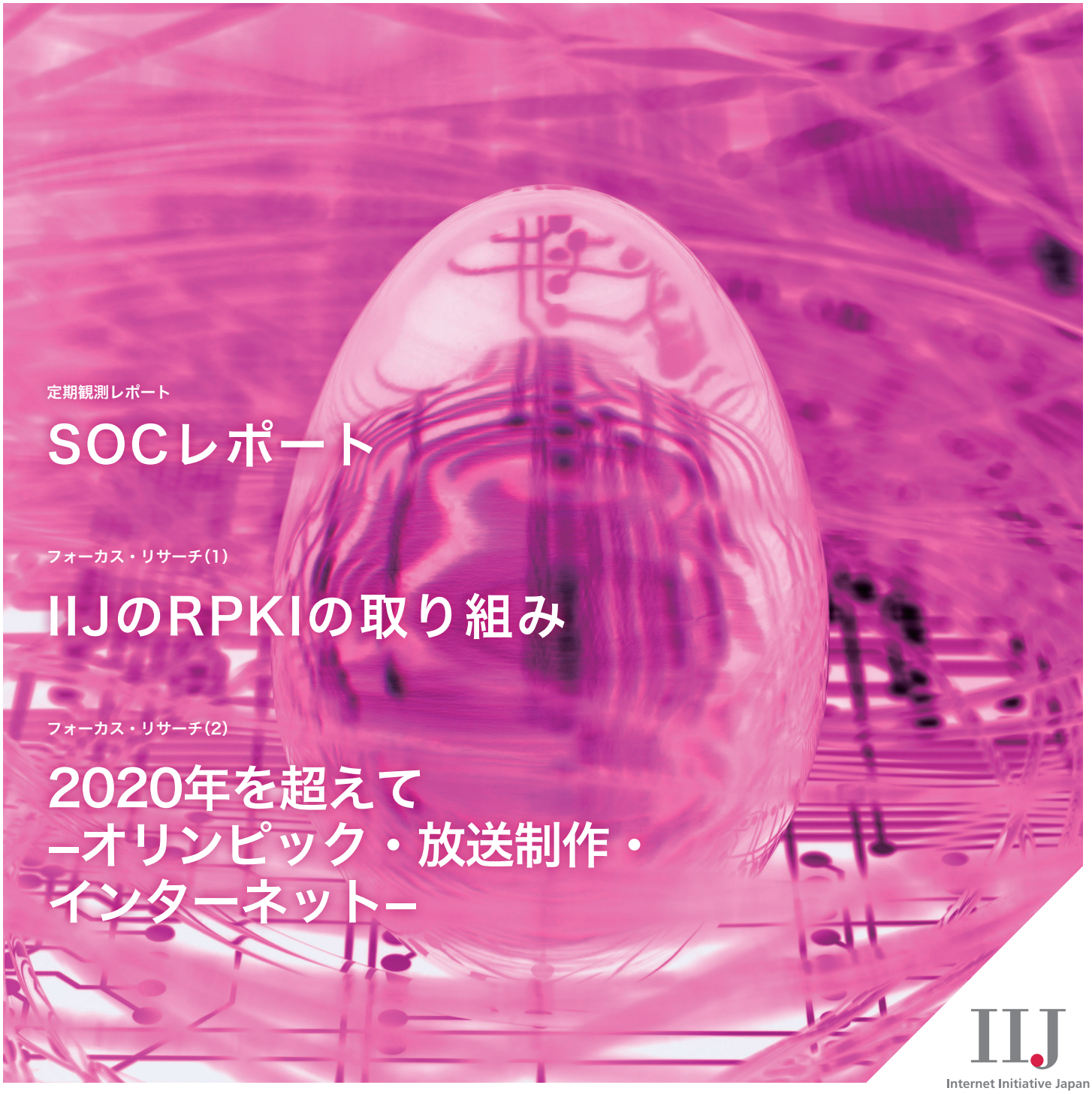
IIR

Internet
Infrastructure
Review

Mar.2021
Vol.50



定期観測レポート

SOCレポート

フォーカス・リサーチ(1)

IIJのRPKIの取り組み

フォーカス・リサーチ(2)

2020年を超えて
–オリンピック・放送制作・インターネット–

IIJ
Internet Initiative Japan

Internet Infrastructure Review

March 2021 Vol.50

エグゼクティブサマリ

一部の国では新型コロナウイルスに対するワクチン接種が開始されてはいるものの、ウイルスの変種も確認され、依然として厳しいロックダウンが続いている地域もあります。日本でも、2020年末に感染者が大幅に増加し、年明けには2回目の緊急事態宣言が発令されるなど、まだ予断を許さない状況です。

新型コロナウイルスにより世界的に人の活動が制限されるなか、インターネットに代表される情報通信技術が社会生活を支えていると実感する毎日です。外出を制限された人の娯楽として動画が消費され、インターネットのトラフィックが大きく伸びたことは「IIR」でも紹介しました。企業がリモートワークを導入し、オンラインでの執務が増えていることは言うまでもありません。フードデリバリーの風景を見ることが増えたと感じている方も多いでしょうが、その注文の多くはインターネットで行われ、決済もオンライン化されています。オンラインショッピングの取扱高も増加していると聞きます。ただ、いずれも以前から存在するサービスであり、これらは、利用者に新しい感動や体験を与えているのか、コロナ禍を契機に社会に浸透したに過ぎないのではないか、という見方もあるかもしれません。

日本でもようやくワクチン接種が始まろうとしており、ポストコロナを見据える段階にきています。世界にはコロナ禍以外にも課題が山積しており、SDGsのように共通の課題も提示されています。そのような大きな社会課題をいかに解決していくのか、それに対し情報通信技術やインターネットがどのように貢献できるのか、情報通信に携わる一員として考えていきたいと思います。

「IIR」は、IIJで研究・開発している幅広い技術を紹介しており、日々のサービス運用から得られる各種データをまとめた「定期観測レポート」と、特定テーマを掘り下げた「フォーカス・リサーチ」から構成されています。

1章の「定期観測レポート」は、SOCレポートです。IIJのSOCでは、自社のサービスを運営することから得られる情報に加え、独自に収集している情報、社外から得られた情報の分析を行っています。2017年からは「wizSafe Security Signal」を通じて、私たちが観測した脅威やセキュリティに関するトピックを発信していますが、本レポートでは2020年のセキュリティインシデントの動向を振り返っています。IIJのSOCが注目したセキュリティインシデントとして、SSL-VPN製品の脆弱性を狙った攻撃、EmotetやIcedIDによる攻撃などを取り上げています。

2章の「フォーカス・リサーチ」では、RPKI（Resource Public-Key Infrastructure）を解説しています。インターネットが世界的に社会のインフラとして機能している今日でも、インターネットのルーティングシステムは経路ハイジャックやオペレータの設定ミスに対して盤石とは言えません。RPKIは、それをより強固にするために、インターネット上で交換される経路情報などの正当性を電子証明書によって検証する仕組みです。本章では、RPKIの概要や動向と共に、IIJの取り組みを紹介しています。

3章の「フォーカス・リサーチ」は、放送制作におけるネットワーク利用についてです。2020年はオリンピックというビッグイベントが予定されていた年であり、多くの職場でリモートワークが進んだ年でもありました。本章では、オリンピックのようなイベント中継で活用できるIPネットワークを用いたリモートプロダクションの仕組みや、放送制作の場におけるインターネットを活用したリモートワークの実証実験について紹介し、これからの展望について述べています。

IIJは、このような活動を通してインターネットの安定性を維持しながら、日々、改善・発展させていく努力を行っています。今後も企業活動のインフラとして最大限に活用いただけるよう、様々なサービスやソリューションを提供し続けてまいります。

島上 純一（しまがみ じゅんいち）
IIJ 取締役 CTO。インターネットに魅かれて、1996年9月にIIJ入社。IIJが主導したアジア域内ネットワークA-BoneやIIJのバックボーンネットワークの設計、構築に従事した後、IIJのネットワークサービスを統括。2015年よりCTOとしてネットワーク、クラウド、セキュリティなど技術全般を統括。2017年4月にテレコムサービス協会MVNO委員会の委員長に就任。

SOCレポート

1.1 はじめに

IIJでは、2016年にセキュリティブランド「wizSafe（ウィズセーフ）」を立ち上げ、お客様が安全にインターネットを利用できる社会の実現に向けて日々活動しています。wizSafeの立ち上げから4年間が経過しますが、SOCではインシデント対応の観点や、運用を最適化する観点から、体制を絶えず変化させています。これまでSOCは、情報分析基盤[*1]で脅威を発見する仕組み作りに注力してきましたが、情報分析基盤を通じて得られる情報を活用する方向へシフトしました。これにより、脅威の発見と情報発信の活動を促進することができました。

SOCでは2017年より、wizSafe Security Signal[*2]を通じてIIJサービスの様々なログを集約している情報分析基盤で観測した脅威や、セキュリティに関するトピックを発信しています。2020年はイベントやカンファレンスの多くがリモート化されました。SOCでも、IIJ Technical NIGHTやJapan Security Analyst Conference（JSAC）2021[*3]にリモートで登壇し、SOCの持つ知見を公開しました。IIJ Technical NIGHTは技術者向けに開催しているセミナーで、専門分野が異なる3名のSOCメンバーが各自の活動を多くの方々へ紹介しました[*4][*5]。JSAC 2021では、仮想通貨事業者を標的とした攻撃キャンペーンに関する脅威情報を能動的に収集した2020年の活動について発表しました[*6]。

本レポートも、SOCで観測した情報をまとめ、読者の皆様の知見として利用いただけるよう情報を発信するものです。第1.2節では、2020年に国内で話題となったセキュリティトピックの振り返り及びセキュリティサービスによる年間統計をまとめます。また、第1.3節では、SOCアナリストが注目したトピックを紹介します。

1.2 2020年セキュリティサマリ

ここでは2020年に話題となったセキュリティインシデントや、SOCが観測した攻撃情報を振り返ります。

1.2.1 インシデントカレンダー

2020年に話題となった主要なセキュリティに関するインシデントの中から、SOCが注目したものを表-1、表-2にまとめます。

＊1　Internet Infrastructure Review（IIR）Vol.38（https://www.iij.ad.jp/dev/report/iir/038/01.html）。
＊2　wizSafe Security Signal（https://wizsafe.iij.ad.jp/）。
＊3　Japan Security Analyst Conference 2021（https://jsac.jpcert.or.jp/）。
＊4　【資料公開】IIJ Technical NIGHT vol.9（https://eng-blog.iij.ad.jp/archives/6453）。
＊5　コロナ禍のIT勉強会、リアルからオンラインへの切り替えで考えた2つのコト（https://eng-blog.iij.ad.jp/archives/7141）。
＊6　JPCERT/CC、「仮想通貨事業者を標的にした攻撃キャンペーンに関する脅威情報のハンティング」（https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_302_kodera_jp.pdf）。

表-1 インシデントカレンダー(1月～6月)

月	概要・URL
1月	**総合電機メーカが利用するウイルス対策システムに対して、セキュリティパッチ未提供の脆弱性を利用した不正アクセスを受け、個人情報及び機密情報が流出した可能性があることを公表した。** 【三菱電機】 "不正アクセスによる個人情報と企業機密の流出可能性について" https://www.mitsubishielectric.co.jp/news/2020/0120-b.pdf "不正アクセスによる個人情報と企業機密の流出可能性について(第2報)" https://www.mitsubishielectric.co.jp/news/2020/0210-b.pdf "不正アクセスによる個人情報と企業機密の流出可能性について(第3報)" https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf
1月	**大手総合電機メーカは、防衛事業部門で利用している社内サーバの一部が不正アクセスを受け、社内他部門と共有しているファイルへアクセスされていたことを公表した。** 【NEC】 "当社の社内サーバへの不正アクセスについて" https://jpn.nec.com/press/202001/20200131_01.html
3月	**Microsoft社は、SMBv3プロトコルに、認証することなくSMBサーバまたはクライアントに対して任意のコードを実行できる脆弱性が存在することを公表した。** 【Microsoft】 "SMBv3 の圧縮の無効化に関する Microsoft ガイダンス" https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/adv200005 "Windows SMBv3 クライアント/サーバーのリモートでコードが実行される脆弱性" https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2020-0796(Microsoft.comに移動します)
3月	**トレンドマイクロは、同社が提供する複数製品において深刻度の高い脆弱性が存在し、既に一部の脆弱性を悪用する攻撃を確認していることを公表した。** 【トレンドマイクロ】 "【注意喚起】Trend Micro Apex One およびウイルスバスター コーポレートエディションの脆弱性(CVE-2020-8467, CVE-2020-8468)を悪用した攻撃を確認したことによる最新修正プログラム適用のお願い" https://appweb.trendmicro.com/supportNews/NewsDetail.aspx?id=3722
4月	**教育プラットフォーム事業会社は、運営するサービスに対する不正アクセスがあり、サービスを使用するためのID及び暗号化されたパスワードなど、約122万人分が閲覧された可能性があることを公表した。** 【クラッシー】 "サービス一時停止の調査報告とパスワード変更のお願い" https://corp.classi.jp/news/1926/
4月	**コンピュータゲーム会社は、同社の提供するネットワークサービスにおいて、第三者による不正ログインにより約16万件のアカウント情報が閲覧された可能性があることを公表した。** 【任天堂】 "「ニンテンドーネットワークID」に対する不正ログイン発生のご報告と「ニンテンドーアカウント」を安全にご利用いただくためのお願い" https://www.nintendo.co.jp/support/information/2020/0424.html
4月	**Microsoft Teamsにおいてユーザが攻撃者の掌握しているTeamsのサブドメインを使用したGIFファイルやリンク先を閲覧することにより、アカウントが乗っ取られる可能性がある脆弱性が公表された。** 【CyberArk】 "Beware of the GIF: Account Takeover Vulnerability in Microsoft Teams" https://www.cyberark.com/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams/
5月	**電気通信事業者は、同社のサービスを運用する海外拠点サーバへの侵入をきっかけとした、国内のサーバに対する不正アクセスが行われ、サーバに保管されていた621社のサービスに関する工事情報などが流出した可能性があることを公表した。** 【NTTコミュニケーションズ】 "当社への不正アクセスによる情報流出の可能性について" https://www.ntt.com/about-us/press-releases/news/article/2020/0528.html
6月	**海外のセキュリティ企業は、Treck社の組み込み製品向けTCP/IPスタックを実装した製品に存在する計19件の脆弱性を総称した「Ripple20」を公表した。Ripple20にはリモートコード実行が可能となる脆弱性も含まれていた。** 【JSOF】 "Overview- Ripple20" https://www.jsof-tech.com/ripple20/

表-2 インシデントカレンダー(7月～12月)

