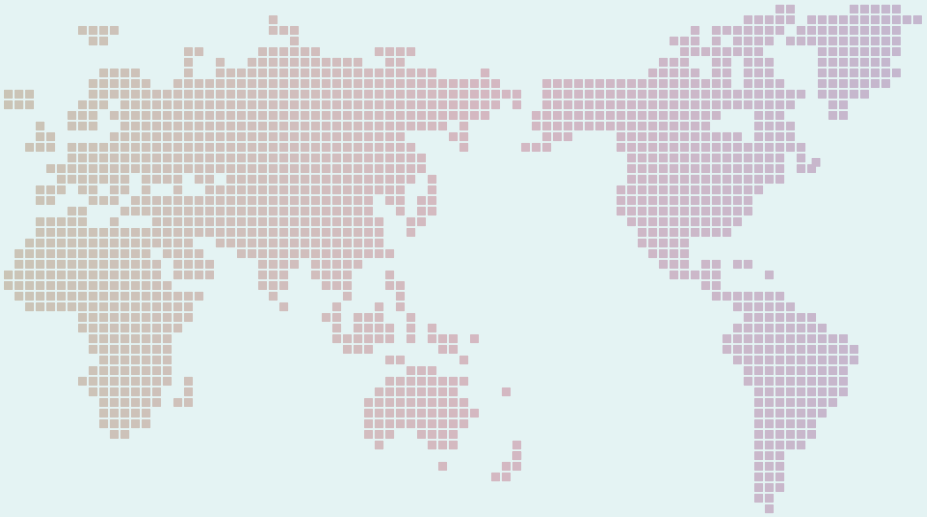
インターネット動向紹介

INTERNET TRENDS INTRODUCTION 2022.02 ― 2022.05



1 オンライン　2 オンライン　3 オンライン　4 オンライン

IPアドレストピック

INTERNET TRENDS INTRODUCTION

1 2022. 2.21 ▸ 3.3 APRICOT 2022／APNIC 53カンファレンス オンライン

2 2022. 1.20 ▸ 2.18 2021年度IPv6対応状況に関するアンケート結果レポート オンライン

IPアドレスに関する動向として、2022年2月下旬から3月上旬にかけてオンラインで行われたAPRICOT 2022／APNIC 53カンファレンス、JPNICで行った2021年度IPv6対応状況に関するアンケート結果レポートを取り上げます。

APRICOT 2022／APNIC 53カンファレンスの動向

■ APRICOT 2022／APNIC 53カンファレンスの概要

APRICOT 2022／APNIC 53カンファレンス（以下、APRICOT 2022／APNIC 53）が2022年2月21日（月）～3月3日（木）にかけて、オンラインにて開催されました。今回も新型コロナウイルス感染症（COVID-19）の流行状況に鑑み、オンラインでの開催となりました。

APRICOT 2022／APNIC 53では2月21日（月）～2月25日（金）はチュートリアルウィークとして、DDoS対応やセグメントルーティングをテーマとしたワークショップが行われ、2月28日（月）～3月3日（木）は議論の場となるカンファレンスウィークが行われました。カンファレンスウィークでは、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「AGM（APNIC General 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は動画、資料、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。

APRICOT 2022／APNIC 53プログラム
https://2022.apricot.net/program

ここでは、APRICOT 2022／APNIC 53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。

■ アドレスポリシーに関する議論の動向

今回のAPRICOT 2022／APNIC 53では3件の提案が行われました。前回のAPNIC 52ではコンセンサス形成のための意思表示に、Zoom Poll（Zoomに搭載された投票機能）のみが利用されましたが、参加者からの要望や、今後オンサイトでのポリシー SIGが再開する可能性を踏まえ、Zoom PollとConfer（https://confer.apnic.net）の両方が使用されました。2種類の投票結果を、チェアが総合的に判断しなければならないのが難しそうではありましたが、上手く取り纏めていたと思います。

ソーシャルイベントとして、オンライン参加のクイズが行われました

提案名	移転ポリシーテキストの統一（提案番号：prop-142）
提案者	Jordi Palet Martinez氏、Amrita Choudhury氏
概要	番号リソース（IPv4、IPv6、AS番号）の移転ポリシーに関する文書を統合し、一つの文書にまとめる。
議論結果	コンセンサス
提案の詳細	https://www.apnic.net/community/policy/proposals/prop-142/

APNICではポリシー文書の見直し、簡潔化をめざした取り組みとして、ワーキンググループを立ち上げ、検討を行ってきました。本提案は、その一つとして提案されたものです。現在の移転に関して規定するポリシー文書は、番号リソース別に記述されています。しかし共通する文言が多いので、統合し、より簡略化するものです。

本提案による変更として、これまでAPNICではAPNIC地域内でのIPv4アドレス移転と、RIR間でのIPv4アドレス移転のみを移転履歴として公開してきました。それが、文書統合により、「すべての移転履歴は公開する必要がある」と変わるので、M&A等による移管や、AS番号の移転履歴に関しても公開に変更になるということが懸念されました。

コンセンサス確認は、1.文書統合すること、2.移転履歴の全公開についての二つに分けて行われました。1.に関しては（移転履歴に関する部分以外に）内容的な変更は無いとして反対なし、2.に関しても正規の手続きを踏んだものであるので、公開されても問題ないだろうとの考え方が多いのか、賛成多数でコンセンサスに至りました。

