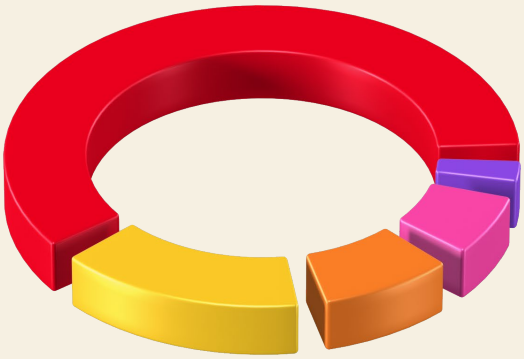
2026年度 データ漏洩/侵害調査報告書（DBIR）

エグゼクティブサマリー

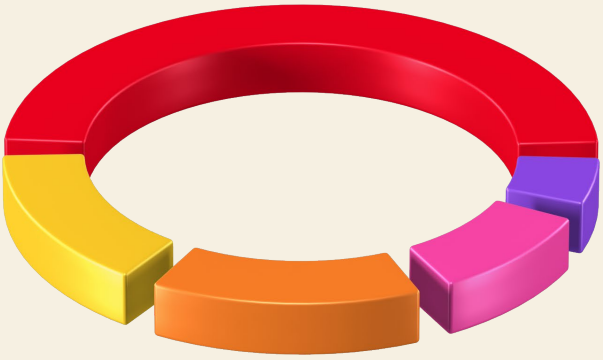
verizon business

2026年



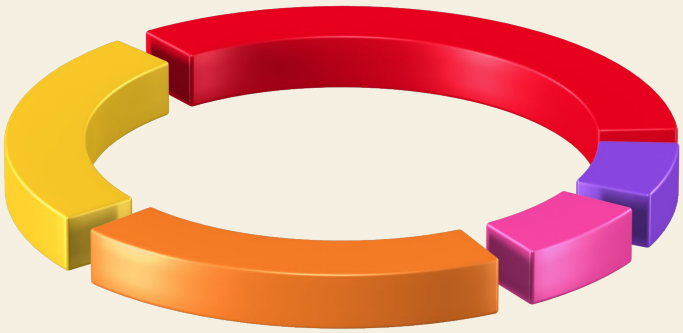
- **61%** システム侵入
- **17%** ソーシャルエンジニアリング
- **10%** 基本Web アプリケーション攻撃
- **8%** 多種多様なエラー
- **3%** 特権の悪用

2025年



- **53%** システム侵入
- **18%** 基本Web アプリケーション攻撃
- **17%** ソーシャルエンジニアリング
- **12%** 多種多様なエラー
- **7%** 特権の悪用

2024年



- **36%** システム侵入
- **25%** 多種多様なエラー
- **22%** ソーシャルエンジニアリング
- **9%** 基本Web アプリケーション攻撃
- **8%** 特権の悪用

表紙について

「唯一不変なるものは変化なり」という格言は、古代ギリシャの哲学者ヘラクレイトスの言葉として広く知られています。彼がサイバーセキュリティの実務に携わったことを示す歴史的な証拠はもちろんありませんが、この考え方はまさに現代のサイバーセキュリティの本質を突いていると言えるでしょう。しかし、脅威環境が絶えず進化し変化していく中でも、「2026年度データ漏洩/侵害調査報告書（DBIR）」では、サイバーセキュリティの基礎原則こそが、こうした変化に立ち向かうために最も重要であることを示しています。言い換えれば、冷静かつ着実にサイバーセキュリティの本質へ向き合う姿勢が求められているということです。

表紙では、私たちが蓄積してきた各年のデータを表す同心円状のリングが、上から降りてきて重なり合い、やがてサイバーセキュリティの知見という土台へと定着していく様子が描かれています。これらは私たちの理解を深め、防御戦略を補完するものであり、過去4年間のインシデントパターンごとに分類されています。

最上部の円は2026年度の報告書を表し、その下が2025年度版、2024年度版と続き、そして2023年度版はすでに土台にしっかりと定着しています。

ゼロデイ攻撃や重大な脆弱性は年々増加しています。生成AI（GenAI）によって強化されたマルウェアは今や珍しいものではなくなり、巧妙化したソーシャルエンジニアリングはデータ漏洩/侵害の前段攻撃として、ますます高い成功率を収めるようになっています。確かに、攻撃のスピードは上がっており、その規模も懸念材料かもしれませんが、それらはすべて、防御側が長年にわたり直面してきている課題です。だからこそ、この新たな世界では、大きな変革ではなく、より高い集中力と俊敏性が求められるのです。必要なのは、革命ではなく、進化です。より良い未来のために協力し合い、共に歩み続けることで、私たちは未来へ備えることができるはずです。

ちなみに、あのリングは実はドーナツチャートです。そう見えても、それは間違いではありません。

目次

はじめに

ベライゾンの2026年度データ漏洩/侵害調査報告書（DBIR）へようこそ。長年にわたり私たちを支えてくださっている読者の皆様、そして今回初めてお読みになる皆様にも、これまで通り、本報告書をお届けできることをうれしく思います。

今年で第19版になるベライゾンのDBIRでは、31,000件を超える実際のセキュリティインシデントを詳細に分析しました。そのうち22,000件以上は、145か国のさまざまな組織で発生したデータ漏洩/侵害であることが確認されています。これは、単年の報告書で分析された件数としては過去最多となります！毎年同じことをお伝えしているように思われるかもしれませんが、他の表現が見つかりません。事実として、調査対象となる件数は毎年増加を続けているのです。これは良いことなのか、そうではないのかは、読者の皆様に判断を委ねます。被害を受けた組織にとっては間違いなく後者になりますが、企業が直面する脅威の実態を明らかにするという私たちの目的においては、確実に前者の立場が当てはまります。

本報告書の全体的なテーマをひと言で表すなら、「変化のなかでも強固な基盤を維持すること」になるでしょう。今日、私たちの生活のあらゆる側面において、かつてないスピードで変化に直面していることは誰もが認めることでしょう。本報告書で提供するインサイトは、企業がサイバーセキュリティにおける変化に対して、最も効果的な方法で対処できるようにサポートすることを目的としています。なお、本報告書のデータセットは2024年10月から2025年11月までの期間を対象としていますが、DBIRチームおよびベライゾンは、本書の発行時点で確認された初期の兆候や傾向に基づき、2026年に入ってからのAIを活用した脆弱性調査や攻撃手法の影響力と能力の高まりを強く認識しており、その点に関する将来を見据えた考察も適宜盛り込んでいます。

