COHESITY

サイバーレジリエンスレポート

リスクに備えるか、晒されるか: 医療機関におけるサイバーレジリエンスの格差

2026年4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。

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、Cohesityは11か国のITおよび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、医療機関からの371名の参加者が含まれていました。調査結果は、迅速かつ自信を持って復旧できるリスクへの備えが整った医療機関と、長期的な混乱や二次的な財務的損失に対して脆弱なままの医療機関との間で、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、日本において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。多くの医療機関は、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、医療機関にとってもはや例外的な出来事ではありません。

85%

回答者の85% が、少なくとも1回の重大なサイバー攻撃を経験しています。

66%

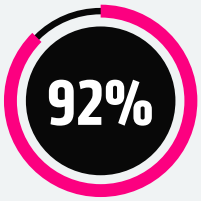
が、過去12か月以内に1回経験

35%

過去12か月間に複数回の重大なサイバー攻撃を経験

重大なサイバー攻撃がもたらす実際のコスト

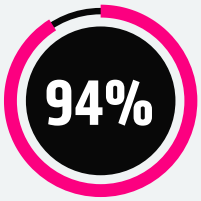
調査対象となった医療機関全体で、財務面および規制面での圧力が共通して見られました：



が収益の減少があったと回答

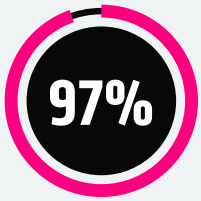
上場している医療機関の 80% が、業績見通しの修正を行ったと回答[1]

が顧客を失ったと回答



が身代金を支払い（1件あたりの平均額は 130万米ドル）

非公開の医療機関の 80% が、成長施策向けの予算を他用途に再配分



が法的または規制上の影響に直面（規制当局による罰金：54%、訴訟または集団訴訟：39%）

[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らがない自信

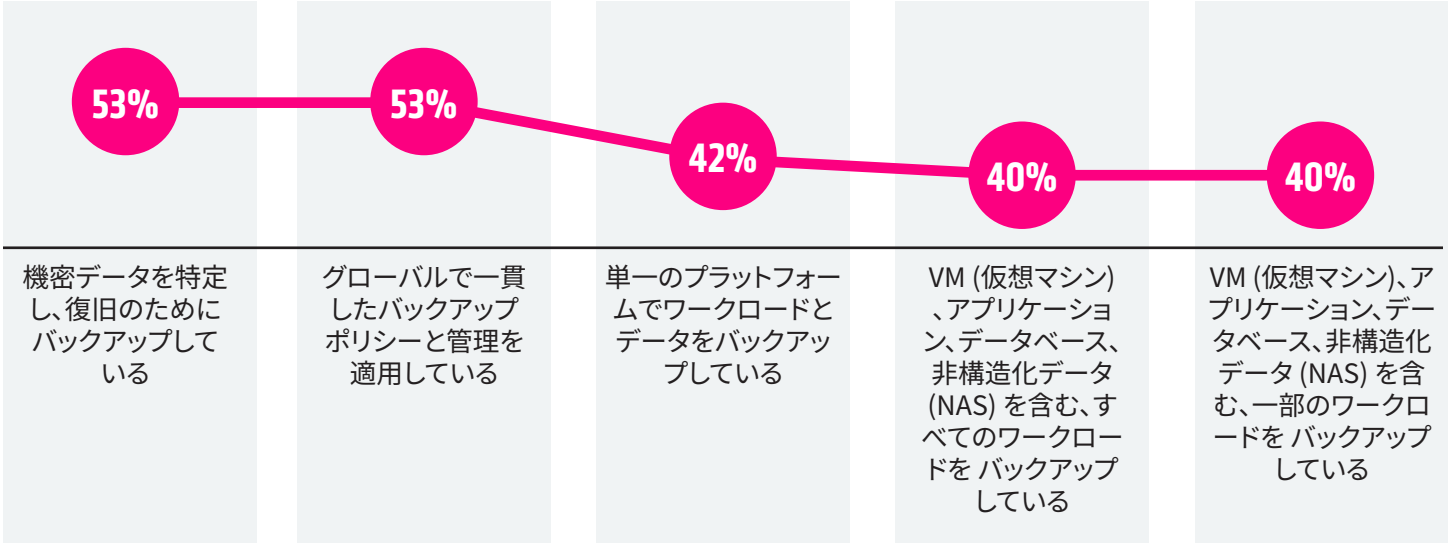
本調査で明らかになった財務面および業務面への影響の大きさを考えれば、組織のレジリエンスに対する懸念が広がっていることが想定されます。しかし、回答者のほぼ半数 (49%) は、所属組織のサイバーレジリエンス戦略が現在の脅威に耐え得ると回答し、高い自信を示しました。この高い自信は、当の組織の多くが実際に被ってきた重大な影響と、鮮明な対照をなしています。

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、あなたの組織では以下のうちどの対応を実施していますか?



