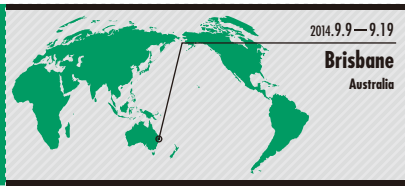
APNIC 38カンファレンス報告



全体およびアドレスポリシー関連報告

2014年9月9日（火）～19日（金）に、オーストラリア・ブリスベンにて、APNIC 38カンファレンスが開催されました。APNICカンファレンスは、APNICの本拠地があるオーストラリアで開催されることが多いと思われる方もいらっしゃるかもしれませんが、実は2010年8月のゴールドコーストでのカンファレンス以来、4年ぶりの開催となります。また、APNICの本拠地であるブリスベンでの開催は、2000年10月以来、およそ14年ぶりとなり、普段はオフィスで業務を行っているAPNICスタッフも多数参加していました。普段はメールや電話でのやり取りを行っていたAPNICスタッフとも、実際に顔を合わせて相談などを行う機会も何度かあり、JPNICスタッフとAPNICスタッフとのコミュニケーションを深める、良い機会となりました。本稿では、このカンファレンスの模様をご紹介します。

◆ APNIC 38カンファレンスの概要

今回のカンファレンスには、47の国や地域から331名の参加登録があり、そのうち、日本からの参加者は15名程度でした。毎年2月～3月に開催されるAPRICOT/APNICカンファレンスに比べて半分程度の参加者数となりますが、その分、参加者同士の距離は近く、アットホームな雰囲気であるように感じました。

カンファレンスは「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）」などから構成されています。その他にも、APNICとの関連の深いAPIX（Asia Pacific Internet Exchange Association）、APTLD（Asia Pacific Top Level Domain Association）、APCERT（Asia Pacific Computer Emergency Response Team）やISOC-AU（The Internet Society of Australia）などの組織が主催する、会議やセッション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、以下の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。

http://conference.apnic.net/38/program

今回はこれらのセッションの中から、主なものをいくつかご紹介します。

◆ IANA機能の監督権限移管に関する提案と、インターネットガバナンス関連の動向について

IANA（Internet Assigned Numbers Authority）は、「ドメイン名」「番号資源」「プロトコルパラメーター」の、三つの重要なインターネット資源に関わる機能を担っています。これらの機能について、米国商務省情報通信局（National Telecommunications and Information Administration; NTIA）が持つ監督権限を移管する意向を2014年3月14日（金）に発表しました。この発表を受けて、移管後においてIANA機能の監督権限がどのようにあるべきかについて、各所で議論が進められています。APNICやJPNICにおいても、IANA機能の監督権限移管に関する情報提供を行っております。

・IANA oversight transition（APNIC Webページ）
http://www.apnic.net/community/iana-transition

・IANA機能の監督権限の移管について（JPNIC Webページ）
https://www.nic.ad.jp/ja/governance/iana.html

日本インターネットガバナンス会議（IGCJ）のメーリングリスト※1や、IP-USERS ML※2でもお知らせしていますが、今回のカンファレンスに先立ち、APNICからは、IANA機能の監督権限移管に関する提案が行われました。

提案では、「円滑なIANA機能の維持」「番号資源に関わるIANA機能についてのICANNとNRO（Number Resource Organization）間の役割・責務の明文化」の2点に重点を絞った内容となっています。提案の背景やその内容について、すべてを紹介することが

※1 日本インターネットガバナンス会議（IGCJ）
https://www.nic.ad.jp/ja/governance/igconf/

※2 IP-USERS メーリングリスト
https://www.nic.ad.jp/ja/profile/ml.html#ipusers

できませんが、APNICのブログ※3に詳細が掲載されていますので、そちらをご覧ください。

カンファレンス期間中には、APNICが主催するものとしては、会議に参加して直接議論できる唯一の機会として、IANA機能の監督権限移管に関する理解を深め、この提案について議論を行うことを目的としたセッションも設けられました。

セッションでは、提案内容が一通り説明された後、議論に移りました。提案内容に踏み込んだコメントや提案への反対意見はなく、原案通りの内容で他の地域インターネットレジストリ（Regional Internet Registry; RIR）に提示することとなりました。なお、2014年12月の各RIRでの提案取りまとめまで、まだ時間は残っていますので、会場での議論は終了しましたが、カンファレンス後も専用のML※4を利用して、議論を継続していくことになりました。

その他のインターネットガバナンス関連の特徴的な動向としては、これまでインターネット業界、インターネットに関連するコミュニティや、政府関係者などで構成されていたPPAC（Public Policy Advisory Committee）によるセッションの再検討が行われたことが挙げられます。

これまでのPPACの参加者にとらわれず、さまざまな関係者を巻き込んだ議論の場とすることを目的として、Cooperation SIGを立ち上げることがAPNIC事務局から発表されました。Cooperation SIGでは、公共政策、ネットワークセキュリティの規制、WHOISのプライバシー等について議論が行われる予定です。

◆ ポリシー提案について

今回のカンファレンスでのポリシー提案は、藤崎智宏氏（日本電信電話株式会社）による、「申請に応じたIPv6デフォルト割り振りサイズの拡張提案」の、1件のみでした。

この提案では、申請者が割り振りを受けるIPv6アドレスの用途を明確にすれば、追加の確認なしに/29（/32を8個分）を上限として割り振りを受けることを可能とする、という内容です。英語での記述となりますが、提案の詳細については、次のWebページをご覧ください。

・prop-111
申請に応じたIPv6デフォルト割り振りサイズの拡張提案（藤崎智宏氏）
http://www.apnic.net/policy/proposals/prop-111

当日の議論では、APNICの審議担当マネージャーから、拡張した割り振りを認める基準が明確ではなく、申請処理に支障を来すのではないかという懸念が示されました。また、IPv6の逆引きでは、/32、/28、/24という単位でゾーンが委任されますが、IPv6の逆引きをできるだけ容易に運用できるよう、割り振りの最大サイズを/29ではなく/28とした方が良いのではないか、というコメントも会場の参加者から出ていました。

前回のカンファレンスから引き続き議論されているこの提案は、残念ながら、今回もコンセンサスに至りませんでした。MLや当日の議論を踏まえて、提案者の藤崎氏より、提案を取り下げとする旨の報告がありました。

◆ コンセンサス確認の方法について

APNICカンファレンスでは、ストリーミングやチャットのサービスが提供されており、直接会場まで出向かなくても、当日の議論に参加することが可能です。しかし、参加者への意思確認は挙手に限られているため、会場以外からの参加者は意思確認に参加できない、という状況になっています。

前回カンファレンスの際に、会場以外からの参加者も意思を表明できるようなシステムを試作することが、APNIC事務局から発表されていました。今回のカンファレンスでは、先ほどご紹介したポリシー提案での議論の際に、試作されたシステムを利用して、会場、会場外を問わずに参加者の意思確認が行われていました。

試作されたシステムは現在も公開されており、次のURLから利用可能です。

・CONFER（CONsensus FEedback in Realtime）
http://confer.apnic.net/consensus/index.jsp

ただし、コンセンサスに至ったかどうかの判断はシステムのみではなく、議論の内容も踏まえて、ポリシーSIGのチェアが行うことになっています。このシステムによる意思表明の結果は、議論の内容と同じく、参考情報として利用されるのみとなっていました。チャットでもコメントを述べることができるような仕組みになっており、リアルタイムに経過が表示されるため、これから意思表明を行おうとする人に影響を与えてしまうのではないか、システムを利用する際の本人確認はどうやって行うかなど、利用者からのコメントが多く寄せられており、本格的に利用するためには、まだまだ解決すべき問題は多いように感じました。

また、こういったシステムの利用にとどまらず、いろいろな背景を持った多くの人が、今後の議論に参加するための方法を考える時期に差しかかっているのではないかとも感じました。

※3 IANA session @ APNIC 38: a discussion proposal（APNIC blog）
http://blog.apnic.net/2014/09/08/iana-session-apnic-38-a-discussion-proposal/

※4 IANAxfer mailing list
http://mailman.apnic.net/mailman/listinfo/IANAxfer

◆ NRO NCの選挙とポリシーSIGのCo-Chair選挙について

今回のカンファレンスでは、RIR全体として外部組織との調整が必要な場合に、全RIRを代表する組織であるNRO（Number Resource Organization）の、アジア太平洋地域を代表するNC（Number Council）の選挙が行われました。

