

情報収集は最大の防衛

ベライゾンの
2022年版データ漏洩/侵害調査報告書の
主な調査結果

2008 2022

ベライゾンは15年にわたり
データ漏洩/侵害パターンを追跡

2022年版調査報告書の概要：

5,212件

におよぶデータ
漏洩/侵害の分析

23,896件

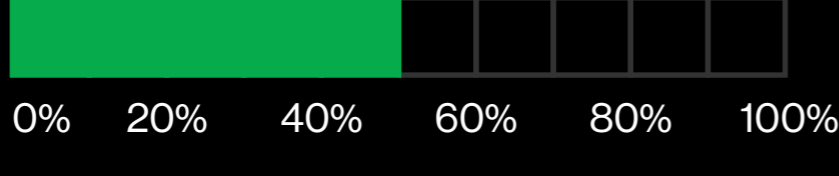
のセキュリティ
インシデントを
調査

87組織

がデータ提供に
協力

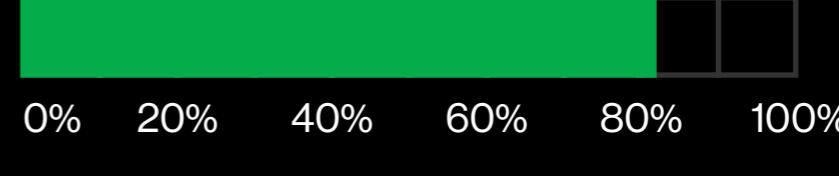
調査結果の概要：

50%以上



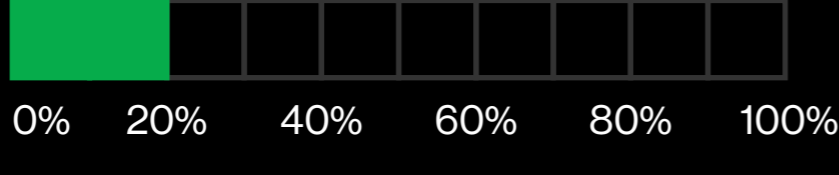
データ漏洩/侵害の半数
以上で、リモート
アクセスあるいはWeb
アプリケーションが
利用されている

