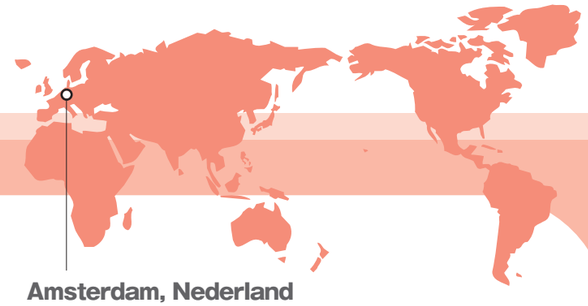


2006.10.2→10.6
第53回RIPEミーティング

2006年10月2日（月）から6日（金）まで、オランダ・アムステルダムにてRIPE53ミーティングが開催されました。当地はオランダの画家レンブラントの生誕400周年を祝し、さまざまな団体や美術館が記念イベントを開催していました。私自身は今回イベントを見学する時間が取れず少々残念です。

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。

■全体報告

◆アドレスポリシーWG

今回のアドレスポリシーWGでは、以下のポリシー提案が議論されました。

(1) IPv6における割り当てポリシーの変更について※1

エンドサイトへの割り当てサイズを/48に限定せずLIRの判断に委ねることと、追加割り振りの利用率計算を/48ベースではなく/56ベースで行うことという二つの要素からなる提案で、前回のAPNICミーティングで提案されたものと同じもの※2です。

会議では、本提案をベースに具体的なポリシー文書を作成する方向でコンセンサスとなり、今後ドラフトされた文書をもとにさらに議論が進められることとなりました。

(2) IPv6におけるPI（Provider Independent）アドレス割り当てについて※3

PIアドレスの割り当てが必要であることを示すことができるエンドサイトに対しては、RIPE NCCと契約書を締結することを条件に/32のPIアドレスの割り当てを行うことができるという提案です。

会議では、割り当てサイズが/32では大きすぎるのではないかという懸念が示され、メーリングリスト（ML）で継続議論することとなっています。

(3) IPv6における割り振りポリシーの変更について※4

初期割り振りの要件の1つである「2年間に少なくとも200の/48の割り当てを行う計画がある」という条件および、「エンドサイトへ/48を超える割り当てを行う際には、RIR/NIRへ割り当て審議申請を提出しなければならない」という条件を両方撤廃しようとする提案です。

Plenaryの模様

上記提案のうち前者の要素については、ARIN、LACNIC、AfriNICにおいては既に撤廃されており、提案理由の中でもそのことが述べられていますが、今回の会議においても結論は出ず、引き続きMLで議論することとなりました。

(4) データベースへ登録する連絡先e-mailアドレスについて※5

RIPE NCCのWHOISデータベースに登録するe-mailアドレスには、常に有効なものが記載されていなければならないとする提案です。

ある特定のIPアドレスに関して問い合わせを行った際、当該IPアドレスに関する連絡先としてWHOISデータベースに登録されていたe-mailアドレスが、機能していなかったことに端を発する提案のようですが、既にRIPE NCCの文書として「正しい情報を登録すること」がLIRには義務づけられており、そもそも本提案が問題の解決となるのかを疑問視する発言もありました。

結局この提案も、引き続きMLで議論されることとなりました。

(5) IPv4におけるPIアドレスの最小割り当てプリフィクスサイズについて※6

IPv4において、PIアドレスの最小割り当てプリフィクスサイズを/24に規定する提案です。具体的には例えば384個のIPアドレスを割り当てる必要がある際は、/24と/25を割り当てるのではなく、/23（/24を2個）を割り当てるべきとする提案です。

現在RIPE NCCにおけるアドレスポリシーでは、PIの割り当てに関して最小プリフィクスサイズを定めていません※7。ルーティングの観点から、/24より小さいプリフィクスはフィルタされる可能性が高いということが、本提案の背景にあることが説明されました。

これも会議での結論は出ず、MLで継続議論されることとなっています。

※1 Proposal to Amend the IPv6 Assignment and Utilisation Requirement Policy
http://www.ripe.net/ripe/policies/proposals/2005-08.html

※2 APNICでの提案の概要とその結果については、以下のURLを参照ください。
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2006/vol392.html

※3 Provider Independent（PI）IPv6 Assignments for End User Organisations
http://www.ripe.net/ripe/policies/proposals/2006-01.html

※4 IPv6 Address Allocation and Assignment Policy
http://www.ripe.net/ripe/policies/proposals/2006-02.html

※5 Contact e-mail Address Requirements
http://www.ripe.net/ripe/policies/proposals/2006-04.html

※6 PI Assignment Size
http://www.ripe.net/ripe/policies/proposals/2006-05.html

※7 APNICでも最小サイズは定められていません。
http://www.apnic.net/docs/policy/add-manage-policy.html#11.1

(6) IPv4における最大割り振り量について※8

現在RIPE NCCでは、LIRへの割り振り量を文書上で規定していませんが、実情としては「最大2年間の需要に対応できるだけのアドレス量を割り振る」運用がなされています。これを「最大1年間の需要に対応できるだけのアドレス量」に変更し、文書化しようという提案がRIPE NCC側からなされました。

当該期間は、APNICでは1年間※9、ARINでは3〜6か月、LACNICでは3か月とされており、RIPE NCCが2年分を割り振るとしているのは長すぎるのではないかということが提案の背景にあります。昨今各地で取り上げられているIPv4アドレスの枯渇に関する話題も関係すると思われます。

会議では、本提案に賛同する意見が複数表明されました。今後MLでさらに議論した後、ポリシー文書のドラフトがなされる見込みです。

(7) IPv4の最小アサインメントウィンドウ※10について

現在RIPE NCCにおける最小アサインメントウィンドウは0※11ですが、これを/21へ引き上げようという提案です。RIPE NCCでは自社インフラへの割り当てについてもアサインメントウィンドウを適用していますが、これを大幅に緩和するものです。

提案の背景としては、CIDRが普及してから相当の時間が経過し、また、トレーニングの成果としてLIR側も割り当てポリシーに慣熟してきたことが挙げられ、RIR側、LIR側双方にとってメリットがあるということが提案者であるRIPE NCCの審議担当者から説明されました。あわせて、審議の比重を割り当て時から、追加割り振り時に移す狙いも説明されました。

これに対し、LIR側からは「確かに双方にとってメリットはあるが、アドレスの無駄使いにつながる懸念は払拭できない」という意見が出され、コンセンサスには至らず、MLで継続議論されることになりました。

本提案は上記(6)の提案とセットで出された感がありますが、厳格化方向の(6)には強い反対意見は出なかった一方で、緩和方向の(7)に対し反対が表明されたのは興味深い動きでした。

◆その他のトピック - PIアドレス割り当て統計

プレナリーセッションにおいて、各RIRにおけるPIアドレス割り当ての統計が紹介※12されていましたので報告します。

これによると、2005年から2006年におけるPA（Provider Aggregatable）アドレス割り振りプリフィクス数と、PIアドレス割り当てプリフィクス数の比は、APNICが90：10、ARINが77：23であるのに対し、RIPE NCCではこの比が逆転し、41：59でPIのプリフィクス数の方が多いという結果になっています。

また、RIPE NCCでは2003年を境にPIプリフィクス数がPAのそれを逆転したことも示されています。これらの背景として、RIPE NCCではPIアドレスの割り当てを受けるのにマルチホームする必要が必ずしも無いこと、また、エンドユーザーとRIPE NCCが直接の契約関係を持つ必要がなく、接続LIRを通じた簡易な申請ができることなどがあると思われます。

しかしこの反面、エンドユーザーとRIPE NCCとの契約関係がないため、PIアドレスの割り当て先を正確に把握することが難しいという大きな問題がありますので、今後議論の対象になることは避けられないものと思われます。

◆おわりに

近年RIPE NCCでは大きなポリシー変更提案がなかったのですが、ここへ来てIPv4アドレス枯渇の進行、RIRにおけるアドレス認証局の実験開始などの動きと絡んだ提案、情報提供がされるようになってきました。今回最後にご紹介したPIアドレス割り当てに関する問題もその一環としての問題提起と捉えることもできるのではないでしょうか。

