COHESITY

サイバーボルトの評価に関するエグゼクティブガイド

エグゼクティブサマリー：サイバー回復力にサイバーボルトが不可欠である理由

どの企業もサイバー攻撃の影響を免れることはできず、効果的な対応と復旧はすべての組織にとって不可欠です。攻撃者は、身代金を支払わせるためにあらゆる手段を講じ、データを保護するためのシステム自体を標的とする場合もあります。従来のバックアップ戦略は、ハードウェア障害や自然災害から保護するために設計されていますが、標的型かつ多段階のサイバー攻撃から組織を保護するには十分ではありません。ランサムウェア攻撃を受けると、本番ネットワークに接続されているデータのバックアップコピーが暗号化されるか、削除される可能性があり、クリーンかつ迅速な復旧はほぼ不可能になります。ITリーダーにとって重要なのは、攻撃が起きるかどうかではなく、いつ起きるかです。攻撃を受けたとき、自信を持って復旧する準備ができていますか？

貴社のような組織がデータの保護と復旧のあり方を見直す中で、サイバーボルトは、最新のサイバー回復力戦略における基盤的要素となっています。サイバーボルトによって、他のすべてに障害が起こった場合でも、復旧に使用できる未改変のデータコピーを確保できます。保管することで、破壊的なサイバー攻撃に直面しても、クリーンで復旧可能なデータを確実に確保するために必要な隔離、検証、制御が実現します。そのため、同業他社では、回復力の必須要件としてサイバーボルトの導入が進んでいます。

課題: サイバー復旧は災害復旧よりもはるかに複雑です

組織は、長年にわたり、ハードウェアの障害、偶発的な削除、自然災害に対応するためにバックアップシステムを設計してきました。これらのシステムは、多くの場合、その目的を十分に果たしてきました。しかし、現在主流となっている破壊的なサイバー攻撃からデータを安全に保護するには不十分です。

その結果、重要なリスク要因が浮上しました。つまり、バックアップデータは、本番データと同様に脆弱である可能性があるということです。脅威アクターはもはや、本番データの暗号化だけに注力しているわけではありません。バックアップリポジトリに侵入し、スナップショットのスケジュールを無効化し、マルウェアを植え付け、メタデータを改ざんすることで、復旧経路を排除します。

これらのリスクは、最新のデータ保護プラットフォームを導入している場合でも存在します。

データ環境がリスクにさらされている理由

「すべてのバックアップに対して安全なデータプラットフォームがあり、すべてのセキュリティアドオンが有効になっている。それで十分ではないか？」と思うかもしれません。結論：いいえ。

このようなプラットフォームは、リスクと攻撃対象領域を大幅に低減します。しかし、それだけではリスクへの曝露を完全に排除することはできません。

理由は以下のとおりです。

- **共有接続：**ほとんどのバックアップシステムは、本番環境ネットワークに接続されたままになっています。その本番環境が侵害されると、攻撃者はすでにバックアップデータへの経路を確保していることになります。
- **認証の重複：**管理資格情報は、複数の環境間で共有されていることが多くあります。攻撃者が特権アクセスを取得すると、本番データと同様にバックアップも容易に削除できるか暗号化できてしまいます。
- **虚偽のイミュータビリティ（変更不可）：**一部の「イミュータブル (変更不可)」バックアップは、ソフトウェアによるロックに過ぎません。ストレージのコントロールプレーンやAPIが侵害されると、イミュータビリティ (変更不可)フラグが解除される可能性があります。
- **潜在的な脅威の残存可能性：**多くの組織は、データの完全性を検証することも、潜在的なマルウェアをスキャンすることもなく、バックアップから復元しており、復旧中に再感染するリスクが高まっています。

ビジネスへの影響

その結果、信頼のギャップが生じます。すなわち、バックアップデータの整合性は、実際よりもはるかに高く認識されているということです。その悪影響は、次のように連鎖的に広がります。

- **ダウンタイムの長期化：**未検証のバックアップか侵害されたバックアップは、復旧時間を数時間から数日、さらには数週間へと長引かせます。
- **運用上の負担：**チームは、復旧計画の実行ではなく、システムやデータセットの再構築に時間を費やすことになります。
- **増大するコスト：**ダウンタイムが1時間延びるごとに、収益損失、規制上のリスク、ブランドへのダメージが増大します。
- **信頼の低下：**IT部門が迅速かつクリーンな復旧を実現できない場合、組織の回復力に対する経営陣と取締役会の信頼は低下します。

