JPNIC Newsletter

for JPNIC Members

No.59
March
2015

JPNIC 一般社団法人 日本ネットワークインフォメーションセンター

No.59
March
2015

JPNIC Newsletter

for JPNIC Members

CONTENTS

巻頭言

▸▸▸Introduction

歴史的な進化を同時に迎えるインターネット

オリンピックが東京で開催される2020年には、インターネットに接続できる端末数は、世界人口をはるかに超える500億となることが予測され、2007年のスマートデバイスの登場以降、ウェアラブル端末、スマートメーター、コネクテッドカーの登場とともに、多様化する端末数は毎年数10億の単位で急増しています（参考:2015年1月末時点で145億ユーザー）。これら膨大なユーザーが接続する上で前提となるのはIPv6であり、既に医療分野や自動車・航空業界などでは、IPv6による積極的なネットワーク化によるアプリケーション開発が推進されています。また、コンテンツの観点からは、これまで人類が過去2000年にわたって2エクサバイトのデータを生成したことを踏まえると脅威的と言える、毎日同容量（2エクサバイト）のデータが生成され続けており、モバイル、ソーシャルと共にデジタル化された情報流通基盤としてのインターネット利用は順調に発展し続けています。さらに、従来テクノロジーの観点で取り扱われて来た“IoT（Internet of Things）”は、2013年には、ビジネス面であらゆる産業分野へ革命的なインパクトを与える、インターネットがもたらす産業革命の時代を迎えたとして世界的な注目を浴びています。

そのような明るい未来を提供するインターネット利用の大前提として、基盤リソースの信頼性と安定性の確保が求められますが、テクノロジー、ガバナンスとポリシーのいずれの重要領域においても、今、インターネット利用を取り巻く環境は大きな節目を迎えています。

テクノロジーの面では、IoT時代のインターネット技術アーキテクチャーの発展により、多様化するエンドポイントを柔軟に利用できるエッジネットワークが登場し、またセキュリティ面からも高度化していくことが期待されています。

ガバナンス、ポリシーの領域では、IANA監督機能のマルチステークホルダーコミュニティへの移管という歴史的な変化が進行中であることに加え、インターネットガバナンスを巡りIGF、NETmundial Initiativeなどマルチステークホルダーが集まり、対話を行いステークホルダー間での調整を促し、人類の連帯や経済発展のためにインターネットが共有された中立で世界的な基盤であることを促進する場をめざした、国際的な活動団体が複数存在します。またポリシーにおいても、各国で整備されるサイバーセキュリティ法案や、データ保管のローカライゼーション、プライバシー保護ポリシーの整備など、多岐にわたる重要な変化が同時進行中です。

インターネットと社会との関わりが深くなった今、これらガバナンス、ポリシー面で議論、取り扱われるテーマと内容は、広範かつ複雑化していることから、従来のインターネットコミュニティの仕組みの中で全体を俯瞰することも難しくなっています。そのような中、インターネットガバナンスを取り巻く世界的状況の変化に応じるべく、2014年にJPNICが発起人となり「日本インターネットガバナンス会議（IGCJ: Internet Governance Conference Japan）」が発足し、日本におけるインターネットガバナンス関連動向を共有、議論する場が設けられたことは非常に頼もしく思います。IGCJの設立を機に、インターネットへ関心を寄せるコミュニティが活性化されると共に、グローバルでオープンなインターネットの健全性を継続的に維持していく上では、このようなインターネットへの影響が少なからず想像される領域の議論や会合へ、日本からの参画メンバーが増えていくことを期待します。

シスコシステムズ合同会社
専務執行役員
最高技術責任者（CTO）
木下 剛
（きのした つよし）

プロフィール

シスコシステムズ合同会社において、専務執行役員 最高技術責任者（CTO）として、戦略事業開発並びにIoEイノベーションセンターを担当。現在、一般財団法人インターネット協会（IAjapan） 副理事長、無線LANビジネス推進連絡会 副会長、IPv6普及・高度化推進協議会 理事、新経済連盟IoT価値創造ワーキンググループ 主査を務め、積極的な社外活動を通じたインターネットの発展へ業界のメンバーとともに取り組む。

インターネットガバナンスの動向
～IANA監督権限移管後の体制に関するコミュニティからの提案～

特集1では、インターネットガバナンスの最新動向として、再びIANA監督権限移管の話題を取り上げます。本稿執筆時点（2015年1月下旬）では、IANAが管理する三つの資源（番号資源（IPアドレス）、プロトコルパラメータ、ドメイン名）の管理方針を検討するコミュニティ（Operational Communities）より、それぞれの資源に関するIANA監督権限移管後の体制についての提案が出そろいつつあり、大きく状況が動いています。JPNIC Newsletterでは、2014年3月に発行したNo.56から、4号連続でインターネットガバナンスに関する話題をお届けしていますが、読者の皆さまにおかれても、ぜひともこの状況を注視していただきたいと思います。

IANA監督権限移管に関しては、2014年7月に組成されたIANA Stewardship Transition Coordination Group（ICG）※1が同年9月に、移管後の管理体制について提案募集を開始しました※2。それに従い、IANAが管理する「IPアドレス」「ドメイン名」「プロトコルパラメータ」という三つの資源について、現時点で方針の検討を実際に行っている組織が、当該資源に関する移管後の管理体制を検討し、2015年1月15日に設定された締め切りまでに、ICG宛てに提案を提出することになりました。つまり、IPアドレスについては「RIRコミュニティ」が、ドメイン名については「ICANNコミュニティ」が、そしてプロトコルパラメータについては「IETF」が、提案を提出することになったのです。執筆時点では、あらかじめ提出遅延の見通しを表明していたドメイン名関連のICANNコミュニティを除き、提案が提出された段階です。

以降では、現時点でのそれぞれのコミュニティによる検討状況をお伝えします。

IPアドレス - サービスレベル協定とレビュー委員会

IPアドレスは、2014年9月から11月にかけて各RIRにより開催されたミーティングを中心に、五つのRIRコミュニティで提案の検討が進みました。これら五つのRIRにおける検討を統合してICGに提出する提案をまとめるために、同年11月に、CRISPチーム（Consolidated RIR IANA Stewardship Proposal Team）※3が、各RIRコミュニティから2名、各RIRの職員1名の総勢15名によって構成されました。JPNICの奥谷泉は、APNIC地域のメンバーに選出されるとともに、CRISPチームのチェアにも就任し、提案をまとめ上げることになりました。

APNICでは、ICGの提案募集要領公表直後に開催されたAPNIC 38カンファレンスで、移管後体制の要旨をたたき台として提案し、コミュニティのラフコンセンサスを取り付けました。RIPEも、APNICと同様の提案内容に基づいて議論を行いました。ARINとAFRINICでは、それぞれコミュニティに対して意向の調査を実施し、それに基づいた議論が行われました。LACNICでは、MONC（Multistakeholder Oversight Number Council）という監督機構を設けることが議論に挙がったのが特徴的です。

結果として、移管後管理体制の大原則に関しては同じ方向性が見えつつも、監督機構という新たな要素が一つのRIRから提案されたという状態で、CRISPチームはIPアドレスに関する統合提案の作成を託されました。

CRISPチームは、全RIRミーティングが終了した12月初旬から本格的な検討を開始し、途中2版のドラフトを公開し、そこで得られた意見を丁寧に勘案しつつ、年末年始休暇の時期も含め、集中的に検討しました。その結果、IPアドレスコミュニティとしての統一提案を、ICGが設定した提出期限である2015年1月15日にICGに提出しました※4。IPアドレスに関する統合提案の要旨は、以下の4点となりました。

（1）ICANNが、IPアドレスなど番号資源に関するIANA機能を引き続き運営し、これをRIRとの契約に基づいて行うこと
（2）IANAサービス提供に関する知的財産関連の権利（商標「IANA」、iana.orgドメイン名、データベースの利用権）は、コミュニティにとどめること
（3）IANAの番号資源に関するサービスレベル合意を、IANA機能運営者であるICANNとRIRとの間で取り交わすこと
（4）各RIRの代表からなるレビュー委員会を組成し、IANA機能の運営が、取り決められたサービスレベルを満たすかどうか、NRO EC（全RIRの最高経営責任者（CEO）からなる、NROのExecutive Council）に助言を行うこと

これらは、APNICとRIPEによる大原則を採用しつつ、LACNICのMONCのアイデアを一部取り入れるとともに、CRISPの検討において立ち上った知的財産権への言及を含めた、という形です。

ドメイン名 - NTIAの役割を整理し、マルチステークホルダーによる機構に置き換え

ドメイン名に関しては、ccTLDとgTLDを一括して、ICANNに設けられたワーキンググループである、Cross Community Working Group to Develop an IANA Stewardship Transition Proposal on Naming Related Functions（以下CCWG）※5で検討が行われました。

ICANNは、そもそもマルチステークホルダーで構成されたコミュニティで、考え方が多様ですので、理事会決定やサービス提供に関する不満の声が少なくありません。そういった状況を反映してか、NTIAが去った後のIANA機能の説明責任機構を考える上では、ICANN自体の説明責任機構を強化する必要があるという考えが、ICANNコミュニティ内に根強くあります。IANA機能に関する監督権限や説明責任の機構と、ICANN自体に関するそれらを整理するのに時間がかかり、2014年10月に開催されたロサンゼルス会議の場で、やっとCCWGが内容の検討に着手しました。

着手後の検討は集中的に急ピッチで進み、その結果、同12月1日には最終提案の様式でドラフト※6が公開され、意見募集にかけられました。内容としては、IANA機能監督に関してNTIA内部に設置されている機構の構造を踏襲することを旨に、IANA機能に関してICANNと契約を結ぶ契約法人（Contract Company）、契約法人の意思決定を担うために法人の外に設けられるマルチステークホルダーレビューチーム（Multistakeholder Review Team, MRT）、直接のサービス受益者であるレジストリの意見をまとめる顧客常設委員会（Customer Standing Committee）、不服申し立てを処理する独立抗告パネル（Independent Appeals Panel, IAP）からなる仕組みで構成されています。

冒頭で述べた通り、当初のICGへの提出期限を過ぎた本稿執筆時点で、提出版は公開されておらず、CCWGでは提案の最終調整を集中的に行っている状況です。

プロトコルパラメータ - 基本的に現行の枠組みを踏襲

プロトコルパラメータに関しては、既存の枠組みをそのまま適用する方向で、検討が進みました。IETFの標準的なプロセスにのっとって、2014年7月にカナダ・トロントで開催されたIETF 90会合でBoFが開催された後、ianaplanというWGが設立されました。WGでは、draft-ietf-ianaplan-icg-responseという名称のインターネットドラフトをRFCとして採択するという作業となりましたが、その9版※7でRFC化に向けてInternet Engineering Steering Group（IESG）の承認が降りたものが、2015年1月6日に、ICGに提出されました。

内容としては、IANA機能についてICANNと取り交わされ、RFC2860として公開されている覚書、およびプロトコルパラメータのレジストリ機能を定めたRFC6220を基とした枠組みだけで、特段に新たな機構が必要ないという見解を示すとともに、移行にあたってプロトコルパラメータは公有のものであることをすべての関係者で確認すること、将来的にICANN以外の団体がIANA機能運営者となる場合の、移行時にあるべき配慮を示したものとなりました。

今後

ICGでは、今後各資源に関する提案を統合する作業に入り、3月までに統合提案の素案を作成、意見募集の上、7月までに最終提案をNTIAに提出するという予定になっています。3資源の提案は、それぞれの既存の枠組みや背景から、違う機構を含んでいます。また、ドメイン名に関しては提案されている機構が複雑であり、これがNTIAで受け入れられるための調整作業は、難航が予想されます。

JPNICでは今後も本件への注視を続け、情報提供に努めてまいります。また、日本の関係者の皆さんの意見を移管後体制に反映させるべく、グローバルな検討への参画や、日本インターネットガバナンス会議（IGCJ）を中心とした意見収集と議論の場の運営などを積極的に行っていきます。ご不明な点などあれば、ingov-query@nic.ad.jpに、ぜひともお気軽にお問い合わせください。

（JPNIC インターネット推進部 前村昌紀）

※1 NTIA IANA Functions' Stewardship Transition
http://ianacg.org/

※2 IANA Stewardship Transition Coordination Group Issues Request for Transition Proposals and Suggested Transition Process Timeline
https://www.icann.org/news/announcement-2014-09-09-en

※3 Consolidated RIR IANA Stewardship Proposal Team（CRISP Team）メンバーの一覧、会議日程、各会議の資料や録音が参照可能
https://www.nro.net/nro-and-internet-governance/iana-oversight/consolidated-rir-iana-stewardship-proposal-team-crisp-team

※4 Response to the IANA Stewardship Transition Coordination Group Request for Proposals on the IANA from the Internet Number Community
https://www.nro.net/wp-content/uploads/ICG-RFP-Number-Resource-Proposal.pdf

※5 CWG to Develop an IANA Stewardship Transition Proposal on Naming Related Functions
https://community.icann.org/display/gnsocwgdtstwrdshp/CWG+to+Develop+an+IANA+Stewardship+Transition+Proposal+on+Naming+Related+Functions

※6 Cross Community Working Group（CWG）On Naming Related Functions Public Consultation on Draft Transition Proposal, 1 December 2014
https://www.icann.org/en/system/files/files/cwg-naming-transition-01dec14-en.pdf

※7 Internet Draft "draft-ietf-ianaplan-icg-response-09", Draft Response to the Internet Coordination Group Request for Proposals on the IANA protocol parameters registries
https://tools.ietf.org/rfc/rfc6220.txt

Internet Week 2014／IP Meeting 2014 開催報告

～あらためて“みんなの”インターネットを考えよう～

Internet Week 2014 ～あらためて“みんなの”インターネットを考えよう～ 開催報告

2014年11月18日（火）から21日（金）まで、JPNICは毎年恒例のInternet Weekを開催しました。本稿ではその模様を簡単に振り返ります。

2013年をさらに超えたプログラム数

今年の総プログラム数は、42（有料プログラム26、無料プログラム10、懇親会1、同時開催イベント5）となりました。会場を横浜から東京に移して以降、最多だった昨年2013年を一つ上回り、わずかではありますが、またしても最多記録を更新しました。

最終的な参加者数は、Internet Week 2013と同水準の約2,650名（延べ人数、同時開催イベントの参加者数を含む）となりました。今年もたくさんの方にご参加いただいたことに、この場を借りて御礼申し上げます。

あらためてインターネットを考える場に

「あらためて“みんなの”インターネットを考えよう」。これが今年のInternet Weekのテーマでした。

実行委員会でテーマを考えていたのは2014年4月上旬。ちょうどOpenSSLの脆弱性が発覚した直後で、今年のInternet Weekは間違いなくセキュリティの話題が中心になるだろうと話していたものです。技術的な話題以外にも、その前月の3月中旬に米国政府がDNSの管理権限を移管する意向を明らかにするなど※1、インターネットガバナンスの分野でも大きな動きがありました。ちょうどこの時期、多くの人の関心を集めていた二つのトピックのどちらにも当てはまるのではないかということで、近年まれに見る早さで決まったのがこのテーマです。

今年の2本柱：セキュリティとインターネットガバナンス

前述のテーマの下、検討されたのがInternet Week 2014のプログラム※2です。

最近ではすっかりInternet Weekの常連となった、各種サイバー攻撃の現状と対策を紹介するプログラムはもちろん、SOC（Security Operation Center）とCSIRT（Computer Security Incident Response Team）の相互理解を促進してより良いインシデント解決をめざすプログラム、最近のセキュリティ人材育成の取り組みを紹介するプログラムなどの新顔も。毎年恒例のDNS DAYでもセキュリティの対応に大きく時間を割くなど、ほぼ毎時間帯、どこかのプログラムでセキュリティの話題が取り上げられていた、と言っても過言ではないかもしれません。

もう一つの柱であるインターネットガバナンスは、「第4回日本インターネットガバナンス会議（IGCJ）」と、「IP Meeting 2014」で取り上げました。2014年6月に発足したIGCJは、Internet Weekまでに3回の会合を重ねてきました。今回は単独開催時よりも幅広い方にご参加いただき、有意義な情報提供と議論を行うことができたのではないでしょうか。「IP Meeting 2014」では、「ビジネスの観点から見たインターネットガバナンス」と題したパネルディスカッションを行いました（内容については「IP Meeting」のところで後述しています）。遠い世界の難しいことに思えてしまう「ガバナンス」ですが、実際にそれを意識してビジネスをしている方の具体的なお話を聴き、ガバナンスの話題をこれまでより身近なもの、今後注意を払っておいた方がいいものだと感じていただけていれば幸いです。

有料プログラムを検討する場であるプログラム委員会ですが、今年は少しメンバーが替わり、若手メンバーが増えました。JPNICのメールマガジンをお読みの方の中にはお気づきの方もいらっしゃるかもしれませんが、9月より毎月、定期号に掲載されるコラムの執筆を、若手メンバーの一部にお願いしていました※3。Internetに対する熱い想いや、他のプログラム委員のアドバイスを受けながらプログラム企画に取り組む姿などが、コラムからもうかがい知ることができるのではないでしょうか。若手に刺激され、ベテランのプログラム委員もこれまで以上に活動した、例年以上に活気のある、近年で最多数のプログラムを生み出したプログラム委員会でした。

※1 米国商務省電気通信情報局がインターネットDNS機能の管理権限を移管する意向を表明
https://www.nic.ad.jp/ja/topics/2014/20140317-02.html

※2 Internet Week 2014 プログラム
https://internetweek.jp/program/

※3 News & Views Colum
https://www.nic.ad.jp/ja/mailmagazine/backnumber/column/

※4 Internet Week 2013 アンケート集計結果
https://www.nic.ad.jp/iw2013/enq/

学割導入!

昨年度の参加者アンケート※4を眺めると、40歳以上の参加者の割合がついに全体の3割を突破しました。チュートリアルプログラムを強化した近年は20代の参加者が増えてきてはいるのですが、それでもまだ年齢層の偏りも見られます。

これからのインターネットを担う若手が参加しやすくなる仕組みはないか、昨年度参加者などに事前アンケートを行い、まずは今年、学割を導入してみようということになりました。対象は25歳以下の学生の方、割引率は事前登録料金より9割引でした。社会人となった後、上司や先輩の勧めなどで参加するのではなく、学生のうちからInternet Weekに興味を持っている方がいるだろうかという不安はありましたが、想定より多くの方に利用されていたようです。Internet Weekのプログラムに参加し、大学の講義とはまた一味違った体験をして、何かを持ち帰っていただけたとしたらうれしい限りです。

Internet Week 2014 開催概要

【正式名称】Internet Week 2014
【テーマ】「あらためて“みんなの”インターネットを考えよう」
【開催地】富士ソフトアキバプラザ
東京都千代田区神田練塀町3 富士ソフト秋葉原ビル
http://www.fsi.co.jp/akibaplaza/cont/info/access.html
【開催日程】2014年11月18日（火）から21日（金）の4日間
［同時開催イベント］
ION TOKYO
IPv6 Summit in TOKYO 2014
第27回JPNICオープンポリシーミーティング
第41回ICANN報告会
第4回日本インターネットガバナンス会議
【開催目的】1. インターネットの発展を推進する
2. インターネットに関する議論の場・交流の場を提供する
3. セミナー開催によるインターネット基盤技術の普及を図る
【対象者】インターネットの技術者および
インターネット技術と社会動向に興味のある方
【内容】インターネットに関するチュートリアル、
最新動向セミナー、ランチセミナー、BoF等
【主催】一般社団法人日本ネットワークインフォメーションセンター（JPNIC）
【協賛】
株式会社日本レジストリサービス
TATA COMMUNICATIONS
株式会社DMM.comラボ
NTTコミュニケーションズ株式会社
Asia Pacific Network Information Centre（APNIC）
株式会社SRA
日本インターネットエクスチェンジ株式会社
Internet Corporation For Assigned Names and Numbers（ICANN）
【後援】
総務省/文部科学省/経済産業省
ICT教育推進協議会（ICTEPC）
IPv6普及・高度化推進協議会（v6pc）
一般財団法人インターネット協会（IAjapan）
Internet Society Japan Chapter（ISOC-JP）
仮想化インフラストラクチャ・オペレーターズグループ（VIOPS）
一般社団法人クラウド利用促進機構（CUPA）
一般社団法人コンピュータソフトウェア協会（CSAJ）
一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）
一般社団法人情報サービス産業協会（JISA）
独立行政法人情報通信研究機構（NICT）
一般社団法人電子情報技術産業協会（JEITA）
一般社団法人日本インターネットプロバイダー協会（JAIPA）
日本シーサート協議会（NCA）
日本セキュリティオペレーション事業者協議会（ISOG-J）
日本DNSオペレーターズグループ（DNSOPS.JP）
一般財団法人日本データ通信協会（Telecom-ISAC Japan）
日本ネットワーク・オペレーターズ・グループ（JANOG）
特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）
日本UNIXユーザ会（jus）
フィッシング対策協議会
WIDEプロジェクト（WIDE）
【URL】https://internetweek.jp/

Facebook https://www.facebook.com/InternetWeek
Twitter https://twitter.com/InternetWeek_jp
ハッシュタグ #iw2014jp

最後に

Internet Week 2014の講演資料、参加者アンケート結果、BoF開催報告書などは、公式Webサイトにて公開しています。

またInternet Week 2015は11月中旬に開催予定です。

2015年は、2月にAPRICOT-APAN 2015が福岡で、11月は94th IETFが横浜で開催されるなど、大きな国際会議が日本にやってくる年でもあります。最新の国際動向に触れ、また国際舞台で日本の技術をアピールし、パワーアップした参加者のみなさま、講演者のみなさまと2015年のInternet Weekを迎えられると思うと、今から楽しみです。

APRICOT-APAN 2015 Webサイト
http://www.apricot-apan.asia/

（JPNIC インターネット推進部 坂口康子）

IP Meeting 2014 ～あらためて“みんなの”インターネットを考えよう～ 開催報告

IP Meetingは、その年のインターネット状況を総括し、今後に向けた議論を行う会合として機能してきました。昨今はInternet Weekのメインプログラムとして、プレナリのような位置づけにもなっています。

今回も、午前中には「Internet Today!」と題し、インターネットの運用にかかる今年のホットトピックを総括しました。そして午後の部は未来を見据えるものとして「ビジネスの観点から見たインターネットガバナンス」と「あらためて“みんなのインターネット”を考える～震災から3年、東京オリンピック・パラリンピックに向け、みんなで作る未来のインフラ～」という二つのパネルディスカッションを実施しました。また合間には、Internet Week 2014の最新動向セッションを紹介するライトニングトーク大会も実施しました。本稿では、午後の部の二つのパネルディスカッションの模様について簡単に報告します。

パネルディスカッション1：ビジネスの観点から見たインターネットガバナンス

2014年は、「インターネットの資源管理体制のあり方」という話題をきっかけに「インターネットガバナンス」が大きく取りざたされた年でした。しかしどうにも、この「インターネットガバナンス」は、多くの技術者にとって遠い世界の話にも映るようです。

「技術者は『統治（ガバナンス）でなくて協調（コオペレーション）』『投票でなくてコンセンサス』を旨としてインターネットの運営をしており、それを『流儀』としているが」とモデレータから前置きがあった上で、今回のセッションでは、「ビジネスサイドから見たインターネットの流儀」という観点から、「実ビジネスへのインパクト」「流儀への疑問」などが議論されました。以降に、パネリストの代表的な発言をまとめます。

モデレータ：
橘 俊男 氏
（Internet Society Japan Chapter/グリー株式会社）

パネリスト：筒井 隆司 氏（ソニー株式会社 渉外部 シニアゼネラルマネージャー（当時））
水越 一郎 氏（東日本電信電話株式会社 ビジネス開発本部）
百崎 知 氏（ソネット株式会社）

日本に聞いて良かった ―そんな世界を作りたい

パネリスト：
筒井 隆司 氏
（ソニー株式会社）

ソニーに入って32年、ずっと海外営業に携わってきました。企業にはコンプライアンスが必要ですが、時代と共に見直しが必要なルールも出て参ります。このルールを適切に変えたり、そもそものルール作りにも貢献していくのが、本日お話しする「政策渉外」という仕事です。

ネットワークの政策課題は多岐に亘り、個人情報の保護や、データの国際移転をどうするか等さまざまな課題があります。個人情報にしても、活用と保護のバランスが重要なのにもかかわらず、いつの間にか保護ありきになっていたり、国境を越えた自由なデータの流通と利活用を通じてイノベーションを推進するのが本来のあるべき姿ですが、内容と目的にあった適切な保護が行われておらず、ビジネス上のリスクが非常に大きいと感じることがあります。自由に発展してきたグローバルなインターネットのイノベーションが様々な国ごとのルール作りによって阻害される懸念もあります。

こうした問題を解決しなくてはなりませんが、悩みは、インターネット関連会議は多岐に亘ることです。ITUのように一国一票制で決められるルールや論点もあれば、誰もが行って発言できるものもあります。ダボス会議のようにインターネットのことがずいぶん話されても小さい話題はあまり議論されないことがあったり、結局「外交上の問題としましょう」という結論になることもあります。

グローバルで活動するとなると「国境」の内側である特定の国のルールだけに従ってビジネスを行うということはありません。米国で商売するのであれば、そこで必要なルールに対して意見を言わなくてはいけないし、他の国でもそうです。先ほどネット中立性の話が出ましたが、米国でFCCがそれに対するパブリックコメントを募集したところ集まった件数は数百万件でした。一方、日本での個人情報保護法の綱領を変更した際のパブコメは数百件です。日本での流儀は、「ルールは誰かが決めるもので、それが決まればその下で正々堂々と勝負していく」というものなのかもしれません。しかし、これが世界で通用しないところなのではないでしょうか。もちろん、「自分がやらなくても誰かについていけばいいのでは」という話は常にあります。しかしこうした“関心が低い”というのが一番の問題なのかもしれません。

インターネットは人間が作ったものです。そのため、そこには「人の意思」があるはずです。なので、本日この場におられる皆様を含め、私たちのこうした活動のゴールが何かと問われれば、「国際的なルール形成やその論点にしっかり入って世界に貢献すること、日本に入ってもらってよかった」という状態を作れるかどうかということだと思います。日本の技術は超一流で、経済もそうです。そこは他国も認めるところです。その国がルール作りに入っておらず、後から「もう少し声を聞いておけばよかったな」という状況になってしまうのではあまりにも残念です。それができるようになるのがうれしいし、皆様にも技術のバックグラウンドを持ってやれることを、ぜひ書き出して実践していただきたいと思います。

困るよりはやってみろ、困ってから話が始まる

パネリスト：
百崎 知 氏
（ソネット株式会社）

入社以来ネットワークエンジニアとして、ISPネットワークの設計・構築・運用をやってきました。IPv4アドレスの在庫枯渇が言われ始めた2008年頃資源管理を任せられ、そこからJPOPMの議論に参加することになり、インターネットのルールがそこから見えてきました。

エンジニアから見ても、インターネットガバナンスのテーマについて、興味を惹かれるワードは多いです。インターネットの資源だけではなく、ネット中立性、迷惑メール、DoS対策、フィルタリング、サイバー犯罪などです。しかし一つ一つを深掘りしていくとわからないことも多くあります。IPv4の枯渇に関しても、売買の話もある中でCGNのような延命技術もある、そもそもIPv6の普及に対してのコストは誰が負担するのか等があります。またネット中立性に関しても、米国とFCCのようなキーワードも聞こえてはきますが、欧米と日本の違いもよくわかりません。DoSやフィルタリングというキーワードではサイバー犯罪を起こさないことが重要だと思いますが、通信の秘密の話や、オーバーフィルタリングの話にもつながります。また、国をまたがった犯罪の場合も国際連携はどうなるんだろうと思います。

ということで、いろいろ気になることはあるけれど、結局「どこで」「誰が」「何を」話し合っているのかわからず、オープンと言いながら実は閉鎖的なのではないかとか、参加する方法としても、個人としても興味を持っていても会社に言うと、短期的・中長期的なビジネスへの影響について聞かれ、卑近な政府のパブリックコメントの方に目が向きがちです。

