HPE Alletra Storage

ビジネスホワイトペーパー

ハイブリッドクラウド全体のデータ保護を最新化

データ制御を確保し、サービス中断などの障害からデータを保護する

HPE

目次

エグゼクティブサマリー

従来のデータ保護方法では、今日の分散型アプリケーションやデータの要件を満たすには不十分です。データ量の急増、ランサムウェアなどの高度なサイバー脅威、規制遵守への圧力、自然災害によるリスク、人為的ミス、ハードウェア障害など、組織は山積する課題に直面しています。こうした問題への対処は、ミッションクリティカルなシステムを保護し、多様な環境にわたるシームレスな運用を確保し、コストのかかるダウンタイムやデータロスを防ぐために不可欠です。

このホワイトペーパーは、拡大し続けるハイブリッド環境全体で、中断やデータロス、絶え間ないサイバー攻撃による脅威からデータを保護するという課題に、組織が対処できるよう支援することを目的としています。クロスクラウドでのデータ保護に関する重要な課題を検証し、ソリューションを探り、業務の中断なく事業継続性を維持するための最新アプローチの重要性を強調します。

現代の脅威に直面する現代のワークロード

今日のデジタル時代では、企業が保有するデータ量は飛躍的に増加し、その重要性も高まっています。そのため、堅牢なデータ保護の必要性はこれまで以上に差し迫った課題となっています。

従来のバックアップ方法やリカバリ方法では、データ量の増大に対応しきれない場合も増えています。この問題への対処として、組織ではストレージとソフトウェアソリューションを組み合わせて使用することが多く、その結果、データサイロが生じています。このアプローチは、大量の帯域幅とコストを消費するだけでなく、ハイブリッドクラウド環境全体でデータを管理し、保護する際に新たな複雑さが生じてしまいます。

ハイブリッドクラウドは、パブリッククラウドの柔軟性とオンプレミスインフラストラクチャのセキュリティを兼ね備えたものとして広く支持されています。しかし、この組み合わせには、最新のデータ保護戦略が緊急に必要となります。機密情報の安全な保管、適切なアクセス管理、また複雑化する規制への準拠を保証する必要があるからです。

サイバー攻撃による侵害は業務に短期的な影響を与えるだけでなく、ブランドの評判にも深刻な悪影響を及ぼす可能性があります。

データ保護の課題には、サイバーセキュリティ脅威の継続的なエスカレーションも加わっています。近年では、脅威アクターが人工知能を採用するケースが増えています。ディープフェイクからワンタイムパスワードボットにいたるまで、企業データへの侵害を目的とした、より巧妙な攻撃を仕掛けるためです。エッジに移動するデータ量が増えるにつれ、この環境が危険にさらされた場合のコスト被害は甚大なものになる可能性があります。たとえば、モノのインターネット（IoT）デバイスを標的として侵害を受けた企業に生じる経済的影響などがこれにあたります。Forrester社による最近のレポートでは、これらの企業は、IoT以外のデバイスへのサイバー攻撃を受けた組織と比較して、累計侵害コストの報告が500万ドルから1,000万ドルに上る可能性が高いことが示されています。[1]

1 『2024年のIoTセキュリティのトップトレンド』、Forrester、2024年3月

2 『サイバーセキュリティに関する懸念が最優先事項であり、データ侵害による被害額の平均が300万ドルを超えているにもかかわらず、全社的なサイバーレジリエンスを実装している企業はわずか2%に留まっています: PwC 2025グローバルデジタルトラストインサイト』、PwC、2024年9月

3 『クラウドセキュリティへの企業の投資拡大』、ガートナー、2024年6月

そのため、テクノロジーリーダーの3分の2（66%）が、2024年に軽減すべき最大のリスクとしてサイバー脅威を挙げている[2]のも驚くに値しません。また、クラウドセキュリティへの投資が2024年には24%増加すると予測されていること[3]も意外ではありません。これは、グローバルセキュリティおよびリスク管理市場のすべての分野の中で最も高い増加率を示しています。結局、サイバー攻撃による侵害を受けることは、業務に短期的な影響を与えるだけでなく、侵害が解決されてから長い時間が経過し、データが回復された後でも、組織の評判に深刻な悪影響を及ぼす可能性があります。

保有するデータに対する脅威の拡大やデータ量の増加を考慮しつつ、ハイブリッドクラウド環境をシームレスに管理するには、データ保護に対する最新の優れたアプローチが必要です。

データ保護における共通課題への対応

長びく中断: 現在のシステムでは、業務中断からの回復に長い時間がかかります。組織は、事業継続性に悪影響を与えずに、中断発生時にバックアップを取得し、迅速に復旧する必要があります。

コストのかかるダウンタイム: 多くの組織では、重要なワークロードのダウンタイムを許容できません。とはいえ、現在利用されているツールではデータ可用性を十分に確保できないのは周知の事実です。

コンプライアンスについての懸念: コンプライアンスの遵守とセキュリティの確保は、すべての企業にとって頭の痛い問題です。機密データが多数の環境に分散している状態では、これが特に重大な問題になります。

停滞するイノベーション: 事業継続性の中断、法外なコスト、データ侵害の脅威への対応はすべて、企業のイノベーションの推進力に悪影響を及ぼします。これらの障害により、ビジネスのアジリティが低下し、迅速なアクションを起こして新たな機会を創出することが難しくなります。

