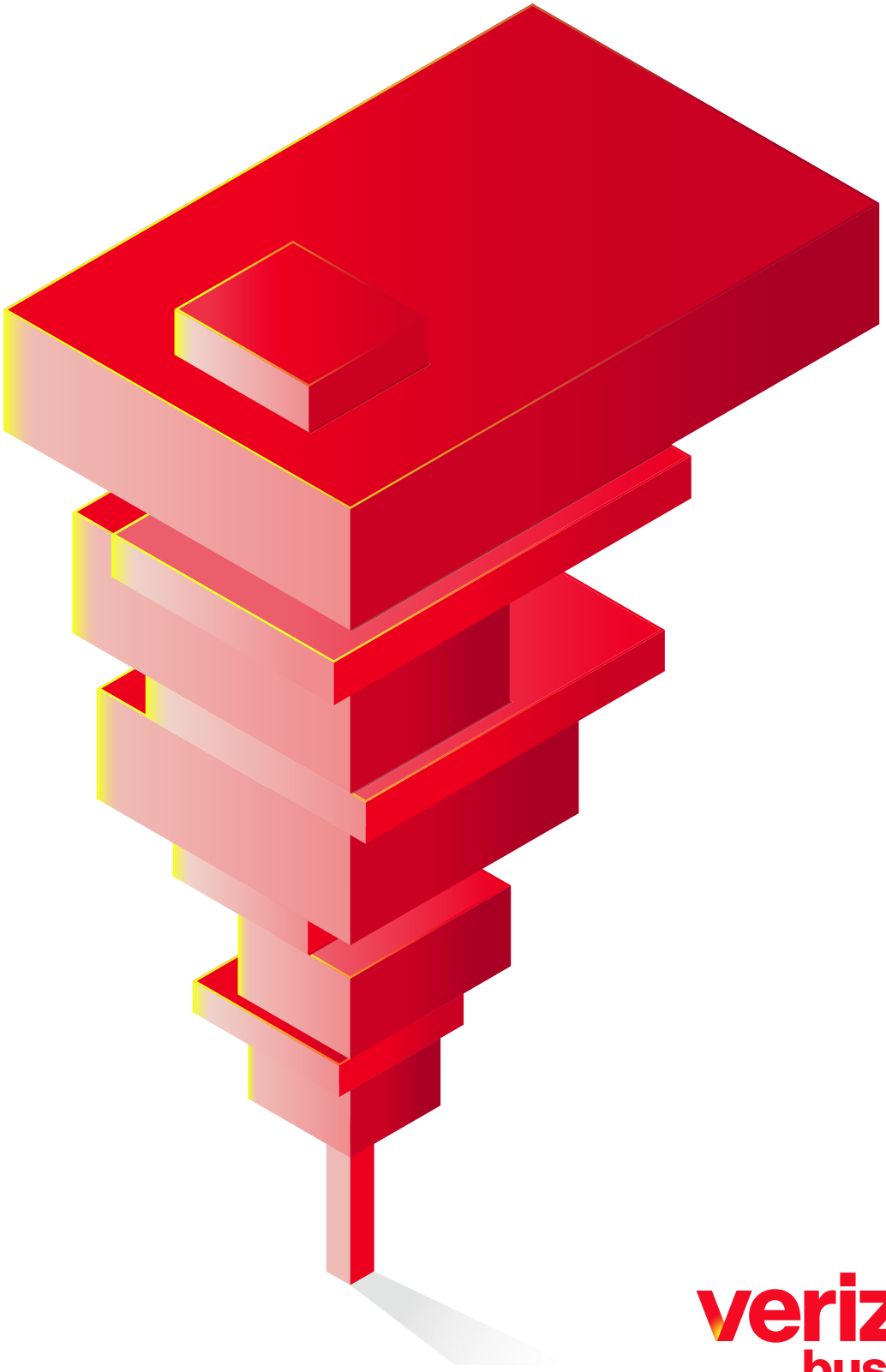
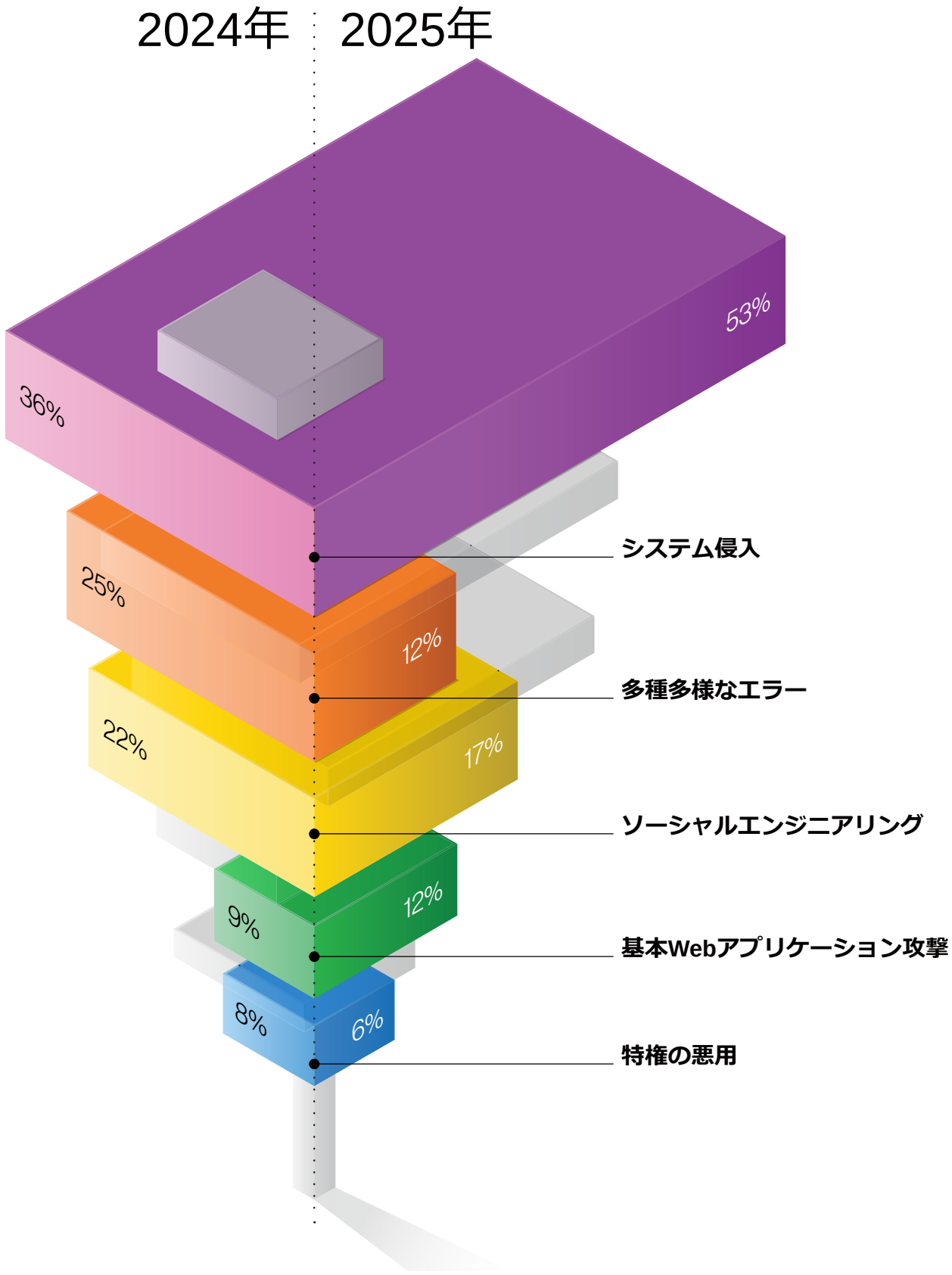
2025年度 データ漏洩/侵害調査報告書（DBIR）

