

COHE5ITY

# 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。そのうち390人は、金融サービス業の組織からの参加者でした。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金融サービス業の組織と、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。

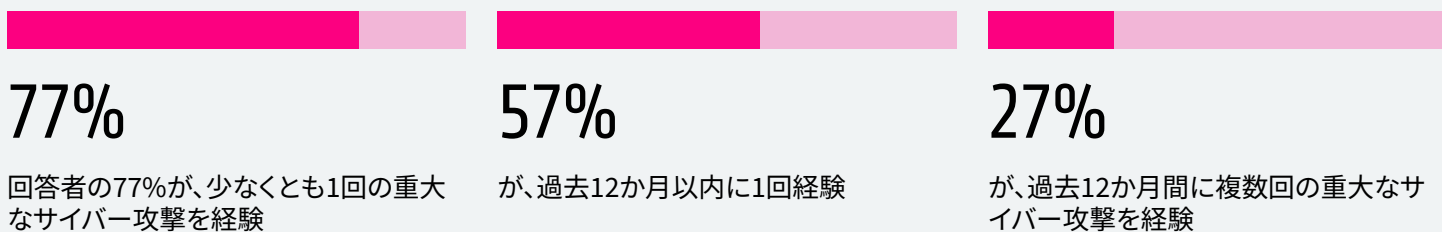
本調査では、実質的な影響を伴うサイバー攻撃がもたらした現実の影響に加え、各金融サービス業の組織がベストプラクティスに照らして自社のサイバーレジリエンスをどのように自己評価したか、また、こうしたインシデントを検知し、対応し、復旧するためにどのような取り組みを行ったのかを分析しています。さらに、そこから得られた教訓に加え、AIと自動化を活用してレジリエンスを加速させ、レジリエンスの分断を埋めようとする取り組みも浮き彫りにしています。



## 重大なサイバー攻撃： 現代ビジネスにおける新たな現実

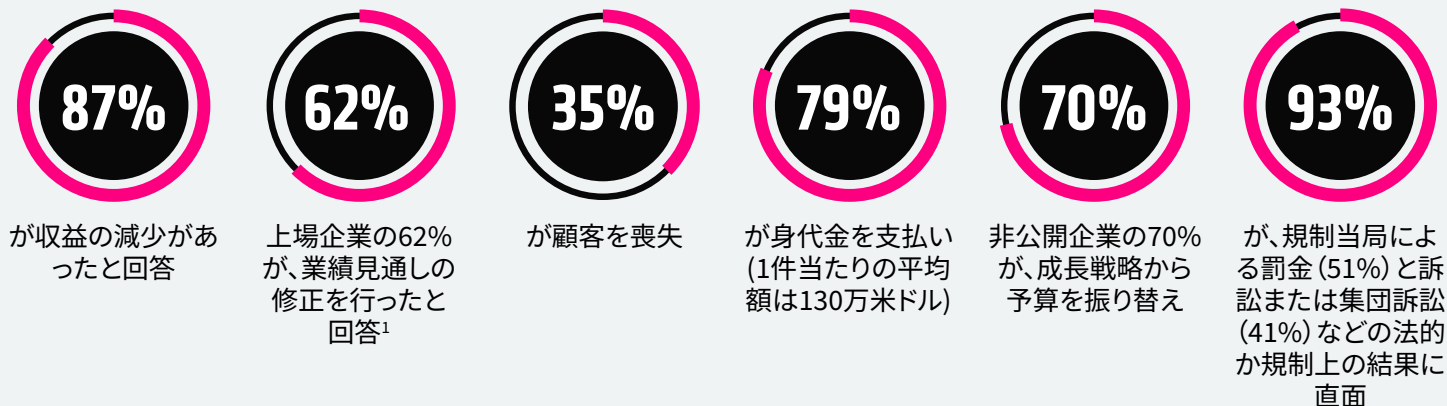
サイバーインシデントは一様ではありません。多くの金融サービス業の組織は、日常的に発生するフィッシング攻撃やマルウェアの探索（プローブ）、システム停止への対応を、ほぼ毎日のように行っています。しかし、重大なサイバー攻撃はそれとは異なります。本調査では、測定可能な財務、評判、運用への影響、または顧客離れを伴うインシデントを「重大なサイバー攻撃」と定義しています。

