JPNIC Newsletter

for JPNIC Members

No.65
March
2017

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

JPNIC Newsletter
for JPNIC Members

No.65
March
2017

CONTENTS

巻頭言

▸▸▸Introduction

大規模災害時のインターネット活用を考える

2016年は、非常に災害が多い年でした。もともと地震や台風、火山噴火など災害が多い日本ですが、熊本地震、鳥取地震、東北・北海道を襲った台風、阿蘇山の噴火などさまざまな災害が発生しました。その中でも、熊本地震においては、4月14日の前震、4月16日の本震と、これまでの常識からは予想しにくい地震であったり、東北・北海道への台風については、東北へ直接上陸するなど、これまでにないルートを通過し大きな被害となったりしました。

東日本大震災において、ソーシャルメディア等インターネットを活用した安否確認、被災者支援などによりインターネットの有効性が認識されたと思いますが、昨年のこれまでの常識と違う大規模災害にあってもインターネット活用が有効であったと思います。

大規模災害発生時は、安否確認のために電話が集中し、つながりにくくなりますので、音声通話での安否確認は難しくなります。そのため、携帯電話やパソコンから、SNSや災害伝言板等を使った安否確認が有効です。そのメリットは、電話と比較するとインターネットは大量のアクセスにも対応できることと、情報が集約されているためいち早く必要な安否情報にたどりつけるといったことで、インターネットならではの特徴を生かせていると思います。

大規模災害発生時は、被災状況の確認、避難所、被災者支援、給水・食料提供などの情報が非常に重要となります。しかし、通常の通信環境が失われ、避難所、仮設住宅といった環境では通信手段が限られてきます。そういった環境の中でも、インターネットを経由してSNS、行政、民間企業、ボランティアなどのWebサイトから必要な情報を比較的容易に収集したり、提供できたりします。この点においても、情報の発信・共有が容易というインターネットの特徴が生かせていると思います。熊本地震においては、ある中学校の校庭に「飲み水ください」と書かれたメッセージが、Twitterなどの SNSを通じて拡散され、メッセージを見た全国の人から「水」が届いて、校庭に感謝のメッセージが書かれたということがあったそうです。

こういった大規模災害時でのインターネット活用のためには、ネットワークの維持、早期復旧とともに避難所でのWi-Fi提供など通信環境をいち早く整えることも重要と思います。また、ボランティアが、被災されたお年寄りにスマートフォンの使い方を教えるケースがあり、これまでインターネットを活用できなかった方の、情報リテラシーを上げる活動も重要です。

インターネット活用の負の点に目を向けると、大量の情報の中には、デマ、あるいは間違った情報が含まれていることが問題となっています。熊本地震においては、写真付きで「動物園からライオンが逃げた」というデマがTwitterで拡散し、問題となりました。このケースでは、投稿された写真をよく見ると街並みが日本ではなかったということで、「情報について自分自身でも調べる」、「情報の発信元を調べる」、「複数の情報を取って比較してみる」などの対応も必要と思います。

災害が多い日本ですが、皆様とインターネットの活用をさらに広げることで、ますます、多くの方に役立つようにしていきたいと思います。

JPNIC理事
斎藤 重成
（さいとう しげなり）

プロフィール

1987年 東北大学工学部卒。同年、第二電電株式会社（DDI）入社。2000年、DDI、ケイディディ株式会社（KDD）、日本移動通信株式会社（IDO）が合併、株式会社ディーディーアイ（KDDI）（現KDDI株式会社） 発足。2008年、ネットワーク建設本部 建設2部長。2015年より、現職であるネットワーク技術本部長。また、2015年よりIPv6のVNE会社である日本ネットワークイネイブラー株式会社（JPNE）の取締役、2016年より日本インターネットエクスチェンジ株式会社（JPIX）の取締役を兼務。

特集／1
Special Article

Internet Week 2016／IP Meeting 2016 開催報告

～見抜く力を！～

『Internet Week 2016 ～見抜く力を！～』開催報告

2016年11月29日（火）から12月2日（金）まで、Internet Week 2016を開催しました。今回は久しぶりに会場を変更して秋葉原を離れ、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にて行いました。

総プログラム数は31、最終的な参加者数は約2,400名（延べ人数、同時開催イベントの参加者を含む）でした。毎年Internet Weekにご注目いただいている方の中には気づかれる方もいらっしゃるかもしれませんが、プログラム数・参加者数とも数字の上では例年より若干減少しているように見えます。これは後で触れますように、一部のプログラム形態を変更した（1日セッションを増やした）ことによるもので、ユニークな参加者数で言いますと、例年と同程度の方々にご来場いただくことができました。

今年のテーマ：見抜く力を！

Internet Weekでは、毎年テーマを設定しています。2016は「見抜く力を!」でした。詳細は高田寛実行委員長の挨拶をご覧いただきたいのですが、インターネットを取り巻くさまざまな課題の本質を見抜く力を、講演者と参加者で共に養っていこう、という想いが込められています。

最終的にこのフレーズに決まったのは7月頃でしたが、そのコンセプトは既に春先からありました。毎年4月、その年度に開催するInternet Weekに向け、まずは実行委員会が召集されます。そこでコンセプトやプログラム企画の進め方の検討が始まります。Internet Weekのプログラム内容が多岐にわたるように、それに携わる実行委員・プログラム委員の専門分野もさまざまです。そのような中でも、今年参加者に持ち帰っていただきたいものは何かを考えたとき、本当に大切なものは何かをいま一度よく考えて、見極めていく力なのではないかという点で、全員が一致しました。後日開催したプログラム委員会でも、このコンセプトに深くうなずく委員が多数見られました。

プログラム委員会での検討を経て完成した今年のプログラムは、ハンズオンを取り入れたものを筆頭に、会場からのコメント・質問を積極的に受け付けるなど、自ら考えたり、手を動かしたりするプログラムが、例年よりも多かったのではないでしょうか。

20回目のInternet Week 変更点 その1：7年ぶりに新会場へ

今年は二つの新しいことにチャレンジしました。

一つ目は会場の変更です。1997年に前身の「IP Meeting」から名を変えて始まったInternet Weekは、初期の頃は横浜を中心に、関西地区で開催したこともありました。その後、2007年に会場を東京に移してからは、秋葉原での開催が続いていましたが、今年はそこからJR総武線で1駅の浅草橋駅近くの会場を使用しました。

新会場の一番の魅力は、広いホワイエ、会場2Fのホール前にある約300平方メートルのスペースです。ここは主に協賛企業様のご協力により、ブース出展、ドリンクサービス等で盛り上げていただきました。コーヒーを飲みながら、参加者間の交流を深めたり、協賛企業様・後援団体様が提供する資料を集めたりと、有意義な休憩時間が過ごせたようでしたら幸いです。午後には、会場ネットワークの設計／構築／運用を担当したNOCチームが、「IPv6で遊ぼう」と題し、会場ネットワークとしても利用されていた、NAT64を利用したIPv6 onlyの実験ネットワークに関する情報共有を行った日もありました。

● NOCチームによる「IPv6で遊ぼう」には多くの参加者に興味を持っていただけました

20回目のInternet Week 変更点 その2：1日プログラムと4日通し券

今年のもう一つの大きな変更点は、1日プログラムを毎日開催したことです。

最終日に1日セッションの「IP Meeting」、それより前の日に2.5時間のセッションが1日に複数行われるのが、最近のInternet Weekのプログラム構成でした。今年は最も大きな会場（2Fホール）で開催するセッションを、すべて1日プログラムとしました。内容は考慮せず形態だけで見ますと、初日から最終日まで会期中は毎日IP Meetingがあるようなイメージです。

この変更に先立ち、2015年の春、前年のInternet Week 2014にご参加いただいた方々とJPNIC会員の皆様を対象にアンケートを実施しました。恒例の「今年のInternet Weekで取り上げてほしいトピック」に加え、Internet Weekの参加費についてお伺いしました。

これまでのようにセッションごとに参加費を支払う形式と、定額の参加費でどのセッションも参加できる形式のどちらがいいかを確認したところ、結果はほぼ半々、強いて言えば前者を支持する方が若干多いといったところでした。

前者を支持する方の主なご意見は、

- 参加費について所属組織に説明しやすい
- 本当にその問題に関心のある意識の高い参加者が集まる
- 参加セッションが少ない人にとっては割高になるのでは

また、後者を支持する方の主なご意見は、

- 空き時間にこれまで参加してこなかったようなセッションにも参加する機会が増え、興味・関心の幅が広がるのでは
- 直前に予定が変わることが多いため、幅を持たせて参加セッションが登録できるとうれしい

ということでした。数的にも内容的にも一方に決め難かったため、どちらのエッセンスも半分ずつ取り入れたのが、今年のプログラム形態です。従来のセッションごとに参加費を設定するプログラム（2.5時間／5時間プログラム）は3分の2程度残し、専門的で対象者を絞ったセッションを中心に割り当てました。また、前述のように1日プログラムを導入しました。ここには、事前アンケート結果やこれまでの参加者数を考慮し、参加者の多くが聴きたいであろう、あるいは聴いてほしいテーマを割り当てました。また1日プログラムを対象に4日通し料金を設定し、加えて1日プログラムに二つ以上申し込むと、お得な料金で参加できるようにしました。

Internet Week プログラム委員長の交代

今年はもう一つ、内部的には大きな出来事がありました。プログラム委員長の交代です。これまではJPNICの前村昌紀が務めていましたが、今年は中津留勇さん（SecureWorks Japan株式会社）に委員長を、中島智広さん（日本DNSオペレーターズグループ／NRIセキュアテクノロジーズ株式会社）に副委員長をそれぞれお願いしました。委員の中では若手にあたるお二人が、委員間の連絡ツールとしてSlackを取り入れ、委員間のコミュニケーションをより活性化させるなど、今年のプログラム委員会には、新しい風が吹いたように思います。

最後に

Internet Week 2016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。会期中の様子はSNSでも発信していましたので、興味のある方はご覧ください。

今年のInternet Weekは、会場の変更、1日プログラムの導入と久しぶりに大きな変更をした年でした。試行錯誤な面もあり、ご不便をおかけしたこともあったかもしれませんが、今年のInternet Weekを少しでも楽しんでいただけたのなら、また少しでもお役に立てたのなら、喜ばしい限りです。アンケートの結果や開催にご尽力いただいた関係者のコメント等も踏まえながら、来年に生かしていきたいと思います。

最後になりましたが、ご講演者の皆様、ご協賛の皆様、プログラム委員をはじめとした協力団体の皆様など、開催にご協力いただいたすべての方々に感謝いたします。

Internet Week 2017は、2017年11月27日（月）の週に開催予定です。ぜひ今から、ご予定に組み入れていただけますと幸いです。次回も多数の方のご参加をお待ちしています。

（JPNICインターネット推進部 坂口康子）

IP Meeting 2016 ～見抜く力を!～ 開催報告

IP Meetingは、その年のインターネットの状況を総括し、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付けにもなっています。

今回も、午前の部は「Internet Today!」と題し、インターネットの「運用動向」、「新技術の標準化動向」、「社会的動向」、そして「セキュリティ」という観点から、各分野の第一人者の方々にご講演いただきました。「見抜く力を!」という今年のテーマのもと、今知るべきトピックが総括され、2016年のインターネットにまつわる各分野の動向等を見抜いていきました。

午後の部では、まずInternet Week 2016の全セッションを「IPv6」、「セキュリティ」、「ネットワーク運用管理」、「社会派」、「DNS」、そして「最新技術」の6分野に分け、プログラム委員がそれぞれの分野の総まとめを紹介しました。その後、Internet Weekの締めくくりとして、インターネットの未来を見抜いていくための「インターネットが作る、未来の暮らしを考える～これからを豊かにするための八つの視点～」と題したパネルディスカッションを実施しました。

本稿では、IP Meeting 2016の最後のプログラムとなった、パネルディスカッションの模様をお伝えします。

パネルディスカッション：「インターネットが作る、未来の暮らしを考える ～これからを豊かにするための八つの視点～」

インターネットは、ヒトが生み出してきたモノの中でも、想像を大きく超えるイノベーションを生み出してきた技術となっています。私達は、インターネットを当たり前のように生活の一部に使い、暮らしの質の向上に役立てています。そして、これから生まれてくるデジタルネイティブな子ども達は、真の意味でインターネットをインフラとして使いこなし、暮らしぶりをさらに変化させていくことでしょう。そうした中では当然、インターネット自体に質の向上が求められていきます。

今回のセッションでは、インターネットを八つの視点からとらえ、今後の人々の暮らしへの関わり等について、それぞれ分野のパネリストの方々にご発表いただき、これからのインターネットと暮らしとの関わりを考察するセッションが展開されました。

［モデレータ］

砂原 秀樹
（慶應義塾大学大学院メディアデザイン研究科／WIDEプロジェクト）

［パネリスト］

IoTの観点：**田中 邦裕**（さくらインターネット株式会社 代表取締役社長）
女性・子どもの観点：**花田 経子**（岡崎女子大学／慶應義塾大学大学院KMD研究所）
AIの観点：**中島 秀之**（東京大学 ／ 公立はこだて未来大学）
社会的観点：**岡村 久道**（弁護士法人 英知法律事務所）
人材育成の観点：**曽根 秀昭**（東北大学 サイバーサイエンスセンター）
アプリケーションの観点：**藤川 真一**（BASE株式会社 取締役CTO）
災害復旧の観点：**辻井 高浩**（奈良先端科学技術大学院大学）

視点1 モデレータより

砂原 秀樹
（慶應義塾大学大学院メディアデザイン研究科／WIDEプロジェクト）

インターネットが、今後どのように人の暮らしを支え、幸せにしていくかという話をしたいと考え、このパネルディスカッションを企画しました。

そのための根本に、インターネットの質を上げるにはどのようにしたら良いのか、といった問いがあると思います。インターネット前提社会において、人間の知覚は大きく拡大してきましたが、一方で課題も増えました。インターネットの質を上げることは、その課題解決に道筋をつけ、人の暮らしを支えるための大きな助けにつながります。

また、そうした課題に接しながら技術者は反省を繰り返し、いい技術を作っていくことが大事なように思っています。さらに、インターネットを取り巻くステークホルダーも、政府、産業界および学術系と、それぞれが真の意味で機能していかなければなりません。インターネットの要素は技術だけではないので、人材に関することや社会、法制度にも視野を拡げて考えていければならないのではないかと思います。今回はさまざまなお立場、そして各分野の第一人者である7名のパネリストの方にお集まりいただきました。参加者の皆さまにとって今後のインターネットと暮らしの質の向上へのヒントとなればと思います。

視点2 IoTの観点

田中 邦裕
（さくらインターネット株式会社 代表取締役社長）

さくらインターネットはデータセンターの会社という印象が強いと思いますが、実はデータセンター事業の売り上げは全体の2割を切っています。かつてハウジング全盛の時期もありましたが、時代とともにクラウド事業へ移行しています。ここで気付くことは、サーバやインターネットで収益を得ることはできますが、そのサービスの中身は変わってきているということです。そして、第4次産業革命（IoTやAIの時代）がやってくる中で、これからも変化があるだろうと思います。

また、私が感じるところとしては、インターネットの時代の大きな流れとして、モノの時代からサービスの時代になり、またモノの時代に戻ろうとしているように思います。というのも、1990年代はハードウェアや半導体を生産する企業が強かった産業構造が、現在はソフトウェアでサービスを提供する企業が中心の産業構造へと移っています。時価総額を見ても、いわゆるBIG5が台頭しているのが良く分かります。また、ソーシャルゲームを例に取ると、昔はゲームカセット（ハードウェア）の内部でデータの書き換えを行っていたものが、現在はオンライン上でサービスが提供されることで、データの書き換えに対して料金を支払うというような時代となっており、つながっている状態でどのようなビジネスを行うのかが肝となっています。今後はサービスとモノの間としてのIoT、そしてその関連事業に軸足が移っていくのではないかと考えており、そこにビジネスチャンスがあるのではないかと思っています。
さくらインターネットとしても、我々独自の構成で、世の中に受け入れられるよう工夫しつつIoTの事業を進めています。

一方でIoTは、社会を変えるインフラになると思いますが、どのような手段で行っていくかは、これからの課題になっていくだろうと思っています。

視点3 女性・子どもの観点

花田 経子
（岡崎女子大学／慶應義塾大学大学院KMD研究所）

子どもに関する話題としては、アナログ教育とデジタル教育における議論があります。教育の現場はアナログな考え方をベースに設計されていますが、デジタルによる教育の可能性が議論されているところです。

子どもにとっての創造的な活動を考えると、彼らにとってはアナログとデジタルに差違はなく、どちらに価値があるかを見極め、自分にとって価値のあるほうを選択する傾向にあると考えています。そういった考えのもと、子どもたちの創造的な活動をデジタル（ICT）から支える際にカギとなるのは、まず、安全であること、次にアナログと共存していけるということ、そして使う側に簡易性と汎用性と応用性を持たせることです。しかし、これを実践していくには教える側の人間も育てていく必要があります。

情報モラルに関する問題については、すべての子どもがインターネットによって何らかの被害を受けているわけではありませんが、保護者・家庭が多様化しており、教える側がその多様化に追いついていないように思います。そのため、子ども向けの情報モラルに関する教育カリキュラムやコンテンツはありますが、必要なところに届いているか、効果は上がっているか、時代に即しているのかを今後検証していく必要があると思います。

次に女性のキャリアパスに関してですが、女性のキャリア形成と男性のそれとに差はありません。しかしながら女性の場合、ライフキャリアがワークキャリアに非常に大きな影響を及ぼします。従って、ライフキャリアとのバランスを図りながらどのようにキャリアを形成していくのかがポイントになっており、そのためのサポートができる仕組みを整備していくことが必要となるでしょう。また、女性人材の活用の課題として、ワーキングマザーへの継続教育が不十分である点が挙げられ、インターネットの分野においては、こうした継続教育にももっと貢献できる点があるのではないかと思っています。ただし、こうした女性への対応は、単に女性優遇ではなく男性も活用できるもので、かつ持続可能性のある仕組みでなければならないと思っています。

視点4 AIの観点

中島 秀之
（東京大学 ／ 公立はこだて未来大学）

知能とは、情報が不足した状況でも上手く機能する能力だと考えています。そういった視点に立つと、自分で情報をすべて取り込んでコントロールするのではなく、環境に計算させるという考え方が大事であり、AIもこうした構造にシフトしていると思います。

環境に計算させるにあたっては、データを入力して計算させるボトムアップ（入力主導）だけでは難しく、予期して計算させるトップダウン（予期主導）が大事になってきます。機械学習はボトムアップがほとんどでしたが、Deep Learningの登場により、暗黙知をAIに組み込むことが可能となり、AIがトップダウンに向かう契機となりました。

情報社会（Society4.0）は、農耕社会（Society2.0）や工業社会（Society3.0）に次ぐ、世の中の仕組みを根本的に変えるような世界観の革新であると思います。そして、この次の世界観にAI（Society5.0）が登場すると言われています。Society4.0（インターネットの時代）もSociety5.0（AIの時代）も情報技術が関係してきますが、情報技術には情報通信と情報処理という二つの側面があると考えており、インターネットは情報通信の側面を担う一方、AIは情報処理という役割を今後担っていくのだと思います。

繰り返しになりますが、Deep learningはAIの一分野であり、暗黙知の扱いが可能になったことによって、AIの分野は大きく進歩し、これからの社会を変える技術になると思います。情報革命によりインターネットが情報の流れに関して時間と距離を縮めてくれましたが、次はAIによってモノの流れに関して効率化を図り、モノの移動の時間と距離も縮めていければと思っています。

視点5 社会的観点

岡村 久道
（弁護士法人 英知法律事務所）

今の世界がどこから来たのかを考えることが、今どこにいるのかの立ち位置確認につながり、そして今の位置を知ることが、未来を考えるスタート地点と言えるのではないでしょうか。我々が追いかけてきた世界はホストコンピュータ時代からダウンサイジングが始まり、端末機器の面ではPCからスマホ、ネットワークの面ではクライアントサーバ時代、クラウド時代、そしてIoTの時代へと進んできましたが、それぞれの環境が変化する間にはそれぞれの壁がありました。

IoTの次に何が出てくるかを考えると、エッジコンピューティングやフォグコンピューティングという技術があり、さらにブロックチェーンやシェアリングエコノミーをどうとらえるのかという話が出てきています。そして、それを阻む壁として、セキュリティやレスポンスのリアルタイム性問題、またプライバシーやデータロックイン等の問題があるようです。モノには2面性があり、技術の進歩や新しい技術の利用には常に多くの課題が伴います。技術革新に伴う現在のような激しい動きがある環境下でも、法律の改正やガイドラインも多く示されており、果たして事業者がどれだけ対応できるのかは未知数です。

また今後は、知的財産権に関しての問題が大きくなるのではないかと思います。今までは人間の精神活動の成果をカバーするために設計されていましたが、AIが登場し、今後自律の方向に進んでいくと、誰がどの権利を取得するのかというのが課題となってきます。加えて、法的責任にも大きな問題が出てくると思います。自動運転を例に取ると、いろいろな原因から起こる事故に関して、どう切り分けて誰がどのように責任を負うのか、レベルごとに整備しなければなりません。さらに、道徳／哲学的に解決不能な問題もあります。

このように考えれば考えるほど新たな問題が出てくる現在ですが、我々の世代は課題を投げかけるとともに、次の世代の人たちにもこうした課題について考えてもらう必要があると思います。

視点6 人材育成の観点

曽根 秀昭
（東北大学 サイバーサイエンスセンター）

私からは、皆さまにとって今後の人材育成を考える契機となればと、現在我々が進めているセキュリティ人材の育成のための施策である「SecCap」を紹介します。

SecCapは文部科学省の人材事業であるenPITのセキュリティ分野を担う活動です。

セキュリティ人材はエキスパートと呼ばれる方々もいますが、SecCapではセキュリティ人材の裾野を広げるためにエキスパートでなくても、何か問題が発生した際に見極めができるような人を育て、ひいてはセキュリティに関する知識が一般市民にも広がることを目的としています。実践セキュリティ人材の輩出が一番の目的となりますが、技術面だけではなく、管理面での判断もできる人材を育てたいと思い、設計しています。そのために、大学院にさまざまなカリキュラム、幅のあるコースを準備しており、基礎的な科目があり、その後に演習科目を履修し、先進科目を学んでいただくという流れとなっています。履修を終えた学生には、修了認定を行っています。

学生数も右肩上がりで、女性の比率も徐々に上昇し、企業にも認知が進んできています。また、SecCapにおける活動は、教授同士も他の授業を見学する等して演習の方法を学んでいます。

そして今年度から、大学学部でもこの試みを実施します。一般技術者として必要となる共通的なセキュリティ対策技術の基礎知識を、またエキスパートをめざす学生には、技術者・研究者として修めるべき専門知識と実践的演習を履修できるように、さまざまなカリキュラムを準備しています。こうした取り組みによって、インターネット業界で全体的な懸案となっている、「情報セキュリティ人材育成」の課題が解決できる糸口ができると、明るい未来が見えてくるのではないでしょうか。

視点7 アプリケーションの観点

藤川 真一
（BASE株式会社 取締役CTO）

現代は、ネットを通じて誰でもモノやサービスの取り引きができる世界となりました。我々のビジネスは、スマートフォン前提の世代向け、つまりHTMLやセキュリティをことさらに意識しない、ごく一般の方たちに向けた、ネットショップ作成サービスを展開しています。こうしたビジネスを展開する中で、日常のリスクを観察していくと、日本人同士での取り引きでは、多少のもめ事は起こるものの、大きな事件は起きていないように感じており、外国との取り引きの方が、リスクが高いように思います。

その他、アプリケーションレイヤーでは、出会い系サイトによる詐欺等、さまざまな問題が起こっています。こういった問題があるのは、インターネット上のリスクがあまり知られていないからであり、情報の非対称性がある中でWebのサービスをどう信用していくかという課題は解決されていないのが実情だと思います。しかしながら、インターネット前提社会のミレニアム世代が、信用やリスクに対する意識や知識を十分にまだ持ち合わせていないとしても、彼らには新しいことに挑戦していく気概があり、彼らが考えていることは重要だと思っています。

