IIR

Internet
Infrastructure
Review

Mar.2024
Vol.62

定期観測レポート

SOCレポート

フォーカス・リサーチ(1)

送信者レピュテーションの構築手法に関する研究

フォーカス・リサーチ(2)

IIJとデータセンターの変遷 ～この30年を振り返って

IIJ
Internet Initiative Japan

Internet Infrastructure Review

March 2024 Vol.62

エグゼクティブサマリ

本年最初の「IIR」Vol.62をお届けします。日本の2024年は能登半島を襲った巨大地震から始まりました。令和6年能登半島地震で被災された皆様に、心よりお見舞い申し上げます。

元日の午後、マグニチュード7.6、最大震度7の地震により、地域に暮らす人々のインフラが一瞬で破壊されました。電気通信のインフラも例外ではありません。移動通信事業者4社は共同で記者会見を開き、地震による被害として、ビルや基地局の停電、中継伝送路や基地局伝送路の断を発表しました。非常時においても、平常時と同じようにスマートフォンでインターネットを利用できることの重要性は、過去の災害時にも指摘されています。先の記者会見でも、利用者にとって移動通信は不可欠であり、その基盤となるのが電力と光ファイバーであることが象徴的に報じられました。

電力の確保には、移動電源車や発電機など、物理的な対処が必要となりますが、今回、伝送路の代替手段として活躍したのは衛星通信でした。従来も災害時には衛星携帯電話が利用されていましたが、この度の地震では、低軌道周回衛星を利用した高速データ通信が、基地局伝送路やWi-Fiスポットとして提供され、非常に有益であったと報告されています。ブロードバンド時代においても、光ファイバーと地上の無線通信を、衛星による無線通信で補完できることが示された事例となりました。

「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」から構成されます。

1章の定期観測レポートは「SOCレポート」です。例年同様、前年に発生したセキュリティに関する出来事から、IIJのSOCが注目したものをまとめると共に、SOCにおける課題解決の取り組みを2点、トピックとして取り上げています。1点目は、SOCで運用しているデータ分析基盤の課題とdbtの導入、2点目は、時間間隔のばらつきに着目したC&C通信の可視化に関する説明となっています。どちらもIIJのSOCが行っている業務の具体的な事例として、興味深く読んでいただけると思います。

2章のフォーカス・リサーチでは、情報処理学会で発表した「送信ドメイン認証技術を用いた送信者レピュテーションの構築手法とフィードバックループを備えたメールシステムに関する研究」から、送信者レピュテーションの構築手法について紹介します。メールはインターネット創世期から現在に至るまで広く利用されているアプリケーションであり、その安全性を保つことが社会的に強く要請されています。ここで提案した手法は、送信ドメイン認証技術の認証結果だけを利用したもので、メールの内容を参照する必要がなく、プライバシー保護の観点からも有益です。実際のメールを利用した検証でも有意な効果が出ており、送信ドメイン認証技術の有効性を検証できたと考えています。

3章のフォーカス・リサーチは、IIJの30周年特別コンテンツとして、データセンターを取り上げます。インターネット前夜を含む1990年代から、カーボンニュートラルやAIなどデータセンターに対して多様な需要が生じた2020年代まで、IIJの取り組みを時代背景と共に紹介しています。この30年間でテクノロジーは大きく進化し、インターネットも社会も大きく変化しました。データセンターはその変化を支えてきた重要なインフラであり、今後も支え続けていくという強い想いを持ちながら、30年間を振り返りました。ぜひご一読ください。

IIJでは、このような活動を通じて、インターネットの安定性を維持しながら、日々改善し発展させていく努力を続けております。今後も企業活動のインフラとして最大限に活用していただけるよう、様々なサービス及びソリューションを提供してまいります。

島上 純一（しまがみ じゅんいち）

IIJ 常務取締役 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し、2023年5月に退任。2021年6月より同協会の副会長に就任。

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（ウィズセーフ）」の立ち上げから一貫して、安全なインターネット利用環境の実現に向けた取り組みを進めています。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、セキュリティ機器のログに加え、バックボーントラフィックを集約した情報分析基盤[*2]を活用したISPならではのデータ分析により、日々高度化するサイバー攻撃に対抗すべく予防措置及び速やかな事後対処に注力しています。

本稿の1.2節では2023年のセキュリティインシデントを振り返り、特に注目した事案をセキュリティサマリとしてカレンダー形式で紹介します。続く1.3節ではデータ分析や情報分析基盤の運用で見えてきた課題の解決へ向けた直近の取り組みとして、「データ分析基盤の運用と分析における課題とdbtの導入」と「時間間隔のばらつきに着目したC&C通信の可視化」について取り上げます。その中で1.3.1節では、データの鮮度やデータマート作成・保守の課題に対応するためにdbtを導入した経緯を紹介し、1.3.2節では、時間間隔のばらつき評価に関する3つの課題に対処するため「移動変動係数」という統計量の適用を検討した結果を共有します。

1.2 2023年セキュリティサマリ

2023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、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 インシデントカレンダー（1月～6月）

月	概要
1月	自治体は、公式Webサイトの閲覧障害が発生しており、Anonymousと名乗る集団からの妨害行為（DDoS攻撃）と見られることを明らかにした。なお、Twitter（現：X）ではAnonymousを名乗る者から攻撃を示唆する内容がへ投稿されている。
1月	Microsoft OneNote形式ファイルを添付した攻撃メールが増加していることをSOCで観測した。1月以降、複数のマルウェア感染活動でOneNote形式ファイルが利用されていることを確認している。
2月	VMware ESXi製品に存在するOpenSLPのヒープバッファオーバーフローの脆弱性（CVE-2021-21974）を悪用したランサムウェア攻撃キャンペーン（ESXiArgs）が行われていることが複数の組織から報告された。同時期にOpenSLPが使用する427番ポートに対するスキャン通信が増加していることをSOCでも確認している。
2月	暗号資産取引所は、従業員がソーシャルエンジニアリング攻撃を受けていたことを公表した。攻撃者は複数の従業員に対してスミッシング攻撃を行い、窃取することができた従業員の認証情報を用いて内部ネットワークへログイン試行したが多要素認証（MFA）によりブロックされた。また、攻撃者は該当の従業員に対してITスタッフを装った電話をかけて攻撃の継続を試みたが、組織内のCSIRTが介入したことで阻止することができたとのこと。
2月	ランサムウェア攻撃グループClopは、ファイル転送ツールのGoAnywhere MFTに存在するゼロデイの脆弱性を利用して130以上の組織からデータを盗み出したと主張していることが明らかとなった。当該の脆弱性にはCVE-2023-0669が割り当てられている。その後、日系企業を含む複数組織が被害を受けたことを公表している。
3月	一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）は、2022年11月以降確認されていなかったEmotetへの感染を狙うメール配布が確認されたことを注意喚起した。メールに添付されたZIP形式ファイルには展開後に500MBを超えるWord形式ファイルが含まれたケースがあり、セキュリティ製品の検知回避を目的とした手法であると見られる（注-1）。
3月	ビジネスコミュニケーションソフトウェアを開発する海外企業は、提供するソフトウェアの正規インストーラから情報窃取型マルウェアに感染する恐れがあることを公表した。その後、侵害調査を行ったセキュリティベンダから、既にサプライチェーン攻撃を受けていたことが報告されており、ソフトウェア開発環境が侵害されていたことで別のサプライチェーン攻撃に繋がったことが明らかになっている。
3月	電気通信事業者は、業務委託先の企業から個人向けインターネットサービス及び映像配信サービスの顧客情報が流出したことを公表した。なお、流出の原因はマルウェア感染ではなく、業務委託先の企業で当該サービスの業務に従事していた元派遣社員が不正に情報を持ち出していたことを続報で明らかにしている。
3月	情報通信及びシステムインテグレーションを提供する企業は、提供する自治体の証明書交付サービスにおいて申請者とは異なる住民の証明書が発行される事象が発生したことを公表した。サービス提供を一時停止し対処を行ったが、後日、原因となったシステムのプログラムの改修において一部の自治体で修正プログラム未適用のままとなる不備があったため、点検及び速やかな修正プログラムの適用作業を行うものとしている。
4月	公共サービスの業務受託などを行うIT企業は、自治体の議会向けに提供するソリューションサービスで使用するサーバが不正アクセスを受けたことを公表した。この不正アクセスにより複数の自治体から議会のインターネット中継サービスを一時停止する報告が相次いだ。
5月	大手自動車メーカの事業戦略会社は、クラウド環境の誤設定により車両関連の情報やドライブレコーダで撮影された映像などを含む顧客情報が外部から閲覧可能となっていたことを公表した。その後、他のクラウド環境の調査を実施した結果、新たに顧客情報の一部が閲覧可能となっていたことを明らかにしている。
5月	Progress Software社は、ファイル転送サービスのMOVEit TransferのWebアプリケーションにSQLインジェクションの脆弱性（CVE-2023-34362）が存在し、既に悪用が確認されていることを公表した。同社は当初、少なくとも過去30日の間に侵害を受けていないか確認するよう案内していたが、その後、他のセキュリティ関連組織から30日よりも更に過去から活動していることが公表されている。
6月	Fortinet社は、製品が使用するFortiOS及びFortiProxyのSSL-VPN機能にヒープベースバッファオーバーフローの脆弱性（CVE-2023-27997）が存在し、限定的なケースにおいて悪用されていた可能性があることを公表した。また、攻撃グループVolt TyhpoonはFortinet社製品のゼロデイの脆弱性を初期アクセスに利用することが複数のセキュリティベンダから報告されているが、本脆弱性の使用は確認されていないことを明らかにしている。
6月	6月以降、旅行予約サイトを通じて予約した利用客に対してフィッシングサイトへ誘導するメッセージが送られる事案が相次いで公表された。原因は宿泊予約情報管理システムが不正アクセスされたことによるもので、一部の宿泊施設ではシステム管理を行う端末がマルウェアに感染していたことを明らかにしている。また、複数のセキュリティベンダからは、利用客を装った問い合わせなどのメールのやりとりで添付ファイルを開かせ情報窃取型マルウェアに感染させる手法を用いていたことが報告されている。

（注-1）マルウェアEmotetの感染再拡大に関する注意喚起（https://www.jpcert.or.jp/at/2022/at220006.html）。

表-2 インシデントカレンダー(7月～12月)