提案名	AS番号のエンドユーザーへの割り当て（提案番号：prop-143）
提案者	Jordi Palet Martinez氏、Anupam Agrawal氏
概要	APNIC Internet Number Resource Policies（https://www.apnic.net/community/policy/resources）のセクション12.4項「AS番号のエンドユーザーへの割り当て」において、「申請したLIRとのコネクティビティを喪失した場合には、このAS番号を返却しなければならない」の条件を削除し、「新しいLIRから接続提供を受ける、もしくはAPNIC/NIRの会員となった場合、同一のAS番号を引き続き利用することができる」という条件を追加する。
議論結果	コンセンサス
提案の詳細	https://www.apnic.net/community/policy/proposals/prop-143/

APNICではLIRがエンドユーザーの代わりに申請を行い、AS番号の割り当てを受けることができます。ただしこの条件として、「申請したLIRとのコネクティビティを喪失した場合には、このAS番号を返却しなければならない」と定められていました。この条件はエンドユーザーが何らかの理由でコネクティビティを提供するLIRを変更したり、APNICやNIRの会員になったりする際に、AS番号を変えなければならないという不便な状況に導いてしまいます。本提案ではこれらのシチュエーションにおいて、同じAS番号を継続して使用できるように文言を変更しようという提案でした。

実装にあたり、デメリットは何ら無く、ユーザーにとって利便性を向上させる要素のみだったことから、本提案は反対なしでコンセンサスへと至りました。

提案名	実験用割り振りアドレスのリザーブプール確保（提案番号：prop-144）
提案者	Anupam Agrawal氏、Simon Sohel Baroi氏、Amrita Choudhury氏
概要	APNIC Internet Number Resource Policiesの5.7項で定められる実験用割り振りIPv4アドレスに関して、/21分をポリシー実装後5年間確保する。
議論結果	コンセンサス
提案の詳細	https://www.apnic.net/community/policy/proposals/prop-144/

APNICでは、実験用のIPv4アドレス割り振りについて、ポリシーの中で規定しています。ただし、ここでは条件を示しているだけであり、アドレスプールの確保は行われていません。IPv4アドレスの在庫が枯渇している状況下において、真に必要な際に機能しない文書になってしまっているのではないかということを危惧し、本提案は行われました。

カンファレンスの前段階では、確保するアドレスサイズが/21で適切であるかどうかが中心として議論されていました。当日も一部の方からは/19程度を求める声が上がっていましたが、そこまでの大きなサイズを求めているのは少数派のようでした。また、期間について、5年と定めているが、その間に確保したアドレスが無くなった場合は追加するのか、失効するのか、5年後にこのポリシーを継続することはあるのか等が懸念されました。

これらは議論の中で明確に対応方法を示すということは無く、その状況になった際に改めてポリシー提案等の形で議論が行われることとなりました。

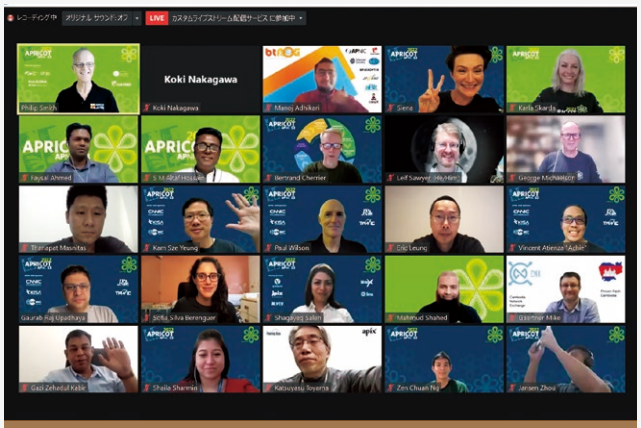
コンセンサス確認では、Conferの方で3割ほどの反対票が見られましたが、最終的にChairの総合判断によりコンセンサスが宣言されました。

■ 次回以降のAPNICカンファレンスについて

次回のAPNIC 54は、2022年9月8日～15日に開催を予定しています。APNIC事務局は次回以降のカンファレンスを、新型コロナウイルス感染症の状況次第ではオンサイトで開催することも検討しているようです。

誌面では割愛したAPRICOT 2022／APNIC 53の様子について、次のURLをご覧ください。

APRICOT 2022／APNIC 53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～
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2022/vol1908.html



オンライン開催であっても、カンファレンスがすべて終了した際の記念撮影は定番になりました

2021年度IPv6対応状況に関するアンケート結果レポート

JPNICでは2014年から毎年IPv6の対応状況について、JPNIC会員をはじめ、IPアドレス管理指定事業者とPIアドレス割り当て先組織等に対してアンケート調査を実施しています。

2022年1月20日から2月18日までの1ヶ月間、IPアドレス管理指定事業者（以下、IP指定事業者）と、PIアドレス割り当て先組織、AS番号割り当て先組織（以下、PI／ASホルダ）に、それぞれの組織属性ごとに設問を分けたアンケートを用意して回答を募集しました。その結果、IP指定事業者から99件、PI／ASホルダからは125件、総数として224件の回答をいただきました。

