2006.6.26→6.30 ICANNマラケシュ会議レポート

[関連記事]　P.24「第16回ICANN報告会レポート」

2006年6月26日から30日まで、マラケシュ(モロッコ)にてICANN会議が開催されました。当地の旧市街地は世界遺産に登録されていますが、会議はそこから徒歩で30分ほどの距離にある国際会議場で開催されました。一度旧市街まで歩いてみましたが、じりじりと焼け付く日差しがこたえました。

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。

■ICANN 2006年度予算案を承認

最終日の理事会で、2006年～2007年度の予算案が承認されました。収入は3,417万9,000ドルを見込んでおり、昨年度比で45%増となります。※1

■理事の交代

会期中に、2名の理事が新たに任命されたことがアナウンスされました。1人目はDavid Wodelet氏であり、ASOが選出したMouhamet Diop氏の任期満了に伴い、ASO選出理事として任命されました。

もう一名はRita Rodin氏で、GNSOが選出したMichael Palage氏が辞任したのに伴い、GNSO選出理事として任命されています。

■新gTLD創設プロセスの促進に関する決議

現在GNSOでは、新gTLD創設時の条件、課題、評価項目などのレポートをとりまとめる作業に入っていますが、これを11月までに完成させ、コミュニティからのコメントを受けることを求める決議が最終日の理事会でなされました。

前回のウェリントン会議でも同様の決議がなされており、今回は念押しともいえる決議で、新gTLD創設のプロセスを何としても早期に進めたい意向が感じられます。

ドメイン名マーケットプレイスワークショップの様子

■Add Grace Period(登録猶予期間)とドメイン名テイスティング

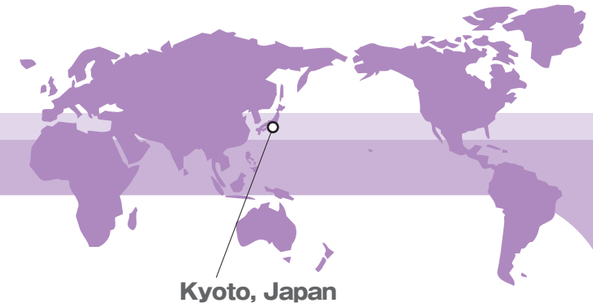
Add Grace Period(登録猶予期間)とは、新規にドメイン名を登録した後一定期間内に登録を取り消せば登録料が不要となる仕組みです。最近この仕組みを利用してドメイン名を一度に大量に登録して、ある程度アクセスのあるドメイン名以外は全て登録を取り消すという、ドメイン名テイスティングという行為が見られます。アクセスのあるドメイン名はWebサイトを立ち上げ、サイト上でオンライン広告を掲載し、そこから収入を得るのが一般的です。

会期中にはドメイン名マーケットプレイスワークショップという会合が設定され、こういう行為が広く行われていることが紹介されました。会場からは、このような登録によりレジストリのシステムに過大な負担がかかっているというコメント、また、本来の目的とは違う使われ方をしているのでAdd Grace Periodは廃止すべきという意見などが出ていました。

また、一度登録されたドメイン名はそれだけで市場性があると見なされ、登録期限切れドメイン名はかなりの確率で再登録されること、その場合において、前登録者の予期しない用途でサイトが構築され、前登録者に対してあらぬ被害が及ぶ可能性があることが紹介されました。このため、登録期限切れの予告がきちんと届くように登録者情報は正確かつ最新のものを登録しておくよう、呼びかけが行われました。

(JPNIC インターネット推進部 穂坂俊之)

※1 Proposed Fiscal Year 2006-2007 Budget
http://www.icann.org/announcements/proposed-budget-2006-07-cln.pdf



ワークショップ報告:日本のドメイン名紛争処理手続の批判的考察
～ADRの運用に関する実証的研究～

2006年7月8日(土)、京都大学百周年時計台記念館・国際交流ホールにて「日本のドメイン名紛争処理手続の批判的考察～ADRの運用に関する実証的研究～」と題したワークショップが開催されました。そこでは、JP-DRP(JPドメイン名紛争処理方針)裁定例検討専門家チーム(2004年11月～2006年3月)による研究成果※1が報告されましたので、概要をご紹介します。

■はじめに

日本では、ADR(Alternative Dispute Resolution:裁判外紛争処理)について学問的な研究はされてきたものの、運用の研究が進んでいないという実態があります。今回のワークショップでは、運用されているADRの実例としてJP-DRP(JPドメイン名紛争処理方針)※2が紹介され、その運用についての研究内容の報告が、前述の専門家チームで活動いただいた早川吉尚氏(立教大学教授)と横山久芳氏(学習院大学助教授)から行われました。また、コメンテーターとして久保次三氏(鹿児島大学教授)と佐藤安信氏(東京大学教授)が加わりました。

■裁定例の特徴

JP-DRPは、JPドメイン名の紛争処理を目的として、ICANNのUDRP※3をモデルに制定されています。JP-DRPとUDRPは、ほぼ同様の条件で運用されていると想像されますが、両者の裁定の勝敗率を見ると、UDRPの場合は申立通りの裁定が出る率が8:1から7:1であるのに対し、JP-DRPの場合はほとんどのケースで移転・取消の申立が認められていることに気付きます。そこで、JP-DRPは申立通りの裁定が下りやすい傾向があるのではないか、という分析に至ります。

■特徴を形成する要因についての考察

JP-DRPの裁定に見られる特徴について探るべく、裁定例を検討した際の考察が発表されました。発表内容の中で印象的であった、次の2点の特徴について記します。

報告が終わってからも参加者同士での議論が続きました。

- 類比判断

JP-DRPの適用対象となるには、申立人が同第4条a.(i)～(iii)の三項目すべてについて申立書で主張する必要があります。(i)については、類似性の存否の判断を必要とされ、この判断基準の置き方が結論に差をもたらす一つの要因ではないかと思われる、との内容で報告されました。

> 参考: JP ドメイン名紛争処理方針
> 第4条　JP ドメイン名紛争処理手続
> (中略)
> a. 適用対象となる紛争
> 第三者(以下「申立人」という)から、手続規則に従って紛争処理機関に対し、以下の申立があったときには、登録者はこの JP ドメイン名紛争処理手続に従うものとする。
> (i) 登録者のドメイン名が、申立人が権利または正当な利益を有する商標その他表示と同一または混同を引き起こすほど類似していること
> (ii) 登録者が、当該ドメイン名の登録についての権利または正当な利益を有していないこと
> (iii) 登録者の当該ドメイン名が、不正の目的で登録または使用されていること
> このJPドメイン名紛争処理手続において、申立人はこれら三項目のすべてを申立書において主張しなければならない。
> (下略)

そもそもUDRPは、サイバースクワッティングのようなドメイン名の濫用的な登録に対処すること(ミニマルアプローチ)を目的としており、裁定の場でもそのような登録であるか否かを客観的に判断しています。対して、JP-DRPでは標識法の類比判断にまで踏み込んだ形で裁定が行われているように見て取れる傾向があり、当初の目的と異なっている点で類比判断の在り方を再検討する必要性が感じられます。

- 専門家アプローチ

先述の如く、UDRPはミニマルアプローチを目的に設計されています。したがって、それに準ずるJP-DRPも、事後的に登録者が濫用者か否かをチェックの上、濫用度の高い使用を排除するシステムであるはずです。

ところが、JP-DRPの裁定例からは、専門家的なアプローチで裁定が行われ、知的財産権を有する側の申立通りの裁定が下りやすいように見て取れます。これは、仲裁機関が知的財産を専門にしているために起こりやすい傾向と言えるのかもしれない、と報告されました。

この傾向については、既判力がないDRPの性質からすると、むしろ専門家的アプローチで包括的に紛争処理が行われ裁判所に出訴する余地を残さない方が、当事者にとって好ましいのではないかとの質問が参加者からありました。これに対しては、ドメイン名登録者は申立があった際にはJP-DRPに従

※1 JP-DRP裁定例検討最終報告書
http://www.nic.ad.jp/ja/drp/index.html#finalreport

※2 JPドメイン名紛争処理方針
http://www.nic.ad.jp/doc/jpnic-00816.html

※3 UDRP
http://www.icann.org/dndr/udrp/policy.htm

Internet Topics
インターネット・トピックス

うものとされており、またDRPが敢えて1回きりの簡便な手続で行えることとしている以上、ドメイン名紛争処理を目的とするDRPはミニマルアプローチが適当であると判断できるとの回答がありました。

