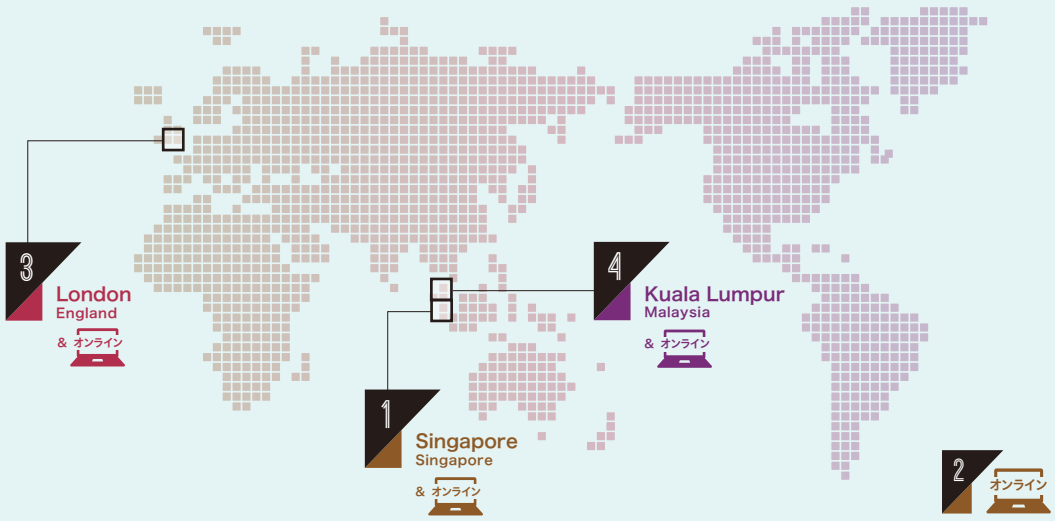
インターネット動向紹介

INTERNET TRENDS INTRODUCTION 2022.09 ― 2023.01



IPアドレストピック

INTERNET TRENDS INTRODUCTION

1 2022. 9.8 ▸ 9.15 シンガポール APNIC 54カンファレンス オンライン

2 2022. 12.2 第43回JPNIC オープンポリシーミーティング オンライン

IPアドレスに関する動向として、2022年9月上旬から中旬にかけて行われたAPNIC 54カンファレンス、2022年12月2日にオンラインで行われた第43回JPNICオープンポリシーミーティングの様子を中心に取り上げます。

APNIC 54カンファレンスの動向

■ APNIC 54カンファレンスの概要

APNIC 54カンファレンス（以下、APNIC 54）が2022年9月8日（木）～9月15日（木）にかけて、シンガポールにて開催されました。今回は、2020年2月にオーストラリア・メルボルンで開催されたAPRICOT 2020/APNIC 49カンファレンス以来となるオンサイト開催となりました。また、Asia Pacific Regional Internet Governance Forum（APrIGF）、Asia Pacific School on Internet Governance（APSIG）、Singapore Network Operators' Group（SGNOG）等のイベントと共同開催となりました。ただし、いまだコロナ禍において渡航困難な参加者がいることが考慮され、オンラインでの参加ツール（Zoom、YouTube Live）も用意されました。

9月8日（木）～9月11日（日）の間は、ネットワーク管理や監視、SDN、IPv6などをテーマとしたワークショップが行われ、9月12日（月）～9月15日（木）は議論の場となるカンファレンスセッションが行われました。

カンファレンスセッションでは、従来と同じく、アドレスポリシーやルーティングセキュリティ、NIR（National Internet Registry; 国別インターネットレジストリ）、ソーシャルな課題など特定分野に関心を持つ人達で議論が行われる「SIG（Special Interest Group）」、カンファレンスの総括および全体報告が行われる「AMM（APNIC Member Meeting）」、その他各種技術に関する講演等が行われました。

会期中のセッションについては、動画、資料および発言録がWebで公開されています。もし興味のある内容がありましたらぜひご確認ください。

APNIC 54プログラム
https://conference.apnic.net/54/program/schedule/

ここでは、APNIC 54で行われたアドレスポリシーに関する議論の動向をご紹介します。

APNICカンファレンスでも、オンサイトでの賑わいが戻ってきました

■ アドレスポリシーに関する議論の動向

今回のAPNIC 54では4件の提案が行われました。最近のAPNICカンファレンスではオンラインでおよそ120名がポリシーSIGに参加していましたが、今回のポリシーSIGではオンラインだけで250名ほど、オンサイトも合わせると300名近くが参加していました。コンセンサス形成のための意思表示方法としては、オンサイトの参加者は挙手で行い、オンラインの参加者はZoom PollとConfer（https://confer.apnic.net）を利用する形式でした。これら3種類の投票の結果をチェアが吟味して、判断が行われました。

提　案　名	ポリシー文書における用語定義の集約・統一（提案番号：prop-145）
提　案　者	Anupam Agrawal氏
概　　要	現在有効なドキュメントで、ドキュメントごとに行われている用語定義を集約する。
議 論 結 果	コンセンサス
提案の詳細	https://www.apnic.net/community/policy/proposals/prop-145/

現在のAPNICのドキュメントでは、ドキュメントごとに用語定義が行われています。ドキュメント間の相互参照関係は正しく規定されておらず、片方のみ参照関係が示されているものが多々存在しています。例として「エンドサイト」という用語は、APNIC-127（APNIC Internet Number Resource Policies; ポリシー文書）とAPNIC-114（APNIC guidelines for IPv6 allocation and assignment requests; IPv6ガイドライン）で用語定義がされており、APNIC-114ではAPNIC-127の参照関係が明記されているものの、APNIC-127側ではその参照関係が明記されていません。このような曖昧な参照関係からあらぬ誤解や、間違った解釈を引き起こさないために、これらの用語定義を集約し、一つのドキュメントにしようというのが本提案となります。