月	概要・URL
7月	**SOCでは、2月以降観測されていなかったマルウェアEmotetの感染を狙うメール配布活動の再開を確認した。感染端末からメールなどを窃取し次の攻撃へ転用する手法や、パスワード付きZIPファイルを添付する手法など手口が巧妙化し、10月まで継続して観測した。**
8月	**2019年に更新プログラムがリリースされたVPN製品の脆弱性が悪用されたことにより、約900台のサーバで使用されていたユーザ名やパスワードなどの情報がハッキングフォーラム上で公開され、第三者が入手可能な状態であったことが報じられた。流出した情報の中には、複数の国内企業に関する情報が含まれていることが後日国内メディアで報じられている。** 【日経クロステック】 "パッチ未適用のパルスセキュア社VPN、日本企業46社のIPアドレスがさらされる" https://xtech.nikkei.com/atcl/nxt/news/18/08605/
9月	**電子決済サービスを提供する企業は、提携先の金融機関において、第三者に同社の電子決済サービスを不正に利用されたことで不正出金されていたことを公表した。その後、他の電子決済サービスを提供する企業や提携先の金融機関においても同様の公表が相次いだ。** 【NTTドコモ】 "一部銀行の口座情報を使用したドコモ口座の不正利用について" https://www.nttdocomo.co.jp/info/notice/page/200908_02_m.html
9月	**JPCERT/CCは、DDoS攻撃を示唆して仮想通貨を要求する脅迫行為及びDDoS攻撃による被害が複数の国内組織で確認されていることを公表した。** 【JPCERT/CC】 "DDoS 攻撃を示唆して仮想通貨による送金を要求する脅迫行為 (DDoS 脅迫) について" https://www.jpcert.or.jp/newsflash/2020090701.html
9月	**海外のセキュリティ企業は、Active Directoryで利用されているNetlogonに存在する特権昇格の脆弱性(CVE-2020-1472)に関するレポートを公開した。本脆弱性は「Zerologon」と名付けられている。比較的容易に悪用可能であり、攻撃者が悪用し得るツールなどにも本脆弱性を利用する機能が実装されている。悪用された場合にドメイン管理者アカウントのパスワードが変更され、ドメイン管理者権限が取得される可能性がある。** 【Secura】 "Zerologon: Instantly Become Domain Admin by Subverting Netlogon Cryptography (CVE-2020-1472)" https://www.secura.com/blog/zero-logon
10月	**特別定額給付金の給付を騙ったメールやフィッシングサイトが確認されたことにより、総務省やフィッシング対策協議会は注意喚起を行った。** 【総務省】 "特別定額給付金の給付を騙ったメールに対する注意喚起" https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000438.html 【フィッシング対策協議会】 "特別定額給付金に関する通知を装うフィッシング (2020/10/15)" https://www.antiphishing.jp/news/alert/kyufukin_20201015.html "[更新] 特別定額給付金に関する通知を装うフィッシング (2020/10/19)" https://www.antiphishing.jp/news/alert/kyufukin_20201019.html
11月	**ゲームソフト開発会社は、攻撃グループ「Ragnar Locker」を名乗る集団から標的型ランサムウェアによる不正アクセスを受けたと公表した。顧客などの個人情報や、社員及び関係者の個人情報など、2021年1月の時点で最大約39万人分の情報が流出した可能性があるとのこと(執筆時点で調査継続中)。** 【カプコン】 "不正アクセスによるシステム障害発生に関するお知らせ" https://www.capcom.co.jp/ir/news/html/201104.html "不正アクセスによる情報流出に関するお知らせとお詫び" https://www.capcom.co.jp/ir/news/html/201116.html "不正アクセスによる情報流出に関するお知らせとお詫び【第3報】" https://www.capcom.co.jp/ir/news/html/210112.html
11月	**SOCでは、マルウェアIcedIDの感染を観測し、12月始めまで継続して観測した。**
11月	**イベント・コミュニケーション管理サービスの運営会社は、運営するサービスが不正アクセスを受け、個人情報を含む最大677万件の顧客情報が窃取されたことを公表した。その後、同サービスを利用していた多数の組織からも本事象の案内や注意喚起が行われた。** 【Peatix】 "弊社が運営する「Peatix(https://peatix.com/)」への不正アクセス事象に関するお詫びとお知らせ" https://announcement.peatix.com/20201117_ja.pdf "弊社が運営する「Peatix(https://peatix.com/)」への不正アクセス事象に関する第三者調査機関による調査結果のご報告と今後の対応について" https://announcement.peatix.com/20201216_ja.pdf
12月	**発電システム事業会社は、MSP(マネージドサービスプロバイダ)を経由した第三者による不正アクセスを受け、サーバ及びPCがマルウェアに感染していたことを公表した。原因はMSPが提供するソフトウェアの脆弱性であるが、当該脆弱性は未公開であり修正プログラム適用などの対策が確立されていないことも公表された。** 【三菱パワー】 "当社ネットワークに対するマネージド・サービス・プロバイダを経由した第三者からの不正アクセスに係る件" https://power.mhi.com/jp/news/20201211.html

1.2.2 IIJマネージドセキュリティサービスにおける観測情報

本項では、2020年にSOCが情報分析基盤を活用して観測した情報についてまとめます。

■ DDoS攻撃

ここでは、IIJ DDoSプロテクションサービスが検出したDDoS攻撃について取り上げます。

2020年は、DDoS攻撃で用いられる手法に前年から大きな変化はありませんでした。そのため、対策方法も従来通りのものが引き続き有効であると考えられます。表-3は2020年に検出した攻撃を月ごとに要約したものです。

各月の最も規模の大きな攻撃では、そのすべてにトランスポートのプロトコルとしてUDPを用いたAmplificationが手法として用いられていました。アプリケーションのプロトコルとしては、DNS、NTP、LDAPなどが多く用いられており、一連の攻撃で複数のプロトコルが用いられる事例も観測しています。一方、各月の最も長く継続した攻撃では、UDPを用いたAmplification以外にSYN Floodも観測しています。

■ IPS/IDS機器が検出した攻撃

ここでは、IIJマネージドIPS/IDSサービスが検出した攻撃について取り上げます。

2020年は、年間を通じてIoT(Internet of Things)機器にマルウェアを感染させる攻撃を観測しました。近年、IoT機器は攻撃者から積極的に狙われる対象となっており、その傾向が継続しています。IoT機器は、その数を急速に増やす一方で、適切なパッチマネジメントが施されずに既知の脆弱性がある状態で動作し続ける事例が存在します。攻撃者は脆弱性を悪用することでそのような機器をマルウェアに感染させ、遠隔から自由に操れる状態にします。攻撃者に掌握されたIoT機器は、DDoS攻撃など別の攻撃の発信源として悪用される恐れがあります。IoT機器に感染するマルウェア(以下、IoTマルウェア)は数多くの種類が確認されており、感染活動に悪用される脆弱性も多岐にわたります。2020年は、Netis/Netcore社製ルータの脆弱性を悪用する攻撃を最も多く検出しました。この攻撃には、ルータをIoTマルウェアの一種であるGafgytの亜種に感染させることを意図したものが多数含まれることを確認しています。

表-3 2020年DDoS観測情報サマリ

月	検出件数(1日あたりの平均)	パケット数(万pps)	最も規模の大きな攻撃に関する観測情報		最も長く継続した攻撃に関する観測情報	
			帯域(Gbps)	主な攻撃手法	継続時間	主な攻撃手法
1	14.45件	約25	2.19	SNMP Amplification	16分	NTP Amplification
2	13.07件	約1114	29.02	SSDP Amplification	1時間50分	SYN Flood
3	16.41件	約999	90.86	DNS及びNTP Amplification	51分	DNS及びNTP、LDAPなどのAmplification
4	24.63件	約184	19.17	DNS Amplification	19分	DNS及びNTP、LDAPなどのAmplification
5	15.06件	約296	32.11	NTP及びLDAP Amplification	22分	NTP Amplification
6	23.33件	約824	21.42	SSDP Amplification	1時間19分	SSDP Amplification
7	11.84件	約93	3.34	NTP Amplification	29分	NTP Amplification
8	11.29件	約743	58.90	DNS及びApple Remote Management Service Amplification	2時間43分	DNS及びApple Remote Management Service Amplification
9	12.73件	約114	11.21	DNS及びLDAP Amplification	23分	LDAP Amplification
10	18.45件	約78	7.54	DNS及びLDAP Amplification	15分	DNS Amplification
11	17.00件	約434	43.23	DNS Amplification	3時間11分	DNS Amplification
12	17.39件	約532	56.56	DNS Amplification	32分	SYN Flood

また、4月にはXTC、9月にはMoziと呼ばれるIoTマルウェアの感染活動が活発になったことを観測しました。4月に観測したXTCの感染活動では、複数の脆弱性（CVE-2020-9054、CVE-2020-5722、CVE-2020-8515）が悪用されることを確認しています[*7]。

■ Webアクセス時に検出したマルウェア

ここでは、IIJセキュアWebゲートウェイサービスを用いたWebアクセス時に検出したマルウェアについて取り上げます。

2020年は、年間を通じて悪意あるJavaScriptを観測しました。確認した事例の多くでは、正規のWebサイトが改ざんされて、悪意あるJavaScriptが挿入されていました。当該Webサイトを閲覧した場合、Cookieや端末の情報などを外部のサイトに送信することや、偽の懸賞サイトや広告を含む別のサイトにリダイレクトすることを確認しています。

また、Emotetに関連する通信を多数検出しています。Emotetについては、第1.3.2項で詳しく述べます。

■ メール受信時に検出したマルウェア

ここでは、メールを受信する際にIIJセキュアMXサービスが検出したマルウェアについて取り上げます。2020年は、攻撃者が時勢に合わせた巧妙なメールを用いてユーザをマルウェア感染に誘導する事例を観測しています。

まず、件名などにユーザの関心を引きやすい単語を用いたメールの事例です。例えば、3月頃からはCOVID-19に関する情報提供を装った、マルウェアを含む英文メールの検出が増加しました。同様に、日本語のメールでも「在宅勤務」、「風邪」、「賞与」といった単語が用いられる事例を観測しています。

続いて、マルウェアを含むメールを送信する時間を攻撃者が工夫したと考えられる事例を紹介します。図-1は、9月に不審なMicrosoft Officeドキュメントを検知するシグネチャで検出したメールの件数を、受信した時刻ごとに集計したグラフです。図の縦軸は対象期間における当該シグネチャの総検出件数を100%として正規化しています。グラフからは、日本国内にある企業の標準的な勤務時間帯に合わせてメールが送信される傾向が見て取れます。この傾向には複数の要因があるものと考えられますが、その1つとしてメールを送信する時刻を攻撃者が意図的に選んだ可能性を示唆しています。

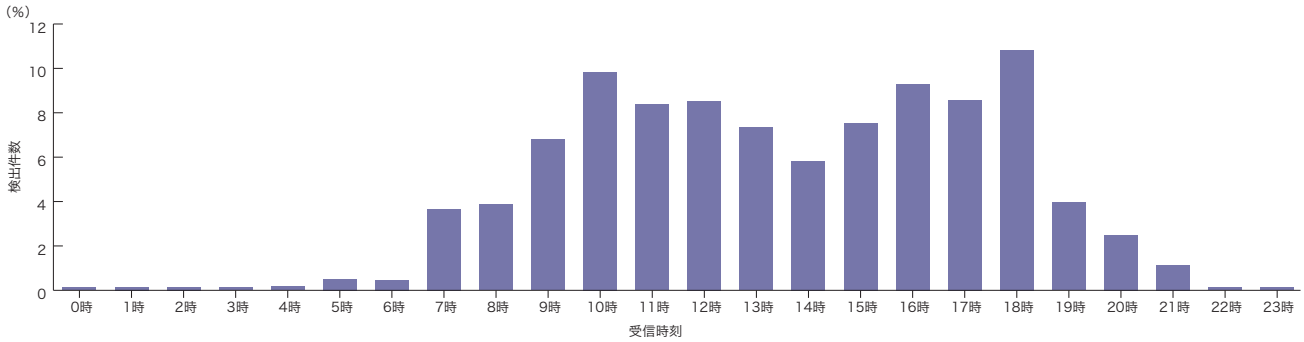


図-1 不審なMicrosoft Officeドキュメントを含むメールの時刻毎の受信件数（2020年9月）

＊7　Mirai亜種（XTC）による感染活動の観測（https://wizsafe.iij.ad.jp/2020/05/967/）。

1.3 セキュリティトピックス

本節では、2020年にSOCで観測した攻撃の中で、アナリストが注目したトピックについて取り上げます。

1.3.1 SSL-VPN製品の脆弱性

Virtual Private Network（VPN）はインターネットなどを通じて組織外から組織内のシステムに接続する際などに使用されます。2020年にはCOVID-19によって勤務形態が急速に変化し、在宅勤務を実現するためにVPNを導入する企業が更に増加しました。このように多く使用されたと思われるVPNですが、組織外から組織内へ接続する仕組みであるため、脆弱性対策には一層の注意が必要です。VPN製品の脆弱性を悪用され、情報が漏えいした事案は2020年にも発生しています。VPN通信には、SSL/TLSで通信を暗号化する方式があり、2019年にはこの方式を用いる製品について複数の脆弱性が公開されています[*8][*9]。2019年に公開されている脆弱性ですが、適切に対処がされておらず、これらの製品を標的とした攻撃が2020年に確認されています[*10][*11]。

SSL-VPN製品を標的とする攻撃として、SOCではFortinet社のFortiOSの脆弱性（CVE-2018-13379）、及びCitrix Systems社のCitrix Application Delivery Controller・Citrix Gatewayの脆弱性（CVE-2019-19781）を狙う通信を観測しています。

■ Fortinet社FortiOSの脆弱性（CVE-2018-13379）を狙った攻撃の観測

図-2に、IIJマネージドIPS/IDSサービスにて検知したCVE-2018-13379を狙う通信の割合を示します。なお、図の縦軸は対象期間における当該シグネチャの総検知数を100%として正規化しています。

当該脆弱性はFortinet社のFortiOSにおけるSSL-VPNの脆弱性で、悪用されると認証なしでリモートから当該製品上の任意のファイルが読み取られる恐れがあります。11月4日及び12月11日に特に多く観測しており、それぞれ全体の10.27%、10.83%を占めています。当該脆弱性を狙う通信は年末にかけて増加傾向にあり、12月の検知数が全検知の37.93%を占めています。前月の11月には当該脆弱性の影響を受けるホストのリストがインターネット上に公開されていました[*12]。これが12月に検知件数が増加した要因になった可能性も考えられますが、関連性を示す明確な証拠は見つかっていません。

