Hewlett Packard
Enterprise

Data Protector

ソフト ウェア バージョン: 10.00

コンセプト ガイド

ドキュメント リリース日 : 2017年 6月
ソフト ウェア リリース日 : 2017年 6月

ご注意

保証

Hewlett Packard Enterprise Development LP製品に関する保証は、製品およびサービスに付属する保証規定に明示されている内容に限定されます。本書のいかなる記述も、追加の保証を構成するものではありません。HPEは、本書の技術的内容や編集に関する誤りや欠落に関して責任を負いません。

ここに記載する情報は、予告なしに変更されることがあります。

権利の制限

機密コンピューターソフトウェア。保持、使用、またはコピーには、HPEからの有効なライセンスが必要です。FAR 12.211および12.212に従って、商用コンピューターソフトウェア、コンピューターソフトウェアドキュメント、および商用品目の技術データは、米国政府に対して、ベンダーの標準商用ライセンスに基づいてライセンスされます。

著作権について

商標について

Adobe™はAdobe Systems Incorporatedの商標です。

Microsoft®およびWindows®は、米国におけるMicrosoft Corporationの登録商標です。

UNIX®は、The Open Groupの登録商標です。

この製品には、'zlib' 汎用圧縮ライブラリのインタフェースが含まれています。Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

ドキュメントの更新情報

このマニュアルの表紙には、以下の識別情報が記載されています。

- ソフトウェアバージョンの番号は、ソフトウェアのバージョンを示します。
- ドキュメントリリース日は、ドキュメントが更新されるたびに変更されます。
- ソフトウェアリリース日は、このバージョンのソフトウェアのリリース期日を表します。

最新のソフトウェア更新をチェックするには、次のサイトを参照してください。
https://softwaresupport.hpe.com/patches

更新状況、およびご使用のドキュメントが最新版かどうかは、次のサイトで確認できます。
https://softwaresupport.hpe.com/manuals

このサイトを利用するには、HPE Passportへの登録とサインインが必要です。HPE Passport IDの登録は、次のWebサイトから行なうことができます。https://hpp12.passport.hpe.com/hppcf/login.do.

適切な製品サポートサービスをお申し込みいただいたお客様は、更新版または最新版をご入手いただけます。詳細は、HPEの営業担当にお問い合わせください。

サポート

HPEソフトウェアサポートオンラインWebサイトを参照してください。https://softwaresupport.hpe.com

このサイトでは、HPEのお客様窓口のほか、HPEソフトウェアが提供する製品、サービス、およびサポートに関する詳細情報をご覧いただけます。

HPEソフトウェアオンラインではセルフソルブ機能を提供しています。お客様のビジネスを管理するのに必要な対話型の技術サポートツールに、素早く効率的にアクセスできます。HPソフトウェアサポートのWebサイトでは、次のようなことができます。

- 関心のあるナレッジドキュメントの検索
- サポートケースの登録とエンハンスメント要求のトラッキング

- ソフトウェアパッチのダウンロード
- 製品ドキュメントへのアクセス
- サポート契約の管理
- HPEサポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェアカスタマーとの意見交換
- ソフトウェアトレーニングの検索と登録

一部のサポートを除き、サポートのご利用には、HPE Passportユーザーとしてご登録の上、サインインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。

HPE Passport IDを登録するには、次のWebサイトにアクセスしてください。
https://hpp12.passport.hpe.com/hppcf/login.do

アクセスレベルの詳細については、次のWebサイトをご覧ください。
https://softwaresupport.hpe.com/web/softwaresupport/access-levels

目次

本書について

本書では、Data Protectorの概念について説明します。Data Protectorの基礎とモデルについて十分に理解するには、本書をお読みください。

対象読者

本書は、Data Protectorの操作に関する概念を理解することに興味があるユーザーや、企業のバックアップ戦略の立案担当者向けに書かれています。詳細な内容については、『*HPE Data Protectorヘルプ*』も併せて参照してください。

第1章: バックアップとData Protectorについて

この章では、バックアップと復元の概念について説明します。以下では、Data Protectorのアーキテクチャー、メディア管理、ユーザーインターフェイス、バックアップデバイス、およびその他の機能について説明していきます。また、Data Protectorのセットアップ時に必要となる、Data Protectorの構成方法などについても最後に簡単に紹介しています。

Data Protectorについて

HPE Data Protectorは、急速に増加するビジネスデータに対して信頼性の高いデータ保護と優れたアクセス容易性を提供する、バックアップソリューションです。Data Protectorは、特に全社レベルでの管理作業や分散環境に適した、包括的なバックアップ機能および復元機能を提供します。以下のリストは、Data Protectorの主要な特長について説明しています。

- **スケーラビリティと柔軟性に優れたアーキテクチャー**

  Data Protectorは、単一のシステムを使用する環境から、複数のサイト上に何千ものシステムが存在するような環境に至るまで、さまざまな状況で使用できます。Data Protectorではネットワークコンポーネントの概念が採用されているため、バックアップ基盤を構成する各コンポーネントは、希望する構成に応じてさまざまなトポロジ内に自由に配置できます。また、バックアップ基盤をセットアップするためのバックアップオプションと選択肢が豊富に用意されているため、必要に応じて、事実上どのような構成でも実装することが可能です。さらに、Data Protectorでは、合成バックアップやディスクステージングなどの、バックアップ分野の高度な概念を利用することができます。

- **集中管理の容易さ**

  Data Protectorでは、操作性に優れたグラフィカルユーザーインターフェイス(GUI)を使用して、中心となる1つのシステムから、バックアップ環境全体を管理できます。このGUIを複数のシステム上にインストールしておくと、複数の管理者がそれぞれローカルにインストールされたコンソールからData Protectorにアクセスできるようになり、管理作業が容易になります。複数のバックアップ環境を単一のシステムから管理することも可能です。また、Data Protectorにはコマンドラインインターフェイス(CLI)も用意されているので、スクリプトを使用してData Protectorを管理することもできます。

- **高パフォーマンスのバックアップ**

  Data Protectorを使用すると、数百ものバックアップデバイスに同時にバックアップすることができます。また、大容量ライブラリ内のハイエンドデバイスもサポートされます。さらに、ローカルバックアップ、ネットワークバックアップ、オンラインバックアップ、ディスクイメージバックアップ、合成バックアップ、オブジェクトミラーリングを伴うバックアップ、並列データストリームの組み込みサポートなど、多様なバックアップがサポートされるため、ユーザー要件に最適なバックアップを実行できます。

- **データセキュリティ**

  データのセキュリティを強化するため、Data Protectorではバックアップを暗号化して他から保護します。Data Protectorには、ソフトウェアベースとドライブベースの2つのデータ暗号化機能があります。

  セキュアな通信

  Data Protector 10.00より前のバージョンでは、暗号制御通信(ECC)を有効にすることでCell Managerとクライアント間の通信を保護することができました。ECCを有効にすると、クライアントはCell Manager上でホストさ

れているCAによって署名されたCRS要求を生成します。この時点で、証明書にあるCAとホスト名が確認されることで、信頼が確立されます。Data Protector 10.00では、Cell Managerとクライアント間のすべての通信はデフォルトで保護されるようになりました。ルートCAの概念ではなく、証明書ピンニングを用いた自己署名証明書が使用されます。新しいセキュリティモデルには、以下の重要な特徴があります。

- Data Protectorのさまざまなエンティティ間のすべての通信は、セキュアTLS 1.2チャネルを介して行われます。
- WindowsクライアントでのData Protectorエージェントのプッシュインストール時に、セッションメッセージブロック(SMB)署名が使用されるようになりました。インストール時にクライアントにセキュアデータが渡され、攻撃者によってデータが変更されることはないため、署名ありSMBトラフィックによってデータ整合性が提供されます。
- Linux/UnixクライアントでのData Protectorエージェントのプッシュインストール時に、SSHプロトコルが使用されるようになりました。SSHキーがインストールサーバーとクライアントの間で事前構成されていない場合は、クライアントごとにパスワードを求めるプロンプトが表示されます。
- Data ProtectorクライアントとCell Managerが、セキュアピアリングを使用して構成されるようになりました。その際、Cell Managerで認証されるよう、クライアント(ローカルにインストールされている場合)に対してコマンドが実行されます。

コマンド実行の一元化

Data Protectorでは、バックアップ、復元、および復旧の各操作を実行するために、クライアントサーバーモデルが採用されています。これらの操作をサポートするために、あるホストのData Protectorエージェントは、INETで接続を行い、同一または異なるホストのData Protectorエージェントと通信します。特定のシナリオでは、あるホストのエージェントが、別のホストのINETと通信してコマンドを実行する結果、セキュリティ侵害クライアントによるリモートコマンド実行の脆弱性が発生します。

Data Protector 10.00では、Data ProtectorクライアントのINETプロセスは、セキュアTLS 1.2チャネルで送信される場合は、Cell Managerからの接続のみを受け入れます。すべてのコマンドがCell Managerを経由します。集中型コマンド実行により、制御とデータの両方がセキュアTLSチャネルで送信されるため、データ整合性が保証されます。さらに、Data Protectorクライアントは、信頼済みで確認済みのCell Managerからの指示とスクリプトのみをリスンし、受け入れるようになったため、セキュリティブリーチのリスクが大幅に軽減されています。

- **混合環境のサポート**

  Data Protectorは異機種環境をサポートしており、大部分の機能はUNIXプラットフォームとWindowsプラットフォームで共通です。UNIXおよびWindows Cell Managerでは、サポート対象のクライアントプラットフォームをすべて制御できます。Data Protectorユーザーインターフェイスを使用すると、各サポート対象プラットフォーム上のすべてのData Protector機能にアクセスできます。サポートされるプラットフォームの一覧については、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。

- **混合環境におけるインストールの容易性**

  インストールサーバーの存在は、インストール作業およびアップグレード作業を容易にします。UNIXクライアントをリモートでインストールするには、UNIX用インストールサーバーが必要です。また、Windowsクライアントをリモートでインストールするには、Windows用インストールサーバーが必要です。リモートインストールは、Data Protector GUIがインストールされていれば、どのクライアントからでも実行できます。インストールサーバーのサポートされるプラットフォームについては、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。

- **高可用性のサポート**

  Data Protectorは、24時間継続されるビジネス運用にも対応しています。今日のようにビジネス環境が全世界的に分散している状況では、全社レベルの情報資源および顧客サービスアプリケーションは常に利用可能である必要があります。Data Protectorでは、以下の機能を実現することにより、高可用性への要求に対応しています。

  - クラスターとの統合によりフェイルセーフオペレーションを確実に実行し、仮想ノードのバックアップにも対応。サポートされているクラスターのリストについては、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。
  - クラスター上でData Protector Cell Manager自体の実行が可能。
  - 一般に使用されている、すべてのオンラインデータベースのアプリケーションプログラミングインターフェイス(API)をサポート。
  - HPE P9000 XPディスクアレイファミリ、EMC Symmetrixなどの高度な高可用性ソリューションとの統合が可能。
  - WindowsおよびUNIXの各プラットフォーム上で、さまざまなディザスタリカバリ機能を提供。
  - バックアップの実行中および実行後にバックアップデータを複製するためのメソッドを提供。この機能により、バックアップのフォールトトレランスの強化やデータの二重化が容易になります。

- **バックアップオブジェクト操作**

  バックアップとアーカイブ方針を柔軟に選択できるように、個別のバックアップオブジェクトに対して操作を行う場合に高度な技術が使用できます。これには、ディスクのステージングやアーカイブに有効なメディアからメディアへのオブジェクトのコピーや、複数のオブジェクトバージョンの増分バックアップから単一フルバックアップバージョンへの集約などが挙げられます。こうした機能をサポートするために、オリジナルのバックアップオブジェクトとコピーまたは集約されたバックアップオブジェクトを検証する機能も用意されています。

- **復元の容易さ**

  Data Protectorでは、どのシステムのどのファイルが、どのメディア上に保存されているかをトラッキングするための内部データベースが用意されています。システム上の任意の部分を復元する場合、目的のファイルやディレクトリを簡単に一覧することができます。その結果、復元するデータにすばやく簡単にアクセスできます。

- **操作の自動化や無人化**

  Data Protectorでは、内部データベースを使用して、Data Protectorメディアに関する情報と、それぞれのメディア上に保存されているデータに関する情報を管理しています。Data Protectorには高度なメディア管理機能が備わっています。たとえば、あるバックアップデータをいつまで復元可能な状態で保持する必要があるかといった点や、どのメディアがバックアップ用として(再)利用可能かといった点をトラッキングしています。

  また、大容量ライブラリをサポートしているため、数日間あるいは数週間にわたって、オペレーターが介入しない状態で処理を継続することも可能です(自動メディア交換)。さらに、Data Protectorでは、新しいディスクがシステムに接続された場合、自動的にそのディスクを検出して(ディスクディスカバリ)、バックアップすることもできます。これにより、バックアップ構成を手動で調整する必要がなくなります。

- **モニター、レポート、通知**

幅広い通知機能が用意されているため、バックアップ状態のチェックや、活動中のバックアップ動作のモニタリング、レポートのカスタマイズなどを簡単に実行できます。Data Protector GUIまたはCLIを使用して、レポートを生成することもできます。

洗練されたユーザーインターフェイスと簡単で使いやすいWebコントロールが搭載された新しいスケジューラーにより、スケジュール管理が容易になります。スケジュールの優先順位、データ保護、繰り返しパターンの設定や、予定の重複の修正を1つのスケジューラーウィザードで行うことができます。

さらに、Data Protectorの監査機能を使用すると、バックアップセッションの情報の一部を収集して、バックアップ操作の概要を調べることができます。

構成の詳細については、『*HPE Data Protector管理者ガイド*』を参照してください。

- **オンラインデータベースアプリケーションとの統合**

  Data Protectorは、Microsoft Exchange Server、Microsoft SQL Server、Microsoft SharePoint Server、Oracle、Informix Server、SAP R/3、SAP MaxDB、Lotus Notes/Domino Server、IBM DB2 UDB、Sybaseのデータベースオブジェクト、SAP HANA、VMware vSphere、およびHyper-Vオブジェクトに対するオンラインバックアップ機能を備えています。個々のオペレーティングシステムでサポートされるバージョンのリストについては、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。

- **他の製品との統合**

  さらに、Data Protectorは、EMC Symmetrix、Microsoft Cluster Server、HPE Serviceguardをはじめとする他のVMwareとの統合も可能です。

これらの統合機能や、最新のプラットフォームおよび統合サポート情報など、Data Protector機能の詳細については、HPE Data Protectorのホームページ(https://softwaresupport.hpe.com/)でご確認ください。

バックアップと復元の概要

この項では、バックアップと復元についてそれぞれの基礎的な概念を説明します。

バックアップとは

バックアップとは、バックアップメディア上にデータのコピーを作成するプロセスのことです。このコピーは、オリジナルのデータが破損した場合に備えて保管されます。

バックアップをわかりやすく抽象化すると、バックアッププロセス、下のような形になります。

バックアッププロセス

通常**ソース**となるのは、ファイル、ディレクトリ、データベース、アプリケーションなど、ディスク上のデータです。作成したバックアップをディザスタリカバリ用として使用する場合は、一貫性のある形でバックアップデータを作成することが大切です。

バックアップアプリケーションとは、バックアップ先 に実 際 にデータをコピーするソフトウェアのことです。また**バックアップ先** とは、テープドライブやディスクベースのデバイスのような、バックアップデバイスを指します。これらのデバイス内 のメディアにデータのコピーが書き込まれます。

復元とは何か

復元とは、バックアップコピーから、オリジナルのデータを再作成するプロセスのことです。このプロセスは、事前準備、実際のデータの復元、およびデータを実際に使用するための何らかの事後処理の3段階に分けることができます。

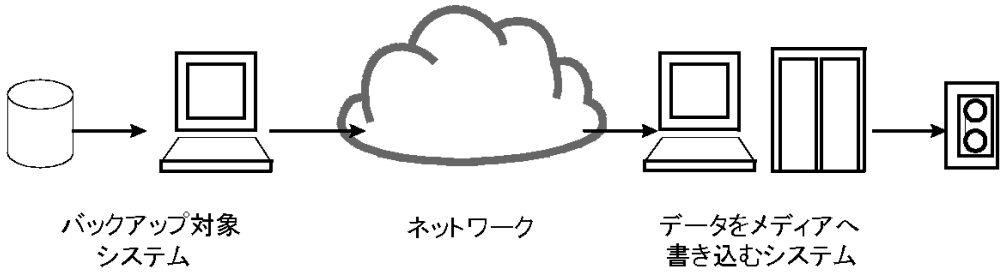
復元プロセス

復元プロセスの**ソース**はバックアップコピーです。また復元アプリケーションとは、復元先に実際にデータを書き込むソフトウェアのことです。**復元先** は通常、オリジナルデータの書き込み先となるディスクです。

ネットワーク環境のバックアップ

ネットワーク環境のバックアップでは、データはネットワークを介して、バックアップ対象のシステムから、バックアップデバイスが接続されているシステム上 のメディアに送信されて保存されます。

ネットワークバックアップ



ネットワーク環境のバックアップを実現するには、次の機能を備えたアプリケーションが必要です。

- バックアップデバイスを、ネットワーク内 の任意のシステムに接続できること。

  これにより、コスト削減を目的として、ローカルバックアップ(大容量データを格納したシステム用)とネットワークバックアップの両方を実行することが可能となります。
- 任意のネットワークパスに、バックアップデータフローを経路指定できること。
- データ量またはネットワークトラフィックが原因でLAN転送の効率が悪い場合は、バックアップデータの転送経路をLANからSANに変更できること。
- 任意のシステムからバックアップ活動を管理できること。

- IT管 理 の枠 組 みに統 合 できること。
- さまざまなタイプのバックアップ対 象 システムをサポート できること。

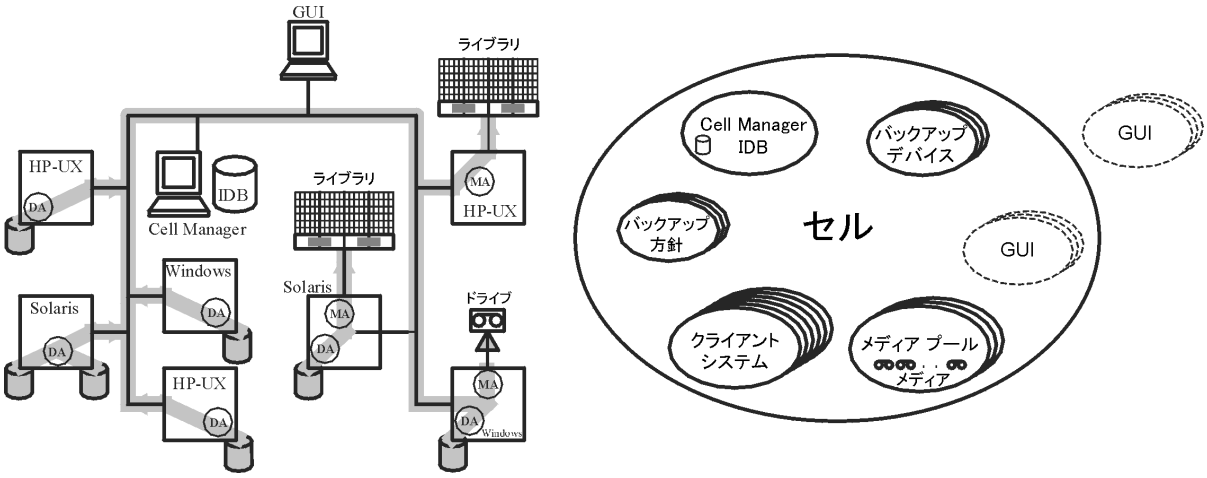
Data Protectorのアーキテクチャー

Data Protectorセル(物 理 的 な構 成 図 と論 理 的 な構 成 図)、下 に示 されているData Protector**セル**は、**Cell Manager**、**クライアントシステム**、および**デバイス**が存 在 するネットワーク環 境 です。Cell Managerは中 央 の制 御 ポイントであり、Data Protectorソフトウェアのインストール先 となります。Data Protectorソフトウェアのインストールが終 了 したら、バックアップ対 象 となる各 システムを追 加 できます。これらのシステムは、セルの構 成 要 素 である、Data Protectorクライアントシステムとなります。Data Protectorを使 用 してファイルのバックアップを実 行 すると、これらのファイルはバックアップデバイス内 のメディアに保 存 されます。

バックアップしたファイルに関 する情 報 は、**Data Protector内 部 データベース(IDB)**内 で管 理 されるため、ブラウザーを使 用 して、システム全 体 、あるいは特 定 のファイルのみを簡 単 に復 元 できます。

Data Protectorを使 用 するとバックアップ作 業 および復 元 作 業 が容 易 になります。Data Protectorユーザーインターフェイスを使うと、即 時 (対 話 型)バックアップが実 行 可 能 です。また、あらかじめスケジュール設 定 されたバックアップを無 人 状 態 で実 行 することもできます。

Data Protectorセル(物 理 的 な構 成 図 と論 理 的 な構 成 図)



> **注 :**
> Data Protector Cell ManagerとData Protectorグラフィカルユーザーインターフェイスシステムは、同じオペレーティングシステム上 で実 行 する必 要 はありません。個 々 のData Protectorコンポーネントでサポートされるオペレーティングシステムのリストについては、『*HPE Data Protector製 品 案 内 、ソフトウェアノート、およびリファレンス*』を参 照 してください。

Cell Manager

Cell Managerは、セルのメインシステムです。Cell Managerは以 下 の働 きをします。

- セル全 体 を一 元 管 理 できます。
- IDBを保 持 します。

  IDBには、バックアップに要 した時 間 、メディアID、セッションIDなど、バックアップに関 する詳 細 情 報 が保 存 されます。

- Data Protectorのコアソフトウェアを実行します。
- セッションマネージャーを実行します。このセッションマネージャーは、バックアップセッションや復元セッションの開始および停止を行うほか、セッションに関する情報をIDBに書き込む働きをします。

バックアップ対象のシステム

バックアップ対象のクライアントシステムには、Data Protector Disk Agent (DA)をインストールしておく必要があります(DAは、**バックアップエージェント**とも呼ばれます)。また、オンラインデータベース統合をバックアップするには、**Application Agent**をインストールしてください。以降の説明では、両方のエージェントを指して、Disk Agentと呼んでいます。Disk Agentは、システム上のディスクからデータを読み取ってMedia Agentに渡したり、Media Agentから受け取ったデータをディスクに書き込んだりする働きをします。

Cell Managerのインストールそのものにより IDBおよび関連構成データのバックアップと復元の手段が提供されますが、Cell Manager上にあるData Protector以外のデータをバックアップして復元できるようにするには、Cell Manager上にDisk Agentもインストールする必要があります。

バックアップデバイスが接続されているシステム

バックアップデバイスが接続されているクライアントシステムには、Data Protector **Media Agent**(MA)をインストールしておく必要があります。このようなクライアントシステムは、**ドライブサーバー**とも呼ばれます。バックアップデバイスは、Cell Managerだけでなく、どのシステムにでも接続できます。Media Agentは、デバイス内のメディアからデータを読み取ってDisk Agentに渡したり、Disk Agentから受け取ったデータをメディアに書き込んだりする働きをします。

ユーザーインターフェイスをインストールしたシステム

Data Protectorは、Data Protectorグラフィカルユーザーインターフェイス(GUI)をインストールしたシステムであれば、ネットワーク上のどのシステムからでも管理できます。そのため、たとえばCell Managerシステムはコンピュータールームに設置しておき、Data Protectorの管理はユーザーのデスクトップから実行することも可能です。

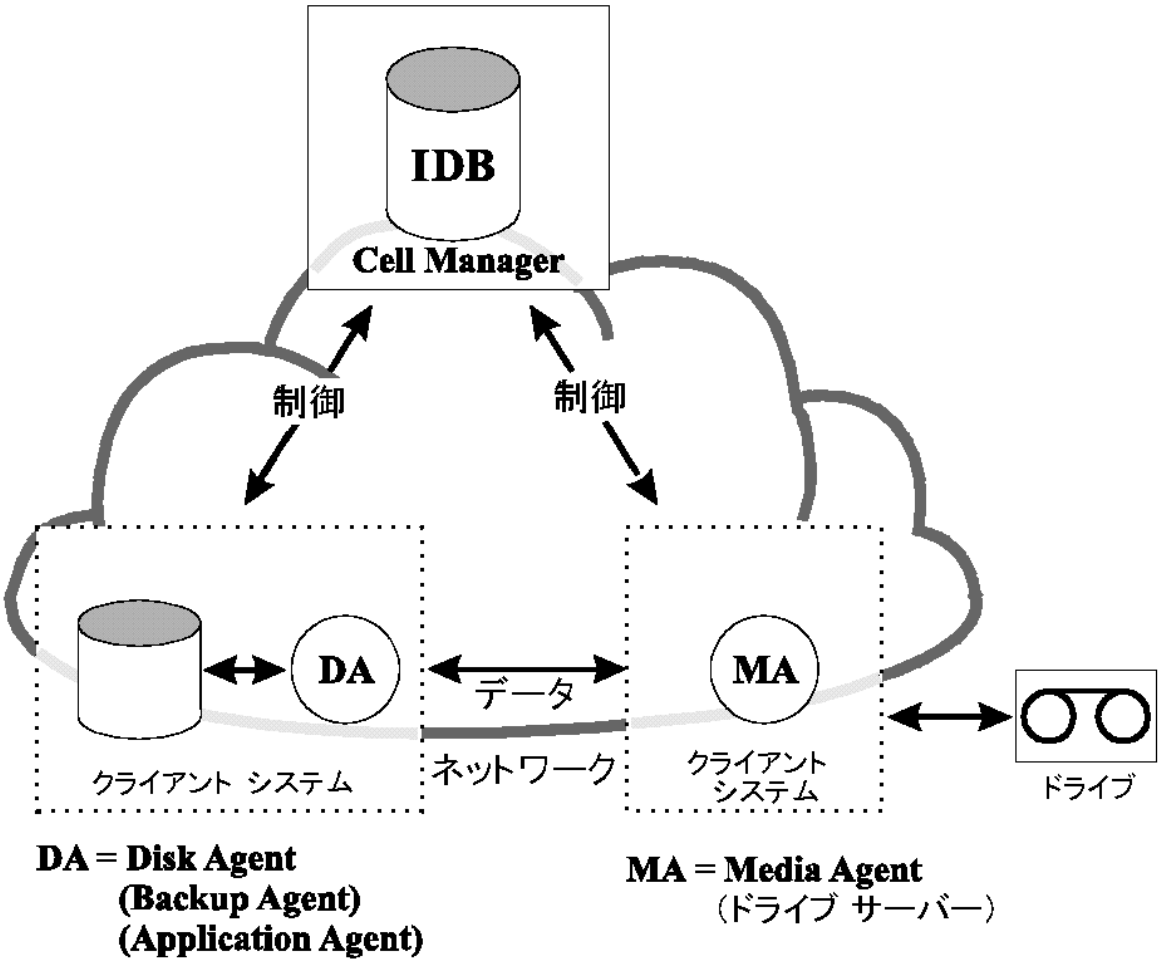
インストールサーバー

インストールサーバーでは、特定アーキテクチャー用のData Protectorインストールパッケージのレポジトリが保持されています。デフォルトでは、Cell Managerが同時にインストールサーバーになります。混在環境では、少なくとも2台のインストールサーバーが必要です。1台はUNIXシステム用で、1台はWindowsシステム用です。

セル内の処理

バックアップ処理および復元処理、次のページに示すとおり、バックアップセッションおよび復元セッションは、Data Protector Cell Managerにより制御され、これらのセッション内でバックアップおよび復元に必要なすべての処理が実行されます。

バックアップ処 理 および復 元 処 理



バックアップセッション

バックアップセッションとは

バックアップセッション、次 のページに示 すバックアップセッションとは、記 憶 メディア上 にデータのコピーを作 成 するプロセスを指 します。バックアップセッションは、オペレーターがData Protectorユーザーインターフェイスを使 って対 話 式 に開 始 することも、Data Protectorスケジューラーにより自 動 的 に開 始 させることも可 能 です。

セッションの動 作

バックアップの実 行 時 には、バックアップセッションマネージャープロセスが、Media AgentとDisk Agentをそれぞれ1つまたは複 数 開 始 して、セッションを制 御 し、生 成 されたメッセージをIDBに書 き込 みます。データはDisk Agentによって読 み取 られた後 、Media Agentに渡 されてメディア内 に保 存 されます。

バックアップセッション

通常のバックアップセッションは、バックアップセッション、上よりも複雑になります。通常は複数のDisk Agentによって複数のディスクから並列にデータが読み取られ、1つまたは複数のMedia Agentにそのデータが渡されます。複雑なバックアップセッションの詳細については、Data Protectorが機能する仕組み、ページ 182を参照してください。

復元セッション

復元セッションとは

復元セッション、下に示すように、復元セッションとは、以前に作成しておいたバックアップデータをディスク上に復元するプロセスを指します。復元セッションは、オペレーターがData Protectorユーザーインターフェイスを使って対話式に開始します。

セッションの動作

以前に作成したバックアップから復元するファイルを選択した後、実際の復元処理を起動します。復元時には、復元セッションマネージャープロセスが、必要なMedia AgentとDisk Agent (それぞれ1つまたは複数)を開始して、セッションを制御し、進捗状況を示すメッセージをIDBに書き込みます。データはMedia Agentによって読み取られた後、Disk Agentに渡されてディスクに書き込まれます。

復元セッション

通常の復元セッションは、復元セッション、上よりも複雑になります。復元セッションの詳細については、Data Protectorが機能する仕組み、ページ 182を参照してください。

企業環境

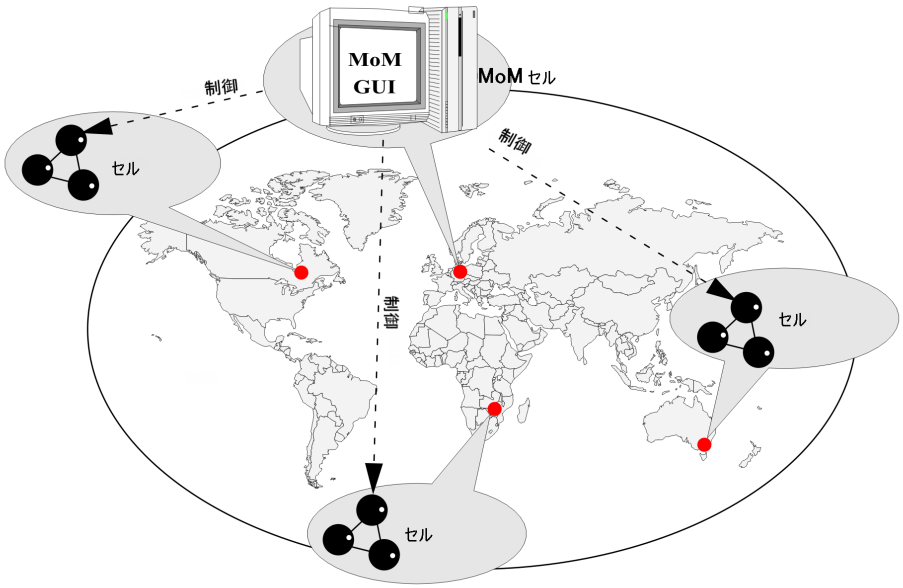
世界規模のData Protector企業環境、次のページに示すように、一般に企業のネットワーク環境は、さまざまなベンダー製品を含む多数のシステムで構成されており、各種オペレーティングシステムが使用され

ています。また、これらのシステムが、時間帯の異なるさまざまな地域に配置されていることもあります。これらのシステムは、さまざまな通信速度のLANまたはWANネットワークによって相互に接続されています。

導入が必要となる場合

このガイドで説明するソリューションは、地理的に離れている複数のサイトに共通の**バックアップポリシー**を適用する必要がある場合に使用できます。また、同一サイトのすべての部門でバックアップデバイスのセットを共有する場合にも使用できます。

世界規模のData Protector企業環境



このような異機種環境のバックアップを構成し管理することは、通常、大変複雑な作業になりますが、Data Protector機能を使用すると容易に実行できます。Manager of Managers (MoM)の詳細については、MoM、次のページを参照してください。

環境内を複数セルに分割する

大規模な環境は、以下のような理由により、複数のセルに分割した方がよいことがあります。

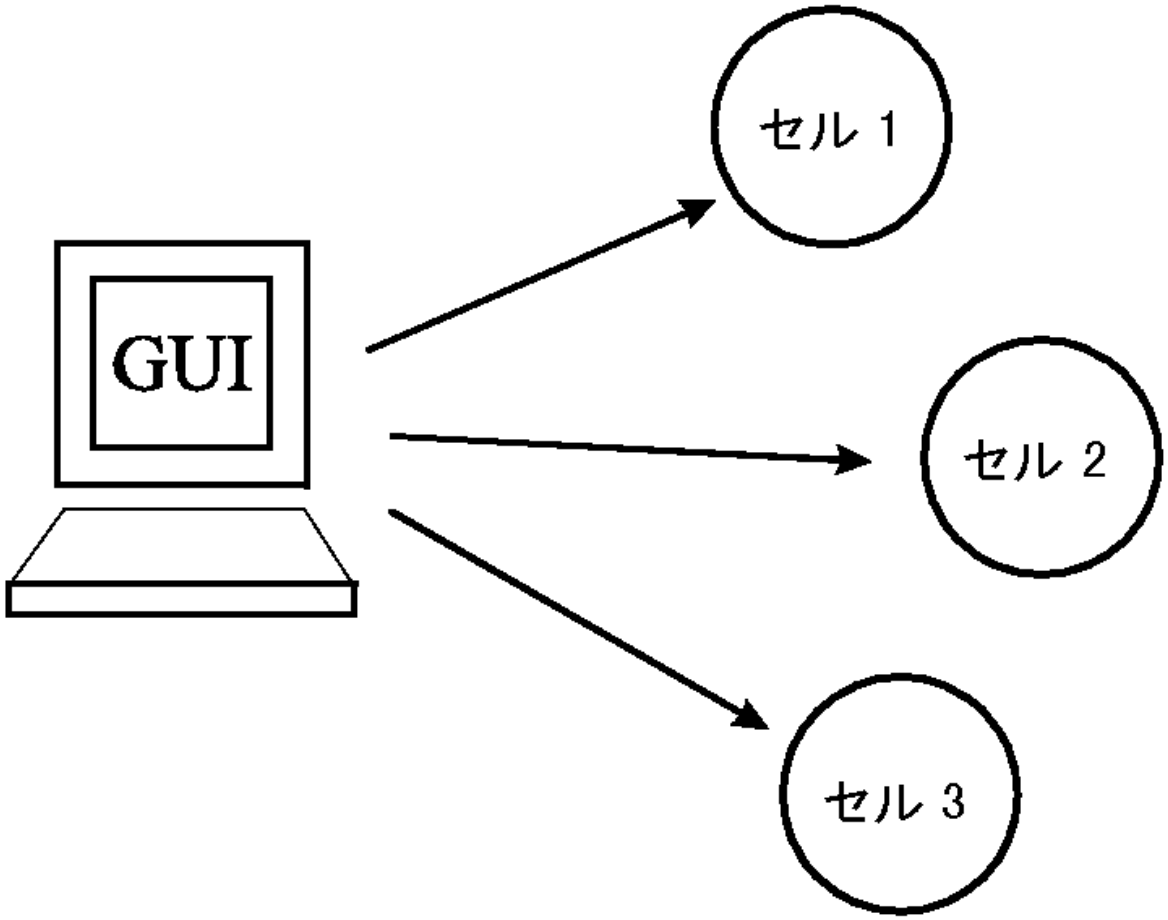
分割が必要となる場合

- 地理的な場所に基づくシステムのグループ化
- 論理的な区分に基づくシステムのグループ化 (部門別など)
- 特定のシステム間の低速なネットワーク接続
- パフォーマンスの考慮
- 管理業務の分割

環境計画時の留意事項の一覧は、バックアップ戦略の計画、ページ 34を参照してください。

Data Protectorでは、複数のセルを一元管理できます。

複数セルを一元管理

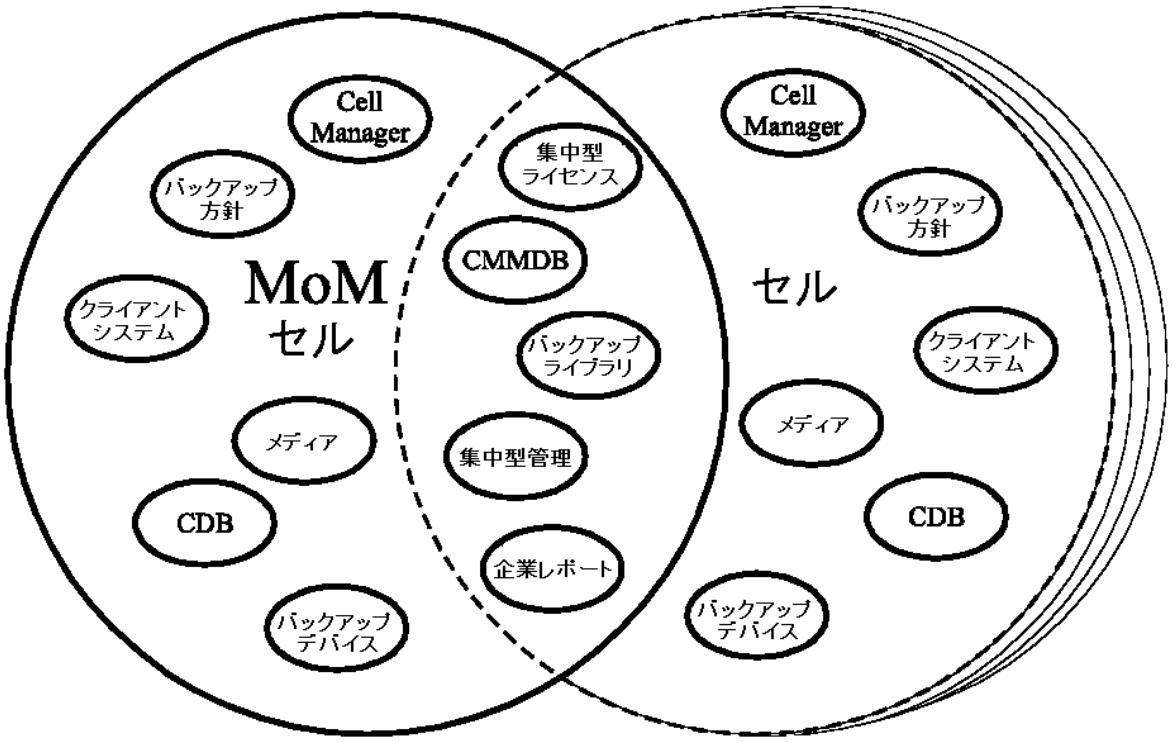


MoM

Data Protectorには、複数セルに分かれた大規模環境を管理するために、Manager-of-Managers (MoM)と呼ばれる機能が用意されています。このMoM機能を使用すると、複数のセルをMoM環境と呼ばれる1つの大きな単位にまとめて、一元管理することができます(複数セルを一元管理 、上参照)。MoMは、バックアップ環境が拡張されても、これに自在に対応できます。また新しいセルの追加や、既存セルの分割も自由です。

MoM環境では、個々のData Protectorセルと中央のMoMセルとを、信頼性が高いネットワークで接続する必要はありません。これは、長距離接続を介して送信されるのは制御情報だけであり、バックアップ作業そのものはそれぞれのData Protectorセル内でローカルに行われるためです。ただしこれは各セルが、それぞれ個別のメディア管理データベースを所有していることが前提になります。

Manager-of-Managers環境



Manager-of-Managersは、以下の機能を提供します。

- **集中型のライセンスレポジトリ**

  ライセンス管理を容易にするための機能です。これは任意選択の機能であり、非常に大規模な環境の場合には有用です。

- **メディア集中管理データベース(CMMDB)**

  CMMDBにより、デバイスやメディアをMoM環境内の複数のセルで共有できます。つまり、CMMDBを使っているあるセル内のデバイスに、同じCMMDBを使っている別のセルからアクセスできます。CMMDBはManager-of-Managers上に置く必要があります。またMoMセルとその他のData Protectorセルとの間に、信頼性の高いネットワーク接続が必要になります。CMMDBは、メディア管理データベースを一元管理するためのオプションの機能です。

- **ライブラリの共有**

  CMMDBを使用すると、マルチセル環境内の複数のセル間で、ハイエンドデバイスを共有できます。そのため、たとえばあるセルから、別のセル内のシステムに接続された複数デバイスを制御できるロボティクスを使用することも可能です。Disk AgentからMedia Agentへのデータパスも、セルの境界に制約されません。

- **エンタープライズレポート**

  Data ProtectorのManager-of-Managersを使用すると、セル単位のレポートだけでなく、全社レベルのレポートも生成できます。

メディア管 理

Data Protectorには強 力なメディア管 理機 能 が備 わっており、次 に示 すような方 法 で、それぞれの環 境 内 にある多 数 のメディアを簡 単 に効 率 よく管 理 できます。

メディア管 理 機 能

- 個 々 のメディアは、**メディアプール**と呼 ばれる論 理 グループにまとめることができます。そのため各 メディアを個 別 に取 り扱 うのではなく、大 容 量 のメディアセットとしてまとめて管 理 できます。
- Data Protectorでは、個 々 のメディアと、そのメディアの状 態 がすべてトラッキングされています(データ保 護 の有 効 期 限 、バックアップ時 にそのメディアを使 用 できるかどうか、各 メディアにバックアップされている情 報 に関 するカタログ情 報 など)。
- 完 全 な自 動 処 理 が可 能 です。Data Protectorでは、ライブラリデバイス内 に十 分 なメディアを用 意 しておくと、メディア管 理 機 能 により、オペレーターによる介 入 操 作 を必 要 とせずにバックアップセッションを自 動 実 行 できます。
- メディアの自 動 交 換 ポリシーを設 定 しておくと、バックアップ用 のメディア交 換 を手 動 で行 う必 要 がなくなります。
- バーコードを使 用 する大 容 量 のライブラリデバイスおよびサイロデバイスで使 われるバーコードの認 識 およびサポートが可 能 です。
- 大 容 量 ライブラリデバイスおよびサイロデバイス内 に存 在 する、Data Protectorが使 用 する全 メディアに対 する認 識 、トラッキング、ブラウズ、および操 作 が可 能 です。
- メディアに関 する情 報 を中 央 で一 元 管 理 し、複 数 のData Protectorセル間 でこの情 報 を共 有 できます。
- メディア上 のデータの追 加 コピーを対 話 式 または自 動 的 に作 成 できます。
- メディアボールティング(安 全 な場 所 でのメディアの保 管 機 能)がサポートされています。

メディアプールとは

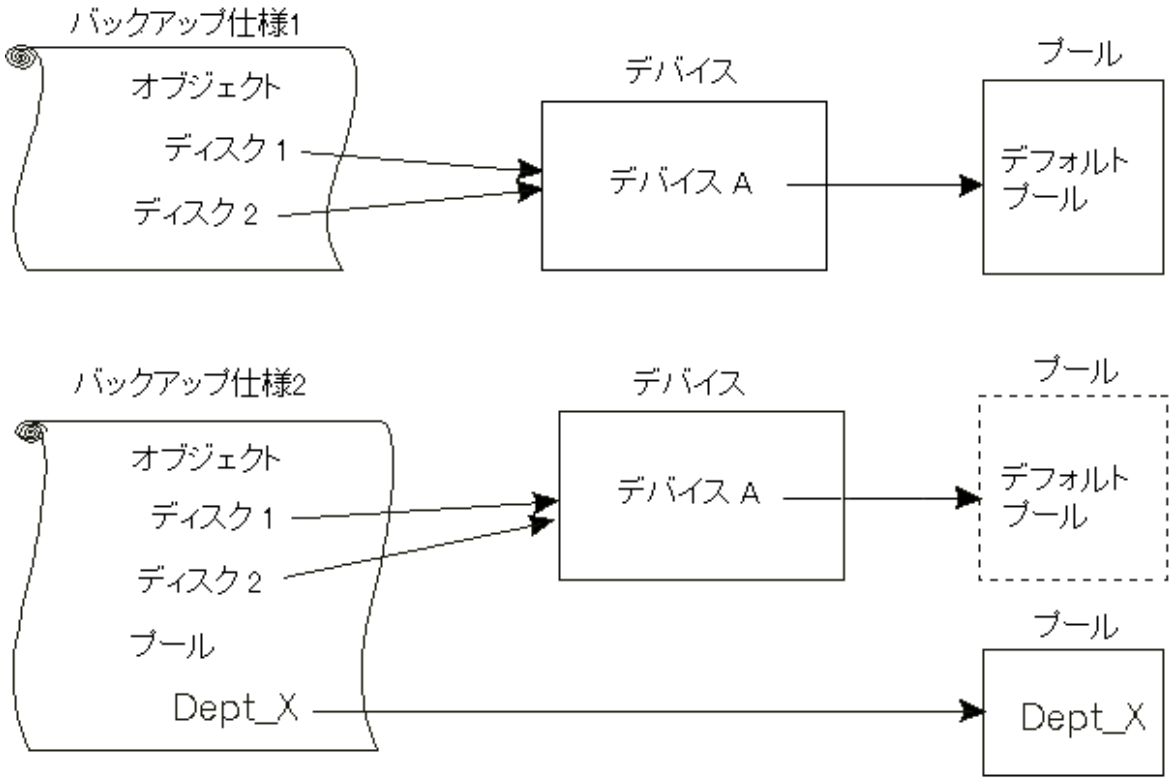
Data Protectorでは、多 数 のメディアを管 理 するためにメディアプールを使 用 します。メディアプールとは、使 用 ポリシー(プロパティ)が共 通 であり、かつ物 理 タイプが**同じ**であるメディアの論 理 的 な集 まりのことです。メディアの使 用 方 針 は、メディア上 に保 存 されているデータに応 じて決 定 します。メディアプールの構 造 やサイズに加 え、プール内 に保 存 するデータのタイプは、ユーザーが自 由 に設 定 できます。

デバイス構 成 時 には、デフォルトのメディアプールが指 定 されます。バックアップ仕 様 の中 でメディアプールを指 定 しなければ、このデフォルトのメディアプールが使 用 されます。

バックアップデバイス

Data Protectorでは各 デバイスを、デフォルトプールなどの使 用 プロパティが個 々 に定 義 された物 理 デバイスとして、定 義 およびモデリングします。このようなデバイス概 念 の使 用 や、バックアップ仕 様 などにより、Data Protectorではデバイスとその使 用 方 針 を容 易 にかつ柔 軟 に構 成 することができます。バックアップデバイスの定 義 は、Data Protectorメディア管 理 データベース内 に保 存 されています。

バックアップ仕 様 、デバイス、およびメディアプールの関 連



バックアップ仕 様 、デバイス、およびメディアプールの関 連 、上 は、バックアップ仕 様 、デバイス、およびメディアプールの関 連 を示したものです。各 デバイスは、バックアップ仕 様 の中 で指 定 されています。各 デバイスはメディアプールにリンクされており、バックアップ仕 様 でこのメディアプールを変 更 することも可 能 です。たとえば上 図 のバックアップ仕 様 2は、デフォルトプールではなくDept_X プールを参 照 しています。

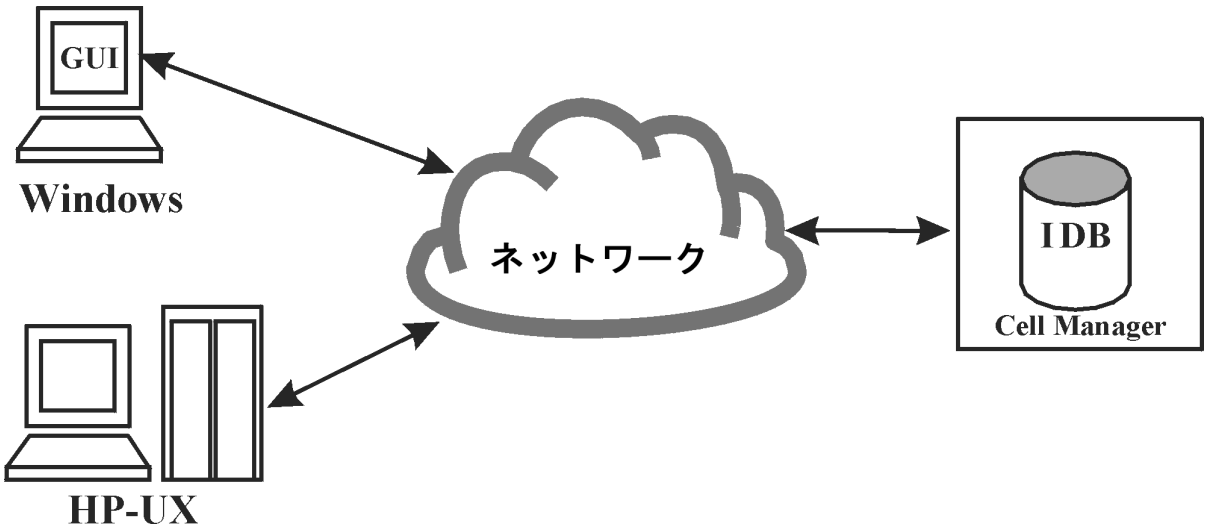
Data Protectorは、多 種 多 様 なデバイスをサポートしています。詳 細 については、『*HPE Data Protector 製 品 案 内 、ソフトウェアノート、およびリファレンス*』を参 照 してください。

ユーザーインターフェース

Data Protectorでは、Windowsプラットフォーム上 でData Protector GUIを使 用 して、すべての構 成 作 業 および管 理 作 業 を簡 単 に利 用 できます。また、コマンドラインインターフェイス(CLI)はUNIXとWindowsのいずれのプラットフォームでも使 用 できます。

Data Protectorのアーキテクチャー上 、Data Protectorユーザーインターフェイスは非 常 に柔 軟 な形 でインストールして使 用 することができます。ユーザーインターフェイスは、Cell Managerシステムから使 用 する必 要 はありません。デスクトップシステム上 にインストールすることができます。Data Protectorユーザーインターフェイスの使 用 、次 のページに示 すように、このユーザーインターフェイスがサポートされているプラットフォームであれば、Cell Managerを使 って、Data Protectorセルを特 に意 識 することなく管 理 できます。

Data Protectorユーザーインターフェイスの使 用



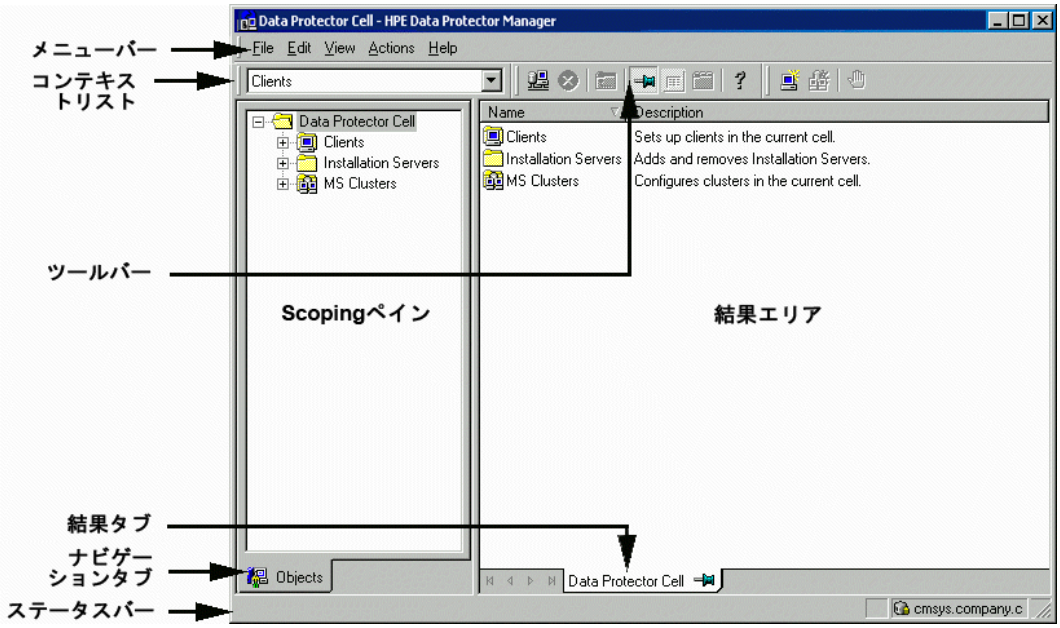
ヒント：
一 般 に、混 合 環 境 では、環 境 内 の複 数 のシステム上 にData Protectorユーザーインターフェイス をインストールしておき、複 数 のシステムからData Protectorにアクセスできるようにしておく方 が便 利 です。

Data Protector GUI

Data Protector GUI、次 のページに示 すData Protector GUIは、以 下 の機 能 を備 えた使 い易 い強 力 な ユーザーインターフェイスです。

- 結 果 タブでは、すべての構 成 ウィザード 、プロパティ、およびリストを使 用 できます。
- Windows環 境 で実 行 されるMicrosoft SQL Server、Microsoft Exchange Server、SAP R/3、Oracle Serverなどや、UNIX環 境 で実 行 されるSAP R/3、Oracle Server、Informix Serverなどのオンライン データベースアプリケーションのバックアップを簡 単 に構 成 して管 理 できます。
- ヘルプトピックや状 況 依 存 ヘルプを含 む包 括 的 なヘルプシステムが用 意 されています。

Data Protector GUI



セットアップ作業の概要

この項では、Data Protectorのバックアップ環境をセットアップするためのさまざまな手順について簡単に説明します。環境の規模と複雑さによっては、以下の手順のすべてが必要とはならないことがあります。

1. ネットワーク構造と編成構造を分析します。どのシステムのバックアップが必要であるかを判断します。
2. Microsoft Exchange、Oracle、IBM DB2 UDB、SAP R/3など、バックアップする必要がある特別なアプリケーションおよびデータベースがあるかどうかを確認します。Data Protectorには、これらの製品に特化した統合機能が備わっています。詳細については、『*HPE Data Protectorインテグレーションガイド*』を参照してください。
3. Data Protectorセルの構成について、以下のような点を決定します。
   - Cell Managerとなるシステム
   - ユーザーインターフェイスのインストール先システム
   - ローカルバックアップまたはネットワークバックアップ
   - バックアップデバイスおよびライブラリを制御するシステム
   - 接続の種類(LANまたはSAN、あるいはその両方)
4. 決定したセットアップ方法に合わせて、必要なData Protectorライセンスを購入します。

   この結果、インストールに必要なパスワードを取得できます。

   別のやり方として、一時パスワードを使用してData Protectorを操作することも可能です。ただし、このパスワードはインストール後60日間のみ有効です。詳細は、『*HPE Data Protectorインストールガイド*』を参照してください。

5. セキュリティ面について考慮します。
   - セキュリティ留意事項を分析します。『*HPE Data Protectorインストールガイド*』を参照してください。
   - どのユーザーグループを構成する必要があるかを考慮します。
   - 暗号化形式のメディアにデータを書き込んでセキュリティを強化します。
6. バックアップの構造について決定します。
   - どのようなメディアプールを定義し、どのように使用するか。
   - どのデバイスをどのように使用するか。
   - 各バックアップデータのコピーはそれぞれいくつ必要か。
   - いくつのバックアップ仕様を作成し、どのようにグループ化するか。
   - ディスクへのバックアップを計画している場合、合成バックアップやディスクステージングなどのアドバンストバックアップ戦略を検討する。
7. Data Protector環境をインストールして構成します。
   - Data Protector Cell Managerシステムをインストールし、Data Protectorのユーザーインターフェイスを使用して、他のシステムにもData Protectorコンポーネントを配布します。
   - 各デバイス(テープドライブ)を、そのデバイスを制御するシステムに接続します。
   - バックアップデバイスを構成します。
   - メディアプールを構成し、メディアを用意します。
   - バックアップ仕様を作成します。IDB用のバックアップ仕様も必要です。
   - 必要に応じてレポートを構成します。
8. 次のような作業について、その方法を確認しておきます。
   - 失敗したバックアップの処理
   - 復元処理の実行
   - バックアップデータのコピーとメディアのボールティング
   - ディザスタリカバリの準備
   - IDBの保守

第2章: バックアップ戦略の計画

この章では、バックアップ戦略の計画方法について説明します。ここでは、Data Protectorセルの設計や、性能、およびセキュリティ上の注意点について取り上げるほか、データのバックアップと復元の方法についても説明します。また、この章では、基本的なバックアップのタイプ、自動バックアップ操作、クラスター化、およびディザスタリカバリについても紹介します。

バックアップ戦略の計画

Data Protectorの構成および管理は容易ですが、多数の異なるクライアントシステムを使用する大規模な環境で、大容量のデータをバックアップするような場合には、事前に適切な設計を行っておくことが大切になります。設計段階を確実に行っておくことで、以降の構成作業が容易になります。

バックアップ戦略の計画とは

バックアップ戦略の計画手順は、以下のとおりです。

1. データのバックアップ頻度や、バックアップデータを別のメディアセットに追加コピーする必要があるかどうかなど、バックアップに関する要件と制約事項を明らかにします。
2. ネットワークやバックアップデバイスにおける定常データ転送速度など、バックアップソリューションに影響を与える要因を明らかにします。これらの要因は、Data Protectorの構成方法や実行するバックアップの種類(ネットワーク経由のバックアップやダイレクトバックアップなど)の選択に影響する可能性があります。たとえばディスクにバックアップすると、合成バックアップやディスクステージングなどのアドバンストバックアップ戦略の利点を活用することができます。
3. バックアップ戦略を構築する準備として、実行するバックアップの構想と、その実装方法を明らかにします。

この項では、準備段階で行うべき作業の詳細について説明します。また、このガイドの以降の部分では、バックアップソリューションの構築に役立つ重要な情報および注意点について説明しています。

バックアップ戦略における要件の定義

バックアップ戦略の目的と制約事項を定義するため、以下の点を検討してください。

- 各自の**組織におけるバックアップと復元のポリシー**

  組織によっては、データの保管および保存に関するポリシーが既に確立されていることがあります。新たに構築するバックアップ戦略は、こうしたポリシーに従ったものでなければなりません。
- バックアップするデータのタイプ

  ネットワーク内に存在するすべてのデータタイプをリストアップします(ユーザーファイル、システムファイル、Webサーバー、大容量リレーショナルデータベースなど)。
- 復旧までに許される最大ダウンタイム

  どれくらいのダウンタイムが許されるかは、バックアップ用のネットワーク基盤および装置に必要な予算に大きく影響します。そのため各データタイプについて、復旧までのダウンタイムが最大どれくらいまで許されるか、つまりバックアップデータから復元するまでの間、どれくらいの時間そのデータを使用できなくても構わないかを明らかにしておきます。たとえば、ユーザーファイルは2日以内に復元できればよいが、大容量データベース内のビジネスデータは2時間以内に復旧しなければならない、といった状況が考えられます。

復旧までの時間は、主として、メディアにアクセスするための時間と、ディスク上に実際にデータを復元するための時間に分かれます。完全なシステム復旧を行う場合は、より多くの手順が必要となるため、さらに多くの時間がかかります。詳細については、ディザスタリカバリ、ページ 102を参照してください。

- 各タイプのデータの保管期間

  各タイプのデータについて、そのデータをどれくらいの期間保管する必要があるかを検討しておきます。たとえば、ユーザーファイルは3週間だけ保管すればよいが、従業員に関する情報は5年間保管するのが妥当である、といったことが考えられます。

- バックアップデータを保存したメディアの保管方法

  安全な外部の保管場所(ボールト)を使用するのであれば、各タイプのデータ毎に、そのデータを保存したメディアをどれくらいの期間、ボールトに保管するべきかを検討しておきます。たとえば、ユーザーファイルをボールトに保存する必要はないが、発注情報は5年間保管しておき、2年後には各メディアを検証しなければならないといったことが考えられます。

- バックアップ時にデータを書き込むメディアセットの総数

  重要なデータは、バックアップ時に複数のメディアセットに書き込むことを検討してください。これによりバックアップのフォールトトレランスが向上し、複数の場所に分けてのボールティングも可能になります。ただし、オブジェクトミラーリングを行うと、バックアップにかかる時間はそれだけ長くなります。

- バックアップするデータの総量

  データタイプごとに、データ総量を見積もっておきます。データ総量は、バックアップに要する時間に大きく影響します。またデータ総量の見積もりは、バックアップに必要なデバイスおよびメディアを選択するうえでも重要です。

- データ総量の将来における増加率

  データタイプごとに、将来におけるデータ増加率を見積もります。データ増加率を見積もっておくと、将来も有効に機能するバックアップソリューションを構築できます。たとえば、100人の従業員を新たに採用する計画がある場合には、ユーザーのデータとクライアントシステムのデータの総量もそれだけ増加するはずです。

- バックアップに要する時間

  それぞれのバックアップ処理に要する時間を見積もります。この値は、データの利用可能時間に直接影響を与えます。たとえば、ユーザーファイルについては、そのユーザーが使用していないときには、いつでもバックアップを実行できますが、トランザクションデータベースについては、バックアップ可能な時間帯が数時間程度しかないことが予想されます。

  またバックアップに要する時間は、実行するバックアップのタイプ、つまりフルバックアップを実行するか、増分バックアップを実行するかによっても異なります。詳細については、フルバックアップ、増分バックアップ、合成バックアップ、ページ 61を参照してください。さらにData Protectorでは、一般に使われている一部のオンラインデータベースアプリケーションに対してバックアップを実行することもできます。詳細については、『*HPE Data Protectorインテグレーションガイド*』を参照してください。

  ディスクにバックアップする場合は、合成バックアップとディスクステージングを活用することができます。これらの高度なバックアップ戦略により、バックアップに要する時間を大幅に短縮できます。詳細については、『合成バックアップ、ページ 66』および『ディスクステージング、ページ 91』を参照してください。

  非常に高速で大容量のディスクを比較的速度の遅いデバイスにバックアップする場合は、複数のDisk Agentを同時に使用して1つのハードディスクをバックアップすることを検討してください。同一のディスクに対して複数のDisk Agentを起動すると、バックアップ速度が著しく向上します。

- バックアップを実行する頻度

データタイプごとに、どれくらいの頻度でバックアップする必要があるかを確認しておきます。たとえば、ユーザーの作業ファイルは1日に1回バックアップし、システムデータは週に1回だけバックアップし、一部のデータベーストランザクションについては1日に2回バックアップするといった方法が考えられます。

バックアップ戦略に影響する各種の要因

バックアップ戦略の実装方法は、さまざまな要因を考慮して決定する必要があります。以下の要因を把握してからバックアップ戦略を策定してください。

- 各企業におけるバックアップおよび保存に対するポリシーと要件
- 各企業におけるセキュリティに対するポリシーと要件
- 物理的なネットワーク構成
- 企業の各サイトで使用できるコンピューター資源および人的資源

バックアップ戦略を構築する準備

バックアップ戦略を構築するには、以下の点を明らかにする必要があります。

- 各社にとってのシステム可用性(およびバックアップ)の重要度
  - 災害に備えてバックアップデータを遠隔地に保存する必要はあるか。
  - ビジネスの継続運用レベルはどの程度か。

    ここでは、すべての重要なクライアントシステムの復旧および復元計画も検討する必要があります。
  - バックアップデータのセキュリティ対策

    構内への不法侵入に対する防御策の必要性を意味します。関連するすべてのデータを不正アクセスから保護するための、物理的なアクセス防止策と電子的なパスワードによる保護策を含みます。
- バックアップするデータの種類

  企業データの種類をリストアップし、バックアップ仕様の中でこれらのデータをどのように組み合わせるかを、バックアップが可能な時間枠も考慮して検討します。企業データは、企業のビジネスデータ、企業のリソースデータ、プロジェクトデータ、個人データなどに分類でき、データの種類別に個別の要件が存在します。
- バックアップポリシーの実装
  - バックアップの実行方法とバックアップオプションの選択

    フルバックアップと増分バックアップの頻度を決定します。また使用するバックアップオプションを選択し、バックアップデータを永続的に保護するかどうかや、バックアップメディアを警備会社に保存するかどうかを決定します。
  - クライアントシステムをグループ化して、バックアップ仕様にまとめる方法

    バックアップ仕様をどのようにグループ化すればよいかを検討します。部門、データの種類、バックアップの頻度などに基づく分類が考えられます。
  - バックアップのスケジュール方法

時間差実行方式の採用を検討してください。これは、ネットワーク負荷、デバイス負荷、バックアップ可能な時間枠などに関する問題を軽減するために、クライアント(バックアップ仕様)ごとに日を変えてフルバックアップを実行するやり方です。

- メディア上のデータとバックアップ関連情報の保持

  以前のバックアップデータが新しいデータで上書きされないように、一定期間保護するかどうかを検討します。この保護策はデータ保護と呼ばれ、セッションベースで実行されます。

  バックアップバージョンに関する情報、バックアップされたファイルやディレクトリの数、データベースに保存されているメッセージなどを、カタログデータベース内に保存しておく期間を決定します。カタログ保護期間内であれば、バックアップデータに簡単にアクセスできます。

- デバイスの構成

  バックアップに使用するデバイスと、それらのデバイスを接続するクライアントシステムを決定します。大量のデータを所有するクライアントシステムにバックアップデバイスを接続すると、多くのデータをネットワークを介さずにローカルにバックアップできるため、バックアップ速度が向上します。

  バックアップするデータ量が多い場合は、以下の点を検討してください。

  - ライブラリデバイスの使用も検討してください。
  - ディスクベースのデバイスへのバックアップを検討してください。ディスクへのバックアップでは、他の利点に加えて、バックアップに必要な時間が短縮され、合成バックアップやディスクステージングなど高度なバックアップ戦略の利点を活用できます。

- メディア管理

  使用するメディアの種類、メディアをメディアプールにグループ化する方法、およびメディア上にオブジェクトを配置する方法を決定します。

  各バックアップポリシーにおけるメディアの使用方法を定義します。

- ボールティング

  メディアを安全な場所(ボールト)に一定期間保管するかどうかを決定します。バックアップの実行中または実行後に保管用の複製を作成するかどうかも検討してください。

- バックアップ管理者とオペレーター

  記憶装置の管理や操作に必要なユーザー権限を決定します。

セルの設計

バックアップ戦略の計画において最も重要な決定事項の1つが、単一セル環境または複数セル環境のどちらを選択するのかという点です。この項では、以下の項目について説明します。

- セルを設計するときに考慮すべき点。
- セルと、一般のネットワーク環境との対応付け。
- セルと、Windowsドメインとの対応付け。
- セルと、Windowsワークグループ環境との対応付け。

単一セルと複数セル

使用する環境において単一セルまたは複数セルのどちらを選択するかは、以下の点を考慮して決定する必要があります。

- バックアップ管理上の問題

  複数セルを使用すると、個々のセル内で、より柔軟な形で管理作業を実行できます。この場合、各セル内では、それぞれ完全に独立した方針でメディアやデバイスを管理できます。たとえば管理対象が複数のグループに分かれているような環境では、データセキュリティ上の理由により、これらのグループを1つのセル内にはまとめたくない可能性があります。一方、複数セルに分割した場合の問題点としては、単一セルの場合に比べて管理作業が煩雑になり、場合によっては各セルに専用の管理者を設ける必要があるといった点が挙げられます。

- セルのサイズ

  Data Protectorセルのサイズは、バックアップ性能およびセルの管理能力に影響を与えます。推奨サイズを超えるセルがあると、そのセルの管理が煩雑になってしまいます。Data Protectorクライアントをセルに編成して管理を効率化する方法については、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。

- ネットワーク上の問題

  最大の性能を得るためには、同一セル内のすべてのクライアントシステムを、同一LAN上に配置する必要があります。ネットワーク構成などのその他のネットワークに関する詳細については、以下の項を参照してください。

- 地理的な配置

  バックアップ対象となるクライアントシステムが地理的に分散している場合、それらのシステムを1つのセル内で管理するのは難しく、また、クライアントシステム間のネットワーク接続に関して問題が発生する可能性があります。さらに、データのセキュリティ面にも注意しなければなりません。

- タイムゾーン

  各セルは、1つのタイムゾーン内にある必要があります。

- データのセキュリティ

  Data Protectorのセキュリティは、セルレベルで提供されます。また、Data Protectorにおける管理業務は、必ず単一セル単位で行われます。たとえば、メディア、バックアップデバイス、バックアップデータなどは、必ず1つのセルに所属します。ただしData Protectorでは、複数のセル間でデバイスを共有したり、別のセルにメディアを移動したりすることも可能なため、個々のメディアに対する物理的なアクセス権は適切なユーザーのみに与えるようにしてください。

- 混合環境

  Data Protectorでは、多数のプラットフォームからなるクライアントシステムを1つのセルにバックアップすることができます。ただし場合によっては、グループクライアントシステムを、プラットフォームごとに個別のセルにまとめた方が便利なこともあります。つまり、1つのセル内にはWindowsクライアントシステムのみを、もう1つのセル内にはUNIXクライアントシステムのみを配置するといった方法です。特に、UNIX環境とWindows環境で、それぞれ個別の管理者とポリシーを設定する場合には、この方法をお勧めします。

- 部門とサイト

  各部門またはサイトに、それぞれ個別のセルを設定することも可能です。たとえば、経理部門、IT部門、製造部門別に、それぞれ専用のセルを設定できます。Data Protectorを使用すると、このように環

境内を複数セルに分割した場合であっても、これらのセル間で共通のポリシーを簡単に構成できます。

クライアントシステムのインストールと保守

環境内に、多数のUNIXクライアントシステムとWindowsクライアントシステムが共存している場合は、Data Protectorを効率よくインストールするための何らかの機構が必要になります。大規模な環境で、各クライアントにローカルな形でインストールを実行することは実際には不可能です。

インストールサーバーとCell Manager

Data Protectorセルの中心となるシステムはCell Managerです。中央のある一点から、各クライアントシステムにData Protectorコンポーネントを簡単に配布(リモートインストール)するには、Data Protectorソフトウェアレポジトリを持ったシステムが必要になります。このシステムをData Protector インストールサーバーと呼びます。デフォルトでは、Cell Managerが同時にインストールサーバーになります。

リモートインストールを実行するたびに、インストールサーバーにアクセスします。インストールサーバーを使用する利点は、特に企業環境において、Data Protectorソフトウェアのリモートインストール、更新、アップグレード、削除などにかかる時間を大幅に短縮できることです。

ソフトウェアのインストールを実際に開始する前に、まずインストールサーバーおよびCell Managerに対するハードウェア要件およびソフトウェア要件を確認しておいてください。また、専用ポート(通常はポート5555/5565)が、セル全体で使用可能でなければなりません。詳細は、『*HPE Data Protectorインストールガイド*』を参照してください。

Cell Managerとインストールサーバーは、ダウンロードされたパッケージ(zip/tar)から直接インストールされます。Cell Managerとインストールサーバーのインストールが終了したら、Data ProtectorのインストールGUIを使用して、さまざまなクライアントシステム上にコンポーネントをインストールできます。

Data Protectorを初めてインストールしたときは、ソフトウェアは60日間有効な一時ライセンスの下で実行されます。このライセンスは、恒久ライセンスを取得するまでの間に、Data Protectorを使用できるようにするためのものです。この間に、必要なライセンスを購入してください。

恒久ライセンスは、この期間内にData Protector環境のセットアップと構成を済ませてから購入するようにしてください。恒久パスワードを取得するには、どのようなシステムをどのData Protectorセルに所属させるかといった点や、各クライアントシステムに接続するデバイスの数、Data Protectorの統合機能を使用するかどうかといった点が明らかになっていなければなりません。

UNIX環境でのセルの作成

UNIX環境では、セルを簡単に作成できます。このガイドで説明する注意点に基づいて、セル内に加えるクライアントシステムと、Cell Managerシステムを決定してください。インストール時には、すべてのクライアントシステムに対してrootアクセス権が必要です。また重要な前提条件として、クリーンな形でノード名を解決したセットアップを行っておき、クライアントシステム同士が、完全修飾されたノード名を使用して互いにアクセスできるようにしておく必要があります。

Windows環境でのセルの作成

Windowsでは2種類の構成方法が存在するため(ドメインまたはワークグループ)、これらのシステムの管理者に対してはさまざまなレベルのサポートが用意されており、この点が、主としてインストール時における

Data Protectorのセットアップ方法に多少の影響を与える可能性があります。

> **重要:**
> また重要な前提条件として、クリーンな形でノード名を解決したセットアップを行っておき、クライアントシステム同士が、完全修飾されたノード名を使用して互いにアクセスできるようにしておく必要があります。

Windowsドメイン

Windowsのドメインは、Data Protectorセルと簡単に対応付けることができます。Windowsのシングルドメインで、ドメインのサイズがData Protectorセルの推奨サイズを超えない場合は、ドメインとセルを1対1で対応付けることをお勧めします。推奨サイズを超える場合には、ドメイン内を複数のセルに分割し、Data Protector Manager-of-Managers機能を使用してこれらのセルを管理するようにしてください。

Data ProtectorセルとWindowsドメインの対応付け

Data ProtectorセルをWindowsドメインに対応付けておくと、Data Protector内部の管理作業も容易になります。管理作業を容易にするには、ドメイン構造内の中心となるWindowsアカウントを使ってすべてのクライアントシステムに対するインストール作業を実行できるような形に、ソフトウェアを配布しておきます。ただしこの他の作業については、Windowsドメイン構造には特に制約されません。これは、すべての操作およびセキュリティ検査が、Windowsのセキュリティではなく、Data Protectorの内部プロトコルによって制御されるためです。

一般的には、Data Protectorをどこにどのような形でインストールするかについて、特に制限はありません。ただし、Windowsの構造や、これらのシステムの最も一般的な構成方法がドメイン環境であることを考えると、操作内容によっては、Data Protectorをシングルドメインモデル、または1つのドメインがマスタードメインとなるマルチドメインモデルに対応付けておく方が、1人のユーザーが環境内の全クライアントシステムを管理できるため、ソフトウェア配布やユーザー構成などの作業効率がよくなります。

Manager-of-Managers機能を使用する複数セル環境内では、構成されている個々のセル内に、バックアップ環境全体にアクセスできる中央の管理者が必要となるため、より注意が必要です。シングルドメイン構成、または1つのマスタードメインを使用するマルチドメイン構成を使用する場合は、1人のグローバルマスタードメインユーザーが、すべてのセルおよびManager-of-Managers環境の管理者となることができます。一方、複数の独立したドメインを使用している場合には、MoM環境の管理者として、複数のユーザーを任命しなければなりません。

Windowsワークグループ

ワークグループを使用する場合は、ドメインの場合のようなグローバルユーザーが存在しないため、一部の構成作業については多少手間がかかるようになります。たとえばソフトウェアを配布するには、そのソフトウェアをインストールするすべてのシステムに、個々にログオンしなければなりません。つまり、ワークグループ環境で100台のシステムにインストールするためには、ログオン作業を100回繰り返す必要があります。このような場合には、ドメイン環境を選択する方が、インストール作業だけでなく、Data Protectorに関連しないその他の管理作業もかなり容易になるはずです。

MoMをワークグループ環境で使用する場合、セルごとに個別の管理者を任命する必要があります。これにより、どのセルからでもMoM環境を管理できるようになります。

Data Protectorは、Windowsのドメイン構造に限定されません。ただし、ユーザー認証が必要な領域(インストール、ユーザー管理)では、管理手順が簡素化されるという利点があります。

混合環境でのセルの作成

混合環境では、UNIX環境でのセルの作成、ページ 39で説明されている要因を考慮に入れます。複数のドメインおよびワークグループに環境が分けられるほど、ソフトウェアを配布し、管理のための環境の準備に必要な留意事項や手順が多くなります。

地理的に離れているセル

Data Protectorを使用すると、地理的に離れた場所にあるセルの管理も容易になります。詳細は、「環境内を複数セルに分割する、ページ 26」を参照してください。

地理的に離れているセルに関する注意点

地理的に離れたセルを構成する場合は、以下の点に注意する必要があります。

- WANを介してデータを送信しないこと

  バックアップ対象クライアントシステムと使用するデバイスは、ローカルな形で構成しなければなりません。
- 各セルを、MoM環境内に構成すること

  地理的に離れたセルを中央で一元管理するには、それらのセルをMoM環境内に構成する必要があります。
- ユーザー構成を考慮すること

  シングルドメイン構成、マルチドメイン構成、およびワークグループ構成の箇所で説明した注意事項についても、考慮しなければなりません。

地理的に離れた場所に対して、単一のセルを構成することができます。この場合、各クライアントシステムから該当するデバイスへのデータ転送が、WANを介して行われないようにする必要があります。WANネットワークはあまり安定した接続ではないため、処理中に接続が中断される可能があります。

MoM環境

MoM環境では、セルと中央のMoMセルとを、信頼性が高いネットワークで接続する必要はありません。これは、長距離接続を介して送信されるのは制御情報だけであり、バックアップ作業そのものはそれぞれのData Protectorセル内でローカルに行われるためです。ただしこれは各セルが、それぞれ個別のメディアデータベースを所有していることが前提になります。

ネットワークの信頼性が低い場合は、Data Protectorのバックアップオプション**[切断された接続の再接続]**を使用して、接続が切れた場合でも自動的に再確立されるようにしておきます。

性能に関する概要と計画上の注意点

基幹業務を行っている環境では、データベースが破壊されていたりディスクに障害が発生した場合のデータ復元に必要な時間を最短に抑えることが、最も重要な要件となります。そのためには、バックアップ性能について理解し、的確なバックアップ計画をたてることが、非常に重要です。さまざまなネットワークに接続されている、プラットフォームが異なるさまざまなクライアントシステムや、大容量データベースのバックアップにかかる時間を最適化するには、かなりの工夫が必要になります。

以下では、バックアップ性能に影響を与える最も一般的な要因について、簡単に紹介していきます。これは、性能については非常にさまざまな要素が考えられるため、すべてのユーザー要件に適した具体的な推奨構成をここで紹介することはできないためです。

インフラストラクチャー

インフラストラクチャーは、バックアップおよび復元の性能に、大きく影響します。特に重要となるのが、データパスの並列化と高速な装置の使用です。

ネットワークバックアップとローカルバックアップ

ネットワーク経由でデータを送信する場合は、新たなオーバーヘッドが生じるため、ネットワーク自体がパフォーマンスに影響を及ぼす要素となります。Data Protectorは、次の場合にデータストリームを別に処理します。

- ネットワークデータストリーム: ディスク→送信元システムのメモリ→ネットワーク→送信先システムのメモリ→デバイス
- ローカルデータストリーム: ディスク→メモリ→デバイス

最大限の性能を得るには、大量のデータストリームを処理できるローカルバックアップ構成を使用してください。

デバイス

デバイスのパフォーマンス

テープに対するデータの読み書きの維持速度はデバイスによって異なります。このため、バックアップと復元のパフォーマンスは、デバイスの種類と機種に依存します。

データ転送速度は、ハードウェア圧縮を使用するかどうかによっても異なります。可能な圧縮率は、バックアップされるデータの性質によって異なります。多くの場合、高速デバイスをハードウェア圧縮オプションをオンにして使用することにより、性能が向上します。ただし、このように性能を向上できるのはデバイスのストリーミングが行われている場合に限ります。

バックアップセッションの開始時と終了時には、バックアップに使用するメディアの巻き戻し、メディアのマウントやアンマウントといった操作のための時間が必要となります。

ライブラリは、多数のメディアに高速かつ自動でアクセスできるので、さらに利点があります。バックアップ時に、新しいメディアまたは再使用可能なメディアをロードし、復元時に、復元対象のデータを含むメディアに迅速にアクセスする必要があります。

ディスクベースのデバイスは、メディアのマウントやアンマウントの必要がないため、従来のデバイスに比べてデータへのアクセスが高速です。このため、バックアップと復元に必要な時間が短縮されます。また、ディスクベースのデバイスでは合成バックアップやディスクステージングなどのアドバンストバックアップ戦略の利点を活用することができ、バックアップと復元の時間がさらに短縮されます。

デバイス以外の高パフォーマンスハードウェア

コンピューターシステムの性能

コンピューターシステム自体の速度は、性能に直接影響を与えます。バックアップ中のシステムでは、ディスクの読み取りやソフトウェアによる圧縮などに伴う負荷が発生します。

ディスクの読取り速度とCPU使用率は、I/O性能やネットワークの種類と同様、システムの重要な性能基準となります。

高度なパフォーマンス構成

Data Protectorゼロダウンタイムバックアップソリューションは、アプリケーションのダウンタイムまたはバックアップモードタイムを短縮する手段を提供するとともに、ネットワークバックアップデバイスの代わりにローカル接続のバックアップデバイスを使用することで、ネットワークのオーバーヘッドを減少させます。アプリケーションダウンタイムまたはバックアップモードタイムは、データの複製を作成するために必要な時間に制限されます。このデータの複製は、その後、バックアップシステム上のローカル接続されたデバイスにバックアップされます。

ハードウェアを並行して使用する

複数のデータパスを並行して使用することは、性能を向上させる上で基本的かつ効率的な方法です。パスにはネットワークインフラストラクチャーが含まれます。この方法は、以下の状況で用いられた場合に、性能向上をもたらします。

並行使用が有効な場合

- 複数のクライアントシステムをローカルに、つまりディスクとそれに関連するデバイスを同一クライアントシステムに接続した状態でバックアップできる場合。
- 複数のクライアントシステムをネットワーク経由でバックアップできる場合。この場合、ネットワーク上のデータ経路を設定して、データパスが重複しないようにすることが必要です。そうでなければ、性能が低下します。
- 複数のオブジェクト(ディスク)を1つまたは複数の(テープ)デバイスにバックアップできる場合。
- クライアントシステム間で複数の専用ネットワークリンクを使用できる場合。たとえば、system_Aにバックアップ対象のオブジェクト(ディスク)が6個あり、system_Bに高速テープデバイスが3台ある場合は、system_Aとsystem_Bとの間で3つのネットワークリンクをバックアップ専用にします。
- 負荷調整

  これはData Protectorの機能であり、どのオブジェクト(ディスク)をどのデバイスにバックアップするかがData Protectorによって動的に決定されます。特に、動的環境において多数のファイルシステムをバックアップする場合は、この機能をオンに設定してください。詳細については、負荷調整の仕組み、ページ107を参照してください。

  ただし、特定のオブジェクトがどのメディアに書き込まれるかは予測できません。

バックアップと復元の構成

最大の性能を引き出すには、あらゆるインフラストラクチャーを効率的に使用する必要があります。Data Protectorは、バックアップや復元を操作するための環境や必要な方法に対応できる高い柔軟性を備えています。

ソフトウェア圧縮

ソフトウェア圧縮は、ディスクからデータが読み込まれる際に、クライアントのCPUによって実行されます。これにより、ネットワーク経由で送信されるデータの量が低減されますが、クライアントでは大量のCPUリソースが必要となります。

デフォルトでは、ソフトウェア圧縮は無効になっています。ソフトウェア圧縮は、処理速度の遅いネットワーク経由で多数のマシンをバックアップする場合にのみ使用してください。これにより、データが圧縮された後ネットワークへ送信されます。ソフトウェア圧縮を使用する場合は、ハードウェア圧縮を無効化してください。両方の方法でデータを圧縮しようとすると、データのサイズが大きくなってしまいます。

ハードウェア圧縮

ハードウェア圧縮はデバイスによって実行されます。デバイスはドライブサーバーから元のデータを受信し、受信したデータを圧縮モードでメディアに書き込みます。ハードウェア圧縮を使うと、テープに書き込まれるデータのサイズが小さくなり、テープドライブがデータを受信する速度が向上します。

デフォルトでは、ハードウェア圧縮は使用可能に設定されています。HP-UXシステムでハードウェア圧縮を有効化するには、ハードウェア圧縮デバイスファイルを選択します。Windowsシステムでは、デバイスの構成中にハードウェア圧縮を有効化します。ハードウェア圧縮を使用するかどうかは、慎重に決定してください。これは、圧縮モードで書き込まれたメディアは、非圧縮モードのデバイスで読み取ることができず、非圧縮モードで書き込まれたメディアは、圧縮モードのデバイスで読み取ることができないためです。

フルバックアップと増分バックアップ

性能を向上させるための基本的な方法は、バックアップされるデータの量を減らすことです。フルバックアップ、および増分バックアップは、慎重に設定してください。注意すべき点は、すべてのクライアントシステムのフルバックアップを同時に実行する必要はないということです。

ディスクにバックアップする場合、合成バックアップやディスクステージングなどのアドバンストバックアップ戦略の利点を活用することができます。

ディスクイメージバックアップとファイルシステムバックアップ

従来は、ファイルシステムをバックアップするよりも、ディスクイメージのバックアップを実行する方が効率的でした。このことは現在でも、負荷の大きいシステムを使用する場合や、ディスクに容量の小さいファイルが多数散在している場合などに当てはまります。ただし、一般的には、ファイルシステムバックアップの使用をお勧めします。

メディアへのオブジェクトの分配

以下に、Data Protectorのバックアップ構成におけるオブジェクトとメディアの対応付けの例を示します。

- 1つのオブジェクト(ディスク)を1つのメディアに格納。

  この方法の利点は、オブジェクトとオブジェクトが格納されるメディアとの関係が固定されている点です。この場合、復元プロセスの実行時には、特定の*1つのメディアだけ*にアクセスすればよいことになります。

  一方、ネットワークバックアップを行う場合にこの方法を使用すると、ネットワークが原因で性能が制限されるため、デバイスストリームを維持できない可能性があります。
- 多数のオブジェクトを複数のメディアに格納。1つのメディアには複数のオブジェクトが保存されますが、1つのオブジェクトは必ず1つのデバイスで処理されます。

  この方法の利点としては、特にネットワーク構成内で使用する場合に、バックアップ時のデータストリームを柔軟に構成できるため、性能を最適化できる点が挙げられます。

  この方法は、それぞれのデバイスがストリームを維持するのに十分なデータを得ることが可能であるということを前提としています。これは、各デバイスは複数ソースのデータを並列に受け取ることができるためです。

  一方、この方法の問題点として、1つのオブジェクトだけを復元する場合に、それ以外のオブジェクトのデータをスキップしなければならない点が挙げられます。さらに、どのメディアにどのオブジェクトのデータが格納されるかを、正確に予測することはできません。

  デバイスストリーミングとバックアップの同時処理数の詳細については、デバイスストリーミングと同時処理数、ページ 107を参照してください。

ディスク性能

Data Protectorでバックアップ対象となるデータはすべて、システム内のディスク上に存在しています。そのため、ディスクの性能は、バックアップ性能に直接影響を及ぼします。ディスクは、本質的にはシーケンシャルなデバイスです。つまり、ディスクに対するデータの読み書きは自由に行えますが、両方を同時に実行することはできません。また、データストリームは一度に1つしか読み書きできません。Data Protectorでは、ファイルシステムをシーケンシャルにバックアップして、ディスクヘッドの動きを低減しています。復元時においても、ファイルシステムは順に復元されていきます。

ただし、オペレーティングシステムは使用頻度の高いデータをいったん**キャッシュメモリ**内に格納することがあるため、上記の問題が、はっきりとした形では表れないこともあります。

ディスクの断片化

ディスク上のデータは、ファイルやディレクトリをブラウズした場合に示される論理的な順番では保存されておらず、実際には物理ディスク全体に小さなブロックの形で分散しています。そのため、ファイルを読み書きする場合、ディスクヘッドはディスク領域全体を移動しなければなりません。ただしこの処理は、各オペレーティングシステムによって異なります。

> **ヒント:**
> バックアップは、あまり断片化されていない大容量ファイルの場合に最も効率よく実行されます。

圧縮

ディスク上のデータが圧縮されている場合、Windowsオペレーティングシステムでは、ネットワークを介してデータを送信する前に、そのデータをまず展開します。そのため、実際のバックアップ速度が低下し、CPUリソースも消費されます。

ディスクイメージバックアップ

Data Protectorでは、UNIXディスクとWindowsディスクのディスクイメージバックアップも可能です。ディスクイメージバックアップの場合は、ファイルシステム構造は無視されて、ディスク全体のイメージがそのままバックアップされます。この場合は、ディスクヘッドはディスク上を直線的に移動していきます。そのため、ディスクのイメージバックアップは、ファイルシステムバックアップに比べて処理時間がかなり短縮されます。

WindowsシステムでのDisk Agentの性能

Windowsのファイルシステムをバックアップする際のDisk Agentの性能は、非同期読み込みを有効にすることで向上させることができます。ディスクアレイ上のデータをバックアップするとき、特に巨大なファイルをバックアップする際に、非同期読み込みを使用するとDisk Agentの性能が向上します。特定の環境において非同期読み込みで性能が向上するかどうかを確認し、最適な非同期読み込みの設定を決めるためには、テストバックアップを行うことを推奨します。

SAN性能

大量のデータを1つのセッションでバックアップする場合は、データ転送にかなりの時間が必要になります。これは、(LAN、ローカル、またはSAN)接続を介してデータをバックアップデバイスに送信するのにかかる時間です。

オンラインデータベースアプリケーションの性能

Oracle、SAP R/3、Sybase、Informix Serverなどのデータベースやアプリケーションをバックアップする場合、バックアップの性能は、対象となるアプリケーションにも依存します。データベースオンラインバックアップとは、データベースアプリケーションをオンライン状態のままバックアップするための機能です。この機能を使用すると、データベースのアップタイムを最大化できますが、アプリケーションの性能に影響が及ぶ可能性もあります。Data Protectorは、一般的なオンラインデータベースアプリケーションすべてを統合して、バックアップ性能を最適化します。

Data Protectorとさまざまなアプリケーションとの統合や、バックアップ性能を向上させるテクニックについては、各『*HPE Data Protectorインテグレーションガイド*』を参照してください。

バックアップ性能を向上させる方法については、これらのオンラインデータベースアプリケーションに同梱されているドキュメント類も参照してください。

セキュリティの設計

バックアップ環境の構築時には、セキュリティ面にも考慮してください。セキュリティ計画を慎重に検討し、実装し、更新することにより、データに対する不法なアクセスや、複製、改変などを防止できます。Data Protector 10.00より前のバージョンでは、暗号制御通信(ECC)を有効にすることでCell Managerとクライアント間の通信を保護することができました。ECCを有効にすると、クライアントはCell Manager上でホストさ

れているCAによって署名されたCRS要求を生成します。この時点で、証明書にあるCAとホスト名が確認されることで、信頼が確立されます。Data Protector 10.00では、Cell Managerとクライアント間のすべての通信はデフォルトで保護されるようになりました。ルートCAの概念ではなく、証明書ピンニングを用いた自己署名証明書が使用されます。

セキュリティとは

バックアップにおけるセキュリティ対策では、通常、以下の点を検討する必要があります。

- バックアップアプリケーション(Data Protector)の管理および操作を実行する権限を誰に与えるか。
- クライアントシステムおよびバックアップメディアに対する物理的なアクセス権を誰に与えるか。
- データを復元する権限を誰に与えるか。
- バックアップデータに関する情報をブラウズする権限を誰に与えるか。

Data Protectorには、これらの問題に対する、セキュリティソリューションが用意されています。

Data Protectorのセキュリティ機能

Data Protectorおよびバックアップデータへのアクセスは、以下の機能に基づいて制御されます。各項目については、以下の項で詳しく説明していきます。

- セル
- Data Protectorユーザーアカウント
- Data Protectorユーザーグループ
- Data Protectorユーザー権限
- バックアップデータのブラウズおよびアクセス権
- データの暗号化

セル

セッションの開始

Data Protectorのセキュリティは、セル単位に制御されます。Data ProtectorのManager-of-Managers機能を使用していない場合には、バックアップセッションおよび復元セッションは、Cell Managerからしか開始できません。そのため、あるセル内のユーザーが、別のローカルセル内のデータをバックアップしたり復元したりすることは、できないようになっています。

特定のCell Managerからのアクセス

さらにData Protectorでは、クライアントシステムにアクセスできるCell Managerを、明示的に構成できます(信頼されるピアの構成など)。

実行前および実行後スクリプトの制限

セキュリティ対策として、実行前/実行後スクリプトに対して、さまざまなレベルの制限を設定できます。これらのスクリプトを任意に使用すると、クライアントシステム側でバックアップ前に何らかの準備作業を行うことが可能になります(たとえば整合性のとれたバックアップを作成するために、アプリケーションを終了させるなど)。

Data Protectorユーザーアカウント

Data Protectorの機能を使用するためには、Data Protector管理作業を行う場合であっても、個人的なデータを復元するだけの場合であっても、必ずData Protectorのユーザーアカウントを取得しておかなければなりません。このユーザーアカウントは、Data Protectorおよびバックアップデータに対する不正アクセスの防止に役立っています。

ユーザーアカウントの設定者

ユーザーアカウントは管理者が作成し、作成時にはユーザーのログイン名、そのユーザーがログインに使用できるシステム、および所属するData Protectorユーザーグループのメンバーシップを指定します。このメンバーシップにより、所属するユーザーの権限が決められます。

アカウントチェックのタイミング

ユーザー権限のチェックは、ユーザーがData Protectorユーザーインターフェイスを起動した時点で、Data Protectorにより実行されます。また、ユーザーが特定のタスクを実行したときにも、ユーザー権限のチェックが行われます。

詳細は、「ユーザーとユーザーグループ、ページ 164」を参照してください。

Data Protectorユーザーグループ

ユーザーグループとは

新しいユーザーアカウントの作成時には、そのユーザーが所属するユーザーグループも指定されます。
個々のユーザーグループに対しては、それぞれ複数のData Protectorユーザー権限が与えられています。グループのメンバーとなったユーザーは、そのグループのユーザー権限が与えられます。

ユーザーグループが必要な理由

Data Protectorのユーザーグループを使用すると、ユーザー構成作業が容易になります。管理者は、個々のユーザーを、各自が使用するData Protector機能に基づいて、いくつかのグループにまとめておきます。これらのグループに対して、たとえば、[end user]グループのメンバーには、個人データをローカルシステム上に復元する権限のみを与え、一方[operators]グループのメンバーには、バックアップの開始およびモニタリングを行う権限を与えるが、バックアップの作成は許可しない、といった設定が可能です。

詳細は、「ユーザーとユーザーグループ、ページ 164」を参照してください。

Data Protectorユーザー権限

ユーザー権限とは

Data Protectorのユーザー権限とは、各ユーザーがData Protectorを使って実行できる処理を定義するものです。ユーザー権限は、個々のユーザー単位にではなく、Data Protectorのユーザーグループ単位で与えられます。あるユーザーグループに追加されたユーザーには、そのユーザーグループに割り当てられているユーザー権限が自動的に与えられます。

ユーザー権限が必要な理由

Data Protectorのユーザーおよびユーザーグループ機能は柔軟性が高く、管理者は特定のData Protector機能を使用できるユーザーを明示的に定義できます。Data Protectorのユーザー権限は慎重に適用するようにしてください。あるデータをバックアップおよび復元することは、本質的にはそのデータのコピーを作成するのと同じことです。

詳細は、「ユーザーとユーザーグループ、ページ 164」を参照してください。

バックアップデータの表示

データのバックアップを作成することは、そのデータの新しいコピーを作成することを意味します。そのため機密情報を取り扱うときには、オリジナルのデータだけでなく、バックアップコピーに対するアクセス権も制限する必要があります。

他のユーザーからデータを隠す

バックアップの構成時には、そのデータを誰でも復元できるようにするか(public)、またはバックアップデータのオーナーしか復元できないようにするか(private)を指定できます。バックアップオーナーの詳細については、バックアップ所有権とは、下を参照してください。

バックアップ所有権とは

誰がバックアップセッションを所有するのか

各[バックアップセッション]およびその内部にバックアップされたすべてのデータには、オーナーが割り当てられます。このオーナーは、対話型のバックアップを開始するユーザー、CRSプロセスを実行しているアカウント、またはバックアップ仕様オプションでオーナーとして指定されるユーザーです。バックアップオーナーの指定方法については、『*HPE Data Protectorヘルプ*』のキーワード「所有権」で表示される内容を参照してください。

バックアップと復元

バックアップ所有権は、データを表示および復元するユーザーの機能に影響を与えます。オブジェクトがパブリックに設定されていない場合、そのメディアセット内に保存されているデータは、メディアセットのオーナーまたは管理者しか見ることができません。プライベートオブジェクトを参照および復元する権限は、*admin*以外のグループにも与えることができます。プライベートオブジェクトの参照および復元が可能なユーザーおよび適用方法については、『*HPE Data Protectorヘルプ*』のキーワード「所有権」で表示される内容を参照してください。

データの暗号化

オープンシステムとパブリックネットワークの普及により、大企業ではデータの安全性が必須になりました。Data Protectorでは、バックアップデータを暗号化して、他から保護されるようにしています。Data Protectorには、ソフトウェアベースとドライブベースの2つのデータ暗号化機能があります。

Data Protectorソフトウェアの暗号化機能は**AES 256ビット暗号化**といい、256ビットの長さのランダムなキーを使用するAES-CTR (Advanced Encryption Standard in Counter Mode)の暗号化アルゴリズムを基

が暗号化と復号化の両方に使用されます。AES 256ビット暗号化では、データの暗号化は、データをネットワーク上で転送する前、およびメディアに書き込む前に行われます。

Data Protectorの**ドライブベースの暗号化**では、ドライブの暗号化機能が使用されます。実際の実装と暗号化の強度は、ドライブのファームウェアによって異なります。Data Protectorは、その機能を有効にして、暗号化キーを管理するだけです。

キー管理機能は、**Key Management Server (KMS)** から提供されます。これはCell Manager上にあります。暗号化キーはすべてCell Managerのキーストアファイルに一元的に保存され、KMSによって管理されます。

バックアップ仕様で、すべてまたは選択したオブジェクトを暗号化したり、同じメディア上で暗号化するセッションと暗号化しないセッションを組み合わせたりすることができます。

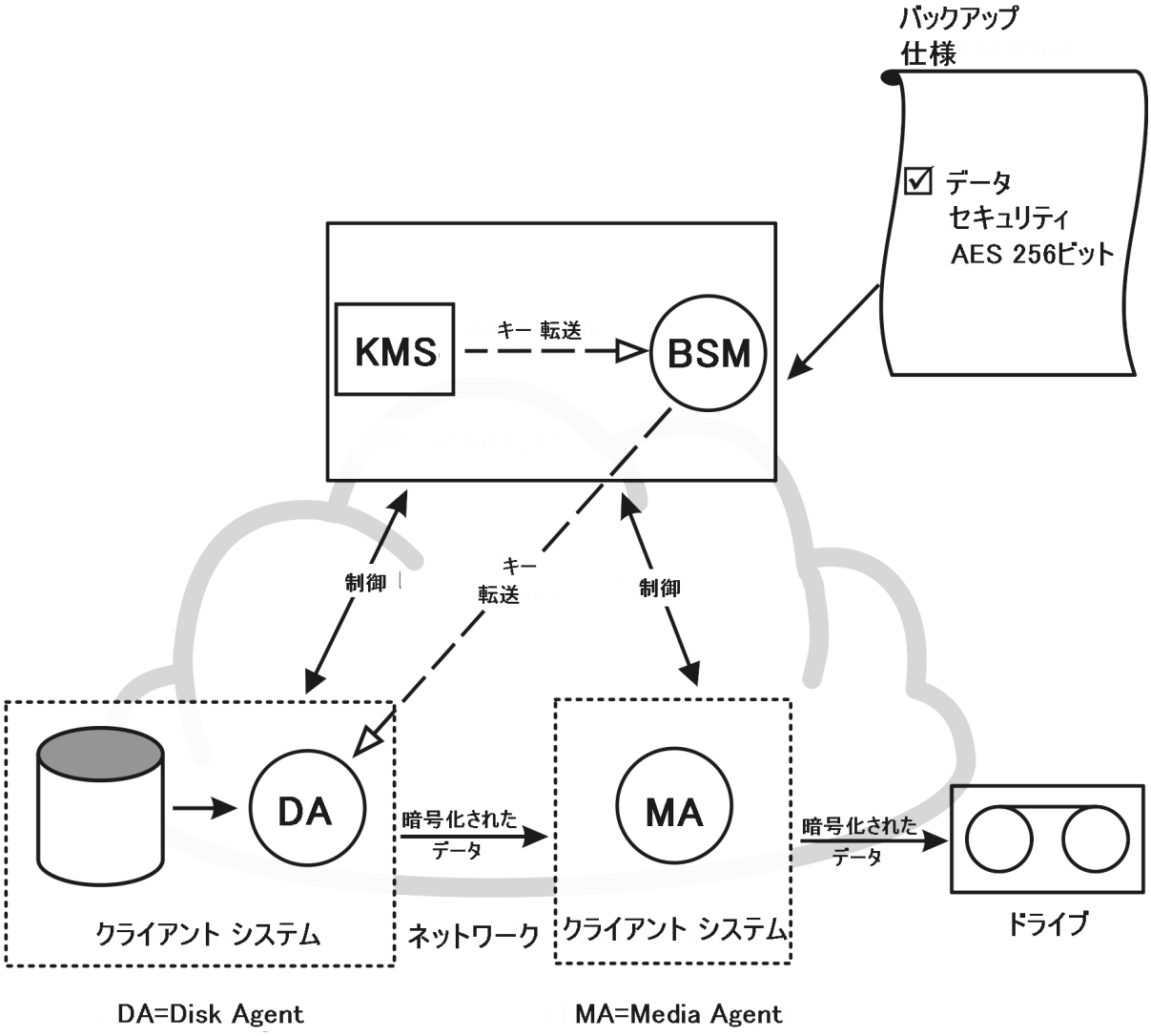
また、Data Protectorでは暗号化機能のほかに、この目的で使用できる組み込み型のアルゴリズム(キーなし)を使用する暗号化機能も備えています。

Data ProtectorでAES 256ビット暗号化機能が動作する仕組み

バックアップセッションマネージャー(BSM)で**[AES 256ビット]**暗号化オプションが選択されているバックアップ仕様を読み込み、Key Management Server (KMS)にアクティブな暗号化キーを要求します。キーがDisk Agent (DA)に転送され、ここでデータが暗号化されます。したがってデータは、ネットワークを介して転送される前およびメディアに書き込まれる前に暗号化されます。

AES 256ビット暗号化を指定したバックアップセッション、次のページでは、**[AES 256ビット]**暗号化オプションが選択されていて暗号化が行われるバックアップセッションの際の、基本的なやり取りを表しています。

AES 256ビット暗号化を指定したバックアップセッション



Data Protectorでドライブベースの暗号化機能が動作する仕組み

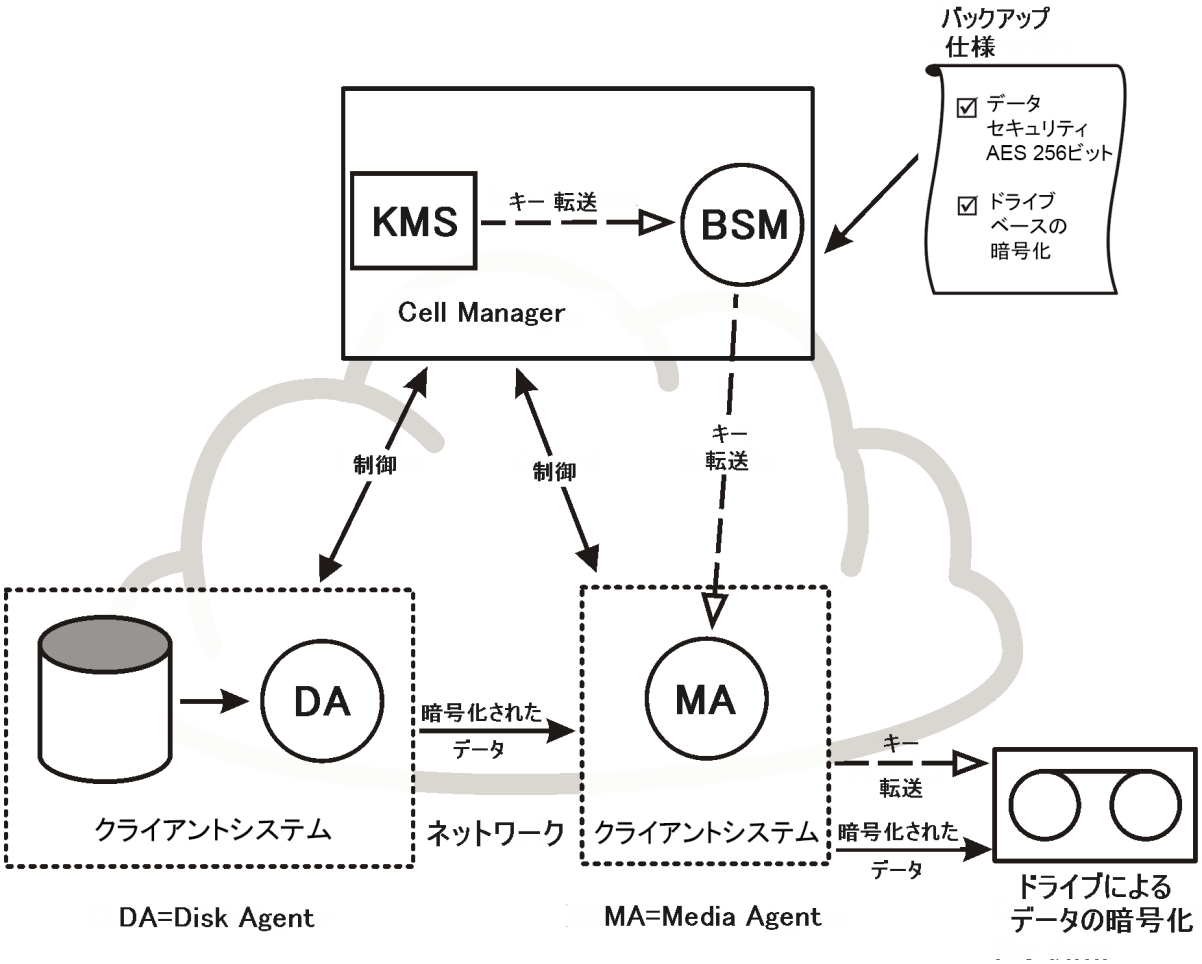
BSMで**[Drive based encryption]**オプションが選択されているバックアップ仕様を読み込み、KMSにアクティブな暗号化キーを要求します。キーがMedia Agent (MA)に転送されます。ここで暗号化のためにドライブが構成され、ドライブに暗号化キーが設定されます。ドライブによってメディアに書き込まれるデータとメタデータの両方が暗号化されます。

暗号化されているバックアップからオブジェクトのコピーや集約の操作をするときには、元のドライブでデータが復号化され、ネットワーク上を転送されて、あて先のドライブで暗号化されます。

メディアの自動コピーセッションの対象となるソースメディアに、暗号化されたデータと暗号化されていないデータの両方が保存されている場合は、対応するターゲットメディアに書き込まれるデータはすべて暗号化されるか、またはすべて暗号化されません(ドライブベースの暗号化の現在の設定による)。

AES 256ビット暗号化とドライブベース暗号化が指定されたバックアップセッション、下は、**[AES 256ビット]**暗号化オプションと**[ドライブベースの暗号化]**オプションを選択した場合の暗号化されたバックアップセッション時における基本的なやり取りを示します。

AES 256ビット暗号化とドライブベース暗号化が指定されたバックアップセッション



暗号化されたバックアップからの復元

Data Protectorでは自動的に復号化キーが取得されるため、暗号化されたバックアップを復元する際に、暗号化に関連する準備は必要ありません。

Data Protectorでのデータ暗号化およびデフォルトのセキュアチャネル通信

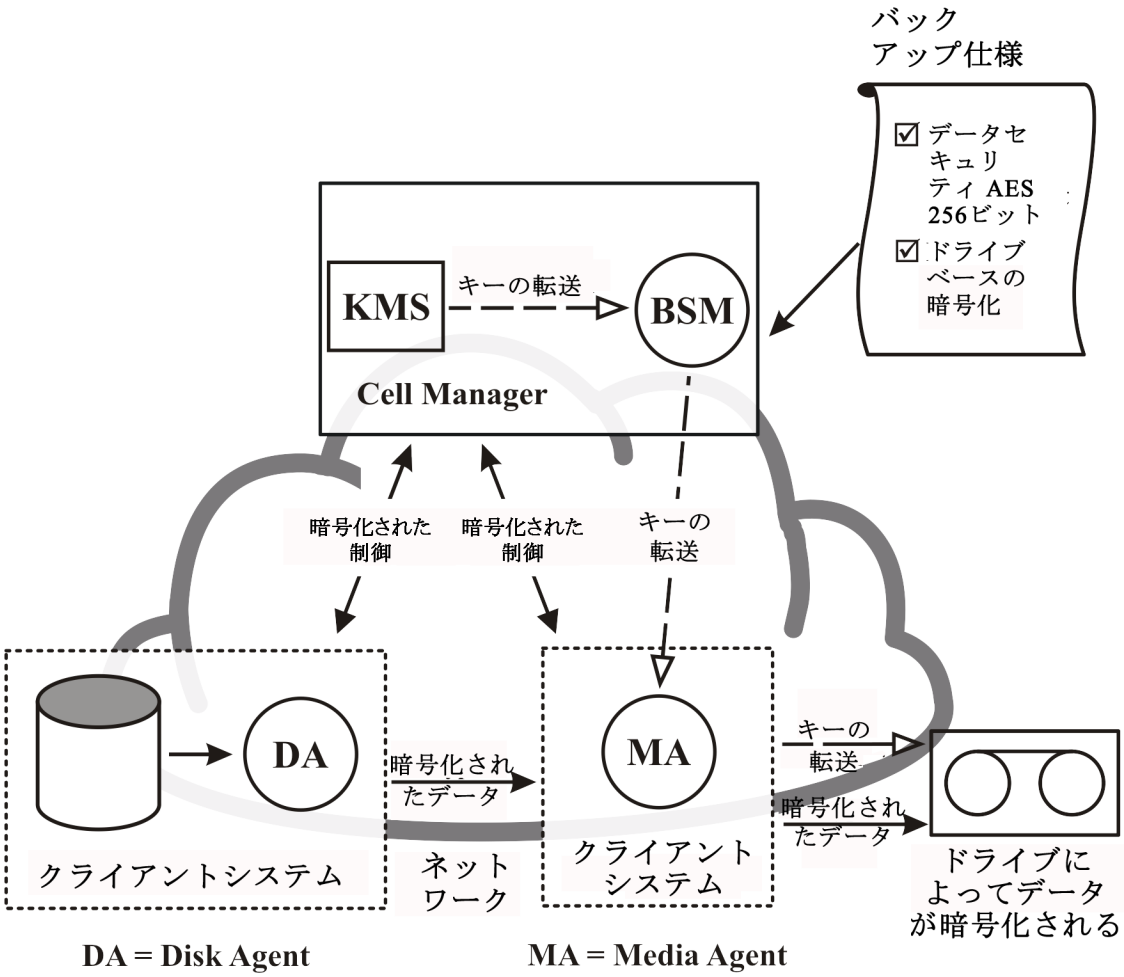
データ暗号化とデフォルトのセキュアチャネル通信を組み合わせることで、システムのセキュリティレベルを容易に最大化することができます。