こうした影響の大きい攻撃は、金融サービス業の組織ではもはや例外的な出来事ではありません。



# 重大なサイバー攻撃がもたらす実際のコスト

調査対象金融サービス業の組織全体で、財務面および規制面での圧力が共通して見られました。



<sup>1</sup>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

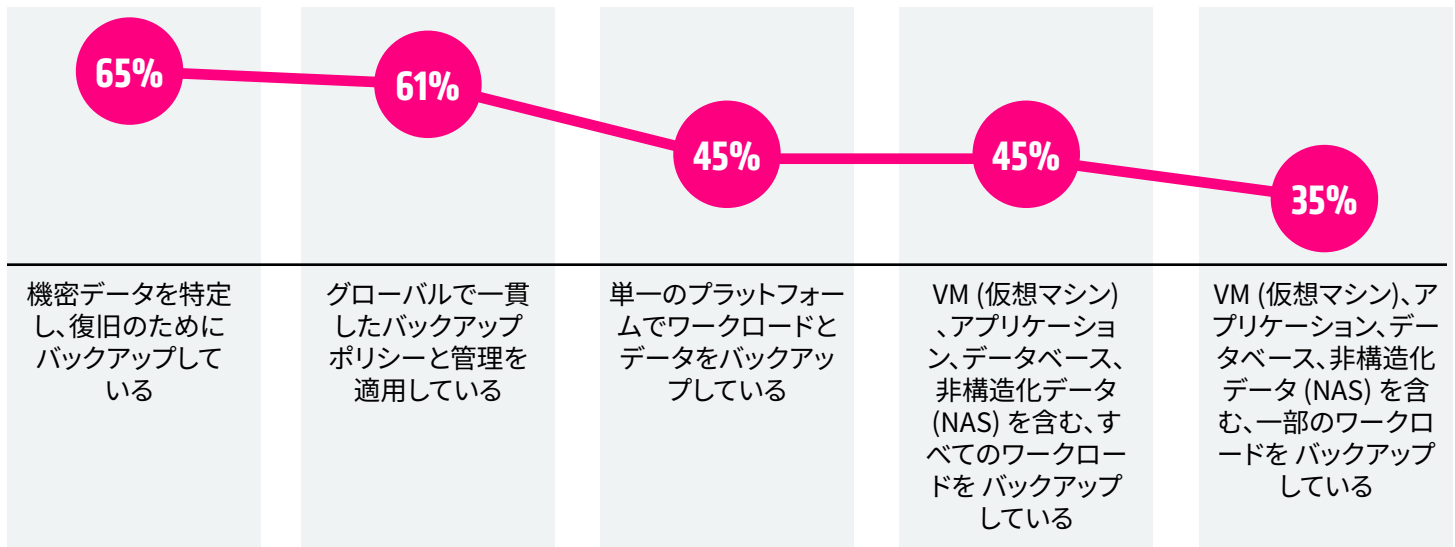
本調査で明らかになった財務面および業務面への影響の大きさを考えれば、組織のレジリエンスに対する懸念が広がっていることが想定されます。しかし、回答者のほぼ半数 (46%) は、所属組織のサイバーレジリエンス戦略が現在の脅威に耐え得ると回答し、高い自信を示しました。この高い自信は、当の組織の多くが実際に被ってきた重大な影響と、鮮明な対照をなしています。