医療機関の半数強が、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。同じ割合で、バックアップポリシーを世界全体で一貫して適用しています。しかし、すべてのワークロードをバックアップしている組織や、単一のプラットフォームに依存している組織は半数未満です。3分の1を超える組織は、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

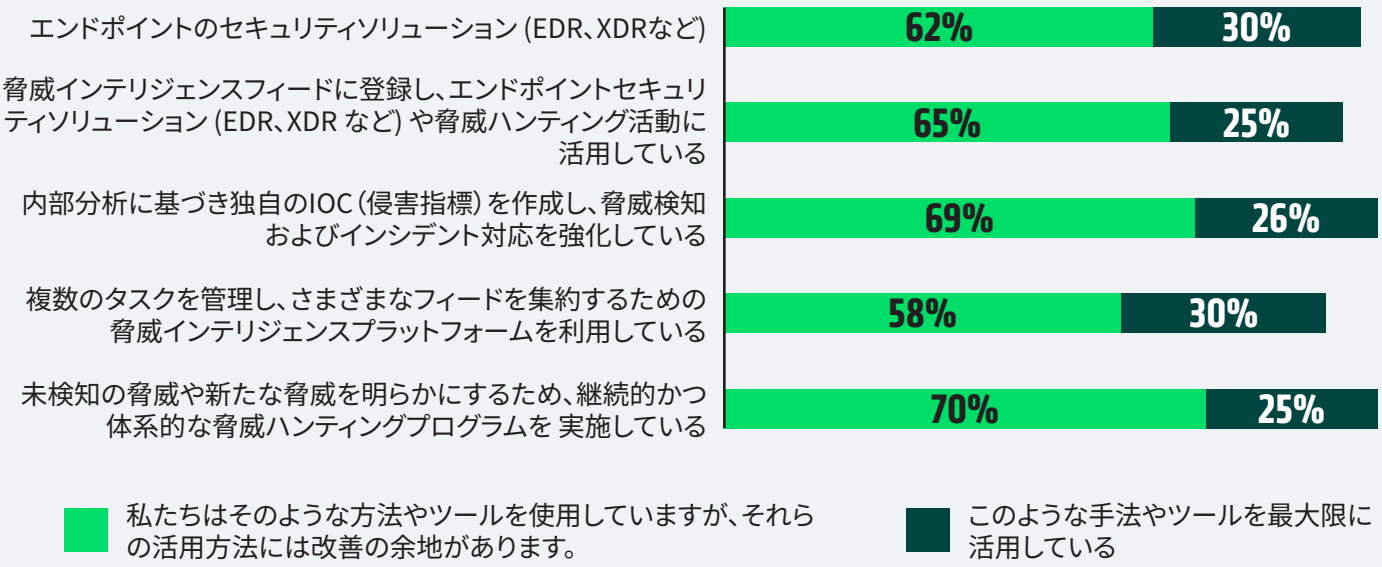
データを常に復旧可能な状態に保つために、あなたの組織ではどのような対策を講じていますか?

60%	バックアップと復旧ソリューションに関連するリスクの高い管理者タスクに対して、追加の認可を要求している
48%	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
44%	「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、うち1つ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
35%	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

多くの医療機関が、バックアップ環境に対するアクセス制御を強化しています, 10社中6社は、高リスク作業の実行に追加の管理者承認を必要としています。多要素認証 (MFA) を徹底している組織、3-2-1バックアップルールを遵守している組織、重要データをイミュータビリティで保護している組織は、いずれも半数未満にとどまっています。最小権限アクセスを適用している組織は、約3分の1に過ぎません。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

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?