- データをネットワーク上で転送してメディアに書き込む前に、ソフトウェア(AES 256ビット)暗号化によってデータを暗号化します。

- バックアップのハードウェア(ドライブベース)暗号化によって、メディアへの保存/移動時のデータへの不正アクセスを防ぎます。
- デフォルトのセキュアチャネル通信によって、セル内のクライアント間にセキュアな通信が提供されます。

デフォルトのセキュアチャネル通信およびデータ暗号化、下に、**[AES 256ビット]**暗号化オプションと**[ドライブベースの暗号化]**オプションが選択され、デフォルトのセキュアチャネル通信が有効な場合の、暗号化されたバックアップセッション時におけるData Protectorセル内での基本的なやり取りを示します。

デフォルトのセキュアチャネル通信およびデータ暗号化



クラスタリング

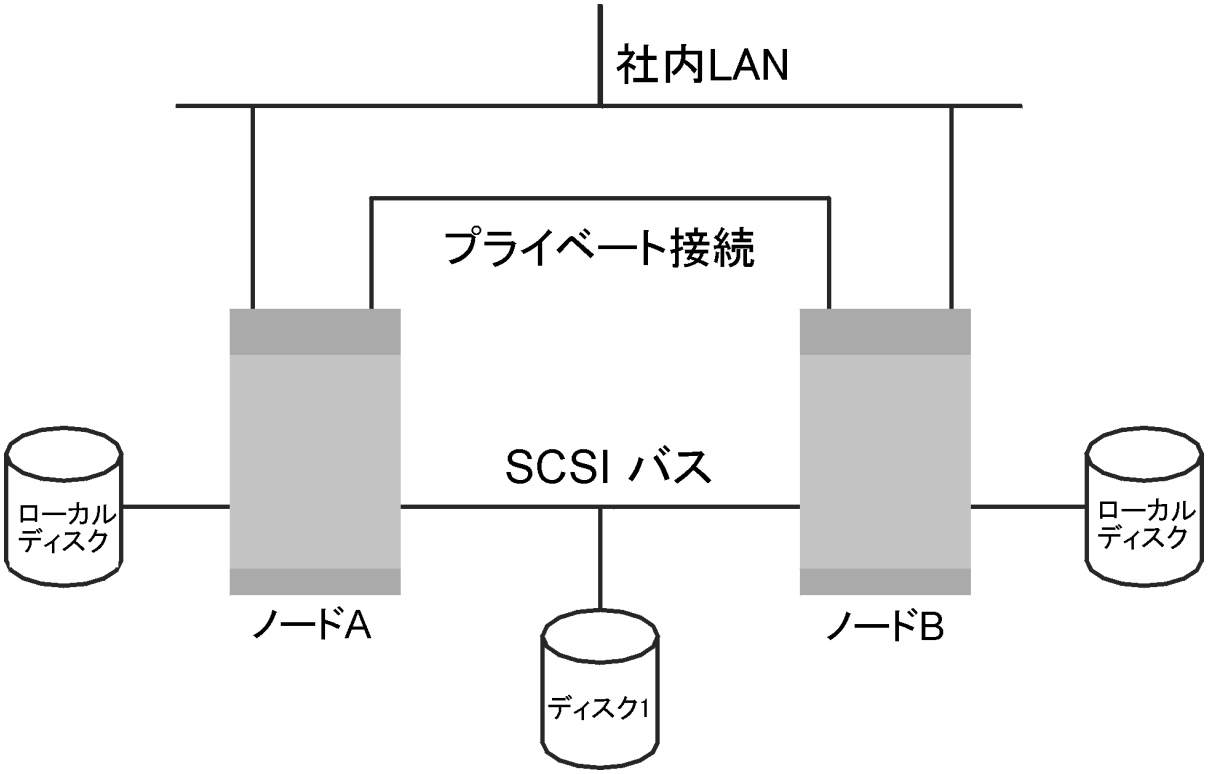
クラスターの概念

クラスターとは、ネットワーク上では単一のシステムとして認識される、複数のコンピューターから構成されるグループを指します。クラスターを形成する複数のコンピューターは単一のシステムとして管理され、以下のことを実現します。

- ミッションクリティカルなアプリケーションやリソースに、最大限の高可用性を持たせることができます。
- コンポーネントの耐障害性が高まります。
- コンポーネントの追加や削除が容易になります。

Data Protectorではクラスタリングを実現するために、Windows Server用のMicrosoft Cluster ServerおよびHP-UX用のMC/Service Guardと統合します。サポートされているクラスターのリストについては、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。

代表的なクラスター



構成要素

- クラスターノード(複数)
- ローカルディスク
- 共有ディスク(ノード間で共有)

クラスターノード

クラスターノードとは、1つのクラスターを構成する複数のコンピューターを指します。クラスターノードは、1つまたは複数の共有ディスクに物理的に接続されています。

共有ディスク

共有ディスクボリューム(MSCSの場合)または**共有ボリュームグループ**(MC/SG、Veritas Clusterの場合)内には、ミッションクリティカルなアプリケーションデータのほか、クラスターの実行に必要なクラスター固有のデータも格納されています。MSCSクラスター内では、共有ディスクはある一時点では1つのクラスターノード上でしか使用できません。

クラスターネットワーク

クラスターネットワークは、すべてのクラスターノードを接続するプライベートネットワークです。このネットワークにより、**クラスターのハートビート**と呼ばれる内部的なクラスターデータが転送されます。ハートビートとはタイムスタンプ付きのデータパケットで、すべてのクラスターノードに配布されます。各クラスターノードでは、このパケットを比較することにより、どのクラスターノードが現在稼働中であるかを判断します。これにより、**パッケージ** (MC/SG、Veritas Clusterの場合)または**グループ**(MSCSの場合)の適切な所有権を決定できます。

パッケージまたはグループとは

パッケージ(MC/SGまたはVeritas Clusterの場合)、またはグループ(MSCSの場合)とは、特定の**クラスター対応**アプリケーションの実行に必要なリソースの集まりを指します。各クラスター対応アプリケーションでは、それぞれの重要なリソースを宣言します。

各グループまたはパッケージ内では、以下のリソースが定義されていなければなりません。

- 共有ディスクボリューム(MSCS)
- 共有ボリュームグループ(MC/SG、Veritas Clusterの場合)
- ネットワークIP名
- ネットワークIPアドレス
- クラスター対応アプリケーションサービス

仮想サーバーとは

ディスクボリュームおよびボリュームグループは、共有されている物理ディスクを指します。ネットワークIP名およびネットワークIPアドレスは、クラスター対応アプリケーションの**仮想サーバー**を定義するリソースです。仮想サーバーのIP名とIPアドレスはクラスターソフトウェアによって認識され、特定のパッケージまたはグループを現在実行しているクラスターノードに割り当てられます。グループまたはパッケージはノード間で移動できるので、仮想サーバーは時間帯によって異なるマシン上に配置されている可能性があります。

フェイルオーバーとは

それぞれのパッケージまたはグループには、通常の場合に実行される「優先」ノードが設定されています。このノードは、**プライマリノード**と呼ばれます。パッケージまたはグループは、他のクラスターノード(**セカンダリノード**のいずれか)に移動することができます。パッケージまたはグループをプライマリクラスターノードからセカンダリクラスターノードに移すことを**フェイルオーバー**、またはスイッチオーバーと呼びます。セカンダリノードは、プライマリノードで障害が発生した場合にパッケージまたはグループを引き継ぎます。フェイルオーバーは、以下に示すような原因により発生します。

- プライマリノード上でソフトウェア障害が発生した場合
- プライマリノード上でハードウェア障害が発生した場合
- プライマリノード上での保守作業を目的として、管理者が意図的に所有権を移した場合

クラスター環境では、複数のセカンダリノードを設定できますが、プライマリノードは1つしか設定できません。

IDBを実行したり、バックアップおよび復元処理の管理などを行うクラスター対応のData Protector Cell Managerには、非クラスター対応バージョンに比べて、以下に挙げる多くの利点があります。

Data Protector Cell Managerの高可用性の実現

Cell Managerのすべての機能が常に使用できます。これはData Protectorの各種サービスが、クラスター内でクラスターリソースとして定義されており、フェイルオーバーの発生時に自動的に再開されるためです。

バックアップの自動再開

バックアップ手順を定義するためのData Protectorバックアップ仕様は、Data Protector Cell Managerでのフェイルオーバーの発生時に対応するセッションを自動再開するように簡単に構成できます。再開に関するパラメーターを定義するには、Data ProtectorのGUIを使用します。

フェイルオーバー時の負荷調整

Data Protector以外のアプリケーションがフェイルオーバーを実行した場合に、バックアップセッションを中止する特殊なコマンドラインユーティリティがあります。Data Protector Cell Managerではこのような場合に、特定のセッションを再開するか中止するかの基準をユーザーが定義できます。アプリケーションよりもバックアップの方が重要度が低い場合は、Data Protectorにより実行中のセッションを中止できます。より重要なバックアップを行っていた場合や、あと少しで処理が終了するような場合には、セッションを継続できData Protectorます。基準の定義方法については、『*HPE Data Protectorヘルプ*』のキーワード「cluster, managing backups」で表示される内容を参照してください。

クラスターのサポート

Data Protectorのクラスターサポートとは、以下の内容を意味します。

- Data Protector Cell Managerがクラスター内にインストールされていること。このようなCell Managerはフォールトトレラントである上、フェイルオーバー後にセル内で自動的に操作を*再開*できます。

  > **注:**
  > Cell Managerがクラスター内にインストールされている場合、クラスターの重要なリソースを、バックアップ対象のアプリケーションと同じクラスターパッケージまたはグループ内に構成する必要があります。これにより、フェイルオーバーが原因で*失敗したバックアップセッション*を自動的に再開できます。上記の構成を行わなかった場合、失敗した*バックアップセッション*を手動で再開する必要があります。

- Data Protectorクライアントがクラスター内にインストールされていること。このような場合、Cell Manager(クラスターにインストールされていない場合)はフォールトトレラントではありません。セル内の処理は、手動で再開する必要があります。

フェイルオーバー後のCell Managerの動作は構成可能です。ただしこれは、(フェイルオーバーのため失敗した)*バックアップセッション*が関連する場合に限られます。失敗したセッションに対して以下を行えます。

- セッション全体を再開する
- 失敗したオブジェクトについてのみ再開する
- 再開しない

Data Protector Cell Managerのフェイルオーバー発生時の*バックアップセッション*の動作オプションの詳細については、『*HPE Data Protectorヘルプ*』のキーワード「cluster, backup specification options」で表示される内容を参照してください。

クラスター環境の例

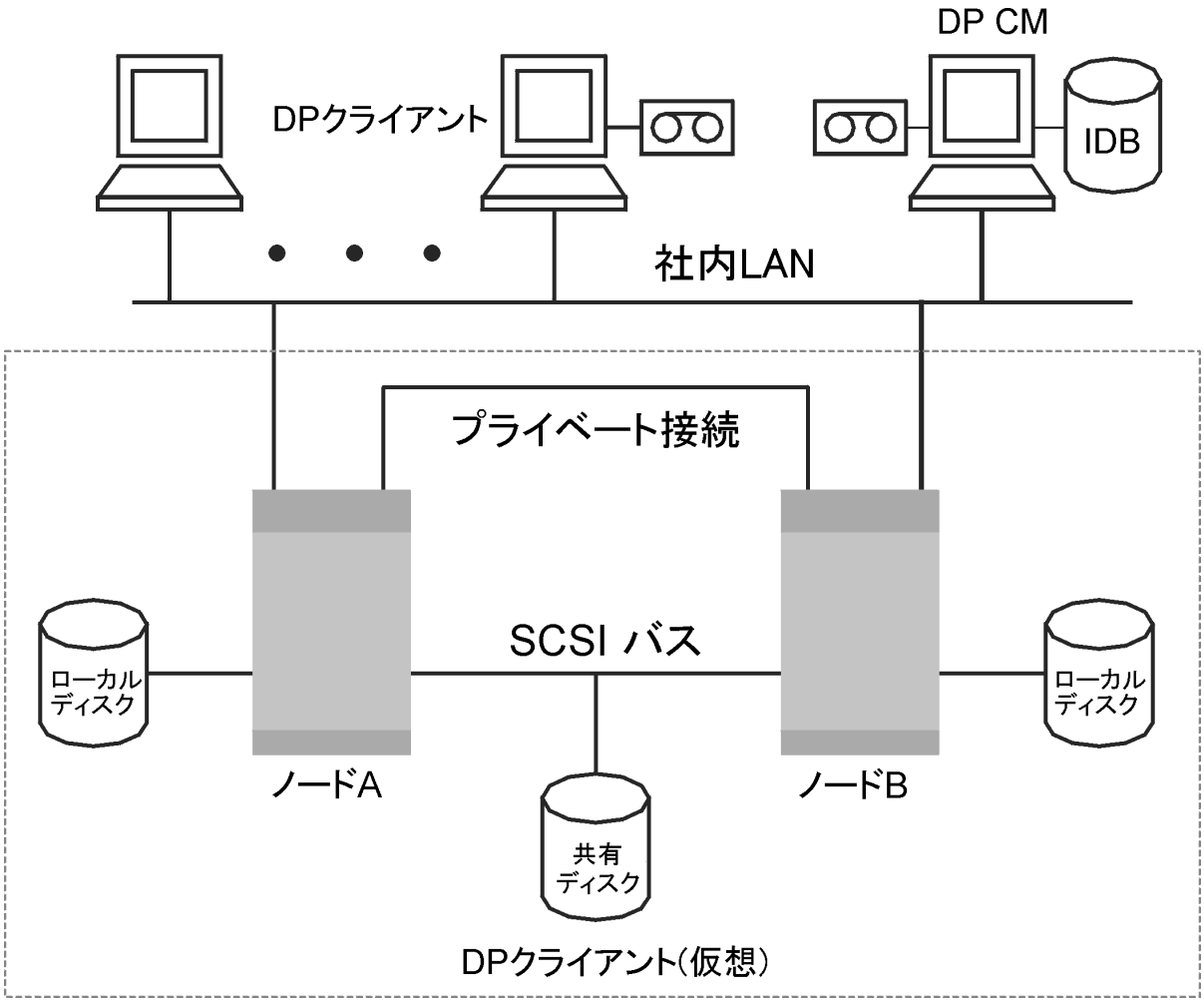
この項では、3つのクラスター構成例を示します。

Cell Managerがクラスター外部にインストールされている構成

下図の環境には以下のような特徴があります。

- Cell Managerは、クラスターの外部にインストールされています。
- バックアップデバイスは、Cell Managerまたは非クラスター化クライアントの1つに接続されています。

Cell Managerがクラスター外部にインストールされている構成



バックアップ仕様を作成するときには、ユーザーはこのクラスター内でバックアップが可能なシステムとして、以下の3つ(またはそれ以上)を認識できます。

- 物理ノードA
- 物理ノードB
- 仮想サーバー

仮想サーバーのバックアップ

バックアップ仕様で仮想サーバーを選択した場合のバックアップセッションでは、パッケージまたはグループが現在どの物理ノードで稼動しているかに関係なく、選択したアクティブ仮想ホスト/サーバーがバックアップされます。

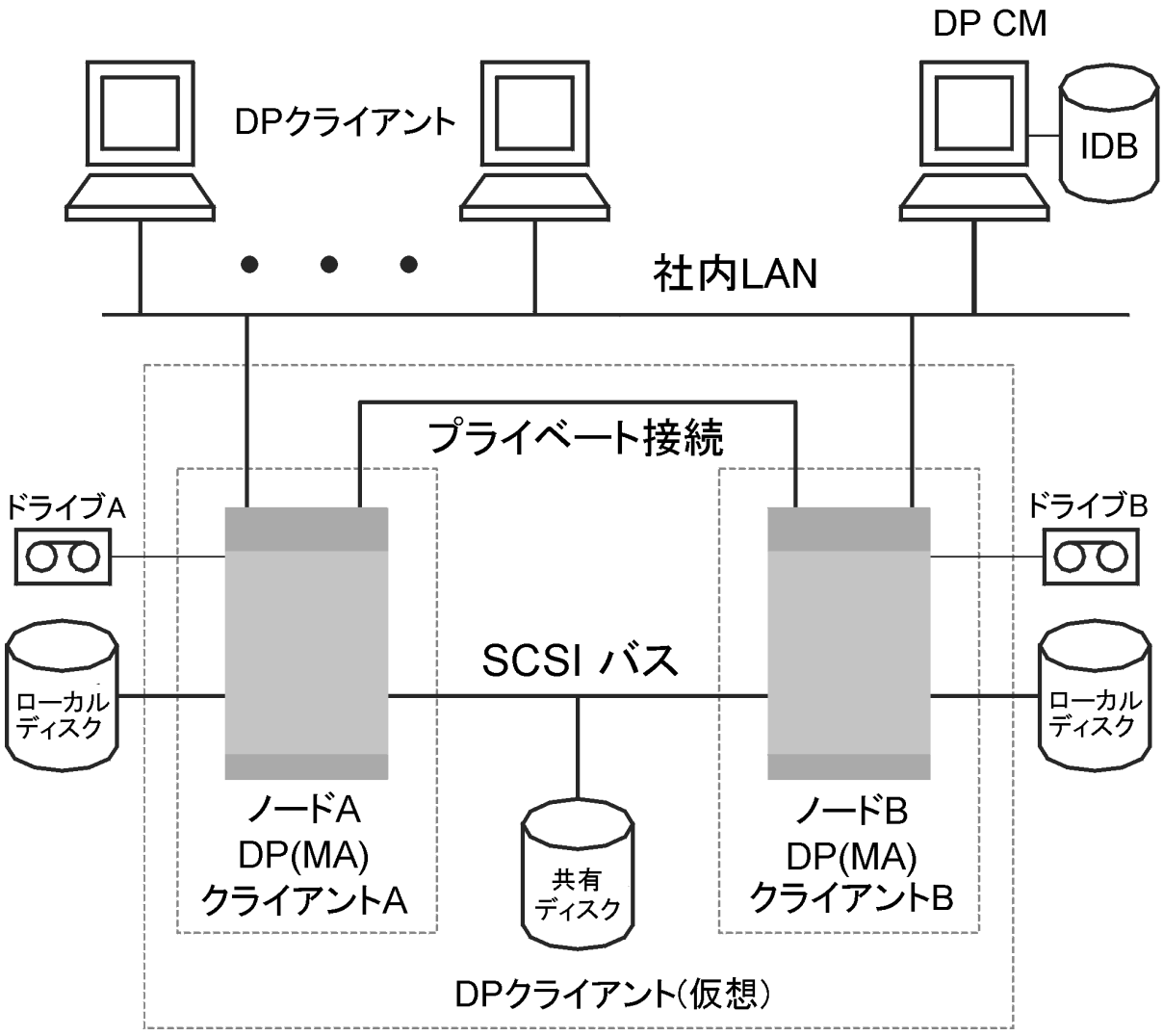
これらのオプションの定義方法については、『*HPE Data Protectorヘルプ*』のキーワード「cluster, backup specification options」で表示される内容を参照してください。

Cell Managerがクラスター外部にインストールされ、デバイスがクラスターノードに接続されている構成

下図の環境には以下のような特徴があります。

- Cell Managerは、クラスターの外部にインストールされています。
- バックアップデバイスは、クラスター内のノードに接続されています。

Cell Managerがクラスター外部にインストールされ、デバイスがクラスターノードに接続されている構成



バックアップ仕様を作成するときには、ユーザーはこのクラスター内でバックアップが可能なシステムとして、以下の3つ(またはそれ以上)を認識できます。

- 物理ノードA
- 物理ノードB
- 仮想サーバー

仮想サーバーのバックアップ

バックアップ仕様で仮想サーバーを選択した場合のバックアップセッションでは、パッケージまたはグループが現在どの物理ノードで稼動しているかに関係なく、選択したアクティブ仮想ホスト/サーバーがバックアップされます。

> **注:**
> この例では、先の例とは異なり、個々のクラスターノードにData ProtectorのMedia Agentがそれぞれインストールされています。さらにユーザーは、Data Protectorの負荷調整機能を使用する必要があります。そのため、両方のデバイスをバックアップ仕様の中に指定しています。負荷調整を、`min=1`および`max=1`と設定しておくと、最初に使用可能になったデバイスのData Protectorみが使用されます。

Cell Managerがクラスター内部にインストールされ、デバイスがクラスターノードに接続されている構成

下図の環境には以下のような特徴があります。

- Cell Managerは、クラスターの内部にインストールされています。

  Data Protectorアプリケーション用統合機能については、このような構成の場合、Data Protectorとアプリケーションを以下のいずれかの方法で構成できます。

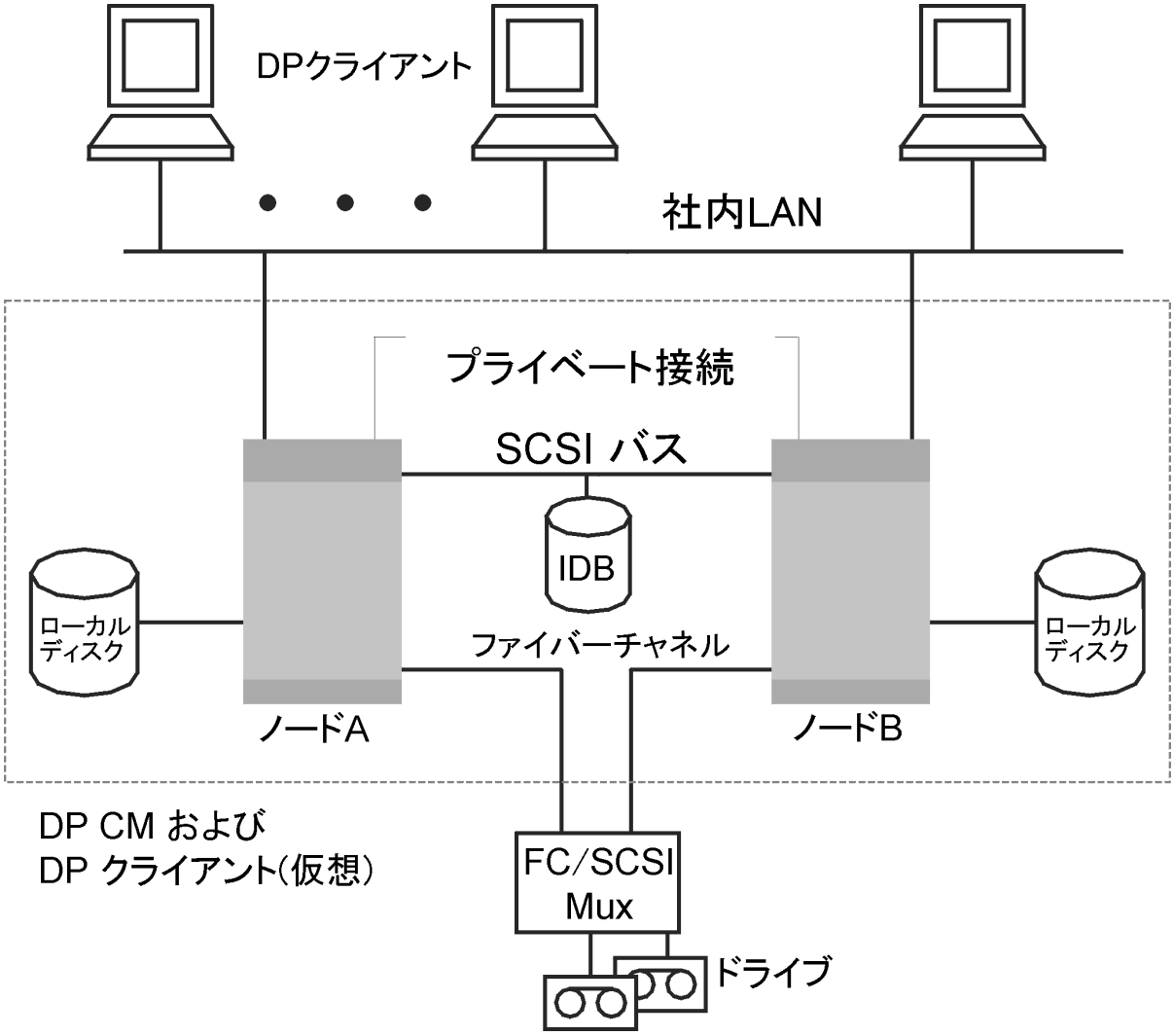
  - Data Protector Cell Managerをアプリケーションと同じノード上で実行するよう構成します(通常の動作時およびフェイルオーバー時共)。つまり、Data Protectorクラスターの重要なリソースは、アプリケーションクラスターの重要なリソースと同じパッケージ(HPE Serviceguardの場合)またはグループ(Microsoft Cluster Serverの場合)内に定義します。

    > **重要:**
    > 上記のような構成の場合に限り、フェイルオーバー中に中止されたData Protectorセッションについて自動的に実行される動作を定義できます。

  - Data Protector Cell Managerをアプリケーションノード以外のノード上で実行するよう構成します(通常の動作時およびフェイルオーバー時共)。つまり、Data Protectorクラスターの重要なリソースは、アプリケーションクラスターの重要なリソースとは別のパッケージ(HPE Serviceguardの場合)またはグループ(Microsoft Cluster Serverの場合)内に定義します。

- バックアップデバイスは、クラスターの共有ファイバーチャネルバスに、FC/SCSI MUXを介して接続されています。

Cell Managerがクラスター内部にインストールされ、デバイスがクラスターノードに接続されている構成



バックアップ仕様を作成するときには、ユーザーはこのクラスター内でバックアップが可能なシステムとして、以下の3つ(またはそれ以上)を認識できます。

- 物理ノードA
- 物理ノードB
- 仮想サーバー

仮想サーバーのバックアップ

バックアップ仕様で仮想サーバーを選択した場合のバックアップセッションでは、パッケージまたはグループが現在どの物理ノードで稼動しているかに関係なく、選択したアクティブ仮想ホスト/サーバーがバックアップされます。

> **注:**
> クラスターでは、共有テープにSCSIバスを使用できません。Media Agentについても高可用性を実現するには、デバイスとのインターフェイスにファイバーチャネルテクノロジを使用してください。この構成では、デバイスそのものは高可用性構成にはなっていません。

この構成では、以下の機能が提供されます。

- Cell Managerのフェイルオーバーが発生した場合に、カスタマイズされた形でバックアップを自動再開できます。

  Data Protectorでは、Cell Managerのフェイルオーバーが発生した場合にバックアップを再開するよう、バックアップ仕様を構成できます。再開に関するパラメーターを定義するには、Data ProtectorのGUIを使用します。
- フェイルオーバー発生時のシステム負荷を制御できます。

  高度な制御機能により、フェイルオーバー発生時におけるData Protectorの動作を定義することも可能です。この処理には、専用コマンドのomniclusを使用します。管理者は、フェイルオーバー発生時に実行すべき処理内容を、Cell Managerを使用して、以下のように定義できます。
  - バックアップシステムに引き継がれたアプリケーションに比べて、バックアップ処理の重要度が低い場合には、Data Protectorにより実行中のバックアップセッションを中止できます。
  - より重要なバックアップを行っていた場合や、あと少しで処理が終了するような場合には、Data Protectorはセッションを継続します。

また、Data ProtectorクラスターのCell Manager/クライアントを、EMC Symmetrix環境またはHPE P9000 XPディスクアレイファミリ環境と統合すると、非常に可用性の高いバックアップ環境を構築できます。詳細については、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参照してください。

フルバックアップ、増分バックアップ、合成バックアップ

Data Protectorのファイルシステムバックアップには、フルバックアップと増分バックアップの2種類があります。

フルバックアップを実行すると、バックアップ対象として選択されたすべてのファイルがファイルシステムにバックアップされます。一方増分バックアップの場合には、前回のフルバックアップ時または増分バックアップ時以降に更新されたファイルのみがバックアップされます。以下では、使用するバックアップタイプの選択方法と、選択結果がバックアップ戦略に及ぼす影響について説明します。

フルバックアップと増分バックアップの比較

	フルバックアップ	増分バックアップ
リソース	増分バックアップに比べて時間を要し、多くのメディア容量を必要とします。	前回のバックアップ以降の変更部分のみをバックアップするため、必要な時間とメディア容量が少なくて済みます。
デバイスの取り扱い	単一ドライブのスタンドアロンデバイスを使用する場合は、バックアップデータの量が1つのメディアのサイズを上回っていると、手動でメディアを交換する必要が生じます。	バックアップ中にメディアを追加する必要性は、あまりありません。
復元	シンプルで迅速な復元が可能です。	複数のメディアが必要になるため、復元に時間を要します。

	フルバックアップ	増分バックアップ
IDBへの影響	IDB内に占めるスペースが大きい	IDBに書き込む情報の量がフルバックアップほど多くありません。

Data Protectorでは、オンラインデータベースアプリケーションの増分または差分バックアップも可能です。ただし処理内容の詳細は、各アプリケーションによって異なります。たとえばSybaseでは、この種のバックアップはトランザクションバックアップと呼ばれ、最後のバックアップ以降に変更されたトランザクションログのみがバックアップされます。

増分バックアップの概念は、ロギングレベルの概念とは無関係である点に注意してください。ロギングレベルとは、IDBに書き込まれる詳細情報の量を定義するためのものです。

> **注:**
> Data Protectorのアプリケーション統合では、さらにさまざまな種類のバックアップ(スプリットミラーバックアップ、スナップショットバックアップ、データムーバーバックアップなど)を使用できます。詳細については、『*HPE Data Protectorインテグレーションガイド*』を個別に参照してください。

フルバックアップ

フルバックアップの場合には、前回のバックアップより後に更新されたファイルがない場合でも、選択されたファイルがすべてバックアップされます。

合成バックアップ

合成バックアップは、通常のフルバックアップを実行する必要のない高度なバックアップソリューションです。代わりに、増分バックアップが実行され、続いてそれがフルバックアップとマージされると、新規合成フルバックアップとなります。詳細については、合成バックアップ、ページ 66を参照してください。

増分バックアップ

増分バックアップの場合には、保護されているファイルのうち、前回の(フルまたは増分)バックアップより後に更新されたファイルのみがバックアップされます。オブジェクトの増分バックアップを実行するには、同一のクライアント名、マウントポイント、および説明を指定して作成された、そのオブジェクトのフルバックアップが事前に存在している必要があります。

増分バックアップは、最後のフルバックアップに依存します。保護されたフルバックアップがない場合に増分バックアップを指定すると、代わりにフルバックアップが実行されます。

従来の増分バックアップ

バックアップオブジェクトに対する増分バックアップの開始時には、まずバックアップオブジェクト内のツリーと、そのオブジェクトの有効な復元Data Protectorチェーン内のツリーが比較されます。前回のバックアップより後にバックアップオブジェクト内の追加のディレクトリがバックアップ対象として選択された場合や、同じバックアップオブジェクトに対してツリー指定が異なるバックアップ仕様が複数存在する場合など、ツリーが一致していない場合には、フルバックアップが自動的に実行されます。この仕組みにより、前回の当該バックアップより後に変更されたすべてのファイルが確実にバックアップされます。

従来の増分バックアップでは、前回のバックアップからファイルが変更されたかどうかを判断する主な条件として、ファイルの更新時刻が使用されます。しかしファイルが名称変更されたり、新しい場所に移動されたり、属性のいくつかが変更された場合は、更新時刻は変更されません。したがって、従来の増分バックアップではファイルが常にバックアップされるとは限りません。このようなファイルは、次回のフルバックアップでバックアップされます。

拡張増分バックアップ

拡張増分バックアップでは、名称変更や移動が行われたファイルや、特定の属性が変更されたファイルも、確実に検出されてバックアップされます。

また、拡張増分バックアップを採用した場合、バックアップ対象として選択されているツリーの一部が変更されたときに、バックアップオブジェクト全体のフルバックアップを行う必要がありません。たとえば、前回のバックアップ以降にバックアップ対象として新たに1つのディレクトリが選択された場合、このディレクトリ(ツリー)についてはフルバックアップが行われ、その他の部分のバックアップは増分型となります。

拡張増分バックアップの使用は、合成バックアップの前提条件となります。

Change Log Providerを使用した増分バックアップ

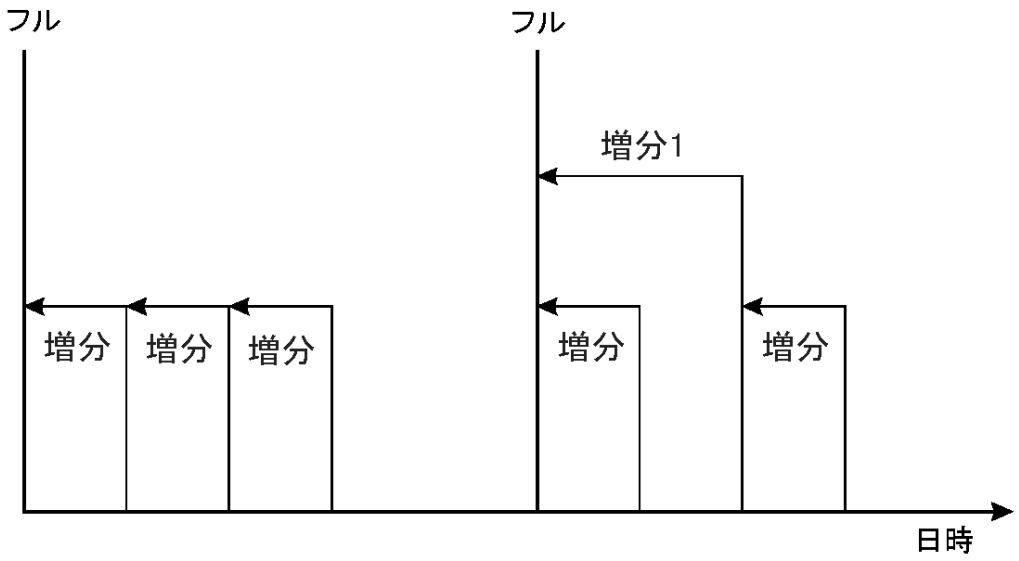
拡張増分バックアップや従来の増分バックアップは、Windows NTFS Change Log Providerを使用して実行できます。Change Log Providerでは、時間を要するファイルツリー検索ではなく、Windows Change Journalへの問い合わせで変更ファイルのリストを取得します。変更ジャーナルではNTFSボリューム上のファイルおよびディレクトリに対して行われたすべての変更が検出および記録されるため、Data Protectorでは、これを追跡メカニズムとして使用して、最後のフルバックアップ以降に変更されたファイルのリストを生成できます。これによって、増分バックアップの速度が改善されます。特に何百万ものファイルのうちごくわずかしか変更されていない環境では速度が改善され、不要なフルバックアップの回数を減らすことができます。

増分バックアップの種類

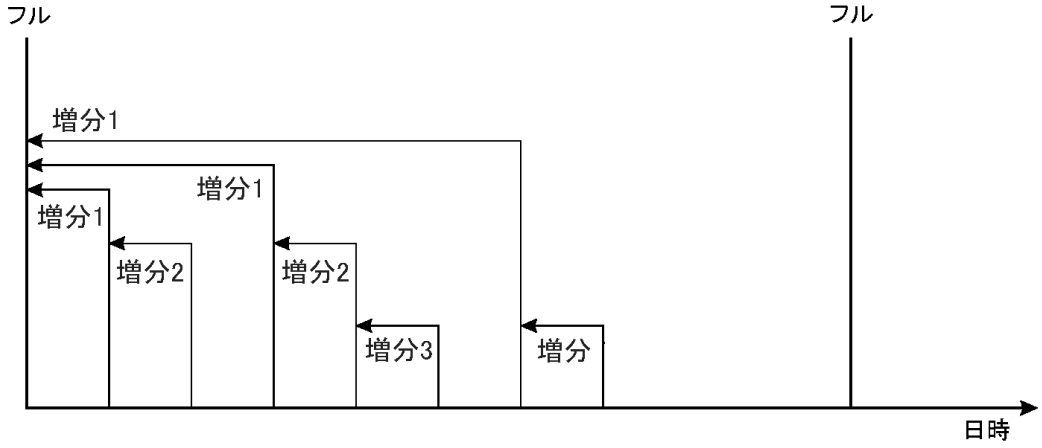
Data Protectorで実行できる増分バックアップには以下の種類があります。

増分	単純な増分バックアップは、増分バックアップ、次のページに示すとおり、まだ保護期限が切れていない最後のバックアップ(フルバックアップ、またはいずれかのレベルの増分バックアップ)をベースとして行われます。
増分1～9	**複数レベル増分バックアップ**は、複数レベル増分バックアップ、次のページに示すとおり、保護されている1つ下のレベルのバックアップのうち、最新のバックアップをベースとします。たとえば増分1バックアップを実行すると、前回のフルバックアップ時より後に更新された、すべてのデータが保存されます。また、増分5バックアップを実行すると、前回の増分4バックアップより後に更新されたすべてのデータが保存されます(増分4バックアップが存在する場合)。増分1～9バックアップでは、既存の増分バックアップは参照されません。

増分バックアップ



複数レベル増分バックアップ



バックアップ実行時の相対的参照関係、下に、さまざまなバックアップタイプの実行時の相対的な参照関係を示します。詳細な説明については、表の下のテキストを参照してください。

バックアップ実行時の相対的参照関係

1	フル	<----	増分1				
2	フル	<----	<----	<----	増分2		
3	フル	<----	増分1	<----	増分2		
4	フル	<----	増分				

5	フル	<----	増分1	<----	増分		
6	フル	<----	増分1	<----	増分2	<----	増分
7	フル	<----	増分1	<----	増分	<----	増分
8	フル	<----	増分1	<----	増分3		
9	フル	<----	増分1	<----	増分2	<----	増分3
10	フル	<----	<----	<----	増分2	<----	増分3
11	フル	<----	<----	<----	<----	<----	増分3

バックアップ実行時の相対的参照関係、前のページの見方

- バックアップ実行時の相対的参照関係、前のページの各行は互いに関係性はなく、異なる状況を示します。
- バックアップの経過時間は、右から左に増加します。したがって左端が一番古く、右端が最新のバックアップになります。
- フルと増分Xは、同じ所有者の保護期限内のオブジェクトを表します。保護されていない既存の増分Xは復元に使用できますが、それより後のバックアップ実行時の参照には考慮されません。

例

- 2行目では、フルで保護期間内のバックアップが実行され、増分2が実行中です。増分1がないため、バックアップは増分1として実行されます。
- 5行目では、フルバックアップが実行され、増分1と他の増分が実行中です。Data Protectorでは、1つ前の増分(増分1)に対して実行中のバックアップを参照します。
- 8行目では増分3が増分2として実行され、11行目では増分3が増分1として実行されます。

バックアップ世代

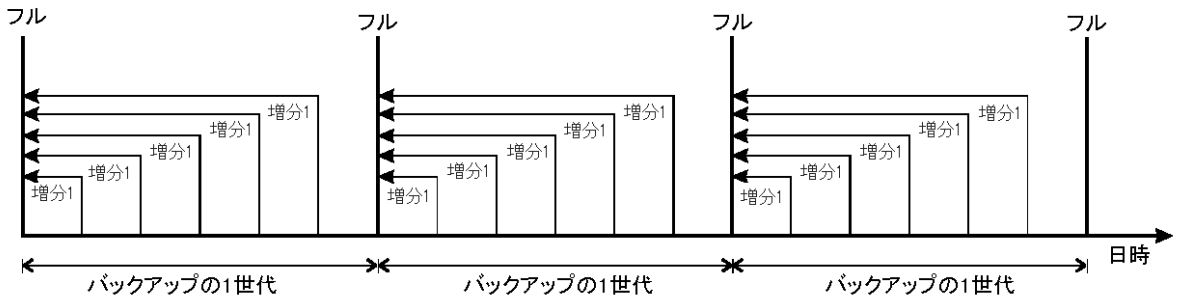
Data Protectorでは、日付/時刻ベースの保護モデルが採用されています。定期的にバックアップを行っている場合は、世代ベースのバックアップモデルと、この日時ベースのバックアップモデルを簡単に対応付けることができます。

バックアップ世代とは

バックアップ世代、次のページに示すように、バックアップ世代は、1つのフルバックアップと、そのフルバックアップをベースとするすべての増分バックアップで構成されています。次のフルバックアップが実行されると、新しいバックアップ世代が作成されます。

バックアップ世代は、フルバージョンのバックアップデータがいくつあるかを把握するのに役立ちます。特定の時点への復元を成功させるには、少なくとも1つのバックアップ世代(1つのフルバックアップと目的の時点までに作成されたすべての増分バックアップ)が必要です。各企業のデータ保護ポリシーに従って、複数のバックアップ世代を保管するようにしてください(3世代など)。

バックアップ世代



適切なデータ保護期間とカタログ保護期間を設定して、フルバックアップおよび増分バックアップの無人実行をスケジュール設定すると、必要な数のバックアップ世代がData Protectorにより自動的に保持されるようになります。

たとえば、週1回のフルバックアップと1日1回の増分バックアップを実行する場合に、3つのバックアップ世代を保管するには、データ保護期間を7*3+6=27日と設定します。1つのバックアップ世代は、1つのフルバックアップと、その次のフルバックアップまでに実行されるすべての増分バックアップで構成されます。式に含まれる6という数値は、4番目のバックアップ世代が作成されるまでに、3番目のバックアップ世代に属する増分バックアップが実行される回数を表しています。

適切なプール使用方法を設定しておくと、保護期間が切れたメディアを自動交換させることもできます。詳細については、メディア交換ポリシーの実装、ページ 155を参照してください。

合成バックアップ

この項では、合成バックアップの概念と、Data Protectorが提供する合成バックアップソリューションについて説明します。

概要

データ量の増加とバックアップウィンドウの短縮に伴い、フルバックアップの実行は、時間とストレージスペースの点でしばしば問題になることがあります。その一方で、増分バックアップを数多く実行することは、復元に必要な時間がそれだけ増えることになり、問題となる場合があります。

ディスクへのバックアップは、パフォーマンスが高い、容量が大きい、ディスクの価格が低下しているなどの理由から一般的になりつつあり、新しい選択肢が出現していますが、業界では、バックアップウィンドウを最小限に抑えること、稼動中のサーバーやネットワークへの負荷を最小限に抑えること、そして、速やかな復元を可能にすることが求められています。このような要件を満たすのが、合成バックアップです。

合成バックアップは、**合成フルバックアップ**を生成する高度なバックアップで、従来のデータのフルバックアップと同等の機能を持ちながら、稼働中のサーバーやネットワークに負荷をかけることがありません。合成フルバックアップは、前回のフルバックアップと任意の数の増分バックアップを使用して作成されます。

合成バックアップを実行することで、定期的なフルバックアップを実行する必要性がなくなります。代わりに、増分バックアップが実行され、続いてそれがフルバックアップとマージされると、新規合成フルバックアップとなります。この処理は何度でも制限なく繰り返すことができ、フルバックアップを再び実行する必要はありません。

復元速度については、合成フルバックアップのバックアップでも従来のフルバックアップでも同じです。復元チェーンは1つの要素のみで構成できるため、復元は可能な限りすばやく簡単に行われます。

合成バックアップの利点

合成バックアップには、次のような利点があります。

- フルバックアップの必要性がなくなります。最初のフルバックアップ以降は、増分バックアップのみが実行されるため、バックアップに要する時間が大幅に短縮されます。
- バックアップオブジェクトの集約がデバイスサーバー上で実行されるため、稼動中のサーバーにもネットワークにも負荷をかけることがありません。
- 合成バックアップの一種である仮想フルバックアップは、さらに効率の良いバックアップです。仮想フルバックアップでは、ポインターを使用してデータが集約されるため、データの不必要な重複がなくなります。
- 合成フルバックアップからの復元速度は、増分バックアップからデータを取得する必要がないため、従来のフルバックアップと同じです。これにより、復元チェーン内の増分バックアップを個々に読み取る必要がなくなります。また、テープデバイスを使用している場合は、複数のメディアのロードとアンロードや、オブジェクトのバージョンの検索も必要ありません。

Data Protectorの合成バックアップの仕組み

Data Protectorの合成バックアップでは、フルバックアップと任意の数の増分バックアップをマージして、新しい合成フルバックアップにすることができます。

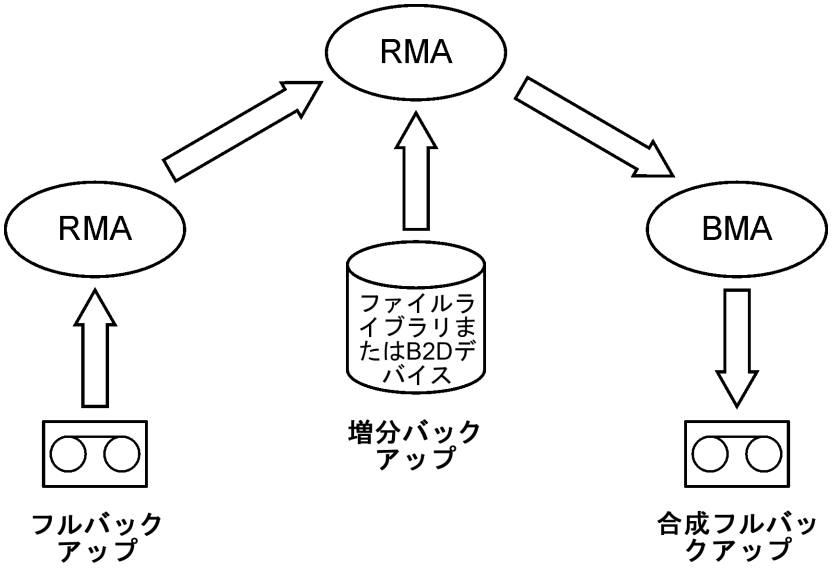
合成バックアップを有効にするには、拡張増分バックアップを使用する必要があります。拡張増分バックアップは、フルバックアップおよび増分バックアップを実行する前にオンにしておく必要があります。

合成フルバックアップは、ディスクまたはテープデバイスに書き込まれるフルバックアップと、ディスクベースのデバイス、Data Protectorファイルライブラリまたは B2Dデバイス(Smart Cacheを除く)に書き込まれる増分バックアップから作成できます。作成した合成フルバックアップも、ディスクまたはテープデバイスに書き込むことができます。

分散ファイルメディア形式を使用する同じファイルライブラリに、すべてのバックアップ(フルおよび増分)を書き込む場合は、さらに効率の良い合成バックアップ(**仮想フルバックアップ**)を使用できます。このソリューションでは、データをコピーするのではなく、ポインターを使ってデータを集約します。これにより、より短時間で集約でき、不必要なデータ複製を行わずに済みます。

以下の図で、合成バックアップと仮想フルバックアップの概念について説明します。これらの図は、フルバックアップと任意の数の増分バックアップから、合成フルバックアップまたは仮想フルバックアップが作成される様子を示しています。

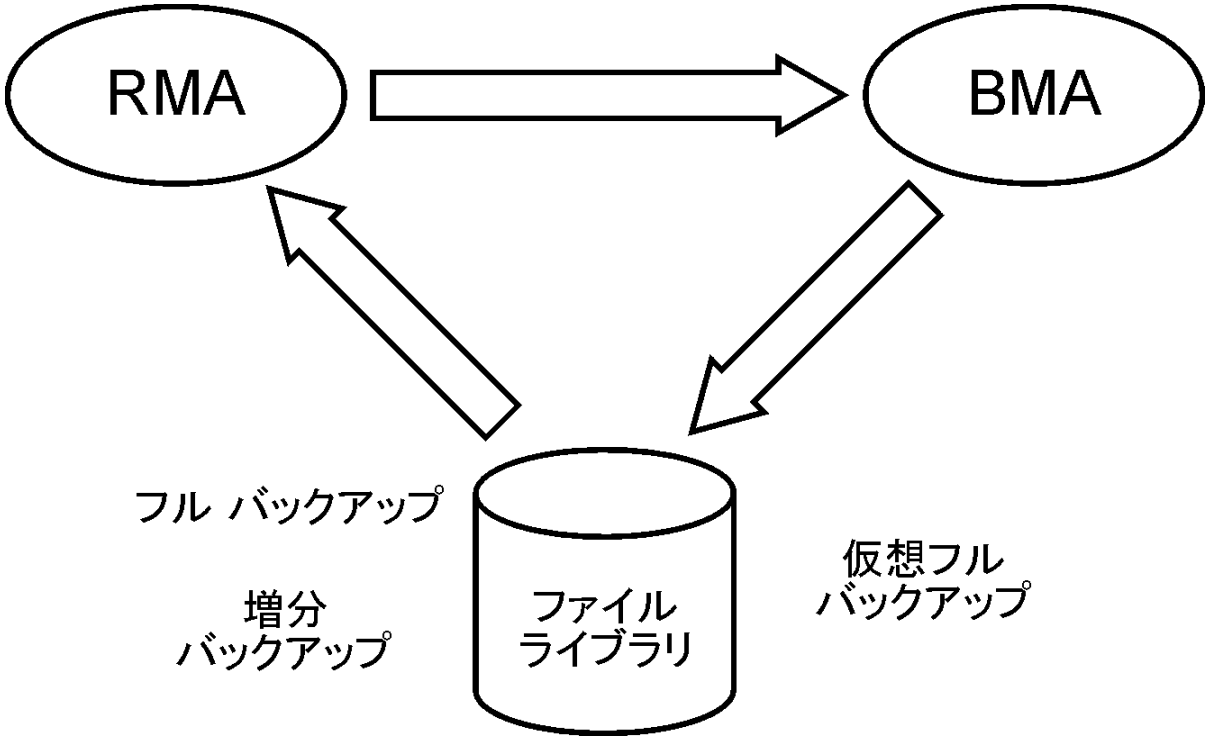
合成バックアップ



合成バックアップ、上は、合成フルバックアップが作成される様子を示しています。Restore Media Agent (RMA)によって、バックアップメディア(テープまたはディスク)からフルバックアップが読み取られます。そのデータは別のRMAに送られ、そのRMAがファイルライブラリまたはB2Dデバイス(Smart Cacheを除く)から増分バックアップを読み取り、データを集約します。次に、集約されたデータはBackup Media Agent(BMA)に送られ、合成フルバックアップがバックアップメディア(テープまたはディスク)に書き込まれます。

その後に、通常は合成フルバックアップがそれ以降の増分バックアップとマージされ、新規の合成バックアップになります。この手順は、それぞれの増分バックアップの後に、または必要な間隔で、何度でも繰り返すことができます。

仮想フルバックアップ



仮想フルバックアップ、上は、仮想フルバックアップが作成される様子を示しています。このタイプのバックアップの場合、分散ファイルメディア形式を使用する1つのファイルライブラリ内にすべてのバックアップが存在します。Restore Media Agent(RMA)は、フルバックアップと増分バックアップに関する情報を読み取り、仮想フルバックアップ用のデータを生成します。生成されたデータはBackup Media Agent(BMA)に送られ、そこで仮想フルバックアップがファイルライブラリ内に作成されます。

合成バックアップとメディアスペースの使用量

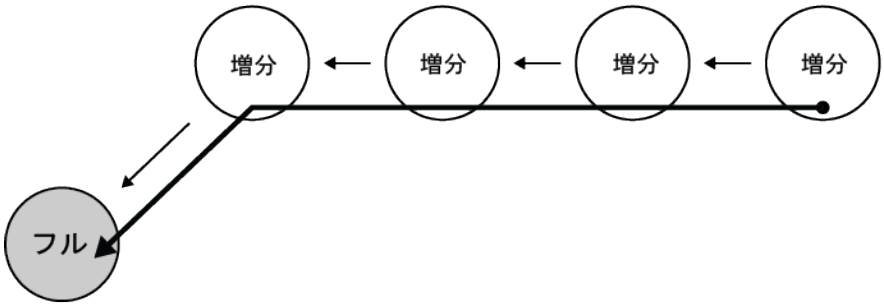
合成バックアップを頻繁に実行し、ソースを保持しておく場合、バックアップメディア上のスペース使用量は一般にかなり大きくなります。ただし、仮想フルバックアップを実行すると、バックアップメディア上のスペース使用量を最小限に抑えることができます。

仮想フルバックアップでは、スペース使用量はバックアップするファイルのサイズに大きく依存します。ファイルのサイズが使用ブロックサイズよりもかなり大きければ、通常の合成バックアップを行った場合に比べて、仮想フルバックアップで節約されるスペースは非常に大きくなります。逆にファイルがブロックサイズよりも小さい場合は、大きな効果がありません。

復元と合成バックアップ

合成フルバックアップからの復元は、従来のフルバックアップからの復元と同じ機能があります。以下の図は、データを可能な限り最新の状態に復元することが必要な状況を想定したときのさまざまな場合を示しています。どの例の場合にも、1つのフルバックアップと4つの増分バックアップのバックアップオブジェクトが存在します。異なっているのは、合成バックアップの使用方法です。

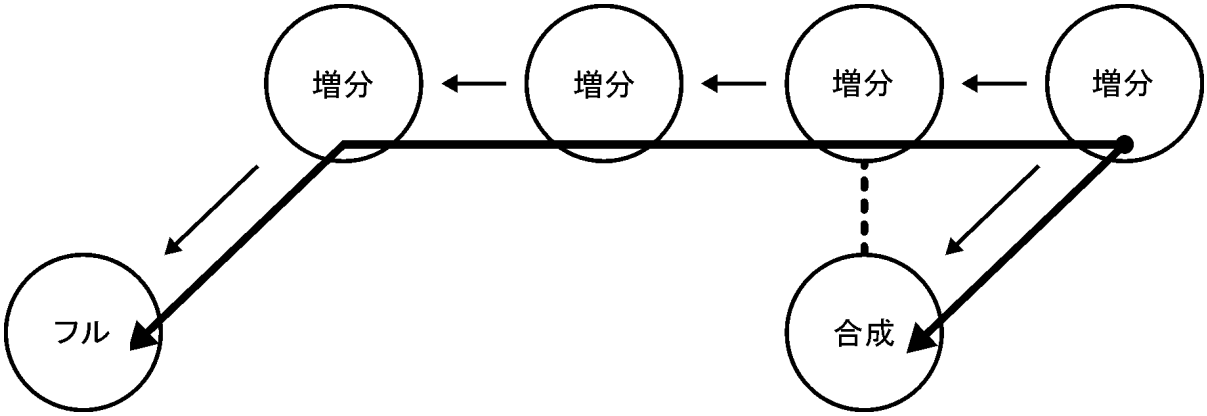
フルバックアップと増分バックアップ



フルバックアップと増分バックアップ、上では、従来のバックアップが実行されています。可能な限り最新の状態に復元するためには、フルバックアップと4つ増分バックアップがすべて必要になります。復元チェーンは5つの要素で構成されており、これらの要素は異なるメディアに存在することがよくあります。

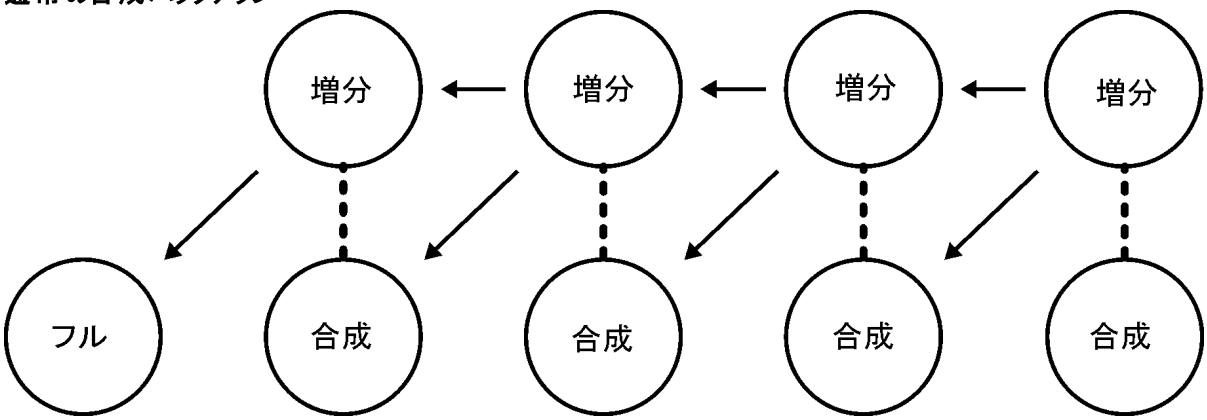
このような復元では、それぞれの増分バックアップを読み取る必要があるため、非常に多くの時間を要する場合があります。テープデバイスを使用している場合は、複数のメディアのロードとアンロードの時間や、復元するオブジェクトバージョンを検索する時間を要します。

合成バックアップ



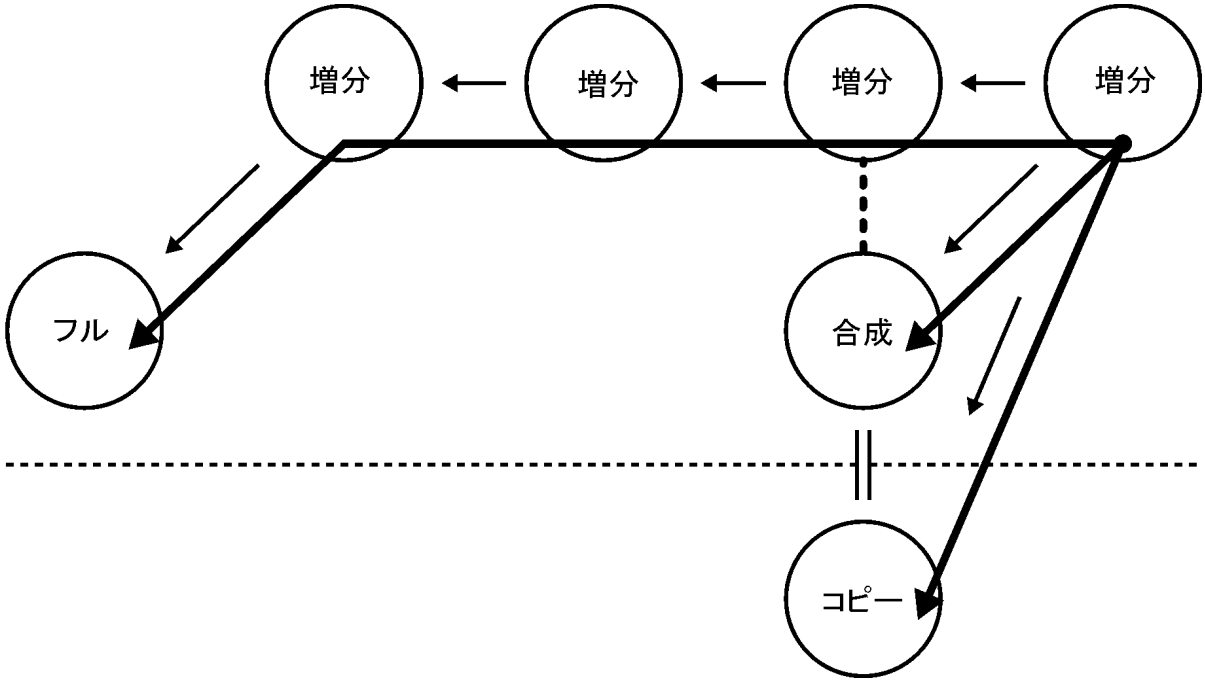
合成バックアップ、上には合成フルバックアップが存在しており、復元用にデフォルトで使用されます。復元チェーンは、2つの要素(合成フルバックアップとそれ以降の増分バックアップ)のみで構成されます。復元は、合成フルバックアップがない場合に比べて大幅に単純かつ高速になります。この図では、想定される両方の復元チェーンを示しています。

通常の合成バックアップ



通常の合成バックアップ、前のページは、それぞれの増分バックアップ後に合成バックアップが実行された状況を示しています。この方式では、可能な限り最新の状態またはバックアップされた任意の時点に、最も単純かつ高速に復元できます。復元に必要な要素は1つのみ(希望する時点の合成フルバックアップのみ)です。

合成バックアップとオブジェクトコピー



合成バックアップとオブジェクトコピー、上では、合成バックアップが、実行された後でコピーされています。これにより、安全性が強化されます。図に示している3つの復元チェーンのいずれを使用した場合でも、可能な限り最新の状態に復元することができます。デフォルトでは、Data Protectorによって最適な復元チェーンが選択され、それには、通常、合成フルバックアップまたはそのコピーが含まれます。メディアが失われた場合や、メディアエラーなどの場合には、別の復元チェーンが使用されます。

合成バックアップからの復元に対するデータ保護期間の影響

合成フルバックアップの前に行われる従来のフルバックアップやすべての増分バックアップのデータが保護されている場合でも、復元の正常な実行が妨げられることはありません。

デフォルトでは、バックアップチェーン内の最新の合成フルバックアップが復元に使用されます。このとき、以前のバックアップがまだ有効であるかどうかや、保護がすでに期限切れでオブジェクトがIDBから削除されているかどうかが影響することはありません。

より安全性を高めるため、データ保護期間は[無期限]に設定して、メディア上のデータが誤って上書きされないようにしてください。

復元時の注意点

最新のデータを復元するには、前回のフルバックアップが格納されたメディアと、それ以降に実行された増分バックアップが格納されたメディアが必要です。そのため、増分バックアップの回数が多ければ多いほ

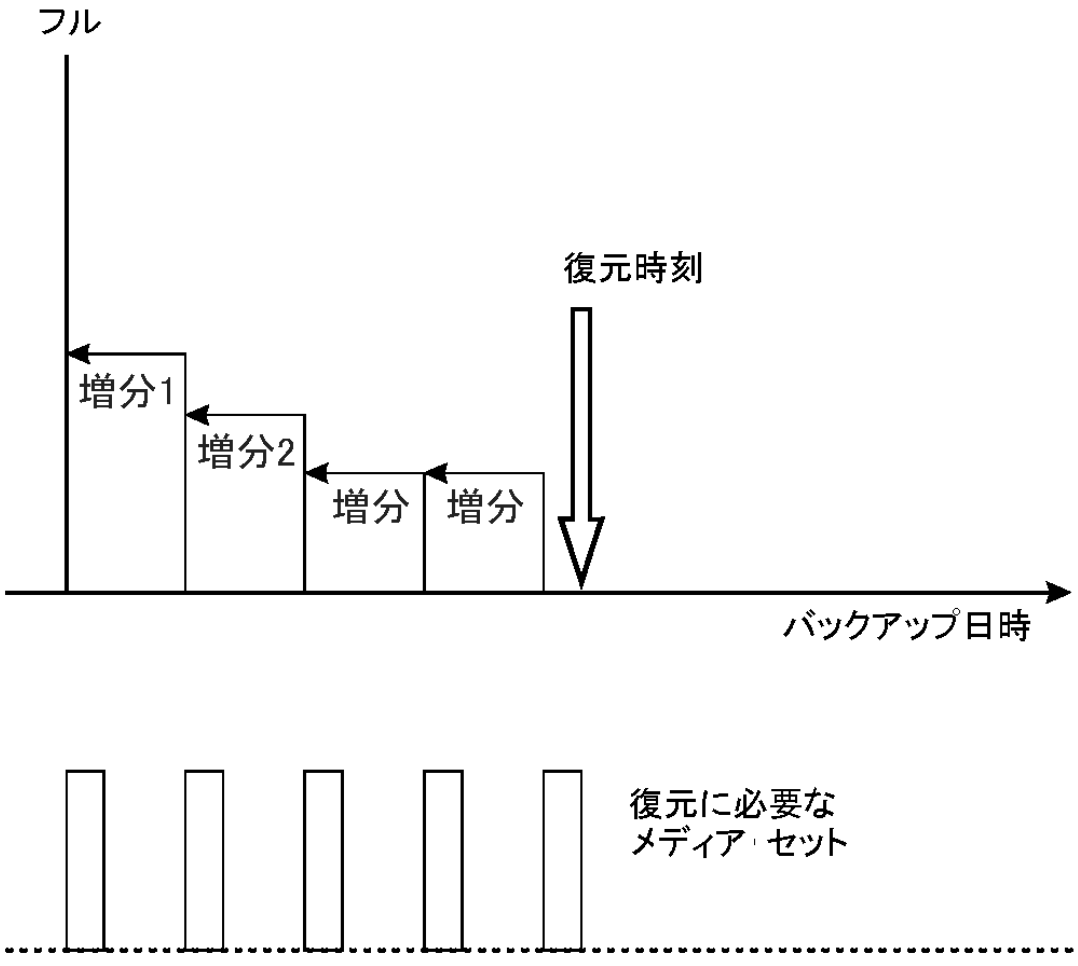
ど、必要となるメディアの数も増加します。スタンドアロンデバイスを使用している場合には、この点が問題となって、復元処理に時間がかかってしまいます。

簡易および複数レベルの増分バックアップからの復元時に必要となるメディア、下に示す簡易バックアップおよび複数レベルの増分バックアップを実行した場合、フルバックアップとそれ以降に作成された増分バックアップの、合計5つの**メディアセット**にアクセスする必要があります。この場合、メディア上で必要とされるスペースは少なくなりますが、復元作業は複雑になります。必要となる一連のメディアセットは、**復元チェーン**とも呼ばれます。

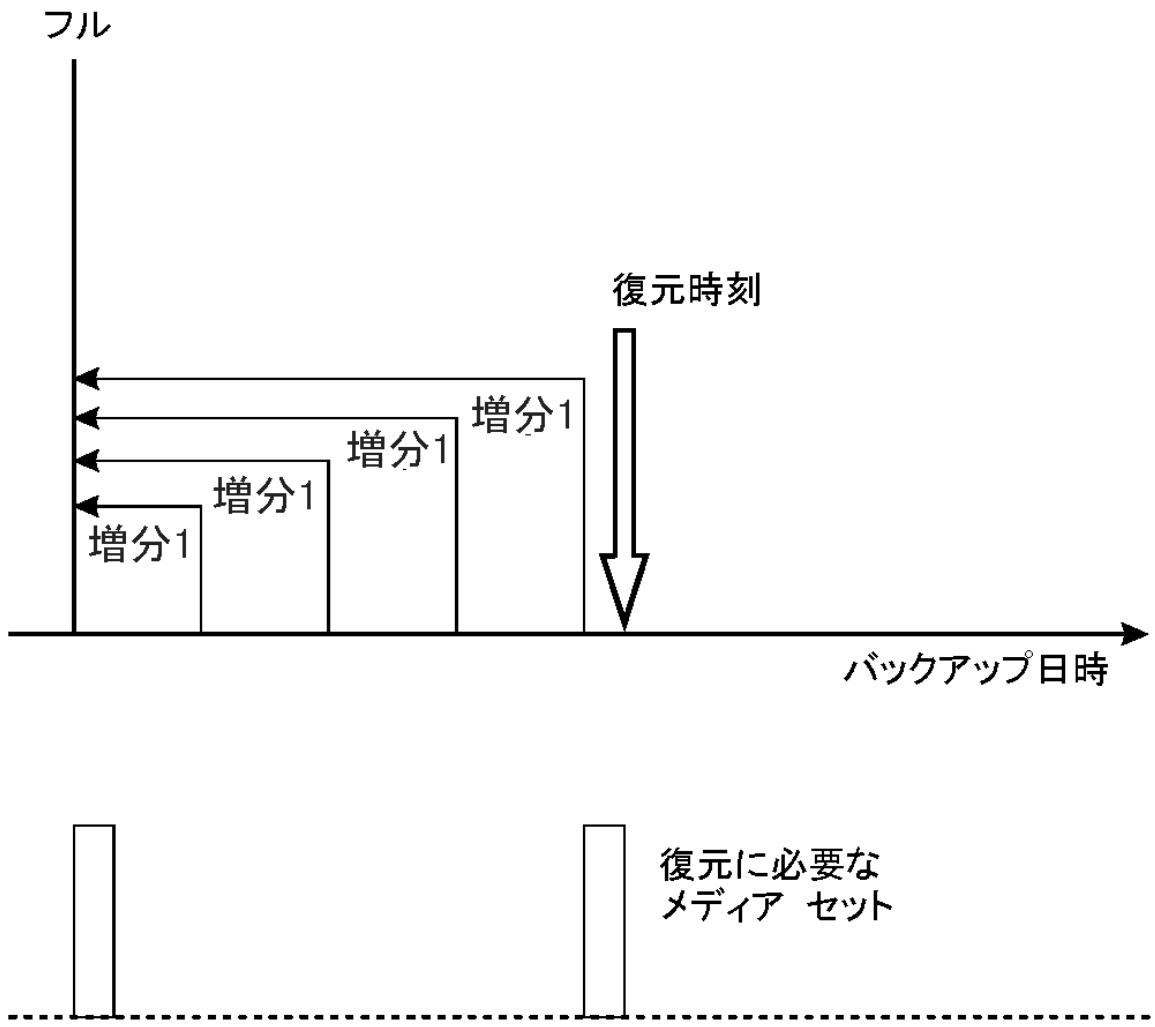
> **ヒント:**
> Data Protectorの**[増分のみ追加可能]**オプションを使うと、フルバックアップと、同じバックアップ仕様内の増分バックアップが同一のメディアセット内に保存されます。

増分バックアップ概念の別の共通な用途については、複数レベルの増分バックアップからの復元時に必要となるメディア、下に示されています。ここでは、メディアに必要な容量は若干大きくなります。この方法では、特定の時点までの復元処理を行うのに、2つのメディアセットしか必要ありません。またこの復元方法の場合には、復元する状態の時刻を変更しない限り、以前に作成された増分1メディアセットに依存する必要がない点に注目してください。

簡易および複数レベルの増分バックアップからの復元時に必要となるメディア



複数レベルの増分バックアップからの復元時に必要となるメディア



復元に必要なフルバックアップと増分バックアップが、必要時にすべて揃っているようにするには、データ保護を適切に設定しなければならない点に注意してください。データ保護が適切に設定されていないと、復元チェーンが切れる可能性があります。

バックアップデータおよびバックアップデータに関する情報の保存

Data Protectorでは、バックアップデータをメディア上に保存しておく期間(データ保護期間)、バックアップデータに関する情報をIDB上に保存しておく期間(カタログ保護期間)、IDBに保存する情報のレベル(ロギングレベル)をそれぞれ指定できます。

バックアップデータ自体に対する保護と、IDBに保存されるデータに関するバックアップ情報に対する保護は、個別に設定できます。メディアのコピー時には、作成するコピーに対して元のメディアとは異なる保護期間を設定できます。

Data Protector内部データベース

復元の性能を考えるうえで、復元作業に必要なメディアをいかにすばやく見つけられるかも重要なポイントになります。メディアに関する情報は、デフォルトではIDBに保存され、復元の性能を向上するとともに、復元するファイルやディレクトリを簡単にブラウズできるようになっています。ただし、すべてのバックアップにおけるすべてのファイル名をIDBに長期間保存すると、IDBのサイズがあまりにも大きくなってしまう可能性があります。

Data Protectorでは、データ保護期間とは独立した形でカタログ保護期間を指定できるため、IDBサイズの拡張と、復元の容易さのバランスを考えた設定が可能です。たとえば、バックアップ後4週間は簡単かつ高速に復元処理を行えるようにカタログ保護期間を4週間に設定しておきます。それ以降、データ保護の有効期限が切れるまでの1年間程度は、多少手間はかかるにしても、復元処理自体の実行は可能になります。このようにエ夫することで、IDB上のスペースを削減できます。

データ保護

データ保護とは

Data Protectorでは、メディア上のデータがData Protectorにより上書きされるのを防止するためのデータ保護期間を指定できます。保護期間は、絶対日付または相対日付のどちらでも指定できます。

Data Protectorでは、さまざまな場所でデータ保護の設定を行うことができます。詳細については、『*HPE Data Protectorヘルプ*』のキーワード「データ保護」で表示される内容を参照してください。

バックアップの構成時に、バックアップオプション**[データ保護]**を変更しなければ、バックアップデータは永久に保護されます。そのためこのオプションを変更しなければ、バックアップ用メディアの数が増え続けることに注意してください。

カタログ保護

Data Protectorではバックアップデータに関する情報が、IDBに保存されます。IDBには、バックアップが実行される度に、そのバックアップデータに関する情報が書き込まれるため、バックアップの数とサイズが増えるにつれて、IDBのサイズも拡張していきます。カタログ保護により、ユーザーが復元時にデータに関すDataProtectorる詳細情報をブラウズできる期間を設定できます。カタログ保護期限が切れると、それ以降に実行されるバックアップで、(メディアData Protector上のデータではなく)IDB内の詳細情報が上書きされます。

保護期間は、絶対日付または相対日付のどちらでも指定できます。

バックアップの構成時に、バックアップオプション**[カタログ保護]**を変更しなければ、バックアップデータに関する情報の保護期間は、そのデータ自体の保護期間と同じになります。そのためこのオプションを変更しなければ、バックアップが実行されて新しい情報が追加される度に、IDBのサイズも拡張し続けることに注意してください。

カタログ保護設定がIDBサイズの増大とパフォーマンスに及ぼす影響の詳細については、『*HPE Data Protectorヘルプ*』を参照してください。

ロギングレベル

ロギングレベルでは、バックアップ時にIDBに書き込むファイルやディレクトリについての詳細情報の量を決定します。データ自体の復元は、バックアップ時のロギングレベルにかかわらずいつでも可能です。

Data Protectorでは、バックアップするファイルやディレクトリについて、どの程度の詳細情報をIDBに書き込むかを4つのレベルで制御できます。詳細については、IDBの主要な調整可能パラメーターとしてのロギングレベル、ページ 174を参照してください。

復元するファイルのブラウズ

IDB内には、バックアップデータに関する情報が保存されています。Data Protectorユーザーインターフェイスを使用すると、この情報を利用して、復元するファイルのブラウズや選択、復元処理の開始などを実行できます。この情報が失われていても、必要なデータ自体がメディア上にまだ保存されている場合には、データの復元は可能ですが、この場合は、どのメディアを使用して、何を復元するのかを(正確なファイル名など)、ユーザー自身が的確に把握していなければなりません。

IDBは、メディア上の実データが上書きされない期間に関する情報も保持しています。

データ保護、カタログ保護、ロギングレベルに対するポリシーは、復元時におけるデータの可用性とアクセス時間に影響を与えます。

ファイルのブラウズとすばやい復元が可能な場合

ファイルをすばやく復元するためには、メディア上に保護されたデータが存在し、かつバックアップデータに関するカタログ情報がデータベース内に存在していなければなりません。カタログ情報がある場合は、Data Protectorユーザーインターフェイスを使用して、復元するファイルのブラウズや選択、復元処理の開始などを実行できるため、Data Protectorにより、バックアップメディアに格納されているデータをすばやく見つけ出すことができます。

ファイルのブラウズはできないが復元は可能な場合

カタログ保護の有効期限は切れているが、データ保護はまだ有効な場合には、Data Protectorのユーザーインターフェイスを使ってファイルをブラウズすることはできませんが、必要なファイルの名前と格納先メディアがわかっていれば、データの復元は可能です。ただしData Protectorでは、必要なデータがどのメディアに保存されているのかがわからないため、復元処理にかかる時間はそれだけ長くなってしまいます。最初にメディア内の情報をIDBにインポートし直して、バックアップデータに関するカタログ情報を再構築してから、復元操作を開始することも可能です。

新しいデータによるバックアップファイルの上書き

データ保護の有効期限が切れると、以降のバックアップ実行時に、メディア上のデータが上書きされます。上書きされる前であれば、そのメディアを使った復元処理はまだ可能です。

> **ヒント：**
> データ保護の有効期限には、そのデータを本当に保存しておく必要がある期間を指定してくださ

い(1年など)。

一方、カタログ保護の有効期限には、バックアップファイルのブラウズや選択、復元処理の開始などを、Data Protectorユーザーインターフェイスを使って容易に実行できる状態に保っておく必要がある期間を指定してください。

セルからのメディアのエクスポート

Data Protectorセルからメディアをエクスポートすると、そのメディアに保存されているバックアップデータに関するすべての情報と、メディア自体に関する情報が、IDBから削除されます。エクスポートされたメディアについては、Data Protectorユーザーインターフェイスを使用して、ファイルのブラウズや選択、復元処理の開始などを実行することはできなくなります。ユーザーインターフェイスを使った処理を可能にするには、目的のメディアをData Protectorセル内に再度読み込む(または新たに読み込む)必要があります。メディアを別のセルに移動するには、この処理が必要です。

メディアのエクスポート中に、メディアに関連する暗号化情報もエクスポートされ、.csvファイルとしてエクスポートディレクトリに配置されます。このファイルは、再インポートまたは別のセルにインポートした後に、暗号化されたバックアップを復元可能にするために必要です。

セルへのWORMメディアのインポート

Data Protectorセルにメディアをインポートすると、そのメディアに保存されているバックアップデータに関するすべての情報と、メディア自体に関する情報が、IDBに追加されます。インポートされたメディアについては、Data Protectorユーザーインターフェイスを使用して、ファイルのブラウズや選択、復元処理などを実行することができます。データ保護の期限がすでに切れたメディアをData Protectorセルにインポートする場合、以降のバックアップ実行時に、メディア上のデータは上書きされます。

WORMメディアの場合、メディア上でのデータの上書きは許可されず、メディアは追加不可能になります。Data ProtectorでWORMメディアにデータを追加するには、データ保護期間を新しいデータがメディアに書き込まれる日付よりも後に設定し、既存データが上書きされないようにします。

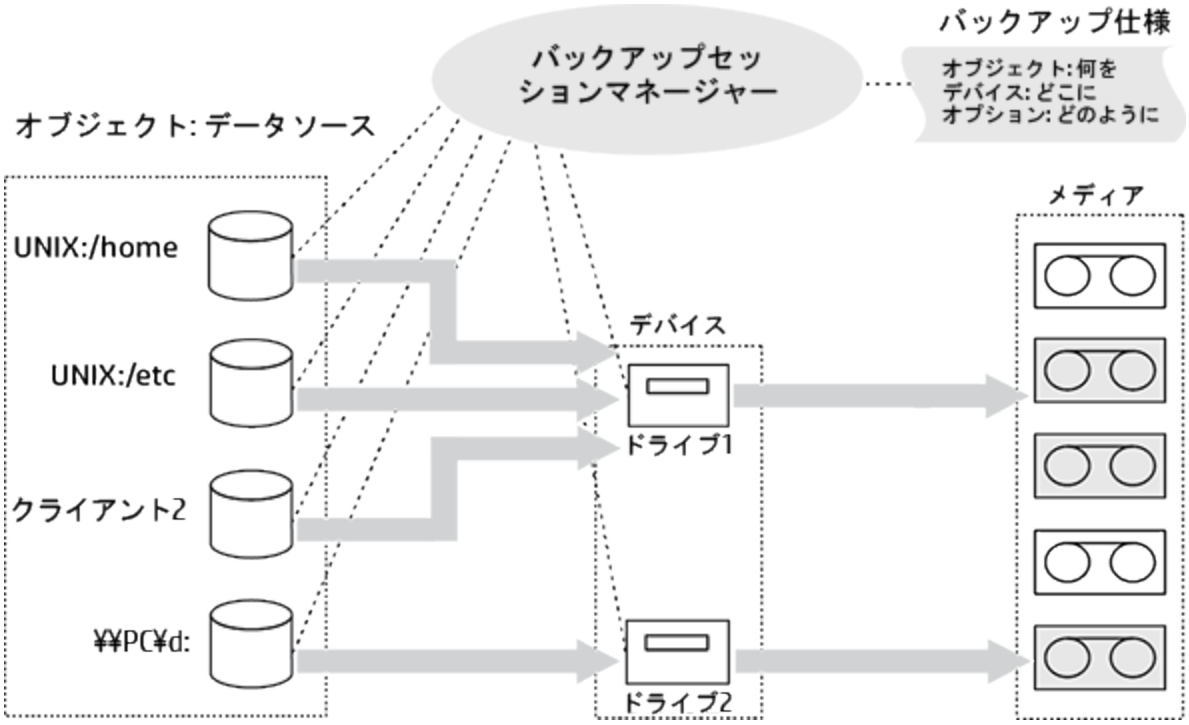
データのバックアップ

データのバックアップ手順は、以下のとおりです(場合によっては、一部の手順のみが必要となります)。

- どのクライアントシステムからどのファイルをバックアップするのかを選択します(ソースデータの選択)。
- どこにバックアップするのかを選択します(バックアップ先の選択)。
- 同一データを別のメディアセットにも書き込むかどうかを選択します(ミラー作成の選択)。
- バックアップ方法を選択します(バックアップオプションの選択)。
- 自動処理が行われるよう、バックアップをスケジュール設定します。

バックアップ仕様では、これらの項目をすべて指定できます。

バックアップセッション



指定した時間になると、バックアップ仕様に基づいてバックアップセッションがData Protectorによって開始されます。ソースデータはバックアップ対象オブジェクト(UNIXシステム上のファイルシステム、またはWindowsシステム上のディスクドライブ)を一覧形式で指定したものであり、バックアップ先は指定した(テープ)デバイスとなります。バックアップセッションの実行時には、指定したオブジェクトがData Protectorによって読み取られ、ネットワークを介してデータが転送され、デバイス内のメディアに書き込まれます。バックアップ仕様では、使用するデバイスも指定します。また、メディアプールも指定できます。メディアプールが指定されなかった場合、デフォルトメディアプールが使用されます。バックアップ仕様では、1つのディスクをスタンドアロンのDDSドライブにバックアップするといった単純な設定もできれば、40台の大規模サーバーを、8台のドライブを搭載したサイロテープライブラリにバックアップするといった複雑な設定も可能です。

バックアップ仕様の作成

バックアップ仕様を作成しておくと、使用するデバイス、バックアップタイプ、バックアップセッションオプションなど、バックアップ上の特徴が共通する複数のオブジェクトを、ひとつのグループにまとめて処理することができます。

バックアップ仕様の構成には、Data Protectorユーザーインターフェイスを使用します。バックアップ仕様内では、バックアップする対象や作成するミラーの数、バックアップに使用するメディアやデバイスを指定する他に、特定のバックアップ動作を指定することも可能です。Data Protectorには、ほとんどの場合に適合するデフォルトの動作が用意されています。Data Protectorバックアップオプションを使用すると、バックアップ動作をカスタマイズできます。

Data Protectorでは、対象となるクライアントに接続されているすべてのディスクをバックアップ時に検出して、バックアップすることも可能です。ディスクディスカバリバックアップ、ページ 188を参照してください。

注意:
バックアップ仕様の変更は、Data Protector**のGUIまたはCLIコマンド**でのみ可能です。バックアップ仕様ファイルの手動での変更はサポートされていません。

バックアップオブジェクトの選択

Data Protectorでは、同一ディスクボリューム(論理ディスクまたはマウントポイント)上で選択されたすべてのバックアップ対象を含むバックアップ単位を、**バックアップオブジェクト**と呼びます。バックアップ対象には、任意の数のファイルやディレクトリ、または、ディスク全体あるいはマウントポイント全体を選択できます。また、バックアップオブジェクトはデータベースエンティティまたはディスクイメージの場合もあります。

バックアップオブジェクトは以下のように定義されます。

- クライアント名: バックアップオブジェクトが存在するData Protectorクライアントのホスト名です。
- マウントポイント: バックアップオブジェクトの存在するクライアント上のディレクトリ構造内で、そのバックアップオブジェクトへアクセスするためのポイントです(Windows上のドライブまたはUNIX上のマウントポイント)。
- 説明: 同一のクライアント名とマウントポイントを持つバックアップオブジェクトを一意に定義します。
- 種類: バックアップオブジェクトの種類(たとえば、ファイルシステムやOracleなど)。

バックアップオブジェクトの定義方法を知っておくことは、増分バックアップの仕組みを理解するうえで大切です。たとえば、バックアップオブジェクトの説明を変更すると、そのオブジェクトは新しいバックアップオブジェクトであるとみなされて、増分バックアップではなくフルバックアップが自動的に実行されます。

バックアップオプションの例

個々のバックアップオブジェクトに対するバックアップ動作をカスタマイズするには、各オブジェクトに対してバックアップオプションを指定します。指定できるバックアップオプションの例を、以下に示します。

- IDBに記録するログ情報のレベル

  Data Protectorでは、ファイルやディレクトリについてどの程度の詳細情報をIDBに記録するかを4つのレベルから選択できます。

  - すべてログに記録
  - ファイルレベルまでログに記録
  - ディレクトリレベルまでログに記録
  - 記録しない

  保存する詳細情報のレベルを変更すると、復元時にData Protectorのユーザーインターフェイスを使ってファイルをブラウズする機能が影響を受けることに注意してください。ロギングレベルの詳細については、IDBの主要な調整可能パラメーターとしてのロギングレベル、ページ 174を参照してください。
- 自動負荷調整

  指定リストに基づくデバイスの動的割り当て。詳細については、負荷調整の仕組み、ページ 107を参照してください。

  Data Protectorにより、どのオブジェクト(ディスク)をどのデバイスでバックアップするかが動的に決定されます。
- 実行前スクリプトと実行後スクリプト

一貫性のあるバックアップを作成するための、クライアント側での準備作業に使用。詳細については、実行前コマンドと実行後コマンド、ページ 186を参照してください。

- データセキュリティ

  データに適用するセキュリティのレベル。

  Data Protectorは、バックアップされたデータに対して、次に示す3つのセキュリティレベルを提供します。

  - なし
  - AES 256ビット
  - 暗号化

  暗号化の詳細については、データの暗号化、ページ 49を参照してください。

バックアップから除外するディレクトリの指定や、特定のディレクトリのみのバックアップも可能です。また後から追加されたディスクもバックアップできます。このようにバックアップは自由に構成でき、動的な設定も可能です。

バックアップセッション

バックアップセッションは、データをクライアントシステムからメディアにバックアップするプロセスです。バックアップセッションは、常にCell Managerシステム上で実行されます。バックアップ処理を始めるとバックアップセッションが開始され、バックアップ仕様に基づいて処理が進められます。

バックアップセッション中は、デフォルト動作、またはData Protectorカスタマイズされた動作に基づいて、データがバックアップされます。

バックアップセッションの詳細、およびセッションの制御方法については、Data Protectorが機能する仕組み、ページ 182を参照してください。

オブジェクトミラー

オブジェクトミラーとは、バックアップセッション中に作成される、バックアップオブジェクトの追加コピーです。各オブジェクトについてミラーを作成するかどうかは、バックアップ仕様の中で定義できます。ミラーは複数個作成することもできます。オブジェクトミラーを作成すると、バックアップのフォールトトレランスが向上し、複数の場所に分けてのボールティングも可能になります。ただし、バックアップセッション中にオブジェクトミラーを作成すると、バックアップにかかる時間はそれだけ長くなります。

詳細については、オブジェクトのミラーリング、ページ 94を参照してください。

メディアセット

バックアップセッションが終了すると、メディア、またはメディアセット上にバックアップデータが生成されています。各バックアップセッションで作成されるメディアの総数は、バックアップ中にオブジェクトミラーを作成するかどうかによって異なります。プールの使用状況によっては、複数のセッションで同一のメディアを共有することも可能です。データを復元するときには、復元元となるメディアがわかっている必要があります。Data Protectorではこの情報をカタログデータベースに保存しています。

バックアップの種類とバックアップのスケジュール設定

スケジュール設定ポリシーでは、バックアップの開始時点と種類(フルまたは増分)が定義されます。フルバックアップおよび増分バックアップの違いを考慮してください。フルバックアップと増分バックアップの比較、ページ 61を参照してください。

スケジュールバックアップを構成するときには、フルバックアップと増分バックアップを組み合わせることができます。たとえば、日曜日にフルバックアップを実行し、平日に毎日増分バックアップを行うことができます。大量データのバックアップを行いながらも、フルバックアップの大量データによるピークを避けるためには、時間差実行方式を採用します。フルバックアップの時間差実行、次のページを参照してください。

スケジュール設定、バックアップ構成、およびセッション

バックアップ構成

バックアップをスケジュール設定すると、そのバックアップ仕様内に指定されているすべてのオブジェクトが、スケジュールされたそのバックアップセッション内でバックアップされます。

単独で、または定期的に実行されるようにスケジュールされたバックアップでは、**[バックアップの種類]**(フルまたは増分)、**[ネットワーク負荷]**、**[バックアップ保護]**の各オプションを指定できます。また、スプリットミラーバックアップまたはスナップショットバックアップで、ディスクへのZDBまたはディスク+テープへのZDB(インスタントリカバリに対応)を実行する場合は、**スプリットミラー/スナップショットバックアップ**オプションを指定します。ディスクへのZDBでは、バックアップの種類は無視され、必ずフルバックアップが実行されます。

1つのバックアップ仕様内で、ディスクへのZDBとディスク+テープへのZDBの処理を両方ともスケジュール設定したり、単独のまたは定期的に実行される個々のスケジュール形式のバックアップに対して、それぞれ異なるデータ保護期間を指定したりすることも可能です。

スケジューラの詳細については、『*HPE Data Protector管理者ガイド*』の「*スケジューラ*」を参照してください。

バックアップセッション

バックアップセッションが開始されると、Data Protectorにより、デバイスなどの必要な全リソースの割り当てが試みられます。必要最小限のリソースが使用可能になるまで、セッションは待ち行列に入れられます。Data Protectorにより、タイムアウトと呼ばれる特別な時間内に、リソースの割り当てが試行されます。ユーザーは、タイムアウトの時間を設定することができます。タイムアウトになってもリソースがまだ使用できない場合は、そのセッションは中止されます。

バックアップ性能の最適化

Cell Managerの負荷を最適化するため、Data Protectorでは、デフォルトでは5つのバックアップセッションが同時に開始されます。これ以上のセッションが同時にスケジュール設定された場合には、処理できないセッションは待ち行列に入れられて、他のセッションの終了後に開始されます。

スケジュール設定のヒントとテクニック

バックアップ世代、データ保護、およびカタログ保護の概念については、フルバックアップ、増分バックアップ、合成バックアップ、ページ 61およびバックアップデータおよびバックアップデータに関する情報の保存、ページ

73の各項目を参照してください。

以下では、これらの概念について、バックアップスケジュール例を使ってわかりやすく説明するとともに、効率的なスケジュール設定のためのヒントを示します。

バックアップに適した時間帯

通常、バックアップ処理は、ユーザー活動の最も少ない時間帯(通常は夜間)に実行されるようスケジュール設定します。フルバックアップは時間がかかるため、週末に実行するようスケジュールを設定してください。

またフルバックアップは、クライアントごと(バックアップ仕様ごと)に、日を変えて実行する方がよい場合もあります。詳細についてはフルバックアップの時間差実行、下を参照してください。

> **注:**
> Data Protectorでは、デバイス使用率の観点から捕らえた、バックアップ可能な時間帯を示すレポートを生成できます。このレポートを使用すると、目的のデバイスが、既存のバックアップにより占有される可能性が低い時間帯を選択できます。

フルバックアップの時間差実行

全システムのフルバックアップを同じ日に実行すると、ネットワーク負荷やバックアップ可能な時間帯に関して、問題が発生する可能性があります。この問題を防ぐには、フルバックアップに対して「時間差実行方式」を採用します。

時間差実行方式

	月	火	水	…
system_grp_a	フル	増分1	増分1	…
system_grp_b	増分1	フル	増分1	…
system_grp_c	増分1	増分1	フル	…

復元のための最適化

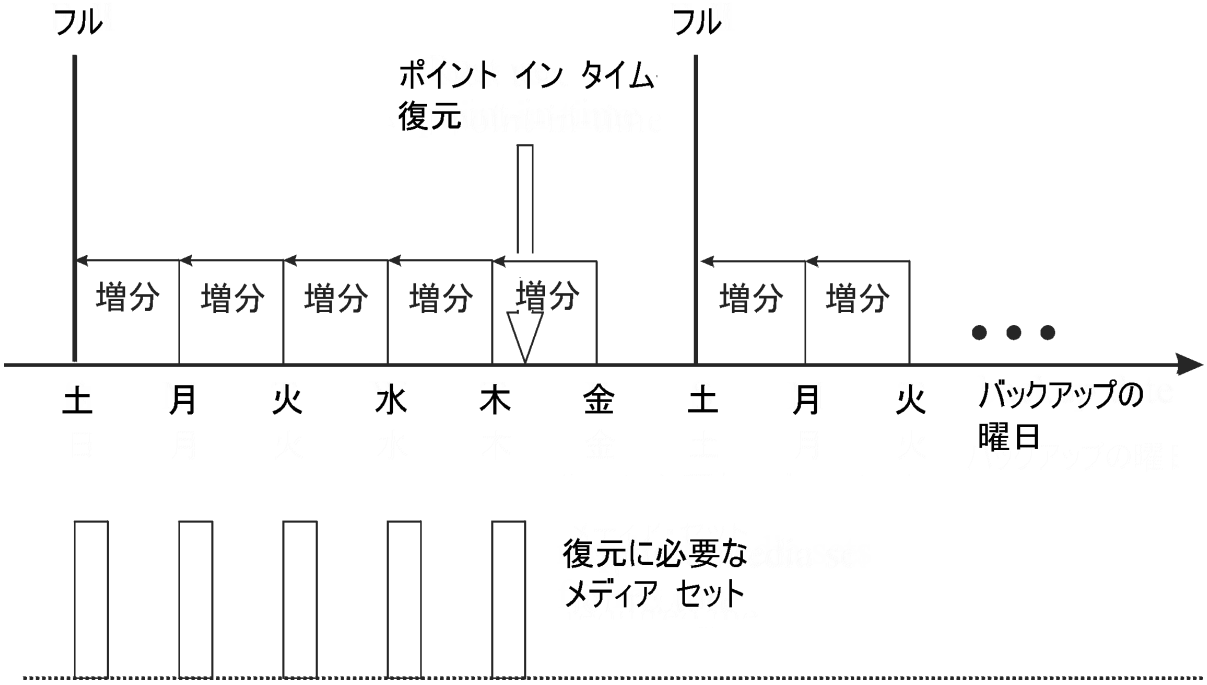
スケジュール設定ポリシーと、フルバックアップおよび増分バックアップをどのように組み合わせるかは、対象となるデータの復元処理にかかる時間に大きく影響します。以下に3つの例を使って、この点を説明します。

特定の時点への復元を行うには、ベースとなるフルバックアップと、目的の時点までに行われたすべての増分バックアップが必要になります。通常、フルバックアップと増分バックアップは、同一メディア上には格納されていないため、フルバックアップと各増分バックアップが格納されたメディアをそれぞれ用意しなければなりません。Data Protectorにおけるバックアップ用メディアの選択方法については、バックアップ用メディアの選択、ページ 158を参照してください。

例1

フルバックアップと1日1回の簡易増分バックアップ、下は、フルバックアップと簡易増分バックアップに基づくスケジュール設定ポリシーを示したものです。

フルバックアップと1日1回の簡易増分バックアップ

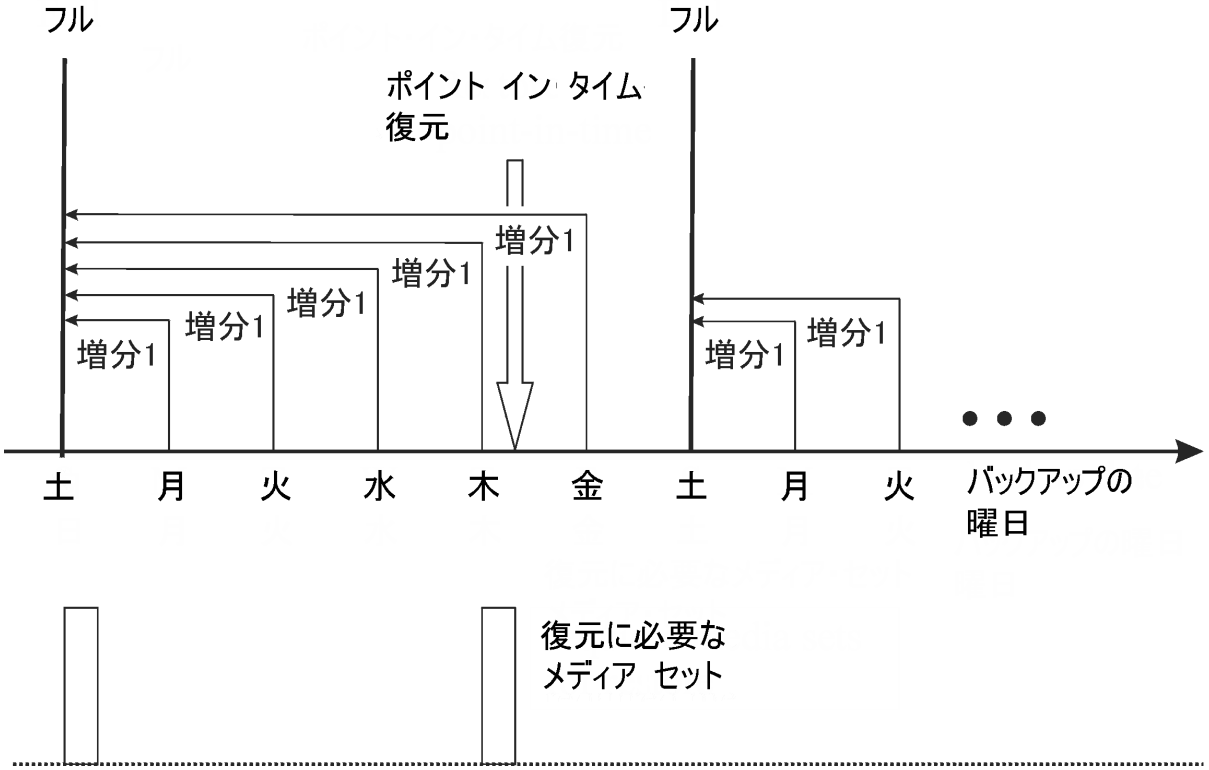


このスケジュールポリシーでは、前日以降の変更だけをバックアップするので、バックアップに必要になるメディア容量と時間が節減されます。ただし、たとえば木曜日のバックアップからファイルを復元するような場合には、フルバックアップと木曜日までの増分バックアップが必要になるため、合計5つのメディアセットが必要です。このため、復元の手順が複雑になり、時間がかかります。

例2

フルバックアップと1日1回のレベル1増分バックアップ、次のページは、フルバックアップとレベル1増分バックアップに基づくスケジュール設定ポリシーを示したものです。

フルバックアップと1日1回のレベル1増分バックアップ

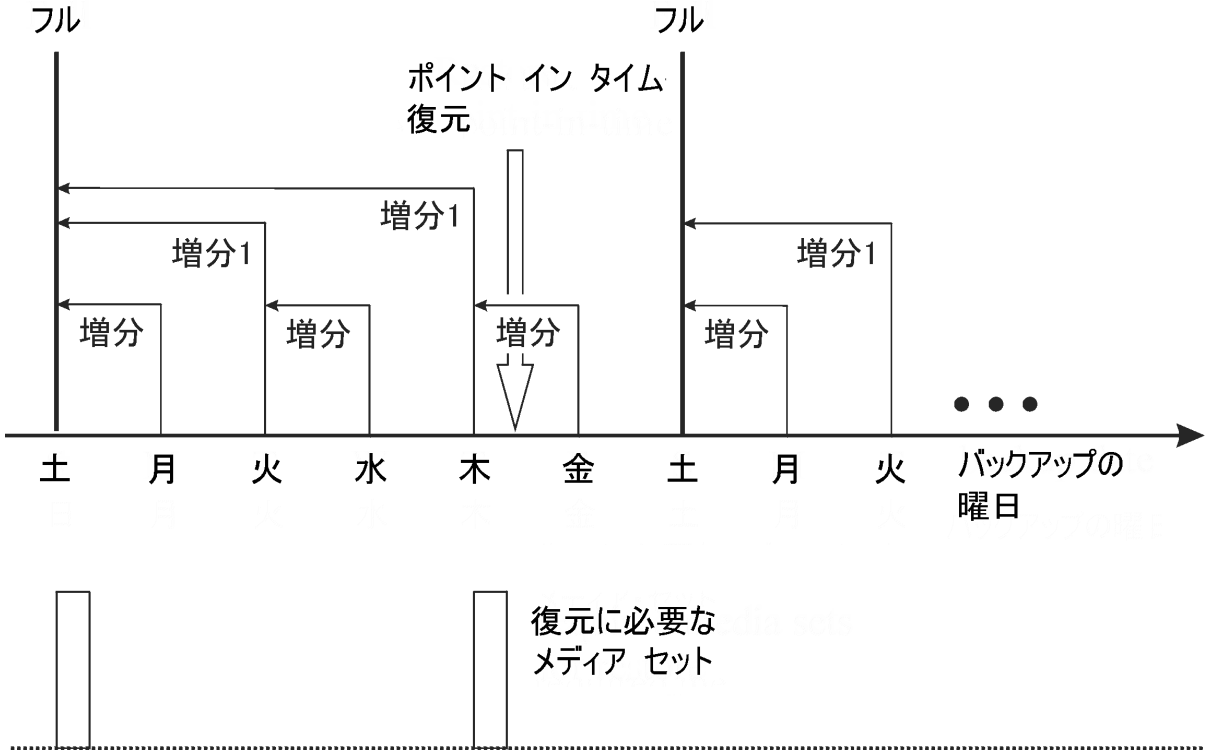


このポリシーでは、毎日、前回のフルバックアップ以降に更新されたデータがバックアップされるため、バックアップに必要なメディアスペースと時間は多少増加します。木曜日のバックアップからファイルを復元するときに必要になるメディアは、前回のフルバックアップと木曜日の増分1バックアップのメディア(つまり2セットのメディア)のみです。これにより、復元が大幅に簡略化され、時間も大きく短縮されます。

例3

環境と要件によっては、前述の2つの方法を組み合わせた形が最適である場合も考えられます。たとえば、以下に示すスケジュール設定ポリシーを設定できます。

フルバックアップと2通りの増分バックアップ



このポリシーでは、週末には変更が多くないという事実を考慮します。データのバックアップに簡易増分バックアップと増分1(差分)バックアップを組み合わせることで、バックアップのパフォーマンスを最適化しています。木曜日のバックアップからファイルを復元するときに必要になるメディアは、前回のフルバックアップと2番目の増分1バックアップのメディア(つまり2セットのメディア)のみです。

操作の自動化や無人化

バックアッププロセスに関する操作やオペレーターの作業を軽減するために、Data Protectorでは、営業時間外に無人バックアップ、つまり自動バックアップを実行できます。以下では、スケジュール設定ポリシーの設定方法や、設定した方針がバックアップ動作に与える影響について説明するほか、スケジュール設定ポリシーの設定例もいくつか紹介しています。ここでは、単一のバックアップを無人状態で実行する方法ではなく、主として数日から数週間の長期にわたって、無人状態でバックアップを実行する方法について説明します。

無人バックアップの注意点

Data Protectorでは、バックアップを簡単にスケジュール設定できます。スケジュール設定ポリシーをどのように設定すれば効率がよくなるかは、それぞれの環境によって異なるため、最適なスケジュール設定ポリシーを設定するには、以下のような事前調査が必要になります。

- システム使用率とユーザー活動が最小になるのはいつか。

  通常は夜であり、ほとんどのバックアップは夜間に実行するようスケジュールされます。Data Protectorでは、バックアップに使用するデバイスについてのレポートを作成できます。

- どのようなタイプのデータが存在しており、各データのバックアップはどれくらいの頻度で行う必要があるか。

  ユーザーファイル、取引情報、データベースのような、頻繁に更新され、かつ企業にとって重要な情報については、規則的にバックアップしなければなりません。一方プログラムファイルのようなあまり変化しない、システム固有のデータについては、それほど頻繁にバックアップする必要はありません。
- 復元処理の容易性は、どの程度重要か。

  フルバックアップおよび増分バックアップのスケジュール方法によっては、最新バージョンのファイルを復元するときに、フルバックアップが格納されたメディアと増分バックアップが格納されたメディアの両方が必要になります。この場合、自動ライブラリデバイスを持っていなければ、復元処理に時間がかかったり、手動によるメディア交換が必要になる可能性があります。
- バックアップするデータの量はどの程度か。

  フルバックアップは増分バックアップよりも時間がかかります。またー般にバックアップ処理は、限られた時間枠内で実行する必要があります。
- どれくらいの量のメディアが必要か。

  メディア交換ポリシーを決定します。メディア交換ポリシーの実装、ページ 155を参照してください。ここでは、対象ライブラリ内に十分な数のメディアを用意しておくことにより、バックアップ時に手動でメディア交換を行わずに済ませる方法について説明しています。
- どのようにマウントプロンプトに対応するか。

  ライブラリを使用するかどうかを決定します。ライブラリを使用すると、自動処理が可能となります。これは、Data Protectorから、すべてのメディア、または大部分のメディアに対するアクセスが可能となり、メディアを手動で処理する必要がほとんどなくなるためです。データ量が非常に多く、1台のライブラリでは対処しきれない場合は、ライブラリの追加を検討する必要があります。詳細については、大容量ライブラリ、ページ 114を参照してください。
- デバイスが使用できない場合の対応をどうするか。

  バックアップ仕様の作成時には、動的な負荷調整またはデバイスチェーンを指定して、複数のデバイスを使用できるようにしておいてください。こうすることで、あるデバイスがオンになっていなかったり、デバイスが接続されているシステムが作動していないなどの原因で、バックアップに失敗することがなくなります。
- すべてのデータのバックアップにはどれくらいの時間が必要か。

  バックアップ作業は、ネットワークの使用率が低く、ユーザーがシステムを使用しない時間帯に実行しなければなりません。そのため、バックアップのスケジュール設定を適切に行って、バックアップによるネットワーク負荷を分散させ、バックアップセッションの効率を最大化することが大切になります。場合によっては、時間差実行方式の採用も検討してください。

  大量データをバックアップする必要があり、バックアップウィンドウに問題が表示される場合、ディスクベースデバイスへのバックアップと、合成バックアップやディスクステージングなどのアドバンストバックアップ戦略を検討してください。
- バックアップ対象の実行中のアプリケーションに対して、どのように準備するか。多くのアプリケーションでは、ファイルが開かれたままですので、バックアップの実行により、整合性のないバックアップが生成されます。

  実行前スクリプトおよび実行後スクリプトを使用して、アプリケーションの状態とバックアップ処理とを同期させることにより、この状況を防止できます。

バックアップデータの複製

バックアップデータの複製には、いくつかの利点があります。データをコピーすると、データの安全性や可用性が向上し、また運用面での利便性も高まります。

Data Protectorには、バックアップデータの複製方法として、オブジェクトコピー、オブジェクトミラー、メディアコピーが用意されています。これらの方法の主な特徴に関して、Data Protector データ重複の方法、下にまとめます。

Data Protector データ重複の方法

	オブジェクトコピー	複製	オブジェクトミラー	メディアコピー
複製の対象	1つまたは複数のバックアップ、オブジェクトコピー、オブジェクト集約セッションで作成される複数のオブジェクトバージョンの組み合せ	バックアップセッション、オブジェクトコピーセッション、またはオブジェクト集約セッションのオブジェクトセット	バックアップセッションのオブジェクトセット	メディア全体
複製のタイミング	バックアップ終了後の任意のタイミング	バックアップ終了後の任意のタイミング	バックアップ中	バックアップ終了後の任意のタイミング
ソースメディアとターゲットメディアのメディアの種類	同じでなくてよい	同じ種類のB2Dデバイスのみに複製可能	同じでなくてよい	同じでなければならない
ソースメディアとターゲットメディアのサイズ	同じでなくてよい	ターゲットデバイスに重複排除済みデータ用の十分な空き領域が必要	同じでなくてよい	同じでなければならない
ターゲットメディアを追加可能かどうか	可	該当なし	可	不可[1]
作成される内容	選択したオブジェクトバージョンを含むメディア	ターゲットB2Dデバイス上に格納された同一のコピー	選択したオブジェクトバージョンを含むメディア	ソースメディアと同じメディア

[1]複製先に使用できるのは、未フォーマットのメディア、空のメディア、または保護期限の切れたメディアに限られます。操作後、ソースメディアとターゲットメディアは追加不可能になります。

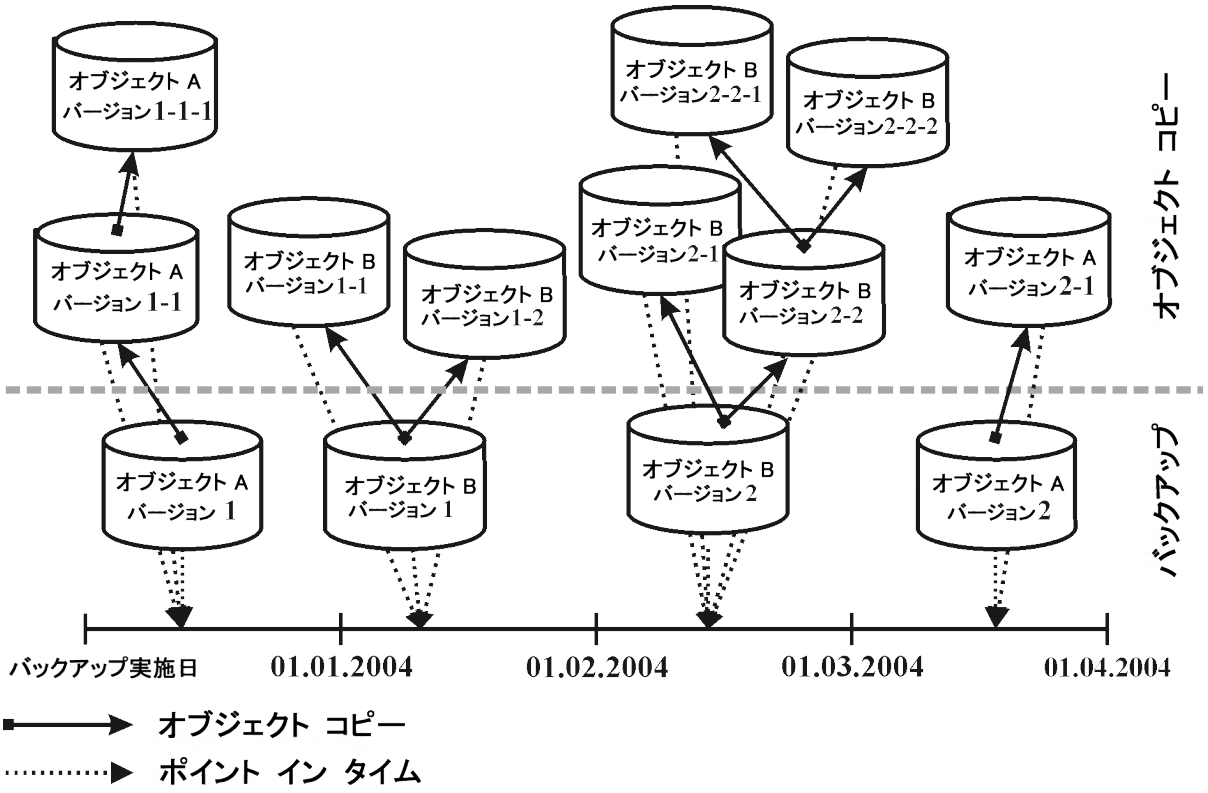
オブジェクトのコピー

Data Protectorには、選択したオブジェクトバージョンを特定のメディアセットにコピーするための、オブジェクトコピー機能が用意されています。1つまたは複数のバックアップ、オブジェクトコピー、オブジェクト集約セッションで作成される複数のオブジェクトバージョンを選択できます。オブジェクトコピーセッションでは、コピー元メディアから読み取られData Protectorたデータが転送されて、コピー先メディアに書き込まれます。

