

エンタープライズハイブリッドクラウドセキュリティにとって不可欠となる改ざん不可能なバックアップ

はじめに

たとえば、あなたの会社がランサムウェア攻撃を受けていたとします。ハッカーは、数百万ドルを支払わなければ重要なデータを一般に公開すると脅迫しています。

業種に関係なく、ビジネスは危険にさらされます。石油・ガス会社であれば、燃料輸送などの作業が極めて予測不可能になってしまいます。医療機関なら、患者の個人情報危険にさらされます。最悪の場合、血液型や投薬のデータにアクセスできず、救命のための医療が遅れてしまうこともあります。小売業なら、顧客の決済情報が流出する可能性があります。

身代金を支払ってもすべてが解決するわけではありません。データを完全に復元できたとしても、金銭的損失を軽減できるほど迅速にシステムを復元できるという保証はありません。

データの破損は、ランサムウェア、自然災害、無人アクセス、偶発的な削除など、さまざまな形で現れます。ランサムウェアやハッキングは最大の懸念事項ですが、あらゆる脅威を防ぐ必要があります。誰でも無人アクセスや偶発的な削除などによってデータを操作する可能性があります。改ざん不可能なストレージによるデータの保護は、復旧の際に確実に復元し、再構築するための方法の 1 つです。

サイバー犯罪者はますます巧妙になっています。従来のリカバリプロセスではもはや十分とは言えません。犯罪者は、本番システムとバックアップ環境の両方を標的にしています。リポジトリやスナップショットを削除したり盗んだりすることで、それを使いものにならなくするのです。マルウェアやデータが破損すると、ビジネスが一瞬にして麻痺し、コストと時間のかかるサービス停止へと追い込まれてしまいます。

それでは、影響を受けにくい企業になるにはどうすればいいのでしょうか。どのくらいの頻度でバックアップを行い、どこに保存すればいいのでしょうか。予測可能な回復力を実現すれば、会社とその収益を守ることができます。

リスクの特定

バックアップとリカバリは、優れた保護戦略の基礎であり、緊急時の最後の手段ではありません。検出と保護は不可欠ですが、改ざん不可能な場所に完全でクリーンなバックアップが保存されていると確信できることに勝るものではありません。

オンサイトストレージとクラウドストレージのリスクとメリットについて考えてみましょう。クラウドストレージは、場所や時間を問わず、あらゆるデバイスから簡単にデータにアクセスできるという点で非常に便利です。ただし、この利便性にはリスクが伴います。つまり、ハッカーがクラウドに侵入する可能性が残るのです。

改ざん不可能なストレージとは、書き込んだデータを変更または削除できないようにする種類のストレージであり、潜在的な災害に対する保護手段として持続可能で適切なソリューションです。クラウドベースのアプリケーションを活用し、データをエッジで使用していれば、ペリタスが場所に関係なくデータを保護します。

ペリタスでは、クラウドストレージとオンプレミスストレージの自律型データ管理を簡素化します。単一の管理プラットフォームが異常検出、エアギャップ、改ざん不可能なボルトのための AI を活用した機械学習を可能にします。

重要なデータの安全性を確保するには、信頼性の高いバックアップが不可欠です。肝心な点は、劣化や損失のないデータ保存が可能なことです。改ざん不可能なバックアップは、最高レベルの保護を提供します。企業は、重要なデータの安全性を保証するために信頼できるバックアップを必要としています。ペリタスでは、WORM (Write Once, Read Many) 形式でこれらのバックアップを作成し、誰もスナップショットを変更または削除できないようにします。

改ざん防止機能は、データの整合性を大きく向上させる可能性があります。包括的なセキュリティ計画やサイバーセキュリティ戦略の一環として改ざん不可能なストレージを活用し、重要なデータを確実に保護しましょう。エアギャップバックアップによる保持ロックと異常検出を活用し、脅威を特定した時点ですぐにそれを制限し、隔離します。最も重要な情報をどのように保護するかを考えましょう。どのくらいの頻度でバックアップを行い、どこに保存すればいいのでしょうか。改ざん防止機能は、データの整合性を大きく向上させる可能性があります。

究極の改ざん防止機能を実現する

データ保護タスクを自動化すれば、常にデータが整理された安全な状態を維持できます。手作業をなくし、コンプライアンス機能や監査およびレポート機能を支援する自動化プロセスを有効にすれば、リスクを最小限に抑えることができます。

