COHESITY

ホワイトペーパー

最新のデータセキュリティとデータ管理に関するトポロジー: ITリーダー向けガイド

リスクを軽減しビジネスレジリエンスを強化するためのブループリントとベストプラクティス

目次

はじめに

データセキュリティとデータ管理に対する新たなアプローチが求められている背景には、3つの要因があります。第一の要因は、デジタルトランスフォーメーションとAPI駆動型インフラの必要性です。ITリーダーは、IT資産のあらゆる側面をモダナイズして、自動化、拡張性、クラウドスケール、ソフトウェア定義アーキテクチャ、「シフトレフト」のセキュリティ原則を実現しようとしています。

第二に、サイバー脅威はますます複雑・巧妙になり、予測が難しくなっています。多くの組織の既存のデータ資産はサイロ化しており、サイバー攻撃による運用リスクが増大しています。最近の調査によると、32%の組織が、バックアップと復旧システムが古いほど迅速な復旧を妨げると考えています。同様に、34%の回答者が、ITチームとセキュリティチーム間で連携が取れていないと、復旧時間も長くなると回答しています。

そして第三に、AIの出現により、リーダーたちは、企業データを生成AI技術がアクセス可能にする最新のデータプラットフォームを探すようになりました。

データの近代化を進めるITリーダーは、先人たちの知見を活かすことで、より多くの成果を得ることができます。このホワイトペーパーでは、設計に関する最も重要な考慮事項と、一般的な企業要件を考慮した最善のデータレジリエンスアプローチの達成方法について説明します。Cohesityの見解は、何千件に及ぶ導入経験とベストプラクティスに関する知識をもとに形成されています。

以下のガイダンスは特定のベンダーに依存しないものですが、わかりやすくするためにCohesityのブランド名を使用します。

設計のポイント

価値あるモダナイゼーションプロジェクトにはリスクが伴います。企業のデータセキュリティとデータ管理に関するプロセスとツールを変革する場合、そのリスクがより顕著です。しかし、これまでに他の人たちが築いてきた成果を活用して構築できるという利点もあります。多くの組織がデータ資産のモダナイズに成功しています。このホワイトペーパーでは、これらのベストプラクティスをカタログ化しました。

ITやサイバーセキュリティのリーダーには、IT資産全体でアジリティ、リスク、コストのバランスを取る任務が課されています。この資産は常に変化し、現在ではオンプレミスのデータセンター、パブリッククラウド、コロケーション施設、エッジロケーションで稼働するデータやアプリも含まれています。膨大な量のアプリ、データ、データソースが多様化し複雑化するにつれて、モダナイゼーションの取り組みは時間の経過とともに規模と範囲が拡大します。

企業データ資産のモダナイズは、以下によってさらに複雑化します:

- 多様なインフラが複数の場所とワークロードを対象とすることで、データの断片化やバックアップと復旧プロセスの非効率化を招いている
- ほとんどの組織でITやサイバーセキュリティに関するスキルが不足
- サイバーセキュリティ環境が急速に変化し、1分間に数百件の攻撃が発生。攻撃の進化と巧妙化に伴い、早期検知の重要性が増している

とはいえ、覚えておくべき「第一の原則」があります。

3:2:1ルールはそのまま

3:2:1ルールでは、少なくとも3つのデータコピーを保持し、これらのバックアップを2つの異なる種類のメディアまたはプラットフォームに保存し、少なくとも1つのコピーをオフサイトで保管する必要があります。

3:2:1ルールの価値が今なお変わらないのは、クラウドネイティブ時代におけるシステムトポロジー設計を支える以下の3つの概念に根ざしているためです:

- ビジネス要件
- 障害ドメイン
- 不可抗力

これらの各概念を詳しく説明します。これらは業界において常に重要なテーマであり、特に近年サイバー攻撃に関する懸念が高まる中で、なお一層注目されています。以前はサイバー攻撃が最前線の課題ではなかったものの、現在では間違いなく中心的な問題となりました。

これらの3つの概念が、時間の経過とともにいかにバックアップと復旧の設計を形作ってきたかを定義し、既存のデプロイメントトポロジーで十分サイバー攻撃に打ち勝てるかという顧客の懸念について考えていきます。

1つずつ見ていきましょう:

ビジネス要件

企業は、ビジネス、規制、コンプライアンス要件を幅広く遵守しなければなりません。これらの要件の多くは、データの現在と過去のコピーの両方を保持する必要性を生み出しています。例えば、コンプライアンスチームは、業界規制

当局からの要請に対応するために、3年前に作られた契約を確認しなければならない場合があります。または、税務チームが進行中の監査のためにファイルを復旧しなければならないこともあります。身近な例としては、重要なファイルが誤って削除され、リストアが必要になる場合があります。

障害ドメイン

IT業界では、ソフトウェアでもハードウェアでも障害が発生することはよく知られています。ハードウェアやソフトウェアのベンダーは、これを回避すべく設計に多大な努力を払っていますが、それでも障害は発生します。ITチームは、障害が起きた際の対応計画を立て、これらの障害が組織やビジネスに悪影響を及ぼさないようにする必要があります。障害の例としては、VMやストレージボリュームの破損、OSパッチの適用失敗といったワークロード障害が挙げられます。どの場合も、ITチームは障害から復旧する必要があり、その復旧の一環として、バックアップと復旧システムからのデータが必要になる可能性があります。

数十年前なら、組織のリーダーは悪意のある行為者によるシステム障害に悩まされることはありませんでした。今日、サイバー攻撃はシステム障害の主要な原因であるだけでなく、おそらく最も顕著な障害要因であり、取締役会からの関心を集めています。

不可抗力

人間が制御できない自然災害などの、合理的な手段によって予測または防止することができないものを指す言葉です。火災、地震、洪水、ケーブル切断などの有害事象はすべて「不可抗力」と見なすことができます。障害ドメインと同様に、IT組織は、不可抗力の可能性を考慮し、それらに対して回復力のあるシステムを設計構築する必要があります。

不可抗力を前にしたときに実践的なガイダンスとなるのが3:2:1ルールです。

システムに障害が発生することを前提として、複数のデータコピーを利用できるようにしておくのが賢明です。障害ドメインの観点から、2種類の異なるメディアやシステムにバックアップを保持することも合理的です。最後に、不可抗力の発生時に備えてこれらのコピーの少なくとも1つを、災害復旧サイトまたはリモートデータセンターの一部など遠隔地に保持することは責任あるガバナンスです。

要件が異なっても、共通点は存在

3:2:1ルールは堅実な実践ですが、コピー数が3つ未満の構成を選ぶ組織もあります。より厳格に3:2:1ルールに従う組織もあれば、さらにコピーを3つ以上保持している組織もあります。(これらの設計選択の根拠については、本ホワイトペーパーの後半で説明します。)

設計に関して、デプロイメントトポロジー (「ブループリント」) を3つのタイプに分類しました。

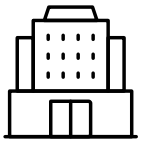
タイプ	説明
基本	コピー数が2つ以下のデプロイメントトポロジー
強化	コピー数が3つのデプロイメントトポロジー
ミッションクリティカル	コピー数が4つ以上のデプロイメントトポロジー

馴染みのある高可用性アーキテクチャは、現在も有効

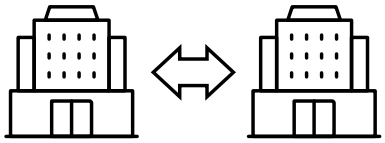
次に取り上げるのは、経験豊富なITリーダーや実務担当者であればより馴染みのある、高可用性アーキテクチャという用語です。

高可用性アーキテクチャは、ITチームが潜在的な障害に対する回復力を高めるための、ハードウェアとソフトウェアシステムの構成指針です。Cohesityの実績では、企業の導入事例の大半が、***アクティブ/アクティブ、アクティブ/スタンバイ、ハブアンドスポーク***という3つの顧客向け高可用性アーキテクチャのいずれかで構成されています。

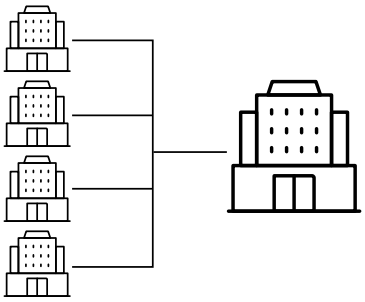
これらの各アプローチは、次のページで説明しています。



アクティブ-スタンバイ
ワークロードは単一のデータセンターで稼働しています。停止時に切り替わるスタンバイの災害復旧サイトが用意されていることがよくあります。



アクティブ-アクティブ
主要なワークロードは2つのデータセンターに分散されています。いずれかのデータセンターが障害を起こした場合でも、残りのデータセンターが全負荷を引き継ぐことができます。