2025年度の報告書発表以降、一部の地域ではサイバー犯罪の性質が大きく変化していることが確認されています。一方で、変化というよりは、スピードや規模が問題になっている他のケースも明らかになっています。本報告書の複数のセクションで取り上げているように、「脆弱性の悪用」は現在、攻撃者が組織環境へ侵入するための最も一般的な初期アクセス経路となっています。このことは基本対策を着実に実践し続けることの重要性を改めて示しています。さらに、“昔から”[1]予測されてきた通り、攻撃者は標的の選定、侵入経路の確保、脆弱性の調査、マルウェアやその他のツールの開発など、攻撃のさまざまな段階において、その攻撃の効果と効率を高めるために、生成AIの活用を進めています。一方で、長年にわたり主要な攻撃手法であり続けている「ソーシャルエンジニアリング」も進化しており、攻撃者はますます音声やその他のモバイルデバイスを活用した手法を駆使して、勤務時間中に利用者の不意を突く攻撃を仕掛けています。

主要な調査結果に加え、業種や地域ごとの最新の事例を含む報告書のハイライトについては、引き続きこのエグゼクティブサマリーをお読みください。また、ぜひこのサマリーを同僚の皆様と共有いただき、さらに現在直面する可能性のある脅威のより詳細な分析については、報告書の完全版をダウンロードしてご確認ください。

1. ここで言う“昔から”とは、過去2回のDBIRで予測されていたことや、数段落前に言及されていたことを指します。

本書の凡例と定義

2026年度 データ漏洩/侵害調査報告書（DBIR）へようこそ。

本報告書を初めて読まれる方は、最初にこのセクションをお読みいただくことをお勧めします。私たちはこの報告書の作成に長い間取り組んできて、使われている言葉が少々難解であることも理解しています。しかし命名規則、用語、定義については慎重に検討し、さらに報告書全体においてこれらを統一させるために多くの時間をかけています。分かりにくい箇所もあるかと思いますが、本セクションの定義によって理解を深めていただければ幸いです。長年の読者の方（ありがとうございます！）で、すでにDBIRの使い方に精通している場合は、次のセクションに進んでください。

このセクションの内容

データ漏洩/侵害調査報告書（DBIR）では、ベライゾンが毎年約100のデータ提供組織から収集している匿名化されたサイバーセキュリティインシデントデータに焦点を当て分析しています。 これらのデータポイントは、Vocabulary for Event Recording and Incident Sharing（VERIS）フレームワーク（詳細は次ページを参照）を用いて正規化されており、この種のデータの統計的に分析するための優れた基盤を提供します。これらのケースには依然として機密性（そしてインシデント対応の難しさ）がつきまとうため、特定のインシデントに関する詳細な情報をすべて把握できていないことがよくあります。

しかしながら、本報告書の最大の特長は、データ収集の幅広さです。特定のベンダーのレポートでは、自ら調査した事例については非常に信頼性の高い形で詳細に記述できますが、本報告書では、大規模なインシデントレスポンス企業、専門的なフォレンジック会社、地方レベルから国家レベルまでの法執行機関、サイバー保険ブローカー、再保険会社など、様々な視点や協力組織のタイプからデータを集約することで、脅威の背景にある真の“実態”に迫ることを目的としています。

VERISフレームワークのリソース

「攻撃（threat action）」、「攻撃者（threat actor）」、「種類（variety）」という言葉が何度も登場します。これらは、一貫性をもって正確にセキュリティインシデントの詳細情報を収集するためのフレームワーク“Vocabulary for Event Recording and Incident Sharing（VERIS）”で使用される用語の一部です。以下に、各用語の定義を示します。

攻撃者（Threat actor）：情報セキュリティ事象の背後にいる人物。フィッシング詐欺を仕掛けている外部の「悪者」の場合もあれば、飛行機の座席ポケットに機密文書を置き忘れた従業員の場合もあります。

攻撃（Threat action）：資産に影響を及ぼすために使用された手口（行為）。VERISでは、「マルウェア」、「ハッキング」、「ソーシャルエンジニアリング」、「不正使用/悪用」、「物理的攻撃」、「エラー」、「環境」という7つの主要攻撃カテゴリーを使用します。大まかな例としては、サーバーのハッキング、マルウェアのインストール、ソーシャルエンジニアリング攻撃によって人の行動に影響を及ぼすことなどが挙げられます。

種類（Variety）:上位カテゴリーをより具体的に分類した区分。例えば、外部の「悪者」を組織犯罪グループに分類したり、ハッキング行為をSQLインジェクションやブルートフォースとして記録しています。

「ベクトル」「動機」「カテゴリー」といった用語も登場しますが、各セクションでは用語体系への理解を深め、それらの用語の解釈を明確にするよう努めています。また、報告書全体を通して「」で示した記述が見られる場合は、VERISの“固有名詞”を指しており、フレームワーク内では特定の意味が結び付けられています。ファンタジーの世界と同じく、物事の本質を正確に見抜き、“正しく名付けること”には大きな意味があります。

詳細情報はこちらをご確認ください。

- github.com/vz-risk/veris ー フレームワークのJavaScript Object Notation（JSON）スキーマとその使用法、ユーティリティスクリプト、列挙リスト、Center for Internet Security（CIS）の重要なセキュリティコントロール、MITRE ATT&CK、および VERISスタイルガイドへのマッピング
- verisframework.org ー フレームワークに関する情報を例や列挙リストとともに提供する、ややユーザフレンドリーなWebサイト

インシデント vs. 漏洩/侵害

本報告書に多く登場するインシデントと漏洩/侵害という言葉は、以下の定義で使用しています。

インシデント：情報資産の完全性、機密性、可用性を損なうセキュリティ事象。

漏洩/侵害：権限のない者への（データ漏洩の可能性だけでなく）データ漏洩が確認されたインシデント。例えば、「分散型サービス拒否（DDoS）」攻撃は、データの流出がないため、ほとんどの場合、データ漏洩/侵害ではなくインシデントに分類されます。だからといって、深刻度が低くなるわけではありません。