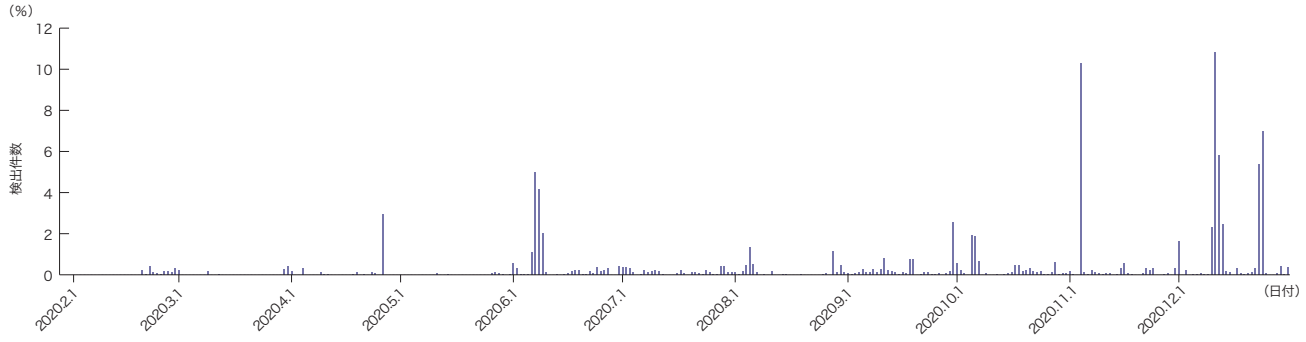


図-2 CVE-2018-13379の検知割合（2020年2月～12月）

＊8　JPCERT/CC、「複数の SSL VPN 製品の脆弱性に関する注意喚起」（https://www.jpcert.or.jp/at/2019/at190033.html）。
＊9　JPCERT/CC、「複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起」（https://www.jpcert.or.jp/at/2020/at200003.html）。
＊10　BAD PACKETS、OVER 14,500 PULSE SECURE VPN ENDPOINTS VULNERABLE TO CVE-2019-11510（https://badpackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/）。
＊11　BAD PACKETS、OVER 25,000 CITRIX (NETSCALER) ENDPOINTS VULNERABLE TO CVE-2019-19781（https://badpackets.net/over-25000-citrix-netscaler-endpoints-vulnerable-to-cve-2019-19781/）。
＊12　JPCERT/CC、「Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性（CVE-2018-13379）の影響を受けるホストに関する情報の公開について」（https://www.jpcert.or.jp/newsflash/2020112701.html）。

■ Citrix Application Delivery Controller・Citrix Gatewayの脆弱性（CVE-2019-19781）を狙った攻撃の観測

図-3に、IIJマネージドIPS/IDSサービスにて検知したCVE-2019-19781を狙う通信の割合を示します。なお、図の縦軸は対象期間における当該シグネチャの総検知数を100%として正規化しています。

当該脆弱性はCitrix Systems社のCitrix Application Delivery Controller及びCitrix Gatewayの脆弱性で、悪用されると認証なしでリモートから任意のコードを実行される恐れがあります。2月18日及び3月13日に特に多く観測しており、それぞれ全検知の13.23%、10.36%を占めています。3月以降は検知件数が減少傾向にあるものの、当該脆弱性を狙う通信は12月まで断続的に観測しています。11月や12月に検知件数が増加している期間もあることから今後も注意が必要です。

■ 対策

CVE-2018-13379及びCVE-2019-19781の脆弱性は2019年に公開されたものですが、2020年の1年間を通して観測しています。対象製品で影響があるバージョンを利用している場合には、修正されたソフトウェアに更新するなどの対応が必要です。VPNに限らず、組織内で使用されている製品の脆弱性情報については、継続的に確認することをお勧めします。

1.3.2 EmotetやIcedIDの観測情報

本項では、2020年に話題となったマルウェア「Emotet」、「IcedID」について取り上げます。はじめにEmotetの特徴を説明し、IIJセキュアMXサービスやIIJセキュアWebゲートウェイサービスで検出されたEmotetに関連する観測情報についてまとめます。次に、IcedIDの特徴を説明し、IIJセキュアWebゲートウェイサービスで検出されたIcedIDに関連する観測情報についてまとめます。

■ Emotetの観測情報

日々、メールを利用しマルウェアの感染を広げる攻撃が行われています。その中でも最たるものはEmotetの感染を引き起こす攻撃で、2020年に猛威を振るいました。Emotetはもともと金融情報などを窃取するバンキングトロジャンと呼ばれるマルウェアでしたが、新たな機能を追加し形態を変化させています。具体的には、自身の拡散機能、ボットネット機能、別のマルウェアを配布するローダ機能が追加されています。自身の拡散機能は感染したコンピュータからメールアドレス、アカウント情報、メール本文、添付ファイルなどのデータを窃取し、C&Cサーバに情報を送信します。更に、Emotetは窃取した情報をもとに送信者に送る形でなりすましたメールを送信し、添付ファイルを開くように誘導します。このような特徴から、Emotetは強力なマルウェアの1つと言えます。Emotetの感

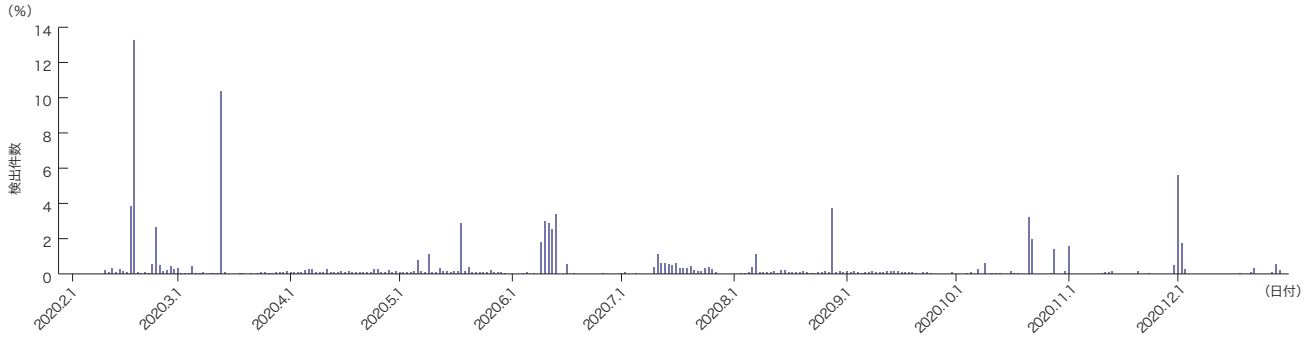


図-3 CVE-2019-19781の検知割合（2020年2月～12月）

染拡大手法としては、docファイルを添付したメールや、docファイルをダウンロードするURLをメール本文や文書ファイルに記載したものが知られています。また、9月には新たな手法としてdocファイルをパスワード付きZIPファイルに圧縮し、送付するという手法も確認されています[*13]。パスワード付きZIPファイルは、圧縮されたファイルの内容を確認できないことから、アンチウイルスやサンドボックスなどによるファイル内容の検査ができません。そのため、パスワード付きZIPファイルは、従来のdocファイルをそのまま添付する形と比較して、ユーザの手元に届いてしまう可能性が高まります。

JPCERT/CCの観測では、7月頃にEmotetに関するメールの配信活動が確認[*14]されました。更にCiscoは、その後活動が継続[*15]したことを報告しています。10月末から活動が少なくなりましたが、12月下旬にEmotetの配信活動が再開[*16]されています。

SOCでは、Emotetに関する攻撃を7月から9月にかけて観測しています。特に9月はEmotetに感染させる攻撃が急増していることを確認しました。

図-4に、7月から10月までにIIJセキュアMXサービスで検出した攻撃について、Emotetに関連する検出割合を示します。図の縦軸は対象期間におけるEmotetに関連する総検出件数を100%として正規化しています。

7月下旬からEmotetの観測が増加していることが分かります。その後、9月15日頃を境に急増し、9月18日にピークを迎えています。

Emotetの通信はIIJセキュアWebゲートウェイサービスでも検出されていました。IIJセキュアWebゲートウェイサービスでは、Emotetに関連するWebアクセスとして、次の2種類を検出していました。

1. Emotetに感染させることを意図したマクロを含む、Microsoft Word 97-2003(doc)形式のファイルをダウンロードする通信
2. 感染後のEmotetによる、Command and Control(C&C)サーバとの通信

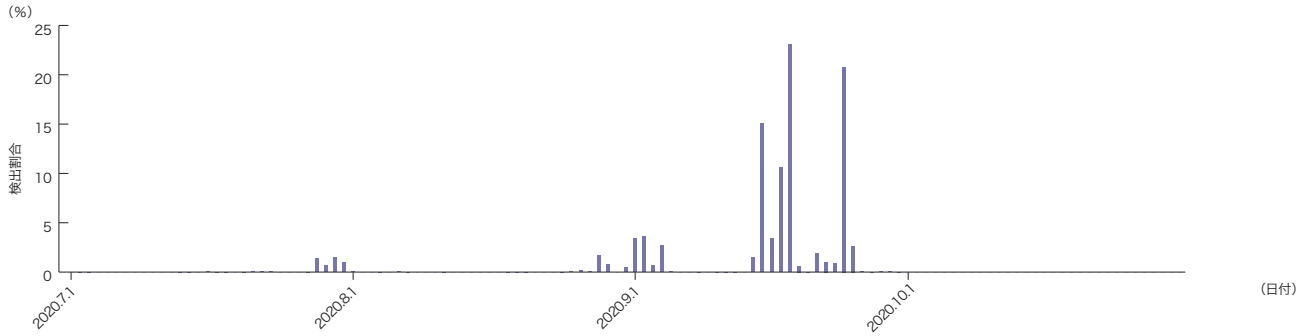


図-4 メール受信時におけるEmotet検出傾向(2020年7月〜10月)

*13 独立行政法人情報処理推進機構 セキュリティセンター、「Emotet」と呼ばれるウイルスへの感染を狙うメールについて 相談急増／パスワード付きZIPファイルを使った攻撃の例(2020年9月2日 追記)」(https://www.ipa.go.jp/security/announce/20191202.html#L13)。
*14 JPCERT/CC、「マルウエア Emotet の感染に繋がるメールの配布活動の再開について (追加情報)」(https://www.jpcert.or.jp/newsflash/2020072001.html)。
*15 Cisco Japan Blog、「活動再開:2020 年の Emotet アクティビティの分析」(https://gblogs.cisco.com/jp/2020/11/talos-emotet-2020/)。
*16 JPCERT/CC、「Emotet などのマルウェア感染に繋がるメールに引き続き警戒を」(https://www.jpcert.or.jp/newsflash/2020122201.html)。

図-5に、7月から10月までにIIJセキュアWebゲートウェイサービスで検出したEmotetに関連する通信の検出割合を示します。図の縦軸は対象期間におけるEmotetに関連する総検出件数を100%として正規化しています。

2019年のIIR定期観測レポート[*17]ではHEUR:Trojan.MSOffice.SAgentの検知のみでしたが、2020年には加えてTrojan-Banker.Win32.Emotetも検知しています。HEUR:Trojan.MSOffice.SAgentではEmotetをダウンロードするdocファイルを検知しています。Trojan-Banker.Win32.Emotetで検知したファイルはすべてEmotetであることを確認しています。HEUR:Trojan.MSOffice.SAgentは7月21日から検知しており、7月28日にピークを迎えています。また、Trojan-Banker.Win32.Emotetは9月2日から検知しており、9月3日にピークを迎えています。

■ IcedIDの観測情報

7月から続いたEmotetが減少した11月には、IcedIDと呼ばれるマルウェアの感染を広げる攻撃を観測しました。IcedIDはもともとEmotet同様バンキングトロジャンの一種でしたが、現在ではこの機能に加えて他のマルウェアのローダとしての機能が追加されています。感染すると、IcedIDは金融機関の資格情報などを窃取し、C&Cサーバに送信します。EmotetとIcedIDはいずれも、マルウェアの拡散方法としてメールが利用されていることや、マルウェア感染方法にdocファイルが利用されている点が共通しています。また、IcedIDは観測初期からパスワード付きZIPファイルを添付し拡散しており、9月以降Emotetが用いた手法と類似していることが確認されています[*18]。このようにEmotetとの共通点が存在しますが、IcedIDはEmotetのようなボットネットの構築を行いません。

図-6に、10月から12月までにIIJセキュアWebゲートウェイサービスで観測したC&Cサーバとの通信回数の割合を示します。図の縦軸は対象期間におけるC&Cサーバに対する合計通信回数を100%として正規化しています。11月3日から通信を観測し始め、11月20日にピークを迎えました。その後12月2日まで継続して通信が発生していることが分かります。また、この11月3日と11月20日では、攻撃に使用されたdocファイルを開いた後の感染までの動作に変化が起きていることが確認されており[*19]、C&Cサーバに対する通信を観測し始めた日と観測した中で最も回数の割合が多かった時期と一致しています。

■ 対策

Emotet及びIcedIDは、どちらもdocファイルを開き、VBAマクロの実行をすることにより感染します。そのため、感染の被害を抑える方法として、ファイルを開いたときにマクロを実行しないようにマクロの自動実行の設定を無効化することが挙げられます。マルウェア感染防止を目的としたマクロの無効化の

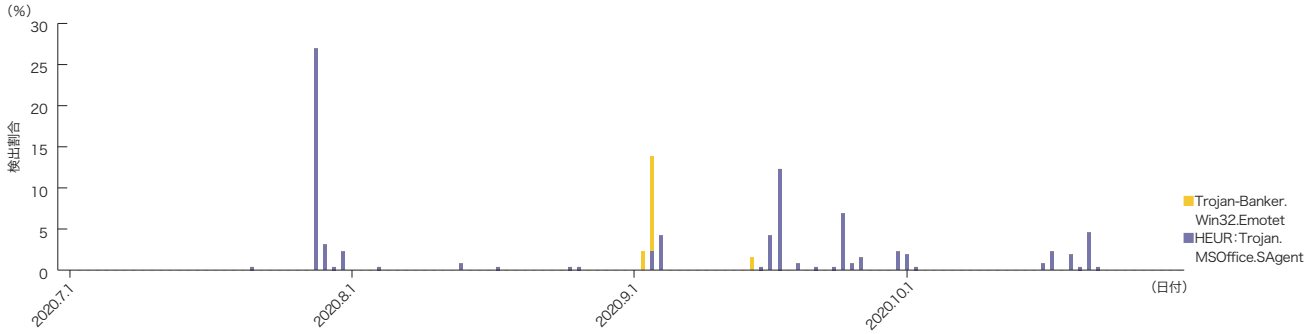


図-5 Webアクセス時におけるEmotet関連通信の検出傾向(2020年7月〜10月)

*17 Internet Infrastructure Review(IIR)Vol.46(https://www.iij.ad.jp/dev/report/iir/046/01.html)。
*18 JPCERT/CC 分析センター(https://twitter.com/jpcert_ac/status/1324561915738091522/)。
*19 IcedIDの感染につながる日本向けキャンペーンの分析(https://mal-eats.net/2020/11/12/analysis_of_the-_icedid_campaign_for_japan/)。

方法については、wizSafe Security Signalの記事[*20]で紹介しています。また、開いても安全だと判断できない添付ファイルを不用意に開かないようにすることも重要です。

1.4 おわりに

本レポートでは、2020年のインシデントカレンダー、各セキュリティサービスの年間統計、SOCアナリストが注目した観測情報を紹介しました。第1.3.1項で取り上げたSSL-VPN製品の脆弱性を狙った攻撃、及び第1.3.2項のEmotetやIcedIDによる攻撃は今後も対象、手段、名前を変えつつ継続していくものと考えられます。また、本稿で取り上げた事例のほかにも、様々なセキュリティ脅威が日々観測されています。第1.2節及び第1.3節で取り上げた内容に関わらず、適切な状況把握及び対処が重要です。SOCでは今後も情報分析基盤で観測した脅威や、セキュリティに関するトピックなどの情報の発信をしていきますので、セキュリティ対策や業務に役立てていただければ幸いです。

