APRICOT 2014/APNIC 37カンファレンス報告

APRICOT 2014/APNIC 37カンファレンスは、2014年2月18日（火）～28日（金）にマレーシアのプタリン・ジャヤで開催されました。

当初、タイのバンコクで今回のカンファレンスの開催が予定されていましたが、タイ国内の反政府デモにより政情が安定しないことから、開催1ヶ月前に急遽、プタリン・ジャヤに開催地を変更することになりました。

全体報告

◆ カンファレンスの構成

2週間の会期中、前半は主にワークショップに充てられます。BGPやMPLSといった、講師の話を聞くだけでは身につきにくいトピックについて、ハンズオンなども含めた演習形式で行われます。

後半は、IRR、DNSやアドレス管理といった、ネットワークの運用者にとって基礎的なトピックに関するチュートリアルが開催されるほか、各種の最新動向の報告やポリシーに関する議論などが行われるカンファレンスが開催されます。

筆者が参加したチュートリアル・カンファレンスのうち、DNSSECに関するチュートリアルでは、参加者がそれぞれ自己紹介を行う時間がありました。DNSやDNSSECの基礎知識を学ぶためにやってきたISPのオペレーターや、ISPのオペレーターにDNSSECを教える際にどのように教えるかを学びに来ている人など、さまざまな背景を持つ人が集まっていました。そして、参加者それぞれが、質問を交えながら講師の説明に耳を傾けていたのがとても印象的でした。

チュートリアルやカンファレンスと併せて、BoFが開催されます。取り上げられるテーマは毎回変わります。今回は、災害時における通信網の再構築、IPv4アドレスのリース、Network Function Virtualization（NFV）、といった旬の話題にフォーカスが当てられたほか、各国におけるIPv6の普及度調査を共有するBoFも開催されました。

各プログラムの内容や、その際に利用された資料の大半は、APRICOT 2014/APNIC 37カンファレンスのWebサイトから参照することが可能です。一部のプログラムでは、当日の発表や質疑応答の内容が発言録として公開されています。

APRICOT 2014 - Program
https://conference.apnic.net/37/program

◆ 他の組織と連携したプログラムのご紹介

今回のカンファレンスでは、「他の組織との連携」が非常に意識されており、ICANN、ISOCやAPCERTといった、これまで連携することが少なかった組織が主体となって検討されたプログラムが多くありました。これらのプログラムが加わることで、これまでのカンファレンスと比べ、より幅広い分野がカバーされるようなった印象を持ちました。そのうち、特徴的なプログラムをご紹介します。各プログラムの詳細については、前述のプログラムページをご覧ください。

- ICANN

ICANNからは、これまでの活動のアップデートのほか、さまざまな立場の話者を招いて、「From Governance to Cooperation: Decoding the Puzzle」と題してインターネットガバナンスに関するパネルディスカッションの時間が設けられました。このパネルディスカッションの模様は、P.28「アドレスポリシー関連報告」で詳しく記述します。

- ISOC

ISOCのプログラムは、ルーティングセキュリティ、DNSSEC、IPv6の普及に関する話題を中心とした構成となっています。

日本におけるルーティングセキュリティやDNSSECへの取り組みについて報告が行われたほか、前回のAPRICOT 2013/APNIC 35カンファレンスで話題となった、オープンリゾルバの全世界的な現状についても報告されました。いずれの内容も、参加者から多くの関心は高く、質問が多く寄せられていました。

- APCERT

APCERTはアジア太平洋地域に所在するCSIRT（Computer Security Incident Response Team）から構成されます。今回のプログラムでは、マレーシア、オーストラリアおよび韓国での活動が報告されたほか、日本のCSIRTであるJPCERTコーディネーションセンター（JPCERT/CC）が提供する、利用中のDNSサーバがオープンリゾルバになってないかどうかを確認するためのWebページが紹介されていました。

これらのプログラムと連動する形で、Network Abuse（ネットワークの不正利用への対応窓口）に関するBoFが開催されました。まずはじめにAPNICより、不正利用を申告する人が参照する、WHOISデータベースの正確性向上への取り組みが紹介されました。引き続いて、APNICデータベースを活用してNetwork Abuseへの対応を行うパキスタンでの事例が紹介されました。JPNICでもAPNICと同様にWHOISデータベースを提供しており、Network Abuseへの対応も行う場面がありますが、これらの報告は日常業務の際に参考となるものでした。

◆ APNIC Member Meetingについて

最終日にはAPNIC Member Meeting（AMM）が開催されました。AMMでは主にAPNICの活動内容に関する報告、期間中に開催されたSIGや各種セッションの報告、次回のAPNIC 38カンファレンスの紹介が行われました。

● 福岡で開催される次回APRICOT 2015/APNIC 39の告知をする前村昌紀

AMMでは通常、これらの報告と併せて、APNIC理事会メンバー（任期2年）を選出するための選挙が行われます。今回は、3名の改選枠に対して、以下の3名のみが立候補したため、選挙は行われませんでした。

・Yan Ma氏（Beijing University of Post and Telecommunication）
・Che-Hoo Cheng氏（Beijing University of Post and Telecommunication）
・前村昌紀（JPNIC）

AMMでは、改選枠以上の立候補がなかったため無投票となったこと、および候補者全員がAPNIC理事会メンバー（EC）として選出されたこと、前村昌紀（JPNIC）が理事会議長となったことがそれぞれ報告されました。

上記3名に加えて、今回の改選対象には含まれない4名、およびAPNIC事務局長Paul Wilson氏の合計8名の体制で、新APNIC理事会がスタートしています。本件に関しては、JPNICからのアナウンスもご覧ください。

APNIC EC（理事）にJPNIC前村昌紀が再選
https://www.nic.ad.jp/ja/topics/2014/20140303-01.html

◆ 次回APNICカンファレンスについて

次回のAPNIC 38カンファレンスは、2014年9月9日（火）～19日（金）に、オーストラリア・ブリスベンで開催されます。また、次回APRICOTとの共催となるAPRICOT 2015/APNIC 39カンファレンスは、APAN 39カンファレンスとも共催となり、2015年2月24日（火）～3月6日（金）に福岡市での開催が予定されています。JPNICは、カンファレンスの実行委員会に参画しており、既に準備を進めています。

APRICOT 2015/APNIC 39カンファレンスは、京都市で開催されたAPRICOT 2005/APNIC 19カンファレンス以来、10年ぶりに日本で開催されることになります。次回はぜひ現地に足を運んでいただき、皆さん自身でカンファレンスの雰囲気を感じ取ってみませんか?