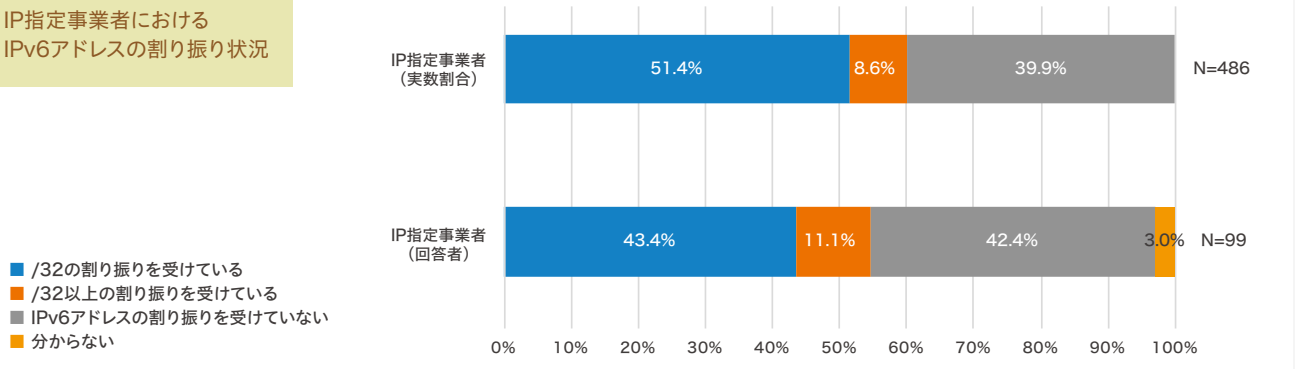
本稿では、アンケート結果の一部を紹介します。

■ IP指定事業者のIPv6対応状況

IP指定事業者におけるIPv6アドレスの割り振り、対応状況について、アンケートの回答結果と実際の割り振り状況との対比をしてみました。

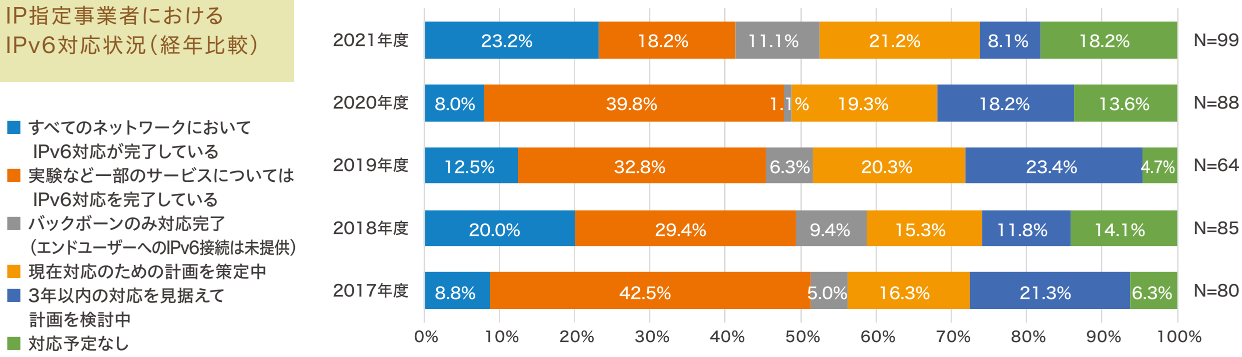
IPv6アドレスの割り振り状況について、アンケート実施時の全IP指定事業者実数と比較すると、アンケート回答者の方がIPv6アドレスの割り振りを受けていない比率が若干高い結果となっています。

IP指定事業者における
IPv6アドレスの割り振り状況



IP指定事業者におけるIPv6対応状況については、「IPv6対応」を済ませている割合は、昨年、一昨年よりも若干ではありますが増加している状況でした。一方で、「対応予定なし」とする回答も増加していました。対応していない理由としては、「IPv4アドレス在庫がある」「コストがかかる」「ユーザーニーズがない」という従来から聞かれる内容であり、特段新たな理由は示されませんでした。

IP指定事業者における
IPv6対応状況（経年比較）

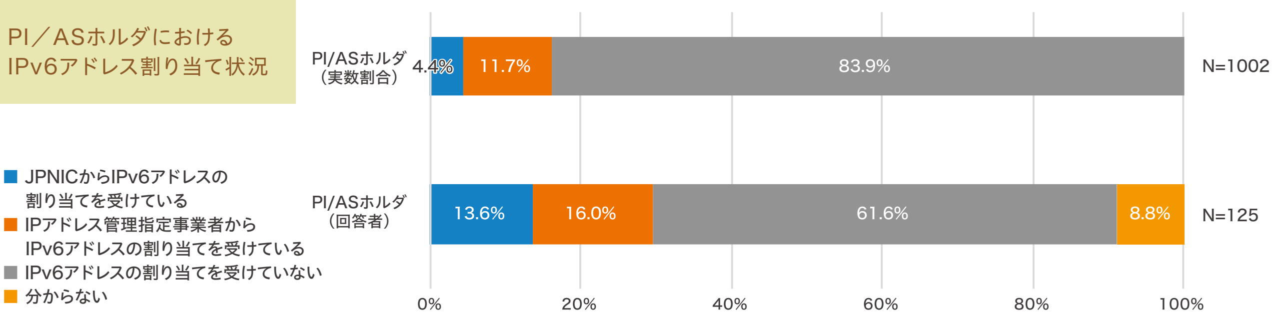


■ PI／ASホルダのIPv6対応状況

PI／ASホルダに関しては、IPv6アドレスの割り当てを受けている状況について確認しています。アンケート回答者のうち、JPNICから直接割り当てを受けているケースと、IP指定事業者から割り当てを受けているケースを合わせると、およそ3割弱の組織がIPv6アドレスの割り当てを受けています。

