http://lists.arin.net/pipermail/ppml/2007-May/006895.html>

ARINに提出されたポリシー提案です。IANAの/8の在庫が少なくなっていくに従って段階的にRIRからLIR/ISPへの割り振りポリシーを厳しくしていき、同時にLIR/ISPに対し、IPv6のサービス準備状況を確認するという提案です。

上記2提案とも、現在ML上での議論が行われている最中です。

また、過去にGeoff Huston氏によるIPv4アドレス在庫枯渇時期の予測^{*2}を何回かご紹介していますが、この予測手法が5月上旬に見直された結果、従来2011年5月-6月とされていたIANA在庫の枯渇時期が、2009年12月と大幅に早まっています。



オープンポリシーフォーラムにおいて、JPNIC IP事業部の穂坂俊之がプレゼンテーションを行いました。

これは2006年から2007年にかけての消費量が予想よりも多く、従来の近似関数から乖離が生じてきたために見直しをかけた結果ということです。

この在庫枯渇時期の見直しは、今後のポリシー議論に大きな影響を与えると思われます。

◆その他の提案

前記に挙げたもの以外のポリシー提案については、以下に提案内容へのリンクと結果のみ示しますので、参考にしてください。

	提案事項	URL
コンセンサ スと判断さ れ、Last Call に付される もの	2007-1: 申請に関するPGP認証の導入	http://www.arin.net/policy/proposals/2007_1.html
	2007-2: PGP認証を前提として、mail-fromをデフォルトの認証手段とする	http://www.arin.net/policy/proposals/2007_2.html
	2007-3: X.509を認証手段として導入	http://www.arin.net/policy/proposals/2007_3.html
	2007-8: 番号資源移管に関するポリシー文書の用語統一	http://www.arin.net/policy/proposals/2007_8.html
	2007-9: ISPへの緊急割り振りポリシーの変更	http://www.arin.net/policy/proposals/2007_9.html
却下されたもの	2007-11: 初期割り振り申請テンプレート記入にあたっての注釈削除	http://www.arin.net/policy/proposals/2007_11.html
	2007-10: エンドサイトへの緊急割り当てポリシーの変更	http://www.arin.net/policy/proposals/2007_10.html

※1 JPNIC News & Views vol.434

[特集] 第23回APNICオープンポリシーミーティングレポート
<http://www.nic.ad.jp/ja/mailmagazine/backnumber/2007/vol434.html>

※2 IPv4 Address Report

<http://www.potaroo.net/tools/ipv4/>

(JPNIC IP事業部 穂坂俊之)