月	概要
7月	港湾輸送団体は、ランサムウェア感染によりターミナルシステムに障害が発生し復旧作業中であることを公表した。この障害発生後、当該団体宛に攻撃グループLockbitを名乗る脅迫文が届いていたことをメディアが報じている。なお、障害発生から約2日半と短い期間で順次業務が再開されている。
7月	Microsoft社は、攻撃グループStorm-0558がExchange Online及びOutlook.comへ不正アクセスし、政府機関を含む約25組織の電子メール及び組織に関連する個人アカウントへアクセスされていたことを公表した。不正アクセスは、Microsoftアカウント(MSA)署名鍵を使用して対象サービスへアクセス可能な偽造トークンを発行する手口であったことを明らかにしている。Microsoftアカウント(MSA)署名鍵の入手方法については、後日、具体的な証拠は無いものの可能性の高い手法についてレポートにて解説している。
8月	16shopと呼ばれるフィッシング作成キットを利用して、他人のクレジットカード情報を窃取し不正利用したインドネシア人の男性が逮捕されたことをメディアが報じた。また、本件は警察庁が国際刑事警察機構(ICPO)、インドネシア警察の他国とサイバー共同捜査で容疑者摘発に至った初のケースであるとのこと。
8月	国内で使用されているモバイル回線対応のIoTルータのログイン画面が改ざんされる事案が多発した。改ざんされたログイン画面には原発の処理水排出を抗議する内容が書かれていることをSOCで確認した。また、X上では改ざんに関与したと見られるアカウントから改ざんに使用した脆弱性を説明するポストが行われている。
9月	セキュリティ企業は、AI研究者がGitHubへオープンソースのAI学習モデルを公開する際に公開データを参照するトークンの設定に誤りがあり、研究者の端末のバックアップを含む38TBのデータを公開していたことを公表した。公開されたデータの中にはAI研究者が所属する企業のサービスで使用するパスワードや秘密鍵、従業員のメッセージなどが含まれていたことを明らかにしている。
9月	ドメインレジストラが運営するオークションサイトに送金・決済サービスで使用されていたドメインが出品されていることが明らかとなり、第三者が取得し悪用する可能性を懸念する声が相次いだ。一部メディアは、当該ドメインを所有していた企業への取材で社内管理の不手際によるものであったと報じている。
9月	脆弱性発見コミュニティのZero Day Initiativeは、メール転送エージェント(MTA)のEximにリモートからコード実行が可能となる脆弱性(CVE-2023-42115)があることを公表した。本脆弱性は前年6月にセキュリティ研究者から報告し、9月にゼロデイとして公開することを開発元へ勧告後、公表に至ったことを明らかにしている(注-2)。
10月	Google社、Cloudflare社、Amazon Web Services社の3社は、HTTP/2プロトコルの脆弱性(CVE-2023-44487)を利用した大規模なDDoS攻撃を8月に観測していたことを公表した。この脆弱性は、1つのTCPコネクション内で複数のHTTPリクエスト及びレスポンスを同時並行処理するHTTP/2のストリームの特徴を悪用し、クライアント側からHEADERSフレームとRST_STREAMフレームを大量送信することでサーバのリソースを枯渇させることが可能となる。この脆弱性はHTTP/2 Rapid Resetと命名されている。
10月	Cisco Systems社は、Cisco IOS XEのWebUI機能に存在する脆弱性(CVE-2023-20198)を公表した。この脆弱性を利用することでユーザ認証せずに最高位特権レベルのアクセス権を取得し新たなローカルユーザを作成することが可能となる。この数日後、同様のWebUI機能にローカルユーザからroot権限でコマンド実行可能となる脆弱性(CVE-2023-20273)が追加で公表された。この2つの脆弱性を組み合わせた攻撃による被害が国内でも報告されており、本脆弱性に関連する通信をSOCでも確認している。
10月	コンタクトセンターを運営する企業は、コールセンタシステムの運用保守に従事する者が顧客情報を不正に持ち出し、第三者へ流出させていたことを公表した。流出は約10年継続していたと想定されている。原因として、運用保守を行う端末で顧客情報のダウンロード及び外部記憶媒体へ書き出すことが可能であり、それらの操作をタイムリーな検知や定期的なログなどのチェックから把握できなかったことを挙げている。
10月	ID管理及び認証サービスを提供する企業は、サポートケース管理システムが不正アクセスを受けていたことを公表した。公表当初、影響範囲は一部の顧客がアップロードしたファイルとしていたが、その後の続報で影響範囲が全ユーザに及んでいたことを明らかにしている。なお、原因については、不正アクセスに使用されたアカウントを調査したところ、同社が管理する端末で従業員が個人のGoogleアカウントへサインインし従業員の個人デバイスにアカウント情報が同期されていたことが判明し、従業員の個人デバイスが侵害されたことでアカウントが窃取された可能性を示唆している。
11月	オンラインストレージ構築用オープンソースソフトウェアのownCloudに、コンテナ環境における機密情報及び設定の漏えいの脆弱性(CVE-2023-49103)が存在することが公表された。なお、公表から数日後、本脆弱性を悪用されていることが複数の組織から報告されている。
11月	Akamai社のSIRTは、InfectedSlursと呼ばれるMiraiの亜種がDDoSボットネットを拡大する攻撃にゼロデイの脆弱性を利用していることを公表した。また、当該の脆弱性が存在する製品の1つは国内で販売されている情報コンセント対応型無線LANルータであることを続報で明らかにしており、工場出荷時にデフォルトで設定されている認証情報を悪用可能である点が問題であることを指摘している。なお、当該ボットネットによるDDoS攻撃が11月以降も継続して行われていることをIIJでも観測している。
12月	Microsoft社及びArkose Labs社は、不正なMicrosoftアカウントやCAPTCHA認証を回避するツールなどを販売しているグループStorm-1152が使用するインフラを差し押さえ、首謀者を特定して刑事告訴状を法執行機関へ提出したことを公表した。Storm-1152は約7億5,000万件もの不正なMicrosoftアカウントを販売していたことや、販売するツールの使用方法のチュートリアル動画や利用者をサポートするチャットサービスを提供していたことも明らかにしている。
12月	セキュリティコンサルティング会社のSEC Consultは、SMTP Smugglingと命名したSMTPの実装における脆弱性を公表した。本脆弱性は、SMTPプロトコルのデータ終端に用いられるシーケンスとは異なるシーケンスを使用した場合でも終端と認識するプロダクトが複数存在し、後続データに2通目のメールを加えることで送信ドメイン認証の1つであるSPFによる送信元の詐称チェックが行われずに配送が可能になるなどの問題を明らかにしている。

(注-2) Exim AUTH Out-Of-Bounds Write Remote Code Execution Vulnerability(https://www.zerodayinitiative.com/advisories/ZDI-23-1469/)。

1.3 セキュリティトピックス

本節では、IIJのSOCにおける課題解決への取り組みについて紹介します。

1.3.1 データ分析基盤の運用と分析における課題とdbtの導入

IIJでは、サイバーセキュリティにおける脅威への適切な予防措置や事後対処に活かすことを目的として「情報分析基盤」というデータ基盤を運用しています。取り組みの詳細については2018年3月30日発行の本レポートのVol.38（https://www.iij.ad.jp/dev/report/iir/038/01.html）の「SOCレポート」にも記載がありますので併せてご覧ください。情報分析基盤は、ソフトウェアのアップデートやデータソースの拡充などを繰り返しながら活用が続いています。ここでは、情報分析基盤の運用を通して見えてきた課題と、その解決に向けてdbt（data build tool）というOSSを導入した取り組みについて紹介します。

課題について述べる前に、前提となるデータ基盤の運用やアーキテクチャについて説明します。なお、この内容は情報分析基盤に限った話ではありません。まず、一般的にデータ基盤に関する業務には、次の2種類の職能を持ったメンバーが携わります。

- データエンジニア
- データアナリスト

より細分化して扱う場合もありますが、ここでは主に前者を「データ基盤を作るメンバー」、後者を「データ基盤を使うメンバー」という意味で使用します。情報分析基盤においても、それぞれのメンバーが開発を担うチームと分析を担うチームに分かれて、連携しながら業務を遂行しています。

また、データ基盤に蓄積するデータは次のような層構造で管理する考え方が現在の主流です。情報分析基盤も、これに相当する形でデータを管理しています（図-1）。

- データレイク層
- データウェアハウス層
- データマート層

データレイク層では、データの生成元であるデータソースから収集または転送されてくるデータを、なるべくそのままの形で保存します。データウェアハウス層では、データレイク層のデータを分析しやすいように構造化データなどに変換します。データマート層では、データウェアハウス層のデータを特定の用途に特化した形で変換します。

データマート層については後述する課題とも関わってくるため、セキュリティというドメインで例を挙げておきます。仮にですが、あるデータ基盤においてIPS/IDSから収集したデータ

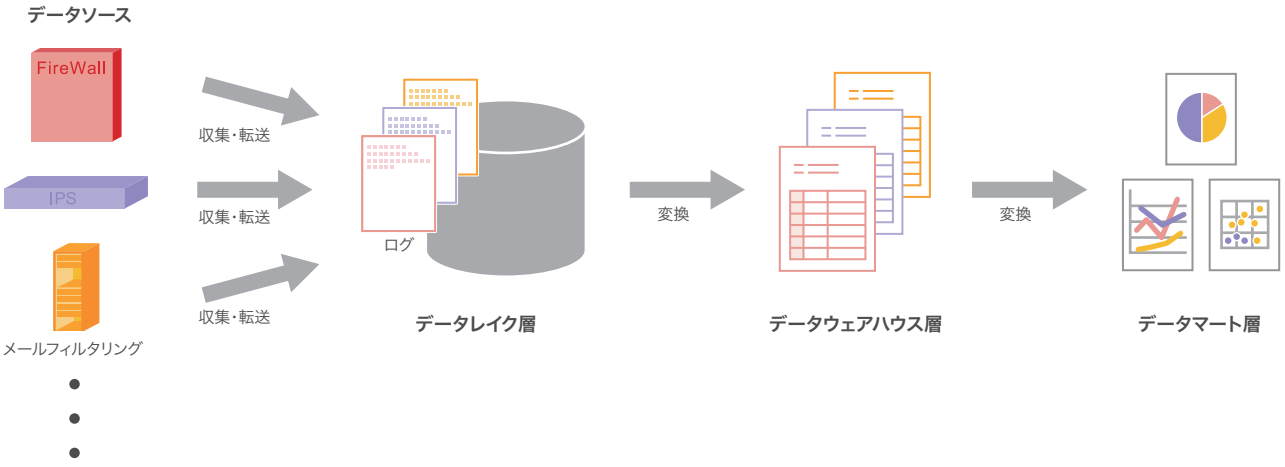


図-1 データ基盤のデータを層構造で管理するイメージ

がデータウェアハウス層に取り込まれているとしましょう。このとき、特定のデータポイント（レコード）には脅威を検出したシグネチャや時刻に関する情報が含まれることにします。もし、このデータから日々の傾向を確認したくなった場合には、検出したシグネチャの種類と件数を日ごとに集計することが考えられます。その際、データアナリストがアドホックに集計するのではなく、あらかじめ集計しておいたものがデータマートに相当します。参照する頻度が高い重要な内容であれば、ダッシュボードなどを使って可視化することも考えられるでしょう。

続いては、情報分析基盤の運用と分析において見えてきた2つの課題について説明します。まず1つ目は、データの品質に関わる課題です。データアナリストが適切な分析をするためには、データ基盤のデータが健全な状態を維持し続ける必要があります。一方で、完全無欠のシステムはこの世に存在しないことから、情報分析基盤でも次のような事象が生じることがありました。

- 特定のデータの鮮度が低下する
- 特定のデータが想定外の状況に陥る

データの鮮度というのは、データが滞りなくタイムリーにデータ基盤へ取り込まれているかどうかを表す概念です。データの鮮度が低下しているというのは、データ基盤へのデータの取り込みが想定よりも遅れていたり、あるいは一時的に停止した状況を表します。データの鮮度が低下した状況では、データアナリストが適時性のある分析を実施できない恐れがあります[*3]。

データが想定外の状況に陥るというのは、やや漠然とした表現ですが、データアナリストから見たときに「データがおかしい」と思える状況です。例えば、本来はユニークであるはずの値に重複が生じたり、あるいは想定していない値が含まれる状況はイメージしやすいでしょう[*4]。このような状況を見過ごしてしまうと、分析した結果の信頼性に関わります。

続いて2つ目は、データマートの作成や保守に関する課題です。定型で繰り返し何度も実施するような業務においては特にデータマートの存在は欠かせません。何故なら、データマートの有無によって作業の効率が大きく変わるためです。

一方で、情報分析基盤においてはデータマートを作成する際に、個別の開発が生じやすいという課題がありました。個別の開発が生じると、開発から保守に至るまで少なくないリソースが費やされます。また、実際に利用できるようになるまでのリードタイムも長くかかる傾向にありました。

情報分析基盤では、これらの課題を解決するためにdbtというOSSを導入しました。dbtにはOSS版のdbt CoreとSaaS版のdbt Cloudがあります。情報分析基盤で導入したのは、前者のdbt Coreです。dbtはデータ基盤が備える基本的な機能を表したETL（Extract Transform Load）の中で、T（データの変換）に特化したツールです。SQLとYAMLの設定だけで、ほとんどの機能を利用できる点が特長として挙げられます[*5]。この「SQLとYAMLの設定だけ」という点は、分析においてSQLを多用しやすいデータアナリストにとって特に扱いやすい長所です。

1つ目の「データの品質に関する課題」は、dbtを使ってデータをテストすることで解決します。自動化されたテストは、ソフトウェアエンジニアリングにおける優れたプラクティスの1つです。そして、その考え方はデータエンジニアリングにおいても有効です。

dbtにはデータをテストする機能が含まれており、テストについてもSQLとYAMLを使って記述できます。dbtにおけるテストの実体は、正常系において抽出されるレコードが0件になる