エグゼクティブサマリー



verizon business


2024年
2025年
53%
36%
システム侵入
25%
12%
多種多様なエラー
22%
17%
ソーシャルエンジニアリング
9%
12%
基本Webアプリケーション攻撃
8%
6%
特権の悪用

表紙について

サードパーティのデータ漏洩/侵害への関与は、この1年を通じて、常に大きなテーマになっていました。サードパーティは顧客データを管理するだけではなく、組織の重要な部分を担っている可能性があります。

私たちの優秀なデザインチームは、組織のセキュリティプログラムにおいてサードパーティへの依存度が高まる中で、いかにバランスを取らなければならないかを表現するデザインに挑戦しました。この表紙の、あり得ないようなバランスの形状に違和感を覚えたなら、あなたは今日の最高情報セキュリティ責任者（CISO）が現在の環境において直面している課題を理解し始めている証拠です。

中心を通る「芯」に対して、インシデントデータセットにおいて最も多く見られたデータ漏洩/侵害を分類したインシデント分類パターンを表現しています（昨年度のデータは中央より左側、今年度のデータは右側）。中表紙にはそれらの数値をより具体的に描写しました。

形としては歪すぎて、立ち続けるにはあまりにも脆すぎるように見えるかもしれませんが、それがしっかりと立ち続けているという事実は、セキュリティ業界がこれまで積み重ねてきた努力と協力の証です。今後も適切な協力体制、組織運営、情報共有を続けることで、サイバーセキュリティを着実に強化し、安心して眠れる夜を何日か過ごすことができるでしょう。

目次

はじめに

ベライゾンの2025年度データ漏洩/侵害調査報告書（DBIR）へようこそ。

今年で18年目を迎える報告書（DBIR）を皆様にお届けできることを、大変嬉しく思います。長年の読者の方も、初めてご覧になる方も、この報告書ではサイバー犯罪の最新状況を綿密に分析した内容に加え、組織が直面する可能性のある脅威、その背後にあるもの、そして自らを守るために何ができるのかといったさまざまなインサイトをご確認いただけます。

今年、ベライゾンのDBIRチームは22,052件の実際のセキュリティインシデントを分析しました。そのうち12,195件は、あらゆる規模と種類の組織内で発生したデータ漏洩/侵害であることが確認されました。これは、単一のレポートで分析された侵害件数としては過去最多となります。これらのインシデントや侵害のケースは、Verizon Threat Research Advisory Center（VTRAC）チームのケースファイル、世界中の協力組織からの多大な支援、そして公開されたセキュリティインシデントから提供されたものです。そして、これらの攻撃は世界139カ国に及んでいます。

