COHESITY

サイバーレジリエンスレポート

リスクに備えるか、されるか: 中規模組織におけるサイバーレジリエンスの格差

2026年5月

誰もがサイバー攻撃の検知や予防について語りますが、ニュースの見出しが伝えている現実はそれとは異なります。予防と検知だけでは、もはや十分ではありません。成熟度の高い企業でさえ、IT運用から経営層、さらにはその先にまで影響が波及する、深刻な業務停止に見舞われています。

Cohesityは、その理由を理解するとともに、レジリエンスを備えた組織と依然として苦戦している組織を分けている要因を明らかにするため、11か国のIT・セキュリティ運用の意思決定者3,200名を対象に調査を実施しました。その中には、中規模組織からの約1,000名の参加者が含まれていました。調査結果は、迅速に自信を持って復旧できるリスクへの備えが整った組織と、長期的な混乱と二次的な財務的損失に対して脆弱なままの組織との間で、レジリエンスの格差が拡大していることを示しています。

本調査では、実質的な影響を伴うサイバー攻撃がもたらした現実の影響に加え、各中規模組織がベストプラクティスに照らして自社のサイバーレジリエンスをどのように自己評価したか、また、こうしたインシデントを検知し、対応し、復旧するためにどのような取り組みを行ったのかを分析しています。さらに、そこから得られた教訓に加え、AIと自動化を活用してレジリエンスを加速させ、レジリエンスの分断を埋めようとする取り組みも浮き彫りにしています。

重大なサイバー攻撃:
現代ビジネスにおける新たな現実

サイバーインシデントは一様ではありません。多くの組織は、日常的に発生するフィッシング攻撃やマルウェアの不正アクセスの試行、システム障害への対応を、ほぼ毎日のように行っています。しかし、重大なサイバー攻撃はそれとは異なります。本調査では、測定可能な財務、評判、運用への影響、または顧客離れを伴うインシデントを「重大なサイバー攻撃」と定義しています。

こうした影響の大きい攻撃は、中規模組織ではもはや例外的な出来事ではありません。

75%

少なくとも1回の重大なサイバー攻撃を経験した

55%

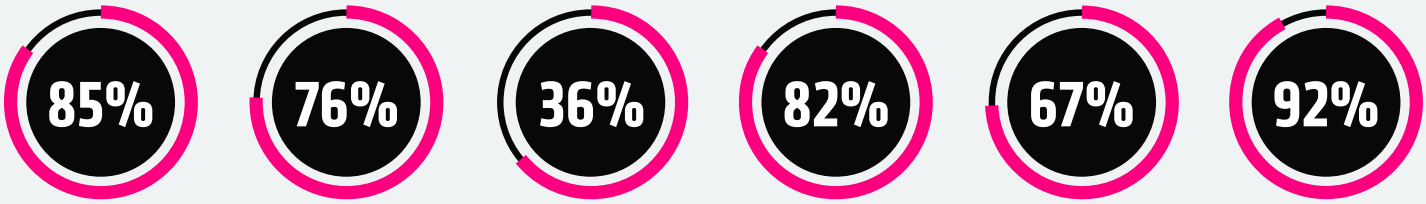
過去12か月以内に1回経験した

25%

過去12か月間に複数回のインシデントを経験した

重大なサイバー攻撃がもたらす実際のコスト

調査対象となった中規模組織全体で、財務面および規制面での圧力が共通して見られました:



収益の減少があったと回答

業績見通しの修正を行ったと回答した上場企業[1]

顧客喪失

身代金の支払い(1件当たりの平均額は130万米ドル)

成長戦略から予算を振り替えた非公開企業

規制当局による罰金(46%)と訴訟または集団訴訟(33%)などの法的あるいは規制上の結果に直面した

[1] サイバーインシデントの発生後に業績見通しの修正を正式に開示している上場企業は比較的少ない一方で、本調査結果からは、財務的および業務的な影響が、公開されている開示資料から把握できる範囲を大きく上回って及んでいることが示唆されています。