## 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

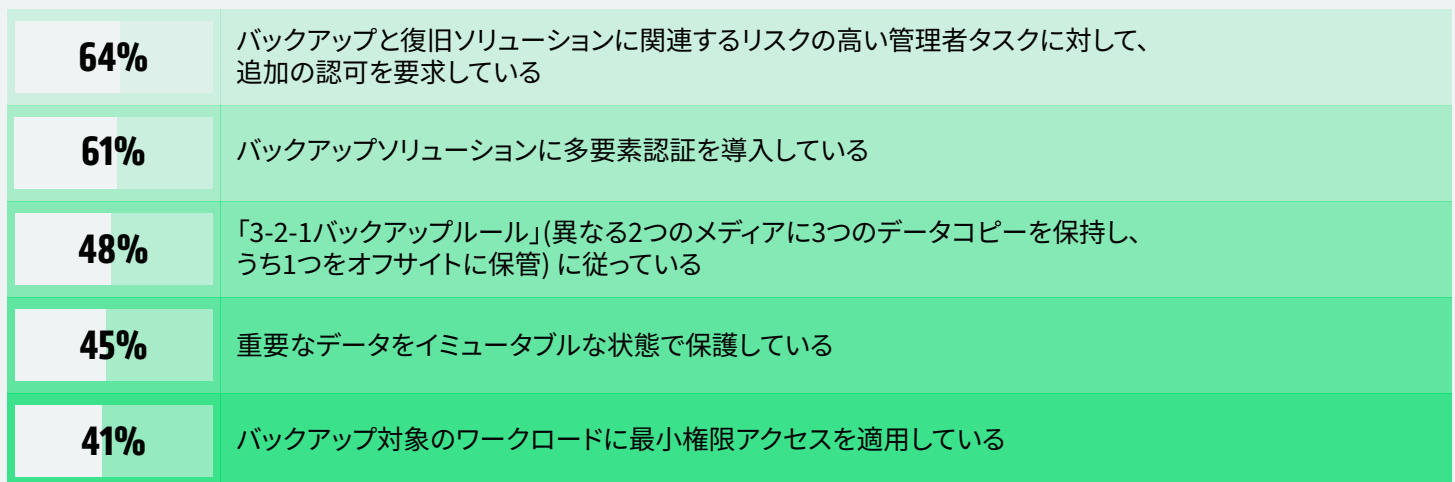
ハイブリッド/マルチクラウド環境全体のデータを保護するために、あなたの組織では以下のうちのどの対応を実施していますか？



金融サービス業の組織の約3分の2が、機密データを特定し復旧に備えてバックアップを確保していますが、グローバルで一貫したバックアップポリシーを適用する割合はやや低くなっています。すべてのワークロードをバックアップしている組織や、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。約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

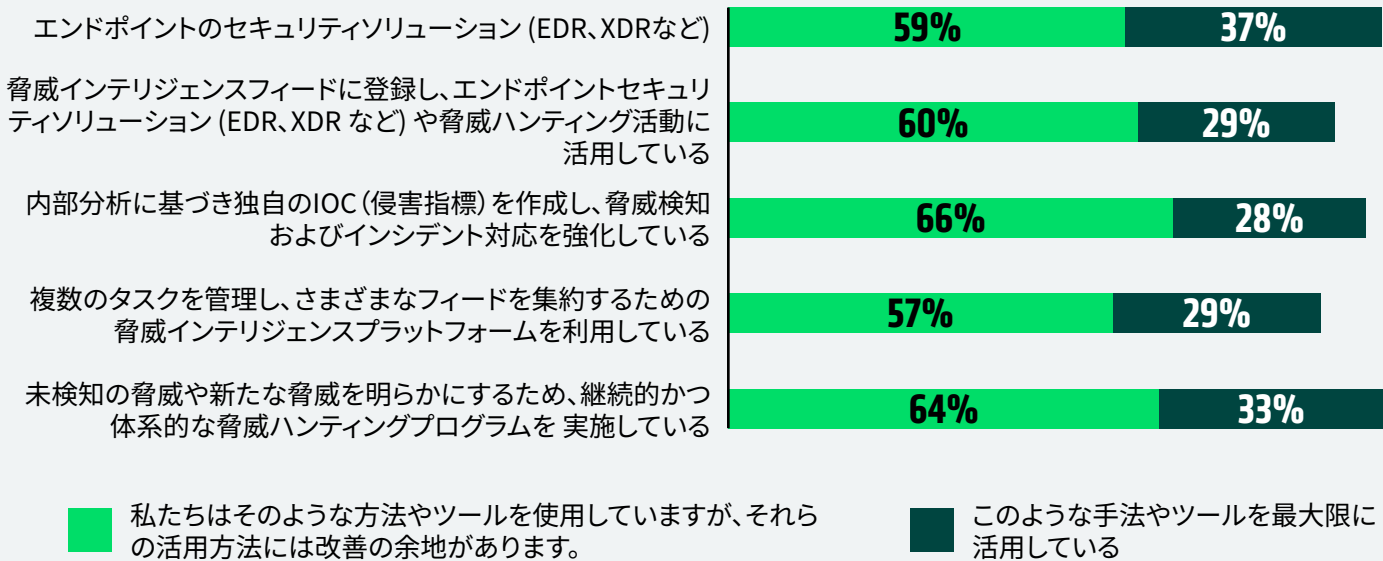
データを常に復旧可能な状態に保つために、あなたの組織ではどのような対策を講じていますか？



