COHESITY

ホワイトペーパー

破壊的なサイバー攻撃発生時の対応戦略を練る方法

Cohesityを使って、ランサムウェアなどのサイバー攻撃からセキュアかつ迅速に復旧

目次

エグゼクティブサマリー

ランサムウェアやワイパー攻撃などの破壊的なサイバー攻撃は、従来の事業継続対策や災害復旧のシナリオであるIT運用とは異なるアプローチが必要です。サイバーセキュリティ運用チームは、適切な調査や脅威への是正対応が実施されるようにするうえで、さまざまな課題に直面しています。製品やサービスの提供をできるだけ早くリストアするだけでは十分ではありません。企業は、復旧がセキュアに行われるようにし、再感染や再攻撃によってさらにダウンタイムが長引いてしまうことを防ぐ必要があるのです。

本ホワイトペーパーでは、破壊的サイバー攻撃への対応におけるベストプラクティスを解説するとともに、Cohesityのソリューションが、企業のセキュアな運用体制の実現にどのように貢献できるかを紹介します。

状況分析:「平時」と「有事」で組織運用が異なる理由

「平時」とは、企業が通常通りに問題なく運用している状況です。セキュリティツールからのアラートは、通常セキュリティオペレーションセンター(SOC) またはマネージドセキュリティサービスプロバイダー (MSSP) のコンソールに届きます。これらのアラートは、優先順位を判断するためにトリアージされ、誤検知を除外するためにチューニングされます。同時に、組織のインフラ内部への侵入の兆候を特定するために、さらなる証拠収集が行われます。SOCアナリストが、攻撃者による企業への攻撃を確信した時点で、インシデントを宣言し、調査を継続します。この段階で、企業は「有事」モードに突入します。

調査の間、企業システムやデータの機密性、完全性、可用性が損なわれたことをアナリストが発見すると、侵害を宣言し、インシデント対応プロセスへと移行します。

攻撃者が発見されるまでに企業内部に侵入して過ごした時間は、潜伏期間と呼ばれます。攻撃者は、セキュリティツールのアラートなどで発見されることがあります。しかし、企業が攻撃を認識するのは、システムが使用不能になってからということが少なくありません。潜伏期間にはさまざまなバリエーションがあります。Ransomware as a Service (RaaS) を使った攻撃ではわずか4〜5日程度であるのに対し、人手によるランサムウェア攻撃では数百日に及ぶこともあり、国家支援型の攻撃では数年にわたることさえあります。

機密性、可用性、完全性が損なわれる事例には以下のようなものがあります:

- **機密性**: 組織のデータが許可されていない第三者に漏洩した状態を指します。これには、ランサムウェア集団による犯罪目的のデータ流出や、国家主体の攻撃者による諜報目的のデータ窃取などが含まれます。後者はしばしばワイパー攻撃の前段階として行われます。
- **完全性**: 破壊的サイバー攻撃の複数の段階において、攻撃者は設定ファイル、レジストリ、ID管理システム、場合によってはファームウェアまでも改変して、被害を受けた組織内での持続的な存在を維持しようとします。これらの変更すべてが、システムの完全性に悪影響を与えます。
- **可用性**: 破壊的なサイバー攻撃は、顧客への製品・サービスの提供に不可欠な、組織のITインフラを利用不能にすることを目的としています。ランサムウェア攻撃による暗号化や、ワイパー攻撃によるデータ削除によって可用性が損なわれます。

すべてのインシデントが必ずしも侵害に繋がるわけではありません。また、SOCは継続的に検知を続け、早い段階でインシデントに対応することで侵害に発展するのを防ぎます。一部の侵害は、組織内の限られた範囲に封じ込められ、標準的なインシデント対応プレイブックによって対処可能です。

ただし、特定のインシデントで (特に、ランサムウェアとワイパー攻撃) では、甚大な影響を受ける可能性があります。顧客に製品やサービスを届けるのに必要なシステムや、インシデントを管理するのに必要なITシステムをダウンさせます。これには、施設への物理的なアクセス管理システム、規制当局や影響を受けた関係者・データ対象者との連絡手段、保険会社・法執行機関・報道機関との連携などが含まれる場合があります。そのような場合、組織は**サイバー危機**を宣言し、インシデントを適切に管理できるよう、通常とは異なるワークフローを実施することがあります。

セキュリティチームとITチームがインシデント、侵害、または危機に対応し、システムを信頼できる状態に復旧させ、再発の脅威を緩和した後、組織は「平時」の運用体制に戻ることができます。

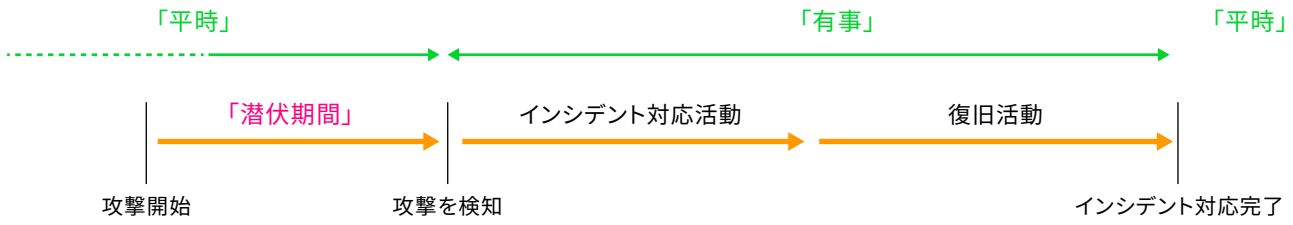

図1. 破壊的なサイバー攻撃下における「有事」と「平時」の段階

なぜ破壊的なサイバー攻撃対策は事業継続対策と異なるのか

破壊的なサイバー攻撃が登場する以前、IT障害の根本原因は、数えるほどしかありませんでした。洪水、火災、機器やソフトウェアの故障、設定ミス、停電などです。これらのインシデントには最小限の調査しか必要とされず、標準的な対応は、直近のバックアップスナップショットをリストアするだけでした。

ですが、ランサムウェアは、格段に複雑です。従来のウイルスやワームとは異なり、スキャンできる単一のバイナリではありません。攻撃者は14の段階からなる攻撃チェーンを通じて攻撃を行い、各段階で目的を達成するために、何百もの手法の中から選択して実行します。攻撃者は常に手法を進化させており、昨日まで有効だったセキュリティ対策の設定が、今日では無力になっていることもあります。

