

モンテビデオウィークを終えて



関連記事 「P.8 特集2 インターネットガバナンスの動向」

2013年9月30日(月)から10月4日(金)までの1週間、私は南米ウルグアイの首都モンテビデオに出張していました。目的は、NRO ECおよびI*(アイスター)の合宿検討会合に参加することでした。本稿では、これらの団体についてご紹介するとともに、会合の内容を取り上げます。なお、それぞれの会合内容に関しては、基本的に公開を前提としたものではないため、概要のご紹介になります。

◆ NRO EC合宿検討会合

NROは「Number Resource Organization」の略で、五つの地域インターネットレジストリ(RIR; Regional Internet Registry)の連合体です。ICANN (The Internet Corporation for Assigned Names and Numbers)や他の団体に対して、IPアドレスやAS番号を管理するレジストリの立場を代表する機能を有しています。特にICANNの中では、2004年に取り交わしたASO-MoUによって、NROがICANNのアドレス支持組織(ASO; Address Supporting Organization)の役割、責任、機能を遂行することが定められています。

その中でEC (Executive Council)は、NROの意思決定を行うグループで、五つのRIRのCEOをメンバーとして構成されます。私はアジア太平洋地域のRIRであるAPNIC (Asia Pacific Network Information Centre)の理事を拝命していますが、その中で、APNICにおける議長とともにNRO ECオブザーバも仰せつかっています。そのため、今回の合宿検討会合に参加したということです。

NROは、5RIRを代表して他団体に対応することと、5RIRの協調活動を行うことを目的としていますが、専任のExecutive Secretaryを1人置く以外、すべての活動はRIRの職員が分担で行っています。世の中に対しても、NROよりも各RIRの方が名前が通っているのが実情で、NROとしてのアイデンティティが確立していないという状況にあります。そういう中で、今回の合宿検討会合は、戦略計画立案を目標として、外部コンサルタントをファシリテータに、ワークショップ形式で、9月30日(月)、10月1

日(火)の2日間にわたって開催されました。

ワークショップは、NRO ECメンバーであるRIRのCEO以外にも、オブザーバ、随行した各RIRの職員も参加しました。全体検討でも積極的に発言が求められ、小グループに分かれた作業も行いながら「強み(Strengths)、弱み(Weaknesses)、機会(Opportunities)、脅威(Threats)」といったそれぞれの側面から分析する、SWOT分析による戦略領域の検討、ビジョン(理想像として追い求める目標)、ミッション(現在全うすべき使命)の検討を行いました。

私はNROが創設された2003年には既にAPNIC理事を務めていましたが、2日間にわたる集中的な検討で、今に至るまで気づかなかったさまざまな点に気づくことができ、NROがどのようなものであるか、何を志向すべきなのか、かなり明確な考えを持つことができるようになりました。今回策定したビジョンとミッションは、正式な採択手順を経て、後日公開される予定です。

◆ I*(アイスター)合宿検討会合

I*(アイスター)は、一般的にはなじみのない言葉だと思いますが、インターネット基盤の技術調整などを行う団体のグループを指し、現段階で、ISOC (Internet Society)、IAB (Internet Architecture Board)、IETF (Internet Engineering Task Force)、IANA (Internet Assigned Numbers Authority)、ICANN、W3C (World Wide Web Consortium)、および五つのRIRの計11組織が参加しています。InternetのIを頭文字にするところが多いことから、Iの後にワイルドカードの*(アスタリスク)を置き、I*(アイスター)と呼んでいます。I*11団体の代表者は、年1、2回会合を持ち情報交換を行っています。これをNROの会合に合わせて、10月2日(水)と3日(木)、モンテビデオにて行いました。

会合は、各団体からの情報共有から始まり、以下の内容がそれぞれ報告されました。

RIR	NRO共同で行った、Global IPv6 Deployment Monitoring Surveyの結果
IETF	最近米国の国家安全保障局(NSA)がPRISMと呼ばれるプログラムで実施しているらしいことが明るみに出た、pervasive tracking(情報行動追尾)に関するIETF内での議論の状況
W3C	マーケティング用途でのtrackingに対する対策を検討する、Tracking Protection Working Groupに関する状況
ICANN	最近国際電気通信連合(ITU; International Telecommunication Union)会議体などで議論が盛んな、インターネットガバナンスの状況

これらはどれも、現在のインターネットにおいて、大きな懸念を持たれている重要課題です。IPv6の普及は、日本でも大手ISPが新規顧客に対してIPv6/IPv4デュアルスタックで提供し始めるなど徐々に浸透していますが、コンテンツ、サービスサイドでの取り組みは停滞している状況です。情報行動追尾は、情報ブロックと併せて、利用者にインターネットに対する懐疑心を引き起こしています。インターネットガバナンスの議論は、ITUなどの会議体で堂々巡りの議論を繰り返すばかりの印象が強く、打開策が望まれています。

そこで、会合に参加した団体トップたちは、これらの重要課題に対して積極的に取り組む意志を明確にし、I*(アイスター)11団体共通の姿勢を示す声明文を発表するべきだということになりました。I*(アイスター)会合でこのような声明が出されるのは、初めてのことです。

この声明文は、「今後のインターネット協力体制に関するモンテビデオ声明」と名付けられ、現地における草案検討の後、各団体における承認プロセスを経て、2013年10月7日(月)に発表されました。JPNICでは、既にこの声明文を、和訳とともにWebでお知らせしています。

インターネット関連10団体が「今後のインターネット協力体制に関するモンテビデオ声明」を発表
<https://www.nic.ad.jp/ja/topics/2013/20131008-01.html>
(現在、IANAはICANNの一部局であるため、10団体となっています)

初めての声明発表に至ったということもありますが、インターネット基盤の運営をリードする団体のトップによる2日間の議論は、非常に密度が濃く、充実したものでした。



◆ インターネット各団体のCEOらの記念撮影

◆ 滞在記

モンテビデオは、ラテンアメリカとカリブ海地域のRIRであるLACNIC (The Latin American and Caribbean IP address Regional Registry)がオフィスを構える場所で、これらの会

