JPNIC Newsletter No.67 NOVEMBER 2017 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

Japan Network Information Center
〒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

JPNIC Newsletter for JPNIC Members

NOVEMBER 2017

No.67

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

Introduction 巻頭言

ライフラインとしてのインターネット

スマートフォンの普及、ソーシャルメディアの活用により、インターネットは多くの人にとって欠かすことのできない、重要な役割を持つこととなりました。1995年1月の阪神淡路大震災によって、被災地では電気・ガス・水道などのライフラインが絶たれた状態においてもインターネットとの接続は保たれていたことから、ライフラインとしてのインターネットの役割が議論されてきました。

ライフラインの要件として、①いつでもどこでも誰でも、②安心安全、③快適の三つが挙げられます。「いつでもどこでも誰でも」は必要不可欠な情報およびサービスがあらゆるときにどこでも誰でも利用できること、「安心安全」は安心して任せられいつも安定して利用できること、「快適」は利用環境や状況に影響を受けにくい性能であることになります。

利用者から見た場合、インターネットへの依存性が高くなった分、利用できないことによる影響も大きく、障害に対する影響をできるだけ局所化することが求められます。元々障害に対する影響の局所化を考え、自律分散システムとして作られたインターネットは、ライフラインとしてのこの要件を満たしていたことになります。

しかしながら、昨今のGoogle社、Facebook社、Microsoft社、Akamai社、Limelight社に代表されるHypergiants（大手コンテンツプロバイダーおよびCDN事業者）へのコンテンツの集中により、Hypergiantsでの障害やHypergiantsと利用者間の経路障害が自律分散システム上でも利用者にとって大きな影響を及ぼすようになってきました。Hypergiantsへのコンテンツ集中および誰もが使えるライフラインとなった分、今まではそこまで騒ぎにならなかった障害が、ニュースとなってマスコミに取り上げられるまでになりました。

サービス利用を意図的に不可能とする経路ハイジャックやDDoS攻撃だけでなく、ドメイン名とIPアドレスを変換するDNSサーバの障害、さらには設定ミスによる意図しない経路ハイジャックによる障害なども、利用者にとっては同様に依存度合いが高いライフラインの消失となってしまうのです。

一元管理者がいないインターネットでは、国内外のステークホルダーと、インターネットの運用上の諸問題に対する取り組みの在り方である「インターネットガバナンス」の中で、途上国における基盤インフラの整備や情報の自由な流通（ネット中立性）、インターネットの在り方などとともに、インターネットのセキュリティ・安定性・復元性についても議論が行われています。

JPNICでは、この「インターネットガバナンス」に対し、国内外のインターネット政策に関する調査研究や、国内外のインターネットガバナンス会議体・組織における議論や政策検討への参画、意見調整、および提言の発信を行っています。具体的な一例として、①インターネットガバナンスに関して、適切な状況認識の上で充実した検討ができる基盤を日本国内に構築する、②インターネットガバナンスに関する提言を行い、グローバルな方向性への反映と日本国内での実装を準備する、という二つの目的のもと発足した日本インターネットガバナンス会議（IGCJ）の事務局として、IGF-Japanと連携し、日本におけるNational IGFとして「Japan IGF」を構成しています。

また、JPNICでは、通信事業者が自身の経路情報を登録するルーティングレジストリ（JPIRR）を運用しています。インターネット上の全経路情報とJPIRRに登録されている経路情報を比較し、差異がある場合にはアラートを発する経路奉行と連携し、経路ハイジャック通知用に登録されたメールアドレスに通知を行うことで、経路ハイジャックに「気づく・知らせる」機能を提供しています。

このように通信事業者やインターネットコミュニティをはじめとした国内外のステークホルダーにより、ライフラインとして日々その重要度が増し、「いつでもどこでも誰でも・安心安全・快適」であるために、さまざまな取り組みがされています。そのような取り組みがされているインターネットではありますが、障害は日々発生しています。

インターネット接続ができない際に、利用する側としても事前に対処する方法を理解、学習しておくことで、原因を確認し、復旧することも可能となります。

例えば、DNSサーバ障害かどうかの確認方法、DNSサーバ障害であった際にPublic DNSサーバなどの他のDNSサーバを参照する方法、ネットワークの障害を確認する方法、さらにはWi-Fiやモバイル等他の通信手段へ切り替えることを理解することで、通常のトラブルに対応することが可能となります。

すでにライフラインとしての役割を果たすインターネットではありますが、電気・ガス・水道と同じように供給網に頼るだけでなく、仕組みを利用者自らが理解することで、さらに利便性が増すと考えます。

長谷部 克幸
（はせべ　かつゆき）

プロフィール

エヌ・ティ・ティ・コミュニケーションズ株式会社ネットワークサービス部担当部長。国内外NTT研究所において計算機ネットワーク、分散情報提供システム、分散IXの研究開発に従事するとともに、ネットワークの設計・構築・運用を行う。NTTでの国内外IPビジネス立ち上げに従事。情報通信研究機構、WIDE Projectにて次世代ネットワークアーキテクチャの研究活動を継続。JPNIC理事（IPv6推進担当）

JPNIC Newsletter for JPNIC Members

No.67

NOVEMBER 2017

CONTENTS

特集1 Special Article

RPKIのAPNICとの連携開始! 海外からも国内経路が検証可能に

～ RPKIの最新動向とルート・リークの対策について ～

2017年7月の下旬にAPNICとJPNICとの間で、RPKIシステムの連携が始まりました。RPKI（リソースPKI）は、IPアドレスなどが記載された電子証明書を発行する認証基盤の技術です。電子証明書を応用することでBGPにおける経路情報をチェックし、不正な経路情報を検知する仕組みとして使うことができるもので、今回のAPNICとの連携によって、国内からだけでなく海外からも、日本の経路情報が検証できるようになりました。

本稿では、この連携の意義についてまとめるとともに、AS運用者が本来は広く公開する意図はなかったにもかかわらず、設定ミスなどによって優先度の高い経路情報が流れてしまうルート・リークについて取り上げ、その対策を考察します。

RPKIの証明書チェーンを本来の形に

リソースPKI（RPKI）は、IPアドレスやAS番号といった、番号資源の分配を証明する認証基盤です。RPKIで配布する電子証明書であるリソース証明書は、レジストリの木（ツリー）構造に合わせた形で発行されるのが本来の形です 図1 。しかし、RPKIは個々のRIRやNIRが独立して作り始めたため、これまではレジストリの木構造の途中からという形になっていました。

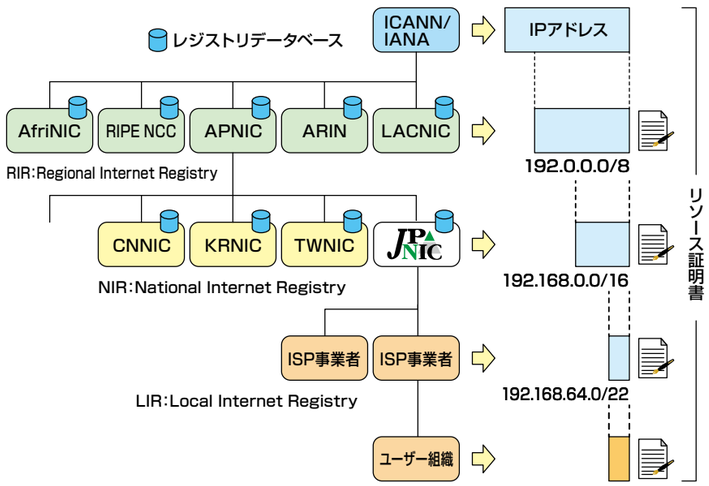
APNICとの連携に至るまで

RPKIを実現するシステムは、地域インターネットレジストリ（RIR）や国別インターネットレジストリ（NIR）といったレジストリがおのおの運用する認証局システムを連携させて、IPアドレスの分配について整合性を保ちながら稼働する仕組みになっています。RPKIシステムは、レジストリデータベースとのデータ連係とともに上位認証局との間で、リソース証明書に記載するIPアドレスについての整合性を保つ連携を行う必要があります。

JPNICでは、まずは試験提供として、2015年3月からRPKIサービスを開始しました。サービス開始当初は、APNICとの連携に先立って、JPNICが分配したIPアドレスのリソース証明書を利用できるようにするために、JPNICのレジストリデータベースに基づくリソース証明書を発行しました。そのため、JPNICから分配されたIPアドレスのリソース証明書は、JPNICのトラストアンカー※1を使って検証する形になっていました。

APNICのRPKIシステムとJPNICのRPKIシステムで、システム間の連携を実現するためには、いくつかの課題がありました。連携システムの開発作業中にもRPKIに関する技術の標準化が進んだことで、連携の形式などにも変更が発生し対応が必要になりました。また、APNICにおける証明書の発行方法が、他のRIRと比べて特殊な方式であったこと※2も、連携にあたって解決しなければいけない課題でした。これらの課題はすべて、実際にRPKIのシステムを運用しながら開発したものを、連携のためのシステムに組み込んでいくような技術課題でした。こういった課題の解決にあたってはAPNICとJPNICの双方で取り組み、APNICで複数の連携形式に対応してもらったり、JPNICでさまざまな証明書ツリーの形に対応できる改良を行ったりすることで、この度の連携が実現しました。

図1 RPKIのリソース証明書の構造



ROAを使った経路広告元の検証も可能に

RPKIを使う仕組みの一つに、ROA（Route Origination Authorization）を使ったBGP経路のオリジン検証（Origin Validation）があります。これまでは、JPNICが分配したIPアドレスを含むROAは、JPNICのRPKIの証明書ツリーを辿ることでしか署名検証を行うことができなかったため、JPNICのトラストアンカーを使わなければ、検証することができませんでした。

この度の連携によりこういった制約が解消され、APNICのトラストアンカーを使って、JPNICのRPKIシステムを使って発行されたROAが検証できるようになりました。RPKI ToolsやRPKI Validatorといった、デフォルトでRIRのトラストアンカーしか持たないオープンソースソフトウェアで、JPNICの分配アドレスを含むROAを検証できます。

BGP経路モニタリングへの応用

BGP経路のモニタリングを行うサービスの一つに、BGPMONがあります※3。BGPMONでは、RIRのトラストアンカーを使ったROAの検証が行われていました。この度の連携によって、JPNICから分配されたIPアドレスについても、BGPMONでROAの検証結果が見られるようになりました 図2 。

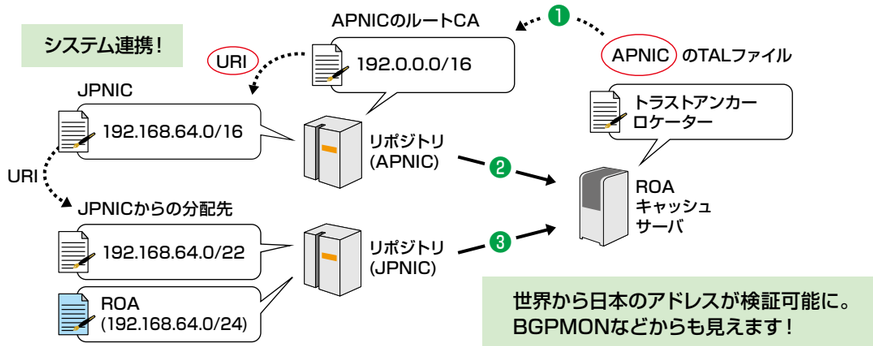
APNICとNIRの連携に役立つ仕組みに

APNICが担当するアジア太平洋地域は、五つのRIRの中でNIRがもっとも多く存在している地域です。各国のNIRから分配された番号資源のRPKIを構築していくにあたっては、それぞれのNIR単位で、自身のリソース証明書を発行する形が考えられます。その際に、各NIRとAPNICとの間でJPNICと同様の連携を行おうとする場合には、この度APNICとJPNICで得られた知識や仕組みが役立つと思われます。JPNICでは、2017年6月にRPKIサービスを開始しAPNICとの接続に向けた作業が進められているCNNICと技術的な情報交換を行っており、双方で技術ノウハウが蓄積されつつあります。

ルート・リークとBGPsec

ルート・リークとは、本来は特定のASや特定のASの間だけで使われている細かい経路情報が、他のASに伝わってしまうことを言います。意図的に細かい経路を扱うことで、ネットワーク的に近い経路を作るといった制御のために使われています。通常は他のASに伝わってしまわないような設定がなされていますが、設定変更のタイミングなどで自AS外に流れてしまうことが起こり得るため、可能な場合には経路情報を受け取るASでフィルタリングするといった対策が採られています。ここで言う細かい経路とは、IPアドレスにおけるネットワーク部を示す、ビット長の長い経路情報のことで、長いほど少ない数のノードを収容したネットワークを示します。例えば、「172.16.0.0/22」よりも「172.16.0.0/24」の方が長い（細かい）経路となり、BGPを使った経路制御においては短いものよりも優先されます。2017年8月25日に起きた通信障害は、このルート・リークが原因とされており、その検知と各ASで利用できる対策技術が、BGPオペレーターの間で話題となっています※4。

図2 APNICのトラストアンカーを使って JPNICから分配されたIPアドレスを含むROAが検証できる



※1 JPNICのトラストアンカー
リソース証明書は、トラストアンカーからツリー状に発行された証明書を収集して検証されます。JPNICのトラストアンカーを使うための設定ファイルであるTAL（Trust Anchor Locator）を下記で公開しています。
https://serv.nic.ad.jp/capub/rpki/jpnic-preliminary-ca-s1.tal

※2 APNICの証明書発行方式
APNICでは、他のRIRから移転されたIPアドレスを別々の認証局で扱うために、トラストアンカーを五つ設けています。2017年10月現在、2018年1月の作業完了をめどに、トラストアンカーを一つに統一する計画が進められています。

※3 BGPMON
https://bgpmon.net/

※4 IRS27 - Inter-Domain Routing Security
http://irs.ietf.to/wiki.cgi?page=IRS27

ルート・リークは、これまでにも国際的に起きているもので、リークそのものをなくすよりも、他のASで影響を受けないようにするにはどうすればいいのか、といった議論が行われてきました。前述の通り、RPKIの連携によって、国際的に日本国内のIPアドレスを検証できるようになりましたので、ここではRPKIを使った経路情報の検査技術であるBGPsecを使って、どのような対策を採ることができるのかについて、考察してみたいと思います。

BGPsecは、BGPの経路情報に対して、オリジン検証(Origin Validation)とパス検証(AS Path Validation)の、2種類の検査を行うことができる技術です。パス検証はまだ実装が進んでいませんが、オリジン検証のオープンソースソフトウェアや、その結果を扱うことのできるルータは増えてきています。

まずはじめに、今後の普及を見越してパス検証の利用について考えてみます。現在の仕様では、ルート・リークが起きた時にも、その経路情報を受け取ったASが正常な署名を付けてしまうことが考えられます。そうすると、ルート・リークの経路が有効なパスとなってしまいます。

受け取ったパスを自動的にASパスに対する署名データであるBGPSEC_PATHに加えるのではなく、指定したASが含まれるパスのみに署名をつけることによってこれを回避し、異常を発見するために使うことができるかもしれません。ただし、まだこのような仕様についての議論はなされていない状況です。この他に、パス検証を行う側で、X.509証明書の証明書チェーンに深さ制限を設けられるように、検証するパス(BGPSEC_PATH)の長さに制限を設けることも考えられます。

また実装にあたっては、RPKIの導入効果について研究しているボストン大学のSharon Goldberg氏が指摘しているように※5、環境によっては受け取ったパスの検証結果がinvalidであっても、使わざるを得ないことも考えられます。パス検証はまだ実験できる状態になっていないため、ルータにおける実装の要件を見つけていくために、各種の想定実験が必要と考えられます。

次に、オリジン検証で検知できることについても考えてみます。ROAには最大プリフィクス長を制限するパラメーターがあり、リーク時の細かい経路が、異常である旨の検知ができる可能性があります。ただし、検知後のアクションに制約があり、優先度を下げた程度では、BGPにおける細かい経路情報を優先する原則が優先されてしまうため、せっかく無効と判定できた経路情報であっても、その判断を経路変更の判断に利用できないという指摘があります。

ここまでで述べたように、RPKIの利用環境は整備されつつありますが、各種のルーティングにおけるインシデントを検知し、もしくは予防する技術に至るまでには、まだ課題があります。実用化のためには、さらなる実験や、ツールの開発を行っていく必要がありそうです。

(JPNIC 技術部／インターネット推進部 木村泰司)

※5 BGP Security in Partial Deployment, Robert Lychev, Sharon Goldberg, Michael Schapira, SIGCOMM'13, August 2013
http://www.cs.bu.edu/~goldbe/papers/partialSec.pdf

JPNICの後藤滋樹理事長がISOCインターネットの殿堂入り

2017年9月18日17時半(PDT、JSTでは9月19日9時半)、Internet Society(ISOC)が、2017年選出の「インターネットの殿堂(Internet Hall of Fame)」入りメンバー 14名を発表しました。その中で、JPNICの理事長を務める後藤滋樹(早稲田大学 理工学術院 基幹理工学部 情報理工学科 教授)が、「インターネットのグローバルな成長と利用に著しい貢献をした個人」として「グローバルコネクター部門」にて殿堂入りを果たしました。

・Visionaries Who Helped Shape the Internet Take Their Place in the Internet Hall of Fame
https://www.internetsociety.org/news/press-releases/2017/visionaries-helped-shape-internet-take-place-internet-hall-fame/

今回の殿堂入りにあたって後藤本人からのコメント

今回の殿堂入りの理由となっている複数の業績は、いずれも私1人が成し遂げたものではありません。多数の友人が実践してくれたものです。先輩の理解と指導も不可欠でした。本来はグループとして顕彰されるべきものです。たまたま私が職場の仲間の年長であったり、大学人は中立であるという想定で、私が名前だけの代表のようになった経緯があります。ただ、私が個人的に遠慮をすると、多くの友人の業績が埋もれてしまうかもしれないと考えて、仲間を代表する気持ちで受けることにしました。関係各位に厚く御礼申し上げます。

・Interview:2017 Internet Hall of Fame Inductee Shigeki Goto
https://youtu.be/n-ds-qBwQXY

・2017年 インターネット殿堂入りメンバー一覧
https://www.internethalloffame.org/inductees

理事長の後藤をはじめ、JPNICは今後もより一層、国内外のインターネットの発展へ貢献してまいります。

特集2 Special Article

Internet Week 2017 ~向き合おう“グローバル”インターネット~開幕!!