APNICには既に用語定義を行うドキュメントとして、APNIC-080（APNIC Definition Document）が存在しています。今回の提案ではこのAPNIC-080にまとめる形で記載すると提案されました。

現在のドキュメント内容から意味的な変更は無く、より簡潔で明確な文章となるものであることから、反対意見は出ず、賛成多数でコンセンサスに至りました。

提　案　名	見出しとコンテンツの整合性確保（提案番号：prop-146）
提　案　者	Anupam Agrawal氏
概　　要	ポリシー文書における各項のタイトルを、以下の通り変更する。 3.1.4 “No Guarantee of contiguous delegation(連続した委譲の非保証)” ↓ “Contiguous Delegation(連続した委譲)” 3.1.6 “Conflict of Goals(目標の相反)” ↓ “Balancing the goals(目標のバランス)”
議 論 結 果	コンセンサス
提案の詳細	https://www.apnic.net/community/policy/proposals/prop-146/

ポリシー文書の3.1項では、番号資源管理における「APNICの目標」を示しています。そのうちの3.1.4項では、割り振り/割り当て先組織への連続した委譲に関して、最大限に努めることを記載しています。一方、3.1.4項のタイトルは「連続した委譲の非保証」となっており、ネガティブに捉えると、APNICは連続した委譲に関して何も努力をしないような、相反するタイトルに見えてしまいます。また、3.1.8項では、申請者とコミュニティ全体とのニーズについて、バランス調整を図る役割を記載していますが、タイトルは“Conflict of Goals（目標の相反）”となっており、内容とかみ合っていないように見えます。

本提案で提案者は3.1.4項のタイトルを“Contiguous Delegation（連続した委譲）”、3.1.8項を“Balancing the goals（目標のバランス）”と変え、実際の認識に近いタイトルに変更しようという提案でした。

当日の議論やメーリングリストの中では、わざわざ変更しなくても意味が通じるのではないかと考える人たちも多くいました。一方で、理解を示す人も一定数いたので、最終投票は積極的に変更したい賛成派と、積極的に変える必要は無いという中立派に分かれました。投票結果としては中立派が半分近くを占めましたが、チェアの判断により、コンセンサスが宣言されました。

提　案　名	歴史的PIアドレスの管理方法について（提案番号：prop-147）
提　案　者	Jordi Palet Martinez氏、Anupam Agrawal氏
概　　要	ポリシー文書の4.2.1項"未使用の歴史的リソースの回収"を削除、新たに4.3"歴史的リソースの管理"を追加し、以下のようにする。 元の保有者である組織が手続きを踏まない場合、2023年1月1日以降対象のアドレスをAPNIC Whoisデータベースから削除し、予約済みアドレスとして扱われる。この後1年間は、元の保有者は手続きを踏むことでリソースを取り戻すことができる。1年が経過したリソースに関しては、再利用可能なアドレスプールへ移り、再びメンバーへの委任が可能となる。
議 論 結 果	コンセンサスに至らず
提案の詳細	https://www.apnic.net/community/policy/proposals/prop-147/

APNICでは、2005年に実装されたprop-017（未使用アドレススペースの回収）を受け、使用されていない歴史的PIアドレスの回収に取り組んでいます。データベースに存在するコンタクト先はもちろんのこと、コミュニティから入手した連絡先を含め、さまざまな手法でコンタクトを図ってきました。そして、APNIC EC（理事会）は、2022年12月末日までに手続きが完了しない組織に関して、対象のアドレスを未割り当てアドレスとして扱う旨を決定しました。これは歴史的PIアドレスホルダーがAPNICと何らかの形で契約を持つことにより、RPKI等のAPNICのサービスを享受できるようになり、インターネット全体の保全を図ることを目的としています。

APNIC事務局は、コンタクト結果としていくつかのデータを提示しましたが、ルーティングテーブル上で確認できる885プリフィクスのうち、コンタクトに反応が無い組織が600近くに及んでおり、こんな状態でこの提案を実施すれば大きな混乱を招くのではないか、取り組み自体は理解できるが、早ければ2024年には再利用されることになるの

で、時期尚早ではないかといった懸念が挙げられました。

参加者の多くも意図として理解しているだけに、反対票は多くありませんでしたが、中立が多くを占め、提案はコンセンサスには至らず、一度提案者に返されることになりました。

なお、本提案の対象はAPNICから直接割り当てられている歴史的PIアドレスです。JPNIC管理下で各組織に割り当てられている歴史的PIアドレスは、既に割り当て先組織の明確化が完了しているため、このたびの対象には含まれません。

提　案　名	IPアドレスのリース禁止（提案番号：prop-148）
提　案　者	Jordi Palet Martinez氏、Amrita Choudhury氏、Fernando Frediani氏
概　　要	以下項目をポリシーに追加する。 5.8項 "インターネット番号リソースのリース" ・いかなるIPアドレスリースを認めないことを明記する。 ・APNIC事務局はそれらのケースを調査し、フォームやメール等による通報体制の整備を行う。 ・違反が確認できた場合は、アドレス委任の失効を行う。
議 論 結 果	コンセンサスに至らず
提案の詳細	https://www.apnic.net/community/policy/proposals/prop-148/