成熟した感のあるIPv4アドレスポリシーにも、今後変更の動きが徐々に出てくる可能性があります。IPv6アドレスポリシーについても同様です。各RIRでの議論を注視しつつ、今後も情報提供に努めたいと思います。

（JPNIC IP事業部　穂坂俊之）

※ 8 IPv4 Maximum Allocation Period
http://www.ripe.net/ripe/policies/proposals/2006-06.html

※ 9 JPNICでも1年間の需要に見合う量を割り振ると規定しています。
JPNICにおけるアドレス空間管理ポリシー（IPv4）
9.4 追加割り振りの基準
http://www.nic.ad.jp/doc/ip-addr-ipv4policy.html

※10 アサインメントウィンドウ
LIR（JPNICにおいてはIPアドレス管理指定事業者）が、RIR/NIRの審議を受けることなく自主的に割り当てることができる最大のアドレス空間です。

※11 Minimum IPv4 Assignment Window
http://www.ripe.net/ripe/policies/proposals/2006-07.html

※12 PI Statistics Update
http://www.ripe.net/ripe/meetings/ripe-53/presentations/rir_stats.pdf

■RIPE NCCにおけるデータベースのセキュリティ動向

インターネット推進部では、ルーティングのセキュリティ向上を視野に入れた登録情報の正当性とデータベースのあり方について調査研究を行っており、その一環としてRIRのデータベース動向を調査しています。今回は、RIPEミーティングに参加してセキュリティに関する議論の動向を調べるとともに、RIPE NCCのスタッフに、RIPEデータベースの仕組みや課題について話を伺ってまいりました。

本稿ではこれらを通じて見えてきたRIPEデータベースのセキュリティの動向について紹介いたします。

◇　　◇　　◇

第53回RIPEミーティングでは、初日に主にLIR向けのチュートリアルが行われ、初日から3日目にかけて全体会議であるPlenaryが行われました。3日目以降はWGのセッションが開かれました。ミーティングの参加登録者は355名で、ここ1年ではほぼ平均的な人数です。

セキュリティに関しては、全体会議であるPlenaryとNCC Services WGでリソース証明書に関する議論が、Database WGでIRTオブジェクトとCRYPT-PWを廃止する案についての議論が行われていました。これらの議論についてご紹介します。

◆リソース証明書に関して

リソース証明書については、Plenaryをはじめ複数のWGで議論が行われていました。リソース証明書はIPアドレスやAS番号が入った電子証明書※1で、WHOISの代わりにIPアドレスの割り振りや割り当てを証明するために使われます。IPアドレスの割り振り構造に従って発行され、そのツリー構造の末端部分ではIPアドレスとAS番号の両方が入った電子証明書が発行されます。この電子証明書はBGPなどにおける経路制御を安全にするために使われることが想定されています※2。リソース証明書の実装は、2006年4月頃よりAPNICとRIPE NCCが中心となって進められてきました。

Plenaryでは、APNICのGeoff Huston氏によって、リソース証明書を使ってIRRの登録情報に電子署名を行うデモが行われました。この電子署名はIRRのroute-setオブジェクトに対して行われるもので、そのroute-setオブジェクトに含まれるrouteオブジェクトがauthorize（認可）されたことを意味しています。routeオブジェクトには広告元（すなわちそのアドレスを持つノードの収容先）となるAS番号が記載されているため、LIRがそのASに対してインターネットでそのIPアドレスを使うことを認可した、という意味になります。この認可の概念はROA（Route Origination Authorization）と呼ばれています。インターネットレジストリの割り振りを意味するリソース証明書は2006年7月の時点で既に実装されていたので、このROAを示すリソース証明書の発行によって、ツリー構造の最上位から末端までのすべてのリソース証明書が発行できる状況になったことになります。

Plenaryの会場では、このプログラムが無事に動作したことに対して賞賛の拍手が送られる一方、リソース証明書の発行に使われるデータベースが信頼に足るかどうかという根本的な疑問が投げかけられていました。リソース証明書自体が信頼できる仕組みであっても、証明書の元になるデータが間違っていたら意味がないためです。RIPE NCCでは既にこの点に着目しており、リソース証明書の導入に関して、予測される効果やインパクトを評価する活動が提案されています。この活動はNCC Services WGで発表されていました。

2007年度のRIPE NCCの活動計画によると※3、RIPE NCCでは2006年度のAPNICの実装プロジェクトへの参加に引き続き、リソース証明書に着目した活動が行われていくとされています。NCC Services WGでのAxel Pawlik氏（RIPE NCC）の発表では、2007年度の本格的な活動に先立って、Evaluation Task Force（評価タスクフォース）の立ち上げが提案されていました。この評価は必要となる業務の詳細やポリシーへの影響を明らかにすることが目標になっています。Evaluation Task Forceは現行の開発活動やトライアルに参加しつつ、まずリソース証明書が持つ目標とその目標に現行のアプローチが適するかどうかを調査して報告することになっています。最終的には2007年5月に予定されている第55回RIPEミーティングで、導入の方向性について決定が行われることとなっています。

これは、これまで実装を行ってきたAPNICをはじめ、リソース証明書の効果に対して同様の疑問が投げかけられているARINコミュニティ、そして認証局に関する調査研究を行ってきた当センターにとっても注目に値する活動だと考えられます。というのも、RIPE NCCのデータベースはアドレスの割り振り／割り当て情報を登録するデータベースと経路に関する情報が登録されるIRRが統一されている上に、インターネットで経路広告されているアドレスとIRRの登録情報を比較する調査プロジェクトが行われてきているためです※4。これによって、RIPE NCCでは、登録されているにもかかわらず実際には使われていないアドレスを調べることができます。使われていないアドレスや登録情報と異なる経路広告の量がわかれば、リソース証明書が現状で何割程度のアドレスに対して発行できるのか、またそれらの管理が現実的なものなのかどうかがわかる可能性があります。

※1 RFC3779
http://www.ietf.org/rfc/rfc3779.txt

※2 Secure Border Gateway Protocol（S-BGP）
--- Real World Performance and Deployment Issues
http://www.ir.bbn.com/sbgp/NDSS00.S-BGP.ps

※3 New or Significantly Developed Activities for 2007
http://www.ripe.net/ripe/draft-documents/gm-october2006/ap-2007.html#3

※4 Routing Registry Consistency Check Project
https://www.ripe.net/projects/rrcc/

◆RIPEデータベースのセキュリティ機能に関して

RIPEデータベースには、ユーザーを認証したりユーザーが編集できる登録情報の範囲を限定するといったデータベースを保護する機能の他に、あるアドレスで起こったコンピュータインシデントに関する連絡先となるIRT（Incident Responce Team）の情報を提供するという、コミュニティのセキュリティを考慮した機能があります。

ここではRIPEミーティングの5日目に行われたDatabase WGの議論の中から、ユーザー認証の機能であるCRYPT-PWの廃止に関する提案と、IRT情報を提供するIRTオブジェクトに関する議論をご紹介します。

RIPEデータベースはLIRに対して四つの認証方式を提供しており、ユーザーは好きなものを選んで使用できるようになっています。現在提供されている認証方式は、CRYPT-PW、MD5-PW、PGP-KEY、X509で、CRYPT-PWとMD5-PWはいわゆるパスワード認証方式です。LIRがメールで申請業務を行う場合、送信するフォームの中であらかじめ登録されているパスワード文字列を記入します。パスワード文字列が正しければ、RIPEデータベースはユーザー本人によって送信されたと判断でき、申請内容のチェックに移ることができます。-PWの前についているCRYPTとMD5は、パスワード文字列をRIPEデータベースの中で処理する方式の名前です。CRYPTは昔のUNIXでパスワード文字列を隠蔽するために使われていた方式で、パスワードとして指定できる文字の長さは8文字です。一方、MD5はメッセージダイジェスト関数のMD5を用いた方式で、RIPEデータベースでは65文字のパスワードをつけることができます※5。

今回の提案は、CRYPT-PWで利用できる文字列が短いために、ブルートフォース攻撃（総当たり攻撃）や辞書攻撃といった基本的な攻撃が通用してしまうため、今後この方式の利用を廃止しようというものです。既に第52回RIPEミーティングで基本的な方針についてはコンセンサスが得られており、今後はスケジュールについて検討したいとのことでした。しかし、約2,300のメンテナーでCRYPT-PWが使われているそうで、完全な廃止にはやや時間がかかりそうです。また変更手続きが間に合わなかったユーザーへの対応なども検討する必要があると考えられます。

