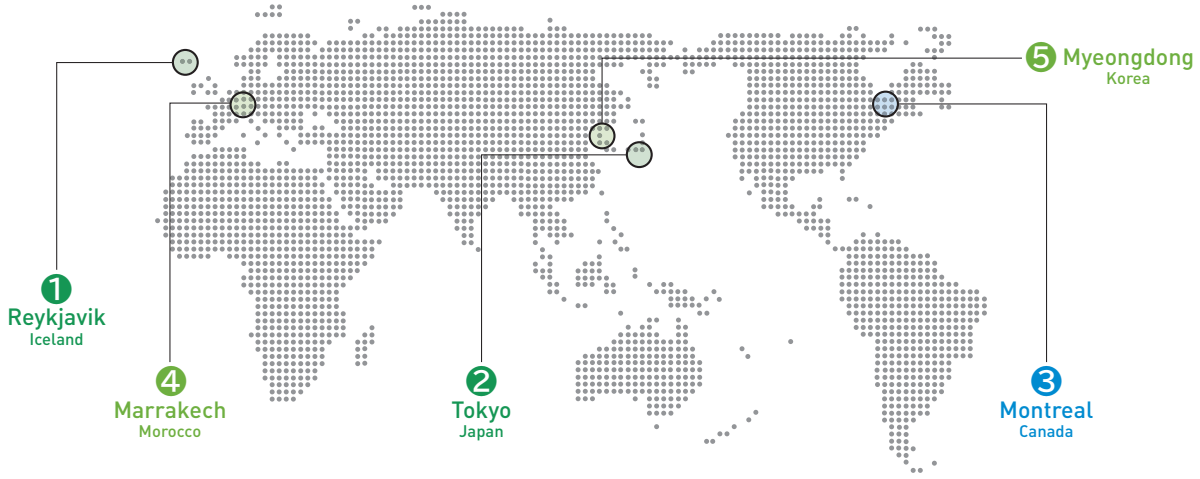
インターネット動向紹介
INTERNET TRENDS INTRODUCTION



インターネット動向紹介

IPアドレストピック

❶ 2019.5.20▶5.24 アイスランド/レイキャビク 第78回RIPEミーティング

❷ 2019.6.21 日本/東京 第36回JPNIC オープンポリシーミーティング

IPアドレスに関する動向として、2019年5月下旬にアイスランドのレイキャビックで行われた第78回RIPEミーティング、2019年6月下旬に東京都で行われた第36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。

第78回RIPEミーティングの動向

◆第78回RIPEミーティングの概要

2019年5月20日(月)～24日(金)の5日間にわたり、アイスランド・レイキャビクで第78回RIPEミーティング(RIPE 78)が開催されました。RIPE NCCは、地域インターネットレジストリ(RIR)の一つで、ヨーロッパ・ロシア・中近東を管轄地域として、IPアドレス・AS番号の分配を行っています。

RIPEミーティングでは、会期初日と2日目に全体会議、3日目と4日目に各種ワーキンググループ(WG)のセッションが開かれます。そして、最終日に再び全体会議が開催されるのが通常の構成です。全体会議とWGのセッションに加えて、チュートリアルやBoFが開催されることもあります。RIPE 78のタイムテーブル、各セッションで利用された資料、発言録、当日の発表風景の映像・音声などは、RIPE 78のWebサイトで公開されていますので、ご興味がある方はご覧ください。

RIPE 78 Meeting Plan
https://ripe78.ripe.net/programme/meeting-plan/

RIPE 78 Meeting Archives
https://ripe78.ripe.net/archives/

ここでは、RIPE 78で議論が行われたアドレスポリシー提案4点のうち、IPアドレスの分配に関する議論と、不正利用に対応する窓口(Abuse)に関する議論を紹介します。JPNICブログでは、アドレスポリシー提案の内容を解説していますので、併せてご覧ください。

RIPE 78でのIPアドレス・AS番号分配ポリシーに関する提案ご紹介
https://blog.nic.ad.jp/2019/2515/


RIPE 78は742名の参加があったとのことです

◆第78回RIPEミーティングにおけるアドレスポリシー議論

提案名	RIPE NCC IRR Database Non-Authoritative Route Object Clean-up(RIPE NCCが管理権限を持たないルートオブジェクトの整理)
提案の詳細	https://www.ripe.net/participate/policies/proposals/2018-06

RIPE NCCにおいては現在、ルーティングに関する情報は、次の通り登録されています。いずれについても、登録は任意に行えるものとなっています。

(1)RIPE NCCから分配を受けたIPアドレス・AS番号に関する情報が登録されたIRRデータベース
(2)RPKI ROAデータベース
(3)運用者が任意に登録した情報が蓄積されたIRRデータベース

このうち、(3)のデータベースに含まれる情報は、IPアドレス・AS番号の分配先組織から同意が得られていないまま登録されている可能性があります。意図しないルーティング情報は、ネットワークの運用において問題を引き起こす可能性があることを、提案者は問題視しているようでした。

今回の提案では、(3)のIRRデータベースに登録されたルーティングに関するオブジェクト(ルートオブジェクト)が、五つのRIRのうちのいずれか一つのRIRによって発行されたRPKI ROAと競合する場合、このオブジェクトはRIPE NCCによって削除されなければならない旨を、ポリシー文書に追加することを目的としています。

ポリシー文書の策定、改定プロセスは、PDP(Policy Development Process)としてまとめられています。

Policy Development Process in RIPE(RIPE地域におけるポリシー策定プロセス)
https://www.ripe.net/publications/docs/ripe-710

この提案は、PDPの初期段階にあり、コミュニティから広く意見を募り、提案内容を精緻なものにする時期にあたるものでした。今回のミーティングでは、質疑応答に目立った内容のものはありませんでした。提案内容では、ROAと競合することが判明してから、ルートオブジェクトが削除されるまでの期間を7日としていましたが、適切な期間をどのように考えるかといったコメントのほか、7日ではなく14日や1ヶ月にするのはどうか、といったコメントが出されていました。

提案名	Validation of "abuse-mailbox"("abuse-mailbox"の項目に登録された電子メールアドレスの定期的な認証)
提案の詳細	https://www.ripe.net/participate/policies/proposals/2019-04

RIPE NCCでは、該当IPアドレスの不正利用に対応する窓口となる電子メールアドレスを、データベースに登録する際、"abuse-c"または"abuse-mailbox"という項目を利用します。これらの項目に登録された電子メールアドレスが機能しているかどうか定期的な確認を行っています。

