

第72回RIPEミーティング報告



今回は、2016年5月23日(月)から27日(金)にデンマーク・コペンハーゲンで開催された、第72回RIPEミーティング(RIPE 72)の様子をレポートします。

RIPEミーティングでは、その時々に着目すべき発表を扱うPlenary(プレナリ、全体会議のこと)セッションから、ワーキンググループおよびBoFのトピックスに至るまで、大変多様な話題が議論されます。本稿ですべてをカバーすることは残念ながらできませんが、アドレスポリシー関連の議論を含む、皆さまに関わりのありそうなトピックスを中心にご紹介します。

◆ 全体概要

事前参加登録者は過去最大で700名を越え、実際には676名の参加があったとの発表がチェアより会議初日にありました。参加者はヨーロッパ地域内のネットワークオペレーターが中心ですが、Europolのような法執行機関、ドイツやスウェーデン等からの政府関係者等幅広い層の参加者を取り込んでいます。今回は、ICANNのCEOおよび理事数名、IETFチェア、ISOCスタッフ等、いわゆるI*団体と呼ばれる組織からの参加も目立ちました。

初日のPlenaryでは、ICANNの新CEOとして着任したばかりのGöran Marby氏が、ボトムアップでさまざまな関係者を取り込むマルチステークホルダープロセスおよびIPv6導入促進の重要性を語りました。また、昨今RIPEは「The RIPE Academic Cooperation Initiative (RACI)」と呼ばれる学術機関の研究と運用の連携強化にも注力しており、RIPE会議中、学術関係者による発表も設けられていました。

また、ミーティング開始前の5月21日(土)および22日(日)には、コミュニティの協力を得ながら実施しているインターネットの計測プロジェクトである、RIPE AtlasのHackathonも行われ、今後の改良点のRIPE Atlas開発者に対するインプットにつながりました。RIPE AtlasのHackathonは、2015年にも実施されています。

そして、今回はデンマーク開催ということで、北欧の国別のIXP、トランジット事業者や市場を比較・紹介する発表もPlenaryで行われ、地域の接続事情の全体像をつかむにはよい発表でした。

Interconnection in the Nordics

<https://ripe72.ripe.net/presentations/10-Interconnection-in-the-nordics-RIPE72-v3.pdf>

ミーティングのプログラムについては、次のWebサイトをご覧ください。

RIPE 72 Meeting Plan

<https://ripe72.ripe.net/programme/meeting-plan/>

基本的には議論・情報交換を中心とした会議であるため、決定事項はありませんでしたが、最終日のClosing PlenaryではBest Current Operational Practices (BCOP) タスクフォースから、RIPEにおけるIPv4アドレス在庫が枯渇したことを踏まえて、今後の進むべき方向をRIPEコミュニティとして明確なステートメントとして出すことがチェアに対して提案されました。

また、今回の会議では、RIPEチェアの選挙実施が発表されました。現チェアのHans Petter Holen氏は、前任のチェアから委任をされてコミュニティの信頼も厚いようですが、暫定的なチェアとして委任されたとして選挙の実施に至ったとの説明がありました。特に不信任が表明されていない状況においても、あえてコミュニティが参加する選挙を行い、コミュニティからの支持を明らかにしようとする点は、ボトムアップの精神を重視しているRIPEコミュニティらしいプロセスだと言えます。



● ミーティングの様子

◆ IANA機能監督権限移管セッション

今回は、2014年3月の米国商務省電気通信情報局 (NTIA) によるIANA機能監督権限を移管する意向の発表から約2年の時を経て、2016年3月10日(木)にグローバルインターネットコミュニティが策定した提案の提出が完了したという、一つのマイルストーンを迎えた後のRIPE会議でした。そして、セッションと同日に米国議会での公聴会が予定されているタイミングでもありました。

番号資源コミュニティの立場から、IANA機能監督権限移管およびICANN説明責任強化に向けた提案とそのプロセスの振り返りが行われました。どちらの提案においても、番号資源コミュニティが重視したポイント、つまり「ボトムアップでコミュニティベースのプロセスの有効性をインターネットコミュニティ内外に証明したこと」と「五つの地域をまたいだ番号資源コミュニティの団結と一貫した姿勢を他のコミュニティにも示せたこと」が反映されたことが強調されました。

セッションの最後に、RIPEチェアよりRIPE地域のCRISP(クリスプ、Consolidated RIR IANA Stewardship Proposal) チームメンバー3名それぞれに表彰とシャンパンが贈られ、サプライズとして筆者にまで、チェアとしての務めへの感謝の印として盾をいただきました。

◆ アドレスポリシー提案

現在RIPE地域で議論中のアドレスポリシー提案は5点あり、各提案の概要は、今回のRIPEミーティングの開催前に公開したJPNIC Blogでご紹介しています。

JPNIC Blog: RIPE 72がコペンハーゲンで開催されます

<https://blog.nic.ad.jp/blog/ripe72-policy-proposal/>

2015-04	RIPE Resource Transfer Policies (RIPE地域における資源の移転ポリシー文書の統合)
2015-05	Last /8 Allocation Criteria Revision (最後の/8からの割り振り基準の見直し)
2016-01	Include Legacy Internet Resource Holders in the Abuse-c Policy (歴史的経緯を持つPIアドレスにもAbuse-cの登録を求める)
2016-02	Resource Authentication Key (RAK) code for third party authentication (第三者認証のためのRIPEデータベースにおけるRAKコードの提供)
2016-03	Locking Down the Final /8 Policy (最後の/8ポリシーの厳正化)

2016-02以外の提案はすべて、IPv4アドレスに関する内容であるためか、この一連の議論に対して「Rearranging the deck chairs on the Titanic(目の前の問題解決に何の役にも立たない)」と表現して個別に皮肉を述べている参加者もいました

が、全体としてはセッションおよびその後のメーリングリストでの議論もそれなりに活発に行われていました。

RIPE会議のプロセスでは提案に対するコンセンサス確認は行わないため、いずれの提案に対する結論にも至っていませんが、2015-04は、組織の吸収合併時にも移転後2年間は移転できないとの制限を設けるべきではないとの指摘があった以外は、懸念は見受けられませんでした。2015-05および2016-03には賛否両論があり、当面コンセンサスに至ることは難しいと思われます。

今回、IRRとRIPEデータベースの連携強化を求めていることから、目新しかった提案である2016-02は、RIPE NCC Servicesワーキンググループで議論され、IRR情報の正確性向上のためという趣旨には賛同が見受けられました。RIPEデータベースとIRRを連携させる仕組みについても、RADBやNTT社のIRR等の主要なIRRの賛同を受けていることが提案者から説明されました。もし今後コンセンサスが得られた場合、他のRIRも、IRRによる認証に協力を求められる動きが広がることも想定されます。一方、RPKIおよび他の対応策も含めて総合的に検討すべきであるとの意見もあり、継続議論となっています。

◆ IPv4アドレスの移転

今回の会議は、RIPE地域がRIR間の移転ポリシーを施行してから間もないことから、ARIN地域からRIPE地域への移転を行った事例紹介がRandy Bush氏により行われました。特にARIN地域は歴史的経緯を持つPIアドレスに対して契約締結を行っていないため、移転申請を行ったアドレスの分配を正当に受けていることの証明に、多くの労力が必要だったそうです。

A Happy Story of Inter-RIR Transfer of Legacy Blocks from ARIN to RIPE

<https://ripe72.ripe.net/presentations/65-160524.ripe-transfer.pdf>

JPNICは、すべての歴史的経緯を持つPIアドレスに対して契約締結を行っているため、JPNIC管理下のIPv4アドレス移転であれば、この問題は発生しませんが、ARINからJPNICへの歴史的経緯を持つPIアドレスを移転する際には、似たような課題に直面する可能性はあります。会議には複数のブローカーが参加しており、円滑な移転を支援するため、JPNICの申請手続きについて個別に質問を受けました。

