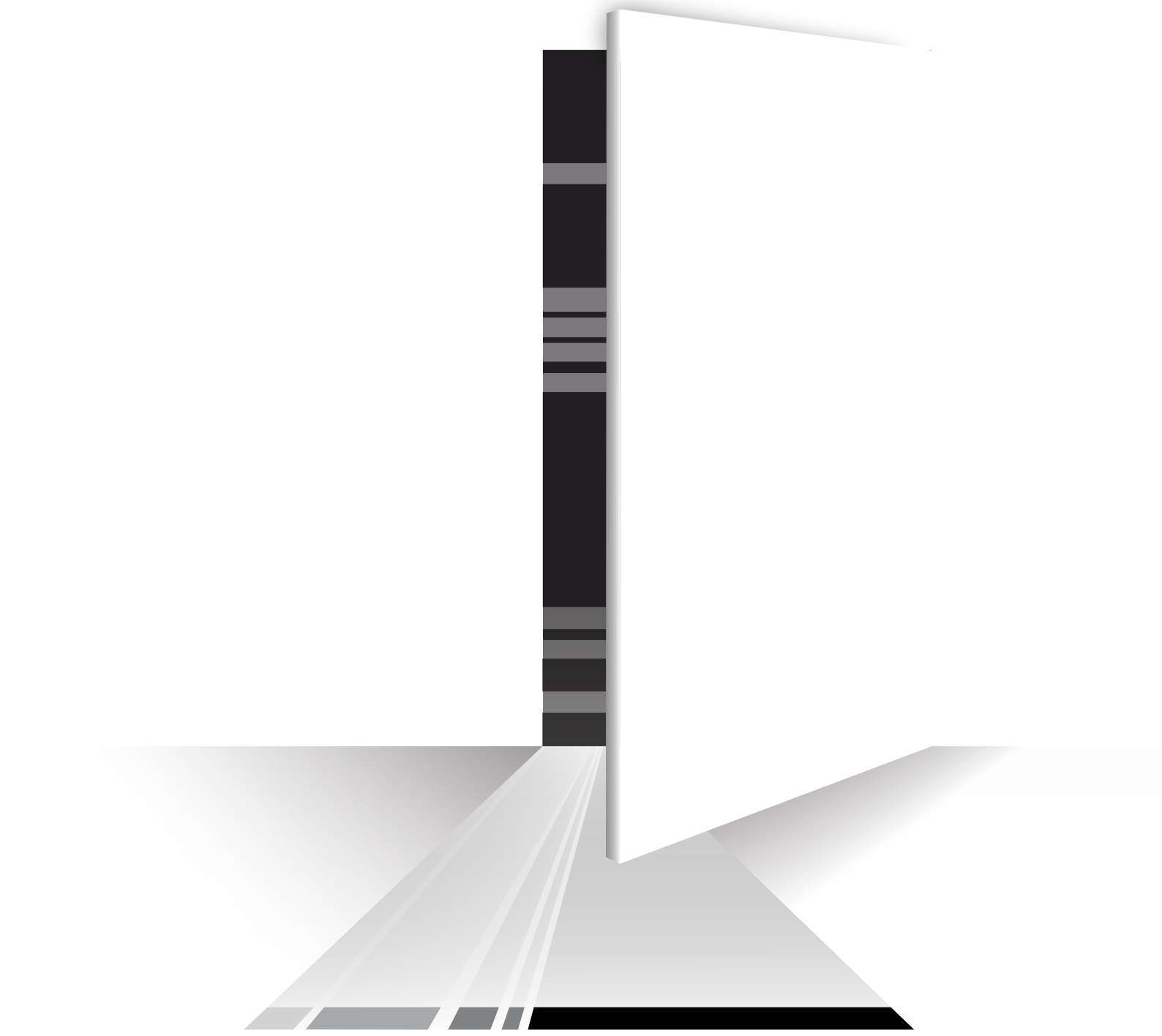
2024年度 DBIR
データ漏洩/侵害調査報告書

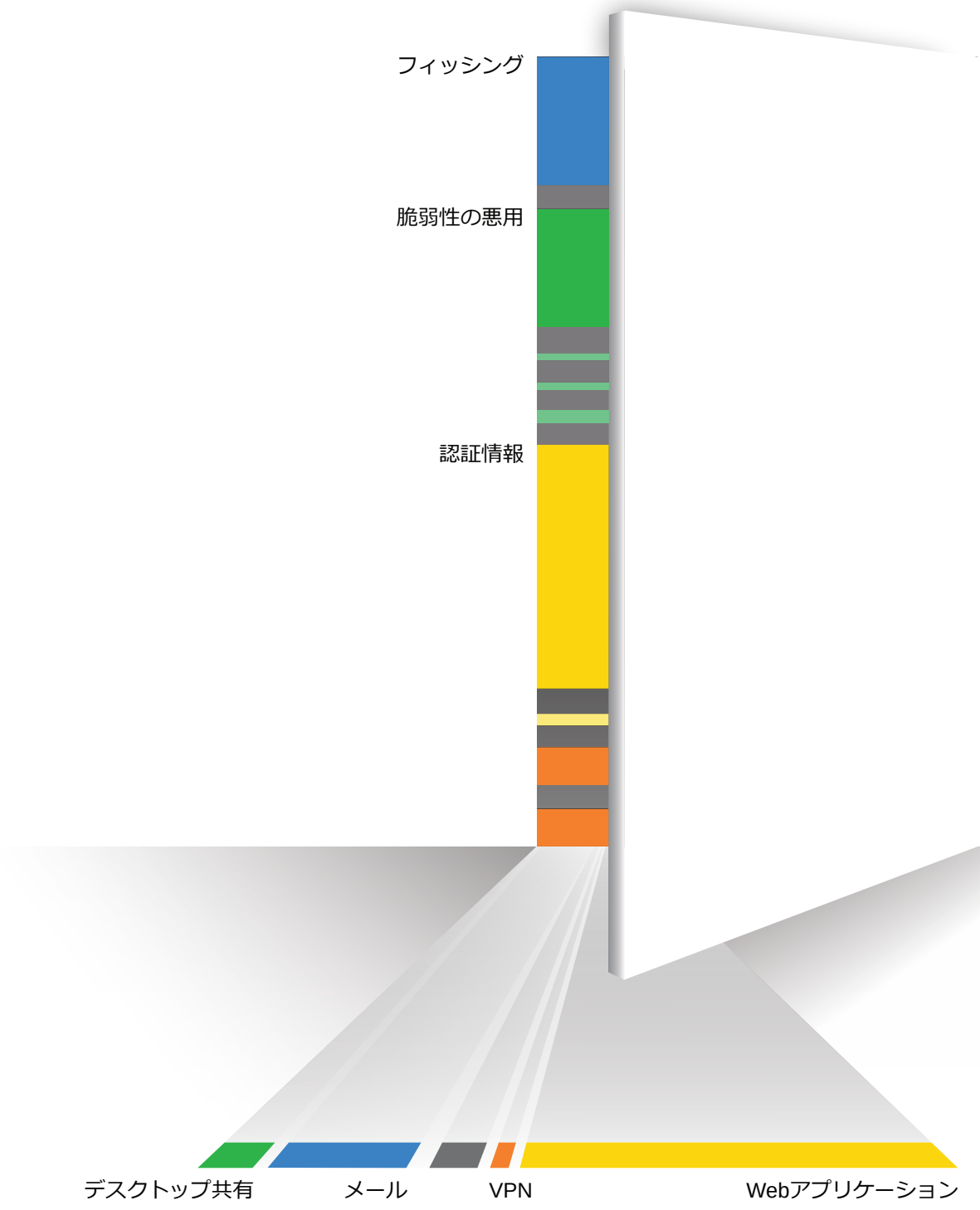
エグゼクティブサマリー



verizon business

表紙について

今年の報告書では、昨今の脅威の状況を踏まえ、データ漏洩/侵害を引き起こす可能性が最も高い攻撃と攻撃経路の組み合わせを特定するため、データ漏洩/侵害に至る経路をより深く掘り下げています。表紙に描かれた、鍵の壊されたドアから漏れ出る光は、部屋の中へ侵入する攻撃者がさまざまな方法を試みていることを表しています。ドアの隙間から見えるパターンは「侵入経路」の組み合わせの割合を示し（図7で詳しく説明）、床の光の帯は攻撃経路の量を示しています。次ページの図は、両パターンの割合と量を色付けし具体化したものです。このアートの意味を理解していただければ幸いです。