脅威の検知・調査ツール自体は広く導入されていますが、その活用度には依然として大きなばらつきがあります。多くの医療機関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、体系的な脅威ハンティングプログラムを利用しているものの、これらを十分に活用できている組織はごく一部に留まっています。侵害指標 (IOC) のカスタム設定や、脅威インテリジェンスプラットフォームなどの高度な機能も、依然として十分に活用されていません。成熟したサイバーレジリエンスは、こうした能力を統合し、可視性・検知・対応を継続的に向上させるインテリジェントなループを構築することによって実現されます。

再感染のリスクに晒される組織

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?

56% 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、年次でエンドツーエンドの模擬演習を実施している

54% 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

53% 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を保護されたオンラインリポジトリに 保管している

36% 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

36% 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

医療機関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、依然としてギャップが残っています。半数を超える組織が、システムを復旧する前にセキュリティコントロール上のギャップを特定し、年1回の復旧リハーサルを実施しています。また、同程度の割合の組織が、対応および復旧を支援するためのオンライン保管型リポジトリを維持しています。一方で、セキュアな調査と復旧のために隔離環境を利用している組織や、すべてのバックアップデータにイミュータビリティを適用している組織は、それより少数に留まっています。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リスクにさらされやすくなります。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ゾーンを組み合わせることで実現されます。

ータ分類は浸透しつつあるが、リスク主導の活用は依然として発展途上

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?

60%

サイバー攻撃発生時、影響を受けたデータに対するコンプライアンス上の義務を判断するため、バックアップデータの分類を 活用している

59%

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

53%

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

52%

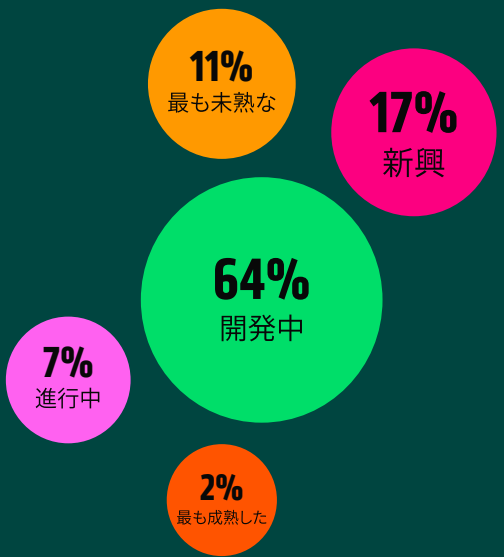
バックアップするシステムを特定し、優先順位を付けている

医療機関では、コンプライアンス、対応、復旧の各局面において、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。10社中6社が、攻撃発生時のコンプライアンス対応を導くためにデータ分類を活用しており、ほぼ同程度の組織がプライバシーおよびセキュリティ違反への対応にも分類を利用しています。一方で、インシデント発生前に重大性を定義している組織や、リスクに基づいてバックアップの優先順位を決定している組織は、それよりやや少なくなっています。これらのギャップは、分類情報をリスク主導で活用する取り組みが依然として発展途上にあることを示唆しています。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、日本の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2%にすぎません。

サイバーレジリエンスの成熟曲線



最も未成熟 (11%): 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、一貫性に欠けます。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 攻撃の重大性評価は大抵見過ごされています。

初期段階 (17%): 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。組織によっては 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。

