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: 日本におけるサイバーレジリエンスの格差

2026年2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は日本全国のIT・セキュリティ運用の意思決定者400名を対象に調査を実施しました。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組織と、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、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、日本ではもはや例外的な出来事ではありません。

64%

日本の組織の64%が、少なくとも1回の重大なサイバー攻撃を経験

45%

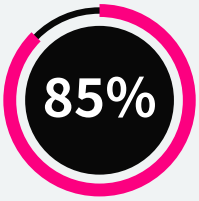
が、過去12か月以内に1回経験

23%

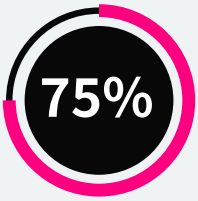
が、過去12か月間に複数回の重大なサイバー攻撃を経験

重大なサイバー攻撃がもたらす実際のコスト

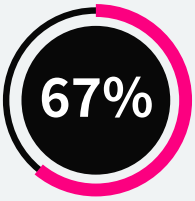
調査対象組織全体で、財務面および規制面での圧力が共通して見られました:



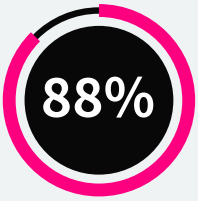
が収益の減少があったと回答



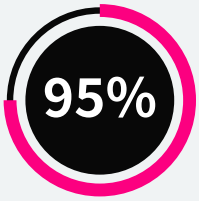
日本の上場企業の75%が、業績見通しの修正を行ったと回答1



日本の非上場企業の67%が、成長投資向けの予算を他の用途へ振り替え



が身代金を支払い(1件当たりの平均額は170万米ドル)



が法的または規制上の影響に直面 (金銭的制裁 (42%) や民事訴訟または規制当局による手続き (37%)など)

[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

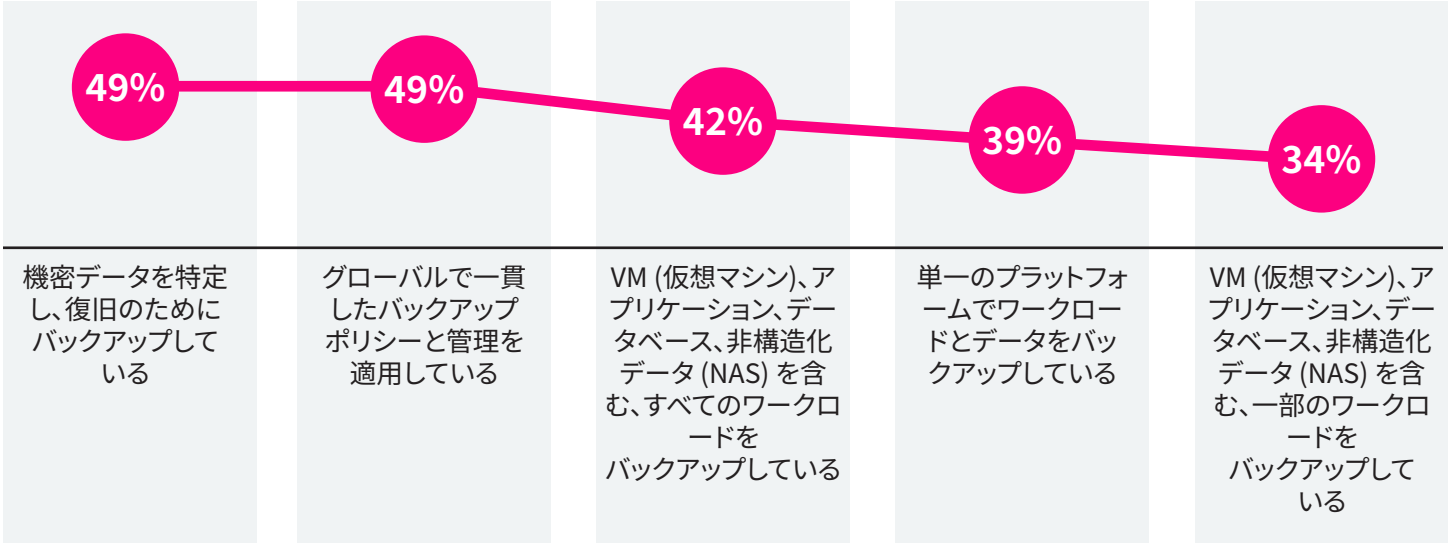
本調査で明らかになった財務面および業務面への影響の大きさを考えれば、組織のレジリエンスに対する懸念が広がっていることが想定されます。しかし、回答者のほぼ半数 (42%) は、所属組織のサイバーレジリエンス戦略が現在の脅威に耐え得ると回答し、高い自信を示しました。この高い自信は、当の組織の多くが実際に被ってきた重大な影響と、鮮明な対照をなしています。

