リスクに備えるか、晒されるか:

COHESITY

公共部門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。世界中の公的機関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。

公的機関のITおよびセキュリティ運用部門の意思決定者399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。

67%
機関の67%が重大なサイバー攻撃を経験

49%
が過去12か月以内に攻撃を受けた

4分の1弱
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。

85%
収益を損失:

42%
が顧客を喪失

61%
やむを得ず財務見通しを修正: 上場企業の61%

97%
が法律や規制上の影響に直面

92%
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。

54%
が、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。

#2 識別
#1 防御
#3 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組織は、わずか4%でした。

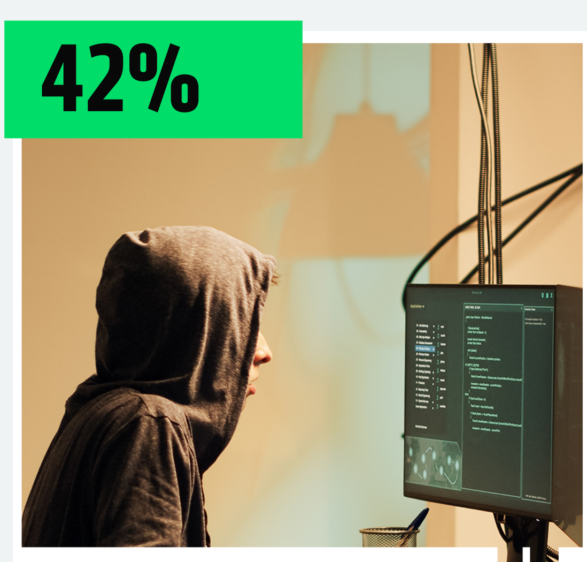
11% 最も未熟な
22% 新興
57% 開発中
8% 進行中
4% 最も成熟した

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

42%



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

98%

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公共部門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。回答者には、公的機関からの参加者399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
6200041-001-EN 6-2026