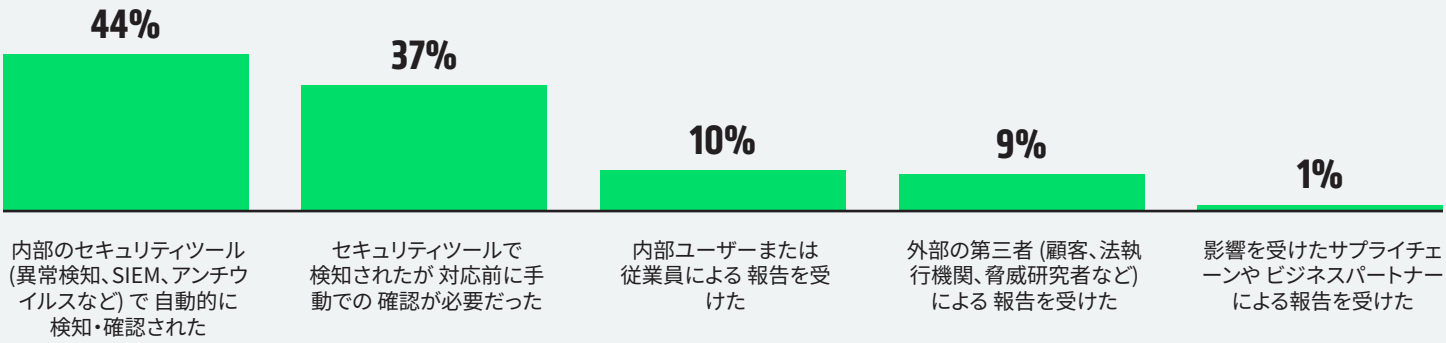
発展途上 (64%): バックアップ、管理者制御、脅威インテリジェンスなどの基本的な施策は 比較的一般的になっていますが、依然としてばらつきがあります。復旧環境の整備、コンプライアンスチェック、セキュリティギャップの 是正は断続的に行われており、レジリエンス施策は部分的にしか効果を発揮していません。

進展中 (7%): 主要な施策の多くが一貫して実施されており、グローバルなバックアップ ポリシー、管理者承認、復旧前の是正などが含まれます。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 (2%): レジリエンスは体系的かつ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や管理者制御は標準的に適用されています。脅威インテリジェンスは最大限に活用され、是正措置によって復旧のセキュリティが確保され、コンプライアンス上の安全策も一貫して遵守されています。