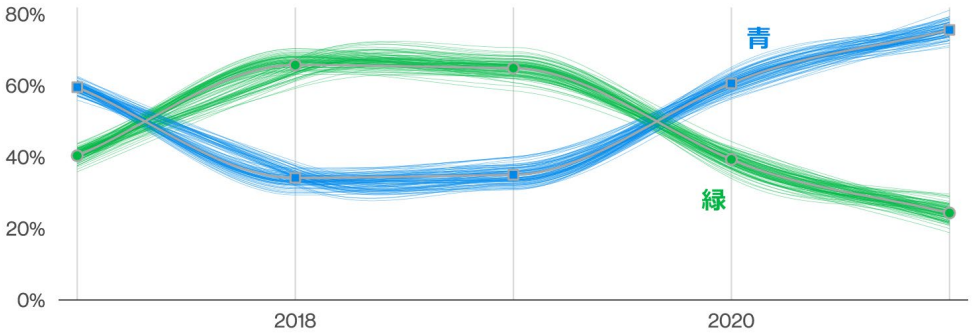


図1. スパゲッティチャートの例

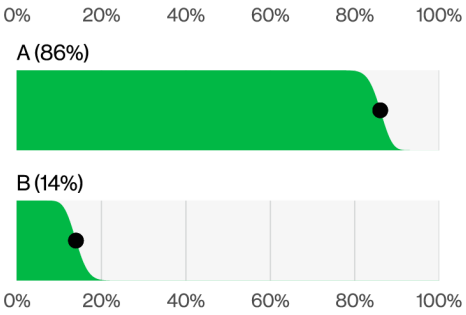


図2. 斜めカットの棒グラフの例（n=230）

業界区分表示

ベライゾンのコーパス（対象データセット）では、被害に遭った組織の分類に関し、北米産業分類システム（North American Industry Classification System：NAICS）の基準に沿っています。この基準では、企業および組織の分類に、2～6桁のコードを使用しています。通常、私たちでは2桁レベルでの分析を行っており、業界区分にNAICSコードを併記しています。例えば、グラフに「金融業（52）」という区分表示がある場合、52という数字は調査結果の値ではなく「金融および保険業」を表すNAICSコードです。図内では、簡潔にするため「金融業」という総称的な区分表示を使用しています。コードおよび分類システムに関する詳細情報は、census.gov/naicsでご確認いただけます。

自分たちのデータに自信をもつ

2019年に斜めカットの棒グラフをDBIRに導入して以来、情報セキュリティについて唯一確かなことは、確かなものは何もないということであると訴え続けてきました。すべてのデータが揃っていても、絶対に正しいと言えることはありません。しかし、データの少ない環境では何も測定ができないと諦めたり、最悪の場合、単に作り話をしたりするのではなく、私たちのチームはきちんと仕事をします。今年度の報告書でも、引き続きこの不確実性を数値で表現しています。

図1～図3はいずれも、真実となりうる現実の範囲を示しています。棒グラフの斜めカット、スパゲッティチャートの糸、ドットプロットの点、ピクトグラムチャートの色など、いずれも独自の方法で業界の不確実性を表現しています。

斜めカットの棒グラフは、毎号のDBIRの読者にはおなじみのものです。棒グラフの斜めカットは、そのデータポイントの95%の信頼水準に対する不確実性を表しています（これは統計的検定のごく標準的なものです）。平たく言えば、2本（またはそれ以上）の棒グラフの斜めカットが重なっている場合、片方がもう片方より大きいとは言えないということです（そんなことをしたら、数学の神様たちに激怒されます）。

斜めカットの棒グラフとよく似て、スパゲッティチャートも、時間という要素が加わり多少複雑にはなっていますが、信頼区間内に存在する可能性のある値という同じ概念を表しています。個々の糸は、各観測の信頼区間内に存在するポイント間のすべての可能なつながりのサンプルを表します。

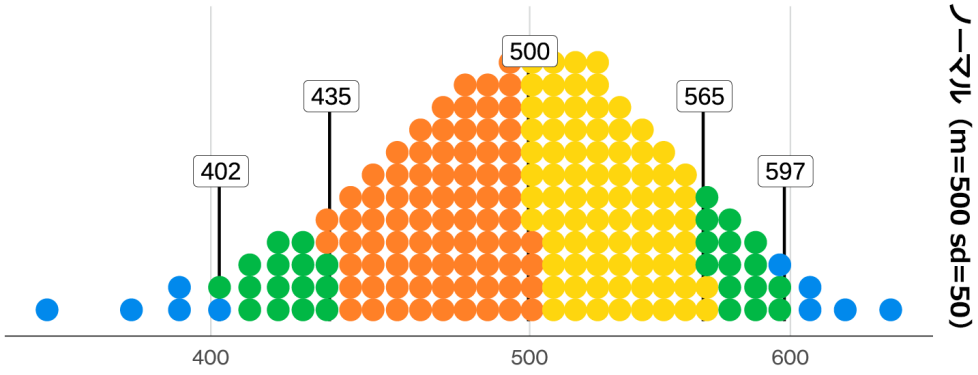


図3. ドットプロットの例（n=10,000 – 各ドットは1つのイベント）
オレンジ：80%の下半分。黄色：80%の上半分。緑：80%–95%。青：異常値。
イベントの95%：402–597。イベントの80%：435–565、中央値：500

見てわかるように、いくつかの糸は他よりも緩く、より広い信頼区間とより小さい標本サイズを示しています。

ドットプロットもよく使われますが、このグラフを理解するコツは、ドットが図のキャプションに記載されている特定のイベント数を表していることを覚えておくことです。これは、組織間での分布状況を理解する上で非常に優れた方法であり、平均値や中央値よりもはるかに多くの情報を提供します。より分かりやすくするために、色や吹き出しを追加しました。統計的に言えば、これは単なる量子化された密度チャートです。統計以外の観点から言えば、色付きの小さなドットを嫌いな人はいないですよね？

主な調査結果

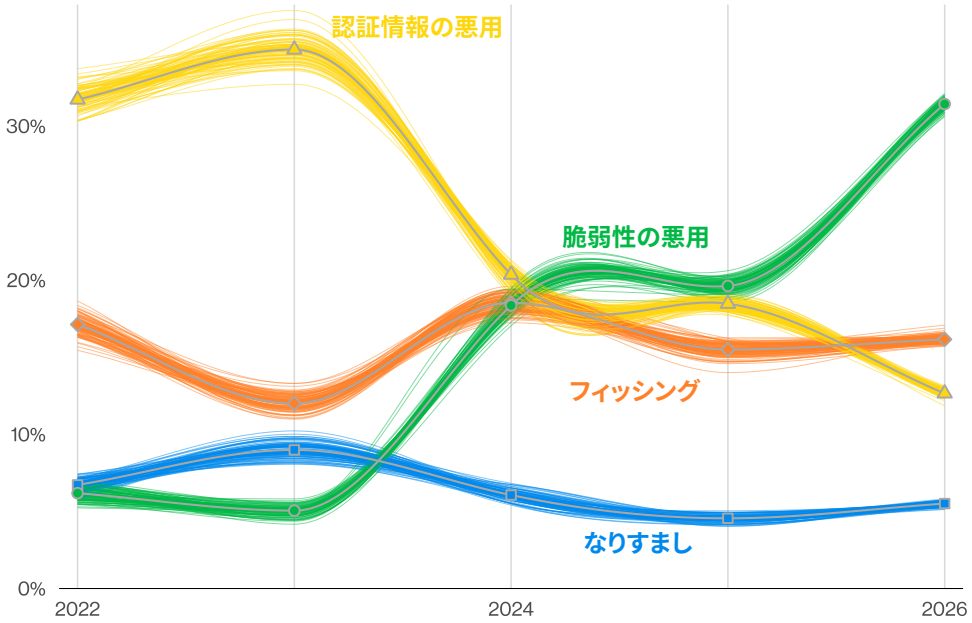


図4.「エラー」および「（内部）悪用」を除くデータ漏洩/侵害における既知の初期アクセス経路の推移（2026年データセット：n=19,905）

脆弱性悪用の増加

「脆弱性の悪用」は、現在、データ漏洩/侵害における最も一般的な初期アクセス経路となっています。今年のデータセットでは、その割合は31%に上昇した一方、以前最も多かった「認証情報の悪用」は13%まで低下しています。