（JPNIC IP事業部 川端宏生）

● 会場となったSunway Resort Hotel & Spa

アドレスポリシー関連報告

今回のAPNIC 37カンファレンスでのポリシー議論は、従来のIPアドレスをはじめとした番号資源に関するポリシーのみではなく、「インターネットのガバナンス」や「gTLDをはじめとしたICANNでのポリシー策定」など、より大きな括りでの「ポリシー」について議論する機会が設けられていたことが特徴的でした。また、アドレスポリシー提案に関する議論では、従来のポリシー提案に加えて「コンセンサス確認のあり方」や「IPv4アドレスリース」に関する議論も行われました。

これらは一見、方法論の話のようですが、コンセンサス確認方法の変更は「議論の内容を尊重しながらコンセンサスを判断するのか、それとも匿名の投票に重点が置かれるのか」、IPアドレスのリースは「アドレスを利用する権利なのか」などの基本的な考え方を問われるものです。アドレスポリシーに関する提案と併せて、主なトピックや、それぞれの議論の様子をご紹介します。

◆ ICANN Updateセッション

これは初の試みとしてICANNのアジア拠点が企画し、これまでAPNICフォーラムで共有されることのなかった、gTLDをはじめとするドメイン名に関する動向が共有されたセッションです。

APRICOT Plenaryの開始前、APNICカンファレンス初日の午前中のセッションでしたが、約60名以上の参加があり、会場はほぼ満席でした。このうち約半数以上がICANN会議の常連参加者、残りが普段ICANNの活動に馴染みのない参加者であったという印象です。

紹介、議論されたトピックスは以下の通りです。

- ドメイン名があらゆる環境で幅広く利用可能な状態（Universal Acceptance）
- 国際化ドメイン名の異体字（Internationalized Domain Name（IDN）Variants）
- gTLD WHOISの再定義および置き換え（Refining and replacing WHOIS）
- 新gTLDの動向（New gTLD update）

マイクの設置されたロの字形のテーブルにICANNの常連参加者が座り、普段ICANNと関わりのない参加者がそれを囲む椅子に座って聞く形に自然となっていたためか、発言はICANNの常連参加者が中心となっていました。

APNIC地域からの声を吸い上げることを目的として考えると、初心者も発言しやすい雰囲気作りなど改善の余地はありますが、常連参加者による発言の様子を含めて、実際のICANN会議の雰囲気をかなり味わうことのできるセッションであったと思います。

当日の発表資料および議論の録音は次のURLよりご覧いただけます。

Asia Pacific Regional Discussions - APRICOT, Feb 2014
https://community.icann.org/display/gseasiawkspc/Asia+Pacific+Regional+Discussions+-+APRICOT%2C+Feb+2014

● 会議の様子

◆ アドレスポリシー提案に関する主な議論

全体としては「1.0.0.0/8レンジのうち、大量のトラフィックを引き寄せることからAPNICがリザーブしてきたIPv4アドレスを今後どう管理するのか」を中心に議論が行われました。

コンセンサスが得られた提案は議論された3点中、prop-109の1点です。これに伴い、「1.0.0.0/24」および「1.1.1.0/24」は、研究目的でAPNIC Labs（研究部門）に割り振られることになります。国内の議論では、APNICに分配することへの公平性について指摘がありましたが、以下に示す通り、公共の実験ために利用されることが確認され、コンセンサスに至りました。

- 実験結果は一般公開する
- 現在の協力者Google社に限らず誰でも実験に協力可能である
- 実験に参加する組織とは情報の取り扱いに関する合意書を締結する

一方、同じく1.0.0.0/8レンジに関する提案であったprop-110は一度Policy SIGでコンセンサスが得られたものの、APNIC総会でPolicy SIGに参加できなかった人による一定数の反対が確認され、コンセンサスに至らず、その後、提案者により取り下げられています。

これは、日本から参加したオペレーターが中心となって、DNS anycast用に、誰もが利用できるアドレスを提供することによるセキュリティリスクを、具体的な懸念点として指摘したことが大きな要因となりました。Policy SIGで通ったものは多くの場合、形式的にはAPNIC総会で意思確認はするものの、そのまま承認されることが多い中、プロセスとして印象的でした。

各提案の結果は文末の「参考：アドレスポリシー提案の結果」よりご確認ください。

◆ その他アドレスポリシーに関わる議論

その他の、アドレスポリシーに関わる議論をご紹介します。

- コンセンサス確認方法の変更：

現在、Policy SIGでの提案は参加者による議論後、賛否の確認を会場での挙手による意思表明により確認しています。

しかし、以下の理由から、上記に代わり「ポリシー提案への賛否をボタン式で意思表明をする形式へ変更する」案が、今回Policy SIGにて、APNIC事務局からコミュニティへの相談、という形で紹介され、議論が行われました。

- リモートでの参加者も意思表明に参加できるようにしたい
- アジア太平洋地域では、他の参加者に見られる形で意思を表明することへの抵抗を持つ人もいる

現時点では、次回の会議に実施を試す方向でAPNIC担当者が準備を進めていると聞いています。

一方、「アドレスポリシー提案に対するコミュニティとしての判断結果は、結果自体のみではなく、議論のプロセスと透明性が大事。投票システムのようなものを導入するとそれが失われるのではないか。」との懸念も、一部の参加者からは表明されていました。

- IPv4アドレスのリース：

IPv4アドレスリースが実際に行われていることを踏まえて、APNICのアドレスポリシーとを見なすべきか議論が行われました。

IPv4アドレスの移転とリースの違いは、IPv4アドレスの分配先である状態は維持しつつ、利用していないIPv4アドレスを他組織で利用することを、当該IPアドレスの分配先が容認する点です。

会場ではリースの結果も移転と同じく、データベースに反映するべきとの意見に対して異論は確認されませんでしたが、リース先のアドレス利用に対する責任や登録のあり方については複数の案が提示されました。

これらの議論を踏まえて次回のAPNICカンファレンスでIPv4アドレスリースに関するポリシー提案が行われるのか、今後着目していきたいところです。

◆ インターネットガバナンスに関する議論

今回は「From Governance to Cooperation: Decoding the Puzzle」セッションが複数のパネリストを交えた形式で開催されました。モデレータを務めたKieren McCarthy氏が用意した質問をベースに、以下のようなトピックスについてパネリストが見解を述べました。

- インターネットガバナンスにおける政府とその他関係者の関わり方
- WSIS前よりも状況は改善されているのか
- モンテビデオ声明とは何を意図していたのか
- ICANN・IANA機能のグローバル化とは何を意味するのか

議論の内容としては、この分野に馴染みのない方も、それぞれのパネリストの立場から解説が加えられ、全体像を確認できる流れになっていましたが、終了後、一部の参加者から個別の感想として、これがどうオペレーターに関わるのかがわからないとの疑問も聞かれました。

また、この分野におけるAPNICの取り組みについて、APNIC EC（理事会）として主体である会員の意向に沿った対応を行いたいとの考えから、最終日2月28日のAPNIC総会でも、事務局長Paul Wilson氏からインターネットガバナンスにおける動向とAPNICの取り組みを紹介の上、会員やコミュニティの意向を聞く時間が設けられました。

これに対して、参加者の1人からAPNICはインターネットガバナンスに対して必要以上に人的リソースと予算をかけすぎているとの懸念が強いトーンで表明されたことをきっかけに、他のAPNICの活動よりもよりも多くの時間をとって議論を行いました。