結果に直面しても揺るがない自信

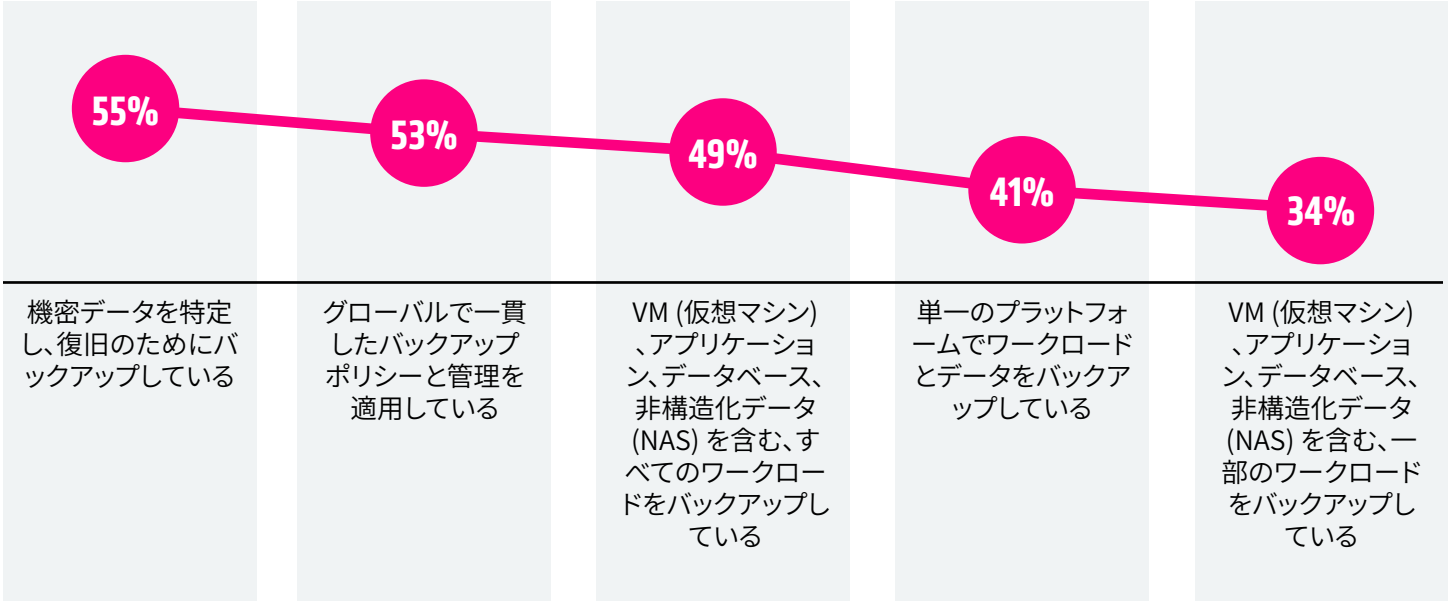
本調査で明らかになった財務面および業務面への影響の大きさを考えれば、組織のレジリエンスに対する懸念が広がっていることが想定されます。しかし、回答者の多く(47%)は、所属組織のサイバーレジリエンス戦略が現在の脅威に耐え得ると回答し、高い自信を示しました。この高い自信は、当の組織の多くが実際に被ってきた重大な影響と、鮮明な対照をなしています。

組織が実施していることと、実施できていないこと

私たちは表層に留まらず、レジリエンスのギャップがどこに存在するのかを明らかにすることを目指しました。この目的を達成するため、サイバーレジリエンスを構成する5つの中核領域(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、データリスク体制の最適化)に関連する主要な実践と能力について、各組織の取り組みを回答者に尋ねました。

ハイブリッドとマルチクラウド環境にまたがるデータ保護の分断

ハイブリッド/マルチクラウド環境全体のデータを保護するために、あなたの組織ではどのような対応を実施していますか?



