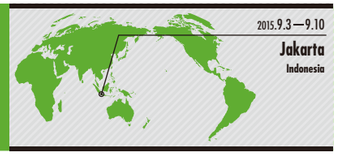
APNIC 40カンファレンス報告



全体概要およびアドレスポリシー関連報告

アジア太平洋地域の地域インターネットレジストリ（RIR）であるAPNICのカンファレンスが、2015年9月3日（木）～10日（木）にかけて、インドネシアのジャカルタで開催されました。本稿では、APNIC 40カンファレンスの模様をレポートします。

◆ APNIC 40カンファレンスの概要

主催者からの報告によると、49の国や地域から612名の参加登録があり、521名が実際に会場に足を運んだそうです。そのうちインドネシアからの登録者は360名程度とAPNICミーティングへ高い関心を寄せていたことがわかります。APNICカンファレンスは通常、春にAPRICOTと共催で1回、秋に単独で1回開催されますが、今回は秋のAPNICカンファレンスとしては、最大規模となったようです。また、カンファレンスではフェローシッププログラムが用意されており、アジア各地から毎回30名程度が利用するそうです。今回は、27名がこのプログラムを利用して参加していました。また、このプログラムとは別に、APRICOT-APAN 2015日本実行委員会が用意した「APNIC 40カンファレンス参加支援プログラム」を利用して、日本から4名が参加していました。いくつかのセッションでは最前列に陣取って、内容を聞き漏らすまいと発表を真剣に聞く姿が印象的でした。

これまでと同様に、会期前半は「ワークショップ」が開催されました。6日（日）からは「チュートリアル」「APOPS（Asia Pacific Network Operators Forum）」「SIG（Special Interest Groups）」「BoF（Birds of a Feather）」「AMM（APNIC Member Meeting; APNIC総会）」の会議・セッションが開催されました。これら以外にも、APNICとの関連の深い、APIX（Asia Pacific Internet Exchange Association）やAPTLD（Asia Pacific Top Level Domain Association）が主催する会議の時間が設けられていました。

当日の資料、ビデオ、発言録は、次のAPNICカンファレンスのページに掲載されています。今回参加できなかった方や現地での発言を聞き逃した方も、これらの資料を一度ご覧になってみてはいかがでしょうか。

program - APNIC40
http://conference.apnic.net/40/program

今回はこれらのセッションの中から、ポリシー提案の結果を中心にご紹介します。

◆ ポリシー提案の結果について

今回は、3点のポリシー提案について議論が行われました。いずれも、継続議論となっている提案です。議論の結果、2点の提案がコンセンサスとなり、1点の提案が継続議論となりました。以降、提案の内容と結果をご紹介します。提案背景や、前回のAPNIC 39カンファレンスではどのような議論が行われたかについては、前号のニュースレターNo.60でご紹介していますので、次のURLも併せてご覧ください。

・APRICOT 2015におけるAPNIC 39カンファレンス報告
https://www.nic.ad.jp/ja/newsletter/No60/0610.html

（1）小規模ネットワークへのIPv4 PIアドレス割り当て基準変更（提案番号：prop-113）	
提案者	Aftab Siddiqui氏、Skeeve Stevens氏
概要	IPv4プロバイダ非依存（PI; Provider Independent）アドレスの割り当て基準を以下の通り変更する。ただし、「3ヶ月以内に申請サイズの25%、1年以内に50%を利用する計画を示す」という点については変更しない。
変更前	プロバイダ集成可能（PA; Provider Aggregatable）アドレスで既にマルチホームしている、または1ヶ月以内にマルチホームする予定がある。
変更後	PAアドレスで既にマルチホームしている、または/24以上のPAアドレスの割り当てを受けており、マルチホームする意志がある、または6ヶ月以内にマルチホームでアドレスを経路広告する意志がある。
提案の詳細	http://www.apnic.net/policy/proposals/prop-113
結果	コンセンサス

前回のカンファレンスでは、会場から出された意見を踏まえた改定案が議論の最中に投稿されるなど、活発な議論が繰り広げられました。ポリシー変更の必要性や変更内容の詳細について、前回の議論において一通り確認されている状況にあることから、今回は、改定案に賛同する意見がいくつか表明されたほかは、前回のように時間を超過するほどの活発な議論は行われませんでした。

インドやパキスタンといった南アジア地域からの参加者の多くが、改定案に賛同する意見を表明していました。経済発展目覚ましいこれらの地域の企業にとって、IPv4アドレスの分配を受けられる可能性が増えることで、ビジネスの展開を加速させることができるのではないか、と考えているようでした。

（2）AS番号割り当ての基準変更（提案番号：prop-114）	
提案者	Aftab Siddiqui氏、Skeeve Stevens氏
概要	AS番号の割り当て基準を以下の通り変更する。
変更前	マルチホームする、かつAS番号の割り当て予定のネットワークが、上流プロバイダの外部経路制御ポリシーとは異なり、明確に定義された単一のものである。
変更後	既にマルチホームしている、またはAPNICからPIアドレスの割り当てを受けており、将来マルチホームする意志がある。
提案の詳細	http://www.apnic.net/policy/proposals/prop-114
結果	コンセンサス

提案の議論に先立って、APNICのGeoff Huston氏からは、APNICで管理する「/8相当の最後のAPNICにおけるIPv4未割り振り在庫」や「IANAからAPNICに再割り振りされたIPv4アドレス在庫」に関する発表が行われていました。

「/8相当の最後のAPNICにおけるIPv4未割り振り在庫」からの割り振りアドレスでは、割り振りが行われているにもかかわらず経路情報が広告されていないIPv4アドレスが、25%程度あることが報告されていました。提案者はこの報告内容を取り上げて、AS番号がより容易に割り当てられるようになることで、こういったIPv4アドレスの経路情報広告促進につながるのではないかというコメントを出していました。

こちらの提案についても、提案番号：prop-113と同様に、一通りの議論と確認が行われている状況にありましたので、改定案に賛同する意見がいくつか表明されるにとどまりました。北米地域を管轄するARINや南米地域を管轄するLACNICにおいても、今回の提案と同様にAS番号の割り当て基準が変更されています。また、ヨーロッパ地域を管轄するRIPE NCCにおいても議論中の状況にありますので、今後の動向を追っておく必要がありそうです。

（3）WHOISでのフィルタリング情報提供（提案番号：prop-115）	
提案者	廣海緑里氏、藤崎智宏氏
概要	IPv4では「ポート番号」を、IPv6では「割り当てアドレスサイズ」の情報をWHOISに追加し、これらの情報でも登録情報を検索できるようにする。
提案の詳細	http://www.apnic.net/policy/proposals/prop-115
結果	ポリシーSIG MLでの継続議論

前回の議論と同様に、WHOISを利用して情報提供を行うことについて、疑問や懸念を示す意見が表明されていました。また、韓国の国別インターネットレジストリ（NIR）であるKRNICでは、いくつかの大手ISP事業者の担当者に対して、提案内容を実装した場合に考えられる影響などについて、事前に意見照会をしたそうです。ISPの担当者からは、WHOISの登録内容は攻撃やSPAM送信の対応の際に利用されていることや、登録にはかなりの業務量が必要となるため、提案には反対するという意見が多く寄せられたとのことです。

疑問や懸念を示す意見が表明される一方で、特にIPv6の情報提供については賛同する意見が表明されていました。提案はメーリングリスト（ML）に差し戻して、継続して議論を行うことがチェアから発表されましたが、MLでの議論と並行して、WHOISでの情報提供が適切かどうか、どのような情報を提供することが適切かといった、それぞれの点について調査が行われる予定です。

◆ IANA機能の監督権限移管に関する議論

2014年3月に発表された、米国商務省電気通信情報局（NTIA）によるIANA監督権限移管に関する議論については、移管後の体制を検討し、提案することに責任を持つICG（IANA Stewardship Transition Coordination Group）が統合提案を作成し、2015年9月8日（火）を締め切りとして意見募集を行っていました。APNICカンファレンスではこれまでも、本件に関するセッションを開催してきましたが、セッションの当日に締切日を迎えるということもあり、APNIC地域からの意見提出に向けて呼びかけが行われました。

セッションでは、ICANNから理事長のSteve Crocker氏とIANA部局の責任者のElise Gerich氏、RIRからICGのメンバーを務めるAPNIC事務局長のPaul Wilson氏とAFRINIC CEOのAlan Barrett氏、全RIRの調整機関であるNRO（Number Resource Organization）ECからChiarのAxel Pawlik氏、各RIRコミュニティの提案をまとめるCRISP（Consolidated RIR IANA Stewardship Proposal）チームからChairの奥谷泉（JPNIC）が登壇しました。セッションは、それぞれの立場からIANA監督権限移管への関わりを紹介する形式で進められました。ここでは詳細までお伝えすることはできませんが、番号資源の分野に限らず、IANA監督権限移管への関心を持つ参加者は多かったのではないでしょうか。セッション中に放映された、NRO制作のIANA監督権限移管についての説明ビデオ（日本語版）は、次のURLから参照することが可能です。ぜひ一度ご覧ください。

IANA Stewardship Transition Update: what Numbers folk need to know
［IANA監督権限の移管: 現状はどうなっているのでしょうか?］
https://www.youtube.com/watch?v=B5n3XgZTaac

◆ 選挙結果のご紹介

APNICカンファレンスでは、情報提供やポリシー提案に関する議論のほかにも、各種選挙が行われます。今回行われたNRO

NCおよび各SIGのChair・Co-Chairの選挙結果をご紹介します。

（1）NRO NC：藤崎智宏氏（日本電信電話株式会社（日本）・再選）
NRO NCは、ICANN理事会がグローバルポリシーを承認する上でアドバイスを行う役割を担います。ポリシーフォーラムより選出された2名と、RIRの理事会が指名する1名の合計3名を、各RIR地域の代表者としています。五つのRIRから合計15名で、NRO NCを構成しています。 2008年4月よりNRO NCとして活躍する藤崎氏は、2016年1月から2年間の任期で、引き続きNRO NCの役割を担います。 APNIC 40における選挙にて藤崎智宏氏がNRO NCに再選出 https://www.nic.ad.jp/ja/topics/2015/20150911-01.html
（2）ポリシーSIG Co-Chair：Sumon Ahmed Sabir氏 （Fiber@home Limited（バングラデシュ））
アドレスポリシーの提案について議論・コンセンサスの確認を行う、ポリシーSIGでは、Co-Chairが空席となっていました。今回、Sumon氏の当選により、Chairである山西正人氏とともに、ポリシーSIGを運営することとなります。
（3）NIR SIG Chair：橘俊男氏（グリー株式会社（日本）・再選） NIR SIG Co-Chair：Ajay Kumar氏（CNNIC（インド）・再選）、 Zhen Yu氏（CNNIC（中国））
NIRに関する議論を行うNIR SIGにおいても、任期満了となるChairおよびCo-Chairの選出が行われました。橘氏は2期目となり、これまで以上の活躍が期待されます。

今回の選挙では、日本国内のアドレスポリシーフォーラムにおいて活躍する藤崎氏と橘氏が当選されました。おめでとうございます!