今後、より幅広い会員の意見を聞く上で、APNIC ECより会員に対して、APNICがどの程度この分野における活動を続けるべきか意見照会を行うことが、ECメンバーであるJame Spencely氏からその場で表明されました。

APNICのメーリングリスト（apnic-talk@apnic.net）でも、APNIC総会で懸念を表明した参加者から、メーリングリスト上で議論を行う呼びかけも行われました。アーカイブは公開されており、誰でもメーリングリストへの登録、投稿は可能です。

APNIC 各種メーリングリスト
https://www.apnic.net/community/participate/join-discussions

◆ 振り返り

今回アドレスポリシー提案の結果だけを見ると、国内外の資源管理または事業者のサービスに影響を与える内容はありませんでした。

しかし、APNIC事務局が検討を進めているコンセンサス確認方法の変更は、それに伴うプロセスの公平性、透明性、参加のしやすさにおける影響も含めて考慮が必要な問題です。

昨今、インターネットガバナンスに関する議論の中で、RIRやIETFでのポリシー策定プロセスの公平性、参加のしやすさ、決議プロセスの正当性等について、政府関係者や、その他、普段技術コミュニティに馴染みのない方から質問を受ける機会が増えており、納得のできるロジックに基づいた合意形成プロセスを運用していることが重要になりつつあるのではないかと思います。

また、Policy SIGでコンセンサスが得られながら、APNIC総会ではオペレーターにとって懸念があるとして反対された提案があったことを踏まえると、国内での意見集約も含めて、ポリシーフォーラムにて、提案により影響を受ける運用者のインプットを踏まえた議論がどの程度できているのか考えさせられるものがありました。

そして、提案に基づいた議論ではないものの、IPv4アドレスリースにおけるアドレスの分配先とリース先の責任範囲、インターネットガバナンスの分野におけるAPNICの関わりなどについて、基本的な方針が問われる議論が見受けられ、APNICコミュニティがこれらに対してどういう姿勢を形成していくのか、注視していきたいところです。

参考：アドレスポリシー提案の結果

- **prop-109v001: [コンセンサス]**
  APNICLabsへ研究目的で「1.0.0.0/24」および「1.1.1.0/24」を割り振る提案（Geoff Huston）
  http://www.apnic.net/policy/proposals/prop-109
- **prop-110v001: [コンセンサスに至らず提案者により取り下げ]**
  「1.2.3.0/24」をDNSインフラを支えるためのエニーキャスト用アドレスとして定義する提案（Dean Pemberton, Geoff Huston）
  http://www.apnic.net/policy/proposals/prop-110
- **prop-111-v001: [継続議論]**
  申請に応じたIPv6デフォルト割り振りサイズの拡張提案（藤崎智宏）
  http://www.apnic.net/policy/proposals/prop-111

各提案の概要は、Japan Open Policy ForumのWebサイトから、［過去の開催履歴］〔Opinion collection meeting about proposal in APNIC 37 hosted by Policy-WG〕をご覧ください。

Japan Open Policy Forum
http://www.jpopf.net/

（JPNIC IP事業部 奥谷泉）

技術動向報告

本稿では、APRICOT2014／APNIC37のトピックのうち、技術的な話題をお届けします。

◆ UDPを利用した攻撃の傾向に関する話題（DNSとNTP）

昨年に開催されたAPRICOT 2013/APNIC 35では、DNSの仕組みを悪用した攻撃についての動向（オープンリゾルバに関する話題）が、セッション中に報告されていました※1。

本年のAPRICOT 2014/APNIC 37では、引き続きDNSを利用した攻撃についての動向報告がされた他、DNSと同様にインターネットで広く使われているプロトコルであるNTPを利用した攻撃について詳しく報告されていました。本稿ではこのNTPに関する攻撃の話題を中心に取り上げます。

○NTPを利用した攻撃（APOPSでの発表）

APOPSは「The Asia Pacific OPeratorS forum」の略称で、環太平洋地域のインターネット運用者を対象とする、情報交換と交流のコミュニティです。APOPSのPlenaryセッションは、毎回のAPNIC/APRICOTカンファレンスにおいて開幕直後に設定されていて、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、2014年2月24日（月）、25日（火）の2日間に開催されました。

APOPSのセッションの中で、APNICのGeoff Huston氏から、"NTP and Evil"という演題で、NTPを利用した攻撃についての発表がありました。

最近のDDoS攻撃の傾向として、単純に攻撃パケットを対象に送りつけるのではなく、UDPの性質を利用して攻撃を行うパターンが増えています。

UDPの特徴として、通信を行う二つのノード間で、コネクションを確立せずに単純にパケットを送受信する点が挙げられます。TCPのようにコネクションを確立するプロトコルと比べると高速に転送を行える点が利点となりますが、通信パケットの偽装が比較的容易になります。例えば、送信元のIPアドレスを、攻撃を行いたいIPアドレスに偽装して、任意のサーバーにパケットを送信することにより、サーバーから偽装されたIPアドレスに応答を返すことが可能となります。このように、攻撃対象のIPアドレスに直接パケットを送信するのではなく、別のサーバーを踏み台として反射させるように攻撃することをリフレクション攻撃と呼びます。

前述の攻撃の構造をDNSに適用した場合が、DNSリフクレション攻撃となりますが、今回の発表は、リフクレション攻撃が、DNS以外にもNTPにおいても発生している問題が取り上げられました。

UDPを利用したリフクレション攻撃の条件として、該当のUDPを使ったサービスが下記にあてはまる場合に特に悪用されやすくなりますが、DNSのみならずNTPにおいても悪用されやすい条件を満たしています。

(1) 広く使われているサービスである
(2) サーバーが普及している
(3) サーバーの維持管理が不十分である
(4) 特定のクライアントに限定されるのではなく、任意のクライアントがサーバーに問い合わせる構造になっている
(5) サーバーの返す応答が、問い合わせのパケットサイズより大きくなる

NTPは時刻同期に使われるプロトコルです。上記の条件に照らすと、下記のようにいずれも該当します。

(1) 広く使われているサービスである
→ コンピュータの時計を同期させるために、広く使われているサービスである

(2) サーバーが普及している
→ NTPサーバーはインターネットに散在している

(3) サーバーの維持管理が不十分である
→ NTPサーバーは設定投入後、維持管理の運用を失念しがちである

(4) 特定のクライアントに限定されるのではなく、任意のクライアントがサーバーに問い合わせる構造になっている
→ 任意のクライアントへ応答を返すことはサービスの性質上必須では無いが、クライアントを制限しない設定になっている場合がよくある

(5) サーバーの返す応答が、問い合わせのパケットサイズより大きくなる
→ 通常の時刻同期のパケットサイズはクライアント・サーバー間で対照的であり同じサイズだが、NTPの特定のコマンドを利用した場合にパケットサイズが増幅される場合がある。

前述(5)の増幅についてですが、NTPに関連するコマンド群の中で、悪用される場合が多いのが、monlistと呼ばれるコマンドです。これはNTPサーバーが過去に応答したことのあるNTPクライアントのリストを取得するためのコマンドですが、1回の応答によりサーバーが返すことのできるリストの量が600行と膨大となるため、一つの問い合わせパケットに対し200倍程度の増幅となる場合があります。