中規模組織の半数強が、復旧のために機密データを特定しバックアップを取得しています。ほぼ同じ割合の中規模組織が、一貫したバックアップポリシーを適用し、グローバルにコントロールしています。すべてのワークロードをバックアップしている組織や、ワークロードやデータの保護に単一のプラットフォームを使用している組織は半数未満です。3分の1は、選択したワークロードのみをバックアップしています。こうした分断は、環境全体にわたる可視性と一貫性を損なう要因となっています。成熟したサイバーレジリエンスは、ゼロトラスト原則で保護された単一のインテリジェントなプラットフォームにおいて、バックアップと復旧を統合できているかどうかにかかっています。

データ回復性に関する対策は一般的だが、成熟度にはばらつきがある

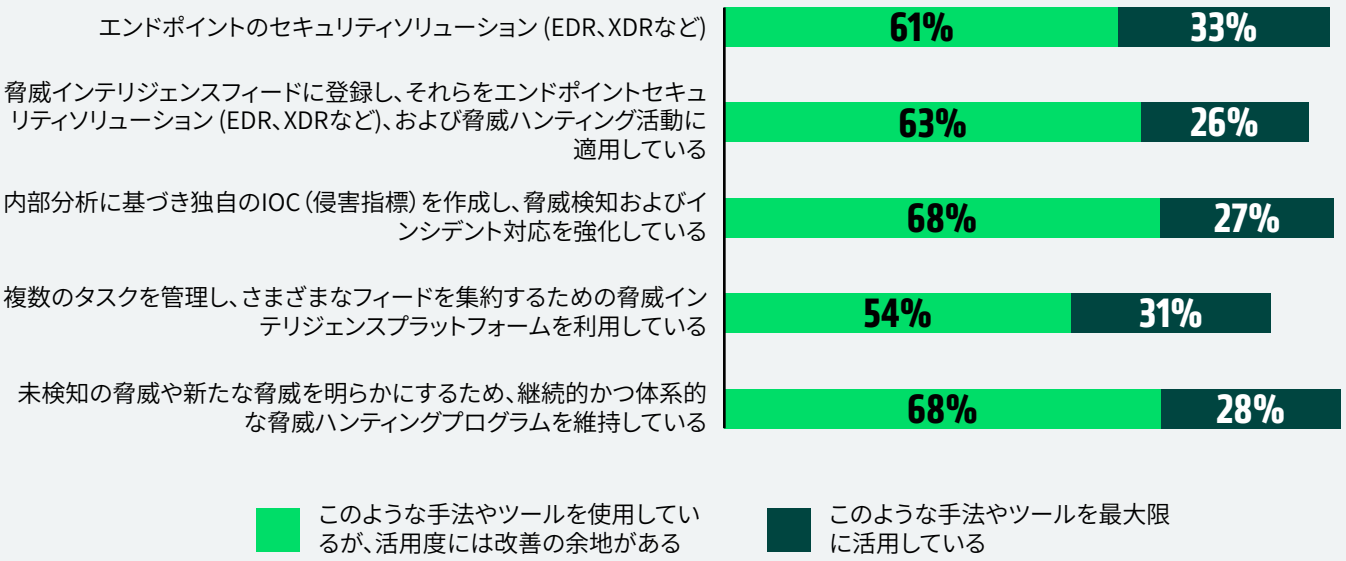
データを常に復旧可能な状態に保つために、あなたの組織ではどのような対策を講じていますか?

60%	バックアップと復旧ソリューションに関連する高リスクの管理者タスクに対して、さらなる認証を要求している
53%	バックアップソリューションに多要素認証を導入している
47%	「3-2-1バックアップルール」(異なる2つのメディアに3つのデータコピーを保持し、そのうちの1つのコピーをオフサイトに保管) に従っている
42%	重要なデータをイミュータブルな状態で保護している
38%	バックアップ対象のワークロードに最小権限アクセスを適用している

多くの中規模組織では、バックアップ環境へのアクセス制御を強化しており、その半数以上では、高リスクなタスクに追加の管理者承認を必要としています。一方で、多要素認証 (MFA) を強制している組織は約半数、また「3-2-1バックアップルール」を遵守している組織も半数近くに留っています。重要データをイミュータブル形式で保護している組織や、最小権限のアクセス権を適用している組織はさらに少数に留まります。こうしたギャップは、完全な復旧の確実性を損ないます。成熟したサイバーレジリエンスには、検証済みで隔離され、改ざん不可能な復旧用コピーが不可欠です。

脅威の検知・調査用ツールの活用は不十分

あなたの組織では、脅威の検知や調査に、以下の手法やツールをどのくらい活用していますか?