＊3　鮮度の低下がどこまで許容できるかは、データアナリストが実施する業務の性質に依存します。
＊4　実際に生じる状況は、データの定義から自明な異常もあれば、要約統計量などを通して見たときにデータの分布が変化するといった発見の難しいケースまで様々です。
＊5　データベース間の差異（SQLの方言など）については、データベースごとに用意されたアダプタで吸収します。

SELECT文です。つまり、あるテストに対応するSELECT文で1件以上のレコードが抽出されるとテストが失敗したことになります。自分でゼロからSELECT文を書くことはもちろん、組み込みやサードパーティ製のプラグインが実装しているテスト用のマクロも利用できます。また、データの鮮度が低下する状況についても「source freshness」という機能で検知が可能です。

従来であれば、情報分析基盤のデータが何らかの想定外の状況に陥っていることは、データアナリストが分析する過程で気づくのが典型的でした。しかし、データアナリストは何らかの目的を持ってデータを分析しています。つまり、そのデータを今まさに必要としていることが多いわけです。そのため、判明した際には業務への影響が大きくなる傾向にありました。一方でdbtの導入後は、データの定義やデータアナリストの経験則を自動化されたテストに落とし込むことで、効率的な発見と対処が可能になりました。

2つ目の「データマートの作成や保守に関する課題」は、dbtを使ってSQLでデータを変換することで解決します。dbtでは、モデルと呼ばれるオブジェクトを、やはりSQLのSELECT文を使って定義できます。モデルに対応するSELECT文によって変換された結果は、ビューやテーブルといった形でアクセスできるようになります。また、モデルを定義する際にはJinja形式のテンプレート言語が利用できます。そのため、頻繁に記述する内容をマクロとしてまとめたり、純粋なSQLでは表現が難しい柔軟なループ処理や分岐処理も可能です。

情報分析基盤では、dbtの導入によって多くのケースにおいてSQLの記述だけでデータマートが作成できるようになりました。セキュリティのIoC（Indicator of Compromise）情報を高速に検索するためのデータマートを短期間で作成して、特定の業務が数十倍に効率化された例もあります。なお、SQLだけでは実現が難しい処理もあることから、個別の開発が全く不要になったわけではありません。一方で、以前よりもデータエンジニアとデータアナリストの分業が進めやすくなった側面があります。具体的には、SQLだけでは実現が難しい処理を、データエンジニアがSQLのユーザ定義関数（User Defined Function）として実装します。その上で、データアナリストが、そのユーザ定義関数を組み込んだSQLを使ってdbtでデータを変換する処理を記述します。この流れでは、それぞれの作業が既存の枠組みを踏襲していることから、以前に比べて必要なリソースの低減やリードタイムの短縮が見込めるようになりました。また、以前よりもデータマートを作成するまでの道筋が具体的になったことで、効率化や新たな分析に関するアイデア自体を出しやすくする効果もあったように感じています。

1.3.2 時間間隔のばらつきに着目したC&C通信の可視化

マルウェアの中には、システムに感染するとインターネット上のC&C（Command and Control）サーバと通信して、攻撃者からの指示を受け取るものがあります。このときに生じる通信（以下、C&C通信）は、あらかじめマルウェアのプログラムによって基本的な振る舞いが定められています。そのため、例えば人間がブラウザなどのアプリケーションをアドホックに操作することで生じる通信に比べると、特定のパターンが現れやすい状況にあります。

特定のパターンを反映しやすい代表的な特徴の1つが、通信の時間間隔です。典型的な例としては、死活監視で用いられるハートビートのような、一定の時間間隔でポーリングする通信をイメージすると分かりやすいでしょう。そのような通信は、生じる時間間隔のばらつきが小さくなる傾向にあります。そこで、今回はセキュリティアナリストが効率的にC&C通信のパターンを捉えられるように、時間間隔のばらつきに着目した統計量を用いて通信の可視化を試みました。

ただし、マルウェアでない正規のアプリケーションであっても、時間間隔のばらつきが小さい通信を生じうる点には留意が必要です。実環境において時間間隔のばらつきが小さな通信を見つけたとしても、その多くは正規のアプリケーションに由来すると考えた方が良いでしょう。そのため本手法は、侵害事象が生じた際にアナリストが視覚的に状況を把握するのを助けることを応用先に想定しています。

まずは、課題とその解決に使えそうな道具について整理しておきましょう。C&C通信は、時間の経過と共に発生するイベント（事象）と捉えることができます。個々のイベントは、典型的には以下の組み合わせで識別される特定のセッション[*6]に属します。送信元がマルウェアに感染したシステムで、送信先が攻撃者の用意したC&Cサーバです。なお、送信元ポート番号をセッションの識別に含めないのは、エフェメラルポートで接続ごとに変わる可能性が考えられるためです。

- 送信元IPアドレス
- 送信先IPアドレス
- トランスポート層のプロトコル
- 送信先ポート番号

次に、記述統計において数値のばらつきを定量的に扱うための代表的な統計量には、「分散」や、それを元にした「標準偏差」があります。ですが、あるセッションに含まれるすべてのイベントを使って、分散や標準偏差で通信の時間間隔のばらつきを評価することにはいくつかの課題があります。

■ a. 異なるセッション同士で値を比較することが難しい

例えば、次のような状況を考えてみましょう。あるセッションAにおいて、イベントの生じる平均的な時間間隔が100秒で、ばらつきを表す標準偏差が10秒だったとします。一方で、セッションBにおいては、イベントの生じる平均的な時間間隔が1000秒で、ばらつきを表す標準偏差が50秒だったとします。標準偏差という統計量の絶対値だけで比べると、セッションAの方がセッションBよりも小さくなります。しかし、平均に対するばらつきの大きさで考えた場合には、セッションBの方がセッションAよりも小さいと言えます。このように、分散や標準偏差だけでは、異なるセッションを比較するには不十分であることが分かります。

■ b. 外れ値の影響を大きく受ける

例えばマルウェアに感染したのが企業の業務で利用されているパソコンであれば、平日の日中帯にしか電源が入っていないかもしれません。端末の電源が入っていなければ、もちろんC&C通信は生じません。仮に端末の電源が入っていない時間帯まで計算に含めると、そのタイミングは外れ値のようにイベントの時間間隔が大きくなります。結果として、集計した分散や標準偏差は、本来の想定よりも大きくなることでしょう。

■ c. イベントの生じる時間間隔が途中で変わる恐れがある

マルウェアによっては、攻撃者が活発に指示を与えるタイミングで、イベントの生じる時間間隔を短くするものがあります。マルウェアの多くは自発的にC&Cサーバへ指示を受け取りに行く[*7]ことから、ポーリングの間隔が長いと動作の反映までに時間を要するためと考えられます。そのような、長短の時間間隔が混ざり合った状況は、単一の分散や標準偏差といった統計量では表現が難しいと言えます。

そこで、上記のような課題に対処するため「移動変動係数」という統計量の利用を検討しました。移動変動係数は、一般的な統計量である「変動係数」に「移動」の考え方を導入したものです。通信間隔から求めた移動変動係数が小さいほど、ばらつきの小さな規則正しい通信と言えます。

＊6　あるノード間での一連のやり取りを便宜的に呼んでいるものでTCPのセッションとは異なります。
＊7　インターネット上のC&Cサーバ側を起点にするとNATやファイアウォールに阻まれる可能性が高いためと考えられます。

まず、「変動係数」は標準偏差を平均で割った統計量です。課題aで述べたとおり、標準偏差だけでは平均の大きさに対するばらつきの大小が判断できません。そこで、標準偏差を平均で割ることで無次元化します。これによって、異なるセッションのばらつき同士を比較できるようになります。

次に、「移動」は局所的なデータを用いて統計量を計算する概念です。主に時系列など連続するデータにおいて、一定数のデータポイントだけを使って統計量を計算します。このとき、計算に用いる一定数のデータポイントの範囲はウィンドウと呼びます。移動では、ウィンドウをずらしながらデータのすべての範囲について統計量を求めます。

つまり、「移動変動係数」は変動係数を移動で求めた統計量です。移動変動係数は、移動標準偏差を移動平均で割って求めます。これにより、課題bやcの影響を低減できます。課題bについては、外れ値の影響を受けるのが、そのイベントを含むウィンドウの範囲だけに限定されます。また、課題cについては、イベントの生じる時間間隔が途中で変わったとしても、時系列での統計量の変化として捉えられることが期待できます。

ここからは、実際に過去の感染事例においてマルウェアが生じたC&C通信を移動変動係数で可視化した様子を紹介します。まず1つ目の事例では、マルウェアが複数のC&Cサーバと同時に通信する様子です。近年のマルウェアは、この事例のように複数のC&Cサーバと同時に通信を試みるケースが多くあります。

図-3の折れ線グラフは、横軸に基準となる時刻からの経過時間を、縦軸に移動変動係数をプロットしています。それぞれの折れ線はセッションを表しており、すべてC&Cサーバへの通信です。このケースでは、それぞれのセッションは送信元IPアド

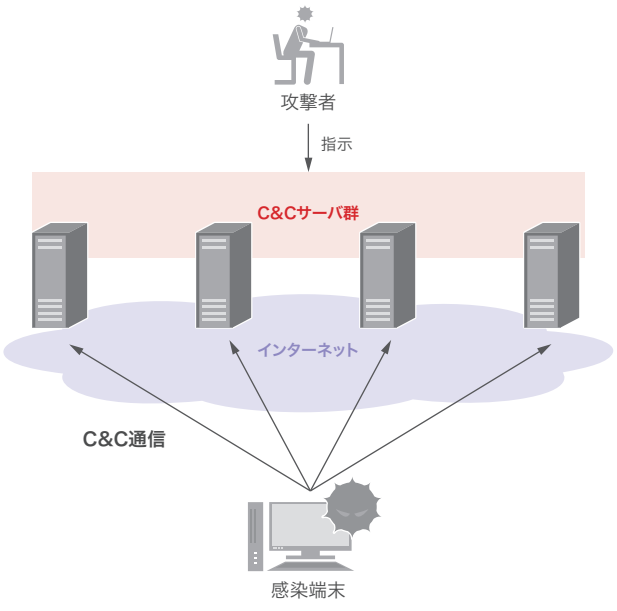


図-2 マルウェアが複数のC&Cサーバへ同時に通信を試みるイメージ

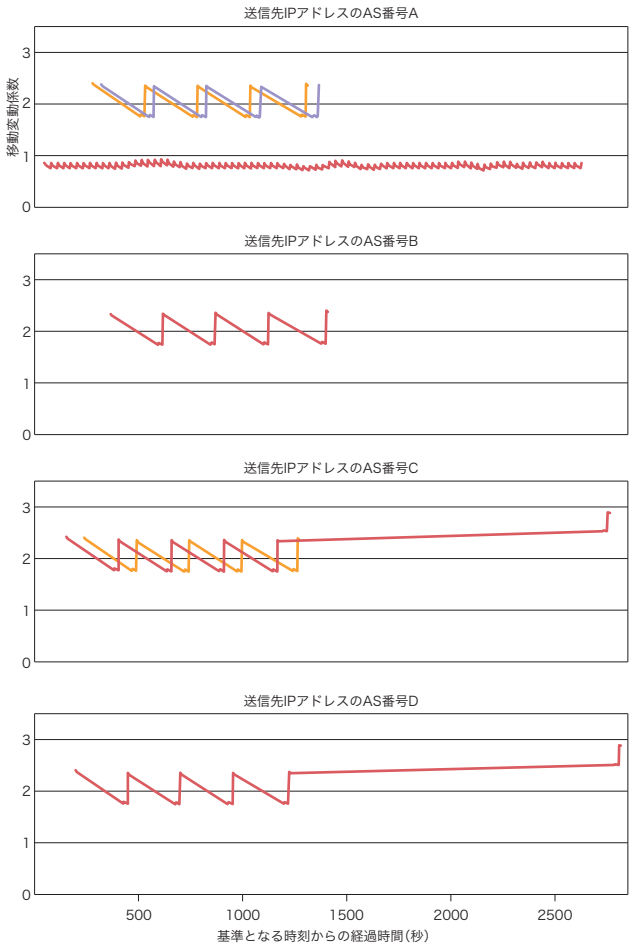


図-3 特徴的なノコギリ状の折れ線を含んだマルウェアからC&Cサーバへの通信

レスとトランスポート層のプロトコルが同一で、送信先IPアドレスとポート番号が異なっていました。見やすさのために、送信先IPアドレスのAS番号ごとにグラフを複数のパネルに分割しています。また、移動変動係数を求める際のウィンドウサイズには10点を用いました。

