APRICOT 2015における APNIC 39カンファレンス報告

アドレスポリシー関連報告

APRICOT-APAN 2015では、さまざまなプログラムがあります。プログラムの一つであるポリシーSIGでは、丸一日かけてアジア太平洋地域のIPアドレス・AS番号の、分配ポリシーについての議論が行われました。本稿では、ポリシーSIGでのアドレスポリシーに関する提案内容と、各提案での議論の様子を中心にご紹介します。

関連記事「P.2 特集1 APRICOT-APAN 2015開催報告」

◆ SIGについて

特定の話題について議論を行うために、APNICではSIG（Special Interest Group）という仕組みが設けられています。ポリシーSIGのほかに、JPNICのような国別インターネットレジストリ（NIR）に関連する話題について議論を行うNIR SIGの、二つのSIGがこれまで設けられていました。今回新たに、公共政策やインターネットガバナンスなど、APNICコミュニティにとって関連のある事項をさまざまな関係者で議論するための、Cooperation SIGが設けられることになりました。

SIGでは、メーリングリスト（ML）上での議論のほか、年に2回開催されるAPNICカンファレンスでは顔を合わせての議論を行います。最近では、ストリーミング中継や、発言をリアルタイムに画面やスクリーン上に映し出すトランスクリプト、チャットによるコメント受け付けなど、会場以外からミーティングに参加するための手段も多く設けられています。

◆ ポリシー提案について

今回は4点のポリシー提案がありましたが、議論が行われた結果、コンセンサスとなった提案はありませんでした。3点の提案が継続議論となり、残る1点の提案は棄却となりました。それぞれの提案の内容と、結果をご紹介します。

（1）'legacy IPv6 address blocks'から割り振りを受けている組織へのIPv6アドレス割り振りサイズ拡張（提案番号：prop-112）	
提案者	藤崎智宏氏
概要	該当する範囲から割り振りを受けている組織に対して、追加割り振りのための利用率を満たしていない場合にも、希望があれば将来の需要予測の提出なしに、最大で/29となるよう割り振りを行う。
提案の詳細	http://www.apnic.net/policy/proposals/prop-112
結果	棄却

現在、APNIC地域におけるIPv6アドレスの割り振りは、2400::/12の範囲から行われています。2400::/12の範囲から割り振りを行う際には、複数回のIPv6アドレス割り振りを受けた場合にも、連続した範囲になるよう考慮された管理が行われています。一方、2400::/12の範囲から割り振りを開始する前に、2400::/12とは異なる範囲からIPv6アドレスの割り振りを受けた組織に対しては、連続した/29の範囲となるようアドレスは予約され、他の組織に割り振りを行わないよう管理されています。

提案者からは、他の組織に割り振りが行われず、利用されないままとなっているこのアドレスブロックの、有効利用を目的とした提案である旨が紹介されました。MLや当日の議論では、効率的な利用に賛成するコメントが出される一方で、アドレスの割り振りは実際の需要に基づき行われるべきだ、とのコメントも出されていました。

挙手およびオンラインで本提案に対する賛否を確認した結果、本提案はコンセンサスには至りませんでした。この提案は、APNIC 37カンファレンスより3回にわたり議論が行われましたが、いずれにおいてもコンセンサスに至らなかったことから、ポリシーSIGチェアより、提案を棄却とすることが発表されました。

（2）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	概要：「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」というIPv4プロバイダ非依存（PI; Provider Independent）アドレスアドレスの割り当て基準を、「PAアドレスで既にマルチホームしている」または「PAアドレスで相互接続している」または「3ヶ月以内にアドレスを経路広告する計画がある」に変更する。
提案の詳細	http://www.apnic.net/policy/proposals/prop-113
結果	ポリシーSIG MLでの継続議論

IPv4アドレスは、APNICやJPNICなどのレジストリからプロバイダ等に分配され、プロバイダはエンドユーザーに分配するという、階層構造により管理が行われています。ただし、特定の

条件を満たす小規模ネットワークや、インターネットエクスチェンジポイントなど一部のケースにおいては、レジストリからエンドユーザーに対して、直接分配が行われています。

この提案は、特定の条件を満たす小規模ネットワークに割り当てる目的で、レジストリからエンドユーザーに対して直接分配を行う際の、基準を変更するものです。インターネットの普及が目覚ましい地域では、レジストリからプロバイダへの割り振りアドレスに限りがあるため、エンドユーザーが希望する数のIPアドレスの分配を受けることも難しい、といったケースもあるようです。現在の基準が緩和されることで、IPv4アドレスの分配を受ける機会の増加につながるとの意見が表明されていました。また、提案には、「3ヶ月以内に割り当てアドレスの25%、1年後までには割り当てアドレスの50%を利用する計画があること」という条件も、併せて撤廃することが含められていましたが、割り当てアドレスの利用予定を確認する条件は必要であるとの意見が、複数表明されていました。

会場から出された意見を踏まえた改定案が、ポリシーSIGの最中にMLに投稿され、それをもとに議論が行われるなど、状況は刻々と変化し、目を離せない状況となっていました。一通りの議論が終了した後に、本提案に対する賛否を確認しましたが、本提案はコンセンサスには至らず、MLで継続議論を行うこととなりました。MLでは、ポリシーSIGの終了後も議論が続きましたが、改定案に賛同する意見が多く寄せられています。

(3) 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	「マルチホームする」かつ「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」というAS番号割り当て基準を、「6ヶ月以内にAS番号を利用する予定がある」に変更する。
提案の詳細	http://www.apnic.net/policy/proposals/prop-114
結果	ポリシーSIG MLでの継続議論

AS番号は、上流接続先のルーティングポリシーに依存せずに、自律ネットワークと定義されるネットワークに対して割り当てられます。提案者からは、上流接続先より提供されるサービスの選択肢が限られる地域では、AS番号の割り当てを受けて、上流接続先に依存しない状況にしておきたいと考えるケースがあると紹介されていました。そのようなケースでは、AS番号の割り当て要件を満たすよう、虚偽の申請を行っているケースもあるため、実態に合うよう割り当て基準を変更したい、という背景があったようです。

提案がMLで紹介された当初は、現行ポリシーの解釈や、具体的な例を挙げた上で、現在有効なポリシーを変更せずともAS番号の割り当てを受けられるケースかどうかという議論が、多くを占めていました。APNIC審議担当の責任者も参加して、APNICでの判断例やポリシーの解釈について、さまざまな議論が行われました。

議論の結果、提案者からは、マルチホームであること(マルチホームする計画であること)は基準から削除せず、マルチホーム実施時期は定めない、とする基準を盛り込んだ改定案が発表されました。しかしながら、本提案への賛否の確認をしたところ、本提案は提案番号:prop-113と同様にコンセンサスには至らず、MLで継続議論を行うこととなりました。その後のMLの議論では、多くが賛成を表明する意見となっています。