セグメント化により、オンプレミスでもクラウドでも、緊急時でも人を介入させずに効率的に対応できるようになります。また、特定のコンテナでのロールバックや分離型リカバリ環境 (IRE) からの取得が可能になるため、重大な障害への対処にも役立ちます。

リソースを一元管理すれば、より統一された監査が可能になります。また、ソフトウェア更新の可視性が向上し、エラーのリスクが大幅に軽減されます。重複排除を組み込んだバックアップシステムや、自動イメージレプリケーション (AIR) を組み込んだクロスドメインレプリケーションを簡単にセットアップできます。また、オブジェクトロックを統合すれば、オンプレミス環境とクラウド環境全体のデータセキュリティとコンプライアンスを強化することもできます。これにより、サードパーティベンダーを選べるようになります。

脅威、ランサムウェア、またはその他の中断に対する堅牢な保護を実現します。改ざん防止機能は信頼性の高いリカバリを可能にし、ダウンタイムと収益の損失を抑え、リスクレベルを低減し、確立されたガバナンスポリシーを満たします。ベリタスでは、コンテナ技術を活用してコストを削減し、効率を高めています。このソリューションは、クラウドベースやエアギャップ IRE など、さまざまなバックアップオプションと以下のような高度な機能により、信頼性を確保しています。

- ・ポリシーに基づく保持ロック
- ・ロールベースのアクセス制御 (RBAC)
- ・パスワードポリシー管理
- ・STIG により強化されたアプライアンス

ニーズに合わせて最適な不変性強度を選択できる Enterprise ロックダウンモードにより、完全に改ざん不可能なストレージとコンプライアンスを実現します。このモードを有効にすると、root を含むユーザーは、一定時間内のデータの変更または削除を制限する二重認証の許可がなければ、データを削除または変更できなくなります

