JPNIC Newsletter
for JPNIC Members

NOVEMBER 2022
No.82

● 特集 1

Internet Week 2022
インターネットの羅針盤～針路を未来に取れ～ 開幕！

● 特集 2

pgp.nic.ad.jpサービスを振り返って

● インターネット10分講座

耐量子計算機暗号とは

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

IETFとグローバルなインターネット

来年2023年3月に、Internet Engineering Task Force（IETF）の第116回会議が日本（横浜）で開催される予定である。IETF会議は年に3回開催されており、通常、北米、ヨーロッパ、アジアでそれぞれ1回ずつ開催されている。日本での開催は、第54回（2002年、横浜）、第76回（2009年、広島）、第94回（2015年、横浜）に続き、4度目となる。これを機に、IETFにおける標準化について考えてみたい。

IETFは、インターネット技術に関する技術標準を策定する団体である。その特徴として、オープン性を重要視している。標準化のプロセスは、IETFに対して技術的に貢献するあらゆる個人に開放されており、そのプロセスや規格もすべて公開されている。このオープン性が、グローバルなインターネットを支える技術標準を策定する団体として重要である。

> We reject: kings, presidents and voting.
> We believe in: rough consensus and running code.
> – David Clark（IETF 1992 Plenary Presentation）

これは、David Clark博士が1992年のIETFプレナリーで発表した、IETFにおける合意形成プロセスを表した有名な格言である。IETFにおける合意とハミングについて記されているRFC 7282でも本文の1段落目で引用され、IETFの信条とされている。IETFは、その他多くの国際標準化団体やデジュール規格とは異なり、組織での参加ではなく、個人として標準化プロセスに参加する。さらに、その合意形成は、「投票」のように厳密に賛否を問うものではなく、「ハミング」により「ラフコンセンサス（rough consensus）」を確認しながら行われる。ラフコンセンサスの詳細については前述のRFC 7282を参照されたい。

このように、IETFでは個人で標準化プロセスに参加するため、その会議自体も排他的な要素を排除するように配慮されている。文頭でも述べたように、IETF会議は、毎年、北米、ヨーロッパ、アジアでそれぞれ1回ずつ開催されており、居住地域の違いによる参加への障壁を低減している（RFC 8719）。また、人種、民族、宗教、性別等が参加の障壁とならないように配慮しながら、会議開催場所の選定を行っている（RFC 8718）。

一般的には、IETFも国際標準化団体であると評される。しかし、上記の合意形成プロセスや排他的な要素の排除への取り組みを鑑みるに、IETFは国や地域、所属組織に依らず「グローバルな」インターネット技術の標準化を遂行する場であり、「国際」標準化団体とは少し違うのかもしれない。

David Clark博士の格言後段にある“We believe in:rough consensus and running code.”の“running code”についても、一言付け加えたい。IETFにおける標準化では、Draft Standard（標準草稿）としてRFC文書を発行するためには、二つ以上の独立かつ相互運用可能な実装、つまりrunning codeが必要とされている（RFC 2026）。この要求により、実装の存在しない技術や相互運用が不可能な技術を標準とせず、「動く」技術を標準文書として発行している。

このように、IETFはオープンなコミュニティと実装に基づく技術により、インターネットのグローバルな発展に大きく寄与してきた。社会情勢によりインターネットの分断が一部で危惧されているが、今後も技術や実装に基づくオープンなコミュニティにより自律・分散・協調システムであるインターネットが維持、発展されていくものと信じたい。

最後に、私は、IETF会議のネットワークを設営、運用するNetwork Operations Center（NOC）ボランティアとしてもIETF会議に参加しているため、その運用についても少しだけ触れておきたい。IETF会議のネットワークへの要求事項には、「フィルタされていないネイティブなIPv4およびIPv6によるインターネットアクセス」という特徴的な要件がある（RFC 8718）。実際には、IETF NOCはAS番号とIPアドレスブロックや機材を開催地に持ち込み、複数のISPとBGPを用いて相互接続することで、この要件を満たすインターネットアクセスを提供している。ネットワークごとにフィルタなどのポリシーが適用されること自体は自律システム（AS: Autonomous System）の考え方に添ったものである。しかし、IETF会議のネットワークがBGPによる相互接続により（グローバルで一つの）**The** Internetの参加者となり、開催地に依らずネイティブなネットワークを提供することは、“running code”と同様に、運用を通じて「動く」インターネットを維持していく上でも重要であるように思う。

JPNIC理事
浅井 大史
HIROCHIKA ASAI

プロフィール

浅井 大史（あさい ひろちか）

2013年東京大学大学院情報理工学系研究科博士課程修了・博士（情報理工学）。同年東京大学大学院情報理工学系研究科特任助教着任。2017年退任。同年、株式会社Preferred Networksにリサーチャーとして入社。2022年、同社シニアリサーチャー・インフラ戦略担当VP。2014年より現在まで、WIDEプロジェクトボードメンバー。2017年より現在まで、慶應義塾大学SFC研究所上席所員。インターネットアーキテクチャ、オペレーティングシステム、システム運用技術に関する研究に従事。

JPNIC Newsletter
for JPNIC Members
NOVEMBER 2022
No.82

CONTENTS

● 巻頭言
IETFとグローバルなインターネット
JPNIC理事　浅井 大史

● 特集 1　02
Internet Week 2022
インターネットの羅針盤～針路を未来に取れ～ 開幕！

● 特集 2　05
pgp.nic.ad.jpサービスを振り返って

● JPNIC会員企業紹介　08
世の中の役に立つことよりさ、毎日の仕事でワクワクすることの方が大事じゃないのかな
～くだらないセオリーよりも思い切って行動することで得られるものがある～
ユニタスグローバル株式会社
代表取締役 CEO 奥野 政樹 氏
Vice President-事業戦略／営業／マーケティング 中村 慎輔 氏
Vice President-技術 吉川 進滋 氏

● インターネットことはじめ　12
第17回 クラウドストレージ

● PICK OUT! JPNICブログコーナー　13
No.08 未来のインターネットに関する宣言

● Internet ♥ You（Internet loves You）　14
国立大学法人東京農工大学
助教
根本 貴弘さん

● 2022年5月～2022年9月のインターネット動向紹介　16
IPアドレストピック …… 16～19
技術トピック …… 20～22
ドメイン名・ガバナンス …… 23～25

● JPNIC活動ダイアリー　26
2022年7月～2022年11月のJPNIC関連イベント一覧 ／ 協賛・後援したイベント ／ これからのJPNICの活動予定

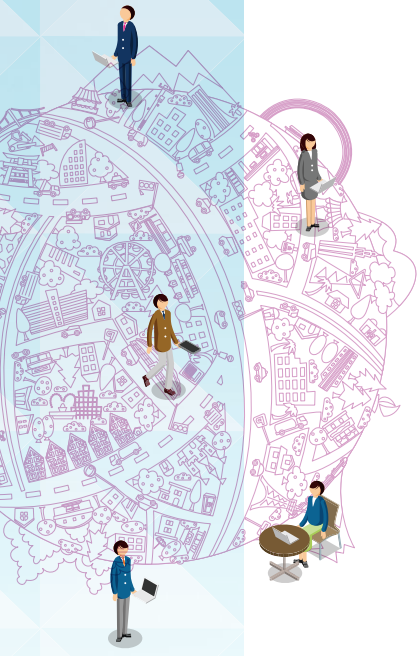
● インターネット10分講座　28
耐量子計算機暗号とは

● 統計情報　32

● 会員リスト　36

● From JPNIC　40

● 編集をおえてのひとこと。/ お問い合わせ先



JPNIC Newsletter 82号
読者アンケートにご協力ください
詳しくはこちら
（所要時間3分程度）
https://forms.gle/Wm2NBz9SCn2oWnMW7

Special Article
特集 1

Internet Week 2022
インターネットの羅針盤 ～針路を未来に取れ～

開幕！

Internet Week 2022を、11月21日（月）から11月30日（水）にかけて開催します。今年は3年ぶりの現地開催も含めた、ハイブリッド形式での開催となります。本号の特集では、実行委員長の挨拶とともに、その概要をお知らせします。

変わらぬ使命と変わりゆく役割
～Internet Week 2022開催によせて～

Internet Week 2022
実行委員長
JPNIC常務理事 長谷部克幸

今年からInternet Weekの実行委員長を務めます、JPNIC常務理事の長谷部克幸です。どうぞよろしくお願いいたします。

■ 新たな四半世紀のスタートに、変わらぬ使命を再確認して

多くの方に支えられて、Internet Weekは昨年2021年に25周年を迎えました。今年は新たな四半世紀へのスタートです。この節目の年に、あらためてInternet Weekの役割を考えてみます。

Internet Weekの前身は「IP Meeting」です。今では最終日に実施するInternet Week締めのプログラムとしてお馴染みかと思います。1990年、インターネットが学術・研究目的で使われ始めた時に、インターネットの運用に関わる人々が一堂に会し、課題解決を行う場として始まりました。Internet Weekと名を変えたのは1997年、インターネットが一般にも広く使われ始め、多くの技術者が必要とされた頃です。そのような方々に正しい情報を伝える場として、60以上のセッションを擁するインターネットの技術に関する総合イベントとなりました。

それぞれの分野で第一人者の方々を講師に迎え、インターネットのことを学びたいなら「Internet Week」しかないと当時は言われました。これからインターネットに関わる方に、自身の知識を常にアップデートしたい方のために、正しい情報を提供することは、今後も変わらずInternet Weekの使命と言えるでしょう。

■ 変わりゆくもの ― インターネットは「みんなのもの」へ

一方で、Internet Weekが始まった頃と比べると、インターネットを取りまく環境は大きく変わりました。例えば2021年9月に発足したデジタル庁が「誰一人取り残されない、人に優しいデジタル化を」と掲げたように、インターネットはごく一部の関係者や最新技術に詳しい人々だけが使うものではなくなりました。むしろ、今インターネットから遠いところにある分野や人々にも積極的に目を向けて巻き込んで、使っていただけるようにするものになりました。

また先ほど述べたように、知識の習得という点では、当時はInternet Weekが唯一と言っていいほどの役割を果たしていましたが、現在はどうでしょうか。大小さまざまなイベント・セミナー・勉強会が開催され、この数年の急激なオンライン開催、オンデマンド配信対応なども相まって、学ぶ場や手段に関して私たちは多くの選択肢を手にしています。

このような中で、Internet Weekはどうあるべきか。まさに今のインターネットを総覧できる場でありたいと考えます。この1年のインターネットに関する技術動向、社会動向、各種事象に対する傾向と対策などが、Internet Weekに来ればわかるという状態です。もっと詳しく知りたい、関係者間で議論したい時には、テーマや対象者をより絞って深堀りするようなイベント・セミナー・勉強会を探してさらに知見を深める。Internet Weekをそのように活用いただけたら幸いです。

■ 今年のテーマに込めた想い

今年のテーマは、「インターネットの羅針盤 ～針路を未来に取れ～」です。まさに先ほど述べたような、Internet Weekがインターネットに関わる方々の羅針盤でありたい、という想いを込めました。ますます巧妙化するサイバー攻撃、「インターネットの精神」をあらためて見つめ直し、考えさせられる社会問題など、私たちが考え、議論すべきことは多くあります。このような航海に細心の注意を払うべき局面で、どちらの方に進むべきかを指し示す、あるいはどちらの方に進むべきか、議論できる場にしたいと考えています。

また、これから1年間、IETF 116（2023年3月）、IGF2023（2023年秋）と、二つの国際会議が日本で開催されます。日本にいながら、世界中の関係者ともダイナミックな議論に参加できる年でもあります。その2023年を前にしての情報収集にもご活用いただけるプログラムとなっています。

■ Internet Weekの新たな試み ― ハイブリッド開催

今年の新しい挑戦の一つが、ハイブリッド開催です。過去2年は新型コロナウイルス感染症対策のためオンライン開催でしたが、今年は会期後半の3日間は、オンライン参加に加え、オフライン会場参加もご提供する予定です。特に講演者と参加者による活発な意見交換を期待するプログラムについては、ハイブリッドで開催します。

もちろん、本稿執筆時点ではまだ予断を許さない状況ではありますので、当日の現地参加が叶わない方もいるかもしれません。また、この数年で働き方が大きく変わるなどして、引き続きオンライン参加を希望する方もいるでしょう。現地参加できない方向けの「おまけ」的な扱いだった以前とは異なり、オンライン参加の方も同じように質問し、意見が言える場となるよう、インターネットの力を最大限活用していきます。今年も多くの方のご参加をお待ちしています。

Intenet Week 2022 プログラム　https://www.nic.ad.jp/iw2022/program/

※下記の内容は2022年11月8日(火)時点のものです。
最新の情報はInternet Week 2022のWebサイトをご覧ください。

参加申込ページ
https://www.nic.ad.jp/iw2022/apply/main/

オンラインWeek　11月21日(月)～25日(金)

11／21(月)

10:00 ～ 10:45	【C11】独法でダークファイバを使ってみた話	ネットワーク運用管理
11:00 ～ 11:45	【C12】5Gモバイルネットワーク入門	ネットワーク運用管理
13:00 ～ 15:45	【C13】取捨選択できる運用組織	
16:00 ～ 16:45	【C14】Wi-Fi航海図 ～みえない電波を理解する～	ネットワーク運用管理
17:00 ～ 18:45	【C15】ルーティングセキュリティ ―インターネット運用の羅針盤―	ネットワーク運用管理

11／22(火)

10:00 ～ 10:45	【C21】コンテンツプロバイダがIPv6対応するための7ステップ	IPv6
11:00 ～ 11:45	【C22】QoEからみたIPv6 ～CDNおよびストリーミング事業者が語る～	IPv6
13:00 ～ 16:00	【H2】AWSクラウドによるIPv6対応Webサイト構築ハンズオン	ハンズオン

11／24(木)

11:00 ～ 11:45	【C31】スプリンターネットを読み解く	社会派
13:00 ～ 14:45	【C33】【学生・若手歓迎】「セキュリティの仕事、どんなことをしているの？どうしたらなれるの？」	セキュリティ
15:00 ～ 16:45	【C34】サイバー攻撃2022	セキュリティ
17:00 ～ 17:45	【C35】サイバー攻撃情報連携の羅針盤	セキュリティ
18:00 ～ 18:45	【C36】サイバー攻撃を止めるには？ 攻撃の動向&abuse対応依頼入門	セキュリティ
19:00 ～ 20:30	【B3】Abuse BoF	

11／25(金)

10:00 ～ 10:45	【C42】PSIRTとSBOMの重要性について	セキュリティ
11:00 ～ 11:45	【C41】NOTICEとかIoTセキュリティとか	セキュリティ
13:00 ～ 13:45	【C43】Threat Intelligence の活用によるセキュリティ対策の効率化と高度化	セキュリティ
14:00 ～ 14:45	【C44】ゼロからはじめるOSINT(Open Source Intelligence)	セキュリティ
15:00 ～ 15:45	【C45】Cyber Hygiene Hunting:セキュリティ実効性確認のすすめ	セキュリティ
16:00 ～ 16:45	【C46】セキュア開発との向き合い方 ～実践して初めてわかる要所と課題感～	セキュリティ
17:00 ～ 17:45	【C47】これからのセキュリティ組織の道標	セキュリティ
18:00 ～ 18:45	【C48】情報処理安全確保支援士が活躍する社会をめざして	セキュリティ

ハイブリッドWeek　11月28日(月)～30日(水)

11／28(月)

10:00 ～ 12:45	【C51】みんな集まれ！インターネットに関わる国際標準化のつどい 第1部 標準化って何なのか？ 日本の取り組み(チュートリアル) 第2部 パネルディスカッション ―使われる技術や制度に携わる魅力と国内での捉え方― 第3部 2023年3月 IETF116横浜に参加しよう！	
13:00 ～ 13:45	13:00 ～ 13:20 【L51】トラフィック分析／可視化のあり方 ―効果的な分析を探る ［提供］インターネットマルチフィード株式会社 13:25 ～ 13:45 ［提供］株式会社SRA	ランチタイムセミナー
14:00 ～ 15:45	【C52】初のハイブリッド開催も支える！ Internet Week 2022配信お悩み相談室	
16:00 ～ 17:45	【C53】激情の劇場　プラットフォームを信じていいですか？@スナックまさこ2.0	社会派
18:00 ～ 18:45	【C54】Peering入門	ネットワーク運用管理
19:00 ～ 20:30	【B5】Peering in Japan BoF	

11／29(火)

10:00 ～ 11:45	【C61】インターネット広告の羅針盤 ～ ポストクッキー、嵐の時代	
12:00 ～ 12:45	【L6】DNSの弱点を振り返り、今後の針路について考える ―ランチのおともにDNS ― ［提供］株式会社日本レジストリサービス	ランチタイムセミナー
13:00 ～ 18:45	【C63】DNS DAY - DNS Update - IETF／RFC動向 - DNSソフトウェア動向 - ドメイン名のライフサイクルマネージメント - ブランドを守るために必要な送信ドメイン認証	
19:00 ～ 20:30	【B6】日本DNSオペレーターズグループ BoF	

11／30(水)

10:00 ～ 11:30	【C71】Web3の羅針盤	
11:45 ～ 12:25	11:45 ～ 12:05 【L71】containerlabで始めるルータ遊び ［提供］日本インターネットエクスチェンジ株式会社 12:05 ～ 12:25 ［提供］株式会社GEAR	ランチタイムセミナー
12:40 ～ 14:15	【C72】サステナブルなインターネットのための情報的健康のすゝめ	社会派
14:30 ～ 18:30	【C73】IP Meeting 2022 ～インターネットの羅針盤 -針路を未来に取れ～ 第1部　インターネット運用動向2022 第2部　IGF2023を睨み、情報社会のいろんなことを語ろう 第3部　2030年目標への羅針盤 第4部　2023年に向けて(クロージング)	

Internet Week 2022 開催概要

正式名称

Internet Week 2022
https://www.nic.ad.jp/iw2022/

Facebook : https://www.facebook.com/InternetWeek
Twitter : https://twitter.com/InternetWeek_jp
ハッシュタグは #iw2022jp

テーマ

「インターネットの羅針盤～針路を未来に取れ～」

会 場

オンライン ＋ 東京大学伊藤謝恩ホール
https://www.u-tokyo.ac.jp/adm/iirc/ja/access.html
※オフライン会場はハイブリッドWeekのみ提供

開催日程

2022年11月21日(月)から11月30日(水) ※土日祝日を除く
[オンライン Week]
11月21日(月)、22日(火)、24日(木)、25日(金)
[ハイブリッド Week]
11月28日(月)～30日(水)

開催目的

1. インターネットの発展を推進する
2. インターネットに関する議論の場・交流の場を提供する
3. セミナー開催によるインターネット基盤技術の普及を図る

対象者

インターネットの技術者および
インターネット技術と社会動向に興味のある方

内 容

インターネットに関するチュートリアル、最新動向セミナー、
ハンズオンセミナー、協賛団体セミナー、BoF等

主 催

一般社団法人日本ネットワークインフォメーションセンター(JPNIC)

協賛団体

NTT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
Asia Pacific Network Information Centre
インターネットマルチフィード株式会社
株式会社SRA
株式会社GEAR
KDDI株式会社
日本インターネットエクスチェンジ株式会社
VIAVIソリューションズ株式会社

後 援 (2022年11月4日時点)

総務省／文部科学省／デジタル庁
一般社団法人ICT-ISAC
特定非営利活動法人ITコーディネータ協会(ITCA)
IPv6普及・高度化推進協議会(v6pc)
一般財団法人インターネット協会(IAjapan)
Internet Society Japan Chapter(ISOC-JP)
仮想化インフラストラクチャ・オペレーターズグループ(VIOPS)
一般社団法人JPCERTコーディネーションセンター(JPCERT/CC)
一般社団法人重要生活機器連携セキュリティ協議会(CCDS)
一般社団法人情報サービス産業協会(JISA)
一般社団法人情報処理安全確保支援士会(JP-RISSA)
一般社団法人セキュリティ対策推進協議会(SPREAD)
一般社団法人ソフトウェア協会(SAJ)
一般社団法人電子情報技術産業協会(JEITA)
一般社団法人日本インターネットプロバイダー協会(JAIPA)
日本MSP協会(MSPJ)
一般財団法人日本情報経済社会推進協会(JIPDEC)
日本セキュリティオペレーション事業者協議会(ISOG-J)
一般社団法人日本スマートフォンセキュリティ協会(JSSEC)
日本ネットワーク・オペレーターズ・グループ(JANOG)
特定非営利活動法人日本ネットワークセキュリティ協会(JNSA)
フィッシング対策協議会
日本UNIXユーザ会(jus)
WIDEプロジェクト(WIDE)

企 画

Internet Week 2022 プログラム委員会

pgp.nic.ad.jpサービスを振り返って

はじめに

OpenPGP公開鍵情報の登録・検索サービスを、2022年9月30日（金）で終了した。

PGPの公開鍵サーバーは、1998年9月中旬に認証実用化実験協議会（ICAT）の管理していたサーバーからJPNICの管理するサーバーpgp.nic.ad.jpに移行したので、かれこれ約24年間にわたりOpenPGP公開鍵情報の登録・検索サービスを提供していた。

pgp.nic.ad.jpのサービスを終了するにあたって、振り返りとして少し書き留めておきたい。

pgp.nic.ad.jpに至るまでの経過

1993年に開始されたPGP公開鍵交換のためのサーバーは、メールで登録・検索・要求を行う実装であった。1993年の年末にようやくNCSA HTTPdが現れたという時代で、Webを介しての動的なコンテンツサービスというものは存在していなかった。当時、MIT、UCSD、ハンブルグ、オックスフォードといった四つか五つぐらいの大学にあるサーバーでPGP公開鍵交換サービスが開始され、どこかに登録すると、相互に共有するという仕組みになっていた。