また、ICANNおよびブローカーであるHilco Streambank社との共同発表として、一部の組織に移転が集中している傾向が共有されました。全体としては、移転を行うトップ10の組織が、移転アドレス総数の40%以上を占めていることが統計で示されました。このことから、IPv4アドレスの移転は一部の組織に集中していることが見て取れます。このほか、移転ではなくリースのように、他社によるアドレス利用を契約を取り

交わして認める事例も確認されており、これらの形態で利用されているアドレスは、実際のアドレス利用者がデータベースに反映されていないことも共有されました。同様の発表はAPRICOT 2016でも行われています。

Market Concentration in the Transfer of IPv4 Space
<https://ripe72.ripe.net/presentations/102-IPv4-Transfers-Indicators-RIPE72.pdf>

◆ 経路ハイジャック

IPv4アドレス在庫が枯渇した今、経路ハイジャックの事例が話題に上るようになってきています。RIPE 72では、プライベートピアリングによる見えないハイジャックの事例が紹介されていました。ハイジャックを行っていた組織は、DE-CIXを経由してYahoo!とプライベートピアリングを行っており、顧客から到達性の問題について報告を受けて確認したところ発覚したそうです。ハイジャックに利用されたAS番号は、AFRINIC管理下の未分配ASだったそうですが、料金の支払いも滞りのない法的にも問題のない顧客だったため、DE-CIXはIRRの登録情報を基に経路を流しており、RIPEのIRRはRIPE地域以外の番号資源について登録資格を確認していないため、今回のような状況に至ったようです。

Invisibly Hijacking (Plenaryでの発表)
<https://ripe72.ripe.net/programme/meeting-plan/plenary/>

Discussion on Invisible IP Hijacking (Anti-Abuse WGでの発表)
<https://ripe72.ripe.net/presentations/165-invisible-hijacking-follow-up.pdf>

このように、アドレスの正当な利用者をどう正しく認識するかという問題は、今後も続いていくかと思われます。ポリシー提案2016-02の議論のもと、IRRとRIPEデータベース間の連携が強化されていくのか着目していきたいところです。

◆ ルーティングセキュリティの強化

昨今、RIPEコミュニティではIRRへのRoute Objectの登録に関して、情報の正確性と正当性の向上についての議論が行われています。今回はルーティングWGにて、人的にデータ認証を行うことによるルーティング情報の正確性向上に向けたNTT社の取り組みへの参加が、Jared Mauch氏により呼びかけられました。また、RIPEのIRRデータベースにおいて、他の地域の番号資源の登録が認められていることで、登録者が正しい資格を持っているのか正確に確認できず、また、地域をまたいだ登録情報の重複にもつながることが問題提起されました。今後は、この問題に対する対応の検討が進められます。

Making Routing Registries Great Again
https://ripe72.ripe.net/presentations/141-making_routing_great_again_ripe72.pdf

Bogon ASN Filtering
https://ripe72.ripe.net/presentations/151-RIPE72_bogon_ASNs_JobSnijders.pdf

ルーティングセキュリティを強化する仕組みとして、RPKIについては、RIPE NCCからIRRとの連携も強めた新たなツール提供の必要性についてコミュニティへ相談が行われたり、DE-CIXが顧客に対してROAをもとにしたValidationを行うサービスも紹介されたりしていました。

RPKI Validator
<https://ripe72.ripe.net/presentations/153-RPKI-Validator-3.0-RIPE72.pdf>

RPKI Validation at IXPs
https://ripe72.ripe.net/presentations/92-2016-05-25_RPKI-Origin_Validation_at_IXPs.pdf

また、ルーティングセキュリティ強化に向けたコミュニティによる取り組みであるMANRS (Mutually Agreed Norms for Routing Security) についても、その活動への支持を表明する組織をどう広げるのかといった議論も行われました。本文書は、日本語の参考訳をJPNICのWebページで提供しています。

MANRS BCOP Update
<https://ripe72.ripe.net/presentations/38-Manrs-Bcop-Ripe72-AMR-WVG.pdf>

Mutually Agreed Norms for Routing Security (MANRS) 翻訳文
<https://www.nic.ad.jp/ja/translation/isoc/20140924.html>

このようにRIPE 72期間中、ルーティングセキュリティの強化に向けて、さまざまなアプローチによる情報交換が行われていました。



● RIPE NCCのRPKI Validator ページ

◆ 会議の振り返り

IPv4アドレスポリシーに関する議論はある程度活発ではあるものの、直接APNIC地域にも関わる内容は見受けられません。しかし、IPv4アドレスの在庫枯渇に伴うハイジャックの問題については、今後も留意が必要です。この対応として、IRRとRIPEデータベースの連携強化を求める2016-02は今後、他のRIRとの連携やIRRとの関係性を踏まえて動向を着目していきたいところです。

また、本稿でカバーすることのできなかったDNS関連やIPv6関連の議論は、JPNIC Blogでご紹介していますので、こちらも併せてご参照ください。

JPNICブログ「RIPE 72ミーティングレポート」
<https://blog.nic.ad.jp/blog/ripe72/>



JANOG38ミーティングレポート ~ゼロレーティングとネット中立性を考える~



2016年7月6日(水)から7月8日(金)に、沖縄県那覇市でJANOG38ミーティングが開催されました。筆者が一参加者として注目したJANOG38ミーティングの様態をご紹介します。

◆ JANOG38ミーティングについて

JANOG38ミーティングは、株式会社オキットをホストとし、「斬」新たなプログラムや「斬」れ味鋭いディスカッションの実現をめざして、「斬」をミーティングテーマとして掲げ開催されていました。ミーティングは大変盛況で、本会議の参加者は586名と最終日に発表がありました。非常に多様なセッションに加え、併設された34の企業展示ブースをスタンプラリーの形式で回る催しや、個々のセッションの結果を5段階で評価して投票するチケットが配布されるなど、趣向の凝らされた運営となっていました。

今回は、これらの多彩なセッションから一部をピックアップして、簡単にご紹介します。JANOGのWebサイトでは、ここに挙げたセッション以外にも、大変多くのセッションの資料が公開されていますので、次のWebページも併せてご参照ください。

JANOG38 プログラム
<http://www.janog.gr.jp/meeting/janog38/program.html>

◆ もっと知りたい方へ

ここでご紹介した内容は5日間にわたって開催されたRIPE 72の会議の、ほんの一部です。

Plenaryセッションやテーマごとの各種運用に関する議論が大変充実していましたので、ぜひアーカイブから資料や動画をご覧ください。ミーティングレポートも発表されています。

<https://ripe72.ripe.net/archives/>
<https://ripe72.ripe.net/programme/report/>

次回RIPE 73会議は、2016年10月24日(月)から28日(金)にスペイン・マドリッドで開催される予定です。

<https://ripe73.ripe.net/>

(JPNIC インターネット 推進部 奥谷泉)

◆ ゼロレーティングを支える技術とローカルレギュレーション

JPNICの岡田雅之、奥谷泉がコーディネーターを務め、「ゼロレーティングを支える技術とローカルレギュレーション」と題して、日本ネットワークイネーブラー株式会社の石田慶樹氏、ノキアソリューションズ&ネットワークス株式会社の幡谷一哲氏、株式会社企のクロサカタツヤ氏によるセッションを行いました。