脅威の状況は組織の規模、業務内容、所在地によって多少異なりますが、これらの要素に関わらず、私たちのデータセット全体を貫く共通テーマが常に存在しており、今年も例外ではありません。その中で特に顕著で注目すべきことは、データ漏洩/侵害の発生と原因において、サードパーティが関連していることです。

ソフトウェアベンダーは長年、自社製品やサービスを利用するユーザに対し、結果的に攻撃対象領域を拡大してしまう側面を持っていましたが、ここ2～3年で時折発生していた（通常は軽微から中程度）インシデントから、企業に壊滅的な被害を与える可能性のある（そして実際に被害を与えている）はるかに広範囲かつ深刻な問題へと変化しつつあります。実際、この傾向は今年の報告書の表紙を飾るほどで、このテーマは本報告書全体に織り込まれています。

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お読みいただき、ぜひ内容を同僚の皆様と共有してください。また、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、報告書の全文をダウンロードしてご確認ください。

主な調査結果

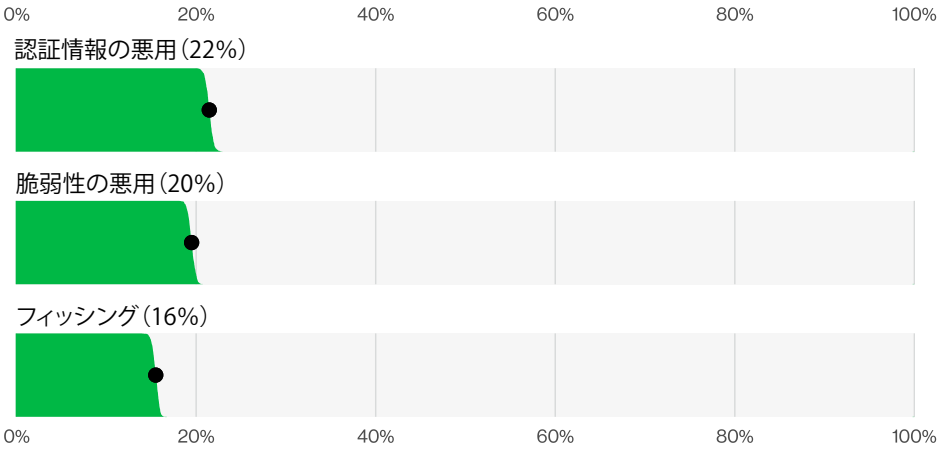


図1. 「エラー」/「（内部）悪用」を除いたデータ漏洩/侵害における上位の主な初期アクセス経路（n=9,891）

「脆弱性の悪用」は、データ漏洩/侵害の初期のアクセス経路として、昨年も増加しており20%に達しました。この値は、依然として最も一般的な経路である「認証情報の悪用」に迫っています。これは昨年と比較して34%の増加であり、エッジデバイスと仮想プライベートネットワーク（VPN）を標的としたゼロデイエクスプロイトが一部影響しています。私たちが定義する「脆弱性の悪用」の標的として、エッジデバイスとVPNの割合は22%で、昨年の3%からほぼ8倍に増加しました。組織はこれらのエッジデバイスの脆弱性へのパッチ適用に多大な努力を払いましたが、ベライゾンの分析によると、年間を通じて完全に修正されたのは約54%に過ぎず、修正完了までの日数の中央値は32日でした。

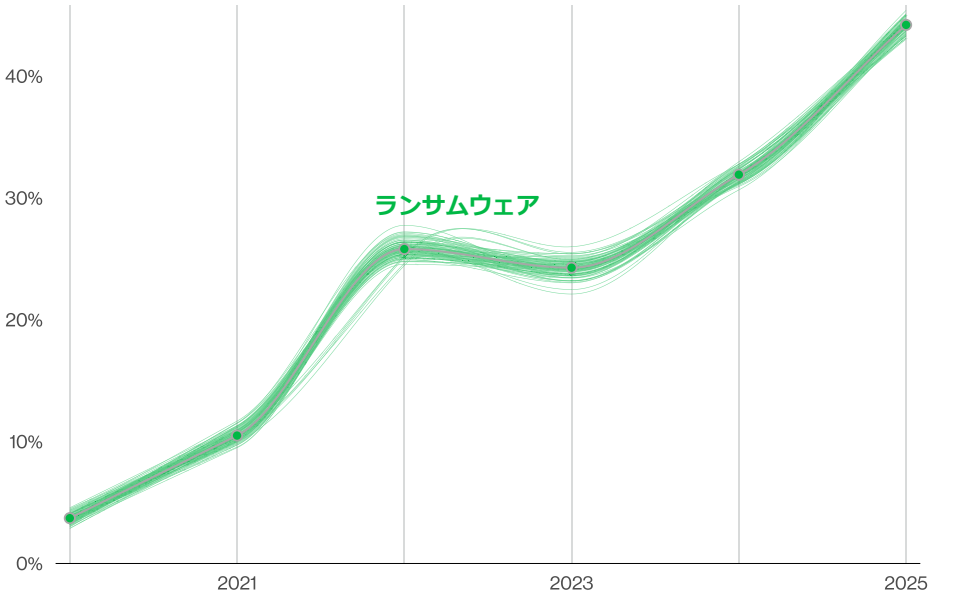


図2. 「ランサムウェア」によるデータ漏洩/侵害の経時的変化（2025年のデータセット：n=10,747）

「ランサムウェア」は、暗号化の有無にかかわらず大幅に拡大し、昨年から37%増加しました。調査したデータ漏洩/侵害全体の44%でランサムウェアが見られ、昨年の32%から増加しています。一方朗報として、ランサムウェアグループに支払われた身代金の中央値は昨年の15万ドルから11万5000ドルに減少しました。支払いを拒否した被害組織は2年前の50%から64%になり、これが身代金の減少の一因となっている可能性があります。