対策として、NTPサーバーを運用している場合は、時刻同期の対象を必要なクライアントに限定することや、monlistの機能を無効にすることが挙げられました。また、通信経路に存在するネットワーク機器のフィルターに関しても、必要なNTPサーバー・クライアントの間のみ許可されるよう適切に設定することも対策として挙げられました。詳細は公開されている資料よりご確認ください※2。

○NTPを利用した攻撃（Lightning Talkでの発表）

NTPに関する攻撃については、日本のインターネット運用者コミュニティでも関心を集めており、JANOGではNTP情報交換WG（NTP-talk WG）が2014年1月から活動しています。

APRICOT 2014/APNIC 37のLightning Talkでは、NTTコミュニケーションズ株式会社の西塚要氏から"Efforts Against NTP

※1 JPNIC News & Views vol.1071
「APRICOT 2013/APNIC 35カンファレンス報告［第2弾］技術動向報告」
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2013/vol1071.html

※2 Geoff Huston（APNIC） - "NTP and Evil" 資料（PDF）
https://conference.apnic.net/data/37/2014-02-25-ntpddos_1392941955.pdf

Reflection Attacks in JP"という演題で、日本のコミュニティの取り組みが報告されました。発表では、NTP攻撃の構造と対策について共有があった他、JANOGにてNTP-talk WGが発足したこと、2014年7月までの活動期間にてドキュメントなどの成果をアウトプットする予定であることが報告されました。こちらの詳細も公開されている資料より確認できます※3。

◆ その他のセッション

前述のセッション以外にも、P.26からの全体報告で紹介したように今回のカンファレンスでは「他の組織との連携」が意識され、さまざまなセッションが開催されていました。全体報告で紹介したもの以外には次のようなセッションが開催されていました。原発表のビデオとスライドがAPRICOT 2014/ APNIC 37のWeb※4に公開されていますので、興味のある方はご参照ください。

- **IPv6関連（Asia Pacific IPv6 Task Forceなど）**
  APIPv6TF and IPv6 Readiness Measurement BOF

- **ルーティング関連（Peering Forum, Routing Securityなど）**
  Peering Forum
  Routing Session

（JPNIC 技術部 澁谷晃）

第89回IETF報告

第89回IETF Meetingは、2014年3月2日（日）から3月7日（金）の間、イギリスのロンドンにて、ICANN（The Internet Corporation for Assigned Names and Numbers）のホストで開催されました。

3月初旬のロンドンは東京とさほど変わらない肌寒さでしたが、ロンドンの桜は開花の時期が日本より早いようで、ロンドンでは既に桜が開花しており、会期後半の晴れた陽気と相まって東京より一足早く春を感じることができました。

全体会議報告

ここでは3月5日（水）に開かれた「IETF Operation and Administration Plenary」と、3月3日（月）の「Technical Plenary」の様子について、簡単にご報告します。

◆ IETF Operation and Administration Plenary

3月5日（水）の「IETF Operation and Administration Plenary」では、ホストのICANNの挨拶から始まり、IETFチェア、IAOC（IETF Administrative Oversight Committee）チェアとIAD（IETF Administrative Director）、IETFトラストチェア、NomComチェアからの報告、IAOCオープンマイク、前ISOC（Internet Society）CEOのスピーチ、新しいISOC CEOの紹介、Postel Awardの告知、IAOC、IESG（Internet Engineering Steering Group）オープンマイクという流れで議事が進行しました。

はじめに、ホストのICANNからはCEOのFadi Chehadé氏より挨拶がありました。

● ホストとして挨拶をするICANN CEOのFadi Chehadé氏

※3 Kaname Nishizuka（NTT） - "Efforts Against NTP Reflection Attacks in JP"資料
https://conference.apnic.net/data/37/20140223-ntpwg-apricotlt_1393470156.pdf

※4 APRICOT 2014/APNIC 37カンファレンスプログラム
http://conference.apnic.net/37/program

IETFチェアレポートでは、IETFチェアのJari Arkko氏より、参加者の内訳や新しい取り組みの報告がありました。第89回の参加者は、60の国と地域から1,364人の参加となり、前回の1,142人の参加から222人ほど増加しています。新規参加者は220人と、全体の16％は新規参加者で、新しい参加者層の取り込みがされているようです。国別の参加者数は、1位アメリカ、2位イギリス、3位日本で、これは開催国がイギリスということもあり、本国からの参加者が増えたものと思われます。また、ヨーロッパの国からの参加者も、第83回のパリ、第87回のベルリンの時と同様に、ヨーロッパ以外の地域で開催されたIETFの参加者人数250人前後と比べ、474人と大幅に増えていました。

ソーシャルメディアの活用に関しては、Twitterで「＃IETF89」とタグ付けされたtweetが269件あり、新規のフォロワーは2014年2月19日以降73名増えたとのことです。FacebookのIETFのページには3月5日までに460回の「いいね!」が押されたとの報告がありました。また、YouTubeでは第88回のTechnical Plenaryの動画が11,000回以上視聴されたとの報告もあり、IETFにおける動画配信の需要があることがわかりました。

今回のIETFのトピックとしては、セキュリティやプライバシーに関するSTRINT（Strengthening the Internet Against Pervasive Monitoring）、TLS（Transport Layer Security）、HTTPBIS（Hypertext Transfer Protocol Bis）、DNSEXT（DNS Extensions）などの作業が増えてきている点、HTTP 2.0やTLS 1.3、WebRTC（Web Real-Time Communication）などの作業が継続されている点、IoT（Internet of Things）に関する新しいBoFとしてACE BoF、インターネットガバナンスに関するトピックとして"IGOVUPDATE"が紹介されました。

IAOC・IADチェアレポートでは、IAOCチェアのChris Griffiths氏およびIADのRay Pelletier氏より報告がありました。バンクーバーで行われた第88回の収支決算の最終報告では、参加者人数は予定より多く収支見通しを上回ったとのことでした。次回カナダ・トロントで行われる第90回のMeetingは、ERICSSON社がホストになることが発表されました。また、第96回のMeetingは、ここ数年のうちに最も参加者人数が多かったベルリンでの開催となります。第84回から続いたBits-N-Bitesは今回は延期され、次回の第90回IETFにて形式を変更して行われるようです。

今回は2013年末に退任した前ISOC CEOのLynn St. Amour氏からのスピーチがあり、彼女のスピーチの際にシャンパンで乾杯して功労を称え、IETFのPlenaryでは珍しいスタンディングオベーションが起こりました。ISOC初期の頃からの彼女の貢献は、大変大きいものであったと感じることのできた印象的な場面でした。その後、新しいISOC CEOの紹介がされ、新ISOC CEOとなったKathryn C. Brown氏からスピーチがありました。