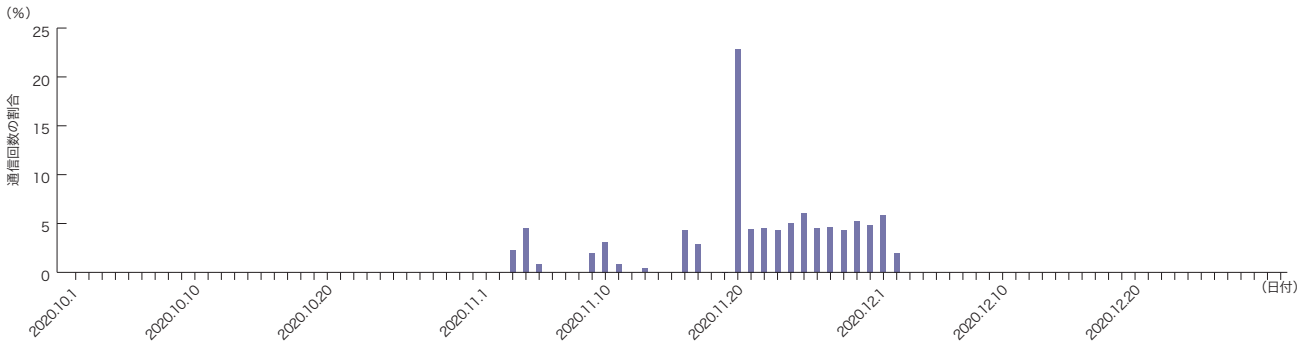
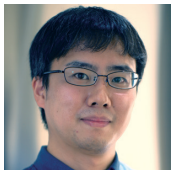
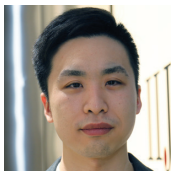


図-6 IcedIDによるC&Cサーバとの通信回数の推移(2020年10月～12月)



執筆者:
鴨川 寛之(かもがわ ひろゆき)
IIJ セキュリティ本部 セキュリティビジネス推進部 セキュリティオペレーションセンター

執筆者:
小林 智史(こばやし さとし)
IIJ セキュリティ本部 セキュリティビジネス推進部 セキュリティオペレーションセンター



執筆者:
森下 瞬(もりした しゅん)
IIJ セキュリティ本部 セキュリティビジネス推進部 セキュリティオペレーションセンター

執筆者:
宮岡 真平(みやおか しんぺい)
IIJ セキュリティ本部 セキュリティビジネス推進部 セキュリティオペレーションセンター

*20 マルウェア感染対策を目的としたVBAマクロ実行の無効化(https://wizsafe.iij.ad.jp/2020/09/1044/)。

IIJのRPKIの取り組み

2.1 経路ハイジャックとは

インターネットはAS(Autonomous System)番号と呼ばれる2バイトもしくは4バイトの数字(例えばIIJは2497)で識別される組織(ネットワーク)が相互に接続することで形成されています。AS間はBGP(Border Gateway Protocol)というルーティングプロトコルで接続、各ASが自身で使用するIPアドレスを経路情報として相手に広告し、それが世界中に伝搬することで地球の反対側からパケットが届くという仕組みです。

各ASが使用するIPアドレスはIANA(Internet Assigned Numbers Authority)機能から地域ごとに委任されたRIR(Regional Internet Registry、アジアはAPNIC:Asia-Pacific Network Information Centre)、更に国ごとのNIR(National Internet Registry、日本はJPNIC:Japan Network Information Center)により厳密に管理され、これらの管理組織から割り振りを受けます。各ASがBGPで経路を広告する際、自身が割り振りを受けたアドレスのみを正確に広告すれば問題はありませんが、何らかの理由により割り振りを受けていないIPアドレスを広告したらどうなるでしょうか。例えばIIJホームページ(www.iij.ad.jp)のIPv4アドレス202.232.2.164を含む経路202.232.0.0/16は当然IIJのみが経路広告すべきですが、IIJではないどこかのASがこの一部である202.232.2.0/24を経路広告するとIIJホームページ宛のパケットはこのASに届いてしまいます(ルーティングの原則として経路長のより長い経路が優先されます)。IIJホームページであれば実質的な影響はあまりありませんが、これがDNSサーバやオンラインバンキングのページだった場合、その影響は容易に想像できるでしょう。

このような事象は経路を乗っ取ることから一般に経路ハイジャックと言われますが、この手のトラブルは現実のインターネットで日常的に発生しています。例えば、著名な動画サイトであるYoutubeのアドレスをGoogleでないASが経路広告してサービスが停止したり、BitCoin関連サイトのアドレスを別のASが経路広告しBitCoinが不正に持ち出されたと言われる事件も発生しています。それではなぜこのようなトラブルが発生してしまうのでしょうか。先に述べたBGPによる経路広告は各ASの自己申告です。自身と接続する相手のASが広告する経路が正当なものかどうか確認するには、日々更新される無数のIPアドレスの割り振り情報を把握し、それをルータに反映させる必要があるため全く現実的ではなく、ほぼ無条件に受け入れるしかありません。このように、現在のインターネットはある意味非常に危ういバランスの上で成り立っているとも言えます。

2.2 RPKIの概要

インターネットがここまで不可欠な社会基盤となった今、このような状況を放置するのは社会全体にとって大きなリスクであり、これを改善すべく考案されたのがRPKI(Resource Public-Key Infrastructure)です。RPKIのアイデアが考案されたのは1998年頃と日本でもやっとインターネットが普及してきた時期であり、研究者の先見の明には驚くばかりです。

RPKIの仕組みを一言で言えば、リソース(IPアドレスやAS番号といったインターネット番号資源)の正当性を電子証明書(X.509)により証明・検証可能にする仕組みです。先に述べたとおり、IPアドレスの割り振りを管理しているのはIANA、RIR、NIRですから、これらの運営組織がツリー構造(正確には5つのRIRを頂点とするツリー)になり、リソースが正しいことを電子証明書で担保します。その情報を使う利用者は、この電子証明書を用いてリソースが正しいことを認知します。RPKI自体はBGPルーティング以外にも使える汎用的な仕組みですが、ここではBGPルーティングに限定して述べます。

IPアドレスの割り振りを受けたASは自身がBGPで経路広告する予定のIPアドレス、その最大経路長及び広告元AS番号をNIRの管理するRPKIシステムに登録し、RPKIシステムがこれに対する電子証明書を発行します[*1]。この電子証明書をROA(Route Origination Authorization)といいます。

このROAを利用するユーザはツリー構造の頂点を示すTAL(Trust Anchor Locator)と呼ばれる事前情報を頼りに、RIR、NIRとツリーを辿りながらROAを取得、検証し、手元に検証済みデータ(VRP:Validate ROA Payload)として保持します。このVRPをルータに提供するのがキャッシュサーバの役割で、RPKI-RTR(RPKI to Router Protocol)というプロトコルを介してBGPルータに情報を供給します。BGPルータは受け取った情報をもとに、経路広告を受けた際にその内容がVRPに照らして正しいかを検証します。例えば、IPアドレス202.232.0/16、最大経路長/17、AS番号2497というVRPがあった場合、IPアドレス202.232.2.0/24、AS番号64496という経路広告は不正であり、これを受信しないことで経路ハイジャックを防ぐことができます。このようにRPKIの情報(ROA)を用いて受信経路の広告元ASを検証することをROV(Route Origin Validation)といいます。検証結果をどう扱うかは各ASの運用ポリシーに委ねられますが、現在は明確に不正な場合のみその経路を受信せず破棄するのが一般的です(この理由は後述します)。

2.3 RPKIの現状

2021年1月現在、インターネット上で交換されるBGP経路情報はおよそ93万経路(IPv4 83万、IPv6 10万)ですが、これに対して有効なROAの数はおよそ21万です。昨年10月時点でのROAはおよそ19万でしたから、4ヵ月で2万も増えており、まさに普及の真っ最中といった状況です。図-1はBGP経路(93万)に対して、ROAで検証可能な経路と検証不可能な経路の割合を示しています。順調に増えているとはいえ、まだ7割を超えるBGP経路は対応するROAが存在せず、ROAを使った広告元ASの検証を行うことができない状態です。先の説明で、現在のROVは明確に不正な場合のみ経路を破棄するのが一般的であると述べましたが、その理由がこれであり、検証不能で正当性が不明なものも受け入れざるを得ない状況です。RPKIが更に普及しすべてのIPアドレスが検証可能になることが期待されますが、それには相当な時間を要するでしょう。

AS別で見ると、BGP経路の存在するAS約71,000のうち約20,000はそれを広告元ASとするROAが存在しています。最も多いASで、そのASを広告元とする約9,600のBGP経路に対して約4,000のROAが存在しますが、このASは経路長/最大経路長/20のROAに加えて、これを細かく分割した/21、/22、/23、/24でもROAを作っていました。通常、このようなケースは経路長/20、最大経路長/24とすれば1つのROAを対応できるはずであり、そのようにする意図は分かりませんが、不必要

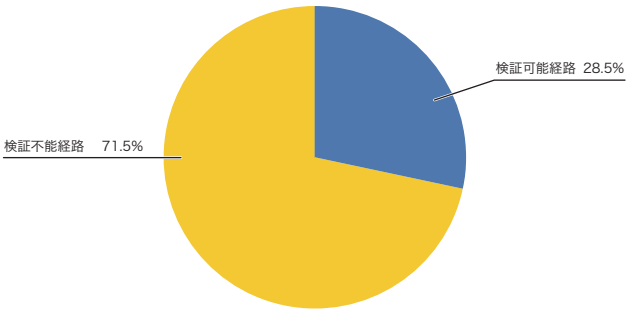


図-1 検証可能経路と検証不可能経路

＊1 IPアドレスの利用者自身が電子証明書を発行することも可能です。この場合は自身がCA(Certification Authority)となり、NRIから割り振りを受けたIPアドレスに関する委任先として信頼性のツリーに組み込んでもらうことになります。

にROAを作成することはルータのリソースをいたずらに消費することになり適切とは言えません。

次に、地域ごとのROA状況を見てみます。図-2はRIRごとのクラスAアドレス割り振り数とROA数を示しています[*2]。

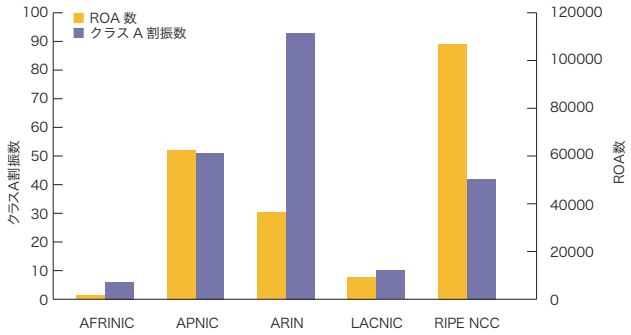


図-2 RIRごとのアドレス割り振り数とROA数

これを見ると、日本を含めたアジア地域を管轄するAPNICやヨーロッパ地域を管轄するRIPE、南アメリカ地域を管轄するLACNICでは割り振りアドレス数に対して多くのROAが作られていることが分かります。また、国単位で見るといくつかの国が100%を達成しているようです[*3]。残念ながら日本の普及率は高いとは言えず、これからの奮闘が期待されます。

ROAの経路長を見てみます。図-3、図-4はそれぞれIPv4とIPv6のROA経路長、及び最大経路長の長さごとの分布を表したものです。一般にインターネット上で交換される経路の長さはIPv4が24まで、IPv6が48までとされていますので、それを超える長さの経路が交換されることはありません。それに対してROAは経路長の長いものが相当数見受けられます。また、図-5はROAの経路長と最大経路長の差異の分布を示したものですが、差がないものが圧倒的に多い半面、差が大きなものもかなり多く存在します。RPKIを使ったROVはあくまでIPアドレス

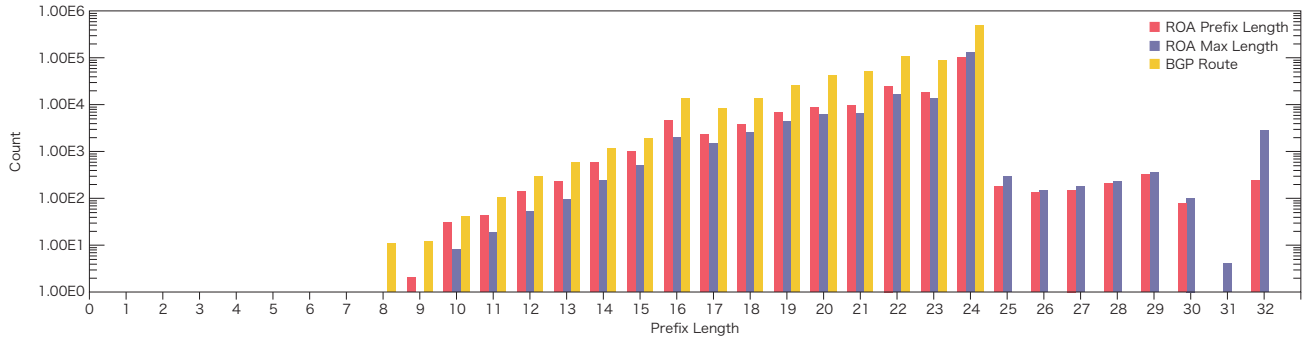


図-3 ROA経路長とBGP経路長(IPv4)

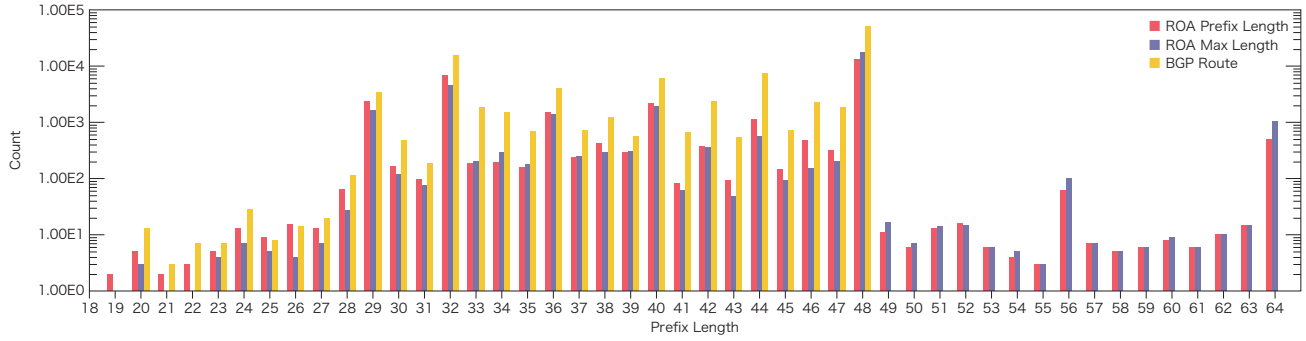


図-4 ROA経路長とBGP経路長(IPv6)

