COHESITY

ホワイトペーパー

digital jump bag™でサイバーレジリエンスを強化

最低限実現可能な対応能力 (MVRC) を迅速にリストアし、インシデント対応を強化する方法

目次

前文

James Blake
サイバーレジリエンス戦略
VP

私は30年以上にわたり、破壊的なサイバー攻撃やデータ窃取に対するサイバー対応の最前線に立ってきました。これまで、国家によるワイパー攻撃へのインシデント対応の指揮から、世界最大の銀行におけるサイバーリスク管理のリーダーまで、さまざまな経験を積んできました。

その中で私が学んだ重要な教訓の一つが、「ジャンプバッグ」の価値です。もともとジャンプバッグとは、攻撃を受けた物理的な現場に駆けつける際に持参する必須のハードウェアやソフトウェアを詰めた物理的なバッグのことを指していました。このバッグには、インシデントを迅速に調査し、証拠を収集し、脅威を緩和するための基本的なツールが詰め込まれます。

ハードウェアやソフトウェアだけでなく、組織内外の主要関係者の連絡先リストの印刷物、クライシスマネジメント計画書、想定されるインシデントに対応するためのワークフロー、携帯電話なども含まれていました。このジャンプバッグの目的は、インシデントに即座に対応できるよう準備をしておくことにあります。インシデント対応中のプレッシャーの中で必要なものを慌ててかき集めるのは、貴重な時間を浪費するだけでなく、重要なものを忘れてしまうリスクにも繋がります。ジャンプバッグには、ツール類、プロセスの詳細、コミュニケーション手段が入っていました。

現在私たちは、遠隔でのデータ取得、EDR/XDR (エンドポイントの検知と対応/拡張された検知と対応)、仮想マシン、クラウドインスタンスが当たり前となった時代に生きています。ジャンプバッグは今でも、現場に持ち込む物理的なコンテナとして使われています。しかし今では、digital jump bag™を準備することのほうが、はるかに実用的です。この保護された信頼性の高いリポジトリは、リモート取得や分析に必要なツールだけでなく、インシデント対応と復旧を成功に導くために必要なあらゆるデジタル資産への迅速なアクセスを提供します。

エグゼクティブサマリー

digital jump bag™はクリーンルームの基盤です。クリーンルームとは、セキュリティ運用チームが攻撃の発生経緯を把握するために必要な調査作業を行う、セキュアで隔離された環境を指します。また、脅威を排除し再発を防止するために、復旧前に是正措置を実施する場としても活用されます。digital jump bagに何を含めるかは、組織の成熟度、体制、プロセス、使用しているツールに応じて異なります。

digital jump bagの本質は、サイバー攻撃への効果的な対応に必要な最小限のツール、文書、プロセスで構成された最低限実現可能な対応能力 (MVRC: Minimum Viable Response Capability) を、迅速にリストアできるようにすることです。MVRCを整備することで、組織は侵害の封じ込め、重要業務のリストア、インシデント中のダウンタイム最小化を迅速に実現できます。

Cohesityクリーンルームソリューションは、破壊的なサイバー攻撃に立ち向かうための、こうした最新のアプローチを支援します。多様なニーズに柔軟に対応できるようにし、運用上のサイバーレジリエンスを継続的に向上させます。

本ホワイトペーパーでは、より強固でアジャイルなインシデント対応戦略を構築するにあたり、組織がdigital jump bagに含めるべき要素をご紹介します。

サイバーレジリエンスで見落とされがちな問題

破壊的なサイバー攻撃では、被害を受けた組織内で使用されているセキュリティツールを回避するケースが多くあります。特に、EDR/XDRの回避機能は、現在多くのランサムウェア攻撃を引き起こしているRansomware as a Service (RaaS) プラットフォームに、あらかじめ組み込まれていることが一般的です。EDR/XDRソリューションはその性質上、エンドポイントに設置され、回避されていなければ、プロセス、ネットワーク接続、ファイルシステムの優れた可視性を提供します。

インシデント対応のベストプラクティス (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、NIST SP800-61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、RE&CTフレームワーク、MITRE D3FENDなど) は、感染したネットワークやホストの隔離によってインシデントの拡大を防止することを推奨しています。エンドポイント制御の世界では、せいぜい組織が既に収集している情報だけでインシデントを調査せざるを得ないという制約が残ります。

しかし、常に進化し続ける攻撃者に直面する中で、事前にどの情報を収集すべきかを完全に把握できるとは限りません。そのため、調査や対応能力は手の打ちようがない存在になってしまうことがあります。同様に、影響を受けたホストのボリュームをリモートでフォレンジックイメージングしようとしても、接続が遮断されてしまえば不可能です。