多くの金融サービス業の組織は、バックアップ環境に関するアクセス制御を強化しており、約3分の2が高リスクなタスクに対して追加の管理者承認を求め、半数強が多要素認証を適用しています。半数近くが3-2-1バックアップルールに従い、半数弱がイミュータビリティによって重要なデータを保護しているが、最小権限のアクセス権を適用している割合は少なくなっています。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

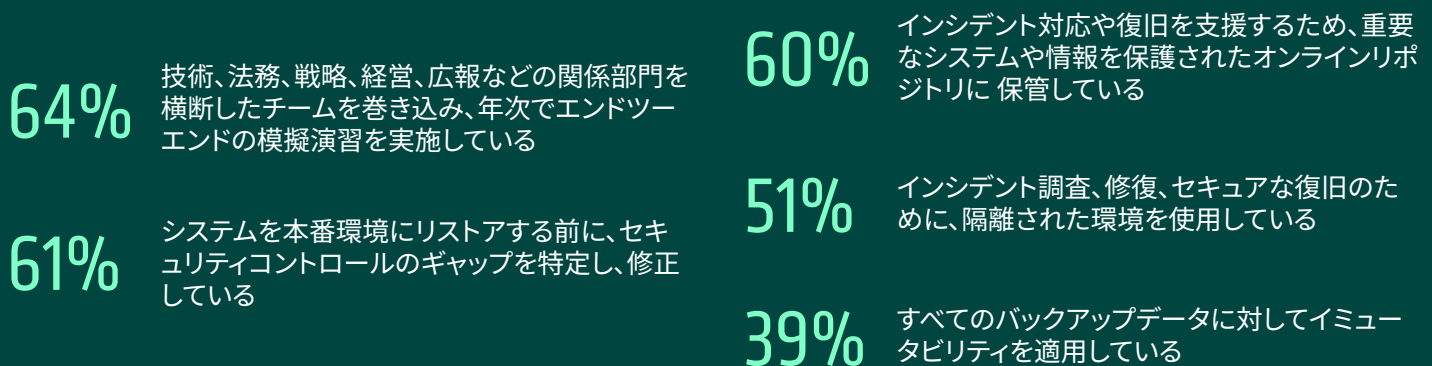
脅威の検知や調査に、以下の手法やツールをどのくらい活用していますか？



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。ほとんどの金融サービス業の組織は、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、構造化された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ないです。侵害指標 (IOC) のカスタム設定と、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は、依然として十分に導入されていません。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。

## 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？



金融サービス業の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。半数を超える組織は、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ている一方で、約3分の2が年1回の復旧リハーサルを実施しています。約6割がオンラインの保管庫 (ボルト) リポジトリを維持しており、半数強が隔離された環境を使用して安全な調査と復旧を行っています。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割合は半数未満です。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。

# デ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？



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



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



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



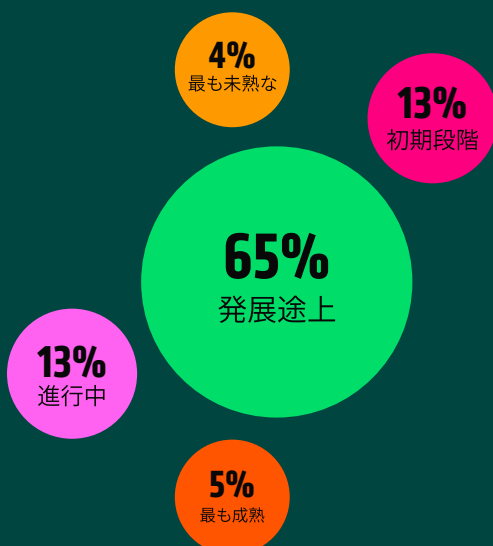
バックアップするシステムを特定し、優先順位を付けている

金融サービス業の組織では、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戦略的に活用する動きが広がっています。約3分の2が、攻撃中にプライバシー違反およびセキュリティ違反に対処して、コンプライアンスの指針となる分類を使用していますが、インシデントの前にリスクに基づいて重大度を定義するか、バックアップを優先する組織の割合はそれより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、金融サービス業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き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



**最も未成熟 (4%):** 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 (13%):** 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。