本提案はリース禁止を明記することを主題とした提案でした。APNICおよびJPNICでは、ポリシー文書において、メンバー（≒JPNICの指定事業者）のネットワークと接続性の無い割り当てを認めない旨を明記しています。これらは経路集成の観点から悪影響を及ぼすため、認められてきませんでした。しかし昨今では、リース事業者を名乗る組織がいくつか現れています。本提案を実装することで、曖昧さを排除し、リースを無くそうというのが提案者の趣旨でした。

メーリングリストを含め、現地の議論はさまざまな意見が飛び交いました。解釈上これまでも禁止されていた行為を明記するだけなので問題なく、コミュニティへの認知も図れるという賛成派の意見、現行の文書でもリース禁止と読み取れるのであれば変更は不要だろうという反対寄りの意見、同じく反対寄りではあるものの、リース禁止によるエンドユーザーへの影響を懸念する意見、ARIN等ではリースは容認されているとして、そもそも禁止するのは理解できないといった意見が入り乱れる形となりました。また、話者によってリースの定義・認識にズレがあり、そこのすり合わせも含め、もう少し時間が必要なのではないかと感じました。

コンセンサス確認では賛成派4割、反対派5割と意見は分かれたまま、チェアはコンセンサスに至らずと判断しました。次回以降も継続して同様の議論が行われる可能性が高いと見られます。本提案は日本にも影響するものですので、皆さまもぜひ一度考えてみてください。

■ 次回以降のAPNICカンファレンスについて

次回のAPRICOT 2023/APNIC 55は、2023年2月20日（月）～3月2日（木）の日程で、フィリピン・マニラで開催されました。カンファレンスの内容は、次号にてご報告いたします。

次々回となるAPNIC 56では、日本にAPNICカンファレンスがやってくる予定となっています。日本での開催は、2015年の福岡以来となります。APNICカンファレンスに関心のある方はぜひお越しいただければと思います。

誌面では割愛したAPNIC 54の様子について、次のURLをご覧ください。

APNIC 54カンファレンス報告 全体概要およびアドレスポリシー関連報告
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2022/vol1954.html

JPNICの現地参加者によるAPNIC 54のフォトレポートをJPNICブログに掲載しています。次のURLからご覧ください。

APNIC54フォトレポート
https://blog.nic.ad.jp/2022/8010/


他のNIRメンバーとも、久々の交流ができました

第43回JPNICオープンポリシーミーティングの動向

2022年12月2日（金）に、第43回JPNICオープンポリシーミーティング（JPOPM43）が開催されました。

JPOPMは、日本におけるインターネット資源のうちIPアドレス、AS番号等の番号資源の管理ポリシーを検討・調整し、コミュニティにおけるコンセンサスを形成するための議論の場です。JPNICとは独立した組織であるJPOPF運営チーム（JPOPF-ST）が主催し、年2回開催されています。今回も前回に引き続き、新型コロナウイルス感染症（COVID-19）の影響により、リモートのみでの開催となりました。

JPOPMのプログラムは、応募のあったポリシー提案や情報提供のプレゼンテーションを中心に構成されます。JPOPM43では、情報提供が6件ありました。本稿では、一部のプログラムをご紹介します。資料や議事録は、次のWebサイトからご覧ください。

第43回JPNICオープンポリシーミーティング開催のご案内
https://jpopf.net/JPOPM43Program

■ インターネット番号資源ホットトピックス

JPOPF-STの谷崎文義氏から、インターネットに関する話題のうち、主に番号資源やポリシーに関わるものや、その周辺で日本国内だとあまり話題になっていないものを取り上げる、インターネット番号資源ホットトピックスの発表がありました。

今回は、昨今話題になることが多い「IPv4アドレスのリース」を学ぶことができる発表がありました。巷間で行われているIPv4アドレスのリースについて、その可否を議論するために必要な情報として、次の内容が紹介されました。

・APNICやJPNICにおけるポリシーではリースの可否等に関する記述が無いこと
・JPNICの割り当てガイドラインにおいては、割り当て先ネットワークがIPアドレス管理指定事業者のネットワークと接続している必要がある旨の記述があることから、リースは実質禁止されていること
・リース禁止について賛成派や反対派の各意見があることと、各意見の理由
・海外で行われているリースサービスの紹介

発表内容は、JPOPF-STのYouTubeチャンネルでご覧いただけます。

【JPOPM43】インターネット番号資源ホットトピックス(2022／12／2)
https://youtu.be/BpPXRJlicQs

■ JPNICからIPアドレスの割り振りを受けてみた

株式会社KDDIウェブコミュニケーションズの森川慶彦氏から、IPアドレス割り振り・割り当て・移転等の際に、実務で役立つ講演がありました。

JPNICのWeb申請システムにログインする際に躓きやすい資源管理カードの紹介から始まり、割り振り申請方法、割り当て報告申請方法、割り当て審議申請方法、IPv4アドレス移転手続き方法などについて、具体的な申請方法ワンポイントなどが、画面のキャプチャー入りで解説されました。また、2022年8月に、同社がいち早くWHOIS割り当て情報の新[Abuse]欄に情報を登録したことについても、JPNIC WHOISの検索結果を用いて紹介されました。本講演は、JPOPF-STのYouTubeチャンネルでご覧いただけます。