合はLACNICオフィスから至近のホテルで開催されました。LACNICオフィスは、中南米地域のインターネット諸団体もオフィスを構える、「Casa de Internet de Latinoamérica y el Caribe」(ラテンアメリカとカリブのインターネットの家)にあり、海岸に面した開放的な雰囲気が漂うオフィスです。10月2日(水)の夕方は、I*(アイスター)関係者と地元のインターネット関係者が一堂に会したレセプションが行われ、歓談の輪が広がっていました。この建物を建設する時点で、こうしたレセプションも収容できるように作ってあるのです。Casa de Internetは、「Internet Hub for Latin America and the Caribbean」と英訳されますが、まさにインターネット関係者みんなが集まるハブとして機能していることが分かります。NRO EC、I*(アイスター)を通じて、この1週間、LACNICの会議参加者に対するもてなしは素晴らしく、Casa de Internetを含め、LACNICのホスピタリティに感銘を受けた1週間でもありました。



◆ LACNICのオフィスが入居する、Casa de Internet

◆ 参考

- ・ Number Resource Organization(NRO)
<http://www.nro.net/>
- ・ インターネット用語1分解説：NROとは
<https://www.nic.ad.jp/ja/basics/terms/nro.html>
- ・ ICANN Address Supporting Organization (ASO) MoU
<http://www.nro.net/documents/icann-address-supporting-organization-aso-mou>
- ・ NRO's 2013 Global IPv6 Deployment Monitoring Survey Results
<http://www.nro.net/documents/2013-ipv6-survey-results>
- ・ W3C Tracking Protection Working Group
<http://www.w3.org/2011/tracking-protection/>
- ・ Casa de Internet de Latinoamérica y el Caribe
<http://www.lacnic.net/en/web/lacnic/casa-de-internet>

(JPNIC インターネット推進部 前村昌紀)

IGFバリ会合報告



関連記事 「P.8 特集2 インターネットガバナンスの動向」

10月22日(火)から25日(金)にかけて、インドネシアのバリでインターネットの課題について議論を行う、インターネットガバナンスフォーラム(IGF)と呼ばれるフォーラムが開催されました。本稿では、このIGFバリ会合についてご紹介します。

◆ IGFとは

インターネットガバナンスフォーラム(IGF)は、政府機関、市民社会、技術コミュニティなどの各種関係者が集まって、現在のインターネットにおける課題について包括的に議論を行うことを目的とした、国際連合(United Nations: UN)主催のフォーラムです。

対象となるテーマは幅広く、

- ・インターネットにおける番号資源やルートDNSの管理
- ・セキュリティや監視における課題への対応
- ・開発途上国を中心としたインフラ整備

だけでなく、それに加え、

- ・インターネットガバナンスについて議論を行う現在の仕組み自体

も、議論の対象として挙げられています。

IGFは国連主催でありながら、政府機関だけでなくインターネットのあらゆるステークホルダー(関係者)に門戸が開かれていることが、大きな特徴と言えます。

2006年にギリシャ・アテネで第1回会合が開かれて以来、今回で8回目となるIGFは、10月22日(火)～25日(金)、インドネシア・バリで開催されました。IGFの経緯を含むインターネットガバナンス全般の状況については、以下にまとめていますのでご覧ください。

インターネットガバナンスとは何か

<https://www.nic.ad.jp/ja/governance/about.html>

◆ 会場と参加者

IGFは国連主催のフォーラムとして国連警護班が配備されます。会場入り口では空港と同じようなセキュリティチェックを行い、入場時点でバッジを付けていないと警備員に呼び止められる点が、インターネット業界における他のカンファレンスと異なります。しかし、全体として物々しい雰囲気はなく、私が参加したことがあるカンファレンスではICANN会議に最も近い印象です。

参加者は合計1,500名、111経済圏からの参加があったと報告されています。(UN News Centerから引用)

参加登録時に自分の属するグループを選択することが求められ、公開参加者リストによると、最も参加者の多かったグループは市民社会(Civil Society)で1/3強、次いで政府・政府機関(Government Delegation・Intergovernmental Organizations)も同じく1/3強、そして技術コミュニティ(Technical Community)、民間組織(Private Sector)、メディア(Media)が三つのグループを合わせて1/3弱の参加者という構成でした。

◆ 技術コミュニティ・民間組織からの参加

技術コミュニティとしては、IETFチェアのJari Arkko氏、セキュリティ分野においてはICANNのSSAC(セキュリティと安定性に関する諮問委員会)メンバーや、JPCERT/CCなどのCERTスタッフによる参加がありました。IETFチェアが参加したことは、技術コミュニティの代表者が参加したとされ、オープニングセレモニーでは本人のスピーチがあり、またセッション中でも紹介されていました。

資源管理に関わるRIRs、ICANNや、IETFの運営母体であるISOCからも、それぞれの代表が参加しており、主に資源管理やインターネット運用の観点から意見を述べる立場を取っていました。JPNICからは筆者が、IPv4アドレスの移転を取り巻く状況を中心に議論を行った「Workshop 144: IPv4 markets and legacy space」セッション*にパネリストとして登壇しました。

技術コミュニティや民間組織は、他のグループと比較すると参加者数としてはやや少なかったかもしれませんが、各セッションにおける技術コミュニティからの発言は活発に行われていたように思います。

民間組織としては、Google社、Microsoft社などの欧米の企業や、BT Group社、Telecom Italia社、Orange社などの電話会社、Netnod、INEXなどIX事業者からの参加が見受けられました。特にGoogle社は15名程度が参加し、そのうちの何人かがパネリストとして登壇しており、1民間企業としてはかなり活発に活動をしていました。

◆ 今回のIGFの特徴

フォーラムとして掲げていた全体テーマ(General Theme)は「かけ橋を造る - 成長と持続可能な発展に向けたマルチステークホルダーによる協力の拡張・強化」でした。以下に示すサブテーマをご覧くださいと、非常に多様なテーマを取り扱っていることが確認できると思います。これらのサブテーマに応じて各種ワークショップが色分けされ、開催されていました。