サイバーボルト：他のすべてが失敗した場合の最後の防衛線

サイバーボルトは、この信頼のギャップに対処します。サイバーボルトは、重要データのクリーンなコピーを保管する、安全で隔離されたイミュータブル (変更不可)リポジトリです。この保管庫は、本番ネットワークや主要なバックアップシステムから意図的に切り離されています。

サイバーボルトを導入すると、3-2-1バックアップルールが更新されます。つまり、3つのデータコピーを異なる2種類のメディアに保存し、そのうち1つはオフサイトコピーで隔離されるため、イミュータブル (変更不可) であるというルールです。

実際には、この最新のバックアップルールは次のように実装されます。

- **データの3つのコピーはイミュータブル (変更不可) でなければなりません：**コピーは、WORM（Write Once, Read Many）、またはオブジェクトレベルのロックを使用して保護し、AIベースの異常検出と定期的な脅威スキャンを使用して継続的に検証し、データがクリーンであることを確認する必要があります。
- **「異なる2種類のメディア」とは、2つの異なるプラットフォームまたは信頼境界にデータを保存することを意味します：**コピーは、同一のコントロールプレーンまたは攻撃対象領域を共有しない異なるシステム上に配置する必要があります。これには、データ隔離用に設計されたディスク、テープ、クラウドストレージの組み合わせが含まれる場合があります。
- **オフサイトに保管する1つのコピーは、分離されていなければならない：**最終コピーは、論理的または物理的なエアギャップによって分離され、隔離されたセキュリティモデルと第三者による保管管理のもとで保護される必要があります。また、このコピーは多要素認証（MFA）、クォーラム、およびデータの完全性チェックによって保護されるべきです。

これらの取り組みにより、3-2-1ルールはサイバー回復力の基盤となる柱へと進化します。サイバーボルトは、重要データの最終的かつクリーンな復旧ポイントとして機能します。サイバーボルトは、イミュータビリティ (変更不可)、隔離、異なるストレージドメイン、厳格な整合性検証を組み合わせることで、バックアップ資産が侵害された最悪のシナリオにおいても、破壊的なサイバー攻撃から組織を安全に復旧できるようにします。

サイバーボルトソリューションの評価

ITリーダーは、サイバーボルトソリューションを選択する際、セキュリティアーキテクチャと運用面での準備の両方を評価する必要があります。何百人ものITリーダーからのフィードバックに基づき、以下の5つの柱が重要な機能要件となります。

1. **データ隔離とアクセス制御：**保管庫のデータは、本番ネットワークからアクセスできないようにする必要があります。強制的なエアギャップ、独立したIDドメイン、MFA、クォーラムベースの管理承認が実装されているかどうかを確認してください。
2. **イミュータビリティ（変更不可）とインテグリティ：**データは改ざん不可能である必要があり、WORMストレージおよび保持ロックポリシーにより、管理者であっても変更や削除ができないようにする必要があります。
3. **自動化とオーケストレーション：**保管庫のレプリケーション、検証、復旧は自動化されている必要があります。ポリシーベースのオーケストレーションにより、人為的ミスを低減し、復旧を迅速化します。
4. **脅威からの保護：**AIベースの異常検出とマルウェアスキャンにより、スナップショット内の潜在的な脅威を検出し、クリーンで侵害されていないデータのみが保存され復元できるようにします。
5. **コンプライアンスおよびレポート：**イミュータブル (変更不可)監査ログ、暗号化、保持管理は、NIST SP 800-209、ISO 27040、DORAなどのフレームワークに準拠し、復旧可能性と回復力の準備を証明できるようにする必要があります。

評価スコアカード - ベンダーとの打ち合わせ時にこのスコアカードを活用してください。

手順：

1. 各カテゴリーについて、各ベンダーに対して1〜5のスコアを割り当てます。1は要件を満たしていない状態、5は要件を完全に満たしている状態を示します。
2. 各ベンダーのスコアにそのカテゴリーのウェイトを掛け合わせ、その結果を該当する加重スコア欄に記録します。
3. 各ベンダーについて、列内のすべての加重スコアを合計し、その合計を表の最下部にある加重合計行に記録します。
4. 加重合計を用いてベンダー全体を比較し、定性的な所見やリスクについて別途に記録してください。