ハブ・スポーク
このワークロードの特徴は、多数のリモートオフィスやブランチオフィスが単一のデータセンターに接続されている点にあります。

図1: 顧客の高可用性アーキテクチャ

いずれの場合も、高可用性アーキテクチャは障害発生時に事業運営が継続できるよう設計されています。**アクティブ/スタンバイ**アーキテクチャでは、「アクティブ」側に障害が発生すると、すべての処理がスタンバイシステムに切り替わります。**アクティブ/アクティブ**システムでは、どちらか一方に障害が発生した場合、もう一方が100%のワークロードを引き受けます。**ハブアンドスポーク**システムでは、支店でのハードウェア障害やその他の問題でデータが破損した場合でも、障害の原因が解消され次第、システムとデータをハブから復元することができます。

責任あるITチームは、これらの高可用性アーキテクチャを設計し、レジリエンス機能が適切に動作することを確認するために定期的にテストを実施しています。

Cohesityのベストプラクティス用ブループリントは、これらの実績ある高可用性アーキテクチャに基づいています。Cohesityでは、バックアップと復旧システムを単独で導入することはありません。私たちは、基盤となるITインフラと密接に連携するよう設計しています。この点については、本ホワイトペーパーの後半で、さまざまなバックアップと復旧のトポロジーと、それらがITの高可用性アーキテクチャにどのように対応しているかを詳しく解説します。

最新のデータセキュリティとデータ管理のためのブループリント: タイプとトポロジー

基本、強化、ミッションクリティカルのバックアップタイプについては、既に説明しました。次に、これらのタイプに関連するトポロジーを紹介します。

まず、いくつかの定義から解説します。データセキュリティとデータ管理システムは、さまざまな方法でデータを保存することができます。データのコピーは、***バックアップ、レプリカ、アーカイブ***のいずれかとして保持することができます。

参考となる経験則は以下の通りです:

- **バックアップ**はプライマリコピーから作成され、重複排除、圧縮、暗号化されたデータとして保存されます。この処理はデータに対して一度だけ行われ、その後、処理済みのバックアップデータはレプリカやアーカイブにコピーできます。
- **レプリカ**は一般的に短期間の保存に使用され、通常は数か月単位で保持され、数年単位での保存には適しません。これらのレプリカは多くの場合、アクティブ/アクティブまたはアクティブ/スタンバイなどのIT高可用性アーキテクチャをサポートします。
- **アーカイブ**は一般的に長期保存用であり、多くの場合数年間保持されます。アーカイブはコンプライアンスや規制遵守の目的で使用されることが多いですが、場合によってはIT高可用性アーキテクチャにも利用されます。
- **バックアップやレプリカからのリストア**は1段階のプロセスで、2段階のプロセスで行うアーカイブからのリストアよりも高速です。アーカイブは、ベンダーのバックアップと復旧システムにダウンロードしてから、ITシステムにリストアする必要があります。
- **ランサムウェア攻撃からのリストア**は、最新のバックアップではない可能性のある、クリーンで感染していないコピーにリストアする必要があるため、複雑になります。組織は、不可抗力によって引き起こされたドメインの障害や機能停止からリストアするのと同じ方法で、ランサムウェア攻撃から単にリストアすることはできません。影響を受けた組織は環境を分析し、復旧対象のコピーがそもそも攻撃の原因となったマルウェアに感染していないことを確認する必要があります。以下の表にトポロジーの一覧を示します。なお、すべてのトポロジーには、データが重複排除、圧縮、暗号化された単一のバックアップがあります。バックアップに加えて、各トポロジーは1つ以上のレプリカおよび1つ以上のアーカイブを保持することが可能です。それぞれのトポロジータイプを管理しやすくするために、B1、B2、E1、E2、M1、M2などの識別子を付与しています。

タイプ	コピー数	トポロジー/コピーの種類
基本	1階層	B1: バックアップ
	2	B2: バックアップとアーカイブ
	2	B3: バックアップとレプリケーション
強化	3	E1: バックアップ、レプリケーション、アーカイブ
	3	E2: バックアップとデュアルレプリケーション
ミッションクリティカル	4	M1: アーカイブによるバックアップとデュアルレプリケーション
	4	M2: バックアップ、レプリケーション、デュアルアーカイブ
	5	M3: バックアップ、デュアルレプリケーション、デュアルアーカイブ

タイプ/トポロジーの組み合わせは、**コピーの数とそれらのコピーの性質**によって定義されます。例えば、常に3つのコピーを含む強化タイプには、2つの異なるトポロジーがあります。1つは「バックアップ、レプリケーション、アーカイブ」で、もう1つは「バックアップとデュアルレプリケーション」です。すべてのデータコピーの組み合わせが上記に記載されているわけではなく、このリストは一般的な展開例を示したものに過ぎません。一部の組み合わせは、ビジネス上または技術上の観点から意味をなさない場合もあります。

どのトポロジーが一般的に使用されているか、どれがそうでないかを理解することは有益です。各パターンの相対的な普及度は、ITチームがデータ資産の追加保護を検討する際の「アップグレード」パスの参考になります。

ブループリント: トポロジー一覧

タイプ、トポロジー、顧客向け高可用性アーキテクチャについて説明したので、次に業界で用いられているブループリントの一覧を示します。

このチャートは、これまでに説明したすべての概念をまとめたものです。すべての構成は、実際に企業がCohesityを用いて大規模に運用している、現実的に人気のある選択肢を表しています。

タイプ	トポロジー/コピーの種類	顧客向け高可用性アーキテクチャ		
		アクティブ/スタンバイ	アクティブ/アクティブ	ハブアンドスポーク
基本	B1 バックアップ (1)	•	•	
	B2 バックアップとアーカイブ (2)	•	•	
	B3 バックアップとレプリケーション (2)	•	•	
強化	E1 バックアップ、レプリケーション、アーカイブ (3)	•	• •	•
	E2 バックアップとデュアルレプリケーション (3)	•	•	
ミッションクリティカル	M1 アーカイブによるバックアップとデュアルレプリケーション (4)	•		
	M2 バックアップ、レプリケーション、デュアルアーカイブ (4)	•	•	
	M3 バックアップ、デュアルレプリケーション、デュアルアーカイブ (5)		•	

ミッションクリティカルのトポロジーについて、ひとつ注意すべき点があります。これらのトポロジーは、企業やその他の大規模な顧客に対して、導入、デモンストレーション、トライアル、あるいは詳細な議論が行われてきたものです。先に述べたように、多くのお客様は導入環境のレジリエンス向上を求めています。この議論には、データの追加コピーを保護する実用的な方法が含まれています。一般的な解決策として、サイバー保管庫の導入による強化が挙げられます。そのため、多くのミッションクリティカルなトポロジーには、サイバー保管庫として設定されたアーカイブが含まれています。(このシナリオではCohesity FortKnoxを提供しています。) 多くのトポロジーは、サイバー保管庫を追加することでサイバーレジリエンスをさらに強化することができます。

ここからは、タイプとトポロジーをグループごとに詳しく解説していきます。

ベーシック

トポロジー	プライマリデータセンター	アクティブ/アクティブ
B1: バックアップ	✓	✓
B2: バックアップとアーカイブ	✓	✓
B3: バックアップとレプリケーション	✓	✓

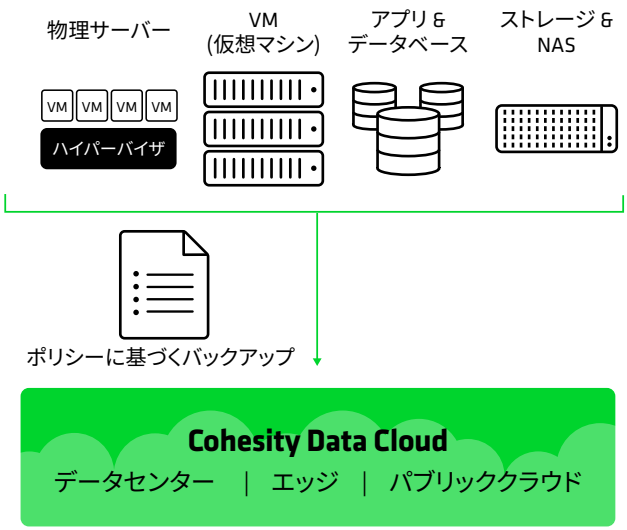
ベーシックは、価値が低〜中程度のデータ、あるいは既に複数のデータコピーを保持しているお客様に人気があります。ベーシックトポロジーは、プライマリデータセンターが単一の場合や、アクティブ/アクティブ方式の場合にも採用されます。

サイバー保管庫とは?