図-3のグラフでは、各パネルに移動変動係数が2前後で推移する特徴的なノコギリ状の折れ線が確認できます。それぞれのノコギリができるタイミングは、少しずつずれていますが近い場所にあります。これは、異なるC&Cサーバであっても、それぞれへ通信を試みるタイミングは類似していたことを意味します。

続いて2つ目の事例では、マルウェアが通信中のC&Cサーバが途中で使えなくなった際に、別のC&Cサーバへフォールバックする様子を示します。このマルウェアは同時に1つのC&Cサーバとしか通信しませんが、利用中のC&Cサーバとの疎通が失われて一定時間が経過すると、別のC&Cサーバに通信先を切り替える機能を有していると考えられます。

図-5の折れ線グラフは、先ほどと同様に横軸が基準となる時刻からの経過時間、縦軸が移動変動係数になっています。それぞれの折れ線がセッションを表している点も同様です。移動変動係数を求める際のウィンドウサイズも先ほどと同じ10点を用いました。ただし、経過時間の単位が先ほどのグラフでは「秒」でしたが、こちらでは「分」になっています。

グラフには2つのセッションが含まれており、いずれも移動変動係数がゼロ付近で安定している時間帯が確認できます。これは言い換えると、通信間隔のばらつきが極めて小さい、規則正しい通信をしている時間帯があるということです。実際には、同時間帯においてマルウェアはおおむね317から320秒程度の間隔でC&Cサーバとの通信を繰り返していました。

また、オレンジ色のセッションについては200分前後から移動変動係数が増加した[*8]後に折れ線が途絶えています。そして、そこから少し経過したタイミングで紫色の折れ線が現れます。これが、マルウェアが通信先のC&Cサーバをフォールバックする様子です。オレンジ色のセッションについては、折れ線

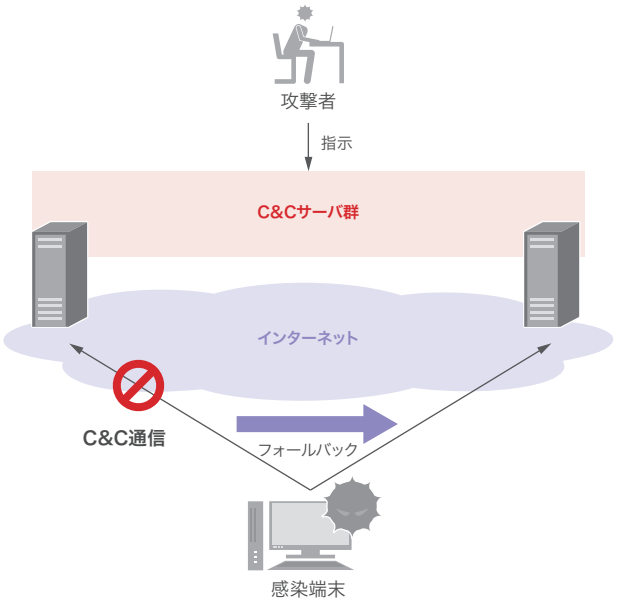


図-4 マルウェアが通信先のC&Cサーバをフォールバックするイメージ

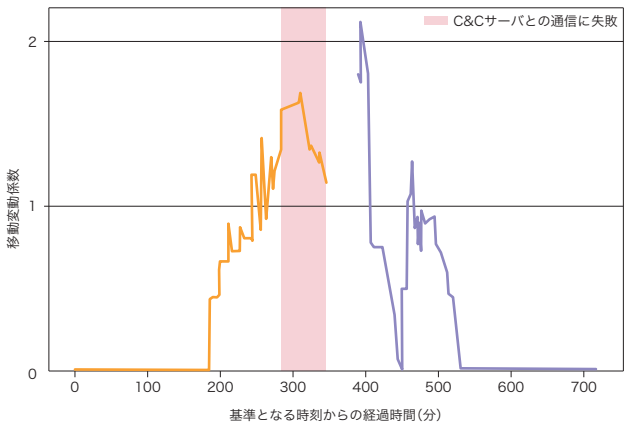


図-5 マルウェアが通信先のC&Cサーバをフォールバックした通信

＊8　移動変動係数の増加は、前述の課題cで示したように途中で通信間隔の規則正しさが崩れたことを意味します。

が途絶える約1時間前からC&Cサーバとの通信に失敗していました。そのため、マルウェアが通信先として使用するC&Cサーバを切り替えたものと見られます。

なお、ここで紹介した内容は代表的な例であり、マルウェアの通信には様々なパターンが存在しています。例えば、通信先のC&Cサーバごとに通信の間隔を変えたり、一定のランダム性を持たせたマルウェアも珍しくありません。これらは、通信の時間間隔のばらつきに由来する検知を避けるためと考えられます。そのような場合でも、移動変動係数ではグラフの形状に類似が見られたり、特定の範囲で値が推移する様子として観察できる事例を確認しています。

ここでは、時間間隔のばらつきに着目した統計量を用いて通信を可視化する試みについて紹介しました。IIJのSOCでは、今後もデータを活用したセキュリティの分析を効率的に進める手法を検討していきます。

1.4 おわりに

本稿では、2023年に観測した事案の中から、SOCの観測で着目したものをいくつかピックアップして紹介しました。1.2節の年間サマリでは、引き続きソフトウェアにおける脆弱性の発覚やランサムウェア攻撃、設定ミス・外部からの攻撃による情報漏えいが発生していることが分かります。1.3.1節では、dbtを利用した自動化されたテストや個別開発が不要なSQLを用いたデータ変換により、データの鮮度・品質やデータマートの作成・保守に関する課題を解決した経緯を説明しました。また1.3.2節では、「分散」やそれを元にした「標準偏差」を用いて時間間隔のばらつきを評価する際に顕在化した、異なるセッションの比較や外れ値の影響、時間間隔の変化といった問題への対処法として「移動変動係数」を導入した流れと実際のケースを例示しました。

引き続きIIJでは、刻一刻と変化する脅威に対応するための情報発信を続けていきます。今後もIIRやwizSafe Security Signalで発信する情報を注視いただき、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:

山口 順也（やまぐち じゅんや）
IIJ 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

鴨川 寛之（かもがわ ひろゆき）
IIJ セキュリティ本部 セキュリティオペレーション部 データ分析課

小林 智史（こばやし さとし）
IIJ セキュリティ本部 セキュリティオペレーション部 データ分析課

送信者レピュテーションの構築手法に関する研究

2.1 はじめに

今から20年前の2004年1月、グローバルで迷惑メール対策を議論するワーキング・グループであるMAAWG(Messaging Anti-Abuse Working Group)にIIJは参加しました。私は2004年4月の最初のFounding Meetingから参加し、その後も継続してメンバー会合であるGeneral Meetingに参加してきました。現在はM^{3}AAWG[*1]と名称を少し変更し、対象範囲も広げて活動しており、2024年2月に20周年となる60回目のGeneral Meetingが開催されました。

MAAWGでの当初の技術的な議論は、電子メールシステムの欠陥ともいうべきメール送信者が誰かを正確に把握できない問題に対する、送信ドメイン認証技術、特にSPF[*2]やDKIM[*3]に関する検討や普及が中心でした。その後も技術的な議論は継続し、DMARC[*4]やARC[*5]、BIMI[*6]といった技術の仕様がM^{3}AAWGメンバーを中心に作られてきました。これら送信ドメイン認証技術の議論では、当初から次のステップとして認証されたドメイン名を受け取るべき送信者であるかの判断、つまり送信者レピュテーションが必要になると考えられてきました。実際、SPFの最初の仕様RFC4408でもドメイン名のレピュテーションについて触れられており、最近でもGoogle社と米国Yahoo社が受信メールの対策強化として、メール送信側に送信ドメイン認証への対応を強く求めています。実際に、この受信施策強化の発表のあと、国内でもDMARCに対応するドメイン名が急増しました。IAjapanの客員研究員としてjpドメイン名の調査を行っていますが、2024年2月の時点で、メールに利用しているドメイン名の約1/4がDMARCレコードを設定しており、これは設定割合が約3倍増加したことを示しています。

IIJ技術研究所では、送信者レピュテーションの構築手法に関する研究を行っています。本稿は、情報処理学会の論文誌で発表した論文[*7]を紹介するものです。論文では、送信者レピュテーションの構築手法とフィードバックループについて述べていますが、本稿ではそのうち送信者レピュテーション部分について紹介します。また本論文は、情報処理学会から特選論文として選定されました。

2.2 送信者レピュテーション

メールの送信元情報を用いて受け取りを判断する手法としては、送信元のIPアドレスを利用し、DNSの仕組みを利用して参照するDNSBL(DNS Block List)が長い間利用されてきました。送信元のIPアドレスは、メール送信者を特定する情報としては適切ではありませんが、メール送信者を示すメールアドレスは信頼できないことから、DNSBLが利用されてきました。これを送信ドメイン認証のSPFやDKIMの普及により、認証した信頼できる情報であるドメイン名を受け取り判断に利用しようというのが、ドメイン名の送信者レピュテーションです。

送信者レピュテーションでは、単に受け取るべきではない負の評価を持つドメイン名以外にも、受け取るべき正のドメイン名も考えられます。それらの評価をドメイン名ごとに数値化すれば、レピュテーションとなります。より単純にドメイン名のBlock ListとAllow Listと捉えることもできます。

送信ドメイン認証技術の普及と共に、独自にドメイン名を登録し、SPFやDKIMの設定を正しく行って送信する迷惑メールも多くなりました。こうした迷惑メールに利用するドメイン名は、使い捨て的に登録し利用されるため、Block Listのドメインレピュテーションを構築したとしても、その効果は残念ながら限定的です。それよりは、受け取るべきAllow Listを構築し、それによって判定できないメールをメールフィルタなどによってメール内容から判断するといった組み合わせ的な手法が効果的である可

＊1　Messaging, Malware and Mobile Anti-Abuse Working Group
＊2　Sender Policy Framework (SPF) for Authorizing Use of Domains in *Email, Version 1 (RFC7208)。
＊3　DomainKeys Identified Mail (DKIM) Signatures (RFC6376)。
＊4　Domain-based Message Authentication, Reporting, and Conformance (RFC7489)。
＊5　Authenticated Received Chain。
＊6　Brand Indicators for Message Identification (Internet-Draft)。
＊7　櫻庭秀次、他: 送信ドメイン認証を用いた送信者レピュテーションの構築手法とフィードバックループの提案, 情報処理学会論文誌, Vol.64, No.1, pp.13-23 (2023)。

能性があります。特に現在は、以前に比べて迷惑メール自体の割合が減っていますので、大部分の受け取るべきメールを、より簡便な送信ドメイン認証と送信者レピュテーションによって判断することができれば、より多くの計算機資源をメール内容の判断に利用することもできるようになります。

本稿では、こうした背景から、特に受け取るべき正規のメールのドメイン名を収集し、レピュテーションとして構築する手法について述べます。

2.3 送信ドメイン認証技術の特徴

送信ドメイン認証技術のSPFやDKIMについては、例えば送信ドメイン認証技術導入マニュアル[*8]などに詳しく述べられていますので、ここでは、送信者レピュテーションの構築手法に関わる部分について示します。