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?



日本の組織のおよそ半数は、機密データを特定し、復旧のためにバックアップを取得するとともに、グローバルで一貫したバックアップポリシーを適用していると回答しています。一方で、すべてのワークロードをバックアップしている組織は42%に留まり、単一のプラットフォームに依存している組織は4割未満 (39%) でした。また、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るのが実情です。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

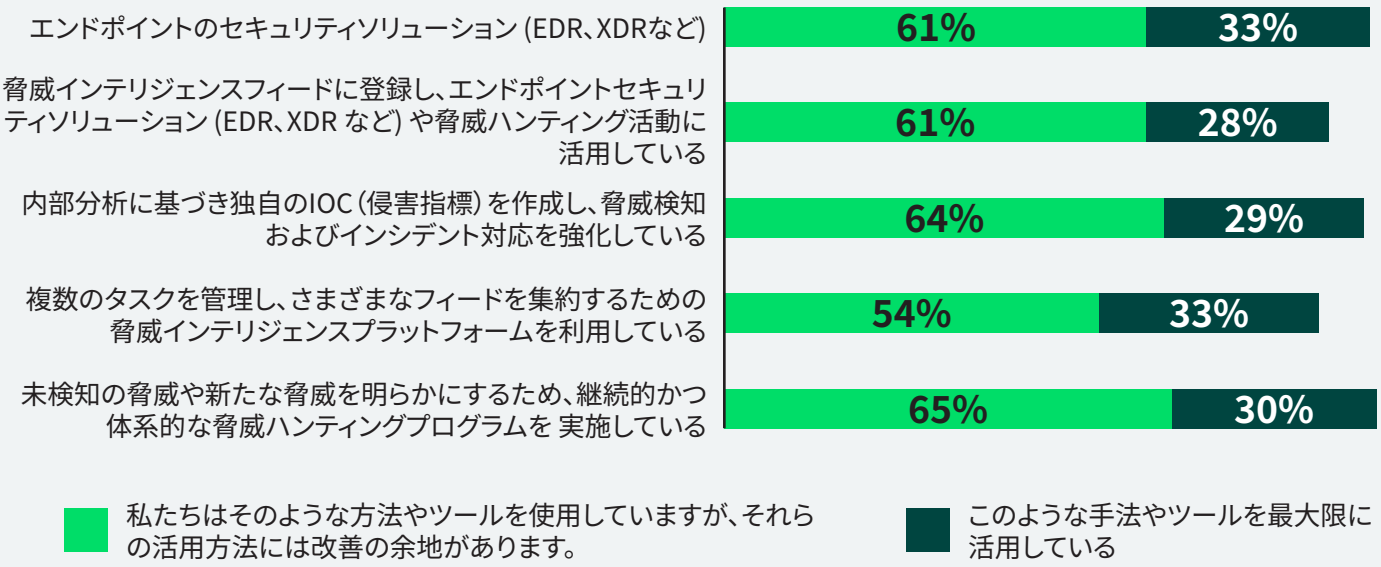
データを常に復旧可能な状態に保つために、あなたの組織ではどのような対策を講じていますか?