オブジェクトコピーセッションの結果、指定したオブジェクトバージョンのコピーを含んだメディアセットが作成されます。

オブジェクトコピーの概念、下は、特定の日時にバックアップしたデータが、その後にどのようにコピーされるかを示しています。この図に示すように、バックアップデータが格納されているメディアから任意のバックアップオブジェクトをコピーすることも、また、オブジェクトコピーが格納されているメディアから任意のバックアップオブジェクトをさらにコピーすることも可能です。

オブジェクトコピーの概念



この図に示す例では、オブジェクトAのバックアップにより1つのオブジェクトバージョン(バージョン1)が作成され、このオブジェクトバージョンの追加コピーが2つ作成されています。バージョン1-1はバックアップにより作成されたオブジェクトバージョンをコピーしたもので、バージョン1-1-1はオブジェクトバージョンのコピーをコピーしたものです。これら3つのオブジェクトバージョンのうちどれを使用しても同じオブジェクトバージョンを復元できます。

オブジェクトコピーセッションの開始

オブジェクトコピーセッションを対話式に開始するか、またはセッションの自動開始を指定することができます。Data Protectorには、**ポストバックアップのオブジェクトコピー**と**スケジュール設定されたオブジェクトコピー**の、2種類の自動オブジェクトコピー機能があります。

ポストバックアップのオブジェクトコピー

ポストバックアップは、ポストバックアップオブジェクトコピーのサブセットであるポストコピーおよびポスト集約オブジェクトコピーと同様、自動オブジェクトコピー仕様で指定されたセッションの完了後に行われます。この場合は、その特定のバックアップセッションで作成された自動オブジェクトコピー仕様に従って、選択されているオブジェクトがコピーされます。

スケジュール設定されたオブジェクトコピー

スケジュール設定されたオブジェクトコピーは、ユーザー定義のタイミングで実行されます。さまざまなセッションからのオブジェクトを、スケジュールされた1つのオブジェクトコピーセッションにおいてコピーできます。

デバイスの選択

コピー元メディアとコピー先メディアには、別々のデバイスを使用する必要があります。あて先デバイスのブロックサイズは、ソースデバイスのブロックサイズより大きくすることができます。ただし、パフォーマンスへの影響を避けるためには、ブロックサイズが同じデバイスを用意し、それらを同じシステムまたはSAN環境に接続することをお勧めします。

オブジェクトコピーは、デフォルトで負荷調整が行われます。Data Protectorは、できる限り多くのデバイスを使用して、使用可能なデバイスを最大限有効に活用します。

ソースデバイスの選択

デフォルトで、Data Protectorは、デバイス構成内のデバイスポリシー設定に従って、オブジェクトコピー用のソースデバイスを自動的に選択します。これにより、使用可能なリソースの利用を最適化できます。元のデバイスを使用する場合に自動デバイス選択を無効にすることも、特定のデバイスを選択することも可能です。

- デバイスの自動選択(デフォルト)

  Data Protectorは使用可能なソースデバイスを自動的に使用します。このデバイスは、オブジェクトコピー用に選択され、交換された元のデバイスと同じライブラリに属し、メディアの種類(例: LTO)が同じです。

  Data Protectorは、最初にオブジェクトを書き込むために使用されたデバイス(元のデバイス)の使用を試みます。元のデバイスがオブジェクトコピー用に選択されていない場合、グローバルオプションを考慮します。最初に代替デバイスを使用するか、一斉に元のデバイスを使用できないようにするには、グローバルオプションAutomaticDeviceSelectionOrderを変更します。

  デバイスタグの指定により、デバイスをさまざまな目的でデバイスグループに分類できます。同じタグのデバイスは、互換性があるとみなされ、互いに交換可能です。使用できない元のデバイスは、同じデバイスタグを持ち、同じライブラリに属する代替デバイスに置き換えることができます。デフォルトで、デバイスタグは定義されません。

  元のデバイスが削除された場合、同じライブラリに属する、同じメディアの種類のデバイスに置き換えられます。このデバイスがオブジェクトコピー用に選択されているかどうか、デバイスタグが元のデバイスと同じであるかどうかは検査されません。

オブジェクトコピーは、バックアップ中に使用されたデバイスより少ないデバイスを使用して開始できます。

- 元のデバイスの選択

  Data Protectorは、元のデバイスをオブジェクトコピーのソースデバイスとして使用し、そのデバイスが使用できない場合には待機します。

あて先デバイスの選択

オブジェクトごとにコピー先デバイスを指定していない場合、Data Protectorはオブジェクトコピー仕様内に指定されているデバイスの中から、以下に示す優先順位に従って自動的に選択されます。

- コピー元デバイスと同じブロックサイズのデバイスが、ブロックサイズが異なるデバイスよりも優先的に選択される
- ネットワーク接続デバイスより、ローカル接続デバイスが先に選択される

各デバイスはセッションの開始時にロックされます。セッションを開始した後にデバイスをロックすることはできません。そのため、開始時に使用不能であったデバイスは、そのセッションでは使用できません。メディアエラーが発生すると、そのコピーセッション内では、エラーの発生したデバイスが回避されます。

コピー元のメディアセットの選択

コピー対象のオブジェクトバージョンが、Data Protectorのデータ複製方法で作成された複数のメディアセットに存在する場合、そのメディアセットはコピー元として使用できます。メディアの位置の優先順位を指定すると、メディアセットの選択を制御できます。

メディアを選択するプロセス全体は、復元と同じです。詳細については、メディアセットの選択、ページ 99を参照してください。

オブジェクトコピーセッションの性能

オブジェクトコピーの性能は、デバイスのブロックサイズや接続方法などの要因に影響されます。オブジェクトコピーセッションで使われる各デバイスのブロックサイズが異なっていると、セッション中にデータの再パッケージ化が必要になるため、時間とリソースが余分に消費されます。また、ネットワークを介してデータを転送すると、新たなネットワーク負荷が発生し、処理時間もそれだけ長くなります。これらの要因による影響は、処理の負荷調整を行うことで最小限に抑えることができます。

オブジェクトコピーを使う理由

バックアップ、コピー、または集約されたデータの追加コピーは、以下のような目的で作成されます。

- ボールティング

  バックアップ、コピー、または集約されたオブジェクトのコピーを作成し、それらを複数の場所に保管できます。

- メディアの解放

  メディア上の保護されたオブジェクトバージョンだけを保管するために、保護されたオブジェクトバージョンをコピーし、メディアを上書きできるようにしておくことができます。

- メディアの逆多重化

  オブジェクトをコピーして、インターリーブされたデータを削減できます。

- 復元チェーンの集約

復元に必要なすべてのオブジェクトバージョンを1つのメディアセットにコピーできます。

- 別の種類のメディアへの移動
  異なる種類のメディアにバックアップをコピーできます。
- 拡張バックアップの概念のサポート
  ディスクステージングなどのバックアップ概念を使用できます。

ボールティング

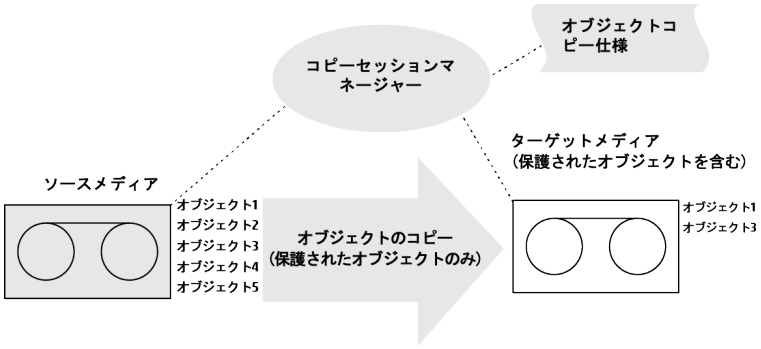
ボールティングはメディアを安全な場所に保管するプロセスを指します。この保管場所はボールトと呼ばれ、この中にメディアが一定期間保管されます。詳細については、ボールティング、ページ 162を参照してください。

復元が必要になった場合に備えて、バックアップデータのコピーは現場に保管することをお勧めします。追加コピーの作成には、それぞれの要件に合わせて、オブジェクトコピー、オブジェクトミラー、またはメディアコピーのいずれかの機能を使用してください。

メディアの解放

オブジェクトのコピー:メディアの解放メディアの解放保護されているバックアップだけを維持し、保護されていないバックアップを上書きすると、メディアスペースの消費を最小限に抑えることができます。同一メディア上に両者が混在している場合には、保護されているオブジェクトのみを新しいメディアセットにコピーし、元のメディアは上書きできるように解放します。メディアの解放、下を参照してください。

メディアの解放

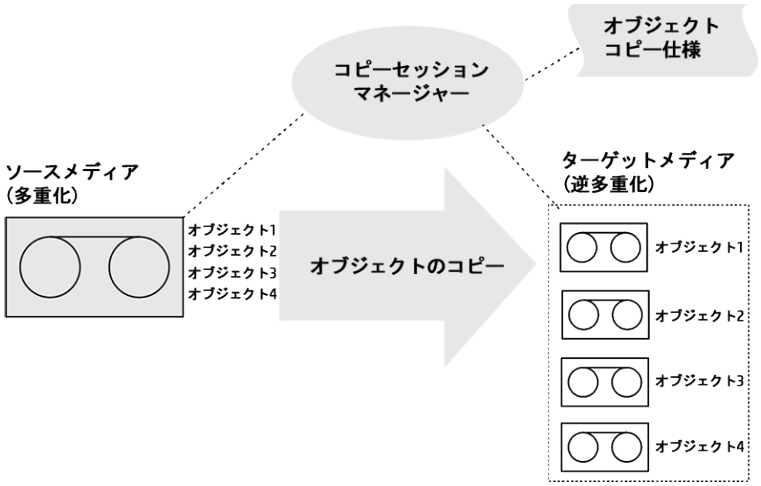


メディアの逆多重化

多重化メディアには、複数のオブジェクトをインターリーブ(断片化)したデータが含まれます。バックアップセッションのデバイス同時処理数に1より大きい値を設定すると、このように多重化されたメディアが生成されます。多重化メディアでは、バックアップデータの機密性が低下する可能性があるほか、復元にも時間がかかります。

Data Protectorには、メディアの多重化を解消するための機能が用意されています。この機能を使うと、多重化されているメディア上の各オブジェクトを、指定した複数のメディアにコピーできます。メディアの逆多重化、次のページを参照してください。

メディアの逆多重化



復元チェーンの集約

オブジェクトバージョンの復元チェーン(復元に必要なすべてのバックアップ)を新しいメディアセットにコピーできます。このようなメディアセットを使用すると、複数のメディアをロードしたり、必要なオブジェクトバージョンをシークしたりする必要がないため、すばやく、効率的に復元を実行できます。

別の種類のメディアへの移動

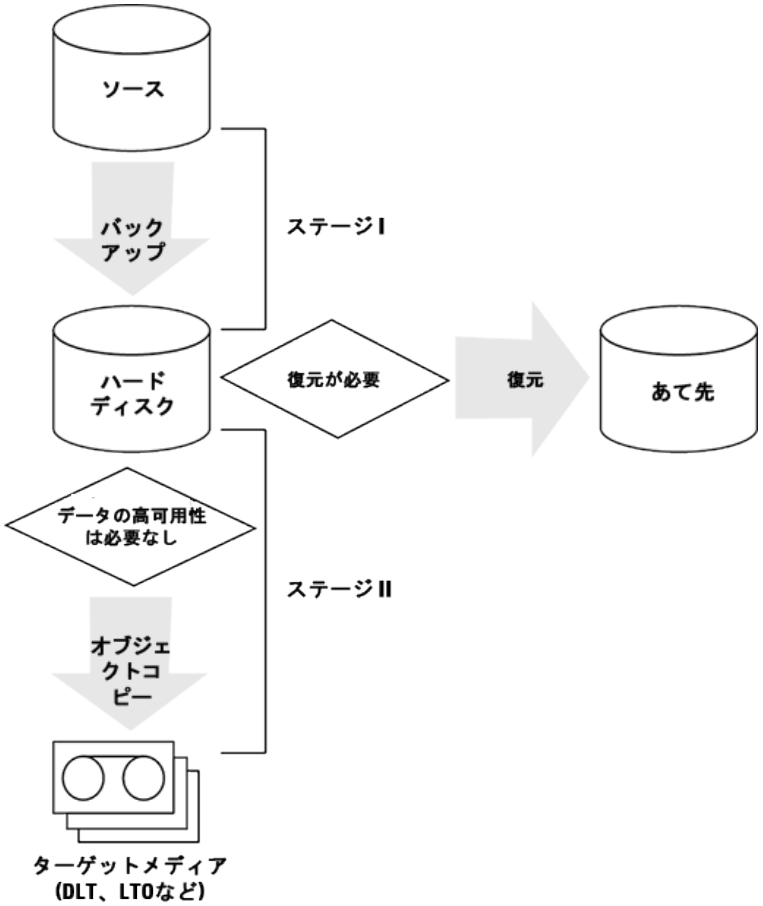
バックアップしたデータを別の種類のメディアへ移動できます。たとえば、あるオブジェクトをファイルデバイスからLTOデバイスに、またはDLTデバイスからLTOデバイスにコピーできます。

ディスクステージング

ディスクステージングの概念は、データを複数の段階(ステージ)に分けてバックアップすることにより、バックアップや復元の性能向上、バックアップデータの保管コストの削減、復元時のデータの可用性やアクセス容易性の強化を図ろうとする考え方に基づいています。

バックアップステージは、ある種類のメディアにデータをバックアップし、その後、そのデータを別の種類のメディアに移動するという操作で構成されています。最初の段階では、高性能でアクセスも容易ではあるが容量に限りがあるメディア(システムディスクなど)にデータをバックアップします。通常バックアップしたデータは、復元に使用される可能性が最も高いバックアップ後の一定期間のみ、アクセスが容易なこれらのメディア上に保管しておきます。一定の期間が経過した後、データは、オブジェクトコピー機能を使って、パフォーマンスと可用性は低いが大容量の保存用メディアに移動されます。ディスクステージングの概念、次のページを参照してください。

ディスクステージングの概念



この手順は、自動処理として実行可能です。

以下の例を考えます。この例では、標準処理としてすぐに実行でき、データセキュリティの強化にもつながる方法について簡単に説明します。ソースの保護とターゲットの保護を別々に設定するオプションを使用します。これは、最初の15日間のディスクからの高速復元機能と、さらに30日間のテープからの標準復元に対する要件です。

- 初期バックアップは、ファイルライブラリを使用するディスクに対して実行します。データとカタログの保護は、45日間の全体要件に設定します。
- 次にポストバックアップコピー操作を実行します。この操作では、初期バックアップをファイルライブラリに残した状態で、バックアップオブジェクトをテープにコピーします。テープに正常にコピーされた場合、そのコピーに対するデータとカタログの保護が45日間に設定されます。
- コピーが正常に作成されたため、ディスクバックアップの保護期間(高速復元を必要とする期間)を15日間に短縮できます。この期間を過ぎれば、より長期のセキュリティのためにテープコピーを残して、コピーを削除できます。それまでは、テープコピーにより、ディスクコピーが破損した場合のセキュリティを確保できます。

ディスクステージングを使用すると、サイズの小さい多数のオブジェクトをテープに頻繁にバックアップする必要もなくなります。このようなバックアップは、メディアが頻繁にロードまたはアンロードされるため、効率がよくありません。ディスクステージングを使用すると、バックアップ時間を短縮でき、メディアの劣化を防止できます。

複製

Data Protectorの複製機能では、Media Agentを介してデータを転送することなく、複製に対応した2つのディスクへのバックアップ(B2D)デバイス間でオブジェクトを複製することができます。

バックアップセッション、オブジェクトコピーセッション、オブジェクト集約セッションのいずれかを1つまたは複数選択できます。複製セッションでは、Data Protectorは1つのバックアップセッションからオブジェクトを読み取り、ソースB2Dデバイスからターゲットデバイスへの複製を開始します。複製セッションを実行すると、指定したセッションのすべてのオブジェクトがコピーされます。

複製機能を有効にするには、複製に対応したデバイスを選択し、オブジェクトコピー仕様で適切なオプションを選択することによってオブジェクトコピー仕様を作成します。

前提条件

- 複製の対象として選択されているデバイスが複製可能であること。
- ソースとターゲットのデバイスの種類が同じであること。
- StoreOnce内で、ソースデバイスとターゲットデバイスが別々のストアに属していること。
- ソースデバイスが少なくとも1つのバックアップ仕様で構成されている必要がある。

複製セッションの開始

複製セッションを対話式に開始するか、またはセッションの自動開始を指定することができます。Data Protectorには、2種類の自動複製機能が用意されています。**ポストバックアップ複製**と、**スケジュール設定された複製**です。

ポストバックアップ複製

ポストバックアップは、ポストバックアップ複製のサブセットであるポストコピーおよびポスト集約複製と同様、自動複製仕様で指定されたセッションの完了後に行われます。そのセッションで書き込まれた自動複製仕様に従って選択されたオブジェクトが複製されます。

スケジュール設定された複製

スケジュール設定された複製は、ユーザーが指定した時刻に開始されます。1つのスケジュール設定された複製セッションで複数のセッションを複製できます。

デバイスの選択

ソースデバイスとターゲットデバイスには、別々のデバイスを使用する必要があります。複製で使用できるのは、B2Dデバイスのみです。

複製を使用する理由

複製は、ボールティングなど、オブジェクトコピーを行うさまざまな用途(ただしメディア操作を除きます)で使用されます。オブジェクトコピーを使う理由、ページ 89も参照してください。.

また、オブジェクトコピーと比較すると、B2Dデバイス間の複製には次のようなメリットがあります。

- B2Dデバイス間で直接データを複製できます。これにより、Media Agentクライアントの負荷を軽減できます。
- 重複排除により、同じデータが複製されることはありません。これにより、ネットワーク負荷を軽減できます。

オブジェクトのミラーリング

Data Protectorには、バックアップセッション中に同一データを複数のメディアセットに同時に書き込むための、オブジェクトミラー機能が用意されています。この機能を使用すると、一部またはすべてのバックアップオブジェクトのミラーを、1つまたは複数の追加のメディアセット上に作成できます。

オブジェクトのミラーリングを使用したバックアップセッションが成功すると、バックアップされたオブジェクトを含む1つのメディアセットと、ミラーリングされたオブジェクトを含む追加メディアセットが作成されます。これらのメディアセット上のミラーリングされたオブジェクトは、オブジェクトコピーとして扱われます。

オブジェクトのミラーリングの利点

オブジェクトミラー機能は、以下の目的に役立ちます。

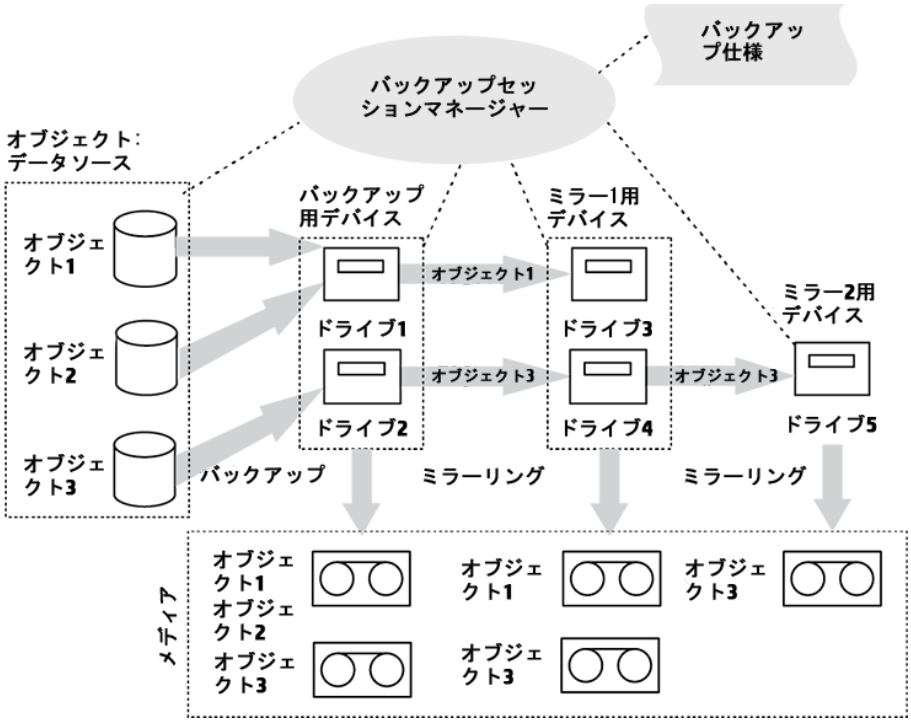
- 複数のコピーが存在するため、バックアップデータの可用性が向上します。
- バックアップデータをリモートサイトにミラー化できるため、複数の場所へのボールティングが容易になります。
- 同じデータが複数のメディアに書き込まれるため、バックアップのフォールトトレランスが強化されます。1つのメディア上でメディア障害が発生しても、他のミラーの作成には影響しません。

オブジェクトミラーの処理内容

オブジェクトミラーの作成を伴うバックアップセッションでは、選択したオブジェクトのバックアップと平行して、バックアップ仕様で指定した数のミラーが作成されます。オブジェクトのミラーリング、次のページを参照してください。

図中のオブジェクト3を例に考えてみましょう。まずDisk Agentがディスクからデータブロックを読み取り、オブジェクトのバックアップを担当するMedia Agentにこのデータを渡します。このMedia Agentは受け取ったデータをドライブ2内のメディアに書き込み、ミラー1を担当するMedia Agentにデータを渡します。ミラー1を担当するMedia Agentはドライブ4内のメディアにデータを書き込み、ミラー2を担当するMedia Agentにデータを渡します。ミラー2を担当するMedia Agentは、ドライブ5内のメディアにデータを書き込みます。セッションが終了した時点で、オブジェクト3は3つのメディア上に格納されています。

オブジェクトのミラーリング



デバイスの選択

オブジェクトのミラーリングは、デフォルトで負荷調整が行われます。Data Protectorは、できる限り多くのデバイスを使用して、使用可能なデバイスを最大限有効に活用します。デバイスは、以下に示す優先順位に従って自動的に選択されます。

- ブロックサイズが同一のデバイスがある場合は、それらが選択される
- ネットワーク接続デバイスより、ローカル接続デバイスが先に選択される

コマンドラインからオブジェクトミラー操作を実行した場合は、負荷調整を使用できません。

バックアップ性能

オブジェクトミラーの作成は、バックアップの性能に影響します。Cell ManagerおよびMedia Agentクライアント上では、ミラーの作成に伴い、別のオブジェクトを追加してバックアップする場合と同等の影響が生じます。これらのシステムでは、ミラーの数に応じてバックアップパフォーマンスが低下します。

一方、Disk Agentクライアント上ではバックアップオブジェクトの読み取りが1回しか行われないため、ミラーの作成に伴う影響はありません。

バックアップパフォーマンスは、デバイスのブロックサイズやデバイスの接続などの要因によっても左右されます。バックアップとオブジェクトのミラーリングに使用するデバイスのブロックサイズが異なる場合、ミラーリングされたデータはセッション中に再パッケージされるため、より多くの時間とリソースが必要になります。また、ネットワークを介してデータを転送すると、新たなネットワーク負荷が発生し、処理時間もそれだけ長くなります。

メディアのコピー

Data Protectorにはバックアップの終了後にメディアをコピーするための機能が用意されています。メディアのコピーとは、バックアップが格納されているメディアの完全なコピーを作成するプロセスを指します。この機能を使用すると、長期保存やボールティングなどの目的でメディアを複製できます。メディアのコピーが終了すると、元のメディアやコピーを外部の保管場所へ移動できます。

手動によるメディアコピーに加えて、Data Protectorには自動メディアコピー機能も用意されています。詳細については、メディアの自動コピー、下を参照してください。

メディアのコピー方法

メディアをコピーするには、メディアの種類が同じデバイスが2つ必要です。一方のデバイスにはソースメディアを、もう一方のデバイスにはターゲットメディアをセットします。ソースメディアとはコピーするデータが格納されているメディアであり、ターゲットメディアとはデータのコピー先となるメディアです。

複数のドライブを持つライブラリ内でメディアをコピーする場合は、その中の1つのドライブをコピー元とし、それとは別のドライブをコピー先として使用できます。

コピー結果

メディアをコピーすると、オリジナルのメディアセットと同じメディアセットがもう1セット作成されます。どちらも復元に使用できます。

ソースメディアには、コピー完了後にData Protectorによって追加不可能マークが付けられ、新しいバックアップデータを追加できなくなります(これにより、オリジナルの内容がコピーと異なることになります)。コピーにも追加不能マークが付けられます。コピーに対するデフォルトの保護設定は、元のメディアと同じになります。

元のメディアのコピーを複数作成することも可能です。ただしコピーのコピー、つまり第2世代のコピーを作成することはできません。

メディアの自動コピー

メディアの自動コピーとは、バックアップが格納されているメディアのコピーを作成する自動操作です。この機能はライブラリデバイスとともに使用します。

Data Protectorには2種類の自動メディアコピー機能が用意されています。1つはポストバックアップのメディアコピー、もう1つはスケジュールされたメディアコピーです。

ポストバックアップのメディアコピー

ポストバックアップのメディアコピーは、バックアップセッションの完了後に実行されます。この場合は、特定のセッション内で使用されたメディアがコピーされます。

スケジュール設定されたメディアコピー

スケジュール設定されたメディアコピーは、ユーザーが指定した時刻に開始されます。この場合は、異なるバックアップ仕様に基づいて使用されている複数のメディアを、単一セッション内でコピーすることも可能です。どのメディアをコピーするかは、自動メディアコピー仕様を作成して指定します。

メディアの自動コピーの動作

最初に、メディアの自動コピー仕様を作成します。自動メディアコピーセッションの開始時に、Data Protectorは、自動メディアコピー仕様内で指定したパラメーターに基づいて、メディアのリスト(ソースメディア)が生成されます。各ソースメディアでは、データのコピー先となるターゲットメディアが選択されます。ターゲットメディアは、ソースメディアと同じメディアプール、フリープール、またはライブラリ内の空きメディアの中から選択されます。

各コピー元メディアについて、ユーザーが自動メディDData Protectorアコピー仕様内に指定したデバイスの中から、1組のデバイスが自動的に選択されます。自動メディアコピー機能には独自の負荷調整機能が備えられています。Data Protectorはできるだけ多くのデバイスを使用し、また可能であればローカルデバイスを使用することにより、使用可能なデバイスを最大限有効に活用しようとします。

自動メディアコピー機能は、マウント要求やクリーニング要求には対応できません。マウント要求が受信されると、該当するメディアのペアに対してはコピーが中止されますが、セッションは続行されます。

使用例については、『*HPE Data Protectorヘルプ*』を参照してください。

バックアップメディアとバックアップオブジェクトの検証

バックアップ管理者は、重要なデータを定期的にバックアップするだけでは十分とはいえません。問題が発生したときに、入手可能な新しいより優れたバックアップ技術を使って、バックアップされたデータを正常に復元できるという信頼性が重要です。Data Protectorのバックアップメディアとバックアップオブジェクトを検証する場合、さまざまなレベルの信頼性に対する復元能力をチェックできます。

メディアの検証とは

Data Protectorのメディアの検証では、あらゆる媒体のデータ形式の有効性をチェックし、IDB内のメディア情報を更新できます。この機能を使用して、Data Protector内に常駐する完全な単一メディアを対話形式でチェックできます。メディアの検証は以下のような場合に必要になります。

- アーカイブのためにメディアをコピーし、そのコピーをボールト内に格納する前にその有効性をチェックしたい場合。
- バックアップメディアが満杯になり、長期保管用のストレージに送信する前に、メディア内のすべてのオブジェクトをチェックしたい場合。

メディアの検証作業

メディアの検証を実行すると、以下が実行されます。Data Protector

- Data Protectorヘッダー内のメディアID、説明、保存場所情報をチェックします。
- メディア上のすべてのブロックを読み取り、ブロックの形式を検証します。
- バックアップ中に巡回冗長検査(CRC)が実行された場合、CRCが再計算され、メディアに格納されているCRCと比較されます。

最初の2つのチェックが正常に終了すると、テープのハードウェアの状態が良好であること、およびすべてのデータが正常に読み取られたことが確認され、当該メディアからの復元能力に対する中レベルの信頼性が得られます。

3番目のチェックが正常に終了すると、各ブロック内でのバックアップデータ自体の一致が確認され、当該メディアからの復元能力に対する高レベルの信頼性が得られます。

オブジェクト検証とは

Data Protectorオブジェクト検証では、バックアップメディアの場合とは逆に、バックアップオブジェクトの有効性をチェックできます。オブジェクトの検証機能を使用して、以下をチェックします。

- 単一または複数のオブジェクト
- 単一または複数のメディア
- 対話形式のセッション、スケジュールされたセッション、または操作後のセッション

以下の場合、オブジェクト検証を使用できます。

- 異なるメディアへのオブジェクトコピー後
- 増分バックアップされたオブジェクトの復元チェーンに対するオブジェクト集約の実行後
- バックアップデバイスの変更後の、指定した時間枠内で生成されたすべてのバックアップオブジェクトのチェックのため

オブジェクト検証作業

オブジェクト検証を実行すると、メディアの検証の場合と同じレベルのデーData Protectorタの検証が実行されます。ただし、メディアの検証では、完全な単一メディアしかチェックされませんでしたが、オブジェクト検証では、以下をチェックできます。

- 単一のバックアップオブジェクト。メディア全体をチェックする必要がないため、規模の大きなバックアップメディアでのチェックにかかる時間を短縮できます。
- 複数のメディアにわたる大規模なオブジェクト
- 複数のメディア上の複数のオブジェクト
- 特定のオブジェクトバージョン(対話形式のみ)

さらに、以下に対して検証を実行できます。

- ネットワークトラフィックを回避するメディアエージェントホスト
- ネットワークへの影響のひとつの要素である別のホスト

オブジェクト検証仕様およびセッションに関する情報は、各種の[セッション仕様]レポートと[時間枠内のセッション]レポートで確認できます。

データの復元

データ復元ポリシーは、各企業の全体的なバックアップ戦略における本質的なポイントとなります。以下の点に注意してください。

- ファイルのバックアップと復元は、本質的にはファイルのコピーと同じことです。そのため、機密データを復元する権限は、権限のあるユーザーにのみ与えるよう注意しなければなりません。
- 権限を与えられていないユーザーが、他のユーザーのファイルを復元できないことを確認します。

この項では、Data Protectorを使った復元ポリシーの実行例を説明します。ファイルシステムデータは復元オブジェクトまたは復元セッションをブラウズすることによって復元できます。デフォルトでは、データは元の場所に復元されます。ただしデータの復元先には、任意の場所を指定できます。

復元に要する時間

データが喪失すると、復元が終了するまでは、そのデータにアクセスできなくなります。通常、ユーザーが日常業務を行えるように、データを復元する作業はできるだけ短時間で終了しなければなりません。そのため、特定のデータの復元に要する時間をあらかじめ予測しておくことが大切になります。

復元に要する時間に対する影響

復元に要する時間は、以下に示すようなさまざまな要因によって影響されます。

- 復元するデータの量。この点は、以下のすべての要因にも直接影響を与えます。
- フルバックアップと増分バックアップの組み合わせ方。詳細については、フルバックアップ、増分バックアップ、合成バックアップ、ページ 61を参照してください。
- バックアップに使用したメディアとデバイス。詳細については、デバイスとメディアの管理、ページ 105を参照してください。
- ネットワークおよびシステムの速度。詳細については、性能に関する概要と計画上の注意点、ページ 41を参照してください。
- 復元するアプリケーションの種類(Oracleデータベースファイルなど)。詳細については、各自の環境に適した『*HPE Data Protectorインテグレーションガイド*』を参照してください。
- 並行復元の使用。データのバックアップ方法によっては、単一の読み取り操作で、複数のオブジェクトを同時に復元できます。並行復元、ページ 191を参照してください。
- 復元するデータを選択する際の速度と容易さは、バックアップに使用したログレベル設定とカタログ保護期間により異なります。IDBの主要な調整可能パラメーターとしてのロギングレベル、ページ 174を参照してください。

メディアセットの選択

復元するオブジェクトバージョンが複数のメディアセット上にある場合は、それらがData Protectorのいずれかの複製メソッドで作成されている限り、どのメディアセットを使って復元処理を行っても構いません。Data Protectorのデフォルトでは、使用するメディアセットが自動的に選択されます。メディアの位置の優先順位を指定すると、メディアセットの選択を制御できます。統合オブジェクトを復元する場合を除き、復元に使用するメディアセットを手動で選択することも可能です。

メディアセットの選択アルゴリズム

デフォルトでは、可用性とData Protector品質に最も優れたメディアセットが自動的に選択されます。たとえば、Data Protectorでは、損失メディアまたは劣化メディアがあるメディアセットは避けます。オブジェクトの完了ステータス、可用性、特定のメディアセットで使用されるデバイスのローカル性などが考慮されます。ライブラリ内に格納されたメディアセットは、スタンドアロンデバイス内のメディアセットよりも先に使用されます。

復元チェーンの選択

合成バックアップを使用する場合、同時点におけるオブジェクトについて、復元チェーンが複数存在することがあります。デフォルトでは、Data Protectorによって、最も有用な復元チェーンが選択され、その復元チェーンの中で最も適切なメディアが選択されます。

メディア位置の優先順位

メディア位置の優先順位を設定しておくと、メディアセットの自動選択をある程度まで制御できます。複数の場所に分けてデータを保管している場合には、この設定が重要な意味を持ちます。メディアを別の場所に保管する場合は、それぞれの復元に対して適切な場所を指定できます。Data Protectorでは、選択したアルゴリズムの状況に複数のメディアセットが一致した場合、最上位の優先順位のメディアセットを使用します。

メディアの保管場所に対する優先順位は、全体レベルで設定することも、復元セッションごとに設定することも可能です。

デバイスの選択

デフォルトで、Data Protectorは、デバイス構成内のデバイスポリシー設定に従って、復元用のデバイスを自動的に選択します。これにより、使用可能なリソースの利用を最適化できます。元のデバイスを使用する場合に自動デバイス選択を無効にすることも、特定のデバイスを選択することも可能です。

- デバイスの自動選択(デフォルト)

  Data Protectorは使用可能なデバイスを自動的に使用します。このデバイスは、復元用に選択され、交換された元のデバイスと同じライブラリに属し、メディアの種類(例: LTO)が同じです。

  Data Protectorは、最初にオブジェクトを書き込むために使用されたデバイス(元のデバイス)の使用を試みます。元のデバイスが復元用に選択されていない場合、グローバルオプションを考慮します。最初に代替デバイスを使用するか、一斉に元のデバイスを使用できないようにするには、グローバルオプションAutomaticDeviceSelectionOrderを変更します。

  デバイスタグの指定により、デバイスをさまざまな目的でデバイスグループに分類できます。同じタグのデバイスは、互換性があるとみなされ、互いに交換可能です。使用できない元のデバイスは、同じデバイスタグを持ち、同じライブラリに属する代替デバイスに置き換えることができます。デフォルトで、デバイスタグは定義されません。

  元のデバイスが削除された場合、同じライブラリに属する、同じメディアの種類のデバイスに置き換えられます。このデバイスが復元用に選択されているかどうか、デバイスタグが元のデバイスと同じであるかどうかは検査されません。

  復元は、バックアップ時に使用したデバイスより少ないデバイスを使用して開始できます。

- 元のデバイスの選択

  Data Protectorは、復元に元のデバイスを使用し、そのデバイスが使用できない場合には待機します。これは、Data ProtectorのSAP MaxDB用統合ソフトウェアおよびDB2 UDB用統合ソフトウェアでの優先オプションです。通常、これらのデータベースは相互に依存するデータストリームでバックアップされるため、復元はバックアップ時に使用したのと同数のデバイスで開始する必要があります。

復元する権限をオペレーターにのみ付与

一般的な復元ポリシーでは、専任のバックアップオペレーター、またはネットワーク管理者にのみ、ファイル復元およびディザスタリカバリを実行する権限が与えられます。

このポリシーが適している場合

このポリシーは、以下の場合に適用します。

- 大規模なネットワーク環境で、復元作業を担当する専任オペレーターが存在する場合。
- 一般のエンドユーザーが、ファイルの復元に必要なコンピューター知識を持っていない場合。取り扱いに注意が必要なデータの復元時には、オペレーターの信頼性が求められます。

必要な作業

このポリシーを実施するには、以下の作業が必要になります。

- 他のユーザーのデータを復元できるバックアップオペレーターまたはネットワーク管理者を、Data Protectorの**operators**ユーザーグループまたは**admin**ユーザーグループに追加します。

  その他のユーザーグループに、新たなユーザー(自分のシステムを復元できるユーザーなど)を追加する必要はありません。Data Protector
- インストール時に、エンドユーザーのシステム上に、Data Protectorユーザーインターフェイスをインストールしないよう注意します。Disk Agentをインストールして、Data Protectorでこれらのシステムをバックアップできるようにします。
- 復元要求を処理するポリシーを決定しておきます。この中では、エンドユーザーがファイル復元を要求する場合の手順も明確にしておく必要があります(たとえば復元処理の請求には必ず電子メールを使い、オペレーターが目的のファイルを見つけてエンドユーザーのシステム上に復元するために必要となる情報を、すべてこのメール内に記入する、など)。またエンドユーザーに、ファイルが復元されたことを知らせる方法も、取り決めておく必要があります。

復元する権限をエンドユーザーにも付与

もう1つの復元ポリシーとして、すべてのエンドユーザーあるいは選択したエンドユーザーに、自分のデータを復元する権限を与える方法もあります。この場合は、セキュリティ面がより強化され、またバックアップオペレーターが多数の復元操作を実行する必要もなくなります。

このポリシーが適している場合

このポリシーは、以下の場合に適用します。

- エンドユーザーが、復元の取り扱いに必要な知識を持っている場合。場合によってはユーザー向けに、基本的なバックアップの概念や復元操作に関するトレーニングを実施する必要があります。
- ライブラリバックアップデバイスを使用しており、この中に、最新のバックアップデータを格納したメディアを用意しておける場合。デフォルトでは、Data Protectorの`end user`ユーザーグループのメンバーは、メディアに対するマウント要求に応答できません。そのためマウント要求が発行された場合には、バックアップオペレーターの手助けが必要になります。大容量ライブラリを使用すると、この問題の発生を防止できます。

必要な作業

このポリシーを実施するには、以下の作業が必要になります。

- Data Protectorの`end users` ユーザーグループに、自分自身のデータを復元できるエンドユーザーを追加します。セキュリティ面を強化するために、これらのユーザーがData Protectorへのアクセスに使用できるシステムを制限することも可能です。
- Data Protectorのユーザーインターフェイスを、エンドユーザーが使用しているシステムにインストールします。Data Protectorではユーザー権限を自動的に確認して、復元機能のみを許可します。
- エンドユーザーシステムのバックアップ構成時に、Data Protectorの**public**オプションをオンにして、エンドユーザーがバックアップデータを使用できるようにしておく必要があります。

ディザスタリカバリ

この項では、ディザスタリカバリの概念について簡単に説明します。ディザスタリカバリの概念、計画、準備、手順の詳細な内容については、『*HPE Data Protectorディザスタリカバリガイド*』を参照してください。

コンピューター障害とは、人為的ミス、ハードウェアまたはソフトウェア障害、自然災害などにより、コンピューターシステムがブート不可能な状態になるイベントを指します。このような場合、システムのブートパーティションまたはシステムパーティションが使用できなくなり、標準的な復元操作を行う前に環境の復旧が必要となります。このためには、ブートパーティションの再作成や再フォーマット、環境を定義するすべての構成情報を含めたオペレーティングシステムの再構築などを実行する必要があります。*最初にこの作業を完了しておかなければ、その他のユーザーデータを復旧できません。*

コンピューター障害が発生した後のシステム(**ターゲットシステム**)は、通常ブート不可能な状態になっており、Data Protectorのディザスタリカバリは、このシステムを元のシステム構成に戻すことを目的としています。影響を受けたシステムとは異なり、ターゲットシステムの場合は、障害が発生したハードウェアはすべて交換されています。

障害の発生は常に重大な問題ですが、以下の要因は状況をさらに深刻化します。

- システムをできる限り迅速かつ効率的にオンライン状態に戻す必要がある。
- ディザスタリカバリを実行するために必要な手順に管理者が十分精通していない。
- 復旧を実行する担当者が、基礎的なシステム知識しか持っていない。

ディザスタリカバリは複雑な作業であり、事前に広範囲にわたる計画と準備を行っておく必要があります。障害に対する準備作業、および障害からの復旧作業については、明確に定義された詳細な作業手順を作成しておかなければなりません。

ディザスタリカバリプロセスは4つのフェーズに分けられます。

1. **フェーズ0**は、ディザスタリカバリを成功させるために必要な計画/準備作業です。

   > **注意:**
   > 障害が発生してからディザスタリカバリの準備をしても遅すぎます。

2. **フェーズ1**で、DR OSのインストールと構成を行います。通常はブートパーティションの再作成と再フォーマットも行います。これは、システムのブートもしくはシステムパーティションは常に使用可能とは限らず、通常の復元操作を行う前に環境の復旧が必要となるためです。
3. 環境を定義するすべての構成情報を含めたオペレーティングシステムとを元の状態に復元する作業は、Data Protector**フェーズ2**フェーズ2で実行します。

4. フェーズ2までの作業が完了して初めて、アプリケーションデータやユーザーデータの復元が可能になります(**フェーズ3**)。

   迅速かつ効率的な復旧を確実に行うには、明確に定義された詳細な作業手順を作成しておく必要があります。

ディザスタリカバリの方法

Data Protectorは、以下のディザスタリカバリの手法をサポートしています。

- 手動によるディザスタリカバリ

  これは基本的で非常に柔軟なディザスタリカバリの手法です。この方法では最初にDR OSをインストールして構成する必要があります。次に、Data Protectorを使ってデータを復元し(オペレーティングシステムファイルを含む)、現在のオペレーティングシステムファイルを、復元したオペレーティングシステムファイルで置き換えます。
- 自動ディザスタリカバリ

  自動システム復旧(ASR)はWindowsシステム上の自動システムで、障害発生時にディスクをオリジナルの状態に再構成(または、新しいディスクがオリジナルのものより大きい場合、パーティションをサイズ変更)します。このようにASRはData Protectorの`drstart.exe`コマンドにより、Data Protectorディスク、ネットワーク、テープ、ファイルシステムへのアクセスを提供するアクティブなDR OSをインストールすることができます。
- ディスクデリバリーによるディザスタリカバリ

  Windowsクライアントの場合は、影響を受けたシステム上のディスク(またはディスクが物理的に損傷している場合は交換用のディスク)を、ホストシステムに一時的に接続します。復元後、新しいディスクを障害が発生したシステムに接続し、ブートします。UNIXシステムの場合は、最小限のオペレーティングシステム、ネットワーク機能、およびData Protectorエージェントがインストールされた補助ディスクを使用して、ディスクデリバリーによるディザスタリカバリを実行します。
- 拡張自動ディザスタリカバリ(EADR)

  拡張自動ディザスタリカバリ(EADR)では、Windowsクライアント用とCell Manager用の完全自動化されたData Protector復旧手法により、ユーザーの操作が最小限に抑えられます。システムは、ディザスタリカバリCD ISOイメージからブートされます。復元時にはData Protectorにより自動的にDR OSのインストールと構成、ディスクのフォーマットとパーティションの作成が行われ、最後に元のシステムがData Protectorとともにバックアップ時と同じ状態に復旧されます。
- ワンボタンディザスタリカバリ(OBDR)とは、WindowsクライアントとCell Manager用に完全に自動化されたData Protector復旧方法で、ユーザーが介在する手間は最小限に抑えられています。システムはOBDRテープからブートされ、自動的に復旧されます。

個々のオペレーティングシステムでサポートされるディザスタリカバリの手法のリストについては、最新のサポート一覧(https://softwaresupport.hpe.com/)を参照してください。

その他のディザスタリカバリの方法

この項では、Data Protectorを使ったディザスタリカバリの概念と、サードパーティ製品のディザスタリカバリの概念を比較します。ここでは、Data Protector以外の復旧方法について簡単に紹介します。

主な復旧方法としては、以下の2つが挙げられます。

オペレーティングシステムのベンダーが提供する復旧方法

大多数のベンダーは、それぞれ独自の復旧方法を提供していますが、通常、復元時は、以下の手順が必要となります。

1. オペレーティングシステムを一から再インストールします。
2. アプリケーションを再インストールします。
3. アプリケーションデータを復元します。

この場合、障害前の状態を再構築するには、オペレーティングシステムやアプリケーションに対して、手動によるさまざまな再構成やカスタマイズが必要になります。このような作業では、統合されたツールではなく、個別のさまざまなツールを使用することになるため、非常に複雑で、時間がかかり、間違いも起こりやすくなります。この方法では、オペレーティングシステム、アプリケーション、これらの構成情報などに関するバックアップデータが、ひとまとまりのセットとして利用されることはありません。

サードパーティ製ツールを使った復旧(Windowsシステムの場合)

通常これらのソフトウェアでは、すばやい復元処理を可能にするために、システムパーティションのスナップショットを提供する何らかの特殊なツールが使われています。この方法を使用する場合の一般的な手順は、以下のとおりです。

1. システムパーティションを復元します(サードパーティ製ツールを使用)。
2. 必要に応じて、標準的なバックアップツールを使用して、その他のパーティションを復元します(一般的には選択的な復元が可能)。

復元時にはこのように、2つの異なるバックアップセットに対して、それぞれ個別のツールを使用した作業が必要になることは明らかです。これを定期的に行うことは困難です。特に大規模な組織でこの方法を実行する場合には、2種類のツールから生成される多数のデータを、複数バージョン(週ごとのバックアップなど)管理しなければならないため、管理作業の負荷が非常に大きくなってしまいます。

一方Data Protectorは、複数のプラットフォームにまたがる包括的で強力な企業向けソリューションであり、バックアップや復元の機能を持ち、クラスタリングにも対応しているため、高速かつ効率的にディザスタリカバリを実行できます。Data Protectorには、大規模な組織のシステム管理を支援するための、集中管理や復元を容易にする機能、高可用性のサポート、モニタリング、レポート、通知などの機能が備わっています。

第3章: デバイスとメディアの管理

この章では、Data Protectorにおけるデバイス管理とメディア管理の概要について説明します。以下ではデバイス、メディアプール、および大容量ライブラリについて、順番に説明していきます。

デバイス

Data Protectorは、市販されているさまざまなデバイスをサポートしています。サポート対象デバイスの最新情報は、https://softwaresupport.hpe.com/を参照してください。

デバイスの種類

デバイスは、次の種類に分類されます。

- テープデバイス
  - スタンドアロンデバイス。「スタンドアロンデバイス、ページ 112」を参照してください。
  - 小規模なマガジンデバイス。「小規模なマガジンデバイス、ページ 113」を参照してください。
  - 大容量ライブラリ。「大容量ライブラリ、ページ 114」を参照してください。
- ディスクベースのデバイス。「ディスクベースのバックアップデバイス、ページ 121」を参照してください。
- クラウドバックアップデバイス。クラウド(Helion)およびクラウド(Azure)デバイスを参照してください。

Data Protectorでのデバイスの使用

Data Protectorでバックアップデバイスを使用するためには、まず、そのデバイスをData Protectorセル内に構成しなければなりません。デバイスの構成時には、デバイスの名前、デバイス固有のオプション(バーコードやクリーニングテープのサポートなど)、およびメディアプールを指定します。このデバイス構成プロセスではウィザードに従って簡単に作業を実行でき、さらにデバイスの検出と自動構成も可能です。Data Protectorでは1つの物理デバイスを、論理デバイス名を変えて何回でも定義でき、それぞれに異なる使用属性を設定できます(たとえばハードウェアデータ圧縮を使用するものと、使用しないものなど)。

以下では、いくつかの特殊なデバイス機能と、Data Protectorにおけるさまざまなデバイスの取り扱い方法について説明します。

ライブラリ管理コンソールのサポート

現在使われているテープライブラリの多くは、リモートシステムからライブラリを構成、管理、監視するための管理コンソールを備えています。リモートで実行可能なタスクの範囲は管理コンソールの実装によって異なり、Data Protectorには依存しません。

Data Protectorは、ライブラリ管理コンソールのインターフェイスに簡単にアクセスするための機能を備えています。管理コンソールのURL (Webアドレス)は、ライブラリの構成時または再構成時に指定できます。GUIでこの作業用のメニューを選択すると、Webブラウザーが起動され、ブラウザー内にコンソールインターフェイスが自動的に表示されます。

この機能に対応しているデバイスの種類の一覧については、https://softwaresupport.hpe.com/を参照してください。

> **重要:**
> ライブラリ管理コンソールを使用する場合は、コンソールから実行できる操作の一部が、通常のメディア管理操作やバックアップセッションまたは復元セッションを妨げる可能性がある点に注意してください。

TapeAlert

TapeAlertは、テープデバイス状態の監視および通知を行うユーティリティであり、バックアップデータの品質に影響する問題点の検出に役立ちます。TapeAlertを使用すると、摩滅したテープの使用から、デバイスハードウェア上の問題に至るまで、何らかの問題が発生した場合にわかりやすい形で警告やエラーが表示され、さらに問題への対処方法も示されます。

Data Protectorは、TapeAlert 2.0を完全にサポートしています(接続するデバイスがこれに対応している場合)。

デバイスリストと負荷調整

複数のバックアップデバイスの使用

バックアップ仕様を構成する場合、複数のスタンドアロンデバイスやライブラリデバイスの複数のドライブをバックアップに指定することもできます。このように指定すると、複数のデバイス(ドライブ)を使ってデータのバックアップを並行して実行できるため、処理の性能が向上します。

デバイス使用率の平均化

デフォルトでは、Data Protectorにより各デバイスの負荷(使用率)が自動的に平均化されるため、すべてのデバイスがほぼ均一に使用されます。この処理は、**負荷調整**と呼ばれます。負荷調整を行うと、各デバイスにバックアップされるオブジェクトの数とサイズが平均化されるため、デバイス全体の使用率が最適化されます。負荷調整はバックアップ時に自動実行されるため、ユーザーは使用するデバイスを複数指定するだけでよく、セッションで使用するデバイスへのオブジェクトの割り当てを細かく指定する必要はありません。

負荷調整の使用に適している場合

以下の場合は、負荷調整を使用してください。

- 多数のオブジェクトをバックアップする場合。
- 複数のドライブを持つライブラリ(オートチェンジャー)デバイスを使用する場合。
- オブジェクトがどのメディアにバックアップされるかを知る必要がない場合。
- 高性能なネットワーク接続がある場合。
- バックアップの堅牢性を高めたい場合。Data Protectorでは、障害が発生したデバイスからデバイスリスト内の他のデバイスに、バックアップ処理を自動的に割り振ります。

負荷調整の使用に適さない場合

以下の場合は、負荷調整を使用しないでください。

- サイズの大きいオブジェクトを少数のみバックアップする場合。一般にこのような場合は、Data Protectorによるデバイス間の負荷調整が効果的に機能しません。
- オブジェクトをバックアップするデバイスを、明示的に選択したい場合。

デバイスチェーン

Data Protectorでは、複数の同じ種類のスタンドアロンデバイスをグループ化して、同じシステムに接続し、1つのデバイスチェーンを構成することができます。ここで同じ種類とは、同じシステムに接続されているデバイスのことです。1つのデバイス内のメディアが一杯になると、バックアップ処理はデバイスチェーン内の次のデバイス内のメディアに自動的に引き継がれます。

負荷調整の仕組み

たとえば100個のオブジェクトを4台のデバイスにバックアップする場合、同時処理数を3に設定し、負荷調整パラメーターMINとMAXをどちらも2に設定したとします。少なくとも2台のデバイスが使用可能な場合はセッションが開始し、3オブジェクトずつ、それぞれ最初に使用できるこの2デバイスに並列してバックアップされます。残りの94個のオブジェクトは保留となり、その時点では特定のデバイスに割り当てられません。

あるオブジェクトのバックアップが終了すると、次の保留オブジェクトのバックアップが開始され、同時バックアップ中のオブジェクトが3未満であるデバイスが割り当てられます。負荷調整により、バックアップ保留中のオブジェクトがある限り、2台のデバイスが確実に同時処理を行うことになります。バックアップ中に1台のデバイスが故障した場合は、予約されている2デバイスのうちの1つが使用されます。故障したデバイスでバックアップ中だったオブジェクトのバックアップは中止され、次の3つの保留オブジェクトが新しいデバイスに割り当てられます。このことは、他のデバイスでバックアップセッションを継続することが可能であれば、デバイス1台の故障により最大で3オブジェクトのバックアップが中止されることを意味します。

デバイスストリーミングと同時処理数

デバイスストリーミングとは

デバイスのパフォーマンスを最大限に引き出すには、デバイスをストリーミング状態に維持する必要があります。十分な量のデータが送られてメディアを常に前へ移動させる状態を、デバイスのストリーミングが維持されていると言います。デバイスストリーミングが維持されていなければ、デバイスがデータを待っている間メディアテープは停止しなければなりません。言い換えると、テープへのデータ書き込み速度がコンピューターシステムからデバイスへのデータ転送速度よりも遅いかまたは等しい場合、デバイスストリーミングが維持されていると言えます。バックアップインフラストラクチャーでネットワークを多用する場合は、そのことにも注意が必要です。ローカルバックアップの場合は、ディスクとデバイスが同一システムに接続されているため、ディスクの処理速度が速くても、同時処理数には通常1を指定すれば十分です。

デバイスストリーミングの構成方法

デバイスでストリーミングを行えるようにするには、デバイスに十分な量のデータを送信する必要があります。このため、Data Protectorでは、データをデバイスに書き込む各Media Agentに対して複数のDisk Agentを起動します。

Disk Agentの同時処理数

各Media Agentから起動されるDisk Agentの数は、**Disk Agent (バックアップ)同時処理数**と呼ばれます。この数は、デバイス用の**拡張**オプションを使用して変更できるほか、バックアップの構成時にも変更可能です。Data Protectorでは、デフォルト値が設定されており、ほとんどの場合はこの数で十分です。たとえば標準的なDDSデバイスの場合であれば、2つのDisk Agentにより、ストリーミングの維持に十分なデータをデバイスに送信できます。また、ライブラリデバイス内に複数のドライブがあり、各ドライブが個別のMedia Agentで制御される場合には、それぞれのドライブごとに個別に同時処理数を設定できます。

性能の向上

バックアップの同時処理数を適切に設定すると、バックアップのパフォーマンスが向上します。たとえば4つのドライブを持つライブラリデバイスがあり、各ドライブは個別のMedia Agentで制御されているとします。このとき、個々のMedia Agentがそれぞれ2つのDisk Agentから同時にデータを受け取ると、8つのディスク上のデータを同時にバックアップできます。

デバイスストリーミングは、ネットワーク負荷や、デバイスに書き込まれるデータのブロックサイズなどの要因にも影響されます。

関連情報については、バックアップセッション、ページ 183を参照してください。

多重データストリーム

Data Protectorでは、ディスクの一部を複数のデバイスに同時にバックアップできます。この機能は非常に大容量で高速のディスクを比較的遅いデバイスへバックアップする場合に役立ちます。複数のDisk Agentが同じディスクから並列にデータを読み取り、複数のMedia Agentに送信します。これによってバックアップ速度が向上しますが、以下のことを考慮する必要があります。

1つのマウントポイントが複数のDisk Agentを通してバックアップされた場合、データは複数のオブジェクトに格納されます。マウントポイント全体を復元するには、1つのバックアップ仕様でマウントポイントの要素をすべて定義した後、セッション全体を復元します。

デバイスのフィルター処理

デバイスのフィルター処理とは

デバイスのフィルター処理は、クラスターセットアップのアクティブノードに基づいて、バックアップ用のデバイスターゲットを選択するためのメカニズムです。

デバイスフィルターを使用すると、バックアップターゲットを近くにあるクライアントに割り当てて、ネットワークトラフィックを減らすことができます。たとえば、Oracle RACメトロクラスターは、2つのデータセンターにまたがって存在する場合があります。デバイスのフィルター処理は、データ発生元のノードを識別して、そのノードに対してローカルのあて先ターゲットに割り当てるメカニズムです。

デバイスのフィルター処理の仕組み

クラスターセットアップでは、各ノードはホストタグと呼ばれる固有名によって識別されます。ターゲットとなる可能性があるデバイスに同じ名前が割り当てられます。バックアップ仕様であて先デバイスを選択する場合は、すべてのノードホストタグと一致するデバイスを選択します。データがストリームされるノードに基づくバックアップ中は、一致するデバイスが使用されます。

デバイスフィルタータグを設定する方法

以下の方法で、デバイスフィルタータグを設定できます。

デバイスフィルタータグは、Cellサーバーホスト内の以下の位置にあるデバイスフィルターファイルに設定する必要があります。

```
<DP configuration>/server/cell/devfilters
```

デバイスフィルターファイルは、それぞれの論理デバイスを1行で設定します。行の形式は、以下のとおりです。

```
<Logical Device Name> <filter tag>[,<filter tag>]*
```

> **注:**
> Logical Device Nameにスペースが含まれている場合は、名前全体を引用符(")で囲む必要があります。エラーの可能性を最小限に抑えるために、すべての論理デバイス名を引用符で囲むことを推奨します。また、フィルタータグは、omnirc変数のようにコンマで区切る必要があります。

または

デバイスフィルタータグは、Data Protector GUIのデバイスプロパティを使用して構成することができます。Data Protector GUIを使用して、ホストタグを設定することもできます。各クライアントには、任意の数のフィルタータグを割り当てることができます。フィルタータグのデフォルトの値は、空にすることができ、任意の英数字を含むことができます。空白文字は使用できません。

デバイスはバックアップセッション中にフィルター処理され、データリストまたはバーリスト内のすべてのデバイスがデバイスフィルターリストに対してチェックされます。ホストタグのすべてのフィルタータグは、特定のホストのバックアップセッションに適用可能なデバイス用のデバイスフィルタータグと一致している必要があります。デバイスフィルターファイル内にデバイスがない場合は、そのデバイスにフィルタータグが割り当てられていないと推定されます。したがって、フィルタータグがクライアントに設定されている場合は、デバイスを使用することはできません。

デバイスのフィルター処理は、デバイスのみに適用できるため、ライブラリ(ロボティクス)をデバイスフィルターファイルに追加する必要はありません。

以下のグローバル変数を使用して、デバイスフィルター機能を制御することもできます。

- EnableDeviceFilters = 0|1(デフォルトではEnableDeviceFiltersは0に設定されています)

  EnableDeviceFiltersグローバル変数を1に設定すると、フィルタータグにホストタグとデバイスフィルターファイルが定義されます。

  EnableDeviceFiltersグローバル変数を0に設定すると、Data Protectorはフィルタータグが設定されているとしても、それを無視します。
- DeviceFilterMatch = 0|1(デフォルトではDeviceFilterMatchは0に設定されています)

  DeviceFilterMatchグローバル変数が0に設定されている場合、デバイスフィルターはAND方式で一致されます。

  DeviceFilterMatchグローバル変数が1に設定されている場合、デバイスフィルターはOR方式で一致されます。

たとえば、devfiltersファイルと、クライアント上のホストタグに以下が含まれている場合を考慮します。

devfilterファイルとクライアント上のホストタグ

devfilterファイル	クライアント上のホストタグ
"HP:Ultrium 1" tag1	<hostname A> tag1
"HP:Ultrium 2" tag2	<hostname B> tag2
"HP:Ultrium 3" tag1,tag2	<hostname C> tag1,tag2

DeviceFilterMatch=0の場合、特定のホストに存在するオブジェクトに対して次のデバイスが使用できます。

ホストA上のオブジェクト:"HP:Ultrium 1"および"HP:Ultrium 3"デバイスが基準に一致します。

ホストB上のオブジェクト:"HP:Ultrium 2"および"HP:Ultrium 3"デバイスが基準に一致します。

ホストC上のオブジェクト: "HP:Ultrium 3"デバイスのみが基準に一致します。

`DeviceFilterMatch=1`の場合、特定のホストに存在するオブジェクトに対して次のデバイスが使用できます。

ホストA上のオブジェクト:"HP:Ultrium 1"および"HP:Ultrium 3"デバイスが基準に一致します。

ホストB上のオブジェクト:"HP:Ultrium 2"および"HP:Ultrium 3"デバイスが基準に一致します。

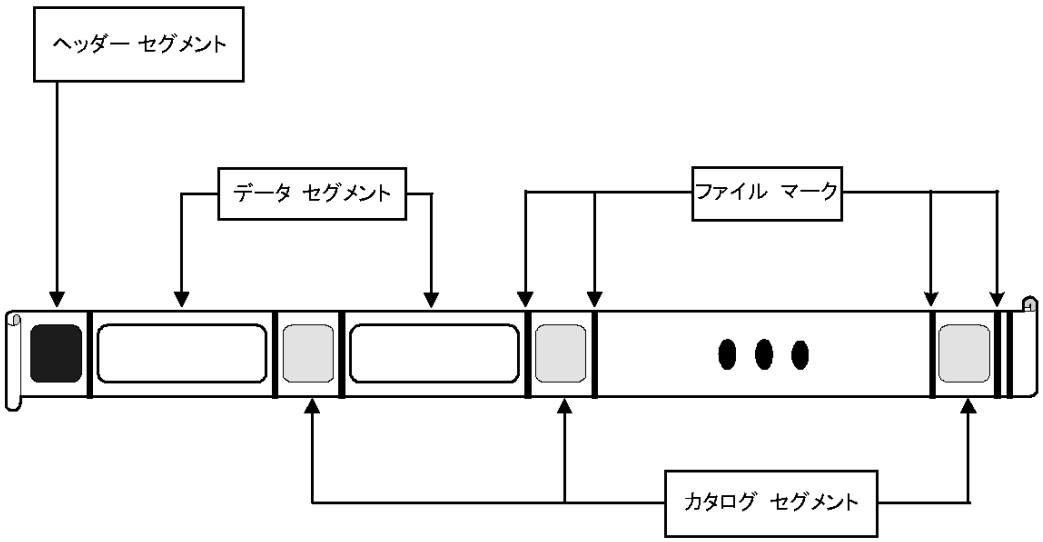
ホストC上のオブジェクト:"HP:Ultrium 1"、"HP:Ultrium 2"および"HP:Ultrium 3"デバイスが基準に一致します。

セグメントサイズ

メディアは、データセグメント、カタログセグメント、ヘッダーセグメントに分かれています。ヘッダー情報は、ブロックサイズと同じ長さのヘッダーセグメントに格納されます。データは、データセグメント内のデータブロックに格納されます。各データセグメントに関する情報は、対応するカタログセグメントに格納されます。この情報は、Media Agentのメモリにまず記録され、その後にメディアのカタログセグメントとIDBに書き込まれます。データフォーマット、下に示すように、個々のセグメントはファイルマークによって分割されます。

> **注:**
> 一部のテープテクノロジでは、メディア内のファイルマークの数に制限があります。セグメントサイズが小さすぎないかどうかを確認してください。

データフォーマット



セグメントサイズ(MB単位)は、データセグメントの最大サイズです。小サイズのファイルを多数バックアップする場合、実際のセグメントサイズはカタログセグメントの最大サイズに制限されることがあります。セグメントサイズはデバイスごとにユーザーが構成できます。セグメントサイズは復元速度に影響を与えます。セグメントサイズが小さくなればなるほど、メディア上のスペースは少なくなります。これはセグメントごとのファイルマークがメディアスペースを消費するためです。ただし、ファイルマークの数が多いと、Media Agentが目的のデータが含まれているセグメントをすばやく見つけ出せるため、復元速度は向上します。最適なセグメント

サイズは、デバイスで使用されるメディアの種類やバックアップデータの種類によって異なります。たとえば、DLTメディアのデフォルトのセグメントサイズは150MBです。

ブロックサイズ

セグメントはユニットとして書き込まれるのではなく、ブロックと呼ばれるユニットより小さなサブユニットとして書き込まれます。デバイスのハードウェアでは、デバイスの種類ごとに固有のブロックサイズの単位でデータを処理します。Data Protectorでは、デバイスに送信するブロックサイズを調整できます。ほとんどのデバイスの種類ではデフォルトブロックサイズ値は256KBです。

ブロックサイズを大きくすると、パフォーマンスが向上することがあります。ただし、ブロックサイズの変更は、テープをフォーマットする*前*に実行しておかなければなりません。たとえば、デフォルトのブロックサイズを使ってすでにデータが書き込まれているテープに、別のブロックサイズのデータを追加することはできません。

注意:
Data Protector Media Agentで制御しているデバイスのブロックサイズを拡張する場合には、オペレーティングシステムでサポートされるデフォルトの最大ブロックサイズを超えないように注意してください。ブロックサイズが最大サイズを超えると、Data Protectorでデバイスのデータを復元できなくなります。ブロックサイズが調整可能かどうか、調整方法については、オペレーティングシステムのドキュメントを参照してください。

注:
種類の違うデバイスで使用できる共通のブロックサイズを使用します。Data Protectorでは、同じブロックサイズでしかメディアにデータを追加することはできません。

Disk Agentのバッファー数

Data ProtectorのMedia AgentとDisk Agentは、転送待ちのデータを一時的に保持するためにメモリバッファーを使用します。このメモリは、複数のバッファー領域に分割されています。総数はデバイスの同時処理数に依存しますが、Disk Agentごとにバッファー領域が1つずつあります。また、各バッファー領域は、そのデバイス向けに構成されているブロックサイズと同じ大きさの、8つのDisk Agentバッファーから構成されています。この値は1～32の範囲で変更できますが、通常変更する必要はありません。この設定を変更する理由としては、主に以下の2つの理由が考えられます。

- メモリの不足

  Media Agentが必要とする共有メモリのサイズは、次のように計算できます。

  ```
  DAConcurrency * NumberOfBuffers * BlockSize
  ```

  たとえばバッファー数を8から4に減らすと、メモリ消費量は約50%削減されますが、性能にも影響が及びます。

- ストリーミング

  利用可能なネットワーク帯域幅がバックアップ中に大きく変動する場合は、デバイスのストリーミングを維持するために、Media Agentが十分な書き込み用データを確保できることが特に重要になります。このような場合は、バッファー数を増やしてください。

デバイスロックとロック名

デバイス名

Data Protectorで使用するバックアップデバイスを構成するときには、同一物理デバイスを名前を変えて何度でも構成できるため、1つの物理デバイスにそれぞれ異なる特徴を定義して複数回定義することも可能です。Data Protectorたとえば、1つのスタンドアロンDDSデバイスを、圧縮デバイスとして定義し、さらに名前を変えて非圧縮デバイスとしても定義することができます。ただし、このような定義の仕方はお勧めできません。

物理デバイスの衝突

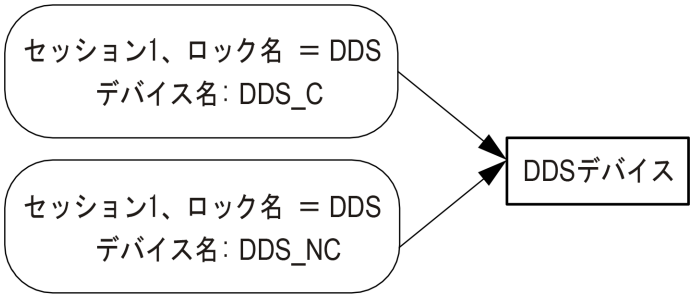
バックアップに使用するデバイスを指定するときに、あるバックアップ仕様内で1つのデバイス名を指定し、別のバックアップ仕様内で同じ物理デバイスの別名を指定していることがあります。このような場合、バックアップのスケジュール方法によっては、Data Protectorが複数のバックアップセッションで同時に同一の物理デバイスを使おうとして、デバイスの衝突が発生する可能性があります。

衝突の防止

この衝突を回避するには、両方のデバイス設定で仮想ロック名を指定します。Data Protectorでは、両方のデバイスでロック名が同じであることを確認し、衝突を回避します。

たとえばデバイスロックとデバイス名、下では、あるDDSデバイスをDDS_Cという名前の圧縮デバイスとして構成し、さらにDDS_NCという名前の非圧縮デバイスとしても構成しています。この場合、両方のデバイス構成内に、DDSという同一のロック名を指定しておきます。

デバイスロックとデバイス名



スタンドアロンデバイス

スタンドアロンデバイスとは、1つのドライブのみを備えたデバイスであり、1度に1つのメディアに対する読み取りまたは書き込みが可能です。

スタンドアロンデバイスは、小規模なバックアップ、または特別なバックアップに使用します。メディアが一杯になった場合、オペレーターはバックアップを続行するために、新しいメディアに手動で交換しなければなりません。

Data Protectorとスタンドアロンデバイス

システムにデバイスを接続し終わったら、Data Protectorユーザーインターフェイスを使って、そのデバイスをData Protectorで使用できるように構成します。このためには、デバイスを接続するシステムに、まずData ProtectorのMedia Agentをインストールしておく必要があります。Data Protectorでは、ほとんどのスタンドアロンデバイスを検出し、自動的に設定することができます。

バックアップ中に、デバイス内のメディアが一杯になると、Data Protectorからマウント要求が発行されます。バックアップを続行するには、オペレーターが手動でメディアを交換しなければなりません。

デバイスチェーンとは

Data Protectorでは、複数のスタンドアロンデバイスをグループ化して、1つのデバイスチェーンを構成できます。1つのデバイス内のメディアが一杯になると、バックアップ処理はデバイスチェーン内の次のデバイス内のメディアに自動的に引き継がれます。

デバイスチェーンでは、複数のスタンドアロンデバイスを使用することにより、あるメディアが一杯になった場合にも、手動でメディアを交換することなく、無人バックアップを継続できます。

スタッカーデバイス

スタッカーデバイスは、デバイスチェーンとよく似ており、デバイス内に複数のメディアを格納しておき、これを順番に使用できます。あるメディアが一杯になると、次のメディアが自動的にロードされて、バックアップに使用されます。

小規模なマガジンデバイス

マガジンデバイスでは、複数のメディアをマガジンと呼ばれる1つの単位にグループ化します。Data Protectorでは、このマガジンを単一メディアのように取り扱います。マガジンは、単一メディアよりも多くのデータを保存でき、複数のメディアの場合に比べて扱いも容易です。サポート対象デバイスの一覧は、https://softwaresupport.hpe.com/を参照してください。

Data Protectorとマガジンデバイス

Data Protectorでは、マガジン用およびメディア用のビューが用意されているため、単一メディアの場合と同じように、セットとしたマガジンを対象に、または単一メディアを対象に、メディア管理タスクを実行できます。

また、マガジンデバイスをData Protectorのマガジンサポートを使用しないで通常のライブラリとして使用することもできます。Data Protectorではマガジンデバイスを検出して、自動的に設定できます。

汚れたドライブのクリーニング

Data Protectorでは、ドライブが汚れたときに、クリーニングテープを使用して自動的にマガジンや他のデバイスをクリーニングできます。

大容量ライブラリ

ライブラリデバイスとは

ライブラリデバイスは、自動化されたデバイスであり、オートローダー、エクスチェンジャー、またはジュークボックスとも呼ばれます。Data Protectorでは、ほとんどのライブラリはSCSIライブラリとして構成されます。これらのデバイスのレポジトリ内には多数のメディアカートリッジが格納されており、複数のドライブを使用して複数のメディアへの同時書き込みが可能です。

一般的なライブラリデバイスでは、デバイス内の各ドライブにそれぞれ個別のSCSI IDが設定され、メディアをスロットからドライブに、またはその逆に移動させるロボティクスにも個別のSCSI IDが設定されます。たとえば、4つのドライブを備えたライブラリの場合には5つのSCSI IDが必要になります(ドライブ用に4つ、ロボティクス用に1つ)。

Data Protectorは、HPEライブラリ、StorageTek/ACSLS、ADIC/GRAU AMLなどのサイロライブラリもサポートしています。サポート対象デバイスの一覧は、https://softwaresupport.hpe.com/を参照してください。

メディアの操作

Data Protectorユーザーインターフェイスには、ライブラリデバイスの管理に便利な、特別なライブラリビューが用意されています。

大容量ライブラリデバイス内のメディアは、そのすべてを1つのData Protectorメディアプールとして構成することもできれば、いくつかのプールに分割することも可能です。

ライブラリの構成

デバイス構成時には、Data Protectorに割り当てるスロット範囲を設定することもできます。こうすることで、ライブラリを別のアプリケーションと共有することが可能になります。割り当てたスロットには、ブランク(新しい)メディアや、Data ProtectorのメディアまたはData Protector以外のメディアを含めることもできます。Data Protectorでは、スロット内のメディアを確認して、メディアの情報をライブラリビューに表示します。この機能では、Data Protectorで使われているメディアだけでなく、すべてのメディアのチェックが可能です。

ライブラリのサイズ

必要なライブラリのサイズは、以下のように見積ります。

- メディアを複数の場所に分散させる必要があるか、または1か所に集中して管理するかを決定します。
- 必要なメディアの数を見積ります。「メディア交換ポリシーの実装、ページ 155」を参照してください。

他のアプリケーションとのライブラリの共有

デバイス内のメディアにデータを保存する機能を持つ他のアプリケーションと、ライブラリデバイスを共有できます。

まずライブラリ内のドライブのうち、Data Protectorで使用するドライブを決定します。たとえば4つのドライブを持つライブラリであれば、そのうち2つのドライブのみをData Protectorで使用するというように設定します。

また、ライブラリ内のスロットのうち、どのスロットをData Protectorで使用するかも決定できます。たとえば、60個あるライブラリスロットのうち、1～40までのスロットをData Protectorで使用するというように設定します。この場合残りのスロットは、他のアプリケーションにより使用および制御されます。

特にHPEの大容量ライブラリや、StorageTek/ACSLS、ADIC/GRAU AMLなどの大容量デバイスを使う場合には、他のアプリケーションとのライブラリ共有が重要になってきます。

挿入および取り出しメールスロット

ライブラリデバイスには、オペレーターがメディアの出し入れに使用する、特別なメディア挿入/取り出し用メールスロットが装備されています。デバイスによっては、複数の挿入/取り出しスロットが装備されていることもあります。メールスロットが1つしかない場合には、メディアは1つずつ出し入れしなければなりませんが、複数のメールスロットがある場合には、1回の挿入/取り出し操作で複数のスロットを操作できます。

Data Protectorでは、1回の操作で複数のメディアの挿入/取り出しが可能です。たとえば、1回の操作で、デバイス上の50個のスロットを選択することも、すべてのメディアを取り出すこともできます。Data Protectorでは、メディアを自動的に正しい順序で排出して、オペレーターがメディアをメールスロットに挿入したり、メールスロットから取り出したりできるようにします。

詳細については、ご使用のデバイスのマニュアルを参照してください。

バーコードリーダーのサポート

Data Protectorは、バーコードリーダーを備えたライブラリデバイスをサポートしています。これらのデバイス内のメディアには、メディアを一意に識別するためのバーコードが貼付されています。

バーコードの利点

バーコードを使用すると、Data Protectorによるメディアの認識、ラベリング、クリーニングテープの検出などを非常に効率よく実行できます。

- デバイスのレポジトリ内にあるメディアを高速にスキャンできます。これは、バーコードを使用した場合、Data Protectorでは実際にメディアをドライブにロードして、メディアのヘッダーを読み込む必要がないためです。
- バーコードはData Protectorにより自動的に読み取られ、メディアの識別に使用されます。
- クリーニングテープのバーコードの先頭を"CLN"としておくと、クリーニングテープの自動検出が可能になります。
- バーコードは、IDB内で管理されているメディアに対する一意の識別子となります。環境内でのバーコードの重複は許されません。

> **ヒント:**
> メディアを初期化する際に、バーコードをメディアラベルとして使用することも可能です。

クリーニングテープのサポート

HPE Data Protectorでは、大部分のデバイスについて、クリーニングテープを使用した自動クリーニングを実行できます。デバイス内のドライブで汚れが検出された場合には、Data Protectorによりクリーニングテープが自動的に使用されます。

- SCSIライブラリでは、クリーニングテープを格納するスロットを定義できます。
- バーコードリーダーを備えたデバイスで、クリーニングテープのバーコードの先頭をCLNとしておくと、Data Protectorによりクリーニングテープが自動的に認識されます。
- クリーニングテープが用意されていないデバイスで、ドライブの汚れが検出された場合は、セッションモニターウィンドウ上にクリーニング要求が表示されます。この場合は、オペレーターが手動でデバイスをクリーニングしなければなりません。

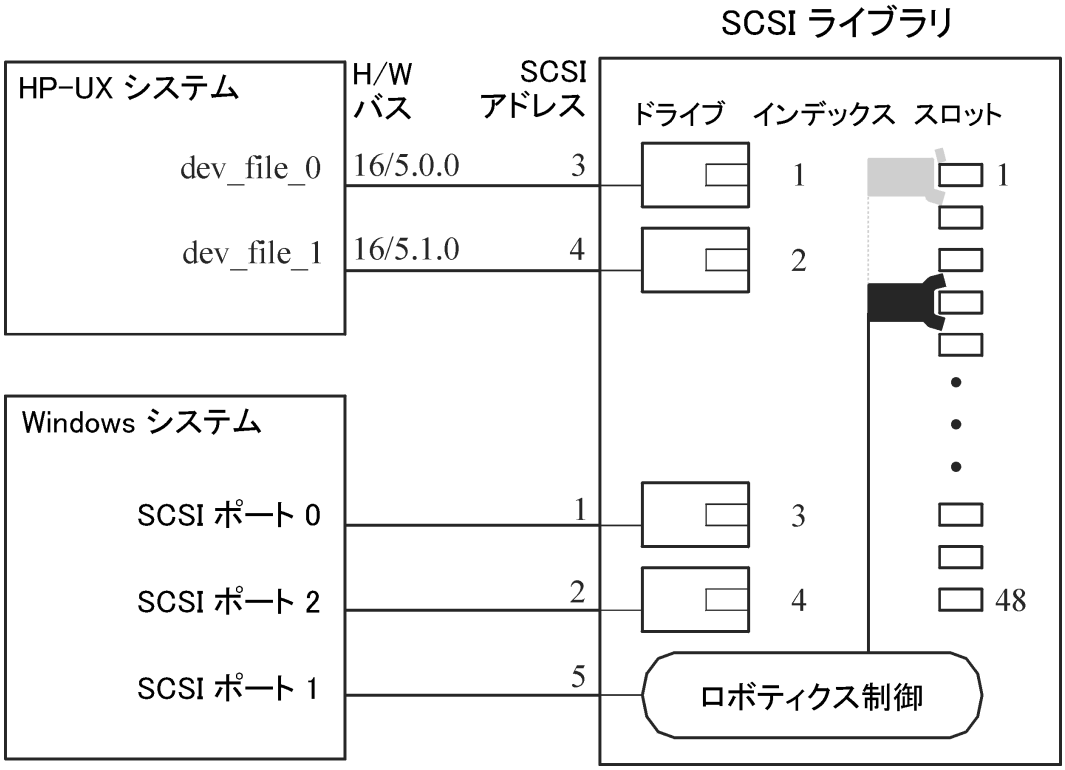
  ドライブが汚れていると、メディア上にデータを正しく書き込めず、バックアップが失敗する可能性があるため、ドライブをクリーニングするまではバックアップを続行できないようになっています。

複数システムによるライブラリの共有

ライブラリの共有とは

デバイス共有機能を利用して、物理ライブラリ内の各ドライブを、個別のシステムに接続することも可能です。これらのシステムでは、ライブラリへのローカルバックアップを実行できます。この結果、バックアップのパフォーマンスは非常に向上し、ネットワークトラフィックは軽減されます。この機能を使用するには、ライブラリ内の各ドライブを、個別のSCSIバスに接続できなければなりません。性能の高いライブラリをこのような形に構成すると、個々のドライブで、各システムからのデータストリームを受け取れるようになるため、性能が非常に向上します。Data Protectorでは、内部処理として、ロボティクスコマンドがロボティクスを管理するシステムにリダイレクトされます。

ドライブを複数のシステムに接続



制御プロトコルとData Protector Media Agent

ライブラリのドライブは、Data Protector Media Agent (General Media AgentまたはNDMP Media Agent)をインストールしている別のシステムと物理的に接続できなければなりません。

Data Protectorでは、ドライブの制御に次の2種類のプロトコルが使用されます。

- SCSI—SCSIまたはファイバーチャネル接続ドライブ向け
  このプロトコルは、汎用Media AgentとNDMP Media Agentの両方に実装されています。
- NDMP—NDMP専用ドライブ向け
  このプロトコルはNDMP Media Agentにのみ実装されています。

一方、ライブラリのロボティクス制御には、次の4種類のプロトコルが使用されます。

- ADIC/GRAU—ADIC/GRAUライブラリロボティクス向け
- StorageTek ACS—StorageTek ACSライブラリロボティクス向け
- SCSI—他のライブラリロボティクス向け
- NDMP—NDMPロボティクス向け

この4つのロボティクス制御プロトコルは、汎用Media AgentとNDMP Media Agentの両方にすべて実装されています。

ドライブ制御

ライブラリ内のドライブ制御を担当するData Protectorクライアントであれば、ライブラリ内のロボティクス制御を担当するどのData Protectorクライアントシステムとも通信することができます。この機能は、ドライブ制御担当側クライアントが使用するドライブ制御プロトコルやプラットフォームの種類とは関係ありません。

また、ロボティクス制御担当側クライアントが使用するロボティクス制御プロトコルやプラットフォームの種類とも関係ありません。そのため、さまざまなプラットフォーム上で実行され、それぞれ異なるロボティクス用プロトコルやドライブ用プロトコルを使用している各Data Protectorクライアント間で、サポート対象ライブラリ内のドライブを共有できます。NDMP Media Agentは、NDMPサーバーのバックアップを制御するクライアントシステム(NDMP専用ドライブ向けに構成されたクライアントシステム)上にのみ必要です。その他のケースでは、2種類あるData Protector Media Agentのどちらを使用しても構いません。

ドライブ制御に必要なData Protector Media Agent、下は、ライブラリに複数のクライアントシステム間で共有されるドライブがある場合について、そのライブラリのドライブ制御を担当するクライアントシステムに必要なData Protector Media Agent (General Media AgentまたはNDMP Media Agent)を示したものです。

ドライブ制御に必要なData Protector Media Agent

	ドライブ制御プロトコル	
	NDMP	**SCSI**
ロボティクス制御プロトコル (ADIC/GRAU、StorageTek ACS、SCSI、NDMP)	NDMP Media Agent	NDMP Media AgentまたはGeneral Media Agent

ロボティクス制御

ライブラリのロボティクスを制御するData Protectorクライアントシステムには、ライブラリ内のドライブで使われているドライブプロトコルの種類(NDMPまたはSCSI)にかかわらず、General Media AgentまたはNDMP Media Agentのどちらをインストールしても構いません。

ロボティクス制御に必要なData Protector Media Agent、下は、ライブラリに複数のクライアントシステム間で共有されるドライブがある場合について、そのライブラリのロボティクス制御を担当するクライアントシステムに必要なData Protector Media Agent (General Media AgentまたはNDMP Media Agent)を示したものです。

ロボティクス制御に必要なData Protector Media Agent

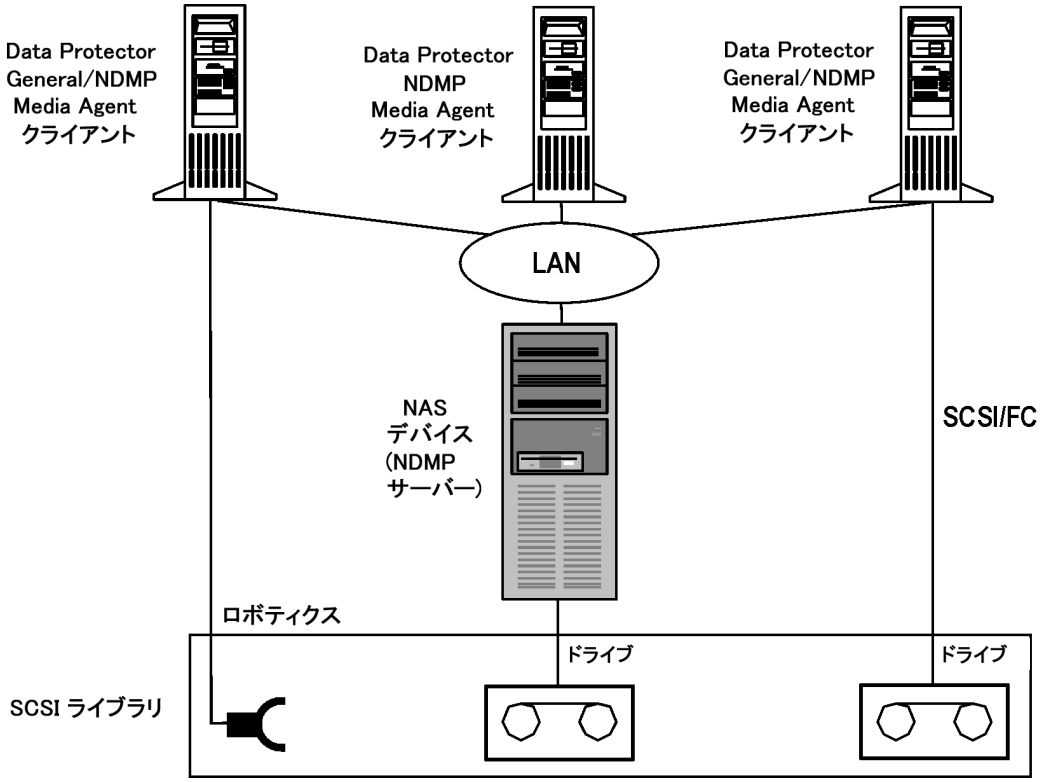
	ロボティクス制御プロトコル			
	ADIC/GRAU	**StorageTek ACS**	**SCSI**	**NDMP**
ドライブ制御プロトコル (NDMP、SCSI)	NDMP Media AgentまたはGeneral Media Agent	NDMP Media AgentまたはGeneral Media Agent	NDMP Media AgentまたはGeneral Media Agent	NDMP Media AgentまたはGeneral Media Agent

一般的な構成例

SCSIライブラリの共有(ロボティクスをData Protectorクライアントシステムに接続)、次のページからADIC/GRAUライブラリまたはStorageTek ACSライブラリの共有、ページ 121は、ライブラリのドライブを共

有する構成と、そのような構成でのData Protector Media Agentの分散に関する例を示しています。

SCSIライブラリの共有(ロボティクスをData Protectorクライアントシステムに接続)

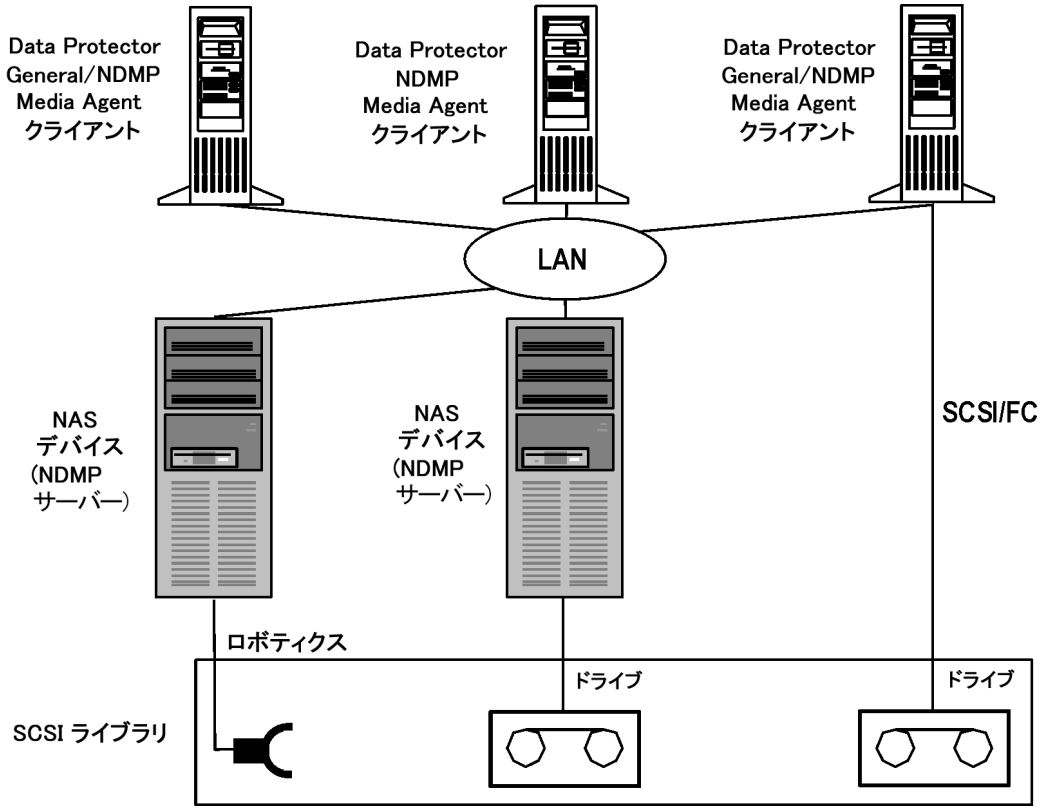


SCSIライブラリの共有(ロボティクスをData Protectorクライアントシステムに接続)、上に示すSCSIライブラリのロボティクスは、General Media AgentまたはNDMP Media Agentのインストールされ Data Protectorクライアントシステムに接続され、そのクライアントシステム上に構成されています。このクライアント上のGeneral Media AgentまたはNDMP Media Agentは、SCSIロボティクス制御プロトコルを使用します。ロボティクスを接続したData Protectorクライアントシステムに、さらに1つ以上のドライブを接続することも可能です。

ライブラリ内のNDMP専用ドライブは、NDMP Media Agentがインストールされ Data Protectorクライアントシステム上に構成されています。このクライアント上のNDMP Media Agentは、NDMPドライブ制御プロトコルを使用します。

ライブラリ内のもう1つのドライブは、General Media AgentまたはNDMP Media Agentのインストールされ Data Protectorクライアントシステムに接続され、このクライアントシステム上に構成されています。クライアント上のGeneral Media AgentまたはNDMP Media Agentは、SCSIドライブ制御プロトコルを使用します。

SCSIライブラリの共 有 (ロボティクスをNDMPサーバーに接 続)



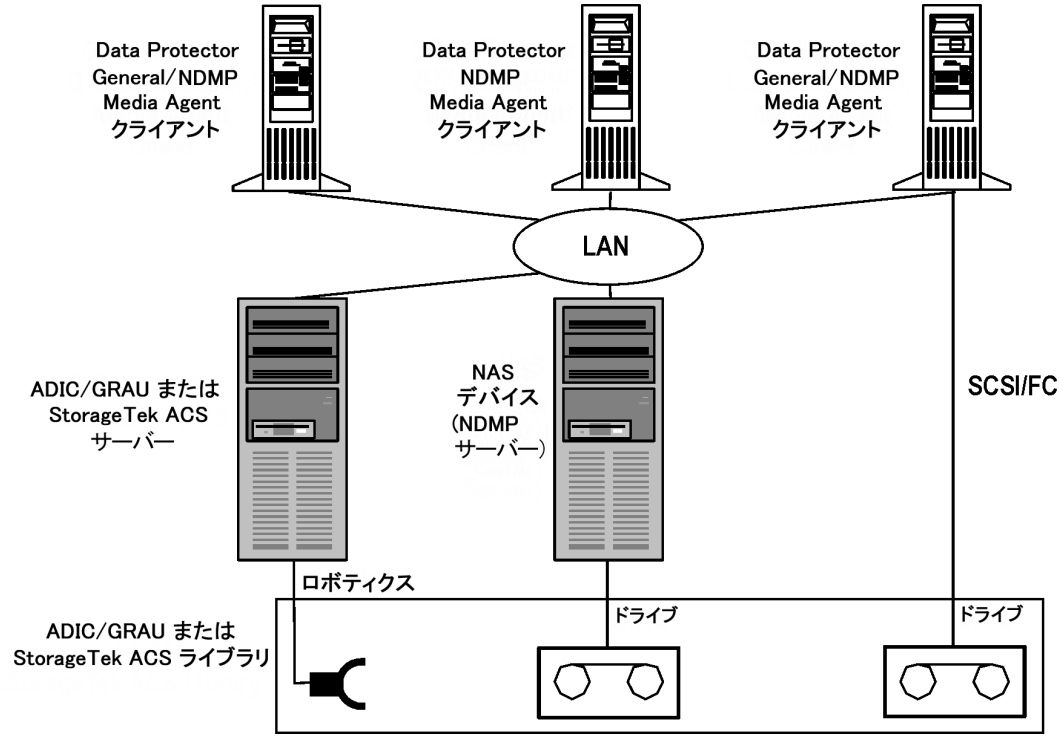
SCSIライブラリの共 有 (ロボティクスをNDMPサーバーに接 続)、上 に示 すSCSIライブラリでは、ライブラリのロボティクスがNDMPサーバーに接 続 され、General Media AgentまたはNDMP Media Agentのインストールされ たData Protectorクライアントシステム上 に構 成 されています。このクライアント上 のGeneral Media AgentまたはNDMP Media Agentは、SCSIロボティクス制 御 プロトコルを使 用 します。ロボティクスを接 続 したNDMPサーバーに、さらに1つ以 上 のドライブを接 続 することも可 能 です。

> **重 要 :**
> ロボティクスを接 続 したNDMPサーバーにNDMP専 用ドライブも接 続 する場 合 は、ロボティクスとNDMP専 用ドライブを担 当 するData Protectorクライアントシステムに、必 ずNDMP Media Agentをインストールしなければなりません。これは、NDMP専 用ドライブの制 御 に、NDMPドライブ制 御 プロトコルが使 用 されるためです。

ライブラリ内 のNDMP専 用ドライブは、NDMP Media AgentがインストールされたData Protectorクライアントシステム上 に構 成 されています。このクライアント上 のNDMP Media Agentは、NDMPドライブ制 御 プロトコルを使 用 します。

ライブラリ内 のもう1つのドライブは、General Media AgentまたはNDMP Media Agentのインストールされた Data Protectorクライアントシステムに接 続 され、このクライアントシステム上 に構 成 されています。クライアント上 のGeneral Media AgentまたはNDMP Media Agentは、SCSIドライブ制 御 プロトコルを使 用 します。

ADIC/GRAUライブラリまたはStorageTek ACSライブラリの共有



ADIC/GRAUライブラリまたはStorageTek ACSライブラリの共有、上に示すADIC/GRAUライブラリ(またはStorageTek ACSライブラリ)では、ライブラリのロボティクスがADIC/GRAUサーバー(またはStorageTek ACSサーバー)に接続され、General Media AgentまたはNDMP Media Agentのインストールされ たData Protectorクライアントシステム上に構成されています。このクライアント上のGeneral Media AgentまたはNDMP Media Agentは、ADIC/GRAUロボティクス制御プロトコルを使用します。ADIC/GRAUサーバーやStorageTek ACSサーバーに、さらに1つ以上のドライブを接続することも可能です。

ライブラリ内のNDMP専用ドライブは、NDMP Media Agentがインストールされ たData Protectorクライアントシステム上に構成されています。このクライアント上のNDMP Media Agentは、NDMPドライブ制御プロトコルを使用します。

ライブラリ内のもう1つのドライブは、General Media AgentまたはNDMP Media Agentのインストールされ たData Protectorクライアントシステムに接続され、このクライアントシステム上に構成されています。クライアント上のGeneral Media AgentまたはNDMP Media Agentは、SCSIドライブ制御プロトコルを使用します。

ディスクベースのバックアップデバイス

この項では、ディスクへのデータのバックアップに関連する概念と、このようなバックアップを支える技術について説明します。また、Data Protectorでサポートされるディスクツーディスクのバックアップの構成についても紹介しています。

企業の営業日には、一日を通して、多くのアプリケーションやデータベースにより、既存のファイルに小規模な変更が頻繁に加えられたり、ビジネスに不可欠なデータを含んだ新しいファイルが大量に作成されたりしています。これらのファイルは、その内容を失うことがないように、直ちにバックアップしなければなりません。このような条件の下では、大量のデータを保存でき、アプリケーションやデータベースの実行を妨げることがない高速メディアが、データ保存のために必要となります。

ディスクベースのデバイスの利点

ディスクベースのデバイスによるバックアップは、さまざまな状況下で効果を発揮します。ディスクベースのデバイスは、実際には特定のファイルまたは特定のディレクトリです。テープにバックアップする代わりに、あるいはテープへのバックアップに加えて、このファイルにデータをバックアップすることができます。ディスクベースのデバイスを使用するメリットが特に大きいと思われる状況を、以下に示します。

- 多くのアプリケーションとデータベースでは、基幹業務データを含むファイルが、継続的に数多く生成または変更されます。こうした状況下でデータを完全に復元できるようにするためには、関連するファイルを頻繁にバックアップしなければなりません。

  通常、このような環境では、テープデバイスでデータストリームを絶え間なく受信することがないため、テープデバイスをスタート/ストップモードで動作させる必要があります。そのため、テープデバイスにより、関連ファイルへのアクセスが制限される可能性があります。また、バックアップデバイスの耐用年限も大幅に短縮されてしまいます。

  代わりにディスクベースのデバイスにバックアップするようにすると、上記の制限事項を解消できます。短期間のバックアップソリューションとしては、ディスクベースのデバイスだけで十分です。一方、長期にわたるバックアップソリューションが必要な場合は、ディスクベースのデバイスに保存したデータを定期的にテープに移すことで、ディスクスペースを解放するという手法が有効です。このプロセスを、**ディスクステージング**と呼びます。
- 大容量の高速ディスクドライブと低速のテープドライブを併用できる環境では、最初にディスクベースのデバイスを使ってバックアップを実行し、その後ディスク上のデータをテープに移すという方法を採ることで、バックアップにかかる時間を大幅に短縮できます。
- バックアップにディスクベースのデバイスを使用すると、**合成バックアップ**などのアドバンストバックアップ方針の利点を活用することができます。
- ディスクベースのデバイスは、最近バックアップしたデータを速やかに復元するのに便利です。たとえば、復元を迅速かつ簡単に行えるように、バックアップデータをディスクベースのデバイスに24時間保管しておくことができます。
- 装置の特性により、ディスクベースのデバイスはテープよりも速やかに使用を開始できます。ディスクベースのデバイスを使用するときには、テープのマウントとアンマウントのような操作を行う必要がありません。またディスクベースのデバイスではテープドライブのような初期化時間が不要なため、特に少量のデータをバックアップまたは復元する場合に、その違いを実感できます。少量のバックアップや復元ではメディアのロードとアンロードにかかる時間の割合が大きくなりますが、ディスクベースのデバイスを使用すると、このロードとアンロードが不要になります。ディスクベースのデバイスを使用する利点は、増分バックアップからの復元を実行するときに、いっそう明らかになります。
- テープの障害やマウントの失敗といったメディアに関するトラブルを最小限に抑えられます。ディスク障害からデータを保護するために、RAIDディスク構成を導入することも可能です。
- テープを取り扱う必要がないため、オーバーヘッドコストが削減されます。
- ディスクベースの記憶スペースは、テープベースの記憶装置に比べても、総じて低価格化が進んでいます。

Data Protector ディスクベースのデバイス

Data Protectorでは、以下のディスクベースのデバイスをサポートしています。

- スタンドアロンファイルデバイス
- ファイルジュークボックスデバイス
- ファイルライブラリデバイス

スタンドアロンファイルデバイス

スタンドアロンファイルデバイスは、ディスクベースのバックアップデバイスのうち最も単純なものです。1つのスロットで構成されており、このスロットにデータをバックアップできます。このデバイスのプロパティは、いったん構成すると変更できません。最大容量は2TBです(このデバイスが動作するオペレーティングシステムで、このファイルサイズがサポートされていることが前提となります)。

ファイルジュークボックスデバイス

ファイルジュークボックスデバイスは、特殊なData Protectorジュークボックスデバイスです。ジュークボックスデバイスは、光学式メディアかファイルメディアのいずれか一方にバックアップするように構成されます。ファイルメディアをバックアップに使用するジュークボックスデバイスを、ファイルジュークボックスデバイスと呼びます。ジュークボックスのバックアップ用メディアの種類は、デバイスの構成の際に指定します。

ファイルジュークボックスデバイスは複数のスロットで構成されており、これらのスロットにデータをバックアップできます。構成は2段階の作業になっています。まずファイルジュークボックスデバイスを作成し、次に1つまたは複数のドライブをそのデバイス用に構成します。デバイスを構成した後、デバイスのプロパティを変更することができます。ジュークボックスデバイスの各スロットの最大容量は、2TBです。デバイス全体の最大容量は、次のとおりです。

```
Number of slots * 2 TB
```

ファイルライブラリデバイス

ファイルライブラリデバイスは、ディスクベースのバックアップデバイスのうち最も複雑なものです。**ファイルデポ**と呼ばれる複数のスロットで構成されており、これらのスロットにデータをバックアップできます。ファイルライブラリデバイスの構成は、1段階の作業で完了します。ファイルライブラリデバイスのプロパティはいつでも変更できます。デバイス全体の最大容量は、そのデバイスが配置されているファイルシステムの最大保存可能容量と同じです。各ファイルデポの最大容量は2TBです。ファイルデポは、必要に応じて自動的に作成されます。

ファイルライブラリデバイスには、高度なディスクスペース管理機能が備わっています。この機能は、データをファイルライブラリデバイスに保存するときに発生する可能性がある問題を予測します。空きディスクスペースの量が、デバイスが機能するために最低限必要と定められている量に近づくと、イベントログに警告メッセージが書き込まれます。この警告を利用すると、ディスクスペースを適切なタイミングで解放して、データを引き続き保存できるようにすることができます。ファイルライブラリデバイスに割り当てられたスペースがすべて使用されると、警告メッセージが、問題解決の方法とともに画面に表示されます。

ファイルライブラリデバイスでは、バックアップに必要なスペースが1つのファイルデポの使用可能スペースよりも大きい場合、自動的に追加のファイルデポが作成されます。

推奨ディスクバックアップデバイス

ディスクベースのバックアップデバイスとしては、ファイルライブラリデバイスを優先的に使用することをお勧めします。ファイルライブラリデバイスは一連のディスクベースのバックアップデバイスの中で、最も柔軟性があり、高度なデバイスです。このデバイスは使用中いつでも再構成することができ、他のディスクベースのバックアップデバイスよりも高度なディスクスペース管理能力を備えています。さらに、合成バックアップのようなアドバンストバックアップ戦略を用いることもできます。

ファイルライブラリデバイスの機能の詳細については、『*HPE Data Protectorヘルプ*』のキーワード「ファイルライブラリデバイス」で表示される内容を参照してください。

データフォーマット

ディスクベースデバイス用のデータフォーマットは、テープ用のデータフォーマットに基づいています。Data Protectorでは、ディスクベースのデバイスにバックアップデータを書き込む前に、そのデータをテープ用のフォーマットに変換します。Smart Cacheデバイスは、データをネイティブフォーマットで保存し、実際のデータとメタデータを分離します。

仮想フルバックアップに使用するファイルライブラリでは、分散ファイルメディア形式を使用する必要があります。この形式は、デバイスのプロパティで選択します。

ディスクへのバックアップデバイス

ディスクへのバックアップ(B2D)デバイスは、重複排除、クラウドストレージ、VMware固有の拡張機能など、より高度な機能を提供します。

HPE Data Protectorには、ディスクへのバックアップデバイスと重複排除が統合されています。重複排除のサポートにより、ディスクへのバックアップデバイスという新たなデバイスの種類、HPE StoreOnceソフトウェア重複排除、HPE StoreOnce Backupシステム、Smart Cache、EMCデータドメインブーストの4つのインターフェイスの種類など、いくつかの新たな概念がData Protectorに導入されています。本書では、ディスクへのバックアップデバイスと重複排除について詳しく説明します。

*ディスクへのバックアップデバイス*は、物理的なストレージディスクにデータをバックアップし、マルチホスト構成をサポートするデバイスで、HP StoreOnceソフトウェア重複排除、StoreOnceバックアップシステム、Smart Cache、EMCデータドメインブーストなど、さまざまなバックエンドに対応しています。本書では、*重複排除技術*の基本原理についても説明します。

Data Protectorは、重複排除に対応した次のバックエンドに対応しています。

- HPE *Data Protectorのソフトウェア重複排除* では、ほぼすべての業界標準ハードウェアでターゲット側の重複排除が行えます。また、さまざまなハードウェア構成に導入できることから、既存ソリューションより優れた柔軟性を発揮するほか、エンタープライズクラスの拡張性を備えています。

  Data Protectorは極めて効率的なHPE StoreOnceエンジンを採用しているため、Data Protectorのソフトウェア重複排除におけるメモリの使用効率が非常に優れています。このため、重複排除をアプリケーションサーバーやバックアップサーバーに導入しても、アプリケーションのパフォーマンスが低下することはありません。また、Data Protectorのソフトウェア重複排除は、仮想マシンにも導入できるうえ、極めて高いスループットを実現します。
- *HPE StoreOnceバックアップシステムデバイスは、重複排除をサポートするディスク間(D2D)バックアップデバイスです。*
- *Smart Cacheデバイスは、ディスクへのバックアップデバイスの一種で、VMwareバックアップからの非段階的な復元を可能にします。*
- *EMCデータドメインブーストデバイス*は、重複排除をサポートするD2Dバックアップデバイスです。

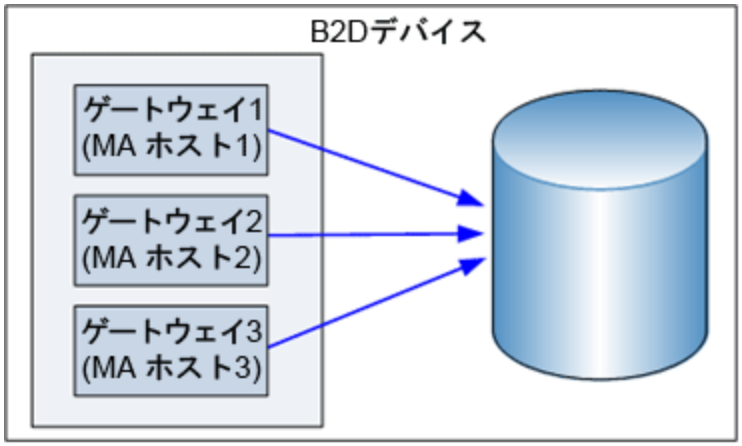
対応システムの完全な詳細については、http://support.openview.hp.com/selfsolve/manualsで、HPE Data Protectorに関する最新のサポート一覧を参照してください。Data Protectorの全般的な操作手順については、『HPE Data Protectorヘルプ』を参照してください。

B2Dデバイスの操作と詳細

ディスクへのバックアップ(B2D)デバイスでは、物理ストレージディスクにデータがバックアップされます。B2Dデバイスは、複数ホスト構成をサポートしています。1台の物理ストレージディスクには、ゲートウェイと呼ばれ

る複数のホスト経由でアクセスできます。各ゲートウェイは、Media AgentコンポーネントがインストールされたData Protectorクライアントです。B2Dデバイスは論理デバイスで、ゲートウェイとストアから構成されます。下図に、複数のゲートウェイを持つ汎用B2Dデバイスとストアとの関係を示します。

B2Dデバイス(論理ビュー)

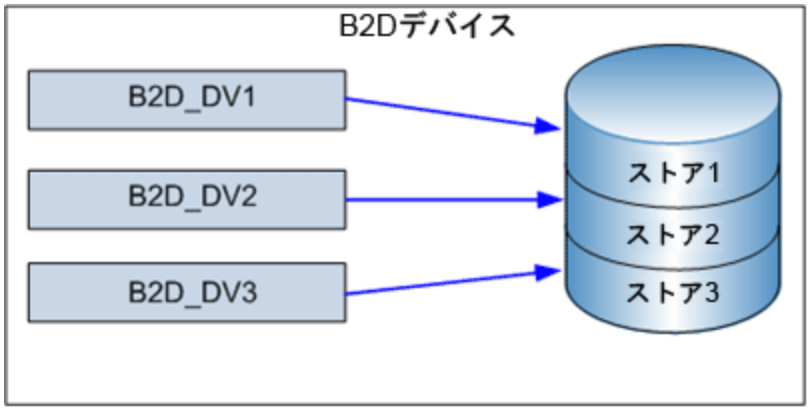


物理ストレージは、ハードディスクのパーティショニングのように、特定のストレージセクションを表す個々のストアにも分割できます。1つのストアはネットワークパスで表され、バックアップアプリケーションが使用します。これらのパラメーターは、他のデバイス構成情報とともに、IDBのデバイス構成に格納されます。