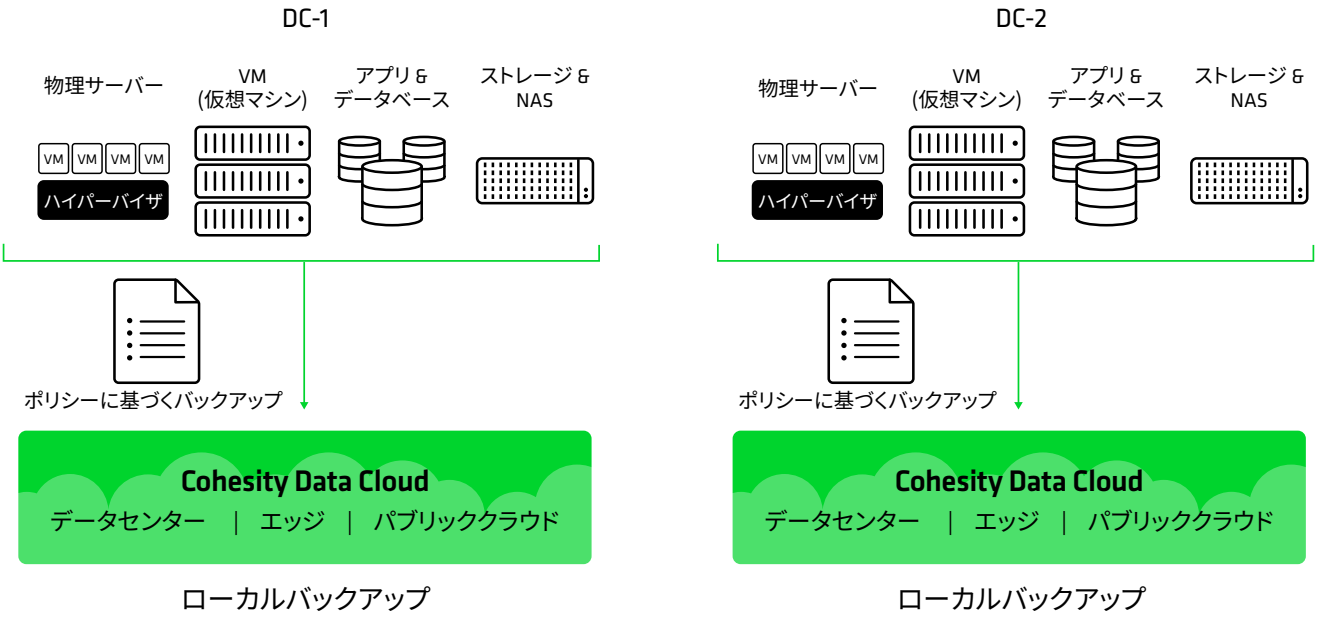
サイバー保管庫には、多くの場合オフサイトに隔離された本番データのコピーが保存されます。クリーンで、分離され、保護されたデータのコピーが常に準備されていることで、企業の本番システムまたはプライマリバックアップシステムを侵害するランサムウェア攻撃やその他のインシデントが発生した場合に、組織は迅速にデータを元の場所へ復旧したり、別のバックアップの場所へ復旧したりすることができます。最新のサイバー保管庫戦略では、バックアップを保護しつつ、一時的なネットワーク接続を可能にする"仮想エアギャップ"テクノロジーを使用することで、必要に応じてクラウドにデータをさらに隔離しつつ、非常に強力なコントロール下におきながらも、必要なリモートアクセスを可能にします。適切に設計されたサイバー保管庫は、堅牢なデータ隔離とサイバーレジリエンス戦略における効果的な要素となり得ます。

ベーシック: B1: ローカルバックアップ

これは、データのバックアップコピーを1つだけに抑えた最小限のアプローチです。多くのITデータセンターでは今もこのアプローチが採用されていますが、災害復旧やバックアップデータの長期保存の仕組みは含まれていません。このアプローチは通常、価値の低いデータに対して用いられます。



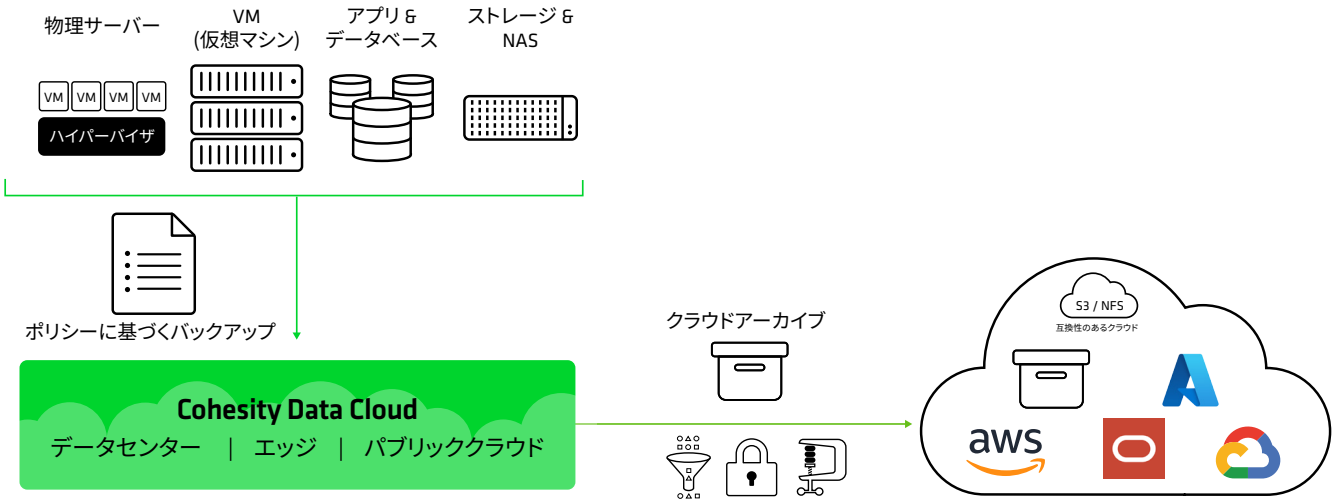
ベーシック: B1: バックアップ (アクティブ/アクティブ)



ローカルバックアップ　　ローカルバックアップ

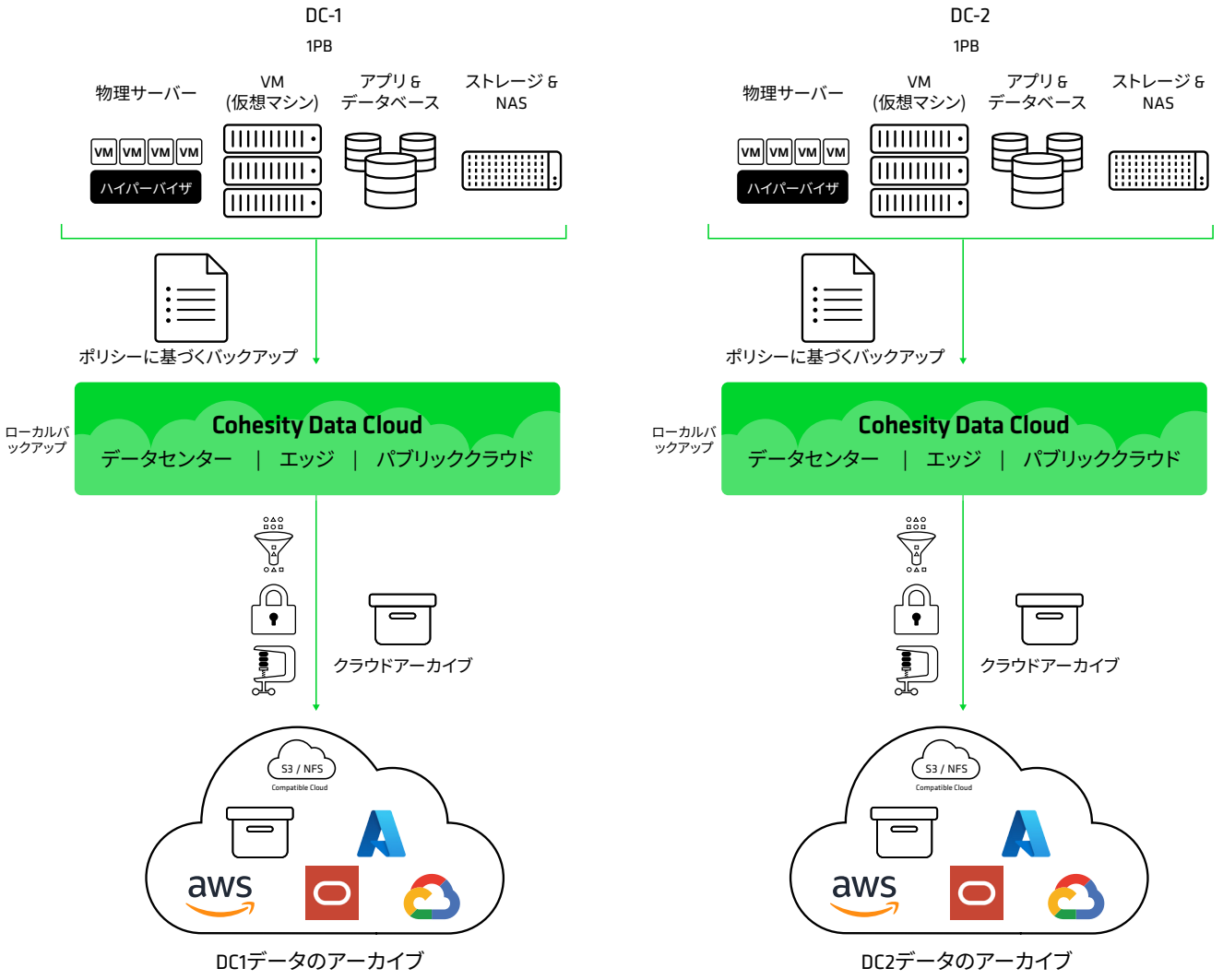
多くのタイプやトポロジーはアクティブ/アクティブ方式に適しています。アクティブ/アクティブ方式は、単一のトポロジータイプを2つ用い、ミラーリングされた状態で相互に連携する構成です。このトポロジーでは、アクティブ/アクティブ方式の2つのデータセンターがあり、それぞれが独自のバックアップを保持します。どちらかのデータセンターで障害が発生しても、もう一方がその役割を引き継ぐことができます。また、各データセンターは、データとワークロードの完全なバックアップを保持しています。利用可能なWAN帯域幅が十分にあるお客様であれば、バックアップもデータセンターから地理的に分離することで、災害対策をさらに強化することが可能です。ワークロードとデータのすべてのレプリケーションはワークロード層で行われるため、このトポロジーではレプリケーションを行う必要はありません。

