リスクに備えるか、晒されるか

COHESITY

中規模組織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。世界中の中規模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。影響を受けない企業はありません。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。

従業員**1,000～1,999**名の組織における**IT**およびセキュリティ運用の意思決定者およそ**1,000**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。

75%
重大なサイバー攻撃を経験した組織。

55%
過去12か月以内に攻撃を受けた組織。

4分の1
複数回の攻撃を経験した組織。

その被害は深刻で、**コストも急騰しています。**

85%	36%	76%	92%	82%
収益の損失	顧客喪失	やむを得ず財務見通しを修正した上場企業	法律や規制上の影響に直面した	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。

47%
自社のサイバーレジリエンス戦略を完全に信頼

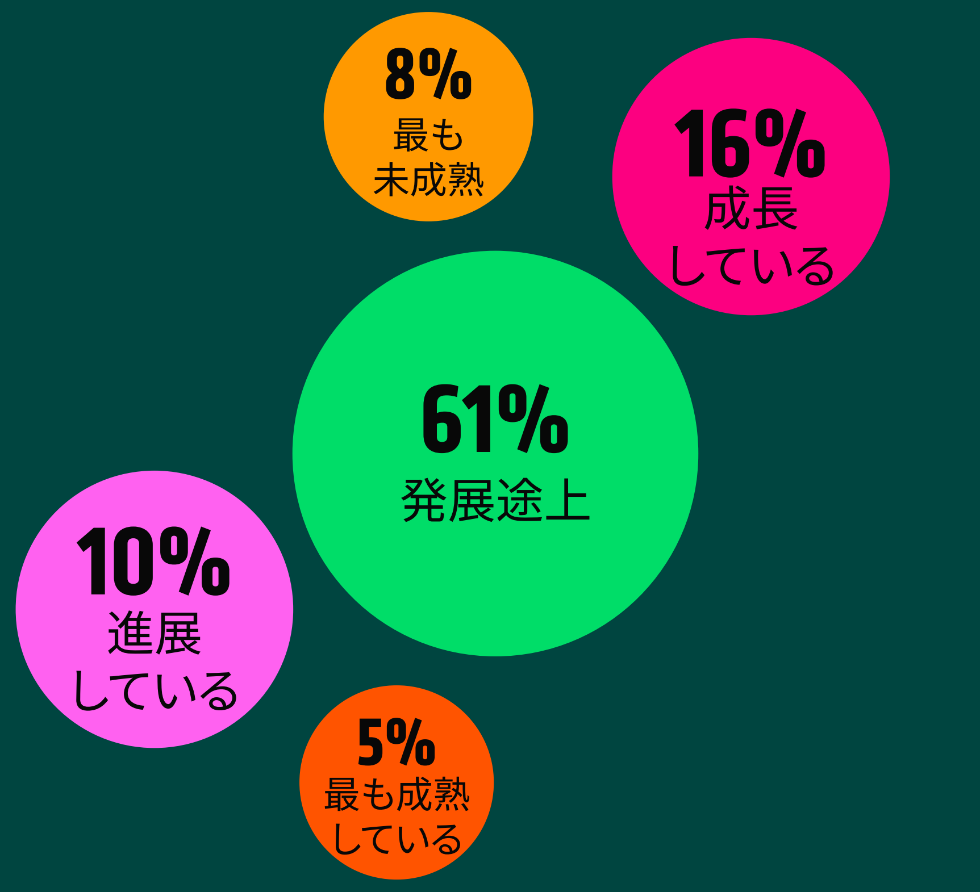
対応と復旧も同じくらい重要な機能であるにも関わらず、大半の組織は未だに予防と検知を優先しています。

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	#1	#2	#4	#5
識別	保護	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、データの復旧、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5%でした。



最もサイバーレジリエンスの高い組織にとって、レジリエンスとは体系的かつ包括的なものです。ベストプラクティスには、機密データがグローバルにバックアップされていること、多要素認証と管理コントロールが適用されていること、脅威インテリジェンスが最大化されていること、修復を通じて復旧が保護されていること、コンプライアンス保護が一貫して実行されていることなどがあります。

ですが、成熟度は静的ではありません。

53%
自社のレジリエンス戦略には伸びしろがあると考えている

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%

検知、対応、復旧の自動化強化は、サイバー攻撃から得た重要な教訓の一つである

37%

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

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を活用する予定である

リスクに対する準備は万全ですか?

- 中規模組織向けの**Cohesityのサイバーレジリエンスソリューションを詳しくご覧ください。**
- この**レジリエンススコアカード**でサイバーレジリエンスの**成熟度を評価**
- 5つのステップを通じた**サイバーレジリエンスのアクションプランによる強化**

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。回答者には、従業員が1,000～1,999人の中規模組織に勤務する977人の参加者が含まれます。

COHESITY VansonBourne

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054
6200013-001-JP 7-2026