RIPE 78時点では、約70,000の対象となる電子メールアドレスについて、到達可能な電子メールアドレスかどうかを機械的に確認している段階でした。機械的な確認が難しい場合には、RIPE NCCの事務局スタッフが手動で確認を行っているとのことです。

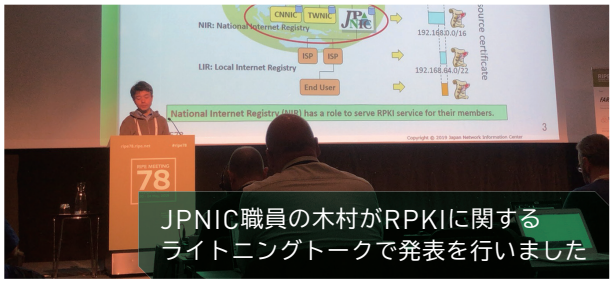
今回の提案では、この対応をさらに進め、割り振り・割り当てを受けた組織の担当者が、メールに記載された検証用のコードを所定のWebページに入力するなどの方法で、機械による対応ではないことを確認することを主眼に置いた内容のように見受けられました。

提案に関する発表の前に、RIPE NCC事務局から、現在実施中の電子メールアドレス確認の進捗状況が報告されていました。事務局での取り組みは完了しておらず、対応を進めている途中であることから、現時点での取り組みが完了後に、その結果を十分に分析してから、提案を進めるかどうか、提案の内容を変更するかどうか、検討した方がよい、というコメントが出されていました。提案が今後どのように改定されていくのかは、現在の取り組みの結果次第のようでした。

◆次回以降のRIPEミーティングについて

次回となるRIPE 79ミーティングは、2019年10月14日(月)～18日(金)にオランダ・ロッテルダムで開催されました。RIPE 80ミーティングは、2020年5月11日(月)～15日(金)に、ドイツ・ベルリンで開催予定です。

Upcoming RIPE Meetings
https://www.ripe.net/participate/meetings/ripe-meetings/upcoming-ripe-meetings



JPNIC職員の木村がRPKIに関するライトニングトークで発表を行いました

誌面では割愛したアドレスポリシー提案や、RIPEミーティングの雰囲気を紹介した内容は、次のURLをご覧ください。

第78回RIPEミーティング報告[前編]全体概要およびアドレスポリシー関連動向
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2019/vol1695.html

RIPEミーティング参加者を対象としたプレナリーセッションや、技術的な動向については、次のURLをご覧ください。

第78回RIPEミーティング参加報告[後編]技術動向～参加者の多様化とコミュニティのあり方を見直す動き～
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2019/vol1696.html

第36回JPNICオープンポリシーミーティングの動向

2019年6月21日(金)に、東京都千代田区のJPNIC会議室にて、第36回JPNICオープンポリシーミーティング(JPOPM36)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。

JPOPM36では、「JPNICにおけるWHOIS正確性向上の検証」のアドレスポリシー提案が議論されましたので、その様子をご紹介します。その他、情報提供が7件ありました。資料や議事録は、次のWebサイトからご覧ください。

第36回JPNICオープンポリシーミーティング開催のご案内
http://jpopf.net/JPOPM36Program

◆JPOPM36におけるアドレスポリシー議論

ポリシー提案 [036-01]	JPNICにおけるWHOIS正確性向上の検証
提 案 者	鶴巻悟氏(JPOPF運営チーム)

これまでAPNICをはじめ、すべてのRIRにおいてWHOIS情報の正確性向上に関する議論が重ねられてきました。北米のARINおよび欧州のRIPE NCCにおいては、既に正確性を検証するためのプログラムが導入されています。APNICにおいても、2019年6月30日(日)から類似のプログラムが導入されました。参考までに、APNICにおける検証プログラムの概要は次の通りです。

1. 半年に1度、APNICよりWHOIS記載の各Abuse窓口に対して電子メールが送信されます(1通目にURL、2通目にパスワード)。
2. 15日間返答が無い場合は、MyAPNIC(APNIC会員がIPアドレスの管理に利用するポータルサイト。JPNICにおけるWeb申請システムに相当)に警告が表示されます。
3. 30日間返答が無い場合は、MyAPNICの機能が一部制限されるなどの、より厳しい対応が行われます。

提案者は、上記の動向を受けて、本JPOPMにおいて以下の二つの提案を行い、いずれも賛成多数で1次コンセンサスに至りました。

<提案1>
・JPNICにおいても、Abuse問い合わせ先の正確性の検証を実施する。
・具体的な検証手法や検証頻度等を検討するためのワーキンググループ(WG)を設置する。

<提案2>
・IPアドレスの割り当て情報やAS番号の割り当て情報におけるAbuse問い合わせ先を明確化するために、APNICにおけるIRT Object(Abuse窓口)に相当する、新たな窓口情報の実装可否について、上記WGで検討を行う。

会場からは、「Abuse窓口以外の[管理者連絡窓口]や[技術連絡担当者]の検証も行わないのか」という質問がありました。これに対し、提案者は、次の通り二つの理由とともに行わない旨を回答しました。


ポリシー提案に関してコンセンサスの確認を行っている様子

・海外における提案はAbuse窓口に特化していること。
・WHOISを見て行われる問い合わせの多くは、Abuseに関するものと理解しているが、Abuseに関する問い合わせは総務部門等に配信される可能性のある管理者連絡窓口等に届くべきではなく、Abuseを担当する部門に直接届くべきであるため。

本提案は、IP-USERSメーリングリストにおける確認を経て、最終コンセンサスに至りました。引き続き、WHOIS abuse連絡先正確性向上の検討WGが発足され、具体的な検討が行われています。次回、2019年11月27日(水)に開催するJPOPM37では、WGでの検討状況について中間報告が行われる予定となっています。

◆JPOPF-STのみなさんにJPNICから感謝状を贈呈しました

日本におけるIPアドレスコミュニティの活動は、APNICでも高く評価されています。

その活動の運営を担ってくださっているJPOPF-STのみなさんに対し、JPOPM36終了直後に時間をいただき、日本のIPアドレスコミュニティの運営を通じ日本のアドレスポリシー議論とコミュニティの発展に貢献したことおよび、日本における番号資源管理業務の円滑な遂行に大きく寄与したことに対して、感謝の意を表し、感謝状をお送りしました。