別の話では、Webの常時SSL化やIPv6への対応も視野に入っています。これはアプリの世界ではApple社が主導しているところでもあり、特にSSLについては、インターネット前提社会においては、多少乱暴でもこうした対応が求められていくのかもしれません。また、ポケモンGOに代表されるようにコンテンツとロケーションビジネスに関しては、今後面白いのではないかと考えています。

最後に、Google検索エンジンの限界と炎上という点についてお話したいと思います。つい先日、とあるキュレーションサイトに関する報道があり、実際にサイトが閉鎖されるという事件がありました。問題のコアはSEOにあったのではないかと思います。検索エンジンはプロの書いた記事かどうかを判断できず、検索の上位に問題のある記事が掲載されていました。こうした問題のある記事を発見した人間が、自身のブログ等により、誤りを指摘し続け、それが他にも波及し、結果的に炎上し、人間がこの問題を鎮火させたように思えました。インターネットにおける炎上は、報道でも取り上げられるようになり、企業も無視できない時代となっています。これは、情報発信力のある個人が力を持ってきたということでもあり、インターネットを使う人たちを味方につけることが、今後重要になってくるのではないかと思います。

視点8 災害復旧の観点

辻井 高浩
（奈良先端科学技術大学院大学）

奈良先端科学技術大学院大学（以下、NAIST）では災害対策の一環として、三つの取り組みを実施してきました。

一つ目は沖縄科学技術大学院大学（以下、OIST）との相互データバックアップです。NAISTとOIST間で、データ保全のため公開情報データの相互バックアップを実施しました。NAIST側の機器は非常用発電機および免震システムを備えたコンテナサーバルームに収容しております。

二つ目は内閣府主催の首都直下型地震を想定した防災訓練です。災害派遣医療チーム（DMAT）から依頼を受け、内閣府主催の首都直下地震を想定した防災訓練に参加いたしました。災害時においてDMATでは、災害時の被害状況のポータルサイトとなっているEMISというシステムに繋ぐことが必須となっており、ここで患者の容態や病院の状況等の入力や閲覧を行い、さまざまな判断を行っていきます。この防災訓練における我々の役割は、DMATが活動する護衛艦いずも内にインターネット環境を提供することでした。自衛隊の規則により護衛艦内でインターネットに接続できる部屋と端末が限定されているため、いつでもどこでもインターネット回線を提供できる衛星地球局を車載したシステムを利用し目的を実現できました。このシステムは専門家がいなくてもすぐインターネットに繋ぐことができ、電源は車から得ることができる仕様となっています。

三つ目は熊本地震対応です。我々は、平常時から、災害時にすぐに衛星を利用したインターネットを使えるよう、企業や病院等と協力して研究を行っています。熊本地震が起きた際には、協力先の病院から依頼があり、主にデータ取得を目的として、熊本へと向かいました。しかしながら、その道中に熊本地震の本震が発生し、DMATより正式の依頼を受け、熊本地震で被害に遭われた方々への支援を行うため、特に被害の大きかった阿蘇に向かいました。ここでは車を使ったインターネットを提供し、主に避難所へのWi-Fiサービス、救護班へのIP電話提供を行ってまいりました。

これらの取り組みを通じて、平常時の端末が緊急時にも使えるということおよび衛星回線の狭帯域を考慮することが重要であることを痛感し、これらの研究を推進し、問題を解決したシステムを構築した上で、DMATにおける情報共有/引き継ぎのシステム開発・研究が必要になってくるのだという認識に至りました。

各講演の後、それぞれのパネリストより一言ずつ程度、お互いの分野における課題等について、自分の立場からどのように考えるのか等のコメントがありました。最後のディスカッションに多くの時間は取れませんでしたが、インターネットのこれからについて、我々がきちんと向き合ったら向き合っただけ、我々の暮らしがこれからも、より豊かになっていくのではないかと感じました。インターネットは社会を支えるものになり、我々の生活を支えていますが、どうしたら安心して使い続けられるか、参加者にとってこれからも考えていく良いきっかけになったのではないかと思います。

（JPNIC総務部 手島聖太）

次世代WHOISをめぐる議論の動向

次世代WHOISをめぐる議論の動向

WHOISは、インターネットレジストリが管理するインターネット資源の登録情報を公開提供するサービスです。IPアドレスやドメイン名の利用者などを検索する時に使います。

WHOISとは
https://www.nic.ad.jp/ja/whois/

WHOISはレジストリ、ユーザーの双方にとって重要なサービスの一つであるため、関係者によって、絶えず在り方や使い勝手の改善に向け、技術的および政策的な観点という双方から検討が続けられています。今回の特集では、その中でも特に注目ポイントである「gTLDのWHOISで議論されている次世代型登録ディレクトリサービス」という新しい技術と、「IPアドレスに関するWHOISの登録情報正確性の向上を目指した、法執行機関による新しいポリシー提案の状況」の2点についてご紹介します。

次世代登録ディレクトリサービスに関する議論

レジストリ登録情報の検索サービスをRegistration Directory Services（RDS）と呼び、具体的にはWHOISを指します。

現在、ICANNにおいて、gTLDのWHOISについて抜本的な見直しが進められており、WHOISに代わる次世代登録レジストリサービスのプロトコルとしてRDAP（Registration Data Access Protocol）の検討が進められています。

RDAPの検討状況

RDAPは、IPアドレス・ドメイン名等のレジストリに登録されたデータにアクセスするためのプロトコルです。WHOISのプロトコルは、RFC 3912で定められていますが、応答の形式が規格上定められておらずフリーテキスト形式であったため、レジストリごとに応答の形式が異なっているなど、プロトコル上の問題があります。RDAPでは、JSON（JavaScript Object Notation）形式での応答となっており、どのレジストリでも統一されたデータを返すようになるといった、WHOISのプロトコルとしての問題の解消が図られています。

RDAPはIETFのweirdsワーキンググループ（WG）で検討が行われ、2015年に関連するRFC 7480～7485が発行されました。現在weirds WGは活動終了となっており、IETFでのRDAPの議論は、登録情報に関するプロトコルを議論するregext WGで取り扱われています。なお、RFC 7480～7484については、株式会社日本レジストリサービス（JPRS）から日本語参考訳が公開されています。

IETF weirds WG
https://tools.ietf.org/wg/weirds/

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

ICANNにおけるWHOISの抜本的見直しに関する検討状況

ICANNにおいてもWHOISの抜本的な見直しがされています。これは2009年10月に締結されたAoC（Affirmation of Commitments；責務の確認）に基づくもので、この契約において、ICANNが定期的に見直すべき重要なポリシーの一つとして、WHOISが挙げられました。これを機に、2010年9月にWHOIS Policy Review Teamが発足し、最終報告書が作成されました。

WHOIS Policy Review Team Final Report
https://www.icann.org/resources/pages/whois-rt-final-report-2012-05-11-en

この最終報告書を受けたICANN理事会がgTLD登録データの収集・維持・アクセス提供の目的を再定義する作業を事務局に指示し、2012年12月にgTLDディレクトリサービス専門家作業部会（Expert Working Group；EWG）が設立されました。

EWGは、gTLD登録データを収集、維持する目的の定義およびデータ保護方法の検討と、gTLDディレクトリサービスに関して、データ保護を勘案しつつ、データの正確性とデータアクセスの問題に対処することができるモデルの提案を目的としました。EWGの最終報告書は、2014年6月に公開されています。この最終報告書は、ICANNの分野別ドメイン名支持組織（Generic Names Supporting Organization；GNSO）により2015年5月に開始された、WHOISのRDSを決めるポリシー策定プロセス（PDP）の土台となっています。

Final Report from the Expert Working Group on gTLD Directory Services：
A Next-Generation Registration Directory Service（RDS）
https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf

現在は、PDP作業部会が設立され、検討が進められています。検討事項は大きく11項目となっています。

ユーザー・目的	誰が登録データにアクセスできるべきか
アクセス制御	ユーザーまたは目的ごとにデータアクセスを制御するためにはどんなステップが取られるべきか
データの正確性	データの正確性を向上させるにはどのようなステップが取られるべきか
データ要素	どのデータが収集、保存、公開されるべきか
プライバシー	データおよびプライバシーを保護するためにはどんなステップが必要か
新旧システム共存	新旧システム共存を可能にするにはどんなステップが取られるべきか
コンプライアンス	これらのポリシーを実施するにはどんなステップが必要か
システムモデル	RDSが充足するべきシステム要件は何か
費用	何のコストがかかり、どのように賄う必要があるか
利益	どんな利益が達成され、どのように測定されるか
リスク	ステークホルダーが何のリスクに直面するか。それがどのように認知・受容されるべきか

作業部会での検討プロセスはフェーズ1からフェーズ3に分かれており、上述の11項目について、フェーズごとに検討が行われます。現在はフェーズ1となっています。

- フェーズ1：次世代RDSに関するポリシー要件の策定
- フェーズ2：フェーズ1で策定されたポリシーの基本設計
- フェーズ3：フェーズ2で設計されたポリシーの実装検討

最新の検討状況や議論に関する情報は、次のWebページから確認できます。

Next-Generation gTLD Registration Directory Services to Replace Whois
https://community.icann.org/display/gTLDRDS/Next-Generation+gTLD+Registration+Directory+Services+to+Replace+Whois

日本のコミュニティにおける議論

RDSに関しては、一般財団法人インターネット協会（IAjapan）とJPNICの共催で開催した第46回ICANN報告会においてディスカッションが行われました。WHOISには、登録した登録者の情報を非表示にしたり、登録者の情報をサービスプロバイダの情報などで置き換えて表示したりするプライバシー・プロキシサービスが提供されています。このプライバシー・プロキシサービスのWHOISの登録データ正確性に関する意見と、登録者のプライバシー保護に関する意見が多く挙げられました。当日の資料および録音は、次のWebページからご覧いただけます。

第46回ICANN報告会
6. WHOIS/次世代登録ディレクトリサービス（RDS）に関するディスカッション
https://www.nic.ad.jp/ja/materials/icann-report/20160804-ICANN/icann46-06-maem.html

WHOISの登録データ正確性について

現在のWHOISにおける問題の一つとして、WHOISに登録する情報を形式的に収集する形になってしまっており、収集した情報がうまく使われていない状態になっていることが挙げられます。加えて、WHOISに多くの情報を登録することによって、攻撃者にインセンティブを与えることになっているという指摘もあります。

これに対し、警察はWHOISをサイバー犯罪の捜査に利用しており、連絡がつかない場合には、犯罪組織がしばらく活動を続け被害者が増えることになるため、登録者に正確に連絡がつくことは重要であり、データの正確性が向上することにより、犯罪者への抑止力になるという意見があります。

一方で、ICANNにおいてプライバシー・プロキシサービス事業者を認定して一定のルールの下にサービス提供を認めようという取り組みがあり、WHOIS上の情報は隠しながらも、登録者に連絡が届くことを担保しようとしていることが紹介されました。

Privacy & Proxy Services Accreditation Issues Working Group
https://gnso.icann.org/en/group-activities/active/ppsa

登録者のプライバシー保護について

プライバシー・プロキシサービスが、WHOISの登録情報に基づいて連絡をしても、本当の登録者に到達できない原因なのではという議論があります。

WHOISに公開された登録者の情報を元にスパムメールが送られる問題も指摘されているため登録者のプライバシー保護を図っていくことは重要ですが、プライバシーを保護するあまり、あまりにも情報を出さない、情報を隠すということになると、WHOIS検索による正当な問い合わせや犯罪捜査での利用という役割を損なう可能性があります。

登録者にとっては、多くの情報を登録することや、正確な情報を登録することは、コストの増加になることを意味しますが、次世代RDSに登録する情報の収集目的を明確化し、登録者にとって過度な負担にならないよう、的確な要件の定義が求められています。

WHOIS登録情報正確性向上に関する議論

米国連邦捜査局（FBI）や、各国の警察といった法執行機関より、サイバー犯罪対応のためにデータベースとしての正確性向上の要請があり、RIRのカンファレンスで議論が始まっています。このWHOIS登録情報正確性向上に関しては、P.21の第31回JPNICオープンポリシーミーティング報告、P.23のAPNIC 42カンファレンス報告、P.27のNANOG 68/ARIN 38ミーティングレポートでも取り上げています。あわせてご覧ください。

WHOIS登録情報正確性向上に関する議論の始まり

アジア太平洋地域のRIRであるAPNICにおいては、2016年2月のAPNIC 41カンファレンスでのPolicy SIGにおいて、WHOIS登録情報の正確性向上について検討と対策が議論されており、不正確な登録情報の報告件数等の現状と、不正確な登録情報に対するサービス拒否など、今後取り得る対応策の検討について共有されました。

APNIC Policy SIG（2） - Improving APNIC Whois Data Quality
https://2016.apricot.net/program#sessions/apnicpolicysig2-improvingapnicwhoisdataquality

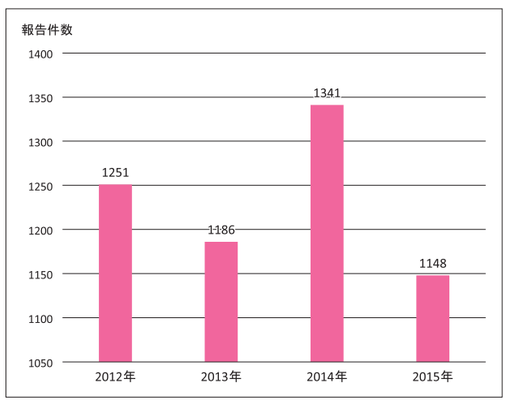


図1：報告された無効な連絡先の数の推移

Report on Whois Data Quality Improvement discussion at APNIC 41
https://www.apnic.net/community/policy/policy-sig/whois-data-quality/apnic-41

この中でAPNICからは、WHOISに登録されているものの連絡がつかない連絡先の報告が年間1,000件以上あり、APNIC WHOISに登録されている情報が不正確だという報告が行われていると説明がありました。

法執行機関からの問題意識の共有

法執行機関から、APNIC 42カンファレンスをはじめ、各RIRでのプレゼンテーションで問題意識の共有が精力的に進められています。

日本のコミュニティでは、2016年11月30日に開催された第31回JPNICオープンポリシーミーティング（JPOPM）において、FBIのJesse Schibilia氏からの発表が行われ、具体的な事例の紹介を含め、次の点が説明されました。

- WHOIS検索は、公安・サイバー犯罪の対応のために、最初に利用されるツールであること
- ISPへの二次割り振りの情報について、当初の分配先から変更があるにもかかわらず、不正確な古いデータになってしまっていること
- WHOIS情報の正確性を欠くことで、迅速な捜査に影響があること、また、IPアドレスのハイジャックは、それらのIPアドレスを利用した複数の犯罪行為につながる可能性があること

当日の議論については、議事録および録音が公開されていますので、あわせてご参照いただければと思いますが、次にこのJPOPMで議論になったポイントを紹介します。

IPアドレスの登録に関するポリシーについて

議論の前提として、IPアドレス管理のポリシーとして規定されるIPアドレスの割り当てを行った場合の対応について、説明します。

JPNICのIPアドレス管理ポリシーでは、「インターネットを利用するあらゆるレベルの人が遭遇するインターネット上のトラブルを解決するための、参照情報として利用できるようにするため」に、割り振りおよび割り当てを行ったIPアドレスに関する情報はレジストリデータベースに登録されなければならないと定めています。

JPNICにおけるアドレス空間管理ポリシー（IPv4）
5.1.2 登録 https://www.nic.ad.jp/doc/ip-addr-ipv4policy.html

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
3.3. 登録 https://www.nic.ad.jp/doc/ip-addr-ipv6policy.html

さらに、日本でLIRに該当するIPアドレス管理指定事業者に対しては、IPアドレスの割り当ておよび再割り振りを行った場合にJPNICデータベースに登録しなければならないこと、またJPNICデータベースに登録した情報に変更が生じた場合に変更を届け出なければならないことを規則に定めています。これらに基づき、IPアドレスに関する情報登録は行われています。

IPアドレス割り当て等に関する規則
第18条（割り当て報告および再割り振り報告）
第19条（ネットワーク情報記載事項変更申請）
https://www.nic.ad.jp/doc/ip-rule.html

WHOIS情報の定期更新を促すための施策

WHOIS情報の定期更新を促すための施策として、JPNICが運用している経路情報のデータベースであるJPIRRと同様の仕組みを実装する意見が、当日の参加者からポリシーの議論を行うIP-USERSメーリングリストに投稿がされています。JPIRRでは、データベースの正確性向上のために、一定期間（1年間）更新のない登録情報について、自動的に削除するというガーベージコレクターを実装しています。

しかし、IPアドレスの登録情報にも同様の仕組みを導入して、古い情報を自動的に削除してしまうと、不都合が大きいことも予想されるため、WHOIS上で更新が行われない情報に印を付けて、LIRの更新を促すといった施策も考えられます。

その他の懸念事項など

技術的な問題として、CGNを用いたアドレス共有が行われている場合についての指摘もあります。IPv4アドレスにおいては、CGNを用いたアドレス共有が行われている場合、WHOISで検索することができるIPアドレスの割り当て情報が正確であっても、実際のIPアドレスのユーザーを特定しきれない可能性が出てきます。この対策として、ポート番号のログを取るといった運用をLIRに求めるといったことが出てくるかもしれません。

また、IPアドレスの登録情報中の連絡先として自身を登録していたことがある担当者から、適切な問い合わせを受けたことがないという経験を交えたコメントがありました。法執行機関からの問い合わせ先は、WHOISの登録情報とは別にしないと運用が困難なのではとの指摘も行われました。

今後のスケジュール

今後のスケジュールとしては、各RIRと法執行機関が連携し説明を行った上で、2017年春にポリシー提案を提出し、2017年秋の施行をめざしていると発表されています。

法執行機関からのポリシー提案により、前述の管理のポリシーに何らかの変更を加える、WHOIS情報正確性向上のためのLIRが遵守すべき事項が追加で定められるといった可能性が考えられますが、本稿執筆時点ではどのようなポリシー提案が行われるのか、明らかにされていません。

LIRにとっては、これまでのIPアドレスの登録管理業務に関して少なからず変更が生じる可能性が高いことから、実効性があり、実施可能な施策となるかどうか、コミュニティで慎重な検討が必要になるでしょう。加えて、すべてのRIRで提案したポリシーがコンセンサスに至るまでを考えると、ポリシーの施行までは、多くの時間が必要になると思われます。

◇　◇　◇

どちらの話題についても、レジストリにとって最も重要なサービスの一つであるWHOISに変更をもたらすものです。そのため、WHOISを利用される皆様には、関心を持っていただき、議論にも参加していただきたいところです。JPNICでは、最新の状況を皆様にお知らせし、WHOISのあり方について議論を進めていければと考えております。

（JPNIC IP事業部／インターネット推進部 角倉教義）

JPIRRへのオブジェクト登録方法のご案内

IRR（Internet Routing Registry）は、インターネット上でのデータの道筋を示す経路情報とその優先性に関する情報を蓄積するデータベースです。IRRに情報を登録することで、BGPの経路情報に関する信憑性や優先性の確認や、登録情報に基づいた経路フィルタの生成に利用することができます。

JPNICでは、JPIRRと呼ばれるIRRを運用していますが、このJPIRRのご利用にあたり、よくご質問をいただくオブジェクトの登録について、最初に登録が必要なMaintainerオブジェクトと、Routeオブジェクトの登録方法を具体的にご案内いたします。

0.IRRのデータベースについて

IRRのデータベースは、経路情報を表す「ルート情報」、ASの情報やルートの生成元（オリジン）を表す「AS情報」およびそのASの「ルーティングポリシー」などが登録されています。加えて、これらの登録情報の管理主体を表す情報も登録されています。IRRでは、これらの情報は「オブジェクト」という形でデータベースに登録されています。代表的なIRRのオブジェクトは文末の**表1**の通りです。

JPIRRは、JPNICからIPアドレスもしくはAS番号の分配を受けている組織が無料で登録いただけます。JPIRRに登録するオブジェクトについて、登録手続の方法やフォームの雛形および記入例など、次のWebページをご参照ください。

JPIRRでのオブジェクト登録について
https://www.nic.ad.jp/doc/irr-registration.html

1.Maintainerオブジェクトの登録

JPIRRサービスの利用には、最初にMaintainerオブジェクトの登録が必要になります。上記「JPIRRでのオブジェクト登録について」の「1.1 Maintainer オブジェクトの新規登録フォーム」に必要事項を記入の上、メールで irr-admin@nic.ad.jp 宛にご送付ください。申請フォームは次のいずれかに該当するメールアドレスよりご送信ください。

- JPNICから分配を受けているIPアドレス・AS番号を管理するための契約者情報もしくは資源管理情報中に登録されている電子メールアドレス
- AS情報中で［管理者連絡窓口］［技術連絡担当者］として登録されている担当者情報（JPNICハンドル）中のd.［電子メイル］、または担当グループ情報中（グループハンドル）の[電子メール]として登録されている電子メールアドレス

メール受領後、JPNICの担当者が申請フォームの内容を確認し、Maintainerオブジェクトを登録します。作業が終わり次第、登録を行ったオブジェクトの内容や各種オブジェクトの管理に必要となる仮パスワード等を記載した登録完了通知のメールが送付されます。

Maintainerオブジェクトの新規登録フォーム

申請者情報（（1）または（2）のいずれかをご記入ください）

（1）資源管理者略称（IPアドレス管理指定事業者略称）：

契約組織名：

（2）AS番号：

AS番号割当先組織名：

mntner:	【必須】Maintainerオブジェクトの名称を、MAINT-AS****の形式で記入してください
descr:	【必須】Maintainerオブジェクトの管理を行う組織名を記入してください
X-Keiro:	【任意】経路ハイジャック情報の通知を希望する場合の通知先メールアドレスを記入してください
admin-c:	【必須】オブジェクトを管理する担当者の情報をJPNICハンドルもしくはグループハンドルで記入してください
tech-c:	【必須】技術的な事項に関する担当者の情報をJPNICハンドルもしくはグループハンドルで記入してください
upd-to:	【必須】オブジェクトの登録内容を更新する際に、認証エラーとなった場合の警告メールの送信先を記入してください
notify:	【任意】オブジェクトの登録内容が変更された際に、通知されるメールアドレスを記入してください
mnt-nfy:	【必須】オブジェクトの登録内容が変更された際に、通知されるメールアドレスを記入してください
remarks:	【任意】Maintainerオブジェクトの管理上、必要な内容を自由に記入することができる項目です
auth:	【必須】認証情報をJPNICで登録します
mnt-by:	【必須】Maintainerオブジェクトの名称(「mntner」の項目と同一)を記入してください
changed:	【必須】申請者のメールアドレスとオブジェクト登録を行った日付をJPNICで登録します
source : JPIRR	【必須】フォームに記載された内容に変更を加えないでください

※【任意】の項目は、登録を希望しない場合、項目ごと（行ごと）削除してください
※「auth」と「changed」の項目は、JPNICで登録を行うので、項目のみ記載し、空欄としてください

2.Routeオブジェクトの登録

Maintainerオブジェクトの登録が完了したら、実際にインターネット上で経路広告が行われているIPアドレスに関する情報であるRouteオブジェクトの登録を行ってください。JPIRRでのオブジェクト登録についての「3.2.1 Route(Route6)オブジェクト登録フォーム」に必要事項を記入の上、メールで auto-dbm@nic.ad.jp 宛にご送付ください。Routeオブジェクトの登録は、自動応答システムとなっており、機械的に処理されます。登録完了後に通知のメールが送付されます。

JPIRRへの申請はHTML形式のメールではエラーとなってしまう場合があります。プレーンテキスト形式のメールで申請してください。また、フォーム以外の文字や記号が入力されていると申請がエラーとなる場合があります。メール本文には申請フォームの内容のみを記載してください。

