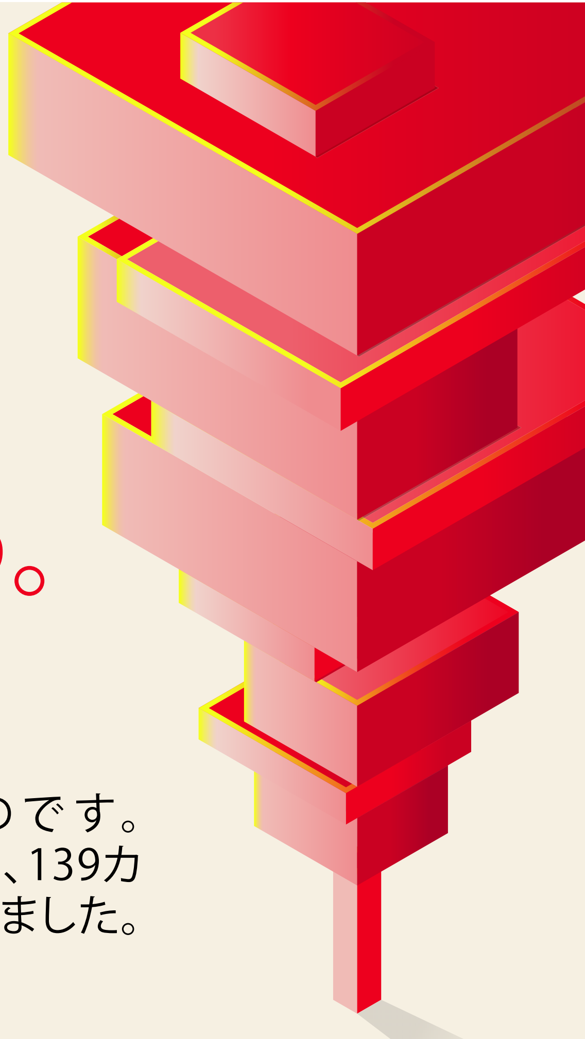
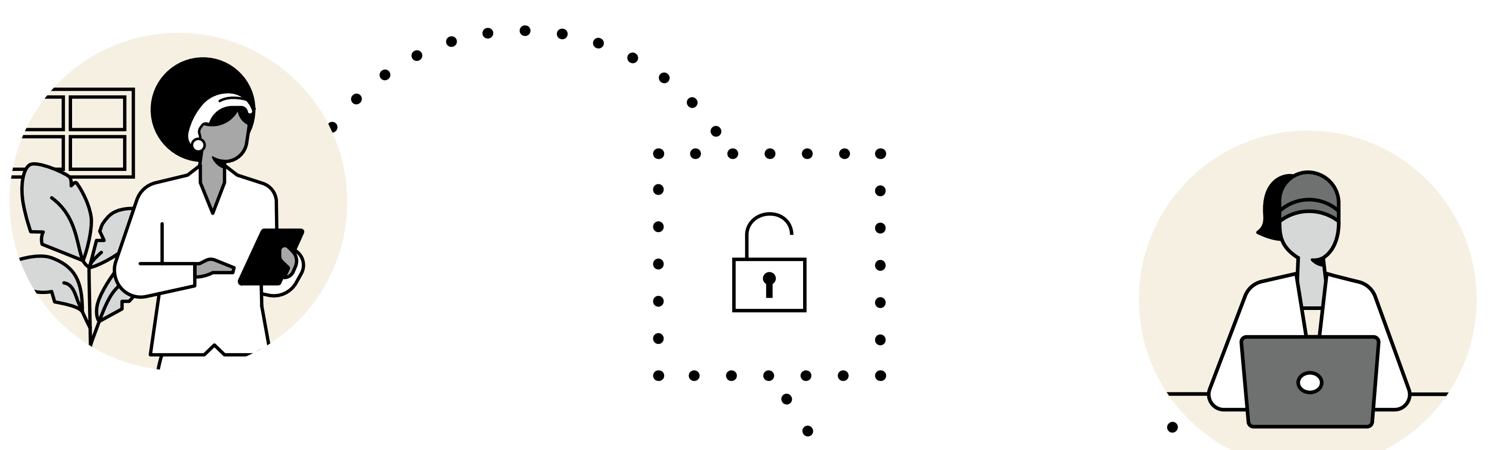
サイバーセキュリティの知識を蓄え、攻撃を阻止しましょう。