ベーシック: B2: バックアップとアーカイブ



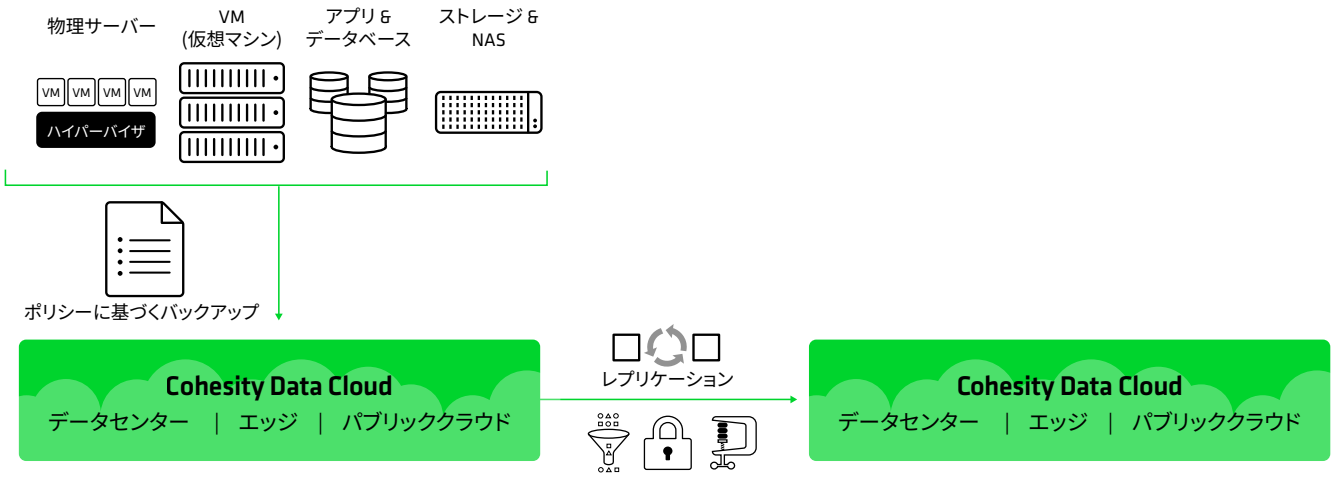
この場合、バックアップは、はるかに長期保存を目的としたアーカイブと組み合わされています。ここではCohesity FortKnoxが人気の選択肢で、このトポロジーのセキュリティを強化します。FortKnoxは隔離されたアーカイブであり、アーカイブへの書き込みやアーカイブからのリストアが行われるときのみ接続されます。また、アーカイブはオンプレミスまたはオフプレミスのプライベートクラウドや、AWS、Google Cloud、Microsoft Azure、Oracle Cloud、あるいはS3/NFS互換のクラウドサービスなどのパブリッククラウドに保存することも可能です。

ベーシック: B2: バックアップとアーカイブ (アクティブ/アクティブ)



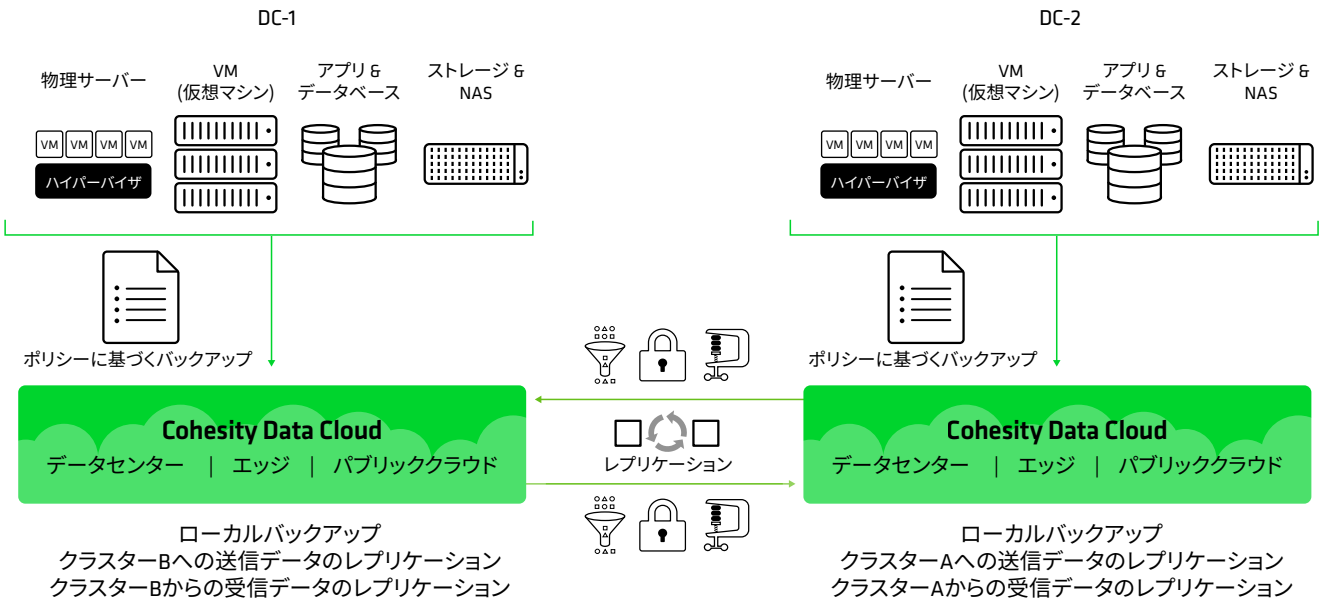
このトポロジーでは、アクティブ/アクティブ方式の2つのデータセンターがあり、それぞれが独自のバックアップとアーカイブを保持します。いずれかのデータセンターで障害が発生した場合、もう一方が役割を引き継ぐことができます。また、各データセンターはアーカイブを通じて自らのデータとワークロードの完全なバックアップを保持しています。ワークロードとデータのすべてのレプリケーションはワークロード層で行われるため、このトポロジーではレプリケーションを行う必要はありません。FortKnoxは、その隔離性とセキュリティ強化の点で、アーカイブとして有用な選択肢です。

ベーシック: B3: バックアップとレプリケーション (災害復旧)



このトポロジーでは、バックアップとレプリカの保持期間がほぼ一致しています。レプリカは地理的に分散され、災害復旧に使用されます。利用可能なWAN帯域幅が十分にあるお客様であれば、バックアップもデータセンターから地理的に分離することで、災害対策をさらに強化することが可能です。このトポロジーは、バックアップが利用できない場合の事業継続性に重点を置いています。レプリカは、アーカイブ利用時に必要な2段階のプロセスを経ることなく、データを直接リストアすることができます。

ベーシック: B3: バックアップとクロスレプリケーション (アクティブ/アクティブ)