Routeオブジェクトの新規登録フォーム

password:	【必須】Routeオブジェクトの登録・情報変更の際に必要なパスワードを記入してください
route:	【必須】登録するアドレスブロックを記入してください
descr:	【必須】アドレスブロックの割り振りや割り当てを受けた組織の名称や、ネットワークの名称を記入してください
X-Keiro:	【任意】経路ハイジャック情報の通知を希望する場合には、通知を希望する電子メールアドレスを記入してください
origin:	【必須】該当するアドレスブロックの経路広告元となるAS番号を、AS****の形式で記入してください
member-of:	【任意】routeに記入したアドレスブロックが登録されているroute-setオブジェクトの名称を記入してください
notify:	【任意】オブジェクトの登録内容が変更された際に、通知されるメールアドレスを記入してください
mnt-by:	【必須】オブジェクトを管理するMaintainerオブジェクトの名称を記入してください
changed:	【必須】申請者のメールアドレスとオブジェクト登録を行った日付を記入してください
source : JPIRR	【必須】フォームに記載された内容に変更を加えないでください

※【任意】の項目は、登録を希望しない場合、項目ごと（行ごと）削除してください

3.登録したオブジェクトの確認

登録したオブジェクトは、WHOISコマンドおよびWebページから検索することができます。

［WHOISコマンド］
% whois -h jpirr.nic.ad.jp MAINT-ASXXXXX
% whois -h jpirr.nic.ad.jp 203.0.113.0/24

［Webページでの検索(JPIRR Gateway)］
https://jpirr.nic.ad.jp/

4.問い合せ窓口・参考情報

JPIRRに関するご質問は、JPIRR担当 irr-query@nic.ad.jp 宛にご連絡をお願いします。
また、JPIRRの登録者のみなさまに役に立つ情報をWebページでご案内しております。あわせてご参照ください。

JPIRR登録者・利用者向けページ
https://www.nic.ad.jp/ja/ip/irr/index.html

（JPNIC 技術部 菊地栄次）

オブジェクトの名称	オブジェクトの役割
Maintainerオブジェクト	・各IRRオブジェクトの管理に必要な認証用のオブジェクト。 ・必ず最初に他のすべてのオブジェクトに先立って登録する必要がある。
Routeオブジェクト Route6オブジェクト	・実際にインターネット上で経路広告が行われれているIPアドレスに関する情報を表すオブジェクト。 ・IPv4アドレスはRouteオブジェクト、IPv6アドレスはRoute6オブジェクトとして登録する。
Aut-Numオブジェクト	・ルーティングポリシーを特定するためオブジェクト。 ・import、export、defaultなどの項目を記入し、自組織のASのルーティングポリシーを外部からも参照できるようにすることが可能。
AS-Setオブジェクト	・経路広告元が同一のAS番号や、その組織に関連のあるAS番号に関する情報を一括管理するためのオブジェクト。

表1：代表的なIRRのオブジェクト

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。

利用者全員が幸せになれる接続環境の提供をめざして

お話しいただいた方

株式会社アット東京

左：常務執行役員 社長補佐/事業企画担当/ソリューション本部長 **小笠原 寛** 氏

中央：ソリューション本部 ネットワークサービス部長 **斎藤 晋一** 氏

右：ソリューション本部 ネットワークサービス部 ネットワークサービスグループ サブグループマネージャー **富岡 正行** 氏

株式会社アット東京

住所：〒135-0061　東京都江東区豊洲5-6-36
設立：2000年6月26日
資本金：133億7850万円
代表者：代表取締役社長　中村 晃
URL：http://www.attokyo.co.jp/
事業内容：http://www.attokyo.co.jp/company/
情報通信システムを一括して集中管理するデータセンター事業（届出電気通信事業者）
・データセンター基本サービス
・ネットワークサービス
・システムインフラ運用サービス
従業員数：243名(2017年1月現在)

今回は、2000年6月に設立され創立17年目を迎えた、株式会社アット東京を訪問しました。同社は長年の経験から得た多岐にわたるノウハウと、高い拡張性・世界最高水準のファシリティで顧客から信頼を得ている、データセンター業界では国内最大級の事業者です。

同社は当初、東京電力のデータセンター事業者として設立されましたが、2012年10月にセコムグループとなりました。そのような経緯を経つつも、セコムと東京電力パワーグリッド、また設立時からの株主であるインテックと、それぞれ異なる企業文化を持つ社員が一丸となり、社員が力を合わせてよりよいサービスをめざし日々努力されています。

当日は、お客様が自分のやりたいことを実現できる場を提供して、そこに集う全員が幸せになれることをめざし、データセンター事業に専心される同社の姿勢が強く感じられるインタビューとなりました。その姿勢は同社が運営するデータセンターのあらゆる点で高水準なファシリティや強固なセキュリティにも現れており、「24時間365日ノーダウンオペレーション」の言葉通り、止まらないサービスを提供し続けるという強い意志に、同社の方々の熱い思いを感じさせられました。

コロケーションを基幹とする特徴的なデータセンター事業展開

―まずは貴社の事業内容や、事業展開の状況について教えてください。

小笠原：当社では、データセンター（DC）事業として、サーバー室単位で提供するコロケーション、サーバー室の中にケージで囲った専用スペースを提供するケージングコロケーション、いわゆるラック貸しのハウジングという、三つのサービスを提供しています。また、センター内のお客様同士をつなぐ構内配線サービスと、インターネットサービスも提供していて、この辺りが主な事業です。事業の割合としてはやはりDC事業が大きく、その中でもコロケーションサービスが相当の割合を占めています。

通常DC事業と言えば、ハウジングをメインとする事業者が多いですが、当社は所有するDCの規模を活かしてお客様の要望に合わせたコンピュータールームを作ることが多く、コロケーションの引き合いが多いのが特徴です。そのためには、お客様からの厳しい要求や細かいカスタマイズへの対応が必要で、決して簡単ではないのですが、お仕着せのセット売りではない点が強みともなっています。

―顧客はどのような業種が多いんでしょうか。

小笠原：ITサービスを提供している事業者様、金融業のお客様が多いですね。昨今ではインターネット関連の事業者様、クラウド事業者やコンテンツ系など大量のトラフィックを扱う大型案件の事業者様も増えてきています。また、従来から、DC in DCと呼ばれる、DCを再販していただけるパートナー様なども主なお客様です。また、外資のお客様も増加していて、そのため営業をはじめあらゆる部門にバイリンガルの社員が多いのも当社の特徴です。

―「アット東京」という貴社の名前はわかりやすいですよね。一目で東京のDCだとわかります。特に外資のお客様にとっては、東京にプレゼンスがあるという強烈なインパクトは、強みになっているのではないでしょうか？

斎藤：私自身は、名付け当時のことをはっきりとは知らないのですが、2000年頃のインターネットの広がりでポピュラーになった場所を表す「@」を使い、東京電力が母体だったDCということもかけて、「東京」とつなげたのではないでしょうか。東京は日本の首都であり、「そこにあるデータセンターだ」というインパクトは確かにあると思いますね。

● DC内部の様子

東京電力グループからセコムグループへ

―貴社は2012年に筆頭株主が東京電力からセコム社になったという経緯があるようですが、そのことについて教えてください。

小笠原：はい。2000年の創業時は東京電力グループでした。創業当時の数年は、同時期に同事業に参入したセコムもまったく同様ですが、「データセンター」という業種がそもそもまだよく知られていない時代で、事業的には厳しかったと聞いています。しかしそうした時期を経て、徐々によいお客様に恵まれ、どんどん売り上げが伸びていきました。

2012年10月にセコムグループ入りしたわけですが、セコムもDC事業者としては中堅として事業をしていたものの、圧倒的な規模を誇るアット東京がセコムグループ入りすることにワクワクしたことを覚えています。一方で自身がアット東京へ赴任する辞令を受けた時には、果たしてこの巨大なDCをどのように販売し、また、品質を維持向上させていくのか見当もつきませんでした。

案の定、アット東京に赴任した直後は、セコムのDCと規模が違いましたから、定常的にメンテナンスや工事関係の投資が発生しており戸惑いを感じたのをよく覚えていますね。

―セコムグループ入りしたことによるシナジーなどがあれば教えてください。

小笠原：DCサービスの面では、セコム社の情報系企業であるセコムトラストシステムズ社の大阪のDCと10Gbpsのネットワークで接続し、DRサイトとしてお客様に提案を差し上げています。またインテック社の富山のDCも同様です。後は、サイバーセキュリティでしょうか。当社のDCのお客様にセコムトラストシステムズ社のサイバーセキュリティサービスを提案できるようになりました。

やはり、それぞれ会社の文化が違うというのがあるのですが、セコムグループ入りしてから4年が経過し、それぞれの良いところが混ざり、またプロパーの社員も増えて、社としてとても良い方向に向かってきていると感じています。

―それぞれの良いところとはどんなところでしょうか。

小笠原：技術部門を中心に東京電力から出向している社員の高い技術力とプロパー社員が融合してスキルの底上げが良い循環で起きていると思いますね。これだけのファシリティの技術とノウハウを持ったDC事業者は他には無いと自負しています。

他のDC事業者の方と会話する機会も頻繁にあるのですが、DCファシリティに対しては保守的な会社が多いようです。当然と言えば当然なのですが、絶対に電気を止めてはいけませんし温湿度も厳しい管理を求められるので、できるかもしれないけど多少グレーな点があると「できない」という回答になりがちでしたね。

DCの根幹部分の設計は安定した堅牢な設備とし、お客様個別の設備についてはいかにお客様のご要望を取り入れながら、SLAとのバランスを鑑み設計、実装していくか、お客様目線で取り組む姿勢がセコムグループ入りして変わったところかもしれませんね。

もう一つはコスト管理でしょうか。一括の発注から分離発注にして自社の社員が管理していくことで、品質を維持向上させながらコストをセーブしていくことがセコムグループ入りして進化したことだなと感じています。

現在は少し理想の形に近づいたのではないかと感じています。さらにお客様にも利用いただきやすいような努力は企業として必要だと感じています。

エンジニア目線で設計をこだわり抜いたデータセンター

―DCと言えば電力供給能力が肝となりますが、貴社のDCでは電源の多重化などに大変力を入れてらっしゃいますよね。

小笠原：都区内のDCは、都内にある世界初の500kV地下式超高圧変電所から地下ケーブルで2系統受電しています。また、火力発電所に隣接する別の変電所からも受電しています。どちらも地下経由なので、災害に非常に強固な構成と言えます。それに非常用自家発電機設備を加えての、合計で四重の電源系統となっています。もちろん、非常用自家発電機はまだ一度も本番で稼働させたことはありませんが。

DCへ電気を供給している変電所は、都心部への電力供給の重要拠点ですし、それを引き込むルートは今話した通り冗長化されています。またDCの建屋内についても、電気、通信系統のどちらも2系統配線しています。どこかに単一障害点があるとダメですからね。引込から受電、センター内の設計まで最高レベルの堅牢性を実現したDCとの自負があります。こういった点でも、当社のセンターはエンジニア目線でしっかり設計しています。

―電気の面だけでなく、広いスペースが必要になると思いますが、その広いスペースをカスタマイズして提供しているんですね。

小笠原：これだけの広いファシリティをお客様の細かいご要望を受けカスタマイズするために、技術系、中でもファシリティエンジニアが多く在籍しています。比較したことはありませんが、DCファシリティエンジニアの社員数としては恐らく日本最高ではないでしょうか。実際に工事やメンテナンスをする際に事業者様にすべ

てをお願いするのではなく、的確に指示し管理することが当社のポリシーにあったDC運営をするためには必要だからです。お客様によっては、「ここの壁を壊したい」「キャッピングをせずに高負荷なシステムを冷却したい」など、さまざまな要望があります。それに応えられるように、建築、電気、空調、通信のそれぞれスペシャリストがいて、それらを統括できるゼネラリストも揃えています。

―本当に細かいカスタマイズにまで対応していらっしゃるんですね。

小笠原：以前、海外のお客様が当社のDCへ来たことがあったのですが、朝から晩までDCを隅々までチェックした後に「いろいろな国のDCを引き渡し前にチェックしているが、ここは要望通り作ってくれるから私はバカンスに来ているようだ」と言われたことがありますよ（笑）。またファシリティの作り込み以外にも、先ほどもお話した通り、海外のお客様により満足いただくためにもバイリンガルのサービスの品質強化に取り組んでいます。

―電力と並んでDCで重要なものと言えば回線ですが、貴社では回線環境の整備にも力を入れてらっしゃると聞いています。

小笠原：従来からサービスを展開していただいているDIX-IE、JPIX社に加えて2016年の7月にBBIX社に当社のDCに接続拠点を新設いただきました。2017年4月からはインターネットマルチフィード社（JPNAP）のIXのサービスを新たに当社のセンターに迎え入れることができます。これで四つのIXが利用できる環境になりました。また、DCのお客様は必ず回線接続をしますが、当社のDCはお客様が多くいらっしゃるので通信事業者様にはPOP（Point Of Presence）を設置いただいています。気づくと20社以上の通信事業者様にPOPを設置いただいていてキャリアホテル化していました。これだけの回線環境が整っているDCは、国内にはそう多くはありません。それに加えて、大きなトラフィックを流す国内外の事業者様が当社のDCに入っていますので、それらの方とDC内で直接接続できるのもメリットですね。

―DC事業では大量の電力消費など環境への配慮が避けては通れませんが、その点での取り組みは何かありますでしょうか。

小笠原：DCの電力使用効率を示す指標にPUE（Power Usage Effectiveness）がありますが、PUEが下がると電気代が下がり価格競争力も上がります。このPUEは1.0に近いほど効率が良いのですが、一般的なDCの運用値は1の後半から2.0くらいだと思います。つまり、お客様に提供する電力と同じくらいの電力をそれ以外で使っているわけです。

当社は東京を拠点にしているので、寒冷地にあるデータセンターのようにはいきませんが、外気を効果的に活用するフリークーリングの仕組みを入れ、冷凍機もインバーターにするなど、空調関係の消費電力を減らしています。また、太陽光パネルを設置したり、室内灯をLEDにしたりするなど、地道にPUEを下げる努力を続けています。PUEが下がるとコスト削減だけではなく、結果的に二酸化炭素排出量も減り環境改善にもつながるわけです。

DC事業へ一意専心

―貴社は他社と比べても、DC事業へかなり軸足を置いてらっしゃるように見受けられます。

小笠原：一般的なDC事業者と比べると、当社のサービス体系も、インターネットサービスと監視サービスの提供と、シンプルだと思います。

これには理由があって、我々がめざすDCは、我々だけが儲かるのではなく、クラウドやセキュリティなどさまざまなサービスを提供するパートナーにDCに入ってもらって、みんながハッピーになろうというものです。そうやってさまざまなパートナーが集まれば、そのサービスを利用したいエンドユーザーも集まってきます。なので、クラウドサービスなどはやらないと決めています。あくまでニュートラルな立場でサービスを提供するというのが当社の考え方です。

―「みんなで集まって場になる」をめざしているということですね。ところで、監視サービスと言えば、貴社サービスの「@EYE」はユニークですよね。

小笠原：これはお客様のオフィスからDC内の状況を監視できるサービスで、日本のDC事業者であまり提供されていないサービスだと思います。本当はDCに入居するユーザー企業様だけでなく、DC事業者様自身にも使ってもらいたいのですが、なかなか難しいようです。

もともと、どこのDCにもBMS（Building Management System）と呼ばれる設備監視システムがあるのが一般的なのですが、それに加えてDCIM（DataCenter Infrastructure Management）である@EYEも導入しています。DCIMはリアルタイムで電力量や温度などさまざまなデータを取得し蓄積でき、後から分析することができます。蓄積したデータを見て電力の効率的な分散を行いお客様がコスト削減できますし、当社の中でもサービスの向上に活用しています。この@EYEは、海外のお客様など個別の要望を細かく注文される方には非常に良い評価をいただいています。

移転制度の導入が与えたIPv6普及への影響

―DCサービスの展開にはIPアドレスが欠かせません。貴社はIPv6について積極的に取り組んでいただいていますが、顧客からの引き合いはどうでしょうか。

斎藤：2011年からデュアルスタックでサービスを投入しています。当初は興味をお持ちになるお客様がそれなりにいらっしゃったのですが、実際に導入にまでいたった例はそれほどありません。それから6年ほど経ちますが、その後もあまり伸びていない印象です。IPv6対応への必要性をまだ強くはお感じになられていないように受け止めています。

―総務省の意向により、モバイルキャリア3社がIPv6をデフォルトで提供することになりましたが、貴社の事業には何か影響がありそうでしょうか。

富岡：IPv6がデフォルトになれば国内の状況もかなり変わるのかなとは思いつつも、我々のIPv6対応は完了しているので、その点では比較的落ち着いています。

これまでのIPv6普及状況としては、ハイパージャイアント系が積極的な一方、国内の動きは緩やかだと感じています。特に、IPv4アドレスの移転ができるようになってIPv4アドレス不足への危機感が薄れてきているのではないでしょうか。当社もIPv4アドレスが無くなるとアンサービスになるため、IANA~APNIC在庫枯渇前後はIPv6の動向を注視していたのですが、アドレス移転や経路分割などが結果として枯渇対策となり、今はそこまでの危機感がなくなっているのかもしれません。

DCを支えるのは人。新しい人材を呼び込みたい

―スペシャリストを多数抱えているというお話がありましたが、人材という面で、貴社では若手の育成や女性の活躍についてどのように取り組んでらっしゃるのでしょうか？

小笠原：ファシリティエンジニアについては、未経験の新卒を充てるのが難しいのですが、とはいえ採用しないと社内の年齢構成がいびつになってしまいます。そのため、最近では定期採用を行うようにしています。

私は日本データセンター協会（JDCC）の運営委員をやらせてもらっているのですが、JDCCも学生さんにDC事業に興味を持ってもらおうと学生さん向けのDC見学をやっています。DCという名前は聞いたことがあっても、DCに関心を持ってくれる学生さんはまだまだ多くないようです。比較的新しい業種ではありますが、今ではDCは社会インフラとなっています。身の回りの多くがIT化されていて、そのシステムのほとんどがDCに入っていると言っても過言ではないと思います。

それらを支えているのがDCです。電気やガス、水道の社会インフラと同じですよね。使えて当たり前で、でもその裏では事業者の方々は大変なご苦労をされている。使えて当たり前なので普段は褒められることなくトラブルがあったら叱られる、そんな事業かもしれません。ただ、ご利用いただいているお客様の事業の根幹を支えているのがDC事業なんだ、そんなプライドをもって社員が頑張ってくれていると思っています。

また、女性は積極的に採用しています。さすがにファシリティ部門には多くはありませんが、営業部門やスタッフ部門としては大勢の女性が働いています。バイリンガルの人材も多く、各部署で活躍していますよ。小さなお子さんがいらっしゃる女性の勤務時間の考慮もして働きやすい環境をめざしています。

人との交流を大事に。コミュニティとの関わり

―自社の人材育成に積極的に取り組まれているのですね。また、「場としてのつながりを大切に」というお話に関連して、コミュニティとの関わりや人材交流についても何かお考えの点があるのでしょうか？

小笠原：DC事業はセキュリティの観点からも宣伝広告は慎重にと考えています。とはいうものの知名度も非常に重要です。今年度は金融系やネットワーク系の国内外のフォーラムへ多く出展しています。意外に当社が海外のお客様に名前を知られていることに驚きました。海外のお客様に多くご利用いただいていますのでその影響が大きいのだと思います。こういう場で会社としての知名度を上げるのも重要ですし、人と人との交流も大変重要だと考えています。若い社員もどんどんそういった場に出していこうと思っています。自らやりたいと手を挙げる人間が出てくるのは、社としても大変良いことだと思っています。

JPNICには地方との架け橋になってほしい

―貴社には会員としてJPNICの活動を日々支えていただいていますが、何かJPNICへのご意見・ご要望などありますでしょうか。

斎藤：JPNICにはいろいろお世話になっていますが、東京と地方の橋渡しのようなことにも取り組んでもらえると嬉しいですね。橋渡しは中立と見られるフラットな立場の組織がよく、その点ではJPNICは適任だと思います。我々はどうしても東京視点になってしまいます。さまざまな立場のステークホルダーの声を集め調整いただく活動を、ますます進めていただければと期待いたします。

止まらないサービスを通じて、世の中のみんなを幸せにしたい

―ご意見ありがとうございます。期待に応えられるように努力してまいります。最後の質問となりますが、インターネットを通じて貴社が実現したいことはどのようなことでしょうか。

小笠原：私たちは、ニュートラルな立場でDCサービスを提供する側で、提供される側から見て、一番使いやすいDCがアット東京だと言ってもらえることを目標にしています。例えば、DCの顧客にはISP事業者様が多いですが、昔と比べるとISPのサービス単価はずいぶん下がっていますよね。少しでもお手伝いができて、共に発展できればと考えています。みなさんがどんどんDCに接続してもらえれば、我々だけでなくITサービスを提供する事業者様、ひいてはそこで提供されるサービスを利用する企業の方も共に発展できると考えています。最終的にはそれが個人の方々に還元されるわけですから、そういう意味で世の中のみんなが幸せになる、そんなDCになれれば嬉しいですね。

そのためには、止まらないDCサービスを提供することがとても重要で、その点では我々は自分たちのサービスが日本で一番堅牢だという自信があります。その自負を胸に、これからもファシリティにも力を入れ「24時間365日ノーダウンオペレーション」を掲げて取り組んでいきたいと思っています。

● DCでは安定した電力供給を実現しています

JPNIC 活動報告

JPNIC Activity Report

2016年12月～2017年3月のJPNIC関連イベント一覧

12月

5(月)	第116回臨時理事会(東京、JPNIC会議室)
16(金)	IETF報告会(97thソウル)(東京、JPNIC会議室)

1月

18(水)～20(金)	JANOG39 [協賛](石川、金沢市文化ホール)
19(木)	第47回ICANN報告会(東京、JPNIC会議室)
26(木)	IGF 2016に関する報告会／第17回日本インターネットガバナンス会議(東京、JPNIC会議室)
28(土)	IPv6ハンズオンワークショップ(広島、広島大学)
30(月)～31(火)	Security Days Fukuoka 2017 [後援](福岡、福岡国際会議場)

2月

6(月)～10(金)	JPNIC技術セミナー
8(水)	第117回通常理事会(東京、JPNIC会議室)
9(木)	IPv6 Summit in MIYAZAKI 2017 [後援](宮崎、宮日会館)
23(木)	Security Days Nagoya 2017 [後援](愛知、JPタワー名古屋ホール&カンファレンス)

3月

8(水)～10(金)	Security Days Spring 2017 東京 [後援](東京、JPタワーホール&カンファレンス)
16(木)	Security Days Spring 2017 大阪 [後援](大阪、ナレッジキャピタル・カンファレンスルーム)
17(金)	第60回臨時総会(東京、アーバンネット神田カンファレンス)

上記イベントのいくつかについては、次号66号にて報告いたします

IPv6関連イベントレポート

JPNICでは、IPv6アドレスの普及啓発のため、セミナーの開催や関連イベントへ参画しています。
本稿では、2016年11月1日(火)および2日(水)にJPNICが開催したIPv6対応セミナー(大阪)および2016年12月12日(月)に開催されたIPv6 Summit in KANAZAWA 2016の様子をご紹介します。

IPv6セミナー(大阪)を開催し、実際に初参加してみました！

◆ セミナーの開催概要

2016年11月1日(火)・2日(水)に、エヌ・ティ・ティ・スマートコネクト株式会社様とJPNICの共催で「IPv6対応セミナー」を開催しました。JPNICでは2015年から全国津々浦々でIPv6の普及啓発に向けたセミナーを企画してきました。高松、岡山、名古屋、福岡、仙台に続き6回目となる今回は、大阪での開催となりました。

今回のセミナーで会場となったのは、グランフロント大阪北館です。大阪駅・梅田駅から歩いて数分の好立地に、ショッピングモールやレストラン、オフィスなどが併設されており、とてもきれいでにぎわっていました。

セミナーは、座学とハンズオンの2日間にわたる構成です。1日目はIPv6に関する最新動向とネットワーク構築に関する基礎的な知識を学び、2日目では実機を用いてネットワークとサーバの構築を体験するという、知識と経験の両方を身につけることができるプログラムとなっています。講師は「IPv6教育専門家チーム」のメンバーが務めるほか、1日目のIPv6の最新動向をお伝えするセッションには、総務省データ通信課からスピーカを迎えてお話しいただきました。