ベライゾンの2025年度データ漏洩/侵害調査報告書（DBIR）の主な調査結果

今こそ、闇に潜む攻撃者を暴くときが来たのです。2025年度データ漏洩/侵害調査報告書（DBIR）では、139カ国で発生した12,195件のデータ漏洩/侵害を分析しました。最も重要な調査結果の概要をご紹介します。



知らぬ間に“共犯者”？

15% → 30%

サードパーティが関与したデータ漏洩/侵害の割合は前年比で2倍に。パートナーやサプライヤーの選定が、これまで以上に重要になっています。

パートナーやサプライヤーと一体化したセキュリティ対策が、脆弱性を低減するカギに。

自社の弱点、把握していますか？攻撃者はお見通しです。

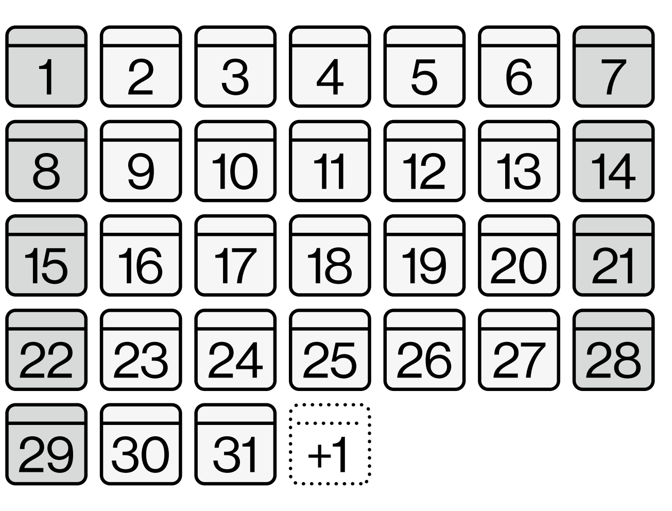
34% ↑

脆弱性の悪用は、データ漏洩/侵害の初期アクセス経路として34%増加し、現在ではデータ漏洩/侵害全体の20%を占めるまでになっています。

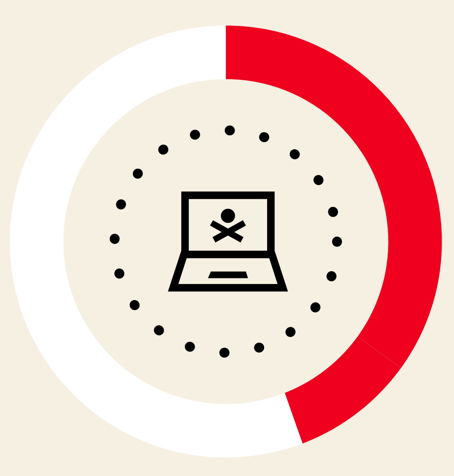
攻撃者は対応が後手になるか、まったく気付かないことを期待しています。

32日

ベライゾンの分析では、境界デバイスの脆弱性のうち、完全に修復されたのは約54%にとどまり、修正までにかかった日数の中央値は32日でした。



さらに多くの組織が人質に取られています。



44%

のサイバーセキュリティ侵害にはランサムウェアが関与しており、前年より37%増加しています。

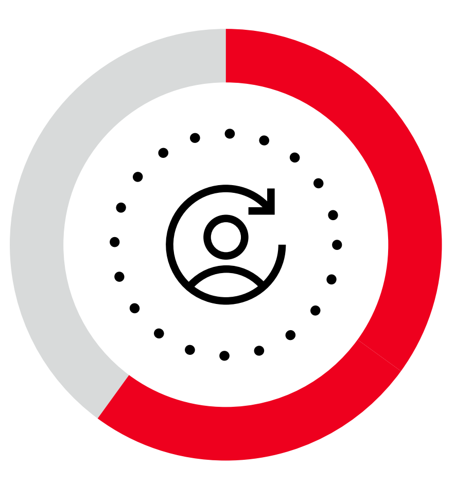
「払わなければどうなるか分かっているな」

$115,000

ランサムウェアは企業に多大な損害を与える可能性があります。
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11万5000ドルでした。