52%	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
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、うち1つをオフサイトに保管) に従っている
43%	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
43%	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

日本の多くの組織では、バックアップ環境へのアクセス制御を強化しており、高リスクな操作には追加の管理者認可を必要とする組織は過半数 (52%) に上ります。一方で、多要素認証 (MFA) を強制している組織は43%、3-2-1のバックアップルールを遵守している組織も約半数 (47%) に留まります。さらに、重要データをイミュータブル形式で保護している組織は43%、最小権限のアクセス権を適用している組織は38%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

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、その活用度には大きなばらつきがあります。エンドポイントのセキュリティソリューション (33%) や脅威インテリジェンスプラットフォーム (33%) を最大限に活用している組織は3分の1に留まり、脅威インテリジェンスフィード (28%)、カスタム侵害指標 (IOC)(29%)、体系的な脅威ハンティングプログラム (30%) を十分に活用している組織は、さらに少数に留まります。成熟したサイバーレジリエンスは、これらの能力を統合し、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?

50% 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

50% 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

50% 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

44% 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

38% 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

日本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。半数の組織は、年次の復旧リハーサルを行い、システム復旧前にセキュリティコントロールのギャップを是正し、対応・復旧用の保管リポジトリを維持しています。一方で、セキュアな調査のため隔離環境を利用している組織は44%、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38%に留まります。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。

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?

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

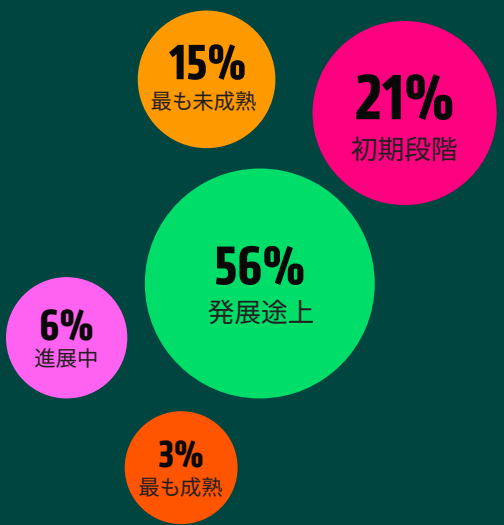
コンプライアンス対応のため、バックアップのプライバシーやセキュリティ違反を特定し、解決している

日本の組織では、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。大半の組織が攻撃時のコンプライアンス対応を導く目的で分類を活用している (57%) 一方、インシデント発生前に重要度を定義する (54%)、あるいはリスクに基づきバックアップの優先順位を付ける (53%) 組織はやや少数に留まります。さらに、プライバシー侵害やセキュリティ違反への対応に分類を活用している組織は半数未満 (49%) に留まります。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3%にすぎません。

サイバーレジリエンスの成熟曲線 (日本)



最も未成熟 (15%): 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 (21%): 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。

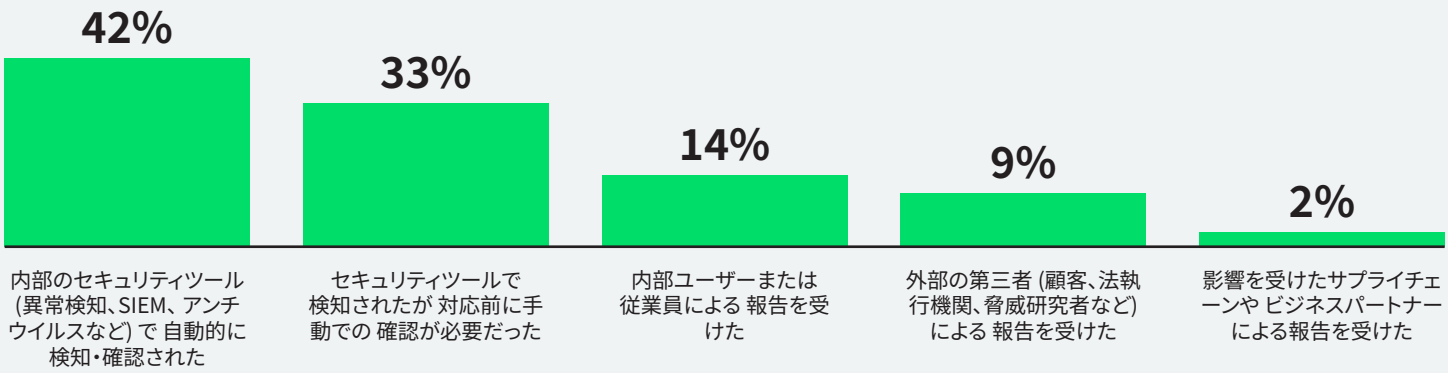
発展途上 (56%): バックアップ、管理者制御、脅威インテリジェンスなどの基本的な施策は 比較的一般的になっていますが、依然としてばらつきがあります。復旧環境の整備、コンプライアンスチェック、セキュリティギャップの 是正は断続的に行われており、レジリエンス施策は部分的にしか効果を発揮していません。