脅威の検出および調査ツールは広く導入されていますが、多くの場合、十分に活用されていません。ほとんどの中規模組織は、エンドポイントセキュリティ、脅威インテリジェンスフィード、カスタムIOC、脅威インテリジェンスプラットフォーム、および体系的な脅威ハンティングプログラムを使用していますが、これらのツールを十分に活用できている組織は少数です。成熟したサイバーレジリエンスは、これらのツールを統合し、可視性、検知、対応を向上させるという継続的かつインテリジェントな仕組みを基盤としています。

不完全なレジリエンス対策は再感染のリスクを高める

サイバー攻撃に対するアプリケーションレジリエンスを確保するため、あなたの組織ではどのような取り組みを行っている、または行う予定ですか?

57% システムを本番環境にリストアする前に、セキュリティコントロールのギャップを特定し、修正している

60% 技術、法務、戦略、経営、広報などの関係部門を横断したチームを巻き込み、年に一度のエンドツーエンドシミュレーションリハーサルを実施している

56% インシデント対応や復旧を支援するため、重要なシステムや情報のオンライン保管型リポジトリを利用している

47% インシデント調査、修復、セキュアな復旧のために、隔離された環境を使用している

33% すべてのバックアップデータに対してイミュータビリティを適用している

中規模組織ではアプリケーションレジリエンスへの取り組みが進展しつつあるものの、依然として課題が残っています。大多数が、システムをリストアする前にセキュリティコントロールのギャップを特定しています。同程度の割合の組織が、オンラインの保管型リポジトリを維持しています。半数以上の組織は、年に一度の復旧リハーサルも実施しています。セキュアな調査と復旧のために隔離されたクリーンルーム環境を利用する組織の割合は低くなっています。すべてのバックアップデータに対してイミュータビリティ(変更不可)を適用している割合はさらに低くなります。こうしたギャップにより、復旧プロセスは再感染やデータ損失の影響を受けやすくなります。成熟したサイバーレジリエンスは、事前の備えと、セキュアで検証可能な復旧環境を組み合わせることで実現されます。

リスク活用の拡大に伴い、データ分類が普及している

データ資産全体のリスクエクスポージャーを最小化するため、あなたの組織ではデータディスカバリーや分類の手法やツールをどのように活用していますか?

コンプライアンス対応のため、バックアップのプライバシーやセキュリティ違反を特定し、解決している

バックアップデータ分類を利用して、影響を受けるデータに対するコンプライアンス義務を決定している

インシデント発生前に、サイバー攻撃の重要度を定義し、理解している

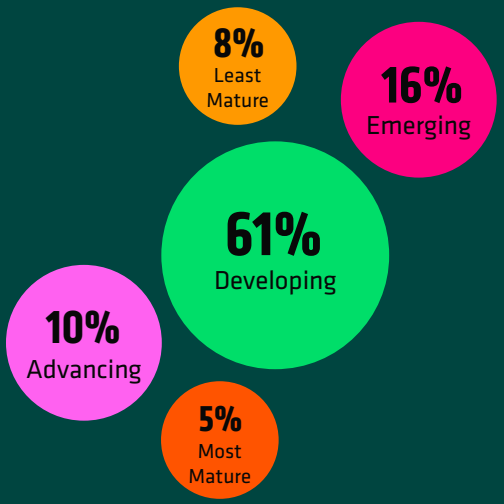
バックアップするシステムを特定し、優先順位を付けている

中規模組織では、コンプライアンス、対応、復旧の各局面で、データ探索と分類をより戦略的に活用する動きが広がっています。約3分の2の組織がプライバシー違反およびセキュリティ違反に対処している一方で、半数を超える組織が、攻撃時のコンプライアンス対応の指針となる分類を使用しています。また、半数以上の組織がインシデント発生前に重大性を定義し、リスクに基づいてバックアップの優先順位を決めています。成熟したサイバーレジリエンスでは、データリスク態勢を最適化し、保護・対応・復旧の指針となる体系的なアプローチとして、データ分類を活用します。