・NRO NC Elections
http://conference.apnic.net/38/elections

現職でインド出身のNaresh Ajiwani氏に代わり、同じくインド出身のAjay Kumar氏が選出されました。2015年1月1日（木）から2016年12月31日（土）まで、グローバルIPアドレスポリシーの施行にあたり、ICANN理事会に勧告を行う役割を担います。

また、ポリシーSIGではCo-Chairの選挙が行われ、現職の山西正人氏が再選されました。今回のカンファレンス直後に、ChairのAndy Linton氏が退任を表明しChairが空席となったため、山西氏は次回カンファレンスまでChair代行を務めることも発表されています。

◆ 次回以降のAPNICカンファレンスについて

APNIC 39カンファレンスは、APRICOT 2015と共催で、2015年2月24日（火）～3月6日（金）に福岡市で開催されました。京都市で開催されたAPRICOT 2005/APNIC 19カンファレンス以来、10年ぶりの日本で開催となりました。このAPNIC 39カンファレンスの概要は、P.17の「『APRICOT-APAN 2015 福岡会合』のご紹介」でも取り上げていますが、詳細は次号にてご報告する予定です。

また、APNIC 40カンファレンス（2015年8～9月頃開催予定）はインドネシア・ジャカルタ、APNIC 41カンファレンス（2016年2～3月頃開催予定）はニュージーランド・オークランド、APNIC 42カンファレンス（2016年8～9月頃開催予定）はバングラデシュ・ダッカでの開催を予定している旨も、併せて発表されています。

（JPNIC IP事業部 川端宏生）

● Opening Ceremony and Keynotesの様子

各RIRにおける逆引きDNSSECの動向報告

筆者は、JPNICにてIPアドレスおよび逆引きDNSの登録管理システムを運用しているため、参加していた各地域の技術者とその方面の意見交換をしましたが、各地域にて逆引きDNSをFTP（File Transfer Protocol）やメールサービスの運用に活用している事例について、話をうかがうことができました。また、今回のAPNIC 38においては逆引きDNSに関する取り組みについて、APNIC技術チームともさまざまな意見交換を実施しました。本稿では、これらの情報の詳細についてご紹介します。

◆ 各RIRにおける逆引きDNSSECの導入状況

国際的な逆引きDNSSEC（Domain Name System Security Extensions）の導入状況を把握するため、世界を五つの地域に分け、それぞれの地域でIPアドレスの割り当て業務を行う組織である地域インターネットレジストリ（Regional Internet Registry; RIR）において、逆引きのDNSにどのくらいDNSSECが導入されているのか、状況を確認しました。

現在、RIRはAPNIC（Asia Pacific Network Information Centre）、ARIN（American Registry for Internet Numbers）、RIPE NCC（Réseaux IP Européens Network Coordination Centre）、LACNIC（The Latin American and Caribbean IP address Regional Registry）、AFRINIC（African Network Information Centre）の五つがあり、すべてのRIRで逆引きDNSSECの登録サービスが提供されています。

APNIC、ARIN、RIPEの3組織では、当日の逆引きDNSのゾーン情報が公開されており、該当3組織についてはそちらを元に状況を確認し、必要に応じて問い合わせを行いました。

APNIC、ARIN、RIPE管理のネームサーバにおけるゾーン情報
APNIC：ftp://ftp.apnic.net/public/zones/
ARIN　：ftp://ftp.arin.net/pub/zones/
RIPE　：ftp://ftp.ripe.net/pub/zones

具体的には、DNSSECの仕組み上、あるゾーンに対してDNSSECを有効にする場合、親ゾーンに対して、子ゾーンの公開鍵から

計算されたDS（Delegation Signer）レコードを登録する※1のですが、各RIRの管理するネームサーバに、どのくらいDSレコードが存在するのか調査を行いました。

なおDNSの運用上は、冗長性のために一つのゾーンに、複数のネームサーバおよび複数のDSレコードを登録することができるのですが、今回の調査においては、あるゾーンに対して一つ以上のDSレコードが登録されているものがあった場合、1件としてカウントを行いました。

例：APNICのゾーン（28.12.202.in-addr.arpa.）の場合	
28.12.202.in-addr.arpa. NS	cumin.apnic.net.
28.12.202.in-addr.arpa. NS	tinnie.apnic.net.
28.12.202.in-addr.arpa. NS	tinnie.arin.net.
28.12.202.in-addr.arpa. DS	38468 5 1（ 0D9C9BFFBBD1BF43022BA374B2CE623470B33565 ）
28.12.202.in-addr.arpa. DS	38468 5 2（ 85AA2B48F1C2B7556337FF019EC1C420F699599E310FE619E1D7BD78F3209189 ）

この場合、28.12.202.in-addr.arpa. というゾーンに対して、三つのネームサーバ、二つのDSレコードが登録されていますが、このゾーンについては、DNSSECが有効になっているゾーンが1件ある、としてカウントしました。

なおAFRINICにおいては、逆引きDNSSECの利用状況について、公開されている情報はあったのですが※2、APNIC 38ミーティングの時点では公開情報が最新のものではなかったので、個別に照会しました。LACNICは、他のRIRのようにはDNSSEC適用ゾーンの情報を公開しておらず、こちらも個別に問い合わせました。

◆ 各RIRにおける逆引きDNSSECの登録状況

このように調べた結果、APNICの場合は405,818のゾーンに対して、それぞれDSレコードが一つ以上登録されているものが184件、ARINの場合は486,403のゾーンに対して457件、RIPEの場合は667,460のゾーンに対して1,254件、AFRINICの場合は28,188のゾーンに対して20件のDSレコードがある、ということがわかりました。LACNICについては件数の分母が不明であるものの、およそ4～5個のゾーンでDNSSECが有効になっている旨の回答がありました。

また、組織数単位についても可能な範囲で確認したところ、APNICの管理下では16組織が逆引きDNSSECを登録しており、ARINの管理下では91の組織が登録しているということでした。RIPEについては確認できなかったため、組織数単位での登録数は不明です。

なお、1ゾーンあたりどのくらいの数のDSレコードの登録があるのかについても、可能な範囲で確認しました。DSレコードは冗長性のため複数登録することが想定されており、同じ鍵についても、ダイジェストを生成する方式についてSHA-1かSHA-256かの二つの方式があります。

APNICの個別のゾーンを確認したところ、APNIC管理下では最大で二つのDSレコードが登録されており、それぞれダイジェストの型において、SHA-1かSHA-256かが異なっていることがわかりました。また、AFRINICにおいては、多い場合は1ゾーンに四つのDSレコードが登録されている傾向があり、四つの内訳としては、二つの異なる鍵について、それぞれ二つのダイジェストの型で登録されているようでした。

◆ DNSSECの検証を有効にしたクエリの統計

APNICに、その他DNSSECに関する統計調査を実施しているか確認したところ、以前から継続して調査を実施しており、対外的に発表することもあるとのことでした。ちょうどAPNIC 38でのAPOPS（Asia Pacific OperatorS Forum）で、Geoff Huston氏が関連の発表※3を実施しており、それによると、APNICの調査対象のサーバに対して、11.5%のクライアントがDNSSECの検証を有効にして、DNSのクエリを送信している統計があるとの共有がありました。

◆ 逆引きDNSSEC登録におけるJPNICおよびAPNICのシステムの連携方式

また、JPNIC管理下におけるIPアドレスの逆引きについて、DNSSECを有効化する場合のJPNICおよびAPNICのシステムの連携方式も、詳細を確認しました。JPNIC管理下のIPアドレスには、(1) APNICのネームサーバがゾーンの委任を行っているものと、(2) JPNICのネームサーバがゾーンの委任を行っているものという、2種類のゾーンがあるのですが、(1) の場合については、ユーザーから登録申請のあったDSレコードを、そのままJPNICがAPNIC連携用のシステムに渡せば、APNICのネームサーバにて署名をすることが可能であることを確認しました。なお、(2) の場合については、JPNICのネームサーバ上で署名を行う必要があるのですが、こちらは別途、実装の方式を検討しています。

これらの検討の状況等につきましては、適宜、皆さまとも共有していきたいと考えています。

（JPNIC 技術部 澁谷晃）

※1 インターネット10分講座「DNSSEC」
https://www.nic.ad.jp/ja/newsletter/No43/0800.html

※2 AFRINICのDNSSECに関する統計
http://www.afrinic.net/en/initiatives/dnssec/dnssec-stats
（注:本稿執筆時点では、2014年9月16日のデータとして公開されている統計があり、筆者からの照会と前後して更新されたものと思われます）