【JPOPM43】JPNICからIPアドレスの割り振りを受けてみた(2022／12／2)
https://youtu.be/pgHWvy717CY

■ 割り当て後のIPアドレスを運用してみた

株式会社インターネットイニシアティブの蓬田裕一氏から、JPNICからIPアドレスの割り振りを受けた後に役立つ講演がありました。

IPアドレス管理指定事業者の運用者が、IPアドレスの割り振りを受けた後に行うべきことは多数あります。お客様への割り当て基準策定およびその基準の運用、IPアドレスの管理、割り当てたIPアドレスのWHOIS登録、RADbやJPIRR等のIRR(Internet Routing Registry)への登録、経路奉行への監視登録、RPKI(Resource Public Key Infrastructure)におけるROA(Route Origin Authorization)の登録、さらに他社が上記各項目を実施することを意識した上での自らのネットワークにおける経路制御など、オペレーターが何を行うべきかを網羅的に学べる内容でした。こちらも、JPOPF-STのYouTubeチャンネルでご覧いただけます。

【JPOPM43】割り当て後のIPアドレスを運用してみた(2022／12／2)
https://youtu.be/99hRsSAtJys

■ 次回JPOPM44の開催について

JPOPM44は、2023年6月～7月頃に開催が予定されています。詳細が決まりましたら、JPOPFのWebページ(http://jpopf.net/)およびIP-USERSメーリングリスト(https://www.nic.ad.jp/ja/profile/ml.html#ipusers)で告知される予定です。

今回誌面で取り上げた内容の他に、JPOPM43の開催報告については、次のURLからご覧ください。

第43回JPNICオープンポリシーミーティング報告
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2022/vol1972.html

動画で分かる！IPアドレス・AS番号管理業務

JPNICでは、IPアドレスやAS番号に関する情報提供として、解説や申請手続き例を動画にまとめる取り組みを進めています。

申請機会が多いものや、動画でご覧いただくことでより理解が深まるものを中心に、随時公開しています。JPNICのWebページにまとめている他、JPNICのYouTubeチャンネルでリスト化していますので、ぜひ参考にしていただければと思います。

動画で分かる！IPアドレス・AS番号管理業務
https://www.nic.ad.jp/ja/ip/shortvideo/

動画で分かる！IPアドレス・AS番号管理業務(JPNICのYouTubeチャンネルでの再生リスト)
https://youtube.com/playlist?list=PLukf915kQpfwW7tg616cmAB0P1vQXgBbJ

IPアドレス・AS番号管理業務を動画で分かりやすく！
https://blog.nic.ad.jp/2023/8512/

技術トピック

INTERNET TRENDS INTRODUCTION

3

2022. 11.5 ▸ 11.11 イギリス／ロンドン IETF 115

オンライン

第115回IETFミーティング（IETF 115）が、2022年11月5日（土）から11日（金）にかけて、イギリス・ロンドンの会場とオンラインでのハイブリッド形式で開催されました。

IETF 115の全体概要

IETF 115は、現地参加者数とリモート登録者数が合計で1,600名を超え、新型コロナウイルス感染拡大の状況が始まる前の水準に戻ってきました。参加者の属する国ごとの参加者数は、米国、イギリス、中国、ドイツ、日本の順に多く、開催地の国が第2位になるなど、現地開催が行われていた頃の様子に近付いています。日本からの参加は10年ほど前よりも低迷していますが、今回は現地参加の人数が増えました。

■ 全体会合（Plenary）より

全体会合ではまずIETFチェアから参加人数などの発表の後、今回や今後のIETFミーティングについて話されます。続いてIABやIRTFのチェアから活動報告や告知が行われます。

IETFミーティングでは毎回新型コロナウイルスの感染例が報告されていて、IETFチェアのラース・エガート（Lars Eggert）氏によるとIETF 115では4例あり、2022年7月のIETF 114は17例、2022年3月のIETF 113は9例とのことでした。IETF 115では、抗原検査キットが無料で配布されており、参加者自身で検査できるようになっていました。

IETF 115のPlenaryの様子は以下で見ることができます。

IETF 115 Plenary
https://youtu.be/UqwL7HBrBiU

■ インターネットの地球環境への影響に関するIABワークショップ

IABチェアのミラ・キューレビント（Mirja Kuhlewind）氏から、2022年12月5日（月）から12日（月）にかけて行われる予定となっていた「インターネットのアプリケーションとシステムの環境への影響ワークショップ（IAB workshop on Environmental Impact of Internet Applications and Systems）」の紹介がありました。ワークショップはポジションペーパーの投稿を受け付け、その内容に応じてグループ分けをして議論が行われます。このワークショップの趣意やアジェンダ、採録されたポジションペーパーは下記のサイトで閲覧できます。

IAB workshop on Environmental Impact of Internet Applications and Systems (eimpactws)
https://datatracker.ietf.org/group/eimpactws/about/

IAB workshop on Environmental Impact of Internet Applications and Systems, 2022
https://www.iab.org/activities/workshops/e-impact/

■ 話題 ―いまのインターネットは何バイトまでのIPv6拡張ヘッダーであればパケットは届くのか―

最後に、IETF 115期間中のミーティングの中から、IPv6に関する話題をお届けします。

IETFミーティングの前に行われるIEPGミーティングで、IPv6拡張ヘッダーに関する調査研究の発表が3件ありました。IPv6拡張ヘッダーは、IPのヘッダーとしてさまざまなものを加えていくことのできるもので、経由ノードを指定するなどいろいろな機能を実現するために利用できる便利なものと言えます。しかし、インターネットにつながるネットワーク機器は、必ずしもIPv6拡張ヘッダーを期待通りに扱えるとは限りません。場合によっては宛先まで届かないことがありえます。果たしてどのような拡張ヘッダーを付与してもそのIPv6のパケットは届くのでしょうか。