(4) 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

IPv4アドレスの通常在庫枯渇以降、グローバルIPアドレスとポート番号との組み合わせを利用して、複数の機器やユーザーがグローバルIPアドレスを共有する技術を採用する組織が多くなってきています。また、IPv6による不正行為なども多くなってきているようです。

不正利用の際には、連絡先の確認やフィルタリングを行うための情報収集手段として、WHOISが利用されています。対象を限定した形で的確に対応を行えるようにするためには、現在のWHOIS登録情報にさらなる情報の追加が必要であると、提案者は考えているようでした。MLや当日の議論では、現在の状況や提案者の問題意識については理解されていましたが、WHOISで提案者が考える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。

他の提案と同様に、本提案でも賛否を確認しましたが、本提案はコンセンサスには至りませんでした。しかしながら、ポリシーSIGチェアからは、この提案はWHOISデータベースに関する問題であり、実装の影響などを慎重に考慮する必要があるとの判断が示されました。その結果、問題意識を深く掘り下げて提案者だけではなく、関係する人とともに議論を進めていく必要があるため、MLで継続して議論することが発表されました。

◆ APNIC Annual General Meetingについて

APNIC 39カンファレンスの最終日には、APNIC Annual General Meeting(AGM)が開催されました。これまでは、APNIC Member Meeting(AMM)と呼ばれていましたが、APNICの定款に合わせ、AGMに変更され、APNICの活動内容に関する報告、APNIC 39カンファレンス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 40カンファレンスの紹介が行われました。

その他にも、APNIC理事会メンバー(EC)を選出するための選挙が行われました。候補者のプロフィールは、APNICのWebサイトで事前に公開されますので、会員の多くはその内容を参考にして、前日までに専用ポータルサイトからオンライン投票を済ませます。その一方で、AGM当日は候補者自身が抱負を述べる機会が設けられますので、その内容を確認して、投票用紙での投票を行う会員も多く見受けられました。

ECの任期は2年となっており、1年ごとに半数が改選となります。今回の選挙では6名の候補者の中から、4名が選出されました。この4名に加えて、今回の改選対象には含まれない3名、およびAPNIC事務局長Paul Wilson氏の8名で、新APNIC理事会が次の通りスタートしています(括弧内は現在の所属および出身国・地域)。2014年3月より議長を務めていたJPNICの前村が、今回の新体制においても引き続き、議長を務めることになりました。

	前村昌紀(JPNIC:日本)
	Ma Yan氏(CERNET:中国)
	Che-Hoo Cheng氏(The Chinese University of Hong Kong:香港)
○	Gaurab Raj Upadhaya氏(Limelight Networks:ネパール)
○	James Spenceley氏(Vocus Communications Limited:オーストラリア)
○	Kenny Huang氏(TWNIC:台湾)
☆	Jessica Shen氏(CNNIC:中国)
	Paul Wilson氏(APNIC事務局長:オーストラリア)

※ ○は今回の選挙で再任されたEC、☆は新任のEC

◆ 最後に

ML上で今回のポリシー提案が紹介された直後から、メールが多く飛び交い、関心の高さがうかがえました。また、当日には、マイクの前に質問者が途切れることなく並ぶだけではなく、関係者が休憩時間にも会場内外で熱心に議論を行うなど、時間をかけてじっくりと議論を行うスタイルになったことが特徴的でした。APNIC管轄地域内であっても、地域によって事情が大きく異なっています。各地域からの参加者それぞれが持つ、IPアドレス・AS番号の分配ポリシーに対する考え方を議論の中ですり合わせていくことが、今後はより重要になってきそうです。

今回出された提案のうち、提案番号:prop-113とprop-114は、MLでの継続議論という結果になりましたが、議論の動向からは、今後のカンファレンスで開催されるポリシーSIGでコンセンサスとなる可能性が高い、と考えています。コンセンサスとなった提案は、その後のプロセスを経て、APNICのポリシーに反映されます。APNICポリシーが変更された場合には、原則としてJPNICポリシーにも反映されることになります。ポリシーSIGでの議論の動向はJPNICでも注視しており、今後も情報提供を行っていく予定です。

(JPNIC IP事業部 川端宏生)

● ポリシーSIGの様子

技術動向報告

本稿では、APRICOT 2015/APNIC 39カンファレンスで、DNS、ルーティングの分野において、興味深かった発表・議論をご紹介します。ここでご紹介しきれなかった発表もありますので、ご興味をお持ちの分野がありましたら、該当プログラムのWebページより、発表資料をご覧ください。なお、発表者の氏名・所属はプログラムのWebページの表記に従っています。

◆ DNS

今回のDNS関連の発表では、各運用者が観測したデータを元に、分析と対応を発表しているものが複数ありました。以下に、個別に説明します。

(1) Drilling Down into DNS DDoS Data: Bruce Van Nice(Nominum)
(2) Random DNS query attack and mitigation approaches: Eddy Winstead(Internet Systems Consortium(ISC))
(3) Water Torture:A Slow Drip DNS DDoS Attack on QTNet: Kei Nishida(Kyushu Telecommunication Network Co.,Inc)

最近のDNSを利用した攻撃の傾向としては、マルウェアをホームゲートウェイなど脆弱なデバイスにインストールし、該当デバイスを攻撃の発信元として攻撃対象の権威ネームサーバに対してランダムなサブドメイン名を大量に問い合わせる事例が増えており、現在考えられる対策が発表されていました。

上記三つの発表とも、共通した攻撃と対応案についての発表がされたのですが、各発表の特徴としては、(1) Drilling Down into DNS DDoS Dataでは世界各国のISPのトラフィックを観測した結果に基づく分析、(2) Random DNS query attack and mitigation approachesではBIND提供元としての情報提供、(3) Water Torture:A Slow Drip DNS DDoS Attack on QTNetでは九州通

信ネットワーク株式会社（QTNet）からの自社の体験に基づく対応が発表されていました。

一昨年のAPRICOT 2013/APNIC 37カンファレンスにおいて話題となった、オープンリゾルバについては継続して話題として取り上げられていました。コミュニティの対応によりオープンリゾルバの件数は減少傾向にあるのですが、DNSを元にした攻撃への取り組みとしてオープンリゾルバのみならずさまざまな性質の攻撃についてコミュニティが立ち向かっている様子が印象的でした。

（4）The Resolvers We Use: Geoff Huston（APNIC）

APNICが設置している、計測用サーバへのDNS問い合わせ（クエリ）の分析から得られた傾向の発表がありました。ユーザーの利用しているDNSキャッシュサーバの分布には特徴があり、ごく少数のキャッシュサーバを多数のユーザーが使っている傾向があるということでした。具体的には、観測できたキャッシュサーバのうち0.7%にて、ユーザー全体の90%のDNSクエリが処理されており、ユーザーの利用しているキャッシュサーバのトップはGoogle Public DNSとなり、ユーザー全体の10%がGoogle Public DNSを利用しているとのことでした。