ゼロレーティングとは、モバイルなどの事業者で実施されていた、特定のアプリやサービスについては課金の対象としないという、サービス提供形態を指していましたが、転じて、インターネットアクセスサービスが提供される際に、通常の利用には課金が行われるが、一部のアプリ、サービスはアクセス料金が無料で提供されるといった、提供形態について用いられるようになりました。

● ゼロレーティングを取り巻くもの

新興国などで、このような一部のサービスが無料という形態

でインターネットが提供されることについて、その構築や利用の拡大が進むよう施策だという主張があります。一方反対派からは、利用コンテンツの偏りが起こり得ることから、インターネットが一部の利用に限定された形で提供されてしまうといった主張があります。ネットワークの中立性といった観点や、特に日本においては、これを実現する上で利用されるDPI (Deep Packet Inspection) 技術と、その利用に対する「通信の秘密」をどう保護するのかといった観点が、議論にて重視されるポイントと考えられると紹介されました。

通信の秘密については非常に長い議論が行われており、「当事者の個別かつ明確な同意があるか」「オプトアウトの用意があるか」「法令に基づく行為であるか」「正当業務行為であるか」などの要件を満たすかどうか、重要なポイントとして挙げられました。

● DPI技術と通信の秘密について

DPI技術の概要と、どのようなケースでゼロレーティングと関係するかという紹介がありました。DPI技術には、通信の秘密と絡めた否定的なイメージがあります。しかしながら、DPIは元々セキュリティの技術として開発されたもので、どの通信が安全なのか、セキュリティ的に危険なものかという判断を可能とする技術です。現在最も多いDPIの使われ方はマーケティングであり、トレンドをビッグデータと絡めて分析することにも利用されているという紹介がありました。

ゼロレーティングに類するエンドユーザーへの料金施策を実施する際に、何をトリガーとするのかを考えると、例えば電話では、0120から始まる番号により無料であると判断します。この場合、DPIは不要です。また、使うアプリケーションによって値段を変えようといった対応を取る場合、DPIでは経路上で通信には不要な領域のデータを見えています。しかしながら、これは通信内容そのものは見なくても実現可能ですので、これだけで通信の内容を見ているということになるわけではありません。DPIが通信の内容を見る必要がある例としては、会社の携帯電話で連絡を取る際、業務の連絡であれば無料、私用の連絡であれば有料、といった場合が挙げられます。

● ゼロレーティングと中立性

産業構造の変化があり、ネットワークのオペレーターとプラットフォームが、それぞれ相手と連携する、またはその機能を取り込もうとする動きがあります。今回のセッションでは、LINE社が提供を予定している、最近話題のLINEモバイルをプラットフォームの例として取り上げていました。変化のポイントとなるプラットフォームの特徴として、自身も

サービスを行う一方、サードパーティーのコンテンツ、事業者をどんどん取り込み、「このプラットフォームの世界を利用すればどれだけ幸せになれるか」を消費者に語り、また、顧客接点をプラットフォームが持ち、顧客の認知やロイヤリティがプラットフォームにあることを宣言し、もはやただのオペレーターにはとどまらず、構造化されていると述べられました。ネット中立性ということ、垂直統合モデルがよいものであるのか、このようなモデルが消費者の利益を守ることになるのかということが、主に海外で議論されてきました。

最も活発に議論がされているのは米国で、米国連邦通信委員会 (FCC) では、ネット中立性原則というもの有三つ掲げられています。これは「ブロックの禁止」「差別的扱いの禁止」「透明性の確保」です。透明性の確保は、今まさに米国上院で議論がされている状態で、大統領選の行方によっても左右されると考えられています。米国では具体的な手段であるDPIについて、明確な規制はない状態です。他の国での例としては、新興国ではかなりゼロレーティングに積極的ですが、インドはゼロレーティングを制限し、ネット中立性を守る方針を打ち出しています。

日本では通信の秘密というポイントはありますが、最近話題となっているLINEモバイルの例ではその点はクリアされるのではないかと、また、そうなる今後広く他の事業者が追従していくことも考えられることから、まさに議論が始まっている状況であるという紹介がなされました。

セッションは、登壇者それぞれの私見の提示から、会場参加者を交えた議論へと移り、非常に多くの意見が挙げられました。プログラムの概要および発表資料は、下記をご参照いただければと思います。

ゼロレーティングを支える技術とローカルレギュレーション
<http://www.janog.gr.jp/meeting/janog38/program/zr>



● 今回のミーティングは「斬」がテーマでした

◆ セキュリティオペレーション: みんなどんなの使ってるの?

ここからは、筆者が注目したその他のセッションを二つご紹介します。

セキュリティと一口に言っても、広範な作業、分野がありますので、それぞれの分野で多様なツールが利用されています。このセッションでは、セキュリティオペレーションの要素、人材育成に関連するトピックスの紹介と、チームメンバーに求められるスキルセットの整理、そしてセキュリティオペレーションで利用されるツールについて紹介され、議論を求めていくというものでした。セキュリティの実践的なツールとして、実行用の隔離環境を整備することや、リバースエンジニアリングなど含めたマルウェア解析が実施されることもあったと紹介がありました。

また、その後に続いたBoF (Birds of a Feather) では、さらなるセキュリティ関係ツールの話題として、Vulsという注目されている脆弱性チェックツールについて、製作者を招いた紹介がありました。

セキュリティオペレーション: みんなどんなの使ってるの?
<http://www.janog.gr.jp/meeting/janog38/program/sox>

◆ Root DNS anycast performance in South Asia & Japan

ルートDNSは、13のルートサーバのIPアドレスが、Anycast技術を利用して世界中に伝播されることで実現されていて、実際には数百のDNSサーバで構成されています。

そのAnycastのパフォーマンスについて、RIPE Atlasを利用して南アジア、および日本で実際にどのように動作しているかという調査の結果報告がありました。レポートでは、ルートDNSサーバが存在する国であっても、リージョン内や海外のサーバを利用して通信を行うケースがあること、その割合の紹介がありました。

Root DNS anycast performance in South Asia & Japan
<http://www.janog.gr.jp/meeting/janog38/program/ripe>

◆ おわりに

今回取り上げたゼロレーティングにまつわる議論に関しては、さまざまな意見がありました。意見の中では、「現実を直視し、抗うというよりもどのように受け止めていけばよいのかを考える必要がある」ということや、「今までのビジネスモデルが本当によいのか、トラフィック

クに対するコストの負担について変えていく必要があるのではないか」という意見が挙がりました。また、「ゼロレーティングという枠組みですべてを議論するのではなく、通信の秘密とは分けて整理をした方がよいのではないか」など、多くのコメントがありました。

議論を受け、アクセス回線、バックボーン回線それぞれにキャパシティがある中、一部のトラフィックが優先制御されるということに不安があることが理解できました。利用者として多くの選択肢があり、また限定された利用目的向けの回線として用意することも可能である、MVNOなどのモバイルインフラでは問題は少ないかもしれませんが、地域や集合住宅の状況によっては選択肢が限定される、固定アクセス回線にもこのような動きが広まる可能性を考えると、個人として不安もあります。今後、一層動向の情報収集を行いたいと思いました。

最後になりましたが、ホストをはじめ運営に携わった方々には、沖縄という絶好のロケーションであることでもありましたが、素晴らしいホスピタリティのご提供、大変ありがとうございました。少し降雨もありましたが、心配されていた台風の直撃もなく、沖縄のよさを実感する滞在となりました。

次回のJANOG39は、2017年1月18日 (水) から20日 (金) に、DMM.comラボ社のホストにて、金沢で開催ということで紹介がありました。冬の金沢ということで魅力の紹介がありましたが、どのようなセッションがなされるのか、今から楽しみです。