レジリエンス成熟度のより明確な全体像

回答を総合的にスコアリングした結果、中規模組織が実務においてどのようにレジリエンスを構築しているか、あるいは構築に苦戦しているかを示す、サイバーレジリエンス成熟度の大まかな指標が明らかになりました。その結果、大多数の組織は「発展途上」の段階に留まり、リスク対応型企業を特徴づける最も成熟した統合的能力を備えているのはわずか5%にすぎません。

サイバーレジリエンスの成熟曲線



最も成熟していない (8%):バックアップ、ポリシー、セキュリティ上の安全策の大半が欠如しているか、または不十分です。MFAや管理者制御はほとんど導入されておらず、復旧時の隔離も行われていません。コンプライアンスや重大性評価は大抵見過ごされています。

初期段階 (16%):一部のレジリエンス施策は実施されていますが、一貫性はありません。組織は、機密データのバックアップ、グローバルポリシーの適用、MFAの利用などを行っていますが、これらを組み合わせていることはほとんどありません。脅威インテリジェンスやコンプライアンス対応も存在しますが、成熟度は低く断片的です。

発展途上 (61%):バックアップ、管理者制御、脅威インテリジェンスなどのコアな施策は、比較的一般的になっていますが、依然としてばらつきがあります。復旧環境、コンプライアンスチェック、セキュリティギャップの是正は断続的に行われており、レジリエンス施策は部分的にしか効果を発揮していません。

進展中 (10%): グローバルなバックアップポリシー、管理者承認、復旧前の是正などを含む主要な施策の多くが一貫して実施されています。脅威インテリジェンスは活用されていますが、十分には最適化されておらず、隔離された復旧環境や完全なコンプライアンス対応には一部課題が残っています。

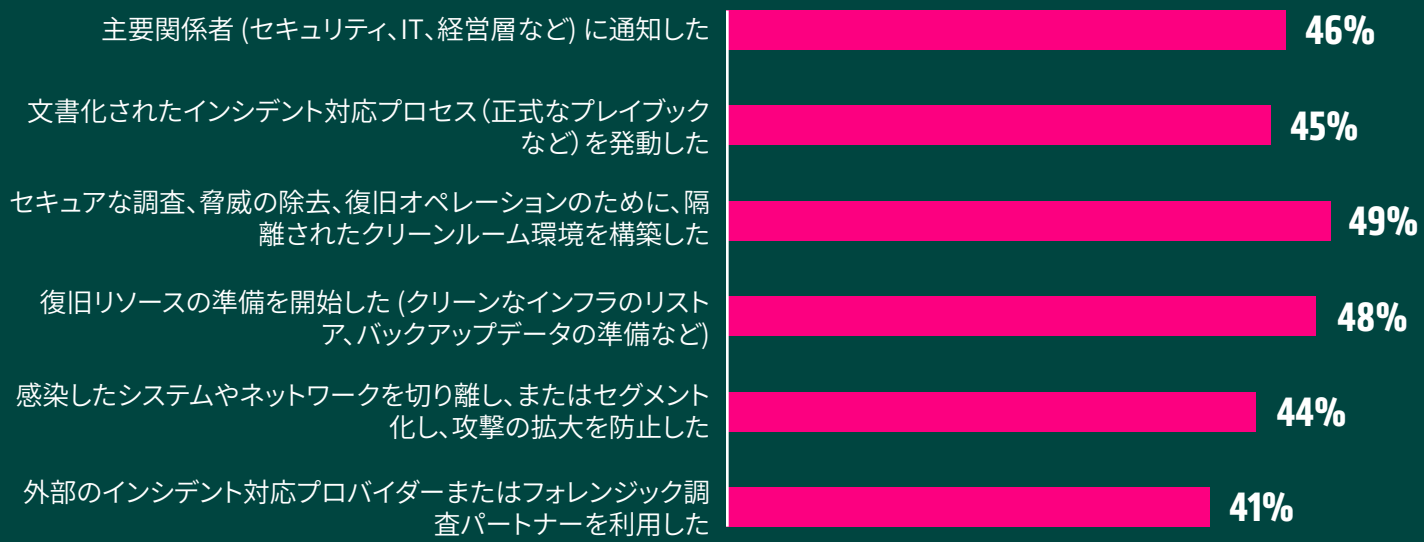
最も成熟している (5%): レジリエンスは組織全体で包括的に実施されています。機密データはグローバルにバックアップされ、MFAと管理者制御は標準的であり、脅威インテリジェンスは最大化され、復旧は是正を通じて保護され、コンプライアンス保護は一貫して遵守されています。