筆者は1994年4月11日からPGP公開鍵サーバーのサービスを開始し、世界に散らばるPGP公開鍵サーバーと相互に公開鍵を交換し共有した。運用していたサーバーは、当時筆者が所属していた株式会社SRAの研究部門の一つであった、ソフトウェア工学研究所内にあった。当時のメールでPGP公開鍵を登録したり取得したりする方法に関しては、MITのサーバーの上にテキストファイル※が残っている。1994年6月時点で筆者のサイトも含めて、世界中で14サイトがサービスしていることがわかる。

1997年当時MIT大学院生だったMarc Horowitz氏によって、TCP/IPで接続可能なPGP鍵サーバーpksd（PGP Public Keyserver）が実装された。この時に、hkp（Horowitz Keyserver Protocol）プロトコルが考案された。これによって、いわゆるインターネット接続可能なPGP公開鍵サーバーの運用が開始されるようになった。hkpプロトコルは現在も、The GNU Privacy Guardで提供されているOpenPGP仕様の暗号ツールgpgで利用可能である。

1996年7月に、PGP公開鍵サーバーをICATに移行した。このバージョンは、それまでと同様にメールによるインタフェースである。MITがHorowitz版PGP鍵サーバーpksdに移行して、しばらくしてICATもpksdに移行した。しかし、当時のpksdは、まだ初期段階で、品質は高くなく、Sunのマシン上ではコンパイルも通らないような不安定なものであった。筆者は、かなりソースコードに手を入れ、パッチを鍵サーバーのコミュニティに還元していった。

ちなみに1998年にpgp.nic.ad.jpに移行した後も、かなりソースコードに手を入れている。その結果、pgp.nic.ad.jp上で動いているpksdは、筆者が長年にわたりコードに手を入れ続けたので、オリジナルのコードからずいぶんと違うものになっている。

Web of Trust

PGPやGnuPGといった、OpenPGP仕様（rfc4880）の公開鍵暗号・電子署名ツール（以降 pgp/gpg/OpenPGP）は中心となる認証局は持たず、相互の信頼によって相手を認証する。最もプリミティブな方法は、お互いが対面で相手を確認し、その際に、相手の鍵に自分の署名を付けるというものである。

ここで一つ、非デジタル的な問題がある。ここにアリスとボブがいて、アリスであることを保証し、ボブであることを保証して、相互認証を行おうとした場合は、公的証明書を確認するなどが必要となる。1対1では行うには効率が良くない。

そこで、鍵署名パーティー（Keysigning Party）が行われるようになる。実際行われる鍵署名パーティーは、本来のセキュリティ的な価値より、集まって自己紹介する一種の親睦を深めるイベントのようなものである。初期の頃は、参加者が、お互いに身分証明書を見せ合い、自分の公開鍵のfingerprintの印刷物を渡す、あるいは読み上げるという素朴なものだった。あちこちでやり方がバラバラだったので、元々効率が悪かったものが、さらに効率が悪くなった。

そこで現れたのが、Zimmermann-Sassaman key-signing protocolである。これが生まれるきっかけとなったのが、the First PGP Keyserver Manager Symposiumでの鍵署名パーティーであった。従来の方法があまりにも効率が悪いので、PGPオリジナル作者である Philip Zimmermannが、Zimmermannとともに参加していた当時PGP社のレン・サスマンに、もっと効率の良い方法を考えるようにと指示を出した。そして、完成したのがEfficient Group Key Signing Methodであり、現在、Zimmermann-Sassaman key-signing protocolと呼ばれるものである。

なぜ、そのようなことを知っているかと言うと、そのシンポジウムに筆者も参加していたからである。各国の鍵サーバー管理者やPGPおよ

※ http://web.mit.edu/Tcl/src/exmh-1.6.1/misc/pgp-keyservers.txt

びGnuPGの関係者が、オランダはユトレヒトにあるSurfnetの会議室に集まり2日間行われた。その中で行われた鍵署名パーティーだったが、20名前後の小さな集まりで行われたにもかかわらず、Zimmermannは最後、ウンザリした顔をしていたのを今でも思い出す。さて、このようにして生まれた鍵署名パーティーであるが、今年の7月(July 24, 2022)にコソボで行われたDebConf22でも行われている。

お互い対面で確認し署名をするという方法ができない場合、「自分が既に署名している信頼のおける公開鍵から署名されている公開鍵は信頼することとする」という方式を使う。これがWeb of Trust(信頼の輪)である。この考え方は既に、1992年のPGP version 2.0に現れる。一元化された(集中型)信頼モデル(centralized trust model)としてのPKI(Public Key Infrastructure)と対比される形で、分散型信頼モデルとしてWeb of Trustは存在している。

しかし、シンプルに考えると今も昔もWeb of Trustは、「友達の友達は友達だ」というレベルである。筆者も初期の頃は、Web of Trustという方法も意味があるのではないかと考えていたが、現在では欺瞞(deception)に対して脆弱な極めて危険な方法論と考えている。1992年から2022年の現在まで使われ続けており、それによってWeb of Trustという方法が安全であるような幻想が、独り歩きしているとすら筆者は考えている。

pksd公開鍵サーバーの問題点

pgp.nic.ad.jpで可動していたpksdが作られた頃は、インターネットは性善説を前提としていていた。誰でも登録可能な公開鍵サーバーであった。今から考えれば牧歌的な時代であったと感じる。勝手に他人の公開鍵を登録することも可能である。自分の公開鍵であるにもかかわらず、一度誰かによって登録されてしまうと、たとえ一つの公開鍵サーバーから消しても、他の運用ポリシーの違う公開鍵サーバーに自動的に登録されるため、すべての公開鍵サーバーから消し去ることは実質的に不可能であった。後にいくつかのOpenPGP仕様に対応した公開鍵サーバーでは、鍵の中に有効なメールアドレスを加えていることを登録条件としているものが出てきた。

2016年に作られたGDPR(General Data Protection Regulation; EU一般データ保護規則)には、当然のこととして対応していない。公開鍵に付けられているメールアドレスや名前などは、そのままむき出しである。自らの意思で登録したならばともかく、第三者が登録しているような公開鍵に付いている個人情報に対して何もプロテクションできないし、オプトアウトも実質できないので、明らかにGDPRに抵触する。これまでの長い歴史的な経緯があり、現在も運用してるという理屈も限界であろうと筆者は考える。

理想と現実のギャップ

1992年当時に筆者が考えていたインターネットの世界は、end-to-endでデータが暗号化され、データが保護される時代が来るというものだった。確かに現在では、TLSで通信路が守られていてend-to-endで保護されているが、データそのものを暗号化するというトレンドは現れなかった。また日本においてはいわゆるPPAP問題のように、ファイルを共通鍵暗号で暗号化し、メールで送り、その後に暗号化に使った鍵をメールで送るという、誤った暗号技術の利用方法が広く使われるといった、残念な状況にまでなっている。

pgp.nic.ad.jpのトラフィックを見ても、日本国内からのアクセスは最初から最後まで低調だった。1990年代の終わり頃は、「インターネットのセキュリティは発展途上なので現状では利用はほとんどないが、あと10年もすれば個人で利用する電子メールやファイルはすべて電子署名付きでやり取りされるようになる」と考えていた。しかし、残念ながらそうはならなかったし、今後もそうはならないだろう。これはPGP/GnuPG/OpenPGPだけではなく、TLS(SSL)もそうであると言える。httpsが急激に普及したのは無料の“Let's Encrypt”が普及したためであり、それまでのように高価な“SSL証明書”を販売していたのではそうはならなかった。では有料と無料の価値がどれだけ違うかと言えば、米国防総省の情報機関NSAの公式WebサイトはLet's Encryptの証明書を利用していると言えばわかってもらえるだろうか。少なくとも、PGP/GnuPG/OpenPGPに限らず公開鍵暗号の個人利用に関しては、現状のアプローチでは利用は広まらないであろう。

現在、PGP/GnuPG/OpenPGPで利用可能な公開鍵サーバーをいくつか挙げておく。

```
keys.openpgp.org
keyserver.ubuntu.com
pgpkeys.eu
```

公開鍵サーバーの代替案として

Web of Trustは信頼するのに十分ではないと説明したが、信頼できるツリー方式というのは十分に考えられる。例えば組織のCA局(Certificate Authorityという言い方は不適切かもしれないが、他に思い付く言葉がないのでここではCAと呼ぶ)にあたるOpenPGP署名用公開鍵をDNSの専用領域に用意しておき、それを使うという方法である。RFC4398ではThe CERT resource record(RR)という形で規定されており、またgpgでは、RRの公開鍵を利用できるようになっている。組織の中で利用する公開鍵は、そのCA(マスター鍵)によって署名を付けてもらう。これで公開鍵の信頼度は、その組織のDNS管理の信頼度に近似できる。組織内のメンバーで利用する際は、同じ信頼度である。pgp/gpg/OpenPGPでは、複数のCA局からの一つの公開鍵に署名を付けることができる。信頼できるCA局(一つまたは複数)の署名が付けられている時、そのCA局が保証している範囲の信頼度で利用することが可能となる。

近年では、個人のブログやgithubでリポジトリを利用している場合も多い。Webページはもちろんのこと、例えばgithubのリポジトリにAscii Armorフォーマットの公開鍵のファイルを置いておくなどが

個人でもできる。例えば、筆者がpublickeysというリポジトリを作成し、その下にpublic.ascというOpenPGPフォーマットの公開鍵ファイルを置いておくとする。この場合、次のようにしてダウンロードしてインポートすることが可能である。このように、リポジトリに公開鍵（署名）を含めておくと、以降、作者からのメッセージとして署名を使うことができる。

```
curl -s https://raw.githubusercontent.com/
SUZUKI-HIRONOBU/publickeys/main/public.asc |
gpg --import
```

この場合、信頼の起点はgithubである。最初に得たものを信じて使うというTOFU（Trust on First Use）の亜流ではあるが、既に活動実績のあるリポジトリで、githubのセキュリティレベルで管理されている点が大きく違う。しかし、これも、これまでyumやaptといったGNU/Linuxのシステムメンテナンスのツール群も、ダウンロードサーバー上に置かれている公開鍵をcurlによってダウンロードし、システムに設定するという方法を使っているので、それを個人ベースに置き換えていると言っても差し支えないであろう。

まとめ

pgp.nic.ad.jpを終了するにあたり、公開鍵サーバーとは何だったのかを振り返ってみた。システムの安全性を確保するためにpgp/gpg/OpenPGPの技術はシステムに組み込まれ広く使われたが、個人ベースの利用は過去も現在も極めて限られている。公開鍵サーバーを経由して個々のユーザーが公開鍵を交換するというモデルは、この30年近い運用をしたものの、現実のニーズに即してはいなかったと言える。システムに組み込まれたpgp/gpg/OpenPGPは広く使われるようになり、一部でPPAP問題のような状況が出てきたにしろ、暗号技術による安全性の確保というのは必須の技術となった。その点は大変良かったと感じる。筆者の目から見たざっくりとした振り返りであるが、何かの役に立てば幸いである。

（元pgp.nic.ad.jp管理者 鈴木裕信）

INFORMATION　国際会議開催のお知らせ

IETFミーティングが7年ぶりに日本にやってきます！

IETF Meetings 2023 3.25 SAT → 31 FRI

第116回IETFミーティングが2023年3月25日（土）～31日（金）の日程で、WIDEプロジェクトのホストにより横浜で開催されることになりました。日本でのIETFミーティング開催は、第54回（2002年、横浜）、第76回（2009年、広島）、第94回（2015年、横浜）に続いて4回目となります。

IETFとは？

IETFは、インターネット技術の標準化を推進するグループで、メーリングリストと年に3回行われるミーティングを通じて、インターネットに関わる標準の文書であるRFC（Request For Comments）を策定しています。IETFにおける技術標準化の議論はワーキンググループ（WG）を単位にして推進されていて、ミーティングやメーリングリストでの議論には誰でも自由に参加することができます。

IETFにおける技術仕様の策定は、ラフコンセンサス（Rough Consensus）とランニングコード（Running Code）を重視しているのが特徴で、まずラフな仕様を作成し、それから相互接続実験や実運用を通じて、工夫、改善を加えながら詳細な仕様を実装していくという、非常に柔軟な仕様策定プロセスとなっています。

最近ではリモート参加という方法もありますが、今回の日本開催は技術標準を議論する場に直接入っていき、多くの技術者と直接話しができる貴重な機会です。会場など詳細が決まりましたらJPNICのWebなどであらためてお知らせしますので、ぜひ多くの皆さまのご参加をお待ちしています。

IETF 116 Yokohama
https://www.ietf.org/how/meetings/116/

JPNIC 2022 member

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。

世の中の役に立つことよりさ、毎日の仕事でワクワクすることの方が大事じゃないのかな

～くだらないセオリーよりも思い切って行動することで得られるものがある～

UNITAS GLOBAL

ユニタスグローバル株式会社（旧:インターナップ・ジャパン株式会社）

住　　所：〒101-0045
　　東京都千代田区神田鍛冶町3-3-12 神田鍛冶町千歳ビル7F
設　　立：2001年4月10日
資 本 金：1億円
代 表 者：奥野 政樹
従業員数：29名（2022年10月22日時点）
ＵＲＬ：https://www.inap.co.jp/

事業内容 https://www.inap.co.jp/about/outline.html

- 法人向けインターネット接続サービス
- クラウド接続サービス
- 拠点間接続サービス
- 日本語／英語ITサポートサービス

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

今回は、2001年4月の創業から今年で22年目を迎えた、ユニタスグローバル株式会社（旧INAP Japan）を取材しました。同社は米国のベンチャー企業であるINAP社とNTTグループの合弁事業としてスタートし、INAPが独自に開発した経路制御の最適化技術を武器に、低遅延で高品質なネットワークサービスを提供されています。

これまではINAP Japanとして事業を行ってきた同社ですが、2022年5月のINAP社からUnitas Global社への事業売却に伴う、ユニタスグローバル株式会社への社名変更を直前に控えたタイミングでの取材となりました。当日は、設立から現在に至るまでの紆余曲折を、代表である奥野様の強い信念を交えつつ時には面白おかしく軽妙に語っていただくとともに、ユニタスグローバルとして新しく生まれ変わった同社が提供を予定している、新サービスなどをご紹介いただきました。

さまざまな文化の差を乗り越えてのスタート

◉ まずは貴社の成り立ちを教えてください。

奥野：当社の設立は2001年4月で、1996年にベンチャー企業として設立された米国インターナップ・ネットワークサービス（INAP）社と、NTTグループによる合弁事業としてスタートしました。INAP社は米国で大成功した勢いで日本進出を考えていた時期で、国内のパートナーとしていくつかの大手キャリアに声をかけており、その一つがNTTグループでした。とはいえ、NTTの掲げる事業戦略にこういった外資ベンチャーとの合弁などはなく、また社内政治的にも当初はあまり乗り気ではない雰囲気でした。反対の声も多かったのですが、それを私がいろいろと策を用いて社内をまとめあげ、新しい会社を作るところまでこぎ着けました。日本の大企業と米国のベンチャーなんて、仕事のやり方も社内意識もどこをとってもミスマッチだらけです。そういう部分を解決して事業を成功させるのはものすごく大変そうだけど、やりがいもありそうだしぜひ自分がやってみたいと思ったんですよね。今と違って、当時の私はそういう部署にいなかったので、インターネット接続自体が商材として売れるなんてことはまだ理解していませんでした。


東京・神田の本社オフィスはJPNICから徒歩圏内です

ただ、私の社内での今後のキャリアを心配する上司などの反対もあり、すぐにこの合弁事業に関わることはできなくて、私が出向してきたのは2003年のことです。合弁の際に国際法務に強いということで契約関係の交渉を任されていたのですが、その際に契約書に社外監査役の規程を入れておいたことが役に立ちました。事業が始まると案の定お互いの文化の差に由来するトラブル続出だったので、そこでいろいろアドバイスをしているうちに米国側から「ぜひ彼を呼んでくれ」と声がかかったんです（笑）。

◉ 設立にあたってはご苦労があったのですね。奥野様が関わられてからは、順調に事業が進むようになったのでしょうか。

奥野：いや、そんなに簡単ではなかったです。私の上に社長がいたんですが、まずはクーデター（笑）を起こしました。私の考えるやり方で、社の運営を根本から変えるところからスタートしました。その後も、しばらくの間の混乱と苦しみは尋常ではなくて、信じられないこともたくさん起こりましたし良い勉強になりました。採用一つとってもかなり難しくて、NTT時代とは比べものにならない苦労がありました。それでも試行錯誤しながら続けていってプロパーの社員をどんどん増やし、NTTからの出向社員を減らしていきました。比率が逆転したのは2005年か2006年頃ですね。最後の出向者は、何と私自身だったんですよ（笑）。

人材採用と育成には自信アリ

◉ 人材採用にはどのようなご苦労があったのでしょうか？

奥野：プロパー採用を始めた当初は、何と受けに来た人を全部採用していたんですよ（笑）。NTT時代の経験があるので、応募者の差などあまりなく短時間の面接では何もわからない、入社後のマネジメントでどうにでもできると思ってたんです。でも実際はそんなことはなく、とんでもない人が来てしまうことがありました。そこで反省をして、採用スキルを磨いていきました。今では我々は採用のプロだと自負していますが、長年の経験からきた結論としては、真面目で一生懸命やるかどうかを見抜くのが面接の肝です。ポイントは応募者がきちんと面接の準備をしてきているかですね。Webサイトを見ているか、経営理念なども含めて当社のことを調べて理解しているか、言葉にするとそんなことかと思われるかもしれませんが、ここをよく見ていけば人材採用で外れはほぼありません。

吉川：当社は学歴や職歴を不問にしていますが、この会社のために何ができるかや、仕事に対するやる気、またNOC（Network Operation Center）という仕事、24時間安定したインターネットを守るという意味がきちんと理解できているかを見ています。また、世の中にはインターネットやPCが好きで、趣味でPCを自作したりネットワークを組んだり、サーバを立てたりしている人がいますが、こういう人は他社では未経験として門前払いでしょう。でも、その中には単に学校を出て資格を持ってるだけの人よりも、用語を知らないだけでよほど肌感覚でネットワークを正しく理解できる人がいるんです。そういう、職歴はないけれども経験をうちで活かしてくれそうな人は、一貫して採用してきています。未経験から入っても、そういう人は数ヶ月で上級レベルになれます。

奥野：「成長を続ける社員の行動により、世の中に付加価値をもたらす」と経営理念に掲げているように、仕事を通じて成長し続けること、そして世の中の役に立つことを考えるより毎日仕事でワクワクできることをとても重視しています。その方が、結果的には世の中のた

めになるんじゃないですかね。だって、ワクワクしてる人は周囲もワクワクさせますからね。あと、うちは採用するとまずNOCに入ってもらいます。そこから営業や技術、また経理などのバックヤード部門に行ったりして活躍というパターンです。他社、特に外資はこういうことはやりませんね。まずはNOCでコアとなる人材を確保し、NOCにいる間に社内のオペレーションを見つつ、いろいろと学んでスキルを身につけて、他部署に行くなりNOCで極めるなりという流れです。

◉ NOCが貴社の人材環流の中心になっているわけですね。以前は、NOC業務は外注されていたと聞きましたが、どういった経緯で内製化されたんでしょうか？

奥野：2008年にお客様を日本語・英語で24時間サポートするNOCを自前で作ったんですが、これは当社自身が大きく変わるターニングポイントになりました。当時はNTT系の企業にアウトソースをしていたんですが、契約更新時に先方から値上げの打診があったんです。こちらの足下を見る内容で、ちょっと応じられないとなったんですよね。ただ、そうなると契約が切れるまでもう1ヶ月しかありません。それまでに大急ぎでNOCを立ち上げる必要が出てきました。そのためにはシフト勤務でバイリンガルサポートができる要員を最低でも7人集める必要があり、急いで採用に取りかかったんですが、2週間経っても1人も集まらず途方に暮れてしまいました。その後は何とか7人集めたんですが、なかなか強者揃いで採用後も手がかかって大変で、一時期おばけ屋敷状態になりましたが、どうにかNOCをスタートさせることができました。後に、契約を切ってきた相手から「そう言えばどうなりました？」と聞かれ、「ああ、NOC、自社に作りましたよ」と返事をした際は、相手はぽかんとしてましたね（笑）。

中村：このNOC設置をきっかけに、当社の体制は大きく強化されていったわけですが、当時はやはり社内で相当議論がありました。できるわけがないとか、フィリピンにある外部のグローバルサポートセンターを使えなどという声もあり、米国本社などはそういう意向でした。ただ、それだと長期にわたってまともなサポートはできないですし、顧客とネットワークの話もできません。それを良しとするのか、それとも自分達でそれができる人材を育てて高品質なサービスを提供していくのか、そういう議論をしたんです。結果、最後は奥野が後者の道を歩むんだと本社を説得したんです。

世間の“常識”にこだわらずベストな道を探る

◉ 貴社のお客様についてお尋ねしたいのですが、貴社サービスの強みからやはり金融機関や外資系企業の方が多いのでしょうか。

奥野：外資系企業は多いですが、日本のお客様もたくさんいます。イメージだと日英サポートで回線品質が高いから、金融やオンラインゲーム、動画配信系の顧客が大半かと思われるかもしれませんが、実際はそういう顧客ばかりではありません。今はオフィス用インターネットの需要が旺盛です。従来は食い込めなかった分野ですが、ここのところのリモートワークの流行でネットワークの帯域や