セキュリティツールだけでなく、インシデント対応の調査、緩和、復旧フェーズには他にも多くのシステムが関与しています。これらのシステムはランサムウェアやワイパーのような破壊的なサイバー攻撃の影響を受けることがありますが、ビジネス影響分析の中では重要視されないことが多いのが現状です。私自身も、物理的アクセス制御が影響を受けたために、インシデント対応者が施設に入れなかった事例に関わったことがあります。また、多くの組織では、VoIPやメールサーバーが攻撃され、報道機関、規制当局、法執行機関、サイバー保険会社、影響を受けたデータ主体との連絡が取れなくなってしまうこともありました。さらに、多くの組織が実施するランサムウェア対応の机上演習は、こうした攻撃者のターゲットを絞った手法による影響を十分に反映できていません。なぜなら、攻撃者は組織がインシデント対応や復旧に苦労することを狙っているからです。

RaaSプラットフォームでは、最近パッチが当てられた脆弱性の悪用をわずか5日以内に組み込むこともあり、これらをシステム内で識別し、本番環境に戻す前に必ずパッチを適用する必要があります。そうしなければ、同じ攻撃者や、同じRaaSプラットフォームを使う別の攻撃者が再び侵入してきます。

また、インシデントの調査では、最初に影響を受けたシステム、いわゆる「ペイシェントゼロ」となる初期アクセス経路を特定し、そこからインシデントの経緯を追っていく必要があります。攻撃者がどのように持続的に侵入状態を維持し、権限昇格を行い、攻撃の他の痕跡を見つけているかを理解することは、復旧後の環境をセキュアな状態に保つために不可欠です。さらに、対応チームは、通知義務に対応するために、漏洩した可能性のあるデータの性質も把握しなければなりません。

暗号化されたシステムの分析だけでは不十分です。通常、ランサムウェアの攻撃者は、攻撃サイクルの最後の数分から数時間にかけて、暗号化プログラムを展開します。それまでの期間は、数日から数百日にわた

り組織のインフラ内に潜伏していることがよくあります。暗号化は非常に目立つ行為であり、セキュリティコントロールやユーザーの検知を引き起こす可能性があります。その時点では既に手遅れです。このようにスピードが求められるため、暗号化プログラムではデータの完全性を重視して設計されないことが多く、その結果、復号鍵の身代金を支払っても大量のデータ損失が生じるケースが少なくありません。攻撃者がどのように侵入してネットワーク内に居座り続けているのかを特定せず、暗号化されたシステムに限定して対応すると、重大な失敗を招く原因となります。

このような対応をする組織は、多くの場合、何度復旧しても再感染を繰り返してしまいます。この「悪循環」は、インシデントを適切に調査し、得られた知見をもとに脅威を是正することで解決されます。

少し想像してみてください。もし最後に実施した机上演習において、電話やメールが使えず、建物への立ち入りもできず、IDやアクセス管理システムも利用できなかったら、結果はどう変わっていたでしょうか?

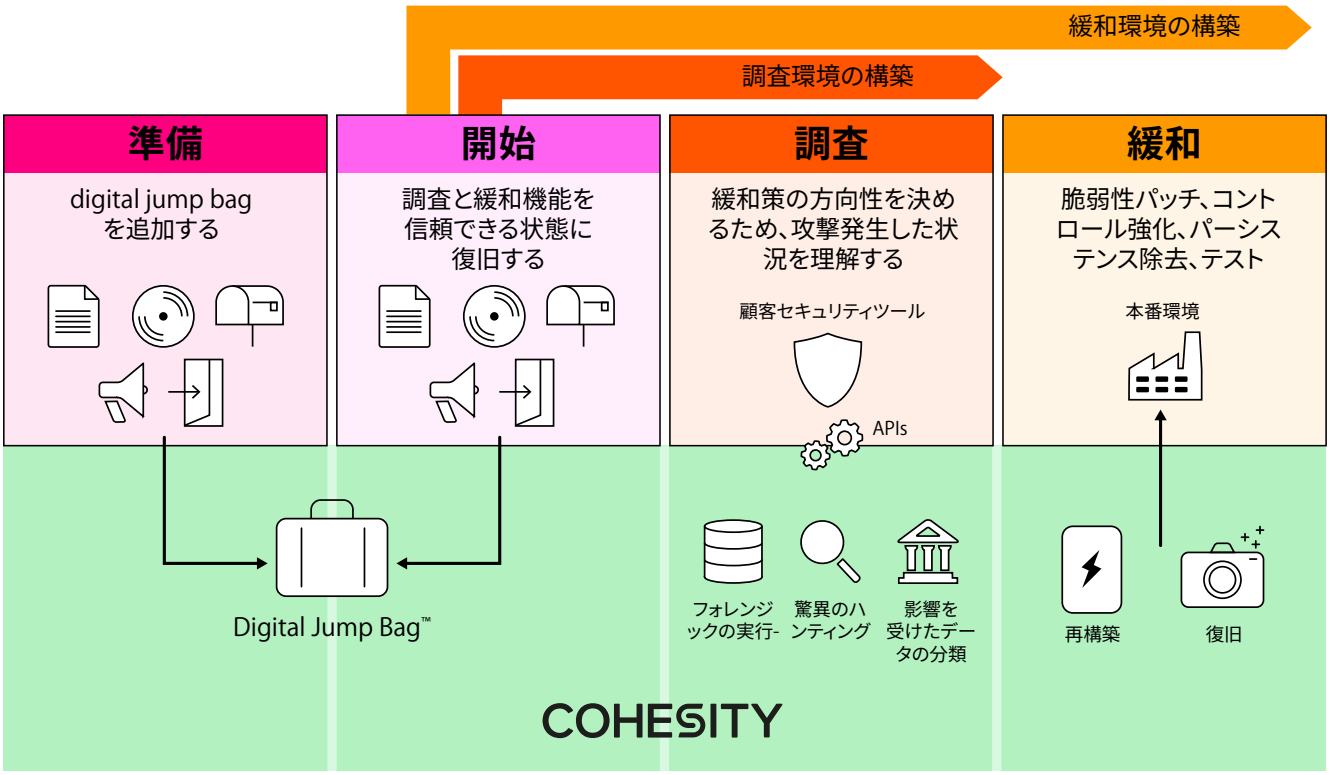
Cohesityクリーンルームソリューションにおけるdigital jump bagの役割