一つ目の発表は「インターネットを通るIPv6拡張ヘッダーテストへのディープダイブ」（Deep Dive into IPv6 Extension Header Testing Across the Internet）で、ムンバイとトロントの間でファイル転送を試み、CDNの有無やサーバからのIPv6パケットに拡張ヘッダーが付い

ているかどうかなどが調査されました。IPv6かと思いきやIPv4で通信していた、といった拡張ヘッダー以外の出来事も発表されていました。

Deep Dive into IPv6 Extension Header Testing Across the Internet, Nalini Elkins, Mike Ackermann, Dhruv Dhody, Praneet Kaur, Dr. Mohit Tahiliani, Dr. Priyanka Sinha, Ameya Deshpande, Dr. Ana Custura

https://www.iepg.org/2022-11-06-ietf115/slides-115-iepg-sessa-deep-dive-into-eh-on-the-internet-ana-custura-dhruv-dhody-michael-ackermann-nalini-elkins-00.pdf

二つ目の発表「IPv6拡張ヘッダーの伝送エッジの計測」(IPv6 EH Traversal Edge measurements)と三つ目の発表「もう一つのIPv6拡張ヘッダー計測」(Another IPv6 EH measurement)は、拡張ヘッダーが到達性にどのように影響するかに関する調査結果です。

「IPv6拡張ヘッダーの伝送エッジの計測」では、拡張ヘッダーに付ける宛先オプション(Destination Option)やホップバイホップオプション(Hop-by-Hop Options)を使って拡張ヘッダーのサイズを変化させてパケットを送信し、RIPE Atlasのプローブを使ってドロップされたかどうかを観測しました。その結果、TCPでは40バイト以下、UDPでは48バイト以下であれば届きやすかったようです。

IPv6 EH Traversal Edge measurements, Ana Custura

https://www.iepg.org/2022-11-06-ietf115/slides-115-iepg-sessa-ipv6-eh-traversal-edge-measurements-ana-custura-00.pdf

「もう一つのIPv6拡張ヘッダー計測」はAPNIC Labsで行われたもので、Webブラウザによる不可視のWebデータのダウンロード・コネクションを使って、フラグメンテーションや拡張ヘッダーの付与など複数の要素を元にパケットがドロップする割合を国別に調査しています。ネットワークの形態や使われやすい機器が異なるのか、国ごとに異なる様相が見られます。地図上に表したドロップ率などは、下記の発表資料をご覧いただければと思います。

IPv6 Extension Headers Again!, Geoff Huston, Joao Damas, APNIC Labs

https://www.iepg.org/2022-11-06-ietf115/slides-115-iepg-sessa-ipv6-extension-headers-again-geoff-huston-joao-damas-00.pdf

KDDI総合研究所の仲野有登氏より、セキュリティエリアについてご報告いただきました。

■ CFRG(Crypto Forum)

暗号関係を担当するグループで、4件の発表がありました。2件が共通鍵暗号に関するもの、2件が公開鍵暗号に関するものでした。

○ Encryption algorithm Rocca-S

筆者から、暗号方式Rocca-Sの提案を行いました。鍵回復攻撃・偽造攻撃に対して、256ビットセキュリティを実現した高速暗号であることを発表しました。状態更新をAESのラウンド関数とXORで構成することで高速な処理を実現しており、ソフトウェア実装においてAES-256-GCMの3倍以上高速であることをアピールし、今後の通信速度の向上にも対応可能な方式として普及をめざしていきます。

○ Classification of properties of AEAD modes

AEAD(Authenticated Encryption with Associated Data)の要件整理に関する発表で、CFRGでAEADをどのように扱っていくかについての議論が行われました。AEADは、メッセージの暗号化とメッセージ認証を同時に実現可能な暗号方式で、

- Nonce hiding
- Online
- Nonce misuse resistance
- Key commitment

など、さまざまな性質が検討されています。今後、それぞれに対して、定義、適用先、性質を満たすアルゴリズムを整理していく予定です。

会場からは、非常に有益なドキュメントであり、利用したいとの意見が挙がっていました。チェアからも、Adoption callの提案がありました。

○ BBS Signatures

開示制御が可能で、ゼロ知識証明に対応したBBS署名についての発表でした。

これまで実装があまり示されていなかったため、今回、実装を追加したことが発表されていました。

hash-to-curveを利用することでメッセージ数に上限を設定する必要が生じており、2の48乗となる見込みであることが話されていました。また、課題として、Proofのテストベクトルが挙げられていました。これは、Proofに乱数要素を含むためテストベクトルの生成が難しいという問題で、解決策が募集されていました。

○ The use of NTRU

耐量子暗号として提案されている、NTRUの利用に関する発表でした。

2022年7月に、米国国立標準技術研究所（NIST）が耐量子暗号の米国標準候補としてKyberを選定していますが、Kyberは特許技術であるため、自由に使えないという制限があります。

NISTが権利保有者と交渉を進めていますが、いつ合意に至るかは現時点で不明です。そこで、Kyberと同程度の安全性を保つと考えられている、NTRUを利用することが提案されています。NTRUを選択した理由として、安全性に加えて、処理性能も十分であること、特許は有効期限を迎えており自由に使えるという点が挙げられていました。

■ TLS（Transport Layer Security）

TLSを担当するグループで、5件の発表がありました。そのうち、4件を紹介します。

○ 8446bis

RFC 8446bisの状況報告が行われ、多くの課題を解決したとの報告がありました。残っている課題として、Unsolicited Extensionsなど5件があります。