【公式MV】Unitas Global@地獄の淵でRock Us Baby!
https://youtu.be/Rb4Jm-MsVXs

品質に対する要求が高まっています。ただ、そういった商品はOCNやKDDIも持っていて、我々の品質はそれらよりも高いと自負していますが、それを評価してもらうためには営業力とマーケティング力が重要かなと思っています。

マーケティングでは、教科書的なものは重視していません。当社が作成したミュージックビデオにもありますが、世間で言われるセオリーなんてものを信じちゃいけません（笑）。「決裁者の許可を取る」方法を重視しろと言われますが、あれは日本じゃダメです。決裁者が決裁をするんじゃないんですよ。NTT時代に当社を作った時、私は決裁権限なんてない一課長でしたしね（笑）。大事なのは社内でこれをやるんだと決めて動く人達で、具体的には面白いことを見つけてきて社内にどんどん火を点けて回る人とそれを止めようとする人で、そこを押さえることが重要です。私は「放火魔と警察官」と言っていますが（笑）、これを重視するのが当社のマーケティングです。相手が大きい会社だと、基本的には決まったところとしか取り引きしないので、どうしようか検討させてしまったら負けです。話は聞いてくれた、面白いね、検討します、じゃダメ。何かよくわからないけど気が付いたら買っていた、これを目指しています。Unitas Globalの一員になることで新しいサービスも増えますし、当社のマーケティングも、もう1ランク上に行きたいと思っています。

◉ 貴社はUnitas Globalグループに入られて社名変更を控えていらっしゃるタイミングですが、今後はどのようなサービスに力を入れていく予定なのでしょうか。

奥野：Unitas Globalグループの一員として、今後はこれから話す2本柱を軸に事業を進めていくことになります。

まず一つ目が、「Unitas MIRO Donuts Net」です。Unitasが得意なドーナツピアリングと、当社が独自に磨き上げてきた最適経路通信の技術であるMIRO（Managed Internet Route Optimizer）を組み合わせたものです。Unitasは高品質通信の世界を作って、そこに世界中のローカル／コンテンツ／サービスプロバイダーを繋いでネットワークを広げてきました。その巨大なリン

グネットワークはドーナツピアリングと呼ばれ、他社のTier1ネットワークを回避して世界中と通信できるというメリットがあります。そこにMIROの技術を乗せることで、さらに他社よりも優れた通信プラットフォームとなります。

二つ目は「Unitas Reach」で、現在米国でNaaS（Network as a Service）として展開されている同サービスを日本にも展開します。世界中にSD-WAN（Software Defined-Wide Area Network）が張り巡らされていて、edge-to-edgeで日本と海外の拠点を接続できます。将来的には、Unitas Reachに繋がれば世界中にリーチできるようになります。

吉川：UnitasのAS1828は世界の隅々までピアリングしていて、まさにドーナツの名にふさわしく世界を1周しています。INAP時代のMIROはピアリングとかあまり関係のない世界でしたが、今後はピアをたくさん張っていき、そこでも通用する最適化技術にMIROをブラッシュアップしていくのが今後の目標です。

あと余談ですが、エンジニアとして個人的にはUnitasになることでAS番号が4桁になるのが密かに嬉しいです（笑）。今はAS17675ですが、AS1828になると国内の古参事業者やJPNICよりも若くなります、これは強く主張したいですね（笑）。

インターネットは人類における技術の大衆化の最高傑作

◉ 貴社には普段からJPNICのメディアに会員広告などを出稿していただいていますが、AS2515のJPNICに対して（笑）、何かご意見やご要望などはありますでしょうか。

奥野：他社のエンジニアと意見交換できるような、交流会などの機会を作ってくれると嬉しいですね。社内に閉じこもっているのは良くないので、当社では社員をJANOGやACCJ（在日米国商工会議所）のイベントなど、いろいろなところに参加させています。業務命令にしないと、自分からはなかなか行きませんから。2022年7月に函館で開催されたJANOG50 Meetingは若い社員4名だけで参加させましたが、せっかく行く以上はつまらないことはするなと言って、自分達をどうアピールするかディスカッションさせました。こういったイベントや展示会に参加する時は結構本気ですよ。イベント出展はエンターテインメントです。つまらない商品説明をしても意味がなくて、来ていただく方、見ていただく方、ブースに来ていただく方を楽しませないといけません。キャラを立たせて信念を持って、目立つユニフォームやオリジナル曲を作ったりして、気合いを入れています。こういう経験をしていくと、OJTや社内資格の勉強なんかよりもよほど成長します。

吉川：外部のイベントは営業担当は行きますが、うちのエンジニアは伝統的に外にあまり出てこなかったんですよ。でも、今後はピアリングなどが増えていくと思うので、国内のコミュニティに顔を出す機会が増えていくかなと思っています。

中村：JPNICは日本を代表する資源管理の団体なので、日本のインターネットがイケているということをどんどん発信していって欲しいですね。アジアのハブは香港、シンガポール、日本で、そこを急成長している中国が狙っています。そういった中で、JPNICの払い出すIPアドレスを使うことにどれだけの価値があるのか。日本の通信事業者は総じて事故が少なく、低遅延で通信できます。そういう障害率が低い環境でビジネスできること、そういったバリューがあると世界に発信してもらえると、日本の事業者は競争上有難いと思います。当社も、日本に高品質なネットワークサービスがあることを世界中の企業に知ってもらうために日々頑張ってますので。

吉川：APNICが最近のインターネットトレンドなどを映像付きで配信していますけど、JPNICも海外向けに日本の情報を発信してもらえると嬉しいです。米国では、「日本のIPアドレスなんてAPNICからもらえばいいんだろう？」ぐらいの認識の人も多いですから。

◉ 本日は業務の話に留まらず、いろいろと貴重なご意見などもいただきましてありがとうございます。最後に伺いたいのですが、皆さまにとって「インターネット」とは何でしょうか？

吉川：答えに困る質問ですね（笑）。「インフラです」としか答えようがないです。私にとっては水道や電気、ガスと同じレベルのインフラの一つで、お金を稼ぐための大事な基盤です。もう2000年ぐらいから、私にとってはそういうものです。

中村：元々は、インターネットは善意の塊で、お互いがASを繋ぎ合って良い通信を作っていくものでした。最近は悪用する話の方が大きくなってしまった印象がありますが、一方で良い話もあります。その時代ごとの良し悪しが、インターネットの良い使われ方、悪い使われ方など状態に表れていると思います。インターネットに対してはポジティブ、ネガティブとそれぞれ見方がありますが、それらには世の人々のインターネットに対する見方が反映されているんじゃないでしょうか。

奥野：電話時代は、相互接続のルールが難しくセキュリティも厳しくて、手間暇がかかるため通信は値段が高いものでした。それが、インターネットは相互接続のルールもセキュリティも電話に比べると緩やかで、その結果値段も安くなり爆発的に広がりました。そういう意味で、インターネットは決して技術革新ではなく、いろいろなルールや手続きを廃止して手を抜いた仕組みなんですよ。簡素化と手抜きにより実現された、人類における技術の大衆化の最高傑作だと思っています。

これまで通信は、のろしから飛脚、郵便、電話と技術革新を経てきましたが、そろそろ次の技術革新がくるんじゃないでしょうか。脳波を使って、他人と直接通信できたりするようになるかもしれません。それができた時に、インターネットははたしてどうなるのか。電話はほぼ役割を終えましたが、郵便は今も残っています。なので、今後コミュニケーションにおける革命が起きても、インターネットもレガシーとして残るのかもしれません。ただ、インターネットが次のステージに進むためには、元々の設計思想を思い出して、セキュリティだのルールだのでガチガチに縛るような、インターネットの良さをスポイルするような考えは改めていく必要がありそうです。

インターネットことはじめ

協力:森下 泰宏(JPRS)

1 データはどこかにある

スマートフォンが普及した2010年代以降、写真や動画などのファイルをインターネット経由で保存・共有する、オンラインストレージサービスの利用が当たり前のことになりました。スマートフォンで撮影した写真や動画は事業者が提供するオンラインストレージに自動的にアップロードされ、インターネット上のどこかに準備されたストレージに保存されるようになります。そのため、こうしたサービスは、クラウドストレージとも呼ばれています。今回は、このクラウドストレージの始まりを探してみましょう。

2 普及のきっかけ

WindowsならOneDrive、macOSやiOSならiCloud、AndroidならGoogleドライブと、いまやクラウドストレージはOSベンダーが提供するものを、それぞれのOSからシームレスに利用できるようになっています。あらかじめ設定しておいた特定のフォルダやドライブにデータを書き込むと、自動的にクラウドストレージにコピーされます。また、複数のデバイスを使っていても、同じアカウントでログインすれば自動的に同期され、どのデバイスでも同じデータが使えます。

実のところ、WinodwsにしてもmacOSにしても、このようなサービスは意外と古くからあるのですが、最初に有名になったものはOSベンダーのものではなく、2008年9月に正式サービスを開始したDropboxでした。専用のクライアントをインストールすると、指定したフォルダーがDropboxのクラウドストレージと同期され、複数のデバイス間でデータを共有できるという機能を、広く認知させたサービスです。以後クラウドストレージは、基本的にサーバーとクライアントのデータを同期する方向で発展してきました。

3 OS標準のサービス

前述した、各OSベンダーが標準提供しているクラウドストレージは、意外と古い歴史を持っています。

iCloudのルーツは2000年1月に提供されたiToolsで、複数デバイス間でのデータ同期をこの時点で実現していました。しかし、当時はスマートフォンなど影も形も無く、Macintoshコンピュータを複数持っている人も限られていたため、データ同期機能はさして話題になりませんでした。以後、.Mac→ MobileMeと変遷を重ね、2011年10月にiCloudサービスが始まり、現在に至っています。

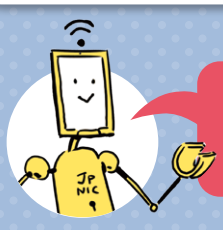
OneDriveは、2008年2月にSkyDriveとしてサービスが始まりました。2013年9月に、Winodws 8.1に機能が統合され、OS標準の機能となっています。Googleドライブは意外と遅く、2012年4月にサービスが始まっています。前述のようにAndroidやChrome Bookでは標準サービスとなっており、WindowsやMacOSでも専用プログラムをインストールすることで利用できます。

4 ファイル共有との違い

ネットワーク越しにデータを読み書きするという点では、いわゆるファイル共有がそのルーツとして挙げられます。Unixならば1984年のNFS、Macintoshだと1984年のAFP、Windowsならば1990年のLAN Manager 2.0などです。ただこれらはクライアントからはただのハードディスクに見え、クライアント上のデータとサーバー上のデータを自動同期するという概念は持っていませんでした。つまり、データはサーバーにしか無かったのです。またネットワーク速度やセキュリティの観点からLANでの利用が前提で、インターネットを経由した広域のファイル共有については考慮されていませんでした。

広域ファイル共有のルーツとしては、古いところで1971年に公開されたFTP、Webの時代になってからは1996年に公開されたWebDAVあたりが相当しそうです。ただこれらは専用のクライアントプログラムでサーバーとデータをやりとりする、という使われ方がメインです。もっともmacOSやWindows 7以降では、WebDAVを使ったネットワークドライブを構成することもできますが、これは広域ネットワークに対応したファイル共有の一種であり、データの自動同期に標準対応しているわけではありません。

このあたりを勘案すると、現代につながるデータの同期機能を備えたクラウドストレージの始まりは、どうやらiToolsと言えそうです。



次回は
「ファイル共有」を
取り上げる予定です。

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

カテゴリー
- IETF
- Internet Week
- IPアドレス
- JPNICからのお知らせ
- JPNICについて
- JPNICのイベント
- アクセス数Top 10
- インターネットガバナンス
- インターネットの技術
- コラム
- ドメイン名
- 他組織からのお知らせ
- 他組織のイベント

dom_gov_team 2022年5月13日 インターネットガバナンス https://blog.nic.ad.jp/2022/7530/

「未来のインターネットに関する宣言」

2022年4月28日に、「未来のインターネットに関する宣言」立ち上げイベントが、対面およびテレビ会議のハイブリッド形式で開催されました。同イベントにて、「未来のインターネットに関する宣言」が発表されました。米国、欧州諸国、オーストラリア、ニュージーランド、日本をはじめとするパートナーが提案し、60ヶ国／地域以上が賛同した本宣言について紹介します。

■「未来のインターネットに関する宣言」立ち上げイベント

2022年4月28日に大臣級の立ち上げイベントが、米国東部夏時間午前7時30分（日本時間同日20時）より約1時間半にわたり、米国の国家安全保障問題担当大統領補佐官のジェイク・サリバン氏が主催して、オンラインと現地会場のハイブリッドで開催されました。

まずアルゼンチンのアルベルト・フェルナンデス大統領の録画メッセージが流され、その後はライブで最初に宣言起草に関わった国々よりオーストラリア、カナダ、日本、英国、欧州委員会の順にスピーチがありました。日本からは金子総務大臣が日本語でスピーチしたものが同時通訳され、IGF 2023を日本で開催することにも触れられていました。

次に署名国より、ジャマイカ、アルゼンチン、ウクライナ、マーシャル諸島、ニュージーランド、カーボベルデ、コロンビアの順にスピーチがありました。ウクライナからはミハイロ・フェドロフ第一副首相兼デジタル改革担当大臣が英語でスピーチし、ウクライナとロシア間の戦争に触れ、情報や新技術への自由なアクセスは、自由と民主主義の原則に基づく人類の未来の発展のための土台となる、と述べました。台湾のオードリー・タン政務委員（デジタル担当）も遠隔参加していましたが、スピーチはありませんでした。

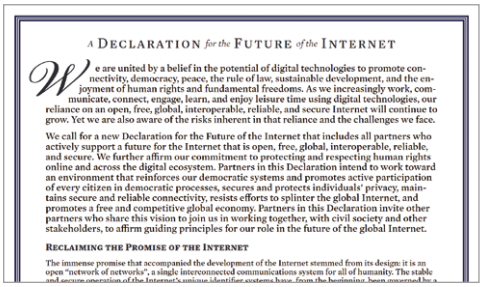
■「未来のインターネットに関する宣言」の内容

前文では、主に次の2点が述べられています。

- 本宣言のパートナーは、オンラインおよびデジタルエコシステム全体における人権の保護と尊重への約束を確認すること
- 本宣言のパートナーは、民主主義システムを強化し、民主主義的プロセスへのすべての市民の積極的な参加を促進し、個人のプライバシーを保証・保護し、安全で信頼できる接続性を維持し、グローバルなインターネットを分断する取り組みに対抗し、自由で競争力のあるグローバル経済を促進する環境をめざして取り組むことを意図している

本文の構造および概要は次の通りです。

1. インターネットへの期待を取り戻すために
2. 我々のビジョン
3. このビジョンを推進するための原則
4. 人権と基本的自由の保護
5. グローバルなインターネット
6. インターネットへの包括的で安価なアクセス
7. デジタルエコシステムにおける信頼
8. マルチステークホルダー・インターネット・ガバナンス



A DECLARATION for the FUTURE of the INTERNET

We are united by a belief in the potential of digital technologies to promote connectivity, democracy, peace, the rule of law, sustainable development, and the enjoyment of human rights and fundamental freedoms. As we increasingly work, communicate, connect, engage, learn, and enjoy leisure time using digital technologies, our reliance on an open, free, global, interoperable, reliable, and secure Internet will continue to grow. Yet we are also aware of the risks inherent in that reliance and the challenges we face.

We call for a new Declaration for the Future of the Internet that includes all partners who actively support a future for the Internet that is open, free, global, interoperable, reliable, and secure. We further affirm our commitment to protecting and respecting human rights online and across the digital ecosystem. Partners in this Declaration intend to work toward an environment that reinforces our democratic systems and promotes active participation of every citizen in democratic processes, secures and protects individuals' privacy, maintains secure and reliable connectivity, resists efforts to splinter the global Internet, and promotes a free and competitive global economy. Partners in this Declaration invite other partners who share this vision to join us in working together, with civil society and other stakeholders, to affirm guiding principles for our role in the future of the global Internet.

RECLAIMING THE PROMISE OF THE INTERNET

The immense promise that accompanied the development of the Internet stemmed from its design: it is an open "network of networks", a single interconnected communications system for all of humanity. The stable

「未来のインターネットに関する宣言」（原文）
https://www.soumu.go.jp/main_content/000812325.pdf

■考察

記載内容については、現在のマルチステークホルダーによるインターネットの運営という考え方を支持していて、全体として好ましいものであると考えます。

当初の同盟を作るという考えに関しては、普遍的なインターネットを守るために一部の国／地域で同盟を形成するというのは矛盾するということにもなり、宣言として出し、追って賛同国を増やすという方策がより妥当だと考えられます。

当初賛同したのは60ヶ国／地域と、国連加盟国が193ヶ国あることを考えると多くなく、今後賛同が増えるか、あるいは賛同ではなく対抗する動きが出てくるかなどについて注視が必要です。

INTERNET LOVEs YOU
インターネット・ラブズ・ユー
No 17

国立大学法人東京農工大学 助教
根本 貴弘さん

国立大学法人東京農工大学助教。博士（メディアデザイン学）。2019年同大学総合情報メディアセンターに着任、大学情報システムの運用や情報教育とそれらに関する研究等に従事。2021年、同大学令和2年度職員表彰を受彰。2011年からIETFでの標準化活動に参加、現在は国際化技術に関する標準化提案を行うとともに、その専門性を活かしてInternationalization DirectorateおよびART Area Review TeamのReviewerとしても標準化活動に貢献。RFC7790共著者。その他、インターネットソサエティ日本支部OfficerおよびIETF Education WG Chair、JPNIC2030年代を見据えた情報通信ネットワークアーキテクチャとその標準化活動に関するアドバイザリーチームメンバー等。

INTERVIEW

東京農工大学で大学ネットワークの運用や国際化技術、国際化文字列等の研究に従事しながら、Internet Engineering Task Force（IETF）やインターネットソサエティ日本支部（ISOC-JP）でも活動されている、根本貴弘（ねもとたかひろ）さんにお話を伺いました。インターネットの分野で大学教員としてのキャリアを歩まれているものの、インターネットに深く関わるようになったのは大学院に進学されてからという根本さんに、これまでの経験や影響を受けてきたもの、今後の目標などを語っていただきました。

根本さんがインターネットを知ったきっかけ

高校1年生の頃に携帯電話を買ってもらい、i-modeを使ったのが最初だと思います。当時は、今ほどパソコンやインターネットに関心がなく、インターネットの利用もメールや着信メロディーのダウンロード程度でした。

パソコンを使うようになったのは、大学に入学してからです。BYOD（Bring Your Own Device）を前提とした授業があるため、入学時にiBook G4を買いました。パソコンを使った授業では、Javaのプログラミングやホームページ作成などに取り組みました。授業以外では、たまにデジカメで撮影した写真を編集したり、インターネットで検索したりする程度のライトユーザーでしたが、mixiが流行したのがきっかけで、よくインターネットを使うようになりました。

大学生の頃について

早稲田大学の人間科学部人間環境科学科に入学し、翌年、人間情報科学科に転科しました。人の生活を豊かにするデザインに関心があり、認知科学やコミュニケーション学、人間工学等の観点から、人と情報の関係を学びたいと思い転科を決めました。また、デザインを通じて社会問題にアプローチする考え方に触れ、この頃の関心が発展して、国際協力の分野に結びついていき、国連大学のグローバルセミナーにも参加し、世界で起きているさまざまな問題について学びました。サークル活動では、繊維研究会という早稲田大学の中でも歴史あるサークルの幹事長をやっていたことがあり、そこでは年に1回、ファッションショーを開催していました。その中で、消費を促すだけではなくて、持続可能な社会の発展について考えることがあり、サークル引退後は、視野を世界に広げ、国際協力について学んでいくこととなりました。

学部時代に学んだ国際協力への関心がきっかけとなり、さまざまな国や地域の人が一緒になって学べる環境があるといいなと考え、いろいろな分野の専門性を持つ人達がコラボレーションし、プロジェクトに取り組みながら研究活動を行う、慶應義塾大学大学院のメディアデザイン研究科（KMD）に進学しました。進学当初はKMDのカリキュラムに従い、デザイン、テクノロジー、マネージメント、ポリシーの各分野について学びました。その中でも、当時は特にデザイン分野に注力しており、授業の課題で作成した制作物を発展させ、コンピュータエンターテイメント技術に関する国際会議に投稿し、ギリシャまで発表しに行く等も行いました。その後、バーチャルリアリティ（VR）やオンライン授業を扱うプロジェクト等と大変悩みましたが、最終的にネットワーク系のプロジェクトを選択し、本格的にインターネット技術について学び始めました。

修士の頃は、イベント会場におけるインターネットの活用に取り組みました。富士スピードウェイで開催される軽自動車の耐久レースで、インターネットを使ったコミュニケーションやテレメトリの実証実験、リアルイベントにおけるインターネットを活用したエンターテイメント性の拡張として、車載カメラの映像やセンサ等の情報を動画コンテンツとして配信し、応援メッセージ等を受け付けるWebシステムの構築等を行いました。