現在の地政学的な緊張により、国家関与によるワイパー型攻撃のリスクが高まり、サイバー脅威はますます深刻化しています。国家支援型の高度な脅威者は、極めて高い能力とリソース、そして動機を有しているため、組織には通常の犯罪ランサムウェアグループ以上のサイバーレジリエンスが求められます。

従来のマルウェアとランサムウェアの調査・修正方法の比較

ウイルスやワームなどの従来型マルウェアは、システム内の悪意あるバイナリをスキャンすることで検出されます。ひとたび識別されると、セキュリティチームによって悪意のあるバイナリが隔離または削除されます。一方で、ランサムウェアやワイパー攻撃は、一連のプロセスを通じて進行し、攻撃者が新たに発表された脆弱性をわずか数日以内に悪用して侵入を果たすことが可能になります。こうした攻撃は、組織のITインフラを利用して「live off the land (環境寄生型)」攻撃を行い、正規のアカウントを悪用したり、設定を変更して権限を昇格させたり、持続的なアクセスを維持したりします。また、機密データを外部送信のためにステージング (準備) したり、OSやアプリケーションに組み込まれたネイティブのスクリプト機能やマクロを使用したりします。こうした活動はすべて、検知・対応・復旧の能力を妨げるためにセキュリティ制御を回避しながら行われるのです。従来のマルウェアとは異なり、単一のバイナリをスキャンして除去できるというものではありません。

セキュアにランサムウェアやワイパー攻撃から復旧するには、インシデントがどのように発生したかを調査する必要があります。組織は、再感染やさらなるダウンタイムを防ぐために、発見された脅威や脆弱性を確実に修正・対処しなければなりません。これこそが、すべてのベストプラクティスに基づくサイバーセキュリティインシデント対応フレームワークの本質です。

将来の同様の攻撃に耐え、現在の攻撃から復旧したシステムが再感染するのを防ぐために、組織は次の3つの重要な領域に対して是正措置を講じなければなりません:

1. **攻撃対象領域**: 最も一般的なランサムウェアの初期侵入経路には、発生頻度の高い順に、インターネットに公開されたインフラの脆弱性、再利用された正規の認証情報、そしてフィッシングメールなどのソーシャルエンジニアリング手法があります。最初に攻撃を受けた「ペイシェントゼロ」(最初の侵入経路や最初に特定された被害者) がどのように侵害されたのかを把握し、その上で復旧したシステム内の脅威を是正する必要があります。これには、脆弱なシステムへのパッチ適用、Webアプリケーションファイアウォール (WAF) などの防御機構の背後に脆弱なシステムを配置すること、そして初期侵入を許したフィッシングメールをユーザーの受信箱から削除することが含まれる場合があります。
2. **回避手法やセキュリティ制御のギャップ**: セキュリティインシデントが「機密性・完全性・可用性」に影響を及ぼす前に、それを未然に防ぐ、あるいは早期に検知することは運用コストを伴いますが、売上損失や風評被害、さらには取引先や影響を受けた個人からの高額な規制罰金や訴訟といったリスクを回避するのに役立ちます。

ランサムウェア集団は、エンドポイント検知と対応 (EDR) や、拡張検知と対応 (XDR) などの一般的なセキュリティ制御を回避するための技術を、RaaSプラットフォームに組み込んでいます。さらに、攻撃者はサイバー脅威インテリジェンス (CTI) のフィードが更新・配信され、攻撃手法が共有される前に行動を起こせる「先手の優位性」も持っています。

ITサービスの提供が中断される前に、既存のセキュリティ制御が攻撃を検知・阻止できなかった理由を把握しない限り、本格的な業務再開はできません。その上で、セキュリティツール群を信頼できる状態に復旧させ、ルールを更新することで、将来の攻撃を早期に検知または防止できる体制を整えることが重要です。

3. **永続化メカニズム**: 一般的なランサムウェアやワイパー攻撃では、攻撃者が多数の痕跡を残していくのが通例です。これらの痕跡が足がかりとなり、システムを復旧しても、完全に把握・除去されていない場合、攻撃者に再びアクセスされるリスクを残すことになります。多くの組織では、数日かけてシステムを復旧させたにもかかわらず、数分以内に再び感染して停止してしまい、その原因が見落とされた持続的な攻撃手法 (永続化メカニズム) であるという事例が後を絶ちません。このような破壊的なサイバー攻撃は複数の段階に分かれて進行するため、脅威ハンティングとフォレンジック分析を組み合わせて、攻撃のタイムラインを構築し、対処すべき痕跡の網羅的なリストを特定する必要があります。

IoC (侵害指標) に関する誤解

侵害指標 (IoC) という概念は、戦術的なサイバー脅威インテリジェンスにおいて重要な要素です。破壊的なサイバー攻撃に対処するために組織が取るべき有時の対応について議論する前に、IoCを定義しておくことが重要です。

IoCは、システムが侵害された***可能性***を示す手がかりを提供します。IoCは敵対的な挙動を探るための出発点にはなりますが、あくまで「標識」のようなものであり、「目的地」そのものではありません。セキュアに復旧するためには、攻撃の全体像を組織として把握し、それに基づいて前のセクションで説明した適切な緩和策を講じる必要があります。例えば、再起動時に特定のコードを再実行させるように変更された設定ファイルはIoCの一例です。同様に、正規のDLLと同名の悪意あるDLLが特定のディレクトリに配置されている場合もIoCに該当します。また、PATH変数を操作して、悪意あるDLLが正規のDLLよりも先に実行されるように仕組まれている場合もIoCの一つです。これらのIoCは、何らかの異常が発生していることを示す手がかりにはなりますが、攻撃の全体像を明らかにするものではありません。

IoCを追跡することは、サイバーセキュリティのインシデント対応において極めて重要ですが、組織はそれらを適切な文脈で適用する必要があります。IoCのみに依存すると、不適切な対応を招くおそれがあります。さらに、十分な調査を行わないまま早期にバックアップから復元すると、再感染を招いたり、他の可用性の問題を引き起こしたりする可能性があります。