Internet Week 2017を11月28日(火)～12月1日(金)の4日間で開催します。
本号の特集では、実行委員長の挨拶とともに、概要をお知らせします。

「Internet Week 2017『向き合おう“グローバル”インターネット』を開催します」

JPNIC 理事／Internet Week 2017実行委員長 高田寛

Internet Week 2017 (IW 2017) を、東京・浅草橋駅前の「ヒューリックホール&ヒューリックカンファレンス」で、2017年11月28日 (火) ～12月1日 (金) に開催します。掲げるテーマは、「向き合おう“グローバル”インターネット」です。

インターネットは、inter- (相互の) 、netというその名の通り、世界中のコンピュータネットワークが相互接続され形成されるネットワークシステムです。相互接続と拡張のしやすさでは群を抜くプロトコルであるTCP／IPの浸透や、WWWというWebシステムの普及などで、インターネットはボーダーレスで低価格、そして望めば誰もがあらゆる情報をやり取りできるプラットフォームになりました。

このインターネット、あえて“グローバル”を強調せずとも、グローバルに動くことこそがもっとも大きな特性、そして利点として発展してきました。しかし今、この“グローバル”という特性に、揺らぎが出てきているのではという点が、今年のインターネットやInternet Weekを考えるにあたり、実行委員、プログラム委員から発せられた問題意識です。

小さかったインターネットにさまざまなプレイヤーが現れ多様化し、インターネット自身が大きくなってグローバル化やフラット化を促す過程で、脅威や分断も顕在化し始めました。また、グローバル化の反動という意味でのローカライゼーション、反グローバライゼーションも進んでいます。さらには、グローバルなプラットフォーマーの台頭で、情報収集の効率化やシステム構築の容易性は高まったものの、彼らの意向次第で大きく左右される世界は、「自律・分散・協調のインターネット」の理念からは少しずつ離れていっていると感じる方もいるでしょう。

もちろんこうした傾向がすべて悪いことだということではありません。しかし今年は「インターネットシャットダウン(＝政府による政策的なインターネットの遮断) をする国があった場合に、アドレス空間の回収、分配禁止を行うべき」などという技術コミュニティによる制裁のような極論まで飛び出し、私たちは今、本当の意味での「協調」が試されているターニングポイントにいると感じています。これからのインターネットを良いものにするためにどのように運営していくか。Internet Week 2017は、インターネットの運用に携わる方々が一堂に会する場です。こうしたインターネットの現況にあらためて向き合い、考え、今後のより良いあり方を議論する契機にしていきたいと思います。

こうしたことを根底に置きつつ、今年も数多くのおもしろいプログラムを提供していく予定です。インターネットに関わる技術者の方々とインターネット基盤技術や社会的な最新動向を共有し、不測の事態に適切に対応できる環境の実現をめざす場として、年に一度のこの場を大いに盛り上げていきます。

今年も、多くの皆さまとお会いできることを楽しみにしています。

Internet Weekのプログラムを企画する委員会の様子

Internet Week 2017 プログラム

1日／半日プログラム　[D1]事前 ¥13,000｜当日 ¥20,000　[D2]事前 ¥11,000｜当日 ¥16,000　[D3]事前 ¥12,000｜当日 ¥18,000

2.5hプログラム　事前 ¥5,500｜当日 ¥8,000　ハンズオン　事前 ¥13,000｜当日 ¥20,000

懇親会　[K1]事前/当日:¥8,000　[K2]事前/当日:¥5,000　同時開催イベント　無料　ランチセミナー　無料　BoF　無料

11／27［月］

	2F ホール	3F Room0
13:00〜18:00	【P1】IPv6 Summit in TOKYO 2017 主催：一般財団法人インターネット協会、IPv6普及・高度化推進協議会	
18:30〜20:30		【K1】itojunに世界的なIPv6普及の進展を報告する会 主催：itojunに報告する会実行委員会

11／28［火］

	2F ホール	3F Room0	3F Room3
9:30〜12:00	【D1】サイバー攻撃に耐える組織と運用 第1部 9:30-12:00 サイバー攻撃最前線2017 セキュリティ	【S1】企業ネットワークIPv6導入指南 〜IPv6対応、進めてますか？〜 IPv6	【S2】君は本当のブロックチェーンを知っているか？ 〜使いどころがわかる150分〜 最新技術
12:15〜13:00	【L1】グローバルDNSは黄金期に入る ［提供］Nominum, inc.		
13:15〜15:45	第2部 13:15-15:45 今求められるSOC、CSIRTの姿とは 〜世界の攻撃者をOMOTENASHIしないために〜	【S4】トラフィックエンジニアリング 〜トラフィック爆発への戦略戦術〜 NW運用管理	【S3】必修・IPv6セキュリティ 〜未対応で大丈夫ですか？〜 IPv6
16:15〜18:45	第3部 16:15-18:45 プロから学ぶ！ 侵害に耐えるサイバーレジリエンス	【S6】今を知り今後に備える！ ルーティングセキュリティ NW運用管理	【S5】テレワークで変わった？！ 働き方の未来 社会派
19:00〜20:30		【B1】これからの生き方と働き方、 技術者目線の3つのポイント	【B2】Peering in Japan BoF

11／29［水］

	2F ホール	3F Room0	3F Room3	3F Room4
9:30〜12:00	【S7】IoTもおまかせ！サーバレスで変わる インフラとの関わり方 最新技術	【H1】インシデント対応 ハンズオン2017	【S8】エンジニアのための 法制度と実務概説 社会派	
12:15〜13:00	【L2】ロンドン五輪会場を支えたNWインフラ BT Diamond IDシリーズのご紹介 ［提供:ジェイズ・コミュニケーションズ株式会社］			
13:15〜15:45	【S9】まるわかりIoT講座 〜スタートダッシュを 決める150分〜 最新技術		【H2】これでわかる！ セグメントルーティング ハンズオン NW運用管理 最新技術	【J1】第33回JPNIC オープンポリシーミーティング (JPOPM33) 主催：ポリシーワーキンググループ
16:15〜18:45	【S11】知らないと困る?! 認証局とHTTPSの最新動向 基盤サービス セキュリティ	【S10】転ばぬ先のIoTセキュリティ 〜コウカイする前に知るべきこと〜 セキュリティ 最新技術		
19:00〜20:30		【B3】ソフトウェアルーター・ スイッチBoF	【B4】インターネットコミュニティBoF 〜インターネット維持・運営のための国際 コミュニティの日本部会を盛り上げよう〜	

11／30［木］

	2F ホール	3F Room0	3F Room3
9:30〜12:00	【S12】キャッチアップ！ 2020に向けたメール運用 基盤サービス	【H3】運用自動化ハンズオン 〜StackStormで実践する インフラ運用革命〜 NW運用管理 最新技術	【S13】国際ローミングの世界と Wi-Fiサービスの今後 NW運用管理 社会派
12:15〜13:00	【L3】向き合おう DNSサーバとサーバ証明書 〜最近のDNSと証明書の関係を踏まえ、運用者がすべきこと〜 ［提供:株式会社日本レジストリサービス］		
13:15〜15:45	【D2】DNS DAY 基盤サービス		【S14】オフィス/公衆Wi-Fiのセキュリティと 混雑解消に向き合おう NW運用管理
16:15〜18:45		【S15】高信頼性運用を実現する SREという新潮流 NW運用管理 最新技術	【J2】第22回日本インターネット ガバナンス会議(IGCJ22)
19:00〜20:30		【B5】日本DNSオペレーターズグループBoF	

12／1［金］

	2F ホール	2F ホワイエ
9:30〜17:30	【D3】IP Meeting 2017 〜向き合おう、"グローバル"インターネット〜	
18:00〜20:00		【K2】懇親会

Internet Week 2017 概要

会期

2017年11月28日(火)〜12月1日(金)4日間

[プレイベント/同時開催イベント]
11月27日(月):IPv6 Summit in TOKYO 2017
itojunに世界的なIPv6普及の進展を報告する会
11月29日(水):第33回JPNICオープンポリシーミーティング
11月30日(木):第22回日本インターネットガバナンス会議

会場

ヒューリックホール&ヒューリックカンファレンス
(東京・浅草橋)

URL

https://www.nic.ad.jp/iw2017/

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)

企画

Internet Week 2017プログラム委員会

協賛

株式会社日本レジストリサービス
Nominum,Inc.
ジェイズ・コミュニケーション株式会社
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
KDDI株式会社
日本インターネットエクスチェンジ株式会社
華為技術日本株式会社
Internet Society

後援

総務省/文部科学省/経済産業省
一般社団法人ICT-ISAC
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)
(ISC)2
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)
国立研究開発法人情報通信研究機構(NICT)
一般社団法人セキュリティ対策推進協議会(SPREAD)
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MSP協会(MSPJ)
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)
一般社団法人日本スマートフォンセキュリティ協会(JSSEC)
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)
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)

登録期間

2017年9月26日(火)〜11月17日(金)

参加費

2.5時間プログラム:事前5,500円(当日8,000円)
1日/半日プログラム:事前11,000円〜13,000円
(当日16,000円〜20,000円)
ハンズオンプログラム:事前13,000円(当日20,000円)
懇親会:5,000円
※無料セッションもあります。

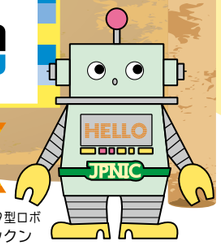
お問い合わせ

Internet Week 2017 事務局(JPNIC内)
E-Mail:iw-info@nic.ad.jp

インターネットことはじめ

第2回 インターネットを支えるTCP/IPの誕生から普及まで

インターネット研究所
ネットソン博士



JP-29型ロボ
ニックン

1973年の開発開始から、2000年代に普及するまで

前号[*1]ではARPANETについて解説しました。今回はインターネットで30年以上使われている通信プロトコル、TCP/IPについてです。

TCP/IPの開発は1973年に始まりました。ARPANETで使われていたNCPに替わるプロトコルとしてです。最初の仕様はRFC 675[*2]として、1974年11月に公開されています。その後、現在のTCP/IPの仕様であるRFC 791[*3]（IP）、792[*4]（ICMP）、793[*5]（TCP）が1981年9月に公開され、1981年11月に公開されたRFC 801[*6]でARPANETのプロトコル切り替え完了日が1983年1月1日と定められました[*7]。

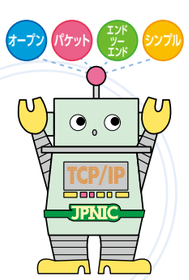
また同じ1983年9月に、TCP/IPを標準サポートした4.2BSDというUnix系のOSが公開されました。ソースコードも含めて教育機関には比較的廉価で提供されたため、RFCとともにTCP/IPのプログラムを作る際に大いに参照されました。この頃はいわゆるUnix系のOSで動作するtelnet、ftp、mailやmhといったところが主なアプリケーションで、インターネット商用化の前でもあったことから、TCP/IPは研究者や技術者が主な利用者であるといった状況でした。

これを大きく変えたのが、1991年に公開されたWWWです。特に、1993年に公開されたNCSA Mosaicというブラウザで、画像を含むファイルをハイパーテキストの形で統合的に扱えるようになり、一気にWWWはブームとなりました。

こうしてWWWがブームとなりましたが、Unix系OS以外、例えば当時使われていたWindows 3.xはTCP/IPには標準対応しておらず、Webブラウザを使うためには別途TCP/IPのプログラムを導入する必要がありました。しかし、1995年のWindows 95の発売で状況は一変します。Windows 95ではTCP/IPが準備されており、加えて「Microsoft Plus!」による拡張機能として同社製のWebブラウザInternet Explorerが無償提供されるようになり、インターネットの商用化の進行とあいまって、TCP/IPが世界的に一気に普及することになりました。

TCP/IPの普及はLANの姿も変えることになりました。当時、LAN内でのファイル共有には別のプロトコルが主流でしたが、インターネットの普及に伴いLAN内でもTCP/IPを使うようになり、Windows、Macintoshともども徐々にではありますが、TCP/IPの利用範囲が広がっていきます。その結果、2017年現在ではLAN内でもほぼTCP/IPのみが使われるという状況になっています。

TCP/IPを特徴づける、四つの項目



TCP/IPにはさまざまな特徴がありますが、代表的な四つとして、オープン、パケット通信、エンドツーエンド、シンプルがあります。

オープンというのは、TCP/IP規格そのものを誰でも無償で自由に参照できることです。仕様が公開されない独自規格や、参照に費用のかかる規格に比べると、開発・実装のハードルが下がります。

パケット通信はデータを複数に分割したパケットの形でやり取りする方法です。通信中に回線を占有する回線交換方式に比べると、一つの回線を複数の通信で同時に使えて回線の利用効率が高まる、ネットワークそのものの堅牢性も向上するといったメリットがあります。

デメリットとしては、通信を制御するためのオーバーヘッドが大きい、帯域保証が難しいといった点が挙げられます。

エンドツーエンドは、複雑なことはなるべく端末側で行い、ネットワークはシンプルに保つという原理、原則です。ネットワークを高機能にすると作るのが大変ですし、使わない機能満載ということにもなりかねません。

シンプルというのは、文字通りです。今日的な観点からはあって然るべき機能[セキュリティなど]もありません。おかげで、比較的作りやすいということになります。

数あるプロトコルの中でTCP/IPが最も普及した理由

TCP/IPが開発された1970年代から1980年代にかけ、広域通信網ではX.25、大型機ではSNA（Systems Network Architecture）、ミニコンピュータではDECNet、パソコンではIPX/SPXやNetBIOS/NetBEUI、AppleTalkなど、それぞれの用途に応じたさまざまな通信プロトコルが使われていました。しかし、TCP/IPはそれらにことごとく打ち勝ち、世界的に覇を唱えることとなりました。

これはもちろん、いくつかの理由が複雑に絡み合った結果です。しかしTCP/IPが本来備えるシンプルさ・オープンさに由来する作りやすさ・使いやすさ、そして、当時普及段階にあったWWWという魅力的なアプリケーション[いわゆるキラーアプリ]にも恵まれたのが大きな理由であることは、間違いないところでしょう。

*1 インターネットことはじめ 第1回 インターネットの先駆け、ARPANETの始まり https://www.nic.ad.jp/ja/newsletter/No66/0320.html
*2 RFC 675 https://tools.ietf.org/html/rfc675
*3 RFC 791 https://tools.ietf.org/html/rfc791
*4 RFC 792 https://tools.ietf.org/html/rfc792
*5 RFC 793 https://tools.ietf.org/html/rfc793
*6 RFC 801 https://tools.ietf.org/html/rfc801
*7 Brief History of the Internet https://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

「インターネットの歴史年表」も見てね!!
https://www.nic.ad.jp/timeline/

次回は、WWWのお話です。

インターネット業界で活躍する“人”をご紹介します

INTERNET YOU

NO. 02

大学共同利用機関法人 自然科学研究機構 国立天文台 / 大江将史

1975年生まれ、2003年奈良先端大情報科学研究科博士課程了。同年、文科省国立天文台天文学データ解析計算センター助手、現、大学共同利用機関法人自然科学研究機構国立天文台天文データセンター助教。同台の情報基盤の設計運用、CSIRT業務、クラウドシステムの設計運用を通して、天文学と情報ネットワークの融合、行動解析に基づくインシデント抑制手法、フラッシュストレージの性能解析に従事。


国立天文台三鷹キャンパス


中継前日に故障したアンテナを修理する大江さん

WIDEプロジェクトのボードメンバーであり、東日本大震災での復興支援にも取り組んでいらっしゃる国立天文台の大江将史さんに、ユニークな経歴、インターネットセキュリティへの問題意識などを語っていただきました。

大江さんのインターネットとの出会い

1台のモデムが人生を変えたと思います。実家は、代々観世流の能楽師を務めており、私は能楽師となるべく修業を積んでいました。能の世界では、役を務めるとご褒美がもらえるという仕組みがあり、中学生2年の頃に興味のあった2400bps/MNP4のモデムをいただきました。そして、通信の面白さに触れ、PC-VAN、Nifty-serve、草の根BBSへの連夜のアクセスや、BBS開局のために徹夜でBBSシステムのプログラミングを行うなど没頭しました。師である父は、没頭する子を見てうすうすダメだと思っていたみたいです。私自身は、能楽師になるつもりで大学に進学しましたが、そこで、不幸にもUNIX（NEWS、FreeBSDとLinux）に出会ってしまい、気持ちは能楽師<コンピューターサイエンスとなり、能楽師への道を離れ奈良先端科学技術大学院大学（NAIST）に進学しました。当時同大学院の山本和彦さんや山口英さんの薫陶を受け、そして、WIDEプロジェクトにて、IPv6、無線LAN、衛星通信、情報セキュリティなど、さまざまなことに取り組みました。

国立天文台での業務

国立天文台では、情報基盤システムの設計運用やSOCを業務としています。また、ネットワークと天文学がリエゾンする課題にも取り組んでいます。例えば、2009年の皆既日食映像を硫黄島から実験衛星でテレビやインターネットへ中継、天文観測データの広帯域伝送などがあります。また、情報セキュリティシステムの開発運用や、フルフラッシュストレージによるクラウドシステムの構築・運用にも取り組んでいます。

大江さんから愛情のこもったメッセージ

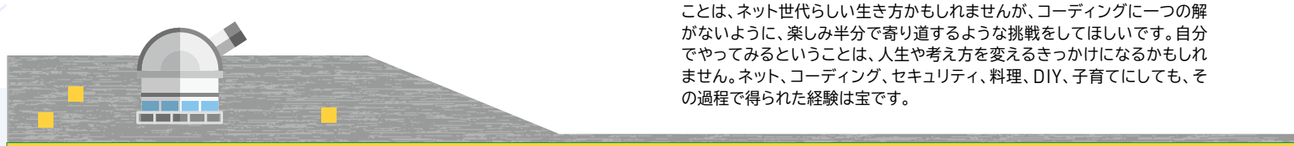
自分は、いい意味で人生を変えた人がたくさんいます。いまの自分があるのは、間違いなく能楽師への道を離れるきっかけとなったUNIXのおかげであり、より学ぼうと進学したNAISTで出会った先生や仲間は、自分の人生を大きく変えたと思います。だから、自分も、人に何か遺せるような生き方をしていきたいと思っています。そして、若い人には、そんないい人に出会えるよう、いろんなことに挑戦してほしいと思います。決めた目標にスマートに進むことは、ネット世代らしい生き方かもしれませんが、コーディングに一つの解がないように、楽しみ半分で寄り道するような挑戦をしてほしいです。自分でやってみるということは、人生や考え方を変えるきっかけになるかもしれません。ネット、コーディング、セキュリティ、料理、DIY、子育てにしても、その過程で得られた経験は宝です。

最近のインターネットに対して思うこと

今の情報セキュリティはいわば城壁を高くし、穴をふさぐ対策に終始しています。しかし、ことの本質は、インターネットを利用する者の情報リテラシーの欠如です。我々は、教育により、道路に飛び出すようなことはしませんし、道端に落ちている水のボトルは飲みません。しかし、今のインターネットは、例えるならば、道路に飛び出す人や封の開いている水を飲む人が多数いる状況で、その対策として、道路に高い柵を作るとか水の検査薬を売るといったことをしているのです。私は、この状況が健全とは感じません。柵や試薬の開発を否定はしませんが、限られたリソースを過度に投入することは問題だと思います。故に、教育システムの長期的な構築が、デジタルネイティブ世代を迎えて、重要なことだと思います。空白期間が長ければ、知識格差が広がり、結果として、社会負担につながります。