フィッシング
脆弱性の悪用
認証情報
デスクトップ共有
メール
VPN
Webアプリケーション

目次

はじめに

ベライゾンの2024年度データ漏洩/侵害調査報告書（DBIR）へようこそ

本書は今年で17回目を迎え、旧来の読者の皆様をまたお迎えするとともに、新しい読者の方に歓迎のご挨拶をさせていただけることを大変嬉しく思います。いつものように、DBIRの目的は、さまざまなタイプの攻撃者と、攻撃者が利用する手口および攻撃するターゲットに光を当てることです。Verizon Threat Research Advisory Center （VTRAC）のチームと共に、私たちにデータやインサイトを共有し続けてくださる世界中の才能ある、寛大で市民意識の高い外部の協力組織の方々のおかげで、私たちは、世界中のあらゆる規模や種類の組織において繰り広げられるサイバー犯罪に関連したトレンドを調査および分析することができるのです。

毎年、私たちは、新しい巧妙な攻撃や、依然として成功が実証されている攻撃バリエーションを目の当たりにしています。MOVEitに影響を与えた脆弱性のような、有名で広範囲に及ぶゼロデイ脆弱性の悪用から、より平凡ではありますが、依然として信じられないほど効果的なランサムウェアやサービス拒否（DoS）攻撃まで、犯罪者は、犯罪は報われないという古い格言が間違っていることを証明するために全力を尽くし続けています。

このようなサイバー脅威の変遷に、私たちは混乱させられ、圧倒され続けています。特に昨年はサイバー犯罪が多発した年でした。私たちは、過去最多となる30,458件の実際に発生したセキュリティインシデントを分析しました。そのうち10,626件はデータ漏洩/侵害が確認されたもので、被害は94か国に及びました。この後のページでは、報告書からの重要なポイントをいくつか取り上げていますので、皆様のお役に立てていただければ幸いです。

業種や地域におけるデータ侵害/漏洩に関する最新の調査結果など、報告書のハイライトで引き続きご確認ください。また、このエグゼクティブサマリーを同僚の方と共有したり、完全版をダウンロードして、現在直面している可能性がある脅威について、さらに詳しくご確認ください。

主な調査結果

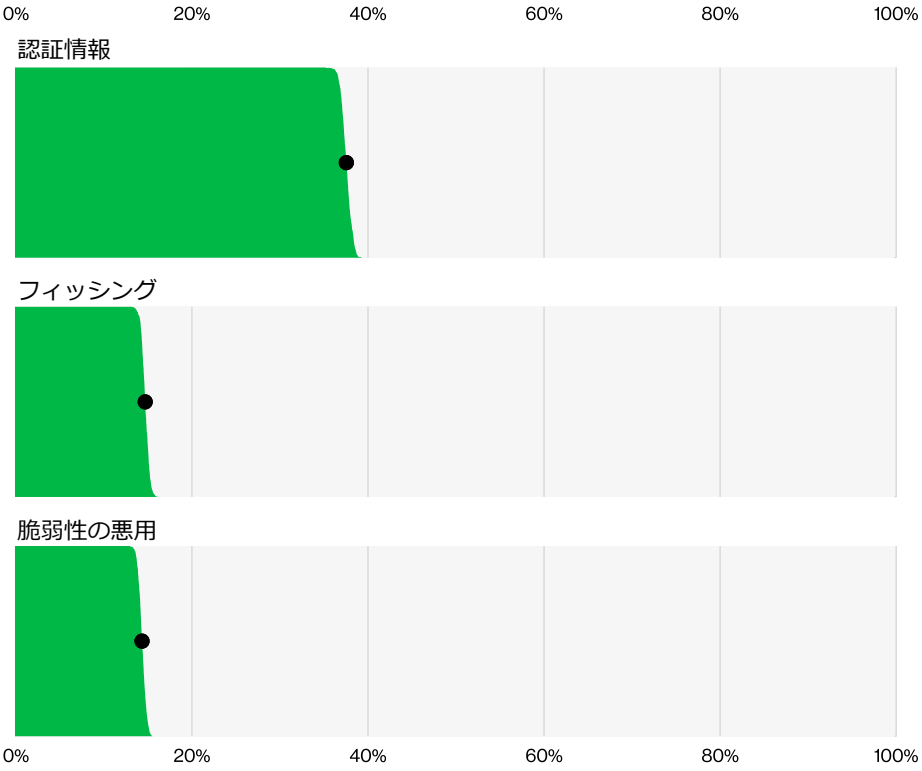


図1. 「エラー」/「（内部）悪用」を除いたデータ漏洩/侵害における上位の主な侵入手段（n=6,963）

侵入経路の分析では、データ漏洩/侵害を開始するためのクリティカルパスとして脆弱性を悪用する攻撃が、前年と比較して大幅に増加していることが確認されています。昨年のほぼ3倍（180%増）もの件数になっていますが、これは、MOVEitや同様のゼロデイ脆弱性の影響によるところが大きく、主に「ランサムウェア」やその他の「脅迫」関連の攻撃者が、Webアプリケーションを最初の侵入経路として利用しています。