博士課程に進学してからは、結婚の予定もあったことから、多少なりとも収入を得たい思いがあり、大学の先生に相談したところ、IETFのInternet-Draft（I-D）の翻訳業務を紹介してもらいました。これを募集していたのが株式会社日本レジストリサービス（JPRS）で、その縁でインターンシップも参加させてもらいました。インターンシップ初日の集合場所は成田空港で、そのまま台湾に行き、ICANNのVariant Issue Projectの会合に参加しました。意味は同じだが字体は異なる異体字という文字列を、トップレベルドメイン名でどう扱うかを検討する会合でした。それ以降は、IETFのPRECIS WGで発表するための準備に取り組みました。PRECIS WGでは、Stringprepに代わるアプリケーションで取り扱う識別子やパスワードを国際化（i18n）するための議論を行っており、私はプロトコルレベルの処理に渡す前にアプリケーション側で行うべき文字列の前処理のガイドラインの策定に取り組んでいました。2012年3月にパリで開催されたIETF 83が初参加で、同時に初めて発表も行いました。その後も、複数のI-Dを並行して執筆し、IETF会合での発表や議論を重ね、贅沢な経験をさせていただきました。インターンシップ終了後も、IETFでの提案は継続しており、学生の身でありながら、IETFに提案しているI-Dの本数が慶應義塾大学の中で1番多い時期もありました。また、PRECIS Derived Property Valueの算出プログラムを世界で最初に実装したことから、PRECIS Frameworkが標準化された際には、IANA Registryに登録するPRECIS Derived Property Valueの検証データの提供に協力しました。

大学教員になられた根本さんの、これまでのキャリアについて

世界を舞台に国内外の人と一緒に何かを作り上げていくことが楽しく、標準化活動は継続したいと思っていました。就職先については強いこだわりはありませんでしたが、ある程度自身の裁量で活動範囲をコントロールできると思い、大学教員としてのキャリアを考え、青山学院大学の情報メディアセンターに就職しました。大学教員ではありましたが、大学のネットワークの調達や運用がメインで、社内IT部門に近い役割でした。私が着任した年から、青山学院大学が箱根駅伝で優勝するようになったり、入試の合格発表がオンライン化したりと、Webページのアクセス集中に備え、慌ただしく対応しました。その年はDNSラウンドロビンで暫定的に対応し、次年度からはロードバランサを導入したのを覚えています。他には、Cisco Networking Academyのインストラクター資格取得や、学生に講習会形式でネットワークを教えることにも取り組みました。青山学院は、大学だけでなく小中高と学校があるため、基幹ネットワーク管理者として考慮する範囲が広くて大変な面がある一方で、私の興味があることも自由にやらせてもらえました。IETFにはほぼ毎回参加しましたし、2017年にInterCommunityという、世界中のISOCの支部をつないで行うISOCの一大イベントのローカルアレンジメントで、東京ノードを青山学院大学に設置させていただきました。その功績が評価され、ISOC本部から感謝状をいただきました。

現在は東京農工大学に移りましたが、業務としては前職とあまり変わらず大学の情報システム運用や調達、新入生向けの情報教育等に取り組んでいます。また、それらに関する研究活動にも取り組み、そこで得た成果を国内外で発表しています。

コミュニティ活動について

IETFでは、主にApplications and Real-Time（ART）エリアやSecurity（SEC）エリアにてi18nに関連する技術提案を見ています。また、PRECIS Frameworkを使用するプロトコルで最新のUnicodeを利用するための提案もおこなっています。一般社団法人情報通信技術委員会（TTC）から受託業務としておこなっている標準化動向調査では、i18nに関連する技術だけでなく、IoT技術についても調査を行なってきました。2022年2月からは、i18nに関する専門家チームであるInternationalization Directorate（i18ndir）及びART Area Review Team（artart）のレビューアーとしても標準化活動に貢献しています。最近だと、EPP（Extensible Provisioning Protocol）というプロトコルでEAI（Email Address Internationalization）を使用するための拡張提案に関するレビューも行っています。IETFで長く貢献されてきた大先輩方に混ざり意見を述べるのは、とても緊張することですが、勉強させていただくことも多々あり、とても良い刺激をもらっています。

ISOC-JPには、2014年からプログラム委員会（PC）メンバーとして関わり始めました。PCを2年務め、インターネット標準化推進委員会（ISPC）ができてからは、そちらに参加し、IETF報告会やIETF勉強会、IETFの現地参加者向けの情報交換会であるGet-Togetherの等の企画や運営等に取り組んできました。2016年3月に設立されたIETF Education WGでは、チェアを務め、IETFのEducation Teamと連携して、IETF新規参加者向け資料の日本語訳を行ってきました。IETF会場で、IETF参加に際して翻訳した資料を見たという人に出会うこともあり、自分たちの活動が日本のインターネットコミュニティに貢献できていることを実感でき、とても嬉しかったです。2017年からは、ISOC-JPのオフィサー（役員）に選挙で選ばれ、チェアも担当しました。多くの方にISOC-JPの活動を知っていただき、参加してもらえるよう、これからも頑張っていきたいです。直近では、2023年3月25日～31日にIETF 116が横浜で開催されるので、それを盛り上げるための活動にも取り組みたいと思っています。

今後の目標について

今後も継続してコミュニティ活動や標準化活動に参加していくためにも、まずは大学の業務をきちんとこなしていきたいと思います。先輩先生方を見ていると、職位が上がるにつれ多忙になっている印象ですので、一層の精進が必要だなと感じています。個人的には、今の道に進むきっかけを作ってくれた慶應義塾大学の加藤朗先生や、JPRSの米谷嘉朗さんをはじめとし、多くの先輩方のおかげで今があると思っています。IETFに参加している方の中には、若者を導いてくれる「おじさん」が多くいらっしゃいました。そこで出会う方々が、気さくに話しかけ、いろいろとアドバイスをしてくださったことは、特に感謝しています。自分も同じように、新たに参加する人を巻き込んでいく雰囲気を守っていきたいです。IETFでは現地会合も再開しているので、その雰囲気作りにうってつけなISOC-JPのGet-Togetherを復活させたい気持ちがあります。

根本さんがプライベートではまっていること

昔から、服が凄く好きです。ショップスタッフと話したり、服飾品に関するうんちくを調べたりするのも好きです。子供の成長に合わせ七五三等のイベントの記念写真で着るスーツを作りたいと思ったことがきっかけで、仕立て服に関心を持ち、友人に渋谷にあるTailor Caidという仕立て屋さんを紹介してもらいました。魅力的な店主の山本さんをはじめ常連さんから、普段なかなか学べない大人のマナーや嗜みを教えてもらっています。またここ最近は、いろいろなことがオンラインにシフトする中で、SNSを通じて国内外のファッション関係の方々と知り合う機会に恵まれ、人脈も広がりました。在宅勤務が始まり通勤時間がなくなったことで、大好きな家族と一緒に過ごす時間が増え、心に余裕を持ちやすくなったことが、仕事や趣味にも良い影響がでたのではないかと思います。

最後にインターネットに対する愛情のこもったメッセージをお願いします！

インターネットは自分にとって、グローバルなもので、自分の世界を広げる道具です。仕事だけでなく、趣味の場面でも、人と人との繋がりを広げてくれるところに魅力を感じています。それ故に、スプリンターネットのようにインターネットそのものを分断せず、いろいろな人が自由に安心して使えるインターネットの維持・発展に貢献していきたいと思っています。また、インターネットを通じて得た繋がりによって、さまざまな活動の機会をいただいていると思いますので、その経験をいろいろな方と共有できる「おじさん」になれたらいいなと思っています。

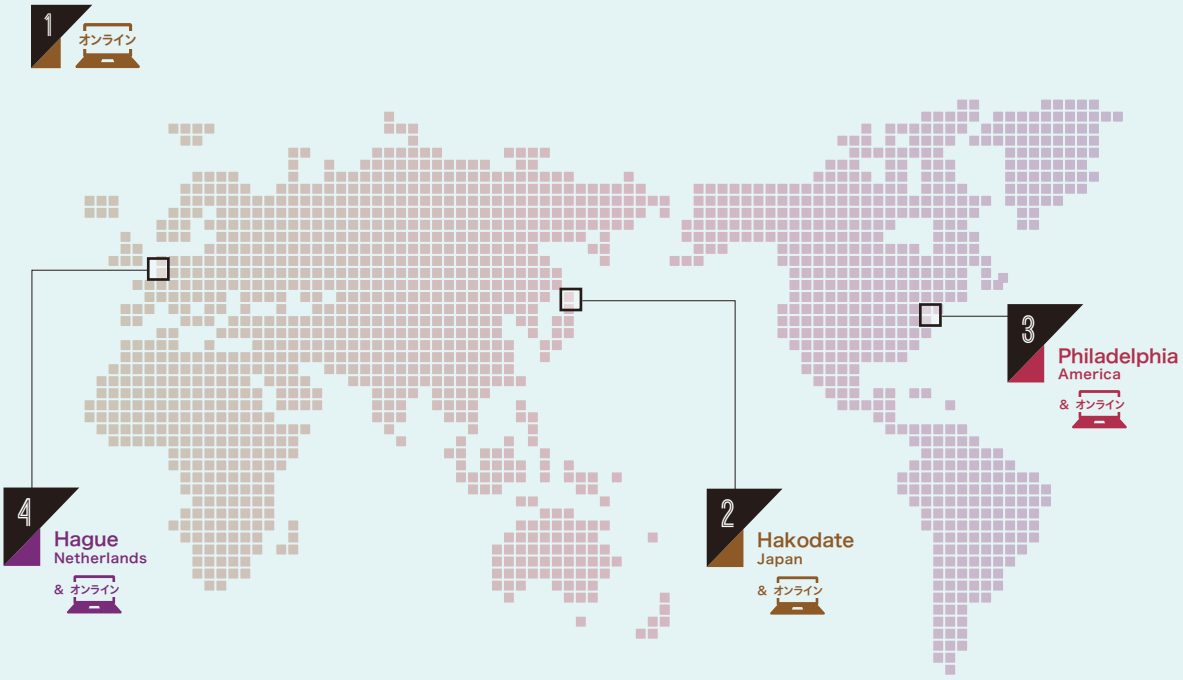
▲ IETF87での発表の様子

▲ IETF95の際に、ISOC-JPの翻訳活動でお会いしたScott Bradnerさん

Tailor Caid店主の山本祐平さんと、新作のグレーフランネルスーツの仮縫い ▶

インターネット動向紹介

INTERNET TRENDS INTRODUCTION 2022.05 ― 2022.09



IPアドレストピック

INTERNET TRENDS INTRODUCTION

1 2022. 6.24
第42回JPNIC
オープンポリシーミーティング
オンライン

2 2022. 7.13 ▸ 7.15
日本／函館市
JANOG50 Meeting
オンライン

IPアドレスに関する動向として、2022年6月24日に開催された第42回JPNICオープンポリシーミーティングの動向を取り上げます。その他、2022年7月に開催されたJANOG50 Meetingで実施したRPKI/ROVに関する野良BoFのレポート、JPNIC WHOISに関する話題を取り上げます。

第42回JPNICオープンポリシーミーティングの動向

2022年6月24日（金）に、第42回JPNICオープンポリシーミーティング（JPOPM42）が開催されました。今回も新型コロナウイルス感染症（COVID-19）の影響により、リモートのみでの開催となりました。

JPOPMは、日本におけるインターネット資源のうちIPアドレス、AS番号等の番号資源の管理ポリシーを検討・調整し、コミュニティにおけるコンセンサスを形成するための議論の場です。JPNICとは独立した組織であるJPOPF運営チーム（JPOPF-ST）が主催し、年2回開催されています。

JPOPMのプログラムは、応募のあったポリシー提案や情報提供のプレゼンテーションを中心に構成されます。今回は情報提供が5件ありました。本稿では、プログラムの一部をご紹介します。資料や議事録は、次のWebサイトからご覧ください。

第42回JPNICオープンポリシーミーティング開催のご案内
https://jpopf.net/JPOPM42Program

■ JPNICからの報告

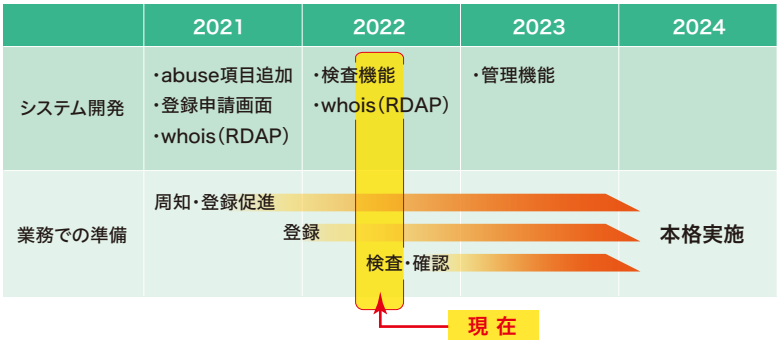
JPNICではポリシーに関することや、JPOPMで議論が行われた内容に関することについて、検討や実装の状況を報告しています。今回、2019年6月に開催されたJPOPM36でコンセンサスとなった『036-01 JPNICにおけるWHOIS正確性向上の検証』について、実装勧告を受けての対応状況について報告を行いました。

JPNICでは、WHOIS正確性向上のための具体的な実装の一つとして、ネットワーク情報、SUBA登録およびAS情報への、ネットワークの不正利用に対応する窓口(Abuse)を登録する機能を開発し、2022年8月22日から実装しました。

IPアドレス管理業務に関するJPNIC文書施行のお知らせ
～移転手続きにおける申請書の統一およびネットワークの不正利用に対応する窓口(Abuse)の登録開始～
https://www.nic.ad.jp/ja/topics/2022/20220822-02.html

今後、ネットワークの不正利用に対応する窓口の登録必須化や、登録されている内容の正確性検査などを順次実装する予定です。JPNICからIPアドレス・AS番号の分配を受けている事業者のみなさまには、ネットワークの不正利用に対応する窓口登録の準備およびご対応をいただけますよう、お願いいたします。

対応の進め方［ ロードマップ ］



2021年度から複数年度に分けて準備

- 登録環境の整備(2021年度、実施済み)
- 登録を促進するための周知活動(2022年度)
- 検査開始と適切な検査手法の調整・検討(2022年度)
- 検査状況の確認など、管理機能の整備(2023年度)

WHOIS正確性向上に関する対応予定

■ インターネットの番号資源管理教室

JPOPF-STメンバーの中川あきら氏が、インターネットの番号資源に関する基礎的な内容を説明するプレゼンテーションを行いました。番号資源について学びたい初心者の方々には、オススメの内容です。また、同じ内容を解説した動画が、JPNICのYouTubeチャンネルにアップロードされています。ご興味のある方はぜひご覧ください。

インターネットの番号資源管理教室
～IPアドレス・AS番号の管理について～
【Internet Week Basic オンデマンド】
https://youtu.be/LA1h6ZF9ZnQ

■ 新しい発信者情報開示制度がワークするために何が必要か

迷惑行為を行った人物の特定にあたり、その発信者情報開示請求の簡易化、迅速化を目的としてプロバイダ責任制限法の改正がなされ、2022年10月より施行されることとなりました。本プログラムでは、そもそものプロバイダ責任制限法と今回の改定内容の説明(一般社団法人インターネットプロバイダ協会 木村孝氏)の後、請求する側の立場としての弁護士(戸田総合法律事務所 中澤佑一氏)、請求を受ける側のCSP(さくらインターネット株式会社 山下健一氏)および請求を受ける側のISP(GMOインターネット株式会社 大場由岐氏、割田太郎氏)から、それぞれの立場での対応状況や懸念点の共有が行われました。

また、発信者の利用プロバイダ特定に利用されるWHOISについて、JPOPMで取り組んできた正確性向上の取り組みについて、JPOPF-STメンバーの鶴巻悟氏から報告が行われました。

■ 次回JPOPM43の開催について

JPOPM43は、2022年12月2日(金)に開催が予定されています。詳細は、JPOPFのWebページで案内されるとともに、IP-USERSメーリングリスト(https://www.nic.ad.jp/ja/profile/ml.html#ipusers)で告知されますのでご確認ください。

第43回JPNICオープンポリシーミーティング開催のご案内
https://www.jpopf.net/JPOPM43Program

今回誌面で取り上げた内容の他に、JPOPM42の開催報告については、次のURLからご覧ください。

第42回JPNICオープンポリシーミーティング報告
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2022/vol1934.html

JANOG50 Meeting「RPKIのROVをいじって考える野良BoF」開催レポート

2022年7月13日（水）～7月15日（金）に、北海道函館市でJANOG50 Meetingが開催されました。JPNICはブース出展や、JPNICスタッフのプログラム登壇、野良BoFの開催などを行いました。

ここでは、「RPKIのROVをいじって考える野良BoF」の様子をご紹介します。現地会場では約30名、オンラインでも約30名と多くの方にご参加いただき、ROVの導入についても参加者も交えながらディスカッションすることができました。

■ ROV導入に関する疑問や検討すべきポイント

ディスカッションタイムでは、参加者も交えてROVの導入に関する疑問や検討すべきポイントについて話し合いました。ディスカッションで出た話題を簡単に紹介したいと思います。

・リスタートすると、ルーティングできるようになるまでに時間がかかるのでは？
→今回のBoFでの模擬環境（80万に近い経路数）でリスタートしてみたところ、通常のBGP機能のリスタートと大きく変わらなかった。

・ROVを導入しても効果がないことがある。どこでROVをするといいのか。
→まずは自ASでの観測は必要である。その上でCDNやDNSなど利用されるサービスを踏まえてトポロジーを見ていく必要もある。
→ROVが行われるといい場所は、必ずしも自ASではない可能性もある。

・ROAキャッシュサーバへの経路が不正経路の影響を受けてしまうことが考えられる。
→キャッシュサーバは自社の環境にあったほうが安心ではある。
→セットアップ自体はDocker利用などで簡略化が可能。ただし、冗長構成や監視を踏まえると実験運用も検討する必要がある。

・Invalid経路の考え方について、dropすると綺麗に落とすことができるが、中身を見ずにdropしてもいいのか？
→以下のような段階的な対応が考えられるので、サービスに応じて検討するといいのではないか。
①Invalid経路をみるだけ
②Local Preferenceを下げる（ベストパスになる可能性を残す）
③Communityの値をセットする（周辺情報などからdrop）
④Invalid経路をすべてdrop

■ ROVの導入効果検証動画

JPNICの模擬環境で行ったROVの効果は、YouTubeで公開しています。不正な経路を流して偽のWebサイトに誘導しているような環境で、BGPルータにROVを導入し不正な経路がdropされる様子をご覧いただけます。ROVの設定やその効果などの概略を知ることができますので、ぜひご覧ください。

【RPKI】ROVで経路をChange
～10分くらいで魅せるROVの効果～
https://youtu.be/l0t2z_Lekzw

今回誌面では割愛したJANOG50 Meetingの参加レポート全文は、JPNICブログをご覧ください。

JANOG50 Meeting 現地参加レポート
https://blog.nic.ad.jp/2022/7746/

「RPKIのROVをいじって考える野良BoF」開催レポート
https://blog.nic.ad.jp/2022/7811/

ネットワークの問い合わせ先検索は、JPNIC WHOISをご利用ください

JPNICは、国別インターネットレジストリ（NIR）として、IPアドレスの登録管理を行っており、JPNICが分配を行ったIPアドレス・AS番号に関する情報を、どなたでも検索することができるWHOISの提供を行っています。

WHOISの検索結果は、当該ネットワーク管理者への問い合わせや、不正利用の通報などの際に参照される場合があります。これに関連し、WHOIS検索に関連してご利用のみなさまにご理解いただきたいことをまとめました。

■ インターネット関連サービスにおけるJPNICの立場

JPNICは、IPアドレス・AS番号を通信事業者等に分配（貸出）を行っていますが、そのIPアドレス等を使ったサービス（ISP等の通信サービス

や、インターネット上のコンテンツサービス）を提供しているわけではありません。

JPNICでは近年、インターネット上の不正行為（迷惑メール送信、不正アクセス、誹謗中傷の書き込みなど）への対応依頼や、IPアドレスの利用者に関する詳細についてのお問い合わせや照会を受けることが多くなってきています。内容を確認すると、JPNICにご連絡いただいても対応することができないものが大半です。そのような依頼や照会に対しては、JPNIC WHOISで改めて検索を行っていただき、連絡先を再度確認いただくようご案内しています。

JPNIC WHOISを活用いただき、実際のネットワーク運用を行っている事業者にご連絡いただきますよう、お願いいたします。

■ JPNICが管理するIPアドレス・AS番号の情報検索には、JPNICのWHOISで検索してください

検索サイトで「IPアドレス検索」と検索すると、JPNICのWHOIS以外にも、さまざまなサイトが出てきます。しかしながら、JPNICでは、JPNIC以外が提供しているIPアドレス・AS番号に関する情報検索について、その内容や検索結果に関与しておらず、正確性を保証いたしません。あらかじめご了承ください。

■ APNIC WHOISを検索した場合について

APNIC WHOISを検索した場合、JPNICが分配したIPアドレスの情報について、その一部が検索結果に表示されます。また、JPNICの情報も検索結果に表示されます。これは、検索されたIPアドレスの分配がJPNICを通じて行われているからです。

APNIC WHOISの検索結果に基づき、インターネット上の不正行為への対応依頼をJPNICに送られるケースが多くございますが、「インターネット関連サービスにおけるJPNICの立場」で説明したとおり、対応することができません。この場合も、JPNIC WHOISの検索を行っていただき、該当のネットワーク管理者に連絡いただくようお願いしています。

