

# Nutanix ユニファイドストレージによるバックアップとサイバーストレージ

## 主な利点

- 改ざん防止バックアップ**: Nutanix の WORM 対応のオブジェクトストレージで、脅威からデータを保護します。
- エンドツーエンドの暗号化**: 送信中と Nutanix Objects に保存されているデータの両方を保護します。
- エアギャップアーキテクチャ**: 管理とデータアクセスのためのネットワークセグメンテーションにより、ランサムウェアのリスクを軽減します。
- 迅速で高粒度なリカバリ**: ダウンタイムが最小限に抑えられ、ポイントインタイムリカバリオプションが可能になります。本番環境に影響を与えることなく、特定の瞬間にデータを正確に復元します。
- 緊密な統合**: バックアップアプリケーションとの緊密な統合と、きめ細かなアクセス制御により、セキュアなタスクの委任とリソースアクセスが可能になります。
- Nutanix Data Lens**: 非構造化データに対する悪意のある攻撃をプロアクティブに検知し、ロックすることで、さらなる保護レイヤーを提供します。

### ソリューション:

- Unified Storage
- セキュリティ
- データ保護

### 製品:

- Nutanix Data Lens
- Nutanix ディザスタリカバリ
- Nutanix ユニファイドストレージ(NUS)

## NUS を使ってみる

テストドライブ

データは、組織や最新のアプリケーションにとって不可欠です。データを活用することで、製品やサービス、ビジネス全体の方向性についての戦略的でデータ主導の意思決定が可能になります。そのため、データの可用性を確保することは、運用とサービスを円滑に稼働させるうえで極めて重要です。

11秒に1つの組織がランサムウェア攻撃を受けていることをご存知ですか？現実的に考えてみましょう。医療機関が突然、重要な患者記録にアクセスできなくなったり、銀行が顧客の財務データから遮断されたりする状況を想像してみてください。

サイバーレジリエンスツールやシステムの更新、厳格なインターネット制御に多額の投資を行っているにもかかわらず、あらゆる規模の組織が依然として脆弱です。サイバー犯罪者はますます巧妙で執拗になり、わずかな脆弱性さえも悪用するようになっています。その結果、攻撃が発生するかどうかではなく、いつ発生するかが問題となっています。

## 不变ストレージ：レジリエントなデータ保護の基盤

現在のデジタル環境では、サイバー攻撃、特にランサムウェアからバックアップデータを保護することが不可欠です。不变ストレージ（イミュータブルストレージ）特に WORM 対応の S3 オブジェクトストレージは、バックアップとリカバリの戦略を強化することをめざす組織にとって不可欠なテクノロジ

一となっています。

WORM テクノロジーはデータの不变性を強制するため、データが保存されると、管理者であっても指定された保持期間内は変更や削除ができなくなります。この不变性により、データの整合性が保証され、バックアップデータは変更されることなく維持され、データの損失や破損が発生した場合でも、復旧のための信頼性が確保されます。

ランサムウェア攻撃の場合、不变性は、保持期間中の不正な変更や削除を防ぐことで保護手段として機能します。この強化されたセキュリティレイヤーにより、組織はバックアップが悪意のある攻撃者に改ざんされることなく無傷で保たれるという確信を持ち、データ侵害に対するレジリエンスを強化します。

Nutanix は、WORM 対応のオブジェクトストレージにより、この分野で堅牢なソリューションを提供し、企業がバックアップ向けにセキュアな不变ストレージを実装できるようにします。Nutanix のソリューションを活用することで、組織はレジリエントなバックアップ戦略を構築し、データ改ざんのリスクを軽減し、重要な資産の完全性を確保できます。

## バックアップデータの隔離による保護

Nutanix Objects は、外部接続を内部ストレージネットワークから分離するためのネットワークセグメンテーションのサポートが組み込まれており、分離されたバックアップを実装するための理想的なプラットフォームを提供します。バックアップ専用の Nutanix Objects クラスタを作成することで、組織はバックアップデータを本番環境ネットワークから効果的にエアギャップすることができます。これにより、本番環境が侵害された場合でも、分離されたバックアップデータは、悪意のある攻撃者の手の届かないところに残ります。

また、Nutanix Objects はきめ細かな RBAC も可能としているため、組織はバックアップ用の Nutanix Objects クラスタへのアクセスを、許可されたバックアップサーバーと管理者のみに制限できます。これにより、不正なデータの変更、削除、流出のリスクが最小限に抑えられます。

ネットワークレベルの分離に加えて、Nutanix Objects はプライマリデータセンターから物理的に離れた場所に展開できるため、物理的な災害や標的型攻撃に対する保護をさらに強化できます。WORM 対応の S3 オブジェクトストレージの不变性と、Nutanix Objects の分離とアクセス制御機能を組み合わせることで、組織は堅牢でセキュアなバックアップとリカバリの戦略を確立できます。

## リカバリの先へ：Nutanix Data Lens のプロアクティブなランサムウェア防御

Nutanix Data Lens (NDL) は、既知の脅威と潜在的な脅威をプロアクティブに検出してブロックする、SaaS ベースのデータセキュリティと分析ソリューションです。NDL は、迅速な検出とブロックを備えたアクティブな防御技術を使用して、統合されたランサムウェアレジリエンスを提供します。シグチャベースの検出を活用して既知の脅威を特定し、挙動ベースの分析を活用して、疑わしい挙動を示す未知の脅威を検出します。

NDL は、従来のランサムウェア保証とは異なり、脅威を検出してブロックする時間と、数分以内で構成されるランサムウェア封じ込めウインドウを提供します。従来の保証は、検出と軽減に関する SLA を伴わず、復旧や適用が可能な復旧費用の補償のみを保証しています。NDL は、ランサムウェア攻撃による被害を 10 分以内に封じ込めることをめざしています。復旧費用の支払いに数日、数週間、数か月かかる可能性のある復旧保証よりもはるかに迅速です。

## まとめ

進化する脅威の状況において、Nutanix は、WORM 対応のエアギャップバックアップと迅速な脅威検出により、重要なデータを保護する包括的なソリューションを提供しています。Nutanix Objects と NDL は、不变性、アクセス制御、プロアクティブなランサムウェア防御を組み合わせて、脅威を迅速に封じ込めます。Nutanix ユニファイドストレージを今すぐご利用いただき、テストドライブでお試しください。

詳しくは、[Nutanix ユニファイドストレージのページ](#)をご覧ください。