IoCが含まれているファイルを安易に隔離したり、IoCを含む古いバックアップスナップショットからファイルをリストアしたりしても、根本原因の解決にはなりません。攻撃者が最初にどのようにして侵入し、それらの変更を加えたのか不明なままでは、再び攻撃を受けるリスクが残ります。さらに、古くて互換性のない構成に戻すことは可用性の問題を引き起こす可能性があります。例えば、攻撃開始以降にバイナリが後のバージョンにパッチ適用されている場合などは特に注意が必要です。

また、バックアップスナップショットにIoCが存在しないからといって、それが「クリーン」である保証にはなりません。IoCはあくまで悪意ある活動の道しるべにすぎないため、それらを取り除いても、攻撃の本質や根本的な脅威は依然として残ったままです。古いスナップショットへの自動ロールバックが行われた場合、インシデント対応チームが攻撃の根本原因に気づかないおそれがあります。

IoCの検知には、サイバー脅威インテリジェンスの収集・分析・共有が欠かせませんが、こうした情報は攻撃者の戦術の進化にしばしば後れを取ります。つまり、攻撃者が行動を変えてから、セキュリティツールがその新たな攻撃手法を認識できるようになるまでにタイムラグが生じることを意味します。これが理由で、世界有数の大企業であっても、十分なサイバーセキュリティ予算と最新の高度なツールを備えた体制を持っているにもかかわらず、ランサムウェアの被害を受けてしまうのです。攻撃者は、サイバーセキュリティツールが検知可能になる前に行動を変え、組織への侵入に成功します。そして、彼らの防御回避能力によって、エンドポイントのセキュリティ制御を無力化します。セキュリティベンダーが新たな攻撃手法を認識し、脅威インテリジェンスをツールに反映する頃には手遅れです。ツールは回避され、検知できなくなっているのです。

この課題を解決するには、Cohesity DataHawkなどのソリューションを使用して、定期的で積極的な脅威ハンティングのような活動を平時にも組み込むことを検討してください。このソリューションなら、従来型のセキュリティコントロールからは独立して動作し、回避されることがありません。DataHawkを活用すれば、サイバー脅威インテリジェンスがまだ把握していない段階で網の目をすり抜けた攻撃も検知できます。

勝利を収めるために: 調査、脅威の解決策、セキュアな復旧

最善のアプローチは、インシデント対応担当者の戦力増強手段としてテクノロジーを活用しながら、レジリエンスを構築して準備を整え、明確なプロセスと運用モデルを定めておくことで、全員が自分のやるべきことを正確に理解できるようにすることです。可能なところにはオートメーションとオーケストレーションを組み込みましょう。さらに、最悪の事態が発生した際に反応的に動くのではなく、的確に対応できるよう、スタッフには適切な訓練と現実的な演習への参加が求められます。

サイバーレジリエンスはお金で買えるものではありません。それは、サイバーインシデント発生後に、組織として適切な行動を取れる準備ができているときに初めて現れる性質です。サイバーレジリエンスを実現するには、破壊的なサイバー攻撃後に組織が直面する現実的な課題を正しく理解し、適切なテクノロジーとサポートを提供できるベンダーと協力して、堅牢なインシデント対応戦略を構築することが不可欠です。

サイバーセキュリティ対応は複雑な活動です。成功は、その複雑さを認めることから始まります。それを無視したり、見て見ぬふりをしたりすれば、最悪のタイミング、つまりインシデント発生時に必ず組織に跳ね返ってきます。

サイバーセキュリティのデジタルフォレンジックとインシデント対応のベストプラクティス

以下は、デジタルフォレンジックやインシデント対応に幅広く受け入れられているフレームワークです:

1. NIST SP800-61「コンピューターセキュリティインシデント対応ガイド」
2. SANS Institute「インシデント対応プロセスの6つのステップ」
3. RE&CTフレームワーク
4. MITRE D3FEND (「データを活用した防御」)

本ホワイトペーパーでは、SANS Instituteのモデルを重点的に扱います。ただし、その他のフレームワークもサイバー攻撃への備えと対応に必要な手順については概ね共通しています:

図2. サイバーデジタルフォレンジックとインシデント対応のベストプラクティス

Cohesityで運用上のベストプラクティスを実現

有事の状況においては、すべてのベストプラクティスに基づくサイバーセキュリティインシデント対応フレームワークに、封じ込め、調査、脅威の緩和、そして最終的な復旧の段階が含まれています。これらの「封じ込め・調査・緩和」の段階を省略して、拙速に復旧へと進んでしまう組織は、攻撃を許した脆弱性をそのまま放置することになります。

攻撃を検知・防止できなかった防御のスキは依然として開いたままであり、復旧しても攻撃者が仕込んだ永続化メカニズムやその他の痕跡までも一緒に復元されてしまいます。その結果、再感染や再攻撃が発生し、ダウンタイムがさらに長期化するという事態が頻発します。復旧を最優先にした対応をとる組織では、ランサムウェア攻撃を受けるたびに繰り返し復旧作業が必要となり、結果として十数回にも及ぶ復旧を余儀なくされるケースが少なくありません。

特定

特定には以下の2段階があります:

1. **インシデントが発生している可能性があるという攻撃の初期認知**: これは、ユーザーや第三者からの報告という形で現れることもあれば、何らかの技術的なセキュリティ制御からのアラートという形を取ることもあります。いずれの場合も、その正当性と影響範囲を確認するためにトリアージを行う必要があります。
2. **攻撃の発生過程の把握**: これにより、脅威の適切な根絶、悪用された脆弱性の除去、そしてセキュリティ対策の強化が実現されます。その結果、システムをセキュアかつ回復力のある状態で復旧させることが可能になります。

それでは、これらの各ステージを詳しく見ていきましょう。

初期認知

初動認知は技術的には「平時」の活動にあたります。というのも、組織が攻撃の進行中であると認識しない限り、有時を宣言することはできないからです。したがって、ランサムウェアなどの攻撃を検知するための仕組みについて議論することが重要です。それによって、インシデント対応のワークフローにどのような影響が出るかを理解できるようになります。

RaaSプラットフォームの登場により、EDRやXDRといった主流のセキュリティ対策を回避する手法が普及し、これらのツールを攻撃に対して無力化しています。サイバー攻撃の手法を分類する上で最も広く使われているMITRE ATT&CKフレームワークにおいても、防御回避という戦術には、他の13の戦術の中で最も多くの手法が含まれており、次に多い戦術の約2倍にのぼります。ランサムウェア攻撃者が用いるこれらの手法は、Cohesity DataProtectの異常検出や、DataHawkの脅威ハンティング機能を回避することはできません。