また、アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁（CISA：Cybersecurity Infrastructure and Security Agency）のKnown Exploited Vulnerabilities（KEV）カタログに記載されている重大な脆弱性のうち、2025年中に組織によって完全に修正されたのはわずか26%で、前年の38%から減少しました。

完全な修正に要した日数の中央値は43日で、前年の32日より約2週間増加しました。中央値で見た場合、今年のデータセットでは、組織が修正する必要のあった重大な脆弱性の数が前年比で50%増加しています。

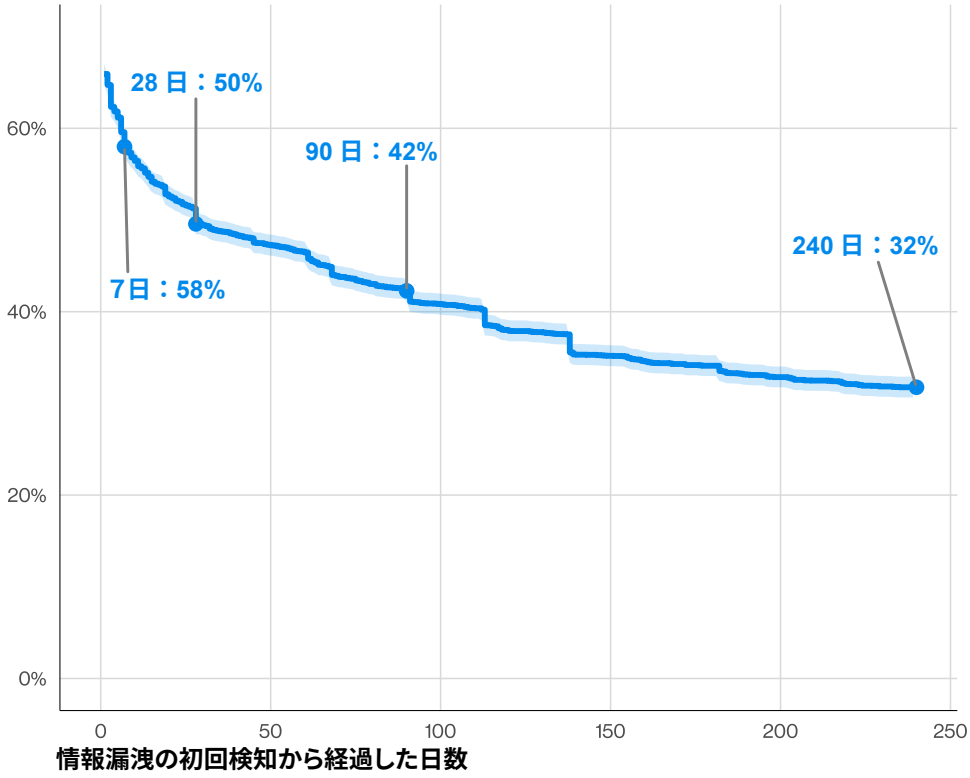


図5. サードパーティのクラウド環境におけるMFA（多要素認証）設定不備の是正状況の推移分析（n=7,513）

増加するランサムウェアとサードパーティが関与するデータ漏洩/侵害

ランサムウェアは今年も増加し、全データ漏洩/侵害において前年の44%から48%に上昇しました。一方で、DBIRのデータセットではランサムウェアの被害を受けた組織の69%が身代金の支払いを拒否しており、支払い件数は引き続き減少傾向にあります。また、支払われた身代金の中央値も引き続き減少傾向にあり、前年の150,000ドルから、今年のデータセットでは139,875ドルに減少しています。

組織がサービスやソフトウェアに関してサードパーティへの依存度を高めるにつれて、リスクにさらされる可能性も高まり、サードパーティが関与したデータ漏洩/侵害は昨年から60%増加し、全体の48%に達しました。

サードパーティのクラウド環境において露呈した問題の修正状況を時系列で見てみると、クラウドアカウント上の多要素認証（MFA）の未設定または設定不備を完全に是正したのはわずか23%にとどまりました。一方、検出された問題の50%は1か月以内に修正されています。

また、脆弱なパスワードやアクセス権限の設定ミスに関しては、検出された問題の50%が解消されるまでに約8ヶ月という長い時間を要しています。

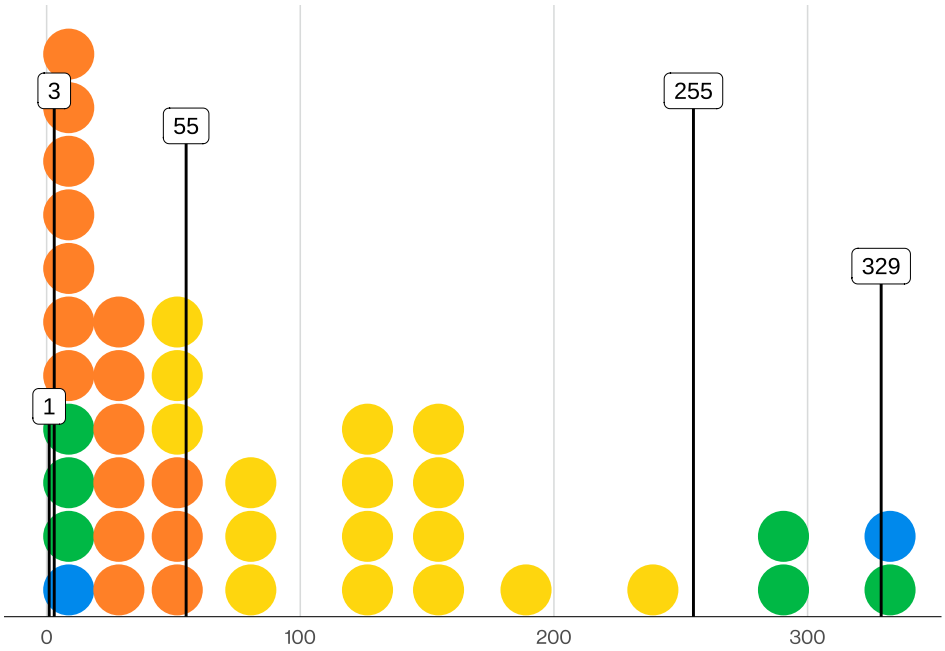


図6. 観測されたATT&CK手法ごとの既知マルウェアの種類の分布
（n=9,897、1ドットは247.43件の観測結果を表す）

脅威環境に影響を与える生成AI

攻撃者は、標的の選定、初期アクセスの獲得、マルウェアやその他の攻撃ツールの開発など、攻撃のさまざまな段階で生成AIを活用しています。中央値で見ると、攻撃者は、15種類の異なる既知の攻撃手法の開発や活用にAIの支援を受けていました。中には40～50種類もの攻撃手法でAIを活用していた「攻撃者」も確認されています。