技術的に興味のあること

共助したことをブロックチェーン技術により記録し、評価する仕組みがあれば、社会負担を軽減するバイアスがかかるのではないかと思います。例えば、車の運転において、直進車が右折車への進路を譲ることを良しとして評価すれば、対面の渋滞が軽減され、道路のインフラコストを軽減できるかもしれません。セキュリティ対策が不十分な人を支援した人を評価すれば、インシデントは減るかもしれません。このように、共助を促す仕組みがあれば、セキュリティ分野では、パラダイムシフトが生じて、適切な産業構造になるのではないかと思います。



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。

誰もが簡単に利用できるITの実現をめざして

KDDI Web Communications

株式会社 KDDI ウェブコミュニケーションズ

住所：〒107-0062 東京都港区南青山2-26-1 南青山ブライトスクエア10階　　設立：1987年2月25日（ホスティング事業創業 1997年8月）
資本金：6,500万円　　代表者：代表取締役社長　山崎 雅人　　従業員数：175名（2017年8月末時点）
URL：https://www.kddi-webcommunications.co.jp/

事業内容 https://www.kddi-webcommunications.co.jp/corporate/profile/

■ クラウド・ホスティング事業　■ ウェブサービス事業　■ プラットフォーム事業

「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。

今回は、1987年に創業され創立30周年を迎えた、株式会社KDDIウェブコミュニケーションズを訪問しました。同社が提供する「CPI」は、1997年にサービス提供を開始したレンタルサーバ分野では老舗と言えるブランドですが、それにとどまらずWebサービスなど魅力的な製品を、数多く提供しています。

それぞれインターネットという共通点はあるものの、なぜこういったさまざまなサービスを提供するに至ったのか。その背景には「ITを家電のように手軽に扱えるものにしたい」という、創業以来の想いがありました。

当日は南青山のオシャレなオフィスを訪問し、お客様にも社員にも優しくありたいという目的のために、ITやインターネットを便利に活用していく、同社のさまざまな取り組みをうかがいました。

さまざまなサービスは、お客様の生活を便利で豊かにするために

―まずは、貴社の成り立ちや主な事業内容について教えてください。

山崎：当社はIT業界では老舗企業で、今年で創業30周年を迎えます。レンタルサーバー事業の開始からもちょうど20年なので、それぞれ節目の年になります。1987年2月に創業したのですが、そこから10年ぐらいは紆余曲折があり、1997年8月に社名を株式会社CPIに変えて、本格的にホスティング事業に取り組むことになりました。その後は2006年7月に社名をServision株式会社に変更し、2007年10月にはKDDIの連結子会社入り、2008年2月に現在の社名になりました。

事業の柱は大きく三つあります。まず、主力となるクラウドホスティング事業の柱は、1997年から提供しているレンタルサーバの「CPI」です。事業用途での利用が大半で、単にWebサーバ、メールサーバという扱いではなく、お客様にとっては事業資産であり大事なコミュニケーションツールですので、お客様のビジネスを止めないことを使命に日々取り組んでいます。

二つ目のWebサービス事業には、海外サービスの日本展開と、自社開発のサービスがあります。海外サービスで最初に展開したのは「Jimdo」です。HTMLやCSSといった知識なしで誰でも無料で簡単に綺麗なWebページが作れ、現在では140万ユーザーとたくさんのお客様にご利用いただいています。次に、開始したのが「Twilio」で、アプリケーションに電話やビデオなどの機能を組み込むためのAPIです。このAPIを使えば、最小限の開発でさまざまなコミュニケーションの手段を構築できます。弊社の受付端末でもこれを利用しています。また、今年5月から開始したデザイン作成サービスの「Canva」は、専門スキルが不要でポスターや名刺などのデザインが無料で作れるというものです。自社開発のサービスとしては、ビジュアルブログサービスの「g.o.a.t」があります。「g.o.a.t」はビジュアルや書き心地を重視したブログです。

三つ目のプラットフォーム事業は、料金システムの構築や運用業務が大変というお客様向けに、当社が代わりに仕組みを提供するサービスを行っています。どちらかと言うと、企業の裏方のサービスなのであまり表には出ていませんが、ISPやケーブルテレビ様をはじめ、KDDIグループ会社などでも使われています。

―海外サービスの日本展開と自社開発サービスが混在していますが、何か理由があるのでしょうか？

山崎：そもそもきっかけとしては、創業者がITを家電のように手軽に使える世界を作りたいというのがあったんですよね。説明書を見なくても簡単に操作でき、買ってきたらすぐ使える。そういうのをめざしていたんです。その流れで、中小企業の方などがオフィスで困っているいろいろなことを助けたい、ビジネス回りをサポートするサービスを提供していこうと事業を増やしてきて、現在に至っています。その目的のためには、どこ製というのはそれほど重要ではありません。

例えば「g.o.a.t」は自社開発ですが、「Jimdo」はドイツ、「Twilio」は米国、「Canva」はオーストラリア生まれです。自社開発にこだわらず、お客様に便利なものをタイミングよく提供することを優先しているので、良いサービスが見つかれば海外のものでも柔軟に扱うようにしています。

―確かに、貴社のサービスはどれも使いやすそうですよね。「g.o.a.t」のサンプルはお洒落でびっくりしました。誰でも簡単にこんなブログが作れるんでしょうか？

山崎：これは社内での新規事業コンテストがきっかけで生まれた副社長肝いりのサービスなんですが、とにかく書き続けたくなることにこだわっています。使い勝手はとても良いですよ。

そもそも、「g.o.a.t」ではビジュアルを前面に押し出していますが、これは書き上げたものが綺麗なのは当然として、ブログを書きたいけれども最初の一歩が踏み出せない人に、その一歩を踏み出してもらうためでもあるんです。「思わず書きたくなる」「すらすらと書けそうな気がする」というのをめざして作りました。特にサービスを開始した時期は、「保育園落ちた」など、インターネット上にすさんだ話題が多かった頃です。そういう重たいことだけではなく、もっと気軽に楽しいことや面白いと思ったものを発信して良いと思ったんですよね。世の中に清濁がある中で、もっと清の部分を協調したいと。このオシャレなビジュアルなら、ネガティブなものは書き出し辛いだろうという意図もあったんです。

―それはすごく素敵なコンセプトですよね。そう言えば、貴社では最近また新しいサービスを開始されたと聞きましたが。

山崎：この度「キッズコレッチオ」というサービスを開始しました。これはお子さんが描いた絵を、ぬいぐるみやデニムバッグ、アートパネルなどに形を変えて残しておけるサービスです。子供が描いた絵は親にとって大事な思い出なので、なかなか捨てられませんよね。でも、しまっておくと間違えて捨ててしまったり、壁に貼っておくとぼろぼろになったりしてしまいます。お子さんが描いた絵のデータを送ってもらえれば、クリエイターがアレンジを加えて一つずつ手作りで作品にしてくれるんですよ。

職場の制限が、やりたい仕事を妨げない環境作りをめざして

―貴社は2016年に本社を青山に移転されたそうですが、本当にお洒落なオフィスですよね。

山崎：ありがとうございます。窓からの景色は青山墓地ビューですけれどね（笑）。今、立地をお褒めいただきましたがそれだけではなく、社員が働きやすいようにあらゆるところに工夫を凝らしています。その一方で、リモートワークの環境作りにも真剣に取り組んでいます。リモートワーク自体は他社でも取り組んでいますが、オフィス自体の魅力も高めることで「ここにいなくても普通に仕事ができる。でも、オフィスが魅力的だからここにも来たい」と思ってもらえるように頑張っています。どちらか極端に振れるのはよくありません。オフィスでみんなといろいろ話をして業務を進めるのと、リモートで1人でやるのと、成果を上げるという目的に応じて両方を使い分けられる社員になって欲しいと思い、どちらも

選べるように選択肢を用意しています。ベンチャーがこういう取り組みをしても、「ベンチャーだからできるんだ」となってしまうかもしれませんが、KDDIというちょっとまじめそうな会社でもできるんだと知ってもらい、「あそこができるなら、うちも」と、後に続く会社が増えるよう頑張りたいと思っています。

―リモートワークと言えば、貴社には完全リモートの社員もいらっしゃると聞きましたが？


東京メトロ外苑前駅すぐ近くの、南青山ブライトスクエアに本社があります

西村：はい、4人がフル在宅勤務で、北海道、群馬、広島、宮古島で働いています。実は、自分も元々大阪採用だったんですよ。自分で大阪にオフィスを手配して、ここにいる森川が設営にきました。こういった地域採用からスタートする社員もいれば、東京勤務から事情で他の地域に移りリモート勤務になる社員もいます。

山崎：そもそも、当社では「どこで働く」という前提はありません。会社や勤務場所が前提ではなく、「このサービス」や「この仕事」をぜひやってみたいという社員を採用しています。それがすべてで、たまたまこのオフィスに来られない場所にいる社員がリモート勤務になっています。例えば、ここにいる西村が「この人と一緒に働きたい」と思えば採用で、居住地は二の次、三の次です。逆に言えば、「採用してしまったけど、東京に来られないらしい。どうしよう？」「じゃあ大急ぎで環境を作らないと！」という部分もありました(笑)。これぐらいの規模だからできるのかもしれませんが、そういった考えで進めています。

―貴社はなんと沖縄の宮古島！にもオフィスを開設されているのですね。

山崎：これも同じです。宮古島の人を採用したのでオフィスを作らないと、と。また、宮古島市の方々と、島で働くことの可能性や重要性を話してきた中で、宮古島オフィスを開設しました。特に、弊社がオフィスを出すことに障害もなかったですし、政策の後押しにもなればと思い、ワークショップなどを通じてITに触れる機会を増やすようなことを積極的に行っています。宮古島オフィスをせっかく作ったので、合宿などにも使っています。本社の社員でも、宮古島に行って普段はできないことをして、何か成果を持って帰ってきてくれればOKです。環境を変えると新しいひらめきがあるかもしれません。ただ、「移住したい！」という社員にはダメと言っています。動機が不純ですから（笑）。

そもそも、この業界は人材の流動性が高いですよね。定着させることが絶対に良いわけではないですが、やりたいことがあるのに場所の問題で働けないのは残念なことです。それ以外にも、子育てや介護といった問題や、入社後に大学で勉強したくなったなどの理由で、キャリアを途中で諦める人もいます。そういう人が働き続けられる仕組みを作れば、長い目で見れば会社として帳尻は合うだろうという考えで、いろいろな制度を整備しています。

ITを活用した地方創生への取り組み

―沖縄と言えば、貴社は「Cloud ON OKINAWA」という地方創生プロジェクトに参画されていますよね。どういうきっかけだったのでしょうか？

山崎：元々、当社は営業職を多く抱えてはいません。説明しなくても使っていただけるサービスを提供したいという考えからです。とはいえ、知ってもらえないことには使い始めていただけませんので、全国でセミナーを開催し、サービスの活用方法や、使うとどうビジネスが伸びるかなどを紹介しています。最初は自分たちで企画することが多かったのですが、地域の方とも繋がりができて、自治体の方から呼ばれる機会も増えました。地域の課題についてお話を聞くことも多く、もちろん我々の手が届かない分野もあるのですが、可能なことはお手伝いするケースもあります。そういった中で、我々のめざす中小企業の課題解決への取り組みが、沖縄県の課題解決にもなるということでスタートしました。

沖縄は観光が主要な産業ですが、クレジットカードの普及率が低かったり、Webページを持たない企業が多くPRが弱かったりするという、内需拡大をめざし海外からの観光客も呼び込むという点では、まだまだ改善の余地がありました。県庁でもIT化を進めていますが、なかなか一筋縄にはいきません。そこで、そういった分野に強いIT企業にも声をかけて、9社で普及のお手伝いをすることになりました。それが「Cloud ON OKINAWA」です。まず沖縄でしっかりと結果を出して、他の市町村でもこういった活動を広げていければと考えています。

―具体的には、どういったことに取り組んでいらっしゃるのでしょうか？

山崎：さまざまありますが、例えばいま手掛けているのは、沖縄のパッションフルーツ農家さんのIT化です。パッションフルーツは流通手段が従来の卸売販売しかなく、直接農家から買うという方法がありませんでした。パッションフルーツが好きな人でも、市場流通品を買う以外の方法がなかったのです。そこで、Webサイト・ECサイトを活用し、収穫したパッションフルーツを現地以外の人に知って買ってもらうための、仕組みを作るといった取り組みのお手伝いをしています

東京では高価で手に入りづらいですが、現地には安くて美味しいものがあります。ただ、現地と需要地を結びつける仕組みがないために、うまく売れていないという話がありました。そこで、作物の品質を均質にするためにIoTを活用し、また収穫したフルーツを首都圏の人に知って買ってもらうための仕組みを作るといった取り組みをお手伝いしています。これは沖縄セルラー電話株式会社などと一緒にやっています。

また、先ほどご紹介した「Canva」を使って、宮古島の高校生に宮古島市職員の名刺をデザインしてもらうプロジェクトも行いました。コンテスト形式で審査をし、最後まで残った入選作品は、実際に現場で使われているんですよ。

―まさに地方創生の取り組みですね。他にも興味深い取り組みがありましたら紹介してください。

山崎：最近だと、福島県国見町での取り組みに関わりました。国見町を活性化させようと、地元出身の若者が中心に活動を行っている「国見カスタムラボ」のお手伝いをしました。この取り組みを多くの人に知ってもらうためにWebサイトがほしいとのことだったので、実際に現地に行き、「Jimdo」を使用し、サイト作成を一緒に行いました。この活動は、地元のテレビの取材を受けました。

1社ではできないことも、力を合わせればできるというのが「Cloud ON」の良いところです。自分たちだけでは限界がありますが、同じ志を持つ人が集まれば、だいたいのことはできるのではないかと思っています。

JPNICに期待すること

―貴社では今度、会員サービスの一環である出張セミナーを受講していただきますが、JPNICのこういった活動についてはいかがでしょうか？

西村：はい、出張セミナーの制度を利用して、IPv6の勉強会を開く予定です。こういう支援はありがたいですね。IPv6に関しては、少しずつですが導入の動きが広がっていて、官公庁案件なども増えてきています。そうなると、お客様への案内やサポート対応などで、技術者だけではなくスタッフにもIPv6の知識が必要になりますから。

―ありがとうございます。会員の皆さまのお役に立てれば幸いです。今、話が出たIPv6に関するJPNICの取り組みに関しては何かありますでしょうか？

森川：IPv6については、一般の人でも理解できるような普及啓発にも取り組んで欲しいですね。IPv6を導入してもIPv4は不要にはならず、運用コストは倍になってしまいます。ネットワーク側の技術者だけが声を上げてもダメで、エンドユーザーから「IPv6が必要だ」という要望が出てこないと、みんななかなかIPv6をやろうというモチベーションが湧かないと思います。カフェの中で女子高生が「IPv6じゃなきゃ！」とか言っているぐらいになれば完璧ですね（笑）。実際には、サービスを利用するユーザーがIPv4かIPv6かを意識することはまずないので、そういう状況にはなりにくいかとは思いますが。


社内には発表などに利用できるオープンスペースがあります（写真は後日実施したJPNIC会員向け出張セミナーの様子）

もっと言えば、「もうIPv4は使わない方が良い」とか「202x年以降は使っちゃダメ」ぐらいな風潮になると、とてもいいですね。例えば、Windows XP（IE 6）の時は、Microsoft社のサポートが終了したことで、結果的に手間や人的コストを削減でき、作業リソースを集中できるようになったWeb制作会社がたくさんありました。今のままだと、数％でもIPv4を使っている人がいる限り、サポートをし続けないといけませんからね（笑）。

インターネットはもっと自由な発想で、気軽に使っていいもののはず

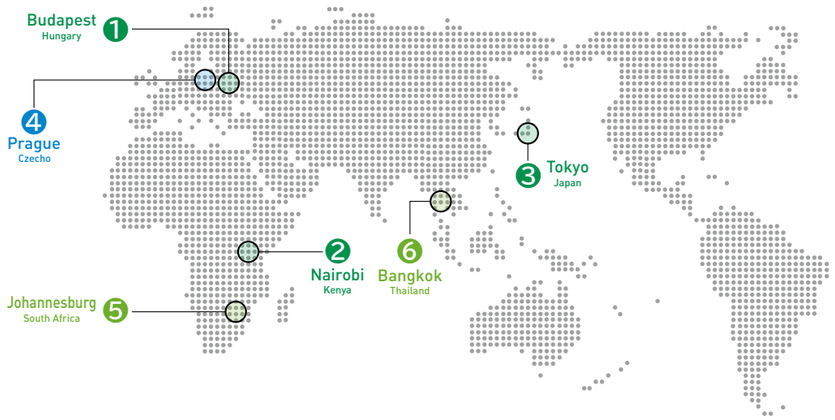
―本日はいろいろなお話のほか、JPNICへのご意見もいただき、ありがとうございました。最後の質問になりますが、貴社にとってインターネットとはどのようなものでしょうか？

山崎：インターネットは本来、存在そのものがグローバルなものです。インターネットを利用することは、一番気軽なグローバルに出て行く出発点なのに、現状はまだまだそうはなっていないように感じます。国外向けと国内向けと、自分たちが垣根を作ってしまっているのは残念なことです。

また、インターネットはいろいろなことをするための手段に過ぎないのに、構築すること自体が目的や課題になってしまう中小企業などがまだまだたくさんあります。でも、もうそんなに構えなくてもいいはずなんです。初期の頃は、環境を構築することは重要かつ大変なことでしたが、今はもっと気軽に使えています。とはいえ、昔のイメージのままで、インターネットを使うことは「難しいもの」、「自分たちには関係無いもの」と思っている人もまだまだいます。

セキュリティの問題とかいろいろ起こっていてその対処も重要ですが、もっと何にでも使って良いし、何でも流して良いと思うんです。インターネットとは、本来そういうものだと思っています。もっと自由な発想の方に時間を使ってもらえるように、より手軽に安心して使える環境づくりのお手伝いができればと思っています。

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



インターネット動向紹介

❶ 2017.5.8▶5.12 ハンガリー/ブダペスト 第74回RIPEミーティング

❷ 2017.5.27▶6.2 ケニア/ナイロビ AFRINIC 26カンファレンス

❸ 2017.6.21 東京/神田 第32回JPNICオープンポリシーミーティング

IPアドレストピック

IPアドレスに関する動向として、2017年5月上旬にハンガリー・ブダペストで開催された第74回RIPEミーティング、2017年5月下旬にケニア・ナイロビで開催されたAFRINIC 26カンファレンス、2017年6月21日に開催された第32回JPNICオープンポリシーミーティングの内容を中心に取り上げます。

第74回RIPEミーティングの動向

◆ RIPEミーティングについて

2017年5月8日（月）～12日（金）にハンガリー・ブダペストで第74回RIPEミーティング（RIPE 74）が開催されました。RIPE NCCは、ヨーロッパ・ロシア・中近東を管轄する地域インターネットレジストリ（RIR）です。APNIC地域では、APRICOT（Asia Pacific Regional Internet Conference on Operational Technologies）カンファレンスが開催され、アドレスポリシーの議論やネットワークの運用に関するさまざまな議論が展開されています。RIPEミーティングは、APRICOTのヨーロッパ版と考えていただければ、イメージできる方が多いかもしれません。