ドメイン名紛争では登録者が答弁書を提出してこないケースが多く、ミニマルアプローチでもサイバースクワッティングなどのケースには有効であることが説明されました。

■これからのJP-DRP

以上の考察をもとに、ADRを運用する上で検討が必要となる次の点が述べられ、今後のJP-DRPの在り方を考える上でも重要であることが伝えられました。

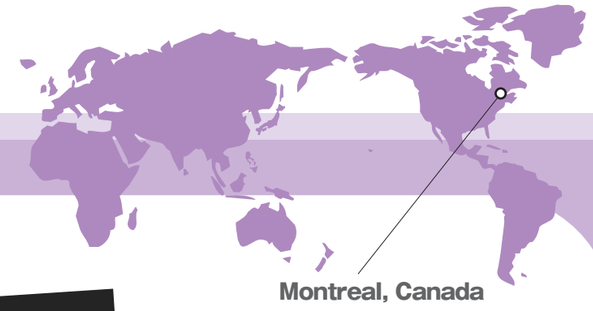
・制度設計の際に重視する特徴の確認
ADRは裁定する人によるイメージの差に裁定が影響を受けやすいため、どのようなADRを実現しようとするのか、内部での不断の検討が必要であること。

・パネリスト研修
ADRの趣旨を個々のパネリストやパネリスト候補者に徹底させるために定期的な研修の機会が必要であること。これは、ADRの当初の目的が見失われないようにする上でも重要と考えられます。

最後の質疑応答では活発な意見交換が行われ、JP-DRPの当初の目的を再確認し改善していくことが、日本のインターネット環境改善にとっても大切であると考えられる、とのメッセージもいただくことができました。今後の取り組みを考える上で非常に参考となる、大変有意義な時間を過ごすことができました。

□参考：ドメイン名紛争処理方針(DRP)
http://www.nic.ad.jp/ja/drp/

(JPNIC インターネット推進部 高山由香利)



2006.7.9→7.14 第66回IETFレポート

2006年7月9日(日)から7月14日(金)まで、カナダのモントリオールにて、第66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、ENUM関連WG、セキュリティ関連WGについてのレポートをご紹介します。

■全体会議報告

◆概要

2006年7月8日、モントリオール国際空港に降り立つと、清潔感のあるロビーと、英語とフランス語が混ざったざわめきに迎えられました。冬には気温がマイナス30度にもなる都市ながら、この時期はTシャツだけで過ごせる快適な気候です。

今回のIETFはカナダ・モントリオールのPalais des Congres de Montreal (モントリオール・パレ会議場)で開かれました。会場は市の中心部から徒歩10分程のところで、同じ規模の国際会議を同時に二つ以上は開けそうな巨大な会場です。

今回の参加登録者数は1,257名で、参加国は44ヶ国でした。米国・ダラスで行われた前回のIETFの時に、いくつかの国からの参加者が米国への入国ができず、IETFの働きかけによって急遽ビザが発行されるという出来事があったようですが、今回はそのような事態への配慮がなされて、カナダで開催された模様です。

IETFでは、WGの会議とPlenaryと呼ばれる全体会議が行われます。WGの会議では主にRFCになる前のドキュメント(Internet-Draft)に関する議論が行われます。議論は基本的にMLで進められますが、IETF期間中にオフラインで打ち合わせることでコンセンサスを確立したり、その場で実装をしてつきあわせたりして(!?)、RFC化を目指します。一方、Plenaryは会期中2回だけ行われます。

“IETF Operations and Administration Plenary”はIETFの運営面の全体会議で、7月12日(水)に開かれました。技術面の全体会議である”Technical Plenary”は7月13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。今回はミーティングのホストを務めるEricsson社のプレゼンテーション


IETF Operations and Administration Plenaryの様子

Internet Topics インターネット・トピックス

とNOC(Network Operation Center)の報告、IAOC(IETF Administratire Oversight Committee)やIASA(IETF Administrative Supporting Activity)、TOOLSチームといったIETFを支える活動の報告と、IETFにおける標準化プロセスの再検討に関する議論などが行われました。

はじめにIETFチェアのBrian Carpenter氏からチェア報告がありました。前回のIETF以降、4つのWGが新設され13WGが終了、RFCが138出されたそうです。IASA報告の中では、RFC Editorの活動報告や前回のIETFの会計報告などが行われました。RFC EditorはRFCの校正を行い、体裁を整えるチームで、2年程前より体制を建て直し徐々に作業効率の向上を図っています。2006年度は2005年度よりもRFC編集作業のペースが58%近く向上しているそうです。

前回のIETFの会計報告によると、ケータリングでの赤字や送迎サービスを予算に入れていなかったことなどが原因で、全体として$55,000程の赤字となってしまったそうです。しかし今回はケータリングのモデル化と改善を進めたとのことでした。これによって休憩時間に出るクッキーがすぐになくなってしまったり、逆に余ったりすることを避けられるようになってきたとのことです。

IETFにおける標準化プロセスの再検討は、2004年以降、IETFチェアのBrian氏自身によって進められてきました。これに関するInternet-Draftは、draft-carpenter-newtrk-questions-00.txtです。これまでWGの会議が何回か開かれてきましたが、方向性が決められず、今回のPlenaryで全体の意見を聞くことになったようです。しかし会場からは再検討の議論自体に意義を見いだせないといった意見が挙げられていました。

□ New IETF Standards Track Discusion (newtrk)
http://www.ietf.org/html.charters/newtrk-charter.html

◆Technical Plenary

Technical PlenaryはIETFの活動の中の技術的な議論を扱う全体会議です。IRTF(Internet Research Task Force)の活動報告、IRTFのSAM RG(Scalable Adaptive Multicast Research Group)の紹介、IABのチェア報告などが行われました。

IRTFは長期的な観点で技術を捉え、リサーチと議論・検討を行うグループです。必要性が認められるとIETFでの標準化作業を行います。SAM RGは前回のIETFの後に結成されました。SAM RGは、複数のマルチキャスト・プロトコルの利点をそれぞれ生かし、展開・普及を図ることを目的としています。IPマルチキャストだけでなくアプリケーション層に分類されるようなものや、中間的な分類(Hybrid)に入るプロトコルも議論の対象に入っています。IPマルチキャストとして分類されるものはXCASTのみとなっています。

□ SAM Research Group
http://www.samrg.org/
□ XCAST
http://www.xcast.jp/

IABのチェア報告では、IAB主催のBoFやワークショップの紹介とRFC Editorのあり方の検討に関する発表がありました。これまで2005年10月のNANOGや2006年3月のAPRICOTで開いてきたIPv6 Multicast BoFが、2006年4月に行われたRIPE Meetingでも行われたそうです。また秋に予定されている"Routing and Addressing"ワークショップのお知らせがありました。

□ IAB-Sponsored Open Meetings (IAB主催のオープンミーティング)
http://www.iab.org/documents/open-mtgs/

IABでは今後30年という長期的な視点で、RFC Editorのあり方について検討しています。(ちなみに、最初のRFCであるRFC1が出たのは1969年4月7日で今年で37年経ったことになります)特にRFC Editorのプロセスの中でIABやIAOC、そしてIETFがどのように関わっているべきかといったことを議論しており、そのために、RFCの目的やミッション、RFC化の役割分担についての整理をしようとしています。またIABではIAOCと共にRFC EditorのRFP(Request for Proposal - 提案依頼書)の作成を進めているそうです。会場からはRFC Editorに関する議論に対して時間をかけ過ぎているといった意見が出ていましたが、ドキュメント(Internet-Draft)の著者の主旨を正確に組み入れ、かつRFC化の作業がコミュニティの必要に応えるようなスピードで行われるための効率化を図るため、慎重な検討が進められている様子がうかがわれました。

この他に、IDN(Internationalized Domain Names)とIDNA(Internationalizing Domain Names in Applications)を組み合わせて使うことの問題点、例えば類似する文字でspoofing(だます行為)が行われてしまうこと等について、DNSのアーキテクチャの中で取り組む考え方などについて紹介されていました。

◇　　◇　　◇

今回のIETFではEricsson社の提供でsocial event(参加者を対象とした会議以外のイベント)が行われました。会場の近くを流れるローレンス川でのディナークルーズです。会場から離れ、技術以外の話題で交流することで、IETFが多様な国からの参加者によって成り立っていることを改めて実感しました。

(JPNIC 技術部 木村泰司)

DNS関連WG報告

◆dnsext WG (DNS Extensions WG)

今回のdnsext WGでは、まずNSEC3の進捗状況が確認されました。フランクフルトにて行われたNSEC3のワークショップ結果が報告され、相互接続性試験において大きな問題は生じなかったことが確認されました。テスト結果の詳細はhttp://www.nsec3.org/に公開されています。残る問題としては、今までのDNSSEC実装との互換性であったり、DNSSECチェインの頂点を指定する方法等があげられていました。

NSEC3の他には、新たにDNS Cookieの話題があがりました。これは、HTTPで利用されているCookieと同様で、DNSサーバは応答時のAdditional Sectionに仮想的なCookieレコードを加え、クライアントに自分のCookieを発行します。クライアントは以後このCookieを利用して問い合わせを行います。これにより、詐称されたIPアドレスからの問い合わせにはCookieが含まれない、もしくは異なったCookieが含まれる可能性が高くなり、その場合には短いエラーメッセージを返答することで、DNSサーバをパケット増幅器として利用したDoSを防ごうというものです。この話題は今回初めて議題にあがったものであり、これからの方向性はまだわかりませんが、議論は続いていくと思われます。

