HP OpenView Storage Data Protector
コンセプト・ガイド

出版年月 **: 2004** 年 **10** 月

Manufacturing Part Number : B6960-99105

リリース **A.05.50**

ご注意

1. 本書に記載した内容は、予告なしに変更することがあります。
2. 当社は、本書に関して特定目的の市場性と適合性に対する保証を含む一切の保証をいたしかねます。
3. 当社は、本書の記載事項の誤り、またはマテリアルの提供、性能、使用により発生した 損害については責任を負いかねますのでご了承ください。
4. 本製品パッケージとして提供した本書、CD-ROM などの媒体は本製品用だけにお使いください。プログラムをコピーする場合はバックアップ用だけにしてください。プログラムをそのままの形で、あるいは変更を加えて第三者に販売することは固く禁じられています。

目次

1. バックアップと Data Protector

2. バックアップ方針の策定

目次

3. メディア管理とデバイス

出版履歴

マニュアルの出版の日付と部品番号は、そのマニュアルの最新の版数を示しています。出版の日付は、最新版ができるたびに変更します。内容の小さな変更に対しては、増刷の際に対応し、出版日の変更は行いません。マニュアルの部品番号は、改訂が行われるたびに変更します。

新版の作成は、記載内容の訂正またはドキュメント製品の変更にともなって行われます。お手元のマニュアルが最新のものか否かは、当社の営業担当または購入された販売会社にお問い合わせください。詳細については、HP の営業担当にお問い合わせください。

表 1　出版履歴

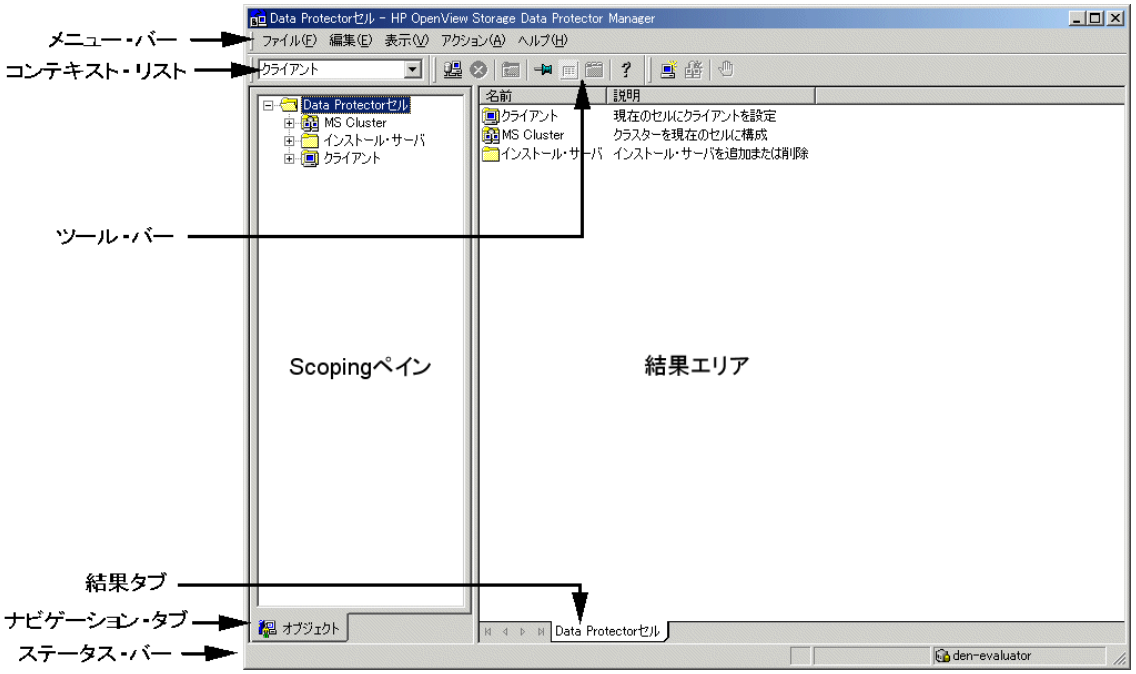
部品番号	出版年月	製品
B6960-99080	2003 年 6 月	Data Protector リリース A.05.10
B6960-99105	2004 年 10 月	Data Protector リリース A.05.50

表記法

字体	説明	例
『マニュアル』	マニュアル名または書籍名	詳細は、『*HP OpenView Storage Data Protector インテグレーション ガイド*』を参照してください。
Italic	コマンドの入力時に指定する必要がある変数	プロンプトで、次のように入力します。 rlogin *your_name* このとき、*your_name* にはログイン名を指定します。
Bold、**ゴシック体**	用語	Data Protector **Cell Manager** は ...
入力	ユーザーが入力する必要があるテキスト	プロンプトで、次のように入力します。**ls -l**
コンピュータ文字	コンピュータディスプレイの項目	次のシステムメッセージが表示されます。 Are you sure you want to remove current group?
	コマンド名	grep コマンドを使用して、...
	ファイル名とディレクトリ名	/usr/bin/X11
	プロセス名	Data Protector Inet が実行中かどうかチェックします。
	ウィンドウ / ダイアログボックス名	[**バックアップ・オプション**] ダイアログ・ボックスで ...
	マン・ページ名	詳細は、omnib のマン・ページを参照してください。
強調	強調表示	次の手順に従う*必要があります*。
キーキャップ	キーボードのキー	**Return** を押します。
[**ボタン**]	ユーザーインタフェースのボタン	[OK] をクリックします。 [**適用**] ボタンをクリックします。

Data Protector では、クロスプラットフォーム (Windows と UNIX) のグラフィカル・ユーザー・インタフェースを提供します。Data Protector のグラフィカル・ユーザー・インタフェースについては、『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。

図 1　　Data Protector グラフィカル・ユーザー・インタフェース



当社へのお問い合わせについて

概要

Data Protector の概要については、以下の Web サイトでご覧いただけます。

http://www.hp.com/go/dataprotector (英語版)
http://h50146.www5.hp.com/products/storage/software/dataprotector/index.html (日本語版)

テクニカル サポート

テクニカル サポート情報については、HP エレクトロニック サポート センタの下記の Web サイトをご覧ください。

http://support.openview.hp.com/support.jsp

http://www.hp.com/support

Data Protector の最新のパッチ情報については、以下をご覧ください。

http://support.openview.hp.com/patches/patch_index.jsp

Data Protector に必要なパッチ情報は、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』を参照してください。

当社では他社製のハードウェアおよびソフトウェアのサポートは行っておりません。他社製製品のサポートは各ベンダーにお問い合わせください。

ドキュメントに関するご意見

ドキュメントに関するお客様のご意見を基に、お客様のご要望を理解し、ご要望に沿ったドキュメントの開発に努めていきたいと思っております。ドキュメントに関するご意見は、当社の以下のドキュメント専用サイトへお送りください。

http://ovweb.external.hp.com/lpe/doc_serv/ (英語版)
http://welcome.hp.com/country/jp/ja/contact_us.html (日本語版)

トレーニング情報

HP OpenView に関して現在可能なトレーニングの情報については、下記の HP OpenView の Web サイトをご覧ください。

http://www.openview.hp.com/training/ (米国)
http://www.hp.com/jp/education (日本)

上記のサイトにリンクすると、トレーニング クラスのスケジュールや、カスタマ サイトでのトレーニング、クラス登録などに関する情報をご覧いただけます。

Data Protector のドキュメント

Data Protector のドキュメントは、マニュアルとオンライン・ヘルプの形式で提供されます。

マニュアル

Data Protector のマニュアルは印刷形式と PDF 形式で提供されます。PDF ファイルは Data Protector のセットアップ時に Windows の場合は User Interface コンポーネントを、UNIX の場合は OB2-DOCS コンポーネントを選択してインストールします。PDF ファイルをインストールすると、マニュアルは Windows では *<Data_Protector_home>*¥docs ディレクトリ、UNIX では、/opt/omni/doc/ja (日本語版)、/opt/omni/doc/C/ (英語版) ディレクトリに保存されます。また以下の URL でも PDF 形式のマニュアルを入手できます。
http://ovweb.external.hp.com/lpe/doc_serv/ (英語版)
http://www.hp.com/jp/manual/ (日本語版)

『*HP OpenView Storage Data Protector コンセプト・ガイド*』

このマニュアルでは、Data Protector のコンセプトを解説するとともに、Data Protector の動作原理を詳細に説明しています。手順を中心に説明している『*HP OpenView Storage Data Protector 管理者ガイド*』と併せてお読みください。

『*HP OpenView Storage Data Protector 管理者ガイド*』

このマニュアルでは、バックアップ管理者が実行する主な構成および管理作業 (デバイスの構成、メディアの管理、バックアップの構成、データの復元など) について説明します。

『*HP OpenView Storage Data Protector インストールおよびライセンス・ガイド*』

このマニュアルでは、お使いの環境のオペレーティング・システムとアーキテクチャを考慮した上での Data Protector ソフトウェアのインストール方法を説明しています。また、Data Protector のアップグレード方法や、環境に適したライセンスの取得方法についても説明しています。

『*HP OpenView Storage Data Protector インテグレーション ガイド*』

このマニュアルでは、さまざまなデータベースやアプリケーションをバックアップ / 復元するための Data Protector の構成 / 使用方法を説明しています。このマニュアルは、バックアップ管理者やオペレータを対象としています。このマニュアルには以下の 4 種類のバージョンが提供されています。

- 『*HP OpenView Storage Data Protector インテグレーション ガイド - Microsoft アプリケーション: SQL Server 7/2000*、*Exchange Server 5.x*、*Exchange Server 2000/2003*、*Volume Shadow Copy Service*』

  このマニュアルでは、Microsoft アプリケーション (Microsoft Exchange Server 2000/2003、Microsoft Exchange Server 5.x、Microsoft SQL Server 7/2000、および Volume Shadow Copy Service) に対応する Data Protector の統合ソフトウェアついて説明します。

- 『*HP OpenView Storage Data Protector インテグレーション ガイド - Oracle*、*SAP*』

  このマニュアルでは、Oracle、SAP R3、SAP DB に対応する Data Protector の統合ソフトウェアについて説明します。

- 『*HP OpenView Storage Data Protector インテグレーション ガイド - IBM アプリケーション: Informix*、*DB2*、*Lotus Notes/Domino*』

  このマニュアルでは、IBM のアプリケーション (Informix、IBM DB2、および Lotus Notes/Domino) に対応する Data Protector の統合ソフトウェアについて説明します。

- 『*HP OpenView Storage Data Protector インテグレーション ガイド - Sybase*、*Network Node Manager*、*Network Data Management Protocol*』

  このマニュアルでは、Sybase、Network Node Manager および Network Data Management Protocol に対応する Data Protector の統合ソフトウェアについて説明します。

『HP OpenView Storage Data Protector Integration Guide for HP OpenView』

このマニュアルでは、HP OpenView Service Information Portal、HP OpenView Service Desk および HP OpenView Reporter に対応する Data Protector 統合ソフトウェアのインストール、構成、使用方法について説明します。このマニュアルは、バックアップ管理者を対象としています。OpenView アプリケーションを使用して Data Protector のサービス管理を行う方法を説明します。

『HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations for UNIX』

このマニュアルでは、UNIX 版の HP OpenView Operations (OVO)、HP OpenView Service Navigator、および HP OpenView Performance (OVP) にを使用して Data Protector 環境の健全性と性能を監視 / 管理する方法について説明します。

『HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations for Windows』

このマニュアルでは、Windows 版の HP OpenView Operations (OVO)、HP OpenView Service Navigator、および HP OpenView Performance (OVP) にを使用して Data Protector 環境の健全性と性能を監視 / 管理する方法について説明します。

『*HP OpenView Storage Data Protector ゼロ ダウンタイム バックアップ コンセプト ガイド*』

このマニュアルでは、Data Protector ゼロ ダウンタイム バックアップとインスタント・リカバリのコンセプトについて解説するとともに、ゼロ ダウンタイム バックアップ環境における Data Protector の動作原理を詳細に説明します。手順を中心に説明している『*HP OpenView Storage Data Protector ゼロ ダウンタイム バックアップ 管理者ガイド*』および『*HP OpenView Storage Data Protector ゼロ ダウンタイム バックアップ インテグレーション ガイド*』と併せてお読みください。

『*HP OpenView Storage Data Protector ゼロ ダウンタイム バックアップ 管理者ガイド*』

このマニュアルでは、HP StorageWorks Virtual Array、HP StorageWorks Enterprise Virtual Array、EMC Symmetrix Remote Data Facility および TimeFinder、HP StorageWorks Disk Array XP に対応する Data Protector 統合ソフトウェアのインストール、構成、使用方法について説明します。このマニュアルは、バックアップ管理者やオペレータを対象としています。ファイルシステムやディスク イメージのゼロ ダウンタイム バックアップ、インスタント・リカバリおよび復元についても説明します。

『*HP OpenView Storage Data Protector ゼロ ダウンタイム バックアップ インテグレーション ガイド*』

このマニュアルでは、Oracle、SAP R/3、Microsoft Exchange Server 2000/2003、および Microsoft SQL Server 2000 データベースのゼロ ダウンタイム バックアップ、インスタント・リカバリ、および標準復元を行うための、Data Protector の構成方法および使用法について説明します。また、Microsoft Volume Shadow Copy Service を使用してバックアップおよび復元を行うための、Data Protector の構成方法および使用法についても説明します。

『*HP OpenView Storage Data Protector MPE/iX System User Guide*』

このマニュアルでは、MPE/iX クライアントの構成方法と MPE/iX データのバックアップおよび復元方法を説明します。

『*HP OpenView Storage Data Protector Media Operations User's Guide*』

このマニュアルでは、オフラインのストレージ・メディアの追跡方法と管理方法を説明します。このマニュアルは、システムの保守とバックアップを担当するネットワーク管理者を対象としています。アプリケーションのインストールと構成、日常のメディア操作、およびレポート作成のタスクについて説明します。

『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』

このマニュアルでは、HP OpenView Storage Data Protector A.05.50 の新機能を説明しています。また、サポートされる構成 (デバイス、プラットフォーム、オンライン データベースの統合、SAN、ZDB)、必要なパッチ、制限事項、既知の問題と対応策についても説明しています。サポートされる構成の 最新情報については以下の URL を参照してください。
http://www.openview.hp.com/products/datapro/spec_0001.html (英語)

オンライン・ヘルプ

Data Protector は Windows および UNIX の各プラットフォーム用にオンライン・ヘルプ (コンテキスト依存ヘルプ ([F1] キー) および [ヘルプ] トピック) を備えています。

本書について

『*HP OpenView Storage Data Protector コンセプト・ガイド*』は Data Protector の概念について説明したものです。このマニュアルに目を通し、Data Protector の基礎知識と基準について十分に熟知してください。

対象読者

本書は、Data Protector 機能の概念を紹介し、企業におけるバックアップ方針の構築にお役立ていただくことを目的としています。より詳しい作業手順については、本書と併せて『*HP OpenView Storage Data Protector 管理者ガイド*』をご覧ください。

本章の構成

本書は、以下の章で構成されています。

第 1 章 1 ページの「バックアップと Data Protector」

第 2 章 27 ページの「バックアップ方針の策定」

第 3 章 123 ページの「メディア管理とデバイス」

第 4 章 179 ページの「ユーザーとユーザー・グループ」

第 5 章 185 ページの「Data Protector 内部データベース」

第 6 章 213 ページの「サービス管理」

第 7 章 233 ページの「Data Protector が機能する仕組み」

第 8 章 251 ページの「データベース・アプリケーションとの統合」

第 9 章 259 ページの「ダイレクト・バックアップ」

第 10 章 273 ページの「ディスク・バックアップ」

第 11 章 281 ページの「スプリット・ミラーの概念」

第 12 章 293 ページの「スナップショットの概念」

第 13 章 307 ページの「Microsoft Volume Shadow Copy サービス」

付録 A 319 ページの「バックアップ・シナリオ」

付録 B 359 ページの「その他の情報」

用語集 本書で使用する用語の定義

1 バックアップと Data Protector

本章の内容

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、メディア管理、ユーザー・インタフェース、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。

この章の構成は以下のとおりです。

Data Protector について

HP OpenView Storage 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。Data Protector の主要な特徴の一覧を以下に示します。

- **拡張性と柔軟性に優れたアーキテクチャ**

  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ー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、事実上どのような形ででも実装することが可能です。さらに、Data Protector では、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。

- **中央管理の容易性**

  Data Protector では、操作性に優れたグラフィック・ユーザー・インタフェース (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。さらに中心となる 1 つのシステムから、複数のバックアップ環境を管理することも可能です。また、Data Protector にはコマンド行インタフェース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。

- **優れたバックアップ性能**

  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ています。さらに、さまざまなバックアップ・タイプがサポートされているため、ユーザー要件に最適なバックアップを実行できます (ローカル・バックアップ、ネットワーク・バックアップ、フル・バックアップ、差分バックアップ、複数レベル増分バックアップ、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、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)。

- **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 と Windows の Cell Manager からは、サポート対象のクライアント・プラットフォームのすべて (UNIX、Windows、および Novell NetWare) を制御できます。Data Protector ユーザー・インタフェースを使用すると、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。

- **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・サーバのプラットフォームとしてサポートされているプラットフォームの一覧は、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』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、24 時間連続で使用される可能性があります。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。サポート対象クラスタの一覧は、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』を参照してください。

  — クラスタ上で 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・インタフェース (API) をサポート。

  — EMC Symmetrix、HP StorageWorks Disk Array XP、HP StorageWorks Virtual Array、HP StorageWorks Enterprise Virtual Array 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、さまざまな障害復旧機能を提供。

  — 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。

- **復元の容易性**

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。

- **自動または無人処理**

  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。例えば、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。この機能を使用すると、バックアップ構成情報を手動で調整する必要がなくなります。

- **サービス管理**

  Data Protector は、バックアップ管理と復元管理のためのソリューションとしては初めてサービス管理機能をサポートしました。Application Response Management (ARM)、および Data Source Integration (DSI) の統合により、システムの管理および設計に必要なデータが提供されるため、サービスレベル管理 (SLM) およびサービスレベル契約 (SLA) の概念が強力にサポートされます。

  この DSI の統合により、スクリプトおよび構成ファイルのセットが提供されるため、ユーザーは Data Protector のレポート機能を使用して、レポートの仕様を追加する場合の指定方法を調べることができます。

- **モニタリング、レポート、および通知機能**

  Web を使用する優れたレポート機能および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。レポートは、Data Protector GUI を使用して作成したり、UNIX または Windows を実行しているシステム上で `omnirpt` コマンドを使用して生成したりすることもできます。さらに、Java ベースのオンライン生成 Web レポートを使用することもできます。

  またレポートは、特定の時間に生成されるように設定しておくこともできれば、バックアップ・セッションの最後やマウント要求時など、事前設定した特定のイベント発生時に生成させることも可能です。

- **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、Oracle、Informix、SAP R/3、Lotus Notes/Domino Server、IBM DB2 UDB、および Sybase のデータベース・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ているバージョンの一覧は、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』を参照してください。

- **その他の製品との統合**

  さらに Data Protector は、EMC Symmetrix、Microsoft Cluster Server、MC/ServiceGuard をはじめとする製品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、以下の HP OpenView Storage Data Protector のホームページでご確認ください。http://www.openview.hp.com/products/datapro/spec_0001.html

バックアップと復元の概要

本項では、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。作成したコピーは、オリジナル・データの破壊や破損に備えて保管しておきます。

バックアップを最も抽象化すると、図 1-1 のような形になります。

図 1-1　　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障害復旧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

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。

図 1-2　　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。

図 1-3　　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。

ダイレクト・バックアップ

ダイレクト・バックアップとは、データを移動するための専用のバックアップ・サーバを使用せずに、SAN 環境でディスクからテープにデータを直接送信するバックアップ方法です。Data Protector のダイレクト・バックアップでは、他の処理への影響が少ないハードウェアベースのミラー化技術を採用することにより、バックアップ処理が実稼動サーバに与える影響を最小限に抑えています。

またこのバックアップ方法では、ファイルシステムに依存しないデータ解決機能が使われます。この機能は、サポート対象のディスク・アレイやブリッジに組み込まれている業界標準の XCOPY 機能と完全に統合されているため、個別のデータ・ムーバ装置を用意する必要はありません。

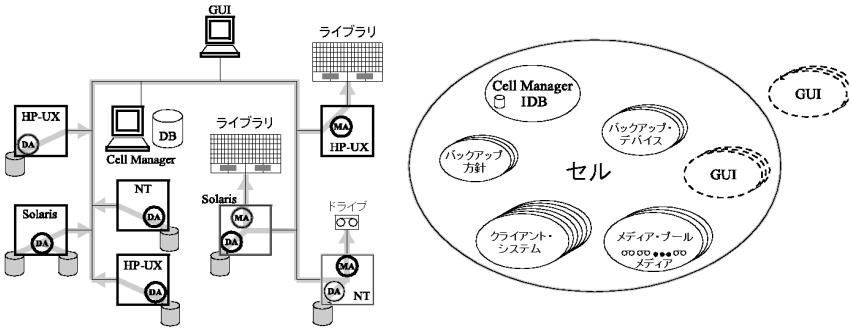
Data Protector アーキテクチャ

Data Protector **セル** (図 1-4 参照) とは、1 つの Cell Manager と、複数の**クライアント・システム**および**デバイス**で構成されるネットワーク環境を指します。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していきます。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・インタフェースを使うと、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。

図 1-4　　Data Protector セル　(物理的な構成図と論理的な構成図)



注記　　GUI と Cell Manager は、UNIX と Windows の各オペレーティング・システムでそれぞれ実行できます。両方を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ているオペレーティング・システムの一覧は、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』を参照してください。

Cell Manager

Cell Manager は、セル内のメイン・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。
- Session Manager を実行します。この Session Manager 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。

バックアップ対象システム

ファイル・システムのバックアップ元となるクライアント・システムには、Data Protector の Disk Agent (DA) をインストールする必要があります。Disk Agent は **Backup Agent** 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。また、Disk Agent を Cell Manager 上にもインストールすることで、Cell Manager 上のデータや、Data Protector の構成情報、IDB などのバックアップも可能になります。

バックアップ・デバイスを接続したシステム

バックアップ・デバイスを接続したクライアント・システムには、Data Protector **Media Agent** (MA) をインストールする必要があります。このようなシステムは、**ドライブ・サーバ**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・インタフェー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・インタフェース (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、例えば Cell Manager システムはコンピュータ・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。

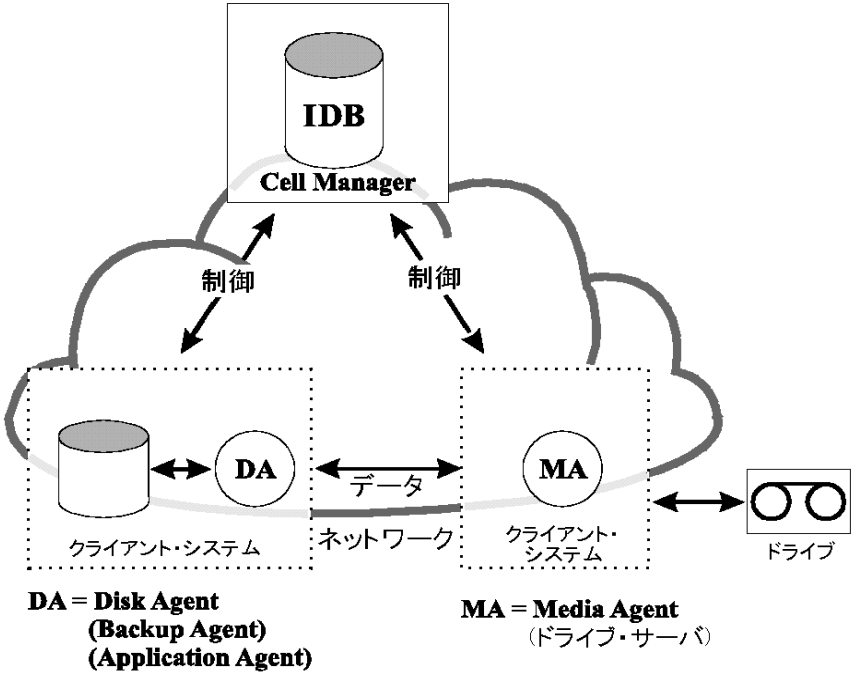
インストール・サーバ

インストール・サーバでは、特定アーキテクチャ用の Data Protector ソフトウェア・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・サーバになります。なお混合環境の場合は、少なくとも 2 台のインストール・サーバが必要です (UNIX システム用に 1 台と、Windows システム用に 1 台)。

セル内の処理

図 1-5 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。

図 1-5　　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

図 1-6 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、オペレータが Data Protector ユーザー・インタフェースを使って対話式に開始することも、Data Protector スケジューラにより自動的に開始させることも可能です。

バックアップの仕組み

バックアップの実行時には、バックアップ用 Session Manager 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。

図 1-6　　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、図 1-6 に示したよりも複雑なものになります。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・セッションの詳細は、233 ページの第 7 章 「Data Protector が機能する仕組み」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

図 1-7 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、オペレータが Data Protector ユーザー・インタフェースを使って対話式に開始します。

バックアップの仕組み

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 Session Manager 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。

図 1-7　　復元セッション

通常の復元セッションは、図 1-7 に示したよりも複雑なものになります。復元セッションの詳細は、233 ページの第 7 章 「Data Protector が機能する仕組み」 を参照してください。