SPFは、メール配送プロトコル(SMTP)上のメール送信者としてのメールアドレスのドメイン名を認証します。認証の方法は、送信側が予めドメイン名のDNS上にSPFレコードとしてメールの送信元のIPアドレスなどを記載し、メール受信側がそれをメール受信時に参照し、正しい送信元からのメールであるかを判断します。この仕組みのため、SPFの送信側の導入は、DNSにSPFレコードを設定するだけなので比較的容易であり、普及も進んでいます。しかしながら、受信側にとって最初のメール送信者以外から送信された場合は、正しく認証できなくなるという課題があります。

DKIMは、送信するメールそれぞれに、メールヘッダと本文からなる電子署名を作成し、関連情報と共にメールヘッダとして記載します。メールの配送経路によらない認証方式を用いていることにより、SPFのような例えば転送されたメールが正しく認証できないなどの課題はありません。しかしながら、送信メールサーバに電子署名を作成しDKIMの署名情報を追加する処理を新たに付け加える必要があるため、SPFに比べて普及がそれほど進んでいないという課題があります。

2.4 送信者レピュテーションの構築手法

ここでは、送信ドメイン認証技術を用いて受け取るべきSPFの認証ドメイン名を収集する手法について述べます。一般的に、受け取るべきではない迷惑メールについては、メール自体が不要なものであるため、収集することは比較的容易です。収集した迷惑メールからその特徴や送信者情報を抽出することで、迷惑メールフィルタのための情報やブロックリストを収集することが行われてきました。その一方で受け取るべきメールについては、メッセージという機密性の高い情報が含まれるといった課題もあり、逆に収集が一般的に難しいという性質があります。また、受け取るべきという判断に利用しますので、誤って迷惑メールの送信元を登録してしまった場合の被害などの影響も大きく、登録に際しては正確性も要求されます。

ここでは、転送メールが受け取るべきメールであることを示し、その送信元を判断し収集する手法について述べます。

2.4.1 転送メールの性質

転送メールは、複数のメールアカウントを利用している場合で、それらを1ヵ所で参照したい場合など、メールを集約する手段として利用されたりします。メールシステムでは古くから利用されてきた仕組みであり、例えばオープンソースのSendmailなどでは、ホームディレクトリの.forwardファイルに転送先のメールアドレスを記述することで、受信したメールを自動的に転送してきました。つまり、転送元でメール転送設定しているのは、転送先のメール受信者であり、このことから

*8　日本データ通信協会迷惑メール相談センター、送信ドメイン認証技術導入マニュアル(https://www.dekyo.or.jp/soudan/aspc/report.html#dam)。

転送先のメール受信者にとって、転送元のメール送信者は受け取るべきメール送信元であると言えます。

こうしたメール転送元を収集することができれば、受け取るべきメール送信元のレピュテーションを構築することができるはずです。

2.4.2 転送メールと送信ドメイン認証技術

一般的なメール転送では、SPFの認証ドメイン名であるエンベロープFrom[*9]は、最初のメール送信者が設定したメールアドレスをそのまま利用します。この仕組みにより、転送先のメール受信側ではSPFの認証が失敗します。一方で、DKIMはメール送信元のIPアドレスを認証に利用しませんので、最初にDKIM署名を追加したメールは、転送先でもDKIM認証ができます。この結果を図-1に示します。図のSDID（Signing Domain Identifier）はDKIM認証での認証ドメイン名です。

また最近では、なりすましメール対策を強化する目的で、SPF認証できないメールを受け取らないメール受信側が増えました。そのため、メール転送時にエンベロープFromを転送元のドメイン名に書き換えて送信するような転送元も存在します。この場合、転送先ではSPF及びDKIMの両方の認証がpassします。しかしながら、それぞれの認証ドメイン名は通常異なります。この結果を図-2に示します。

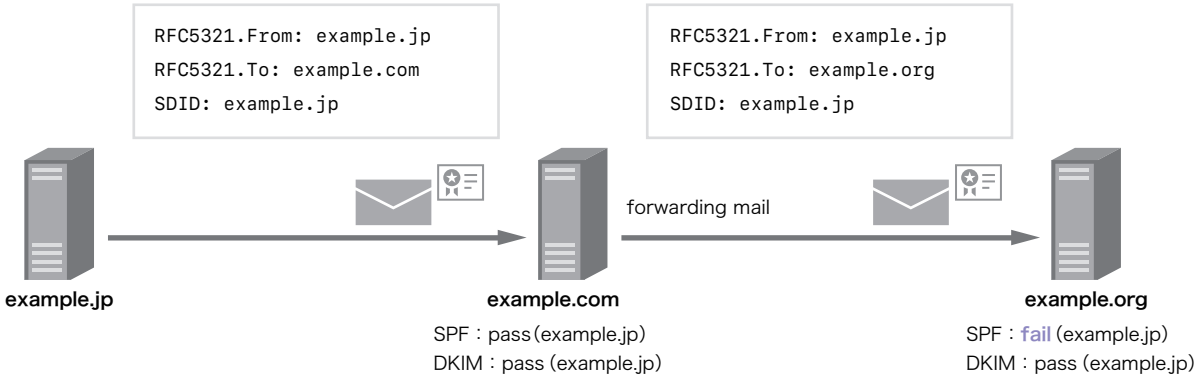


図-1 転送メールの送信ドメイン認証結果

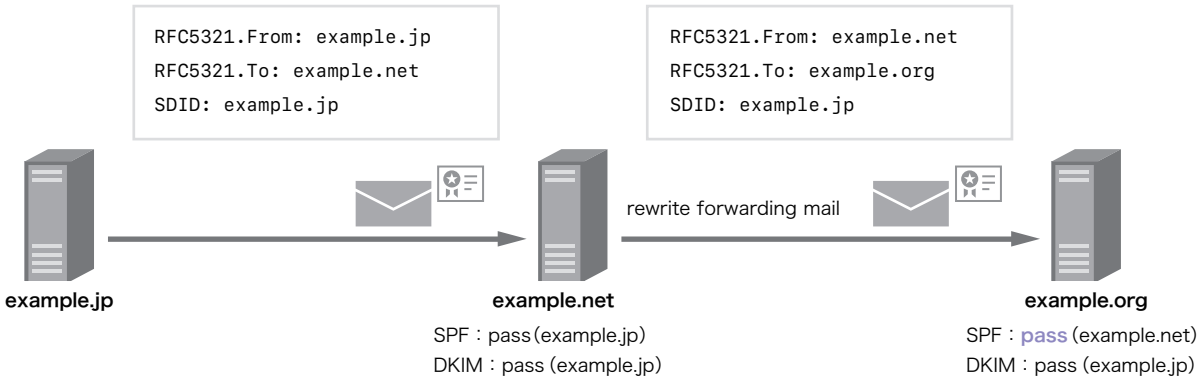


図-2 送信者情報を書き換える転送メールの送信ドメイン認証

＊9　メール配送の規格（SMTP）上の送信者メールアドレスで、その規格番号からRFC5321.Fromと表現する場合があります。

2.4.3 送信ドメイン認証結果を利用した転送メール元の判断

転送メールの転送方法が2種類あること、それぞれでSPFとDKIMの認証結果が異なることを示しました。そこで、送信ドメイン認証の結果を利用して、転送メールかどうかを判断し、その転送メールの送信元をレピュテーションとして収集します。まず、転送時にRFC5321.Fromを書き換えない転送元は、以下の認証結果の条件から判断し、受け取るべきSPF認証ドメイン名を収集します。

- SPFの認証が失敗し、DKIMの認証がpassする送信元IPアドレス
- 上記のIPアドレスから送信され、SPFの認証がpassするSPF認証ドメイン名

最初の条件では、転送メールの送信元IPアドレスを収集します。送信メールサーバが複数ある場合もあるため、より広く正規のメール送信元を収集するために、その送信メールの管理元を得る目的で、転送メールの送信元IPアドレスから送信され、かつSPF認証がpassするSPF認証ドメイン名を収集します。これが2つ目の条件です。この転送元のIPアドレスと、そこから送信されるSPF認証ドメイン名の両方が、受け取るべき送信者レピュテーションとなります。このIPアドレスは、受け取るべき正規の送信元ですので、そこから送信されるメールで、転送メールではないメールも、受け取るべきメールと判断します。これにより、IPアドレスだけでなくSPFの認証ドメイン名を送信者レピュテーションとして利用できることになります。

次に転送時にエンベロープFromを書き換える転送元を、以下の条件から判断し、同様に受け取るべきSPF認証ドメイン名を収集します。

- SPFとDKIMの両方の認証がpassし、それぞれのドメイン名の関連がない送信元IPアドレス
- 上記のIPアドレスからDKIM認証し、そのDKIM認証ドメイン名が複数得られるメール送信元IPアドレス
- 上記IPアドレスから送信され、SPFの認証がpassするSPF認証ドメイン名

転送メールでなく、SPFとDKIMの両方に対応した送信メールは、通常それぞれのドメイン名が同じか上位ドメイン名が同じであるなど、関連が強いことが期待できます。例えばDMARCでは、組織ドメイン名を定義し、SPFかDKIMの認証ドメイン名とヘッダ上の送信ドメイン名が同じか、同じ組織ドメイン名を持つことを前提としています。こうした仕様もあり、通常のメールでもSPFとDKIMの認証ドメイン名は、高い関連性があります。最初のメール送信元がDKIM対応している場合、転送時にSPFの認証ドメイン名を書き換えると、最初のDKIM認証ドメイン名と転送先でのSPF認証ドメイン名は関連のないドメイン名となることが一般的です。メール転送時にエンベロープFromを書き換える転送元を判断するために、SPFとDKIMの認証ドメイン名の関連性に着目します。この送信元IPアドレスを機械的に収集するために、同じ送信元IPアドレスからのメールで、SPF認証がpassし、さらにDKIMの認証ドメイン名が複数得られるメール送信元のIPアドレスを、メール転送元と判断し収集します。このメール転送元IPアドレスと、そこから送信されたSPF認証ドメイン名が、受け取るべき送信者レピュテーションとなります。

2.5 送信者レピュテーションの構築と検証

これらの手法の有効性を確かめるために、実際に送信者レピュテーションを構築し、受信メールに対して適用します。利用したのは、実際のメールサービスで受信したメールの受信ログです。このメールサービスでは、メール受信時にSPFとDKIMの送信ドメイン認証を行い、更にすべてのメールに迷惑メールフィルタを適用していますので、それらの結果をログから得ることができます。送信者レピュテーションによる判定結果の評価基準として、この迷惑メールフィルタの判定結果を利用しました。

つまり、SPFとDKIMの認証結果から送信者レピュテーションを構築します。次に受信したメールを送信者レピュテーションに適用し、それが迷惑メールフィルタの結果と比較し、迷惑メールでないメール(ham)に該当したか、迷惑メール(spam)に該当したか、それぞれの数を計測します。

送信者レピュテーションは、2019年9月の1ヵ月間の受信メールのログ、約3億4千万通から構築しました。この時の迷惑メール（spam）割合は11.7%で、SPFの認証pass割合は71.1%、DKIM認証pass割合は38.1%でした。これらのデータから抽出できた転送元IPアドレスは15,169、通常の転送元から送信されたSPFドメイン名数は744,660、転送時に送信ドメイン名を書き換えるドメイン名数は11,164得られました。

これら抽出した受け取るべき送信者レピュテーションを、レピュテーションの収集期間の直後、2019年10月の1週間、約3千6百万通の受信メールに適用しました（表-1）。適用には、同じく受信メールのログを利用しました。2つのレピュテーションの違いを以下に示します。

(1) 転送時に送信者情報を書き換えない通常の転送元（IP）とSPF認証ドメイン名
(2) (1)に転送時に送信者情報を書き換える送信元とSPF認証ドメイン名を追加

表-1のham（%）は、迷惑メールフィルタで迷惑メールと判定されなかったメールの中で、構築した送信者レピュテーションが適用できた割合。つまり真陽性（TP：True Positive）の割合を示しています。spam（%）は、迷惑メールフィルタで迷惑メールと判定されたメールで、送信者レピュテーションが適用されてしまった割合。つまり偽陽性（FP：False Positive）の割合を示しています。今回の評価は、例えばメールフィルタでの迷惑メール判定の場合の正の意味と異なり、受け取るべきメールが正となるため、レピュテーションとしての正解（TP）と誤判定（FP）の関係には注意が必要です。