要は、「なんとなく興味はあるが、それは個人の興味にとどまり、誰が何をやっているのかわからなくて、わからないものを会社に説明するしようとするとよりわからない」「今の事業やビジネスに対して、いつにどのくらいの影響があるかを必ず聞かれるが、会社に経営の目線でどのように興味を持たせられるのかがわからないので、はじめられない」という状況だと思います。また日本の会社では、自身で手の届かないところ、例えば「ITUでこれが決まり、こういう影響が出る」となると「そうか、それが時代だよな。そういう時代に残っていける戦略を考えろ」と受け入れてしまう傾向があります。

本当は、困ることを回避ばかりするのは本末転倒ではないか、と思うのです。「やってみて困るというよりやってみろ、困ってから初めて話が始まる」のでは、そこから学ぶのではないかと思っています。

次々新しいテーマが出てくるインターネットは、常に変わり広がっていくものです。また、ルールは視点により捉え方も違います。僕らのような企業は、「インターネット」という商品を売っていますが、自分たちがインターネットの一部になりながら、それが思った通りのインターネットになっているなと思えると、本当のインターネットの会社になれるのではないかと思います。

日本の企業が“インターネットガバナンス”の考え方に適さない理由

パネリスト：
水越 一郎 氏
（東日本電信電話株式会社）

パソコン通信を振り出しに、ISP運用を行い、今はNTTでフレッツの開発を行っています。IPアドレスと縁があって、CIDRを導入する1998年頃、JPNIC IP-WGの主査となり、2009年にはIPv6の割り当てで関係者と議論し、最近も可能な限りJPOPMには参加しています。

そのように、IP関連のポリシーについては個人としても会社としてもその節目節目に関与してきたつもりです。しかし「インターネットガバナンス」という括りになるとジャンルが広すぎますね。ドメイン名の話も知的財産の話になると複雑ですし、ネット中立性の話もタダのり論はけしからんとは思いますが、どこで何が決まっているのか、米国の世論で決まっているのか、国内事業者としてはFCCにいくわけにもいかないし……と感じます。このように海外からの圧力は受けているはずなのに、それに対して何をするかということについては何もできていません。海外は遠いという話もあります。

そのような訳で、私自身も興味はあっても、今一つ響かないというのが実感です。分野が広すぎて興味が絞れないのと同時に、何とかなるだろうというノンポリズムやリバタリアン的な考えもあります。会社としてもドメスティックなビジネスをやっているという理由から、ほとんど響いていないように感じています。直接的な利益のにおいがしないため、スコープを定めにくく、CSR的な考え方でやっていくものなのかもしれません。

日本の会社がこうした問題に取り組むにあたって、適していないという点がいくつかあります。会社としては「ポジションを取らない」という判断をすることは、意思決定の一つです。しかしそのためにはまず「参加している」ことが必要であるし、しかも行った先でアジェンダが生まれるということもあるので、本来は行かないと何も始まらないのに、「目的と結果を持って出張に」となってしまう点です。動いている問題に対処するのは難しいのではと感じます。またこうした政策的なことは、「流れを見続けている」「相手の顔がわかる」という個人の存在感も必要になるものですが、日本の会社は「そろそろ別の人を……」となり、継続性も難しいところがあります。本来は教育のために派遣しているわけではないはずです。

こうした活動のゴールと問われれば、標準化とか文書を出すということだけではなく、文書へどれだけ貢献できたかも一つのゴールではないか、とは思います。エンドレスジャーニーではありますね。

技術の世界もビジネスの世界も、どうもこうした話題に無関心ではなさそうだというのがパネルディスカッションでわかったことです。しかし、関与方法も立場によってさまざまで、すべての領域にすべての人が関与するのはとても壮大なことだというのも見えています。そのため「関与している人を支援することも重要ではないか」「とかく継続的にやっていくことが、裾野を広げるための秘策では」とパネルディスカッションは締めくくられました。

（注：各講演者のコメントの内容は、当日の話をもとに編集を行ったものです。また、各講演者の所属は、開催当時のものです。）

パネルディスカッション2：～あらためて“みんなのインターネット”を考える

2020年のオリンピック・パラリンピックの開催地が東京に決まりました。そうした状況を受け、2012年のロンドンオリンピックでどういう現象が起こったのか、セキュリティ等はどうだったのかなどの教訓を振り返り、生かしつつこれからのネットワークインフラに期待されていること、我々が未来に向けて準備すべきことを議論するパネルディスカッションが行われました。パネリストは以下の通りです。

BTはロンドンオリンピックにおける唯一の通信プロバイダーとして、Wi-FiやCATV網、モバイルネットワークの接続なども含め、オリンピックの通信およびそのセキュリティを担当していました。そのBTのフィリップ・モリスさんからロンドンで起こったことを伺った後に、2020年に向けてのディスカッションが行われました。

モデレータ：
江崎 浩 氏
（JPNIC副理事長、東京大学）

コメンテータ：
吉田 友哉 氏
（インターネットマルチフィード株式会社）

パネリスト：**フィリップ・モリス 氏**
（BT（ブリティッシュ・テレコム））
小山 覚 氏
（NTTコミュニケーションズ株式会社 経営企画部 マネージドセキュリティサービス推進室 担当部長）
鈴木 茂樹 氏
（総務省情報通信国際戦略局長）
丸山 充 氏
（神奈川工科大学情報ネットワーク・コミュニケーション学科教授）【ビデオ出演】

2012年ロンドンオリンピックで起こったこと

パネリスト：
フィリップ・モリス氏
（BT（ブリティッシュ・テレコム））

オリンピックに必要なキャパシティ

まず初めに考慮すべきは、オリンピックの開催規模の巨大さです。オリンピックは国家にとって、平和時における最大のロジスティクスが要求されると言われています。そして失敗は決して許されません。通信においても放送、ネットワーク、Webと何一つ落とすわけにはいきません。ロンドンオリンピックでは、17日間に1,100万枚のチケットが売れ、多くの交通渋滞が生まれました。多くの人が複数のデバイスを持ち込んでおり、ケーブルも一から計画して敷設する必要がありました。Webとテレビの視聴者は約50億人、世界人口の5/6が見た計算になります。

オリンピックにおけるスポンサーの役割と苦労

通信の提供者としての我々に対する情報やオーダーを受け入れる体制が必要です。オーダーのピークは、大会の13ヶ月前である2011年7月でした。それらのオーダーをさばき、実現していかねばなりません。

最大の難しさは、「オリンピックでは、タイムラインに対する変更が無い」ことです。こちらの準備の度合いはまったく斟酌されず、開会式は絶対に決まった日付に行われます。ロンドンオリンピックでも、とあるスポンサーが、あるオーダーに合わせられず、軍隊の派遣で解決するようなことも発生しました。一方、タイムラインは絶対的に決まっているのに、要求は変わっていきます。例えば、スポンサー契約時には「会場は100Mbpsで接続できれば良い」とされていたものが、最終オーダーは「10Gbps」と100倍になり、400台敷設すれば良いとされていたアクセスポイントも「1,600台」と4倍になりました。そうしないとデバイスを収容できないという結論になったわけです。こうした進化のスピードは、契約書締結時には誰にも想像できませんでした。しかしスポンサーである以上、破綻させるわけにはいきません。実際、2010年にスポンサーのNortel Networks社が経営破綻し、その影響でBTも通信設備の設計をやり直す必要が出ましたが、開会まで1年未満の時間しかありませんでした。スポンサー契約になかったことも、そういう状態になればやらざるをえません。

ロンドンオリンピックにおける通信環境整備の状況

入札時の2005年初頭、いわゆるスマートフォンはまだありませんでしたが、2007年にiPhoneが生まれ、モバイルの環境が急激に変わりました。2009年には当初の計画のままではダメだと、ぎりぎりにインフラの計画を変更しました。また、携帯端末のスポンサーは他社でしたが、BTはSIMカードのスポンサーとして、その中のセキュリティも考慮しなくてはなりませんでした。これは認証も自動的に行い、ユーザーの音声を暗号化するというとても大きなプロジェクトでした。当時モバイルに関しては、2Gと3Gが主流で4Gは使われていませんでした。

Wi-Fiの敷設にも挑戦がありました。別々のWi-Fiサービスや指向性のアンテナを組み合わせて、選手用、選手の家族用、プレス用、パブリックWi-Fi等々に分けて敷設する必要があります。帯域幅も検討が必要でした。

また東京オリンピックでは、東京地区に集中して競技が行われると思いますが、ロンドンの場合は開催地が国全体に散らばっていました。そのことから5,500kmのケーブルを用意し、すべてつなぐことが必要でした。

国際オリンピック委員会の要求 ～深刻度=シビリティへの対応～

一つの鍵は、一発で成功する方法論が必要だということです。とにかく本番で成功させるために、裏でテストをしたり、冗長性や可用性を上げたり、問題が起こった際にすぐに修正できるようにしなくてはなりません。開催地によっては1年前から空いているところもあったので、早めにコンペを始め、各スポンサーが政府と協力して包括的に多くの準備を行っていきました。

また、技術のオペレーションセンターを立ち上げ、600名がオペレーションセンターに在席しました。うち180名がBTから、それ以外が他社と政府関係者です。このオペレーションセンターでの銘は、「“深刻度1”の事象は発生させない」でした。オリンピックは国際オリンピック委員会（IOC）が管理しており、IOCが開催都市に対して制定したルールに開催都市が準拠することで大会が運営されます。その一つが「（問題の）深刻度=シビリティ」であり、何か問題が起きた際にそれが競技にどの程度の深刻さを与えるかの指標です。深刻度1は、例えばタイムを取ることができない等競技自体に影響が出たり、放送が止まってしまったり、電気が落ちて感電するなどという命を脅かす事象が起こったりすることです。深刻度2は、冗長性が何か欠ける類いのもので、競技にとって必須なサービスが落ちるということではありません。この深刻度に関しIOCは、問題解決に要する時間を、以前の北京オリンピックの半分に短縮するよう求めてきました。これはとても厳しいものですが、同様の基準が、今後のリオデジャネイロや東京でも求められる可能性が高いと思います。

競技に影響がある、命が脅かされることは発生させないというのが前提でしたから、競合他社であっても、全員が協力することを学ばねばなりませんでした。結果として深刻度1の事象は無く、深刻度2は21ケースが報告されました。深刻度2の事象の大半は、半分を占める屋外の開催地に起因する、「トラックがケーブルを踏んだ」「水があふれ、光ケーブルがだめになった」等のケースでしたが、冗長化を再度取りながらクリアしました。

セキュリティ

Webセキュリティに関しても、いろいろありました。50TB以上のトラフィックがプロキシサーバに寄せられ、2億以上の悪意のあるアクセスがブロックされました。イギリスが6個の金メダルを獲得し、一番の誇らしい日であったスーパーサタデーには、1億2,800万のイベントが検知されました。また、3万人のメディアが複数のデバイスを持ち大会を取材していましたが、ほとんどの人がセキュリティに気を配っていなかったため、6割程度がマルウェアに感染し、スパムも増え、ISPの手にも負えず、プレスのネットワークは分割しなくてはなりませんでした。ブラックリスト化もできず、機器の修理にもかなり追われました。

IOCの主導で、事前に政府とともに“War Gaming”と題した大きなリハーサルやシミュレーションもしました。最初は簡単なものから、CERT（Computer Emergency Response Team）のテスト、完全な統合されたテストまで、あえてプレッシャーをかけながら、どの程度やれているか、方法論がわかっているか、本番さながらの演習をし、チェックしました。セキュリティを担保しながらシステムを見ていくのです。可用性のサービスレベルとセキュリティのサービスレベルは、大体同じくらい重要視しました。また、統合されたまったく新しい「サイバープラットフォーム」というプラットフォームを構築し、多くのデータや分析がビジュアルとしても一目でチェックできるようにもしました。

「Security by Design=計画的なセキュリティ対策」という考え方があります。必ずどんなことにもセキュリティの考えをベースに入れました。ここが一つの成功に向けた大きなドライバになったと思います。こうした教訓は、インターネット、車、ビルマネジメント、その他の公共政策にも生かせると考えています。

またセキュリティにとって重要だったポイントは、ツールや技術ではなく、人の振る舞いやスキルセットに焦点を当てたということです。行動やスキルに対する投資も、大きな注力範囲になりました。

2020年東京オリンピックに向けてのディスカッション

― 2020年に向けての現在の検討状況は？

鈴木氏

2020年にはオリンピック・パラリンピックだけでなく、「ICTによるおもてなし」で情報通信基盤をとことん利用して観光もしてもらい、日本は安心で安全で快適に過ごせるということを感じて欲しいと、今から取り組み始めています。超高速のブロードバンド、第4/5世代のワイヤレスブロードバンド、Wi-Fiの性能も上がり、放送も4K/8Kの世界となるでしょう。

いろいろな観点からどれだけのインフラを整備したら良いかを議論していきますが、問題は「セキュリティ」です。本日（2014年11月22日）解散した国会で、「セキュリティ基本法」が成立し、来年から内閣の情報セキュリティセンター（NISC）が法律に基づき設置される組織となり、体制も拡充されることになりました。通信網のネットワークだけではなく、エネルギーや運輸金融などあらゆる通信のセキュリティを考えなければならない状況になります。鉄道が止まる、金融に問題が起こる、電気が止まって街がダウンすることもあり得ます。なぜなら、重要インフラのバックボーンはすべて情報通信ネットワークだからです。ネットワークが止まったら困るものはまとめて対策する必要があります。既にオリンピックの部局として20の部局ができていますが、このうちの一つに「情報通信局」があります。また大会運営用の情報基盤をどうするか、そこのセキュリティをどうするかという意味ではセキュリティ対策室もできていると聞いているので、大会全体の基盤の整備とセキュリティ対策、情報通信基盤の運営とセキュリティを一体となって進めていくことを考えています。

ー ロンドンでは、4K放送が行われていましたか? ロンドンでは、ブロードキャスト以外のメディアもサポートしていたのでしょうか? また2020年には、4Kになると思っていいでしょうか?


モリス氏

2012年の時点で、すべてのカメラが4K対応していましたが、ユーザー側が未対応であるためHDに変換して配信していました。当時直接4Kに取り組んだのはBBCだけでしたが、2020年にはすべての映像が4Kになるでしょう。また、NetFLIXやビデオオンデマンド、またタブレットやスマートフォンで映像をダウンロードできる「オーバーザトップ」というサービスもサポートしていました。そのため、2008年の北京から2012年の間に、コアネットワークの帯域が24Gbpsから160Gbpsと750%も拡大しました。


鈴木氏

周波数は2700MHzまでに拡張する予定ですが、その理由は、2020年にはほとんどの人がスマートフォンやウェアラブル端末を持ち、その場で好きなシーンをリアルタイムに4K映像を流す時代になってくるのではないかと想定しているからです。どれだけ周波数があったら良いか明言できませんが、「出せるだけ出す」ことに決めたのが2700MHzです。


小山氏

正直あんまり想像したくない世界ですね。1km²にいる10万人からのアップロードは、「攻撃」以外の何ものでもありません。Wi-FiやLTEでパケットを運ぶ人の気持ちも考えて、今後の利用に向けた設計していかなければいけないのではないでしょうか。また現実問題として、資金の問題も大きいように感じます。1ヶ所切れたとしても大丈夫な冗長性を備える設備の投資額は、何百億円という規模になりかねません。スポンサーになるとどこからも資金はやってこず、自分で出さねばなりません。


鈴木氏

国内のスポンサーはまだ決まっていませんが、スポンサーは資金だけではなく、さまざまなオーダーに応えなくてはならないという状況は、ある意味恐ろしいことだと思っています。ファシリティの準備をする文部科学省にも、Wi-Fiのスポットなどもたくさん置けるよう大容量の光ファイバーを依頼していますが、実際問題としてどこまでできるかは、「どれだけスポンサーが集まるか」で決まる要素と、「あと6年間のどこで見切って設備の準備を始めるのか」という要素があると思います。結構難しい問題ですね。

ー「最初の予想は裏切られる、これが学んだことだ」という話もありました。


モリス氏

絶えまない変更要求に対し、その管理をどうするか、どこでバランスを取るかについては、運営委員会とスポンサーの間だけでなく、IOCとの間でも決まることもあります。時にIOCが仲介者にもなったり、場合によっては政府も資金を調達してくれたりすることもあります。長く利用できる施設は、公的な資金できちんと整備すべきである一方、一時的な施設はそれなりに扱うというバランスを、全体的に見て決めねばなりません。

ー すべてのインフラにネットワークは関わり、物理セキュリティからサイバーに至るまでセキュリティが必要になるという話もありましたが、2020年は2012年とどういう状況が変わってくると思いますか? また、日本におけるセキュリティ議論はどう進んでいますか?


モリス氏

特にビル関係の図面などは、2DのCADデータではなく、3Dモデリングされたものとなるでしょう。パイプなどの連結情報や電源の位置など一つをとっても、テロリストや攻撃者にとって、貴重な情報になり得ます。そのため、開催地のインフラの情報に誰がアクセスできるのか、下請けも含めて把握する必要があります。それぞれのアクセス権限を管理し、漏れないようにしないとなりません。

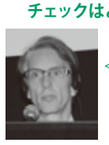
また、チケット発行のシステムも、おそらく2020年には物理的な紙ではなく、SuicaやPASMOのようなシステムを使っていくでしょう。それの権限と複数の要素での認証が必要になります。

さらには、密度の高いところにあるビルなど、子供がフェンスを登らないようにしなくてはいけないなども含めて、どういう物理セキュリティの仕組みを引くのかという観点も必要になるでしょう。ロンドンでは、選手村も含めて、一つの大きなフェンスを作ってガードしましたが、東京の場合は、もう少しそれぞれの拠点が分散されるのではないでしょうか。川があったりお台場があったり、それぞれを守る必要があります。


鈴木氏

電力などのエネルギー網はスマートシティなどと呼ばれネットワークでコントロールされますし、鉄道もしかりです。自動車や信号も高度道路交通システム(ITS)でコントロールされているため、侵入される可能性はあります。またドローン(無人小型飛行機)などを使ってのテロも考えられるでしょう。ネットワークがあることの便利さの反面、新しいセキュリティリスクも生まれています。この対策をこれから具体的に検討していかねばなりません。また、オープンデータは悪い人にとっても使い勝手の良いデータです。その辺はNISCがこれから検討していくでしょう。

ー 日本でもサイバーの攻撃に対しては机上でシナリオを作り実機で演習していますが、ロンドンでは物理的なセキュリティも含め、チェックはどのようにされていたのでしょうか?


モリス氏

ロンドンオリンピックの準備は、Olympic Development Authority(ODA)が会場作りを担当し、これが組織委員会である、London Organising Committee of the Olympic and Paralympic Games(LOCOG)に引き継がれました。ODAでは会場作りの初めから、「Security by Design」の概念がきちんと取り入れられていました。セキュリティセンサーやモーションセンサーを入れてセキュリティを担保した後で、LOCOGやBTに運営が引き継がれましたが、引き継ぎもすべてモニターされた上で、ビックデータ分析ツールに入れられ、完全な形で行われました。作業員の認証も厳しく行われ、また人によって立ち入れる場所とそうでない場所も厳しく決められていました。また、要素認証としてバッチだけでなく生体認証を入れ、誰がどこに行ったかのトラッキングもされていました。物理的なセキュリティエキスパートもおり、爆弾やMPUが仕掛けられそうな場所の巡回をしていました。

ー 攻撃を受けている人に手を差し伸べるにはモニタリングも必要になるものですが、日本だと現時点ではこれが通信の秘密に抵触し、また情報共有も容易でありません。そういう障壁が取り除かれる状況が日本で実現するでしょうか?


小山氏

運用については今までの10年で変わってきたと思います。当初は、電話の時代の考えしかなかったものが、インターネットの進化により少しずつでも変わっています。しかし今のままで間に合うかと言うと、現状の取り組みで足りないと感じるのがやはり情報共有です。どのオリンピックでも、軍や諜報機関の情報を使っていますが、日本ではその議論を行っておらず、攻撃が来た際に守れるのかということは通信の秘密以前の問題としての課題なのかもしれません。

ー ロンドンでは「OCCT=オリンピックサイバーコントロールチーム」というものを作ったという話がありました。その構造を簡単に説明してください。


モリス氏

BTを含む各責任省庁からの代表者がOCCTに集まり、ここでさまざまな計画内容、開発内容、脅威、攻撃者といった情報を集めることができました。事前演習のWar Gamingのシナリオの話もしましたが、このシミュレーションはOCCTが作ったシナリオに基づいて実行したものです。また重要だったのは、OCCTの代表者が内務省大臣の直属であり、この人物が、軍隊に警告をするとか、CERTを関与させるとか、分析にかけるとか、特定のシステムを切り離してオフラインにする等を判断し、決定できました。ロンドンではSuicaに似た「オイスターカード」というシステムが鉄道などで使われていますが、これがハッキングを受けるような事態が起こった場合に、鉄道のゲートがオープンモードになり、誰でも無料で交通機関に乗れるようになるというようなことまで決まっていました。


鈴木氏

ぜひ日本でもそうした仕組みを作るべきですね。実は本日の国会の解散で流れてしまったのですが、オリンピック担当大臣やスポーツ庁を置くという話も出ていました。それができると体制強化がされ、国家安全保障局もでき、NISCとの両建てにもなります。イギリスの例を参考にしたいですね。

ー オリンピックに向けて、ネットワークに関わる我々に期待されることは何でしょうか。


小山氏

日本のISPは、「通信の秘密の侵害罪」を恐れて動けなくなることを危惧しています。「オリンピックで何を守るのか」といった議論の際に「可用性だ」という声は返ってきますが、ウィルスが出回ることで例えばどこかのISPがこけたとしても開会式がきちんとできれば良い、というほどの張り詰めた中での運用が必要になると聞きます。我々ISPは2020年までに「回復力」をどれだけ持てるようになるのでしょうか。スポンサーはたくさんの要求を満たす必要があるとの話を聞きましたが、スポンサーにならない事業者、そしてISPは、「一番に自分を守ること」を真剣に考えるべきでしょう。2013年に300Gbpsの攻撃があったことを鑑みても2020年のトラフィックは膨大です。今からきれいにしておく必要があります。また、AntinnyによるDDoSで得た教訓は、「管理者不在の脆弱なネットワークやシステムもできるだけなくしたい」ということです。そのためにISPのためのガイドラインも第3版ができました。これにより、ボットネットを利用したDDoSやリフレクション攻撃に対しても、IP53B(53番ポートのブロッキング)の導入が可能になっています。

皆でできることは、IoTのセキュリティ対策に尽きるのではないでしょうか。皆がたくさんのデバイスを持っています。野良IoTをどう作らないか、素のグローバルアドレスを渡す今の状況は変えないといけないのかもしれません。IoTデバイスのハンドリングネットワークをどう作るかを皆さんと考えていきたいですね。


モリス氏

オリンピックには本当に多くのプレイヤーが関与せねばなりません。我々は通信のスポンサーとして多くのWGを立ち上げることで、Wi-Fiについても主要なオリンピックWi-Fiだけでなく、その周りの地区のホテルやファストフードの無料Wi-Fiなどのセキュリティの共有等もやりました。どこのWi-FiもSecurity by Designということです。まずは明確なビジョンが必要です。それに沿った形で人に正しい行動をしてもらえるようなインスピレーションを与え、また、適切な訓練や明確なコミュニケーションを通じて、透明性をあげ、適切な要件を見つけられるように一人一人のモチベーションをあげていくのです。「人」が大きなプロジェクトの成功の鍵になります。


鈴木氏

インフラ整備とセキュリティが必要とされる中、基本的にインフラを作るのは民間の通信事業者の皆さんです。その上でサービスを提供するのも、民間のISPやコンテンツプロバイダー、アプリケーションプロバイダーの皆さんとなります。政府やナショナルキャリアが基本の安全対策はやるかもしれませんが、個々のサービスとユーザーについてのセキュリティ意識を高めないと、オリンピック中に不具合は起きるのではないでしょうか。社会全体でセキュリティを考えていかないといけないでしょう。

最後に、以下の4点が重要なものとしてまとめられました。

(1) 超高速ブロードバンド時代がやってきそうだ
- 4K/8K も個人のワイヤレスデバイスが4K/8Kの映像を通信するような時代

(2) Security by Design(計画的なセキュリティ対策)が必要
- タイムラインに変更はないが、要求はどんどん変わっていく
- “回復力” “可用性”がすべてのインフラに求められる

(3) Olympic Cyber Control Team (OCCT)
- 規則、規制をどうしていくか
- すべてのシステム横断的なビックデータ解析、オープンデータも必要

(4) Olympic CERT
- サイバーだけではなく、すべての業界での物理的セキュリティも必要

(注:各講演者のコメントの内容は、当日の話をもとに編集を行ったものです。また、各講演者の所属は、開催当時のものです。)

(JPNIC インターネット推進部 根津智子)

JPNIC 会員 企業紹介

「会員企業紹介」は、JPNIC会員の、興味深い事業内容・サービス・人物などを紹介するコーナーです。

インターネットを通じて、九州をきらきらと輝かせる。九州に根ざし、お客様原点で。

お話しいただいた方
九州通信ネットワーク株式会社
取締役 常務執行役員
技術本部長
池田 正信 氏

九州通信ネットワーク株式会社

住所：〒810-0001　福岡県福岡市中央区天神一丁目12番20号
設立：1987年（昭和62年）7月1日
資本金：220億2,000万円
代表者：代表取締役社長　秋吉 廣行
URL：http://www.qtnet.co.jp/
事業内容：http://www.qtnet.co.jp/annai/
1. 電気通信事業
2. 電気通信設備およびこれに附帯する設備の工事ならびに保守
3. 電気通信および情報処理に関する機器・ソフトウェアの開発、製作、販売および賃貸
4. 一般放送事業
5. 電力の購入、販売

従業員数：573名　（2014年3月末日現在）

今回は、「QTNet（キューティーネット）」の愛称で知られる、九州通信ネットワーク株式会社を訪問しました。
同社は、J.D.パワー社の「2014年日本固定ブロードバンド回線サービス顧客満足度調査」において顧客満足度No.1を獲得するなど、複数の顧客満足度ランキングで実に高い評価を受け続けています。また、2015年2月下旬から3月上旬に福岡にて開催されたAPRICOT-APAN 2015といったコミュニティ活動にも、多くのリソースを投じて協力されています。
同社が高い顧客満足度を維持し続ける理由や、コミュニティへの積極的な貢献が意味するものを探るべく、お話をうかがいました。

事業概要と主力サービスについて

―まずは、貴社のご紹介をお願いします。

池田：社名は「九州通信ネットワーク株式会社」ですが、CM効果などもあり、皆さまには略称の「QTNet」の方がよく知られています。かつて社名を「QTNet」へ変更してはとの話もありましたが、お客さまにより親しんでいただけるよう、正式名には堅実な従来の社名を残したまま「QTNet」を常用しております。

弊社が提供している通信サービスには、個人向けと法人向けの二つのサービスがあります。個人向けについては、光ブロードバンドサービス「BBIQ（ビビック）」をブランド名として、光インターネットに光電話と光テレビをセットにしたトリプルプレイサービスを提供しています。法人向けについては、ネットワークの仮想化技術の一つであるVLAN（Virtual Local Area Network）を利用した広域イーサネットサービス「G-VLAN」をはじめとして、廉価なVPNサービス「Branch-VPN」などを提供しています。

1987年の会社設立から成長を続け、2013年度には売上高が500億円を超えました。個人と法人の売上高比率は、法人向けが若干多いかもしれませんが、おおむね半々となっております。

さらなる高みをめざしたサービス展開

―主力サービスBBIQやG-VLANの提供状況を教えてください。

池田：「BBIQ光インターネット」は、離島を除く九州各県の主要地域でサービスを展開しており、世帯カバー率は約6割です。近年は、さらに事業者間の競争が激しくなっているものの、着実に契約数を伸ばし、2014年度末の累計契約数は、約33万回線と見込んでいます。九州のFTTH世帯普及率は、35.3%と全国から3年6ヶ月遅れているものの、まだまだ伸びしろがあると考えています。

多チャンネル放送サービスの「BBIQ光テレビ」は、これまでの福岡、北九州、鹿児島などに加え、2014年9月より熊本でもサービス提供を始めました。また、他の地域においても、地元のCATV事業者と提携しながら進めており、例えば大分では、地元の大分ケーブルテレビ株式会社（OCT）と連携し、弊社の光インターネットと光電話に、OCTの放送サービスを合わせたトリプルプレイサービスを提供しています。