(JPNIC 技術部 佐藤秀樹)



●懇親会には多くの方が参加していました

NETmundial Initiativeを振り返って

2016年7月7日(木)に公表された「NETmundial Initiative 宣言」によって、NETmundial Initiativeの活動が実質的に終了となりました。本稿では、NETmundial Initiative調整評議会のメンバーであった筆者が、18ヶ月の活動を振り返ります。

◆ はじめに

2016年7月21日に、JPNICから「NETmundial Initiative宣言の公表および活動の終了について」というアナウンスをしました(以下、NMI宣言と呼びます)。

NETmundial Initiative宣言の公表および活動の終了について
<https://www.nic.ad.jp/ja/topics/2016/20160721-01.html>

NETmundial Initiative(以下、NMIと呼びます)は、2014年4月にブラジル・サンパウロで開催されたNETmundial会合の協調精神を引き継ぎ、NETmundial会合の成果文書である、NETmundial 声明に示されたインターネットガバナンスに関する原則の実施を推進するために、ICANN、CGI.br(ブラジルインターネット調整委員会)、世界経済フォーラム(World Economic Forum, WEF)の三者の呼びかけで始まった活動です。声明で示された原則とロードマップに従って、「全ステークホルダー間での、実践的な協力関係を媒介するプラットフォーム提供をめざして」いるとしていました。この辺りの経緯については、2015年11月に発行したNo.61で詳解していますので、そちらもぜひご覧ください。

NETmundial Initiativeの活動について
<https://www.nic.ad.jp/ja/newsletter/No61/0630.html>

私は、NETmundial会合のマルチステークホルダー実行委員会(Executive Multistakeholder Committee, EMC)に引き続き、NMIの調整評議会(Coordination Council, CC)のメンバーを務めました。

この度のNMI宣言は、原文を一読しても少し分かりにくいのですが、今までの活動の整理を行った上で、既存の成果物の継承先などを示しており、冒頭のアナウンスにも示した通り、事実上NMIとしての活動の終了を意味しています。本稿では、調整評議会メンバーの目から、18ヶ月のNMIの活動を振り返ってみたいと思います。

◆ NMIのこれまでの活動

まず、NMIに関してJPNICが行ったアナウンスを示しながら、それぞれのタイミングでNMIがどのような活動を行ってきたかを示していきます。

2015年2月5日

NETmundial Initiative運営規約の策定に向けての意見募集(期限:2月16日)および調整評議会メンバーに前村昌紀選任のお知らせ

調整評議会メンバーの選定は2014年末でしたが、運営パートナーと呼ばれている設立発起3団体:ICANN、CGI.br、WEFによる立ち上げ準備は2014年春ごろから進んでおり、その段階で、進め方が不透明であるなどの指摘が相次ぎました。「I*」と呼ばれる技術コミュニティ関連団体でも、このNMIに対して一歩引いた立場を取る団体が目立つ中、不透明であればなおさらのこと、運営に影響を及ぼしうるポジションに誰かを置くべきと考え、JPNICの機関決定を経て、NETmundial会合でEMCを務めた私が出馬するという方向性を固めました。

2015年4月8日

NETmundial Initiativeによる「スタンフォードコミュニケ」の公表および運営規約案に関する意見募集開始について

2015年3月31日にスタンフォード大学で行われた作業会合は、当初は運営規約を採択する目的で計画されたものでしたが、よりコミュニティの声を反映した運営規約を作るべく、作業会合と位置づけ、運営規約案を採択して意見募集するという目的に変更しました。

2015年7月10日

NETmundial Initiativeによる「サンパウロコミュニケ」の公表および運営規約の公開について

2015年6月30日にサンパウロで開催された調整評議会会合は、運営規約を採択して正式に活動を開始するという一方で、「設立会合」と位置づけられました。運営規約が、調整評議会が考えたNMIの形が最も良く表現された文書です。「IV.活動の範囲」に挙げられた六つの活動項目のうち、1.のNETmundial会合成果の実施推進、2.~4.の触媒機能の他に、5.~6.の途上国支援も活動範囲に含まれ、意欲的なものになっています。

2016年2月28日:「マドリッドコミュニケ」

実はJPNICからのアナウンスで、一つだけ会合成果が抜けてい

ます。それは2016年2月28日のマドリッドコミュニケで、私自身がAPNICカンファレンスとの競合でマドリッド会合に参加できなかったのが一因です。

マドリッドコミュニケを読むと、発足時に調整評議会が任期満了を迎える2016年6月以降の体制を、CGI.brを中心にした体制で検討する必要があること(つまり、ICANNとWEFが運営パートナーから降りること)と、この体制が定まるまで、次期調整評議会のメンバー候補の推薦を凍結すること、などが示されていて、この時点でNMIの活動が縮小方向に転回したことが分かります。2015年6月に採択した運営規約には意欲的な活動項目が並んでいたわけですが、この転回は、8ヶ月後の2016年2月の段階で、これらを持続的な活動に結びつける算段が付かなかったことを意味します。

2016年7月21日:NETmundial Initiative宣言の公表

そしてここに至ります。あえて簡潔にこの2年弱を表現すると、「成功に終わったNETmundial会合の精神を引き継いで、さらに協調的な活動を推進する媒介機能を作ろうと野心的な取り組みをやってみたが、軌道に乗せることができなかった」ということになると思います。

方針検討に専心した活動でも事務局機能などを含めコストは掛かります。さらに、グローバルなインターネットに関する、マルチステークホルダーの活動となると、掛かるコストは跳

ね上がりますし、途上国支援という要素が必要になるのも必定でした。グローバルな協調活動を推進する媒介機能というアイデアは魅力的で、ソリューションマップのベータバージョンを眺めてもワクワクするものがありましたが、一方でそれを形にするのは、そうそうたるメンバーをもってしても難しすぎたということかもしれません。

◆ NMI調整評議会メンバーとしての活動を終えて

NETmundial会合のEMCは、正味半年、成果文書の取りまとめを行う作業でした。一方で今回はそれよりも長く、運営規約をはじめとするルールを作って活動を設計するという作業でした。NMIはNETmundial会合に引き続きマルチステークホルダー構成でしたが、各セグメントからのメンバーは、それぞれに有能でしたので刺激を受けましたし、良い経験になりました。

今後は、NETmundialフォローアップトラックとして、NETmundial声明の実施を見守る活動が残るわけですが、NMI宣言にも示されている通り、関連の国際会合で度々肯定的に取り上げられていることを含め、NETmundial声明が広くステークホルダーに受け入れられていることを実感します。また、NMIを通じて生み出されたソリューションマップと協調プラットフォームに関しても、今後1人でも多くの皆さんのお役に立てばと願うばかりです。

(JPNIC インターネット推進部 前村昌紀)



● NMI宣言が掲載されているNETmundialのブログページ

APrIGF2016レポート



2016年8月26(金)～29日(月)に、台湾・台北にてアジア太平洋地域におけるインターネットガバナンスフォーラム会議である、APrIGF2016が開催されました。本稿では、このAPrIGF2016の様子をご紹介します。

◆ はじめに

APrIGFの正式名称は「Asia Pacific Regional Internet Governance Forum」というもので、本会議はその名の通り、インターネットガバナンスについて、アジア太平洋地域の視点から議論を行う会議です。「IGF」と言うと、2005年の世界情報社会サミット(WSSIS)チュニスアジェンダを受けて開催された2006年のアテネ会合以来続いている国連管轄のフォーラムが有名ですが、この台北で開催されたIGFは「リージョナルIGF」と呼ばれるものです。