これからますますコミュニティが発展していくことを期待すると共に、JPNICとしても協力を続けてまいります。

今回誌面で取り上げた内容の他に、JPOPM36の開催報告については、次のURLからご覧ください。

第36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/2019/vol1698.html

IPアドレスに関連する普及啓発活動の報告

JPNICでは、各地のNOGや勉強会に参加し、講演を行ったり、参加者の方との意見交換を行ったりすることで、インターネットの発展に寄与できるよう取り組んでいます。

2019年6月から7月に開催された地域NOGの様子を紹介しながら、こういった取り組みへの思いをまとめました。JPNICにできることでしたら、ぜひご相談ください。また、JPNICの役職員がお近くにまいりましたら、ぜひお声がけください。

各地のNOGや勉強会で会いましょう
https://blog.nic.ad.jp/2019/2802/

2014年から継続して行っているIPv6対応状況に関するアンケートについて、2018年度の調査結果をJPNICブログで報告しました。JPNICとしては、さらなる情報発信や普及啓発のために活動を進めてまいります。

2018年度IPv6対応状況に関するアンケート調査結果報告
https://blog.nic.ad.jp/2019/2532/

インターネット動向紹介

技術トピック

❸ 2019.7.20▶7.26　カナダ/モントリオール　第105回IETFミーティング

技術関連の動向として、2019年7月20日(土)から26日(金)にかけてカナダのモントリオールにて開催された、第105回IETFミーティングに関するトピックをご紹介します。

第105回IETFミーティング 全体会議報告

JPNICの塩沢啓より、第105回IETFの全体会議についてご報告いたします。


全体会議の様子

■ 参加者人数の近況

全体会議でのチェア発表によると、48ヶ国/地域から1,079名が参加しました。2018年夏のモントリール開催は1,078名でしたので、ほぼ同規模となりました。ハッカソンのオンサイト参加者は280名で、前回よりも参加人数は少なくなったものの高い水準を維持し、42のプロジェクトが実施されました。

■ IETF Technical Plenary

Technical Plenaryでは、プリンストン大学のArvind Narayanan氏と、ネットワークセキュリティで著名なSteven M. Bellovin氏の2名を講演者に迎え、「インターネット上のプライバシー」に関する講演が行われました。

Narayanan氏のプレゼンテーションでは、自身がリーダーを務めるWeb Transparency and Accountability Projectという取り組みについて紹介されました。100万もの膨大なWebサイトから、クッキーや異なるサイト間のトラッキングデータなどを計測し、そのデータを公開するという研究です。一方で、IoT機器間の通信を測定することの難しさについても言及し、IoT機器におけるプライバシー問題について警鐘を鳴らしました。

Bellovin氏は、企業や政府による過剰な個人情報の収集や機械学習といった、昨今のプライバシーに関する懸念点について解説しました。また、個々の技術的な評価や議論にとどまらず、最後にはプライバシーに関する諸問題に対して、これからIETFとしてどう取り組んでいくべきかについて議論されました。

■ IETFに初めて参加して

今回、筆者はIETFに初めて参加しました。IETFでは、初参加者でも議論に参加できるように、手厚いサポートがされていました。2日目の日曜日午後にはチュートリアルセッションが開催され、IETFの概要説明だけではなく、WGのチェアを務める方たちと話す機会も設けられました。

また、IETF 105の開催前には、Webinarも複数開催されました。内容はオンサイトと同じでしたので、チュートリアルの日には現地に行けないという方は、Webinarだけでも参加してみると、IETFの雰囲気が分かると思います。また、チュートリアルの資料は、ISOC-JPのEducation WGによる日本語訳※1が毎回公開されます。いきなり英語だとハードルが高いですが、このような日本語での導入があると、分かりやすかったです。

会合に参加するまでは、事前準備として興味のあるWGのメーリングリストに登録して、議論を追いかけました。また、IETFチェアによる、IETF 105のホットトピックスを紹介する記事※2が、会合開催前に掲載されます。初参加だと、今回はどんな議論が注目されているのかなかなか分かりませんが、チェアの視点から今回の見所が解説されているため、大変参考になりました。なお、会期終了後には、IETF 105のハイライトを紹介する記事※3も掲載されます。

その他に、会期中はISOC-JPのISPC(Internet Standardization Promotion Committee)が企画した「Get Together」と呼ばれる、日本からの参加者が集まる懇親会にも参加しました。他の参加者と交流できただけでなく、各WGの最新動向も聞くこともできました。初参加で分からないことも多く、またIETFでは複数のWGが並行して進むため参加できないWGもあるので、このような現地での情報交換の場は、とても貴重に感じました。

※1 Newcomer's Tutorial 資料(日本語訳)
https://www.isoc.jp/wiki.cgi?file=slides%2Fedu%2Fietf%2D105%2Dnewcomer%2Dslides%2Djp%2Epdf&page=IETFEduWG&action=ATTACH

※2 IETF 105 Preview
https://www.ietf.org/blog/ietf105-preview/

※3 IETF 105 Highlights
https://www.ietf.org/blog/ietf-105-highlights/

第105回IETFミーティング ADD BoF報告

第105回IETF（IETF 105）では、「DNS（Domain Name System）の処理を行うアプリケーション（Applications Doing DNS、略称「ADD」）」というBoFが開かれました。本稿では、JPNICの木村泰司より、このBoFで行われたDNS関連技術の標準化に関する議論についてご紹介します。

■ ADD BoFの背景 - DoTやDoHの登場

IETFでは、DNSの伝送路（トランスポート）においてTLS（Transport Layer Security）やHTTPSを用いることで、問い合わせの内容を第三者に傍受されないようにする、DoT（DNS over TLS）、DoH（DNS over HTTPS）といった仕組みが作られています。これらは、トランスポートが暗号化されたり、どのフルリゾルバが使われているかを分かりにくくしたりするといった、通信上の変化だけでなく、アプリケーション自体がDNSの問い合わせ先に関わる処理を行うようになるという、変化をもたらします。

ADD BoFは、これらの変化を踏まえて、今後の標準やベストプラクティス、ガイダンスを策定する取り組みについて、議論するために開かれました。会場には250名以上が集まり、立ち見の人もいました。

Applications Doing DNS（add）
https://datatracker.ietf.org/wg/add/about/

DNSは長らく、UDP（User Datagram Protocol）の53番ポートを使って、平文で問い合わせ応答が行われる仕組みとして使われてきました。これがスノーデン事件を機に、IETFにおいて状況が変わってきます。大規模な通信傍受を攻撃行為とみなし、その影響が及ばないようにプロトコルを策定していこう、という考え方が出てきたのです（RFC7258）。この考え方を受けて、問い合わせ応答の内容を第三者に分かりにくくする、DoTやDoHが作られてきました。