RIPE 74ミーティングの様子

RIPEミーティングでは、その時々で最新の内容が取り上げられ、参加者による活発な議論が繰り広げられるのが特徴です。今回は、アドレスポリシー関連の議論を中心に紹介します。

◆ 全体概要

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

RIPE 74 Meeting Plan
https://ripe74.ripe.net/programme/meeting-plan/

各セッションで利用された資料、発言録、当日の発表風景の映像・音声などは、次のWebサイトでまとめて公開されています。

RIPE 74 Meeting Archives
https://ripe74.ripe.net/archives/

◆ アドレスポリシー提案について

現在、RIPE地域で議論中のアドレスポリシー提案は2点あり、RIPE 74期間中にも議論が行われました。各提案の概要は、JPNIC Blogで紹介しています。

JPNIC Blog：RIPE 74がブダペストで開催中です
https://blog.nic.ad.jp/blog/ripe74-policy-proposal/

2016-04：IPv6 PI Sub-assignment Clarification
（IPv6 PIアドレス再割り当てを明確化する提案）
https://www.ripe.net/participate/policies/proposals/2016-04

2016-04は、割り当てを受けたIPv6プロバイダ非依存アドレスについて、ゲストネットワークやオフィスのWi-Fiホットスポットなど、特定の用途への割り当てを目的とする場合に、再割り当てを明確化するための提案です。前回のRIPEミーティングでも議論が行われたこの提案は、MLでの議論を踏まえた改訂予定の内容がミーティング当日に紹介され、その内容を元に議論が行われました。

用語の使い方について、会場からいくつかのコメントが出されていましたが、提案内容の変更に結びつくような性質のものではありませんでした。反対意見は出されておらず、提案の実装に向けて、着実にプロセスを進めている印象を受けました。

2017-01：Publish statistics on Intra-RIR Legacy updates
（地域内におけるレガシーリソースの統計情報公開に関する提案）
https://www.ripe.net/participate/policies/proposals/2017-01

2017-01は、現在のRIR体制以前に割り当てを受けたIPアドレス・AS番号（以下、レガシーリソース）について、分配先組織に変更があった場合に、その内容を統計として公開することを目的としたものです。

RIPE NCCの管理するレジストリデータベース（以下、RIPEデータベース）は、レガシーリソースの分配先組織とRIPE NCCとの契約手続きが完了していない状態であっても、特に申請者の制限なく登録情報の書き換えが可能となっています。該当のIPアドレスが乗っ取られ、データベース登録情報も併せて書き換えられてしまうと、正当な分配先の特定が難しくなってしまうことを、提案者は懸念しているようです。

会場からは、統計として公開するよりも、データベース登録情報からリソースの分配先を特定できるようすることの方が望ましい、といった趣旨のコメントが出されていました。また、現在のレガシーリソースの管理状況や、データベース登録情報の詳細についてのコメントが多かったように思えました。

RIPE地域におけるポリシー策定プロセスでは、提案に対するコンセンサスの確認はMLで行うこととなっています。オフラインミーティングでの確認は行われませんが、2016-04は提案の実装に向けてプロセスを進めること、2017-01はML上で議論を継続することが、プログラムの最後にチェアから発表されています。

◆ その他ポリシー関連の議論

◎ WHOISの登録情報に関する発表や議論から

IPアドレス・AS番号の分配ポリシーに関連する内容として、WHOISの登録情報に関する発表および議論を紹介したいと思います。

（1）Cooperation WG

このWGでは、IPv4アドレスの共有技術であるキャリアグレードNAT（CGN）を利用した、インターネットアクセスに対する犯罪捜査の事例が、欧州刑事警察機構（European Police Office：Europol）より紹介されていました。

特にモバイル事業者を中心に、CGNの導入が進んでいる現在では、サービス提供事業者から提示されたIPアドレスなどの情報を元に、法執行機関による捜査を進めた場合にも、犯人が特定できないケースがあるとのことでした。ライフル銃の販売サイトを捜査した際には、ポート番号を特定できなかったため、IPアドレス情報の提供を受けたにもかかわらず、運営組織の特定に至らなかったとのことでした。また、児童ポルノサイトの捜査の際には、提供を受けたIPアドレスから、容疑者を50人に絞り込むところにまでは至ったそうです。しかし、このケースにおいてもポート番号を特定できなかったため、この50人すべてに対して調査を行ったことから、当初の予定よりも数ヶ月遅れて解決することとなったそうです。このような状況を受け、CGNの利用自粛や、共有するユーザー数の制限などの動きを取る国も出てきていることが、併せて報告されていました。

会場からは、法執行機関からの要請に対応することが目的でなくとも、ネットワークの運用に必要な情報は、記録しておくことが重要である旨のコメントが出されていました。

（2）データベースWG

データベースWGでも、WHOISの正確性向上のための発表と議論が行われました。この話題は、過去2回のRIPEミーティングにおいて、Europolから継続して発表が行われています。

Europolによると、RIPE NCCのメンバーが、エンドユーザーや2次ISPにIPアドレスを割り当てる際に、割り当て先の情報がデータベースに登録されないか、正しく登録されていないケースが見られるそうです。法執行機関での捜査の際に、RIPEデータベースに登録されたIPアドレスから対象国を特定しようとしても、どの国に協力要請を送ればよいのか判別に迷うことがあり、適切に判断できる情報が登録されている状態になっていることが望ましいとのことでした。

会場からは、RIPEデータベースは、ネットワークのオペレーションに必要な情報を提供するためにあり、データベース登録情報を検索できるWHOISではなく、ルーティング情報を検索できるコマンドなどを利用した方が、特定が容易になるのではないかといったコメントが出されていました。また、RIPEデータベースの登録情報の精度について、発表者と同じような印象や問題意識を持つ参加者もいました。法執行機関での捜査目的ではなくとも、データベースの登録情報の精度向上が図られるのであれば、発表者の考える取り組みには賛成したいとコメントを述べていました。

WHOISの正確性向上のための議論は、RIPE地域だけではなく、ARIN地域やAPNIC地域でも同様に行われています。RIPE地域においては、EuropolがRIPE NCCをはじめとする、関係者との議論を続けているそうです。発表者からは次回RIPE 75ミーティングで、何らかの提案を考えているとの発言がありました。WHOISの正確性向上については、各RIRでの議論の動向を注視し、随時紹介できればと考えています。

◆ 次回以降のRIPEミーティングについて

次回のRIPEミーティングは、2017年10月22日（日）～26日（木）に、アラブ首長国連邦・ドバイでの開催が予定されています。また次々回は、2018年5月14日（月）～18日（金）に、フランス・マルセイユでの開催が予定されています。

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

AFRINIC 26カンファレンスの動向

◆ AFRINIC 26カンファレンスについて

2017年5月21日（日）～6月2日（金）までの日程で、ケニアの首都ナイロビでアフリカインターネットサミット（AIS）'17が開催されました。その中のミーティングの一つとして、2017年5月27日（土）～6月2日（金）にAFRINIC 26カンファレンスが開催されました。AISはAfNOG（The African Network Operators Group）とAFRINIC（African Network Information Centre）の共催で、AF*（アフスター）と呼ばれる、アフリカ地域におけるインターネット諸団体の連合体がパートナーとして参画して、それぞれのミーティングを開催します。そのため、サミットという言葉に引けをとらない、インターネットの大祭典となっています。AFRINIC 26カンファレンスの中から、アドレスポリシーに関する議論について紹介します。


AFRINIC 26カンファレンスの様子

◆ Public Policy Discussionについて

5月31日（水）終日にわたり、アドレスポリシーに関する議論が行われました。提案の一覧は、AFRINICのWebから参照できます。

Policy Proposals
https://www.afrinic.net/fr/community/policy-development/policy-proposals

当日議論されたのは、この中で"Under Discussion"（議論中）と"Last Call"（ラストコール）となっている八つの提案でしたが、うち一つは、他の類似提案との調整が行われた結果、一覧から削除となりました。

この中でもっとも大きな話題を呼んだのは、"Anti-Shutdown-02"提案です。これは、国内から主に海外に対するインターネットによる通信を、政府が政策的に遮断する「インターネット遮断」を行う政府に対するアドレス空間の回収、分配禁止を行うべきとするものです。前日5月30日には、インターネット遮断自体に関して議論するセッションも持たれました。

この他、AFRINICは五つのRIRのうち、唯一IPv4の在庫が残っているRIRであるため、枯渇直前の分配調整のための「ソフトランディングポリシー」が議論されています。どれも当日の議論では賛否とも多く意見が示され、一つを除いて継続審議となっています。唯一、会場でのコンセンサスが確認されラストコールとなったのは、IPアドレスの分配後、利用状況のレビューを行って利用率が足りないものに関してAFRINICへの返却を行うとする、"Internet Number Resources Review by AFRINIC"という提案でした。このように、RIRの厳しい執行を含むポリシーだけがラストコールに至っているというのは、非常に印象的でした。

◆ 次回のAFRINICカンファレンス・AISについて

次回AFRINICミーティングは、2017年11月26日（日）からナイジェリアのラゴスで、1年後の次回AISは、2018年4月29日（日）からセネガルのダカールで開催予定です。

第32回JPNICオープンポリシーミーティングの動向

2017年6月21日（水）に、東京・神田のJPNIC会議室において、第32回JPNICオープンポリシーミーティング（JPOPM32）が開催されました。「JPOPM」は、日本におけるインターネット資源のうちIPアドレス・AS番号等の番号資源の管理ポリシーを検討・調整し、コミュニティにおけるコンセンサスを形成するための議論の場です。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（以下、ポリシーWG）が主催し、開催しています。

ポリシー提案およびWHOIS正確性向上に関するパネルディスカッションを中心に、当日の議論を紹介します。当日の資料や議事録は、次のWebサイトからご覧ください。

第32回JPNICオープンポリシーミーティングプログラム
http://jpopf.net/JPOPM32Program

◆ ポリシー提案について

◎ ポリシー提案 [032-01] 初期割り振り基準に関する記述修正の提案

本提案は、「JPNICにおけるIPv6アドレス割り振りおよび割り当てポリシー」5.2.1項の初期割り振り基準の条項において、「または」「読点」「改行」の組み合わせが複雑であり複数の解釈が生じてしまうため、文章を明確化したいという提案でした。

JPNICにおけるIPv6アドレス割り振りおよび割り当てポリシー
https://www.nic.ad.jp/doc/jpnic-01167.html

本ミーティングにおいて、本提案は「提案」ではなく「校正」と位置付けられ、今後の手続きはポリシー策定プロセス（ポリシーディベロップメントプロセス）に則る対応ではなく、コミュニティからの意見として、ポリシーWGがJPNICに修正が好ましい旨を申し送りし、JPNICで対応を検討することとなりました。

◎ ポリシー提案 [032-02] JPNICにおけるIPアドレスポリシー策定の改定の提案

本提案は、「JPNICにおけるIPアドレスポリシー策定プロセス」における不備の修正や記載事項明確化についての3点および組織名称「ポリシーWG」の改名1点の計4点から成る提案であり、いずれもコンセンサスに至りました。

JPNICにおけるIPアドレスポリシー策定プロセス
https://www.nic.ad.jp/doc/jpnic-01177.html

（1）現文書においては、JPNICのみが臨時ミーティングの開催権を持つことになっているが、本フォーラムを運営するべきポリシーWGにも開催権を持たせる
（2）現文書においては、ポリシーの提案があった場合にWebまたはIP-USERSメーリングリストで提案を公開することになっているが、両方を必須とする
（3）現文書においては、提案者は提案したポリシーに関するQAをJPOPMで行うこととなっているが、IP-USERSメーリングリストとJPOPMの両方で行うことを必須とする
（4）現文書において定義されている「ポリシーワーキンググループ」というフォーラム運営団体の組織名を「JPOPF運営チーム（JPOPF Steering Team）」に改名する

IP-USERSメーリングリスト上での意見照会（ラストコール）の手続きに進み、提案内容への本質的な反対意見がなかったため、IP-USERSメーリングリスト上でもコンセンサスに至りました。

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


コンセンサス確認の様子

◆ WHOIS登録情報正確性向上に関するパネルディスカッション

前回のJPOPM31（2016年11月開催）では、FBI（米国連邦捜査局）の担当者からWHOIS登録情報の正確性に関して問題提起がありました。今回のJPOPM32では、国内の大手ISPや警察庁の担当者が招かれ、国内におけるWHOIS正確性について議論を行いました。

大手ISPは、法執行機関からの問い合わせについて、以下のように分析していました。

・問い合わせ先はWHOISの登録情報を参照しているように思われる。正しい問い合わせ先に連絡を行っている
・連絡は電話または内容証明郵便で行われる。電子メールで行われることは無い
・通常、海外の法執行機関から直接問い合わせが来ることは無い

懸念点はWHOISの正確性より、むしろ通信当事者と開示するべき顧客情報が一致しないことで、例えばPPPoE方式において他人のアカウントの不正使用により取得したIPアドレスを使って犯罪等が行われた場合、対応が複雑化するといったことが挙げられました。また、国内事業者からIPアドレスを割り当てられた日本国外に所在する企業からは、情報の開示は容易ではないであろう、という話がありました。

警察庁は、警察法第1章2条で国民の身体・生命・財産を守るための手段の一つとして、刑事訴訟法で規定されている任意捜査を行っています。この任意捜査の一つとして「公開情報」からの捜査があり、現状公開されていて有効であるWHOISを捜査に使用していると説明がありました。発表者の知る限り、警察庁としてWHOIS検索結果の不正確性により捜査に影響が出た経験は無いとのことです。国際捜査の観点においては、各国の法執行機関同士が緊密に連携を取り合っており、各国の法執行機関には他国の私企業に直接問い合わせ等を行う権限は無いとのことです。最後に、国民の安全・安心のために引き続きWHOISを利用させていただけるよう強いメッセージがあり、締めくくられました。

◆ APNIC 44カンファレンスに向けた事前の意見交換ミーティング

APNIC 44カンファレンスに提出されるポリシー提案に対して、日本のコミュニティの意見を取りまとめるための臨時ミーティングが2017年9月5日（火）に、東京・神田のJPNIC会議室で開催されました。APNIC 44カンファレンスでのポリシー提案の詳細は、JPNIC Blogをご参照ください。

APNIC 44でのIPアドレス・AS番号分配ポリシーに関する提案ご紹介
https://blog.nic.ad.jp/blog/apnic44-policy-proposal/

このミーティングで取り交わされた意見は、IP-USERSメーリングリストで報告が行われました。また、英語に翻訳を行った上で、ポリシーWGメンバーからAPNICでのアドレスポリシーを議論するAPNIC Policy SIGのsig-policyメーリングリストにも共有が行われました。

APNIC Policy SIG
https://www.apnic.net/community/policy/policy-sig/

◆ 次回JPOPM33について

2017年11月29日（水）に、Internet Week 2017の同時開催イベントとして、東京・浅草橋のヒューリックホール&ヒューリックカンファレンスで開催を予定しています。

「IPv6対応状況に関するアンケート」2017結果報告

JPNICがこの数年、毎年継続的に実施しているIPv6対応状況に関するアンケートを、今年も2017年5月16日から6月19日の約1ヶ月間実施しました。

「IPv6対応状況に関するアンケート」2017結果報告
https://blog.nic.ad.jp/blog/2017-ipv6_survey/

今回は、IPアドレス管理指定事業者とPIアドレス割り当て先組織から198件の回答を得ることができました。アンケート結果を見ると、少しずつ進展している状況がうかがえます。引き続き、普及促進、啓発のための活動を進めていく中で、こういった調査結果を広報しながら、IPv6が着実に進展している状況を伝えていきたいと考えています。

インターネット動向紹介

技術トピック

❹ 2017.9.1 チェコ / プラハ　第99回IETFミーティング

技術関連の動向として、第99回IETFミーティングで行われたハッカソンについてと、2016年から2018年にかけて行われているルートゾーンKSKロールオーバーについてご紹介します。

IETFハッカソンの歴史

IETF Meetingでのハッカソン（Hackathon）は、それほど昔から行われていたわけでは無く、2015年のIETF 92（ダラス）で初めて開催され、それ以来毎回のIETF Meetingで行われています。

IETF 92で最初のハッカソンが行われたきっかけは、IETF 91（ホノルル）のLunch Speaker Seriesでの、Cisco Systems社Chief ArchitectのDave Ward氏による講演「Open Standards, Open Source, Open Loop」※1でした。

この講演では、現在のIETFなどの標準化団体（Standards Developing Organization、以下SDO）での、標準化プロセスにおける問題として、

- SDO自体に自己存続のためのバイアスが働くようになっており、例えばホットな新技術に関するグループは、複数のSDOに重複して乱立して分かりにくくなっており、SDO間の調整がうまくいっていない点
- Open Source Software（以下OSS）でデファクト標準ができる期間に比べ、SDOでの標準化には時間がかかる点
- SDOとOSS団体との連携が弱い点

などを指摘していました。そして、IETFにおける改善策として、IETFのモットーである「rough consensus and running code」を引き合いに出し、アジャイル的な手法を用いてrunning codeを標準化プロセスの中に組み込み、会話よりもコード書きやアイデア出しを重視し、より迅速に標準化を行うべきだと述べていました。

この講演への解答として、次回のIETF 92ではCisco社によるスポンサーの元、IETFハッカソンが初めて開催されました。その際に目標として設定されたのは、前述した講演の流れを汲み、running codeを書きIETFへフィードバックすることや、OSSとOpen Standardsの隔たりを埋めることでした。この目標は、現在のハッカソンでも変わっていません。

IETFハッカソンの規模としては、初回のIETF 92では、プロジェクト数（IETF的にはTechnology数）は6プロジェクトだったものが、8回目の開催となるIETF 99では27プロジェクトとなり、過去最大となりました。

IETFハッカソン: DOTS

DOTSプロトコルの実装をテーマにIETFハッカソンに参加されたNTTコミュニケーションズ株式会社の西塚要氏よりご報告いただきましたので一部ご紹介します。

■ DOTSプロトコルとは？

DOTSとは、DDoS Open Threat Signalingの略称です。DDoS対策における（組織間の）防御依頼の標準化をめざして、DOTS WGが2015年に発足しました。IETFの中では比較的新しいWGで、2017年中に「ユースケース」「アーキテクチャ」「リクワイヤメント」の3本のドラフト、および、DOTSプロトコルを策定する2本のスタンダードトラックドラフトのWGラストコールをめざしています。

DOTSプロトコルの有用性を理解するために、現在のDDoS対策について簡単におさらいいたします。あるサービスがDDoS攻撃を受けてしまった時、そのサービスの運用者はどのような対策ができるでしょうか。規模の小さいDDoS攻撃であれば、自組織内で対処ができるかもしれません。しかし、インターネットへつながる回線が輻輳させられてしまうほどの大規模な攻撃であった場合には、上流のサービスプロバイダや専門のDDoS対策事業者に防御（ミチゲーション（緩和）やスクラビング（除去）と呼ばれます）を依頼する他に、回線の輻輳を避ける方法はありません。しかし、防御依頼を受け付ける窓口はメールあるいは電話だったりするかもしれません。そのため、防御を発動するまでの時間がかかり、その間は攻撃が成立し続けてしまいます。