AIを活用したマルウェアや攻撃ツールの開発の多くは、すでによく知られた攻撃手法に関連していました。同様の機能を持つ既知のマルウェアは、中央値で55種類が確認されています。

一方、AIを活用したマルウェアの検知事例のうち、既知のマルウェアが1種類以下しか確認されていない、あまり一般的ではない攻撃手法は2.5%未満でした。

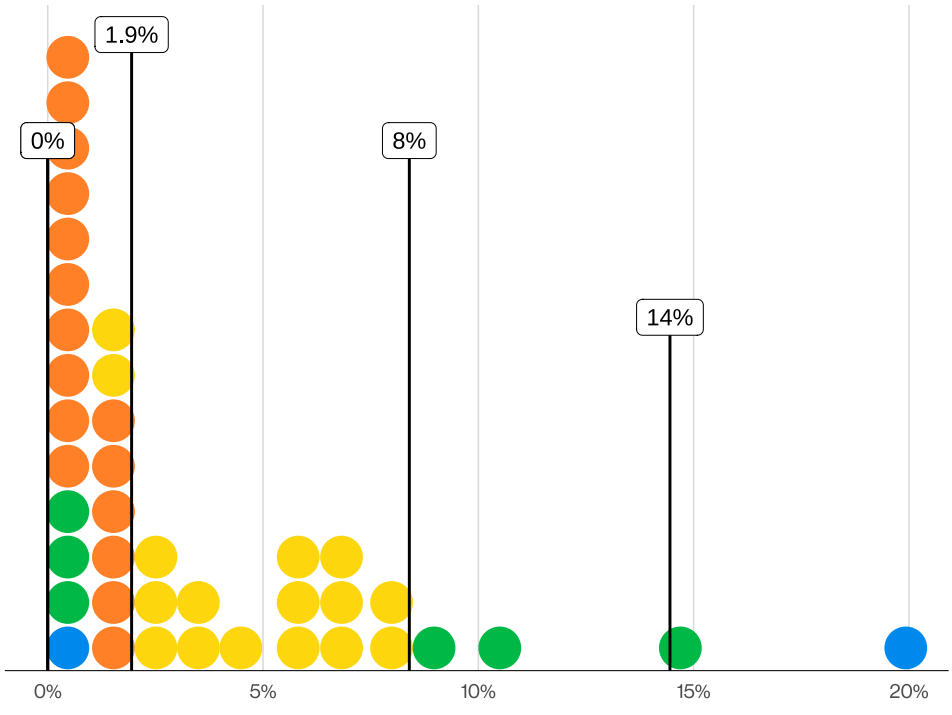


図7.「メール」以外の手段を用いた模擬ソーシャル攻撃の成功率分布
（n=35、1ドットは0.88件の攻撃を表す）

モバイル中心のソーシャルエンジニアリング

データ漏洩/侵害の62%に人的要素が関与しており、前年の60%からわずかに増加しています。また、「ソーシャルエンジニアリング」は、DBIRで分析したデータ漏洩/侵害パターンの中で3番目に多く、全件数の16%を占めています。

フィッシング攻撃のシミュレーションでは、モバイル中心の手法（音声やテキストメッセージなど）における“クリック”率の中央値は、電子メール経由の場合よりも40%高くなっています。

さらに、「なりすまし」は、ランサムウェアや恐喝を目的とした攻撃への初期アクセス経路として、より一般的になっており、全データ漏洩/侵害のうち、6%に達した一方、「フィッシング」は前年と同じ16%にとどまっています。「なりすまし」とは、攻撃者が架空のシナリオを通して信頼関係を築き、ユーザを騙して意図せず組織に損害をもたらすような行動を取らせる戦術です。音声通話を利用することが多く見られますが、他に電子メールやSMSを利用したケースも確認されています。

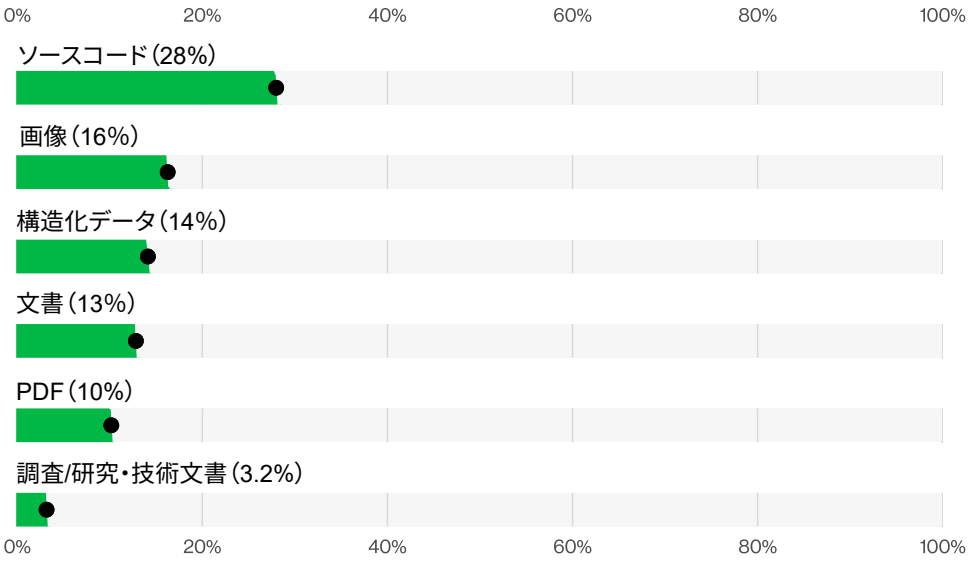


図8. 生成AIツールへの未承認送信が検知されたデータタイプ（n=858,440）

シャドーAIのポリシー違反と悪意ある内部関係者

許可されていない生成AIサービス（「シャドーAI」）の利用状況に関して、ユーザの67%が会社の端末から個人のアカウントを使用してAIサービスにアクセスしており、これは前年よりわずかに減少しています。しかし、従業員の45%が会社の端末からAIを日常的に利用している（承認済みか否かを問わず）とみなされており、これは前年の15%から大幅に増加しています。