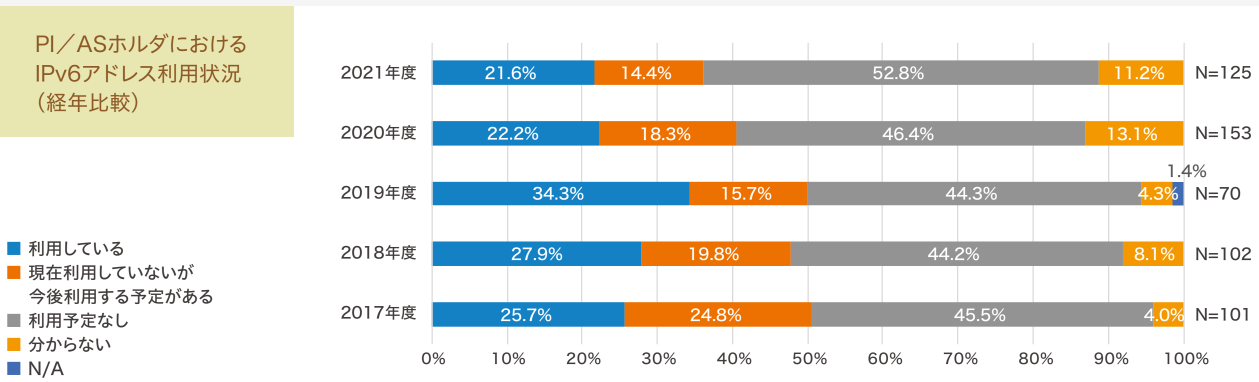
IPv4のPIアドレスあるいはAS番号の割り当てを受けている契約者のうち、IPv6の特殊用途用PIアドレスの割り当てを受けている、あるいはIP指定事業者からIPv6アドレスの割り当てを受けてWHOISデータベースに割り当て情報が登録されている組織を確認すると、全体の15%程度に留まることが分かりました。

PI／ASホルダにおける
IPv6アドレス割り当て状況



また、PI／ASホルダにおけるIPv6利用状況を経年で比較したところ、利用している割合が例年よりも低い結果となってしまいました。

PI／ASホルダにおける
IPv6アドレス利用状況
（経年比較）



誌面では割愛したアンケートの設問およびその結果は、次のJPNICブログをご覧ください。過去のアンケート結果もJPNICブログに掲載していますので、併せてご参照ください。

企業、事業者、学校のIPv6最新状況
～2021年度IPv6対応状況に関するアンケート結果～
https://blog.nic.ad.jp/2022/7339/

技術トピック

3

2022. 3.19 ▸ 3.25　オンライン開催　IETF 113

オンライン

2022年3月下旬にオーストリア・ウィーンの会場とオンラインでの同時開催となった第113回IETFミーティング（IETF 113）について、開催概要や会合でのホットトピックを取り上げます。

第113回IETFミーティングで行われたHotRFCやBOF

2022年3月19日（土）から25日（金）にかけて開催された第113回IETFミーティング（IETF 113）は、会場とオンラインでの同時開催となりました。開催地は、オーストリア・ウィーンでした。WGの会合が行われる時間帯は、日本時間の18時から翌日の3時前後でした。参加者は1,300名を超えて、新型コロナウイルスの影響で落ち込んだ参加人数が、2年ほど経ってようやく以前のように戻りつつあります。

■ HotRFC

Hot RFCのRFCは、「Request for Conversation（対話のリクエスト）」の略で、IETFにおける活動紹介などが行われるセッションです。今回は、これまでのようにライトニングトーク形式に戻りました。発表タイトル訳とURLを紹介します。

○ **アプリケーションにおける簡単なQoS対応**
（Easy Selection of QoS）
ドナルド・エストレイク（Donald Estlake）

詳細：
https://datatracker.ietf.org/doc/draft-eastlake-dnsop-expressing-qos-requirements/

DNSのサービス識別子を使って、アプリケーションがQoSに対応する方式の提案。

○ **コンピューター仕様のインターネット・ドラフト**
（Computerate Specifying: Verified Internet-Drafts）
マーク・プティハグエニン（Marc Petit-Huguenin）

詳細：
https://datatracker.ietf.org/doc/html/draft-petithuguenin-computerate-specifying

インターネット・ドラフト（I-D）のペトリネットや拡張BNF（Backus-Naur Form）、HTTPの構造を自動的にチェックするライブラリ。

○ **IEEE 802.1におけるデータセンター輻輳管理のイニシアティブ**
（Data Center Congestion Management Initiatives in IEEE 802.1）
ポール・コンドン（Paul Congdon）

データセンターにおける、輻輳管理に関する標準化活動を行うIEEE 802.1 WGの紹介と、サイドミーティングの告知。本WGでは、リモートDMA（RDMA）や、AI／HPC（High Performance Computing）といった技術を使って、低遅延・低損失・高信頼性のEthernetを実現する方式に注目している。

○ **複数者署名DNSSECのためのRFCの調整**
（RFC Adjustments for Multi-Signer DNSSEC）
ウリッチ・ヴィサー（Ulrich Wisser）

詳細: https://github.com/DNSSEC-Provisioning

サービスプロバイダを移転する際などに利用できる複数社署名DNSSEC、一つのDNSゾーンに対して複数の署名が施されたものにおいて、異なるアルゴリズムを使うためにRFCの修正など。

○ **産業用ネットワークにおけるPLCの仮想化**
（Virtualization of PLC in Industrial Networks）
キラン・マヒジャニ（Kiran Makhijani）

詳細: https://datatracker.ietf.org/doc/draft-km-iotops-iiot-frwk/

大規模な工場などで使われる、機械の制御で使われるPLC（プログラマブルロジックコントローラ）の仮想化に関するアーキテクチャの提案。課題定義のインターネット・ドラフトが作成されている。

○ **クラウドアプリケーションのための広域ネットワークの自動スケーリング**
（Wide Area Network Autoscaling for Cloud Applications）
ベルタ・セラカンタ（Berta Serracanta）