グローバルIGFと同じように毎年ホスト国が異なりますが、リージョナルIGFは国連が主催するグローバルIGFと異なり、地域のコミュニティから草の根的に発展したものです。APrIGFは2010年香港で開催されたのが最初でした。

◆ 全体概要

今回のAPrIGFは台湾情報基盤振興協会(NII)が主催し、そのCEOのKuo Wei Wu氏はAPNIC ECメンバー、ASO選出のICANN理事を務める等、APNICやJPNICとも親交があり、番号資源コミュニティに深く関わってきた方です。

政府関係者やローカル企業の招待などにかなり力を入れていたこともあり、今年のAPrIGFは過去最大の参加者数を記録し、事前の参加登録者数は500人を超え、会期中は現地の参加者は300人以上で、遠隔参加は380人にも上ったとのことでした。

地元台湾からも政府関係者、学生、企業の方の参加が見受けられ、日本からも開催地が近いことから企業、大学、総務省から合計10数名の方が参加・登壇されていました。

プログラムは人権とプライバシー、セキュリティ、資源管理など幅広い内容構成のもと、3日間にわたって1日3コマ、おおむね常時3トラックがバラレルで走り、合計約30セッションが開催されました。

◆ プログラム・議論の様子

グローバルIGFでは、特にメインセッションにおいては比較的概念的な議論が中心であることと比較すると、APrIGFは特定のテーマに対して、地域内各国の事例紹介を踏まえた具体的な・現実的な事情に基づいた議論が充実していました。プログラム一覧からは、多岐にわたるトピックスが議論されたことが見てとれます。

プログラム一覧

<https://2016.aprigrf.asia/program/agenda/>

なお、オープニングプレナリーでは、2016年5月に逝去された奈良先端科学技術大学院大学の山口英先生への追悼の時間が設けられ、村井純先生からのビデオメッセージに続き、会場からも山口先生と親交のあったみなさんからのメッセージが寄せられました。



● オープニングプレナリーでは故山口英氏への追悼の時間が設けられました

今回の会合では、筆者は「アジア太平洋地域におけるIPv6」というセッションを企画し、モデレーションを行いました。

IPv6については2015年、2016年とグローバルIGFでもIPv6 Best Practices Forumと呼ばれる議論の場が設けられ、最適な実例を文書化する取り組みがあるため、アジア太平洋地域のIGFでも同じ議論を行い、グローバルな場に地域の状況をイン

ットする必要性を感じたためです。同じアジア太平洋地域における会議ですが、技術面でのフォーカスが強いAPNIC会議では共有されない、政府・企業・国全体としての取り組みについて意見交換を行い、スリランカ、アフガニスタン等、あまり聞くことのできない個別事情を聞くことができました。あわせて、グローバルIGFにおけるBest Practices Forumの動向を共有したことにより、アジア太平洋地域とグローバルな動向の連携にもつながったように思います。

その他にも、

- ・通信を仲介する事業者の政府に対する情報提供に関する、ユーザーのプライバシー保護の責任を取り巻く課題に対する香港、中国、韓国等の事例
- ・TPPIにおいて電子商取引章および著作権保護の切り口から、TPP署名国、署名していない国それぞれからの登壇者が見解を紹介する

など、一般メディアで取り上げられているテーマも取り上げられていました。これらに日本からのインプットはありませんでしたが、日本は地域の中でどういう立場にあるのか、議論に参加してもよいテーマだったかもしれません。

◆ グローバルとの連携強化

グローバルIGFにおいては、国・地域別IGF(NRI)との連携強化は特に今年は重視されており、そういった動きも踏まえて、APrIGF事務局の提案により急遽、「IGF Intersessional Work / National & Regional Initiatives」が開催されました。

過去にグローバルIGFのMAG(プログラムを検討するグループ)のチェアを務めたMarkus Kumar氏と、現MAGメンバーとして筆者が動向を紹介しました。参加者との議論では、グローバルなIGFとの連携強化に加え、それぞれの国ごとの課題や事情を踏まえた議論が活発に行われ、今後も定期的実施してほしいとの要望が寄せられました。

日本としてもグローバルIGFとの連携強化に取り組んでいきたいところです。

◆ APrIGF2016の振り返り

「アジア太平洋地域」と言うと、多くの議論の場ではオーストラリア、ニュージーランドの参加者が発言の中心となることが多いのですが、今回のAPrIGFでは、地域内の参加

者がバランスよく発言していたように思います。グローバルな場でも一定のプレゼンスのある香港、中国、インドに加え、ローカルホストを務めた台湾、韓国、フィリピンからの参加が目立ち、南アジアからもインドの他にネパール、スリランカ等の国からの参加が見受けられました。そして、英語が母国語・公用語ではない国からも、複数の方が立派にモデレーションを務められていたことは励まされる現象です。

筆者のAPrIGFへの参加は、2010年の香港以降6年ぶりでした。通常、グローバルな場でアジア太平洋地域からの議論の参加は活発ではないことから、APrIGFでここまで活発な議論が行われていることを想定していませんでした。実際には、登壇者・参加者はグローバルな場で議論される問題もよく追った上で各国の事情を紹介しており、議論のレベル・問題への認識共に、日本国内の議論と比較して大変高いものでした。それぞれの国における議論が、APrIGFと同じレベルであるかはまた別の可能性はあるものの、日本インターネットガバナンス会議(IGCJ)にも関わっている立場から、大変よい刺激を受けました。

◆ 次回のAPrIGF

次回2017年のAPrIGFは、オーストラリアのccTLDである、.auのレジストリであるauDAがローカルホストを務め、オーストラリア・メルボルンで開催される予定です(最終日程は調整中とのことです)。リモートでも参加が可能ですので、ぜひ参加されてみてはいかがでしょうか。

(JPNIC インターネット推進部 奥谷泉)



● 会場の様子

第96回IETF報告



2016年7月17日(日)から22日(金)にかけて、ドイツの首都ベルリンにて、第96回IETFミーティングが開催されました。会場はインターコンチネンタル・ベルリンで、3年前の第87回IETFミーティングと同じ会場での開催となりました。本稿では、この第96回IETFミーティングの様子を、全体会議の報告を中心にお届けします。その他の動向については、P.36で概要と詳細なレポートへのURLをご紹介しますので、そちらも併せてご参照ください。

◆ ミーティング参加人数の近況

ここ2年ほどの参加登録者の数は1,000名から1,350名くらいで推移しています。今回は1,348名と多かったのですが、日本からの参加者数は2年前と比べるとやや少ない状況にあります。

開催場所	参加登録者数(括弧内は日本から)
第91回(ホノルル)	1,080名(76名)
第92回(ダラス)	1,176名(65名)
第93回(ブラハ)	1,358名(60名)
第94回(横浜)	1,198名(345名)
第95回(プエノスアイレス)	1,002名(41名)
第96回(ベルリン)	1,348名(52名)

この推移は、横浜開催は国内出張として参加しやすかったために人数が多く、一方、プエノスアイレス開催は旅費や旅程全体として時間がかかってしまうので日本からの参加者が少なかったのかもしれませんが、南米よりは日本から行きやすいベルリン開催でも、52名にとどまってしまったのを見ると、日本からの距離だけが原因ではないのかもしれませんが。



● 全体会議(プレナリー)の様子

◆ IETFハッカソン

IETFミーティングの直前の土曜日と日曜日に、IETFハッカソン(IETF Hackathon)が開催されました。IETFハッカソンとは、IETFで策定されたプロトコルについて、開発者同士の議論や協調を促進すると共に、ユーティリティ開発やアイデア出