これらが普及すると、DNSサーバやネットワーク管理に影響があると考えられています。Webサーバがリゾルバの役割を担ったり、ローカルのリゾルバがバイパスされてしまったりするためです。さらに、DoHで使うリゾルバを選択する仕組みが改良されると、どのDNSリゾルバが使われているかも分かりにくくなります。具体的には、ユーザー環境において、どのようなDNSの問い合わせ応答が行われているのかが、DNSサーバやネットワークの運用を行っている側では把握できなくなるのです。DNSを使って、マルウェアが行っている通信を判別することも、行いにくくなります。CDN（Content Delivery Network）のような、従来のDNSを想定した仕組みの動作にも影響があると考えられます。これらについて、「ADD BoFイントロ」で述べられています。

ADD BoFイントロ - これまでの経緯（ADD BoF Intro, How we got here）
https://datatracker.ietf.org/meeting/105/materials/slides-105-add-add-bof-intro-00.pdf

■ DNSの変化に関わるこれまでの議論

これらのDNSにおける変化について、DoH WGやDPRIVE WGで議論となり、前回のIETF 104で行われたサイドミーティングを経て、ADDのメーリングリストが作られました。前述の資料によると、論点を集めた文書として次の三つが挙げられています。

Centralized DNS over HTTPS（DoH）Implementation Issues and Risks
https://tools.ietf.org/html/draft-livingood-doh-implementation-risks-issues-03
-DoHの普及によって中心的なDNSサーバができることのリスクなど

DNS over HTTPS（DoH）Considerations for Operator Networks
https://tools.ietf.org/html/draft-reid-doh-operator-00
-通信事業者に関わるDoHの法律に関連する整理やCDN、captive portalのような仕組みへの影響

Recommendations for DNS Privacy Client Applications
https://tools.ietf.org/html/draft-bertola-bcp-doh-clients-00
-DoHクライアントによるDNSの仕組みなどへの影響

これらは、ブロッキングやCDN、DNSリゾルバを提供するサービスについて、技術的な側面を押さえておくためにはとても参考になる文献であると、筆者には思われました。

■ ADD BoFにおける議論

BoFでは、MozillaやGoogle社といった、DoHを使えるWebブラウザや、サービスを提供している組織の技術者から考え方が説明され、続いて議論が行われました。これらはすべて、IETFの参加者としての発言ですので、所属組織を代表したものではなく、発表者個人の見解ということになります。

DNS in Applications（アジェンダでは Mozilla's vision for DNS & apps）, Martin Thomson氏
- -ユーザーのセキュリティとプライバシーは基本であり、オプションではない（Mozilla Manifesto）。それにのっとってHTTPSの導入が進められてきた。
- -DNSは一貫した名前空間を持つものではなくなってきている。もし一貫したものであったなら、DoHをデフォルトにしていた。
- -DNSは効果的な「control point」になっていない。おのおののリゾルバサーバは、プライバシー保護において重要だが、既にcaptive portalやマルウェア検知において、DNS応答の内容が変わるといったことが起きている。
- -DNSを使ったコンテンツブロッキングは、オーバーブロッキングなどの懸念もある。

Google's perspective, Kenji Baheux氏
- -ユーザーのネットワークにおいてリゾルバがある状態、リゾルバがおのおののネットワークで提供されていること

に、変化を起こそうとしているわけではない。
-DoHは使う時に有効にできるものであればよい。DNSサーバの提供者は、プライバシーに関する要件に従っているべき。

ブラウザ以外のデバイス(アジェンダでは Non-browser apps doing DNS), Jim Reid氏
-運用やポリシーとして検討すべき事項としては、DNSSECのトラストアンカーをどのように設定するのかという点、DoTやDoHをどのように選択するのかという点、何にフォールバックするのかという点、ローカルのリゾルバーを選択するのか、ベンダーが指定するものを選択するのかといった点がある。
-DNSの問い合わせ応答に関する情報漏洩や、悪意のあるリゾルバの脅威についての明文化も必要。

この他に、WebサーバがDoHサーバのURLをWebクライアントに伝える方式の提案や、DoHサーバの運用やCDNなどへの影響に関するドキュメント化の提案、DoHにおけるHTTP PUSHの利用可能性などについてプレゼンテーションがあり、議論されました。

会場では、WGを作成して議論する場を設けるべきといった意見の他、DNSの名前解決が特定のリゾルバに集中しやすい状況になると、そのリゾルバの利用状況さえ手に入れば、大規模な傍受が行われやすくなるという懸念が挙げられていました。

今回紹介したプレゼンテーション資料は、下記のADD BoFのページにあります。

Applications Doing DNS(add) BOF
https://datatracker.ietf.org/meeting/105/materials/agenda-105-add-04.html

■ 議論を受けて

今回の議論を聞いていて、発表者の多くは、理想の姿を明確にしようとし、そこに近づくようにデプロイしていく、もしくはプロトコルを扱っていくという姿勢であることが印象に残りました。自組織の事業に都合がいいかどうか、他の事業に都合のいいことを自組織もやるべきかどうか、といった視点もあるかもしれませんが、全体を俯瞰して、例えば大規模な通信傍受への対策のためにはどういうプロトコルが必要なのかといった視点は、間違いなく存在しています。

「利用者の多いWebブラウザが仕様を変えたから仕方がない、自組織のサービスを変えていこう」という「追いかける姿勢」では、追いつくこと、ひいては技術の仕組みにおいてリーダーシップを発揮することは難しいはずです。大手の海外の事業者が提供するサービスを利用するだけでなく、生み出す側になるには、グローバルな理想像の議論に参加し、根本的な趣意を押えていくことが重要であるように思われました。

第105回IETFミーティング トランスポートエリア関連報告

GE Global Researchの西田佳史様より、トランスポートエリアに関するトピックについてご報告いただきましたのでご紹介します。

■ Multipath TCP WGについて

筆者は10年間ほど、IETFのMultipath TCPワーキンググループ(WG)という、TCPの拡張技術の標準化を行うグループのコチェア(共同議長)を務めてきましたが、今回のモントリオールの会議では、WGの収束がかなり真剣に議論されました。もしWGの収束が正式に決定されるとなると、WGは実質的に消滅し、今後関連する技術の議論は他のWGへと移管されることになります。筆者としては、立ち上げ時から関わってきたWGが無くなることに関して寂しさを感じる部分はありますが、発足からかなり長い時間が経過し、標準化の作業もかなり落ち着いてきたので、そろそろ区切りをつけてもいいかもしれないという気持ちもあります。