法人向けのG-VLANサービスは、九州全域でサービスを展開しております。G-VLANは、帯域保証型のサービスとして、複数拠点間を高品質・高信頼度のネットワークで構築するサービスであり、高い信頼性を必要とされるお客さまに多くご利用いただいております。一方、「拠点の規模や重要度に応じてアクセス回線を選択したい」「通信コストを抑えたい」というお客さまには、G-VLANとBranch-VPNを使い分けることをご提案するなど、お客さまのご要望に応じたメリハリのあるネットワークサービスを提供しています。

―J.D.パワー社の「日本固定ブロードバンド回線サービス顧客満足度調査」で総合満足度全国1位を獲得されていますが、どのような取り組みをされていますか。

池田：J.D.パワー社の評価にもあるように、九州に根ざしたビジネススタイルに対して評価をいただいていると思います。私たちも、九州の独自性を出したいとの想いでサービスをスタートしましたし、お客さまにより近いところで仕事をしたいと考えています。そのため、お客さまのご意見・ご要望などを「お客さまの声」として取りまとめ、毎週開催される社長・本部長クラスの会議で、お客さま目線で対応方針を議論し、即断即決に努めています。また、コールセンターは、一般的にはなかなかつながらない印象がありますので、弊社ではそのようなことが極力無いよう応答率を高める努力をしています。一般的なコールセンターでは、応答率70～80%程度だと聞いておりますが、弊社は90%をめざして取り組んでおり、おおむね1回のコールでかかるようにしています。これも、評価いただいている点だと思います。

お客さまの声という点で一番印象的だったのは、テレビ番組の編集ですね。番組編成にあたっては、コンテンツ提供側の都合や設備の関係で、今まで放送していた番組が提供できなくなることもあります。このような場合、すぐにお客さまより厳しいご意見が届きますが、これまで「仕方ない」ということで、なかなか幹部までは届いておりませんでした。しかし、現在はすべての情報が幹部まで上がってきますので、会社の判断として対応を決定できるようになりました。

―言うは易しですが、応答率を90%まで上げるなど、お客さま満足度を向上させるのは、並大抵ではないですよね。他にはどのような取り組みをされていますか。

池田：そうですね。例えば、料金については、光ブロードバンドがISP料金込みで月額三千円台でご利用いただける長期利用割引や、スマホとセットでご加入いただくとスマホの利用料を割り引くサービスなども導入しています。また、電気と通信のセット販売も2014年7月に始めました。これは、マンションへの電力を弊社が高圧電力で一括契約し、低圧電力へ変圧して従来よりも安い料金で入居者や共用部に電気を供給するサービスです。BBIQとのセット利用で、さらに電気代を安く設定しています。このようにして、これからも、お客さまにご満足いただけるサービスを提供し続けていきます。

より盤石なインフラ整備へ向けて

―通信インフラ環境について教えてください。

池田：2015年3月1日に、九州電力から光ファイバー心線貸し事業とそれに関連するすべての光ファイバーケーブルを譲り受けました。弊社は、これまで弊社が保有していたケーブルに、今回譲り受けたケーブルを合わせ、9万kmの光ファイバーケーブルを保有することとなりました。これに伴い、日韓海底ケーブル（KJCN：Korea-Japan Cable Network）も弊社で保有することになり、今後は国際サービスの提供もより強化したいと考えております。

―KJCNの運用や地理的に韓国が近いことによる効果はありますか。

池田：弊社は、KJCNの運用に携わることで、APAN（Asia Pacific Advanced Network）と連携して将来の国際ネットワークの在り方について検討を行うなど、将来技術の動向や利用、技術面で知見を得ています。今後は、APANなどへのサービス提供を通じて、学術面などでも九州に貢献したいと思っています。一方で、料金面については、当初は距離の近さによるメリットがありましたが、国際回線サービスの市場価格が値下がりし、東京から迂回して提供した方が安くなるといった状況も出てきており、最近では価格メリットを以前ほどは出しづらくなりました。従って、今後は、九州に事業所を持つ韓国企業もたくさんありますので、そのようなお客さまに地理的優位性を訴求し、ご利用いただく営業活動が必要と考えております。

―また、新総括局の設置を進めていらっしゃるそうですね。

池田：弊社のネットワークは、各サービスシステムの頂点となる「総括局」から、各県庁所在地に設置する中心局、中心局配下でお客さま回線を収容する伝送端局・分散拠点局まで、階層的に構成しています。現在、最も重要である総括局機能を地理的に分散した二系列構成とするため、新しい総括局の建設を進めております。これにより、地震などの大規模災害時においても、安定したサービスの提供が可能となります。また、新総括局は、信頼性および機能拡張性を考慮し、免震構造にしており、総括局・BCP（Business Continuity Planning）・ネットワークセンター・データセンターの四つの機能を具備しています。

―耐震という点では、東日本大震災はリスクを大きくとらえるきっかけになったかと思いますが、BCPの観点や災害対策への需要はありますか。

池田：直接的な影響としては、総括局の新設を具体化することになったことですね。以前から話はありましたが、東日本大震災を機に加速されました。既存の設備も、主に自治体のハザードマップに照らして災害対策を講じていましたが、あの震災でハザードマップも基準が変わり、それまでの洪水対策に加え、津波対策についても検討項目に追加されています。このため、現在、新しいハザードマップにより対象箇所を見直し、対策を進めております。また、弊社は他社と提携してデータセンターサービスを提供しているのですが、やはり、お客さまのBCP対策としてのニーズは、確実に増加しているように感じます。昔、提携先のデータセンターが免震構造のデータセン

ター新設についてJANOGで発表した際に、「素晴らしいけれどもすごく高コストだよね」という話がありましたが、震災が実際に起こったことで、もしもの時への備えがとても重要である、ということをあらためて強く実感しました。

地元九州への貢献を第一義に

―ところで、コーポレートスローガン「きらきらつながる」は、素敵ですね。いつ頃からですか。このスローガンによる変化はありましたか。

池田：将来ビジョン策定の一環として、社内でワークショップを設置し、議論を重ね、2010年5月に制定しました。気持ちは、かなり変わりましたよ。弊社の存在意義や役割の表れでありますし、ロゴの星は、九州各県の県庁所在地を表しています。「つながる」というのがキーワードとなっており、九州とつながってしっかりした事業を行い、「九州のお客さまが“光”輝くように。」という私たちの想いを込めています。その想いを私たちは忘れないように、そしてお客さまにも伝わるように、とスローガンを決めて、それが効果を発揮していると思っています。手前味噌ですが、いいスローガンだと思います。

―ネットワークに関係しているものとして、「つながる」という言葉には打たれます。ただ、「きらきら」は、重厚さには欠ける印象もあるかもしれません。

池田：「きらきら」には、弊社コア事業である光ファイバー通信サービスの「光」と、お客さまのくらしをよりよく「輝かせたい」という熱い想いを込めています。私たちの想いを端的に表し、今では「きらきらつながるQTNet」として、九州のお客さまに広く浸透しています。

―生まれ育った地元に対しては、皆それぞれ思うところがあると思いますが、九州の方の地元愛はすごいですね。特に、福岡の方の地元愛は強いように思います。

池田：はい、社員たちは弊社で働いているのを自慢にしていますよ（笑）。福岡は街の規模もちょうど良いですし、繁華街である天神と博多の距離も適度です。また、海も山も川もあって、食べ物もおいしいですしね。多趣味な人でも、博多だったら山登りからサーフィンなど何でもできます。私の出身は熊本なんですけどね（笑）。

―APRICOT-APAN 2015もスポンサーいただき、ありがとうございました。また、APRICOT-APAN 2015実行委員会の相談役である「アドバイザリーボード」へ貴社社長にご参画いただいたり、ネットワークチームへのエンジニアの方のご参加、回線を提供いただいたりなど、大変ご尽力いただきました。APANや学術とのつながりという話がありましたが、APRICOTをスポンサーする意義はどのようなものでしたか。

池田：九州でこのような会合が開催される機会は、なかなかありませんので、弊社が少しでもお役に立てるのであれば大変喜ばしいことです。貴重な地元開催ということで、ぜひとも協力させていただこうとスポンサーになりました。

JPNICに望むこと

―今まで貴社についてのお話を伺ってきましたが、ここでJPNICへの要望をお伺いできればと思います。

池田：弊社としては、今回のAPRICOT-APAN 2015でもそうですが、JPNICがいろいろな調整や情報展開をしてくれているのがありがたいですね。個人的にも、IPv6の普及は頑張ってほしいです。ゲーム業界をはじめ、IPv6にすると良いことは一杯あるので、うまくアピールしていただきたいですね。良い情報を、ますますタイムリーに提供してくれればと思います。

―IPv6はなかなか普及しない感じがあります。貴社におけるIPv6対応は、どのような状況でしょうか。

池田：今のところ、法人向けはIPv6対応していますが、個人向けは未対応です。もともと利用者のニーズが無い、というのが直接的な理由です。ただ、サービスの競争力を高めるためには、設備投資は必要になりますが、タイミングとしてはそろそろかな、と考えています。お客さまがIPv4とIPv6を意識しなくても両方に対応できるような形で進めていきたいですね。

―ゲーム業界など、IPv6の機も熟しはじめていますよね。JPNICとしては、次はコンテンツ提供事業者のみなさんにIPv6へ移行してもらうのが課題です。そして、「良い情報をタイムリーに流す」、これは、私どもとしても常に意識し、課題としているところです。事業者の皆さまがなかなか独自に入手できない情報を、いかにうまく伝え理解していただくか、というところがJPNICの存在意義だと思っています。

―最後に、貴社にとって、「インターネットとはどのような存在か」お聞かせください。

池田：何でもできるという意味で、魔法の小箱ですよね。今でも情報がこれだけ溢れているので、もっともっと充実していけば、違う世界が出てくるような気がします。世界中を無意識につなげる、ただでさえすごい技術ですが、まだ極限までは使い切れていないのではないか、と感じています。歴史は浅いですから、まだまだこれからが楽しみですね。

―まだまだ、こんなもんじゃないはず、ということですよね。そうすれば事業的にも広がりますし、楽しみですよね。JPNICとしても、お手伝いできればと思います。

● コーポレートスローガンが存在感を放つエントランス

JPNIC 活動報告 JPNIC Activity Report

JPNIC活動カレンダー（2014年12月～2015年3月）

12月

5日 10日 15日 20日 25日 31日

5（金）	第54回臨時総会（東京、アーバンネット神田カンファレンス）
19（金）	IETF報告会（91stホノルル）（東京、JPNIC会議室）

1月

5日 10日 15日 20日 25日 31日

29（木）	第5回日本インターネットガバナンス会議（IGCJ）会合（東京、JPNIC会議室）

2月

5日 10日 15日 20日 25日 28日

2（月）～6（金）	JPNIC技術セミナー（東京、アーバンネット神田ビル） インターネットとは／ネットワークセキュリティ概説／BGPインターネットルーティング／DNS基礎／DNSSEC基礎／入門IPv6／IPv6ハンズオン ～ネットワーク編／IPv6ハンズオン ～サーバー編
18（水）	第107回通常理事会（東京、JPNIC会議室）
24（火）～3/6（金）	APRICOT-APAN 2015（福岡、JR博多シティ・福岡国際会議場）

3月

5日 10日 15日 20日 25日 31日

2（月）～6（金）	39th APAN Meeting（福岡、福岡国際会議場）
5（木）～6（金）	Security Days 2015［後援］（東京、JPタワー（KITTE））
6（金）	APNIC 39（福岡、福岡国際会議場）
20（金）	第55回臨時総会（東京、アーバンネット神田カンファレンス） 第108回臨時理事会（東京、アーバンネット神田カンファレンス）

「APRICOT-APAN 2015 福岡会合」のご紹介

2015年2月24日（火）から3月6日（金）にかけて、福岡市の福岡国際会議場およびJR博多シティにて、APRICOT-APAN 2015が開催されました。APRICOT会合としては10年ぶり、APAN会合としては9年ぶりの日本開催となりました。会合の模様は、今夏発行予定の次号にて詳しくご報告する予定ですが、本稿では、このAPRICOT-APAN 2015 福岡会合について簡単にご紹介いたします。

◆ はじめに

久しぶりに日本で、インターネット基盤運営技術の大きな国際会議が開催されました!

アジア太平洋地域における、インターネットの基盤運営に関わる技術者が集う年1度のフォーラムである「APRICOT（Asia Pacific Regional Internet Conference on Operational Technologies）」と、アジア太平洋地域における研究ネットワークの相互接続を行い、研究開発活動を共同で行う、「APAN（Asia Pacific Advanced Network）」の合同会合である「APRICOT-APAN 2015」です。2015年2月24日（火）から同3月6日（金）まで行われ、会場は、福岡市の福岡国際会議場およびJR博多シティでした。

- APRICOT-APAN 2015 日本語Webサイト
  http://jp.apricot-apan.asia/

JPNICは、本会合の実行委員会にも参画していましたので、このAPRICOT-APAN 2015 福岡会合について、簡単にご紹介したいと思います。

◆ APRICOT、そしてAPANとは ～両者の合同会議開催は、今回で2度目です～

APRICOTは、前述しましたが、アジア太平洋地域のインターネット基盤の発展のために、技術者に必要な知識や技術を向上させることを目的として年1度開催される、非営利のフォーラムです。

1996年にシンガポールで最初に開催されて以来、毎年2月下旬から3月上旬に、アジア太平洋地域のさまざまな都市で開催されており、今回の福岡会合が、20回目の開催となります。日本で前回開催されたのは2005年の京都会合になりますので、実に10年ぶりです。

アジア太平洋地域の地域インターネットレジストリであるAPNICは、「8月あるいは9月」と「2月から3月」と年度に2回の会合を開催していますが、2月から3月にかけての会合は、APRICOTと同時開催にすることを恒例としています。

一方のAPANは、1997年に活動を開始し、二つの側面を持ちます。一つは、アジア太平洋地域における学術ネットワークプロジェクトの相互接続という側面で、国際回線で接続された総体として、アジア太平洋地域全体をカバーする学術ネットワークとなっています。もう一つは、そのネットワーク基盤を用いた、基盤技術や応用技術の研究の場としての側面です。APANは年に2回会合を開催しています。日本では過去に7回開催されていますが、2006年1月の東京開催が最後ですので、こちらも9年ぶりと、久しぶりになります。

なお、APRICOTとAPANが合同で会議を開くのは、2011年の香港開催に続いて、2回目です。ちなみに1回目の香港では、商用と学術、双方のインターネット基盤運営関係者が一堂に会して、参加者は1,000人を超えました。このような大きなネットワークイベントが、日本ではしばらく開催されていない状況をかんがみ、今回協賛をしてくださっている主要5社に加えて、JPNICを含む関連団体が準備グループを組成し、実に「APRICOT-APAN 2011香港」の開催直後から、この2回目を日本で開催すべく準備企画を進めてきました。この準備グループがそのまま構成員となって、2014年3月に「APRICOT-APAN 2015 日本実行委員会」が発足し、アジア太平洋地域のインターネット関係者を福岡に呼ぶべく、開催に向けた準備を進めてまいりました。実行委員会の顔ぶれは、開催概要のページからご覧いただけます※1。

◆ APRICOT-APAN 2015の構成とプログラム

APRICOT-APAN 2015の日程では、全体としてAPRICOTの構成をベースとしました。APRICOTは、前半をワークショップウィーク、後半をカンファレンスウィークと位置づけました。

ワークショップウィークでは、第一線のエンジニアが、主に初心者を対象にして、DNSやルーティング、インターネットエクスチェンジ構築などのインターネット基盤技術の実機演習を、ワークショップとして開催しました。その後のカンファレンスウィークでは、数多くのセッションで発表が行われ、インターネット基盤の運営に関する最新技術が議論されました。

今回はAPRICOTとAPANが併催となるため、APANのプログラムもカンファレンスウィークに並びました。APAN会合は、基本的にAPAN参加各国からの研究発表を基調としています。ネットワーク基盤技術だけでなく、農業、医療に対するネットワークの適用など、商用のインターネットではなかなか見られない、最先端の技術を垣間見ることができます。

※1 APRICOT-APAN 2015開催概要
http://jp.apricot-apan.asia/about/

今回の会合において、具体的にどのようなプログラムが開催されたのかについては、次のURLからご覧いただけます。

APRICOT 2015 Program
https://2015.apricot.net/program

APAN 39 Program
http://apan.net/meetings/Fukuoka2015/schedule.php

◆ おわりに

今回の会合は、商用を中心としたインターネット基盤技術のAPRICOT、IPアドレスの管理方針を議論するAPNIC、学術ネットワークのAPANが、福岡に集結する、またとない機会となりました。常に拡大し成長し続けるインターネットを支えているのは、その時々の最新技術だけでなく、それを使ってネットワーク基盤を構築して運営するエンジニアです。そういうエンジニアが集い、情報交換を行うことで、初めてインターネット全体が円滑に動きます。アジア太平洋地域、また世界各国からエンジニアが集まるAPRICOTやAPANの会合は、常に活気に溢れています。今回の会合に参加された方々は、インターネット基盤を作り動かす人々の息遣いを感じることができたのではないかと思います。

なお、冒頭でも記した通り、本会合の詳しいレポートについては、今夏発行予定の次号にてお届けする予定です。

APRICOT-APAN 2015 開催概要

○**日 程** 2015年2月24日（火）から3月6日（金）まで

○**会 場** [ワークショップ（2月28日（土）まで）]
JR博多シティ
http://www.jrhakatacity-eventspace.jp/access/
[カンファレンス（3月2日（月）から）]
福岡国際会議場
http://www.marinemesse.or.jp/congress/access/

○**主 催** APRICOT-APAN 2015 日本実行委員会

○**共 催** 国立情報学研究所（NII）

○**後 援** 農林水産省/文部科学省/経済産業省/総務省/福岡県/福岡市/IPv6普及・高度化推進協議会（v6pc）/一般財団法人インターネット協会（IAjapan）/Internet Society Japan Chapter（ISOC-JP）/HD-PLCアライアンス/仮想化インフラストラクチャ・オペレーターズグループ（VIOPS）/九州ギガポッププロジェクト（QGPOP）/九州インターネットプロジェクト（QBP）/九州産業大学/九州大学 情報基盤研究開発センター/一般社団法人クラウド利用促進機構（CUPA）/Cyber Kansai Project（CKP）/一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）/情報処理学会 インターネット運用研究会（IOT研究会）/電子情報通信学会インターネットアーキテクチャ研究専門委員会（IEICE IA研究専門委員会）/一般社団法人日本インターネットプロバイダー協会（JAIPA）/日本学術振興会産学協力研究委員会インターネット技術第163委員会（ITRC）/日本シーサート協議会（NCA）/一般財団法人日本情報経済社会推進協会（JIPDEC）/日本DNSオペレーターズグループ（DNSOPS.JP）/日本ネットワーク・オペレーターズ・グループ（JANOG）/特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）/日本UNIXユーザ会（jus）/WIDEプロジェクト（WIDE）

○**協 賛** 株式会社インターネットイニシアティブ/インターネットマルチフィード株式会社/NTTコミュニケーションズ株式会社/ソフトバンクBB株式会社/日本インターネットエクスチェンジ株式会社/Microsoft Corporation/株式会社日本レジストリサービス/Arbor Networks, Inc/IPv4 Market Group/Afilias Limited/アラクサラネットワークス株式会社/Alcatel-Lucent/A10ネットワークス株式会社/NTTアドバンステクノロジ株式会社/Curvature Solutions Pte Ltd./独立行政法人情報通信研究機構/セイコーソリューションズ株式会社/Digital Japan Investment Management G.K./株式会社デンソー/日商エレクトロニクス株式会社/日本電信電話株式会社/Netka System Co.,Ltd/Nominum, Inc./Vidyo Japan. Inc./三井情報株式会社/アカマイ・テクノロジーズ合同会社/九州通信ネットワーク株式会社/独立行政法人産業技術総合研究所/ジュニパーネットワークス株式会社/株式会社DMM.comラボ/楽天株式会社/Google Inc./Internet Corporation or Assigned Names and Numbers（ICANN）/TEIN*Cooperation Center（TEIN*CC）/Equinix, Inc./Internet Society（ISOC）/Network Startup Resource Center（NSRC）/一般社団法人日本ネットワークインフォメーションセンター

○**内 容** ワークショップ、チュートリアル、カンファレンス、ワーキンググループセッション、併設展示・デモ、レセプション、ソーシャルイベント

○**URL** http://jp.apricot-apan.asia/（日本語）
https://2015.apricot.net/（英語）
（日本語）（英語）

○**使用言語** 英語

○**対 象 者** ネットワーク運用に携わる技術者
アジア各国のインターネットインフラに興味をお持ちの方
アドレスポリシー策定・資源管理に興味を持つ方

○**お問い合わせ先**
APRICOT-APAN 2015日本実行委員会 事務局
（株式会社イーサイド内）
apricot-apan-office@e-side.co.jp

ICANNロサンゼルス会議報告および第41回ICANN報告会開催報告

2014年10月12日(日)から16日(木)に米国ロサンゼルスで第51回ICANN会議が開催され、本会議の報告会を11月19日(水)にJPNICと一般財団法人インターネット協会(IAjapan)の共催にて開催しました。報告会はこの時期の恒例となる、Internet Week 2014の同時開催イベントとしての開催となりました。本稿では、ロサンゼルス会議の概要を中心に、報告会の様子も併せてご紹介します。

関連記事「P.2 特集1 インターネットガバナンスの動向」

ICANNロサンゼルス会議報告

◆ ロサンゼルス会議の特徴

今回のロサンゼルス会議で、最も多く聞かれたキーワードは「説明責任(Accountability)」でした。本稿では、IANA機能の監督権限移管と、ICANN自身の説明責任に関する議論の動向をご紹介するとともに、引き続き議論されている、新gTLDやWHOISに関する議論の動向を取り上げます。

また、オープニングセッションでは、開催地の政府関係者として、米国商務長官のPenny Pritzker氏がIANA監督権限移管の提案に向けて、ICANNとコミュニティが一丸となって協力し、検討を進めていくことが重要というスピーチを行いました。米国政府の長官が、ICANN会議に参加し、スピーチを行うことは初めてのことです。米国政府の姿勢として新しい発表はありませんでしたが、商務長官自らが、ICANN会議に出向いてスピーチを行ったことで、IANA機能を取り巻くこの一連の動きを重視し、コミットしていることが見て取れました。

● オープニングセッションでスピーチをするPenny Pritzker氏

◆ ドメイン名におけるIANA機能の監督権限移管提案に関する進捗

P.2からの特集1で詳しく紹介していますが、ICANNの各コミュニティからは、IANA機能の監督権限移管に関して、ドメイン名についての提案を提出することになっています。この議論を進めるに当たって、ICANNコミュニティでは、ICANN自身の説明責任機構を整備する必要があるとして、両者を関連付ける論調が根強い状況です。前回のロンドン会議では、ICANNの説明責任に関する検討の進め方にコミュニティから懸念が示され、大きな議論がありました※1。今回は、ICANN側が本件に関してコミュニティに大きく歩み寄る姿勢を見せ、コミュニティが懸念しているICANNの説明責任に関する課題について、ICANNコミュニティが主体となり検討できる枠組みを提示したため、多くの参加者がこれを受け入れました。これによって、IANA機能の監督権限移管に向けた議論も、前向きな姿勢で進めるスタートラインに立ったと言えそうです。

また、ICANN自身が2015年1月までにドメイン名の監督権限移管に関する提案を作る必要があることから、今回のロサンゼルス会議では、ドメイン名に関する移管提案を検討するワーキンググループ「ドメイン名に関連するIANA監督権限移管提案立案のためのクロスコミュニティワーキンググループ(Cross Community Working Group to Develop an IANA Stewardship Transition Proposal on Naming Related Functions)」を、各支持組織(SO)や諮問委員会(AC)の代表者により組成して、対面会議が実施されました。

ドメイン名に関する提案を2015年1月までに策定する上で、ロサンゼルス会議がICANNコミュニティとして対面で議論を行う最後のタイミングでしたので、どの程度進捗があるのか、個人的には着目していました。しかし、結論としては、全体として議論した以下のセッションのいずれにおいても、進め方の確認や意向表明が目立ち、具体的な提案内容の方向性が見えてくるような議論は確認できませんでした。

・Meeting of the CWG to Develop an IANA Stewardship Transition Proposal on Naming Related Functions
http://la51.icann.org/en/schedule/mon-iana-stewardship-naming

・Community Discussion with the IANA Stewardship Coordination Group (ICG)
http://la51.icann.org/en/schedule/thu-icg-community

ドメイン名以外の二つの資源に関しては、IPアドレスについては各RIRのフォーラムで、プロトコルパラメータについてはIETFで、それぞれ内容の議論が進んでいる状況ですので、ICANNにおけるドメイン名に関する提案の検討は、大きく出遅れている状況です。しかし、CWGのメンバーからは、上記のセッションで、2015年1月の期限に間に合わせることに意欲的な意見が表明されていましたので、今後の検討の進展に期待したいと思います。

◇ 参考情報:
・IANA Department - Who, What, Why?
http://la51.icann.org/en/schedule/mon-iana
・SSAC Report
[SAC068]: SSAC Report on the IANA Functions Contract (10 October 2014)
[SAC067]: Overview and History of the IANA Functions (15 August 2014)

◆ ICANNの説明責任に関する議論

また、ICANNの説明責任に関する課題のうち、IANA機能の監督権限移管による影響を受けるものについては、その対応案を移管に関する提案と同期して、NTIAに提出することが求められています。ICANNの説明責任機構に関する議論については、IANA機能の監督権限移管に関する検討との関係性が、ICANNコミュニティも納得のいく形で整理されたことが、今回の大きな成果です。

まず、本件に関する検討を行う「ICANNの説明責任強化に関するクロスコミュニティワーキンググループ(Cross Community Working Group on Enhancing ICANN Accountability)※2」を設立することにし、ロサンゼルス会議の会期中にドラフティングチームを組成して、チャーターの起草作業が進められました。筆者はアドレス支持組織(ASO)の代表として、このチームに参加しました。現在、意見募集中のチャーターでは、IANA機能の監督権限との関連性をもとに、議題を二つの「Work Stream」に分けることになりました。

・Work Stream 1 : 監督権限移管までに解決すべき課題
・Work Stream 2 : 監督権限移管後も、長期的に解決すべき課題

Work Streamを二つに分けたことで、IANA提案の提出時期が長期的課題の解決に影響されなくなり、「長期的なICANNの説明責任に関する課題への対応が明らかになるまで、IANA提案が提出できない」という状態を避けることができそうです。

◆ 新gTLDに関して

2012年から実施された新gTLD第1ラウンドについては、オークションによる収入の取り扱いが今後の理事会での決議事項として残っているものの、全体としては着々とプロセスが進行している印象です。さらに、第1ラウンドの結果を検証し、次回第2ラウンドに向けた改善をまとめようという動きも出てきました。

一方、第1ラウンドによる新gTLDの実際の導入が進んでいることに伴い、後述する名前衝突の問題や、TLD Universal Acceptanceの問題も出てきています。しかしながら、これらは会議全体の中で、大きな議論はされていませんでした。

これらの問題を含め、今回確認された主な進捗を、以下にまとめてご紹介します。

◇ 申請処理状況:
・ロサンゼルス会議時点で、新gTLD418件の委任を完了と発表
・競合する文字列(Contention Set)については、233件のうち、約半数を超える120件が解決済み
・オークションに伴う収入、コストを公開

ロサンゼルス会議時点でのオークションによる収入は、13,904,785USドルと発表されています。最終的な合計額が確定してから、理事会で対応を検討することになります。

・新gTLDに関する進捗報告セッション
http://la51.icann.org/en/schedule/mon-new-gtld

◇ 名前衝突
現在適用されている、衝突の恐れがあるドメイン名のリストを提示して対応を促したり、報告窓口を設置したりするなどの対策は、今回のラウンドの新gTLD申請のみに対して、2年間のみ有効なものとして適用されます。

これを踏まえ、将来的に次のラウンドの開始が決定した場合に備える必要性や、既存のgTLDも視野に入れた長期的な対策に向けた質問が、今回の会議でコミュニティに投げかけられました。今後大きな進捗がありましたら、JPNICの名前衝突問題に関する情報提供ページで、随時情報更新を行ってまいります。名前衝突問題自体に関する説明も、このページをご参照ください。