物理ストレージディスク上の個々のストアにアクセスできるのは1台のB2Dデバイスのみですが、複数のB2Dデバイスが同じ物理ストレージ上の異なる複数のストアにアクセスすることはできます。

> **注:**
> 物理ディスクの制限事項の一部は、クラウドベースのデバイスには該当しません。

同じ物理ディスク上の3つの異なるストアにアクセスする3つのB2Dデバイス



B2Dデバイスを構成する際には、次の点に注意してください。

- 1つの重複排除サーバーノード上で複数のストアを構成できます。これらのストアは、CPU、メモリ、ディスクI/O、重複排除システムあたりの接続数といったリソースを共有します。ただし、個々のストアはそれぞれ独自の重複排除ドメインとして表され、異なるストアにまたがる重複排除は行われません。

- 個々のストアには専用のB2Dデバイスを個別に構成する必要があります。同じB2Dデバイスに2つのストアを構成することはできません。
- 個々のB2Dデバイスは、1つのストアを排他的に使用する必要があります。複数のB2Dデバイスが同じストアにアクセスすることはできません。

特定のゲートウェイで起動できるMedia Agentの数は、次によって定義されます。

- ゲートウェイ上限値。各B2Dゲートウェイは、平行ストリームの最大数までに制限されています。この上限値はGUIで指定します。
- ストアへの接続上限値。個々のB2Dデバイスでは、ストアあたりの最大接続数が決められています。この上限値はGUIで指定します。この値が指定されていない場合、使用可能な最大数が使用されます。
- 物理ストレージディスクの物理接続上限値。この値は物理ストアから読み出されます(下記を参照)。
- 実行中の動作によっては、次の入力パラメーターに従って、各Session Managerがゲートウェイ上のMedia Agentの数を調整します。
    - バックアップ対象のオブジェクトの数
    - オブジェクトの場所
    - 物理接続上限値
- オブジェクトの場所
- 物理接続上限値

物理接続上限値(物理的に可能な最大数)については、セッション中に検証が行われます。GUIに入力された値は使用可能な接続数と照合され、物理上限値を超えている場合には、物理上限値が使用されます。物理接続上限値はGUIでは設定できません。(注:最大値を使用する場合は、オプションのチェックを外してください。)アクティブなデータ接続がない場合、物理接続の上限値は100です。この上限値に達した後はデータ接続をしても失敗します。

大容量の物理ストアが小容量のストア(前述のストア1、ストア2、ストア3)に分割されている場合は、各分割ストアに対して接続数の上限が決められています。

デバイスのロック

デバイスのロックは、複数のシステムの間で同じデバイスを共有している場合に、そのデバイスに対する複数のシステムからの同時アクセスを防ぐことを目的としています。B2Dデバイスでは決められた接続上限値を守る必要があり、ゲートウェイあたりの最大並行システム数とストアあたりの最大接続数が、これらの接続上限値にあたります。Data Protectorでは、両方のリソースのロックの数が保持されており、上限に達するとロック要求が拒否されます。ロック要求が認められた場合は、ゲートウェイとストアの両方のロックの数が増加します。ロックの数は、ゲートウェイのロックが解除されると減少します。これにより、B2Dの接続上限値が、特定のセッション中だけでなくCell Manager全体で考慮されるようになっています。

オブジェクト集約

ゲートウェイおよびゲートウェイ/ストア/デバイスの接続上限値に対応するには、オブジェクトのコピーおよび集約機能を次のように設定します。

- B2Dデバイスをソースとして使用する場合は、オブジェクトのコピー用に最低1個、オブジェクトの集約用に最低n個の接続を確保します。nは集約に使用するソースメディアの数を表します(詳細は次の段落を参照)。
- B2Dデバイスをターゲットとして使用する場合は、最低m個の接続を確保します。mはコピー/集約仕様の最小デバイス設定を表します。他の種類のデバイスを並行して使用する場合は、最小設定に達するようにCSM(Copy and Consolidation Session Manager)が調整を行い、調整できない場合はセッションを終了します。

バックアップ済みのデータ(フルバックアップおよび増分バックアップ)を集約する際には、使用可能な接続がストアに十分あることを確認してください。わかりやすくするために、6個の増分バックアップの集約セッションを例に考えてみます。この場合、1(フル)+6(増分)+1(ターゲット)となり、接続数が8になります。集約セッションは、6〜10個の増分バックアップに対して毎週実行することをお勧めします。

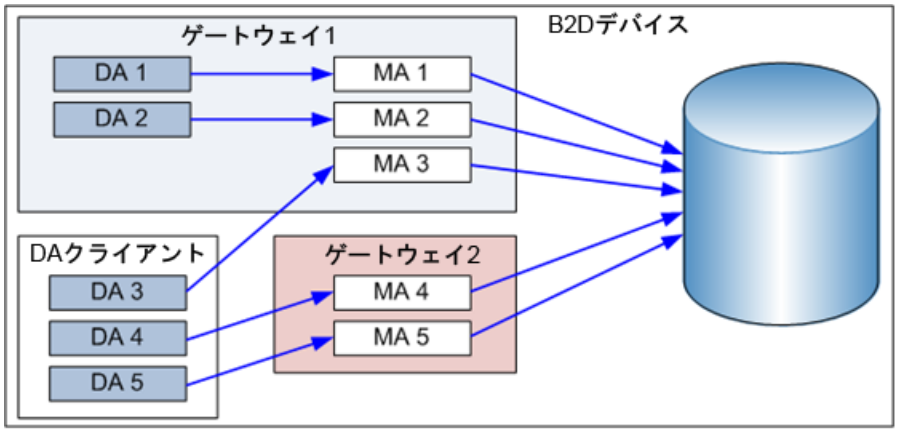
B2Dデバイスを使用したデータのバックアップ

B2Dデバイスへのバックアップは、テープベースのデバイスへのバックアップとほぼ同じです。主な違いとして、Session Managerが定義済みのゲートウェイ上にMedia Agentを動的に生成する点と、Media Agentがデバイス固有のAPI経由でデバイスと通信を行う点が挙げられます。

以下に、1台のB2Dデバイスと2台のゲートウェイ(ゲートウェイ1およびゲートウェイ2)を使用したバックアップセッションの例を示します。5つのオブジェクト(DA1〜DA5)がバックアップ対象です。ここで、2つのオブジェクトがゲートウェイ1のローカルに存在し、3つのオブジェクトが両ゲートウェイのリモートに存在します。物理ストレージへの接続数は6です。バックアップ仕様は次のように構成されています。

- 負荷調整(最大)パラメーターは5(セッション中にMedia Agentを5つまで使用可能)。
- B2Dデバイスの接続上限値は10。
- 両ゲートウェイの接続上限値は5。

2つのゲートウェイ(ローカルおよびリモートオブジェクト)を使用したバックアップ構成の例



上記の構成に基づき、Session ManagerがMedia Agentを動的に5つ起動します。5つのMedia Agentは、ゲートウェイが2台使用されているため、2台のゲートウェイに負荷が分散されます。Disk Agentは、ゲートウェイ1のローカルDisk Agentがそのゲートウェイ上のMedia Agentに割り当てられるよう、負荷調整アルゴリズムによってMedia Agentの間で負荷が分散されます。他のDisk Agentについては、すべてのMedia Agentに対してリモートのため、2台のゲートウェイの間で負荷の調整が行われます。

バックアップ仕様を作成する際には、B2Dデバイスをターゲットとして選択することができます。また、特定のゲートウェイの選択も可能です。B2Dデバイスをターゲットデバイスとして選択した場合は、最新のデバイス構成情報に基づいて、すべてのゲートウェイがバックアップ処理中に選択されます。ただし、この選択は

負荷調整型のバックアップでのみ行えます。静的バックアップ(負荷未調整型)の構成時には、各オブジェクトはゲートウェイにのみ割り当て可能で、B2Dデバイスに割り当てることはできません。

B2Dデバイスでは、特殊なデータ形式を使用して読み/書きアクセスの高速化と重複排除率の向上を実現しています。この形式では、バックアップ用に実データからメタデータが分割されます。データ形式は、B2Dデバイスの選択時に自動的に設定され、B2Dデバイスに対してのみ使用されます。

ゲートウェイ

ディスクへのバックアップ(B2D)デバイスは、事前に定義したゲートウェイにアクセスするように構成する必要があります。ゲートウェイ(正しくは*ゲートウェイクライアント*)は、Media Agentコンポーネントがインストールされたクライアント(64ビットシステム必須、下記を参照)です。ゲートウェイは、セル内の他のクライアントと同様にバックアップできます。ゲートウェイは一意の名前で識別され、ゲートウェイ名にはデバイスから物理ストアへのネットワークパス名が含まれます。デフォルトの命名規則では、ファイルライブラリと似ていて、*DeviceName_gwnumber*となります。ゲートウェイはGUIのドロップダウンリストから選択しますが、ゲートウェイとして作動できないクライアントは一覧には表示されません。

ゲートウェイの接続は、デバイスとゲートウェイ間の通信を確保する目的で、検証(チェック)することができます。何らかの理由でゲートウェイが使用できない場合は、エラー状態が表示されます。ゲートウェイは、このほかにも次のプロパティと機能を備えています。

- ゲートウェイ名や拡張オプションなど、ゲートウェイのプロパティは[ゲートウェイのプロパティ]ダイアログで変更できます。複数のゲートウェイのプロパティを同時に変更可能です。
- ゲートウェイは有効または無効にできます。ゲートウェイを有効または無効にするには、[デバイス]リストで有効または無効にするゲートウェイを右クリックし、[ゲートウェイを使用可能にする]または[ゲートウェイを使用不可能にする]を選択します。
- Media Agentコンポーネントは64ビットクライアントシステムにのみインストールできます。したがって、ゲートウェイとして指定するクライアントには、必ず64ビットシステムを使用してください。
- 個々のゲートウェイは、シングルセッションまたはマルチセッションを問わず、複数のMedia Agentの同時起動が可能なホストとして表されます。このため、ゲートウェイはMedia Agentホストと呼ばれることがあります。
- ライブラリベースのデバイスに例えると、B2Dデバイスはライブラリ、ゲートウェイはライブラリ内のドライブに相当します。

ソース側ゲートウェイ

各デバイスには、ソース側ゲートウェイを1台構成することもできます。この(仮想)ゲートウェイは、ソース側重複排除が有効になっている場合、バックアップ済みシステム上で自動的に拡張されます。このようなゲートウェイは、デフォルトで「*デバイス名*_Source_side」と命名されます。

StoreOnceライブラリ(重複排除ストア)

StoreOnceライブラリ(または重複排除ストア)は、StoreOnceソフトウェア重複排除インターフェイスが使用する物理ストレージディスクです(StoreOnceソフトウェア重複排除には、HPE Labsが開発したHPE StoreOnce Backupシステム技術が採用されています)。物理ディスクのサポート容量は、20TB(の重複排除済みデータ)です。通常、重複排除率が20:1の場合、この値は400TBのデータのバックアップに相当します。複数のストアが使用されている場合でも、サポートする合計容量は20TBと変わりません。CLIコマンドの詳細については、『HPE Data Protectorコンセプトガイド』を参照してください。

1つのStoreOnceソフトウェア重複排除システムに複数の重複排除ストアをホストできます。この場合、ストアは同じルートディレクトリを共有します。Data Protectorではボリュームあたり最大32個のストアがサポートされていますが、ホストするストアを1個のみにするとパフォーマンスが最高(重複排除率に基づく)になります。重複排除ストアの構成は単一のステージですべて行えます。

重複排除ストアからの期限切れバックアップデータの削除

Data Protectorでは、クリーンアップセッションが自動で定期的に開始され、物理ストア内のバックアップ済みデータが削除されます。非保護データの削除には、数種類の方法が採用されています。

- 非保護のB2Dバックアップオブジェクトの手動削除

  Data Protectorでは、ストア内にある非保護のバックアップ済みオブジェクトの一覧が作成されます。削除時には、まずストアからオブジェクトが削除され、次にメディア(オブジェクトの)情報がData Protectorのデータベースから削除されます。ただし、ストアからメディアを削除しても、単にデータの廃止がストアに指示されるだけで、ディスクスペースが解放されることはありません。
- 非保護のB2Dバックアップオブジェクトの自動削除

  この方法は上記と同じですが、Data Protectorによって自動で定期的に行われます。削除の間隔は、グローバルオプションファイルで設定できます。
- スロット削除直後の削除

  スロットを削除すると、IDBからのスロットの削除、スロット内のオブジェクトの削除、およびストアからのスロット自体の削除が行われます。この動作は、リサイクルと削除の動作と同じです。

非保護のB2Dバックアップオブジェクトを削除すると、関連するスロットが直ちに削除されます。アイテムを削除しても、ディスクスペースは直ちに解放されません。期限切れのファイルと非保護のチャンクは次回のメンテナンス時に削除され、その結果ディスクスペースが解放されることがあります。

> **注:**
> 冗長データとは、ストア内で参照されなくなったデータを指します。データが期限切れになると、保護日付も期限切れとなります。

重複排除ストアからの冗長データの消去

Data Protectorは、ストレージスペースを最適化するスペース管理(メンテナンス)ユーティリティを備えています。メンテナンスユーティリティはデフォルトで起動され、バックグランドで稼働します。

データチャンクは、インデックステーブルで参照されなくなると冗長化しますが、データがストアから自動的に削除されることはありません。削除はメンテナンスユーティリティの実行に行われ、ディスクスペースが解放されます。

StoreOnceソフトウェアストアの安定性

StoreOnceソフトウェア重複排除は、ストアの整合性を検証するメカニズムを内蔵しています。データの損失を防ぐ(最少に抑える)には、次の点に注意してください。

- 無停電限現装置(UPS)を使用してください。これにより、StoreOnceソフトウェア重複排除システムのフォールトトレランスを強化できます。UPSを使用すると、主電源が落ちた場合でも、コンピューターの

動作を短時間維持できるほか、電力サージからも保護できます。

- ストアはRAIDアレイとして構成する必要があります。重複排除ストアのディレクトリ構造上の理由から、1台のディスクが壊れると、ストア全体が使用できなくなります。ハードウェアRAIDの使用をお勧めします。
- クリティカルなデータに対しては、重複排除ストアからテープへのオブジェクトコピーを行うことをお勧めします。バックアップ中は、ストアへの書き込みを行わないでください。

重複排除の統計情報

重複排除を使用したバックアップセッションでは、オブジェクトバージョンが完了するたびに、たとえば次のようなバックアップ統計情報がData Protectorに表示されます。

```
Source-side Deduplication Statistics for dd2.company.com:/C "C:".

      Using device: "b2d_Source_side [GW 13148:3:649335383]@dd2.company.com":

           Mbytes Total: .................        35 MB

           Mbytes Written to Disk: .......         1 MB

           Deduplication Ratio: ..........      35.0 : 1
```

統計情報には次の情報が含まれます。

- The type of the deduplication (source-side, target-side, and server-side)
- Information about the device.
- Mbytes Total: オブジェクトバージョン(バックアップするデータ)の元のサイズ
- Mbytes Written to Disk: 重複排除後にディスクに書き込まれる実サイズ(1MB未満の場合は「1MB」と表示されます)
- Deduplication Ratio:「ディスクへの書き込みデータ量[MB]」で割った「合計容量[MB]」(以下の注記を参照)

重複排除率を解釈する際には、次の点に注意してください。

- 「ディスクへの書き込みデータ量[MB]」の値が1MB未満の場合は1MBに切り上げられます(切り上げを行わないと非現実的な計算結果となる)。
- 通常、重複排除率は10:1～20:1のオーダーを想定してください。誤った比率(4435:1など)は無視してください。この現象は、分母(ディスクへの書き込みデータ量[MB])の数値が非常に小さい場合に発生します。

バックアップの統計情報に表示される比率は現在のセッションに適用されます。CLIに表示される比率はストア全体に適用されます。

重複排除率

重複排除を使用して削減したストレージ容量は、通常、比率として表現されます。重複排除前のバックアップデータの合計が、重複排除済みデータに必要なストレージの実容量と比較されます。たとえば比率が10:1の場合は、重複排除を使用しなかった場合の10倍のデータが格納されることを表します。

重複排除率を最も大きく左右する要因を次に示します。

- データ保持期間。
- バックアップ間の変更量。
- ファイルサイズ。ファイルが小さいと重複排除率が低くなることがあります。

ただし、特定の環境におけるストレージの削減量は多くの要因によって左右されます。比率は、サマリー画面(デバイスの追加後)、[デバイス]コンテキスト([デバイス] > [ストア])、およびバックアップ操作後のバックアップ統計情報に表示されます(代表的な出力については「重複排除の統計情報、前のページ」を参照)。

より高い重複排除率を実現するため、256 KBのブロックサイズを使用するようにB2Dデバイスを構成することをお勧めします。

制限事項

- データの重複排除はデータのアーカイブには適していません。
- StoreOnceソフトウェアエージェントは、クラスター環境ではサポートされていません。
- 複数のB2Dデバイスによる同一ストアへのアクセスには対応していません。つまり、個々のB2Dデバイスに専用のストアを構成する必要があります。同じストアには2台目のデバイスを構成しないでください。
- バックアップ済みデータ(フルバックアップおよび増分バックアップ)の集約に必要な接続の数が最大接続数を超えている場合、集約できない復元チェーンが終了します。「オブジェクト集約」も参照してください。
- ディザスタリカバリは、ローカルゲートウェイを持つDisk Agentクライアントでサポートされています。ローカルゲートウェイを持つDisk Agentクライアントでディザスタリカバリを実行するには、ディザスタリカバリの設定で[元のネットワーク設定を使用]を選択する必要があります。
- オブジェクトのミラーリングは、ソース側重複排除では対応していません。
- 自動メディアコピーはB2Dデバイスではサポートされていません。
- B2Dデバイス間での複製を有効にする場合、選択した複製先デバイス上の各ストアの接続最大数は、バックアップ仕様で構成した負荷調整の最大値と同数以上に設定する必要があります。
- ソース側ゲートウェイはオブジェクトの集約に選択できません。フルバックアップには、別のゲートウェイが自動的に選択されます。増分バックアップには、別のゲートウェイを手動で選択する必要があります。ゲートウェイは、ソース側ゲートウェイと同じB2Dデバイスに属する必要があります。
- ソース側ゲートウェイはオブジェクトのコピーに選択できません。次のいずれかの操作を行ってください。
  - 読み込むソースデバイスをソース側でないゲートウェイに手動で切り替える。ゲートウェイは、ソース側ゲートウェイと同じB2Dデバイスに属する必要があります。
  - ソース側でないゲートウェイの[プロパティ]ウィンドウで[ポリシー]タブを表示し、[ゲートウェイをオブジェクトコピーのソースゲートウェイとして使用可]を選択する。ソース側ゲートウェイが、このゲートウェイに自動的に切り替わります。
- 暗号制御通信を有効にすると除外処理は行えません。StoreOnceSoftwareデーモンを実行するセルメンバーを保護すると、デーモンは保護済みの接続のみを処理します。
- StoreOnceSoftwareサービス/デーモンは、システム(セルメンバー)に対して暗号制御通信を有効にした後で、手動で再起動する必要があります。
- ファイバーチャネル(FC)で構成されたStoreOnce Backupシステムデバイスへのソース側重複排除バックアップは、FCに接続されたシステムでのみ実行できます。したがって、このバックアップを実行する前に、

システムが次の要件を満たすことを確認する必要があります。

- Data Protector Disk Agentがインストールされていること。
- Data Protector Media Agentがインストールされていること。
- ファイバーチャネル接続が構成されていること。

バックアップ中に、[システムはソース側重複排除の準備ができています]オプションを使用して、ソース側重複排除をサポートしないシステムを除外することができます。ただし、このオプションでは、FC接続を持たないシステムを除外しません。FC接続は、FCで構成されたStoreOnce Backupシステムデバイスに対してソース側重複排除バックアップを実行するための要件の1つです。

システムがFC接続を持つかどうかを検証するには、StoreOnce Backupシステムデバイスを追加する際に、[チェック]をクリックしてゲートウェイを検証します。

- 複製の対象として選択されているデバイスは複製可能である必要があります。
- 複製の対象として選択するソースとターゲットのデバイスの種類が同じである必要があります。
- StoreOnce内で、ソースデバイスとターゲットデバイスが別々のストアに属している必要があります。
- ソースデバイスが少なくとも1つのバックアップ仕様で構成されている必要があります。
- StoreOnceバックアップシステムやデータドメインブーストの場合、ファイバーチャネル(FC)で構成されたデバイスへの複製はサポートされません。ターゲットデバイスは常にIPアドレスで構成する必要があります。
- データドメインデバイスで対話型の複製を実行する場合、複製のために選択できるセッションは一度に1つだけです。
- ソースとターゲットのデータドメインデバイスには同じバージョンのデータドメインOS (DDOS)をインストールする必要があります。詳細については、データドメインのドキュメントを参照してください。

Smart Cache

この項は、今後のリリースに合わせて変更される可能性があります。

Smart Cacheは、ディスクへのバックアップデバイスの一種で、VMwareバックアップからの非段階的な復元を可能にします。Smart Cacheデバイスは、以下のマウントポイントの1つで動作が可能です。

- NAS共有(CIFSおよびNFS)
- ファイルシステムでフォーマットされたディスク(SAN、iSCSI、ローカル)

Smart Cacheデバイスは、GUIを使って構成されます。詳細については、『HPE Data Protectorヘルプ』の「ディスクへのバックアップデバイスを構成する」を参照してください。

> **注:**
> Smart Cacheデバイスは、Windows x64およびLinux x64オペレーティングシステムでのみサポートされます。

> **注:**
> Smart Cacheデバイスは、VMwareバックアップのターゲットとしてのみ利用できます。

> **重要:**
> Smart Cacheデバイスへの暗号化またはAES 256ビット暗号化されたVMwareバックアップとオブジェクトコピーはサポートされていません。ただし、ハードウェア暗号化されたテープデバイスとの間のオブジェクトコピーはサポートされています。

クラウド(Helion)およびクラウド(Azure)デバイス

この項では、クラウド(Helion)およびクラウド(Azure)へのデータのバックアップに関連する概念と、このようなバックアップを支える技術について説明します。

Data Protectorクラウド(Helion)およびクラウド(Azure)のバックアップデバイス

クラウド(Helion)およびクラウド(Azure)のディスクへのバックアップデバイス

Data Protectorは、Cloud資格情報で構成された、クラウド(Helion)およびクラウド(Azure)デバイスとして知られる新しいディスクへのバックアップ(B2D)デバイスをサポートしています。クラウド(Helion)およびクラウド(Azure)デバイスは、WindowsおよびLinuxのMedia Agentホスト上で構成可能です。Media Agentは、オブジェクトコピー操作において、オンプレミスのバックアップデバイスからクラウド(Helion)およびクラウド(Azure)にデータを転送するクラウドゲートウェイとして機能するように改良されています。

これらのオブジェクトコピー操作の実行は、対話型の実行、スケジュールに基づく自動実行、またはポストバックアップジョブアクションとして構成することができます。クラウド(Helion)およびクラウド(Azure)へのオブジェクトコピーを使用すると、バックアップ管理者は、テープを使用しないでバックアップジョブをオフサイトで電子的に複製でき、オフサイトのアーカイブコピーとして使用することもできます。クラウドに転送されるすべてのデータは送信前に暗号化と圧縮が行われ、この状態でクラウドに格納されます。

クラウド(Helion)およびクラウド(Azure)デバイスは、Data Protector GUIを使用して構成されます。詳細については、『*HPE Data Protectorヘルプ*』の「クラウドデバイスを構成する」を参照してください。

> **注:**
> クラウドデバイスのオブジェクトコピーは試験済みであり、以下でサポートされています。
>
> - ソースデバイス: ファイルライブラリデバイスおよびStoreOnceデバイス
> - クラウドHelion: VMwareバックアップ仕様。
> - クラウドAzure: ファイルシステムバックアップ仕様。

ディスクへのバックアップデバイス

ディスクへのバックアップデバイス(本書ではB2Dと略記します)では、重複排除インターフェイスと共に、重複排除技術を使用してデータをディスクにバックアップします。データの重複排除とは、重複するデータのバックアップを省略することでバックアップデータのサイズを縮小するデータ圧縮技術です。

重複排除プロセスでは、データストリームを管理しやすいデータのチャンク(またはブロック)に分割します。次に、データチャンクの内容を相互に比較し、同じ内容のチャンクが見つかった場合に、そのチャンクを一意のチャンクへのポインターに置き換えます。つまり、同一内容のチャンクが20個見つかった場合は、一意のチャンクが1個だけ保持(バックアップ)され、残りの19個はポインターに置き換えられます。バックアップデータは重複排除ストアと呼ばれるディスクベースのあて先デバイスに書き込まれます。復元処理を実行すると、一意のチャンクが複製されて、ポインターで識別される正しい位置に挿入されます。重複排

除型のバックアップおよび復元処理では、復元処理をバックアップデータのリハイドレーションと呼ぶことがあります。

一般的に数種類の重複排除技術が利用でき、通常はハードウェアベースのソリューションとソフトウェアベースのソリューションに大別されます。これらのソリューションは、ファイル単位(シングルインスタンス)やブロック単位の重複排除といったサブグループに、さらに分類することができます。

StoreOnceソフトウェア重複排除について

Data ProtectorのStoreOnceソフトウェア重複排除は、ブロック単位で重複排除を行うソフトウェアベースのソリューションです。

StoreOnceソフトウェア重複排除を使用する際には、以下の点に注意してください。

- 重複排除は、ディスクベースのデバイスへのバックアップのみを対象としており、テープドライブやライブラリといったリムーバブルメディアには使用できません。
- Data Protectorでは、重複排除に対してソフトウェアのみのアプローチを採用(つまりStoreOnceソフトウェア重複排除を使用)しているため、バックアップデータを格納する標準的なハードディスク以外に特別なハードウェアは必要としません。
- 重複排除処理では、重複するデータが削除され、データのコピーが1つと、一意のデータへの参照リンクだけが残されます。重複排除処理で格納するデータは一意のデータのみのため、必要なストレージ容量を削減することができます。
- StoreOnceソフトウェア重複排除は、ハッシュベースのチャンク化技術を使用してデータストリームをまとまった大きさのデータチャンクに分割します。
- バックアップ仕様でStoreOnceソフトウェア重複排除インターフェイスを備えたディスクへのバックアップデバイスを指定することで、重複排除型のバックアップが行われます。

重複排除を使用するタイミング

データの重複排除に対応したB2Dデバイスを使用する典型的な例は、バックアップする電子メールのファイルシステムに、1MBの同じ画像ファイルが添付された100件の電子メールが含まれるような場合です。このシステムを従来のバックアップ技術でバックアップすると、100件の添付インスタンスがすべてバックアップされるため、約100MBのストレージスペースが必要になります。これに対し、重複排除に対応したB2Dデバイスを使ったバックアップでは、実際に格納する添付ファイルは1件だけです。他のすべてのインスタンスは一意の格納済みコピーを参照します。この例では重複排除率が約100:1となります。この例はファイルレベルの重複排除と呼ばれるもので、B2Dデバイスと重複排除を使用する利点を理解するのに役立ちます。

重複排除技術を使用するかどうかを決める際には、ほかにも次の点を考慮してください。

- データによっては重複排除に適さないものがあります。たとえばデータベースファイルなど、コンピューターが自動的に作成するデータに対しては重複排除が効果的に行われません。写真、ビデオ、音声、イメージ、地震データは、すべて重複排除が効果的に行われないデータの例です。
- 重複排除を行う前にデータを圧縮しないでください。重複排除率に影響を与えるうえ、重複排除に続けて圧縮が行われるため必要ありません。
- 重複排除を行う前にデータを暗号化しないでください。重複排除率が1:1になり、重複排除を行わなかった場合と同じ結果になります。

B2Dデバイスと重複排除の利点

一般的には、データの重複排除を行うとバックアップサービス全体の速度が上昇し、全体のストレージコストが減少します。また、ストレージに必要なディスクスペースも大幅に減少します。データの重複排除はディスクベースのシステムであるため、復元サービスのレベルが極めて高く、テープ(または他のメディア)処理のエラーも減少します。このほかにも、重複排除には次のような利点があります。

- データの重複排除はデータ量が多い方が適しています。
- Data Protectorでは、実績のある重複排除アルゴリズムを採用することでデータの整合性を確保しています(StoreOnceソフトウェア重複排除にはHPE StoreOnce Backupシステム向けにHPE Labsが開発した重複排除技術が採用されています。これらのシステムではハードウェアベースの重複排除を使用しています。HPE StoreOnce製品の詳細。
- 重複排除に対応したディスクからディスク(D2D)型のストレージは、ローカルアプリケーションとリモートアプリケーションの両方で、最適なバックアップおよび復元方法として急速に広まっています。
- 複製に対応したD2Dシステムの復元総コストは、テープベースのシステムの復元コストより格段に低くなっています。データの重複排除バックアップでは、従来のディスクバックアップ技術より容量とコストを大幅に節約できます。

重複排除のパフォーマンス

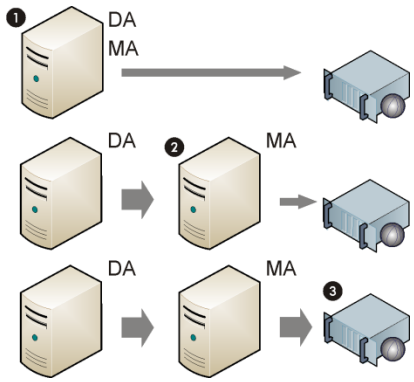
重複排除のパフォーマンスを左右する要因は数多くあります。例として、ハードウェアとネットワークの速度、ストレージディスクの設定方法、ストアのサイズ、データの重複排除率、および同時実行中のバックアップの数などが挙げられます。また、複数のストリームを使用してバックアップを行うとパフォーマンスが大幅に向上しますが、1つのストアに対して同時にデータを読み書きできるストリームの数は、ターゲットデバイスによって制限が異なります。

重複排除とData Protectorとの統合の仕組み

Data Protectorは、各種の重複排除設定に対応しています。

- *ソース側* 重複排除 - ソース側(バックアップされるシステム)でデータの重複排除が行われます。
- *サーバー側* 重複排除 - Media Agentシステム(ゲートウェイ)でデータの重複排除が行われます。
- *ターゲット側* 重複排除 - ターゲットデバイス(StoreOnce BackupシステムまたはStoreOnceソフトウェアシステム)のデータに対して重複排除が行われます。

重複排除の設定



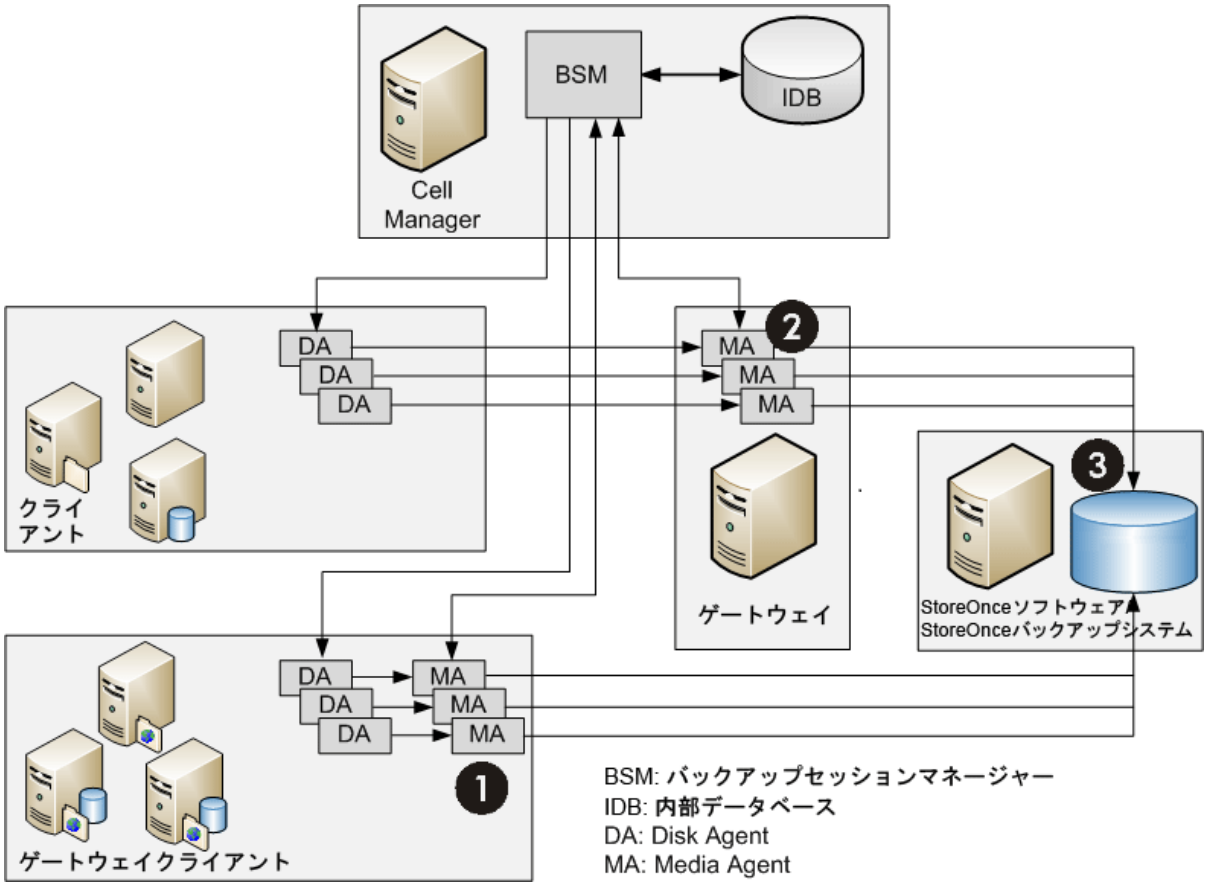
(1)ソース側重複排除

(2)専用Media Agentクライアント上でのサーバー側重複排除

(3)デバイス上でのターゲット側重複排除

データの重複排除とData Protectorとの統合を以下の図に示します。クライアント上のDisk Agentがデータを読み込み、Media Agent(ゲートウェイ)がターゲットデバイスに書き込みます。重複排除は、図**重複排除の設定**に示すとおり、さまざまなステージで行うことができます。B2Dデバイス構成はIDBに格納されます。

重複排除とData Protectorとの統合



ソース側重複排除

ソース側重複排除(1)では、バックアップされるクライアントにDisk Agentと共にMedia Agentがインストールされ、クライアントがゲートウェイ(ソース側ゲートウェイ)になります。重複排除はクライアント上のMedia

Agentが行い、重複排除済みデータのみをターゲットデバイスに送るため、ネットワーク全体のトラフィックが減少します。同時ストリームは、負荷調整設定によって数が制限されます。1つのMedia Agentによるローカルオブジェクトのバックアップが終了すると、次のクライアントシステムで別のMedia Agentが新たに起動します。

ただし、バックアップされるシステムが重複排除をサポートしている必要があります。詳細については、サポート一覧を参照してください。

サーバー側重複排除

サーバー側重複排除(2)では、重複排除は別のMedia Agentクライアント(ゲートウェイ)上のMedia Agentが行います。このため、バックアップ済みシステムとターゲットデバイス上の負荷は低下しますが、Disk AgentとMedia Agent間のネットワークトラフィックの量は減少しません。

Media Agentクライアントが重複排除をサポートしている必要があります。詳細については、サポート一覧を参照してください。サーバー側重複排除では、重複排除をローカルで行えないクライアントからのデータの重複排除が行えます。

ターゲット側重複排除

重複排除処理はターゲットデバイス(3)で行われます。バックアップ対象のデータは、クライアント(ゲートウェイ)上にインストールされたMedia Agentから受け取ります。

StoreOnceソフトウェアシステムを使用したターゲット側重複排除

次に、StoreOnceソフトウェア重複排除システムが重複排除済みデータをStoreOnceライブラリ(物理ストアであり、重複排除ストアとも呼ばれます)に書き込みます。

StoreOnceソフトウェア重複排除システムでは、ローカルまたはリモートを問わず、複数のMedia Agentから接続が行えます。また、同期メカニズムを備えているため、複数のMedia AgentによるStoreOnceライブラリの同時使用も可能です。Media Agentは、StoreOnceライブラリに対し、オブジェクトバージョンという形でデータの読み込みと書き込みを行います。個々のオブジェクトバージョンは、StoreOnceライブラリでは1つのアイテムとして表されます。重複排除のパフォーマンスを最適化するため、Disk Agentの並行処理には対応していません(つまり、Disk AgentとMedia Agentが1対1でやり取りを行い、ストリームの多重化は行われません)。基本的なローカルおよびリモートオフィスへの導入の詳細な構成については、『*HPE Data Protector Administration Guide*』を参照してください。

StoreOnce Backupシステムデバイスを使用したターゲット側重複排除

Data Protectorから見ると、この重複排除は、StoreOnceソフトウェアシステムを使用したターゲット側重複排除とほとんど変わりはありません。ただし、別のStoreOnceソフトウェア重複排除システムは存在せず、重複排除はStoreOnce Backupシステムデバイス自体で行われます。

StoreOnceソフトウェア重複排除のシステム要件

	CPU速度/コア数[1] (StoreOnceソフトウェア専用)	**物理メモリ**[2] (StoreOnceソフトウェア専用)	**ディスク数**[1](ストア専用)
最小要件 (1TBのストア用)	2.8 GHz/2コア	4 GBのRAM	1
推奨要件	2.8 GHz/4～6コア	6 GBのRAM	4以上(RAID5使用時)

(並行接続数が5の10TBのストア用)			
(1) パフォーマンスを最大に高めるには、各並行ストリームに対してコア数を1.3、ディスク数を0.8、増設RAMを50MBに構成し、StoreOnceソフトウェア重複排除システム専用の物理システムを使用してください。 (2) 1TBのストア容量あたり300MBのRAMが必要です。			

StoreOnceソフトウェアサーバーでのウイルス対策に関する留意事項

この項では、StoreOnceソフトウェアサーバーでウイルス対策製品を使用している場合、または使用を予定している場合の留意事項を示します。

- StoreOnceソフトウェアのルートディレクトリは、ファイル構造が複雑なため、スケジュールされたスキャンまたはリアルタイムスキャンを実行することはお勧めできません。
- StoreOnceソフトウェアのメンテナンスプロセスに関係するフォルダーのファイルをスキャンすると、StoreOnceソフトウェアに障害が発生する可能性があります。
- ファイルを隔離先に移動したり、ウイルススキャナーがStoreOnceライブラリフォルダー構造内でセキュリティリスクを認識してファイルを削除したりすると、ストアが破損し、使用不能になります。

推奨事項

- ウイルスのリアルタイムスキャンを無効にします。
- ウイルススキャナーの「除外リスト」にStoreOnceソフトウェアのルートディレクトリを追加します。
- 定期的に`--get_server_properties`コマンドを実行してストアルート情報を確認します。

Data ProtectorとStorage Area Network

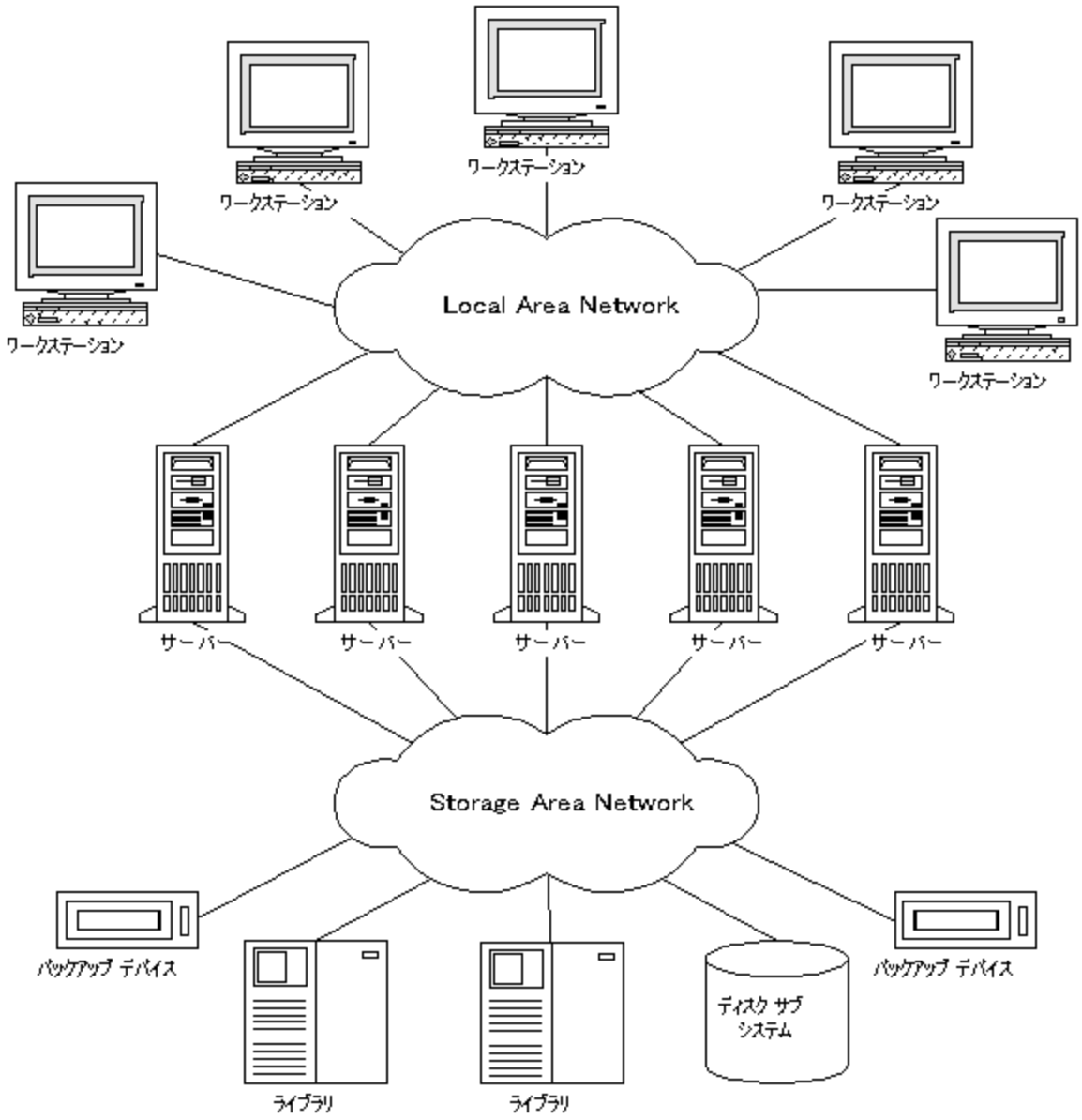
企業内のどこにどのような形でデータを保存するかは、ビジネスに重大な影響を及ぼす可能性があります。ほとんどの企業にとって、情報はますます必要不可欠なものとなりつつあります。今日ではテラバイト単位のデータに、ユーザーがネットワークを介してアクセスできなければなりません。Data ProtectorはSANベースのファイバーチャネルテクノロジを実装しており、必要となるデータストレージソリューションを提供します。

Storage Area Network

Storage Area Network (SAN)では、すべてのネットワークリソース間で*any-to-any*の接続が可能となるため、複数のクライアントシステム間でデバイスを共有でき、デバイスの可用性だけでなくデータトラフィックの性能も向上します。

SANの概念を導入すると、複数のデータ記憶デバイスおよびサーバー間での情報交換が可能になります。サーバーは、任意のデバイス上のデータを直接取得でき、従来型のLANを介したデータ転送の必要はありません。SANは、サーバー、バックアップデバイス、ディスクアレイ、およびその他のノードから構成され、これらがすべて高速なネットワーク接続(通常はファイバーチャネル)で接続されています。この専用の高速ネットワークにより、従来型のLANは記憶装置の処理から解放されます。

Storage Area Network



ファイバーチャネル

ファイバーチャネルは、高 速 のコンピューター相 互 接 続 に関 するANSI標 準 です。この標 準 では、光 ケーブルまたは銅 線 ケーブルを使 用して、大 容 量 データファイルの双 方 向 送 信 が可 能 です。ファイバーチャネルは情 報 の格 納 、転 送 、および取り出しに関して、現 時 点 における最 も信 頼 性 が高く高 性 能 のソリューションです。

ファイバーチャネルは、ノード間を次 の3種 類 の物 理トポロジ(およびそのバリエーション)で接 続 できます。

- ポイントトゥポイント
- ループ

- スイッチ式

ポイントトゥポイント、ループ、およびスイッチ式のファイバーチャネルトポロジは、それぞれの環境における接続や将来的な要件に合わせて適宜組み合わせることも可能です。

サポートされる構成の一覧について、https://softwaresupport.hpe.com/を参照してください。

ポイントトゥポイントトポロジ

ポイントトゥポイントトポロジでは、2つのノード、一般的にはサーバーとバックアップデバイスを接続することができます。この方法では、性能の向上と長距離間のノードの接続という基本的な利点が得られます。

ループトポロジ

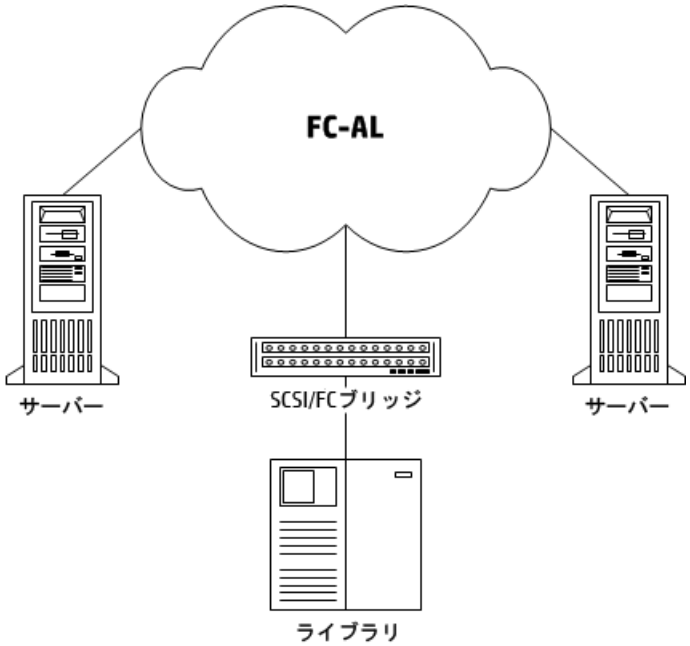
ループトポロジは、FC-AL (Fibre Channel Arbitrated Loop)標準をベースにしています。ノードとなるのはサーバー、バックアップデバイス、ハブ、スイッチなどです。ループ内のすべてのノードは、そのループ内の任意のノードと通信でき、すべてのノードが同一の帯域幅を共有します。FC-ALループの実装には、通常FC-ALハブと自動ポートバイパスが使用されます。自動ポートバイパスを使うと、ループへのノードのホットプラグが可能になります。

LIP

LIP(Loop Initialization Primitive)は、さまざまな場合に起動されますが、最も一般的には、新しいデバイスの導入時に起動されます。新しいデバイスには、すでにループに属していたデバイスに電源を入れたものや、アクティブなデバイスでスイッチポートを移動したものもあります。LIPが起動されると、テープのバックアップ処理など、SAN上の進行中のプロセスが予期せず中断される場合があります。これによってSCSI/FCブリッジとノード(SCSIデバイス)間のSCSIバス接続がリセットされます。「Loop Initializationプロトコル、次のページ」を参照してください。

バックアップや復元中にSCSIバスがリセットされると、書き込みエラーとして記録されます。Data Protectorでは、書き込みエラーが発生したときにはすべての操作を中止します。バックアップを実行していた場合は、(メディアにすでにバックアップされている情報をコピーした後)メディアを再フォーマットしてバックアップを再開することをお勧めします。

Loop Initializationプロトコル



スイッチ式トポロジ

スイッチ式トポロジでは、スイッチに接続されたすべてのノード間でany-to-anyの接続が可能となります。ファイバーチャネルプロトコルには自動構成および自動管理機能があるため、スイッチは簡単にインストールして使用できます。スイッチは、接続されている装置(ノード、FC-ALハブ、その他のFCスイッチなど)を自動的に検出し、それに合わせて自分自身を構成できます。スイッチは、接続されているノードにスケーリングされた帯域幅を提供します。スイッチ式トポロジでは、ノードの真のホットプラグ機能が実現されます。

> **注:**
> ホットプラグとは、リセットや通信の再確立などのプロトコル機能を指します。ホットプラグの最中は進行中のデータ転送は中断されますが、テープデバイスなどの一部のデバイスではこの動作に対応できない点に注意が必要です。ノードをループに接続したり、ループから切り離したりすると、バックアップ処理や復元処理が中断されて、処理が失敗する可能性があります。そのため、ループへのノードの接続や切り離しは、関連するハードウェアを使用したバックアップ処理や復元処理が行われていない時間帯にのみ実行してください。

SANにおけるデバイスの共有

Data Protectorでは、SANのコンセプトがサポートされており、SAN環境内のバックアップデバイスを複数のシステムの間で共有できます。つまり同一の物理デバイスに対して複数のシステムからのアクセスが可能です。そのため個々のデバイスに対するローカルバックアップを任意のシステムから実行できます。データはSANを介して転送され、バックアップに従来型のLANの帯域幅は必要ありません。そのためこの種のバックアップは、「LANフリーな」バックアップとも呼ばれます。また、通常SANベースのファイバーチャネルテクノロジの処理速度はLANテクノロジよりもはるかに優れているため、バックアップの性能も大幅に向上します。

ただし、複数のコンピューターシステムが、同一デバイスに同時にデータを書き込まないようにするための、なんらかの機構が必要になります。特に複数のアプリケーションが同一デバイスを使用する場合は問題

がより複雑になります。こうした問題を解決するには、関連するすべてのシステム間で、デバイスへのアクセスを同期化する必要があります。このためには、ロックメカニズムを使用します。

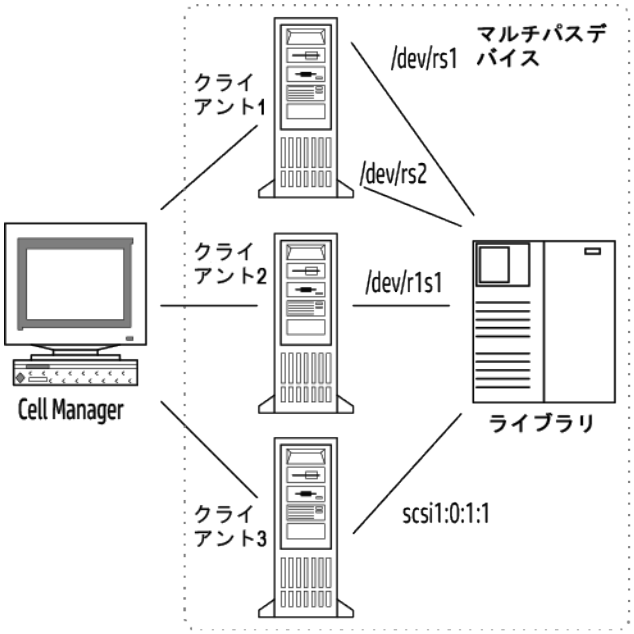
SANテクノロジでは、複数のシステムからライブラリのロボティクスデバイスを制御するための、非常に優れた方法が用意されています。そのため、1つのシステムからのみロボティクスを制御できるようにも(従来の方法)、またはライブラリを使用する個々のシステムからロボティクスに直接アクセスできるようにも構成できます(関連するすべてのシステム間でロボティクスへの要求を同期化できることが前提)。

物理デバイスに対する複数パスの構成

通常、SAN環境のデバイスは複数のクライアントに接続されているため、複数のパス、つまり、クライアント名とSCSIアドレス(UNIX上ではデバイスファイル)の組み合わせからアクセスが可能です。Data Protectorでは、これらのパスのいずれかを使用できます。同一物理デバイスに対するすべてのパスをまとめて、1つの論理デバイスとして構成することも可能です。これを、**マルチパスデバイス**と呼びます。

たとえば、デバイスが`client1`に接続されて`/dev/rs1`および`/dev/rs2`として構成され、`client2`上では`/dev/r1s1`、`client3`上では`scsi1:0:1:1`として構成されているとします。このため、`client1:/dev/rs1`、`client1:/dev/rs2`、`client2:/dev/r1s1`、`client3:scsi1:0:1:1`。マルチパスデバイスには、このテープデバイスへの4つのパスすべてが含まれています。

マルチパスの構成例



複数のパスを使う理由

Data Protectorの以前のバージョンでは、デバイスは1つのクライアントからしかアクセスできませんでした。この問題を回避するには、複数の論理デバイスを、ロック名を使用して単一の物理デバイスとして構成する必要がありました。このようにして、複数のシステムから単一の物デバイスへのアクセスの構成にロック名を使用する場合は、各システムですべてのデバイスを構成する必要がありました。たとえば、単一のデバイスに接続されているクライアントが10個あった場合は、同じロック名のデバイスを10個構成する必要がありました。Data Protectorの今回のバージョンでは構成が簡略化され、すべてのパスについて単一のマルチパスデバイスを構成するだけで済むようになっています。

マルチパスデバイスを採用すると、システムが障害に強くなります。Data Protectorは、最初に定義されているパスを試します。クライアント上のすべてのパスがアクセス不可能だった場合、Data Protectorはその次に定義されているクライアント上のパスを試します。リストされているパスがすべて利用不可能だった場合にのみ、セッションは中断されます。

パスの選択

バックアップセッション中は、構成時に定義された順序でデバイスパスが選択されます。ただし、バックアップ仕様で優先クライアントが選択されている場合は、その場合は、選択されている優先クライアントが最初に使用されます。

グローバル変数LANfreeが1に設定されている場合(デフォルト値は0)、バックアップセッションマネージャー(BSM)は、優先ホストを使用したり、パスの構成順序に従ったりすることなく、ローカルパスを使用します(ローカルパスがマルチパス構成で使用可能な場合)。

復元セッションでは、次の順序でデバイスパスが選択されます。

1. すべてのオブジェクトが同じターゲットクライアントに復元される場合は、オブジェクトの復元先クライアント上のパス
2. バックアップに使用されたパス
3. その他の利用可能なパス

直接ライブラリアクセスが有効な場合は、構成されている順序に関係なく、最初にローカルパス(あて先クライアント上のパス)がライブラリ制御に使用されます。

以前のバージョンとの互換性

Data Protectorの以前のバージョンで構成されたデバイスはアップグレード時に再構成されず、変更を行わずに以前のリリースのData Protectorと同じように使うことができます。ただし、新しいマルチパス機能を使用するためには、それらのデバイスをマルチパスデバイスとして再構成する必要があります。

デバイスのロック

デバイスロック機構は、Data Protectorのみが複数のシステムから渡されたデータやコマンドを使ってデバイスを操作する場合だけでなく、複数のアプリケーションが同一デバイスを使用する場合にも対処できなければなりません。デバイスのロックは、複数のシステムの間で同じデバイスを共有している場合に、そのデバイスに対する複数のシステムからの同時アクセスを防ぐことを目的としています。

複数アプリケーション間のデバイスロック

Data Protectorと少なくとも1つの別のアプリケーションが、複数のシステムで同一デバイスを共有するためには、各アプリケーションが同一(共通)のデバイスロック機構を使用する必要があります。このロック機構は、複数のアプリケーションにわたって機能するものでなければなりません。Data Protectorは、現時点ではこのモードをサポートしていません。そのためこのような形でデバイスを共有する必要がある場合は、運用規則を設けることにより、ある一時点では1つのアプリケーションのみがすべてのデバイスに排他的にアクセスできるようにしてください。

Data Protectorのデバイスロック機構

あるドライブを使用するアプリケーションはData Protectorのみであるが、複数のシステムでそのドライブを使用する可能性がある場合は、デバイスロック機構を使用する必要があります。

また、あるロボティクス制御を、Data Protectorのみが複数のシステムで使用する場合は、ライブラリ制御とそれを使用するすべてのシステムが同一セル内にある場合に限り、Data Protectorで内部的に処理することができます。このような場合は、そのデバイスへのアクセスの同期はすべて、Data Protectorにより内部的に制御されます。

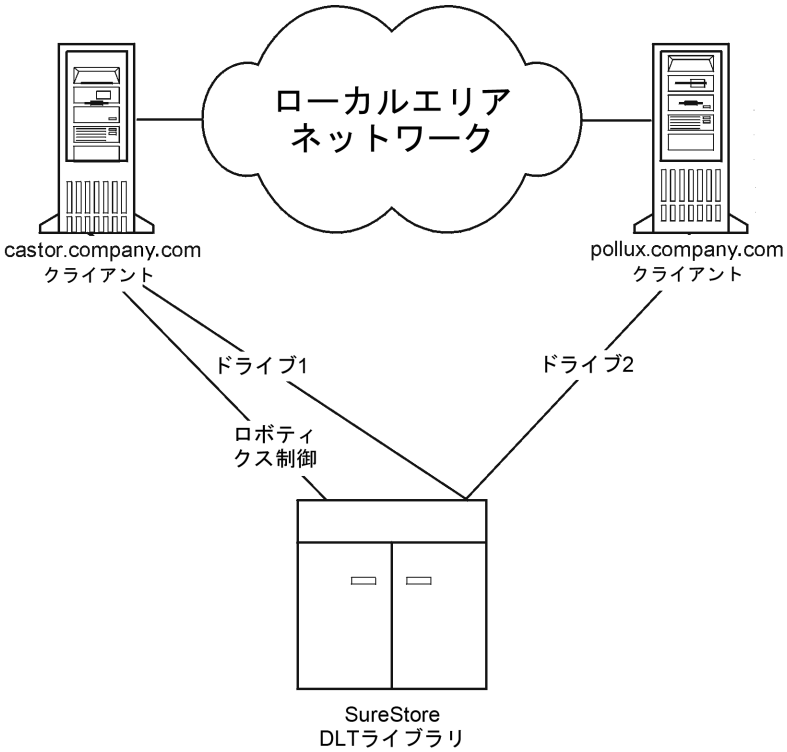
間接ライブラリアクセスと直接ライブラリアクセス

SCSIライブラリデバイスでのData Protectorの構成時には、クライアントシステムがライブラリロボティクスにアクセス可能な方法として、間接ライブラリアクセスと直接ライブラリアクセスがあります。

間接ライブラリアクセス

この構成はSANを導入する場合も、従来型のSCSIによる直接接続環境でも使用できます。この構成では各システムは、ライブラリロボティクスへの直接アクセス権を持つクライアントシステムに要求を転送することにより、ライブラリロボティクスへのアクセスが可能になります。この方法は間接ライブラリアクセスと呼ばれます。間接ライブラリアクセス、下の例では、2台のクライアントシステムが、1台のHPE DLTマルチドライブライブラリに接続されています。クライアントシステム`castor`がロボティクスと最初のドライブを制御しており、クライアントシステム`pollux`が2番目のドライブを制御しています。`pollux`上のData Protector Media Agentがロボティクスを制御するには、`castor`上で実行されているプロセスと通信する必要があります。このData Protectorのライブラリ共有機能は、ライブラリやドライブのホスト名が異なっている場合に自動的に使用されます。

間接ライブラリアクセス



この構成では、ロボティクスを制御するクライアントシステム(この例の場合は`castor`)で障害が発生すると、共有ライブラリを使用できなくなる点に注意してください。

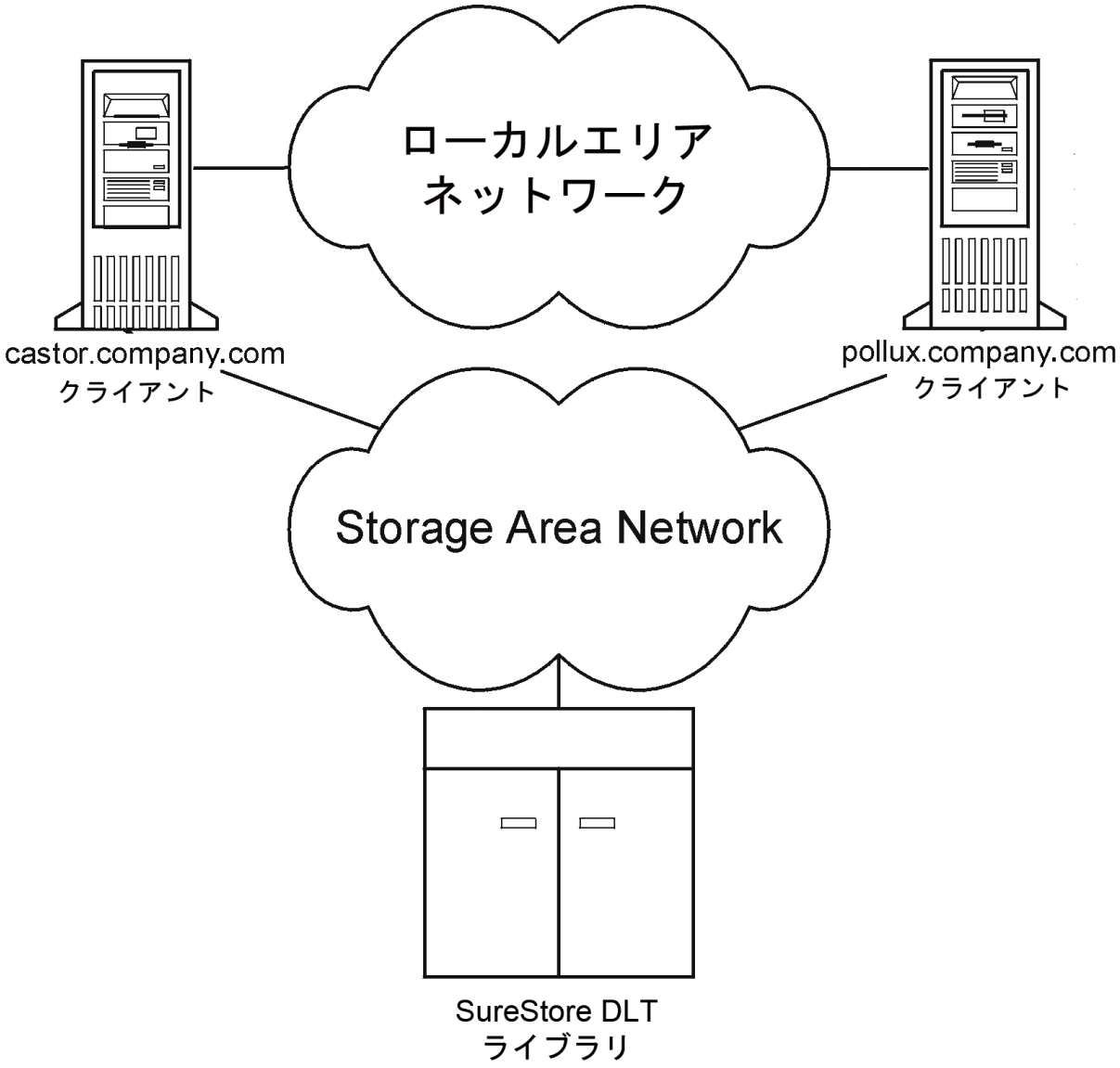
直 接ライブラリアクセス

SANの概 念を導 入する場 合は、SCSIライブラリとともにData Protectorを構 成するときに、個 々のクライアントシステムからライブラリロボティクスとドライブに直 接アクセスできるように構 成できます。この方 法は直 接ライブラリアクセスと呼 ばれます。

この場 合は、ロボティクスに対 する単 一の「制 御クライアントシステム」は存 在しません。そのため、ロボティクスを制 御するシステムで障 害が発 生しても、他 のシステムでは問 題なくライブラリを使 用できます。再 構 成の必 要はありません。ロボティクスは複 数のクライアントシステムから制 御できます。

直 接ライブラリアクセス、下 は、2台 のクライアントシステムにSANを介して接 続されたHPE DLTマルチドライブライブラリを示したものです。これらのクライアントシステムは、ライブラリと両 方のドライブにアクセスできます。ライブラリとの通 信にはSCSIプロトコルが使 われています。

直 接ライブラリアクセス



クラスター内のデバイス共有

SANの概念と組み合わされることが多いクラスター化は、ノード間でのネットワークリソース(ネットワーク名、ディスク、テープデバイスなど)の共有を基盤に構築されます。

クラスター対応アプリケーションは仮想ホスト上で実行されるため、その時々でクラスター内の任意のノード上で実行されている可能性があります。そのため、これらのアプリケーションをローカルバックアップするには、実際のノード名ではなく仮想ホスト名を指定してデバイスを構成する必要があります。各物理デバイスに対するデバイス構成を必要に応じて複数定義し、デバイスロック機構にはロック名を使用してください。詳細については、デバイスのロック、ページ 143を参照してください。

静的ドライブ

静的ドライブとは、クラスター内の実ノード上に構成されるデバイスです。これらのドライブは、共有されていないディスクを持つシステムのバックアップに使用できます。ただし、クラスター対応アプリケーションは、クラスター内の任意のノードで実行される可能性があるため、これらのアプリケーションのバックアップには静的ドライブは使用できません。

浮動ドライブ

浮動ドライブは、仮想システム名を使用して、仮想ホストに構成するデバイスです。クラスター対応アプリケーションをバックアップする場合は、この浮動ドライブを構成してください。浮動ドライブを使うと、クラスター対応アプリケーションが現在どのノード上で実行されていても、Data Protectorはそのノード上で確実にMedia Agentを開始できます。

メディア管理

エンタープライズ環境で大量のメディアを管理する場合に、深刻な問題が生じることがあります。Data Protectorのメディア管理機能を使用すると、柔軟かつ効率的にバックアップデータをメディアに割り当てることができます。これは、メディアの自動での割り当て方法や厳密な割り当て方法を定義することにより、さまざまに実現できます。

メディア管理機能

Data Protectorは以下に示すようなメディア管理機能を備えており、大量のメディアを簡単に効率よく管理できます。

- メディアをメディアプールと呼ぶ論理グループに分けることにより、個々のメディアを意識せずに大量のメディアをグループとして一括管理できます。
- Data Protectorでは個々のメディアと、そのメディアの状態がすべてトラッキングされています(データ保護の有効期限、バックアップ時にそのメディアを使用できるかどうか、各メディアにバックアップされている情報に関するカタログ情報など)。
- メディアへの物理的なアクセスを行わずに、Data Protector Cell Managerから別のにメディア関連のカタログデータをすべて転送できます。
- メディアの自動交換ポリシーを設定でき、テープを手動で交換する必要がありません。

- 特定のバックアップに使用するメディアとデバイスを明示的に定義できます。
- デバイスの種類(スタンドアロンデバイス、マガジンデバイス、ライブラリデバイス、大容量のサイロデバイスなど)に合わせて、それぞれに最適な形でメディアを管理できます。
- 完全な自動処理が可能です。ライブData Protectorラリデバイス内に十分な数のメディアを用意しておけば、メディア管理機能により、何週間にもわたってオペレーターによるメディア交換の必要なしにバックアップを実行できます。
- バーコードに対応した大容量ライブラリやサイロデバイスに対して、バーコードの認識とサポートが可能です。
- Data Protectorのメディアフォーマットやその他の一般的なテープフォーマットを自動認識できます。
- Data Protectorでは、Data Protectorで初期化(フォーマット)した空のメディアにのみ書き込みを行います。バックアップ時に、他のフォーマットData Protectorのテープに上書きすることはないため、他のアプリケーションが使っているメディアに偶発的にデータを上書きする危険はありません。
- ライブラリデバイスおよびサイロデバイス内で、Data Protectorが使用しているすべてのメディアを認識、トラッキング、ブラウズ、および操作でき、これらのメディアを他のアプリケーションが使用しているメディアと区別できます。
- 使用中のメディアに関する情報を中央で一元管理し、複数のData Protectorセル間でこの情報を共有できます。
- メディアボールティング(安全な場所でのメディアの保管機能)がサポートされています。
- メディア上のデータの追加コピーを対話式または自動的に作成できます。

この章では、上記の機能をさらに詳しく説明します。

メディアのライフサイクル

一般的なメディアのライフサイクルは、以下の各段階から構成されます。

1. バックアップに使用するための準備をします。

   準備には、で使用するためのメディアの初期化Data Protector(フォーマット)、およびメディアのトラッキングに使うメディアプールへのメディアの割り当てが含まれます。

   詳細については、バックアップ開始前のメディア管理、ページ 157を参照してください。
2. メディアをバックアップに使用します。

   ここでは、バックアップ用メディアの選択基準やメディア状態のチェック方法、新しいバックアップデータをメディアに追加する方法、メディア上のデータを上書きするタイミングなどを定義する必要があります。

   詳細については、バックアップセッション中のメディア管理、ページ 158を参照してください。
3. データストレージのメディアを安全な場所(ボールト)に長期間保管します。Data Protectorのデータ複製方法のいずれかを使って、ボールティング用にバックアップしたデータのコピーを作成することができます。

   詳細については、バックアップセッション後のメディア管理、ページ 162を参照してください。
4. メディア上のデータが不要になったら、新しいバックアップに再使用できるように、メディアをリサイクルします。
5. メディアを廃棄します。

使用期限が切れたメディアには不良マークが付加され、Data Protectorでは使用されなくなります。(メディア状態の計算、ページ 161を参照)。

メディアプール

Data Protectorのメディアプールでは大量のメディアをまとめて管理できるため、管理者の負担が大幅に軽減されます。

メディアプールとは

メディアプールとは、使用パターンとメディアプロパティが共通のメディアの論理的なセット(グループ)のことです。プール内のメディアは物理タイプも同一でなければなりません。たとえば一つのメディアプール内にDLTメディアとDAT/DDSメディアを混在させることはできません。

メディアが現在どこに存在するかは、プールとの対応付けには関係ありません。メディアがドライブ、ライブラリのリポジトリスロット、ボールト、またはその他の場所にあるかどうかは問題ではありません。リサイクルされ、セルからエクスポートされるまで、常にそのプールに属します。

複数のデバイスで、同一プールに所属するメディアを共有することも可能です。

メディアプールのプロパティの例

プールのプロパティ例を以下に示します。

- 追加可能

  このオプションを設定するData Protectorと、バックアップセッションの実行時に、プール内のメディアの空きスペースにデータが書き込まれます。

  このオプションが選択されていない場合は、各メディア内には同一セッションのデータのみが格納されます。
- 増分のみ追加可能

  バックアップセッション時には、増分バックアップが実行された場合に限り、メディアにデータが書き込まれます。そのため、メディア内に十分なスペースが残っている場合には、フルバックアップと増分バックアップがすべて同一のメディア上に保存されるようになります。
- メディア割り当てポリシー

  バックアップ用メディアの選択方法については、厳密さが異なるいくつかの設定レベルが用意されています。厳密な設定では、使用するメディアがData Protectorにより指定され、緩やかな設定では、Data Protectorは新しい(空の)メディアも含め、使用可能な任意のメディアを使用します。

各デバイスにはデフォルトプールが設定されています。バックアップ仕様内でこのプールを変更することも可能です。

その他のメディアプールプロパティの詳細については、『*HPE Data Protectorヘルプ*』のキーワード「メディアプール、プロパティ」で表示される内容を参照してください。

メディアプールとDCディレクトリ

Data Protectorでは、メディアプールに対してターゲットのDCディレクトリを設定できます。ターゲットDCディレクトリを指定すると、メディアプールのすべてのメディア情報が指定されたディレクトリに保存されます。

IDBのDCBF部分とDCディレクトリの詳細については、IDBアーキテクチャー、ページ 167を参照してください。

メディアプールの使用方法

メディアプールの使用方法の大部分はユーザーが自由に設定できます。たとえば、以下のような基準でプールを定義できます。

- システムプラットフォームごと(UNIXシステム用、Windows Vistaシステム用、Windows 7用に、それぞれ個別のプールを設定するなど)。
- システムごと(システムごとに個別のプールを設定するなど)。
- 組織構造ごと(部門Aの全システム用に1つのプールを設定し、部門Bの全システム用にもう1つ別のプールを設定するなど)。
- システムのカテゴリごと(大容量データベースを実行するシステムや、基幹業務を実行するシステムなどについて、それぞれ個別のプールを設定するなど)。
- バックアップの種類ごと(すべてのフルバックアップ用に1つのプールを設定し、すべての増分バックアップ用にもう1つ別のプールを設定するなど)。
- 上記の条件の組み合わせ。その他。

メディアプールの概念を簡単に理解するには、これらのプールをバックアップデータの保存先と考え、またデバイスは、バックアップデータとメディアプール間の転送メカニズムであると考えてください。

あるシステムカテゴリと目的のプールとを対応付けるには、対象となるシステムを同一のバックアップ仕様内ですべてリストアップし、使用するプールを指定します。オブジェクトデータがメディア上にどのように保存されるかは、デバイス、プール、およびバックアップ仕様の定義時に指定したオプションに基づいて決定されます。

このように、同一タイプのバックアップに使用するメディアを1つのメディアプール内にまとめておくと、グループレベルで共通のメディア取り扱いポリシーを適用できるため、各メディアを個別に管理する必要がなくなります。プール内の全メディアは1つのセットとしてトラッキングされ、同一のメディア割り当てポリシーが適用されます。

デフォルトのメディアプール

Data Protectorでは、さまざまなメディアタイプ別に、デフォルトのメディアプールが用意されています。これらのデフォルトメディアプールを使用すると、独自のメディアプールを作成しなくても、簡単にバックアップを実行できます。ただし、大規模な環境で、効率よくバックアップを管理するためには、目的に応じたメディアプールを作成する必要があります。バックアップの実行時には、使用するメディアプールを指定できます。

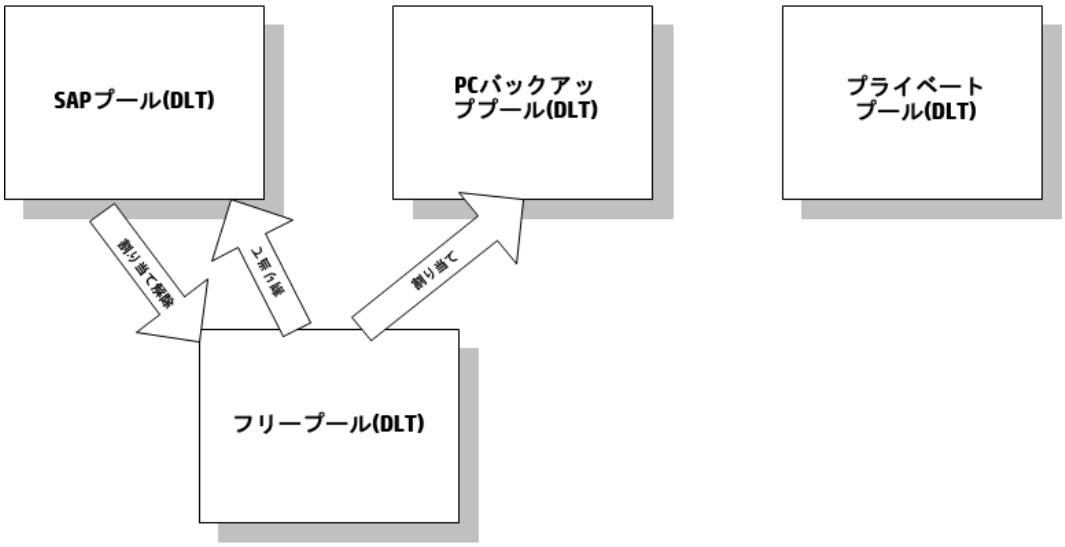
フリープール

あるメディアプールに割り当てたメディアの容量が不足した場合、同じ種類であっても他のプールにあるメディアを代用することはできません。他のプールのメディアを使用すると、不要なマウント要求が発生してオペレーターによる操作が必要になります。この問題を解決するにはすべてのメディアを1つのプールに配置するシングルプールモデルを使用します。この方法ではフリーメディアを共有できますが、メディアプールを使用する第1の利点(メディア管理の利便性、重要度に基づくデータの分類など)を活用できなくなります。この問題点をカバーするためにフリープールを使用します。

フリープールとは

フリープールは、同じ種類のメディア(DLTなど)で構成される補助ソースで、通常のプール内にあるすべてのフリーメディアが不足した場合に使用します。メディア(フリーメディア)不足に起因するバックアップの失敗を防止するのに役立ちます。

フリープール



フリープールを使用するタイミング

メディアは、以下の2つのイベント時に通常のプールとフリープールの間で移動されます(フリープール、上を参照してください)。

- 割り当て時。メディアはフリープールから通常のプールに移されます。
- 割り当て解除時。メディアは通常のプールからフリープールに移されます。割り当て解除を自動で行うかどうかは、GUIで指定できます。フリープール、上のPCバックアッププールの例では、メディアは自動的には割り当て解除されません。

保護(割り当て済み、または使用中)メディアは特定の通常プール(SAPプールなど)に所属しますが、Data Protectorのフリーメディアはフリープールに(自動的に)移動できます。このフリープールは、後に、このフリープールを使用するように構成されたすべてのプールに対して、フリーメディアを割り当てる際に使用されます。

フリープール、上のプライベートプールなど、通常のプールの中にはメディアをフリープールと共有しないように構成できるプールもあります。

フリープールの利点

フリープールには、以下の利点があります。

- プール間でフリーメディアを共有できます。

  すべてのフリー(保護されていない空の)メディアをフリープールにまとめて、フリープールの使用をサポートするすべてのメディアプール間で共有できます。
- バックアップ時のオペレーターの手動での作業を軽減します。

  すべてのフリーメディアが共有されている場合、マウント要求の必要性が低くなります。

フリープールのプロパティ

フリープールには、以下のような特徴があります。

- フリープールを使用するよう構成すると、フリープールを手動でまたは自動的に作成できます。通常のプールにリンクされているフリープールや空でないフリープールは削除できません。

- 通常のプールと異なり、割り当てポリシーオプションがありません。
- Data Protectorメディアのみ(不明のメディアまたは空のメディアを含まない)で構成されます。

メディア品質の計算

メディアの品質ではプール間の平均値が計算されます。メディア状態要素はフリープールに対してのみ構成可能で、フリープールを使用するすべてのプールによって継承されます。

フリープールの制限事項

フリープールには、以下の制限があります。

- 各プールに異なる状態要素は選択できません。その代わりにフリープールを使用するすべてのプールは、このフリープールに構成された状態要素を使用できます。
- メディアを手動で移動すること(保護メディアをフリープールへ移動したり、自動的に割り当て解除されるように構成されている、非保護メディアを通常のプールへ移動すること)はできません。
- フリープール内のメディアに対してインポート、コピー、リサイクルなどの操作は実行できません。
- マガジンをサポートするプールでフリープールは使用できません。
- フリープール使用時に、プール内に一時的な不整合が生じる場合があります(通常のプール内の非保護メディアが割り当て解除プロセスを待機しているなど)。
- メディアの保護期限が切れた後に保護期間を変更(たとえば無期限に変更)すると、メディアがフリープール内にあってもバックアップ用に割り当てられません。
- フリープールから割り当てられた場合は、異なるデータ形式タイプを持つメディアを使用でき、自動的に再フォーマットされます。たとえばNDMPメディアは、通常のメディアに再フォーマットされます。

フリープールの詳細については、『*HPE Data Protectorヘルプ*』のキーワード「フリープール、特性」で表示される内容を参照してください。

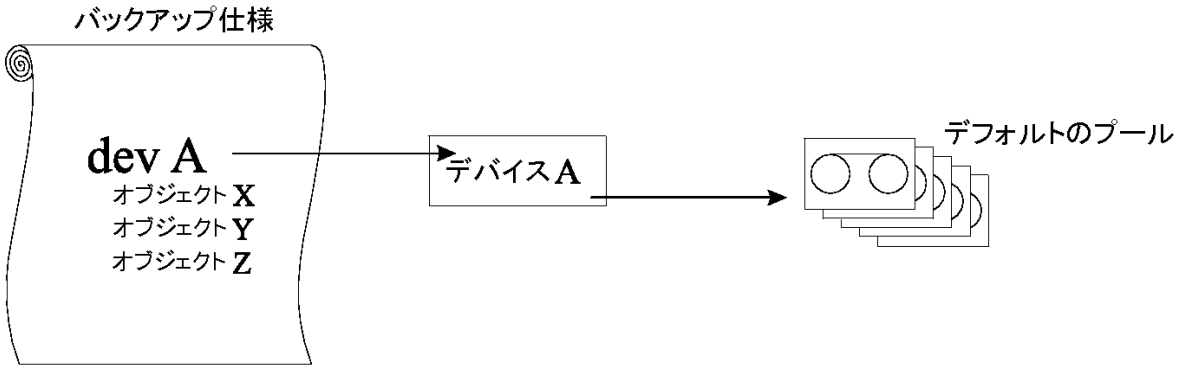
メディアプールの使用例

バックアップ環境を選択する上で検討の対象となる可能性のある構成例を以下に示します。

例1

単一デバイス/単一メディアプールの単純な対応付け、次のページに示すモデルでは、すべてのオブジェクトが同一のメディアプールにバックアップされます。このバックアップ仕様ではプールを指定していないため、デバイス定義で指定されているデフォルトのプールが使われます。

単一デバイス/単一メディアプールの単純な対応付け

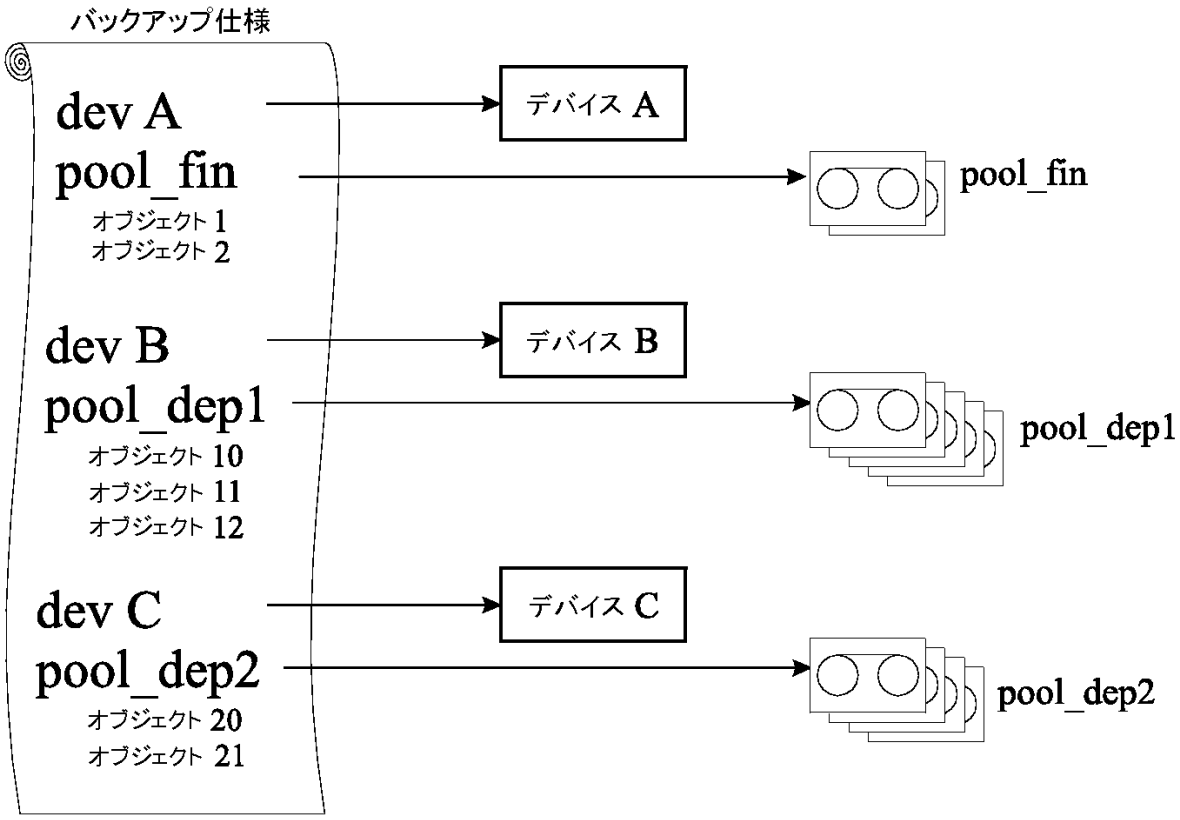


例2

大容量ライブラリデバイス内には、多数の物理ドライブが装備され、さまざまな部門やアプリケーションで使われる多数のメディアが格納されています。この場合、大容量ライブラリを使用する場合のメディアプール構成例 、次のページに示すように、各部門別のメディアプールを構成して、ライブラリ内のドライブのうち、どのドライブを実際のデータ転送に使用するかを指定できます。図の中でバックアップ仕様からメディアプールに伸びている矢印は、バックアップ仕様の中でそのメディアプールを指定していることを示します。バックアップ仕様の中でメディアプールを指定していない場合は、デバイス定義で指定されているデフォルトプールが使用されます。

メディアプールと大容量ライブラリデバイスとの関連については、大容量ライブラリ、ページ 114を参照してください。

大容量ライブラリを使用する場合のメディアプール構成例

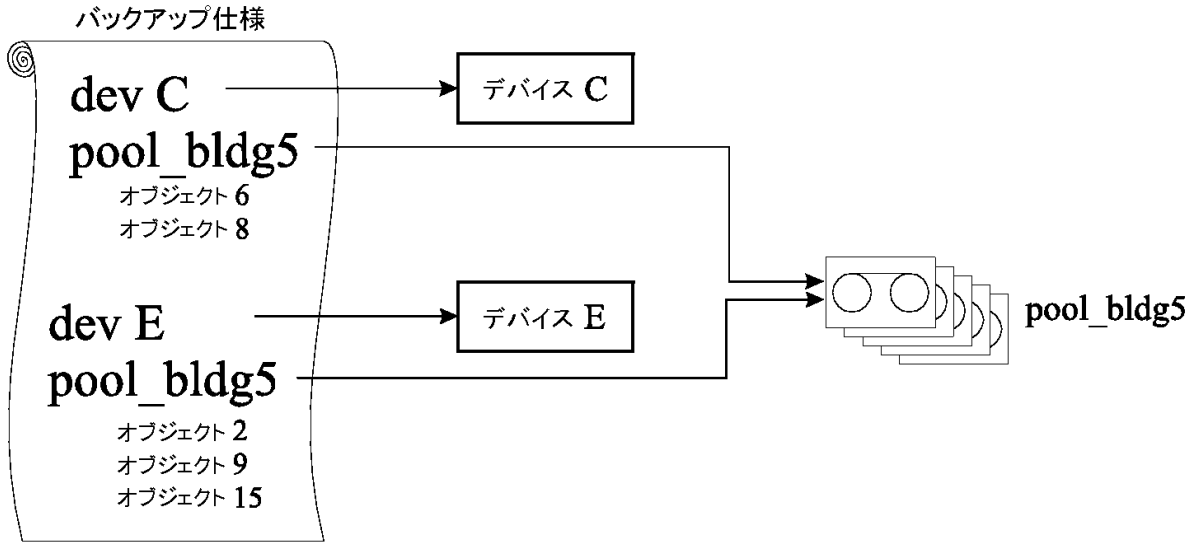


例3

複数デバイスと単一メディアプールの対応付け、次のページは、複数のデバイスから、同一メディアプール内のメディアに、データを同時にバックアップする場合の例を示したものです。どのプールを使用するかにかかわらず、複数のデバイスを並列に使用すると、性能は向上します。

詳細については、デバイスリストと負荷調整、ページ 106を参照してください。

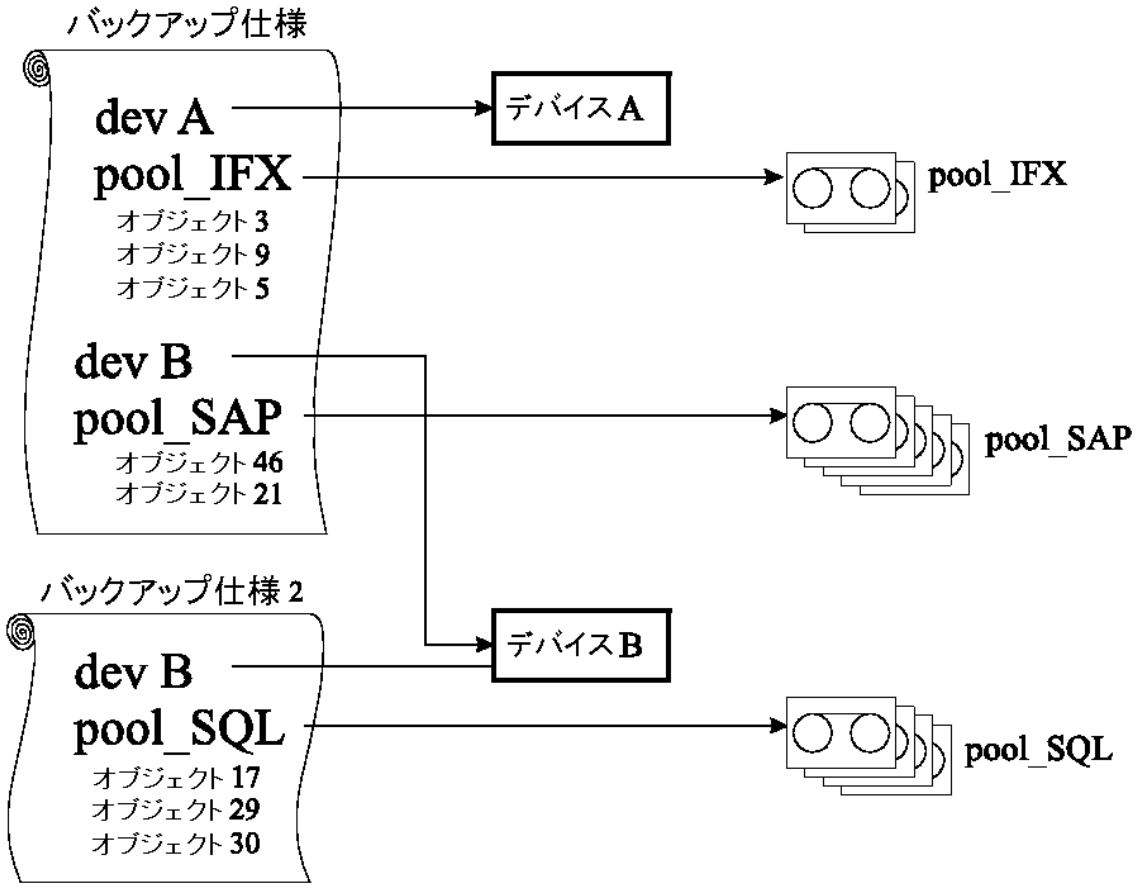
複 数 デバイスと単 一 メディアプールの対 応 付 け



例 4

この例 では、複 数 のデバイスを使 用して、複 数 のメディアプール内 のメディアに、データを同 時 にバックアップしています。1つのデバイスを複 数 のプールに対 応 付 けるには、それぞれ個 別 のバックアップ仕 様 を作 成 する必 要 があります。ここに示 す例 では、データベースアプリケーション別 に、専 用 のメディアプールを設 定 しています。

複数デバイスと複数メディアプールの対応付け



メディア交換ポリシーの実装

メディア交換ポリシーとは

メディア交換ポリシーとは、以下に示すような、バックアップ時のメディア使用方法を定義するものです。メディア交換ポリシーを定義するときは、以下の点を考慮する必要があります。

- いくつのバックアップ世代が必要か。
- メディアをどこに保管するか。
- メディアの使用頻度はどの程度か。
- どの時点でメディアの上書きを許可して、以降のバックアップで再使用できるようにするか。
- メディアの使用期限はどれくらいに設定するか。

従来のバックアップツールを使用するこれまでのバックアップ戦略では、メディア交換ポリシーをあらかじめ完全な形で定義しておき、これをバックアップアプリケーションではなく、管理者自身が制御する必要がありました。Data Protectorでは、通常、オプションを指定することによりメディア交換ポリシーを実装し、次回以降のバックアップ時に適切なメディアが自動的に選択されるようにすることができます。

メディア交換とData Protector

自動メディア交換と自動メディア操作

Data Protectorでは、メディア交換およびメディア操作が以下のように自動化されています。

- メディアはメディアプールにグループ化されるため、単独のメディアを管理する必要はなくなります。Data Protectorでは、メディアプール内の各メディアを自動的に追跡および管理します。
- バックアップされるデータがどのメディアに書き込まれるかを決める必要はありません。それは、Data Protectorによって行われます。管理者は、メディアプールにバックアップを行います。
- Data Protectorでは、指定したメディア交換ポリシーと使用オプションに基づいて、メディアプールから自動的にメディアが選択されます。必要に応じて、自動選択機能を無効にし、手動でメディアを選択することも可能です。
- Data Protectorで構成したメディアについては、Data Protectorユーザーインターフェイスを使用して、メディア位置のトラッキングおよび表示が可能です。
- Data Protectorでは、メディアの上書き回数と使用年数がトラッキングされており、メディアの状態が常に把握されています。
- Data Protectorにはセキュリティ機構が備わっているため、保護されたデータが入っているメディアが、Data Protectorにより偶発的に上書きされる危険はありません。

メディア交換に必要なメディアの数

必要なメディア数の見積もり

次の点を検討すると、フルメディア交換で必要になるメディアの総数を見積もることができます。

- 各メディアの容量について、完全に使い切るようにするのか、またはメディアによっては追記不可能として一部分しか使わないようにするのかを決定します。
- バックアップ対象となるシステムと、バックアップデータの保存に必要なメディアスペースを明らかにします。この作業には、バックアッププレビューが役立ちます。
- 2つのフルバックアップ間で実行する増分バックアップの回数など、バックアップの頻度を決定します。
- 1つのバックアップ世代で必要となるメディアの量を明らかにします。1つのバックアップ世代の中には、1つのフルバックアップと、次回のフルバックアップまでの間に実行される一連の増分バックアップがすべて含まれます。複数のデバイスを使用する場合は、ハードウェア圧縮の使用も検討してください。
- メディアの保護期間を決定します。
- 何世代分のバックアップ世代を保持するかを決定します。この数を超えると、一番初めに作成したバックアップ世代を上書きします。

以上の点を明らかにすると、フルメディア交換で必要となるメディアの総量を見積ることができます。メディア量については、さらに以下の点を考慮する必要があります。

- ディレクトリおよびファイル情報用として、メディア上のデータData Protectorの約10%分のオーバーヘッドがメディアに追加されます。この情報はバックアップのプレビューサイズに計算済みです。
- メディアの最大使用期限が切れたら、メディアを交換しなければなりません。
- バックアップするデータ量の増加も予測する必要があります。

バックアップ開始前のメディア管理

バックアップ用にメディアを使用するためには、まずそのメディアをData Protectorで使用できるように初期化(フォーマット)しなければなりません。メディアの初期化(フォーマット)は、手動で行っておくこともできれば、バックアップ用にメディアが選択された時点で、Data Protectorにより自動的に初期化(フォーマット)されるように設定しておくことも可能です。バックアップ用メディアの選択、次のページを参照してください。

メディアの初期化またはフォーマット

Data Protectorでは、バックアップに使用するメディアが、まず初期化(フォーマット)されます。初期化では、各メディアに関する情報(メディアID、説明、およびメディア位置)がIDB内に保存され、同時にこの情報がメディア自身(メディアヘッダー)にも書き込まれます。メディアを初期化(フォーマット)するときには、そのメディアが所属するメディアプールも指定する必要があります。

設定したプールポリシーによっては、メディアがあらかじめ初期化(フォーマット)されていない場合に、バックアップ時にData Protectorデフォルトラベルを使用した初期化(フォーマット)が自動的に実行されます。ただし、このようなメディアを使用すると、バックアップ処理に通常よりも時間がかかります。詳細については、バックアップ用メディアの選択、次のページを参照してください。

Data Protectorメディアのラベリング

Data Protectorで使用するメディアを追加するために、メディアを初期化(フォーマット)するときには、このメディアを後から識別できるように、メディアラベルを付加しなければなりません。デバイスにバーコードリーダーが装備されている場合は、メディアラベルの先頭にバーコードがメディアの説明として自動的に表示されます。このバーコードは、IDB内で管理されている各メディアに対する一意の識別子となります。メディアを初期化する際に、バーコードをメディアラベルとして使用することも可能です。

また、各メディアに対しては、Data Protectorによって、そのメディアを一意に識別するメディアIDが自動的に割り当てられます。

ANSI X3.27ラベルも、他のシステム上での識別用として、テープに書き込まれます。Data Protectorでは、これらのラベルと一緒に他の情報をメディアのヘッダーとIDBに書き込みます。

メディアラベルを変更すると、メディア自体ではなく、IDB内のメデData Protectorィアラベルが変更されます。そのため、書き換えていないメディアをいったんエクスポートしてからインポートし直すと、IDB内のメディアラベルがメディア上のメディアラベルで置き換えられます。テープ上のメディアラベルは、メディアを再初期化(フォーマット)しない限り変更できません。

ラベルの使用目的

これらのラベルは、そのメディアがData Protectorメディアであることを示します。バックアップ時または復元時にメディアがロードされると、Data Protectorは、そのメディアのメディアIDをチェックします。メディア管理システムでは、個々のメディアに関する情報を保持しており、そのメディアに対して要求された動作を実行してもよいかどうかをData Protectorに通知します。たとえば、メディア上に新しいバックアップ情報を書き込もうとした場合、メディア管理システムにより、メディア上の既存データの保護期限が切れているかどうかがチェックされます。ユーザー定義のラベルは、メディアを識別するために使用します。

位置フィールド

バックアップメディアは通常さまざまな場所に保管されています。たとえば、バックアップメディアは復元時にすぐに使用できるように社内に置いておき、バックアップデータのコピーを保管したメディアは安全性を考慮して社外に保管するといったケースが考えられます。

Data Protector各メディアの位置フィールドは、オペレーターが自由に変更できます。このフィールドを使用すると、メディアの場所を追跡することができます。「ライブラリ内、社外、vault_1」などは、分かりやすい位置フィールドの例です。

複数のメディアセットに存在するオブジェクトバージョンを復元する場合には、メディアの位置を設定する方法が便利です。メディアの位置の優先順位を設定することができます。この優先順位は復元に使われるメディアセットの選択に影響します。復元用のメディアセットの選択の詳細については、メディアセットの選択、ページ 99を参照してください。

バックアップセッション中のメディア管理

バックアップセッション中には、Data Protectorにより、バックアップ用メディアが自動的に選択され、どのデータがどのメディアに保存されたかもトラッキングされています。このように、どのデータがどのメディアにバックアップされたかをオペレーターが正確に把握する必要はなく、メディア管理が容易になります。同一セッション内でバックアップされたバックアップオブジェクトは、メディアセットと呼ばれます。

以下では、次の項目について説明します。

- Data Protectorによる、バックアップ用メディアの選択方法
- フルバックアップおよび増分バックアップの、メディアへの追加方法
- メディア状態の計算方法

関連情報については、以下の項を参照してください。

- フルバックアップと増分バックアップ、ページ 44
- メディアプール、ページ 148

バックアップ用メディアの選択

Data Protectorでは、メディア割り当てポリシーに基づいて、バックアップ用メディアが自動的に選択されます。これによって、メディア管理およびメディア処理が簡素化されます。バックアップオペレーターは、手動でバックアップ用メディアを管理する必要はありません。

メディア割り当てポリシー

メディア割り当てポリシーを使うと、バックアップ用メディアの選択方法を制御できます。メディア割り当てポリシーとしては、「緩和」ポリシーと「厳格」ポリシーを指定できます。前者の場合は、新しいメディアや空のメディアも含め、適切なメディアが任意に使用されます。一方、後者を指定した場合は、事前に定義された順番でメディアが使用できないと、メディアが均一に使用されません。さらに事前割り当てリストを使用することも可能です。

事前割り当てメディア

Data Protectorでは、事前割り当てリストを使用して、メディアプール内のどのメディアをバックアップに使用するかを明示的に指定できます。このリストは、「厳格」メディア割り当てポリシーと組み合わせて使用してください。この場合、メディアは指定された順番どおりに使用されます。この順番どおりにメディアが見つからなければ、Data Protectorによりマウント要求が発行されます。

メディアの状態

バックアップ用メディアの選択時には、各メディアの状態も考慮されます。たとえば、状態が「良好」のメディアは、状態が「普通」のメディアよりも優先的に使用されます。詳細については、メディア状態の計算、ページ 161を参照してください。

バックアップセッション中にデータをメディアに追加

メディアスペースの使用効率と、バックアップおよび復元時の効率を考えて、前回のバックアップ時にメディア内に残っているスペースを、以降のバックアップで使用するかどうかを選択できます。Data Protector これは、メディア使用ポリシーで設定します。

メディア使用ポリシー

利用可能なメディア使用ポリシーは、以下のとおりです。

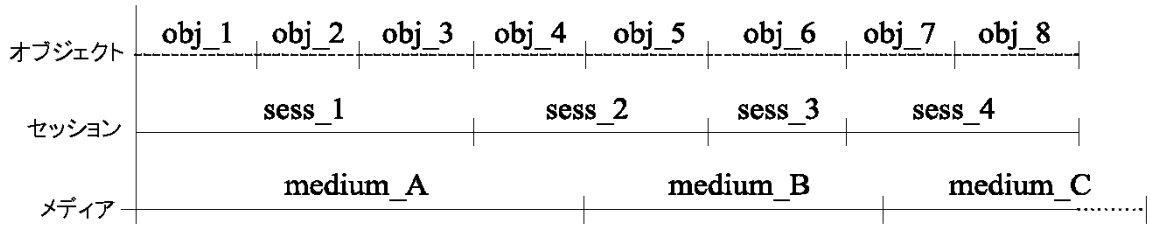
メディア使用ポリシー

ポリシー	説明
追加可能	バックアップセッション時には、まず初めに、前回のバックアップセッションで最後に使用されたメディア上に残っているスペースにデータが書き込まれます。このセッションで2本目以降に使われるメディアについては、テープの先頭からデータが書き込まれるため、保護期限が切れているテープまたは新しいテープのみが使用されます。この方針を選ぶとメディアスペースを節約できますが、1つのメディア内に複数のメディアセットのデータが含まれる可能性があるため、ボールティング作業は多少複雑になります。
追加不可能	バックアップセッション時には、使用可能な最初のバックアップ用メディアの先頭から、データが書き込まれます。各メディアには単一セッションからのデータのみが格納されています。このため、ボールティング作業が容易になります。
増分のみ追加可能	バックアップセッション時には、増分バックアップが実行された場合に限り、メディアにデータが書き込まれます。そのため、メディア内に十分なスペースが残っている場合には、フルバックアップと増分バックアップがすべて同一のメディア上に保存されるようになります。

オブジェクトのメディアへの分配

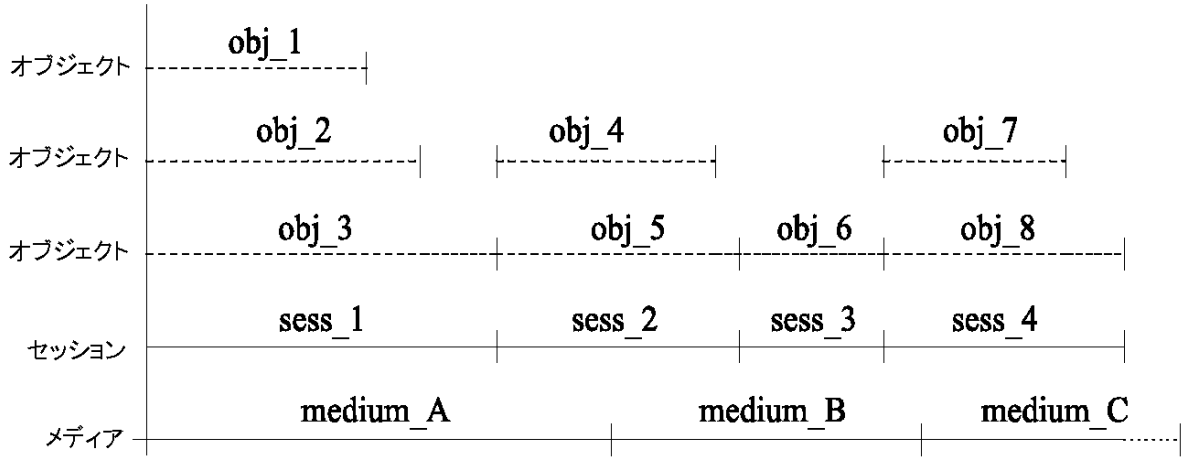
以下の各図は、複数のオブジェクトを複数のメディアに分配する方法の例を示したものです。

1つのメディアに複数のセッションとオブジェクトを分配する(順次書き込み)



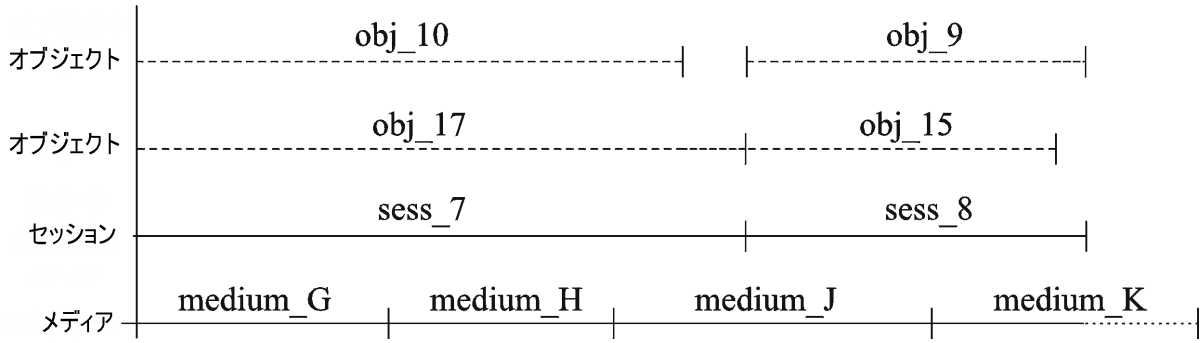
1つのメディアに複数のセッションとオブジェクトを分配する(順次書き込み)、前のページの例では、メディアの使用法に[追加可能]を指定した状態で、4つのセッションにわたって、8つの順次書き込みを実行しています。データは、4つのセッションにわたって書き込まれますが、1度に書き込まれるオブジェクトは1つだけになります。3つのメディアは、同一のメディアプールに所属しています。*medium_A*と*medium_B*はすでに一杯になっていますが、*medium_C*にはまだ多少のスペースが残っています。

1つのメディアに複数のセッションとオブジェクトを分配する(同時書き込み)



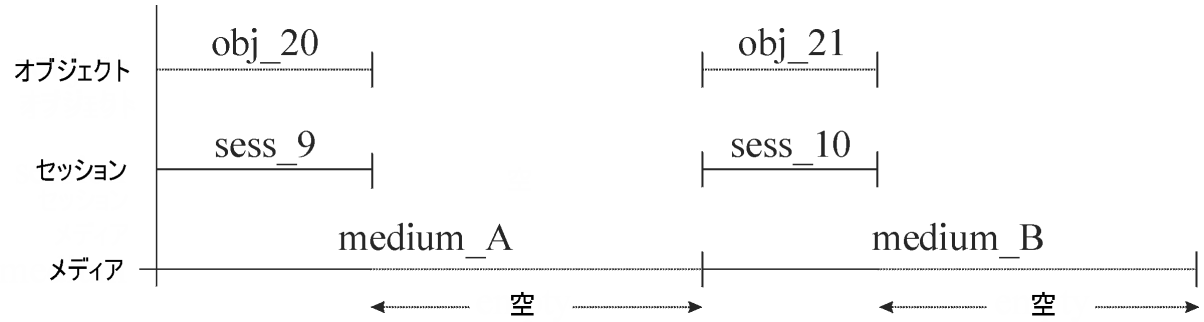
1つのメディアに複数のセッションとオブジェクトを分配する(同時書き込み)、上の例では、4つのセッションで、並列処理を有効にして同時書き込みを可能にした状態で、8つのオブジェクトを書き込んでいます。この場合、*obj_1*、*obj_2*、*obj_3*は*sess_1*で同時にバックアップされ、*obj_4*と*obj_5*は*sess_2*で同時にバックアップされました。*obj_1*は*system_A*の、*obj_2*は*system_B*の情報である場合もあれば、これらのオブジェクトが同一システム上の別のディスク上の情報である場合も考えられます。メディア使用ポリシーは、[追加可能]に設定されています。

1セッションあたり複数のメディアを使用し、1つのオブジェクトを複数のメディアに分配する



1セッションあたり複数のメディアを使用し、1つのオブジェクトを複数のメディアに分配する、前のページの例では、2つのセッションで4つのオブジェクトをバックアップしており、バックアップオブジェクトの最初のペアは*sess_7*で、2番目のペアは*sess_8*で、それぞれ同時に書き込まれます。この場合、1つのオブジェクトが、複数のメディアにまたがって書き込まれる可能性があることに注目してください。メディア使用ポリシーは、[追加可能]に設定されています。

各オブジェクトを個別のメディアに書き込む



各オブジェクトを個別のメディアに書き込む、上の例では、オブジェクトごとに1つのバックアップ仕様を作成し、メディアの使用法には[追加不可能]を指定しています。この方法では、メディアの消費量が多くなります。この方法で、メディアの使用法を[増分のみ追加可能]に変更すると、同一オブジェクトの増分バックアップのみが同じメディア上に保存されるようになります。

フルバックアップと増分バックアップに対する方針が復元性能とメディア使用に与える影響の詳細については、フルバックアップと増分バックアップ、ページ 44を参照してください。

バックアップ時の複数メディアセットへのデータ書き込み

Data Protectorのオブジェクトミラー機能を使用すると、バックアップセッション中に、一部またはすべてのオブジェクトを、複数のメディアセットに同時に書き込むことができます。詳細については、オブジェクトのミラーリング、ページ 94を参照してください。

メディア状態の計算

メディア状態要素

Data Protectorでは、**メディア状態要素**を使用して、使用中のメディアの状態を計算します。プール全体の状態は、プール内の最も状態の悪いプールによって決まります。たとえば、メディアプール内のある1つのメディアの状態が不良になると、プールの状態も直ちに不良になります。そのメディアをプールから取り除くと、プールの状態は普通または良好に戻ります。

