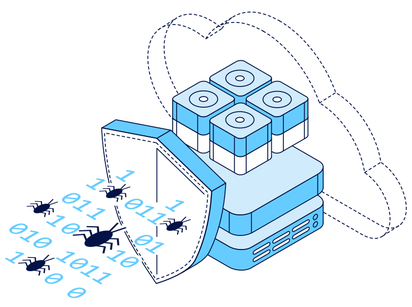
アジア太平洋版

2022 ランサムウェア・トレンド・レポート

2022年1月、ある独立系調査会社が、無作為に選んだ**1,000**名のITリーダーを対象に、自社環境にランサムウェアが及ぼした影響、およびそれに対する修復手段と将来を見据えた戦略について調査を実施しました。回答者の役職は、最高情報セキュリティ責任者（CISO）、セキュリティプロフェッショナル、バックアップ管理者、IT運用の4種類で、アジア太平洋、欧州、中東およびアフリカ、南北アメリカの16の国のさまざまな規模の組織を代表しています。アジア太平洋地域からも**200**人が参加しました。

拡大するランサムウェア



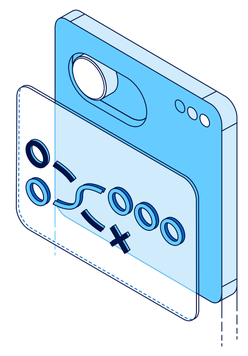
97%

バックアップリポジトリの感染を試みたランサムウェア攻撃の割合。うち**73%**が成功

52%

暗号化されてしまった本番データの割合。復元できたのは、そのうち**68%**

身代金≠修復



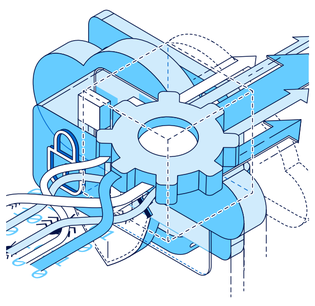
18%

身代金を支払わずに復元に成功した組織の割合

36%

身代金を払ってもデータを復元できなかった組織の割合

存続のためのテクノロジー



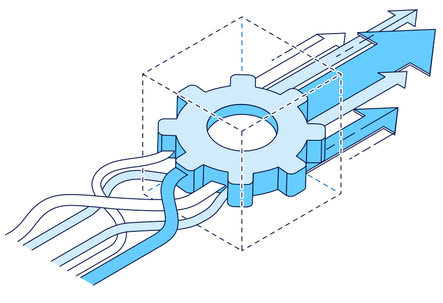
84%

復元力の確保をバックアップログやメディアの可読性に依存している組織の割合。裏を返せば、リストアやテストの機能で定期的にテストを行っている組織はわずか**16%**

41%

ランサムウェア攻撃を受けた際、データを復元する前にまず分離されたサンドボックスにリストアを行った組織の割合

組織の連携



55%

バックアップとサイバーセキュリティの間で大幅なまたは全面的な見直しが必要と考えている組織の割合

29%

サイバーチームのランサムウェアのプレイブックで、検証や清浄な状態であることを確認する業務が盛り込まれている割合

安全なバックアップは企業の最終防衛線

ランサムウェアは、1件あたり200万ドル（米国）近くもの被害を及ぼす災害です。Veeam®は、安全なバックアップは、ランサムウェア攻撃に対抗する企業の最終防衛線であると考えています。Veeamのソフトウェアは安全設計。独自ハードウェアのロックインもないので、オンプレミス、クラウドを問わず、現在ご利用中のアーキテクチャとも機能します。信頼できるバックアップがあれば、ダウンタイムやデータ消失に違いが生まれ、高額な身代金を払う必要もなくなります。

詳細はこちら：www.veeam.com/jp

レポート全文のダウンロードはこちら