□dnsext WG
http://www.ietf.org/html.charters/dnsext-charter.html
□第66回IETF dnsext WGミーティングのアジェンダ
http://www3.ietf.org/proceedings/06jul/agenda/dnsext.html

◆dnsop WG (Domain Name System Operations WG)

dnsop WGでは、まずdraft-ietf-dnsop-reflectors-are-evilに関して議論が行われました。パケット増幅器になるのを防ぐためには、エラーメッセージを返さずにそのまま問い合わせパケットを破棄すればいいのではないか、draftのタイトルに“recursive”という単語を入れた方がいいのではないか、TSIGの代わりにSIG(0)を推奨するのはどうか、といった議論がなされました。

また、draft-ietf-dnsop-default-local-zonesとdraft-ietf-dnsop-respsizeをWorking Group Last Callすることが確認され、期限切れで放置されているdraft-ietf-dnsop-inaddr-requiredを更新することが確認されました。

他には、draft-papas-dnsop-long-ttlに関する発表が行われ、関心を集めていました。これは、NSレコードならびにそれに関連づけられたAもしくはAAAAレコードのTTLを調査したdraftです。その結果によると、調査したNSレコードの約半数が12時間未満のTTLであり、1/3が1時間未満のTTLであったということです。中にはTTLを0としているTLDも存在しました。これに関して、TTLをもっと長く設定するよう推奨するかという議論が行われ、WGとしては分析を示すのみで、推奨は見送るという結論に達しました。

□dnsop WG
http://www.ietf.org/html.charters/dnsop-charter.html
□第66回IETF dnsop WGミーティングのアジェンダ
http://www3.ietf.org/proceedings/06jul/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)

■IPv6関連WG報告

本稿では、IPv6に関連したトピックスとして、v6ops、shim6の各ワーキンググループ(以下、WG)の動向と、会議では直接は話題になっていませんが、ipv6 MLでのIPv6アドレス割り当てに関する議論について紹介します。

◆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、7月12日(水)の午前、9:00～11:30の枠で開催されました。

今回は、IPv6網でのセキュリティ的観点についてのドラフトが多く議論されました。主なものは以下の通りです。

- IPv6ネットワーク防御(draft-ietf-v6ops-nap-01)
- IPv6ネットワークでのICMPv6のフィルタ手法
(draft-ietf-v6ops-icmpv6-filtering-recs)
- IPv6ネットワークでのセキュリティ概論
(draft-ietf-v6ops-security-overview)
- IPv6におけるポートスキャン
(draft-ietf-v6ops-scanning-implication)

IPv6ネットワーク防御(draft-ietf-v6ops-nap-01)のドラフトは、IPv4で、NATで担保されているセキュリティを、IPv6ではどのように実現できるかを記述しています。ミーティングでは、内部ネットワークのトポロジを隠蔽するのにホストルートを使うという記述や、内部でULA(Unique Local IPv6 Unicast Addresses : RFC4193)を使うことを推奨することの是非に関する議論、NATとファイアウォールを同等に扱っている記述を変更する提案などが行われました。

IPv6ネットワークでのセキュリティ概論(draft-ietf-v6ops-security-overview)は、IPv6/IPv4共存時の課題や、IPv6ネットワーク運用時におけるセキュリティ上の問題などを述べています。ミーティングでは、IPv6の断片化ヘッダを利用したときに発生する問題や、拡張ヘッダ等のファイアウォールでのフィルタに関する問題について議論されました。

その他の二つのドキュメントも含め、今後、WGのラストコールがかけられることになっています。

IPv6ネットワークの利用が広まり、運用のノウハウ、運用時の問題や課題などが具体的に議論されるようになってきています。

□v6ops WG
http://www.ietf.org/html.charters/v6ops-charter.html
http://www.6bone.net/v6ops/
□第66回 IETF v6ops WG のアジェンダ
http://www.ietf.org/ietf/06jul/v6ops.txt

◆shim6 WG(Site Multihoming by IPv6 Intermediation WG)

shim6 WGでは、IPv6に特化した、通信を実施するエンドホスト間の連携によりマルチホームを実現するshimと呼ばれる方式のプロトコル策定を目的としています。今回のセッションでは、基本仕様のレビューとともに、拡張仕様の検討、およびshim6 WGの今後の方向について議論が行われました。

shimプロトコルの基本仕様は、過去のミーティングにてほぼ決定され、軽微な修正が施されるのみという状況になっています。

しかしながら今回、基本仕様の一部に特許上の問題があることが議論となり、WGとして、この問題が解決するまでは基本仕様の標準化を止めることとなりました。

WGの今後の方向性の議論では、NANOGやAPRICOT2006といったオペレータミーティングでの議論もかんがみ、このまま標準化を進めるのでなく、一度ExperimentalとしてRFC化し、実装からのフィードバックを得、機能の追加を図った上で再度標準化を開始してはどうか、という提案があり、これに対して多くの議論が実施されました。標準の肥大化を懸念する意見や、これ以上の機能追加には反対する意見が多く出されましたが、議論の途中で時間切れになり、shim6 WGについての明確な方向性は決まりませんでした。今後、継続的に議論されることになりそうです。

□shim6 WG
http://www.ietf.org/html.charters/shim6-charter.html
□第66回 IETF shim6 WG ミーティングのアジェンダ
http://www.ietf.org/proceedings/06jul/agenda/shim6.txt

◆intarea meeting (Internet Area Open Meeting)

Internetエリアの各WGのトピックの紹介や、どのWGにも属さないトピック、またエリア全体のトピック等が扱われるInternetエリアのオープンミーティングで、IPv6のアドレス選択を定義している、RFC3484の改版に関する議論が実施されました。

RFC3484では、ノードが複数の始点・終点アドレスを持つ場合に、通信を開始する際に単一ペアの始点・終点アドレスを選択するアルゴリズムを定義してます。現在提案されているRFC3484の改版提案は、ノードが複数の始点アドレスを持つ場合に、過去の通信失敗履歴等を利用することで、自動的に通信相手に応じて動的に始点アドレスの利用可否を判定するようにする、となっています。これに対し、通信の成否が判定できるのはTCPのようなプロトコルのみであり、一般的にするのは困難、有用だが既存実装へのインパクトが大きい、などの意見が出されました。改版の方向性が決まるのには、もう少々時間がかかりそうです。

□第66回 IETF intarea ミーティングのアジェンダ
http://www.ietf.org/proceedings/06jul/agenda/intarea.txt

◆その他 ipv6関連事項

その他、IETF66の会期中に、エンドサイトへのIPv6アドレス割り当てサイズの推奨値を記述しているRFC3177の改版について、ipv6 WGのMLに投稿されました(ipv6 WGは、第64回IETFにてface-to-faceミーティングを終了しましたが、IETFのWGとしては存在しており、MLも存続しております)。v6ops WGでも、IPv6の経路制御に関するガイドラインの議論で話題になっています。

この議論は第63回IETFに始まっています。RFC3177ではIPv6アドレスのエンドユーザー割り当てサイズとして、統一的に/48が推奨されています。この/48という値は、ユーザー毎に約65,000個のサブネットを構築できるものですが、SOHOや家庭向けには大きすぎて無駄である、という意見のもとに、文書の改版が進んでいるものです。

今回投稿された案では推奨サイズに関する記述を削っていますが、この変更に賛成する意見がある一方、固定サイズを明記すべきだ、/48をやめるべきではない、といった元のRFCを支持する意見もあり、議論が続いています。

IETFは技術的な内容のみを扱うべきで、アドレスの割り当てサイズに関するルールはRIR(地域インターネットレジストリ)で扱うべきである、という意見も多く、実際に各RIRでアドレス割り当てサイズの検討が進んでいます。

第66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。

□第66回IETF全体プログラム
https://datatracker.ietf.org/public/meeting_agenda_html.cgi?meeting_num=66
□第66回IETFWGアジェンダ、発表資料
https://datatracker.ietf.org/public/meeting_materials.cgi?meeting_num=66
□第66回IETF 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)

■ENUM関連WG報告

本稿では、第66回IETFでのENUMワーキンググループ(以下、WG)の動向についてレポートします。

◆ENUM (tElephone Number Mapping) WG

本WGは、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について標準を定めたり、運用手続きの様々な側面を調べてドキュメント化することが目的となっています。

ミーティングでは、まず議題を確認した後、各インターネットドラフトについてレビューが行われました。

最初のレビューとして、ENUMに必要なEDNS0(Extension Mechanisms for DNS)※1について話し合いが行われ、RFC3761にEDNS0のサポートを追加するドラフトについて、WGラストコールをかけることが合意されました。

次に、ここ数回にわたりWGでの議論対象となってきた、ENUMの実装時の問題と経験を記したドラフトについて議論が行われましたが、コンセンサスが得られなかったため、Chair及び著者とでドラフトを検討した上でWGに報告することとなりました。

※1 EDNS0 (Extension Mechanisms for DNS, RFC2671)
http://tools.ietf.org/html/rfc2671.txt
http://www.nic.ad.jp/ja/translation/rfc/2671.html (日本語翻訳版)