メディアには、良好、普通、不良の3つの状態があります。

各メディアについて以下を使用し、状態を計算します。

- 上書き回数

  メディアの使用回数は、そのメディアが上書きされた回数として定義されます。ここで、使用回数とは、メディアに対してこれまでに行われた上書きの回数を意味します。上書き回数のしきい値を超過したメディアは、[不良]状態と見なされます。
- メディアの使用期間

メディアの使用期間は、メディアのフォーマットつまり初期化以降の経過月数として計算されます。月数のしきい値を超過したメディアは、[不良]状態と見なされます。

- デバイスエラー

  なんらかのデバイスエラーが発生すると、メディアが不良状態と見なされます。たとえばバックアップ中にデバイス障害が発生した場合、そのデバイスでバックアップに使われていたメディアは不良状態と見なされます。

バックアップセッション後のメディア管理

データをメディア上に保存した後は、そのメディアおよびメディア上のデータを、適切に保護しなければなりません。以下の点に注意してください。

- メディアの上書きを防止する。

  データ保護期間はバックアップの構成時に指定しますが、バックアップ以降にも変更可能です。データおよびカタログ保護の詳細については、バックアップデータおよびバックアップデータに関する情報の保存、ページ 73を参照してください。
- 物理的損傷からメディアを保護する。

  永久に保存するデータが書き込まれているメディアは、安全な場所に保管することをお勧めします。
- バックアップデータのコピーを作成し、そのコピーを安全な場所に保管する。

  (バックアップデータの複製、ページ 86を参照)。

以下の項では、メディアをボールトに保管する方法と、そのようなメディアを復元する方法について説明します。

ボールティング

ボールティングとは、重要な情報を格納したメディアを、一定期間、別の安全な場所に保管するプロセスを指します。この安全な場所は、**ボールト**と呼ばれます。

Data Protectorでは、ボールティングに関して、次の機能がサポートされています。

- データ保護ポリシーとカタログ保護ポリシーがサポートされています。
- ライブラリ内のメディアを簡単に選択し、取り出すことができます。
- **[メディア位置]**を調べると、メディアが保管されている物理的位置を確認できます。
- 指定した期間内に使われたバックアップメディアに関するレポートを作成できます。
- 指定したメディアをバックアップ中に使用したバックアップ仕様に関するレポートを作成できます。
- 指定した位置に保管されており、かつ指定した期間内にデータ保護期限が切れるメディアに関するレポートを作成できます。
- 復元に必要なメディアの一覧と、そのメディアが保管されている物理的位置を表示できます。
- 一定の基準に基づいて、メディアビューに表示するメディアをフィルタリングできます。

ボールティングの実施

ボールティングの実施方法は、各企業のバックアップ戦略と、データおよびメディアを扱うポリシーによって異なります。一般的な実施手順は、以下のようになります。

1. バックアップ仕様を構成するときに、適切なデータ保護ポリシーとカタログ保護ポリシーを設定します。
2. Data Protector内でボールトを構成します。これは基本的には、そのメディアを保管するボールトの名前を指定するだけの作業です
3. ボールト内のメディアに対する適切な保守方針を設定します。
4. 必要に応じてボールティング用にバックアップしたデータの追加コピーを作成します。バックアップ時にオブジェクトミラー機能を使うか、バックアップ後にオブジェクトコピーまたはメディアコピー機能を使います。
5. ボールトに移すメディアを選択し、そのメディアを取り出して、ボールトに格納します。
6. ボールトに格納されているメディアのうち、保護期限が切れたものを取り出して、ライブラリ内に戻します。

ボールティングの使用例

ここで、企業のバックアップポリシーで、データを毎日バックアップする必要があると仮定します。また、週に1回フルバックアップを実行し、これを保管場所に格納して、5年間保管する必要があります。さらに、保管場所に格納されているメディアのうち、1年以内に作成したデータについては、簡単に復元できるようにしておかなければなりません。5年が経過したメディアは、再使用しても構いません。

これは、Data Protectorが1週間に一度のフルバックアップと、毎日の増分バックアップを行うように設定されていることを意味します。データ保護期間は5年に設定します。カタログ保護期間は1年に設定します。こうすることで、1年間はデータのブラウズや復元を簡単に実行でき、さらにデータそのものの復元は5年間可能になります。フルバックアップで作成されたメディアについてはコピーを作成し、保管場所に格納しておきます。バックアップ後1年が経過したメディアについては、Data Protectorのデータベースから、そのメディア上のデータに関する詳細情報が自動的に削除されます。これにより、新しい情報を保存するためのスペースがデータベース内に確保されます。

ボールト内のメディアからの復元処理

保管場所内のメディアからデータを復元する方法は、一般のメディアからの復元方法と変わりません。データ保護とカタログ保護のポリシーによっては、以下に示す以外の手順が必要になることもあります。

1. 保管場所からメディアを取り出して、デバイスに挿入します。
2. メディアのカタログ保護がまだ有効な場合には、Data Protectorユーザーインターフェイスを使用して復元対象を選択することにより、簡単にデータを復元できます。

   メディアのカタログ保護期限が切れている場合には、そのメディア上のバックアップデータに関する詳細情報はData Protector内には保存されていません。その場合は、復元するファイルまたはディレクトリを手動で指定する必要があります。予備のディスクにオブジェクト全体を復元し、復元されたファイルシステム内で目的のファイルやディレクトリを検索することも可能です。

> **ヒント:**
> カタログ保護期限がいったん切れた後に、メディア上にバックアップされているファイルおよびディレクトリに関する詳細情報をData Protectorに再度読み込むには、メディアをいったんエクスポートしてから、インポートし直します。次に、メディア上の詳細なカタログデータを読み取るよう指示します。こうすると、Data Protectorユーザーインターフェイスを使用したファイルやディレクトリの選択が、再び可能になります。

データ保護ポリシーおよびカタログ保護ポリシーが復元処理に与える影響の詳細については、バックアップデータおよびバックアップデータに関する情報の保存、ページ 73を参照してください。

第4章: ユーザーとユーザーグループ

この章では、Data Protectorのセキュリティ、ユーザー、ユーザーグループ、およびユーザー権限について説明します。

ユーザーに対するセキュリティの強化

Data Protectorには優れたセキュリティ機能が備わっており、権限のないユーザーによるデータのバックアップや復元を防止しています。Data Protectorセキュリティ機能を使用すると、権限のないユーザーからデータを隠したり、データを暗号化したり、各ユーザーを職務に基づいてグループ化したりすることが可能になります。

この項ではデータのバックアップや復元、バックアップセッションの進捗状況のモニタリングにData Protectorを使用する場合の、セキュリティ関連問題について説明します。

バックアップデータへのアクセス権

データのバックアップを行い、そのデータを復元することは本質的にデータのコピーと同じことです。このため、データへのアクセスをアクセス権のあるユーザーのみに制限することが重要です。

Data Protectorには、次のユーザー関連のセキュリティ機能があります。

- Data Protectorの機能を使用するすべてのユーザーを、Data Protectorユーザーとして構成する必要があります。

バックアップデータの表示

- バックアップデータは、そのバックアップのオーナーしか見ることができません。他のユーザーに対しては、データがバックアップされているという事実さえも知らされません。そのため、たとえばバックアップオペレーターがバックアップを構成したような場合には、そのバックアップオペレーターまたはシステム管理者しかそのデータをブラウズしたり復元したりすることができません。他のユーザーもこのデータを見ることができるようにするには、Data Protectorの**[パブリック]**オプションを使用します。手順については、『*HPE Data Protector*ヘルプ』を参照してください。

ユーザーとユーザーグループ

Data Protectorを使用するには、特定の権限を付与されたData Protectorユーザーとして Data Protector構成に追加されている必要があります。ただし、あるユーザーが使用しているシステムをバックアップするために、そのユーザーを構成に追加する必要は必ずしもないことに注意してください。

ユーザーは、特定のユーザー権限(セル内のセッションの監視、バックアップの構成、ファイルの復元など)を持つユーザーグループにまとめられます。

定義済みのユーザーグループ

バックアップ構成を簡略化するために、Data ProtectorではData Protector機能にアクセスするための特定の権限を持つ事前定義されたユーザーグループを用意しています。デフォルトでadmin、operator、end-userという3つのユーザーグループが用意されています。たとえば、adminユーザーグループのメンバーのみが、Data Protectorの

すべての機能にアクセスできます。オペレーターは、デフォルトでバックアップの開始およびモニタリングを行うことができます。詳細については、『*HPE Data Protectorヘルプ*』のキーワード「ユーザーグループ」で表示される内容を参照してください。

> **ヒント:**
> 小規模な環境では、1人のユーザーですべてのバックアップ関連作業を実行できます。このユーザーは、Data Protectorの[Admin]ユーザーグループに所属しなければなりません。この場合は、その他のユーザーをData Protector構成内に追加する必要はありません。

ユーザーグループのカスタマイズ

環境に応じて、どのデフォルトのData Protectorユーザーグループを使用するのか、または変更して使用するのか、新しいユーザーグループを作成するのかを決定します。

[Admin]ユーザーグループのデフォルトのメンバー

以下のユーザーは、インストール時に、Data Protectorの[Admin]ユーザーグループに自動的に追加されます。

- UNIX Cell Managerシステム上のUNIX rootユーザー
- Windows Data ProtectorシステムにCell Managerをインストールしたユーザー

これらのユーザーはData Protectorのすべての構成を行え、またすべての機能を使用できます。詳細については、『*HPE Data Protectorヘルプ*』のキーワード「ユーザーグループ、admin」で表示される内容を参照してください。

Data Protectorユーザー権限

Data Protectorユーザーには、各自が所属するユーザーグループのData Protectorユーザー権限が与えられます。

UNIX Data Protector上で実行されているCell Manager内のWindowsドメインからユーザーを構成する場合は、構成時にドメイン名またはワイルドカードグループ"*"を指定する必要があります。

さらに、セルの特定のシステムへのユーザーアクションを制限することで、Data Protectorのユーザーグループに用意されているユーザーセキュリティレイヤーを補うこともできます。

各ユーザーグループに与えられるData Protectorユーザー権限の詳細については、『*HPE Data Protectorヘルプ*』を参照してください。

第5章: 内部データベース

この章ではData Protector内部データベース(**IDB**)のアーキテクチャー、使用方法、および操作方法について説明します。データベースの各部やレコード、データベースの増大や性能の推奨管理方法、データベースサイズの計算式について説明します。これらはデータベースを効果的に構成、保守するために必要な情報です。

IDBについて

IDBはCell Manager上に置かれる埋め込みデータベースです。バックアップ対象のデータとバックアップデータの格納先バックアップメディアのほか、バックアップ、復元、オブジェクトコピー、オブジェクト集約、オブジェクト検証、およびメディア管理の各セッションの結果や、構成済みのバックアップデバイスとライブラリなどに関する情報を保持します。

IDBを使う理由

IDBに保存された情報を利用することで、以下のことが可能になります。

- 復元が高速で便利。IDBに保存されている情報によって復元に必要なバックアップメディアを迅速に検出できるため、復元を高速に行うことができます。また復元対象のファイルやディレクトリをブラウズすることもできます。
- バックアップ管理が可能。IDBに保存されている情報によって、どのようにバックアップが行われたかを確認できます。Data Protectorのレポート機能を使用して、さまざまなレポートを作成することも可能です。
- メディア管理が可能。IDBに保存されている情報によって、バックアップセッション、オブジェクトコピーセッション、およびオブジェクト集約セッション中のメディアの割り当て、メディア属性のトラッキング、異なるメディアプールに属するメディアのグループ化、テープライブラリ内のメディア位置のトラッキングなどを行えます。
- 暗号化/復号化管理。IDBに保存されている情報によって、暗号化されたバックアップまたはオブジェクトコピーセッション用に暗号化キーを割り当て、暗号化されたバックアップオブジェクトの復元に必要な復号キーを提供できます。

IDBのサイズと増大に関する考慮事項

IDBは非常に大きくなる場合があります。IDBのサイズはバックアップ性能やCell Managerシステムに大きく影響します。したがって、Data Protector管理者は、IDBについて十分理解し、必要に応じて、どの情報をどのくらいの期間にわたってIDBに維持するかを決定する必要があります。復元時間および機能性の側面とIDBのサイズと増大の側面のバランスを取るのは、管理者の役目です。Data Protectorでは、これらのバランスをとる上で特に重要なパラメーターとして、**ロギングレベル**と**カタログ保護**の2つがあります。「IDBの増大と性能、ページ 173」も参照してください。

IDBの場所と使用する内部エンコード

IDBの場所

IDBは以下のディレクトリのCell Manager上に格納されます。

Windowsシステムの場合:`Data_Protector_program_data\server\db80`

UNIXシステムの場合:`/var/opt/omni/server/db80`

IDBの内部テキストエンコード

IDBは、すべてのテキスト情報をUnicode 2バイト形式またはUTF-8形式のいずれかで保存します。この2つの形式を使用することで、ファイル名とメッセージの他言語ローカライズを完全にサポートできます。

Manager-of-Managers環境のIDB

Manager-of-Managers(MoM)環境では、メディア集中管理データベース(CMMDB)をローカルのメディア管理データベース(MMDB)の代わりに使用できます。CMMDBを使用すると、複数のセル間でデバイスやメディアを共有できます。MoM機能の詳細については、企業環境、ページ 25を参照してください。

IDBアーキテクチャー

IDBの構成要素を以下に示します。

- MMDB(メディア管理データベース)
- CDB(カタログデータベース)
- DCBF(詳細カタログバイナリファイル)
- SMBF(セッションメッセージバイナリファイル)
- 暗号化キーストア

IDBの各部分は、特定のData Protector情報(レコード)を格納し、IDBのサイズと増加にさまざまな影響を与えます。各部分はCell Manager上の個別のディレクトリに置かれます。IDBの構成要素、次のページを参照してください。

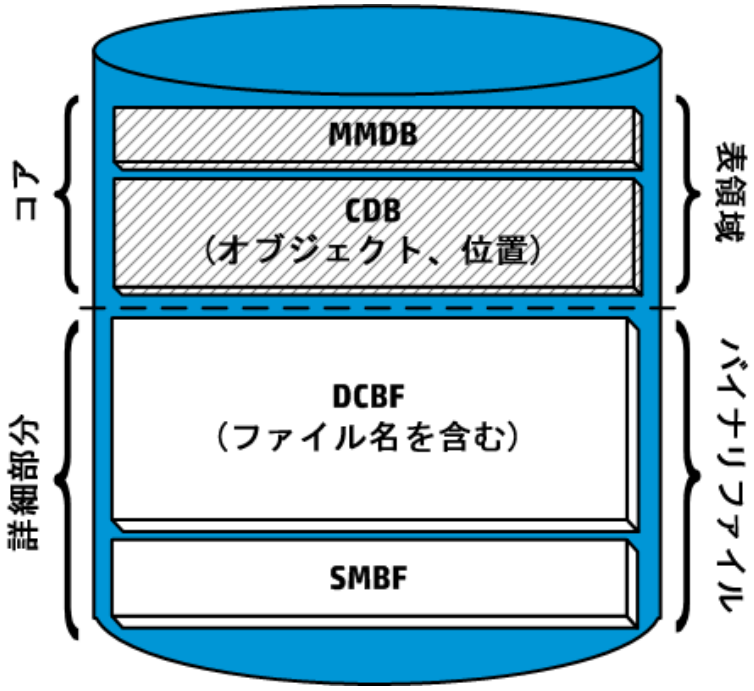
堅牢性についての注意事項は、『*HPE Data Protectorヘルプ*』のキーワード「IDBの堅牢性」で表示される内容を参照してください。

基礎となる技術

MMDBとCDBの各部分は、表領域を含む組込みデータベースを使って実装されています。このデータベースは、hpdp-idb、hpdp-idb-cp、およびhpdp-asプロセスにより制御されます。CDB部分とMMDB部分はIDBのコア部分を構成します。

IDBのDCBFおよびSMBFの各部分はバイナリファイルで構成されています。更新は、トランザクションを使用せず、直接行われます。

IDBの構成要素



メディア管理データベース(MMDB)

MMDBレコード

メディア管理データベースには、以下の項目に関する情報が格納されます。

- 構成されているデバイス、ライブラリ、ライブラリドライブ、スロット
- Data Protectorメディア
- 構成されているメディアプールとメディアマガジン

MMDBのサイズと増加

MMDBのサイズはそれほど大きくなりません。MMDBの大部分は、Data Protectorメディアに関する情報が占めるのが普通です。

カタログデータベース(CDB)

CDBレコード

カタログデータベースには、以下の項目に関する情報が格納されます。

- バックアップ、復元、オブジェクトコピー、オブジェクト集約、オブジェクト検証、およびメディア管理の各セッションに関する情報。これは、Data Protectorのモニターウィンドウに送信される情報のコピーです。
- バックアップされたオブジェクトとそのバージョン、およびオブジェクトコピーに関する情報。暗号化されたオブジェクトバージョンの場合、キーID(KeyID-StoreID)も格納されます。
- バックアップしたオブジェクトのメディア上の位置。Data Protectorは、各バックアップオブジェクトについ

て、バックアップに使用するメディアやデータセグメントの情報を保存します。オブジェクトコピーとオブジェクトのミラーリングについても同様です。

CDBのサイズとサイズの増大

CDBレコードは、IDBのうち、ごく一部のスペースを占有します。詳細については、IDBの増大と性能、ページ 173を参照してください。

詳細カタログバイナリファイル(DCBF)

DCBF情報

IDBの詳細カタログバイナリファイル部分には、次の情報が保存されます。

- バックアップファイルのパス名(ファイル名)とクライアントシステム名に関する情報。バックアップとバックアップの間に作成されたファイル名はDCBFに追加されます。
- ファイルメタデータ。これは、バックアップされたファイルバージョン、そのファイルサイズ、変更時刻、属性/保護、およびバックアップメディア上のバックアップコピーの場所に関する情報です。

Data Protectorがバックアップに使用する各メディアに対して、1つのDC(詳細カタログ)バイナリファイルが作成されます メディアが上書きされると、DCバイナリファイルが削除され、新しいDCバイナリファイルが作成されます。

ファイル名およびファイル属性部分のサイズとサイズの増大

DCBFのうち、サイズとその増加率が最も大きいのはファイル名部分です。ファイル名部分のサイズの増大は、バックアップの数と同様に、バックアップ環境のサイズの増大と変動率に比例します。

IDB内のファイルまたはディレクトリは約100バイトを占めます。

DCBFのその他の部分のサイズとサイズの増大

[**すべてログに記録**]オプションを使用してファイルシステムのバックアップを行うのが一般的な環境では、DCBFはIDBで最も大きな割合を占めます。IDBの増大と性能: 主要な調整可能パラメーター、ページ 174を参照してください。

デフォルトでは、DCバイナリファイル用に`dcbf0`から`dcbf4`の5つのDCディレクトリが構成されます。DCディレクトリを複数作成してCell Manager上の別のディスクに配置し、IDBサイズを拡張することができます。詳細については、『*HPE Data Protectorヘルプ*』のキーワード「DCディレクトリ」で表示される内容を参照してください。DCディレクトリとDCバイナリファイルに関するデフォルト値および最大値に関連した制限については、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』の「*制限および推奨事項*」の章の「*内部データベースの拡張性*」の項を参照してください。

セッションメッセージバイナリファイル(SMBF)

SMBFレコード

セッションメッセージバイナリファイルには、Data Protectorセッション中に生成されたセッションメッセージが保存されます。バイナリファイルは、セッションごとに1つずつ生成されます。バイナリファイルは、年と月に基づいて分類されます。

SMBFのサイズと増加

SMBFのサイズは以下の要素によって決定されます。

- 実行されたセッション数(1セッションにつきバイナリファイルが1つ作成されるため)。
- セッション内のメッセージ数。1つのセッションメッセージは約200バイトを占めます。[Report level]オプションを指定すると、バックアップ中、復元中、およびメディア管理中に表示されるメッセージ数を変更できます。これによってIDBに保存されるメッセージ数も変わります。詳細については、『*HPE Data Protectorヘルプ*』を参照してください。

暗号化キーストアとカタログファイル

暗号化されたバックアップ中に手動または自動で作成されたすべてのキーは、キーストアに保存されます。キーは、オブジェクトコピー、オブジェクト検証、および復元の各セッションにも使用できます。ハードウェア暗号化の場合、これらのキーはオブジェクト集約セッションにも使用できます。

ソフトウェア暗号化の場合、キーID(各キーIDはkeyIDとStoreIDで構成される)は、暗号化されたオブジェクトバージョンにマップされます。このマッピングはカタログデータベースに格納されます。メディア内の異なるオブジェクトに、異なる(ソフトウェア)暗号化キーを設定できます。

ハードウェア暗号化の場合、キーIDがメディアIDにマップされ、これらのマッピングはカタログファイルに保存されます。このファイルは、暗号化メディアを別のセルにエクスポートするのに必要な情報を含みます。詳細については、『*HPE Data Protectorヘルプ*』のキーワード「暗号化」で表示される内容を参照してください。

IDBの操作

バックアップ中

バックアップセッションが開始されると、IDBにセッションレコードが作成されます。また、そのセッションのオブジェクトごと、およびオブジェクトミラーごとにオブジェクトバージョンレコードが作成されます。これらのレコードはすべてIDB内に保存され、バックアップされたデータ、日時、場所に関する情報を含みます。

バックアップに対してソフトウェア暗号化が要求された場合、関係するエンティティ(ホスト)の有効な暗号化キーがキーストアから取得され、バックアップに使用されます。キーID(KeyID-StoreID)は、オブジェクトバージョンにリンクされ、CDBレコードに含められます。ホストとKeyID-StoreIDとのマッピングは、キーストア内のカタログにも格納されます。

バックアップ中にバックアップセッションマネージャーがメディアを更新します。すべてのメディアレコードはMMDBに保存され、ポリシーに従ってバックアップに割り当てられます。関係するメディアがハードウェア暗号化を要求したドライブ内にある場合、まず、エンティティ(メディア)の有効な暗号化キーがキーストアから取得されます。メディアとKeyID-StoreIDとのマッピングは、キーストア内のカタログに記録され、メディアにも書き込まれます。

データセグメントがテープに書き込まれ、次にカタログセグメントに書き込まれると、このデータセグメントの一部である各オブジェクトバージョンに対して、メディア位置レコードがCDBに保存されます。また、カタログがDC (詳細カタログ)バイナリファイルに保存されます。Data Protectorメディア1つにつき、1つのDCバイナリファイルが保持されます。DCバイナリファイル名は、*MediumID_TimeStamp*.datです。バックアップ中に

メディアが上書きされると、古いDCバイナリファイルが削除されて新しいDCバイナリファイルが生成されます。

バックアップ中に生成されたすべてのセッションメッセージは、セッションメッセージバイナリファイル(SMBF部分)に保存されます。

内部データベースバックアップの仕様の構成に応じて、IDBバックアッププロセスはバックアップされたアーカイブログファイルを削除でき、IDB回復に必要な新しいアーカイブログファイルの作成を開始します。

> **注:**
> Incrモードでの内部データベースバック(PostgreSQL)中に、構成ファイルがフルとしてバックアップされます。

復元時

復元構成時にData ProtectorはCDB部分とDCBF部分で一連の照会を行い、ユーザーがバックアップデータの階層(ファイルシステム、アプリケーションオブジェクト)をブラウズできるようにします。これらのブラウズ照会は、2段階で行われます。最初の段階では、特定のオブジェクト(ファイルシステムまたは論理ドライブ)を選択します。オブジェクトのバックアップバージョンやコピーが多数ある場合は、この手順に多少時間がかかります。これは今後のブラウズに必要なルックアップキャッシュを作成するためにData ProtectorがDCBFをスキャンするためです。2番目の手順では、ディレクトリをブラウズします。

特定のファイルバージョンを選択すると、Data Protectorは必要なメディアを決定し、選択したファイルが使用するメディア位置レコードを検出します。これらのメディアはMedia Agentから読み込まれ、選択したファイルを復元するDisk Agentにデータが送信されます。関係するメディアに対してハードウェア暗号化が行われた場合、Media Agentは最初にキーID(KeyID-StoreID)を検出し、Key Management Server (KMS)によってキーストアから取得されるキーを要求します。

関係するバックアップに対してソフトウェア暗号化が使用された場合、Disk Agentは暗号化されたデータを取得したときに、検出されたKeyID-StoreIDをKMSに送信し、キーストアから取得される関連する復号キーを要求します。

オブジェクトコピー時またはオブジェクト集約時

オブジェクトコピーセッションまたはオブジェクト集約セッション中では、バックアップと復元セッション中と同じ処理が実行されます。基本的には、データは復元されるときと同様にソースメディアから読み取られ、バックアップされるときと同様にターゲットメディアに書き込まれます。IDBの操作という点では、オブジェクトコピーセッションまたはオブジェクト集約セッションで行われることと、バックアップと復元で行われることは同じです。詳細については、バックアップ中、前のページおよび復元時、上を参照してください。ソフトウェア暗号化を使用するオブジェクト集約はサポートされていないため、これは当てはまりません。

オブジェクトの検証時

オブジェクト検証セッション中に、復元セッション中と同じデータベースプロセスが実行されます。基本的に、データは復元している場合のようにソースメディアから読み込まれ、確認を実行するホストDisk Agentに送信されます。IDB操作という点では、オブジェクト検証セッションで行われることと、復元セッションで行われることは同じです。検証セッション中に生成されるすべてのセッションメッセージは、セッションメッセージのバイナリファイルに保存されます。詳細については、復元時、上を参照してください。

メディアのエクスポート

メディアをエクスポートすると、暗号化された情報が含まれる場合、関連するキーがCell Manager上でキーストアからfilename.csvファイルにエクスポートされます。このファイルは、別のセルでメディアを正常にインポートするために必要です。

削除されたアイテム

さらに、複数のアイテムが削除されます。

- エクスポートしたメディアのすべてのメディア位置レコードがCDBから削除されます。
- その他のメディアに位置レコードがないすべてのオブジェクトとオブジェクトコピーがCDB部分から削除されます。
- 30日を超える古いセッション(メディアが上書きまたはエクスポートされているセッション)が削除されます。また、このようなセッションのセッションメッセージも削除されます。
- MMDB部分からメディアレコードが削除され、そのメディアのDCバイナリファイルがDCBFから削除されます。

詳細カタログの削除

特定のメディアから詳細カタログを削除すると、対応するDCバイナリファイルが削除されます。メディア上のすべてのオブジェクトバージョンとオブジェクトコピーのカタログ保護を削除しても同じ結果が得られます(DCバイナリファイルに対して次に行う日常の保守作業でバイナリファイルが削除されます)。その他のレコードはすべてCDBおよびMMDB内に保持されます。このため、バックアップオブジェクト全体の復元は実行できますが、単一のファイルを復元することはできません。

IDB管理の概要

IDB構成

Data Protectorのバックアップ環境の設定において、最も重要な手順の1つがIDBの構成作業です。初期構成では、IDBのサイズやIDBディレクトリの位置、IDBの破損や障害時におけるIDBのバックアップの必要性、IDBのレポートおよび通知の構成など、内部ポリシーを設定できます。

> **重要:**
> HPEIDBのバックアップを毎日実行するようにスケジュール設定することを強くお勧めします。IDBバックアップ用のバックアップ仕様の作成は、IDBの構成作業の一部です。

> **注意:**
> IDB構成になんらかの変更(内部データベースサービスとアプリケーションサーバーユーザーアカウントのパスワードの変更など)を行った場合、内部データベースを常にバックアップします。これを怠ると、オンラインIDB復元とオフラインIDB復旧が正常に実行できなくなる場合があります。

IDBの保守

IDBの構成が完了すると、保守作業は最低限に軽減され、主として通知とレポートへの対処のみが必要になります。

IDBの復旧

IDBのファイルが無くなったり破損した場合は、IDBの復旧が必要になります。復旧手順は破損の程度によって異なります。

詳細については、『*HPE Data Protectorヘルプ*』のキーワード「IDB、復旧」で表示される内容を参照してください。

IDBの増大と性能

IDBを適切に構成、保守するには、IDBの増大や性能に影響する重要な要素や主要な調整可能パラメーターを理解する必要があります。このパラメーターは必要に応じて適用できるのでIDBの増大や性能を効果的に調整できます。

IDBの増大や性能に影響を与える重要な要素

IDBの増大や性能に影響を与える重要な要素を以下に示します。

- ロギングレベルの設定

  ロギングレベルでは、バックアップ時にIDBに書き込まれる詳細データ量を定義します。ロギングレベルが詳細になるほど、IDBのストレージ容量の消費に大きく影響します。詳細については、IDBの増大と性能: 主要な調整可能パラメーター、次のページを参照してください。
- カタログ保護設定

  カタログ保護は、IDBでのバックアップデータに関する情報の保管期間を決定します。カタログ保護の期間を長くすると、IDBへの影響が増大します。詳細については、IDBの増大と性能: 主要な調整可能パラメーター、次のページを参照してください。
- バックアップファイル数

  Data Protectorでは、各ファイルおよびファイルの各バージョンを記録します。IDBへの影響は、バックアップの種類によって異なります。バックアップの種類については、フルバックアップと増分バックアップ、ページ 44を参照してください。
- バックアップの数

  バックアップを頻繁に行えば行うほど、IDBに保存される情報量は増加します。
- ファイルシステムの変動

  バックアップとバックアップの間に作成または削除されるファイル数は、IDBのファイル名部分の増大に重大な影響を与える可能性があります。ファイルシステムの変動に起因するIDBの増大を回避するには、[`Log Directories`]ロギングレベルを使います。
- バックアップ環境の増大

  セル内でバックアップされているシステムの数はIDBの増大に影響を与えます。このため、バックアップ環境の増大についての計画を立ててください。
- オブジェクトコピーとオブジェクトミラーの数

作成するオブジェクトコピーおよびオブジェクトミラーの数が多いほど、IDBに格納される情報量が増えます。オブジェクトコピーとオブジェクトミラーについても、バックアップされたオブジェクトと同じ情報がIDBに格納されます。

IDBの増大と性能: 主要な調整可能パラメーター

ロギングレベルとカタログ保護は、IDBの増大と性能を左右する要素のうちの主なものです。これらの要素がIDBに与える影響は、設定によって異なります。

IDBの主要な調整可能パラメーターとしてのロギングレベル

ロギングレベルとは

Data Protectorロギングレベルでは、バックアップ時にバックアップするファイルやディレクトリについてIDBに書き込む詳細情報の量を決定します。データは、バックアップ時のロギングレベルに関係なく、いつでも復元できます。

次の4つのロギングレベルが使用できます。

ロギングレベル

レベル	説明
すべてログに記録	バックアップされるファイルやディレクトリに関するすべての詳細情報(名称、バージョン、属性)を記録します。
ファイルレベルまでログに記録	バックアップされるファイルやディレクトリに関するすべての詳細情報(名称とバージョン)を記録します。これは、バックアップファイルおよびバックアップディレクトリに関する全詳細情報の約30%に相当します。
ディレクトリレベルまでログに記録	バックアップディレクトリに関するすべての詳細情報(名称、バージョン、属性)を記録します。これは、バックアップファイルおよびバックアップディレクトリに関する全詳細情報の約10%に相当します。
記録しない	バックアップファイルおよびディレクトリに関する情報をIDBに記録しません。

設定によって、IDBの増大や復元データのブラウズのしやすさに影響が生じます。

ロギングレベルとバックアップ速度

バックアップ速度は、どのロギングレベルを選択してもほとんど変わりません。

ロギングレベルと復元時のブラウズ

保存される情報のレベルを変更すると、復元時にData Protector GUIを使用したファイルのブラウズ機能も影響を受けます。[No Log]オプションを設定すると、ブラウズが不可能になり、[Log Directories]オプションを設定すると、ディレクトリのブラウズが可能になり、[Log Files]オプションを設定すると、完全ブラウズが可能になりますがファイル属性(サイズ、作成日付、変更日付など)は表示されません。

データの復元は、ロギングレベルの設定とは関係なく、いつでも行えます。

- データをブラウズする代わりに、いつでも手動でファイルを選択し復元できます(ファイル名が分かっている場合)。
- バックアップデータに関する情報はメディアから検索できます。

ロギングレベルと復元速度

復元速度は、対応するバックアップセッションが[Log All]、[Log Directories]、[Log Files]のどのロギングレベルを使用して実行してもほとんど変わりません。

[No Log]ロギングレベルを使用してバックアップセッションを実行した場合、単一ファイルを復元する場合に復元速度が速くなる可能性があります。この場合は、Data Protectorがオブジェクトの先頭からすべてのデータを読み取って復元対象のファイルを見つけることが必要になるためです。

システム全体を復元する場合は、バックアップオブジェクト全体が読み取られるので、ロギングレベルは影響しません。

IDBの主要な調整可能パラメーターとしてのカタログ保護

カタログ保護とは

カタログ保護は、IDBでのバックアップデータに関する情報の保管期間を決定します。バックアップデータの実際のメディア上の保管期間を決定するデータ保護とは異なります。カタログ保護がない場合でもデータは復元できますが、その場合はデータをData ProtectorのGUIで表示することはできません。

カタログ保護の概念は、最新の保存データが最も重要かつアクセス頻度も最大であるという事実に基づいています。古いファイルは頻繁に検索されないため、新しいファイルよりも検索に時間がかかります。

カタログ保護の期限切れ

カタログ保護期限が過ぎても、情報はすぐにIDBからは削除されません。Data Protectorは一日に一度自動的に削除作業を実行します。IDB内の情報はメディア単位でまとめられているため、メディアの全オブジェクトのカタログ保護期限が終了した時に完全に削除されます。

性能への影響

カタログ保護設定は、バックアップオブジェクトをブラウズする速度に影響します。

カタログ保護と復元

カタログ保護期限が過ぎたデータは[No Log]オプションを使用してバックアップしたデータと同様に復元されます。IDBの主要な調整可能パラメーターとしてのロギングレベル、前のページを参照してください。

ロギングレベルとカタログ保護の推奨使用方法

カタログ保護の常用

常に適切なレベルのカタログ保護を設定してください。ただし、[Log None]オプションが設定されている場合は例外です(この場合、カタログ保護を設定しても設定は適用されません)。

カタログ保護を[Permanent]に設定している場合、メディアをエクスポートまたは削除しない限りIDBの情報は削除されません。この場合、セル内のファイル数が変わらなくても、IDBのサイズはデータ保護期限が切れるまで直線的に増加します。たとえば、データ保護期間が1年で、メディアをリサイクルする場合、

1年を過ぎるとIDBはそれほど拡張しなくなります。新しいカタログとOBDBから削除されたカタログの容量はほぼ同じです。カタログ保護を4週間に設定した場合、4週間を過ぎるとIDBはそれほど拡張しなくなります。このため、カタログ保護を1年に設定した場合のIDBの大きさはこの場合の13倍になります。

少なくとも最新のフルバックアップがカタログ保護に含まれるように設定することをお勧めします。たとえば、フルバックアップのカタログ保護を8週間に設定して、増分バックアップを1週間に設定します。

同一セル内で異なるロギングレベルを使用

1つのセルが、毎日多数のファイルを生成するメール(または同種の)サーバー、少数のファイルにあらゆる情報を保存するデータベースサーバー、多数のユーザーのワークステーションなどで構成されていることはよくあることです。これらのシステムはそれぞれの変動の仕方がかなり異なるため、すべてに適合する1つの設定を決定することは困難です。このため、以下に示すロギングレベル設定で複数のバックアップ仕様を作成することをお勧めします。

メールサーバー: [Log Directories]を使用します。

データベースサーバー: 独自の復元ポリシーがあるため、ログは必要ありません。このため、[No Log]オプションを使用します。

ワークステーションおよびファイルサーバー: [Log All]または[Log Files]オプションを使用すると、さまざまなバージョンのファイルの検索と復元が可能です。[Log Directories]または[No Log]オプションを設定したバックアップでは、メディアから比較的短時間でカタログをインポートでき、選択したオブジェクトをブラウズできます。メディアからのカタログのインポートについては、『*HPE Data Protectorヘルプ*』のキーワード「インポート、メディアからカタログを」で表示される内容を参照してください。

オブジェクトコピーに異なるロギングレベルを設定

バックアップ対象のオブジェクトと、そのオブジェクトのコピーやミラーでは、ロギングレベルは同じでも、異なっていてもかまいません。オブジェクトコピーのロギングレベルは、バックアップポリシーに応じて、ソースオブジェクトのロギングレベルよりも詳細度が高いレベルや低いレベルに設定できます。

たとえば、バックアップセッションで正常にバックアップされたことを確実にするためにだけオブジェクトミラーを作成するような場合であれば、オブジェクトミラーには[No Log]オプションを指定するだけで十分です。バックアップの性能を向上させたい場合は、バックアップ対象のオブジェクトに[No Log]オプションを指定しておき、後から行われるオブジェクトコピーセッションでそのオブジェクトに[Log All]オプションを指定することもできます。

小規模のセルでの設定

セル内のファイル数が比較的少なく、将来もファイル数が増加しない場合で、セル内のシステムが通常の業務を実行している場合は、常にData Protectorのデフォルトの[Log All]オプションを使用できます。ただしこの場合、IDBの増大に注意し、適切なカタログ保護レベルを設定することが必要です。

大規模のセルでの設定

ファイル数が極度に増加する場合や、毎日多数のファイルが生成される場合に、[Log All]オプションを使用すると、比較的短期間でIDBの増大の問題が生じます。この場合、以下の方法があります。

- 許容できる一番低いレベルまでロギングレベルを下げます。

  [Log Files]オプションを使用するとIDBのサイズを減らすことができ、[Log Directories]オプションを使用すると、さらにサイズを減らせます。ただし、実際の増加はセル内のファイルシステムの性質に左右されます。
- カタログ保護を最小値に設定します。

- セルを2つに分割します。

  最終的なソリューションとしては、別のIDBを導入して、システムの半分をもう一方のIDBに転送する方法があります。

第6章: サービス管理

サービス管理、レポート、および監視機能は、管理者がバックアップ環境を効率よく管理するのに役立ちます。この章では、サービス管理機能の概念について説明するとともに、Data Protectorをスタンドアロンな形で使用する場合に得られる利点と、HPEサービス管理製品と統合した場合に得られる利点について、それぞれ説明します。

Data Protectorとサービス管理

Data Protectorはサービス管理機能をサポートしており、[[[Undefined variable DP.DP_OVO_full]]]サービス管理アプリケーションとの統合が可能です。

Data Protectorの機能

ここで説明する機能は、Data Protectorに組み込まれており、インストール後すぐに使用できます。

主要な機能

- 実行中のセッションを監視する機能が組み込まれているため、バックアップ環境内で発生した出来事にただちに対応できます。
- Data Protectorに組み込まれている通知およびレポート用エンジンを使用すると、さまざまな形式(ASCII、HTML、スプレッドシート互換形式など)で作成された要約レポートや即時警告を受け取って、これをさまざまな方法(電子メール、SNMP、Windowsシステム上でのみ可能なブロードキャスト、ファイルへの書き込み、外部コマンドへの送信など)で配布できます。Data Protectorの組み込み通知エンジンでは、SNMPを介して警報を送信できるため、SNMPトラップを受け取ることができるアプリケーションであれば、事実上どのアプリケーションとも統合することが可能です。
- Data Protectorバックアップセッション監査監査では、Data Protectorのセル全体で長期にわたって実行されたすべてのバックアップタスクに関する情報が保存され、監査および管理のため必要に応じて、統合的かつ印刷可能な形式でこの情報が提供されます。
- Data Protectorでは、主要かつ重大なイベントをWindowsのイベントログに送ることができるため、これを利用してさまざまな興味深い統合機能を開発できます。

SNMPトラップ

SNMPトラップの使用により、Data Protectorのイベント発生時、またはData Protectorのチェックおよび保守の機構の結果としてSNMPトラップが送信されたときに、サービス管理アプリケーションがSNMPトラップメッセージを受信および処理できるようになります。Data ProtectorのSNMPトラップの構成の詳細については、『*HPE Data Protectorヘルプ*』のキーワード「SNMP、レポートの送信方法」で表示される内容を参照してください。

Data Protectorモニター

Data Protectorモニターは、Data Protectorユーザーインターフェイスの一部であり、現在実行中のバックアップ、復元、およびメディア管理の各セッションの監視や修正処置の実行に使用します。モニター内にはセル内のすべてのセッションが表示され、これらのセッションに関する詳細メッセージと現在の状態をチェックできます。複数セル環境では、他のセルにあるシステム上で実行中のセッションを監視することも可能です。モニターのユーザーインターフェイスからは、バックアップや復元、メディア管理の各セッションを中止したり、「マウント」要求に応答したりすることができます。

Manager-of-Managers機能を使用する場合は、1つのユーザーインターフェイスから、複数のセルで実行中のセッションを同時に監視できます。

レポートと通知

Data Protectorのレポート機能では、バックアップ環境の管理と計画にとって、強力でカスタマイズ可能な柔軟性のあるツールを提供しています。Data Protectorには豊富なレポート機能が組み込まれており、システム管理者は従来からこれらの機能に立脚してCell Managerを管理してきました。これらのレポート機能は、ITサービスプロバイダーが、SLAに定義されたデータ保護レベルを達成していることを実証する際にも役立ちます。サービスレベル管理に特に関係が深い組み込みのレポート機能は、以下のとおりです。

- インベントリ/ステータス関連レポート。たとえば、保護されていないシステムに関する情報を示すData Protector向けに構成されていないクライアントレポート、スケジューリングされているバックアップ、オブジェクトコピー、オブジェクト集約をすべて一覧表示する*セッション仕様スケジュール*レポート、メディアインベントリレポートである*プールのリスト*レポートなど。
- 稼動率関連レポート。たとえば、Data Protectorライセンスの使用状況を示す*ライセンス*レポートや、バックアップ、オブジェクトコピー、またはオブジェクト集約に現在使われていないために使用可能なデバイスの一覧を示す*Data Protectorが使用していない構成済みデバイス*レポートなど。
- 問題関連レポート。たとえば、バックアップ、コピー、および集約に失敗したセッションに関連する情報を示す*Session Statistics*レポートなど。管理者は、失敗したジョブとその原因を示す電子メールレポートを、毎時、毎日、または週1回のペースで受け取ることができます。

Cell Managerに従来から組み込まれているこれらのレポート機能と通知機能を利用すると、以下のような処理も可能です(これらの機能は従来のバージョンより大幅に機能拡張されています)。

- 事前構成された多数のレポートが用意されており、たとえば、指定した時間帯に実行されたセッションに関するレポート、IDBレポート、デバイス使用状況レポートなどを作成できます。
- これらのレポートはパラメーターを指定してカスタマイズすることもできます(対象となる時間帯、バックアップ、コピー、および集約の仕様、*バックアップグループ*など)。
- さまざまな出力形式を選択できます(ASCII、HTML、スプレッドシート互換形式など)。
- これらのレポートに対して、Data Protectorの組み込みスケジューラーを使ったスケジューリングも可能です。
- 何らかのイベントに基づいて、これらのレポート送信を開始することも可能です(デバイス障害、マウント要求、セッションの終了時など)。
- さまざまな配布方法の中から、レポートを受け取る方法を選択できます(電子メール、SNMP、Windowsシステムでのみ可能なブロードキャスト、ファイルへの書き込み、外部コマンドへの送信など)。

これらの出力形式、配布方法、スケジュール方法、開始方法などの大部分は、自由に組み合わせられます。

以下にいくつかの例を示します。

レポートと通知に関する問題

- 毎朝7:00に、24時間以内に実行されたバックアップ、コピー、および集約の各セッションに関するレポートを作成し、これをASCII形式の電子メールの形でバックアップ管理者のメールボックスに送信します。さらに同じレポートを、Webサーバー上にHTMLファイル形式で書き込んで、他のユーザーもこの情報を利用できるようにします。
- デバイス障害やマウント要求が発生した場合は、ブロードキャストメッセージをただちにバックアップ管理者のWindowsワークステーションに送信し、さらに外部コマンドを開始して、バックアップ管理者のポケットベルを呼び出します。
- バックアップセッションの終了時には、バックアップされたシステムを所有しているエンドユーザーに、バックアップ状態を示すレポートを、ASCII形式の電子メールで送信します。

イベントロギングと通知

Data Protectorのイベントログは、Data Protector関連の通知すべてを管理する中央レポジトリです。Data Protectorイベントログに記録されるイベントは、プロセスまたはユーザーのどちらかによってトリガーされたイベントです。Data Protectorの組み込み通知エンジンは、ログエントリに基づいて、警報の送信やData Protectorレポート機構の開始などを実行します。イベントログは、Data ProtectorやHPEソフトウェア管理アプリケーションでSLAへの適合を示すレポートを生成するための情報ソースとなります。さらにレポート機能に加えて、ログエントリからHPEソフトウェア管理アプリケーションにData Protector SPI(SMARTプラグイン)経由で情報を提供することにより、予防処置や修正処置を実施することも可能です。

Data Protectorの組み込み通知エンジンは、SNMPを介して警報を送信できるため、SNMPトラップを受け取ることができるアプリケーションであれば、事実上どのアプリケーションとも統合することが可能です。

イベントログへのアクセスはData Protectorの**[Admin]**グループに属するユーザーおよび[Reporting and notifications]のユーザー権限を持つData Protectorユーザーに限られています。Data Protector**イベントログ**内のすべてのイベントは、イベントログビューアーを使用して表示または削除できます。

Data Protectorログファイル

サービス管理アプリケーションの中には、特定のログエントリに関して、モニターするログファイルと時間を指定できるものがあります。特定のエントリがファイル内で検出された場合、動作を指定できます。

このようなサービス管理アプリケーションを構成することにより、特定のログエントリ(Data Protectorイベント)についてData Protectorログファイルをモニターしたり、特定のData Protectorイベントが検出された場合に実行される動作を定義できます。

Data Protectorのログファイルの詳細については、『*HPE Data Protectorトラブルシューティングガイド*』と『*HPE Data Protectorヘルプ*』を参照してください。

Windowsアプリケーションログ

一部のサービス管理アプリケーションは、Windowsアプリケーションログを監視します。

Data ProtectorメッセージとData Protectorサービスに関連するメッセージ(停止している場合)をすべてWindowsアプリケーションログに自動転送する方法は、『HPE Data Protectorトラブルシューティングガイド』を参照してください。

Data Protectorのチェックおよび保守の機構

Data Protectorには日常のセルフチェックや保守のための、さまざまな自動化された機構が備わっており、処理の信頼性や予測可能性の向上に役立っています。Data Protectorのセルフチェックや保守の処理には次のものがあります。

- 「空きメディア不足」のチェック
- 「Data Protectorライセンス期限」のチェック

詳細については、『*HPE Data Protectorヘルプ*』のキーワード「Data Protectorが実行するチェック」で表示される内容を参照してください。

中央管理、分散環境

Data ProtectorのMoM機能を使用すると、管理者は複数のData Protector Cell Managerから構成される企業環境を一元管理することができます。MoMシステム管理者は、単一のコンソールから、企業全体にわたる構成、メディア管理、監視、ステータスレポートの作成などの作業を実施できます。MoMを使用すると、多数のData Protector Cell Managerを、1つを管理している場合と同じように簡単に管理できます。またITサービスプロバイダーは、スタッフを増員することなしに、より大規模なクライアント環境を管理することが可能になります。MoMの詳細については、『*HPE Data Protectorヘルプ*』のキーワード「MoM環境」で表示される内容を参照してください。

Data Protectorが提供するデータの使用

データの用途

Data Protectorが提供するデータは、以下に示すような形で使用できます。

- バックアップオペレーター、エンドユーザー、管理者などに、電子メール形式でレポートを定期的に送信できます(Data Protector組み込みレポート機能の電子メール送信機能を使用)。
- バックアップレポートがWebサーバーに書き込まれ、各ユーザーが必要に応じて使用できるようになります(Data Protector組み込みレポート機能のHTMLレポート作成機能を使用)。
- Data Protectorの主要かつ重大なイベントを、Data Protectorなどのネットワーク管理ソリューションに送信できます(組み込み通知エンジンのSNMPトラップ送信機能を使用)。

第7章: Data Protectorが機能する仕組み

この章では、Data Protectorが機能する仕組みについて説明します。ここでは、Data Protectorのプロセス(UNIXの場合)とサービス(Windowsの場合)、バックアップセッションと復元セッション、およびメディア管理セッションについて、順に説明していきます。

Data Protectorのプロセス(サービス)

Data Protectorでは複数のプロセス(UNIXの場合)とサービス(Windowsの場合)がバックグラウンドで実行されており、これらのプロセス(サービス)により、バックアップセッションおよび復元セッションの実行が可能になります。また、必要な通信パスの確立、バックアップセッションおよび復元セッションの起動、Disk AgentおよびMedia Agentの起動、バックアップされたデータに関する情報の保存、メディア管理などの各種機能が実行されます。

プロセスまたはサービス

プロセス(サービス)	説明
CRS	CRS (Cell Request Server)プロセス(サービス)は、Data Protector Cell Manager上で実行されます。CRSは、バックアップセッションおよび復元セッションの開始および制御を担当しています。このサービスは、Data ProtectorをCell Managerシステム上にインストールした時点で開始され、システムが再起動されるたびに再起動されます。
MMD	MMD (Media Management Daemon)プロセス(サービス)は、Data Protector Cell Manager上で実行され、メディア管理およびデバイス操作を担当しています。このプロセスは、Cell Request Serverプロセス(サービス)により開始されます。
Inet	Data Protector Inetサービスは、Data Protectorセル内の個々のWindowsシステム上で実行されます。Inetは、セル内のシステム間の通信と、バックアップおよび復元に必要なその他のプロセスの開始を担当しています。Data Protector Inetサービスは、Data Protectorをシステム上にインストールした時点で開始されます。UNIXシステム上では、システムのinetデーモン(INETD)により、Data ProtectorのInetプロセスが開始されます。
KMS	KMS(Key Management Server)プロセス(サービス)は、Cell Manager上で動作し、Data Protectorの暗号化機能のためのキー管理を提供します。このプロセスは、Data ProtectorをCell Managerにインストールしたときに開始されます。
hpdp-idb	Data Protector内部データベースサービス(hpdp-idb)は、IDBを実行するサービスです。内部データベースサービスは、内部データベースからの情報を必要とするプロセスによってCell Manager上でローカルにアクセスされます。このサービスは、Cell Manager上のIDBからManager-of-Manager(MoM)上のIDBへの転送に関するメディア管理情報に対してのみリモートでアクセスされます。
hpdp-idb-cp	Data Protector内部データベース接続プーラー(hpdp-idb-cp)サービスは、hpdb-idbへの開いた接続のプールを提供します。プールされた接続を使用できるので、要求のたびに新しい接続を開く必要がなく、hpdp-idb接続の拡張性が確保されます。このサービスは、Cell Manager上で実行され、ローカルプロセスによってのみアクセスされます。
hpdp-as	Data Protectorアプリケーションサーバー(hpdp-as)サービスは、HTTPS接続(Webサービ

プロセス(サービス)	説明
	ス)を介したIDBへのGUI接続に使用されます。このサービスはCell Manager上で実行され、hpdp-idb-cpサービスへのローカル接続があります。

Data Protectorのプロセスおよびサービスを、手動で開始または停止する方法は、『*HPE Data Protector ヘルプ*』を参照してください。

コピーセッションマネージャー(CSM)の再接続機能

Data Protectorは、コピー、集約、または複製セッションを実行しているときに、Media Agent(BMA、RMA、またはMMA)とCSM間で切断された接続を再接続しようとします。

デフォルトでは、Data Protectorの切断された接続の再接続機能は使用可能になっています。

切断された接続の再接続機能を無効化するには、セルサーバーでomnircオプションOB2_CSM_NORECONを1に設定します。

Data Protectorでは、デフォルトで20分ごとに再接続を試みます。このタイムアウト時間を変更するには、セルサーバーとクライアントでomnircオプションOB2RECONNECT_RETRYを設定します。セルサーバーとクライアントの値は同期している必要があります。

> **注:**
> クライアントのOB2RECONNECT_RETRYオプションは、エラーの後にクライアントが再接続を試行する時間を表します。サーバーのOB2RECONNECT_RETRYオプションは、クライアントの再接続をサーバーが待つ時間を表します。

Cell Manager間の複製に関する制限

Cell Manager間の複製を実行する場合は、MSMとCSMの間では再接続は有効になりません。修復できるのは、MAとCSMの間の接続のみです。

バックアップセッション

この項では、バックアップセッションの開始方法、バックアップセッション中の処理内容、および関連するプロセスとサービスについて説明します。

あるバックアップ仕様が開始されると、バックアップセッションと呼ばれる処理が実行されます。バックアップセッションでは、ソース(通常はハードディスク)上のデータが、バックアップ先(通常はテープメディア)にコピーされます。バックアップセッションの実行後には、バックアップメディア上にデータのコピー(メディアセット)が作成されています。

スケジュール形式または対話形式のバックアップセッション

スケジュール形式のバックアップセッション

スケジュール設定されたバックアップセッションは、指定時刻にData Protectorスケジューラーによって起動されます。スケジュール形式のバックアップセッションの進捗状況は、Data Protectorモニターでモニタリングできます。

対話形式のバックアップセッション

対話式複製セッションは、Data Protectorユーザーインターフェイスから直接開始します。この場合はData Protectorモニターがすぐに起動され、バックアップセッションの進捗状況を監視できます。なお、複数のユーザーが同じバックアップセッションをモニターできます。ユーザーインターフェイスをセッションから切断して、モニターを停止することもできます。セッションは、その後、バックグラウンドで継続されます。

バックアップセッションにおけるデータフローとプロセス

バックアップセッション中の処理内容

バックアップセッションにおける情報の流れは、バックアップセッションにおける情報の流れ(1)、次のページに示すような形になります。これは標準的なネットワークバックアップを実行する場合のデータフローやプロセスです。その他のバックアップ方法(スプリットミラーバックアップなど)におけるデータフローやプロセスについては、関連する章を参照してください。

バックアップセッションが開始されると、以下の処理が実行されます。

1. BSM(バックアップセッションマネージャー)プロセスが、Cell Managerシステム上で開始されて、バックアップセッションを制御します。このプロセスにより、バックアップ仕様内に指定されているバックアップ対象、オプション、バックアップ用メディアとデバイスなどの情報が読み取られます。
2. BSMにより、IDBがオープンされて、生成されるメッセージのほか、バックアップデータに関する詳細や、使用するデバイスやメディアに関する情報など、バックアップセッションに関する情報がデータベース内に書き込まれます。
3. BSMにより、バックアップ用デバイスが構成されているシステム上で、Media Agent (MA)が起動されます。ドライブが並列に使用される場合は、ドライブごとに個々のMedia Agentが開始されます。同一セル内で開始できるMedia Agentの数は、セルの構成と購入しているライセンスの数とによって制約されます。

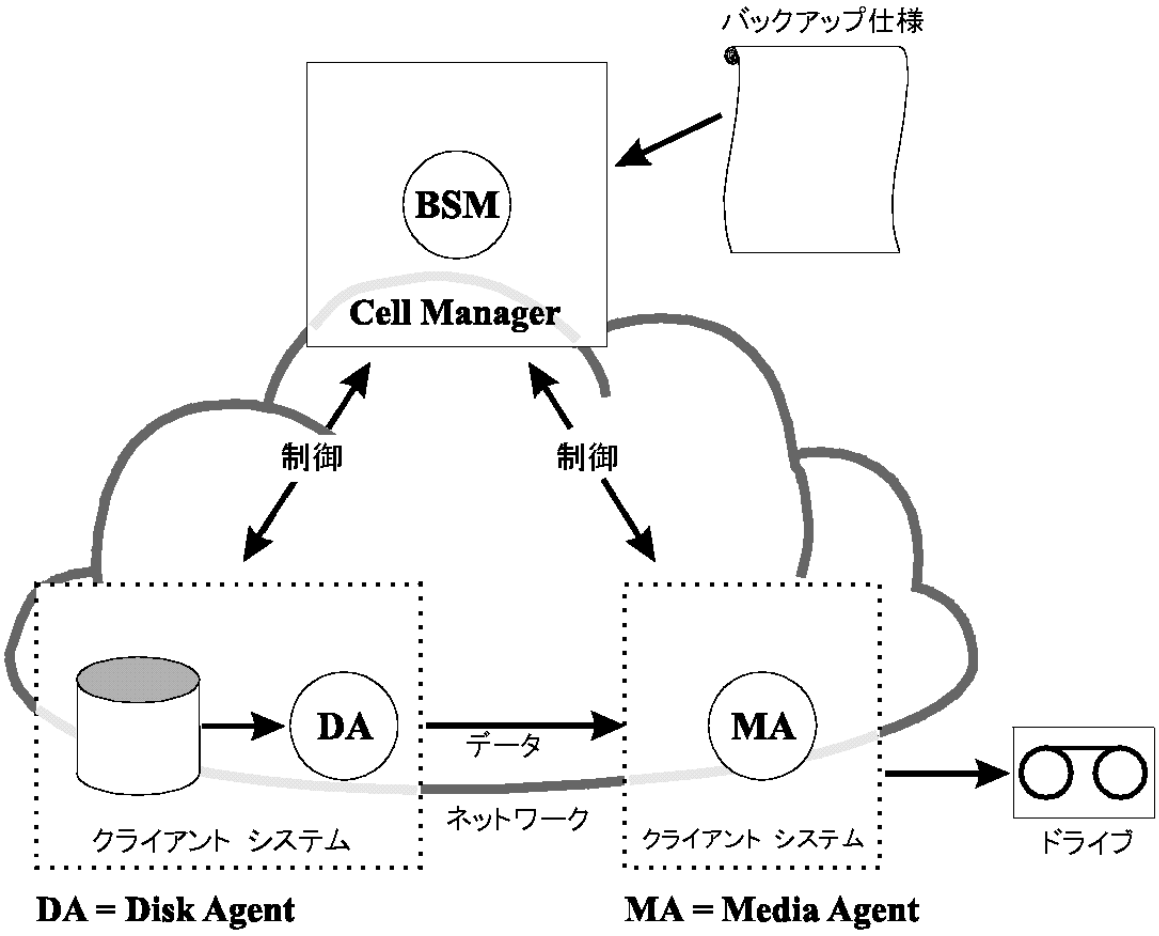
   オブジェクトミラーの作成を伴うバックアップセッションの場合は、BSMにより、ミラー作成用のMedia Agentも開始されます。
4. BSMにより、並行してバックアップされるディスクごとに、個々のDisk Agent(DA)が起動されます。実際に起動されるDisk Agentの数は、バックアップ仕様に構成されたDisk Agentの同時実行数に基づいて決められます。これは、デバイスストリーミングを維持するために、同時に開始できるDisk Agentの数を示すものであり、これらのDisk Agentから1つのMedia Agentにデータが並行して送られます。
5. Disk Agentによりディスク上のデータが読み取られてMedia Agentに送信され、このMedia Agentによ

りメディアに書き込まれます。

オブジェクトミラーの作成を伴うバックアップセッションでは、ミラーオブジェクトの書き込みに使用される各Media Agentが、デイジーチェーン方式で連結されます。個々のMedia Agentは受け取ったデータをメディアに書き込み、処理が終わると、チェーン内の次のMedia Agentにデータを渡します。

6. セッションの進捗状況はBSMによりモニタリングされており、必要に応じて新しいDisk AgentやMedia Agentが開始されます。
7. バックアップセッションが終了したら、BSMによりセッションが閉じられます。

バックアップセッションにおける情報の流れ(1)

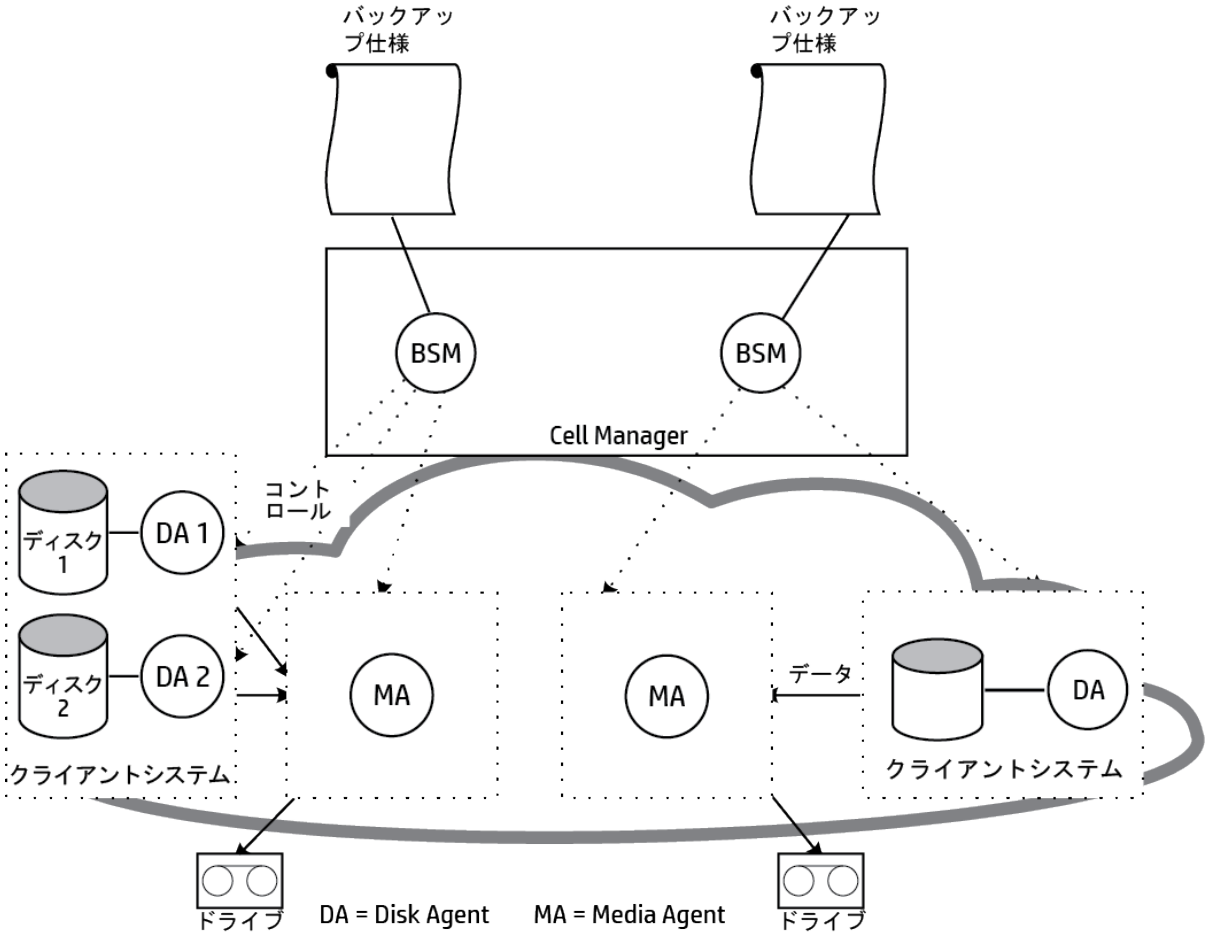


同時に実行できるセッションの数

セル内では同時に複数のバックアップセッションを実行できます。同時に実行できるセッションの数は、デバイスの可用性やCell Managerの構成(たとえば、プロセッサーの速度、メインメモリの容量など)、セル内のリソースによって制限されます。Data Protectorのプロセスがシステムの能力を超えないよう、同時実行できるバックアップセッションの最大数は制限されます。この最大数は変更可能です。

バックアップセッションにおける情報の流れ ー 複数のセッション、次のページは、同時実行されている複数のセッションを示しています。

バックアップセッションにおける情報の流れ ー 複数のセッション



実行前コマンドと実行後コマンド

Data Protectorの実行前コマンドを使うと、バックアップセッションまたは復元セッションの開始前に何らかの処理を実行できます。Data Protectorの実行後コマンドを使うと、バックアップセッションまたは復元セッションの終了後に何らかの処理を実行できます。典型的な実行前処理としては、データの整合性をとるためのデータベース停止処理などが挙げられます。

実行前コマンドおよび実行後コマンドは、バックアップ仕様に対して設定して、Cell Managerシステム上で実行することもできれば、バックアップオブジェクトオプションとして指定して、それぞれのDisk Agentが実行されているクライアントシステム上で実行することもできます。

実行前スクリプトコマンドおよび実行後スクリプトコマンドは、実行可能ファイルまたはシェルスクリプトとして作成できます。これらはData Protectorが提供するものではなく、バックアップオペレーターなどが自分で記述する必要があります。

コマンドの起動と場所

バックアップセッション用の実行前および実行後コマンドは、それぞれバックアップセッションの前および後に起動します。これらはデフォルトではCell Manager上で実行されますが、別のシステムも選択できます。

Windowsシステム

実行前および実行後スクリプトは、Cell Manager上で実行された場合はData Protector CRSによって起動されます。リモート実行された場合は、Data Protector Inet Serviceアカウント(デフォルトではローカルシステムアカウント)で実行されます。

Cell Managerおよび他のシステムのスクリプトはData_Protector_home\binディレクトリに格納します。ユーザーは、ファイル名または相対パス名のみを指定します。

スクリプトが*Data_Protector_home*\binディレクトリにある場合は、ファイル名だけを指定します。それ以外の場合は、スクリプトのフルパス名を指定します。

実行前コマンドおよび実行後コマンドでサポートしている拡張子は、.bat、.exe、および.cmdのみです。サポートされていない拡張子(.vbsなど)を使用したスクリプトを実行するには、そのスクリプトを起動するバッチファイルを作成します。そして、そのバッチファイルを実行前コマンドまたは実行後コマンドとして実行するようにData Protectorを構成します。これにより、サポートされていない拡張子のスクリプトが起動されます。

パス名を指定するのに引用符("")を使用する場合、円記号と引用符(\")を組み合わせて使用しないでください。パス名の末尾に円記号を入力するには、二重の円記号として入力してください(\\)。

> **注:**
> perl.exeを直接使用することはできません。

UNIXシステム

実行前スクリプトと実行後スクリプトは、バックアップセッションオーナーのアカウントで実行されます。ただし、例外として、バックアップセッションオーナーにBackup as rootパーミッションが付与されている場合は、rootで実行されます。

Cell ManagerまたはリモートUNIXクライアント上では、バックアップ仕様の実行コマンドを以下のディレクトリに置く必要があります。

HP-UXシステム、Solarisシステム、Linuxシステムの場合:/opt/omni/lbin

その他のUNIXシステムの場合:/usr/omni/bin

コマンドを/opt/omni/lbinまたは/usr/omni/binディレクトリに置いた場合は、ファイル名だけを指定します。他のディレクトリに置いた場合は、フルパス名を指定する必要があります。

詳細については、『*HPE Data Protectorヘルプ*』の「*バックアップ仕様を対象とする実行前/実行後コマンド*」を参照してください。

バックアップセッションにおける待ち行列

タイムアウト

バックアップセッションが開始されると、Data Protectorにより、デバイスなどの必要な全リソースの割り当てが試みられます。いずれかのリソースが使用できるようになるまで、セッションは待ち行列に入れられます。タイムアウトになってもリソースがまだ使用できない場合は、そのセッションは中止されます。

負荷の最適化

Cell Managerの負荷を最適化するために、Data Protectorは、デフォルトでは、最大5つのバックアップセッションを同時に開始できるようになっています。このデフォルトの値は、Data Protectorグローバルオプションを使用することにより変更可能です。これ以上のセッションが同時にスケジュール設定された場合には、処理できないセッションは待ち行列に入れられて、他のセッションの終了後に開始されます。

バックアップセッションにおけるマウント要求

バックアップセッション中に新しいバックアップ用メディアが必要になり、そのメディアが使用可能でない場合には、Data Protectorからマウント要求が発行されます。

Data Protectorは、次のいずれかの場合にマウント要求を発行します。

マウント要求の発行

- バックアップメディア上のスペースが不足したが、使用可能な新しいメディアがない場合。
- Data Protectorのメディア割り当てポリシーにより特定のメディアが要求されたが、そのメディアがデバイス内にない場合。
- バックアップに使用するメディアの順番が事前割り当てリスト内に指定されているが、この順番でメディアを使用できない場合。

詳細については、バックアップセッション中にデータをメディアに追加、ページ 159およびバックアップ用メディアの選択、ページ 158を参照してください。

マウント要求への対応

マウント要求に対応するには、要求されたメディアをセットし、バックアップ処理を続行するようData Protectorに指示します。

Data Protectorでは、マウント要求が発行された場合の動作を、次のような形で事前に設定できます。

オペレーターに通知を送付

Data Protectorの通知機能を使って、マウント要求に関する情報をオペレーターに電子メールで送信することができます。オペレーターはこの情報に基づいて、必要なメディアを手動でロードしたり、セッションを停止したりするなど、何らかの適切な操作を行います。詳細は、「レポートと通知、ページ 179」を参照してください。

マウント要求への自動応答

マウント要求への応答を自動化することも可能です。このためには、必要な動作を実行するためのスクリプトまたはバッチプログラムを記述しなければなりません。

ディスクディスカバリバックアップ

ディスクディスカバリバックアップの場合は、バックアップセッションの開始Data Protector時点で、まずバックアップ対象となるシステム上の詳細なディスク一覧が自動的に作成されて、すべてのディスクがバックアップ範囲に含まれます。そのため、バックアップ構成時にシステム上に存在していなかったディスクも含めて、すべてのローカルディスクのバックアップが可能になります。構成が時々刻々急激に変更されるような環境で

は、このディスクディスカバリバックアップが特に有効です。バックアップ時に特定のディレクトリのみを選択したり、除外したりすることも可能です。

標準的なバックアップとの違い

標準的なバックアップの場合は、バックアップ構成時に、バックアップするディスク、ディレクトリ、またはその他のオブジェクトを、バックアップ仕様内に明示的に指定しておく必要があります。この場合、指定されたオブジェクトのみがバックアップ対象となります。そのため、システムに新しいディスクを追加したり、別のオブジェクトをバックアップしたりする場合には、バックアップ仕様を手動で変更して、これらの新しいオブジェクトを追加する必要があります。ディスクディスカバリバックアップと標準的なバックアップのどちらを使用するかは、バックアップの構成時に選択できます。

バックアップセッションの再開

ネットワークの問題などによって正常に完了しなかったバックアップセッションや中止されたバックアップセッションは、Data Protector再開セッション機能を使用して再開できます。失敗したバックアップセッションを再開すると、Data Protector失敗したセッションが中止されたところからバックアップが再開されます。

復元セッション

この項では、復元セッションの開始方法、復元セッションの処理内容、および関連するプロセスとサービスについて説明します。

復元セッションでは、バックアップコピー(通常はテープメディア)からディスクへデータが戻されます。

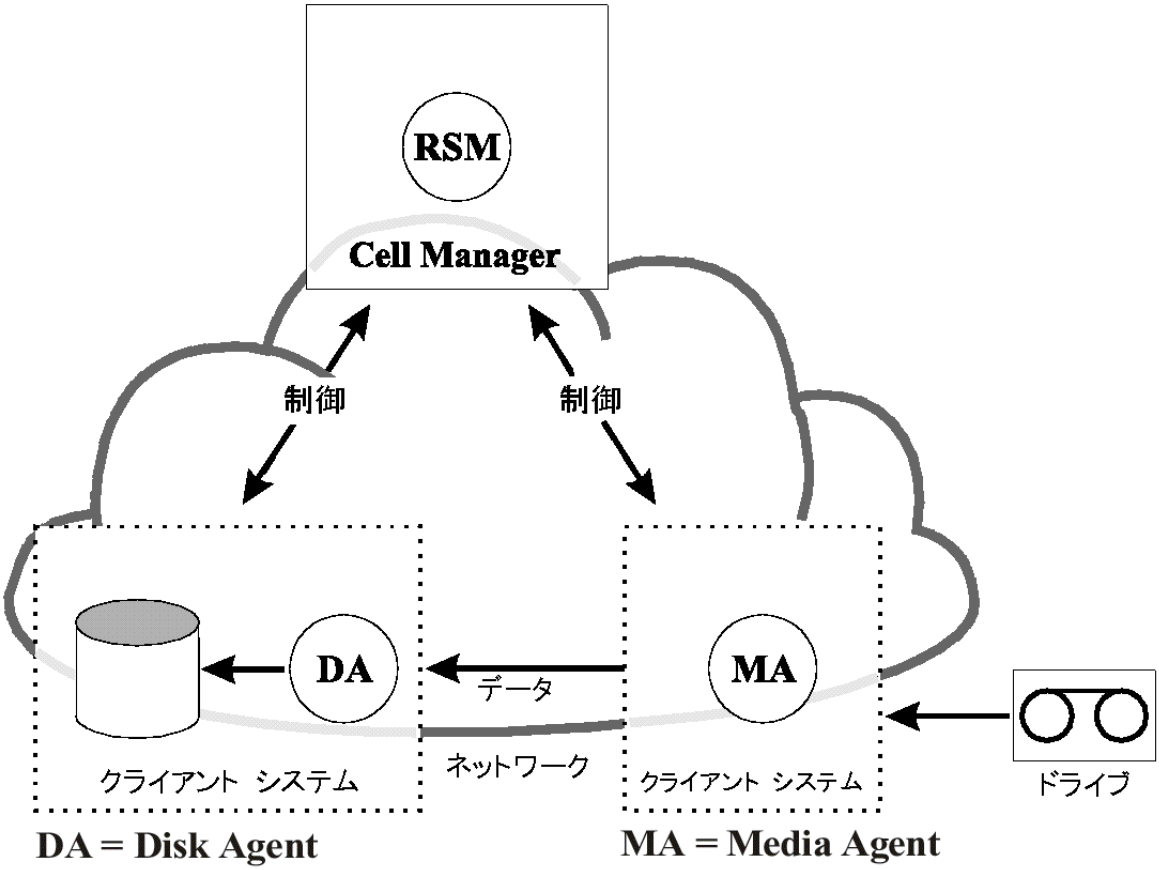
復元セッションは対話形式で起動されます。Data Protectorで何を復元するかを指定すると、Data Protectorによって必要なメディアが判断され、いくつかのオプションが選択されて、復元が開始されます。ユーザーはセッションの進行状況をモニターできます。

復元セッションにおけるデータフローとプロセス

復元セッションの情報フロー、次のページのように復元セッションが開始されると、以下の処理が実行されます。

1. 復元セッションマネージャー(RSM)プロセスは、Cell Managerシステム上で開始されます。このプロセスによって、復元セッションが制御されます。
2. RSMによってIDBがオープンされ、復元に必要なメディアの情報が読み取られ、復元セッションの情報(生成されるメッセージなど)がIDBに書き込まれます。
3. RSMにより、復元に使用するデバイスがあるシステム上で、Media Agent (MA)が起動されます。並行して使用される各ドライブで、新たにMedia Agentが起動されます。
4. 並行して復元される各ディスクに対して、RSMによりDisk Agent (DA)が起動されます。起動されるDisk Agentの実際の数は、復元を選択したオブジェクトに依存します。詳細については、並行復元、ページ 191を参照してください。
5. Media Agentによりメディアからデータが読み取られ、ディスクにデータが書き込まれるDisk Agentに対して、そのデータが送信されます。RSMにより、セッションの進行状況がモニターされ、必要に応じて新規のDisk AgentやMedia Agentが起動されます。
6. 復元セッションが完了すると、RSMによりセッションがクローズされます。

復元セッションの情報フロー



同時に実行できる復元セッションの数

セル内では、多数の復元セッションを同時に実行できます。同時に実行できるセッションの数は、Cell Managerや、デバイスを接続しているシステムなど、セル内のリソースによって制限されます。

複製セッションにおける待ち行列

タイムアウト

復元セッションが起動されると、Data Protectorにより、バックアップデバイスなどの必要なすべてのリソースの割り当てが試行されます。必要最小限のリソースが使用可能になるまで、セッションは待ち行列に入れられます。Data Protectorにより、タイムアウトと呼ばれる特別な時間内に、リソースの割り当てが試行されます。ユーザーは、タイムアウトの時間を設定することができます。タイムアウトになってもリソースがまだ使用できない場合は、そのセッションは中止されます。

復元セッションにおけるマウント要求

マウント要求は、復元セッションで復元に必要なメディアがデバイス内で使用可能でない場合に出されます。Data Protectorでは、マウント要求が発生したときに実行する処理を構成することができます。

マウント要求への対応

マウント要求に対応するには、要求されたメディアまたはメディアのコピーをセットし、Data Protectorに復元処理を実行するよう指示します。

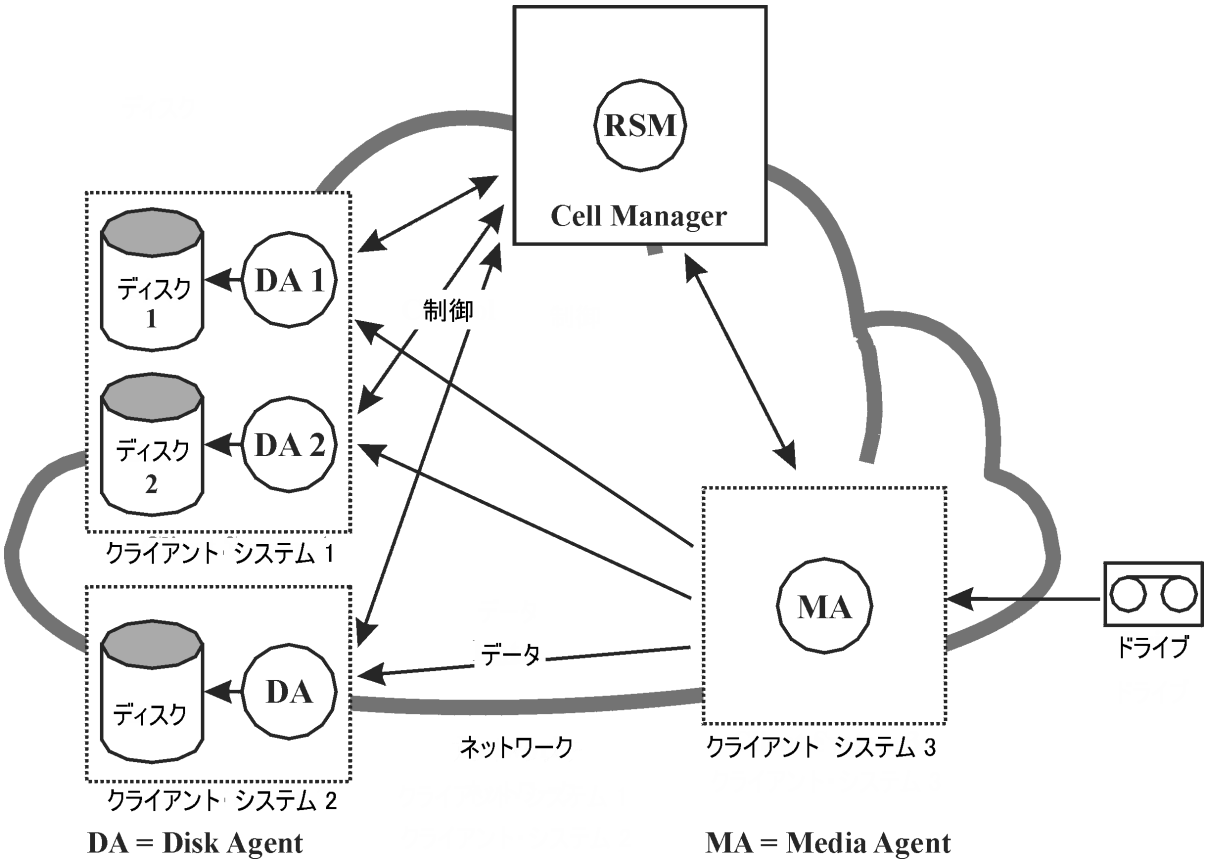
並行復元

並行復元では、複数オブジェクトのインターリーブデータがメディアから単一パスで同時に読み取られ、復元されます。並行復元により、同一メディアから複数オブジェクトを復元する際のパフォーマンスが大幅に改善されます。詳細については、並行復元セッションのフロー、下を参照してください。

標準的な復元との比較

複数のDisk Agentからのデータは(ほとんどの場合)、多重化されメディア上に保存されます。1つのメディアに複数のセッションとオブジェクトを分配する(順次書き込み)、ページ 159を参照してください。標準的な復元の場合、Data Protectorによってメディアから多重化されたデータが読み取られ、選択されたオブジェクトで必要な部分だけがアセンブルされます。次のオブジェクトが復元される際には、両オブジェクトが同じメディア上にあり、多重化を使用して書き込まれると想定して、Data Protectorでメディアを巻き戻し、次のオブジェクトの部分を読み取る必要があります。

並行復元セッションのフロー



並行復元では、Data Protectorによって、選択されたすべてのオブジェクトの多重化データが読み取られ、直ちに全オブジェクトに必要な部分がアセンブルされて、正しいDisk Agentに正しいデータが送信さ

れます。これにより、メディアからの読み取りパフォーマンスが向上します。選択されたオブジェクトが異なる物理ディスクに書き込まれる場合には、パフォーマンスがさらに向上します。この場合、データは同時に複数のディスクにコピーされます。

高速な複数の単一ファイル復元

Data Protectorでは、復元パフォーマンスを向上させるために不連続のオブジェクト復元が使用されます。あるファイルかツリーが復元された後、少なくとも1セグメントがファイル間またはツリー間にある場合、Data Protectorの位置は、メディア上の次のファイルまたは次のツリーに、直接、移動されます。

個々の復元オブジェクト内では、複数のDisk Agentを起動することができます。この方法により、メディア中のさまざまな場所に存在する複数の単一ファイルの復元処理は、Data Protectorがメディア内をトラバースするよりはるかに高速になります。

復元セッションの再開

ネットワークの問題などによって正常に完了しなかった復元セッションは、Data Protector再開セッション機能を使用して再開できます。失敗したセッションを再開すると、Data Protectorは、失敗したセッションが中止したところから新規セッションで復元を続行します。

オブジェクトコピーセッション

ここでは、オブジェクトコピーセッションの開始方法、セッション中の処理内容、および関連するプロセスとサービスについて説明します。

オブジェクトコピーセッションとは、バックアップ、コピー、または集約されたデータの追加コピーを別のメディアセット上に作成するプロセスです。オブジェクトコピーセッション中に、選択されたバックアップ、コピー、または集約オブジェクトがソースからターゲットメディアへコピーされます。

> **注:**
> **再接続**機能は、デフォルトで使用可能になっています。詳細については、コピーセッションマネージャー(CSM)の再接続機能、ページ 183を参照してください。

自動および対話形式のオブジェクトコピーセッション

自動オブジェクトコピーセッション

自動オブジェクトコピーセッションは、スケジュールを設定して開始することも、バックアップ、オブジェクトコピー、またはオブジェクト集約の直後に開始することも可能です。スケジュール設定されたオブジェクトコピーセッションは、Data Protectorスケジューラーで指定した時刻に開始されます。一方、ポストバックアップ、ポストコピー、またはポスト集約オブジェクトコピーセッションは、指定したセッションの終了後に開始されます。自動オブジェクトコピーセッションの進行状況は、Data Protectorモニターで確認できます。

対話形式のオブジェクトコピーセッション

対話形式のオブジェクトコピーセッションは、Data Protectorユーザーインターフェイスを使用してオペレーターが直接開始します。Data Protectorモニターがすぐに起動され、セッションの進行状況を監視できま

す。複数のユーザーが同一のバックアップセッションをモニタリングすることも可能です。ユーザーインターフェイスをセッションから切断して、モニターを停止することもできます。セッションは、その後、バックグラウンドで継続されます。

オブジェクトコピーセッションにおけるデータフローとプロセス

オブジェクトコピーセッションにおける情報の流れは、オブジェクトコピーセッションにおける情報の流れ、次のページに示すような形になります。オブジェクトコピーセッションが開始されると、以下の処理が実行されます。

1. CSM(コピーおよび集約セッションマネージャー)プロセスが、Cell Managerシステム上で開始されます。このプロセスは、オブジェクトコピー仕様に指定されたコピー対象、オプション、使用するメディアとデバイスなどの情報を読み取ります。またこのプロセスは、オブジェクトコピーセッション全体を制御します。
2. CSMがIDBをオープンし、コピーに必要なメディアの情報を読み取り、オブジェクトコピーセッションの情報(生成されるメッセージなど)をIDBに書き込みます。
3. CSMにより、デバイスがロックされます。セッションは、すべての読み取りMedia Agentと必要な最小限の書き込みMedia Agentがロックされるまで、バックアップと同じタイムアウトの時間を使用して待ち行列に入れられます。タイムアウトになってもリソースがまだ使用できない場合は、そのセッションは中止されます。
4. CSMにより、コピー用デバイスが構成されているシステム上でMedia Agentが開始されます。Media Agentは、バックアップポリシーに従って割り当てられたソースメディアとターゲットメディアをロードします。
5. Media Agentがコピー元メディアからデータを読み取り、コピー先メディアを担当するMedia Agentに接続します。

   オブジェクトごとにコピー先デバイスを指定していない場合、Data Protectorはオブジェクトコピー仕様内に指定されているデバイスの中から、以下に示す優先順位に従って自動的に選択されます。

   - コピー元デバイスとブロックサイズが同じデバイスは、ブロックサイズが異なるデバイスよりも優先的に、コピー先デバイスとして選択される
   - ネットワーク接続デバイスより、ローカル接続デバイスが先に選択される
6. コピー先メディアを担当するMedia Agentが、コピー元メディアを担当するMedia Agentからの接続を受け入れ、コピー先メディアへのオブジェクトコピーの書き込みを開始します。

   コピー元デバイスのブロックサイズがコピー先デバイスのブロックサイズよりも小さい場合は、オブジェクトコピーセッションのこの段階でブロックの再パッケージ化が行われます。
7. 正常にコピーされたすべてのオブジェクトに対して、CSMは、コピーセッションに指定されたオプションに従ってIDB保護エントリを更新します。

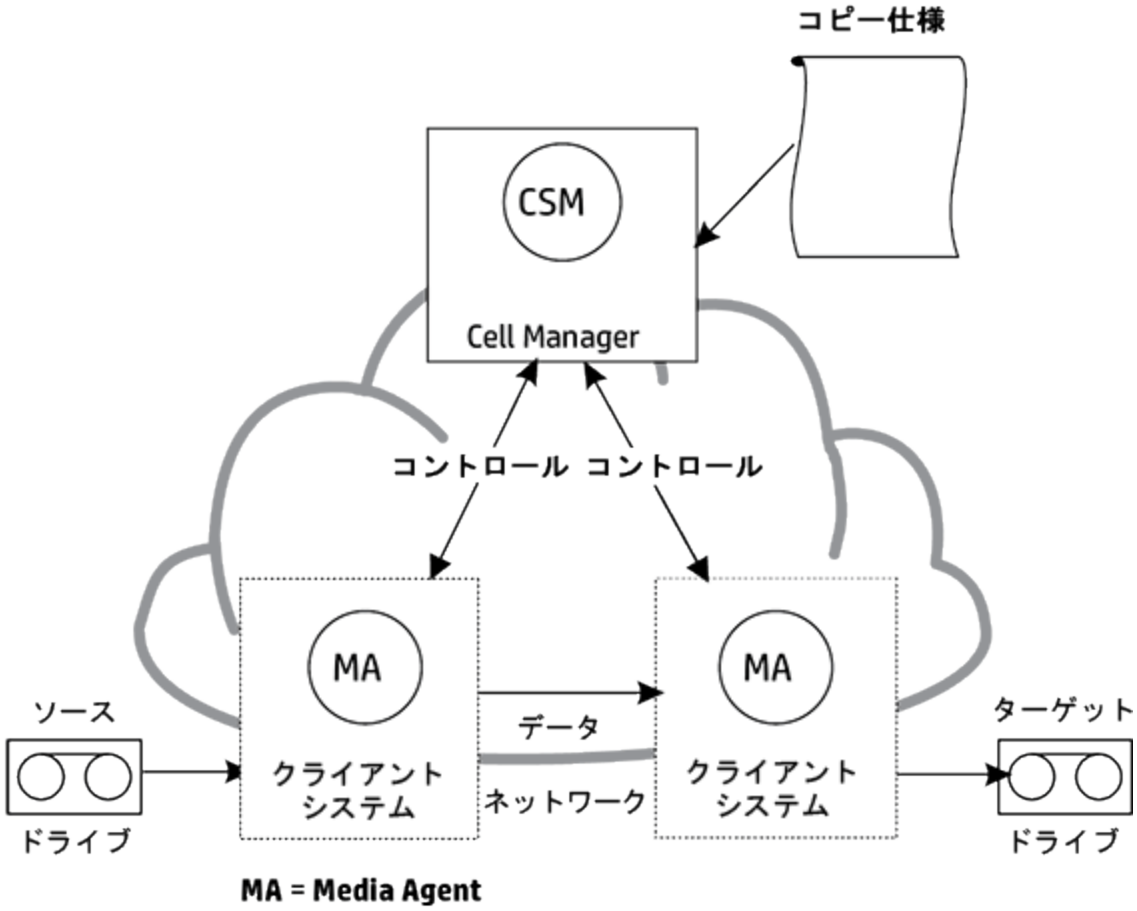
   セッションにリサイクルオプションが指定されている場合、リサイクルを可能にするために失敗したソースオブジェクトの保護も更新されます。
8. オブジェクトコピーセッションが終了したら、CSMによりセッションが閉じられます。

同時に実行できるセッションの数

セル内では同時に複数のオブジェクトコピーセッションを実行できます。同時に実行できるセッションの数は、Cell Managerや、デバイスを接続しているシステムなど、セル内のリソースによって制限されます。

ただし、同じオブジェクトコピー仕様から2つ以上のオブジェクトコピーセッションを並行して実行することはできません。

オブジェクトコピーセッションにおける情報の流れ



オブジェクトコピーセッションにおける待ち行列

タイムアウト

オブジェクトコピーセッションが開始されると、Data Protectorは、必要な全リソースの割り当てを試みます。いずれかのリソースが使用できるようになるまで、セッションは待ち行列に入れられます。タイムアウトになってもリソースがまだ使用できない場合は、そのセッションは中止されます。

オブジェクトコピーセッションにおけるマウント要求

オブジェクトコピーセッションのマウント要求は、オブジェクトコピー処理に必要なソースまたはターゲットのメディアが使用可能でない場合に行われます。

マウント要求への対応

マウント要求に対しては、必要なメディアをセットして、マウント要求を確認し、応答します。要求されたソースメディアにコピーメディアがある場合は、オリジナルメディアの代わりにコピーをセットすることも可能です。

複製セッション

この項では、複製セッションの開始方法、複製セッションの処理内容、および関連するプロセスとサービスについて説明します。

複製セッションとは、複製に対応したディスクへのバックアップ(B2D)デバイス上に、バックアップデータ、コピーデータ、集約データの追加コピーを作成するプロセスです。複製セッションでは、バックアップオブジェクト、コピーオブジェクト、集約オブジェクトをソースデバイスで選択するとターゲットデバイスに直接複製され、Media Agentクライアントを経由した転送は行われません。さらに、データは重複排除後にネットワーク転送されるので、ネットワーク負荷も軽減されます。

> **注:**
> **再接続**機能は、デフォルトで使用可能になっています。詳細については、コピーセッションマネージャー(CSM)の再接続機能、ページ 183を参照してください。

自動複製セッションと対話式複製セッション

自動複製セッション

自動複製セッションは、スケジュールを設定して開始することも、バックアップ、オブジェクトコピー、またはオブジェクト集約の直後に開始することも可能です。スケジュールした複製セッションは、Data Protectorスケジューラーを使って、指定した時刻に開始されます。一方、ポストバックアップ、ポストコピー、またはポスト集約の複製セッションは、指定したセッションの終了後に開始されます。自動複製セッションの進捗は、Data Protectorモニターで確認できます。

対話式複製セッション

対話式複製セッションは、Data Protectorユーザーインターフェイスから直接開始します。Data Protectorモニターがすぐに起動され、セッションの進行状況を監視できます。1つの複製セッションを複数のユーザーがモニターできます。ユーザーインターフェイスをセッションから切断して、モニターを停止することもできます。セッションは、その後、バックグラウンドで継続されます。

複製セッションにおけるデータフローとプロセス

複製セッションにおける情報の流れは、オブジェクトコピーセッションにおける情報の流れ、ページ 194に示すような形になります。複製セッションが開始されると、以下の処理が実行されます。

1. CSM(コピーおよび集約セッションマネージャー)プロセスが、Cell Managerシステム上で開始されます。このプロセスは、コピー仕様(および有効な複製オプション)を読み取り、複製の対象、使用するオプション、使用するデバイスを特定します。またこのプロセスは、複製セッションの制御も行います。
2. CSMがIDBを開き、複製に必要なデバイスの情報を読み取り、複製セッションの情報(生成されるメッセージなど)をIDBに書き込みます。
3. CSMにより、デバイスがロックされます。タイムアウトになってもリソースがまだ使用できない場合は、そのセッションは中止されます。
4. CSMは、複製対象として構成されているデバイス間で複製プロセスを開始します。
5. CSMは、正常に複製されたすべてのオブジェクトについて、複製セッションで指定されたオプションに従ってIDB保護エントリを更新します。

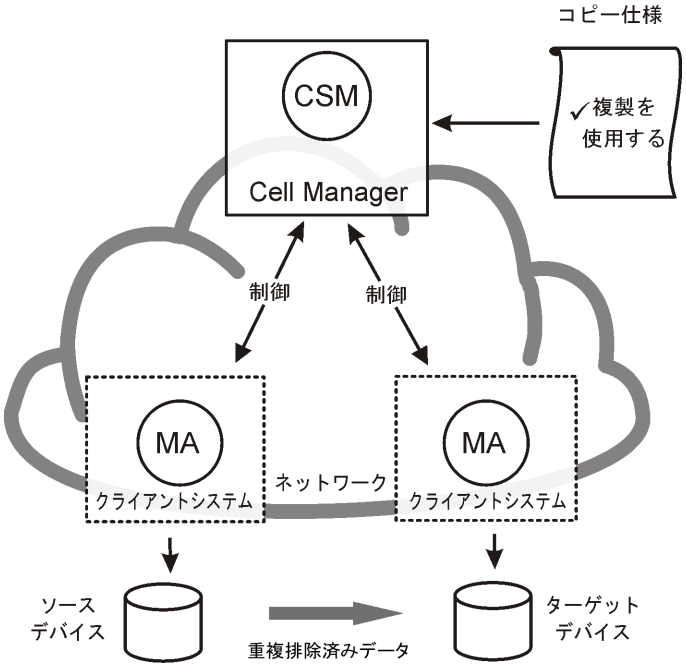
   セッションにリサイクルオプションが指定されている場合、リサイクルを可能にするために失敗したソースオブジェクトの保護も更新されます。
6. 複製セッションが終了したら、CSMによってセッションが閉じられます。

同時に実行できるセッションの数

セル内では、多数の複製セッションを同時に実行できます。同時に実行できるセッションの数は、Cell Managerや、デバイスを接続しているシステムなど、セル内のリソースによって制限されます。

ただし、同じ複製仕様から2つ以上の複製セッションを並行して実行することはできません。また、対話式複製セッションを2つ以上並行して実行することもできません。

複製セッションの情報フロー



複製セッションにおける待ち行列

タイムアウト

複製セッションが開始されると、Data Protectorは、必要な全リソースの割り当てを試みます。いずれかのリソースが使用できるようになるまで、セッションは待ち行列に入れられます。タイムアウトになってもリソースがまだ使用できない場合は、そのセッションは中止されます。

オブジェクト集約セッション

この項では、オブジェクト集約セッションの開始方法、セッション中の処理内容、および関連するプロセスとサービスについて説明します。

オブジェクト集約セッションとは、フルバックアップと少なくとも1つの増分バックアップで構成されるバックアップオブジェクトの復元チェーンを、そのオブジェクトのために新規に集約されるバージョンにマージするプロセスです。オブジェクト集約セッションでは、Data Protectorによってソースメディアのバックアップデータが読み取られ、データがマージされ、集約されたバージョンがターゲットメディアへ書き込まれます。

詳細については、合成バックアップ、ページ 66を参照してください。

> **注:**
> **再接続**機能は、デフォルトで使用可能になっています。詳細については、コピーセッションマネージャー(CSM)の再接続機能、ページ 183を参照してください。

自動および対話式のオブジェクト集約セッション

自動オブジェクト集約セッション

自動オブジェクト集約セッションは、スケジュールするか、または、バックアップ直後に開始させることができます。スケジュールしたオブジェクト集約セッションは、Data Protectorスケジューラーで指定された時間に起動されます。

ポストバックアップオブジェクト集約セッションは、指定されたバックアップセッションの終了後に起動されます。自動オブジェクト集約セッションの進行状況は、Data Protectorモニターで参照できます。

対話式オブジェクト集約セッション

対話式オブジェクト集約セッションは、Data Protectorユーザーインターフェイスから直接起動されます。Data Protectorモニターがすぐに起動され、セッションの進行状況を監視できます。複数のユーザーが、同じオブジェクト集約セッションをモニターできます。ユーザーインターフェイスをセッションから切断して、モニターを停止することもできます。セッションは、その後、バックグラウンドで継続されます。

オブジェクト集約セッションにおけるデータフローとプロセス

オブジェクト集約セッションが開始されると、以下の処理が実行されます。

1. CSM(コピーおよび集約セッションマネージャー)プロセスが、Cell Managerシステム上で開始されます。このプロセスにより、集約するオブジェクトや使用するオプション、メディア、およびデバイスに関するオブジェクト集約仕様が読み取られます。これにより、オブジェクト集約セッションが制御されます。
2. CSMによりIDBがオープンされて、復元に必要なメディアに関する情報が読み取られるほか、オブジェクト集約セッションに関する情報(生成されるメッセージなど)がIDBに書き込まれます。
3. CSMにより、デバイスがロックされます。セッションは、すべての読み取りMedia Agentと必要な最小限の書き込みMedia Agentがロックされるまで、バックアップと同じタイムアウトの時間を使用して待ち行列に入れられます。タイムアウトになってもリソースがまだ使用できない場合は、そのセッションは中止されます。
4. CSMにより、セッションで使用されるデバイスがあるシステム上のMedia Agentが起動されます。Media Agentは、バックアップポリシーに従って割り当てられたソースメディアとターゲットメディアをロードします。

   あて先デバイスがオブジェクトに対して指定されていない場合は、ユーザーが以下に記載順の優先順位に従ってオブジェクト集約仕様で選択した中から、Data Protectorによって自動的に選択されます。

   - ソースデバイスと同じブロックサイズを持つあて先デバイスが、異なるブロックサイズのものより先に選択される
   - ネットワーク接続デバイスより、ローカル接続デバイスが先に選択される

5. 1つのMedia Agentが、フルオブジェクトバージョンを読み込みます。このMedia Agentは、増分オブジェクトバージョンを読み込む別のMedia Agentにデータを送信します。この2つ目のMedia Agentが実際の集約を行い、ターゲットメディアにデータを書き込むMedia Agentにデータを送信します。

フルバックアップと増分バックアップが同じファイルライブラリまたはB2Dデバイス(Smart Cacheを除く)にある場合、同じMedia Agentがすべてのバックアップを読み込んでこれらを集約します。

ソースデバイスのブロックサイズが、あて先デバイスのブロックサイズよりも小さい場合は、ブロックが再パッケージされます。

6. オブジェクト集約セッションが終了したら、CSMによりセッションが閉じられます。

同時に実行できるセッションの数

セル内では同時に複数のオブジェクト集約セッションを実行できます。オブジェクト集約セッションは、バックアップセッションと同じように扱われ、最大数も同じ要因で制限されます。

オブジェクト集約セッションにおける待ち行列

タイムアウト

オブジェクト集約セッションが開始されると、Data Protectorは、必要な全リソースの割り当てを試みます。いずれかのリソースが使用できるようになるまで、セッションは待ち行列に入れられます。タイムアウトになってもリソースがまだ使用できない場合は、そのセッションは中止されます。

オブジェクト集約セッションにおけるマウント要求

オブジェクト集約セッションのマウント要求は、オブジェクト集約処理に必要なソースまたはターゲットのメディアが使用可能でない場合に行われます。

マウント要求への対応

マウント要求に対しては、必要なメディアをセットして、マウント要求を確認し、応答します。要求されたソースメディアにコピーメディアがある場合は、オリジナルメディアの代わりにコピーをセットすることも可能です。

オブジェクト検証セッション

この項では、オブジェクト検証セッションの開始方法、セッション中の処理内容、および関連するプロセスとサービスについて説明します。

オブジェクト検証セッションは、指定したオブジェクトに割り当てられたメディアセグメントを検証するプロセスで、ヘッダーセグメント内の情報を確認し、フォーマットを検証するためにデータセグメント内のデータブロックを読み取ります。オリジナルのバックアップ中に巡回冗長検査(CRC)が実行された場合、CRCの再計算およびオリジナルとの比較も行われます。

Data Protectorは、バックアップのソースであったホスト上でオブジェクトの検証を実行し、復元パス内のData Protectorコンポーネントの効率的な検証、別のホスト上にある別の保存場所への復元能力の検証、または関係するMedia Agentのあるホスト上で直接、データのみの検証を行うことができます。

自動および対話型オブジェクト検証セッション

自動オブジェクト検証セッション

自動オブジェクト検証セッションは、Data Protectorスケジューラーを使用して指定した時間に実行するか、あるいは指定したバックアップ、オブジェクトコピー、またはオブジェクト集約セッションの完了直後にバックアップ後のオブジェクト検証セッションとして実行するよう指定できます。Data Protectorモニターでこのようなセッションの進行状況をモニタリングできます。

対話型オブジェクト検証セッション

対話型オブジェクト検証セッションは、Data Protectorのユーザーインターフェイスから直接開始できます。Data Protectorモニターがすぐに起動され、セッションの進行状況を監視できます。複数のユーザーが同一のオブジェクト検証セッションをモニタリングすることも可能です。ユーザーインターフェイスを使って他の操作を実行し、必要に応じてセッションをバックグラウンドで続行させることができます。

オブジェクト検証セッションにおけるデータフローとプロセス

オブジェクト検証セッションを開始する場合、基本のプロセスフローは以下のようになります。

1. Restore Session Manager (RSM)プロセスは、Cell Managerシステム上で開始され、以下のいずれかによってトリガーされます。
   - スケジュール設定されたセッションの場合、Data Protectorのスケジューラー
   - バックアップ後のセッションの場合、End of Sessionイベント
   - 対話形式のセッションの場合、GUIまたはCLIからのユーザー

   このプロセスにより、検証セッションが制御されます。
2. RSMによりIDBがオープンされて、検証するオブジェクトに関する情報が読み取られるほか、検証セッションに関する情報(生成されるメッセージなど)がIDBに書き込まれます。
3. RSMにより、オブジェクトの検証に関係するソースシステム上でMedia Agent (MA)が起動されます。並行して使用される各ドライブで、新たにMedia Agentが起動されます。
4. あて先ホスト上のDisk Agents (DA)によりデータ検証が実行され、これにより並行して使用される各あて先ディスクに対してRSMによりDisk Agentが起動されます。起動されるDisk Agentの実際の数は、検証を選択したオブジェクトに依存します。このプロセスは、復元の場合と同様です。詳細については、並行復元、ページ 191を参照してください。
5. Media Agentはメディアからオブジェクトデータを読み取り、オブジェクトの検証を実行するDisk Agentに送信します。RSMにより、セッションの進行状況がモニターされ、必要に応じて新規のDisk AgentやMedia Agentが起動されます。
6. オブジェクト検証セッションが完了すると、RSMによりセッションがクローズされます。

オブジェクト検証を使用するプロセスフローのバリエーション

オブジェクト検証プロセスでは、復元のためにデータが要求されたポイントから、データがあて先ホストに到達したポイントまでの復元処理がエミュレートされます。そのポイントを超えると、検証プロセスによるデータの書き込みは行われず、アプリケーション統合オブジェクトの場合、アプリケーション統合とのやり取りは行われません。

メディア管理セッション

メディア管理セッションは、メディアの初期化、内容のスキャン、メディア上のデータの検証、メディアのコピーなど、メディアに対する特定の操作を行う場合に実行されます。

IDBへのログの記録

生成されたメッセージなど、メディア管理セッションに関する情報が、IDB内に保存されます。

Data Protectorモニターとメディア管理セッション

メディア管理セッションは、モニターウィンドウを使ってモニタリングできます。Data Protector GUIを閉じると、セッションはバックグラウンドで実行されます。

メディア管理セッションにおけるデータフロー

メディア管理セッションが開始されると、以下の処理が実行されます。

1. メディアセッションマネージャー(MSM)プロセスは、Cell Managerシステム上で開始されます。このプロセスにより、メディアセッションが制御されます。
2. MSMにより、メディア管理セッションで使用するデバイスが接続されているシステム上で、Media Agent(MA)が開始されます。
3. 要求した処理がMedia Agentにより実行され、生成されたメッセージが、進捗状況のモニタリングに使用するData Protectorユーザーインターフェイスに送られます。このとき、セッションもIDB内に保存されます。
4. セッションが終了したら、MSMによりセッションが閉じられます。

実行できるセッションの数

セル内では同時に複数のメディア管理セッションを実行できます。ただし、これらのセッションが同一のリソース(デバイスやメディアなど)を使用しない場合に限ります。

第8章： アプリケーションとの統 合

この章 では、Data Protectorとデータベースアプリケーションとの統 合 について簡 単 に説 明します。

データベースアプリケーションとの統 合

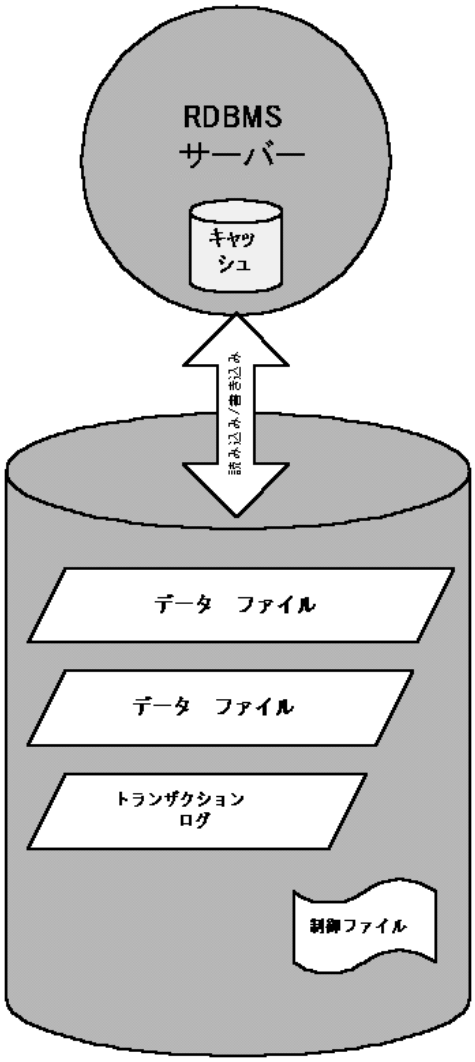
この項 では、Data Protectorとデータベースアプリケーションとの統 合 について簡 単 に説 明します。サポートされるアプリケーションの詳 細 なリストは、最 新 のサポート一 覧 (https://softwaresupport.hpe.com/)を参 照 してください。

データベース操 作 の概 要

ユーザーから見 ると、**データベース**は、情 報 を1つに集 めたものです。データベース内 のデータは、**テーブル**内 に保 存 されています。リレーショナルテーブルは複 数 の列 で構 成 され、各 テーブルにはそれぞれ名 前 がつけられています。データはテーブル内 の各 行 に保 存 されます。テーブルは相 互 に関 連 付 けることができ、データベースという形 で実 際 の関 連 付 けが行 われます。データはこのように**リレーショナル形 式** で保 存 することも、抽 象 データ型 やメソッド のような**オブジェクト指 向** の構 造 として保 存 することもできます。また、オブジェクトを他 のオブジェクトと関 連 付 けたり、オブジェクト内 に他 のオブジェクトを包 含 することも可 能 です。データベースは通 常 サーバー(マネージャー)プロセスにより管 理 されて、データの整 合 性 と一 貫 性 が保 たれます。

リレーショナル形 式 の構 造 またはオブジェクト指 向 の構 造 のいずれを使 用 する場 合 も、データベース内 のデータは**ファイル**に保 存 されます。内 部 的 には、これらのデータベース構 造 によりデータからファイルへの論 理 マッピングが提 供 され、データ型 の異 なるデータは個 別 に保 存 できます。これらの論 理 領 域 は、Oracleでは**表 領 域** 、Informix Serverでは**dbspace**、Sybaseでは**セグメント**など、さまざまな名 前 で呼 ばれています。

リレーショナルデータベース



リレーショナルデータベース、上は、典型的なリレーショナルデータベースと、その内部にある以下の構造を示したものです。

データファイルは、データベース内のすべてのデータが保存される物理ファイルです。データファイルはランダムに変更され、非常に大容量になる可能性があります。物理ファイルの内部は、複数のページに分割されています。

トランザクションログには、すべてのデータベーストランザクションが処理を続行する前に、最初にそれらのトランザクションが保存されます。なんらかの障害により変更データをデータファイルに永久に書き込めなくなった場合も、このログファイルから変更情報を取得できます。復旧処理を行う場合は、必ず次の2つの作業が必要になります。1つ目はトランザクションをメインデータベースに適用する作業で、**ロールフォワード**と呼ばれます。2つ目はコミットされていないトランザクションを削除する作業で、**ロールバック**と呼ばれます。

制御ファイルには、データベースの物理構造、たとえば、データベースの名前、データベースに所属するデータファイルやログファイルの名前と場所、データベース作成時のタイムスタンプなどが保存されています。この制御データは、制御ファイルに保存されます。これらのファイルは、データベースの操作に非常に重要です。

データベースサーバープロセスの**キャッシュ**内には、データファイルの中の使用頻度の高いページが保存されます。

以下に、標準的なトランザクション処理手順を示します。

1. 最初に、トランザクションがトランザクションログに記録されます。
2. 次に、トランザクションにより要求された変更内容が、キャッシュ内のページに適用されます。
3. 変更されたページは、ディスク上のデータファイルに随時一括して書き込まれます。

データベースおよびアプリケーションのファイルシステムバックアップ

オンライン状態のデータベースは絶えず変更されています。またデータベースサーバーは、接続ユーザーへの迅速な応答や性能の向上を図るために、複数のコンポーネントで構成されています。たとえばデータの中には、内部キャッシュメモリや一時的なログファイルに保存されているものもあります。これらのデータは、**チェックポイント**でディスクに一括して書き込まれます。