● 1日目に行われた最新動向・基礎解説セミナーの様子

上の写真が1日目の会場の様子です。若手からベテランまで、多くの技術者の皆様に参加していただきました。また、2日目のハンズオンでは、機器の台数の関係上1日目より参加人数に限りが出てしまいましたが、少人数ゆえに積極的に質問がされていました。

◆ セミナーの内容を一部ご紹介！

実は私も今回初めてこのIPv6対応セミナーに参加しました。当日はスタッフとして会場運営を手伝いましたが、せっかくの機会ということでセミナーも受講し、IPv6について勉強しました。簡単ではありますが、受講体験記ということでセミナーの内容を一部ご紹介します。

1.IPv6の最新動向について

このセッションではIPv6対応の導入編として、IPv4アドレス在庫枯渇後の世界におけるIPv6を取り巻く状況や、総務省のIPv6対応ガイドラインが解説されました。

APNICのIPv4アドレスの在庫は2011年4月15日に枯渇しましたが、IPv4アドレスはまだ最小限を貰うことができるそうです。しかし、いつまでも貰えるわけではなく、現在のペースで分配が続いた場合、あと3年程度でなくなってしまいます。一方で、移転という手段でIPv4アドレスを譲ってもらう方法もありますが、オークションサイトでのIPv4アドレスの平均落札価格も年々高くなってきているそうで、IPv4を利用し続けることも、継続的なコスト増大というリスクが発生することが分かりました。

2.入門編

IPv6入門編と題されたこのセッションでは、IPv6の主な機能や特徴の紹介と、IPv6導入にむけた設計・構築・運用の方法が紹介されました。

そもそも、IPv6はIPv4と互換性がなく、IPv4を前提として作ったプログラムはIPv6の処理ができません。また、パケット形式やプロトコルが備える機能も異なっているので、セキュリティ対策などに注意が必要となっています。

では、実際にIPv6へ対応するにはどのようにしたらよいのでしょうか。IPv4からIPv4/IPv6対応ネットワークへの移行時の検討が重要となります。その対応モデルとしては

- IPv4/IPv6 Dual Stack Model
- IPv4 Networkと別にIPv6 Networkを構築するParallel Stack Model
- 一部をDual Stackに、一部をIPv4/IPv6それぞれに独立させるHybrid Model

IPv6 Seminar in Osaka

の三つがあります。このような共存技術は、構築が比較的容易で、既存機器がIPv6に対応していなくても、Parallel Stack Modelのように、IPv6ネットワーク用機器を追加する形でも対応が可能となります。一方で、デメリットとしては、ネットワーク側でIPv4 NAT/NATPTを維持し続ける必要があり、またIPv4/v6の両方の不具合を確認するという管理コストの増大も招いてしまうことが挙げられます。

三つの共存技術を紹介しましたが、実際の運用としては、IPv4で構築した機器にIPv6のプロトコルスタックを共存させる「IPv4/IPv6 Dual Stack Model」を採用することが多いようです。

3.ネットワーク構築編

2日目のハンズオンセッションでは、まずIPv6のネットワークを構築しました。実機を触る前に、座学でIPv4とIPv6におけるアドレス設定やルーティングの違いが解説されました。特にIPv6ではアドレスの自動設定がIPv4と異なるため、注意が必要だそうです。

ハンズオンでは、ルータにIPv6アドレスの設定、OSPFv3の設定をした後、経路切り替えの確認を行いました。ルータを設定することが初めての経験だったので、特にルーティング設定方法の話を聞いても最初は、難しくてよく理解できませんでした。しかし、講師の方に教えてもらいながらコマンドを入力してみることで、なんとかIPv6のネットワークを構築することができました。実際に自分の手を動かしてみると、より理解が深められるなあと改めて感じました。

4.サーバ構築編

ハンズオンセッション後半のサーバ構築編では、DNS(BIND 9)、SMTP(postfix)、POP(dovecot)、Apache、NTPなど、基礎サービスの設定方法を学び、ハンズオンではApacheの設定を行いました。Apacheは RHEL5/CentOS5以降、標準でIPv6 Readyになっているそうで、IPv4とIPv6環境でそれぞれWebサイトを作って、異なるサイトが表示されるかアクセスしてみるデモを行いました。

5.セミナーを受けてみて

IPv6対応セミナーに参加する前までは、「IPv6対応セミナーって、ものすごい専門家が、ものすごく専門的な講義をするんだろうな。聞いても分からないのでは？！」と少し不安に思っていました。しかし実際に受講してみると、入門編ではIPv6の特徴や運用する際に気をつけるポイントが紹介されていたり、ハンズオンでは実機を触りながら自分の手でネットワークやサーバを構築できたりと、かなり実践的でわかりやすい内容でした。

また、ハンズオンでは一歩進んだ中級用の資料も用意されており、IPv6についてある程度詳しい技術者の方々にとっても、さらに知識を深めることができる内容だったのではないかと思います。私のようなIPv6初心者でも、2日間のセミナーを通して、IPv6の最新動向から設計・構築・運用についてまで、幅広く学ぶことができました。

◆ 終わりに

一部しかご報告できず恐縮ですが、もしセミナーにご興味を持った方がいらっしゃいましたら、今後も各地で開催予定ですのでぜひ一度足をお運びください。また、「もっとこんなことを学びたい！」「当地でもぜひ開催して欲しい！」などなどご要望がございましたら、tech-seminar@nic.ad.jp までご連絡ください。最後になりましたが、今回大阪でのIPv6対応セミナーには、エヌ・ティ・ティ・スマートコネクト株式会社様の多大なご協力を賜りました。この場を借りてお礼申し上げます。

（JPNIC インターネット推進部 塩沢啓）

IPv6 Summit in KANAZAWA 2016 レポート

2016年12月12日（月）に石川県金沢市で、一般財団法人インターネット協会の主催によりIPv6 Summit in KANAZAWA 2016が開催されました。当日は午前にチュートリアルを実施した後、午後はIoTをテーマに基調講演とパネルディスカッションが行われました。

このIPv6 Summit in KANAZAWA 2016の模様をJPNICブログでご紹介しています。レポートは次のURLからご覧ください。

IPv6 Summit in KANAZAWA 2016 レポート
https://blog.nic.ad.jp/blog/ipv6_summit8/

● 右手がコーディネータをつとめるアラクサラネットワークス株式会社の新善文氏
パネリスト：左手前から、IPv6普及・高度化推進協議会の渡辺露文氏、北陸先端科学技術大学院大学の丹康雄氏、金沢大学の大野裕之氏、一般社団法人コード・フォー・カナザワ理事の井澤志充氏

第31回JPNICオープンポリシーミーティング報告

2016年11月30日（水）に、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にて、Internet Week 2016との同時開催イベントとして、第31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。今回は番号資源の管理ポリシーに関する提案はなく、8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34名（関係者含まず）の皆様に参加いただきました。リモート参加では、ユニークなアクセス数は63、平均で15人前後のアクセスがありました。以降、情報提供された中から、三つのトピックスについて報告します。

関連記事：P.23 APNIC 42カンファレンス報告

◆ Prop-116：Prohibit to transfer IPv4 addresses in the final /8 block紹介と意見交換

2016年9月下旬から10月上旬にスリランカにおいて行われたAPNIC 42で提案され、コンセンサスに至らず継続議論となったProp-116に関して、提案者の藤崎智宏氏（日本電信電話株式会社）から提案内容の紹介が行われました。Final /8ポリシーとして今までとは異なる配布がされている103/8が、新規事業者向けに分配するという本来の目的ではなく、そのアドレスそのものを移転することを目的に取得されているように見えることから、Prop-116では103/8ブロックの移転を禁止する等のポリシーの改定提案が行われています。

◆ WHOIS登録情報正確性向上に向けての動向と意見交換～法執行機関からの要望への対応～

WHOISは昨今、ネットワークトラブルシューティング目的で技術者が利用するだけではなく、公安・サイバー犯罪対策のために法執行機関にも利用されています。

WHOISに現状登録されている情報は、正確と言い難いものも散見され、その状況を重く見た米国FBIのJesse Schibilia氏から、WHOIS登録情報正確性向上に向けて、現状の課題や事例の紹介が行われ、また、法執行機関の連携によるWHOISに関するポリシー提案の現状や、今後の予定などが説明されました。Schibilia氏らは、2017年秋の施行を目標に、五つのRIRでWHOISに関するポリシー提案を進めていくとのことでした。

● 米国FBIのJesse Schibilia氏によるプレゼンテーション

◆ 米国政府からのIANA機能監督権限移管完了のご報告

米国政府からグローバルインターネットコミュニティへのIANA機能監督権限移管が、2014年3月の米国政府からの発表から約2年半の期間を経て、2016年10月1日についに完了しました。今回は、この課題に長期にわたり深く関わってきたJPNICの奥谷泉氏から、全体のまとめとして、これまでの経緯や各方面の動き、振り返りなどの発表が行われました。その他、現状の日本におけるポリシー策定プロセス（PDP）の解説、APNIC 42やARIN 38、NANOG 68のカンファレンスレポ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

今回のJPOPMはポリシー提案はなかったものの、WHOIS登録情報正確性向上やIANA機能監督権限移管完了等、興味深い話題が多数話されました。特にWHOIS登録情報正確性向上については、各RIRでの提案が予定されていることや、仮にWHOISのポリシーの変更が行われた場合に関係する方々に大きな影響が予想されることから、今後のJPOPMでも継続的に取り上げていくことになると思います。

当日行われた議論に関しては当日の議事録をご参照ください。また、今回のJPOPMでは新しい試みとして、ポリシーWGメンバーからの発表として「知らないと損するIPアドレスの話」と「アドレスポリシー解説」を行いました。どちらの発表も、みなさんがポリシーを読み解いていくための足掛かりとなるような発表を目指しました。

当日の発表資料、議事録および録音は、次のサイトに掲載しております。

第31回JPNICオープンポリシーミーティングプログラム
http://jpopf.net/JPOPM31Program

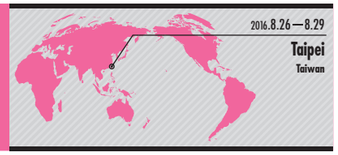
なお、第32回JPNICオープンポリシーミーティングについては2017年7月をめどに開催を予定しております。詳細が確定し次第、IP-USERSメーリングリストにてお知らせいたします。

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

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 谷崎文義）

APrIGF2016 in Taipei レポート



本稿では、2016年8月26日（金）～29日（月）に台湾・台北で開催された、APrIGF2016の様子をご報告します。正式名称を「Asia Pacific Regional Internet Governance Forum」とする本会議は、その名の通り、インターネットガバナンスについて、アジア太平洋地域の視点から議論を行う会議です。グローバルIGFと同じように毎年ホスト国が異なりますが、リージョナルIGFは国連が主催するグローバルIGFと異なり、地域のコミュニティから草の根的に発展したものです。APrIGFは2010年香港で開催されたのが最初でした。

◆ 全体概要

今回のAPrIGFは台湾情報基盤振興協会（NII）が主催し、事前の参加登録者が500人超、現地での参加者も300人以上、遠隔参加者は380人と、過去最大の参加者数を記録したということです。日本からも開催地が近いためか企業、大学、総務省から合計10数名の方が参加・登壇されていました。

プログラムは人権とプライバシー、セキュリティ、資源管理など万遍ない内容構成のもと、3日間にわたって、1日3コマ概ね常時3トラックがパラレルで走り、合計約30セッションが開催されました。

● オープニングセッションの様子

◆ プログラム・議論の様子

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

Program Agenda
https://2016.aprigf.asia/program/agenda/

筆者は「アジア太平洋地域におけるIPv6」というセッションを企画し、モデレーションを行いました。IPv6については2015年、2016年とグローバルIGFでもIPv6 Best Practices Forumと呼ばれる議論の場が設けられ、最適な実例を文書化する取り組みがあるため、アジア太平洋地域のIGFでも同じ議論を行い、グローバルな場に地域の状況をインプットする必要性を感じたためです。同じアジア太平洋地域における会議ですが、技術面でのフォーカスが強いAPNIC会議では共有されない、政府・企業・国全体としての取り組みについて意見交換を行い、スリランカ、アフガニスタン等、あまり聞くことのできない個別事情を聞くことができました。あわせて、グローバルIGFにおけるBest Practices Forumの動向を共有したことにより、アジア太平洋地域とグローバルな動向の連携にもつながったように思います。

その他にも、

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

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

◆ グローバルとの連携強化

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

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

◆ APrIGF2016の振り返り

「アジア太平洋地域」の議論の場ではオーストラリア、ニュージーランドの参加者が発言の中心となることが多いのですが、今回のAPrIGFでは、地域内の参加者がバランスよく発言を行っていたように思います。グローバルな場でも一定のプレセンスのある香港、中国、インドに加え、ローカルホストを務めた台湾、韓国、フィリピンからの参加が目立ち、南アジアからもインドの他にネパール、スリランカ等の国からの参加が見受けられました。

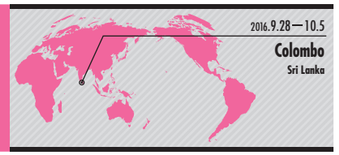
通常、グローバルな場でアジア太平洋地域からの議論への参加は活発ではないことから、APrIGFでここまで活発が議論が行われていることを想定していませんでした。実際には、登壇者・参加者はグローバルな場で議論される問題もよく追った上で、各国の事情を紹介しており、議論のレベル・問題への認識共に、日本国内の議論と比較して大変高いもので、それぞれの国における議論がAPrIGFと同じレベルであるかはまた別の可能性はあるものの、日本インターネットガバナンス会議（IGCJ）にも関わっている立場から、大変よい刺激を受けました。

◆ 次回のAPrIGF

次回2017年のAPrIGFは、7月26～29日にタイのバンコクで開催される予定です。

（JPNIC インターネット推進部 奥谷泉）

APNIC 42カンファレンス報告



関連記事：P.21 第31回JPNICオープンポリシーミーティング報告

2016年9月28日（水）～10月5日（水）にわたり、APNIC 42カンファレンスがスリランカのコロンボで開催されました。39の国や地域から443名の参加登録があり、332名が実際に会場に足を運んだとのことです。また、APNIC会員約5,600のうち133から参加がありました。本稿ではこのAPNIC 42カンファレンスの様子を、アドレスポリシーおよび技術動向を中心にご紹介します。

アドレスポリシー関連報告

◆ カンファレンスの構成について

APNIC 42カンファレンスではこれまでと同様に、会期を大きく二つに分けてプログラムが構成されました。

会期前半は「ワークショップ」が開催されました。10月3日（月）からは「チュートリアル」「SIG（Special Interest Groups）」「BoF（Birds of a Feather）」「AMM」の会議・セッションが開催されました。これら以外にも、APNICと関連の深い、APIX（Asia Pacific Internet Exchange Association）やFIRST（the Forum of Incident Response and Security Teams）が主催する、会議・セッションが設けられていました。

当日の資料、ビデオ、発言録は、APNICカンファレンスのページ（https://conference.apnic.net/42/program#）に掲載されています。

◆ アドレスに関するポリシー提案の結果について

今回は、ポリシー提案1点のみについて議論が行われました。提案の内容についてご紹介します。

・「APNICにおける最後の/8相当のIPv4未割り振り在庫」の移転禁止提案（提案番号：prop-116）

提案者	藤崎智宏氏
概　要	「APNICにおける最後の/8相当のIPv4未割り振り在庫」の移転を禁止する旨をポリシーに追加する （提案の詳細）http://www.apnic.net/policy/proposals/prop-116 （補足事項） ・上記在庫から割り振りを受けたIPv4アドレスが不要となった場合、割り振りを受けた組織はAPNICに返却する ・M&A（事業移管や吸収合併など、その事実を書面などで客観的に確認できるケース）による移管で、移管先組織が上記在庫から/22の割り振りを受けることとなった場合、/22を超えるアドレスについてはAPNICに返却する
結　果	継続議論

現在APNIC地域では、1組織あたり「APNICにおける最後の/8相当のIPv4未割り振り在庫」から/22（1,024アドレス）、「IANAから再割り振りされたIPv4返却在庫」から/22の、合計/21（2,048アドレス）の割り振りが行われています。特に「APNICにおける最後の/8相当のIPv4未割り振り在庫」からの/22の割り振りは、これから新規参入する組織に対して、必要最小限の割り振りを行うことを目的として考えられています。

新規の割り振りは堅調に伸びる一方で、M&Aによる移管や、IPv4アドレスの分配先を変更するIPv4アドレス移転制度を利用して、複数の/22を他の組織から受け取るといったケースも増えてきているようです。一つの組織が複数の/22を他の組織から受け取るような、本来の目的とは異なるアドレスの分配を防ぐことを目的として、今回提案が行われました。

当日の議論では、移転を禁止することで、WHOISデータベースに登録された分配先組織ではなく、その分配先組織と私的な契約を結んだ第三者にアドレスを利用させるようなケースが出てくるのではないかと懸念するコメントが出されていました。データベース登録情報から実際のアドレス利用者がわからなくなってしまった場合、分配先を登録しておくためのWHOISデータベースの信頼性が損なわれることや、不正利用の際に連絡先を把握できなくなってしまうことを危惧する参加者が多かったのではないでしょうか。

この提案は、継続議論とする結果となりましたが、提案者は今回の議論内容を踏まえて提案内容を改訂し、次回以降のカンファレンスにおいてさらなる議論が行われる予定です。

・「SIGの運営方法を定めたSIGガイドライン」の改訂

IPアドレス・AS番号の分配ルールであるポリシーの変更提案ではありませんが、今回のAPNICカンファレンスでは、「SIGの運営方法を定めたSIGガイドライン」の改訂についても議論が行われています。こちらについても議論の結果、継続議論となっていますが、ここではその改訂点について、簡単にご紹介します。

1. 現行のガイドラインでは、会場にいる参加者すべてがSIG Chair選挙において投票できるようになっています。この投票資格を、参加登録を行っている者（リモート参加者を含む）に限定するよう変更しようというものです。

2. SIG ChairおよびSIG Co-Chairの任期は2年となっており、原則として隔年でChairとCo-Chairの選挙を行っています。この原則を維持できるよう、任期途中でChairまたはCo-Chairが辞任した場合に、新たに選出されたChairまたはCo-Chairの任期を、辞任した者の任期を引き継ぐこととする旨を定めようというものです。

特に1.については、APNICが現在提供するリモート参加の方法では、本人確認の方法がありません。この状態でリモート参加者まで対象に含めてしまうと、特定の候補者を当選させたいために、1人で複数投票するようなケースが起きることを懸念する参加者が多かったように思いました。そのため、「IETFのリモート参加者のように、通常の参加者と同様の参加登録を行った者のみとする」「過去のAPNICミーティングに参加経験がある者のみとする」「現地での参加者のみとする」「APNIC会員に限定する」など、何らかの形で投票資格を限定すべきとのコメントが多く出されていました。

◆ WHOISの正確性向上について

前回のAPNIC 41カンファレンスと同様に、アドレスポリシーSIGでは、WHOISの正確性向上に関する話題が取り上げられていました。

今回は、スリランカ警察やFBIをはじめとする法執行機関からの、WHOISに対する考え方が紹介されていました。スリランカ警察の担当者からは、サイバー犯罪では対象のIPアドレスを把握した上で、さまざまなツールを利用して捜査を行う点、それらの捜査を行うための基礎データとしてWHOISを利用している点が紹介されました。WHOISに登録された情報のうち、特にIPアドレスの割り当て先組織に関する情報が正確に登録されていることが、迅速な捜査につながると指摘していました。

FBIの担当者からは、実際に起きたサイバー犯罪の例として、米国カリフォルニア州で起きた事例が紹介されました。この事例では、不正確で長期間登録情報の更新が行われていないWHOIS情報から、対象のIPアドレスを選び出し、そのアドレスをハイジャックしてスパムを大量送信し、その結果、数百万ドルの損害をもたらしたそうです。FBIでは、そのようなWHOIS情報が、犯罪に利用されることに注目しているそうです。

これらの法執行機関からの報告では、WHOISの正確性を非常に重要視していることが明らかになりました。またFBIでは、すべてのRIRを対象にして、登録情報を正確にするためのポリシー提案を行うことも予定しているとのことでした。

◆ 選挙結果のご紹介

APNICカンファレンスでは、情報提供やポリシー提案に関する議論のほかにも、各種選挙が行われます。今回行われたNRO NCおよびNIR（国別インターネットレジストリ）に関わる事項について議論を行うNIR SIGの、Chair選挙結果をご紹介します。

NRO NC	Brajesh Jain氏（Citycom Networks Pvt Ltd.（インド）・初当選）
NRO NCは、ICANN理事会がグローバルポリシーを承認する上で、アドバイスを行う役割を担います。ポリシーフォーラムより選出された2名と、RIRの理事会が指名する1名の合計3名を、各RIR地域の代表者とし五つのRIRから合計15名で、NRO NCを構成しています。 Brajesh氏は、任期満了に伴い退任するAjay Kumar氏（インド）に代わり、2017年1月から2年間の任期でNRO NCの役割を担います。	

NIR SIG Chair	Shyam Nair氏（Sify Technologies（インド）・初当選）
NIRに関する議論を行うNIR SIGにおいても、退任した橘俊男氏（日本）に代わる、新たなChairの選出が行われました。	

● カンファレンスの様子

（JPNIC IP事業部 川端宏生）

技術動向報告

◆ オープニング・プレナリでの発表について

APNIC 42が開催されたスリランカは、インド、バングラデシュ、ミャンマーなどが面する、ベンガル湾にある島国です。ベンガル湾地域の人口を約13億人と計算すると、米国の約3億人を大きく上回ることから、インターネット人口も米国のそれを大きく上回ると考えられています。

この地域のコネクティビティを支えるのは、インドの東岸とバングラデシュの南岸、ミャンマーの南岸を結ぶ海底ケーブルです。現在のスリランカの経済成長に見られるように、今後この地域が経済発展していくことを踏まえると、インターネットの物理的な接続の施策も、重要な位置づけになると考えられます。地政学的な視点を交えた興味深い発表でした。

Connectivity in the Bay of Bengal　Rohan Samarajiva氏
http://cgi1.apnic.net/conference_data/files/APSr107/samarajiva_presentation_apnic_oct16_1474455927.pdf

◆ APNIC 42で開催された技術的なセッションのテーマ

APNICカンファレンスでは、IPアドレスポリシーの議論が行われるPolicy SIGや、APNICの総会であるAMMの他に、技術的なセッションが開かれています。これまで、これらのセッションはAPOPS（The Asia Pacific OPeratorS forum）と呼ばれていましたが、今回のAPNICカンファレンスでは、テーマごとに個別のセッションが開かれていました。

これまでのAPNICカンファレンスでは、DNSやIPアドレス・ルーティングを中心とした、技術的な話題がAPOPSで取り上げられてきましたが、今回はインシデント対応により重点を置いたプログラム構成に変わってきたようです。例えば、3日目に国際的なCSIRTをメンバーとする非営利のFIRSTによるセッションが開かれており、また、インシデントに関する調査研究で知られる米国の非営利組織、Team CYMRU所属の方による講演が注目を集めていました。

1日目	https://conference.apnic.net/42/program#/schedule/day/6
- IPv6移行ストラテジー（チュートリアル） - ネットワークの性能 - DNSとインターネット番号資源（INR）のセキュリティ	
2日目	https://conference.apnic.net/42/program#/schedule/day/7
- IoTイントロダクション - ネットワーク運用 - IXPデザインと運用のベストカレントプラクティス - ネットワークSSR - IPv6対応計測BoF	
3日目	https://conference.apnic.net/42/program#/schedule/day/8
- FIRSTテクニカル・コロキア	

3日間のセッションに加えて、国別インターネットレジストリ（NIR）の動向を踏まえて3点報告します。

【1】FIRSTテクニカル・コロキア

FIRSTテクニカル・コロキア（TC）は、FIRST主催のセキュリティに関するセッションです。テクニカル・コロキアとは技術的なセミナーの意味で、APNIC 42の参加者も参加できるという位置づけで開催されました。