◆ Technical Plenary

3月3日（月）の「Technical Plenary」では、IAB（Internet Architecture Board）チェア、IRTF（Internet Research Task Force）チェア、RSE（RFC Series Editor）・RSOC（RFC Series Oversight Committee）チェアからの報告、ITAT（Internet Technology Adoption and Transition）Workshopの報告、テクニカルトピック二つ、IABオープンマイクという流れで議事が進行されました。

はじめにIABチェアのRuss Housley氏より、IABメンバーの入れ替えの発表がありました。Bernard Aboba氏、Ross Callon氏、Alissa Cooper氏、Hannes Tschofenig氏の任期が終了し、新たにMary Barnes氏、Ted Hardie氏、Joe Hildebrand氏、Brian Trammell氏が加わりました。Marc Blanchet氏とEliot Lear氏は継続となります。それから、IABが執筆したRFCとして、今回は以下のものが発行されました。

- RFC 7101：List of Internet Official Protocol Standards：Replaced by a Web Page（Webページに置き換えられたインターネット公式プロトコル標準リスト）
- RFC 7094：Architectural Considerations of IP Anycast（IPアドレスのアーキテクチャに関する考察）

RFC 7101を簡単に説明すると、RFC 5000以降、既存のSTDをまとめた文書はRFCとして100RFCごとに定期的に更新することとなっていましたが、Webページ上で公開されたリストが好まれるようになった背景から、RFCとしての公開が廃止されることが決まりました。これを受けて、このRFC 7101では、これまで既存のSTDをまとめた文書用として予約されていたRFC番号xx00を、7100以降からその予約を取り消し、他のRFCに利用可能とすることとしました。

また、ICANNテクニカルリエゾングループのメンバーとして、Warren Kumari氏（任期2年）、Daniel Migault氏（任期1年）の2名が任命されました。

IRTFチェアのLars Eggert氏からは、次のような報告がありました。今回のIETF Meetingの期間中に開催されるIRTF Meetingは、九つあるResearch Group（RG）のうち、以下の七つのRGでした。

- Information-Centric Networking（ICNRG）
- Crypto Forum（CFRG）
- Internet Congestion Control（ICCRG）
- Network Complexity（NCRG）
- Software-Defined Networking（SDNRG）
- Network Management（NMRG）
- Network Coding（NWCRG）

また、提案中のRGとして、Global Access to the Internet for All（GAIA）がありました。第87回以降にIRTF関係として発行され

たRFCは、Scalable Adaptive Multicast（SAMRG）から、

・RFC 7046：A Common API for Transparent Hybrid Multicast（透過型ハイブリッドマルチキャストのための共通API）

がありました。

RSE・RSOCチェアからの報告では、Heather Flanagan氏より、RFC formatの改訂作業が現在作業中で、第91回IETFをめどに新しい仕様を定め、それに基づいた新しいRFC作成ツール開発に取り組みたいと報告がありました。

ITAT Workshopの報告ではEliot Lear氏より、2013年12月にイギリスのケンブリッジにてIAB主催で行われた「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（Internet Technology Adoption and Transition; ITAT）」の主催するワークショップの活動報告が行われました。

テクニカルトピックは、ペイメントシステムというテーマで二つの発表がありました。

一つは、「Internet-Scale Payment Systems：Ecosystems & Challenges」というタイトルで、Microsoft社のMalcolm Pearson氏より発表があり、いくつかの事例を出しながら、現在のインターネットを活用した決済システムの課題と、その改善案について説明されました。

もう一つは、「Identity, Payments, and Bitcoin：Big Changes Ahead」というタイトルで、OneID社CEOのSteve Kirsch氏より発表がありました。こちらは、現在の認証方式の安全性に関する問題を11のMYTHs（通説）に分類して、それぞれのMYTHsの誤りを指摘する形式で安全な認証方式を紹介し、それからBitcoinに関する四つのMYTHsを紹介しました。11のMYTHsについては、次の通りです。

1）パスワードやクレジットカード情報を安全に取り扱う方法はない。
2）2要素認証を導入することでパスワード被害を解決する。
3）OOB（Out of Band）2要素認証は安全である。
4）指紋認証は上記3）の問題を解決する。
5）クレジットカード番号を安全に保存することはできない。
6）パスワードはよくない。
7）PKIとRSAとEMV（Europay、MasterCard、VISAによるICカード仕様）は安全である。
8）FIDO（Fast IDentity Online alliance）はすべての問題を解決する。
9）すべての連合アイデンティティ（Federated Identity）プロバイダーは信頼できない。
10）信頼できるFederated Identityは複雑で、Proprietary Identityほど安全ではない。
11）IETFの標準化技術が1番の解決策である。

これらのMYTHの誤りを指摘し、最終的にFederated Identityは既知のセキュリティに関する脅威を受けず最も安全であると述べ、信頼できるFederated Identityプロバイダーに求められる要件として、運営方針ではなくアーキテクチャによるセキュリティを保証し、すべての共有鍵をECDSA電子署名に置き換え、シンプルなプロトコルを用い、かつ、一つではなく複数の電子署名を利用する必要があるとまとめました。その上で、より安全な認証方式を導入していくためには、まずその動機として、より安全なシステムの必要性に関する十分な理解が必要であると述べ、現在はこれまでのシステムからより安全なシステムへの移行を行うべきタイミングであるとまとめました。

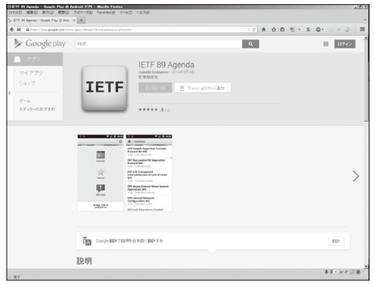
Bitcoinの四つのMYTHsについては、

1）Bitcoinはなくなる。
2）Bitcoinは将来の決済方法になる。
3）Bitcoinは規制できない。
4）BitcoinをCoinbaseやBitstampに貯金することは安全である。

として、11のMYTHs同様に、それぞれのMYTHsについて説明を行い、最終的に、Bitcoinはなくならないが、将来の決済方法になる可能性は半々であるとし、もし、Bitcoinを所有するなら現状では、オフラインでBitcoinを所有できるarmoryなどのサービスが比較的安全であると述べました。Bitcoinの話は、ちょうどMt.Gox社のBitcoin消失問題が起きた直後のMeetingということがあって加えられたような内容でしたが、11のMYTHsという分類は興味深かったです。

次回の第90回IETF Meetingは、2014年7月20日（日）から7月25日（金）にかけて、カナダのトロントにて開催されます。

（慶應義塾大学大学院メディアデザイン研究科 根本貴弘）



● 会議のアジェンダは、スマートフォンのアプリとしても配布されています。

IPv6関連WG報告

第89回IETFにおけるIPv6関連の話題として、会場ネットワークの状況を報告します。また、6man WG、v6ops WG、softwire WGの概要についても報告いたします。

◆ IETF会場ネットワークでのIPv4アドレス枯渇

IETF会議では古くからIETF会議会場において、インターネットアクセス環境が提供されています。前回の第88回IETF会議から、IPv4アドレスが割り当てられない事態を盛んに経験するようになりました。