データベース内のデータはバックアップ中にも変更される可能性があるため、データベースファイルの有効なファイルシステムバックアップを作成するには、データベースサーバーを特殊モードまたはオフライン状態にしなければなりません。データに整合性がなければ、データベースファイルをバックアップしても意味がありません。

次に、データベースまたはアプリケーションのファイルシステムバックアップを構成する手順を示します。

- 対象となるすべてのデータファイルを確認します。
- データベースを停止および開始するための2つのコマンドを選択するか、2つのスクリプトやアプリケーションをそれぞれ用意します。
- すべての仮想マシンファイルが含まれるファイルシステム**バックアップ仕様**を構成するには、シャットダウンコマンド、スクリプト、またはアプリケーションを**実行前コマンド**として指定し、開始コマンド、スクリプト、またはアプリケーションを**実行後コマンド**として指定する必要があります。

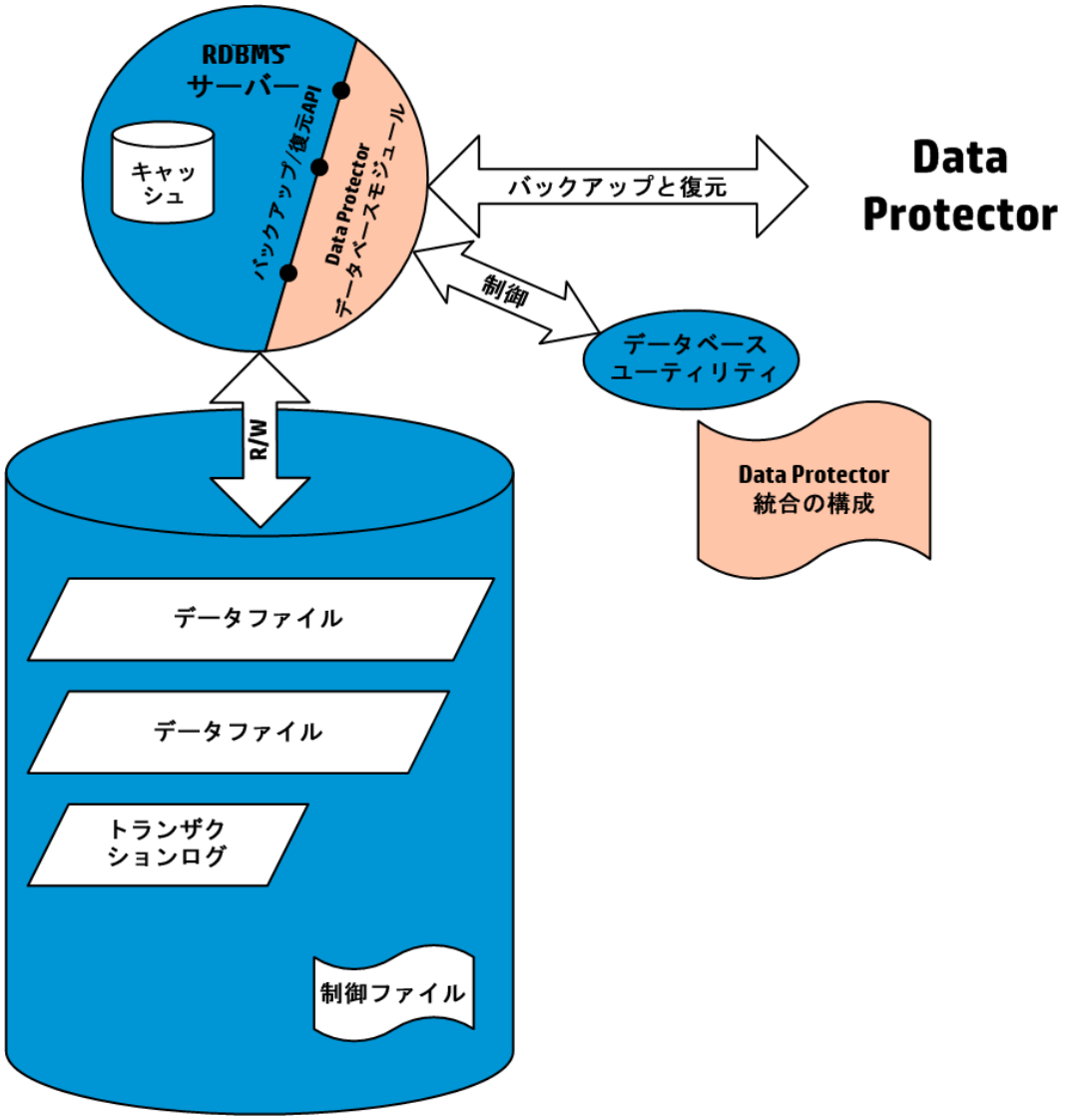
これは、比較的簡単で明瞭な構成方法ですが、バックアップ中にデータベースにアクセスできないという、大きな欠点があります。これは、ほとんどのビジネス環境で、受け入れられることではありません。

データベースおよびアプリケーションのオンラインバックアップ

バックアップ中にもデータベースを停止せずに済むように、各データベースベンダーでは、データベースを一時的に特殊モードにしてデータをテープに保存できるようにするためのインターフェイスを用意しています。これらのインターフェイスを使用すると、バックアップ中または復元中もサーバーアプリケーションをオンライン状態のままにでき、ユーザーの利用が引き続き可能になります。Data Protectorを始めとするバックアップ製品では、これらのアプリケーション固有のインターフェイスを使って、データベースアプリケーションの論理ユニットのバックアップや復元を実行できます。バックアップAPIの機能はデータベースベンダーによって異なります。Data Protectorの統合機能は、主要なデータベースおよびアプリケーションで利用可能です。サポートされる構成の一覧については、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。

バックアップインターフェイスの主 要 目 的 は、データベースを停 止 することなく、(たとえディスク上 のデータが整 合 性 のない状 態 であっても)バックアップアプリケーションに整 合 性 のあるデータを提 供 することにあります。

Data Protectorとデータベースの統 合



Data Protectorとデータベースの統 合 、上 は、リレーショナルデータベースとData Protectorの統 合 方 法 を示したものです。Data Protectorでは、データベースサーバーにリンクされる**データベースライブラリ**が提 供 されます。データベースサーバーは、Data Protectorに対してデータを送 信 したり、データを要 求 したりします。データベースユーティリティは、バックアップ処 理 や復 元 処 理 の開 始 に使 用 されます。

以 下 に、Data Protectorの統 合 機 能 を使 用 してデータベースをバックアップするための典 型 的 な構 成 手 順 を示します。

1. データベース/アプリケーション固 有 のエージェントを、データベースシステムにインストールします。
2. データベースごとに、Data Protectorの統 合 ソフトウェアを構 成 します。Data Protectorでデータベースを処 理 するために必 要 なデータは、データベースシステムの構 成 ファイルまたはレジストリエントリに保

存されます。通常、この情報には、パス名や、ユーザーの名前とパスワードが含まれます。

3. Data Protectorのユーザーインターフェイスを使用して、バックアップ仕様を準備します。

データベースとの統合ソフトウェアを使用すると、データベースが常にData Protector**オンライン**状態に保たれるという重要な利点に加えて、以下の利点もあります。

- データファイルの場所を指定する必要はありません。これらは、異なるディスク上に置くことができます。
- データベースの論理構造をブラウズできます。データベース中のあるサブセットのみを選択することも可能です。
- アプリケーション側でバックアップ操作を感知して、どの部分がバックアップされたかを追跡できます。
- 複数モードによるバックアップが可能です。**フル**バックアップのほかにも、(ブロックレベルの)**増分**バックアップやトランザクションログのみのバックアップも選択できます。
- 複数のモードによる復元が可能です。またデータファイルの復元後に、データベースにより自動的にトランザクションログを復元し、構成内容に従ってそれらのトランザクションをデータベースに適用することもできます。

仮想環境との統合

この項では、Data Protectorと仮想環境との統合について簡単に説明します。サポートされる環境の詳細なリストは、最新のサポート一覧(https://softwaresupport.hpe.com/)を参照してください。

詳細については、『*HPE Data Protectorインテグレーションガイド*』を参照してください。

仮想マシンのオンラインバックアップ

Data Protectorでは、仮想環境に用意されている特定のインターフェイスを使用して、仮想マシンの稼動中に仮想マシンのバックアップを実行します(オンラインバックアップ)。仮想環境によっては、仮想マシン内のアプリケーションを整合性のある状態に移してからバックアップを開始できます。

データベースとのData Protector統合ソフトウェアを使用すると、仮想マシンが常にオンライン状態に保たれるという重要な利点に加えて、以下の利点もあります。

- データファイルの場所を指定する必要はありません。
- 仮想環境側でバックアップ操作を認識し、どの部分がバックアップされたかを追跡できます。
- 複数モードによるバックアップが可能です。
- 複数モードによる復元が可能です。

VMware ESXiを使用したOpenStackクラウドインフラストラクチャーでのVMのバックアップおよび復元

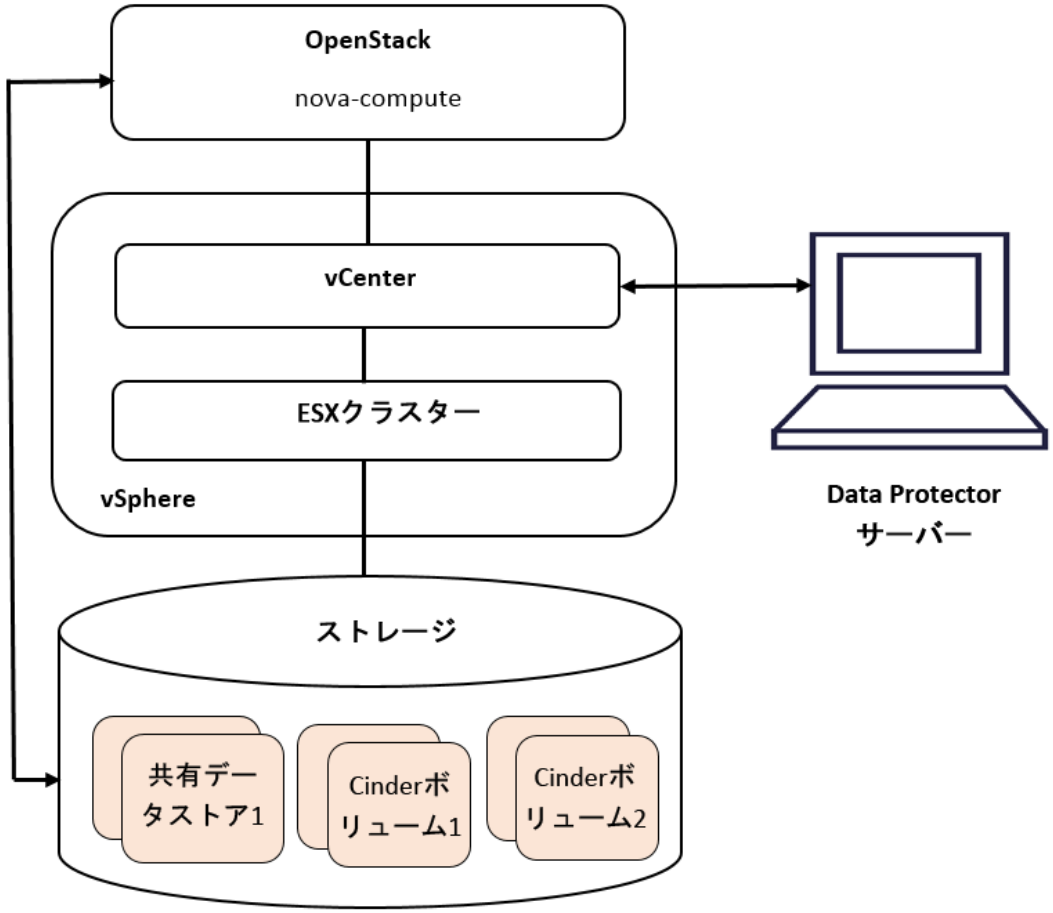
OpenStackは、あらゆるタイプのクラウド向けのオープンソースのクラウドコンピューティングプラットフォームです。ハイパーバイザーとしてvSphereまたはESXiを使用しているOpenStack環境では、Novaインスタンスとして知られるVMを使用して、計算が割り当てられます。Novaインスタンス用のディスクは、Cinderストレージボリューム(シャドウVMと呼ばれる)から作成されます。VMwareでは、VMがプライマリオブジェクトと見なされますが、クラウドOpenStackでは、ディスクがプライマリオブジェクトと見なされます。これらのCinderディスクは、vCenterのコンテキストではシャドウVMとして扱われます。これらのシャドウVMは、ブートできず、

vCenterでは“volume-id”という別 のVMとしてリストされます。シャド ウVMまたはCinderボリュームは、OpenStackダッシュボードによって管 理されます。

OpenStackの詳 細については、以 下を参 照してください。

http://docs.openstack.org/admin-guide/common/get_started_with_openstack.html

OpenStack、VMware vCenter、およびData Protectorとの統 合



vStorage APIメソッドを使 用して、Data ProtectorはNovaインスタンスのバックアップおよび復 元を実 行します。シャド ウVMを選 択することはできませんが、Novaインスタンスに関 連付 けられているシャド ウVMがバックアップおよび復 元されます。

Microsoftボリュームシャド ウコピーサービス

概 要

従 来のバックアップ処 理は、バックアップアプリケーション(バックアップを開 始および実 行するアプリケーション)とバックアップ対 象アプリケーションが直 接交 信しながら実 行されます。このバックアップ方 式では、バックアップアプリケーションがバックアップ対 象のアプリケーションのそれぞれに対 応した個 別のインターフェイスを使

用する必要があります。アプリケーション固有の実装の数を減らす効果的な方法の1つが、バックアップおよび復元プロセスに関連する要素間を調整する機能を導入する方法です。

VSS

ボリュームシャドウコピーサービス (VSS)は、Microsoft社によりMicrosoft Windowsオペレーティングシステム上に採用されたソフトウェアサービスです。このサービスは、バックアップアプリケーション、バックアップ対象アプリケーション、シャドウコピープロバイダー、およびオペレーティングシステムと連携して、ボリュームシャドウコピーおよびシャドウコピーセットの管理を実現します。

VSSは、任意のアプリケーションのバックアップと復元を、そのアプリケーションの機能に関係なく取りまとめる、統一通信インターフェイスを提供します。バックアップアプリケーションは、VSS仕様に準拠しているアプリケーションであれば、バックアップ対象のアプリケーションを個々に処理する必要はありません。

シャドウコピー

シャドウコピーとは、オリジナルボリュームの特定時点における複製であるボリュームを指します。データのバックアップには、オリジナルボリュームではなくこのシャドウコピーが使われます。オリジナルボリュームはバックアップ処理中も更新が可能ですが、ボリュームのシャドウコピーは同じ内容に維持されます。

シャドウコピーは基本的にはスナップショットバックアップであり、バックアップの最中もアプリケーションやユーザーはボリュームにデータを書き込むことができます。バックアップ処理には、元のボリュームのシャドウコピー内のデータが使用されます。

シャドウコピーセットとは、同じタイミングで作成されたシャドウコピーの集合を指します。

ライター

ライター**とは、元のボリューム上のデータに対する変更を開始するあらゆるプロセスを指します。**通常、ライターとなるのは、ボリューム上に永続的な情報を書き込むアプリケーション(たとえばMicrosoft SQL Server用のMSDEライターなど)またはシステムサービス(システムライターやレジストリライターなど)です。ライターはシャドウコピーの同期プロセスにおいて、データの整合性を保証する働きをします。

シャドウコピープロバイダー

シャドウコピープロバイダーとは、ボリュームシャドウコピーの作成および提供に関わる処理を実行するなんらかの実体を指します。シャドウコピープロバイダーはシャドウコピーデータの所有者であり、シャドウコピーを公開する働きをします。シャドウコピープロバイダーはソフトウェア(システムプロバイダーやMS Software Shadow Copy Providerなど)の場合もあれば、ハードウェア(ローカルディスクやディスクアレイ)の場合もあります。

ハードウェアプロバイダーの例としてはディスクアレイが挙げられます。ディスクアレイには特定時点におけるディスク状態を提供するための独自のハードウェア機構が備わっています。ソフトウェアプロバイダーは物理ディスクを操作し、ソフトウェア機構を使用して特定時点におけるディスク状態を提供します。システムプロバイダーであるMS Software Shadow Copy Providerはソフトウェア機構であり、Windows Server 2003以降のWindowsオペレーティングシステムに組み込まれています。

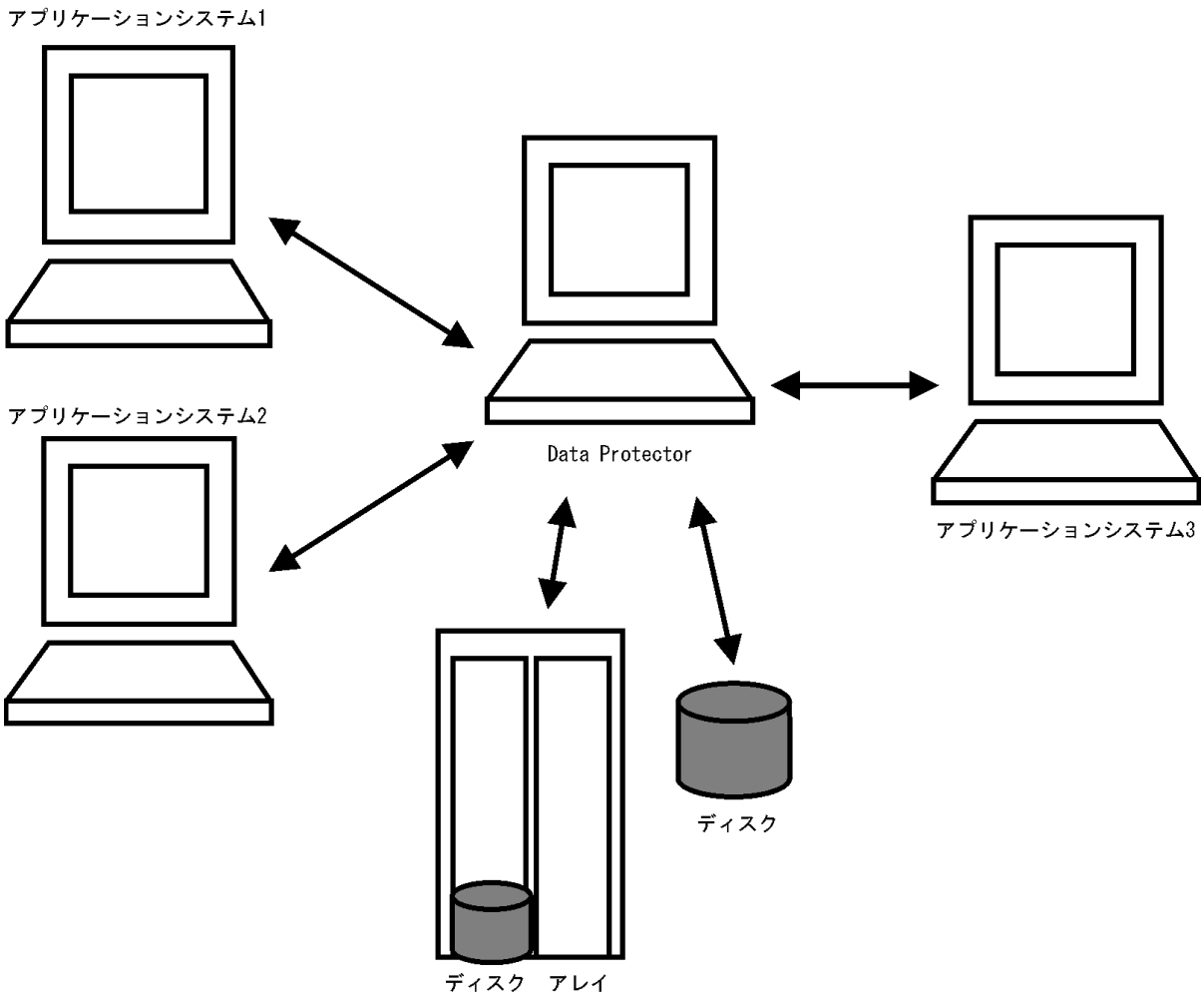
VSSではシャドウコピーの作成時に、まずすべてのハードウェアプロバイダーが優先して使用され、その後はじめてソフトウェアプロバイダーが使用されるようにします。いずれのプロバイダーでもシャドウコピーを作成できなければ、VSSはシャドウコピーの作成に(常に使用可能な)MS Software Shadow Copy Providerを使用します。

Data ProtectorとVSS

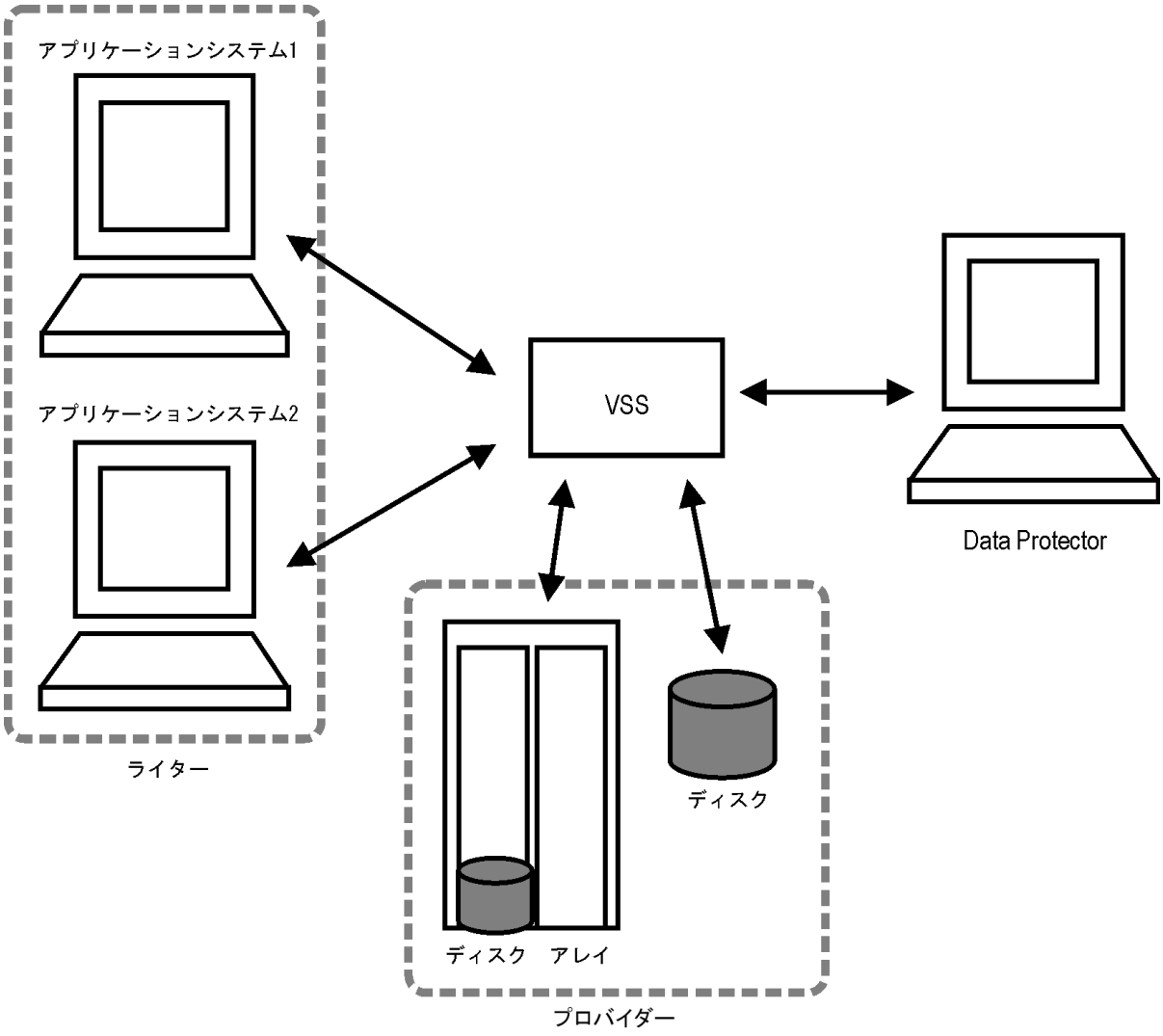
ボリュームシャドウコピーサービスはバックアップおよび復元時の、バックアップアプリケーション、ライター、およびシャドウコピープロバイダー間の調整を可能にします。

従来のバックアップモデルに関係する要素、下とVSSバックアップモデルに関係する要素、次のページは、従来のバックアップモデルとVSSコーディネーターを使用したモデルの違いを示しています。

従来のバックアップモデルに関係する要素



VSSバックアップモデルに関係する要素



VSSの利点

ボリュームシャドウコピーサービスを使用する利点は以下のとおりです。

- すべてのライターに対して共通のバックアップインターフェイス。
- すべてのシャドウコピープロバイダーに対して共通のバックアップインターフェイス。
- ライターがアプリケーションレベルでデータの整合性を提供できる。バックアップアプリケーションからの介入が不要。

Data Protectorは、Microsoftボリュームシャドウコピーサービスを次の2つのレベルでサポートしています。

- MicrosoftボリュームシャドウコピーサービスとDataProtectorでZDBおよびインスタントリカバリ機能を含むVSS対応ライターのシャドウコピーバックアップおよび復元が可能になります。
- Disk Agent機能を使ったVSSファイルシステムバックアップが可能でData Protectorす。

Data ProtectorのVSS統合機能では、VSS対応のライターについてのみ、整合性のあるシャドウコピーバックアップが保証されます。この場合の整合性はライター側で提供されます。アプリケーションがVSSに対応していない場合、シャドウコピーデータの整合性はアプリケーションレベルでは保証されませんが、非VSSのファイルシステムのバックアップに比べて向上しています。

次の表はData ProtectorのVSS統合バックアップ、VSSファイルシステムバックアップ、および非VSSファイルシステムバックアップの違いを簡単にまとめたものです。

VSSを使用する利点

	Data Protector VSS統合バックアップ	**VSSファイルシステムバックアップ**	**非VSSファイルシステムバックアップ**
開いているファイル	開いているファイルはありません。	開いているファイルはありません。	ファイルが開いていると、バックアップが失敗する可能性があります。
ロックされているファイル	ロックされているファイルはありません。	ロックされているファイルはありません。	ロックされているファイルは、バックアップ時にスキップされます。
データの整合性	ライターにより提供されます。	整合性の破綻(電源障害の場合など)。	なし(本質的に)

Data Protectorとボリュームシャドウコピーの統合

Data ProtectorとMicrosoftボリュームシャドウコピーサービスを統合すると、VSS対応ライターを完全にサポートできるようになります。このサポートには、VSS対応ライターの自動検出やバックアップ/復元機能が含まれます。統合ソフトウェアの主な目的は、アプリケーションデータのバックアップです。

統合の詳細については、『*HPE Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*』を参照してください。

VSSファイルシステムとディスクイメージのバックアップと復元

アプリケーションの中にはボリュームシャドウコピーサービスに対応していないものもあります。このようなアプリケーションの場合は、シャドウコピーの作成時にデータの整合性が保証されません。VSSではこれらのアプリケーションのアクティビティを調整して、整合性のあるバックアップを実行することはできません。ただし、ファイルシステムバックアップよりも優れたデータ整合性を実現できます。Microsoftではこのようなデータ整合性状態を「クラッシュ時整合状態」と呼んでいます。シャドウコピーボリュームの準備中には、VSSにより、保留中のすべてのI/O操作がコミットされ、新たな書き込み要求は保留されます。このようにしてシャドウコピーの作成中はファイルシステム上のすべてのファイルが閉じられ、ロックは解除されます。

Microsoftボリュームシャドウコピーを使用すると、バックアップ対象アプリケーションの関与なしにボリュームシャドウコピーを作成できます。この場合シャドウコピーボリュームの作成とバックアップは、Data Protectorにより実行されます。このやり方は、VSSに対応していないアプリケーションに使用できます。

> **重要:**
> VSSに対応していないアプリケーションをバックアップする場合は、アプリケーション側から見たデータ整合性は保証されません。データの整合性は、電源障害の場合と同じです。Data Protectorでは、アプリケーションがシャドウコピーの作成に積極的に関与していない場合は、データの整合性を保証できません。

VSSファイルシステムとディスクイメージバックアップのデータの整合性は、非VSSファイルシステムのバックアップよりも向上しています。VSSでは、ボリュームのシャドウコピーバックアップを作成できます。シャドウコピーバックアップは、特定の時点でのファイルの正確なコピーです。開いているファイルもすべて含まれます。たとえばVSSファイルシステムまたはディスクイメージバックアップでは、排他的に開かれているデータベースや、オペレーターやシステムアクティビティにより開かれているファイルもバックアップの対象になります。このようにして、バックアップ中に変更が加えられたファイルも適正にコピーされます。

VSSファイルシステムおよびディスクイメージバックアップの利点は以下のとおりです。

- アプリケーションやサービスを実行したままでコンピューターをバックアップできます。バックアップの実行中もアプリケーションはボリュームへのデータ書き込みを継続できます。
- 開いているファイルもバックアップ中にスキップされません。これはシャドウコピーの作成時に、これらのファイルがシャドウコピーボリューム上では閉じた状態になるためです。
- ユーザーを締め出すことなくバックアップをいつでも実行できます。
- バックアッププロセス中でも、アプリケーションシステムのパフォーマンスにはほとんど影響はありません。

バックアップと復元

VSSファイルシステムおよびVSSディスクイメージバックアップは、Windows Server 2003以降のオペレーティングシステムで、追加のバックアップオプションとして実装されています。VSSファイルシステムバックアップを有効にするには、WinFSのオプションとして指定してください。ディスクイメージバックアップの実行中、VSSライターがデフォルトで使用されます。データ整合性のレベルは、従来の方法によるアクティブボリュームのバックアップに比べて多少向上しています。Windowsファイルシステムとディスクイメージのバックアップと復元の詳細については、『*HPE Data Protectorヘルプ*』を参照してください。

VSSファイルシステムおよびVSSディスクイメージバックアップでは、アプリケーションがVSSに対応していないため、データ整合性の向上にアプリケーションが関与することは事実上できません。ただしこの場合も、Data Protectorとプロバイダーは連携してボリュームシャドウコピーの作成にあたります。VSSバックアップを使用すると、バックアップ中のシステムI/O動作の有無に関わりなく、特定時点におけるデータ状態をバックアップすることが可能になります。

バックアップ仕様に指定されたボリュームのバックアップをData Protectorが要求すると、VSSにより、保留中のすべてのI/O操作がコミットされ、新たな書き込み要求は保留されて、シャドウコピーボリュームの準備が行われます。

シャドウコピーの作成が終了したら、Data Protectorによる通常のバックアップ手順が開始されます。ただし、バックアップ中はソースボリュームではなく新たに作成されたシャドウコピーが使用されます。シャドウコピーの作成に失敗した場合は、Data Protectorは従来の方法によるバックアップを行います(ただし、バックアップ仕様でフォールバックが指定されている場合)。

このように、ファイルが開かれていたりサービスが実行中であっても、コンピューターのバックアップが可能です。この種のバックアップではファイルがスキップされることはありません。VSSを使用するとシャドウコピーの作成中も、実ボリューム上で実行中のサービスやアプリケーションが中断されることはありません。バックアップが終了するとシャドウコピーは削除されます。

VSSファイルシステムバックアップを使用してバックアップしたデータは、通常と同様の手順で復元できます。

Windows Vista、Windows 7、Windows 8、Windows Server 2008、Windows Server 2012の各 システムでは、EADRやOBDRに対 応している場 合 、VSSディスクイメージ バックアップ機 能 を使 用したディスクイメージとしてのボリュームのバックアップが可 能 です。アンマウントされたボリューム、NTFSフォルダーにマウント済 みのボリューム、およびCONFIGURATIONオブジェクトは、ディスクイメージとしてバックアップできません。このため、そのようなオブジェクトはファイルシステムオブジェクトとしてバックアップする必 要 があります。

> **注:**
> VSSディスクイメージ バックアップのカスタマイズには、omnircオプションを使 用します。

第9章: ゼロダウンタイムバックアップとインスタントリカバリ

この章では、ゼロダウンタイムバックアップとインスタントリカバリの基本的な概念を紹介します。データベースアプリケーションなど、大量のデータを操作するアプリケーションには、従来のデータバックアップ方法は適していません。データベースをオフラインにする必要がある場合や、アプリケーションで対応している場合には、そのデータがテープへストリーミングされている間に「ホットバックアップモード」になります。前者の場合は、アプリケーション操作の大幅な中断が発生することがあります。また、後者の場合は、大きなトランザクションログファイルが生成されることがあり、アプリケーションシステムに過剰な負荷がかかることになります。

現在のストレージ環境において、データの可用性に対する要件は常に増え続けています。情報リソースの可用性を高める場合は、Data Protectorゼロダウンタイムバックアップ(ZDB)ソリューションを使用して、アプリケーションのダウンタイムを削減し、基幹的なデータを常時利用可能にすることで、ビジネスニーズを満たすことができます。

ゼロダウンタイムバックアップとは、アプリケーションシステムに対するバックアップ操作の影響を最小限に抑えるために複製技術が使用されるバックアップアプローチのことをいいます。バックアップされるデータの複製が最初に作成され、それ以降のバックアップ操作はすべてオリジナルのデータではなく複製データに対して実行されます。

バックアップは、アプリケーションをオンラインで使用可能な状態に維持したままバックグラウンドで実行されるため、バックアップ中の環境に対する影響を最小限に抑えることができます。復旧にかかる時間も、インスタントリカバリ機能を使用することによって削減され、大量のデータの復旧を何時間もかかることなく数分で実行できます。これにより、ZDBおよびIR機能は、可用性の高いシステムと基幹的なアプリケーションに適したものになります。

Data Protector ZDBおよびIRの技術は、ディスクベースアレイのミラーおよびスナップショット技術を利用しています。ZDBおよびIRの基本原理を以下に示します。

- バックアップされるデータのコピーを高速作成した後、オリジナルのデータではなくコピーに対してバックアップ操作を実行します。
- アレイに保持されたデータのバックアップコピーをアレイのオリジナルの位置に復元して、高速復旧を促進します。

ゼロダウンタイムバックアップ(ZDB)およびインスタントリカバリ(IR)には、従来のバックアップ方法や復元方法と比べて2つの大きな利点があります。

- セッション中にアプリケーションシステムで発生するダウンタイムや影響を最小限に抑えることができる
- 復元にかかる時間を短縮できる

比較テーブル - テープのバックアップおよび復元と、ZDBおよびIR

機能	テープのバックアップおよび復元	ZDBおよびIR
データの可用性	アプリケーション操作は、バックアップセッション中、バックアップメディアへのデータのストリーミングが完了するまでオフラインにしておく必要があります。	アプリケーションダウンタイムは最小限に抑えられるため、バックアップ中の環境への影響は減ります。
バックアップ速度	テープへの書き込みには、非常に時間がかかる場合があります。	ディスクへの書き込みは、ほとんど瞬時に行われます。

復旧時間	復元には長時間かかる可能性があり、この間アプリケーションを使用することはできません。	大量のデータの復旧には何時間も何日もかかることはなく、数分で行われます。
障害の影響	データの復旧に必要なダウンタイムが原因で、障害によって多数の問題が生じる可能性があります。	障害の影響は、復元が高速で行われるために最小限に抑えられます。
データストレージの容量	通常、テープストレージの容量は限られています。	ディスクベースアレイは、何テラバイトものデータを保持することができるため、同じデータのコピーを複数作成することができます。
柔軟性	データはテープメディアにのみ格納することができます。データのコピーは一度に1つだけ作成できます。複数のコピーを作成する場合は、コピーの作成が必要になるたびにアプリケーションをオフラインにする必要があります。	ディスクアレイをプライマリデータストレージとして使用するか、またはアレイにコピーが作成されてからテープにデータをストリーミングすることができます。単一バックアップを実行してから、ソースに影響を与えることなくテープに複数回コピーできるため、データの複数コピーを作成することは簡単です。拡張バックアップソリューションとして、ディスクおよびテープの各バックアップ技術を結合することができます。

ディスクアレイとストレージの仮想化技術

RAID技術を使用する大容量ディスクアレイには、膨大な量のデータを含む大規模なアプリケーションデータベースを格納できます。ストレージの仮想化では、ディスクアレイは通常多くの仮想ディスクに分割されます。仮想ディスクはディスクアレイ内で簡単にコピーでき、ディスクアレイ技術および空きストレージ容量によっては多数回コピーできることがあります。これによりコピーしたデータに対して操作を行うことが可能になり、オリジナルデータをリスクから解放できます。特に、高可用性が求められるミッションクリティカルな分野において、アプリケーションに対する効率的なバックアップソリューションが可能になります。

ゼロダウンタイムバックアップ

テープにバックアップする従来の方法は、大規模なデータベースアプリケーションにはあまり適しません。データベースをオフラインにするか、(アプリケーションで対応している場合)テープへのデータのストリーミング中に「ホットバックアップモード」にする必要があります。

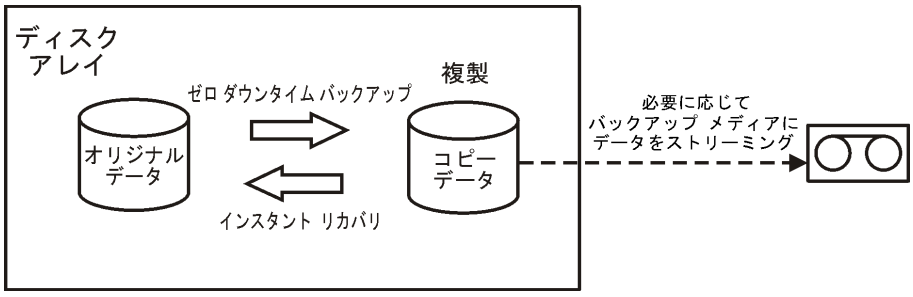
前者の場合は、アプリケーション操作の大幅な中断が発生することがあります。また、後者の場合は、大きなトランザクションログファイルが多数生成されることがあり、アプリケーションシステムに過剰な負荷がかかることになります。

ゼロダウンタイムバックアップ(ZDB)では、中断を最小限に抑制するため、ディスクアレイテクノロジが使用されます。一般的に、データのコピーまたは**複製**は、ディスクアレイ上で作成または管理されます。これは非常に高速に行われるため、アプリケーションのパフォーマンスに及ぼす影響は最小限に抑えられます。複製は、それ自体がバックアップになることが可能であるほか、アプリケーションによるソースデータベースの使用をそれ以上妨げずにテープにストリーミングすることができます。

複製は、バックアップ対象データの正確なコピー(ミラー、スナップクローン)の場合もあれば、仮想コピー(スナップショット)の場合もあります。これは、複製の作成に使用されるハードウェアおよびソフトウェアによって異なります。

ZDBでは、**複製**(この場合は、複製を作成または保持するプロセスを指す)が、アプリケーションの中断を最小化するうえで重要な要因になります。

ゼロダウンタイムバックアップとインスタントリカバリの概念



オンラインおよびオフラインでの複製の作成

データベースアプリケーションの場合、データベースがオンラインまたはオフラインのいずれの状態でもバックアップを実行できます。

- **オンラインバックアップ**

  データベースは、バックアップ対象のセクションの複製が作成される間、ホットバックアップモードになります。このモードでは、データベースに対するすべての変更が、データベースそのものではなくトランザクションログに書き込まれます。データベースの機能が完全に回復するまでは、トランザクションログから更新されます。これによって、アプリケーションを停止することなく、データベースを操作することができます。
- **オフラインバックアップ**

  データベースの操作は、複製が作成される間、停止されます。この間、トランザクションは実行できません。

複製の作成後、データベースは通常の動作に戻ります。テープへのデータのストリーミングなど、以降のいずれのバックアップ操作も複製で実行され、データベースはオンラインのまま影響を受けません。

両方の場合とも、アプリケーションに対する影響は、複製が作成される期間に限定され、標準的なテープバックアップ方法よりも非常に小さくなっています。オンラインバックアップでは、データベース操作はまったく停止されず(ダウンタイムがゼロ)、パフォーマンスへの影響は最小限に抑制されて、トランザクションログに対する増分情報の書き込みにより主に影響される可能性があります。

複製の作成

複製プロセスでは、ある瞬間のアプリケーションデータまたはファイルシステムデータの複製が作成されます。

複製するソースまたはオリジナルデータオブジェクトを含むボリュームは、**ソースボリューム**と呼ばれます。これらは、同数の**ターゲットボリューム**に複製されます。複製プロセスが完了したときに、ターゲットボリュームのデータによって複製が構築されます。

現在のところ、基本的な複製方法には次の2種類があります(詳細はZDBと複製技術を参照)。

- **スプリットミラー**

  ミラーはソースデータの動的な複製で、ソースデータとの同期がとられます。ソースに対するすべての変更も、ミラーに適用されます。

  この方法では、アプリケーションを通常どおり使用しながら、ファイルシステムデータまたはアプリケーションデータの複製を作成および保持することができます。

  複製を作成するために、ミラーは一時的にソースから分割されます。データはミラーからバックアップされ、次にミラーではソースとの再同期がとられます。

  詳細については、『スプリットミラー複製』を参照してください。

- **スナップショット**

  スナップショット複製は、特定の時点でデータのコピーを行うことによって作成されます。スナップショットはソースボリュームから独立しているフルコピーか、ソースボリュームに依存している仮想コピーになります。

  詳細については、『スナップショット複製』を参照してください。

ZDBの種類

複製の作成後は、いずれの方法でもバックアップが可能です。この複製は、それが作成されたアレイに接続されている**バックアップシステム**にマウントされます。ZDBの利点を最大限に生かすには、分離したコンピューターシステムにする必要があります。ZDBには、次の3つの形式があります。

- **ZDBからテープ** – テープへのZDBを参照
  1. 複製内のデータは、選択したテープバックアップの種類に従ってテープにストリーミングされます。

     HPE P6000 EVAディスクアレイファミリ、HPE P9000 XPディスクアレイファミリ、HPE 3PAR StoreServ Storage (HPE P6000 / HPE 3PAR SMI-Sエージェントを介して)、EMC Symmetrix、およびSMI-Sエージェントに対するプラグインであるストレージプロバイダー(NetApp Storage、EMC VNX、およびEMC VMAX):

     フル、増分、増分1-9

     HPE P4000 SANソリューション、HPE 3PAR StoreServ Storage (HPE 3PAR VSS Agentを介して):

     フル
  2. ストリーミングが完了したら、複製は破棄してかまいません。

  データは、Data Protectorの標準的な技術を使用してテープから復元できます。
- **ZDBからディスク** – ディスクへのZDBを参照

  複製は、ディスクアレイに保持され、バックアップとして使用されます。

  インスタントリカバリ(インスタントリカバリ参照)を使用してデータを復元することで、完全な複製を復旧できます。
- **ZDBからディスク+テープ** – ディスク+テープへのZDBを参照
  1. 複製内のデータは、選択したテープバックアップの種類に従ってテープにストリーミングされます。

     HPE P6000 EVAディスクアレイファミリ、HPE P9000 XPディスクアレイファミリ、HPE 3PAR StoreServ Storage (HPE P6000 / HPE 3PAR SMI-S Agentを介して)、EMC Symmetrix:

     フル、増分、増分1-9

HPE P4000 SANソリューション、HPE 3PAR StoreServ Storage (HPE 3PAR VSS Agentを介して):

フル

2. 複製はディスクアレイ上に保持されます。

これは次の2通りの方法でデータを復元できるため、柔軟性の高い方法と言えます。

- Data Protectorを使用してテープから復元する標準的な方法(個々のバックアップオブジェクトを個別に復元可能)
- インスタントリカバリ(インスタントリカバリ参照)を使用して、複製から直接、完全な複製を復元する方法

サポートされているディスクアレイ

サポートされている複製技術とZDBの種類およびディスクアレイファミリ

ZDBの種類/ディスクアレイファミリ	テープへのZDB、ローカル	テープへのZDB、リモート	テープへのZDB、リモート+ローカル	ディスクへのZDB、ローカル	ディスク+テープへのZDB、ローカル
HPE P4000 SANソリューション	スナップショット	なし	なし	スナップショット	スナップショット
HPE P6000 EVAディスクアレイファミリ	スナップショット	なし	スナップショット	スナップショット	スナップショット
HPE P9000 XPディスクアレイファミリ	スプリットミラー/スナップショット	スプリットミラー	スプリットミラー/スナップショット	スプリットミラー/スナップショット	スプリットミラー/スナップショット
HPE 3PAR StoreServ Storage	スナップショット	なし	なし	スナップショット	スナップショット
EMC Symmetrix	スプリットミラー	スプリットミラー	スプリットミラー	なし	なし
EMC VNXストレージファミリ	スナップショット	なし	なし	なし	なし

ZDBの種類/ディスクアレイファミリ	テープへのZDB、ローカル	テープへのZDB、リモート	テープへのZDB、リモート+ローカル	ディスクへのZDB、ローカル	ディスク+テープへのZDB、ローカル
EMC VMAX ストレージファミリ	スナップショット	なし	なし	なし	なし
NetApp Storage	スナップショット	なし	なし	なし	なし

ローカルおよび**リモート**は、複製が作成されるディスクアレイを指します。つまり、ソースデータと同じディスクアレイ(ローカル)なのか、リモートサイトにある別のディスクアレイ(リモート)なのかという意味です。各種用語とその意味については、以下を参照してください。

- ローカル複製
- リモート複製
- リモートプラスローカル複製

ZDBデータのインスタントリカバリと復元

インスタントリカバリ

インスタントリカバリでは、データの復元先のディスクアレイに複製が存在する必要があります。アプリケーションシステムとバックアップシステムが無効化されるほか、複製の内容が元の場所に直接復元されるか、ソースボリュームの内容の代わりに複製の内容がシステムのアクセス先として設定されます。復元はディスクアレイ内部で実行されため、非常に高速に実行されます。

復元が完了すると、関連するデータベースやファイルシステムのセクションは複製が作成された時点の状態に戻り、アプリケーションシステムも再び使用可能になります。

関連するアプリケーションまたはデータベースにより、これが必要なすべてのものになります。別にバックアップされ、アーカイブされたトランザクションログファイルの適用など、完全な復元には追加の処理が必要な場合もあります。

詳細については、「インスタントリカバリ」を参照してください。

ZDBデータの他の復元方法

テープにバックアップされたデータは、標準的なData Protectorの復元処理を使用して復元できます。

詳細については、『*HPE Data Protectorコンセプトガイド*』を参照してください。

ただし、特定のディスクアレイファミリでは、先にテープからデータを復元して複製を更新し、その後、複製の内容を元の場所に復元することができます。これは**スプリットミラー復元**と呼ばれます。複製の内容を

元の場所に復元することは、インスタントリカバリと類似したプロセスです。この段階でのみアプリケーション操作を中断する必要があり、アプリケーションへの影響が最小限に抑えられます。

詳細については、「スプリットミラー復元」を参照してください。

> **注:**
> 複製は、データマイニングなど、インスタントリカバリ以外の目的で使用することができます。Data Protectorでは、このような目的で複製を作成し、管理することができますが、インスタントリカバリのために作成した複製はインスタントリカバリのみに使用する必要があります。そうしない場合、バックアップしたデータが失われることがあります。

ZDBの種類の復元可能性

ZDBの種類と復元の可否

	復元可能性		
ZDBの形式と方法	**個々のオブジェクト**	**ディザスタリカバリ**	**インスタントリカバリ**
テープへのZDB、ローカル	可	可	不可
テープへのZDB、リモート	可	可	不可
テープへのZDB、リモート+ローカル	可	可	不可
ディスクへのZDB、ローカル	不可	不可	可
ディスク+テープへのZDB、ローカル	可	可	可

第10章: ZDBと複製技術

Data Protectorでサポートされているディスクアレイ統合のうち、HPE P4000 SANソリューション、HPE P6000 EVAディスクアレイファミリ、HPE 3PAR StoreServ Storage、NetApp Storage、EMC VNX、およびEMC VMAX Storage Family統合はスナップショット、EMC Symmetrix Disk Array統合はスプリットミラー、HPE P9000 XPディスクアレイファミリ統合はスプリットミラーとスナップショットの複製技術をサポートしています。どちらの技術も、指定されたソースデータを含むボリュームのコピーが作成されます。これらのコピーは、同じディスクアレイの別の論理ボリュームに作成されて、ホストシステムに表示することができます。どの場合も、複製のために選択されたデータが論理ボリュームのごく一部であっても、ディスクアレイ上の完全な論理ボリュームしか複製できません。

複製されるソースデータを含むボリュームは、ソースボリュームと呼ばれます。これらは、複製データを含むターゲットボリュームと同じ数だけ複製されます。複製プロセスが完了したときに、ターゲットボリュームのデータによって複製が構築されます。

複製は、同じディスクアレイに作成するか(ローカル複製)、または別のリモートディスクアレイに作成する(リモート複製)ことができます。特定のディスクアレイファミリでは、これら2つの複製方法を組み合わせて、最高レベルのデータ保護を得ることもできます(リモートプラスローカル複製)。

オペレーティングシステムから見た場合、ソースデータの特定セットの複製の内容は、複製の作成に使用される方法に関係なく同じです。ただし、使用される方法によって次のような機能に影響が出る可能性があります。

- 複製の速度
- 使用するストレージスペースの量
- 関与するアプリケーションへの影響
- データセキュリティ

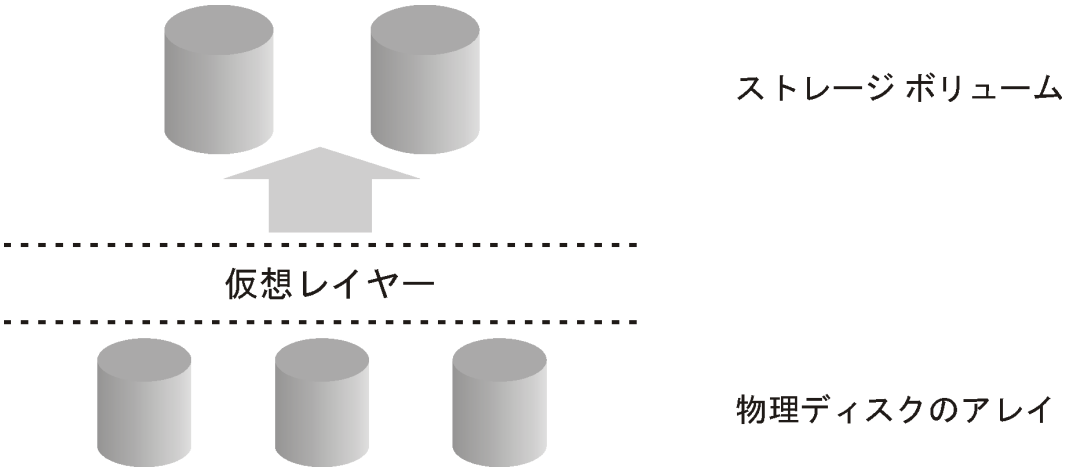
ディスクアレイの種類によっては、特定のハードウェアまたはソフトウェアの制限を受ける場合もあります。使用可能な複製技術は、ディスクアレイの種類とインストールされた複製ソフトウェアによって決まります。

ディスクアレイの基本

使用可能な複製技術は、ディスクアレイの種類、インストールされているファームウェアやソフトウェアによって異なります。

ディスクアレイでは、ディスク仮想化技術がサポートされているため、仮想ディスクや論理ボリュームなどの作成が可能です。

ディスク仮 想 化



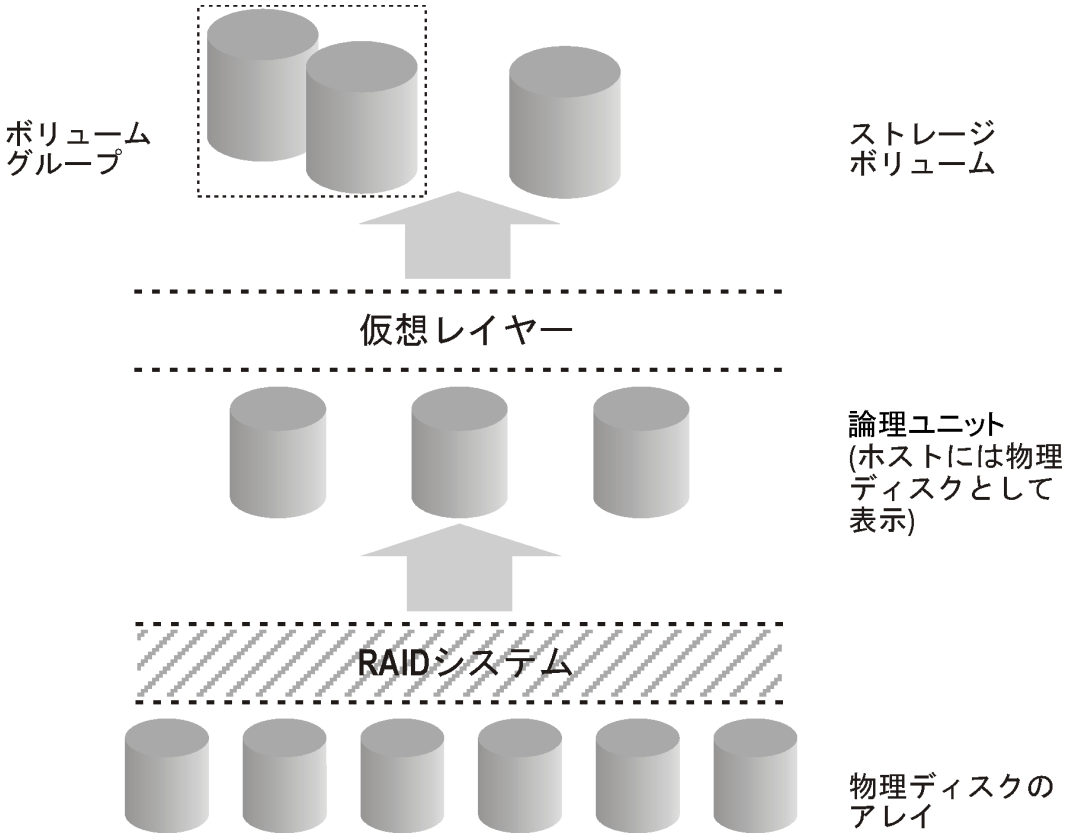
物 理 ディスクのアレイは、データストレージの1つの大 きなブロックとして構 成されています。これは、複 数 の仮 想 ストレージブロックに分 割 することができ、ホストシステムまたはオペレーティングシステムから使 用 されます。

このようなブロックにはさまざまな呼 び名 がありますが、基 本 的 な作 成 の技 術 は同じであるため、本 書 では分 かりやすいようにすべてストレージボリュームと呼 びます。

RAID技 術

ディスクアレイでは、RAIDシステムによって使 用 可 能 なストレージに適 用 される**RAID技 術** を使 用 して、データの冗 長 化 を行 い、データ保 護 を強 化 します。

RAIDによるディスク仮 想 化



RAIDにはいくつかのレベルがあり、それぞれにデータの冗 長 性 、速 度 、アクセス時 間 などのレベルが異 なります。使 用 可 能 なストレージ容 量 によって、これらの属 性 の間 でバランスを調 整 できる場 合 があります。

RAIDシステムは、複 数 の物 理 ディスクにデータを分 散 させ、論 理 ユニットとしてホストから使 用 することで動 作 します。論 理 ユニットは、上 記 のディスク仮 想 化 の図 では物 理 ディスクと見 なすことができます。仮 想 化 後 に最 終 的 にホストのオペレーティングシステムから使 用 できるのは、仮 想 ディスクまたはストレージボリュームということになります。

複 製 技 術

基 本 的 な複 製 処 理 は、次 の3つの枠 組 みで実 行 されます。

- ローカル(ソースボリュームとターゲットボリュームが同じディスクアレイに存 在)
- ローカル – HP-UX LVMミラーと統 合 (ソースボリュームとターゲットボリュームが同じディスクアレイに存 在 するが、少 なくとも2つのディスクアレイが必 要)
- リモート(ソースボリュームとターゲットボリュームが別 々 のディスクアレイに存 在)
- リモートプラスローカル(リモートのディスクアレイでのリモートプラスローカル複 製)

複 製 の作 成 にどちらの方 式 が使 用 されても、オペレーティングシステムから見 ると、ソースボリュームとその複 製 の内 容 は同 一 です。ただし、使 用 される方 法 によって次 のようなことに影 響 が出 る可 能 性 があります。

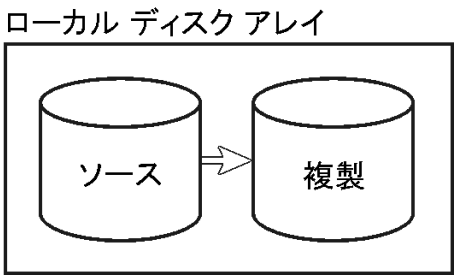
- 複 製 の速 度
- 使 用 するストレージスペースの量
- 関 与 するアプリケーションへの影 響
- データセキュリティ

以 降 の項 では、上 記 の各 枠 組 みで行 われる複 製 方 法 について説 明 します。

ローカル複 製

ローカル複 製 では、データが同 じディスクアレイ内 で複 製 されます。つまり、ソースボリュームとターゲットボリュームが同 じディスクアレイにあるということです。

ローカル複 製



ローカル複 製 には、次 の2通 りの技 術 があります。

- スプリットミラー
- スナップショット

ローカル複 製 の利 点

- Data Protectorでサポートされるすべての種 類 のディスクアレイ上 で使 用 できる。
- Data Protectorでサポートされるすべてのアプリケーション統 合 で使 用 できる。
- 複 製 プロセスおよび同 期 プロセスは、すべてローカルディスクアレイで実 行 されます。これは、処 理 が高 速 で、アプリケーションシステムの中 断 が最 小 限 に抑 えられることを意 味 します。
- あらゆる種 類 のZDB(インスタントリカバリも含 む)で対 応 が可 能 なため、バックアップ方 法 を柔 軟 に選 択 できる。

欠 点

- ソースデータと複 製 の両 方 が、ディスクアレイまたはローカルシステムの致 命 的 な障 害 に対 して無 防 備 である。

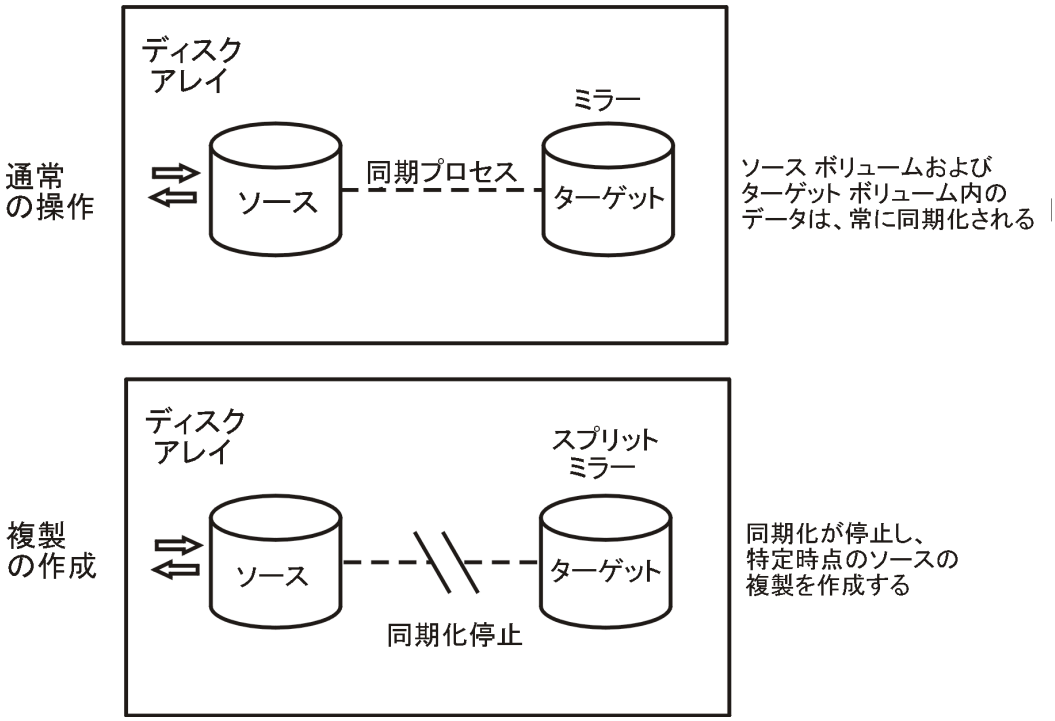
ローカル複 製 には、次 の2通 りの方 法 があります。

- スプリットミラー複 製
- スナップショット複 製

スプリットミラー複 製

ディスクアレイの用 語 では、**ミラー**はソースボリュームの動 的 なコピーです。

スプリットミラー複 製



ミラーが最 初 に作 成 されるとき、ミラーのデータはソースボリュームのデータと同 一 になるまで同 期 されます。アプリケーションを平 常 どおりに使 用 している間 、ミラーはソースボリュームと同 期 された状 態 が保 たれ、ソースボリュームに対 するすべての変 更 がミラーに適 用 されます。

管 理 作 業 (*バックアップ*など)の目 的 で、特 定 時 点 のデータの複 製 を保 持 しておく場 合 は、以 下 の手 順 に従 います。

1. ミラー関 係 にあるボリューム間 の同 期 が停 止 し(ミラーが切 り離 され)、ソースボリュームの独 立 した複 製 が残 されます。
2. 複 製 を使 って*バックアップ*などの作 業 を行 います。アプリケーションでは、実 質 的 な影 響 を受 けずに、引 き続 きソースデータを使 用 できます。
3. 必 要 に応 じて、複 製 に対 する作 業 が完 了 した後 、別 の管 理 作 業 でミラーデータが必 要 になるまで、2つのデータセットを再 同 期 化 することも可 能 です。

分 割 は非 常 に高 速 に行 われるため、アプリケーションシステムに及 ぼす影 響 は最 小 限 に抑 えられます。

スプリットミラー複 製 をサポートするData Protectorディスクアレイ統 合 は、次 のとおりです。

- HPE Business Copy P9000 XP構 成 を使 用 したHPE P9000 XPディスクアレイファミリ統 合 。インスタントリカバリのために使 用 される3つのファーストレベルミラーの作 成 を可 能 にします。
- TimeFinder構 成 を使 用 したEMC Symmetrix Disk Array統 合 。この統 合 を使 用 したインスタントリカバリは不 可 能 であり、利 用 できるZDBはテープへのZDBだけです。

スプリットミラー複 製 の特 徴

- スプリットミラー複 製 はソースボリュームの完 全 な複 製 (クローン)で、ホスト やオペレーティングシステムから見 ると、複 製 が作 成 された時 点 のソースとまったく同じになります。

  物 理 ディスクまたは論 理 ユニット のレベルでは、ソースストレージブロックの内 容 の完 全 な物 理 コピーが存 在 することになります。
- オリジナルからは完 全 に独 立 しています。

  データのコピーが物 理 的 に独 立 しているため、ソースボリュームに影 響 する部 分 的 なハードウェア障 害 がディスクアレイで発 生 しても、ターゲットボリュームは正 常 かつ使 用 可 能 な状 態 が高 い確 率 で維 持 されます。

スナップショット 複 製

スナップショット 複 製 は特 定 の時 点 で瞬 時 に作 成 され、即 座 に使 用 可 能 になります。スプリットミラー複 製 とは異 なり、最 初 にデータはコピーされませんが、オリジナルストレージの複 製 が仮 想 化 を通 じて作 成 されます。その時 点 では、複 製 は仮 想 コピーです。実 際 のデータは、ソースと複 製 の両 方 で共 有 されます。

その後 、最 初 にソースボリュームにあるデータが変 更 される際 に、まずオリジナルデータがスナップショットにコピーされ、次 にソースデータが更 新 されます。時 間 が経 過 するにつれて、スナップショットでは、(未 変 更 ソースデータへのポインターの形 式 で)その独 立 データと共 有 データが部 分 的 に参 照 されます。ただし、ホストシステムまたはオペレーティングシステムから見 ると、スナップショットには作 成 された時 点 のソースボリュームの完 全 なコピーが常 に含 まれています。

スナップショット 複 製 をサポートするData Protectorディスクアレイ統 合 は、次 のとおりです。

- HPE Business Copy P6000 EVA構 成 を使 用 したHPE P6000 EVAディスクアレイファミリ統 合 。インスタントリカバリ用 に大 量 の複 製 セットをディスクアレイに作 成 できます。標 準 スナップショット およびvsnapによって構 成 される複 製 セット内 の複 製 の最 大 数 はP6000 EVAストレージシステムのファームウェアバージョンによって制 限 されますが、スナップクローンで構 成 される複 製 セット内 の複 製 の最 大 数 は、ディスクアレイの残 りのストレージ容 量 によってのみ制 限 されます。
- HPE Business Copy P9000 XP構 成 を使 用 したHPE P9000 XPディスクアレイファミリ統 合 。インスタントリカバリ用 に大 量 の複 製 セットをディスクアレイに作 成 できます。その場 合 、メンバーの数 は、ディスクアレイモデル、インストールされているディスクアレイのファームウェアバージョン、およびディスクアレイ上 のターゲットストレージプールの残 りのストレージ容 量 によって制 限 されます。
- HPE 3PAR StoreServ Storage統 合 、NetApp Storage統 合 、EMC VNXストレージファミリ、およびローカルコピー構 成 を使 用 したEMC VMAXストレージファミリ統 合 。標 準 スナップショット とvsnapsで構 成 される複 製 セット内 の複 製 の最 大 数 は、ファームウェアによって制 限 されます。

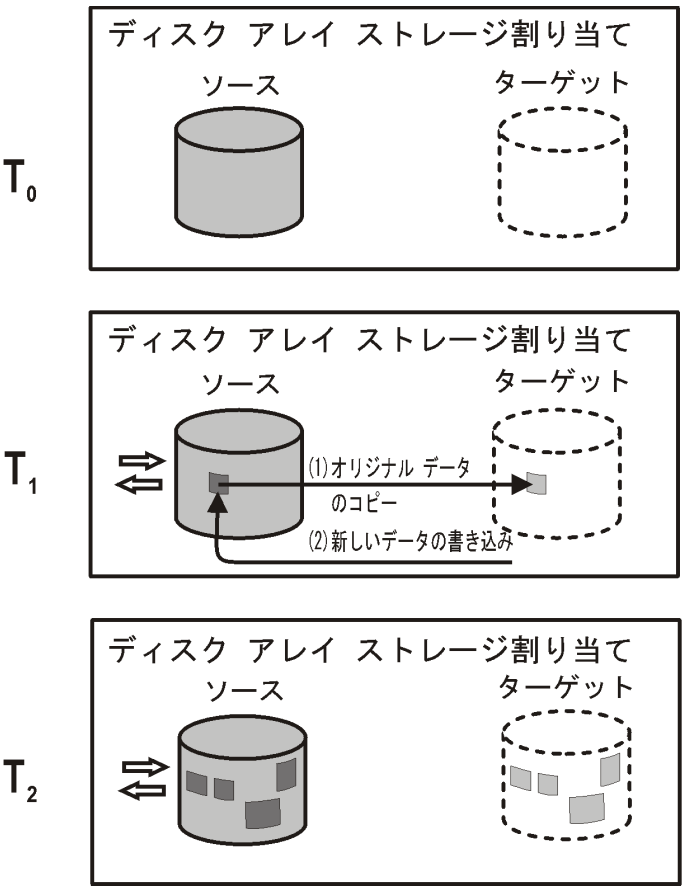
Data Protectorでサポートされているアレイ統 合 を使 用 すると、以 下 のような種 類 のスナップショットを作 成 できます。

- **標 準 スナップショット**(「事 前 割 り当 てスナップショット」、「完 全 割 り当 てスナップショット」、または単 に「スナップショット」とも呼 ばれる): すべてのソースデータのフルコピーを保 持 するためにスナップショット が作 成 される際 、十 分 なスペースが割 り当 てられます。
- **Vsnap**(「実 質 的 に容 量 を必 要 としないスナップショット」または「デマンド割 り当 てスナップショット」とも呼 ばれる): スペースは事 前 に割 り当 てられません。
- **スナップクローン**: 最 初 は標 準 スナップショットとして開 始 され、その後 、スナップクローンが作 成 時 点 のソースボリュームの完 全 な物 理 コピーになるまで、バックグラウンド でデータがコピーされます。

これらの詳 細 については、以 下 で説 明 します。

標 準 スナップショット

標 準 スナップショットの作 成



1. T_0の時 点 では、ソースボリュームによって消 費 されている分 と同じストレージ容 量 が、ターゲットボリューム用 のディスクアレイに割り当 てられています。

   データはソースストレージブロックからコピーされません。代 わりに、オリジナルデータを保 持しているストレージブロックにポインターがマッピングされ、コピーは完 全 に仮 想 的 なものとなります。ただし、ホストから見 た場 合 、T_0の時 点 でソースボリュームの完 全 な複 製 がターゲットボリュームに存 在 し、使 用 できるようになっています。

2. スナップショットの作 成 後 にT_0ソースデータを更 新 する必 要 が生 じた場 合 は、まずソースデータがターゲットのストレージブロックにコピーされ、このコピーにスナップショット内 のポインターが再 マッピングされます。その後 のみ、ソースデータが更 新 されます。

   これは、「コピーオンライト」と呼 ばれます。

3. スナップショットは、部 分 的 に実コピー(ソースデータをコピー済 み)、部 分 的 に仮 想 コピーになっています。複 製 がアクセスされる際 、以 前 にコピーされているデータはターゲットストレージブロックから読 み込 まれ、コピーされていないデータはソースストレージブロックから読 み込 まれます。したがって、ホストから見 た場 合 、T_0の時 点 でのソースデータの完 全 な複 製 がまだ存 在 していることになります。

標 準 スナップショットの特 性

- 標 準 スナップショットは、元 のデータの独 立した複 製 ではありません(ただし、時 間 が経 つとソースボリュームの1つ1つのストレージブロックが更 新 され、コピーされている可 能 性 はあります)。
- ソースボリュームのすべてのデータが変 更 された場 合 でも、スナップショット用 に十 分 なスペースが確 保 されます。
- スペースの観 点 からは非 効 率 的 です。変 更 されるすべてのデータのために十 分 なスペースが常 に予 約 されますが、通 常 はその一 部 分 のみしか使 用 されません。スナップショットが存 在 する間 、予 約 済 みスペースの残りを他 の目 的 で使 用 することはできません。

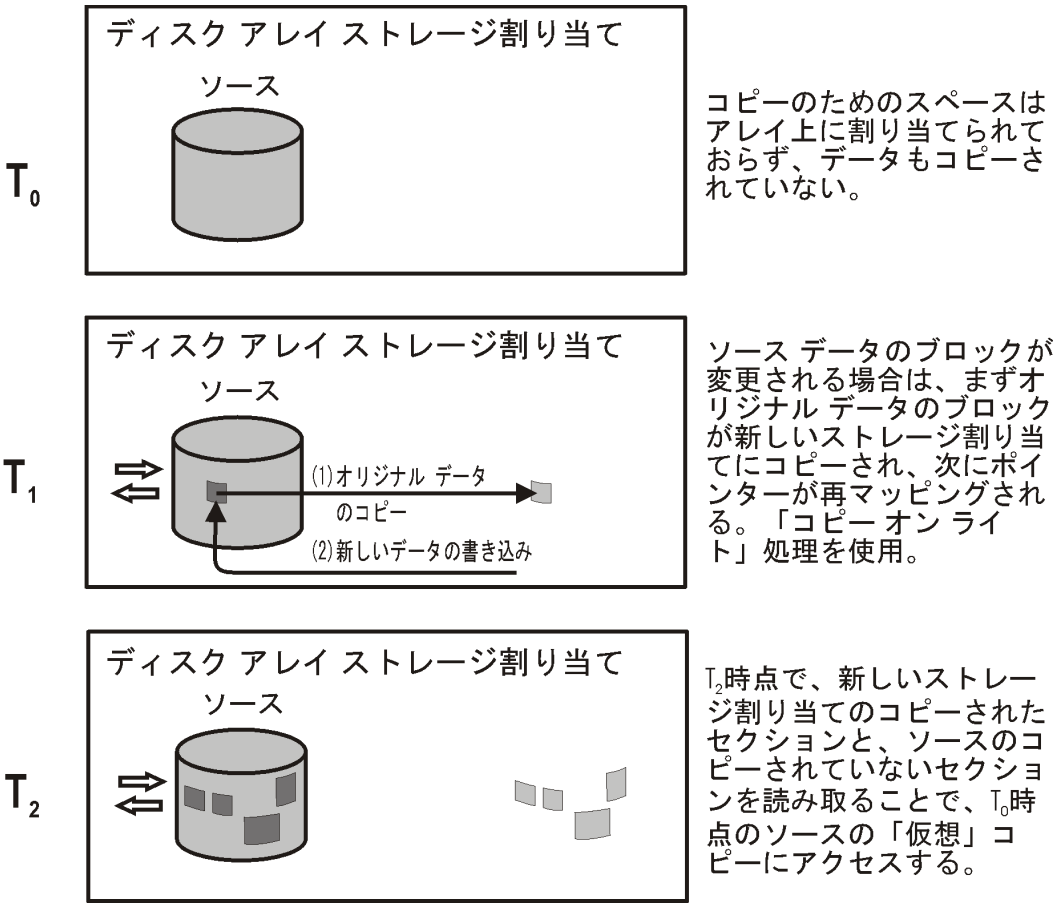
アプリケーションのパフォーマンスへの影 響

バックアップシステムからスナップショットにアクセスする際 、ソースボリュームと複 製 の両 方 からディスクブロックが読 み込 まれます。したがって、アプリケーションシステムとバックアップシステムの両 方 のディスクリソースが使 用 されるため、ディスクアレイの負 荷 が極 端 に高 いとアプリケーションのパフォーマンスが低 下 します。

Vsnap

Vsnapスナップショットでは、最 初 の時 点 でストレージ容 量 は予 約 されません。それ以 外 の点 では、プロセスは標 準 スナップショットと非 常 に類 似 しています。

Vsnapの作 成



1. T_0の時 点 では、標 準 スナップショットと同 様 にポインターのみがターゲットにコピーされますが、ターゲットボリュームではスペースは予 約 されません。このスナップショットでは、ポインターで必 要 とされる以 外

のストレージスペースは占 有 されません。

2. スナップショットの作 成 後 にT_0ソースデータを更 新 する必 要 が生 じた場 合 は、標 準 スナップショットとして「コピーオンライト」が使 用 されます。ストレージスペースは、変 更 されたデータに対 してのみ必 要 です。
3. 標 準 スナップショットと同 様 に、このスナップショットも実 コピーと仮 想 コピーで構 成 されています。

Vsnapの特 性

- 標 準 スナップショットと同 様 に、Vsnapは元 のデータの独 立 した複 製 ではありません。
- Vsnapでは、複 製 のサイズの増 大 に対 応 する十 分 なスペースを確 保 する、独 立 したディスク容 量 管 理 が必 要 です。ディスクアレイのスペースを使 い切 ると、Vsnapの更 新 は失 敗 し、ディスクアレイの一 般 的 な動 作 に支 障 をきたすことがあります。
- スペース効 率 に優 れています。Vsnapでは、必 要 なスペースのみが使 用 されます。
- 短 期 間 だけ存 続 することが想 定 されています。Vsnapでは必 要 となるストレージが動 的 であるため、スナップショットの作 成 後 にソースボリュームに対 して多 くの変 更 があった場 合 、ディスクアレイのスペースが不 足 する可 能 性 があります。ディスクアレイに対 するその他 のストレージ要 求 も、ディスクアレイでストレージが不 足 する原 因 となる可 能 性 があります。

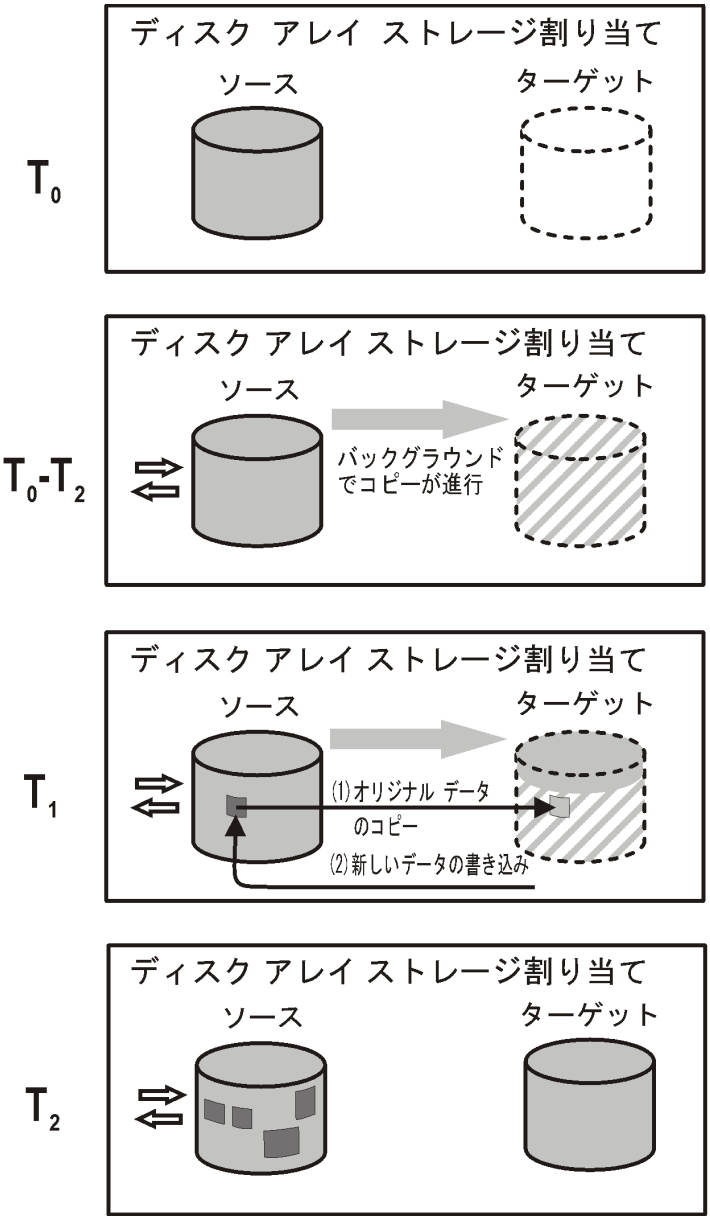
アプリケーションのパフォーマンスへの影 響

標 準 スナップショットと同 様 に、バックアップシステムからスナップショットにアクセスする際 、ソースボリュームと複 製 の両 方 からディスクブロックが読 み込 まれます。したがって、アプリケーションシステムとバックアップシステムの両 方 のディスクリソースが使 用 されるため、ディスクアレイの負 荷 が極 端 に高 いとアプリケーションのパフォーマンスが低 下 します。

スナップクローン

スナップクローンは最 初 は標 準 スナップショットですが、最 後 はスプリットミラー複 製 と同 様 の完 全 な複 製 (またはクローン)になります。

スナップクローンの作 成



Data Protectorのスナップクローンは、その作 成プロセスを高 速にし、データをコピーするときのソースボ リュームへの影 響を少 なくするために、**コンテナー**と呼 ばれるストレージオブジェクトとともに作 成されます。 コンテナーとは、後 で標準 スナップショット、Vsnap、スナップクローンとして使 用するために事 前に割り当 て られるディスクアレイ上 のスペースであり、空きディスクスペースから作 成されるものと、不 要になったスト レージボリュームから変 換されるものがあります。

スナップクローンの作 成のプロセスは、以 下のとおりです。

1. サイズとストレージ冗 長レベルがソースボリュームと同じコンテナーがディスクアレイに作 成されます(そのようなコンテナーが存 在しない場 合)。
2. ソースボリュームのキャッシュ書き込 みポリシーがライトスルーモードに設 定され、キャッシュのすべての

データが物 理 ディスクに書 き込 まれます。

3. 標 準 スナップショットが作 成 され、完 全 コピー用 に十 分 なスペースが割 り当 てられます。
4. バックグラウンドプロセスが、未 変 更 のデータをソースストレージブロックからターゲットストレージブロック にコピーする処 理 を開 始 します。この時 点 で、キャッシュ書 き込 みポリシーは自 動 的 にライトバック モードに戻 ります。
5. バックグラウンドプロセスでコピーされる前 のソースデータを更 新 する場 合 は、標 準 スナップショットの場 合 と同 様 に、まずソースデータのコピー(コピーオンライト)が行 われます。

   バックグラウンドコピープロセスの実 行 中 、標 準 スナップショットと同 様 に、スナップショットを使 用 する必 要 がある場 合 、コピーは部 分 的 に仮 想 コピー、部 分 的 に実 コピーとなります。
6. ターゲットのストレージの場 所 にデータがすべてコピーされた時 点 でバックグラウンドプロセスが停 止 し、T_0時 点 でのソースのスタンドアロン複 製 (クローン)が保 持 されます。

スナップクローンの特 徴 (コピー完 了 後)

- スナップクローンはソースボリュームの完 全 な複 製 であり、ホストやオペレーティングシステムから見 れば、作 成 時 点 ではスナップクローンはソースと同 一 です。

  物 理 ディスクまたは論 理 ユニットのレベルでは、ソースストレージブロックの内 容 の完 全 な物 理 コピーが存 在 することになります。
- オリジナルからは完 全 に独 立 しています。

  完 全 な物 理 コピーであるため、ソースボリュームの内 容 が失 われたり、損 傷 したりしても、ターゲットボリュームの内 容 には影 響 しません。
- 長 期 間 保 持 することが想 定 されています。

アプリケーションのパフォーマンスへの影 響

- バックグラウンドのデータコピープロセスは、リソースの競 合 により、アプリケーションのパフォーマンスに影 響 を及 ぼす可 能 性 があります。大 規 模 なデータベースのスナップクローンを作 成 している際 は、コピーに非 常 に長 い期 間 を要 する場 合 があります。

  コンテナーを使 用 すると、データコピープロセスがアプリケーションのパフォーマンスに及 ぼす影 響 が低 減 されます。アプリケーションがバックアップモードになっている必 要 がある時 間 枠 も大 幅 に短 くなります。
- クローン化 プロセスの終 了 前 にシステムからスナップクローンへのアクセスがあると、まだコピーされていないディスクブロックがソースボリュームから読 み込 まれます。テープへのZDBまたはディスク+テープへのZDBの場 合 、アプリケーションシステムとバックアップシステムの両 方 を使 用 してデータが読 み込 まれるので、アプリケーションのパフォーマンスが低 下 することがあります。これを避 けるために、Data Protectorではクローン化 プロセスが処 理 中 の場 合 、テープへのスナップクローンデータのコピーが最 大 で90分 まで遅 延 されます。この遅 延 時 間 はデフォルト値 であり、バックアップ仕 様 を構 成 するときにData ProtectorのGUIで変 更 することができます。

ローカル複 製 とHP-UX LVMミラーの統 合

ローカル複 製 とHP-UX LVMミラーの統 合 は、完 全 なバージョンを得 るために複 製 する必 要 があるストレージの量 が少 なくなる特 別 な統 合 です。また、LVMミラーは、スプリットミラーおよびスナップショットアレイのリモートプラスローカル複 製 環 境 でHPE Continuous Access (CA)またはEMC Symmetrix Remote Data Facility (SRDF)が果 たす機 能 と同 じような機 能 が得 られるように構 成 することもできます。

ローカル複 製 とLVMミラーの統 合 の利 点

- Data Protectorでサポートされるすべての種 類 のディスクアレイ上 で使 用 できる。
- 使 用 されているディスク全 体 の一 部 を複 製 することにより、ディスクスペースの使 用 量 を削 減 できる。
- LVMミラー環 境 は、純 粋 なCA環 境 またはSRDF環 境 に比 べて、セットアップと管 理 が容 易 である。
- I/Oチャネルにエラーが発 生 しても、LVMが複 製 ソースからデータを復 旧 できる。
- LVMミラー環 境 はCA/SRDFライセンスが不 要 であるため、CA環 境 またはSRDF環 境 に比 べてコスト が低 い。BCライセンスは、複 製 を作 成 するシステム上 でのみ必 要 である。

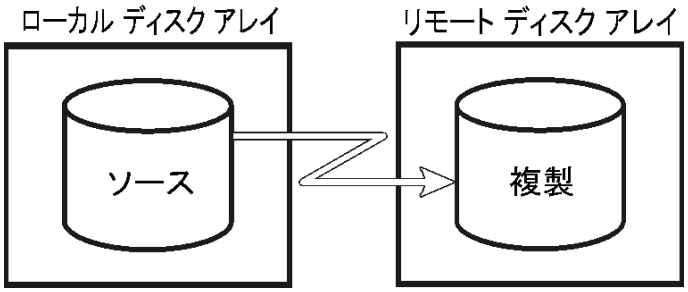
欠 点

- LVMミラー構 成 のセットアップはより複 雑 となることがあり、BCまたはTimeFinder環 境 に対 する要 件 より もより厳 密 な要 件 が必 要 である。
- LVMミラー構 成 により、インスタントリカバリの実 行 方 法 が複 雑 になる。特 定 のディスクアレイでは、 LVMミラー構 成 でバックアップしたデータのインスタントリカバリはサポートされていません。

リモート複 製

リモート複 製 では、データが別 のリモートディスクアレイに複 製 されます。複 製 されたデータは、このリモート ディスクアレイから、さらにローカルの使 用 可 能 なメディアにバックアップできます。一 度 確 立 されると、リモー ト複 製 は自 動 的 に続 行 され、持 続 的 なリアルタイムリモート複 製 が行 われます。

リモート複 製



リモート複 製 の利 点

- ストレージシステムの損 失 などの甚 大 な障 害 からも保 護 できます。リモートディスクアレイが別 の(リモー ト)コンピューティングセンターに配 置 されている場 合 、リモート複 製 を行 うことで、コンピューティングセン ター全 体 が破 壊 される場 合 であっても、実 環 境 とバックアップ環 境 の両 方 を同 時 に損 なうような、火 災 やその他 災 害 によるリスクを排 除 できます。
- ディザスタリカバリに適 している。
- 重 要 なデータの継 続 的 な可 用 性 が保 証 される。

欠 点

- ネットワークやファイバーチャネル接 続 の転 送 速 度 が、アプリケーションやデータベースのパフォーマンスに 大 きく影 響 する。
- 同 期 転 送 が必 要 なため、アプリケーションシステムに影 響 を及 ぼす可 能 性 がある。
- 少 なくとも2つのディスクアレイとそのライセンスが必 要 なため、高 コストである。
- 同 期 をリモートで保 持 する必 要 があるため、パフォーマンスやアプリケーションに影 響 を及 ぼす可 能 性 がある。

スプリットミラー複 製

ローカルミラーと同じように、ソースボリュームの複 製 がターゲット ボリュームで作 成 および保 持 されますが、この複 製 の場 合 のみターゲット ボリュームがリモート ディスクアレイに存 在 します。 構 築 された後 、ターゲット ボリュームはローカルディスクアレイのソースボリュームと同 期 した状 態 が保 たれます。

ある特 定 の時 点 のソースボリュームの複 製 が必 要 な際 には、ミラーボリューム間 の同 期 が停 止 されます。このとき、リモート ディスクアレイには、ローカルディスクアレイにあるソースボリュームの不 変 のコピー(独 立 した複 製)が存 在 します。

ただし、アレイが別 々 のサイトにインストールされている場 合 は、継 続 的 なリモート同 期 が数 キロメートルにまたがって行 われることがあるため、アプリケーションのパフォーマンスに影 響 を及 ぼす場 合 があります。Data Protectorでは、リモートシステムへのリンクは通 常 、同 期 されている必 要 があります。ただし、CAでは非 同 期 通 信 がサポートされます。Data Protectorでは、ミラーにデータをコピーする際 に同 期 モードに変 更 され、その後 で非 同 期 モードに戻 されます。

この構 成 は、(特 にクラスター環 境 において)ディザスタリカバリの目 的 で選 択 することができます。この場 合 、潜 在 的 な利 点 がCAリンクを保 持 する欠 点 を上 回 ります。 バックアップ目 的 でリンクを切 断 すると、ディザスタリカバリの対 象 範 囲 を狭 め、フェイルオーバーが不 可 能 になります。リモートプラスローカル複 製 と比 較 してください。

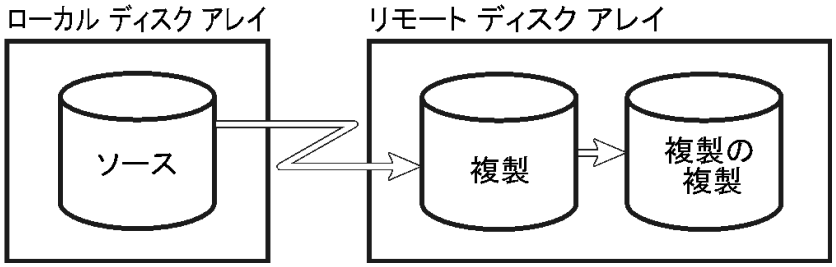
Data Protectorは、HPE P9000 XPディスクアレイファミリ Continuous Access HPE構 成 を使 用 するP9000 XPでリモート複 製 にミラー化 技 術 を使 用 すること、およびSymmetrix Remote Data Facility構 成 を使 用 するEMC Symmetrix Disk Arrayでリモート複 製 にミラー化 技 術 を使 用 することをサポートしています。

Data Protectorでは、HPE P6000 EVAディスクアレイファミリでのリモート複 製 はサポートされていません。リモート複 製 を使 用 して作 成 されたZDBからのインスタントリカバリセッションもサポートされていません。つまり、データをバックアップできるのは、テープへのZDBセッションだけです。

リモートプラスローカル複 製

リモートプラスローカル複 製 では、リモート複 製 とローカル複 製 の両 方 が使 用 されます。複 製 は、リモート複 製 によってリモート ディスクアレイに作 成 された後 、ローカル複 製 用 のソースボリュームとして使 用 されます。

リモートプラスローカル複 製



この構 成 は通 常 、リモートサイトがディザスタリカバリサイトとして機 能 し、リモートペアの分 割 が不 可 能 な場 合 に使 用 します。フェイルオーバーを自 動 化 するために、クラスターアプリケーションを使 用 することができます。

Data Protectorは、以 下 のディスクアレイで、リモートプラスローカル複 製 をサポートしています。

- HPE P6000 EVAディスクアレイファミリとHPE Continuous Access + Business Copy (CA+BC) P6000 EVAの組 み合 わせ構 成
- HPE P9000 XPディスクアレイファミリとHPE Continuous Access P9000 XP + HPE Business Copy P9000 XPの組 み合 わせ構 成
- EMC Symmetrix Disk ArrayとSymmetrix Remote Data Facility + TimeFinderの組 み合 わせ構 成

リモートプラスローカル複 製 の利 点

リモート複 製 の利 点 に加 えて、以 下 のような利 点 があります。

- アプリケーションシステムやデータベースに影 響 を与 えることなくテープバックアップを作 成 できる。
- 自 動 フェイルオーバーが可 能 である。
- P6000 EVAアレイでは、フェイルオーバーが発 生 した場 合 のData Protectorの動 作 を変 更 したり、複 製 方 向 に従 うか、複 製 の場 所 を維 持 するかを選 択 したりすることができる。

欠 点

リモート複 製 の欠 点 と同 様 です。

スプリットミラー複 製

リモートでの複 製

リモート複 製 の場 合 と同 様 に、個 別 のアレイ上 に存 在 するソースボリュームとターゲットボリュームがミラーボリュームとして構 成 されます。

構 築 された後 、リモートディスクアレイのミラーボリュームはソースボリュームと同 期 した状 態 が保 たれます。Data Protectorでは、アレイ間 のリンクは同 期 されている必 要 があります。

ローカルでの複 製

リモート複 製 の段 階 のターゲットボリュームが、リモートディスクアレイでローカル複 製 用 のソースボリュームになります。

複 製 が必 要 になると、ローカルのミラーボリューム間 の同 期 は停 止 され(ミラーが分 割 され)ますが、リモートのミラーボリューム間 の同 期 は維 持 されます。このとき、リモートディスクアレイのローカル複 製 (複 製 の複 製)は、ローカルディスクアレイのソースボリュームの不 変 のコピー(独 立 した複 製)になります。

スナップショット 複 製

リモートでの複 製

データは、アプリケーションシステムからローカルアレイのソースボリュームに書 き込 まれ、リモートディスクアレイのターゲットボリュームに複 製 されます。データの複 製 がバックグランドで進 行 している間 、アプリケーションは影 響 を受 けることなく続 行 されます。

ローカルでの複 製

リモート複 製 の段 階 のターゲットボリュームが、リモートディスクアレイでローカル複 製 用 のソースボリュームになります。

スナップショット複 製 のボリュームが特 定 の時 点 で作 成 され、すぐに使 用 できる状 態 になります。詳 細 については、スナップショット複 製 を参 照 してください。

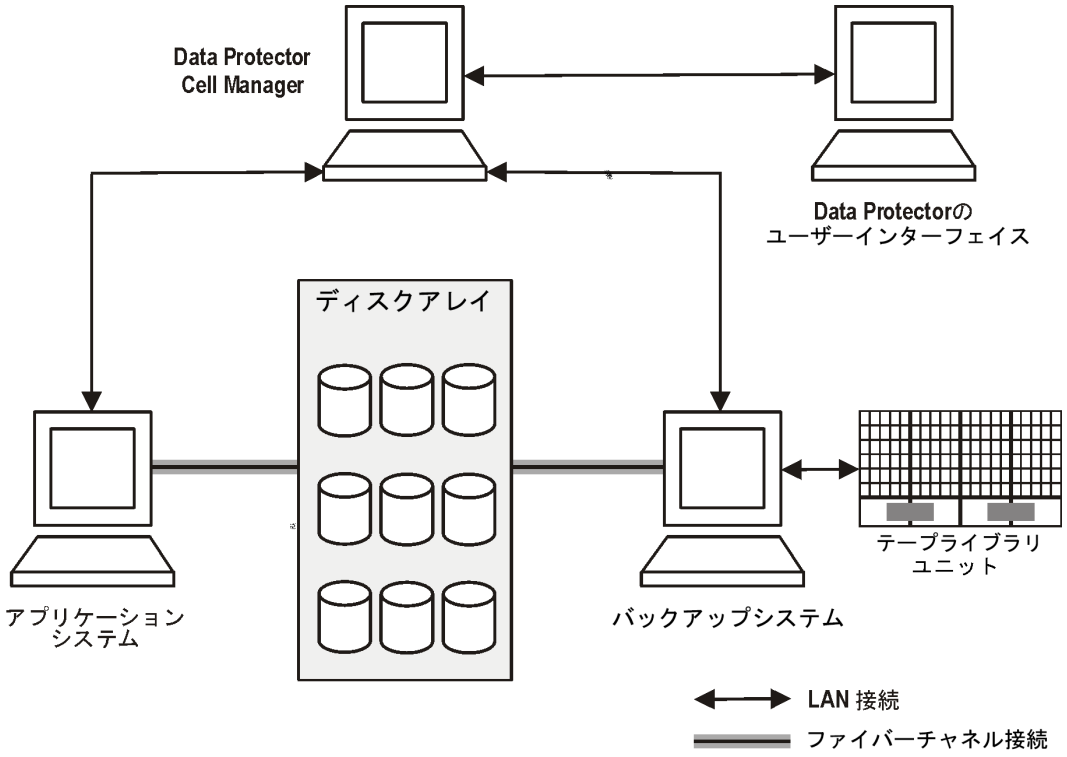
> **注:**
> リモートプラスローカル複 製 により、フェイルオーバーがある場 合 とない場 合 の複 製 の作 成 を理 解 し、管 理 できるようになるので、ソースサイトまたはあて先 サイトでZDBを実 行 することが可 能 になります。

第11章: Data ProtectorによるZDBとインスタントリカバリ

Data Protectorセル

Data Protectorでは、**セルの管理**という概念が使用されています。次の図は、ZDBおよびIRに使用されるセルのセットアップ方法を示しています。

ZDBおよびIRに使用されるData Protectorセルのセットアップ

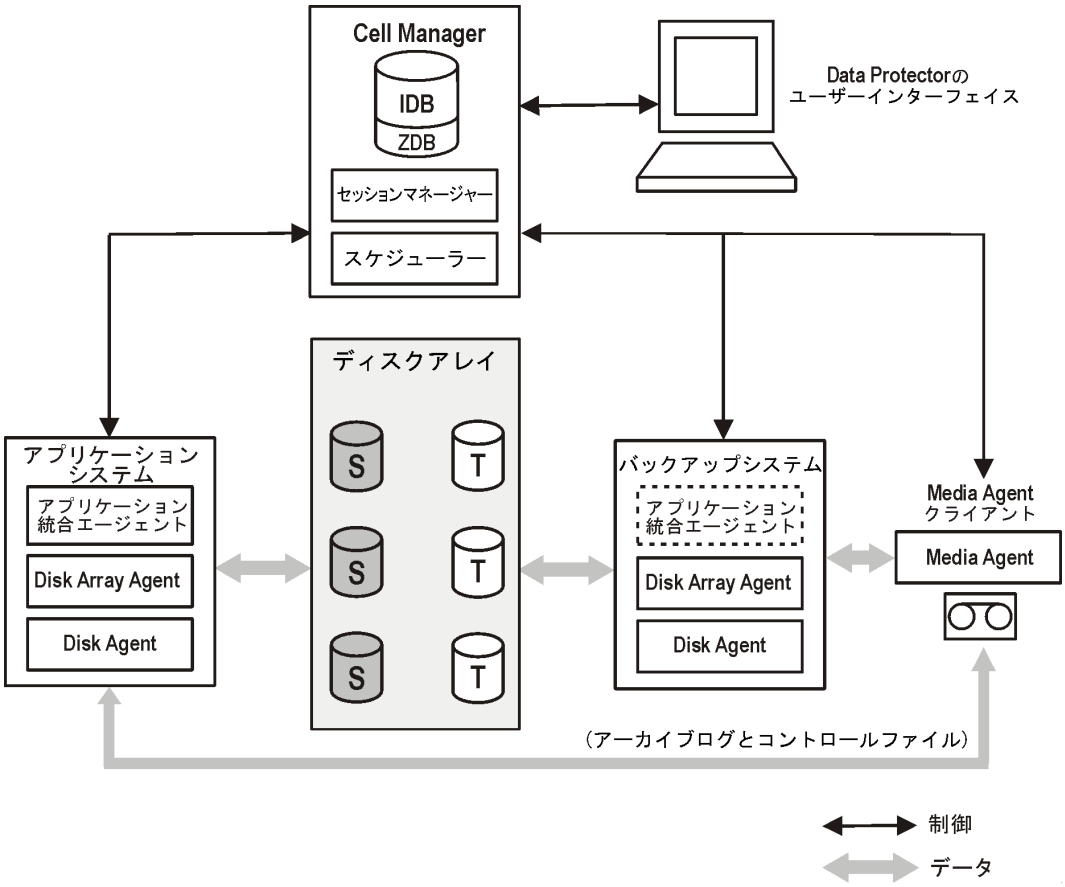


ZDB技術およびIR技術を使用するためには、バックアップ対象のアプリケーションデータベースまたはファイルシステムデータが、アプリケーションシステムとバックアップシステムの両方が直接接続されているディスクアレイに存在する必要があります。ZDBおよびIRには、ライブラリやその他ストレージデバイスは必要に応じて使用します。

セルコンポーネント

一般的なData Protectorセルの場合、次の図に示すように、処理を行うソフトウェアコンポーネントがハードウェアにインストールされている必要があります。

ZDBおよびIRに必要なソフトウェアコンポーネントの場所



Cell Manager

Cell Managerは、セルのメインシステムです。Cell ManagerがData Protectorセルで実行する機能、Cell Managerへのアクセス方法、Cell Managerと他のData Protectorコンポーネントとの共存については、Data Protectorのアーキテクチャーを参照してください。

アプリケーションシステム

複製を作成する各アプリケーションシステムには、以下のData Protectorコンポーネントがインストールされている必要があります。

- **ディスクアレイエージェント**または**ZDBエージェント** - Data Protector Cell Managerと、アプリケーションデータベースやファイルシステムがインストールされているディスクアレイとの間のやり取りが制御されます。サポートされているディスクアレイの種類ごとに、専用のエージェントがあります。
- **アプリケーション統合エージェント** - Data Protector Cell Managerとアプリケーションとの間のやり取りが制御されます。Data Protectorは、データベースアプリケーションのバックアップセッションや復元セッションでデータベースの状態を制御するなどの機能を実行することを、このエージェントに要求します。このエージェントがないと、ファイルシステムバックアップしか実行できません。

バックアップシステム

データがメディアバックアップの対象かどうかに関係なく、作成した複製の格納先となるシステムで、その後のプロセスではこのシステムを使用して複製へのアクセスが行われます。バックアップシステムとアプリケーションシステム間の接続は、ZDBとIRセッションに関係するプロセスの調整にのみ使用されます。バックアップシステムは、さまざまなアプリケーションを実行する複数のアプリケーションシステムにサービスを提供できます。また、さまざまなチェックおよび管理機能もこのシステムで実行されます。

バックアップシステムは以下の要件を満たす必要があります。

- 妥当な時間内にバックアップを実行可能であること。
- 有効なData Protector ZDBエージェントがインストールされていること。場合によっては、アプリケーション統合エージェントも必要になります。
- アプリケーションシステムと同じオペレーティングシステムを使用していること。

通常は、アプリケーションシステムとは別のシステムをバックアップシステムにします。

ZDBデータベース

ZDBデータベースは、Cell ManagerのData Protector内部データベース(IDB)の拡張です。このデータベースには、インスタントリカバリに必要な複製に関するアレイ固有の情報が保持されます。

ZDBデータベースには、Data ProtectorのZDBに標準対応(一部のファミリではIRにも標準対応)するディスクアレイファミリごとに以下の独立したセクションがあります。

- HPE P6000 EVAディスクアレイファミリ用のSMISDB、HPE 3PAR StoreServ Storage、NetApp Storage、EMC VMAXストレージ、およびEMC VNXストレージ。
- XPDB(HPE P9000 XPディスクアレイファミリ)

さらに、別のセクションには、ファイルシステムまたはボリューム管理構成などのオペレーティングシステム情報が含まれています。

- SYSDB

ZDBに保存される情報は、ディスクアレイによって細部が異なります。一般的には、各セクションには次のような情報が保存されます。

- ディスクアレイに保持されている複製に関する情報は次のとおりです。
  - バックアップセッションID
  - バックアップセッションを実行した時間
  - バックアップセッションに使用されたバックアップ仕様の名称
  - セッションで作成されたターゲットボリュームの名称、ID、およびWWN
  - ***HPE P6000 EVA ディスクアレイファミリ:***ターゲットボリュームが存在するディスクアレイユニットの名前とID
  - ***HPE P6000 EVA ディスクアレイファミリ:***ターゲットボリュームの種類(標準スナップショット、Vsnap、またはスナップクローン)

- ホームに関する情報(CA+BC構成)
- バックアップセッションに使用したソースボリュームID
- インスタントリカバリにターゲットボリュームを使用できるかどうか(IRフラグ)
- ターゲットボリュームが削除可能かどうか(削除フラグ)
- セッションに関連するアプリケーションシステムおよびバックアップシステム

- 複製セットローテーションおよびその他の用途から除外されたディスクアレイボリューム。
- 追加の構成情報
  - ***HPE P6000 EVAディスクアレイファミリ:*** 定義されたディスクグループペア関係
  - ***HPE P9000 XPディスクアレイファミリ:*** 検出されたP9000 XPアレイコマンドデバイス
- ディスクアレイのセキュリティ関連の情報
- ***XPのみ:***ディスクへのZDBセッション中に計算されるCRC。
- ***XPのみ:***XPコマンドデバイスに関する情報。
- ***EVAのみ:***ディスクグループペアに関する情報。
- ***EVAのみ:***インスタントリカバリ後にソースボリューム上に残る情報。

この情報は、複製の作成時にZDBデータベースに書き込まれ、複製の削除時にZDBデータベースから削除されます。

ZDBデータベースに格納されるのは、バックアップ仕様で**[バックアップ後に複製を保持]**オプションが選択されているZDBセッションに関する情報だけです。このバックアップオプションを選択せずに実行されたテープへのZDBセッションで作成された複製は、バックアップ後にZDBデータベースから削除されます。

テープへのZDBセッションに関する情報と、ディスク/テープへのZDBセッションに関する情報の一部は、IDBの他の部分にも保存されます。

ZDBデータベースの各セクションとその用途の詳細については、『HPE Data Protector Zero Downtime Backup Administrator's Guide』を参照してください。

ユーザーインターフェース

ZDB処理およびIR処理の実行には、Data Protectorのグラフィカルユーザーインターフェイス(GUI)またはコマンドラインインターフェイス(CLI)を使用できます。

GUI

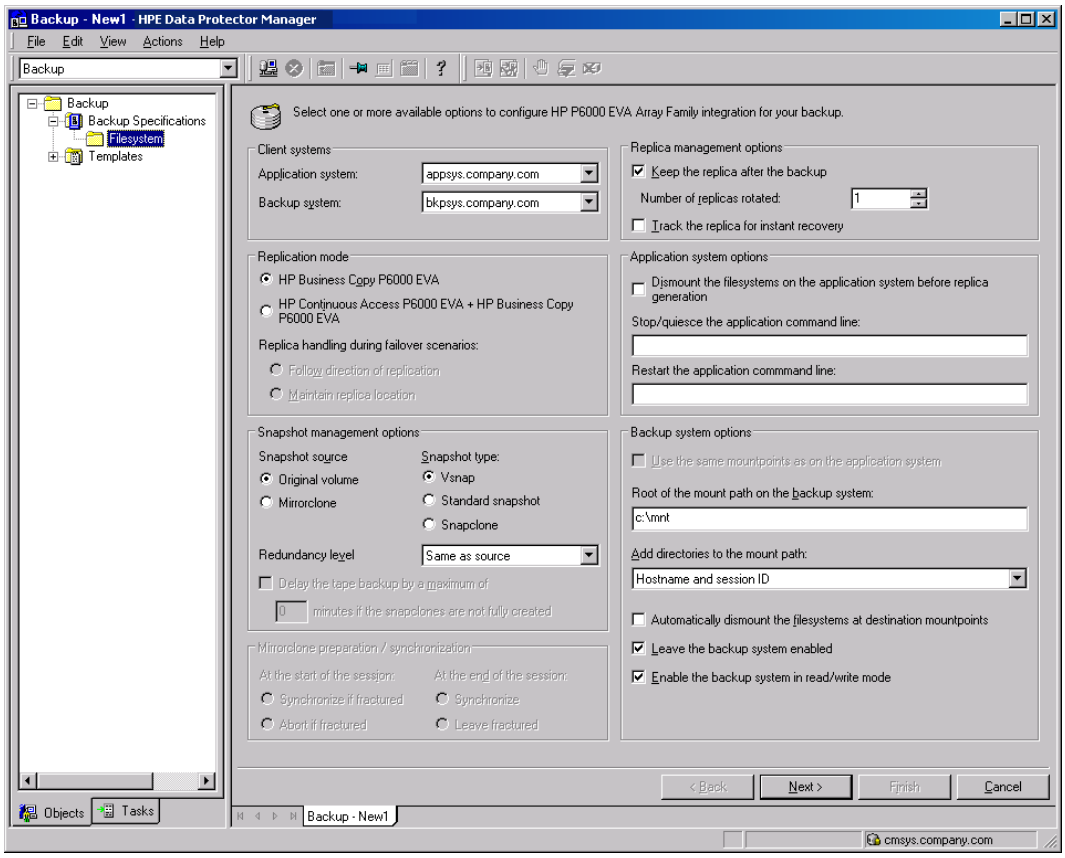
GUIを使用すると、1台のシステムでZDB環境を管理できます。実行できる内容は次のとおりです。

- ZDBのバックアップ仕様を作成してスケジュールし、ZDBセッションを開始する
- アクティブな処理を監視する
- Data Protectorのレポート機能と通知機能を使用する
- **[インスタントリカバリ]**コンテキストで、インスタントリカバリの対象としてマークされたセッションをブラウズして必要なオプションを定義し、インスタントリカバリセッションを開始する

- **[復元]**コンテキストで、バックアップメディアに保存されているセッションをブラウズして必要なオプションを定義し、Data Protectorの標準復元手順をテープから実行する

次の図はGUIウィンドウの例ですが、ここではP6000 EVAアレイで実行されているZDBセッションのバックアップオプションが選択されています。

Data Protector GUI



CLI

CLIでは、GUIで実行可能なZDB処理およびIR処理のほとんどを実行できます。また、次のような一部の管理タスクはCLIでのみ実行可能です。

- ZDBデータベースの照会、同期、削除
- ZDBデータベースの整合性チェック
- 不要になった複製または複製セットと、ZDBデータベースに保存されている関連情報の手動削除
- Data Protectorでの使用から複製を除外する、またはでの使用に複製を含める
- ***HPE P6000 EVA ディスクアレイファミリ:***ディスクグループペアの設定

使用可能なコマンドの詳細については、『HPE Data Protector Command Line Interface Reference』を参照してください。

Data Protectorで使用できるディスクアレイ統合ソフトウェア

Data Protectorでは、次の各種ディスクアレイを使用して複製を作成できるほか、ほとんどの場合、複製セットも作成することができます。

Data Protectorで使用できるディスクアレイ

複製の種類	サポートされているディスクアレイ	略称
スプリットミラー	HPE P9000 XPディスクアレイファミリ	P9000 XPアレイ
	EMC Symmetrix Disk Array	EMC
スナップショット	HPE P4000 SANソリューション	P4000 SANソリューション
	HPE P6000 EVAディスクアレイファミリ	P6000 EVAアレイ
	HPE P9000 XPディスクアレイファミリ	P9000 XPアレイ
	HPE 3PAR StoreServ Storage	3PAR StoreServ
	NetApp Storage	NetApp
	EMC VNXストレージファミリ	EMC VNX
	EMC VMAX Storage Family	EMC VMAX

