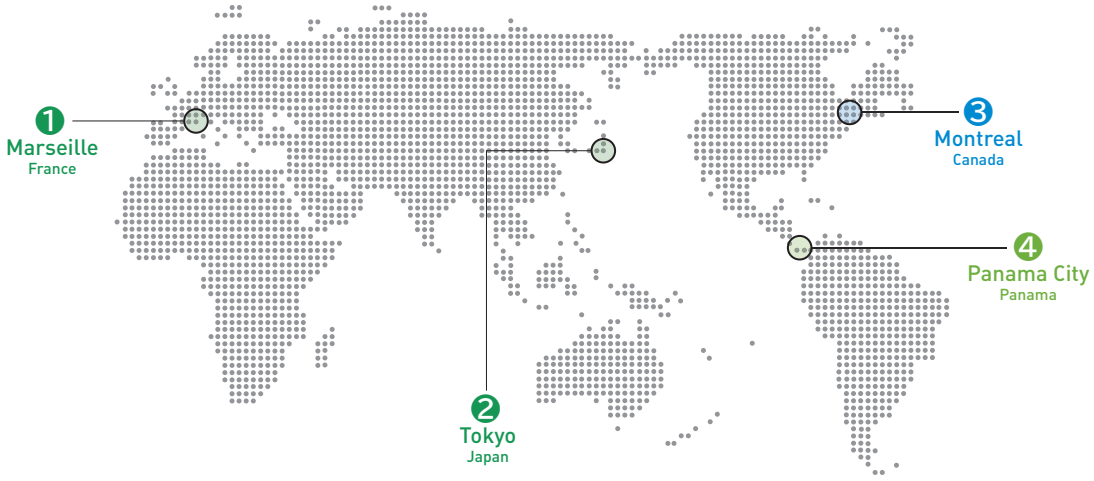
インターネット動向紹介
INTERNET TRENDS INTRODUCTION



インターネット動向紹介

IPアドレストピック

❶ 2018.5.14▶5.18
フランス/マルセイユ
第76回RIPEミーティング

❷ 2018.6.19 日本/東京
第34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、2018年5月中旬にフランスのマルセイユで開催された第76回RIPEミーティングの様子と、2018年6月19日に開催された第34回JPNICオープンポリシーミーティングを中心に取り上げます。

第76回RIPEミーティングの動向

◆ カンファレンスの概要

第76回RIPEミーティング(RIPE 76)は、2018年5月14日(月)～18日(金)にフランス・マルセイユで開催されました。

RIPEミーティングでは、その時々で最新の内容が取り上げられ、参加者による活発な議論が繰り広げられるのが特徴です。ここでは、アドレスポリシーの議論についてご紹介します。

なお、RIPEミーティングは、全体会議、各種ワーキンググループ(WG)によるセッション、チュートリアルおよびBoFにより構成されています。各セッションの構成は、RIPE 76のWebサイトからご覧ください。

RIPE 76 Meeting Plan
https://ripe76.ripe.net/programme/meeting-plan/

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・音声なども、まとめて公開されています。

RIPE 76 Meeting Archives
https://ripe76.ripe.net/archives/

また、RIPE 76の様子は、JPNICブログでもご紹介していますので、併せてご覧ください。

RIPE 76がマルセイユで開催されました
https://blog.nic.ad.jp/blog/ripe76-policy-proposal/

RIPE 76の開催地となった港町マルセイユ

◆アドレスポリシー提案について

RIPE 76では、4点の提案について議論が行われました。提案内容について議論と併せてご紹介します。

【1】2017-02：Regular abuse-c Validation
（"abuse-c"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）
https://www.ripe.net/participate/policies/proposals/2017-02

2017-02は、RIPE NCCのデータベース中で"abuse-c"または"abuse-mailbox"の項目に登録された電子メールアドレスについて、機能しているかどうかの定期的な確認を目的とした提案です。なお、"abuse-c"や"abuse-mailbox"とは、WHOIS情報で、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登録するための項目です。

ML上や複数のオフラインミーティングで議論が重ねられてきた提案のため、質疑応答での会場からのコメントは多くありませんでした。コメントの中心は、RIPE NCCから伝えられた無効な電子メールアドレスの数に対するものでした。10～25%程度といった幅のある予測ではなく、もう少し精緻な数を調べて、その内容を元に議論した方が良いのではないかという趣旨でした。

RIPE地域におけるポリシー策定プロセスでは、提案に対するコンセンサスの確認はMLにおいて行うこととなっています。この提案は、提案内容をポリシー文書に反映するために、ML上でコミュニティに対して最終の意思確認を行う、ラストコールの状態となっていました。

今回の議論はラストコールを取り下げるほどの内容ではないと判断したチェアからは、ML上でのラストコールを継続する旨の宣言がありました。

現在、RIPE NCCをはじめとする各RIRでは、abuse-cを含むWHOIS登録情報の正確性に関する議論が盛んに行われています。2018年4月に開催された北米地域を管轄するARINのミーティングにおいても、WHOIS登録情報の正確性向上を目的とした提案について、議論が行われました。詳細は次のURLをご覧ください。

News & Views vol.1592「ARIN 41ミーティング報告」
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2018/vol1592.html

中南米地域を管轄するLACNICでは、RIPE地域とほぼ同様の内容で提案が提出されており、その提案について議論が行われています。また、RIPE NCCのポリシー担当マネージャーからは、WHOIS登録情報の正確性に関する提案の位置づけで、アフリカ地域を管轄するAFRINICでの提案について説明が行われていました。このAFRINICの提案では、無作為に抽出した割り当て情報について、その割り当て情報に含まれるIPアドレスの利用状況を確認するそうです。AFRINICからの問い合わせに対して、割り当て先組織から返事がない場合や、その割り当てがIPアドレスの分配ポリシーに従った割り当てであることが確認できない場合には、割り当てを取り消すといった内容です。

また、会場の参加者からは、APNICフォーラムへも提案の提出を予定している旨の発言もありました。2018年9月にニューカレドニア・ヌメアで開催されたAPNIC 46カンファレンスにおいて、WHOIS登録情報の正確性向上に関する議論が行われました。詳細については、次号にて取り上げる予定です。

【2】2018-01:Organisation-LIR Clarification in IPv6 Policy
（IPv6アドレスポリシーにおける"Organization"と"LIR"の明確化）
https://www.ripe.net/participate/policies/proposals/2018-01

2018-01は、IPv6アドレスのポリシー文書に記述されている"Organization"と"LIR"の記述を明確にすることを目的とした提案です。

現在有効なIPv6アドレスに関するポリシー文書では、アドレスの分配先を表す用語として"Organization"と"LIR"の記述が混在していると提案者は指摘しています。この混在した記述を"LIR"に統一するよう修正することが目的の一つとして挙げられています。また、IPv4アドレスに関するポリシー文書とIPv6アドレスに関するポリシー文書では、用語の利用方法が異なっていると提案者は分析しています。