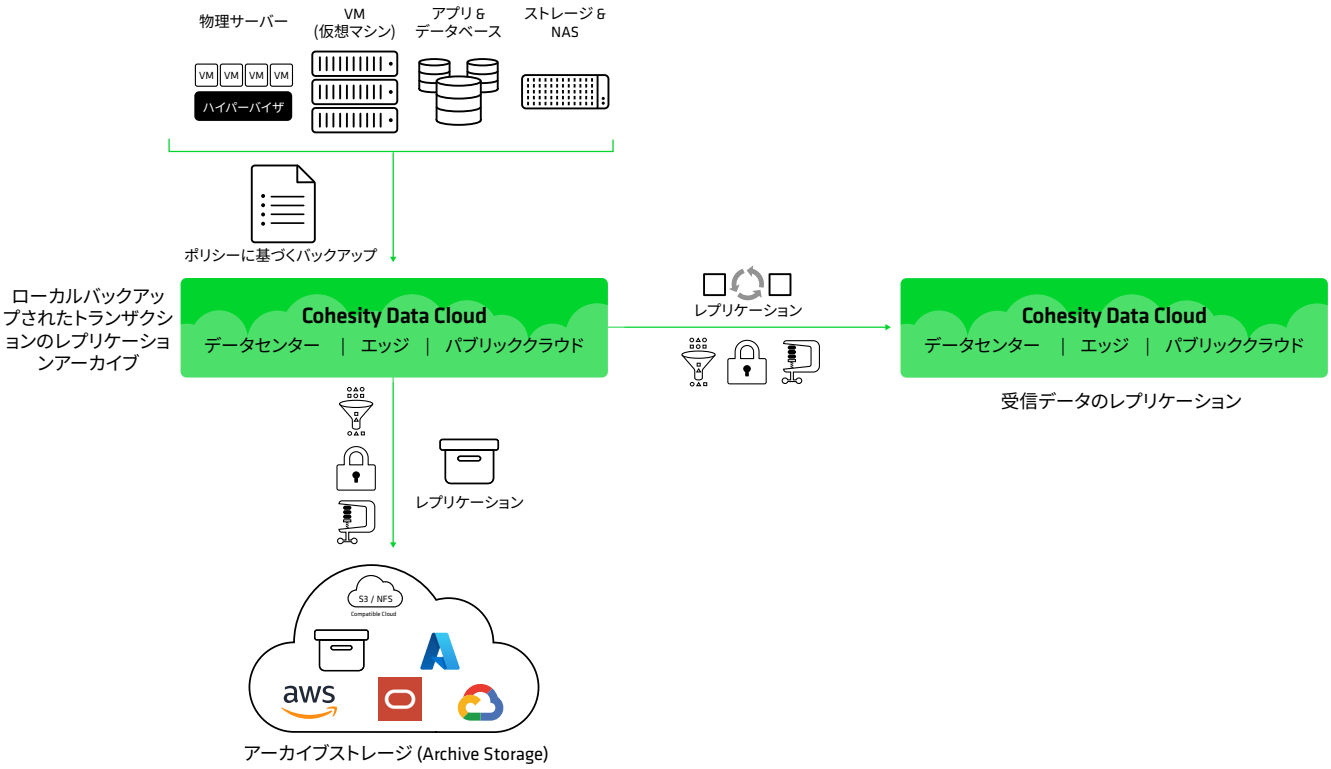
この場合、バックアップとレプリケーションのクラスターが相互にレプリケーションされます。第1サイトのバックアップは第2サイトのレプリカになり、その逆も同様です。

強化トポロジー (業界ごとの採用を含む)

強化トポロジーは、価値の高いデータで人気があります。「バックアップ、レプリケーション、アーカイブ (E1)」が最も一般的なのに対し、「バックアップとデュアルレプリケーション (E2)」はそれほど一般的ではありません。一般的に使われているトポロジーには下記の印が付けられており、業界別の注目されている人気の構成も併せて示しています。

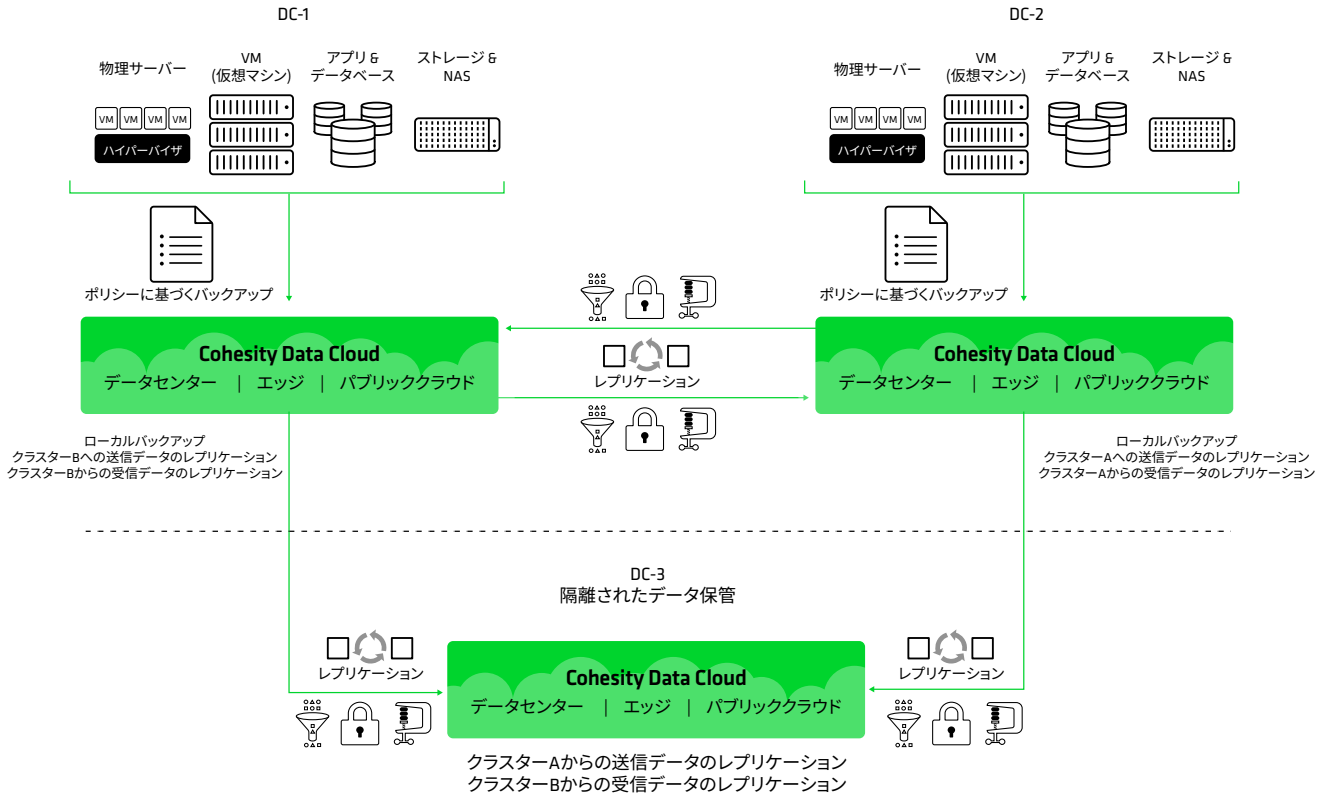
トポロジー	プライマリデータセンター	アクティブ/アクティブ	ハブアンドスポーク
E1: バックアップ、レプリケーション、アーカイブ	✓ すべてのタイプ	✓ 金融機関	
E2: バックアップとデュアルレプリケーション	✓ 政府機関	✓ 小売チェーンや一部の政府機関でイースト/ウェストモデルを採用	

強化: E1: バックアップ、レプリケーション、アーカイブ



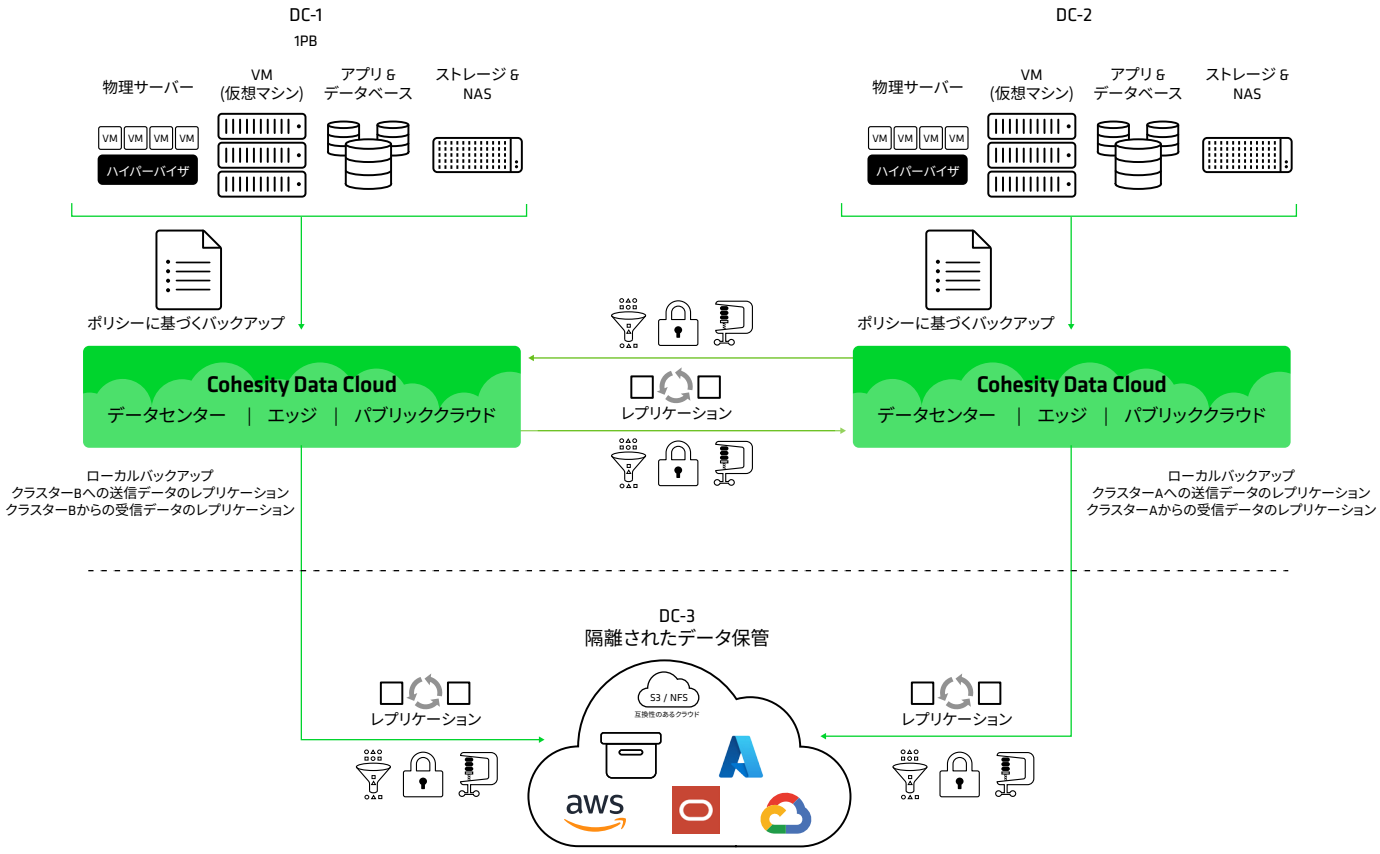
バックアップとレプリカは概ね同じ保持期間(例: 1日に2回の取得を90日間) ですが、アーカイブは数か月から数年にわたって保存されます。バックアップやレプリカからの復旧は1段階のプロセスですが、アーカイブからの復旧は2段階で行われます。つまり、まずアーカイブからデータを読み出し、その後リストアを実施します。また、アーカイブはオンプレミスまたはオフプレミスのプライベートクラウドや、AWS、Google Cloud、Microsoft Azure、Oracle Cloud、あるいはS3/NFS互換のクラウドサービスなどのパブリッククラウドに保存することが可能です。FortKnoxは隔離性とセキュリティを強化するため、このトポロジーに非常に適した選択肢です。また、Cohesity Data Cloudを利用すれば、アーカイブはプライマリクラスターまたはセカンダリクラスターのいずれからでもリストアすることができます。