82%



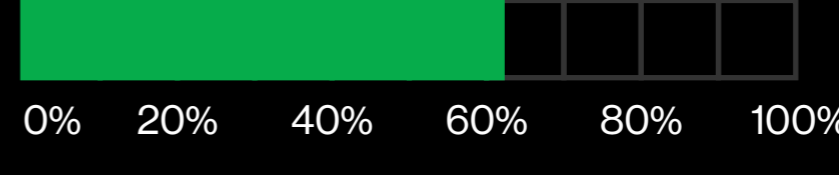
人的要因による
データ漏洩/侵害は
82%にも上る

20%



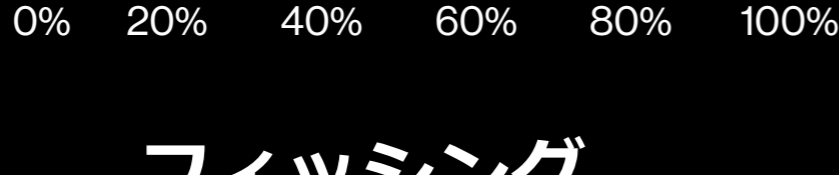
データ漏洩/侵害の
20%にソーシャル
エンジニアリングが関与

62%



システム侵入インシデントの
62%はパートナー絡みの
もので、大半は単一の
サプライチェーンへの
侵害が原因

66%



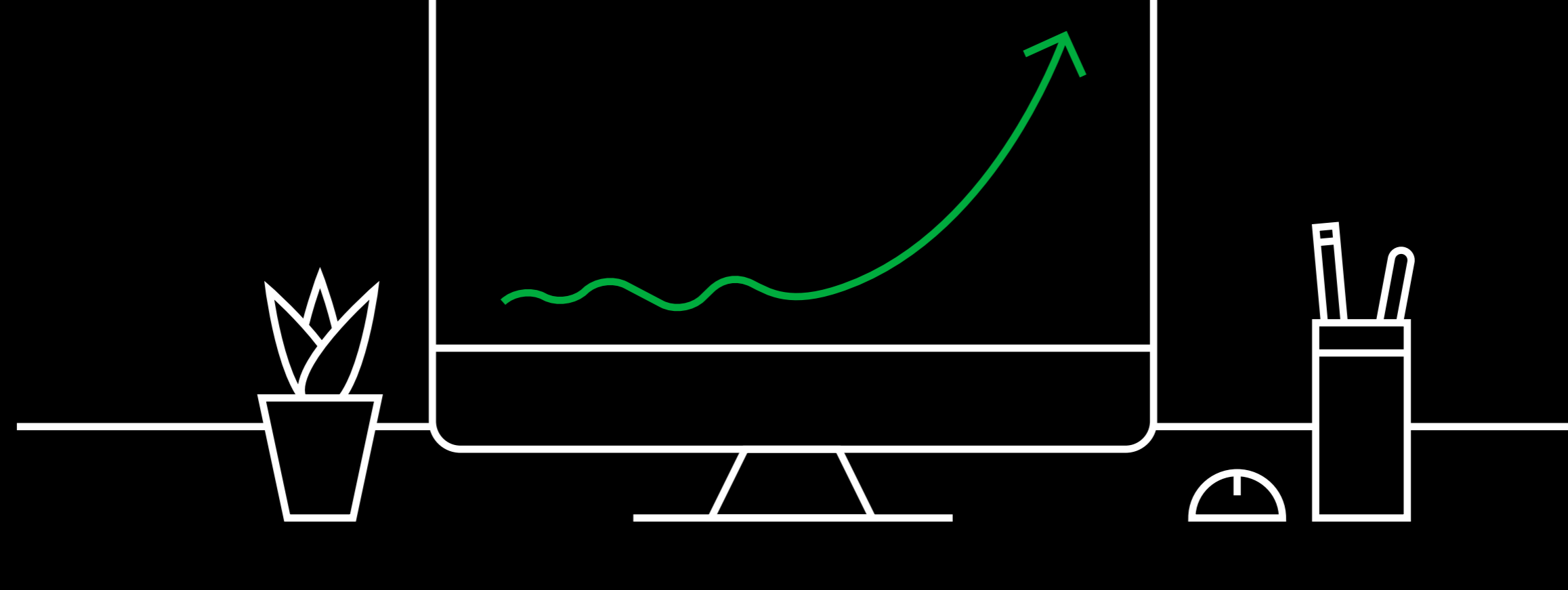
フィッシング、
盗まれた認証情報、
ランサムウェアが、
データ漏洩/侵害の
約3分の2を占める