今回はこの"LIR"の用法を、IPv4アドレスに関するポリシー文書と揃えることで、IPv6アドレスの分配の際にも、1組織が複数のLIRを登録可能と解釈できるようにしたいと提案者は説明していました。RIPE NCCからは、この提案内容の分析において、現在有効なIPv6アドレスに関するポリシーでも既に対応は可能としており、現時点で、700メンバーが複数のLIRの登録を行っているそうです。

すべてのRIRで統一された内容のIPv6アドレスに関するポリシー文書は、約15年前に制定されました。文書の制定当初は"LIR"の概念を持たないRIRもあったことから、現在のポリシー文書のような記述になっていると、会場からコメントが出されていました。

"LIR"という用語の定義を正しく理解する必要性についてのコメントや、他の文書での用語の使われ方と整合を取る必要があるのではないかといったコメントも見受けられました。この提案は議論を行うフェーズのため、今後もMLや次回以降のオフラインミーティングの場で議論が行われます。

【3】2018-02：Assignment Clarification in IPv6 Policy
（IPv6アドレスポリシーにおける割り当ての明確化）
https://www.ripe.net/participate/policies/proposals/2018-02

2018-02は、割り当てを受けたIPv6プロバイダ非依存アドレスについて、再割り当てとするケースを明確化することを目的とした提案です。「ゲストネットワークやVPNなどにIPv6アドレスを割り当てるような特定の用途では、再割り当てとみなさない」とする内容を追加するものです。

IPv6アドレスに関するポリシー文書の該当部分は、この提案が議論される前に、2016-04の提案として議論され、変更された内容です。2016-04での議論を行っていた際に、さらなる修正が必要とされていました。また、RFC8273（Unique IPv6 Prefix per Host）が2017年12月に発行され、このRFC8273に準拠したIPv6アドレスの割り当てについても、ポリシー文書には考慮して記載する必要があると考えている、と提案者から説明がありました。

このような背景もあり、2016-04での提案に基づいてポリシー文書が改定されるのを待ってから、改めてポリシー文書を改定する提案を行ったようでした。今回のように、該当部分が立て続けに変更になる提案はとても珍しいかもしれません。提案者は、IPv6アドレスの現在の利用実態に合わせて、今回対象となった文書以外にも、他の文書についても修正の必要性を強く感じているようでした。

提案者が、再割り当ての定義が不足していると強く主張する一方で、会場からは、ポリシー文書を変更する必要性について疑問を示すコメントが出されていました。

【4】2018-03：Fixing Outdated Information in the IPv4 Policy
（IPv4アドレスポリシーにおける利用されていない情報の修正）
https://www.ripe.net/participate/policies/proposals/2018-03

2018-03は、IPv4アドレスに関するポリシー文書中で、古くなった情報を修正／削除することを目的とした提案です。提案には二つの項目が含まれています。一つ目は参照先のRFCを修正することです。二つ目は、RIPE NCCのデータベース中で割り振り／割り当てIPv4アドレスに関する情報に登録された、そのアドレスの状態を表す情報（ステータス）について、現在利用されておらず不要となったステータスを削除することです。

提案者による発表後の質疑応答では、参照するドキュメントについてのコメントがありました。この提案についても2018-02と同様に、議論の初期フェーズにあり、WGによる作業が続けられています。


RIPE 76の様子

◆RIPE 76以降のミーティングについて

RIPE 77は、2018年10月15日（月）～19日（金）に、RIPE NCCのオフィスのあるオランダ・アムステルダムで開催されました。また、その次のRIPE 78は、2019年5月20日（月）～24日（金）に、アイスランド・レイキャビクでの開催が予定されています。

第34回JPNICオープンポリシーミーティングの動向

2018年6月19日（火）に、東京都千代田区のJPNIC会議室にて、第34回JPNICオープンポリシーミーティング（JPOPM34）が開催されました。JPOPMは、日本におけるIPアドレスおよびAS番号の管理に関するポリシーを検討し、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。なお、JPOPF運営チームは、以前ポリシーワーキンググループ（ポリシーWG）と呼ばれていましたが、2017年6月21日（水）のJPOPM32において、関連するポリシー提案が行われ、コンセンサスに至り、2017年12月20日（水）に名称変更となりました。JPOPM32での提案内容や経緯は、次のWebページをご参照ください。

032-02：JPNICにおけるIPアドレスポリシー策定プロセスの改定の提案
http://jpopf.net/p032-02-v2

JPOPM34では、ポリシー提案が3件、情報提供が8件ありました。ポリシー提案を中心に当日の議論をご紹介します。資料や議事録は、次のWebサイトからご覧ください。

第34回JPNICオープンポリシーミーティングプログラム
http://jpopf.net/JPOPM34Program


JPOPM34でのコンセンサス確認の様子

◆ポリシー提案について

◎[034-01] Final /8（103/8）ブロック枯渇対応

現在、APNICおよびJPNICでは、最後の/8（Final /8とも言われ、103/8のブロックから分配が行われます）相当のIPv4アドレスプールからの割り振りと、IPv4アドレス返却プールからの割り振りの二つを受けることが可能です。

本提案は、約2年後と予測されている最後の/8相当のIPv4アドレス（103/8）在庫枯渇後の対応について、

- 最後の/8相当のIPv4アドレスプールに待機リストを新設し、103/8アドレスの返却があった際に待機リストの順に割り振り・割り当てを実施する
- 上記アドレスプールおよびその他のIPv4アドレス返却プールからの割り振り・割り当てサイズを、枯渇後には現在の/22から/24に変更する

と定めるものです。

本提案は、APNIC Policy-SIGにおいて継続議論となっているもので、提案者より過去のAPNICでの提案や議論の経緯について説明がなされました。会場からも活発な議論が展開されましたが、考慮すべき事項が多く提案内容全体のコンセンサスを取ることが困難だったことから、

1. 枯渇時のポリシーを明確にしておくべきか
2. 返却用アドレスプールと103/8アドレスプールをマージすべきか
3. 2.でマージするとなった場合、枯渇後にIPv4返却アドレスの待機リストを引き継ぐべきか
4. 枯渇後の割り振りサイズを縮小させるか

の4点について採否を実施しました。その結果、1.の枯渇時のポリシーを定めることについてはコンセンサスとなり、2.以下の具体的な内容については継続議論となりました。

◎[034-02] 割振・割当 IPv6アドレスの広告

本提案は、IPv6アドレスの分配(割り振り・割り当て)を受けた組織が、分配を受けたIPv6アドレスを分割して経路広告をする場合に、分配を受けたサイズ(経路長)での経路広告も行うことを推奨するというものです。

賛成反対双方の意見や、経路広告という運用課題をアドレスポリシーで定義すべきか、過去の事例などを踏まえて明確にすべきといった意見が会場より出されました。採否の結果、賛成反対が拮抗し、コンセンサスに至らず継続議論となりました。

◎[034-03] IPv6の逆引き設定

IPv6アドレスを割り当てたコンシューマーユーザーから逆引き委譲の請求が無い場合には、割り当て元のアドレス保持者が逆引きDNS登録を実施することを必須とする提案です。