しかし、朗報もあります。攻撃を受けた企業の大半（64%）は身代金を支払っていません。

ほとんどのデータ漏洩/侵害に共通する要因とは？
それは「人」です。

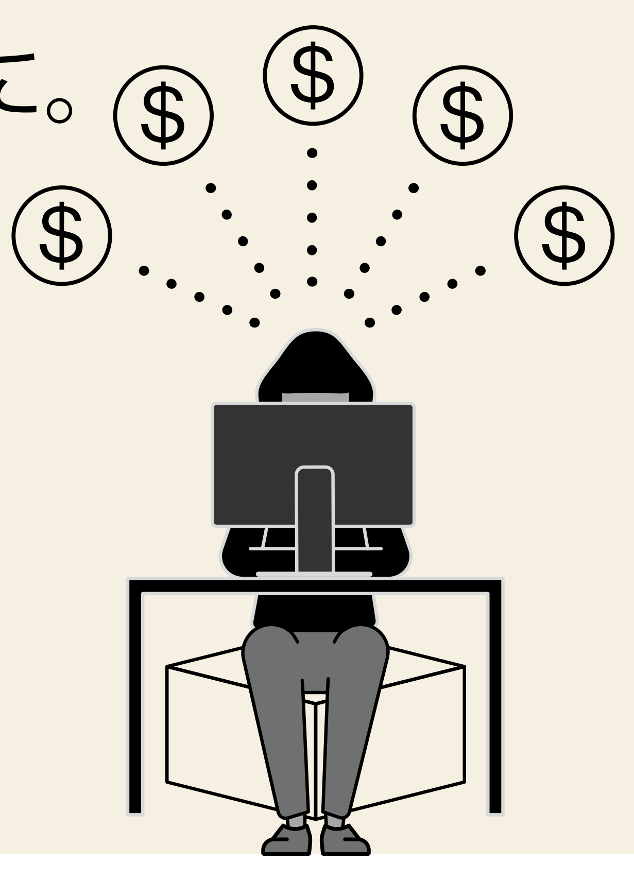


60%

サイバーセキュリティ侵害における人的要因の関与は前年とほぼ同水準で、60%にのぼりました。

認証情報の悪用やフィッシングなどのソーシャル攻撃が、この種のデータ漏洩/侵害の主な要因でした。

国家の注目は金銭に。



28%

スパイ活動を動機とした攻撃は、セキュリティ侵害の17%を占めています。しかし、国家が関与していたのはスパイ活動だけではありません。国家支援型のインシデントの約28%は、金銭的な動機によるものでした。

すべてのデバイスが標的になり得ます。

30%

管理対象のデバイス

46%

管理対象外のデバイス

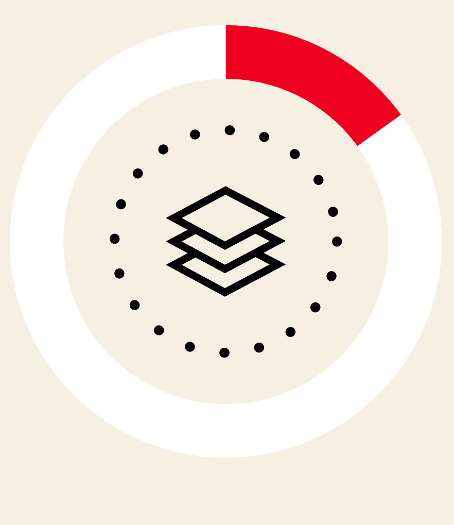
「インフォスティーラー」の認証情報ログを分析した結果、データ漏洩/侵害を受けたシステムの30%が企業支給のデバイスであることが判明しました。しかし、侵害されたデータに企業のログイン情報が含まれていたシステムの46%は管理対象外、つまり個人所有のデバイスか、企業のポリシー外で使用されていたのです。

ボットも犯行に加担しています。

2x

データによると、攻撃者はAIを活用して攻撃を強化しています。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。

従業員が 生成AIと何を共有しているかご存知ですか？



15%

の従業員は、会社のデバイスで生成AIプラットフォームに定期的にアクセスしており、情報漏洩のリスクを高めています。

DBIRは、最も包括的で信頼できるサイバーセキュリティ侵害の報告書です。

攻撃者が用いる攻撃の手口を知れば、自社のシステムをより的確に守ることができます。まずは2025年度データ漏洩/侵害調査報告書（DBIR）を読むことから、セキュリティ体制の強化への第一歩を踏み出しましょう。

常に変化する脅威の状況に対応するために、ベライゾンの担当者にぜひご相談ください。経験豊富な私たちのチームがお客様のデータを「闇」から守ります。

報告書を読む：verizon.com/dbir