*2　各RIRへの割り振りは、IANAのデータを利用(https://www.iana.org/numbers)。IPv4アドレスの有効利用のため国際的なアドレス移転も行われる現状ではRIRへの割り振りと実際の利用地域には差異が生まれ、正しく利用地域を示すわけではありません。

*3　NLnet Labs、RPKI TOOLS(https://nlnetlabs.nl/projects/rpki/rpki-analytics/)。

とその広告元ASの組み合わせが正しいかを検証しているに過ぎず、広告元ASも含めて詐称されると対処できません。一般に経路ハイジャックは正規のBGP経路より経路長の長い経路を不正に流すことでその経路を乗っ取りますが、実際に広告するBGP経路よりROAの最大経路長が長いということはこのリスクを助長することになります。ですので、BGP広告経路とROAの最大経路長は極力同じ長さにしておくのが望ましいと考えられます。ただ、誤ってROAの最大経路長より長い経路を広告してしまうとROVで破棄されることになって経路障害を引き起こしますので、細心の注意を払う必要があります。

ここまでがROAの状況ですが、このROAを使いROVを行うとどの程度不正な経路が検出されるでしょうか。後で説明しますが、IIJは2020年末にROVを導入しているため、現在IIJ網内には原則として不正な経路は存在しません。そのため少し古いデータになりますが、IIJがROVを開始する以前である2020年8月頃の状況を見てみます。図-6はIIJが受信するBGP経路に対してROVを実施した結果を示しています。"valid"は検証結果が正当、"invalid"は不正、"not found"はROAがなく検証不可能を示します。この図のとおり、2020年8月時点ではおよそ3,000経路、全体の0.3%が不正な経路でした。

この不正な経路約3,000の内訳は図-7のとおりです。およそ半数は広告元ASは正しいもののその経路長が不正なもの(mismatch length)、およそ3割は広告元ASが不正なもの(mismatch origin)、残りの2割が広告元AS及び経路長がいずれも不正なもの(mismatch origin and length)です。経路長が不正なものに関してはその多くが本来AS外に広告すべきではないAS内部の経路長の長い経路を誤って広告してしまっている(漏らしている)ケースと考えられます。一方、広告元AS及び経路長が不正なものは、悪意ある経路ハイジャックの可能性もありますが、あるASに割り振られたアドレスの一部を切り出して別のASから広告するケース(一般にパンチングホールと呼ばれる)でも多く発生していると考えられます。パンチングホールを行う場合、割り振りを受けたアドレスと切り出したアドレスをそれぞれ異なる広告元AS、経路長でそれぞれROAを作成すべきですが、切り出したアドレス分のROA作成を失念しているのではないかと想像します。ただ、実際にはどの

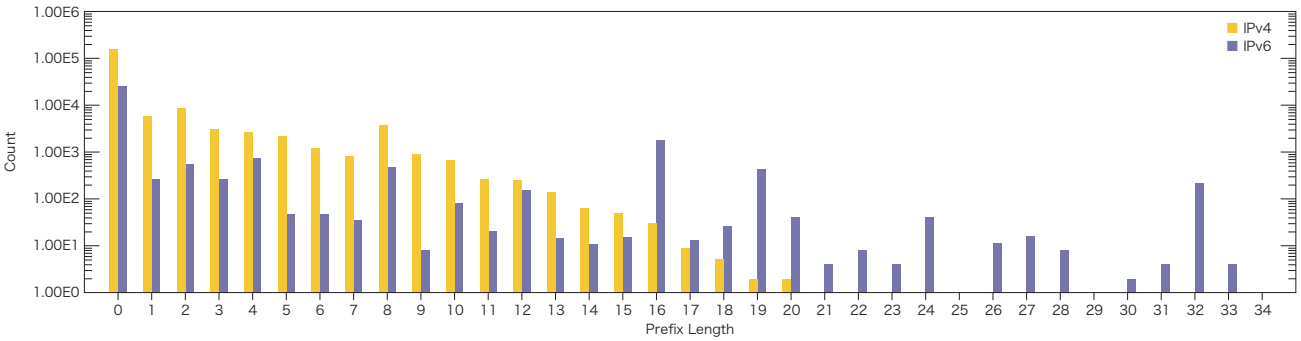


図-5 ROA経路長と最大経路長の差

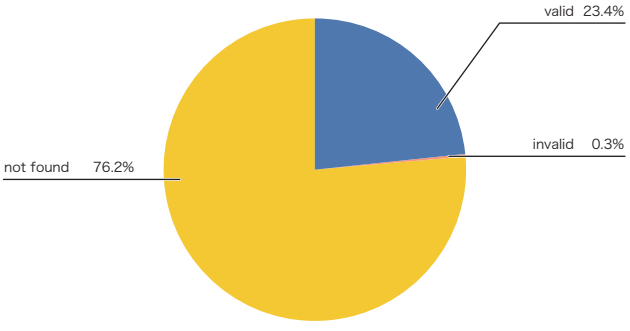


図-6 ROV結果の内訳

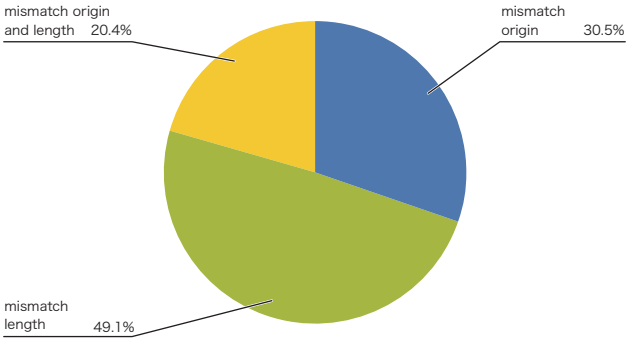


図-7 不正経路の内訳

ケースにおいても本当の意図は当事者にしか分からず、考慮漏れによるものか、設定ミスによる経路ハイジャックか、悪意ある経路ハイジャックかは外部からは判別できません。そのため、ROVで不正と判定された経路を一律破棄することになり、それにより本来失うべきでない経路を失う可能性はゼロではありません。ROAと広告経路を正しく管理することはIPアドレスの割り振りを受けたASの責務であり、ROVで経路を破棄したASには一切非はありません。

ROVで不正と判定される約3,000経路は一律破棄されますが、必ずしもそのすべてで到達性を失うとは限りません。例えば、192.0.2.0/25を破棄したとしても、それを包含する192.0.2.0/24が存在すれば到達性は保たれます。ただし、実際にはこの例の192.0.2.0/25と192.0.2.0/24で広告元ASが異なるケースが多く存在し、この場合192.0.2.0/24が存在したとしても本来到達すべき場所までパケットが到達するかの客観的な判断は困難です。広告元ASが異なる場合を許容すれば約3,000経路のうち約2,500経路が、広告元ASが同じ場合のみ許容すれば約1,500経路は代わりになる経路が存在します。つまり、厳しく見て約500経路（全BGP経路のおよそ0.04%）、緩く見て約1,500経路（同0.15%）はROVにより到達性を失うと推定されます。

もちろん、経路ハイジャック自体を軽減するのがROVの目的ですので不正な経路を破棄することは正しい行為ですが、ROVの導入により仮に不正であってもそれまで成立していた通信を阻害することになる可能性もありますので、その影響は事前に確認するのが望ましいでしょう。

表-1 試験経路の保持状況

経路	RPKI	route views	RIS
93.175.146.0/24	正当	28 AS	287 AS
93.175.147.0/24	不正	13 AS	207 AS
2001:7fb:fd02::/48	正当	N/A	290 AS
2001:7fb:fd03::/48	不正	N/A	205 AS

それでは、世界ではどの程度のASがROVを導入しているのでしょうか。ROAと違い、各ASのROV導入有無を外部から正確に把握することは困難です。各ASの自己申告にはなりますが、RPKIを啓蒙する目的で作成されたWebページhttps://isbgpsafeyet.com/によればおよそ100のASがROVを導入しています。もう少し客観的な情報として、ヨーロッパのRIRであるRIPE NCCが計測目的で広告している経路[*4]があり、この中に意図的にROVが正当あるいは不正となるよう調整した経路が含まれますので、この経路をどの程度のASが保持しているかでROVの導入状況を推測したのが表-1です。route views[*5]及びRIS[*6]は計測目的で各ASと接続し、その経路を収集しているプロジェクトですが、いずれも正当なものに比べて不正な経路を保持しているASは半分から2/3程度でした。ただし、あるAS自体が不正な経路を保持していないからといって必ずしもそのASがROVを導入しているとは限らず、その上流に位置するASがROVを導入すればそこを伝搬した経路を取得している下流のASも不正な経路を保持しなくなります。そのため、この結果がそのままROVを導入しているASを表しているわけではありませんが、ROVの目的である「不正な経路を伝搬させない」という効果は確実に見られます。今後ROVの導入が進めば、この数字も変化するものと思われます。

2.4 IIJの取り組み

IIJもRPKIに取り組んでいます。まず、IIJがJPNICから割り振りを受けたIPアドレスの大半（IPv4 82%、IPv6 100%）に対して2020年末にROAを作成しました。これによりROVを導入しているASを介してIIJのIPアドレスが経路ハイジャックされるリスクを軽減できます。各ASへのROV導入が進めばこの効果はより増していきます。一部できていないものに関しては、特別な事情がありROAを発行してもらっているJPNICのシステムが対応できないことによるもの、割り振りアドレスのすべてもしくは一部を顧客のASで広告していて調整が必要になるもので、いずれ解消する予定です。

IIJが割り振りを受けたIPアドレスのROA作成は順調に進んでいますが、IIJのASであるAS2497が広告元になった経路全体

＊4　RIPE NCC、"Routing Certification Beacons"（https://labs.ripe.net/Members/markd/routing-certification-beacons/）。
＊5　Routeviews、"University of Oregon Route Views Project"（http://www.routeviews.org/routeviews/）。
＊6　RIPE NCC、"RRC00 -- RIPE-NCC Multihop, Amsterdam, Netherlands -- Peer List"（http://www.ris.ripe.net/peerlist/all.shtml）。

で見ると、およそ3割程度しかROAがありません。これは、IIJのサービスを利用する顧客が、IIJのアドレスではなく、顧客自身で直接JPNICなどから割り振りを受けたアドレス(Provider Independent Address)を使い、AS2497を広告元にする場合があることに起因します。ROAの作成はBGPで経路広告するASではなく、アドレスの割り振りを受けた組織が行う必要があり、この場合は顧客自らが行うべきものです。これらのケースではIIJから顧客に対してROAの作成を促していきます。

ROVに関しては、IIJと他のASとの接続点においてROVの導入を進めており、2020年末時点で5割強の接続に導入しました。AS間の接続は一般に、AS同士の対等な接続であるピア、上流ISPに接続するアップストリーム(もしくはトランジット)、顧客に接続を提供するカスタマーの3つに分類されますが、IIJから見たピア及びアップストリームにはすべてROVを導入済みです。IIJから接続サービスを購入いただいている顧客へは現時点では導入できていませんが、顧客との接続点は以前から厳密な経路のフィルタを実施しており、不正な経路の流入はほぼありません。そのため既にIIJ網内には不正な経路はほとんどない状況ですが、それでも顧客にもROVを導入することでより確実に不正な経路を抑止することができますので、早ければ2021年度中にも顧客向けにROVを導入する計画です。

サービス利用顧客も含めたRPKIの導入は顧客の理解や協力が不可欠ですが、RPKIの重要性や必要性はまだ十分に浸透しているとは言えません。RPKIは顧客自身の通信安定性の向上、更にはインターネット全体の安定性向上に繋がる必要不可欠なものと考えますので、様々な場を通じてRPKIの啓蒙を行っています。

2.5 将来に向けて

ここまで説明したRPKIを使った広告元AS検証ですが、これによりインターネット上で日々発生している様々な経路障害すべてに対応できるわけではありません。先に説明したとおり、広告元AS検証はあくまでIPアドレスと広告元ASの組み合わせを検証しているにすぎず、広告元AS自体を詐称された経路ハイジャックは検知できません。

また、経路ハイジャックと並び頻繁に発生するトラブルとして、経路リークと呼ばれるものがあります。これはあるASから受信した経路を本来すべきない別のASに広告し伝搬させてしまう事象で、設定ミスにより発生しがちな事象です。これが発生すると、通信が本来経由すべきでないASを経由してしまい、著しい通信遅延やパケットロスなどの障害が発生します。実際、インターネット上では年に何度かこの事象が発生しており、そのたびに著名なサービスや大きなISPがその被害を受け、その影響の大きさから一般のニュースにもなるほどの障害に発展しています。広告元AS検証はこの経路リークに対しては無力です。

このような事象に対応するべく様々な技術や仕組みが検討、議論されており、一部では標準化や導入が進んでいるものもありますが、RPKIのアイデアは2000年より前に考案されたものが今になってやっと普及してきたくらいですから、その浸透には長い時間を要することでしょう。それでも、ここまでインターネットが社会的に重要な基盤となった今、ひとたび大きな障害が発生すればその影響は計り知れません。ですので、インターネットを形成する各ASは不断の努力を持ってこれに望むべきであり、IIJもその一員としてインターネットコミュニティと共に精力的に取り組んで行きます。

執筆者:
堀 高房(ほり たかふさ)
IIJ 基盤エンジニアリング本部 ネットワーク技術部 ネットワーク運用課長。
IIJバックボーンネットワークの運用に従事。

2020年を超えて –オリンピック・放送制作・インターネット–

3.1 はじめに

「2020年」はどのような一年として人々に記憶されたでしょうか。誰にとっても人生はそれぞれ異なるものですが、多くの人に2020年は「コロナ禍が始まった年」という出来事で共有され思い出されるでしょう。新型コロナは猛威を奮いつつ、広範囲にわたり社会に大きな影響を与えました。その1つが東京オリンピック・パラリンピック競技大会の延期です。2020年は、その意義に様々な論があるにせよ「東京でオリンピック・パラリンピックが開催された年」として記憶されるはずだったのです。

3.2 オリンピック・パラリンピックと放送制作

放送、特にテレビジョン放送は近年ビッグイベント、殊にオリンピックやワールドカップのような巨大スポーツイベントと分かち難く結びつくようになりました。視聴率を求めるメディアは大規模なイベントを欲し、イベント主催者はその影響力をより効果的にするためマスメディアに依存します。広い帯域の電波を用いた放送はリッチメディア(視覚、聴覚)という特性を持つため、世界的に多くの人が関心を寄せるビッグイベントの模様を伝えるにあたり非常に支配的なポジションに位置しています。全世界で各国市民がほぼ同時にリッチメディアを受容できる仕組みは、放送以外にはありません。インターネットはこのような超大規模配信については未だ苦手としています。