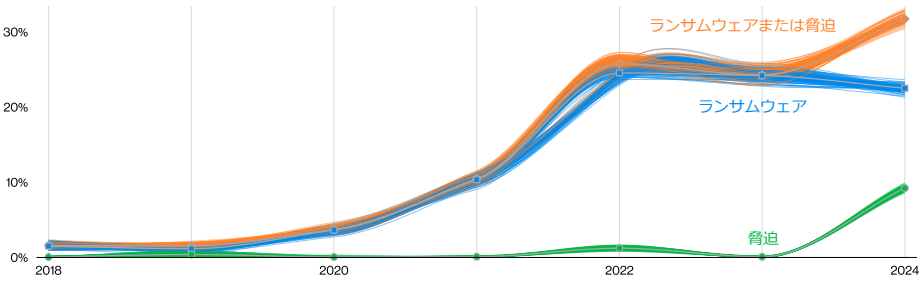


図2. 「ランサムウェア」と「脅迫」によるデータ漏洩/侵害の経時的変化

全侵害のおよそ3分の1が「ランサムウェア」またはその他の「脅迫」手口を使用しています。「脅迫」攻撃だけでもこの1年で増加し、現在では全データ漏洩/侵害の9%を占めています。従来のランサムウェアの攻撃者がこれらの新しい手口に移行した結果、「ランサムウェア」の割合は23%とやや減少しました。しかし、攻撃者が同じであるとしたら、この2つの脅威を合わせるとデータ漏洩/侵害における割合は大きくなり、32%に達します。「ランサムウェア」は全業種の92%に出現し、最大の脅威となっています。

図3. データ漏洩/侵害における上位の主な要因

セキュリティ意識がもたらす影響を明らかにするために、悪意ある「特権の悪用」を除外して、人的要素の関与に関する計算を修正しました。今年のデータセットでは、人的要素がデータ漏洩/侵害の68%に関与しており、これは昨年の分析結果とほぼ同じです。

今年のDBIRでは、サードパーティが関与する侵害の概念を拡大し、パートナーのインフラが影響を受ける場合や、直接的または間接的なソフトウェアにおけるサプライチェーンの問題（サードパーティのソフトウェアの脆弱性によって影響を受ける場合を含む）なども視野に入れました。つまり、サードパーティが関与する侵害とは、組織がより優れたセキュリティ実績を持つベンダーを選択することで、軽減または防御できる可能性のある侵害と考えられます。この数字が今年は15%に達し、前年比68%増となったのは、「ランサムウェア」や「脅迫」攻撃でのゼロデイエクスプロイトの利用が主な原因です。

今年のデータセットでは、「エラー」が関与したデータ漏洩/侵害の件数が増加し、現在では28%に達していますが、これは、新たにデータ漏洩/侵害の通知が義務化された組織を含めるためにデータ提供組織の数が増加したためです。これは、メディアや従来のインシデント対応によるバイアスによって信じ込まされている現状認識以上に、エラーが蔓延しているのではないかという私たちの疑念を裏付けるものです。