進展中 (6%): 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 (3%): 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。

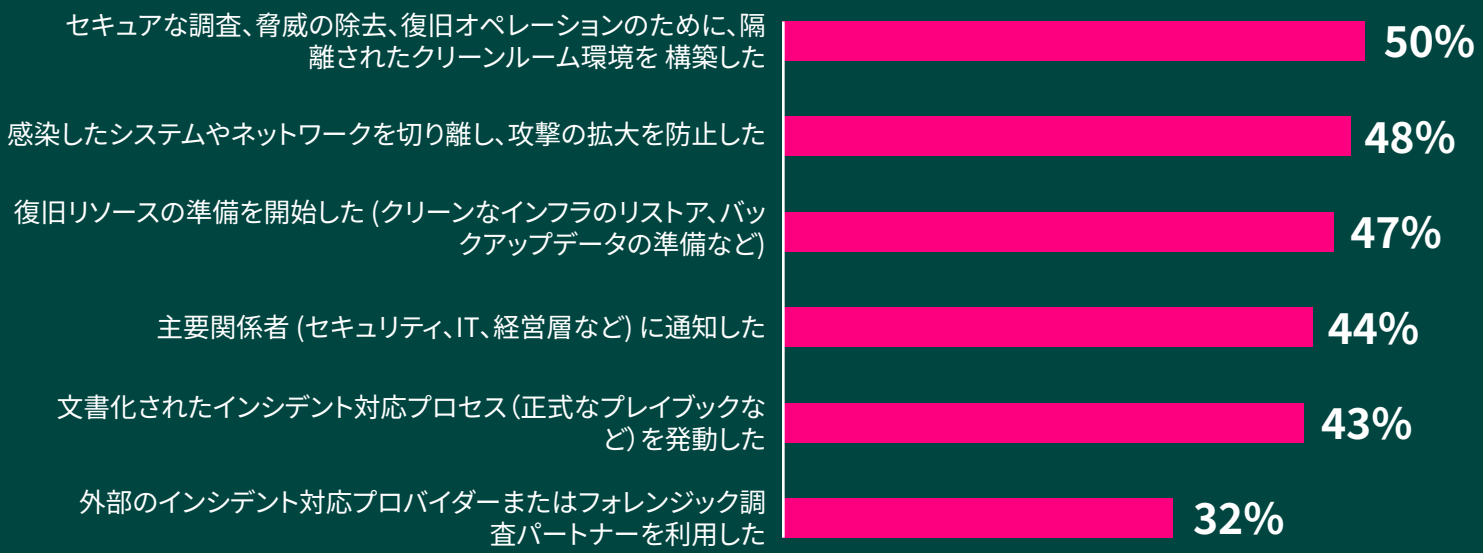
攻撃下におけるレジリエンス

攻撃を特定する方法



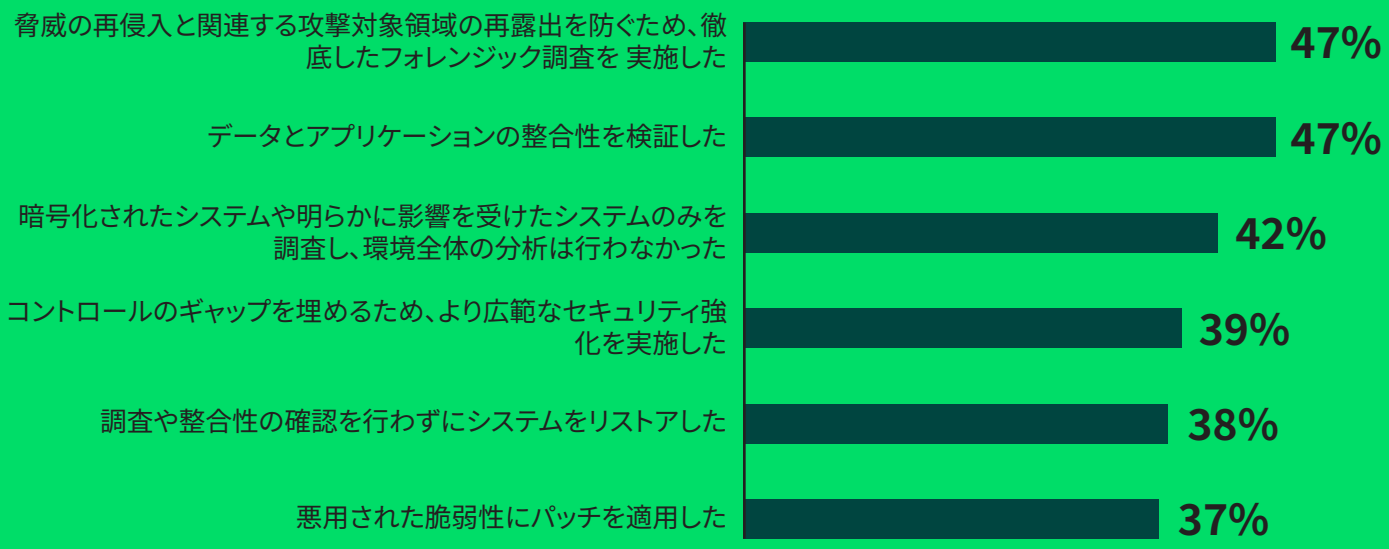
サイバー攻撃発生時、日本の多くの組織はインシデントを内部で検知しています。42%の組織は、内部のセキュリティツールで攻撃を自動的に検知・確認したと回答しました。さらに33%は、ツールによって検知されたものの、対応前に手動で確認する必要があったと答えています。