# 組織のサイバーレジリエンスを向上させる

# 5つの重要なステップ

COHESITY

*どこでも回復力を発揮*

# はじめに

ランサムウェア攻撃が増え、その影響がますます深刻化していることは、現代のサイバーセキュリティ体制に課題があることを浮き彫りにしています。予防に多額の投資を行ったとしても、今日の脅威に対抗するには十分ではありません。

残念ながら、サイバー攻撃は今後もなくなることはないでしょう。その頻度、深刻度、規模のいずれにおいても、サイバー攻撃は常に変化し続けています。

ここまでは、厳しい現実の一部です。

でも、ご安心ください。実績のある方法を使えば、サイバー攻撃への耐性は高められます。実際、貴社のような企業がすでにこの手法で考え方を変え、成果を出し始めています。

---

**このeBookでは、サイバーレジリエンスに向けた5つのステップとして、このプレイブックをご紹介します。5つのステップすべてにおいて具体的な行動を取ることで、サイバー対応と復旧に関するベストプラクティスに沿った取り組みが可能になります。セキュリティ、コスト削減、リスク軽減の面でも、大きなメリットが得られます。**

## 簡単な背景説明

**ランサムウェアなどのサイバー脅威に対する認知度が高まっているにもかかわらず、サイバー攻撃は依然として業務、財務、評判に甚大な損害をもたらし続けています。実際、サイバー攻撃は世界中の企業にとって最大の脅威です。**

**実際に以下のような経済的損失が生じています:**

**54万ドル**
ダウンタイム1時間あたりの損失額[1]

**10億米ドル以上**
ランサムウェアに対する年間支払額[2]

**Sophos社の「ランサムウェアの現状2024年版」[3]では、さらに衝撃的な統計が報告されています:**

調査対象となった組織のうち、59%が昨年ランサムウェアの被害を受け、**そのうち94%がバックアップを標的にされたと回答しました。**さらに、**バックアップへの侵害は57%が成功していました。**

**さらに、以下のようなデータもあります:**

- **70%の攻撃がデータを暗号化**
- **身代金として要求された金額は平均200万ドル**
- **復旧までに1か月以上要した組織は34%**

今こそ、新しい、より効果的な戦略、機能、ソリューションが必要な時です。

[1]Splunk、「ダウンタイムの隠れたコスト: グローバル2000が直面する4,000億ドルの問題 (https://www.splunk.com/en_us/pdfs/gated/ebooks/the-hidden-costs-of-downtime.pdf)」
[2]Chainalysis、「ランサムウェアの支払いは2023年に10億ドルを超え、2022年の減少後に過去最高を記録」、2024年2月7日: https://www.chainalysis.com/blog/ransomware-2024/
[3]Sophos、「ランサムウェアの現状2024年版: https://www.sophos.com/en-us/content/state-of-ransomware」

### サイバーレジリエンスが特に困難になる理由は2つあります:

**1. サイバー復旧は災害復旧とは異なる**

組織に堅牢な災害復旧プロセスが導入されているとしても、それだけではサイバー攻撃からの復旧には対応できません。

火災や洪水、停電、設定ミスといった災害であれば、原因を迅速に特定し、対応を進めることができます。しかしサイバー攻撃では、数百もの事象が同時多発的に発生しており、それらをひとつひとつ調査・修復する必要があります。さらに、攻撃者が復旧作業を妨害し、身代金の支払いを迫ってくることもあります。

**2. 知識豊富な組織や専門家でさえ、ランサムウェア攻撃がどれほど破壊的であるかを過小評価する可能性がある**

信頼できるシステムが復旧の助けになると考えたり、何が起こったのかを把握するためにデータや証拠に頼ったりするかもしれません。

しかし、サイバー攻撃の場合、その調査に使いたいはずのシステムそのものがダウンしていたり、システムが回避されたり侵害されている可能性もあります。正常なデータと不正なデータが混在すると、復旧までの道のりは長く、より困難になります。そのため、多くの優れた組織であっても、迅速で確実、かつクリーンな復旧に今なお苦戦しているのが現状です。

# サイバーレジリエンスを向上させる**5つの重要なステップ**を確認

**これは実践的な設計図だとお考えください。各ステップを踏むごとに、サイバーレジリエンスの成熟度が確実に高まっていきます。**

ステップ1

# すべてのデータを保護

**簡単に聞こえるかもしれませんが、多くの組織がまだこの重要な最初のステップを踏んでいません。その原因は、データの無秩序な増殖にあると考えられます。**

オーガニックデータの増加により、断片化とサイロ化が進み、攻撃対象領域が大幅に拡大し、組織はこれまで以上に危険にさらされることになります。同時に、大規模なデータの管理と保護は、運用効率にますます大きな負担をかけます。