詳細: https://arxiv.org/abs/2109.02967

Kubernetesのような、クラウド・オーケストレータにおいて扱われるアプリケーションに、必要性に応じて帯域を自動的に割り当てるなどする提案。手法とプロトタイプシステムが、研究論文としてまとめられている。

これらの一覧は「HotRFC Session Abstracts」で閲覧できます。セッションの動画は、YouTube動画「IETF 113:HotRFCs」で閲覧することができます。

HotRFC Session Abstracts
https://datatracker.ietf.org/meeting/113/materials/agenda-113-hotrfc-sessa-09

IETF 113:HotRFCs
https://www.youtube.com/watch?v=rt-2H_AAucc&list=PLC86T-6ZTP5j9ZuU-yMJWRmGtFcrMKtye

■ IETF 113で行われたBOF

IETF 113では、三つのBOFが開かれました。

○ コンピューター資源の最適化に配慮したネットワーク（Computing-Aware Networking）

詳細：
https://datatracker.ietf.org/meeting/113/materials/slides-113-can-chairs-slides-05
情報：
https://datatracker.ietf.org/group/can/about/

ネットワークリソースの最適化だけでなく、メモリやCPU処理といったコンピューター資源の、最適化に配慮するネットワークの議論です。WG設立ではなく、ディスカッションを目的としたBOFです。

○ QUICを使ったメディア（Media Over QUIC – MOQ）

詳細：
https://datatracker.ietf.org/meeting/113/materials/agenda-113-moq-06
情報：
https://datatracker.ietf.org/group/moq/about/

ライブのストリーミングや音声や映像の配信のために、QUICを利用することに関するユースケースの紹介などを通じた、議論のためのBOFです。

○ ドメイン内とドメイン間の送信元アドレス検証（Source Address Validation in Intra-domain and Inter-domain Networks）

情報: https://datatracker.ietf.org/group/savnet/about/

RFC5210に記述されている、送信元アドレス検証のアーキテクチャ（source address validation architecture – SAVA）は、BGPで言われるドメイン間やアクセスネットワークなど、さまざまなレベルで適用可能です。より厳格に検証するなどの、要件を想定した仕組みが提案されています。

■ 会場とオンラインの同時開催の様子

IETF 113は、ここ2年の開催形態とも違っていました。現地参加者もオンラインツールであるMeetEchoに表示され、現地とオンラインが、少なくともオンライン参加者にとってはシームレスな形になっていました。そのため、現地での参加方法が動画で解説されていました。

Tips for IETF 113 Participants
https://www.youtube.com/watch?v=3r0UY4dYz2Y

今後のいわゆる「ハイブリッド」開催されるイベントは、現地参加者とオンライン参加者が互いにどのように見え、どのように関わるものになるのか、IETF 113にあったように、工夫されていくように思いました。

IoTデバイスマネジメント関連のトピック

ネットワーク接続機能を有したデバイスを活用するIoTでは、大量のデバイス群による、ビッグデータの創出や多様なサービス提供が期待される反面、膨大な数のデバイス展開や、ライフサイクル管理が課題とされます。IETFではsecエリアを中心に、このようなIoTデバイスのネットワークを介した管理に寄与する、標準の策定が並行して進んでいます。

今回は、その中で三つのWGの活動を紹介します。

■ SUIT WG（Software Updates for IoT）

SUIT WGでは、IOTデバイスのソフトウェア更新をスコープに活動しています。具体的にはマニフェストと呼ばれる、ソフトウェアの配布URIや更新時に実行するコマンドを記したフォーマットを規定しており、IOTデバイスはマニフェストのパーサーを動作させることで、ソフトウェアの更新を実行することができます[※1]。

既に、マニフェストを中心としたソフトウェア更新モデル、ならびにマニフェストに記載する情報のモデリングは、いずれもRFC 9019、RFC 9124として標準文書を発行済みであり、現在はマニフェストのバイナリ記述方法や、高度なソフトウェア更新機能、ソフトウェア更新の結果報告機能が議論されています。

○マニフェストのバイナリ記述方法[※2]

マニフェストは、改ざんなどの攻撃への対策として、署名を含めることができます。今回のIETF 113では、この署名アルゴリズムとしてHSS-LMS方式の耐量子計算機暗号アルゴリズムを追加し、実装を必須化すべきという提案がなされました。IoT機器は数十年単位で運用されることも多く、長期間安全性を確保するために必要という狙い

で提案がなされましたが、リソース制約が大きいIoT機器に対して実装を強制することは可能なのかという指摘があったほか、耐量子計算機暗号アルゴリズムはHSS-LMS以外の方式の提案や標準化が行われており、これらの比較なども踏まえて議論すべきとの指摘がありました。またこれに関連し、暗号化アルゴリズムに関する規定は、バイナリ記述方法の文書から分離すべきという意見も出されました。

○高度なソフトウェア更新機能

高度なソフトウェア更新機能として議論されている対象には、暗号化されたファームウェアを用いた更新(Firmware Encryption)※3、ならびにソフトウェア間の依存関係を表現できるマニフェストの拡張(Multiple Trust Domains)※4があります。IETF 113では、暗号化されたファームウェア更新機能について、ARM社のHannes Tschofenig氏がハッカソンを実施し、同氏が提案する更新手法についての報告、ならびにドラフトのアップデートを行いました。後者はマニフェストの拡張として、今回のIETF 113からWGアイテムとして追加されました。こちらは提案者から、実装によるフィードバックが欲しいとのコメントが寄せられています。

■ RATS WG(Remote ATtestation procedureS WG)