◆ 次回以降のAPNICカンファレンスについて

次回のAPNIC 41カンファレンスは、APRICOT 2016と共催となり、2016年2月15日（月）～26日（金）にニュージーランド・オークランドで開催されます。ニュージーランドでのAPNICカンファレンスの開催は2008年8月以来、約7年半ぶりとなります。また、2016年9月頃開催予定のAPNIC 42カンファレンスは、バングラデシュ・ダッカで、2017年9月頃開催予定のAPNIC 44カンファレンスは台湾・台中での開催を予定している旨も、併せて発表されています。

APNICカンファレンスは、RIRやNIRのスタッフ、APNICメンバーに限らず、どなたでも自由に参加することが可能です。今回の報告に目を通されて、興味を持たれた方は、一度参加してみてはいかがでしょうか。特に日本国外での開催の場合には、ポリシーに関わる熱のこもった議論のほかに、開催地のインターネット事情を垣間見られる場面に遭遇するかもしれません。JPNICからは、職員が毎回参加していますので、多くの方と会場でお目にかかれることを楽しみにしています。

（JPNIC IP事業部 川端宏生）

● NIR SIGのメンバー

技術動向報告

APNICカンファレンスでは、毎回開幕直後に、環太平洋地域のインターネット運用者を対象とした情報交換と交流の場となるAPOPS（The Asia Pacific OPeratorS forum）が行われ、年間の動向や注目すべきテクノロジーについて共有と報告がなされます。今回のAPOPSは、2015年9月8日（火）に、APOPS 1～2の二つのセッションが開催されました。

本稿では、APOPSで紹介された、ICANNによるルートゾーンのKSK（鍵署名鍵）更新に関する二つの講演と、Policy SIGにおけるIPv4アドレスの移転と経路ハイジャックの話題について報告します。

◆ ルートゾーンのKSK（鍵署名鍵）更新に関する話題

○DNS Root Zone KSK Rollover

ICANNのElise Gerich氏から、"DNS Root Zone KSK Rollover"という題名にて、ICANNが実施を予定するルートゾーンのKSK更新の現状と、今後の動向が紹介※1されました。ルートゾーンのKSKは、ルートゾーンに署名するための鍵です。これは、DNSのDNSSECの検証（バリデーション）をルートからたどって行うために必要となるもので、DNSSEC検証に対応したDNSキャッシュサーバーは、ルートゾーンのKSKの公開鍵を保持しています。DNSSECの検証やKSKの役割など、DNSSECの基本的な仕組みの詳細は、No.43※2をご参照ください。

KSKはセキュリティ上の観点から、一定期間で更新することが推奨されています。ICANNがDNSSECの運用方針を定めた文書であるDPS※3には、5年経過した後にKSKの更新を行うよう定めており、ICANNがルートゾーンのKSK運用を開始した2010年から今年で5年を迎えることになるため、KSKの更新が必要になります。

ICANNはルートゾーンのKSK更新について、ベリサイン社および米国商務省電気通信情報局（NTIA）と協力し、以前からルートゾーンKSK更新計画を策定していました。ICANN、ベリサイン社、NTIAの3者は、ルートゾーン管理パートナーと呼ばれています。2014年12月、ICANNはルートゾーン管理パートナーに加えて、コミュニティの有志とルートゾーンKSK更新計画を策定する設計チームを編成しました。その設計チームが本年2015年8月にドラフトを公開※4したため、DNSSECの運用経験のある技術者にコメントを寄せてほしいとの要請がありました。

○ Testing Rolling Roots

前述のGerich氏の発表を受けて、ルートゾーンKSK更新計画設計チームのメンバーであるAPNICのGeoff Huston氏から、"Testing Rolling Roots"という題名にて技術的な詳細の発表※5がありました。DNSSECの利用率については、APNICが継続的に実施している観測の統計では、DNSSECの検証を有効にしてDNSの問い合わせを行っているクエリが、全体の14%になっているということでした。

ルートゾーンのKSK更新に併せてキャッシュサーバー側にあるKSKも更新しないと、DNSSECの検証ができなくなることになりますが、KSKの更新については、キャッシュサーバー側は手動で更新するほかに、自動で更新する手段があり、自動更新についてはRFC5011で詳細が定められています。こちらにのっとれば自動でキャッシュサーバー側も更新されるはずですが、RFC5011の通り自動更新されるキャッシュサーバーがどのくらいあるのか、事前に測定するのは難しい状況ということでした。

また、ルートゾーンがKSKを更新する際には、現行のKSKをいきなり削除するのではなく、新しいKSKと現行のKSKを併存させた併存期間を設けた後、現行のKSKを削除することになります。併存期間中はDNSのパケットサイズが増えるので、その増えたパケットをキャッシュサーバー側が取り扱えるかどうかも課題となります。実験として、観測対象のDNSキャッシュサーバーに対して、併存期間中に想定されるパケットサイズである1,440バイトのレスポンスを処理できるか試したところ、全体の1%のキャッシュサーバーがDNSの名前解決に失敗したとのことでした。ただし参考として、現状ORGドメイン名が1,650バイトのパケットサイズでレスポンスを返しており、これによりインターネット上で特に問題が見られないことからすると、パケットサイズの点はルートゾーンについてもおそらく問題ないのではないかという見解が述べられました。

さらに、KSK更新の実施時期も検討課題となります。前述のDPSでは四半期（1月・4月・7月・10月）のどこか初めの日に鍵更新を行うと規定されていますが、2016～2017年のカレンダーでは、いずれの四半期も初めの2日間が土日を含んでしまい、インターネットの運用者の業務態勢に影響が出ることが考えられます。

このように検討課題はあるものの、KSK更新に関する設計チームは今秋にとりまとめを行い、ルートゾーンパートナーへ提出する予定とのことでした。

◆ IPv4アドレスの移転と経路ハイジャックの話題

APNIC 40のPolicy SIGでは、国際的なIPv4アドレスの在庫枯渇状況に加えて、アジア太平洋地域における移転状況のほか、移転後のアドレスが経路ハイジャックにあっていた事例が発表されていました。

APNICのHuston氏によると※6、RIRにおいては、ARINではIPv4アドレス在庫がほぼ枯渇（当該発表時点）しており、/10のIPv4アドレスをIPv6移行のために保持している状態で、RIPE NCCは最後の/8とIANA返却アドレスからの割り振り分、AFRINICは約2.5個分の/8、LACNICは二つの/11、APNICは最後の/8とIANA返却アドレスからの割り振り分を残している状態です。AFRINICを除くとしても、今後、IPv4アドレスを入手するために、アドレスの移転が行われていくことが考えられます。実際にアジア太平洋地域では、2010年以降IPv4アドレスの移転件数・サイズ共に増加傾向にあります。

この講演の後、Dyn社のJim Cowie氏から、国際移転されたIPv4アドレスを使い始めたところ、実は他のネットワークで経路広告されていた、という事例が紹介されました※7。また別の事例として、ヨーロッパでアドレス移転元になることが多いルーマニアから、2014年10月、イランのモバイル通信会社にIPv4アドレスの移転が行われたところ、移転されたアドレスのうち半分ほどは、米国の大手通信会社において経路広告されていたことが分かったことも紹介されました。結局、モバイル通信会社が移転を受けたアドレスの分だけ細かい経路情報を広告し、そのアドレスに対する到達性を得られるようにしたということでした。

※1 DNS Root Zone KSK Rollover, Elise Gerich（ICANN）
https://conference.apnic.net/data/40/apnic40-gerich_1441676606-clean.pptx

※2 No.43 インターネット10分講座「DNSSEC」
https://www.nic.ad.jp/ja/newsletter/No43/0800.html

※3 DNSSEC Practice Statement for the Root Zone KSK Operator（DPS）
https://www.iana.org/dnssec/icann-dps.txt

※4 Design Team Review of Plan for DNS Root Zone KSK Change
https://www.icann.org/public-comments/root-ksk-2015-08-06-en

※5 Testing Rolling Roots, Geoff Huston（APNIC）
https://conference.apnic.net/data/40/2015-09-08-kskroll_1441514429.pdf

※6 The Status of APNIC's IPv4 Resources: Exhaustion & Transfers, Geoff Huston（APNIC）
https://conference.apnic.net/data/40/2015-09-09-ipaddrs_1440921336.pdf

※7 IPv4: Mining Strategic Reserves, Jim Cowie（Dyn）
https://conference.apnic.net/data/40/mining20strategic20reserves20cowie20apnic202015_1441819312.pdf

この影響で、Cowie氏の知る移転の事業者では、インターネットで経路広告できることが確認されていないIPv4アドレスは、取り扱わないことになったとのことです。国内でも、IPアドレスの移転を受ける時には、実際にインターネットで経路広告して使うことのできるアドレスであるかどうかの確認が重要であると言えます。

◆ 終わりに

ルートゾーンKSK更新はDNSSEC検証に影響の大きいものとなります。2015年11月から逆引きDNSSECのサービスを開始したJPNICとしても、動向を注視していきます。

（JPNIC 技術部／インターネット推進部 木村泰司）
（JPNIC 技術部 澁谷晃）

第94回IETF報告

全体会議報告

第94回IETF Meetingは、2015年11月1日（日）から11月6日（金）の間、神奈川県横浜市にあるパシフィコ横浜にて、WIDEプロジェクトのホストで開催されました。今回のIETF Meetingは、2002年に横浜で開催された第54回IETF Meeting、2009年に広島で開催された第76回IETF Meetingに続き、日本で開催される3度目のIETF Meetingとなります。会場はみなとみらい駅近くということもあって、駅に併設された商業施設内にレストランやカフェも多くあり、開催地としては快適に過ごせる場所であったのではないかと思います。

本稿では、このIETF横浜会合のレポートをお届けします。

◆ 6年ぶりの日本でのIETF開催

今回のIETF Meetingは、開催前からISOC-JPとJPNICが共催してIETF勉強会という、IETF Meetingの参加をより有意義にするための勉強会が開かれたり、W3C TPAC（Technical Plenary/Advisory Committee Meetings Week）と開催時期を近づけたり、IETFとW3C TPAC両方のイベントに参加する人向けに参加料金の割引プログラムが用意されたりと、会期前から今回のMeetingを盛り上げようとする試みが行われていました。

・IETF勉強会
　第1回：https://www.nic.ad.jp/ja/topics/2015/20150618-01.html
　第2回：https://www.nic.ad.jp/ja/topics/2015/20150910-01.html

また、国内開催ということもあり、国外で開催されるIETF Meetingでは60人から80人程度の日本人参加者が、今回は364人と多かったことがとても印象的でした。11月1日（日）のNewcomers' Orientationも、通常の英語によるオリエンテーションの他に、日本語によるオリエンテーションも開催され、さらに11月3日（火）に開催されたSocial Eventでは、日本の伝統文化を楽しんでもらう趣向が凝らされていました。開会挨拶の際には鏡開きが行われ、その酒を注いだIETF 94の焼印が押された枡が、今回のSocial Eventのお土産として配られていました。料理は、職人による寿司や天ぷら、おでんなど、日本の代表的な料理が振る舞われ長い行列ができていました。また、飴細工職人や切絵師による出店も設けられていて、その場で飴や切絵を作ってもらえ、こちらも順番待ちの列ができているなど、海外からの参加者の評判も良かったようです。

さて、ここからは11月4日（水）に開かれた「IETF Operations, Administration, and Technical Plenary」の様子について、簡単にご報告します。


● 会場では数々の日本の伝統文化が紹介されていました（写真は江戸紙切り）

◆ IETF Operations, Administration, and Technical Plenary

11月4日（水）の「IETF Operations, Administration, and Technical Plenary」は、会期中の各WGの会合スケジュール問題を改善する一環として、これまで別日程で開催されていた「IETF Operation and Administration Plenary」と「Technical Plenary」の二つの全体会合を一つにまとめて、会期中の全体会合の時間を短縮する目的で試みられました。