- DNSセッション 参考URL

・DNS Session
https://conference.apnic.net/39#sessions/dnssession
- Drilling Down into DNS DDoS Data
- Random DNS query attack and mitigation approaches
- The Resolvers We Use

・Lightning Talks
https://conference.apnic.net/39#sessions/lightningtalks
- Water Torture:A Slow Drip DNS DDoS Attack on QTNet

・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

◆ ルーティング

今回のルーティング関連の発表では、RPKI関連の話題の他、DNSと同様に各運用者が観測したデータを元に分析と対応を発表しているものが複数ありました。本稿では、そのうちいくつかのセッションについて報告します。

（1）BGP in 2014：Geoff Huston（APNIC）

2014年のBGPの動向として、IPv4の経路数がハードウェア性能上の閾値となる51万2000を超えたものの、IPv4アドレス数が絶対的に不足している等の事情から、経路数の増加傾向としてはやや低減しつつあることと、アドレスの再利用の傾向が見られることが紹介されました。IPv6アドレスの経路数は、その絶対数はIPv4と比べると少なく2万程度であるものの、増加傾向は見られるということでした。

会場から、観測した経路数が51万2000を超えたタイミングについて、発表のあったものと異なる時期で観測したとのコメントがありました。こちらについては、観測するルータが保持するiBGP（AS内部で使われるBGP経路）の経路数などの要因により51万2000を超える時期に差異はあることは十分あり得ることであり、BGPがどのように運用者に見えるかは性質上異なるという議論がされていました。

（2）Where are we with securing the Routing System?：Geoff Huston（APNIC）

現在のインターネットルーティングは運用者同士がゆるやかに信頼しあって経路情報を交換するするモデルから成り立っており、誤った経路が流れる現象を検知・防止するためのセキュリティ技術の確立が課題となっています。この発表ではルーティングセキュリティの担保に役立つものとして、IRR、逆引きDNS、RPKIといった複数の技術の特徴や今後の展望が整理されて紹介されていました。

（3）Selective blackholing - how to use and implement：Job Snijders（NTT Communications）

DDoS攻撃への対策として、全トラフィックを落とすのではなく、地域を指定して選択的にトラフィックを落とすことで、必要なサービス用通信は維持しつつ、DDoS攻撃を避ける手法について、発表者のASでの利用経験を踏まえた紹介がされていました。

（4）BGP Flowspec（RFC5575）Casestudy and Discussion：Shishio Tsuchiya（Cisco Systems G.K.）

本発表もDDoS攻撃への対策が取り上げられていました。こちらでは、許可された通信を所定の条件で「フロー」として定義する技術にて対策する案について、JANOG35で実施された議論の内容を踏まえて紹介されていました。

- ルーティングセッション 参考URL

・APOPS 1
https://conference.apnic.net/39#sessions/apops1
- BGP in 2014

・Routing Session
https://conference.apnic.net/39#sessions/routingsession
- Where are we with securing the Routing System?
- Selective blackholing - how to use and implement
- BGP Flowspec（RFC5575）Casestudy and Discussion

第92回IETF報告

全体会議報告

第92回IETF Meetingは、2015年3月22日（日）から3月27日（金）の間、米国のダラスにあるフェアモント・ダラスというホテルにて、米グーグル社のホストで開催されました。ソーシャルイベントでは、IETFロゴの焼き印が入ったカウボーイハットを、参加者の頭のサイズに合うように調整して配っており、参加者からは好評だったようです。

◆ IETF Operation and Administration Plenary

3月25日（水）の「IETF Operation and Administration Plenary」では、はじめにウェルカムスピーチが行われ、

・ホストの米グーグル社の挨拶
・IETF Chairからの報告
・IAOC（IETF Administrative Oversight Committee）ChairとIAD（IETF Administrative Director） Chairからの報告
・IETF Trust Chair、 Nomcom Chairからの報告
・IETF CodeMatchの報告
・IETF Hackathonの報告
・2015 Jonathan B. Postel Service Awardのノミネート期間の紹介
・次回第93回IETF Meeting開催地の紹介
・IAOCオープンマイク
・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。

◯IETF Chairレポート
IETF Chairレポートでは、IETF Chair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92回の現地参加者は、57の国と地域から1,176人の参加となり、前回の1,080人の参加から96人ほど増加しています。また、2014年の同時期に英国ロンドンにて開催された、第89回の参加者数の1,400人弱と比較すると、200名程度参加者が減ったことがわかります。新規参加者は全体の15%弱の172人で、今回も新しい参加者層の取り込みは継続的に進んでいるようです。新規参加者が継続して増える一方で、全体の参加人数がほぼ横ばいになっている状況です。国別の参加者数は、1位米国、2位中国、3位日本、4位ドイツとなっており、参加者全体の約半数を米国、約7割を上位4ヶ国が占める割合となっていました。また、開催国米国の隣国カナダからの参加者数は6位となっていましたが、紹介されたグラフを見る限りでは、日本やドイツとほぼ同じ参加者数であることがわかりました。

また、IETFの会場ネットワークについての新たな試みとして、今回から会場のワイヤレスネットワークを利用するにあたり認証が必要になったことと、会場ネットワークのDNS（meeting.ietf.org）にDNSSECが導入されたと報告がありました。ワイヤレスネットワークについては、会場のほぼすべてのワイヤレスネットワークに接続する場合に認証が必要となり、これまで会場でよく利用されていたSSID「ietf」も対象となっていました。

前号でも報告しましたが※1、IESGが進めている八つのIETFエリア（応用分野（APP）、インターネット分野（INT）、運用管理分野（OPS）、リアルタイム応用・基盤分野（RAI）、ルーティング分野（RTG）、セキュリティ分野（SEC）、トランスポート分野（TSV）、その他分野（GEN））の再編作業については、進捗報告がありました。この再編は2015年の夏頃を完了のめどとしており、現在の決定事項として、応用分野（APP）とリアルタイム応用・基盤分野（RAI）を統合して、応用・リアルタイム分野（ART）とすることが決定されました。これに伴い、現在応用分野（APP）とリアルタイム応用・基盤分野（RAI）に合わせて4名いるエリアディレクターを、一つのエリアにまとめることで3名に減らすと報告がありました。また、エリアの再編が完了するまでは、他のエリアではエリアディレクターの変更は行わないと報告されました。