一方、IRTオブジェクトに関する議論は潜在的な問題を抱えたままの提案となりました。今回の提案はWHOISを使って、あるIPアドレスを元にinetnumオブジェクトが検索された場合、検索時のオプションに-cが指定されていなくてもWHOISのサーバは関連するIRTオブジェクトを返すというものです。このことでWHOISでIPアドレスを調べるだけでIRTオブジェクトが自動的に表示されるようになります。このことはユーザーの観点では便利になるという意味でとてもよいことです。またIRTオブジェクトは一旦一つのメンテナーに対して定義しておけば、そのメンテナーによって管理されている割り振り／割り当て情報のすべてに対して適用されるという意味で、LIRにとっても利便性は高いと言えます。そのためRIPE NCCではIRTオブジェクトの利用を推奨しています。

IRTオブジェクトの普及に関する潜在的な問題は、abuse-mailboxという類似した連絡先情報の存在です。abuse-mailboxはinetnumやinet6numといった個々の割り振り／割り当て情報に付加される情報で、そのアドレスブロックにおける abuse（不正や不具合に対する連絡）用のメールアドレスが記載されています。abuse-mailboxは2004年1月の第47回RIPEミーティングで採用されたもので、それ以降多くのinetnum/inet6numで登録されてきました。一方、IRTオブジェクトは100程度に留まっており、利用されているものは60程度に留まっているようです。しかし両者共に効果が見えにくいことなどから、議論の余地が大きいため、RIPEのコミュニティの中でも扱いにくい話題になっているようです。

◇　◇　◇

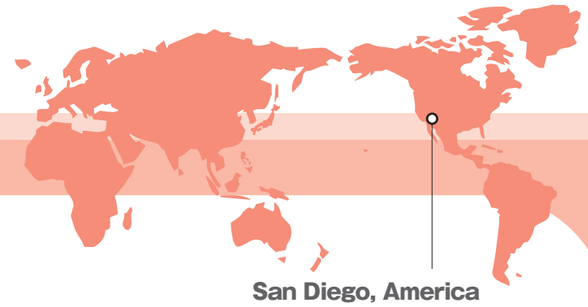
RIPE NCCでのヒアリングの結果、RIPEデータベースは、IPアドレスの割り振り／割り当て情報とIRRが統合されたシステムであるだけでなく、LIRがAS管理者に対して経路情報（routeオブジェクト）の登録認可する機構を備えていることがわかりました。この機構によって、IPアドレスの割り振り先とASの運用が別の組織によって行われていても、どのIPアドレスがどのASから経路広告されるのかが、絞り込めるようになっています。

他の組織によって間違った経路広告をされてしまうことで、本来は自分のネットワークで使われるべきIPアドレスが使えなくなってしまうことは“経路ハイジャック”と呼ばれています。これを検出し防止するためには、RIPEデータベースが持つ機構は有効です。この後の調査で、ARINのコミュニティでもIPアドレスとAS番号の組み合わせがわかる仕組みが提案されていることがわかりました。今後、機会がありましたらこれらの仕組みの違いや、JPNICでの取り組みについてご紹介したいと思います。

（JPNIC 技術部 木村泰司）

※5 Crypted password generation
https://www.ripe.net/cgi-bin/crypt.cgi

Internet Topics
インターネット・トピックス



2006.11.5→11.10
第67回IETF報告

■全体概要

◆概要

第67回IETFは2006年11月5日（日）～10日（金）、アメリカ・サンディエゴにあるSheraton San Diego Hotel & Marinaで開かれました。サンディエゴはアメリカ西海岸のカリフォルニア州の南部にある人口120万人程の都市で、南へ30km程行くとメキシコとの国境があります。町のすぐ近くにアメリカ海軍の基地があり、ダウンタウンから徒歩圏内にある海沿いのマリーナパークからは、湾内に軍艦が停泊している様子が見られます。

IETFが開かれたSheraton Hotelはダウンタウンから車で15分ほど離れた所にあります。サンディエゴ空港とヨットハーバーに隣接していて眺めは良いのですが、ショッピングセンターや飲食店はほとんどなく、また鉄道の駅が近くにありません。そのためか、IETF開催中の夕方頃から夜にかけて、会場の裏手とダウンタウンの中心地にあるGaslamp地区との間で、参加者のためにチャーターされたバスが臨時運行していました。

オンラインのサービスとしては、前回と同様にミーティング参加者向けのメーリングリストが提供されていました。さらに今回は参加者が情報交換を行うためのブログとWikiが設置されていました。メーリングリストではSheraton Hotelのゲストルームにあるインターネット接続機器の不具合や、会場の無線LANに関する情報交換が行われていました。

今回のIETFの参加登録者は1,199名で、41ヶ国からの参加がありました。日本からの参加者は全体の10%強で、55%近くを占めるアメリカに次いで2番目の参加者数です。全体の人数はここ3回程は大きな変化はないようです。

初日の11月5日（日）に各種チュートリアルとレセプションが、11月6日（月）～11月10日（金）にWGとBoFが、8日（水）と9日（木）の夜にPlenary（全体会議）が行われました。


Plenaryの模様

◆IETF Operations and Administration Plenary

IETF Operations and Administration Plenaryは、IETFの運営全般に関する報告と議論が行われる全体会議です。このPlenaryでは、NOC（Network Operation Center）リポートやホストプレゼンテーション、IETFチェアの報告などが行われました。

NOCリポートではIETF会場のネットワークの利用状況などについて報告されました。会場では毎回無線LANを使ったインターネットへの接続サービスが提供されており、最近では無線チャンネルの有効利用と効率化のために、802.11aの利用が推奨されています。IETF期間中に802.11aを利用していた端末は全体の25%程で、前回に比べて徐々にその数が増えつつあるようです。

IETFチェアのBrian Carpenter氏からは、IASA（IETF Administrative Support Activity）とIAD（IETF Adminstrative Director）の活動報告が行われました。前回の第66回IETF以降二つのWGが設立され、12のWGがクローズ、現在120程のWGが活動しているとのことです。RFCは99出され、新規のInternet-Draftは440程作成されたとのことです。ちなみに去年の同じ期間には100程度のRFCが出され、新しいInternet-Draftは435作成されていましたので、昨年と比べると若干少なかった模様です。

また今回はJon Postel賞の受賞者の発表がありました。Jon Postel賞はRFCの編纂やIANA（Internet Assigned Numbers Authority）としてIPアドレスの管理などに貢献したJonathan B. Postel氏にちなんで1999年に設けられたもので、技術的な貢献やリーダーシップの発揮といったコミュニティに対する継続的な貢献のあった人物に対して贈られます。受賞者は毎年選ばれ、クリスタルグローブと賞金2万ドルが贈られます。

今年の受賞者は、南カリフォルニア大学のISI（Information Sciences Institute）におけるRFC Editorのco-leaderであったJoyce K. Reynolds氏と、Bob Braden氏でした。Jon Postel氏より引き継いでRFCの編纂にあたり、RFCの品質向上や現在に至るRFCの認知度向上に対する貢献が称えられました。

□ Postel Awards
http://www.isoc.org/awards/

会場での参加者の発言に基づいて議論を行うオープンマイクの時間には、主にIETFで提供されてるツールに関して議論が行われていました。IETFによるツールの提供は、IETFの予算の中で行われているにも関わらず、開発の際に参加者が意見を出す機会が設けられていない、という指摘から議論が始まりました。これについて、オープンソースにすることでノウハウがたまりやすくなる（と同時に多くの人の考えを反映できる）、ツールの位置付けを知っているところでないと開発が難しいことから、事務局の契約が特定の会社に結びつきやすいのではないか、といった意見が挙げられていました。その他にIETFの音声中継は参加者でなくても聞くことができるが著作権の提示がないといった指摘が挙げられていました。この件についてはIPR（Intellectual Property Rights）WGで議論されていく模様です。

Internet Topics
インターネット・トピックス

□ IETF TOOLS
http://tools.ietf.org/

□ IPR（Intellectual Property Rights）WG
http://www.ietf.org/html.charters/ipr-charter.html