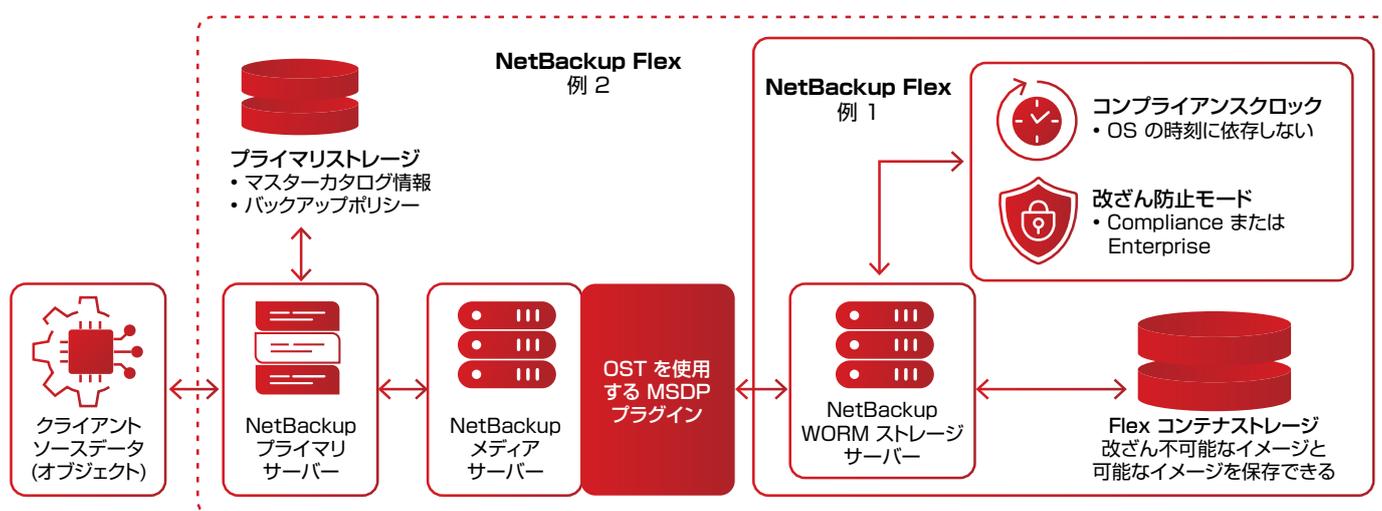


図 1. Veritas Flex Appliance に搭載されているさまざまなセキュリティ機能

万能型

データセキュリティに万能なアーキテクチャはありません。アプリケーションと環境は非常に複雑なため、インフラ全体でデータを保護する効果的な方法を探す必要があります。ベリタスは、オンプレミスとクラウドにおける改ざん防止機能に加えて、AI を活用した異常検出とマルウェアスキャンを提供することで、侵入不可能なポルトを実現します。さらなるセキュリティを確保するために、ベリタスアプライアンスを構成して WORM ストレージサーバー IRE を作成し、余分な手間をかけることなく保護された重要なデータのコピーをエアギャップに格納できます。

改ざん不可能なストレージを使用する理由

コンプライアンス

医療、政府機関、金融サービスなど規制の厳しい業界では、データを変更せずに一定期間保持すること（データ保持）が義務付けられています。IRE を使用した改ざん不可能なストレージを利用すれば、規制上の義務に準拠した記録の保持が可能になります。

ディザスタリカバリ

改ざん不可能なストレージは、災害時に極めて有益です。クラウド上に改ざん不可能なバックアップコピーがあれば、特定のリカバリ時間目標 (RTO) とリカバリポイント目標 (RPO) 内にデータを利用可能にすることが求められる場合でも、中断による影響を最小限に抑えることができます。たとえば、ファーストレスポnder、軍事機関、防衛施設などでは、データがいつまでもオフラインであってはなりません。常に妥協のないデータ利用を保つことが重要なのです。

データセキュリティ

機密情報を守るためには、不正アクセスからデータを保護することが重要です。顧客データの保護を義務付ける GDPR、HIPAA、CCPA、PCI DSS などの規制はますます増え続けています。

監査

改ざん不可能なストレージでは、データを監査するためのツールを提供しています。すべてのログが記録されるため、管理者は変更の履歴を簡単に追跡でき、変更もすべて記録されているため、データ履歴の再構築も可能です。

NetBackup™ と NetBackup Flex は、OpenStorage Technology (OST) API を使用しています。これは、柔軟でストレージに依存しない改ざん不可能なバックアップマネージャです。ベリタスまたはサードパーティのストレージを使用すれば、企業はプライマリ、セカンダリ（重複排除）、および自動イメージレプリケーション (AIR) によるクロスドメインレプリケーションをサポートし、あらゆるバックアップストレージ階層におよぶ無制限の構成オプションを利用できます。これにより、オンプレミスとクラウドでデータの安全性とコンプライアンスが保たれ、Amazon (AWS) S3 オブジェクトロックとの併用が可能になります。改ざん不可能なイメージポリシーを管理し、サードパーティのアプライアンスを活用できるため、ベンダーに依存する必要がありません。

コンテナ技術をベースとした NetBackup Flex と Flex Scale は、マルチテナント機能によってデータ保護を強化します。これには以下のメリットがあります。

- ・ クラウドを含むマルチポイントバックアップリポジトリを備えたエアギャップソリューション
- ・ ポリシーベースの保持ロック、ロールベースのアクセス制御、およびパスワードポリシー管理
- ・ STIG で強化されたサイバーセキュリティ

ベリタスアプライアンスは FIPS 140-2 データ暗号化認証に準拠し、Cohasset Associates 社による改ざん不可能性評価¹を受けています (Compliance モードの場合)。

- ・ 証券取引委員会 (SEC) の 17 CFR § 240.17a-4(f)
- ・ 金融業規制機構 (FINRA) 規則 4511
- ・ 商品先物取引委員会 (CFTC) の規制 17 CFR § 1.31(c)-(d)