DataProtectのAIベースの異常検出などから発せられるアラートは、**信頼性**が高く、誤検知ではないと判断できる**確度**が高いだけでなく、アラートを確認するだけでSOCアナリストが「何が起きているか」を把握できるだけの詳細な情報も備えています。これにより、初期トリアージと調査のスピードが上がり、システムをセキュアに本番環境へ復旧させるまでの時間が短縮されることにも繋がります。

トリアージの段階で、インシデント対応に必要なシステムが影響を受けていることが明らかになった場合、あるいは組織全体でシステムの暗号化や削除が、あらかじめ定められた閾値を超えていることが判明した場合、組織は**サイバークライシス**を宣言することができます。あらかじめ定義されたサイバー危機対応ワークフローを導入することで、通常のサイバー侵害対応の範囲を超えて、特定の対応を実施するためのエスカレーション手順や、インシデント対応者に与えられる事前承認された権限を組織内で明確に定めることができます。

しかし、インシデント対応に必要となるシステムが影響を受けたり、利用不可だったり、信頼できなかったりすることが判明する場合があります。このような状況で発生しうる課題には、以下のようなものがあります:

- インシデント対応関係者の連絡先一覧を利用できない (経営陣、規制当局、サイバー保険会社、委託IRベンダー、サプライチェーンパートナー、報道機関など)

- インシデント対応のワークフロー自体を参照できない
- サイバー保険契約書や委託したIRベンダーとの契約書を確認できない
- 物理的なアクセス制御システムや建物の環境制御のための管理サーバーや構成設定がダウンしている
- 関係者と連絡を取るために必要な通信手段 (EメールやVoIPなど) が利用不能、または信頼できない
- ルーターやスイッチの設定、あるいはファームウェアが信頼できない状態にある場合、SaaSアプリケーションやインターネットへ接続すると、盗聴や妨害を受けるリスクがある
- セキュリティツールそのものが回避されたり、無効化されたりして使用不能になっている

当然のことながら、ほとんどの組織は最も重要なアプリケーションの復旧を優先します。それは、製品やサービスの提供を再開するために不可欠なものであり、最小構成で成立する会社 (MVC) とも呼ばれます。しかし、破壊的なサイバー攻撃を受けた組織は、インシデントを適切に管理するためには、一定のアカウント、アプリケーション、インフラがどうしても必要であるという現実に直面します。これらのシステムによって、単に重要な本番システムを復旧させるだけでなく、**セキュアな状態**での復旧を実現し、かつ組織が負っている各種の規制要件にも適合できるようにすることが可能になります。

Cohesityは、このようなインシデント対応と復旧の遂行に必要不可欠なインフラとリソースの最小構成を「最低限実現可能な対応能力 (MVRC) 」と定義しています。このMVRCに含まれる構成要素のいずれかを信頼できない、または利用不可能な状態にあると仮定してみてください。この場合、組織はそれらのリソースを迅速に再構築し、信頼できるツールセットを整えて、対応を進める必要があります。**Cohesityのクリーンルームソリューション**を使えば、組織はMVRCを迅速に信頼できる状態で再構築し、インシデント対応に必要なリソースを数分で利用可能にします。

攻撃の発生過程の把握

初期トリアージが完了し、破壊的なサイバー攻撃が進行中であるという確信が得られた時点で、アナリストはインシデントを宣言し、より深い調査を進めます。通常、ランサムウェアグループがサーバーやエンドポイントに暗号化ツール (エンクリプター) を展開するのは、攻撃の最後の段階です。これは、検知型のセキュリティ制御を最も作動させやすく、かつエンドユーザーにも影響が最も目に見える「騒がしい」段階だからです。

調査や修復作業の対象を暗号化されたシステムだけに限定してしまうと、攻撃の根本原因を特定することは困難です。むしろ、それ以外の範囲にも調査を広げる必要があります。暗号化されていないシステムの方が重要な手がかりを含んでいる可能性があり、そこには攻撃者が復旧後に再侵入するための「永続化メカニズム」が残されていることがあるからです。

このような深いレベルでの識別について詳しく見ていく前に、もう一つの重要な点を理解しておく必要があります。それは、ベストプラクティスに基づくインシデント対応プロセスの一要素である封じ込めが、この識別作業の妨げとなる可能性があるということです。

封じ込め

封じ込めは、すべてのインシデント対応フレームワークにおいて必須の要素です。攻撃の拡大を防ぎ、コマンド＆コントロール通信やデータ流出を遮断する役割を果たします。しかしながら、この「封じ込め」はセキュリティ運用チームにとっていくつかの課題ももたらします:

- **リモートイメージングは単独では機能しません。**現在、多くの組織はハードディスクを物理的に取得する方式から、リモートによるフォレンジックイメージングに移行しています。しかし、感染したホストやそのホストが属するネットワークを隔離すると、組織がこの調査作業を実施する能力が突然失われてしまう可能性があります。**DataProtect**は、インシデント対応者がファイルレベルでフォレンジック分析を行えるUIとAPIを提供しており、最新のスナップショットだけでなく、組織の保持期間内で保存された一連のスナップショット全体にわたって調査を行うことが可能です。これにより、デジタルフォレンジックアナリストは「時間をさかのぼる力」を得ることができ、攻撃者が既に痕跡を消去してしまったファイルやバイナリ、設定の差分 (デルタ) などを迅速に識別することが可能になります。従来のエンドポイントセキュリティソリューションやSIEM (セキュリティ情報イベント管理) は、ログの保持期間が限られているのが一般的ですが、Cohesityは、バックアップが保持されている全期間にわたり、イベントやログの内容を調査できるため、強力な証拠保全を保証するイミュータブルプラットフォーム上での対応が可能です。さらに優れている点は、この調査機能がネットワークに接続不要であることです。DataProtectはファイルシステムのオフラインコピーを使用するため、盗聴や妨害のリスクを受けることなく、セキュアに調査を行えます。