◆Technical Plenary

Technical Plenaryは、IETF全体に関係した技術に関する議論を行う全体会議です。IAB（Internet Architecture Board）のチェアレポート、IRTF（Internet Research Task Force）の活動報告、テクニカルプレゼンテーションなどが行われました。

IABのチェアレポートはIABチェアのLeslie Daigle氏によって行われました。IABではインターネットのアーキテクチャの観点で、WGとは独立したドキュメント作成を行っており、中にはRFCになっているものがあります。最近作成されたドキュメントは以下の三つです。

□ draft-iab-iwout-report-00.txt
"Report from the IAB workshop on Unwanted Traffic March 9-10, 2006"
（※2006年1月現在、draft-iab-iwout-report-01.txt が出ています）

□ draft-iab-multilink-subnet-issues-00.txt
"Multilink Subnet Issues"
（※2006年1月現在、draft-iab-multilink-subnet-issues-02.txtが出ています）

□ draft-iab-net-transparent-01.txt
"Reflections on Internet Transparency"

はじめのInternet-Draftは、2006年3月に行われた"IAB Unwanted Traffic Workshop"の報告です。Technical Plenaryの後半でサマリー報告も行われました。質疑応答の際のLeslie Daigle氏の補足によると、このワークショップは主に（コミュニティの）意識向上を図ることが目的であったようです。

インターネットの利用者に対する脅威はCode RedやBlasterワームが流行した2001年～2003年頃に比べて深刻になりつつあります。ワークショップでは"アンダーグランドエコノミーの発展"を主な要因と位置づけ、現状の問題を明文化して今後の活動の方向性を探るための議論が行われた模様です。

あるWebサイトではクレジットカード情報や銀行口座に加えて、ISPで稼動しているルータのアカウントやボットネットが売り買いされています。このような経済活動の結果、スパムメールやDDoS攻撃といった"Unwanted Traffic"を生み出す基盤が維持され、またマルウェア（不正な挙動をするソフトウェア）の発達を促すような競争が行われている、と言われています。一方でさまざまなデータが全てHTTPの中でやりとりされていたり不正行為を隠すためのIPアドレスの詐称や、インターネットの経路広告の交換をハイジャックできてしまうことなど、"Unwanted Traffic"を止められない現状が指摘されています。

これに対して、中長期的な対策と短期的にできる活動が挙げられていました。中長期的には、まずルーティングのセキュリティ向上を図る点が挙げられていました。そのため、IRR（Internet Routing Registry）の登録情報をクリーンアップして、経路情報の検証ができるようにすることが必要だと指摘されていました。次にボットネットを止めること、そしてTCPのMD5オプションやパケットフィルタリングのBCP（Best Current Practice）といった既存の技術の普及を図ること、といった提案がなされていました。

短期的にできることとしては、既にRFCになっているhost requirement、route requirement、ingress filteringに関するドキュメントを更新することや、IABによる啓発活動、IRTFにおける効果的な対策に関する調査などが挙げられていました。Security Area DirectorのSam Hartman氏によると、このワークショップのリポートは興味深く、一読することが薦められていました。

□"Report from the IAB workshop on Unwanted Traffic March 9-10, 2006"
http://www.ietf.org/internet-drafts/draft-iab-iwout-report-00.txt
（※2006年1月現在、draft-iab-iwout-report-01.txtが出ています）

Technical Plenaryの後半では、IABのInternet-Draftである"Reflections on Internet Transparency"とIAB Routing and Addressing Workshopの報告が行われました。

□ Reflections on Internet Transparency
http://www.ietf.org/internet-drafts/draft-iab-net-transparent-01.txt

このドキュメントはインターネットの原則的な考え方である「透過性」に関するもので、これまでのIABの見解を見直し、新たな透過性の考え方に関する議論を紹介したものです。プレゼンテーションでは、TCP/IPの階層モデルの中で、さまざまなプロトコルが透過性に影響する要素を持っているという点が紹介されていました。

IAB Routing and Addressing Workshopは、2006年10月18日にオランダのアムステルダムで開かれたもので、近年の経路情報の増大にどのように対処すべきかについて、主にバックボーンオペレーターを対象として行われたものです。現在、Tier-1レベルのISPでは交換されている経路情報が20万経路に達しているという報告があります。もし現在のままIPv6とのdual stack（IPv4とIPv6を同時に使える構成）にすると50万経路に達するという予測が立っており、インターネットのアーキテクチャとしては規模拡張性に欠けるのではないか、と指摘されています。会場では現在最も普及しているBGPにこだわらず、この問題を解決するための議論を行うBoFを今後開くことの提案がありました。試しに会場で挙手をしてもらったところ、多くの人が賛成に手を挙げていました。その他にIPv6は今後様子を見ながら検証すべき、（ルーティングにおける）セキュリティに関する議論も必要である、といった意見が挙げられていました。

□ The IAB Workshop on Routing and Addressing
http://www.iab.org/about/workshops/routingandaddressing/index.html

このワークショップは第53回RIPEミーティングの後、同じアムステルダムで行われていました。今後も、ISPのコミュニティとIETFのコミュニティの情報交換が進んでいくと思われます。

◇　　◇　　◇

次回の第68回IETFは、2007年3月18日～23日、チェコ共和国のプラハで開かれる予定です。

（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、ここ数回の会議と同様にDNSSECに関連する話題が中心となりました。NSEC3の状況報告がなされ、解決された問題点や、米国ダラスにて行われたワークショップにて新たに見つかった問題点等が報告されていました。具体的には、NSEC3PARAMというリソースレコードが新たに追加されたことによって、NSEC3にて利用されているアルゴリズムを特定することが容易になったという報告や、DNAMEによって別名が存在するゾーンにおけるNSEC3の扱い方が定められたといった報告がなされました。

このように、NSEC3は一歩ずつ仕様決定に向けて進んでいるのですが、その一方でDNSSECに関する新たな提案がなされました。Signature-Only DNSSECと名付けられたもので、提案者はDNSSEC liteとも呼んでいました。これは、現在提案されているDNSSECと以下の点で異なっています。

- 署名の検証をDNSサーバが行うのではなく、エンドノードが行う
- NSEC/NSEC3を用いず、署名のみを行う
- ツリー構造にとらわれない署名が可能となる

ここ数回の会議でNSEC3が話し合われ、仕様決定に向かっていたところにこの新たな提案がなされたため、会場では多数の質問が出ました。しかし、全ての人が否定するわけではなく、肯定的な意見も見られました。そのため、引き続きメーリングリストにて議論を行い、NSEC3を用いた従来のDNSSECとDNSSEC liteとのそれぞれの利点、欠点を引き続き議論していこうという方向にて会議は終了しました。

□dnsext WG
http://www.ietf.org/html.charters/dnsext-charter.html

□第67回IETF dnsext WGミーティングのアジェンダ
http://www3.ietf.org/proceedings/06nov/agenda/dnsext.txt

◆dnsop WG（Domain Name System Operations WG）

dnsop WGでは、まずWG Last Call直前のドラフトに関して議論が行われました。

具体的には、default-local-zonesやreflectors-are-evil、respsizeといったドラフトに関してステータスの確認とアップデートすべき点が確認されました。default-local-zonesに関しては、IPv4の他にもIPv6も考慮したlocal zonesの定義を加えることが確認されました。また、reflectors-are-evilのドラフトに関しては、大きな指摘も無く、WG Last Callに向かうことが確認されました。respsizeに関しては、いったんWG Last Callをする方向になったのですが、その後いくつかの修正が著者によって加えられたため、再度レビューが必要だという意見が出ました。そのため、まだWG Last Callは行われていません。

その他には、SPF RRを利用した攻撃を防止するための対策や、AS112と呼ばれる、プライベートアドレス空間に対するDNS問い合わせを吸収するためのプロジェクトをWGとして認めるという確認がなされました。さらに、DNAMEに関するdnsext WGのドラフトを運用上の観点からレビューすることも確認されました。

□dnsop WG
http://www.ietf.org/html.charters/dnsop-charter.html

□第67回IETF dnsop WGミーティングのアジェンダ
http://www3.ietf.org/proceedings/06nov/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、11月6日（月）の午前9:00〜11:30という、ミーティング初日の朝一番の枠で開催されました。当初、ミーティング会場として小さめの部屋が予定されていたのですが、開始直後に部屋がいっぱいになり、急遽別の広い部屋で実施していた別のWGミーティングと部屋を入れ替えるという、IETFでも珍しい事態となりました（参加人数を予測して部屋を割り振っているはずなのですが）。最終的には、150名程度という多くの参加者によって、議論が実施されています。