■ Multipath TCPの技術動向について

Multipath TCPはTCPの拡張技術の一つで、この拡張を利用すると、TCPで複数の通信経路を用いた通信が可能になります。従来のTCPでは、Wi-Fiと携帯電話の二つの通信回線があったとしても、一つのTCPコネクションで利用できるのは、どちらか片方の回線に限定されていました。一方、Multipath TCPを利用する場合は、一つのコネクションで二つの回線を同時に利用したり、どちらかの回線を通信状況に応じて選択しながら通信したりするといった、柔軟な運用が可能になります。この技術はApple社の提供する、Siriなどのサービスで利用されています。Apple社では、Multipath TCPで遅延の小さなネットワークを優先的に利用することで、迅速なレスポンスを実現することを目的としているようです。

今後のMultipath TCP技術の動向は、セキュリティ機能の強化などの、機能拡張に関して議論が進められていくことになると思われます。Multipath TCPには、まだこのような技術的課題が残っているので、WGを収束するには早いのではという意見もあるのですが、一方でセキュリティのような機能拡張は、Multipath TCPには必要ないかもしれないという意見もあります。この背景には、昨今のIETFでQUICという新しいトランスポート技術の議論が、活発になってきたことがあげられます。

■ QUICの技術動向について

QUICは、UDPの上位層として設計されているトランスポートプロトコルで、TCPの上位互換となるような機能を提供できるように、設計開発が進められています。QUICは、TCPの持っている問題点に対する改善策を採り入れて、通信の効率化、高速化や、安全性の強化などを目標としています。また、QUICの開発に伴って、HTTP技術の改変

も進んでいます。今までのHTTPは、トランスポート層のプロトコルにTCPを利用していましたが、これをQUICに置き換えた、新しいHTTPを開発するというものです。このQUICをベースにしたHTTPは、HTTP/3として、現在標準化のための議論が進められています。

■ QUICとTCPの違いについて

ここでQUICとTCPの違いについて、簡単に説明してみたいと思います。

一つは、セキュリティ面の強化です。現在、TCPを用いた通信を暗号化する場合は、上位層でTLSを利用するのが通常となっています。これは、TCPに暗号化の技術がなかったためです。近年、この問題に対処するためにtcpcryptという、TCPのセキュリティ拡張が開発され標準化されましたが、まだ技術の普及が進んでいません。また、長い歴史を持つTCPでは、多くの既存アプリケーションがあるため、暗号化機能を持たない過去のバージョンとの、互換性を保つ必要があります。このため、暗号化を行わない通信も、引き続きサポートしていくことが求められています。

これに対し、過去の資産のないQUICは、すべての通信を暗号化し、暗号化しない通信は一切サポートしない、という設計になっています。こういった点から、先ほどのMultipath TCP WGの例では、Multipath TCPで難しい課題がありそうなセキュリティ拡張を考えるよりも、QUICでマルチパス通信を行うことを検討した方が楽なのではないかという意見が出るようになりました。

また、通信遅延の低減もQUICが注力している点です。TCPはデータ送信を開始する前に、通信手順の確認作業のため、最低でも3回のメッセージの交換を行う必要があります。また前述の通り、TCPで暗号化を行う場合はTLSを利用する必要がありますが、TLSの暗号化手順を確認するため、ここでもメッセージの交換が必要になります。

ここで問題となるのは、TLSのメッセージ交換は、TCPの通信が確立した後でないと、行うことができないという点です。つまり、TCP+TLSで通信を行う場合、データが転送できる準備が整うまで合計で7、8回程度の、メッセージ交換が必須となってしまうのです。たかがこの程度という見方もあるかもしれませんが、RTT(Round Trip Time)の比較的大きな回線では、体感できるほどの差が出る可能性があります。QUICでは、暗号化の機能がプロトコル内にあるので、TCPによる通信の確立とTLSの暗号化手順の確認に相当するものを、同時に行うことができるため、データ送信の準備が整うまでの時間を大幅に短縮できるメリットがあります。

また、HTTPなどの通信では、比較的短い間隔で同じ相手と通信を行うことがよくありますが、このような場合、QUICはさらに低遅延な通信を行うことができます。この仕組みは、TLSの最新バージョン1.3でも採用されている0-RTTと呼ばれるもので、過去の通信で利用したセッションに関するパラメータをキャッシュしておくことによって、2回目以降の通信では、通信のセットアップの開始時からデータ転送を行うことを可能にするものです。

さらにQUICには、TCPで指摘されていた問題点に対する対策が、いくつか取られています。例えば、TCPにはロストしたパケットが再送されて正しく受信されるまで次のパケットを処理できない、ヘッドラインブロッキングと呼ばれる問題がありますが、QUICではストリームという概念を導入することで、この問題を軽減することができます。またRTTの計測は、通信の性能を左右する要素の一つですが、QUICではホスト内での遅延とネットワークの遅延を区別する仕組みが導入されていて、TCPよりも高い精度でRTTの計測を行うことが可能になっています。その他、バージョン番号の導入や、機能拡張を柔軟にするパケットフォーマットの工夫により、新しい機能を比較的簡単に追加していくことができる設計となっている点なども、TCPになかった特徴です。

このように有利な特徴を持つQUICですが、TCPの方にメリットがあると思われるケースもあります。例えばTCPでは、TOE(TCP Offload Engine)という、NICレベルで高速にパケットを処理する技術の普及が進んでいます。またTCPには、PEP(Performance Enhancing Proxy)という中継ノードを利用して転送性能を向上させる手法がありますが、パケットヘッダまで暗号化するQUICでは、この方式を利用することには困難や制約があります。さらに、インターネット上にはUDPのトラフィックを遮断したり、転送速度を制限したりしているサイトも存在しています。加えてISPの観点からは、QUICトラフィックを観測しても通信状況がわからないため、問題があった場合に対処が難しい技術という理由で、積極的に採用したくないといった意見もあります。

いろいろな視点はありますが、QUICは現在IETFにおいて、とても注目を集めているようです。IETFミーティングでは、1週間の間に100以上のミーティングが並行して行われますが、昨今のIETFミーティングではQUIC WGのミーティングは毎回150名程度の参加者がおり、参加者数の多いWGの上位5位内に常に入っています。また、QUIC WG以外のミーティングでも、QUICの性能解析、deploymentの状況などに関する議論が、多く行われている印象を受けました。