明らかに、データ保護に対する現在のアプローチはもはや機能していません。データ主導の時代におけるビジネスニーズを満たすには、新しいソリューションが必要です。

運用の合理化とセキュリティ強化で事業を円滑化

運用の中断を減らし、複雑さをシンプルにするためには、ワークロードをスムーズに動かし、場所を問わずにデータを厳重に保管できるよう設計されたソリューションが不可欠です。

ハイブリッド重視のデータ保護を達成するためにHPEが提案するソリューションは、レガシー課題の克服とエッジからクラウドまでの管理統合の2つです。このアプローチにより、重要なアプリケーションのパフォーマンスが高速かつ信頼性の高いものとなり、データロスとダウンタイムを最小限に抑え、組織は絶えず変化するセキュリティとコンプライアンスの要件に対応し、優位性を確保できます。

障害が発生した場合、HPEの継続的なデータ保護（CDP）により、業界をリードするリカバリポイント目標（RPO）とリカバリ時間目標（RTO）を実現し、数分以内に復旧できます。

さらに、HPEのソリューションは、詳細なレポート、監査ログ、グローバルなマルチサイトダッシュボードなど、コンプライアンスの維持と、常に変化するデータと規制要件に先手を打てるように設計されています。統合型のオールインワンソリューションにより、クラス最高のストレージ、コンピューティング、ネットワーキング、ソフトウェアを使用して、迅速なエアギャップリカバリが可能になります。

ワークロードをスムーズに実行するための3つの留意事項

企業が、データ保護を念頭に置いてハイブリッドクラウドエクスペリエンスをアップグレードしたい場合、次の3つの要素を考慮する必要があります。

- **常時ビジネスを維持する:** オンプレミスとクラウドの両アプリケーションの保護、回復、モビリティを合理化
- **データロスとダウンタイムを最小限に抑える:** 業界をリードするRPOとRTOにより、CDPを通じて数分でリカバリ
- **鉄壁の防御を提供する:** 分散型ゼロトラストアーキテクチャーにより、重要なデータを保護

Zerto, a Hewlett Packard Enterprise companyによる最新鋭のデータ保護

Zertoは、企業が業務中断なくビジネスを継続できるように、データの保護、回復、モビリティを簡素化し、プライベート、パブリック、ハイブリッド環境全体での継続的な可用性を実現します。

モダナイゼーションとクラウド導入のリスクと複雑さを軽減することで、企業はセキュリティの脅威を回避したり、コンプライアンス要件への違反を懸念したりすることなく、ビジネスイノベーションの推進に集中できます。

進化する脅威を軽減

—ランサムウェアやその他のマルウェアをリアルタイムで識別し、無効化できる高度な脅威検出および対応ソリューション

—オンデマンドのサンドボックスにより、本番環境とほぼ同一のコピーでパッチテスト、フォレンジック分析、サイバーセキュリティ演習を容易に実行

—オフラインの分離されたリカバリ環境（IRE）と、ランサムウェア攻撃を受けた最悪の事態でも最後の防御線として機能する、改ざん不可能なデータボールト（IDV）を組み合わせた、セキュアなオンプレミスの顧客管理型ソリューション

業務中断の削減とダウンタイムの短縮

—業界をリードするRPOとRTOを備えたCDPなら、数分で復旧が可能

—自動フェイルオーバーおよびフェイルバックプロセスによってダウンタイムを短縮し、個々のファイルのリカバリから仮想化アプリケーション全体のリカバリにいたるまで、状況を問わずに事業継続性を維持

コスト効率の高い安全なアーキテクチャーを構築

—過剰なコストをかけずに、耐障害性とセキュリティに優れたアーキテクチャーのための自動化された非中断テストを提供するソリューション

—詳細なレポート、監査ログ、グローバルなマルチサイトダッシュボードなど、コンプライアンスの維持と、常に変化するデータと規制要件への先手を打つ対応が可能

—クラス最高のストレージ、コンピューティング、ソフトウェアを使用して迅速なエアギャップリカバリを可能にする統合型のオールインワンソリューション

万一ほかのすべてが失敗した場合でも、Zerto Cyber Resilience Vaultはゼロトラストアーキテクチャーを提供し、不変のデータコピーを、隔離されたオフラインの状態で安全に保持します。

データが未来へと導く

ハイブリッドクラウドと飛躍的に増大するデータ量は、どちらもデータ主導の世界において恒久的な要素です。しかし、脅威が続く状況下にあっても、それらは事業継続性やイノベーションを止める理由にはなりません。

重要なデータを安全に守り、保護することは、これからも企業の永続的な責務となります。適切なツールと最新のアプローチを導入することで、企業は自信を持ってこの課題に立ち向かうことができます。また、今後何年、何十年にもわたってデータ主導型のビジネスで成功できる態勢を確保し続けることができます。

HPEについて

HPEは、場所を問わずあらゆるデータの価値を引き出すことで組織における迅速な成果の実現をサポートするEdge-to-Cloudカンパニーです。数十年にわたって未来を再考し、イノベーションによって人々の生活や働き方を進化させてきたHPEは、すべてのクラウドとエッジで一貫したエクスペリエンスを実現する、他にはないオープンでインテリジェントなテクノロジーソリューションを提供することで、お客様が新しいビジネスモデルを開発したり、新たな方法で連携したり、運用のパフォーマンスを高めたりできるようサポートしています。

詳細はこちら

HPE.com/Zerto

Visit HPE.com

今すぐチャット

a50011803JPN, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com