RATS WGは、リモートアテステーションと呼ばれる、ネットワークを介して遠隔でデバイスの正常性を検証する技術をスコープとしたWGです。

RATS WGが標準化を進めるリモートアテステーションでは、検証対象とされるAttester、Attesterから収集したEvidenceと呼ばれる値群を基に検証・評価を行うVerifier、Verifierの検証結果(Attestation Result)を利用するRelying Partyが規定されており、3者間でやり取りされる情報のフォーマット(EAT: Entity Attestation Token)の規定も行っています。

IETF 113のRATS WGのミーティングでは、WGの活動スコープを改定するRecharterが行われました。これまでの議論に加え、

・Evidenceに加え、Attestation Resultの伝送プロトコル
・Endorsement、Reference Valueのフォーマット

の2点も、RATS WGで取り扱う対象に拡張されました。前者は、既存の伝送プロトコルの採用を前提としています。後者はVerifierに対し、検証の参考や基準となる情報のフォーマットを、新たにRATS WGで規定することが可能になりました。

このほか、Attestation Resultの取り扱いに関する提案(Attestation Result Framing)も行われました。提案内容は、Attestation Resultをシステムの安全性を示す尺度として意味を持たせる、クロスプラットフォームに対応した絶対的なデバイスの識別子の規定、Relying Partyでの機械学習などの利用を目的としたEvidence情報のResultへの全コピーなどがあったものの、RATS WGの方針として安全性の判断はプロトコル利用者のポリシーに依拠する点、既存の各業界で標準となっているデバイス識別子への対応や、プロトコル利用者によって拡張可能な識別子を規定している点、Relying PartyとVerifierの同居構成も現行可能にしている点などから、いずれも新規対応は行わない方向となりました。

■ TEEP WG(Trusted Execution Environment Provisioning)

TEEP WGが対象とするTEEとは、ARM TrustZoneやIntel SGXに代表される、ハードウェアベースの実行環境隔離機構を指します。この機構では、ソフトウェアの実行環境をTEEとREE(Rich Execution Environment)の2種類に分け、TEEはREEからの侵害を受けない構成になっています。暗号化や認証など重要な処理をTEE上に実装することで安全性を確保できますが、このTEE領域に対するアプリケーションやデータの配信・管理を行うプロトコルがTEEPです。

TEEPでは、アプリケーションの配信に関わるアーキテクチャを規定したTEEP Architectureと、配信サーバ・デバイス間のメッセージフォーマットを規定するTEEP Protocolの二つが、現在の主な活動アイテムです。

IETF 113では、TEEP Architectureのエリアディレクターのレビューと、その対応が報告されました※5。ディレクターからのコメントには、End Userの権利やTrust Modelに対する懸念が寄せられました。TEEPでは、TEE領域で動くアプリケーションは配信サーバが管理し、デバイスの所有者は介入することはできません。したがって、デバイスの所有者であっても、どのようなアプリケーションが動作するかを把握したり、制御したりすることが困難になると言えます。議論においては、End Userに対する透明性の確保や、アテステーションなどにより対応ができるのではないか、というコメントが寄せられました。

TEEP Protocolは、国立研究開発法人産業技術総合研究所の塚本明さんや私などから、前述したRATSにおけるEATの埋め込み方法や、メッセージの保護に使う暗号化スイートを宣言するフィールドの改善などを提案した※6ほか、TEEPにおけるRATSの使用法についても提案が行われました。

IoTデバイス関連のWGは、同時並行で標準化が進められていますが、それぞれの標準を相互に組み込んで使う前提で議論が進められています。例えば、TEEPでは配信するアプリケーションのメタデータの伝送はSUIT、配信先のデバイスのチェックにはRATSを使います。

紹介した三つのWGは、COVID-19の影響下においても、議論はリモートで活発に続けられています。一方で、これらWGがターゲットとするIoTデバイスを用いた検証やフィードバックは、個人個人の活動にとどまっており、今後対面会議が再開された際には、ハッカソンなどの開催も期待される状況です。

※1 JPNIC News & Views vol.1680 第104回IETF報告 [第2弾] IoT関連報告 ～IoT機器の安全なライフサイクル管理～
※2 A Concise Binary Object Representation(CBOR)-based Serialization Format for the Software Updates for Internet of hings(SUIT) Manifest
※3 Firmware Encryption with SUIT Manifests
※4 SUIT Manifest Extensions for Multiple Trust Domains
※5 TEEP Architecture draft-ietf-teep-architecture-16
※6 IETF113 TEEP Hackathon

ドメイン名・ガバナンス

INTERNET TRENDS INTRODUCTION

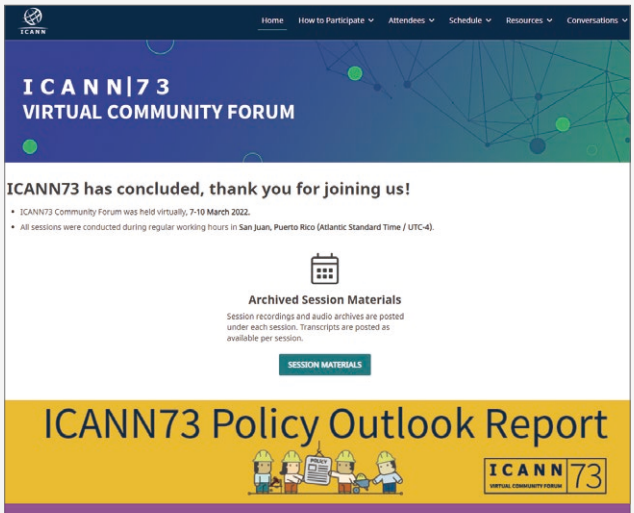
4

2022. 3.7 ▸ 3.10　第73回ICANN会議　オンライン

本稿では、2022年2月～2022年5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73回ICANN（The Internet Corporation for Assigned Names and Numbers）会議や、EUにおけるエンドツーエンド暗号化の規制を巡る動向などをご紹介します。