他の新たな試みとしては、土曜日にIETF開催前のターミナルルームを使用して、第1回となるIETF Hackathonを行ったとの報告がされました。IETFでは全般的に、提案内容が実装可能であるものとみなして議論がされていますが、まれに実装が考慮されていない提案もあり、それに気づいた参加者から指摘を受けるというような場面があります。しかし、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は、David Clark氏が"We reject kings, presidents and voting. We believe in rough consensus and running code"と端的に言い表した通り、IETFの肝はrunning codeなのです。そのため、今回のHackathonのように、running codeの重要性をイベントとしてあらためてきちんと示していこうとする姿勢は、大事であると感じまし

※1 第91回IETF報告［第1弾］全体会議報告
https://www.nic.ad.jp/ja/newsletter/No59/0650.html

た。このイベントは継続して行う予定で、第2回IETF Hackathonは、第93回IETFの直前の2015年7月18日（土）から19日（日）の2日にかけて行われるそうで、現在、準備や参加者を募集していると呼びかけがありました。

○IAOC・IAD Chairレポート
IAOC・IAD Chairレポートでは、IAOC ChairのChris Griffiths氏およびIADのRay Pelletier氏より報告がありました。

今回の会議の収支決算速報では、参加者人数は予測の1,120人より多く、参加費およびスポンサー費の合計は、130万ドルになったとの報告がありました。一方で、ハワイで行われた第91回の収支決算最終報告では、参加者人数は予測を132人下回り、参加費は収入見通しを6万8千ドル下回ったとの報告がありました。また、ハワイ会合のスポンサー費は予算案より5万7千ドル下回り、そのためBits-N-Bitesがキャンセルされたとの報告がありました。なお、ハワイ会合の純利益は、56万5千ドルとなったとのことでした。今回は、IETFの2014年会計報告もありました。2014年は430万ドルの収入に対して580万ドルの支出があり、別途ISOCから160万ドルの資金援助があったとのことです。この他に、米シスコ・システムズ社から82万6千ドル分の機材やソフトウェアの提供等があったとの報告があり、参加者から拍手が起こりました。

また、今回は第91回の段階では決まっていなかった、第93回IETF Meetingのホストがcz.NICとBrocade社に決まり、会場からは大きな拍手が起こりました。一方、IETF史上初となる、南米はアルゼンチン・ブエノスアイレスにて開催される第95回IETF Meetingのホストは、まだ決まっていないとのことでした。

最後に、IADのRay Pelletier氏より、謝辞として第92回IETF Meetingのスポンサーとなった各企業やNOCメンバー、Hackathonを開催したメンバーが紹介されました。ホストおよびWelcome Receptionのスポンサーをした米グーグル社の他に、回線提供をした米タイム・ワーナー・ケーブル社、そして、今回のBits-N-Bitesをスポンサーした各社が紹介されました。また、NOCメンバーの紹介では、日本のWIDE Projectからの参加者として、浅井大史氏が紹介されました。

○IETF CodeMatch
IETF CodeMatch（https://codematch.ietf.org/）とは、IETFで標準化されるプロトコルを実装するコードを、学生や研究者、民間企業のエンジニア等、さまざまな人々の間で共有するためのマーケットプレイスを指し、また、それを作ることを目的として行われている活動です。今回は、その活動の紹介や、モックアップサイト（http://codematch.inf.ufrgs.br/）の紹介等が行われました。

○2015 Jonathan B. Postel Service Award
次回第93回IETF Meetingでは、2015 Jonathan B. Postel Service Awardの発表があるとのことで、はじめにインターネットの発展に貢献したJonathan B. Postelの功績についての紹介と、過去の受賞者の紹介がありました。また、2015年3月25日（水）から5月15日（金）の期間で、ノミネートを受け付けているとの報告がありました。

○第93回IETF
次回のIETF Meetingは、2015年7月19日（日）から7月24日（金）にかけて、チェコのプラハにて開催されます。CZ.NICのCEOであるOndrej Filip氏より、開催地となるプラハの魅力について説明がありました。プラハの美しい街並みや文化の紹介があり、早めに現地入りして観光を楽しんでみてはいかがでしょうかと話されていました。また、チェコと言えばビールの個人消費量が世界一の国でもあり、取りすぎたビールのカロリーは、その美しい街を散策することで消費してくださいとのアドバイスもありました。

◆ Technical Plenary

3月23日（月）の「Technical Plenary」では、IAB（Internet Architecture Board）Chair、RSE（RFC Series Editor）・RSOC（RFC Series Oversight Committee）Chairからの報告、Technical Topicが一つ、IABの主な活動の報告が二つ、IABオープンマイクという流れで議事進行がされました。

○IAB Chairレポート
はじめにIAB ChairのRuss Housley氏より、IAB memberの入れ替えについて発表がありました。Joel Halpern氏、Eliot Lear氏、Xing Li氏の任期が終了し、新たにRalph Droms氏、Robert Sparks氏、Suzanne Woolf氏が加わりました。Jari Arkko氏、Russ Housley氏、Andrew Sullivan氏、Dave Thaler氏は継続となります。また、IAB Chairが、Housley氏からSullivan氏に交代すると発表がありました。

それから、IAB Workshopとして、2015年1月26日（月）から27日（火）の期間に、スイスのチューリッヒでSEMI（IAB Workshop on Stack Evolution in a Middlebox Internet）を開催したと報告がありました。また、2015年6月19日（金）にドイツのベルリンにて、CARIS（IAB/ISOC Workshop on Coordinating Attack Response at Internet Scale）を開催すると発表がありました。

○Technical Topic
Technical Topicでは、Hannes Tschofenig氏とDave Thaler氏から、“Smart Object Architecture”と題した発表がありました。近年増加している、インターネットとの連携を想定したセンサーやスマート家電等、また、それを制御する携帯端末やネットワークについて具体的な製品例等を交えながら、現状の関連技術についてまとめた発表がありました。

○IABの主な活動報告
IABの主な活動報告としては、前述したSEMIの活動報告と、Unicode 7.0の問題点について報告がありました。Unicode 7.0から新たに追加された、ARABIC LETTER BEH WITH HAMZA ABOVE（U+08A1）という文字は、同一の字形を表すARABIC LETTER BEH（U+0628）と、ARABIC HAMZA ABOVE（U+0654）を用いた結合文字列（combining character sequence）と等価の関係になっておらず、利用者の混乱を生む可能性を指摘されたと報告がありました。

IETFのいくつかのプロトコルでは、Identifierとして用いる文字列は比較一致の機会を増やすため、文字列の比較を行う際に前処理として、文字列に対して正規化処理を行います。これにより、異なる文字コードによる入力があった場合でも、等価の関係にある文字は同一の文字として一致させることが可能となるのですが、このARABIC LETTER BEH WITH HAMZA ABOVE（U+08A1）はそのような等価の関係を示す情報を持たないため、Identifierとして使用する場合、問題が生じると報告がありました。これに対しIETFでは、LUCID（Locale-free UniCode Identifiers）BoFを開催し、Identifierとして使用するUnicodeテーブルに対して、IETF独自のパッチを当てるか検討を行っていくと報告がされました。