・名前衝突セッション
http://la51.icann.org/en/schedule/wed-name-collision

・名前衝突問題についてまとめたJPNICのページ
https://www.nic.ad.jp/ja/dom/new-gtld/name-collision/

◇ Universal Acceptance
新たに追加されたTLDが、正しい電子メールアドレスとして識別されない、正しいWebサイトとして認識されないといったこの問題は、これまでは国際化ドメイン名(IDN)を中心とした問題として捉えられてきましたが、新gTLDにおいても同様の問題が、実際に発生していることが報告されています。

Facebookのようなメジャーなアプリケーション、公共機関の提供しているWebサイトなどでも問題が確認されており、「.city」など100を超える新gTLDの申請を行った、大手のレジストリであるDonuts社などは、ICANNだけではなくコミュニティ全体として、周知と対策の促進を検討するよう呼びかけています。

Universal Acceptanceセッション:
http://la51.icann.org/en/schedule/wed-universal-acceptance

※1 JPNICニュースレター No.58「ICANNロンドン会議報告および第40回ICANN報告会開催報告」
https://www.nic.ad.jp/ja/newsletter/No58/0550.html

※2 Cross Community Working Group on Enhancing ICANN Accountability
https://community.icann.org/display/acctcrosscomm/Cross+Community+Working+Group+Home

◇第1ラウンドの検証
新gTLDプログラム第1ラウンドの検証、次の第2ラウンドに向けての検討事項のたたき台が、ICANNから発表されています。GACからは、「今回のラウンドでGACが提出したセーフガードに関する勧告への、ICANNの対応に満足していない。これが適切に対応されるまでは、次のラウンドを開始すべきではない」といった意見もあるようですが、ICANNからも、「現在のラウンドにおける課題が整理されるまで、次のラウンドを進める意向がない」ことが説明されたことから、長期的な検討事項として整理に着手したと見ておくのがよさそうです。

https://centr.org/system/files/share/centr-report-icann51-20141017.pdf

◇その他
新gTLDの導入に伴う政府間国際組織(IGO)・非政府間国際組織(INGO)に関わる名称の保護、国コードと重複する2文字TLDの申請、IDNラベルの生成に向けた検討パネルなどについても、継続して検討が行われています。

◆ gTLD WHOISに関する検討

最後にドメイン名の登録者・利用者として押さえておきたい議論としては、gTLD WHOISの見直しを視野に入れた検討です。gTLD WHOISのあり方を根本的に検証した最終報告書が、理事会に提出されたことを機に、理事長のSteve Crocker氏からも、WHOISについては重要な検討課題として長期的に、慎重に抜本的見直しを行っていくという姿勢が、オープニングセッションで示されました。

現時点では、長期的な計画の議論が中心ですが、WHOIS登録者、利用者の立場から、今後ドメイン名のWHOISにおいてどのような変更があり得るのか知っておく上で、ご確認いただくとよさそうです。詳細を後述します。

◇gTLD WHOISの抜本的な見直し
情報の参照権限・公開など、gTLDのWHOISのあり方を抜本的に検証した、専門家グループ(EWG)の報告書が理事会に提出されました。これからICANN理事会が、内容の検証とポリシー策定プロセス(PDP)の必要性について検討に入ります。登録情報に関するプライバシーが大きな課題となるとCrocker氏は述べていました。

なお、ICANN会議に参加する、技術的な専門家による個別の会議では、全gTLDに関わるWHOIS情報を1ヶ所に集約する現在の案を、疑問視するコメントも確認されました。

◇その他の動向:
プライバシー・プロキシサービスに対する対応として、ドメイン名の登録者の代理として事業者の連絡先を登録している場合、代理の事業者が登録者に連絡を取れるようにすることを、レジストラ契約上求める方向で議論が進んでいます。

また、英語以外の言語で登録された、連絡先情報の変換と翻訳の必要性が、専門のWGで検討されています。しかしながら、登録情報の変換と翻訳は、必須としない意見が優勢となっていました。

・WHOIS Updateセッション:
http://la51.icann.org/en/schedule/mon-whois

(JPNICインターネット推進部／IP事業部 奥谷泉)

第41回ICANN報告会開催報告

ICANNロンドン会議の開催を受け、恒例となっているICANN報告会をIAjapanとの共催で開催しましたので、簡単にご報告します。

今回の報告会は、当該週に開催されたInternet Week 2014との同時開催プログラムの一つであったこともあり、会場はほぼ満席となりました。今回もまた、シンガポールにあるICANNアジア拠点のKelvin Wong氏にご登壇いただき、ICANNスタッフと日本のユーザーが直接意見を交換する、貴重な機会ともなりました。

・日時:2014年11月19日(水) 16:15〜18:45
・会場:富士ソフトアキバプラザ(東京・秋葉原)

右のプログラムのうち、特徴的なものを次ページ以降でご報告します。

プログラム: (話者 敬称略)

ICANNロサンゼルス会議概要報告	JPNIC 奥谷 泉
ICANN政府諮問委員会(GAC)報告 総務省総合通信基盤局電気通信事業部データ通信課 山口 修治	
新gTLD関連報告 株式会社日本レジストリサービス(JPRS) 遠藤 淳	
ICANN APAC Hubとジャパン・リエゾンについて	ICANN Kelvin Wong
ICANN国コードドメイン名支持組織(ccNSO)関連報告/ ICANNルートサーバー諮問委員会(RSSAC)関連報告 株式会社日本レジストリサービス(JPRS) 堀田 博文	
ICANNのアカウンタビリティに関するパネルディスカッション モデレーター:前村昌紀(JPNIC) パネリスト:奥谷泉(JPNIC)、北村泰一(ISOC-JP)、Kelvin Wong(ICANN)、堀田博文(JPRS)、村上嘉隆(株式会社ブライツコンサルティング)、山口修治(総務省)	

◆ ICANN政府諮問委員会(GAC)報告

総務省の山口氏より、GACの動向に関して、主に次の3点についてご報告いただきました。

(1) 次世代WHOIS:課題(正確さ、国内法との関連、プライバシー／プロキシー認定の課題、言語サポート、理事会での扱いなど)との関連性と、今後必要となる作業を並べたスケジュール表を要請

(2) IANA監督権限移管およびインターネットガバナンスの今後の展開:GACとして理事会に助言すべく、包括的な原則を作成することで合意

(3) 新gTLD関連のGACロサンゼルス助言

- 消費者保護の観点等からセーフガード助言を行った文字列
- 政府間機関(IGO)名称の保護、および赤十字/赤新月社の各国内関連名称等の保護
- 新gTLDのセカンドレベルにおける2文字名称解放
- 将来の新gTLD申請に向けた、現行新gTLDプログラムのレビュー作業

◆ ICANN APAC Hubとジャパン・リエゾンについて

ICANNのKelvin Wong氏より、まずはじめにICANNのグローバル化を実現するための一環である、アジア太平洋オフィスの状況をご報告いただきました。続いて、日本に対するエンゲージメント強化の一環として、これまで日本を含むアジア地域のアウトリーチなどを担当しているWong氏に加え、大橋由美氏がジャパン・リエゾンとして任命され、日本のコミュニティに特化した情報提供を開始したことが紹介されました。当日は大橋氏も会場に来られており、ご挨拶いただきました。その他には、2014年9月に東京にて新gTLDレジストリ向け、およびレジストラ向けの会合を開催したことなどが報告されました。

◆ ICANNのアカウンタビリティに関するパネルディスカッション

パネルディスカッションでは、ICANNのアカウンタビリティについて議論しました。ICANNのアカウンタビリティ機構の現状などについてJPNIC前村より説明した後、各ステークホルダーより、ICANNのアカウンタビリティに対するお考えをお話しいただきました。パネリストからの主な発言は次の通りです(括弧内は所属コミュニティ)。

[Kelvin Wong氏(ICANN)]
コミュニティからのフィードバックをいただきたい。
[村上嘉隆氏(ビジネス/GNSO 知的財産部会)]
ICANNが規模が拡大した結果、アカウンタビリティに関する明確化の声がより高まっている。
[堀田博文氏(ccTLDレジストリ/GNSO gTLDレジストラ部会)]
アカウンタビリティの定義の明確化が必要ではないか。
[奥谷泉(ASO/GNSO ISP部会)]
ICANNはマルチステークホルダーと言いながら、欧米中心で議論しており、また、技術コミュニティからの意見があまり見受けられないなど、地域やステークホルダーが偏った議論になっているように思う。
[山口修治氏(GAC)]
複雑な状況の中で組織運営をよくやっており、徐々にではあるが改善もしてきていると思う。一方、ICANNにおける日本のプレゼンスは高いとは言えず、これを改善していく必要がある。

少々時間が不足気味でしたが、活発な議論を行うことができました。

◆ 最後に

もしかしたら「ICANNのアカウンタビリティ」というような大きなテーマをきちんと話すためには、もっとディスカッションする時間が必要だったのかもしれません。こうした重要なテーマについては、ICANN報告会という場にとどまらず、日本インターネットガバナンス会議(IGCJ)の場なども利用し、今後、そうした議論が日本でもっと活発にできる土壌や雰囲気を生成していけるよう、JPNICとしても努力してまいります。

日本インターネットガバナンス会議(IGCJ)
https://www.nic.ad.jp/ja/governance/igconf/

(JPNIC インターネット推進部 山崎信)

● パネルディスカッションでは、「ICANNのアカウンタビリティ」を取り上げました

第54回JPNIC臨時総会および講演会の報告

2014年12月5日(金)、第54回JPNIC総会(臨時総会)を東京都千代田区のアーバンネット神田カンファレンスにて開催いたしました。今回の総会では、2件の報告事項のほか、2014年度補正予算案の1議案につき、会員の皆様にお諮りしました。以下にその模様を簡単にご報告します。

◆ 理事長挨拶、その他

総会の開会に先立って後藤滋樹理事長から、Internet Week 2014が多くの参加者を得て、盛況裏に閉幕したことが報告され、会員の皆様からのご協力に対する感謝が述べられました。

また、2015年2月下旬～3月上旬にかけて、福岡で開催されるAPRICOT-APAN 2015はJPNICも実行委員の一員として準備を進めており、会員の皆様の参加も大いに期待したい旨が伝えられました。

最後に、JPNIC事務局長、理事、そして監事として多大に貢献をいただいた成田伸一さんが2014年7月に急逝されたことについて、あらためて弔意が表されました。

その後、議長選任、議事録署名人指名の後、報告事項の説明を行いました。

● 開会の挨拶をする後藤理事長

◆ 報告事項:逆引きDNSへのDNSSEC導入の検討状況について

伊勢IP事業部次長より、JPNIC管理下の逆引きDNSに対し、DNSSEC導入を検討している旨とその計画が報告されました。概要は次の通りです。

【導入検討の背景】
・逆引きDNSの活用についてヒアリング調査を行ったところ、多くの組織が日常的に逆引きDNSを活用しており、逆引きDNSの安定的、継続的な提供が求められている
・キャッシュポイズニング攻撃により、DNSに対する危険性が高まっており、早期の対策が必要となっている
・IANAおよび各RIRではDNSSECの導入は完了しているので、JPNICが導入を行うことで、ルートゾーン、RIR管理のゾーンから連なる逆引きゾーンの信頼の連鎖を完成させる必要がある

【導入の進め方】
・2015年度前半に、レジストリシステム高機能化の一環として、DNSの改修および業務体制の整備を完了し、2015年度後半から事業者による登録を開始する
・2015年度末までに、少なくとも五つのIPアドレス管理指定事業者が利用する状況をめざす
・2016年度より、普及啓発活動の対象を全契約者(IPアドレス管理指定事業者およびPI割り当て先組織)へ拡大し、順次利用者の増加を図る

これに対し、その必要性や費用対効果などに対する質問や意見が寄せられました。導入の計画と予算については、次回総会でお諮りする2015年度事業計画および収支予算に組み込まれる予定です。

◆ 報告事項:インターネットガバナンスにかかわるトピックスのご紹介

次に、前村インターネット推進部部長から「インターネットガバナンスにかかわるトピックスの紹介」と題し、「ドメイン名政策委員会」と「日本インターネットガバナンス会議(IGCJ)」という二つの事項について報告いたしました。

前者のドメイン名政策委員会は、JPNICの役割の一つであるJPドメイン名の公共性の担保という観点からの報告であり、後者のIGCJは、インターネットガバナンスに関するさまざまな課題を日本の幅広い関係者で話し合うことができる「場」をめざして、JPNICが積極的に取り組んでいる活動の紹介です。IGCJについては会員の皆様にも積極的に関与して欲しい、とのお願いもありました。

◆ 第1号議案:2014年度補正予算案承認の件

本議案は、2014年3月14日(金)に開催の第52回通常総会にて承認された、2014年度当初の収支予算に変更が生じたため、各数値が見直された、補正予算案についてお諮りしたものです。変更となる経常収益、費用などについて林事務局長が説明を行いました。

議案の説明に引き続き議場に質疑を求めましたが、質疑は無く、その後当議案の賛否を会場にお諮りした結果、原案の通り可決されました。

経常収益予算　516,290,000円(当初予算比　＋900,000円)
経常費用予算　534,940,000円(当初予算比 －10,980,000円)

以上をもって、総会は閉会となりました。

◆ 総会講演会:インターネット信頼性に向けた技術のご紹介

総会に引き続いて、「インターネット信頼性に向けた技術のご紹介」と題し、「DNSSEC」および「RPKI(リソースPKI)」という二つの技術の紹介がありました。

DNSSECに関しては、株式会社日本レジストリサービスの松浦孝康さんから紹介がありました。DNSSECはよりセキュアなDNSの運用を実現するための技術ですが、その導入に向けた全体的な状況が俯瞰された後、現状の課題と今後の展望が述べられました。現在DNSSECは、一般への普及段階に進んでいる過程と言えそうですが、各組織がDNSSECに対応するには、そのリスク軽減や、費用と運用の課題などを継続して解決していく必要があることも述べられました。

RPKIに関しては、インターネットマルチフィード株式会社の吉田友哉さんから紹介がなされました。まず初めにインターネットの経路制御を脅かす脅威について説明され、その後、取り得る対応策のうち「予防」の役目をするRPKIについての解説と、現在の取り組みが話されました。

インターネットマルチフィード社とJPNICは、IPアドレスとAS番号の正しい組み合わせであるROA(Route Origin Authorization)のキャッシュサーバを運用しています。PKIの知識も必要とされるそうしたサーバ運用の難しさも語られながらも、東京オリンピックなども視野に入れた日本全体の経路情報の信頼性向上に向けては、こうしたキャッシュサーバを運用する組織が増えることや、BGPルータでの設定についても各組織がきちんと対応していくことが、安心・安全な通信インフラを作るのであり、そういう世界をめざしていこうという力強い言葉で講演は終わりました。

この第54回臨時総会の資料・議事録、また講演会の資料およびビデオは、JPNIC Webサイトにて公開しています。

JPNIC第54回総会(臨時総会)
https://www.nic.ad.jp/ja/materials/general-meeting/20141205/

第54回総会講演会
https://www.nic.ad.jp/ja/materials/after/20141205/

(JPNIC 総務部 手島聖太)

● DNSSECについて講演を行う松浦孝康氏

● RPKIについての講演を行う吉田友哉氏

第27回JPNICオープンポリシーミーティング報告

2014年11月18日(火)に、東京都千代田区の富士ソフトアキバプラザにて、第27回JPNICオープンポリシーミーティング(JPOPM)を開催いたしました。今回のJPOPMは、11月18日(火)～21日(金)にかけて開催されたInternet Week 2014の同時開催イベントとして、初日の午後に開催されました。本稿では、このJPOPMの模様をご紹介します。

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。年2回の開催で、JPNICとは独立した組織であるポリシーワーキンググループ(ポリシーWG)が主催し、近年この時期のミーティングはInternet Weekの中で開催しています。また、プログラムについては、ご応募いただいたポリシー提案や、情報提供プレゼンテーションから構成しています。

今回は3件の提案と6件の情報提供がありました。ミーティングには、オンサイトで約50名(関係者含まず)の皆様に参加いただきました。今回も、JPNICの協力により、映像ストリーミング、Jabberチャット、Twitterによるリモート参加環境を構築しました。ストリーミングにおいては、ユニークなアクセスは89人(セッション)、平均で15人前後のアクセスがありました。

以下、提案議論の概略、および、いくつかの情報提供トピックスについて報告します。

◆ 今回議論された提案について

027-01 JPNICにおけるアドレス移転支援について
027-02 エンドユーザIPアドレス割り振り・割り当てサイズの明確化
027-03 レガシーIPv6アドレス空間の有効利用に関する提案

これらのうち、027-01、027-02の2件はすぐにポリシーの変更が伴う提案ではなく、現行のポリシーとその周辺の制度において課題となっている点の改善提案であり、番号資源コミュニティに対する議論の提起となっています。それぞれの提案について簡単に紹介します。

1. JPNICにおけるアドレス移転支援について(027-01)

027-01は、IPアドレス移転制度の利用を希望する組織のうち、移転する組織が移転を受け入れる組織を見つけることが難しいという認識からの提案です。本提案は、IPアドレスを有効利用するために情報提供の方法を検討して、適切な移転の活用がより進むための施策の検討と実施を、レジストリに依頼したいという内容です。議論の結果、コミュニティからのニーズは確認されたため、コンセンサスと同等の扱いとなりました。ただしポリシーではないため、実装勧告等は行わず、今後の進め方についてはJPNICとポリシーWGの間で協議して進める予定になっています。

2. エンドユーザIPアドレス割り振り・割り当てサイズの明確化(027-02)

027-02は、アドレスプリフィクス内における個別の利用状況の把握が該当ネットワークの運用者以外にとって難しく、別ネットワークが攻撃を受けた際、被攻撃側ネットワークでフィルター(ブロック)を実施するケースにおいて、関係ないアドレス領域までをフィルターの対象にしてしまうという、オーバーブロッキングの可能性があるという認識に基づいた提案です。利用者に割り当てたアドレスのプリフィクスサイズを知るために必要な施策を、レジストリに依頼したいということが提案されました。

これは提案者の考える問題を解決するための一つの施策が、ポリシーの変更を必要とする可能性があることから、本フォーラムに提案したことが補足されました。ニーズや必要性について多くの意見が交わされ、議論の結果、提案そのものがポリシーの特定部分を変更する内容ではなかったためコンセンサスとせず、一度提案者へ戻し、今後の問題解決の活動についても提案者に委ねることになりました。ただし、必要な議論を行うために本フォーラムを活用することについては歓迎することとしました。

3. レガシーIPv6アドレス空間の有効利用に関する提案(027-03)

027-03は、特定のIPv6アドレスブロックからの割り振りを受けている組織に対して、最大で/29までの割り振りを要求ベースで行えるようにするという提案です。この提案は日本のコミュニティの判断だけで実施できるものではなく、APNICのポリシーフォーラムでのコンセンサスが必要となる提案です。割り振りのポリシーが過去と現在で異なることで不公平感があるという意見がある一方、提案者からはアドレスの死蔵を防ぐための有効活用であるという説明が行われました。

議論の結果、本ミーティングにおいてはコンセンサスと判断してポリシー策定プロセス(PDP; Policy Development Process)プロセスを進めることとなりました。発行日現在、オンラインフォーラム(IP-USERSメーリングリスト)にてラストコールを実施中ですが、その中でコミュニティからの反対の意見や質問が投稿され、提案者からの説明が行われる等の議論がされています。ラストコールは2014年12月26日(金)までの期間で実施されましたが、追加の意見が出たため2015年1月9日(金)まで期間が延長されました。最終的にはコンセンサスに至ったとの判断が行われています。

◆ ポリシーの施行について(報告)

前回開催のJPOPMでは提案が無かったため、実装についての報告はありませんでしたが、最近のポリシーの変更に伴い実施された「JPNICに返却済みIPv4アドレスからの割り振り」と「AS番号移転」についての報告がありました。割り振りの件数等、情報の詳細については、右記第27回JPOPMプログラムのURLから当日発表の資料をご参照ください。

◇　◇　◇

その他、現状の日本におけるPDPの解説、国際IPv4アドレスの移転について、APNIC 38カンファレンス参加報告、ベトナムの国別インターネットレジストリ(NIR)であるVNNIC(Vietnam Network Information Center)の担当者からの発表、番号資源におけるIANA機能の監督権限移管に関する状況アップデート等のセッションを開催しました。

◆ ミーティングを振り返って

今回、数回ぶりに提案およびそれについての議論のあるJPOPMでした。情報提供を通じて番号資源利用者コミュニティを盛り上げていくことも重要ですが、各種提案があり、それに対する議論が実施できる方がミーティングが充実することは自明です。運営に関わる者としての手前味噌な評価ではありますが、内容としてとても良かったと考えています。一方で、ポリシーに直接変更を加えることではない内容であっても、最終的にポリシーに影響を及ぼす可能性を意識して議論することが重要であることを気付かされたミーティングでもありました。今後も、コミュニティのニーズや実情に注意を払って運営してまいります。

◇　◇　◇

◆ 第27回JPNICオープンポリシーミーティング(今回)の資料について

当日の発表資料および議事メモは、次のURLに掲載しております。

第27回JPNICオープンポリシーミーティングプログラム
http://www.jpopf.net/JPOPM27Program

◆ 第28回JPNICオープンポリシーミーティングについて

2015年6月を目処に開催を予定しております。詳細が確定し次第、IP-USERSメーリングリストにてお知らせいたします。

JPNICメーリングリスト
https://www.nic.ad.jp/ja/profile/ml.html

◇　◇　◇

最後になりますが、オンサイト、リモートともに議論にご参加いただいた皆様、ご発表いただいた皆様、ありがとうございました。

次回のミーティングでも、アドレスポリシーに関してご意見をお持ちの方の提案や、プレゼンテーションのご応募をお待ちしています。今回ご参加いただけなかった方も、ぜひともご参加ください。

(ポリシーワーキンググループ/グリー株式会社 橘俊男)

● 会場の様子。たくさんの方々にご参加いただきました。

インターネット A Scene of Internet History

歴史の一幕

東京大学 情報基盤センター
ネットワーク研究部門
准教授
中山 雅哉

インターネットワークの起こりと広がり ～林英輔先生の功績を中心に～

日本国内では、1980年代半ばまでは大学や研究所などの組織内部においてLANの構築が行われるようになり、1980年代後半から徐々に、組織のLAN同士を相互に接続した「インターネットワーク」という組織間接続が進められるようになりました。

1984年10月には、UUCPプロトコルによるJUNET（Japan/Japanese University NETwork）の実験が、また同年にはDECnetプロトコルによるHEPNET-J（High-Energy Physics Network Japan）の構築が、さらに1985年4月にはRSCSプロトコルによるBITNETJP（Because It's Time Network in Japan）の運用が始められたことが、これらの代表です。

その後、米国などで1981年頃から研究が進められてきたIPによる「インターネット」が、国内でも 1988年のWIDE（Widely Integrated Distributed Environment）、JAIN（Japan Academic Inter-university Network）、1989年のTISN（Todai International Science Network）などで始められました。さらに1992年には学術情報センターによるSINET（Science Information NETwork）が全国の大学研究機関を相互接続する運用ネットワークとして発足することになります。

一方、JAINの活動は、旧帝大の大型計算機センターなどを中核として各地の大学等をUUCPやIPによる相互接続する「地域ネットワーク」を構成する形に進展しました。

東京大学を中心として1992年に運用が始まった地域ネットワークがTRAIN（Tokyo Regional Academic InterNetwork）です。それまでの「インターネットワーク」は、共同研究などを中心とした「実験」として組織間を相互接続するものが多かったのですが、TRAINは「運用ネットワーク」をうたった最初の「インターネットワーク」の一つでした。当時は、各大学はN1プロトコルを用いて大型計算機同士を接続する形態がとられていましたが、組織同士をIPによる接続形態に切り替えるようにプロモーションを進めたこともあり、関東甲信地区の多くの大学等が、TRAINに接続されることとなりました。

TRAINを円滑に運営するために、各組織が「共通経費」と呼ばれる分担費用を支払うための仕組みを検討したり、相互接続するネットワークの「AUP（Acceptable Use Policy）」に配慮した加入承認の仕組みを作るなど、さまざまな課題の解決が必要でした。これらに尽力された、後述する故林英輔先生の貢献は大変に大きなものでした。

特にTRAINでは、初等教育機関として山梨大学付属小学校（1994年）を日本国内で初めてIP接続することが承認され、その後も、100校プロジェクトや山梨県・アイオワ州国際教育交流プロジェクトの参加校などの、初等中等機関の接続を受け入れてきました。学術研究ネットワークが多かった当時では、教育機関を接続組織として受け入れてインターネットの利用推進に尽力されたことは、現在の教育機関でのインターネット利用にも大きな影響を与えることになりました。

100校プロジェクトが終了する頃からは、各自治体で教育用ネットワークの構築が行われるようになりましたが、山梨大学を定年退官された故林英輔先生は、その後、勤務された麗澤大学において、NPO法人「柏インターネットユニオン（KIU）」を創設され、千葉県柏市の学校でLAN環境の整備をする「Net Day」の活動や、柏市の学校をインターネットに接続する地域ネットワーク環境の提供活動などに尽力されています。

さて、話をTRAINに戻しますと、各参加組織におけるインターネット利用の需要拡大に伴うトラフィックの増加が主な要因で、設立から7年後の1999年にTRAINは解散に至りました。既に国内でも各種商用ISPが増えてきており、「共通経費」による運営形態だけでは十分な運用が困難になることが予想されたためです。

TRAINの解散にあたり、「東京地域アカデミックネットワークの歩み-TRAIN活動報告書-」（2000年3月発行）がまとめられましたが、林英輔先生の書かれた巻頭の挨拶を最後にご紹介します。

『かつて我が国にインターネットが普及しはじめた初期、TRAINという名の学術系地域ネットワークがあった。それは、当時の大学にインターネットの安定した利用環境をもたらすのに貢献し、7年間活動すると、活動を止め、組織を解散した。その活動の痕跡は何も残っていない。ただ、当時そのネットワークの構築や運用に携わった人が残っていて、未だにネットワークをやっている。間もなくこんな風に語られることになるだろうと思います。今ではインターネットの利用は飲み水がほしければ水道の蛇口をひねるのと同じように、容易に利用環境が手に入る時代になりつつあります。その昔、美味しい水を求めて澤の源流の泉をたずねたり、深く井戸を掘る人達がいました。TRAINが解散して一年経って、TRAINに関わった人々によるTRAINの活動の歩み、すなわち活動報告書をお届けします。』

このように1990年代後半、商用のネットワークが未発達だった頃、日本全国でいくつか地域ネットワークが生まれ、この地域ネットワークから初等・中等教育の現場や自治体へのネットワーク作りが広がり、そして地域IXへの展開まで至り、ネットワークが広がってきました。2014年5月に急逝された麗澤大学の林英輔先生は、これらの活動に尽力されてきました。

先生のご冥福を心よりお祈りいたします。

APNIC 38カンファレンス報告

全体およびアドレスポリシー関連報告

2014年9月9日（火）～19日（金）に、オーストラリア・ブリスベンにて、APNIC 38カンファレンスが開催されました。APNICカンファレンスは、APNICの本拠地があるオーストラリアで開催されることが多いと思われる方もいらっしゃるかもしれませんが、実は2010年8月のゴールドコーストでのカンファレンス以来、4年ぶりの開催となります。また、APNICの本拠地であるブリスベンでの開催は、2000年10月以来、およそ14年ぶりとなり、普段はオフィスで業務を行っているAPNICスタッフも多数参加していました。普段はメールや電話でのやり取りを行っていたAPNICスタッフとも、実際に顔を合わせて相談などを行う機会も何度かあり、JPNICスタッフとAPNICスタッフとのコミュニケーションを深める、良い機会となりました。本稿では、このカンファレンスの模様をご紹介します。

◆ APNIC 38カンファレンスの概要

今回のカンファレンスには、47の国や地域から331名の参加登録があり、そのうち、日本からの参加者は15名程度でした。毎年2月～3月に開催されるAPRICOT/APNICカンファレンスに比べて半分程度の参加者数となりますが、その分、参加者同士の距離は近く、アットホームな雰囲気であるように感じました。

カンファレンスは「チュートリアル」、「APOPS（Asia Pacific Network Operators Forum）」、「SIG（Special Interest Groups）」、「BoF（Birds of a Feather）」、「AMM（APNIC Member Meeting; APNIC総会）」などから構成されています。その他にも、APNICとの関連の深いAPIX（Asia Pacific Internet Exchange Association）、APTLD（Asia Pacific Top Level Domain Association）、APCERT（Asia Pacific Computer Emergency Response Team）やISOC-AU（The Internet Society of Australia）などの組織が主催する、会議やセッションの時間が設けられていました。