会場からは、逆引き委譲がされていないプリフィクスに対して、割り当て元事業者が一律に逆引きを設定することに対する懸念などが表明されました。採否の結果、賛成反対は拮抗しましたが賛否の意見を持たない参加者が過半数を占め、継続議論となりました。

◆次回 JPOPM35について

2018年11月28日(水)に、Internet Week 2018の同時開催イベントとして、東京・浅草橋のヒューリックホール&カンファレンスで開催を予定しています。

◆情報提供プログラム：IPv4アドレスの枯渇・移転制度開始前後で経路はどう変わった？

エヌ・ティ・ティ・コミュニケーションズ株式会社の吉田友哉氏から、IPv4アドレスの在庫枯渇やアドレス移転制度が制定されたことによる、インターネット上のIPv4経路数への影響に関する調査結果が発表されました。

JPNICでは2011年8月より国内での移転が、また2013年6月より国際移転が可能になりましたが、結論としてこの前後で経路数の増減に大きな変化は見られませんでした。つまり、移転が実施されたことによる経路増大への影響は軽微であったということです。

しかし、移転されたプリフィクス数とそれらが広告されている経路数を比較すると3倍超となっており、APNIC地域全体の経路数の伸び(約1.1倍)と比べ大きくなっているため、今後移転されたプリフィクスが増加すると全体の経路数増加の要因になることが懸念されます。

また、APNIC地域で/24のプリフィクス長で広告されているアドレスレンジの内訳を見ると、最後の/8相当のIPv4アドレス(103/8)から/24で広告されている数が、約2万経路と他のレンジより圧倒的に多いことがわかりました。今後当面の間は、103/8からの広告が経路の増加要因となりそうですが、103/8自体の残数が少ないことから、最大で3万経路程度までの増加にとどまるのではないかとの見解が示されました。

JANOG42ミーティングでの発表

JPNICは、現在株式会社インターネットイニシアティブと共同で、「Pool Protection Project (PPP)」と名づけたプロジェクトに取り組んでいます。PPPでは、JPNICの管理する未分配のIPv4アドレスを利用して、そのアドレスに関する経路情報がインターネット上でどのように観測されるのか、どのようなトラフィックが観測されるのかを日々モニタリングしています。不正利用と思われるケースが見受けられた際には、該当の組織に連絡を行っています。監視されていることが広く知れ渡ることで、不正利用を未然に防ぐ効果が出ることを期待しています。

2018年7月11日(水)～13日(金)に、三重県・津市で開催されたJANOG42ミーティングで、JPNICから「あなたのIPv4アドレス、狙われていませんか？」と題したセッションを応募し、発表を行いました。PPPの取り組みの他、IPアドレスの不正利用に関しての最新の事例を紹介しました。JPNICブログに発表の様子を掲載していますので、ご覧ください。

あなたのIPv4アドレス、狙われていませんか？
～JANOG42ミーティングでの発表から～
https://blog.nic.ad.jp/blog/janog42-report-ppp/

World IPv6 Launch 6周年

Internet Society(ISOC)の提唱により、この日を境にIPv6にデフォルトで対応しようという呼びかけである、"World IPv6 Launch"がスタートしたのが、2012年6月6日でした。2018年で6周年となりましたが、日本におけるIPv6を取り巻く環境がどのように変化したかまとめたものを、JPNICブログで公開しました。IPアドレスやネットワークの他、携帯サービスやホームルータの対応状況も含めた網羅的な内容となっていますので、ぜひご覧ください。

また、JPNICのIPv6アドレス分配状況をまとめたブログ記事も公開しています。こちらも併せてご覧ください。

6th Anniversary of World IPv6 Launch ~ 日本のIPv6普及状況 ~
https://blog.nic.ad.jp/blog/june6_ipv6/

JPNICのIPv6アドレス分配を振り返る
https://blog.nic.ad.jp/blog/ipv6alloc/

インターネット動向紹介

技術トピック

❸ 2018.7.14▶7.20　カナダ/ モントリオール　第102回IETFミーティング

技術関連の動向として、第102回IETFミーティングに関するトピックと、2016年から行われていたルートゾーンKSKロールオーバーに関する話題についてご紹介します。

第102回IETFミーティング BoFおよび全体会議報告


モントリオール会合の様子

第102回IETFミーティング(以下、IETF 102)は、2018年7月14日(土)から20日(金)にかけて、カナダのモントリオールにあるホテル、フェアモント・クイーンエリザベスで開催されました。

IETF 102は、元々はサンフランシスコで開催される予定でしたが、2017年にプラハで開催された第99回IETFミーティングの場において、モントリオールでの開催に変更されました。米国への入国審査が厳しくなりつつある状況を受けての変更決定でしたが、この影響により会期日程が1週間前倒しとなりました。また、会期中にはFIFAのワールドカップが行われていたため、ハッカソン会場で試合を見ている人が現れたり、併催のミーティングの時間が変更されたりしていました。

本稿では、BoFと全体会議という二つのトピックを中心に、IETF 102の模様をご紹介します。

■ BoF

IETF 102では、BoF(Birds of a Feather - 特定のトピックについて集まる会合)は三つ行われました。

○DNS Resolver Identification and Use(driu)

DoH(DNS over HTTPS)やDoT(DNS-over-TLS)が現れることで、端末におけるDNSサーバを指定する方法が、IPアドレスだけではなくなってきました。DHCPやDHCPv6でネームサーバの情報を配布するにはどのようにすればいいのか。そのような観点を発端に、いくつもの論点が挙げられて議論されました。HTTPSやTLSが使われるということは、TLSのサーバ認証が行われるということであり、セキュリティの観点での議論も必要です。会場では、DHCPでネームサーバ情報を配布する場合のセキュリティや、クラウド事業者などから提供された複数のDNSサーバのリストがある時に、どのように選択するかといった実現方法について議論されました。

このBoFの議論について、JPNICブログで補足と解説を行っていますので、ご覧いただければと思います。

DNS over HTTPSとDHCP －IETF102における議論－
https://blog.nic.ad.jp/blog/dns-driu/

DNS Queries over HTTPS(DoH)
https://datatracker.ietf.org/doc/draft-ietf-doh-dns-over-https/

○国際化に関わるレビュープロセス(i18nrp)

IETFの中で、国際化ドメイン名(IDN)などの、アルファベットではない文字列についてドキュメントレビューをする人が、少ないという問題が起きています。このBoFでは、チームを作ってレビューするドキュメントを選択することなどが提案されていました。MLを作ってディスカッションが続けられる模様です。

IETF-102:i18nrp
https://datatracker.ietf.org/meeting/102/session/i18nrp

○The label“RFC”(rfcplusplus)

IETFでのRFC化までのプロセスとしては存在しないはずの、例えばWGに属さないPS(Proposed Standard) RFCがあるという指摘がありました。RFCとひとくくりに言っても、そのプロセスによって意味が異なります。ただ、BoFに同席していたエリアディレクターを含めて、会場では今後何か対策を採るべきといった意見は挙がりませんでした。