強化: E1: データ保管庫を使ったアクティブ/アクティブ



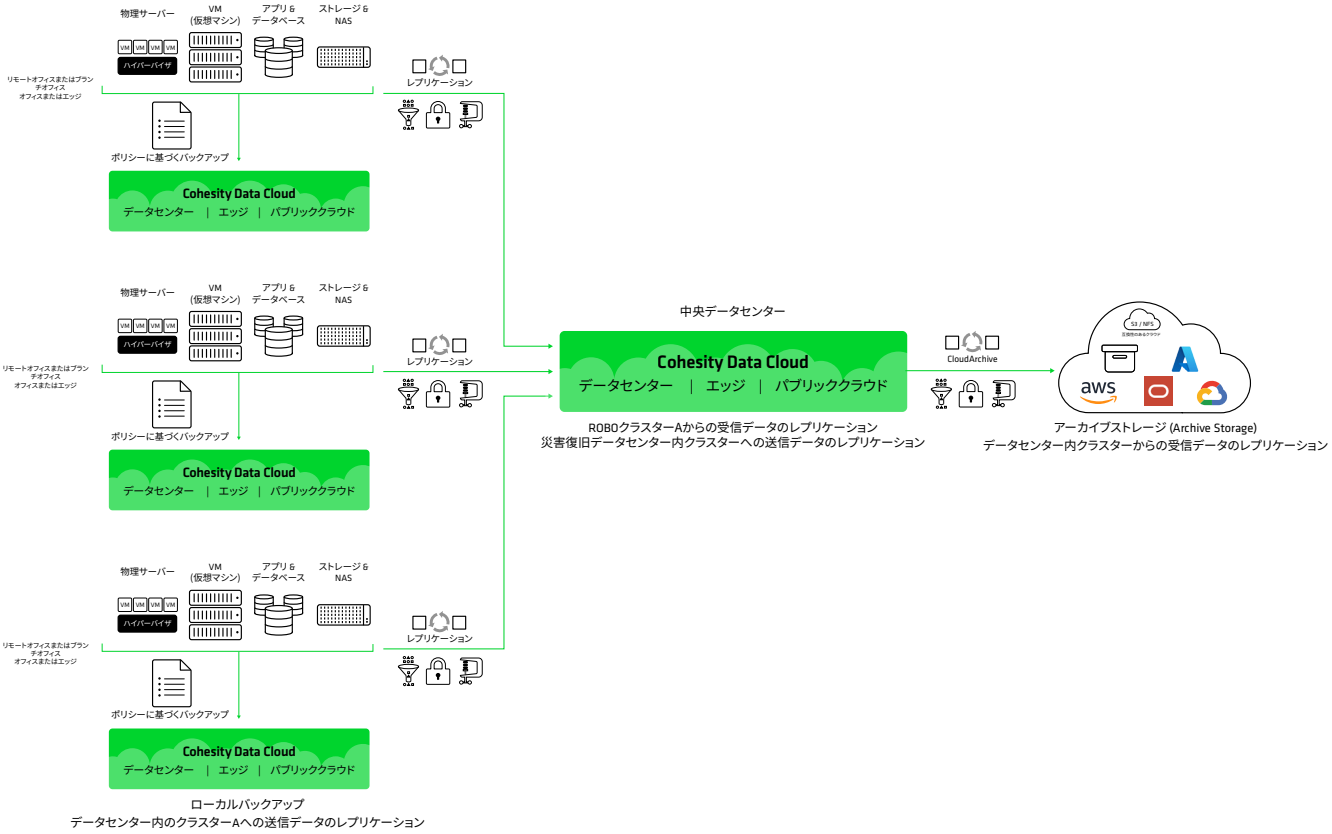
このトポロジーもまた**アクティブ/アクティブ**方式の一種です。この方式では、相互にレプリケーションされたデータセンターが、単一の隔離されたデータ保管庫を共有します。隔離は物理的に行われており、データ保管庫は使用していないときはネットワークから切り離されています。この保管庫はレプリカであるため、どちらのデータセンターもレプリカから1段階で復旧可能です。また、このアーキテクチャは拡張可能で、複数のアクティブ/アクティブ構成が同じデータ保管庫を共有して利用することも可能です。

強化: E1: 隔離アーカイブを使用したアクティブ/アクティブ



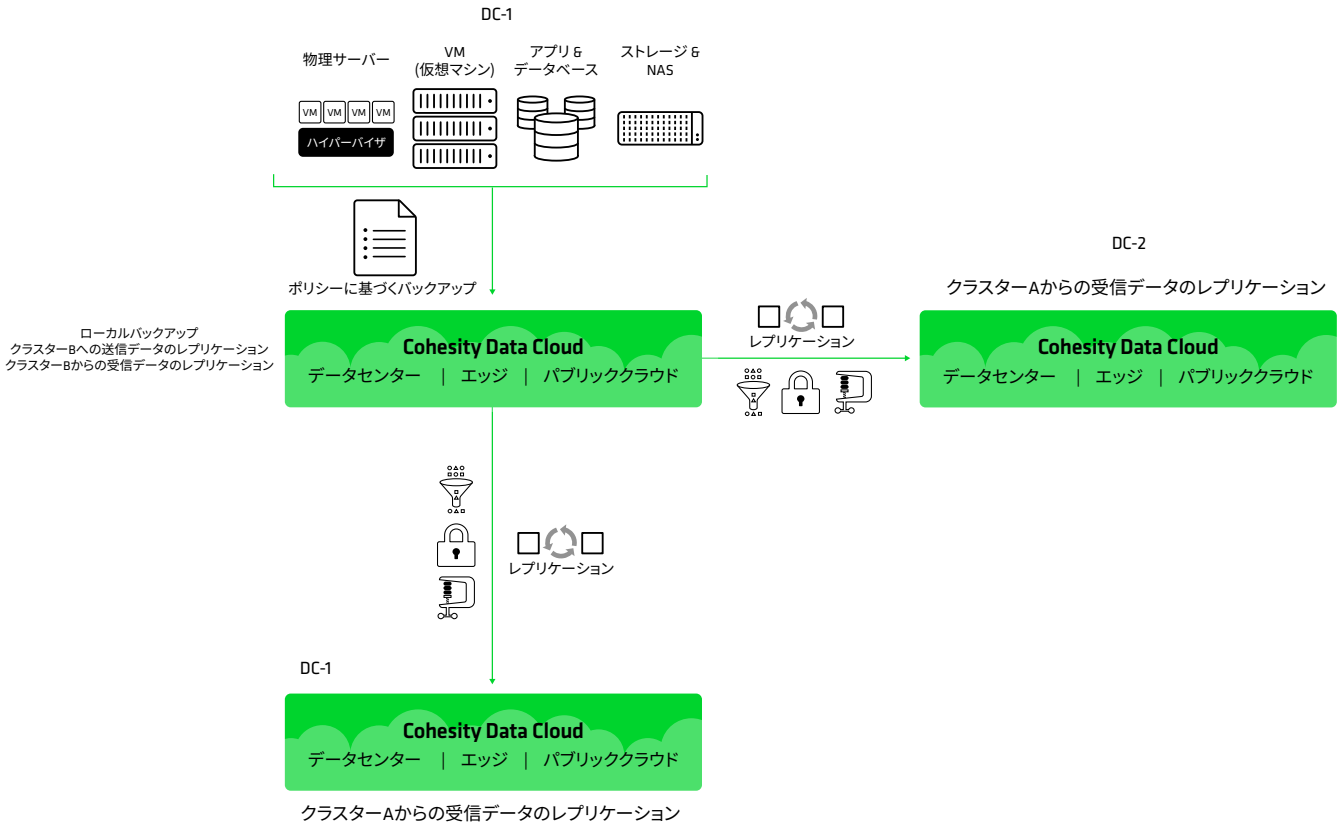
上図は別の**アクティブ/アクティブ**方式の例です。この場合、相互にレプリケーションされたデータセンターが、単一の隔離されたアーカイブを共有しています。このユースケースには、隔離性とさらなるセキュリティを備えたFortKnoxのアーカイブ方式が非常に適しています。また、このアーキテクチャは拡張可能で、複数のアクティブ/アクティブ構成が同一の隔離されたアーカイブを共有して利用することも可能です。Cohesity Data Cloudでは、アーカイブを任意のバックアップまたはレプリカにリストアすることができます。