※3 Geoff Huston（APNIC） - DNSSEC validation: What if everyone did it?
https://conference.apnic.net/data/38/2014-09-16-dns-measure_1410315749.pdf

RPKIの動向

本稿では、APNIC 38カンファレンスへの参加を通じて把握することができた、アジア太平洋地域におけるリソースPKI（Resource Public-Key Infrastructure; RPKI）提供の状況についてご報告します。

◆ RPKIとは

RPKI※1は、インターネットのルーティングセキュリティ技術で、IPアドレスの記載された電子証明書（以下、リソース証明書）と、AS番号が記載されたROA（Route Origin Authorization）と呼ばれる電子署名の付いたデータを使って、不正な経路情報を検出できる技術です。

このRPKIは、JPNICとインターネットマルチフィード株式会社により、2014年10月1日から試験提供が開始された「ROAパブリックキャッシュ情報の配信」においても用いられています。BGP（Border Gateway Protocol）ルータの運用者は、ROAキャッシュサーバに蓄積されているROAを参照することにより、誤った経路情報を自動で判別できるようになります。ROAとRPKIを利用した経路制御の導入が進められることにより、誤った経路情報からインターネットをより強固に守ることができるようになると考えられています。

◆ NIRにおけるRPKIへの取り組み状況

APNICでは、APNICから直接IPアドレスの分配を受けているAPNICメンバーに対して、既にリソース証明書が発行できるようになっています。IPアドレスに関するWeb申請システムである"MyAPNIC"では、IPアドレスの分配を受けたAPNICメンバーがWeb上でROAを作成する機能の他に、ROAの作成などを自組織のサーバで行うことができる下位認証局を接続する機能も提供されています。※2

一方、国別インターネットレジストリ（National Internet Registry; NIR）からIPアドレスの割り振りを受けている、アジア太平洋地域のISP事業者は、リソース証明書の発行を受けることはまだできません。RPKIは技術的に、IPアドレスやAS番号の分配を行うレジストリが、分配先に対してリソース証明書を発行する必要があるからです。NIRの中で、JPNICも含め、RPKIのサービスを提供しているところはまだありません。

APNIC 38の期間中に情報交換を通じて見えてきたことは、CNNIC（China Internet Network Information Center）やVNNIC（Vietnam Internet Network Information Center）、IRINN（Indian Registry for Internet Names and Numbers）は、RPKIに関心を示してはいるものの、まだ実験提供には至っておらず、KRNIC（Korea Network Information Center）やTWNIC（Taiwan Network Information Center）は、実験的な提供を通じて動向を把握している状態だということです。

KRNICは、前々回のAPNIC 36カンファレンスのNIR SIGで、RPKI実験環境を整えたことを発表していましたが※3、"本番提供にはまだ遠い"というのが担当者の見解でした。

◆ JPNICにおけるRPKIへの取り組み状況の報告

JPNICからは、NIRのミーティングであるNIR SIGと、NIRのホストマスターの会合であるNIRホスト・マスターで、RPKIシステムの開発状況を報告しました。JPNICで取り組んでいる開発の特徴は、以下の3点です。

1. RPKI Toolsの日本語対応（多言語対応）
2. Web申請システムとRPKIシステムの認証連携
3. レジストリデータベースとRPKIシステムのデータ連携

RPKIの適用箇所として、ルートサーバが有効かどうかという質問が挙がった他、後日に「言語の種類が多いアジア太平洋地域における、RPKIの導入に資する開発であり、RPKI Toolsにフィードバックすべきだ」といったコメントをいただきました。

◇ IPアドレスの移転とRPKIの業務手順

今後、異なるNIR間でもIPアドレスの移転が行われる可能性があることを考えると、RPKIを提供するNIRにおいては、IPアドレスやAS番号の移転に技術的に対応できるようにしておくことが必要になってくると考えられます。RPKIの仕様策定を行っているIETF SIDR（Secure Inter-Domain Routing）WGでは、移転の際に、どのような手順でリソース証明書を更新していくべきかの議論が行われています。この議論では、移転手続きの途中においても、アドレスが証明された状態を途切れさせないようにすることが前提となっています。

しかし、移転時にリソース証明書をどのように扱うのかという、業務手順はまだ整理されておらず、筆者とAPNICのRPKI担当者とでも相談を行っています。アジア太平洋地域にはNIRが存在するため、RIRのみの場合よりも手順が複雑になることが

※1 リソースPKI（RPKI）
https://www.nic.ad.jp/ja/rpki/

※2 Resource Certification - Guide to Resource Certification in MyAPNIC
http://www.apnic.net/__data/assets/pdf_file/0015/52602/ResCertGuide.pdf

※3 JPNICニュースレター No.55「APNIC 36カンファレンス報告 - RPKIの動向報告」
https://www.nic.ad.jp/ja/newsletter/No55/0692.html

想定されます。

大まかなアドレスの移転とリソース証明書更新の手順は、以下のようになると考えられています。

1. 当事者間での移転の合意
2. 移転先のリソース証明書の再発行（移転後のアドレスを含める）
3. 移転元のリソース証明書の再発行（移転前のアドレスを削除する）

2と3の期間中、同じIPアドレスが二つのリソース証明書に記載された状態になるのが特徴です。これによって、移転するIPアドレスの有効性を保ち、リソースPKIが使われたBGPルーティングに影響が出ないようにできると考えられています。

もう一つの検討課題として考えられていることは、移転の業務手順です。移転がAPNICメンバーと、NIRの下に存在するLIR（Local Internet Registry、JPNICの場合はIPアドレス管理指定事業者など）との間で行われる場合には、2の前や3の後に、NIRのリソース証明書を再発行する手順が入ってきます。証明書の再発行と共にタイミングを合わせるために、APNICやNIR同士の連絡が重要になってくるかもしれません。

今後、アドレスポリシーの上で移転を行うことができるNIRと情報交換を行って、実施可能で証明書の利用者が困らないような業務手順を探っていく必要があると考えられます。

（JPNIC 技術部／インターネット推進部 木村泰司）

● NIR SIGでは、筆者からJPNICにおけるRPKIに関する活動を紹介しました

ARIN 34ミーティング報告

2014年10月9日（木）と10日（金）の2日間、米国のメリーランド州ボルチモアにて、ARIN 34ミーティングが開催されました。本稿では、このミーティングの模様をご紹介します。

◆ 今回のARINミーティング

今回のARIN（American Registry for Internet Numbers）会議は、秋に開催される会議の通例として、NANOG（The North American Network Operators' Group）ミーティングとの併催でした。今回は、アドレスポリシーに関する議論に加え、IANA（Internet Assigned Numbers Authority）機能の監督権限移管に向けた、ARIN地域としての提案に関する議論が行われたことが、大きな特徴です。

P.2からの特集1で詳しく取り上げていますが、「番号資源」に関わる監督権限移管の提案は、各地域インターネットレジストリ（RIR; Regional Internet Registry）で議論された提案をグローバルに一つにまとめたものを、2015年1月に提出することが求められています。すなわち、APNIC（Asia Pacific Network Information Centre）地域で議論した内容が他のRIR地域と異なる場合は、APNIC地域内での再調整が必要となります。そこで筆者は、ARIN 34の1ヶ月前に、APNIC 38にてAPNIC地域として議論した移管提案と比較する視点で、本会議におけるARIN地域の議論に着目していました。

アドレスポリシーについては、10点の提案が議論された中、「日本も含めたAPNIC地域でも検討すべきか」という視点で着目しておきたい議論としては、「IPv4アドレス移転要件の見直し」と「ARIN地域外でのIPv4の利用」の2点が挙げられます。

特に前者の「IPv4アドレス移転要件の見直し」は、アドレスの必要性を確認する要件を緩和する方向に進めるものであり、これまでのARINコミュニティの姿勢と大きく異なります。APNIC地域における要件も、これに合わせて見直すべきかということを検討するための材料として、今後も注視すべきかと思います。

今回の報告では、IANA機能の監督権限移管の議論も含めた、これら3点に絞ってご報告します。

◆ IPv4アドレス移転要件の見直し

今回の会議では、移転するIPv4アドレスに対して、移転先での必要性を確認した上で、移転を承認する要件を緩和する方向に議論が進められていました。これは、数年前にARIN地域で移転ポリシーを施行した際に、必要性の確認を行わないことが投機目的のアドレス売買につながると消極的であった、当時のARIN地域の姿勢と比べると、かなり大きな変化が見て取れます。