なお、このBoFとは別に、IAB(Internet Architecture Board)のRSOC(RFC Series Oversight Committee)という委員会が、RFCのメタデータや新たな形式を検討しています。

IETF-102 : rfcplusplus
https://datatracker.ietf.org/meeting/102/session/rfcplusplus

RFC Editor Program: The RSOC
https://www.iab.org/activities/programs/rfc-editor-program/

■ 全体会議からのトピック

○ジョン・ポステル賞 - スティーブン・フーター氏

ジョン・ポステル賞(Jonathan B. Postel Service Award)は、技術面やリーダーシップの発揮といった、コミュニティに対して貢献の

あった人や組織に贈られるもので、毎年ISOCによって選出されます。今回の受賞者は、非営利法人NSRC(Network Startup Resource Center)のディレクターである、スティーブン・フーター(Steven G. Huter)氏です。NSRCにおいて、120ヶ国以上でインターネットの発展に、文化の壁を越えて貢献したことが認められました。NSRCは1992年に設立された非営利組織で、インターネットの普及のための援助やトレーニングのためのワークショップの開催、Routeviewsのようなインターネット運用に役立つツールの開発プロジェクトを推進しています。

○会場での議論

会場から自由な意見が述べられるオープンマイクの時間には、「BoFが2回に制限されているのを撤廃すべき」「座って議論する場所が多かったので、またこの会場で開催して欲しい」「アジア開催時の旅費が厳しい」といった意見が挙げられました。

BCP25(RFC2418)によると、BoFの開催は2回に制限されています。この制限を避けるために、サイド・ミーティングと呼ばれるミーティングが開催されています。しかし、そのオンライン中継はなく、またIETFのアジェンダページには載らないといった点が、悩ましいということのようです。ただ、実際には2回以上開かれているBoFがあるという情報もあり、オンライン中継やアジェンダの見え方(一部ではGitHubが使われています)などを踏まえて、ミーティングの形態を考える必要がありそうです。また、アジア開催の旅費については、一つの地域の視点ではなく、複数の地域からの視点で痛みを分け合う必要があると、IAOCから回答が行われていました。

次回のIETF 103は、2018年11月3日(土)から9日(金)まで、タイのバンコクで開催されます。

詳細なレポートは次のURLをご覧ください。
第102回IETF報告　[第1弾]全体会議報告
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2018/vol1614.html

第102回IETFミーティング セキュリティエリア関連報告

セコム株式会社IS研究所の伊藤忠彦様より、セキュリティエリアのTRANS WGにおけるCTに関する議論についてご報告いただきましたのでご紹介します。

■ TRANS WGとは

IETF TRANS(Public Notary Transparency) WGは、2014年に設立された、CT(Certificate Transparency)に関する検討を行うWGです。CTとは、認証局が証明書を発行した際のログを、公開のログサーバに登録することで、証明書発行の透明性を確保する仕組みです。

■ CT技術誕生の背景

CT技術登場の背景としては、認証局から不正に証明書が発行されるインシデントが相次いだことが挙げられます。2011年頃から、認証局に対する不正アクセスや運用上のミスによって、本来発行してはならない証明書が不正に発行されるという事件が相次ぎました。そして、その中にはGoogleやYouTubeなど、メジャーサイトに対する証明書も含まれていたことが発覚しました。Webブラウザは Webサイトの証明書を検証し、サイト利用者はその証明書の情報(記載事項)に基づいてWebサイトの運営者を確認します。そのため、証明書の不正発行は、フィッシングなどの悪用につながりやすくなります。このような事件を受けて、認証局の証明書発行という行為は、高いリスクと影響力を潜在的に持つという認識が広がりました。

証明書の不正発行がもたらすインシデントに対応するべく、2013年にGoogle社がCTという概念を提唱しました。Transparencyという言葉にあるように、CTは証明書発行の透明性を確保する仕組みです。CTは2013年に、RFC6962※1として仕様が定められました。

■ CTの仕組み

CTでは、認証局が証明書発行を行う際に、公開されているCTログサーバに対して、証明書発行の記録を登録します。ドメイン名の登録者はCTログサーバを監視することで、自身の持つドメイン名に対する証明書を、不正に発行している認証局が存在するか否かを確認することができます。また、一部のWebブラウザでは、証明書検証の際にCTログサーバにログ(CTログ)が存在するかを確認し、存在しない場合は警告を行います。

CTを利用して証明書発行プロセスを透明化することにより、認証局の不適切な証明書発行が行われた場合、それを確認することができます。しかし、認証局が発行するすべての証明書がCTログサーバに登録されるため、公開することを前提とせずに利用されていたサーバ証明書等も、公開されてしまうという問題点もあります。

■ IETF 102 TRANS WGにおける議論

IETF 101では、TRANS WGは開催されなかったため、今回のWGは8ヶ月ぶりのWGとなりました。その期間において、Certificate Transparency Version 2.0(CT V.2)※2に関するドキュメントの整備は、メーリングリストにて大きく進みました。今回、WGにおける議論は、CT V.2策定後に、CT V.2を実装・運用する時期や、その運用で得た知見をいかにIETFへ還元するか、といったものでした。IETF 102のTRANS WGでは、あまり多くの議論は行われませんでしたが、以降、それらの動向の裏で、私が行っていた活動を紹介いたします。

■ CT適用の例外規定に関する議論の行方

IETF 100(2017年11月)以前は、Google社はChromeブラウザにおいて、署名検証を行う際にPublic Root認証局から発行されるすべてのサーバ証明書について、CTログサーバに記録されているログを確認する方針でした。CTログをWebブラウザがどのように扱うのかに関しては、Webブラウザでトップシェアを占める、Chromeの提供元であるGoogle社の意向に大きく左右されます。また、何社かの認証局が、特定の企業内ネットワークに

※1 RFC6962"Certificate Transparency"
https://tools.ietf.org/html/rfc6962

※2 Certificate Transparency Version 2.0
https://datatracker.ietf.org/doc/draft-ietf-trans-rfc6962-bis/

おけるCT適用除外や一部ログ情報の部分的削減を要望しましたが、それらの要望をGoogle社は受け入れない見通しでした。

その経緯から判断する限りにおいては、Google社はCTログ登録に例外を認めず、あらゆるサーバ証明書に対して適用すべきと考えているように見受けられました。しかし、それらの判断は一般的なWebサイト向け証明書の発行を前提とした判断であり、IoT向けの証明書発行を考慮した判断ではありませんでした。

そこで私は、IETF 100にて、大量のIoT機器向け証明書がCTログサーバに登録された場合、CTログサーバのスケーラビリティという点で問題が発生し得る点を指摘し、その問題解決策を提案しました。これは、Google社が管理するWebブラウザの仕様で解決を行うのではなく、IETFの規定するログサーバの仕様で解決を図るものでした。