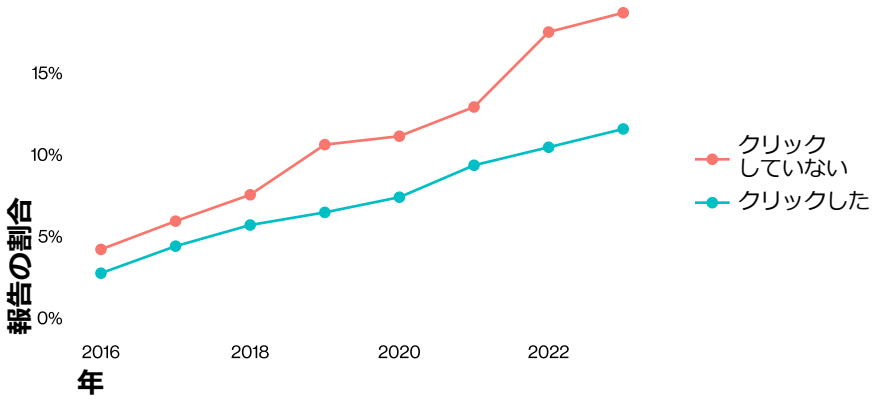


図4. クリック状況別フィッシングメールの報告の割合

フィッシングの報告は全体的にここ数年増加傾向にあります。2023年にパートナーから寄せられたセキュリティ意識向上に関するトレーニングデータでは、フィッシングシミュレーションにおいてユーザの20%がフィッシングを報告し、11%がメールをクリックしたことを報告していますが、一方、メールを開いてから悪意あるリンクをクリックするまでの時間の中央値は21秒で、その後データを入力するまでにさらに28秒しかかからないという事実があります。ここから、ユーザがフィッシングメールに引っかかるまでの時間の中央値は60秒未満という憂慮すべき事実が浮かび上がります。

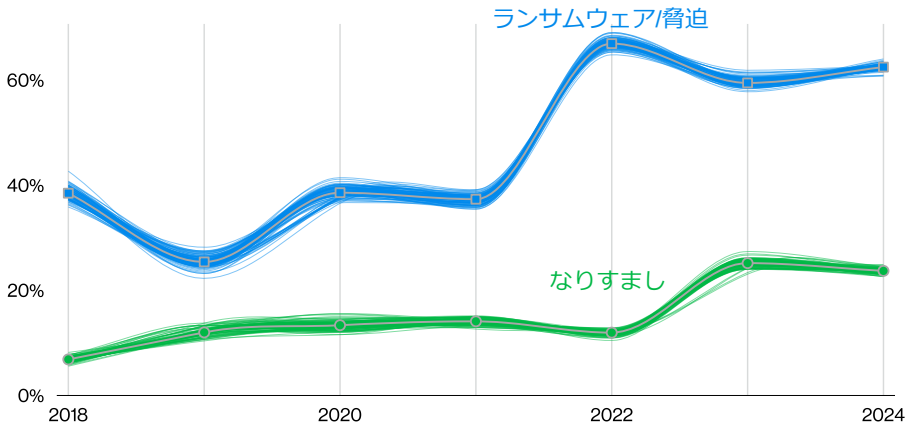


図5. 金銭目的を動機とする主な攻撃の種類の経時的変化

金銭目的を動機とする攻撃者は、通常、投資対効果（ROI）が最も高い攻撃手法に固執します。

過去3年間、「ランサムウェア」とその他の「脅迫」攻撃の組み合わせによるデータ漏洩/侵害は、これらの攻撃のほぼ3分の2（59%～66%の間で変動）を占めています。

FBIのインターネット犯罪苦情センター（IC3）のランサムウェア苦情データによると、これらの攻撃に関連する損失の中央値は46,000ドル（95%のケースで3ドル～1,141,467ドルの間）でした。また、身代金交渉のデータ提供組織からの報告からは、最初に要求された身代金と企業収益の比率の中央値は1.34%でしたが、80%のケースで0.13%～8.30%の幅があることがわかりました。

同様に、過去2年間で「なりすまし」（その大半は「ビジネスメール詐欺（BEC）」）が関与するインシデントが、金銭目的を動機とする攻撃の4分の1（24%～25%）を占めるようになりました。BECによる被害金額の中央値は両年とも約5万ドルでした。

業種別のハイライト

以前の報告書でも述べたように、ある業種では夜も眠れないほど深刻であっても、別の業種ではレーダーにかすりもしません。それは、サイバー犯罪の格好の餌食となる「攻撃対象領域」にすべて集約されるからです。特定のタイプの攻撃者の特徴、各業種を支えるテクノロジー基盤、組織が扱い保持するデータの種類、そのデータへのアクセスと運用などを考慮して、セキュリティ上の複雑な要素を混ぜ合わせた強力なカクテルができあがります。