◇ 会場の反応
今回の会議では、移転アドレスの必要性を確認する要件の緩和を求める提案が、複数提出されていました。提案内容からはその背景は明らかではありませんが、移転が想定に基づくものであった移転ポリシー施行時とは異なり、IPv4アドレスの在庫枯渇が進み、実際に移転が行われている現状においては、要件を緩和した方が実態に合っていると考える人が増えてきているようにも思えます。そうは言っても、全体としては、慎重派の意見が目立ち、一度にすべてのサイズの移転において要件を撤廃するのではなく、小さなサイズから要件緩和をして様子を見ようとする意見が表明されていました。

結果として、今回の会議では合意に至らずに、継続議論となりましたが、要件緩和自体に懸念を示す意見は少なく、必要性の確認対象とすべき移転サイズについて意見が分かれたことが、コンセンサスとならなかった主な要因と言えそうです。

◇ APNIC地域からの視点
APNIC地域では、ポリシー施行当初は、需要確認の要件がなかったものの、ARIN地域とのRIR間移転を実現するために、需要確認の要件を追加した経緯があります。

これを踏まえて、今後ARIN地域の要件が緩和された場合、APNIC地域としては「ARINに合わせて要件緩和をしたい」のか、「現状の要件を残す」のか、コミュニティの意思と方針を整理していく必要性が出てきます。

◆ ARIN地域外でのアドレスの利用

「ARIN地域外でのアドレスの利用」は文字通り、ARINから分配を受けたIPv4アドレスの、ARIN地域外での利用を認めることを、ポリシー上、明確にすることを求めたものです。この提案も、IPv4アドレス在庫枯渇に伴い、実体化している課題への対応を目指しています。ただし、ARINから分配を受けたアドレスの一部は、ARIN地域内で利用することが前提となります。

◇ 解決したい課題
・現在のアドレスポリシーでは、ARINから分配を受けたIPv4アドレスの利用をARIN地域内に限定するべきか、他の地域でも利用できるのか、明確ではない
・一方、他のRIR地域での在庫枯渇が進む中、複数のRIR地域に拠点を持つ企業からは、ARINから分配を受けたアドレスを、他の地域でも利用できるようにしたいとのニーズも確認されている

◇ 会場の反応
会場では、Microsoft社やGoogle社などの企業の参加者から、「既にそういう使い方をしている」との意見が複数表明されました。一方、FBI（米国連邦捜査局）などの法執行機関からの参加者は、アドレス利用者の実態がつかめなくなり、連絡が取れなくなるとして懸念を示しており、継続議論となりました。

◇ APNIC地域からの視点
APNIC地域内でも、このようなケースは考えられると同時に、申請者が所在地外のRIRを自由に選択できると解釈する余地を与えかねない、といったことなども考えられることから、どこまでをアドレスポリシーで明文化するべきか、バランスを踏まえて考慮することが大切なように思います。

◆ IANA機能の監督権限移管に向けた議論

2014年9月に開催されたAPNIC地域でのAPNIC 38での議論に続き、ARIN 34では、ARIN地域としての提案策定に向けた議論を行いました。

◇ 今回の議論とARIN地域の現状
会議では、提案すべき内容に踏み込んだ議論は行わず、背景と現状の報告、ARIN地域としての提案策定に向けたプロセス案を紹介し、プロセスとして適切であるかについて議論を行いました。ARIN地域では、IANA機能の現状と今後に関する調査を実施し、コミュニティの意向を確認した上で、提案の策定を進めるとし、ARIN 34の後に、実施した調査の結果が公開されています。

IANA Stewardship Transition - ARIN Community Input
https://www.arin.net/participate/governance/iana_survey.pdf

◇ 他のRIRとの比較
他のRIR地域では、調査という形を取らず、具体的な提案をもとに各コミュニティの意思確認が進められています。なお、ARIN地域における調査結果の中で、印象に残ったものとしては、NTIAに代わりIANA機能の監督を行う第三者機関の設立を支持する意見が、過半数となっていた点でした。これは、APNIC地域で議論した提案には含まれていない要素です。

◇ 今後
この調査結果を踏まえて、ARIN地域として、どういう提案を策定するのか検討が行われます。その後全RIR地域における議論を経て、CRISP（The Consolidated RIR IANA Stewardship Proposal）Teamが各RIRコミュニティの意向を尊重しながら内容をすり

合わせ、番号資源として一つの提案にまとめられます。

◆ ARIN 34とNANOG 62に参加して

ARINは、オペレーターによる議論の参加も促進しており、NANOG会議のセッションの中で、ARIN 34で議論するアドレスポリシー提案を、NANOGの参加者と議論する形式をとっています。NANOG 62では、それ以外にも、政策に関わるテーマを扱ったプログラムとして、ネット中立性へのFCC（米国連邦通信委員会）法案検討に向けたFCC担当者による発表や、ICANN会議へオペレーターの参加を呼びかけるセッションなど、「運用」を軸としながらも、技術的な枠にとらわれない内容が見受けられました。

一方、NANOGが終わりARIN会議が始まると、約3分の2の参加者が去る現状を目の当たりにすると、もともと政策的な話に興味がある人以外に、ポリシー策定に関わってもらおうとすることは、なかなかのチャレンジであることが感じ取れます。

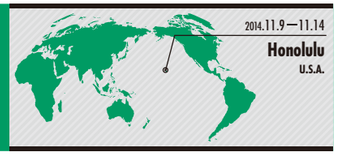
ARIN会議単体で見た場合、APNIC地域と比較するとポリシー提案の数も多く、提案への議論が活発に行われていますが、参加者の1人が「数は多いが、特筆すべき議論は、移転における必要性確認要件の撤廃に関する議論くらい」との感想を述べていたことも印象的で、議論が活発なのがよいと一概には言えないのかもしれません。

参考：
・ARIN 34ミーティングプログラム
https://www.arin.net/participate/meetings/reports/ARIN_34/ppm.html

・ARIN地域における提案一覧
https://www.arin.net/policy/proposals/

（JPNIC インターネット推進部/IP事業部 奥谷泉）

第91回IETF報告



全体会議報告

第91回IETF Meetingは、2014年11月9日（日）から11月14日（金）の間、ハワイのホノルルにあるヒルトン・ハワイアン・ビレッジにて、米シスコ・システムズ社のホストで開催されました。本稿では、そのレポートをご紹介します。

◆ はじめに

ちょうど四半世紀ぶりに、第15回IETF以来のIETF Meetingがハワイにて開催されました。ハワイは、イーサネットの礎と言えるALOHAnet発祥の地で、インターネット史において大変縁のある場所で、IETF Meetingも比較的早期にこの地で開催されていました。1989年当時のIETF Tシャツには、1987年に上映された映画「Revenge of the Nerds 2」の副題「Nerds in Paradise」の文字がプリントされていたそうです。このTシャツは数あるIETF Tシャツの中でもコアなファンがいる大変人気の1枚のようで、なんと今回は公式IETF Tシャツとは別に、一部の有志によって当時と同様のピンクのボディに「Nerds in Paradise 2.0」の文字をプリントし、現代版としてアレンジを加えて、もう一つの公式IETF Tシャツとして復刻されました。

先に「もう一つのTシャツ」を取り上げてしまいましたが、今回の公式IETF Tシャツは米シスコ・システムズ社のロゴが入ったIETFオリジナルデザインのアロハシャツでした。意図して作られたものであるかは定かではありませんが、服好きの著者としては、米シスコ・システムズ社のアロハシャツとはずいぶんこちらも洒落を効かせた一着だなぁと思わず感心してしまいました。というのも、会場となったヒルトン・ハワイアン・ビレッジの敷地内のビーチの名前にもなっていたハワイの英雄デューク・カハナモク、彼がデザインしたアロハシャツを販売していた企業の一つが、今は無きシスコ・カジュアルズ社なのです。彼の名を冠したアロハシャツは、アカデミー賞にて数々の賞を獲得した映画「地上より永遠に」の劇中で、主演のモンゴメリー・クリフトをはじめとする出演者等が着用し注目を集め、それまでローカルな位置づけであったハワイアンファッションを米国本土ではやらせるきっかけとなった歴史的なブランドです。そんな現在においてもヴィンテージとして大変人気が高い、伝説的なブランドを持つアロハシャツメーカーと同名の「シスコ社」がアロハシャツを作った!という、こちらもまた歴史的な一着でした。

さて、ここからは11月12日（水）に開かれた「IETF Operation and Administration Plenary」と、11月10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