まず、会場から、NAT-PTの後継プロトコルについての提案がありました。IPv6とIPv4間のプロトコル変換を実施するNAT-PT（RFC2766）は、運用上・セキュリティ上の問題の多さから、その文書のステータスをHistoricに変更することになっています（当初、Experimentalステータスにしよう、ということになっていましたが、IETFの文書ステータスの関係から、Proposed Standard ステータスからはExperimentalステータスへの移行ができないため、Historicにする方向で検討が進んでいます）。

NAT-PTに関する問題は、draft-ietf-v6ops-natpt-to-exprmntl-03.txtに詳述されています。しかしながら、IMSネットワークでのアドレス変換の必要性があるとの意見があり、再度提案/議論が実施される予定になっています。

この後、RFC化に向けた、ラストコール（WGLC:Working Group Last Call）を目指す五つのWGドキュメントのレビューと、WGとして取り組んでいる二つのトピックについての議論がありました。

レビューされたドキュメントは、以下の五つです。

- 802.16ネットワーク（WiMAX等）におけるIPv6デプロイメントシナリオ
  （draft-ietf-v6ops-802-16-deployment-scenarios）
- IPsecを用いた、IPv6トンネルのセキュア化
  （draft-ietf-v6ops-ipsec-tunnels）
- IPv6ユニキャストアドレス割り当て
  （draft-ietf-v6ops-addcon）
- 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）
- IPv6におけるポートスキャン
  （draft-ietf-v6ops-scanning-implications）

これらのドキュメントは、関連WGへの意見照会後に、WGLCへと進むことになっています（2007年1月の時点で、上記五つのドキュメントのうち、“802.16 ネットワーク”以外のドラフトはWGLCがかかり、MLでの議論が進んでいます）。

これらのドキュメントについての議論に続いて、IPv6ネットワークのリナンバリングについてと、複数アドレス選択に関するドラフトについて、議論されました。

後者は、NTTとIntec Netcoreの共同提案です。IPv6ノードは同時に複数のIPv6アドレスを持つことがあります。このような環境で通信を開始する際、一つのアドレスを選択する必要がありますが、アドレスの選択を間違えると通信ができない可能性があります。そこで正しいアドレスを選択するためのアドレス選択ポリシーを、ノードに提供できるようにしよう、というものです。v6ops WGとして取り組みを進めていくことが合意され、今後、アドレス選択の手法を含めて議論が実施されることになっています。

v6opsの文書についての議論が終わった後、オープンな議論として、IPv6のマルチホーミングについての議論が実施されました。今回は、特に、ルーティングの観点からの問題提起として、現状、IPv4ネットワークはマルチホーム関連の経路情報の多さが問題になっていますが、IPv6も同じ方向に進み始めていることが指摘されました。この問題は、IETFのプレナリセッションでも提起されており、今後、解決に向けての議論が加速されそうです。

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

□第67回IETF v6ops WGのアジェンダ
http://www3.ietf.org/proceedings/06nov/agenda/v6ops.txt

◆shim6 WG（Site Multihoming by IPv6 Intermediation WG）

shim6 WGは、従来のルーティングによるマルチホームではなく、エンドホスト間でのインタラクションによって、IPv6におけるマルチホームを実現するプロトコルを策定するWGです。今回のセッションでの主なトピックは、基本スペックのWGLCと実装状況の紹介等でした。

基本スペックは、下記の三つのドキュメントから構成されており、プロトコル自体を記述したものと、ハッシュを用いてアドレス情報を安全に交換するHBAという方式について記述したもの、そして通信障害検出とアドレスペア選択の方式を記述したもの、となっています。

1. Level 3 multi-homing shim protocol
2. Hash Based Addresses （HBA）
3. Failure Detection and Locator Pair Exploration Protocol for IPv6 multi-homing

いくつかの小さな問題に関するディスカッションがありましたが、結局ドキュメントのレビューワーが少なく、その場ではWGLCには至らず、メーリングリストで継続審議ということになりました。

基本スペック以外のいくつかの提案について更新状況を紹介した後、ソウル大学とETRI（韓国電子通信研究院）が共同で進めている実装の進捗状況について発表がありました。OSはLinuxで、現在はユーザーランドのデーモンとして実装を進めているとのことでした。他にも全部で四つ程進行している実装はあるようですが、まだ基本スペックの実装が完了しているものは無いようです。

最後に、WGのネクストステップとしては、基本スペックをIESGに提出し、次のIETF68ではセッションを持たず、IETF69にて実装から得られた知見等も含めて基本スペックや拡張モジュールの検討を行ってはどうか、という提案がチェアからなされました。

一時はIETF全体から多くの注目を集めていたshim6 WGですが、メーリングリストや今回のセッションでもあまり多くのレビューワーを集められないという状況になっているようです。トラフィックエンジニアリングに対するオペレーターからの要求に応えられていないことや、IPv6でもPIアドレスが利用可能になったことから、興味関心を無くしてしまった人が少なからずいるように思われます。

□shim6 WG
http://www.ietf.org/html.charters/shim6-charter.html

□第67回IETF shim6 WGミーティングのアジェンダ
http://www.ietf.org/proceedings/06nov/agenda/shim6.txt

◆intarea meeting （Internet Area Open Meeting）

Intareaのミーティングでは、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ます。今回は、認証関連のトピックや、アドレス詐称の防止などについて議論が実施されました。

IPv6には直接は関係ありませんが、このミーティングの最後の話題としてGeoff Huston氏より、インターネットにおける「名前」についてのプレゼンテーションが実施されました。DNSをはじめとして、インターネット上ではいろいろな「名前」が定義され、それぞれの層（インターネットのプロトコル階層）での「アドレス」とのマッピングが実施されています。IPアドレスについても、IPアドレスそのものに意味を持たせようという提案や、IPアドレスの持つ位置特定機能と、ノードの識別子としての機能を明確に分離する提案などが現在も議論されています。また、マッピングも、同じ目的のマッピングが違う階層で実施されていたり（モバイルIPとshim6、HIP など）等、統一性が無く、プロトコルも百花繚乱となってしまっています。

特に提案や結論のあるプレゼンテーションではなかったのですが、インターネットの利用に大きく関わってくる、「名前」のあり方について、今後検討を進めていく必要があると感じました。

□第67回IETF intareaミーティングのアジェンダ
http://www.ietf.org/proceedings/07nov/agenda/intarea.txt

第67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
https://datatracker.ietf.org/public/meeting_agenda_html.cgi?meeting_num=67

WGアジェンダ、発表資料
https://datatracker.ietf.org/public/meeting_materials.cgi?meeting_num=67

（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）

■セキュリティ関連WG報告

第67回IETFではセキュリティエリアのセッションが21行われました。その中の二つがBoFで、残りの19セッションがWGでした。本稿では、この中からSIDR WGとPKIX WGを中心に報告いたします。リソース証明書についてはAPNICやRIPE NCCの動向を踏まえてお送りしたいと思います。

◆SIDR WG （Secure Inter-Domain Routing WG）

SIDR WGはネットワーク・ドメイン間の経路制御に適用できる新たなセキュリティの仕組みを策定・開発することを目的としたWGです。このWGは2006年4月に結成され、WGとしてのセッションが開かれるのは前回の第66回IETFに続いて今回が2回目となります。

SIDR WGでは、IPアドレスの割り振りを電子証明書で証明する認証基盤の検討が進められています。この電子証明書はリソース証明書と呼ばれ、主にルーティングの安全性向上のために使われるとされています。

セッションの最初にWGのステータスの確認が行われました。SIDR WGの趣意書で示されたマイルストーンでは、以下の三つのinitial draftが投稿される予定でした。

－inter-domain routing security
ドメイン間のルーティングセキュリティ

－certificate objects
電子証明書の内容と処理手続き

－securing origination of routing information
経路情報の発信元情報を安全にする手法

このうち2番目はリソース証明書の書式に関するもので、すでにAPNICのGeoff Huston氏によって進められています。1番目と3番目は、これまでに大きな取り組みがなく、今回のミーティングで活動を開始することが確認されました。またルーティングセキュリティアーキテクチャについてのInformational RFCと、セキュアオリジンメカニズムに関するProposed Standard RFCが作られることが予定されていましたが、これらは議論があまり行われてきていなかったことから、作成を取りやめる可能性がチェアによって示されました。これまでリソース証明書の議論に注力してきており、セキュアなルーティングアーキテクチャの具体化に、手が回っていなかったのが実情のようです。