当日の資料、ビデオ、発言録は、以下のAPNICカンファレンスのページに掲載されています。今回参加できなかった方や現地での発言を聞き逃した方も、これらの資料を一度ご覧になってみてはいかがでしょうか。

http://conference.apnic.net/38/program

今回はこれらのセッションの中から、主なものをいくつかご紹介します。

◆ IANA機能の監督権限移管に関する提案と、インターネットガバナンス関連の動向について

IANA（Internet Assigned Numbers Authority）は、「ドメイン名」「番号資源」「プロトコルパラメーター」の、三つの重要なインターネット資源に関わる機能を担っています。これらの機能について、米国商務省情報通信局（National Telecommunications and Information Administration; NTIA）が持つ監督権限を移管する意向を2014年3月14日（金）に発表しました。この発表を受けて、移管後においてIANA機能の監督権限がどのようにあるべきかについて、各所で議論が進められています。APNICやJPNICにおいても、IANA機能の監督権限移管に関する情報提供を行っております。

・IANA oversight transition（APNIC Webページ）
http://www.apnic.net/community/iana-transition

・IANA機能の監督権限の移管について（JPNIC Webページ）
https://www.nic.ad.jp/ja/governance/iana.html

日本インターネットガバナンス会議（IGCJ）のメーリングリスト※1や、IP-USERS ML※2でもお知らせしていますが、今回のカンファレンスに先立ち、APNICからは、IANA機能の監督権限移管に関する提案が行われました。

提案では、「円滑なIANA機能の維持」「番号資源に関わるIANA機能についてのICANNとNRO（Number Resource Organization）間の役割・責務の明文化」の2点に重点を絞った内容となっています。提案の背景やその内容について、すべてを紹介することが

※1 日本インターネットガバナンス会議（IGCJ）
https://www.nic.ad.jp/ja/governance/igconf/

※2 IP-USERS メーリングリスト
https://www.nic.ad.jp/ja/profile/ml.html#ipusers

できませんが、APNICのブログ※3に詳細が掲載されていますので、そちらをご覧ください。

カンファレンス期間中には、APNICが主催するものとしては、会議に参加して直接議論できる唯一の機会として、IANA機能の監督権限移管に関する理解を深め、この提案について議論を行うことを目的としたセッションも設けられました。

セッションでは、提案内容が一通り説明された後、議論に移りました。提案内容に踏み込んだコメントや提案への反対意見はなく、原案通りの内容で他の地域インターネットレジストリ（Regional Internet Registry; RIR）に提示することとなりました。なお、2014年12月の各RIRでの提案取りまとめまで、まだ時間は残っていますので、会場での議論は終了しましたが、カンファレンス後も専用のML※4を利用して、議論を継続していくことになりました。

その他のインターネットガバナンス関連の特徴的な動向としては、これまでインターネット業界、インターネットに関連するコミュニティや、政府関係者などで構成されていたPPAC（Public Policy Advisory Committee）によるセッションの再検討が行われたことが挙げられます。

これまでのPPACの参加者にとらわれず、さまざまな関係者を巻き込んだ議論の場とすることを目的として、Cooperation SIGを立ち上げることがAPNIC事務局から発表されました。Cooperation SIGでは、公共政策、ネットワークセキュリティの規制、WHOISのプライバシー等について議論が行われる予定です。

◆ ポリシー提案について

今回のカンファレンスでのポリシー提案は、藤崎智宏氏（日本電信電話株式会社）による、「申請に応じたIPv6デフォルト割り振りサイズの拡張提案」の、1件のみでした。

この提案では、申請者が割り振りを受けるIPv6アドレスの用途を明確にすれば、追加の確認なしに/29（/32を8個分）を上限として割り振りを受けることを可能とする、という内容です。英語での記述となりますが、提案の詳細については、次のWebページをご覧ください。

・prop-111
申請に応じたIPv6デフォルト割り振りサイズの拡張提案（藤崎智宏氏）
http://www.apnic.net/policy/proposals/prop-111

当日の議論では、APNICの審議担当マネージャーから、拡張した割り振りを認める基準が明確ではなく、申請処理に支障を来すのではないかという懸念が示されました。また、IPv6の逆引きでは、/32、/28、/24という単位でゾーンが委任されますが、IPv6の逆引きをできるだけ容易に運用できるよう、割り振りの最大サイズを/29ではなく/28とした方が良いのではないか、というコメントも会場の参加者から出ていました。

前回のカンファレンスから引き続き議論されているこの提案は、残念ながら、今回もコンセンサスに至りませんでした。MLや当日の議論を踏まえて、提案者の藤崎氏より、提案を取り下げとする旨の報告がありました。

◆ コンセンサス確認の方法について

APNICカンファレンスでは、ストリーミングやチャットのサービスが提供されており、直接会場まで出向かなくても、当日の議論に参加することが可能です。しかし、参加者への意思確認は挙手に限られているため、会場以外からの参加者は意思確認に参加できない、という状況になっています。

前回カンファレンスの際に、会場以外からの参加者も意思を表明できるようなシステムを試作することが、APNIC事務局から発表されていました。今回のカンファレンスでは、先ほどご紹介したポリシー提案での議論の際に、試作されたシステムを利用して、会場、会場外を問わずに参加者の意思確認が行われていました。

試作されたシステムは現在も公開されており、次のURLから利用可能です。

・CONFER（CONsensus FEedback in Realtime）
http://confer.apnic.net/consensus/index.jsp

ただし、コンセンサスに至ったかどうかの判断はシステムのみではなく、議論の内容も踏まえて、ポリシーSIGのチェアが行うことになっています。このシステムによる意思表明の結果は、議論の内容と同じく、参考情報として利用されるのみとなっていました。チャットでもコメントを述べることができるような仕組みになっており、リアルタイムに経過が表示されるため、これから意思表明を行おうとする人に影響を与えてしまうのではないか、システムを利用する際の本人確認はどうやって行うかなど、利用者からのコメントが多く寄せられており、本格的に利用するためには、まだまだ解決すべき問題は多いように感じました。

また、こういったシステムの利用にとどまらず、いろいろな背景を持った多くの人が、今後の議論に参加するための方法を考える時期に差しかかっているのではないかとも感じました。

※3 IANA session @ APNIC 38: a discussion proposal（APNIC blog）
http://blog.apnic.net/2014/09/08/iana-session-apnic-38-a-discussion-proposal/

※4 IANAxfer mailing list
http://mailman.apnic.net/mailman/listinfo/IANAxfer

◆ NRO NCの選挙とポリシーSIGのCo-Chair選挙について

今回のカンファレンスでは、RIR全体として外部組織との調整が必要な場合に、全RIRを代表する組織であるNRO（Number Resource Organization）の、アジア太平洋地域を代表するNC（Number Council）の選挙が行われました。

・NRO NC Elections
http://conference.apnic.net/38/elections

現職でインド出身のNaresh Ajiwani氏に代わり、同じくインド出身のAjay Kumar氏が選出されました。2015年1月1日（木）から2016年12月31日（土）まで、グローバルIPアドレスポリシーの施行にあたり、ICANN理事会に勧告を行う役割を担います。

また、ポリシーSIGではCo-Chairの選挙が行われ、現職の山西正人氏が再選されました。今回のカンファレンス直後に、ChairのAndy Linton氏が退任を表明しChairが空席となったため、山西氏は次回カンファレンスまでChair代行を務めることも発表されています。

◆ 次回以降のAPNICカンファレンスについて

APNIC 39カンファレンスは、APRICOT 2015と共催で、2015年2月24日（火）～3月6日（金）に福岡市で開催されました。京都市で開催されたAPRICOT 2005/APNIC 19カンファレンス以来、10年ぶりの日本で開催となりました。このAPNIC 39カンファレンスの概要は、P.17の「『APRICOT-APAN 2015 福岡会合』のご紹介」でも取り上げていますが、詳細は次号にてご報告する予定です。

また、APNIC 40カンファレンス（2015年8～9月頃開催予定）はインドネシア・ジャカルタ、APNIC 41カンファレンス（2016年2～3月頃開催予定）はニュージーランド・オークランド、APNIC 42カンファレンス（2016年8～9月頃開催予定）はバングラデシュ・ダッカでの開催を予定している旨も、併せて発表されています。

（JPNIC IP事業部 川端宏生）

● Opening Ceremony and Keynotesの様子

各RIRにおける逆引きDNSSECの動向報告

筆者は、JPNICにてIPアドレスおよび逆引きDNSの登録管理システムを運用しているため、参加していた各地域の技術者とその方面の意見交換をしましたが、各地域にて逆引きDNSをFTP（File Transfer Protocol）やメールサービスの運用に活用している事例について、話をうかがうことができました。また、今回のAPNIC 38においては逆引きDNSに関する取り組みについて、APNIC技術チームともさまざまな意見交換を実施しました。本稿では、これらの情報の詳細についてご紹介します。

◆ 各RIRにおける逆引きDNSSECの導入状況

国際的な逆引きDNSSEC（Domain Name System Security Extensions）の導入状況を把握するため、世界を五つの地域に分け、それぞれの地域でIPアドレスの割り当て業務を行う組織である地域インターネットレジストリ（Regional Internet Registry; RIR）において、逆引きのDNSにどのくらいDNSSECが導入されているのか、状況を確認しました。

現在、RIRはAPNIC（Asia Pacific Network Information Centre）、ARIN（American Registry for Internet Numbers）、RIPE NCC（Réseaux IP Européens Network Coordination Centre）、LACNIC（The Latin American and Caribbean IP address Regional Registry）、AFRINIC（African Network Information Centre）の五つがあり、すべてのRIRで逆引きDNSSECの登録サービスが提供されています。

APNIC、ARIN、RIPEの3組織では、当日の逆引きDNSのゾーン情報が公開されており、該当3組織についてはそちらを元に状況を確認し、必要に応じて問い合わせを行いました。

APNIC、ARIN、RIPE管理のネームサーバにおけるゾーン情報
APNIC：ftp://ftp.apnic.net/public/zones/
ARIN　：ftp://ftp.arin.net/pub/zones/
RIPE　：ftp://ftp.ripe.net/pub/zones

具体的には、DNSSECの仕組み上、あるゾーンに対してDNSSECを有効にする場合、親ゾーンに対して、子ゾーンの公開鍵から

計算されたDS（Delegation Signer）レコードを登録する※1のですが、各RIRの管理するネームサーバに、どのくらいDSレコードが存在するのか調査を行いました。

なおDNSの運用上は、冗長性のために一つのゾーンに、複数のネームサーバおよび複数のDSレコードを登録することができるのですが、今回の調査においては、あるゾーンに対して一つ以上のDSレコードが登録されているものがあった場合、1件としてカウントを行いました。

例：APNICのゾーン（28.12.202.in-addr.arpa.）の場合	
28.12.202.in-addr.arpa. NS	cumin.apnic.net.
28.12.202.in-addr.arpa. NS	tinnie.apnic.net.
28.12.202.in-addr.arpa. NS	tinnie.arin.net.
28.12.202.in-addr.arpa. DS	38468 5 1（ 0D9C9BFFBBD1BF43022BA374B2CE623470B33565 ）
28.12.202.in-addr.arpa. DS	38468 5 2（ 85AA2B48F1C2B7556337FF019EC1C420F699599E310FE619E1D7BD78F3209189 ）

この場合、28.12.202.in-addr.arpa. というゾーンに対して、三つのネームサーバ、二つのDSレコードが登録されていますが、このゾーンについては、DNSSECが有効になっているゾーンが1件ある、としてカウントしました。

なおAFRINICにおいては、逆引きDNSSECの利用状況について、公開されている情報はあったのですが※2、APNIC 38ミーティングの時点では公開情報が最新のものではなかったので、個別に照会しました。LACNICは、他のRIRのようにはDNSSEC適用ゾーンの情報を公開しておらず、こちらも個別に問い合わせました。

◆ 各RIRにおける逆引きDNSSECの登録状況

このように調べた結果、APNICの場合は405,818のゾーンに対して、それぞれDSレコードが一つ以上登録されているものが184件、ARINの場合は486,403のゾーンに対して457件、RIPEの場合は667,460のゾーンに対して1,254件、AFRINICの場合は28,188のゾーンに対して20件のDSレコードがある、ということがわかりました。LACNICについては件数の分母が不明であるものの、およそ4～5個のゾーンでDNSSECが有効になっている旨の回答がありました。

また、組織数単位についても可能な範囲で確認したところ、APNICの管理下では16組織が逆引きDNSSECを登録しており、ARINの管理下では91の組織が登録しているということでした。RIPEについては確認できなかったため、組織数単位での登録数は不明です。

なお、1ゾーンあたりどのくらいの数のDSレコードの登録があるのかについても、可能な範囲で確認しました。DSレコードは冗長性のため複数登録することが想定されており、同じ鍵についても、ダイジェストを生成する方式についてSHA-1かSHA-256かの二つの方式があります。

APNICの個別のゾーンを確認したところ、APNIC管理下では最大で二つのDSレコードが登録されており、それぞれダイジェストの型において、SHA-1かSHA-256かが異なっていることがわかりました。また、AFRINICにおいては、多い場合は1ゾーンに四つのDSレコードが登録されている傾向があり、四つの内訳としては、二つの異なる鍵について、それぞれ二つのダイジェストの型で登録されているようでした。

◆ DNSSECの検証を有効にしたクエリの統計

APNICに、その他DNSSECに関する統計調査を実施しているか確認したところ、以前から継続して調査を実施しており、対外的に発表することもあるとのことでした。ちょうどAPNIC 38でのAPOPS（Asia Pacific OperatorS Forum）で、Geoff Huston氏が関連の発表※3を実施しており、それによると、APNICの調査対象のサーバに対して、11.5%のクライアントがDNSSECの検証を有効にして、DNSのクエリを送信している統計があるとの共有がありました。

◆ 逆引きDNSSEC登録におけるJPNICおよびAPNICのシステムの連携方式

また、JPNIC管理下におけるIPアドレスの逆引きについて、DNSSECを有効化する場合のJPNICおよびAPNICのシステムの連携方式も、詳細を確認しました。JPNIC管理下のIPアドレスには、(1) APNICのネームサーバがゾーンの委任を行っているものと、(2) JPNICのネームサーバがゾーンの委任を行っているものという、2種類のゾーンがあるのですが、(1) の場合については、ユーザーから登録申請のあったDSレコードを、そのままJPNICがAPNIC連携用のシステムに渡せば、APNICのネームサーバにて署名をすることが可能であることを確認しました。なお、(2) の場合については、JPNICのネームサーバ上で署名を行う必要があるのですが、こちらは別途、実装の方式を検討しています。

これらの検討の状況等につきましては、適宜、皆さまとも共有していきたいと考えています。

（JPNIC 技術部 澁谷晃）

※1 インターネット10分講座「DNSSEC」
https://www.nic.ad.jp/ja/newsletter/No43/0800.html

※2 AFRINICのDNSSECに関する統計
http://www.afrinic.net/en/initiatives/dnssec/dnssec-stats
（注:本稿執筆時点では、2014年9月16日のデータとして公開されている統計があり、筆者からの照会と前後して更新されたものと思われます）

※3 Geoff Huston（APNIC） - DNSSEC validation: What if everyone did it?
https://conference.apnic.net/data/38/2014-09-16-dns-measure_1410315749.pdf

RPKIの動向

本稿では、APNIC 38カンファレンスへの参加を通じて把握することができた、アジア太平洋地域におけるリソースPKI（Resource Public-Key Infrastructure; RPKI）提供の状況についてご報告します。

◆ RPKIとは

RPKI※1は、インターネットのルーティングセキュリティ技術で、IPアドレスの記載された電子証明書（以下、リソース証明書）と、AS番号が記載されたROA（Route Origin Authorization）と呼ばれる電子署名の付いたデータを使って、不正な経路情報を検出できる技術です。

このRPKIは、JPNICとインターネットマルチフィード株式会社により、2014年10月1日から試験提供が開始された「ROAパブリックキャッシュ情報の配信」においても用いられています。BGP（Border Gateway Protocol）ルータの運用者は、ROAキャッシュサーバに蓄積されているROAを参照することにより、誤った経路情報を自動で判別できるようになります。ROAとRPKIを利用した経路制御の導入が進められることにより、誤った経路情報からインターネットをより強固に守ることができるようになると考えられています。

◆ NIRにおけるRPKIへの取り組み状況

APNICでは、APNICから直接IPアドレスの分配を受けているAPNICメンバーに対して、既にリソース証明書が発行できるようになっています。IPアドレスに関するWeb申請システムである"MyAPNIC"では、IPアドレスの分配を受けたAPNICメンバーがWeb上でROAを作成する機能の他に、ROAの作成などを自組織のサーバで行うことができる下位認証局を接続する機能も提供されています。※2

一方、国別インターネットレジストリ（National Internet Registry; NIR）からIPアドレスの割り振りを受けている、アジア太平洋地域のISP事業者は、リソース証明書の発行を受けることはまだできません。RPKIは技術的に、IPアドレスやAS番号の分配を行うレジストリが、分配先に対してリソース証明書を発行する必要があるからです。NIRの中で、JPNICも含め、RPKIのサービスを提供しているところはまだありません。

APNIC 38の期間中に情報交換を通じて見えてきたことは、CNNIC（China Internet Network Information Center）やVNNIC（Vietnam Internet Network Information Center）、IRINN（Indian Registry for Internet Names and Numbers）は、RPKIに関心を示してはいるものの、まだ実験提供には至っておらず、KRNIC（Korea Network Information Center）やTWNIC（Taiwan Network Information Center）は、実験的な提供を通じて動向を把握している状態だということです。

KRNICは、前々回のAPNIC 36カンファレンスのNIR SIGで、RPKI実験環境を整えたことを発表していましたが※3、"本番提供にはまだ遠い"というのが担当者の見解でした。

◆ JPNICにおけるRPKIへの取り組み状況の報告

JPNICからは、NIRのミーティングであるNIR SIGと、NIRのホストマスターの会合であるNIRホスト・マスターで、RPKIシステムの開発状況を報告しました。JPNICで取り組んでいる開発の特徴は、以下の3点です。

1. RPKI Toolsの日本語対応（多言語対応）
2. Web申請システムとRPKIシステムの認証連携
3. レジストリデータベースとRPKIシステムのデータ連携

RPKIの適用箇所として、ルートサーバが有効かどうかという質問が挙がった他、後日に「言語の種類が多いアジア太平洋地域における、RPKIの導入に資する開発であり、RPKI Toolsにフィードバックすべきだ」といったコメントをいただきました。

◇ IPアドレスの移転とRPKIの業務手順

今後、異なるNIR間でもIPアドレスの移転が行われる可能性があることを考えると、RPKIを提供するNIRにおいては、IPアドレスやAS番号の移転に技術的に対応できるようにしておくことが必要になってくると考えられます。RPKIの仕様策定を行っているIETF SIDR（Secure Inter-Domain Routing）WGでは、移転の際に、どのような手順でリソース証明書を更新していくべきかの議論が行われています。この議論では、移転手続きの途中においても、アドレスが証明された状態を途切れさせないようにすることが前提となっています。

しかし、移転時にリソース証明書をどのように扱うのかという、業務手順はまだ整理されておらず、筆者とAPNICのRPKI担当者とでも相談を行っています。アジア太平洋地域にはNIRが存在するため、RIRのみの場合よりも手順が複雑になることが

※1 リソースPKI（RPKI）
https://www.nic.ad.jp/ja/rpki/

※2 Resource Certification - Guide to Resource Certification in MyAPNIC
http://www.apnic.net/__data/assets/pdf_file/0015/52602/ResCertGuide.pdf

※3 JPNICニュースレター No.55「APNIC 36カンファレンス報告 - RPKIの動向報告」
https://www.nic.ad.jp/ja/newsletter/No55/0692.html

想定されます。

大まかなアドレスの移転とリソース証明書更新の手順は、以下のようになると考えられています。

1. 当事者間での移転の合意
2. 移転先のリソース証明書の再発行（移転後のアドレスを含める）
3. 移転元のリソース証明書の再発行（移転前のアドレスを削除する）

2と3の期間中、同じIPアドレスが二つのリソース証明書に記載された状態になるのが特徴です。これによって、移転するIPアドレスの有効性を保ち、リソースPKIが使われたBGPルーティングに影響が出ないようにできると考えられています。

もう一つの検討課題として考えられていることは、移転の業務手順です。移転がAPNICメンバーと、NIRの下に存在するLIR（Local Internet Registry、JPNICの場合はIPアドレス管理指定事業者など）との間で行われる場合には、2の前や3の後に、NIRのリソース証明書を再発行する手順が入ってきます。証明書の再発行と共にタイミングを合わせるために、APNICやNIR同士の連絡が重要になってくるかもしれません。

今後、アドレスポリシーの上で移転を行うことができるNIRと情報交換を行って、実施可能で証明書の利用者が困らないような業務手順を探っていく必要があると考えられます。

（JPNIC 技術部／インターネット推進部 木村泰司）

● NIR SIGでは、筆者からJPNICにおけるRPKIに関する活動を紹介しました

ARIN 34ミーティング報告

2014年10月9日（木）と10日（金）の2日間、米国のメリーランド州ボルチモアにて、ARIN 34ミーティングが開催されました。本稿では、このミーティングの模様をご紹介します。

◆ 今回のARINミーティング

今回のARIN（American Registry for Internet Numbers）会議は、秋に開催される会議の通例として、NANOG（The North American Network Operators' Group）ミーティングとの併催でした。今回は、アドレスポリシーに関する議論に加え、IANA（Internet Assigned Numbers Authority）機能の監督権限移管に向けた、ARIN地域としての提案に関する議論が行われたことが、大きな特徴です。

P.2からの特集1で詳しく取り上げていますが、「番号資源」に関わる監督権限移管の提案は、各地域インターネットレジストリ（RIR; Regional Internet Registry）で議論された提案をグローバルに一つにまとめたものを、2015年1月に提出することが求められています。すなわち、APNIC（Asia Pacific Network Information Centre）地域で議論した内容が他のRIR地域と異なる場合は、APNIC地域内での再調整が必要となります。そこで筆者は、ARIN 34の1ヶ月前に、APNIC 38にてAPNIC地域として議論した移管提案と比較する視点で、本会議におけるARIN地域の議論に着目していました。

アドレスポリシーについては、10点の提案が議論された中、「日本も含めたAPNIC地域でも検討すべきか」という視点で着目しておきたい議論としては、「IPv4アドレス移転要件の見直し」と「ARIN地域外でのIPv4の利用」の2点が挙げられます。

特に前者の「IPv4アドレス移転要件の見直し」は、アドレスの必要性を確認する要件を緩和する方向に進めるものであり、これまでのARINコミュニティの姿勢と大きく異なります。APNIC地域における要件も、これに合わせて見直すべきかということを検討するための材料として、今後も注視すべきかと思います。

今回の報告では、IANA機能の監督権限移管の議論も含めた、これら3点に絞ってご報告します。

◆ IPv4アドレス移転要件の見直し

今回の会議では、移転するIPv4アドレスに対して、移転先での必要性を確認した上で、移転を承認する要件を緩和する方向に議論が進められていました。これは、数年前にARIN地域で移転ポリシーを施行した際に、必要性の確認を行わないことが投機目的のアドレス売買につながると消極的であった、当時のARIN地域の姿勢と比べると、かなり大きな変化が見て取れます。

◇ 会場の反応
今回の会議では、移転アドレスの必要性を確認する要件の緩和を求める提案が、複数提出されていました。提案内容からはその背景は明らかではありませんが、移転が想定に基づくものであった移転ポリシー施行時とは異なり、IPv4アドレスの在庫枯渇が進み、実際に移転が行われている現状においては、要件を緩和した方が実態に合っていると考える人が増えてきているようにも思えます。そうは言っても、全体としては、慎重派の意見が目立ち、一度にすべてのサイズの移転において要件を撤廃するのではなく、小さなサイズから要件緩和をして様子を見ようとする意見が表明されていました。

結果として、今回の会議では合意に至らずに、継続議論となりましたが、要件緩和自体に懸念を示す意見は少なく、必要性の確認対象とすべき移転サイズについて意見が分かれたことが、コンセンサスとならなかった主な要因と言えそうです。

◇ APNIC地域からの視点
APNIC地域では、ポリシー施行当初は、需要確認の要件がなかったものの、ARIN地域とのRIR間移転を実現するために、需要確認の要件を追加した経緯があります。

これを踏まえて、今後ARIN地域の要件が緩和された場合、APNIC地域としては「ARINに合わせて要件緩和をしたい」のか、「現状の要件を残す」のか、コミュニティの意思と方針を整理していく必要性が出てきます。

◆ ARIN地域外でのアドレスの利用

「ARIN地域外でのアドレスの利用」は文字通り、ARINから分配を受けたIPv4アドレスの、ARIN地域外での利用を認めることを、ポリシー上、明確にすることを求めたものです。この提案も、IPv4アドレス在庫枯渇に伴い、実体化している課題への対応を目指しています。ただし、ARINから分配を受けたアドレスの一部は、ARIN地域内で利用することが前提となります。

◇ 解決したい課題
・現在のアドレスポリシーでは、ARINから分配を受けたIPv4アドレスの利用をARIN地域内に限定するべきか、他の地域でも利用できるのか、明確ではない
・一方、他のRIR地域での在庫枯渇が進む中、複数のRIR地域に拠点を持つ企業からは、ARINから分配を受けたアドレスを、他の地域でも利用できるようにしたいとのニーズも確認されている

◇ 会場の反応
会場では、Microsoft社やGoogle社などの企業の参加者から、「既にそういう使い方をしている」との意見が複数表明されました。一方、FBI（米国連邦捜査局）などの法執行機関からの参加者は、アドレス利用者の実態がつかめなくなり、連絡が取れなくなるとして懸念を示しており、継続議論となりました。

◇ APNIC地域からの視点
APNIC地域内でも、このようなケースは考えられると同時に、申請者が所在地外のRIRを自由に選択できると解釈する余地を与えかねない、といったことなども考えられることから、どこまでをアドレスポリシーで明文化するべきか、バランスを踏まえて考慮することが大切なように思います。

◆ IANA機能の監督権限移管に向けた議論

2014年9月に開催されたAPNIC地域でのAPNIC 38での議論に続き、ARIN 34では、ARIN地域としての提案策定に向けた議論を行いました。

◇ 今回の議論とARIN地域の現状
会議では、提案すべき内容に踏み込んだ議論は行わず、背景と現状の報告、ARIN地域としての提案策定に向けたプロセス案を紹介し、プロセスとして適切であるかについて議論を行いました。ARIN地域では、IANA機能の現状と今後に関する調査を実施し、コミュニティの意向を確認した上で、提案の策定を進めるとし、ARIN 34の後に、実施した調査の結果が公開されています。

IANA Stewardship Transition - ARIN Community Input
https://www.arin.net/participate/governance/iana_survey.pdf

◇ 他のRIRとの比較
他のRIR地域では、調査という形を取らず、具体的な提案をもとに各コミュニティの意思確認が進められています。なお、ARIN地域における調査結果の中で、印象に残ったものとしては、NTIAに代わりIANA機能の監督を行う第三者機関の設立を支持する意見が、過半数となっていた点でした。これは、APNIC地域で議論した提案には含まれていない要素です。

◇ 今後
この調査結果を踏まえて、ARIN地域として、どういう提案を策定するのか検討が行われます。その後全RIR地域における議論を経て、CRISP（The Consolidated RIR IANA Stewardship Proposal）Teamが各RIRコミュニティの意向を尊重しながら内容をすり

合わせ、番号資源として一つの提案にまとめられます。

◆ ARIN 34とNANOG 62に参加して

ARINは、オペレーターによる議論の参加も促進しており、NANOG会議のセッションの中で、ARIN 34で議論するアドレスポリシー提案を、NANOGの参加者と議論する形式をとっています。NANOG 62では、それ以外にも、政策に関わるテーマを扱ったプログラムとして、ネット中立性へのFCC（米国連邦通信委員会）法案検討に向けたFCC担当者による発表や、ICANN会議へオペレーターの参加を呼びかけるセッションなど、「運用」を軸としながらも、技術的な枠にとらわれない内容が見受けられました。