し、サンプルコードの作成などが行われるイベントです。今回は5回目で、150名以上が参加し、20以上の「プロジェクト」と呼ばれる一連の作業が進められました。

IETFハッカソンでは、はじめに、提案されたプロジェクトを説明するプレゼンテーションがあります。参加者はあらかじめ、興味とスキルにあったプロジェクトに参加して、目標と達成方法を議論してから作業に入ります。

作業を行ったチームに対して、さまざまな賞が贈られました。おのおののチームにどのような賞が贈られたのかなどの詳細は報告スライドを、各チームの資料はIETF 96のハッカソンページをご覧くださいだと思います。

(IETF 96ハッカソンのチーム)

- ILA
IPv6 Identifier Locator Addressing (ILA) を実装し相互接続実験を行ったチーム。draft-herbert-nvo3-ila-02の実装を行いました。
- PCE-based Central Control
ラベルDBの実装を行い、Path Computation Element Communication Protocol (PCEP) の上でTLSを動作させました。
- I2RS
I2RS (Interface to Routing System) のためのYANGのデータモデルに関する実装とガイド作りに取り組みました。
- YANG / NETCONF / RESTCONF
YANGモデルのカタログとレジストリのツールを作りました。
- TLS 1.3
NSS、Apache、Firefox、ProtoTLS、MITLS、BoringSSLなどで、TLS 1.3の実装の相互接続テストを行いました。
- BGP-Flowspec / BGP-LS
draft-gredler-idr-bgp-ls-segment-routing-ext-02のセグメントルーティングの実装を行いました。

- IoT Bootstrapping for Noobs
<https://tools.ietf.org/html/draft-aura-eap-noob-01> の nimble out-of-band 認証の実装が行われました。
- DNS / DNSSEC / DPRIVE / DANE
DNSSECを応用する技術について、さまざまなオープンソースのプログラムを持ち寄った相互運用テストが行われました。
- IETFハッカソンの報告スライド
<https://www.ietf.org/proceedings/96/slides/slides-96-hackathon-23.pdf>
- IETF 96ハッカソンページ
<https://www.ietf.org/registration/MeetingWiki/wiki/96hackathon>

◆ アプライド・ネットワーク・リサーチワークショップ

技術研究の観点で活動しているIRTF (Internet Research Task Force) および学会のACM (Association for Computing Machinery) とISOCの共催で、アプライド・ネットワーク・リサーチワークショップ (Applied Networking Research Workshop - ANRW) が開かれました。今回はIETF 96ミーティング前日である2016年7月16日(土)の開催です。研究を公募する国際会議と同じ形式で、事前に論文とポスターが募集され、査読を通じて採否が決定されます。

テーマはMultipath、SDN、Routing and Peering、Transport Quality and “Happy Eyeballs”、Measurement、Internet Mediaと多岐にわたりました。論文(フルペーパー)は17応募され、うち9が採録されました。またショートペーパーとポスターは合わせると、応募が13で、うち採録が9でした。ワークショップのWebページでは、論文の他にプレゼンテーションの動画も見ることができます。

- Applied Networking Research Workshop 2016
<https://irtf.org/anrw/2016/>

◆ IETF 96全体会議からのトピック

IETF 96ミーティングでは、全体会議(プレナリー)は7月21日(水)に行われました。トピックとして3点報告したいと思います。

○プロトコルと技術のシンプルさ

IETFで策定されたプロトコルを実装するにあたって、複雑さが増してきていることを指摘したプレゼンテーションです。類似した目的のために技術としての選択肢がたくさんあり、このことで実装の相互運用性を確保することが難しくなっ

てきています。例えば、VPNやカプセル化のための、IP in IPやIPsec、MPLSやVXLANといったプロトコルがあるが故に、異なるプロトコルを実装した製品と相互接続できないケースが出てきていると指摘しています。

今日のインターネットは、マルチベンダーもしくはマルチサービスプロバイダーが相互に接続し、運用することによって成り立っていますので、標準化はとても重要です。その標準化活動においては、標準化された技術が実装されて製品に組み込まれていくことを踏まえて、選択肢を適切な数にとどめておくことも重要であるという指摘でした。

発表者のRoss Callon氏は、第1回IETFミーティングから参加しており、30年間にわたるIETFでの貢献に対して、会場からはスタンディングオベーションが送られていました。

- Keep it Simple, The Cost of (too many) Standards, Ross Callon
<https://www.ietf.org/proceedings/96/slides/slides-96-ietf-plenary-11.pdf>

○IETF基金

IETFの活動を長期的にサポートしていくための、基金が設立されました。ミーティングに参加するための金銭的な補助をはじめ、IETFの活動における検討課題に取り組むための、サポートのための基金とされています。現在のところ、ARINやRIPE NCC、AfriNICといったRIRの他に、企業や個人が寄付を行っています。

- IETF Endowment
<http://www.sustainietf.org/>

○IETFシスターズ

IETFの参加者は男性が多いのですが、女性同士で意見交換をしたり、助言を得たりするための場が設けられています。IETF 96ミーティング期間中の7月21日(木)には、ランチ会合が開かれていた模様です。下記のページでは、メーリングリストも紹介されています。

- IETF Systems (IETFブログの記事)
<https://www.ietf.org/blog/2016/07/ietf-systems/>



今回のIETF 97は、2016年11月13日(日)から18日(金)にかけて、韓国のソウルで開催されます。

(JPNIC 技術部/インターネット推進部 木村泰司)

IPv6関連WGの動向

IPv6基本プロトコルの保守を行うことが目的の6man (IPv6 maintenance) WGでは、IPv6基本仕様のInternet Standard (IS) 化に向けて残項目の整理が行われるなど、IPv6関連WGの標準化動向は終盤を迎えつつあると言えるようです。

この6man WGに加えて、v6ops (IPv6 operation) WGや移行技術を扱うその他のWGの動向、maprg (Proposed Measurement and Analysis for Protocols Research Group) における発表など、主な議論の概要について富士通株式会社松平直樹氏にレポートをご執筆いただきました。

詳しい内容については、次のURLをご覧ください。

第96回IETF報告「IPv6関連WG報告 ～6man WG、v6ops WG、maprg WG～」
<https://www.nic.ad.jp/ja/mailmagazine/backnumber/2016/vol1427.html>



DNS関連WGの動向

DNS関連のInternet-Draftについては、前回の会合から今回までの間に、RFC7901、RFC7873、RFC7871の三つがRFCとして発行されました。それに加えて、三つのInternet-DraftがIESG (Internet Engineering Steering Group) Evaluationの段階にあり、五つのInternet-DraftがWG Last Callを行う段階となっています。

今回のIETF会合に関して、dnsop (Domain Name System Operations) WGとdnssd (Extensions for Scalable DNS Service Discovery) WGの二つのWGに関する動向を中心に、ルート

ゾーンのDNSSEC鍵更新の話題も交えて、DNS関連の話題について東京大学の関谷勇司氏にレポートをご執筆いただきました。

詳しい内容については、次のURLをご覧ください。

第96回IETF報告「DNS関連WG報告」
<https://www.nic.ad.jp/ja/mailmagazine/backnumber/2016/vol1428.html>



セキュリティ関連の動向

IETFではセキュリティに関する議論が多岐にわたって行われており、扱う分野が広がることはあっても減ることはない状況です。そのため、すべてに関して取り上げることはできませんが、NTTコミュニケーションズ株式会社の西塚要氏と、株式会社レピダムの前田薫氏のお二人に、今回のIETF会合のレポートをご執筆いただきました。