11月3日（火）に開催されたSocial Eventの開会式の際にも着用していた、赤い法被を羽織ったIETF ChairのJari Arkko氏のウェルカムスピーチから始まり、ホストプレゼンテーションが続き、各ホットトピックの報告として、以下のトピックごとに報告がありました。

- IETF-wide issues
- Administrative topics
- Invitation to IETF 95
- NomCom update and requests
- New research groups
- Progress in format work
- Meeting calendar updates

その後、IAB（Internet Architecture Board）ChairからのIAB活動報告、Technical Topicが一つ、IABとIAOC（IETF Administrative Oversight Committee）、IESG（Internet Engineering Steering Group）オープンマイクという流れで、議事進行がされました。

○ホストプレゼンテーション

ホストプレゼンテーションでは、WIDEプロジェクトの代表である江崎浩氏より挨拶がありました。今回のNOCボランティアは、加藤朗氏、関谷勇司氏、大江将史氏が中心となり、WIDEプロジェクトのNOCメンバーとIETF NOCメンバーが協調して、会場ネットワークを準備したと紹介がありました。また、今回のNOCボランティアは会場ネットワークに加えて、会場近くにあるよこはまコスモワールドの観覧車「コスモクロック21」の頂上付近で利用可能な、SSID「ietf-wheel」というWi-Fiネットワークを提供しているという紹介もあり、会場からはNOCボランティアの貢献に対する拍手がありました。そして、今回のIETF Meetingのスポンサーをした各組織の紹介があり、今回のIETF Meetingはこれら各組織の協力のもと実現することができたと謝辞を述べ、会場からも大きな拍手が起こりました。

○IETF-wide issues

IETF-wide issuesでは、IETF ChairのJari Arkko氏より、参加者の内訳やIETFの全般的なホットトピックについて報告がありました。第94回の現地参加者は、52の国と地域から1,298人の参加となり、前回の1,358人の参加から60人ほど減少していました。また、2015年の同時期に米国ハワイにて開催された、第91回の参加者数の1,109人と比較すると、189人程度参加者が増えたとのことでした。新規参加者は全体の約21%の278人で、ここ数年開催されているIETF Meetingの中でも、今回は特に新規参加者が多い回となったことがわかります。国別の参加者数は、1位米国、2位日本、3位中国、4位ドイツとなっており、日本からの参加者数は、全体の参加者数の1/4程度の割合となっていました。

今回はホットトピックとして、.onionとGen-ART（General Area Review Team）の紹介がありました。

・.onion
.onionは、経路情報の匿名化を行う、Torネットワークで利用するトップレベルドメイン名です。このドメイン名を既存のドメイン名と同様にDNSで利用することを防ぐために、RFC6761 “Special-Use Domain Names”に従い、.onionの予約を行うことを記述した、RFC7686“The“.onion”Special-Use Domain Name”が発行されたとの紹介がありました。

・Gen-ART
Gen-ARTは、RFCの品質向上を目的として、General Area Directorと共に、IETF LC（Last Call）中のI-D（Internet Draft）を多角的にレビューするためのチームです。今回、Arkko氏より、そのレビュワーとして参加しているボランティアの紹介がされると、会場から拍手が起こりました。

また今回のRecognitionでは、会期中に25周年を迎えるBMWG（Benchmarking Methodology Working Group）の紹介が行われました。BMWGは、これまでに34本のRFCを発行し、インターネット技術に大きな貢献をしています。初代BMWG Chairを務めたScott Bradner氏をはじめとした、BMWGに関わったボランティアの方々に感謝の意が述べられ、会場からもその貢献を讃えた拍手が起きていました。

・その他
その他のホットトピックとしては、Code & Hackathonとして、Code SprintやIETF Hackathonの紹介がありました。インターネットの発展形態と、IETFが行っている標準化プロセスを端的に表現した言葉として、David Clark氏が述べた“We reject kings, presidents and voting. We believe in rough consensus and running code”という言葉があります。この“Running Code”をIETFでは重要視しており、近年イベントを通じてさまざまなWGにて議論中の提案を、実際に実装するイベントが開催されるようになりました。今回開催された第3回IETF Hackathonは、10月31日（土）と11月1日（日）の2日にわたり開催され、参加者は2日合わせて100人程度だったと報告がありました。

また、Arkko氏のスライドには、IETF HackathonにてSFC（Service

Function Chaining）に関する実装を行った日本人チームの写真が掲載されており、“Running Code”においても日本からの貢献があることが印象的でした。第4回IETF Hackathonは、第95回IETF Meetingの直前の2016年4月2日（土）と3日（日）の2日にかけて行われるそうで、現在、準備や参加者募集していると呼びかけがありました。

○Administrative topics

Administrative topicsでは、IAOC ChairのTobias Gondrom氏と、IETF Trust ChairのBenson Schliesser氏から報告がありました。

Gondrom氏からは、はじめに次回以降のIETF Meetingについての報告がありました。第95回のホストは、ラテンアメリカとカリブ海地域を担当する地域インターネットレジストリ（RIR）である、LACNICに決まりました。第96回はベルリン、第97回はソウルで開催される予定ですが、第98回は開催地を予定していたモントリールの会場ホテルと調整がまとまらず、開催のめどが立たなかったため、現在、開催地を北米地域から再度探しているとのことでした。第99回はヨーロッパ地域での開催が決まっており、最終契約を行っているとのことです。第100回は開催地をアジア太平洋地域と決めたが、契約などについてはこれから行うそうです。

IASA（IETF Administrative Support Activity）に関する予算報告では、2016年から2018年にかけての予算が決まったとの報告がありました。また、Acknowledgmentsでは、NOCボランティアと会場のネットワーク機器や回線を提供した企業、Code Sprintの参加者の紹介がありました。

最後に、11月5日（木）の昼には慶應義塾大学の村井純氏による“Japan x Internet”と題したTech Talk、そして、その晩にはBits-N-Bitesが開催されるという紹介がありました。

● 村井純氏による“Japan x Internet”と題したTech Talkの案内

Schliesser氏からは、IETF Hackathonにて作成されたコードなどの著作物（IPR; Intellectual Property Rights）の取り扱いをまとめた、Hackathon IPRの紹介がされました。

○Invitation to IETF 95

Invitation to IETF 95では、LACNICのCTO Carlos Martinez氏より、第95回IETF Meetingの紹介が行われました。また、2016年1月でIETFは30周年を迎えることとなり、第95回は30周年を迎えた後で最初のIETF Meetingとなるようです。ホストを務めるLACNICの紹介動画を流した後、ブエノスアイレスの魅力について紹介がありました。

○NomCom update and requests

NomCom update and requestsでは、NomCom（Nominating Committee） ChairのHarald Alvestrand氏より、NomComの活動の進捗報告がされました。はじめにNomComのメンバーの紹介がされ、今回は男性37名、女性6名の、計43名の推薦があったとの報告がありました。また、今回のIETF Meetingにて43名中39名の面接を行う予定であり、年末までには候補者をまとめられる予定であると報告がありました。

○New research groups

New research groupsでは、IRTF ChairのLars Eggert氏より、会期中に開催されるRG（Research Group）の紹介がありました。今回開催されるRGの会合は、以下の五つです。

- Crypto Forum（CFRG）
- Information-Centric Networking（ICNRG）
- Network Function Virtualization（NFVRG）
- Network Management（NMRG）
- Software-Defined Networking（SDNRG）

またこの他に、以下の四つのProposed RGの会合も開催されるとの報告もありました。

- Proposed Human Rights Protocol Considerations（HRPC）
- Update on the Internet Research Task Force at Proposed Thing-to-Thing（T2TRG）
- Network Machine Learning Research Group（NMLRG）
- Proposed How Ossified is the Protocol Stack（HOPSRG）

RGの紹介の後は、IRTFとISOCが共催したワークショップ“Research and Applications of Internet Measurements（RAIM）”が、10月31日（土）に開催されたとの報告がありました。

○Progress in format work

Progress in format workでは、RSE（RFC Series Editor）のHeather Flanagan氏から、RFC formatの改訂作業のゴールと進捗についての報告がありました。改訂作業のゴールとしては、XMLによる記述は変更しない一方で、アウトプットのファイル形式はplain textやPDF、HTMLに対応することをめざしているとのことです。また、図表については、従来のASCIIアートによる表現ではなくSVG（Scalable Vector Graphics）ファイルを利用可能とすること、文字については、Non-ASCII文字も利用可能とすることが説明され、今後も作業を継続するとのことでした。

○IAB Chairレポート

ChairのAndrew Sullivan氏から、IABの活動内容の紹介がありました。また、今回はBoFの開催が少なかったことを受けて、IABではBoFの開催を手伝う姿勢があるので、BoFを開催したい人はぜひ気軽に声をかけて欲しいとのことでした。

○Technical Topic

今回のTechnical Topicは、計測結果に基づくエンジニアリングがインターネット技術においても重要であるという観点から、IABのBrian Trammell氏とCAIDA（Center for Applied Internet Data Analysis）のAlberto Dainotti氏からそれぞれ、“Measurement-Driven Protocol Engineering”と“Measuring and Monitoring BGP”と題した発表がありました。

Trammell氏からは、IABが取り組んでいるIP Stack Evolutionプロジェクトを例に、このプロジェクトではインターネットはUDP上で正しく動作することを前提に設計が進められているが、本当にインターネットはUDPでカプセル化したパケットが増大しても問題なく動作するのかという問いかけをし、計測を行うことの必要性について説明していました。また一方で、計測を行うツールはいろいろとあるものの、実際にはインターネットの計測を行うことは困難であり、計測結果のデータが不足しているため、計測したデータを共有できる仕組みを持つ必要があるとのことでした。

Dainotti氏からは、「アラブの春」の際に行われた国単位でのブロッキングや、東日本大震災の時に発生したBGPの変化、MITM BGP attacksなど、BGPに大きな変化が見られた代表的な出来事の紹介がありました。

○IAB、IAOC、IESGオープンマイク

今回のオープンマイクは、これまで「IETF Operation and Administration Plenary」と「Technical Plenary」でそれぞれ別に設けられていたオープンマイクが、一つにまとめて行われました。会場から「今回はBoFが少なかった」という声があった一方で、IAB ChairのSullivan氏からは、Bar BoFについては「開催については特に許可を取る必要はないので、必要に応じて開催して問題ない」などの、BoFに関する話がありました。また、「W3C TPACやOpenStack Summit等、関連するイベントがIETFと会期が近くまとまっていて参加しやすかった」という声もありました。

◇　◇　◇

次回のIETF Meetingは、2016年4月3日（日）から4月8日（金）にかけて、アルゼンチンのブエノスアイレスにて開催されます。

（青山学院大学 情報メディアセンター 根本貴弘）

IETF会合に初めて参加して

今回のIETFは日本ということで、参加しやすいミーティングだったのではないでしょうか？ また、初めてIETFに参加する場としても、よい機会だったのではないかと思います。筆者もその1人です。

IETFでは、初回参加者向けに、専用のオリエンテーションやイベントを用意するといった取り組みを実施しています。本稿では、実際にIETFに初めて参加した筆者より、初回参加者向けの各種企画へ参加した感想と、初めて参加するWGとして選んだRDAP（Registration Data Access Protocol）関連の議論を行っている、Extensible Provisioning Protocol Extensions（EPPEXT） WGの報告をお伝えします。

◆ 事前の準備

今年は、Internet Society日本支部（ISOC-JP）とJPNICの共催で、日本でもIETF勉強会が開かれるなど、IETF 94横浜ミーティングに向けて準備の取り組みがありました。勉強会そのものには、残念ながら私は都合が合わず参加できなかったのですが、豊富な資料が公開されていたので、空き時間に確認していました。会期前後で自分と同じく日本からIETFに初めて参加される方と話をしたところ、「この資料を参照することで安心して参加できた」という声を聞きました。