企業環境

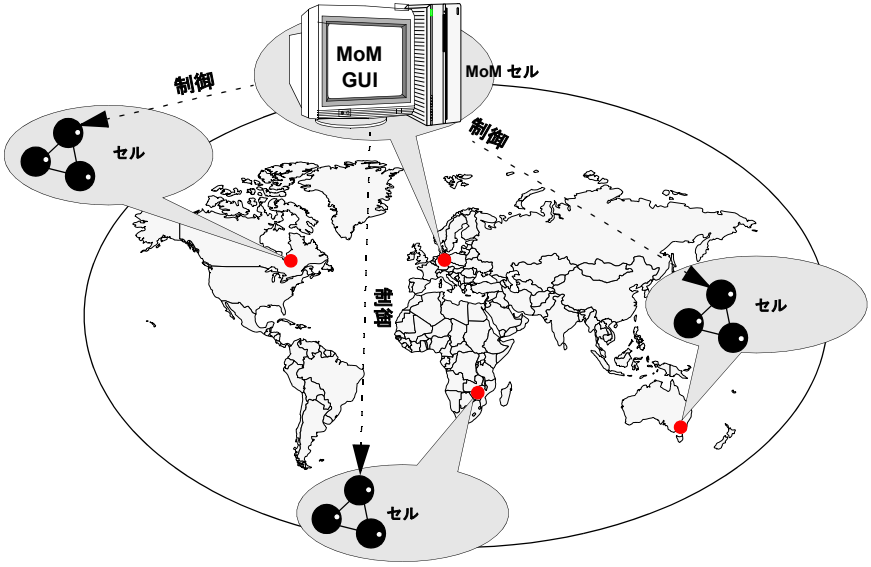
企業環境とは

図 1-8 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

本書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**バックアップ方針**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。

図 1-8　　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) の詳細は、17 ページの「MoM」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。

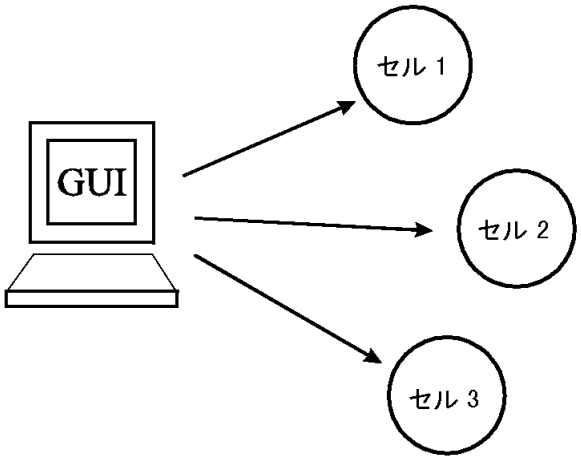
分割が必要となる場合

- 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
- 性能の向上
- 管理業務の分割

環境構築時の注意点については、27 ページの第 2 章 「バックアップ方針の策定」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。

図 1-9　　複数セルを一元管理

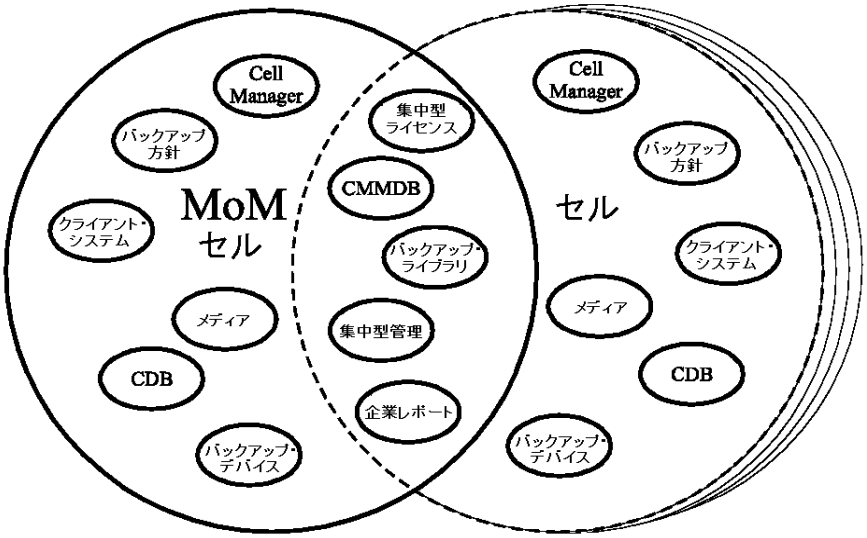


MoM

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 (図 1-9 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。

図 1-10　　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。

- **CMMDB (Centralized Media Management Database: 集中型メディア管理データベース)**

  CMMDB を使うと、1 つの MoM 環境に含まれる複数のセル間で、デバイスとメディアを共有できます。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 を使う場合は、このデータベースを MoM セル内に配置しなければなりません。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任意選択の機能である点に注意してください。

- **ライブラリの共有**

  CMMDB を使用すると、1 つの環境内の複数セル間で、ハイエンド・デバイスを共有できます。そのため、例えばあるセルから、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。

- **企業レポート**

  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方針を設定しておくと、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、対話式で、または自動的に作成することができます。
- 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、使用方針 (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、プール内に保存するデータのタイプなどは、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、メディア管理データベース内に保存されています。

図 1-11　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

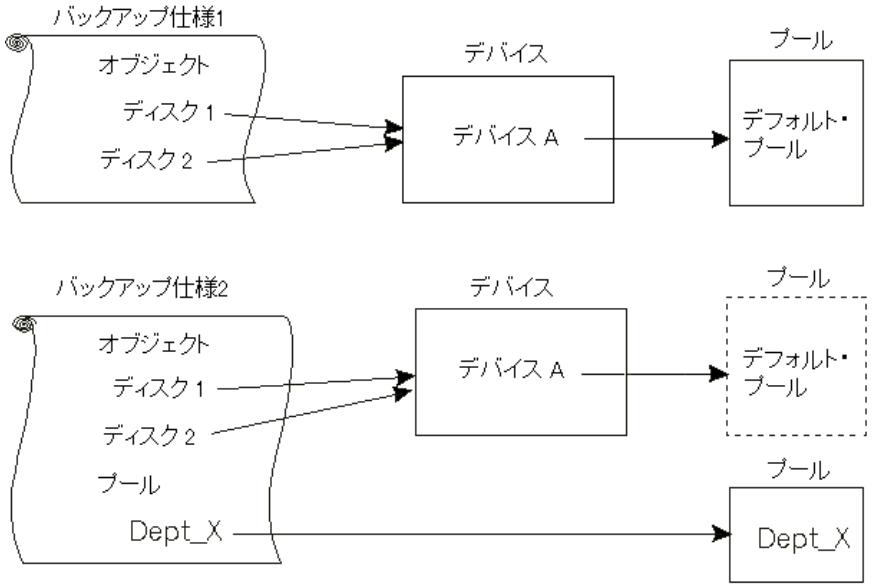


図 1-11 は、バックアップ仕様、デバイス、およびメディア・プールの関連を示したものです。各デバイスは、バックアップ仕様の中で指定されています。各デバイスはメディア・プールとリンクされていますが、このメディア・プールはバックアップ仕様内で変更することも可能です。例えば上図のバックアップ仕様 2 は、デフォルト・プールではなく Dept_X プールを参照しています。

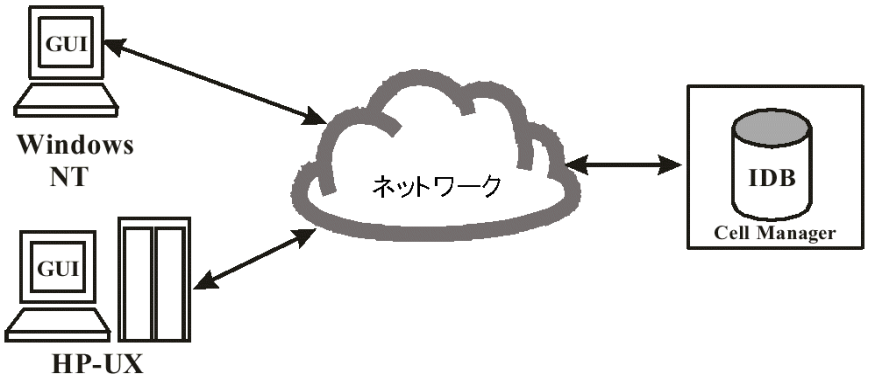
Data Protector は、多種多様なデバイスをサポートしています。詳細は、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』を参照してください。

ユーザー・インタフェース

Data Protector では、グラフィカル・ユーザー・インタフェースを使用して、すべての構成作業および管理作業を簡単に実行できます。Data Protector GUI は、UNIX プラットフォーム上の X11/Motif、および Windows プラットフォーム上で実行可能です。さらに UNIX と Windows のいずれのプラットフォームでも、コマンド行インタフェースを使用できます。

Data Protector のアーキテクチャ上、Data Protector ユーザー・インタフェー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。このユーザー・インタフェースは、必ずしも Cell Manager システム上で使用する必要はなく、ユーザーのデスクトップ・システム上にインストールすることも可能です。図 1-12 に示すように、このユーザー・インタフェースを使用すると、HP-UX、Solaris、Windows のいずれの Cell Manager を使っている Data Protector セルであっても、特に意識することなく管理できます。

図 1-12　　Data Protector ユーザー・インタフェースの使用



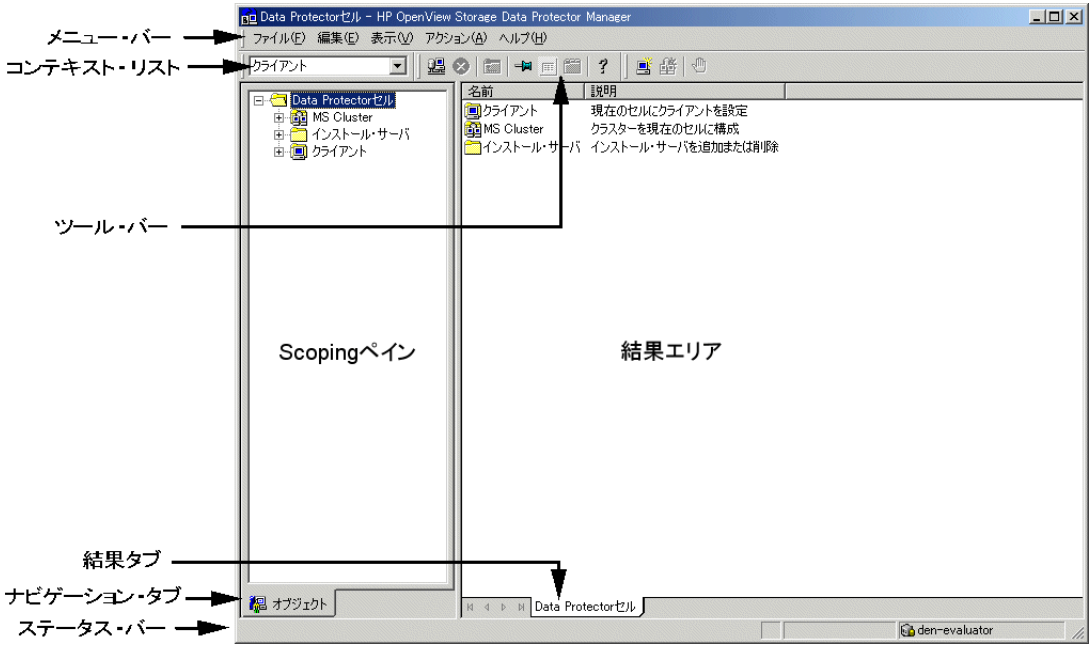
ヒント　一般に、混合環境では、環境内の複数のシステム上に Data Protector ユーザー・インタフェースをインストールしておき、複数のシステムから Data Protector にアクセスできるようにしておく方が便利です。

Data Protector GUI

図 1-13 に示すとおり、Data Protector GUI は、以下に示す機能を備えた使い易い強力なインタフェースです。

- 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、Microsoft Exchange、SAP R/3、Oracle8 などや、UNIX 環境で実行される SAP R/3、Oracle8、Informix 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・ナビゲータと呼ばれる、コンテキスト依存型のオンライン・ヘルプ・システムが用意されています。

図 1-13　　Data Protector GUI



Data Protector のセットアップ作業の概要

本項では、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、必ずしも以下のすべての手順を実行する必要はありません。

1. ネットワークと組織構造を分析して、バックアップする必要があるシステムを決定します。
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。
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・インタフェースをインストールするシステム
   - バックアップ方法 (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。ライセンスを購入すると、インストールに必要なパスワードを入手できます。

   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。詳細については、『*HP OpenView Storage Data Protector インストールおよびライセンス・ガイド*』を参照してください。
5. セキュリティ面を検討します。
   - セキュリティ上、注意すべき点を分析します。『*HP OpenView Storage Data Protector インストールおよびライセンス・ガイド*』を参照してください。
   - 構成の必要なユーザー・グループを検討します。
6. バックアップ構造を決定します。
   - 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。

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・インタフェースを使用して、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。
   - バックアップの失敗への対処
   - 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
   - 障害復旧の準備
   - IDB の保守

2　バックアップ方針の策定

本章の内容

この章では、バックアップ方針の策定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、基本的なバックアップのタイプ、自動バックアップ操作、クラスタ化、および障害復旧方法についても紹介します。

この章の構成は以下のとおりです。

バックアップ方針の策定

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。

バックアップ方針の策定とは

バックアップ方針の策定手順は、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。
3. バックアップ方針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。

本項では、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、本書の以降の部分では、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。

バックアップ方針における要件の明確化

バックアップ方針の目的と制約事項を明らかにするため、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方針**

  組織によっては、データの保管および保存に関する方針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方針は、こうした方針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、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

バックアップ方針の策定

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。例えば、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、105 ページの「障害復旧」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。例えば、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。例えば、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

  各データ・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

  各データ・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。例えば、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・データとクライアント・システム・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。例えば、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、65 ページの「フル・バックアップと増分バックアップ」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大部分のオンライン・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、『*HP OpenView Storage Data Protector インテグレーション ガイド*』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。

  さらに、大量のデータをバックアップする必要があり、バックアップに使用できる時間も限られている場合は、ダイレクト・バックアップの使用も検討してください。ダイレクト・バックアップを使用すると SAN の速度を活用し、ネットワーク・トラフィックを減少させ、バックアップ・サーバーがボトルネックとなるのを回避できます。

- バックアップを実行する頻度

  各データ・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。例えば、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。

バックアップ方針に影響する各種の要因

バックアップ方針の実装方法は、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方針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方針と要件
- 各企業におけるセキュリティに対する方針と要件
- 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資源および人的資源

バックアップ方針の策定

バックアップ方針を構築する準備

バックアップ方針を構築するには、以下の点を明らかにする必要があります。

- 各企業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

    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。
- バックアップ方針の実装
  - 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

    時差実行方式の採用を検討します。この方式ではネットワーク負荷、デバイス負荷、およびバックアップ可能な時間枠に関する問題を回避するために、クライアント (バックアップ仕様) ごとに日を変えてフル・バックアップが作成されます。
  - メディア上のデータとバックアップ関連情報の保護期間をどのように設定するか。

以前のバックアップ・データを新しいデータで上書きできないように、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、ライブラリ・デバイスの使用も検討してください。

  大量のデータをバックアップする必要がある場合、またはネットワークを使用するとバックアップ速度が低下すると思われる場合は、ライブラリ・デバイスを Fibre Channel ブリッジ経由で SAN に接続して、ダイレクト・バックアップを実行できるようにシステムを構成することを検討してください。

- 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。

  各バックアップ方針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

  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

バックアップ方針の策定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。本項では、以下の点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。例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ごと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。Data Protector セルの推奨最大サイズは、100 クライアント・システムです。200 を超えるクライアント・システムを含むセルは管理しにくくなります。

- 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。その他、ネットワーク構成などに関する詳細は、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。

- 時間帯

  1 つのセル内が、複数の時間帯に分かれてはいけません。

- 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。例えば、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、各クライアント・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バックアップ方針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ごとに、それぞれ個別のセルを設定することも可能です。例えば、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バックアップ方針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、各クライアントごと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 (プッシュ) 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・サーバにもなります。

リモート・インストールを実行するたびに、インストール・サーバにアクセスします。インストール・サーバを使用する利点は、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、アンインストール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) が、セル全体で使用可能でなければなりません。詳細については、『*HP OpenView Storage Data Protector インストールおよびライセンス・ガイド*』を参照してください。

Cell Manager とインストール・サーバは、CD から直接インストールします。Cell Manager とインストール・サーバ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、その他の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。本書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。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。例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。

前述したように、Data Protector は必ずしも Windows ドメイン環境で使用しなくても構いませんが、ドメイン環境を選択する方が、ユーザー認証が必要となるタイプの管理作業を、より効率よく簡単に実行できます (インストール、ユーザー管理など)。

混合環境でのセルの作成

混合環境でも、36 ページの「UNIX 環境でのセルの作成」に記載されている要因を考慮する必要があります。環境内が多数のドメインやワークグループに分かれていればいるほど、ソフトウェアを配布したり、管理作業のために環境を整備したりする作業に、より多くのアカウントや手順が必要になってきます。

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。詳細については、16 ページの「環境内を複数セルに分割する」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またがって 1 つのセルを構成することも可能ですが、この場合は、各クライアント・システムとバックアップ・デバイス間のデータ転送に WAN が使われないことを、必ず確認しておかなければなりません。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、中心となる MoM セルと各セルを、信頼性の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のみであり、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実行されるためです。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** (Reconnect broken connections)] 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がクラッシュ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

インフラストラクチャは、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、送信自体が新たなオーバーヘッドとなるため、ネットワークが性能を左右する要素となります。Data Protector では状況により、以下に示すとおりデータ・ストリームの処理方法が異なります。

ネットワークのデータ・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

ローカルのデータ・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。

ネットワーク / サーバ・バックアップとダイレクト・バックアップ

ネットワークおよびサーバ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、ネットワークやサーバによっても性能が左右されます。Data Protector では状況により、以下に示すようにデータ・ストリームの処理方法が異なります。

ネットワークのデータ・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

ダイレクト・データ・ストリーム

ディスク→デバイス

最大限の性能を得るには、大量のデータ・ストリームについてはダイレクト・バックアップ構成を使用してください。

デバイス

デバイスの性能

デバイスの種類とモデルは、デバイスがテープへデータを書き込む (またはテープからデータを読み取る) 速度の面で、性能に影響を与えます。

データ転送速度は、ハードウェア圧縮が使用されてい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。

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。

デバイス以外の高性能ハードウェア

コンピュータ・システムの性能

コンピュータ・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。

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。ネットワークのインフラストラクチャもこれに含まれます。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。
- 複数のXCOPYエンジンを使用して、オブジェクト(ディスクまたはファイル)を複数の(テープ)デバイスに直接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。例えば、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。

  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

どのようなインフラストラクチャが設定されている場合でも、最大の性能を得るためにはそれを効率的に使用しなければなりません。Data Protector には高い柔軟性が備わっているため、使用環境と希望するバックアップ / 復元の実施方法に合わせることができます。

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使用不可能に設定されています。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した場合は必ず、ハードウェア圧縮を使用不可能にしてください。これは、データの圧縮を二重に行うと、逆にデータのサイズが大きくなるためです。

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。ハードウェア圧縮により、テープに書き込まれるデータの量が低減されるので、テープ・ドライブのデータ受信速度が向上します。

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。ハードウェア圧縮を使用可能に設定するには、HP-UX システムではハードウェア圧縮デバイスファイルを選択し、Windows システムではデバイス構成時にハードウェア圧縮オプションを選択します。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 (複数レベル) 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しなくても構わないということです。

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 (raw ボリューム) 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配布

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るが、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、151 ページの「デバイス・ストリーミングと同時処理数」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。同様に、同時に読み込みまたは書き込みできるデータ・ストリームは 1 つだけです。Data Protector は、ファイルシステムを順にバックアップしていくことにより、ディスク・ヘッドの動きを低減させています。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・システムによっては、アクセスしたデータをいったん**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。

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 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。この機能はデータベースの稼動時間を最大化するのに役立ちますが、バックアップ中はアプリケーションの性能に影響が出る可能性があります。Data Protector は、一般に使われることが多い各種のオンライン・データベース・アプリケーションと統合して、バックアップを効率よく実行できます。

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、『*HP OpenView Storage 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。

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

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 (例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 のユーザー・アカウント

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、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オン名、そのユーザーがログオ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が指定されます。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・インタフェー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 179 ページの第 4 章 「ユーザーとユーザー・グループ」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、例えば、[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 179 ページの第 4 章 「ユーザーとユーザー・グループ」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。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。そのため 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。

詳細は 179 ページの第 4 章 「ユーザーとユーザー・グループ」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。オーナーとは、そのバックアップを構成し、バックアップ・セッションを開始 (あるいはスケジュール設定) したユーザーを指します。バックアップ・オーナーの詳細については、49 ページの「誰がバックアップ・セッションを所有するのか」を参照してください。

データの暗号化

オープン・システムおよび公共ネットワークの普及により、大規模な企業環境では、データ・セキュリティ対策が欠かせないものとなっています。Data Protector では、ファイルシステムおよびディスク・イメージのデータを判読できないような形に暗号化することも可能です。データの暗号化は、ネットワークを介したデータ転送前、およびメディアへの書き込み前に実行されます。Data Protector では、ある特定の内蔵アルゴリズムを使ってコード化を行います。

誰がバックアップ・セッションを所有するのか

バックアップ所有権とは

バックアップ仕様を作成した Data Protector ユーザーは、実行中のバックアップ・セッションおよび作成されるメディア・セットのオーナーになります。この所有権は Data Protector ユーザーに対するものであり、各システム（プラットフォーム) のユーザーに対するものではないことに注意してください。そのため、バックアップ・セッションは、必ずしもオーナーのユーザー名では実行されていません。

バックアップを開始できるユーザー

各ユーザーは、自分が作成したバックアップ仕様しか実行できません。そのため、バックアップ管理者がバックアップ仕様を作成した場合には、他のユーザーはこのバックアップ仕様に基づくバックアップを開始することができません。バックアップ・オーナーの変更方法については、『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。バックアップ・オーナーを変更すると、新しいオーナーは、実際には所有していないデータへのアクセスや復元も可能になる点に注意してください。

バックアップ所有権と復元

バックアップ所有権は、データの復元時にも影響します。[private]/[public] オプションが [private] に設定されている場合には、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。

クラスタ

クラスタの概念

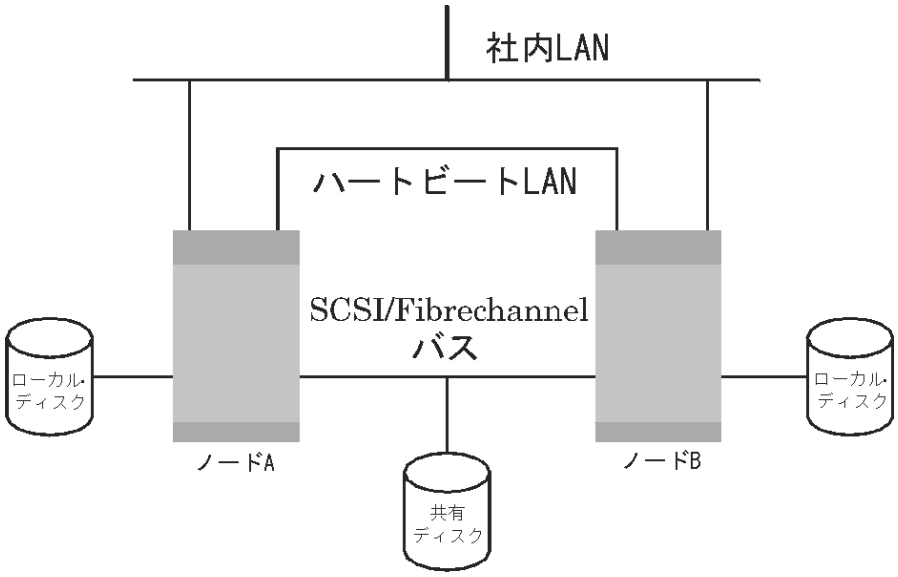
クラスタとは

クラスタとは、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から構成されるグループを指します。このコンピュータ・グループは単一のシステムとして管理され、以下の利点が得られるように設計されています。

- 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 ではクラスタ化を実現するために、Windows Server 用の Microsoft Cluster Server、HP-UX 用の MC/Service Guard、Solaris 用の Veritas Cluster、および Novell NetWare 6 Cluster Services との統合が可能です。サポートされているクラスタの一覧は、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』を参照してください。

図 2-1　　代表的なクラスタ



構成要素

- クラスタ・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・ノード

クラスタを構成するコンピュータは、**クラスタ・ノード**と呼ばれます。これらのコンピュータは、1 つまたは複数の共有ディスクに物理的に接続されます。

共有ディスク

共有ディスク・ボリューム (MSCS、Novell NetWare Cluster Services 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、クラスタの実行に必要なクラスタ固有のデータも格納されています。MSCS クラスタ内では、共有ディスクはある一時点では 1 つのクラスタ・ノード上でしか使用できません。

クラスタ・ネットワーク

クラスタ・ネットワークは、すべてのクラスタ・ノードを接続するプライベートなネットワークです。このネットワークにより、**クラスタのハートビート**と呼ばれる内部的なクラスタ・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・ノードに配布されます。各クラスタ・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・ノードが現在稼動中であるかを判断します。これにより、**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) 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、Novell NetWare Cluster Services の場合)
- 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
- クラスタ対応アプリケーション・サービス

仮想サーバとは

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、クラスタ対応アプリケーションの**仮想サーバ**を定義するリソースです。仮想サーバの IP 名と IP アドレスはクラスタ・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・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。このようなノードを**一次ノード**と呼びます。パッケージまたはグループは、別のクラスタ・ノード (いずれかの**二次ノード**) に移動させることができます。パッケージまたはグループを一次クラスタ・ノードから二次クラスタ・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。二次ノードは、一次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。

- 一次ノード上でソフトウェア障害が発生した場合
- 一次ノード上でハードウェア障害が発生した場合
- 一次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

クラスタ環境では、複数の二次ノードを設定できますが、一次ノードは 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対応の Data Protector Cell Manager には、非クラスタ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、クラスタ内でクラスタ・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行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ます。この基準を定義する方法の詳細については、『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。

クラスタのサポート

Data Protector のクラスタ・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。

注記　Cell Manager がクラスタ内にインストールされている場合、クラスタ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・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内にインストールされていること。このような場合、(クラスタ内にインストールされていない) Cell Manager はフォールト・トレラントではなくなり、セル内の操作も手動で再開しなければなりません。

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 でフェイルオーバーが発生した場合のバックアップ・セッションの動作を指定するオプションの詳細については、『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。