シャドーAIは、2025年にベライゾンのデータ損失防止（DLP）データセットで検出された悪意のない内部関係者による行動の中で3番目に多く、その割合は前年の4倍に増加しています。

外部の生成AIモデルに送られたデータタイプで最も多かったのはソースコードで、次いで画像やその他の構造化データでした。さらに、DLPポリシー違反の3.2%では、調査/研究データや技術文書が未承認のAIシステムにアップロードされていることが確認されています。こうした行為は知的財産の漏洩リスクにつながる可能性があります。

業種別のハイライト

“はじめに”でも触れたように、今年は22,000件を超えるデータ漏洩/侵害を分析しました。これは、私たちが単年の報告書で分析した件数としては過去最多となります。このセクションでは、これらのデータ漏洩/侵害を業種別に考察します。業種ごとに直面する脅威は異なります。その主な理由は、業種によって攻撃対象領域（アタックサーフェス）が異なるためです。

このセクションを読む際には、いくつかの留意すべき点があります。業種による違いは、規制や報告要件の違い、それに伴う外部からの監視レベルの違い、そして特定の業種におけるサンプル数など、さまざまな要因の影響を受ける可能性があります。こうしたさまざまな要因によって、報告書内での業種ごとの見え方が変わる場合があります。そのため、業種間の比較を行う際には、その点を念頭に置くことが大切です。

多くの読者が、自社の業界に関する特定の結果を確認するためにこのセクションを参照しています。その際には、自社の業種で主に見られる侵害の傾向に注目してください。また、特定の業種や侵害の動向についてさらに詳しい見解を知りたい場合は、報告書全文の該当セクションをご参照ください。そうすることで、防御する必要のある攻撃について、より深い理解が得られるはずです。

教育サービス業

（NAICS 61）

「教育サービス業」における脅威の中心は、金銭目的の外部攻撃者です。これらの攻撃者は「ランサムウェア」や「脆弱性の悪用」に加え、「盗まれた認証情報の悪用」を多用しています。

発生件数	インシデント1,302件、確認されたデータ漏洩1,252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」がデータ漏洩/侵害の83%を占めている
攻撃者	外部（78%）、内部（22%）（漏洩/侵害）
攻撃者の動機	金銭目的（78%）、スパイ活動（21%)、イデオロギー（2%）（漏洩/侵害）
漏洩したデータ	内部情報（64%）、個人情報（41%）、その他（26%）、機密情報（19%）（漏洩/侵害）
初期のアクセス経路	脆弱性の悪用（34%）、フィッシング（22%）、認証情報の悪用（8%）（漏洩/侵害）
その他の要因	人的要素（68%）、サードパーティ（40%）
昨年との比較	「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」は、昨年、一昨年と同様に、依然として上位3つの侵害パターンとなっています。

金融および保険業
（NAICS 52）

この業界は引き続き、金銭目的の外部攻撃者から集中的に狙われています。「ランサムウェア」による「システム侵入」、「フィッシング」、「脆弱性の悪用」、「盗まれた認証情報の悪用」が主な脅威となっています。また、人的ミスやサードパーティとの関係に起因するリスクも、依然として重大な要因となっています。

発生件数	インシデント3,809件、確認されたデータ漏洩1,300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」、「その他全て」がデータ漏洩/侵害の81%を占めている
攻撃者	外部（88%）、内部（12%）（漏洩/侵害）
攻撃者の動機	金銭目的（98%）、スパイ活動（3%）（漏洩/侵害）
漏洩したデータ	内部情報（53%）、個人情報（43%）、その他（28%）、認証情報（26%）（漏洩/侵害）
初期のアクセス経路	脆弱性の悪用（22%）、フィッシング（20%）、認証情報の悪用（15%）（漏洩/侵害）
その他の要因	人的要素（65%）、サードパーティ（34%）
昨年との比較	「システム侵入」は2022年以降、最も多い侵害パターンで、攻撃者の動機は主に金銭目的です。

医療および社会福祉業
（NAICS 62）

医療および社会福祉業界の組織では、「ランサムウェア」による「システム侵入」と後を絶たない人的ミスが主な脅威となっています。金銭目的の外部攻撃者が、「脆弱性の悪用」、「フィッシング」、「盗まれた認証情報の悪用」を通じて侵害を試みています。従業員によるミスや「設定ミス」は、依然としてデータ漏洩/侵害の慢性的な要因となっています。

発生件数	インシデント1,492件、確認されたデータ漏洩1,438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」がデータ漏洩/侵害の81%を占めている
攻撃者	外部（81%）、内部（19%）（漏洩/侵害）
攻撃者の動機	金銭目的（99%）、スパイ活動（2%）（漏洩/侵害）
漏洩したデータ	内部情報（65%）、個人情報（37%）、認証情報（25%）、その他（19%）（漏洩/侵害）
初期のアクセス経路	脆弱性の悪用（20%）、フィッシング（14%）、認証情報の悪用（11%）（漏洩/侵害）
その他の要因	人的要素（54%）、サードパーティ（32%）（漏洩/侵害）
昨年との比較	ベライゾンがデータの分析を開始して以来、「多種多様なエラー」はこの業種における上位のパターンであり続けています。また、「システム侵入」は、2年連続で1位でした。

製造業
（NAICS 31–33）

この業種におけるデータ漏洩/侵害の件数は引き続き増加しており、その主な要因は「ランサムウェア」攻撃の増加です。

発生件数	インシデント3,627件、確認されたデータ漏洩2,713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91%を占めている
攻撃者	外部（95%）、内部（5%）（漏洩/侵害）
攻撃者の動機	金銭目的（87%）、スパイ活動（15%）（漏洩/侵害）
漏洩したデータ	内部情報（81%）、認証情報（26%）、その他（22%）、個人情報（17%）（漏洩/侵害）
初期のアクセス経路	脆弱性の悪用（38%）、フィッシング（13%）、認証情報の悪用（11%）（漏洩/侵害）
その他の要因	サードパーティ（61%）、人的要素（56%）（漏洩/侵害）
昨年との比較	「製造業」における主な侵害パターンは昨年と変らず、その攻撃者の大半は金銭的な利益を目的にしています。

公務
（NAICS 92）

「公務」は、金銭目的の犯罪者と国家支援型の攻撃者の双方から主な標的にされており、「脆弱性の悪用」や「ランサムウェア」による「システム侵入」が頻繁に発生しています。さらに、この業界では、特に膨大な事務連絡や文書のやり取りに伴う誤送信などの「多種多様なエラー」や意図的なデータの不適切処理による、内部インシデントの発生率が非常に高いという問題に直面しています。