HPEでサポートされる現時点での構成一覧は、https://softwaresupport.hpe.com/を参照してください。

HPE P4000 SANソリューション

HPE P4000 SANソリューションでは、スナップショットの作成がサポートされています。スナップショットは、「Redirect-On-Write」技術をベースにし、必要に応じて割り当てられるストレージ領域を使用します。このディスクアレイファミリでは、Data Protectorはローカル複製のみをサポートしています。

HPE P6000 EVAディスクアレイファミリ

Data ProtectorのP6000 EVAアレイ統合では、標準スナップショット、Vsnap、スナップクローンの作成がサポートされています。

Data ProtectorのP6000 EVAアレイ統合で可能な構成は、次のとおりです。

- ローカル複製
- LVMミラーと統合されるローカル複製
- リモートプラスローカル複製(データ保護は最高レベル)

P6000 EVAアレイの他の構成例については、サポートされている構成、ページ 280を参照してください。

P6000 EVAアレイストレージボリューム

P6000 EVAアレイでは、物理ディスクを**ディスクグループ**に編成する仮想化技術が採用されています。各ディスクグループはストレージプールとして機能し、そこから**仮想ディスク**が割り当てられます。1つの仮想ディスクが複数のディスクグループに属することはできませんが、1つのディスクグループ内の複数の物理ディスクにまたがることは可能です。物理ディスク上の仮想ディスクの配置を正確に指定することはできませんが、保護特性を選択することで制御できます。この場合は、RAID技術を使用して、データの冗長性、速度、アクセス時間をさまざまなレベルで設定します。

ローカル複製

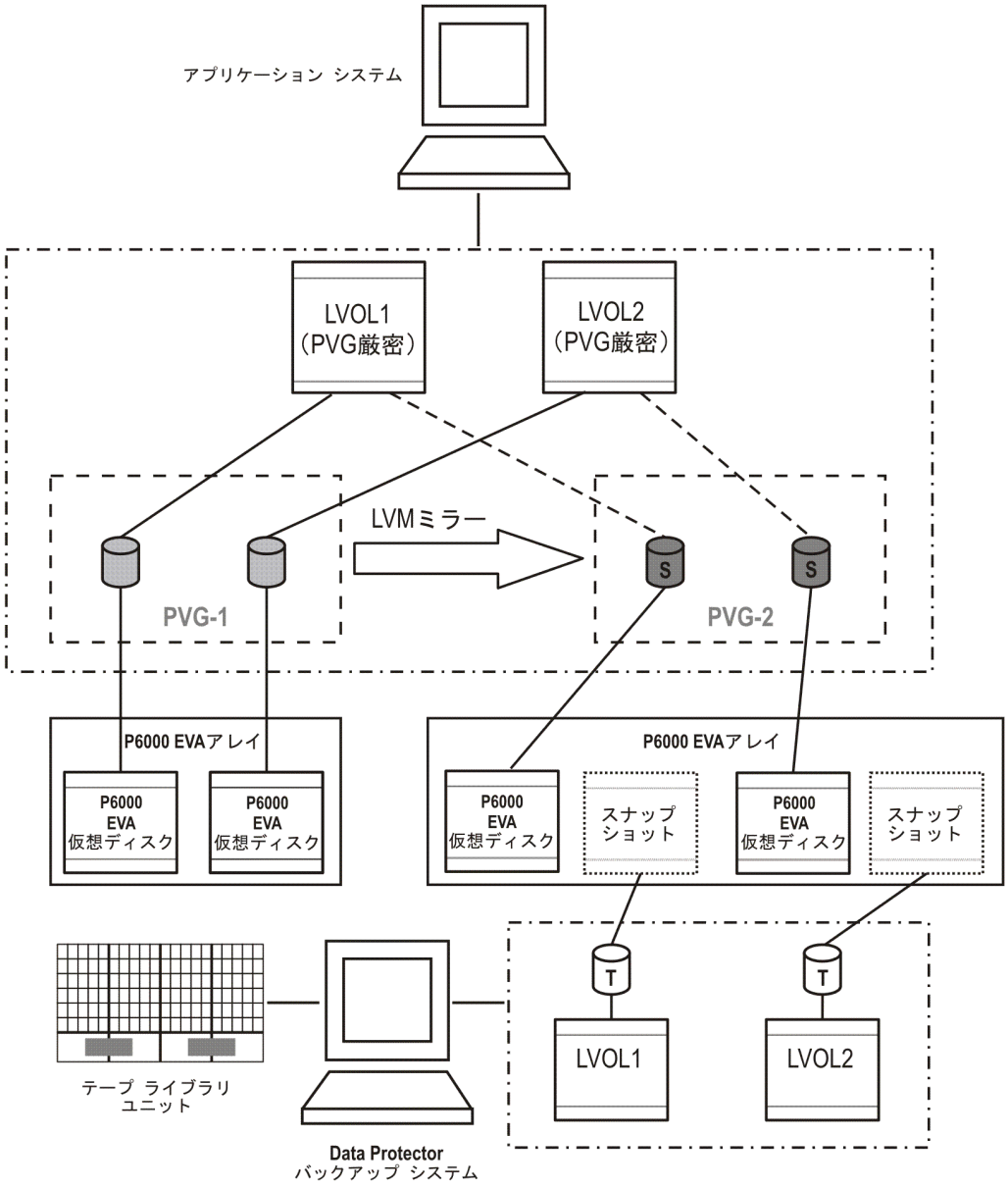
ローカル複製の場合は、**HPE Business Copy (BC) P6000 EVA configuration**構成を使用します。この構成を使用すると、使用されるスナップショットの種類に関係なく、インスタントリカバリに使用可能な複製を作成することができます。大規模な複製セットはディスクアレイに作成できます。標準スナップショットおよびvsnapによって構成される複製セット内の複製の最大数はP6000 EVAストレージシステムのファームウェアバージョンによって制限されますが、スナップクローンで構成される複製セット内の複製の最大数は、ディスクアレイの残りのストレージ容量によってのみ制限されます。

LVMミラーと統合されるローカル複製

Data ProtectorのP6000 EVAアレイ統合は、ボリュームグループが1つのP6000 EVAアレイ(または複数のP6000 EVAアレイユニット)から別の1つのP6000 EVAアレイ(または複数のP6000 EVAアレイユニット)にLVMミラー化される構成のLVMミラーをサポートしています。LVMミラー化されたソースボリュームとそのLVMミラーは同じ論理ボリュームに属します。

この構成では、物理的に別々のサイトにあるアレイが少なくとも2つは必要になります。

LVMミラー構成例 – P6000 EVAアレイの場合

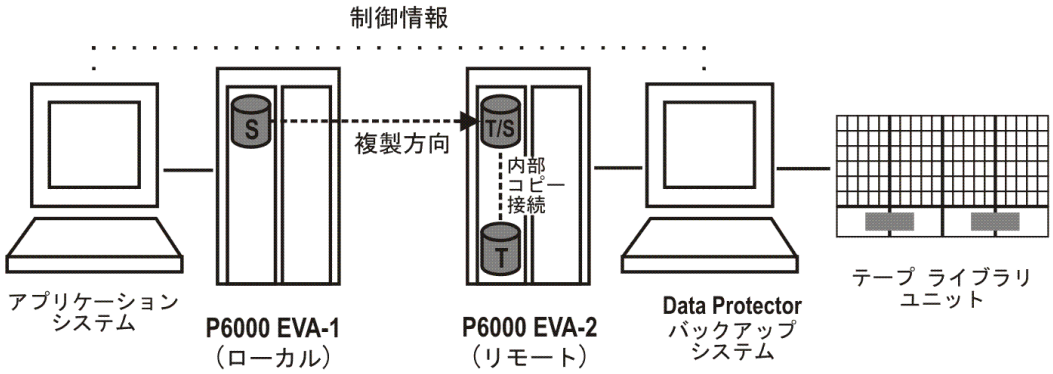


リモートプラスローカル複製

リモートプラスローカル複製には、HPE BC P6000 EVAとHPE Continuous Access (CA) P6000 EVAの組み合わせを使用します。この構成では、スナップショット複製をリモートマシン上に作成した後、この複製のローカル複製をリモートマシン上に作成できます。

この構成では、物理的に別々のサイトにあるアレイが少なくとも2つは必要になります。

HPE CA+BC P6000 EVA構成の例



HPE P9000 XPディスクアレイファミリ

Data ProtectorのP9000 XPアレイ統合で可能な構成は、次のとおりです。

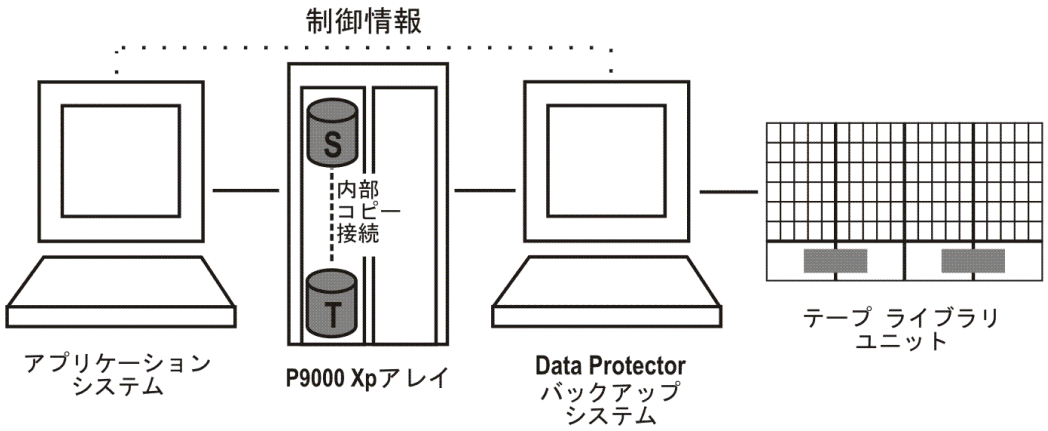
- ローカル複製
- LVMミラーと統合されるローカル複製
- リモート複製
- リモートプラスローカル複製(データ保護は最高レベル)

この場合は、ソースボリュームがアプリケーションシステムに接続され、別システムのバックアップシステムがターゲットボリューム用のディスクアレイに接続されます。複製からテープへのデータのストリーミングは、ミラーの分離後またはスナップショットの作成後に可能になります。この結果、バックアップ処理中もアプリケーションシステムはオンラインで使用可能な状態になっています。

ローカル複製

ローカル複製の場合は、**HPE** Business Copy (BC) P9000 XP構成を使用します。このため、インスタントリカバリ用の**ファーストレベルミラー**または**スナップショットストレージに使用されるボリューム**(複製セット)を作成することができます。

HPE BC P9000 XP構成の例

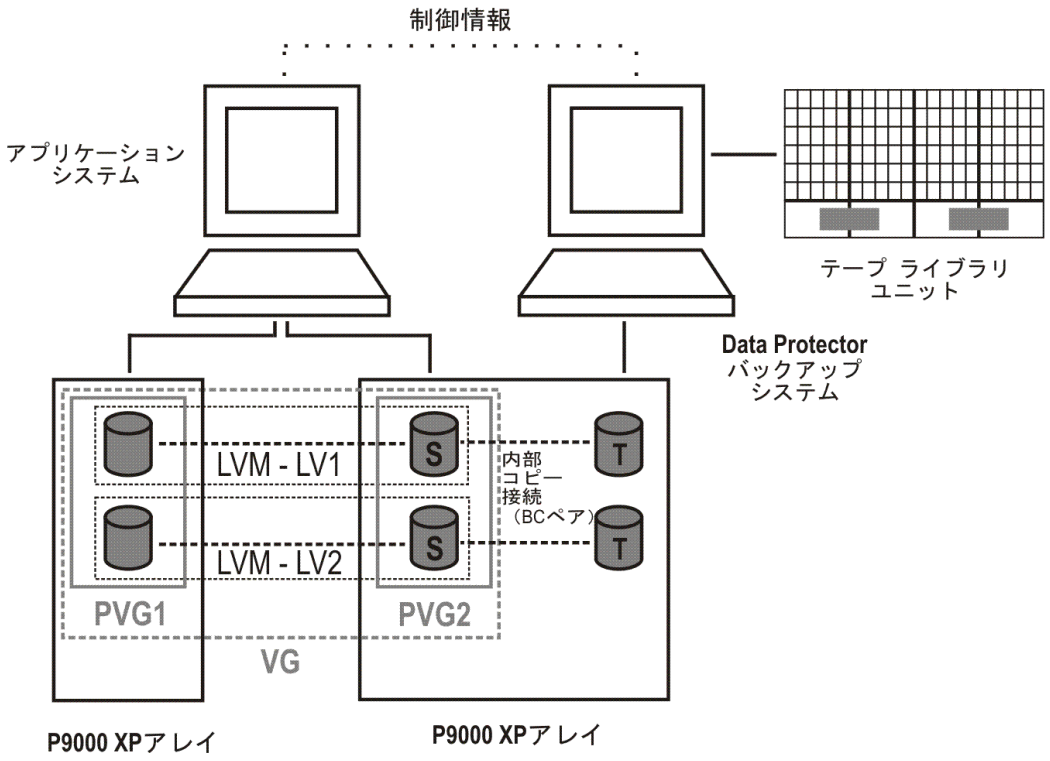


P9000 XPアレイの他の構成例については、サポートされているHPE P9000 XPディスクアレイファミリ構成、ページ 288を参照してください。

LVMミラーと統合されるローカル複製

Data Protector P9000 XPアレイ統合は、ある物理ディスク(LDEV)上の論理ボリュームから別の物理ディスク(LDEV)上の論理ボリュームへミラー化される構成で、HP-UX論理ボリュームマネージャーミラー(LVMミラー)をサポートしています。

LVMミラー構成例 – P9000 XPアレイの場合



リモート複製

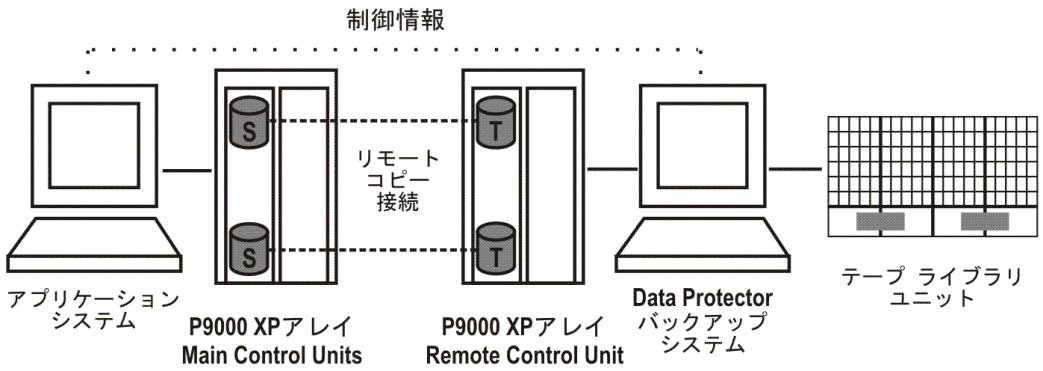
リモート複製の場合は、**HPE** Continuous Access (CA) P9000 XP構成を使用します。このため、遠く離れた場所にあるリモートシステムにリモートスプリットミラー複製を作成することができます。

HPE CA P9000 XPでは、次の2種類のインターフェイスがサポートされています。

- 拡張シリアルアダプター(ESCON): 遠隔用
- ファイバーチャネル(FC): 最大距離2km

シングルモードファイバマルチプレクサー内蔵のFCスイッチを使用することで、ファイバーチャネルの距離を伸ばすことができます。

HPE CA P9000 XP構成の例



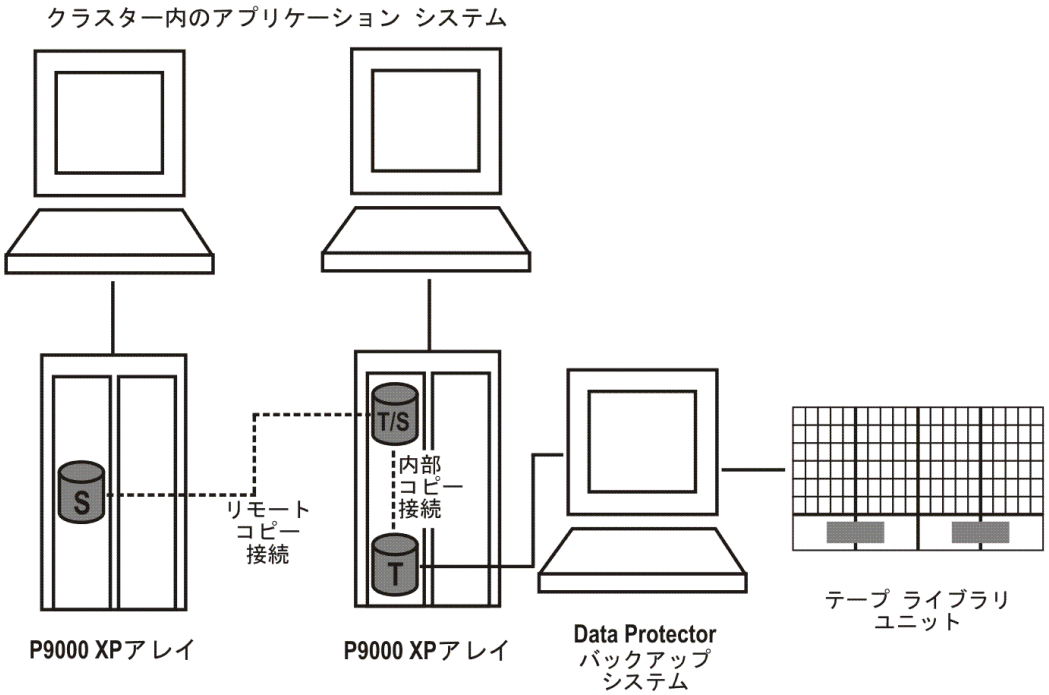
リモートプラスローカル複製

リモートプラスローカル複製には、HPE CA P9000 XPとHPE BC P9000 XP構成の組み合わせを使用します。このため、スプリットミラー複製をリモートシステムに作成した後、その複製のローカルスプリットミラー複製またはスナップショット複製をリモートシステムに作成できます。

物理的に別々のサイトに、サポートされているアレイが少なくとも2つは必要になります。

複製が必要になった時点で、統合ソフトウェアによってBCペアが分割されます。データの整合性を保つために、BCペアを分割する前にCAペアのステータスがチェックされます。これにより、メインコントロールユニットのすべてのデータがRemote Control Unitにも確実に保持されます。

クラスターでのHPE CA P9000 XP構成



クラスター構成の詳細については、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参照してください。

HPE 3PAR StoreServ Storage

HPE 3PAR StoreServ Storageではスナップショットの作成がサポートされています。スナップショットは「コピーオンライト」テクニックをベースとし、必要に応じて割り当てられるストレージスペースを使用します。このディスクアレイファミリでは、Data Protectorはローカル複製のみをサポートしています。

EMC Symmetrix

Data Protector EMC統合ソフトウェアを使用した場合は、次の構成が可能です。

- ローカル複製
- LVMミラーと統合されるローカル複製
- リモート複製
- リモートプラスローカル複製

この統合ソフトウェアを使用した場合は、テープへのZDBおよびスプリットミラー復元に使用できるスプリットミラー複製を1つ作成することができます。

> **注：**
> インスタントリカバリはサポートされていません。

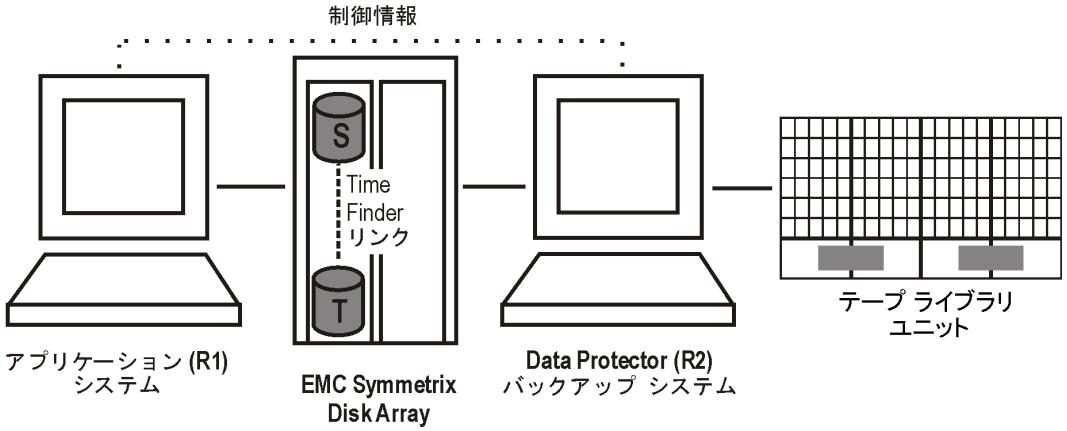
この場合は、ソースボリュームがアプリケーションシステムに接続され、別システムのバックアップシステムがターゲットボリューム用のディスクアレイに接続されます。複製からテープへのデータのストリーミングは、ペアを分割してから行われます。こうすることで、バックアップ処理中もアプリケーションシステムはオンラインで使用可能な状態になります。

EMC Symmetrix構成のその他の例については、サポートされているEMC Symmetrix構成、ページ 299を参照してください。

ローカル複製

ローカル複製の場合は、**EMC Symmetrix TimeFinder構成**を使用します。

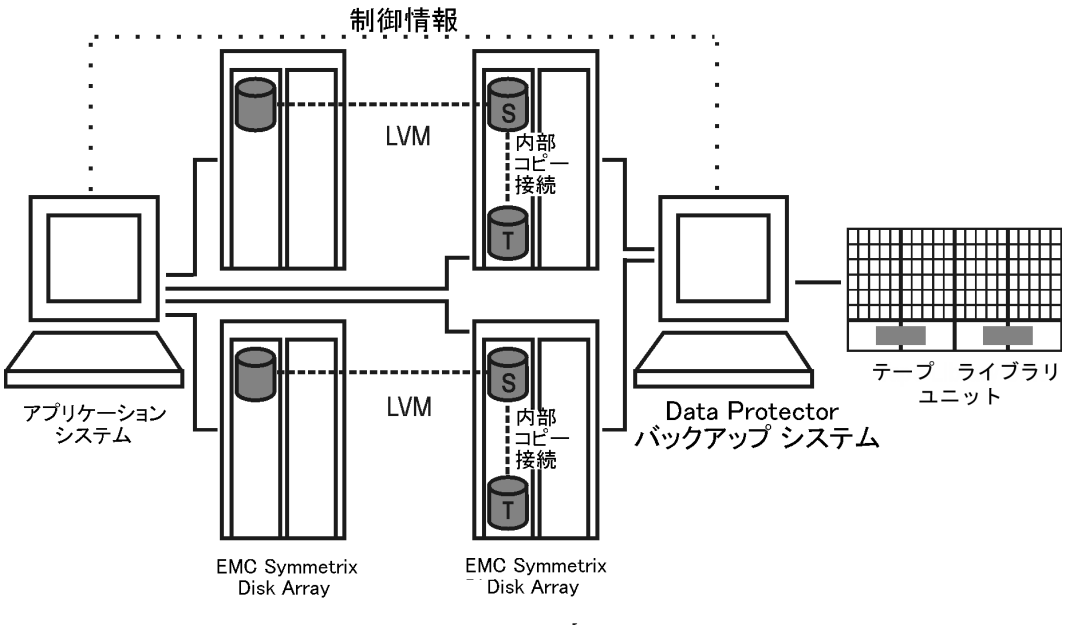
TimeFinder構成例



LVMミラーと統合されるローカル複製

Data Protector EMC統合では、ある物理ディスク上の論理ボリュームから別の物理ディスク上の論理ボリュームへミラー化される構成で、LVMミラーがサポートされています。

LVMミラー構成例 - EMCの場合



リモート複製

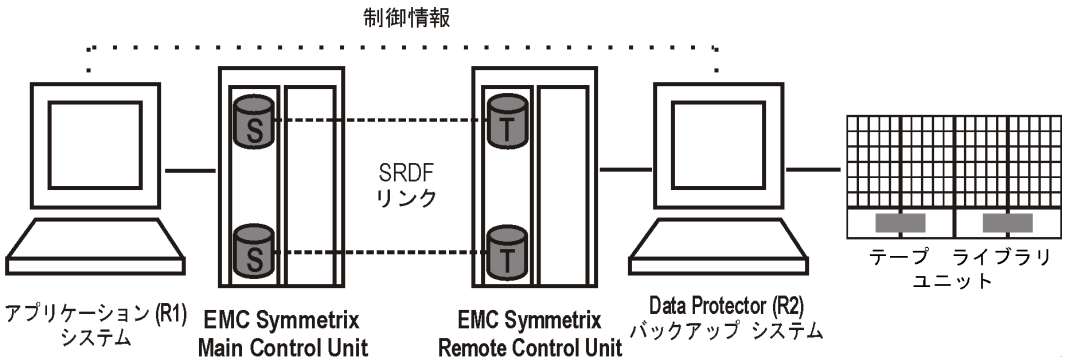
リモート複製には、EMC Symmetrix Remote Data Facility(SRDF)構成を使用します。このため、リモートシステムにスプリットミラー複製を作成できます。

制限事項

この環境では、クラスター構成はサポートされていません。

物理的に別々のサイトに、少なくとも2つのディスクアレイが必要になります。

SRDF構成例



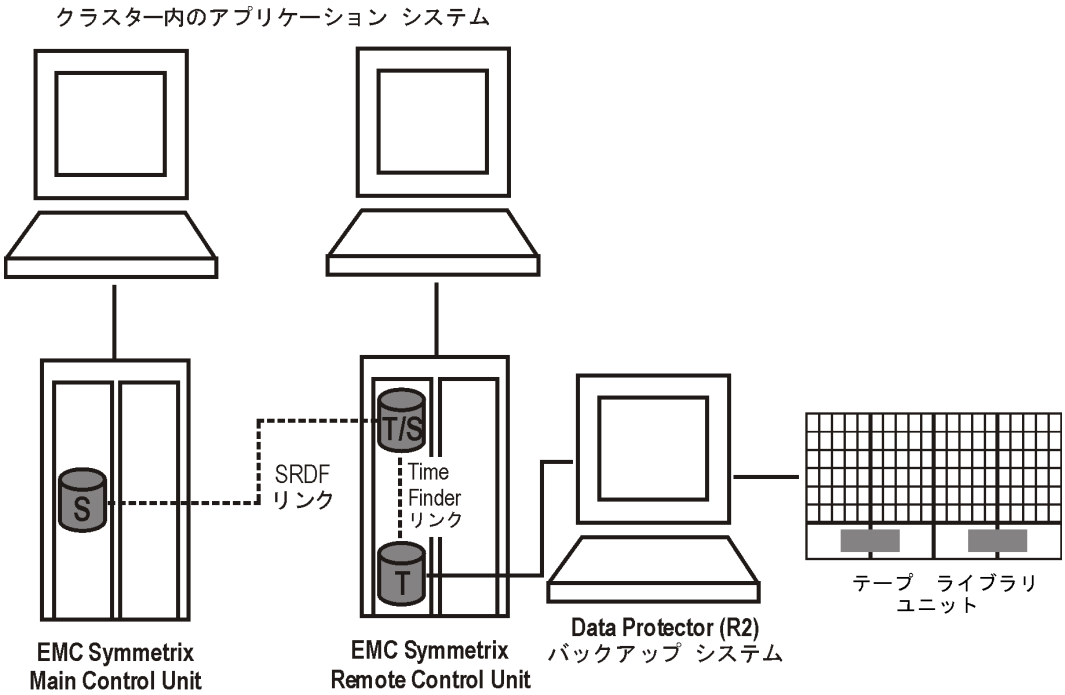
リモートプラスローカル複製

リモートプラスローカル複製には、SRDFとTimeFinder構成の組み合わせを使用します。このため、スプリットミラー複製をリモートシステムに作成した後、その複製のローカル複製をリモートシステムに作成できます。物理的に別々のサイトに、少なくとも2つのディスクアレイが必要になります。

複製が必要になった時点で、統合ソフトウェアによってTimeFinderペアが分割されます。データの整合性を保つために、TimeFinderペアを分割する前にSRDFペアのステータスがチェックされます。これにより、EMC Symmetrix Main Control Unitのすべてのデータが EMC Symmetrix Remote Control Unitにもあることが保証されます。

この構成は通常、リモートサイトがディザスタリカバリサイトの役割を担い、SRDFペアの分割が不可能な場合に使用します。

クラスターでSRDF構成とTimeFinder構成を併用した例

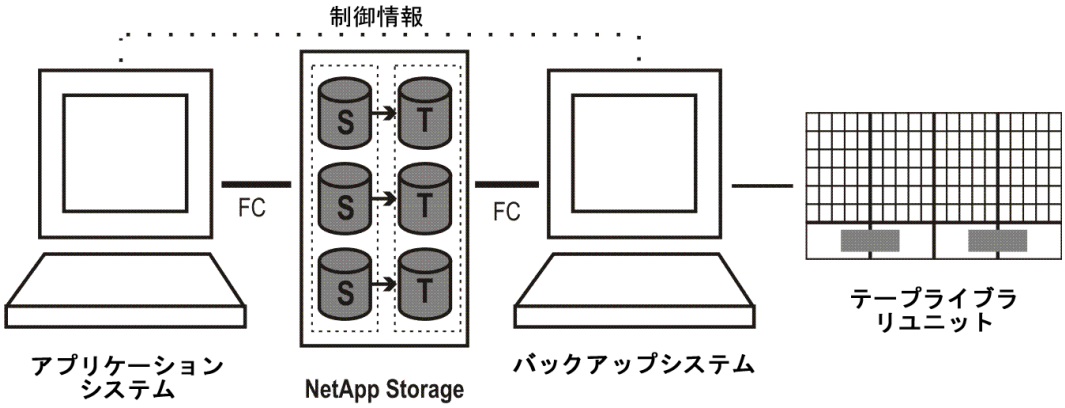


クラスター構成の詳細については、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参照してください。

NetApp Storage

NetApp Storageは、シンプロビジョニング(仮想スナップショット)タイプの複製の作成、および完全に割り当てられたプロビジョニングタイプの複製の作成をサポートします。NetApp Storageを使用する場合、Data Protectorがローカル複製のみをサポートします。

NetApp Storage構成例



EMC VNXストレージファミリ

EMC VNXストレージファミリは、シンプロビジョニングタイプの複製 (VNXスナップショット)の作成をサポートし、これは、「Redirect-On-Write」技術をベースにしています。EMC VNXストレージファミリでは、Data Protectorはローカル複製のみをサポートしています。

EMC VMAXストレージファミリ

EMC VNXストレージファミリは、ローカル複製の作成をサポートし、2種類のスナップショットがサポートされています:TimeFinder/クローンおよびTimeFinder VPスナップ。詳細については、EMC VMAXのドキュメントを参照してください。

アプリケーションの統合

Data Protectorでは、サポートされているディスクアレイについて、次のデータベースアプリケーションおよび複製の種類(オンラインまたはオフライン)との統合が可能です。

- Oracle – オンラインバックアップとオフラインバックアップ
- SAP R/3 – オンラインバックアップとオフラインバックアップ[1]

[1]EMC VNXおよびEMC VMAXストレージファミリではサポートされていません。

- Microsoft SQL Server – オンラインバックアップ
- Microsoft Exchange Server – ファイルシステムベースのオフラインバックアップ
- VMware仮想環境 – オンラインバックアップ[1]

また、Microsoft SQL ServerとMicrosoft Exchange ServerもData Protector Microsoft Volume Shadow Copy Service用統合ソフトウェアを通じてサポートされています。詳細は、『*HPE Data Protector Zero Downtime Backup Integration Guide*』を参照してください。

オンラインバックアップとオフラインバックアップの詳細については、「アプリケーションまたはデータベースの稼動のフリーズ」を参照してください。

Data Protectorでサポートされているあらゆるデータベースアプリケーションと仮想環境アプリケーションで、すべての複製方法(ローカル、リモート、リモートプラスローカル)を利用できます。ただし、すべてのアプリケーション統合ソフトウェアですべてのZDBエージェントやそのプラットフォームがサポートされているわけではありません。詳細については、最新のサポート一覧(https://softwaresupport.hpe.com/)を参照してください。

アプリケーションデータの整合性

論理ボリュームまたはディスクの単純なZDBでは、ファイルシステムの整合性のみ保証されますが、アプリケーションデータの整合性は保証されません。このようなバックアップのインスタントリカバリ後には、データベースは適切に復元されない可能性があります。サポートされている統合の場合、Data Protectorではアプリケーションがバックアップモードに設定されるか(オンラインバックアップの場合 – この期間中、アプリケーションが実行可能な操作が減少することもある)、シャットダウン(オフラインバックアップの場合)されますが、ユーザーはトランザクションログを別途バックアップする必要があります。非統合アプリケーションの場合、バックアップがデータベースリカバリのために使用できるようにする必要があります。アプリケーションをシャットダウンするか、または実行前スクリプトを使用して、適切なモードに設定します。

トランザクションログ

データベースアプリケーションをオンラインでバックアップする場合は、データベースを完全に復旧できるように、データベーストランザクションログのアーカイブを別途バックアップする必要があります。このトランザクションログは、同じゼロダウンタイムバックアップセッションで残りのデータベースデータとしてバックアップしないでください。

データベーストランザクションログのアーカイブは、ZDBセッションの後でData Protectorの通常のバックアップセッションを単独で実行する方法でのみ、ディスクまたはテープにバックアップできます。バックアップセッションを開始するスクリプトは、Data ProtectorのZDBバックアップ仕様の**[実行後]**オプションで指定することが可能です。この方法では、トランザクションログのバックアップは、複製の作成完了後に自動的に開始されます。

復元

サポートされている各種データベースアプリケーションで使用できる復元方法の詳細については、https://softwaresupport.hpe.com/のサポート一覧を参照してください。

[1]NetApp StorageおよびHPE 3PAR StoreServ Storageでサポートされています。

インスタントリカバリを使用すれば、複製が作成された時点の状態にデータベースを復旧することができます。ただし、ほとんどの場合、データベースを完全に復元するには、その後でトランザクションログを適用する必要があります。これらのログを使用すると、特定の時点まで、データベースをロールフォワードすることもできます。ZDBのバックアップ時間が短縮されれば、データベースの完全復旧時に適用されるアーカイブログファイルデータの量が小さくなります。

データベースアプリケーションでのData Protectorディスクアレイ統合ソフトウェアの使用方法の詳細については、『*HPE Data Protector Zero Downtime Backup Integration Guide*』を参照してください。

アプリケーションの統合とMicrosoftボリュームシャドウコピーサービス

従来のバックアップモデルでは、バックアップアプリケーションが、アプリケーションとバックアップシステム、およびディスクアレイといった、バックアッププロセスに含まれるさまざまなシステムとコンポーネントを調整します。これは、Data Protector HPE P9000 XPディスクアレイファミリ用とHPE P6000 EVAディスクアレイファミリ用の統合ソフトウェアにも当てはまります(HPE P9000 XPエージェントとHPE P6000 / HPE 3PAR SMI-Sエージェントがディスクアレイを制御し、Data Protector用統合ソフトウェアがデータベースアプリケーションとのやり取りを行います)。

Windowsシステムでは、統一されたバックアップ/復元サービスであるMicrosoftボリュームシャドウコピーサービス(**VSS**)が、バックアッププロセスに必要なコンポーネントを連動させます。VSSモデルにより、アプリケーション(**ライター**)およびディスクアレイ(**プロバイダー**)に標準化インターフェイスが提供されます。

ライターにより、アプリケーションとのやり取りが行われ、バックアップ可能な項目のリストが提供されます。また、ライターによってオペレーティングシステムレベルおよびアプリケーションレベルのデータの整合性が確保されます。

ハードウェアプロバイダーは、ディスクアレイエージェントに取って代わってその機能を実行しますが、Data Protectorから見ると、その動作はディスクアレイエージェントと同じです。

Data ProtectorのMicrosoftボリュームシャドウコピーサービス用統合ソフトウェアでのゼロダウンタイムバックアップセッションでバックアップしたデータのインスタントリカバリを実行するときは、Microsoft Virtual Disk Serviceまたはディスクアレイエージェントを使用することができます。ただし、使用できるかどうかは、バックアップを実行した方法にも依存します。

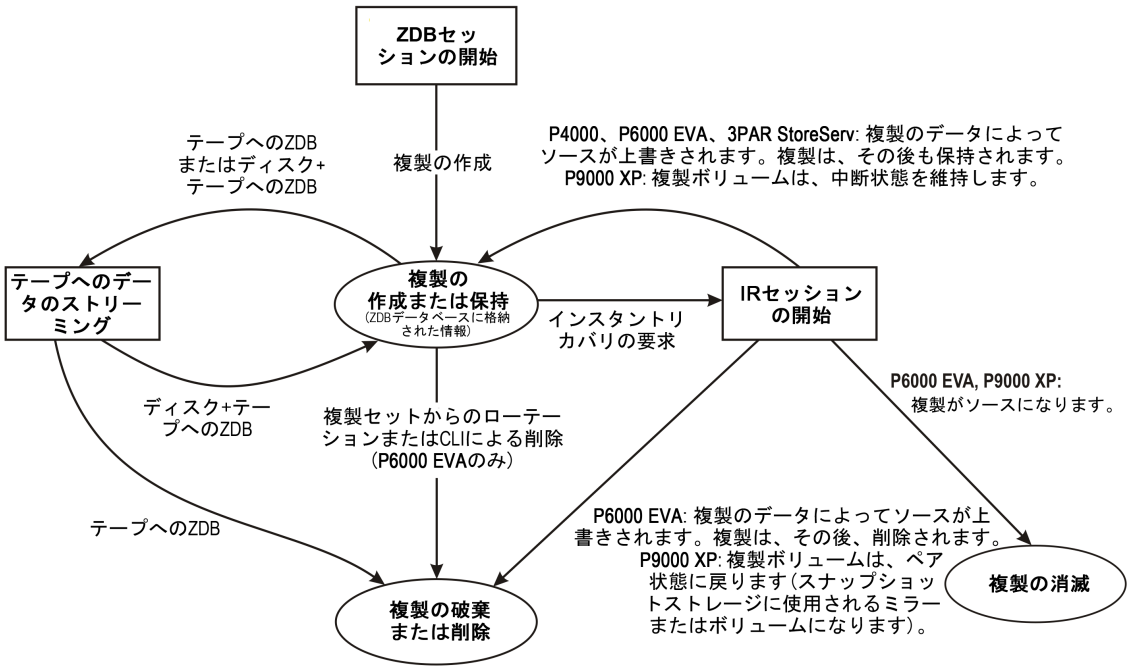
Data ProtectorのMicrosoftボリュームシャドウコピーサービス用統合ソフトウェアの使用方法の詳細については、『HPE Data Protector Zero Downtime Backup Integration Guide』を参照してください。

第12章: ZDB複製のライフサイクル

概要

この章では、複製のライフサイクルについて説明します。概要は、次の図に示しています。

複製のライフサイクル



複製のライフサイクルは次の要因によって決まります。

- ディスクアレイのモデル
- ZDBセッションおよびIRセッションに必要なData Protectorコンポーネント
- ゼロダウンタイムバックアップセッションに対して選択したオプション
- インスタントリカバリの方法(使用可能な方法から選択、または特定の復元の種類によって強制的に決定)
- インスタントリカバリセッションに対して選択した他のオプション

複製の作成

スプリットミラー複製技術とスナップショット複製技術では、基本的な考え方は同じです。どちらの技術でも、指定したデータオブジェクトを含めたストレージボリューム(ソースボリューム)のコピーまたはイメージを生成します。これらのコピーは、同じディスクアレイの別のストレージボリューム(ターゲットボリューム)に作成されて、ホストシステムがアクセスできる状態になります。

いずれの場合も、ディスクアレイのソースボリューム全体しか複製できません。複製のために選択されたデータがソースボリュームの小さなスペースのみを占めている場合でも、ソースボリューム全体が複製されます。

複製が作成されるZDBセッションは、バックアップ仕様によって定義されます。このバックアップ仕様には、**ZDBセッションの実行に必要な以下のすべての情報が含まれています。**

- バックアップ対象のアプリケーションまたはファイルシステムデータの種類
- バックアップ対象のソースデータ
- 作成される複製(または複製セット – 複製セットのローテーション、下参照)の種類
- データが格納されているディスクアレイの種類
- 使用するアプリケーションシステムとバックアップシステム
- 複製管理オプションと複製マウントオプション

Data Protectorと完全に統合されていないアプリケーションでは、複製前にアプリケーションを停止し、複製後にアプリケーションを再起動するというオプションも設定できます。

作成したバックアップ仕様はCell Managerに格納され、いつでも確認したり更新したりできます。

バックアップ仕様を作成したら、オペレーターがData Protectorのユーザーインターフェイスを使用してバックアップセッションを開始することも、指定した時刻に自動的に開始されるようにスケジューリングすることもできます。

> **注:**
> いくつかのデータベースアプリケーションでは、オンラインバックアップセッションが実行される場合、現在データベースで使用されているログファイルもバックアップする必要があります。これは、ログをファイルにバックアップすることによって行われます。これにより、必要に応じてこのファイルをテープにストリーミングすることが可能になります。
>
> 通常、ログファイルを複製対象のボリュームに含めることはお勧めしません。統合エージェントによっては、これを行うことはできません。また、一部の復元シナリオが削減または制限されるエージェントもあります。

バックアップが正常に終了すると、バックアップセッションの詳細がIDBのZDB関連部分に保存されます。

複製セット

複製セットとは、同じバックアップ仕様を使って異なる時点で作成された複製の集まりです。複製セットは、通常、インスタントリカバリの目的で複製を作成する際に、使用されます。複製セットに対して定義できる複製の最大数は、複製の種類、ディスクアレイのモデル、インストールされているディスクアレイのファームウェアのリビジョン、ターゲットボリュームに使用されているスナップショットの種類(スナップショット複製の場合のみ)の1つまたは複数の要因によって決まります。

Data Protectorでは、複製セットの各メンバーを、**複製セットローテーション**に従ってインタラクティブに使用したりスケジューラーで指定した時間に使用したりできます。特定のディスクアレイモデルは、複製セットのローテーションをサポートしない点に注意してください。

複製セットのローテーション

ZDBおよびインスタントリカバリに使用されるバックアップ仕様を作成する際には、複製セットの複製の最大数を指定する必要があります。バックアップが実行されるたびに、新しい複製が作成され、セットに追加されます。指定した最大複製数に達すると、作成される次の複製によって、セット内の最も古い複製が置き換えられます。複製の種類によっては、置き換えは最も古い複製を直接上書きして行われますが、それ以外の場合は新しい複製を作成する前に最も古い複製を削除する必要があります。

複製のスケジュール設定

複製セッションを自動的に実行する場合、バックアップ仕様の作成時または変更時に、Data Protectorの**スケジューラー**に詳細な必要回数を入力します。特定の時刻に1つのセッションをスケジューリングするか、日、週、月の期間に繰り返される通常セッションをスケジューリングすることができます。

複製の使用

作成した複製または複製セットの処理は、使用するZDBの形式によって異なります。

- ***テープへのZDB:***複製のデータをテープにストリーミングします。その後、複製は破棄されます。
- ***ディスクへのZDB:***インスタントリカバリ用に複製がディスクアレイで保持されます。
- ***ディスク+テープへのZDB:***複製のデータをテープにストリーミングした後、インスタントリカバリ用にその複製がディスクアレイで保持されます。

ディスクへのZDBセッションおよびディスク+テープへのZDBセッションの終了後、1つまたは複数の複製をディスクアレイで保持しておくことができます。複製セットのローテーションを行うと、同じバックアップ仕様を使用してさまざまな時点で作成された複製のセットを保持しておくことができます。この場合、新しい複製ができるたびに、セット内の最も古い複製がその新しい複製に置き換えられます。それぞれの複製は、一巡して複製セットから削除されるか、Data ProtectorのCLIを使用して削除するか、特定のインスタントリカバリの方法を使用してセッションで「消費」されるまで存在します。

テープへのZDB

テープへのZDBでは、通常、複製はディスクアレイに一時的に保存されるだけです。これにより、テープへのバックアッププロセスを段階的に効率よく行うことができます。

作成された複製はバックアップシステムにマウントされ、バックアップ仕様で指定されているバックアップオブジェクトがテープ(またはその他のバックアップメディア)にストリーミングされます。

バックアップの完了後、複製はバックアップには不要になるため、デフォルトでは自動的にディスクアレイから削除されます。ただし、同じバックアップ仕様を使用する今後のテープへのZDBセッションに備えて、ディスクアレイに複製を保存してディスクアレイのスペースを確保することもできます。この場合、バックアップ用の十分なスペースがディスクアレイに確保されます。

> **重要:**
> 複製は、インスタントリカバリには使用*できません*。

利点	欠点
バックアップおよびディザスタリカバリに適している	ディザスタリカバリの場合、高可用性システムの大規模なデータベースでは全セッションの復元に非常に時間がかかる可能性がある
個々のデータオブジェクトをテープバックアップから復元できる	
デフォルトでは、複製はディスクアレイから削除さ	インスタントリカバリは実行できない

利点	欠点
れ、スペースが解放される	
幅広いテープライブラリのサポート	

ディスクへのZDB

ディスクへのZDBの場合、複製はディスクアレイに保持され、インスタントリカバリのバックアップイメージとして使用されます。

複製は、ディスクアレイで1つまたは複数保持することができます。複製セットローテーションを使用して、異なる時点で作成された複製のセットを管理することができます。ここでは、新しい複製が、セット内の最も古い複製に置き換えられます。

利点	欠点
バックアップおよびインスタントリカバリに適している	複製用のディスクスペースが恒久的に必要になる
	テープへのZDBと比べて、ディスクアレイのサポートが限定されている

ディスク+テープへのZDB

ディスク+テープへのZDBとは、基本的にディスクへのZDBとテープへのZDBを組み合わせたものです。

複製は、ディスクへのZDBとまったく同じようにディスク上に作成され、次に、複製は、バックアップメディア以外のテープにストリーミングされます。ディスクの複製を保持し、テープへのZDBとは異なり、インスタントリカバリに使用することができます。

複製方法とディスクアレイのサポートは、ディスクへのZDBと同じです。

同じバックアップ仕様を使って、ディスクへのZDBセッションと同じスケジュールで、ディスク+テープへのZDBを指定することができます。つまり、同じバックアップ仕様を使って、ディスクへのZDBを1週間に6日実行し、ディスク+テープへのZDBを7日目に実行するなど、より高度なバックアップ管理を設定することができます。これにより、より融通性の高い復元が可能になります。同じ複製セットが、両方の種類のセッションに使用されることに、注意してください。

利点	欠点
バックアップおよびインスタントリカバリに適している	複製用のディスクスペースが恒久的に必要になる
個々のデータオブジェクトをテープバックアップから復元できる	テープへのZDBと比べて、ディスクアレイのサポートが限定されている

利点	欠点
ディスクへのZDBとディスク+テープへのZDBを高度に組み合わせることが可能	
テープを使用しながら、複製セットローテーションも使用できる	

インスタントリカバリ

ディスクへのZDBセッションまたはディスク+テープへのZDBセッションで作成された複製を使用すると、インスタントリカバリでデータオブジェクトを特定の時点の状態に復元することができます。プロセスの詳細については、インスタントリカバリ、ページ 267を参照してください。

インスタントリカバリセッションの後、複製がどうなるかは、ディスクアレイのモデル、選択した有効なインスタントリカバリの方法、インスタントリカバリに対して(GUIで)選択または(CLIで)指定した他のオプションによって決まります。

- HPE P4000 SANソリューションの場合、、復元複製のデータがソースボリュームにコピーされ、複製がディスクアレイに保持されます。ただし、インスタントリカバリ用に選択した各ターゲットボリュームでは、より新しいターゲットボリュームが同じソースボリュームに存在する場合、新しいターゲットボリュームは所属する複製セットに無関係に自動的にディスクアレイから削除されます。
- HPE P6000 EVAディスクアレイファミリの場合:
  - ディスクの切り換えによって、複製は、複製としての役割を終えます。
  - 複製データをソースボリュームにコピーすると、複製がディスクアレイに保持されます。
- HPE P9000 XPディスクアレイファミリの場合:
  - ディスクの切り換えによって(スプリットミラー復元の場合)、複製は、複製としての役割を終えます。
  - ソースボリュームを再同期する(スプリットミラー複製の場合)、またはデータをスナップショットからソースボリュームに復元する(スナップショット複製の場合):

    – Data Protector HPE P9000 XP Agentのみが使用される場合は、インスタントリカバリセッションに対して(GUIで)選択または(CLIで)指定したオプションによって、複製をディスクアレイに保持できるかどうかが決まります。

    – Data Protector MSボリュームシャドウコピー統合とData Protector HPEP9000 XP Agentが使用される場合は、複製はディスクアレイ上に保持されます。
- HPE 3PAR StoreServ Storageの場合は、複製のデータがソースボリュームにコピーされ、複製がディスクアレイに保持されます。

複製の削除

複製は、自動または手動で削除できます。

- *自動*
  - 複製が複製セットの最も古いメンバーになると、セット内に新しい複製が作成される際に自動的に上書き(または削除)されます。

    ただし、複製を使用対象から除外して保護することができます。詳細については、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参照してください。

  - テープへのZDBに使用される複製は、保持することを明示的に指定しない限り、セッションの終了後に自動的に削除されます。

  - 削除されるようにインスタントリカバリのオプションで指定した場合、複製はインスタントリカバリの終了後に削除されます。

  - 特定のインスタントリカバリの方法を使用するセッションの後、複製は、複製として使用されなくなることがあります。HPE P9000 XPディスクアレイファミリまたはHPE P6000 EVAディスクアレイファミリでは、ディスクを切り換える方式のインスタントリカバリを使用すると、複製は復旧済みのソースになり、複製としての役割を終えます。

  - HPE P4000 SANソリューションでは、同じソースボリュームについて作成されたターゲットボリュームがインスタントリカバリに使用されると、(複製全体ではなく)ターゲットボリュームが自動的にディスクアレイから削除されます。このようなターゲットボリュームは、別の複製セットに所属する場合であっても削除されます。新しいターゲットボリュームの自動削除は、ディスクアレイ自身により実行されます。

- *手動*

  Data Protectorで使用する必要がなくなったら、Data ProtectorのCLIを使用して複製をディスクアレイから削除できます。

第13章: ZDBセッションプロセス

ZDBプロセスの概要

従来のData Protectorのバックアップでは、バックアップセッション全体にわたって、つまりバックアップメディアへのデータのストリーミングが完了するまで、アプリケーションの動作は影響を受けます。Data Protectorのゼロダウンタイムバックアップでは、アプリケーションの動作が影響を受けるのは、複製が作成される間だけです。

ZDBプロセスの主な手順は次のとおりです。

1. バックアップ対象のデータオブジェクトを特定します。「データオブジェクトの特定」を参照してください。
2. アプリケーションデータベースの稼動をフリーズします。「アプリケーションまたはデータベースの稼動のフリーズ」を参照してください。
3. 指定のデータオブジェクトを含む複製を作成します。「複製の作成」を参照してください。
4. テープへのバックアップが必要な場合は、複製をテープにストリーミングします「複製からテープへのストリーミング」を参照してください。
5. インスタントリカバリを実行できるようにする場合は、セッションに関する情報を記録します。「セッション情報の記録」を参照してください。

データオブジェクトの特定

バックアップ対象のデータは、次のように特定され、準備されます。

1. Data Protectorは、アプリケーションシステムとバックアップシステムでプロセスを開始します。
2. バックアップセッションマネージャーによってZDBのバックアップ仕様が読み込まれ、アプリケーションシステム上のアプリケーション統合エージェントとディスクアレイエージェント、およびバックアップシステム上のディスクアレイエージェントに必要な命令が渡されます。

   アプリケーションシステムのZDBエージェントが、データオブジェクトから対応するファイルシステム(存在する場合)、ボリュームグループ(存在する場合)、基盤となっているストレージボリュームを特定します。これらのデータオブジェクトは、バックアップ仕様から直接取得されるか、サポートされているアプリケーション統合のいずれかから得られます。
3. アプリケーションシステムが準備され、データが整合性のある状態になります。オンラインバックアップの場合、データベースはそのままになります。オフラインバックアップでは、データベースはオフラインになります。ZDBオプションの**[複製生成前にアプリケーションシステム上のファイルシステムをアンマウントする]**(HPE P6000 EVAディスクアレイファミリ、HPE 3PAR StoreServ Storage、NetApp Storage、EMC VMAX Storage、EMC VNX Storage)または**[アプリケーションシステム上のファイルシステムをアンマウントする]**(HPE P9000 XPディスクアレイファミリ)が選択されている場合、関係するファイルシステムはアンマウントされます。

アプリケーションまたはデータベースの稼動のフリーズ

複製を作成する間は、アプリケーションの稼動または該当するデータベースのセクションをフリーズする必要があります。

アプリケーションデータベースまたはファイルシステムは、アプリケーション統合エージェントによって必要な状態に設定されます。「オフライン」複製の場合はすべてのデータベースの更新が停止し、「オンライン」複製の場合はすべてのデータベースの更新の経路がログファイルに変更されます。

- 複製を**オフライン**で行う場合、複製の作成中はデータベースがオフラインになり、すべてのファイルI/Oが停止します。このデータベースは、通常は、たとえば未適用のREDOログを適用するなどの方法で、整合性のある状態に戻されます。

  複製の作成にはほとんど時間はかかりませんが、その間アプリケーションはオフラインになるため、高可用性アプリケーションには適していません。
- 複製を**オンライン**で行う場合、複製の作成中は、データベースが**ホットバックアップモード**になります。このモードではデータベースはオンラインのままですが、データベースは更新されず、代わりにすべてのデータベースI/Oがトランザクションログファイルに転送されます。複製の作成が完了した後、データベースにトランザクションログファイルが適用され、最新の状態になります。

  この複製方法ではアプリケーションへの影響が最小限に抑えられるため、稼動状態を中断したくない場合には最適です。

これらの処理に関連する手順は、Data Protectorでサポートされているデータベースアプリケーションでは、バックアップ時に自動的に制御できます。また、その他のアプリケーションやファイルシステムのバックアップでも同様の動作をセットアップすることが可能です。この場合は、実行前オプションおよび実行後オプションを使用して、複製の前後にスクリプトが実行されるように指定します。

いずれの場合も、バックアッププロセスによってアプリケーションへの影響があるのは複製の作成時だけです。「オンライン」の場合は、データベース操作はまったく停止されず(ダウンタイムがゼロ)、パフォーマンスへの影響が最小限に抑えられます。主に、トランザクションログに書き込む必要のある情報の増加という影響に限られます。

オンラインバックアップとオフラインバックアップは、いずれもZDB複製技術を使用せずに、Data Protectorで使用することもできます。ただし、従来のテープバックアップの場合は、バックアップセッションの間、データベースをホットバックアップモードに設定するかオフラインにする必要があるため、アプリケーションおよびデータベースの稼動への影響は大きくなります。

複製の作成

1. 複製が作成されます。
2. アプリケーションシステムが動作を再開します。アンマウントされたファイルシステムは、すべて再マウントされます。

   オフラインバックアップの場合は、データベースをオンラインに戻して、通常の稼動を再開できます。

   オンラインバックアップの場合は、トランザクションログファイルと、複製の作成中にキャッシュされた情報がデータベースに適用されます。
3. バックアップシステム環境が複製のディスクおよびデータに合わせて準備されます。スキャンが行われ、新しいデバイスが検出されます。また、ボリュームグループがインポートされ、アクティブ化されます。さらに、ファイルシステムがマウントされます。

データオブジェクトの複製

データベースまたはファイルシステムが必要な状態になると、アプリケーションシステムおよびバックアップシステムのディスクアレイエージェントがトリガーされ、複製が実行されます。

2つのディスクアレイエージェントはペアとして機能します。

- アプリケーションシステムのエージェントによって、特定のデータがそのデータを含むボリュームに変換されます。
- バックアップシステムのエージェントによって、複製に必要なボリュームが割り当てられます。

次に、ディスクアレイにより、そのディスクに複製が作成されます。

複製方法は、使用されたディスクアレイの種類、ディスクアレイがローカル複製とリモート複製のどちらを対象として構成されているか、LVMミラーが必要かどうかなどによって異なります。スプリットミラーおよびスナップショットの複製の実行方法については、「複製技術」を参照してください。

複製からテープへのストリーミング

1. テープへのZDBおよびディスク+テープへのZDBでは、複製がテープへストリーミングされます。
2. バックアップシステムがクリアされます。また、ファイルシステムがアンマウントされます。さらに、新しいボリューム管理システムが非アクティブになり、削除されます。

テープへの複製のバックアップ

マウントポイントの作成

複製内のデータをテープやその他のバックアップメディアに移動するには、まず複製をバックアップシステムにマウントする必要があります。

Data Protectorでは、バックアップシステム上にマウントポイントが作成され、そのポイントに複製内のファイルシステムがマウントされます。このプロセスは、バックアップの対象がアプリケーション、ディスクイメージ、ファイルシステムのいずれかによって異なります。

テープへのデータの移動(標準)

バックアップ仕様の定義に従って、データオブジェクトがData Protector Media Agentを使用してテープにストリーミングされます。

Data Protectorテープ上のセッション情報とIDB内のセッション情報が従来のテープバックアップを実行した場合と同じになるよう、複製からではなくオリジナルの場所からデータオブジェクトを取得しているかのように、情報がテープに書き込まれます。これにより、テープへのZDBおよびディスク+テープへのZDBセッションのデータオブジェクトは、標準的な復元手順でアプリケーションシステムに直接格納できるようになります。

増分ZDB

増分ZDBは、ファイルシステムのテープへのZDBまたはディスク+テープへのZDBセッションであり、非ZDBの増分セッションで使用される条件と同じ増分バックアップData Protector条件を満たすファイルだけがテープにストリーミングされます。複製は、フルZDBセッションでも増分ZDBセッションでも同じ方法で作成されます。

Windowsシステムでは、**[アーカイブ属性を使用しない]**ファイルシステムオプションは増分ZDBの動作に影響します。このオプションが選択されていない場合は、増分バックアップを指定した場合でも、フルバック

アップが実行されます。このため、変更されていない可能性のあるファイルをバックアップしないようにするためには、ZDBバックアップ仕様の作成時にこのオプションを選択してください。

作成後の複製

複製の作成後は、以下のようになります。

- *ディスクへのZDB*および*ディスク+テープへのZDB*では、複製はインスタントリカバリ用にディスクアレイで保持されます。複製が複製セットに属している場合は、そのセットで最も古い複製になるまで、ディスクアレイで保持された後、同じバックアップ仕様を使用して実行された次回のディスクへのZDBセッションまたはディスク+テープへのZDBセッションで作成された複製に置き換えられます(複製が使用対象から除外されている場合を除く)。
- *テープへのZDB*セッションの後、データがテープにバックアップされたとき、デフォルトでは複製が自動的に削除されます。複製をディスクアレイに残しておくことは可能ですが、この複製はインスタントリカバリには使用できません。

ZDBオプションの詳細については、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参照してください。

バックアップシステムへの複製のマウント

Data Protectorは、バックアップシステムにマウントポイントを作成し、複製のファイルシステムをそのマウントポイントにマウントします。マウントポイントのパスは、アプリケーションまたはファイルシステムのバックアップが実行されているかどうかと、GUIで選択したバックアップ仕様のオプションによって異なります。また、ZDBセッションが完了した後もファイルシステムがマウントポイントのパスにマウントされた状態にしておくことを選択できます。

VSS統合では、GUIで選択したバックアップ仕様のオプションによって、マウントポイントがバックアップシステムに作成されるかどうかと、複製のファイルシステムが読み取り/書き込みモードと読み取り専用モードのどちらでマウントポイントのパスにマウントされるかが決まります。

セッション情報の記録

この段階で、作成した複製を次のセッションで再利用することができます。インスタントリカバリが有効になっている場合は、さらにIRセッション情報がIDBに保存され、IRが必要な場合に複製が保持されます。

IDBへのセッション情報の書き込み

Data Protectorの従来のバックアップと同様に、セッション全体にわたってIDBにZDBセッション情報(復元に使用できるバックアップメディアやデータオブジェクトに関する情報など)が書き込まれます。

- *ディスクへのZDB*および*ディスク+テープへのZDB*の場合は、複製に関するディスクアレイ固有の情報もインスタントリカバリ用にZDBデータベースに書き込まれます。
- *テープへのZDB*の場合は、複製をバックアップ後にディスクアレイで保持する場合でも、インスタントリカバリの情報はZDBデータベースに記録されません。

ZDBデータベースは、Cell ManagerのIDBの拡張です。ZDBデータベースには、Data ProtectorのZDBとIRに標準対応するディスクアレイごとに以下の独立したセクションがあります。

- HPE P6000 EVAディスクアレイファミリ、HPE 3PAR StoreServ Storageファミリ、NetApp Storage、EMC VMAX Storage、およびEMC VNX Storageのディスクアレイ用SMISDB
- HPE P9000 XPディスクアレイファミリのディスクアレイ用XPDB

情報は、複製の作成時にZDBデータベースに書き込まれ、複製の削除時にZDBデータベースから削除されます。

ZDBデータベースのセクションとその用途に関する詳細については、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参照してください。

第14章: インスタントリカバリおよびその他のZDBセッションからの復元技術

概要

インスタントリカバリでは、完全な複製をアプリケーションシステムへの影響を最小限に抑えながら高速で復元します。バックアップ仕様で指定されたデータオブジェクトに含まれるすべてのボリュームは、特定の時点の状態に戻ります。

ZDBセッションが終了すると、関連付けられている復元オブジェクトと復元セッションを次のGUIコンテキストで表示することができます。

- テープへのZDBまたはディスク+テープへのZDBの完了後、**[復元]**コンテキストで、テープからデータオブジェクトを復元できます。
- テープへのZDBまたはディスク+テープへのZDBの完了後、**[インスタントリカバリ]**コンテキストで、複製からの復元ができます。

また、Data ProtectorのCLIを使用する方法もあります。

復元の方法は、実行したZDBセッションの種類や、使用されているディスクアレイの種類によって異なります。以下の項では、復元に使用可能な方法について説明します。

インスタントリカバリ

利用できる処理

ローカルの複製:

- ディスクへのZDBからの復元
- ディスク+テープへのZDBからの復元

> **注:**
> EMCアレイ上では、インスタントリカバリはサポートされていません。テープへのZDBのみが可能です。

機能

完全な複製を、アプリケーションシステムへの影響を最小限に抑えながら高速で復元することができます。バックアップ仕様で指定されたデータオブジェクトに含まれるすべてのボリュームは、特定の時点の状態に戻ります。

詳細情報

「インスタントリカバリ」を参照してください。

さまざまな種類の複製が必要になるほか、ディスクアレイのいくつかの制限事項があるため、詳細な復元プロセスはディスクアレイの種類ごとに異なります。詳細については、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参照してください。

Data Protectorの標 準 復 元

利 用 できる処 理

ローカルおよびリモートの複 製:

- テープへのZDBからの復 元
- ディスク+テープへのZDBからの復 元

機 能

個 々 のバックアップオブジェクトを、テープからアプリケーションシステムに直 接 復 元 することができます。

標 準 復 元 が行 える対 象 は、実 際 にテープにストリーミングされた内 容 によって異 なります。つまり、テープへのZDBまたはディスク+テープへのZDBのバックアップ仕 様 に依 存 します。ソースボリュームの完 全 な内 容 がバックアップ仕 様 で選 択 された場 合 、すべてのオブジェクトがテープにストリーミングされます。そうでない場 合 は、ソースボリューム全 体 が複 製 される場 合 でも、選 択 されたバックアップオブジェクトだけがテープにストリーミングされます。

スプリットミラー復 元

> **注:**
> 最 新 のSANに接 続 された極 めて高 速 なテープドライブの速 度 であれば、アプリケーションシステムに直 接 復 元 するほうが、スプリットミラー復 元 よりも時 間 がかからないことがほとんどです。

利 用 できる処 理

特 定 のディスクアレイモデル上 にあるローカルの複 製:

- テープへのZDBからの復 元
- ディスク+テープへのZDBからの復 元

ディスクイメージ、ファイルシステム、およびファイルシステムベースのアプリケーションのバックアップに使 用 できます。

機 能

アプリケーションシステムへの影 響 を最 小 限 に抑 えて、個 々 のバックアップオブジェクトから複 製 全 体 の内 容 に至 るまで、任 意 のものを復 元 することができます。スプリットミラー復 元 を使 用 すると、部 分 的 に破 損 していながらも使 用 可 能 なシステムに対 して、影 響 度 が低 い復 元 を実 行 することができます。

スプリットミラー復 元 が行 える対 象 は、前 述 の標 準 復 元 と同 様 に、実 際 にテープにストリーミングされた内 容 によって異 なります。

詳 細 情 報

「スプリットミラー復 元 」を参 照 してください。

インスタントリカバリ

インスタントリカバリでは、失 われたデータや破 損したデータは、以 前 にディスクアレイの他 のボリュームに複 製 された既 存 の正 常 なデータで置 き換 えられます。以 前 に複 製 されたこのデータは、完 全 なストレージボリュームレベル上 で処 理 されます。その後 のプロセスは、復 元 されるアプリケーションによって異 なります。

- *ファイルシステム*が複 製 されている場 合 は、この手 順 のみで、複 製 が作 成 された時 点 の状 態 にデータを戻 すことができます。
- *データベースアプリケーション*では、インスタントリカバリの実 行 後 に、トランザクションログファイルの復 元 および適 用 など、データベースを完 全 に復 元 するための追 加 操 作 の実 行 が必 要 となる場 合 があります。この方 法 では、その時 点 のログファイルが存 在 する場 合 、複 製 の作 成 時 より後 の時 点 まで、データベースを復 元 できる可 能 性 があります(一 般 的 に**ロールフォワード**と呼 ばれています)。通 常 、これには別 の*バックアップメディア*や*バックアップデバイス*を使 用 する必 要 があります。詳 細 については、『*HPE Data Protector Zero Downtime Backup Integration Guide*』を参 照 してください。

インスタントリカバリでは、ソースボリュームに代 わってターゲットボリュームがシステムに提 示 されるか(このインスタントリカバリ方 法 はスナップクローンがある場 合 にのみ使 用 できます)、またはデータのコピー操 作 が実 行 され、ソースボリュームにあるデータがターゲットボリュームにあるデータによって置 き換 えられます。この処 理 はディスクアレイ内 部 で実 行 され、他 の*バックアップメディア*や*バックアップデバイス*を必 要 としません。このため、インスタントリカバリは非 常 に高 速 に実 行 されます。

Data Protectorのディスクアレイエージェントのみを使 用 するインスタントリカバリセッションでは、バックアップ仕 様 で指 定 されている*バックアップオブジェクト*を個 別 に指 定 して復 元 することはできず、インスタントリカバリの対 象 として*バックアップオブジェクト*セット全 体 しか選 択 できないので、復 元 できるのは複 製 全 体 のみです。また、LVMが構 成 されたUNIXシステムでは、複 製 を構 成 するボリュームが復 元 されるだけでなく、これらのボリュームが存 在 するボリュームグループ全 体 も複 製 の作 成 時 点 の状 態 に戻 ります。

Data ProtectorのMicrosoftボリュームシャドウコピーサービス用 統 合 ソフトウェアを使 用 するインスタントリカバリセッションでは、インスタントリカバリセッションに使 用 される各 ボリュームに格 納 されているすべての*バックアップオブジェクト*が選 択 されている限 り、*バックアップ仕 様* で指 定 されている*バックアップオブジェクト*をインスタントリカバリの対 象 として個 別 に選 択 することができます。復 元 されるのは、インスタントリカバリの対 象 として選 択 されているオブジェクトが存 在 するボリュームだけで、同 じボリュームグループの他 のボリュームはそのまま残 されます。

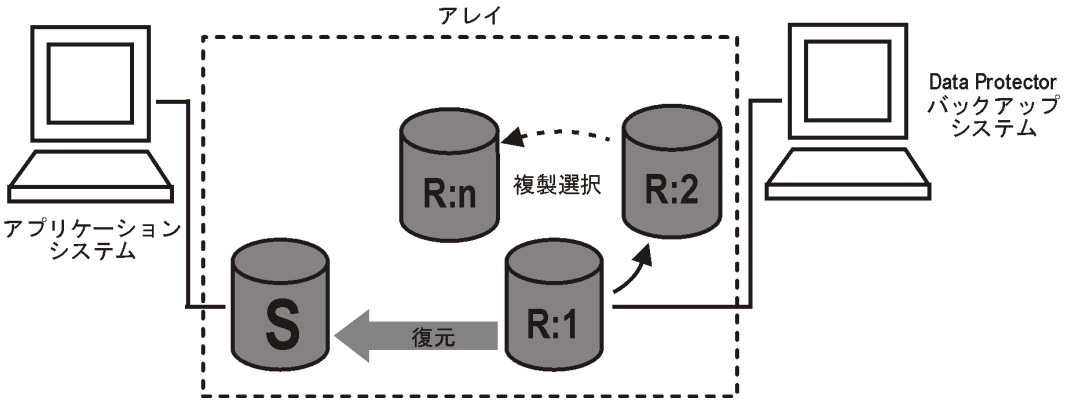
複 製 をData ProtectorのGUIで直 接 表 示 したり選 択 したりすることはできませんが、インスタントリカバリ用 に複 製 を作 成 したセッションを表 示 および選 択 することは可 能 です。

さまざまな種 類 の複 製 が必 要 なうえにディスクアレイのいくつかの制 限 事 項 があるため、復 元 プロセスの詳 細 はディスクアレイの種 類 ごとに異 なるほか、Data ProtectorのMicrosoftボリュームシャドウコピーサービス用 統 合 ソフトウェアが使 用 されるかどうかによっても異 なります。HPE P4000 SANソリューション、HPE P6000 EVAディスクアレイファミリ、HPE P9000 XPディスクアレイファミリ、HPE 3PAR StoreServ Storageの詳 細 については、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参 照 してください。Data ProtectorのMicrosoftボリュームシャドウコピーサービス用 統 合 ソフトウェアの詳 細 については、『*HPE Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*』を参 照 してください。

インスタントリカバリプロセス

インスタントリカバリの例 を次 に示 します。

インスタントリカバリの例



1. 復 元 する複 製 を決 定 し、その複 製 を作 成 したZDBセッションを選 択 します。
2. インスタントリカバリのオプションを選 択 します。これらは、主 にインスタントリカバリの方 法 とデータの安 全 レベルを選 択 するためのオプションです。

   これらのオプションにより、オペレーティングシステム、選 択 したインスタントリカバリ方 法 、ディスクアレイのモデルに応 じて以 下 のことが可 能 になります。

   - ***LVMが構 成 されたUNIXシステム:*** インスタントリカバリに使 用 されるボリュームグループの構 成 が、復 元 対 象 の複 製 の作 成 後 に変 更 されていないかどうかを確 認 できます。

     このチェックによって、復 元 対 象 の複 製 内 のデータに対 して実 行 されたCRCが、複 製 の作 成 時 点 のCRCと一 致 しているかどうかも確 認 できます。

   - 特 定 のインスタントリカバリの方 法 では、データを復 元 した後 のいずれかの手 順 で問 題 が発 生 したときのために、インスタントリカバリセッション後 もディスクアレイで複 製 を保 持 することができます。

   - ***HPE P6000 EVA ディスクアレイファミリ:*** バックアップシステム以 外 のシステムが複 製 にアクセスできないようにすることができます。

3. 必 要 に応 じて、さらに安 全 を期 すためにインスタントリカバリセッションのプレビューを実 行 できます。

   > **注 :**
   > Data ProtectorのMicrosoftボリュームシャドウコピーサービス用 統 合 ソフトウェアを使 用 するインスタントリカバリセッションでは、インスタントリカバリのプレビューを使 用 することはできません。

4. インスタントリカバリを開 始 します。

その後 、Data Protectorでは次 の処 理 が行 われます。

1. アプリケーションシステムとバックアップシステムで処 理 が開 始 されます。
2. IDBからセッション情 報 が抽 出 され、さらにZDBデータベースからセッションに関 連 するアレイ固 有 の情 報 が抽 出 されます。
3. 必 要 なチェックが実 行 され、インスタントリカバリを正 常 に実 行 するために必 要 な条 件 がすべて満 たされていることが検 証 されます(指 定 したインスタントリカバリのオプションも検 証 されます)。
4. いずれかのボリュームグループを(LVMが構 成 されたUNIXシステムで)非 アクティブ化 してアプリケーションシステムが準 備 され、複 製 に関 連 付 けられているすべてのファイルシステムがアンマウントされます。
5. 元 のデータが復 元 されます。

ディスクアレイのモデル、インスタントリカバリの方 法 (使 用 可 能 な 方 法 から選 択 するか、特 定 の複 製 の種 類 によって強 制 的 に決 まります)、インスタントリカバリセッションに対 して選 択 する他 のオプション に応 じて、以 下 のインスタントリカバリの方 法 を使 用 することができます。

- HPE P4000 SANソリューションでは、以 下 の1つのインスタントリカバリの方 法 だけが使 用 可 能 で す。
  - 複 製 データをソースボリュームにコピーする

    複 製 のデータが元 のストレージにコピーされ、ソースボリュームは保 持 されません。複 製 は保 持 されますが、インスタントリカバリに対 して選 択 した複 製 よりも新 しい複 製 が複 製 セットに存 在 する場 合 は、その新 しい複 製 がディスクアレイから削 除 されます。

    この方 法 では、Data ProtectorのMicrosoftボリュームシャドウコピーサービス用 統 合 ソフトウェ アとData Protector HPE P4000 Agentとが使 用 されます。

- HPE P6000 EVAディスクアレイファミリでは、次 の2つのインスタントリカバリの方 法 が使 用 可 能 で す。
  - ディスクを切 り替 える

    選 択 したスナップクローン複 製 がオリジナルのソースボリュームに置 き換 えられます。オリジナル のソースボリュームに対 して作 成 されたすべてのホストプレゼンテーションは、実 質 的 に新 しい ソースボリュームとなる、復 元 されたスナップクローンボリュームに対 して作 成 されます。Data Protectorの場 合 、スナップクローン複 製 は関 連 する複 製 セットから削 除 されます。インスタン トリカバリをもう一 度 実 行 することはできません。古 いソースボリュームを保 持 することも削 除 す ることも可 能 です。

    この方 法 では、ゼロダウンタイムバックアップセッションで使 用 されるData Protectorコンポーネン トに応 じて、Data Protector HPE P6000 / HPE 3PAR SMI-S Agentのみが使 用 されるか、 Data ProtectorのMicrosoftボリュームシャドウコピーサービス用 統 合 ソフトウェアとMicrosoft Virtual Disk Serviceとが使 用 されます。
  - 複 製 データをソースボリュームにコピーする

    複 製 からのデータが元 のストレージにコピーされます。ソースボリュームを保 持 することも保 持 しないことも可 能 です。

    ソースボリュームを保 持 する場 合 、プロセスはターゲットボリュームに使 用 されているスナップ ショットの種 類 によって異 なります。

    – ターゲットボリュームが標 準 スナップショットまたはvsnapの場 合 、まず同 じディスクグループ内 にソースボリュームの新 しいスナップショットが作 成 され、その後 に既 存 の複 製 からのデータが ソースボリュームに復 元 されます。元 のデータは、新 しく作 成 されたスナップショットに保 持 され ます。

    – ターゲットボリュームがスナップクローンの場 合 、まずソースボリュームのディスクグループ内 にコ ンテナーが作 成 され、次 に既 存 の複 製 からのデータがコンテナーに復 元 され、最 後 にソースボ リュームがコンテナーと共 に切 り替 えられます。

    ソースボリュームを保 持 しないことを選 択 すると、事 前 の処 理 を実 行 せずに既 存 の複 製 から のデータがソースボリュームに復 元 されます。

    この方 法 では、ゼロダウンタイムバックアップセッションで使 用 されるData Protectorコンポーネン トに応 じて、Data Protector HPE P6000 / HPE 3PAR SMI-S Agentのみが使 用 されるか、 Data ProtectorのMicrosoftボリュームシャドウコピーサービス用 統 合 ソフトウェアとData Protector HPE P6000 / HPE 3PAR SMI-S Agentとが使 用 されます。

- HPE P9000 XPディスクアレイファミリでは、次 の2つのインスタントリカバリの方 法 が使 用 可 能 で す。
  - ディスクを切り替 える

    選 択したスプリットミラー複 製 が元 のソースボリュームで置 き換 えられます。オリジナルのソース ボリュームに対 して作 成 されたすべてのホストプレゼンテーションは、実 質 的 に新 しいソースボ リュームとなる、復 元 された複 製 ボリュームに対 して作 成 されます。Data Protectorの場 合 、 複 製 は関 連 する複 製 セットから削 除 されます。インスタントリカバリをもう一 度 実 行 することは できません。古 いソースボリュームを保 持 することも削 除 することも可 能 です。

    この方 法 では、Data ProtectorのMicrosoftボリュームシャドウコピーサービス用 統 合 ソフトウェ アとMicrosoft Virtual Disk Serviceとが使 用 されます。
  - ソースボリュームを(スプリットミラー複 製 を使 用 して)再 同 期 するか、データを(スナップショット複 製 を使 用 して)スナップショットからソースボリュームに復 元 する。

    スプリットミラー複 製 を使 用 すると、ソースボリュームは選 択 した複 製 のボリュームに再 同 期 さ れます。スナップショット複 製 を使 用 する場 合 は、選 択 した複 製 のデータがソースボリュームに コピーされます。

    この方 法 では、ゼロダウンタイムバックアップセッションで使 用 されるData Protectorコンポーネン トに応 じて、Data Protector HPE P9000 XP Agentのみが使 用 されるか、Data Protectorの Microsoftボリュームシャドウコピーサービス用 統 合 ソフトウェアとHPE P9000 XP Agentとが使 用 されます。

- HPE 3PAR StoreServ Storageでは、以 下 の1つのインスタントリカバリの方 法 だけが使 用 可 能 で す。
  - 複 製 データをソースボリュームにコピーする

    複 製 のデータが元 のストレージにコピーされ、ソースボリュームは保 持 されません。複 製 は関 連 する複 製 セット内 に保 持 されます。

    この方 法 では、HPE 6000とHPE 3PAR SMI-S Agentのいずれか、またはData Protectorの Microsoftボリュームシャドウコピーサービス用 統 合 ソフトウェアとData Protector HPE 3PAR VSS Agentの両 方 を使 用 できます。

6. 無 効 化 されていたすべてのボリュームグループが再 度 有 効 化 され、アンマウントされていたすべての ファイルシステムが再 マウントされます。

インスタントリカバリの完 了 後 、ソースボリュームの内 容 は複 製 が作 成 された時 点 の状 態 に戻 ります。

インスタントリカバリとLVMミラー

LVMミラーと、HPE BC P6000 EVA構 成 またはHPE BC P9000 XP構 成 とを使 用 してHP-UXシステムで 実 行 されたZDBセッションのインスタントリカバリがサポートされています。ただし、追 加 で手 動 の手 順 を実 行 する必 要 があります。詳 細 については、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参 照 してください。

クラスターでのインスタントリカバリ

インスタントリカバリは、アプリケーションシステム上 のクラスター環 境 で実 行 されているアプリケーションまた はファイルシステムでサポートされます。ただし、実 行 する必 要 がある手 順 が増 えます。詳 細 について は、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参 照 してください。VSS統

合 に固 有 の情 報 については、『*HPE Data Protector Zero Downtime Backup Integration Guide*』を参 照 してください。

スプリットミラー復 元

> **注 :**
> 最 新 のSANに接 続 されたテープドライブの速 度 であれば、アプリケーションシステムに直 接 復 元 す るほうが、スプリットミラー復 元 よりも時 間 がかからないことがほとんどです。

スプリットミラー復 元 では、まずバックアップシステムでバックアップオブジェクト がテープから複 製 (既 存 の複 製 または復 元 用 に新 しく作 成 された複 製)に移 動 されます。次 に、アプリケーションシステムが使 用 可 能 な ソースボリュームに複 製 のデータが復 元 され、ソースボリュームの既 存 の内 容 が事 実 上 置 き換 えられま す。この複 製 は、完 全 なセッションまたは個 々 のバックアップオブジェクトの復 元 に使 用 することができます。

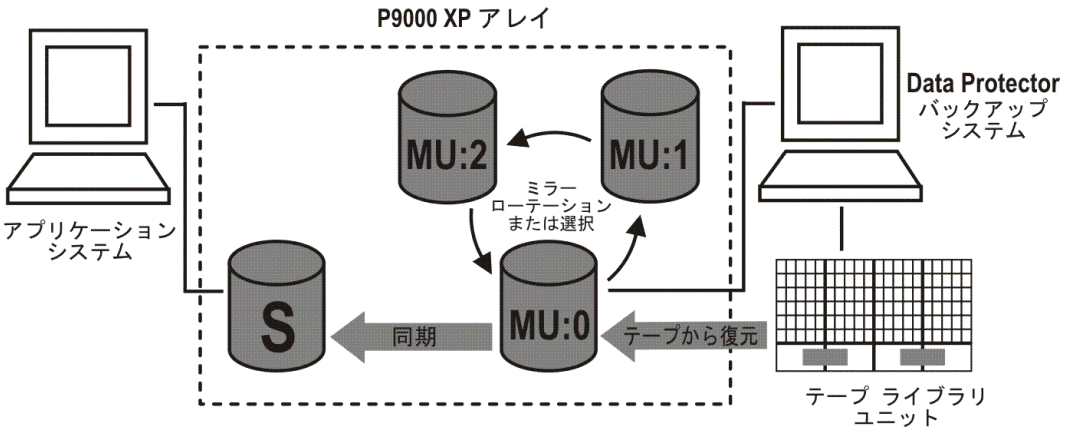
この方 法 は、テープへのZDBセッションまたはディスク+テープへのZDBセッションにより以 下 の条 件 で作 成 さ れたファイルシステムおよびディスクイメージからのデータの復 元 に使 用 できます。

- P9000 XPアレイでHPE Business Copy (BC) P9000 XP構 成 を使 用 している場 合 。
- EMCでSymmetrix TimeFinder構 成 、SRDF構 成 、またはその組 み合 わせ(SRDF+TimeFinder)の構 成 を使 用 している場 合 。

スプリットミラー復 元 のプロセス

P9000 XPアレイでのスプリットミラー復 元 のプロセスの例 を以 下 に示 します。

スプリットミラー復 元 の例



1. 復 元 に使 用 する複 製 を選 択 するか、ソースボリュームの最 新 の複 製 となる新 しい複 製 を作 成 しま す。
2. バックアップシステムを通 じて、必 要 なオブジェクトをテープから複 製 に復 元 します。
3. 複 製 からデータを復 元 します。事 実 上 、ソースボリューム上 のデータが、複 製 に格 納 されているデー タで置 き換 えられます。

処 理 が完 了 すると、以 下 のように、選 択 した複 製 の内 容 でソースボリュームの内 容 が置 き換 えられてい ます。

- テープから複 製 に復 元 されたバックアップオブジェクトは、ZDBセッションが実 行 された時 点 の状 態 に戻 ります。
- 残りの内 容 は、複 製 作 成 時 点 の状 態 に戻 ります。

第15章: ZDBの計画

概要

ZDB戦略の計画を行う際は、以下の手順を考慮に入れる必要があります。

1. 次のようなバックアップの要件と制限事項を定義します。
   - バックアップを実行する頻度。
   - バックアップデータを別のメディアセットにコピーする必要があるかどうか。
2. ディスクアレイのパフォーマンスに影響を及ぼす要因を把握します。
3. バックアップの概念とその実装方法をサポートするバックアップ戦略を準備します。

この章では、バックアップソリューションの計画およびZDBパフォーマンスの向上に役立つ重要な情報および留意事項について説明します。

復旧の柔軟性

特定の時点への復旧を柔軟に行えるようにするには、以下の点に留意する必要があります。

- 複製を定期的に作成し、ディスクアレイに保存しておく。
- ログファイルを定期的にバックアップする。

ディスクアレイのスペースの使用量を管理するために、以下の作業を行います。

- スケジュールを設定したZDBバックアップセッションに基づいてバックアップポリシーを定義して、それぞれが特定の時点に対応する、時系列順の複製を設定します。このような複製セットの複製の数は、ディスクアレイの空き容量と必要な時間範囲によって決まります。

  特定の種類のスナップショット複製では、ディスクアレイのモデルやインストールされているディスクアレイのファームウェアリビジョンによってセットの複製の最大数が制限されることがあります。
- ***HPE P6000 EVAディスクアレイファミリ:*** 適切なスナップショットの種類を選択します。

スプリットミラーディスクアレイ

HPE P9000 XPディスクアレイファミリ統合ソフトウェアおよびEMC Symmetrix Disk Array統合ソフトウェアには、バックアップポリシーを定義できる以下のオプションが用意されています。

- オリジナルデータのミラーコピーをテープに移動する。
- ミラーを分割した状態に保つか、または再同期する。
- 次のバックアップに使用するディスクを準備する。

バックアップポリシーの例については、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参照してください。

この章では、スプリットミラーディスクアレイのパフォーマンスに関する一般的な推奨事項と制限事項を紹介します。

スナップショット ディスクアレイ

Data ProtectorのHPE P4000 SANソリューション統合を使用する場合は、バックアップ方針を策定するときに以下の事項を考慮してください。

- インスタントリカバリ - ディスクアレイ固有の考慮事項、次のページを参照してください。

Data ProtectorのHPE P6000 EVAディスクアレイファミリ統合を使用する場合は、バックアップ方針を策定するときに以下の事項を考慮してください。

- スナップショットの種類(標準スナップショット、vsnap、スナップクローン)
- 複製の冗長レベル - 『HPE Data Protector Zero Downtime Backup Administrator's Guide』を参照してください。
- 他のディスクアレイに固有の考慮事項 - 参照情報 ディスクアレイ固有の考慮事項、次のページ
- インスタントリカバリ - ディスクアレイ固有の考慮事項、次のページおよび『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参照してください。

Data ProtectorのHPE P9000 XPディスクアレイファミリ統合を使用する場合は、バックアップ方針を策定するときに以下の事項を考慮してください。

- 複製の種類(スプリットミラーまたはスナップショット) - 参照情報 ディスクアレイ固有の考慮事項、次のページ
- インスタントリカバリ - ディスクアレイ固有の考慮事項、次のページおよび『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参照してください。

Data ProtectorのHPE 3PAR StoreServ Storage用統合ソフトウェアを使用する場合は、バックアップ方針を策定するときに以下の事項を考慮してください。

- 複製の作成 - ディスクアレイ固有の考慮事項、次のページを参照してください。

Data Protector NetApp Storage用統合ソフトウェアを使用する場合は、バックアップ方針を策定するときに以下の事項を考慮してください。

- 複製の作成 - ディスクアレイ固有の考慮事項、次のページを参照してください。
- スナップショットの種類(シンプロビジョニングまたは完全割り当て)
- VMware用仮想化ZDB統合ソフトウェアの場合のトランスポーテーションモード

Data Protector EMC VNXストレージファミリ用統合ソフトウェアを使用する場合は、バックアップ方針を策定するときに以下の事項を考慮してください。

- VMware用仮想化ZDB統合ソフトウェアの場合のトランスポーテーションモード

Data Protector EMC VMAXストレージファミリ用統合ソフトウェアを使用する場合は、バックアップ方針を策定するときに以下の事項を考慮してください。

- スナップショットの種類(TimeFinder/CloneまたはTimeFinder VP Snap)
- VMware用仮想化ZDB統合ソフトウェアの場合のトランスポーテーションモード

ディスクアレイ固 有 の考 慮 事 項

P4000 SANソリューションの複 製 セット

複 製 セット の作 成 は可 能 ですが、このディスクアレイファミリでは複 製 セット のローテーションはサポートされていません。

P4000 SANソリューションでのインスタントリカバリ

インスタントリカバリに使 用 するターゲットボリュームを選 択 したときに、選 択 したターゲットボリュームよりも新しいターゲットボリュームが同じソースボリュームに存 在 する場 合 、新しいターゲットボリュームは、所 属 する複 製 セットに無 関 係 に自 動 的 にディスクアレイから削 除 されます。特 定 の新しいターゲットボリュームが、そのSmartCloneがディスクアレイに存 在 するなどの理 由 で削 除 できない場 合 、インスタントリカバリセッションは失 敗 します。また、インスタントリカバリ用 に選 択 したソースボリュームに、Data Protector以 外 で作 成 された新しいスナップショット が存 在 する場 合 、インスタントリカバリセッションは失 敗 します。

いくつかのZDBバックアップ仕 様 に同じソースボリュームが含 まれる場 合 、特 定 ZDBバックアップ仕 様 を基 にインスタントリカバリセッションを実 行 すると、その他 のZDBバックアップ使 用 を基 にインスタントリカバリセッションを実 行 することが不 可 能 になる場 合 があります。以 下 の操 作 を以 下 の順 序 で実 行 した場 合 に、このような問 題 が発 生 します。

1. 特 定 ZDBバックアップ仕 様 (仕 様 A)を基 にインスタントリカバリセッションを実 行 し、インスタントリカバリ用 に選 択 したボリュームの新しいターゲットボリュームをディスクアレイから削 除 する。削 除 されたターゲットボリュームは、別 のZDBバックアップ仕 様 (仕 様 B)を基 にZDBセッション(セッションB)に作 成 された。
2. ZDBセッション(セッションB)に対 応 するインスタントリカバリセッションを開 始 する。

P6000 EVAアレイでの複 製 の作 成

特 定 のソースボリュームの新しいスナップクローンを作 成 できるのは、そのボリュームを対 象 とした前 のスナップクローンの作 成 が終 了 している場 合 だけです。終 了 していない場 合 、この処 理 がData Protector、指 定 した間 隔 で指 定 した回 数 まで自 動 的 に再 試 行 されます。標 準 スナップショットとvsnapには、この制 約 はありません。

ゼロダウンタイムバックアップセッションの実 行 中 、アプリケーションシステムのパフォーマンスに影 響 する時 間 は、以 下 のようにミラークローンを使 用 して短 縮 できますが、ディスクアレイのストレージスペースの使 用 量 が増 加 します。

1. HPE Command View (CV) EVAを使 用 して、アプリケーションデータが置 かれている元 のストレージボリュームのミラークローンを作 成 します。

   ミラークローンの作 成 は、Data ProtectorのZDBセッションがすでに実 行 されているときに発 生 した場 合 、時 間 がかかることがあります。また、その状 況 でミラークローンを作 成 するとバックアップウィンドウを短 縮 できなくなります。この手 順 を行 うと、そのような状 況 を回 避 することができます。
2. ZDBセッションで使 用 されるZDBバックアップ仕 様 で、スナップショット のソースとしてミラークローンを選 択 します。

詳 細 は、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参 照 してください。

P6000 EVAアレイでの複 製 セット のロー テーション

以 下 のような場 合 は、複 製 を再 使 用 することができません。

- スナップクローンであるいずれかのターゲット ボリュームにスナップショット が接 続 されている場 合 。
- 再 使 用 するターゲット ボリュームのいずれかがシステムに存 在 する場 合 。

「再 使 用 」は、ある複 製 が複 製 セット から削 除 され、新 しい複 製 が作 成 されることを意 味 しています。これは、複 製 セット の複 製 が指 定 最 大 数 に達 し、新 しい複 製 が必 要 になったときに最 も古 い複 製 で発 生 することがほとんどです。

再 使 用 の対 象 の複 製 が使 用 中 であり、別 のセッションによってロックされている場 合 、Data Protector HPE P6000 / HPE 3PAR SMI-S Agentは新 しい複 製 を作 成 し、既 存 の複 製 を削 除 対 象 として設 定 します。そのような余 分 な複 製 は、後 でomnidbsmisコマンドを使 用 して削 除 することができます。詳 細 は、『*HPE Data Protector Command Line Interface Reference*』を参 照 してください。

特 定 のZDBセッションでData Protectorによって自 動 的 に作 成 されたミラークローンは、インスタントリカバリに使 用 できないので、複 製 セット のロー テーションから除 外 されます。

詳 細 は、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参 照 してください。

P6000 EVAアレイでのインスタントリカバリ

インスタントリカバリは、ターゲット ボリュームに使 用 されているスナップショット の種 類 に関 係 なく実 行 することができます。インスタントリカバリ用 に選 択 したものよりも新 しい複 製 が複 製 セット に存 在 する場 合 、新 しい複 製 は使 用 されているスナップショット の種 類 (標 準 スナップショット 、vsnap、スナップクローン)に関 係 なく保 持 されます。

ゼロダウンタイム バックアップセッションに使 用 されるスナップショット の種 類 を選 択 する前 に、以 下 の事 項 を考 慮 してください。

- インスタントリカバリで最 も高 速 なのはディスクを切 り替 える方 法 です。この方 法 は、スナップショット の種 類 がスナップクローンの場 合 にのみ使 用 できます。
- 標 準 スナップショット またはvsnapで構 成 される複 製 をインスタントリカバリに選 択 したとき、選 択 した複 製 よりも新 しい複 製 が複 製 セット に存 在 する場 合 は、インスタントリカバリの処 理 時 間 が通 常 よりも長 くなります。この理 由 は、ソースボリュームだけでなく、新 しい複 製 もセッション中 にすべて更 新 しなければならないためです。そのような状 況 では、複 製 セット の複 製 の数 をよく考 えて定 義 しないと、インスタントリカバリの所 要 時 間 が長 くなることがあります。

ミラークローンのスナップショット が、対 応 するゼロダウンタイム バックアップセッションで作 成 された場 合 、インスタントリカバリの実 行 中 、ミラークローンスナップショット からのデータは、ミラークローン自 身 ではなく、元 のボリュームに復 元 されます。

P9000 XPアレイでの複 製 の種 類 の選 択

ZDBバックアップ仕 様 を作 成 するときに、目 的 の複 製 の種 類 をData ProtectorのGUIで直 接 選 択 することはできません。ただし、適 切 なミラーユニット (MU)番 号 または番 号 の範 囲 を使 用 して、特 定 の複 製 の種 類 がData Protectorで使 用 されるようにすることは可 能 です。特 定 の番 号 のMUに属 するソースボリュームがゼロダウンタイム バックアップセッションで使 用 される場 合 、Data Protector HPE P9000 XP Agentはペアになっている仮 想 ディスクの種 類 に応 じて複 製 の種 類 を選 択 します。このため、HPE P9000 XPリモート Webコンソールを使 用 してこの仮 想 ディスクを事 前 に構 成 しておく必 要 があります。

P9000 XPアレイでのインスタントリカバリ

インスタントリカバリに使 用する複 製を選 択したときに、選 択したものよりも新しい複 製 が複 製 セットに存 在 する場 合 、新しい複 製 は種 類 (スプリットミラー、スナップショット)に関 係なくセッション後 も保 持されま す。

バックアップポリシーの適 用 範 囲 内 で実 行されているZDBセッションで使 用される複 製 の種 類 を選 択 する 前 に、インスタントリカバリにスプリットミラー複 製 を選 択したときにインスタントリカバリ処 理 が最 も高 速 で 実 行されることと、P9000 XPアレイの機 能 である簡 易 復 元 モード がディスクアレイの複 製 ボリュームの事 前 構 成 中 に有 効になることを考 慮してください。

3PAR StoreServシステムでの複 製 の作 成

3PAR StoreServシステム上 で複 製 の作 成 が呼 び出 されるたびに、実 際 には各 ソースボリュームに2つの スナップショット (1つの読 み取 り専 用 スナップショットと1つの読 み書 きスナップショット)が作 成 されます。読 み 書 きスナップショット のみが外 部 アプリケーションに公 開 され、読 み取 り専 用 スナップショット はストレージシス テム内 部 で使 用 されます。ストレージスペースの消 費 の詳 細 については、HPE 3PAR StoreServ Storage のマニュアルを参 照してください。

NetApp Storageシステムでの複 製 の作 成

NetApp Storageシステム上 で複 製 の作 成 が呼 び出 されるたびに、実 際 には各 ソースボリュームに2つのス ナップショット (1つの読 み取 り専 用 スナップショットと1つの読 み書 きスナップショット)が作 成 されます(LUNク ローン)。読 み書 きスナップショット のみが外 部 アプリケーションに公 開 され、読 み取 り専 用 スナップショット は ストレージシステム内 部 で使 用 されます。ストレージスペースの消 費 の詳 細 については、NetAppのマニュア ルを参 照してください。

並 列 処 理

ロック

バックアップデバイスのロック

通 常 の(ZDBではない)Data Protectorのバックアップセッションおよび復 元 セッションでは、バックアップセッショ ンまたは復 元 セッションの最 初 にセッションで使 用 されるテープデバイスがロックされ、セッションの最 後 にロッ クが解 除 されます。ZDB用 統 合 ソフトウェアを使 用 すると、テープデバイスのロックの方 法 が変 わり、テープ デバイスとの転 送 に必 要 な期 間 のみデバイスがロックされるようになります。

- テープへのZDBセッションまたはディスク+テープへのZDBセッションでは、複 製 の作 成 後 、複 製 された データがテープへストリーミングされる前 にロックがかかります。
- 特 定 のディスクアレイファミリでサポートされているスプリットミラー復 元 セッションで、複 製 が作 成 されてか ら、バックアップデータがテープデバイスから複 製 に移 動 されるまでにロックが発 生 します。

テープデバイスとの間 のデータ転 送 が終 了 した時 点 で、デバイスのロックは解 除 されます。

ディスクへのZDBセッションまたはインスタントリカバリセッションでは、テープデバイスは使 用 されないため、テープデバイスはロックされません。

ディスクのロック

ZDBセッションまたはインスタントリカバリセッションが、別 のセッションで使 用 中 の可 能 性 があるストレージボリュームにアクセスしないようにするために、Data Protectorでは、内 部 ディスクロックメカニズムが導 入 されています。これにより、他 の操 作 で使 用 されている間 、ストレージボリュームはロックされます。

要 求 された処 理 に必 要 なストレージボリュームをロックできない場 合 (他 のプロセスによってすでにロックされている場 合)は、Data Protectorから警 告 が表 示 され、セッションは中 止 されます。

バックアップシナリオ

バックアップ戦 略 は、フルバックアップと増 分 バックアップで構 成 できます。これらのセッションは、ZDBのみ、または非ZDBのみでなくてもかまいません。さまざまなやり方 で組 み合 わせることができます。以 下 の組 み合 わせがサポートされます。

バックアップシナリオ

フルバックアップ	増 分 バックアップ
ZDB	ZDB
ZDB	非ZDB
ZDB	非ZDBとZDB
非ZDB	ZDB
非ZDB	ZDBと非ZDB

注:
ZDBと非ZDBセッションで同じオブジェクトをバックアップしたい場 合 には、バックアップの種 類 ごとに別 々 のバックアップ仕 様 を作 成 します。たとえば、ディスク+テープへのZDB用 に1つ、テープへのZDB用 に1つ、非ZDBセッション用 に1つ、それぞれバックアップ仕 様 を作 成 します。

バックアップ仕 様 で選 択 したバックアップオブジェクトが必 ず一 致 するようにしてください(同 じクライアント、マウスポイント、および説 明)。一 致 しない場 合 、Data Protectorではこれらのバックアップを別 のオブジェクトとして扱 うため、復 元 時 にテープからの増 分 バックアップとフルバックアップを同 じ復 元 チェーンに含 めることができなくなります。

以 下 は、増 分 ZDBセッションの利 点 の一 部 です。

- インスタントリカバリの精 度 に優 れている(バックアップ仕 様 で`Track the replica for instant recovery`オプションを選 択 した場 合)。
- バックアップ時 のアプリケーションシステムのパフォーマンスへの影 響 を低 減 できる。
- テープにストリーミングされるデータの量 を削 減 できる。

例

複 製 を2、3日 ごとに作 成 してその複 製 をインスタントリカバリ用 に保 持 しておくことにより、インスタントリカバリの精 度 を高 め、さらにテープにストリーミングされるデータの量 を削 減 したいという場 合 には、以 下 のようなバックアップ戦 略 を使 用 することができます。

- 日 曜 日 に、ディスク+テープへのフルZDBセッション
- 火 曜 日 と木 曜 日 に、ディスク+テープへの増 分 ZDBセッション
- その他 の曜 日 に、テープへの増 分 ZDBセッション

このシナリオでは、以 下 のようにバックアップを構 成 します。

- ディスク+テープへのZDBバックアップ仕 様 を作 成 し、日 曜 日 のフルバックアップ、火 曜 日 および木 曜 日 の増 分 バックアップをスケジュールします。
- テープへのZDBバックアップ仕 様 を作 成 し、月 曜 日 、水 曜 日 、金 曜 日 、および土 曜 日 の増 分 バックアップをスケジュールします。

データを復 元 するには、複 製 (迅 速 な復 元)またはテープのバックアップを使 用 することができます。2つの復 元 の種 類 を組 み合 わせて、まず複 製 を復 元 し、次 にテープから指 定 したバックアップの個 々 のファイルを復 元 することもできます。

付録A: サポートされている構成

概要

この付録では、各種ディスクアレイでサポートされている構成に関する情報を示します。示されている構成は、HPEによってサポートされています。サポートされる構成の最新情報については、https://softwaresupport.hpe.com/にある最新のサポート一覧を参照してください。リストに記載されていないデータバックアップ構成は必ずしもサポートできないという意味ではありません。最寄りのHPE営業担当またはHPE相談窓口に、サポートされるその他の構成がないかお問い合わせください。

単一ホスト(BC1)構成は、1つのシステムがアプリケーションシステムおよびバックアップシステムとして機能する構成ですが、パフォーマンスに問題があるためお勧めしません。BC1構成では、ファイルシステムバックアップとディスクイメージバックアップのみを実行することができます。

Linuxプラットフォームを基盤とする、HPE P6000 EVAディスクアレイファミリおよびHPE 3PAR StoreServ Storageの単一ホスト(BC1)構成はサポートされていません。単一ホスト(BC1)構成では、1つのLinuxシステムがアプリケーションシステムおよびバックアップシステムとして機能します。

次の表に、Data Protectorでサポートされているディスクアレイで、複製の作成機能があるものを示します(ほとんどの場合は、複製セットも作成できます)。

Data Protectorで使用できるディスクアレイ

ディスクアレイファミリ	略称	サポートされる複製方法
HPE P4000 SANソリューション	P4000 SANソリューション	スナップショット
HPE P6000 EVAディスクアレイファミリ	P6000 EVAアレイ	スナップショット
HPE P9000 XPディスクアレイファミリ	P9000 XPアレイ	スプリットミラー、スナップショット
HPE 3PAR StoreServ Storage	3PAR StoreServ	スナップショット
EMC Symmetrix Disk Array	EMC	スプリットミラー
EMC VNXストレージファミリ	EMC VNX	スナップショット
EMC VMAXストレージファミリ	EMC VMAX	スナップショット
NetApp Storage	NetApp	スナップショット

サポートされているどの構成でも、ZDBバックアップ仕様には1つのアプリケーションシステムと1つのバックアップシステムしか含めることができません。ただし、各アプリケーションシステムに対して複数のZDBバックアップ仕様を用意し、それらを使用して同じアプリケーションシステムを別々のファイルシステムに同時にバックアップすることは可

能です。複数のアプリケーションシステムがある構成については、マウントポイントの作成を参照してください。どの構成でも、元のデータとバックアップデータを同種類の複数のディスクアレイに分散することができます。

各構成に固有の動作パターンがあり、バックアップ/復旧機能を保証するための制御機能についての固有の要件があります。

サポートされているHPE P6000 EVAディスクアレイファミリ構成

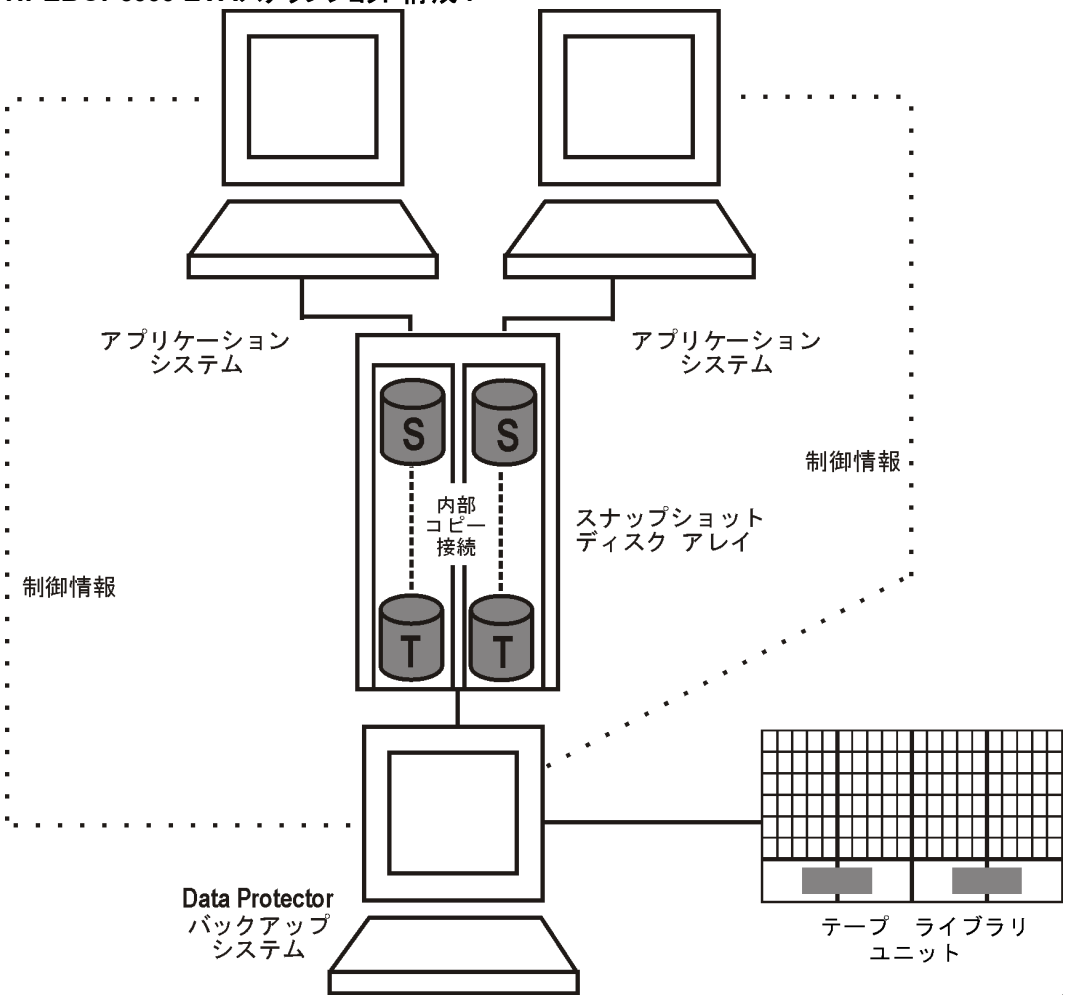
ローカル複製の構成

ローカル複製には、HPE BC P6000 EVA構成が使用されます。

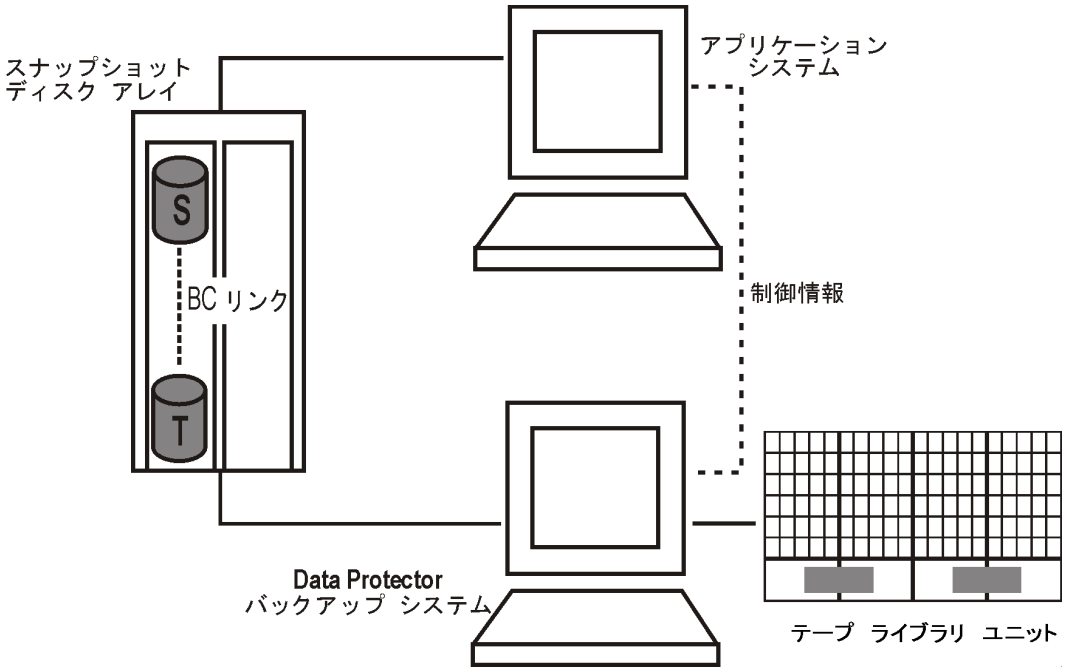
個別のバックアップシステムをディスクアレイに接続する必要があります。複製が作成されると、Data Protectorはバックアップシステムの新しいディスクをスキャンし、デバイスファイルを作成するほか(UNIXシステムの場合)、ファイルシステムをバックアップシステムにマウントするのに必要なその他の手順をすべて実行して、複製データにアクセスできるようにします。データが複製からテープへストリーミングされる間も、アプリケーションシステムは動作を継続できます。

HPEBCP6000 EVAスナップショット構成1、次のページ～HPEBCP6000 EVAスナップショット構成3、ページ283は、サポートされているローカル複製の構成の例です。