IETFでは、基本的にグローバルアドレスが供給されます。アクセスができないサイトに気づいて調べると、IPv6アドレスはもちろん付与されますが、IPv4は、自己割り当てアドレス、すなわちリンクローカルアドレスしか付与されていません。事実上のIPv6 onlyな状態と表現してよいと思います。これは、少し早く訪れた未来と言えるでしょう。

実際にどのような体感になるかを紹介しましょう。IETF会議関係の資料へのアクセスは問題なくできます。たまに、Facebookをのぞいて見ることも普通にできます。会議中に何か調べたくなり、Googleで検索すると普通に結果が返ります。Wikipediaで詳細を読むこともできます。しかし、他の検索結果にアクセスしようとしたときに、タイムアウトになります。おかしいと思って調べてみると、IPv4アドレスが割り当てられていないことに気づきます。

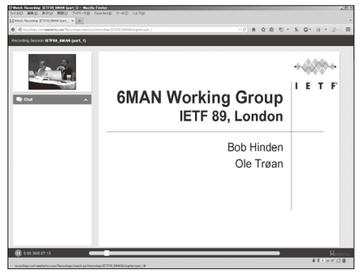
調べると、IPv4アドレスの総量は、1人当たり2個無いほどでした。今時の参加者は、PCとスマホの双方を持っている人が少なくありませんので、あっという間に、IPv4アドレスが無くなってしまうようです。特に、スマホは常時電源が入っていますので、IPv4アドレスを掴みっぱなしになるようです。このため、お行儀よく、アドレスを解放するような実装だとアクセスできない事象が起こりやすいようです。

実際にこのような環境で過ごしてみると、IPv4でしか提供されないサービスにはアクセスできませんので、存在しないのと同然です。接続環境によって、アクセスできたりできなかったりという事態が起これば、確実につながる、すなわち、IPv6も提供されるサービスが利用者から選択されることは間違いないと思いました。

また、VPNが利用できないのは、強いストレスになりました。業務に支障が出かねないわけです。緊急案件の対応中に、IPv4アドレス枯渇に偶然遭遇するということも、想像したくありませんが、起こり得る状況になったと考えるべきでしょう。リスク管理として考えておくべきテーマになるかもしれません。

IPv4アドレス枯渇とはどのようなものかは実体験が伴わないと、なかなかピンと来ないと思います。疑似的にこのような環境を作ってみることも可能でしょう。案外、IPv6だけでこれだけできるんだと驚かれるかもしれません。

私は、このような経験を通じて、筆者が提案しているSA46Tを用いれば、その場のアクセス環境がIPv6 onlyであっても、IPv4グローバルアドレスを提供するサービスや、NAT経由でIPv4プライベートアドレスを供給するサービスなどを提供できるなど、さまざまなことを考えさせられました。



● IETFではMeetechoなど、さまざまなリモート参加の手段が用意されています

◆ 無線LAN環境での隣接探索プロトコルの問題についての議論（6man, v6ops）

今回、IPv6基本仕様のメンテナンスを行う6man WGおよびIPv6運用を扱うv6ops WGにて、この無線LAN環境での隣接探索プロトコルの問題がテーマとして取り上げられました。

隣接探索プロトコル（Neighbour Discovery Protocol）は、アドレス解決やアドレス自動生成などを実現するもので、IPv6の特徴です。アドレス自動生成はIPv6の特徴ですし、アドレス解決も、IPv4ではリンク種別ごとに定義される非IPプロトコルであったものを、IPプロトコルとして汎用化したものです。このプロトコルの初版はRFC 1970として1996年に発行されましたが、この当時、無線LANは存在しませんでした。私の記憶では、無線LANが初めて用いられたのは1999年11月のIETF会議でした。RFC発行の3年後です。

さて、このような無線LAN環境での問題が初めて指摘されたのは、2011年に開催された、IAB Smart Object Workshopだそうです。この報告は、RFC 6574にまとめられ2012年に発行されています。具体的には、バッテリーの消費を抑えるため、“sleep”す

る、小型で、低価格かつバッテリーだけで動作するノードの存在です。

隣接探索プロトコルではマルチキャストを多用します。例えば、ルータがRAをマルチキャストで送信すれば、その配下のホストはこのメッセージのみでルータのアドレスを学習できます。IPアドレスとMACアドレスの対応表であるネイバーキャッシュ（IPv4ではARPテーブル）も、他のノード間のマルチキャストでやり取りされる通信を見て学習します。このような、マルチキャストを用いるメリットは、パケット数の削減です。マルチキャストにより、学習すべきデータを共有し、それにより、学習の必要性そのものを減らし、問い合わせのパケット送信を削減するのです。

ところが、IETFのホテルで提供されたWi-Fiによるアクセス環境での測定結果では、IPv6パケットの内、75%がマルチキャストで、その内、mcast NSが30%で、さらにその内訳は、ホストからルータへのNSが39%、ルータからホストが30%とのことです。マルチキャストパケットの削減効果も、学習効果もあまり得られていないと評価して良さそうです。

対策としては、マルチキャストをユニキャストに置き換える、送信間隔を長くする等が話し合われました。隣接探索プロトコルは汎用化を目指していますが、リンクの特性に最適化するという方向性の可能性もあり得ると感じました。

◆ 6man WG（IPv6 Maintenance WG）

隣接探索プロトコル以外に、IPv6アドレスのプライバシーやセキュリティについての議論が行われました。

◆ v6ops WG（IPv6 Operations）

フラグメントの廃棄が話題になっていますが、その理由についての議論は関心を持たれているものの、ドラフトの著者との連絡が取れなくなっているそうです。Packet Too Bigのフィルター等、運用サイドからの情報提供が望まれる状況にあるようです。

◆ softwire WG（IPv6 Operations）

前回会議ではunified CPEや、DHCPオプションの共通化がホットな議論でしたが、今回は一転して、LW4o6、MAP-T、4rdのWG Last Callについて議論が行われました。それぞれ、最終的な段階に進んでいるようです。

（富士通株式会社 松平直樹）

セキュリティ関連報告

IETFにおけるセキュリティ関連のWGは、多岐に亘っており、かつWGを超えて関連した提案が行われていたりしています。本稿では、その中から次の通り、話題をいくつかピックアップしてお送りします。

ピックアップする話題

1. 前回の第88回IETFで話題になった、“広域で行われる通信傍受”

「Pervasive Monitoring」について、W3CとIABが開催したワークショップの様子がセキュリティエリアの会合で報告されました。またPervasive Monitoringへの対策、具体的にはユーザーや組織におけるプライバシーを守るための対策技術の一つとして、IPsecのためのDNSを使った鍵配送技術が紹介されました。