表-1 送信者レピュテーションの適用結果

レピュテーション	ham（%）	spam（%）
(1)	47.45	3.01
(2)	58.01	3.26

2.6 考察

送信ドメイン認証技術を用いてメール転送元を判断し、それらを送信者レピュテーションとして構築することで、受け取るべきメール（ham）の約58%のメールを判断することができました。この時期、SPFの認証割合は7割程度であることから、そのうちのかなりの割合を送信者レピュテーションによって判定することができたと言えます。これは、転送時に送信者情報を書き換える転送元を検知し、それらを利用して送信者レピュテーションを追加できたことで、より効果を上げることができました。TP（真陽性）の割合を10pt以上高めることができています。それにもかかわらずFP（偽陽性）の割合は0.25ptだけの増加に抑えられています。送信者レピュテーションの適用期間では、受信メールに対するspam割合は約9%でしたので、誤判定したメールの実数としてはかなり低いものとなりました。また、このFPの原因についてもある程度は分かっていますので、よりFP割合を減らすことも可能と考えています。

本手法による送信者レピュテーションの構築手法は、メールの内容を参照して判断することなく、送信ドメイン認証技術の認証結果だけを利用しています。一般的なメールフィルタの手法と異なり、簡易的な手法であるにもかかわらず、高い精度の判定結果を得ることができました。転送メールの送信元判定についても、普及率が低いDKIMの認証結果を利用してはいますが、レピュテーション利用時に送信側がDKIMに必ず対応している必要はなく、転送元判定のために数通のDKIM認証されたメールだけを利用します。そのためDKIMの普及率が低くても、十分送信者レピュテーションを構築することができます。今回は送信者レピュテーションの構築及び適用対象として、普及率の高いSPFの認証ドメイン名を利用しましたが、SPFの普及率がよ

り高くなれば、更に判定できるメールを増やすことも期待できます。DKIMあるいはDMARCの普及率が高くなれば、それらの認証ドメイン名も送信者レピュテーションとして利用することも考えていくことができると思います。

これまでメール転送によってSPFの認証が転送先で失敗してしまうことは、SPF認証の欠陥と考えられてきました。しかしながら、逆にこのネットワーク方式のSPFと電子署名方式のDKIMそれぞれの特徴を活用する、送信者レピュテーションの構築手法を本稿で示し、その高い評価結果を示すことができたことは、SPFの普及のためにも有益であると考えています。

2.7 おわりに

フィッシングなどの迷惑メールの内容がより高度化し、本物と見分けがつかなくなってきている現在では、信頼できる送信者情報を利用してメールの受け取りを判断できる本手法の意義は大きいと考えています。また、送信者レピュテーション構築手法として、メール内容を参照する必要がないことは、プライバシー保護の観点からも有益な手法といえます。更に本手法の検証時に示したように、例えば受信メールログを利用して送信者レピュテーションが構築できる手法であるということは、自組織で受信するメールに適した送信者レピュテーションが得られるということであり、より精度の高い判定も期待できます。本レピュテーションで適用できないごく少数の受信メールに対しては、より多くの計算機資源が利用できるようになるわけですので、それらを活用し、メール内容などから深く判断する、といったことも可能になります。

送信ドメイン認証技術は、これまで導入しなくてもメールが届くという状態が続き、特に比較的新しいDMARCなどの普及がなかなか進んできませんでした。しかしながら今回、Google社や米国Yahoo社などの新たな受信対策の発表により、DMARCおよびそのベースとなるSPF、DKIMの普及が進んできたことは、なりすましメールの対策ができるようになったのと同時に、こうしたドメインレピュテーションが適用できる機会が増えることにもつながります。引き続き、より精度の高いドメインレピュテーションに関する研究を続けていきます。

執筆者:
櫻庭 秀次（さくらば しゅうじ）
IIJ 技術研究所 技術連携室 シニアリサーチエンジニア。博士(工学)。
メッセージングセキュリティに関する研究開発に従事。また快適なメッセージング環境実現のため、社外関連組織と協調した各種活動を行う。M^{3}AAWG(Messaging, Malware and Mobile Anti-Abuse Working Group)の設立時からのメンバー。JPAAWG(Japan Anti-Abuse Working Group)会長。迷惑メール対策推進協議会 座長代理、幹事会 構成員、技術WG 主査。一般財団法人インターネット協会 迷惑メール対策委員会 委員長、客員研究員。電気通信大学 協力研究員。

IIJとデータセンターの変遷〜この30年を振り返って

3.1 1990年代 「始まりはスペースの有効活用」

1985年の日本電信電話公社民営化(いわゆる通信の自由化)以前から、システムインテグレータではダウンサイジングの流れの中で計算機センターに設置されるコンピュータの小型化によって空いたスペースで他社のコンピュータを預かるビジネスがあり、国際通信会社ではこちらも交換機や伝送装置の小型化に伴って空いた通信局舎のスペースに外資系金融機関のディーラーホンや構内電話交換機を預かるビジネスがありました。いずれの建物も一般の建築物よりも頑丈に造られおり、それが今のデータセンターの原形であったと回想されます。

通信の自由化以前から、国際通信は国際電信電話株式会社(以下KDD、現在のKDDI)が専業で行っていましたが、自由化以降は複数の新規参入電気通信事業者(以下NCC)が参入し、更に自前の伝送装置を持たない第2種電気通信事業者(一般、特別)によってパソコン通信が普及し始めます。

1992年、IIJが創業し、苦労の末に特別第2種電気通信事業者として免許が交付されインターネットサービスを提供できるようになりました。最初に通信機器を設置したのは、千代田区大手町にあるKDD大手町ビル(現在はKDDI大手町ビル)でした。その後、千代田区神田神保町の岩波書店の地下にNSPIXP-1が設置されインターネットエクスチェンジ(以下、IX)での相互接続実験が始まると専用回線でルータを張り出しました。その後KDD大手町ビルにNSPIXP-2が設置されると、インターネットサービスプロバイダ(以下ISP)が集まり始めました。

ISPは専用回線や電話回線を大量に使うため、通信局舎にネットワーク機器を設置して伝送装置や交換機に構内接続することは理にかなっていますが、NTTの局舎はまだ広く解放されておらず、ISPは国内外に接続する必要があることから、KDDやNCC各社の通信局舎を使うのは当然の成り行きでした。NSPIXP-3は大阪にも開設され、1997年には日本インターネットエクスチェンジ株式会社やインターネットマルチフィード株式会社が設立されて商用IXが始まりました。日本におけるインターネットの骨格が形成された時代でした。

まだ、データセンターという言葉を使うこともなく、伝送設備の隣に一緒に置かれることからCo-Location、顧客の機器を預かることからHousingとも言われていましたが、冷房がキンキンに効いた「無機質で寒い部屋」というイメージで、1ラックあたり1〜2KVAを供給すれば十分だった時代です。

3.2 2000年代 「インターネットデータセンター」

1990年代の後半からのインターネット接続サービスの爆発的な拡大に伴って、たくさんのISPがこぞって通信局舎を借りてサービスを提供し始めました。こうした時代の後半となる1998年10月にIIJはソニーとトヨタ自動車と合弁で株式会社クロスウェイブ コミュニケーションズ(以下CWC)を設立し、NCCとして全国網を整備して行きました。その翌年には全国にアクセスポイントを開設しました。

それと同時に国内主要都市(札幌、仙台、東京、名古屋、大阪、福岡)において床耐荷重が少し大きなビルを選定し、無停電電源装置と非常用発電機を設置したデータセンターを開設し、その後、埼玉県川口市、神奈川県横浜市に土地から建物まで自社所有のデータセンターを建設しました。このときのコンセプトは「人に優しいデータセンター」で、統一した動線や休息のできるカフェテリアの設置、会議スペースやキッティングルームの整備など、無機質な計算機センターや通信局舎から

表-1 計算機センターと通信局舎の特徴的な違い

特徴	計算機センター	通信局舎(電報電話局)
空調方式	水冷(汎用大型機)	空冷(伝送装置、電話交換機)
電源供給	主として交流(3相200V) 発電機によるバックアップ	主として直流(DC-48V) CVCFによって交流でも供給可能
建物構造	オフィスビルと同等の設計 フリーアクセス床	電報電話局として設計 スラブ床
提供方法	スペース貸しが主体	ラック貸しが主体

インターネット時代のインテリジェントな建物へと変貌を遂げたのです。

CWCは、データセンター開設と同時にLANの標準インタフェースであったEthernetで接続できる広域LANサービスを提供しました。物理的に離れていてもLANとしてつながれて、あたかも1つのビルに入っているかのように使える通信サービス(“バーチャルビルディング”と呼んでいました)で、距離によらない料金体系と合わせて一世を風靡し、今ではL2通信サービスのデファクトスタンダードになっていると言っても過言ではありません。

こうしたネットワークとデータセンターの進化によって、メールサービスやWebサービス、セキュリティ対策としてのファイアウォールやリモートアクセスに必要な機器を各社が設置するようになり、ISPだけでなくいわゆるコンテンツプロバイダなどのOTT事業者も集まり、レンタルサーバサービスや各種ホスティングサービスの登場によって、単なる機器の置き場ではなくこれらのシステムをインターネットに接続するための機能を提供する場所になっていきました。

こうして、「インターネットデータセンター」と呼ばれるようになり、床耐荷重も1トン/平米を超え、電力供給も複数の電源フィードが敷設され1ラック当たり4〜6KVAを前提として電源設備や空調設備が設計される時代になりました。インターネットが以前から雲(クラウド)に例えて語られていたこともあり、インターネットデータセンターはクラウドサービスの提供拠点や接続拠点へと変化していきます。

3.3 2010年代「クラウドサービスへの対応」

ネットワークを介してコンピューティングリソースを提供するクラウドサービスでは、利用者に代わってサービス提供事業者がサーバなどのIT機器を所有運用しますが、大量のIT機器を高密度で実装し効率良く運営するために、1ラック当たり10KVAを超える電力を供給し冷却できるハイパースケールデータセンターの建設が2010年代には進んでいきます。

その受電容量は50MW規模になり、一般家庭(100V 50A 契約)の1万軒に相当します。単に規模が大きいだけではなく、省エネ性も備え、ハイパースケールデータセンターの普及によりエネルギー効率を示す指標であるPUE(Power Usage Effectiveness:データセンター全体の消費電力をIT機器の消費電力で除した値。1が最も良く日本の平均値が1.7)が改善されています。IIJは、クラウドサービス基盤を収容するデータセンターのために、10KVA/ラックの高密度実装を可能にし、外気冷却を用い高い省エネ性を持つコンテナモジュール「IZmo (イズモ)」を開発し、日本で初めての商用の外気冷却コンテナデータセンターの運用を2011年に開始しました。当時IIJは、他社から借りたデータセンターを再販する事業形態で、自社でデータセンターを建設したり、電気設備や空調設備を開発したりした経験はなく、その開発はゼロからのスタートでした。北米で先行しているGAFAなどのデータセンターの現地調査を行い、消費電力を低減するためには空調に外気冷却方式を導入することが最も効果があると判断し、段階的な設備増強が行えるコンテナと組み合わせる設備コンセプトを固め、パートナー企業と実証機を設計/製造し、1年間の実証を経て「松江データセンターパーク(以下松江DCP)」の構築を行うことができました。