攻撃下におけるレジリエンス

攻撃を特定する方法

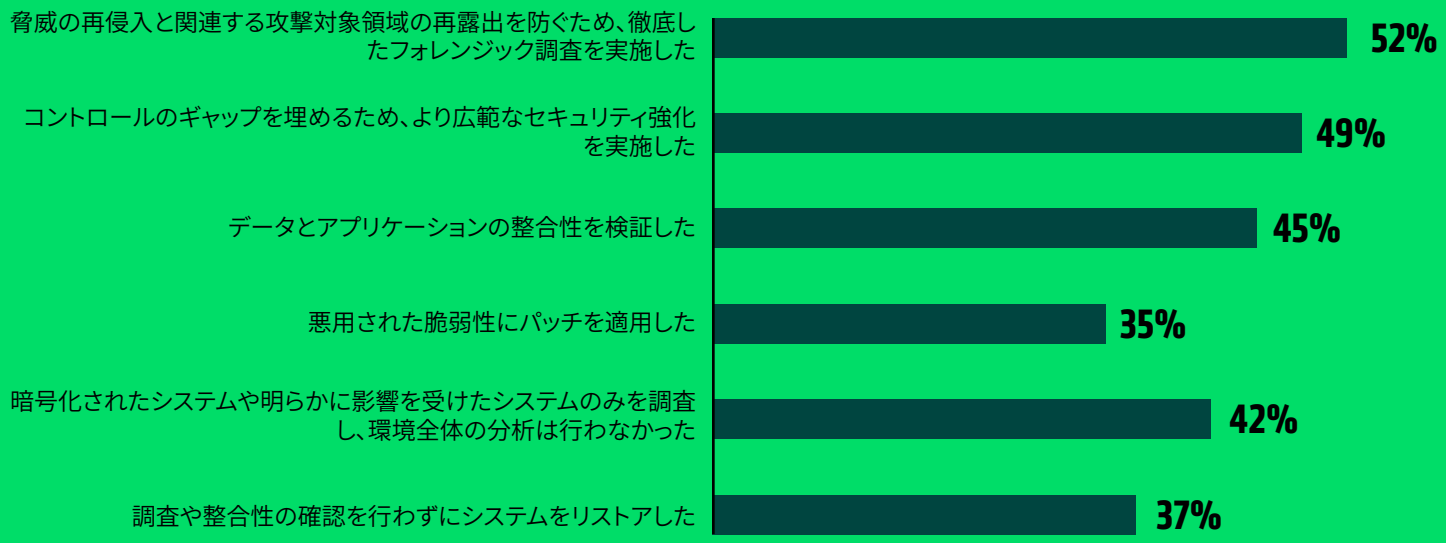
サイバー攻撃の際、大多数の中規模組織は内部でインシデントを検知し、ほとんどのケースがセキュリティツールによって自動的に特定・確認されています。その他の多くはツールでフラグ付けされるものの、手動での検証が必要です。従業員や外部関係者が報告するインシデントは、はるかに少なくなります。検知は主にツール主導ですが、人間による検証は依然として重要な役割を果たしています。