digital jump bagはCohesityクリーンルームソリューション全体の基盤であり、インシデント対応と復旧の重要なフェーズを支援します。これにより、組織はクリーンなデータを本番環境に安全に復元できるようになります (下図参照)。

各段階の内容を順に確認します。

準備

この段階では、digital jump bagに何を含めるかを選定します。例えば、緩和環境で復元される階層的かつ相互依存するシステムを支えるネットワークやハイパーバイザーの構成情報などです。後続の段階を円滑に進めるための推奨事項については、「digital jump bagの内容とは?」の セクションをご参照ください。



開始

この段階では、digital jump bagからコミュニケーション、コラボレーション、インシデント調査に必要なツールを復旧し、隔離されたクリーンルーム環境内の信頼できる状態にMVRCを再構築します。また、digital jump bagは調査環境と緩和環境も構築します。

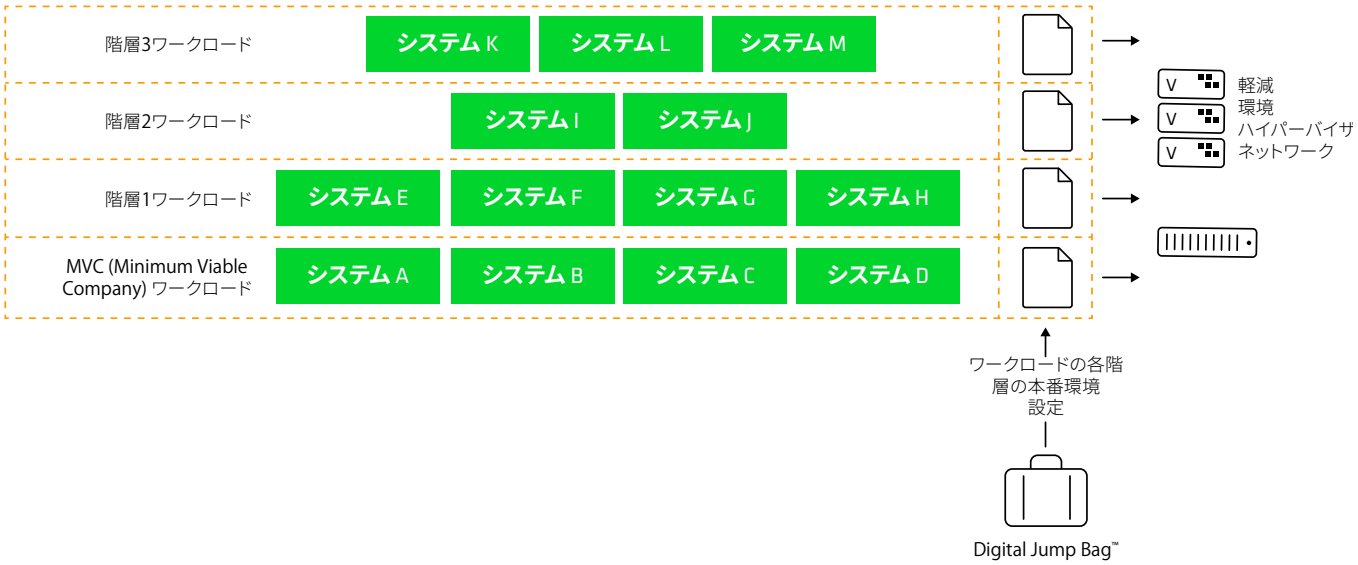
調査

セキュリティ運用チームは、隔離されたクリーンルーム内で信頼できる状態に復旧されたセキュリティツールと、データ分類、脅威ハンティング、ファイルシステム・フォレンジクスのためのCohesity固有の機能を活用して、インシデントにおけるエンドツーエンドの全体的なタイムラインを把握します。クリーンルーム内でセキュリティツールが信頼できる状態に復旧され、かつCohesityのセキュリティ機能はエンドポイント制御に対する防御回避技術の影響を受けないため、封じ込めによる回避や隔離の課題を克服できます。