DOTSは、そのような防御依頼の方法について、新しくDOTSプロトコルを策定します。DOTSプロトコルは、利用者側のDOTSクライアントから提供者側のDOTSサーバに対して、攻撃を受けているIPアドレスなどの情報とともに防御を依頼します。依頼を受けたDOTSサーバ側は、認証および防御依頼のバリデーションを実施した上で、DDoS対策を実施します。人間を介さない防御受付のインタフェースが規定されることで、DDoS対策の自動化の道が広がります。また、プロトコル標準化によって、複数の対策事業者に対して共通のプロトコルで防御依頼をすることができるようになります。防御依頼を受けた対策事業者が、さらに別の対策事業者に防御依頼をするような事業者間連携も実現するかもしれません。大きな枠組みで言えば、防御依頼情報をやり取りしてセキュリティオートメーションを実現するプロトコル、と言えます。以上の「自動化による時間短縮」「連携による対策規模と効率の上昇」が期待される効用です。

期待されるDOTSプロトコルですが、現在はまだ標準化の最中です。筆者（注:西塚氏）はDOTSプロトコルのPoC（概念実証）実装となるDDoS対策ソフトウェアの開発を進めておりましたが、DOTSプロトコルの標準化のイニシアティブをとるために、オープンソースとして公開すると同時に、IETF 99においてハッカソンに出場することを決めました。

■まさかの受賞！？

筆者は、株式会社レピダムの岡田耕司氏と一緒に、DOTSプロトコルの実装をテーマとして参加しました。ハッカソンに合わせて、開発中のソフトウェアをGitHubで公開しましたので、当日会場では、実装の変更に加えて、ドキュメントの充実、docker-composeの作成など、誰でも簡単に試す（ディプロイできる）ための開発を実施しました。ハッカソン中は、我々のプロジェクトに興味を持って話しかけてきた人と議論をしたりなど、黙々と作業するだけではない機会も得ることができます。

2日目の午後には、プロジェクトごとに3分ずつ成果を発表しました。ジャッジから2、3の質問を受けますが、
- 何人がプロジェクトに参加していたか
- 実際にこの2日間で達成したことは何か
- WGはどこで、標準化のステータスはどのくらいか

というような質問が共通していました。

最後に、優れたプロジェクトに対する表彰がありました。
- IETF標準に対してどれだけ貢献したか
- 新しい人たちをIETFでの活動に惹きつけることができたか

というのが基準になるとのことです。

自分たちのプロジェクトはまさか受賞しないだろうと思ったので、突然名前を呼ばれた時は驚きました。しかし、受賞した名目は、“Best Name”賞。我々のソフトウェアは、DOTSプロトコルをGo言語で実装しているので、“go-dots”という名称です。“Waiting for go-dots”というタイトルでプレゼンを行ったのですが、サミュエル・ベケットの有名な不条理劇「ゴドーを待ちながら（Waiting for Godot）」をもじったタイトルが好評だったようです。次はぜひ名前ではなく中身で賞を狙いたいと思います。

他のプロジェクトでは、QUICについて、複数の実装間の相互接続性を試験していたチームが、“Best Interop”賞を受賞していました。会場だけではなく日本からのリモート参加もあり非常に活発に活動していました。

各プロジェクトのテーマや写真は、ハッカソンをスポンサーしたシスコ社のブログに詳しく記載されています。


IETF 99の様子

https://communities.cisco.com/community/developer/opensource/blog/2017/07/23/running-code-is-king-at-ietf-99-in-prague

■ DOTS WG での発表

IETF会期中のDOTS WGにおいて、ハッカソンでの経験についてのプレゼン※2を行いました。DOTSプロトコルのオープンな実装としては、我々のソフトウェアが一番乗りでしたので、大変注目されました。

発表では、実際に実装をする上で見つけた、現状のドラフトで考慮が漏れている点や問題点などを、仕様へのフィードバックとして伝えました。この時に実感したのが、“Running Code”を持っていることの強さです。実装をした時に見つけたファクトを元にしているので、発言力が目に見えて変わるのを実感しました。

DOTSに注目している会社として、Arbor社、Radware社、Cisco社、Verisign社などが挙げられます。次回のIETF 100では、ハッカソンにて彼らと相互接続試験をすることをめざします。他のWG参加者に実装を促すことができたのも、成果の一つです。

■ デモ@Bits-n-Bites

IETF会期中に、Bits-n-Bitesという全体の懇親会が開かれます。スポンサーのブースに加えて、ハッカソンの参加者には、成果物をデモすることができる機会が与えられるため、スペースをいただいてデモをしました。デモの内容は、DOTSプロトコルを利用して、ネットワーク越しに、DDoS対策を有効化するというものです。具体的には、RTBH（Remotely Triggered Black Hole）を利用して、DOTSクライアントから伝えられた特定宛先のパケットを破棄するというシナリオです。

Bits-n-Bitesでのデモは、IETF参加者全体に対してアピールできる大変良い機会になりました。DDoS対策に興味を持って

※1 Open Standards, Open Source, Open Loop
https://www.ietf.org/meeting/91/91-speaker-series.html
http://blogs.cisco.com/news/open-standards-open-source-open-loop

※2 Go implementation of DOTS
https://www.ietf.org/proceedings/99/slides/slides-99-dots-dots-hackathon-report-00.pdf

いる参加者は多く、休み無く人が訪れ、説明とデモで忙しかったです。IETF参加者の中でもDOTSプロトコル自体を知らないという人が結構いましたが、DOTSプロトコルの狙いについて理解してもらうだけでなく、動くデモがあるということで、標準化が進んでいる印象を与えることができました。

特に、セキュリティエリアのエリアディレクターであるKathleen Moriarty氏にデモを見せて、よくやってくれたと高い評価を得たことがとても嬉しかったです。中身だけでなく、IETFでのプロトコル標準化に貢献している点が評価されたものと思います。

■ プロトコル実装の難しさと面白さ

ハッカソンをきっかけに、WGでの発表や懇親会でのデモなど、数多くのアクティビティを実施することができました。ハッカソンに参加することで、たくさんの機会や人とのつながりを得ることができるので、IETFに参加されている方には、次回以降ハッカソンにも参加されることを強くお勧めします。

RFC化される前のドラフトに基づいてプロトコル実装をしてみましたが、このフィールドの値が決められていない、値と値の関係がドキュメントでは不明瞭など、数多くの検討箇所を見つけることができました。また、実装にあたって、TLS/DTLSを利用しましたが、よい既存のライブラリが見つからないなど、他のIETFプロトコルの実装の状況に引きずられるなどの問題もありました。今もまさにこのような難しさに直面しているわけですが、まだ決まっていない仕様に対して提案できるというのがまた面白いと感じます。これらは、“Running Code”に価値を置いている、IETFならではの経験と言えるのではないでしょうか。

最後に、OSS化した我々のソフトウェアを紹介します。go-dots自体のインストールは1コマンドで済みますし、docker環境があれば先ほど説明したデモがすぐに再現できます。ぜひ、フィードバックをいただければと思います。

https://github.com/nttdots/go-dots

西塚氏によるレポートの全文は次のURLをご覧ください。➡
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2017/vol1525.html

IETFハッカソン: MILE

IETF MILE（Managed Incident Lightweight Exchange）WGに関わる国立研究開発法人 情報通信研究機構 サイバーセキュリティ研究所の鈴木未央氏よりハッカソン参加のご報告をいただきましたので一部ご紹介します。

■ MILEからのハッカソン参加

筆者（注：鈴木氏）らはこのハッカソンで、自らがMILE WGで関わっているドラフトや、RFCに関係する実装を行いました。読者の中には、MILEがどのようなWGであるかご存じでない方も多いと思いますので、まずMILEについて簡単にご説明します。

◎MILE WGの概要

前提となる問題認識としては、近年増加するセキュリティの脅威に対して、現状では組織間や機器間における、情報共有の仕組みが整備されていないという点が挙げられます。増加する脅威に対して、効率的に防御策を講じるためには、各組織は組織の枠を超えて情報連携、協調、自動化を行う必要があると考えられます。このような認識の元、インシデントレスポンス関連の技術をIETF内で標準化する場所として、MILE WGは発足しました。MILEとは、Managed Incident Lightweight Exchangeの略称となります。MILEの現在のチェアは、Cisco社のNancy Cam-Winget氏と、著者の同僚である国立研究開発法人 情報通信研究機構（NICT）の高橋健志となります。MILEのWebページは、

https://datatracker.ietf.org/ wg/mile/about/

です。

MILEは、IETF内ではSecurity Areaに属し、セキュリティオートメーションに関連する四つのWGの一つです。MILE以外の三つのWGとして、エンドポイントのセキュリティ状態の監視・評価技術の検討を行うSACM（Security Automation and Continuous Monitoring）、DDoS対策のためのシグナリング技術を検討しているDOTS、機器のセキュリティ設定・制御のためのシグナリング技術を検討しているI2NSF（Interface to Network Security Functions）があり、それぞれ異なるテーマを扱っています。

MILEでは、主にインシデントデータのフォーマット、データを交換する際のトランスポート、それらを利用する際のガイドラインという、三つを柱として議論を行っています。MILEは他のWGに比べると、比較的小規模な人数で議論を行っており、IETF Meetingではほぼ毎回にわたって最も狭い部屋でミーティングが行われていますし、普段のMLの流れはそれほど速くはありません。

◎MILEプロジェクトのハッカソン

今回のハッカソンで筆者らが取り組んだ実装は、下記の二つとなります。

- iodef2stix、stix2iodef

筆者らが関わるIODEFと、類似の標準規格であるSTIX（Structured Threat Information eXpression）との間で、フォーマットを相互変換可能なコンバータを実装しました。STIXは、米政府系機関のMITREが主導して標準化を進めているフォーマットで、現在販売されているセキュリティ機器の中には、STIXのフォーマットで出力が可能なものもあります。STIXについて詳しくは、本家のドキュメント※3や、日本語でしたら独立行政法人 情報処理推進機構（IPA）さんの記事※4をご覧ください。

- DAEDALUS IODEFプラグイン

NICTで運用中のDAEDALUSというアラートシステム向けに、IODEF出力を可能とするプラグインを実装しました。DAEDALUSについて詳しくは、NICT Newsの記事※5をご覧ください。この二つをハッカソン中に実装し、GitHubのリポジトリ※6に公開しました。

■ 最後に

最後に、筆者がIETFハッカソンに参加した雑感を述べておきます。筆者は、IETFのハッカソンに参加するのは初めてだったのですが、IETFハッカソンのdutyは、事前のプロジェクト登録と3分の成果発表のみのため、思っていたよりも参加の敷居は低いと感じました。ただし、ハッカソンの期間は実質2日間と短いため、成果を出すためには、プロジェクトのどの部分を事前に準備し、どの部分を期間中に誰が行うかの、事前計画が重要であると思われました。筆者は初めてということもあり、そのあたりの感覚が分からず、あまり事前準備をせずにハッカソンに臨んでしまったのですが、他のプロジェクトの成果発表を聞く限りでは、事前準備をしっかりと行っているプロジェクトが多いように見受けられました。

また、IETFハッカソンのモチベーションという意味では、このような場で作られた標準化前のプロトコルに関わる実装は、そのプロトコルが標準化されたあかつきにはリファレンス実装となる可能性が高く、各社の機器やソフトウェアを実装する際に利用されたり、参考にされたりする場合が多々ありますので、やりがいのあるイベントだと思います。さらに、ハッカソンやBits-n-Bitesでのデモを通して、さまざまな人とのつながりを得たり、フィードバックをもらえたりするのも利点だと思います。

鈴木氏によるレポートの全文は次のURLをご覧ください。➡
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2017/vol1529.html

IETF 99に関するその他の動向

◎全体会議報告

IETFミーティングの全体会議では、米国への入国に関する諸問題によるIETF 102会場の米国以外への変更に関するトピック、およびIETFのWebサイトのデザイン変更に関するトピックがありました。これらについてJPNICの木村がレポートしています。

詳しい内容は次のURLをご覧ください。➡
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2017/vol1524.html

◎セキュリティエリア関連報告

セキュリティエリアでは、量子計算機の実現に先立ち、それに対抗できる暗号アルゴリズムを準備すべきかどうかなどの議論がcfrg（Crypto ForumResearch Group）および saag（Security Area Advisory Group）で行われました。その議論の概要について株式会社レピダムの菅野哲氏よりご報告いただきました。

詳しい内容は次のURLをご覧ください。➡
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2017/vol1527.html

ルートゾーンKSKロールオーバーが行われています・・・あらためて対応のお願い

2016年10月からルートゾーンKSKロールオーバーが行われています。JPNIC Web等でお知らせしています通り※7、この期間中にさまざまな作業が実施されてきました。特に、2017年9月19日にはDNSメッセージの応答サイズが変更される作業が行われました。IPフラグメンテーションの発生に関する影響が懸念されましたが、大きな混乱も見られず無事終了しました。しかしその後の2017年9月28日、ICANNが2017年10月11日に予定されていた新しい鍵での署名開始（実際のロールオーバー）の実施を延期すると発表しました※8。ICANNによれば相当数のリゾルバがロールオーバーに対応しておらず、このまま実施を継続した場合、ユーザーに多大な影響が出る可能性があるため、延期を決定したとのことです。今後のロールオーバー作業がどのようなスケジュールで行われるかは、2017年10月時点では未定です。これらの背景について、JPNIC Blogでご紹介しております※9。対応がお済みでない方はお早めにお願いします。

※3 Cyber Threat Intelligence Technical Committee
https://oasis-open.github.io/cti-documentation/

※4 情報処理推進機構｜脅威情報構造化記述形式STIX概説
http://www.ipa.go.jp/security/vuln/STIX.html

※5 NICT News「対サイバー攻撃アラートシステムDAEDALUSとその社会展開」
http://www.nict.go.jp/publication/NICT-News/1403/01.html

※6 IETF MILE WG
https://github.com/milewg

※7 2017年9月19日以降に一部のDNS応答のサイズ増大によりインターネット利用に影響が出る恐れがあります～DNS、ネットワーク機器の確認のお願い～
https://www.nic.ad.jp/ja/topics/2017/20170802-01.html

※8 ICANNがルートゾーンKSKロールオーバーの実施延期を発表
https://www.nic.ad.jp/ja/topics/2017/20170928-01.html

※9 JPNIC Blog :: 延期となったKSKロールオーバーについて
https://blog.nic.ad.jp/blog/postponed-ksk-rollover/

インターネット動向紹介

ドメイン名・ガバナンス

⑤ 2017.6.26▶6.29
南アフリカ / ヨハネスブルグ
第59回ICANN会議

⑥ 2017.7.26▶7.29
タイ / バンコク
APrIGF2017ミーティング

本稿では、2017年6月～9月にかけての、ICANN（The Internet Corporation for Assigned Names and Numbers）やAsia Pacific regional Internet Governance Forum（APrIGF）などの情報を中心に、ドメイン名およびインターネットガバナンスに関する動向をご紹介します。

ICANN関連の動向

◆ 第59回ICANNヨハネスブルグ会議

南アフリカ共和国のヨハネスブルグで、2017年6月26日（月）～29日（木）の4日間にかけて、第59回ICANN会議（ICANN 59）が開催されました。今回は年3回開催されるうち、「ミーティングB（ポリシーフォーラム）」と呼ばれるポリシー検討に重点を置いた会議で、1万3,000人を超える参加者がありました。

ICANN 59での主な議論の内容は次の通りです。

◎gTLDに関する議論

1. 次回新gTLD募集手続きに関するポリシー策定

本件を検討する作業部会（GNSO New gTLD Subsequent Procedures PDP Working Group）」では、本会議開始時点で以下の結論に至っていました。

・次回以降の新gTLD追加手続きを実施しない理由は見当たらない
・各申請ラウンドにおける申請書または申請者に制限は設けない

会期中は次のトピックスについて議論が行われ、申請者へのサポートについて十分な周知が行われるよう、ICANNにおけるグローバルステークホルダーエンゲージメントチームと本WGのCo-Chairが、対応を相談することが決定しました。

・gTLD申請者への申請支援
・円滑な申請に向けてのRegistry Service Providers（RSP）プログラムの是非
・申請登録が一般に開かれていないgTLD（Closed　Generics）への対応
・レジストリ・レジストラ垂直統合（Vertical Integration）
・政府諮問委員会（GAC）の早期警告に伴う予測可能性への影響
・GAC勧告による申請者の言論の自由への影響
・IDN異体字を扱うTLDsへの対応

また、今後は以下のように作業を進めることが確認されました。

・これまで2回に分けて既に実施した、意見募集の内容を踏まえた暫定報告書を2018年1月に発表・意見募集予定
・その後、提出された意見のまとめを2018年3月に公開検討し、2018年第3四半期に最終報告書を発表予定


理事会の様子

▽gTLDにおける競争、消費者の選択肢と信頼に関する評価（CCT-Review）

第1次報告書案では、新gTLD導入に伴うポジティブな影響を示唆するとともに、効果と成功度合いを計測する上で、データ収集について改善の必要性を指摘しています。

また、DNSの不正利用に関する中間報告書およびドメイン名パーキング※に関するレポートも発表されています。前者によると、不正行為は既存のTLDから新gTLDにシフトしており、特定の不正行為は新gTLD空間の方が多い傾向が見受けられるものの、全体数は増えていないことが示されています。後者のドメイン名パーキングについては、新gTLDにてパーキングされているドメイン名の比率が、既存のgTLDよりも20%高いことが確認されました。

※ドメイン名パーキング
ドメイン名登録業者やホスティング業者などにより提供される、利用していないドメイン名をユーザーから預かるサービスです。そのドメイン名にアクセスした際に、ユーザー自身が構築したWebページの代わりに、業者側が用意したページが表示されるようになります。

2. gTLDにおける国および地域名の登録

この議論は今回の会議における最大の争点となり、複数の場でセッションが設けられ、議論が行われました。

国および地域名の登録をどの程度認めるべきかの検討においては、TLD名における2文字コードの保護以外は合意に至りませんでした。また、GNSOはGNSOポリシーとして検討を進めたいと考える一方、他の関係者はコミュニティ横断での幅広い検討を支持しています。そのため、本会議では今後の進め方（GNSOのプロセスとして進めるのか、コミュニティ横断で検討を進めるのか）についても、合意に至りませんでした。また、2文字だけではなく3文字の国および地域名を登録保護対象にするべきかについても、GAC、GNSO、国コードドメイン名支持組織（ccNSO）で、それぞれ立場が異なっている状況です。これらの議論は、次ラウンドの検討にも影響を及ぼすため、今後の動向が注視されます。

3. 全gTLDにおけるすべての権利保護メカニズム（RPM）の評価

「優先登録」「商標保護」の二つの分類に基づき検討している、各サブチームより進捗報告が行われ、継続検討すべき課題・質問について議論が行われました。また、レジストラへの質問も議題に挙げられ、議論されました。