□Secure Inter-Domain Routing （sidr）
http://www.ietf.org/html.charters/sidr-charter.html

今回のBoFでは主に四つの話題について議論されました。

1.Geoff氏によるリソース証明書に関するI-Dの02版について
2.Stephen Kent氏によるCPS（Certification Practice Statement）CP（Certificate Policy）に関するドラフトドキュメント
3.ROA（Route Origination Authorization）のデータ形式に関する提案

4.RIPEドキュメントとなっているRPSLとROAとの整合性

ここでは1と4についてご報告いたします。

一つ目のGeoff氏のリソース証明書に関するプレゼンテーションでは、何点かの改良を行った、リソース証明書に関するドラフトドキュメントの02版について説明されました。リソース証明書には全て（割り振り先の）証明書を発行するために認証局であることを示すビットが立つことが想定されていましたが、このビットが立っていないEE証明書が新たに紹介されていました。しかし複数の割り振り元があるマルチホームの状態である場合などで、これらの証明書がどのように使われるか、といった具体的な使い方が明らかになっておらず、今後も検討が進められると考えられます。

Geoff氏のプレゼンテーションの後半では、“リソース証明書の利用”と題して、電子署名のWebインターフェースのデモが行われました。このWebのプログラムは10月に行われた第53回RIPEミーティングや第18回ARINミーティングで使われたものとほとんど同じです。Webアプリケーションとして動作するもので、サーバ側にある鍵を使って電子署名が行われます。このデモについて、RIRのミーティングでは、このデモの動作の内容については特に議論されませんでしたが、SIDR WGでは運用面でさらに突っ込んだ議論になりました。結局、リソース証明書をエンドユーザー同士でどのように交換するかのガイドラインが必要になることがわかりました。

リソース証明書のモデルはシンプルですが、証明書の構造は徐々に複雑になってきました。また第53回のRIPEミーティングではルーティングセキュリティにおける効果がわからないという指摘を受けてもいます。IETFのSIDR WGとしては仕様を検討してドキュメント策定を進めることになりますが、利用モデルが見えない中で複雑化が進んでいった場合に、運用しやすいものになるのか、という懸念は残ります。

四つ目の議論は、ROAではASパスを保護できないという点についてです。ROAは経路情報の発信元がIPアドレスを利用する権利を持つことを保証します。しかし経路情報が伝播するASパスの正しさを保証することはできません。これはルーティングにおけるセキュリティの要件をまとめているRPSEC WGのドキュメントに依存する議論となりそうです。RPSEC WGでは、ASパスのセキュリティに関するドキュメント作成にも取り組んでおり、2007年の3月頃にWG last callになる見込みであるとのことです。RPSEC WGのドキュメントがまとまる頃には、SIDR WGで扱われるプロトコルが増え、ASパスの安全性向上を図るプロトコルが現れるかもしれません。

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

PKIX WGは電子的な認証基盤の規格であるITU-TのX.509をインターネットに適用して新たな規格作りを行っているWGです。PKIXは長寿のWGで、参加者は顔なじみの方が多いようです。

はじめにドキュメントステータスの確認が行われました。新たにRFCになったのは以下の二つです。

- Internet X.509 Public Key Infrastructure Subject Identification Method（SIM）（RFC 4683）
  http://www.ietf.org/rfc/rfc4683.txt

> 個人が特定できるような識別子（米国のソーシャルセキュリティナンバーなど）を直接電子証明書に載せる代わりに、一方向性ハッシュ関数の結果を入れるなどして、第三者に対して匿名性を確保する手法を提案したRFC。元々は韓国のJongwook Park氏によって提案され、後に前チェアのTim Polk氏によって引き継がれた。

- Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List（CRL）Profile（RFC 4630）
  http://www.ietf.org/rfc/rfc4630.txt

> RFC3280に記述された、ディレクトリ文字列のエンコードに関する部分を変更したドキュメント。ディレクトリ文字列は証明書の発行元や発行先の記述のために使われる文字列で、一時期は国際化と相互運用性を図るためにUTF-8の利用が推奨された。しかし実装の現状を鑑みて、移行期限であった2003年12月31日という記述は削除された。なお、本RFCでは、UTF8StringとPrintableStringの二つが推奨されている。

IESGのレビューを受けているドキュメントは以下の六つで、これらはまだ修正のための検討の余地が残っているようです（2007年1月現在）。

- Certificate Management Messages over CMS
- Certificate Management over CMS（CMC） Transport Protocols
- CMC Complience Document
- Server-based Certificate Validation Protocol（SCVP）
- Lightweight OCSP Profile for High Volume Environments
- Internet X.509 Public Key Infrastructure Subject Alternative Name for expression of service name

最後のSubject Alternative Name for expression of service nameは、DNSのリソースレコードに記述されたホスト名とサービス名を証明書のSubjectAltNameフィールドに載せ、ホスト認証だけでなく個々のサービスを行って

いるサーバの認証を行えるようにしたものです。マッチングルールを用いて、メールサーバのような同一のサービスを複数のサーバで提供している場合にもSRV RRと証明書を組み合わせて認証できるようになっています。

セッションの中で多くの議論が行われたのが、Elliptic Curve Cryptography公開鍵識別子に関するデザインチームのレポートです。アルゴリズムの識別子を定義しているRFC3280に則った方法では、楕円暗号を使った鍵交換プロトコルのEC-DHとEC-MQVを識別することができません。そこで、識別のための三つの手法を比較することになりました。議論はメーリングリストで継続されることになっています。

最後に"Certificates in CRLs"と題してMicrosoftのStefan Stantesson氏によるindividualドラフト（WGのドラフトではない個人作成のドキュメント）の紹介が行われました。このドキュメントでは、CRLの中に証明書データを入れておいて、CRLの署名検証のときに行われるパス構築（検証したい証明書と信頼されたCAまでの間の証明書のツリー構造を作ること）の補助をする仕様が提案されています。CRLを発行した認証局の鍵が変更されたときなど、そのCRLの署名を行った鍵を見つける必要がある場合には、RFC4325で定義されているCRL拡張を使って鍵の識別子を読み出して探す方法があります。しかし検証対象のCRLが古く、それを発行した認証局の証明書がネットワークを使って得られなかったり、必要な数の証明書を入手するまでに多くのネットワークアクセスを伴う可能性があります。このドキュメントでは、これらの処理を軽減させるために、CRL拡張の中に入った証明書データを使うことを提案しています。会場では、このドキュメントをWGドキュメントとするかどうかについて議論されましたが、今後メーリングリストを使って方向性が決められることになりました。

□Internet X.509 Public Key Infrastructure
Authority Information Access Certificate Revocation List (CRL) Extension
http://www.ietf.org/rfc/rfc4325.txt

◇　　◇　　◇

IETFでは、議論の合理性や方向性などについて真剣に話し合われることがしばしばありますが、セッションの終了後や休憩時間には、まれにユーモラスな遊び（?）が繰り広げられていることがあります。ある方は、IETFやRIPEミーティングなどの国際会議で出会った人々と有名なテレビ番組の人形を一緒に写真におさめて、Webページにまとめています。光栄なことに私も撮っていただきました。

□Bert meets the stars
http://bert.secret-wg.org/Stars/

この写真を撮ってらっしゃる方は、WGのチェアやIABのメンバーなどをされていて、RIRのミーティングなどでも大変活躍をされている方です。ちなみに写真のコメント文には、それぞれの方の専門分野をからめたシャレが書かれています。私もいつか自分の専門分野についてのコメントをいただけるようになれたらと、密かに思いました。

（JPNIC 技術部 木村泰司）

2006.10.30→11.2 IGFアテネ会合報告

［関連記事］ P.59「IGFアテネ会合に参加して」

2006年10月30日から11月2日までの4日間、インターネットガバナンスフォーラム（IGF：The Internet Governance Forum）がギリシャのアテネで開催されました。IGFはインターネットガバナンスのさまざまな問題に関して各界の利害関係者が対話を行うフォーラムで、2005年11月の世界情報社会サミット（WSIS）チュニス会議で設置が決定されたものです。