「ランサムウェア」は小規模組織にも大きな影響を与えています。大規模組織では、ランサムウェアはデータ漏洩/侵害の39%を占めていますが、中小企業においてはランサムウェア関連のデータ漏洩/侵害が全体の88%に達しています。

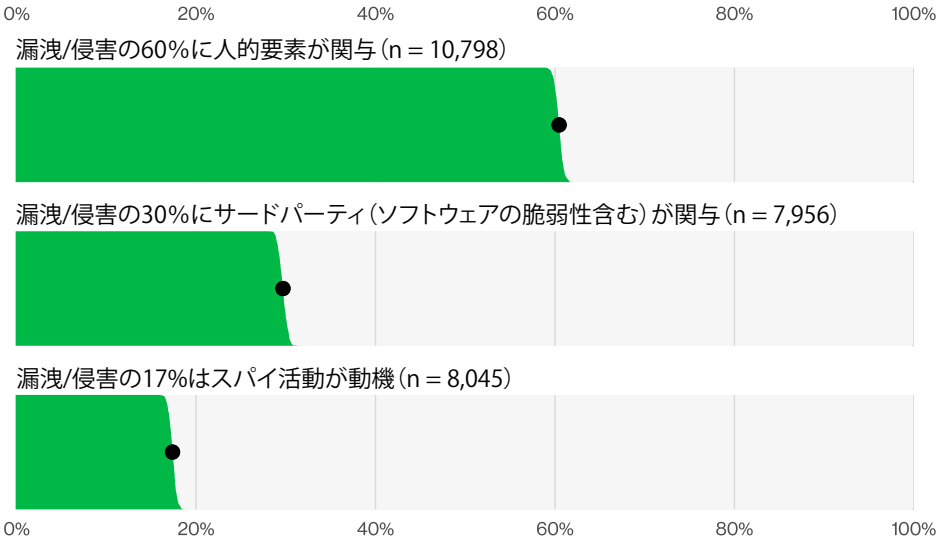


図3. データ漏洩/侵害における上位の主な要因

データ漏洩/侵害における人的要素の関与は昨年とほぼ同じで60%前後で推移していますが、サードパーティが関与した割合は15%から倍増の30%に達しました。

今年は、サードパーティ環境での「認証情報の悪用」に関する注目すべきインシデントが発生しました。ベライゾンの調査によると、GitHubリポジトリで発見された漏洩機密情報の修復にかかった時間の中央値は94日でした。

また、今回の分析では、スパイ活動が動機となったデータ漏洩/侵害が大幅に増加し、17%に達しています。この増加は、協力組織の構成の変化が一因となっています。これらのデータ漏洩/侵害では、70%のケースで「脆弱性の悪用」が初期アクセス経路として利用されており、パッチ未適用のリスクが浮き彫りになっています。しかし、国家支援を受けた攻撃者の関心はスパイ活動だけではないことも判明しました。これらの攻撃者が関与するインシデントの約28%には金銭的な動機がありました。一部報道では、攻撃者が報酬を水増しするために二重取りをしている可能性があるという憶測が出ています。