クラスタ環境の例

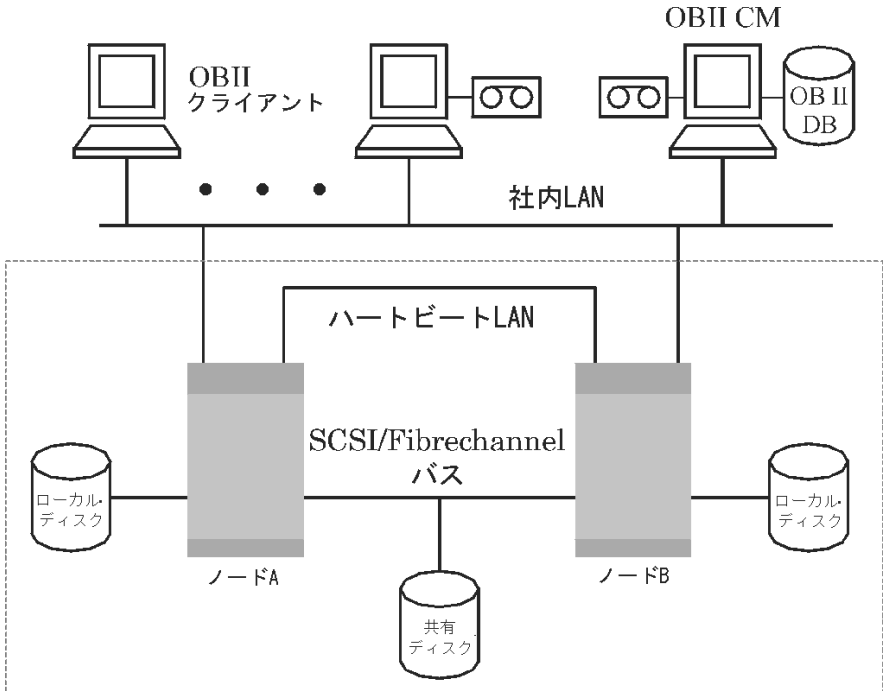
本項では、3 つのクラスタ構成例を示します。

Cell Manager がクラスタ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 または非クラスタ化クライアントの 1 つに接続されています。

図 2-2　　Cell Manager がクラスタ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

仮想サーバのバックアップ

バックアップ仕様で仮想サーバを選択した場合、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実行されている物理ノードに関係なく、選択されたアクティブな仮想ホスト / サーバがバックアップされます。

以下に、この構成で予想されるバックアップ動作を示します。

表 2-1 バックアップ動作

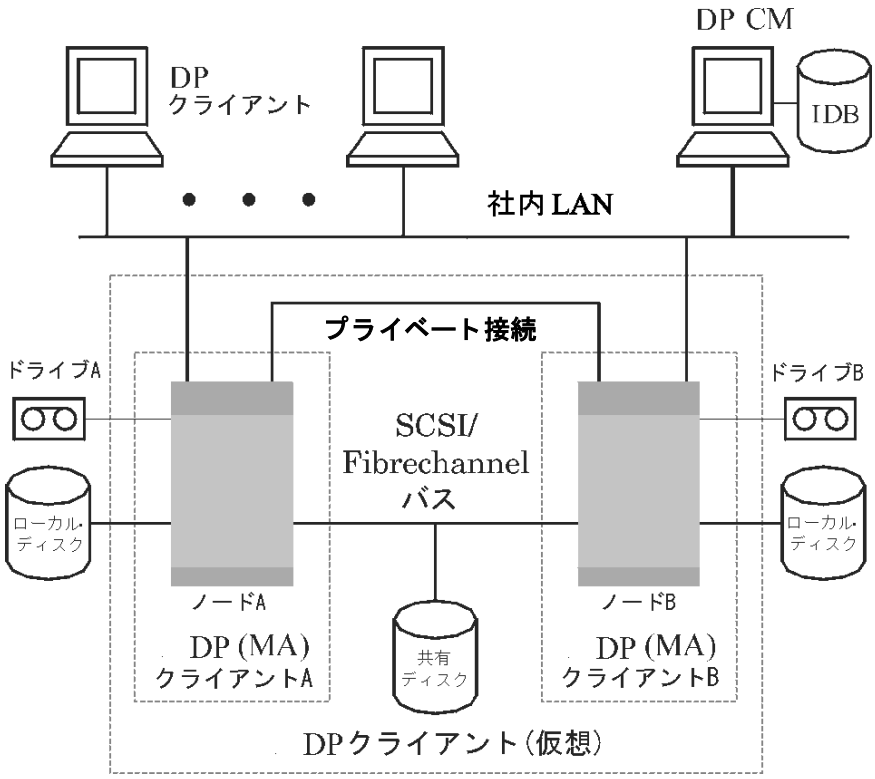
条件	結果
バックアップ開始前にノードのフェイルオーバーが発生	バックアップ成功
バックアップ中にノードのフェイルオーバーが発生	**ファイルシステム / ディスク・イメージのバックアップ :** バックアップ・セッションは失敗します。このセッションでバックアップが完了しているオブジェクトは復元に使用できますが、失敗したオブジェクト (実行中および保留中) については、セッションを手動で再開してもう一度バックアップする必要があります。
	アプリケーションのバックアップ : バックアップ・セッションは失敗します。セッションを手動で再開する必要があります。

Cell Manager がクラスタ外部にインストールされ、デバイスがクラスタ・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、クラスタ内のノードに接続されています。

図 2-3　Cell Manager がクラスタ外部にインストールされ、デバイスがクラスタ・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

仮想サーバのバックアップ

バックアップ仕様で仮想サーバを選択した場合、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実行されている物理ノードに関係なく、選択されたアクティブな仮想ホスト / サーバがバックアップされます。

注記 この例では、先の例とは異なり、個々のクラスタ・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みが使用されます。

以下に、この構成で予想されるバックアップ動作を示します。

表 2-2 バックアップ動作

条件	結果
バックアップ開始前にノードのフェイルオーバーが発生	自動デバイス切り換え機能 (負荷調整機能) により、バックアップは正常に終了します。
バックアップ中にノードのフェイルオーバーが発生	**ファイルシステム / ディスク・イメージのバックアップ :** バックアップ・セッションは失敗します。このセッションでバックアップが完了しているオブジェクトは復元に使用できますが、失敗したオブジェクト (実行中および保留中) については、セッションを手動で再開してもう一度バックアップする必要があります。
	アプリケーションのバックアップ バックアップ・セッションは失敗します。セッションを手動で再開する必要があります。

重要 このような構成でのバックアップ処理中にフェイルオーバーが発生すると、MA がセッションを正常に中止できないことがあります。この場合はメディアが破損します。

Cell Manager がクラスタ内部にインストールされ、デバイスがクラスタ・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。

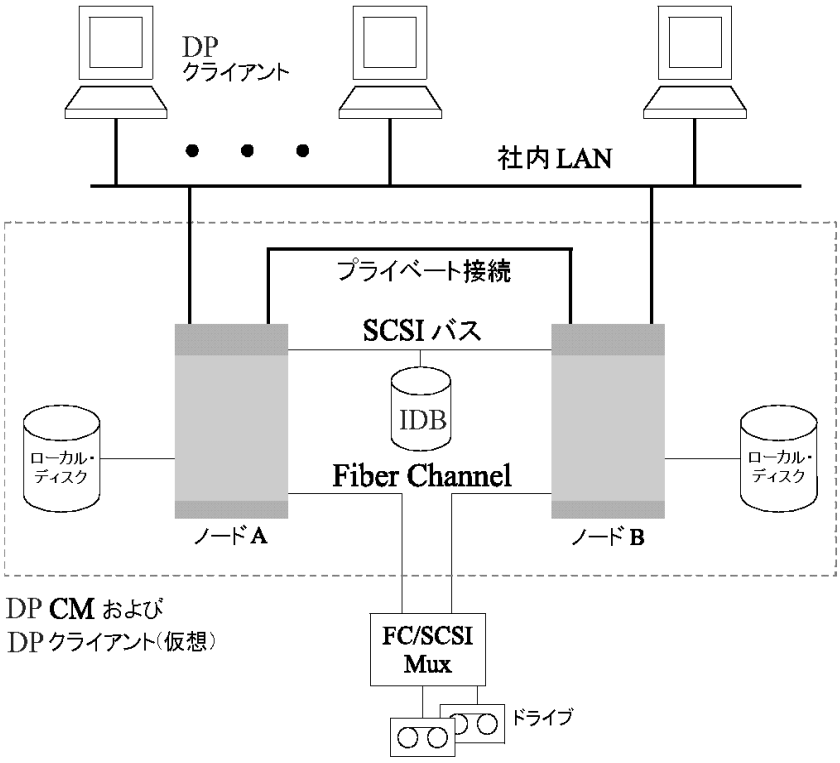
  — Data Protector Cell Manager をアプリケーションと同じノード上で実行するよう構成します (通常の動作時およびフェイルオーバー時共)。つまり、Data Protector クラスタの重要なリソースは、アプリケーション・クラスタの重要なリソースと同じパッケージ (MC/ServiceGuard の場合) またはグループ (Microsoft Cluster Server の場合) 内に定義します。

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 クラスタの重要なリソースは、アプリケーション・クラスタの重要なリソースとは別のパッケージ (MC/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、クラスタの共有 Fibre Channel バスに、FC/SCSI MUX を介して接続されています。

図 2-4　Cell Manager がクラスタ内部にインストールされ、デバイスがクラスタ・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

仮想サーバのバックアップ

バックアップ仕様で仮想サーバを選択した場合、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実行されている物理ノードに関係なく、選択されたアクティブな仮想ホスト / サーバがバックアップされます。

注記　クラスタでは、SCSI バスに共有テープを接続することはできません。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フェースに Fibre Channel 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、専用の `omniclus` コマンドを使用します。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、セッションを継続できます。

これらのオプションの定義方法については、『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。

以下に、この構成で予想されるバックアップ動作を示します。

表 2-3 バックアップ動作

<table>
<tr><th>条件</th><th colspan="2">結果</th></tr>
<tr><td>バックアップ開始前にフェイルオーバーが発生</td><td colspan="2">バックアップは正常に終了します。</td></tr>
<tr><td rowspan="2">バックアップ中に、アプリケーションと Cell Manager のフェイルオーバーが発生した場合 (Cell Manager とアプリケーションは同じノード上で実行)。</td><td>ファイルシステム / ディスク・イメージのバックアップ :
バックアップ・セッションは失敗します。このセッションでバックアップが完了しているオブジェクトは復元に使用できます。失敗したオブジェクト (実行中および保留中) については、セッションが自動的に再開されて再度バックアップされます。</td><td rowspan="2">重要
セッションを再開するには、適切な Data Protector オプションを選択することが必要です。Cell Manager のフェイルオーバー発生時に実行可能な各種 Data Protector アクションを定義する方法については、『HP OpenView Storage Data Protector 管理者ガイド』を参照してください。</td></tr>
<tr><td>アプリケーションのバックアップ
バックアップ・セッションは失敗します。セッションは自動的に再開されます。</td></tr>
<tr><td rowspan="2">バックアップ中に、アプリケーションのフェイルオーバーが発生したが、Cell Manager 自体のフェイルオーバーは発生していない場合 (Cell Manager はアプリケーションとは別のノード上で実行)。</td><td colspan="2">ファイルシステム / ディスク・イメージのバックアップ :
ファイルシステムがインストールされているノードがフェイルオーバーすると、バックアップ・セッションが失敗します。このセッションでバックアップが完了しているオブジェクトは復元に使用できますが、失敗したオブジェクト (実行中および保留中) については、セッションを手動で再開してもう一度バックアップする必要があります。</td></tr>
<tr><td colspan="2">アプリケーションのバックアップ
バックアップ・セッションは失敗します。セッションを手動で再開する必要があります。</td></tr>
</table>

重要 このような構成でのバックアップ処理中にフェイルオーバーが発生すると、MA がセッションを正常に中止できないことがあります。この場合はメディアが破損します。

また Data Protector クラスタの Cell Manager/ クライアントを、EMC Symmetrix 環境または HP StorageWorks Disk Array XP 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、『*HP OpenView Storage Data Protector ゼロ ダウンタイム バックアップ 管理者ガイド*』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

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、選択されたファイルシステム内の全ファイルが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方針に及ぼす影響について説明します。

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。例えば 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 にバックアップされる詳細情報の量を定義するためのものです。

注記 Data Protector のアプリケーション用統合機能を使用すると、さらにさまざまな種類のバックアップが可能になります (ダイレクト・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・バックアップなど)。詳細は、『*HP OpenView Storage Data Protector インテグレーション ガイド*』を参照してください。

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時以降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。

フル・バックアップの利点

フル・バックアップの利点は、以下のとおりです。

- 復元処理を非常にすばやくかつ簡単に実行できます。最新のフル・バックアップが格納されたメディアさえ用意すれば、その時点の状態にファイルを簡単に復元できます。
- 復元処理の信頼性が高くなります。すべてのデータが同一のバックアップ・セッション内でバックアップされているため、復元処理を単純な形で実行できます。

フル・バックアップの問題点

フル・バックアップの問題点は、以下のとおりです。

- バックアップ処理に時間がかかります。
- 同一バージョンのファイルが何度もバックアップされることがあるため、メディアおよびIDB 上で余分なスペースが使われます。

増分バックアップ

増分バックアップの場合には、まだ保護期限が切れていない前回の (フルまたは増分) バックアップ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。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、説明、およびツリー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なければなりません。

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、そのバックアップ・オブジェクトの有効な復元チェーン内のツリーが比較されます。有効な復元チェーン内には、ツリー指定がそのバックアップ・オブジェクトと同じで、保護期限の切れていない最新のフル・バックアップと後続の増分バックアップ (存在する場合のみ) がすべて含まれています。バックアップ・オブジェクト内のツリーを変更するなどしてツリーが一致していない場合や、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ような場合には、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開始されます。この仕組みにより、前回の当該バックアップ以降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。

増分バックアップの利点

増分バックアップの利点は、以下のとおりです。

- メディア上に占めるスペースが少なくて済みます。
- IDB 上に占めるスペースが少なくて済みます。
- 対象となるデータが少ないため、処理にかかる時間が短くなります。

増分バックアップの問題点

増分バックアップの問題点は、以下のとおりです。

- 復元処理に時間がかかります。これは、前回のフル・バックアップ・データと、目的の日時までの間に実行されたすべての増分バックアップ・データを使って、作業を行う必要があるためです。

- 復元時に多数のメディアが必要になることがあります。これは、フル・バックアップとそれ以降の増分バックアップが、同一メディア上に保存されていない可能性があるためです。

  詳細については、141 ページの「バックアップ用メディアの選択」を参照してください。

  復元処理に影響するその他の要因については、69 ページの「復元時の注意点」を参照してください。

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。

Inc	このタイプのバックアップは、図 2-5 に示すとおり、前回作成した*何らかの*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) のうち、まだ保護期限が切れていないバックアップをベースとして行われます。このタイプのバックアップでは、前回の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るため、**差分バックアップ**とも呼ばれます。
Inc1 ～ 9	**複数レベル増分バックアップ**は、図 2-6 に示すとおり、まだ保護期限が切れていない、1 つ下のレベルの前回の複数レベル増分バックアップをベースとして行われます。例えば Inc1 バックアップを実行すると、前回のフル・バックアップ時以降に更新された、すべてのデータが保存されます。また、Inc5 バックアップを実行すると、前回の Inc4 バックアップ以降に更新されたすべてのデータが保存されます (Inc4 バックアップが存在する場合)。他のレベルでも同様です。Inc1 ～ 9 バックアップでは、既存の Inc バックアップは*参照されません*。

図 2-5　　差分バックアップ

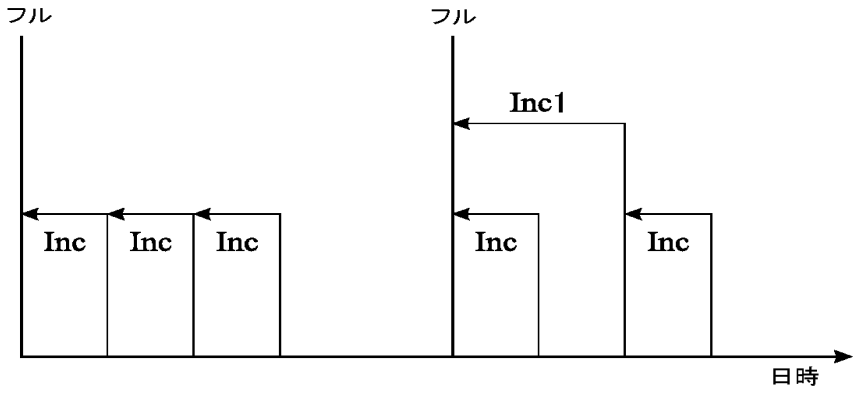
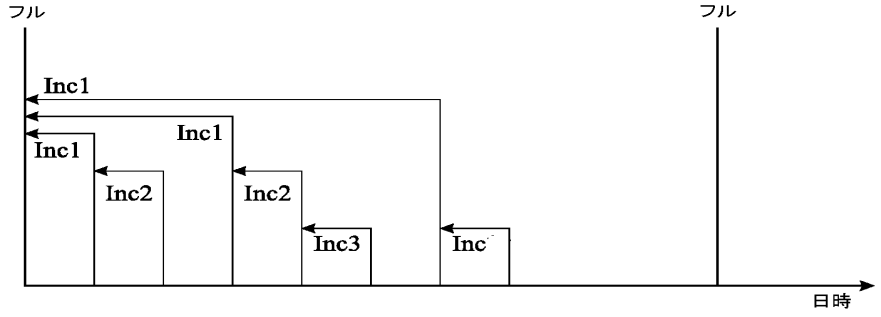


図 2-5 および図 2-6 は、さまざまなタイプの増分バックアップを示したものです。増分バックアップは、前回のフル・バックアップをベースとして実行されます。増分バックアップの開始時には、ベースとなる保護期限が切れていないフル・バックアップが存在するかどうかが、Data Protector により必ずチェックされます。保護期限が切れていないフル・バックアップが存在しない場合には、Data Protector は増分バックアップではなくフル・バックアップを開始します。

図 2-6　　複数レベル増分バックアップ



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。

メディア・セット

図 2-7 に示す差分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、**バックアップ・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 (Appendable on Incrementals Only)] 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。

図 2-8 は、もう 1 つの一般的な増分バックアップの実行方法を示したものです。この方法では、メディア上で必要となるスペースは多少増加します。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 Inc1 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。

図 2-7　差分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

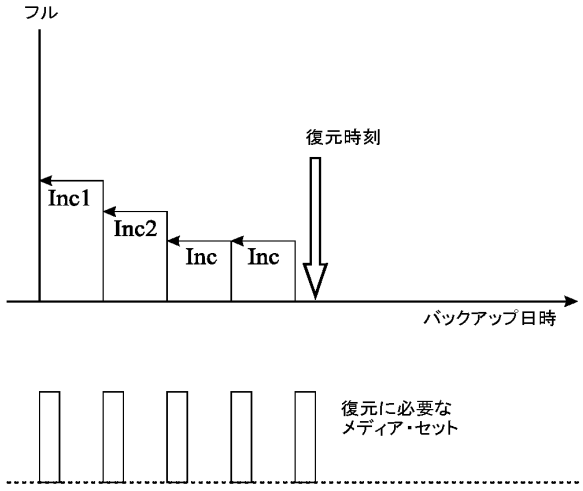
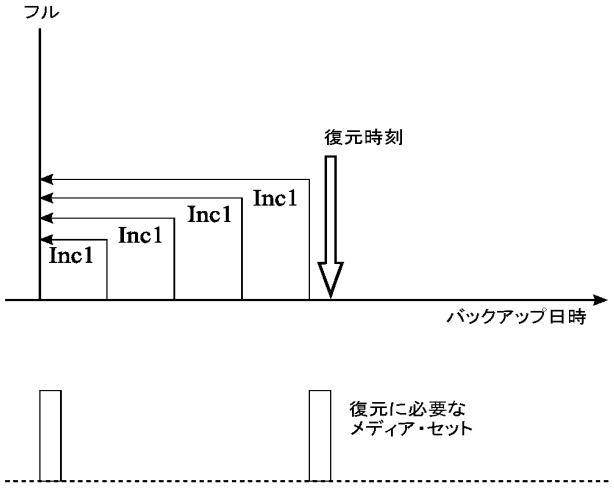


図 2-8　複数レベルの増分バックアップからの復元時に必要となるメディア



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。詳細については、付録 B を参照してください。

バックアップの種類とスケジューリング

スケジュール設定された無人バックアップを構成する場合、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も可能です。例えば、毎週日曜日にフル・バックアップを実行し、営業日には増分バックアップを実行する、といった方法です。大量のデータをバックアップする必要があり、フル・バックアップにおいてシステム負荷が集中するのを防ぐには、「時差実行方式」を採用します。詳細については、82 ページの「フル・バックアップの時差実行」を参照してください。また、バックアップを効率的にスケジュール設定する方法については、80 ページの「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」も参照してください。

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。例えば、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。このように工夫することで、IDB 上のスペースを削減できます。

データ保護 (Data Protection)

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。詳細は『*HP OpenView Storage Data Protector 管理者ガイド*』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 (Data Protection)] 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 (Catalog Protection)

カタログ保護とは

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 (Catalog Protection)] 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。

カタログ保護の設定が IDB サイズの増大と性能に及ぼす影響の詳細については、203 ページの「IDB の主要な調整可能パラメータとしてのカタログ保護」を参照してください。

Data Protector で採用されている保護モデルは、バックアップ世代に対応付けることができます。詳細については、359 ページの付録 B 「その他の情報」を参照してください。

ロギング・レベル

ロギング・レベルとは

ロギング・レベルでは、バックアップ時に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。しかしながら、データ自体の復元は、指定したロギング・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。詳細は、201 ページの「IDB の主要な調整可能パラメータとしてのロギング・レベル」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・インタフェースを使用すると、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・レベルに対する方針は、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・インタフェースを使用して、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・インタフェー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・インタフェー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・インタフェースを使用して、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・インタフェー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。

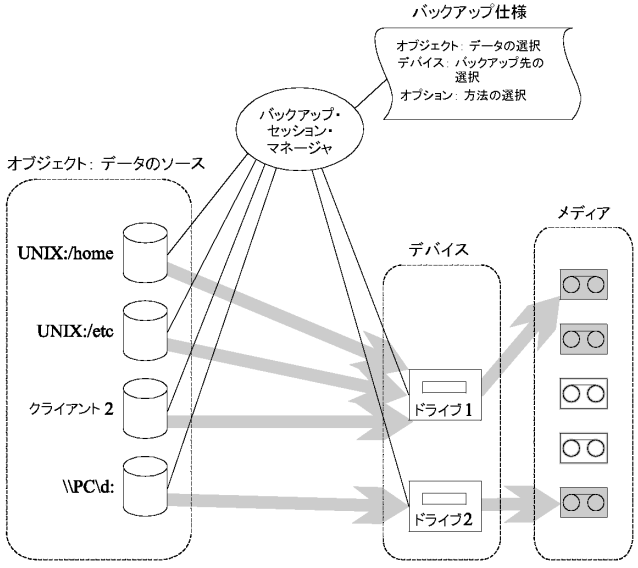
データのバックアップ

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。

図 2-9　　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。このときメディア・プールも指定できますが、指定しなければ、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

バックアップ仕様とは

バックアップ仕様を作成しておくと、実行スケジュール、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作成方法

バックアップ仕様の構成には、Data Protector ユーザー・インタフェースを使用します。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。ほとんどの場合は、Data Protector に用意されたデフォルトのバックアップ動作をそのまま使用できますが、Data Protector のバックアップ・オプションを使用すると、バックアップ動作のカスタマイズも可能です。

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。詳細については、241 ページの「ディスク・ディスカバリ・バックアップ」を参照してください。

バックアップ・オブジェクトの選択

バックアップ・オブジェクトとは

Data Protector では、同一ディスク・ボリューム (ローカル・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。さらに、バックアップ・オブジェクトはデータベース・エンティティやディスク・イメージ (raw ディスク) を選択することもできます。

バックアップ・オブジェクトは以下のように定義されています。

- 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 : クライアント名とマウント・ポイントの指定が同一のバックアップ・オブジェクトを一意に定義する働きをします。
- 種類 : ファイルシステムや Oracle などのバックアップ・オブジェクトの種類。

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。例えば、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 (Log All)]

  — [ファイル・レベルまでログに記録 (Log Files)]

  — [ディレクトリ・レベルまでログに記録 (Log Directories)]

  — [ログなし (No Log)]

  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・インタフェー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、201 ページの「IDB の主要な調整可能パラメータとしてのロギング・レベル」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

  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、239 ページの「実行前コマンドと実行後コマンド」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・セッションとは

バックアップ・セッションとは、クライアント・システム上のデータを、メディアにバックアップするプロセスを指します。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、233 ページの第 7 章 「Data Protector が機能する仕組み」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

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。

詳細は、96 ページの「オブジェクト・ミラーの作成」を参照してください。

メディア・セット

メディア・セットとは

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。プール使用方針によっては、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。一方、データを復元するときには、どのメディアを使用すればよいのかがわからなければなりません。Data Protector では、この情報をカタログ・データベース内で管理しています。

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

スケジュール設定方針とは、データをバックアップするタイミングと、実行するバックアップのタイプ (フル・バックアップまたは増分バックアップ) を定義したものです。

バックアップの種類については、以下の点に注意してください。

バックアップの種類

- フル・バックアップは増分バックアップに比べて終了するまでに時間がかかり、より多くのメディアを必要とします。
- 1 つのドライブのみを備えたスタンドアロン・デバイスを使用する場合に、バックアップ・データが単一のメディア内に収まらなければ、手動でメディアを交換する必要があります。
- 復元処理にフル・バックアップを使用する場合は、増分バックアップごとのメディアを用意する必要がないため、データを容易にかつすばやく復元できます。
- フル・バックアップでは、増分バックアップに比べて、より多くのバックアップ・データ関連情報がカタログ・データベース内に保存されるため、データベース・サイズの拡張もそれだけ速くなります。
- 増分バックアップでは、環境内の更新状況がチェックされ、前回のバックアップ以降に更新された情報のみがバックアップされます。そのため、バックアップ処理に要する時間はかなり短縮されますが、復元時の性能は低下します。