一方、NANOGが終わりARIN会議が始まると、約3分の2の参加者が去る現状を目の当たりにすると、もともと政策的な話に興味がある人以外に、ポリシー策定に関わってもらおうとすることは、なかなかのチャレンジであることが感じ取れます。

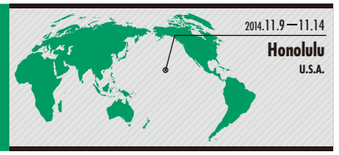
ARIN会議単体で見た場合、APNIC地域と比較するとポリシー提案の数も多く、提案への議論が活発に行われていますが、参加者の1人が「数は多いが、特筆すべき議論は、移転における必要性確認要件の撤廃に関する議論くらい」との感想を述べていたことも印象的で、議論が活発なのがよいと一概には言えないのかもしれません。

参考：
・ARIN 34ミーティングプログラム
https://www.arin.net/participate/meetings/reports/ARIN_34/ppm.html

・ARIN地域における提案一覧
https://www.arin.net/policy/proposals/

（JPNIC インターネット推進部/IP事業部 奥谷泉）

第91回IETF報告



全体会議報告

第91回IETF Meetingは、2014年11月9日（日）から11月14日（金）の間、ハワイのホノルルにあるヒルトン・ハワイアン・ビレッジにて、米シスコ・システムズ社のホストで開催されました。本稿では、そのレポートをご紹介します。

◆ はじめに

ちょうど四半世紀ぶりに、第15回IETF以来のIETF Meetingがハワイにて開催されました。ハワイは、イーサネットの礎と言えるALOHAnet発祥の地で、インターネット史において大変縁のある場所で、IETF Meetingも比較的早期にこの地で開催されていました。1989年当時のIETF Tシャツには、1987年に上映された映画「Revenge of the Nerds 2」の副題「Nerds in Paradise」の文字がプリントされていたそうです。このTシャツは数あるIETF Tシャツの中でもコアなファンがいる大変人気の1枚のようで、なんと今回は公式IETF Tシャツとは別に、一部の有志によって当時と同様のピンクのボディに「Nerds in Paradise 2.0」の文字をプリントし、現代版としてアレンジを加えて、もう一つの公式IETF Tシャツとして復刻されました。

先に「もう一つのTシャツ」を取り上げてしまいましたが、今回の公式IETF Tシャツは米シスコ・システムズ社のロゴが入ったIETFオリジナルデザインのアロハシャツでした。意図して作られたものであるかは定かではありませんが、服好きの著者としては、米シスコ・システムズ社のアロハシャツとはずいぶんこちらも洒落を効かせた一着だなぁと思わず感心してしまいました。というのも、会場となったヒルトン・ハワイアン・ビレッジの敷地内のビーチの名前にもなっていたハワイの英雄デューク・カハナモク、彼がデザインしたアロハシャツを販売していた企業の一つが、今は無きシスコ・カジュアルズ社なのです。彼の名を冠したアロハシャツは、アカデミー賞にて数々の賞を獲得した映画「地上より永遠に」の劇中で、主演のモンゴメリー・クリフトをはじめとする出演者等が着用し注目を集め、それまでローカルな位置づけであったハワイアンファッションを米国本土ではやらせるきっかけとなった歴史的なブランドです。そんな現在においてもヴィンテージとして大変人気が高い、伝説的なブランドを持つアロハシャツメーカーと同名の「シスコ社」がアロハシャツを作った!という、こちらもまた歴史的な一着でした。

さて、ここからは11月12日（水）に開かれた「IETF Operation and Administration Plenary」と、11月10日（月）の「Technical Plenary」の様子について、簡単にご報告します。

◆ IETF Operation and Administration Plenary

11月12日（水）の「IETF Operation and Administration Plenary」では、ホストのシスコ社の挨拶から始まり、IETFチェア、IAOC（IETF Administrative Oversight Committee）チェアとIAD（IETF Administrative Director）、IETFトラストチェア、NomComチェアからの報告、IAOCオープンマイク、IESG（Internet Engineering Steering Group）オープンマイクという流れで議事進行されました。

IETFチェアレポートでは、IETFチェアのJari Arkko氏より、参加者の内訳や新しい取り組みの報告がありました。第91回の参加者は、50の国と地域から1,080人の参加となり、前回の1,175人から95人ほど減少しています。また、昨年の同時期にバンクーバーにて開催された第88回の1,189人や、その他1,200人前後で推移してきた近年の参加者数と比較すると100名程度減ったことがわかります。新規参加者は136人と、全体の1割強は新規参加者で、新しい層の取り込みは継続的に進んでいるようです。国別の参加者数は、1位米国、2位中国、3位日本、4位カナダとなっており、参加者全体の約半数を米国、約7割を上位4ヶ国が占める割合となっておりました。また、近年中国からの参加者の増加に伴い、ビザの発行に関する諸問題が増えてきており、IETFとしても改善に向けた検討が続けられるとの報告がありました。

続いて、今年の9月および10月に試験的に行われた、IESGのテレチャットを公開する取り組みについて報告がありました。この取り組みは、IESGの公平性を保つことを目的として、IETF参加者もオブザーバーとしてテレチャットに参加できるように実施したとのことでした。また、今後も知見の収集のためにテレチャットの公開を継続するとの報告がありました。

また、2015年夏頃を目処に現在ある八つのIETFエリア（応用分野（APP）、インターネット分野（INT）、運用管理分野（OPS）、リアルタイム応用・基盤分野（RAI）、ルーティング分野（RTG）、セキュリティ分野（SEC）、トランスポート分野（TSV）、その他分野（GEN））の再編をIESGが進めているとの報告がありました。このエリア再編の目的には、新たなWGのサポート体制の整備や、エリアディレクターの人数の調整などがあげられました。また一方で、IESGでは、この再編に伴い影響を受ける可能性のあるAPPエリアやRAIエリアについては、エリアを統合するなどして今後も応用分野に関する活動を継続していくことを検討していると報告がありました。

今回のRecognitionでは、中南米からのIETFへの参加者増加に貢献したAlvaro Retana氏、IETF Datatrackerの改善に貢献したLars Eggert氏、20年以上にわたりインターネットおよびIETFに貢献してきたBert Wijnen氏等3名が紹介されました。また、Bert Wijnen氏は、スピーチの際に氏の十八番であるオランダ語による歌を披露し、参加者から拍手喝采を浴びていました。

IAOC・IADチェアレポートでは、IAOCチェアのChris Griffiths氏およびIADのRay Pelletier氏より報告がありました。今回の会議の収支決済速報では、参加者数は予測の1,200人より少なく、参加費およびスポンサー費の合計は150,000ドルの赤字であることが報告されました。そのため、今回のBits-N-Bitesもスケジュールされないことがあらためて伝えられました。一方で、トロントで行われた、第90回の収支決算の最終報告では、参加者数は予測を超え、参加費およびスポンサー費ともに収支見通しを上回り、192,349ドルの収益があったとのことでした。また、これまでのIETF継続に伴う純利益は640,000ドルとなったとのことでした。

IETFチェアレポートでも触れられた、ビザの発行に関する諸問題についての今後の対策については、検討を続けるとともに、必要な参加者へ会議参加を証明するための招待状を発行するなどの方針について報告がありました。また、IAOCではこの問題に対して十分な理解があるため、問題が生じた際はぜひ連絡を取ってほしいと述べられていました。

また、第95回IETF Meetingおよび第98回IETF Meetingの開催地が決定したとの報告がありました。第95回はIETF史上初となる南米で、アルゼンチン・ブエノスアイレスにて開催されることが決まりました。また第98回は、カナダ・モントリオールにて開催されることが決まりました。

最後に、各スポンサーの紹介がありました。ホストのシスコ社の他に、Welcome ReceptionをスポンサーしたNBCユニバーサル社、回線提供をしたタイム・ワーナー・ケーブル社、そして、休憩時の飲食物を提供した各社が紹介されました。会期初日の日曜日に開催されたWelcome Receptionでは、スポンサーがNBCユニバーサル社であったこともあり、参加者にはミニオンのぬいぐるみが配られ、一部の参加者は至る所（自室やビーチ、ターミナルルームなど）で、このミニオンを撮影し、参加者のメーリングリストに投稿することが会期中はもとより会期後もしばらくはやっておりました。


● IETF Operation and Administration Plenaryの様子

◆ Technical Plenary

11月10日（月）の「Technical Plenary」では、IAB（Internet Architecture Board）チェア、IRTF（Internet Research Task Force）チェア、RSE（RFC Series Editor）・RSOC（RFC Series Oversight Committee）チェアからの報告、ITU（International Telecommunication Union）Plenipotentiary Conferenceの報告、IABに関する問題の報告が二つ、IABオープンマイクという流れで議事進行がされました。

はじめにIABチェアのRuss Housley氏より、第90回IETF Meetingからのハイライトについて紹介がありました。まず、IRTFチェアにLars Eggert氏が、ISE（Independent Submission Editor）にNevil Brownlee氏が、それぞれ再任したことが紹介されました。続いて、IABが執筆したRFCとして、RFC7322「RFC Style Guide」が発行されたことが紹介されました。最後に、2015年のICANN NomComメンバーとして、John Levine氏が選ばれたことが紹介されました。

IRTFチェアのLars Eggert氏からは、次のような報告がありました。今回のIETF Meetingの期間中に開催されるIRTF Meetingは、八つあるResearch Group（RG）のうち、以下の四つのRGでした。

- Software-Defined Networking（SDNRG）
- Information-Centric Networking（ICNRG）
- Internet Congestion Control（ICCRG）
- Network Management（NMRG）

また、提案中のRGとして、Datacenter Latency Control（DCLCRG）およびNetwork Function Virtualization（NFVRG）がありました。第90回以降にIRTF関係として発行されたRFCは、今回はないとのことでした。

最後に、Applied Networking Research Prizeの紹介がされました。2014年は過去最多となる46人の推薦者の中から、Sharon Goldberg氏、Misbah Uddin氏、Tobias Flach氏、Robert Lychev氏、Kenny Paterson氏、Keith Winstein氏の6名が受賞しました。

RSE・RSOCチェアからの報告では、Heather Flanagan氏より、RFC formatの改訂作業の進捗としてdraft-flanagan-rfc-frameworkの紹介があり、新たなRFC formatの作業は順調に進んでいる旨の報告がありました。また、その機能として、図表の挿入をできるようにするとの紹介があり、猫の絵を例にあげて、従来のASCIIアートによる表現からSVGファイルによる表現が可能となる点を紹介し、参加者にこの機能を使ってみたいか問いかけがあり、多くの参加者が挙手をしていました。

Sally Wentworth氏からは、ITU Plenipotentiary Conferenceについて報告がありました。これは、ITUの最高意思決定機関として4年に1度開催されます。2014年は開催年にあたり、10月20日から11月7日の期間に開催されました。インターネット関連の議論ではITUがスコープとする、プライバシーや監視、人権、インターネットガバナンスとそれに関する政策などの諸問題を中心に話し合いがされましたが、これらインターネットの運用に関する諸問題についてはITUの条約やその定義の変更、範囲の拡大には至らなかったとの報告がありました。また、この結論は投票ではなく、参加者の合意形成により導かれたとのことでした。

IABに関する問題として、以下の二つについて報告がありました。

・IP Stack Evolution
Joe Hildebrand氏より、IPv4とIPv6が共存し進化し続ける今日において、このような共存環境がトランスポート層において、さまざまな影響を引き起こす可能性について説明がありました。そして、この問題に関連するWGとしてTransport Services（TAPS）WG、TCP Increased Security（TCPINC）WG、Advanced Queue Management（AQM）WGやその他のAPPエリアの紹介がありました。また、2015年の1月26日から27日の期間でIAB Workshop on Stack Evolution in a Middlebox Internet（SEMI）を行い、その結果を次回IETF Meetingにて発表するとの報告がありました。

・Privacy and Security
Ted Hardie氏より、プライバシーとセキュリティに関する諸問題について、現在IABではInternet Scale Resilience、Confidentiality、Trustの三つのエリアに分類を行ったところで、今後この三つのエリアごとにプライバシーとセキュリティに関する諸問題について取り組んでいくと説明がありました。

（青山学院大学 情報メディアセンター 根本貴弘）

IPv6関連WG報告

本稿では、第91回IETFにおけるIPv6関連のWGについて、6man WG、v6ops WG、6lo WG、Homenet WGの議論を中心に報告します。

◆ 6man WG（IPv6 Maintenance, Int Area）

6man WGのワーキンググループでは、IPv6プロトコルの基本仕様そのものについてのメンテナンス（見直しや拡張）を議論しています。

ワーキンググループ文書として議論進行中のもの（Working Group Draft）のうち、二つに関して取り上げられました。すでにこのWGで取り上げられている個人文書（Individual Draft）七つについて継続議論があり、今回初めて投稿された文書（new Individual Draft）五つについての発表が予定されていましたが、Atomic Fragmentやv6GEOといった最初の提案で時間がかかってしまい、新しく投稿された5文書については、時間切れで議論されませんでした。

本稿では、議論のあった中からいくつかを取り上げます。なお、今回問題提起された、個人文書の一つ「Deprecating the Generation of IPv6 Atomic Fragments」が会期後、WGドキュメントに「昇格」しました。

1. Efficient ND Design Team報告
前々回のミーティングでも議論された「Efficient ND」は、第89回IETF報告で「無線LAN環境での近隣探索プロトコル（ND）の問題についての議論」として解説された問題点※の改善策を検討するものです。今回、デザインチームが発足し、まとまった報告がされました。

プロトコルに手を入れるにしろ、環境にあったオプションの運用を提示するにしろ、まずは問題分析をきちんとするところから出発しているようです。そのため、このデザインチームのカバー範囲は、近隣探索プロトコルのトラフィック計測から機能ごとの問題分析、問題改善として使えそうなテクニックやオプションの検討と広範囲になっています。6man WG単体ではなく、v6ops WGと共同での検討事項となっています。

問題フィールド特定のための計測結果は、マルチキャスト通信の影響やバッテリへのインパクトについてまとめた二つの文書として書き起こされています。

- draft-vyncke-6man-mcast-not-efficient
- draft-desmouceaux-ipv6-mcast-wifi-powerusage

また、重複検出（DAD）については、別の文書に課題整理がされています。

- draft-yourtchenko-6man-dad-issues

マルチキャストのRS（ルータ探索）と定期的なRA（ルータ広告）、リンクアドレス解決のためのNS（近隣者発見）とNA（近隣者要請）、DAD、Wi-Fiと携帯電話網の混在環境、軽量端末などの端末側のパケット送出特性、mDNS（マルチキャストDNS）のトラフィックボリュームなどが改善対象として選ばれていました。デザインチームからは、主にRS/RAとDADの改良点として、RAの送出に関してタイマーを設けて間隔を長くできるようにすることや、RAにリフレッシュオプションを設けること、DADに関しては手動設定の場合にのみ実施することやさらに手を加える道など四つのアプローチが提示され、議論がされました。レビュー対象の文書は、次の三つとなっています。

- draft-yourtchenko-6man-dad-issues
- draft-krishnan-6man-maxra
- draft-nordmark-6man-rs-refresh

参加者からはデザインチームの活動報告に賛同するコメントが得られ、引き続きデザインチームによる検討が継続されます。

2. Recommendation on Stable IPv6 Interface Identifiers（draft-ietf-6man-default-iids）
セキュリティとプライバシーへの配慮のため、MACアドレス由来のインタフェースID（IID）からRFC7217で定義されている隠ぺいされたIIDの適用を促す文書です。これが必須のものとして採用されると、主にIPv6をトンネルで運搬する技術の実装に影響が出ます。セキュリティとプライバシーは守るべきですが、運用上は特定ができると都合が良い場合もあるなど、柔軟性を求める声もあり慎重な議論がされていました。これも継続議論となっています。

余談ですが、この議論の途中で使われた“ambiguous”という単語がなぜかはやり出し、IPv6系の人が集まるWGやBoFのそこかしこで使われていました。

3. Deprecating the Generation of IPv6 Atomic Fragments（draft-gont-6man-deprecate-atomfrag-generation）
IPv4ノードとIPv6ノードがSIIT（Stateless IP/ICMP Translation Algorithm）を使って通信している際の、IPv6のAtomic Fragmentについてです。問題指摘と廃止の提案については、現状の運用観測に基づいたものですが、実装側や運用を正すべきであるといった意見や、Atomic Fragmentを必要とするMANET（Mobile Ad hoc NETwork）の例などがあげられ、簡単に廃止できるものではないことから、コンセンサスには至らず、継続議論となりました。

4. Including Geolocation Information in IPv6 Packet Headers（IPv6 GEO）（draft-skeen-6man-ipv6geo）
データリンクに使われるプロトコルは多種多様で、必ずしも位置情報を含むように作られていませんが、その上位レイヤのIPは共通利用されています。そこで、IPv6ヘッダに位置情報を含めるようにしようという提案です。位置情報についてもプライバシーへの配慮が必要であるため、これを利用する際には暗号化を必須とするべきであるといった意見が寄せられ、この提案も継続議論となっています。

※ JPNICニュースレター No.57「第89回IETF報告 IPv6関連WG報告」
https://www.nic.ad.jp/ja/newsletter/No57/0650.html

◆ v6ops WG（IPv6 Operations、OPs & Mgmt Area）

v6ops WGでは、文字通り、IPv6ネットワークの運用管理に関する事項やIPv4ネットワークへの導入、共存技術など幅広い事項を扱っています。今回も午前と午後に二つのセッション枠が確保され、6to4の廃止、ULAの利用考察、マルチプリフィクスの運用ガイド、拡張ヘッダの利用状況調査、DNS64/NAT64環境で利便性を高めるための専用TLDの提案など、さまざまな提案や報告がされました。

なかでも、6to4プロトコルの廃止については、運用被害を防ぐ方向で議論が白熱しています。運用サイドの意見を取り入れるため、チェアからNANOGなどの運用者向けメーリングリストにも議事録が共有され、意見が募られました。

1. Deprecating Connection of IPv6 Domains via IPv4 Clouds（6to4）（draft-ietf-v6ops-6to4-to-historic）

IPv4上でIPv6の通信を行えるようにする6to4技術について、そろそろ役目を終えて廃止にする時期なのではという提案です。Windows OSなどで参照されるアドレスポリシーテーブルでも、Teredoには規定があるが6to4はなくなっているという指摘を受けて、Teredoも廃止してもいいのではという意見も出たりしていました。

アドレスポリシーテーブルでは、6to4はNativeのIPv6より優先度を下げるといった評価のための参照がされているため、テーブルから削除すると問題が起きるだろうという指摘や、6to4のために予約されているアドレス（192.88.99.0/24）をフィルタすれば廃止と同じ意味合いとなるといった意見があり、

（1）6to4の廃止
（2）RFC3068（6to4リレールータのためのエニーキャストプリフィクス）をhistoricステータスにする
（3）192.88.99.0/24をフィルタする

という三つの内容に分割して、それぞれ議論することになりました。

2. IPv6 Extension Headers in the Real World（draft-gont-v6ops-ipv6-ehs-in-real-world）

IPv6の拡張ヘッダは、フィルタされて運用に支障をきたす場合が見られます。SI6 Tool Kitの作者である本文書の筆者は、このツールを用いてパブリックなインターネットにおけるIPv6拡張ヘッダの扱い、フィルタ状況について調査を実施し、まとめました。拡張ヘッダの種類ごとの状況はなかなか興味深いものがあります。調査方法とその結果について、質疑がたくさんありました。

最終的には、実装と運用のガイドとなる文書作成をめざしているようですが、ガイドラインの作成には、実装に関する部分があたかも第2の拡張ヘッダの提案をしているように見受けられる部分があるなど問題があるため、待ったがかけられ、調査結果部分を一つの文書として分離してまとめることになりました。

ICMPv6の安易なフィルタも同様ですが、フィルタすることによってブラックホールとなるといった、どういう問題が起きるかを本文書で確認しておくと、健全な運用のイメージがわいて良いのではないかと思います。

3. Design Choices for IPv6 Networks（draft-ietf-v6ops-design-choices）

IPv4とIPv6のdual-stackネットワークやIPv6 onlyのネットワーク構築時の、「デザインチョイス」についてのガイドライン文書です。外部接続や経路制御の手法選択がメインであるため、現在のもっと広範な設計を予想させるようなタイトルから、範囲を絞ったもっとわかりやすいタイトルに変更した方がいいという指摘が出ていました。

その一方で、DHCPやSLAAC（StateLess Address AutoConfiguration）など内部の運用術に関して扱った方が良いという「広範」をめざすべきという意見も出ていました。また、いずれにしてもセキュリティに関してはしっかり書いておくべきだろうといった意見もあり、引き続き内容を厚くしていくことになりました。

4. A Special Purpose TLD to resolve IPv4 Address Literal on DNS64/NAT64 environments（draft-osamu-v6ops-ipv4-literal-in-url）

DNS64/NAT64を運用している環境で、IPv6端末がIPv4のみのアプリケーションサーバに明示的にアクセスする場合のURLとして、「.v4」をTLDとして指定するとIPv6アドレスにIPv4アドレスをマッピングする仕組みの提案が継続議論されています。

この仕組みの有用性は多くの参加者から賛同されているようでしたが、新しいTLDを作ることに難色を示す人が多かったように思われます。代わりに、「v4only.arpa」はどうかといった提示もされていました。また、DNSSECやcookieがうまく動作しないのでは、ということも指摘されていました。指摘事項に関して文書を更新するとともに、DNSOPSでも議論するということになりました。

今回の私の参加目的として、v6opsでの発表というのがありました。15分ほど時間をもらえ、国内で実施している中小規模の組織向けルータのIPv6に関するセキュリティテストについて報告をしました。"Introducing IPv6 vulnerability test program in Japan, <draft-jpcert-ipv6vullnerability-check>"という文書名で公開されていますので、ぜひご一読いただき、コメントをいただければと思います。

◆ 6lo WG（IPv6 over Networks of Resource-constrained Nodes WG）

6lo WGでは、省電力で低電力な軽量端末が接続されるIPv6ネットワークの技術について議論をしています。

IoTという言葉の盛り上がりも見られる中、粛々と軽量クライアントのための近隣探索や、おサイフケータイなどでも使われているNFC上のIPv6パケットの転送技術などが話し合われています。こちらでも、RFC7217ベースのインタフェースIDの利用に関する議論がされました。

"IPv6 mapping to non-IP protocols"については、6man WGのチェアとも相談するようにという指示が出ていました。

◆ Homenet WG（Home Networking WG）

Homenet WGでは、最近の多種多様なデバイスとそれが属する多様な通信網を念頭においた家庭内ネットワークの接続手法や、管理手法が議論されています。

1. Routing
2. Addressing / Configuration
3. Naming
4. Service Discovery
5. Security / Border Discovery

のカテゴリが提示されており、これに従って議論が開始されましたが、最初のルーティングに関する議論だけでほぼ一つのセッション枠を使い切ってしまう事態になり、急遽空いている部屋を探して、別の日にも議論がされました。家庭内のデバイス管理のために、.homeというTLDを使う提案などもされていました。


● 初心者からの質問を受け付けることのできる言語を示すための缶バッジ

IPv6のプロトコルを基盤とした次の展開に向けた議論が多数行われていることを、あらためて感じたIETF91のオンサイトミーティングでした。

（株式会社インテック　廣海緑里）

セキュリティ関連WG報告

近年、IETFにおけるセキュリティ関連のWGは、分野が多岐にわたっています。本稿では、セキュリティエリアのWGと、セキュリティエリアの総括が行われる会合であるSAAG（Security Area Advisory Group）ミーティングから、いくつかの話題をピックアップして報告したいと思います。

◆ Transport Layer Security（TLS）v1.3の議論

TLS WGでは、SSL/TLSの次のバージョンである1.3の策定に向けて、検討が活発に行われています。前回の第90回IETFミーティングに続いて、今回もミーティング期間以外に開催されるInterim（中間）ミーティングが開かれていました。

TLS 1.3に関しては、TLSの通信を始める前の、暗号アルゴリズムを選択したり暗号化に使う鍵を決めたりする重要なやり取りである「ハンドシェイク」に議論が集まっています。v1.3のハンドシェイクの案に対して、ハンドシェイク中にやり取りされるメッセージそのものを暗号化したり、メッセージの改ざんを検知するのに役立つ電子署名を加えたりする案が挙げられています。WGミーティングでは、ハンドシェイクが通信の安全性を大きく左右するため、拙速にコンセンサスを取るのではなく、慎重に議論を進めることになりました。

またハンドシェイクを簡素化し、オーバーヘッドを少なくする0-RTTと呼ばれる方式も提案されています。議論されているハンドシェイクの候補は、次の資料で見ることができます。

TLS 1.3のハンドシェイク候補の議論に使われたスライド
http://www.ietf.org/proceedings/91/slides/slides-91-tls-2.pdf

なおSSL/TLSの圧縮機能は、BEAST（Browser Exploit Against SSL/TLS）やCRIME（Compression Ratio Info-Leak Made Easy/Compression Ratio Info-Leak Mass Exploitation）といった攻撃手法が生まれたことを背景として、TLS 1.3では盛り込まれないことになっています。

◆ I2NSF（Interface to Network Security Functions）BoF

I2NSFは、ファイアウォールやユーザー認証サーバといったネットワークセキュリティ機能を、ネットワークの仮想化機能VNF（Virtualized Network Functions）の環境内や、ホスティングの環境において、設置したり設定したりすることができるプロトコル、そしてデータモデルを検討するグループです。第91回ミーティングで1回目のBoFが開かれました。

本グループの設立に向けた意図をまとめたInternet-Draftによ

ると、近年におけるネットワーク仮想化技術の発展に伴って、以下のようなニーズが高まっているとしています。

- 複数の拠点に分かれた企業のネットワークのために必要最小限のネットワークセキュリティ機能を運用する
- クラウド型のデータセンターで稼動させながら、クライアントにネットワークセキュリティ機能を提供する
- 多数のサイトやユーザー、もしくは低電力のセンサーネットワークに対して一貫したセキュリティポリシーを適用する

これらに対して、本グループでは、仮想化環境で稼動するセキュリティ機能を"仮想ネットワークセキュリティ機能" - Virtual Security Functionと呼んで、クラウド型のデータセンターでの提供や従来の機器との共存がしやすいように標準化することを目標としています。

Interface to Network Security Functions Problem Statement
https://tools.ietf.org/html/draft-dunbar-i2nsf-problem-statement-01

I2NSF BoFには80名ほどが集まりました。IETFで行われる1回目のBoFとしては人数は多くない方ですが、アジェンダやプレゼンテーションの内容は、ある程度練られたもので、アイデア段階で開かれるBoFとは様子が違っていました。このBoFでは、WG化に向けて趣意書を作成するためというよりは、取り組む課題を明確化するために議論されていました。

本グループのInternet-Draftには、課題の明文化の他に、データセンターなどを挙げて利用ケースを説明したものがあります。まだWGではありませんが、次のページが設けられ、まとめられています。

Interface to Network Security Functions（i2nsf） - Documents
https://datatracker.ietf.org/wg/i2nsf/documents/

◆ BGPSEC – Origin ValidationとPath Validationの分離

SIDR WGは、PKI技術を使ったBGPルーティングのセキュリティの仕組みを検討しているWGです。大きな動きとして二つ挙げられます。

一つはBGPSEC（Border Gateway Protocol Security Extension）において、Origin Validation（経路情報のAS番号を確認する方式）とPath Validation（経路情報のASパス情報を確認する方式）が独立した扱いになったことです。これまではPath Validationが行われる際には、必ずOrigin Validationが行われるという位置づけでした。今後、RPKIキャッシュやBGPルータの実装において、おのおのが独立してvalid（有効である）やinvalid（無効である）という扱いに変わってくると考えられます。

もう一つは、リソース証明書やROA（Route Origin Authorization）といったデータファイルの取得に使われていたrsyncに代わるプロトコルが、本格的に検討されていることです。第91回IETFミーティング期間中に、複数のプロトタイプの実装同士を突き合わせる作業も行われていた模様です。このプロトコルは、RPKI Repository（またはRetrieval） Delta Protocol - RRDPと呼ばれています。まだ個人ドラフトですが、rsyncは処理が重く、またRTT（往復遅延時間）の大きい環境で伝送効率が下がることが分かっていることから、注目されています。

RPKI Repository Delta Protocol（Internet-Draft）
https://tools.ietf.org/html/draft-tbruijnzeels-sidr-delta-protocol