その中でもオリンピック・パラリンピック放送は特別なものです。極めて多くの競技が短期間のうちに実施される中で番組が制作され、世界中に配信されています。オリンピック・パラリンピックの場合、2008年以降はIOCによって設立されたOlympic Broadcasting Services(OBS)がすべての競技の模様を国際映像として制作しており、契約を結んだ各国の放送局はこの供給を得ています。日本の場合はJapan Consortiumという放送局の連合体がIOCと契約を結んでいます。供給された映像は各国語のコメンタリー(アナウンサーや解説者による実況など)や独自取材映像は入っていませんので、それらを挿入するため、各国の放送局においても制作作業が実施されることになります。こうした大規模イベントでは急なデマンドも発生しがちです。予定にない(=期待されていなかった)選手が決勝に勝ち上がったために中継を急遽編成することになったり、注目度の高い競技の時間が重なったり…こうした不確定要素に対しては、どうしても制作上の資源不足が生じます。

一般的にこのようなイベント番組制作は「現場」で実施されています。例えばスタジアムの駐車場に大型トラックを改造した中継車を派遣し、その中にスタジアム内からのカメラやマイクを集約し、車の中でスタッフが映像や音声の編集作業を実施する。ビデオスイッチングが代表的な編集作業の例ですが、それ以外にもビデオカメラの絞り制御やマイクの音響調整など、制作には非常に多様な作業が求められます。それ故、制作には多くの放送エンジニアの稼働が必須となるのです。

中継車は独立して機能することが前提で、制作に不可欠な機器がすべて搭載されます。局舎にある機器と同等の機能を持ち、入出力の数が少し抑えられた機器が車の中に装備されています。しかし、その機器は中継車の非稼働時は全く用いられません。スペースに制約のある中継車の機器を都度着脱するのは現実的ではないからです。ただし高価な機器などの場合はどうしても使い回しをせざるを得ず、現場に持ち込まれることもあるようです。いずれにせよ、効率が良い話ではありません。

更に同時進行するイベントへ対応する場合、放送エンジニアの稼働確保は困難な課題となります。放送エンジニアは機器を操

作するために現場に赴かなければならず、その結果移動時間のオーバーヘッドが生じます。するとイベントの掛け持ちが不可能になってしまい、複数の放送エンジニアをそれぞれの現場へ別途充当しなければならなくなるからです。また日帰り圏にない箇所で開催されるイベントを中継するため、放送エンジニアが遠方のホテルに連泊することもよくある話です。

3.3 リモートプロダクションへの流れと壁

それを、IPが解決できるかもしれないと思われるようになりました。IPを用いた遠隔放送番組制作、「リモートプロダクション」です(図-1)。端的に言えば、カメラやマイクにIPゲートウェイを備え付け、現場で収録した高い品質のまま映像・音声をIPによって遠距離へ運び、制作作業は局舎で実施しようというものです。すると、1つの場所にリソースを集めることで成立していた番組制作の方法論が変わります。現場に持っていく機器は最小限のもので良くなりますし、作業のために移動する必要もありません。経費削減が図れるだけでなく、効率も良くなり、作業品質もアップすることは間違いありません(出張が好きなエンジニアには、残念なニュースかもしれませんね。)。

機器やそれを扱うエンジニア・オペレータを集約し効率良く運用したいという要望は、ICT業界ではよくある話でしょう。この十数年オンプレミスからクラウドへ、ソリューションからサービスへといった継続的な流れの中で、常にICTの導入による省力化や投資のスリム化が求められてきました。ネットワーク技術の進展に伴い、この傾向が放送制作の分野にも訪れたと見ることもできます。この2、30年来様々なメディアがIPを用い流通するようになった中、最後の大物として残っていた領域が放送制作技術だったのです。

10GbEや100GbEといった高速イーサネット普及の後押しもあり、放送機器のIP対応は順調に進みつつあります。この5、6年で急速にIPへの対応が進み、現在では放送機器にはごく当たり前にイーサネットのインタフェースが設けられるようになりました(主にSFP+もしくはQSFPが採用されています)。こうした技術革新を受け、欧米を中心として大規模な放送局設備のIP技術導入が相次いでいます。IP技術を無視しては将来展望が語れないまでに、放送機器分野でのIP技術普及は進みました。

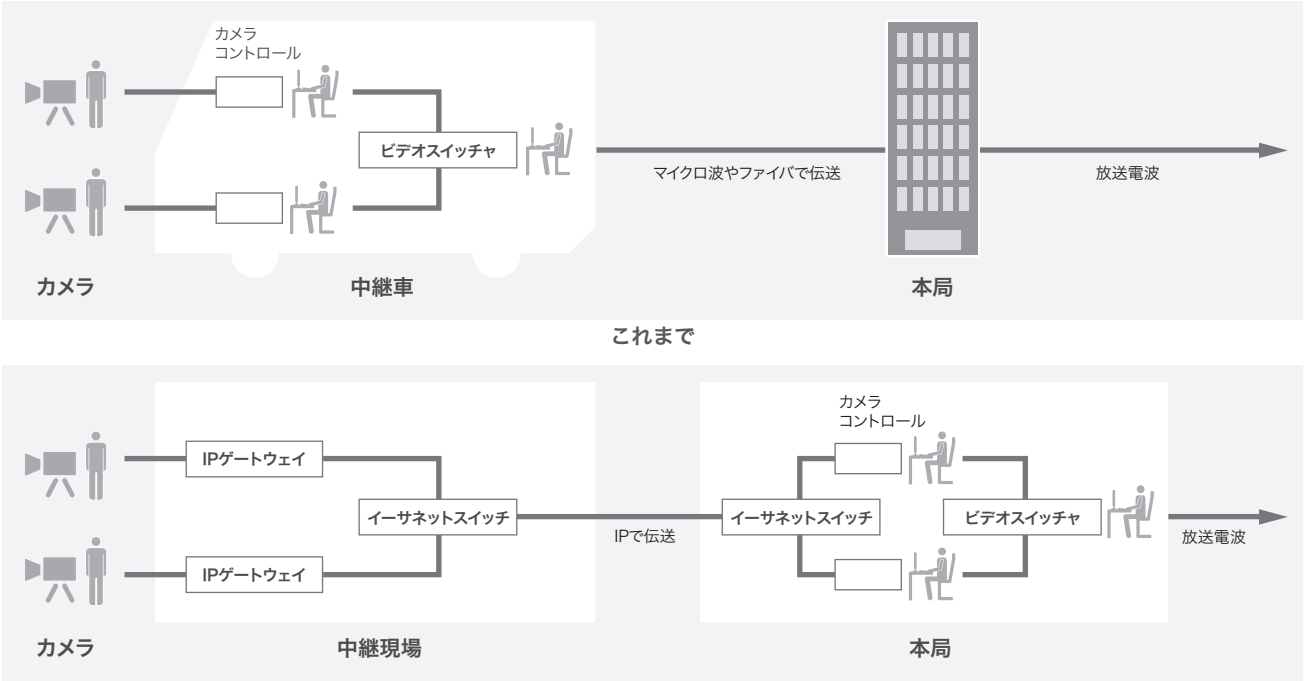


図-1 リモートプロダクションの概念図

局舎内のIP対応と同様、リモートプロダクションを実現するには大容量回線の確保が必須となります。大規模なスポーツイベント中継では10台以上のカメラや何十本にも及ぶマイクが収録のために設営されます。これらのソースを現在の制作クオリティを落とさずに伝送しようとすると、10GbEクラス、あるいは100GbEの回線を複数本確保しなければなりません（フルハイビジョンの映像を圧縮せずにIPで伝送すると1.5Gbps程度、4K映像だと13Gbps程度の帯域です）。これはOTT（Over The Top）向けにネット中継をするのに比べ、段違いにハイクオリティな環境です。こうした大容量回線は通信キャリアからサービス提供されていますが、ほとんどの場合回線は年間契約で、また月額コストも高価です。放送局の観点から見ると、番組単位の予算から支出するという規模感からはみ出てしまいます。敷設のための事前調整もかなりの時間がかかるため、週末のイベントのために回線を3日間だけ敷設するというようなカジュアルな使い方は、まだまだ難しいのが実情です。

リモートプロダクションは「働き方改革」の一種と言えますし、俯瞰すれば「デジタル化」の文脈で捉えることもできるでしょう。デジタル化はワークフローを促進するだけではなく、それを根本から変えてしまう可能性があります。逆に言えば最終的にワークフローそのものの改革を目指さない限り、デジタル化はその効果を最大化できません。しかし、リモートプロダクションのPoCを経た制作現場からはこんな意見も散見されました。曰く「これまで人が集まることで制作の集約化が図られていた現場の手法にメスを入れる形になる」。まさに「密」によって成立していたコミュニケーションを、IPはいわば分断してしまうことが問題となるようです。これは既に技術の問題ではなく、デジタル化に対する組織論の範疇です。少子化を迎える社会に対して産業界がどのように備えるべきか、その試金石という側面をも持ち合わせているようです。

このように、リモートプロダクションを日常的に実施するにはまだ解決すべき課題が残っています。喩えるなら登山道を5合目、あるいは8合目まで登ってきたわけですが、本当に苦しいのはこれからなのでしょう。登山に求められるスキルもギアもバジェットもタイミングも徐々に揃いつつあるのですが、それを一気に揃えるのは難しいと関係者は感じています。登頂を諦め引き返す人も、あるいはおられるかもしれません。

しかし、IPネットワークが寄与できるポイントは他にもあるのではないか。何も始めから世界最高峰を目指すのではなく、もっと「自分がいま頂上まで登れる山」から攻めるやり方もあるだろう。そう思っていた矢先、コロナ禍が世界を覆い尽くしました。そしてリモートプロダクションの導入より遥かに緊急性が高く、誰にとっても喫緊の課題が浮上してきました。それはコロナ禍における職場での感染対策、分かりやすく言えば「3密回避」です。

3.4 リモートワークとネットワーキングの重要な関係…VidMeet Onlineでの試み

こんにち、コロナ禍に対する企業の対策として「リモートワーク」が重要視されています。これまでリモートワークは「働き方改革」的な文脈で取り上げられてきましたが、ウイルス感染に対する非常に有効な策としても注目されるようになりました。それは放送局でも例外ではなく、2020年3月の段階で欧州の放送局におけるリモートワークについてのワークショップが開催されていたほどです。職場の出社人数が制限されてしまったので、これまでの制作に必須とされた体制が構築できない。それを回避するため、自宅から職場へVPNでアクセスし、リモートから放送局舎内のリソースをコントロールする。そのような発表や議論の中には生放送に必須の「スイッチャー」を遠

隔から操作したという剛の者もおり、そこまでやるのか、とその体重の乗せっぷりに驚いたほどです。

それでは、リモートワークを可能とするネットワーキングとはどのようなものでしょうか。筆者はこれこそ2020年に追求すべき課題であると考え、デモンストレーションという形で世に問いました。2020年10月より12月まで有志によりオンラインで開催された「VidMeet Online」です。

VidMeetはVideo over IPについて扱う勉強会として2017年に開始されたイベントです。筆者が主催し、これまで9回のミーティングをIIJにて開催してきましたが、コロナ禍の折り活動停止を余儀なくされていました。そんな2020年の初夏、放送機器やIP機器メーカやプロバイダの有志によるオンラインミーティングが開かれました。各種催し物のオンライン化や中止が進む中、自分たちの手でオンラインイベントを主催できないか議論したのです。方向性が定まっていく中で、イベント名にVidMeetの名前を付けることになりました。VidMeetはコミュニティに貢献する場であり、このイベントにも相応しい名前として評価されたのだと思います。

VidMeet Onlineのテーマは「インターネット・データセンター・クラウド × 放送機器が生む新たな運用スタイル」です。放送機器をデータセンターやクラウドに集約し、それらをインターネットでつないだときに何が起きるのだろう？という関心がありました。このイベントの訴求ポイントは、容易に入手可能なリソースである「リモートネットワーキング」がどのように放送制作現場へ貢献できるかというところにあります。リモートプロダクションより更にフットワークを軽くして、今できることを追求したのです(図-2)。

今回は「データセンターを放送局舎として、また参加各社のオフィスを中継現場として見立てる」というコンセプトのもと、データセンターと参加各社を接続するためにフレッツ光回線

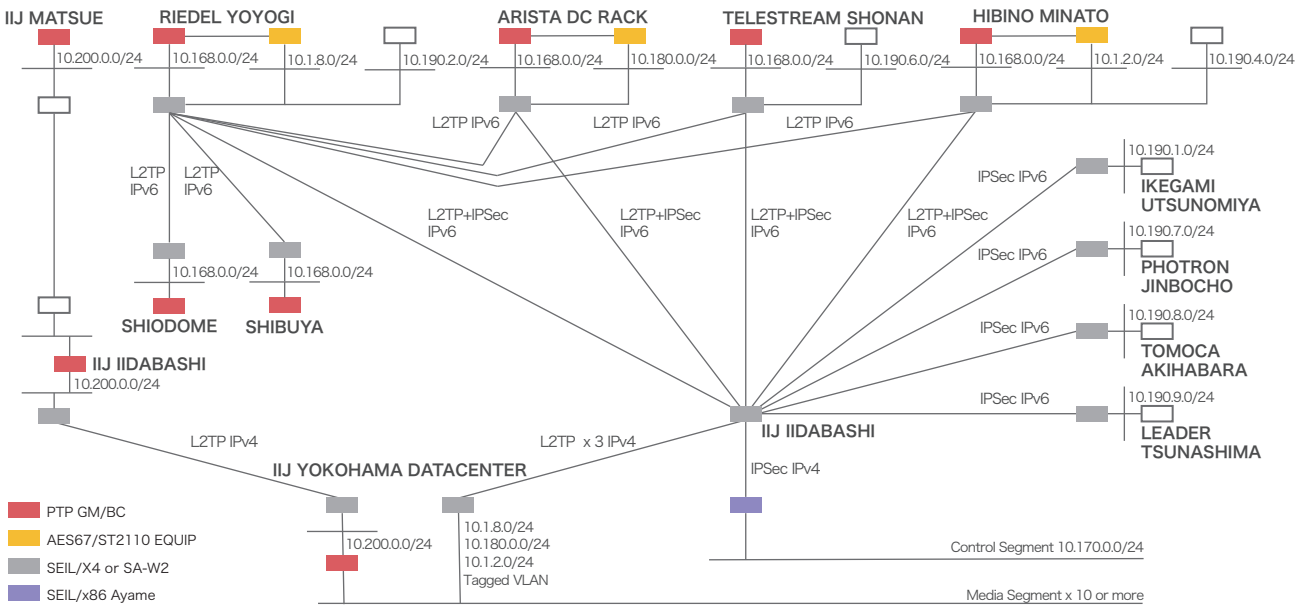


図-2 VidMeet Onlineネットワーク構成

を用い、その接続をインターネットVPNによって確立しました(図-3)。

放送機器をデータセンターに設置しようと決めた理由は2つありました。1つは、局舎システムのアウトソースを考えた際、その移設先としてデータセンターが候補に挙がるはずだからです。すべての放送機器を移せるとは思いませんが、可能性を探ってみたいと考えました。データセンターに移設が可能なリソースは、最終的にはクラウドへの移行も見えてきます。もう1つの理由は、放送機器を大容量インターネット回線に接続し、リモートコントロールしたかったからです。データセンターに設置した放送機器のデモンストレーションをインターネット越しに実現できるならば、その技術はそのままリモートネットワーキングで活用できることを意味します。デモを受けたユーザは、期せずしてこの技術の実用性を証明してみせたことになるわけです。