11月12日（水）の「IETF Operation and Administration Plenary」では、ホストのシスコ社の挨拶から始まり、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、IESG（Internet Engineering Steering Group）オープンマイクという流れで議事進行されました。

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91回の参加者は、50の国と地域から1,080人の参加となり、前回の1,175人から95人ほど減少しています。また、昨年の同時期にバンクーバーにて開催された第88回の1,189人や、その他1,200人前後で推移してきた近年の参加者数と比較すると100名程度減ったことがわかります。新規参加者は136人と、全体の1割強は新規参加者で、新しい層の取り込みは継続的に進んでいるようです。国別の参加者数は、1位米国、2位中国、3位日本、4位カナダとなっており、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おりました。また、近年中国からの参加者の増加に伴い、ビザの発行に関する諸問題が増えてきており、IETFとしても改善に向けた検討が続けられるとの報告がありました。

続いて、今年の9月および10月に試験的に行われた、IESGのテレチャットを公開する取り組みについて報告がありました。この取り組みは、IESGの公平性を保つことを目的として、IETF参加者もオブザーバーとしてテレチャットに参加できるように実施したとのことでした。また、今後も知見の収集のためにテレチャットの公開を継続するとの報告がありました。

また、2015年夏頃を目処に現在ある八つの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））の再編をIESGが進めているとの報告がありました。このエリア再編の目的には、新たなWGのサポート体制の整備や、エリアディレクターの人数の調整などがあげられました。また一方で、IESGでは、この再編に伴い影響を受ける可能性のあるAPPエリアやRAIエリアについては、エリアを統合するなどして今後も応用分野に関する活動を継続していくことを検討していると報告がありました。

今回のRecognitionでは、中南米からのIETFへの参加者増加に貢献したAlvaro Retana氏、IETF Datatrackerの改善に貢献したLars Eggert氏、20年以上にわたりインターネットおよびIETFに貢献してきたBert Wijnen氏等3名が紹介されました。また、Bert Wijnen氏は、スピーチの際に氏の十八番であるオランダ語による歌を披露し、参加者から拍手喝采を浴びていました。

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。今回の会議の収支決済速報では、参加者数は予測の1,200人より少なく、参加費およびスポンサー費の合計は150,000ドルの赤字であることが報告されました。そのため、今回のBits-N-Bitesもスケジュールされないことがあらためて伝えられました。一方で、トロントで行われた、第90回の収支決算の最終報告では、参加者数は予測を超え、参加費およびスポンサー費ともに収支見通しを上回り、192,349ドルの収益があったとのことでした。また、これまでのIETF継続に伴う純利益は640,000ドルとなったとのことでした。

IETFチェアレポートでも触れられた、ビザの発行に関する諸問題についての今後の対策については、検討を続けるとともに、必要な参加者へ会議参加を証明するための招待状を発行するなどの方針について報告がありました。また、IAOCではこの問題に対して十分な理解があるため、問題が生じた際はぜひ連絡を取ってほしいと述べられていました。

また、第95回IETF Meetingおよび第98回IETF Meetingの開催地が決定したとの報告がありました。第95回はIETF史上初となる南米で、アルゼンチン・ブエノスアイレスにて開催されることが決まりました。また第98回は、カナダ・モントリオールにて開催されることが決まりました。

最後に、各スポンサーの紹介がありました。ホストのシスコ社の他に、Welcome ReceptionをスポンサーしたNBCユニバーサル社、回線提供をしたタイム・ワーナー・ケーブル社、そして、休憩時の飲食物を提供した各社が紹介されました。会期初日の日曜日に開催されたWelcome Receptionでは、スポンサーがNBCユニバーサル社であったこともあり、参加者にはミニオンのぬいぐるみが配られ、一部の参加者は至る所（自室やビーチ、ターミナルルームなど）で、このミニオンを撮影し、参加者のメーリングリストに投稿することが会期中はもとより会期後もしばらくはやっておりました。


● IETF Operation and Administration Plenaryの様子

◆ Technical Plenary

11月10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、ITU（International Telecommunication Union）Plenipotentiary Conferenceの報告、IABに関する問題の報告が二つ、IABオープンマイクという流れで議事進行がされました。

はじめにIABチェアのRuss Housley氏より、第90回IETF Meetingからのハイライトについて紹介がありました。まず、IRTFチェアにLars Eggert氏が、ISE（Independent Submission Editor）にNevil Brownlee氏が、それぞれ再任したことが紹介されました。続いて、IABが執筆したRFCとして、RFC7322「RFC Style Guide」が発行されたことが紹介されました。最後に、2015年のICANN NomComメンバーとして、John Levine氏が選ばれたことが紹介されました。

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、八つあるResearch Group（RG）のうち、以下の四つのRGでした。

- Software-Defined Networking（SDNRG）
- Information-Centric Networking（ICNRG）
- Internet Congestion Control（ICCRG）
- Network Management（NMRG）

また、提案中のRGとして、Datacenter Latency Control（DCLCRG）およびNetwork Function Virtualization（NFVRG）がありました。第90回以降にIRTF関係として発行されたRFCは、今回はないとのことでした。

最後に、Applied Networking Research Prizeの紹介がされました。2014年は過去最多となる46人の推薦者の中から、Sharon Goldberg氏、Misbah Uddin氏、Tobias Flach氏、Robert Lychev氏、Kenny Paterson氏、Keith Winstein氏の6名が受賞しました。

RSE・RSOCチェアからの報告では、Heather Flanagan氏より、RFC formatの改訂作業の進捗としてdraft-flanagan-rfc-frameworkの紹介があり、新たなRFC formatの作業は順調に進んでいる旨の報告がありました。また、その機能として、図表の挿入をできるようにするとの紹介があり、猫の絵を例にあげて、従来のASCIIアートによる表現からSVGファイルによる表現が可能となる点を紹介し、参加者にこの機能を使ってみたいか問いかけがあり、多くの参加者が挙手をしていました。

Sally Wentworth氏からは、ITU Plenipotentiary Conferenceについて報告がありました。これは、ITUの最高意思決定機関として4年に1度開催されます。2014年は開催年にあたり、10月20日から11月7日の期間に開催されました。インターネット関連の議論ではITUがスコープとする、プライバシーや監視、人権、インターネットガバナンスとそれに関する政策などの諸問題を中心に話し合いがされましたが、これらインターネットの運用に関する諸問題についてはITUの条約やその定義の変更、範囲の拡大には至らなかったとの報告がありました。また、この結論は投票ではなく、参加者の合意形成により導かれたとのことでした。

IABに関する問題として、以下の二つについて報告がありました。

・IP Stack Evolution
Joe Hildebrand氏より、IPv4とIPv6が共存し進化し続ける今日において、このような共存環境がトランスポート層において、さまざまな影響を引き起こす可能性について説明がありました。そして、この問題に関連するWGとしてTransport Services（TAPS）WG、TCP Increased Security（TCPINC）WG、Advanced Queue Management（AQM）WGやその他のAPPエリアの紹介がありました。また、2015年の1月26日から27日の期間でIAB Workshop on Stack Evolution in a Middlebox Internet（SEMI）を行い、その結果を次回IETF Meetingにて発表するとの報告がありました。

・Privacy and Security
Ted Hardie氏より、プライバシーとセキュリティに関する諸問題について、現在IABではInternet Scale Resilience、Confidentiality、Trustの三つのエリアに分類を行ったところで、今後この三つのエリアごとにプライバシーとセキュリティに関する諸問題について取り組んでいくと説明がありました。

（青山学院大学 情報メディアセンター 根本貴弘）

IPv6関連WG報告

本稿では、第91回IETFにおけるIPv6関連のWGについて、6man WG、v6ops WG、6lo WG、Homenet WGの議論を中心に報告します。

◆ 6man WG（IPv6 Maintenance, Int Area）

6man WGのワーキンググループでは、IPv6プロトコルの基本仕様そのものについてのメンテナンス（見直しや拡張）を議論しています。

ワーキンググループ文書として議論進行中のもの（Working Group Draft）のうち、二つに関して取り上げられました。すでにこのWGで取り上げられている個人文書（Individual Draft）七つについて継続議論があり、今回初めて投稿された文書（new Individual Draft）五つについての発表が予定されていましたが、Atomic Fragmentやv6GEOといった最初の提案で時間がかかってしまい、新しく投稿された5文書については、時間切れで議論されませんでした。

本稿では、議論のあった中からいくつかを取り上げます。なお、今回問題提起された、個人文書の一つ「Deprecating the Generation of IPv6 Atomic Fragments」が会期後、WGドキュメントに「昇格」しました。