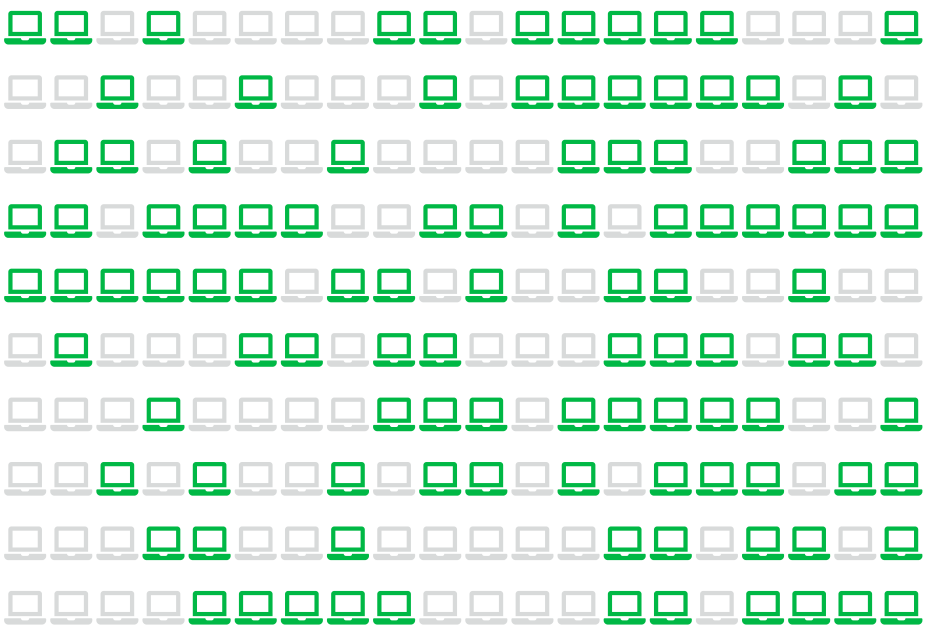


図4. 「インフォスティーラー」のログに記録された企業ログインを持つ管理対象外のデバイスの割合（各アイコンは0.5%）

窃取された認証情報に関して、情報窃取型マルウェア（インフォスティーラー）の認証情報ログを分析した結果、データ漏洩/侵害に遭ったシステムの30%が企業支給のデバイスであることが明らかになりました。しかし、漏洩/侵害したデータに企業のログイン情報が含まれていたシステムのうち46%は管理対象外であり、個人認証情報とビジネス認証情報の両方がホストされていました。これらの問題は、BYOD（個人所有デバイスの業務利用）プログラム、または企業所有デバイスが許可されたポリシーの範囲外で使用されていることに起因している可能性が高いと考えられます。

2024年にランサムウェア攻撃者によって公開された被害組織のインターネットドメインと、インフォスティーラーのログとマーケットプレイスの投稿を照合したところ、被害者の54%のドメインが認証情報流出データ（例えば、認証情報でアクセスできたとされるURL）に含まれており、被害組織の40%はデータ漏洩/侵害された認証情報に企業のメールアドレスが含まれていたことがわかりました。これは、これらの認証情報がランサムウェアによるデータ漏洩/侵害に利用された可能性があることを示唆しており、初期アクセス経路としてアクセスブローカーが関与していた可能性を示しています。

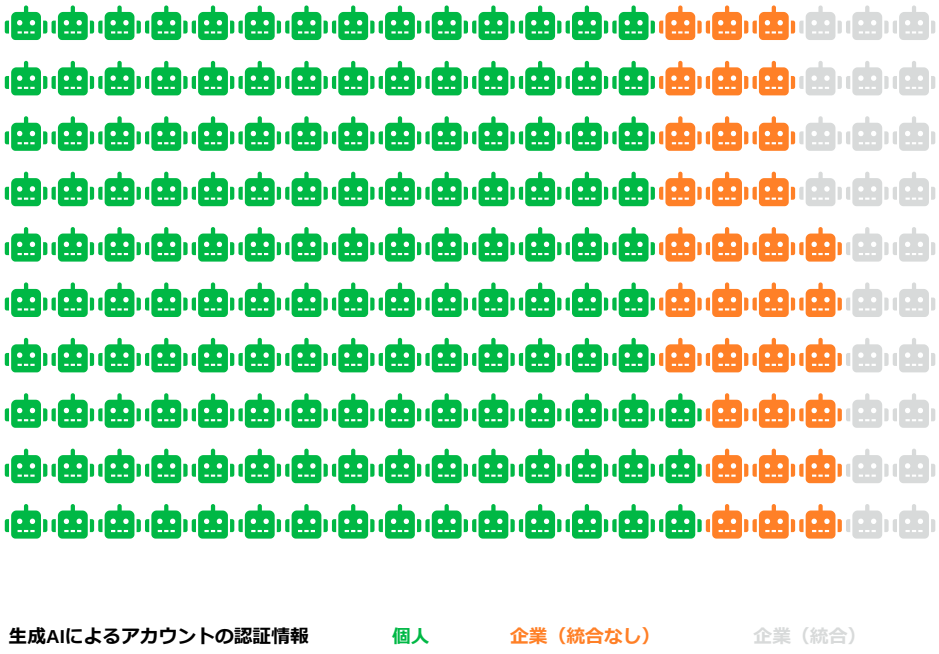


図5. 生成AIサービスへのアクセスアカウントタイプの割合 （各アイコンは0.5%）

2025年初頭時点で、生成型人工知能（生成AI）は、AIプラットフォーム自体が報告しているように、攻撃者による利用の証拠があるにもかかわらず、まだ世界を席巻していません。一方、ベライゾンのパートナー企業から提供されたデータによると、悪意あるメールに含まれる合成テキストは、過去2年間で倍増しています。

AIに起因するより身近で新たな脅威は、企業の機密データが生成AIプラットフォーム自体に流出する可能性です。従業員の15%が会社のデバイスから生成AIシステムに定期的にアクセスしていたという報告もあります（少なくとも15日に1回）。さらに懸念されることは、これらの従業員の多くが、アカウントのIDとして会社以外のメールアドレスを使用していたり（72%）、または統合認証システムを導入せずに会社のメールアドレスを使用していた（17%）ことです。これは、企業ポリシーに違反している可能性が高いことを示しています。

業種別のハイライト

冒頭で述べたように、今年は22,052件のセキュリティインシデントを調査し、そのうち12,195件はデータ漏洩/侵害であることが確認されました。このセクションからは、これらのインシデントとデータ漏洩/侵害を分類し、業種固有の観点から考察します。ご想像のとおり、ある業種では頻繁に発生する問題が、別の業種ではほとんど発生しない場合があります。各業種が直面する脅威の違いは、多くの場合、各組織に対する固有の攻撃対象領域に起因します。