- ・人権、表現の自由、インターネット上の自由な情報の流動(Free Flow)
- ・ダイナミックな連携
- ・セキュリティ：法的および他の枠組み、スパム、ハッキング、サイバー犯罪
- ・アクセス/多様性：成長と持続可能な発展のエンジンとしてのインターネット
- ・インターネットガバナンスの原則
- ・マルチステークホルダーによる協力の原則
- ・トピックごとのオープンフォーラム

このうちバリのIGFでは、米国国家安全保障局(National Security Agency: NSA)による監視活動の問題が明るみに出たタイミングであったため、「The big elephant in the room(無いものであるかのように扱われている大きな問題)」として表現された以下二つのテーマが、対応が迫られる新たな課題として最も注目されていました。

- ・サイバーセキュリティの脅威(Threats of cybersecurity)
- ・広範囲に浸透しているインターネットにおける監視活動(Wide spread surveillance)

具体的な課題が明確であったこともあり、今までのIGFで最も議論内容が充実している会議だったと、複数の参加者から聞いています。

実際、これらの問題は複数のセッションで議題として取り上げられ、政府としての対応、運用コミュニティとしての対応、市民団体からの懸念を共有する場となっていました。米国政府からも10名程度の参加があり、監視を取り扱ったセッションも含め、複数のパネルで登壇していました。

また、2014年5月頃にブラジルでインターネットガバナンスに関するミーティングを開催することがブラジル政府関係者より、オープニングセレモニーをはじめとした各種セッションで紹介されました。IGFとの違いも含めて、詳しくは次号以降のJPNICニュースレターで別途ご紹介する予定です。

会場のネットワーク運用に関わるものとしては、ネットワークがIPv6対応をしており、20%程度のユーザーがIPv6を利用していることが最後のオープンマイクセッションで共有されていました。

◆ プログラム構成

135のワークショップが実に11ものパラレルセッションとして開催され、メインホールでは、以下を取り上げたパネルディスカッションが、テーマごとに行われました。これらはいずれも、今回のIGFでの六つのサブテーマに即したものとなっています。

- ・マルチステークホルダーによる協力における政府の役割
- ・インターネットガバナンスの原則
- ・マルチステークホルダーによる協力の原則
- ・法的およびその他枠組み：スパム、ハッキング、サイバー犯罪
- ・成長および継続的な発展の原動力としてのインターネット
- ・インターネット上の人権、表現の自由および自由な情報の流通

興味のあるテーマでのセッションがあれば、各セッションの発言録(トランスクリプト)が以下よりご覧いただけます。

<http://www.intgovforum.org/cms/igf-2013-transcripts>



● アジア太平洋地域のコラボレーションについて議論したセッション

◆ セキュリティと監視に関する議論

セキュリティや管理をテーマとしたセッションは複数開催されていましたが、特に最終日の10月25日(金)には監視をテーマとしたセッション「TAKING STOCK: EMERGING ISSUES - INTERNET SURVEILLANCE」がメインホールで行われ、中国政府が暗に米国を指して、監視活動を行っている政府を批判する一幕もありました。

このセッションには当事者である米国政府の代表者も登壇しており、米国は市民のプライバシーを尊重していること、議論の余地がある監視活動については情報公開をする指示が大統領から出ていること、そしてIGFで議論することを重視しており、議会で予算が承認されなかったため直前の週末で政府が閉鎖されていたにもかかわらず、十数人で頑張って参加しに来たとの発言がありました。

一方、この問題に対するIETFの立場は、今に始まったことではな

いので必要以上に大騒ぎする必要はない、とはいえ、セキュリティ上必要な対策が取れるよう、また、過度な監視が行われることを防ぐよう、プロトコルの見直しを検討しているというものでした。

また、この他に興味深かったセッションとして、「Google Open Forum」では、それぞれの国におけるインターネットの自由度を調査するプロジェクトが紹介され、Webサイトへのアクセス制限の状況や、その他データを収集することにより、監視の傾向を知ることができると述べられていました。

IGFの会期中、セキュリティについては、以下のような意見なども発表されていました。

- ・現実社会で違法な行為は、オンラインでも違法と見なすべきではないか
- ・インターネットはグローバルだが、法制は国レベルで行っている
- ・技術的な連携に加え、外交ルートから協力を依頼できることも重要
- ・政府間の連携としてのサイバー犯罪条約(通称ブダペスト条約)の紹介
- ・政府、法執行機関、技術コミュニティが連携して対処していくことが大切
- ・セキュリティ対策において、民間組織が政府や法執行機関に対して、どのような情報提供をどこまで行うべきか明確な基準が必要
- ・国レベルではCERTが頑張っているが、地域単位での国をまたいだ連携が必要。CERTが他のCERTと連携してこの役割を果たしていくべき

現に、メインホールでのセッション「FOCUS SESSION (SECURITY): LEGAL AND OTHER FRAMEWORKS: SPAM, HACKING AND CYBERCRIME」では、政府関係者としては米国とスリランカの代表者が登壇し、いずれもCERTとの連携の必要性を重視する立場を取っていました。

このセッションでは、監視について、以下のような意見が表明されていました。

- ・プライバシーと人権を侵害するべきではない
- ・政府がセキュリティの脅威に対応するために求める情報において、基本方針を明確にしておくべき
- ・スウェーデンがIGFの前週に開催されたサイバーセキュリティカンファレンスにて、「監視活動に対する人権に関する7原則」を定義したことを紹介

個人のプライバシーは尊重するべきという点に対する異論はなく、ただし、具体的にどこまでの行為がセキュリティを守る上で許容されるのかという点については、合意事項は確認されていませんでした。



● 閉会式ではAfrINICのAnne-Rachel Inne氏のスピーチの中でモンテビデオ声明についての話がありました

◆ IGFを振り返って

次回のIGFは、2014年9月にトルコ・イスタンブールでの開催が予定されています。この他、2014年には前述のブラジルでのインターネットガバナンスに関するミーティングも開催が予定されており、2013年からIGFの設置開催を決めた世界情報社会サミット(WAIS)開催後10年を迎えた節目となる「WSIS+10」として、現状の検証や今後のあり方を検討する議論も国連で進められています。