このように、より多くのデータがより多くの場所に存在し、それを効率的に管理する能力が低下している状況により、攻撃者にとって格好の環境が整っています。

## ステップ1の注目すべき利点

- ☑ セキュリティの強化
- ☑ リスクの低減
- ☑ コンプライアンスとガバナンスの向上
- ☑ コスト削減とROI改善
- ☑ IT効率の向上

## ステップ1を実行する重要なアクション

**1. 次のような1,000以上のデータソースをサポートする、最新のデータプラットフォームを導入:**

- 仮想マシン (VM)
- SaaSアプリケーション
- データベース
- NAS環境 (非構造化データ)

**2. プラットフォームがオンプレミス、クラウド、SaaS環境で動作することを確認**

あらゆる場所にデータが存在するため、プラットフォームには共通のUIとAPIによって統合された柔軟な導入モデルが必要です。

**3. 直感的なUIで操作をシンプルにする**

使いやすいUIがあれば、比較的小規模なチームでも大規模なシステム全体をスムーズかつ無駄のない運用が可能です。当社のお客様は、単一のUIとAPIのセットによって、プラットフォーム上でワークフローを自動化し、効率的な運用を実現しています。

**4. 強力なストレージ圧縮を実現**

強力なデータ圧縮機能を備えたプラットフォームを使用する必要があります。これにより、ペタバイト規模で実行する場合、大幅な節約が実現します。当社には、業界標準の独自のファイルシステムがあります。非常に強力なストレージ圧縮により、TCOが削減されます。

ステップ2

# データが常に復旧可能であることを保証

**攻撃者はバックアップを標的にします。攻撃者は、この最後の防衛線に影響を与えることができれば、組織には他に手段がないため、身代金を支払う可能性がはるかに高くなることを分かっています。**

最新のデータプラットフォームであれば、最初から復旧可能なバックアップが保証されていると考えたくなりますが、それは必ずしも事実ではありません。

攻撃者のアクセスを困難にし、万が一侵害された場合にもクリーンなバックアップから確実に復旧できるようにするには、複数の対策が必要です。

## ステップ2の注目すべき利点

- ☑ **より迅速でセキュアな復旧**
- ☑ **攻撃に対する保護の強化**
- ☑ **監査対応**
- ☑ **ゼロトラストの準拠**

## ステップ2を実行する重要なアクション

**1.** **次のような強力な機能を構成してプラットフォームを強化:**

- 多要素認証 (MFA)
- イミュータビリティ (データの変更や削除が不可能)
- ロールベースのアクセス制御 (RBAC)
- 職務の分離 (重要なタスクを複数の担当者に分割)

**2.** **サイバー保管を実装**

最も重要なデータのエアギャップコピーと、**3-2-1-1 バックアップルール** (データのコピー3つ、異なるメディア2つ、オフサイト1つ、イミュータブル1つ) を遵守することで、緊急時にいつでもデータのコピーを利用できるようになります。

Cohesityでは、高度なキー管理システムも提供しているため、攻撃を受けた場合でも顧客のデータへのアクセスが可能です。

このアクセスにより、バックアップは常に復旧可能になります。

ステップ3

# 脅威を検知して調査

**このステップは、脅威スキャン機能と脅威ハンティング機能を組み合わせた機能に関連しています。**

## ステップ3の注目すべき利点

- **早期の脅威検知と緩和**
- **バックアップの整合性を保証**
- **インシデントからの復旧を迅速化してダウンタイムを短縮**
- **ITチームと情報セキュリティチームの共通認識**

## ステップ3を実行する重要なアクション

**1.** バックアップの脅威を定期的にスキャンして、予防的に対処してください。このプロアクティブな**脅威スキャン**を、一貫した衛生管理の実践のように考えてください。これには、次のようなメリットがあります:

- 変更が加えられた箇所を可能な限り早く特定して排除する
- マルウェアやその他の脆弱性を識別する

**2.** 特定の脅威を探す時に**脅威ハンティング**機能を起動します。Cohesityが厳選した脅威フィードと、CrowdStrike社、Palo Alto Networks社、Cisco社など、データセキュリティアライアンスに加盟するセキュリティエコシステムベンダーとの統合により、これらのベンダーの集合的な知見と、Cohesityがこれらのシステムにもたらすデータを組み合わせたメリットが得られます。

また、情報セキュリティチームとITチームが同じ情報基盤で運用できるため、対応の一貫性とスピードが向上します。

これまで長年にわたり、私たちはお客様のサイバー攻撃からの復旧を支援してきました。その中で明らかになったのは、ネイティブな脅威スキャンと脅威ハンティング機能が、データプラットフォームに不可欠であるということです。