実は、IETFがTCPやUDPに代わるトランスポートプロトコルの開発と標準化を試みたのは、今回が初めてではありません。過去にはSCTPやDCCPという、二つのプロトコルが標準化されました。ただし、この二つのプロトコルは、現状でそれほど普及していません。これらのプロトコルの普及にあたり妨げとなった大きな要因は、NATを新しいトランスポートプロトコルに対応するように、更新する必要があることです。また、新しいプロトコルの特長を生かしたキラーアプリケーションの存在も重要になります。しかし、UDP上のプロトコルであるQUICは、NATを更新する必要はありませんし、Webアプリケーションという大きなターゲットも既に持っています。QUICが今後どの程度普及していくのかは、今の時点ではっきりとは分かりませんが、過去のプロトコルにあった普及における問題を克服している点で、期待が持てると思います。

インターネット動向紹介

ドメイン名・ガバナンス

④ 2019.6.24▶6.27
モロッコ／マラケシュ
第65回ICANNマラケシュ会議

⑤ 2019.8.12▶8.16
韓国／ミョンドン
Asia Pacific Internet Governance Academy

本稿では、2019年5月～8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65回ICANN（The Internet Corporation for Assigned Names and Numbers）マラケシュ会議での議論の動向や、Asia Pacific Internet Governance Academy（APIGA）の活動などを中心にご紹介します。

第65回ICANNマラケシュ会議

◆はじめに

2019年6月24日（月）から27日（木）まで、モロッコ・マラケシュにて第65回ICANN会議（ICANN65）が開催されました。今回も、これまでの毎年6月開催のICANN会議と同様、「ポリシーフォーラム」と呼ばれるフォーマット※1での開催でした。本稿では、このICANN65について、GNSO関連の動向を中心にご報告します。


会場のPalmeraie Conference Center Marrakech

◆オープニングセレモニーおよびマルチステークホルダーエートス賞授賞式

会期初日である6月24日（月）の8時から30分間枠で開催された、Welcome Coffeeが実質的にオープニングセレモニーとなりました。まず、ICANN事務局のポリシー担当より、High Interest Sessionおよび分野別ドメイン名支持組織（GNSO）のポリシー策定セッションについてブリーフィングがあったのち、ICANNオンブズマンから挨拶がありました。

ICANNのマルチステークホルダーモデルに対して卓越した貢献を行った人に贈られる、マルチステークホルダーエートス賞の授賞式が、6月のポリシーフォーラムで開催されるのが通例となっており、今回も初日の18時より、ホワイエにて開催されました。選考者は、各支持組織（SO）/諮問委員会（AC）から1～2名のパネリストからなる選考委員会で、1名または2名が選定されることになっています。

今回は、gTLD登録データの暫定仕様（Temporary Specification）に関する迅速ポリシー策定プロセス（Expedited Policy Development Process, EPDP）チームの、フェーズ1における議長を務めたKurt Pritz氏が受賞しました。Pritz氏は他にも、次期新gTLD申請ラウンドに関するポリシー検討にも貢献しており、その前には2012年までの9年間ICANN職員を務めました。

◆gTLD登録データの暫定仕様に関する迅速ポリシー策定プロセスの検討状況

2019年4月にEPDP検討チームフェーズ2の議長がJanis Karklins氏に決まり、その新体制で同チームはICANN65会期中に2回会合を実施しました。具体的な内容は次の通りです。

1. 非公開gTLD登録データの要求者に関する雛形フォーマットについて議論

   EPDPチームは、非公開gTLD登録データの要求者（法執行機関、統一ドメイン名紛争処理方針（UDRP）関係者等）のユースケースと質問に関する、包括的な雛形に対する評価を開始しました。

2. 非公開gTLD登録データの要求者に関するユースケースの実例を調査

   同チームは、商標権侵害に対する紛争解決手段に訴える目的で非公開登録データの入手を行う、個人または関係組織のユースケースに関して包括的に議論し、また法執行機関が犯罪捜査をする際のユースケースについて評価しました。

3. 統一アクセスモデル（Unified Access Model, UAM）に関する各国データ保護委員会（DPA）へのアウトリーチに関する次の段階についてのすり合わせ

   技術研究グループ（Technical Study Group, TSG）による非公開WHOISデータへのUAM案を、GDPRの下での基本的な想定事項および妥当性について試すためにICANN事務局が各国DPAに提示することになっており、EPDPチームと事務局間で意見交換が行われました。

※1 ICANNの会議種別とは
https://www.nic.ad.jp/ja/basics/terms/icann-meeting-strategy.html

4. フェーズ2のプロジェクト計画案を評価

他に非公開WHOISを利用することになる利用者グループの認定方法などについても議論されました。

◆次期新gTLD申請ラウンドに関する検討状況

会期中に3回セッションが開催され、トップレベルにおける地理的名称に関する文字列の扱いに特化して検討を行っている分科会(作業トラック5)では、首都でない都市名および都市名でない地名(山、川、谷、湖など)文字列の扱いなどについて議論されました。

作業トラック5以外では、申請待ち行列および委任頻度の制限についても議論されました。加えて、ICANN事務局のグローバルドメイン部門(GDD)が、次期申請ラウンドの事前計画作業(ポリシーの実装、作業負荷、コストなど)で利用するための案を共有した上で、作業トラックを束ねるWGとGDDとの対話を行いました。

◆gTLDにおける商標権保護機構(RPM)の評価

2012年のgTLD募集ラウンドでは、UDRPに加えて商標権を保護する新たな機構（TMCH(Trademark Clearinghouse)、URS（Uniform Rapid Suspension)、PDDRP（Trademark Post-Delegation Dispute Resolution Procedure))※2が導入されましたが、それらを振り返り評価するのがフェーズ1で、UDRPそのものを評価するのがフェーズ2になります。これまでフェーズ1の検討が行われており、2018年12月以降サンライズ(商標権者などを対象にした優先登録)とTrademark Claimsに関して検討が行われてきました。ICANN65では、これらのRPMに関する勧告案の検討が行われました。

◆新gTLDオークション収入使途の検討

2012年のgTLD募集ラウンドに際しては、文字列競合が起こった場合に、つまり同じ文字列を複数の申請者で取り合いになった場合に、オークションにより登録者が決定されました。それによって生じた収入の使い道を検討する、オークション収入に関するコミュニティ横断作業グループ(CCWG)は、初回報告書に対して提出された意見の評価を終えたところです。今回の会合では、最終報告書の公開前に、解決が必要な論点について議論されました。最終報告書のたたき台が議論されましたが、その中にはICANN事務局内に資金分配部門を作る案、財団を作る案、および外部慈善団体と連携する案が挙げられています。