例えば、グローバル展開している金融機関は、地域密着型の物流会社とは異なる脅威に直面する可能性があります。しかし、多くの場合、両者の間には驚くほど多くの共通点があるかもしれません。結局のところ、報告書の他の箇所でも指摘しているように、攻撃者は私たちが想像するほど組織の規模、業種、地理的な場所を気にしていないようです。今日のサイバー犯罪者はやや実利主義者で、「手元にあるものは何でも喜んで盗む」という考え方に傾倒しています。このセクションを深く理解するには、業種によって異なる報告要件やそれに応じた精査のレベル、特定の業種におけるサンプル数など、他の要素も考慮する必要があります。したがって、特定の業種のセキュリティ体制を判断する際には、これらの要因やその他の要因を念頭に置くことをお勧めします。最後に、業種は北米産業分類システム（North American Industry Classification System：NAICS）の基準に沿って分類されていることにご留意ください。

教育サービス業
（NAICS 61）

頻度	インシデント1,075件、確認されたデータ漏洩851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80%を占めている
攻撃者	外部（62%）、内部（38%）（漏洩/侵害）
攻撃者の動機	金銭目的（88%）、スパイ活動（18%）（漏洩/侵害）
侵害されたデータ	個人情報（58%）、内部情報（49%）、その他（35%）、認証情報（12%）（漏洩/侵害）
昨年との比較	「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」は、過去2年間と同様に、依然として上位3つのパターンです。
サマリー	「教育サービス業」では、インシデント数とデータ漏洩/侵害件数はともに減少しましたが、確認された攻撃は過去に見られた傾向とほぼ同じでした。「システム侵入」が圧倒的に多く、金銭目的の「外部」攻撃者によって実行されています。

金融および保険業
（NAICS 52）

頻度	インシデント3,336件、確認されたデータ漏洩927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74%を占めている
攻撃者	外部（78%）、内部（22%）、パートナー（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（90%）、スパイ活動（12%）（漏洩/侵害）
侵害されたデータ	個人情報（54%）、その他（44%）、内部情報（35%）、認証情報（22%）（漏洩/侵害）
昨年との比較	「システム侵入」は、より複雑な攻撃が主流となったため、再び上位のパターンとなっています。これは、攻撃者がより多くの労力を費やさなければならなくなっているということであれば、少しは希望が持てるかもしれません。
サマリー	「金融および保険業」は依然として、「金銭目的」の攻撃者が支配的であり、攻撃者は入手可能なあらゆるデータタイプを狙うのが通例です。ただし、今年は「スパイ活動」を目的とした攻撃が増加しています。

医療および社会福祉業
（NAICS 62）

頻度	インシデント1,710件、確認されたデータ漏洩1,542件
上位3つのパターン	「システム侵入」、「その他全て」、「多種多様なエラー」がデータ漏洩/侵害の74%を占めている
攻撃者	外部（67%）、内部（30%）、パートナー（4%）、複数（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（90%）、スパイ活動（16%）（漏洩/侵害）
侵害されたデータ	医療情報（45%）、個人情報（40%）、内部情報（32%）、その他（24%）（漏洩/侵害）
昨年との比較	昨年から順位は変わったものの、攻撃パターンは同じままです。
サマリー	「医療および社会福祉業」は依然としてサイバー攻撃の主要な標的であり、今年はインシデントと漏洩がわずかに増加しています。「システム侵入」（「ランサムウェア」を含む）が、「多種多様なエラー」を上回り、データ漏洩/侵害の主な原因となっています。この業種への攻撃者の動機としては、「スパイ活動」が増加していることが懸念されます。

製造業
（NAICS 31-33）

頻度	インシデント3,837件、確認されたデータ漏洩1,607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85%を占めている
攻撃者	外部（86%）、内部（14%）（漏洩/侵害）
攻撃者の動機	金銭目的（87%）、スパイ活動（20%）（漏洩/侵害）
侵害されたデータ	内部情報（64%）、その他（37%）、個人情報（33%）、認証情報（22%）（漏洩/侵害）
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」、「基本Webアプリケーション攻撃」は依然として上位3つのパターンであり、攻撃の大部分は引き続き金銭目的の「外部」の攻撃者により行われています。
サマリー	今年のデータ漏洩/侵害の5件に1件は、「スパイ活動」目的の攻撃者によるものでした。これは昨年の3%を大幅に上回っています。「内部情報」（機密性の高い計画書、報告書、メール）は、これまでのところ最も多く盗まれているデータです。また、攻撃を受けた組織の90%以上は、従業員数1,000人未満の中小企業でした。

小売業
（NAICS 44-45）

頻度	インシデント837件、確認されたデータ漏洩419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93%を占めている
攻撃者	外部（96%）、内部（3%）、パートナー（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（100%）、スパイ活動（9%）（漏洩/侵害）
侵害されたデータ	内部情報（65%）、その他（30%）、認証情報（26%）、決済情報（12%）（漏洩/侵害）
昨年との比較	この業種の上位3つのパターンは、昨年から攻撃方法も順位も変わっていません。
サマリー	「小売業」ではサイバーインシデントが増加していますが、その標的は「決済カード」データからアクセスしやすい他の種類のデータへと移行しています。昨年と比較して、「スパイ活動」を目的とした攻撃が顕著に増加しました。企業は、より高度で検知が困難な脅威に注意する必要があります。

