COHESITY

ホワイトペーパー

破壊的なサイバー攻撃が蔓延する世界におけるサイバーレジリエンスの確立

Cohesityの「破壊的なサイバー攻撃に対するレジリエンス成熟度モデル」を活用し、ビジネスを評価します。

目次

エグゼクティブサマリー

データは、営利組織にとっても非営利組織にとっても生命線です。ITへの依存度が高まっているプロセスやワークフローにとってデータは欠かせない要素であり、「紙とペン」で行う手作業のプロセスに戻ろうとすれば、組織が製品やサービスを提供する機能に多大な影響を及ぼしかねない大きな混乱が生じます。

これまで、このような混乱は事業継続や災害復旧の領域であり、洪水、火災、停電、設定ミス、機器の故障といった明確に定義された少数のシナリオに起因するものでした。今日、最も発生する可能性の高い混乱は、破壊的なサイバー攻撃によるものです。

本ホワイトペーパーでは、IT運用チームがこれまで事業継続や災害復旧シナリオへの対応に使ってきた従来のアプローチでは、なぜこのような新たな脅威に対応できないのかについて、詳しく確認していきます。また、セキュリティ運用チームがこれまで非破壊的なサイバー攻撃の対処に用いてきたインシデント対応プロセスが、なぜ不十分なのかについても検討します。

最後に、Cohesityの「破壊的なサイバー攻撃に対するレジリエンス成熟度モデル」を活用して、組織が破壊的なサイバー攻撃に対するレジリエンスを高めるために講じることが可能な、実用的な手順をご紹介します。このモデルを使えば、現在のレジリエンスの成熟度を評価し、将来的にレジリエンスを向上させていくためのロードマップを策定することが可能です。

新たな脅威と、従来式アプローチが不十分な理由

ランサムウェアのルーツは1989年に発生した「AIDS Trojan」まで遡ることができますが、このような攻撃が容易に収益化されるようになったのは、それから約20年後に暗号通貨が登場してからのことであり、今日のような猛攻撃に繋がりました。

2012年には別の種類の破壊的な攻撃が登場しましたが、この時発見されたのがFlameやShamoonといったワイパー型マルウェアです。この2つのマルウェアは、それぞれイランとサウジアラビアの石油会社の利益に関連するデータを狙い、破壊しました。犯罪者が金銭的利益を得るために使用するランサムウェア攻撃とは異なり、こうしたワイパー型攻撃は、他国の利益や経済を害するために国家やその党派が行うものです。現在の地政学的状況から、近年ではワイパー型攻撃が世界中で著しく増加しています。

情報セキュリティという学問が始まり、破壊的なランサムウェア攻撃が台頭するまでは、この分野で組織が直面する主な影響はデータの窃取でした。詐欺や物品の窃取とは違い、データを窃取されても組織にはまだデータのコピーが残っています。そして、このデータを使って引き続き商品やサービスを顧客に提供することができます。こうした攻撃による影響は、評判の低下、データが盗まれたパートナーやデータ主体からの訴訟の可能性、規制当局による罰金といった二次損失です。

現在のような、ランサムウェアやワイパー型攻撃などの破壊的なサイバー攻撃が蔓延する時代では、こうした二次損失に、組織が商品やサービスが提供できなくなる一次損失も加わっています。二次損失の大部分は、(インシデントを防ぐための適切な管理体制が整っていないことが原因であり、インシデント発生前にその原因が発生しているという意味で) 埋没費用です。これに対し、対応や復旧に時間をかけるほど、組織の一次損失は増えていきます。組織のデータの機密性を狙った攻撃では、非効率的で非効果的な対応や復旧プロセスでも許容できる余裕がありました。組織にとって重要なデータの完全性や可用性が脅かされるような攻撃が横行する現在、もはや私たちにそのような余裕は残されていません。