□IETF勉強会の開催レポート
第94回IETFミーティング横浜開催に向けて
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2015/vol1323.html

IETF横浜ミーティングへの参加の前に
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2015/vol1348.html

□IETF勉強会の資料
第1回IETF勉強会
https://www.isoc.jp/wiki.cgi?page=PreIETF93

第2回IETF勉強会
https://www.isoc.jp/wiki.cgi?page=PreIETF94

◆ 参加当日の状況

参加する前に迷ったのが、当日に行う必要があるレジストレーションの詳細です。「レジストレーションでは何をするのか？」ということ自体が謎でしたが、参加経験者に話を聞くと、単に自分の名前を名乗ってバッジをもらうだけとのことでした。また、参加者数が1,000人を超す規模の大きなミーティングなので、「当日は大行列の中に待つことになるのか？」といった疑問もありました。こちらも参加経験者に話を聞くと、特に準備をせず並ぶだけで問題無いとのことでした。実際、当日レジストレーションに行ってみると、1,000人が一斉に並んでいるということは無く、数十名程度が何列かに分かれて並んでいるだけで、それほど心配することはありませんでした。受付で渡されたものはネームカードと、初参加者であることを示すニューカマーバッジ（シール状になっており、ネームカードの上に貼り付けるもの）でした。なお各会場では、机付きでPC用に電源のある席は前の方に数列しか無く、大半の席は単に椅子が置いてあるだけなのですが、参加者は特に問題にする様子は無く、ラップトップPCを膝に置いて参加していました。

◆ 初日のオリエンテーション

IETF 94初日の11月1日（日）は、Newcomers' Orientationという、IETF初参加者向けのセッションがありました。日本語のオリエンテーションが併催され、私は日本語のセッションに参加しました。担当は、株式会社レピダムの林達也氏とエヌ・ティ・ティ・コミュニケーションズ株式会社の小原泰弘氏で、今回用いた資料は元々英語版で作成されていたものを、日本語版に直したものとのことでした。

□Newcomers' Orientation 日本語版資料URL
http://wiki.tools.ietf.org/group/edu/attachment/wiki/IETF94/94-newcomers-japanese.ppt?format=raw

オリエンテーションの演題は「IETFの構造とインターネット標準の標準化プロセス」というもので、内容は、IETFがどういった団体でどのように運営されているのか、また、RFCなどインターネット標準となるIETF文書がどのようなプロセスで策定されているのかが、わかりやすく解説されていました。


● Newcomers' Orientationの様子

IETFの組織構造※1に関しては、IETFで扱う技術分野は多岐にわたることから、分類としてまず大きく技術分野をエリアというくくりで分け、さらにエリア内にワーキンググループ（WG）を置いて管理している構造になっています。初参加者は、自分が興味のある技術分野がどのエリア・WGで扱われているのか、確認するところから始める必要があると感じました。

ほかに、オリエンテーションの中で、ハム（Hum）という賛同を示す発声方法の練習をしたり、オープンマイクで話すときの注意点を聞いたりしました。IETFでは、ある議論について賛成の意思表示をするため、ハム（Hum）という口を閉じて、唸り声を出すような方法を採ることがあるということでした。また、オープンマイクで話すときは、議事メモを残す都合や遠隔参加者への配慮のため、必ず名前を伝えてからマイクで発言するようにとのことでした。それに加えて、セッション参加中にはブルーシートという、所属と名前を記入する紙が回されるので、適宜記入する必要があるという案内もありました。こうした諸案内により、私はセッションに参加した際に、作法的な面で戸惑うことはありませんでした。

なお、先にレジストレーションデスクでもらったニューカマーバッジを付けていると、それなりに先輩参加者が配慮して接してくれるので、この機会に必要な挨拶・情報交換など交流をすると良いという話もありました。

オリエンテーションの良かった点としては、初参加者向けに必要な情報が、2時間程度でまとまって提供されることがあります。IETFのWeb上に、初心者向けのガイド※2が載っていて、有益な情報が満載されているとは思うのですが、文章量が多いため、初参加者がいきなりこれを読むよりは、こういった口頭での導入があると助かると感じました。

◆ Newcomers' Meet and Greet

オリエンテーションの後、ヨコハマ グランド インターコンチネンタルホテルのBayview Roomという部屋で、初参加者向けの集まりがありました。こちらではお酒が提供され、懇親会のように歓談するスタイルとなっていました。初参加者向けの配慮としては、IETFのエリア・WG一覧の紙資料（5ページ程度）が入口で渡された点と、室内に複数設置してあるテーブルにIETFのエリアを示すプレートがそれぞれ立てられており、その近くにエリアディレクターやWGチェアがいて、話ができるようになっていた点があります。会場は大盛況で、かなり大きな声で話さないと至近距離でも何を言っているのか聞き取りづらいほどでした。また、先のオリエンテーションで話のあった、ニューカマーバッジを付けていると先輩参加者が配慮してくれるというのはその通りで、この集まりの最中に、チェアの何人かがニューカマーバッジを付けている私を見つけて話しかけてくれ、円滑にコミュニケーションを取ることができました。

◆ 参加したセッションの報告

ここまで書いたように、筆者は今回の横浜会合がIETF会合初参加だったのですが、初めて議論に参加するWGとして、下記のWGを選びました。

○Extensible Provisioning Protocol Extensions（EPPEXT） WG

筆者が今回のIETFに参加した動機は、各種技術の最新動向を追うことのほか、RDAP（Registration Data Access Protocol）関連の動向について情報収集することにありました。RDAPは、WHOISに置き換わるプロトコルとして、WEIRDS（Web Extensible Internet Registration Data Service）というWGにおいて標準化が進められたもので、RFC7480～7485において文書化され、WEIRDS WGは2015年3月に活動を終了しました。WEIRDS参加者用MLはその後も残っており、RDAP関連の議論が散発的にされていたのですが、EPPEXT WGの方でもRDAP関連の提案がされることがあり、扱う技術が重複していました。そのため、RDAP関連の議論を継続して行う場として、WEIRDS WGとEPPEXT WGを統合した、REGEXTという新たなWGを発足させることをML上で議論していました。今回のIETF横浜では、まずはEPPEXT側の残課題について確認と議論がされた後、新WGのマイルストーンについて議論がされました。チェアの提示したマイルストーンについて異論は無く、新しいWGのチャーター（設立趣意書）の作成を別途進めていくということになりました。

◆ IETF 94参加者向けML

会期前後を通じて、IETF 94参加者向けMLにも登録していました。MLには2種類あり、初参加者向けの［94-1st-timers］と、IETF 94参加者全体向けの［94attendees］とがありました。

初参加者向けの［94-1st-timers］ MLはあまり流量は無かったのですが、会期1週間ほど前に初参加者向け情報がまとまって投稿され、まずはそのメールを見て活動計画を立てれば良いという点で役立ちました。

IETF 94参加者全体向けの［94attendees］のMLはとても活発に投稿があり、主に海外から参加した人の疑問と、それに対する回答がされていました。内容は、空港から会場への移動方法の詳細や、日本でのお金や通信のことといった現地滞在の基本的なノウハウから、各種観光情報のやりとりなど多岐にわたっていました。私は余裕が無く、海外参加者に回答をすることはできなかったのですが、日本人の参加者がボランティア精神を発揮して、積極的に回答されていました。

会期終了後の［94attendees］では、「横浜開催のIETFに参加できて良かった」という、海外からの声が多く投稿されていました。参加経験者に話を聞くと、他の開催地ではあまりそういった感想は無いようで、日本的な社交辞令の範囲でなく、実際に日本人のおもてなしに満足いただいた方が多くいらっしゃったのではないかと思われます。もちろん、私も今回の参加に満足した1人です。初参加者向けに、さまざまな取り組みをしていただいた皆様に感謝いたします。

（JPNIC 技術部 澁谷晃）

● IETF 初参加者を示すバッジ

※1 IETFの組織構造
https://www.nic.ad.jp/ja/tech/ietf/section3.html

※2 IETFのタオ：初心者のためのインターネット技術タスクフォースガイド
https://www.nic.ad.jp/ja/newsletter/No43/0800.htmlhttps://www.ietf.org/tao-translated-ja.html

セキュリティ関連報告

本稿では、セキュリティエリアの全体的な議論が行われるSecurity Area Advisory Group（SAAG）と、最近、サーバ証明書の検証技術として話題に上っているCT（Certificate Transparency）を検討しているTRANS WG、経路ハイジャックの対策技術であるBGPSECの仕様検討を行うSIDR WGを取り上げて報告いたします。

◆ セキュリティエリア全体会合 - Security Area Advisory Group（SAAG）

SAAGは、IETFのセキュリティエリアWGの状況報告と、セキュリティに関わるディスカッションが行われるオープンフォーラム（参加資格などがない会合）です。毎回IETF期間中に行われる会合では、セキュリティエリアWGの活動報告と招待講演などが行われています。今回は130名ほどが参加していました。以下、SAAG会合における招待講演とその講演資料を紹介します。

RESTCONFやNETCONFのための暗号鍵を格納するYANG（Yet Another Next Generation）データモデル, Kent Watsen氏
RESTCONFのためのHTTPSと、NETCONFのためのSSHやTLSで使われる暗号鍵を格納するYANGデータモデルに関する解説
・発表スライド https://www.ietf.org/proceedings/94/slides/slides-94-saag-4.pdf
ルーティングプロトコルで使われる暗号設定のためのYANGデータモデル, Russ Housley氏
ルーティングプロトコルのOSPF（Open Shortest Path First）やRSVP（Resource Reservation Protocol）で使われる、暗号通信や認証のためのYANGデータモデルの解説
・発表スライド https://www.ietf.org/proceedings/94/slides/slides-94-saag-5.pdf
ITU-TとISO/IEC JTC1（国際標準化機構と国際電気標準会議の第一合同技術委員会）で検討されているIoTデバイスのための暗号利用方式, 吉田博隆氏（日立製作所）
IoTデバイスのような計算性能の低いデバイスでの利用を想定した、暗号利用方式の紹介
・発表スライド https://www.ietf.org/proceedings/94/slides/slides-94-saag-2.pdf
IPv6への移行技術におけるセキュリティ脅威分析, Marius Georgescu氏（奈良先端大/WIDEプロジェクト）
移行技術における脅威の分類と、CE（カスタマーエッジ）とPE（プロバイダーエッジ）という構成を取るMAP-Tについてのケーススタディ
・発表スライド https://www.ietf.org/proceedings/94/slides/slides-94-saag-3.pdf
MaRNEWワークショップの報告, Natasha Rooney氏
モバイル通信などの無線通信における暗号通信を踏まえた最適化に関するワークショップの報告。MaRNEWはManaging Radio Networks in an Encrypted World（暗号化される世界における無線ネットワークの管理）の略
・発表スライド https://www.ietf.org/proceedings/94/slides/slides-94-saag-1.pdf

自由討論（オープンマイク）の時間には、会場の参加者から、W3CではWebにおける認証や暗号APIに関する標準化活動が行われていて、セキュリティやプライバシー保護についての検討やレビューでIETFとも連携したいといった意見が挙げられていました。またJabberによるリモートの参加者からは、IETFでもIoTのセキュリティに着目した活動を行うべき、といった意見が出されていました。