- Meet Remaiten: LinuxベースのルータやIoTデバイス用のボットネット開発,
  Afifa Abbas氏, Banglalink Digital Communications Limited
  http://cgi1.apnic.net/conference_data/files/APSr107/afifa-apnic-change_1475632543.pdf

- DDoSMon.net: グローバル DDoSモニタリングシステム,
Yiming Gong氏, Network Security Research Lab,Qihoo 360
http://cgi1.apnic.net/conference_data/files/APSr107/ddosmon-apnic-42_1475580565.pdf

- 技術/運用/ポリシーの枠を超えた情報共有による協力について,
Merike Kaeo氏, FARSIGHT Security
http://cgi1.apnic.net/conference_data/files/APSr107/information-exchange-collaboration-across-technical-operational-policy-boundaries.pdf

この他に、フィッシングを行うグループにとっては、Webページを使ったフィッシングと、自動預払機（ATM）におけるスキミングが、金銭をだまし取る「手段」として同列に位置づけられていることから、スキミングの実態を映像で紹介する講演もありました。

【2】インターネットにおけるIPv6の性能

国際的に導入が進められているIPv6の信頼性や通信速度に注目した調査が、APNICで行われています。チーフサイエンティストのGeoff Huston氏によって講演されました。世界のIPv6のネットワークに信頼性はあるのか、IPv6のネットワークは「速い」のかという、素朴な疑問に応える調査です。前回のAPNIC 41に続いて、さらに蓄積されたデータを分析した結果が報告されました。

信頼性については、TCPのコネクションがすべて確立するのかどうか、通信速度については遅延（RTT）を比較して調査されています。具体的には、Google社のAdWordsに登録された小さな画像を、あらかじめデュアルスタックのサーバに置いておき、ユーザーのWebブラウザから取得される様子を観測します。

その結果、アクセスされたユニキャストのIPv6アドレスの1.5%が、TCPコネクションの確立に失敗していることがわかります。単純に比べられるデータではありませんが、同じ調査でIPv4が0.2%と示されており、また前回の2015年の調査結果と大きく変わっていません。6to4のネットワークは、コネクション確立の成功率が低いことも、変わらず観測されました。通信速度については、IPv6のパケットがIPv4と違って、ネットワーク的に遠いルータを経由していると考えられるアドレスも見つかりました。講演のスライドには、国別の比較結果なども入っています。

IPv6 Performance（revisited）,Geoff Huston氏, APNIC
http://cgi1.apnic.net/conference_data/files/APSr107/ipv6-performance-revisited.pdf

【3】RPKIの動向 ～APNICの五つのCAとNIRの動き～

リソースRPKI（RPKI）は、IPアドレスなどのアドレス資源の割り振り／割り当ての証明書を発行する公開鍵基盤（PKI）です。インターネット経路制御のセキュリティ技術である、BGPSECなどで利用することができます。現在、アジア太平洋地域では、APNICとJPNICでRPKIのリソース証明書発行サービスが提供されており（JPNICは試験提供）、他のNIRでも調査研究やシステム開発が進められています。

APNICでは、MyAPNICで提供されているRPKIのGUIを改良し、IRR（Internet Routing Registry）のrouteオブジェクトを同じ画面に表示して比較できるようになりました。しかし、以前から大きな課題になっている、JPNICとAPNICのRPKIシステムが連携していない点については、進展がありませんでした。Huston氏は、APNICのRPKIシステムが複雑になっていて、JPNICとの接続を妨げる要因の一つになっていることと、APNICの五つの認証局（CA）について説明し、これを一つにすべきかどうかを問いかけていました。

RPKIトラストアンカー, Geoff Huston氏, APNIC
http://cgi1.apnic.net/conference_data/files/APSr107/2016-10-3-rpki-ta_1475113158.pdf

NIRの中では、中国のNIRであるCNNICの取り組みが活発です。テストベッドを運用しており、ISPを交えた技術検証を行っています。またCNNICは、RPKIの標準化活動を行っているIETF SIDR WGでも、RPKI運用上の課題を指摘するInternet-Draftを発表するなどしています。現在、RPKIシステムの開発を行っており、2016年12月までに一旦完了するとしています。その他のNIRでは、韓国のKRNICやインドのIRINNも、RPKIのサービス提供に前向きで情報収集をしていました。

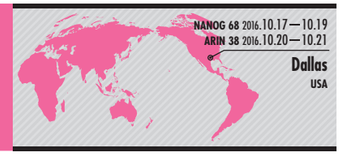
◆ 次回以降のAPNICカンファレンスについて

次回のAPNIC 43カンファレンスはAPRICOT 2017と共催となり、2017年2月20日（月）～3月2日（木）に、ベトナム・ホーチミンシティでの開催が予定されています。

また、2017年9月頃開催予定のAPNIC 44カンファレンスは台湾・台中で、2018年春に開催予定のAPRICOT 2018/APNIC 45カンファレンスはネパール・カトマンズでの開催が予定されている旨も、併せて発表されています。

（JPNIC 技術部／インターネット推進部 木村泰司）

NANOG 68/ ARIN 38ミーティングレポート



米国テキサス州ダラスで開催された、NANOG（The North American Network Operators' Group）のミーティングであるNANOG 68（2016年10月17日（月）～19日（水））と、北米地域を担当する地域インターネットレジストリ（RIR）であるARIN（American Registry for Internet Numbers）のARIN 38（2016年10月20日（木）～21日（金））ミーティングに参加しました。秋のミーティングの恒例として、NANOGとARINは連続して開催されています。また、今回はDNSに関する計測・研究について情報交換・議論を行っているDNS-OARC（The DNS Operations, Analysis, and Research Center）※1のミーティングも10月15日（土）～16日（日）に開催されました。本稿では、NANOG 68およびARIN 38について興味深かった内容をご報告します。

NANOG 68について

◆ 全体概要

NANOG 68は、開催日前日時点で1,012名の参加登録があったと報告されました。その一方で、ほとんどの参加者は個別の会議等、参加者とのネットワーキングに注力していたようで、一部のPlenaryセッション以外はセッションへの参加者数は100名程度のこともありました。アジェンダのページ※2から、議論の映像や資料が参照いただけます。

3日間で約30セッションもの多様な議論が行われ、最終日にはVint Cerf氏もIoTに関するキーノート講演「Internet of Things」を行いました。NANOGのflickrでは、さまざまな写真が掲載されています。

NANOG 68（NANOGによるフォトアルバム）
https://www.flickr.com/photos/nanog/sets/72157675237661236

◆ オープニングキーノート講演：IANA Transition

IANA機能を担っていたJon Postel氏に近しかった当時を知る立場から、Scott Bradner氏による、IANA機能を取り巻く歴史と、そこから見たIANA監督権限移管についての発表でした。期待していたほど移管を受けた今後の話は少なく、過去の経緯に重点が置かれていましたが、当事者ならではのエピソードが紹介されたという点で興味深く、また運用コミュニティのオープニングセッションで、このようなテーマが扱われることが新鮮でした。

エピソード例：
1. 当初RIRは、新たな組織化されたIANA（つまりICANN管理下のIANA）には消極的だったが、Jon Postel氏としてはプロトコルパラメータも含めて一緒に管理するとの意向であった
2. 当時米国政府の中では、IANAの管理に関する権限を手放すことは、インターネットのガバナンスを米国が手放すことであるとの懸念があったが、なんとかICANNという民間組織の設立を説得した
3. 一方、ICANNにおける仕組みは、Jon Postel氏の意向とは異なる形で実装された部分も少なくない

◆ Desperately Seeking Default

最近のグローバルな経路情報から見える事象について指摘した、APNICのチーフサイエンティストであるGeoff Huston氏の発表です。同様の発表は、P.23でもレポートしている通りスリランカ・コロンボで開催されたAPNIC 42カンファレンスでも行われています。主な内容は次の通りです。

- グローバルな経路情報は、どの上流もある程度共通の情報を持ち、最終的な到達性はどこも変わらない前提で上流を選んでいる可能性があること
- 一方で、インターネットから見えるグローバルな経路情報を見ていくと、Tier1レベルのISPでもまちまちであること
- 計測から、Peer to Peerの接続よりも、CDNや大手コンテンツへのアクセスが主流となっていること

◆ Security Track

このセッションは、セキュリティに関する各種計測・研究者からの発表のシリーズでした。印象的だったのは、中国からの発表者2名による、DDoSをリアルタイムに検出できるシステム・研究の紹介です。誰でも登録すれば、DDoSのリアルタイムに状況分析した結果を送ってくれるそうです。

※1 DNS-OARC
https://www.dns-oarc.net/

※2 NANOG 68 Agenda
https://nanog.org/meetings/nanog68/agenda

会場では、セキュリティ分野における専門家から取り組みを評価する意見や、DDoS攻撃を受けた場合、多くの時間が状況分析に費やされているため、リアルタイムの分析が受けられることは助かるといったコメントがありました。この発表は、APNIC 42カンファレンスのFIRSTセッションでも行われています。中国からの技術者が、昨今IETFで積極的に提案していることは耳にしていましたが、NANOGでも発表していることが印象的でした。

◆ その他

1.Large BGP Communities
32ビットのBGP Communityは、2バイトAS番号では問題ないが、4バイトAS番号においてはビット数が足りず、本来の目的が実現できないため、BGP Communityを拡張する提案が現在IETFで行われているそうです。

2.The Best of OARC25
NANOG 68と背中合わせで開催した、DNS-OARCのミーティングにおける議論の紹介です。ひとまとめにDNS関連の動向が確認できます。なお、DNS-OARCは欧州地域のRIRであるRIPE NCC（RIPE Network Coordination Centre）の会議、ICANNの会議等、業界におけるさまざまな会議と併せて開催しています。

3.Internet-scale virtual networking with ILA
Facebook社が、物理的な機器の大規模移動を頻繁に行うため、IPv6におけるila機能（アドレスの識別子としての役割と、物理的な場所を示す役割を分ける機能）を利用した事例の紹介です。

◆ NANOG38ミーティング後：Dyn社への攻撃

そして、NANOG 68会議開催後ではありますが、DNSサービスを提供しているDyn社に対して攻撃が行われたことについて、NANOGのメーリングリスト（ML）で議論が活性化しました。

Dyn社は、セキュリティ対応のためトラフィックの遮断目的でBGPハイジャックが行われている事例を紹介した「Back Connect's Suspicious BGP Hijacks」の発表を行い、その直後に攻撃が行われたことから、報復攻撃を受けたのではないかとの見方もありますが、真相は定かではありません。また、監視カメラ等のIoTを踏み台にした可能性があることから、BBCや一般メディアでも取り上げられています。

NANOGのMLでは、オペレータとしてできることを考えようという議論の中で、JANOG（JApan Network Operators' Group）のMLでも紹介されているMutually Agreed Norms for Routing Security（MANRS）※3等、必要最低限の対策をとることなどを呼びかける投稿も見受けられます。

ARIN 38について

◆ 全体概要

ARIN 38の参加者は、NANOG 68参加者の約10%強となる約130名でした。ARIN地域では、IPv4アドレス移転時における必要性証明要件に関する議論が続いています。今回は、合計八つの提案が議論されました。事前に登録することで、ポリシー提案に対してオンラインでの支持表明も可能でした。また、カリブ海を中心にフェローの参加も促進しており、やる気のある新たな参加者も見受けられました。

また今回は、ARIN Advisory Council（ARIN AC）およびARIN理事の選挙が実施され、理事メンバーとしてBill Sandiford氏、Patrick Gilmore氏が就任しました。そして、これまで理事長を務めてきたVint Cerf氏がこの会議で理事の退任を発表し、副議長であるPaul Anderson氏が議長の座を引きつぐことになりました。ミーティングの様子は、ARINのFacebookページにいろいろな写真が掲載されています。

ARIN 38（ARINによるフォトアルバム）
https://www.facebook.com/media/set/?set=a.10153828908241290.1073741845.60264976289&type=3

● 退任の挨拶を行ったVint Cerf氏（ARINのFacebookページより引用）

◆ WHOIS登録情報の正確性向上に向けた法執行機関による発表

連邦捜査局（FBI）、アメリカ麻薬取締局、カナダ警察といった法執行機関より、WHOISは従来想定された用途であるネットワークのトラブル解決のみではなく、公安のために利用されていることが事例を交えて紹介されました。同様の発表は、APNIC 42でも行われています。

特にARINやRIPE地域において、ローカルインターネットレジストリ（LIR）ではないISPへの再割り振りが比較的多く、情報が正確に維持されていないことについて問題視しているようです。今後は2017年春に向けて、全RIR地域でポリシー提案として議論を進めていくとのことでした。

関連記事：P.23 APNIC 42カンファレンス報告

ARIN会議ではFBI、RIPE会議では欧州刑事警察機構（Europol）が定期的に参加しており、インターネットが経済社会活動の基盤となっている今日では、RIRのミーティングも、従来のような運用者、アドレス管理担当者のみではなく、こういった法執行機関など、より幅広い関係者も交えた議論が必要な局面を迎えているようです。

◆ アドレスポリシー動向

ARIN 38での議論の中心は、IPv4アドレス移転の要件緩和でした。ARIN地域は、投機目的でのアドレス移転を防止するため、移転ポリシー施行時からIPv4アドレス移転時の必要性証明を重視してきましたが、実態に合わないことから、この要件を緩和される方向で各種提案が議論されました。個々の提案については、JPNICブログで紹介していますので、ご参照ください。

ARIN 38がダラスで開催されます
https://blog.nic.ad.jp/blog/arin38-policy-proposal/

この他に、APNIC、RIPEでもAS番号の割り当てに関し、マルチホーム要件を撤廃するなど緩和する傾向があることから、ARIN事務局からのポリシー実装報告の中で、AS番号割り当てにおけるマルチホーム要件撤廃についての賛意が表明されました。これにより、ARIN地域でも今後AS番号の割り当て要件が緩和される方向に進むと思われますが、一方で、AS番号の割り当てが増えることでルーティングにどのような影響を及ぼすのか、注視していきたいところです。

◆ その他

ARINコミュニティメンバーのボランティア活動として、ARINミーティングでIETFにおける議論の共有を行っており、今回は2016年7月開催のIETF 96について、包括的な報告がありました。その他にも、参加者の情報交換を目的とした非公式会合であるIEPG Meetingでの、ルーティングやDNS、IPv6に関する議論について共有されました。詳細については、「IEPG Meeting - July 2016 @ IETF 96」※4も併せてご参照ください。

◆ 次回のミーティングについて

次回のNANOG 69ミーティングは、2017年2月6日（月）～8日（水）に米国ワシントンDCで開催されます。また、次回のARIN 39ミーティングは、2017年4月2日（日）～5日（水）に、米国ルイジアナ州のニューオーリンズで開催されます。

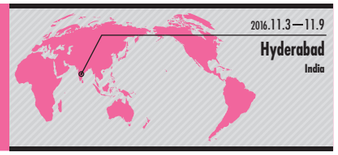
（JPNIC インターネット推進部 奥谷泉）


● ARIN 38ミーティングの様子

※3 Mutually Agreed Norms for Routing Security（MANRS）
https://www.routingmanifesto.org/manrs/

※4 IEPG Meeting - July 2016 @ IETF 96
http://iepg.org/2016-07-16-ietf96/index.html

ICANNハイデラバード会議報告



2016年11月3日（木）から9日（水）にかけて、インドのハイデラバードにて第57回ICANN会議が開催されました。また、このハイデラバードの会議で当センターの前村昌紀がICANN理事を拝命しました。本稿では、このハイデラバード会議の様子をご紹介します。また、前村からの所信表明についてもお届けします。

◆ はじめに

第57回ICANN会議は、ハイデラバードにあるHyderabad International Convention Centre（HICC）で7日間にわたり開催されました。

2015年10月に発表された、「新会議戦略※1」にのっとった3度目となる今回の会議は、「会議C」という7日間構成の大規模版であるとともに、年次総会（Annual General Meeting）とも位置づけられます。参加者数は3,200人を超え、過去最大を数えました。うち1,000人以上は、インドからの参加者とのことです。

また、ICANN会議のプレイベントとして、India School of Internet Governance※2という、学生向けの教育イベントが行われました。JPNICからは、奥谷泉が講師として参加しましたが、充実したプログラムや受講者の真摯な参加姿勢に感心したようです。これらは、インドにおけるICANNへの関心の高さを印象付けました。

◆ 資源管理ポリシーに関する検討の進捗は小康状態

資源管理ポリシーなどに関する検討活動では、作業部会ごとにそれぞれの進捗がありましたが、今回のハイデラバード会議で特に大きな節目を迎えたものはありませんでした。以降、主だった項目について簡単に状況を記します。

・次世代登録ディレクトリサービス（RDS）

ポリシー策定プロセスの初期にあたる、作業部会の検討が始まりました。利用目的やデータ要素などに関する、基本的要件を検討している段階です。

・新gTLD次回ラウンドに向けた手続き

作業部会は「申請者支援」「法規制・契約」「異議申立手続き」「技術運用事項」の、四つのワークトラック（WT）に分かれて次の5点を論点として検討が開始されています。

（1）レジストリ契約のタイプ分け
（2）緊急バックエンドレジストリ事業者（EBERO）の要否
（3）継続的申請受付の可能性
（4）1文字のみからなるIDN TLDの可否
（5）TLD名前衝突問題への対処

・権利保護メカニズム（RPM）のレビュー

新gTLDの委任後紛争解決手続き（PD-DRP）と、Trademark Clearinghouse（TMCH）に焦点を当てた検討が進んでいます。

・オークション収益に関するクロスコミュニティ作業部会

申請者間で競合した文字列に対するオークションの収入について検討する作業部会において、趣意書が採択されました。作業部会メンバーが寄附金受領者となり得るケースが大きな問題となっていましたが、作業部会加入にあたり、利害宣誓を厳格に行うという条件が盛り込まれました。

◆ JPNIC奥谷がリーダーシップアワードを受賞

今回のICANN会議は、2016年10月1日のIANA監督権限移管以降、初めての会議でした。年次総会で授賞されるリーダーシップアワードは通常1名なのですが、今年はIANA監督権限移管の提案検討に携わった、五つのコミュニティ会議体すべての議長に授与されることが決定されました。オープニングセレモニーの中で実施された授賞式において、CRISP（Consolidated RIR IANA Stewardship Proposal）チームの議長を務めたJPNICの奥谷泉も、この賞を受けました。※3

◆ 理事の退任と就任

現在ICANN理事は、選任方法に依らず年次総会のタイミングで就任するように決まっています。今回20名の理事のうち5名が入れ替わるということで、理事会は大きな陣容変更となりました。現在の理事会の陣容は、JPNICのICANN理事会ページでご覧いただけます。※4

ASO選出	Kuo-Wei Wu → 前村昌紀
GNSO選出	Bruce Tonkin → Becky Burr
指名委員会選出	Erika Mann → Maarten Botterman Bruno Lanvin → Khaled Koubaa
RSSACリエゾン	Suzanne Woolf → Kaveh Ranjbar

11月8日（火）に行われた年次総会が理事会陣容切り替えのタイミングで、通常の理事会と、新陣容による役職指名のための理事会が続けて行われました。退任する理事は通常の理事会までが任期、就任する理事は役職指名理事会からが任期、となります。このタイミングで、私も理事に就任したことになります。この後行われたパブリックフォーラムでは、開催地域であるアジア太平洋地域の理事として、一つの区分の司会も行いました。

◆ 説明責任の強化に向けた検討

ICANNの説明責任強化に向けた取り組みについてはハイデラバード会議開催の前日、11月2日（水）にCCWT-ACCT（Cross Community Working Group on Enhancing Accountability）の会合が開催され、終日議論が行われました。この説明責任強化については、IANA機能監督権限移管の一環として検討が行われているものですが、移管後の体勢ではICANNコミュニティがICANNの運用に関わる重要な意思決定に関して権限を持つようになったことが大きなポイントです。この話題に関しては議論の動向も含めてJPNICブログで詳しくご紹介していますので、そちらをぜひご覧ください。

コミュニティがより参画できるICANNへ
～ICANNの説明責任強化に向けた検討～
https://blog.nic.ad.jp/blog/ccwg-acct/

◆ 終わりに

ヘルシンキ会議から4ヶ月間の、ICANN理事見習い期間がついに終わりました。ハイデラバード会議でも、各支持組織、諮問委員会との対話を通じて相互理解が深まったとも感じます。これから3年間の任期を、しっかり務めてまいります。

ハイデラバード会議の資料や記録は、こちらのページからご覧いただけます。

ICANN57 | Hyderabad
https://meetings.icann.org/en/hyderabad57

次のICANN会議は、2017年3月11日から16日にかけて、デンマークのコペンハーゲンで開催されます。

（JPNIC インターネット推進部 前村昌紀）

※1 第56回ICANNヘルシンキ会議報告
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2016/vol1417.html

※2 India School on Internet Governance（inSIG）
http://isig.in/

※3【速報】JPNIC奥谷泉が2016年ICANNリーダーシップ賞を受賞
https://blog.nic.ad.jp/blog/2016-icann-leadership-award/

※4 ICANN理事会メンバー
https://www.nic.ad.jp/ja/icann/about/organization.html#3

ICANN理事就任にあたって

前村 昌紀

2016年6月に選任が決まってから約4ヶ月が経ちましたが、ようやく任期開始を迎え、これから3年間ICANNの理事を務めてまいります。

ICANNは、RIRsやIETFに比べて、圧倒的にマルチステークホルダーによる組織です。さまざまな、時に相反する考え方のステークホルダーを抱えるコミュニティに対して示す理事会の判断は、時に極めて難しいこともあり得ます。グローバルな公益とは何かという、ICANN設立以来一貫した問いかけも存在します。これらは、ICANNが安定的な運営とサービス提供を行えるようになっている今日でも、いまだ実験的な取り組みと言えるのではないかと思うほどです。

JPNICからもお伝えしてきた通り、2016年10月1日、インターネットの黎明から一貫して米国が担ってきたIANAに対する監督権限が、グローバルなインターネットコミュニティに移管されました。2014年以来2年半にわたって検討して準備をしてきた、純粋にコミュニティがリードする新たなインターネットの運営体制が、ちょうど始まったところです。その要所を占めるICANNでは、IANA部局を子会社化するとともに、IANA監督権限移管に最低限必要とされた、新たな説明責任機構が施行されたばかりです。このような時代の転換点で、要所の運営に関与することにわくわくするとともに、責任の重大さを感じずには入られません。

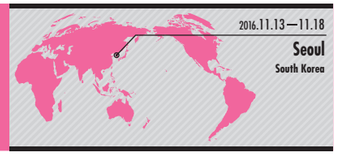
実は、6月に選任が決まった直後に理事会議長であるSteve Crocker氏から連絡があり、6月最終週に開催されたICANNヘルシンキ会議の理事会活動に招待されました。ヘルシンキ会議の場で必要な手続きを整えて、議決権をはじめとする権能は持たないまま、いわば「見習い」として、今まで理事会の活動に参加してきました。ヘルシンキ会議とハイデラバード会議の間には、9月にブリュッセルで開催された理事会合宿会合もありました。これらの会合以外にも、メーリングリストなどでのやり取りも日常的に行っています。

また、理事会の定員は20名ですが、このたび私と同時に理事に就任する5名を加え、メンバーは一時的に25名となっています。この25人は、黎明期からインターネットに関わっている技術者、ICANNのそれぞれの事業分野に精通した専門家、組織経営に長年の経験を持つエグゼクティブなど、それぞれに非常に高い専門性を持つ人々が集まっており、なおかつ、礼儀を踏まえながら、実に闊達な手加減のない議論が繰り広げられます。従って、新参者として学ばなければならないことがたくさんあることのプレッシャーよりも、刺激と充実感の方が勝るという感じがしています。

これからの任期3年間、責任を全うするとともに、ICANNがもっとよくなることに少しでも貢献できるよう、全力で取り組んでまいります。同時に、この務めを通じて知ったことは(守秘義務を負う部分は話せませんが)、できるだけ皆さまと共有していくとともに、皆さまからのご意見もぜひともたくさん伺ってまいりたいと思います。