インターネットガバナンスを取り巻く状況については、JPNICでも今後、さまざまなイベントなどでご紹介していく予定です。これを読んでくださったみなさんの観点からも、議論されている問題についてご意見がありましたら、ぜひお聞かせください。

◆ 参考情報

IGF : <http://www.intgovforum.org/cms/>
IGF Bali: <http://igf2013.or.id/>

(JPNIC インターネット推進部/IP事業部 奥谷泉)

※ IGF2013 main session and workshop transcripts
<http://www.intgovforum.org/cms/igf-2013-transcripts/1484-ws-144-markets-and-legacy-space>



● ソーシャルイベントでのバリ舞踊

第88回IETF報告



全体会議報告

第88回IETF Meetingは、2013年11月3日(日)から11月8日(金)の間、カナダのバンクーバーにて開催されました。

11月の初め日本はまだ暖かく、「バンクーバーは最低気温3度、最高気温9度です」と聞いて、「何を着て行こうか?冬の用意かな」という状態でした。到着してみるとバンクーバーはすっかり秋、きれいな紅葉でした。さすがに日本の装いのまま来た人は慌ててコートやマフラーを現地調達していました。会議が終わって、バンクーバーから日本に戻ってくると日本も寒くなり、私たちにはIETF会議がちょうど耐寒訓練になったようでしたが、日本にいた人からは「バンクーバーから寒さを持ってきた」と言われてしまいました。

さて、ここでは11月6日(水)に開かれた「IETF Operation and Administration Plenary」と「Technical Plenary」の様子について、感想を交えて報告します。今回は午前中に「Technical Plenary」、夕方に「Operation and Administration Plenary」という、1日にPlenaryが集中するスケジュールとなっていました。

◆ Technical Plenary

午前中の「Technical Plenary」では、IAB(Internet Architecture Board) Chair、IRTF(Internet Research Task Force) Chair、RSE(RFC Series Editor) and RSOC(RFC Series Oversight Committee) Chairの報告と、「Technical Topic: Internet Hardening(インターネットのセキュリティ強化)」の発表がありました。

○IAB Chair Report

はじめにIAB ChairのRuss Housley氏より、2014年のICANN Nominating Committee(NomCom; 指名委員会)にRuss Mundy氏を指名したとの報告がありました。

IABは、ISOC(Internet Society)、IEEE(The Institute of

Electrical and Electronics Engineers, Inc.)、W3C(World Wide Web Consortium)とともに、OpenStand主義^{※1}への支持を表明しました。これらの団体は、技術革新や国境を越えた商取引のために、効果的かつ効率的な標準化プロセスを作り出してきましたが、今後はこのような「標準化原則」の重要性を掲げ、グローバルなオープンスタンダードの新たな枠組みの確立を目指すとのことです。

また、IABチェアは九つの他のインターネット団体とともに、「モンテビデオ宣言」^{※2}に署名しました。

それ以外にIABが最近発行したその他の文書としては、RFC 6950:「Architectural Considerations on Application Features in the DNS」が報告されました。

続いて、IABの主催するワークショップの予定が発表されました。2013年12月に英国ケンブリッジで「インターネット技術の採用と移行に関するワークショップ(Workshop on Internet Technology Adoption and Transition; ITAT)」が、2014年2月に英国ロンドンで「インターネットのセキュリティ強化に関するワークショップ(Workshop on Internet Hardening)」が開催されるそうです。

それから、IABが執筆したRFCとして、2013年には以下のものが発行されました。

- RFC 6852: Affirmation of the Modern Paradigm for Standards
- RFC 6912: Principles for Unicode Code Point Inclusion in Labels in the DNS
- RFC 6943: Issues in Identifier Comparison for Security Purposes
- RFC 6949: RFC Series Format Requirements and Future Development
- RFC 6973: Privacy Considerations for Internet Protocols
- RFC 6950: Architectural Considerations on Application Features in the DNS

上記のRFC以外にも、インターネットドラフトも複数執筆中という事です。

○IRTF Chair Report

IAB Chair Reportの次には、IRTF ChairのLars Eggert氏より、IRTF Chair Reportがありました。

IETF Meetingの期間中に開催されるIRTF Meetingは、Network Complexity(NCRG; ネットワーク複雑性研究グループ)、Software-Defined Networking(SDNRG; ソフト

ウェア定義ネットワーク研究グループ)、Internet Congestion Control (ICCRG; インターネット輻輳制御研究グループ)、Information-Centric Networking (ICNRG; 情報セントリックネットワーク研究グループ)、Network Management (NMRG; ネットワーク管理研究グループ)、Network Coding (NWCRG; ネットワーク符号化研究グループ [提案])の、六つの研究グループ (Research Group; RG) です。これ以外に、IRTF Open Meetingを5日(火)の午後で開催しました。

IRTF関係のRFCとして、Scalable Adaptive Multicast (SAMRG; スケーラブル適応マルチキャスト研究グループ)からRFC 7019: "Application-Layer Multicast Extensions to Resource Location And Discovery (RELOAD)"が発行されました。

続いて、2013年度のネットワーク研究賞 (Networking Research Prize) 4本のうちで、今回の発表分になっていた Idilio Drago氏の受賞が発表となりました。また、2014年度の Networking Research Prize候補の募集をしているそうです。

○ RSE and RSOC Chair Report

RSE and RSOC Chair Reportでは、RSEメンバーの紹介がありました。

それから報告として、IAOC (IETF Administrative Oversight Committee)がRFC Production Center and RFC Publisher Statementsの作成および契約と、RFC Series Editor契約のレビューと助言のまとめを完了したそうです。その他には、RFC Style Guideの議論が続いており、RFC format WGで作業がされています。

○ Technical Topic: Internet Hardening

続いて、今回のテクニカルトピックは「Internet Hardening」でした。IABのAlissa Cooper氏が司会を務めました。

この話題は、米国国家安全保障局 (NSA) の盗聴問題に端を発して、「インターネットを敵の監視から守ることができるのか?」「誰/どのような組織が働かなくてはならないのか?」という課題について考えてみようというものでした。

