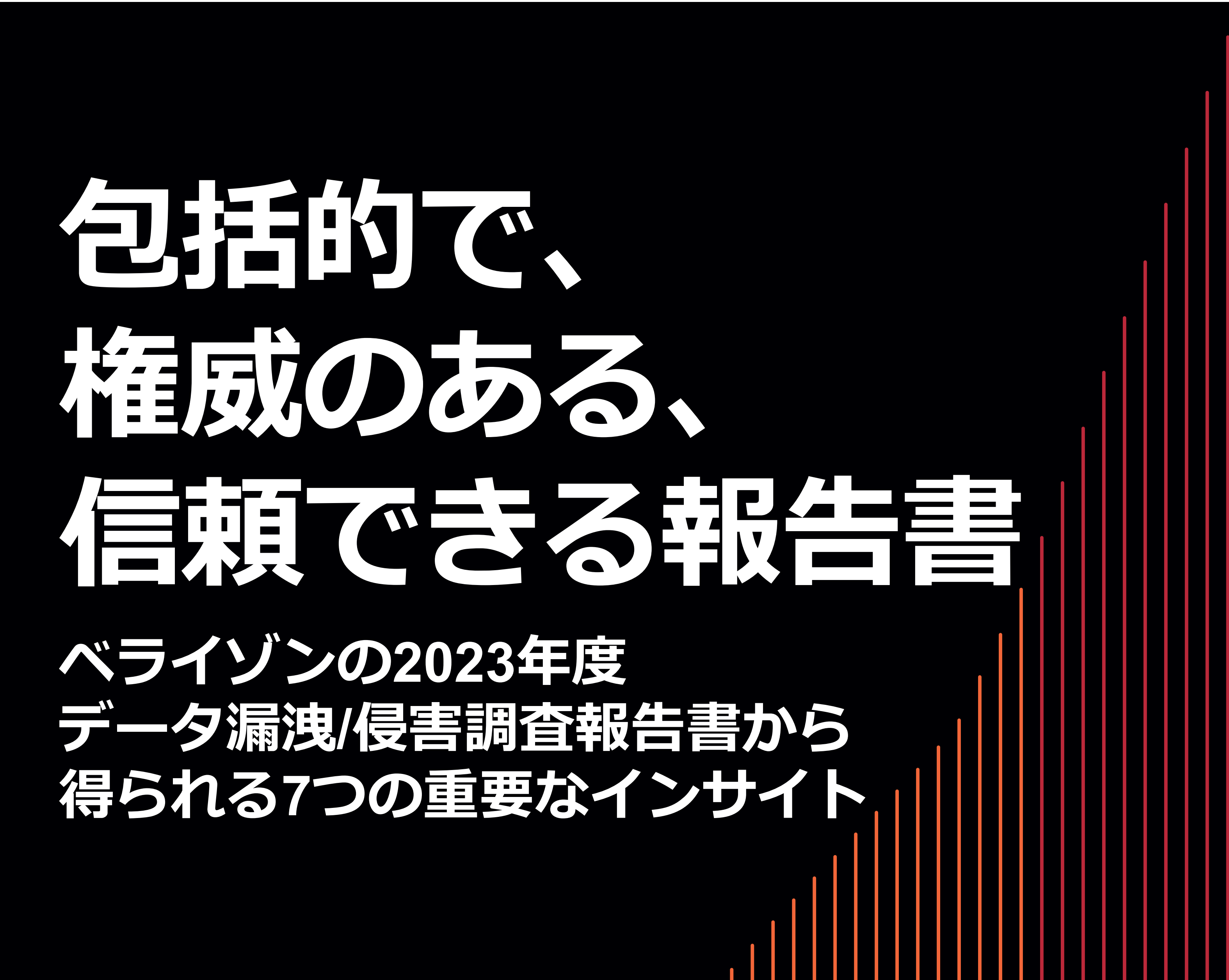
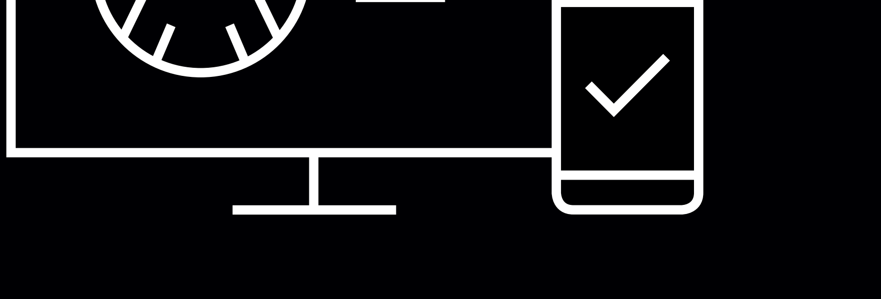
包括的で、権威のある、信頼できる報告書