その後、CA/Browser Forumに参加する何社かも交え議論を行い、紆余曲折の末、Google社もCT適用除外規定の有用性を認めました。そして、Google社は、適用除外機能はCTログサーバ機能ではなく、Webブラウザの機能で実装することが適切であると判断しました。その後Google社は、2018年6月にChromeブラウザの機能として、CT適用除外機能を設けたことを発表しました。この機能は、すべてのIoT機器に発行される証明書に対して適用することはできないものの、CTログサーバに無用なスケーラビリティが求められないこととなりました。そして、当該機能はログサーバで解決しなくても良いものとなり、CT V.2には盛り込まないこととなりました。

■ おわりに

これまでの活動により、CTの適用除外規定を通し、IoT機器へ証明書を発行する上での、課題の一部を解決することができました。今回制定された除外規定は、どのようなIoT機器にも適用可能というわけではありませんが、悪用されるリスク等を考慮すると、現状において妥当なものであると考えています。今後、CT V.2策定後に、運用結果等も踏まえ、実社会への影響度合い等を加味し、より多くのIoT機器で証明書が利用可能な仕組み作りに取り組みたいと考えています。

詳細なレポートは次のURLをご覧ください。
第102回IETF報告 セキュリティエリア関連報告
～TRANS WGにおけるCTに関する議論について～
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2018/vol1615.html

第102回IETFミーティング IoT関連報告

株式会社レピダムの永田貴彦様よりIoTに関連するいくつかの標準化動向についてご報告いただきましたのでご紹介します。

■ はじめに

日本政府の科学技術基本法第5期で、基本指針の一つとして「Society 5.0(ソサエティ 5.0)」[※3]が提唱されるなど、IoTがますます注目を集めています。総務省のIoT機器に関する脆弱性調査等[※4]では、生活に密接に関わる重要インフラで利用されるIoT機器でも、多くの機器で脆弱性が検出されるなど、サイバー攻撃の脅威への対策が不十分である実態が浮き彫りとなりました。

IoTにおける課題にはさまざまなものがありますが、そのうちの一つがファームウェアやソフトウェアの安全な管理です。ここに位置づけられる検討がIETFでも行われており、本稿ではIETF 102で特に注目されていた、セキュリティ・エリア(SEC)のSUIT WGとTEEP WGを紹介します。SUITとTEEPは密接な関係がありますが、SUITがファームウェア更新、TEEPが信頼できる実行環境(TEE)でのアプリケーションの配備に焦点を当てており、住み分けがされています。

また関連する話題として、アプリケーション・アンド・リアルタイム・エリア(ART)から、CBOR WGを紹介します。

■ IETF標準化動向：SUIT

○SUITとは

SUITは「Software Updates for Internet of Things」の略であり、IETF 100で最初の会合(BoF)が実施されました。SUITでは、リソース制約が非常に厳しいデバイスにも適用可能なファームウェアアップデートについて議論しています。

SUITでは次の二つについて標準化を行っており、それぞれインターネットドラフト(I-D)として、投稿されています。

1. ファームウェアイメージの転送メカニズム
2. ファームウェアイメージに関するメタデータを提供するマニフェスト、end-to-endでイメージを守るための暗号化情報

○SUITの標準化動向

次に、IETF 102を含めたSUITの標準化動向を三つ紹介します。

1. IETF 102 hackathon

SUITは、今回初めてhackathonに参加しましたが、リモート参加を含めて19名が参加するなど非常に盛況でした。また、best projectの一つに選ばれるなど、注目を集めていました。

2. SUIT Architecture

SUITアーキテクチャでは、ファームウェアアップデートのアーキテクチャが「A Firmware Update Architecture for Internet of Things Devices」[※5]としてまとめられています。SUITアーキテクチャでは、SUITで満たすべき要件が10個定義されており、情報セキュリティのCIA(「機密性(Confidentiality)」「完全性(Integrity)」「可用性(Availability)」)の観点で、幅広く要件が挙げられています。

※3 ソサエティ 5.0 - 政府広報オンライン
https://www.gov-online.go.jp/cam/s5/

※4 総務省｜IoT機器に関する脆弱性調査等の実施結果の公表
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000154.html

※5 A Firmware Update Architecture for Internet of Things Devices
https://datatracker.ietf.org/doc/draft-ietf-suit-architecture/

※6 Firmware Updates for Internet of Things Devices - An Information Model for Manifests
https://datatracker.ietf.org/doc/draft-ietf-suit-information-model/

3. SUIT Information Model
これは、マニフェスト用の情報モデルです。マニフェストに必要な項目をピックアップしたものが「Firmware Updates for Internet of Things Devices - An Information Model for Manifests」[※6]のI-Dとして整理されています。脅威モデルを基にセキュリティ要件のリストアップ、およびユーザーストーリーを基にユーザビリティ要件のリストアップを行っており、これらを整理した結果をマニフェストの項目としてまとめています。

■ IETF標準化動向：TEEP

○TEEPとは

次に、IoTセキュリティ関連のWGからTEEPを紹介します。

TEEPは「Trusted Execution Environment Provisioning」の略であり、信頼できる実行環境(Trusted Execution Environment (TEE))での、アプリケーションのライフサイクル管理に関するプロトコルの標準化を目的としています。

TEEの具体的な実装としては、ARM社のTrustZoneとIntel社のSGXが挙げられます。TEEPでは、これらさまざまなTEEで実行される信頼されたアプリケーションに対し、ライフサイクル管理プロトコルの標準化を行っています。

TEEPプロトコルでは、次の三つの課題解決をめざしています。

1. デバイス管理者またはサービスプロバイダが、TEE環境にアプリケーションを配備する前の、デバイスのセキュリティ状態確認方法
2. TEE側からデバイス管理者またはサービスプロバイダが、アプリケーション管理権限を持っているかの確認方法
3. TEEが正しいことの保証

なおTEEPは、IoTのみにフォーカスした標準ではなく、IoTはTEEPで複数定義されているユースケースのうちの一つとなっています。

○TEEPの標準化動向

次に、IETF 102を含めたTEEPの標準化動向を紹介します。

TEEPでは、IETF 102時点で、次の二つがI-Dとして議論されています。

1. Trusted Execution Environment Provisioning（TEEP）Architecture
TEEPのユースケース、TEEなどのコンポーネント間の関連、トラストアンカー(認証の基点)、キーと証明書種別など、TEEPプロトコルの基になるアーキテクチャが定義されています。

2. The Open Trust Protocol(OTrP)
プロトコルの具体的な内容を定義しています。OTrPの目的は、さまざまなデバイスの異なるTEEで動作する、信頼されたアプリケーション(Trusted Application、TA)を管理するための、相互運用の可能な(interoperable)プロトコルを定義することです。

OTrPでは、TAM(Trusted Application Manager)とTEE間の信頼されたメッセージプロトコルを定義しており、end-to-endのセキュリティメカニズムを使用しています。プロトコルとしては大きく分けて、1.デバイス情報取得、2.セキュリティドメイン管理、3.TA管理、の三つに分類されます。