VidMeet Onlineのデモンストレーションでは次のような実験を実施しました。

- 操作用ハードウェアパネルをオフィスに置き、VPN経由でデータセンターに設置した映像プロセッサを制御
- オフィスで生成した音声パケットをVPN経由でデータセンターの音声プロセッサに投入、ミキシングを実施
- データセンターに設置した映像パケット分析装置をオフィスからWebブラウザ経由で操作
- オフィスに設置した放送カメラ用ロボットアームをインターネットVPN経由で制御
- VPN経由でのネットワークスイッチの設定投入及び運用
- データセンターに設営したビデオサーバを遠隔制御
- PTPパケットをVPN越しに送出し、複数の遠隔地点で放送機器を同期駆動

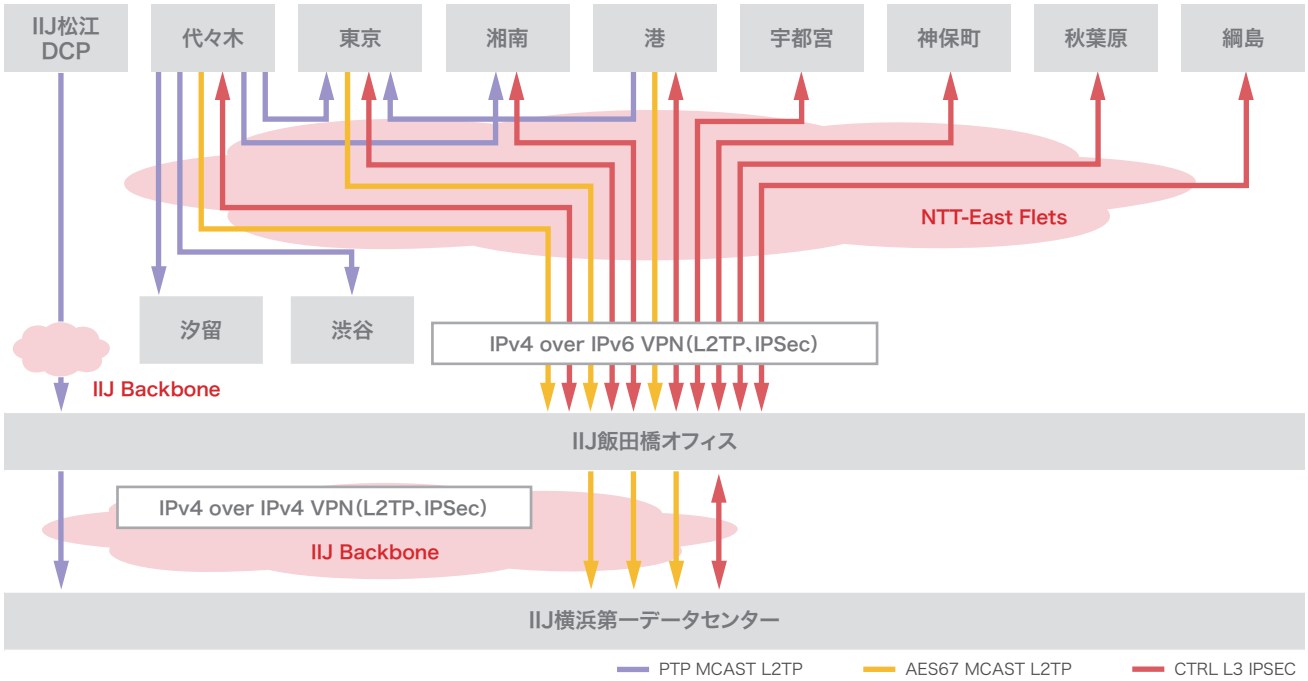


図-3 VidMeet Online VPN上のフロー

またデータセンターにVMware ESXi用のサーバを仮想基盤として整備の上、仮想サーバにアプリケーションをインストールし、主に制御系のサーバを運用しました。

- 仮想サーバにインストールした制御サーバで、データセンター及び遠隔地に設営したビデオサーバの機器制御
- 仮想サーバに監視アプリケーションをインストールし、各種機器のモニタリング
- 仮想サーバ上の制御用メタデータサーバにて、機器間のインターオペラビリティを確認

図-4 ラックマウントされた放送機材

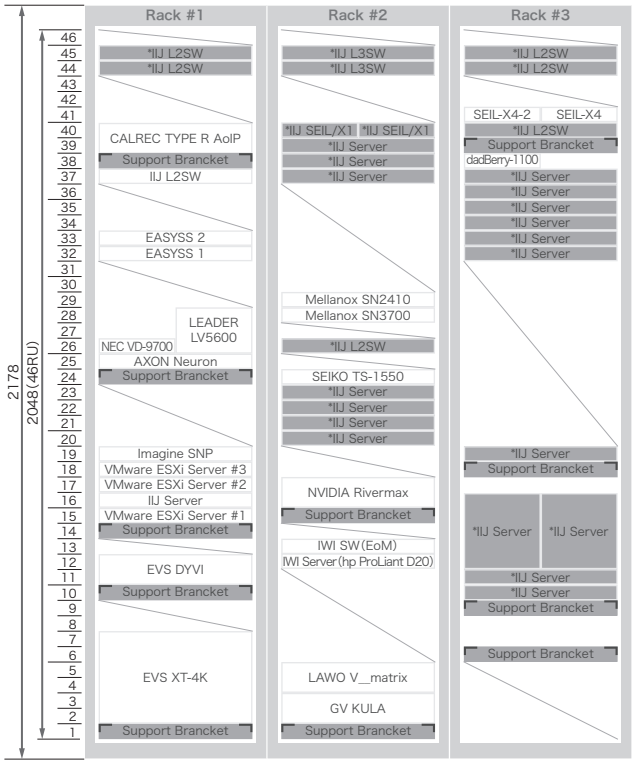


図-5 ラックマウント構成図

普段は通信用のルータやスイッチ、サーバが設置されるデータセンターのラックですが、VidMeet Onlineでは放送局舎や中継車で見かけるような機器が並びました。通信事業者のラックとしては珍しい光景でしたので、許可を受け特別にお目にかけたいと思います(図-4、図-5、表-1)。

実際にVidMeet Onlineのネットワークを構築して感じたのは「案外、実用に足るのでは？」ということでした。VPN構築はL2TP、IPsec、OSPFといった汎用的なプロトコルしか用いておらず、一般的な構成になりました。しかしそのネットワーク

表-1 VidMeet Online参加社一覧

アリスタネットワークスジャパン合同会社 / Arista Networks, Inc.
池上通信機株式会社 / IKEGAMI TSUSHINKI CO.,LTD.
伊藤忠ケーブルシステム株式会社 / ITOCHU Cable Systems Corp.
株式会社インターネットイニシアティブ / Internet Initiative Japan Inc.
株式会社インテリジェント ウェイブ / Intelligent Wave Inc.
エヌビディア合同会社 / NVIDIA Corporation
オタリテック株式会社 / OTARITEC Corp.
サーヴァンツインターナショナル株式会社 / Servants International Corporation
セイコーソリューションズ株式会社 / Seiko Solutions Inc.
Telestream Japan合同会社 / Telestream Japan GK
日本電気株式会社 / NEC Corporation
株式会社テクノハウス / TECHNO HOUSE INC.
トモカ電気株式会社 / TOMOCA Electronics Co., Ltd.
ネットワークアディションズ株式会社 / Network Additions Co., Ltd.
ヒビノ株式会社 / Hibino Corporation
株式会社フォトロン / PHOTRON LIMITED
株式会社マクニカ / Macnica, Inc.
株式会社メディアリンクス / Media Links Co., Ltd.
リーダー電子株式会社 / Leader Electronics Corporation
RIEDEL Communications Japan株式会社 / Riedel Communications Japan KK
One Diversified Japan合同会社 / One Diversified Japan GK

を用いて展開された実験は前述のように非常に幅が広いものとなり、リモートコントロール、あるいはリモートワークを意識した実証として世界的にもあまり例がないイベントになったと考えています。

こうした実験をデモンストレーションという形で2020年10月6日から12月11日にかけて継続実施し、その成果をウェビナーや参加各社のセミナーといった形で公表しました。主催ウェビナーは16回を数え参加者は述べ300人を超えました。各社からのウェビナーや発表資料はアーカイブされていますので、ぜひWebサイト https://vidmeet.tv/ を訪問していただければと思います。

特筆しておきたいのが、このプロジェクトそのものもリモートネットワーキングによって運営されたということです。データセンターへの機器持ち込みや撤収、参加各社でのフィジカルな作業はあったものの、据え付けられた機器はすべてネットワーク経由でコントロールされました。ミーティング及びウェビナーはZoomで実施され、メンバーが物理的に集うことはありませんでした。プロジェクトマネージメントの観点でも、ネットワークは大いに活用できます。今後は「現場にいる重要性」と「オンラインでもできること」をいかに区分していくか、改めて問われるのではないでしょうか。

3.5 ネットワークのたどる先はクラウド

このように、VidMeet Onlineでは放送機器リモートコントロールの技術的可能性を示すことができました。今後はこの知見をいかに実運用に、あるいは実提案に落とし込んでいけるかが鍵となります。中継車などのシステムをモバイルVPN接続することで、クラウドで一元監視できる可能性が出てきました。もちろん現場でのモバイル利用は100%安心とは言い切れず、例えば人が集まるイベント会場などでは輻輳が発生し得ます。クラウド利用を前提とすると回線の選択は更に重要になります。モバイルだけではなくフレッツの利用やクラウド直結ネットワークサービスの導入など、検討すべきシナリオはまだまだあるでしょう。

放送制作や放送局のシステムにおいて、クラウドを利活用するシーンは間違いなく増大する方向にあります。これは他業界においては何年も前から起きている事象であり、放送局においても、Webサーバや動画配信での取り組みは既に始まっています。クラウドはインターネットをはじめとするICT領域における最良の果実の1つであり、利用せずにおく手はありません。その一例が、クラウドを基盤としたネットワーク機器に対する一括管理と監視です。

放送制作システムは規模や演出、つまり番組の内容によって機器の構成が毎回異なります。これまでは現場で機器を組み上げて対応していましたが、IP化するとそう簡単にはいきません。IPアドレスのアサインから始まりネットワークスイッチの設定、PTPの導入、更に機器同士の相互接続の確認や監視設定などが求められます。このように複雑なシステムをIPエンジニアの力なしに組み上げるにはかなりの困難を伴います。放送局でのIPエンジニアの育成はまだ端緒にあり、放送エンジニアが本業の合間を縫って手探りでIP技術を習得しているのが現状でしょう。

このような環境下では、ICT分野で活用されているツールの導入が有効と考えられています。ネットワークスイッチの集中管理アプリケーションや、放送機器監視用モニタツールが代表的な例です。例えばネットワークスイッチの大規模な導入と運用管理は手作業では到底スケールできず、ツールを使った一括で

の管理が効率的です。このようなツールは、毎回環境が動的に変わっていく現場にも適しています。エンジニアの負荷軽減という観点でも、現場に赴かずとも導入や運用ができるツールの存在は大きなサポートになります。「現場に行かなくていい」あるいは「事前に作業ができる」ことは、つまり「3密を回避」することに他なりません。

むしろネットワーキングの良さを実感できるのは、リモート監視や機器の運用といった、ある意味地味な領域からかもしれません。ネットワーキングは自分の手元でも世界のどこでも区別なく作業できるようにするための技術であり、機器がつながることで今まで不可避だった作業の手間を軽減できるかもしれない。逆に考えると、ネットワーキングは作業品質をより高めるために欠かせない技術であるともいえます。リモートプロダクションとまったく同じメリットが目指せるわけです。

このようにネットワーキングを用いたサービスやソリューションは、放送制作の現場に寄与できる余地がまだまだあることが示されました。更に開拓すべき領域もたくさん残されています。

ここで一点指摘しておきたいのは、こうしたネットワーキングの応用は必ずしもコロナ禍によって生み出されたものではないということ。これまでも存在していた手法が、コロナ禍によって誰の目にも明らかに映し出された現象だということです。実際ICT分野の多くのエンジニアはそのように仕事を続けてきています。自宅からのリモートワークはもちろん、オフィスからデータセンターやクラウド上にあるサーバを操作することもネットワークの応用です。こうした技術がコロナ禍への対策として有効と認められ、あらためて2020年になって着目された事象だったといえるでしょう。

3.6 クラウドとソフトウェアの大きな可能性

もう一点、重要な動きが起きています。それは「ソフトウェア化への流れ」です。もともと放送機器は放送局にしか販売できない、非常に狭い領域をターゲットとした商材です。放送局の数は限られており、かつ新規参入しにくい分野でもあるため、どうしても製品のコストは増加します。そこでコモディティであるIAサーバを利用したソフトウェア化への流れが起きたのです。もちろん、映像や音声のリアルタイム処理をするような機器ではLSIやFPGAがプロセッサとして採用されることが多く、こうした製品は今後も専用ハードウェアの形を取り続けるでしょう。一方、制御サーバの類はそこまで高いプロセッシング能力を必要とせず、CPUで賄える場合が多いのです。すると製品はソフトウェアのみで実装でき、専用のハードウェアを自社で開発・維持する必要がなくなるため、保守性や拡張性の面から見てもメリットが生じます。

ソフトウェア化の流れはこの10年で加速しました。かつてはIAサーバを用いたアプライアンスも多く見かけましたが、最近ではソフトウェア単体での販売も本格化してきています。仮想化技術への対応も進み、更に一歩進んでメーカが自らSaaS提供を始める事例も増えつつあります。SaaSの母体となる環境は、言うまでもなくクラウドです。

将来的にはソフトウェア化された制御サーバはクラウドで稼働させ、局舎や中継車に置かれた放送機器をネットワーク越しにコントロールする、という形態が一般化するでしょう。制御サーバをクラウドで動かすことで、多くのシステムを一括管理できるメリットが生じます。また既設のネットワークやVPNと組み合わせれば、制御サーバへのアクセスが場所を問わず可能になります。つまり手元のPCから現場の放送機器を監視・制御できるわけです。リモートワーク下にあっては、こ

のような運用支援形態が求められるようになるのではないでしょうか。

もちろん、制御サーバは必ずしもクラウドに設置される必要はありません。被制御機器との通信でレイテンシが厳しく問われるような場合は、それをクリアするネットワークトポロジを構成する必要があります。アプリケーションの特性に応じた上で、制御サーバをクラウドで稼働させることのメリットとデメリットの評価を下せば良いのです。あるいはクラウドを選ぶのではなく、局舎内にサーバクラスタを保有するという手法が一般的になるかもしれません。ここで重要なのは制御サーバを仮想基盤に設置することです。これにより機器間のマイグレーションを容易にし、将来的にクラウドと往来するハードルを下げることにもつながります。つまり、ソフトウェア化によるメリットを最大化するための準備をしておくべきです。