◆ TRANS（Public Notary Transparency）WGで行われている議論

TRANS WGは、Webブラウザなどで不正に発行された疑いのあるサーバ証明書を検知するための仕組みである、CT（Certificate Transparency）を検討しているWGです。このWGは2014年3月頃に設立され、CTの仕様を定めたRFC6962の修正や拡張を行う形で検討が進められています。

・Certificate Transparency（RFC6962）
https://tools.ietf.org/html/rfc6962

CTは、さまざまな認証局から発行される証明書のハッシュ値を、ログサーバと呼ばれるサーバで集中的に記録する仕組みです。TLS（Transport Layer Security）で通信するWebブラウザなどが、サーバ証明書を検証する際にログサーバに問い合わせを行い、類似した証明書が存在するかどうかを確認することができます。サーバのFQDNが同一であり、不正に発行された可能性があるサーバ証明書が見つかった場合に、ユーザーに警告するといった用途が考えられています。Google Chromeなどで実装されており、複数のログサーバが立ち上がっています。

・Certificate Transparency
http://www.certificate-transparency.org/
・Known Logs - Certificate Transparency
http://www.certificate-transparency.org/known-logs

CTのログは、全体の整合性を保ったまま一部を改変することが難しく、さらにログから特定の証明書を検索しやすいマークルハッシュ木（Merkle Hash Tree）と呼ばれるデータ構造が使われています。また証明書は署名付き証明書タイムスタンプ（SCT:Signed Certificate Timestamp）と呼ばれるタイムスタンプが付与される形で記録されます。TRANS WGでは、ログサーバへの問い合わせ仕様の他、CTを使ったサーバ証明書監視の方式などについてI-Dが作成され、検討が進められています。

WG会合では、実装状況の報告の他、CTログサーバの挙動やあり方に関する意見募集、DNSを使ったCTといった新しい方式の検討などが行われました。

Gossiping in CT, Linus Nordberg氏
CTログサーバの不正な挙動やプライバシーに関する課題を整理したドキュメント案。CTログの信頼性のモデルについても言及されている
・発表スライド https://www.ietf.org/proceedings/94/slides/slides-94-trans-3.pdf
・ドキュメント案 https://tools.ietf.org/html/draft-ietf-trans-gossip-01
脅威分析（Threat analysis）, Steve Kent氏
CTログに起こりうる不具合や攻撃モデルを列挙しているドキュメント案
・発表スライド https://www.ietf.org/proceedings/94/slides/slides-94-trans-0.pdf
・ドキュメント案 https://tools.ietf.org/html/draft-ietf-trans-threat-analysis-03
DNSSECを使ったCTログ（DNSSEC logging）
DSレコードやゾーンの階層を記録する案。AレコードやAAAAレコードそのものではなく、DNSの階層に変化が起きていないかどうかを監視できるという案
・ドキュメント案 https://tools.ietf.org/id/draft-zhang-trans-ct-dnssec-03.txt

次のWebページでは、この他の検討内容を見ることができます。

・Trans Status Pages
https://tools.ietf.org/wg/trans/

◆ BGPSECに関わる標準化の動向

SIDR（Secure Inter-Domain Routing）WGは、BGPのためのセキュリティ技術であるBGPSECの検討を行っているWGです。五つのRIRやJPNICで提供されている、RPKIのリソース証明書とROA（Route Origination Authorization）を使って、BGP経路情報が正しいかどうかを確認できるOrigin Validationと、ASの電子証明書を使ってASパスの情報に電子署名を行い、ASパスが正しいものであることを確認できるPath Validationが検討されています。この二つを合わせてBGPSECと呼ばれています。今回は議題が多く、11月3日（火）と11月5日（木）の2回、会合が行われました。いくつか目立った動きのあるものをご紹介します。

RRDP実装報告（RRDP Implementation Experience）, Tim Bruijnzeels氏（RIPE NCC）
RPKIで使われているRsyncに代わる、差分転送プロトコルのRPKI Repository Delta Protocolのパイロット実装の報告です。httpsを使ってXML形式のメッセージをやり取りします。RPKI署名検証サーバ（RPKIキャッシュサーバとも呼ばれる）におけるキャッシュの機能はオプション（付加機能）として位置づけられています
・発表資料 https://www.ietf.org/proceedings/94/slides/slides-94-sidr-3.pdf
・ドキュメント案 https://tools.ietf.org/html/draft-ietf-sidr-delta-protocol-01
RPKI検証サーバにおける観測など（A Few Years In The Life Of An RPKI Validator）, Rob Austein氏（Dragon Research）
五つのRIRを含むさまざまなRPKIリポジトリから発行されたデータを収集し統計を取った結果の報告。特にRIPE地域のオブジェクトが単純増加傾向にある。Rsyncの異常終了などにより、接続が切れてしまうこともしばしば起きている
・発表資料 https://www.ietf.org/proceedings/94/slides/slides-94-sidr-1.pdf
RPKIの認証局における運用ミスや故意で起きる問題について（Misoperation or malicious operation of CA）, Yu Fu氏（CNNIC）
RPKIの上位認証局でリソース証明書に誤ったIPアドレスが記載されることにより、リソース証明書が無効になってしまう問題の指摘です。RPKI Toolsを使って検証が行われたという報告もされました。アドレス移転の際に起きうる問題として挙げられていますが、会場では認証局が不整合が起きないようにデータベースに基づいて発行すれば問題は起きないはず、といった意見が挙げられていました
・発表資料 https://www.ietf.org/proceedings/94/slides/slides-94-sidr-7.pdf

この他の話題についてはSIDR WGのステータスページをご覧いただければと思います。

・Sidr Status Pages
https://tools.ietf.org/wg/sidr/

（JPNIC 技術部／インターネット推進部 木村泰司）

● IETF 94ではWIDEプロジェクトがローカルホストを務めました

IPv6関連WG報告

本稿では、横浜で開催されたIETF 94の会期中における、IPv6に特化した内容を議論するワーキンググループ（WG）での議論内容を紹介します。

◆ 6man WG（IPv6 Maintenance WG）

6man WGは、IPv6のプロトコル自体のメンテナンスを実施するWGです。今回は、11月4日（水）の朝一のコマ（9:00-13:00）にて開催されました。前日の夜に盛大なソーシャルイベントがあったにも関わらず、100名程度の参加者を集め、活発な議論が実施されました。

● IETF 94の会場となったパシフィコ横浜

ミーティングは、いつも通りチェアによるアジェンダ、Note Well（権利等の注意事項）の確認、およびWGの関連文書ステータス報告より始まりました。ミーティングの時点で、WG文書のうちRFC発行待ちの文書が2件、WGラストコール中の文書が1件、WGラストコール待ちの文書が1件存在しています。また、WGで議論中の文書が6件、WGの議論文書とするかどうか検討中の文書が3件となっており、IPv6のプロトコル自体の検討も継続的に実施されていることがわかります。この後、チェアより、他のWG（conex（Congestion Exposure） WG, ippm（IP Performance Metrics） WG）における議論内容で、IPv6プロトコルに関連して6man WGに照会があった、2件の案件対応について報告がありました。2件とも拡張ヘッダに関するものですが、他のWGにおいても、拡張ヘッダを使用したIPv6自体の機能拡張が検討されているようです。

今回のミーティングでは、次のWGドラフト2件、個別ドラフト5件について議論されました。

WGドラフト
Host routing in a multi-prefix network （マルチプリフィクスネットワークにおけるホストルーティング） draft-ietf-6man-multi-homed-host
IPv6 specifications to Internet Standard （IPv6仕様の“インターネット標準”化） draft-ietf-6man-rfc2460bis, draft-hinden-6man-rfc4291bis
個別ドラフト
IPv6 Hop-by-Hop Header Handling （IPv6 Hop-by-Hop拡張ヘッダの処理について） draft-baker-6man-hbh-header-handling
Transmission and Processing of IPv6 Options （IPv6オプションの転送と処理について） draft-gont-6man-ipv6-opt-transmit
IPv6 Universal Extension Header （IPv6ユニバーサル拡張ヘッダ） draft-gont-6man-rfc6564bis
Support for adjustable maximum router lifetimes per-link （リンクごとの最大ルータ有効期間調整機構のサポート） draft-krishnan-6man-maxra
IPv6 Segment Routing Header （IPv6セグメント経路制御ヘッダ）（SRH） draft-previdi-6man-segment-routing-header

アジェンダには、以下の3件の個別ドラフト（うち、新規2件）が上がっていましたが、時間切れで次回送り（プレゼンテーションスライドはプロシーディングに収録）となりました。

個別ドラフト
Multiple Provisioning Domains using Domain Name System （ドメイン名システムで利用する複数プロビジョニングドメイン） draft-stenberg-mif-mpvd-dns
新規個別ドラフト
Uplink access technology indications in Router Advertisements （ルータ広告中でのアップリンク情報通知） draft-krishnan-6man-uat
DNS Name Autoconfiguration for Internet of Things Devices （IoT（Internet of Things）デバイスにおけるDNS名自動設定） draft-jeong-homenet-device-name-autoconf

議論されたアイテムの中から、いくつかを紹介します。

◆ Host routing in a multi-prefix network（マルチプリフィクスネットワークにおけるホストルーティング）,draft-ietf-6man-multi-homed-host

複数のアップリンクを持つネットワークにおける、ホストの動作についての変更提案です。特に、同一リンク上に複数のルータがある場合のホストと、複数のアップリンクを持つホスト（スマートフォン等）を対象にしています。前者の場合、現在の仕様では、複数のルータにおいてステートレスアドレス自動設定（StateLess Address AutoConfiguration: SLAAC）を利用した場合に、ホストがどのルータをパケット送出先として選択するかについての、明確な規定がありませんでした。このため、ホストが選んだルータによっては、BCP38に定義されており多くのISPで採用されている、送信元アドレス詐称を防ぐためのイングレスフィルタリング※1により、通信ができない可能性があります。

後者の場合でも、ホストが選んだルータと送信元アドレスの組み合わせによっては、通信に失敗します。また、現状のICMPv6リダイレクトの仕様では、複数のアップリンクをホストが持つ場合（無線LANとLTE回線に接続されるスマートフォン等が想定されています）、ルーティング最適化のために片方のアップリンクルータが、ホストにICMPリダイレクトを送信するような場合に対応できないことを問題としています。

これらの状況を改善するため、送信元アドレスにより、転送するルータを選択する（SLAACによりアドレスを付与したルータに、対応した送信元アドレスを持つパケットを送信する）こと、およびホストがリンクの違うアップリンクルータから受け取ったリダイレクトを処理するよう、ホストの動作を変更する提案です。複数のルータからのSLAACに対応する変更には、いくつかの賛成が表明されましたが、ICMPリダイレクトに関する動作については、否定的な意見も提起されました。このドラフトについては、MLでの議論の後、WGラストコールに向けて調整が実施されることになっています。

◆ IPv6 specifications to Internet Standard（IPv6仕様の“インターネット標準”化）, draft-ietf-6man-rfc2460bis,draft-hinden-6man-rfc4291bis

現在のIPv6の基本仕様は、1998年に発行されたRFC2460にて規定されており、この文書はDraft Standardという位置づけになっています。従来より6man WGにおいて、「IPv6の仕様をインターネット標準仕様の最終段階である“インターネット標準（Internet Standard）”に昇格させ、IPv6の仕様は完全にできあがったことを世の中に知らしめ、普及の後押しをすべきだ」という議論がありましたが、なかなか作業が先には進みませんでした。しかしながら、IETFにおける標準化プロセスの見直しにより、Draft Standardカテゴリが廃止（RFC6410）されてから数年がたち、従来Draft Standard カテゴリにあったRFCのカテゴリ見直しが必要になったこともあり、IPv6仕様の“インターネット標準”化を本格的に実施することとなり、その作業が進んでいます。

