ソリューション概要

InfiniBox®のデータ保護機能：ランサムウェア、自然災害、システム障害、人的ミスなど、あらゆる脅威からデータを保護するInfiniBox

課題

今日の世界では、データに対する脅威がかつてないほど高まっています。自然災害の発生が増加傾向にあるうえに、単純な人的ミスで貴重なデータがすべて失われてしまう可能性もあります。今日ではさらにサイバー犯罪によるリスクも増しており、特にランサムウェアやマルウェアは、企業の最高経営責任者や最高情報セキュリティ責任者にとって最大の懸念事項のひとつとなっています。

もし、こうした脅威が非常に恐ろしいと感じるならば、対策が十分でない証拠かもしれません。ほとんどの企業では、さまざまな脅威に備えてデータ保護（バックアップ）のための一般的な対策を実施しています。また多くの企業が、システムの中断やサイバー攻撃の発生時にでもデータの信頼性と可用性を維持できるよう、事業継続計画を策定しています。しかし、ランサムウェアやマルウェアの増加に伴い、計画がしだいに複雑化しているのが現状です。

周到に準備している組織でも、常にデータを十分に保護できているとは限りません。InfinidatのInfiniBoxとInfiniBox SSAではこのような状況に対応するため、InfiniSafe®リファレンスアーキテクチャーを採用してデータの耐障害性やサイバーレジリエンスなどを高める最新のデータ保護機能を提供しています。このアーキテクチャーにより、お客様はデータの安全性、可用性、信頼性を常に維持するための最適なツールとテクノロジーによる適切なプロセスを確立できます。

このソリューション概要では、発生する可能性が最も高く、かつ深刻な脅威のひとつであるサイバー犯罪とランサムウェアについて説明します。

> 「...近年はサイバー犯罪が深刻化しており、CEOを対象にFortuneが2021年5月に実施した調査、およびKPMGが2021年3月に実施した調査では、ビジネスに対する最大の脅威として「サイバーセキュリティのリスク」が挙げられています」

急増しているサイバー犯罪

- 企業が懸念すべきなのは、サイバー攻撃が発生するかどうかではなく、いつどのくらいの頻度で発生するかです。

  今日、サイバー攻撃の発生は不可避であり、すべての企業が十分な対策を行う必要があります。

- サイバー犯罪の攻撃手法は1つだけではありません。一般的な攻撃としては、次のようなものが挙げられます。

  フィッシング詐欺、オンラインIP盗難、インターネット詐欺（国連関係者になりすまして多額の資金を提供するので受取手続きをしてほしいと依頼する内容の詐欺が多数報告されています）

- 標的型攻撃（APT）のような高度なマルウェア攻撃は多くのリソースを要しますが、成功すれば多大な見返りが得られます。APTを使用するハッカーが標的にするのは、貴重なデータが多数存在するネットワークや資金力のある企業です。当該企業にとって不名誉な情報を公開すると脅して、金銭を要求する場合もあります1。

- 事実、近年はサイバー犯罪が深刻化しており、CEOを対象にFortuneが2021年5月に実施した調査2、およびKPMGが2021年3月に実施した調査3では、ビジネスに対する最大の脅威として「サイバーセキュリティのリスク」が挙げられています。

- 多くのサイバー攻撃は実行に先立って数か月にわたり入念に計画されているという事実を示す資料が多数提供されています。企業の環境に侵入した攻撃者の平均滞留時間は9か月間を超えています。

1 「What is an Advanced Persistent Threat?」、Kaspersky
2 「Fortune 500 CEO Survey」
3 「KPMG 2021 CEO Outlook Pulse Survey」
4 「Revealed: The Supermarkets that Will Sell You Malware for $50」、Forbes

INFINIDAT

ランサムウェア

ランサムウェアはマルウェアの一種です。ただし、ハイリスク、ハイリターンのAPT攻撃と異なり、ハッカーはダークウェブでランサムウェアを手軽に購入できます。その多くは安価で、ランサムウェアをCaaS（サービスとしてのサイバー犯罪）として提供している先進的な犯罪グループも存在します4。

ランサムウェア攻撃では、アクセス可能なすべてのファイルとボリュームを自動的に暗号化するソフトウェアが利用されます。ネットワーク接続されたコンピューターがランサムウェア攻撃を受けた場合、暗号化プロセスはネットワークにも波及し、バックアップやアーカイブが保存されているプライマリストレージとセカンダリストレージにも被害が及びます。多くのケースではセカンダリストレージが初めに標的とされ、そのためにリカバリがより困難になって攻撃者が優位に立つことになります。そのような状況を確保したうえで、ハッカーは復号キーと引き換えに、攻撃相手に金銭を要求します。