■ IETF標準化動向：CBOR

○CBORとは

CBORは、Concise Binary Object Representationの略であり、CORE、ACE、SUITなど、IETFのさまざまなWGから参照されています。現在はRFC7049が発行されており、以下の特徴があります。

- JSONフォーマットをバイナリで表現し、JSONよりもサイズが小さい
- JSONよりもデータ型の種類が多い
- CBORパーサーが小さなコードサイズにできるように設計(解析しやすいフォーマットなど)
- 拡張性のあるデータフォーマット

IoTなどリソース制約の厳しい環境向けに、CBORパーサーサイズ削減の優先度が高い点が特徴的です。また、CBORの型はMajor Typeと呼ばれ、符号なし整数、テキスト文字列、マップ、日時型など、JSONと比べてさまざまな型が定義されています。

CBORのフォーマットは、Major Typeが1byteで定義され、その後0～Nbytesで実際の値が定義されます。この1byteのMajor Typeの表現は「Initial Byte」と呼ばれ、RFCでは「Appendix B. Jump Table」にまとまっています。

○CDDLとは

CBORにおけるデータ構造記述のために、CDDL(Concise Data Definition Language)の標準化が行われています。また、JSONのデータモデルはCBORデータモデルのサブセットであるため、CDDLはJSONデータ構造の定義にも使えます。CDDLの基本的な構文はABNF(Augmented Backus-Naur Form)に着想を得ており、ABNFに近い形になっています。

■ おわりに

今回は、IETFでのIoT向けの標準化動向を紹介しました。IETFでは、IoTに関連したセキュリティやプロトコルなど、さまざまな標準化が行われていること、着実に標準化が進んでいるということが、皆様に伝われば幸いです。

詳細なレポートは次のURLをご覧ください。
第102回IETF報告 IoT関連報告
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2018/vol1617.html

ルートゾーンKSKロールオーバーが実施されました

延期となっていたルートゾーンKSKロールオーバーは、2018年10月11日、ルートゾーンのレコードに署名する鍵を変更する実際のロールオーバーが行われました。2018年10月末現在、大きなトラブルがあったという報告はなく、無事に作業が終了したと考えられます。

今後の予定としては、2019年第1四半期に元のKSKを失効する作業が行われます。

最初のルートKSKロールオーバーが正常に完了
https://www.icann.org/news/announcement-2018-10-19-ja

インターネット動向紹介

ドメイン名・ガバナンス

2018.6.25▶6.28
④ パナマ共和国 / パナマシティ
第62回ICANNパナマシティ会議

本稿では、2018年5月～9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62回ICANN（The Internet Corporation for Assigned Names and Numbers）パナマシティ会議での主なトピックについて取り上げます。また、欧州連合（EU）の一般データ保護規則（General Data Protection Regulation; GDPR）が、2018年5月25日より施行され、本パナマシティ会議でも多くの議論が行われました。その中でも、GDPRがWHOISでの情報公開に与える影響が大きな話題となっています。このWHOISのGDPR対応に関する動向についても、併せてご紹介します。

第62回ICANNパナマシティ会議

2018年6月25日（月）から28日（木）まで、パナマ共和国の首都パナマシティにて、第62回ICANN会議が開催されました。毎年6月の会議は「ポリシーフォーラム」と呼ばれるフォーマット※1での開催となっていて、コミュニティ横断セッションが数多く配置され、ポリシー議論を深化させることに重点を置いた会合です。そのため、オープニングセレモニーなどのフォーマリティを排除し、4日間という一番短い会期という簡素な仕立てです。今回のICANN会議は、欧州連合の一般データ保護規則（GDPR）が施行されて初めての会議ということで、GDPRに大きな関心が寄せられました。本稿でもこれを中心に、会議の模様をお伝えします。


パナマシティ会議の様子

◆ オープニングおよびマルチステークホルダーエートス賞授賞式

ポリシーフォーラムのオープニングは、セッション開始前の午前8時半から、ホワイエで立ったままで行うという、簡素さを強調した仕立てになっています。また、このタイミングで、ICANNコミュニティにおける貢献が顕著な人を毎年表彰する、マルチステークホルダーエートス賞の発表が行われます。

今年は、2018年3月に惜しくも事故で亡くなった、フランスのStéphane Van Gelder氏に授賞されました。Van Gelder氏は、分野別ドメイン名支持組織（GNSO）評議会の議長や、指名委員会（NomCom）議長などの要職で活躍し、コミュニティからの信望を集める人物でした。そのため、参加組織が早い時期から次々と、Van Gelder氏推薦を打ち出していました。当日は、奥様のJulieさんがご挨拶なさり、集まったメンバー全員で、故人の人柄と業績を振り返りました。

◆ GDPR施行直後のICANN会議

パナマシティ会議までの2ヶ月間は、ICANNの内外でGDPR関係の出来事がいくつか並びました。

1）2018年5月17日：gTLD登録データのGDPR適合のための暫定仕様書（TempSpec）※2を理事会が承認
2）同5月25日：GDPR施行
3）同6月18日：TempSpecでは検討待ちとなっている、非公開データ項目に対するアクセス認定要領の議論に向けた、いわゆる統一アクセスモデル（UAM）の発表

1）に関して、このTempSpecはコミュニティでの議論や意見聴取を通じて検討されたものの「暫定」に過ぎず、今後GNSOのPDP（ポリシー策定プロセス）を踏む必要があります。今回は、十分に検討範囲が限定され、かつ1年以内という短期間で仕様の正式化が求められるため、Expedited PDP（EPDP）という、初期調査などを割愛した迅速なプロセスのPDPが、初めて使われることになりました。

6月25日（月）の17時から開催された、「High Interest Session: Community Input to GNSO Expedited PDP Charter Development」は、このEPDPに関する公開セッションでした。EPDPにおいても、通常のPDPと同様、チャーターと申請書を準備した上で、作業チームの設立をGNSO評議会で承認する必要があります。このセッションは、チャーターと申請書のドラフティングチーム（DT）が、準備状況を説明した上で、コミュニティの意見を聞くものでした。七つの各セクションで、限られた時間ながら活発な質疑が交わされ、それぞれに関する検討状況が説明されました。DTメンバー、フロアからの発言者ともに、1年という限られた時間でEPDPを進めるべく、効率的、建設的に検討を進めようとしている印象を強く受けました。

3）は、GDPRへの適合のために、TempSpecの中で非公開

※1 ICANN会議の種別
6日間構成の会議A（コミュニティフォーラム）、4日間構成の会議B（ポリシーフォーラム）、7日間構成の会議C（年次総会）の3種類があります。
https://www.nic.ad.jp/ja/basics/terms/icann-meeting-strategy.html

※2 Temporary Specification for gTLD Registration Data
https://www.icann.org/resources/pages/gtld-registration-data-specs-en

とされた登録データに対して、どのような資格のユーザーに、どのような手続きでデータを提供するのかに関して、モデルの構成要素が提示され、コミュニティの議論を喚起するものです。したがってこちらも、パナマシティ会議が初の対面議論の場となりました。