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。

単独のまたは定期的に実行されるスケジュール形式のバックアップについては、それぞれ**バックアップの種類**（フルまたは増分）、**ネットワーク負荷**、および**バックアップ保護**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。スプリット・ミラー・バックアップおよびスナップショット・バックアップについては、バックアップの種類は無視されて、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。

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 では、デバイスなどの必要な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ない場合には、セッションは待ち行列に入れられます。待ち行列に入れられたセッションについては、一定時間が経過するまでリソースの再割り当てが試みられます。この時間がタイムアウトです。タイムアウトまでの時間はユーザーが変更できます。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、65 ページの「フル・バックアップと増分バックアップ」および 72 ページの「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」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 82 ページの「フル・バックアップの時差実行」を参照してください。

注記 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「時差実行方式」を採用します。

表 2-4 時差実行方式

	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

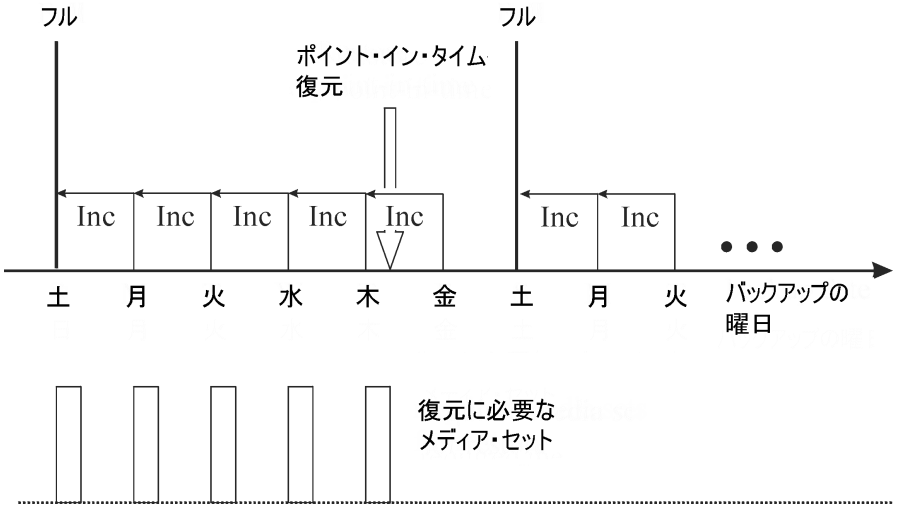
スケジュール設定方針と、フル・バックアップおよび増分バックアップをどのように組み合わせるかは、対象となるデータの復元処理にかかる時間に大きく影響します。以下に 3 つの例を使って、この点を説明します。

ポイント・イン・タイム復元を行うには、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、141 ページの「バックアップ用メディアの選択」を参照してください。

例 1

図 2-10 は、フル・バックアップと差分バックアップに基づくスケジュール設定方針を示したものです。

図 2-10　　フル・バックアップと 1 日 1 回の差分バックアップを実行

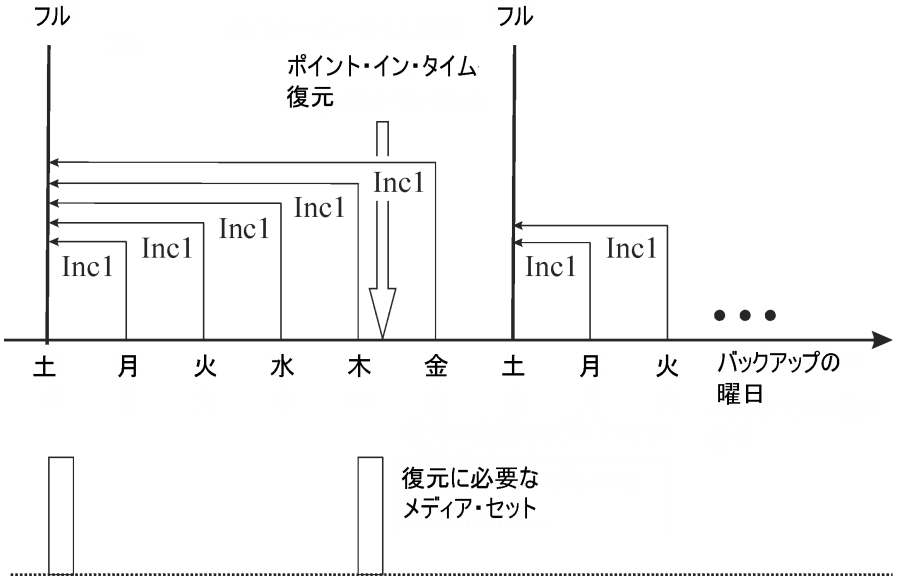


この方針では、前日から更新されたデータのみがバックアップされるため、バックアップに必要なメディア・スペースと時間は減少します。ただし、例えば木曜日のバックアップからファイルを復元するような場合には、フル・バックアップと木曜日までの増分バックアップが必要になるため、合計 5 つのメディア・セットが必要です。復元処理は複雑になり時間もかかります。

例 2

図 2-11 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方針を示したものです。

図 2-11　フル・バックアップと 1 日 1 回のレベル 1 増分バックアップを実行

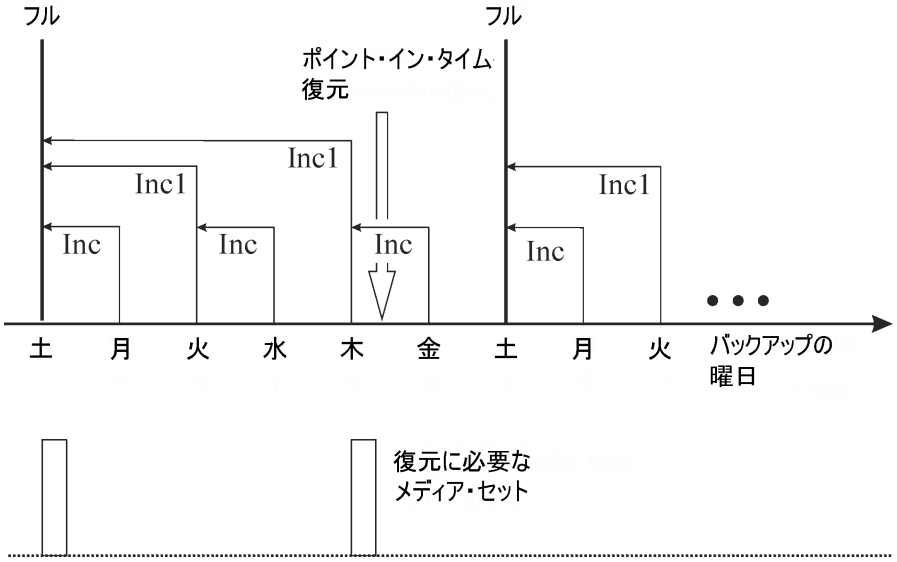


この方針では、毎日、前回のフル・バックアップ以降に更新されたデータがバックアップされるため、バックアップに必要なメディア・スペースと時間は多少増加します。ただし、例えば木曜日のバックアップからファイルを復元するには、フル・バックアップと木曜日の増分バックアップしか必要ないため、合計 2 つのメディア・セットのみが必要となります。そのため復元処理が簡単になり、処理時間も大幅に短縮されます。

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。例えば、以下に示すスケジュール設定方針を設定できます。

図 2-12　フル・バックアップと複数タイプの増分バックアップを実行



この方針は、週末にはあまりデータ更新が行われない点を考慮しています。データのバックアップは、バックアップ性能を最適化するために、差分バックアップと、レベル 1 の増分バックアップを組み合わせた形で行われます。この場合、例えば木曜日のバックアップからファイルを復元するには、フル・バックアップと 2 番目のレベル 1 増分バックアップの合計 2 つのメディア・セットのみを用意すればよいことになります。

自動または無人処理

バックアップ・プロセスに関する操作やオペレータ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、スケジュール設定方針の設定方法や、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、スケジュール設定方針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。スケジュール設定方針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方針を設定するには、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。

  通常は夜間であるため、大部分のバックアップは夜間に実行するようスケジュール設定することになります。Data Protector では、バックアップに使用されているデバイス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。また一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。

メディア交換方針を決定します。詳細については、136 ページの「メディア交換方針の実装」を参照してください。ここでは、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。

- マウント・プロンプトにどのように対応するか

  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、ライブラリの追加も検討する必要があります。詳細については、158 ページの「大容量ライブラリ」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、時差実行方式の採用も検討してください。

- バックアップ実行前に、実行中アプリケーションへの対処は必要か。

  多くのアプリケーションでは、ファイルが開かれたままになっている場合、一貫性のない形でバックアップが作成される可能性があります。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・データを複製することには、さまざまなメリットがあります。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・データの複製メソッドとして、オブジェクトのコピー、オブジェクト・ミラー、メディア・コピーの 3 つの機能が用意されています。これらの機能の主な特徴に関して、表 2-5 にまとめます。

表 2-5 Data Protector のデータ複製メソッド

	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
複製の対象	1 つまたは複数のバックアップ・セッションで作成される異なるオブジェクト・バージョンの任意の組み合わせ	1 つのバックアップ・セッションで作成されるオブジェクトのセット	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	バックアップ中	バックアップ終了後の任意のタイミング
複製元と複製先のメディアの種類	同じでなくてよい	同じでなくてよい	同じであることが必要
複製元と複製先のメディアのサイズ	同じでなくてよい	同じでなくてよい	同じであることが必要
複製先メディアへの追加書き込み	はい	はい	不可[a]
作成される内容	選択したオブジェクトのバージョンを含むメディア	選択したオブジェクトのバージョンを含むメディア	複製元と完全に同じ内容のメディア

a. 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。複製の終了後は、複製元メディアと複製先メディアの双方とも、データの追加書き込みはできなくなります。

オブジェクト・コピーの作成

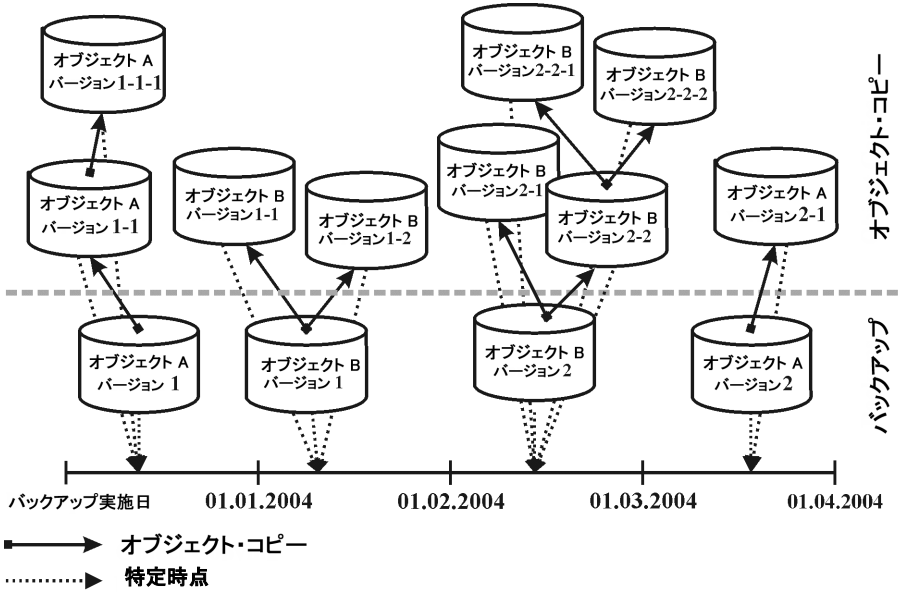
オブジェクト・コピーとは

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。この機能を使用すると、コピー元として、1 つまたは複数のバックアップ・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・セッションが終了すると、指定したオブジェクト・バージョンのコピーを格納したメディア・セットが完成しています。

89 ページの図 2-13 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。

図 2-13　　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・セッションは対話形式で開始することも、自動的に開始することも可能です。Data Protector では、**バックアップ後のオブジェクト・コピー**と**スケジュール方式のオブジェクト・コピー**という、2 種類の児童オブジェクト・コピー方法が用意されています。

バックアップ後オブジェクト・コピー

バックアップ後のオブジェクト・コピーは、自動オブジェクト・コピー仕様で指定したバックアップ・セッションの終了後に開始されます。この場合は、そのバックアップ・セッションで作成され、自動オブジェクト・コピー仕様内で選択されているバックアップ・オブジェクトが、自動的にコピーされます。

スケジュール方式のオブジェクト・コピー

スケジュール方式のオブジェクト・コピーは、ユーザーが指定した日時に行われます。さまざまなバックアップ・セッションで作成されたオブジェクトを、1 つのスケジュール方式のオブジェクト・コピー・セッションでまとめてコピーすることも可能です。

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。このときコピー先デバイスのブロック・サイズが、コピー元デバイスのブロック・サイズより大きくてもかまいません。ただし性能への影響を考えると、同じシステムまたは SAN 環境に接続された、同じブロック・サイズのデバイスを使用することをお勧めします。

オブジェクト・コピーの作成時には、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。

オブジェクト・コピー仕様内にコピー元デバイスを指定しなければ、デフォルトのデバイスが使用されます。デフォルトでは、オブジェクトの書き込みに使用されたデバイスがコピー元デバイスになります。オブジェクトごとにコピー先デバイスを指定しなければ、オブジェクト・コピー仕様内に指定したデバイスの中から、以下の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ます。

- ローカルに接続されているデバイスが、ネットワークに接続されているデバイスよりも優先的に選択されます。

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。またメディア・エラーが発生したデバイスは、そのコピー・セッションでは使われません。

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。メディア位置の優先順位を指定することによって、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。詳細は、102 ページの「メディア・セットの選択」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・データの追加コピーは、以下に示すようなさまざまな目的に使用されます。

- ボールティング

  バックアップ・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

  メディア上に保護期限の切れていないオブジェクト・バージョンがある場合は、そのオブジェクト・バージョンのみを別のメディアにコピーすることで、元のメディアを上書きできるように解放することができます。

- メディアの多重化 (データの断片化) の解消

  オブジェクトをコピーすると、データのインタリービング (断片化) を解消できます。

- 復元チェーンの統合

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

  バックアップ・データを別の種類のメディアにコピーすることが可能です。

- 高度なバックアップ手法のサポート

  ディスクステージングなどのバックアップ手法を使用できます。

ボールティング

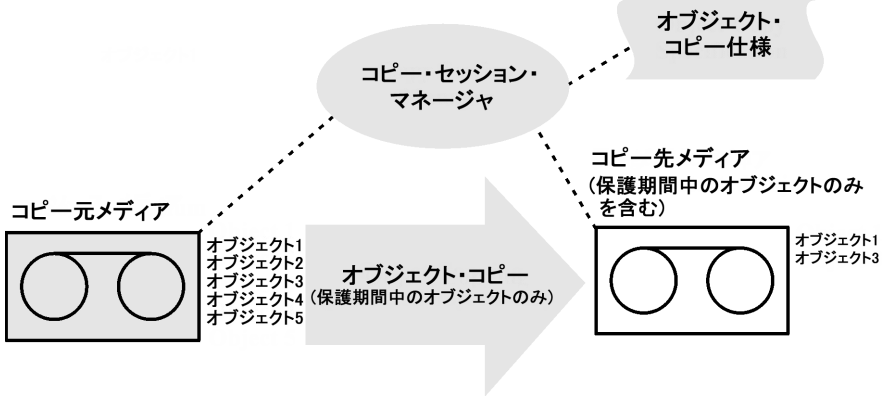
ボールティングとは、メディアを安全な場所に保管するプロセスを指します。この保管場所はボールトと呼ばれ、この中にメディアが一定期間保管されます。詳細については、146 ページの「ボールティング」を参照してください。

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

保護期限の切れていないバックアップ・データのみを保持するメディアと、上書き可能なバックアップ・データのみを保持するメディアを別にすると、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、保護期限の切れていない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。92 ページの図 2-14 を参照。

図 2-14　　メディアの解放

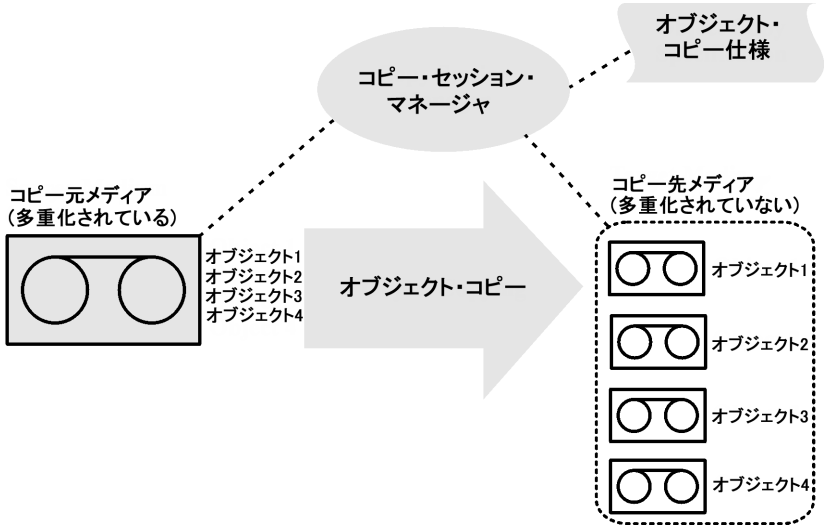


メディアの多重化 (データの断片化) の解消

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。93 ページの図 2-15 を参照。

図 2-15　　メディアの多重化 (データの断片化) の解消



復元チェーンの統合

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・セットを作成しておくと、複数のメディアをロードしたり、必要なオブジェクト・バージョンを探したりする手間が省けるため、復元処理をすばやく簡単に実行できます。

別の種類のメディアへの移動

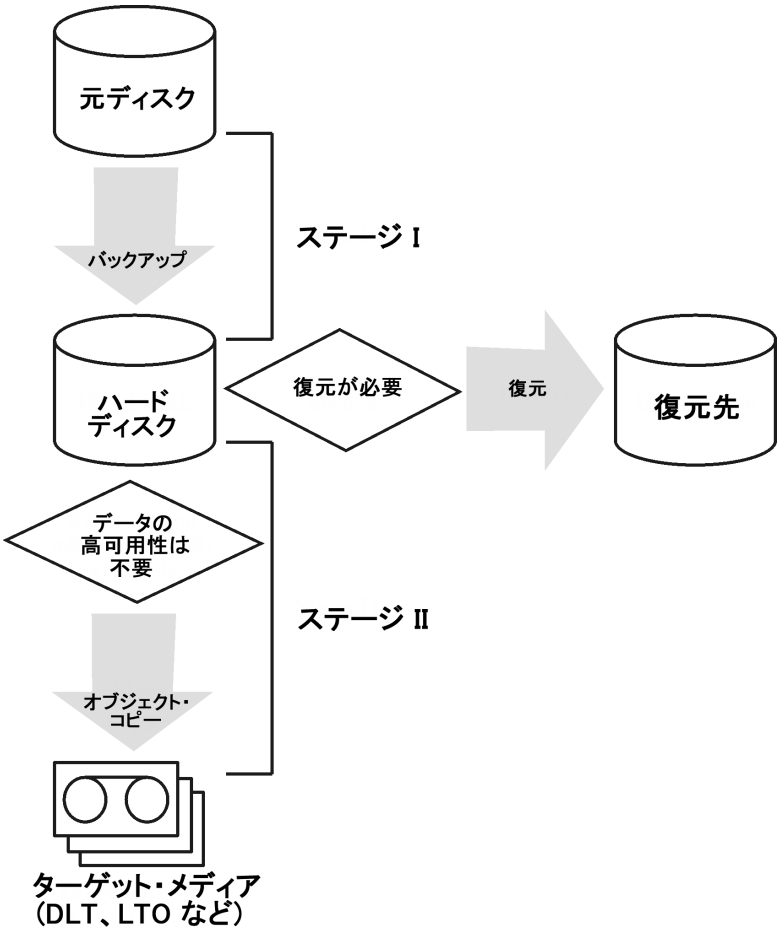
バックアップしたデータを別の種類のメディアへ移動できます。例えば、あるオブジェクトをファイル・デバイスから LTO デバイスに、または DLT デバイスから LTO デバイスにコピーできます。

ディスクステージング

ディスクステージングとは、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た手法です。

この手法によるバックアップは、ある種類のメディアにデータをバックアップする段階と、バックアップしたデータをさらに別の種類のメディアにコピーする段階に分けて行います。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。一定期間が経過したデータは、オブジェクト・コピー機能を使用して、性能やアクセス容易性に劣るものの容量が大きいメディアに移して保管します。95 ページの図 2-16 を参照。

図 2-16　　ディスクステージングの概念



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。そのようなバックアップでは、メディアをいちいちロードおよびアンロードしなければならないため、作業に手間がかかります。ディスクステージングは、バックアップ時間の短縮やメディア劣化の軽減を図るうえでも有効です。

オブジェクト・ミラーの作成

オブジェクト・ミラーとは

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・ミラーの作成を伴うバックアップ・セッションが正常に終了すると、バックアップ・オブジェクトを格納したメディア・セットに加えて、ミラー・オブジェクトを格納した追加のメディア・セットも作成されています。これらのメディア・セット上のミラー・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・ミラーを作成する利点

オブジェクト・ミラー機能は、以下に示すようなさまざまな目的に使用できます。

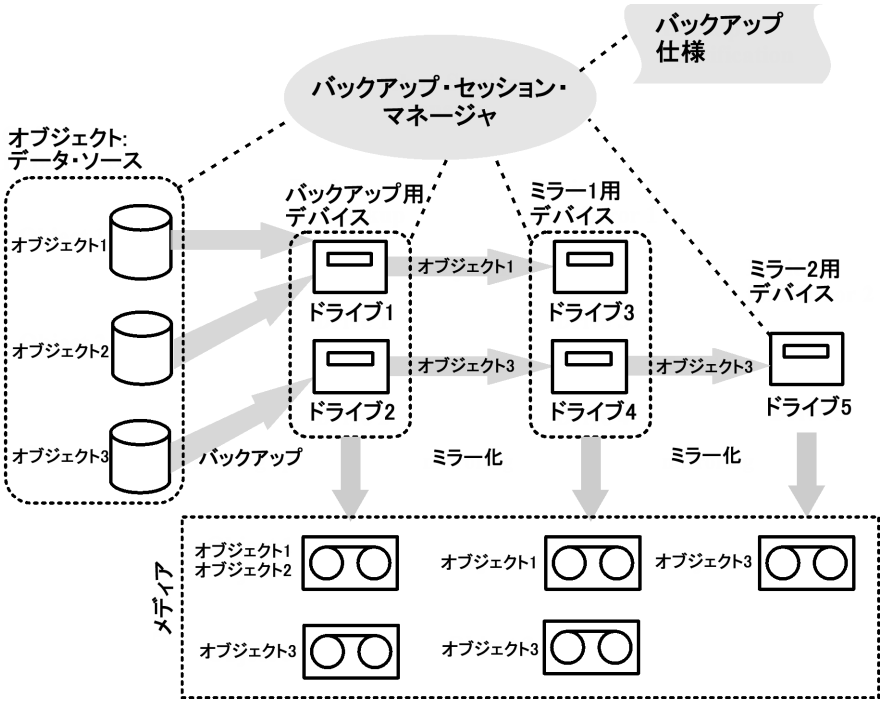
- 複数のコピーが存在するため、バックアップ・データの可用性が向上します。
- バックアップ・データをリモート・サイトにミラー化できるため、複数の場所へのボールティングが容易になります。
- 同一データを複数のメディアに書き込むことにより、バックアップ・データのフォールト・トレランスが向上します。1 つのメディアで障害が発生しても、他のミラーの作成には影響しません。

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。97 ページの図 2-17 を参照。

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。

図 2-17　　オブジェクト・ミラーの作成



デバイスの選択

オブジェクト・ミラーの作成時には、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、それらが選択されます。
- ローカルに接続されているデバイスが、ネットワークに接続されているデバイスよりも優先的に選択されます。

コマンド行からオブジェクト・ミラー操作を実行したときには、負荷調整は行われません。

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。これらのシステム上では、作成するミラーの数が増えるほど、バックアップ性能は低下します。

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も影響されます。バックアップやオブジェクト・ミラーの作成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、セッション中にミラー・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。

メディアのコピー

メディアのコピーとは

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。詳細は、99 ページの「自動メディア・コピー」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、内容がまったく同じ 2 つのメディア・セット、つまり元のメディア・セットとそのコピーが得られます。どちらのメディア・セットも復元に使用できます。

コピーが終了すると元のメディアには追加不可能 (non appendable) マークが付けられて、新しいバックアップ・データは追加できなくなります。これは元のメディアの内容がそのコピーと異ならないようにするためです。同様にコピーにも追加不可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。

自動メディア・コピー

自動メディア・コピーとは

自動メディア・コピーとは、バックアップ・データが格納されたメディアのコピーを自動作成するプロセスを指します。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 つはバックアップ後のメディア・コピー、もう 1 つはスケジュール方式のメディア・コピーです。

バックアップ後のメディア・コピー

バックアップ後のメディア・コピーは、バックアップ・セッションの終了後に開始されます。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。

スケジュール方式のメディア・コピー

スケジュール方式のメディア・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。

自動メディア・コピーの仕組み

始めに、自動メディア・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、自動メディア・コピー仕様に指定されているパラメータに基づき、メディア (コピー元メディア) の一覧が Data Protector により作成され、個々のコピー元メディアについて、データのコピー先となるメディアがそれぞれ選択されます。コピー先メディアは、コピー元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・コピーには独自の調整機構が備わっています。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。マウント要求が発行された場合は、その要求に関係するメディア・ペアに対する処理は打ち切られますが、セッションは続行されます。

使用例については、363 ページの「自動メディア・コピーの例」を参照してください。

データの復元

データ復元方針は、各企業の全体的なバックアップ方針における本質的なポイントとなります。以下の事項を考慮した上で方針を策定してください。

- 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。

本項では、Data Protector を使った復元方針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も影響されます。

- 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、65 ページの「フル・バックアップと増分バックアップ」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。詳細は、123 ページの第 3 章 「メディア管理とデバイス」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、40 ページの「性能に関する概要と計画上の注意点」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『*HP OpenView Storage Data Protector インテグレーション ガイド*』を参照してください。