4. 新gTLDによるオークション収入の扱いに関する検討

2017年8月時点での新gTLDによるオークション収入は、US$ 233,455,563（約256億円）となっています。この収入を割り当てるメカニズムを検討する、コミュニティ横断のWGが設立され、第2回の対面での会合が開催されました。本WGでは具体的な資金の割り当ては行わず、割り当てるメカニズムの検討のみを行います。報告書が2017年末に発表され、意見募集が行われる予定です。

新gTLDによる莫大なオークション収入が、どのような目的の活動に対してどの程度割り当てられるのか、インターネットコミュニティに対してどのように還元されるのかといった観点から、一部関係者からは注視されています。

5. WHOISに代わる次世代のレジストリ検索サービス（Registry Directory Service：RDS）

既存のWHOISにおける、EU一般データ保護規則（GDPR）を中心としたプライバシー保護対応と、次世代のgTLD　WHOISの検討がそれぞれ行われました。

特に、WHOISのプライバシー保護対応はGDPRの影響を検討する上で非常に着目され、現地法への準拠と、WHOISとして必要な機能・対応をどう維持するのかの整理がポイントとなりました。また、新gTLD WHOISに関する検討としては、WHOISに登録する最小限のデータセットについて、コミュニティの意向確認が行われました。本件を検討している作業部会としては今後、2018年春をめどに、全体の提案への意見募集を行うことを想定しているということです。

◎GDPRに関する議論

本セッションでは、ICANN自体、そしてgTLD WHOISへの影響と、今後の対応を確認する議論が行われました。特に、欧州のドメイン名登録者を抱えている事業者の関心は大きいようです。レジストラの中には「GDPRの影響が明らかになるまでWHOISへの情報登録が難しい」との意見も表明されていましたが、議論の結果、gTLDとそのICANN認定レジストラおよびICANN自身がGDPRに完全に適応するためには、まだ遠い道のりであることが確認されました。

◎ICANN説明責任強化に関する議論

コミュニティ横断の作業部会であるCCWG-ACCTの下にある九つのサブグループのうち、ICANNの法管轄を議論するJurisdictionサブグループでの検討に関する議論が紛糾しました。米国が敵対的だと判断した国に対しては、米財務省外国資産管理室（OFAC）による規制が入ること等から、ICANNが米国カリフォルニア法の下で運営されていることについて、ロシア、中国、イランなどが懸念を示していました。ブラジルも、結論として米国の管轄であることに反対はしないものの、プロセスについて問題提起をしていました。一方、これらの意見は全体の中で必ずしも主要な意見ではなく、CCWG-ACCT　Co-Chairは、現行法管轄の下でサービス契約、紛争処理といった各種法的対応への影響・必要な対策の検討を進めることを強く推奨し、現在その方向で議論が進められています。CCWG-ACCT全体としては、2018年6月をめどに最終的な提案の策定をめざして、検討が進められています。

◎強化されたコミュニティの権限の施行

IANA機能監督権限移管後、ICANN説明責任強化に関する対応である新たなコミュニティ権限を行使して、ICANNの基本付属定款の改定をコミュニティ関係者が承認する、初めてのプロセスが施行されました。これに伴い、定義されたプロセスに基づきコミュニティフォーラムが開催され、本プロセスに参加する支持組織・諮問機関として、At-Large諮問委員会（ALAC）、アドレス支持組織（ASO）、ccNSO、GAC、GNSOが改定案へのコメントを表明しました。基本付属定款の改定ではあるものの、実質的な影響はないため、プロセスを試す上でちょうどよいものとして位置づけられていました。

◎第49回ICANN報告会

本ヨハネスブルグ会議に関する報告会を、2017年8月8日（火）に東京・神田のJPNIC会議室で開催しました。

当日のプログラムは次の通りです。

1. ICANNヨハネスブルグ会議概要報告
2. 国コードドメイン名支持組織（ccNSO）関連報告
3. ICANN政府諮問委員会（GAC）報告
4. ICANN理事からの報告
5. 次世代gTLD RDSポリシー策定WG検討状況報告
6. レジストリ・レジストラ関連状況報告
7. 次期新gTLD募集手続き検討状況報告

本報告会の資料および音声は、次のURLで公開しています。

第49回ICANN報告会
https://www.nic.ad.jp/ja/materials/icann-report/20170808-ICANN/

◎次回のICANN会議

次回の第60回ICANN会議は、アラブ首長国連邦（UAE）のアブダビで、2017年秋に開催される予定です。本アブダビ会議の報告は、2018年3月発行の次号68号で取り上げる予定です。

ICANN60 | Abu Dhabi（2017年10月28日～11月3日）
https://meetings.icann.org/en/abudhabi60


ICANN報告会の様子

◆ その他ICANN関連の話題

◎ICANN理事の活動紹介

昨年2016年11月からICANN理事を務めているJPNICの前村昌紀が、ICANN理事の日々の業務や、理事の目から見たヨハネスブルグ会議の様子をブログ記事としてまとめました。いつもの会議報告とは、また異なる目線でのレポートをお楽しみください。

ICANN理事業務の一コマ
～ヨハネスブルグ会議の様子から～
https://blog.nic.ad.jp/blog/icann-board-activity/

◎WHOISにおけるプライバシー／プロキシサービス

WHOISはインターネットにおいて、管理責任の所在を示し、トラブル解決の際にとても有用なデータベースです。一方、氏名や連絡先が公開されることから、登録に躊躇するユーザーも一定数います。そのような需要に応え、ドメイン名を登録する際に登録者の連絡先ではなく、登録業者などの連絡先を代理（プロキシ）で表示するサービスが各社から提供されています。こういったサービスは便利ではあるものの、利用にあたっては注意が必要な面もあります。サービスが生まれた背景や、各TLDにおける状況、注意点などをブログ記事としてまとめました。サービスの利用を考えられている方は、利用前にぜひ一度ご覧ください。

WHOISにおけるプライバシー／プロキシサービス
https://blog.nic.ad.jp/blog/whois-privacy-proxy/

◎ICANN神戸会議の開催が決定

ヨハネスブルグ会議の会期直前に開催されたICANN理事会の決議に基づき、2019年3月に第64回ICANN会議の神戸での開催が決定しました。これまで以上に、ますます日本からのICANNへの貢献を高めていければと思います。

・第64回ICANN会議（2019年3月）の日本での開催が決定
https://www.nic.ad.jp/ja/topics/2017/20170628-01.html

◎David Conrad氏とのオープンセッション

2017年9月1日（金）にJPNIC会議室にて、ICANN最高技術責任者（CTO）David Conrad氏とのオープンセッションを、ICANNとJPNICの共催で開催しました。会場は満席となり、加えて遠隔参加者も30名以上にものぼるなど、大変盛況の会合となりました。

当日はConrad氏から、次の内容についてたっぷり話していただきました。
・CTOオフィスの活動
・DNSSEC普及状況
・ルートゾーン鍵署名鍵（KSK）ロールオーバー
・IPv6普及状況
・識別子システム関連の不正利用
・IANA機能を担う組織Public Technical Identifiers（PTI）の現状

その後の質疑応答セッションでは、技術的な質問および技術以外の質問との両方が活発になされましたが、Conrad氏は気さくな人柄を感じさせる話しぶりで、いずれにも丁寧に回答されていました。


David Conrad氏との
オープンセッションでの記念撮影

本セッションの当日発表資料は、次のURLで公開しています。

ICANN最高技術責任者（CTO）David Conrad氏とのオープンセッション
https://www.nic.ad.jp/ja/materials/icann/20170901-conrad/

インターネットガバナンス関連の話題

◆ インターネットシャットダウンに関する議論

関連 P.16 AFRINIC 26カンファレンスの動向

「インターネットシャットダウン」とは、国内から主に海外に対するインターネットによる通信を、政府が政策的な理由から遮断する行為を指します。2017年5月21日（日）から6月2日（金）に、アフリカインターネットサミット（AIS）'17の一部として開催されたAFRINIC 26カンファレンスにおいて、この「インターネットシャットダウン」に対抗するための、「アンチシャットダウン」に関する提案が議論されました。この提案は、「インターネット遮断」を行う政府に対する、アドレス空間の回収、分配禁止を行うべきとするものです。AIS'17での議論に先立ち、2017年5月8日（月）～12日（金）にハンガリー・ブダペストで開催されたRIPE 74において情報共有のために紹介されましたが、その際も大きな議論を呼び起こしました。

当日の会場でも、この提案の是非が議論されましたが、一国の政府の政策的な処置に対して制裁を下すような内容のアドレスポリシーであることから、RIRやIPアドレスのポリシーがやるべきことの範囲を超えているとする意見が、政府関係者や技術コミュニティからは多く聞かれました。その一方で、この提案に賛成する声も一定数存在していました。本提案は賛否とも多く意見が示されたことから、継続審議となっています。

このような提案が提出され議論されることは、ポリシー策定プロセスの健全性を示すものですが、こういった議論がされること自体に、いくつかの政府からは大きな懸念が示されています。そのため、AFRINICからは2017年4月に、議論中の提案とAFRINICの関係を明確にする声明※1が、AIS'17会期最終日の6月2日には、インターネット遮断に懸念を示すとともに、アンチシャットダウンポリシーのインターネット遮断に対する有効性を否認する声明※2が、AF*団体合同で公表されています。

このような明確化の努力の一方で、しばらくの間本件に関する議論は続きそうです。

◆ APrIGF 2017

2017年7月26日（水）～29日（土）にタイのバンコクで、Asia Pacific regional Internet Governance Forum（APrIGF）2017ミーティングが開催されました。APrIGFは、アジア太平洋地域におけるインターネットガバナンスに関する議論を行うミーティングです。今年で8回目の開催となり、約45ヶ国から700名近い登録者がありました。

◎今年のテーマ

今年のAPrIGFのメインテーマは、「Ensuring an inclusive and sustainable development in Asia Pacific: A regional agenda for internet governance」です。グローバルな場でも着目されている持続可能な発展に、アジア太平洋地域からの視点を加えることにフォーカスをしています。

◎サブテーマごとの議論

今年は新たな試みとして、各サブテーマについて登壇者が語るパネルセッションが開催されました。ハイライトされたポイントは次の通りです。

・アクセス、エンパワーメント、多様性
僻地や地方、太平洋の小さな島々も含めた接続性、ICTへのアクセスが必要だとして、具体的な取り組みとしてトンガでの光ファイバーケーブルの整備や、フィジーの世界銀行の接続提供プロジェクトへの参加が紹介されました。

・サイバーセキュリティ、プライバシー、より安全なインターネット
データプライバシーとデータ保護にはさまざまな規制があり、企業等に混乱と見通しの悪さが生じているが、中小企業では対応するリソースがないという問題が議論されました。また、国をまたがるデータ移転については、自由な情報の流通を実現できる包括的な規制のセットが必要との意見がありました。

・オンライン上の人権
「オフラインにおける影響」「プライバシーとデータ保護」「ジェンダーとセクシャリティ」の三つの分野において、人権について

問題意識を持った人だけではなく、より幅広い関係者での検討が必要だとされました。

・デジタル経済と革新の実現
オンラインアクセスが限られる人もいるなかで、政府がすべてにおいてデジタル化を進めることは問題だとの認識が示されました。また、企業には政府ほどプライバシー対策が求められないことや、大企業だけに有利な状況をなくす環境整備が必要だという意見がありました。

APrIGFのプログラムは、以下のURLで公開されています。動画や発言録も提供されていますので、興味のあるプログラムがありましたらぜひご覧ください。

APrIGF 2017 Program
https://2017.aprigf.asia/program/

本会合のより詳しいレポートをJPNICブログにて公開しています。詳細については次のURLをご覧ください。

APrIGF 2017 現地レポート
https://blog.nic.ad.jp/blog/aprigf2017/

JPドメイン名関連の話題

◆ 汎用JPドメイン名の累計登録数が100万件を突破

2001年にスタートした汎用JPドメイン名の登録数が、2017年9月1日時点で累計100万件を突破しました。汎用JPドメイン名は、従来の属性型・地域型JPドメイン名とは異なり、「○○○.jp」と第2レベルに直接登録でき、日本に住所があれば法人・個人を問わずに登録できることから導入当初から人気を集めています。

また、汎用JPドメイン名の登録開始にあたっては、2001年5月の先願登録開始に先立ち、2月に既存の属性型・地域型JPドメイン名登録者を対象とした優先登録申請が、4月に先着順による競争を緩和するための同時登録申請が受け付けられました。現在ではこのような仕組みは、「サンライズ」や「ランドラッシュ」という形で、.jp以外の他のTLDにおいても導入されるようになっています。

※1 AFRINICによる声明
https://www.afrinic.net/en/library/news/2131-statement-on-internet-shutdowns-policy

※2 AF*による共同声明
https://www.afrinic.net/en/library/news/2141-common-statement-by-af-on-internet-shutdowns-in-africa

JPNIC

活動カレンダー

JPNIC Activity Report

2017年8月～12月 JPNIC活動報告

JPNICイベントカレンダー https://www.nic.ad.jp/ja/event/

8月

8（火）
東京

第49回ICANN報告会（JPNIC会議室）

ヨハネスブルクで開催された、第59回ICANN会議の内容をお伝えしました。前回に引き続き、次期新gTLD募集や、WHOISの次世代サービスなどが議論されています。

詳細は⇒P.23

9月

1（金）
東京

David Conrad氏とのオープンセッション（JPNIC会議室）

ICANN最高技術責任者David Conrad氏の来日に伴い、主にDNSに関連する話題の解説と、質疑応答が行われました。中でもKSKロールオーバーに関しては質疑も多くなりました。

詳細は⇒P.24

IETF報告会（99thプラハ）（TECH PLAY SHIBUYA）

プラハで開催されたIETF 99では、1,000名以上の参加者が集まり、未来のインターネットに向け、今後の技術・プロトコルについて議論を行いました。また、IETF Hackathonも定着し、多くの積極的な活動が行われました。これらの状況を報告しました。

詳細は⇒P.18

12（火）
東京

第21回JPNIC評議委員会（JPNIC会議室）

10月

2（月）
6（金）
東京

JPNIC技術セミナー（JPNIC会議室）

4月、6月の開催に比べて、やや応用に重きを置いた構成で開催したところ、BGPとRPKIに人気がありました。

19（木）
20（金）
東京

初心者向け「インターネット入門」フォローアップ研修（JPNIC会議室）

4月に行った『初心者向け「インターネット入門」』に続く入門者向けの研修を行いました。今回は比較的少人数でグループワークを行い、コミュニティにおいて人のネットワークを作るという目的も掲げています。

11月 ▼ 12月

8（水）
東京

第121回臨時理事会（JPNIC会議室）

11/28（火）
12/1（金）
東京

Internet Week 2017（ヒューリックホール&ヒューリックカンファレンス）

今年は「向き合おう、“グローバル”インターネット」をテーマに、セキュリティ、最新技術、ネットワークの運用管理、基盤サービスなどの20を超えるセッションとハンズオンを開催しました。

詳細は⇒P.5

後援したイベント

8月22日（火） IoT推進委員会 第7回シンポジウム （東京、日比谷図書文化館）	9月26日（火） Security Days Fall 2017 大阪 （大阪、ナレッジキャピタル・カンファレンスルーム）	
9月26日（火） 第16回迷惑メール対策カンファレンス （大阪、ナレッジキャピタル・カンファレンスルーム）	9月27日（水）～29日（金） Security Days Fall 2017 東京 （東京、JPタワーホール&カンファレンス）	9月29日（金） 第17回迷惑メール対策カンファレンス （東京、JPタワーホール&カンファレンス）

これからのJPNICの活動予定

2018年2月5日（月）～9日（金） JPNIC技術セミナー

2018年3月16日（金） 第62回臨時総会

など

インターネット 10min 分 講座

おさえておきたい基本や、最新動向を解説するコーナーです。

VPNとは（Virtual Private Network）

VPN（Virtual Private Network）は、通信事業者のネットワークやインターネットなどの公衆ネットワーク上で作られる、仮想的な専用ネットワークの総称です。VPNと言っても、通信事業者がサービス化しているようなVPNや、インターネットなどの公衆網を用いるVPN、スマートフォンやPCから利用するVPNのように、多種多様なVPNの仕組みやサービスが存在しています。

本稿ではVPNの入門者に向けて、インターネットや専用線などとの比較から技術的な仕組みに至るまでを全般的に取り上げ、解説します。

1 VPNが必要とされる理由

VPNを使う理由は二つあります。安価に通信内容の漏洩を防ぐことと、ある程度の通信品質を確保することです。

特定の拠点同士を結ぶ技術として、専用線やインターネットを用いた通信が挙げられます。専用線では、物理的に2点間を、他のユーザーなどと共有しない専有ネットワークとして接続します。ケーブルの物理的な経由地を指定することで地理的リスクを避けることも可能ですが、通信路を専有するため非常に高価ですし、1対1（エンドツーエンド）の接続となるため、複数の拠点がある場合にはその数だけ専用線が必要となってきます。その一方で、他のユーザーの影響で障害が発生することや、輻輳して通信ができないなどの問題を考える必要はなくなります。そのため、高信頼性を求めるようなケースで利用されます。

それに対して、インターネットを用いた通信は、通信事業者の設備を数多くのユーザーで共有しているため非常に安価ですが、その反面、通信の盗聴や改ざんなどリスクが存在します。また、インターネットで接続されているすべてのサーバや端末に対して、経由する区間で帯域が保証されていないため、混雑時に通信が遅いといった問題があります。通信内容の保護は暗号化で対応可能ですが、通信品質の確保はそのままでは困難です。

そこで、通信内容の漏洩を防ぎつつ、ある程度の通信品質を確保する手段として、VPN（Virtual Private Network）が利用されるようになってきました。多種多様なVPN技術ですが、ある地点とある地点をセキュアに通信ができるように繋ぐという目的は共通しています。具体的な利用ケースとしては、遠隔地に拠点を持っている企業が拠点間を接続する場合や、手元のPCやスマートフォンなどの端末から、企業の情報システムにインターネットを経由してアクセスする場合等に利用されます。VPNを利用することで、中継点で通信内容が盗聴されたり改ざんされたりするのを防ぎつつ、悪意のある攻撃者から通信を守ることができます。

通信事業者が提供するようなIP-VPN（L3VPN）や広域イーサネット等（L2VPN）のVPNサービスは、専用線より安価かつインターネットより高品質なネットワークとしてサービス化されていることが多いです。そのようなサービスは、インターネットのように設備を複数のユーザーで共有しますが、論理的にユーザー同士の通信を分離し、セキュアなネットワークを提供します。また、ユーザー自身でインターネット等の公衆網を利用して構築する、インターネットVPNがあります。なお、通信事業者でもインターネットを利用したVPNサービスを提供しているケースもあります。