JPNIC以外のサイトでIPアドレスを検索した場合、APNIC WHOISの検索結果が引用されることがあるようです。

今回誌面では割愛した内容を含む全文は、JPNICブログをご覧ください。

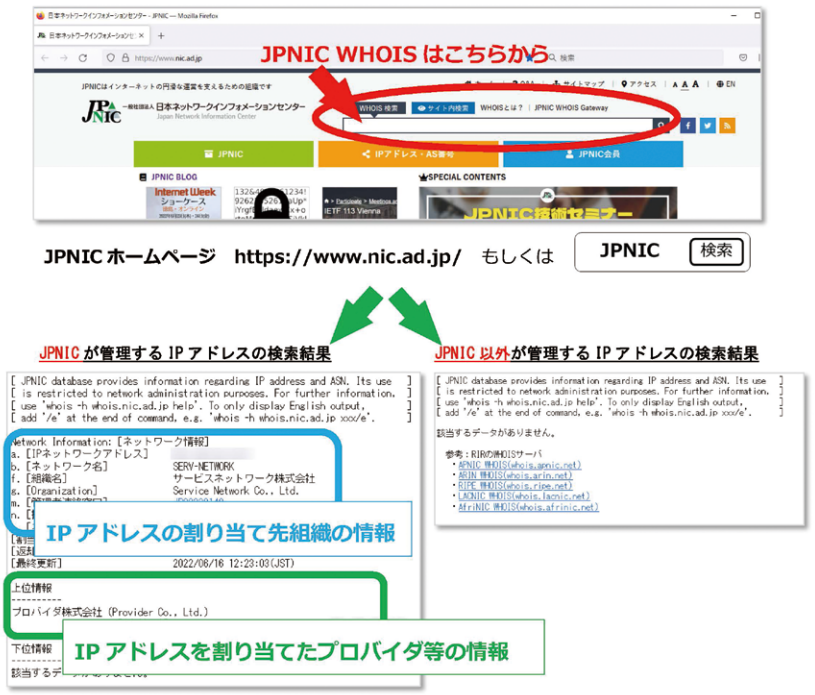
インターネットの健全な運用を支える立場として、インターネット情報の不正利用や犯罪行為への対応は、重要な課題と考えています。JPNIC WHOISの提供を通じて、速やかな問題解決に貢献できるよう、引き続き取り組んでまいります。

ネットワークの問い合わせ先検索は、JPNIC WHOISをご利用ください
https://blog.nic.ad.jp/2022/7861/

IPアドレスは JPNIC WHOISでの 検索をお願いします

私どもは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）では、APNIC（Asia Pacific Network Information Centre）およびJPNIC以外で提供されているIPアドレス、AS番号に関する情報については一切関知いたしておりません。それらの情報を基づいた問い合わせや照会には、原則として対応いたしかねます。あらかじめご了承ください。

IPアドレス、AS番号に関する情報は、JPNIC WHOISでの検索をお願いします。



※連絡先の詳細は検索画面中のリンクを選択してご確認をお願いします

技術トピック

INTERNET TRENDS INTRODUCTION

3

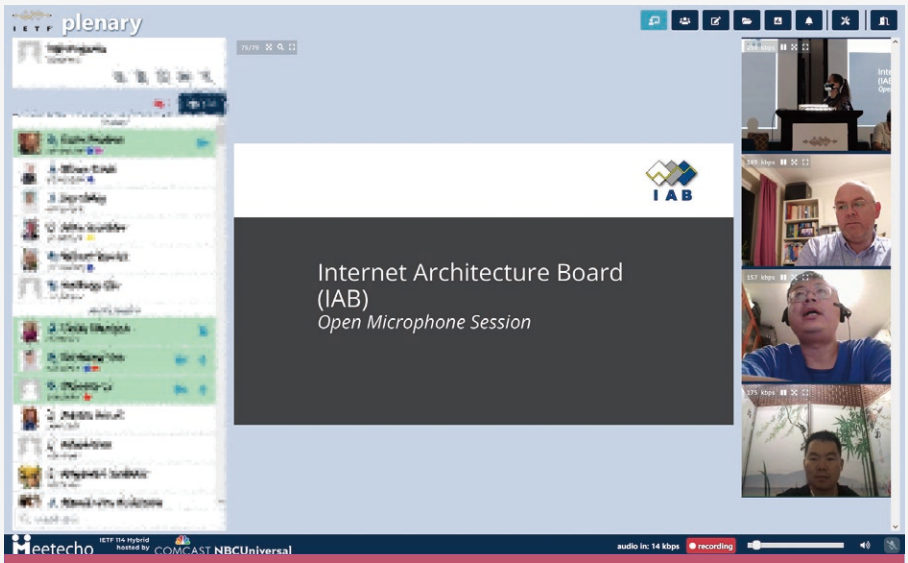
2022. 7.23 ▸ 7.29　アメリカ／フィラデルフィア　IETF 114　オンライン

2022年7月23日（土）から29日（金）にかけて、第114回IETF（IETF 114）がフィラデルフィアで開催されました。このIETF 114についてホットトピックをお伝えします。

第114回IETFミーティング

IETF 114は、米国・フィラデルフィアの会場とオンラインでの、ハイブリッド開催となりました。前回に続いて参加者は1,400名を超えています。日本からの参加者は、オンライン43名、現地参加4名、合計47名で、前回の54名と比べて減少しています。

今回の全体会議で、2023年3月25日（土）から3月31日（金）にかけて行われる第116回IETFミーティングは、日本の横浜で開催されることが発表されました。発表された時に会場では拍手が起こり、会場にいる参加者の日本開催への期待が感じられました。



全体会議におけるIABに関する議論の様子

■ IABの動向

IAB（Internet Architecture Board）では、他の標準化団体との協力を行う二つの”サポートグループ”が作られました。

○ IETF-IEEEグループ

米国電気電子学会（IEEE）のプロジェクト802との協力のためのグループです。RFC7241に記載されています。

○ IAB-ISOCポリシーコーディネーショングループ

IAB、ISOCのインターネットにおけるポリシーに関連する活動の情報共有と、協力のためのグループです。

IABでは2022年10月17日（月）から10月21日（金）に、「暗号技術を使ったネットワークにおける管理手法」（Management Techniques in Encrypted Network- M-TEN）ワークショップが開催されました。

IAB workshop on Management Techniques in Encrypted Networks (M-TEN), 2022
https://www.iab.org/activities/workshops/m-ten/

■ Hot RFC

Hot RFC（Request for Conversation）は、IETFにおける活動紹介などが行われるセッションです。今回もさまざまな活動が紹介されていました。発表タイトル訳とURLを紹介します。

○ エネルギー問題に対してこれまでにIETFができたことは何か（What has the IETF ever done for Energy）

トレス・エカート（Toerless Eckert）

詳細:
https://github.com/toerless/energy/raw/main/what-has-the-ietf-ever-done-for-energy.pdf

消費エネルギーを低減させることとサステイナブルなエネルギー利用、そして6LOWPAN等の低エネルギーネットワークに関する

取り組みをまとめ、エネルギー消費に対する意識を広めることを目的とした活動。

○ **グリーン・ネットワークの課題と可能性（Challenges and Opportunities in Green Networking）**
アレクサンダー・クレム（Alexander Clemm）

詳細:
https://datatracker.ietf.org/doc/html/draft-cx-green-metrics-00

二酸化炭素排出量の削減をテーマに、ネットワーク技術自体を「環境にやさしい」ものにする検討。電力消費量の削減のための可視化を提案する。

○ **ネットワークとプロトコルのための耐量子暗号における課題と可能性（Challenges and Opportunities in Post-Quantum Cryptography for networks and protocols）**
ソフィア・セリ（Sofia Celi）

詳細:
https://datatracker.ietf.org/doc/slides-114-hotrfc-sessa-challenges-and-opportunities-in-post-quantum-cryptography-for-networks-and-protocols/

NISTで行われた耐量子暗号の選定プロセスが、最初のマイルストーンに達した。現在利用されているTLS、DNSSEC、IPsecといったプロトコルへの影響と、移行に関わる課題を示す。

○ **セキュア・エレメントのインターネット（Internet Of Secure Elements）**
パスカル・ウリエン（Pascal Urien）

詳細:
https://datatracker.ietf.org/doc/draft-urien-coinrg-iose/05/

“セキュア・エレメント”は、銀行のキャッシュカード、SIM、電子パスポートなどで使われている。実装としてはJavaカードがあり、60億枚以上使われているとされる。セキュア・エレメントをTLSサーバで使うためのInternet-Draftの紹介。

○ **TLSにおけるアテステーション（Attestation within TLS）**
ハネス・ショフェニグ（Hannes Tschofenig）

詳細:
https://datatracker.ietf.org/doc/html/draft-fossati-tls-attestation-00

ネットワークを使ってセキュアな機能提供を行うアテステーション（証明）の方式を、TLSを使って提供できるようにするための提案。

○ **未来のインターネットのためのインフラ、衛星ネットワークLEO（The LEO satellite networking, the flying infrastructure for future Internet.）**
リン・ハン（Lin Han）

詳細:
https://datatracker.ietf.org/doc/slides-114-hotrfc-sessa-the-leo-satellite-networking-lin-han/

NTN(Non-Terrestrial Network – 非地上系ネットワーク)、衛星のネットワークにおける、IPのネットワークを提案。次回のIETF 115でサイドミーティングを開催する予定。

○ **エンド間のセキュリティを超えて（Beyond End-to-End security）**
フィリップ・ハラム-ベイカー（Phillip Hallam-Baker）

詳細:
https://datatracker.ietf.org/doc/slides-114-hotrfc-sessa-beyond-end-to-end-security-phillip-hallam-baker/

現在のプロトコルは、エンド間の通信データを暗号化するなどによりセキュアになるとされる。しかし、その通信には通信相手の識別子を得るために第三者が介在する。エンド間に留まらない仕組みMathematical Mesh（数学的メッシュ）の提案。

■ ピックアップ

DANE（DNS-Based Authentication of Named Entities）の話題をピックアップして紹介します。

○ **DANE Portal, IEPGミーティングより**

DANE Portal※1は、S/MIMEの公開鍵を登録・検索のできる有志によるWebサービスです。Thunderbirdのようなメールクライアントで、送信相手のメールアドレスを元に証明書を検索することができます。Webの“HTTPS everywhere”のように、電子メールのS/MIMEが使われるようになることをめざしている、とされています※2。

DANEはなかなか普及していかないプロトコルであるような声がありますが、このような仕組みの登場によって変わっていくかもしれません。

IEPG(Internet Engineering and Planning Group)ミーティング※3は、IETFミーティングの前日に登録なしで参加できる非公式の会合で、運用や研究といったさまざまな観点で発表が行われます。

※1 https://daneportal.net/
※2 IEPGミーティングにおいてDANE Portalが紹介されたスライドKurer and DANEportal.net https://iepg.org/2022-07-24-ietf114/slides-114-iepg-sessa-kurer-and-daneportalnet-00.pdf
※3 The IEPG, https://iepg.org/

グリー株式会社後藤ひろゆき氏より、QUICおよびHTTPに関する動向についてご報告いただきました。

IETF 114における各ワーキンググループ(WG)の会議については、変わらずプロトコルの議論が行われています。既存のプロトコルのメンテナンスについて議論するもの、新しいプロトコルを議論するもの、それぞれ議論のフェーズは異なっていますが、今回は私の参加したQUIC WGの様子を紹介していきます。

■ QUIC WG

QUIC WGでは、去年QUIC Version 1をRFC 9000※4として発行しました。さらに、QUICと合わせて標準化が進められていた待望のHTTP/3も、RFC 9114※5として発行が完了しています。HTTP/3については、その後の拡張やメンテナンスはHTTP WGで行われることとなっています。引き続きQUIC WGとしては、QUICプロトコルのメンテナンスと拡張について議論を続けています。

QUIC Version 1の標準化後に行われた、いくつかの取り組みを紹介します。まずは、「RFC 9221 An Unreliable Datagram Extension to QUIC」※6、「RFC 9287 Greasing the QUIC Bit」※7を取り上げたいと思います。RFC 9221は、QUICで信頼性のないアプリケーションデータの送信を可能にします。もともとQUICでは、パケットロストして失われたアプリケーションデータは再送されますが、それが不要なユースケースでこの拡張仕様は有用です。RFC 9287では、QUICにはQUIC Bitと呼ばれるQUICの通信だと識別するのに使えるbitがありますが、それを分かりづらくする方法を定義します。これにより、ミドルウェアの不適切な実装により新しいプロトコルの通信が阻害される、"硬直化"のリスクを減らします。

RFC目前になっている仕様としては、QUICv2などもあります。これは機能的にはQUICv1と同じですが、鍵導出に用いるパラメータなどが異なっています。実装が適切にパラメータを変えたり、バージョンのネゴシエーションを行うために、QUICv2というプロトコルが用意されました。これにより、将来の新しいQUICバージョンを標準化する際のリスクを低減しています。

IETF 114では続き物の議論もありますが、「Multipath QUIC」※8や「Multicast QUIC」※9といった、新しいQUIC拡張の議論が行われています。「Multipath QUIC」は、Multipath TCPのように複数のパス(エンドポイントにとっては複数のネットワークインタフェース)を使って、コネクションを確立する仕組みを定義します。モバイル端末では、Wi-Fiとキャリアネットワーク両方を使う例や、サーバ間の通信でも複数回線を使うユースケースがあります。現在は、QUICにおいてパスごとの再送制御を行うために、パケット番号の付与方式を議論しています。また、「Multicast QUIC」は、マルチキャストでデータを送信できるようにする提案仕様です。まだWGドキュメントにはなっていませんが、著者らによってここ数年議論されてきたテーマになります。まだまだ議論が始まったばかりですが、興味を持っているメンバーで議論が続けられるでしょう。

■ HTTP WG

HTTP WGは、引き続きHTTPのメンテナンスおよび拡張を行っています。特に最近は、HTTP/3の標準化に合わせてHTTP全般のメンテナンスが行われてきました。HTTP/3は、HTTPメッセージのやり取りを効率化するプロトコルでしたが、HTTPメッセージの意味は変わりません。今までHTTPメッセージの意味は、HTTP/1.1の仕様の一部として標準化されていましたが、独立したHTTPセマンティクス仕様として、別途切り出し整理されました。それが、「RFC 9110 HTTPSemantics」※10です。また、HTTPセマンティクスの整理に合わせて、HTTP/1.1やHTTP/2のエラッタ修正も含め、RFCが合わせて改訂されています。

IETFの本会合がリモート中心となり、HTTP WGはこの2年間は個別開催の中間会議のみを行っていました。IETF 114ではハイブリッド開催となり、現地での参加者も見込まれることから、本会合でのミーティングが久々に開催されました。とはいえ、今まで通り粛々と取り組みが進められているという印象で、特に変わったことはありませんでした。

IETF 114で議論されたトピックのうち、「alt-svc」を紹介します。「alt-svc」は、すでに標準化されている仕組みですが、利用用途の拡大に伴い議論が盛り上がっています。alt-svcの用途例としては、クライアントに対してサーバのHTTP/3対応をHTTPレスポンスヘッダで通知するのに使われています。クライアントはこのヘッダを見て、HTTP/3でサーバに繋ぎにいきます。このalt-svcの仕組みは現状上手くいっていますが、複数のCDNを使う場合や、新しくHTTPS DNSレコードでシグナリングを行う場合など、ユースケースや利用手段が拡大しています。現状に合わせて整理しようという動きがあります。

※4 https://datatracker.ietf.org/doc/html/rfc9000
※5 https://datatracker.ietf.org/doc/html/rfc9114
※6 https://datatracker.ietf.org/doc/html/rfc9221
※7 https://datatracker.ietf.org/doc/html/rfc9287
※8 https://www.ietf.org/archive/id/draft-ietf-quic-multipath-02.html
※9 https://www.ietf.org/archive/id/draft-jholland-quic-multicast-02.html
※10 https://www.rfc-editor.org/rfc/rfc9110.html

ドメイン名・ガバナンス

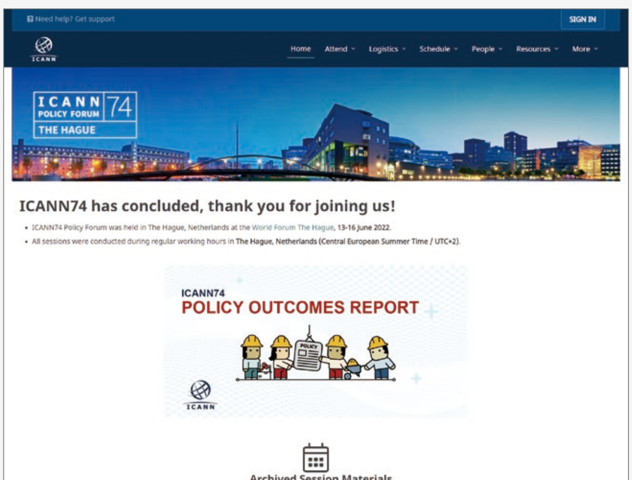
4

2022. 6.13 ▸ 6.16 オランダ／ハーグ　第74回ICANN会議　オンライン

本稿では、2022年5月～2022年9月にかけての、ドメイン名およびインターネットガバナンスに関する動向として、第74回ICANN（The Internet Corporation for Assigned Names and Numbers）会議やインターネットガバナンスに関連した動きと、JPNICからお知らせしたドメイン名のドロップキャッチやうっかり失効に関する注意喚起の記事などをご紹介します。

第74回ICANN会議

第74回ICANN会議（以下、ICANN74）は、2022年6月13日（月）から16日（木）まで、オランダ・ハーグとオンラインのハイブリッド形式で開催されました。現地会場が設定されるのは、新型コロナウイルス感染症のパンデミック以来では初となり、101の国・地域より1,817名の参加がありました。本稿では、主にプレナリーセッションと分野別ドメイン名支持組織（Generic Names Supporting Organization, GNSO）に関する動向についてお伝えします。



ICANN74では、久々に現地会場も設定されたハイブリッド開催となりました

■ プレナリーセッション

○ICANNの優先順位は誰が設定するのか

ICANNでは、誰が優先順位を設定し、何を優先順位とするのかが明確でないことに懸念が高まっていました。ICANNコミュニティとICANN理事会およびICANN org（事務局）との話し合いは継続されていましたが、さまざまなICANNコミュニティグループが、異なる解釈で異なる優先順位を主張しているというリスクが認識されていました。本セッションでは、2017年のICANN 59における同名セッションでの議論や、その後の変化をカバーした上で、文書化可能な優先事項を特定することをめざして議論されました。ICANN orgのXavier Calvez氏はセッション中に、今後コミュニティからの意見募集の機会を設ける予定と発言しています。

○地政学、立法、および規制の策定に関する討論

本セッションでは、ICANNを取り巻く状況について、政府や政府間組織（IGO）によるDNSへの注目の高まりといった課題、ICANNのエコシステムへの影響、その軽減策が共有されたのち、以下のIGOの状況がICANN orgの政府エンゲージメント部門（GE）より共有されました。

・2022年の国際電気通信連合（ITU）
・国連総会委員会審議（両委員会とも情報通信関連のセキュリティを対象）
・欧州評議会（Council of Europe, CoE）
・経済協力開発機構（OECD）

次いで、各国で検討されている、もしくは立法された法律についてGEから紹介がありました。

・中国サイバーセキュリティ法、データセキュリティ法（PIPL）
・ロシア個人情報保護法
・「インドIT法2000」の改正
・米国サイバーインシデント通知法
・有害コンテンツ対策にDNSブロッキングを活用できる可能性がある、オンラインでの安全性に関するカナダの議論
・EUのデジタルサービス法（DSA）
・EUの工芸品および工業製品（Craft and Industrial, CI）向け地理的表示（Geographical Indication, GI）保護規則案

■ gTLD関係

ICANN 74で開催されたセッションのうち、注目すべきと思われるものの状況を記載します。単一セッションとは限らず、複数のセッションをまとめている場合もあります。

○EPDPフェーズ2（SSAD）

GNSO評議会を支援するために、関心のある理事会およびEPDPフェーズ2メンバー（GNSO、ALAC、GAC、SSAC）から構成される、EPDP-TempSpecフェーズ2小チームが設立されました。小チームは予備報告書を提出し、仮定を評価・テストするためのツールとしての「概念実証」を推奨しました。GNSO評議会は、ICANN理事会に対し、SSAD勧告の検討を一旦停止し、ICANN orgに「軽量版SSAD」の設計コンセプトの策定を依頼することを推奨しました。

ICANN orgはこのセッションで、「軽量版SSAD」をWHOIS Disclosure Systemという名称で提案しました。その取り組み方は次の通りです。

・既存のICANNリソースを利用
・開発および立ち上げにかかる時間を短縮
・既存または類似のユーザーインタフェースの再利用により、すべてのユーザーが取り入れやすくする

○排他的一般名詞（Closed Generic）TLD

ICANN 72以降毎回開催されてきた、本件に関するAt-Largeのポリシー・セッションにて、構想文書によって組み立てられたGNSOとGAC間での議論の提案、およびGNSO評議会の小チームによる検討内容の報告、などが行われました。

○DNS Abuse

ICANNの報告によれば、DNSの不正利用（主に迷惑メール）もマルウェア、フィッシング、ボットネットも、減少傾向にあることが示されました。ccNSOでは、セッション：DNS AbuseにおけるccTLDの役割が開催され、.HK（香港）からの共有がありました。ICANN外でレジストリ・レジストラが立ち上げた、DNS Abuse Instituteからは、NetBeacon（DNSの不正利用報告サービス）の立ち上げについて報告されました。

GNSO評議会の小チームは、gTLDポリシー策定を通じて特に対処すべきDNS不正利用関連の問題があるかどうかを検討することを任務としています。ICANN 74のセッションで、本チームは作業の進捗に関する最新情報を提供し、審議を継続しました。

○移転ポリシーの見直し

2021年2月にGNSO評議会はポリシーを見直すPDPを開始することを決議し、翌3月にその作業を行う作業部会（WG）のチャーターを承認しました。WGの使命は、「登録機関間および登録者間の移転の容易性、安全性および有効性を向上させるために、移転ポリシーの見直しを行い、ポリシーの変更が必要であるかどうかを決定する」こととなっています。今回のセッションでは、登録者変更の要求事項に焦点を当てる、フェーズ1Bについて主に共有されました。

○EPDP-IDNs

GNSO評議会は、国際化ドメイン名に関するEPDP-IDN（Expedited PDP on Internationalized Domain Names）を開始し、次の2点について政策提言を行いました。