強化: E1: バックアップ、レプリケーション、アーカイブ (ハブアンドスポーク)



多くのトポロジーは、**ハブアンドスポーク** (ファンイントポロジーとも呼ばれます) に拡張することができます。ハブアンドスポークモデルでは、各拠点に独自のバックアップがあり、これらのバックアップは中央データセンター内の単一の統合されたCohesity Data Cloudに複製されます。中央データセンターでは、レプリカがFortKnox、またはその他のプライベート/パブリックアーカイブに保存されます。FortKnoxは、バックアップとレプリカの両方が侵害された場合でも完全な隔離を提供するため、非常に適した選択肢です。Cohesity Data Cloudを利用すれば、アーカイブはプライマリクラスターまたはセカンダリクラスターのいずれからでもリストアすることができます。

強化: E2: バックアップとデュアルレプリケーション



このトポロジーは、アーカイブからの2段階のリストアプロセスではRTO (復旧時間目標) を十分に低く抑えられない場合に適しています。この構成では、3つのコピー (バックアップおよび両方のレプリカ) すべてを利用して、データを1段階のプロセスでリストアすることが可能です。

強化: E2: アクティブ/アクティブ・ハブを使用したハブアンドスポーク

このトポロジーは、いくつかの異なるモデルを組み合わせています。各リモート拠点はそれぞれでバックアップを行い、そのバックアップは中央データセンターに複製されます。この中央データセンターには、バックアップとして災害復旧用のデータセンターも存在します。両者はミラーリングされており、左側のプライマリデータセンターは右側のデータセンターの災害復旧サイトとして機能し、その逆も同様です。

ミッションクリティカル

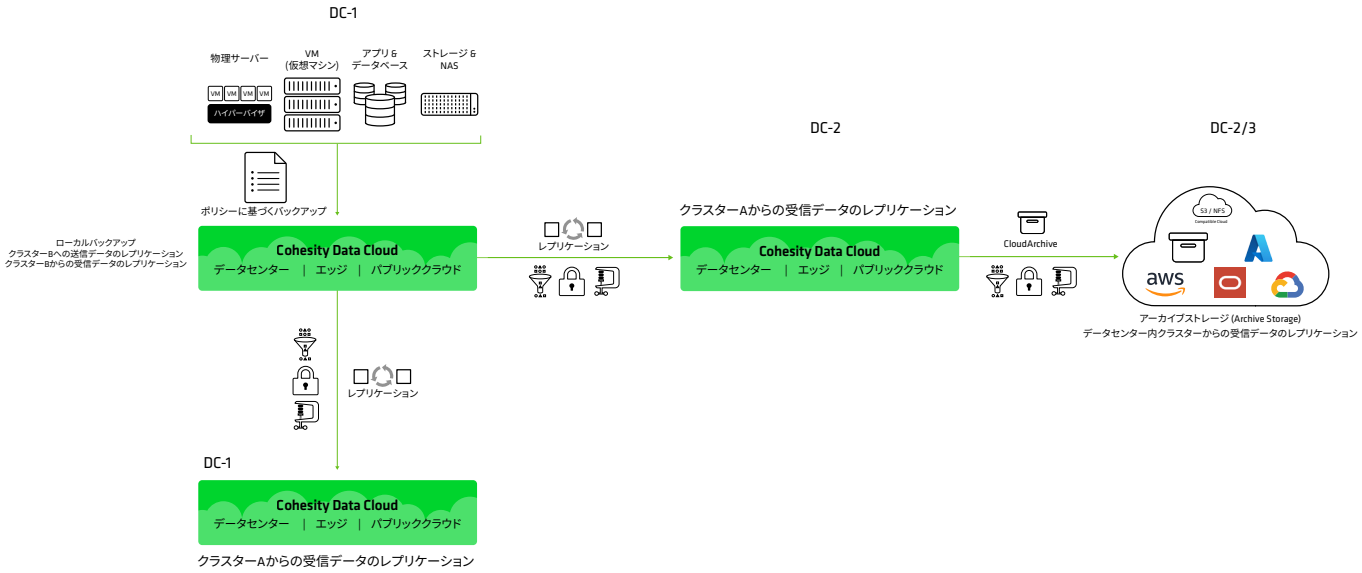
トポロジー	単一のデータセンター	アクティブ/アクティブ	ハブアンドスポーク
アーカイブによるバックアップとデュアルレプリケーション	✓		✓
バックアップ、レプリカ、デュアルアーカイブ	✓	✓	
バックアップ、デュアルレプリカ、デュアルアーカイブ		✓	

ミッションクリティカルは、特定の企業における最も価値の高いデータのトポロジーとして台頭しています。これは、最小構成で成立する会社 (MVC) を運営するために必要なデータを指します。

貴社にとっての最小構成で成立する会社 (MVC) とは?

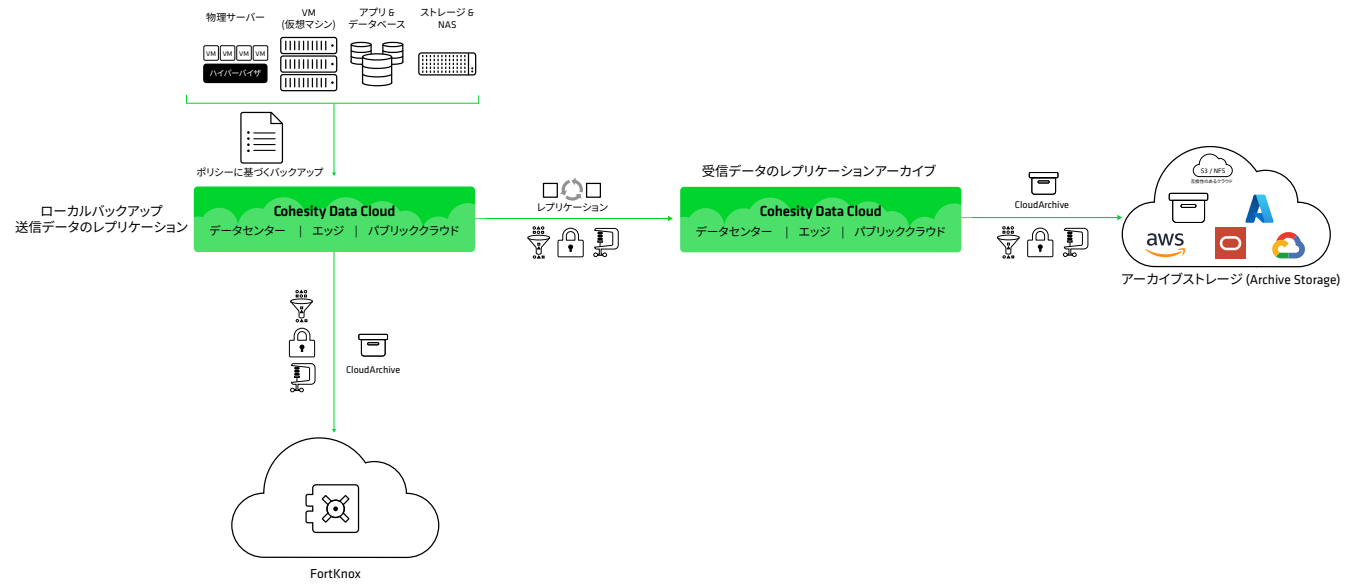
MVC (Minimum Viable Company、最小構成で成立する会社) とは、ビジネスが最低限機能するために復旧が必要なアプリケーション、インフラストラクチャ、プロセスの集合体を指します。これらのシステムは最優先で復旧されるべきであり、その他のシステムは二次的な優先順位となります。ITリーダーは、インシデントの対応と復旧戦略の策定、そしてデータトポロジーの設計において、MVCを活用する必要があります。