モバイルデバイスとそれぞれのアプリを導入し、デジタル環境を整備しているハイテク大企業におけるリスクの特徴は、ベンダーがサポートするPOSシステムやシンプルなeコマースプラットフォームに依存する小規模なファッション小売業とは明らかに異なります。結局のところ、企業が直面する脅威は、業種、規模などによって異なります。さらに、これらの調査結果は報告要件にも影響されるため、業種によってその観点からの精査のレベルが異なる可能性があります。このセクションでは、報告書で取り上げている9つの業種の概要を説明しています。最後に、業種の分類は北米産業分類システム（NAICS）に基づいています。

宿泊および飲食業
(NAICS 72)

頻度	インシデント220件、確認されたデータ漏洩106件
上位3つのパターン	「システム侵入」、「ソーシャルエンジニアリング」、「基本Webアプリケーション攻撃」がデータ漏洩/侵害の92%を占めている
攻撃者	外部（92%）、内部（9%）複数（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（100%）（漏洩/侵害）
侵害されたデータ	認証情報（50%）、個人情報（28%）、決済情報（19%）、システム情報（19%）、その他（16%）（漏洩/侵害）
昨年との比較	ランサムウェアとソーシャル攻撃は、この業種では依然として根強い問題であり、インシデントの35%を占めています。
サマリー	「ソーシャルエンジニアリング」が劇的に増加しており、現在ではこの業種におけるインシデントの25%を占めています。そのうち「なりすまし」は昨年の2倍以上に増加し、インシデント全体でも20%を占めています。

教育サービス業
(NAICS 61)

頻度	インシデント1,780件、確認されたデータ漏洩1,537件
上位3つのパターン	「システム侵入」、「ソーシャルエンジニアリング」、「多種多様なエラー」が侵害の90%を占める
攻撃者	外部（68%）、内部（32%）（漏洩/侵害）
攻撃者の動機	金銭目的（98%）、スパイ活動（2%）（漏洩/侵害）
侵害されたデータ	個人情報（83%）、内部情報（20%）、その他（18%）、認証情報（9%）（漏洩/侵害）
昨年との比較	この業種では昨年と同じ3つのパターンが大半を占めています。個人情報を盗む「外部」の攻撃者がデータ漏洩/侵害の大半を占めています。
サマリー	内部攻撃者の犯行による「多種多様なエラー」と「外部」攻撃者者による「脅迫」が、引き続きこの業種の”カリキュラム”を構成しています。

金融および保険業
(NAICS 52)

頻度	インシデント3,348件、確認されたデータ漏洩1,115件
上位3つのパターン	「システム侵入」、「多種多様なエラー」、「ソーシャルエンジニアリング」が侵害の78%を占める
攻撃者	外部（69%）、内部（31%）（漏洩/侵害）
攻撃者の動機	金銭目的（95%）、スパイ活動（5%）（漏洩/侵害）
侵害されたデータ	個人情報（75%）、その他（30%）、銀行情報（27%）、認証情報（22%）（漏洩/侵害）
昨年との比較	「多種多様なエラー」は、この業種を悩ませ続けています。昨年同様、「誤送信」はこの業種にとって目の前の課題となっています。
サマリー	今年の「金融および保険業」においてトップの脅威は、「多種多様なエラー」と「基本Webアプリケーション攻撃」を抜いて「システム侵入」となり、「ソーシャルエンジニアリング」の増加とともに、より複雑な攻撃へシフトしていることを示しています。また、欧州・中東・アフリカ（EMEA）の状況把握が進んだため、「ランサムウェア」攻撃が同地区で健在であることが明らかになりました。

医療および社会福祉業
(NAICS 62)

頻度	インシデント1,378件、確認されたデータ漏洩1,220件
上位3つのパターン	「多種多様なエラー」、「特権の悪用」、「システム侵入」が侵害の83%を占める
攻撃者	内部（70%）、外部（30%）（漏洩/侵害）
攻撃者の動機	金銭目的（98%）、スパイ活動（1%）（漏洩/侵害）
侵害されたデータ	個人情報（75%）、内部情報（51%）、その他（25%）、認証情報（13%）（漏洩/侵害）
昨年との比較	「システム侵入」によるデータ漏洩/侵害が、依然として攻撃パターンの上位3つに入っています。
サマリー	今年の「医療および社会福祉業」では、例年と比べて大きな変化が見られました。内部関係者が意図的に引き起こすデータ漏洩/侵害は、2018年以降着実に減少していましたが、再び2位に急浮上しています。興味深いことに、攻撃者が好む標的として「個人情報」が「医療情報」を上回っています。