最初にBruce Schneier氏がイントロダクションとして、現在のインターネットを取り巻く状況について話をしました。次にBrian Carpenter氏は、これまでのIETFで何が良かったかを話しました。1990年代半ばにはEコマースのために強い暗号が必要となりましたが、多くの政府はより強力な暗号の使用を制限したがりました。IETFでも、この束縛について議論を重ねました。

その後、政府機関の方がIETFに来たこともありました。Stephen Farrell氏は、IETFアクティビティのポテンシャルについて話をしました。IETFはHTTPやTLS、あるいはIPsecを使い、技術的なアプローチがあることを示しました。オープンマイクでも「国ごとのポリシーの問題もあるが、技術的に取り組んでいくことも重要である」といった発言がありました。



● Technical Plenaryの様子

◆ Operation and Administration Plenary

夕方の「IETF Operation and Administration Plenary」では、最初にスポンサーのHuawei社より挨拶がありました。今回のスポンサーTシャツには、IETFのキーワードを組み合わせたデザインが使われていましたが、それを見せて「これがIETFです」と笑わせていました。

続いてIETF ChairのJari Arkko氏より、今週(今回のIETF)のトピックとして、これからのトランスポートプロトコル、WebRTCの重要な決定、広がる監視と可能なセキュリティ、その他の進展、HTTP2.0やTLS1.3の作業が継続していることが挙げられました。

その次には、参加者の内訳や新しい取り組みの報告がありました。今回は54の国と地域から1,142人が参加しました。初めての参加者は123人でした。前回のフロリダでは1,407人でしたので、少し減っています。地域ごとの集計では、米国、中国と続き、日本、カナダの順ですが、日本とカナダは同じぐらいでした。

今回、新たにビデオ中継とソーシャルメディア活用の試みをしました。YouTubeでは最大276人が見ていました。トータルでは、7日(木)の15:30までで748人が見ていたそうです。Twitterでは「#IETF88」のタグがついたものが827ツイート、Facebookでは327の「いいね!」がつけました。

また、IETFとしてのアンチハラスメントポリシーを作ろうとしているそうです。前回に引き続き実施されているメンタープログラムには、58人が参加しました。それから「Top 10 Things to Know Before Your First IETF Meeting」という、IETF入門ビデオが作成されているそうです。

次に、IAOCチェアのChris Griffiths氏とIADのRay Pelletier氏から、報告がありました。今回は参加費を払った参加者とスポンサーが若干予定より多く、収支見通しも予定より上回りそうだと報告がありました。ベルリンの収支決算の最終報告では、参加者は予定より多かったのですが、ホストがつかなかったことや、付加価値税を支払わなければならなかったことにより、若干のマイナスとなりました。次回第89回のミーティングは、ICANNがホストになることが発表されました。

次回のIETF Meetingは、2014年3月2日(日)から3月7日(金)にかけて、英国ロンドンにて開催されます。

(アラクサラネットワークス株式会社 新善文)

※1 Open Stand: Principles for The Modern Standard Paradigm
<http://open-stand.org/>

※2 インターネット関連10団体が「今後のインターネット協力体制に関するモンテビデオ声明」を発表
<https://www.nic.ad.jp/ja/topics/2013/20131008-01.html>

IPv6関連WG報告 ~6man WG, v6ops WGについて~

カナダのバンクーバーにて開催された第88回IETFのWorking Group (WG)のうち、筆者が会合に参加したIPv6に関連するWGの中から6man WGとv6opsWGについて、主な議論の概要をご紹介します。

◆ 6man WG (IPv6 Maintenance WG)

6man WGは、IPv6プロトコルのメンテナンスを目的としたWGです。まず、最初のチェアからのプレゼンでは、6man WGの新しいチャーターとマイルストーンが紹介され、U/Gビットやフラグメンテーション、拡張ヘッダに関する議論を行うことが示されました。なお、IPv6 over Foo (何らかの仕組み上でIPv6を使用)に関する議論は、新設された6lo (IPv6 over Networks of Resource-constrained Nodes) WGにて行われることになっています。その他にも、産業用無線ネットワークへの適用を目的とした6tisch (IPv6 over the TSCH mode of IEEE 802.15.4e) WGも新設されるなど、M2M (Machine to Machine) やIoT (Internet of Things) 関連の標準化も活発化してきている状況です。

今回のセッションで筆者が特に興味を持ったのは、Deprecating EUI-64 Based IPv6 Addresses (draft-gont-6man-deprecate-eui64-based-addresses-00)で、「Modified EUI-64 FormatのようなHardware AddressをInterface ID (IID) に埋め込むようなIID生成方法は、セキュリティの観点から望ましくないため廃止しよう」という提案です。具体的には、ノードはHardware AddressをIIDに含めてはいけなかったことや、

代替となるIID生成方法として、「A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (IPv6 Stateless Address Autoconfiguration) (IPv6ステートレスアドレス自動構成において意味的に理解しにくいインタフェースIDの生成方法) (draft-ietf-6man-stable-privacy-addresses-16)」を使用すべきとしています。

本提案をWGアイテムとすべきかどうかについての会場のハミングでは、賛同者多数となったものの、要求水準 (Requirement Level) をMUST NOTにすべきかSHOULD NOTにすべきかについては、検討が必要ということになりました。これを受けて、現在メーリングリスト (ML) 上にて、WGで採択するかどうかの再確認が行われている状況です。

その他のトピックとしては、マルチキャストの抑制や省電力が求められるネットワーク (例えば、ワイヤレスやバッテリー駆動のデバイスなど) におけるND (Neighbor Discovery、近隣探索) の最適化を行った方式である、Wired and Wireless IPv6 Neighbor Discovery Optimizations (有線/無線でのIPv6近隣探索最適化) (draft-chakrabarti-nordmark-6man-efficient-nd-04) や、プライバシーやセキュリティの観点からさまざまなアドレス生成の方式について比較検討、整理を行っている Privacy Considerations for IPv6 Address Generation Mechanisms (IPv6アドレス生成メカニズムにおけるプライバシーの考慮) (draft-ietf-6man-ipv6-address-generation-privacy-00) の議論が行われるなど、IPv6普及による実践的なテーマへと議論の軸が移ってきていることが感じられました。