西塚氏にはDOTS (DDoS Open Threat Signaling) WGを中心にDDoS対策技術に関する議論について、前田氏にはWebにおける認可プロトコルの仕様を扱うOAuth WGと、SSL/TLSの次バージョンである1.3策定の最終検討段階に入ったTLS WGでの議論について、ご紹介いただいています。

それぞれの詳しい内容については、次のURLをご覧ください。

第96回IETF報告「セキュリティ関連報告(1) ～DDoS対策技術についてDOTS WGを中心に～」
<https://www.nic.ad.jp/ja/mailmagazine/backnumber/2016/vol1429.html>



第96回IETF報告「セキュリティ関連報告(2) ～OAuth、TLS編～」
<https://www.nic.ad.jp/ja/mailmagazine/backnumber/2016/vol1431.html>



次世代WHOISプロトコル「RDAP」のご紹介

IPアドレスやドメイン名の参照のために使われているWHOISプロトコルについて、置き換えるための議論が現在行われています。本稿では、WHOISの後継プロトコルと言われている、RDAPについてご紹介します。

◆ RDAPとは

RDAP (Registration Data Access Protocol) は、策定から長時間経過しさまざまな課題が指摘されているWHOISプロトコルの後継を意図して、標準化されたプロトコルです。IETFのweirds (Web Extensible Internet Registration Data Service) ワーキンググループ (WG) にて関連のRFC (RFC7480～7485) が2015年に発行され、weirds WGは同年に活動終了しました。RDAPの議論は、IETFでは現在ではregext (Registration Protocols Extensions) WGで取り扱われています。

RDAPの主な特徴としては、応答の際にJSON (JavaScript Object Notation) 形式のデータを返すように標準が定められており機械可読性が高いこと、RDAPサーバー間の連携により、クライアントからのクエリを適切なサーバーにリダイレクトできる機能があることが挙げられます。

従来のWHOISプロトコルは、応答の形式が規格上定められておらず、フリーテキスト形式であったことから、各レジストリにより応答の形式が異なっていました。そのため、機械的な解読にかけるには、オペレーターがその差を意識して対応する必要がありました。また、従来のWHOISプロトコルでは、WHOISサーバー間の連携が規格上定められておらず、オペレーターがどのレジストリで管理されている情報であるのかを、あらかじめ確認してからWHOISサーバーに問い合わせる必要がありました。一方、RDAPの場合は、どのレジストリも統一されたJSON形式でデータを返すことから、機械的な処理が容易となっています。

また、RDAPにはbootstrapと呼ばれる機能があり、RDAPサーバーに問い合わせるクライアントは、目的のIPアドレスがどの地域インターネットレジストリ (RIR) で管理されているかを、bootstrap管理ファイルを参照した状態で問い合わせることができます。これにより、人手でRIRの管理状態を確認しなくても済むので、機械的な処理が容易になります。RIRによっては、管理外IPアドレスの問い合わせがあった場合、自動的に適切なサーバーへリダイレクト処理する機能をサービスしているところもあります。現時点では、APNIC・ARIN・RIPE NCCのサーバーがその機能を備えています。

例えば、APNICのRDAPサーバーで管理されている「202.12.30.

110」のIPアドレスを、ARINのRDAPサーバーへ問い合わせた場合、自動的にAPNICのRDAPサーバーにリダイレクトされて応答が返ることを確認できます。APNICのRDAPサーバーからは、以下のような問い合わせ結果が返ってきます (長い一部を省略しています)。

```
{
  "handle": "202.12.30.0 - 202.12.30.255",
  "startAddress": "202.12.30.0",
  "endAddress": "202.12.30.255",
  "ipVersion": "v4",
  "name": "JPNIC-NET-JP",
  "type": "ASSIGNED PORTABLE",
  "country": "JP",
  "objectClassName": "ip network",
  "entities": [
    {
      "handle": "IRT-JPNIC-JP",
      "vcardArray": [
        {
          "vcard": [
            [
              {
                "version": {},
                "text": "4.0"
              },
              {
                "kind": {},
                "text": "group"
              },
              {
                "email": {},
                "pref": "1"
              },
              {
                "text": "hostmaster@nic.ad.jp"
              },
              {
                "adr": [
                  {
                    "label": "Urbannet-Kanda Bldg 4F, 3-6-2 Uchi-Kanda\\nChiyoda-ku, Tokyo 101-0047, Japan"
                  },
                  {
                    "kind": {},
                    "text": "group"
                  },
                  {
                    "email": {},
                    "text": "hostmaster@nic.ad.jp"
                  }
                ]
              },
              {
                "roles": [
                  "abuse"
                ]
              },
              {
                "objectClassName": "entity"
              }
            ]
          }
        }
      ]
    }
  ],
  "port43": "whois.apnic.net"
}
```

◆ 各RIRにおけるRDAPサービス提供について

現在、五つのRIRにてRDAPがサービス提供されています。

- APNIC
<https://rdap.apnic.net/>
- ARIN
<https://rdap.arin.net/registry>
- RIPE NCC
<https://rdap.db.ripe.net/>
- LACNIC
<https://rdap.lacnic.net/rdap/>
- AFRINIC
<https://rdap.afrinic.net/rdap/>

JPNICでは各RIRのサービス状況を調査しており、個別にAPNICに照会したところ、APNICのRDAPサーバーについては2016年1月の統計情報にて、月間60万程度のクエリ量、2qpsとなっている旨の回答がありました。

また、Registration Operations Workshops (ROW) という、レジストリに関するオペレーションを議論するワークショップがあるのですが、2016年4月に開催された4th ROWミーティングの資料によると、LACNICでは月間18万程度のクエリ量(2015年5月~2016年3月)、ARINでは113qps(期間は不明)との情報があります。

◆ RDAPクエリの形式

RDAPのクエリには所定の形式があり、IPアドレス・AS番号・ドメイン名を定められた方式で問い合わせることができます。

IPアドレスを問い合わせる場合は、該当RDAPサーバーのURLの配下に「ip/192.0.2.0/24」または「ip/2001:db8::/32」のように、目的のIPアドレスを付けると応答が返ります(サブネットマスクはIPアドレスの後に、さらにスラッシュを付けることとなります)。

AS番号の場合は同様に「autnum/NNNN」と目的の番号を付けることとなります。

ドメイン名の場合は、ドメインを管理しているレジストリのRDAPサーバーのURL配下に「/domain/example.domain」と問い合わせることとなります(RIRはドメイン名についてのサービスは提供しておりません)。

◆ 参考リンク集

IETF weirds WG (現在は活動終了)
<https://tools.ietf.org/wg/weirds/>

IETF regext WG
<https://tools.ietf.org/wg/regext/>

IANA IPv4 Address Space Registry (アドレス空間ごとのRDAPサーバーのリンク掲載)
<http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml>

IANA IPv6 Address Space Registry (アドレス空間ごとのRDAPサーバーのリンク掲載)
<http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml>

LACNICのRDAPについての発表資料(4th ROWミーティングの資料)
<http://regiops.net/wp-content/uploads/2016/04/3-Agustin-Formoso-LACNIC%E2%80%99s-RDAP-implementation.pdf>

ARINのRDAPについての発表資料(4th ROWミーティングの資料)
<http://regiops.net/wp-content/uploads/2016/04/7-Andrew-Newton-The-State-of-RDAP-in-the-RIR-Space.pdf>

第37回ICANN報告会 [7. WHOISに関する動向]
<https://www.nic.ad.jp/ja/materials/icann-report/20130820-ICANN/20130820-7.pdf>

JPNIC Newsletter No.63
 「APRICOT 2016/APNIC 41カンファレンス報告 - 技術動向報告」
<https://www.nic.ad.jp/ja/newsletter/No63/0620.html>