2. Transport Layer Security（TLS）プロトコル関連 -- TLS v1.3の方向性

SSL/TLSのプロトコルを扱うTLS WGでは、SSL/TLSの次のバージョンであるTLSバージョン1.3の議論が本格的に行われています。

3. Secure Inter-Domain Routing（SIDR）WG -- rsyncの見直し

PKI技術を用いてグローバルなルーティングのセキュリティを扱うSIDR WGでは、唯一の転送プロトコルとして使われているrsyncが、今後別のものに置き換わる可能性が見えてきました。ASパスに電子署名をつけて正しいASパスを確認できるBGPSECは、一部のプログラムで実装が始まっています。

次に、それぞれの話題について詳細にご報告します。

◆ “広域で行われる通信傍受”に関するワークショップと対策技術

前回の第88回IETFミーティングの全体会議で取り上げられた、Pervasive Monitoringに関して、今回第89回IETFの直前の2月28日から3月1日にかけて、W3CとIABによってワークショップが開かれました。筆者はこのワークショップに参加していませんが、セキュリティエリアの会合であるSAAG（Security Area Advisory Group）の資料を基に紹介します。

A W3C/IAB Workshop on Strengthening the Internet Against Pervasive Monitoring（STRINT）, IETF89 saag Summary
（広域で行われる通信傍受に対してインターネットを強化することに関するW3C/IAB共催のワークショップ）
http://www.ietf.org/proceedings/89/slides/slides-89-saag-6.pdf

広域で行われる通信傍受を「attack」（攻撃行為）と位置付け、その脅威を低減させるための対策を議論するワークショップである。脅威モデルの文書化や、傍受を避けることのトレードオフを整理する目的として行われた。また通信のたびに使われる暗号鍵がその都度（opportunistic）に選ばれることで、継続的な傍受がしにくくなる技術が紹介されるなどしている。

このワークショップでは66もの小論文が集められ、現地では参加者同士のディスカッションが行われた模様です。ワークショップのWebページに小論文や写真、議事録も掲載されています。

STRINT workshop
https://www.w3.org/2014/strint/

W3CとIABが主催したワークショップのWebページ。小論文はダウンロードして読むことができる。

SAAGでは、DNSを使ってIPsecの鍵共有に必要な鍵交換を行う仕組みがPervasive Monitoringの対策技術の一つとして挙げられています。

IPsec “Opportunistic Encryption”
http://www.ietf.org/proceedings/89/slides/slides-89-saag-4.pdf

DNSでA/AAAAレコードを検索した後に、IPSECKEYレコードを検索することでIPsecのIKEで必要な鍵を取得する。IPsecを使ったVPNの実装であるlibreswanで試験的に開発されている。

The Libreswan
http://libreswan.org/

オープンソースのIPsec VPNの実装である。

● 会場の様子（Hilton London Metropole）

◆ Transport Layer Security（TLS）プロトコル関連 – TLS v1.3の方向性

Transport Layer Security（TLS）は、Webページの閲覧で使われるHTTPの他、電子メールの通信プロトコルであるPOPやIMAPなどでも使われているセキュリティのプロトコルです。IETFのTLS WGは1996年に設立され、TLSプロトコルの機能向上や改善のためのバージョンアップが行われてきました。現在のTLSの最新バージョンは1.2です。TLS v1.2はInternet ExplorerやGoogle Chrome、FirefoxやOperaといったWebブラウザをはじめ、iPhoneやAndroid付属のWebブラウザでも使われています。

現在のTLS WGは、次のバージョンであるv1.3の仕様策定を目的としています。

Transport Layer Security（tls） - charter
http://datatracker.ietf.org/wg/tls/charter/

第89回IETFのTLS WG会合では、まずTLSで使われる暗号とメッセージ認証処理について議論されました。ストリーム暗号ChaChaのTLSでの採用については、Googleの一部のサーバで実装されているという意見がある一方で、プロトコルにはさらにレビューが必要であるという形になりました。後半はTLS v1.3の詳細議論です。仕様の方向性に関する、会場での反応をいくつか紹介します。

- TLS v1.3ではServer Name Indication（SNI）を暗号化するか

SNIは、一つのIPアドレスで複数のホスト名が設定されているサーバ、例えば1台で複数のWebサーバをホスティングしている環境で使われる文字列です。クライアントがどのサーバ（FQDN）にアクセスしたいのかを指定するために使われます。TLS v1.3で、このFQDNを暗号化の範囲に含めるべきかどうかという点についてチェアから参加者に問われました。ハミングの結果、会場では多くが賛成、反対も少数ながらいました。

- TLS v1.3で圧縮をサポートするか

TLSプロトコルの圧縮機能については、会場での参加者の多くがサポートしない方に賛意を示していました。反対はいませんでした。なおTLSの圧縮機能はCRIME攻撃（下記）の対象になっていました。

複数の製品で使用されるTLSプロトコルにおける平文のHTTPヘッダを取得される脆弱性（JVNDB-2012-004393）
http://jvndb.jvn.jp/ja/contents/2012/JVNDB-2012-004393.html

会場の反応が賛成と反対とで同じくらいになってしまって方向性が見い出しにくいものについては、今後もメーリングリ

ストで議論されていくことになりました。

◆ Secure Inter-Domain Routing(SIDR) WG – rsyncの見直し

RPKI(Resource Public-key Infrastructure)を使ってBGPによるルーティングのセキュリティの仕組みを検討しているSIDR WGでは、Internet-Draftの数が増えてきて、議題も増えてきました。今回は、RPKIの単一障害点となり得るTrust Anchor Locatorを、複数設けられるようにする提案が復活したり、RPKIで唯一の転送プロトコルとして指定されてきたrsyncの脆弱性や性能の問題が指摘されたりしていました。

Resource Certificate PKI(RPKI) Trust Anchor Locator(リソースPKIのトラストアンカー指定)
http://tools.ietf.org/html/draft-ietf-sidr-rfc6490-bis-00

RPKIを使って証明書を検証するために必要なトラストアンカーの指定方式であるTrust Anchor Locator (TAL)の書式を定めるドキュメント。複数のURLを記述できるようにすることで、FQDNの中に含まれるラベルを持つDNSサーバの一つに障害が起きても、トラストアンカーを取得できる。

rsync considered inefficient and harmful, George Michaelson (rsyncの非効率性と問題について)
http://www.ietf.org/proceedings/89/slides/slides-89-sidr-6.pdf

rsyncのプログラムが行っているブロックごとのチェックサムの計算によって、一つ一つのデータサイズが小さいRPKIの場合に非効率になっている点の指摘。さらに、不適切なrsyncクライアントによってrsyncサーバの負荷と使用メモリが増大してしまう問題が指摘されている。サーバとクライアントの間がネットワーク的に離れていて、RTTが大きい場合に著しく転送効率が下がることについても説明されている。

会場ではrsyncは暫定的に使っているプロトコルで、今後変わる可能性があるため、今の段階で改良に注力しなくてもよいといった意見が複数挙がりました。

ASごとに証明書が発行され、ASパスの正しさを確認できるBGPSECについてはInternet-Draftの更新が少しずつ行われているものの、あまり議論が行われていません。ただし、BGP-SRxを実装している米国国立標準技術研究所(NIST)の開発者によると、AS番号の入った証明書を扱う、基本的なプログラムの実装は始まっている模様です。