さらに、Cohesityのデータセキュリティアライアンスは、セキュリティオペレーションセンターで使用される多様なセキュリティベンダーツールを豊富に揃えており、これらはCohesityソリューションと連携するよう事前に構成されています。

緩和

IT運用チームは、セキュリティ運用チームがインシデントについて明らかにした情報をもとに、システムを復旧してクリーンアップするか、信頼できる状態に再構築するかを選択します。調査段階では、相互依存するシステムを含めた完全な復旧は行いませんが、緩和段階ではそれが求められます。

お客様の多くは、インシデント復旧期間中に開発環境を緩和環境として再利用しています。相互依存するシステムは、本番環境と同じネットワーク構成で緩和環境に展開されます。これらのネットワークまたはハイパーバイザーの構成は、相互依存するシステムの各階層ごとに、digital jump bagに保存されています。その内容は下図の通りです。



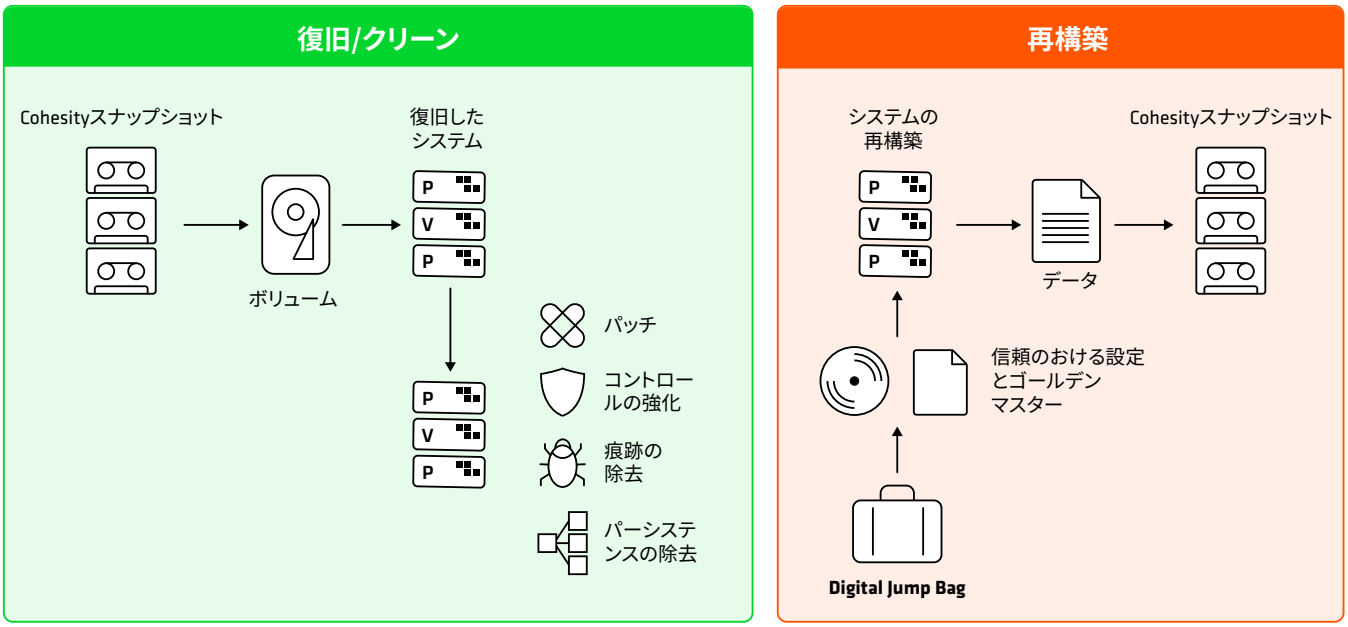
Cohesityクリーンルームとインシデント対応のベストプラクティスとの整合

Cohesityクリーンルームソリューションでは、「復旧してクリーンアップする」か「信頼できる状態まで再構築する」かの戦略を、インシデント時にシステムごとに、是正措置の労力や残留リスクに基づいて柔軟に適用できます。以下に各選択肢の簡単な説明を示します:

- **復旧してクリーンアップする**: システムはスナップショットから復旧され、調査段階でセキュリティ運用チームが示した緩和ステップが実施されます。データは通常、悪意あるペイロードを含まないため、システムの再構築と並行してデータの復旧が可能であり、最終的な復旧時間の短縮に寄与します。
- **システムを信頼できる状態に再構築する**: digital jump bagには、既知の正常な構成情報、インストールスクリプト、ゴールデンマスターのインストールイメージが含まれています。システムを再構築した後、復旧は再構築済みシステム上のスナップショットからデータを回復します。

「jump bagを活用した最低限実現可能な対応能力(MVRC)の確立」セクションでは、それぞれのアプローチの比較について詳述しています。

セキュリティ運用チームの調査ニーズに応える環境と、IT運用チームが緩和策を適用して安全な状態への復旧を確実に行う環境の両方を整備することは、組織が効果的かつ適切なサイバーレジリエンスにおける責任共有モデルを実現するのに役立ちます。このアプローチは、ITとセキュリティ運用のリソースを最大限に活用できるようにすることで、セキュアな復旧をより迅速に行えるよう最適化します。



Cohesityクリーンルームは、ワークロードを復旧してクリーンアップするか、信頼できる状態へ迅速に再構築するかという選択肢をお客様に提供します。

システムが再構築または復旧された後、該当するワークロードの階層に対して機能テストおよび性能テストを実施できます。テスト完了後にスナップショットを取得し、その後、相互に依存するワークロード全体を本番環境へリストアします。この時点で、インシデントの全範囲が調査され、脅威が緩和され、性能と機能がリストアされていることが確信できます。これらのテストケースは、各依存関係のあるワークロードの復旧階層ごとにdigital jump bagに保管しておくことが可能です。調査や緩和の過程で見落としがあった場合でも、緩和フェーズ終了時に取得したスナップショットを基盤としてさらなる調査と緩和を実行できるため、最初からやり直す必要はありません。

Cohesityクリーンルームとインシデント対応のベストプラクティスとの整合性

Cohesityのdigital jump bagとMVRCは、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」、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」、RE&CTフレームワーク、MITRE D3FENDに示されたサイバーインシデント対応のベストプラクティスと整合しています。このアプローチにより、これらの方法論を既に採用している組織は、Cohesityクリーンルームソリューションを既存のワークフローに容易に統合することができます。また、インシデント対応と復旧の成熟度を向上させたいお客様は、Cohesityクリーンルームソリューションを採用することで、これらのベストプラクティスを実践的に運用できるようになります。

Cohesityクリーンルームとインシデント対応のベストプラクティスとの整合

セキュリティとITオペレーションの連携でレジリエンスを実現

サイバーレジリエンスはチームスポーツです。IT運用部門、あるいはセキュリティ運用部門だけで完結するものではありません。統合されたプロセスと補完的なツールを持つことが必要です。また、単一のベンダーがサイバーレジリエンスをすべて提供できるわけでもありません。Cohesityクリーンルームソリューションは、セキュリティ運用チームが調査環境を活用し管理できる一方で、IT運用チームが緩和環境を所有し活用できるよう設計されています。このようなチーム間の役割分担と引き継ぎにより責任共有モデルが確立され、作業の抜け漏れを最小限に抑えることが可能になります。インシデントの初期調査や緩和で攻撃の一部を見落とした場合でも、既に緩和済みのスナップショットを調査段階に遡って繰り返し復元できる機能により、調査時間と最終的な復旧時間を短縮できます。

セキュリティ運用チームが調査環境でワークロードの調査を完了次第、IT運用チームおよび緩和環境へ引き渡して再構築、復旧、クリーンアップを実施します。これにより、IT運用とセキュリティ運用のリソースを最も効率的に活用することが可能となります。

より迅速な対応、よりスマートな復旧: Cohesity CERT (サイバー事案対応チーム)

多くの組織は効果的なサイバーインシデント対応の専門知識やリソースを欠いています。影響を最小限に抑えるため、Cohesityは専任のサイバー事案対応チーム (CERT) サービスを導入し、世界トップクラスのデータセキュリティソリューションをさらに強化しています。

Cohesity CERTは、エキスパートによるサイバー攻撃からの迅速な復旧を提供するため、ダウンタイムを最小限に抑えながら、データを確実にリストアしてオペレーションを迅速に再開することができます。

