

マルチクラウドの データ保護・復旧

Lawrence Miller

- ✓ 現状のデータ管理の課題
- ✓ マルチクラウドのデータ保護・復旧のユースケース
- ✓ マルチクラウドのデータ保護・復旧ソリューションの要件

この論文では

データは現代のビジネスにとって極めて重要であり、ランサムウェアやハードウェアの故障、その他の原因によるデータ損失は、業務を深刻な影響を及ぼす可能性があります。これらのリスクを軽減するために、効果的なデータバックアップと復旧が不可欠です。この技術概要では、特にマルチクラウド環境におけるデータ管理の課題と解決策について説明しています。

要点:

- マルチクラウド構成にはメリットがある一方で、データ、管理や保護が複雑です。
- 現状のデータ保護に必要な機能として、クラウドネイティブ対応、即時復旧、サイバーレジリエンスが挙げられます。

目次

2	現状のデータ管理の課題
4	マルチクラウドのデータ保護・復旧のユースケース
5	マルチクラウドのデータ保護・復旧ソリューションの要件
6	顧客事例

データはすべてのビジネスの要です。そのデータが失われたらどうなるでしょうか？ランサムウェア、サービス拒否 (DoS) 攻撃、悪意のある内部関係者、ハードウェア障害、あるいは単純な人的ミスなど、原因が何であれ、データが失われるとビジネスは機能しません。データが不可欠な現在のビジネスにおいて、迅速かつ効果的にデータをバックアップ・復旧できる体制を確保する必要があります。

この技術概要では、データ管理の課題、マルチクラウドのデータ保護・復旧のユースケース、そして最新のデータ保護・復旧ソリューションに求められる機能や対策について説明します。

現状のデータ管理の課題

データ保護の重要性を理解しているにもかかわらず、複雑なITインフラやデータのサイロ化、急増するデータへの対応に、多くの組織が苦慮しています。その背景として、さまざまなユースケースに対応するため、複数のデータ保護ツールや製品をその都度導入してきたことが挙げられます。また、従来のソリューションは保守コストが高く、新しい技術との相互運用性に欠ける点も課題となっています。このため、多くの企業がマルチクラウドインフラ環境を活用したクラウドファースト戦略を採用しています。

データ保護の重要性を理解しているにもかかわらず、複雑なITインフラやデータのサイロ化、急増するデータへの対応に、多くの組織が苦慮しています。

マルチクラウド構成では、災害復旧能力の向上、最適な技術の活用、アプリケーション・ワークロードの最適化、リスク低減を目的として、複数のクラウドプロバイダーのクラウドコンピューティングサービスを使用します。しかし、これには課題も伴います。マルチクラウド戦略を採用している組織の87%が、マルチクラウド管理は企業クラウドの主要な3つの課題のひとつになっていると回答しています。

理由？場合によっては、マルチクラウドは意図的な戦略ではなく、分散化されたIT管理や広範なシャドウITの結果として構成されていることもあります。例えば、人事部門は給与管理にSaaSアプリケーションを利用し、DevOpsチームはAWSでアプリケーションを構築し、IT部門はMicrosoft Azureで中核インフラを管理しているケースが考えられます。また、マルチクラウドが意図的に導入されている場合でも、戦略上の理由からデータは分散されます。意図的であるかどうかにかかわらず、データは至る所に分散しています。その結果、IT環境が複雑化し、データ保護やセキュリティの課題が増えています。

データの民主化は、データの増加と複雑化の要因のひとつです。最小権限のセキュリティ原則を採用するのではなく、すべての企業ユーザーがすべてのデータやデータタイプに容易にアクセスできるようにすることで、データ管理の課題がさらに増えています。AIへの取り組みが加速する中、データ量は今後も指数関数的に増加し、マルチクラウドやハイブリッド構成全体に分散配置された個別のツール間でデータが散在する状況は、今後さらに大きな課題となります。

これに対応するため、オンプレミスおよびハイブリッド・マルチクラウド環境全体にわたってシステムやワークロードを保護し、完全に統合されたきめ細かなバックアップと即時復元機能を提供するとともに、サイバーレジリエンスを強化し、脅威を検知し、サイバー攻撃からの迅速な復旧を可能にする最新のデータ保護・復旧ソリューションが、組織に求められています。このため、今日および将来にわたってビジネスユースケースに対応する、データ管理と保護の単一の統合ソリューションが必要です。

クラウドネイティブで完全に統合され、きめ細かなバックアップと即時復旧機能を提供するとともに、サイバーレジリエンスを強化し、脅威を検知し、サイバー攻撃からの迅速な復旧を可能にする最新のデータ保護・復旧ソリューションが、組織に求められています。