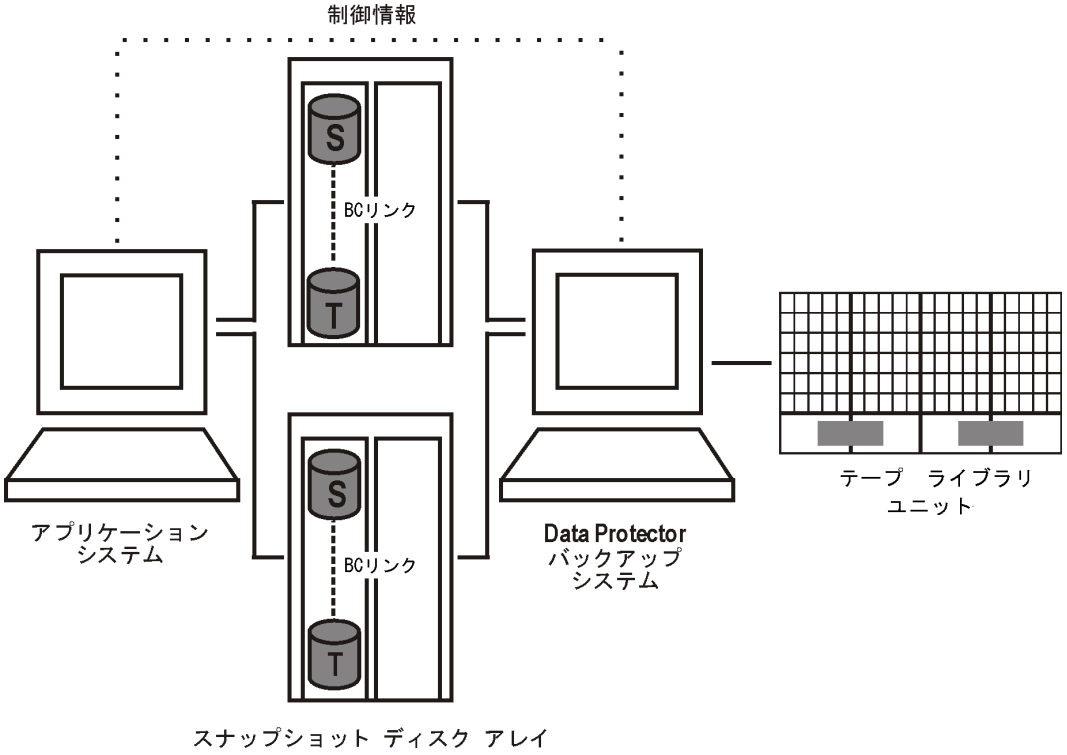
HPEBCP6000 EVAスナップショット構 成1



HPEBCP6000 EVAスナップショット構 成2



HPEBCP6000 EVAスナップショット構 成 3

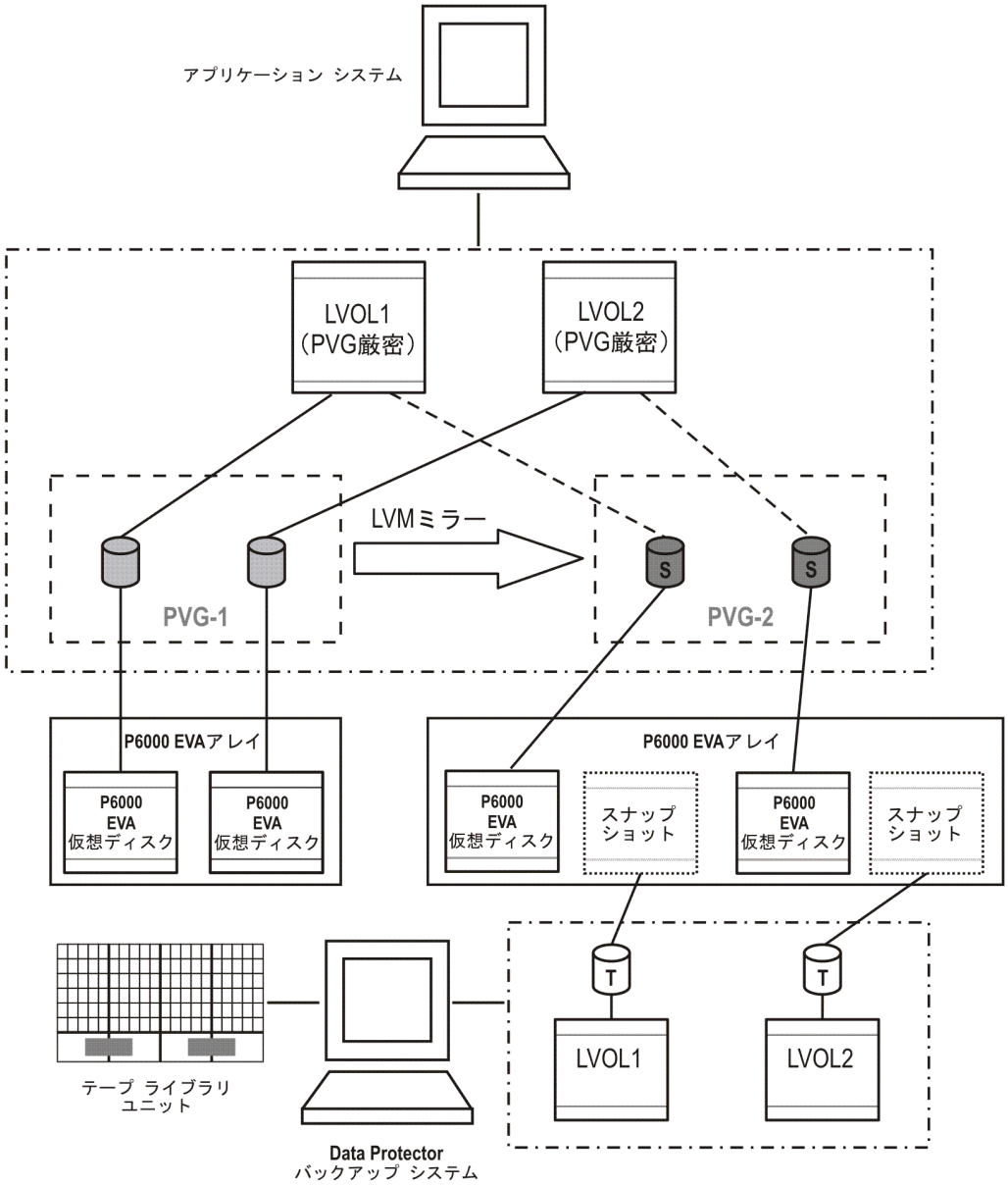


ローカル複 製 の構 成とHP-UX LVMミラー

ボリュームグループの物 理 ボリュームを物 理 ボリュームグループ(PVG)にグループ化 し、ミラー作 成 用 のPVG-strictポリシーを指 定 することをお勧 めします。これにより、1つの論 理 ボリュームのミラーがさまざまなPVGに属 するようになり、同 じディスクへの論 理 ボリュームのミラー操 作 などといった特 定 の状 況 を回 避 できます。

サポートされているLVMミラー構 成 1、下 ～ サポートされているLVMミラー構 成 3、ページ 286は、P6000 EVAアレイでサポートされているLVMミラーの構 成 の例 です。

サポートされているLVMミラー構 成 1

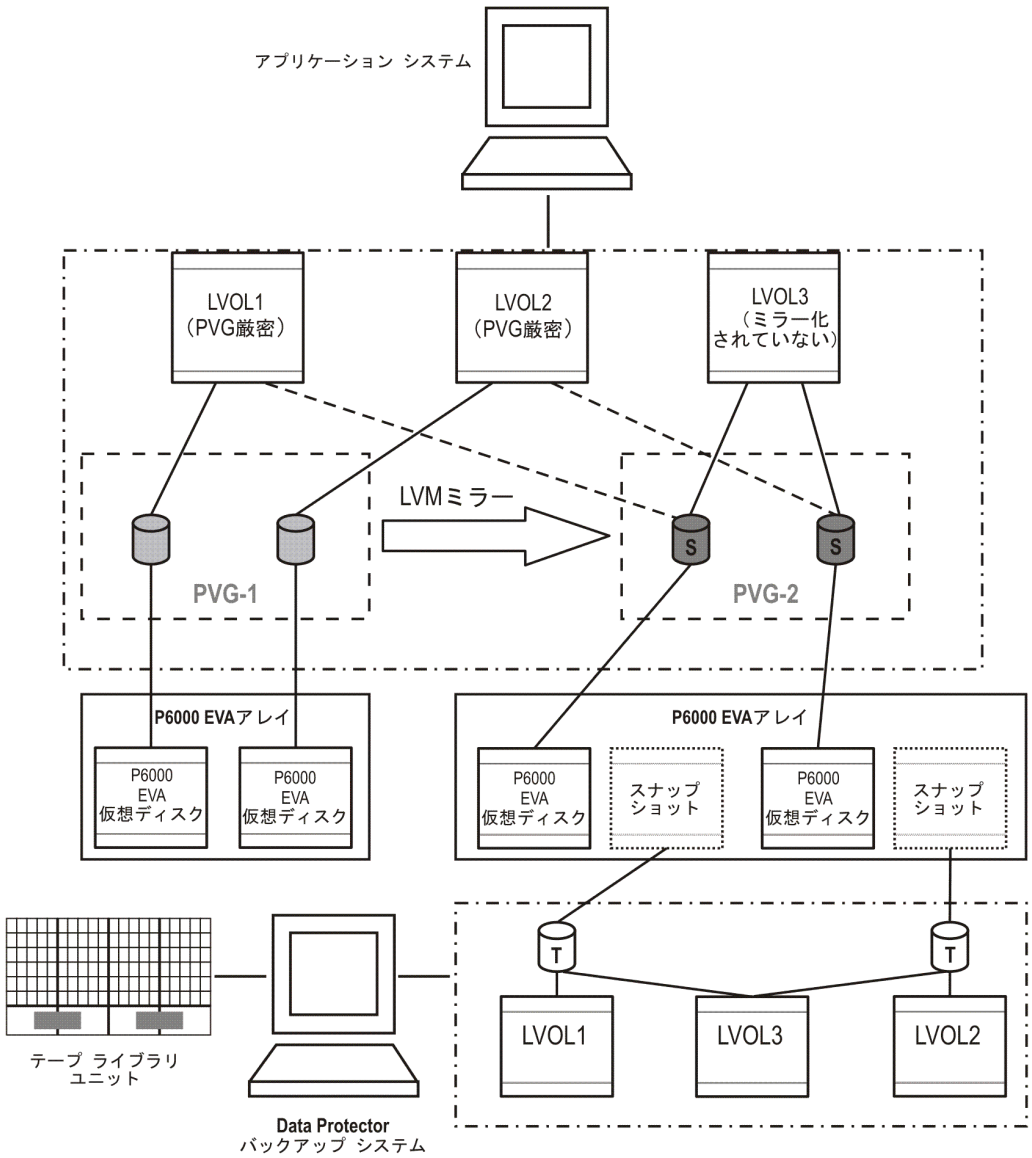


ボリュームグループ内 のすべての論 理 ボリュームがバックアップ仕 様 でバックアップオブジェクトとして指 定 され ます。すべての論 理 ボリューム(およびそのエクステント分 散)は、PVG内 のさまざまな物 理 ボリューム上 にあ ります。

複 製 は、このPVGで見 つかったストレージボリュームに対してのみ作 成 されます。この後 、これらの複 製 は、選 択 されたバックアップオブジェクトの今 後 のバックアップで使 用 できるよう、バックアップシステムに提 示 されます。

PVG-1とPVG-2は両 方 とも、ミラー選 択 ルールを満 たしています。ただし、HPE P6000 / HPE 3PAR SMI-S Agentは常 に二 次ミラーを選 択 しようとするため、HPE BC P6000 EVAペア複 製 にはPVG-2が選 択 されます。

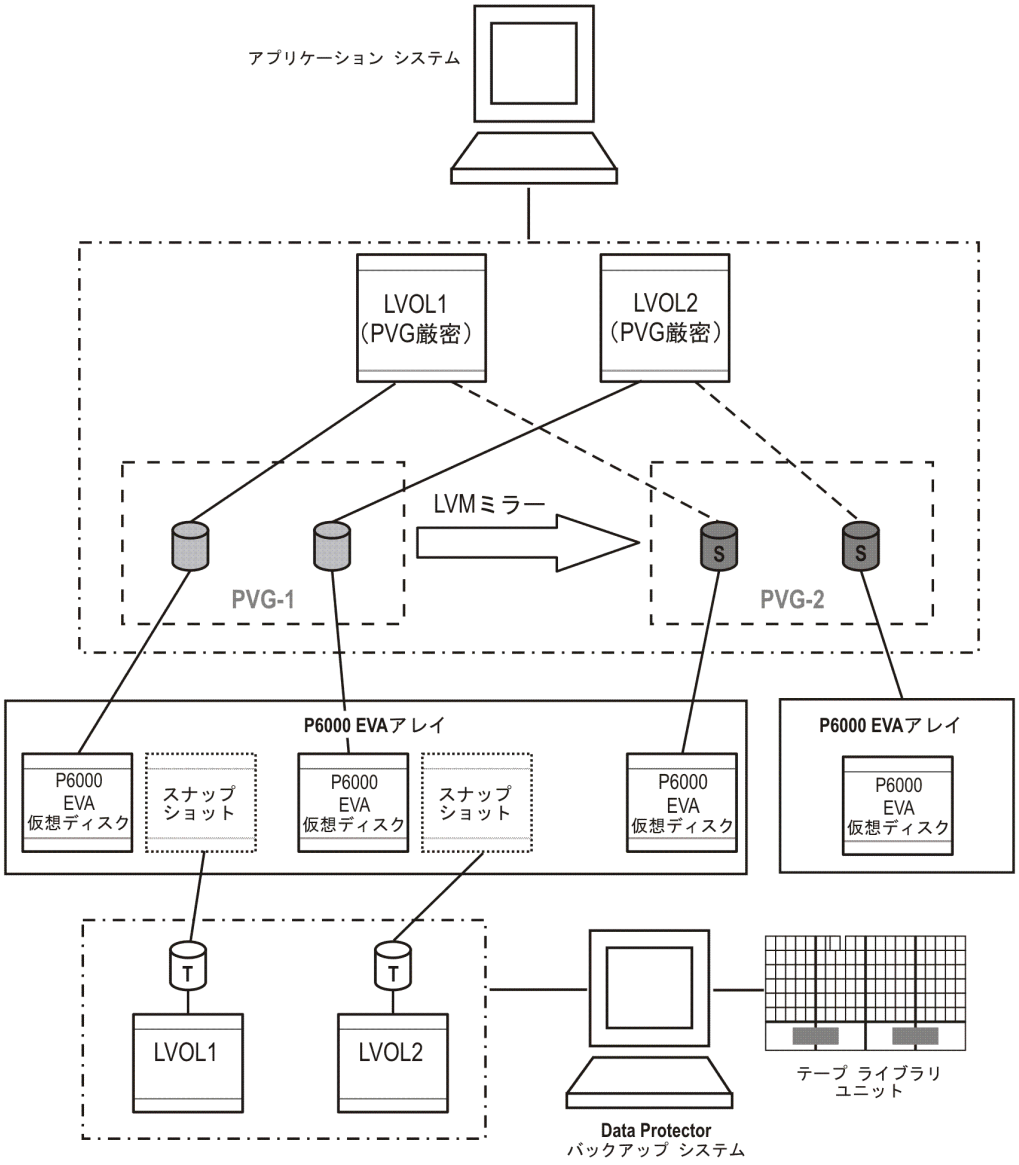
サポートされているLVMミラー構 成 2



選 択 された論 理 ボリュームだけがバックアップ仕 様 に含 まれます。ここでも、選 択 されるPVGは、そのボリュームグループのすべての論 理 ボリュームをホストするPVGです。

この構 成 では、PVG-2のみがミラーセット選 択 ルールを満 たすことができます。このためBCペア複 製 にはPVG-2が選 択 されます。

サポートされているLVMミラー構 成 3



二 次ミラーのメンバーの一 部 が一 次ミラーディスクアレイによってホストされています。このため、これらのメンバーは複 製 の候 補 になりません。したがって、BCペア複 製 には一 次ミラーセットが選 択 されます。

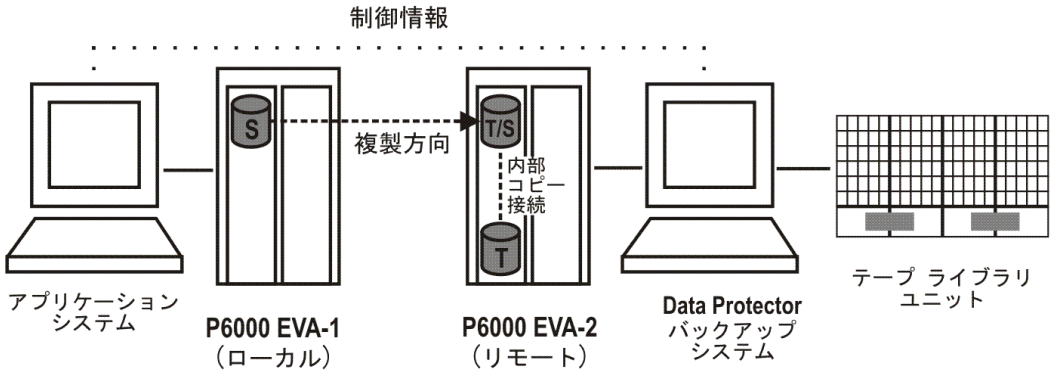
LVMミラーとミラー選 択 ルールの詳 細 については、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参 照 してください。

リモートプラスローカル複製の構成

P6000 EVAアレイでのリモートプラスローカル複製には、HPE CA+BC P6000 EVA構成が使用されます。

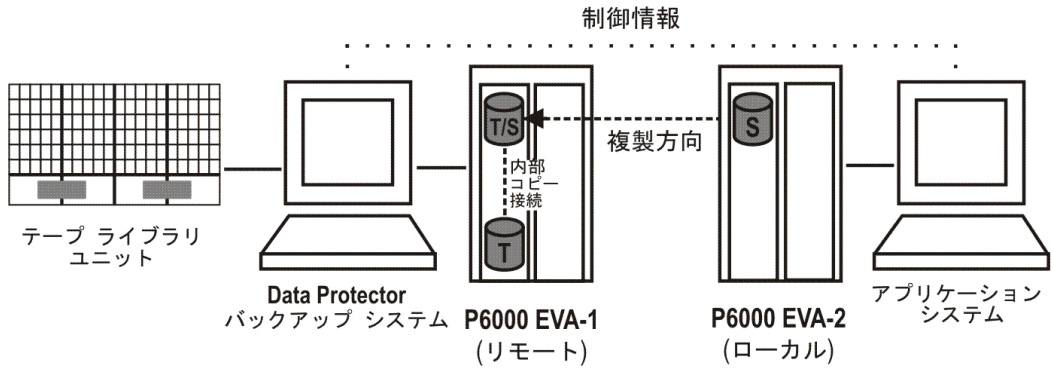
HPE CA+BC P6000 EVA構成1、下 ～ サポートされているHPE P6000 EVAディスクアレイファミリ構成、ページ 281は、P6000 EVAアレイでサポートされているリモートプラスローカル構成の例です。

HPE CA+BC P6000 EVA構成1



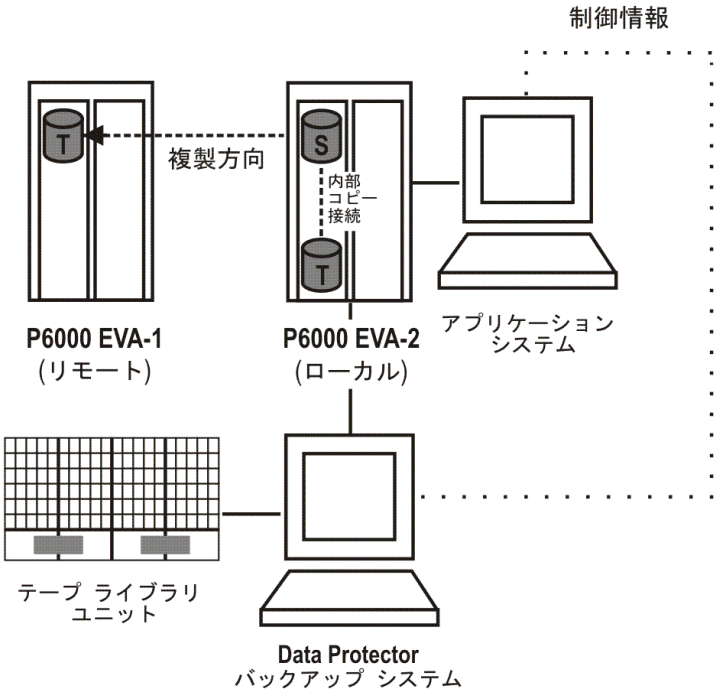
この構成は、理想的な(非フェイルオーバー)シナリオを表しています。

HPE CA+BC P6000 EVA構成2



この構成は、複製の方向が逆となるフェイルオーバーシナリオを表しています。

HPE CA+BC P6000 EVA構成3



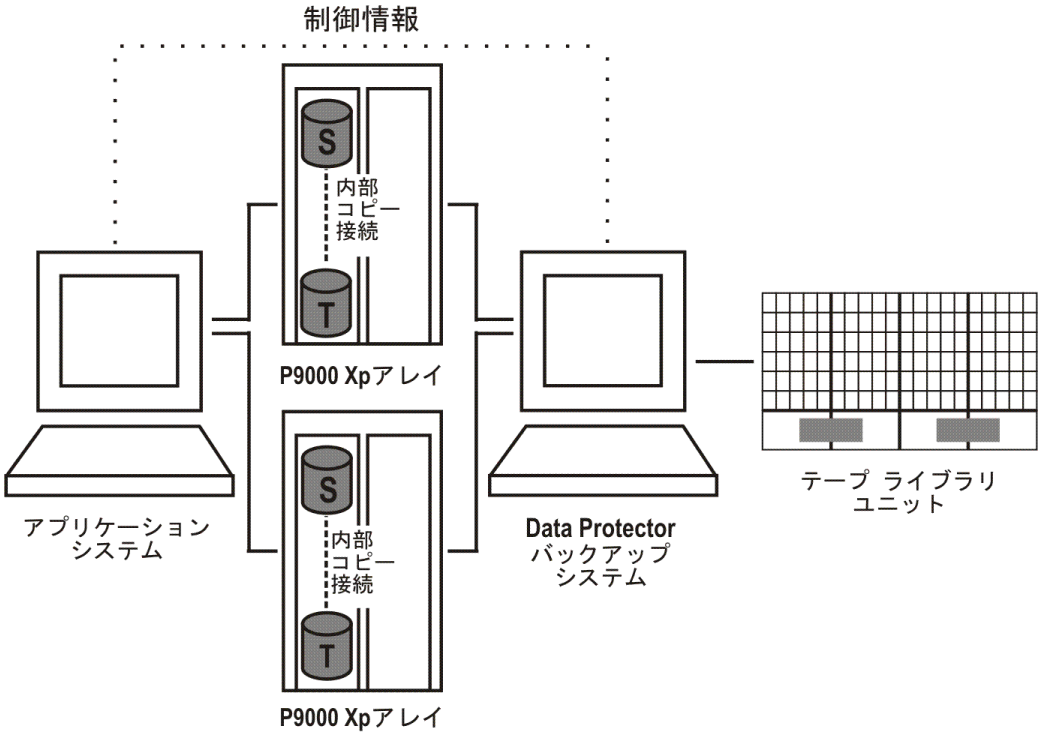
この構 成は、複 製 場 所 が維 持 されるフェイルオーバーシナリオを表しています。

サポートされているHPE P9000 XPディスクアレイファミリ構 成

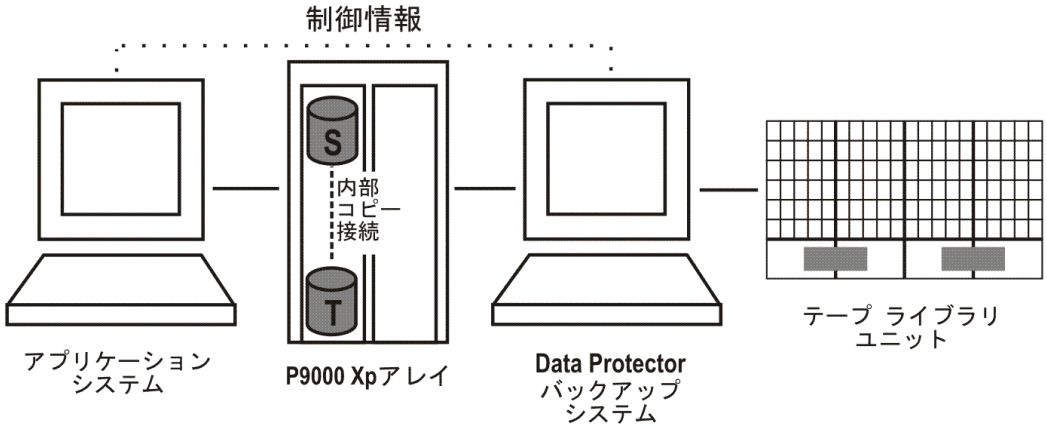
ローカル複 製 の構 成

HPE BC P9000 XP構 成 1、下 ～ HPE BC P9000 XP構 成 3、次 のページは、P9000 XPアレイでサポートされているローカル複 製 の構 成 の例 です。

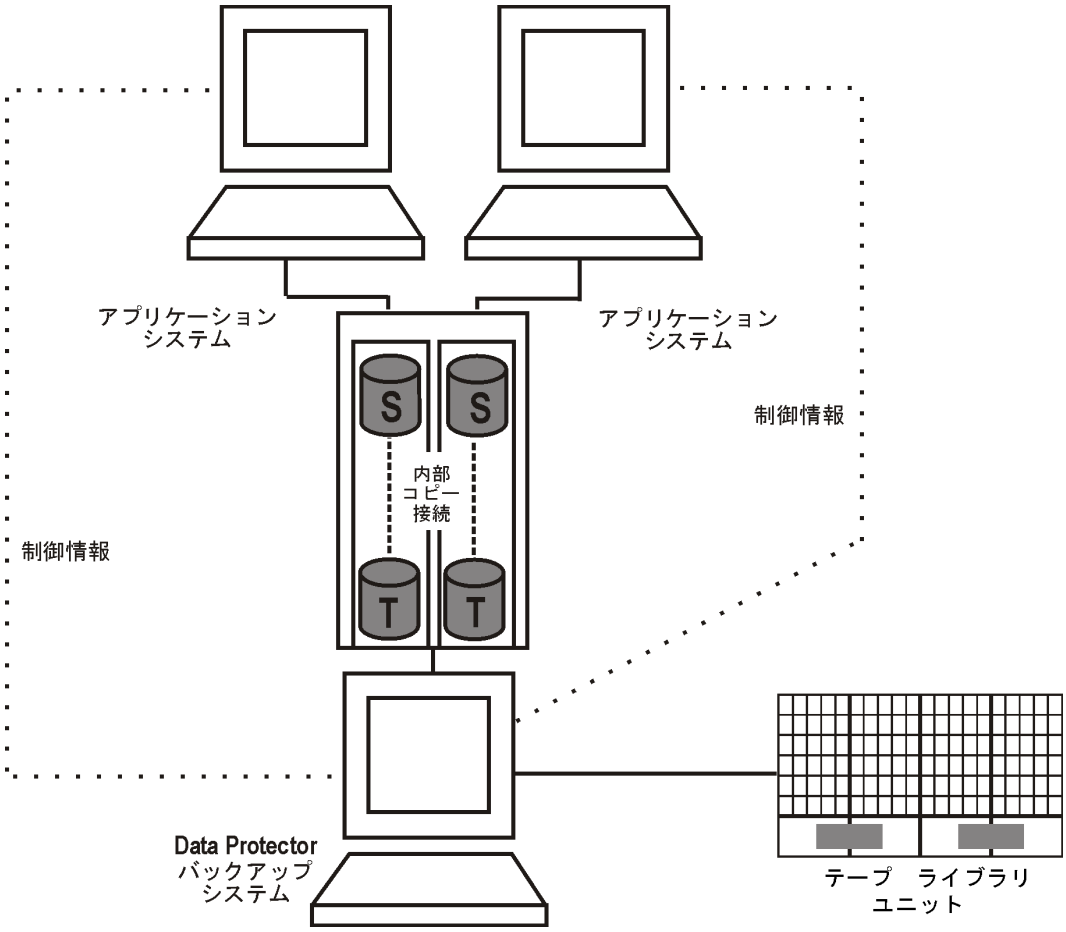
HPE BC P9000 XP構 成 1



HPE BC P9000 XP構成2



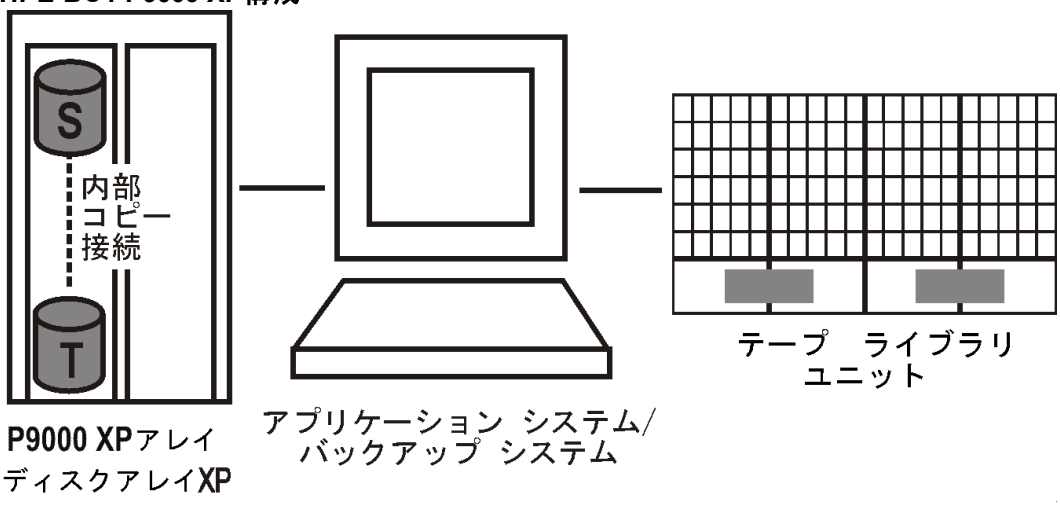
HPE BC P9000 XP構成3



単一ホスト(BC1)構成

次の図は、単一ホスト構成(**BC1構成**)を示しています。

HPE BC1 P9000 XP構成

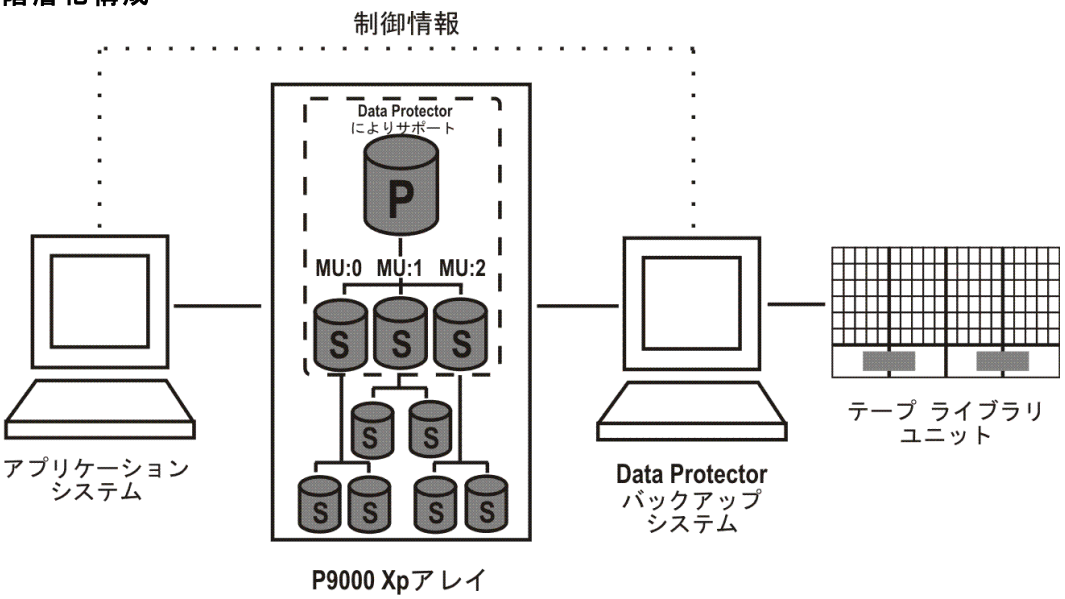


階 層 化 構 成

HPE P9000 XPディスクアレイファミリでは、ファーストレベルの各ミラーまたは各 スナップショット ボリューム に、追 加 のセカンドレベルのミラーまたはスナップショット ボリュームを構 成 することができます。これを**階 層 化 構 成** と呼 びます。ただし、ゼロダウンData Protectorタイムバックアップ、インスタントリカバリ、スプリットミラー復 元 の各 セッションではファーストレベルミラーまたはスナップショット ボリュームのみが使 用 されます。

次 の図 は、階 層 化 構 成 の例 です。この例 では、MU:0、MU:1、MU:2がData Protectorによってサポートされるファーストレベルミラーで、その下 にある6つのミラーがセカンドレベルミラーです。

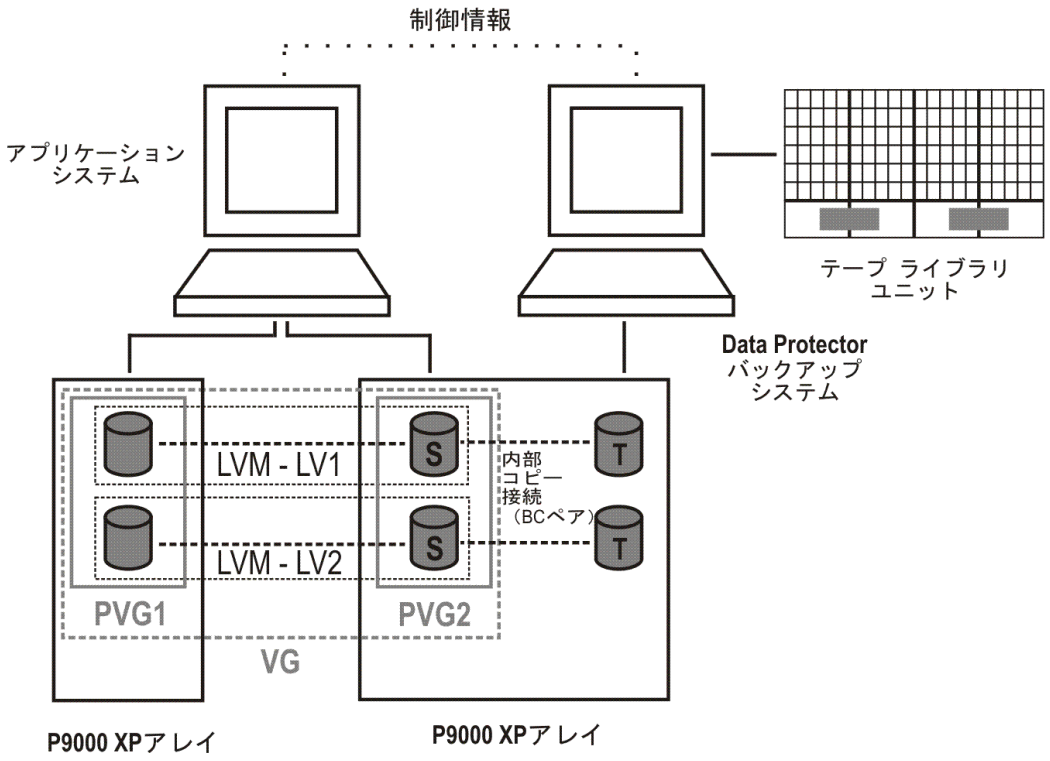
階 層 化 構 成



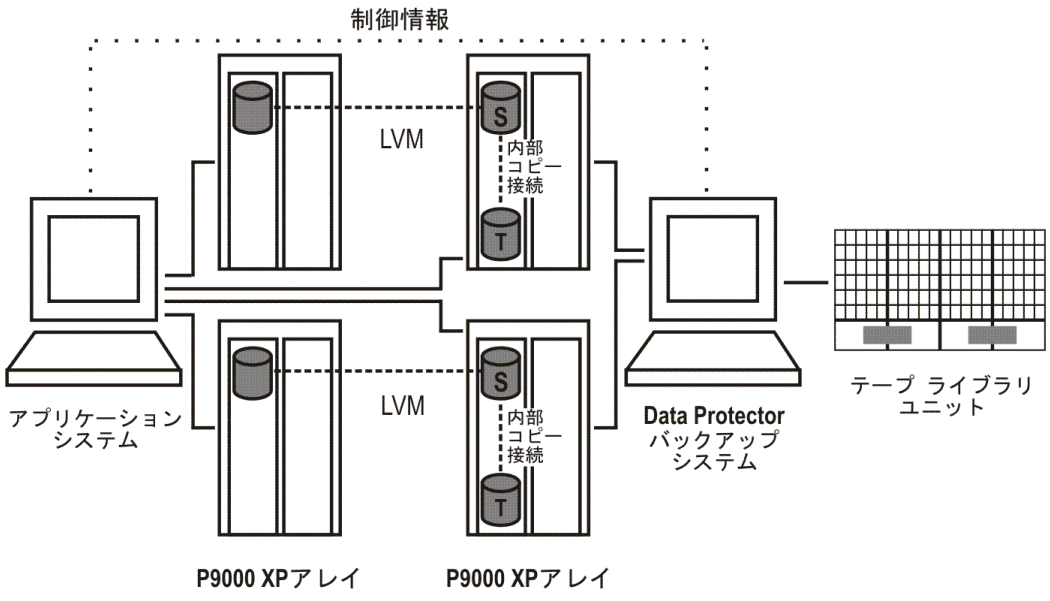
ローカル複 製 の構 成 とHP-UX LVMミラー

LVMミラー構 成 1、下 ～ クラスターでのLVMミラー構 成 、ページ 293は、P9000 XPアレイでサポートされているLVMミラーの構 成 の例 です。

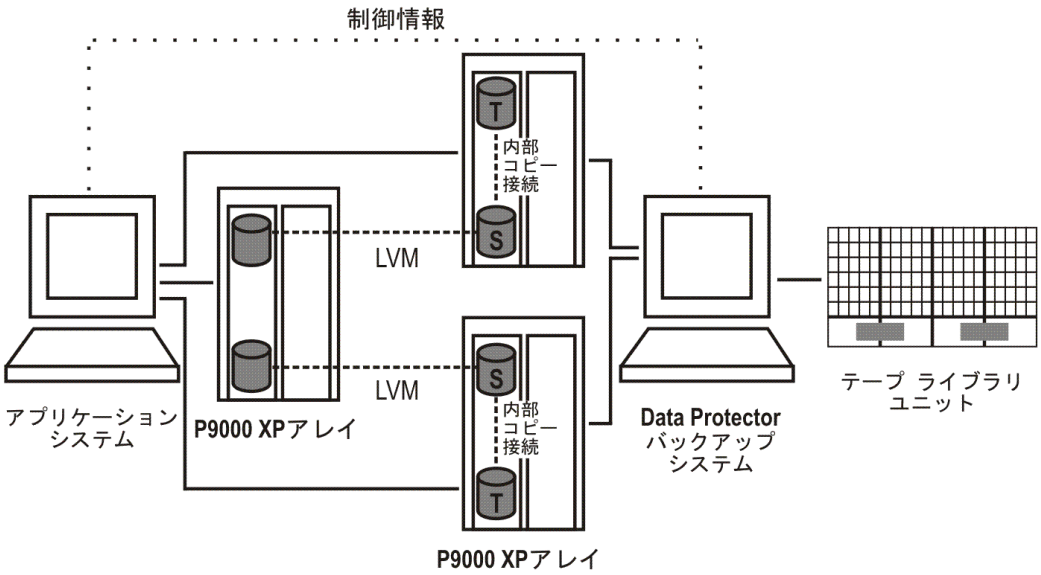
LVMミラー構 成 1



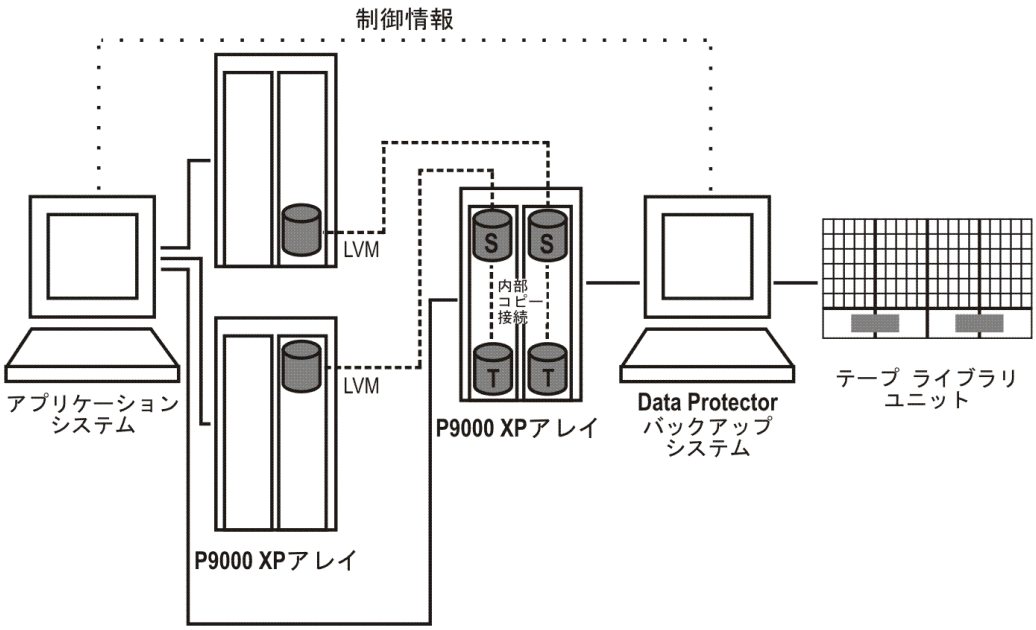
LVMミラー構 成2



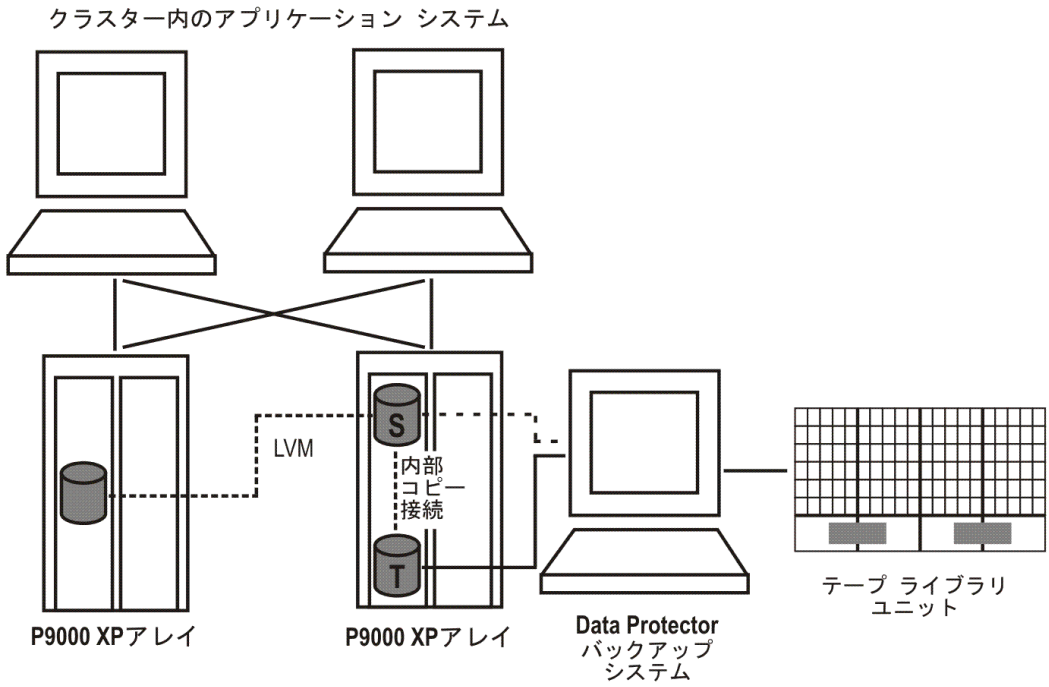
LVMミラー構 成3



LVMミラー構 成4



クラスターでのLVMミラー構 成



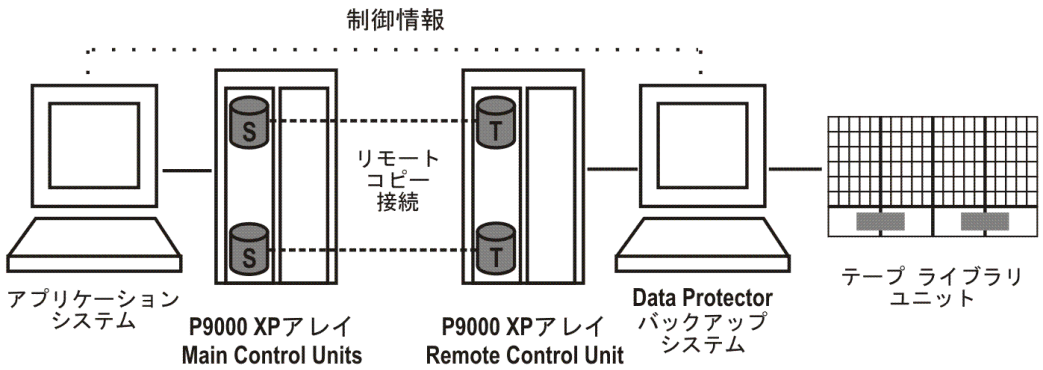
リモート複製の構成

バックアップシステム1つとP9000 XPアレイ1つを使用して、複数のメインディスクアレイをバックアップすることができます。「HPE CA P9000 XP構成4、次のページ」を参照してください。この方法では、一元的なバックアップ サイトを構築できます。物理的に別々のサイトに、少なくとも2つのディスクアレイが必要になります。

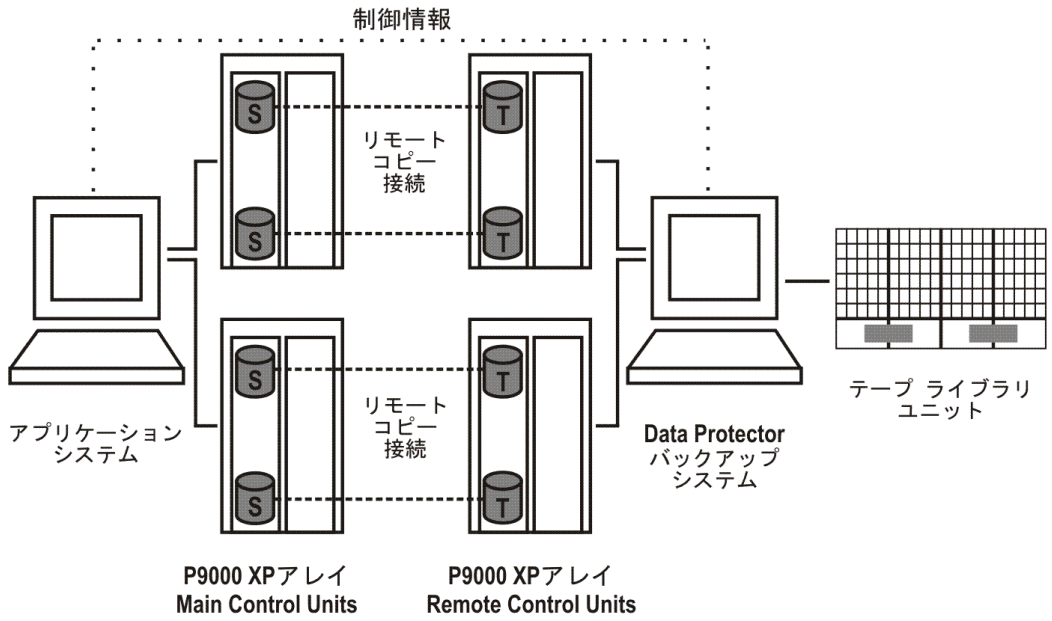
Data Protectorセッション中、ゼロダウンタイムバックアップにディスクアレイ間のミラー(CA)リンクが使用されます。同時にデータの可用性を十分な高値に維持するには、追加ミラー(CA)が必要です。

HPE CA P9000 XP構成1、下 ～ HPE CA P9000 XP構成4、次のページは、P9000 XPアレイでサポートされているリモート複製の構成の例です。

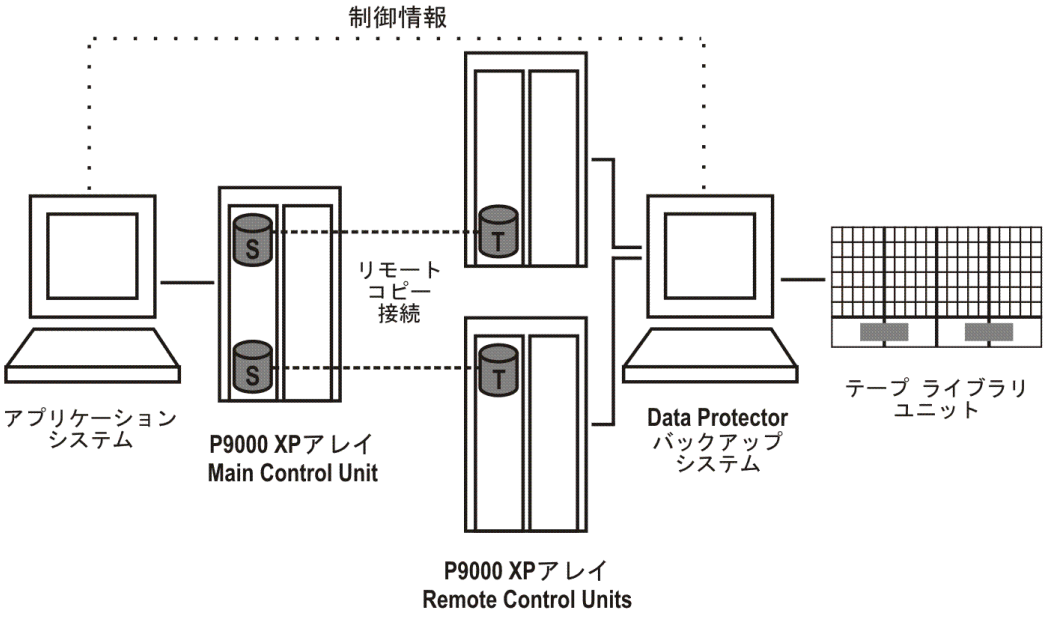
HPE CA P9000 XP構成1



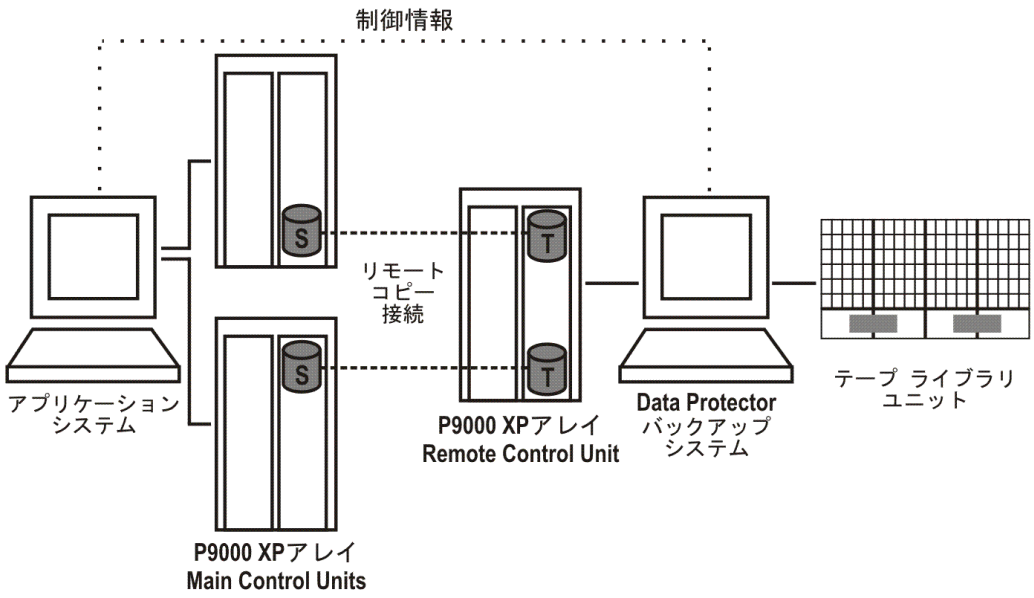
HPE CA P9000 XP構 成2



HPE CA P9000 XP構 成3



HPE CA P9000 XP構 成4



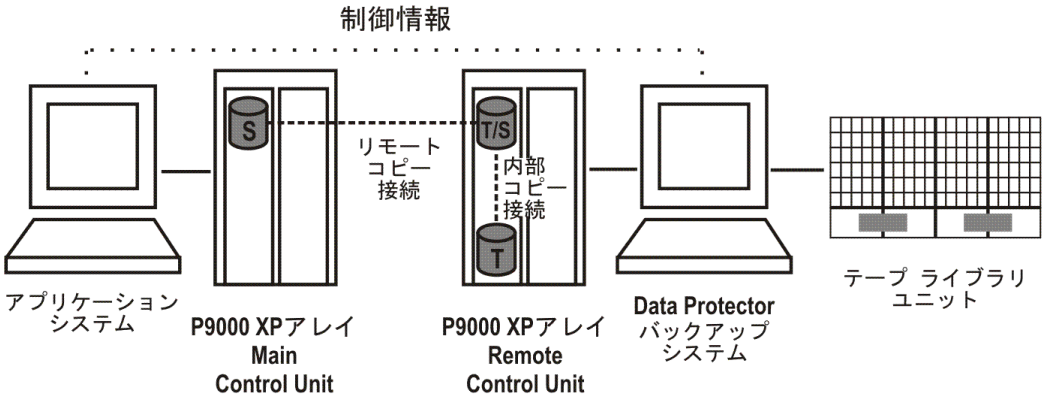
リモートプラスローカル複製の構成

制限事項

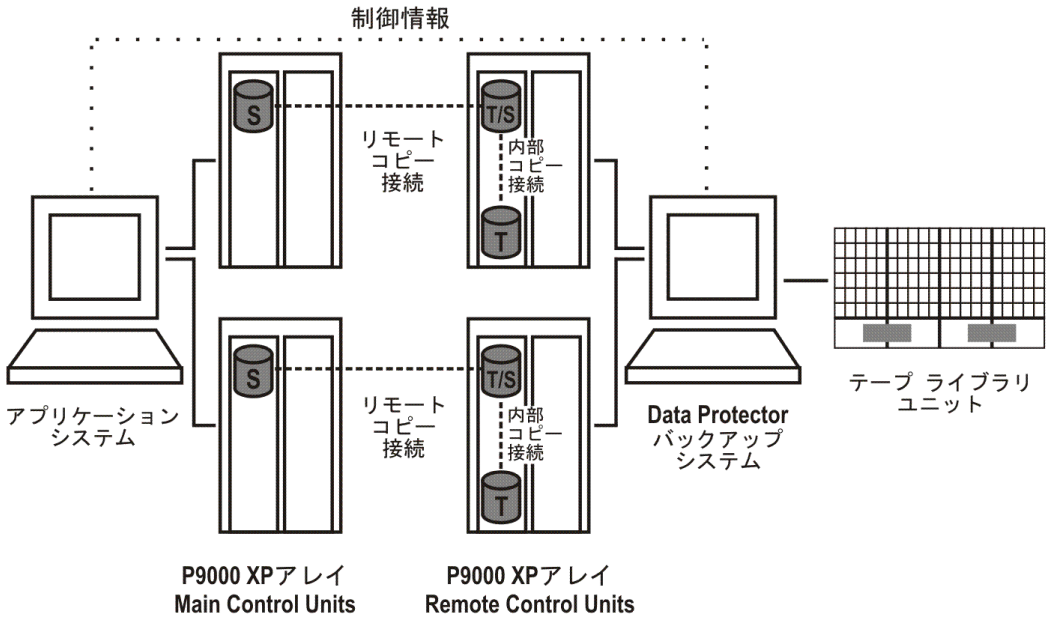
- HP-UXでは、バックアップシステムにはBCターゲットボリュームのみを接続することをお勧めします。何らかの理由でCAターゲットボリュームを接続する場合は、特別な注意が必要です。詳細については、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参照してください。
- CA+BCの組み合わせ構成の一部としての非同期CA構成は、サポートされていません。

HPE CA+BC P9000 XP構成1、下 ～ HPE CA+BC P9000 XP構成4、次のページは、P9000 XPアレイでサポートされているリモートプラスローカル複製の構成の例です。

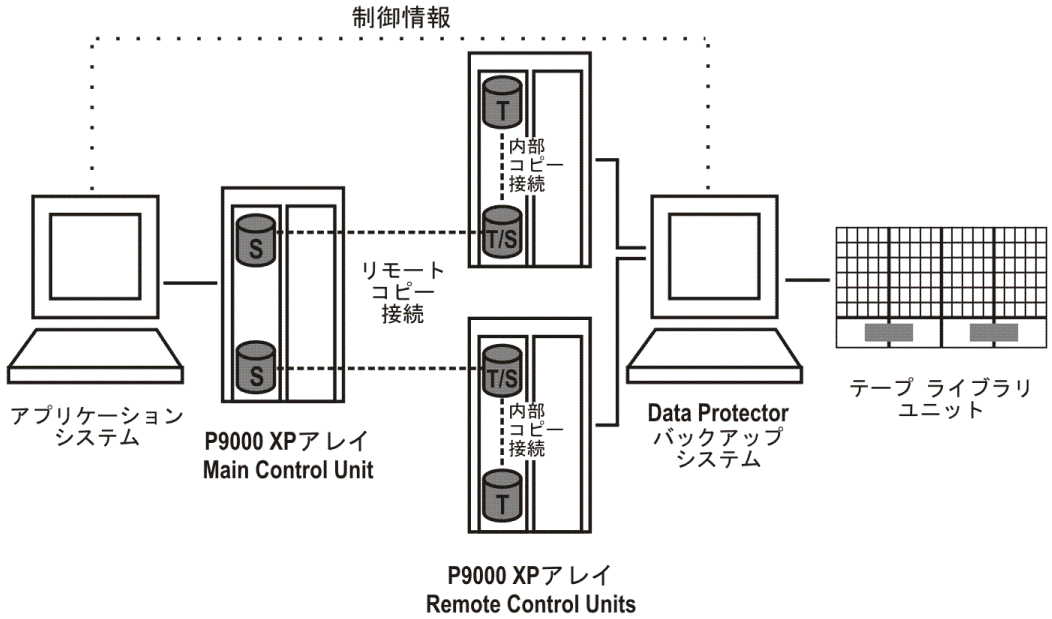
HPE CA+BC P9000 XP構成1



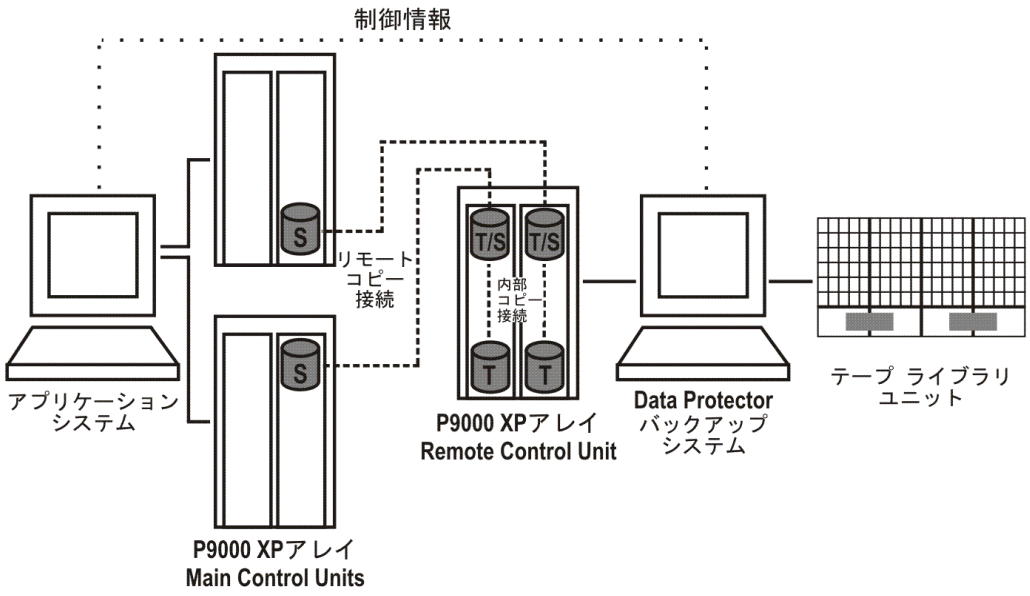
HPE CA+BC P9000 XP構 成2



HPE CA+BC P9000 XP構 成3



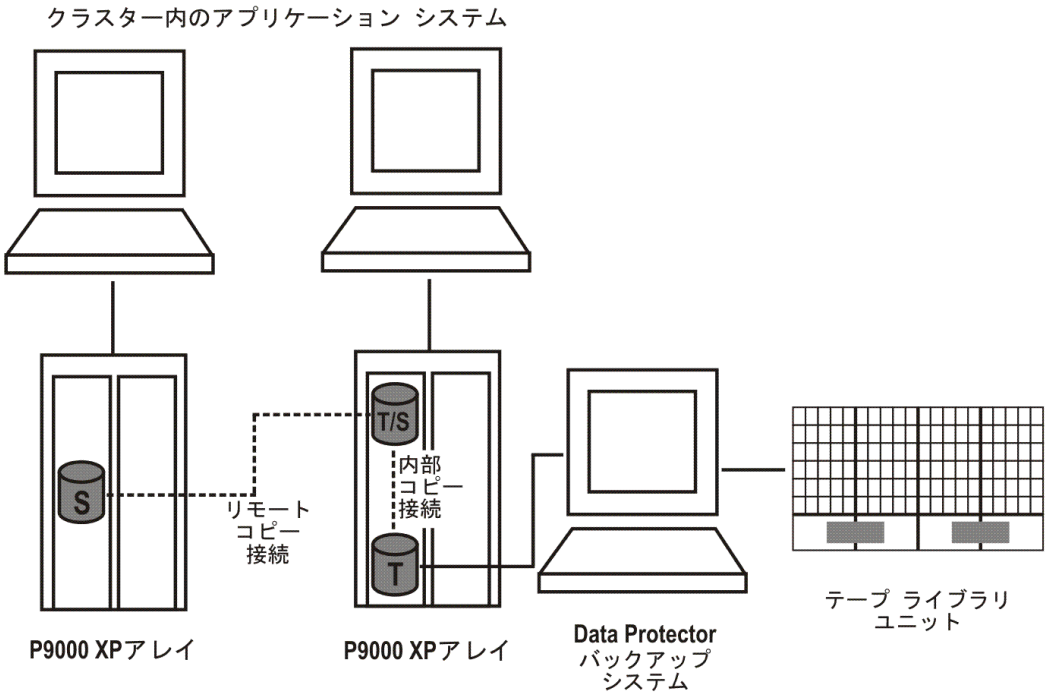
HPE CA+BC P9000 XP構 成4



クラスター構 成

次 の図 は、クラスター内 のHPE CA+BC P9000 XPアレイ構 成 の例 です。

クラスター内 のHPE CA+BC P9000 XP構 成



クラスター構 成 の詳 細 については、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参 照 してください。

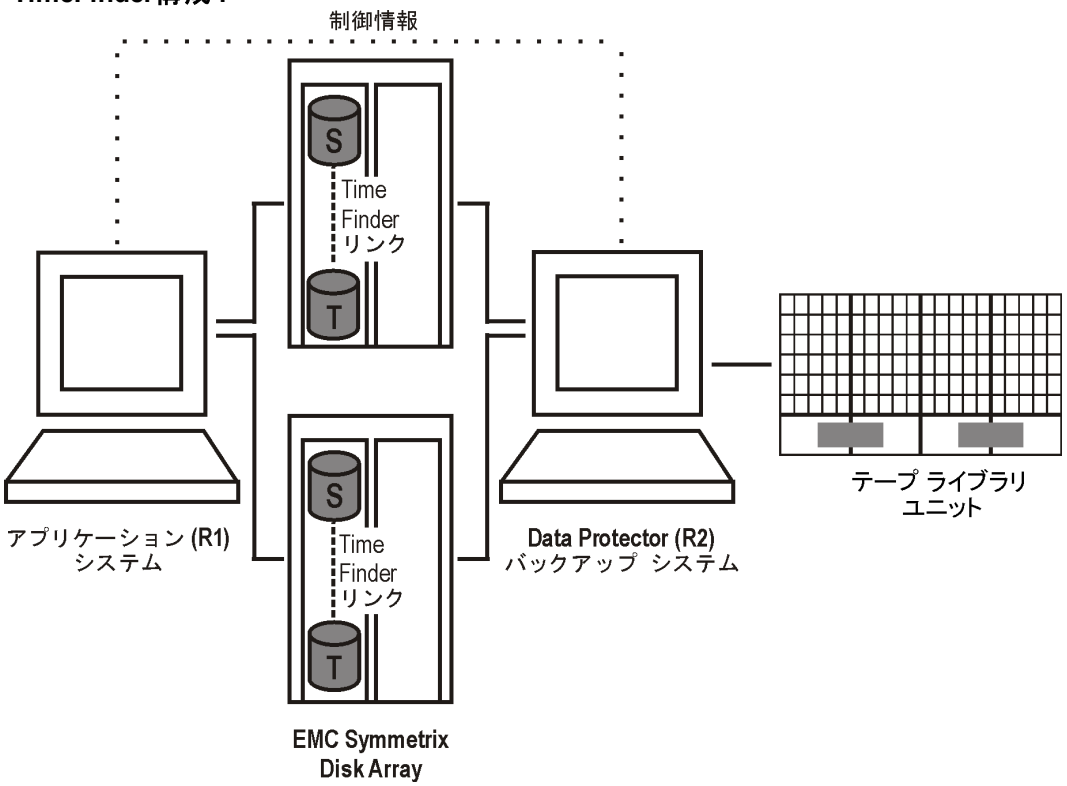
サポートされているEMC Symmetrix構 成

ローカル複 製 の構 成

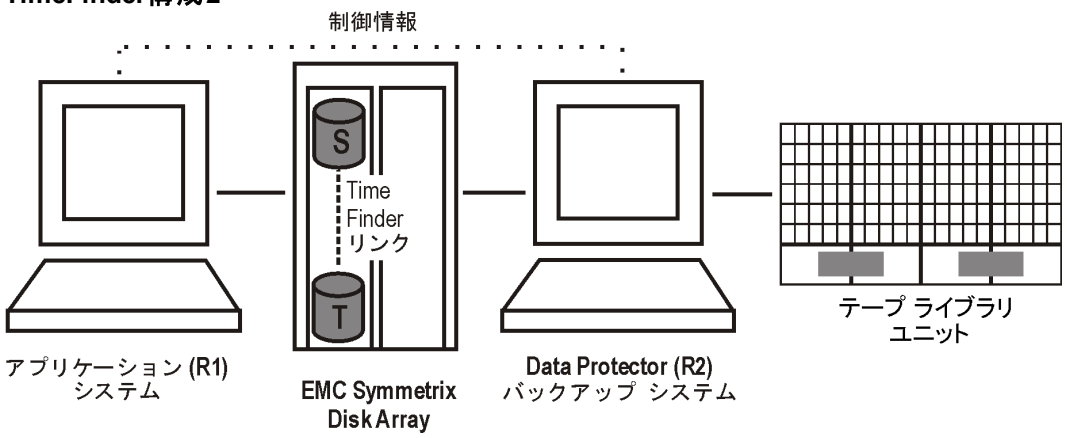
ローカル複 製 の場 合 は、**EMC Symmetrix TimeFinder構 成**を使 用 します。

TimeFinder構 成 1、下 ～ TimeFinder構 成 3、次 のページは、EMCでサポートされているローカル複 製 の構 成 の例 です。

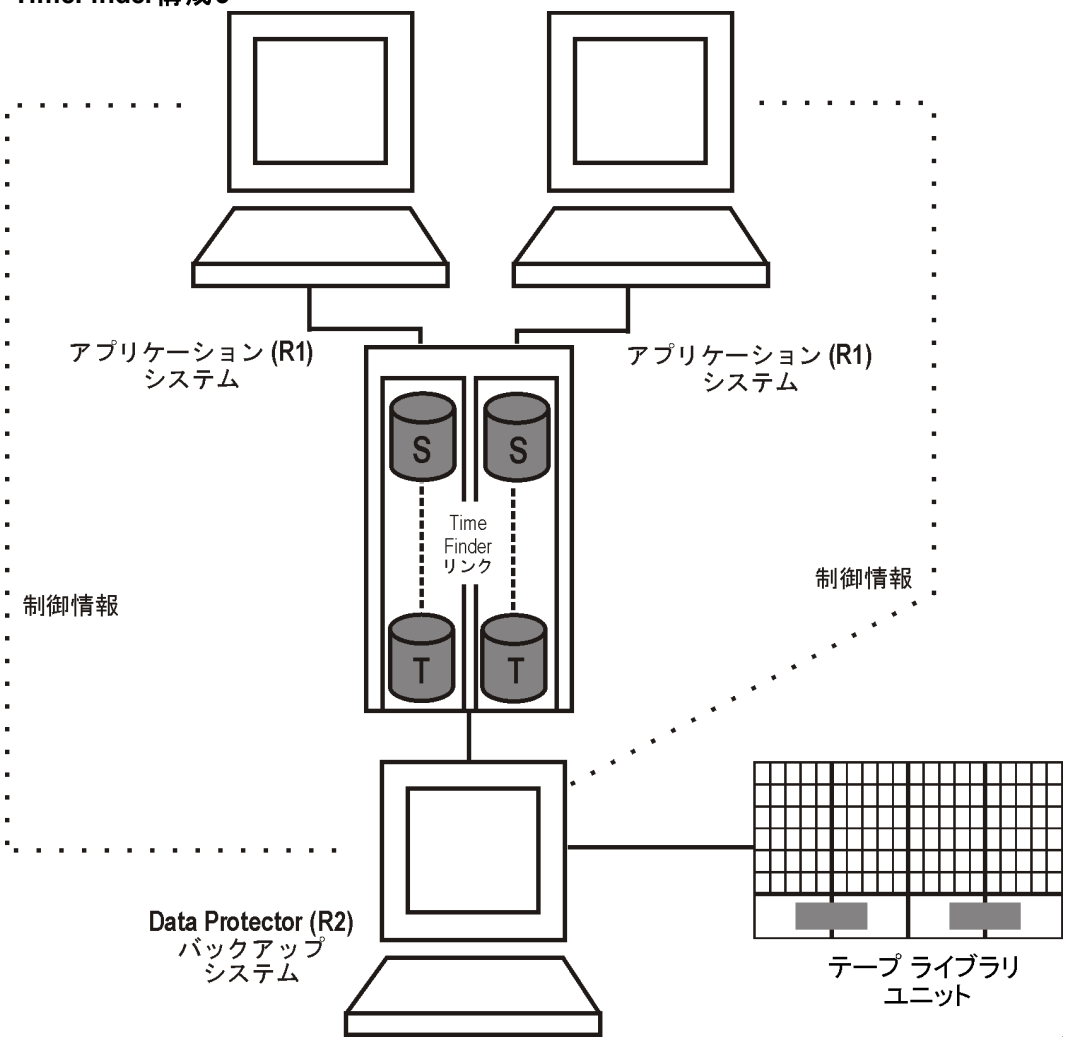
TimeFinder構 成 1



TimeFinder構 成 2



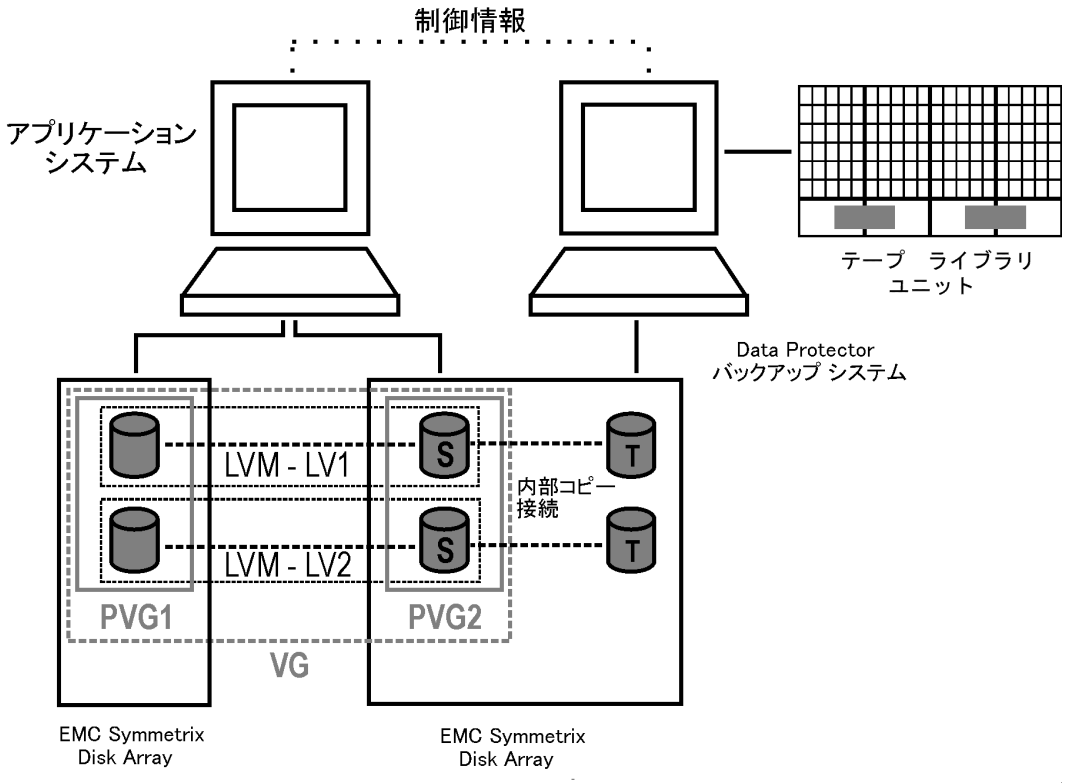
TimeFinder構 成3



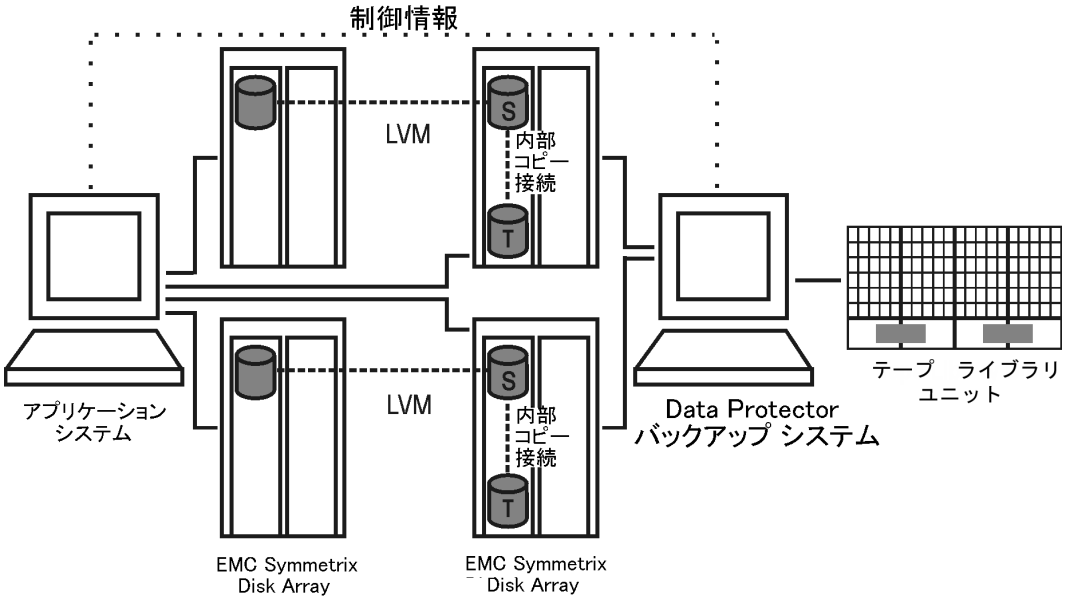
ローカル複 製 の構 成 とHP-UX LVMミラー

LVMミラー構 成 1、下 ～ LVMミラー構 成 5、ページ 302は、EMCでサポートされているLVMミラーの構 成 の例 です。

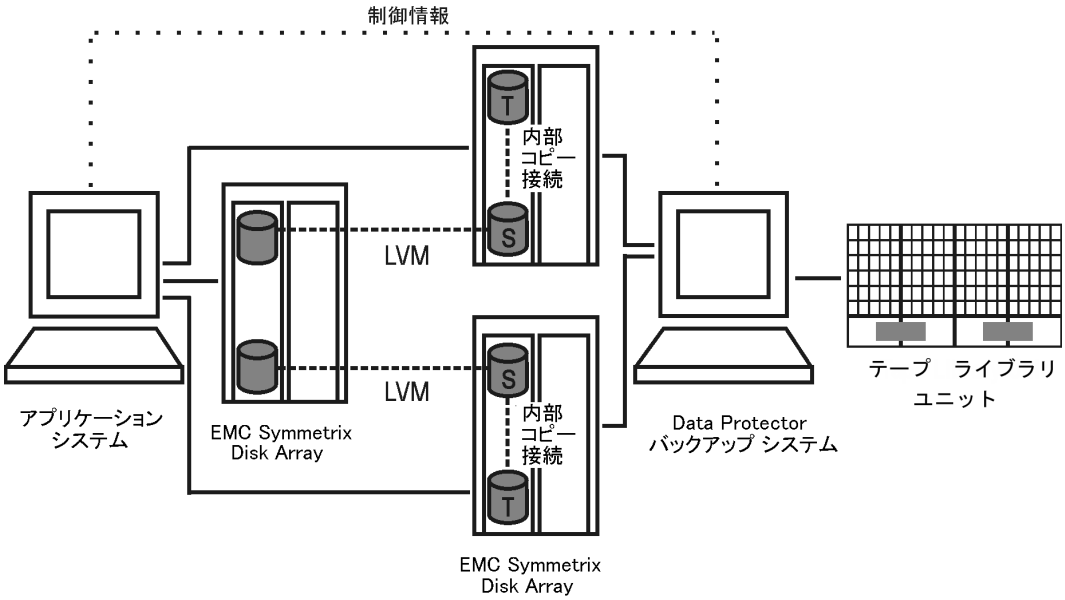
LVMミラー構 成 1



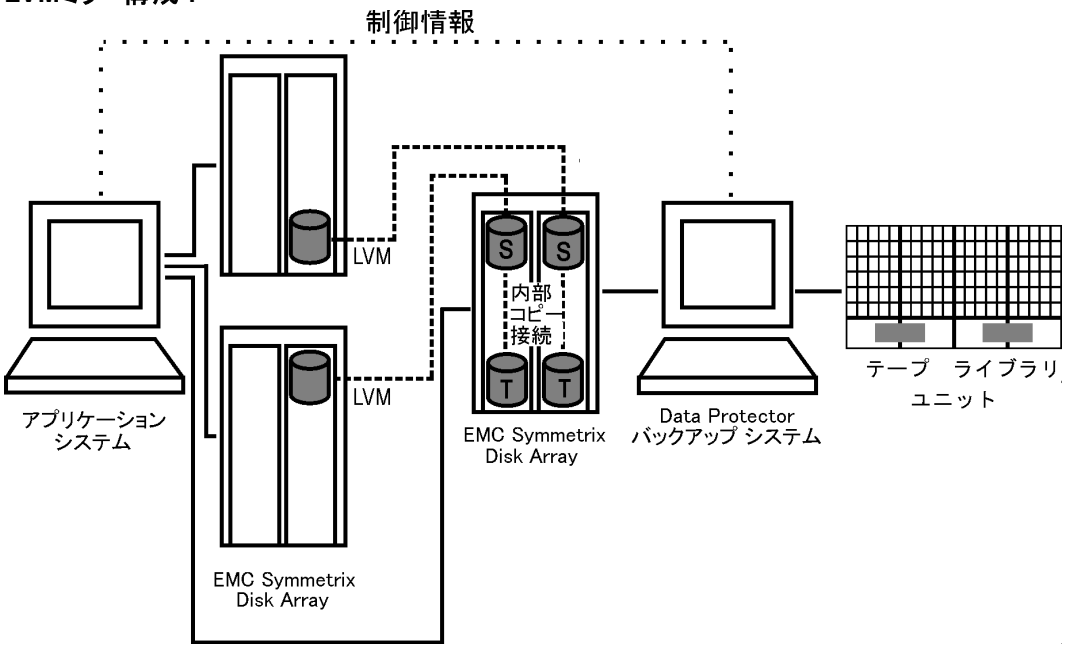
LVMミラー構 成2



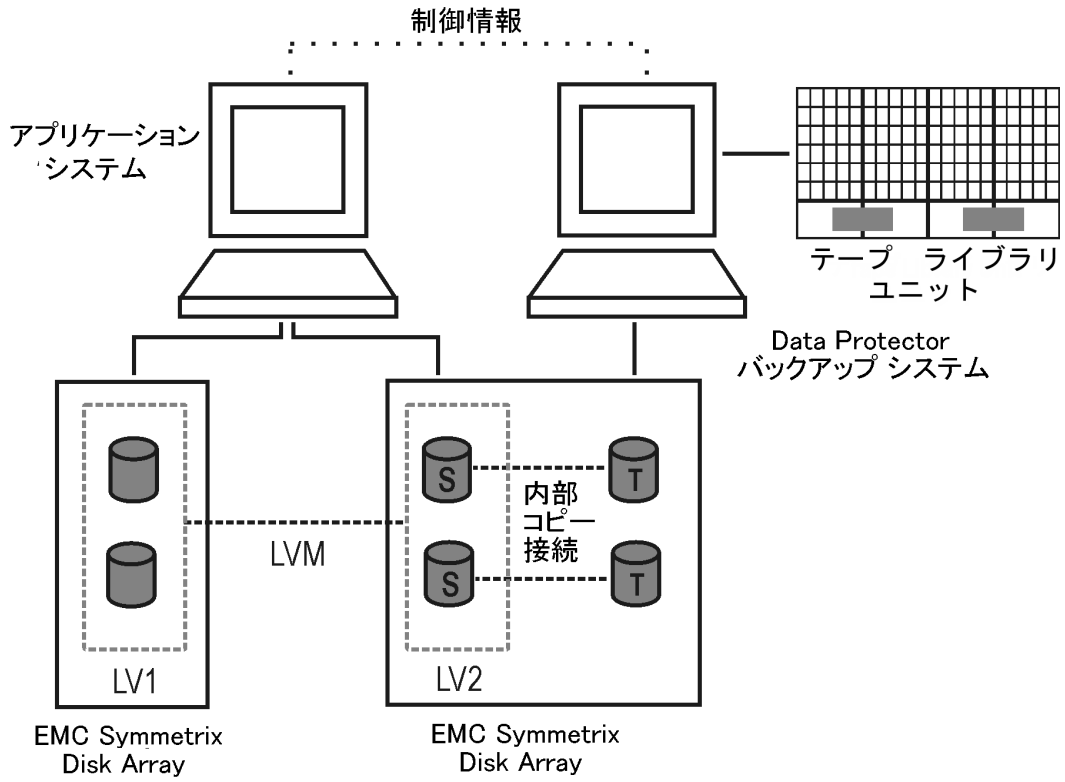
LVMミラー構 成3



LVMミラー構 成4



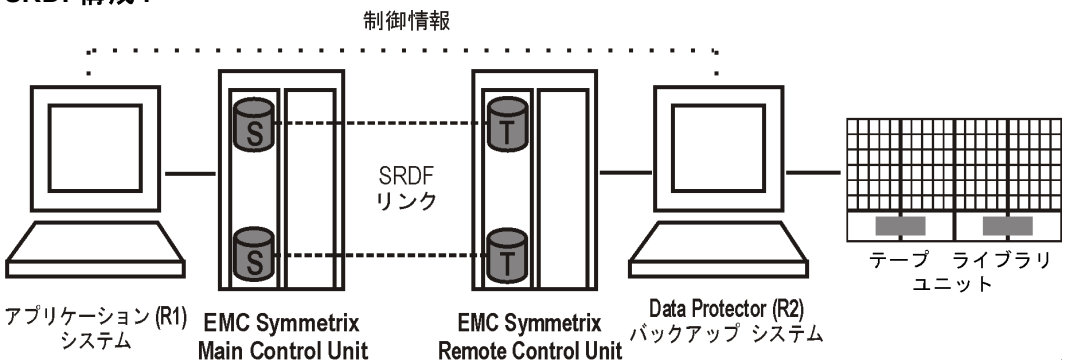
LVMミラー構 成5



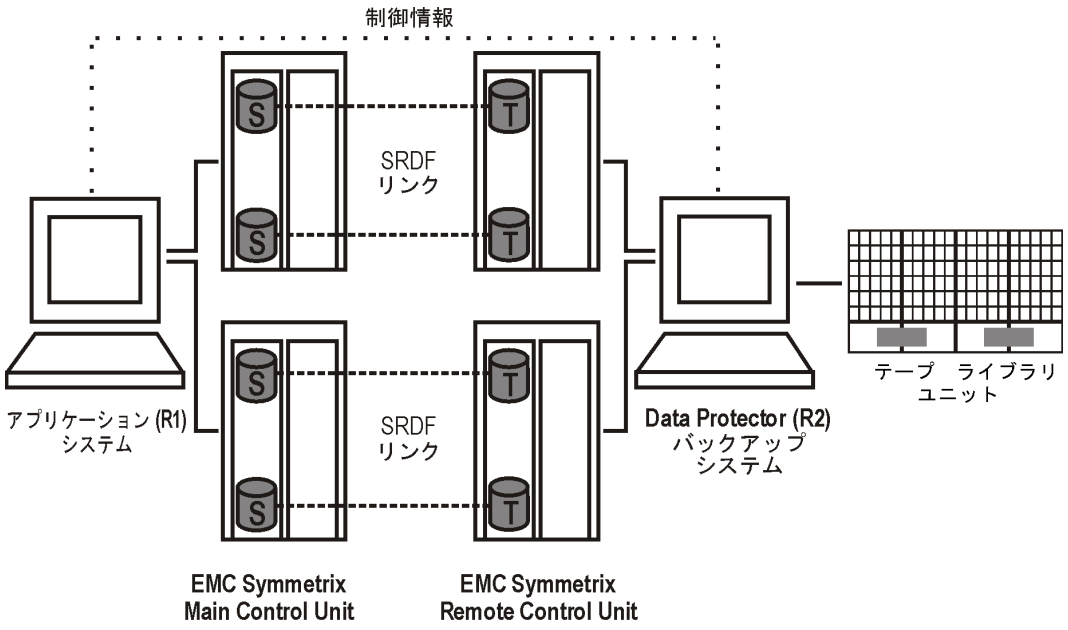
リモート複 製 の構 成

SRDF構 成 1、下 ～ サポートされているEMC Symmetrix構 成 、ページ 299は、EMCでサポートされている リモート複 製 の構 成 の例 です。

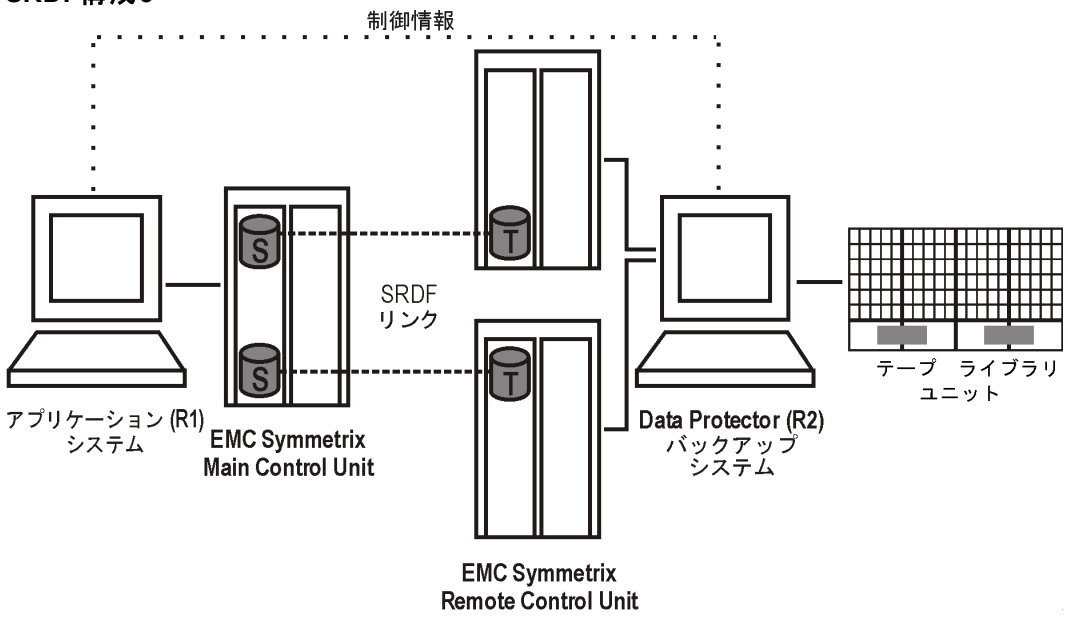
SRDF構 成 1



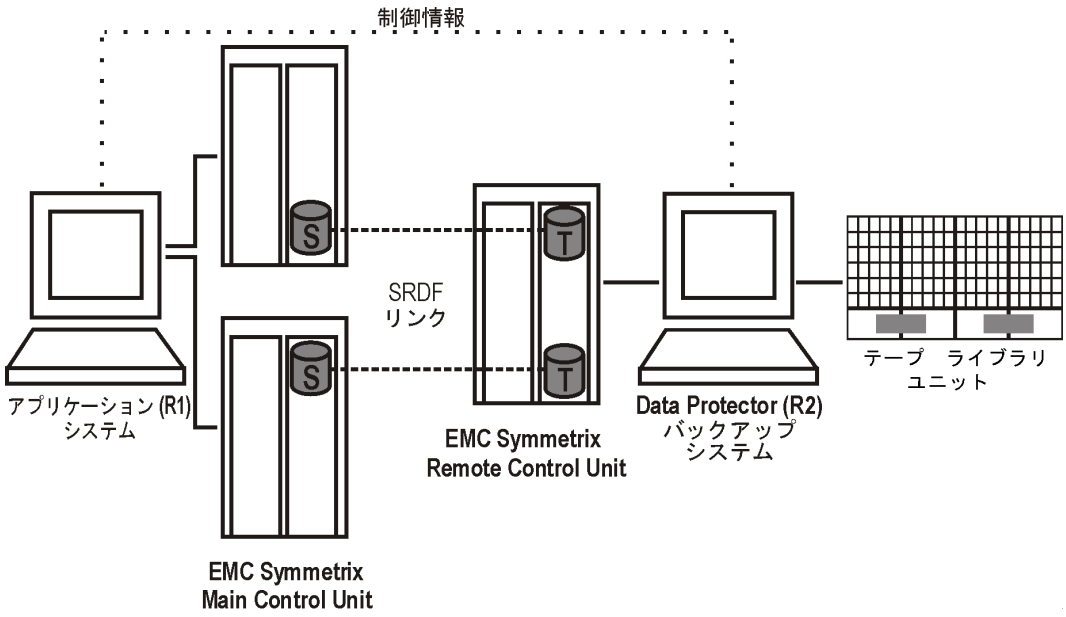
SRDF構 成 2



SRDF構 成3



SRDF構 成4

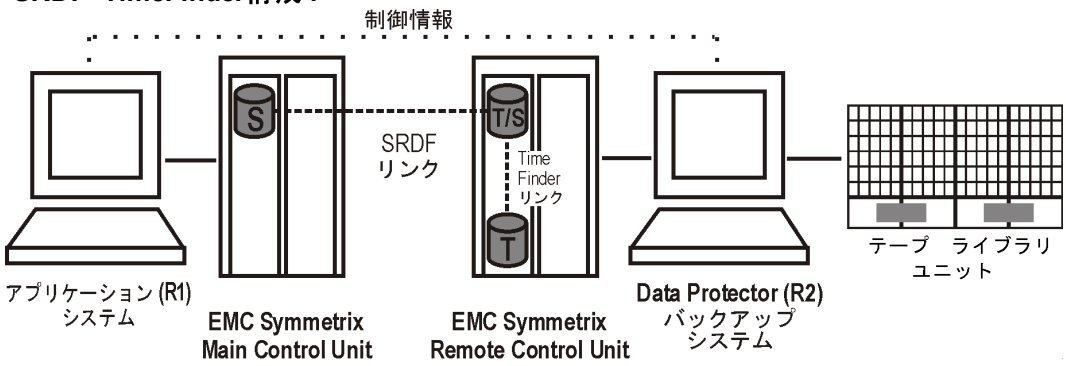


リモートプラスローカル複製の構成

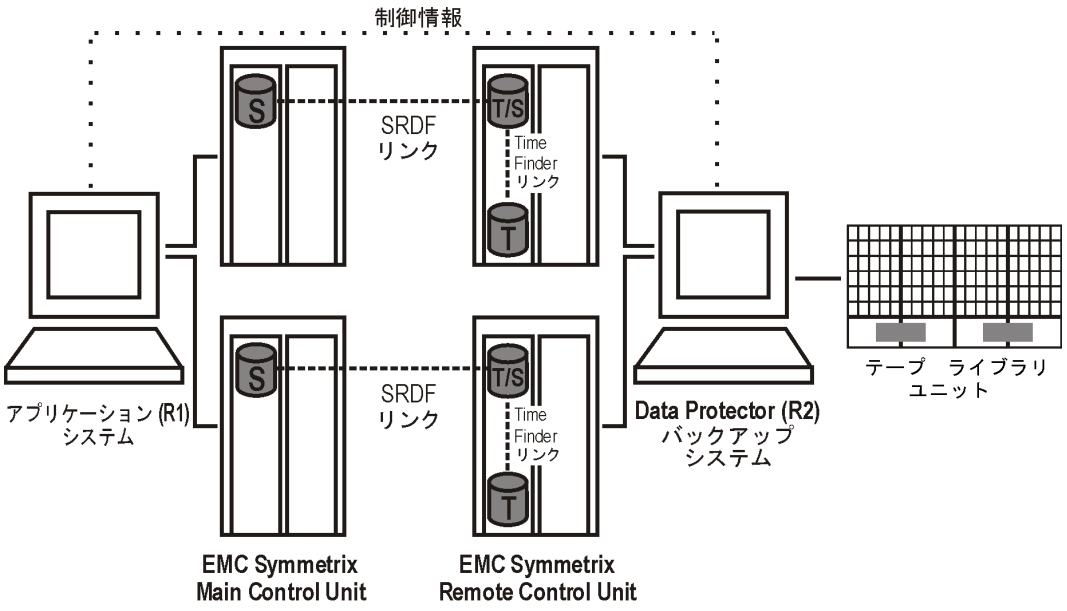
バックアップシステムにはTimeFinderターゲットボリュームのみを接続することをお勧めします。何らかの理由でSRDFターゲットボリュームも接続する場合は、特別な注意が必要です。詳細については、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参照してください。

SRDF+TimeFinder構成1、下 ～ SRDF+TimeFinder構成4、次のページは、EMCでサポートされているリモートプラスローカル複製の構成の例です。

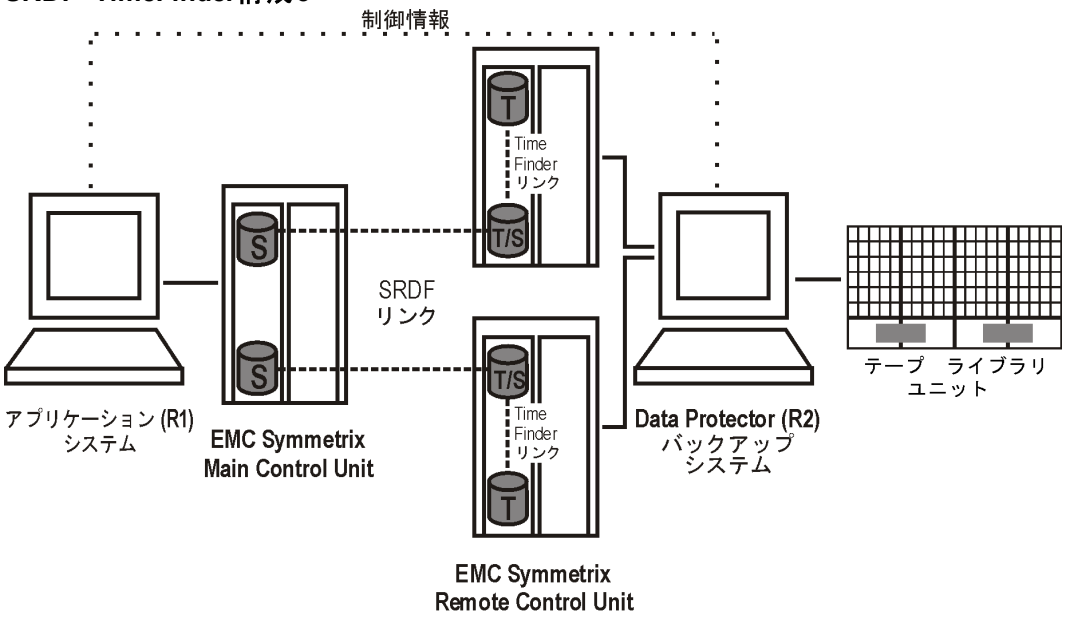
SRDF+TimeFinder構成1



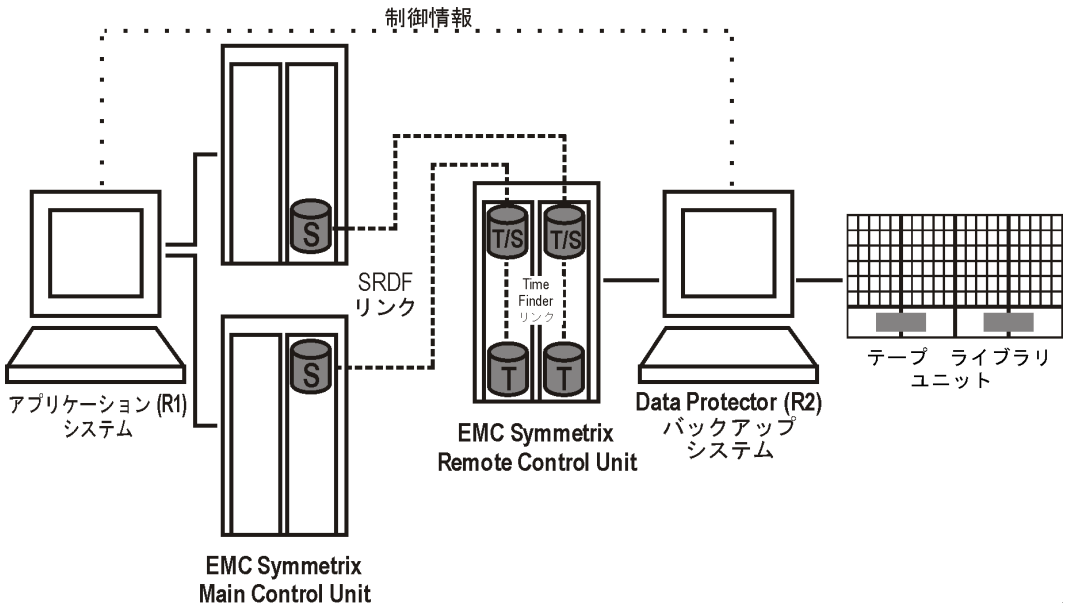
SRDF+TimeFinder構成2



SRDF+TimeFinder構 成 3



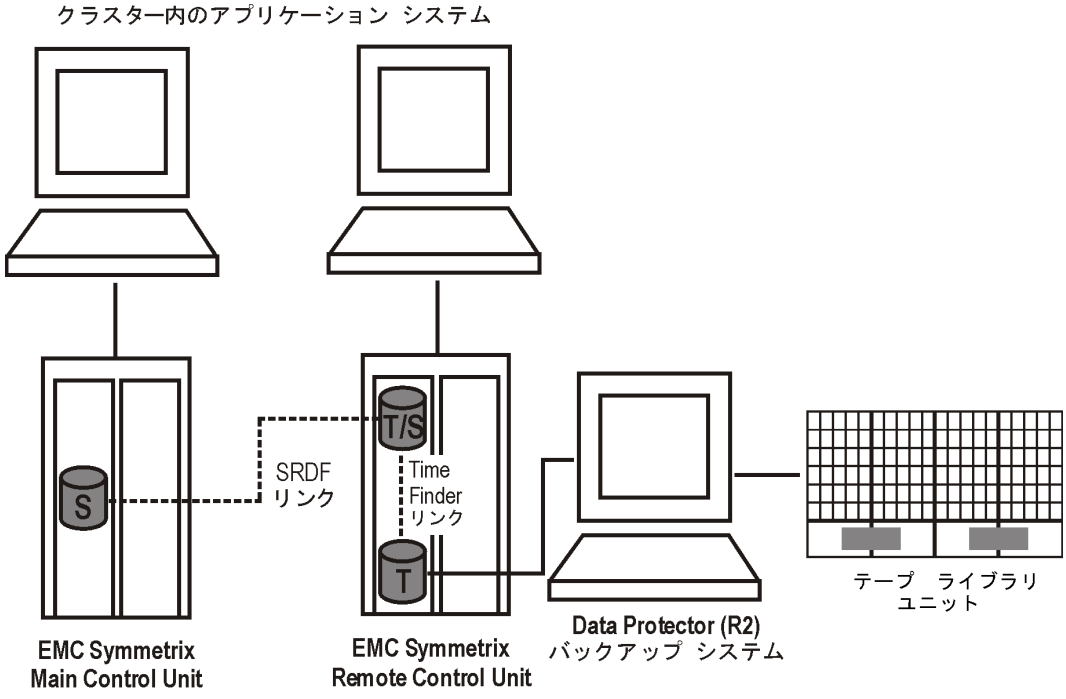
SRDF+TimeFinder構 成 4



クラスター構 成

次 の図 は、クラスターでのSRDF+TimeFinder構 成 の例 です。

クラスターでのSRDF+TimeFinder構 成



クラスター構 成 の詳 細 については、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』を参 照 してください。

サポートされているHACMPクラスター構成

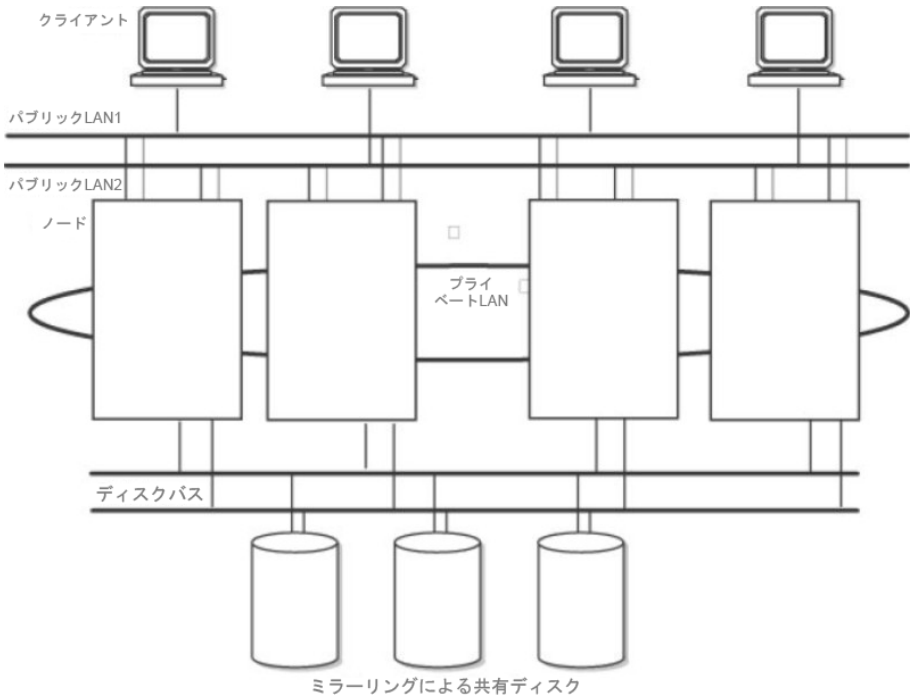
HACMPソフトウェアは、UNIXベースのミッションクリティカルなコンピューター環境を構築するためのIBMのソリューションで、高可用性(HA)とクラスターのマルチプロセッシング(CMP)に基づいています。これは、アプリケーションなどの重要なリソースを確実に処理できるようにします。

HACMPクラスターを作成する主な理由は、ミッションクリティカルなアプリケーションに対して可用性の高い環境を提供することです。たとえば、HACMPクラスターでは、クライアントアプリケーションにサービスを提供するデータベースサーバープログラムを実行できます。クライアントがサーバープログラムにクエリを送信すると、サーバープログラムは共有外部ディスクに格納されているデータベースにアクセスして、要求に応答します。

HACMPクラスター内でアプリケーションを確実に使用できるように、アプリケーションはHACMP制御化に置きます。HACMPは、クラスター内のコンポーネントに障害が発生した場合でも、アプリケーションが引き続きクライアントプロセスを処理できるようにします。コンポーネントに障害が発生した場合、HACMPは、アプリケーションおよびアプリケーションにアクセスするために必要なリソースをクラスター内の別のノードに移動します。

クラスター全体は、ネットワーク上のHACMPクラスター全体を表す仮想サーバー名(仮想環境のドメイン名)を介してアクセスされます。

一般的なHACMPクラスターの設定



図からわかるように、HACMPクラスターは次の物理コンポーネントから構成されています。

- ノード
- 共有外部ディスクインターフェイス
- ネットワーク

- ネットワークインターフェイス
- クライアント

ノード

ノードはHACMPクラスターの中核を形成します。各ノードは一意の名前で識別され、AIXオペレーティングシステム、HACMPソフトウェア、およびアプリケーションソフトウェアを実行するプロセッサーが含まれています。1つのノードが、一連のリソースディスク、ボリュームグループ、ファイルシステム、ネットワーク、ネットワークアドレス、およびアプリケーションを所有することができます。

共有外部ディスクインターフェイス

各ノードは、1つまたは複数の共有外部ディスクデバイス(複数のノードに物理的に接続されているディスク)にアクセスできます。共有ディスクには、ミッションクリティカルなデータ(一般には、データ冗長性用にミラー化またはRAID構成されたデータ)が格納されます。HACMPクラスター内のノードには、オペレーティングシステムおよびアプリケーションのバイナリデータを格納する内部ディスクもありますが、これらのディスクは共有されません。

ネットワーク

HACMPソフトウェアは、AIXオペレーティングシステムの独立した階層化コンポーネントとしてTCP/IPベースのネットワークで動作するように設計されています。ノードはネットワークを介して、次のことを行います。

- クライアントがクラスターノードにアクセスできるようにする。
- クラスターノードがハードビートメッセージをやり取りできるようにする。
- データへのアクセスを逐次化する(同時アクセス環境の場合)。

HACMPソフトウェアが定義する通信ネットワークは2種類あります。これは、使用している通信インターフェイスがTCP/IPサブシステムに基づくTCP/IPベースであるか、または非TCP/IPサブシステムに基づくデバイスベースであるかで決まります。

クライアント

クライアントは、クラスター内のノードにLAN経由でアクセスできるプロセッサーです。クライアントは、"フロントエンド"アプリケーションまたはクライアントアプリケーションを実行して、

クラスターノード上で実行しているアプリケーションをサーバーに照会します。

StoreOnce CatalystデバイスとVTLデバイスのパフォーマンスベンチマーク

環境:

- 使用されるStoreOnce重複排除システムは、B4210単一ノード物理デバイスです。各テストケース用に別個のストアが作成されます。
- Cell Managerは、Windows Server 2008物理サーバーです。
- Disk Agentは、500 GBのバックアップ対象データを持つWindows Server 2008サーバーです(データを別のサーバーに送信する場合)。
- Media Agentは、Windows、CentOSおよびHP-UXオペレーティングシステムの3つの異なるサーバーにインストールされています。
- Data Protectorパッチバンドル9.04を使用して、このテストを実施しました。

			Disk AgentとMedia Agentが同一サーバー上に存在	**同一ネットワーク内の異なるサーバー上のDisk AgentとMedia Agent**
バックアップデータ	**種類**	**ゲートウェイ**	**時間(時間:分:秒)**	**時間(時間:分:秒)**
500 GB	Catalyst over Ethernet	Windows	1:32:0 (90.57 MB/s)	2:27:12 (56.61 MB/s)
500 GB	Catalyst over Fibre Channel		1:47:55 (77.22 MB/s)	2:34:17 (54.01 MB/s)
500 GB	VTL		1:41:24 (82.18 MB/s)	2:37:54 (52.77 MB/s)
500 GB	Catalyst over Ethernet	CentOS	58:30 (142.45 MB/s)	1:52:21 (74.17 MB/s)
500 GB	Catalyst over Fibre Channel		1:23:11 (100.18 MB/s)	1:52:25 (74.12 MB/s)
500 GB	VTL		1:45:13 (79.20 MB/s)	1:56:45 (71.37 MB/s)
500 GB	Catalyst over Ethernet	HP-UX	59:34 (139.89 MB/s)	3:0:7 (46.26 MB/s)

500 GB	Catalyst over Fibre Channel		1:53:42 (73.29 MB/s)	3:04:54 (45.06 MB/s)
500 GB	VTL		1:48:30 (76.80 MB/s)	3:43:34 (37.27 MB/s)

フィードバックを送信

このドキュメントに関するご意見は、ドキュメンテーションチームまで電子メールでお送りください。お使いのシステムに電子メールクライアントが設定されている場合は、上のリンクをクリックすると、電子メールウィンドウが開き、件名行に次の情報が入力されます。

コンセプトガイド (Data Protector 10.00)に関するフィードバック

本文にご意見、ご感想を記入の上、**[送信]**をクリックしてください。

電子メールクライアントが利用できない場合は、上記の情報をコピーしてWebメールクライアントの新規メッセージに貼り付け、AutonomyTPFeedback@hpe.com宛にお送りください。

お客様からのご意見、ご感想をお待ちしています。