2 VPNの基本的な仕組み

先述の通り、VPNでは多数のユーザーで設備や通信路を共有しています。その設備にユーザーを接続するだけでは、それぞれのネットワークが繋がり通信ができてしまいます。そのため、VPNを実現するためには、装置内や通信路内でユーザーのネットワークごとに論理的に分離する機能が必要になります。また、インターネットを用いたVPN（インターネットVPN）のようにインターネットを通信媒体として利用する場合は、暗号化機能や認証機能を利用するケースが多いです。

装置内でユーザーのネットワークが混ざらないようにするために、ユーザーごとにルーティングやフォワーディングを行うVRF（Virtual Routing and Forwarding）や、VLAN（Virtual Local Area Network）を用いています。また、共有する通信路でのユーザーの論理的な分離は、一般的にヘッダの中にユーザー識別子を挿入するか、データのフレームやパケットを、ユーザー識別子を含んだヘッダでカプセリングすることで実現します。

そのような技術で、ユーザーは、L2VPNではスイッチ、L3VPNではルータに接続しているようにネットワークを利用することができます。

3 VPNで利用される技術

VPNに求める機能や構成の違いにより、プロトコルや仕組みは異なります。特に、OSI参照モデルのどのレイヤーでカプセル化を行うのかにより、選択される技術は大きく異なります。また、バックボーンで利用される技術と、インターネットのような公衆ネットワークで利用される技術でも違いがあります。

まずは、設備や通信路を共有した場合でも、ユーザーごとの通信が混ざらないようにするために、どのような技術を利用し実現されているのかを解説します。

通信事業者のバックボーンで利用される技術

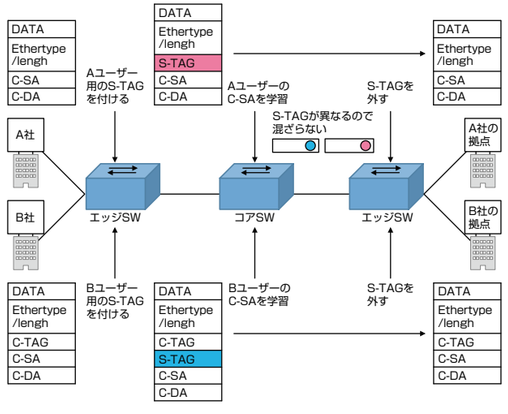
通信事業者によるVPNサービスのバックボーンは、事業者内で閉じているネットワーク（閉域網）で構築されています。また、装置が設置されているようなデータセンターや通信ビルに、関係者以外が立ち入ることができないよう物理的なセキュリティも担保されています。そのため、バックボーン内では暗号化よりも、大容量の通信を処理することができ、多数のユーザーを識別する機能が必要とされます。基本的に、通信事業者がバックボーンを持つVPNサービスでは、VPNに関わる処理は事業者のバックボーンで行われ、ユーザー拠点に設置する装置は基本的な機能のみで実現することができます。

■Layer2VPN（L2VPN）

通信事業者が提供するLayer2VPNサービスは、広域イーサネットとも呼ばれます。最も初期の段階のLayer2VPNでは、IEEE 802.1QやIEEE802.1adで規格化されているVLAN taggingやVLANを重ねる（QinQ）仕組みを用いて、ユーザーごとのネットワークの識別をしています。

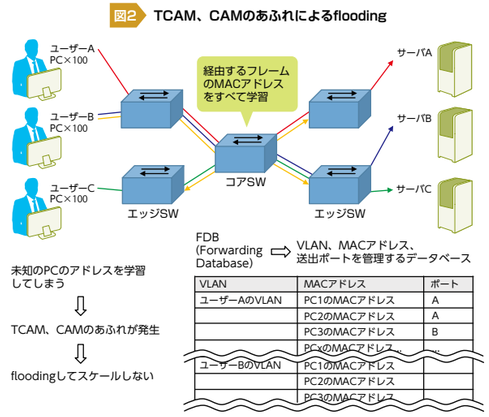
図1 Layer2VPNのイメージ

C-SA	Customer Sauce MAC Address
C-DA	Customer Destination MAC Address
C-TAG	Customer VLAN Tag
S-TAG	Service Tag



スイッチが、ユーザーを接続しているポートから受信したフレームのヘッダにVID（VLAN Identifier）を付加して、バックボーンに送信します。ユーザーの送信元MACアドレス（C-SA）は、経由するすべてのスイッチで学習され、ユーザーの送信先MACアドレス（C-DA）まで転送されます。そして、ユーザーが接続している事業者のスイッチでVIDを取り除き、ユーザーの装置へ転送されます。簡単な仕組みでユーザー分離は可能ですが、経由するスイッチすべてでユーザーのMACアドレスを学習する必要があります。図1

図2 TCAM、CAMのあふれによるflooding

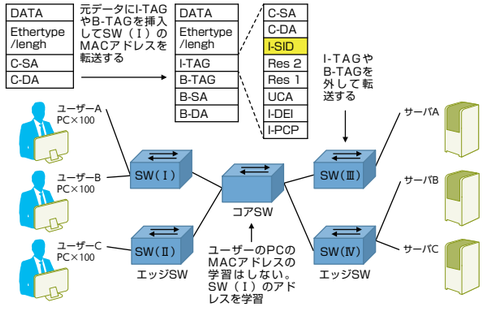


スイッチは高速にフレームを転送するために、CAM（Content Addressable Memory）やTCAM（Ternary Content Addressable Memory）等の特徴的なハードウェアを搭載しています。これらはMACアドレステーブルを検索するために利用されますが、登録できるMACアドレスの数には限りがあります。最大値を超えた場合は、登録できないMACアドレス宛の通信が繋がっているすべてのインタフェースから送信（flooding）されるため、非常に効率が悪くなります（図2の黄緑の通信）。また、VID（VLAN ID）の範囲も12bitしかないため、0-4095の範囲の4096（うち二つは予約済み）のネットワークしか識別ができません。そのため、ネットワーク全体でのユーザー収容数も限られてしまうことからスケールしない仕組みです。その結果、現在では大規模なL2VPNで利用されるケースは少なくなっています。

先述のMACアドレスの増大やVIDの不足を解決するために、IEEE802.1ah（PBB）ないしは類似の独自規格を利用してL2VPNを構築することができます。通称Mac-in-Macと呼ばれるこの仕組みは、通常のフレームにバックボーン区間装置インタフェースのMACアドレスとI-TAG（Service Instance Tag）やB-TAG（Backbone Tag）を付加することで、カプセリングを行います。その結果、コアスイッチは網内にある装置のMACアドレスを学習するだけで済むようになります。ユーザー装置のMACアドレスをコアスイッチが学習する必要がなくなるため、スケールするネットワークとなります。図3

図3 Mac-in-Macのしくみ

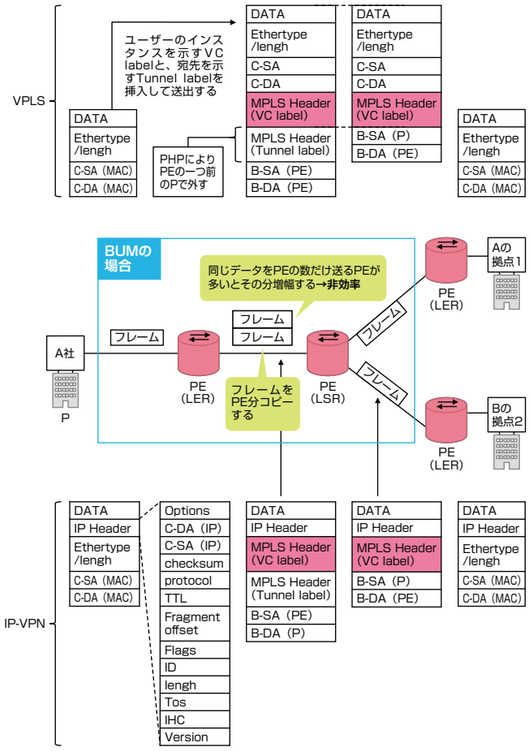
C-DA	Customer Destination MAC Address	B-SA	Backbone Sauce MAC Address
C-SA	Customer Sauce MAC Address	I-TAG	Backbone Sauce Instance Tag
B-DA	Backbone Destination MAC Address	B-TAG	Backbone VLAN Tag
		I-SID	Backbone Service Instance Identifier



しかし、この技術だけで構築するL2VPNには課題があります。標準のEthernet Frameには、ループを防ぐような仕組みがありません。そのため、物理的にループとなるようなトポロジを作ると、BUM（Broadcast, Unknown Unicast, Multicast）がループし続けることになります。ループを防ぐために、送信元MACアドレスを用いたフィルタを行うことや、Spanning Tree系統のプロトコルを利用しブロッキングポート（通信しないポート）を作る必要があります。場合によっては、物理的には隣接する装置であっても、他の離れた場所にあるスイッチを経由するなど、トラフィックの制御が難しい部分もあります。IEEE802.1aq（SPB）とPBBを用いて通信を行うことで、効率的なL2ネットワークを構築することもできますが、導入はデータセンター間のネットワーク等限定的のようです。

前述のIEEE802.1adやIEEE802.1ahでは、EthernetでL2VPNを実現する仕組みでしたが、MPLS（Multi Protocol Label Switching）ラベルを用いた仕組みでL2VPNを実現するためのVPLS（Virtual Private LAN Service）が、RFC 4761／RFC 4762で標準化されています。VPLSは、ユーザーから見ると通常のL2スイッチに接続しているように見えますが、バックボーンでは元のデータにユーザーネットワークを識別するラベル（VC Label）と、ルータ間の転送用（Tunnel label）の二つのMPLSヘッダを付けて転送されます。そのため、コアルータでユーザーのMACアドレスを学習する必要がなく、ユーザーが接続されているPE（Provider Edge）ルータでのみ学習を行えば良いことになります。また、バックボーン区間はL2ネットワークではないため、ループなどの問題を解決することができ、効率的なネットワークの利用が可能となります。

図4 VPLSとIP-VPNの比較



一方で、BUMの処理には課題があります。通常のL2スイッチでBUMを受信した場合は、接続されているリンクすべてにフレーム送信（Flooding）が行われます。VPLSでは、BUMを受信したPEルータが他のPEルータ宛に送信します。この時PEルータは、自分以外のPEルータの数だけフレームをコピーして網に送信します。その結果、必要のないPEルータにも送信することや、増幅したBUMトラフィックが同じリンクに何度も流れることで、帯域の使用効率が非常に悪くなります。図4 また、ユーザーネットワークの数が増えるとPEルータ間の仮想的なトンネル（PW: Pseudo Wire）が大量になり、スケールが難しくなるという課題もあります。

最近では、EVPN（RFC 7432／RFC 7623）のように、Data PlaneとControl Planeを分離した仕組みも標準化されてきました。それぞれのPEルータがData PlaneでMACアドレスを学習していたVPLSの仕組みとは異なり、Control Plane（MP-BGP）で広告することでUnknown Unicastの抑制も実現されています。このような新しい技術も出てきてはいますが、広域イーサネットサービスではMac-in-Macやそれに類する技術、VPLSがまだまだ主流のようです。

■Layer3VPN（L3VPN）

L3VPNでも、VPLS同様にMPLS技術を用いたIP-VPN（RFC2547bis）が利用されています。ユーザーから見ると、IP-VPNのバックボーンが一つの大きなルータのように見えるネットワークを構成します。

IP-VPNでは、MP-BGPによりPEルータが接続されているユーザーのネットワーク情報をそれぞれのPEルータが持っているため、VPLSのようにData PlaneからMACアドレスを学習する必要はありません。ユーザーが接続するPEルータはユーザーごとにVRFを持つことで、個別のRIB（Routing Information Base）を持ちます。パケットを受信したら、宛先のネットワークアドレスをもとに、VC LabelとTunnel Labelが付加されMPLS網へ送られます。最後のPEルータの一つ手前のP（Provider）ルータやPEルータで、Tunnel LabelとVCラベルが取り外され、適切なVRFへ送られルーティングされます。図4

インターネットVPNで利用される技術

インターネットVPNでは、通信事業者が持つようなバックボーンが存在しないため、ユーザーの拠点に置かれる装置の機能を利用し、インターネット経由でそれぞれの装置を接続します。さまざまなプロトコルが存在しますが、多くのルータでIPsecの実装があり利用されています。

IPsecは、暗号化技術や認証技術を用いて、通信が盗聴されたとしても内容が漏れることを防ぐことや、改ざんの検知などを行えるようにするための仕組みです。IPsecでは目的ごとにプロトコルを選択することができ、暗号化により通信が漏れても内容がわからないようにするためのESP（Encapsulating Security Payload）や、ESPよりも多くのヘッダ部分も認証をすることでより強力な認証機能を提供するAH（Authentication Header）があります。一般的に、ESPによる暗号化と認証で十分なケースが多いためESPが選択されます。

IPsecで通信を行う場合、SA（Security Association）を利用して暗号化等を行います。SAには暗号化のための鍵や、暗号化やハッシュのアルゴリズムなどの情報を含んでいます。手動で設定をすることもできますが、一般的にIKE（Internet Key Exchange）を用いて自動的に生成します。一定期間ごとや通信量ごとに新しいSAを生成することで、盗聴された場合でも解読を困難にしています。

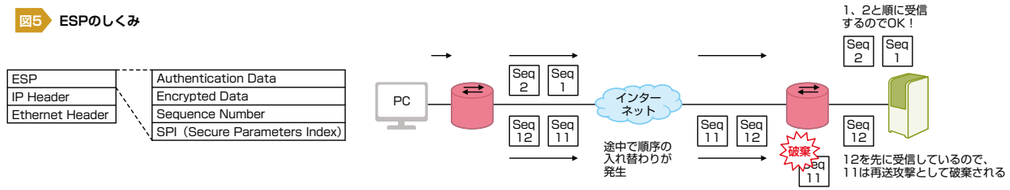
ESPには、TCPやUDPのようにポート番号などの概念がありません。そのため、一般的な家庭やオフィスで利用されているような、NAPT（Network Address Port Translation）を利用しているプライベートネットワークで利用することができません。しかしそのような場合であっても、NAT-T（Traversal）を利用することでIPsecによる通信が可能となります。NAT-Tは、ESPパケットをUDPでカプセリングすることで通信を可能にします。

ESPでは、シーケンス番号により再送攻撃を防いでいます（anti-replay）。順番に数字を大きくしていくことで、受信したシーケンス番号よりも小さな番号のパケットを受信した場合に破棄を行います。そのため、パケットが送信した順番通りに到達する通信路で利用する場合では効果的です。しかし、インターネットのように到着順が保証されていないネットワークでは、パケット順序の入れ替わりなどは恒常的に発生します。そのため、インターネットVPNでIPsecを利用する場合は、anti-replayを無効化するなどの検討も必要になります。図5

IPsec以外のプロトコルでは、OpenVPNなどの実装もあります。OpenVPNでは、NAT配下のネットワークからでも、TCPやUDPを利用してVPN接続を行うことができます。PCやサーバ上で動作する実装となっているため、一般的なルータ等では実装されていません。

インターネットVPNでは、文字通りインターネットを利用しています。そのため、通信事業者が提供する閉域網のようにインターネットから繋がらないVPNと比較して、インターネット自体の障害の影響を受けることや、攻撃を受ける可能性があります。またIKEなどの、UDPで通信を行うプロトコルを利用していることも多いため注意が必要です。認証に対するレスポンスを行うため、詐称した送信元アドレスに対してDoSを行ってしまうケースもあり注意が必要です。
https://jvn.jp/vu/JVNVU91475438/

図5 ESPのしくみ



4 インターネットVPNのトポロジ

インターネットVPNでは、特定の終端装置が決まっていないため、さまざまな形のトポロジを取ることができます。具体的には、ハブアンドスポーク型やフルメッシュ型のトポロジを作ることが多いのではないでしょうか。

ハブアンドスポーク型では、センターとなる装置に対して、それぞれの拠点から接続をします。拠点同士の通信は必ずセンター拠点を経由します。そのため、通信が遠回りする結果、遅延や速度が出ないなどの問題が発生する場合があります。しかし、新しく接続先を追加するときには、新しいルータの設定とセンター側の設定のみで済むため非常に安易です。

フルメッシュ型では、すべての拠点のルータ間でVPN接続をするため、拠点同士で直接通信ができて効率的です。しかし、新しい拠点のルータを追加するたびに、設定済みのすべてのルータを再設定する必要があります。また、VPNの接続先が増えてきた場合に、装置の最大VPN数を超えてしまうと、すべての拠点で装置を増強しなくてはなりません。

最近では、ダイナミック（マルチポイント）VPNの実装がある装置も増えてきています。ダイナミックVPNは、通常はハブアンドスポーク型でセンター拠点に対してVPN接続をしますが、拠点間の通信が発生した場合に、拠点間で通信ができるVPNを自動で構成します。設定は簡易となり、フルメッシュ型の恩恵を受けることもできる仕組みです。ベースには標準的なプロトコルが利用されていますが、さまざまな標準的なプロトコルを組み合わせた独自プロトコルであるケースが多いです。

5 セキュリティとVPN

ここまでセキュリティの向上を目的としたVPNについて説明をしてきましたが、悪意のある攻撃者が通信を秘匿するために、カプセリングや暗号化が利用されるケースも多々あります。

VPNで利用されるような技術が悪意のある通信で用いられると、管理者はVPNを利用しているという事実やVPNを終端している対向装置のIPアドレスや通信量などの、限られた情報しか知ることができません。そのため、通信内容を確認することができず、正規の通信か悪意のある通信か判断をすることができません。

通信内容の判断できないため、企業内ではVPNで利用されるプロトコルをファイアウォール等で制限する場合があります。しかし、マルウェアは標準的なVPN用のプロトコルが利用できない環境でも動作するように、一般的なHTTPやHTTPS、ICMP、DNS等のプロトコルを用いることで、通信を行うケースがあります。データを埋め込むことが可能なフィールドに、暗号化したデータを埋め込むことで実現が可能です。データの内容で判断できないため、通信の傾向を監視するなどの対策が必要となります。

6 最後に

本稿では、VPNの入門者を対象として、過去の技術から現在一般的な技術について簡単に紹介をしてきました。新しいプロトコル等が出てきていますが、核となる技術は変わっていないため、まずは基本について理解を深めることが大切です。

VPNサービスはその特性上、一つの事業者の中で閉じてしまう傾向が強いネットワークサービスです。しかし、現在ではオンプレミス型の業務システムではなく、クラウド上のサーバで業務システムを動作させる企業なども増えてきています。そのため、今後は事業者内で閉じたネットワークから、他事業者も含めセキュアに相互接続し、環境の変化に耐えられることを期待します。

（インターネットマルチフィード株式会社 高橋祐也）

From JPNIC

Dear Readers,

On September 19, 2017, the Internet Society announced fourteen people as inductees to the Internet Hall of Fame. We are delighted and proud that Prof. Shigeki Goto of Waseda University, who serves as President and Chair of the Board of Trustees of JPNIC, has been selected as one of the inductees as a Global Connector. The category of Global Connectors recognizes and celebrates individuals from around the world who have made significant contributions to the global growth and use of the Internet. Prof. Goto has taken a leading role in expanding the global Internet infrastructure particularly for the academic network and International Domain Name and for the Asia Pacific region. Under the leadership of President Goto, JPNIC keeps contributing to the Internet both domestically and globally.