今回のミーティングでは、前回の議論に基づき実施された改版の状況や、作業を進める上での留意点、今後の方針が議論になりました。現在、改版が進んでいる文書は以下の2文書です。

- RFC2460（draft-ietf-6man-rfc2460bis）：IPv6の基本仕様 RFC2460を更新している文書および訂正（Errata）の取り込み、内容の更新等
- RFC4291（draft-hinden-6man-rfc4291bis）：IPv6アドレス構造 RFC4291を更新している文書および訂正（Errata）の取り込み、参照の更新等

今後、RFC2460の改版文書については、WGラストコールを実施予定となっています。RFC4291の改版ドラフトについては、WGアイテムとすることがミーティングでは同意を得て、MLにおいてWGアイテム化の最終確認を実施することになっています。

その他、“インターネット標準”化に向けたプロセスを進めるため、“RFC1981-IPv6パスMTU探索”のレビュアー募集等が実施されています。

IPv6標準仕様群の“インターネット標準”化は着実に進行しており、IPv6のさらなる普及に向けた動きも活発化しそうです。

□6man WG
http://datatracker.ietf.org/wg/6man/charter/
□第94回 IETF 6man WGのアジェンダ
http://www.ietf.org/proceedings/94/6man.html

◆ v6ops WG（IPv6 Operations WG）

v6opsは、IPv6に関するオペレーション技術および共存・移行技術に関する議論を実施するWGです。IPv6の普及を受け、提案数が多いセッションとなっており、このところ毎回2コマを使っての開催となっています。今回も、月曜の朝一（9:00-11:30）、月曜の最終（17:10-19:10）の2コマにて開催されています。

参加者もそれぞれ150名程度で、IPv6の実利用について多くの人が興味を持っていることがうかがえます。

ミーティングは、チェアによるNote Wellの確認およびアジェンダの紹介から始まりました。今回のミーティングでは、次の項目が議論されました。

※1 イングレスフィルタリング
RFC2827（BCP 38）で解説されている、送信元を偽装したIPパケットの転送を防ぐ手法の一つです。

Identifier-locator addressing for network virtualization （ネットワーク仮想化のための識別子-ロケータ分離アドレス構造）
draft-herbert-nvo3-ila
Host address availability recommendations （ホストアドレスの有効性に関する推奨）
draft-ietf-v6ops-host-addr-availability
Unique IPv6 Prefix Per Host （ホストごとのユニークIPv6プリフィクス割り当て）
draft-jjmb-v6ops-unique-ipv6-prefix-per-host
Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World（実ネットワークにおけるIPv6拡張ヘッダを含むパケットの破棄に関する観測）
draft-ietf-v6ops-ipv6-ehs-in-real-world>
Operational Implications of IPv6 Packets with Extension Headers （拡張ヘッダを含むIPv6パケットに対する運用上の影響）
draft-gont-v6ops-ipv6-ehs-packet-drops
Some Design Choices for IPv6 Networks（IPv6ネットワークの設計）
draft-ietf-v6ops-design-choices
IP/ICMP Translation Algorithm（rfc6145bis）（IP/ICMP変換アルゴリズム）
draft-bao-v6ops-rfc6145bis
Temporal and Spatial Classification of Active IPv6 Addresses （実利用されているIPv6アドレスに関する時間的・空間的分類）

これらのトピックスの中から、いくつかを紹介します。

◆ Identifier-locator addressing for network virtualization（ネットワーク仮想化のための識別子-ロケータ分離アドレス構造），draft-herbert-nvo3-ila

ネットワークの仮想化を実施するために、IPv6を利用する提案です。Facebook社では、IPv4アドレスの不足やネットワーク構築の柔軟性等の理由から、同社のデータセンター内でIPv6の利用を進めています。IPv6のアドレス空間の広大さを有効活用し、従来からのホストに対するアドレスでなく、データセンター内でネットワーク上を移動するタスクごとにIPv6アドレスを付与することで、ネットワーク仮想化を実現するというものです。この機構を実現するため、IPv6のアドレスをネットワーク上での位置情報を示すロケータ部と識別子部分に分離し、外部との通信にはDNSを用いてアドレスマッピングを実施します。実現には、nvo3（Network Virtualization Overlays）WGで議論されている、プラットフォームを利用できるとしています。

参加者からは、「この機構をインターネットワイドで利用する予定なのか」「機構自体はモバイルIPv6と同等だが、そちらの利用は検討したのか」「特にアドレスマッピングの際のセキュリティ課題の解決が重要であり、モバイルIP機構にはその検討も織り込んである」等の意見が挙げられました。

本件については、議論を継続することとなりました。

◆ Some Design Choices for IPv6 Networks（IPv6ネットワークの設計），draft-ietf-v6ops-design-choices

午後のセッションで実施の予定でしたが、時間の関係から午前中のセッションにて実施されることになりました。

IPv6ネットワークを構築する際に参考にできる、設計方針に関するドラフトです。これまで議論を重ねてきており、今回すぐに合意ができるだろう、という著者の導入から議論が始まりました。前回からの変更点として、企業ネットワークに関する扱いの変更（別文書にするべきという意見があったが、記述を継続）や、企業ネットワークで利用するアドレス種別についての詳述、組織内で利用する経路制御プロトコルに関するサーベイ結果の追加等が説明されました。

会場から、「企業ネットワークにおいては、その規模や形態によって要求条件がまちまちであり、サンプルとできる設計指針を決めることが困難であること」「NAT66を推奨すべきかの合意が無いこと」等、非常に白熱した議論になりました。かなりの時間を使いましたが議論が収束せず、午後のセッションに持ち越しとなりました。

2コマ目のセッションは、“Some Design Choices for IPv6 Networks”の議論の続きから始まりました。午前中のセッションでの議論を受け、ドラフトの著者より、IPv4関連の記述をなくすことおよびNAT66/NAPT66に関するコメントを追加することが述べられました。これらの変更を織り込んだドラフトを発行後、WGラストコールを実施することとなりました。

◆ IP/ICMP Translation Algorithm（rfc6145bis）（IP/ICMP変換アルゴリズム），draft-bao-v6ops-rfc6145bis

IPv4とIPv6間の変換についてはRFC6145にて記述されており、これはNAT64（RFC6146）や、464XLAN（RFC6877）の構成要素の一つとなっています。このRFCについて、6man WG で議論されRFC化された、フラグメントに関する変更、RFC発行後の訂正（Errata）、アドレスマッピングアルゴリズムの更新を取り込み、改版しようという提案です。マッピングアルゴリズムの更新に関するコメント等がありました。このドラフトはWGドラフトではありませんが、この後のプロセスを進めることも鑑み、WGドラフトにした後でWGラストコールを実施し、プロセスを進めることとなりました。

□v6ops WG
http://datatracker.ietf.org/wg/v6ops/charter/
□第94回 IETF v6ops WGのアジェンダ
http://www.ietf.org/proceedings/94/v6ops.html

（NTTネットワーク基盤技術研究所 藤崎智宏）

dhc WG関連報告

本稿では、IPv6の普及に伴い新たな利用方法が生まれつつあるDHCP（Dynamic Host Configuration Protocol）について、検討を行っているdhc WGを中心にIETFでの議論の動向をご紹介します。

◆ IPv6時代のDHCP

DHCPは、インターネットの初期から使われている「枯れた」プロトコルですが、最近ではIPv6の普及に応じた新しい利用法が注目されています。今回の報告でもご紹介する、一種の移行技術としてのDHCP 4o6がその一例です。また、IPv6の広大なアドレス空間を活かすために、末端のホストにもDHCPでプリフィクスを配布するという利用方法も提案されています。

IETFでのDHCP関連の議論は、dhc（Dynamic Host Configuration）WGで行われています。現在、dhc WGは主にIPv6用のプロトコルである、DHCPv6の拡張機能の標準化について議論しています。具体的には、現状の基本プロトコル仕様であるRFC3315に、ISP等から家庭やオフィスネットワークにプリフィクスを自動配布する仕組みとして使われているprefix delegation（RFC3633）を統合した形の改訂仕様策定、冗長化のためのフェイルオーバー機能の標準化、セキュリティやプライバシー改善のための拡張機能の標準化などが対象となっています。

以降では、このdhc WGの議論を中心に、DHCP関連の動向をご紹介します。

◆ DHCP 4o6 Hackathon

IETF Hackathonは、IETF直前の土日を使って、策定中の最新プロトコル機能を集中的に開発するという派生イベントで、第92回IETFから継続的に開催されています。dhc WGとしては前回に続いての2回目の開催で、今回は、IPv4のホスト設定プロトコルとしてのDHCPv4を、DHCPv6のオプションとして定義することでIPv6ネットワーク上で動作させるという、DHCP 4o6プロトコル（RFC7341）がテーマとして選ばれました。筆者もこのイベントに参加し、Hackathonで開発の主対象であった、Internet Systems Consortium（ISC）が従来のISC DHCPサーバに替わる新たなDHCPサーバとして開発中の、Keaサーバの開発を手伝ったほか、自作のクライアント実装を用いてKeaとの相互接続性も検証しました。短時間でしたが、最低限の相互接続性まで確認でき、また個人的に以前から興味のあったKeaサーバの実装や設定方法などの理解が深まったこともあり、WGとしても個人としても有意義なイベントになったと思います。

“running code”を重んじるというのが建前だったはずのIETFも、仕様先行の悪癖が目立って久しくなっていますが、このHackathonのようなイベントや、ドラフト仕様への実装状況の記載を推奨する動き（RFC6982）など、IETFを「手を動かす」エンジニアの集まりとして再構築しようとする試みは、筆者自身も開発者なので嬉しく思います。

● バッジを付けることで自分が理解できる言語を示せます

◆ dhc WGミーティング

次に、11月5日（木）午後に開催された、dhc WGのミーティングの概要をご紹介します。まず、もっとも時間をかけて議論された、2件の発表について詳述します。

1. Relay Initiated Release

この提案は、米Juniper社のSunil Gandhewar氏によるもので、DHCP（IPv6とIPv4の両方）のクライアントが、アドレスその他のネットワーク資源を割り当てられたまま移動してしまったような場合に、クライアントに代わってリレーエージェントから、それらの資源を解放できるようにするというものです。これにより、（特にIPv4の場合）割り当て用アドレスプールの利用効率を上げたり、サーバが管理する状態を減らして、負荷を下げたりすることを目的としています。今回のIETFに先立って、個人ドラフトからWGドラフトとしての採択の是非がMLで議論されている中での発表となりました。

当初ML上では、おそらくすでにこの機能を独自仕様として用いている製品のユーザーと思われる人たちからの賛成が相次ぎ、そのまますんなりと採択されるかのように見えました。しかし、資源の「リース」という、DHCPにおける根本的な概念の性質（リースは有効期限で管理され、その間割り当てを受けたクライアントはその資源を利用できると仮定できる）を覆す提案であることから、提案への懸念を表明する声も多く上がるようになりました。

ミーティングにおける発表と質疑応答でも、相反する二つの立場がぶつかる形となりました。提案の著者は、独自に集計した統計情報などから、サーバが保持するクライアントの状態数が膨大になり得ることや、自ら解放メッセージを出すクライアントがほとんど存在しないことなどを理由として、提案の必要性を訴えました。一方、この拡張の悪影響を懸念する人からは、クライアントが実際にリソースを保持している期間などの統計がなければ、リレーエージェントによる解放が安全かどうかはわからないといった指摘が挙がり、結局、明確な合意は得られませんでした。なお、会合後に現時点ではWGドラフトとしての採択は見送るとの結論が、WGのチェアからMLにて通知されました。