また、既存のサブスクリプションの一環として、Cohesityのすべてのお客様にご利用いただけます。

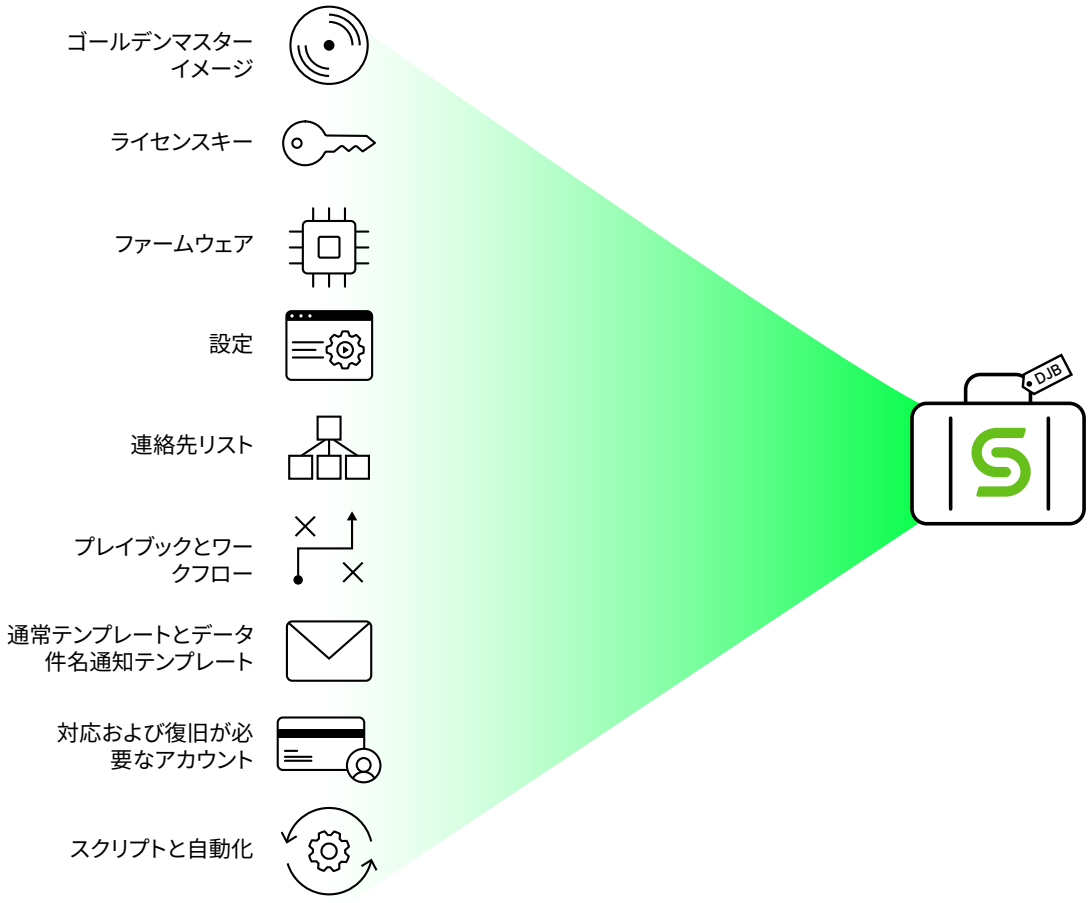
digital jump bagの内容とは?

digital jump bagの内容は、各組織のトリアージ、調査、緩和のプロセスや、それらを実現するために使用しているツールによって異なります。

一般的に、Cohesityのお客様のdigital jump bagには、以下の項目がよく含まれています:

ドキュメント

- 法執行機関、情報共有・分析センター、保険会社、契約しているインシデント対応チーム、規制当局などの外部組織に加え、社内関係者も含む連絡先リスト
- ネットワーク図
- 組織の構成管理データベース (CMDB) のバックアップやダンプファイル (存在する場合)
- インシデント対応のランブック/ワークフローのコピー
- インシデント対応サービスの委託契約書、サイバー保険に関する契約書とポリシー文書
- アプリケーションやツールのユーザーマニュアル