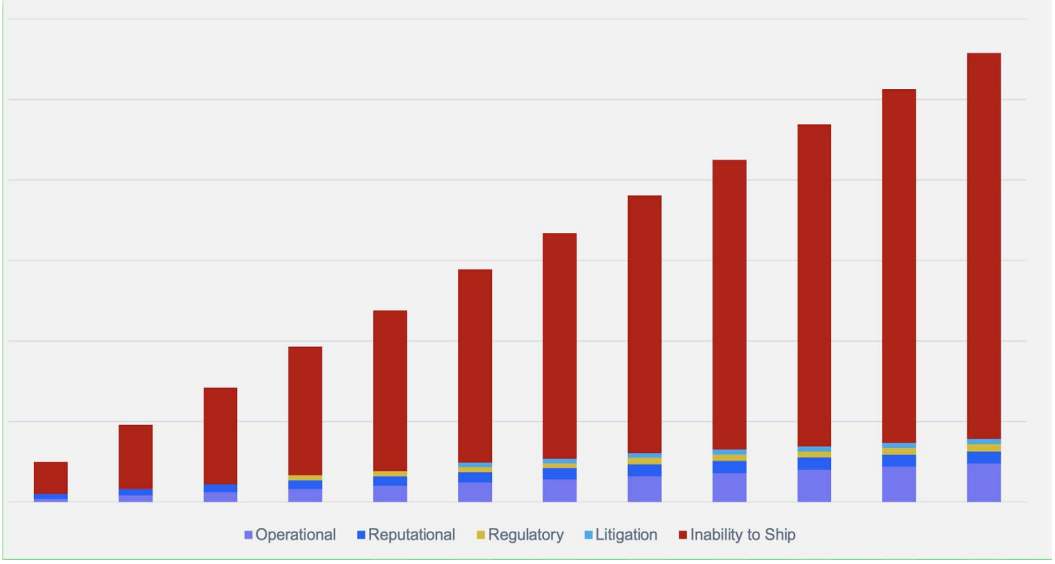


***図1:** さまざまな種類の損失に対する時間の影響の目安*

近年はRamsomware as a Service (RaaS) が発展したことで、防御する側の事態はさらに悪化しています。私たちがこれまで直面していたのは、独自のインフラを実行して攻撃を行う、数十名程度のランサムウェアオペレーターです。ランサムウェアオペレーターにはインフラの実行に必要な技術的スキルを集結させる必要があったため、攻撃の数には限りがありました。

しかしこのようなオペレーターの多くが、自分たちのランサムウェアプラットフォームやツールキットを、技術スキルを必要とせず、攻撃を実行する人的リソースだけを必要とする「アフィリエイト」に提供するほうが儲かることに気付きました。その代わり、アフィリエイトは通常受け取った身代金の80%を手に入れるのに対し、プラットフォーム運営者が受け取るのは20%です。また、RaaSによって、プラットフォーム運営者が他のプロバイダーと差別化するため、プラットフォームが持つ攻撃ツールの革新により力を入れるようになりました。その結果、主な攻撃ベクトルがフィッシング攻撃からより成功率の高い技術へと移行しました。その一例が、インターネットに接続されたインフラの脆弱性の悪用です。これは、組織がパッチ適用して攻撃対象領域を閉鎖するよりもずっと前の、数日以内に発生する可能性があります。もうひとつ増加傾向にあるのが、以前の攻撃で窃取した資格情報の再利用です。

私たちは、より深刻な影響を及ぼす攻撃の増加という問題に直面していますが、サイバーセキュリティに対する支出の大半が、これまでは保護と検知に費やされてきました。これは、機密性に対する攻撃を重視していたためです。毎日のように押し寄せる侵入の試みに組織が飲み込まれてしまわないよう、予防と検知にお金をかけることは重要ですが、今日の破壊的なサイバー攻撃の量と巧妙さに対処するには十分ではありません。過去12か月のニュースをざっと確認すると、サイバーセキュリティの予算に数千万ドルもかけている組織の多くが、ランサムウェアによって業務に大きな支障をきたしています。つまり、保護と検知にお金をかけるだけでは不十分だということです。私たちがいくら堀を広げたり壁を高くしたりしても、敵はより性能の高いボートや背の高いはしごをつくるだけです。もしくは、ソーシャルエンジニアリングを使って正面から城門を突破するかもしれません。

NISTのサイバーセキュリティフレームワーク2.0のような最新のサイバーセキュリティフレームワークや、**EU Network and Information Security (NIS2) 指令**2.0や**EUデジタル・オペレーショナル・レジリエンス法 (DORA)** といった規制のほとんどが、レジリエンスの構築を重視しています。レジリエンスとは、予防や検知を行えるだけでなく、対応や復旧を通じてサイバー攻撃に耐える能力のことですが、対応と復旧の2つはこれまであまり投資されなかった分野です。

企業には通常、130種を超えるサイバーセキュリティツールがインストールされていますが、その大半は、サイバー攻撃の被害を防ぐのに十分な統合や運用ができていません。予防と検知にこれ以上投資しても、サイバーリスクはほんのわずかしか緩和されないばかりか、ユーザーとの摩擦増加、組織のアジリティ低下、アラート疲れの悪化、ライセンスコストの上昇、管理するセキュリティインフラの増加が起こる可能性があります。一方、対応と復旧にお金をかければ、最新のフレームワークと規制、最新のサイバー攻撃の脅威に必要となるサイバーレジリエンスが実現します。

サイバーレジリエンス達成における5つの障壁

従来のBC/DRの復旧アプローチは、サイバー攻撃には適していません。

サイバーセキュリティからサイバーレジリエンスへ移行する際に多くの組織で最も大きな障壁となるのは、対応機能は最高情報セキュリティ責任者 (CISO) が監督するチームが所有し、復旧機能は最高情報責任者 (CIO) が監督するチームが所有しているということです。この2つの機能は元々他の脅威に対応するために構築されたものであるため、互いにほぼ独立して機能が構築されていました。これまで、CISOはデータ窃取攻撃を、CIOは災害復旧と事業継続 (BC/DR) を対処していたのです。BC/DR戦略は、洪水、火災、地震、停電、機器の故障、設定ミスなど、数が限られていて理解しやすい脅威シナリオを中心に展開されました。

サイバーセキュリティに莫大な予算をかけ、BC/DRプログラムが十分に確立されている組織でもランサムウェア被害に遭ってしまう理由は、この2つの側面が破壊的なサイバー攻撃に耐えるという目的に適合していないためです。結果として、莫大なコストと顧客への多大な迷惑が生じます。

CIOによるBC/DR計画は、少数の十分に定義された根本原因に対応できるよう設計されるものです。自動化とオーケストレーションが復旧で大きな役割を果たし、通常はシステムの最後のスナップショットが復旧に使用されます。