- 並列復元の使用。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。詳細については、248 ページの「並行復元」を参照してください。
- ロギング・レベルの設定。詳細は、201 ページの「IDB の主要な調整可能パラメータとしてのロギング・レベル」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。デフォルトでは、使用するメディア・セットは Data Protector により自動的に選択されます。メディア位置の優先順位を設定しておくと、このメディア・セットの自動選択をある程度まで制御できます。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。例えば、一部のメディアが存在しなくなっていたり不良であったりするメディア・セットは選択されず、オブジェクトの完結状態やメディア・セットの位置などが比較されます。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。

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。メディアを複数の場所に保管している場合は、特定の復元処理に対して、どの保管場所を優先するかを指定できます。複数のメディア・セットが選択条件に合致した場合、優先順位の最も高いメディア・セットが選択されます。

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。

復元する権限をオペレータにのみ付与

一般的な復元方針では、専任のバックアップ・オペレータ、またはネットワーク管理者にのみ、ファイル復元および障害復旧を実行する権限が与えられます。

この方針が適している場合

この方針は、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、オペレータの信頼性が求められます。

必要な作業

この方針を実施するには、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。
- 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・インタフェー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。
- 復元要求に対する対処方針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 (例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 つの復元方針として、すべてのエンド・ユーザーあるいは特定のエンド・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・オペレータが多数の復元操作を実行する必要もなくなります。

この方針が適している場合

この方針は、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

この方針を実施するには、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。
- エンド・ユーザーが使用するシステム上に、Data Protector ユーザー・インタフェースをインストールします。Data Protector では、ユーザー権限が自動的にチェックされるため、エンド・ユーザーについては復元処理のみが許可されます。
- 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。

障害復旧

この項では、実行可能なさまざまな障害復旧方法について簡単に説明します。また各種の障害復旧方法とオペレーティング・システムの有効な組み合わせを示す表も掲載しています。この表は、本章の以降の部分に目を通す際の参考にしてください。

コンピュータ障害とは

コンピュータ障害とは、人的エラー、ハードウェアまたはソフトウェアの障害、自然災害などにより、コンピュータ・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。通常このような状況が発生した場合は、システムのブート・パーティションやシステム・パーティションが使用不能になっているため、標準的な復元作業を開始する前に、まず環境を復旧しなければなりません。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・データを復旧できません。*

元のシステムとは

元のシステムとは、システムにコンピュータ障害が発生する前に、Data Protector によってバックアップされた時点のシステム構成を指します。

ターゲット・システムとは

ターゲット・システム とは、コンピュータ障害が発生した後のシステムを指します。通常ターゲット・システムはブート不可能な状態になっており、Data Protector の障害復旧は、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。クラッシュし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。

ブートおよびシステム・ディスク / パーティション / ボリュームとは

ブート・ディスク / パーティション / ボリュームとは、ブート・プロセスの初期段階で必要なファイルを含むディスク / パーティション / ボリュームを指します。一方、**システム・ディスク / パーティション / ボリューム**とは、オペレーティング・システム・ファイルを含むディスク / パーティション / ボリュームを指します。

注記 Microsoft の定義は上記とは逆で、ブート・パーティションはオペレーティング・システム・ファイルを含むパーティション、システム・パーティションはシステムのブート・プロセスの初期段階で必要なファイルを含むパーティションを示します。

ホスティング・システムとは

ホスティング・システムとは、Disk Agent がインストールされ、ディスク・デリバリーによる障害復旧に使用される作業用の Data Protector クライアントのことです。

補助ディスクとは

補助ディスクとは、最小限のオペレーティング・システムに加えて、ネットワーク機能と Disk Agent がインストールされたブート可能なディスクです。このディスクは持ち運びが可能で、UNIX クライアントに対するディスク・デリバリーによる障害復旧の第 1 フェーズで、ターゲット・システムをブートするために使われます。

障害復旧オペレーティング・システム (DR OS) とは

障害復旧オペレーティング・システム (DR OS: Disaster recovery operating system) とは、障害復旧プロセスを実行中のオペレーティング・システム環境を指します。このオペレーティング・システムにより、ディスク、ネットワーク、テープ、およびファイルシステムへのアクセスといった基本的な実行時環境が Data Protector に提供されます。Data Protector による障害復旧を開始するには、最初に障害復旧オペレーティング・システムをインストールして構成しておかなければなりません。

DR OS は一時的な OS とすることも、アクティブな OS とすることもできます。**一時的な DR OS** は、ターゲット・オペレーティング・システムの構成データとともに別のオペレーティング・システムを復元するためのホスト環境として、排他的に使用されます。この OS は、ターゲット・システムが元のシステム構成に復元された後で削除されます。一方**アクティブ DR OS** は、自身の構成データを元の構成データで上書きすることにより、Data Protector 障害復旧プロセスのためだけではなく、復元されたシステムの一部として引き続き実行されます。

クリティカル・ボリュームとは

クリティカル・ボリュームとは、システムのブートに必要なボリュームと、Data Protector ファイルを指します。オペレーティング・システムの種類に関係なく、クリティカル・ボリュームには以下のものが含まれます。

- ブート・ボリューム
- システム・ボリューム
- Data Protector の実行可能ファイル
- IDB (Cell Manager の場合のみ)

注記　IDB が存在しているボリュームはすべてクリティカル・ボリュームです。

前述したクリティカル・ボリュームのほかに、Windows システムでは、CONFIGURATION もクリティカル・ボリューム・セットに含まれます。各種サービスは CONFIGURATION バックアップの一環としてバックアップされます。

ただし CONFIGURATION に含まれる項目の中には、システム、ブート、Data Protector、または IDB 以外のボリュームに配置できるものもあります。この場合は、以下のボリュームもクリティカル・ボリューム・セットに含める必要があります。

- ユーザー・プロファイル・ボリューム
- Certificate Server データベース・ボリューム
- ドメイン・コントローラの Active Directory Service ボリューム
- Microsoft Cluster Server 上のクォーラム・ボリューム

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。
- 管理者が障害復旧手順に不慣れである。
- 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。

障害復旧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。

復旧の過程

障害復旧プロセスは 4 つのフェーズに分けられますが、障害復旧を成功させるには、それ以前に *フェーズ 0*(準備フェーズ) を実行しておくことが重要です。*フェーズ 1* では DR OS をインストールして構成します。通常このフェーズにはブート・パーティションの再作成や再フォーマットも含まれますが、これは障害発生時には、システムのブート・パーティションやシステム・パーティションが使用不可能なケースが多く、通常の復旧処理を開始する前に環境の復旧が必要になるためです。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 Data Protector を元の状態に復元する作業は、*フェーズ 2* で実行します。ここ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 (*フェーズ 3*) が可能になります。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。

整合性のある適切なバックアップ

大きな障害が発生した場合は、対象となるシステムをまずバックアップ時の状態に戻す必要があります。さらにシステムは、バックアップ時と同じ状態で稼動し機能していることが期待されます。これは、場合によってはかなり難しい作業を伴います。例えば一部のアプリケーションは、シャットダウンされている場合であっても、完全には非アクティブな状態になりません。

UNIX システム上ではさまざまな理由により、システムの起動後直ちに一部のデーモンやプロセスがアクティブになります (HP-UX の場合であれば、実行レベル 2 のライセンス・サーバなど)。このように起動後直ちに開始されるプロセスにより、データがメモリに読み込まれたり、実行時になんらかのファイルに「ダーティ・フラグ」が書き込まれたりする可能性さえあります。標準の処理ステージ (標準実行レベル 4) で実行されるバックアップでは、このようなアプリケーションを問題なしに再開することは期待できません。例えばこのような不完全な復元処理の後でライセンス・サーバを再開すると、ファイルから読み込まれたデータに不整合性が検出されて、サービスが予想どおりに開始されないことがあります。

Windows システム上では、システムの稼動中に多数のファイルがシステムによりロックされており、置き換えができない場合があります。例えば、現在使用中のユーザー・プロファイルは復元できません。復元するにはログイン・アカウントを変更するか、関連するサービスを停止する必要があります。

バックアップ時にシステム上でアクティブになっている内容によっては、特定のアプリケーション用のデータに整合性がなく、復元後の再開や実行に問題が生じる可能性があります。

理想的には関連するパーティションをオフラインに設定してバックアップを作成するのが一番ですが、ほとんどの環境ではこの方法は使用できません。

プロセスの概要

さまざまなタイプの多数のシステムを含む大規模な環境で障害復旧を行う場合、作業は以下の手順に沿って進められます。

1. **計画**

   復旧計画は IT 管理部門が担当し、以下の点を明らかにする必要があります。

   - 復旧するシステムを決定し、復旧のための時間枠と復旧レベルも明らかにしておきます。ネットワークが適切に機能するために必要なシステム (DNS サーバ、ドメイン・コントローラ、ゲートウェイなど)、Cell Manager、および Media Agent クライアントは、いずれも重要なシステムです。
   - 復旧方法を決定します (必要な準備作業に影響します)。

- IDB が格納されているメディア、更新済みの SRD ファイルのある場所など、復旧時に必要となる情報の入手方法を明らかにしておきます。
- 復旧プロセス全体にわたる、詳細な手順チェックリストを作成します。
- 復旧が適切に行われるかどうかを確認するためのテスト計画を作成して実行します。

2. **復旧の準備**

   実行する復旧方法によって、以下のような準備作業が必要になります。

   UNIX システムの場合 :

   - 最小限のオペレーティング・システム、ネットワーク・リソース、Data Protector Disk Agent などがインストールされた補助ディスクなどの、復旧用ツールの作成。
   - 格納構造を収集するための実行前スクリプトの作成や、その他のクライアント固有の準備。

   Windows システムの場合 :

   - **System Recovery Data (SRD、システム復旧データ)** を更新して安全な場所へ保管。セキュリティ上の理由により、SRD ファイルへのアクセスを制限する必要があります。

   すべてのシステムで必要な作業 :

   - 障害復旧計画に基づくテストの実行。
   - 整合性のあるバックアップの定期的な作成。

3. **復旧手順の実行**

   事前にテストしておいた手順およびチェックリストに従って、クラッシュしたシステムを復旧します。

手動による障害復旧方法

この方法はターゲット・システムを元のシステム構成に戻すための、基本的かつ非常に柔軟性の高い障害復旧方法です。サポートされているオペレーティング・システムの詳細は、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』を参照してください。

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。

手動による復旧では、パーティション情報、ディスクのミラー化やストライピング化に関する情報など、フラット・ファイル内には保持されていない格納構造に関する情報を事前に収集しておくことが重要になります。

アシスト付きの手動による障害復旧 (Windows クライアントの場合)

Windows クライアント向けのアシスト付きの手動による障害復旧の一般的な手順は、以下のとおりです。

フェーズ 1:

1. 障害が発生したハードウェアを交換します。
2. オペレーティング・システムを再インストールします。必要なパーティションの作成とフォーマットも行います。
3. サービス・パックを再インストールします。
4. 新しいディスクに対するパーティションの再作成を手動で行い、元のドライブ文字の割り当てを使って格納構造を構築します。

ヒント 手動による障害復旧のフェーズ 1 は、自動配布ツールと組み合わせることも可能です。

フェーズ 2:

5. Data Protector の `drstart.exe` コマンドを実行します。これにより DR OS がインストールされ、クリティカル・ボリュームの復元が開始されます。
6. `drstart` コマンドが終了したら、コンピュータを再ブートします。
7. 復旧対象が Cell Manager の場合、または高度な復旧作業を実行する場合は、さらに追加の作業が必要になります。詳細については、『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。

フェーズ 3:

8. Data Protector の標準的な復元手順に従って、ユーザー・データとアプリケーション・データを復元します。

UNIX Cell Manager の障害復旧

手動による UNIX Cell Manager の一般的な障害復旧手順は、以下のとおりです。

フェーズ 1:

1. 障害が発生したハードウェアを交換します。
2. 新しいディスクのパーティションを手動で再作成し、格納構造を再構築します。
3. オペレーティング・システムを再インストールします。
4. パッチを再インストールします。

フェーズ 2:

5. Data Protector Cell Manager を再インストールします。
6. メディアから他のすべてのファイルを容易に復元できるよう、IDB の最新バックアップを復元します。
7. Data Protector 構成情報 (`/etc/opt/omni`) を、バックアップしておいた最新の Data Protector 構成情報で置き換えて、以前の構成を再作成します。

フェーズ 3:

8. Data Protector の標準的な復元手順に従って、ユーザー・データとアプリケーション・データを復元します。
9. システムを再ブートします。

ディスク・デリバリーによる障害復旧

この方法は Windows と UNIX の各クライアント上でサポートされています。サポートされているオペレーティング・システムの詳細は、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』を参照してください。

Windows クライアントの場合は、クラッシュし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、ホスティング・システムに一時的に接続します。復元が終了したら、このディスクを障害が発生したシステムに接続し直してブートできます。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・デリバリーによる障害復旧を実行します。

この方法を使用すると、すばやく簡単にクライアントを復旧できます。Windows システムの場合は、オペレーティング・システムの状態も自動的に復元されます。

ヒント この方法は、ホットスワップが可能なハード・ディスク・ドライブを使える場合は特に便利です。この場合は、電源が入ってシステムが稼動しているままの状態で、ハード・ディスク・ドライブをシステムから取り外し、新しいドライブを接続できます。

ディスク・デリバリーによる障害復旧 (Windows クライアントの場合)

Windows クライアントのディスク・デリバリーによる障害復旧の一般的な手順は、以下のとおりです。

フェーズ 1:

1. 交換用ディスクをホスティング・システムに接続します。
2. 交換用ディスクのパーティションを手動で再作成し、格納構造を再構築します。Windows のマウントポイントの詳細については、『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。

フェーズ 2:

3. Data Protector のディスク・デリバリー・ウィザードを使用して、元のシステムの重要なディスクを、この交換用ディスク上に復元します。
4. ホスティング・システムをシャット・ダウンして、交換用ディスクを取り外し、このディスクをターゲット・システムに接続し直します。ホットスワップが可能なハード・ディスク・ドライブを使用している場合は、システムをシャット・ダウンする必要はありません。
5. 交換したディスクから、ターゲット・システムを再ブートします。

フェーズ 3:

6. Data Protector の標準的な復元手順に従って、ユーザー・データとアプリケーション・データを復元します。

ディスク・デリバリーによる障害復旧 (UNIX クライアントの場合)

UNIX クライアントの場合は、(持ち運び可能な) 補助ディスク上に、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 エージェントをインストールして、ディスク・デリバリーを実行します。

UNIX クライアント向けの、補助ディスクを使った障害復旧の一般的な手順は以下のとおりです。

フェーズ 1:

1. 障害が発生したディスクを新しいディスクと交換し、ターゲット・システムに補助ディスクを接続して、この補助ディスク上にインストールされている最小限のオペレーティング・システムを使ってシステムを再ブートします。
2. 交換用ディスクの再パーティション化と以前の格納構造の再構築を手動で行い、このディスクをブート可能な状態にします。

フェーズ 2:

3. Data Protector の通常の復元手順に従って、この交換用ディスク上に、元のシステムのブート・ディスクを復元します ([Restore into] オプションを使用)。
4. システムをシャットダウンし、補助ディスクを取り外します。ホットスワップが可能なハード・ディスク・ドライブを使用している場合は、システムをシャット・ダウンする必要はありません。
5. システムを再ブートします。

フェーズ 3:

6. Data Protector の標準復元手順で、ユーザー・データとアプリケーション・データを復元します。

高度な自動障害復旧 (EADR)

Data Protector では、Windows の Cell Manager およびクライアント向けに、高度な障害復旧手順が用意されています。サポートされているオペレーティング・システムの詳細は、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』を参照してください。

EADR 手順では、関連するすべての環境データが、バックアップ時に自動的に収集されます。フル・バックアップの実行時には、セル内のすべてのバックアップ対象クライアントについて、一時的な DR OS のセットアップと構成に必要なデータが収集されて 1 つの大きな **DR OS イメージ・ファイル**にまとめられ、バックアップ・テープ上 (および必要に応じて Cell Manager 上) に保存されます。

さらにこのイメージ・ファイルに加えて、ディスクを適切にフォーマットしてパーティションを作成するために必要な、**フェーズ 1 スタートアップ・ファイル** (**P1S ファイル**) も、バックアップ・メディアと Cell Manager 上に保存されます。障害発生時には、高度な自動障害復旧ウィザードを使用して、バックアップ・メディアから DR OS イメージを復元し (フル・バックアップ時にこのイメージを Cell Manager 上に保存していない場合)、このイメージを**障害復旧 CD ISO イメージ**に変換します。この CD ISO イメージは、任意の CD 作成ツールを使用して CD 上にコピーして、ターゲット・システムのブートに使用できます。

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。

重要 バックアップ・メディア、DR イメージ、SRD ファイル、および障害復旧 CD へのアクセス権は適切に制限することをお勧めします。

Windows クライアントに対する高度な自動障害復旧の一般的な手順は、以下のとおりです。

EADR の手順

フェーズ 0:

1. クライアントのフル・バックアップを実行します。
2. 高度な自動障害復旧ウィザードを使用して、クラッシュしたシステムの DR OS イメージ・ファイルから DR CD ISO イメージを作成し、そのイメージを CD 上にコピーします。フル・バックアップ時に DR OS イメージが Cell Manager 上に保存されていない場合は、高度な自動障害復旧ウィザードにより、バックアップ・メディアからイメージが復元されます。

重要 ハードウェア、ソフトウェア、または構成を変更したときには、新しいバックアップを実行して新しい DR CD を作成する必要があります。IP アドレスや DNS サーバの変更など、ネットワーク構成を変更した場合も、同じように新しい DR CD を作成する必要があります。

フェーズ 1:

3. 障害が発生したハードウェアを交換します。
4. 障害復旧 CD からターゲット・システムをブートし、復旧の範囲を選択します。この復旧処理は完全に自動で行われます。

フェーズ 2:

5. クリティカル・ボリューム (ブート・パーティション、オペレーティング・システム、Data Protector を含むパーティション) が自動的に復元されます。

フェーズ 3:

6. Data Protector の標準復元手順で、ユーザー・データとアプリケーション・データを復元します。

重要 最初に復元する必要がある重要なシステム (特に DNS サーバ、Cell Manager、Media Agent クライアント、ファイル・サーバなど) については、障害復旧 CD をあらかじめ用意しておいてください。

ワンボタン障害復旧 (OBDR)

ワンボタン障害復旧 (OBDR) とは、Windows クライアントおよび Cell Manager 向けの高度に自動化された Data Protector 復旧方法であり、ユーザーの介入は最小限で済みます。サポートされているオペレーティング・システムの詳細は、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』を参照してください。

この方法では、関連するすべての Windows 環境データが、バックアップ時に自動的に収集されます。フル・バックアップ時には、一時的な DR OS のセットアップと構成に必要なデータが収集されて 1 つの大きな OBDR イメージ・ファイルにまとめられ、バックアップ・テープ上に保存されます。障害発生時には、OBDR デバイス (CD ROM をエミュレートできるバックアップ・デバイス) を使用して、OBDR イメージ・ファイルと障害復旧情報を格納したテープからターゲット・システムを直接ブートできます。

次に Data Protector により障害復旧オペレーティング・システム (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、最後に元のオペレーティング・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元されます。

重要 ハードウェア、ソフトウェア、または構成を変更したときには、新しい OBDR ブート・テープを作成する必要があります。IP アドレスや DNS サーバの変更など、ネットワーク構成を変更した場合も、同じように新しい OBDR ブート・テープを作成する必要があります。

Cell Manager 用にワンボタン障害復旧を使用する一般的な手順は、以下のとおりです。

ワンボタン障害復旧手順

フェーズ 0:

1. OBDRバックアップを準備します(Data Protectorワンボタン障害復旧ウィザードを使用するバックアップ仕様を作成します)。

フェーズ 1:

2. 復旧テープからブートし、復旧の範囲を選択します。

フェーズ 2:

3. デフォルトでは、クリティカル・ボリューム (ブート・パーティション、オペレーティング・システム、および Data Protector を含むパーティション) が復元されます。

フェーズ 3:

4. Data Protector の標準的な復元手順に従って、上記以外のパーティションを復元します。

重要　　OBDR ブート・テープへのアクセス権は適切に制限することをお勧めします。

自動システム復旧

ASR (Automated System Recovery) とは Windows システム上で使用可能な自動システム復旧機能で、障害発生時にディスクを元の状態に戻すことができます。新しいディスクが元のディスクよりも大きい場合は、パーティションのサイズ変更も可能です。復旧対象には、ディスクのパーティション設定や論理ボリューム構成 (ファイル・フォーマット、ドライブ文字割り当て、ボリューム・マウントポイント、ボリューム特性など) も含まれます。このように、ASR を使用すると Data Protector の `drstart.exe` コマンドによるアクティブ DR OS のインストールが可能になり、この DR OS により Data Protector ディスク、ネットワーク、テープ、およびファイルシステムなどへのアクセスが可能になります。

上記の操作を経て Data Protector によりターゲット・システムが元のシステム構成に戻され、最後にすべてのユーザー・データが復元されます。

サポートされているオペレーティング・システムの詳細は、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』を参照してください。

Windows クライアントに対する ASR による障害復旧の一般的な手順は、以下のとおりです。

ASR の手順

フェーズ 0:

1. クライアントのフル・バックアップを実行します。
2. Data Protector バイナリを格納した ASR フロッピーを用意し、構成を変更する都度 1 枚目のフロッピーを更新します。

フェーズ 1:

3. Windows のインストール・メディアからブートし、**F2** キーを押して ASR モードに入ります。

4. ASR セット内の (更新済みの) 1 枚目のフロッピーを挿入します。
5. 再ブート後、DR インストールおよび SRD ファイル (a:¥) の位置に関する情報を指定します。
6. 要求にしたがって、ディスクを交換します。

フェーズ 2:

7. すべての重要なオブジェクトが自動的に復元されます。システムを再ブートし、Windows インストール・メディアと ASR ディスクを取り出します。

フェーズ 3:

8. Data Protector の標準的な復元手順に従って、ユーザー・データとアプリケーション・データを復元します。

ASR は、障害に備えた準備作業 (の一部) の実行と、ブート・パーティションの再作成、再フォーマットの実行に使用されます。容易な集中管理、高性能なバックアップ、高可用性のサポート、容易な復元、モニタリング、レポート作成、通知などのその他の機能はすべて、Data Protector により提供されます。

各種の障害復旧方法の概要

表 2-6 は、Data Protector が提供する各種の障害復旧方法の概要を示したものです。サポート対象プラットフォームの一覧については、120 ページの表 2-7 を参照してください。

表 2-6 障害復旧方法の概要

	フェーズ 0	フェーズ 1	フェーズ 2	フェーズ 3
手動による障害復旧	クライアントのフル・バックアップ、IDB バックアップ (Cell Manager の場合のみ)。SRD ファイルの更新 (Windows の場合のみ)。DR OS のインストールと構成に必要な情報を元のシステム上で収集。	DR OS をネットワーク機能とともにインストール。ディスクのパーティションを再作成し、元の格納構造を再構築。	`drstart` コマンドを実行して、クリティカル・ボリュームを自動的に復旧。高度な復旧作業を実行する場合は、追加の作業が必要。『*HP OpenView Storage Data Protector 管理者ガイド*』を参照。	Data Protector の標準的な復元手順に従って、ユーザー・データとアプリケーション・データを復元します。

表 2-6 障害復旧方法の概要 (続き)

	フェーズ 0	フェーズ 1	フェーズ 2	フェーズ 3
ディスク・デリバリーによる障害復旧 (DDDR)	クライアントのフル・バックアップ、IDB バックアップ (Cell Manager の場合のみ)、補助ディスクの作成 (UNIX の場合のみ)。	Windows の場合 : 交換用ディスクをホスティング・システムに接続。 UNIX の場合 : 補助ディスクをターゲット・システムに接続。 すべてのシステム: 交換用ディスクのパーティションを再作成し、元の格納構造を再構築。	Windows の場合 : DDDR ウィザードを使用してクリティカル・ボリュームを復元し、交換用ディスクをホスティング・システムから取り外して、ターゲット・システムに接続し直す。 UNIX の場合 : 元のシステムのブート・ディスクを交換用ディスク上に復元し、補助ディスクを取り外す。 すべてのシステム : システムを再ブート。 高度な復旧作業を実行する場合は、追加の作業が必要。詳細は『*HP OpenView Storage Data Protector 管理者ガイド*』を参照。	Data Protector の標準的な復元手順に従って、ユーザー・データとアプリケーション・データを復元します。
高度な自動障害復旧 (EADR)	クライアントのフル・バックアップ、IDB バックアップ (Cell Manager の場合のみ)。SRD の準備と更新。DR CD の準備。	DR CD からシステムをブートし、復旧の範囲を選択。	クリティカル・ボリュームの自動復元。 高度な復旧作業を実行する場合は、追加の作業が必要。詳細は『*HP OpenView Storage Data Protector 管理者ガイド*』を参照。	Data Protector の標準的な復元手順に従って、ユーザー・データとアプリケーション・データを復元。

表 2-6 障害復旧方法の概要 (続き)

	フェーズ 0	フェーズ 1	フェーズ 2	フェーズ 3
ワンボタン障害復旧 (OBDR)	OBDR ウィザードを使用してクライアントのフル・バックアップを実行。SRD の準備と更新。	OBDR テープからターゲット・システムをブートし、復旧の範囲を選択。	クリティカル・ボリュームの自動復元。	Data Protector の標準的な復元手順に従って、ユーザー・データとアプリケーション・データを復元。
自動システム復元 (ASR)	クライアントのフル・バックアップを実行し、更新済みの SRD ファイルと DP バイナリを格納した ASR フロッピーを準備。	Windows のインストール・メディアからシステムをブートして、ASR モードに移行。ASR フロッピーを挿入。	クリティカル・ボリュームが復元。高度な復旧作業を実行する場合は、追加の作業が必要。詳細は『*HP OpenView Storage Data Protector 管理者ガイド*』を参照。	Data Protector の標準的な復元手順に従って、ユーザー・データとアプリケーション・データを復元。