第73回ICANN会議

第73回ICANN会議（以下、ICANN73）は、2022年3月7日（月）から10日（木）までオンラインのみで開催され、146の国・地域より1,578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。



ICANN73も、引き続きオンラインでの開催となりました

■ プレナリーセッション

○グローバルな公益の枠組みは役に立つか？

グローバルな公益（Global PublicInterest, GPI）の枠組みは、ICANN理事会の決定を必要とする特定の文脈や問題に焦点を当てるように設計されていますが、この枠組みについて議論されました。GPIの枠組みがICANN理事会の審議の一部となった例が取り上げられ、各部会のパネリストがICANNコミュニティがICANN理事会とのやり取りで、どのようにフレームワークを使用すれば最も効果的かについて議論を展開しました。

https://73.schedule.icann.org/meetings/N79ABoMmic8ihMi8n

○DNS Abuseに関する対話の進展

本セッションでは、DNSの不正利用に対する業界の対応について議論され、新機軸として不正に登録されたドメイン名と、悪意を持って登録されたドメイン名の区別について検討されました。

https://73.schedule.icann.org/meetings/Ak56QBFwurEqC4LuP

■ 地政学、立法、および規制の策定に関する討論

インターネット、とりわけDNSに関する規制・立法の動きについて、共有ならびに議論されました。政府間組織、各国ならびにEUでの動き、コミュニティは何ができるのか、という部分に分けて発表および議論がなされました。

参加者からの質問の中に、ICANNは米国政府から干渉は受けないのか、ICANNを特定の政府の管轄下から外し、ある種の国際条約の下に置くという議論はされているのか、という質問がありました。これに対し、ICANN事務総長Marby氏は、地球上に存在する限りはどこかの国の管轄権に服さなければならず、条約の下に置くということはすなわち国連のシステムということになる、現在のICANNのシステムを維持するために、2016年にIANA監督権限を米国政府から移管した際に、多数の国が支持したことからもわかるように、世界中の国々やIGOの支持を受けて独立性を保つために戦っている、との回答がありました。

■ gTLD関係

ICANN73では、gTLDに関する主要なポリシーに関するセッションは開催されませんでしたが、開催されたセッションのうち、一部の状況を記載します。

○移転ポリシー評価PDP

WGでは、移転先および移転元の承認フォーム（FOA）とAuthInfoに関連する審議が大幅に進展しており、初期報告書への提言を固めつつあります。次に注目すべきは、NACKingとして知られている、移転の取り消しまたは拒否についてとなります。

○国際化ドメイン名に関するEPDP

同WGは、七つの主要トピックのうち最初の、ルートゾーンラベル生成ルールの技術的活用に関する勧告（RZ-LGR）を用いた、gTLDおよび異体字gTLDラベルの一貫した定義に焦点を当てたものとなる、トピックAに関する実質的な審議の第1段階がほぼ終了しています。現在、WGでは、異体字gTLDの「同一事業者」原則に関するチャーター上の質問と、レジストリ運用者が申請または運用するための法的および運用上の枠組みに関する質問について、最初の審議が進められています。

○登録データ精度向上検討チーム

GNSO評議会は、2021年7月22日の会合で、登録データ精度に関するスコーピングチームの設立と指示書を採択し、現在の実施と報告、精度の測定、有効性など、精度に関連する多くの側面を検討するよう命じました。その中で、実施と報告、および正確性の測定のトピックに焦点を当て、ICANN事務局と協力して既存の要求事項の解釈と実施、および報告について理解すること、およびギャップ分析を行い、GNSO評議会に対する勧告の検討および策定に役立てる予定となっています。

■ 第63回ICANN報告会

第73回ICANN会議での議論を紹介する報告会を、2022年4月26日（火）に、こちらも完全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. ICANN73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. ICANN理事からの報告
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

第63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63回ICANN報告会
https://www.nic.ad.jp/ja/materials/icann-report/20220426-ICANN/

■ 第74回ICANN会議

次回ICANN74は、2022年6月13日（月）～16日（木）の日程で、オランダ・ハーグでの現地開催ありのハイブリッド形式で開催されました。この会議の内容は、次号82号でご紹介いたします。

なお、今回ご紹介した第73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73回ICANN会議報告
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2022/vol1913.html

EUにおけるエンドツーエンド暗号化の規制を巡る動向

エンドツーエンド（E2E）暗号化（E2EE）とは、端末間の全部の通信経路でコンテンツを暗号化することを意味し、通信経路の途中の仲介者がデータを復号化して内容を読むことが事実上不可能となります。利用者にとっては安心ですが、犯罪などに使われた例もあるため、法執行当局からはこれまでテロや児童虐待などの対策の際に問題となるという主張がなされてきました。そのエンドツーエンド暗号化について、EUにおいて規制すると解釈できる可能性のある内容の規則案が2022年5月に欧州委員会より提案されましたので、内容を追ってみたいと思います。

◆ 規則案提出の背景

オンラインでの児童の性的虐待がパンデミックで増えていることもあり、その脅威に包括的に対応するため、2020年以降欧州委員会は次々と戦略を打ち出してきています。すでに一部のプロバイダーは、自社のサービス上でオンライン児童性的虐待を検知、報告、削除する技術を自主的に使用しているもののプロバイダー間でばらつきがあり、デジタルサービス法を補完しオンライン児童性的虐待の検出、報告、除去に関する統一的な連合規則が必要である、との立場を欧州委員会は取っています。