これは破壊的なサイバー攻撃とは対照的です。破壊的なサイバー攻撃は、バックアップを利用できないように積極的に狙って攻撃の成功率を高めます。このような敵は脆弱性を悪用して組織の内部に侵入するため、MITRE ATT&CKにある数百の手法を任意に組み合わせて繰り返し使用します。そして一旦侵入すると特権を昇格し、バックアップからの復旧後も永続性を維持して組織全体を水平方向に移動し、データを盗んで、最終的には削除や暗号化を行います。

破壊的なサイバー攻撃の被害額が最も大きくなる組織とは、バックアップが敵によって使用できなくなるような組織や、脅威や脆弱性を取り除くための適切な是正措置を講じずに攻撃されたシステムを復旧し、同じシステムを数秒から数分で再感染させてしまうような組織です。

調査が緩和に繋がらない

破壊的なサイバー攻撃から復旧する場合、IT運用チームはセキュリティ運用チームを頼って、再感染や再攻撃を防ぐために必要な手順を把握します。セキュリティチームによる調査では以下のことを明らかにします:

- どの脆弱性が悪用されたのか (システムを本番稼働に戻す前にIT運用チームがパッチを適用するため)
- どの悪意のあるアカウントと認証プロバイダーをシステムから削除すべきか
- どのメールがユーザーの受信トレイに残されたまま、再びクリックされるのを待っているのか
- どの永続化メカニズムが変更された設定ファイル内に存在し、削除を必要としているのか
- バイナリやライブラリが悪意のあるものと差し替えられたか
- レジストリやドメインフォレストに加えられた変更はあるか
- 攻撃を阻止または検知できなかったのはどのコントロールか (再発を防止できるよう制御を強化するため)
- 復旧システムから削除が必要なその他の攻撃アーティファクト

また、LOL (「環境寄生型」) 攻撃がますます蔓延し、環境を管理するために使用するツール自体が、環境に対する攻撃に使用されています。PowerShellやSSHが利用できない場合の復旧への影響とは?

CIOが単独で目標復旧時間 (RTO) を約束することがありますが、これは単に、ディスク、パイプ、復旧ソフトウェアの速度といった要素を指すものであり、対応段階で行う封じ込め、調査、根絶にかかる時間は含まれていません。インシデントが発生して初めて組織が学ぶことになるのは、想定外の対応時間を追加するか、追加せずに何度も復旧を繰り返してその度にRTOを伸ばすか、どちらかが必要だということです。そうしなければ、ほぼ即座に再感染してしまいます。CIOとCISOは協力し、対応と復旧の両方を実現できる達成可能なRTOについて、取締役会や上級幹部と現実的な期待値を設定する必要があります。

セキュリティ制御が利用できない場合

CISOは、データ窃取シナリオを想定して多くの能力を構築していたのかもしれません。また、組織は主要なIT、セキュリティ、ビル施設の機能までもが攻撃後に機能しなくなることを想定していたのかもしれません。実際の事例では、ドアのアクセス制御システムが消去され、対応を開始するのに必要な建物や部屋への物理的なアクセスが不可能になりました。また、VoIPやメールシステムも影響を受け、保険会社、ビジネスパートナー、規制当局、法執行機関、報道機関との連絡が取れなくなりました。(報道機関はLinkedInを使って同組織の従業員に接触し、何が起きているのかを確認しなければなりませんでした。その結果、従業員でさえお互いに連絡を取れなかったために、何が起きているのか把握していないことがわかりました。否定的な方法が続きました。)

BC/DRでは多くの場合、重要な業務アプリケーションを第一に優先します。これは、これらがIT運用チームが業務部門と連携し、セキュリティとは切り離して作成したものであるためです。しかし、信頼できる最低限実現可能な対応能力 (MiViRC) を取り戻し、IT部門とセキュリティ運用部門が社内外の関係者と協力してインシデントを管理できるようにすることが重要です。

破壊的サイバー攻撃の後でセキュリティコントロールが機能しない場合があります

SANS Instituteのインシデント対応のライフサイクルにおける6つのステップでも、**NISTのSP800-61r2にあるコンピューターセキュリティインシデント対応ガイドでも**、ほとんどすべてのサイバーインシデント対応フレームワークにおいて、ランサムウェアやワイパーのような攻撃の蔓延を防ぐ上で封じ込め段階が重要です。ここでの課題は、調査、根絶、復旧で、エンドポイントへのアクセスに依存してしまうことです。**EDR (エンドポイントの検知と対応)** や**XDR (拡張検知と対応)** といったリモートフォレンジック・イメージングやエンドポイントのセキュリティ制御が、今日のセキュリティ対策として一般的です。