以下に示す手順は、次のフェーズに進む前に完了しておかなければなりません。

- フェーズ 0: クライアントのフル・バックアップと IDB のバックアップ (Cell Manager の場合のみ) を実行し、さらに管理者は DR OS のインストールと構成に必要な情報を元のシステムから収集しておかなければなりません。UNIX 上でディスク・デリバリーによる障害復旧を実行する場合は、補助ブート・ディスクの作成も必要です。
- フェーズ 1: DR OS をインストールして構成し、元の格納構造を再構築して、すべてのボリュームの復元が可能な状態にしなければなりません。UNIX 上のディスク・デリバリーによる障害復旧に使用する交換用ディスクは、ブート可能でなければなりません。
- フェーズ 2: クリティカル・ボリュームを復元します。高度な復旧作業を実行する場合は、追加の作業を実施します。詳細は『*HP OpenView Storage Data Protector 管理者ガイド*』を参照。
- フェーズ 3: アプリケーション・データが正しく復元されているかどうかを確認します (データベースの整合性チェックなど)。

障害復旧方法とオペレーティング・システムの対応

次の表は、サポートされる障害復旧方法とオペレーティング・システムの組み合わせを示したものです。これらの組み合わせについては、以下の項で詳しく説明します。

注記 これらの障害復旧方法を実際に運用する前に、個々の方法の制限事項について確認しておいてください。

表 2-7 サポートされる障害復旧方法とオペレーティング・システムの対応

	Cell Manager	クライアント
Windows 2000	• 補助付き手動障害復旧 • 高度な自動障害復旧 • ワンボタン障害復旧	• 補助付き手動障害復旧 • ディスク・デリバリーによる障害復旧 • 高度な自動障害復旧 • ワンボタン障害復旧
32 ビットの Windows XP/Server 2003[a]	• 補助付き手動障害復旧 • 自動システム復旧	• 補助付き手動障害復旧 • ディスク・デリバリーによる障害復旧 • 自動システム復旧
64 ビット Windows Server 2003		• 補助付き手動障害復旧 • 自動システム復旧
HP UX 11.x	• 手動による障害復旧	• 手動による障害復旧 • ディスク・デリバリーによる障害復旧
Solaris 7/8	• 手動による障害復旧	• ディスク・デリバリーによる障害復旧
Tru64/AIX		• ディスク・デリバリーによる障害復旧

a. Windows XP Home Edition では ASR は使用できないため、サポートされていません。

その他の障害復旧方法

本項では、Data Protector を使った障害復旧の概念と、他社製品の障害復旧の概念を比較します。ここでは、この問題を詳しく取り上げることはしませんが、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・システムを一からインストールし直します。
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。

他社製ツールを使った復旧 (Windows 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 (他社製ツールを使用)。
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、クラスタ化にも対応しているため、高速かつ効率的に障害復旧を実行できます。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。

3　メディア管理とデバイス

本章の内容

本章では、Data Protector におけるメディア管理とデバイス管理の概要について説明します。以下ではメディア・プール、デバイス、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。

この章の構成は以下のとおりです。

メディア管理

バックアップ・セッションの構成が終了したら、次に、バックアップ・セッションが途中で中断されないようにするための、適切なメディア管理が大切になります。大容量のバックアップ操作を実行する場合は、数千ものメディアの管理が必要になることも珍しくありません。

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)。
- メディアの自動交換方針を設定でき、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。
- メディアのデータの追加コピーを対話的または自動的に作成します。

本章では、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、Data Protector で使用するためのメディアの初期化 (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。

   詳細は、139 ページの「バックアップ開始前のメディア管理」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。

   詳細は 141 ページの「バックアップ・セッション中のメディア管理」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。

   ボールティングの詳細は、146 ページの「バックアップ・セッション後のメディア管理」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 (Poor) マークが付加され、Data Protector では使用されなくなります。

   詳細は、145 ページの「メディア状態の計算」を参照してください。

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。例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。つまりメディアがドライブ内にあるか、ライブラリのレポジトリ・スロット内にあるか、または保管場所やその他の場所にあるかといったことは、プールとの対応付けとは無関係です。各メディアはリサイクルされてセルからエクスポートされるまでは、指定されたプールに所属しています。

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 (Appendable)]

  このオプションを設定すると、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 (Appendable on Incrementals Only)]

  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。

- メディア割り当て方針

  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が、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・プールのプロパティの詳細は、『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。

メディア・プールと dcbf 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 dcbf ディレクトリを設定できます。ターゲット dcbf 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 dcbf ディレクトリの詳細は、189 ページの「IDB のアーキテクチャ」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・プールはユーザーが自由に設定できます。例えば、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 2000 システム用、Windows XP 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 (各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方針を適用できるため、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方針が適用されます。

デフォルト・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。

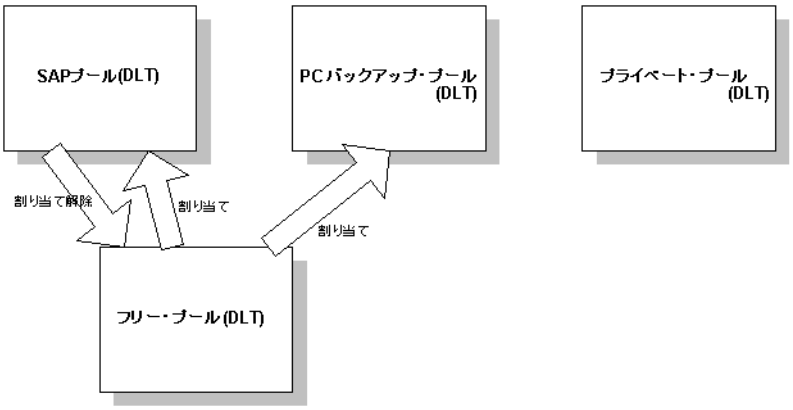
フリー・プール

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。

図 3-1　　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（図 3-1 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。図 3-1 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、後ですべてのプールにフリー・メディアを割り当てる際に使用されます。

図 3-1 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・プールは自動的に作成されます。使用中のフリー・プールや空でないフリー・プールは削除できません。
- Data Protector では各メディア・タイプ (DDS など) に対して 1 つのフリー・プールしかサポートしないため、フリー・プールはメディア・タイプ固有のプールになります。
- 通常のプールと異なり、割り当て方針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

フリー・プールには、以下の制限があります。

- フリー・プールは Data Protector によって自動的に作成されるため、同じメディア・タイプのフリー・プールを複数作成することはできません。
- 各プールごと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、そのフリー・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 (例えば無期限に変更) 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・プールについての詳細は、Data Protector のオンライン・ヘルプで「フリー・プール」をキーワードに指定して確認してください。

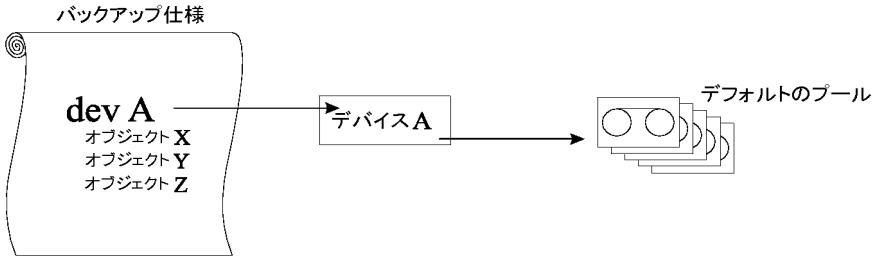
メディア・プールの使用例

バックアップ環境を選択する上で考慮可能な構成例を以下に示します。

例 1

図 3-2 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。

図 3-2　　単一デバイス / 単一メディア・プールの単純な対応付け

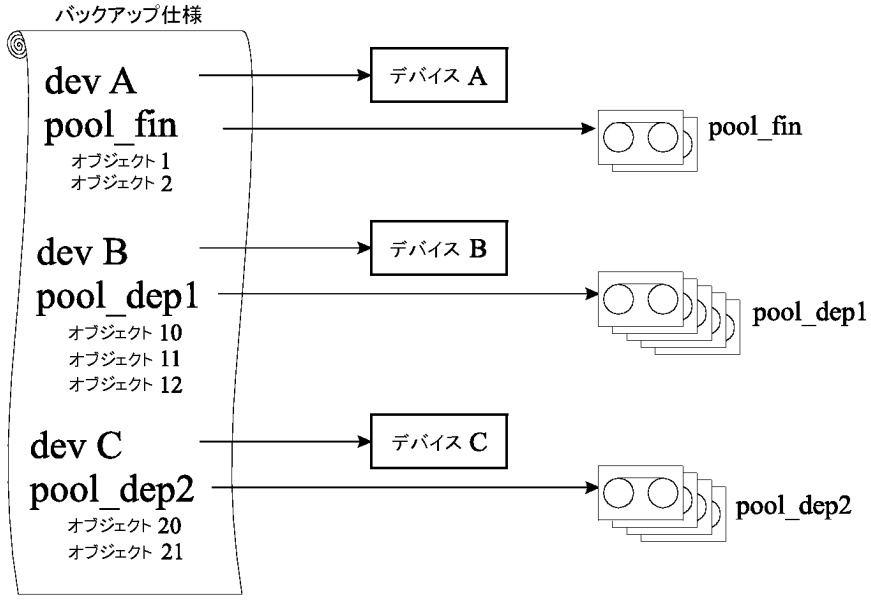


例 2

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、図 3-3 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、158 ページの「大容量ライブラリ」を参照してください。

図 3-3　　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

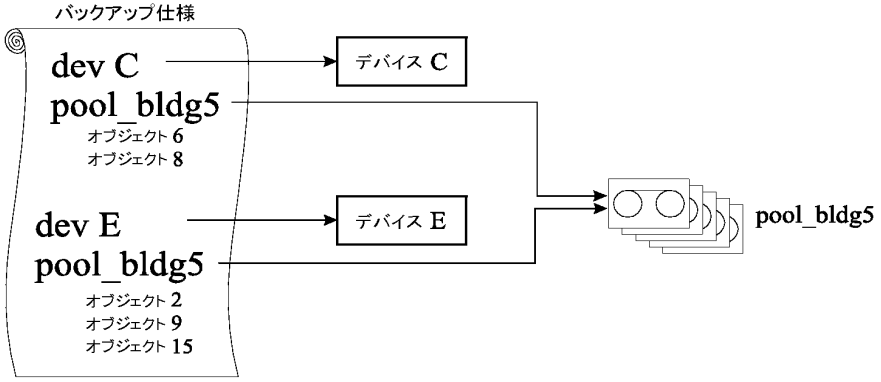


例 3

図 3-4 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。

詳細は、150 ページの「デバイス・リストと負荷調整」を参照してください。

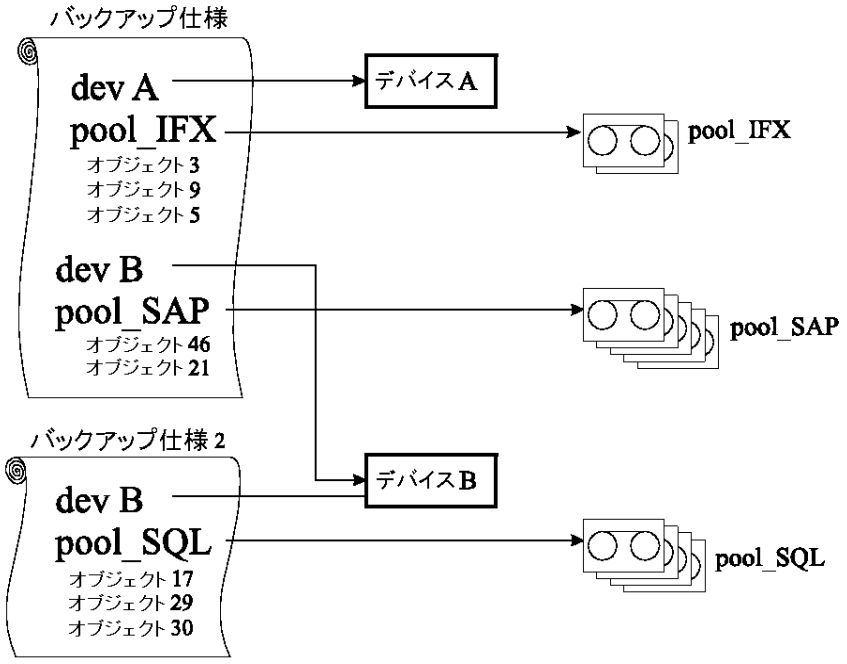
図 3-4　　複数デバイスと単一メディア・プールの対応付け



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。

図 3-5　　複数デバイスと複数メディア・プールの対応付け



メディア交換方針の実装

メディア交換方針とは

メディア交換方針とは、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。メディア交換方針を定義するときは、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、メディア交換方針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方針を実装し、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

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。

自動メディア交換と自動メディア操作

- 複数のメディアをメディア・プール内にまとめられるため、それぞれのメディアを個別に管理する必要がありません。メディア・プール内の各メディアは自動的にトラッキング、管理されます。
- バックアップ・データを書き込むメディアは、Data Protector により自動的に選択されるため、バックアップ先となるメディア・プールを指定するだけでよく、使用するメディアを個別に指定する必要はありません。
- Data Protector では、指定したメディア割り当て方針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・インタフェースを使用して、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を保持するかを決定します。この数を超えれば、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。詳細は、141 ページの「バックアップ用メディアの選択」を参照してください。

メディアの初期化 (フォーマット)

メディアの初期化 (フォーマット) とは

Data Protector では、バックアップに使用するメディアを、まず初期化 (フォーマット) しなければなりません。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) 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。

設定したプール方針によっては、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。詳細は、141 ページの「バックアップ用メディアの選択」を参照してください。

Data Protector メディアのラベリング

Data Protector で使われるメディア・ラベル

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。メディアの初期化時に、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。

各メディアに対しては、Data Protector によっても、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。

他のシステムで識別するために、ANSI X3.27 ラベルもテープに書き込まれます。Data Protector では、ラベルは他の情報とともにメディアのヘッダと IDB に書き込まれます。

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、そのメディアのメディア ID が自動的にチェックされます。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が判断されます。例えば、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 (Location)] 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。例えば、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。

各メディアの [位置 (Location)] フィールドは、オペレータが自由に変更できます。このフィールドは、メディア位置のトラッキングに役立ちます（ライブラリ (In Library)、オフサイト (off-site)、ボールト 1(vault_1) など)。

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・セット選択の詳細は、102 ページの「メディア・セットの選択」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

バックアップ中の処理内容

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、以下の項も参照してください。

- 65 ページの「フル・バックアップと増分バックアップ」
- 128 ページの「メディア・プール」

バックアップ用メディアの選択

Data Protector では、メディア割り当て方針に基づいて、バックアップ用メディアが自動的に選択されます。そのため、バックアップ・オペレータが手動でバックアップ用メディアを管理する必要はなく、メディアの管理と取り扱いが容易になります。

メディア割り当て方針

バックアップ用メディアの選択方法は、メディア割り当て方針に基づいて決定されます。方針に [Loose] と指定した場合は、新しいメディアや空のメディアも含めて、適切な任意のメディアが使用されるようになります。一方 [Strict] と指定した場合には、メディアの使用状況を均一化するために、事前に定義された順番でメディアがロードされなければなりません。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、メディア割り当て方針の [Strict] 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。例えば、状態が [良好 (Good)] のメディアは、状態が [普通 (Fair)] のメディアよりも優先的に使用されます。詳細は、145 ページの「メディア状態の計算」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。これは、メディア使用方針で設定します。

メディア使用方針

選択できるメディアの使用方針は、以下のとおりです。

[追加可能 (Appendable)] 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 (Non Appendable)] 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るため、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 (Appendable on Incrementals Only)] 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散

以下の図は、複数のオブジェクトを複数のメディア上に保存する場合の例を示したものです。

図 3-6　1 つのメディア上に複数セッションの複数オブジェクトを格納（順次書き込み）

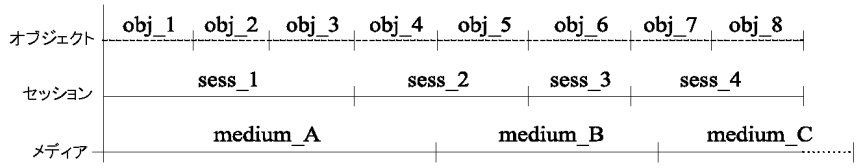


図 3-6 では、メディア使用方針に [追加可能 (Appendable)] を指定した状態で、4 つのセッションにわたって、8 つの順次書き込みを実行しています。データは、4 つのセッションにわたって書き込まれますが、1 度に書き込まれるオブジェクトは 1 つだけになります。3 つのメディアは、同一のメディア・プールに所属しています。*medium_A* と *medium_B* はすでに一杯になっていますが、*medium_C* にはまだ多少のスペースが残っています。

図 3-7　1 つのメディア上に複数セッションの複数オブジェクトを格納（並列書き込み）

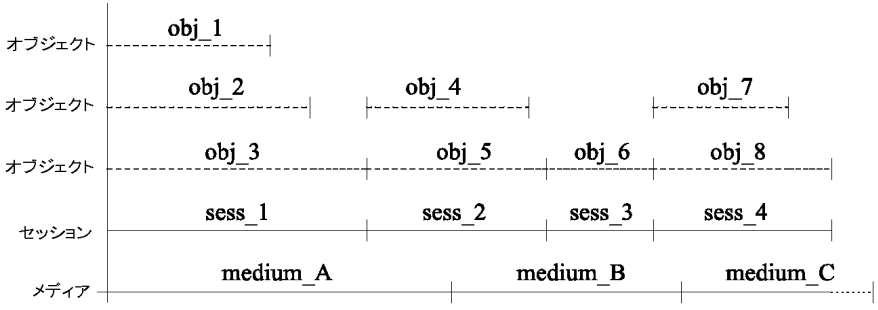


図 3-7 の例では、4 つのセッションで、並列処理を有効にして同時書き込みを可能にした状態で、8 つのオブジェクトを書き込んでいます。この場合、オブジェクト *obj_1*、*obj_2*、および *obj_3* は、*sess_1* セッション内で同時にバックアップされ、オブジェクト *obj_4* と *obj_5* は *sess_2* セッション内で同時にバックアップされる、というようになります。*obj_1* は *system_A*

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個別のディスク上の情報である場合も考えられます。メディア使用方針は、[追加可能 (Appendable)] に設定されています。

図 3-8　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格納

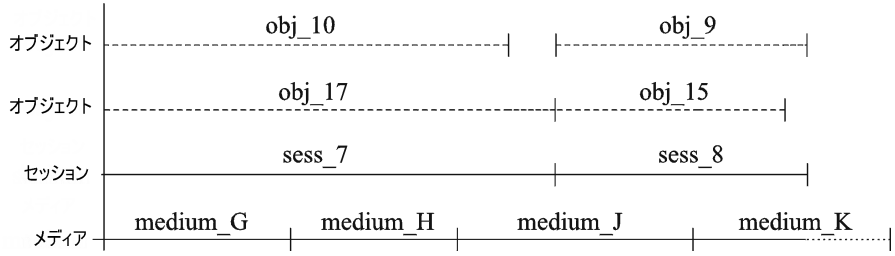


図 3-8 の例では、2 つのセッション内で 4 つのオブジェクトをバックアップしており、バックアップ・オブジェクトの最初のペアは *sess_7* で、2 番目のペアは *sess_8* でそれぞれ同時に書き込まれます。この場合、1 つのオブジェクトが、複数のメディアにまたがって書き込まれる可能性があることに注目してください。メディア使用方針は、[追加可能 (Appendable)] に設定されています。

図 3-9　各オブジェクトを個別のメディアに格納

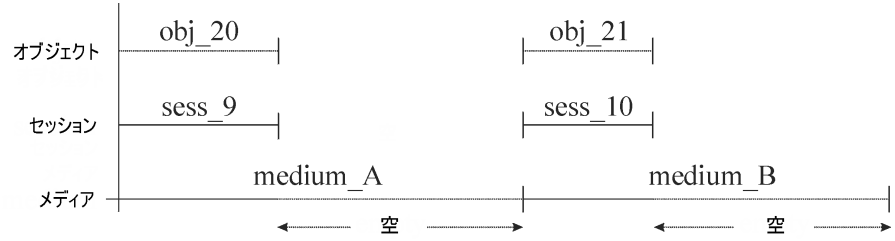


図 3-9 の例では、オブジェクトごとに 1 つのバックアップ仕様を作成し、メディア使用方針には [追加不可能 (Non Appendable)] を指定しています。この場合、メディア消費量は大きくなります。この方法で、メディア使用方針を [増分のみ追加可能 (Appendable on Incrementals Only)] に変更すると、同一オブジェクトの増分バックアップのみが同じメディア上に保存されるようになります。

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量に与える影響は、65 ページの「フル・バックアップと増分バックアップ」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。詳細は、96 ページの「オブジェクト・ミラーの作成」を参照してください。

メディア状態の計算

メディアの状態要素

Data Protector では、**メディアの状態要素**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。例えば、メディア・プール内のある 1 つのメディアの状態が不良 (Poor) になると、プールの状態も直ちに不良 (Poor) 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 (Fair) または良好 (Good) に戻ります。

メディアの状態には、[良好 (Good)]、[普通 (Fair)]、[不良 (Poor)] の 3 種類があります。

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。メディアの上書き回数が指定されたしきい値を超えると、不良 (Poor) マークが付加されます。

- 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。メディアの使用期間が指定された月数を超えると、不良 (Poor) マークが付加されます。

- デバイス・エラー

  ある種のデバイス・エラーが発生すると、メディアに不良 (Poor) マークが付加されます。例えばバックアップ中にデバイス障害が発生した場合は、そのデバイスでバックアップに使われていたメディアには、不良 (Poor) マークが付加されます。

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。以下の点に注意が必要です。

- 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。データ保護とカタログ保護は、72 ページの「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」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。

  詳細は、88 ページの「バックアップ・データの複製」を参照してください。

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

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、しばしば**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。

- データ保護方針とカタログ保護方針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** (media location)] 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に対する取り扱い方針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、適切なデータ保護期間とカタログ保護期間を設定します。
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 (Vault_1 など)。
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。

ボールティングの例

ここで、ある企業において、以下のようなバックアップ方針を実装する場合を想定してみます。この企業では、データのバックアップを毎日実行します。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。

この例の場合、週に 1 回フル・バックアップを実行し、それ以外の日は毎日増分バックアップを実行するよう、Data Protector で設定することになります。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。

保管場所内のメディアを使った復元処理

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方針によっては、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・インタフェー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・インタフェー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。

データ保護方針およびカタログ保護方針が復元処理に与える影響は、72 ページの「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」を参照してください。

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、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』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)、およびデフォルト・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 (例えばハードウェア・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。リモートから実行できる作業の範囲は、各ライブラリに実装されている管理コンソールによって異なります。

Data Protector は、ライブラリ管理コンソールのインタフェー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 ブラウザが起動され、ブラウザ内にコンソール・インタフェー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、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』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・デバイス状態のモニタリング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) 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。
- バックアップ処理の堅牢性を増したい場合。Data Protector では、あるデバイスに障害が発生した場合に、デバイス・リスト内の別のデバイスに、バックアップ処理を自動的にリダイレクトすることが可能です。

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節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・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

デバイスの性能を最大限に引き出すには、ストリーミングの維持が重要になります。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・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。ネットワーク依存度の高いバックアップ・インフラストラクチャでは、この点に注意が必要です。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 (Concurrency) 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・ストリーミングを維持するには、デバイスに十分な量のデータを送り続ける必要があります。Data Protector ではデバイス・ストリーミングを維持するために、デバイスにデータを書き込む働きをする個々の Media Agent に対して、複数の Disk Agent を開始できます。

Disk Agent の同時処理数

1 つの Media Agent に対して開始される Disk Agent の数を、**Disk Agent (バックアップ) の同時処理数**と呼び、デバイス用の**拡張**オプションで指定するか、バックアップの構成時に変更できます。ただし、ほとんどの場合は、Data Protector のデフォルト値を変更する必要はありません。例えば標準的な 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、バックアップ性能が向上します。例えば 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。

関連情報は、236 ページの「バックアップ・セッション」を参照してください。

複数のデータ・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 1 つのディスクのデータを並行して読み込み、そのデータを複数の Media Agent へ送信します。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。

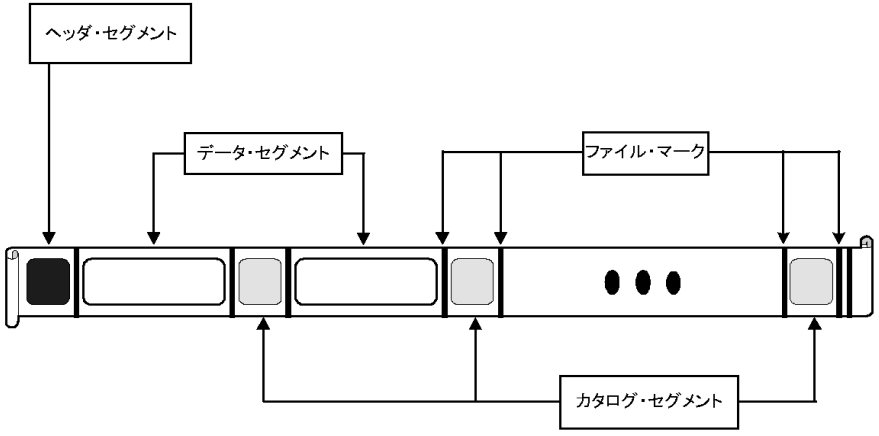
1 つのマウント・ポイントが複数の Disk Agent を通してバックアップされた場合、データは複数のオブジェクトに格納されます。マウント・ポイント全体を復元するには、1 つのバックアップ仕様でマウント・ポイントの要素をすべて定義した後、セッション全体を復元します。

セグメント・サイズ

メディアの内部は、複数のデータ・セグメントとカタログ・セグメント、および 1 つのヘッダ・セグメントから構成されています。ヘッダ情報は、ブロック・サイズと同じ長さのヘッダ・セグメントに格納されます。また、データは、データ・セグメントのデータ・ブロックに、各データ・セグメントについての情報は、対応するカタログ・セグメントのカタログ・ブロックに格納されます。このカタログ情報は最初に Media Agent メモリに格納され、次にメディア内のカタログ・セグメントと、IDB に書き込まれます。図 3-10 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。