これはなぜでしょうか? それは、攻撃を受けている最中には、他のセキュリティシステムが無効化されていることや、オフラインになっている可能性があるからです。

ステップ4

# アプリケーションのレジリエンスを実践

**「実践」に関しては、先述のステップ1〜3を実行していれば万端です。ここまでに、プラットフォームを立ち上げ、強化し、サイバー保管を使用して導入を拡張しました。**

**また、定期的な脅威スキャンと脅威ハンティングの良い経験を積んできました。順調です!**

このステップ4では、インフラ、データ、アプリケーションの対応と復旧プロセスを実際に実践することで、準備レベルを次のレベルに引き上げます。実際の攻撃中に、システムがダウンし、極度のプレッシャーの中で初めて対応しようとしても、それでは手遅れです。

「すべてをオンラインに戻すのは時間のかかるプロセスです。定期的にテストしながら日常業務を続けるにはどうしたらいいのか?」と考えている方もいるでしょう。

## ステップ4の注目すべき利点

- ☑ **より高速で安全な復旧**
- ☑ **RTOの改善**
- ☑ **再感染のリスク低下**
- ☑ **中断と金銭的リスクの軽減**

**ここでオーケストレーションが役に立ちます。**

オーケストレーションを活用すれば、インシデント対応や復旧のワークフローを自動化でき、攻撃後のシステム復旧をリハーサルすることも可能になります。こうしたリハーサルにより、対応と復旧の習熟度が高まります。また、オーケストレーションを通して、手動作業を減らしつつプロセスの最適化が進みます。

自動化の重要な例を1つ挙げます。Cohesityのクリーンルームソリューションでは、分離された環境を立ち上げてフォレンジック分析を実施することができます。そこで感染データを詳細に調査し、何が起きたのかを把握し、攻撃のアーティファクトを完全に排除することで、復旧に向けた安全性を確保できます。このアプローチは、スピード、自動化、強力なフォレンジックを独自に組み合わせて提供し、インシデント対応者がITチームと連携できるようにします。その結果、サイバー対応と復旧が迅速化されます。

このステップでは、Cohesity CERT (サイバー事案対応チーム) とも連携します。これらの専門家は、巧妙なランサムウェア、データ漏洩、ターゲットを絞った攻撃など、インシデントへの対応と処理を行います。お客様が単独で行う必要は決してありません。

## ステップ4を実行する重要なアクション

**1. オーケストレーションとリハーサルを実践**
- 対応と復旧のプロセスを自動化
- インフラ、データ、アプリケーションの復旧手順が順序通りに行われているかなどを含め、対応計画を洗練させるために復旧リハーサルを実施

**2. クリーンルームを使用**
- フォレンジック分析用に独立したセキュアな環境を構築
- インフラ、データソース、アプリケーションをリストアする前に脅威を特定し、除去

**3. 専門家のサポートを受ける**
- 攻撃を受けた場合は、CohesityCERTに連絡

ステップ5

# データに関するリスク体制を最適化

**ランサムウェア集団の手口が悪化しているだけでなく、オンプレミス、SaaS、クラウド、エッジ環境など、管理すべきデータの量がこれまで以上に増えていることも課題です。誰もが、「誰にも知られていない、管理もされていないS3バケットに何か重要なものが残っているのでは?」と常に考えています。**

保護されていないS3バケット以外にも、孤立したデータベース、公開された資格情報など、リスクは隠れています。データセキュリティ体制の管理 (DSPM) やデータ分類などの予防的な対策は、これらのリスクを軽減するのに役立ちます。

## ステップ5の注目すべき利点

- ☑ **データの可視性と分類の強化**
- ☑ **プロアクティブなリスクの特定と緩和**

## ステップ5を実行する重要なアクション

**1. データの場所を把握**

- 環境をスキャンして、どのデータがどこにあり、どのような保護レベルが設定されているのかを評価します。これは、DSPMの全ツール群で行えます。
- CyeraやBigIDなど、業界トップクラスのベンダーとの完全統合により、バックアップ資産に含まれているものを把握し、適切に保護されていることを確認できます。

**2. 侵害によって何が影響を受けたか、またはデータ流出の場合には何が起こったかを評価する**

- Cohesity製品に搭載されたデータ分類機能で、必要な対応範囲を確保し、リスクを軽減
- インシデントが発生した際の、弁護士からの質問にはすぐに回答する(「どのようなデータが影響を受けたのか?」「それはどの程度機密性が高いのか?」「自社のリスクは?」「影響を受けた顧客は何人か?」「どのような種類の記録が影響を受けたか?」など)

# 結論

これで、組織のサイバーレジリエンスを向上させる5つの重要なステップを理解し、これらのステップを組織の環境に実装するのに必要な実用的な情報が得られました。

Cohesityは、サイバーレジリエンスを最大限に高めるための最適なパートナーとして、このステップの各段階でお客様をサポートします。

**ランサムウェアから安全かつセキュアに復旧するための参考資料として、以下をお勧めします:**

「破壊的なサイバー攻撃発生時の対応戦略を練る方法」

COHESITY

*どこでも回復力を発揮*



6100028-002-EN 6-2025