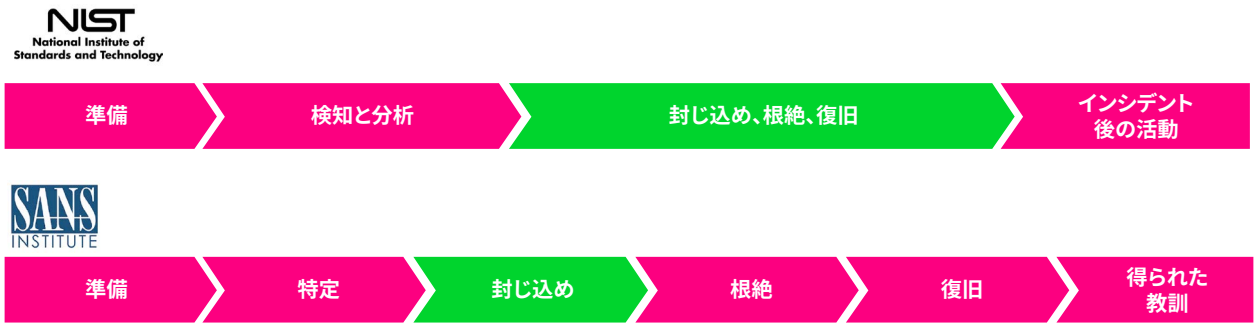


***図2:** 封じ込めはインシデント対応のベストプラクティスではありますが、セキュリティツールを妨害する可能性があります*

セキュリティ制御は信頼できないことがあります

サイバー攻撃における攻撃者の行動を分析するデファクトスタンダード、MITRE ATT&CKフレームワークには、攻撃者が行うエンドツーエンドの手順を示す14の戦術が定義されています。「防御回避」という戦術は、攻撃者がセキュリティ制御を回避するための手法を示しています。***この「防御回避」という戦術には、他のどの戦術よりも多い42の手法が含まれている点に注目してください。***バックアップを保護せず、エンドポイント上にある検知型セキュリティ制御に全面的に依存している状態では、それらが侵害されるリスクがあります。その結果として、ランサムウェアやワイパー型攻撃の進行に気付けず、組織は復旧不能な状態に陥る可能性があります。

まとめると、バックアップ自体が標的にされていない場合、多くの組織が破壊的なサイバー攻撃への対応でCIOチームに従来型のBC/DRプロセスや技術を使わせようと計画しています。CISOチームがインシデントの調査を終え、必要な是正措置や再感染のリスクを確立するまで、CIOチームは復旧作業に移ることができません。同時に、CISOチームはこのような攻撃が自分たちの対応機能に与える影響を考慮しておらず、対応能力の復旧をCIOチームに依存している場合があります。

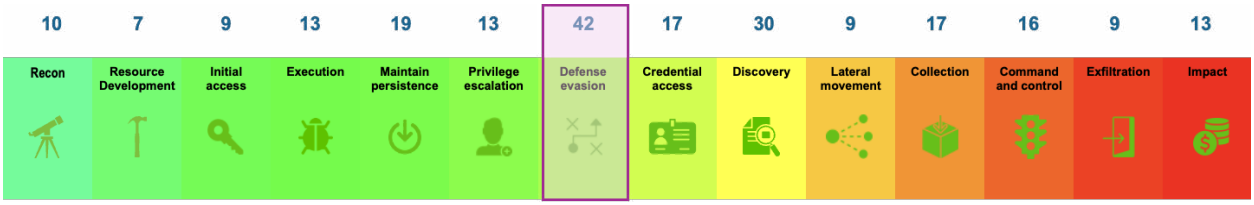


図3: *防衛回避は全14の戦術の中でATT&CKの手法数が最多*

サイバーセキュリティからサイバーレジリエンスへの移行

この種のインシデントを日常的に処理しているインシデント対応を考慮した企業のほとんどが、破壊的なサイバー攻撃の中で達成可能なRTOを最小化するための鍵は、隔離された対応と復旧環境を確立することだということを理解しています。このような組織はインシデント後に顧客と連携してこうした環境の確立に取り組む必要がありますが、これが、再攻撃が起こる可能性を最小限に抑えながらシステムを復旧させる鍵です。

従来のBC/DRシナリオを実現してきた背景から、データ管理ベンダーはIT運用チームの復旧ニーズのみを重視した隔離環境を提供していることが多く、サイバーレジリエンスの実現に必要な対応と復旧の本質的な関係を忘れてしまっています。

インシデントの根本原因に対処しなければ、再攻撃後に復旧を繰り返さなければならなくなり、本番システムの復旧に大幅な遅れが生じる可能性があります。こうした復旧の試みが繰り返される度に業務部門と約束したRTOが伸び、復旧計画の策定時に許容できるとみなした時間をはるかに超えた停止が発生することになります。

Cohesityは影響を抑える上で、セキュリティ運用チームの対応ニーズを、IT運用チームの復旧ニーズと同様に重要なものと考えています。攻撃の性質を理解しないままシステムの復旧を急ぐアプローチでは、攻撃対象領域や攻撃のアーティファクトを取り除くことはできません。継続的な攻撃によって、復旧したシステムが数分のうちに再感染してしまいます。ランサムウェアの集団は、以前攻撃したが身代金の支払いを拒否された組織を再度攻撃する、「二重」攻撃を使用することが多くなっています。このような攻撃者は、最初にアクセスを得るために使用した脆弱性と同じものが封鎖されていない場合、そこを利用します。

Cohesityは、対応機能と復旧機能の両方の効果と効率を高めるために、どちらのチームも使用できる単一プラットフォームを構築しました。

クリーンルーム

クリーンルームにはさまざまな定義がありますが、Cohesityでは、セキュリティ運用チームがどのように攻撃が発生したのかを把握するため、必要な調査手順を実施することのできる隔離環境と定義しています。インシデントの時系列を作成することで、脅威を根絶して再発を防止するため、復旧段階で講じるべき是正措置を示すことができます。