○ 8447bis

RFC 8447がRFC 8447を廃止することになっており、混乱を招く可能性があるため、更新することが提案されました。この文書はIANA向けの文書なので、IANAにとって扱いやすいように対応するという結論になりました。

もう一つの提案として、この文書中の表で、Recommended欄に新しく"D"を追加することが提案されました。DはSHOULD NOTあるいはMUST NOTを示すことになっていますが、どちらを指すかは文脈で判断することになっています。

○ Obsolete Key Exchange

TLSにおける鍵交換で、RSA方式の非推奨、安全でないFFDHEの制限、などを提案しています。この中で、FFDHEで利用している有限体が安全かどうかをクライアントで検証できないという課題があり、その解決策の議論で先に進めない状態に陥っています。そこで、すべてのFFDHEを非推奨にすること、もしくは有限体に関する要件を設定しないことが提案されています。すべてのFFDHEを非推奨とすることについて投票が実施され、賛成されました。

○ SSLKEYLOGFILE

SSLKEYLOGFILEは、TLSで利用される環境変数で、NSS（Network Security Services）で文書が公開されていますが、RFCとしてきちんと標準化することが提案されました。現時点の内容をRFCとし、IETFで変更を管理することが想定されています。

TLS WGの項目として採用するかどうかについて投票が行われ、賛成多数となりました。この結果を受けて、Adoption callが出されています。

■ SAAG（Security Area Open Meeting）

SAAGは、セキュリティ・プライバシーに関する議論を担当するオープンフォーラムです。今回は4件の発表があり、そのうち3件を紹介します。

○ Implementation report from EDUROAM's adoption of EAP／RADIUS

EDUROAMは、教育機関・研究機関向けに広く利用されているローミングサービスで、学生や研究者向けにインターネットサービスを提供しています。所属組織がIDプロバイダー、訪問先の組織がサービスプロバイダーに相当していて、訪問先の組織に接続しようとした場合に所属組織で認証が行われ、認証に成功すれば接続ができるようになっています。いくつかの課題が紹介されており、安全性に関するものとして、危殆化した技術を使っていることが紹介されていました。運用上の課題として、認証要求処理の効率化、有効期限切れのクレデンシャルを用いた接続要求の対処、などが紹介されていました。

○ Role of formal verification in the standards process

TLS1.3など、Formal verificationによって検証を実施しているが、今後も実施した方がいいのか、実施が必須なのか、などが議論されていました。

- 外部の専門家に依頼する必要があるため専門家との関係構築が重要である
- 攻撃者のモデルや検証の前提条件などがあり、証明が付いているからといってそれが完璧とは限らないことに注意が必要である
- プロトコルに証明を付けるのが必須になるのであれば、プロトコル設計の時からそれを意識して設計する必要がありそう

などの意見が挙がっていました。

○ HTTP message signatures

HTTP WGで検討されている課題についての、共有が行われました。HTTPメッセージの順序が入れ替わった場合でも正しく署名が検証できるよう、署名したデータの順番を平文で検証者に送信し、検証者で元の順番に並び替えを行ってから署名検証を実施することが提案されていました。中間者が署名を追加する場合にも、対応できるように検討されています。これによってサーバ <-> クライアントでメッセージの真正性を確保できるようになっています。セキュリティの専門家に対して、安全性評価と実装の依頼がされていました。

ドメイン名・ガバナンス

INTERNET TRENDS INTRODUCTION

4

2022. 9.17 ▸ 9.22 マレーシア／クアラルンプール 第75回ICANN会議 オンライン

本稿では、2022年9月～2022年12月にかけての、ドメイン名およびインターネットガバナンスに関する動向として、第75回ICANN（The Internet Corporation for Assigned Names and Numbers）会議や日本インターネットガバナンスフォーラム2022の話題をご紹介します。

第75回ICANN会議

第75回ICANN会議（以下、ICANN75）は、2022年9月17日（土）から22日（木）までマレーシア・クアラルンプールで開催され、112の国・地域より1,957名の参加がありました。本稿では、主にプレナリーセッションと、分野別ドメイン名支持組織（Generic Names Supporting Organization, GNSO）に関する動向についてお伝えします。

■ プレナリーセッション

○インターネットの分断、DNSおよびICANN

まず、ICANN事務局最高技術責任者のJohn Crain氏が、エンドユーザーが単一のインターネットを利用するための規範とセーフガードを定義する上で、マルチステークホルダーによる作業が重要であると述べました。次いで、セキュリティと安定性に関する諮問委員会（SSAC）のRam Mohan氏からはインターネットの分断についての説明があり、重要なインフラの障害や利用者体験の低下を引き起こす可能性が述べられました。また、アドレス支持組織（ASO）のPaul Wilson氏は、データの流れが阻害されることもまた、インターネットの分断であり、分断はローカルなレベルで政府によって行われる傾向があると指摘しました。GNSOのJames Bladel氏は、ビジネス界におけるインターネットの分断を、企業が顧客に到達するのを阻む摩擦と表現しました。同じくGNSOのFarzaneh Badii氏は、相互運用可能で安全なインターネットへのアクセスはすべての人が自己表現できるようになるため、人権にとって重要であると述べました。

本セッションで浮上したことは、インターネットの分断について普遍的な運用上の定義は現時点では存在していないこと、ICANNはその任務と一貫性のある方法でインターネットの分断を対処すべき、といったことでした。