□ 6man WG

<http://tools.ietf.org/wg/6man/>

□ 第88回IETF 6man WGのアジェンダ

<http://www.ietf.org/proceedings/88/agenda/agenda-88-6man>

◆ v6ops WG (IPv6 Operations WG)

v6ops WGは、IPv6運用上の問題解決のための議論を第一優先として、その他にはIPv6普及に向けた運用上のガイドラインなども取り扱うWGです。

今回のセッションで筆者が特に興味を持ったのは、DHCPv6/SLAAC Address Configuration Interaction Problem Statement (DHCPv6/SLAACアドレス構成対応問題に関するステートメント) (draft-liu-bonica-v6ops-dhcpv6-slaac-problem-00) です。一般的なホストでは、DHCPv6やStateless Address Autoconfiguration (SLAAC) を実装していますが、これらの挙動はRA (Router Advertisement、ルータ広告) の「A (Autonomous address configuration)」「M (Managed address configuration)」「O (Other configuration)」の各

フラグ状態によって変化します。なお、このドキュメントでは、Windows 7、Linux、Mac OS X、iOS、Androidの各ホストにおける挙動が異なっている点が指摘されています。例えば、Mフラグを「M=1」から「M=0」に変化させた場合、Windows 7ではDHCPv6にて取得したアドレスをリリースするのに対し、LinuxやMac OS Xではアドレスをリリースせずにそのまま保持し続けるといったように、ホストにより挙動が明らかに異なっています。

このようにホストごとに挙動が異なっているのは、RFC2462^{*1}やRFC4862^{*2}で定義されてきたSLAACの仕様、曖昧さが残っていることに起因しています。

本ドキュメントについて、会場では問題点の共有が行われ、問題がある(Problem Statement)として6man WGに対して提示すること、およびオペレータ向けの現時点でのガイドラインとして、v6ops WGのWG Itemとして取り扱うことで検討が進んでいます。

その後、本ドラフトは2013年11月26日(火)に、draft-ietf-v6ops-dhcpv6-slaac-problem-00として、WG Draftとして発行されています。

その他のトピックとしては、T-Mobile USA社が464XLATを利用したIPv6サービスを開始したことに伴い、CLAT(customer-side translator)内部で必要となるローカルなIPv4アドレスについて、IANAから適切なアドレスプールの割り当てを要求する464XLAT CLAT IPv4 Address(draft-byrne-v6ops-clatip-00)の提案や、モバイルネットワークにおいてローミングを行う際の想定シナリオや、それに伴いローミングに失敗するケースの分析などがされているIPv6 Roaming Behavior Analysis(draft-chen-v6ops-ipv6-roaming-analysis-02)など、実際のIPv6サービスに関連する提案も増えてきている状況です。

なお、今回のv6ops WGで最初に行われたプレゼンでは、Microsoft社のChris Palmer氏から、Microsoft社のTeredoサービスとXbox Oneに関するプレゼンが行われ、Windows向けのTeredoサービスに関しては、2014年の前半にはサービスを終息する予定であるとの報告がありました。またXbox Oneに関しては、Teredo + IPv6 IPsecによるP2P Connectionの確立を行っており、IPv6 Nativeよりも時には信頼性が高い側面があることなどが紹介され、身近なゲーム機での実装ということもあって、多くの参加者が興味を持って聞いていました。

また、11月5日(火)の昼には「IPv6 -- What Does Success Look Like?」と題して、恒例のISOC Briefing Panelが開催されたり、11月7日(木)の夜にはBits-N-Bitesにて、Huawei社やChina Telecom社がSDN(Software-defined networking)や、NFV(Network Functions Virtualization)の要素を取り入

れた「OpenV6 : Unified IPv6 Transition」のデモを行うなど、IPv6に関連する話題が盛りだくさんの第88回IETFでした。

□ v6ops WG

<http://tools.ietf.org/wg/v6ops/>

□ 第88回IETF v6ops WGのアジェンダ

<http://www.ietf.org/proceedings/88/agenda/agenda-88-v6ops>



● Bits-N-Bitesでは多くの参加者が交流を深めていました

(NECアクセステクニカ株式会社 川島正伸)

※1 RFC2462 "IPv6 Stateless Address Autoconfiguration"
<http://www.ietf.org/rfc/rfc2462.txt>

※2 RFC4862 "IPv6 Stateless Address Autoconfiguration"
<http://www.ietf.org/rfc/rfc4862.txt>

セキュリティ関連WG報告 ~ RPKIの動向 ~

本稿では、セキュリティ関連WGのうち、インターネットのルーティングセキュリティ技術として注目されている、リソースPKI(Resource Public-Key Infrastructure; RPKI)の動向をまとめてお送りします。

RPKIは、IPアドレスの記載された電子証明書(以下、リソース証明書と呼びます)と、AS番号が記載されたROA(Route Origin Authorization)と呼ばれる電子署名のついたデータを使って、不正な経路情報を検出できるセキュリティの技術です。

今回のIETFでは、WGでの議論に加えて、LACNICからエクアドルでのRPKI導入に関する興味深い発表がありましたので、SIDR WGの報告と併せて、このLACNICのプレゼンテーションについても取り上げます。

◆ SIDR WG - BGPSECの仕様策定は足踏み状態、Origin Validationの改良が続く

SIDR(Secure Inter-Domain Routing)WGは、インターネットにおける経路制御のための、PKI技術を使ったセキュリティの仕組み、すなわちRPKIを使ったセキュアなルーティングの仕様を検討しているWGです。第88回IETFミーティングでは、2時間半のミーティングが1回行われました。参加者は40名ほどで、多くが常連の顔ぶれでした。

SIDR WGでは、経路情報のAS番号とIPアドレスの組み合わせを確認するOrigin Validation(経路広告元ASの検証技術)と、ASパスを確認するPath Validation(ASパスの検証技術)の二つの技術課題に取り組み、この二つが合わさったものはBGPSECと呼ばれています。WGでは、Origin ValidationのRFC化が2013年初頭に済み、今度はPath Validationのドキュメントを準備している段階です。