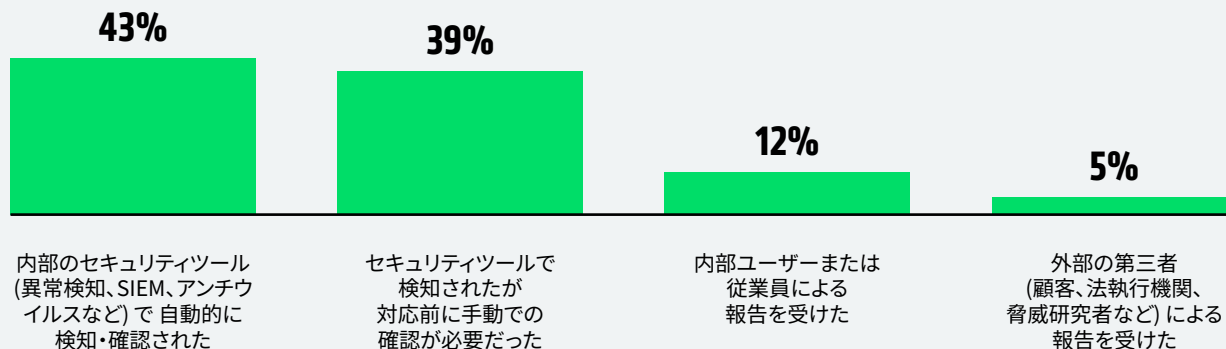
**発展途上 (65%):** バックアップ、管理者制御、脅威インテリジェンスなどの基本的な施策は比較的一般的になっていますが、依然としてばらつきがあります。復旧環境の整備、コンプライアンスチェック、セキュリティギャップの是正は断続的に行われており、レジリエンス施策は部分的にしか効果を発揮していません。

**進捗中 (13%):** 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 (5%):** 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。