今回のIGFをどのように運営するかについては、事前にアドバイザリーグループで議論が積み重ねられました。このグループは政府、民間、NGOなどさまざまな背景を持つ46名のメンバーからなり、それ自体がマルチステークホルダーを体現しているようなメンバーでした。

このアドバイザリーグループにより、今回のIGFのテーマが「開放性（Openness）」「セキュリティ（Security）」「多様性（Diversity）」「アクセス（Access）」の四つに絞られ、IGFのメインセッションとしてこの四つのテーマが議論されました。

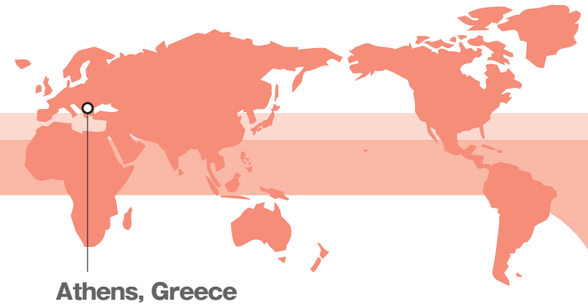
会合の形式ですが、パネリストが壇上に並び、発言はリアルタイムの速記録がスクリーンに投影され、フロアの出席者も司会者の指名を受けられれば発言可能という形で、ICANNやRIRの会合と似た雰囲気を感じました。しかしそれらの会議に出席した経験のない方にとっては、こういった形式は非常に新鮮だったようです。

会議の参加者は、事前登録ベースで1,200名弱でした。国連関連のイベントだけあって政府関係者も多かったのですが、研究者やインターネット関連団体、市民メンバーからの参加も多く、あるワークショップでは政府関係者4、研究者及び学術関係者4、その他2といった割合でした。参加者が多かったせいか会場の無線LANの通信品質が悪く、プログラムの更新情報等を得るのに四苦八苦でしたが、国連関連イベントでインターネット接続環境が提供されることを素直に感謝する方が良いのかもしれません。

会議の結論から言いますと、設定されたテーマについて今回のIGFで何らかの拘束力を持つ決議や宣言がなされたということはなく、従って既存のICANN体制に影響を与えるものではありません。会合のまとめは、最終日にそれぞれのセッションの司会進行役が「個人的感想」としてセッションの報告を行うことでそれに代えています。IGFはまずは対話の場として機能したということだと思いますが、メインセッションでは多くのテーマが結局のところ発展途上国に

メインセッション（Openness Session）の模様

Internet Topics インターネット・トピックス



対するインフラ構築の支援をどう実現するかというところに収斂し、前途の多難さも感じました。開放性もセキュリティも多様性も大事だけれど、インターネットへのアクセスさえもなければ何も始まらない、という端的な意見が多く聞かれ、そういう観点からは今回最も参加者間の利害が先鋭化したメインセッションは「アクセス」だったと思います。

また、今回のIGFではメインセッションと並行して36ものワークショップが開催されています。インターネット関連団体が、自身が取り組むテーマについて自由に説明、議論をする場というものですが、IGF事務局はその結論には関知せず、あくまで諸団体が付随的に開催するイベントという位置づけでした。

この中では、私は「DNSとルートゾーンファイル管理」というワークショップに出席しました。ルートゾーンの管理が現在どう行われているかについて説明、議論するワークショップで、現にルートサーバを管理しているVeriSign社やAutonomica社の担当者もパネルに加わっていました。進行中、ルートゾーンファイルの変更、更新の最終承認権限を米国政府が保持していることに不満を表明する参加者が複数いて緊迫した場面もありましたが、その管理体制下で現に問題が発生していない状況で、体制の議論をすることにどれほどの意味があるのかといった冷静な意見も出され、その場は混乱することなく収まっていました。

元々IGFは拘束力のないプロセスに基づいて進められるという約束事があった以上、対話の場として機能することが重要な訳ですが、このように率直な意見交換が実際に運用に携わる層やユーザーとして利用する層との間でなされることによって、少しでも議論が建設的な方向へ進めばIGF開催の意義があったということになるのではないでしょうか。

IGFはまず5年間維持し、その間にIGFを継続するかどうかの検討が行われます。2007年はブラジル（リオデジャネイロ）での開催、2008年はインド、2009年はエジプトでの開催がそれぞれ決まっており、2010年のIGFにはリトアニアとアゼルバイジャンが立候補しているという状況です。この間にインターネットガバナンスを巡る議論がどういった方向に向かうのか、IGFの行く末はどうなるのか、引き続き動向を追っていきたいと思います。

□ The Internet Governance Forum
http://www.intgovforum.org/

（JPNIC インターネット推進部 穂坂俊之）

［関連記事］ P.57「IGFアテネ会合報告」

IGFアテネ会合に参加して

◆チュニスアジェンダにおける設計論と、その実装

IGF－インターネットガバナンスフォーラムが開催されたのは2006年10月末から11月初めのことであり、それから既に1ヶ月以上経ってしまいました。会合の様子はJPNIC穂坂によって、News & Views vol.408※1で報告されていますのでそちらに委ねるとして、ここでは私が出席者として感じたことを述べたいと思います。

IGFはWSISチュニス会合のステートメント、チュニスアジェンダで国際連合の管轄下で設置されることが明言されました。以下に77章の和訳※2を引用します。

> 77. IGFは監督機能を持たず、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。逆に、それらと関与し、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。インターネットの日常的又は技術的な運用業務には関与しない。

つまり、「政策の立案や推進」を行うものではなく、もっぱら「マルチステークホルダー間の対話の促進」を目的として設置されるものと定義されました。チュニスアジェンダが発表されたときに見受けられた否定的な捉え方として、「結局ICANNの問題は先送りか」「IGFは対話だけに終始するガス抜きの場になるのか」といったものがありましたが、私にとっては国際連合がこのようなインターネット的なアプローチの会合を維持することを明言したことが、とても印象的でした。

そしてIGF発足会合（Inaugural IGF Meeting）と銘打たれた今回のIGFは、そのように設計された会合がどのように実装されたかを目の当たりにする初めての機会だった、と言えます。

◆「一般の」人々からのインターネットへの要請

会合の様子を目の当たりにしての印象はいくつかにまとめられます。まず第一に、このIGFは、全世界の「一般の人々」からの、インターネットに対する要請が呈される場であったということです。ここで「一般の人々」というのは、技術者や愛好者に限ることなく「インターネットを仕事や日常生活におけるツールとして利用している方々」という意味合いであり、「一般の」とは「偏りのない」「全般的な」という意味合いを含みます。

※1 News & Views vol.408【臨時号】IGFアテネ会合報告
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2006/vol408.html

※2「情報社会に関するチュニスアジェンダ（仮訳）」
http://www.soumu.go.jp/s-news/2005/pdf/051119_1_2.pdf

Internet Topics
インターネット・トピックス

IGFアテネ会合に参加して

メインセッションの中では、特にオープニングセレモニーにおけるスピーチにその特徴がとてもよく現れています。そこでは既に日常的社会活動の大きな部分をインターネットに依存している先進国、今からインターネット上の知識を吸収して発展しようとする発展途上国、あるいはビジネスプレイヤーなどそれぞれの立場から、インターネットに対して抱く期待、要望、懸念などがきっちり練り上げられた文章で呈されていました。

それ以外にも、メインセッションのパネルディスカッションが、インターネットの専門家ではないジャーナリストによって司会進行されたことにも、広く一般的な視点からインターネットを見つめなおすという姿勢が示されたと思いますし、どのセッションでもスピーカーやパネリストを、満遍なくいろいろな領域から選んで配置したことからも、議論の一般性にこだわって構成したことがうかがえます。

これと対照的に、私が普段JPNICの仕事で付き合うような、RIRs、ICANN、ISOCの人々は、多数参加して会場にはいるのですが、意識的にだろうと思えるほど発言せず、静かにセッションを聴いているように見えました。