これからも、皆さまからのご指導ご鞭撻とご高配のほど、よろしくお願いいたします。

第97回IETF報告



2016年11月13日（日）から18日（金）にかけて、韓国の首都ソウルにあるコンラッド・ソウルにて、第97回IETFミーティング（IETF 97）が開催されました。本稿では、このIETF 97の様子を、全体会議の報告を中心にお届けします。その他の動向については、概要と詳細なレポートへのURLをご紹介していますので、そちらも併せてご参照ください。

◆ 参加人数

今回の参加者はここ2年で最少の982人と1,000人を下回りました。リモートを除いた日本からの参加者は53人で、前回のIETF 96（ベルリン開催）とほぼ同じです。2年間で見ると日本の参加者も減少傾向にあるようです。国別の内訳順位は、米国、中国、韓国、日本、ドイツ、フランス、カナダ、イギリス、残りはその他の国で、開催地の韓国よりも中国の参加者が多かったのが印象的です。


● IETF 97の会場となったコンラッド・ソウル

◆ 全体会議からのトピック

IETFミーティングの期間中に必ず行われる、全体会議（plenary）からのトピック（2点）です。全体会議のすべての資料は発表資料「IETF 97 meeting materials」のページで見られます。

IETF 97 meeting materials（全体会議を含むIETF97の発表資料のページ）
https://datatracker.ietf.org/meeting/97/materials/
（このページはミーティング全体の報告が掲載された後はアクセスできなくなります）

○ジョン・ポステル賞（Jonathan B. Postel Service Award）

ジョン・ポステル賞は、技術面やリーダーシップの発揮といったコミュニティに対して継続的な貢献のあった人に贈られるもので、毎年ISOC（Internet Society）によって選出されています。今回の受賞者はタイにある、アジア工科大学副学長のカンチャナ・カンチャナスット氏（Kanchana Kanchanasut氏）でした。カンチャナスット氏は、アジア工科大学をはじめとする、タイ周辺諸国を含めたインターネット接続のほか、インターネット・エデュケーション・リサーチ研究所の立ち上げ、南アジアにおける初の中立的なIXである、バンコク・ニュートラルIX（BKNIX）の立ち上げなどへの貢献が認められました。

Kanchana Kanchanasut Honored with Jonathan B. Postel Service Award
https://www.internetsociety.org/news/kanchana-kanchanasut-honored-jonathan-b-postel-service-award

○技術全体会議（Technical plenary）
～インターネット・アーキテクチャへのアタック～

技術全体会議は、参加者全員が集まることのできる大ホールで、IAB（Internet Architecture Board）などによって企画された、技術トピックについて議論を行う全体会議です。今回のテーマはDDoS攻撃です。DDoS攻撃は、設定やソフトウェアの不備が改善されにくいIoTノードが悪用されるようになり、スケーラビリティ（規模拡張性）を持つようになりました。このようなDDoS攻撃が成立しやすい状況はなぜできたのか、誰がどのような対抗策をとれば良いのか、IETFとしてはどうすればいいのか、といった観点で議論が行われました。これらの観点の説明は、あらかじめIETF Blogに掲載され、共有されていました。

Attacks Against the Architecture, IETF Blog
https://www.ietf.org/blog/2016/10/

技術全体会議では、はじめに、数多くのDDoS攻撃に対処してきたCloudFlare社の技術者であるNick Sullivan氏から、DDoS攻撃の仕組みや実態、技術的対策についての解説が行われました。DDoS攻撃は、1Mbpsのトラフィックを500Gbpsほどに増幅させることのできる"増幅攻撃"の一種で、権威DNSサーバに対する攻撃やICMPのSYNパケットが届く攻撃、HTTPやHTTPSのアクセスが数多く届く攻撃が多く観測されています。

対策としては、上流プロバイダでDDoS攻撃のパケットを廃棄するようなBGP経路制御を行ったり、ECMP（Equal Cost Multi Path）を使って分散させたり、BPF（Berkeley Packet Filter）を使った帯域制限を行ったりすることが挙げられています。発表の最後には、対策のコストを下げる考え方が簡潔に述べられていました。

How to stay online: Harsh realities of operating in a hostile network（Nick Sullivan）
https://www.ietf.org/proceedings/97/slides/slides-97-ietf-sessb-how-to-stay-online-harsh-realities-of-operating-in-a-hostile-network-nick-sullivan-01.pdf

次に、2016年10月下旬にDDoS攻撃を受けて話題になったDyn社のAndrew Sullivan氏による、まとめと議論の呼び水となる発表です。Dyn社は、国際的なBGP経路制御の異常やDNSのトラフィックを監視・分析して、BLOGなどで情報発信していることで知られる会社です。ホスティングサービスも行っています。このDDoS攻撃にはオープンソースのMiraiが使われた上に、Twitterなどの有名なサイトがアクセスできなくなったことが話題となりました。

The Internet's Architecture is Under Attack（Ironically）（Andrew Sullivan）
https://www.ietf.org/proceedings/97/slides/slides-97-ietf-sessb-the-internets-architecture-is-under-attack-ironically-andrew-sullivan-00.pdf

このプレゼンテーションでは、次のような論点が挙げられていました。

- IoTの考え方でIPのノードが数多く繋がってくると、結果的にDDoS攻撃のために使われるノードが増えて、被害が大きくなってしまうという点
- IPで接続されたカメラ等のデバイスは、脆弱性が発見されても改修されにくく、脆弱性を持ったまま運用されてしまうという点
- インターネット・アーキテクチャにおいて「賢いエッジと何もしないネットワーク」という原則的な考え方があり、そのお陰でノードの機能を拡張することの容易さが担保されてきた点（DDoS攻撃への対策のためにネットワーク機器に機能を加えるという考え方は、この考え方に反してしまう）
- BGP38のような対策はあっても、普及しないと効果が現れにくく、仮にインターネット接続の免許制度があったとしても全世界に普及するとは考えにくく、攻撃する側が有利であり続けるという点
- 自動車社会の始まりのときと同じように、多くの人によって運用される仕組みに存在する危険性は、なくすことができないという点

会場では良いテーマ設定への賛辞に続いて、さまざまな意見が出されました。IoTのデバイスに対してPCIDSS（Payment Card Industry Data Security Standard）のような基準への準拠を法制化するというアイディア、その意見に対して、国によって法制度の効果が違うという指摘、IoTデバイスのアップデート方法に関する技術的なアイディア、アクセスネットワークとデータセンターの要件を分けて考えるべきという意見などです。しかし、具体的にプロトコル策定の場においてどうすべきか、という結論までには至りませんでした。DDoS攻撃が容易にできてしまうという問題の性質について、共通理解が得られたという様子でした。


● 全体会議の様子

◆ 新たに設立されたWG

前回のIETF 96以降に新たに設立されたり、活動が始まったりしたBoFを紹介します。

○QUIC WG
https://datatracker.ietf.org/wg/quic/charter/
Google社で開発され、WebブラウザのChromeなどで実装されている、Webのプロトコル QUICをドキュメント化して標準化するWGが設立されました。設立後初めての会合が開かれ、400名近くの参加者が集まりました。詳しくはコーナーの最後で紹介している「セキュリティエリア関連報告」をご覧ください。

○L2SM（L2VPN Service Model）WG
https://datatracker.ietf.org/wg/l2sm/charter/
プロトコル階層モデルの第2層におけるVPN（Virtual Private Network）のYANG（Yet Another Next Generation）モデルを策定することを目的としたWGです。

○SECEVENT（Security Events）WG
https://datatracker.ietf.org/group/secevent/charter/
WebのAPIにおける、イベント・メッセージを安全に伝えるためのプロトコル策定を行うWGです。

○IPWAVE（IP Wireless Access in Vehicular Environments）WG
https://datatracker.ietf.org/group/ipwave/charter/
車などの乗り物における通信方式を扱うWGです。車同士の通信方式と、インターネットに繋がる乗り物のユースケースを扱います。趣意書では、IEEE802.11-OCBの上でIPv6を使う方式の策定を最初に行うとしています。

○LPWAN（IPv6 over Low Power Wide-Area Networks）WG
https://datatracker.ietf.org/group/lpwan/charter/
IoT向け機器のIPv6を使った通信方式を扱うWGです。策定されるプロトコルは、低消費電力の広域ネットワーク用無線技術であるSIGFOX、LoRa、WI-SUN、NB-IOTと組み合わせて使われることが想定されています。

前回に引き続き、IETF 97でも「Bad Attitude Pecha Kucha」が開催されました。これは非公式の会合で、参加者が持ち寄った画像のみのスライドを使って、ジョークのライトニングトークが行われます。前回好評であったためか、多数の参加者が集まりました。今回の内容は、初めてエリア・ディレクターになった方の体験談や、略語の多いIETFを皮肉って架空の下ネタWGの趣意を説明するといったものでした。ビデオが下記で公開されています。

Bad Attitude Pecha Kucha Slides & Videos
http://snaggletooth.akam.ai/

次回のIETF 98は、2017年3月26日（日）から31日（金）まで、米国のシカゴで開催されます。

（JPNIC 技術部／インターネット推進部 木村泰司）


● Bits-n-Bitesの様子

IPv6関連WG報告

v6ops（IPv6 operation）WGはIPv6を展開するにあたっての課題、sunset4（Sunsetting IPv4）WGは、IPv4に依存しないアプリケーションやホスト、ネットワークの実現を目指したWGです。IETF 97におけるこれらのIPv6関連WGでの主な議論の動向について、株式会社ブロードバンドタワーの國武功一氏にレポートをご執筆いただきました。

詳しい内容については、次のURLをご覧ください。

第97回IETF報告「IPv6関連WG報告
～v6ops、sunset4 WGに関して～」
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2016/vol1456.html

トランスポートエリア関連報告

IETFにおけるトランスポート層の活動については、一部の機能が現在のインターネットでの利用に最適なものではなくなってきたことから、再び活発に議論が行われるようになってきました。その中でも、Google社が提唱する「QUIC」は、近年大きな注目を集めています。このトランスポートエリアでの議論の動向について、GE Global Researchの西田佳史氏にレポートをご執筆いただきました。

詳しい内容については、
次のURLをご覧ください。

https://www.nic.ad.jp/ja/mailmagazine/backnumber/2016/vol1457.html

セキュリティエリア関連報告

今回のIETF 97における大きな話題は、2013年から検討が続けられてきていたTLS1.3の仕様がようやく固まり、会期終了直後には正式にバージョン名も決定したことです。ヤフー株式会社の大津繁樹氏にTLS（Transport Layer Security）WGにおける議論の概要をレポートしていただきました。

詳しい内容については、次のURLをご覧ください。

https://www.nic.ad.jp/ja/mailmagazine/backnumber/2016/vol1460.html

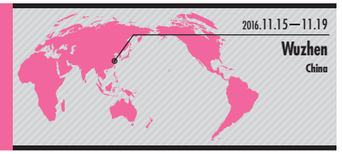
DNS関連WG報告

DNS関連では、プロトコルや運用方法に関する議論のほか、DNSサービスのスケーラブルな拡張機能や、名前解決におけるプライバシー問題などが議論されています。これらのDNS関連WGの動向について、東京大学の関谷勇司氏とJPNICの小山祐司にてレポートをまとめています。

詳しい内容については、次のURLをご覧ください。

https://www.nic.ad.jp/ja/mailmagazine/backnumber/2016/vol1465.html

第3回烏鎮サミットレポート



2016年11月15日（火）～19日（土）にかけて、中国・烏鎮でWorld Internet Conference Wuzhen Summit（以下烏鎮サミット）が開催されました。ICANN理事の初ミッションとしてこの烏鎮サミットに参加してきましたので、本稿ではこの会合の様子をお伝えします。今回で第3回となる烏鎮サミットですが、私は初めての参加です。世界各国から1,600人を超える参加者があったようです。会場となったWuzhen International Internet Exhibition and Convention Center（WIIECC）は、今年初お披露目となる新たに建設された会場です。最新鋭の設備が整った堂々たるもので、会場名に「インターネット」を冠するものは世界に類がなく、中国の烏鎮サミットに対する意気込みが感じられました。

◆ 中国ICT業界の勢いを感じる展示と関連セッション

烏鎮サミットは「中国政府のインターネット政策に関するプロパガンダの場」として認識されることが多いのですが、今回現地で参加してみたら、別の観点での盛り上がりも感じ、印象が変わりました。その一因は、非常に盛況な展示会場です。WIIECCには大小取り混ぜて八つの展示ホールがあるのですが、このすべてに展示が設置され、Alibaba社やTencent社などのネットサービス事業者、キャリア、あるいは自動運転機能などを盛り込もうとする自動車メーカーなど大手の大きな


● 烏鎮は水郷として栄えてきた町で、サミット会場は景観地区内にあります

ブースだけでなく、スタートアップ企業が数多くひしめくように展示をしているスペースもあり、非常に活況で、中国のICT業界の総覧の様相を呈していました。展示以外にも、会議場メインホールでは、インターネットに限らず、AI、スーパーコンピューター、半導体などの最新技術15件に授けられる「最新科学技術業績賞」の受賞セッションが開催されるなど、中国のICT技術の盛り上がりが強く感じられました。

これに呼応して、China-Africa Internet Cooperation Forum というセッションが興味深く感じられました。このセッションはタイトルの通り、中国とアフリカ諸国の協力関係をテーマとしており、つまり、国際支援、開発投資などを扱うものです。中国が近年展開しているアフリカ諸国への開発投資は目を見張るものがあり、アフリカ諸国からの期待も高いものがあるようです。これが、参加者の中で特にアフリカ諸国の方が多く感じられた理由のようにも思われます。

また、中国では近年「一帯一路」というスローガンで、中央アジア、東南、南アジアの開発と経済圏構築を標榜しており、これをタイトルに掲げたセッションも持たれていました。中国ICT業界を総覧できる展示は、海外からでも見に来たいと考える会社は多いのではないかと思います。そして実際に、アフリカ諸国を始めとする世界各国からの関心が集まっています。中国の勢いと意気込みを感じさせるには余りあるものでした。

◆ 変わらぬ中国のインターネット政策の論調

2015年の第2回烏鎮サミットには、習近平主席も参加したことが話題になりましたが、今回はビデオメッセージに留まりました。論調は変わらず、「サイバー主権の重要性」「途上国にも公平となるためのインターネットガバナンス修正の必要性」と言った言葉が踊っていました。これは、オープニングセレモニーにおける政府高官、はたまた個別セッションにおける担当官のスピーチにおいても論調は一緒でした。

今回、書面におけるステートメントとしては、ハイレベル諮問委員会（High-level Advisory Committee, HAC）が採択したとする「烏鎮レポート」が、会期後に発表されました。第2回の際に組織委員会から発表された「烏鎮イニシアティブ」よりも表現は穏やかになっている感があります。会合中に発せられる言葉はこれよりは強く響いた印象がありますが、中国政府の一貫した主張は、垣間見ることができます。また、こういった中国の主張に、列席した発展途上国の高官から同調する発言が聞かれることもありました。中国の主張はこれらの国々に受け入れられやすいものと言えます。

◆ 登壇セッション

今回ICANN理事としてのミッションで、もう一人の理事 Asha Hemrajani氏とともに烏鎮サミットに出席しました。我々は Forum on Global Governance in Cyberspace というセッションにおいて、私はCNNICのCEO、Xiaodong Lee氏とともに、この中のパネルディスカッションの一つの共同モデレーターを務め、Hemrajani氏はスピーチを行いました。

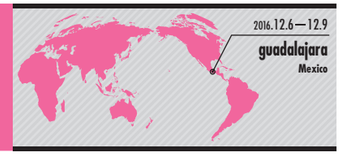
私が担当したパネルディスカッションでは、中国内外の6人の専門家をパネリストに招き、インターネットのインフラや技術革新について議論しました。それぞれの立場からの見解が披露された後、議論はセキュリティ脅威への対処などに焦点があたりました。AIやスーパーコンピューティングなど華やかな先端技術を支えるために、セキュアで安定したインターネットインフラを整備することの重要性が強調される結果となりました。

このセッションでは中国のCyberspace Administration of China（CAC）の担当官による発表もあり、中国の論調に沿ったものでした。この担当官とは席が隣合わせとなり、少し情報交換を行いました。このような話し合いを通じてお互いの考えを擦り合わせることが必要で、それこそがこのミッションの目的だと認識しているところです。

（JPNIC インターネット推進部 前村昌紀）

● パネルディスカッションの様子（右端が筆者）

IGFグアダラハラ会合（IGF 2016）報告



2016年12月6日（火）～9日（金）（Day 0:12月5日（月））にかけて、メキシコ・グアダラハラで「Internet Governance Forumミーティング（IGF 2016）」が開催されました。IGFはインターネットガバナンスに関する課題について、さまざまな関係者で幅広く議論するための国連主催の会合です。200を超えるセッションのうち、半数以上のプログラムは公募に基づき「Multistakeholder Advisory Group（MAG）」と呼ばれるプログラム委員（さまざまな地域や立場より構成された約50名のメンバー）が選定します。私自身も本年までTechnical CommunityからのMAGメンバーを務め、プログラム選定にも関わってきました。本稿では、このIGF 2016についてご報告します。

◆ IGF 2016の特徴と主な議論のテーマ

今回のメキシコでの会議は、IGF開催期限の延長が2025年までと国連総会にて承認されてから初めての開催でした。そのため最終日には、今後10年のIGFの改善について、国連事務局やMAGのチェアが参加者からヒアリングを行うセッションも開催されました。政府に限らず、誰もが参加できる場としてのIGFの改善は、開発のための科学技術委員会（CSTD）等、国連のその他の場でも議論されてきたテーマです。本セッションは、IGFの運営に責任を持つ国連経済社会局（UNDESA）の担当者に、IGF参加者が直接インプットを行える機会でした。


● IGF グアダラハラ会合の様子

またIGFとしては、今後10年の改善に対するインプットを待たず、既に並行してできる改善は一部進めています。年に1度の会議での議論で終わるのではなく、課題に対する検討を継続的に進め、具体的な成果を示すべく、過去3年は"Intersessional Work"として括られる各種活動を実施しています（以下、「成果文書・継続活動」参照。初心者向けプログラムや屋外スペースを利用して気軽に議論できる場を設ける等の試みも行いました）。

なお、National Regional IGFとの連携強化、日本のIGFへの関わりはJPNICブログでもご紹介していますので、詳しくはそちらをご覧ください。

・JPNICブログ：IGF 2016開催中です
https://blog.nic.ad.jp/blog/igf2016/

◆ 主な議論のテーマ

今回のIGFは「インターネットを基盤とした継続的な発展」が会議のメインテーマでした。これは、インターネットを基盤として国連の2030年ミレニアム開発目標をどう支援できるのかを念頭に置いたものです。

また、IGF 2016ではTPPなど貿易協定のあり方を議論したセッションも開催されました。これはインターネットが基盤となる経済活動への着目が増えてきていること、また、国際的な貿易協定の中でインターネットが関わる場面が増えた動向を反映していると言えそうです。

その他、主に議論されたテーマは、以下の通りです。

- 「（途上国や都市部以外の地域への）アクセス提供」（IXP、IPv6普及促進、コミュニティネットワークの提供）
- 「サイバーセキュリティ」（政府、法執行機関、その他関係者間の連携のあり方、IoTセキュリティ）
- 「人権」（監視とプライバシー、忘れられる権利、インターネット情報へのアクセス）
- 「若者の参加促進」

IGF2016各セッションのアーカイブや、MAG議長による会議の総括は、IGFのWebサイトをご覧ください。

IGF Webサイト
https://www.intgovforum.org/multilingual/

◆ 成果文書・継続活動

ここでご紹介する活動は、会議開催の数ヶ月前からオンラインで議論を重ね、その成果もオンラインで残ったり、または活動が継続されたりすることに重点が置かれています。IGF開催期間延長の国連による承認が必要となる目前の2014年から、これらの取り組みを開始/再活性化を行うことで、特定の課題に対して年に一度の会議で議論して終わるのではなく、交渉ではない形で、特定の課題に対して具体的な対応を示すことをめざしたものです。

◇ Best Practices Forum
毎年、その年に重視される四～五つのテーマが選定され、今年は「Gender and Access」「IPv6」「IXP」「Cyber security」の四つのテーマについて取り組みました。いずれのテーマもIGF会議の半年以上前から誰もが参加できるメーリングリストと電話会議での議論を経て文書化に取り組み、意見募集の上、最終的な文書はIGFのWebサイトで公開され、主な関係者機関やコミュニティへ周知されます。

◇ Policy Options for Connecting and Enabling the Next Billion(s) - Phase II
2015年に続き、次の10億人をインターネットにつなげる上での各種施策について文書化しました。

◇ Dynamic Coalitions
特定のテーマについて継続的に議論・活動を行うグループで、参加は誰にでも開かれており、現在は16のテーマに対して、Dynamic Coalitionグループが設けられています。

◆ 資源管理・技術動向に関する議論

JPNICは番号資源の管理を担うレジストリとして、資源管理や技術動向に関わる議論を軸に参加しましたので、それらに関する議論を簡単にご紹介します。

◇IPv6の導入に向けた経済要因に関する取り組み
2015年より継続しているIPv6に関する最適事例を文書化する取り組みで、2016年は経済的モチベーションに重点を置き、ケーススタディを公募して20を超える事例を集め、文書化しました。

◇ IoTとインターネット
IoTを取り巻く検討課題に対して、別の仕組みで検討するのではなく、既存のインターネットにおける決めごとの枠組みの中で対応していくこと、IoTベンダーはインターネットのエコシステムを認識してその中で対応していくこと、複数の標準化活動間の連携の重要性等が語られました。

◇ DNSの分断化
Yeti DNSの目的とRoot DNSとの関係および影響について、IABチェアのAndrew Sullivan氏、L-rootの運用者であるRIPE NCCのCIO Kaveh Ranjbar氏、Yetiに関わっているPaul Vixie氏が議論を行いました。

Yeti DNSは、IANAの管理するすべてのTLDデータをYeti DNSシステムに反映し、実際のルートDNSへの影響に関する各種実験を実施しています。しかしこの実験は、技術的にAlternative Rootとなり得る可能性があるため、その影響についてさまざまな意見があることから、登壇者それぞれの立場から議論が行われました。

Yeti DNS:
https://www.yeti-dns.org/

Paul Vixie氏によるYetiの目的を説明した執筆記事:
http://www.circleid.com/posts/20160330_let_me_make_yeti_dns_perfectly_clear/

◇ IXPおよびCDNを利用したコンテンツデリバリーのあり方
Cloudflare社、Ams-IX、ISOC、CGI.br等のパネリストが、途上国における中小ISPによるコンテンツソースとして、IXPに接続してCDN cacheとそのコストを共有する利点と課題を議論しました。

◇ その他資源管理・技術動向に関する議論
CGNの利用に伴う法執行機関とIPアドレス利用者の特定における課題、国際化ドメイン名や国際化電子メールアドレスについて議論するセッションも開催されました。

◆ 次回のIGF

来年のIGF 2017はスイスがホスト国となり、2017年12月18日（月）～21日（木）にジュネーブで開催されることが、Closing Ceremonyで発表されました。

（JPNIC インターネット推進部 奥谷泉）


● IGF グアダラハラ会合の様子

インターネット A Scene of Internet History
歴史の一幕

JPNIC理事
佐野 晋

Internet Week開催から20年。Internet Weekのはじまり

"Internet Week（以下、IW）"は文字通り、「この1週間はインターネットの基盤技術や最新動向を学ぼう」を主旨とし、1997年からもう20年続いているイベント である。近年は11月末から12月にかけて開催されているが、そこでインターネットに関する技術の研究・開発、構築・運用・サービスに関わる人々を集め、議論し、学んで、理解と交流を深められる場にしたいと毎年ながらに試行錯誤をしている。

「'97年にIWがはじまった」と述べたが、前身とも原型とも言える会合は、1990年から続いていた"IP Meeting"だ。当時、学術系を中心に、IPを使ったインターネットが整備されはじめていたが、携わる人は全国でもまだ数少なく、こうした数少ない日本のインターネット関係者が相互接続に向け情報交換できる唯一のオンサイトの場が、JEPG/IP（Japanese Engineering & Planning Group /IP）が主催となり開催していた、"IP Meeting"であった。IP Meetingのはじまりについては、次の記事に詳しい。