その後、ENUMサービス関連ドラフトのレビューが行われ、vCardを登録する提案についてはラストコールがかかることになりました。その他のENUMサービス関連ドラフトについては、追加のレビューが必要ということで保留となっています。

VoIP相互接続およびNGN関連などで関心が高まっている、インフラストラクチャENUM(キャリアENUM)※2については、ドラフトが三つ議論されました。

1点目として、インフラストラクチャENUMにおいて、プライバシーの問題から事業者が保有している番号などの内容を極力外部に知られたくないという動機を満足させるために、ENUMを利用する際に外部からは見えない事業者のグループに割り当てられたE.164 Resolution Namespace (ERN, E.164名前解決用名前空間)を返すようにするというものです。ERNとしてはプライベートENUMに紐付けられた名前が想定されていますが、具体的にどのような問い合わせ方法を用いるかという点には言及されていません。ERNはENUMサービスの一つとして登録されることになります。

2〜3点目として、以前から議論になっている、ユーザENUMとインフラストラクチャENUMを並存させる方法ですが、以下の二つの案／ドラフトが提案されました。

1. 国別コードの上位レベルにインフラストラクチャENUM用のドメイン名ツリーとしてie164.arpaを導入する。
2. 従来の国別コードの下にサブドメイン (サブドメイン名はinfrastructure)を作り、インフラストラクチャENUMであることを示すEBL (ENUM Branch Location Record、IETF65ではBLRと略していたようです) という新しいDNSリソースレコード (RR)を導入する。

これらは前回のIETF65の直後にMLに提出された、いわゆる「ダラス協定(Dallas Treaty)」を受けてのものです。ダラス協定はユーザENUMとインフラストラクチャENUM(キャリアENUM)を並存させる方法をできるだけ速やかに決めようというもので、できるだけ早く暫定的な解決策を使えるようにすることと並行して、長期的な解決策も提案することを目指しています。

最後に、Chairの一人であるPatrik Faltstrom氏よりRFC3761bis(改良版)へ向けて、次世代ENUMについてのアイデアが紹介されました。現在はNAPTRレコードを検索すると、対象ドメイン名に紐付けられているすべてのURIが返って来るのに対し、以下の2点に分離することが提案内容となっています。

1. あるドメイン名にどんなサービスが存在するか
2. ある特定のサービスについて、どのURIを使うか

具体的には、DNSに登録するリソースレコードとして現在使用しているNAPTRレコードではなくURIレコードを使うことを想定しています。現在すでに使われているシステムとの後方互換性を妨げるものではないということでしたが、具体的な互換性実現のための方策についてまでは議論されませんでした。この紹介についての反応は、好意的なものが多かったように思います。

□ENUM WG
http://www.ietf.org/html.charters/enum-charter.html
□第66回IETF ENUM WGミーティングのアジェンダ
http://tools.ietf.org/wg/enum/agenda66.txt
http://www3.ietf.org/proceedings/06jul/agenda/enum.txt
□JPNICのENUM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)

■セキュリティ関連WG報告

第66回IETFでは、セキュリティエリアのセッションが18行われました。BoFはNetwork Endpoint Assessment BoF※3とHandover and Application Keyingand Pre-authentication BoF※4の二つでした。またPKIX WGと前回WGになったSIDR WGとのジョイントセッションが行われました。

本稿では、PKIX WGとSIDR WG、及びインターネットの経路制御における電子証明書の動向について報告いたします。

◆SIDR WG (Secure Inter-Domain Routing WG)

第64回および第65回のIETFでBoFが開かれていたSIDRが、2006年4月18日にWGになりました。今回のIETFで行われるミーティングがWGとして行われる初めてのミーティングです。

※2 インフラストラクチャENUM(キャリアENUM)
ENUMを用いて電話網の経路制御を行う技術。主に番号ポータビリティやIP電話の相互接続への利用が考えられています。

※3 Network Endpoint Assessment (NEA) (Proposed NEA WG Charter)
http://www3.ietf.org/proceedings/06jul/agenda/nea.txt
NEAは、ネットワークに接続するエンドポイント(ホスト等)のOSやパッチの適用状況に関する情報(posture)を交換し、エンドポイントの安全性が確認された場合にのみ会社のネットワークへの接続を許可するといった仕組み構築のために利用できます。

※4 Handover and Application Keying and Pre-authentication (HOAKEY)
モバイルネットワークにおけるハンドオーバーのための、認証情報を交換する仕組みに関するBoFです。第65回IETFに続いて2回目です。

SIDRはSecure Inter-Domain Routingの略で、ネットワーク・ドメイン間の経路制御におけるセキュリティメカニズムを開発することを目標としています。具体的には、暗号技術を使ってBGP(Border Gateway Protocol)メッセージの認証を行うための仕組みの実現や、BGPで使われるTCPコネクションを保護するための仕組みの改良に取り組んでいます。

RPSEC WGで議論されてきたセキュリティの要件にのっとり、利用や展開(deployment)を含めて検討を行います。

今回のWGセッションでは、はじめにIPアドレスやAS番号が入った“リソース証明書”の実験を行っているAPNICのGeoff Huston、George Michaelson両氏による、二つのドキュメントプレゼンテーションが行われました。また経路制御プロトコルをより安全に利用するためのトランスポート層(TCP)のセキュリティに関するドキュメントプレゼンテーションが行われました。

リソース証明書に関するプレゼンテーションは以下の二つです。

“A Profile for X.509 PKIX Resource Certificates”
draft-huston-sidr-res-certs-01.txt

（IPアドレスとAS番号の利用権を検証するための電子証明書のプロファイルを定めたもの。この証明書はリソース証明書と呼ばれる。）

“A Profile for Resource Certificate Repository Structure”
draft-huston-sidr-repos-struct-00.txt

（リソース証明書を保持するリポジトリの構造を定めたもの。Subject Key Identifier(SKI)やAuthority Key Identifier(AKI)を使って電子証明書を検索できるようにするため、Subjectにそれらのハッシュ値を含めた名前を使う。）

APNICではRFC化に先立ち、これらの仕様を前提として実装を進めているようです。主な論点は、リソース証明書のSubjectとトラストポイント(信頼点)の二つです。SKIのハッシュ値をSubjectに含めるのは、リソース証明書の証明書パスにおける一意性を維持することを意図しています。本来、Subjectは電子証明書の発行対象の識別子を入れるために使われますが、証明書を識別しやすくするために特殊な使われ方がされているようです。

またリソース証明書に想定されるツリー構造の頂点をどうするか、トラストポイントをどう想定するか、といった点については議論が収束していない様子です。IPアドレスとAS番号の管理を行っているインターネットレジストリの構造からすると、IANAが頂点となる認証局を運用し、RIRの認証局がその下位認証局となって、IANAの認証局を多くの利用者がトラストポイントと位置づけることが考えられます。しかしRIRの中にはその認証局の運用可能性に疑問を持っているところが多いようです。

技術の標準化の観点では、絶対的な頂点の存在を決めることよりもRelying Party(証明書検証者)が、必要十分なリソース証明書の検証ができるか、という点が重要です。そのため、頂点の認証局については、今のところは先に延ばせる議論ではあります。

トランスポート層のセキュリティについては右記のドキュメントに関するプレゼンテーションが行われました。

“Key Change Strategies for TCP-MD5”
draft-bellovin-keyroll2385-00.txt

（BGPのような長期的なTCPセッションにおける、MD5オプションのための鍵変更の方式です。既存の方式と互換性がありながら、片方のエンドだけで実施できるようになっています。）

“Authentication for TCP-based Routing and Management Protocols”
draft-bonica-tcp-auth-04.txt

（MD5に代わる、より強度の高い暗号アルゴリズムを使ったTCPオプションの取り決めです。）

“Automated key selection extension for the TCP Authentication Option”
draft-weis-tcp-auth-auto-ks-01.txt

（TCPのExtended Authenticationオプションのためのセッションキーの交換方式と、そのためのノンス(暗号文を変化させるためのランダム値)を使ったメッセージ認証の方式の取り決めです。）

“The TCP Simple Authentication Option”
draft-touch-tcpm-tcp-simple-auth-01.txt

（MD5オプションに代わる認証のためのTCPオプションです。IPsecのように別途のSA (Security Association)を確立する方式を提案しています。）

TCPにおける認証方式の改善は、強度と運用の容易さ、既存のTCPとの互換性といった様々な要素が関係しています。ネットワーク・セキュリティの大家であるSteven Bellovin氏を中心に慎重に検討が進められているようです。

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

PKIX WGは7月10日(月)の17時40分～21時に行われました。18時50分からはSIDR WGとのジョイントミーティングです。約50名の参加がありました。

第65回IETF(2006年3月)以降、AC Policies Extension (RFC4476)とGOST Cryptographic Algorithms(RFC4491)の二つがRFCになりました。RFC3280の部分的な変更であるDirectoryStringのUTF-8の処理に関するドキュメントは、RFC3280の改定作業とは独立して、RFC Editor's queueに入っており、RFCになる直前の段階にあります。(2006年8月、RFC4630となりました)