		ベンダー1		ベンダー2		ベンダー3		ベンダー4	
カテゴリー	加重	スコア	加重スコア	スコア	加重スコア	スコア	加重スコア	スコア	加重スコア
隔離/エアギャップ	10								
イミュータビリティ (変更不可)/WORM	10								
アクセス制御の分離	10								
強力な認証（MFA/クォーラム）	8								
脅威の検知/異常	8								
感染したスナップショットの復旧をブロック	8								
復旧のオーケストレーション	8								
クリーンルーム/検証	8								
コンプライアンス/監査可能性	8								
SaaSのシンプルさ/TTV	7								
ハイブリッド/マルチクラウドの柔軟性	8								
TCO/運用オーバーヘッド	7								
加重合計									

最新のサイバーボルトは、測定可能なビジネス成果をもたらします。

- **回復力：**バックアッププラットフォームが侵害された場合でも、そのままの状態を維持する、物理的または論理的に隔離された復旧用コピー。
- **継続性：**組織は、保管されたバックアップにより、攻撃の範囲に関係なく、復旧に使用できるデータコピーを確保できます。
- **コンプライアンス：**イミュータブル (変更不可) ストレージと保持ポリシーの適用により、データ保護と復旧準備が整っていることの監査可能な証跡を提供します。
- **信頼：**復旧ポイントは影響範囲の外部に保持され、使用前に検証できるため、復元されるデータがクリーンで侵害されていないことを確保できます。

サイバーボルトは、IT運用、セキュリティ、コンプライアンスを連携させることで、危機が発生しても、ギャンブルではなく、クリーンな復旧を保証します。

バックアップ依存からレジリエントな復旧へ：Bethany Children's Health Center

多くの組織は、データ保護戦略の標準的な要素としてサイバーボルトを取り入れています。その一例が、複雑な医療ニーズを持つ子どもたちにケアを提供する、オクラホマ州のBethany Children's Health Centerです。同センターは、継続的な医療提供をサポートするため、機密性の高い医療データを保護し、サイバー攻撃や災害が発生した場合に迅速に復元できる必要があります。Bethanyは、オンプレミスと隔離されたクラウド保管であるCohesity FortKnoxの両方にイミュータブル (変更不可) バックアップを保存することで、これらの要件を満たしています。

回復力を強化するため、Bethanyでは、「3-2-1」の原則に従い、3つのデータコピーを2種類の異なるメディアに保持し、そのうち1つをオフサイトに保管しています。2つのイミュータブル (変更不可)バックアップはオンプレミスで維持され、3つ目はCohesity FortKnoxに保存されます。

Cohesity FortKnoxは、DataProtect環境とNetBackup環境向けに提供されるマネージドサイバーボルトサービスで、AWS、Azure、GCPで利用できるほか、最もセキュアな環境向けのオンプレミスソリューションとしても提供されています。FortKnoxは、隔離、イミュータビリティ (変更不可)、自動化を組み合わせて、企業規模で高速、クリーンで、検証済みの復旧を実現します。

FortKnoxは新しい防御層を追加します。これは、重要なデータの安全性、コンプライアンス、復旧可能性を確保するセキュアなエアギャップ型保管です。

サイバーレジリエンスを評価するための次のステップ

回復力計画は、もはや通用しない前提に依存してはなりません。サイバー攻撃の攻撃性が高まるにつれ、事業継続性は、最後の、最も安全なデータコピーの強度にますます左右されるようになってきています。サイバーボルトは、サイバー復旧を強化し、ダウンタイムを削減する積極的なアプローチを提供します。

まずは次の点を評価します。

- **すべてのデータソースに対して、SaaS、オンプレミス、クラウドのデータを最新の単一プラットフォームでバックアップしていますか？**
- **多要素認証 (MFA)、イミュータビリティ、RBAC (ロールベースのアクセス制御) で、プラットフォームを強化していますか？**
- **3-2-1のバックアップルールを遵守していますか？**
- **バックアップデータを本番ネットワークから隔離するために、どのような分離対策を講じていますか？**
- **どのくらいの頻度でバックアップをスキャンして脅威がないか調べていますか？**
- **サイバー対応計画をどのくらいの頻度でテストしていますか？**
- **前回のサイバー対応テストでは、どの程度の時間で復旧できましたか？**

今こそ、サイバー回復力を技術的な目標から戦略的に不可欠な取り組みへと引き上げる時です。仮定ではなく、準備こそが究極の競争上の優位性です。

最新のサイバーボルトが、データを保護し、復旧体制を強化し、いかなる脅威下においても安心して運用できる確信をどのようにもたらすのかご確認ください。
詳細はこちらhttps://www.cohesity.com/ja-jp/platform/fortknox/

COHESITY

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

4500065-001-JA 2-2026