(JPNIC 技術部 澁谷 晃)

自組織サーバのIPアドレスに対する経路情報が、インターネットで存在しているのかどうかを調べるには、RIPE NCCが運営しているRIPEstatと呼ばれるWebサイトが利用できます。あらかじめIPアドレスが分かれば、閲覧しているWebサイトがどの通信事業者のネットワークに収容されているのか、そしてインターネットからの到達性がどれくらいあるのかを見ることがもできます。

RIPEstat
<https://stat.ripe.net/>

下図はJPNIC Blogのサーバが含まれているIPアドレスを検索した結果です。経路情報が欠けることなく観測されていることが分かります。(図)

◆ 経路情報の監視方法

経路情報がなくなったり、おかしい経路情報がインターネットに流れたりした時に気づくためには、どのような方法があるのでしょうか。海外のものにはBGPmonのサービスがあります。BGPmonにユーザー登録をすると、限られた数の経路情報を監視することができます。一方、国内で利用できるものとして、JPNICでは二つの方法を提供しています。

経路奉行

- JPIRRのroute objectにメールアドレスを記述しておく方法
- JPNICでおかしな経路情報が観測された時には、登録されているメールアドレスに通知が送られる
<https://www.nic.ad.jp/doc/jpnic-01077.html#3>

ROA (Route Origin Authorization)

- 本来の経路情報をROAとして登録しておく方法
- 対応したBGPルータなどで経路情報をチェックするために利用できる
- 国際的に普及が始まっている方式で、国内外の多くの箇所で経路情報をチェックするために使うことができる
<https://www.nic.ad.jp/ja/rpki/howto-usepubcache.html>

◆ ROAの確認方法

また、ROAが登録されているかどうかを確認できるように、下記のWebサイトを公開しています。

RPKI Validator (日本語版)
<http://roa2.nic.ad.jp:8080/bgp-preview>

このRPKI ValidatorにIPアドレスを入力すると、ROAと経路情報を比較した結果が表示されます。具体的には、ROAに対応したBGPルータにおいてどのように見えるかについて、RRC (Remote Route Collector) を使って再現しています。RPKI Validatorでは、ROAに記載されている本来の経路情報と、RRCによって収集された経路情報を比較しています。ROAに記載された通りの経路情報があれば「Valid」、ROAの記載と違う経路情報があれば「Invalid」、ROAの記載はあっても該当する経路情報が見つからない場合には「Unknown」となります。

RPKI ValidatorはRRCによって蓄積された経路情報を定期的にダウンロードしているため、最終更新日が画面に表示されます。またピア先(接続先)が多いほど、インターネットの主要

インターネットからの到達性を確認するために ~ 経路情報の確認について ~

重要なWebサイトを構築してもインターネットの一部からそのサーバにアクセスできなくなることがあります。本稿ではインターネット側からの到達性に注目して、到達性の確認方法と監視の技術を紹介します。

◆ はじめに

経路情報がなくなる事件はどれくらい起きているのでしょうか。右にURLを挙げたインターネットの経路情報を調査しているDyn ResearchやBGPmonのブログなどを見てみると、海外では高い頻度で起きていることが分かります。国内では、JPNICで観測できるものは月に10件以上あります。ただしネットワーク機器のメンテナンスに伴って経路情報が変更されるような通常のものも含まれています。

Dyn Researchのツイート
<https://twitter.com/DynResearch>

BGPmonのブログ
<http://www.bgpmon.net/blog/>

図 RIPEstatでの検索結果

RRC	IXP Location	Location	IPv4 peers seeing	IPv4 Visibility
RRC00	RIPE-NCC Multihop	Amsterdam, Netherlands	14 of 14	100%
RRC01	LIHX	London, United Kingdom	7 of 7	100%
RRC03	AMS-IX / NL-IX	Amsterdam, Netherlands	6 of 6	100%
RRC04	CEIX	Geneva, Switzerland	8 of 8	100%
RRC05	VIX	Vienna, Austria	4 of 4	100%
RRC06	DIX-IE	Tokyo, Japan	2 of 2	100%
RRC07	Nethod	Stockholm, Sweden	5 of 5	100%
RRC10	MIX	Milan, Italy	10 of 10	100%
RRC11	NYIX	New York City, US	9 of 9	100%
RRC12	DE-CIX	Frankfurt, Germany	13 of 13	100%
RRC13	MSK-IX	Moscow, Russian Federation	11 of 11	100%
RRC14	PAIX	Palo Alto, US	7 of 7	100%
RRC15	PTTMetro	Sao Paulo, Brazil	15 of 15	100%
RRC16	NOTA	Miami, US	3 of 3	100%
RRC18	Catnix	Barcelona, Spain	1 of 1	100%
RRC19	NAP Africa 1B	Johannesburg, South Africa	6 of 6	100%
RRC20	SwissIX	Zurich, Switzerland	18 of 18	100%

● RIPEstatでの192.41.192.0/24の検索結果

な箇所であることがわかります。その地点からのVisibilityは、より広範囲からの到達性に影響することになります。

210.173.160.0/19や210.251.160.0/20と入力すると「Valid」と表示されます。これはROAが登録済で、しかもインターネットで観測されている経路情報と一致していることを意味しています。「5より多くのピア先」の観測ですので、インターネットの狭い範囲からではなく、比較的広域のインターネットから到達性があると考えられます。

● 検証結果が「VALID」となる例

2001:7fb:ff03::/48 (RPKI Validatorの例) を入力すると、ROAに対応した経路情報がないため「Unknown」と表示されます。ROAは登録されていても、実際には経路情報が存在しないケースです。将来的に現れる経路情報を予めROAとして登録されたものである可能性もあるため、静観しておいても問題ありません。

● 検証結果が「UNKNOWN」となる例

93.175.147.0/25 (RPKI Validatorの例) と入力すると「INVALID ASN」と表示されます。これは本来とは異なるネットワークでIPアドレスが使われていることを示しています。この例は、ネットワーク機器を不適切に操作してIPアドレスを勝手に使い、本来のネットワークへの到達性を奪っているようなケースではなく、RPKI Validatorでこの表示が出ることを見込んであえて設けられたアドレスです。

● 検証結果が「INVALID ASN」となる例

IPアドレスを入力しても、「No matching records found」と表示される場合にはROAが存在していないことを示しています。ROAがないと本来の経路情報が分からないため、インターネットで存在すべき経路情報があるかどうかの判定を行うことができません。

なおWebブラウザのFirefoxには、アクセスしているWebサーバが、ROAとして登録されているIPアドレスの範囲に入っているかを簡単に確認できるAdd-onがあります。

RPKI Validator :: Add-ons for Firefox

<https://addons.mozilla.org/ja/firefox/addon/rpki-validator/>

◆ ROAを登録するためには

ROAを登録するにはどうすればいいでしょうか。JPNICのIPアドレスの申請で使われている電子証明書の発行を受けていて、インストールされている場合は、そのWebブラウザで下記のWebサイトにアクセスするとROAの登録ができます。電子証明書がインストールされていない場合や、入手方法をお知りになりたい場合、またROAの詳細などにつきましては下記までお問い合わせください。

JPNIC RPKIシステム

<https://rpki.nic.ad.jp/>

お問い合わせ先: JPNIC RPKI担当

rpki-query@nic.ad.jp

インターネットからサーバへの到達性が失われる要因はいろいろと考えられますが、インターネット上に正しい経路情報がなければ、IPパケットが転送されてくることはありません。この機会に、経路奉行やROAの登録をご検討いただければと思います。

(JPNIC 技術部／インターネット推進部 木村泰司)