（青山学院大学 情報メディアセンター 根本貴弘）

● 会場のThe Fairmont Dallas（ホテルの公式Webサイトより引用）

IETFにおける暗号技術に関する動向（楕円曲線）

本稿では、第92回IETFにおけるセキュリティ関連の報告のうち、セキュリティエリアでの技術的な動向に大きく影響すると予想される、IRTF（Internet Research Task Force）にある暗号のグループであるCFRG（Crypto Forum Research Group）で議論された「新しい楕円曲線の動向」について報告したいと思います。

◆ NISTが承認した楕円曲線以外を選定することに関する動向

第90回IETFで開催されたIRTFにある暗号のグループであるCFRGにおいて、新しい楕円曲線としてNUMS Curves（Nothing Up My Sleeve Curves - バックドアのない楕円曲線）や、高速化が期待できるCurve25519、Curve41417、E-512といった楕円曲線が提案されたことが報告されました。これらの楕円曲線に関する議論について、今回の会合で方向性が決定したことが共有されたので報告します。

1. CFRGで検討した楕円曲線に関する状況について
IETFで検討されているTransport Layer Security（TLS）や、X.509証明書を含む暗号技術を用いたアプリケーション向けに利用されることを想定した、素体上の楕円曲線のための確定的なパラメータ生成アルゴリズムを規定することを目的としたInternet Draft（I-D）の第2版が投稿されたことが報告されました。

なお、このI-Dで規定された楕円曲線の安全性レベルは、等価安全性の観点から128bitセキュリティおよび224bitセキュリティを実現することができます。等価安全性とは、米国商務省国立標準技術研究所（NIST）によって提唱されている、公開鍵暗号や共通鍵暗号のような異なる種類の暗号技術に対しても、同一の評価尺度で安全性を表すようにした基準です。例えば、128bitセキュリティでは共通鍵暗号は128bitの鍵長、RSAのような素因数分解問題に基づく方式であれば3072bitの鍵長、ECDSAのような楕円曲線上の離散対数問題に基づく方式であれば、256bitの鍵長となります。詳細はI-D※1をご確認いただけたらと思います。

ここでは、今回の会合で報告された変更点を示します。

- 追加された楕円曲線
以前から有力視されていたCurve25519に加えて、Goldilocksという楕円曲線が追加されました。この楕円曲線は、224bitセキュリティの安全性を実現することができ、2^448 - 2^224-1で3 mod 4と合同という条件を満たす特徴を持った素数を利用しており、これは広いアーキテクチャでの高いパフォーマンスを期待できます。現状のステータスは、異なるパラメータサイズで動作するようにアルゴリズムを微修正している状況ですが、アルゴリズムの正しさの確認は行われていない状況とのことです。今後、専門家によるレビューで確認されることが予想されます。

- Diffie-Hellman鍵交換のためのu-value
このI-Dで記述されているCurve25519やCurve448を用いた楕円曲線上のDiffie-Hellman鍵交換を実現するために、GF（2^255-19）やGF（2^448-2^224-1）からなる要素であるu-valueを送信することを決定しました。

- ゼロ出力に関するチェック
現在のI-Dに記述されている手順において、間違った位数が入力された場合の確認処理が不十分であることが報告されました。

- パラメータ生成
エドワード曲線を生成し、同型写像や同種を得るために必要となるパラメータ生成を使用します。このI-Dでは、SAGEというPythonベースの数学ライブラリを用いて、Curve25519やCurve448向けのu=5に関するベースポイントを生成したとのことです。

これらのトピックについては、CFRGのメーリングリスト上でIETF 92までの間に活発に議論されていたため、方針に影響を与えるような大きな質問はなく、スムーズな合意形成が行われました。

2. CFRGで検討した楕円曲線の今後について
CFRGのco-chairであるKenny Paterson氏から、CFRGで検討した楕円曲線に関する状況やElliptic Curves for Security（draft-irtf-cfrg-curves-02）を踏まえて、楕円曲線に関する現状の活動と今後について発表がありました。本稿では、発表でのポイントとなる部分を抜粋して報告します。

- Research Group（RG）としての決定事項について
RGは、新しい楕円曲線としてCurve25519（128bitセキュリティ）とGoldilocks曲線（224bitセキュリティ）の二つの曲線を選択しました。これらの曲線は確定的な方法で生成される特性を持っており、Elliptic Curves for Security（draft-irtf-cfrg-curves-02）で規定されているものとなります。

- IETF/IRTF以外での取り組みについて
IETF/IRTFで議論した結果について、2015年6月11日にNIST主催で開催されるWorkshopであるElliptic Curve Cryptography Standards※2に対して、IETF/IRTFとしてのインプットとして提案したことが共有されました。また、World Wide Web Consortium（W3C）とも情報交換を実施していることも共有されました。

- 新しい楕円曲線を用いた署名方式に関する検討について
新しい楕円曲線を決定しただけでは、我々が生活の中で利用しているような鍵交換やデジタル署名として利用することができません。次のステップとして、今回選択した新しい楕円曲線を用いたデジタル署名方式を定義することに注力することが報告されました。いくつかの選択肢としてのデジタル署名候補として、下記のような方式が共有されました。

［新しい楕円曲線上でのECDSA］
従来、NIST曲線を利用したECDSAは標準化されており、正しい演算が行われたかどうか、正しく実装されているかを確認するためのテストベクタが公開されていますが、今回のように楕円曲線を変更することで得られるデジタル署名の結果が異なる値になるため、新たなテストベクタが必要となります。

［脱ランダム化された（De-randomised）ECDSA］
脱ランダム化されたECDSAは、一般的な故障モード攻撃を避ける特徴があり、署名値であるrを署名対象データであるメッセージのハッシュ値と署名鍵による生成か、署名鍵を含まない擬似乱数関数（Pseudo-Random Function; PRF）を用いた生成が可能になるデジタル署名です。

［EdDSA］
通常のDSAとは異なり、DSAと同様な離散対数問題に基づいた方式であるシュノア署名の変形版です。この方式は、脱ランダム化に関する仕組みを活用しており、よく利用されているECDSAとは異なる検証方法を利用します。オープンソースコミュニティへの採用実績としては、OpenSSHに実装されています。

これまでの取り組みや方針が共有されるだけではなく、CFRG参加者に対していくつかの質問が投げかけられました。ここで投げかけられた質問は、今後の楕円曲線に関する方針に大きく影響を与えるため、次に示す四つの質問を共有したいと思います。