クリーンルームは通常、セキュリティ運用チームが所有します。この調査段階では、システムの復旧は行いません。システムは隔離環境で調査するため、相互依存性はほとんど関係ありません。隔離することで、既知の優れたセキュリティツールを使用して防衛回避 (前述) を回避し、攻撃者が対応策を観察したり妨害したりできないようにして、既に復旧したマシンがクリーンルーム内のシステムによって再感染するリスクがないようにします。

クリーンルームは、Cohesityがわずか数分で確立可能な最低限実現可能な対応能力 (MiViRC) の一部であり、これに依存しています。信頼できる、既知の優れたインフラを構築することで、対応と復旧プロセスにおけるコラボレーション、コミュニケーション、その他のワークフローをサポートします。セキュリティ運用ツールを隔離環境で使用した既知の良好な状態にリストアすることで、組織は攻撃者が使用する多くの回避手法を避けることができます。

また、Cohesityではクリーンルームでのセキュリティ運用チームのニーズに応える、多数のネイティブ機能を提供しています。Cohesity DataHawkの脅威ハンティング機能を利用すると、インシデント対応者はMITRE ATT&CKフレームワークでランサムウェアオペレーターが使用する170,000件以上のセキュリティ侵害インジケーター (IoC) を集めたフィードを確認できます。これは、攻撃者が攻撃のライフサイクル全体で使用する手法を組織が理解するのに役立ちます。

このフィードは、顧客独自の脅威インテリジェンスフィードや、サードパーティが提供するフィードでさらに強化することが可能です。顧客のセキュリティ運用チームがフォレンジック段階でシステム上で発見したアーティファクトは、Cohesityにフィードバックして影響を受けた他のシステムを探すことができます。そして、こうしたシステムを調査範囲に加えることができます。

Cohesityの脅威ハンティングはエンドポイントのエージェントに依存していないため、XDRやEDRシステムに対して使われる防御回避手法の影響を受けません。また、完全にパッシブのため、攻撃者に検知されたり妨害されたりする可能性がありません。Cohesityの脅威ハンティングはバックアップを使用しているため、組織が封じ込めでホストやネットワークを隔離した場合でも引き続き機能します。さらに、多くの組織ではバックアップの保存期間が、セキュリティソリューションが通常保持するログの保存期間よりも長くなっています。そのため、事前に配置されて長期間潜伏するワイパー型攻撃など、ローアンドスロー攻撃を実施する国家主体の活動を検知する機会が得られます。

従来のデジタルフォレンジックでは、調査員は事後に取得したフォレンジックイメージ1つを使用し、システムがどのように特定の状態に達したのかについて仮説を立てていました。Cohesity DataProtectでは、フォレンジック調査員がインシデント全体の時系列を自由に確認し、ファイルシステムの状態のイメージをわずか数秒で読み込むことができます。今では、ツールを使ってファイルシステム同士を比較し、設定の差異を迅速に特定して永続化メカニズムや悪意のあるアカウントを見つけ出すことが可能です。また、サンドボックスで爆発するバイナリを抽出し、DataHawkの脅威ハンティング機能に提供するIoCを増やすこともできます。

多くの組織では、データベースなどの構造化されたデータストアに保存されたデータの規制との関わりを十

分に把握しているかもしれませんが、大半の組織には規制データやその他の機密データを含む非構造化データが大量にあります。このデータは組織全体に分散しているため把握することが困難です。そして、破壊的なサイバー攻撃を受けた場合、暗号化されたり削除されたりする可能性が高くなっています。Cohesity DataHawkのデータ分類機能は高度なAI/MLベースの検知を使用し、この分散した規制データをバックアップから直接検索して分類します。そのため、データの機密漏洩があった場合に規制当局やデータ主体に通知するという規制要件に遵守しやすくなります。

Cohesityは、セキュリティ運用チームが使用する既存のツールに組織のデータのコンテキストをもたらすため、データセキュリティアライアンスを立ち上げました。クラウド、コンテナ、ハイパーバイザー (数秒で起動可能なインフラ) が利用される時代において、簡単に置き換えることができないのがデータです。また、コンプライアンス規制があり、攻撃者が最終的に盗み、暗号化し、消去しようとしているのもデータです。Palo Alto Networks、Cisco、CrowdStrike、ServiceNow、Tenable、Qualys、BigID、Okta、Securonix、CyberArk、Zscalerといった主要なセキュリティベンダーや、MandiantやTCSのようなセキュリティ関連のプロフェッショナルサービス提供に長けた組織との関係を構築することで、Cohesityは、データコンテキストを活用してサイバー対応と復旧を革新する取り組みの最前線に立ち、既存のサイバーセキュリティへの投資からより大きな価値を引き出せるよう支援しています。

ステージングの重要性

ステージングルームは通常IT運用が所有する復旧環境であり、システムは既知の正常なソースから再構築されるか、復旧されて削除されます。ステージングルームでは、セキュリティ運用チームが定義した脅威の緩和手順が実施されます。また、復旧と緩和手順によって本番環境に問題が再度発生しないことを確認するために、機能のリストアをテストする前に個々のホスト間の相互依存関係を満たす場所でもあります。脅威が緩和されたシステムはその後、最後にもう一度バックアップされ、万が一漏れがあった場合に最初から対応措置をやり直す必要がないよう、ベースラインを提供します。