発生件数	インシデント3,634件、確認されたデータ漏洩2,410件
上位3つのパターン	「システム侵入」、「多種多様なエラー」「特権の悪用」がデータ漏洩/侵害の80%を占めている
攻撃者	外部（56%）、内部（44%）（漏洩/侵害）
攻撃者の動機	金銭目的（69%）、スパイ活動（33%）、イデオロギー（2%）（漏洩/侵害）
漏洩したデータ	個人情報（50%）、内部（39%）、その他（37%）、機密情報（30%）（漏洩/侵害）
初期のアクセス経路	脆弱性の悪用（40%）、フィッシング（20%）、認証情報の悪用（8%）（漏洩/侵害）
その他の要因	人的要素（69%）、サードパーティ（36%）
昨年との比較	この業種における上位2つの攻撃パターンは昨年と変わりません。一方で、今年は「基本Webアプリケーション攻撃」に代わって「特権の悪用」が上位パターンの1つになりました。また、この業種を標的とする「外部」の攻撃者の割合は、前年とほぼ同水準を維持しています。

小売業

（NAICS 44 – 45）

「小売業」は、脆弱性の悪用、認証情報の窃取、フィッシングなどの外部の攻撃者からの絶え間ない脅威に直面しています。こうした攻撃は、ランサムウェア攻撃やデータの窃取につながることが多く、サードパーティのシステムや企業の内部データが、ますます価値の高い標的となっています。

発生件数	インシデント997件、確認されたデータ漏洩806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」がデータ漏洩/侵害の95%を占めている
攻撃者	外部（99%）、内部（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（85%）、スパイ活動（19%）（漏洩/侵害）
漏洩したデータ	内部情報（84%）、認証情報（26%）、機密情報（20%）、その他（14%）（漏洩/侵害）
初期のアクセス経路	脆弱性の悪用（42%）、認証情報の悪用（14%）、フィッシング（9%）（漏洩/侵害）
その他の要因	サードパーティ（68%）、人的要素（58%）（漏洩/侵害）
昨年との比較	上位3つの侵害パターンは変わらないものの、その順位に変動がありました。これらのパターンはここ数年一貫して上位を占めていますが、どのパターンが最も多く確認されるかは年によって異なります。

中小企業

小規模な組織は、「ランサムウェア」による影響を特に大きく受けており、他の業種や組織と同様の脅威に多く直面していますが、そうした脅威に対応できるリソースが限られていることが少なくありません。

発生件数	インシデント7,256件、確認されたデータ漏洩7,152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」がデータ漏洩/侵害の100%を占めている
攻撃者	外部（100%）（漏洩/侵害）
攻撃者の動機	金銭目的（100%）（漏洩/侵害）
漏洩したデータ	内部情報（97%）、認証情報（31%）、システム（1%）、その他（1%）（漏洩/侵害）
初期のアクセス経路	脆弱性の悪用（26%）、認証情報の悪用（13%）、フィッシング（9%）（漏洩/侵害）
その他の要因	サードパーティ（55%）、人的要素（45%）（漏洩/侵害）
昨年との比較	「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」は、引き続き中小企業におけるデータ漏洩/侵害の主な要因となっています。

その他の業種別主要データ

すべての業種を詳細に検証するための十分なスペースや時間、場合によってはデータもないため、以下の表にその他の業種の概要を掲載します。

業種（NAICS）	発生件数	上位3つのパターン	攻撃者	攻撃者の動機	漏洩したデータ
農業（11）	インシデント223件、確認されたデータ漏洩219件	「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」がデータ漏洩/侵害の91%を占めている	外部（100%）（漏洩/侵害）	金銭目的（71%）、スパイ活動（29%）、イデオロギー（1%）（漏洩/侵害）	内部情報（70%）、その他（43%）、機密情報（36%）（漏洩/侵害）
管理・支援及び廃棄物処理並びに除去サービス業（56）	インシデント422件、確認されたデータ漏洩419件	「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98%を占めている	外部（99%）、内部（1%）（漏洩/侵害）	金銭目的（100%）（漏洩/侵害）	内部情報（96%）、認証情報（28%）、その他（2%）、システム（2%）（漏洩/侵害）
建設業（23）	インシデント843件、確認されたデータ漏洩828件	「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95%を占めている	外部（99%）、内部（1%）（漏洩/侵害）	金銭目的（97%）、スパイ活動（5%）（漏洩/侵害）	内部情報（86%）、認証情報（34%）、その他（13%）、機密情報（6%）（漏洩/侵害）
芸術、娯楽、およびレクリエーション業（71）	インシデント587件、確認されたデータ漏洩483件	「システム侵入」、「ソーシャルエンジニアリング」、「その他全て」がデータ漏洩/侵害の82%を占めている	外部（86%）、内部（14%）（漏洩/侵害）	金銭目的（89%）、スパイ活動（20%）、イデオロギー（1%）（漏洩/侵害）	内部情報（54%）、個人情報（45%）、その他（31%）、機密情報（20%）（漏洩/侵害）
情報産業（51）	インシデント1,703件、確認されたデータ漏洩1,099件	「システム侵入」、「基本Webアプリケーション攻撃」、「その他全て」がデータ漏洩/侵害の79%を占めている	外部（89%）、内部（11%）、複数（1%）（漏洩/侵害）	金銭目的（84%）、スパイ活動（16%）、イデオロギー（2%）（漏洩/侵害）	内部情報（52%）、個人情報（39%）、その他（31%）、認証情報（24%）（漏洩/侵害）