公務
（NAICS 92）

頻度	インシデント1,422件、確認されたデータ漏洩946件
上位3つのパターン	「システム侵入」、「多種多様なエラー」、「基本Webアプリケーション攻撃」がデータ漏洩/侵害の78%を占めている
攻撃者	外部（67%）、内部（33%）、パートナー（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（76%）、スパイ活動（29%）、イデオロギー（2%）（漏洩/侵害）
侵害されたデータ	個人情報（47%）、内部情報（44%）、その他（41%）、機密情報（17%）（漏洩/侵害）
昨年との比較	この業種は、政府が国民から収集した膨大なデータへのアクセスを狙う、高度な攻撃者の脅威に悩まされ続けています。攻撃の大部分は「外部」の攻撃者によるものですが、内部関係者による単純な「エラー」によるものも相当数あります。
サマリー	今年のデータ提供組織の構成によりインシデントの報告件数は減少していますが、確認された漏洩/侵害の件数は横ばいです。これは、攻撃者が政府機関への攻撃を緩めていないことを示しています。「ランサムウェア」は依然として大きな脅威であり、あらゆるレベルの政府機関におけるデータ漏洩/侵害の30%に影響を与えています。「エラー」は依然として根深い問題であり、中でも「誤送信」が最も多く発生しています。

その他の業種

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）	頻度	上位3つのパターン	攻撃者	攻撃者の動機	侵害されたデータ
農業（11）	インシデント80件、確認されたデータ漏洩55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96%を占めている	外部（96%）、内部（4%）（漏洩/侵害）	金銭目的（98%）、スパイ活動（33%）、イデオロギー（2%）（漏洩/侵害）	内部情報（67%）、その他（39%）、機密情報（35%）（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153件、確認されたデータ漏洩145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97%を占めている	外部（95%）、内部（3%）、パートナー（2%）（漏洩/侵害）	金銭目的（100%）（漏洩/侵害）	内部情報（83%）、認証情報（31%）、個人情報（10%）、その他（8%）（漏洩/侵害）
建設業（23）	インシデント307件、確認されたデータ漏洩252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96%を占めている	外部（97%）、内部（3%）（漏洩/侵害）	金銭目的（77%）、スパイ活動（23%）（漏洩/侵害）	内部情報（77%）、認証情報（31%）、その他（23%）、機密情報（21%）（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493件、確認されたデータ漏洩293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76%を占めている	外部（71%）、内部（29%）（漏洩/侵害）	金銭目的（97%）、スパイ活動（18%）、イデオロギー（3%）、愉快（1%）（漏洩/侵害）	個人情報（58%）、その他（39%）、内部情報（32%）、認証情報（18%）（漏洩/侵害）
情報産業（51）	インシデント1,589件、確認されたデータ漏洩784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82%を占めている	外部（83%）、内部（17%）、パートナー（1%）（漏洩/侵害）	金銭目的（78%）、スパイ活動（36%）、イデオロギー（1%）（漏洩/侵害）	その他（62%）、内部情報（51%）、個人情報（37%）、機密情報（27%）（漏洩/侵害）

表1. その他の業種一覧

業種（NAICS）	頻度	上位3つのパターン	攻撃者	攻撃者の動機	侵害されたデータ
事業経営業（55）	インシデント113件、確認されたデータ漏洩107件	「システム侵入」、「ソーシャルエンジニアリング」、「特権の悪用」がデータ漏洩/侵害の99%を占めている	外部（97%）、パートナー（2%）、内部（1%）（漏洩/侵害）	金銭目的（99%）、スパイ活動（1%）（漏洩/侵害）	内部情報（95%）、認証情報（33%）、医療情報（1%）、個人情報（1%）、システム（1%）（漏洩/侵害）
鉱業、採石業、石油・ガス採掘業（21）	インシデント64件、確認されたデータ漏洩52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96%を占めている	外部（98%）、内部（6%）、複数（4%）（漏洩/侵害）	金銭目的（100%）、スパイ活動（3%）、怨念（3%）（漏洩/侵害）	内部情報（59%）、認証情報（43%）、システム（20%）、その他（18%）（漏洩/侵害）
その他のサービス（81）	インシデント683件、確認されたデータ漏洩583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79%を占めている	外部（68%）、内部（33%）（漏洩/侵害）	金銭目的（69%）、スパイ活動（31%）（漏洩/侵害）	個人情報（57%）、内部情報（48%）、その他（44%）、機密情報（18%）（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2,549件、確認されたデータ漏洩1,147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（93%）、内部（7%）、パートナー（1%）（漏洩/侵害）	金銭目的（88%）、スパイ活動（17%）（漏洩/侵害）	内部情報（70%）、その他（25%）、認証情報（24%）、個人情報（24%）（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339件、確認されたデータ漏洩320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84%を占めている	外部（64%）、内部（36%）（漏洩/侵害）	金銭目的（100%）（漏洩/侵害）	個人情報（70%）、内部情報（40%）、その他（27%）、銀行情報（17%）（漏洩/侵害）
運輸および倉庫業（48–49）	インシデント361件、確認されたデータ漏洩248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（94%）、内部（7%）、複数（2%）、パートナー（1%）（漏洩/侵害）	金銭目的（98%）、スパイ活動（16%）、イデオロギー（1%）（漏洩/侵害）	内部情報（67%）、その他（25%）、認証情報（22%）、個人情報（20%）（漏洩/侵害）
公益事業（22）	インシデント358件、確認されたデータ漏洩213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92%を占めている	外部（92%）、内部（8%）、複数（1%）（漏洩/侵害）	金銭目的（70%）、スパイ活動（66%）、怨念（1%）（漏洩/侵害）	内部情報（80%）、機密情報（61%）、その他（42%）（漏洩/侵害）
卸売業（42）	インシデント330件、確認されたデータ漏洩319件	「システム侵入」、「ソーシャルエンジニアリング」、「特権の悪用」がデータ漏洩/侵害の98%を占めている	外部（97%）、内部（3%）（漏洩/侵害）	金銭目的（100%）（漏洩/侵害）	内部情報（93%）、認証情報（24%）、その他（3%）、個人情報（3%）、システム（3%）（漏洩/侵害）