初期段階のリソース: コラボレーションとコミュニケーション

- 法執行機関、情報共有・分析センター、保険会社、契約しているインシデント対応チーム、規制当局、報道機関、影響を受けたデータ主体などの外部関係者や内部関係者とのコミュニケーションが必要になる可能性があります。この体制を整えるため、digital jump bagに以下のようなものが含まれることがあります:
  - セキュアな接続を確保するための、既知の正常なルーターとスイッチのファームウェアと設定 (もしくは、組織で信頼できる待機機器を保有している場合もあります)
  - 対応と復旧に必要なリソース (Cohesity Heliosへのアクセスを含む)に対してのみ入出力を制限するための、ファイアウォールソフトウェアと設定
  - 調査環境と緩和環境を含む他システムの再構築の基盤として使用される、ベースOSのインストールメディアとライセンスキー
  - Windowsの無人インストール用Answerファイルから、Ansibleプレイブック、TerraformによるInfrastructure as Codeまで、さまざまな自動化とオーケストレーション用スクリプト
  - 音声通信管理 (VoIP) サーバーのソフトウェアと設定。これは本番のVoIP環境全体ではないことを理解しておくことが重要です。対応と復旧活動に関連する回線のみが含まれます。調査完了後、発見された脅威が緩和され次第、本番VoIP構成はオンラインに戻されます。
  - メールサーバーのソフトウェアと設定。VoIPサーバー同様、本番環境の機能ではありません。対応と復旧活動に必要な通信のみを可能にします。
  - 組織で使用されているチケット管理や会議ツールなど、その他のコラボレーションツール
  - 規制当局や影響を受けるデータ主体への通知用テンプレート

調査段階環境のリソース

セキュリティ運用チームは通常、調査フェーズで使用される環境を管理しています。この環境では、攻撃のタイムラインをエンドツーエンドで把握することに注力し、組織が本番環境の復旧に関して適切な判断を下せるようにするとともに、再感染や再攻撃を防ぐための対策を講じます。組織内では、Cohesityのネイティブなセキュリティ運用機能を活用して、データ分類、脅威ハンティング、ファイルシステム・フォレンジックなどの作業を行うほか、Cohesityは他のセキュリティ運用ツールのサポートも提供します。Cohesityによる脅威ハンティングは、インシデントの封じ込めに影響されません。このハンティングはパッシブなため攻撃者に検知されず、エンドポイントセキュリティ製品に一般的な回避技術の影響も受けません。調査環境では、システムは通常、隔離された状態で調査されます。

- セキュリティソフトウェアのインストールメディアと設定。これにより、クリーンルーム内の信頼できる状態へツールを再インストールでき、ツールや対応活動が回避されたり妨害されたりしていないことを確信できます。
- セキュリティツールはクリーンルーム内の信頼できる状態に再インストール可能です。このツールセットは、セキュリティインシデント対応チームの好みに大きく依存しますが、一般的に以下のようなものが含まれます:
  - Palo Alto Networks、Cisco XDR、CrowdStrikeといった、EDR (エンドポイントの検知と対応) やXDR (拡張された検知と対応) ツール
  - Dissect、Flare、Redline、Sleuth Kit、Autopsy、CyLR、UAC (Unix-like Artifacts Collector) のようなフォレンジック収集・分析ツール
  - Cortex、Kuiper、MISPなどの侵害指標 (IoC) や証拠共有ツール
  - Event Log Explorer、Event Log Observer、Hayabusa、LogonTracer、Windows Event Log Analyzer (WELA) などのイベントログ解析ツール
  - Qualys、Rapid7 neXpose、Tenable Nessus、OpenVASなどの脆弱性スキャナー

– Wiresharkなどのパケットキャプチャ・解析ソフトウェア

– Netflow/SFlow解析ツールVolatility、Memoryze、Orochi、Rekall、WindowsSCOPEなどのメモリキャプチャ・解析ツール

– Cuckoo、CAPA、CAPE、Ghidra、Joe Sandbox、Mastiff、Radare 2、Valkyrie Comodoなどのサンドボックス、マルウェアのリバースエンジニアリング・解析ツール

– Internet History ForensicsのようなWebブラウザ履歴フォレンジックツール

– これらの多くは、Kali LinuxやSANS InstituteのSIFT Workstationといったセキュリティソフトウェアディストリビューション内で利用可能です。各ツールを個別にインストールする代わりに、これらをdigital jump bag内に格納しておくことができます。

緩和段階環境のリソース

IT運用チームは通常、緩和環境を管理しています。緩和環境では、システムのOSやアプリケーションが、digital jump bagに保存された信頼できるインストールメディアと構成情報から再構築されるか、バックアップスナップショットから復旧されます。その後、調査段階でセキュリティ運用チームが得た情報をもとにクリーンアップが行われます。脆弱性のパッチ適用や、将来の同種攻撃を防止・検知するための不足しているコントロールやルールの適用など、脅威を緩和するための是正措置が講じられます。また、持続的侵入のメカニズム、悪意あるアカウント、その他の攻撃の痕跡も除去されます。緩和環境では、製品やサービスを提供するための相互依存するシステムが集められ、再構築または緩和処置が行われます。最終的に、バックアップスナップショットからデータをリストアして、性能と機能のテストが実施されます。この時点でスナップショットが取得され、システムは本番環境に復旧されます。