ベライゾンの2023年度データ漏洩/侵害調査報告書から得られる7つの重要なインサイト



データを狙うサイバー犯罪者は、価値の高い企業を標的に、さまざまな攻撃を仕掛けている

この内容は、過去1年間のサイバー犯罪の傾向を分類し分析した、ベライゾンの2023年度データ漏洩/侵害調査報告書から得られた紛れもない教訓です。本報告書では、深いインサイトと独自の機知を交えて、世界中の企業に向けられた、最も普及し、急成長している危険な攻撃パターンを探っています。



「なりすまし」が増えている

50%

2022年に確認されたソーシャルエンジニアリング攻撃のインシデントの50%が「なりすまし」によるものでした。巧妙なシナリオに騙だまされて情報を提供したり、データ漏洩/侵害につながる恐れのある行為を実行させたりします。

「データを取り戻したければ、金を払え」

「ランサムウェア」とは、データを悪意を持って暗号化し、そのデータの返却や解除のために身代金を要求する手口です。被害件数はデータ漏洩/侵害全体の24%に上っています。ランサムウェアは、組織的犯罪者によるインシデントの62%以上、金銭目的を動機とするインシデントの59%で使用されています。

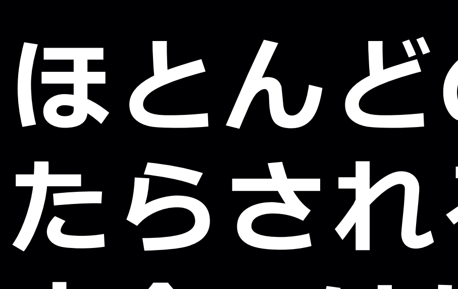
24%

脅威が増加している

32% 以上

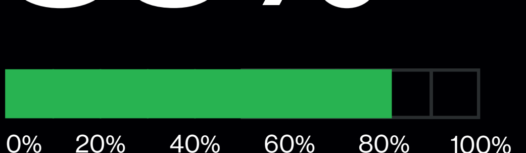
Log4jの脆弱性スキャニングの32%以上が、Log4jリリース後30日以内に発生しています。この利用度の高いJavaベースのユーティリティの欠陥が悪用され、サーバーがハッカーに支配される可能性があります。

このことは、概念実証（PoC）から大規模な悪用に至るまでの展開スピードが、いかに速いかを示しています。



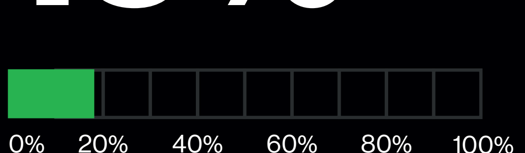
ほとんどの脅威は外部からもたらされる。しかし、内部も安全ではない

83%



データ漏洩/侵害の83%は外部からのもので、主に金銭目的を動機とする組織的犯罪グループによる攻撃です。

19%

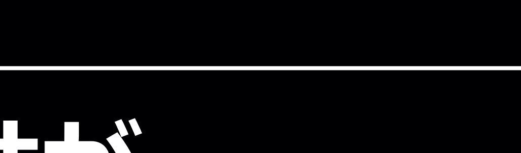


19%は内部関係者が関わっており、悪用や単純な人的ミスなど、意図的であるかどうかに関わらず損害をもたらしています。

人的要素への耐性が高いシステムが必要

データ漏洩/侵害の74%は、エラー、特権の悪用、盗まれた認証情報の悪用、ソーシャルエンジニアリングなどの人的要素が関わっています。

74%

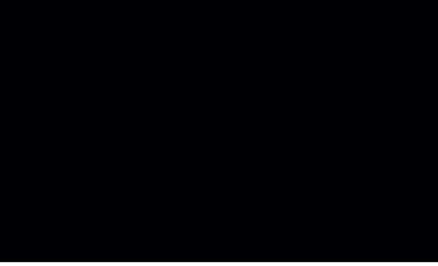


悪意ある攻撃者は巧妙で執拗、しかも、成功体験が多すぎる

49%

外部の攻撃者によるデータ漏洩/侵害の49%は盗まれた認証情報の悪用によるもので、フィッシングは外部からの攻撃の12%を占めています。データ漏洩/侵害の5%には、脆弱性を悪用する攻撃手法が使われています。

これは、多様な攻撃経路を想定する必要があることを示しています。



そして、ご想像通り、（ほぼ）いつもお金が目的

データ漏洩/侵害の95%は、金銭目的を動機としています。

95%

組織の保護は、直面する脅威を認識することから始まります。データ漏洩/侵害を検知するまでの平均時間を短縮することで、効果的に回復する方法が大きく変わってきます。

データ漏洩/侵害の全体像については、ベライゾンの「2023年度データ漏洩/侵害報告書（DBIR）」をご覧ください。そして、お近くのベライゾンビジネスの担当者に、お客様のインフラをサイバー攻撃から守るために、ベライゾンがどのようなご支援をしているのかをご相談ください。

DBIRは、verizon.com/dbirでお読みいただけます。

verizon✓