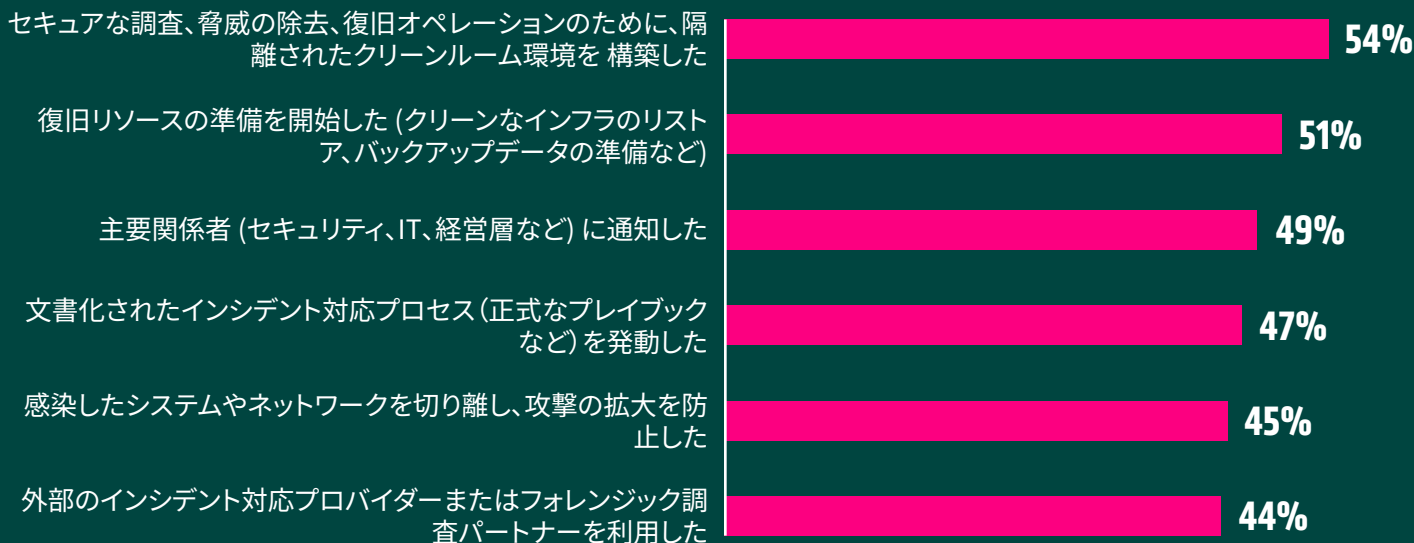
# 攻撃下におけるレジリエンス

## 攻撃を特定する方法



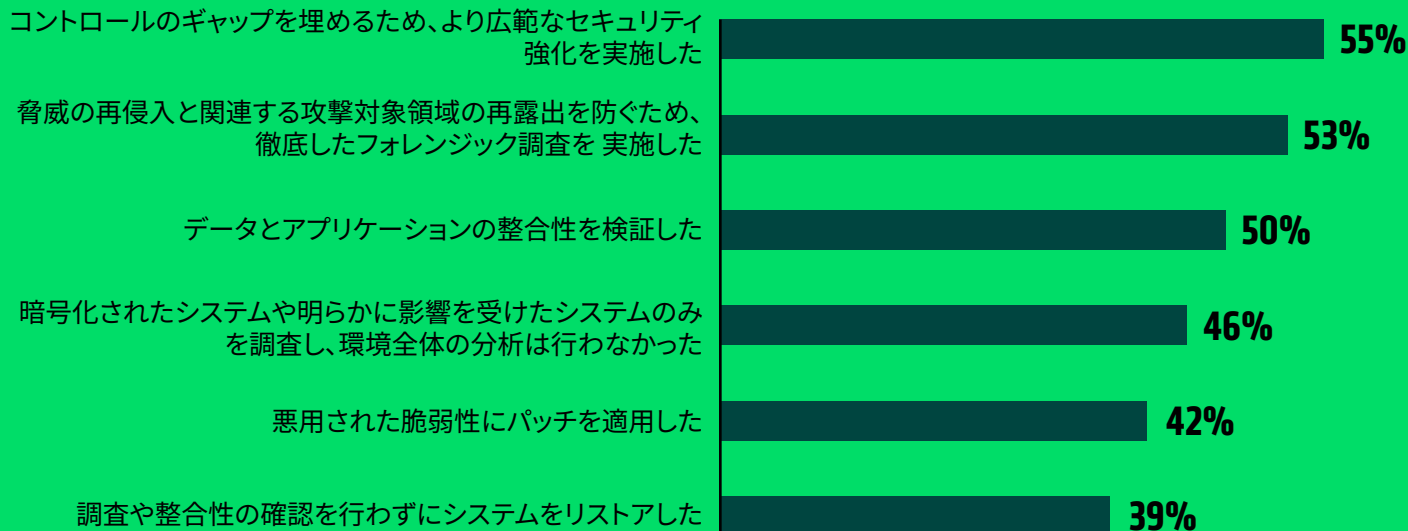
サイバー攻撃発生時、多くの金融サービス業の組織はインシデントを内部で検知しています。ほぼ半数の組織は、内部のセキュリティツールで攻撃を自動的に検知・確認したと回答する一方で、ツールによって攻撃が検知されたものの、対応前に手動で検証する必要があったと回答した組織は、これよりやや少数に留まりました。第三者によって特定されたのはごく一部であり、検知は主に内部的で行われていますが、依然として人間による確認に依存していることが示されています。

## 攻撃確認後の行動



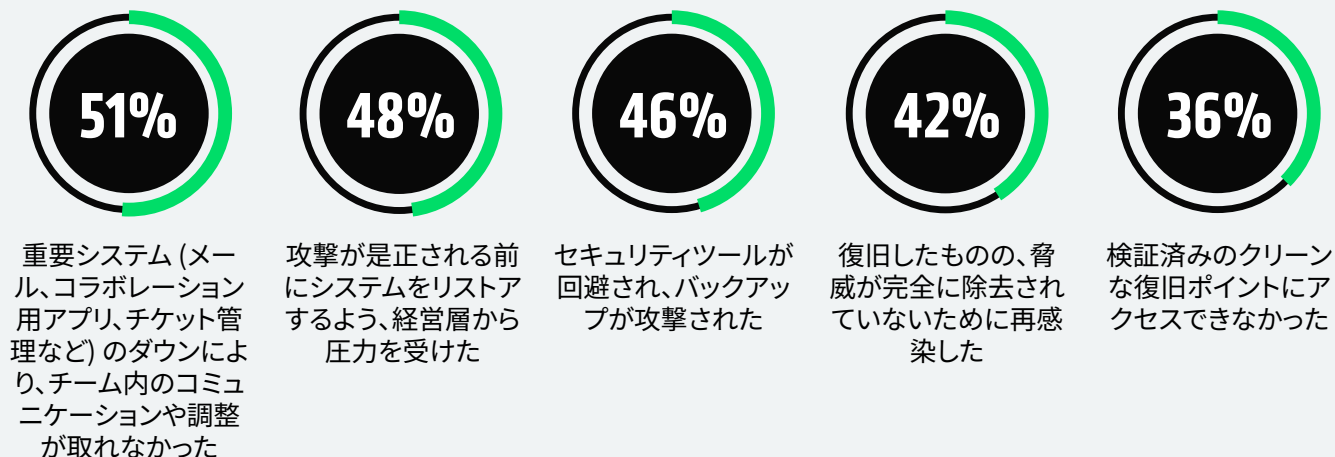
攻撃が確認された後、金融サービス業の組織は復旧を支援するためにさまざまな対応を取りました。半数強は、クリーンなインフラストラクチャの復旧かバックアップデータのステージングを開始した一方、これをわずかに上回る割合が、安全な調査と復旧のために隔離されたクリーンルーム環境を確立しました。それより少ない割合は、主要な利害関係者に通知、感染したシステムの封じ込め、正式なインシデント対応プレイブックの発動、外部のインシデント対応またはフォレンジック専門家の関与といった対応を実施しました。これらの違いは、重要な対応プロセスにおいて、対応手順がまだ完全には標準化されていないことを示しています。