> 「OFFSITEにこのシステムを導入したところ、パフォーマンス、コスト効率、管理性が著しく向上したことに非常に驚きました。... Infinidatの改竄防止機能を備えたスナップショット機能は、ランサムウェアからのデータ保護に大いに役立っています」
>
> — OFFSITE、**最高技術責任者**

身代金の支払いが無駄な理由

ランサムウェア攻撃を受けた組織の多くは、データをすべて失うよりは、身代金を支払って復号キーを入手しようと考えます。

しかし、そううまくはいきません。ランサムウェアの被害状況を調査したSophosのレポート「ランサムウェアの現状2021年版」によると、過去12か月間に身代金を支払った組織の92%はすべてのデータを復旧できておらず、実際に復旧できたデータは全回答者の平均で65%でした。つまり、一部のデータのみ復旧できた組織もあれば、全データを復旧できた組織や、まったく復旧できなかった組織もあることがわかります。さらに同レポートでは、2021年上半期の平均復旧コストが既に2020年の2倍になっていることも報告しています。復旧のコストは、最終的には数百万ドルにまで達する可能性があります。

さらに、各国政府はランサムウェアに関して、身代金の支払いやインシデントの報告に関する規則、規定、法律の制定を進めています。今日の企業は、自社がビジネスを行う個々の地域における要件を常に把握しておく必要があります。

ソリューション

InfinidatのInfiniBoxはAIベースの高度なストレージシステムソリューションです。運用が容易でありながら、前例のない100%の可用性、優れたパフォーマンス、総所有コストの大幅な削減を実現します。管理プレーンとデータプレーンを分けることで、システムアーキテクチャに強力なデータ保護を提供します。

InfiniBoxにはさまざまな防御機能が備わっています。たとえば、スナップショット/改竄防止機能を備えたスナップショット、レプリケーション、暗号化、アクセス管理機能はデータの確実な保護を実現し、ストレージプールキャパシティのしきい値アラートは脅威の迅速な検知に役立ちます。ローカルスナップショットとレプリケーションスナップショットによる迅速なリカバリも可能です。

InfiniSafe：InfiniBoxファミリー用のリファレンスアーキテクチャー

プライマリストレージを保護するためのサイバーレジリエンスを備えた環境をいかに構築するかを理解することが、これまでになく重要になっています。企業における重要なデータ資産の保護を強化するには、多層的な防御戦略が必要です。InfiniSafeのリファレンスアーキテクチャーには、より強力なサイバーレジリエンスを確立するうえで役立つ、簡単に実装できる方法が示されています。その基礎となるアプローチは、以下の4つの柱で構成されます。

- **改竄防止機能を備えたスナップショット**
- **リモートの論理的エアギャップ**
- **隔離されたフォレンジック環境**
- **ほぼリアルタイムのリカバリ**

データを保護するには、ロックされていて変更不可能なコピーを作成できることが非常に重要です。そのようなコピーはそれ自体が論理的にエアギャップされたものとみなせますが、レプリケーションのベストプラクティスに基づいてその対象を拡大し、ディザスタリカバリの場合と同様に改竄防止機能を備えたセカンダリコピーを作成することも重要です。このコピーが作成されたら、さらにデータのテストや検証を行う必要があります。隔離された環境（ゼロトラスト環境とも呼ばれます）を構築することで、データのクリーンさの検証が必要なときのみ有効化される、本番環境から分離された環境を利用できるようになります。データの検証やテストを実行する際の自社のニーズに最も適したツールやアプリケーションも使用できます。以上のプロセスによりデータのポイントインタイムコピーの検証が完了したら、当該のデータは数秒から数分でリカバリできるようになります。InfiniBoxファミリーの製品ではこれらの機能すべてを、特定のベンダーやツールセットが必要な専用ソリューションを導入することなく利用でき、ベンダーやツールへのロックインが発生しません。

スナップショット：データ保護と事業継続性をサポート

Infinidatのスナップショットメカニズム「InfiniSnap®」は、拡張性やパフォーマンスを損なうことなく重要なデータを確実に保護します。InfiniSnapでは、ロック不要のRedirect on Write（書き込み時にリダイレクト）方式を使用してスナップショット/改竄防止機能を備えたスナップショットを作成し、必要に応じて迅速にリストアできるようにします。