○地政学、立法、および規制の策定に関する討論

本セッションでは主に、国連をはじめとする政府間組織（IGO）での活動、欧州での法規制検討状況、アジア太平洋地域での法規制の状況、コミュニティにできることは何かといったことが、情報共有および議論されました。

2022年開催のITU全権委員会議では、インターネットプロトコルベースのネットワークや、IPv4からIPv6への移行促進などについての決議が予定されていることが共有されました。また、欧州連合（EU）においては、今年中に可決見込みのデジタルサービス法（DSA）、および「ネットワークと情報システムのセキュリティに関する指令（NIS指令）」の改訂版であるNIS2指令について主に触れられました。アジア太平洋地域では、中国で2021年11月に施行された個人情報保護法（PIPL）、インドのIT Act 2000、日本で2022年4月に改正された個人情報保護法などについて触れられました。

■ gTLDポリシー関係

○EPDPフェーズ2（SSAD）

EPDP-TempSpecフェーズ2小チームは、ICANN75期間中に二つのセッションを開催しました。最初のセッションでは、ICANN事務局がWHOIS情報公開システム設計文書の概要を説明し、その後質疑応答が行われました。この設計文書は、非公開のgTLD登録データの申請送信と受信のプロセスを、申請者とICANN公認レジストラの両方にとって簡素化するシステムの概要を示しています。この設計は、GNSO評議会によって、非公開gTLD登録データへの標準的なアクセスと開示のシステムの推奨に関する、ICANN理事会との議論に情報を提供するために要請されたものです。第2セッションでは、小チームが設計の検討を開始しました。また、GNSO評議会がICANN理事会に対してWHOIS開示システムの導入を推進するよう支持を確認することを、推奨するかどうかの検討も行われました。

○gTLD登録データ正確性範囲検討チーム

ICANN75のセッションにおいて、登録データ正確性に関する範囲決定チームは、課題1（実施と報告）および課題2（正確性の測定）についての、記述の概要と関連する推奨事項を参加者に提供しました。また、レジストラが管理するドメイン名の正確性の状況を報告するための、レジストラを対象とした調査の検討が開始されました。この調査の結果は、課題3（有効性）および課題4（影響と改善）の作業に役立つことが期待されます。

○DNS Abuse

ICANN75では、GNSO評議会が立ち上げた「DNS不正利用に関する小チーム」が、報告書に盛り込まれる予定の取り組みの成果を共有するためのセッションを開催しました。チームでは、コミュニティへの働きかけやコラボレーションと、契約交渉の可能性を並行して行う、多方面からのアプローチについて議論しました。さらに、GNSO評議会は、さらなる緩和措置が必要な場合、PDPを追求することができます。小チームは、ICANN75の直後にGNSO評議会に報告書を提出す

る予定で、GNSO評議会はその後、報告書で提案された勧告を実行するかどうかを決定します。

○移転ポリシーの見直し

移転ポリシーレビューPDP作業部会は、2022年6月21日にパブリックコメント用のフェーズ1Aトピックに関する初期報告書を公表しました。作業部会は、提出期間の終了後、2022年9月にパブリックコメントの提出物のレビューを開始しました。ICANN75のセッションで、作業部会は予備勧告1および2に関するフィードバックについて議論しました。このフィードバックでは、移転元FOAと移転先FOAを廃止し、代わりに登録者への通知と、転送承認コード（TransferAuthorization Code、旧AuthInfo Code）のセキュリティ対策を強化することが提案されました。

○国際化ドメイン名に関する迅速ポリシー策定プロセス（EPDP-IDNs）

ICANN75では、チームは二つのセッションを開催しました。最初のセッションでは、EPDP-IDNsチームは、審議の効率化を図るため、初期報告書を2部構成で公表する計画について議論しました。加えて、ICANNは、IDN導入に伴うリスクを定量化するため、リスク分析に関するプレゼンテーションを行いました。第2セッションでは、新gTLDプログラムのストローマンプロセスフローを確認しました。EPDP-IDNsのチャーター質問と予備勧告は、このプロセスフローにマッピングされています。このレビューの主な目的は、既存のgTLDレジストリのための独立したラウンドの実行可能性を分析することです。また、複数の申請ラウンド間に、異体字をアクティブにすることの可能性を分析することです。

ICANN報告会はオンラインでの開催です。

■ 理事の交代

最終日には年次総会となる理事会が開催され、4人の理事が任期を迎え退任し、新たな理事が加わりました。2016年11月から6年間、ASO選出で理事を務めてきたJPNICの前村も退任となりました。前村からの読者の皆さまへのメッセージがありますので、本稿と併せてぜひご覧ください。

ICANN理事在任の6年間を振り返って
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2022/vol1965.html

■ 第65回ICANN報告会

第75回ICANN会議での議論を紹介する報告会を、2022年10月20日（木）に、オンラインにて開催いたしました。当日のプログラムは次の通りです。

1. ICANN75会議概要報告
2. 国コードドメイン名支持組織（ccNSO）関連報告
3. ICANN政府諮問委員会（GAC）報告
4. TLDでの1文字IDN及びSLDでの日本語ドメインラベルについて
5. GNSOレジストリ・レジストラ部会報告
6. 次期新gTLD申請手続きポリシー検討状況報告
7. ICANN理事会に関する報告

第65回ICANN報告会の資料と動画は次のURLで公開していますので、本稿と併せてぜひご覧ください。

第65回ICANN報告会
https://www.nic.ad.jp/ja/materials/icann-report/20221020-ICANN/

■ 第76回ICANN会議

第76回ICANN会議は、メキシコ・カンクンで2023年3月11日から16日まで開催されました。この会議の内容は、次号84号でご紹介いたします。

なお、今回ご紹介した第75回ICANN会議のさらに詳細なレポートは、JPNIC Webでご覧いただけます。詳しくは次のURLをご覧ください。

第75回ICANN会議報告
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2022/vol1963.html