## 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、金融サービス業の組織はフォレンジック調査と是正措置を組み合わせ実施していました。半数以上は、より広範なセキュリティ強化策や完全なフォレンジック調査を実施しました。また、半数は、データとアプリケーションの整合性の検証を行いました。目に見える影響を受けたシステムの範囲を超えた調査を行うか、悪用された脆弱性を修正した組織は、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



対応プロセス全体を通じて、チームは多くの課題に直面しました。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。

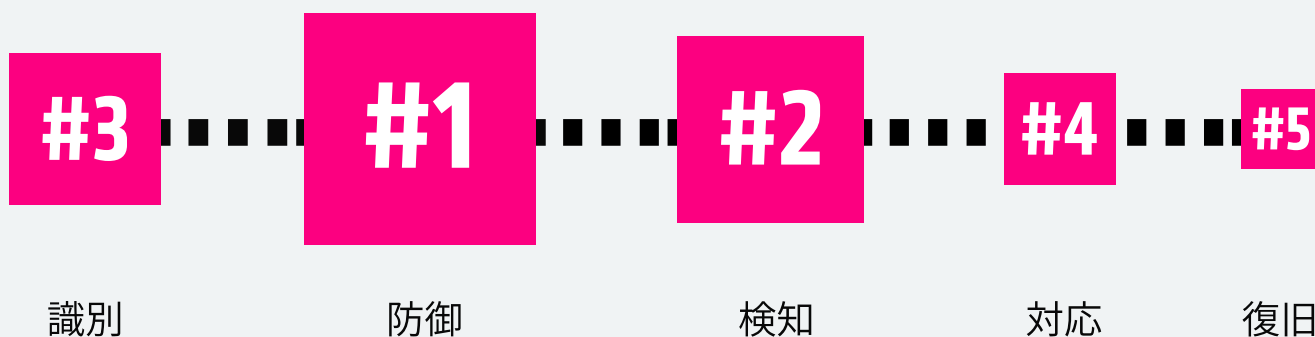
# レジリエンスへの投資が依然として不十分な領域

十分に準備された金融サービス業の組織であっても、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、復旧がいかにか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、金融サービス業の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、金融サービス業の組織が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。金融サービス業の組織の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ことを見込んでいます。49%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。39%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ことを見込んでいます。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

金融サービス業の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：

- [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の金融サービス業向け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/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。



© 2026 Cohesity, Inc. 著作権所有。

Cohesity、Cohesityのロゴおよびその他のCohesityのマークは、米国および/または国際的にCohesity, Inc.またはその関連会社の商標です。その他の名前は、それぞれの所有者の商標である場合があります。本資料は (a) Cohesityおよび当社の事業・製品に関する情報を提供することを目的としており、(b) 作成時点で事実であり正確と考えられているものの、事前通知なしに変更される可能性があり、(c) 「現状のまま」提供されます。Cohesityはあらゆる明示的または黙示的な条件、表明、あらゆる種類の保証を否認します。

## COHESITY

[cohesity.com](https://cohesity.com)

1-855-926-4374

2625 Augustine Drive, Santa Clara, CA 95054

2000086-001-JP 5-2026