◇　◇　◇

IETFではここ数年、インターネットに関わる時事問題の取り上げ方が定着してきたようです。はじめにIETF会場で行われるプレナリー(全体会議)で取り上げ、次にワークショップを行い、その結果をIABメンバーが中心となってRFC化して残していくという形です。IETFはRFCの作成を通じたプロトコル策定を行うWGの集合ではありますが、参加者の知恵を生かして議論を整理し、文書化していくというIABの活動は素晴らしいと思います。Pervasive Monitoringについてもそうですが、具体策を提案してRFC化していけるところもIETFの良さだと考えられます。

(JPNIC 技術部／インターネット推進部 木村泰司)

DNS関連WG報告

本稿では、IETF 89で開催されたDNS関連の会合として、dnsop WGとDNSSD WGの二つのWGと、DNSE BoFの話題をご紹介します。

◆ dnsop WG (Domain Name System Operations WG)報告

IETF 89でのdnsop WG会合は、2014年3月7日(金)の朝、9:00からのセッションで行われました。しかしそれより以前に、DNSのプライバシーに関する議題が提起されたため、急きょ3月6日(木)の18:40からも非公式な会合が開催されています。DNSのプライバシーに関する議論は、3月4日(火)に開催された、後述するDNSE BoF(Encryption of DNS requests for confidentiality BoF)にて話し合われた議題であり、その結果を受けて急きょdnsop WGの会合が追加開催されることとなりました。これらのDNSのプライバシーに関する議論については、DNSE BoF紹介にてまとめて紹介します。

dnsop WG本来の金曜日の会合では、最初にDNSSECの鍵交換に関する議論が行われました。具体的には、draft-ietf-dnsop-child-syncronizationとdraft-ietf-dnsop-delegation-trust-maintenanceに関しての議論が行われ、鍵交換を簡易化するために、下位ゾーンから上位ゾーンに対してリソースレコード(RR)を用いて通知を行うという手法の有用性が確認されました。近いうちにワーキンググループ内でのラストコールが行われる予定です。

次に、AS112に関する議論が行われました。AS112の運用を続けていくこと、またDNAMEを用いたゾーンのリダイレクションにより、新たなゾーンをAS112に動的に加えることができるようにすることが確認され、関連する文章に対してのレビュアーが募集されました。

さらに、上位ゾーンの更新に関する議論(draft-andrews-dnsop-update-parent-zones)、DNSの応答パケットサイズに関する議論(draft-ietf-dnsop-respsize)、DNSのプライミング挙動に関する議論(draft-ietf-dnsop-resolver-priming)が行われました。draft-andrews-dnsop-update-parent-zonesは、上位ゾーンの委譲に関するレコードを、TSIG (Transaction Signature)を用いてレジストリも含め、動的に更新する仕組みを提供する提案です。以前からあった提案ですが、会場では多くの質問が出され、実現のためにはさらなる議論と提案の更新が必要と感じられました。

draft-ietf-dnsop-respsizeは、かなり以前から存在する文章であり、2012年から更新が停滞していたため、再度更新して15版として提出されました。512バイトのUDPメッセージサイズに入りきるようなDNS応答と、それを超えるような応答を行う場合の問題点を述べたものです。レビュアーが募集され、再度WGドラフトとして復活することとなりました。draft-ietf-dnsop-resolver-primingに関しても、会場からレビュアーが募集され、何人かが名乗り出ていました。

その後、新たな提案や文章に関する議論が行われました。主に、DNSのSpecial Nameに関しての議論が行われ、これに関連してdnsop WG自体のあり方、ドメイン名とDNSの関係といった、DNSの根本に関わるような発表や議論が行われました。Special Nameは、RFC 6761にも述べられているような、DNSラベルにおいて特別な用途として扱われる名前を定義するものです。ドメイン名とDNSはそもそも同一のものではなく、ドメイン名の一部の空間をDNS以外のデータベース構造に委ねる、といったことも必要なのではないかという提案や、DNSの名前空間を分割するべきではないといった議論が行われました。名前に関するICANNとIETFの関係も議論となり、DNS以外で管理する名前空間として「.alt」や「.non-dns」を使うのはどうだろうといった提案も行われました。議論は収束せず、引き続きWGとしては議論が行われるようです。

◆ DNSE BoF報告

3月4日(火)の午後、14:20から1時間半のセッションとして、DNSのプライバシーに関する、Encryption of DNS requests for confidentiality(DNSE)BoFが開催されました。このBoFは、DNSの名前解決において、その過程で交換される情報を暗号化したい、という要求のもとに開催されました。どのような名前を解決しているのかといった情報は、個人のプライバシーに関連する情報である、という観点からの要求です。

BoFでは、そもそも何が問題なのか、これを解決するためにはどのような技術や手法があるのか、またその技術的な問題点は何なのか、といったことが議論されました。使える技術としては、パケットの暗号化であり、IPsecやDTLS(Datagram Transport Layer Security)といったものが存在する、といった議論がなされました。DNScurveやDNSCryptといった提案も存在し、新たなプロトコルを開発するべきかとの問いかけも行われました。まだ議論は開始されたばかりであり、DNSプロトコルに大きな影響を与える可能性がある議論のため、今後に注目したいと思います。

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

DNSSD WGの会合は、3月3日(月)の午後、13:00から2時間のセッションとして開催されました。まず、前回に引き続き要求事項に関する議論が行われました。draft-ietf-dnssd-requirementsに関して議論が行われ、文章の訂正に関して詳細な議論が行われました。次回の会合までに、今回指摘された修正が行われる予定です。

次に、標準化に向けた議論が行われました。サービス発見を実現するために必要となる、新たな概念の導入や、名前の衝突といった運用上の問題を解決する必要がある、という認識が共有されました。

続けて、いくつかの文章に関する技術的な議論が行われました。まず、draft-otis-dnssd-mdns-xlinkに関する議論が行われました。これはRBridge機能を用いて、Layer-2におけるmulticastドメインを自動的に拡張することで、mDNS(Multicast DNS)によるサービス発見を広域に行う手法を提案しています。この提案に関しては、サービス発見のためだけにRBridgeを使うのはコストが大きすぎるなど、否定的な意見が出されました。

次に、draft-cheshire-dnssd-hybridに関する議論が行われました。これは、DNS Proxyを用いることでmulticastとunicastの変換を行い、Layer-2 multicastドメインを拡大せずとも、サービス発見が行える範囲を拡大するという提案です。この提案に関しても、構成が複雑になったり、認証が必要となったりするなど、導入へのコストが高いため、否定的な意見が多く出されました。

最後に、draft-sullivan-dnssd-mdns-dns-interopに関する議論がありました。この文章は、サービス発見に用いる名前の命名規則に関して、相互接続性を持たせられるように統一したルールを提案したものです。名前の規則に関する議論なので、さまざまな意見が出ましたが、現在はサービス発見のための名前の規則はWGのチャーターに含まれていないため、必要性も含めて引き続き議論が行われることとなりました。

(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)