1. Efficient ND Design Team報告
前々回のミーティングでも議論された「Efficient ND」は、第89回IETF報告で「無線LAN環境での近隣探索プロトコル（ND）の問題についての議論」として解説された問題点※の改善策を検討するものです。今回、デザインチームが発足し、まとまった報告がされました。

プロトコルに手を入れるにしろ、環境にあったオプションの運用を提示するにしろ、まずは問題分析をきちんとするところから出発しているようです。そのため、このデザインチームのカバー範囲は、近隣探索プロトコルのトラフィック計測から機能ごとの問題分析、問題改善として使えそうなテクニックやオプションの検討と広範囲になっています。6man WG単体ではなく、v6ops WGと共同での検討事項となっています。

問題フィールド特定のための計測結果は、マルチキャスト通信の影響やバッテリへのインパクトについてまとめた二つの文書として書き起こされています。

- draft-vyncke-6man-mcast-not-efficient
- draft-desmouceaux-ipv6-mcast-wifi-powerusage

また、重複検出（DAD）については、別の文書に課題整理がされています。

- draft-yourtchenko-6man-dad-issues

マルチキャストのRS（ルータ探索）と定期的なRA（ルータ広告）、リンクアドレス解決のためのNS（近隣者発見）とNA（近隣者要請）、DAD、Wi-Fiと携帯電話網の混在環境、軽量端末などの端末側のパケット送出特性、mDNS（マルチキャストDNS）のトラフィックボリュームなどが改善対象として選ばれていました。デザインチームからは、主にRS/RAとDADの改良点として、RAの送出に関してタイマーを設けて間隔を長くできるようにすることや、RAにリフレッシュオプションを設けること、DADに関しては手動設定の場合にのみ実施することやさらに手を加える道など四つのアプローチが提示され、議論がされました。レビュー対象の文書は、次の三つとなっています。

- draft-yourtchenko-6man-dad-issues
- draft-krishnan-6man-maxra
- draft-nordmark-6man-rs-refresh

参加者からはデザインチームの活動報告に賛同するコメントが得られ、引き続きデザインチームによる検討が継続されます。

2. Recommendation on Stable IPv6 Interface Identifiers（draft-ietf-6man-default-iids）
セキュリティとプライバシーへの配慮のため、MACアドレス由来のインタフェースID（IID）からRFC7217で定義されている隠ぺいされたIIDの適用を促す文書です。これが必須のものとして採用されると、主にIPv6をトンネルで運搬する技術の実装に影響が出ます。セキュリティとプライバシーは守るべきですが、運用上は特定ができると都合が良い場合もあるなど、柔軟性を求める声もあり慎重な議論がされていました。これも継続議論となっています。

余談ですが、この議論の途中で使われた“ambiguous”という単語がなぜかはやり出し、IPv6系の人が集まるWGやBoFのそこかしこで使われていました。

3. Deprecating the Generation of IPv6 Atomic Fragments（draft-gont-6man-deprecate-atomfrag-generation）
IPv4ノードとIPv6ノードがSIIT（Stateless IP/ICMP Translation Algorithm）を使って通信している際の、IPv6のAtomic Fragmentについてです。問題指摘と廃止の提案については、現状の運用観測に基づいたものですが、実装側や運用を正すべきであるといった意見や、Atomic Fragmentを必要とするMANET（Mobile Ad hoc NETwork）の例などがあげられ、簡単に廃止できるものではないことから、コンセンサスには至らず、継続議論となりました。

4. Including Geolocation Information in IPv6 Packet Headers（IPv6 GEO）（draft-skeen-6man-ipv6geo）
データリンクに使われるプロトコルは多種多様で、必ずしも位置情報を含むように作られていませんが、その上位レイヤのIPは共通利用されています。そこで、IPv6ヘッダに位置情報を含めるようにしようという提案です。位置情報についてもプライバシーへの配慮が必要であるため、これを利用する際には暗号化を必須とするべきであるといった意見が寄せられ、この提案も継続議論となっています。

※ JPNICニュースレター No.57「第89回IETF報告 IPv6関連WG報告」
https://www.nic.ad.jp/ja/newsletter/No57/0650.html

◆ v6ops WG（IPv6 Operations、OPs & Mgmt Area）

v6ops WGでは、文字通り、IPv6ネットワークの運用管理に関する事項やIPv4ネットワークへの導入、共存技術など幅広い事項を扱っています。今回も午前と午後に二つのセッション枠が確保され、6to4の廃止、ULAの利用考察、マルチプリフィクスの運用ガイド、拡張ヘッダの利用状況調査、DNS64/NAT64環境で利便性を高めるための専用TLDの提案など、さまざまな提案や報告がされました。

なかでも、6to4プロトコルの廃止については、運用被害を防ぐ方向で議論が白熱しています。運用サイドの意見を取り入れるため、チェアからNANOGなどの運用者向けメーリングリストにも議事録が共有され、意見が募られました。

1. Deprecating Connection of IPv6 Domains via IPv4 Clouds（6to4）（draft-ietf-v6ops-6to4-to-historic）

IPv4上でIPv6の通信を行えるようにする6to4技術について、そろそろ役目を終えて廃止にする時期なのではという提案です。Windows OSなどで参照されるアドレスポリシーテーブルでも、Teredoには規定があるが6to4はなくなっているという指摘を受けて、Teredoも廃止してもいいのではという意見も出たりしていました。

アドレスポリシーテーブルでは、6to4はNativeのIPv6より優先度を下げるといった評価のための参照がされているため、テーブルから削除すると問題が起きるだろうという指摘や、6to4のために予約されているアドレス（192.88.99.0/24）をフィルタすれば廃止と同じ意味合いとなるといった意見があり、

（1）6to4の廃止
（2）RFC3068（6to4リレールータのためのエニーキャストプリフィクス）をhistoricステータスにする
（3）192.88.99.0/24をフィルタする

という三つの内容に分割して、それぞれ議論することになりました。

2. IPv6 Extension Headers in the Real World（draft-gont-v6ops-ipv6-ehs-in-real-world）

IPv6の拡張ヘッダは、フィルタされて運用に支障をきたす場合が見られます。SI6 Tool Kitの作者である本文書の筆者は、このツールを用いてパブリックなインターネットにおけるIPv6拡張ヘッダの扱い、フィルタ状況について調査を実施し、まとめました。拡張ヘッダの種類ごとの状況はなかなか興味深いものがあります。調査方法とその結果について、質疑がたくさんありました。

最終的には、実装と運用のガイドとなる文書作成をめざしているようですが、ガイドラインの作成には、実装に関する部分があたかも第2の拡張ヘッダの提案をしているように見受けられる部分があるなど問題があるため、待ったがかけられ、調査結果部分を一つの文書として分離してまとめることになりました。

ICMPv6の安易なフィルタも同様ですが、フィルタすることによってブラックホールとなるといった、どういう問題が起きるかを本文書で確認しておくと、健全な運用のイメージがわいて良いのではないかと思います。

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

IPv4とIPv6のdual-stackネットワークやIPv6 onlyのネットワーク構築時の、「デザインチョイス」についてのガイドライン文書です。外部接続や経路制御の手法選択がメインであるため、現在のもっと広範な設計を予想させるようなタイトルから、範囲を絞ったもっとわかりやすいタイトルに変更した方がいいという指摘が出ていました。

その一方で、DHCPやSLAAC（StateLess Address AutoConfiguration）など内部の運用術に関して扱った方が良いという「広範」をめざすべきという意見も出ていました。また、いずれにしてもセキュリティに関してはしっかり書いておくべきだろうといった意見もあり、引き続き内容を厚くしていくことになりました。

4. A Special Purpose TLD to resolve IPv4 Address Literal on DNS64/NAT64 environments（draft-osamu-v6ops-ipv4-literal-in-url）

DNS64/NAT64を運用している環境で、IPv6端末がIPv4のみのアプリケーションサーバに明示的にアクセスする場合のURLとして、「.v4」をTLDとして指定するとIPv6アドレスにIPv4アドレスをマッピングする仕組みの提案が継続議論されています。

この仕組みの有用性は多くの参加者から賛同されているようでしたが、新しいTLDを作ることに難色を示す人が多かったように思われます。代わりに、「v4only.arpa」はどうかといった提示もされていました。また、DNSSECやcookieがうまく動作しないのでは、ということも指摘されていました。指摘事項に関して文書を更新するとともに、DNSOPSでも議論するということになりました。