Cohesity SmartFilesは、既知の良好なインストールメディアをイミュータブルストレージに保存する機能を提供し、攻撃者の手が届かないことを保証します。その後はWindowsやLinuxシステムに迅速にマウントできるため、ITオーケストレーションやスクリプトツールでシステムを再構築することができます。システムのゴールデンコピー (マスターコピー) はCohesity DataProtectでバックアップしてクローンすることで、セキュリティ運用チームの調査結果に従い、タイムライン上のスナップショットから設定とデータを復元することができます。

- 攻撃の影響を軽減するために、事前に対策を講じておくことで、必要なときに信頼できるリソースを確保できるようにします。
- [a] 堅牢なプラットフォーム、3-2-1バックアップルールの遵守、明確なコミュニケーション手順によって、インシデント対応の備えを強化しましょう。

- 破壊的なサイバー攻撃は、組織の対応と復旧能力を標的にします。
- エンドポイントのセキュリティコントロールが、インシデント発生後に必ずしも信頼できるとは限りません。

- どのように攻撃されたのかを把握し、脆弱性をなくし、コントロールを増強するまでは、再度攻撃を受けやすくなります。
- ランサムウェアやワイパー攻撃への対応で組織がシステムを隔離すると、従来のセキュリティツールが機能するのは難しくなります。

- 脆弱性への対応、予防や検知策の追加、永続化メカニズムやその他の攻撃アーティファクトの根絶をせずに復旧した場合、再攻撃を受ける可能性があります。
- 緩和と復旧によって、機能上の問題が発生する場合があります。

図4: *攻撃から復旧までの経過を示すインシデントのタイムライン*

ITとセキュリティの連携でサイバーレジリエンスを実現

セキュリティ運用チームが使用する対応時のワークフロー、チーム、テクノロジーを、IT運用チームが使用する復旧時のワークフロー、チーム、テクノロジーと連携させることが、サイバーレジリエンスを強化する鍵です。これらの機能を単独で重視しても、サイバー攻撃発生時の影響が大きくなるだけです。

2つのチームに単一のプラットフォームを提供するというCohesityのアプローチは、既存のセキュリティツールと統合しながら、セキュリティ運用チームによる対応を加速させます。これによって対応と復旧の両方の効率と効果が高まり、レジリエンスの強化と影響の縮小に繋がります。

インシデント対応におけるクリーンルームの活用方法

多くの組織では、インシデントを迅速に調査し、データ復旧時にシステムが再感染しないようにするための適切な環境が整っていません。

組織の備えと対応力を強化しつつ、新たなリスクを招くことなくインシデント対応戦略を構築するための実践的なポイントを解説するオンデマンドウェビナーをぜひご覧ください。

ウェビナーを視聴する

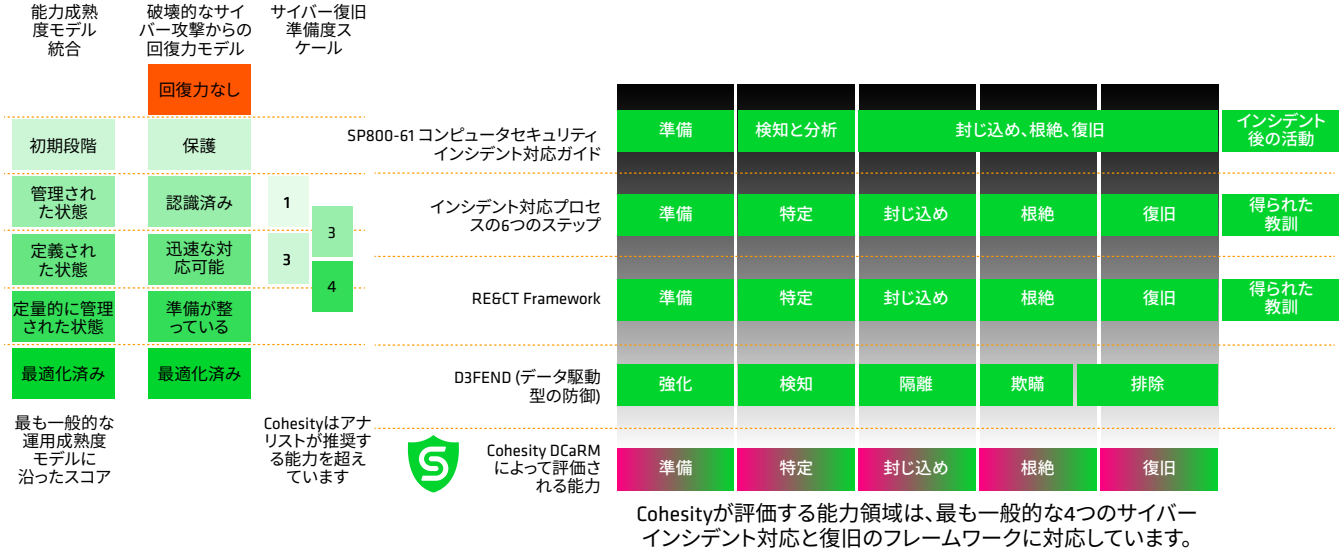
Cohesityの「破壊的なサイバー攻撃に対するレジリエンス成熟度モデル」のご紹介