こういった背景により、児童虐待防止規則案（以下、「本規則案」）が策定されました。本規則案は、オンライン児童性的虐待の防止と対策に関する明確で調和のとれた法的枠組みの確立をめざすものであり、本提案は、プロバイダーが、憲章に規定された基本的権利およびEU法の一般原則と矛盾しない形で、リスクを評価・軽減し、必要に応じて、サービス上の虐待を検知・報告・除去する責任について、法的確実性を提供しようとするものである、としています。

◆ 規則案の内容

本規則案は「欧州議会および欧州理事会規則」、つまりいわゆるEU規則で、各加盟国における立法を必要としません。本規則案は主に次の要素から構成されています。

・プロバイダーに対して、既知および新規の児童性的虐待資料の検出、報告、削除、ブロック、および児童への勧誘に関する義務を、オンライン交換に使用される技術に関係なく課す
・規則の実施を可能にする機関として、「児童性的虐待に関するEUセンター」（以下、「EUセンター」）を設立

本規則案では、性的虐待の被害者である児童とその基本的権利を保護し、それによって一般社会の利益となる重要な目的を達成するための措置と、他の利用者やプロバイダーの基本的権利との間に公正なバランスを確立するために、強固な条件と保護措置に従った、的確な措置を定めているとしています。プロバイダーがその責任を果たせるようにするため、EUセンターを設立し、この規則の実施を促進・支援するとしています。具体的には、この規則に基づくプロバイダーのオンライン児童性的虐待の検出、報告、児童性的虐待素材の除去の支援に役立てようとするものです。EUセンターは特に、プロバイダーが検出義務を果たすために利用することが求められる、オンライン児童性的虐待の指標に関するデータベースを作成し、維持・運営する予定です。EUセンターは、欧州刑事警察機構（Europol）との緊密な協力が必要、と書かれており、Europolの代表者はEUセンターの運営委員会（Management Board）のメンバーになり、EUセンターの代表者はEuropolの運営委員会メンバーとなることになっています。

◆ エンドツーエンド暗号化との関係

規則案中の説明では、エンドツーエンド暗号化技術を含む技術に対しては中立、ということのようです。規則案によれば、各プロバイダーが対象となるコンテンツを検出する際にどのような方法を使うかは、プロバイダーに任されることになります。検出後、児童性的虐待の可能性を示す情報をEUセンターに報告することになります。

対象となるサービスがエンドツーエンド暗号化技術を使っている場合は、プロバイダーがバックドア、クライアントサイドスキャン、安全な孤立領域（secure enclave）などの方法を使って利用者の手元で復号化後のコンテンツを取り出す必要が出てくることは確実です。特にパーソナルコンピューター、スマートフォン、およびタブレットのオペレーティングシステムは寡占化が進んでいるため、数社が同意して対応すれば多くの場合クライアントサイドスキャンにより内容を取り出せる、ということになる可能性が高そうです。

なお、クライアントサイドスキャンとは、利用者側でメッセージのコンテンツ（テキスト、画像、動画、ファイル）をスキャンし、意図した受信者にメッセージが送信される前に、不愉快なコンテンツのデータベースとの一致を確認するシステムです。

Internet Society（ISOC）によるクライアントサイドスキャンの問題点は次の通りです。

・犯罪者に利用されやすい脆弱性ができてしまう
・技術的・プロセス的な新たな課題を生み出す
・別の用途（政敵などの通信遮断など）に使われる可能性がある
・犯罪者が別のサービスに移る可能性が発生する

2021年にApple社が児童性的虐待素材（Child Sexual Abuse Materials, CSAM）のクライアントサイドスキャンを行うと発表した際は、反対が多いため凍結されたと報道されましたが、2019年よりApple社のクラウドメールサービスではクライアントサイドスキャンが行われていると報道されており、本稿執筆時点では、米国、英国、カナダ、豪州、ニュージーランドでは標準搭載チャットアプリ、検索アプリなどでクライアントサイドスキャンが行われていると読める記載があります。

なお、規則案は本稿執筆時点では欧州議会とEU理事会は通過しておらず、まだ法律にはなっていませんが、EUセンターはすでに構築に向けて準備が進められているという報道もあります。

この規則案については、「児童の性的虐待は加盟国および世界の他の国々によって対処されなければならない重大な犯罪であるが、欧州委員会がこの規則案で採用したアプローチが、通信のセキュリティとユーザーのプライバシーに壊滅的な影響を与えることを懸念する」として2022年5月22日にISOCをはじめとする団体および個人が共同で声明を出しています。

◆ 今後の動きについて

この後想定されるプロセスは、通常立法手続きであれば、欧州議会での審議およびEU理事会での決定ということになります。上記の反対声明などがどの程度取り入れられるのか、ロビイングがなされているのか、今後法律が成立または却下ということになるのかはまったくわかりませんが、注目すべきものと思われます。また、「エンドツーエンド暗号化及び公共の安全に関する国際声明」に署名した日本を含む他の国々で、今後どのような法案が提出されるのかについても注視すべきと思われます。

このEUにおけるエンドツーエンド暗号化規制を巡る動向については、JPNICブログで詳しくご紹介していますので、次の記事も併せてご覧ください。

エンドツーエンド暗号化規制のその後
https://blog.nic.ad.jp/2022/7632/

エンドツーエンド暗号化と法規制
https://blog.nic.ad.jp/2020/5545/