3.7 ネットワークを利用したクロック供給の可能性

更に、ネットワークが放送制作の場に大きく寄与し得る可能性がある分野について紹介します。「PTP over WAN」と呼ばれる技術です。

放送システム全般にわたり、映像・音声は標本化・量子化・符号化され、時間的に区切られたデジタルデータとして扱われます。このデータを元通りに再生するためには、時間軸の物差しとなるクロックが必須になります。このクロックとは、私たちが日常生活を送る上で意識している「絶対時刻」- 1970年1月1日午前9時0分といったような - ではなく、「相対時刻」のことで、タイミングを合わせるためのものです。デジタル機器の中にも、このクロック装置は必ず装備されています。放送機器の場合、全体を統括する同期信号用の装置が別途用意され、個々の機器に供給されます。すべての機器が同じタイミングでデータをハンドリングしないと、映像や音声の収録・再生時にずれが生じてしまうからです。

これまで映像機器に対するクロックは同軸ケーブルを経由して供給されており、Black Burst信号と呼ばれ広く使われていました。しかし放送機器のIP化に伴い、このクロックもIPを用いて供給されるようになりました。ネットワークを用いた時刻情報同期のために開発されたプロトコル、PTP (Precision Time Protocol) です。イーサネットやIPを伝送路として用い、ナノ秒オーダーでの同期精度を確保できます。源信号としてGNSSを利用し、衛星から供給された信号より高精度時刻情報を生成します。この情報は非常に高精度であるため、同期用のクロックとして用いることが可能です（絶対時刻情報も含まれています）。そしてこの高精度時刻情報をネットワークに送出するための装置を、PTP GrandMaster (GM) と称しています。このプロトコルはIEEEで規格化されましたが、応用範囲は広く、様々な規格化団体から各産業での利用形態にフィットしたプロファイルが発刊されるに至っています。

しかし、この技術の導入には一定の障壁が存在します。PTPパケットが通過する経路上において、すべてのネットワーク機器がPTPに対応する必要が生じます。PTP GMとそれを受ける放送機器だけではなく、その間をつなぐネットワークスイッチの対応も求められるのです。PTP対応の機器は、PTPのパケットに対してのみ特別な処理を実施します。正確性を保つため、PTP対応の機器はGMを源とする上流からの時刻情報を受信し続け、補正しています。更に下流へPTPパケットを送出する際も、この補正された時刻情報をパケットに打刻します。このようにPTP対応機器は一つ一つのイーサネットポートごとにパケットを処理しなければなりません。ネット

ワーク設計において、このようなPTPのフローを意識する必要があるのです。

現状、PTPに対応しているネットワークスイッチはおおむねミドルクラスかそれ以上の機種です(価格で言えば百万円以上の機種でしょうか)。全メーカの全機種で対応しているわけではないため、導入に当たってはしっかりした選定が求められます。また、既設LAN、あるいはWANにPTP技術を導入するのはなかなか難しいと思われます。機器のリプレースや、サービスでの対応を問うことにつながるからです(PTPに対応したWANサービスは、おそらく存在していません)。経路上に非対応の機器があると、PTPパケットは元の打刻情報を保ったままフォワードされます。こうなるとプロトコル上の正確性は担保できなくなり、パケット到着時の時間的なゆらぎが発生し、時刻が補正できる範囲を超えてしまいます。

放送の現場では、GNSS衛星からの信号が入感するか試さない限り判明しないという問題もあります。いつでも上空が開けた場所に中継車を設営できるとは限りません。一般的に良好なロケーションでは10個程度のGNSS衛星からの電波を受信できますが、衛星捕捉数が少なくなるとクロックの精度に影響してきます。例えばビルの谷間に中継車を設営すると上空の見通しが限られてしまい、GNSS衛星からの電波が十分に受信できない場面もありえます。こうなると、PTPをネットワーク越しに提供する方が良いのではないかという議論があります。リモートプロダクションやリモートコントロールが前提であれば、ネットワークは必ず敷設されるからです。

これらの課題を解決する技術が「PTP over WAN」です。PTP非対応のネットワーク越しであっても、遠隔地にPTPを供給することを目的としています。

PTP over WANへのアプローチは複数のメーカで試みられています。IIJは「RPTP Alliance」に参画し、この技術の技術開発を推進しています。RPTP Allianceは次世代のPTP提案を目的とし、2019年に立ち上げられたプロジェクトです。これまで高価な専用ネットワークを必要としていたPTP広域伝送に対し、長距離での高精度の同期を可能とし、PTPと互換であり、またPTPを通せないネットワークでも同期可能とした「RPTP(Resilient PTP)」技術の実証と普及を目的としています。現在RPTP Allianceは株式会社メディアリンクス、ネットワークアディションズ株式会社、セイコーソリューションズ株式会社及びIIJで活動が進められています。

RPTPにおいて、PTPのプロトコルに手を加えることはしていません。従って既設PTP GMの対応は必要ありません。受信側装置での同期アルゴリズムに改良を加えることで、非対応ネットワークで生ずるゆらぎにも適用できるようにしています。これにより整流されたPTPパケットを再配布する仕組みになっています。これまでのPTPの同期アルゴリズムはLANでのクリーンな状況を想定されており、技術的に見てRPTPはチャレンジングな開発です。しかしすべての機器がPTP対応である必要がなくなるため、ネットワーク構成の厳密さが緩和され、より手軽に使えるようになることが期待できます。

RPTP AllianceはVidMeet Onlineにも参加し、IIJバックボーン上でPTP over WANの実験を実施しました。IIJ松江データセンターパークとIIJ横浜第一データセンター間にL2ネットワークを構成し、PTPの疎通を確保。そしてIIJ松江DCPにGMを設置し、IIJ横浜第一DCまでPTPパケットを伝送しました。更にPTPからBBへと同期信号変換を行うことで、放送機器にPTP及びBBの同期信号源を同時に供給するという内容です。複数メーカの放送機器へPTPやBBを配布するのは

RPTP Allianceとして初めての経験になりましたが、いずれも問題なく同期を確立でき、放送機器の正常な稼働を確認しています(図-6)。

またIIJバックボーン以外の広域イーサネットサービスを用いた実験においても、遠隔地へのPTP供給に成功しています。更にPTPからBB同期信号を生成、同軸ケーブルを経由して放送制作用のカメラに供給したところ、カメラは正常に作動し、撮影した映像が問題なく伝送できることを確認できました(図-7)。

これらの結果はRPTPの有効性を立証していると考えています。RPTP AllianceではRPTPを実用レベルの技術として確立し、ビジネス展開へと繋げるべく、活動を継続していく予定です。

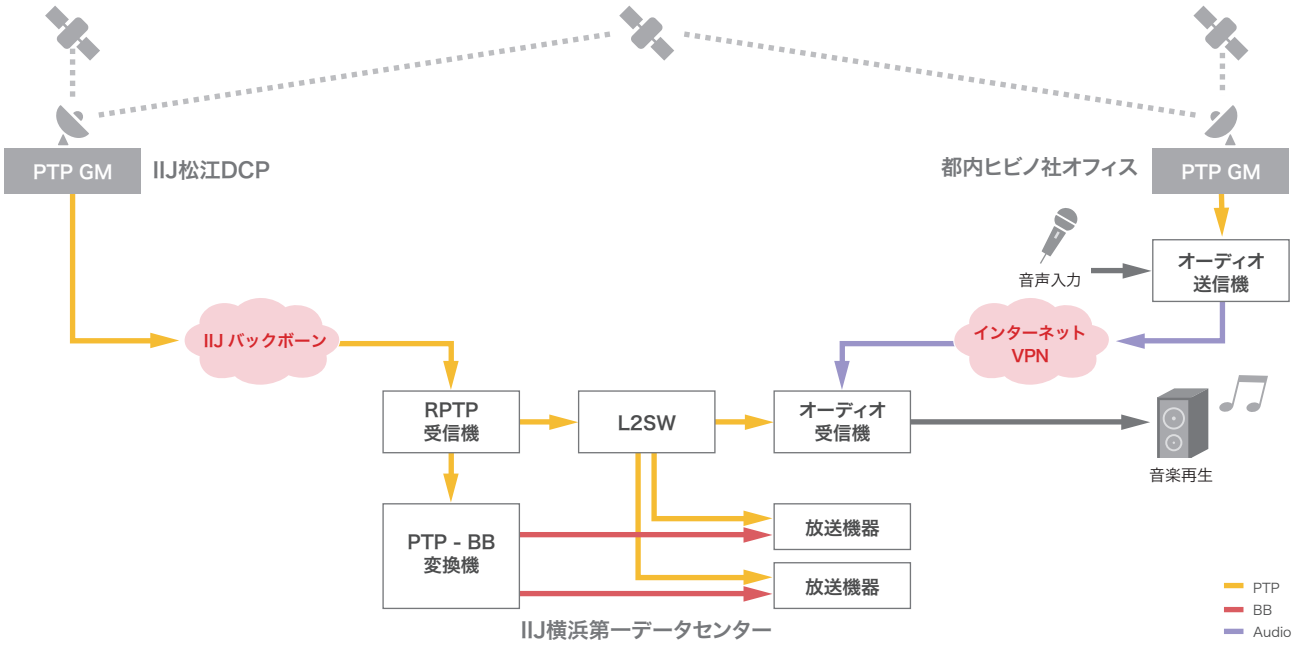


図-6 VidMeet Onlineでの実験

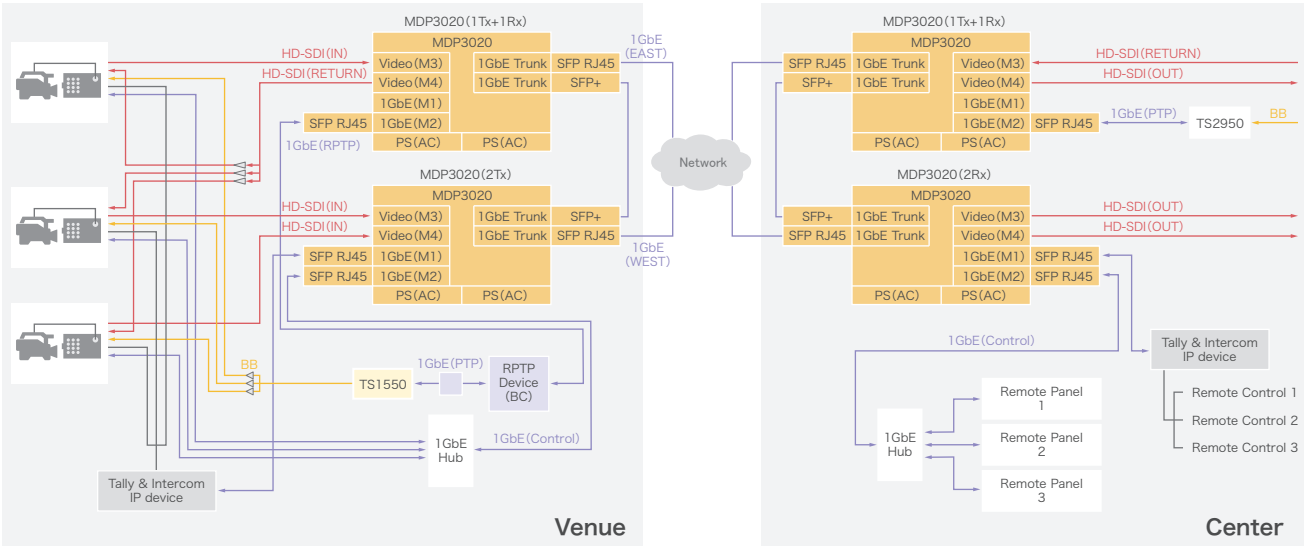


図-7 PTP-BB変換に成功

3.8 VidMeet Onlineを通じて見えてきたこと…2021年、そしてその先へ

最終的には、大容量回線が中継現場に敷設されることになっていくでしょう。2019年のラグビーワールドカップでは、決勝戦が行われた横浜国際総合競技場にIP回線が敷設され、決勝戦の模様はオーストラリアの編集プロダクションにおいて制作が実施されました。バックアップ用のクルーと機器は新横浜に設置されましたが、基本的なオペレーションはオーストラリアで行われたとのことです。このように、リモートプロダクションは世界的には既に現実の選択肢となっています。増大する要求に対して効率化を図るリモートプロダクションという手法は、ごく普通の光景となり、重要度を増していくはずです。

しかしオリンピック・パラリンピックは夏季と冬季に2年ごとに開催されるために間隔があり、そもそもホストカントリーは毎回異なります。気軽に試すフィールドではありません。上述したように、IPが放送制作に貢献できる場はもっと身近なところにもあるのです。まずは、現在IPネットワーク化されていないシステムを一部でも構わないので接続していくこと。既に普及している、安価で身軽に導入できる技術の適用範囲を見定めていくこと。こういう試みを日常的なオペレーションやシステムに取り入れていけば、技術と経験が蓄積されていくでしょう。

筆者もこうした放送機器のIP化のビジネス展開を模索してきました。実際のところ、IIJサービスの中で最も基本的な場所に位置する「接続サービス」がキーテクノロジーと認められお客様にご採用いただいているという実感があります。接続サービスはIIJの中で最も歴史が深く技術にも営業にも豊富な経験があり、更にサービス内容も多彩に展開しており、お客様に安心してお使いいただける最良のものの1つです。回線接続が安定していなければ、その上に立つクラウドサービスも意味を失いかねません。専用線のみならずフレッツやモバイルなど多様なカバレッジがあることも、訴求点の1つだと捉えています。接続サービスの重要性について再認識をいただけるようになったのは、相互理解の賜物であると信じています。

今後、放送機器とIPネットワークの関係性はより深化すると考えられます。クラウドの真価を発揮するにも、リモートプロダクション、あるいはリモートワークにおいても、ネットワーキングは欠くべからざるパートを構成することになります。放送制作という機動力・即応能力が求められる現場において、いかに使いやすく、多くの要求に答えられるためのネットワークがどのようなものであるか、その進化を手助けできるよう努力を続けていきたいと考えています。

執筆者:
山本 文治（やまもと ぶんじ）
IIJ ネットワーククラウド本部 デジタルコンテンツ配信部。
1995年にIIJメディアコミュニケーションズに入社。2005年よりIIJに勤務。主にストリーミング技術開発やVideo over IPの普及活動に従事。
2017年よりVidMeetを主宰する。

March 2021 Vol.50

IIJ
Internet Initiative Japan

株式会社インターネットイニシアティブ(IIJ)について

IIJは、1992年、インターネットの研究開発活動に関わっていた技術者が中心となり、日本でインターネットを本格的に普及させようという構想を持って設立されました。
現在は、国内最大級のインターネットバックボーンを運用し、インターネットの基盤を担うと共に、官公庁や金融機関をはじめとしたハイエンドのビジネスユーザに、インターネット接続やシステムインテグレーション、アウトソーシングサービスなど、高品質なシステム環境をトータルに提供しています。
また、サービス開発やインターネットバックボーンの運用を通して蓄積した知見を積極的に発信し、社会基盤としてのインターネットの発展に尽力しています。

本冊子の情報は2021年3月時点のものです。

IIJ-MKTG019-0050

株式会社インターネットイニシアティブ
〒102−0071 東京都千代田区富士見2-10-2　飯田橋グラン・ブルーム
E-mail：info@iij.ad.jp　URL：https://www.iij.ad.jp