表1. その他の業種一覧

業種（NAICS）	発生件数	上位3つのパターン	攻撃者	攻撃者の動機	漏洩したデータ
事業経営業（55）	インシデント103件、確認されたデータ漏洩101件	「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98%を占めている	外部（100%）（漏洩/侵害）	金銭目的（100%）（漏洩/侵害）	内部情報（96%）、認証情報（35%）、多要素認証情報（3%）、その他（2%）（漏洩/侵害）
鉱業、採石業、石油・ガス採掘業（21）	インシデント72件、確認されたデータ漏洩70件	「システム侵入」、「その他全て」、「基本Webアプリケーション攻撃」がデータ漏洩/侵害の96%を占めている	外部（100%）（漏洩/侵害）	金銭目的（97%）、スパイ活動（1%）、イデオロギー（1%）（漏洩/侵害）	内部情報（74%）、認証情報（31%）、個人情報（17%）、その他（9%）（漏洩/侵害）
その他のサービス（81）	インシデント900件、確認されたデータ漏洩885件	「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」がデータ漏洩/侵害の85%を占めている	外部（81%）、内部（19%）（漏洩/侵害）	金銭目的（78%）、スパイ活動（23%）（漏洩/侵害）	内部情報（66%）、個人情報（38%）、その他（28%）、機密情報（20%）（漏洩/侵害）
専門的・科学的・技術的サービス業（54）	インシデント3,578件、確認されたデータ漏洩2,558件	「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91%を占めている	外部（97%）、内部（3%）（漏洩/侵害）	金銭目的（96%）、スパイ活動（5%）（漏洩/侵害）	内部情報（80%）、認証情報（31%）、個人情報（14%）、その他（11%）（漏洩/侵害）
不動産業、レンタル及びリース業（53）	インシデント505件、確認されたデータ漏洩499件	「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」がデータ漏洩/侵害の85%を占めている	外部（79%）、内部（22%）（漏洩/侵害）	金銭目的（100%）（漏洩/侵害）	内部情報（63%）、個人情報（43%）、認証情報（24%）、その他（16%）（漏洩/侵害）
運輸および倉庫業（48–49）	インシデント689件、確認されたデータ漏洩652件	「システム侵入」、「基本Webアプリケーション攻撃」、「その他全て」がデータ漏洩/侵害の89%を占めている	外部（99%）、内部（1%）（漏洩/侵害）	金銭目的（89%）、スパイ活動（15%）、イデオロギー（1%）（漏洩/侵害）	内部情報（84%）、認証情報（27%）、機密情報（16%）、その他（14%）（漏洩/侵害）
公益事業（22）	インシデント638件、確認されたデータ漏洩597件	「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」がデータ漏洩/侵害の94%を占めている	外部（97%）、内部（3%）（漏洩/侵害）	スパイ活動（71%）、金銭目的（36%）（漏洩/侵害）	内部情報（85%）、機密情報（68%）、その他（21%）（漏洩/侵害）
卸売業（42）	インシデント1,057件、確認されたデータ漏洩1,048件	「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」がデータ漏洩/侵害の99%を占めている	外部（100%）（漏洩/侵害）	金銭目的（100%）（漏洩/侵害）	内部情報（98%）、認証情報（29%）（漏洩/侵害）

表1. その他の業種一覧（続き）

地域別の分析

このセクションでは、マクロ的な地域の視点からデータ漏洩/侵害を分析し、地域によって異なる傾向や共通して見られる傾向を明らかにします。

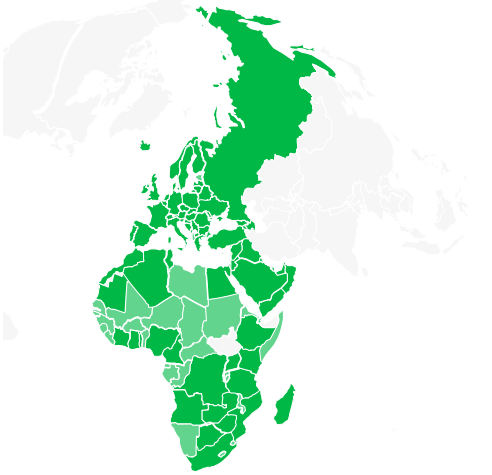
なお、各地域における分析の深さは、地域の情報開示規制、ベライゾンのデータセット、データ提供組織の事業展開地域など、さまざまな要素の影響を受けています。ご自身がお住まいの地域がこれらのページに十分に反映されていないと感じられる場合は、ぜひデータ提供組織としてのご参加をご検討ください。また、同じ地域の他の組織の方々にも、ぜひご協力を呼びかけていただければ幸いです。

データのある地域　　データのない地域

アジア太平洋地域（APAC）

発生件数	インシデント5,229件、確認されたデータ漏洩2,855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」がデータ漏洩/侵害の97%を占めている
攻撃者	外部（99%）、内部（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（70%）、スパイ活動（36%）（漏洩/侵害）
漏洩したデータ	内部情報（70%）、認証情報（36%）、その他（35%）、機密情報（30%）（漏洩/侵害）
初期のアクセス経路	脆弱性の悪用（42%）、認証情報の悪用（25%）、フィッシング（15%）（漏洩/侵害）
その他の要因	サードパーティ（69%）、人的要素（71%）（漏洩/侵害）

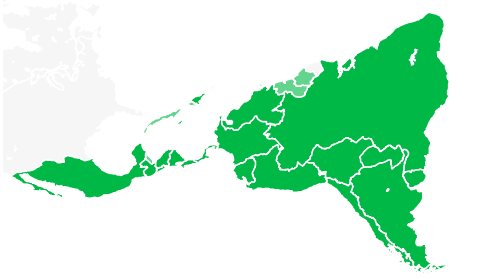
欧州、中東、アフリカ（EMEA）



発生件数	インシデント8,245件、確認されたデータ漏洩6,060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」がデータ漏洩/侵害の92%を占めている
攻撃者	外部（80%）、内部（20%）（漏洩/侵害）
攻撃者の動機	金銭目的（76%）、スパイ活動（27%）（漏洩/侵害）
漏洩したデータ	内部情報（73%）、その他（49%）、個人情報（34%）、機密情報（24%）（漏洩/侵害）
初期のアクセス経路	脆弱性の悪用（47%）、フィッシング（28%）、認証情報の悪用（6%）（漏洩/侵害）
その他の要因	サードパーティ（54%）、人的要素（70%）（漏洩/侵害）

データあり　　データのない地域

中南米、カリブ海地域（LAC）



発生件数	インシデント813件、確認されたデータ漏洩718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98%を占めている
攻撃者	外部（99%）、内部（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（90%）、スパイ活動（11%）（漏洩/侵害）
漏洩したデータ	内部情報（93%）、認証情報（23%）、機密情報（24%）、その他（3%）（漏洩/侵害）
初期のアクセス経路	脆弱性の悪用44%）、フィッシング（20%）、認証情報の悪用（5%）（漏洩/侵害）
その他の要因	サードパーティ（74%）、人的要素（57%）（漏洩/侵害）

北アメリカ（NA）

発生件数	インシデント12,371件、確認されたデータ漏洩8,426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87%を占めている
攻撃者	外部（88%）、内部（12%）（漏洩/侵害）
攻撃者の動機	金銭目的（98%）、スパイ活動（3%）（漏洩/侵害）
漏洩したデータ	内部情報（77%）、認証情報（36%）、個人情報（9%）、その他（8%）（漏洩/侵害）
初期のアクセス経路	脆弱性の悪用（30%）、認証情報の悪用（20%）、フィッシング（12%）（漏洩/侵害）
その他の要因	サードパーティ（43%）、人的要素（59%）（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セキュリティに関する知見が必要です。

DBIR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、侵害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セキュリティの知見をぜひご確認ください。

2026年度DBIR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考えなら・・・。

もしお客様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へのデータ提供や調査協力にご興味を持たれた方は（そうであってほしいです）、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、ご感想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、LinkedInで Verizon Business（または執筆者の1人）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。