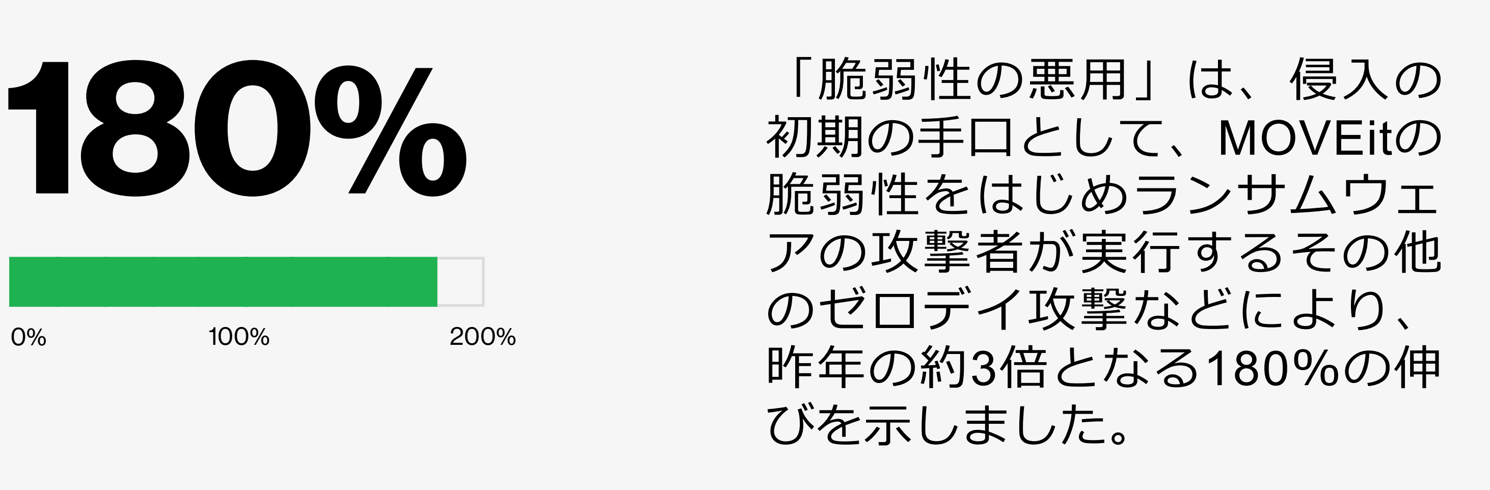
# 彼らの
# 侵入手口を
# データから
# ”覗き”見る。

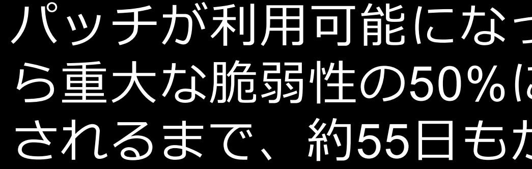
## ベライゾンの2024年度
## データ漏洩/侵害調査報告書
## から得る主なインサイト

昨年はサイバー犯罪者にとって記録的な年でした。ベライゾンの「2024年度データ漏洩/侵害調査報告書」によると、過去最高の1万件以上のデータ漏洩/侵害が発生し、その被害は94カ国に及びました。ベライゾンは、このような活動を追跡・分析し攻撃パターンの傾向を報告書としてまとめるとともに、刻々と変化するサイバー脅威に対応するための情報を提供しています。以下はその一部を抜粋したものです。



## さらされる脆弱性。

180%



「脆弱性の悪用」は、侵入の初期の手口として、MOVEitの脆弱性をはじめランサムウェアの攻撃者が実行するその他のゼロデイ攻撃などにより、昨年の約3倍となる180%の伸びを示しました。