一方、内部ユーザー (14%) や外部の第三者 (9%) からの報告に依存していた割合は比較的少なく、検知の大部分は内部ツールで行われています。ただし、依然として人による確認が必要な部分があることが示されています。

攻撃確認後の行動



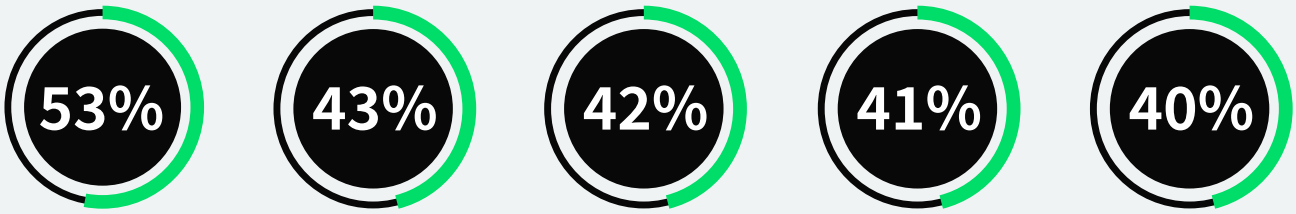
攻撃が確認されると、日本の組織は復旧支援のため、さまざまな対応を講じました。約半数がクリーンなインフラのリストア (47%) や、隔離されたクリーンルーム環境の構築 (50%) を開始しています。感染したシステムの封じ込め (48%) を行った組織は約半数に上り、関係者への通知 (44%) や正式なインシデント対応手順の発動 (43%) を行った組織は約4割でした。一方、外部のインシデント対応やフォレンジックの専門家を活用した組織は32%に留まり、重要な対応プロセスの実行には依然としてばらつきが見られます。