インターネット 歴史の一幕:第1回　日本インターネットミーティング（IP Meeting'90）
https://www.nic.ad.jp/ja/newsletter/No43/0320.html

1990年には40名ほどだったIP Meetingの参加者は、毎年、倍々のペースで増え、4年後の94年には600人を数えるようになる。こうしたペースで人数が急増すると、情報交換という役割を越え、技術そのものを教えたりキャッチアップしたりする普及啓発の側面も求められるようになった。IP Meetingはそうした需要に対し、チュートリアルやワークショップも開くなどで対応した。インターネット利用の質的・量的な拡大とともに、会議は大幅に拡大していった。それまでも財政的な面などで支援をしていたJPNICに運営体制に関する相談が持ちかけられたのは、1997年1月（IP Meeting '96を開催した翌月）である。当時のJPNICの運営委員会資料でそれが確認できる。JEPG/IPとしては、「IWを作ることに意義を感じており、JPNIC、日本インターネット協会（IAJ）、Internet Conference、World Wide Web Consortium（W3C）などのいくつかのグループを巻き込んで開催したい」ことと併せ、このままJEPG/IPが主催となるのか、それともJPNICが主催となるのか、または関連団体で実行委員会を作って運営していくのかなどの開催形態の選択肢も議論された。

その後関係者で何度かの「企画会議」なる場が持たれ、JPNICからはIW'97をJEPG/IPとJPNICとの共催にしたい、そして4日間で開催してはどうか、またJPNICが企画できるチュートリアルについてやJPNIC会員には参加割引を適用して欲しいというような提案を行った。1997年4月1日に開かれた企画会議で、IW'97はパシフィコ横浜で開催し、日程としては1997年12月16～19日ということに決まった。

こうして1997年12月16日～12月19日にパシフィコ横浜で最初のIWが開催された。最終的には、IP Meetingを主催してきたJEPG/IPに加えてJPNICが共同主催者となり、WIDEプロジェクト（WIDE）、日本ソフトウェア科学会、日本UNIXユーザ会（jus）、IAJ、JAVAカンファレンス、コンピュータ緊急対応センター（JPCERT）、電子ネットワーク協議会などの参加を得て、従来のIP Meeting（全体会議、チュートリアル、ワークショップ）に加え、各団体がインターネットに関連したカンファレンスやワークショップを持ち寄って実施する形となった。具体的には、

- JEPG/IPが従来のチュートリアル、全体会議、ワークショップ
- JPNICがチュートリアルとワークショップ
- IAJがJapan WWW Conference
- Javaカンファレンスがその 名の通りのJava Conference
- JPCERTがワークショップ
- 日本ソフトウェア科学会インターネットテクノロジ研究会・WIDE・jusが共同開催でのInternet Conference
- 電子ネットワーク協議会主催によるENC Conference '97

が、IW'97の中で開催された（そしてこの中の目玉は、なんと言ってもInternet Conferenceに坂本龍一氏が出演したことであった。） またJPNICは、その場に来られなかった人への普及啓発に役立つように、チュートリアルの「レクチャーノート」を作成し,Web上に公開した。

こうして、Internet Weekとしては初めてのIW'97は大成功に終わった。当時の資料を見ると 、来場者数はそれまでの約7倍の4,129人であり、また「ほぼスケジュール通りに各種の会議を運営進行することができた」とある。しかし、うまくいったからこその課題も残った。'97の後、参加者だけでなく「IWに参加したい」という団体が増え、再びIWの規模拡大の課題が持ち上がった。

そのため、1992年に神戸で開催されたISOC主催の国際会議 INET'92 からこの業界を支えていた（株）ジェイコム（現：（株）JTBコミュニケーションデザイン）にプロとして運営をお願いし、また5月の段階から、97年を上回る数の参加団体からの協力を得て、主催としての実行委員会を結成し、全体企画を行った。多くの会議が同一会場と時期に開催されることの効果を、より一層発揮できるようなプログラム構築の調整には大変な労力がかかり、そのため、IW'98実行委員会は12回、JPNICでの教育ワーキンググループも6回も開催されたと記録に残っている（なお、この数にはその他の打ち合わせは数に入っていない）。

そして1998年12月15日から1998年12月18日にIW'98が国立京都国際会館で開催された。当時はまだインターネットの一般利用が当たり前とは言えない時代だったが、IW'98への問い合わせの基本はメールとし、あえてWebページに電話番号を載せなかった。参加登録は自前のシステムを作ったが、どのプログラムも金額が異なり、クレジットカード決済に対応していない時代だったので、入金確認や受講票発行などの問い合わせに対応するジェイコムの部署は連日徹夜であった。また、今のようなWi-Fiも夢の時代であったため、アクセスコーナーにケーブルを配線するのに防火扉に引っかかるなど、今では笑い話となるような局面もあった。

こうして開催されたIW'98の参加者数は延べで約5,000人。JPNICはジェイコムと協力し、IW'98実行委員会の事務局として開催準備から運営までの業務を行った。ここから、IW'99（横浜）と'00（大阪）が7,500人、'01（横浜）と'02（横浜）が9,000人と、参加人数はうなぎ登りに増えていく。

しかし、こうした生みの苦しみを経ることで、今に20年も続くIWの原型ができたことになる。

（団体の名称は当時の名称を使用しています）

10'00"00 インターネット10分講座

MIN SEC 1/100S INTERNET

CSIRT (Computer Security Incident Response Team)

今回のインターネット10分講座では、サイバー攻撃など昨今のセキュリティインシデントの増加にともない企業や大学などに設置が進んでいる「CSIRT(シーサート)」について、その背景から設置にあたっての注意、活用のためのノウハウなどを取り上げます。

◆ 1.Computer Security Incident Response Team(CSIRT)設置の背景

国内で継続的に発生しているサイバー攻撃を背景に、昨今Computer Security Incident Response Team (CSIRT、シーサート)を設置する動きが活発化しています。その要因として二つのインシデントがあります。一つ目は2011年に防衛産業組織で発生した標的型サイバー攻撃です。

当該インシデント発生以降、シーサート設置に関する議論は活発化し、当時の政府の情報セキュリティ対策を検討・推進等を行う会議である「情報セキュリティ対策推進会議」において、『情報セキュリティ対策に関する官民連携の在り方について』が公開されました。「漠然と組織間で情報共有を行うのではなく、各組織が情報セキュリティインシデントに関する緊急時対応の機能を有した専門的な部隊「CSIRT」を組織し、官民を含む各組織内CSIRT等の間で、専門的、実務的な連携を図ることが必要」※1とシーサートに言及しています。

さらには2013年には『金融機関等コンピュータ・システムの安全対策基準・解説書(第8版追補)』や2014年には『政府機関の情報セキュリティ対策のための統一基準群』においてもシーサートに言及しています。

そして二つ目のインシデントは2015年に公共機関で発生した標的型サイバー攻撃です。

2015年に発生したインシデント以降は、シーサート設置の議論がさらに活発化するとともに、より一層シーサートの拡充に関する議論が深まっています。また政府機関や民間企業に限らず、地方自治体や学術機関等においてもシーサート設置の議論が活発化するなど、拡大と深化が進んでいます。特に2015年に公開された『サイバーセキュリティ経営ガイドライン』においては「サイバー攻撃を受けた場合、迅速な初動対応により被害拡大を防ぐため、CSIRT(サイバー攻撃による情報漏えいや障害など、コンピュータセキュリティにかかるインシデントに対処するための組織)の整備」や「CSIRT間における情報共有や、日本コンピュータセキュリティインシデント対応チーム協議会(略称:日本シーサート協議会)等のコミュニティ活動への参加による情報収集等を通じて、自社のサイバーセキュリティ対策に活かす」※2など、シーサート間連携や日本シーサート協議会のコミュニティ活用についても言及しています。日本シーサート協議会は2017年1月現在で203の組織が加盟する大きな組織となりました。特に2013年以降のシーサート設置が多く、2016年の1年間で加盟組織数が約2倍近く増加するなど、国内におけるシーサート設置が加速していることが伺えます**(左ページ図1)**。

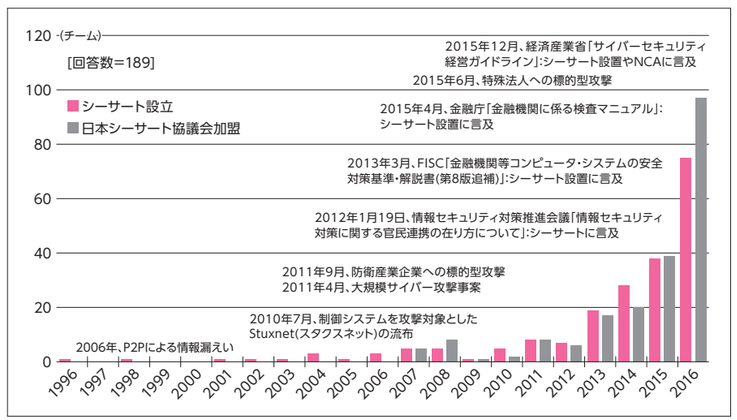


図1:日本シーサート協議会への新規加盟数と加盟チームの設立年の推移

◆ 2.シーサートとは何なのか

シーサートとは「コンピュータセキュリティにかかるインシデントに対処するための組織の総称(機能)であり、インシデント関連情報、脆弱性情報、攻撃予兆情報等を収集、分析し、対応方針や手順の策定などの活動」を行うチームのことです。シーサートは組織の成り立ちや歴史、セキュリティに対する意識、資源等によってシーサートの設置および活動内容が異なるため、百社百様のシーサートがあります。しかしながら、シーサートとして共通して持つべき定義と機能があります。次からその定義と機能について述べていきます。

2.1. シーサートの定義付け

シーサート設置において定義すべき項目は次の四つです。一つ目は「Mission(ミッション(使命))」、二つ目は「Service(サービス(役務内容))」、三つ目は「Constituency(コンスティチュエンシー(活動範囲))」、そして四つ目は「Incident(インシデント)」です。

2.1.1. Mission(ミッション(使命))

既に述べたように外的要因が強まり、経営層が「シーサートを設置せよ」と号令を出す組織もあるようですが、どのような背景であったとしても組織にとって「なぜシーサートが必要なのか」「シーサートでは何を行うのか」といった活動の軸となるミッションを定める必要があります。ミッションを定めておくとシーサート活動に迷いや停滞が生じた時に立ち返ることができ、シーサート活動の大きな助けとなります。

またミッションを検討するに当たっては一個人や一組織だけではなく、関連するさまざまな組織で話し合いをし、シーサート活動を行う予定のメンバーはもちろんのこと、組織全体で共通認識を持っておくように準備、検討をしておきましょう。

2.1.2. Service(サービス(活動内容・役務))

シーサートが提供するサービスはさまざまです。そのためシーサートのミッションに照らし合わせて「シーサートの業務・役務・活動として何をやるべきなのか」を既存(またはシーサート設置に当たって拡張、利用可能な)資源と照らし合わせながら検討する必要があります。

この活動内容の検討で大切なことは「今できることに留めること」です。これはシーサート設置時に、活動内容の対象を広げてしまうと、資源の拡大が今後難しくなることや、活動を行う人員やチームの疲労が進む可能性があるからです。経営層からはより幅広い活動を期待されるかもしれませんが、限られた資源の中で何ができるのかを検討し、できる活動内容から始めるようにしましょう。

日本シーサート協議会が公開している『CSIRTスタータキット』においては、サービスを大きく三つに分類しています**(図2)**。

インシデント 事後対応サービス	・インシデントハンドリング ・コーディネーション ・オンサイトインシデントハンドリング ・インシデントハンドリングサポート ・コンピュータ・フォレンジックス ・アーティファクトハンドリング
インシデント 事前対応サービス	・セキュリティ関連情報提供 ・脆弱性情報ハンドリング ・インシデント/セキュリティイベント検知 ・技術動向調査 ・セキュリティ監査/査定 ・セキュリティツールの開発
セキュリティ品質向上 サービス	・リスク評価・分析 ・事業継続性、災害復旧計画作成・改変 ・セキュリティコンサルティング ・セキュリティ教育/トレーニング/啓発活動 ・製品評価・認定

図2:シーサートのサービス概要※3

一つ目はインシデント発生時の支援内容である「インシデント事後対応サービス」です。例えばインシデント発生時にオンサイト(直接訪問しての)支援を行うのか、また不正プログラムの解析や端末のフォレンジックを行うのかなど、インシデント発生後に活躍するサービスです。

二つ目はインシデントを発生させないことや被害の最小化等を目的とした「インシデント事前対応サービス」です。当然ですがインシデントは発生しないに越したことはありません。そこで普段からインシデントや脆弱性に関する情報収集や、組織内のシステムの異常を早期発見できる仕組み、また早期対処可能な運用体制の構築等を行っておく必要があります。

※1 情報セキュリティ対策推進会議「情報セキュリティ対策に関する官民連携の在り方について」(平成24年1月19日)
http://www.nisc.go.jp/conference/suishin/ciso/dai4/pdf/1-1.pdf

※2 経済産業省「サイバーセキュリティ経営ガイドライン」(平成27年12月28日)
http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf

※3 出展元:日本シーサート協議会「CSIRTスタータキット」

そして三つ目は組織におけるインシデント対応能力を普段から向上させることを目的とした「セキュリティ品質向上サービス」です。ここでは組織のリスク把握や教育・トレーニングの提供等を行い、普段から組織のセキュリティ知識や対応力の向上を図っておく必要があります。

なお、三つのカテゴリに記載されているすべてのサービスを自組織で提供できる組織は、ほぼ存在しません。大切なことは自組織で提供できないサービスを知り、提供できないサービスがあれば代替案をどのようにするのかを検討、準備しておくことです。組織によって提供可能なサービスは異なりますが、自組織の身の丈に合ったサービスを検討し、定義付けていきましょう。

2.1.3. Constituency（コンスティチュエンシー（活動範囲））

組織には数多くのシステムや部門が存在します。組織が有するシステムは自組織で構築・運用しているシステムもあれば、外部に運用を委託しているシステム、または外部サービスを利用している場合もあります。組織が把握、管理しなければならない情報システムは数多く存在し、また組織内外に関係者および関係組織がまたがるため、情報システムのマネジメントは大きな課題です。

シーサート設置時からすべてのシステムに対して、定義したサービスを提供できるのであれば検討する必要はありませんが、資源には必ず限りがあり、サービスの提供範囲を限定しなければなりません。例えば、グローバルに展開している組織であれば、まずは国内のシステムを活動範囲にし、国内で得た経験を活かしてグローバルに展開をしていくように活動範囲を設定する、またはお客様に提供しているサービスで、企業の利益に直結するシステムを対象とし、他のシステムにおいては初期の活動段階では対象とせず、シーサートの活動範囲を追って拡大していくなど、組織によってシーサートの活動範囲の検討を行い、定義付けを行っておくことが必要です。

この活動範囲の定義付けを適切に行わないと、後に自分たちのシーサート活動を苦しめることになります。

インシデントが発生した際に、資源が少ないにもかかわらず、組織全体のシステムに対して対応を求められ、責任も負う可能性があります。（無理をしているにもかかわらず）インシデント対応ができた場合でも、また同じようなことが起こった場合に同様の対応を求められ、現場では疲労や不満が募っていくことでしょう。

また責任が伴うため、シーサートが機能していなかったと経営層が判断すれば、シーサートの予算削減や責任者の処分、場合によってはシーサート自体を解散という議論にも発展しかねません。活動範囲を明確にし、責任の所在を明らかにするとともに、経営層と活動範囲の事前の認識合わせを行っておきましょう。

これらの「ミッション（使命）」「サービス（活動内容）」「コンスティチュエンシー（活動範囲）」はシーサート活動の根幹となります。シーサートを設置し、活動を行うとさまざまな課題に衝突しますが、この三つの要素が確立されていれば、立ち返り、シーサートの検討や活動の確認を行うことができます。シーサートの活動を継続的に行うためにも適切に定義し、また定義した組織は現状に合致したものになっているのか、定期的な確認や見直しを行っていきましょう。

2.1.4. Incident（インシデント）

さて「ミッション」「サービス」「コンスティチュエンシー」の議論をより深く、現実的に行うために必要なことが「インシデント」の定義付けです。

組織にとって何がリスクなのか、守るべき情報資産は何なのかを理解していないとインシデントの定義を行うことは難しいでしょう。何から何を守るべきなのか、脅威や守るべき対象を明確にし、組織にとって何が普段と異なる事象なのか。そしてその事象は組織にとってどれだけ重要な事象なのか（何がインシデントなのか）を定義しておくことが必要です。

例えば会社概要を掲載しているWebページが改ざんされてしまう事象と、組織が運営しているECサイトが改ざんされてしまう事象では組織にとって影響度合いが異なります。このように組織におけるインシデントを、リスクや情報資産を理解した上で定義しておくことが大切です。

2.2. 必要な四つの機能

百社百様あると言われるシーサートですが、シーサートとして持つべき機能があります。ここではその代表的な四つの機能について述べていきます。

2.2.1. Point of Contact

シーサートになくてはならないものが「Point of Contact（＝公開された信頼できる窓口）」です。自組織だけで情報収集やインシデント発生後の対処や調査など、シーサートの活動を行うことは難しく、必ず外部連携が必要となります。またせっかく外部組織が脆弱性やインシデント情報を発見したとしても、通報先がわからないと通報できず、また通報できた場合でもたらい回しにされ、インシデントの発見が遅れることになります。シーサートの顔とも言えるPoint of Contactを定め、定めた窓口を必ず公開するようにしましょう。日本シーサート協議会では加盟組織の外部連携窓口を集約し公開しています。これによりJPCERT/CCや法執行機関、他のシーサートからなどの通報を受けやすい環境を整備しています。

なお、インシデントをはじめとするセキュリティ関連の報告（通報）や問い合わせは、WHOIS DBに登録された連絡先に送付することが国際的にも事実上の標準となっています。当該連絡先にインシデントに関する情報が届いた場合、Point of Contactが中心となり、シーサート全体に速やかに伝わるよう準備しておきましょう。

2.2.2. 技術的な対応

シーサートはサイバー空間に関するインシデントに対して活躍する組織です。サイバー空間の脅威や情報システムに関する最低限の技術的な知識が必要となります。外部から脆弱性情報などを受け取った場合、技術的な視点で脅威を推し量り伝達することや、調整活動、対外的な協力推進などが求められます。この対応を行うためには技術的な知識は必要不可欠です。しかし、誤解をしてほしくないことは、「ホワイトハッカー」と言われるような高度なセキュリティ人材が必要というわけではありません。これらの対応は技術的な要素が関係するとはいえ、外部との折衝や調整を行うことが多く、技術力だけでは不足しています。また考え方によっては技術的な知識は学習によって習得していくことが可能です。そのため技術力が高い人材を発掘するのではなく、「コミュニケーション能力」の高い人材を発掘し、シーサート活動を行うメンバーに加えていきましょう。

2.2.3. 部署（部門）横断

情報システムやセキュリティを所管する組織がシーサートの取りまとめとなっている傾向が強いですが、シーサート活動は部署横断的に行う必要があります。例えばインシデントが発生した際に、公式見解や記者向けの発表を仕切る広報部門や法的な解釈を必要とする場合には法務部門が関連します。またセキュリティ戦略を立案する部門やサイバーセキュリティ教育を実施する教育部門など、シーサートにはさまざまな部門が関係しています。サイバーセキュリティ対策の推進を特定の部門だけが頑張れば良いという「お任せモデル」から組織全体で頑張る「連帯モデル」へと変更していきましょう。

2.2.4. 「レスポンス（Response）」ではなく「レディネス（Readiness）」

既存のインシデントレスポンス体制を活用して、シーサートを構築する組織は多く、既存の体制を活用することはシーサート設置においても正しいプロセスです。しかし、インシデントレスポンス（インシデント発生後の対応）の観点を強く持っている組織は多いですが、インシデントレディネス（インシデントを発生させないようにするための事前対応）の観点が不足している組織が多いのも事実です。このレディネスの観点がないと、今までのインシデント対応体制と何が違うのかという議論に発展するケースも見られます。インシデントレスポンス（事後対処）などの実践的な活動経験を元に、インシデントレディネス（事前対処）を進めることの重要性を理解し、被害の未然防止に努めていくようなシーサート活動を行う必要があります（**図3**）。

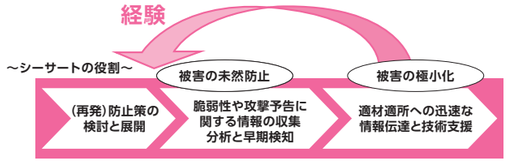


図3：インシデントレディネスとレスポンス概要

◆ 3.日本シーサート協議会加盟状況から見るシーサート

日本シーサート協議会では加盟組織向けに毎年アンケートを実施し、シーサートの現状や活動状況の把握を行っています。ここでは2016年に実施したアンケート内容に基づき述べていきます。

シーサートは技術的な対応を含むため「情報システム管理部門系」が取りまとめを行っている傾向が強く、次いでセキュリティ対策を組織内で専門的に行う「セキュリティ対策部門系」が取りまとめている割合が多くなっています。また割合としては多くはないですが、より部署横断的な観点から「経営企画部門系」や「総務部門系」、さらには組織全体のリスク管理を行う「リスク対策部門系」が取りまとめているシーサートもあります（**図4**）。

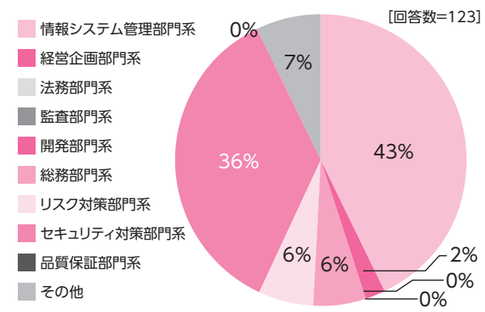


図4：シーサートの取りまとめ部署

情報システム管理部門系やセキュリティ対策部門系がシーサートの取りまとめを行うことは設置がスムーズに進むというメリットがありますが、既存業務の延長線上の要素が強く、より部署横断的にしにくいといったデメリットもあります。

次にシーサートで活動するチーム人数についてです。シーサート設置時においては5名未満が37％、10名未満の割合は合計83％と非常に多く、20名以上でスタートをしているシーサートはわずか2％しかありません。これよりスモー

ルスタートでシーサートを発足している組織が多いことがわかります**(図5)**。

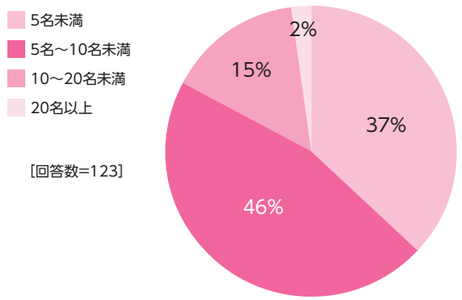


図5：シーサートのチーム人数(設立時)

しかし、活動開始後は割合が大きく変化し、5名未満で活動をしていたシーサートは11%と大きく減少しています。また10名未満の割合も活動前は8割強あった組織も5割弱に減少しています。一方で10名以上の割合は17%から52%まで大きく上昇し、シーサート活動を行うに当たっての拡充が行われていることがわかります。これは活動後にシーサートの必要性を深めることができた組織や、外部連携を行うに当たってさまざまな部門の担当者が連携しなければシーサート活動が難しいことを理解した組織が増加し、より部署横断的にシーサートを支援していることが要因と言えます**(図6)**。

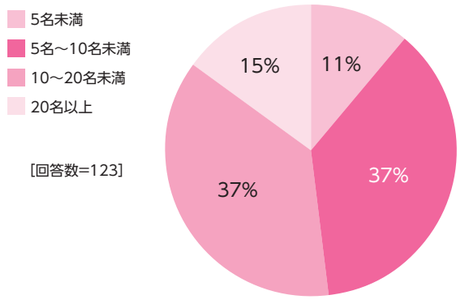


図6：シーサートのチーム人数(活動後)

また実装の形態として独立部署(専任型)でシーサートを実装している組織は12%と少なく、傾向としては金融業界の組織が専任型で行っている傾向が見られます。国内のシーサートのほとんどは兼務型であり、部署横断的にシーサートが設置されています。シーサートの実装形態に確たる答えはないですが、組織内のシーサート活動が最大限発揮できる体制で設置することが望ましいです**(図7)**。