## より迅速な対応が必要。

パッチが利用可能になってから重大な脆弱性の50%に適用されるまで、約55日もかかる可能性があります。実に危険な遅れです。

55日

---

## より多くのトレーニングが必要。

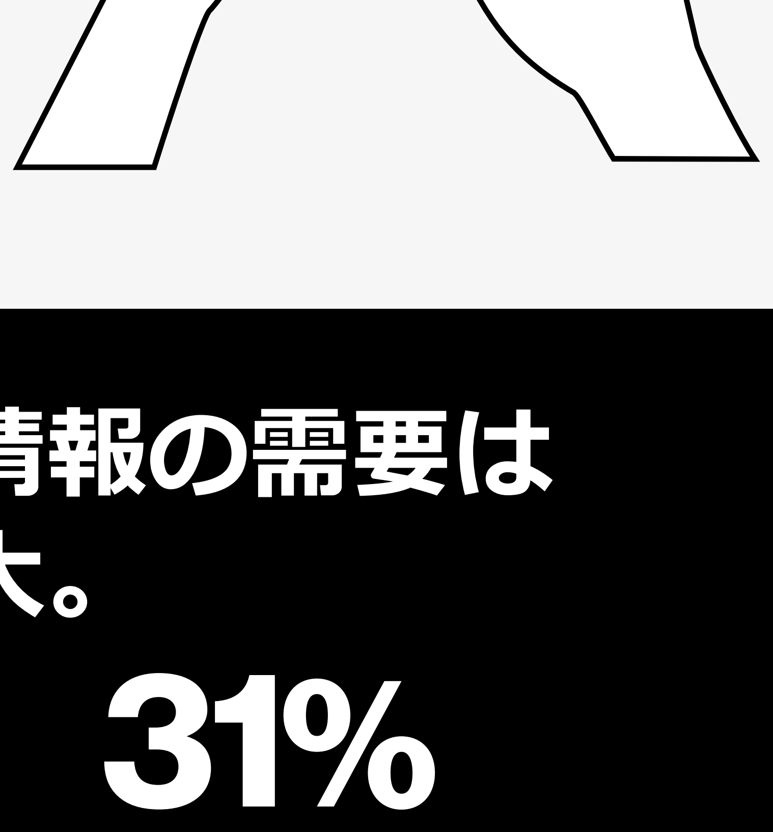
68%

データ漏洩/侵害の68%は、悪意のない人的要素が関係しており、「ソーシャルエンジニアリング」攻撃の犠牲者あるいは何らかの「エラー」を犯した人によるものでした。

## あっという間に騙される「フィッシング」

< 60 秒

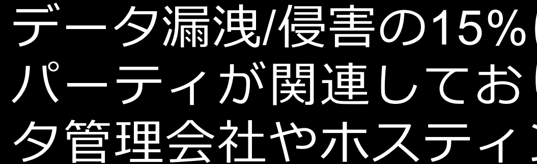
フィッシングメールに騙されるまでの時間は中央値で60秒未満です。



## 盗まれた認証情報の需要は依然として絶大。

過去10年間におけるすべてのデータ漏洩/侵害の31%は、「盗まれた認証情報の悪用」が関連しています。

31%



---

## サードパーティの選択は賢く。

15%

データ漏洩/侵害の15%はサードパーティが関連しており、データ管理会社やホスティングパートナーのインフラが侵害されたり、ソフトウェアのサプライチェーンが直接的または間接的な要因になっています。

## 「素晴らしいデータだ。もし何かあったらどうしよう」

2023年のデータ漏洩/侵害の32%は、「ランサムウェア」を含む何らかの「恐喝」手法が関連しています。

32%

$46,000

「ランサムウェア」または何らかの「恐喝」による、金銭的動機に基づくインシデントに関連する損失額の中央値は46,000ドルでした[1]。

## 詐欺の犠牲は高くつく。

$50,000

2022年と2023年の「ビジネスメール詐欺（BEC）」による損失額の中央値は約5万ドルでした[1]。

---

## サイバー脅威はますます複雑かつ危険になっています。

現在の傾向と悪質な攻撃者が使用する新たなテクニックをより深く理解することで、組織の保護にお役立てください。サイバーセキュリティ侵害情報の信頼できる情報源であるベライゾンの2024年度データ漏洩/侵害調査報告書の完全版で、包括的な考察をお読みください。

また、ベライゾンの経験豊富なチームが、サイバー攻撃との継続的な戦いにおけるお客様の組織の取り組みをどのようにサポートできるか、ベライゾンの担当者にお問い合わせください。

報告書を読む：verizon.com/dbir

verizon✓
business

1. 米国連邦捜査局インターネット犯罪苦情センター（FBI IC3）に基づく