マルチクラウドのデータ保護・復旧のユースケース

マルチクラウドのデータ保護・復旧は、多くのユースケースに対応します。主な例は以下のとおりです：

- **バックアップと復旧。**データは、悪意のある行為に限らず、さまざまな原因で失われる可能性があるため、データのバックアップは復旧に不可欠な最初のステップです。データの喪失や損失を防ぐために、データのコピーを安全な場所に作成・保管するためのプロセスとツールが重要です。
- **データのセキュリティおよびコンプライアンス。**業界ごとに、データの取り扱いに関する規則は異なります。例えば、一般データ保護規則 (GDPR) は、欧州連合の居住者の個人を特定できる情報 (PII) を管理または処理するすべての企業に適用されます。業界の規制に従ってデータを適切に管理できない企業は、法的責任、金銭的損失、財務的な不利益を被る可能性があります。
- **ランサムウェア対策 (保護、検知、復旧)。**ランサムウェアに対する最も効果的な防御策は、身代金の支払いを回避しながら迅速な復旧を可能にする、改ざん不可能なデータバックアップを確保しておくことです。さらに、効果的に対応するための戦略を事前に策定しておくことも重要です。NISTなどのフレームワークに基づいて戦略を策定することで、サイバーセキュリティのベストプラクティスに沿った、堅牢なデータ保護・検知・復旧体制を構築できます。
- **長期保管とアーカイブ。**定期的に新しいデータを生成しながら既存データも保持する必要がある企業にとって、新旧いずれのデータも迅速に取得できるデータアーカイブは重要です。特定の業界では、コンプライアンスや規制要件により、データの長期保管が求められます。
- **災害復旧とビジネス継続。**変化の激しい「常時稼働」が求められるビジネス環境では、ダウンタイムは企業の評判と利益の両方に悪影響を及ぼします。障害やその他の重大な事象から迅速かつ完全に復旧するため、最大許容停止時間 (MTD)、目標復旧時間 (RTO)、目標回復時点 (RPO) に関する、厳格さを増す要件に対応する必要があります。

マルチクラウドのデータ保護・復旧ソリューションの要件

データの価値がますます高まる中、マルチクラウド環境に対応した最新のデータ保護・復旧ソリューションが不可欠です。主な要件：

- **一元管理。**単一の統合ソリューションにより、マルチクラウド、ハイブリッド、オンプレミス環境全体を、グローバルかつ大規模に管理できます。また、潜在的なランサムウェア攻撃を検知し、異常を特定し、追加のキャパシティ計画などの対応策を提案するインテリジェントなグローバルアシスタントの機能が求められます。
- **オンプレミス、クラウド、SaaSデータの保護。**データがあらゆる所に存在している現在、最新のデータ保護・復旧には、オンプレミス、マルチクラウドやハイブリッド環境、さらにはSaaSアプリケーションに至るまで、データ保護が求められます。オンプレミスおよびクラウド展開において、セルフマネージドまたは「サービスとして」に対応できる柔軟な導入オプションを検討する必要があります
- **大量データの即時復元。**サイバー犯罪者の狙いは、可能な限り多くのデータを漏洩または破壊することです。そのため、すべてのデータを迅速に復旧できる体制が必要です。スナップショットを常に完全な状態で保持し、復旧時間を短縮できるソリューションにより、数百規模のVM、大規模データベース、大容量の非構造化データを、規模に応じて任意の時点および場所へ即時に復元できます。
- **サイバー復旧。**バックアップの完全性を検証し、例えばバックアップ自体がランサムウェア攻撃の標的となった場合でも、「クリーン」な復旧ポイントを特定できるように、データを細かなレベルで確実に復元できるソリューションが必要です。
- **無制限の拡張性。**複雑でリスクが高く、コストもかかるオンプレミス環境でのフォークリフトアップグレードを排除し、業務の混乱を回避しながら容易に規模を拡張するため、スケールアウト型のハイパースケール・アーキテクチャと分散ファイルシステムを採用する必要があります。これにより、グローバル検索機能に加え、可変長のグローバル重複排除および圧縮を通じて、データ量とストレージフットプリントを削減できます。

データの価値がますます高まる中、マルチクラウド環境に対応した最新のデータ保護・復旧ソリューションが不可欠です。

顧客事例

Ausenco: Cohesity DataProtect Delivered as a Serviceにより、セキュリティを強化し、管理時間を短縮

多国籍のエンジニアリングおよびコンサルティングサービスプロバイダーである同社は、3,000人以上の従業員が利用するMicrosoft 365 (M365) の重要データ約100TBをバックアップしています。同社が以前利用していたセルフマネージドのクラウド基盤で運用するバックアップソリューション (Veeamソフトウェア) は、セキュリティ要件を満たせず、管理に週20時間を要していました。Cohesity DataProtect Delivered as a Serviceへの移行により、同社はバックアップ基盤の管理に費やしていた週20時間の工数を削減するとともに、ファイル復旧に関する4時間のサービスレベル契約 (SLA) を導入し、サイバー保険要件を満たす不変バックアップを確保することで、追加コストなしで安心して運用できる環境を実現しています。