2. Moving forward on Secure DHCPv6

Secure DHCPv6とは、公開鍵方式によるDHCPv6クライアント・サーバ間の認証プロトコルです。RFC3315で規定されている、共有鍵方式のプロトコルの置き換えとして提案、議論されてきました。なお、筆者もこのドラフトに共著者として関わっています。Secure DHCPv6のドラフトは、すでにWGのラストコールを終え、IESGでのレビューにかけられる直前の状態となっていたのですが、この段階で担当のarea directorやセキュリティの専門家による事前レビューで多くの懸念が指摘され、差し戻された形になっていました。指摘事項は主に、このプロトコルの利用シナリオが不明確であること、厳密な安全性を犠牲にして利便性を求める"TOFU（Trust on First Use）"モードが安易に導入されていること、の2点でした。

一方、IETF全体でプライバシーを重視する動きが高まっているのに呼応する形で、DHCPv6に暗号化機能を導入する提案も、独立した個人ドラフトとして提出されていました。この提案は、Secure DHCPv6のオプションを一部利用しており、その意味では関連する技術となっています。

そこで、WGのミーティング前に、これらのドラフトの著者、WGチェア、セキュリティ技術の専門家などの関係者による小規模な非公式ミーティングを開き、今後の方向性を話し合いました。その結果、このグループ内では以下の方針で合意されました。

- 認証と暗号化機能を単一ドラフトに集約し、（このプロトコル内では）暗号化を必須とする
- TOFUモードはこの単一ドラフトの対象外とする
- 利用シナリオはプロトコルとは別なドラフトで扱う

公式のWGミーティングでは、チェアがこの経緯を説明し、暗号化ドラフトの著者である清華大学のLishan Li氏が、統合プロトコルの概要を紹介しました。参加者からは大きな反対の表明や問題点の指摘もなく、提案した方向性はすんなりと受け入れられました。DHCPv6のプロトコルそのものとはやや独立した話題のため、そもそもあまり興味を持たれていなかったという面もありそうですが、チェアを含めて「声の大きい」人を交えて事前に意見のすり合わせをしていたのが、奏功した例だと言えるでしょう。IETFのミーティングは議論に十分な時間が与えられないことも多く、また単純な誤解などから大きく「炎上」してしまうようなことも珍しくないので、このように事前に話を付けておくという手法はしばしば取られています。

3. その他の発表

前記2点の発表以外に、dhc WGミーティングでは以下の発表が行われました。タイトルと概要をそれぞれご紹介します。

- YANG Data Model for DHCPv6 Configuration:
  DHCPv6の設定情報を、IETFの標準モデル言語であるYANG（Yet Another Next Generation）を使って記述するという提案です。現状では、基本的に進捗報告のみです。

- DHCPv6 Failover Update:
  DHCPv6サーバ冗長化のための、フェイルオーバープロトコルの仕様ドラフトです。80ページに及ぶ大きなドキュメントで、レビューの負荷が問題になりそうです。

- DHCPv6 Prefix Length hint issues:
  prefix delegationでクライアントから通知する、プリフィクス長の扱いの曖昧さに伴う問題を指摘して、処理の指針を提案しています。WGドラフトとして採択されそうです。

- DHCPv6bis update & issues discussion:
  RFC3315の改訂仕様（前述）の現状報告です。改定項目はWeb上のissue管理ページにまとめられていて、随時MLなどでWGとして議論して改訂が進められています。

（Infoblox, Inc. 神明達哉）


● IETF 94の様子

DNS関連WG報告

IETF 94では、WIDE Projectを中心としてスポンサーやコントリビュータ各社からのボランティアによってNOC（ネットワークオペレーションセンター）メンバーが構成され、会場内外のネットワーク構築と運用が行われました。私もNOCメンバーの一員として、少しだけ設営と運営に関わらせていただきました。前回の横浜開催であるIETF 54でも、学生としてNOCメンバーボランティアに参加していました。その経験をふまえ前回と今回との会場ネットワーク環境を比較すると、ネットワークを取り巻く環境は格段の進歩を遂げていることを、あらためて実感することができました。

本稿では、DNSに関連するWGとして、dnsop WG、dprive WG、dnssd WGの動向をご報告します。

◆ dnsop WG（Domain Name System Operations WG）報告

dnsop WGの会合は、150分枠で開催されました。まずは恒例の、Internet-Draftの状況確認から行われました。前回の会合から、3本のRFCが発行されたことが報告されました。RFC7583、RFC7646、RFC7686です。他にもWGラストコールが行われているInternet-Draftが6本あり、活発な活動が行われていることを感じられました。次に、draft-jabley-dnsop-refuse-anyに関する発表と議論が行われました。このInternet-Draftは、ANYクエリによってパケットサイズの大きな返答が返ってしまうことを防ごうという趣旨の提案です。昨今、DNSを用いた増幅攻撃が問題となっているため、ANY!=ALLの解釈のもとに、返答パケットのサイズを減らす提案が行われました。WG Internet-Draftとする方向で議論が行われました。

さらに、RFC6761bisに関する発表と議論が行われました。RFC6761は、"Special-Use Domain Names"というタイトルであり、ドメイン名の空間をDNS以外の用途（「従来のドメイン名とIPアドレスの相互変換ではなく、サービス発見のため」「DNSの仕組みは使いながらも、そのセマンティクスは従来のDNSではない」など）に使う場合の注意事項を述べたものです。しかし、この特別なドメイン名を決定するプロセスや条件に関する記述が不十分だという意見が出され、文書を改定するためのデザインチームから報告が行われました。特に、RFC2860にて述べられているIANAの役割定義に関するMoU（覚書）に反するのではないかといった意見が出され、議論が続きました。今後も議論が継続される模様です。

他にも、draft-jabley-dnsop-ordered-answers、draft-ogud-dnsop-maintain-ds、draft-muks-dnsop-dns-message-checksums、draft-muks-dns-message-fragments、draft-wessels-edns-key-tagに関する発表と議論が行われました。それぞれの概要を紹介します。

draft-jabley-dnsop-ordered-answersは、DNSの返答パケットにおけるそれぞれのセクションにて、どの順番でRR（Resource Record）を並べるかを提案したものです。

draft-ogud-dnsop-maintain-dsは、DSレコードの管理において、DSを初めて導入する場合とDSを消す場合について、CDSとCDNSKEYレコードを用いて子ゾーン側からその意思を示す手法を提案しています。

draft-muks-dnsop-dns-message-checksumsは、UDPパケットのフラグメントを用いて偽の情報を覚え込ませようとする攻撃を防ぐために、EDNSオプションとしてDNSメッセージのチェックサムを定義しようという提案です。

draft-muks-dns-message-fragmentsは、DNSの返答パケットがフラグメントされる場合の問題点を述べ、DNSメッセージのフラグメントを廃止しようという提案です。

最後に、draft-wessels-edns-key-tagは、RootゾーンのKSK更新が計画されているため、新しいKSKに更新された際に、リゾルバサーバのトラストアンカーがどの程度更新されたかを判別できるように、Key IDをつけようという提案です。

他にもいくつかの発表と議論が行われ、時間いっぱい会合が行われました。dnsop WGは、引き続き活発な議論が行われていくと思われます。

● 日本開催ということもあり、スポンサーには多くの日本企業が名前を連ねました

◆ dprive WG（DNS Private Exchange WG）報告

dprive WGの会合は、120分の枠で開催されました。まず、Internet-Draftの状況が確認され、続いてdraft-ietf-dprive-dnsodtlsに関する議論が行われました。この文書は、DTLS（Datagram Transport Layer Security）をDNSに用いるという提案です。今回は、DTLSでのパケットサイズ増加による、フラグメントの問題に関して議論が行われました。どのようにフラグメントを防ぐか、という意見が交換されましたが、DNSに限らずDTLSを利用した場合に発生する問題であるため、フラグメント自体を発生しないようにする手法を提案する方向になりました。

次に、draft-ietf-dprive-dns-over-tlsに関する発表と議論が行われました。DNS-over-TLSのドラフトは、WGラストコールに向けて問題点を改善しており、その経過報告が行われました。この文書は、TLSを用いたDNSサーバの認証を提案しており、その実装の進捗状況についても報告されました。ポート番号としては、853番が割り当てられています。

さらに、draft-krecicki-dprive-dnsencについての発表と議論が行われました。これは、トランスポート層プロトコルとは独立させて、DNSのトランザクションを暗号化しようという提案です。NSK RRという新しいリソースレコードで、サーバの公開鍵を公開することで、DNSトランザクションを暗号化します。当然、DNSSECとの併用が必要となります。この提案に対して、サーバに対してのDDoSを容易に行うことができるのではないか、またアプリケーションレベルで暗号化を再度定義するのは冗長なのではないか、といった意見が出されました。引き続き議論が行われます。

この他にも、draft-wing-dprive-profile-and-msg-flows、draft-am-dprive-evalといった文書に関して、発表と議論が行われました。drpive WGでは、DNS over DTLS、DNS over TLSといった提案を基本とし、DNSのプライバシー問題解決という重要かつ困難な問題を解決するため、引き続き議論が行われます。

◆ dnssd WG（Extensions for Scalable DNS Service Discovery WG）報告

dnssd WGは、DNSを用いたサービス発見を、さまざまな範囲にて行うプロトコルを実現するためのWGです。まず、Internet-Draftの確認が行われました。draft-ietf-dnssd-hybridならびにdraft-ietf-dnssd-pushがWGラストコール直前であること、またdraft-ietf-dnssd-mdns-dns-interopのWGラストコールが終了し、IESGレビューに回す前の修正段階であることが報告されました。

会合では、draft-otis-dnssd-scalable-dns-sd-threatsについての発表と議論が行われました。これはdnssdを実現するにあたっての、セキュリティ脅威を分析した文書です。dnssdにおけるサービス発見範囲はマルチキャストによって限定されているため、いくつかのセキュリティ的な懸念点が存在することを述べています。まだ広く理解を得られる文書となってはいないといった指摘があり、引き続き議論が行われます。

次に、draft-ietf-dnssd-pushと、draft-ietf-dnssd-hybridに関する発表と議論が行われました。

draft-ietf-dnssd-pushは、DNSのレコードが変更された場合にその更新を動的に通知する仕組みを提案した文章です。今までのDNSでは、たとえ権威DNSサーバにおいてレコードが更新された場合でも、リゾルバDNSサーバにおいてキャッシュの保持時間が残っている間は、再度権威DNSサーバへの問い合わせを行わない仕様となっています。そのため、ユーザーには古いレコード情報が返答される結果となります。この提案では、限られた範囲内のリゾルバDNSサーバに対してレコードの更新を通知することで、頻繁なレコード更新に追従できるサービス発見を実現することを目的としています。

またdraft-ietf-dnssd-hybridは、Multicast DNSによるサービス発見の結果を、Unicast DNSの名前空間にマッピングする手法を提案しているものです。

どちらの発表も、前回会合からの改善点についてのまとめでした。また、大きな問題点の指摘も無く、WGラストコールが行われることが確認されました。

最後に、draft-aggarwal-dnssd-optimize-queryに関する発表と議論が行われました。この文書は、dnssdの規模性を危惧し、その規模性を向上させるために、TXT RRにAllJoynに従ったkey/valueペアの情報を入れることで、クライアントに検索のためのヒントを与え、検索回数を減らすという提案です。AllJoynは、Allseanアライアンスによって IoTのために制定された規格であり、機器のプロファイルや、機器と機器の連携に関する情報などを提供するフレームワークです。このAllJoynをどうdnssdに組み込んでいくのか、今回の発表と文章からでは、まだはっきりと理解できませんでした。