- ここまでに列挙した三つのデジタル署名方式以外に検討すべき方式はあるか？
- TLSプロトコルに関するNISTの遵守事項をどの程度考慮すべきか？
- 他のアプリケーションに関して遵守事項をどの程度考慮すべきか？
- タイムリーに役立つ結論を得るための議論をどのように構造化すべきか？

上記の質問を受けて会場で行われた議論の抜粋を以下に示します。

- NIST曲線であるP-256やP-384上でのECDSAを取り扱っているのではないため、IETF/IRTFとしてはNISTの遵守事項について考慮すべきではないのでは？
- IETF/IRTFとしてNISTと関わりあうべきであり、考慮しなくて良い存在ではない
- 銀行やそれ以外の高付加価値の組織に受け入れられるかどうかを考慮すべきでは？
- シュノア型のデジタル署名の変形版であるEdDSAでは、既存のECDSAと異なるAPIになることが予想される

今回の第92回IETFにおいて、新しい楕円曲線に関する議論について方向性は示されましたが、これらの楕円曲線の応用として検討されているデジタル署名方式を取り巻く状況は、会合での議論からも予想できるように、まだ方向性の確定までに時間が掛かりそうな状況です。ここでの決定がIETFで検討されているさまざまなエリアのWGへの仕様検討にも影響があることから、今後とも注目することが重要になると思います。

◆ 参考：楕円曲線関連の発表資料

- CFRGで検討した楕円曲線に関する状況についての発表資料
http://www.ietf.org/proceedings/92/slides/slides-92-cfrg-0.pdf

- Curves - next stepの発表資料
http://www.ietf.org/proceedings/92/slides/slides-92-cfrg-8.pdf

（NTTソフトウェア株式会社 菅野哲）

※1 Elliptic Curves for Security（draft-irtf-cfrg-curves-02）
http://tools.ietf.org/html/draft-irtf-cfrg-curves-02

※2 Workshop on Elliptic Curve Cryptography Standards
http://www.nist.gov/itl/csd/ct/ecc-workshop.cfm

IPv6関連WG報告 ～6man WG、v6ops WG、sunset4 WG～

第92回IETFで筆者が会合に参加した、IPv6に関連するWorking Group（WG）の中から、6man WG、v6ops WG、sunset4 WGについて、主な議論の概要を報告いたします。

◆ 6man WG（IPv6 Maintenance, Int Area）

6man WGは、IPv6の仕様およびアーキテクチャのメンテナンスと、最新化を行うWGです。IETFにおけるIPv6関連トピックの受け皿となり、IPv6の仕様拡張や変更に関して、責任を持っています。6man WGから下記のRFCが発行されたことが、チェアから報告されました。

RFC7421 - Analysis of the 64-bit Boundary in IPv6 Addressing
https://tools.ietf.org/rfc/rfc7421.txt

IPv6ユニキャストアドレスのインタフェース識別子（IID）が64-bitで固定されていることの利点および可変にしたときの影響について、調査結果をまとめたInformational RFCです。

今回は一つのワーキンググループドラフト、11の個人ドラフト（そのうち四つが新規ドラフト）が話し合われましたが、特に議論を集めた3項目について紹介いたします。

（1）Validation of IPv6 Neighbor Discovery Options
（draft-ietf-6man-nd-opt-validation）
2015年3月にワーキンググループドラフトとして提出されたもので、IPv6近隣探索（ND）におけるNDメッセージのオプション情報の評価について、推奨のルールを決めています。Source Link-Layer Address（SLLA）オプションとTargetLink-Layer Address（TLLA）オプションについて、オプション内のリンクレイヤアドレスに、ブロードキャストアドレス・マルチキャストアドレスまたは受信ノードのリンクレイヤアドレスが指定されている場合は、このオプションを無視しないと、パケットの転送を反復させる攻撃が可能となってしまいます。それ以外のオプションについての記述は、既存の文書（RFC4861、RFC2464）と大きな変更が無いので、この二つのオプションの記述のみに絞るべきかどうかが議論されています。

（2）A survey of issues related to IPv6 Duplicate Address Detection
（draft-yourtchenko-6man-dad-issues, draft-nordmark-6man-dad-approaches）
近隣探索プロトコルの無線環境における問題についての議論の一環です。重複検出（DAD）について、問題点と解決に向けたアプローチが、それぞれまとめられています。「アドレス重複が起こる確率は低いので、配慮する必要は無いのでは」という意見がある一方、「実際にアドレス重複が起きたらトラブルシュートするのは時間がかかるので、解決手段を得るためには必要だ」という意見もありました。こちらは多くの関心を集めており、引き続き議論されていく予定です。

（3）IPv6 Neighbor Discovery Optional Unicast RS/RA Refresh
こちらも近隣探索プロトコル（ND）に関連し、定期的なマルチキャストのルータ要請（RA）は無線環境には適さないことから、ユニキャストでルータ探索（RS）を更新できるように、RSメッセージにR-flagを追加しようという提案です。また、RAメッセージにオプションを追加して、ルータ側から更新時間を通知できるようにします。この提案は「IPv6のRFC全体に影響を与えることから、問題の解決策としてはよいアプローチではない」という意見が大勢を占めました。

◆ v6ops WG（IPv6 Operations, Ops Area）

v6ops WGは、IPv6を全世界に展開するにあたっての緊急の課題、特に運用上の課題に対処することに焦点を当てたWGです。また、新しいネットワークや既存のIPv4ネットワークにIPv6を導入するためのガイドラインや、IPv4/IPv6共存ネットワークの運用ガイドラインを作成することも目的としています。

今回のv6ops WGでは、“IPv4 as a service”と呼ぶ、新しいプロジェクトを始める提案がチェアからなされました。IPv6のネットワーク上において、IPv4を必要なサービスとして提供する（ただし、徐々に減らしていく）というシナリオを前提として、IPv4 over IPv6技術の展開における運用ガイダンスを書くというプロジェクトです。対象とする技術は、現在、次の九つです。

（1）464XLAT（RFC 6877）
（2）SIIT-DC（draft-anderson-v6ops-siit-eam, draft-ietf-v6ops-siit-dc, draft-ietf-v6ops-siit-dc-2xlat）
（3）MAP-E encapsulation（draft-ietf-softwire-map）
（4）MAP-T translation（draft-ietf-softwire-map-t）
（5）RFC6145 translation（stateless translation to an IPv4-embedded IPv6 Address）
（6）RFC6146 translation（stateful translation IPv6 clients->IPv4 servers）
（7）DS-LITE（RFC 6333）
（8）Lightweight 4over6（draft-ietf-softwire-lw4over6）
（9）LISP（4 over 6, various RFCs and drafts）

これらの技術に関する経験の集約には、オペレーターからの意見が重要なので、各地のNOG（Network Operators Group）と連携しながら進めていきたいと表明されました。これらの技術の利用が既に始まっている日本から、多くの貢献ができるのではないかと筆者は考えています。