- 組織が「復旧してクリーンアップする」方法ではなく「再構築」を選択した場合、digital jump bagにはアプリケーションスタックに必要なインストールメディアと構成情報が含まれます。
- 現在の相互依存するワークロードに必要なネットワークまたはハイパーバイザーの構成。これにより、緩和環境はワークロードが最終的に復旧される本番環境を再現できます。
- ワークロードのテストケース

jump bagを活用した最低限実現可能な対応能力 (MVRC) の確立

digital jump bagを使ってMVRC内のシステムを構築する際、お客様には、事前に構築されたシステムを復旧するか、信頼できるソースから再構築するかという2つの選択肢があります。

- **最低限実現可能な対応能力 (MVRC) を維持する:** MVRCに必要なシステムを構築し、それらのボリュームレベルのバックアップを取得してdigital jump bagに保存します。もし、対応や復旧に必要なシステムに影響を与えるサイバーセキュリティインシデントやセキュリティツールの回避が疑われた場合、これらのスナップショットを復旧してMVRCを確立します。
- **digital jump bagのリソースから再構築する**: ここでは、MVRCに必要なシステムの信頼できる構成情報やゴールデンマスターイメージがdigital jump bagに保存されています。サイバーセキュリティインシデントによって対応や復旧に必要なシステムに影響が及ぶ、もしくはセキュリティツールの回避が疑われる場合には、digital jump bagがマウントされます。これらのシステムは、スクリプトやオーケストレーションツールを用いて再構築されます。

各戦略には下表に示すようなメリットとデメリットがあります:

MVRCを維持、バックアップ、インシデント発生後のスナップショットからのリストア	
メリット	**デメリット**
対応中の機能的なシステムへの迅速なアクセス	パッチ適用やアップデートには、再構築、更新/パッチ適用、バックアップといった複数のステップが必要であり、継続的なリソースも求められます。これらのステップは、対応や復旧に影響を及ぼすエラーを引き起こす可能性もあります。もし組織がITシステムの安全性を維持できず、インシデントの影響を受けていた場合、構築しバックアップされたMVRCシステムが同様の問題を抱えないと保証できるでしょうか?
必要な要素のみをリストア可能	digital jump bag内で指数関数的に多くの容量を占有し、ライセンスコストが発生する
	対応中に更新やパッチ適用が必要となる場合があり、遅延を引き起こす可能性がある
	インフラストラクチャの依存関係を生じる可能性がある
要件	
digital jump bagからMVRCを構築し、テストを成功させる	
MVRCのバックアップを取得し、法的目的で保全するために訴訟ホールドを有効化し、複製およびオフサイトアーカイブを行う	

インシデント発生後、信頼できるソースからMVRCを再構築する。	
メリット	**デメリット**
比較的容易にソースを維持できる。例えば、OSやアプリケーション、構成の新バージョンが出た場合、それを単純にジャンプバッグにエクスポートすればよい。	インフラの再構築に時間がかかる
レプリケーションとアーカイブによる持ち運びやすさ	
ハードウェアやプラットフォームの変更に柔軟	
digital jump bag内のバックアップのフットプリントは大幅に小さくなる (例えば、Windows Server 2025のイメージ1つが約3.6GBで、複数のシステム間で共有可能なのに対し、そのイメージを使用したMinimum Viable Response Capabilityの各サーバーは約35GBを必要とする) 。	
要件	
digital jump bagを追加してアップデートするプロセスを確立する	
コンテンツを使用していくつかのシナリオを実施する	
必要なハードウェアを手元に置くか、既存のハードウェアを安全にワイプするプロセスを定義する	

結論

巧妙化し破壊性の増すサイバー攻撃に直面する中、組織はリアクティブな復旧から戦略的なレジリエンスへと移行しなければなりません。そのためには、包括的なdigital jump bagをインシデント対応戦略に統合し、サイバー攻撃に迅速に対応できる態勢を整える必要があります。十分に準備されたdigital jump bagは、MVRCを実現し、クリーンルームの基盤となります。これにより、セキュリティチームはインシデントの調査、脅威の封じ込め、そして最小限の影響での業務リストアに必要なツール、プロセス、ドキュメントを備えることができます。

Cohesityクリーンルームソリューションは、インシデント対応を迅速化し調査を支援する信頼性の高い環境を提供するとともに、二次攻撃のリスクを最小限に抑えます。

モジュラー設計により、Cohesityは迅速に隔離環境を構築し、対応と復旧プロセスを支援するとともに、チームが協力して脅威の緩和をより迅速に進められるようにします。

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12,000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ノゼに本社を置き、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。

Cohesityがどのように最新のデータセキュリティの実現を加速するかについては、www.cohesity.com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、ブログがきっとお役に立つはずです。

- 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
- 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生み出す方法
- 経営層のための最新のデータセキュリティとデータ管理に関するガイド

Cohesityの詳細はこちら

COHESITY

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

2000056-002-EN 4-2025