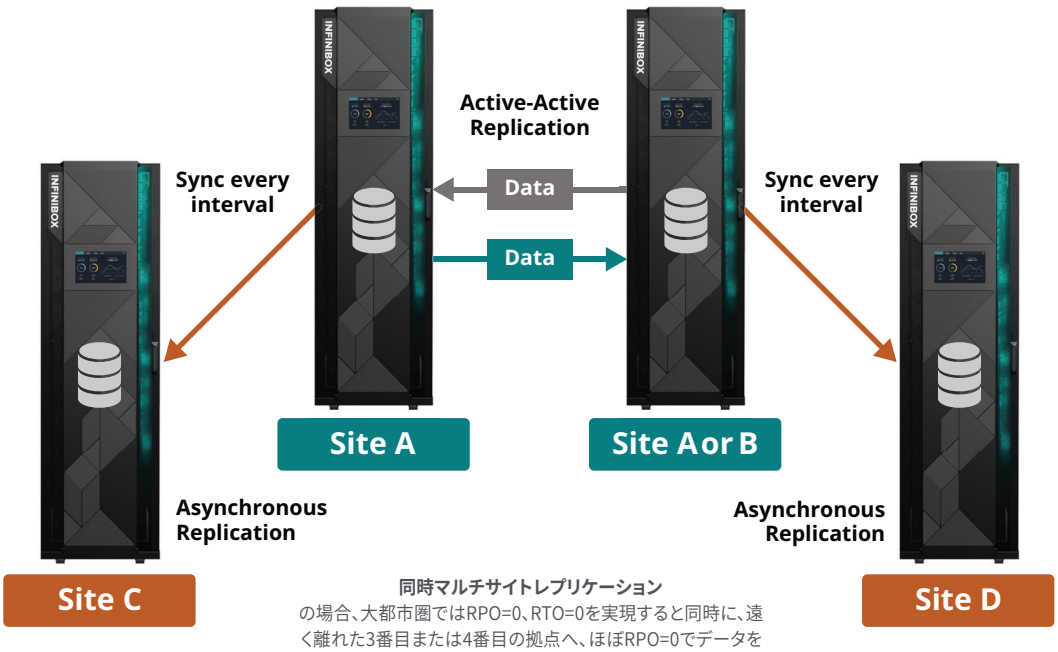
スナップショットには読み取り専用と書き込み可能があり、各データセットには最大1,000のスナップショットを格納できます。InfiniSnapでは、ボリューム、ファイルシステム、整合性グループについて改竄防止機能を備えたスナップショットを取得できます。ファイルを誤って削除または変更した場合、スナップショットディレクトリを使用すれば、目的のファイルを容易に選択して、元の状態に戻すことができます。

- **改竄防止機能を備えたスナップショット：** 改竄防止機能を備えたスナップショットの場合、決められた保持期間内は変更や削除を行えません。管理者はロックの有効期限を延長することは可能ですが、短縮することはできません。この機能を使用して隠しスナップショットをバックアップイメージに適用すれば、スナップショットをより確実に攻撃から保護できます。
- **脅威の検知：** ランサムウェアがデータを暗号化するとデータサイズが増大し、結果としてデータのスナップショットのサイズが増大します。管理者は、キャパシティ使用量のしきい値を設定しておき、スナップショットボリュームが突然増加して平均パラメータを上回ったときに警告を受け取ることができます。攻撃を検知した場合は、データにすぐにアクセスしてテストし、最新の有効なスナップから迅速にリカバリできます。

レプリケーション：事業継続性をサポート

スナップショットに加えてレプリケーションを利用することで、脅威にさらされているデータを保護し、すみやかに復元できます。環境の変化に応じてさまざまなニーズに対応できるよう、InfiniBoxには複数のレプリケーションタイプが用意されています。

- **非同期レプリケーション：** 目標復旧ポイント（RPO）を4秒に設定できます。IPインフラストラクチャを使用するため、複雑さが軽減され、多大なコストもかかりません。
- **同期レプリケーション：** ミッションクリティカルなアプリケーションでは、RPO=0秒、400マイクロ秒未満の遅延でのレプリケーションが可能です。WANで通信速度の低下や障害が発生したときは、同期レプリケーションが非同期モードになります。その後、WANが復旧した時点で、不足しているすべてのデータが自動的にレプリケーションされ、I/Oを中断することなく同期レプリケーションが再開されます。
- **アクティブ/アクティブレプリケーション：** InfiniBoxシステムでは、複数のリモート拠点にまたがり、整合性グループに対して読み取りと書き込みを同時に実行できます。ボリュームは外部イメージであり、同じボリュームへのマルチパスとして実装されます。同期レプリケーションでは、常にボリュームの整合性が維持されます。プライマリ/セカンダリ関係がないため、どのボリュームに更新データを書き込むときでも余分なラウンドトリップが発生しません。必要であれば、単独のノードまたはクラウドベースの仮想マシン上に外部の軽量なwitness（監視）を配置できます。