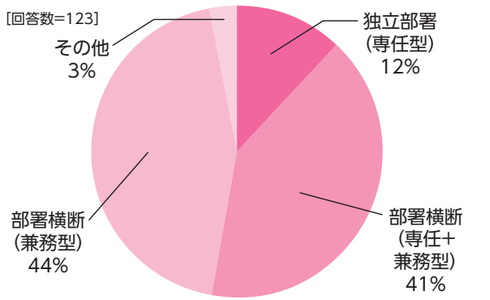


図7：シーサートの実装形態

シーサートの対象としている利用者も変化しています。組織のお客様(顧客)を対象としているシーサートは昨年まで6割前後であったのが4割に減少しています。これは2016年の加盟組織にユーザー組織の加盟が多く進んだことが要因と言えます。またグループ会社全体を利用者としている組織も増加しています。これは加盟組織の増加も一つの要因ですが、運用が進んでいく中でコンスティチュエンシー(活動範囲)の拡大が進んでいることも要因の一つと言えるでしょう**(図8)**。

図8：シーサートのサービス利用者

◆ 4.シーサート設置における勘違い

4.1. 「とりあえずシーサートを作れ」

シーサート設置の背景で述べた通り、政府機関が公開している文書等から経営層も徐々にシーサートを目にまたは耳にする機会が増えてきています。「当社にシーサートがないのであれば早く作れ」といった経営層の言葉がきっかけでシーサート構築が進むことも少なくはありません。しかし、経営層の一言の浅深には大きな差があります。

シーサートは組織の危機管理の一つとなるため、本来は経営層自らがタクトを振り構築を行う方が望ましいですが、往々にして自ら構築に関与することはありません。直接的な構築は行わずとも、最低限組織の危機管理という観点から、指針や方針を示し、シーサートの設置を促すようにしましょう。指針や方針を示されて構築されたシーサートと、すべてを現場に任せて構築されたシーサートでは、組織全体の理解の深さや浸透度が異なります。もし指針や方針を示さず、部下や現場に構築すべてを任せるのであれば、権限および財源の移譲を行った上で構築をすべきです。シーサートは既存の危機管理体制を活用するとはいえ、「とりあえず」で設置できるものではありません。

下図9の通りシーサート構築はプロジェクトの立ち上げから設置に至るまでに数々のプロセスがあります。このプロセスを理解した上で権限と財源を移譲して設置を指示する組織と、理解や移譲を行わずに設置を行おうとしている組織では設置スピードや設置後のシーサートの活動内容に大きな差が生じます。「言うは易し、行うは難し」設置を指示することは素晴らしいことですが、さらに組織に貢献するシーサートにするために、とりあえずではなくシーサートを理解した上で設置を指示し、組織全体で設置を進めていきましょう。

項目①	項目②
プロジェクトの立上げ	目標(構築きっかけの明確化)
	メンバ構成
	スケジューリング
	プロジェクト運営ルール
	経営者/意思決定者の合意
守るべき対象と脅威の把握	社内システムやネットワークの把握
	過去のインシデント情報
	既存のリスク分析結果
既存のインシデントレスポンス体制	既存のインシデントへの事前対応
	既存のインシデントへの事後対応
	既存のセキュリティ向上に向けた取り組み
	既存のインシデントレスポンスに関連する社外組織
	インシデントレスポンスに有効な社外連携体制の確立
既存のセキュリティポリシー およびセキュリティ関連文書	セキュリティポリシー
	災害復旧計画・事業継続性計画
	セキュリティに関連する制約事項や規制
	物理セキュリティに関する制限
基本構想の検討	ミッション、サービスコンスティチュエンシーの定義付け
	インシデントの定義付け
サービスの検討 「インシデント事後対応サービス」	インシデントハンドリング
	コーディネーション
	オンサイトインシデントレスポンス
	インシデントハンドリングサポート
	コンピュータ・フォレンジックス
	アーティファクトリハンドリング
サービスの検討 「インシデント事前対応サービス」	セキュリティ関連情報提供
	脆弱性ハンドリング
	インシデント・セキュリティイベント検知
	技術動向調査
	セキュリティ監査・査定
	セキュリティツールの管理
	セキュリティツールの開発
サービスの検討 セキュリティ品質向上サービス	リスク評価分析
	事業継続性、災害復旧計画作成・改変
	セキュリティコンサルティング
	セキュリティ教育・トレーニング・啓発
	製品評価・認定
社内体制の検討	
社外連携の検討	
リソースの検討	人的リソース
	設備リソース
比較検討	
構築スケジュール検討	
構築	経営層の承認とリソース確保
	社内調整の実施
	サービス対象の説明
	体制整備
	必要文書の作成
シミュレーション	
実施	周知
	サービス対象への提供
	社外連携体制の確立
検証(再検証)	

図9：シーサートの構築プロセス

4.2. 「予算がない」

セキュリティ対策はお金をかければいくらでも実施できることはあり、すべてにおいて最高峰の組織的、人的、物理的、技術的セキュリティ対策を行うことは不可能です。また組織規模や経営層の意識によっても投資できる予算は組織によって異なります。昨今シーサートを構築した組織においてもシーサート活動を行うための予算がない、少ないといった声も聞こえています。

シーサートは情報システム管理部門やセキュリティ対策部門などが中心で、部署横断的ではない(または組織全体にシーサートを理解されていない)シーサートも存在し、シーサート活動が不透明になっている組織が見られます。シーサート活動を牽引する限られた組織は必要ですが、その限られた組織で予算のやりくりを余儀なくされてしまうケースも少なくはありません。

シーサートはもはや「組織になくてはならないもの」と言っても過言ではなく、社会的な責任を果たすという意味においても必要となっています。またシーサートはインシデントに対して適切に対応が行うことができるといった組織のイメージを向上させる効果ももたらし、マーケティング活動の一環とも捉えることが可能です。

つまり情報システム管理部門やセキュリティ対策部門などの限られた部門で予算確保や運営を行うのではなく、CSR活動を行う部門やマーケティング(セールス含む)活動を行う部門においても予算を確保し、シーサートの活動を支援する必要があります。人材だけではなく財源も部署横断的になるように検討していきましょう。

もし部署横断的な予算確保が難しいのであれば、経営層の直接的な予算枠を確保するといったことを検討するのも一つです。経営層が本当にシーサートを理解していれば直接的な予算付けを行うことも不可能ではありません。現場がより経営層の理解を深めていく活動を行うとともに、経営層はシーサートの構築面だけではなく、運用面も踏まえた予算について理解し、双方で合意形成を図っていきましょう。

4.3. 「インシデント対応時にしか活躍しない」

「インシデントが発生した時にはシーサートが活躍する」これも間違った考えではないですが、シーサートで大切なのは先に述べた通りレスポンス(Response)ではなくレディネス(Readiness)です。インシデントを発生させないための活動、または発生しても被害を最小化するための準備が極めて重要です。実空間(社会)のインシデントの例で考えてみましょう。

例えば、私たちは大規模な火災を起こさないためにさまざまな準備を行っています。発生時の問い合わせ先(119番)

を覚えておく。消火器を常備する。検知できるように火災報知機を設置する。原因となる火元の対策をする（例：ガスの元栓を閉めるなど）。そして避難訓練を実施するなどです。これらはいずれも火災に備えるための準備です。

サイバー空間においても同様に普段からの活動、事前の準備が重要になります。119番の記憶はインシデントが発生した時に、どこに通報すれば良いのかを理解しておく、問い合わせ先の事前理解です。消火器の常備は万が一、インシデントが発生しても初期対処を行えるようにする事前準備です。火災報知機は早期検知体制の確保、ガスの元栓を閉めるなどは普段からの運用、避難訓練はインシデントが発生しても冷静かつ的確に対処、回避するための準備です。いずれも準備が大切なことが理解できます。

重複しますが、サイバー空間も同様にレスポンス（Response）ではなくレディネス（Readiness）の視点に重きを置き、インシデントを発生させないようにするための事前対処をシーサート活動で実施することが重要です。

4.4. 「日本シーサート協議会に加盟したから一人前のシーサート」

日本シーサート協議会は各組織で構築したシーサートを一人前のシーサートと認めるための団体ではありません。むしろ加盟はスタートラインに立ったに過ぎず、いかに加盟組織との情報連携などを行っていくのかを検討し、実行していくことが大切になります。

現在、日本シーサート協議会には18のワーキンググループが存在し、各ワーキンググループで活発な議論や成果物の発表が行われています。例えば各組織で発生したインシデントを共有し合い、自組織への活用や対応のアドバイスなどを行うワーキンググループや、収集した海外の情報を共有し合い、組織内への報告方法・テンプレートを検討するワーキンググループなど活動はさまざまです。また昨今では同業種・業態のシーサート間においてインシデント情報の共有をはじめとした連携強化が行われるなど、日本シーサート協議会という「場」を活用した活動が見られます。一方で、シーサートを一人前と判断するための評価手法が必要であることも認識しており、既に日本シーサート協議会ではその検討も開始しています。

日本シーサート協議会への加盟はシーサート活動の一つに過ぎず、ゴールではなくスタートであることを、未加入の組織も加入済みの組織も理解しておきましょう。

4.5. 「コンスティチュエンシー（活動範囲）が拡がらない」

シーサートは最初から組織全体の活動範囲とすることは難しく、まずは対応可能な範囲からシーサートを設置しようと述べました。述べた内容に相違はないですが、シーサートを構築するのであれば、設置したシーサートを今後どのように発展させていくのか、すなわち組織全体の活動範囲となるためにはどうすれば良いのか、スモールスタートといえども中長期の計画も検討しておくべきです。

例えば情報系と言われる業務関連のシステムと、重要インフラ事業者に見られる制御系と言われるシステムでは歴史、概念、運用方法等が大きく異なります。そのため情報セキュリティ最高責任者（CISO）が情報系、制御系いずれにも存在するケースなどもあります。情報系を優先してシーサートを構築すると後に制御系を含めた組織全体としてのシーサートを構築するのが難しいような組織も見られます。このような場合にも経営層（者）の意識が重要で、直接的な指示を出す必要があります。インシデントが発生した場合、より深く頭を下げなくて済むよう、経営層（者）も直接的にシーサート構築や活動範囲の拡大に向けた動きの指示・支援などを行いましょう。

◆ 5.これからのシーサートを考える

これだけシーサートという言葉が新聞や雑誌、政府機関が公開している文書などに記述されている昨今において、シーサートの設置が進んでいることは日本シーサート協議会の加盟数から見ても明らかです。まだまだシーサートは増えていく必要があり、日本シーサート協議会としても加盟組織数の目標を約3,000と定めています。しかし、数の追及も必要ですが、今後必要なのはシーサートの「質」の追及です。現在、シーサートは百社百様あると言われていますが、定義が必要な四つの要素や四つの機能が適切に構築され機能しているのか、また事前対処（Readiness）を適切に考慮された体制になっているのかなど、シーサートを見極めていく段階に入っていると考えます。

日本シーサート協議会ではシーサート構築のガイドである「CSIRTスタータキット」や必要な人材やシーサートの役割を定義した「CSIRT人材の定義と確保」などを公開しています。またシーサートを適切に評価できるための評価手法の検討や、組織において必要な訓練や演習の在り方、情報システムに存在するさまざまなログの分析手法の共有や検討など、多様な議論をワーキンググループの活動を通じて実施しています。

今後もさまざまな「場」を提供し、日本のさらなるセキュリティ向上に貢献してまいります。一日も早く日本シーサート協議会の「仲間」として皆様にお会いできる日を楽しみにしています。

（日本シーサート協議会 副運営委員長 萩原健太）

From JPNIC

Dear Readers

The big news from JPNIC is that Mr. Akinori Maemura of JPNIC assumed office as an ICANN Board Member on November 8, 2016. He was nominated by the Address Supporting Organization's Address Council (ASO AC). ICANN is an organization with a philosophy to support and manage one global Internet with multiple stakeholders, a vision that has yet to be experienced by anyone . Many of the adjustments between multi-stakeholders that may happen in the future will not be easy, but JPNIC will contribute to the stability of the Internet by being involved in activities supporting ICANN.

"Special Article 1" is a report on Internet Week 2016, which was held from November 29 to December 2, 2016, and its main plenary program IP Meeting 2016 . Internet Week celebrated its 20th anniversary, in line with this, a new venue was chosen and the program composition was changed. The total number of participants was more than 2,400 people and the number of sessions provided was 32. The panel discussion at the IP Meeting focused on life in the future generated by the Internet.

"Special Article 2 " covers two trends of discussion on the next generation WHOIS, namely Registration Data Access Protocol (RDAP) and the FBI's initiative to improve the accuracy of WHOIS registration information on IP addresses . WHOIS is a service that publishes registered information to search for IP address and domain name holders . Since WHOIS is one of the most important services for both registries and users, reviews of WHOIS are continually being pursued from both technological and political viewpoints to improve its usability and stability.

"Introducing JPNIC Members " focuses on JPNIC members engaged in interesting activities. This time we visited AT TOKYO Corporation, which runs the second largest data center in Japan, and was established in 2000 as a group company of Tokyo Electric Power Company Holdings, Inc (TEPCO). As its name suggests, AT TOKYO is a Tokyo-based large-scale data center equipped with an abundant power supply system backed by TEPCO. They have a strongly built and spacious center, flexible customized service and excellent bilingual support.

"Internet Terms in 10 Minutes " takes a look at Computer Security Incident Response Team (CSIRT) . This type of team is being actively established within organizations to handle many cyber attacks that are continuously occurring in Japan. This corner gives you a comprehensive explanation of the team's mission, service, scope of activities, constituency and definition of incidents. It is useful not only for organizations that are planning to create a CSIRT but also for organizations that want to reaffirm the role of a CSIRT.

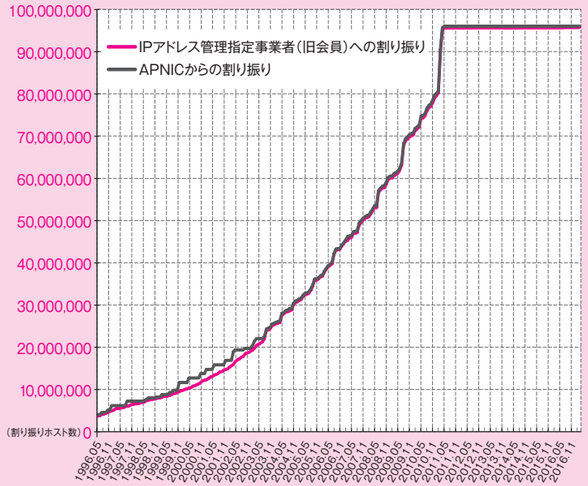
Issue 65 also covers many reports like APrIGF 2016, APNIC 43 in Colombo, NANOG 68/ ARIN 38, ICANN Hyderabad, JPNIC Open Policy Meeting , IGF 2016 in Guadalajara and IETF 97 Meeting in Seoul.

We do hope this newsletter will be valuable for many readers. Your comments and feedback are highly appreciated and always welcome at jpnic-news@nic.ad.jp.

統計情報
Statistics Information

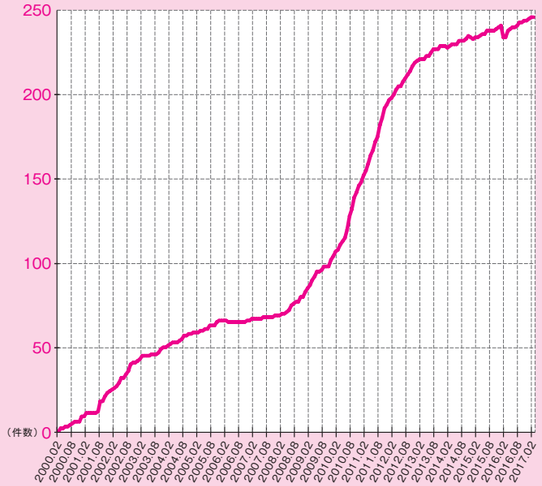
IPv4アドレス割り振り件数の推移

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。(2017年3月現在)



IPv6アドレス割り振り件数の推移

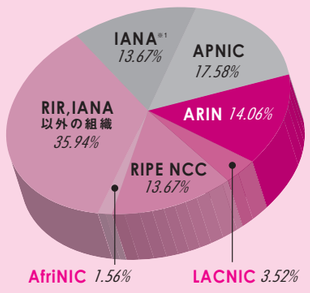
IPv6アドレスの割り振り件数の推移です。なお2011年7月26日より、IPアドレス管理指定事業者および特殊用途用PIアドレス割り当て先組織が、初めてIPv6アドレスの分配を受ける場合の申請方法は簡略化されています。(2017年3月現在)



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

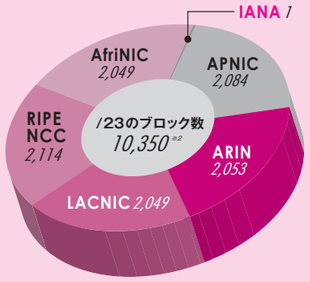
各地域レジストリごとのIPv4、IPv6、AS番号の割り振り状況です。APNICはアジア太平洋地域、ARINは主に北米地域、RIPE NCCは欧州地域、AfriNICはアフリカ地域、LACNICは中南米地域を受け持っています。**2011年2月3日に、IPv4アドレスの新規割り振りは終了しています。**

●IPv4アドレス(/8単位)



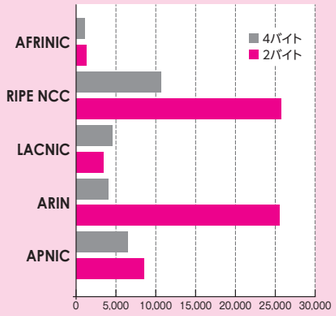
※1 IANA:Multicast(224/4)
RFC1700(240/4)
その他(000/8,010/8,127/8)

●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

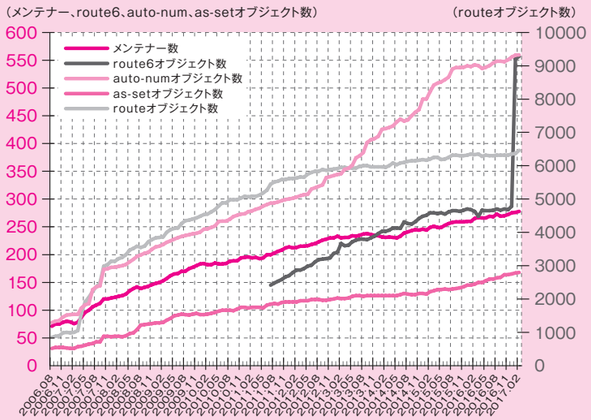
●AS番号※3



※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AS4,199,845,260個があります

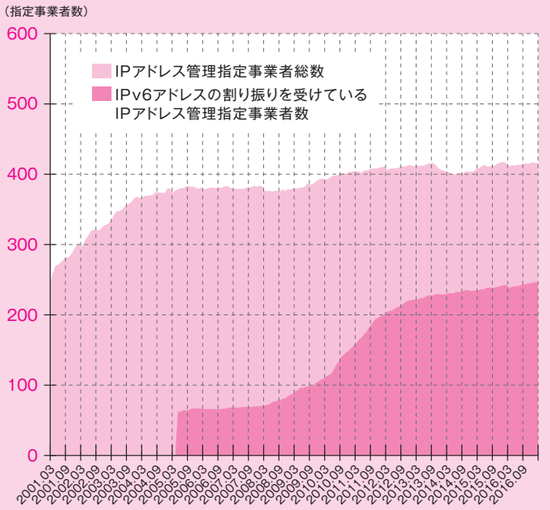
JPIRRに登録されているオブジェクト数の推移

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。(2017年3月現在)

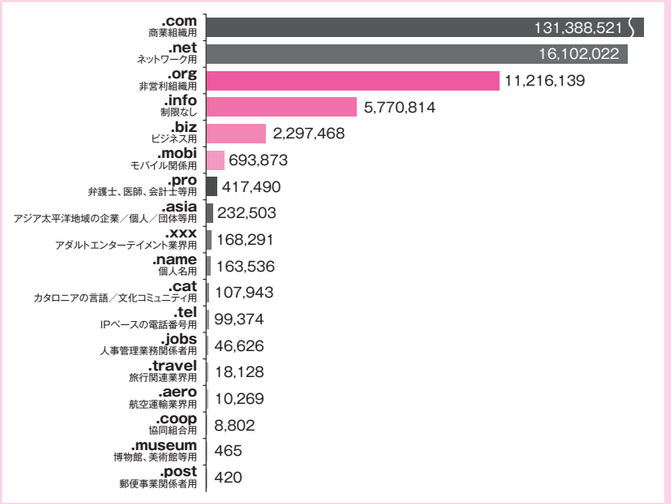


主なgTLDの種類別登録件数

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(2016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

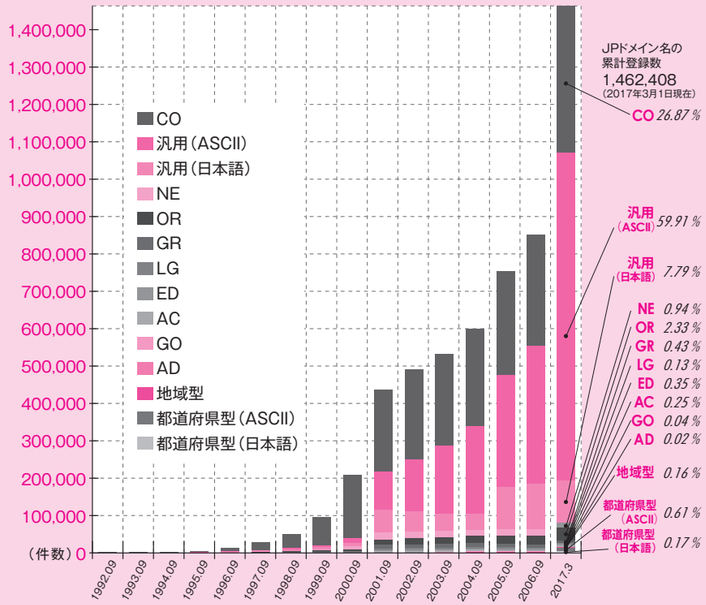


統計情報
Statistics Information

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、2017年3月現在では146万件に到達しています。

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。
(2017年3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

	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　8件
2015年	7件	移転　5件　取下げ 1件　取消 1件
2016年	9件	移転　6件　取下げ 3件
2017年	1件	係属中 1件

会員リスト
2017年1月24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

会員リスト

2017年1月24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
- 株式会社グローバルネットコア
- 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
- 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
- 株式会社ディーネット
- 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
- 株式会社ビークル
- BBIX株式会社
- ビットアイル・エクイニクス株式会社
- 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

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	ご利用方法
- 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	

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

2017年1月24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
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	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	今井 聡	北村 和広	佐々木 泰介	島上 純一	福田 健平
伊藤 竜二	岩崎 敏雄	木村 和貴	佐藤 秀和	城之内 肇	三膳 孝通
井樋 利徳	太田 良二	小林 努	式場 薫	橋本 吉正	吉宮 秀幸

賛助会員

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

https://blog.nic.ad.jp/

週に1〜2回、スピーディー＆カジュアルに情報を発信しています。
ニュースレターで取り上げていない話題も豊富にありますので、ぜひご覧ください!

JPNIC BLOG

JPNIC　ブログ

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64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65号
2017年3月17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 ISBN978-4-902460-40-7
©2016 Japan Network Information Center

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/

JPNIC Newsletter
NO.65
for JPNIC Members March 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
〒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

Business Connection Data Center

アット東京のデータセンターは、高品質のサービスと
ビジネスが加速・融合しあえる環境を提供し
新たな価値を創出します。

株式会社 アット東京

〒135-0061 東京都江東区豊洲5-6-36
Tel:03-6372-3500 Mail:at-sales@attokyo.co.jp
http://www.attokyo.co.jp/

記載されている情報は2017年3月現在のものです。サービス内容や仕様、その他の情報は予告なしに変更されることがあります。