情報産業
(NAICS 51)

頻度	インシデント1,367件、確認されたデータ漏洩602件
上位3つのパターン	「システム侵入」、「基本Webアプリケーション攻撃」、「ソーシャルエンジニアリング」が侵害の79%を占める
攻撃者	外部（79%）、内部（21%）、複数（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（87%）、スパイ活動（14%）（漏洩/侵害）
侵害されたデータ	その他（46%）、個人情報（45%）、認証情報（27%）、内部情報（22%）（漏洩/侵害）
昨年との比較	上位3つの攻撃パターンは昨年と同じで、順位も変わっていません。昨年よりもデータ漏洩/侵害の件数が増加していることを考えると、少し興味深い結果です。
サマリー	データセット全体でデータ漏洩/侵害のサンプル数は昨年より増加していますが、この業種で発生したインシデントは大幅に減少しています。「システム侵入」のパターンでは、「ランサムウェア」と「盗まれた認証情報の悪用」が引き続き大半を占めていますが、「ソーシャルエンジニアリング」のパターンでは、「フィッシング」攻撃がわずかに減少し、「なりすまし」が増加しています。また、この業種を標的にした「スパイ活動」や、国家の支援を受けた攻撃者も若干増加しており、検知機能を強化する必要性が増しています。

製造業
(NAICS 31–33)

頻度	インシデント2,305件、確認されたデータ漏洩849件
上位3つのパターン	「システム侵入」、「ソーシャルエンジニアリング」、「多種多様なエラー」が侵害の83%を占める
攻撃者	外部（73%）、内部（27%）（漏洩/侵害）
攻撃者の動機	金銭目的（97%）、スパイ活動（3%）（漏洩/侵害）
侵害されたデータ	個人情報（58%）、その他（40%）、認証情報（28%）、内部情報（25%）（漏洩/侵害）
昨年との比較	昨年の上位3つのパターンのうちの2つがまだ残っており、「金銭目的」の動機がほとんどが攻撃の原動力となっています。
サマリー	「製造業」では「エラー」絡みのデータ漏洩/侵害が増加しています。「盗まれた認証情報を悪用」してハッキングした後に、マルウェアをインストールする手口がある程度普及しています。

専門的・科学的・技術的サービス業
(NAICS 54)

頻度	インシデント2,599件、確認されたデータ漏洩1,314件
上位3つのパターン	「ソーシャルエンジニアリング」、「システム侵入」、「多種多様なエラー」が侵害の85%を占める
攻撃者	外部（75%）、内部（25%）（漏洩/侵害）
攻撃者の動機	金銭目的（95%）、スパイ活動（6%）（漏洩/侵害）
侵害されたデータ	個人情報（40%）、認証情報（38%）、その他（33%）、内部情報23%）（漏洩/侵害）
昨年との比較	この業種では、「個人情報」「認証情報」が依然として上位を占めています。
サマリー	「ソーシャルエンジニアリング」は、この業種が直面している最大の脅威の1つであり、データ漏洩/侵害の40%を占めています。また、「誤送信」などのエラーも増加しています。

公務
(NAICS 92)

頻度	インシデント12,217件、確認されたデータ漏洩1,085件
上位3つのパターン	「多種多様なエラー」、「システム侵入」、「ソーシャルエンジニアリング」が侵害の78%を占める
攻撃者	内部（59%）、外部（41%）（漏洩/侵害）
攻撃者の動機	金銭目的（71%）、スパイ活動（29%）（漏洩/侵害）
侵害されたデータ	個人情報（72%）、内部情報（37%）、その他（31%）、認証情報（17%）（漏洩/侵害）
昨年との比較	「システム侵入」と「ソーシャルエンジニアリング」の攻撃パターンが、依然としてこの業種の上位3つに入っています。
サマリー	この業種では「多種多様なエラー」、特に「誤送信」が急上昇しており、データ漏洩/侵害につながるミスの共通性を反映しています。「システム侵入」が第2位、「ソーシャルエンジニアリング」がそれに続きます。内部関係者による要因が圧倒的に多いことは、従業員の不注意がもたらす潜在的な結果を浮き彫りにしており、「エラー」がデータ漏洩/侵害の大半を占めています。

小売業
(NAICS 44–45)