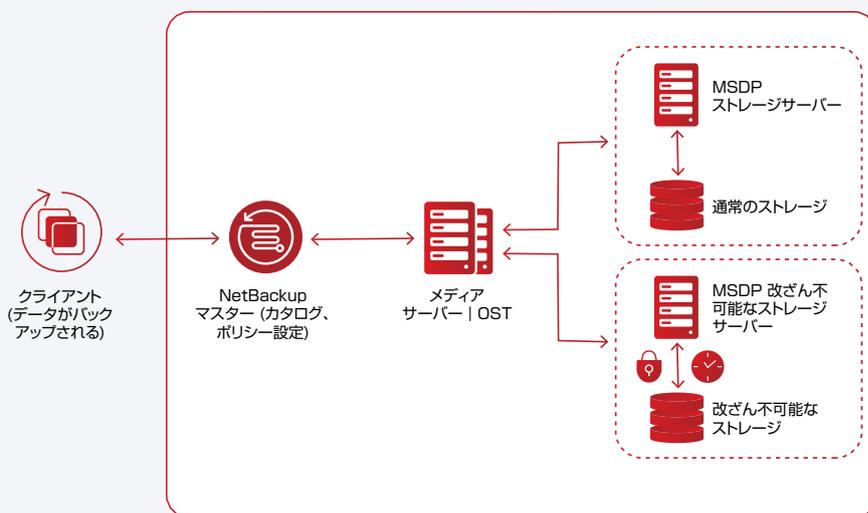


図 2. ベリタスがランサムウェア攻撃から IT サービスを保護する仕組み

ベリタスは、複数の環境で動作するように設計されているため、リカバリ戦略を柔軟に定義できます。ベリタスには幅広いテクノロジーが組み込まれており、バックアップデータを常に最新の状態に保つためのさまざまなオプションをサポートしています。可視性とレポート作成のためのさまざまなオプションにより、最大限の信頼性とパフォーマンスを提供しています。

コンプライアンス保証を強化するために、ベリタスアプライアンスには、Veritas File System に基づく独自のシステムクロックが組み込まれています。これは管理者でも変更できないため、保持期間を制御できるというメリットがあります。

ベリタスの強み

ベリタスを使用すると、改ざんおよび消去不可能なインフラを構築できるため、偶発的な削除や意図的な変更のリスクからデータを保護できます。ベリタスのテクノロジーは、データのバックアップから複雑さを排除するため、サイバーセキュリティ戦略に確信を持てるため、ダウンタイムを確実に回避できます。強化された OS、コンテナの分離、ゼロトラストアーキテクチャ上に構築されたアプライアンスを使用することにより、データのナビゲーションと管理を簡素化できます。ベリタスは、より安全なハイブリッド環境やマルチクラウド環境を効率的かつ効果的に実現できるよう、バックアップデータとファイルの保護をサポートします。

その他の情報：

- Cohasset 社による [NetBackup の改ざん不能性評価](#)の全文を読む
- [NetBackup の分離型リカバリ環境](#)を備えたエアギャップソリューションの詳細を見る
- [アプライアンスのベストプラクティスとサイジングに関する推奨事項](#)を確認する
- [NetBackup Flex の統合および API ガイド](#)を確認する
- [NetBackup Flex アプライアンスのセキュリティ](#)を使用したインストールと設定の詳細を確認する

詳細については、[NetBackup Flex アプライアンス](#)のページをご覧ください。

1. [veritas.com/form/whitepaper/cohasset-associates-immutability-assessment-for-netbackup](https://www.veritas.com/form/whitepaper/cohasset-associates-immutability-assessment-for-netbackup)

ベリタスについて

Veritas Technologies は、マルチクラウドデータ管理のリーダーです。データの保護、リカバリ能力、コンプライアンスを確保するために、Fortune Global 100 の 95% を含む、先進企業 80,000 社以上が、ベリタスのソリューションを導入しています。ベリタスは、ランサムウェアのようなサイバー攻撃がもたらす脅威に対してお客様が必要とする回復力を提供し、大規模な環境でも信頼できると評価をいただいております。単一の統合されたアプローチを通じ、800 以上のデータソース、100 以上のオペレーティングシステム、1,400 以上のストレージターゲット、60 以上のクラウドをサポートしており、ベリタスの実行能力に匹敵するベンダーは他にありません。Cloud Scale Technology により、ベリタスは運用にかかる煩雑さや業務量を削減しつつ優れた価値を提供する、自律型データ管理の戦略を提供しています。ベリタステクノロジーズ合同会社は、Veritas Technologies の日本法人です。

VERITAS™

ベリタステクノロジーズ合同会社
〒107-0052 東京都港区赤坂 1-11-44
赤坂インターシティ 4 階
[veritas.com/ja/jp](https://www.veritas.com/ja/jp)

各国オフィスとお問い合わせ先については、
弊社の Web サイトを参照してください。
[veritas.com/ja/jp/company/contact](https://www.veritas.com/ja/jp/company/contact)