SIDR WGでは、ルーティング技術者の観点でBGPSECに関する意見収集を行う目的で、Inter-Domain Routing（IDR） WGとの合同でミーティングが開かれました。第91回IETFミーティング期間中に行われた合同ミーティングでは、BGPSECの仕組みに関する質疑応答を通じて理解が深められた様子です。長いASパスが不正に生成されることによってコンバージェンスの時間が長くなり、ルーティングに支障が出るような行為ができてしまうのではないかといった、運用の観点ならではの意見交換も行われています。

この他に、RPKIの認証局によるROAの失効に気付けるような新たな署名付きオブジェクトの提案や、不正な証明書を見つけやすくするためのCertificate Transparencyに似たアイデアが提案されていました。これらを含めて、RPKIについて活発に研究が行われている、ボストン大学の研究グループによる論文が次のURLで公開されています。

Hardening the RPKI Against Faulty or Misbehaving Authorities, BUSEC: Boston University Security Group
http://www.cs.bu.edu/~goldbe/papers/RPKImanip.html


● 今回のSIDR WGのミーティングは、IDR WGとの合同開催でした

◇ ◇ ◇

第88回IETFミーティング以降、大規模な通信傍受（pervasive monitoring）への対策として、さまざまなWGで通信プロトコルに暗号化機能を持たせることが検討されています。第90回IETFミーティングで初めてWGの会合が開かれたTCPINC（TCP Increased Security） WGでは、インターネットのほとんどの通信で使われているプロトコルであるTCP（Transport Control Protocol）に、認証なしの暗号化機能を持たせることが検討されています。

TCP Increased Security（tcpinc）
https://datatracker.ietf.org/wg/tcpinc/charter/

2014年11月14日には、IAB（Internet Architecture Board）から「インターネットの機密性に関する声明」が出されました。通信相手の認証を行わなくても、通信を暗号化することは大規模な通信傍受に対して有効であり、プロトコルの検討の際には、基本的な考え方として暗号化の機能を盛り込むことが推奨される、としています。

IAB Statement on Internet Confidentiality
https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/

インターネットプロトコル（IP） が生まれて以降、インターネットにおけるプロトコルには「シンプルさ」が求められてきたと言えますが、社会情勢に応じて、変化が起きているように感じられます。

（JPNIC 技術部／インターネット推進部 木村泰司）

DNS関連WG報告

本稿では、第91回IETFミーティングにおけるDNS関連のWGのうち、特に動きのあったものとして、dnsop WG、dprive WG、dnssd WGの概要を報告します。dprive WGについては、今回初めて取り上げています。

◆ dnsop WG（Domain Name System Operations WG）

第91回IETFにおいては、火曜日に2時間の枠において、dnsop WGの会合が開催されました。今回の会合では、複数の議題が予定されており、時間内にて議論が行われましたが、特に興味深かったのが、DNSトランスポートをTCPで行うことに関する議論でした。

まず、チェアから現状のWGドラフトに関する確認が行われました。その後、DNS Cookiesに関する発表が行われました。以前から提案されていたドラフトであり、Webの場合と同様に、DNSサーバとクライアントの間においてもCookieと呼ばれる固有のトークン値を提供しようとするものです。実際には、以前にメッセージを交換したDNSサーバやクライアントのCookiesを記憶しておくことで、なりすましや外部からの攻撃を判別しやすくするという手法です。BIND 9.10.1b1に試験的に実装されたことが報告され、WGドラフトとして採用してもいいのでは、といった議論がなされました。

次に、QNAME minimisationに関する発表が行われました。これは、ある名前を解決する場合に、DNSサーバへの問い合わせの回数を減らすことで、どのような名前を引いたかということを推測しにくくし、プライバシーを強化しようという提案です。DNSサーバが担当するZoneの切れ目を学習することで、余分な問い合わせを減らすという手法が用いられています。この提案に関しては、まだWGドラフトになったばかりであり、引き続きレビューを行うことが確認されました。

続いて、DNS Transport over TCPに関する議論が行われました。発表においては、現在のDNSサーバの実装と、TCP Fast Openを用いたDNS問い合わせクエリに関する実装例が紹介されました。TCPにて問い合わせを行うことの利点と欠点が議論され、TCPで行うことの可能性について議論が行われました。WGドラフトとして、引き続き議論を行うことが確認されました。

また、IPv6の逆引きゾーンに関するドラフトである、draft-howard-dnsop-ip6rdns、ならびに新たな提案であるdraft-wkumari-dnsop-root-loopbackに関する発表も行われました。前者は、逆引きによるホストの認証や、メールサーバの認証を行っている運用手法に対して、IPv6の逆引きが適切な名前で設定されていることを期待しないよう指摘するガイドラインをめざした文書です。後者は、Root DNSの仕組みに関する新たな提案で、リゾルバDNSサーバにRoot Zoneのコピーを持たせることで、Root DNSサーバへの無駄な問い合わせを減らすという手法の提案です。新たな提案であるため、その目的や概要等が説明され、また議論されました。このRoot DNSに関する新たな提案に関しては、


● 第91回IETFの会場となったHilton Hawaiian Village

その後、香港にてワークショップが開催される旨がアナウンスされました。このワークショップはdnsop WGとは独立して行われたものでしたが、この提案と、もう一つの別のRoot DNSに関連する提案を中心に、次世代のRoot DNSの構造に関するワークショップが開催されました。dnsop WGとしては、引き続き議論を行っていくのではないかと思われます。

◆ dprive WG（DNS PRIVate Exchange WG）

dprive WGは、クライアントとDNSサーバの間の名前解決における、プライバシー問題を解決するために設立されたWGです。

(1) draft-hallambaker-privatedns
(2) draft-hzhwm-dprive-start-tls-for-dns
(3) draft-hoffman-dprive-dns-tls-alpn
(4) draft-hoffman-dprive-dns-tls-https
(5) draft-hoffman-dprive-dns-tls-newport

といったI-Dが取り上げられ、議論が行われました。具体的には、クライアントとリゾルバDNSサーバの間の通信を、何かしらの方法を用いて暗号化することを目標としています。

(1) draft-hallambaker-privatednsは、DNSトランスポートプロトコルとして、よりセキュリティに優れた仕組みを提案しているドラフトです。JSONベースのJCX（JSON Service Connect）プロトコルを用いて、DNSクライアントとリゾルバサーバ、ならびにDNSサーバ間の通信を行うという手法です。当然、従来のDNSトランスポートプロトコルとは大きな違いがあるため、どのような用途に適しているのか、またどう実現するのかといった説明や議論が行われました。

次に、(2) draft-hzhwm-dprive-start-tls-for-dnsに関する発表がありました。このドラフトは、TLSを用いてDNSトランスポートを暗号化し、その性能劣化を最小限にする方法を議論したものです。EDNS0のフラグとしてTLS OK（TO）ビットを用意し、TOビットが有効なクライアントとDNSサーバ間においてTLSを用いた通信を行います。また、TCPとTLSを用いることによる性能劣化を防ぐために、通常のTCPによるDNS問い合わせにSTARTTLSを用いてTLSを追加し、さらにTLS接続を継続して使いまわすという手法を提案しています。この点に関して、遅延の増加傾向やDNSサーバのCPU負荷の変化傾向等、数値的な評価も発表されました。さらに、試験的な実装も公開されています。

最後に、(3) draft-hoffman-dprive-dns-tls-alpn、(4) draft-hoffman-dprive-dns-tls-https、(5) draft-hoffman-dprive-dns-tls-newportに関する発表がありました。これらは、それぞれ別の手法にてDNSトランスポートにセキュリティを導入するための手法を提案しているものです。draft-hoffman-dprive-dns-tls-alpnは、TLS ALPN（Application Layer Protocol Negotiation）を用いてDNSトランスポートの暗号化方式を決定する手法を提案しています。draft-hoffman-dprive-dns-tls-httpsは、DNSの問い合わせや応答のトランザクションを、HTTPのURIフォーマットに変換して行うことを提案したものです。最後に、draft-hoffman-dprive-dns-tls-newportは、DNSクライアントとDNSリゾルバサーバの間でTLSを用いたDNSトランスポート通信を用いる場合に、ポート番号を443ではない別のポート番号を用いることを提案するものです。これを実現するための手法がいくつか提起され、議論が行われました。

dprive WGはまだ議論が開始されたばかりであり、今後も引き続いてDNSトランスポートのプライバシー問題解決に向けた議論が行われると思います。

◆ dnssd WG（Extensions for Scalable DNS Service Discovery WG）

dnssd WGでは、まずDNS Long-Lived Queriesに関する発表が行われました。これはDNSを利用したサービス発見において、DNSサーバとの通信を状態管理することで、新たなサービス追加や削除などのイベントを管理できるようにする手法を提案したものです。この機能はすでにMac OS XのBonjour等に実装されており、dnssd WGでは、DoSに対する懸念点や、トランスポートプロトコルのTCPへの変更や、TLSの利用などが議論されました。TCPへの変更に関して、引き続き議論が行われる様子です。

次に、draft-rafiee-dnssd-mdns-threatmodel-01に関する発表がありました。このドラフトは、DNSSDによってローカルネットワークを越えてサービス通知が行われるにあたって、ネットワークの内部情報が漏れたり、名前の衝突が発生したり、なりすましが行われたりするような、DNSSDにおける脅威について分析したものです。会場の議論では、同じような脅威は別のプロトコルにも存在するため、よりDNSSDに特化した脅威について明確にすべき、といった意見が出ました。引き続き議論が行われます。

さらに、draft-cheshire-homenet-dot-homeに関する発表が行われました。これは、.homeという特殊なトップレベルドメインを、家庭内部のデバイス管理に利用するという提案です。会場では、.localドメインとの違いや利用方法の差異、dnsop WGやhomenet WGとの連携に関する議論が行われました。

また、draft-ietf-dnssd-hybrid-00に関する発表と議論も行われました。Multicast DNSによるサービス発見の結果を、Unicast DNSの名前空間にマッピングする手法を提案しているものです。新たにWG draftして発行され、WGラストコールに向けて改訂を進めることが確認されました。

（JPNIC DNS運用健全化タスクフォースメンバー／
東京大学 情報基盤センター 関谷勇司）

From JPNIC

Dear Readers,

JPNIC issues triannual newsletters covering various topics concerning JPNIC activities and the Internet Industry to deliver our news to JPNIC Members and other stakeholders in the industry. Since its Issue 57 in August 2014, we provide the summary in English.

"Special Article 1" covers recent developments on Internet Governance, focusing on IANA Stewardship transition. Since September 2014, the communities on three IANA resources, IETF for protocol parameters, ICANN for domain names and RIRs for IP numbers had been discussing their proposals on respective resources until January 15, 2015. This article overviews three proposals and identifies the key points for the development of integrated proposal by ICG - IANA Stewardship Coordination Group.

"Special Article 2" of issue 59 reports "Internet Week 2014" which is held annually by JPNIC in late November, and its plenary program "IP Meeting 2014". "Rethinking 'our' Internet" was the theme of Internet Week 2014. With it also applied to its plenary, IP Meeting 2014 successfully draw audience's attention with two interesting panel discussion sessions which are "Internet Governance from business point of view" and "Future infrastructure to be constructed by 'us' all - Three years after the disaster, toward Tokyo 2020 Olympic Paralympic Games". This articles mainly covers these sessions.

"A Scene on the Internet History" is titled "Emergence and Deployment of Internetworking - with focus on the achievement of Professor Eisuke HAYASHI", to overview how the Internet was emerged among academic networks and then deployed toward municipalities and schools.

"Introducing JPNIC Member" which focuses on a JPNIC member with interesting activities in every issue this time introduces Kyushu Telecommunication Network Co., Inc. (QTnet). QTnet is a telecom operator serving Kyushu area mainly with FTTH, and sponsored APRICOT-APAN 2015 which was held in Fukuoka from late February to early March. QTnet, as a company rooted in the region, put a considerable contribution for network infrastructure of the conference as well as valuable suggestions for APRICOT-APAN 2015.

"Internet terms in ten minutes" picks up "SSL/TLS" which recently gathers a lot of attention for vulnerabilities associated with them.

Issue 59 further covers APRICOT-APAN2015, JPNIC General Meeting in December 2014, ICANN 51 Meeting, APNIC 38 Conference and IETF 91 meetings with detailed reports and statistics published by JPNIC.

We do hope these articles are useful for a lot of readers. If you have any questions or feedback, please feel free to contact us at jpnic-news@nic.ad.jp. Your input is always highly appreciated.

10'00"00 インターネット10分講座

MIN SEC 1/100S INTERNET

SSL/TLS 20年の歩みと動向

昨年2014年は、SSL（Secure Sockets Layer）とTLS（Transport Layer Security）というプロトコルがリリースされてから20年が経過し、HeartBleedやPOODLEなどの脆弱性でも話題となった年でもありました。今回の10分講座では、SSL/TLS暗号通信プロトコルの動向を紹介します。

◆ SSL/TLSとは

SSL/TLSは最も普及している暗号通信プロトコルの一つで、TCP/IPの4レイヤーモデルのトランスポート層とアプリケーション層との間に位置するため、広く使われているHTTPばかりでなく、SMTPなど任意のプロトコルを安全に送受信する目的で使用することができます。特にWebにおいて暗号通信機能を提供できるようになったことにより、オンラインショッピング、オンラインバンキングやユーザー認証を必要とする各種オンラインサービスの普及に重要な役割を担ってきました。

SSL/TLSには暗号化、認証、改ざん検知の三つの主要な機能があります。暗号化により通信の盗聴を防ぐことができ、認証によりサーバやクライアントが正しい通信相手であるか確認することができ、改ざん検知により通信中のデータの不正あるいは障害によるデータの誤りを検知することができます。

◆ SSL/TLSの歩み

SSL 1.0プロトコルは、1994年にネットスケープコミュニケーションズ社により開発されましたが、公開前に設計に問題が発見されたことで公開はされず、同1994年にSSL 2.0として公開され、翌1995年にはセキュリティ上の問題を修正したSSL 3.0が公開されました。ブラウザとしてはNetscape Navigator 1.1や、Microsoft® Internet Explorer 2.0に初めてHTTPS機能が搭載され、サーバ側でもApache HTTP ServerをHTTPS対応にするための、OpenSSLの前身となったライブラリ、SSLeayがリリースされ、SSLの普及が大いに加速されました。

1996年以降、SSLの標準化はネットスケープコミュニケーションズ社からIETF TLSワーキンググループに移管され、1999年にSSL 3.0とほぼ同等のRFC 2246 TLS 1.0が、2006年にはCBCブロック暗号モードに対する攻撃への対応などセキュリティ機能を強化したRFC 4346 TLS 1.1が、2008年には暗号アルゴリズムの移行のためにSHA-256、GCMなどを導入したRFC 5246 TLS 1.2がリリースされました。2015年1月現在では、TLS 1.3の策定が行われています。

SSL/TLSのプロトコル、実装ライブラリ、対応Webブラウザ、各種脆弱性や問題の、20年にわたる歴史を年表に整理しましたのでご覧ください。

◆ SSL/TLSの課題と議論

2014年は、ShellShockなどさまざまな脆弱性が発見された年でしたが、その中で、SSL/TLSについてもHeartBleedやPOODLEなどの脆弱性があった年でした。前述の年表をご覧いただくとお気づきになるかもしれませんが、2005年までは単にソフトウェアのアップデートやパッチを適用し、弱い暗号からの移行に対応していればセキュリティ対策として十分であったものが、今回は事情が異なり、より複雑になってきているように思います。これらの問題は、大きく四つに分類することができます。

(1) ソフトウェアの実装上の問題やバグ
(2) 暗号アルゴリズムの危殆化（きたいか）※への対応
(3) 認証局の運用上の問題
(4) SSL/TLSプロトコルの設計上の問題

※暗号アルゴリズムの安全性のレベルが低下した状況、または、その影響により、暗号アルゴリズムが組み込まれているシステムなどの安全性が脅かされる状況を指します

(1) のソフトウェアの実装上の問題については、使用するソフトウェアやライブラリの脆弱性情報を注視し、適切にソフトウェアアップデートやパッチを適用することで解決できます。

(2) の暗号アルゴリズムについては、米国の暗号輸出規制に対応した暗号はもちろんのこと、MD5、DES、RC4などの今となっては弱い暗号の利用を控える必要があります。BEASTなどCBCブロック暗号モードに関連した脆弱性が多く発見され、GCMモードなどの認証暗号を使った暗号が推奨されています。ただし、フィーチャーフォンや古いゲーム機など後方互換性のために、3DESやRC4などの古い暗号スイートを使わざるを得ないケースもあるので注意が必要です。さらに、SHA-1を使用したSSLサーバ証明書についても、Google Chrome™やFirefoxなどのブラウザ、Microsoft製品では2017年1月以降使用できなくなるため、サーバ管理者の方は、SHA-2アルゴリズムを使ったサーバ証明書の移行計画を立てておく必要があるでしょう。

(3) については、2011年頃はDigiNotar社やTURKTRUST社など、SSLサーバ証明書を発行する認証局が攻撃を受け不正な証明書を発行してしまう事件が多発し、認証局の信頼が損なわれました。それまでは証明書失効リスト（CRL）やOCSP（Online Certificate Status Protocol）などPKIの失効の仕組みだけで証明書が信頼できるか判断できたのが、それだけでは十分ではないとされたのです。不正に発行された証明書を検知するための仕組みとして、インターネットドラフト“Public Key Pinning Extension for HTTP”や、“RFC 6962 Certificate Transparency”など、SSL/TLSを補強する技術が実装されつつあります。

(4) についても2010年以降、BEAST、CRIME、POODLEなどSSL/TLSのプロトコル設計上の欠陥をつく攻撃が顕著になってきています。このような場合では、プロトコルを正しく実装したソフトウェア自体には問題はないので、ソフトウェアアップデートでは対応できません。多くの場合、暗号スイートの設定、圧縮設定の無効化、SSL/TLSプロトコルバージョンの設定など、サーバやクライアントの設定により対策する必要があります。

◆ 脆弱性の歴史

さて、ここからはSSL/TLSに関連した主要な脆弱性の歴史について、振り返ってみたいと思います。

1）MD5不正CA証明書（2008）

2007年にMD5のハッシュ衝突攻撃が発表されましたが、これを応用して、MD5 with RSA署名アルゴリズムのSSLサーバ証明書を発行する認証局を利用して、不正なCA証明書に作り変えてしまうという攻撃方法が、Alexander Sotirov氏らの研究グループによって発表されました。発行される証明書のシリアル番号が予測できれば、検証で無視されるフィールドをうまく作り込むことにより、不正な中間CA証明書が作れてしまうというものでした。中間CA証明書を不正作成できたということは、そこから任意のドメイン名のSSLサーバ証明書を発行できるということです。不正CA証明書のハッシュ衝突を計算するために、SONY Play Station 3 200台で構成されたクラスタで、わずか1、2日で計算できたということでも話題となりました。

2）DebianのOpenSSL RSA鍵生成問題（2008）

2008年に、Linuxのディストリビューションの一つであるDebianが提供する、OpenSSLのパッケージのみに発生した脆弱性がありました。直接的なSSL/TLSの脆弱性ではありませんが、SSLサーバ証明書の再発行を必要としたサイトもあり、相当数の影響がありました。DebianのOpenSSLでは、疑似乱数の初期値が固定になっており、生成されるRSA鍵の種類が非常に限定的になっていたことがわかりました。そのため、すべての場合を調べれば、生成される可能性のある秘密鍵のすべてが得られるようになっていました。このような方法で他人が秘密鍵を持っている恐れのある公開鍵はブラックリスト化され、問題がある鍵かどうかのテストサイトもいくつか公開されました。

3）証明書識別名のNULL終端問題（2009）

C言語ではNULL文字（“\0”）を文字列の終端記号として扱いますが、SSLサーバ証明書のドメイン名を表す証明書の識別名では、NULL文字を途中で使うことができます。例えば、攻撃者がwww.example.com用のフィッシングサイトを作りたいとしても、example.comドメインの管理権限はないので通常なら認証局は証明書を発行しませんが、攻撃者がevilsite.jpドメインのオーナーであるとすれば、以下のような識別名の証明書は発行してもらえる可能性があります。

CN=www.example.com\0.evilsite.jp, O=Evil Site, C=US

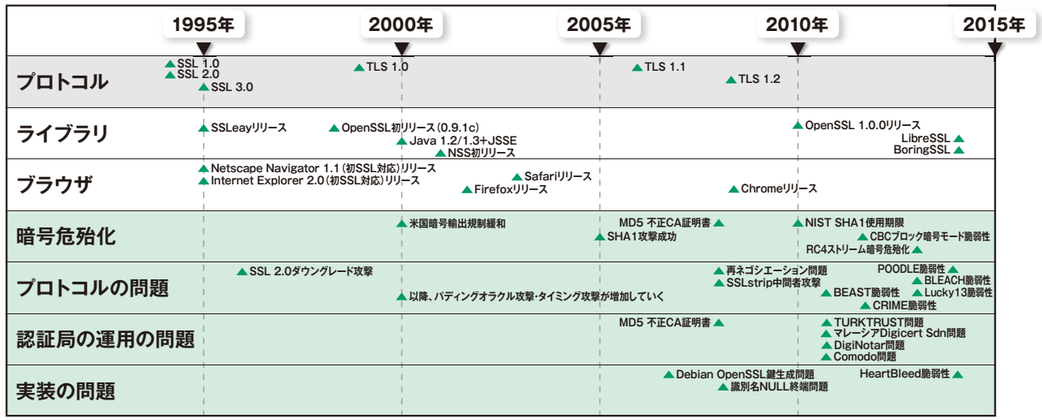
この問題が発生した当時の一部のブラウザでは、NULL文字を文字列の終端記号であるとして扱ってしまったため、上のような名前の証明書をwww.example.comドメイン用であると勘違いしてSSL通信を開始してしまいました。この脆弱性はBlackHat 2009でDan Kaminsky氏らのグループにより発表され、後にすべてのブラウザのアップデートで問題解決されました。

4）再ネゴシエーション問題（2009）

2009年にSSL 3.0以降で導入された再ネゴシエーションのプロトコルに設計上の脆弱性があり、クライアント側の要求に対して任意のデータが挿入できる脆弱性が発見されました。この攻撃に対する緩和策は、サーバが再ネゴシエーションを禁止するか、“RFC 5746 Transport Layer Security（TLS）Renegotiation Indication Extension”というTLS拡張を使用することです。問題発覚以降のアップデートでは、すべてのサーバ、ブラウザ、ライブラリでこのセキュアな再ネゴシエーション機能が有効になっています。

5）DigiNotar不正証明書発行事件（2011）

2011年にオランダ政府の証明書発行業務も行っている、オランダの認証局DigiNotar社がハッキング攻撃を受け、不正に531枚のSSLサーバ証明書を発行するという事件がありました。2011年か



図：SSL/TLS20年の歴史

ら2012年にかけては、英国Comodo社、マレーシアDigicert Sdn社、トルコTURKTRUST社など、認証局のシステムの不備をついたハッキング攻撃により、不正な証明書を発行してしまうという事件が多発しました。その中でも、DigiNotar社の事件は最大級のものでした。

この事件は、運用監査なども適切に実施し、運用上不正な証明書を発行するなどあり得ないと考えられていた認証局が、Google、FacebookやMicrosoftなどの著名サイト用のワイルドカードドメインの証明書を不正発行してしまい、中間者攻撃により通信を盗聴された可能性が高いというもので、認証局の信頼を完全に損なわせるような事件でした。

6)BEAST(2011)

BEASTは、2011年にThai DuongとJuliano Rizzoらの研究グループにより発見された脆弱性で、CBCブロック暗号モードであれば、AESなどの強い暗号でもセッションクッキーが解読され、ハイジャックされる可能性があるというものです。実際にJavaアプレットの脆弱性と組み合わせて、paypal.comサイトに対してハイジャックのデモを行いました。一時、BEAST対策としてRC4ストリーム暗号を使うことが推奨されましたが、RC4暗号にも脆弱性が発見されたため、現在ではCBCモードの初期ベクタ(IV)の処理が変更されたTLS 1.1を使うか、GCMモードなどの認証暗号を使うしか解決策がありません。

7)CRIME(2012)

CRIMEは2012年に発見された、TLSのデータ圧縮機能を使ってセッションクッキーを解読する攻撃です。同じ文字であれば、圧縮後のデータサイズが小さくなる圧縮の性質を利用して、さまざまなデータを埋め込むことによりデータサイズの変化を見ながら、クッキーのすべてを解読しセッションハイジャックする攻撃です。この攻撃は、AESやGCMやSHA-256など強固な暗号を利用していたとしても、使用する暗号に関係なく攻撃が可能であるという特徴があります。サーバの設定によりTLSデータ圧縮を無効化することにより攻撃の緩和が可能です。現在策定中のTLS 1.3では、TLSデータ圧縮は無効化されています。

8)HeartBleed(2014)

2014年に発見された当時のOpenSSL 1.0.1系のバージョンすべてに影響する脆弱性で、認証クッキーやパスワードなどメモリ上の情報が、外部から取得可能となる脆弱性です。これは、“RFC 6520 Transport Layer Security(TLS) and Datagram Transport Layer Security(DTLS) Heartbeat Extension”というTLS拡張の、OpenSSLによる実装の不備をついたものです。Heartbeat(死活確認)で要求されるデータサイズは本来小さいものですが、クライアント側で大きな値を設定すると、サーバ側でメモリの境界を越えて結果を返してしまい、場合によってはクライアントにセッションクッキーやユーザーのパスワードなどの情報が見えてしまう可能性があるというものでした。OpenSSLのアップデートにより、問題は解決しています。ただ、OpenSSLの古いメモリ管理により起きた問題で、今後も同様の脆弱性が発見される可能性があるため、OpenSSLを作り直そうという動きが生まれ、LibreSSLやBoringSSLなどの、OpenSSLのリプレースをめざすプロジェクトが発足しました。

9)POODLE(2014)

POODLEは、2014年に発見されたSSL 3.0プロトコルの、パディングに関する設計上の不具合をついた攻撃で、CBCブロック暗号モードを使っている場合に、セッションクッキーを盗聴される恐れがあります。この脆弱性はTLS 1.0以降では発生せず、SSL 3.0でのみ発生するものです。SSL 3.0とTLS 1.0では、プロトコルにあまり違いがないと言われていますが、小さな違いの一つとしてパディング生成があります。ブロック暗号では決められたブロックサイズの倍数でデータを送りますが、ブロックサイズの倍数にならない場合には、何らかのデータで「詰め物」をし、倍数になるように調整します。これをパディングと呼びます。TLS 1.0では決められたパディング値を使いますが、SSL 3.0では任意の値をパディングに使えます。これを利用して、さまざまな値を埋め込んでみてクッキーの値を推測するのです。POODLE攻撃を緩和するには、TLS 1.0以上を使う、もしくはブロック暗号GCMモードやストリーム暗号を使うなどの方法があります。TLS 1.0では、影響が全くないとされていましたが、TLS 1.0であってもパディングの正しさを確認せず、POODLE攻撃の影響を受ける実装が発見されました。

◆ SSL/TLSの注目すべきトピック

1)LibreSSLとBoringSSL

OpenSSLのHeartBleed脆弱性をきっかけに、これまでOpenSSLで問題視されていたソースコードの複雑さの解消と、今後脆弱性が含まれにくくするために、ソースコードの改変をしたいという動きが生まれました。その一つが、OpenBSDが開発に着手したLibreSSLです。

LibreSSLには次に示すような、大きな特徴があります。

・OpenSSL 1.0.1gからソースコードを分岐させた
・OpenSSLと公開APIが完全互換
・メモリ管理を独自のものではなくシステムコールに置き換え、メモリ関連の脆弱性を低減
・現時点では暗号スイートがOpenSSLより古いが、今後、新しい強固な暗号スイートをサポートする
・古いプラットフォームのサポートを廃止

また、同様にGoogle社も、OpenSSLからソースコードを分岐させた、独自のBoringSSLの開発を開始しました。将来的には、Google ChromeやAndroid™などでOpenSSLの使用を止め、BoringSSLへ移行するよう計画しています。

2)PFS対応

エドワード・スノーデン氏の暴露により、米国国家安全保障局(NSA)が米国全国民の通信を盗聴していたという疑惑が語られており、SSL/TLS暗号通信であっても、暗号化されたままの通信データを巨大なデータベースに保管しておけば、将来、サーバの廃棄されたハードディスクから盗んだり、秘密鍵を解読したりすることにより、SSL/TLS暗号通信をすべて解読できる可能性があります。