頻度	インシデント725件、確認されたデータ漏洩369件
上位3つのパターン	「システム侵入」、「ソーシャルエンジニアリング」、「基本Webアプリケーション攻撃」が侵害の92%を占める
攻撃者	外部（96%）、内部（4%）（漏洩/侵害）
攻撃者の動機	金銭目的（99%）、スパイ活動（1%）（漏洩/侵害）
侵害されたデータ	認証情報（38%）、その他（31%）、決済情報（25%）、システム情報（20%）（漏洩/侵害）
昨年との比較	上位3つの攻撃パターンは変化がないだけでなく、順位も昨年と同じです。「金銭目的」を動機とする攻撃者によって依然と標的にされています。
サマリー	この業種では通常、「ペイメントカード」の情報が盗まれることが多いですが、攻撃者の焦点は「認証情報」に移りつつあります。「フィッシング」が減少する一方で、「なりすまし」が増加しています。「サービス拒否（DoS）」攻撃は、「小売業」にとって依然として悩みの種であり、顧客へのサービス提供や商品の販売に支障をきたしています。

地域別の分析

2024年度DBIRでは、改めて各地域のサイバー攻撃をマクロ的観点から考察します。世界のサイバー攻撃のトレンドが地域によってどのように異なり、またどのような共通性を持っているのか、読者の皆様が迅速かつ簡単に知るための一助となれば幸いです。これまでも述べてきたように、データ提供協力組織の有無、各地域の情報開示規制、ベライゾン所有のデータ数など、さまざまな要因によって、それぞれの地域についての可視性は変動します。読者の皆様が、サイバー犯罪についてのよりグローバルな見解をご覧になり、有益な情報として参考にしていただければ幸いです。

アジア太平洋地域（APAC）

頻度	インシデント2,130件、確認されたデータ漏洩523件
上位3つのパターン	「システム侵入」、「ソーシャルエンジニアリング」、「基本Webアプリケーション攻撃」が侵害の95%を占める
攻撃者	外部（98%）、内部（2%）（漏洩/侵害）
攻撃者の動機	金銭目的（75%）、スパイ活動（25%）（漏洩/侵害）
侵害されたデータ	認証情報（69%）、内部情報（37%）、機密情報（24%）、その他（17%）（漏洩/侵害）

欧州、中東、アフリカ（EMEA）

頻度	インシデント8,302件、確認されたデータ漏洩6,005件
上位3つのパターン	「多種多様なエラー」、「システム侵入」、「ソーシャルエンジニアリング」が侵害の87%を占める
攻撃者	外部（51%）、内部（49%）、（漏洩/侵害）
攻撃者の動機	金銭目的（94%）、スパイ活動（6%）（漏洩/侵害）
侵害されたデータ	個人情報（64%）、その他（36%）、内部情報（33%）、認証情報（20%）（漏洩/侵害）

北アメリカ（NA）

頻度	インシデント16,619件、確認されたデータ漏洩1,877件
上位3つのパターン	「システム侵入」、「ソーシャルエンジニアリング」、「基本Webアプリケーション攻撃」が侵害の91%を占める
攻撃者	外部（93%）、内部（8%）（漏洩/侵害）
攻撃者の動機	金銭目的（97%）、スパイ活動（4%）（漏洩/侵害）
侵害されたデータ	個人情報（50%）、認証情報（26%）、内部情報（19%）、その他（16%）（漏洩/侵害）

常に情報を得て脅威に備える

今日の脅威に立ち向かうには、信頼できる情報源からのインテリジェンスが必要です。

DBIRの完全版には、防御の準備や組織の教育に役立つ攻撃者、攻撃、攻撃のパターンに関する詳細がまとめられています。組織を保護するために必要なインテリジェンスを入手してください。

2024年度DBIRの完全版は、verizon.com/dbirでご確認いただけます。

サイバーセキュリティの世界をより安全な場所にしたいとお望みなら・・・。

もしあなたの組織でインシデントやセキュリティ関連のデータを持っており、毎年発行されるベライゾンDBIRへのデータ提供組織になることにご興味を持たれた方は（そうであってほしい）、その手続きはとても簡単でわかりやすいものです。dbircontributor@verizon.com宛にメールを送信していただくだけです。

DBIRの改善に関するご意見、ご質問をお待ちしております。お気軽にdbir@verizon.comまでメールでご連絡ください。または、X（@VZDBIR）までお問合せいただくか、VERIS GitHubページ（https://github.com/vz-risk/veris）をご覧ください。

verizon business