95%

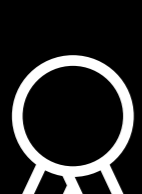


データ漏洩/侵害の
95%は、5ステップ
以下で行われている

ランサムウェアは
昨年度より13%増加し、
過去5年間の合計を
上回るほど急増



データ漏洩/侵害の
4つの主要経路：



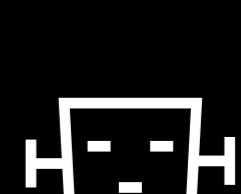
認証情報



フィッシング



脆弱性の悪用



ボットネット

これらすべてに対処できなければ、組織の安全は確保されない。

攻撃者の特徴

4/5

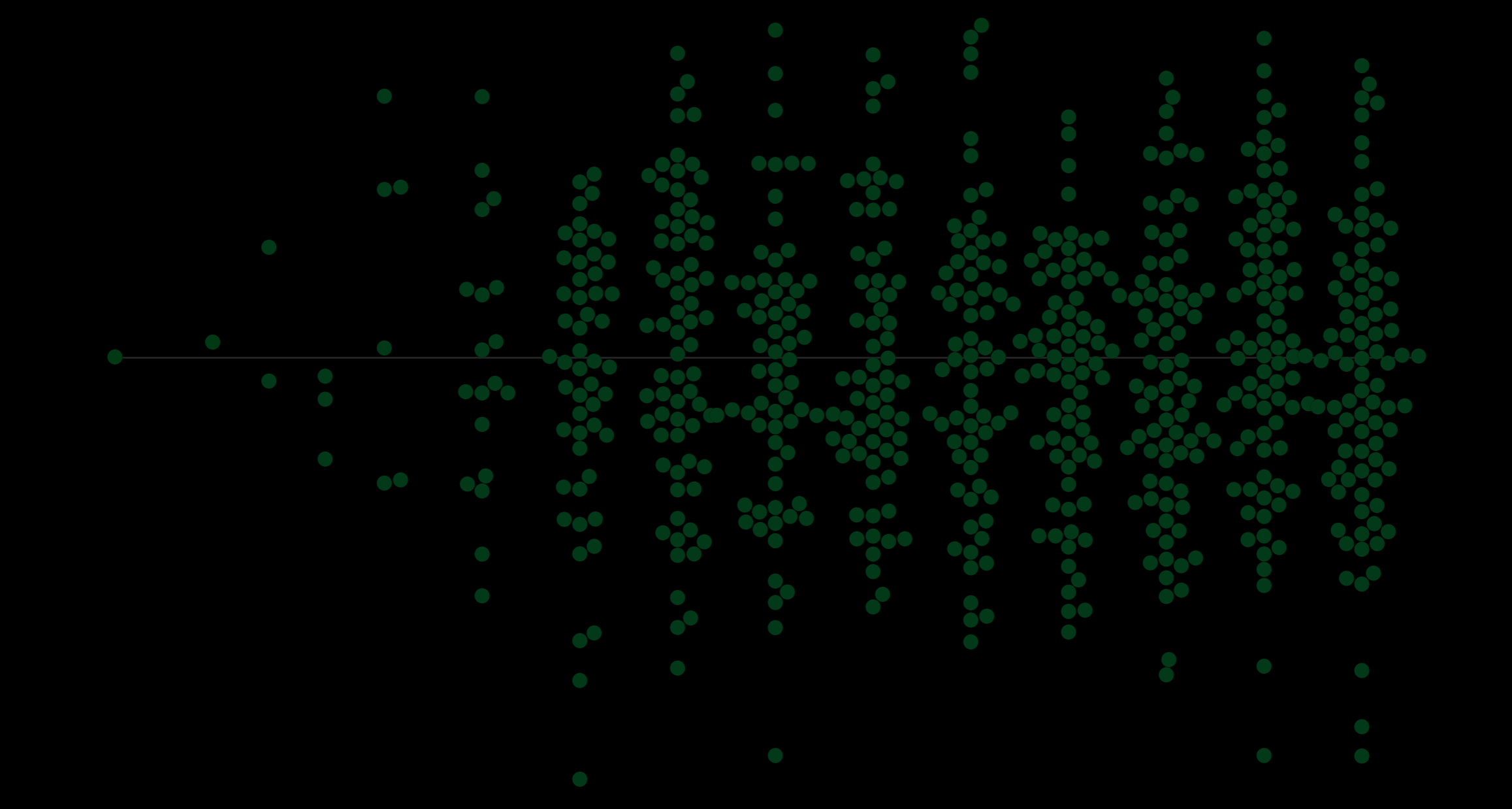
ほぼ5件中4件が
組織犯罪によるもの

#1

動機の1番は
金銭目的

#2

2番目は
スパイ活動



組織の安全を確保することが非常に重要。
その第一歩として、ベライゾンのデータ漏洩/侵害調査報告書は
最適です。

12の業界と世界の4地域に焦点を当てた、データ漏洩/侵害の
最新動向に関するより詳細な分析については、2022年版の
データ漏洩/侵害調査報告書（DBIR）の完全版をダウンロード
してください。

[報告書を読む](#)

verizon

Network details & coverage maps at vzw.com. © 2022 Verizon. RFP2400522