- **エンドポイントソリューションが隔離され、クエリとレスポンスのやり取りが不可能になります。**EDRやXDRなどのエンドポイントソリューションのアーキテクチャには違いがありますが、ほとんどの場合、エンドポイントからのテレメトリを受信する中央管理サーバーが存在します。封じ込めによってこの管理サーバーとエンドポイントとの通信が断たれると、アナリストは管理サーバーに既に送信されていた情報しか利用できなくなり、リアルタイムで「クエリ＆レスポンス形式」でエンドポイントを深堀り調査することができなくなります。
- 封じ込めには、インシデント対応と復旧作業を実施するための「隔離された環境」を構築することも含まれます。Cohesityのクリーンルームソリューションは、そうした環境を柔軟に構築できるアプローチを提供します。このソリューションにより、組織はインシデント対応におけるベストプラクティスに沿った行動が可能になり、セキュリティ部門とIT運用部門との間で適切な責任共有モデルを採用することができます。このアプローチは、復旧後の再感染を防ぎ、長期的なダウンタイムを回避する上でも有効です。

- Cohesityのクリーンルームソリューションの仕組み:
- MVRCや、影響を受けた、あるいは回避されたインフラを迅速にリストアできるようにし、インシデントの調査と是正に不可欠な体制を整えます。
- Cohesity Data Cloudプラットフォームのネイティブなセキュリティ機能と他のセキュリティツールを併用し、セキュリティ運用チームが攻撃の全体像をエンドツーエンドに把握し、将来の攻撃を防ぐための適切な是正措置を計画できるような、隔離された調査用の環境を構築します。
- セキュリティ運用チームの調査結果をもとに、是正措置を講じるための隔離された緩和環境を構築します。この環境では、既知の正常なインストールイメージや構成からの迅速なシステム再構築、システムの復旧と脆弱性へのパッチ適用、回避されないようにするためのコントロール強化などが行われ、将来的に同様の攻撃を防止・検知できる体制の構築が可能になります。最後に、システムを本番環境に復元する前に、機能性やパフォーマンスのテストを行うことができます。

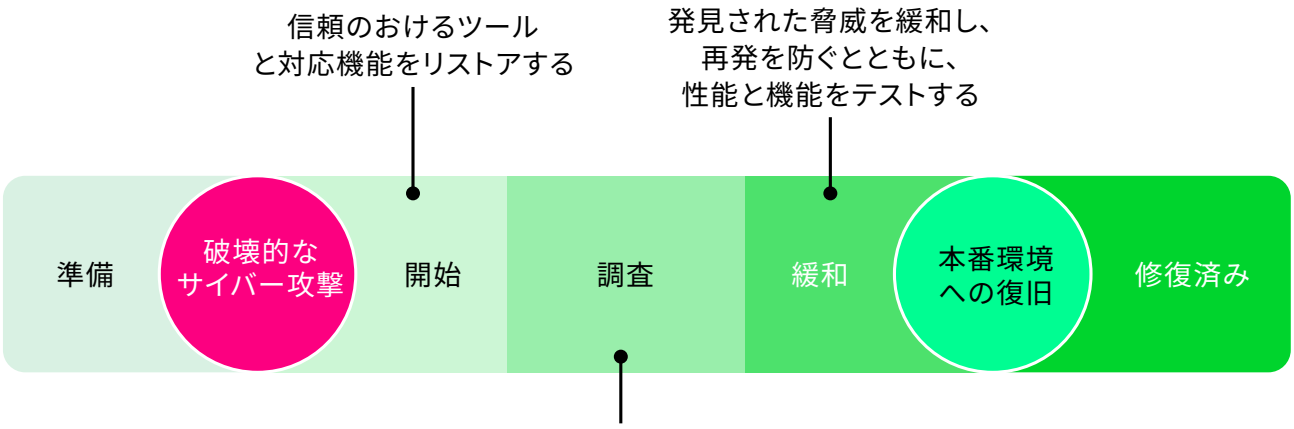

図3. サイバー攻撃からの是正措置に導く、Cohesityのクリーンルームソリューションの4段階

特定プロセスの見直し: Cohesityのクリーンルームソリューションによる支援

デジタルフォレンジックとインシデント対応のベストプラクティスに従った組織は、既に感染したネットワークとホストの封じ込めを完了しています。この段階では、インシデントの調査と修復に必要なインフラが信頼できる状態で再構築されており、インターネットへの接続、クラウドベースのIT・業務・セキュリティサービスの利用が再び可能になっています。また、社内外の関係者との通信手段も復旧されています。何より、セキュリティ・IT運用チームがインシデント対応と復旧を行うために必要なすべてのドキュメントやリソースに、すぐにアクセスできる状態にあります。

ここからは、封じ込めで隔離された環境下で調査対象の資産を扱う際、Cohesityのクリーンルームソリューションが「より深い調査」を支援する方法を詳しく見ていきます。

攻撃で悪用された脆弱性の特定

ランサムウェア集団や、ワイパー攻撃を事前に準備する国家レベルの攻撃者は、最も一般的に、インターネットに公開されている資産の脆弱性を利用して初期侵入を果たします。攻撃者の中には、脆弱性を悪用して侵入し、システムに永続化メカニズムを仕込んだ後に、他の攻撃者が侵入できないようにその脆弱性に自らパッチを適用するといった手口を用いるケースも確認されています。

組織は、攻撃の発生時点でどの脆弱性が存在していたかをどのように特定すればよいのでしょうか? これは、攻撃者によりシステムがワイプされていたり、封じ込め措置によって脆弱性スキャンが実行できなかったりすると、さらに困難になります。

Cohesity CyberScanは、Tenableの脆弱性管理ライセンスを活用して、バックアップスナップショットをスキャンできるようにすることで、組織に対する解決策を提供します。これにより、たとえシステムが封じ込めによってアクセス不能になっていたり、ワイプされていたり、侵入後に攻撃者自身によってパッチが適用されていた場合であっても、セキュリティチームは攻撃時点で存在していた脆弱性を特定することが可能になります。

ファイルシステムフォレンジックの実施

ファイルシステムフォレンジックは、インシデント対応の重要な分野です。多くの組織では、フォレンジックイメージングのためにリモート取得ツールを使用しています。しかし、一度封じ込め対策が講じられると、フォレンジックイメージングが必要なシステムには、もはやアクセスできないことがよくあります。