この提案に関連する形で、日本でのMAP-Eの利用状況について、日本ネットワークイネイブラー株式会社（JPNE）の中川

あきら氏が発表を行いました。中川氏の発表では、日本におけるIPv6普及状況とIPv6トラフィックが増加していること、JPNEがMAP-Eを選択した理由と現状で特に大きな問題が発生していないことが報告されました。

JPNEがMAP-Eを選択した理由としては、「ステートレスであるためログ収集が不要で運用が楽なこと」「カスタマサポートが容易なこと」「エンド-エンドで通信が可能であること」が挙げられていました。また、「速度測定結果ではIPv6通信とIPv4通信が同程度であること」「ポート利用状況の統計データからユーザーに十分な数のポートが割り当てられていること」「接続判定ページが提供されており、トラブルシュートが容易になっていること」などの実用的な情報提供がされました。

会場の参加者は非常に興味を持っており、スライドの内容について詳しく知りたいという内容の質問が相次ぎました。また、日本のIPv6の普及状況について、日本のコンテンツプロバイダに対してIPv6でのサービスを促してはどうか、という突っ込んだ内容の発言もありました。

インドからは、MAP-Tのトライアルについての発表がありました。発表の構成は中川氏とほぼ同様でしたが、MAP-TとMAP-Eを比較して、「MAP-TはQoS/SLAなど顧客単位のポリシー適合が容易であること」「DPI装置の利用が容易であること」などが挙げられ、国が異なれば選択される技術が異なることが、興味深かったです。

また、中国からは、CERNETとChina Telecom社における、MAP-TとMAP-Eの同時提供のトライアルについての発表がありました。同一のBR（Border Relay）とCPE（Customer Premises Equipment）で、MAP-TモードとMAP-Eモードを自動的に変更できるという、非常にユニークな構成となっています。MAPによるアドレス共有比率について実際のユーザーで試した結果、「1/256（1ユーザーあたり255 port）はOK」「1/512（1ユーザーあたり127 port）では、一部のユーザーに影響があったかもしれない」など、興味深いデータが提供されていました。

2日目のv6ops WGでは、2件のドラフトが、WGLC（Last Call）となることの同意が得られました。

- Some Design Choices for IPv6 Networks
（draft-ietf-v6ops-design-choices）

IPv6ネットワークをデザインするにあたり、ルーティングに関してどのような選択肢があり、それぞれにどのようなメリット・デメリットがあるのかを、網羅的に調査したドラフトです。リンクローカルアドレスしか付与されていないインタフェースについて、“unnumbered”と呼ぶか“link-local-only”と呼ぶか（あるいはそれ以外か）という議論に、白熱するという一幕もありましたが、ミーティングでは後者に落ち着き、WGLCをすべきかの採決が行われ、賛成多数となりました。

- Close encounters of the ICMP type 2 kind（near misses with ICMPv6 PTB）
（draft-jaeggli-v6ops-pmtud-ecmp-problem）

「ロードバランサ環境下で、ICMPv6type 2“Packet Too Big”（PTB）メッセージ応答が元のサーバに返らない」問題です。こちらもWGLCをすべきかの採決が行われ、賛成多数となりました。

また、データセンター内ネットワークのIPv6化に関して、次のような注目すべき発表が行われました。

- SIIT-DC
（draft-anderson-v6ops-siit-eam, draft-ietf-v6ops-siit-dc, draft-ietf-v6ops-siit-dc-2xlat）

“IPv4 as a service”プロジェクトでも取り上げられている、IPv6で構成されたデータセンター内ネットワークにおいて、IPv4での接続性を提供する方法に関する一連のドラフトです。

draft-anderson-v6ops-siit-eamは、RFC6145にて定義され、464XLATではCLAT側で使われている、ステートレスなIPv4/IPv6変換（Stateless IP/ICMP Translation（SIIT））のアドレスマッピングルールを、緩和することを提案するものです。元は、draft-ietf-v6ops-siit-dcに含まれていた内容でしたが、単体で有用と見なされ、切り出されました。

RFC6145では、IPv6アドレス（64:ff9b::/96）の中にIPv4アドレスを埋め込むなど、RFC6052で定義されたマッピングルールしか認めていません。しかし、464XLATで利用するにはこの制約は不都合であるため、任意のIPv6アドレスに静的にマッピングする方法が求められています。事実、Androidの464XLAT実装では、RFC6052のルールを既に使っていないというコメントが会場から出されました。そのため、このドラフトはRFC6145をアップデートするものとして、ワーキンググループドラフトとして採用される予定です。

draft-ietf-v6ops-siit-dcとdraft-ietf-v6ops-siit-dc-2xlatは、共に前回のIETF 91にて、ワーキンググループドラフトに採用されています。例えるならば、データセンター側にステートフルNAT64または464XLATを提供し、IPv4ネットワークからIPv6データセンター内の、IPv6/IPv4サーバに接続できるようにする提案です。特に、464XLATに類似した手法を使った場合、データセンター内でIPv4のみのソフトウェアやデバイスをサポートできるようになります。これらの二つのドラフトは、利用形態やレファレンスが多く重複することから、一つのドラフトとしてまとめられることとなりました。

◆ sunset4 WG（Sunsetting IPv4, Int Area）

sunset4 WGは、IPv6への完全な移行に向けて、アプリケーション・ホスト・ネットワークが、IPv4への依存無しに機能することをめざすWGです。他のWGに対して、プロトコルの策定に際してIPv4に依存しないよう、働きかけを行うことも目標にしています。

前回のIETF 91ではミーティング自体が開催されず、MLの流量も少ないため、残念ながらあまり活発ではなくなってしまったWGです。なぜこちらのWGを取り上げたかというと、“IPv4 as a service”プロジェクトについて、v6ops WGとsunset4 WGのどちらが適切か、という議論があったためです。しかし、両WGの違いはどこなのか、という議論にすり替わり発散してしまったため、特に決定事項はありませんでした。

ワーキンググループドラフトとして、IPv6移行の最終段階においてIPv4を実際に無効化するときの難しさについて列挙したdraft-ietf-sunset4-gapanalysisが残っており、MLで引き続き議論をしていくことが確認されました。

（NTTコミュニケーションズ株式会社 西塚要）

● IETFに初めて参加する人向けの情報をまとめたWebページ

DNS関連WG報告

本稿では、DNSに関連した議論の動向として、DNSへの問い合わせをプライバシー情報と見なして前回の第91回IETFから検討を行っているdprive WGと、定例的に報告しているdnsop WGの活動を取り上げてご紹介します。