また「一般」とは、国際連合の視点に立つと「全世界」ということになるようです。特に、中近東や南米より群を抜いてアフリカからの参加者が目立ちました。穂坂の報告にもあったように、「まずはインターネットに対するアクセスが欲しいんだ」という強いアピールが呈されました。彼らに取ってインターネットは、貧困の窮状を世界に伝えることができる、また発展に必要な知識を手に入れることができる格好のツールとなるだろうにも関わらず、「それがないために発展を手に入れることができず、先進国との格差が広がっていく一方なんだ」という主張が、実にさまざまな形で見受けられました。

◆「マルチステークホルダリズム」と「対話」

今回耳にした単語で最も興味深かったものを上げるとすると、「マルチステークホルダリズム」でしょう。英語でmultistakeholderism。stakeholderは日本語で「利害関係者」と訳すと、「多利害関係者主義」と無理やり訳すことができます。ただし、今回のIGFにおけるステークホルダーの散らばりを見ていると、利害が大きく相反するというよりも、一つのテーマに対して取り扱う方向性や問題意識が異なる、つまり立場が異なるといった意味合いで捉えるべきだと思います。

いずれにしても、multi-stakeholderという表現にさらに接尾辞をつけたという、この複雑な単語を聞いたのは今回が初めてですが、それが自然に受け入れられたほど、マルチステークホルダーのアプローチ、つまりマルチステークホルダリズムが徹頭徹尾貫かれていました。

メインセッションのスピーカーリスト※3を見ていただくと分かりますが、オープニングプレナリが結果的に国連や政府の高官が多くなっていたのを除き、どのセッションでも、政府、インターネットコミュニティ、ビジネスセクター、市民社会、アカデミズムとさまざまな分野から、しかも地域分散も考慮に入れられた人選になっていました。

これは、インターネットコミュニティで従来取り入れられてきた「オープンでボトムアップな」仕組みのどれよりも、マルチステークホルダリズムにこだわっているように見えます。

これと一見独立しているように見えて、実は深い関わりがあるように思えるのが、「対話」です。ここでのマルチステークホルダリズムは、一つのテーマに対して専門を異にする人々が議論を行うということであり、それらの人々の間で議論を収束させるのがそもそも難しいという先天的性質をはらんでいます。先進国対発展途上国のように、発展の度合いなどの尺度で分けた場合には、確かに対立構図が浮かび上がるわけですが、同じテーマを扱うにしても、全く分野が違う人々が話し合う場合、「一定の結論を出す」ことよりも「他の分野の人々の考え方の背景を理解する」ことの方がとても重要であるように見えます。

つまり、ここでマルチステークホルダリズムを取る以上、おのずと結論付けよりも対話の方が重要となるということであり、参加者それぞれが自分が執行力を持つフィールドで、対話を通じて得られた背景理解によってより良い方針や政策を打ち出していくという、まさにチュニスアジェンダに示された機能の妥当性が再確認されます。また利害対立がある場合においても、対立の解消に向けてやはり相互の背景理解は重要であり、そのような場としてIGFが機能し得ることを示唆します。

◆「外交官モデル」から「劇場モデル」へ

これまで述べてきたように、IGFは先進国からも発展途上国からも参加者が集まり、発展途上国支援の文脈を色濃く帯びるものであるという意味で「国連的」でしたが、一方で「マルチステークホルダー」による「対話」は、「ラフコンセンサス」につながっていく「インターネット的」でありました。

今回JPNICからの参加者3名は、経団連（日本経済団体連合会）の視察団に仲間入りさせていただきました。経団連視察団の皆さんは当初このIGFに対して戸惑いを隠せなかったご様子でした。冒頭にチュニスアジェンダを引用したように、そもそもこの会合が何らかの明確な成果物を目指して開催されるものではないという点が大きい要因だったようです。

※3 The Internet Governance Forum（IGF）- Panellists
http://www.intgovforum.org/list%20of%20panellists.ph

Internet Topics
インターネット・トピックス

IGFアテネ会合に参加して

たとえばWSISでは、ジュネーブ行動計画※4やチュニスアジェンダという形で、明確な成果物が残されることが予め決まっており、それが導出される道筋を追うということができたと同時に、結果に影響を及ぼそうとする場合、その道筋に沿ってアクションを起こすことが定石と言えるでしょう。しかしながらこのIGFにおいては、結果として打ち出される予定のものはなく、最終日に予定されているのは前日までの議論のまとめだけでした。この状態では、全体の中でどこに注視してよいか見当がつかないばかりでなく、後に残るような成果が本当に出るのか疑わしいということです。

本当に実体的な成果に結び付くかどうか、それは現時点ではまだ分かりませんが、経団連視察団のまとめの会合でとても深く印象に残ったことは、団員の皆さんが敏感に、インターネットコミュニティの意思決定プロセスの性質と同じものをIGFにお感じになっていたことです。

ここで指摘されることは「ラフコンセンサス&ランニングコード」というインターネットの根底に流れる大方針ではなく、それに基づいた、参加者が誰でも自分の意見を述べてコンセンサスを目指すオープンでボトムアップなプロセスや、その弊害である、声が大きい人が影響力を持ってしまうこと、会議運営者と仲良くしておくことが議事を運ぶ上で大きな影響を及ぼすことなど、インターネット業界における会議の進み方や問題点を、的確に言い当てていらっしゃるように思いました。

その極めつけは、視察団団長をお務めになった、野村総合研究所の理事長、村上輝康さんの、「IGFでの交渉の進め方は、外交官モデルではなくて劇場モデルであった」というご指摘でした。外交官モデルというのは、国連の会議がそれにあたるでしょう。宣言の採択に水面下で諸国と交渉し、自分の主張がより強く反映されるような文面になるように頑張るようなモデルです。

それに対して劇場モデルというのは、どんな文言を宣言に盛り込むかということよりも、参加者が人としてどういう主張を持っているか、それをどう他の参加者全員に印象付けるかということが非常に重要であるモデルです。また今回は特にメインセッションでも会場からの意見も積極的に取り上げたので、発言そのものが議論の流れに影響を及ぼし、それが参加者に与える印象を大きく左右するといったことで、既にそれを織り込んだ議事運営戦略が見受けられたという指摘がありました。

◆今後のIGFはどうなるのか

私は経団連視察団の皆さんが敏感にインターネット的なアプローチの性質と問題点を言い当てられるのを見てから、ちょっと大げさかもしれませんが「このように世界は動いていくのかもしれない」と思うようになりました。つまり、やり方が変わったら、それが重要な任務である方々はちゃんと追従して対応し、新たなやり方で任務を果たすのです。それが重要になればなるほど、機敏に対応するようになるのでしょう。

このIGFの準備にあたったのは、ニティン・デサイ国連事務総長特別補佐を議長とするIGFアドバイザリーグループ※5でしたが、チュニスアジェンダに示された設計を良い形で実装できたと思います。そしてその参加者がその設計を理解して、新たな進め方を身につけようとしています。

「対話だけで物事が進むわけがない」という否定的な見方はありますが、私には上記のような敏感な反応が、物事が進む兆しのように見えるのです。少なくとも希望を持って信じるに価するし、信じて取り組むことで物事の進み方は加速するのではないかと思います。

来年のIGFはリオデジャネイロとなります。ブラジル政府がICANN体制に批判的であるということもあり、次はICANN体制を中心テーマに据えるとも言われています。2006年12月8日に公開された、ICANNの戦略計画2007-2010のドラフト※6の中でも、multistakeholderの参画の促進をはじめとしたポリシー策定体制の充実が中心に据えられていまして、この説は本当かもしれません。

私もインターネットの資源管理に携わる身として、ICANNの問題がどう扱われるかには注視しています。しかしそれだけにとどまらず、本稿で申し上げたような、「一般」からのインターネットに対する要請に関して「マルチステークホルダー」が「対話」することで、「既存の組織と関与し、その能力を活用」して政策を推進していくという、チュニスアジェンダで示された設計図が、今後どのように実現されていくのか、大きな期待とともに見守りたいと思います。

（JPNIC IP分野担当理事 前村昌紀）

※筆者の肩書きは2006年11月当時のものです。

※4 World Summit on the Information Society
http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0

※5 The Internet Governance Forum （IGF）
Advisory Group - List of Members
http://www.intgovforum.org/ADG_members.htm

※6 ICANN Strategic Plan July 2007 - June 2010
http://www.icann.org/strategic-plan/draft_stratplan_2007_2010_clean_final.pdf

Internet Topics
インターネット・トピックス