・すべてのトップレベルドメイン（TLD）の定義と、ルートゾーンの異体字gTLDの委譲を促進するための異体字ラベルの管理
・IDN実装ガイドラインを将来どのように更新すべきか

EPDP-IDNsは、そのチャーター質問の半分近くについて、第1段階の審議をほぼ終了しています。ICANN 74の期間中、チームは二つのセッションを開催しました。最初のセッションでは、予備勧告案のプレビューや未解決項目の注意喚起を含む進捗状況のアップデートが行われました。2番目のセッションでは、ICANN orgがIDNテーブルとセカンドレベルでのIDN実装について発表しました。レジストリとレジストラのメンバーも、それぞれの会社でIDNテーブルがどのように実装されているかについて、経験を共有しました。

■ 第64回ICANN報告会

第74回ICANN会議での議論を紹介する報告会を、2022年7月28日（木）に、オンラインにて開催いたしました。当日のプログラムは次の通りです。

1. ICANN74会議概要報告
2. 国コードドメイン名支持組織（ccNSO）関連報告
3. ICANN政府諮問委員会（GAC）報告
4. ルートDNSサーバーシステムに関する報告（RSSAC及びRSS GWG）
5. 日本語ルートゾーンLGRに関する報告
6. GNSOレジストリ・レジストラ部会報告
7. 次期新gTLD申請手続きポリシー検討状況報告
8. ICANN理事からの報告

第64回ICANN報告会の資料と動画は次のURLで公開していますので、本稿と併せてぜひご覧ください。

第64回ICANN報告会
https://www.nic.ad.jp/ja/materials/icann-report/20220728-ICANN/

■ 第75回ICANN会議

次回ICANN75は、2022年9月17日（土）～22日（木）の日程で、マレーシア・クアラルンプールでの現地開催ありのハイブリッド形式で開催されました。この会議の内容は、次号83号でご紹介いたします。

なお、今回ご紹介した第74回ICANN会議のさらに詳細なレポートは、JPNIC Webでご覧いただけます。詳しくは次のURLをご覧ください。

第74回ICANN会議報告
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2022/vol1932.html

制裁がインターネット基盤運営に及ぼす影響

ロシアのウクライナ侵攻が始まって以来、こういった国際紛争がインターネット基盤運営に及ぼす影響を、JPNICでもブログ記事などで公開しています。

ウクライナ侵攻とインターネット
https://blog.nic.ad.jp/2022/7359/

スプリンターネットに抗うインターネット
https://blog.nic.ad.jp/2022/7495/

また、国際大学GLOCOM六本木会議（2022年6月7日開催）やJANOG50（同7月14日開催）など、国内のカンファレンスでこのような話題を取り扱うことも増えてきました。これらにおいて、インターネット基盤運営はグローバルなインターネットコミュニティの自治に委ねられており、国の影響を基本的に受けない、という説明をしてきているのですが、本稿では例外的に影響を受ける場合もある、というお話をしたいと思います。

まず最初に、RIPE NCCが2021年11月にRIPE Labsというブログページで公表した記事です。

How Sanctions Affect the RIPE NCC
（制裁はどのようにRIPE NCCに影響するのか）
https://labs.ripe.net/author/athina/how-sanctions-affect-the-ripe-ncc/

これはRIPE NCCの最高法務責任者であるAthina Fragkouliによる記事で、欧州連合における制裁実施がRIPE NCCによるIPアドレス管理の業務に与えていることが解説されています。Legal Contextのセクションを抄訳します。

・RIPE NCCはオランダ法に基づく社団であり、オランダとEUによる規制下にある。EUのものを含め規制を実施するのはオランダ政府である。
・特定国への特定製品、役務の提供が禁じられているが、RIPE NCCのサービスには該当がない。
・一方で、特定の個人や法人に向けた、経済資源（economic resource）や資金を凍結すること、経済資源や資金を提供することの禁止には影響を受けることになった。
・IPアドレスの登録が経済資源と認定されたからである。
・これによって、制裁対象となっているごく限られた個人や法人に対して、新規のIPアドレス登録ができなくなった。

続いて、Discussions with the Dutch Authoritiesではオランダ政府当局との制裁規定適用に関する議論が紹介されており、すでに登録されているIPアドレスの登録削除までは不要と結論されていることが示されています。

文中でたびたび示されていますが、RIPE NCCはオランダ法による社団である以上、EUやオランダの法に従う必要が当然あり、それはNCCの事業運営上、最重要課題であると位置付けています。その上で、遵法性を維持する上での細かな確認を当局と行うとともに、IPアドレスの提供という事業の目的が最大限維持されるように、配慮に余念がないことがわかります。

さらに、2022年9月5日には、RIPE NCCでグローバルエンゲージメントを統括するChris Buckridge名で、この続編とも言える記事が公開されました。

Towards a Sanctions Solution Space
（制裁の対処策検討の場に向けて）
https://labs.ripe.net/author/chrisb/towards-a-sanctions-solution-space/

この記事では、制裁がインターネット基盤運営に与えるインパクトを分析、記録することを目的とするプロジェクトに、RIPE NCCが資金拠出していることが示されています。RIPE NCCの意図としては、このような活動を通じて、制裁とインターネット基盤運営の関係を見つめなおし、その輪を拡げていくことで本件に関する理解を増進して、政府においても、的確な、インターネット基盤運営に不必要な悪影響を及ぼさない政策検討につながることをめざしているようです。これはまさに、さまざまなステークホルダーによって運営されるインターネットの、問題解決の進め方とも言えます。

サイバー主権、ITU、インターネット

インターネットガバナンスの文脈で耳にする「サイバー主権」という言葉に関連して、最近注目を集めている「China's War for Control of Global Internet Governance」というペーパーや、2022年9月のITU全権委員会議における事務総長選挙について、JPNICブログでご紹介しています。詳しくは、次の記事をご覧ください。

サイバー主権、ITU、インターネット
https://blog.nic.ad.jp/2022/7803/

ドメイン名のうっかり失効やドロップキャッチとその対策について

ドメイン名に関連するお困りごととしてJPNICにお問い合わせをいただくことが多い、ドメイン名の登録期限切れと、手放したドメイン名の第三者による再登録について、それが起こる状況と取り得る対策について、JPNICのメールマガジンでご紹介しています。独自ドメイン名の登録・利用をされている場合には、ぜひご注意いただきたい内容となりますのでご一読ください。

登録期限切れや手放したドメイン名にご注意！
～うっかり失効やドロップキャッチとその対策～
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2022/vol1940.html

JPNIC Activity Diary

JPNIC 活動ダイアリー

2022年7月 ～ 2022年11月 JPNIC活動報告

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

2022年7月

1 2 3 4 5 6 7 8 9 10 **11** 12 13 14 15 16 17 18 19 20 21 **22** 23 24 25 26 27 **28** 29 30 31

11（月） オンライン

IGF 2023に向けた国内IGF活動活発化チーム 第21回会合（オンライン）

https://www.nic.ad.jp/ja/materials/igf/20220711/

22（金） オンライン

JPNICトークラウンジ第8回（オンライン）

インターネットガバナンス推進に関して、国内で最初に名前の挙がるリーダーであり、現在は「IGF2023に向けた国内IGF活動活発化チーム」のチェアでもいらっしゃる加藤 幹之さんに、今までのインターネットガバナンスの流れを踏まえた上で、日本開催となるIGF2023や、今後の国内IGF活動にかける想いをうかがいました。

28（木） オンライン

第64回ICANN報告会（オンライン）

第64回ICANN報告会はオンラインで開催され、ICANN74の会議概要に始まってCCNSO、GAC、RSSAC、日本語ルートゾーンLGR、GNSOレジストリ・レジストラ部会、次期新gTLDに関して報告が行われました。

関連記事 P.23 ドメイン名・ガバナンス

https://www.nic.ad.jp/ja/materials/icann-report/20220728-ICANN/

2022年8月

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 **22** 23 24 25 26 27 28 29 30 **31**

1（月） オンライン

IGF 2023に向けた国内IGF活動活発化チーム第22回会合（オンライン）

https://www.nic.ad.jp/ja/materials/igf/20220801/

22（月） オンライン

IGF 2023に向けた国内IGF活動活発化チーム第23回会合（オンライン）

https://www.nic.ad.jp/ja/materials/igf/20220822/

31（水） オンライン

RPKIハンズオン ～ROVを体験／JANOG50野良BoFキャッチアップ～（オンライン）

JANOG50で行われた「RPKIのROVをいじって考える野良BoF」でのデモ動作を、リモートのハンズオン形式で参加者の皆さまにご体験いただきました。

https://youtu.be/l0t2z_Lekzw

2022年9月

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

1（木） オンライン 第31回JPNIC評議委員会（オンライン）

https://www.nic.ad.jp/ja/materials/council/2022/0901/

2（金） オンライン IETF 114報告会（オンライン）

IETF 114の議題から、NTP、セキュリティなどを中心とした報告が行われました。珍しいところでは、リモートで参加した学生からの、参加報告も行われています。

関連記事 P.20 技術トピック

https://www.nic.ad.jp/ja/topics/2022/20220822-01.html

16（金） オンライン IGF 2023に向けた国内IGF活動活発化チーム第24回会合（オンライン）

https://www.nic.ad.jp/ja/materials/igf/20220916/

2022年10月

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

3（月） オンライン IGF 2023に向けた国内IGF活動活発化チーム第25回会合（オンライン）

https://www.nic.ad.jp/ja/materials/igf/20221003/

3（月）▶7（金） オンライン JPNIC技術セミナー（オンライン）

2022年10月開催の技術セミナーは、IPv6、DNS、セキュリティ、PKIの座学と、RPKIとDNSSECのハンズオンを開催しました。普及に向けてDNSSECのハンズオンは無料化されています。

https://www.nic.ad.jp/ja/tech/seminar/

20（木） オンライン 第65回ICANN報告会（オンライン）

https://www.nic.ad.jp/ja/materials/icann-report/20221020-ICANN/

2022年11月

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

21（月）▶30（水） 東京 オンライン Internet Week 2022

（東京大学伊藤謝恩ホール+オンライン）

2022年のInternet Weekは、21日から25日までをオンラインWeekとして、28日から30日をハイブリッドWeekとして開催することになりました。オンサイトでの開催は3年ぶりです。

関連記事 P.2 特集1 Internet Week 2022

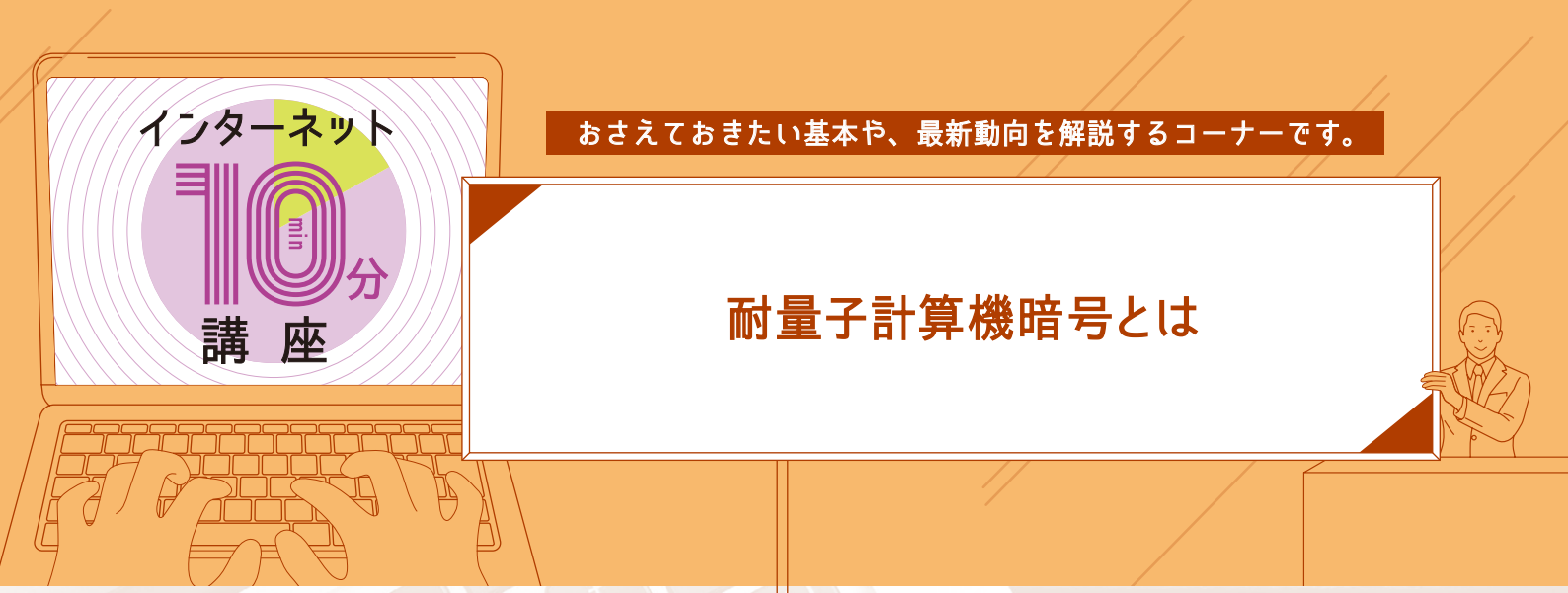
https://www.nic.ad.jp/iw2022/

協賛・後援したイベント

2022年10月4日(火)～7日(金)、13日(木)	Security Days Fall 2022	2022年7月13日(水)～15日(金)	JANOG50
		2022年11月7日(月)～8日(火)	第22回迷惑メール対策カンファレンス

これからのJPNIC活動予定

□ 2023年3月 第72回総会（臨時） など



おさえておきたい基本や、最新動向を解説するコーナーです。

耐量子計算機暗号とは

1 はじめに

量子計算機は、現代の社会において最重要と言って差し支えない研究領域である。本稿は前号（No.81）のインターネット10分講座「暗号技術から見る量子計算機のいま」の続きであり、前回の講座では、量子計算機が実用化された際にはRSA暗号など従来の暗号技術が使えなくなること、また、量子計算機の研究がどのような現状にあるかを紹介した。本稿では、量子計算機が実用化されたあとでも、安全性を保証する技術として注目されている「耐量子計算機暗号」の現状を解説する。前号同様に耐量子計算機暗号について数式を出さずに現状のみを説明するため、詳細を知りたい方は各所で引用している文献・記事を参照されたい。

2 耐量子計算機暗号とは

まず、耐量子計算機暗号の概念について述べたい。耐量子計算機暗号は、一般に「量子計算機が実用化されても、安全性を保つことができる暗号技術」として知られている。厳密には、耐量子計算機暗号は「量子計算機にも安全性が示されている」暗号ではなく、「量子計算機による効率的な解析方法が知られていない」暗号となる。前号では、「ショア（Shor）のアルゴリズム」により、現在の暗号技術が効率的に解かれてしまうことは述べた。ショアのアルゴリズムは、本稿執筆時点ではまだ現実的な脅威とはなっていないものの、暗号技術の本来の役割に鑑みると、安全性が損なわれる前に対策がなされることが望ましい。

詳細は次節で述べるが、耐量子計算機暗号は、その安全性の根拠となる問題に基づいて分類される。興味深い点は、いくつかの代表的な方式は、ショアのアルゴリズムが発見された1994年よりも前に提案されていることである。これらの方式は、公開鍵暗号の概念が初めて登場した1974年から、公開鍵暗号の具体的な構成を求める中で提案されてきた。一方、現在最も発展している暗号技術は、ショアのアルゴリズムが登場した以降の1997年に提案された、格子暗号と呼ばれる方式である。以降では、これらの暗号方式について、全体像を説明する。なお、耐量子計算機暗号の基礎知識については九州大学・縫田光司先生の書籍「耐量子計算機暗号」[※1]が日本語での専門書として出版されている。

※1　縫田光司, “耐量子計算機暗号,” 森北出版, 2020.

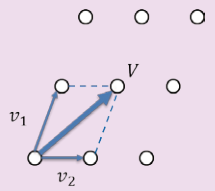
3 耐量子計算機暗号の代表的な枠組み

前述した通り、耐量子計算機暗号は安全性の根拠となる問題に基づいて提案されている。既存の主な方式は格子暗号、符号ベース暗号、多変数公開鍵暗号、同種写像暗号の四つである。以下では、最も発展している暗号技術として格子暗号の詳細を述べる。符号ベース暗号、多変数多項式暗号、同種写像暗号については概要のみを述べる。

3-1 格子暗号

格子暗号は、高次元の格子に基づく公開鍵暗号技術である。格子暗号は、耐量子計算機暗号としての有望さが最も期待される暗号技術であり、量子計算機に対して安全であることに加えて、さまざまな利点を有している。ここで言う格子とは大まかには、実数上に定義される一次独立なベクトルによって表される集合として定義される。また、そのベクトルを基底と呼び、各基底が持つ要素数を次元、基底の数を階数と呼ぶ。これだけだと何だかよくわからない読者が多いと思うので、図1に例を示す。図1で表される全体が格子であり、図中のベクトルv_1,v_2が基底となる。また、図1では次元と階数はいずれも2となる。格子暗号で最もよく知られる問題である最短ベクトル問題(Shortest Vector Problem, SVP)は、格子の基底v_1,v_2が与えられた状態で、そこから計算される最短ベクトルVを計算する問題である。図の例は2次元ベクトルであるため簡単に思われるが、これらのベクトルが存在する空間が3次元あるいはより高次元になった場合、および、基底の数を増やした場合をそれぞれ考えてもらいたい。この時、さまざまな方面を向いた多数のベクトルが散見される状態となり、最短ベクトルの計算が複雑になることが想像できるだろう。この難しさが格子暗号の安全性の根拠となる。

図1 格子とその基底の例



興味深いことに、格子暗号は量子計算機に対する安全性を持つことに加え、二つの利点を持つ。まず、従来の暗号技術よりも高機能な暗号技術の実現が可能な点である。その代表的な例が準同型暗号と呼ばれる、暗号文に対する何らかの操作によって復号することなく、中身の平文に対する操作が行える暗号技術である。準同型暗号は、データの秘匿性を満たしたままデータ操作が可能な技術として、昨今ではデータ提供者のプライバシーを保障したAIの学習機能などへの応用が期待されている。公開鍵暗号の歴史としては、暗号文の操作から平文の積あるいは和を計算できる方式が知られていたが、平文の和と積の両方を実現する準同型暗号、あるいは、平文に対する任意の関数を計算できる準同型暗号(完全準同型暗号と呼ばれる)は、公開鍵暗号が登場した1970年代から未解決問題として知られていた。この30余年の未解決問題が、2009年にクレイグ・ジェントリーによって解決された[※2]。このジェントリーの方式はもちろん、既存の完全準同型暗号は格子に基づいている。直観的には、従来の暗号が剰余演算による整数であることに対し、ベクトルとして定義される高次元の数学的概念を導入したことで、より複雑な計算が可能になったと言える。もう一つの利点は、高速性にある。実は、格子暗号はRSAや楕円曲線に代表される暗号技術より高速である。一つの例として、格子暗号の実装結果[※3]を表1に示す。文献[※4]の著者らは格子暗号のライブラリを開発し、RSAおよびECDHとその性能を比較評価している。表に示す通り、格子暗号は従来の暗号技術と比べて100倍以上の高速性を持つ。すなわち、格子暗号の実装を推し進めることは理論的な安全性に加えて、スループットの改善という実用面からも有益と言える。

表1 格子暗号のベンチマーク:鍵交換回数毎秒 [※3]

方式	128 bit	256 bit
RSA	310回／秒	—
ECDH	5,930回／秒	1,610回／秒
格子	1,020,000回／秒	508,000回／秒

※2 Craig Gentry, "Fully homomorphic encryption using ideal lattices," STOC 2009, pp.169–178, 2009.
※3 Carlos Aguilar-Melchor, Joris Barrier, Serge Guelton, Adrien Guinet, Marc-Olivier Killijian, Tancrede Lepoint, "NFLlib: NTT-Based Fast Lattice Library," CT-RSA 2016, pp. 341-356, 2016.
※4 Robert J. McElice, "A Public-Key Cryptosystem based on Algebraic Codint Theory," DSN PR 42-44, pp. 114-116, 1978.