DataProtectは、アナリストに対し、ファイルシステムの単一スナップショットだけでなく、バックアップ保持期間全体にわたる時系列スナップショットへのアクセスを提供します。これにより、フォレンジック調査員は、インシデントのタイムラインをさかのぼって確認できるだけでなく、バックアップの保持期間全体にわたって調査を行うことが可能になります。一連の

図4. Cohesityのクリーンルームは、インシデント対応におけるベストプラクティスに準拠

ボリュームの時系列データを迅速にマウントし、比較することで、悪意のある差分を特定することができます。ファイルオブジェクトは、リバースエンジニアリング、動作検証、またはクラウドベースのサービスへの送信による解析のために抽出できます。

従来のデジタルフォレンジックでは、インシデント対応者は通常、攻撃後のシステムイメージを一つ取得し、その状態に至るまでの仮説を立て、それを裏付ける証拠を集めていきます。一方、DataProtectを使用すれば、たとえ封じ込め対策によって感染ホストが隔離されていても、インシデント対応者はより広範なインシデントタイムラインにわたってファイルシステムの変更履歴を可視化することができます。

脅威ハンティング

IoCのハンティングは、インシデント対応者が通常行うべきもう一つの作業です。この有事のハンティング活動は、大きく以下の2つのカテゴリーに分類されます:

第三者から提供されるIoCのスキャン: これらのIoCは、サイバー脅威インテリジェンスベンダー、政府機関、または他の組織 (同業他社など) といった第三者から提供されることがあります。Cohesityのユーザーは、DataHawkを利用することで、ランサムウェアや国家支援型行為者によって使用されている117,000件以上のIoCが頻繁に更新されるフィードを活用できます。DataHawkの脅威スキャン機能は、組織がライセンス契約を結んでいる**商用のCrowdStrike脅威インテリジェンスフィード**にも対応しており、他の第三者から提供されるYARA形式のIoCも取り込むことができます。

自組織で発見したIoCのスキャン: インシデント対応者が調査中に痕跡を発見すると、それらのIoCが組織全体のインフラに存在していないかを調べるハンティングを行います。その結果、インシデント対応の対象に追加すべきシステムがあるかどうかを判断します。

通常、このようなハンティングは発見された痕跡を記述するYARAルールを作成することで行われます。YARAルールは、不要な誤検知を避けつつ検出を可能にします。Cohesityを活用すれば、前節で述べた通り、フォレンジック分析を実施し、ファイルシステム上の痕跡を抽出し、Cuckooのようなサンドボックスで実行することが可能です。Cuckooはプラグインを通じて、当該ファイルに関連するIoCに基づくYARAルールを自動生成することもできます。DataHawkのハンティング機能はエンドポイントのエージェントに依存していません。システムが封じ込めのために隔離されている場合でも動作を継続できます。これは、エンドポイントセキュリティ製品によるハンティングを無力化してしまう一般的な防御回避技術の影響を受けません。

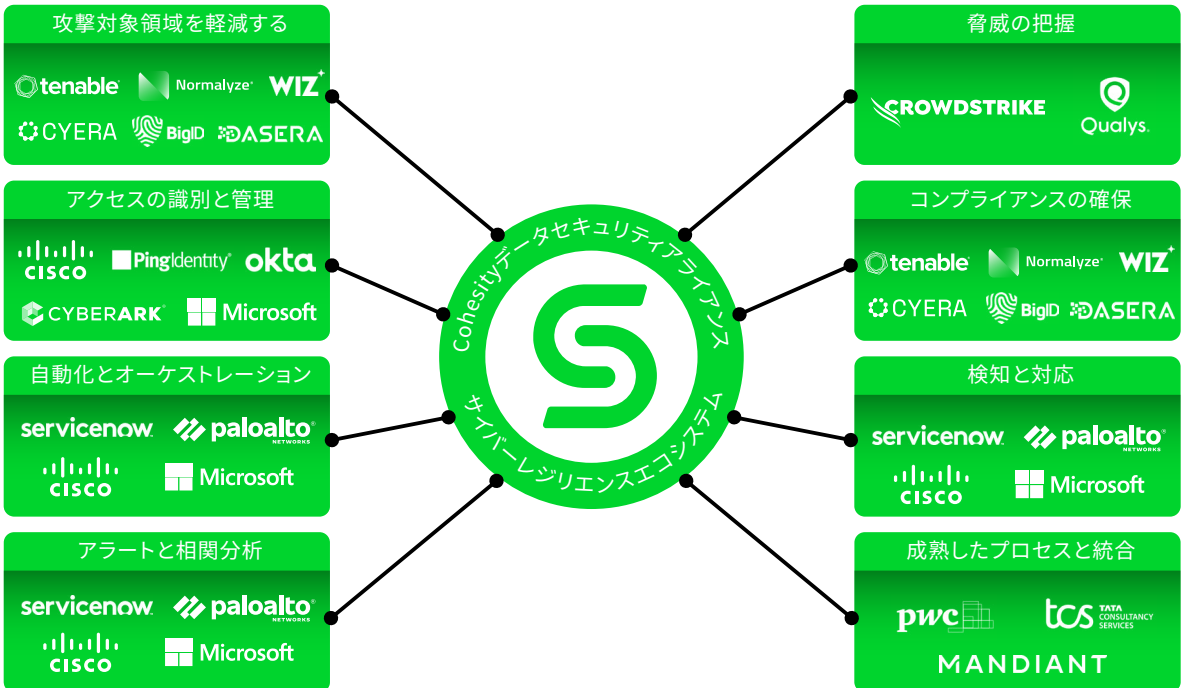

図5. Cohesityデータセキュリティアライアンス: サイバーレジリエンスのためのエコシステム

Cohesityグローバル検索のような機能により、インシデント対応者はバックアップされたインフラ全体を横断してファイルを迅速にハンティングすることができ、特定の痕跡やファイルを探す際の調査を効率的に進めることが可能になります。

規制遵守の実現

堅牢なインシデント対応プロセスの整備を義務付けるだけでなく、HIPAA、DORA、NIS 2など、最近改訂された多くのコンプライアンス規制では、サイバーセキュリティ侵害の発生時に、規制当局と影響を受けたデータ主体への通知を義務付けています。侵害の性質を理解することは、インシデント対応の識別フェーズの一部であり、その影響を把握し、速やかに通知することも同様に重要です。