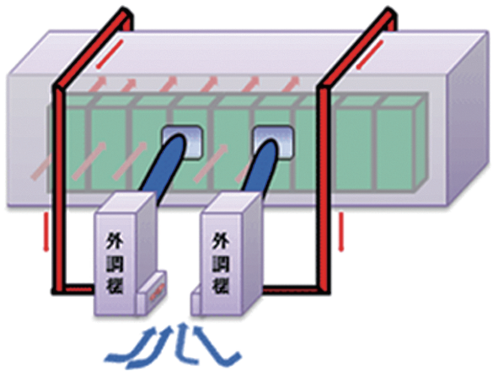
表-2 データセンター建設時の考慮事項

建設時の考慮項目	内容
建物構造	耐震構造、免震構造、免震床
受電系統	3スポットネットワーク、異変電所からの受電
電源供給	UPSの冗長化(待機冗長、並列冗長、共通予備方式)
通信回線	マルチキャリア、キャリアニュートラル、管路の冗長化
災害考慮	活断層からの距離、航空路直下の回避、ハザードマップ
地盤	地盤強度(N値)、液状化可能性指数
指標	PUE、WUE、PLM値、Tierレベルによる分類

IZmoは、最初に実装した出雲地方とクラウド(雲)にちなんで命名しましたが、その高い省エネ性能や設置が容易なことから、国内だけでなく、ロシアの水力発電所、ラオスのナショナルデータセンターなど海外に輸出し利用されています。現在は、ウズベキスタン国営通信事業者にデータセンターを提供するプロジェクトが進行中です。そして、エッジコンピューティングの普及に伴い、エッジコンピューティング環境や拠点のデジタル/IT基盤を、短期間で容易に構築、運用できるソリューション「DX edge (ディーエックス・エッジ)」として国内外に販売を行っています。

松江DCPは受電容量4MWと中規模なセンターですが、2010年代後半から本格的に外資のクラウド事業者向けに複数のハイパースケールデータセンターの建設が進んでいきます。そして、千葉ニュータウン中央駅周辺の印西地区からその集積が始まりました。「INZAI」といえば国際的にも通じるほど、データセンターの集積地として知名度が高い地域になっています。集積した理由は、地盤が強固、大手町30km圏内、海底ケーブル陸揚局からルート確保が容易、古くから電算センターが立地しておりインフラ整備が進んでいたなど複合的な理由が挙げられていますが、海外でもデータセンターは1ヵ所に集積する特徴があり、日本も例外ではないということになります。大阪の彩都地域や、京阪奈地区にも集積していて、今後も国内では大規模な複数の開発計画が進んでおり、この傾向は変わらないと考えられます。

IIJも2019年、事業規模の拡大に伴い、この印西地区(白井市は印西市に隣接)にハイパースケールデータセンターとして、「白井データセンターキャンパス(以下白井DCC)」を構築し、運用を開始しました。4万平方メートルの敷地に、最大受電容量50MWまで拡張可能で、松江DCPがコンテナ単位(9ラック)で増設するのに対し、白井DCCは、サービス基盤の増設単位が大きくなったことに対応するため、最初に1000ラック規模のシステムモジュール棟を建設し、その中を4つのモジュールに分割し、順次増設できる構造としました。また、外気冷却方式を大規模に実装し松江DCPと同様に高い省エネ性を備えています。空調は外気冷却に加えハイパースケールデータセンターでも多く取り入れられている壁吹き出し方式とし、低速で大容量のエアフローにより、従来の2重床の下から勢い良く冷気を吹き出す方式に比べ、省エネで働きやすい環境を実現しています。



2009年の企画初期の外気冷却コンテナモジュールコンセプト
(社内資料より抜粋)

2019年に運用開始した白井データセンターキャンパス

図-1 無から有を生み出し新しいデータセンターの形を創造

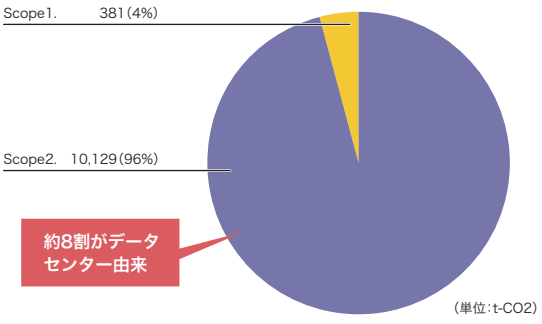
2010年代は、クラウドサービスの普及に伴い、ハイパースケールデータセンターの集積が進んだことや外資系事業者の市場参入などによりデータセンター業界が大きく変容しました。IIJは、この変化に対応するため、図-1のようにゼロからコンテナモジュールを開発し、ハイパースケールデータセンターの構築まで漕ぎ着けました。そして、2023年には白井DCC 2期棟の運用を開始し、現在は2026年の運用開始に向け3期棟の検討を進めており、AIや量子コンピューティングなど、これまで以上の激変が予測される2020年代に向けて、新たなデータセンターの形を模索し続けています。

3.4 2020年代「次世代のデータセンター」

こうした変遷をたどったデータセンターには、これから何が必要とされるでしょうか。データセンター設備のライフサイクルは10年以上と、IT機器の3〜5年と比較して長く、中長期視点で社会的な潮流や技術動向を捉えることが求められます。サステナビリティの要請や、生成AI/LLM、ポスト5Gといった技術革新が進みつつある中で、次世代のデータセンターに向けてIIJが注力する3つのテーマを紹介します。

■ カーボンニュートラル

IT機器を集約し効率的に運用するデータセンターの利用は、社会全体の省エネに貢献する一方、施設自体のエネルギー消費が注目されています。2023年に改正省エネ法が施行され、データセンター業にベンチマーク制度(PUE1.4以下)が導入されたことに加え、新たに非化石エネルギーへの転換計画の提出も義務付けられました。また、東証プライム上場企業にTCFD提言に基づく気候変動リスクの情報開示が実質的に義務化されたこともあり、データセンターのカーボンニュートラル化は喫緊の課題となっています。IIJにおいても、温室効果ガス排出量(Scope1、2)[*1]の約8割をデータセンターが占めており、「再生可能エネルギーの利用」と「エネルギー効率の向上」への目標を設定し取り組んでいます(図-2)。



IIJ単体2022年度実績

算定方法:「サプライチェーンを通じた温室効果ガス排出量算定に関する基本ガイドライン(Ver2.3)」(環境省、経済産業省)

・**再生可能エネルギーの利用**※1
2030年度におけるデータセンター(Scope1、2)の再生可能エネルギー利用率を85%まで引き上げる

・**エネルギー効率の向上**
2030年度まで技術革新の継続により、データセンターのPUEを業界最高水準の数値(1.4)※2**以下にする**

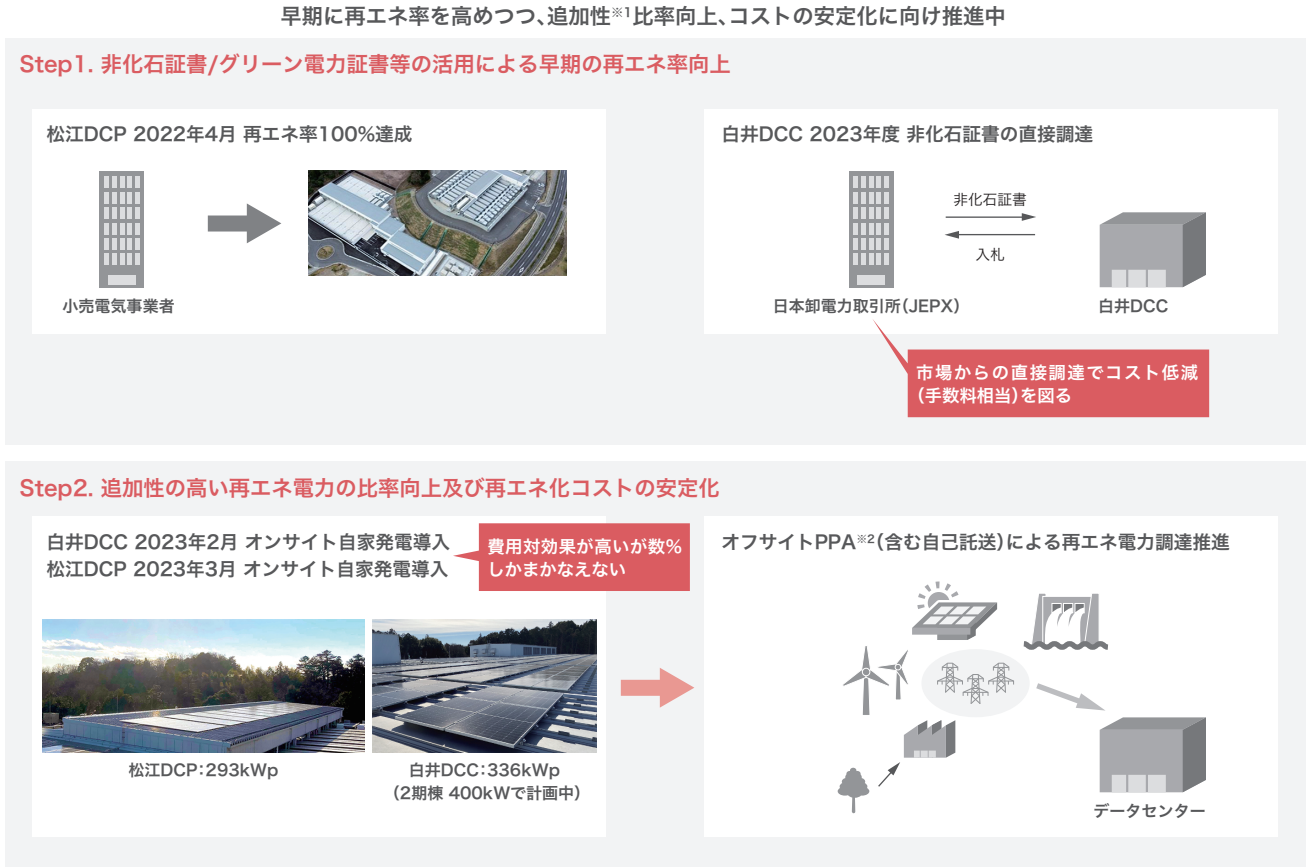
TCFD(Task Force on Climate-related Financial Disclosures)提言に基づく情報開示より

※1:再生可能エネルギーの利用には、非化石証書活用による実質再生可能エネルギーを含む。
※2:2022年4月時点において、資源エネルギー庁はデータセンター業におけるベンチマーク指標及び目指すべき水準をPUE1.4以下と設定し、達成事業者は省エネ優良事業者とみなされる。

図-2 IIJのカーボンニュートラルへの取り組み

＊1 Scope1、2(自社での温室効果ガス排出):自社での燃料の使用や工業プロセスによる直接排出及び自社が購入した電気・熱の使用に伴う間接排出(GHGプロトコル定義)。

「再生可能エネルギーの利用」は電力の「量」に加え、CO2を排出しない「発電種別」を意識する新たな取り組みです。IIJデータセンターでは、納期、コスト動向などにより各調達手法を評価し、複数の手法を組み合わせることで、早期に再エネ率を高めつつ、追加性の高い電力比率の向上、調達コストの安定化を図っています(図-3)。これまでに、一般社団法人日本卸電力取引所(JEPX)の「再エネ価値取引市場」に加入し市場から直接証書を調達したり、データセンター敷地内に太陽光発電設備を導入することで再エネ調達コストの低減を実現してきましたが、従来からの省エネ性の追求と合わせオフサイト電力の調達などによりカーボンニュートラルの達成を目指しています。そしてこれらのリソースを活用し、データセンター利用者へ環境価値を提供する新サービスを開始(2023年10月)しました(図-4)。2024年7月には、環境価値をデジタルアセット化(トークン化)して提供する計画で、環境価値取引のビジネス開発につながる取り組みも進めています(図-5)。また、データセンター内の蓄電池を利用したVPP(バーチャルパワープラント・仮想発電所)事業への参画(2023年度～)や、環境省が進める脱炭素先行地域に島根県松江市の共同提案者として参画し災害時に蓄電池による地域への電力供給を計画しており、電力網の安定化やレジリエンス強化といった社会課題の解決に貢献するデータセンターの新たな役割へも挑戦しています。



※1:新たな再エネ設備の増加・投資を促す効果があること。
※2:Power Purchase Agreement。電気使用者(需要家)と需要家に電気を売る電力事業者(PPA事業者)間で結ぶ電力販売契約。