Let us briefly introduce the contents of this newsletter as follows.

・Special Article 1 features the Resource PKI (RPKI) system cooperation between APNIC and JPNIC which has made it possible to verify routing information in Japan from overseas. This collaboration has greatly improved convenience of certificate verification using APNIC's trust anchor. RPKI is a part of authentication infrastructure that certifies holders of number resources such as IP addresses and AS numbers. In addition, it plays a major role in improving the reliability of internet routing.

・Special Article 2 covers "Internet Week 2017". Internet Week is JPNIC's annual technical event for Internet infrastructure engineers. This year it will be held from November 28th to December 1st. More than 30 programs will be coordinated and provided by a number of Japanese Internet associations under this year's theme of "Face eye-to-eye the 'Global' Internet（向き合おう、'グローバル'インターネット）". Along with deepening knowledge about technology, Internet Week is the best opportunity to think about and understand the global characteristics of the Internet and the development of society.

・In "Prologue to the Internet: its Technologies and Services", this time the JP29-type-robot "Nic-kun" and "Dr. Netson" of the Internet Institute will explain about TCP/IP, the protocol that has made it possible to communicate all over the world on the Internet. TCP/IP has been used for over 30 years, so they describe it from its birth to popularization and why it has spread so far.

・ "Internet loves you" is a section that focuses on "a person" who is active in the Internet industry. This time, Mr. Masafumi Oe for the National Astronomical Observatory is introduced. What kind of relationship is there between the Astronomical Observatory and the Internet? It also takes note of Mr. Oe's spirit of taking on challenges, non-straightforward career and influence on other people.

・For "Introducing JPNIC members", we visited KDDI Web Communications Co., Ltd. They started providing rental server services in 1997 and are well-established as a unique web service provider as well. Their uniqueness is not limited to their services. They also have an ambitious attempt to adopt and admit geo-free-workplace for their employees and provide a platform by actively collaborating with other companies' services for small and medium enterprises in rural areas which enable easy handling of IT.

・ "Internet 10 Minutes Course" covers VPNs (Virtual Private Networks), which enable private networks using encryption over a public network and which are attracting attention from security aspects. This time we explain what kinds and techniques are actually available and how they are used.

In addition, "Internet Topics", "JPNIC Activity Report", "Statistics" etc., which cover the past several months, are also delivered.

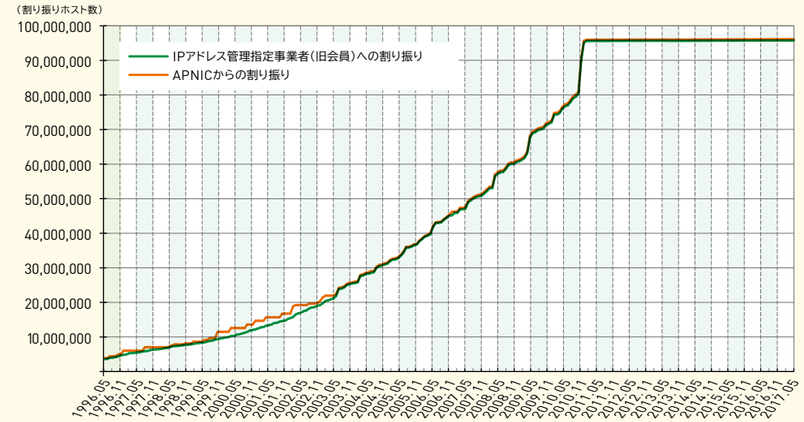
This newsletter, which was largely updated in terms of its design and its sections in the previous issue, has received a positive response from our readers as well. Have you noticed another big change in this issue? We have made the newsletter full color from this issue! If you have any comments or feedback, feel free to contact us at jpnic-news@nic.ad.jp. Your comments are always welcome.

統計情報 Statistics Information

01

IPv4アドレス 割り振り件数の推移

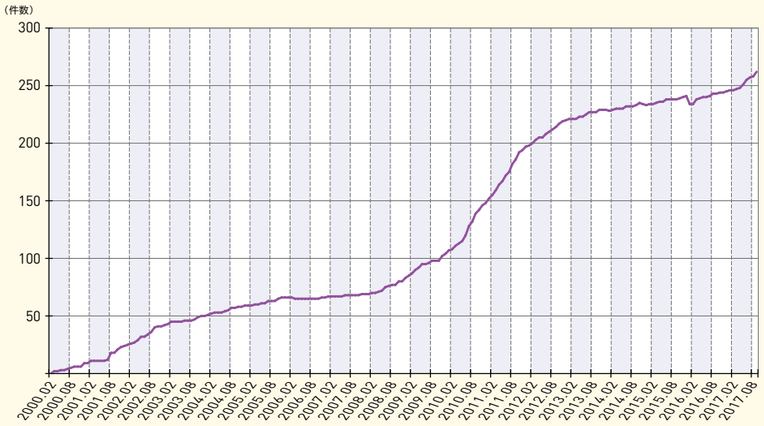
IPv4アドレスの割り振り件数の推移です。JPNICでは必要に応じて、APNICよりアドレスの割り振りを受けています。



02

IPv6アドレス 割り振り件数の推移

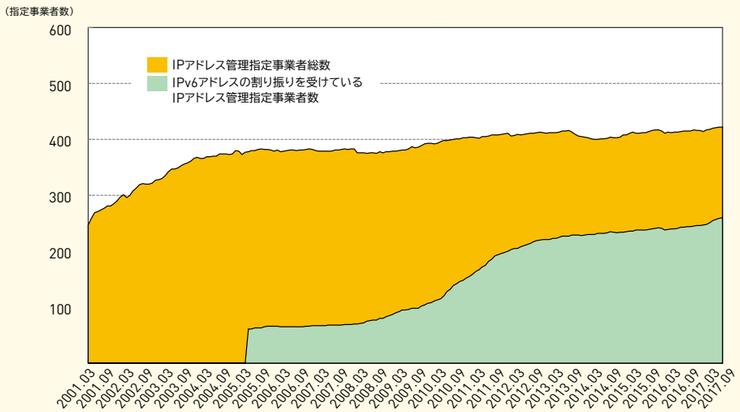
JPNICでは、かつてAPNICで行う割り振りの取り次ぎサービスを行っていましたが、2005年5月16日より、IPアドレス管理指定事業者を対象にIPv6アドレスの割り振りを行っています。



03

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。
（2017年9月現在）

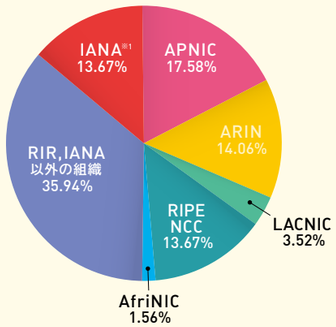


統計情報 Statistics Information

04 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

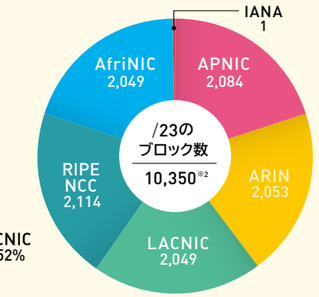
各地域レジストリごとのIPv4、IPv6、AS番号の割り振り状況です。APNICはアジア太平洋地域、ARINは主に北米地域、RIPE NCCは欧州地域、AfriNICはアフリカ地域、LACNICは中南米地域を受け持っています。
2011年2月3日に、通常のIPv4アドレスの割り振りは終了しています。

IPv4アドレス(/8単位)



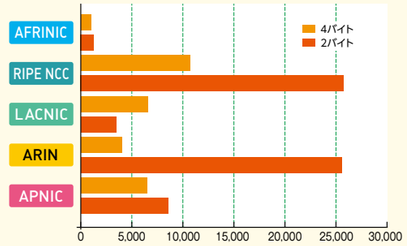
※1 IANA:Multicast(224/4) RFC1700(240/4)
その他(000/8,010/8,127/8)

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

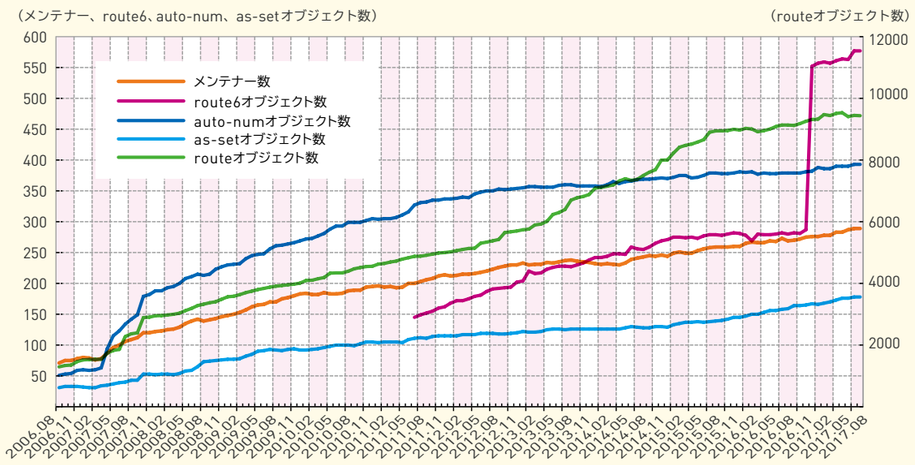
AS番号※3



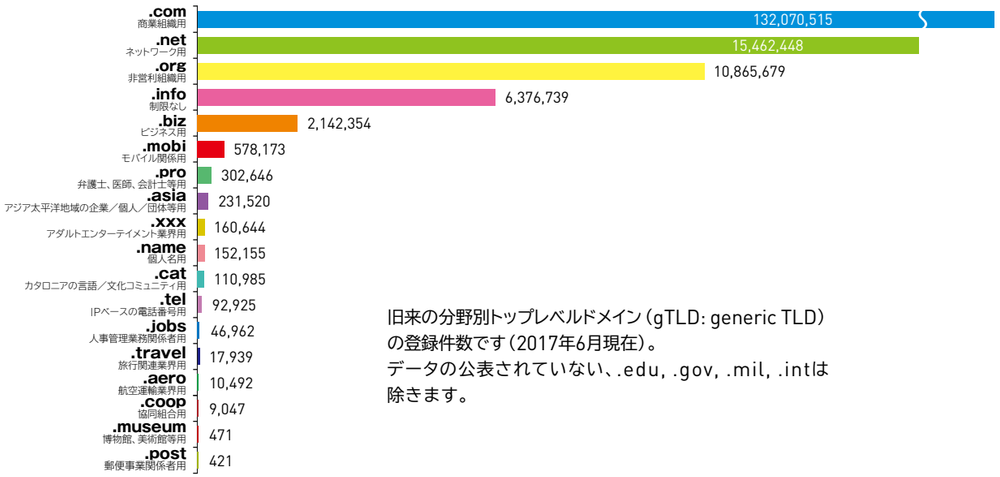
※3 この他に、IANA(Reserved)の2バイトAS1042個(0、23456、64496-65535)、4バイトAS95,032,832個(65536-65551、65552-131071、4200000000-4294967295)、4バイトAS4,199,843,212個があります

05 JPIRRに登録されているオブジェクト数の推移

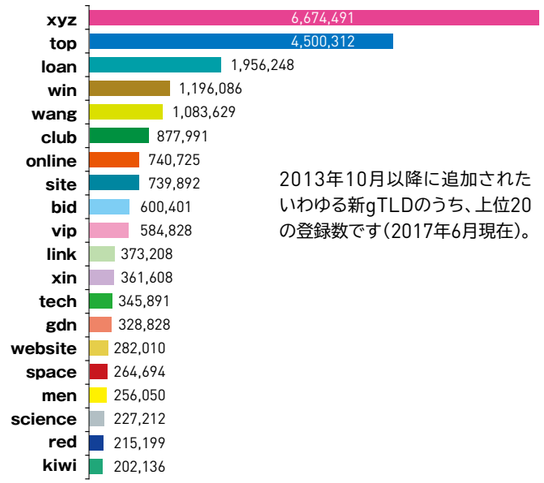
JPNICが提供するIRR(Internet Routing Registry)サービス・JPIRRにおける各オブジェクトの登録件数の推移です。JPNICでは、2006年8月より、JPNICからIPアドレスの割り振り・割り当て、またはAS番号の割り当てを受けている組織に対して、このサービスを提供しています。JPIRRへのご登録などの詳細は、右記Webページをご覧ください。https://www.nic.ad.jp/ja/irr/



06 主なgTLDの登録数



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(2017年6月現在)。
データの公表されていない、.edu, .gov, .mil, .intは除きます。



2013年10月以降に追加されたいわゆる新gTLDのうち、上位20の登録数です(2017年6月現在)。

それぞれのデータは、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/registry-reports

統計情報 Statistics Information

07 JPドメイン名の登録数

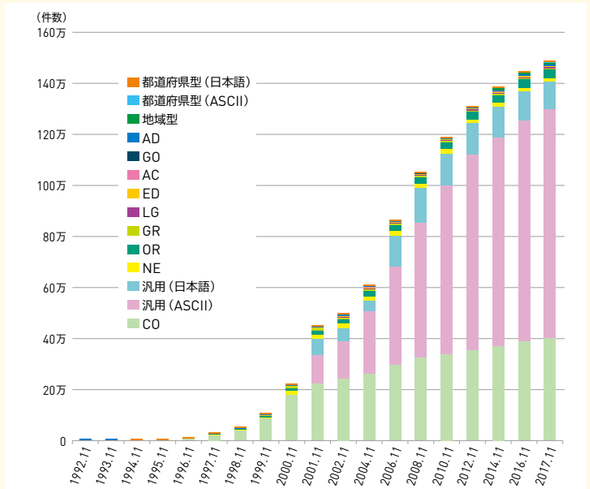
JPドメイン名の登録件数は、2001年の汎用JPドメイン名登録開始により大幅な増加を示し、2003年1月1日時点で50万件を超えました。その後も登録数は増え続けており、2008年3月1日時点で100万件を突破、2017年11月現在では148万件に到達しています。

JPドメイン名の種類と最新の登録数

2017年11月時点の登録総数：1,487,824件

属性型・地域型JPドメイン名			
AD	JPNIC会員等	259	0.02%
AC	大学など高等教育機関	3,607	0.24%
CO	企業等	402,213	27.03%
GO	政府機関等	587	0.04%
OR	その他法人組織	34,907	2.35%
NE	ネットワークサービス	13,576	0.91%
GR	任意団体	6,214	0.42%
ED	小中高校など初等中等教育機関	5,242	0.35%
LG	地方公共団体	1,884	0.13%
地域型	地方公共団体、個人等	2,269	0.15%
汎用JPドメイン名			
ASCII	組織・個人問わず誰でも	896,815	60.28%
日本語		108,379	7.28%
都道府県型JPドメイン名			
ASCII	組織・個人問わず誰でも	9,440	0.64%
日本語		2,432	0.16%

JPドメイン名登録数の推移

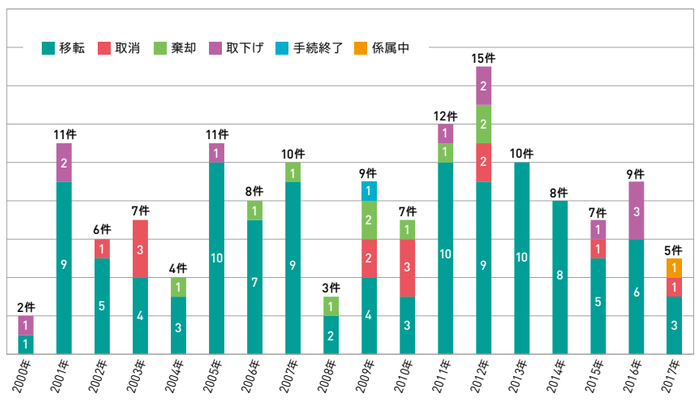


08 JPドメイン名紛争処理件数

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。（2017年11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/

※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

2017年11月14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NTT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未開放日を除く）

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

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
- エクイニクス・ジャパン・エンタープライズ株式会社
- 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QTnet
- 株式会社キューデンインフォコム
- 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
- 株式会社グローバルネットコア
- 株式会社ケーブルテレビ品川
- 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
- Coltテクノロジーサービス株式会社
- さくらインターネット株式会社
- 株式会社シーイーシー
- 株式会社シナプス
- GMOインターネット株式会社
- 株式会社ジュピターテレコム
- スターネット株式会社
- ソニーネットワークコミュニケーションズ株式会社
- ソフトバンク株式会社
- 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
- 株式会社データドック
- 株式会社DMM.comラボ
- 株式会社ディジティ・ミニミ
- 株式会社電算
- トーンモバイル株式会社
- 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
- 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
- BBIX株式会社
- 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
- 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

非営利会員

公益財団法人京都高度技術研究所
大学共同利用機関法人 情報・システム研究機構 国立情報学研究所
サイバー関西プロジェクト
塩尻市
地方公共団体情報システム機構
東北学術研究インターネットコミュニティ
農林水産省農林水産技術会議事務局筑波産学連携支援センター
広島県
特定非営利活動法人北海道地域ネットワーク協議会
WIDEインターネット

推薦個人正会員（希望者のみ掲載しております）

浅野 善男
伊藤 竜二
井樋 利徳
今井 聡
岩崎 敏雄
太田 良二
北村 和広
木村 和貴
小林 努
佐々木 泰介
式場 薫
島上 純一
城之内 肇
橋本 吉正
福田 健平
三膳 孝通
吉宮 秀幸

賛助会員

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

編集をおえてのひとこと。

前号では表紙や紙面の一部がフルカラーになるなど、誌面をリニューアルしました。なかなか評判だったようで、うれしい限りです。この点や前号の振り返りを踏まえて検討し、今号から全ページフルカラーにパワーアップしました！

ところでみなさん、好きな色はありますか？私は、今号のメインカラーになっている青が好きです。高校1年生の頃、私はバレーボール部に所属しており、お気に入りのブルーのジャージをよく着て練習していました。それを見た女子バレーボール部の同級生が「青が似合うね♥」と褒めてくれたのです！この一言が、青を好きになるきっかけでした。まさに、私の淡い〝青〟春です。

今後のニュースレターで、表紙のカラーがどのように移り変わっていくかも、注目していただければと思います。次号もお楽しみに。角

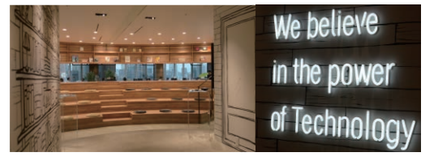
次回予告

Internet Week 2017
～向き合おう、“グローバル”
インターネット開催報告
etc.

ご期待ください

会員企業紹介の取材で、東京都港区の株式会社KDDIウェブコミュニケーションズの本社を訪れました。


本社が入居するビル



オシャレな本社オフィス

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。
▶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66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

詳しくはこちら

JPNICニュースレター 第67号 2017年11月27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 ISBN978-4-902460-42-1

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 http://jpnic-ca.nic.ad.jp/