インシデントによって通信手段が影響を受けた場合でも、CohesityはMVRCの一環として、通信機能のリストアを支援します。コミュニケーション用のテンプレートは、クリーンルームの基盤となるDigital Jump Bag™に保管しておくことができます。さらに、DataHawkはバックアップをスキャンして機密データや規制対象データを識別することができ、組織が規制要件を満たすのを支援します。これは、重要なデータストアが暗号化されたり消去されたりするような破壊的なサイバー攻撃の後に、特に価値の高い支援となります。

セキュリティ運用ツールの統合

サイバーレジリエンスはチームで取り組むべき課題であり、単一のベンダーのソリューションだけでインシデントの調査と是正をすべて完結させることはできません。そのため、Cohesityはデータセキュリティアライアンスを設立しました。この協調的なエコシステムにより、データそのもの、そして時間の経過に伴うデータの変化の力を、共通のガバナンス、調査、復旧のために、より広範なセキュリティツールやサービスへ統合することが可能になります。

自動化とオーケストレーション

CohesityはAPI連携に対応しており、SOAR (セキュリティオーケストレーション・自動化・対応) プラットフォームがこれらの調査タスクを駆動できるようになっています。これにより、アナリストの効率がさらに向上します。

根絶と復旧

Cohesityでは、根絶と復旧の段階を緩和に統合しています。なぜなら、Cohesityにとって、組織が破壊的なサイバー攻撃から復旧を試みる際には、再感染や同様の攻撃が再び成功しないように、適切な対策を講じることが不可欠であると考えているからです。

Cohesityのクリーンルームソリューションは、高速なボリューム復旧をサポートしており、脅威の除去対策を講じる前に、ファイルシステム全体を迅速に復旧することが可能です。これにより、セキュアなシステム復旧が実現されると同時に、信頼できるソフトウェアイメージや既知の正常な構成からのシステム再構築も迅速に行うことができます。各アプローチには長所と短所があります:

復旧とクリーンのアプローチ	
長所	**短所**
インシデント発生前の管理が容易	調査ではより詳細な分析が必要
	一般的に、是正措置に要する時間がシステムの再構築より長い
再構築のアプローチ	
長所	**短所**
データの復旧、システムの再構築、インシデントの調査を並行して行うことで、システムをセキュアな状態へ最短で復旧させる機会を提供する	システムが信頼できる状態にあるため、通常はそれほど詳細な調査を行う必要がない
是正措置にかかる時間は短く、通常は構成設定のセキュリティを確認し、コントロールを強化し、脆弱なシステムにパッチを適用する程度で済む	再インストール用スクリプトの作成にスキルが必要
	インストールメディア、ライセンスキー、構成ファイル、スクリプトは、Digital Jump Bag内に保管しておく必要がある

Cohesityのお客様の一部は、ボリュームレベルのバックアップとシステム再構築の両方をサポートすることを選択しています。これにより、各侵害ホストに対して、クリーンアップに必要な作業量や、攻撃の痕跡が残らないという確信の度合いに応じて、最も適切でセキュアな復旧方法を選択することが可能になります。

多くのお客様は、自社の開発環境をCohesityのクリーンルームによる緩和環境として再利用しています。このアプローチにより、隔離されたクリーンルーム環境での脅威の除去作業と並行して、本番サーバーを初期化することが可能です。この緩和環境は、Digital Jump Bagに保存された設定を使用して本番環境の構成を模倣するように設定されています。

調査フェーズで発見された脅威が、復旧やクリーンアップ、または信頼できる状態への再構築によって除去された後、システムテストを行うことができます。このテストは、機能テストやパフォーマンステストの形で実施され、是正措置、パッチ適用、コントロールの強化がシステムの提供能力に影響を与えていないことを確認します。

最後に、以下の2つの目的でシステムのスナップショットを取得します:

1. 攻撃の痕跡が見落とされていた場合でも、最初からやり直す必要はありません。是正措置後に取得したスナップショットは、新たな調査や追加の是正措置のベースラインとして機能し、次の調査段階に引き継がれます。
2. 緩和環境が本番環境を模して構成されているため、このスナップショットをそのまま「リフト＆シフト」して本番ネットワークへ展開することが可能です。

得られた教訓

サイバーレジリエンスを確立しようとするすべての組織は、継続的改善を信条として掲げるべきです。何がうまくいき、何がうまくいかなかったのか、そして何を改善できるのかを理解することは、継続的なダウンタイムを防ぎ、将来のインシデントにより効果的かつ効率的に対応するために不可欠です。ことわざにもあるように、「いかなる計画も、敵と接触するまでは完璧」です。現実世界の攻撃をシミュレーションすることは、技術的な復旧力をテストし、プロセス改善を促し、自動化の機会を特定し、アナリストやインシデント対応者に実戦感覚を培わせるためにも重要です。

Cohesityのクリーンルームソリューションの最大の利点の一つは、本番システムに影響を与えることなく、インシデント全体をエンドツーエンドでシミュレーションできる点です。DataProtectを使用すれば、本番システムをクローン作成し、これを社内のレッドチームや外部のペネトレーションテスト企業が用いて、エンドツーエンドのランサムウェア攻撃やワイパー攻撃をシミュレーションすることができます。その後、是正されたシステムのベースラインスナップショット取得直後まで、対応と復旧の全ワークフローを一貫して実行することができます。このような取り組みによって、組織は実際の攻撃に即したシナリオを通じて、適切な人材・スキル・プロセス・技術が整っているかを確認でき、破壊的なサイバー攻撃が現実に発生した際の影響を最小限に抑えられます。