同時マルチサイトレプリケーション
の場合、大都市圏ではRPO=0、RTO=0を実現すると同時に、遠く離れた3番目または4番目の拠点へ、ほぼRPO=0でデータを非同期にレプリケーションできます。

INFINIDAT

- **同時マルチサイトレプリケーション：** InfiniBoxでは、一次レプリケーションサイトから離れた場所にある別のサイトへ、複数の整合性グループを同時にレプリケーションできます。そこからさらに、3番目のリモート拠点へ非同期にレプリケーションできます。

暗号化：暗号化されたデータを保護

ランサムウェア攻撃を受けると暗号化したファイルが再暗号化されるため、スナップショットとレプリケーションの防御が極めて重要です。元の暗号が強力なほど、ハッカー側の再暗号化が難しくなります。

- **連邦情報処理標準（FIPS）140-2に準拠：** Infinidatの暗号化モジュールは、米国国立標準技術研究所（NIST）が発行したFIPS 140-2規格を満たしています。この規格に基づき、InfiniBoxは、米国政府機関および規制対象業界のITプロジェクトで使用することが認められています。
- **AES-256暗号化を採用した標準の自己暗号化ドライブ（SED）：** InfiniBoxでは、FIPS 140-2準拠のAES-256暗号方式を用いた 標準の自己暗号化ドライブ（SED）を使用します。AES-256は、このタイプのドライブでサポートされている最も強力な認証キーです。
- **キー導出関数（KDF）：** Infinidatは米国連邦政府によって承認されたKDFテクノロジーを採用しています。KDFでは、ドライブごとにグローバルに一意なキーが生成されます。Infinidatのプラグイン可能なキーマネージャーを使用すれば、KMIP（Key Management Interoperability Protocol）経由で外部キーを容易に管理できます。
- **サードパーティとの統合：** プログラミングでカスタマイズしたり、多大なコストをかけたりしなくても、Thales、VMware、Oracle TDE、Microsoft TDEなどの暗号化製品と密に統合できます。

アクセス管理：不正侵入を阻止

サイバー攻撃者がネットワークに侵入する経路はいくつかありますが、最も危険度が高いのは管理者の認証情報です。InfiniBoxは、サイバー攻撃者が侵入できないように構成されています。すべてのアクセスがAPI経由で行われ、管理者の認証情報が使用されていても、このAPIによってスナップショットへのあらゆる変更が阻止されます。

InfiniBoxのアクセス管理は攻撃者の侵入を許しません。

- **ロールベースのアクセス制御（RBAC）：** RBACは本システムの制御プレーンで実行され、ローカルアカウントおよびドメイン/LDAPグループを保護します。グループに割り当てられたロールに基づき、全ての制御、一部のキャパシティプールの制御、または読み取り専用の権限がユーザーに付与されます。ローカルアカウントはユーザーが無効化またはロックできるため、Infinidat技術者がメンテナンスを行うときのみ有効にできます。セッション認証も管理アクセスの保護に役立ちます。
- **ホスト認証：** iSCSIは、CHAPを利用してデータプレーン上のホストを認証します。別のホストのデータへ不正にアクセスできないようにするため、CHAPでは多要素ホスト認証が義務付けられています。
- **サードパーティのアクセス管理の統合：** Infinidatは、CyberArkなど、エンタープライズ対応の外部の特権アクセス管理ソリューションと連携しています。
- **管理ステーションへのアクセスと監査：** アクセス管理には、安全なリンクを介した管理ステーションへのアクセスも含まれます。さらに監査証跡には、マシンの構成や状態、またはコンポーネントを変更するすべての操作が記録されます。構成を変更した管理者も記録されます。

まとめ

ビジネスを成功に導くうえで、データの保護は欠かせない要素です。エンタープライズ対応のInfiniBoxには、データの耐障害性とサイバーレジリエンスを高め、全社規模でのサイバーセキュリティ戦略の一環としてストレージを活用するためのさまざまな機能が備わっています。

InfiniBoxを導入すれば、優れたパフォーマンス、100%の可用性、手間のかからない容易な運用、総所有コストの大幅な削減に加え、ランサムウェア攻撃も阻止することができます。サイバー攻撃の犠牲になるのは、十分な対策をしていない組織です。そのため、強力なデータ保護対策が重要になります。

InfiniBoxには、改竄防止機能を備えたスナップショット、強力なレプリケーション、高度な暗号化、厳重なアクセス管理など、サイバー攻撃の阻止に役立つさまざまな機能が備わっています。さらに、これらの機能は、お客様の予算、スタッフ、ビジネス目標に合わせたパッケージとしてご利用いただけます。