今回の私の参加目的として、v6opsでの発表というのがありました。15分ほど時間をもらえ、国内で実施している中小規模の組織向けルータのIPv6に関するセキュリティテストについて報告をしました。"Introducing IPv6 vulnerability test program in Japan, <draft-jpcert-ipv6vullnerability-check>"という文書名で公開されていますので、ぜひご一読いただき、コメントをいただければと思います。

◆ 6lo WG（IPv6 over Networks of Resource-constrained Nodes WG）

6lo WGでは、省電力で低電力な軽量端末が接続されるIPv6ネットワークの技術について議論をしています。

IoTという言葉の盛り上がりも見られる中、粛々と軽量クライアントのための近隣探索や、おサイフケータイなどでも使われているNFC上のIPv6パケットの転送技術などが話し合われています。こちらでも、RFC7217ベースのインタフェースIDの利用に関する議論がされました。

"IPv6 mapping to non-IP protocols"については、6man WGのチェアとも相談するようにという指示が出ていました。

◆ Homenet WG（Home Networking WG）

Homenet WGでは、最近の多種多様なデバイスとそれが属する多様な通信網を念頭においた家庭内ネットワークの接続手法や、管理手法が議論されています。

1. Routing
2. Addressing / Configuration
3. Naming
4. Service Discovery
5. Security / Border Discovery

のカテゴリが提示されており、これに従って議論が開始されましたが、最初のルーティングに関する議論だけでほぼ一つのセッション枠を使い切ってしまう事態になり、急遽空いている部屋を探して、別の日にも議論がされました。家庭内のデバイス管理のために、.homeというTLDを使う提案などもされていました。


● 初心者からの質問を受け付けることのできる言語を示すための缶バッジ

IPv6のプロトコルを基盤とした次の展開に向けた議論が多数行われていることを、あらためて感じたIETF91のオンサイトミーティングでした。

（株式会社インテック　廣海緑里）

セキュリティ関連WG報告

近年、IETFにおけるセキュリティ関連のWGは、分野が多岐にわたっています。本稿では、セキュリティエリアのWGと、セキュリティエリアの総括が行われる会合であるSAAG（Security Area Advisory Group）ミーティングから、いくつかの話題をピックアップして報告したいと思います。

◆ Transport Layer Security（TLS）v1.3の議論

TLS WGでは、SSL/TLSの次のバージョンである1.3の策定に向けて、検討が活発に行われています。前回の第90回IETFミーティングに続いて、今回もミーティング期間以外に開催されるInterim（中間）ミーティングが開かれていました。

TLS 1.3に関しては、TLSの通信を始める前の、暗号アルゴリズムを選択したり暗号化に使う鍵を決めたりする重要なやり取りである「ハンドシェイク」に議論が集まっています。v1.3のハンドシェイクの案に対して、ハンドシェイク中にやり取りされるメッセージそのものを暗号化したり、メッセージの改ざんを検知するのに役立つ電子署名を加えたりする案が挙げられています。WGミーティングでは、ハンドシェイクが通信の安全性を大きく左右するため、拙速にコンセンサスを取るのではなく、慎重に議論を進めることになりました。

またハンドシェイクを簡素化し、オーバーヘッドを少なくする0-RTTと呼ばれる方式も提案されています。議論されているハンドシェイクの候補は、次の資料で見ることができます。

TLS 1.3のハンドシェイク候補の議論に使われたスライド
http://www.ietf.org/proceedings/91/slides/slides-91-tls-2.pdf

なおSSL/TLSの圧縮機能は、BEAST（Browser Exploit Against SSL/TLS）やCRIME（Compression Ratio Info-Leak Made Easy/Compression Ratio Info-Leak Mass Exploitation）といった攻撃手法が生まれたことを背景として、TLS 1.3では盛り込まれないことになっています。

◆ I2NSF（Interface to Network Security Functions）BoF

I2NSFは、ファイアウォールやユーザー認証サーバといったネットワークセキュリティ機能を、ネットワークの仮想化機能VNF（Virtualized Network Functions）の環境内や、ホスティングの環境において、設置したり設定したりすることができるプロトコル、そしてデータモデルを検討するグループです。第91回ミーティングで1回目のBoFが開かれました。

本グループの設立に向けた意図をまとめたInternet-Draftによ

ると、近年におけるネットワーク仮想化技術の発展に伴って、以下のようなニーズが高まっているとしています。

- 複数の拠点に分かれた企業のネットワークのために必要最小限のネットワークセキュリティ機能を運用する
- クラウド型のデータセンターで稼動させながら、クライアントにネットワークセキュリティ機能を提供する
- 多数のサイトやユーザー、もしくは低電力のセンサーネットワークに対して一貫したセキュリティポリシーを適用する

これらに対して、本グループでは、仮想化環境で稼動するセキュリティ機能を"仮想ネットワークセキュリティ機能" - Virtual Security Functionと呼んで、クラウド型のデータセンターでの提供や従来の機器との共存がしやすいように標準化することを目標としています。

Interface to Network Security Functions Problem Statement
https://tools.ietf.org/html/draft-dunbar-i2nsf-problem-statement-01

I2NSF BoFには80名ほどが集まりました。IETFで行われる1回目のBoFとしては人数は多くない方ですが、アジェンダやプレゼンテーションの内容は、ある程度練られたもので、アイデア段階で開かれるBoFとは様子が違っていました。このBoFでは、WG化に向けて趣意書を作成するためというよりは、取り組む課題を明確化するために議論されていました。

本グループのInternet-Draftには、課題の明文化の他に、データセンターなどを挙げて利用ケースを説明したものがあります。まだWGではありませんが、次のページが設けられ、まとめられています。

Interface to Network Security Functions（i2nsf） - Documents
https://datatracker.ietf.org/wg/i2nsf/documents/

◆ BGPSEC – Origin ValidationとPath Validationの分離

SIDR WGは、PKI技術を使ったBGPルーティングのセキュリティの仕組みを検討しているWGです。大きな動きとして二つ挙げられます。

一つはBGPSEC（Border Gateway Protocol Security Extension）において、Origin Validation（経路情報のAS番号を確認する方式）とPath Validation（経路情報のASパス情報を確認する方式）が独立した扱いになったことです。これまではPath Validationが行われる際には、必ずOrigin Validationが行われるという位置づけでした。今後、RPKIキャッシュやBGPルータの実装において、おのおのが独立してvalid（有効である）やinvalid（無効である）という扱いに変わってくると考えられます。

もう一つは、リソース証明書やROA（Route Origin Authorization）といったデータファイルの取得に使われていたrsyncに代わるプロトコルが、本格的に検討されていることです。第91回IETFミーティング期間中に、複数のプロトタイプの実装同士を突き合わせる作業も行われていた模様です。このプロトコルは、RPKI Repository（またはRetrieval） Delta Protocol - RRDPと呼ばれています。まだ個人ドラフトですが、rsyncは処理が重く、またRTT（往復遅延時間）の大きい環境で伝送効率が下がることが分かっていることから、注目されています。

RPKI Repository Delta Protocol（Internet-Draft）
https://tools.ietf.org/html/draft-tbruijnzeels-sidr-delta-protocol

SIDR WGでは、ルーティング技術者の観点でBGPSECに関する意見収集を行う目的で、Inter-Domain Routing（IDR） WGとの合同でミーティングが開かれました。第91回IETFミーティング期間中に行われた合同ミーティングでは、BGPSECの仕組みに関する質疑応答を通じて理解が深められた様子です。長いASパスが不正に生成されることによってコンバージェンスの時間が長くなり、ルーティングに支障が出るような行為ができてしまうのではないかといった、運用の観点ならではの意見交換も行われています。

この他に、RPKIの認証局によるROAの失効に気付けるような新たな署名付きオブジェクトの提案や、不正な証明書を見つけやすくするためのCertificate Transparencyに似たアイデアが提案されていました。これらを含めて、RPKIについて活発に研究が行われている、ボストン大学の研究グループによる論文が次のURLで公開されています。

Hardening the RPKI Against Faulty or Misbehaving Authorities, BUSEC: Boston University Security Group
http://www.cs.bu.edu/~goldbe/papers/RPKImanip.html


● 今回のSIDR WGのミーティングは、IDR WGとの合同開催でした

◇ ◇ ◇

第88回IETFミーティング以降、大規模な通信傍受（pervasive monitoring）への対策として、さまざまなWGで通信プロトコルに暗号化機能を持たせることが検討されています。第90回IETFミーティングで初めてWGの会合が開かれたTCPINC（TCP Increased Security） WGでは、インターネットのほとんどの通信で使われているプロトコルであるTCP（Transport Control Protocol）に、認証なしの暗号化機能を持たせることが検討されています。