3-2 符号ベース暗号

符号ベース暗号は、ショアのアルゴリズム登場前から存在する暗号技術であり、誤り訂正符号に基づいて構成される。ここで言う誤り訂正符号とは、元は通信技術の信頼性を保証する技術として情報理論分野で提案された。誤り訂正符号とは大まかには、送信者が何らかの通信路を介して受信者にデータを送信する際、その一部がノイズなどで変化しても、高い確率で元のデータに復元する技術である。誤り訂正符号の詳細は割愛するが、この時誤り訂正符号では、誤りが訂正できるような何らかの数学的構造を用意する。その構造に対するある種のランダムな変換を施すことで、元のデータの特徴が隠されたような別の構造が生成できる。この時、そのランダムな変換を秘密にできたならば、変換後の構造から元のデータの構造を計算できないことが予想される。これが符号ベース暗号の直観である。初めて提案された符号ベース暗号は、1978年のマクリース(McElice)暗号である。誤り訂正符号そのものが複雑であることから本稿では詳細は割愛するが、この方式が登場して40年以上経つものの、いまだに破られていない。このため、安全性は高く信頼できると言える。一方で、符号ベース暗号はディジタル署名方式において効率的な構成が知られていない。符号ベースのディジタル署名は、提案されては、その安全性の問題が指摘されている。

3-3 多変数多項式暗号

多変数多項式暗号は、多変数多項式からなる連立方程式の困難性を安全性の根拠とする暗号技術である。直観的には多変数の連立方程式の解は、一意に定まらないことが根拠となる。多変数多項式暗号も、ショアのアルゴリズム以前から存在していた暗号技術であ

る※5。なお、多変数多項式暗号では一般に二次の多項式を用いる。多変数の連立二次多項式の解を計算する問題は、Multivariate Quadratic（MQ）問題と呼ばれる。

多変数多項式暗号の評価にはMQ問題の困難性だけではなく、具体的なパラメータに対する計算量の評価も重要となる。この評価に対してMQ問題を解答するコンテスト”Fukuoka MQ Challenge”（https://www.mqchallenge.org/）が、2015年4月より開催されている。名前から想像される通り、これは我が国発祥の評価であり、福岡に拠点を置く九州大学と九州先端科学技術研究所の研究者が中心に企画していたことが名前の由来である。MQ問題の主なパラメータとしては変数の個数、方程式の個数、および方程式の係数が定義される体の種類が挙げられる。Fukuoka MQ Challengeでは、本稿を執筆している2022年9月時点では変数の個数や方程式の個数に応じてType IからType VIの6種類が定義されており、近年では2020年8月に台湾のBo-Yin Yang教授のチームによってType IIIの変数38個、方程式76個の場合が解かれている。2022年1月に各Typeにおいて新たなチャレンジが追加されたが、本稿執筆時点では解いた報告はされていないようである。これらの評価は、多変数多項式暗号において今後も継続評価されるべき重要課題と言えるだろう。

※5 Aviezri S. Fraenkel, Yaacov Yesha, “Complexity of Solving Algebraic Equations,” Information Processing Letters, Vol. 10, No. 4-5, pp.178-179, 1980.

3-4 同種写像暗号

同種写像暗号は上述した耐量子計算機暗号のうち、最も新しく登場した暗号技術である。これはECDH（楕円曲線ディフィー・ヘルマン鍵共有）などの基盤となる楕円曲線に対し、同種写像と呼ばれる写像を用いた暗号技術である。従来の楕円曲線暗号が単一の曲線における点の動きを考えることに対し、同種写像暗号では複数の楕円曲線同士の関係を考える点が異なる。楕円曲線暗号も詳細に述べると高度な数学的知識が必要となるため詳細は割愛するが、多くの教科書が出版されており、例えば大阪大学・宮地充子先生の書籍※6がある。

さて、同種写像は楕円曲線から楕円曲線への写像の一種であることは先にも述べたが、実は同種写像の概念は公開鍵暗号の概念よりも先に存在している。例えば同種写像に関する有名な結果として、1971年にベルーの公式（Velu’s formula）※7が示されている。ベルーの公式の詳細は割愛するが、その証明としてまず同種写像を選び、それに合わせて値域となる楕円曲線を求めている。これに対し、二つの楕円曲線が与えられた状況で、それらの楕円曲線を結びつける同種写像を求める問題は、同種写像問題と呼ばれ、同種写像暗号の安全性の根拠となっている。代表的な手法としては、鍵共有方式であるSIDH※8が知られている。

※6 宮地充子, “代数学から学ぶ暗号理論: 整数論の基礎から楕円曲線暗号の実装まで,” 日本評論社, 2012.
※7 Jacques Velu, “Isogenies Entre Courbes Elliptiques,” Comptes Rendus Hebdomadaires des Seances de l’Academie des Sciences, pp.2380231, 1971.
※8 David Jao, Luca De Feo, “Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies,” PQCrypto 2011, pp.19-34, 2011.

4 耐量子計算機暗号の現状

アメリカ国立標準技術研究所（National Institute of Standards and Technology, NIST）は、2016年から耐量子計算機暗号に関する標準化規格の選定を進めている（https://csrc.nist.gov/projects/post-quantum-cryptography）。2022年7月には暗号方式として一つの方式が、ディジタル署名として三つの方式が標準化対象として選ばれたことが報道されている※9。選ばれた方式は暗号化方式としてCRYSTALS-KYBER、ディジタル署名としてCRYSTALS-Dilithium, FALCON, SPHINCS+である。また、上記の四つの方式とは別に新たなラウンドとして、暗号化方式としてBIKE、Classic McEliece、HQC、SIKEの四つの方式が標準化規格の候補として継続議論されている。加えてディジタル署名方式が特に数に乏しいなどの理由もあり、（本稿執筆時点では）2022年10月1日までさらに新たな候補の提出も受け付けている。

上記の方式において前節で述べた種類で分けると、標準化されるものではCRYSTALS-KYBERとCRYSTALS-Dilithium、FALCONが格子暗号、SPHINCS+がハッシュベース署名（本稿では割愛する）である。また、まだラウンドに残っているものとして、BIKE、Classic McEliece、HQCが符号ベース暗号、SIKEが同種写像暗号である。格子暗号が多く、それ以外の方式がまだ発展途上にあることがこの結果から伺える。この実質的に格子暗号しか現状では標準化が決まっていないことが、新たなラウンドが追加された背景にはある。もし仮に格子暗号に有効な量子計算機のアルゴリズムが発見された場合、かつてショアのアルゴリズムが発見された時以上の衝撃が世の中に発展する可能性が高いためである。なお、選定の途中で標準化候補から外れてしまった方式には、安全性上の問題が見つかっている方式も多い。符号ベース暗号のディジタル署名などが、安全性上の問題が見つかった代表的な例と言える。

ところで、上述した計8個の方式は、既存の暗号ライブラリliboqs（https://github.com/open-quantum-safe/liboqs）にも実装されている。興味のある読者に向けたベンチマークとして、liboqsを用いて計測した各方式の性能を表2、表3にそれぞれ示す。これらの表においては、public keyが公開鍵のバイトサイズ、secret keyが秘密鍵のバイトサイズ、ciphertextあるいはsignatureが暗号文あるいは署名のバイトサイズにそれぞれ相当する。また、計算時間はkeygen/sが毎秒あたりの鍵生成回数、encaps/s

あるいはsign/sが毎秒あたりの暗号化回数あるいは署名回数、decaps/sあるいはverify/sが毎秒あたりの復号回数あるいは検証回数である。これらの性能はUbuntu 18.04.6 LTS（Bionic Beaver）上で、Intel® Core™ i7-8700K CPU 3.70GHzを搭載した32GBメモリを持つマシン上で計測した。コンパイラはgcc 8.4.0を用いている。

まず暗号化方式について、CRYSTALS-KYBERはKyber512とKyber768いずれも同種写像暗号によるSIKEを除く他の方式と比べて各バイトサイズと計算時間のバランスが取れているように見受けられる。特に毎秒あたりの暗号化回数と復号回数の数値が高く、これらが標準化されたことは順当に思える。BIKEが継続して審議されていることも同様である。一方、ディジタル署名は、ハッシュベース署名であるSPHINCS+は公開鍵と秘密鍵のバイトサイズが小さいものの、署名のサイズが大きくなっている。FALCONは署名回数の数値が高いものの、検証回数の数値が低い。これに対しCRYSTALS-Dilithiumは、バイトサイズと計算時間のバランスが取れている。このため、CRYSTALS-Dilithiumが総合的にみて最も優れているようにみえる。耐量子計算機暗号の研究開発では、これらの計算時間をいかに改善するかが議論されている。

表2 各暗号化方式の性能評価

Algorithm	public key	ciphertext	secret key	shared secret key	keygen/s	encaps/s	decaps/s
BIKE-L1	1541	1573	5223	32	20.3	9.5	7.2
BIKE-L3	3083	3115	10105	32	22.9	12.0	7.0
Classic-McEliece-348864	261120	128	6452	32	1.1	11.9	4.1
Classic-McEliece-348864f	261120	128	6452	32	1.1	12.1	4.2
Classic-McEliece-460896	524160	188	13568	32	0.9	13.0	3.8
Classic-McEliece-460896f	524160	188	13568	32	1.1	12.8	3.7
Classic-McEliece-6688128	1044992	240	13892	32	1.2	14.9	3.6
Classic-McEliece-6688128f	1044992	240	13892	32	1.2	15.1	3.5
Classic-McEliece-6960119	1047319	226	13908	32	1.5	15.6	3.8
Classic-McEliece-6960119f	1047319	226	13908	32	1.2	14.6	3.7
Classic-McEliece-8192128	1357824	240	14080	32	1.3	17.5	3.6
Classic-McEliece-8192128f	1357824	240	14080	32	1.2	17.3	3.6
HQC-128	2249	4481	2289	64	2.1	2.5	2.3
HQC-192	4522	9026	4562	64	2.3	2.9	2.7
HQC-256	7245	14469	7285	64	2.7	3.3	3.2
Kyber512	800	768	1632	32	3.8	4.0	6.8
Kyber768	1184	1088	2400	32	4.1	4.1	6.5
Kyber1024	1568	1568	3168	32	4.6	4.4	6.3
SIKE-p434	330	346	374	16	4.9	5.0	5.0
SIKE-p503	378	402	434	24	1.3	1.3	1.3
SIKE-p610	462	486	524	24	6.5	6.5	6.5
SIKE-p751	564	596	644	32	1.3	1.3	1.3

表3 各ディジタル署名方式の性能評価

Algorithm	public key	secret key	signature	keygen/s	sign/s	verify/s
Dilithium2	1312	2528	2420	3.3	5.8	3.8
Dilithium3	1952	4000	3293	3.5	5.9	3.6
Dilithium5	2592	4864	4595	3.3	5.6	3.7
Falcon-512	897	1281	690	2.6	19.9	1.0
Falcon-1024	1793	2305	1330	2.3	21.9	1.0
SPHINCS+-SHA256-256f-robust	64	128	49856	2.1	2.0	1.0
SPHINCS+-SHA256-256f-simple	64	128	49856	3.1	2.9	1.1
SPHINCS+-SHA256-256s-robust	64	128	29792	2.1	2.2	1.0
SPHINCS+-SHA256-256s-simple	64	128	29792	3.0	3.0	1.0

※9 NIST, “PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates,” https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4.

5 最後に

耐量子計算機暗号は、代表的な方式の選定やライブラリ実装を含めて、大きく進展しているように見受けられる。その一方で、格子暗号のみが大きく先行しているなど、各方式が万遍なく発展しているとは言い難い現状にあると著者は感じている。格子暗号や符号ベース暗号において、量子計算機を用いた解析方法が提案される可能性もいまだあり得ることから、今後は継続して格子暗号以外のさまざまな枠組みから方式を設計していくことが望ましい。我が国においても耐量子計算機暗号の研究開発が盛んであり、国主導のプロジェクトなども展開されている。著者はもちろん、我が国が総力を挙げて、今後も耐量子計算機暗号の研究開発に取り組み、世界的な成果を上げていくことが期待される。

（大阪大学　大学院情報科学研究科　矢内直人）

※著本の研究は、総務省の「電波資源拡大のための研究開発（JPJ000254）」における委託研究「安全な無線通信サービスのための新世代暗号技術に関する研究開発」の成果として実施されている。

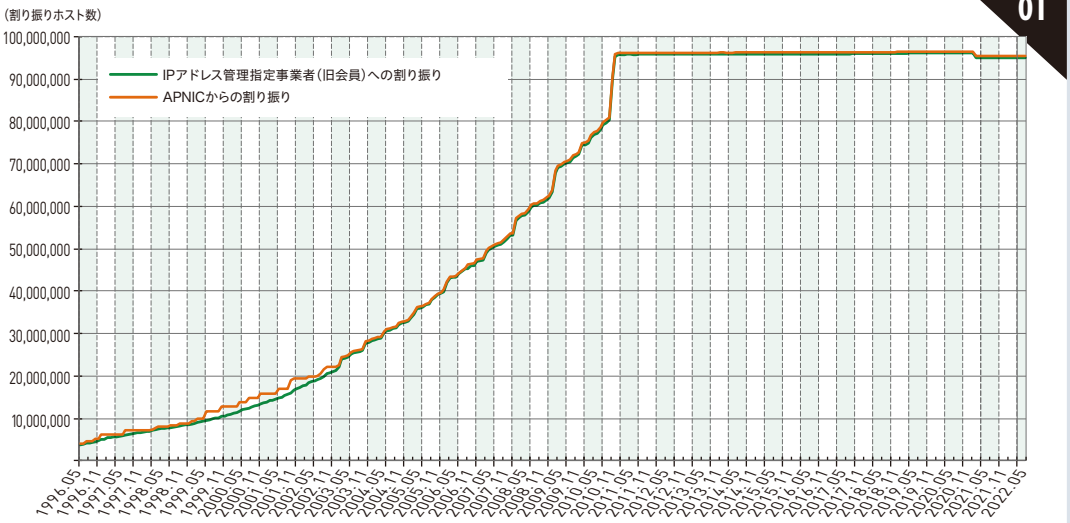
統計情報

IPv4

IPv4アドレスの割り振り件数の推移

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

01

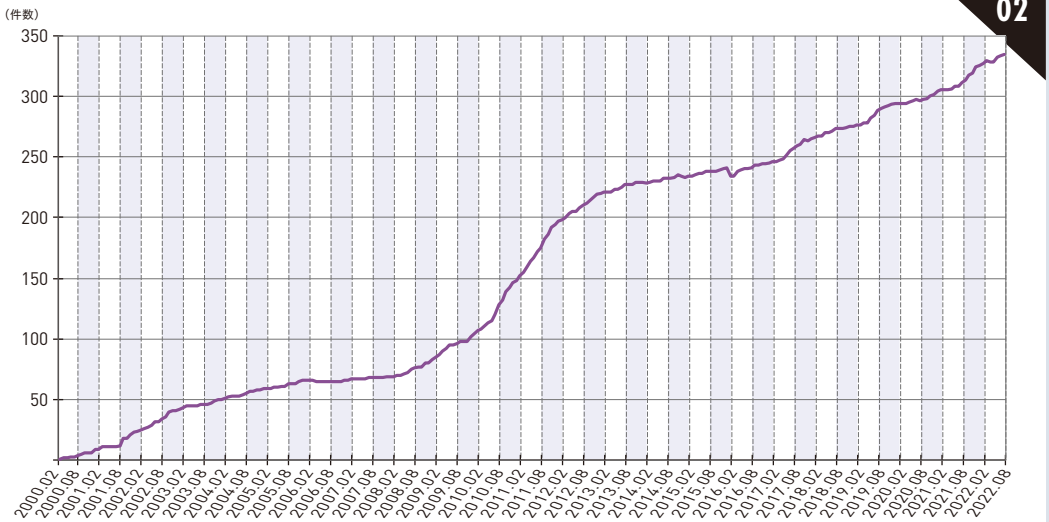


IPv6

IPv6アドレス割り振り件数の推移

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

02

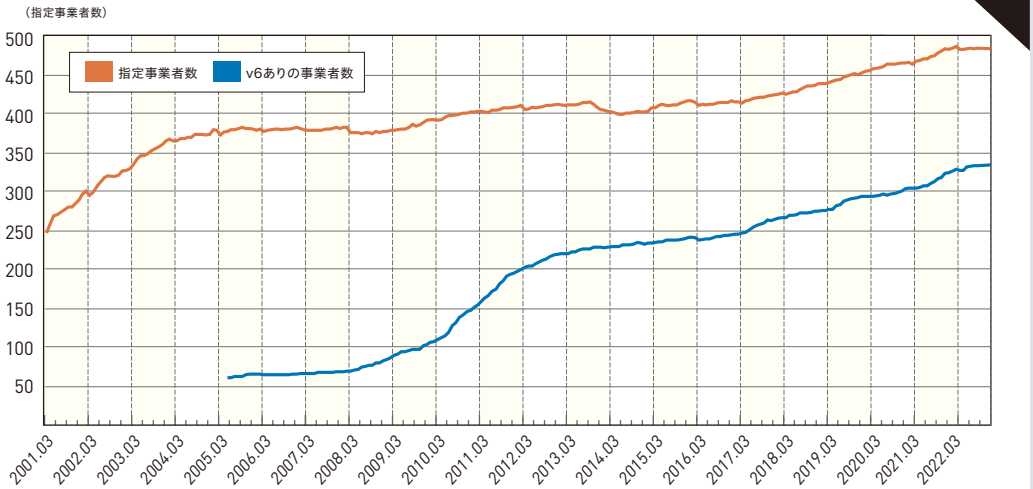


LIR

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。

03



JPNIC Webにも、IPアドレス・ドメイン名に関する統計を掲載していますので、ご覧ください。
https://www.nic.ad.jp/ja/stat/

04

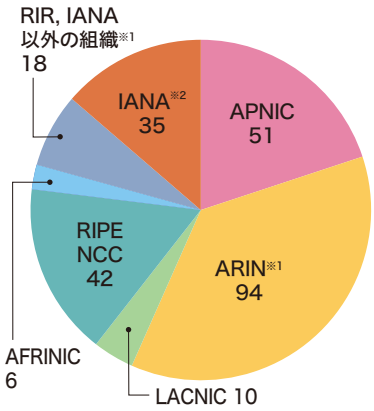
RIR

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

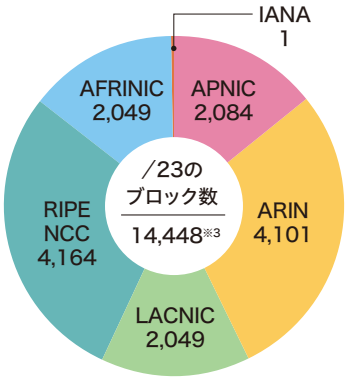
各地域レジストリごとのIPv4、IPv6、AS番号の割り振り状況です。APNICはアジア太平洋地域、ARINは主に北米地域、RIPE NCCは欧州地域、AFRINICはアフリカ地域、LACNICは中南米地域を受け持っています。