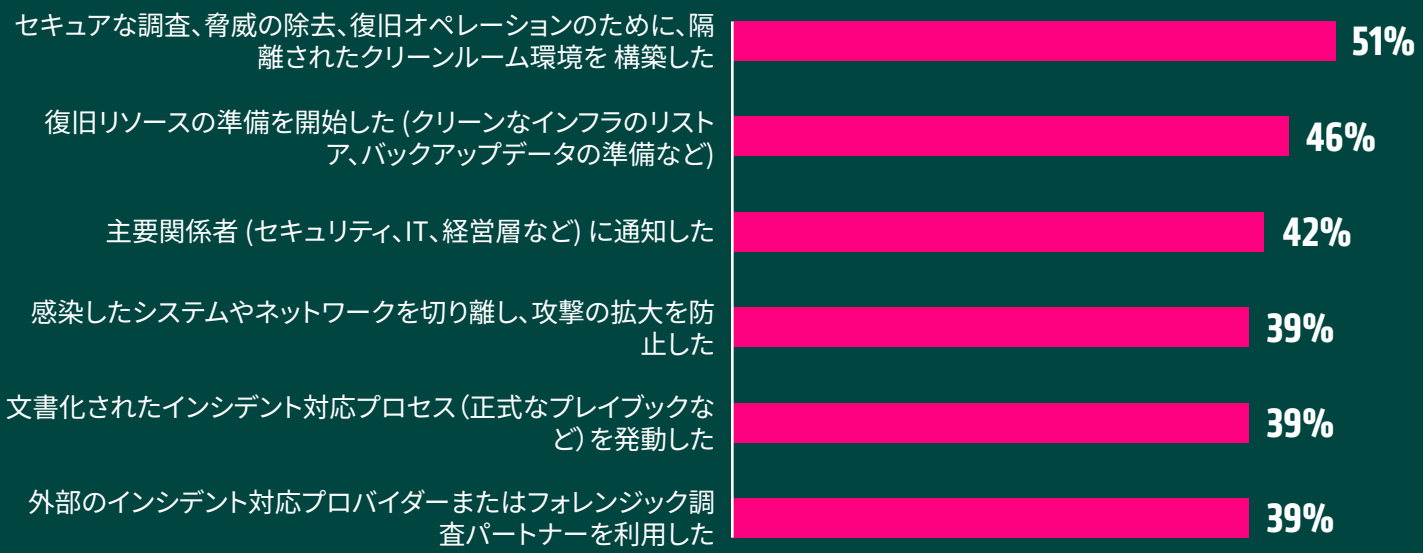
攻撃下におけるレジリエンス

攻撃を特定する方法



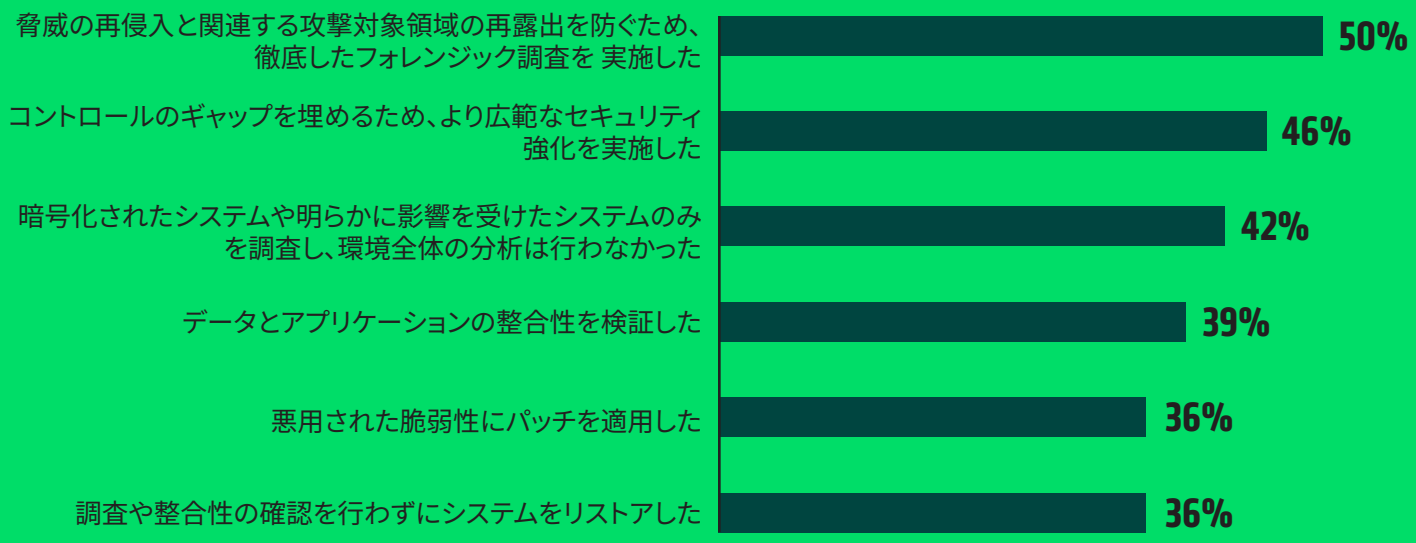
サイバー攻撃が発生した場合、医療機関のほぼ半数が、自社のセキュリティツールによって攻撃が自動的に検出・確認されたと回答しました。一方で、3分の1以上の組織では、ツールによって攻撃は検知されたが、対応を取る前に手作業による確認が必要だったと報告されています。第三者からのアラートは、はるかに少ない頻度でした。検知は主として内部で行われているものの、依然として人による確認に依存していることが伺えます。

攻撃確認後の行動



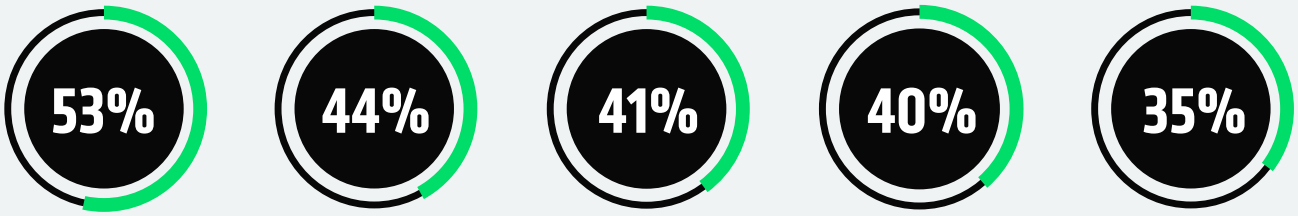
攻撃が確認された後、医療機関は復旧を支援するためにさまざまな対応を取りました。半数弱の組織が、クリーンなインフラの復元やバックアップデータのステージングを開始しました。半数を超える組織は、セキュアな調査と復旧のために隔離されたクリーンルーム環境を構築しました。約10社中4社は、主要な利害関係者に通知、感染したシステムの封じ込め、正式なインシデント対応プレイブックの発動、外部のインシデント対応またはフォレンジック専門家の関与といった対応を実施しました。これらの違いは、重要な対応プロセスにおいて、対応手順がまだ完全には標準化されていないことを示しています。