将来、サーバ証明書の秘密鍵が漏洩したとしても、通信内容を解読されることはないようにすることを、Perfect Forward Secrecy(PFS)と呼んでいます。具体的には、ECDHEやDHEを含む暗号スイートを使用することで、PFSに対応することができます。ECDHやDHなどの鍵交換アルゴリズムと比較して「E、ephemeral(つかの間の、短命な)」がついています。TLS 1.3では、ECDHEやDHE などPFS対応の暗号スイートを使用します。

DHEやDHで使用されるDiffie-Hellman鍵共有アルゴリズムの実装では、現時点で弱いとされている1,024bit以下のDH鍵を使用する実装が多いためにDHEを使うのは問題があり、ECDHEを使う方がよいと考えられます。

3)SHA-2サーバ証明書への移行

現状では、数多くのサイトでSHA-1 with RSA署名アルゴリズムのサーバ証明書を使っていますが、米国の標準化機関である米国立標準技術研究所(NIST)の暗号アルゴリズムの移行に関するガイドライン SP800-131Aでは、SHA-1を2013年12月31日以降署名と検証には使ってはならないとしています。しかしながら、米国政府のサイトですら、多くがSHA-1の証明書を使用しています。

このような状況を受けて、Microsoft社はすべての製品において2017年1月1日以降、SHA-1証明書を使用した際にエラーとするというポリシーを公表しました。また、Google Chromeでは、2014年11月より段階的にSHA-1証明書を使用した場合にアラートを表示するようにし、Microsoft社製品と同様に2017年1月1日以降にエラー表示になります。Firefoxも同様のポリシーを公表しています。

すべてのサーバ管理者の方は、2016年末までにSHA-256 with RSAなどのSHA-2証明書へ移行する必要があります。証明書の有効期限が1年や2年であるケースが多いことを考慮すると、2015年中にはSHA-2証明書への移行を検討しなければなりません。レガシーな環境では、SHA-2証明書へ対応できないケースもあるでしょうから、そのような場合には、システム全体の更改も検討しなければなりません。

4)Certificate Transparency

Certificate Transparencyは、DigiNotar社やTURKTRUST社などの認証局への攻撃による不正証明書発行事件を受けて、2013年にExperimental RFC 6962として公開された、不正に発行された証明書を検証するための仕組みの一つです。認証局が、不正な意図しない証明書を発行していないことを示す監査記録を公開サーバに公表することにより、あるサイトに不正な証明書が別途出ていないかを判定することができます。

既に、Google ChromeがCertificate Transparencyに対応しており、例えばCertificate Transparencyに対応した、DigiCert社のサイト(https://www.digicert.com)を表示した場合に、「公開監査が可能です。」と表示されます。一方、対応していないサイトでは「公開監査記録がありません。」と表示されます。

5)Public Key Pinning

Public Key Pinning、もしくは Certificate Pinningもまた、DigiNotar社のような不正証明書発行事件から利用者を守るための技術で、“Public Key Pinning Extension for HTTP”というスタンダードトラックのインターネットドラフトになっており、既に、Google ChromeやFirefoxで実装されています。

サイトの証明書のハッシュ値を、何らかの方法で取得し、それとサイト証明書とを比較し、一致していなければ警告を出すというものです。サイト証明書のハッシュを提供する方式としては「ブラウザに組み込む」と「サイトのHTTPヘッダでハッシュ値を提供する」という、二つの方式があります。

GoogleやFacebookなど著名なサイトを閲覧する場合には、ブラウザ組み込みのPinningのハッシュ値を使うことができます。そうでないサイトの場合には、HTTPヘッダ方式を使用します。

6)OCSP Stapling

“RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”は、あるサーバ証明書が失効しているかどうかを確認するためのプロトコルで、現在多くのブラウザでは、もう一つの失効検証方法である、CRLよりも優先して使用される失効検証方法です。ただ、OCSPには現在二つの問題があると言われています。

・OCSPレスポンスが取得できない場合でも、多くのブラウザが検証成功としてしまう。DoS攻撃により検証妨害した場合に偽サイトでも有効としてしまう可能性がある
・サイトのアクセス記録がOCSPレスポンダサーバ、つまり認証局側にも残ってしまい、プライバシー上の問題がある。アクセス記録は本来Webサイトしか持つべきでない

これらの問題を解決するのが“RFC 6066 Transport Layer Security(TLS) Extensions: Extension Definitions”で規定されたOCSP Staplingです。Staplingとはホッチキス留めのことで、TLSのセッションにおいて拡張領域にOCSPによる、証明書の状態を入れることができます。OCSP Staplingを使用することにより、前述のOCSPの問題を解決することができます。

・サイトに接続できれば必ず証明書の失効状態を確認でき、認証局のOCSPに接続する必要がない
・失効検証のために認証局のOCSPレスポンダに接続する必要がないので、認証局にはアクセスログは残らず、プライバシーの懸念がない

OCSP Staplingは多くのブラウザ、サーバで対応しており、サーバに設定を行うだけで利用可能になります。

◆ おわりに

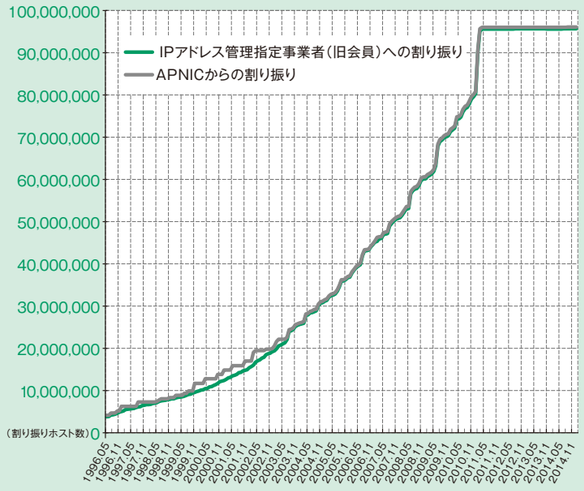
SSLの誕生から20年が経ち、SSL/TLSが社会インフラの重要なプロトコルとなったと同時に、さまざまなセキュリティ上の問題も顕在化してきています。今後も、こうした動向に注目しながら安全にSSL/TLSを利用していく必要があるでしょう。

(富士ゼロックス株式会社 漆嶌 賢二)

統計情報
Statistics Information

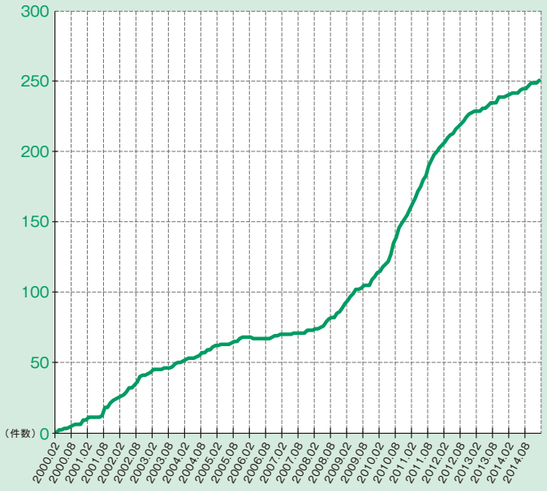
IPv4アドレス割り振り件数の推移

IPv4アドレスの割り振り件数の推移です。2011年4月15日にアジア太平洋地域におけるIPv4アドレスの在庫が枯渇したため、現在は、1IPアドレス管理指定事業者につき、最後の/8ポリシーに基づき/22、返却済みアドレスから/22をそれぞれ上限とする割り振りを行っています。(2015年1月現在)



IPv6アドレス割り振り件数の推移

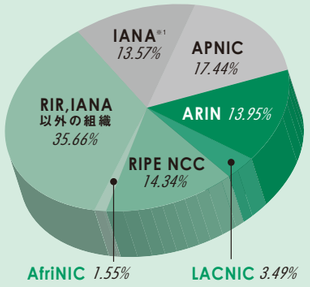
IPv6アドレスの割り振り件数の推移です。なお2011年7月26日より、IPアドレス管理指定事業者および特殊用途用PIアドレス割り当て先組織が、初めてIPv6アドレスの分配を受ける場合の申請方法は簡略化されています。(2015年1月現在)



地域インターネットレジストリ(RIR)ごとのIPv4アドレス、IPv6アドレス、AS番号配分状況

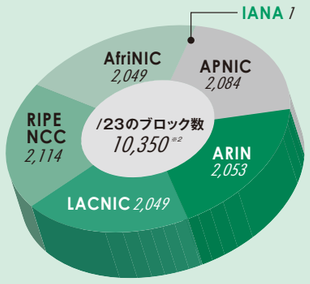
各地域レジストリごとのIPv4、IPv6、AS番号の割り振り状況です。APNICはアジア太平洋地域、ARINは主に北米地域、RIPE NCCは欧州地域、AfriNICはアフリカ地域、LACNICは中南米地域を受け持っています。**2011年2月3日に、IPv4アドレスの新規割り振りは終了しています。**

●IPv4アドレス(/8単位)



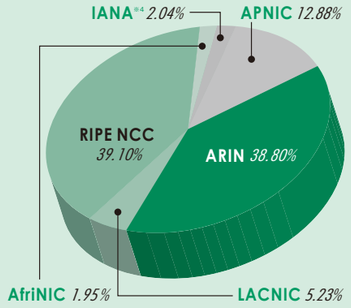
※1 IANA:Multicast(224/4)
RFC1700(240/4)
その他(000/8,010/8,127/8)

●IPv6アドレス(/23単位)



※2 IANAからRIRに割り振られた/23のブロック数10,349

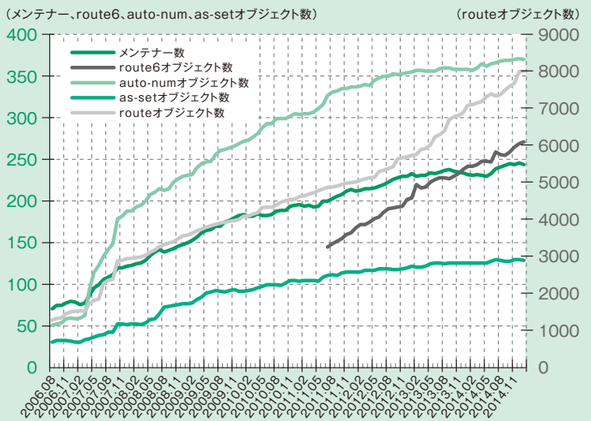
●AS番号(2バイト※3)



※3 この他に4バイトAS番号があり、各RIRへの割り振りが始まっています。
割り当て済みの4バイトAS番号は1%未満です。
※4 IANA:AS番号 0, 23456, 64198-65535

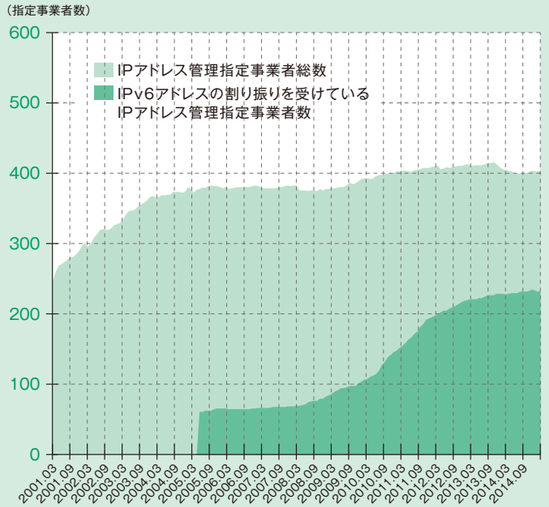
JPIRRに登録されているオブジェクト数の推移

JPNICが提供するIRR(Internet Routing Registry)サービス・JPIRRにおける各オブジェクトの登録件数の推移です。2006年8月より、JPNICからIPアドレスの割り振り・割り当て、またはAS番号の割り当てを受けている組織に対して、このサービスを提供しています。JPIRRへのご登録などの詳細は、右記Webページをご覧ください。https://www.nic.ad.jp/ja/irr/



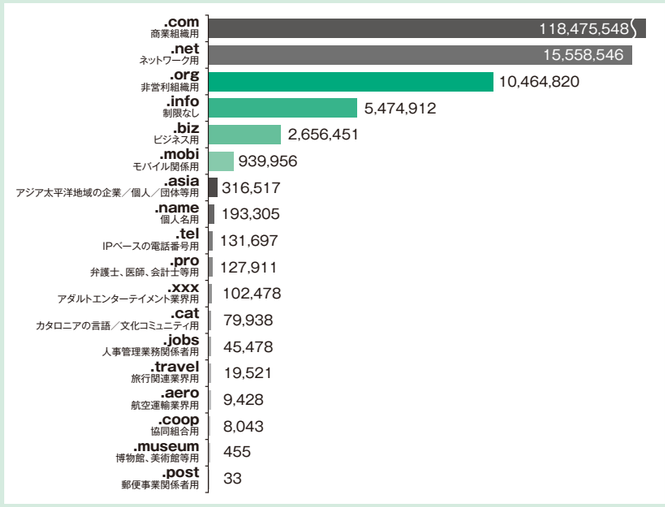
IPアドレス管理指定事業者数の推移

JPNICから直接IPアドレスの割り振りを受けている組織数の推移です。(2015年1月現在)



主なgTLDの種類別登録件数

旧来の分野別トップレベルドメイン(gTLD: generic TLD)の登録件数です(2014年10月現在)。
データの公表されていない、.edu, .gov, .mil, .intは除きます。



※右記のデータは、各gTLDレジストリ(またはスポンサー組織)がICANNに提出する月間報告書に基づいています。これら以外の2013年10月以降に追加されたgTLDについては、ICANNのWebサイトで公開されている月間報告書に掲載されていますので、そちらをご覧ください。

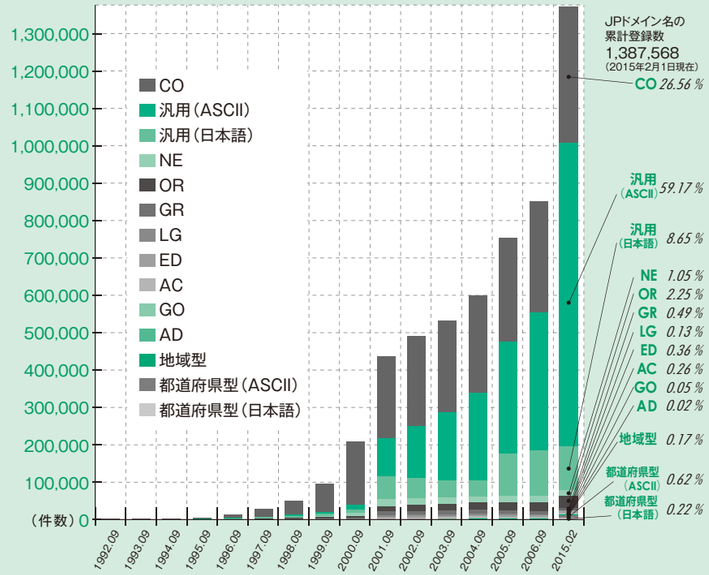
Monthly Registry Reports
https://www.icann.org/resources/pages/reports-2014-03-04-en

統計情報
Statistics Information

JPドメイン名登録の推移

JPドメイン名の登録件数は、2001年の汎用JPドメイン名登録開始により大幅な増加を示し、2003年1月1日時点で50万件を超えました。その後も登録数は増え続けており、2008年3月1日時点で100万件を突破、2015年2月現在で約138万件となっています。

属性型・地域型JPドメイン名	
AD	JPNIC会員
AC	大学など高等教育機関
CO	企業
GO	政府機関
OR	企業以外の法人組織
NE	ネットワークサービス
GR	任意団体
ED	小中高校など初等中等教育機関
LG	地方公共団体
地域型	地方公共団体、個人等
都道府県型JPドメイン名	
ASCII	組織・個人問わず誰でも(英数字によるもの)
日本語	組織・個人問わず誰でも(日本語の文字列を含むもの)
汎用JPドメイン名	
ASCII	組織・個人問わず誰でも(英数字によるもの)
日本語	組織・個人問わず誰でも(日本語の文字列を含むもの)



JPドメイン名紛争処理件数

JPNICはJPドメイン名紛争処理方針(不正の目的によるドメイン名の登録・使用があった場合に、権利者からの申立に基づいて速やかにそのドメイン名の取消または移転をしようとするもの)の策定と関連する業務を行っています。この方針に基づき実際に申立てられた件数を示します。
(2015年2月現在)

※申立の詳細については下記Webページをご覧ください
https://www.nic.ad.jp/ja/drp/list/

	申立件数	結　果
2000年	2件	移転　1件　取下げ 1件
2001年	11件	移転　9件　取下げ 2件
2002年	6件	移転　5件　取消 1件
2003年	7件	移転　4件　取消 3件
2004年	4件	移転　3件　棄却 1件
2005年	11件	移転 10件　取下げ 1件
2006年	8件	移転　7件　棄却 1件
2007年	10件	移転　9件　棄却 1件
2008年	3件	移転　2件　棄却 1件
2009年	9件	移転　4件　取消 2件　棄却 2件　手続終了 1件
2010年	7件	移転　3件　取消 3件　棄却 1件
2011年	12件	移転 10件　取下げ 1件　棄却 1件
2012年	15件	移転　9件　取下げ 2件　取消 2件　棄却 2件
2013年	10件	移転　10件
2014年	8件	移転　7件　係属中 1件

※取 下 げ：裁定が下されるまでの間に、申立人が申立を取り下げること
移　　転：ドメイン名登録者(申立てられた側)から申立人にドメイン名登録が移ること
取　　消：ドメイン名登録が取り消されること
棄　　却：申し立てを排斥すること
手続終了：当事者間の和解成立などにより紛争処理手続が終了すること
係 属 中：裁定結果が出ていない状態のこと

会員リスト
2015年2月16日現在

JPNICの活動はJPNIC会員によって支えられています

S会員

株式会社インターネットイニシアティブ

エヌ・ティ・ティ・コミュニケーションズ株式会社

株式会社日本レジストリサービス

A会員

富士通株式会社

B会員

株式会社エヌ・ティ・ティ・ドコモ

KDDI株式会社

C会員

株式会社エヌ・ティ・ティ ピー・シー コミュニケーションズ

ビッグローブ株式会社

JPNIC会員はメンバーズラウンジをご利用いただけます

JPNIC会員のみなさまに向けたサービスの充実を目的とし、JPNICオフィス(東京・神田)の会議室等を無償提供しております。当センターは、JR神田駅からは徒歩1分、また東京メトロ神田駅、大手町駅、JR新日本橋駅からも至近ですので、出張の空き時間でのお仕事スペース等として有効にお使いいただけます。

■ご提供するサービスについて

利用可能日時

- 月～金／ 10:00 ～ 17:30 (1 時間単位／ Wi-Fi および電源利用可)
（祝日等の当センター休業日および当センターが定める末開放日を除く）

提供可能なサービス

- JPNIC の会議室の使用 (1 時間単位、1 日 3 時間まで)
- JPNIC が講読している書物 / 雑誌 / 歴史編纂資料等の閲覧
- お茶のご提供

ご利用方法

お問い合わせ先

- 総務部会員担当　member@nic.ad.jp

※ご希望の日時に施設の空きがない、ご利用人数がスペースに合わない等、ご利用いただけない場合がございます。その場合はあしからずご了承ください。
※JPNICは事前に予告することで本サービスを中止することがございます。

会員リスト

2015年2月16日現在

D会員

- 株式会社アイテックジャパン
- アイテック阪急阪神株式会社
- 株式会社朝日ネット
- 株式会社アット東京
- アルテリア・ネットワークス株式会社
- 株式会社イージェーワークス
- e-まちタウン株式会社
- イッツ・コミュニケーションズ株式会社
- インターナップ・ジャパン株式会社
- インターネットエーアールシー株式会社
- インターネットマルチフィード株式会社
- 株式会社インテック
- 株式会社ASJ
- 株式会社エアネット
- AT&Tジャパン株式会社
- 株式会社SRA
- SCSK株式会社
- 株式会社STNet
- NRIネットコム株式会社
- 株式会社エヌアイエスプラス
- エヌ・ティ・ティ・スマートコネクト株式会社
- 株式会社エヌ・ティ・ティ・データ
- 株式会社エネルギア・コミュニケーションズ
- 株式会社オージス総研
- 株式会社オービック
- 大分ケーブルテレコム株式会社
- 株式会社大垣ケーブルテレビ
- 株式会社大塚商会
- 沖縄通信ネットワーク株式会社
- オンキヨーエンターテイメントテクノロジー株式会社
- 関電システムソリューションズ株式会社
- 株式会社キッズウェイ
- 株式会社キューデンインフォコム
- 九州通信ネットワーク株式会社
- 近畿コンピュータサービス株式会社
- 近鉄ケーブルネットワーク株式会社
- 株式会社倉敷ケーブルテレビ
- 株式会社クララオンライン
- 株式会社グッドコミュニケーションズ
- KVH株式会社
- 株式会社ケーブルテレビ可児
- ケーブルテレビ徳島株式会社
- 株式会社ケイ・オプティコム
- 株式会社KDDIウェブコミュニケーションズ
- 株式会社コミュニティネットワークセンター
- さくらインターネット株式会社
- 株式会社シーイーシー
- GMOインターネット株式会社
- GMOクラウドWEST株式会社
- ジャパンケーブルネット株式会社
- 株式会社ジュピターテレコム
- スターネット株式会社
- ソネット株式会社
- ソフトバンクテレコム株式会社
- 中部テレコミュニケーション株式会社
- 有限会社ティ・エイ・エム
- 鉄道情報システム株式会社
- 株式会社DMM.comラボ
- 株式会社ディーネット
- 株式会社ディジティ・ミニミ
- 株式会社電算
- 東京ケーブルネットワーク株式会社
- 東芝ビジネスアンドライフサービス株式会社
- 東北インテリジェント通信株式会社
- 豊橋ケーブルネットワーク株式会社
- 株式会社ドリーム・トレイン・インターネット
- 株式会社長崎ケーブルメディア
- 株式会社新潟通信サービス
- ニフティ株式会社
- 日本インターネットエクスチェンジ株式会社
- 株式会社日本経済新聞社
- 日本情報通信株式会社
- 日本通信株式会社
- 日本ネットワークイネイブラー株式会社
- 株式会社日立システムズ
- 株式会社ビークル
- 株式会社ビットアイル
- 株式会社PFU
- ファーストサーバ株式会社
- 富士通エフ・アイ・ピー株式会社
- 富士通関西中部ネットテック株式会社
- 株式会社フジミック
- 株式会社フューチャリズムワークス
- フリービット株式会社
- 株式会社ブロードバンドセキュリティ
- 株式会社ブロードバンドタワー
- 北陸通信ネットワーク株式会社
- 北海道総合通信網株式会社
- 松阪ケーブルテレビ・ステーション株式会社
- 丸紅OKIネットソリューションズ株式会社
- ミクスネットワーク株式会社
- 三菱電機インフォメーションネットワーク株式会社
- 株式会社南東京ケーブルテレビ
- 株式会社メイテツコム
- 株式会社メディアウォーズ
- 山口ケーブルビジョン株式会社
- ユニアデックス株式会社
- リコージャパン株式会社
- 株式会社両毛インターネットデータセンター
- 株式会社リンク

会員リスト

2015年2月16日現在

JPNICの活動はJPNIC会員によって支えられています

非営利会員

公益財団法人京都高度技術研究所	地方公共団体情報システム機構	特定非営利活動法人北海道地域ネットワーク協議会
国立情報学研究所	東北学術研究インターネットコミュニティ	WIDEインターネット
サイバー関西プロジェクト	農林水産省研究ネットワーク	
塩尻市	広島県	

推薦個人正会員（希望者のみ掲載しております）

淺野 善男	佐藤 秀和	沼尻 貴史
井樋 利徳	式場 薫	福田 健平
岩崎 敏雄	島上 純一	三膳 孝通
太田 良二	城之内 肇	湯口 高司
北村 和広	友近 剛史	
小林 努	外山 勝保	

賛助会員

アイコムティ株式会社	株式会社サイバーリンクス	姫路ケーブルテレビ株式会社
株式会社Eストアー	株式会社さくらケーシーエス	ファーストライディングテクノロジー株式会社
株式会社イーツ	株式会社シックス	株式会社富士通鹿児島インフォネット
伊賀上野ケーブルテレビ株式会社	株式会社JWAY	プロックスシステムデザイン株式会社
イクストライド株式会社	セコムトラストシステムズ株式会社	株式会社マークアイ
伊藤忠テクノソリューションズ株式会社	株式会社ZTV	株式会社ミッドランド
株式会社イプリオ	ソニーグローバルソリューションズ株式会社	株式会社悠紀エンタープライズ
株式会社キャッチボール・トゥエンティワン	株式会社つくばマルチメディア	
グローバルコモンズ株式会社	デジタルテクノロジー株式会社	
株式会社グローバルネットコア	虹ネット株式会社	
株式会社ケーブルネット鈴鹿	日本インターネットアクセス株式会社	
株式会社ケイアンドケイコーポレーション	ネクストウェブ株式会社	
株式会社コム	株式会社ネット・コミュニケーションズ	
サイバー・ネット・コミュニケーションズ株式会社	BAN-BANネットワークス株式会社	

JPNIC CONTACT INFO ▶お問い合わせ先

JPNIC Q&A https://www.nic.ad.jp/ja/question/

JPNICに対するよくあるお問い合わせを、Q&Aのページでご紹介しております。

詳しくはこちら

JPNIC Contact Information

JPNICでは、各項目に関する問い合わせを以下の電子メールアドレスにて受け付けております。

一般的な質問	query@nic.ad.jp	JP以外のドメイン名	domain-query@nic.ad.jp
事務局への問い合わせ	secretariat@nic.ad.jp	JPドメイン名紛争	domain-query@nic.ad.jp
会員関連の問い合わせ	member@nic.ad.jp	IPアドレス	ip-service@nir.nic.ad.jp
JPドメイン名※1	info@jprs.jp	取材関係受付	press@nic.ad.jp

※1 2002年4月以降、JPドメイン名登録管理業務が（株）日本レジストリサービス（JPRS）へ移管されたことに伴い、JPドメイン名のサービスに関するお問い合わせは、JPRSの問い合わせ先であるinfo@jprs.jpまでお願いいたします。

JPNICニュースレターについて

▶すべてのJPNICニュースレターはHTMLとPDFでご覧いただけます。

▶JPNICニュースレターの内容に関するお問い合わせ、ご意見は jpnic-news@nic.ad.jp 宛にお寄せください。

詳しくはこちら

▶なおJPNICニュースレターのバックナンバーの冊子をご希望の方には、一部900円（消費税・送料込み）にて実費頒布しております。現在までに1号から58号までご用意しております。ただし在庫切れの号に関してはコピー版の送付となりますので、あらかじめご了承ください。

ご希望の方は、希望号、部数・送付先・氏名・電話番号をFAXもしくは電子メールにてお送りください。
折り返し請求書をお送りいたします。ご入金確認後、ニュースレターを送付いたします。
宛先 FAX:03-5297-2312 電子メール:jpnic-news@nic.ad.jp

JPNICニュースレター ▶第59号
2015年3月19日発行

発行人 後藤滋樹
発行 一般社団法人日本ネットワークインフォメーションセンター
住所 〒101-0047
東京都千代田区内神田3-6-2
アーバンネット神田ビル4F
Tel 03-5297-2311
Fax 03-5297-2312
編集 インターネット推進部

制作・印刷 図書印刷株式会社

ISBN ISBN978-4-902460-34-6

JPNIC認証局に関する情報公開

JPNICプライマリルート認証局
(JPNIC Primary Root Certification Authority S2)のフィンガープリント
SHA-1:C9:4F:B6:FC:95:71:44:D4:BC:44:36:AB:3B:C9:E5:61:2B:AC:72:43
MD5:43:59:37:FC:40:9D:7D:95:01:46:21:AD:32:5E:47:6F

JPNIC認証局のページ
https://jpnic-ca.nic.ad.jp/

一般社団法人 日本ネットワークインフォメーションセンター
〒101-0047 東京都千代田区内神田 3-6-2 アーバンネット神田ビル4F
Tel 03-5297-2311 Fax 03-5297-2312