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。

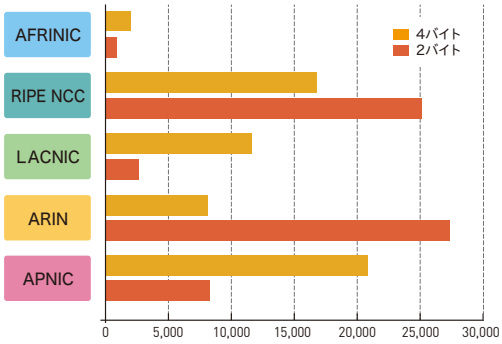
IPv4アドレス（/8単位）



IPv6アドレス（/23単位）



AS番号※4



※1 集計に変更があり、前号80号から「RIR、IANA以外の組織」が1ブロック減、「ARIN」が1ブロック増となりました。

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

※3 IANAからRIRに割り振られた/23のブロック数14448

※4 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AS4,199,848,092個があります

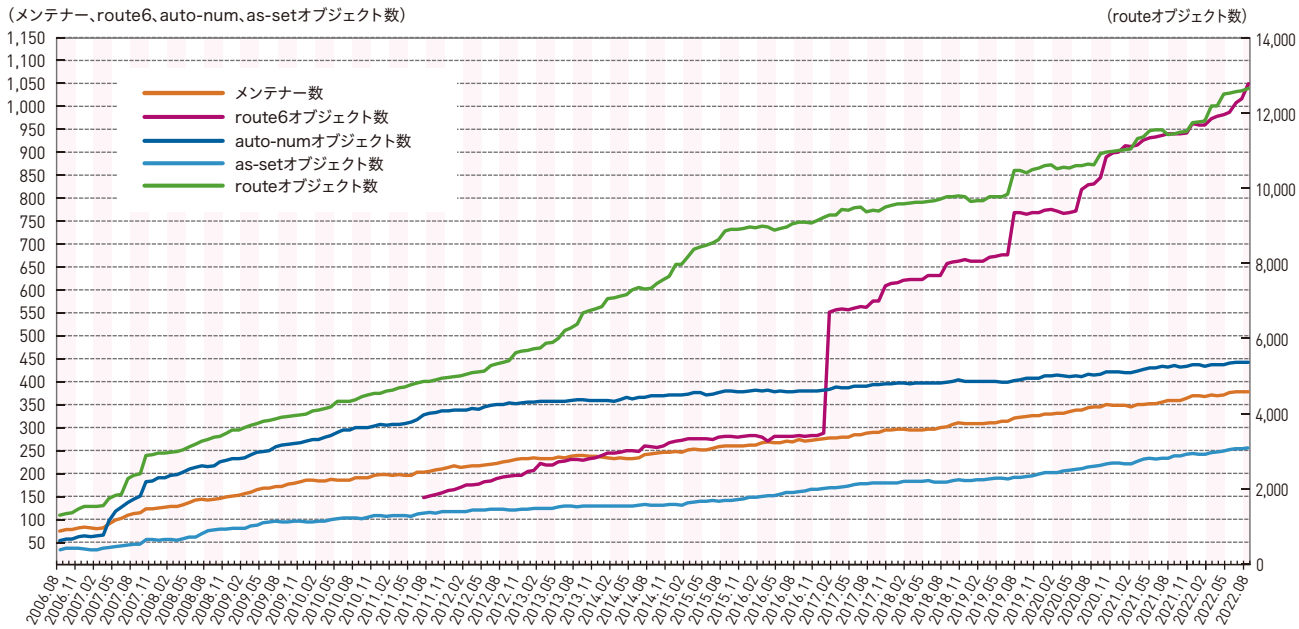
05

JPIRR

JPIRRに登録されているオブジェクト数の推移

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

https://www.nic.ad.jp/ja/irr/



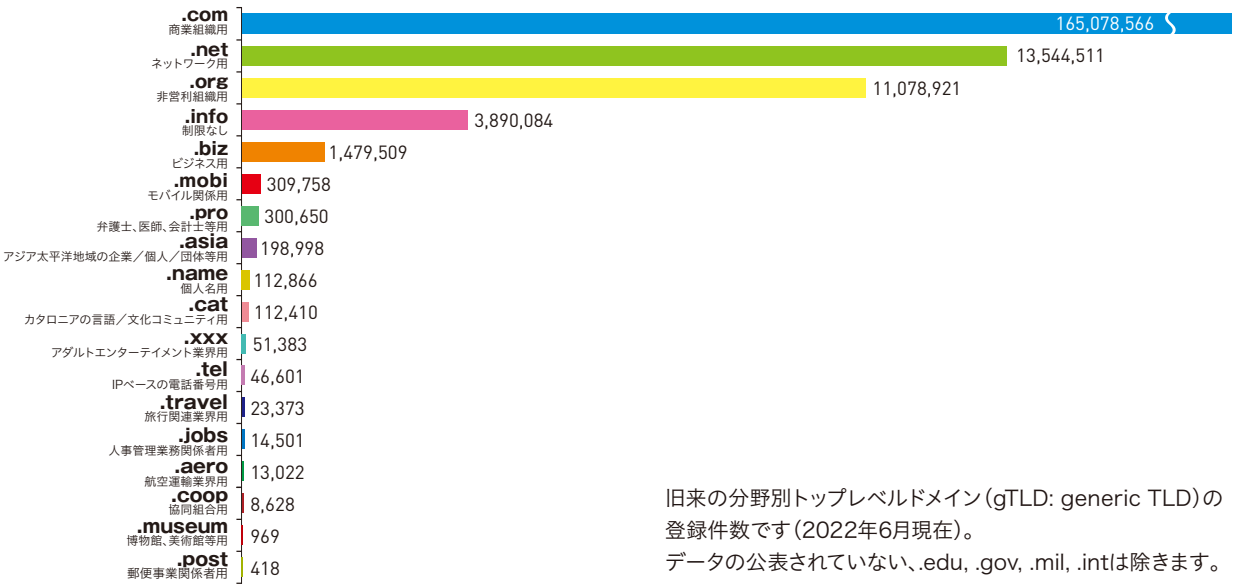
06

gTLD

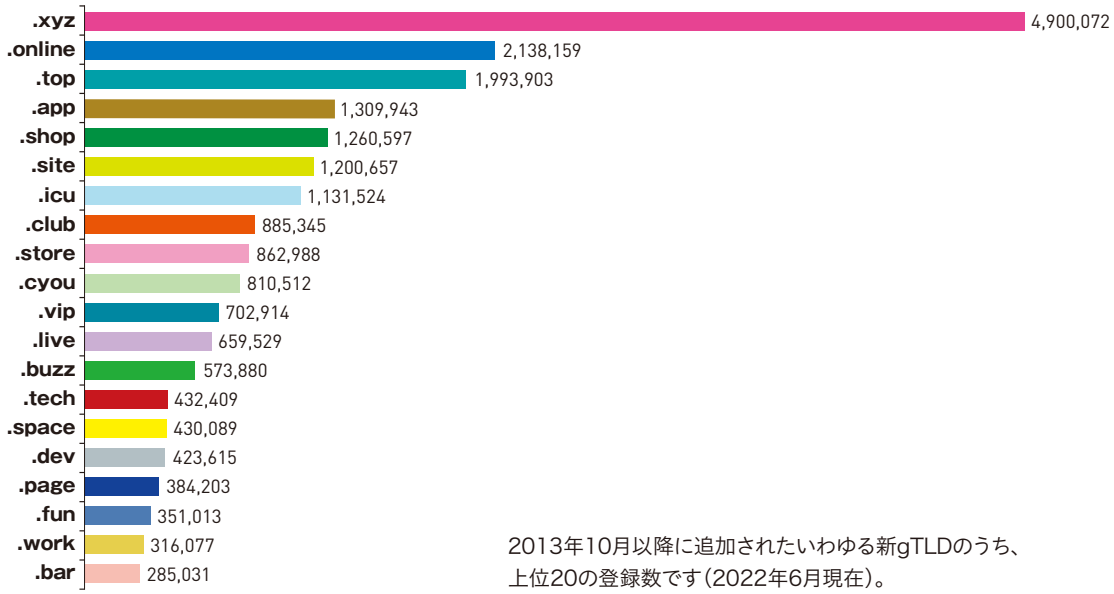
主なgTLDの登録数

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

Monthly Registry Reports
https://www.icann.org/resources/pages/registry-reports



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(2022年6月現在)。
データの公表されていない、.edu, .gov, .mil, .intは除きます。



2013年10月以降に追加されたいわゆる新gTLDのうち、上位20の登録数です(2022年6月現在)。

JP DOMAIN NAME

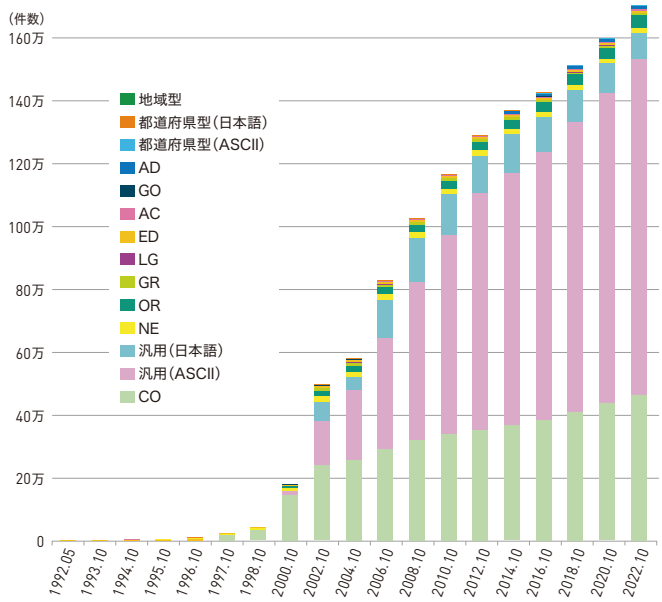
07

JPドメイン名の登録数

JPドメイン名の登録件数は、2001年の汎用JPドメイン名登録開始により大幅な増加を示し、2003年1月1日時点で50万件を超えました。その後も登録数は増え続けており、2008年3月1日時点で100万件を突破、2022年10月現在では約170万件を超えています。

2022年10月時点の登録総数：1,713,403件

属性型・地域型JPドメイン名			
AD	JPNIC会員等	250	0.02%
AC	大学など高等教育機関	3,805	0.22%
CO	企業等	465,470	27.17%
GO	政府機関等	754	0.04%
OR	その他法人組織	39,638	2.31%
NE	ネットワークサービス	12,860	0.75%
GR	任意団体	5,561	0.33%
ED	小中高校など初等中等教育機関	6,340	0.37%
LG	地方公共団体	1,898	0.11%
地域型	地方公共団体、個人等	2,093	0.12%
汎用JPドメイン名			
ASCII	組織・個人問わず誰でも	1,077,904	62.91%
日本語		85,908	5.01%
都道府県型JPドメイン名			
ASCII	組織・個人問わず誰でも	9,438	0.55%
日本語		1,484	0.09%



DISPUTE RESOLUTION

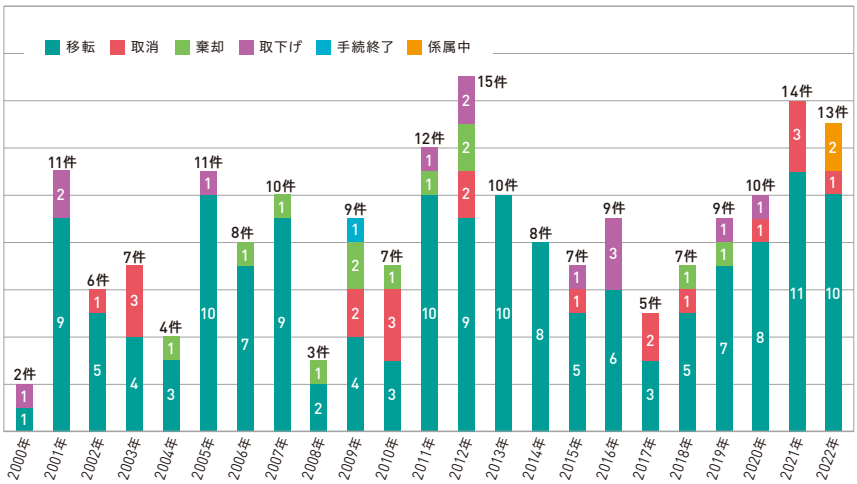
08

JPドメイン名紛争処理件数

JPNICはJPドメイン名紛争処理方針（不正の目的によるドメイン名の登録・使用があった場合に、権利者からの申立に基づいて速やかにそのドメイン名の取消または移転をしようとするもの）の策定と関連する業務を行っています。この方針に基づき実際に申立てられた件数を示します。（2022年10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



JPNIC MEMBERS LIST

会員リスト

JPNICの活動は
JPNIC会員によって
支えられています

2022年10月19日現在

S 会員

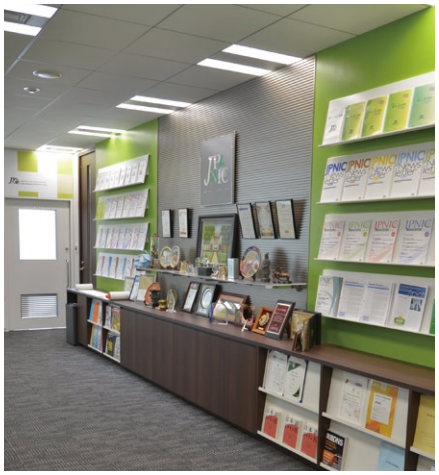
- 株式会社インターネットイニシアティブ
- エヌ・ティ・ティ・コミュニケーションズ株式会社
- 株式会社日本レジストリサービス

B 会員

- 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
- 富士通株式会社



JPNIC会員のみなさまには さまざまな特典をご用意しております

会員向けWebページでは、会員の方がご利用いただける各種特典をご紹介しております。会費分類に応じた特典の内容については、下記のWebページをご覧ください。

■会員の種類・特典・会費
https://www.nic.ad.jp/ja/member/guide/join.html

ご利用特典

お問い合わせ先 企画総務部会員担当
member@nic.ad.jp

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IDCフロンティア
- 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
- イッツ・コミュニケーションズ株式会社
- インターナップ・ジャパン株式会社
- インターネットマルチフィード株式会社
- 株式会社インテック
- 株式会社ウインテックコミュニケーションズ
- 株式会社ASJ
- 株式会社エアネット
- AT&Tジャパン株式会社
- エクイニクス・ジャパン・エンタープライズ株式会社
- 株式会社SRA
- SCSK株式会社
- 株式会社STNet
- NRIネットコム株式会社
- 株式会社エヌアイエスプラス
- エヌ・ティ・ティ・スマートコネクト株式会社
- 株式会社エヌ・ティ・ティ・データ
- 株式会社NTTドコモ
- 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
- OTNet株式会社
- 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
- 株式会社オプテージ
- 株式会社QTnet
- 近鉄ケーブルネットワーク株式会社
- 株式会社GEAR
- 株式会社倉敷ケーブルテレビ
- 株式会社クララオンライン
- 株式会社グローバルネットコア
- 株式会社ケーブルテレビ品川
- ケーブルテレビ徳島株式会社
- 株式会社KDDIウェブコミュニケーションズ
- 株式会社コミュニティネットワークセンター
- Coltテクノロジーサービス株式会社
- さくらインターネット株式会社
- 株式会社シーイーシー
- 株式会社シナプス
- GMOインターネット株式会社
- JCOM株式会社
- 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
- 株式会社TAM
- 鉄道情報システム株式会社
- 合同会社DMM.com
- 株式会社ディジティ・ミニミ
- 株式会社デジタルアライアンス
- 株式会社電算
- 東京ケーブルネットワーク株式会社
- 東芝デジタルマーケティングイニシアティブ株式会社
- 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
- 株式会社ドワンゴ
- 株式会社長崎ケーブルメディア
- 日本電信電話株式会社

D 会員

- ニフティ株式会社
- 日本インターネットエクスチェンジ株式会社
- 株式会社日本経済新聞社
- 日本情報通信株式会社
- 日本通信株式会社
- 日本ネットワークイネイブラー株式会社
- 株式会社日立システムズ
- BBIX株式会社
- 株式会社PFU
- 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
- 株式会社まほろば工房
- 丸紅ネットワークソリューションズ株式会社
- ミクスネットワーク株式会社
- 三菱電機インフォメーションネットワーク株式会社
- 株式会社メイテツコム
- 株式会社メディアウォーズ
- ヤフー株式会社
- 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
- 株式会社両毛システムズ
- 株式会社リンク

非営利会員

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

推薦個人正会員（希望者のみ掲載しております）

- 淺野 善男
- 池上 聡
- 伊藤 竜二
- 岩崎 敏雄
- 太田 良二
- 木村 和貴
- 小林 努
- 佐々木 泰介
- 式場 薫
- 島上 純一
- 城之内 肇
- 任田 大介
- 中西 和也
- 三膳 孝通
- 森田 裕己
- 森信 拓
- 安江 律文
- 吉田 友哉

賛助会員

- ■アイコムティ株式会社
- ■株式会社アシスト
- ■株式会社イーツ
- ■伊賀上野ケーブルテレビ株式会社
- ■イクストライド株式会社
- ■伊藤忠テクノソリューションズ株式会社
- ■株式会社イプリオ
- ■インターネットエーアールシー株式会社
- ■FRT株式会社
- ■グローバルコモンズ株式会社
- ■株式会社ケーブルネット鈴鹿
- ■株式会社ケイアンドケイコーポレーション
- ■株式会社ゲンザイ
- ■株式会社コム
- ■サイバー・ネット・コミュニケーションズ株式会社
- ■株式会社サイバーリンクス
- ■株式会社さくらケーシーエス
- ■株式会社JWAY
- ■株式会社Geolocation Technology
- ■セコムトラストシステムズ株式会社
- ■株式会社ZTV
- ■ソニーグローバルソリューションズ株式会社
- ■株式会社つくばマルチメディア
- ■デジタルテクノロジー株式会社
- ■株式会社トーカ
- ■株式会社長野県協同電算
- ■株式会社新潟通信サービス
- ■虹ネット株式会社
- ■日本インターネットアクセス株式会社
- ■ネクストウェブ株式会社
- ■株式会社ネット・コミュニケーションズ
- ■晴れの国ネット株式会社
- ■BAN-BANネットワークス株式会社
- ■姫路ケーブルテレビ株式会社
- ■株式会社富士通鹿児島インフォネット
- ■プロックスシステムデザイン株式会社
- ■株式会社マークアイ
- ■松阪ケーブルテレビ・ステーション株式会社
- ■株式会社MIXI
- ■三谷商事株式会社

From JPNIC
Japan Network Information Center
JPNIC Newsletter
for JPNIC Members
No.82

Dear Readers,

This issue of the newsletter highlights the following two special articles.

Now, it's that time again this year! In Special Article 1, we cover Internet Week 2022. This year's theme is "The Internet Compass - Steer the a Course for the Future!", which expresses our hope that Internet Week could will act as be a compass for those involved in the Internet. Thanks to your tremendous support, Internet Week celebrated its 25th-anniversary last year in 2021. This year marks the start of a new quarter century. In this milestone year, we will once again consider the role of Internet Week. In addition, one of the new challenges this year is to hold the event in an on-site and online hybrid format. For the past two years, the conference was held online due to measures against COVID-19, however this year we offer on-site sessions in addition to online sessions during the latter three days of the conference. We hold hybrid sessions, especially for programs where lively exchanges of opinions between speakers and participants are to be essential.

In Special Feature 2, we focus on the registration and search service for public key information on for PGP, which had been provided at "pgp.nic.ad.jp" which and was terminated on September 30, 2022. Since its release, it had been used for registration and search for PGP public keys on public servers since its release. However, we have decided to discontinue this service because we believe that it has fulfilled its role in providing such a service . This page article is a review of the service as a page in the history of the Internet.

In "Prologue to the Internet: its Technologies and Services", the "JP29-type-robot "Nic-kun" and Dr. Netson of the Internet research institute explain the development of cloud storage services. Online storage services have become widespread since around 2010 when smartphones became popular. Let's take a look at how cloud storage services, with their ability to provideof data synchronization, have evolved over the years.

In "Pick Out!", we introduce featured articles from the JPNIC blog. This time, we feature an article on the launch event, held on April 28, 2022, in a hybrid face-to-face and videoconference format on April 28, 2022, where "The Declaration for the Future of the Internet" was presented. The Declaration was proposed by partner countries including the United States, European countries, Australia, New Zealand, Japan, multiple countries in Europe, and others.so on and It was endorsed by over 60 countries and regions. For the full text, visit https://blog.nic.ad.jp/2022/7530/ !!

"Introducing JPNIC Members" focuses on a particular JPNIC member engaged in interesting activities. This time, we visited Unitas Global Co., Ltd., headquartered in Chiyoda-ku Tokyo. They have earned the trust of their customers for their low-latency network environment enabled by their unique intelligent routing technology , positive problem-solving skills, and bilingual support for customers' global business development. In May 2022, they joined Unitas Global, headquartered in Illinois, USA, allowing them to be more competitive oin services. Not justBoth their business is unique, theirand culture areis unique as well. Their president and all employees are fully committed to entertaining and delighting not only their customers, but all stakeholders., And they have produced a music video (https://youtu.be/5bSItHjuaHE) to commemorate their 20th anniversary. During the interview, we got to hear a variety of impressive stories, including their philosophy on business and human resources.

"The Internet Loves You" is a corner in which we introduce a person who is active in the Internet industry. This time, we introduce Dr. Takahiro Nemoto, who is engaged in research, at The Tokyo University of Agriculture and Technology (TUAT), focused on university network operations, internationalized technologies, internationalized strings, etc., while also beingHe is also active in the Internet Engineering Task Force (IETF) and Internet Society Japan Chapter (ISOC-JP). Although he has a career as a researcher in the field of the Internet, it was not until he entered graduate school that he became deeply involved in the Internet. He talks about his experiences, and influences, he had and his goals for the future.

In our "10 Minute Internet Course", we explore the keyword "Quantum-Resistant Cryptography (Post-Quantum Cryptography)". In the previous issue (No. 81), Associate Professor Naoto Yanai, Graduate School of Information Science and Technology, Osaka University, explained the current status of quantum computers and what will change with the advent of quantum computers. In this issue, he explains the development and the current status quo of quantum-resistant cryptography, which is attracting attention as a technology that couldto guarantee the security of quantum computers even after they are put into practical use. The explanation is easy to read without and avoids using mathematical formulas, making it and is best to a good read for beginners!!

In addition, you'll also find "Internet Topics", "JPNIC Activity Reports", "Statistics" etc., for the past several months. If you have any comments or feedback, please feel free to contact us at jpnic-news@nic.ad.jp. Your comments are greatly appreciated!!

編集をおえてのひとこと。

感染症対策を続けながらとなりますが、約2年半ぶりに岡山にある実家に帰省したり、音楽イベントに参加したりという機会がありました。

そのイベントは「THE TRAD × ギター・マガジン 渋谷音楽祭 TALK&SESSIONS」というものだったのですが、私の好きなラジオ番組とギタリスト専門誌のコラボしたもので、トークやミニライブで3時間、みっちり楽しませてもらいました。出演者が大変豪華だったのですが、その中でも森 大翔(もり やまと)さんのギターテクニックが素晴らしく、それでいて今年19歳という若さですから、感心しきりでした。

当日披露された「すれ違ってしまった人達へ」という楽曲にハマり、リピートしています。皆さまも、ぜひミュージックビデオをご覧になってみてください。

出不精な私ですが、直接刺激を感じ、体験をする価値を思い出す機会になりました。Internet Week 2022では、人数など限られますが、3年ぶりの現地参加があります。ご参加の方にとって有意義な機会となるよう、精一杯準備いたしましたので、ぜひお楽しみください。

そして、率直な感想をいただけると幸いです。

角

久々に岡山に帰省し、行きつけの喫茶店にも寄ることができました

JPNIC Newsletter 82号 読者アンケートご協力のお願い

今号のご感想や、今後のよりよい誌面作成のために、読者の皆さまからのご意見をいただきたく、JPNIC Newsletterに関するアンケートを実施いたします。何とぞご協力お願い申し上げます。多くの皆さまからのご回答を、心からお待ちしております。

ご回答はこちら

https://forms.gle/Wm2NBz9SCn2oWnMW7

次回予告

Internet Week 2022 開催報告 etc.

ご期待ください

JPNIC CONTACT INFO ▼お問い合わせ先

JPNIC Q&A

詳しくはこちら

https://www.nic.ad.jp/ja/question/

一般的な質問	query@nic.ad.jp
JPNICへのお問合わせ	secretariat@nic.ad.jp
IPアドレスについて	ip-service@nir.nic.ad.jp

JPNICニュースレターについて

詳しくはこちら

▶すべてのJPNICニュースレターはHTMLないしPDFでご覧いただけます。
▶JPNICニュースレターの内容に関するお問い合わせ、ご意見は jpnic-news@nic.ad.jp 宛にお寄せください。
▶なおJPNICニュースレターのバックナンバーの冊子をご希望の方には、一部900円(消費税・送料込み)にて実費頒布しております。現在までに1号から81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82号 2022年11月18日発行

発行人 江崎浩
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2-12-6 内神田OS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 ISBN978-4-902460-57-5

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-256 : 9C:D3:CE:D6:DB:14:BA:72:EC:01:01:5A:6B:6F:72:A7:94:35:84:3B:37:6B:99:E7:5D:F0:A4:55:B5:CD:8B:05
JPNIC認証局のページ http://jpnic-ca.nic.ad.jp/

JPNIC Newsletter
No.82 NOVEMBER 2022
for JPNIC Members
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2-12-6 内神田OSビル4F
Tel 03-5297-2311 Fax 03-5297-2312