注記　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。

図 3-10　　データ・フォーマット



セグメント・サイズ (MB 単位) は各データ・セグメントの最大サイズです。小さなファイルを大量に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よって制限を受けます。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。例えば、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

セグメントのデータは実際はブロックに保存され、カタログ・セグメントのカタログ情報はカタログ・ブロックに書き込まれます。デバイスのハードウェアは、デバイスタイプ固有のブロック・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のサイズを調整することができます。すべてのデバイスのデフォルト・ブロック・サイズ値は 64 KB です。

このブロック・サイズを大きくすると処理速度が向上します。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。例えば、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。

注記 追加可能 (appendable) なプール内のメディアについては、すべて同一のブロック・サイズを使用してください。Data Protector では、ブロック・サイズが同じメディアにしかデータを追加できません。

Disk Agent バッファの数

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・バッファを使用します。このメモリは複数のバッファ領域に分割されています (各 Disk Agent に 1 つずつ、デバイスの同時処理数によって異なる)。また、各バッファ領域は、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。この値を変更する理由としては、通常以下の 2 つが考えられます。

- 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。

  `Disk Agent` **の同時処理数 * バッファ数 * ブロック・サイズ**

  例えばバッファ数を 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。例えば、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

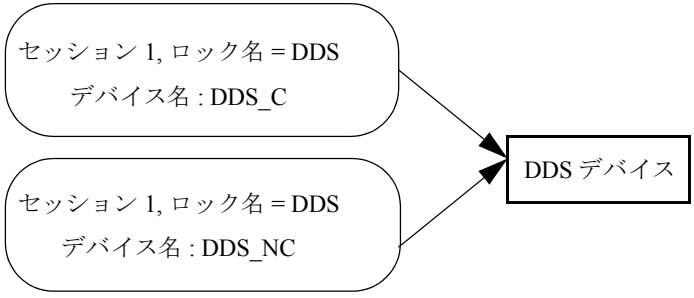
バックアップに使用するデバイスを指定するときに、あるバックアップ仕様内で 1 つのデバイス名を指定し、別のバックアップ仕様内で同じ物理デバイスの別名を指定していることがあります。このような場合、バックアップのスケジュール方法によっては、複数のバックアップ・セッションで同時に同一の物理デバイスを使おうとして、デバイスの衝突が発生する可能性があります。

衝突の防止

デバイスの衝突を防止するには、両方のデバイス構成時に仮想ロック名を指定してください。こうすると、デバイスのロック名が同一かどうかが自動的にチェックされて、衝突が防止されます。

例えば図 3-11 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。

図 3-11　　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

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のみが可能です。

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・インタフェースを使って、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かなければなりません。Data Protector では、大部分のスタンドアロン・デバイスを検出して、自動的に構成できます。

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。

このようにデバイス・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・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・デバイスとは

マガジン・デバイスでは、複数のメディアが、マガジンと呼ばれる単一のユニットにまとめられます。Data Protector では、マガジンは単一のメディアとして扱われます。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。サポート対象のデバイスの一覧は、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』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、マガジンに対するメディア管理タスクを実行できます。

また、Data Protector のマガジン・サポートを使用せずに、通常のライブラリとしてマガジン・デバイスを使用することも可能です。マガジン・デバイスであれば、Data Protector による検出と自動構成が可能です。

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、エクスチェンジャ、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-II 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。例えば、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、HP StorageWorks 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。サポート対象のデバイスの一覧は、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』を参照してください。

メディアの操作

Data Protector ユーザー・インタフェースには、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、空の (新しい) メディア、Data Protector メディア、または非 Data Protector メディアのいずれかが格納されることになります。Data Protector ではスロット内のメディアをチェックして、そのメディアに関する情報をライブラリ・ビュー内に表示できます。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 箇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。詳細は、136 ページの「メディア交換方針の実装」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。例えば 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。例えば、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 HP 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 / 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。例えば、1 つのデバイス内の 50 個のスロットを選択して、これらのメディアを 1 回の操作で取り出すことも可能です。メディアは正しい順番で自動的に取り出されるため、オペレータは挿入 / 取り出しメールスロットから順番にメディアを取り出すことができます。

詳細については、使用するデバイスに添付されているマニュアルを参照してください。

バーコード・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

HP 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。

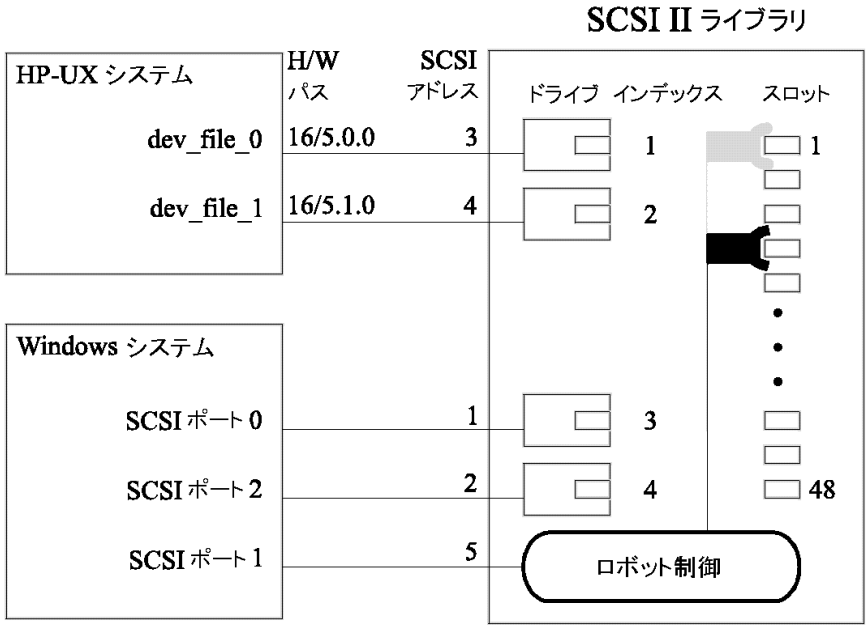
  ドライブが汚れていると、メディア上にデータを正しく書き込めず、バックアップが失敗する可能性があるため、ドライブをクリーニングするまではバックアップを続行できないようになっています。

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。この場合、これらのシステムでは、それぞれローカル・バックアップが可能になるため、性能が非常に向上し、また、ネットワーク・トラフィックも減少します。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-II 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、ロボティクス制御用のコマンドを、ロボティクスを管理するシステムに内部的にリダイレクトすることも可能です。

図 3-12　　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 Fibre Channel 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。

表 3-1 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。

表 3-1 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。

表 3-2 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。

表 3-2 ロボティスク制御に必要な 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 または 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

図 3-13 から図 3-15 までの図は、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。

図 3-13　SCSI ライブラリの共有 (ロボティスクを Data Protector クライアント・システムに接続)

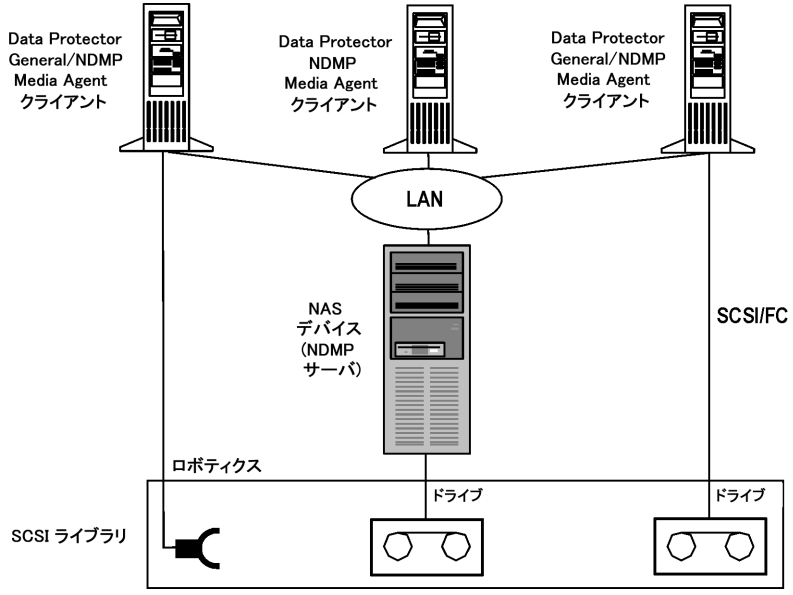


図 3-13 に示す SCSI ライブラリのロボティクスは、General Media Agent または NDMP Media Agent のインストールされた Data Protector クライアント・システムに接続され、そのクライアント・システム上に構成されています。このクライアント上の General Media Agent または NDMP Media Agent は SCSI ロボティクス制御プロトコルを使用します。ロボティクスを接続した Data Protector クライアント・システムに、さらに 1 つ以上のドライブを接続することも可能です。

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た Data Protector 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 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。このクライアント上の 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。

図 3-14　　SCSI ライブラリの共有 (ロボティクスを NDMP サーバに接続)

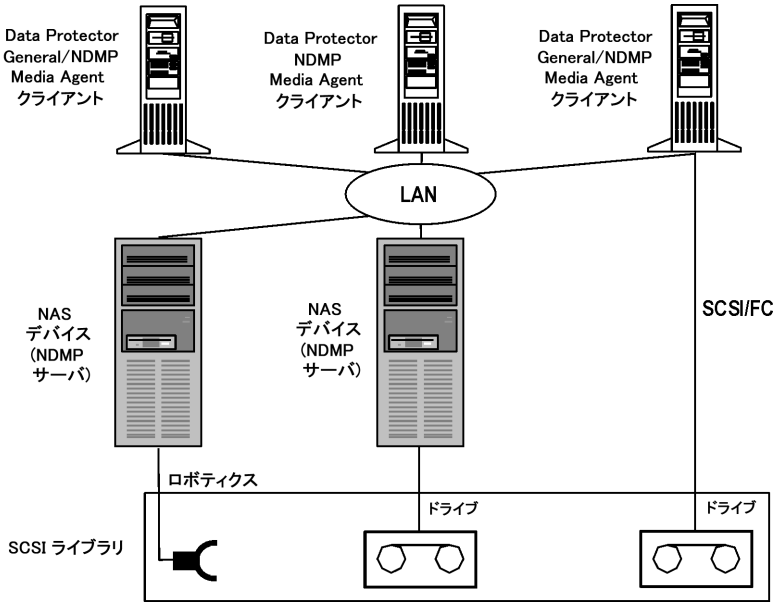


図 3-14 に示す SCSI ライブラリでは、ライブラリのロボティクスが NDMP サーバに接続され、General Media Agent または NDMP Media Agent のインストールされた Data Protector クライアント・システム上に構成されています。このクライアント上の General Media Agent または NDMP Media Agent は、SCSI ロボティクス制御プロトコルを使用します。ロボティクスを接続した NDMP サーバに、さらに 1 つ以上のドライブを接続することも可能です。

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。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 つのドライブが、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。このクライアント上の 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。

図 3-15　　ADIC/GRAU ライブラリまたは StorageTek ACS ライブラリの共有

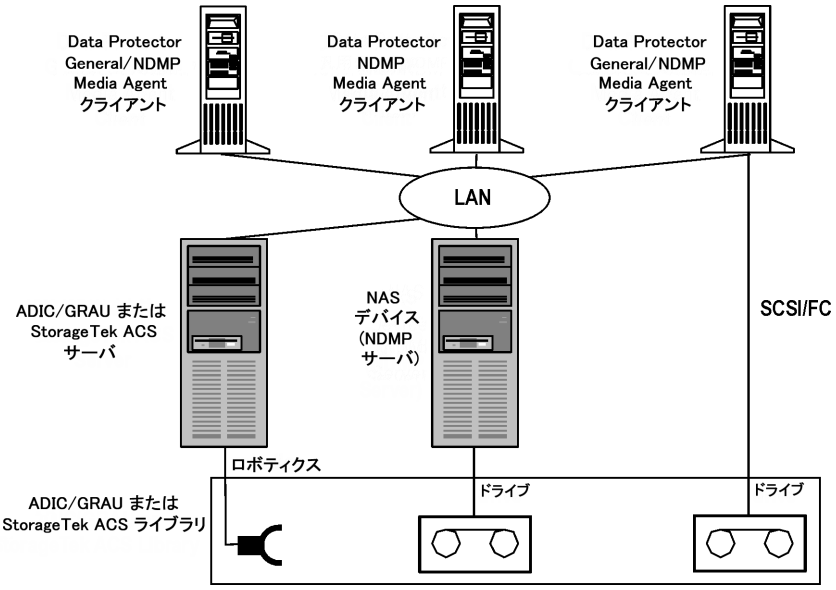


図 3-15 に示す ADIC/GRAU ライブラリ (または StorageTek ACS ライブラリ) では、ライブラリのロボティクスが ADIC/GRAU サーバ (または StorageTek ACS サーバ) に接続され、General Media Agent または NDMP Media Agent のインストールされた Data Protector クライアント・システム上に構成されています。このクライアント上の General Media Agent または NDMP Media Agent は、ADIC/GRAU ロボティクス制御プロトコルを使用します。ADIC/GRAU サーバや StorageTek ACS サーバに、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。

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 (Storage Area Network) ベースの Fibre Channel テクノロジを実装しており、新たなデータ記憶ソリューションの提供が可能です。

Storage Area Network

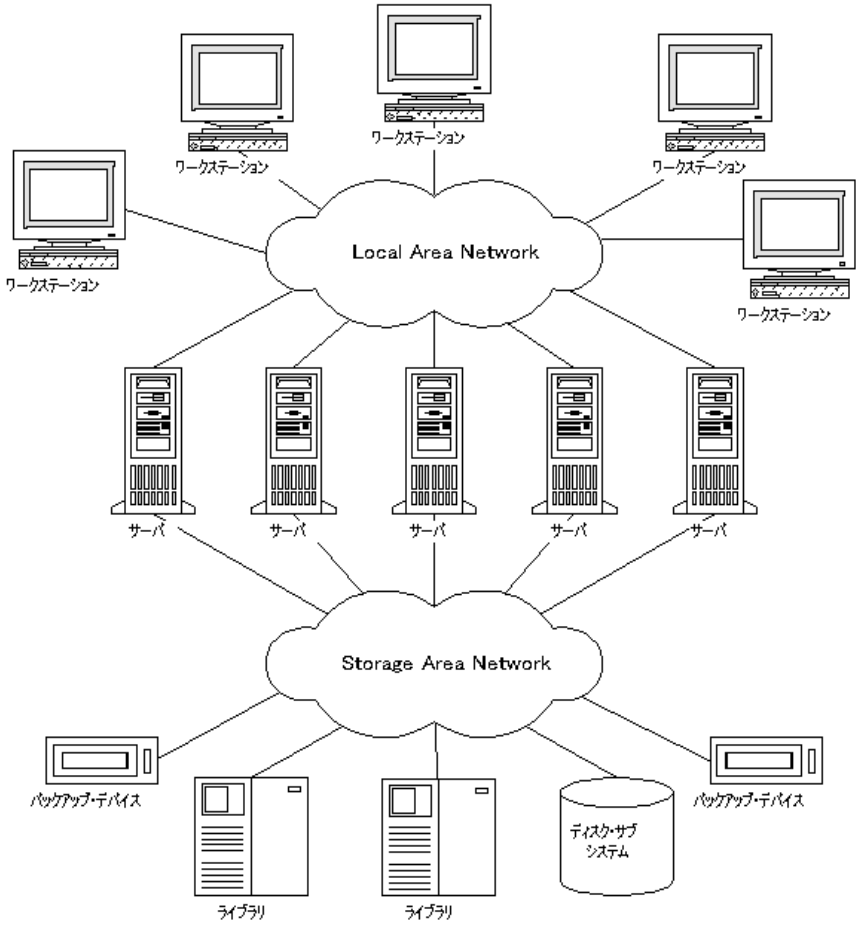
図 3-16 に示す Storage Area Network (SAN) は、ネットワークを介した記憶管理の新しい方式であり、記憶装置専用のネットワークを使用して、記憶管理とサーバ管理を切り離すことができます。

SAN を導入すると、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間での情報交換が可能になります。サーバは、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、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 Fibre Channel) 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。

Data Protector のダイレクト・バックアップ機能は、SAN および Fibre Channel の技術を効果的に活用しています。

図 3-16　　Storage Area Network



Fibre Channel

Fibre Channel は、高速のコンピュータ相互接続に関する ANSI 標準です。光ケーブルまたは銅線ケーブルを使って、大容量データ・ファイルを最大 4.25GB/ 秒で双方向送信でき、30km の範囲にあるサイト間を接続できます。Fibre Channel 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。

Fibre Channel は、ノード間を次の 3 種類の物理トポロジー (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 Fibre Channel トポロジーは、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。

サポート対象構成の詳細については、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』または http://www.openview.hp.com/products/datapro/spec_0001.html を参照してください。

ポイント・トゥ・ポイント・トポロジー

ポイント・トゥ・ポイント・トポロジーでは、2 つのノード、一般的にはサーバとバックアップ・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・トポロジー

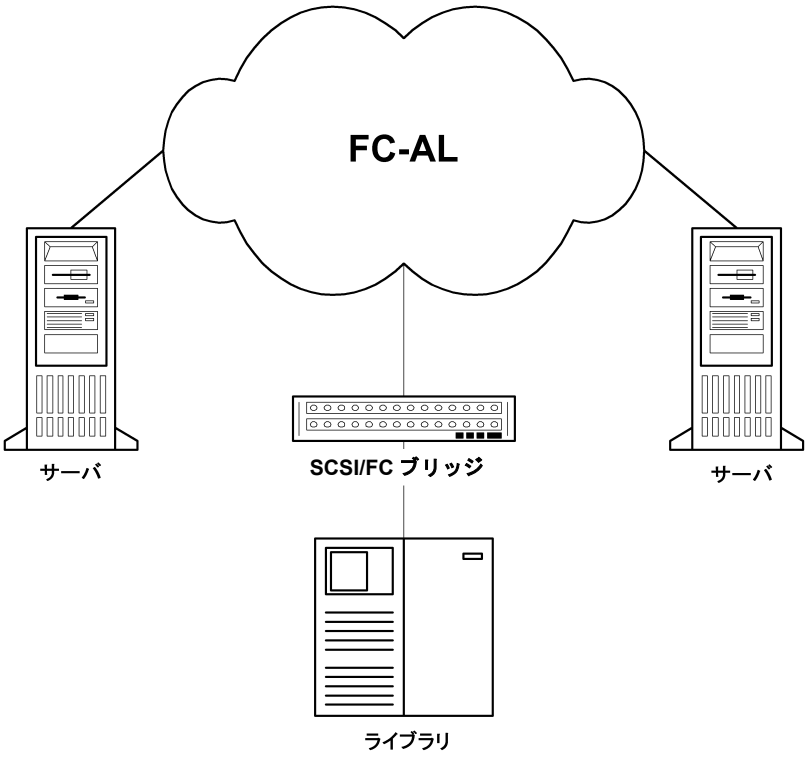
ループ・トポロジーは、FC-AL (Fibre Channel Arbitrated Loop) 標準をベースにしており、最大 126 台のノードを接続できます。ノードとなるのはサーバ、バックアップ・デバイス、ハブ、スイッチなどです。ループ内のすべてのノードは、そのループ内の任意のノードと通信でき、すべてのノードが同一の帯域幅を共有します。FC-AL ループの実装には、通常 FC-AL ハブと自動ポート・バイパスが使用されます。自動ポート・バイパスを使うと、ループへのノードのホットプラグが可能になります。

LIP

LIP (Loop Initialization Primitive) プロトコルはさまざまな場合に起動されますが、最も一般的なのは新しいデバイスが導入された場合です。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 ブリッジとノード (SCSI デバイス) 間の SCSI 接続がリセットされます。詳細は、図 3-17 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 は書き込みエラーが発生するとすべての処理を中止します。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。

図 3-17　　Loop Initialization プロトコル



スイッチ式トポロジー

スイッチ式トポロジーでは、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。Fibre Channel 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ーでは、ノードの真のホットプラグ機能が実現されます。

注記 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 は SAN の概念をサポートしており、SAN 環境のバックアップ・デバイスを複数のシステム間で共有できます。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 Fibre Channel 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・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。このために使われるのがロック機構です。

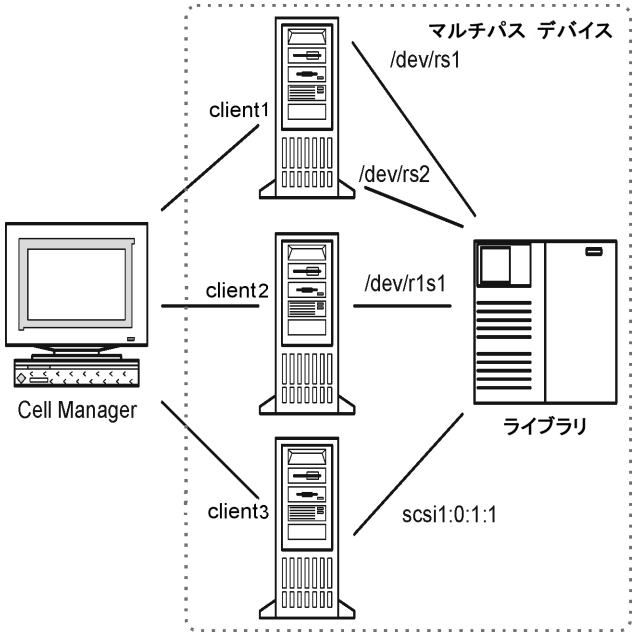
SAN テクノロジでは、複数のシステムからライブラリのロボティクス・デバイスを制御するための、非常に優れた方法が用意されています。そのため、1 つのシステムからのみロボティクスを制御できるようにも (従来の方法)、またはライブラリを使用する個々のシステムからロボティクスに直接アクセスできるようにも構成できます (関連するすべてのシステム間でロボティクスへの要求を同期化できることが前提)。

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 (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 は、このうちの任意のパスを使用できます。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。

例えば、あるデバイスが client1 上では、/dev/rs1 および /dev/rs2 として、client2 上では /dev/r1s1 として、また client3 上では scsi1:0:1:1 として構成されています。このため、client1:/dev/rs1、client1:/dev/rs2、client2:/dev/r1s1、および client3:scsi1:0:1:1 という 4 つの異なるパスを通してデバイスにアクセスすることができます。したがって、マルチパス・デバイスにはこのテープ・デバイスへの 4 つのパスすべてが定義されています。

図 3-18　　マルチパスの構成例



複数パスを使う理由

Data Protector の従来のバージョンでは、1 つのクライアントからのみデバイスにアクセスできました。そのためロック名を使用して、1 つの物理デバイスに対して複数の論理デバイスを定義する方法が採られてきました。しかし、ロック名を使用して複数のシステムから同一物理デバイスにアクセスできるようにする場合は、個々のシステム上にすべての論理デバイスを構成しなければなりません。例えば、10 台のクライアントが 1 つのデバイスに接続されている場合であれば、同じロック名を持つ論理デバイスを 10 個構成する必要があります。Data Protector の現在のバージョンでは、すべてのパスを単一のマルチパス デバイスとして構成することにより構成を簡便化することができます。

マルチパス デバイスは、システムの耐障害性の向上にも役立ちます。通常 Data Protector は、最初に定義されているパスからアクセスを試みます。1 つのクライアントのすべてのパスにアクセスできない場合は、次のクライアントのパスを使って試行します。定義されているいずれのパスも使用できなかった場合に限り、セッションは中止されます。

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パスが選択されます。ただし、次の場合は例外となります。

- バックアップ仕様で推奨クライアントが選択される。この場合、推奨クライアントが最初に使用されます。
- 直接ライブラリ・アクセスが使用可能になっている。この場合、ローカル・パス (対象クライアント上のパス) が最初に使用されます。

復元時には、次の順番でパスが選択されます。

- ローカル・パス
- バックアップ時に使用されたパス
- その他の使用可能なパス

以前のバージョンとの互換性

従来のバージョンの Data Protector 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・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。ロック機構の目的は、複数のシステム間で共有されるデバイスが、ある一時点では単一のシステムとのみ通信できるようにすることにあります。

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。

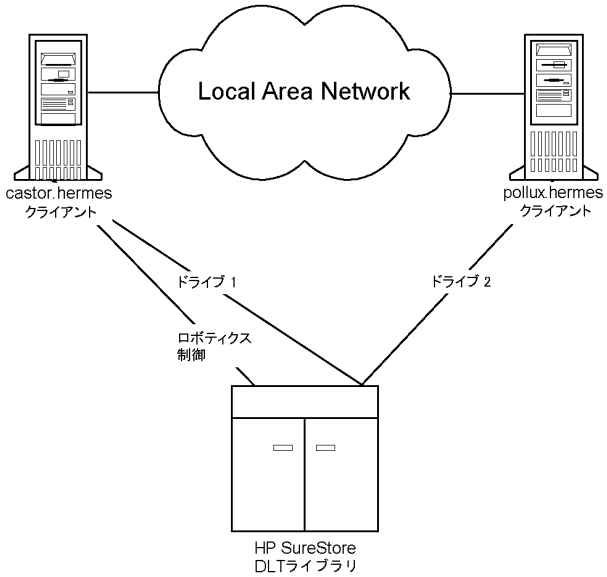
間接ライブラリ・アクセスと直接ライブラリ・アクセス

SCSI ライブラリ・デバイスとともに Data Protector を構成する場合は、クライアント・システムからライブラリ・ロボティクスにアクセスする方法として、直接ライブラリ・アクセスまたは間接ライブラリ・アクセスのいずれかを選択できます。

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。図 3-19 の例では、2 台のクライアント・システムが、1 台の HP StorageWorks 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。