攻撃確認後の行動



攻撃を確認した後、中規模組織は脅威を封じ込め、復旧を開始するためにさまざまな措置を講じました。同様の割合の組織が、復旧リソースの準備を開始し、隔離されたクリーンルーム環境を構築し、主要関係者に通知し、感染したシステムを切り離し、対応手順を発動しました。外部のインシデント対応パートナーを利用した組織は、やや少数に留まりました。これらのパターンから、対応措置が幅広く採用されているものの、重要なアクション全体において、依然として完全に標準化されていないことがわかります。

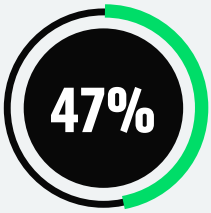
システムとデータの再稼働前に講じる手順



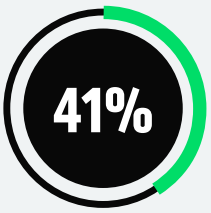
システムとデータの再稼働前に、中規模組織はフォレンジック調査と修復作業の組み合わせを採用しました。約半数が完全なフォレンジック調査やより広範なセキュリティ改善を実施したり、データとアプリケーションの整合性を検証したりした一方で、同程度の割合の組織は、明らかに影響を受けたシステムのみに焦点を当てていました。同じような割合の組織が、悪用された脆弱性に対するパッチ適用を行ったり、調査や整合性確認を行わずにシステムをリストアしました。これらのギャップは再感染や残存リスクを高める可能性があります。

攻撃対応中に直面した課題

重要システム (メール、コラボレーション用アプリ、チケット管理など) のダウンにより、チーム内でのコミュニケーションや連携が不可能になった

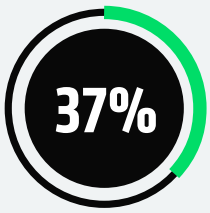


攻撃が是正される前にシステムをリストアするよう、経営層から圧力を受けた



セキュリティツールが回避され、バックアップが攻撃された

復旧したものの、脅威が完全に除去されていないために再感染した



検証済みのクリーンな復旧ポイントにアクセスできなかった

攻撃中、チームは運用上および技術的な大きな課題に直面しました。約半数のチームは、システムがオフラインの間のコミュニケーションに苦慮し、修復が完了する前にシステム復旧を求められるプレッシャーを感じていました。また、セキュリティツールの回避、バックアップへの攻撃、復旧後の再感染、クリーンな復旧ポイントへのアクセス不足なども報告されています。これらの課題は、準備不足によって対応が複雑になったり、障害が長期化する可能性を示しています。

レジリエンスへの投資が依然として不十分な領域

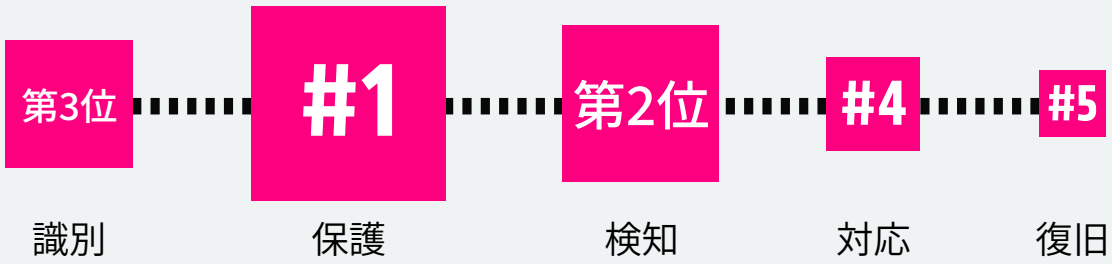
十分に準備された組織であっても、攻撃が発生するとレジリエンスを維持することは容易ではありません。運用上の圧力が高まる中、連携の不備、不完全な復旧対応、再感染のリスクが顕在化し、統一されたプロセスや継続的な保証がなければ、復旧がいかに脆弱になり得るかが明らかになります。