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、組織はフォレンジック調査や修復作業などを実施しました。約半数の組織が詳細なフォレンジック調査 (47%) やデータ・アプリケーションの整合性確認 (47%) を行った一方、より広範なセキュリティ強化策を実施した組織は39%に留まりました。悪用された脆弱性に対するパッチ適用を行った組織は37%、十分な調査や整合性確認を行わずにシステムをリストアした組織は38%に上り、再感染や残存リスクの可能性が残されています。

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、チーム内のコミュニケーションや調整が取れなかった

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

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

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

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。半数以上の組織が、重要システム停止中の連携やコミュニケーションに苦労し (53%)、約4割の組織は、リストア完了前に業務再開を求める経営層からの圧力に直面しました (41%)。さらに、セキュリティツールの回避 (40%)、再感染 (42%)、クリーンな復旧ポイントの欠如 (43%) といった課題が重なり、対応はさらに困難になりました。

レジリエンスへの投資が依然として不十分な領域

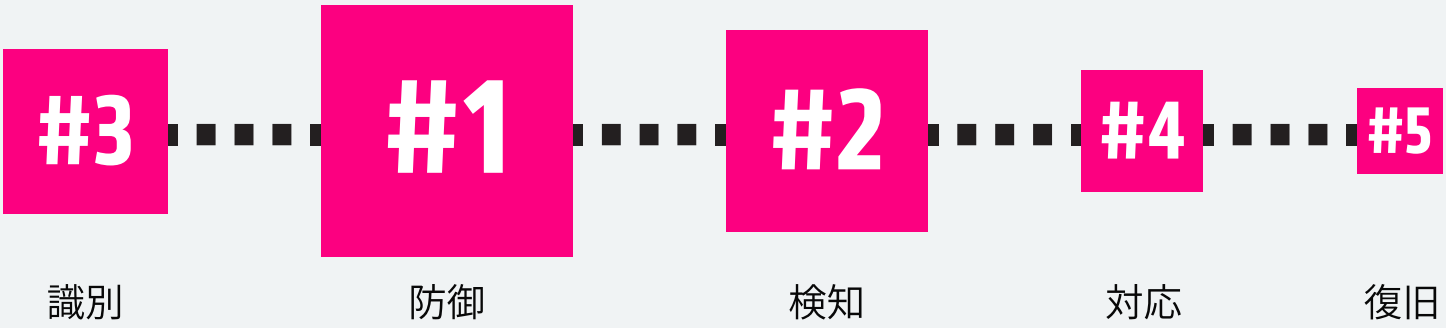
十分に準備された組織であっても、攻撃が発生するとレジリエンスを維持することは容易ではありません。運用上の圧力が高まる中、連携の不備、不完全な復旧対応、再感染のリスクが顕在化し、統一されたプロセスや継続的な保証がなければ、復旧がいかに脆弱になり得るかが明らかになります。

こうした課題は、日本の組織が現在のサイバーレジリエンス予算を配分する方法にも反映されています。多くの組織は、経済産業省 (METI) やデジタル庁、各業界規制当局が示すガイドライン、あるいはISO/IEC 27001に準拠する一方で、NISTのサイバーセキュリティフレームワークを参照し、5つのコア機能 (識別、保護、検知、対応、復旧) に基づき、成熟度をベンチマークしています。

しかし、これらの領域への予算配分を見ると、多くの組織は未だに予防、防御、検知に重点を置いており、対応や検証済みの復旧に割り当てられるリソースは相対的に少数に留まっています。その結果、レジリエンスの成熟度は依然として防御重視に偏っており、攻撃後の対応にこそ最も重点を置くべきであるにも関わらず、リストアへの投資は十分とはいえないことが明らかになっています。

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。日本の組織の51%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。半数以上 (59%) 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。一方で31%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

日本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

2000091-001 EN 2-2026