◆インターネットガバナンスに関するコミュニティ横断作業部会(CCWG IG)

本セッションは、理事会のインターネットガバナンスWGと、共同で開催されました。セッションでは、ICANNが得意としているインターネットガバナンスの議論が、サイバーやデジタルと称して、政府間で話されるようになってきている点について議論が行われました。例えば、世界貿易機関(WTO)でドメインネームシステム(DNS)に関する議論がなされるようになっている状況、ICANNとしては声を上げ続けなければならない、といった意見が出されました。

他に、2019年3月のクライストチャーチ銃乱射事件を受けて、ニュージーランドのアーダーン首相とフランスのマクロン大統領が開催した会合「Christchurch Call to Action Summit」およびその成果物である合意「Christchurch Call (to eliminate terrorist & violent extremist content online)」※3が、インターネットガバナンスをどの程度まで再定義したのか、という質問もありました。

さらに、ICANNがITU-D(国際電気通信連合 電気通信開発部門)のメンバー申請を提出したこと、2019年6月10日(月)に公表された国連デジタル協力に関するハイレベルパネルによる報告書、および国連軍縮研究所(UNIDIR)が主催するサイバーセキュリティに関する規範に関する会議、インターネットに関するITU理事会作業部会などについて報告がありました。2019年11月のIGF(Internet Governance Forum)では、各国議員が参加するセッションも開催されるとの報告もありました。

外の世界でのめまぐるしい動きを受けて、ICANN関係者・会議参加者ができることは何か、という問いかけでもあったのではないかと感じるセッションでした。

◆第55回ICANN報告会

本マラケシュ会議での議論を紹介する報告会を、2019年8月8日(木)に東京・JPNIC会議室にて開催しました。当日のプログラムは次の通りです。

1. ICANN政府諮問委員会(GAC)報告
2. ICANN65マラケシュ会議概要報告
3. 国コードドメイン名支持組織(ccNSO)関連報告
4. ICANN理事からの報告
5. DNSルートサーバーシステム諮問委員会(RSSAC)報告
6. 次期新gTLD募集手続きポリシー策定プロセス検討作業部会報告
7. ICANN WHOIS暫定ポリシー策定プロセス検討状況

第55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55回ICANN報告会
https://www.nic.ad.jp/ja/materials/icann-report/20190808-ICANN/

◆第66回ICANN会議

次回ICANN会議は、2019年11月2日(土)から7日(木)にかけて、カナダのモントリオールにて開催されました。本会議の内容は、次号74号にてご紹介いたします。

ICANN66 | Montreal | ICANN Public Meetings
https://meetings.icann.org/en/montreal66

※2 新gTLDにおける商標保護策
https://www.nic.ad.jp/ja/dom/new-gtld/trademark.html

※3 Christchurch Call
テロや暴力を組織化したり促進したりする目的での、ソーシャルメディアの利用に終止符を打つために、国家と企業が誓約合意書に署名を行うというもので、日本国政府も署名しました。企業側は、いわゆるGAFAまたはプラットフォーマーと呼ばれるところはおおむねすべて入っています。

Asia Pacific Internet Governance Academy（APIGA）のご紹介

APIGAは名前が示す通り、アジア太平洋地域を対象とした、インターネットガバナンスに関する能力開発プログラムで、ICANNとKISA（Korea Internet and Security Agency）が共催しています。2016年に始まり今年が4回目の開催で、KISAが共催ということから毎年韓国で行われています。今年は2019年8月12日（月）から16日（金）までソウルの中心街、ミョンドンで開催されました。

Asia Pacific Internet Governance Academy
https://apiga.asia/

APIGAでは、18歳から35歳までを対象にして参加者を募集し、韓国国内からと韓国以外のAP地域の各国からが半数ずつになるように、参加者が選定されます。2019年の参加者は、50名に上りました。フェローシッププログラムによって参加のための旅費滞在費が支給されることから、参加者はフェローと呼ばれることが多いです。

共催であるICANNとKISA以外に、APIGAには以下のAP地域内のインターネット関連団体が協賛しています。

APNIC（Asia Pacific Network Information Centre）
APTLD（Asia Pacific Top Level Domain Association）
Internet Society（ISOC）
Dot Asia Organization Limited
Korea Internet Governance Alliance（KIGA）
株式会社日本レジストリサービス（JPRS）
TWNIC（Taiwan Network Information Center）

講師陣は、これらの団体において第一線でインターネットの運営調整に携わる担当者が務めるとともに、前年度のフェローがメンターとして招待され、セッションの補助や講師を務めます。プログラムの中には座学もありますが、講師陣は努めてセッションをインタラクティブにしようとしているようです。以下、APIGAにおける面白い取り組みを、二つほど紹介いたします。

◆ APNICとDot AsiaによるIPGO（アイピーゴー）

トランプ大のカードをたくさん使うので、カードゲームという括り方はできると思いますが、カードを端末やIPアドレスとして使い、インターネットの成り立ちをエミュレートするゲームです。以下のように進んでいきます。

1）まず、フェロー達は五つほどのグループに分かれます。このグループは、それぞれ太平洋に浮かぶ島国で、果物の名前が付いています。それぞれの国にはカードが配られますが、このカードは、PCやスマートフォンなどの絵が描いてあり、端末に対応します。

2）フェローのうち数名が、図形の名前（円、正方形、三角形など）のISPに指名されます。ISPには大小あり、複数の国をカバーするものも、一つの国でしかサービスを提供しないものもあります。

3）各ISPは、それぞれ大きさに応じた数のカードをAPNIC職員から受け取ります。カードには番号が書いてあります。IPアドレスということです。各ISPは各国にて、端末にIPアドレスを割り当てていきます。

4）ISPは相互接続しています。相互接続のダイヤグラムが会場スクリーンに提示され、ISP担当のフェローはステージ上でリボンを接続回線として、相互接続をします。

5）二つの端末の通信を実現するためには、ルーティングが必要です。スクリーンにはルーティングテーブルが提示され、二つの端末の通信におけるパケットの動きを実演します。

