リスクに備えるか、晒されるか:

COHESITY

日本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。病院や政府機関、グローバル企業が被害に遭う度に、日常化した脅威を思い知らされます。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。

日本のITおよびセキュリティ運用企業の意思決定者400名を対象としたアンケートで、その現実が明らかになりました。

64%
深刻なサイバー攻撃を受けたことがある:

45%
過去12か月間に被害に遭った:

4分の1弱
複数回の攻撃を受けたことがある:

その被害は深刻で、コストも急騰しています。

収益を損失:

顧客を損失:

やむを得ず財務見通しを修正: 上場企業の

法律や規制上の影響に直面:

過去12か月間で身代金支払いが発生:

明白な証拠があるにも関わらず、多くの組織は自らのレジリエンスを過信しています。

42%
自社のサイバーレジリエンス戦略を完全に信頼:

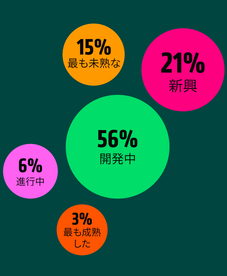
未だに大半の組織は、対応と復旧も同じくらい重要な機能であるにも関わらず、予防と検知を優先しています。

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。

識別　防御　検知　対応　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組織は、わずか3%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。

51%

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:

31%

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、日本版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。

Vanson Bourne社が、2025年に従業員1,000名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（うち日本人400名）を対象に調査を実施しました。

COHESITY　VansonBourne

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054
6200022-001-JP 2-2026