会期中の6月26日(火)の17時から開催された、「Cross-Community Session: Accreditation and Access to Non-Public WHOIS Data Post-GDPR」が、この統一アクセスモデル(UAM)に関する公開セッションでした。こちらはUAMの発表が、会期の前週と直前だったことから、GNSO評議員、セキュリティと安定性に関する諮問委員会(SSAC)チェア、欧州委員会担当官、ICANN事務局をはじめとする、9人のパネリストが自身の考え方を示すセッションでした。

パネリストたちが示した重要と考えるポイントを、以下に列挙します。

・欧州委員会の担当官、Cathrin Bauer-Bulst氏：
GDPRはデータ処理を禁じているわけではなく、正当な目的に基づいて責任を持って行うことを求めている。プライバシーとデータ提供のバランスを、認定、認証、アクセス、説明責任の観点で取っていくことが重要。

・レジストリ部会のKeith Drazek氏：
認定認証とアクセスに対する法的整合性、および、その法的根拠が管轄法によって異なり得ることから、モデルが柔軟であることが重要。

・ICANN CEOのGöran Marby氏：
異なる目的の利用者は異なる要請を持っており、それを擦り合わせて「統一した」モデルを作ることが重要。

・知的財産部会のFabricio Vayra氏：
UAMは単なる議論のためのモデルであり、これから認定、認証、アクセスを行う機構を早期に構築することが重要。

また、SSACチェアのRod Rasmussen氏は、SSACが会期直前の6月14日(木)に発表した、SAC101「SSAC Advisory Regarding Access to Domain Name Registration Data」を紹介し、その中で指摘されている、RDS(Registration Directory Service)へのアクセスに関する問題点の勘案を求めました。

TempSpecにおいては、非公開データに対するアクセスは、レジストリが照会に応じて個別に処理している状況で、法執行機関、セキュリティ専門家、知的財産権専門家など、それぞれの業務のために非公開データへのアクセスが必要な立場からは、早期の解決が望まれています。多様な観点があるだけでなく、認定基準、認証方法などの詳細にもさまざまな課題があり、今後の議論に注視が求められます。

◆ 説明責任に関するコミュニティ横断作業部会の作業完了

今回のパナマシティ会議でGDPR以外に大きな節目となるものとして、説明責任に関するコミュニティ横断作業部会(CCWG-ACCT)の、作業終了が挙げられます。CCWG-ACCTは、IANA監督権限移管の議論が行われた際に、米国商務省電気通信情報局(NTIA)による監督がなくなった後の、ICANN自身の説明責任機構強化を検討するために設置されました。監督権限移管までに必要な事項を検討するワークストリーム1(WS1)が完了した後は、それ以外の内容を扱うワークストリーム2(WS2)が進行中でした。WS2はパナマシティ会議の会期中、6月24日(日)に全体会議を行い、九つの領域に関する勧告を含む最終報告書を仕上げて作業を終了しました。今後、最終報告書はCCWGに参加する各支持組織、諮問委員会に送られ、それぞれの承認を待つことになります。

◆ 第52回ICANN報告会

本パナマシティ会議での議論を紹介する報告会を、2018年9月4日(火)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パナマシティ会議概要報告
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. ルートサーバーシステム諮問委員会(RSSAC)報告
5. 次期新gTLD募集手続き検討状況報告
6. ICANN WHOIS暫定ポリシー策定プロセス検討状況
7. ICANN理事からの報告


第52回ICANN報告会の様子

本報告会の資料および音声は、次のURLで公開しています。

第52回ICANN報告会
https://www.nic.ad.jp/ja/materials/icann-report/20180904-ICANN/

◆ 今後のICANN会議

次回のICANN会議は、2018年10月20日(土)から25日(木)にかけて、スペインのバルセロナで開催される年次会合です。この内容は、2019年3月発行予定の次号71号で取り上げます。また、次々回は前号でお伝えした通り、2019年3月9日(土)～14日(木)にかけて、神戸で開催されます。

ICANN63 | Barcelona
https://meetings.icann.org/en/barcelona63

ICANN64 | KOBE
https://www.icann64.jp/

WHOISのGDPR対応に関する動向

◆ WHOISデータ収集についてのICANNによる法的措置

ICANNは、GDPR対応で個人情報の収集を止めたドイツのレジストラに対し、法的手段(仮処分申請)をドイツの裁判所に対して起こしました。本稿では、その経緯についてご紹介します。

○背景

前述の通り、2018年5月25日にGDPRが施行されるのを控えた5月17日に、ICANN理事会はICANNの各種契約およびポリシーのGDPRへの適合を目的とした、「gTLD登録データのGDPR適合のための暫定仕様書」(TempSpec)を承認しました。TempSpecでは、レジストラによる個人情報を含むデータ収集は今まで通り行い、WHOISでの表示項目を制限するとしています。具体的には、登録管理者や技術連絡担当者などの情報は表示されず、レジストラ、登録の状態、登録日および更新日のみの表示となっています。その代わり、登録者と連絡を取る必要がある場合のために、匿名化された電子メールアドレスを掲載するか、Webフォームが用意されるとしています。

○ICANNによる仮処分申請

2018年5月25日にICANNは、ドイツのICANN公認(gTLD)レジストラであるEPAG社がWHOISデータを収集するよう、ドイツのボン地裁に仮処分申請を行いました。これは、新規ドメイン名登録の際にGDPRへの抵触を回避する目的で、登録管理者および技術連絡者情報を収集しないことを、EPAG社がICANNに連絡してきたことを受けてのものです。なお、EPAG社は、このような対応を取るのは新規登録のみで、既存の情報は維持するという方針を示していました。

これに対しICANNは仮処分申請において、

- GDPR施行後の登録管理者および技術連絡担当者情報の収集がGDPRに抵触するかどうか、ICANNとEPAG社との間で認識に差がある。
- 両情報の収集はICANN-EPAG社間の契約で義務づけられたものであり、GDPRとも矛盾せず、TempSpecでもすべての登録項目の収集を義務づけている。この点についてドイツの裁判所に確認したい。
- EPAG社の行為が続けば、法執行機関、セキュリティ目的、知的財産権保持者などによる、正当な目的での完全なWHOIS登録データへのアクセスができなくなる。

というような主張をしています。

一方、GDPR発行前後にEUからICANNに送られていたレターにおいては、TempSpecに定まっていない部分があり、早急な解決が必要だという指摘がなされていました。

○地裁による仮処分申請の却下とICANNの不服申し立て

5月29日に、ボン地裁は差し止め請求を却下しました。つまり、EPAG社がドメイン名の新規登録時に、登録管理者および技術連絡者情報を集める必要はないとの判断です。しかしICANNの主張によれば、これらの情報の収集がGDPRに違反するという判断も示されませんでした。

仮処分申請却下の決定を受けて、6月13日にはICANNが不服申し立てを行いました。地裁による再検討が実施された結果、7月19日には申し立ての控訴裁送りが決定しました。それを受けたケルン高裁による判断は8月3日に下され、結果としてICANNによる申し立ては再度退けられることとなりました。その理由としては、仮処分によって保護すべき重大な損害はなく、GDPRの解釈は不要だということが示されました。