表1. その他の業種一覧

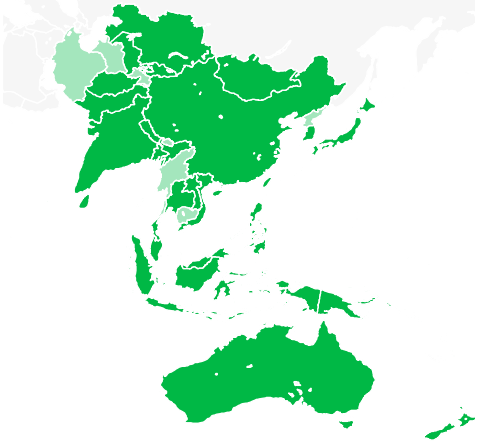
地域別の分析

サイバー犯罪が世界の地域ごとにどのように異なる（あるいは異ならない）のかについて、私たちはよく質問を受けます。このセクションでは、マクロ的地域の視点からサイバー犯罪を分析しています。このグローバルな視点が、皆さまにとって有益で有意義なものとなることを願っています。なお、各地域における可視性は、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。

ご自身の地域をこれらのページに掲載したいとお考えの場合は、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、お取引先やクライアントにもご協力を呼びかけていただければ幸いです。

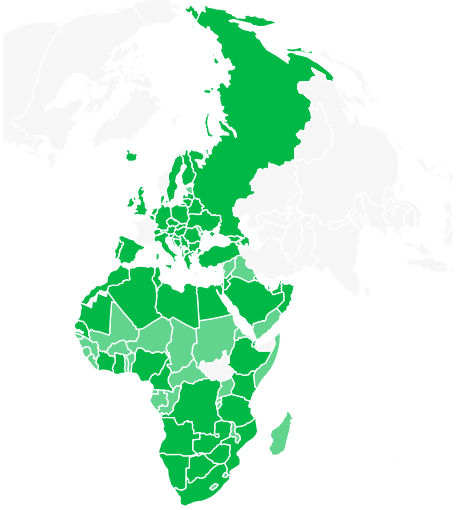
データあり　　データなし

アジア太平洋地域（APAC）



頻度	インシデント2,687件、確認されたデータ漏洩1,374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（83%）、スパイ活動（34%）（漏洩/侵害）
侵害されたデータ	内部情報（78%）、その他（41%）、機密情報（33%）（漏洩/侵害）

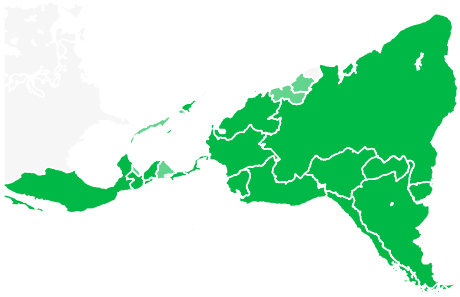
欧州、中東、アフリカ（EMEA）



頻度	インシデント9,062件、確認されたデータ漏洩5,321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89%を占めている
攻撃者	外部（71%）、内部（29%）（漏洩/侵害）
攻撃者の動機	金銭目的（87%）、スパイ活動（18%）（漏洩/侵害）
侵害されたデータ	内部情報（62%）、個人情報（49%）、その他（37%）、機密情報（13%）（漏洩/侵害）

データあり　　データなし

中南米、カリブ海地域（LAC）



頻度	インシデント657件、確認されたデータ漏洩413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99%を占めている
攻撃者	外部（100%）、パートナー（1%）、複数（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（84%）、スパイ活動（27%）（漏洩/侵害）
侵害されたデータ	内部情報（97%）、機密情報（27%）、その他（24%）（漏洩/侵害）

北アメリカ（NA）

頻度	インシデント6,361件、確認されたデータ漏洩2,867件
上位3つのパターン	「システム侵入」、「その他全て」、「ソーシャルエンジニアリング」がデータ漏洩/侵害の90%を占めている
攻撃者	外部（91%）、内部（5%）、パートナー（5%）、複数（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（95%）、スパイ活動（9%）（漏洩/侵害）
侵害されたデータ	内部情報（49%）、医療情報（35%）、認証情報（23%）、その他（17%）（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インテリジェンスが必要です。

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、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セキュリティインテリジェンスをぜひご確認ください。

2025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、LinkedInで Verizon Business（または著者の 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。