6）その次にはDNSを模します。ISPのリゾルバに対して、ホストネームに対応するIPアドレスを尋ねると、まずルートDNSサーバに尋ね……という名前解決のシーケンスを、フェロー達がパケットとなって実演します。後半ではポイズニングも発生し、フェロー達が持っている、名前にIPアドレスが対応したカードには署名が付されて、真正性が確認できるようになります。DNSSECの模擬ということです。

インターネットの模擬ゲームというのは、おそらく世界中でここにしかないのではないでしょうか。APNICの担当者に聞くと、まだまだ開発途上ということで、今後ももっと精緻なエミュレーションとなっていくのでしょう。

◆ モックICANNセッション（Mock ICANN Session）

モックとは「模擬」という意味で、ICANNで繰り広げられる議論を、本番さながらに実習しようというものです。フェロー達は1日目に、モックICANNセッションにおける、自分の役割を割り当てられます。役割は、ICANNの分野別ドメイン名支持組織（GNSO）の中からレジストリとレジストラ、At-Large諮問委員会（ALAC）と政府諮問委員会（GAC）のプレイヤーなどで、国や社名などまで具体的な役割が指定され、フェロー達はそれらを演じることになります。議論のテーマは、

・レジストリやレジストラは、DNS Abuse問題に責任を取るべきか
・次回新gTLD募集ラウンドでは、申請者支援プログラムは維持されるべきか
・文字列競合の解決手段として、オークションは適切か

といった、概論的ではありながら現実感にも富むテーマで、自分に割り当てられた立場を念頭に意見表出をし、ステークホルダーグループとしての立場を協議して決めるなど課題に取り組みます。会期中、課題の検討に際しては、実際にICANNのGNSO、GAC、ALACでリーダーシップポジションを努めるコミュニティメンバーが電話会議で模擬検討に参加するなど、「本物」を体験する仕掛けもあり、最終日には全員が口の字に並んだ会議卓を囲んでの、モックセッションに取り組みます。

フェロー達はとても器用に、「発展途上国のGAC代表」「米国の大手レジストリ」などの役割を演じ、不案内なテーマにも都度都度検索で調べるなどして取り組み、活発な議論を繰り広げています。

これ以外にも、地域インターネットレジストリ(RIR)やIETFの議論に関しても、紹介や実習があります。朝から夕方まで会議室で演習、昼食と夕食も講師陣とフェローが一緒にとって、とても濃密な1週間を過ごして、インターネットの運営の一端を学んでいきます。講師陣も非常に献身的に取り組み、夕食が終わった後にその日1日の振り返りを行い、一段落するのは午後10時頃という毎日が続きます。

1週間を通じて、英語でインターネットに関する議論を行うという訓練をするのですが、議論を通じて何かを決めていくというプロセスでは、学ぶことも多いようです。チームビルディング的な要素も多分にあり、フェロー同士、あるいは講師とも仲良くなり、その後もSNSなどでやり取りが続いていたりする人達もいるようです。

人材育成は、JPNICにおけるインターネット基盤整備事業の中で、これからもっと重要な位置を占めるのではないかと考えていて、JPNICとしてもこのAPIGAに対する日本からのフェロー参加促進をはじめとして、何らかの事業推進ができないか、検討しようと考えているところです。

G7・G20エンゲージメントグループについて

2019年の6月28日(金)～29日(土)に大阪でGroup of Twenty(G20)が開催され、直近の8月24日(土)～26日(月)に主要国首脳会議(Group of seven, G7)が先日フランスで開催されました。G7やG20には、例えば「Business 20(B20)」など関連する多くの*20および*7が存在し、これらはエンゲージメントグループと呼ばれます。エンゲージメントグループは、各国政府から独立した、国際社会におけるステークホルダー(企業、非営利団体、市民団体等)により形成された団体で、G7/G20で議論される各分野について、提言の発表などを主に行っています。

ここでは、G7に関連する主なエンゲージメントグループを簡単にご紹介します。

○Business 7(B7)
G7と連携する公式プラットフォームを目指していて、G7各国の経済団体が集まり、企業活動およびグローバルな貿易活動に影響を及ぼす、包括的なテーマに関して勧告を作成しています。

○Civil 7(C7)
G7諸国の市民社会組織や、国際連帯関係者が主に集まるエンゲージメントグループで、G7諸国の非政府関係者の提言を国家指導者に対し、政府の説明責任として幅広く推進することを目指しています。

○Labour 7(L7)
労働者の利益を代表し、G7に先立ち労働組合運動の主要メッセージを伝えるエンゲージメントグループで、G7各国の主要な労働組合の集まりとなっています。

○Science 7(S7)
科学アカデミーが毎年集まり、重要課題に関する共同声明を準備するエンゲージメントグループです。

○Think Tank 7(T7)
研究機関が集まり、主要なテーマに関する分析と提言を表明するためのエンゲージメントグループです。

○Women 7(W7)
女性および少女の権利問題に取り組むG7諸国と途上国の市民社会組織の集まりで、ジェンダー平等が一般市民にとって目に見える課題となることを目標として掲げています。

○Youth 7(Y7)
グローバルガバナンスに関する課題への取り組みを希望する、主にG7諸国出身の若者が集まるエンゲージメントグループです。

G7に関連したエンゲージメントグループをご紹介しましたが、G20にも同様のグループが存在します。これらのエンゲージメントグループについて、より詳しく設立目的や主な活動内容等をまとめた記事を、JPNICブログにて公開しています。詳しくは次のURLをご覧ください。

G7・G20エンゲージメントグループについて
https://blog.nic.ad.jp/2019/2935/

gTLD「.amazon」問題の状況

「.amazon」というgTLDの申請に関して、米国発祥のオンライン小売企業Amazon.com, Inc.(以下、アマゾン社)とアマゾン協力条約機構(ACTO/OCTA)との間で、7年にもわたり係争が続いています。gTLD「.amazon」は、2012年にICANNが募集を行った、いわゆる新gTLDの申請の一つです。この時の募集では、国および都市名gTLDの申請の場合は、当該自治体による支持もしくは反対しない旨の表明が必要でした。しかし、.amazonについては新gTLDの審査基準を記載した「新gTLD申請者ガイドブック」に該当する明確な基準はなく、後付けで議論が進んだのが実情と言えます。

この7年間の経緯と、その間に行われた、アマゾン社とACTO、ICANNなど関係者による対応状況などをまとめた記事を、JPNICブログにて公開しています。対立点である、アマゾン社とACTO側の主張などをわかりやすく表にまとめていますので、次のURLからぜひご覧ください。

.amazon gTLD問題の状況
https://blog.nic.ad.jp/2019/2599/