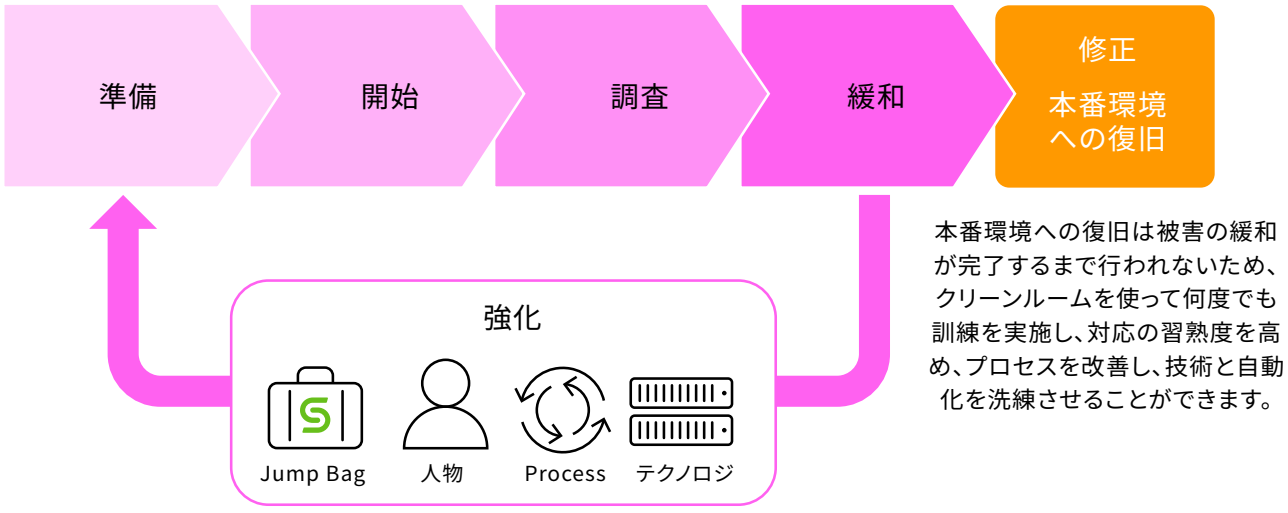

図6. Cohesityのクリーンルームソリューションは、現実的な訓練を通じて継続的な改善を可能にします。

まとめ

Cohesityは、復旧において大きな価値を提供し、有事におけるデジタルフォレンジックやインシデント対応の各段階を、効果的かつ効率的に行えるようにします。Cohesity独自のサイバーレジリエンス手法は、セキュアな復旧を達成するまでの時間を短縮し、同様の攻撃が再度発生しても、さらなるダウンタイムに繋がらないという確信を組織にもたらします。

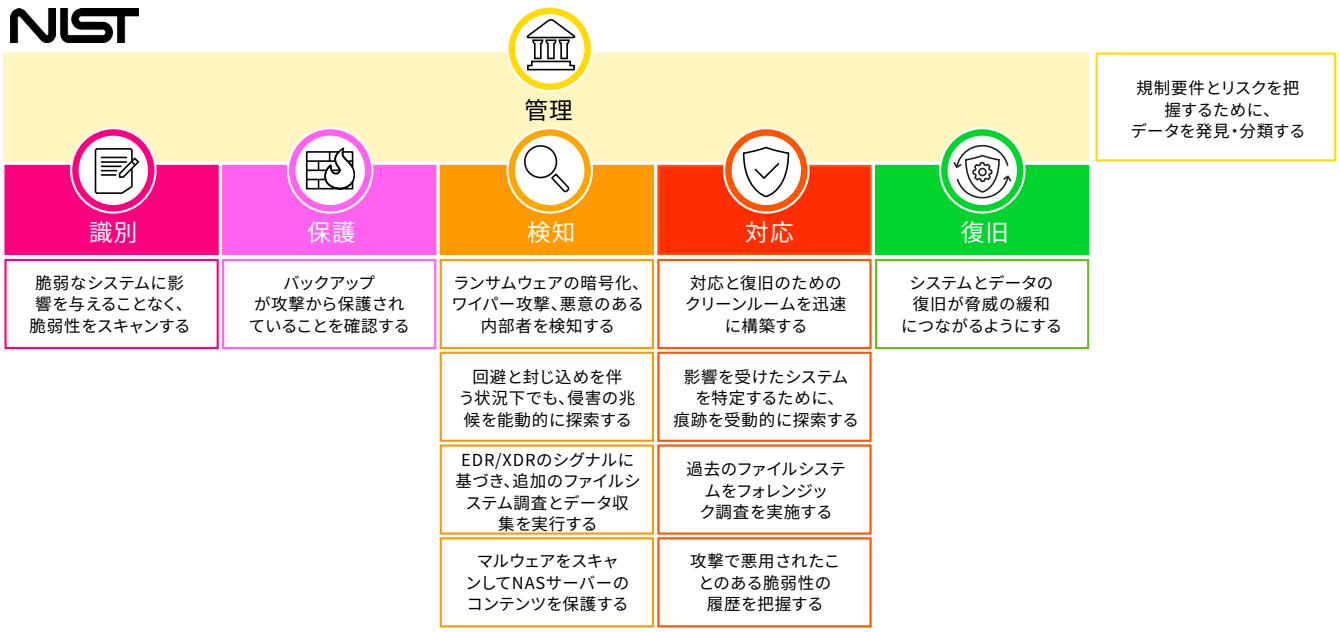

図7. Cohesityを活用して、サイバーインシデント対応や、NISTのサイバーセキュリティフレームワークのベストプラクティスを実現

Cohesityについて

CohesityはAIを活用したデータセキュリティのリーダーです。Fortune 100のうち85社以上、Global 500の約70%を含む13,600社を超えるお客様が、膨大なデータに対して生成AI (Gen AI) によるインサイトを提供しながら、Cohesityを利用してレジリエンスを強化しています。Veritas社のエンタープライズ向けデータ保護事業との統合により誕生したCohesityのソリューションは、オンプレミス、クラウド、エッジ環境におけるデータのセキュリティと保護を実現します。NVIDIA、IBM、HPE、Cisco、AWS、Google Cloudなどと連携し、Cohesityはカリフォルニア州サンタクララに本社を置き、世界各地にオフィスを展開しています。詳しくは、CohesityのLinkedIn、X (旧Twitter)、Facebookをご覧ください。

おすすめの資料

以下のホワイトペーパー、ガイド、およびブログ記事が、きっとお役に立つはずです。

- digital jump bag™でサイバーレジリエンスを強化
- 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のクリーンルーム設計のご紹介
- AIを活用したデータセキュリティに関するガイド: 飛躍的なビジネス成果を実現する方法
- 経営層のための最新データセキュリティとデータ管理ガイド
- 最新のデータセキュリティとデータ管理に関するトポロジー: ITリーダー向けガイド

Cohesityの詳細はこちら

COHESITY

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

2000058-002-EN 4-2025