SIM(Subject Identification Method)、SCVP(Server-based Certificate Validation Protocol)、Lightweight OCSPの三つがWG Last Callを終え、Area Directorのレビュー中です(9月14日現在、SIMはIESGレビューを終え、RFC Editor's queueに入っています)。SCVPのSは以前Simpleでしたが、Server-basedに変わりました。

SIMは元々韓国のJong-Wook氏から出されたドキュメントでしたが、Tim Polk氏が引き継ぎ、現在IESGからのコメントに対応中です。SCVPは27版になり、いよいよIESGによるレビューの段階に入りました。前回のIETF以降、編集上の変更や定義づけに関する追記といった比較的軽微な変更がなされた模様です。

Lightweight OCSPは、オンラインで証明書検証処理を依頼するためのプロトコルのOCSPを改良したものです。大量のやりとりに適するよう、メッセージサイズを小さくしたり、返答結果のキャッシングを行うことができるようになっています。

X.509v3形式の電子証明書の基本的なプロファイルを記述したRFC3280の後継となるドキュメント、通称3280bisについてはnameConstraintsフィールドのエンコーディングに関する追記が行われています。またCRL Distribution PointsやAIA(Authority Information Access)/SIA(Subject Information Access)といったフィールドで、httpsを使用することに関する注意事項の追記が行われました。電子証明書の検証のためにhttpsが使われると、その処理のために更に電子証明書の検証が必要になり、場合によっては本来の検証処理が終わらなかったり、状態が複雑になりすぎたりします。これを避けるための注意喚起のための追記が行われたようです。他にも議論が収束していない点が残っていますが、部分的にドキュメントを分割して、3280bisの対象外とするなどして整理を進める模様です。

◆Joint PKIX/SIDR Meeting

PKIX WGの2セッション目に、PKIX WGとSIDR WGのジョイントミーティングが行われました。内容はSecure BGP(S-BGP)の提案者であるStephen Kent氏による“A PKI for Internet Address Space”というプレゼンテーションです。PKIX WGの参加者に加えて、SIDR WGのチェアであるSandra Murphy氏らが加わった形で意見交換が行われました。

Stephen Kent氏は、IPアドレスとAS番号の使用権を示す電子証明書を使ってインターネットのルーティングプロトコルであるBGPの安全性の向上を図る仕組み“S-BGP”の提案をしています。これは、RFC3779に記述されている電子証明書の拡張フィールドを使ってIPアドレスの割り振りとAS番号の割り当てを証明し、経路情報として広告されたprefixが、所有者(利用者)によって正しく使われていることを検証できるようにする仕組みです。インターネットにおける経路情報の中で、誤ったIPアドレスとAS番号が使われると、経路ハイジャックと呼ばれる大規模な利用不能攻撃が可能になります。S-BGPがうまく利用されると、このような攻撃を未然に防ぐことができると考えられています。

このセッションでは、RIRが運営する認証局を使ってこの電子証明書の発行を行う概念モデルが紹介されました。電子証明書の入手にはrsyncが使われることとなっています。

□ rsync
http://rsync.samba.org/

ここでもトラストポイントに関する議論が行われました。APNICやRIPE NCCからの参加者の間では、RIRが運用する認証局がトラストポイントとなることを想定して議論が行われています。しかし本来、トラストポイントとはプロトコルの提案者が決めるものではなく、電子証明書の検証を行う者(Relying Party)が決めるものです。Address Space PKIの構造に含まれるとされるJPNICでも、トラストポイントとして利用されることを想定した認証局を運用していることから、筆者はRIRの認証局だけがトラストポイントになるわけではないことを会場で確認しました。これは、例えば日本国内のISPの間で経路情報の交換を行う場合に、APNICやRIPE NCCの認証局を利用する必要はないと考えられるためです。

会場では、この他に割り振りを受けたアドレスブロックを使ったまま地域を移動し、割り振り元を別のRIRに変更するケースの扱い方などについて議論が行われました。

◇　　◇　　◇

IETFの会場でAPNICの方々と情報交換することでわかってきたことですが、APNICでは、Address Space PKIに関する開発プロジェクトが2006年末の終了を目標として進んでいるようです。既にIPアドレスとAS番号が入った電子証明書の発行やリポジトリの設置が実験的に行われていました。今後、MyAPNICという申請業務用のWebシステムに組み込まれることが考えられており、実用化に向けた活動が今後も引き続いて行われていくことが考えられます。

(JPNIC 技術部 木村泰司)

Whoisを巡る最近の議論について

P.66「インターネット10分講座：WHOIS」

Whois（「ふーいず」と読みます）とは、ドメイン名やIPアドレスなど、いわゆるインターネット名前・番号資源の登録関連情報を、インターネット内で閲覧可能とするために、インターネットの初期から採用されていた仕組みです。UNIX系のコンピュータではwhoisというコマンドを使ってこれらの情報を閲覧することができますが、最近ではドメイン名登録機関のWebページにwhois情報を検索するための入力用窓が設けられていて、whoisコマンドを使わなくてもwhois情報を見ることができるようになっている場合が多くあります。

Whoisは、インターネット上で技術的なトラブルが発生した場合に、トラブル発生元の担当者を調べ、その人への連絡方法を知るために利用できます。“whois”（「誰が」）という名前はこれに由来します。このような使い方がwhoisの当初の設計意図であったと思われ、実際インターネットが研究者間のネットワークであった十数年前には、「whois情報はネットワークの管理目的にのみ使用すること」というような簡単な約束でさほどの問題も生じませんでした。しかし、インターネットの発展に伴い、いろいろな問題が生じてきました。ひとつはwhois情報がダイレクトメールや迷惑メールに利用され、プライバシーの侵害とも言える事態を生じたことです。他方では、消費者を騙すなどの悪徳サイトが出現すると、その運営者を特定するために役立つという面も出てきました。そのほか、いわゆるサイバースクワッターを特定するためにも有効利用されてきました。さらに、whois情報の中にはかなりの虚偽が含まれているという点も指摘されました。このようにwhois情報提供の功罪がいろいろ出てきたため、ICANNではgTLDにおけるwhois情報の在り方についての議論が数年前から始められました。

ICANNでは当初、これまでwhoisで提供されている情報のうち、どれをどのように表示するか、という議論に多くの時間をかけましたが、堂々巡りの議論で決着がつきませんでした。その経過を簡単に総括しますと、プライバシー保護を重視する立場と情報公開を重視する立場の間で、「表示の方法」という表面的な問題だけを話し合っても妥協点は見つからなかった、と言えるでしょう。このため、2005年中頃になり、「whoisの目的は何か」という根本問題に戻って議論をやり直そう、という機運が出てきました。数か月の議論の後、これについて二つの定式化が候補として示されました。

1. DNSデータの設定にかかわる諸問題を解決できる人(組織)に連絡を取るために充分な情報を提供する
2. 当該ドメイン名の登録と使用にかかわる諸問題を解決できる人(組織)に連絡を取るために充分な情報を提供する

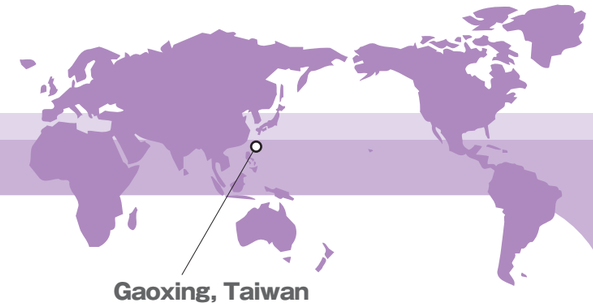
1の方が2に比べて提供される情報量は少なくなると考えられ、従ってプライバシー保護に対してはより配慮したものになることが予想されますが、1では当該ドメイン名登録が引き起こす社会的な問題に対しては配慮しないということになると思われます。また、ドメイン名のレジストラはICANNとの契約により自己の顧客情報をデータとして第三者に有料で提供する（「バルクアクセス」という）ことが禁止されておらず、従って1の方が営業上有利だという事情があります。

GNSO評議会の中でも1と2は支持が拮抗していましたが、結局2006年4月12日の投票により1を採択しました。ところが、これに対してはGAC(政府諮問委員会)を中心として異論が噴出しました。犯罪捜査や消費者保護の観点から、1では困る、という主張です。これを受けて、GNSO評議会は「これはあくまでも登録情報の一部を一般へ情報公開する目的であって、登録者から情報を収集する目的ではない。法律上の要請や知的財産権保護の必要による場合には非公開情報でも適切な閲覧者に提供する」との補足的な説明を行いましたが、いかにも後付で歯切れが悪いものでした。さらに「登録機関が登録者から収集する個人情報については、その目的や利用方法などに関して別途検討する」という決定を行って、事態の進展を図っています。

このように、プライバシー保護と情報公開という二つの価値観の間でwhoisに関する混沌とした議論が続いていますが、2006年6月30日にマラケシュで開催された理事会では、「理事会が2007年の早い時期に検討できるようにwhoisに関する提案事項を纏めることをGNSOに求める」と決議されました。理事会が設定したこの期限に向けてどのように議論を進めて行くのか、注目されるところです。