「日本インターネットガバナンスフォーラム2022～IGF2023日本開催を見据えて～」開催報告

日本インターネットガバナンスフォーラム2022（日本IGF2022）が、2022年10月26日（水）から28日（金）までハイブリッドで開催されました。主催は「IGF2023に向けた国内IGF活動活発化チーム」で、政府、ビジネス、市民社会、技術コミュニティからの参加者が集い、IGFの原則であるマルチステークホルダーアプローチで活動を行っています。本稿では、このフォーラムの模様を一部抜粋する形でご紹介します。

■【プレイベント】バーチャル美少女ねむさんとのトークイベント「メタバース時代のインターネットガバナンス」

プレイベントでは、バーチャル美少女ねむさんをお呼びしました。ねむさんは、「世界最古のバーチャルYouTuber」「メタバース原住民」を名乗っていて、生身の人間ではなく、メタバース上のアバターをアイデン

ティティとして、メタバース文化の発展のために講演や執筆も精力的に行っています。セッションの前半は、バーチャルYouTuberのことをよく知らない参加者のために、メタバースがどのような技術によって実現されているかについて解説がありました。その後には参加者の素朴な疑問に答える質疑応答などが続き、これまでのものとまったく異なる、メタバースの世界を垣間見ることができるセッションとなりました。

日本インターネットガバナンスフォーラム2022の様子

■【第1日】開会式とオープニングセッション

国連IGF事務局のChengetai Masangoさんのビデオメッセージ、総務省国際戦略局次長の小野寺修さんと慶應義塾大学教授の村井純さんのご挨拶の後、日本IGF2022の全体テーマである「今、改めて問われるインターネットの自由」と題したオープニングセッションに移りました。小野寺さん、遠隔参加であった村井さんとともに、司会進行を務める、活発化チームチェアの加藤幹之さん、同プログラム委員長でオープニングセッションの司会を務める上村圭介さんが壇上に並んでセッションが開始されました。

村井さんは冒頭、人類が生み出したグローバルな空間であるインターネットは、当初圧倒的な便益で歓迎されたが、不正利用にどう対処するかに関する答えがなかった。今インターネットは、実社会と切っても切り離せなくなったが、このグローバル空間に必要な規律を各国政府とともに考えて、やり遂げなければならないと指摘しました。途中上村さんは、全体テーマ設定の理由として、ウクライナ情勢をはじめとする最近世界中で起こっていることを眺めるにつけ、インターネットの自由というものが変質してきたのではないかと思ったからと述べました。またセッション後半では、ロシアや中国が現在のインターネットの考え方に反する方針を掲げているように見えるという会場からのコメントに対して、村井さんは「中露もグローバルマーケットを実現しているインターネット自体に反対しているわけではなく、そこに望みがある」と述べました。

■【第2日】特別セッション「IGF2023日本開催に向けて」

最後のセッションは「IGF2023日本開催に向けて」と題されました。JPNICの前村からはIGF2023のローカルホストを務める日本政府に対して、グローバルコミュニティへのメッセージの打ち出し方などの対応方針を進言するために、民間団体や企業を会員とする「日本IGFタスクフォース」の設立を準備中だと紹介しました。その後には、APC（Association for Progressive Communications）が制作した「Futures of internet governance: A case」というタイトルの、インターネットガバナンスが失敗した2031年の物語がビデオで流され、それを元に議論が行われました。

壇上や会場からは、ビデオのいろいろなエピソードに対する感想やコメントが寄せられました。問題を解決することに目がいきやすいIGFですが、問題自体に目が行き過ぎてそれを拡散するような結果にならないように、また、ポジティブな未来像を示すことの重要性も指摘され、最後はIGF2023や国内IGF活動に参加を呼び掛ける壇上からのメッセージで締められました。

■ おわりに

日本インターネットガバナンスフォーラムは、今回初めてのハイブリッド開催となりました。プログラム委員会は丹念にプロセスを構築し、ここで紹介できなかったテーマセッションは、公募の上で審査をして採用。その結果、電気通信事業法改正、オンライン海賊版対策、スプリンターネット、日本のインターネット基盤と多彩なテーマでどれも充実したセッションが集まり、会場とオンラインを合わせると参加者は100人を超えました。

なお、今回ご紹介した日本インターネットガバナンスフォーラム2022のさらに詳細なレポートは、JPNIC Webでご覧いただけます。また、同会合の資料と動画も公開しております。詳しくは次のURLをご覧ください。

日本インターネットガバナンスフォーラム2022開催報告
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2022/vol1959.html

日本インターネットガバナンスフォーラム2022 資料/動画
https://www.nic.ad.jp/ja/materials/igf/20221026/

サイバー主権、ITU、インターネット

上記でご紹介した日本国内におけるIGFだけではなく、国連主催のIGF2022が2022年11月下旬～12月上旬にエチオピアで、アジア太平洋地域のIGFであるAPrIGFが2022年9月中旬にシンガポールで開催されました。それぞれのレポートをJPNICブログで公開していますので、詳しくは次の記事をご覧ください。

インターネットガバナンスフォーラム（IGF）2022速報
https://blog.nic.ad.jp/2022/8275/

APrIGF 2022報告
https://blog.nic.ad.jp/2022/8440/