今回のミーティングで行われた、主なプレゼンテーションを簡単に紹介します。

□ An Out-Of-Band Setup Protocol For RPKI Production Services(RPKI発行サービスのための out-of-band の鍵セットアッププロトコル)

リソース証明書は、発行先と発行元の間でセキュアな通信を行うために、最初におのおのの公開鍵や名称を交換しますが、そのプロトコルの策定を提案するプレゼンテーションです。特にプロトコルの定まっていない現在は、USBメモリや電子署名付きのメールなどさまざまな方法で行われています。

□ A Publication Protocol for the Resource Public Key Infrastructure(RPKIのデータ公開プロトコル)

リソース証明書やROAを公開するための、XML(Extensible Markup Language)ベースのプロトコルの提案です。現在はrsyncが使われていますが、この公開プロトコルに転送プロトコルなどを加えることで、rsyncの代替になることを含めて検討されています。

□ A Fail-safe Mechanism for the RPKI(RPKIのためのフェイルセーフの機構)

特定のROAの署名検証に使われる認証局(Certificate Authority; CA)を、通常のRIRのものと別にする事ができる方式の提案です。RIRと異なるCA、すなわちRIRのプリフィクスを扱えるLTAM(Local Trust Anchor Management)に代わる方式で、独自のRPKIのツリー構造を構築できるようにするために提案されています。

WGで行われている議論は、IPアドレスの移転への対応のように、Origin Validationの仕組みを補強したり、特定の用途で使うた

めに考えられているもので、まだまだPath ValidationのRFC化に向けた議論には至っていない状況です。日本国内ではAS Pathを使った経路フィルターが導入されているASが多いと言われており、今後のPath Validationの動向が気になるところです。

◆ エクアドルにおける急速な導入 - 総プリフィクスの90%がカバーされる

エクアドルは、ラテンアメリカの地域インターネットレジストリ(RIR; Regional Internet Registry)であるLACNICから、IPアドレスの割り振りを受けている国です。経路情報としては、8,800ほどのプリフィクスが観測されています。

2013年9月に、このうちの90%をカバーするリソース証明書とROAが、一斉に発行されました。ROAにはIPアドレスとAS番号が書かれているため、インターネットの他のASからROAに書かれているIPアドレスが経路広告された場合には、検出することができます。検出自体はエクアドル国内でなくてもできるため、例えばヨーロッパやアジアにあるASであっても、エクアドル国内のプリフィクスが経路広告されたときには、それを観測できることとなります。

IETFミーティングの初日に行われたIEPG(Internet Engineering and Planning Group)ミーティングでは、LACNICのスタッフであるSofia Silva Berenguer氏によって、このイベントについてプレゼンテーションされました。

RPKI and Origin Validation Deployment in Ecuador
<http://iepg.org/2013-11-ietf88/RPKI-Ecuador-Experience-v2b-1.pdf>

今回、RPKI導入の主役となったのはNAP.ECというIXPで、エクアドル国内の97%のネットワークを収容しています。RPKIを導入するイベントは2013年の7月と9月に行われ、9月にROAの一斉発行が行われました。このイベントは、RPKIが普及しないために導入効果が上がらず、同時にそのことが普及の足止めになっている、いわゆる「鶏卵問題」を解消するため、LACNICの協力のもと開催に至ったとのことでした。ROAの発行だけでなく、NAP.ECで経路情報を配布しているルートサーバに、RPKIの電子署名の検証を行う「RPKI cache」が導入されているとのこと。ただし、検証結果に応じてルートサーバの挙動を変えるわけではないようです。

今後、不適切な経路情報の検出が実際にはどの程度できるようになり、インターネット経路制御の運用に役立つかが注目されます。今回の話題は、LACNICのブログに詳しく掲載されています。

Deployment of RPKI and BGP Origin Validation in Ecuador, LACNIC
<http://labs.lacnic.net/site/RPKIandOriginValidationEcuador>

RPKIの可視化サイトで知られている、オランダにあるSurfnetのRPKI Dashboardによると、2013年12月12日現在、RPKIを使って経路広告元ASの判定ができるプリフィクスは22,808あります。国際的な経路情報の総量は515,101観測されていることから、そのうちの4.4%ほどであることがわかります。またROAの発行の段階で、既にAS番号が実際の経路と異なっているものが1,196あります。従って、ISPなどにおいて実運用されているとは、まだまだ考えにくい段階にあると言えます。

今後、実際にRPKIが使われていくためには、発行数を増やすだけでなく、IPアドレス担当者と経路制御の担当者が連絡し合い、正しいASが入ったROAが発行されていく必要があると考えられます。

□ RPKI Dashboard
<http://rpki.surfnet.nl/>

(JPNIC 技術部 / インターネット推進部 木村泰司)



● バンクーバー市内の様子

DNS関連WG報告

本稿では、IETF 88におけるDNS関連の動きとして、dnsop WG、dnssd WG、dnsext WGの概要を報告します。dnsext WGは、メーリングリスト(ML)での議論の報告になります。

◆ dnsop WG報告

今回のIETF 88はバンクーバーにて開催され、dnsop WGの会合が開催されました。会合の時間は90分であるにもかかわらず、多くの議題が詰め込まれており、案の定時間が不足し消化不良に感じました。

まず、DNS Prefetchの性能評価に関する報告がなされました。

これはdraft-wkumari-dnsop-hammerにて提案されている、Hammer Timeを用いたDNSレコードPrefetch(事前読み込み)の有用性を確認するための性能評価です。SURFnetにて、ユーザーにリゾルバDNSサーバとして提供されているUnboundを用いて、データ収集が行われました。Unboundの設定を変更し、Prefetchが有効な場合と無効な場合とで、ユーザーからのクエリ数の比較と、キャッシュ的中率の比較がなされました。結論としては、Prefetchによる性能向上は、ごく限られた範囲と限られた名前へのみ見られ、全体として大きな性能向上に貢献するものではない、との結果になりました。この結果を踏まえ、draft-wkumari-dnsop-hammerを実データの解析結果を含んだ新たなinternet-draftとすることが合意されました。引き続きDNSレコードPrefetchの有用性は議論されるようです。