(JPNIC インターネットガバナンス・DRP分野担当理事 丸山直昌)

Internet Topics
インターネット・トピックス



2006.9.4→9.8
第22回APNICオープンポリシーミーティングレポート

このたび、2006年9月4日(月)～9月8日(金)、台湾第2の都市として知られている高雄で開催された第22回APNICオープンポリシーミーティングへ参加してきました。

JPNICからの参加は私を含めた職員4名と、APNIC EC(理事)でもあるIP分野担当理事の前村昌紀というメンバーです。

高雄は南部の工業都市でもあるそうですが、街の西側を流れている愛河の周辺には小さなカフェやバーが立ち並び、街全体はのんびりしている印象を受けました。

ミーティング会場であったGrand Hi-Lai Hotelは漢神デパートと隣接した街の中心にあり、参加者からの評判もよかったようです。本稿ではこのような環境で開催されたAPNIC22の様子をお伝えします。

■ミーティング概要

開催期間：2006年9月4日(月)～9月8日(金)
会場：台湾　高雄　GRAND HI-LAI HOTEL
参加者：157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/22/program/

※ 台湾のNIRであるTWNICがローカルホストを務めました。

■ミーティング全体について

今回のミーティングは、少なくとも私が参加した中では内容の濃さにおいてトップ3に入るミーティングだったのではないかと感じています。

まず1点目としては、これまでのAPNICオープンポリシーミーティングはどちらかといえばポリシー議論が中心という傾向がありましたが、今回はオペレーションに関する話題が随分充実したミーティングでした。

今回初の試みとして、従来BoFセッションとして開催してきたAPOPSに水曜日のセッション枠を終日割り当て、運用に関する議論・情報共有が集中して行われました。内容も、12点の発表のうち、バングラデシュ、中国、台湾、フィリピン等、地域内の運用状況の紹介や、BotNet、DoS攻撃への対策、RIRによる電子証明書の実装等、多岐にわたるトピックスが取り挙げられ、個人的にはBoTNetとAS-pathの分析の話が興味を引かれました。

また、ポリシーSIGにおいても提案事項が9点提出され、これは過去で最多の提案数とのことです。しかしながら、提案数が多い状況にもかかわらず、議論はさほど発散せず、また、IPv6アドレスポリシーについては日本のコミュニティからいただいていた意見をスムーズに通すことができて胸をなでおろしています。

それから、過去数回にわたって議論を続けているAPNICの料金体系の見直しについては、今回のミーティングにおいても、APNICから提示された案を基に引き続き議論が行われました。現時点ではまだ新料金体系についての結論は出ていませんが、TWNICのCEO、Ching-Ming Liang氏がFEE-WGのチェアを務め、引き続きメーリングリストで議論を行うことになっています。

そして、特にAPOPSセッションにおいては、これまでの発表者を常連が占めていた状態と比べて、初の発表者が多く見受けられたことが新鮮でした。今後、APNICオープンポリシーミーティングの構成がどのように変わっていくのかはまだわかりませんが、今回のようにオペレーショナルな話題も多く盛り込むことによって、参加者層が広がっていくとよいのではないかと考えます。

■提案事項の結果

[コンセンサスの得られた提案]
prop-033-v001　IPv6における割り当てポリシーの変更について
prop-035-v001　マルチホームネットワークへのIPv6 PIアドレスの新設について
prop-038-v001　機能しない逆引きDNSに関するAPNICポリシーの変更について


2006年9月7日に行われたポリシーSIGの様子

prop-039-v001　IANAからの新たな割り振りアドレスの到達性向上に向けての提案
prop-041-v001　クリティカルインフラストラクチャに対するIPv6アドレスの割り当てについて

[コンセンサスの得られなかった提案]
prop-034-v001　エンドユーザーへのIPv6 PIアドレスの新設について
prop-036-v001　IPv6割り振り基準の変更について
prop-037-v001　APNICデータベースにおける電子メールによる情報更新の廃止について
prop-040-v001　非会員に対するAPNIC料金改訂の提案

■参考情報

APNIC22公式ページ
http://www.apnic.net/meetings/22/
提案事項一覧
http://www.apnic.net/docs/policy/proposals/

※ 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ご参照いただけます。

(JPNIC IP事業部 奥谷泉)

Internet Topics
インターネット・トピックス

2006.9.4→9.8 第22回APNICオープンポリシーミーティングレポート

IPv6における割り当てポリシーの変更について

本稿では、「IPv6における割り当てポリシーの変更について」の提案において、コンセンサスに至るまでの議論の内容をご紹介します。

これまでのIPv6ポリシーでは、エンドサイトへの割り当てサイズについては、基本的に一律/48として運用されていましたが、この提案は、割り当てサイズに柔軟性を持たせ、サイズの判断はLIRに一任することを明らかにしたものです。

・エンドサイトへの割り当てサイズ/48に限定せず、LIRの判断に委ねる。

・追加割り振りにおける利用率の計算は/48の割り当てではなく、/56ベースに変更する。

APNICのGeoff Huston氏、IIJのRandy Bush氏により提出されたこの提案は、上記の文面を文字通りに解釈すると、実質的な影響は無いと考えられます。

しかし、この提案に至るまでの過去1年間はIPv6においても効率的な分配が必要であるとの議論が展開されてきたため、これが施行された場合、今後IPv4と同じく、効率的な分配を目指した方向に進むのではないかとの懸念が国内の事業者から表明されていました。

もちろん、「効率的な分配」の考えは、それ自体決して悪いものではありませんが、IPv4と同じ程度に求められることになった場合、その膨大なアドレス空間によるIPv6特有のメリットが失われてしまいます。

実際、LIRの「判断」が完全にLIRに一任されるものなのか、それともIPv4におけるアサイメントウィンドウ内の割り当てと同じく、効率的な割り当てを考慮した上で判断することが求められるのかによって意味合いが異なってきます。

そして、もしも効率的な分配を意識した上での判断が求められる場合、現在/48ベースでサービスを提供している事業者に影響があることが確認されていました。これら事業者の中では/48での割り当ての継続が認められなかった場合、1,000万円以上の対応コストが発生する事業者も、複数存在することがJPNICの調査では明らかになっています。

一方、ここにあげた影響が無いことが確認された前提で、個人ユーザと法人ユーザへの割り当てサイズを分けることによるサービスの差別化、柔軟な割り当てサイズによる追加割り振り申請のタイミング調整等が、提案が施行された場合のメリットとしてあげられていました。

それでも一部の方からはどういう形であれ、提案の施行に反対とのご意見も表明されていましたが、

・/48は、1ノードに64ビット割り当てた場合、65,536個のサブネットを作れるほど大きなサイズであること。

・/48の割り当てについては、IPv6アドレスの施行時に、ある程度運用を進めてみてから再度割り当てサイズの見直しを行うことを前提に合意されたこと。

を考慮すると、既存の事業者への影響を及ぼさないこと、現在以上に審議が厳しくならないことが確認できれば、提案そのものに反対する強い理由は無いとJPNICは判断しました。

そして、この他国内からいただいたすべてのご意見は、JPNICのスタンスと異なるもの含めて、プレゼンテーションにまとめ、ミーティングで発表を行いました。また、国内からあげられた懸念についても、提案の施行によって影響されるものではないことを、公式なセッション場だけでなく、事前に個別に話し合ったときにも提案者に確認することができました。

既存のサービスには影響を及ぼさずに、事業者が希望すれば、/48より小さな割り当てについても選択の幅が広がったことを考えると妥当な結果だったのではないかと思います。

なお、大筋の方針について、ミーティングでの賛同は得られましたが、具体的な実装にあたっては

・割り当てサイズに関するガイドライン策定の必要性

・初回割り振り基準への影響

・データベース登録単位

などについて、APNICとも確認をとりながら今後明確にしていく予定です。

(JPNIC IP事業部 奥谷泉)

Internet Topics インターネット・トピックス

2006.9.4→9.8 第22回APNICオープンポリシーミーティングレポート

マルチホームネットワークへのIPv6 PIアドレスの新設について

本稿では「マルチホームネットワークへのIPv6 PIアドレスの新設について」の提案がコンセンサスに至るまでの議論と、APNICミーティングにおける結果を全体として振り返ってみたいと思います。

まず、「マルチホームネットワークへのIPv6 PIアドレスの新設について」の提案ですが、これは2005年12月に開催されたJPNICオープンポリシーミーティングでのコンセンサスをもとに、アジア太平洋地域全体におけるポリシーとして実を結んだものです。その後、APNICミーティングでのコンセンサスを目指して、NTTの外山勝保氏をチェアとした、9名のボランティアメンバーからなるIPv6 PIワーキンググループにて検討を進めてきました。

PIアドレスとは、LIRを介さずにRIR、またはNIRから直接エンドサイトに分配されるIPアドレスを指します。RIR/NIRからLIR、そして、LIRからエンドサイト、という流れで分配が行われている一般のIPアドレス管理構造とは異なり、グローバルな経路表の増加につながるという理由で、IPv4においては技術的な要件によって必要とされる一部の場合に限定して、分配が認められています。