本ホワイトペーパーでは、サイバーレジリエンスを向上する実証済みの概念をいくつか解説します。次に取るべき論理的なステップは、組織のレジリエンス能力を評価し、どこをどう改善できるのかを把握することです。

そのために、Cohesityの**「破壊的なサイバー攻撃に対するレジリエンス成熟度モデル」**をご紹介します。

この成熟度モデルは、ランサムウェアやワイパー型攻撃といった破壊的なサイバー攻撃に対するレジリエンスを組織が構築・強化できるよう支援するために設計されています。このモデルには、組織がサイバー攻撃に対して回復力を持ち、有効かつ効率的な運用を実現するための明確なベンチマークと構造化されたロードマップが設定されています。

Cohesityのモデルは、SANS Institute社のインシデント対応プロセスの6つのステップ、RE&CT Framework、MITREのD3FEND、NISTのSP800-61 コンピュータセキュリティ インシデント対応ガイドなど、最も一般的なサイバーセキュリティの対応と復旧フレームワークに対応しているため、ベストプラクティスを実現するための道筋を提供します。



Cohesityが評価する能力領域は、最も一般的な4つのサイバーインシデント対応と復旧のフレームワークに対応しています。

***図5:** Cohesityの「破壊的なサイバー攻撃に対するレジリエンス成熟度モデル」と、一般的な対応復旧フレームワークとの参考対応関係*

この成熟度モデルでは、サイバーレジリエンス達成に必要な以下の5段階にわたり、組織の運用能力を評価することができます:

1. インシデントに対する備え
2. 攻撃の特定と調査
3. 攻撃拡大の封じ込め
4. 将来の攻撃を防止するための脅威の根絶と攻撃対象領域の削減
5. セキュアな状態へのシステムの復旧

本モデルにおける成熟度レベルは、以下の表に示されています:

成熟度レベル	説明
回復力なし	組織には、製品やサービスの提供に深刻な影響を及ぼすことなく、破壊的なサイバー攻撃に耐える回復力がありません。
回復可能	組織は災害復旧と事業継続性の能力を構築していますが、この能力は敵対者による攻撃の影響を受ける可能性があり、再感染や再攻撃を防止するための適切な調査段階や是正段階に欠けています。
強化済み	組織は、敵対者による攻撃から復旧する能力を守っています。
認識済み	組織には、回避できず、インシデント対応の封じ込め段階による影響を受けない破壊的なサイバー攻撃の早期段階でハンティングする能力があります。インシデント対応にあたっては、IT部門とセキュリティ運用部門の間で責任を分担する「共同責任モデル」も策定されています。
迅速な対応可能	組織は、インシデント対応と関係者とのやり取りに必要なツールを、信頼できる状態まで復旧することができます。また、インシデントの調査、脅威の根絶、本番環境への復旧前のシステムテストを行える隔離された環境が整っています。 組織は、さまざまな攻撃シナリオを想定したエンドツーエンドの攻撃演習を実施することで、継続的な改善を推進しています。そして、インシデント対応者が将来のあらゆる状況に対処し、プロセスを最適化し、効果と効率を高めるための自動化の機会を見出せるようにします。万が一攻撃による影響を受けた場合、インシデントの管理と対応に必要なインフラとリソースを迅速に復旧することができます。
最適化済み	組織には、プロセス、人材、テクノロジーの継続的な最適化を促すためのメトリクスとテレメトリーが導入されています。データをプロアクティブに発見して分類することで、エンドツーエンドのガバナンスと規制遵守を確保しています。システムを復旧するだけでなく、インフラを信頼できる状態まで迅速に再構築する能力があります。こうしたタスクを並行して行えるよう、インシデント調査、インフラの再構築、データの復旧が最適化されます。

***図6:** Cohesityの「破壊的なサイバー攻撃に対するレジリエンス成熟度モデル」における各成熟度レベルの主要な貢献要素の概要*

Cohesityの「破壊的なサイバー攻撃に対するレジリエンス成熟度モデル」は、特定のベンダーに依存しない中立的なロードマップを提供します。このアプローチにより、ユーザーはサイバーレジリエンスの確立と、それに伴う適切なガバナンス、人材、プロセスの整備を進めながら、ベストプラクティスに基づく対応・復旧フレームワークと整合させることが可能になります。このロードマップは、テクノロジーが運用の成果を主導するのではなく、それを支援・最適化する役割を果たすことを保証します。

それでは、各成熟度レベルについてもう少し詳しく見ていきましょう:

- **回復可能**: このレベルにある組織は、災害復旧や事業継続において成熟した体制を備えている可能性があります。重要なサービスとそれを支えるインフラを特定するために、適切なビジネスインパクト分析 (BIA) を実施し、目標復旧時点 (RPO) と目標復旧時間 (RTO) を策定しています。このような組織は、敵対者による攻撃からデータを守るために必要な保護機能を、データ管理プラットフォーム上に十分に備えていない可能性があります。また、破壊的なサイバーインシデントを、サイバー攻撃特有の複雑な要素を考慮せずに、従来型の災害復旧や事業継続のシナリオとして扱ってしまう傾向があります。このレベルでは、サイバーインシデントへの対応において、IT部門とセキュリティ運用部門との緊密な連携体制が整っていません。
- **強化済み**: このレベルでは、組織が敵対者からの攻撃を受けることは避けられないという前提を認識して、その影響を軽減するための保護策を講じています。組織は、最小権限アクセス、イミュータビリティ (バックアップの不正な改ざんや削除の防止)、職務分離 (悪意ある、または侵害された管理者による有害な変更を防ぐ)、保管庫 (攻撃者の手の届かない場所に復旧手段を確保する) といったセキュリティ原則を実装しています。保管庫は、3-2-1原則といったセキュアなバックアップの慣行に従う上でも組織を支援します。
- **認識済み**: このレベルにある組織は、IT部門とセキュリティ運用部門の間で明確に定義された共同責任モデルを採用しています。こうした組織は、攻撃者がエンドポイントセキュリティを回避した場合でも、脅威ハンティングやデジタルフォレンジックの実施