この高裁の判断が本件に関する最終判断ということはなく、ドイツの司法制度も日本と同様に三審制のため、今後ICANNがさらに連邦最高裁に上訴する可能性が残されています。

本件については、より詳しい情報をJPNICブログにて公開しています。詳細は次のURLをご覧ください。

WHOISデータ収集についてのICANNによる法的措置
https://blog.nic.ad.jp/blog/icann-gdpr-whois-legal-action/

◆ ICANNによる非公開WHOISデータへのアクセスモデル案

WHOISのGDPRへの準拠を目的として2018年2月28日にICANNが公開したモデル案では、欧州経済領域(EEA)内に存在するデータのWHOISでの公開に制限がかかり、非公開項目については認証された者のみがアクセスできるとされました。しかし、この時点では認証に関する具体的な記述はありませんでした。

この非公開WHOISデータへのアクセス方法に関して、より詳細な案である「Framework Elements for a Unified Access Model for Continued Access to Full WHOIS Data」※3が、2018年6月18日にICANNから公開されました。その後、この案をベースに、欧州データ保護委員会(European Data Protection Board、EDPB)へ照会した結果や、コミュニティから寄せられた意見を踏まえて改訂した「Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data - For Discussion」※4が、8月20日に公開されました。ここではこのアクセスモデル案についてご紹介します。

○アクセスモデル案の目的と概要

認証された利用者に対し、非公開部分も含む完全なWHOISデータへのアクセスを提供するための枠組み(統一アクセスモデル、UAM)を示して、議論を喚起することがアクセスモデル案の目的です。このUAMで記載されている内容は、5月17日にICANN理事会が承認したgTLD登録データのための暫定仕様書(TempSpec)では、今後の課題とされていたものです。

※3 Framework Elements for a Unified Access Model for Continued Access to Full WHOIS Data - For Discussion
https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-18jun18-en.pdf

※4 Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data - For Discussion
https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-20aug18-en.pdf

○利用資格

UAMを利用して非公開部分も含む完全なWHOISデータへアクセスする資格があるのは、利用規則(Terms of Use)で縛られた、正当な権利を持つ利用者グループ群、となっています。これら利用者グループの特定は、ICANNの政府諮問委員会(GAC)が行うことになっていて、法執行機関、知的財産権者、運用セキュリティ研究者、個人であるドメイン名登録者が例として挙げられています。加えて、特定の正当な目的のために、ICANN自身およびレジストラに対してUAMを通じたアクセスが承認される見通しです。

○実装方法

中央管理されたデータ置場が作られるのではなく、レジストリとレジストラがそれぞれ現在の要件に沿うものを維持することが求められています。非公開WHOISデータへのアクセスのためにRDAP(Registration Data Access Protocol)を使ってサービスを提供する必要があり、TempSpecでは2018年12月中旬までに実装が必須となっています。

UAMにおいて利用者の認証に使用される技術的な方法は、「トークンまたは証明書のシステムに依存する」となっており、それ以上の詳細は記載されていません。ICANN GNSOの提案によれば、ICANNのレジストラ用Webシステムを一時的に使うこと、および中央管理されたホワイトリストによるIPアドレスベースの制限を掛けた上でTCPポート43を使ったアクセスを許可することが提案されましたが、案では取り入れられませんでした。

○利用規則(Terms of Use)

利用規則は、UAMの下での第三者による非公開WHOISデータ利用において、遵守が求められる決まりで、特にデータ利用の適切な制限や、データアクセスの適切な手続きの策定などが想定されています。単一規則ですべてカバーするとは限らず、適格な利用者グループごとに別のものが作成される可能性もあります。

利用規則の執行および監視は認証組織体が行うこと、そのためにICANNと各認証組織体間で覚書を交わすことが想定されています。レジストリ・レジストラのUAMで要求されている事項への遵守状況は、ICANN事務局の契約コンプライアンス部門が担当します。

○アクセスモデル案を巡る論点

改訂案では、前版と比べて用語が明確に定義されたほか、認証からアクセスからまでの一連の手続きフローを図式化し、WHOISの利用者と認証機関、レジストリ・レジストラの三者関係がよりわかりやすくなるなど改善が図られましたが、依然として未解決な部分が少なからず残っています。具体的な論点は以下の通りです。

1. 利用者は個々のアクセス要請のたびに正当な利用目的を示すべきか
2. 非公開WHOISデータすべての項目へのアクセスを認めるべきか
3. 登録者からの要望があればアクセスログは提供すべきか
4. レジストリ・レジストラの両方がアクセスを提供すべきか、それともレジストラのみが提供すべきか
5. 非公開WHOISデータへのアクセスを有料とすべきか
6. 利便性の観点からWHOIS情報を一元化したポータルをICANNが運営すべきか

上記の論点に加えて、コミュニティから寄せられた意見の中で重要と思われるものを以下に列挙します。

・利用資格(Eligibility)

認証した利用者が不正行為を働いた場合や、認証基準が甘すぎる場合などを想定し、認証機関の責任が追加の論点として想定されています。

・手順の詳細(Process Details)

非公開データへのアクセスはレジストラからの提供に限定すべきという意見や、認証済みの提供者と利用者の間で重ねてアクセス同意書を締結する必要があるのかという声が挙がっています。また、アクセス権限を与える範囲についても、WHOIS項目すべてか、目的に応じた項目のみにするかで意見が分かれているほか、費用についても無償・有償どちらの声もあります。

・技術的な詳細(Technical Details)

利用者の利便性や不正利用の監視等のために、集約型のWHOISリポジトリ、もしくはWHOIS情報を一元化したポータルをICANNが運営すべき、という提案もされています。

○最後に

統一的な認証方法や基準、認証ユーザに対するデータ提供方法などの詳細が定まらない限り、各レジストリ・レジストラが手動対応を迫られることから、一刻も早い確定と実装が求められますが、前述のように課題はまだまだ残っています。

ICANNが公開したブログ記事“Possible Unified Access Model Published for Community Input”※5では、コミュニティからのフィードバックを歓迎するとして、意見受付用のメールアドレス(gdpr@icann.org)が公開されています。非公開WHOISへのアクセス方法案についてご意見のある方は、ぜひメールをお送りください。

本件については、より詳しい情報をJPNICブログにて公開しています。詳細は次のURLをご覧ください。

ICANNによるGDPRに対応するWHOISモデル案について
https://blog.nic.ad.jp/blog/icann-gdpr-whois-model/

ICANNによる非公開WHOISデータへのアクセスモデル案
https://blog.nic.ad.jp/blog/whois_unified_access_model/

ICANNによる非公開WHOISデータへのアクセスモデル案(続報)
https://blog.nic.ad.jp/blog/whois_unified_access_model-2/

※5 Possible Unified Access Model Published for Community Input
https://www.icann.org/news/blog/possible-unified-access-model-published-for-community-input