リスクに備えるか、晒されるか:

COHESITY

金融サービス業におけるサイバーレジリエンスの格差

サイバー攻撃はもはや単発の出来事ではなく、デジタル世界では常態化しています。世界中の金融サービス業の組織がますます標的にされており、日々その現実を改めて思い起こさせられます。影響を受けない組織はありません。脅威の頻度が高まり、巧妙性が増すことで、金銭、業務、評判への測定可能な被害をもたらす深刻なサイバー攻撃が急増しています。

金融サービス業の組織のITおよびセキュリティ運用の意思決定者およそ400名を対象としたグローバル調査により、この実態が明らかになりました。

77%
金融サービス業の組織の77%が重大なサイバー攻撃を経験

57%
が過去12か月以内に攻撃を受けた

4分の1
が複数回の攻撃を経験

その被害は深刻で、コストも急騰しています。

87%
が収益損失を経験

35%
が顧客喪失を経験

62%
上場している金融サービス業の組織の62%が、やむを得ず財務見通しを見直した

93%
が法規制上の影響に直面

79%
が過去12か月間に身代金を支払った

明白な証拠があるにもかかわらず、多くの金融サービス業の組織は自らのレジリエンスを過信しています。

46%
が、自社のサイバーレジリエンス戦略を完全に信頼

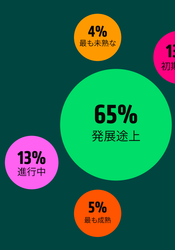
だに大半の組織は、対応と復旧も同じくらい重要な機能であるにも関わらず、予防と検知を優先しています。

順序はNISTのサイバーセキュリティフレームワークに基づいています。図のサイズは、サイバーレジリエンスへの投資割合を降順に表しています。

#3 識別 #1 防御 #2 検知 #4 対応 #5 復旧

自信と支出パターンが示すのは一部の側面のみ

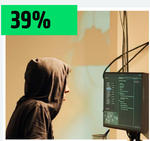
真のレジリエンスは、それを支える実践と能力にかかっています。実際のパフォーマンス指標に照らして評価すると、データ保護、データ復旧、脅威の検知と調査、アプリケーションレジリエンス、データリスク最適化という5つの必須領域すべてで成熟度が確認できた金融サービス業の組織は、わずか5%でした。



レジリエンス強化の必要性を認識することで、自動化やAIによって実現される次の進化が促されています。脅威が加速し複雑化する中で、検知の加速、対応の効率化、復旧の強化を実現するためには自動化が重要です。

56%

サイバー攻撃から得た重要な教訓の一つとして、検知、対応、復旧の自動化強化を挙げた回答者

39%

主体的な判断も含め、脅威の検知・対応においてAIが中心的な役割を果たすと考えている回答者

99%

2026年までにデータセキュリティ運用を支援するためにAIを活用する予定の回答者

リスクに対する準備は万全ですか?

詳細な調査結果については、サイバーレジリエンスに関する金融サービス業の業界レポートをダウンロードいただけます。

ランサムウェアレジリエンスのワークショップをご予約ください。

CohesityのeBook「**サイバーレジリエンス実現のための5つのステップ**」を入手すると、今すぐ成熟度を高めることができます。

調査はVanson Bourneが実施し、2025年に北米、アジア太平洋、欧州、ラテンアメリカの地域において、従業員1,000人以上の組織に所属するITおよびセキュリティリーダー3,200名を対象に行われました。回答者の中には、金融サービス業の組織からの参加者390名が含まれています。

COHESITY VansonBourne

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054
620003A-001-JP 5-2026