図-3「再生可能エネルギーの利用」への取り組み

■ AI制御・自動化

データセンターにおいてカーボンニュートラルを実現するためには、使用するエネルギーの低減が必要不可欠です。サーバなどIT機器以外で消費されるエネルギーとして最も大きな割合を占めるものは、IT機器を冷却するための空調機器です。データセンターのPUEを最良値の1.0に近づけるため、IT機器の冷却に外気を積極的に用いたり、高効率な機器を採用しています。また、白井DCCでは、AI技術を活用して、省エネ性能をさらに向上させる取り組みを行っています。センサーやIT機器から得られたデータをAIに学習させることで、より効果的な空調システム全体の制御を目指しています。このような空調システムの自動的に加え、データセンターの入退館時の受付業務を自動化する「自動受付システム」をはじめ、データセンターサービスを提供する上で必要となる各種業務の自動化も推進し、データセンターで業務を行うオペレータの業務負荷軽減を図っています。国内の労働人口の減少、働き方改革といった動向から、データセンターの規模が拡大する中で提供品質を維持するにあたり、オペレーション要員の追加、育成といった人手に頼った体制維持が困難な状況になっていくと予想されるからです。自動化の領域は順次拡大することを考えており、例えば前節で述べたデータセンター利用者向けに環境価値付きの電力を供給する取り組みについても、電力需給マッチングプラット

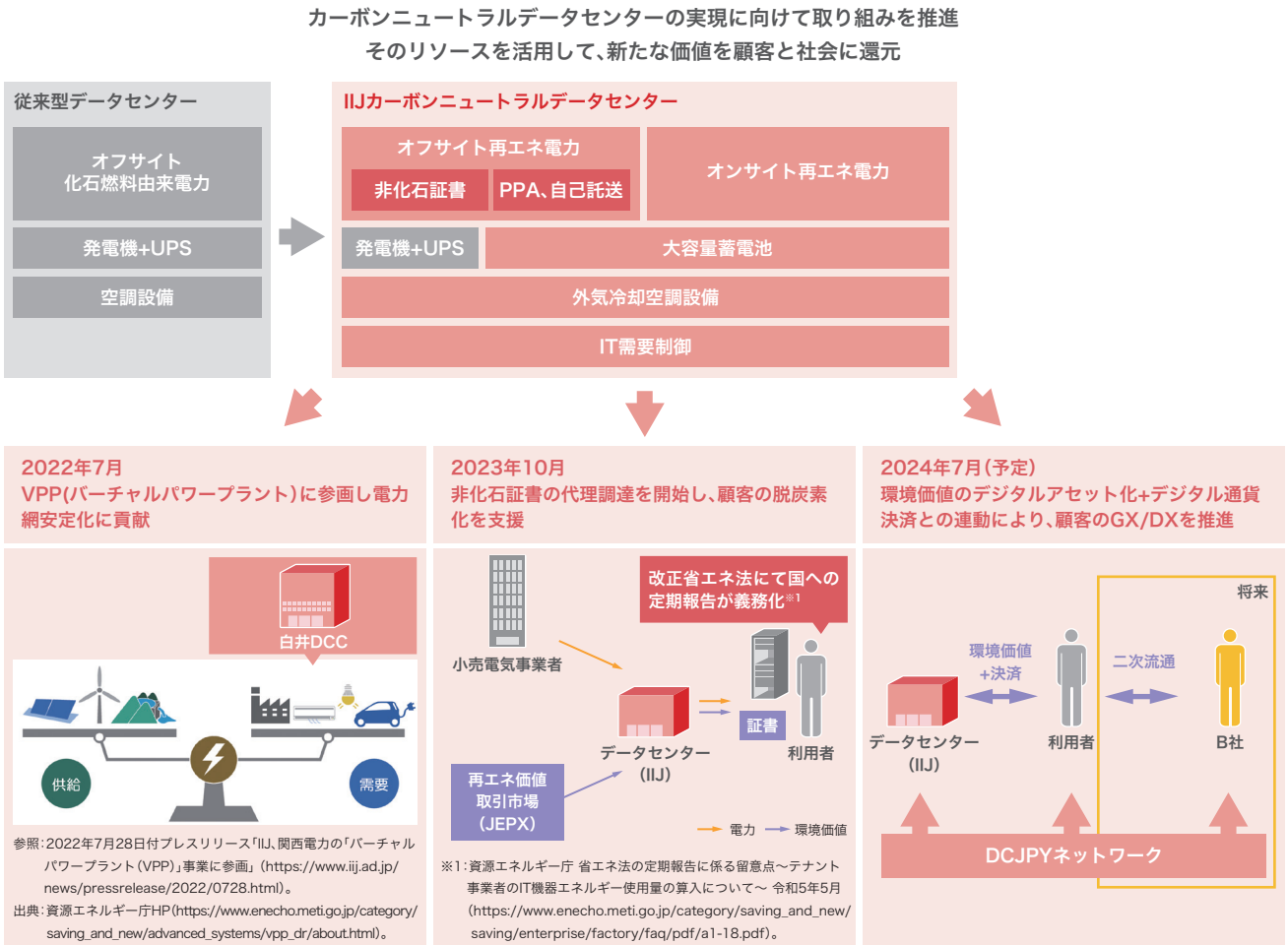


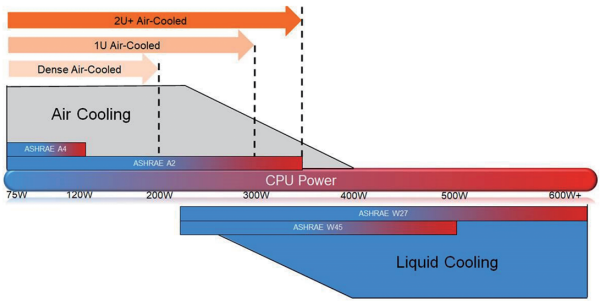
図-4 カーボンニュートラルデータセンターの先にあるもの

フォームの構築やデジタル通貨を用いた決済などを活用することで、単純な自動化に留めず、高度化、高品質化の達成を図りたいと思っています。

■ サーバ高密度化・水冷対応

生成AI/LLMなどの技術の活用が様々な分野で進み、CPU/GPUの処理能力が増大していく中で、これらのCPU/GPUを大量に効率良く設置できることが次世代のデータセンターには求められます。今後導入されるデータセンター向けCPUは、TDP（Thermal Design Power）が300Wを超えており、AI需要への対応のため今後更に増加していくと考えられます。アメリカ暖房冷凍空調学会「ASHRAE（アシュレー）」によれば、このTDPが300Wを超えると、従来の空冷ではなく水を使った水冷の冷却方式を導入する必要があるとされています（図-6）。

空気により冷却できるNW機器などのIT機器も混在するため、今後のデータセンターには空冷/水冷のハイブリッド冷却機能を備え、かつカーボンニュートラルを実現するための高い省エネ性能を実現することが求められます。IT機器とファシリティの結びつきも強くなり、これまでに大規模データセンター・クラウドサービスの構築・運営に実績を持つIIJの強みが生かせる領域であると考えています。IIJは、経済産業省、新エネルギー・



出典：Ashrae Emergence and Expansion of Liquid Cooling in Mainstream Data Centers（https://www.ashrae.org/file%20library/technical%20resources/bookstore/emergence-and-expansion-of-liquid-cooling-in-mainstream-data-centers_wp.pdf）。

図-6 TDP（CPU Power）と冷却方式

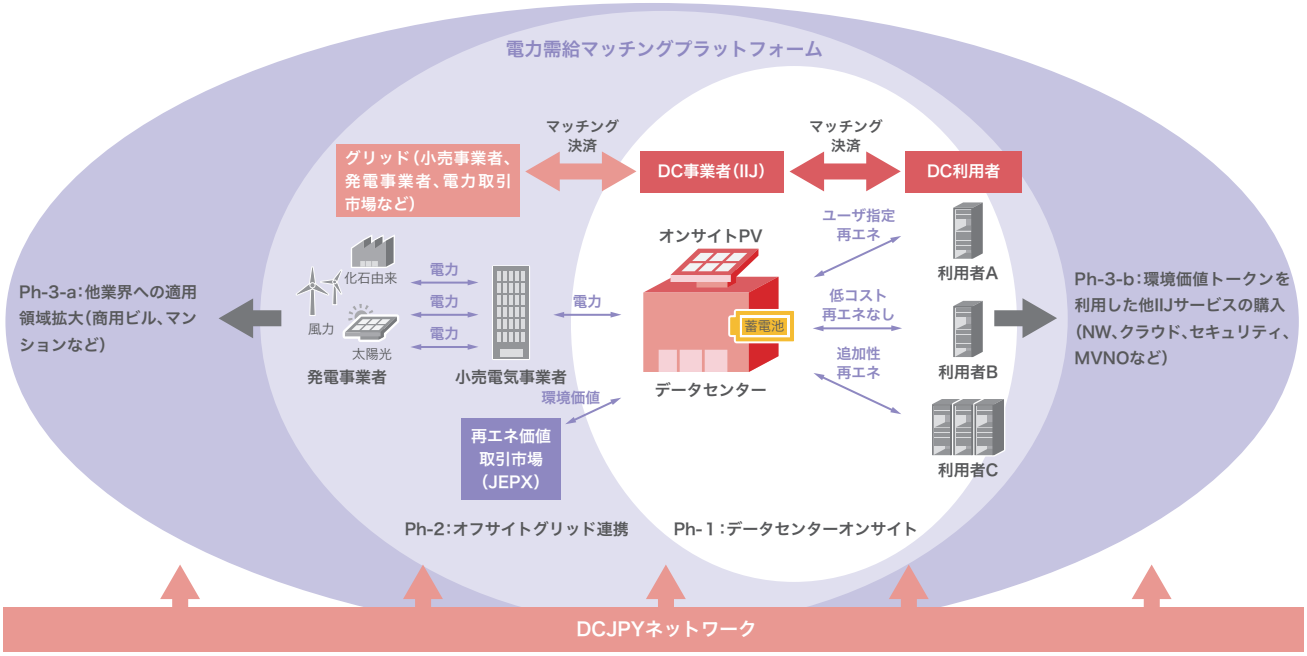


図-5 脱炭素ニーズの本格的な高まりに向けて

産業技術総合開発機構(NEDO)の公募「ポスト5G情報通信システム基盤強化研究開発事業／ポスト5G情報通信システムの開発(委託)」に株式会社Preferred Networks、国立大学法人北陸先端科学技術大学院大学と「超高効率AI計算基盤の研究開発」を共同提案し採択されました。IIJは高密度データセンターの基盤技術に関する研究開発を担い、高密度データセンターレファレンスモデルの開発や、空冷空調技術と水冷技術を組み合わせたハイブリッド冷却方式の確立、AI計算基盤に対応する省エネ評価指標の策定と評価方法の開発に取り組んでいきます。

3.5 まとめ

データセンターは、ITシステムの利用者から意識をされることは多くないものの、最近ではデジタル化社会を支える重要インフラとして認知が進みつつあります。計算機センター/通信局舎、コロケーション、クラウド、ハイパースケールとこれまでたどったデータセンターの道のりを踏まえ、今後も新しいデータセンターの形を追求し、社会を支えるインフラの運営を続けていきます。

執筆者:

山井 美和(やまい よしかず)
IIJ 常務執行役員 基盤エンジニアリング本部長

久保 力(くぼ いさお)
IIJ 基盤エンジニアリング本部 基盤サービス部長
2008年にIIJに入社。データセンター事業を統括し、松江DCP、白井DCCを構築。早期のカーボンニュートラル実現を目指す。

堤 優介(つつみ ゆうすけ)
IIJ 基盤エンジニアリング本部 基盤サービス部 データセンター基盤技術課長
2015年IIJに入社し国内外でのデータセンター構築に従事。電力分野での新技術検証等、次世代データセンターの技術開発を推進中。

三村 恭弘(みむら たかひろ)
IIJ 基盤エンジニアリング本部 基盤サービス部 データセンター基盤技術課

March 2024 Vol.62

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2024年3月時点のものです。

IIJ-MKTG019-0062

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