TCP Increased Security（tcpinc）
https://datatracker.ietf.org/wg/tcpinc/charter/

2014年11月14日には、IAB（Internet Architecture Board）から「インターネットの機密性に関する声明」が出されました。通信相手の認証を行わなくても、通信を暗号化することは大規模な通信傍受に対して有効であり、プロトコルの検討の際には、基本的な考え方として暗号化の機能を盛り込むことが推奨される、としています。

IAB Statement on Internet Confidentiality
https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/

インターネットプロトコル（IP） が生まれて以降、インターネットにおけるプロトコルには「シンプルさ」が求められてきたと言えますが、社会情勢に応じて、変化が起きているように感じられます。

（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、第91回IETFミーティングにおけるDNS関連のWGのうち、特に動きのあったものとして、dnsop WG、dprive WG、dnssd WGの概要を報告します。dprive WGについては、今回初めて取り上げています。

◆ dnsop WG（Domain Name System Operations WG）

第91回IETFにおいては、火曜日に2時間の枠において、dnsop WGの会合が開催されました。今回の会合では、複数の議題が予定されており、時間内にて議論が行われましたが、特に興味深かったのが、DNSトランスポートをTCPで行うことに関する議論でした。

まず、チェアから現状のWGドラフトに関する確認が行われました。その後、DNS Cookiesに関する発表が行われました。以前から提案されていたドラフトであり、Webの場合と同様に、DNSサーバとクライアントの間においてもCookieと呼ばれる固有のトークン値を提供しようとするものです。実際には、以前にメッセージを交換したDNSサーバやクライアントのCookiesを記憶しておくことで、なりすましや外部からの攻撃を判別しやすくするという手法です。BIND 9.10.1b1に試験的に実装されたことが報告され、WGドラフトとして採用してもいいのでは、といった議論がなされました。

次に、QNAME minimisationに関する発表が行われました。これは、ある名前を解決する場合に、DNSサーバへの問い合わせの回数を減らすことで、どのような名前を引いたかということを推測しにくくし、プライバシーを強化しようという提案です。DNSサーバが担当するZoneの切れ目を学習することで、余分な問い合わせを減らすという手法が用いられています。この提案に関しては、まだWGドラフトになったばかりであり、引き続きレビューを行うことが確認されました。

続いて、DNS Transport over TCPに関する議論が行われました。発表においては、現在のDNSサーバの実装と、TCP Fast Openを用いたDNS問い合わせクエリに関する実装例が紹介されました。TCPにて問い合わせを行うことの利点と欠点が議論され、TCPで行うことの可能性について議論が行われました。WGドラフトとして、引き続き議論を行うことが確認されました。

また、IPv6の逆引きゾーンに関するドラフトである、draft-howard-dnsop-ip6rdns、ならびに新たな提案であるdraft-wkumari-dnsop-root-loopbackに関する発表も行われました。前者は、逆引きによるホストの認証や、メールサーバの認証を行っている運用手法に対して、IPv6の逆引きが適切な名前で設定されていることを期待しないよう指摘するガイドラインをめざした文書です。後者は、Root DNSの仕組みに関する新たな提案で、リゾルバDNSサーバにRoot Zoneのコピーを持たせることで、Root DNSサーバへの無駄な問い合わせを減らすという手法の提案です。新たな提案であるため、その目的や概要等が説明され、また議論されました。このRoot DNSに関する新たな提案に関しては、


● 第91回IETFの会場となったHilton Hawaiian Village

その後、香港にてワークショップが開催される旨がアナウンスされました。このワークショップはdnsop WGとは独立して行われたものでしたが、この提案と、もう一つの別のRoot DNSに関連する提案を中心に、次世代のRoot DNSの構造に関するワークショップが開催されました。dnsop WGとしては、引き続き議論を行っていくのではないかと思われます。

◆ dprive WG（DNS PRIVate Exchange WG）

dprive WGは、クライアントとDNSサーバの間の名前解決における、プライバシー問題を解決するために設立されたWGです。

（1）draft-hallambaker-privatedns
（2）draft-hzhwm-dprive-start-tls-for-dns
（3）draft-hoffman-dprive-dns-tls-alpn
（4）draft-hoffman-dprive-dns-tls-https
（5）draft-hoffman-dprive-dns-tls-newport

といったI-Dが取り上げられ、議論が行われました。具体的には、クライアントとリゾルバDNSサーバの間の通信を、何かしらの方法を用いて暗号化することを目標としています。

（1）draft-hallambaker-privatednsは、DNSトランスポートプロトコルとして、よりセキュリティに優れた仕組みを提案しているドラフトです。JSONベースのJCX（JSON Service Connect）プロトコルを用いて、DNSクライアントとリゾルバサーバ、ならびにDNSサーバ間の通信を行うという手法です。当然、従来のDNSトランスポートプロトコルとは大きな違いがあるため、どのような用途に適しているのか、またどう実現するのかといった説明や議論が行われました。

次に、（2）draft-hzhwm-dprive-start-tls-for-dnsに関する発表がありました。このドラフトは、TLSを用いてDNSトランスポートを暗号化し、その性能劣化を最小限にする方法を議論したものです。EDNS0のフラグとしてTLS OK（TO）ビットを用意し、TOビットが有効なクライアントとDNSサーバ間においてTLSを用いた通信を行います。また、TCPとTLSを用いることによる性能劣化を防ぐために、通常のTCPによるDNS問い合わせにSTARTTLSを用いてTLSを追加し、さらにTLS接続を継続して使いまわすという手法を提案しています。この点に関して、遅延の増加傾向やDNSサーバのCPU負荷の変化傾向等、数値的な評価も発表されました。さらに、試験的な実装も公開されています。

最後に、（3）draft-hoffman-dprive-dns-tls-alpn、（4）draft-hoffman-dprive-dns-tls-https、（5）draft-hoffman-dprive-dns-tls-newportに関する発表がありました。これらは、それぞれ別の手法にてDNSトランスポートにセキュリティを導入するための手法を提案しているものです。draft-hoffman-dprive-dns-tls-alpnは、TLS ALPN（Application Layer Protocol Negotiation）を用いてDNSトランスポートの暗号化方式を決定する手法を提案しています。draft-hoffman-dprive-dns-tls-httpsは、DNSの問い合わせや応答のトランザクションを、HTTPのURIフォーマットに変換して行うことを提案したものです。最後に、draft-hoffman-dprive-dns-tls-newportは、DNSクライアントとDNSリゾルバサーバの間でTLSを用いたDNSトランスポート通信を用いる場合に、ポート番号を443ではない別のポート番号を用いることを提案するものです。これを実現するための手法がいくつか提起され、議論が行われました。

dprive WGはまだ議論が開始されたばかりであり、今後も引き続いてDNSトランスポートのプライバシー問題解決に向けた議論が行われると思います。

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

dnssd WGでは、まずDNS Long-Lived Queriesに関する発表が行われました。これはDNSを利用したサービス発見において、DNSサーバとの通信を状態管理することで、新たなサービス追加や削除などのイベントを管理できるようにする手法を提案したものです。この機能はすでにMac OS XのBonjour等に実装されており、dnssd WGでは、DoSに対する懸念点や、トランスポートプロトコルのTCPへの変更や、TLSの利用などが議論されました。TCPへの変更に関して、引き続き議論が行われる様子です。

次に、draft-rafiee-dnssd-mdns-threatmodel-01に関する発表がありました。このドラフトは、DNSSDによってローカルネットワークを越えてサービス通知が行われるにあたって、ネットワークの内部情報が漏れたり、名前の衝突が発生したり、なりすましが行われたりするような、DNSSDにおける脅威について分析したものです。会場の議論では、同じような脅威は別のプロトコルにも存在するため、よりDNSSDに特化した脅威について明確にすべき、といった意見が出ました。引き続き議論が行われます。

さらに、draft-cheshire-homenet-dot-homeに関する発表が行われました。これは、.homeという特殊なトップレベルドメインを、家庭内部のデバイス管理に利用するという提案です。会場では、.localドメインとの違いや利用方法の差異、dnsop WGやhomenet WGとの連携に関する議論が行われました。

また、draft-ietf-dnssd-hybrid-00に関する発表と議論も行われました。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。新たにWG draftして発行され、WGラストコールに向けて改訂を進めることが確認されました。

（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）