システムとデータの再稼働前に講じる手順



システムを再稼働させる前に、医療機関はフォレンジック調査と是正措置を組み合わせて実施していました。半数が完全なフォレンジック調査を実施し、半数弱がより広範なセキュリティ強化策を導入しました。一方で、データおよびアプリケーションの整合性の確認、悪用された脆弱性の修正、または目に見える影響範囲を超えた調査を行った組織は、それより少数に留まりました。さらに、3分の1を超える組織が、十分な調査や整合性の確認を行わないままシステムをリストアしており、再感染や残存リスクが生じる余地を残しています。

攻撃対応中に直面した課題



ローカライズチームは、プロセス全体を通じて重大な課題を報告しました。多くの組織が、重要なシステムが停止している状況下での連絡や連携に苦慮していました。半数近くの組織が、是正対応が完了する前に業務をリストアするよう圧力を受けたと回答しています。さらに、セキュリティツールの回避、再感染、クリーンな復旧ポイントの不足が困難を一層深刻化させており、より強固なレジリエンス対策の必要性が浮き彫りになっています。

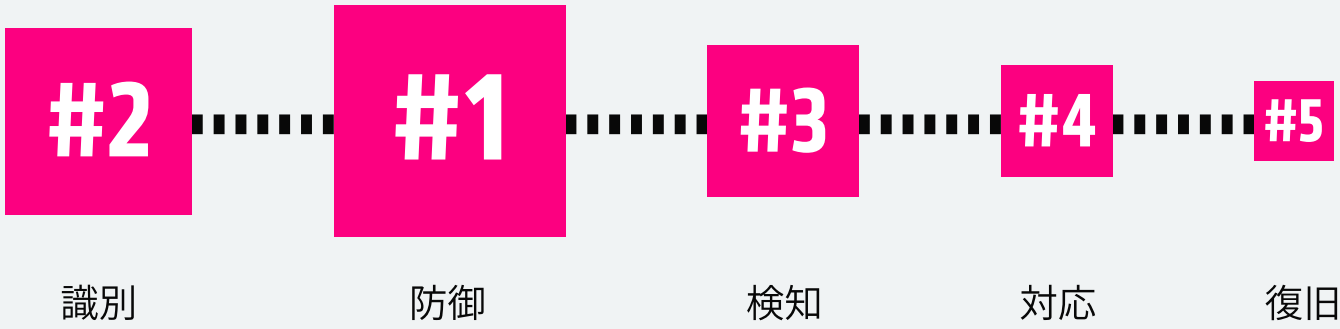
レジリエンスへの投資が依然として不十分な領域

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、医療機関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。

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。



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、日本の組織が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、自然言語での脅威クエリや文脈分析が可能な、より新しい生成AIベースのアシスタントも、意思決定を簡素化し加速させる手段として採用が進んでいます。医療機関の61%は、サイバー攻撃後に得られた最大の教訓の一つとして、検知・対応・復旧の各段階における自動化強化の必要性を挙げています。これは、統合型の自動化・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が効率性・一貫性・有効性を向上させる増幅要因として、これらのプロセス全体を支えていることを示しています。

将来を見据えると、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担うようになると多くの組織が予測しています。54%の組織は、AI が人間の意思決定を支援し、分析や推奨の精度を高めつつ、最終的な判断は人間が行う形になると見込んでいます。一方で、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予測しています。これは明確な方向性を示しています。AI は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、確信を高める役割を果たすことが期待されています。

今始まるレジリエンスの未来

医療機関はサイバーレジリエンスの強化において着実な進展を遂げていますが、攻撃後の対応、復旧、そして備えの検証については、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生み出す要素です。復旧を迅速化し、顧客の信頼を維持し、他の組織が対応できない状況でも事業を継続するために、人材、製品、プロセスへ投資する組織こそが、未来を切り拓くことができます。混乱がほぼ避けられない時代において、レジリエンスは単なる防御ではなく、組織の実行力そのものなのです。

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:

- ランサムウェアレジリエンスのワークショップを予約
- 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
- Cohesityのサイバーレジリエンスソリューションを詳しく確認

調査方法

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 (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

2000076-001-JP 4-2026