次に、draft-hardaker-dnsop-csyncnに関する発表と議論が行われました。この文章は、子ゾーンの先頭に存在する親ゾーンを示すNSレコードを、親ゾーンが自動的に取り込むことによって、委譲関係の更新を行うという提案です。従来は、子ゾーンを担当するDNSサーバを変更する場合には、子ゾーンのゾーンファイル先頭にあるNSレコードを更新し、かつ親ゾーン中にある委譲のためのNSレコードとグルーレコードを更新するための依頼を、親ゾーンの管理者に対して行う必要がありました。この提案は、それを自動化するものです。この提案に対しては、レジストラは独自のプロトコルでそれを実現しているため、本当に必要なかという意見や、レジストラだけではなく通常のゾーン委譲でも有効だとする両方の意見が出され、継続議論となりました。

さらに、draft-kumari-ogud-dnsop-cdsに関する発表と議論が行われました。これは、CDSとCDNSKEYという二つの新たなリソースレコードを用いて、DNSSECの更新鍵を子ゾーンから親ゾーンに対して通知する手法を提案しています。ここ数回のdnsop WGの会合にて議論されてきた話題です。議論では、csyncと混乱しやすいので違いを明確にした方がいいという意見や、新たなリソースレコードを追加するのでdnsop WGの範疇ではないのでは、といった意見が出されました。引き続き議論が行われていくようです。

また、draft-fujiwara-dnsop-ds-query-increaseに関する発表と議論も行われました。これは株式会社日本レジストリサービスの藤原和典氏による発表であり、DNSSECの普及にともないJPゾーンを受け持つDNSサーバに対するDSレコードの問い合わせ数が増加していることを報告したものです。この報告に対して会場からは、仕様通りの動作なのでそれほど大きな問題ではない、といった意見が大勢を占めました。あまり注目されなかったようです。

この他にも、複数のドラフトに関する発表がありました。その中で特に今後の議論に関連すると思われるものを抜粋して紹介します。

まず、draft-jabely-dnsop-as112-dnameですが、通称AS112と呼ばれる、プライベートアドレス空間の逆引きを担当するDNSサーバにおいて、その担当するゾーンを動的に増減させる手法を提案した文章です。この提案に関しても、ここ数回のdnsop WG会合で議論されてきました。APNICにて試験を行った結果、問題なく機能しそうだという報告を受けたため、WGドラフトとして議論が継続されることになりました。

draft-jabley-dnsop-flush-reqsは、リゾルバDNSサーバに対して、保有するリソースレコードのキャッシュを消去するための通知機構を提案したものです。前回のIETF 87にて一度却下された提案であるため、再度その必要性を提案する文章となっています。引き続き議論が行われると思われまます。

最後に、edns-tcp-chain-queryならびにedns-tcp-keepaliveに関して報告します。これは、DNSSECの導入によってDNSサーバと通信する回数や、通信のデータサイズが大きくなっているため、名前解決に時間がかかるという問題を解決するための提案です。具体的には、DNSSECに関連する複数のリソースレコードを取得するにあたって、UDPパケットにて複数回通信を行うのではなく、一つのTCPセッションを用いて通信を行うという手法です。これにより、DNSサーバに対するTCPクエリ数は増加しますが、結果として問い合わせにかかる時間を短縮できるという提案です。この提案の有用性については、会場からも賛同する声が多くあつたため、今後も議論されていくと思われまます。

◆ dnssd WG報告

Extensions for Scalable DNS Service Discovery(dnssd WG)は、このレポートでは初めて取り上げるWGで、DNSでサービスを探し出すスケーラブルな拡張機能を検討するものです。

dnssd WGの会合は、2時間の枠にて開催されました。まず、dnssdのサービスに利用するためのTLDを確保しようという提案がなされました。これに関して、本当にTLDが必要なのかという意見や、TLDとしての.localは既にあるサービス発見と混乱しやすいといった意見、またTLDでなくても.arpaの下のドメインでもいいのではないか、といった議論がなされました。最終的に、急いでTLDを確保する必要はない、という合意が得られました。

次に、draft-lynn-dnssd-requirementsに関する発表がありました。この文章は、dnssd自体の必要性に関して述べた文章です。サービス発見に関して、DNSを用いるのが規模的に優れているといった意見や、DNSをこういった用途に使うべきなのかといった根本的な意見が交換されました。結論としては、現状のDNSを壊さない限りはいいのではないかと、という意見にまとまりました。

その他にも、dnssdのアーキテクチャに関する発表と議論がなされました。ユニキャストのDNS応答を用いて、どのようにサービ

ス発見を行うか、またクライアントにどのように通知するか、といった議論がなされました。dnssd WGはまだ初期段階であり、今後議論が続いていくものと思われまます。

◆ dnsext WG報告

dnsext WGは、既にIETFでの会合を開催しないため、今回もメーリングリストでの議論を中心に報告します。前回のIETF 87からの議論としては、SPFレコードの扱いに関する議論が続けられて行われました。SPFリソースレコードを用いるのではなく、TXTレコードにSPF情報を書くのが一般的となっているため、SPFリソースレコードを廃止するという提案です。WGの会合が開催されないため、メーリングリスト上の議論だけでは明確な結論は出ませんでした。廃止しても良いという意見が多く見られました。

また、draft-wouters-edns-tcp-chain-queryに関する議論もありました。これは、DNSSECなどのサイズの大きなデータをDNSサーバとやり取りする場合、UDPではなくTCPを率先して用いるというEDNSオプションの提案です。さらに、TCPセッションを確保したままにする、draft-wouters-edns-tcp-keepaliveという提案もなされました。この提案に関しては、有用だとする意見が出され、メーリングリストで議論が継続されています。

他には、draft-gieben-auth-denial-of-existence-dnsに関する議論や、ゾーン自体の動的な追加、削除を行うプロトコルを定義してはどうか、などの提案がなされましたが、いずれも散発的な議論で終わりました。

(JPNIC DNS運用健全化タスクフォースメンバー / 東京大学 情報基盤センター 関谷勇司)



● 今回の会場となったHyatt Regency Vancouver