IPv6においては、特に経路の集約がより重要な問題となることから、ポリシー策定当初、IPv6におけるPIアドレスは基本的に認められていませんでした。

しかし、IPv4と同じく、マルチホーム接続を行っているネットワークにおいてPIアドレスが認められない場合、そのネットワークはLIR管理下のアドレスのパンチングホール※1を行う以外に運用することができない状態になります。

IPv6 PIアドレスのニーズについては、2005年12月のJPNICオープンポリシーミーティングで確認されましたが、割り当て対象を検討するにあたっては、マルチホーム以外にも、純粋にISPとは独立したIPアドレスが欲しいとのニーズからPIアドレスの割り当てを希望する組織もあるのでは、との意見もありました。しかし、今回は対象を技術的な理由からLIR経由で分配されるPAアドレスでは対応できない、マルチホームネットワークに対象を絞りました。

この度のAPNICミーティングでは、国内のIPv6 PI WGにより策定された提案の他に、同様の趣旨で別途Jordi Palet氏より類似の提案が出されていました。しかし、こちらの提案については、提案の論旨が明確ではないこと、割り当てサイズが、最小割り振りサイズ(/32)と同一であるのは大きすぎることから、参加者からの支持は得られない結果となりました。

国内からの提案がアジア太平洋地域のコンセンサスを得ることができた要因としては、文書のみでは伝わりにくい点が多かったため、一部の参加者とは外山さんが個別に時間をとり、提案への趣旨を説明してきたことも大きいですが、ミーティング当日にも支持する意見が強かったことを考えると、提案内容が、経路増加の問題も意識していることを明確にしながらも、技術的に必要なケースについては認めるべきとした主張に説得力があったということができるのではないかと思います。

なお、ARIN地域においては既に2006年9月1日よりIPv6におけるPIアドレスの分配を開始しており、APNICが施行を正式に決定すれば、JPNICでも施行する方向で検討を進めています。

現在の状況についてですが、この提案も含め、この度のミーティングでコンセンサスの得られたすべての提案について、APNICのメーリングリストで、提案に対するコメントの最終的な募集を行っています。

もし提案内容、または結果についてご意見がありましたら、直接sig-policy@apnic.netで表明していただくことも可能ですし、国内におけるポリシーフォーラムであるip-usersメーリングリスト(ip-users@nic.ad.jp)でお聞かせいただければ、JPNICが代表してAPNICのメーリングリストで情報を共有いたします。

また、12月に開催予定のJPNICオープンポリシーミーティングでも、これら提案の国内での施行について、発表を予定しています。

最後に、ミーティング結果全般に関する感想としては、今回ご紹介した2点の提案の他にも、JANOG18での議論をベースにしたIANAからの新たな割り振りアドレスの到達性向上に向けての提案を含め、国内の意見が非常によく反映された結果となったミーティングだったと感じています。

もちろん、単純に日本の意見が通るのがよいということではありませんが、国内で議論を重ねた意見や提案が、アジア太平洋地域全体においても納得してもらえることができたということではあるのかもしれません。

今後も国内のポリシーフォーラムが地域全体におけるポリシー議論へも貢献できるよう、実際のサービスへの影響、そして、インターネット全体にとってもなにがよいのかのバランスを考慮しながら議論を進めていけるとよいのではないかと考えます。

(JPNIC IP事業部 奥谷泉)

※1 パンチングホール
ISPは通常、経路数増加防止のために個々のネットワークに分配を行ったIPアドレスブロックを集約し、まとまった単位でグローバルインターネットへの経路広告を行っています。
パンチングホールとは、主に冗長的なネットワーク構成実現を目的として、ISPがまとめて経路広告を行っているアドレスブロックの一部をより小さく区切り、自ISPあるいは他ISPから別途経路広告を行う手法です。
本来ひとつに集約して広告されていた経路がまた別の経路として広告されるため、パンチングホールはインターネット全体の経路数の増大につながると言われています。

Internet Topics インターネット・トピックス

2006.9.4→9.8 第22回APNICオープンポリシーミーティングレポート
技術関連セッションレポート

2006年9月6日(水)はプレナリー、APOPS、Lightning Talksと技術・運用に関するセッションが目白押しでした。まずはオープニングを飾るプレナリーについてお伝えします。

■プレナリー

プレナリーとは個々のセッションが始まる前に行われる全体会議のことです。基調講演はスポンサーでもある台湾最大の電気通信事業者、中華電信(Chunghwa Telecom)の副社長、Shyang-Yih Chen氏より台湾における業界の現状、現在進行中の国家プロジェクト、同社のインターネットサービスについて、NGN(Next Generation Network)に関する計画などの紹介がありました。その後、パネルセッションとしてIPv4の枯渇問題について吉田友哉氏(NTTコミュニケーションズ株式会社、JPNIC IPアドレス検討委員)および前村昌紀(JPNIC IP分野担当理事)およびGeoff Huston氏 (APNIC)より発表がありました。会場の入り口には英訳された当センターの報告書「IPv4アドレス枯渇に向けた提言」が積まれており、人気だったようです。

■APOPS

APOPS(The Asia Pacific OperatorS Forum)とは、APNICオープンポリシーミーティングに併設されるインターネットオペレーターのためのフォーラムです。毎週ML(apops@apops.net)に投稿される経路表についての統計レポートでお馴染みの方もいらっしゃるかもしれません。前回のAPNICオープンポリシーミーティング(APNIC 21)までは、BoFとして夕方1時間だけ開かれていたのが、今回はIPv6以外の技術的なセッションを全て引き受ける形となり、3日間のうちのほぼ1日を費やしての開催となりました。

APOPSではさまざまな分野にわたっての発表がありました。セキュリティ関連ではブロードバンド化に伴い迷惑メール送信元およびDDoS攻撃元となっているBotnetについて、実験環境にて実際に動作させてみた様子、作用メカニズムなどについて発表が行われました。また、DNS amplification attack(IPソースアドレス偽造およびパケット増幅によるDNSへのDoS)についての発表が行われました。いずれも日本からの参加者からの発表でした。

運用関連ではバングラデシュでの海底ケーブルへの接続による同国のISPの運用面での変化、BGP経路情報中のASパス分析結果の考察(Tier-1と呼ばれる大手ISPのステータスの確認、プライベートASの誤った広告、複数のASからの同じIPアドレスプレフィックスの広告、隣接しないASの繰り返し、X relationship(2個のASがお互いの経路を広告し合う、など)などがありました。

なお、従来の技術的なSIG(Special Interest Group)は消滅したわけではなく、メーリングリストも存続しており議題があればいつでも再開されるとのことです。最後に、APOPSに技術的な発表をほぼ集約させるという、新しいフォーマットについてチェアより会場に対して質問があり、過半数を上回る支持を得られたようです。

■Lightning Talks

APOPSの後、1時間ほどにわたってLightning Talks(稲妻のようにすばやい発表とでもいう意味なのでしょうか)が行われ、従来APOPSで発表されていたようなJANOGアップデートなどが議題となっていました。一つ一つのプレゼンテーションは10分以内で、内容はタイムリーなものという条件がつきました。何時間も掛けて準備するという性格のものではなく、会場に来てから比較的軽い話題を発表／共有したいという人のためという印象を受けました。事前にプレゼンテーション枠は全て埋まり、関心の高さを示していました。

■IPv6 Technical SIG

今回のAPNICミーティングで唯一開催された技術系のSIGです。IPv6の割り振り/割り当て統計情報、6Boneの終了、IPv6エンドサイトにおける複数プレフィックスの併用ツールの紹介(これはインターネットとキャリア閉域網の併用という日本で切実なニーズのため開発されたということでした)、日本および台湾それぞれの地域でのIPv6普及状況などが発表されました。

■参考情報

APNIC22公式ページ
http://www.apnic.net/meetings/22/

APOPS
http://www.apops.net/

特集「第22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/2006/vol387.html

特集「報告書『IPv4アドレス枯渇に向けた提言』の公開にあたって」
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2006/vol355.html

(JPNIC 技術部/インターネット推進部 山崎信)

Internet Topics インターネット・トピックス

2006.9.4→9.8 第22回APNICオープンポリシーミーティングレポート

APNICにおけるリソース証明書の動向

APNICではリソース証明書と呼ばれる電子証明書を発行する仕組みを作るプロジェクトが進んでいます。このプロジェクトは2006年4月頃から始まった1年間のプロジェクトで、2007年4月以降、APNIC会員に対する試験的なサービスを始めることを目標に進められています。