ミッションクリティカル: M1: アーカイブによるバックアップとデュアルレプリケーション



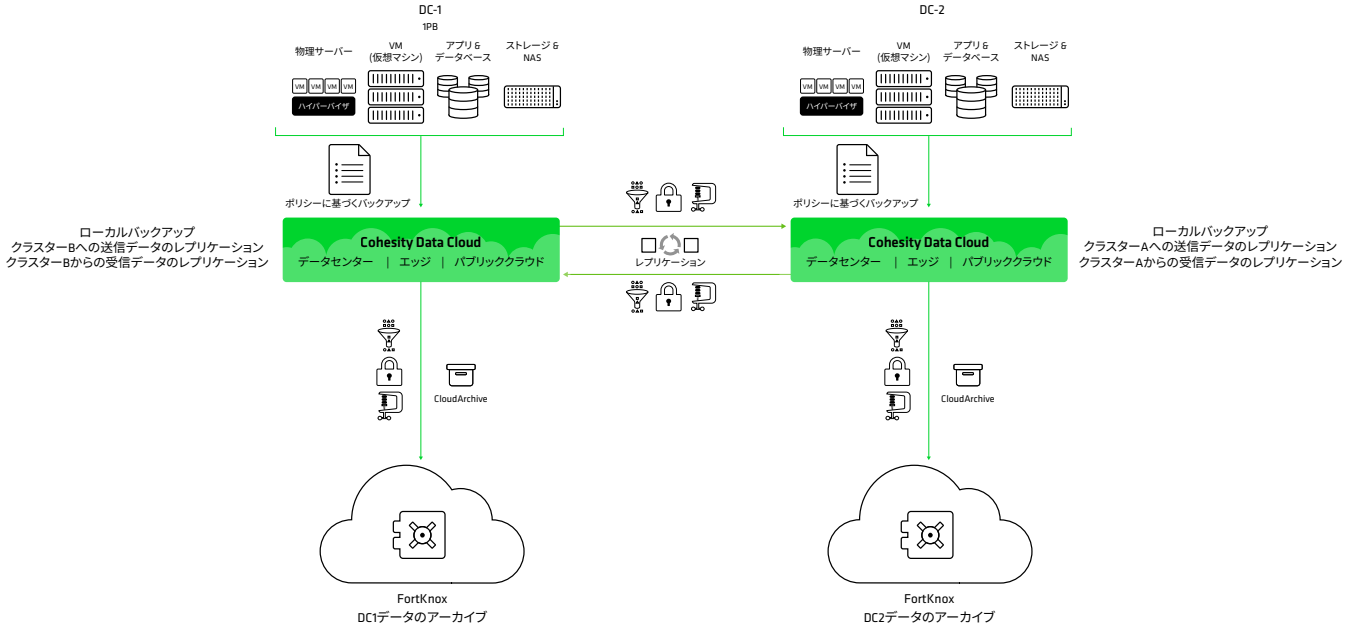
耐障害性アーキテクチャは厳格なRTO (復旧時間目標) およびRPO (復旧時点目標) 要件を満たしており、長期保存要件と組み合わされています。2つ目のレプリカは災害復旧とランサムウェア対策をさらに強化します。Cohesity Data Cloudを利用すれば、アーカイブはプライマリクラスターまたはセカンダリクラスターのいずれからでもリストアすることができます。2つ目のレプリカにエアギャップを追加することで、レジリエンスが強化されます。

ミッションクリティカル: M2: FortKnoxを活用し、デュアルアーカイブ構成のバックアップとレプリケーション (ローカルバックアップ起点)



この耐障害性アーキテクチャでは、2つ目のレプリカの代わりにFortKnoxを使用しており、FortKnoxが追加のセキュリティと隔離を提供します。1つ目のアーカイブはコンプライアンス活動に利用でき、FortKnoxのアーカイブはランサムウェアに対するレジリエンスを強化します。Cohesity Data Cloudを利用すれば、アーカイブはプライマリクラスターまたはセカンダリクラスターのいずれからでもリストアすることができます。

ミッションクリティカル: M2: FortKnoxを使用したローカルからのクロスレプリケーションとアーカイブ



これは、**ベーシックトポロジーで紹介したアクティブ/アクティブ**モデルに、二重のFortKnoxアーカイブを加えたものです。各クラスターにDC1とDC2の両方のコピーが含まれているため、各FortKnoxインスタンスにもDC1とDC2のコピーが含まれています。Cohesity Data Cloudを利用すれば、アーカイブはプライマリクラスターまたはセカンダリクラスターのいずれからでもリストアすることができます。

ミッションクリティカル: M3: アクティブ/アクティブ・ハブとFortKnoxアーカイブによるハブアンドスポーク

これは、**強化**タイプで紹介したものに類似していますが、この場合は各レプリカが長期アーカイブとしてFortKnoxに接続されています。レプリカは左右両方のスポークのコピーを保持しているため、各FortKnoxアーカイブも両方のコピーセットを保有しています。Cohesity Data Cloudを利用すれば、アーカイブはプライマリクラスターまたはセカンダリクラスターのいずれからでもリストアすることができます。

結論と次のステップ

多くの企業リーダーは、重要データの保護を強化したいと考えています。こうした意思決定者と新たなアプローチを議論する際に、ブループリントは不可欠です。本ホワイトペーパーで紹介した設計は、同様のデータ保護要件を持つ類似の状況で、他の経営者がどのような対策を講じてきたかを理解する手助けとなります。

データのコピーに関しては、「多ければ多いほど良い」というわけではありません。Cohesityもお客様も、データのコピーを増やすことが、運用コストやライセンスコスト、さらにはハードウェアコストの増加に繋がることを理解しています。場合によってCohesityは、単にコピーを増やすのではなく、異なる種類のコピーを利用することを推奨しています。

多くの場合、会社のコンプライアンス活動やサイバーレジリエンスの向上のためにアーカイブの使用を推奨します。そのため、多くのお客様はデータのコピー数は変えずに、使用するコピーの種類を変更することを選択します。例えば、オンサイトにあるセキュアでないアーカイブを、コンプライアンスとランサムウェアレジリエンス対策の両方に活用可能なコピーを提供する、FortKnoxのような隔離されたアーカイブに置き換えることがあります。

ブループリントは、すべての関連する実績ある選択肢を検討し、その中から自社の導入に最適なものを情報に基づいて選択できるため、非常に有用です。

以下の表は、障害ドメイン、不可抗力、サイバー保護に関連する各トポロジーの利点をシンプルにまとめたものです。

タイプ	基本		強化	ミッションクリティカル	
コピー数	1	2	3	4	5
トポロジー	バックアップのみ	バックアップとリポジトリ (レプリカまたはアーカイブ)	バックアップとデュアルリポジトリ (レプリカとアーカイブ、またはデュアルレプリカ)	バックアップ、デュアルレプリカ、アーカイブ	バックアップ、デュアルレプリカ、デュアルアーカイブ
ハードウェアやソフトウェア障害ドメインからの保護	★	★ ★	★ ★ ★	★ ★ ★ ★	★ ★ ★ ★
不可抗力からの保護		★	★ ★ ★	★ ★ ★ ★	★ ★ ★ ★
サイバー保護	★	★ ★	★ ★ ★	★ ★ ★ ★	★ ★ ★ ★

最新のデータセキュリティとデータ管理への道のりは、険しく感じられるかもしれません。お客様がリスクとコストを抑えながら、より良いビジネス成果をより迅速に達成できるよう支援するため、このブループリント情報をまとめました。

ここからは、次のステップとして以下を推奨します:

1. 貴社の状況に最も適したブループリントを特定します。
2. 現在のソリューションと比較し、最新のデータプラットフォームのROI (投資対効果) とTCO (総所有コスト) を評価します。比較する際の重要ポイントは以下の通りです:
    a. データ保護の効率性
    b. 運用効率
    c. リスクとコンプライアンス
3. 製品デモ、実績あるROIやTCOの算出結果、ロードマップの優先事項への対応状況を基に、ソリューションを選定します。
4. 最も適切なブループリントに従って選択したソリューションを導入し、前のステップで作成したロードマップの実行に進みます。

最新のプラットフォームを導入したら、サイバーレジリエンスに関する初期KPIを設定し、この基準に対して定期的に進捗を測定します。そこから、次のフェーズへ進むタイミングを把握できるようになります。

Cohesityについて

Cohesity はAIを活用したデータセキュリティのリーダーです。Fortune 100のうち85社以上、Global 500の約70%を含む13,600社以上のエンタープライズ顧客が、膨大なデータに対して生成AI (Gen AI) によるインサイトを提供しながら、Cohesityを活用してレジリエンスを強化しています。Veritas社のエンタープライズ向けデータ保護事業との統合により誕生したCohesityのソリューションは、オンプレミス、クラウド、エッジ環境におけるデータのセキュリティと保護を実現します。NVIDIA、IBM、HPE、Cisco、AWS、Google Cloudなどと連携し、Cohesityはカリフォルニア州サンタクララに本社を置き、世界各地にオフィスを展開しています。詳しくは、CohesityのLinkedIn、X (旧Twitter)、Facebookをフォローしてください。

Cohesityの詳細はこちら

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000050-002 EN 4-2025