こうしたパターンは、中規模組織が現在どのようにサイバーレジリエンスの予算を配分しているかを反映しています。本調査では、回答者に対し、NISTサイバーセキュリティ フレームワークの5つの主要機能（識別、保護、検知、対応、復旧）に対して、支出をどのように配分しているかを尋ねました。

その結果、多くの組織は依然として予防・保護・検知に多くの投資を行っている一方で、対応や検証済みの復旧に対する資金は比較的少ないことが分かりました。その結果、成熟度の傾向は依然としてリストアよりも防御に偏っており、最も重要な局面である攻撃後におけるレジリエンスを強化するという、未活用の機会が浮き彫りになっています。

NISTサイバーセキュリティフレームワーク

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。



レジリエンスを加速・強化する要素としてのAIと自動化

調査結果からは、特に検知速度の向上や対応精度の強化において、中規模組織がAIをサイバーレジリエンス向上の強力な推進要因と位置付けていることも明らかになりました。ほぼすべての回答者が、異常検知、ユーザー行動分析、AIによる脅威調査・対応といったツールを、セキュリティ体制の強化に有効であると評価しています。

さらに、自然言語での脅威検索や文脈分析が可能な生成AIベースのアシスタントも、意思決定の簡素化・迅速化の手段として導入が進んでいます。中規模組織の56%は、サイバー攻撃後に得られた主要な教訓の一つとして、検知・対応・復旧の各段階における自動化の強化の必要性を挙げています。これは、AIを中核とした統合型自動化・オーケストレーションプラットフォームへの需要が高まっていることを示しており、AIがこれらのプロセスにおける効率性・一貫性・有効性を向上させる増幅要因として機能していることを示しています。

将来に向けた見通しでは、多くの組織が2026年末までにAIがサイバー防御において一層戦略的な役割を果たすと見込んでいます。56%の組織は、AIが人間の意思決定を支援し、分析や提言の精度を向上させる一方で、最終判断は人間が行う形になると見込んでいます。37%の組織は、AIが検知と対応の中核を担い、一部の判断を自律的に行うようになると見込んでいます。これは明確な方向性を示しています。AIは単なる支援ツールから、サイバーレジリエンスの運用基盤へと進化しており、検知、対応、復旧の各段階において、スピード、精度、確信を向上させる役割を果たすことが見込まれます。

今始まるレジリエンスの未来

中規模組織はサイバーレジリエンスの向上において着実な進展を遂げつつあるものの、攻撃後の対応力、復旧力、そして備えの検証に関しては、依然として改善の余地があります。サイバーレジリエンスは、大きな競争優位性をもたらします。復旧の迅速化、顧客の信頼維持、そして他が稼働できない時の事業継続を実現するために、人、モノ、プロセスに投資する組織こそが、未来を切り拓きます。混乱が避けられない時代において、レジリエンスは単なる保護ではなく、組織の実行力なのです。

危機が訪れる前に、以下の対応でレジリエンスを構築することができます。

- 中規模組織向けCohesityのサイバーレジリエンスソリューションについて学ぶ
- このレジリエンススコアカードであなたの組織のサイバーレジリエンス成熟度を評価
- 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

方法論

COHESITY

Cohesityは、2025年9月にVanson Bourne社に委託し、IT・セキュリティ分野の意思決定者3,200名を対象に調査を行いました。本レポートはその結果に基づいています。調査対象は、米国 (500)、ブラジル (200)、英国 (400)、ドイツ (400)、フランス (400)、アラブ首長国連邦/サウジアラビア (100)、オーストラリア (200)、韓国 (200)、日本 (400)、インド (200)、シンガポール (200) の組織です。対象となった組織はいずれも従業員1,000名以上で、金融サービス、公共部門、医療分野を中心に、公共・民間を問わず幅広い業種が含まれています。

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000049-001-JP 7-2026