本稿では、リソース証明書の概要を紹介するとともに、第22回APNICミーティングの参加を通じてわかってきた、プロジェクトの考え方と状況についてご報告いたします。

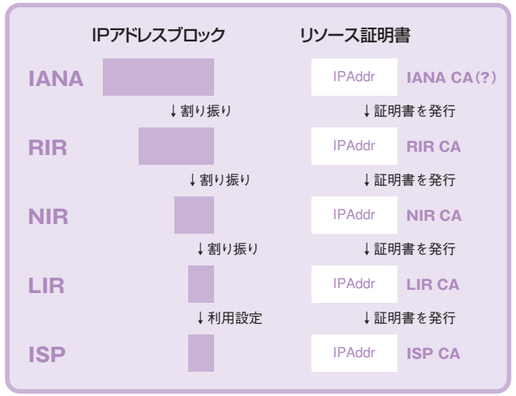
■リソース証明書とは

リソース証明書は、IPアドレスとAS番号の利用権利を示す電子証明書です。2004年6月に発行されたRFC3779※1でその構造が提案されました、インターネットレジストリのIPアドレスの割り振り構造と同じツリー構造でPKI(Public-Key Infrastructure)の認証局を構築することで、利用されているIPアドレスとAS番号の正当性を保証するための仕組みです。リソース証明書の構造を右図に示します。(わかりやすさのために一部単純化しています)

リソース証明書はアドレスの割り振り先に対して発行されます。証明書の発行元はCA(Certification Authority)と呼ばれています。割り振り先がさらに割り振りを行うとそこでもリソース証明書が発行されるので、割り振り先にはCAとしての証明書が発行されることになります。右の図のIANA CAの部分は現在の提案内容としては存在せず、RIRが頂点になる案が有力です。

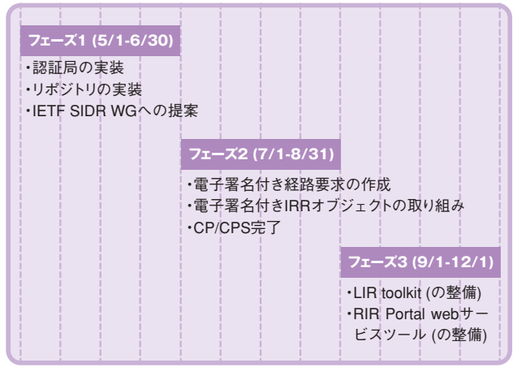
証明書の書式には基本的にX.509v3の形式が使われ、IPAddr(IPアドレス)やASIdentifier(AS番号)の値はX.509v3拡張フィールドと呼ばれる拡張の一つとして証明書の中に記載されます。発行元のリソース証明書は、発行先のリソース証明書に記載されるアドレスブロックを、内包するようなアドレスブロックが記載されます。

この証明書は、ルーティングのセキュリティとアドレス資源管理のセキュリティに役立つと考えられています。ルーティング・セキュリティのための応用として代表的なのがS-BGP※2です。S-BGPはBBNテクノロジー社のStephen Kent氏によって提案されたプロトコルで、ルーティングプロトコルのBGPを拡張し、ルータ間で交換される経路情報の正当性を電子的に確認できるようにするものです。



■APNICにおけるリソース証明書プロジェクトの進捗状況

APNICではリソース証明書について以下のスケジュールが立てられています。



フェーズ1は7月上旬に行われた第66回IETFに向けた活動、フェーズ2は9月上旬に行われた第22回APNICミーティングに向けた活動であることが読み取れます。認証局の実装はRIPE NCCと共同で開発が進められており、既にフェーズ1の“認証局の実装”と“リポジトリ”の実装が完了していることは、第66回IETFの会期中に行ったJPNICとAPNICの打ち合わせの際に確認されています。

第22回APNICミーティングでは、オペレーター向けのセッションであるAPOPSで、APNICのGeoff Huston氏によって進捗状況が報告されました。今回新しく発表があったのは以下の4点です。

a. APNICのWebポータルで証明書発行サービスを提供すること
b. LIRが証明書管理に利用できるツールの提供
c. IRRのrouteオブジェクトに対する電子署名
d. Webインターフェースを持つ電子署名ツール

aは、AP地域のコミュニティに対して情報提供することでフェーズ3で取り組むPortal webでの実装に関する意見集約を開始したものと考えられます。b、c、dについては実際の画面イメージが提示され、フェーズ2の実装が完了に近いことが示されました。ただし署名ツールの利用者をLIRの中のどの立場にするのか、その電子署名をどのように検証するのか、といった利用面での検討はまだ進んでいないようです。

※1 X.509 Extensions for IP Addresses and AS Identifiers
http://www.ietf.org/rfc/rfc3779.txt

※2 Secure BGP Project (S-BGP)
http://www.ir.bbn.com/projects/sbgp/

■リソース証明書にかかわる課題

リソース証明書の実装は、RIPE NCCとAPNICを中心に順調に進められているように見えます。しかしその背景には、証明書の発行だけでは解決できない大きな課題があります。筆者はその課題について第22回APNICのAPOPSのセッションで発表して参りましたので[※3]、その内容を通じて紹介いたします。

一つはリソース証明書に入るアドレスブロックが運用に適するように調節できない問題です。リソース証明書に入るアドレスブロックはアドレスの割り振り元によって決められます。しかしISPでは、割り振られたアドレスをさらに分割し、ネットワークの接続先に応じて伝達される経路情報を切り替えるような運用がしばしば行われます。従ってISPがリソース証明書に記載されるアドレスブロックをあらかじめ選択できるようにしておく必要があります。そうでないと、追加割り振りがあったような場合に、ルータに既に設定された多くの証明書を一斉に入れ替える必要が出てきてしまいます。また逆に接続先に対して不必要な経路の情報を、リソース証明書を通じて伝えてしまうことにもなりかねません。

もう一つはISPにおけるリソース証明書の管理の煩雑さです。リソース証明書が使われるようになると、ISPではルータと経路の管理の他にCAの管理を行う必要が出てきます。CAはCA自身の暗号鍵の管理や証明書の失効処理といった複雑な業務を必要とします。その上、アドレスの割り振りや返却といった処理はインターネットレジストリによって行われるため、ISPでその情報を基にした証明書管理を行うことは、一部を自動化したとしても煩雑なものになると考えられます。

これらの課題に対して、私はIRRと外部RA(Registration Authority)の二つを使う解決案のプレゼンテーションをいたしました。IRRはISPのルーティング・オペレーターによって登録情報の管理が行われています。IRRに登録されているrouteオブジェクトを使ってリソース証明書の発行が行うことができれば、経路制御のために都合のよい証明書の発行ができると考えられます。また外部RAと呼ばれている“証明書管理を行うユーザ”を設けることで、ISP自身が自分に発行される証明書の申請管理を行うことができ、また同時にISPでCAのシステムを持たなくてすみます。

これらの課題と解決策は証明書管理に限定されたものですが、S-BGPの利用にはさらに大きな課題があります。それはルータにおけるリソース証明書の扱いです。経路情報を交換するたびに電子証明書を検証していたのでは経路を確定するまでに時間がかかり過ぎてしまいます。またリソース証明書が完全に検証できなかったからといって接続を切ってしまうと、接続が切れやすいネットワークができてしまうかもしれません。リソース証明書の検証のタイミングや検証結果を経路情報にどのように反映すべきか、といった検討が必要です。

■リソース証明書の今後

第22回APNICミーティングの発表を見る限り、APNICにおけるプロジェクトは順調に進んでいます。このまま進んでいけばフェーズ3も無事終了し、2007年4月にはAPNICのWebポータルであるMyAPNICで試験的に利用できるようになる可能性があります。

一方、前述した課題をクリアするためには、インターネットレジストリとIRRの関係作りが重要になってくると考えられます。これまではIPアドレスの割り振り構造であるインターネットレジストリとルーティング・オペレーターの信頼構造の根拠となるIRRは分離しており、またそれが望ましいと考えられてきました。インターネットレジストリが経路制御に関与しないという歴史的な状況が守られてきた反面、ルータの設定における簡単なアドレスの打ち間違いが他のネットワークの接続性を失わせてしまったり、本来割り振られていないアドレスがIRRに登録されてしまい、アドレスが不正利用されてしまう可能性がある状況になっています。

多くのルーティング・オペレーターに使われているRADB[※4]は、ARINと運営組織が異なるだけでなく、インターネットレジストリと連動する仕組みを持っていません。ARINではPKIに関するワークショップを開くなどしていますが、リソース証明書の利用については未だ先が見えない状況です。

一方、RIPE NCCで運用されているRPSLベースのレジストリシステムはIRRとインターネットレジストリが連携する仕組みを持っているようです。RIPE NCCのレジストリシステムは、IRRを兼ねているだけでなく、LIRがrouteオブジェクトを登録できるユーザを限定する機能を持っています。詳細については、今後調査を進めていく予定ですが、リソース証明書の管理にこの仕組みが使われると前述の課題は解決し、ルーティング・オペレーターにとって使いやすいリソース証明書ができることになります。RIPE NCCの2006年度の活動計画にある電子証明書がどのような形で実装されていくのか、RIRの中で注目されると思われます。

(JPNIC 技術部/インターネット推進部 木村泰司)

※3 Route Origination Authorization (ROA) with IRR
http://www.apnic.net/meetings/22/program/apops-abstract.html#roa

※4 RADB
Meritという米国の研究機関によって運営されているpublicなインターネットルーティングレジストリ(IRR)の一つです。