課題

鉱業会社によるバッテリー用金属需要の急増を背景に、Ausencoのエンジニアリングおよびコンサルティングサービス事業は継続的に拡大しています。同社は、3,000人以上の従業員が利用するM365の重要なデータ約100TBをバックアップしています。「Microsoftは基本的なデータ保護機能を提供していますが、当社のビジネスには十分とはいえません。無期限に保持している一部のSharePointやOneDriveのファイルを、サイバー攻撃によって失うことは絶対に避ける必要があります。」Kalpesh Bhathella氏、Ausencoオペレーショナルサービス担当ディレクター

2022年まで、同社のITチームは、Amazon Web Services (AWS) のInfrastructure as a Service (IaaS) を利用し、VeeamソフトウェアでM365のデータをバックアップしていました。しかし、インフラとソフトウェアの管理に大きな負担が伴い、IT管理者1名の業務時間の50%を占めていました。もう一つの課題として、サイバー攻撃からの復旧に不可欠な不変バックアップコピーの取得に、追加のインフラと管理時間が必要でした。「セキュリティは、見込み客から常に質問を受ける最優先事項

であり、最近ではサイバー保険への加入を確認されるケースも増えています。不変コピーが不可欠でしたが、現状では管理負担を増やす余裕はありませんでした。」Kalpesh Bhathella氏

解決策

CohesityとRubrikを評価した結果、同社はCohesity DataProtect Delivered as a Serviceを採用しました。このサービスは、M365などのSaaS向けのバックアップ/復旧機能を提供するとともに、今後計画されているその他のクラウド環境やオンプレミス環境のデータにも対応します。「ITが中核ビジネスではない当社にとって、インフラの自社管理は合理的とは言えません。フルマネージドのクラウドサービスは理にかなっており、不変バックアップを標準で提供しているのはCohesityだけでした。」Kalpesh Bhathella氏

同社は、Cohesityのクラウドサービスを約2週間で導入・稼働させ、現在ではITチームが管理に手間をかける必要はほとんどなくなっています。「初期設定後、Cohesityは問題なく稼働しています。サポートが必要になることはまれですが、Cohesityがすぐに解決してくれます。エスカレーションが必要になったことは一度もありません。」Kalpesh Bhathella氏

成果

Ausencoにとって、Cohesityソリューションの最大のメリットは、セキュリティ体制の強化です。「サイバー攻撃を防ぐために可能な限りの対策を講じていますが、Cohesityの不変バックアップコピーからクリーンなM365データを復元できることが、確実なセーフティネットになっています。さらに、不変バックアップをオフサイトに保管することで、見込み客からよく質問される、サイバー保険の要件も満たしています。」

より強力なセキュリティは、コストアップではなく、コストダウンを実現します。「クラウドインフラの月額費用が不要になり、その分でCohesity DataProtect Delivered as a Serviceのコストを十分に補填しています。さらに、バックアップソフトウェアとクラウドインフラの調整や管理に要していた週20時間の工数を削減しています。」Kalpesh

Bhathella氏以前はバックアップ管理に業務時間の50%を費やしていた担当者が、現在では、より付加価値の高いデジタルトランスフォーメーションの取り組みに時間を充てて注力しています。また、不変バックアップを他のサイバーセキュリティ対策と組み合わせることで、同社はサイバー保険料を有利な条件で契約しています。

また、M365のメールやファイル復旧において、4時間のサービスレベル契約 (SLA) を初めて導入したことで、同社の多忙なエンジニアリング、コンサルティング、オペレーションチームからも高い評価を受けています。「以前のバックアップソリューションでは、失われたExchange、SharePoint、またはOneDriveのファイルを復元するのに数週間かかることがありました。IT管理者が何百ものバックアップを逐一調べる必要があったからです。Cohesityの検索エンジンは、まさにバックアップのGoogle検索のような存在です。ファイル名やフレーズを入力するだけで、一覧が表示され、ほとんどの場合、必要なファイルが最上位に表示されます。」
Kalpesh Bhathella氏

現在、同社はM365に加え、オンプレミスおよびAWSの仮想マシンを含む他のワークロードの保護にも、Cohesity DataProtect Delivered as a Service を活用する準備を進めています。耐障害性を高めるため、Kalpesh Bhathella氏は、特定のワークロードをMicrosoft Azureにバックアップするハイブリッドクラウド構成を計画しています。これにより、ITチームは、単一のCohesityインターフェースから、あらゆるクラウドのバックアップおよび復元を一元的に可視化・管理できます。

「Cohesity DataProtect Delivered as a Service により、ビジネス成長に伴って必要となるあらゆるタイプのデータを保護するための機能が揃いました。不変バックアップ、迅速な復元、優れたサポートが確保され、インフラ管理に苦慮する必要もありません。」
Kalpesh Bhathella氏

Cohesityのソリューション導入による主なメリット：

- 不変コピー — サイバー保険の要件
- M365のメールおよびファイル復元を最大99% (2週間から4時間に) 短縮
- 管理に要する週20時間の工数を削減
- 追加コストなし

詳細

最新のデータ保護および復旧ソリューションの詳細については、<https://www.cohesity.com/solutions/backup-and-recovery>をご覧ください。

COHESITY