◆ dprive WG（DNS Private Exchange WG）報告

DNS Private Exchange WGの会合は、2015年3月23日（月）の午後に90分間のセッションとして開催されました。このWGは、前回の第91回IETFから活動しており、今回で2回目の会合となります。DNSに問い合わせた名前はプライバシーに関する情報であり、この情報を攻撃者が盗み見ることによって、多くの情報を得ることができてしまうという問題を解決するためのWGとなります。

まず、Internet-Draftの確認から行われました。DNSのプライバシーに関する検討事項について述べたドラフト文書が、IESG（Internet Engineering Steering Group）のレビューに回されたことが確認され、このプライバシーに関する検討事項を解決するために現行提案されている手法について、確認が行われました。

次に、draft-am-dprive-eval-00に関する発表が行われました。この文書は、DNSの問い合わせに含まれるプライバシー情報を、攻撃者が盗み見る手法に関してのパターン分類や、それを防ぐための代表的な手法と、その効果の評価手法に関して述べたものです。dprive WGの出発点となる文書となっています。この発表に関しては、攻撃者が何を狙っているのか、また攻撃のパターン分類は適切かといった議論、ならびに「攻撃者」という定義が当てはまるのかといった用語的な議論が行われました。引き続き、議論される模様です。

さらに、Private DNSに関する発表が行われました。これは、プライバシーを保った状態で使うことのできるDNSサーバ、もしくは名前解決の仕組みを提供する手法をまとめた発表でした。Online Certificate Status Protocol（OCSP）での経験を元に、プライバシーが確保されることで、ネットワーク環境によって動作しなかったり、名前解決が遅延してしまうようなことが発生してはならない、という目標が示されました。また、実現手法として、HTTPS上でのJSON（JavaScript Object Notation）を用いた名前解決や、TCPでのTLS（Transport Layer Security）を用いた名前解決が提案されました。誰もが名前解決に使える従来のようなDNSサーバと、プライバシーを確保したい場合に用いるDNSサーバを、ユーザーが用途に応じて切り替えられることが必要だ、という議論が行われました。

関連して、draft-hzhwm-dprive-start-tls-for-dnsに関する発表と議論が行われました。これは名前の通り、DNSのトランザクションにTLSを用いる、という提案です。通常の53番ではなく、TLSを用いたTCPにて通信するための専用ポート番号を割り当てることを提案しています。この提案に関しては、DNSはUDP53番ポートと定義しているミドルボックス等も存在するため、新たなポート番号での名前解決が、必ずどの環境でもできるとは限らないといった指摘がありました。また、TLSのオーバーヘッドに関する質問も出ました。これに関しては、実装上の工夫として、TCP Fast Open（RFC7413）※1の利用等が提案されていました。

draft-wijngaards-dnsop-confidentialdnsに関する発表と議論も行

われました。この文書は、opportunistic encryption、つまり必要な場合だけ暗号化を要求することを、DNSサーバとクライアントとの間で可能にする手法を提案したものです。ENCRYPTというリソースレコード（RR）を定義し、このRRを用いて鍵を交換することで通信を暗号化します。TLSに比べてアプリケーションレベルで暗号化を行うため、この方が負荷が高いのではないかといった議論や、鍵のやりとりはTCPにするべきでは、といった議論が行われました。引き続き議論が行われるようです。

最後に、このWGをどのように進めるべきか、の議論が行われました。現在出ている提案が列挙され、ハミングによる確認が行われました。有力であったのはDNS over TLSでしたが、引き続き議論が行われます。

◆ dnsop WG（Domain Name System Operations WG）報告

dnsop WGの会合は、3月24日（火）の午後、2時間のセッションとして開催されました。まずいつも通り、Internet-Draftの確認が行われました。その後、draft-ietf-dnsop-qname-minimisationに関する発表が行われました。この文書は、DNSのプライバシー確保にも関連するものであり、DNSへの問い合わせにおいて省けるものはなるべく省いて、名前問い合わせを減らそうという提案です。最終的に解決したい名前を問い合わせるDNSサーバの数を減らす、もしくは名前を問い合わせる回数を減らすことで、プライバシー情報である、解決したい名前が漏れることを防ぎます。大きな反対はありませんでしたが、引き続き議論が行われることとなりました。

次に、draft-ietf-dnsop-root-loopbackに関する発表がありました。前回の第91回IETFにてWG draftとなった文書で、ホスト自身がルートDNSゾーンを有して、ユーザーからの名前解決要求に応じて、手元に保持するルートDNSゾーンから、TLDに関するRRの検索を行うことを可能にする提案です。これにより、今までルートDNSサーバに問い合わせて得ていた情報が、手元に保持するゾーンにて得られるため、名前解決に要する最終的な時間を短縮することが可能になります。また、手元に保持しているゾーンの情報が正しいものであるかどうかは、DNSSECを利用して確認します。ルートDNSゾーンはDNSSECにて署名されているため、改竄から守られており、手元に保持しているものが改竄されたとしても判別できます。

さらに、draft-ogud-dnsop-any-notimpに関する発表が行われました。この文書は、DNSサーバに対する問い合わせを拒否するための手法について提案したものです。例えば、明らかに攻撃であり、返答を行いたくないような問い合わせに対しては、REFUSEDやNOTIMP、もしくはRTYPE＝NULLなどの返答を行うという提案であり、またそのためのフィルタリング記述方法を定義しようという提案です。この提案に関しては、多くの意見が出されました。その動機がうまく述べられていないため誤用される心配があるといった指摘や、必要に応じて既に行われているのだから標準化してしまえばいい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。

他にも、

- Minimal IXFR（Incrememtal xfer）に関する発表と議論
- アプリケーションによって隠れて使われているTLDの存在の紹介
- ICANNの新gTLDプログラムの現状に関する報告
- NSEC（Next Secure）を用いたネガティブキャッシュの提案
- EDNSの正しい実装の普及具合

に関する報告等が行われました。

Minimal IXFRは、DNSSECで署名されたゾーンを転送する場合の、データ転送量を削減するための提案です。アプリケーションによって隠れて使われているTLDとして、.onionの紹介があり、さらに.mailや.home、.corpといったものも、実際のTLDとして使うことを避けた方がよい、という提案がなされました。NSECによるネガティブキャッシュの提案は、NSECを用いることで存在しないとわかっている範囲の名前は、積極的にネガティブキャッシュとして保持することで、DNSサーバへの無駄な問い合わせを減らすという提案です。特に、RFC6761※2にて定義される特別なドメイン名や、今回の会合で紹介されたような特別なTLDに関しては、取り出して集中議論する必要があるという意見が出され、次のIETF会合までにWebEXによる中間会合が開催さ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）

● IETFではさまざまなリモート参加の手段が用意されています

※1 RFC7413"TCP Fast Open"
https://tools.ietf.org/html/rfc7413

※2 RFC6761"Special-Use Domain Names"
https://tools.ietf.org/html/rfc6761