（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）

IGFジョアンペソア会合（IGF 2015）報告

2015年11月10日（火）～13日（金）にかけて、ブラジル・ジョアンペソアでインターネットガバナンスフォーラム（IGF）が開催されました。さまざま関係者により幅広い議論を行うための国際連合主催の会合で、今回で10回目となります。本稿では、IGFの概要とともに、主なトピックをご紹介します。

◆ IGFの特徴

IGFは国連主催の会議ではありますが、リモート参加も含めて誰でもが参加できます。「政府」「学術」「市民」「民間」「技術コミュニティ」といったそれぞれの立場の関係者が平等に参加する資格を持つ、いわゆる「マルチステークホルダーアプローチ」で議論できることが特徴です。

No.47 インターネット10分講座「IGF（Internet Governance Forum）とは」
https://www.nic.ad.jp/ja/newsletter/No47/0800.html

プログラムのうち、100を超える「ワークショップ」と呼ばれるセッションは、すべて公募に基づき選定されます。筆者は、このプログラムを選定するプログラム委員会に相当するマルチステークホルダーアドバイザリーグループ（Multistakeholder Advisory Group; MAG）のメンバーを2014年から務めています。

No.58「IGFの特徴とイスタンブール会合のプログラムについて」
https://www.nic.ad.jp/ja/newsletter/No58/0650.html
About the MAG
http://www.intgovforum.org/cms/magabout

また、例年通り、開会日の前日11月9日（月）をDay0と呼び、この日も関連する各種会議が開催されました。

◆ 会議の雰囲気

国連主催の会議のため、入場時のセキュリティチェックや、オープニングやクロージングセレモニーでのスピーチはありますが、それ以外はいわゆる政府間会議よりもおそらくカジュアルです。服装の面でも、ネットワークオペレータの会合のようにTシャツとジーンズの人はあまり見かけませんが、スーツにネクタイの方も少数派であり、まちまちです。参加者がスタンドマイクに立ち発言するところは、インターネットコミュニティの他の会議と共通しています。参加者数は、IGF 2015では2,400名（116ヶ国以上）を超える参加登録があり、参加者は前述した五つの立場を選択した上で登録をします。

IGFの参加者リスト
http://www.intgovforum.org/cms/igf2015-participantslist

JPNICも属する技術コミュニティからの参加は、RIR、ISOC、ICANN、ccTLD、IEEE、IAB、W3Cなど主要なインターネット団体が中心です。RIRのCEO達をはじめ、IAB、ISOC、ICANNなどからもCEOやチェアが参加し、かなりコミットしていることが見て取れます。また、インターネットの父として知られているVint Cert氏も参加しており、オープニングでスピーチをしたり、その他複数のパネルでも登壇したりしていました。

民間からの参加としては、欧米の大手組織（21st Century Fox社、Amazon社、Cisco社、 CloudFlare社、Ericsson社、Facebook社、Google社、Microsoft社、Mozilla財団等）の参加が多く見受けられました。日本からは総務省4名、業界・コミュニティから4名の参加があり、そこに加えてJPNICからは2名参加しました。日本政府代表として、総務省の阪本泰男総務審議官がオープニングでスピーチをしています。

◆ IGF 2015の特徴

2015年は、IGFおよびインターネットガバナンスにとって重要な年です。というのも、IGFの開催は無期限に保証されているものではなく、国連総会で承認されている活動年限は今年、2015年までとなっており、2016年以降の開催の是非は、2015年12月にニューヨークで開催される国連総会で加盟国により決議されるからです。IGFは、政府間中心での議論ではなく誰もが参加できる会議であり、ボトムアップでオープンなインターネットコミュニティの精神とも親和性があります。ただ一方で、「対話のみで具体的な成果がない」との批判も一部から受けてきました。

2015年はこれらの批判に対応し、IGF開催継続の承認を得るために、具体的な実績を示すことが重要でした。そのため、IGF 2015では対話よりも、課題に対して一歩踏み込んだ成果を出すことに重点が置かれました。その内容については、後述の「IGF 2015での成果の提示に向けた三つの取り組み」でご紹介しています。

また、今回の三つの成果の中でBest Practices（最良事例）として取り上げられているテーマや、ネットワーク事業者に関わりのある議論を見ても、ネットワークの運用やサービスが技術コミュニティだけで完結するものではなくなってきています。運用者が蓄積した経験を共有したり、セキュリティなどの分野においては、政府も含めた異なる立場の関係者と、課題解決に向けた連携が求められたりする傾向が、さらに強まっていることが見て取れます。

◆ IGF 2015のテーマ

IGF 2015のテーマは「インターネットガバナンスの進化：持続可能な発展の促進（Evolution of Internet Governance: Empowering Sustainable Development）」でした。このテーマ設定は、インターネットガバナンスに関するグローバルな議論およびIGFの開始から10周年を迎えたタイミングであることが、背景の一つとして挙げられます。テーマに対してさらにサブテーマが設けられ、着目されている課題が反映されています。

◆ IGF 2015での成果の提示に向けた三つの取り組み

IGF 2015は、前述の通り国連総会で実績を示す必要から、具体的な成果に重点を置き、三つの取り組みがなされました。

・各種Best Practices文書の策定
 - IPv6も含むテーマごとに策定されたBest Practices文書へのリンクは、以下の通りです。
 http://www.intgovforum.org/cms/best-practice-forums/2015-bpf-outs

・Connecting the Next Billion（次の10億をつなげる）文書の策定
 - 地域・国単位のIGFにも参加を促した共通のテーマ
 http://www.intgovforum.org/cms/policy-options-for-connection-the-next-billion/cnb-outdocs

・Dynamic Coalitionsの再活性化
 - 特定の課題に特化して継続的に検討を行うグループ
 http://www.intgovforum.org/cms/dynamiccoalitions

いずれの取り組みも、会議での一度限りでの議論ではなく、課題の継続的な検討をめざしました。各テーマのBest Practicesの検討グループは、会議の半年以上前からオンラインでの議論を元に文書を策定し、IGF会議での議論に臨みました。検討グループも、リモートも含め、誰でも参加できました。

なお、2015年にBest Practicesとして取り上げられた六つのテーマの中でも

・IXPの設立環境
・IPv6の導入促進環境
・スパム対策
・CSIRT（Computer Security Incident Response Team）の設立

といった技術コミュニティに関わりの深いテーマが複数見受けられます。特に「IPv6導入を可能にする環境作りの最良事例（BPF（Best Practices Forums）Creating an Enabling Environment for IPv6 Adoption）」は、RIR関係者が積極的に関わり、文書化しました。後の項で概要をご紹介します。

◆ IGF 2015のプログラム

IGFでは多くのプログラムが並行して行われ、IGF 2015では4日間で100を超えるセッション、最大で11のパラレルセッションが開催されました。従って、すべてのセッションに参加することは不可能であり、自らの関心分野を基に取捨選択が必要です。筆者は、JPNICの活動にも関わる分野として、IANA機能の監督権限移管に関わるパネル、番号資源コミュニティについて紹介したOpen Forum、IPv6に関するパネル（IPv6のBest Practicesとは別）に登壇しました。次項でネットワーク事業者に関わりのある議論についてご紹介しますが、全体としてどのようなセッションがあったのかはIGFの公式ページより確認可能です。

・IGF公式ページ
「セッションスケジュール」「セッション概要」「各セッションの発言録」が参照可能
http://www.intgovforum.org/cms/home-36966

・すべてのワークショップの動画
https://www.youtube.com/user/igf/videos

● 筆者からは日本における IPv6 への取り組みを紹介しました

◆ ネットワーク事業者に関わりのある議論

ここでは、ネットワーク事業者にも関わりのある三つのセッションを紹介します。

◇ IPv6導入を可能にする環境作りの最良事例：
BPF Creating an Enabling Environment for IPv6 Adoption

・IPv6 Promotion Councilや民間、各国政府での取り組みを包括的にまとめたもの

・例えばドイツ政府は、自らLIR（日本国内におけるIPアドレス管理指定事業者のようなもの）となり、希望する省庁にIPv6を割り当てるというユニークな取り組みを行っている

・APNICの藤井美和氏と筆者を通して、日本の事例として総務省および国内のISPの取り組みを紹介

・IPv6は、今後アクセスの課題やIoTと絡めて関心が寄せられており、2016年も最良事例に取り組むことが提案されている

・IPv6の導入促進環境における最良事例文書
http://www.intgovforum.org/cms/documents/best-practice-forums/creating-an-enabling-environment-for-the-development-of-local-content/581-igf2015-bpfipv6-finalpdf

◇ ゼロレーティングとネット中立性：
A dialogue on“zero rating”and network neutrality

・携帯事業者またはISPの対応として、特定のアプリケーションまたはサービスのデータに対して課金しないゼロレーティングについて法制化をしている国もすでにある
 - 携帯事業者によるデータ量の上限を緩和し、ユーザーが利用しやすい環境につながるので支持といった意見もある
 - 一方、特定のコンテンツ事業者が費用負担を行うことによるゼロレーティングは、情報の自由な流通に反するとして警戒する姿勢を示す政府もいる

・法制化が必要なのか、またその場合どういう対応が適切なのかは今後さらなる研究が必要

◇ サイバーセキュリティと信頼の向上：
Enhancing Cybersecurity and building digital Trust

・サイバーセキュリティは技術コミュニティのみで解決する問題ではなく政策的な検討が必要だが、政府のみではなくさまざまな関係者が参加し連携するべき

・サイバーセキュリティの課題は広く、どの問題に対して具体的にどう連携するのか、ということが今後の検討課題
 - IoTなど従来にないセキュリティの課題も浮上
 - サイバーセキュリティに関する国際協定、一定のセキュリティ基準を満たす技術の標準化を求めることの是非

・プライバシーを保護し、暗号化を維持しながらサイバー犯罪に対応することが課題
 -「WS 141 Law enforcement in a world where encryption is ubiquitous」（暗号化が至るところで使われている環境における法執行）でも議論
 - プロトコルの標準化において、法執行機関等が裏で復号できる方法を認めるかといった議論も含まれるため、IETF関係者も参加

◆ 2015年12月の国連総会に向けて

2015年12月の国連総会では、世界情報サミット（WSIS）の開催から10周年を迎え、その成果の振り返りと評価（WSIS+10）（http://unpan3.un.org/wsis10/）が国連の加盟国により行われます。IGFはWSISをきっかけとして立ち上がった会議であり、IGFの活動年限の延長に関する決議も、このWSIS+10と無関係ではありません。「課題解決は政府間中心で検討を進めないと効果がない」といった一部の主張がある中、WSIS+10においてマルチステークホルダーアプローチによる成果が適切に評価されることが重要となります。IGF 2015では、12月の国連総会での評価に向けて、国連のWSIS+10のファシリテーター2名を招待し、IGFの参加者が成果文書のドラフトを基に意見表明を行う機会としてメインセッションを開催し、議論が行われました。

◆ 次回以降のIGF

2016年以降の開催については、2015年12月の国連総会での承認事項であるため、本稿執筆時点での開催日程は未定ですが、次回2016年のIGF 2016は、メキシコがホストを務める意向をすでに発表しています。

（JPNIC インターネット推進部 奥谷泉）

● IGF は国連主催の会合です