が可能です。さらに、ホストやネットワークが隔離されている封じ込めの段階においても、脅威ハンティングを継続することができます。脅威インテリジェンスは活用されているものの、情報が古くなっていることが多く、Ransomware as a Service (RaaS) プラットフォームや最新の脆弱性に関する確定情報の定期的な更新が行われていません。また、システムが影響を受ける前の攻撃初期段階を検知し追跡するための多層防御モデルも欠如しています。

- **迅速な対応可能**: このレベルでは、同じ行為者による再攻撃や再感染を防ぐため、組織はシステムを本番環境に復旧させる前に、インシデントの調査や脅威の除去といった必要な対応を実施しています。封じ込めの要件を満たすために、調査と修復を行うための隔離された環境が整備されています。この成熟度レベルでは、継続的な改善と訓練の取り組みも導入されており、インシデントに対応し、セキュアに復旧するために必要なプロセス、人材、テクノロジーが事前に備えられています。(SOCアナリストやインシデント対応担当者、経営幹部が初めてランサムウェアやワイパー型攻撃を経験するのが、まさに自社のデータが人質に取られたり、全システムが消去された本番の事態であってはなりません。模擬対応訓練は有用ですが、実際の状況で求められるエンドツーエンドのワークフロー、スキル、テクノロジーを検証するものではありません。)

組織はまた、サイバーレジリエンスに必要なすべての要素を備えるために、現実的な攻撃シナリオに基づいた訓練を実施しています。同じインシデントは2つとありません。訓練の内容に変化を持たせることで、組織はプロセスの最適化をより効果的に図ることができます。組織は定期的に自動化の機会を探るとともに、スタッフの間に対応動作の習慣化を築くことにも取り組んでいます。

そしてこの段階にある組織は、ネットワークやセキュリティツールに対する信頼を迅速に回復できるだけでなく、対応活動を即座に開始するためのリソースも数分以内に確保できる体制を整えています。最悪の事態においても、攻撃の調査、連携、情報共有を確実に行える信頼性の高い手段を備えています。言い換えれば、セキュリティ制御が回避され、ドアのアクセスシステムが停止し、構成管理データベース (CMDB) やチケット管理システム、メール、IP電話が使えない状況 (つまり、法執行機関、サイバー保険会社、報道機関、規制当局、影響を受けたデータ主体とすら連絡が取れないようなシナリオ) にも備えているということです。

- **最適化済み**: このレベルは、サイバーレジリエンスの到達点、いわば最上位の状態を表しています。この組織は、使用するデータが確実に復旧可能であるだけでなく、そのライフサイクル全体を通じて適切なリスク管理措置が講じられていることを確認して分類するための積極的な取り組みを行っています。ワークフローは、各種規制や影響を受けたデータ主体への通知義務に適合するよう最適化されており、その結果として、組織は罰金を回避しつつ、DORA、NIS2、HIPAA、英国健全性規制機構 (PRA)、米国証券取引委員会 (SEC) など、該当する規制への準拠が可能となっています。「迅速な対応可能」レベルでは、ワークフロー内での自動化の機会を模索するのに対し、「最適化済み」レベルでは、インシデント対応と復旧プロセス全体のガバナンス、オーケストレーション、管理をエンドツーエンドに追求します。この成熟度レベルに達することで、経営幹部、取締役会、外部のステークホルダーに対し、組織がサイバーレジリエンスの最前線にあることへの確かな信頼を与えることができます。

サイバー攻撃への備えと対応が不可欠となった現在、このようなモデルの重要性はかつてないほど高まっています。これらの攻撃は、今日の組織にとって製品やサービスの提供を脅かす最大の脅威となっています。Cohesityのサイバーセキュリティ専門家や経験豊富な実務担当者は、何十年にもわたるサイバーインシデント対応と復旧の経験をもとにこのモデルを設計しました。これにより、組織の現在の能力を把握し、業界や地域の同業他社と成熟度を比較し、組織の成熟度をベンチマークすることができます。さらに、将来的に取り組むべき改善点や、その進捗を継続的に測定できるロードマップを手にすることができます。

著者紹介

James Blakeにはサイバーインシデント対応で30年以上の運用経験があり、30社以上のFortuneやFTSE 100企業でエンドツーエンドのセキュリティ運用機能を構築してきました。また、複数国家にわたるワイパー型攻撃や数十件のランサムウェア攻撃など、何百件もの大規模なインシデントの事後対応に関わってきました。Cohesityでは、Head of Global Cyber Resiliency Strategyを務めています。

Cohesity.comの詳細はこちら

COHESITY

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

2000059-002 EN 4-2025