図 3-19　　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。

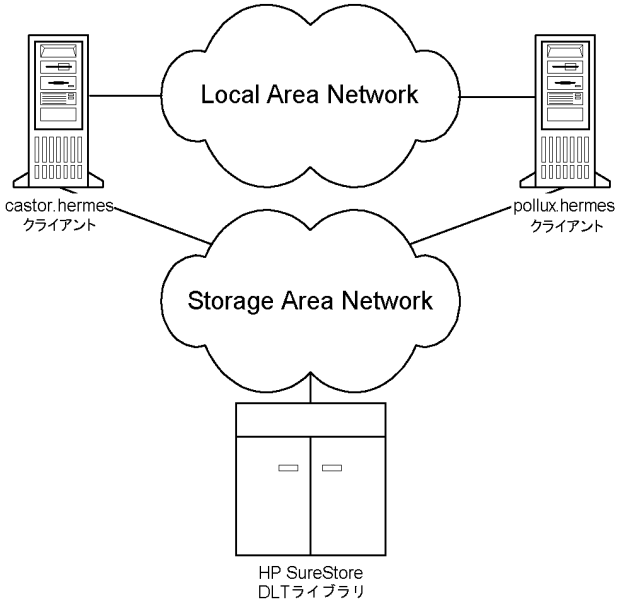
直接ライブラリ・アクセス

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、再構成の必要もありません。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。

図 3-20 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 HP StorageWorks 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。

図 3-20　　直接ライブラリ・アクセス



クラスタ内のデバイス共有

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。詳細は、174 ページの「デバイス・ロック」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、クラスタ対応アプリケーショは、クラスタ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

クラスタ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。

4　ユーザーとユーザー・グループ

本章の内容

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。

この章の構成は以下のとおりです。

Data Protector 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 の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、各ユーザーを作業内容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。

本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 には以下に示す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。他のユーザーには、そのデータがバックアップされていること自体がわからないようになっています。そのため、例えばバックアップ・オペレータ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 [**パブリックにする** (Is public)] オプションを使用します。詳細については『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。

ユーザーとユーザー・グループ

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モニター、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。

事前定義されたユーザー・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。例えば、[Admin] ユーザー・グループのメンバーのみがすべての Data Protector 機能にアクセスでき、[Operator] ユーザー・グループのメンバーは、デフォルトではバックアップの開始とモニターを実行できます。

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。

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 Cell Manager システム上の Windows 管理者
- Data Protector 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。

ユーザーとユーザー・グループ

事前定義されたユーザー・グループの使用

Data Protector が提供するデフォルトのグループを以下に示します。

表 4-1 Data Protector の事前定義されたユーザー・グループ

ユーザー・グループ	アクセス権
Admin	Data Protector の構成、バックアップと復元の実行、およびその他のすべての操作を行えます。
Operator	バックアップの開始、およびマウント要求への応答が行えます。
End-user	自分が所有するオブジェクトを復元できます。さらに、自分の復元セッションについては、セッションのモニタリングと、マウント要求への応答が行えます。

注記 [Admin] グループには非常に強力な権限が与えられています。Data Protector の [Admin] ユーザー・グループのメンバーには、Data Protector セル内の全クライアントに対して、システム管理機能を実行する権限があります。

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。例えば、[Admin] ユーザー・グループのすべてのメンバーには、Data Protector [Admin] ユーザー・グループの権限が与えられます。

UNIX Cell Manager 上で実行されている Data Protector 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。

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、オンライン・ヘルプ、または『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。

ユーザーとユーザー・グループ

5 Data Protector 内部データベース

本章の内容

この章では Data Protector 内部データベース (IDB) のアーキテクチャ、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。

この章の構成は以下のとおりです。

IDB について

Data Protector 内部データベース (IDB) とは

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、バックアップ・データの格納先メディア、バックアップ / 復元 / コピー / メディア管理の各セッションの結果、構成済みの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 を使用する 3 つの主な理由を以下に示します。

- 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
  Data Protector では、IDB に保存されている情報によって、バックアップ・セッションやコピー・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。

IDB のサイズおよびサイズの増大に関する注意点

IDB は非常に大きくなる場合があります。IDB のサイズの変動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。このため Data Protector の管理者は IDB を十分理解し、必要に応じて IDB に保存する情報や保存期間を決定する必要があります。管理者は復元時間や機能とのバランスを調整すると同時に IDB のサイズやサイズの増大の調整も行う責任があります。これらの調整を支援するために、Data Protector では、**ロギング・レベル**と**カタログ保護**という 2 つの重要なパラメータを用意しています。199 ページの「IDB の増大と性能」も参照してください。

Windows Cell Manager 上の IDB

IDB の場所

Windows Cell Manager 上の IDB は *<Data_Protector_home>*¥db40 ディレクトリにあります。

IDB の形式

Windows Cell Manager 上の IDB では、すべてのテキスト情報が 2 バイトの UNICODE 形式で保存されます。このため、ASCII 形式で情報を保存する UNIX Cell Manager 上の IDB に比べて、IDB のサイズの増大が多少速くなります。

UNICODE 形式では、ファイル名やメッセージの他言語へのローカライズが完全にサポートされます。

UNIX Cell Manager 上の IDB

IDB の場所

UNIX Cell Manager 上の IDB は /var/opt/omni/server/db40 ディレクトリにあります。

IDB の形式

HP-UX および Solaris Cell Manager 上の IDB では、すべてのテキスト情報が ASCII のシングルバイト形式およびマルチバイト形式で保存されます。

ASCII 形式の場合、ファイル名やメッセージの他言語へのローカライズに制限があります。ファイル名が 2 バイト形式 (UNICODE など) のファイルをバックアップした場合、ファイル名が ASCII 形式に変換され、Data Protector のユーザー・インタフェースに正しく表示されない場合があります。ただし、ファイルやファイル名は正常に復元されます。

詳細は、372 ページの「国際化」を参照してください。

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 機能の詳細は、15 ページの「企業環境」を参照してください。

IDB のアーキテクチャ

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)、ファイル名とその他の CDB レコードの 2 つの部分から構成
- 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)
- SIBF (NDMP 統合用のサーバレス統合バイナリ・ファイル)

以上の IDB の構成要素は、それぞれ特定の Data Protector 情報 (レコード) を保存しており、IDB のサイズやサイズの増大にさまざまな点で影響を与えます。各構成要素は Cell Manager 上の別々のディレクトリに配置されています。詳細は、図 5-1 を参照してください。

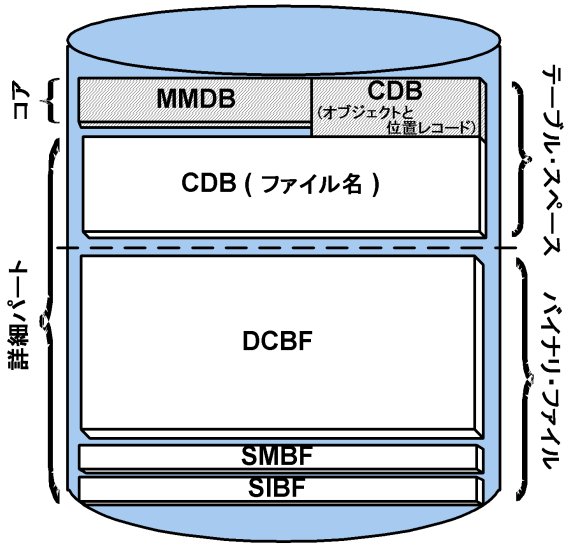
データベースの強度に関する注意点や IDB ディレクトリの再配置によるデータベース強度の最適化に関する推奨事項については、『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。

基礎となる技術

MMDB と CDB の各部分は、テーブル・スペースを含む組込みデータベースを使って実装されています。この組込みデータベースは RDS データベース・サーバ・プロセスが制御しています。MMDB や CDB への変更はすべてトランザクション・ログを使って更新されます。トランザクション・ログは `db40¥logfiles¥syslog` ディレクトリに保存されます。CDB (オブジェクトと位置レコード) と MMDB 部分は IDB のコア部分を構成します。

IDB の DCBF、SMBF、および SIBF の各部分はバイナリ・ファイルで構成されています。更新は直接 (トランザクションなしで) 行われます。

図 5-1　　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では、以下の情報を保存しています。

- 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 のサイズとサイズの増大

MMDB のサイズはそれほど大きくなりません。MMDB で一番大きな割合を占めるのは通常 Data Protector メディアに関する情報で、容量は 30MB 程度です。詳細は、206 ページの「IDB サイズの見積もり」を参照してください。

MMDB の場所

MMDB は以下のディレクトリにあります。

- Windows の場合 : *<Data_Protector_home>*¥db40¥datafiles¥mmdb
- UNIX の場合 : /var/opt/omni/server/db40/datafiles/mmdb

カタログ・データベース (CDB)

CDB レコード

カタログ・データベースでは、以下に関する情報を保存しています。

- バックアップ、復元、コピー、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。
- バックアップ・オブジェクトのメディア上の位置に関する情報。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・コピーやオブジェクト・ミラーについても同様に情報を保存します。
- 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。ファイル名は 1 つのクライアント・システムごとに 1 度だけ保存されます。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 CDB に追加されます。

ファイル名のサイズとサイズの増大

CDB で最も大きな容量を占め、またサイズの増大が速いのはファイル名の部分です。通常、データベース全体の 20% をこの情報が占めています。

ファイル名部分の増大速度はバックアップ環境の増大速度や変動には比例しますが、バックアップ回数には比例しません。

ファイルまたはディレクトリは、HP-UX または Solaris Cell Manager の場合は IDB の約 50 ～ 70 バイト、Windows Cell Manager の場合は 70 ～ 100 バイトを占めます。

ファイル名は、fnames.dat ファイルに保存されます。また、長さに応じてその他のいくつかのファイルにも格納されます。各ファイルの最大サイズは 2 GB です。いずれかのファイルの空きスペースが少なくなってくると、新しいファイルを追加して IDB のファイル名部分のサイズを拡張することを促すメッセージが表示されます。

CDB (オブジェクトと位置レコード) のサイズとサイズの増大

ファイル名以外の部分の CDB レコードが IDB で占める割合はそれほど大きくありません。中規模のバックアップ環境では 100MB 程度になります。詳細は、206 ページの「IDB サイズの見積もり」を参照してください。

CDB の場所

CDB は以下のディレクトリにあります。

- Windows の場合 : *<Data_Protector_home>*¥db40¥datafiles¥cdb
- UNIX の場合 : /var/opt/omni/server/db40/datafiles/cdb

詳細カタログ・バイナリ・ファイル (DCBF)

DCBF の情報

詳細カタログ・バイナリ・ファイル部分にはファイルのバージョン情報が保存されます。この情報には、ファイル・サイズ、変更時刻、属性 / 保護などのバックアップ・ファイルに関する情報が含まれます。

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、古いバイナリ・ファイルが削除され、新しいファイルが作成されます。

DCBF のサイズとサイズの増大

[**すべてログに記録** (Log All)] 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 (通常 80%)。各バックアップ・ファイルの各バージョンごとに約 30 バイトが使用されます。実際に何をどのくらいの期間 IDB に保存するかは、ロギング・レベルとカタログ保護で指定できます。200 ページの「IDB の増大と性能 に関する主要な調整可能パラメータ」を参照してください。

デフォルトでは、DC ディレクトリ (db40¥dcbf ディレクトリ) が DC バイナリ・ファイル用に構成されます。このディレクトリのデフォルトの最大サイズは 4GB です。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。1 つのセルに対して最大 10 のディレクトリを作成することができます。

DCBF の場所

デフォルトでは、DCBF は以下のディレクトリにあります。

- Windows の場合 : *<Data_Protector_home>*¥db40¥dcbf
- UNIX の場合 : /var/opt/omni/server/db40/dcbf

Cell Manager のディスク・スペースを考慮して、必要であれば DC ディレクトリを再配置します。DC ディレクトリを複数作成して、これらを別々のディスクに配置することができます。メディア /DC バイナリ・ファイル数がかなりの数 (数千) に増加した場合、またはスペースが不足している場合のみ DC ディレクトリを複数作成してください。詳細は、『*HP OpenView Storage Data Protector 管理者ガイド*』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、バックアップ、コピー、復元、メディア管理の各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。1 つのセッションにつき 1 つのバイナリ・ファイルが作成されます。ファイルは年毎や月毎に分類されます。

SMBF のサイズとサイズの増大

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。セッション・メッセージの容量は、Windows の場合約 200 バイト、UNIX システムの場合約 130 バイトです。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は変更できます。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。詳細は、『*HP OpenView Storage Data Protector 管理者ガイド*』の「表示されるメッセージ数の変更」を参照してください。

SMBF の場所

SMBF は以下のディレクトリにあります。

- Windows の場合 : *<Data_Protector_home>*¥db40¥msg
- UNIX の場合 : /var/opt/omni/server/db40/msg

SessionMessageDir グローバル・オプションを編集してディレクトリの場所を変更することもできます。Data Protector のグローバル・オプション・ファイルの詳細は、『*HP OpenView Storage Data Protector 管理者ガイド*』の「グローバル・オプション・ファイル」を参照してください。

サーバレス統合バイナリ・ファイル (SIBF)

SIBF レコード

サーバレス統合バイナリ・ファイルには、NDMP の加工されていない復元データが保存されます。このデータは NDMP オブジェクトの復元に必要です。

SIBF のサイズとサイズの増大

SIBF のサイズはそれほど大きくなりません。詳細は、206 ページの「IDB サイズの見積もり」を参照してください。NDMP のバックアップでは、SMBF はバックアップされるオブジェクトの数に比例して増大します。バックアップされるオブジェクトごとに約 3KB 使用されます。

SIBF の場所

SIBF は以下のディレクトリにあります。

- Windows の場合 : `<Data_Protector_home>¥db40¥meta`
- UNIX の場合 : `/var/opt/omni/server/db40/meta`

IDB の操作

バックアップ時

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 CDB に保存され、いくつかの属性が与えられます。バックアップ中に Backup Session Manager 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、方針に従ってバックアップに割り当てられます。

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 となります。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セッション・メッセージは、いずれも、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。

トランザクション・ログの作成が可能な場合、IDB バックアップは古いトランザクション・ログを削除して IDB の復旧に必要な新しいトランザクション・ログの作成を開始します。

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・データがある仮想ファイルシステムをブラウズできるようにします。このブラウズのための照会には 2 つの手順が含まれています。最初の手順では、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複数ある場合は、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 に詳細が送信されます。

オブジェクト・コピー時

オブジェクト・コピー・セッションでは、バックアップと復元のセッションと同じ処理が実行されます。復元時と同様にコピー元メディアからデータが読み込まれ、バックアップ時と同様にコピー先メディアにそのデータが書き込まれます。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。詳細は、195 ページの「バックアップ時」および 195 ページの「復元時」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、以下が削除されます。

- 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 日以上経過した不要なセッション (メディアが上書き、またはエクスポートされたセッション) が削除されます (この日数を変更するには、グローバル・オプション・ファイルの `KeepSession` 変数を使用します)。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

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いずれも CDB と MMDB に保持され、これらのメディアから復元を行えます (ただしブラウズはできません)。

ファイル名の削除

ファイルが関連のメディアにバックアップされているかどうかは DC バイナリ・ファイルで知ることができますが、ファイル名は実際には CDB に保存されます。少なくとも 1 つの DC バイナリ・ファイル内でバックアップ済みとしてマークされているファイル名は「使用中」とみなされます。時間が経つと、実際には使用されていないファイル名が増加します。このようなファイル名を削除するために、Data Protector はすべての DC バイナリ・ファイルをスキャンして、使用されていないファイル名を削除します。

ファイル・バージョンの削除

ファイル・バージョンの削除は OmniBack II A.03.50 以前のバージョンでは保守作業の主要な部分を占めていましたが、Data Protector Draft では、自動的に実行される、補助的な日常保守作業になりました。

あるメディアに保存されているすべてのオブジェクト・バージョンのカタログ保護期限が切れた場合、自動的に実行される DC バイナリ・ファイルの日常保守作業により、それぞれのバイナリ・ファイルが削除されます。

IDB 管理の概要

IDB の構成

Data Protector のバックアップ環境の設定手順のうち、最も重要なものに IDB の構成作業があります。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、内部方針を設定できます。

重要　IDB 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。

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。

詳細は、『*HP OpenView Storage Data Protector 管理者ガイド*』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を理解する必要があります。このパラメータ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。

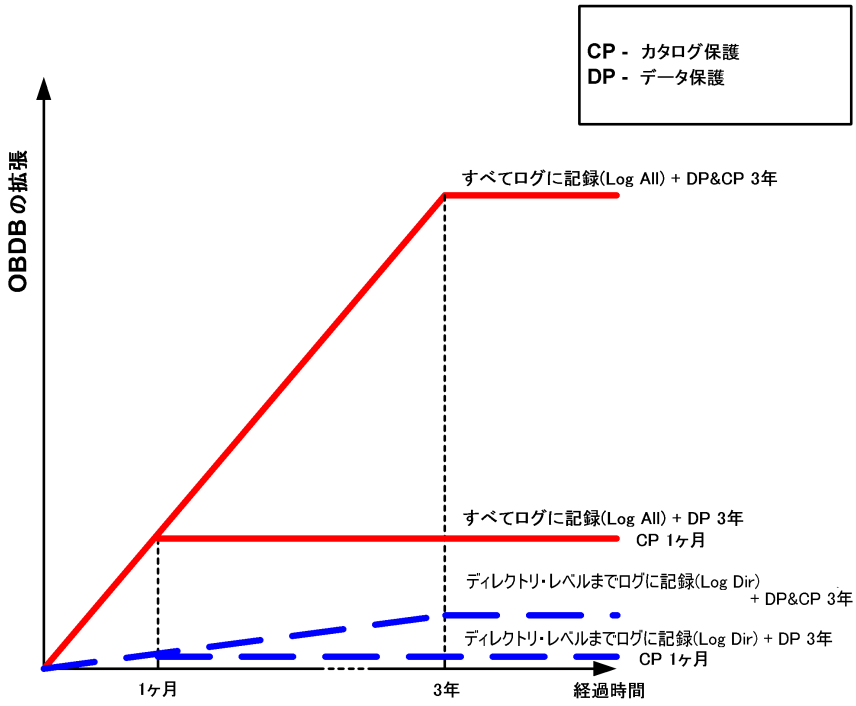
- ロギング・レベルの設定
  バックアップ時に IDB に書き込まれる詳細情報の量は、ロギング・レベルの設定によって決まります。詳細度を高めるようにロギング・レベルを変更すると、IDB への影響が増大します。詳細は、200 ページの「IDB の増大と性能 に関する主要な調整可能パラメータ」を参照してください。
- カタログ保護の設定
  バックアップ・データに関する情報が IDB に保管される期間は、カタログ保護の設定によって決まります。カタログ保護の期間を長くすると、IDB への影響が増大します。詳細は、200 ページの「IDB の増大と性能 に関する主要な調整可能パラメータ」を参照してください。
- バックアップ・ファイル数
  Data Protector では、各ファイル、および各ファイルのそれぞれのバージョンをトラッキングしています。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、65 ページの「フル・バックアップと増分バックアップ」を参照してください。
- バックアップ回数
  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ます。[システム処理能力のレポート (Report on System Dynamics)] でシステム変動に関する情報が取得できます。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、[ディレクトリ・レベルまでログに記録 (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。
- ファイル名に使用されるエンコード方式 (UNIX のみ)
  ファイル名のエンコード方式によって、ファイル名の各文字が IDB 内に占めるサイズは 1 ～ 3 バイトと異なります。例えば、Shift-JIS 形式のファイル名の場合に各文字が IDB 内で最大 3 バイトを占めるのに対し、純粋な ASCII 形式のファイル名の場合は 1 バイトしか必要ありません。このように UNIX 上では、文字のエンコード方式が IDB のファイル名部分の増大に影響を及ぼします。なお Windows 上では、すべての文字が IDB 内で 2 バイトを占めます。
- オブジェクト・コピーおよびオブジェクト・ミラーの数
  作成するオブジェクト・コピーやオブジェクト・ミラーの数が増えると、IDB に保存される情報はそれだけ多くなります。オブジェクト・コピーおよびオブジェクト・ミラーについては、ファイル名情報を除き、バックアップ・オブジェクトの場合と同様の情報が IDB に保存されます。

IDB の増大と性能 に関する主要な調整可能パラメータ

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。ロギング・レベルの設定とカタログ保護の設定によって影響がどのように変動するかを、201 ページの図 5-2 に示します。

図 5-2　　ロギング・レベルとカタログ保護が IDB の増大に与える影響



IDB の主要な調整可能パラメータとしてのロギング・レベル

ロギング・レベルとは

バックアップしたファイルやディレクトリに関する詳細情報がどの程度 IDB に書き込まれるかは、ロギング・レベルによって決まります。ただし、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、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 に記録するかを以下の 4 つのレベルから選択できます。

表 5-1

すべてを記録	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。
ファイルのレベルで記録	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。
ディレクトリのレベルで記録	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、バックアップ速度、および復元データの表示の容易度に影響が生じます。

性能への影響

バックアップ時に IDB に書き込まれるデータの量はロギング・レベルによって決まります。これは IDB の速度やバックアップ・プロセスにも影響を及ぼします。

ロギング・レベルと復元のブラウズ

保存される情報のレベルを変更すると、復元時に Data Protector GUI を使用してブラウズできるファイルも変わります。[ログなし (No Log)] オプションが設定されている場合、ブラウズはできません。[ディレクトリ・レベルまでログに記録 (Log Directories)] オプションが設定されている場合は、ディレクトリをブラウズできます。[ファイル・レベルまでログに記録 (Log Files)] オプションが設定されている場合はすべてをブラウズできますが、ファイル属性 (サイズ、作成日や更新日など) 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

[すべてログに記録 (Log All)]、[ディレクトリ・レベルまでログに記録 (Log Directories)]、[ファイル・レベルまでログに記録 (Log Files)] オプションが設定されている場合、復元速度はほぼ同じです。

[ログなし (No Log)] オプションを設定すると、単一ファイルを復元する場合に処理速度が低下する可能性があります。これは、復元するファイルを見つけるために、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る必要があるためです。

システム全体を対象とした復元の場合、すべてのオブジェクトを必ず読み込むためロギング・レベルの設定はほとんど影響しません。

IDB の主要な調整可能パラメータ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。カタログ保護を設定しなくてもデータは復元できますが、Data Protector GUI でのブラウズができなくなります。

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。

期限切れのカタログ保護

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

カタログ保護の設定は、バックアップの性能には影響を与えません。

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 [ログなし (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。詳細は、201 ページの「IDB の主要な調整可能パラメータとしてのロギング・レベル」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、[ログなし (No Log)] 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 [無期限 (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。例えば、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 [無制限 (Permanent)] 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。例えば、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、複数のシステム (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、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、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非常に困難です。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・サーバには、[ディレクトリ・レベルまでログに記録 (Log Directories)] オプションを使用します。
- データベース・サーバには独自の復元方針があるため、ログは必要ありません。このため、[ログなし (No Log)] オプションを使用します。

- ワークステーションには、異なるバージョンのファイルを検索および復元できるように [すべてログに記録 (Log All)] または [ファイル・レベルまでログに記録 (Log Files)] オプションを使用します。[ディレクトリ・レベルまでログに記録 (Log Directories)] または [ログなし (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方法についての詳細は、『*HP OpenView Storage Data Protector 管理者ガイド*』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、バックアップ方針に応じて、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。

例えば、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 [ログなし (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 [ログなし (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 [すべてログに記録 (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少なく将来もファイル数が増加しない (1,000,000 未満) 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 [すべてログに記録 (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

ファイル数が数千万に増加した場合や毎日万単位でファイルが生成される場合に [すべてログに記録 (Log All)] オプションを使用すると、比較的短期間でバックアップ速度や 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。

- ロギング・レベルを使用可能な一番低いレベルに設定します。[ファイル・レベルまでログに記録 (Log Files)] オプションを使用すると IDB のサイズを 3 分の 1 まで減らすことができ、[ディレクトリ・レベルまでログに記録 (Log Directories)] オプションを使用すると、約 10 分の 1 にまで減らせます。ただし、これ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。

[システム処理能力のレポート (Report on System Dynamics)] を構成して、特定のクライアント上でのファイル名の増大の変動に関する情報を通知することができます。

IDB サイズの見積もり

主にファイルシステム・バックアップを実行する場合、状況によっては IDB のサイズがかなり大きくなる可能性があります (16GB 以上)。ディスク・イメージまたはオンライン・データベースのバックアップを実行する場合は、IDB のサイズが 2GB を超えることはほとんどありません。

IDB のサイズ見積もりに関する推奨方法

IDB のサイズを見積もる際の最も便利で推奨される方法は、Internal Database Capacity Planning Tool を使用することです。このツールは以下のディレクトリにあります。

- UNIX Cell Manager の場合 :
  `/opt/omni/doc/C/IDB_capacity_planning.xls`
- Windows Cell Manager の場合 :
  `<Data_Protector_home>¥docs¥IDB_capacity_planning.xls`

このツールを使うと、オンライン・データベース (Oracle、SAP R/3) を使用する環境内での IDB サイズを見積もることもできます。

IDB のサイズを見積もるその他の方法

IDB がバックアップ開始後 1 年でどれくらいのディスク・スペースを占めるかを、以下の情報を使って見積もることができます。

基本的な式

サイズの計算は、データベースの重要な部分について個別に行います。基本的な式は以下のとおりです。

$$IDB = MMDB + CDB(obj + pos) + CDB(Fnames) + DCBF + SMBF$$

CDB (obj + pos) は、ファイル名を除いた CDB のサイズであることに注意してください。

IDB の各部分についての詳細は、189 ページの「IDB のアーキテクチャ」を参照してください。

モデル

計算をより簡単に分かりやすくするために、バックアップ環境を少し単純化して考えます。バックアップ仕様は 1 つのみで、ファイルシステムのバックアップ用に作成されていると仮定します。

単純化した環境での IDB のサイズを見積もった後、他のバックアップ仕様についても見積もりを行い、その結果を合計します。

IDB サイズ計算用の入力パラメータ

ここで使用している計算式には、バックアップ環境および Data Protector 設定値の 2 種類の入力があります。

バックアップ環境の入力パラメータ

バックアップ環境には以下の入力パラメータがあります。

- *AmountOfData*
  フル・バックアップに含まれるデータの量。この情報を取得するには、バックアップを実行して Data Protector を使って測定します。
- *NoOfFiles*
  フル・バックアップに含まれるファイルおよびディレクトリ数。この情報を取得するには、バックアップを実行後 [システム処理能力のレポート (Reports on sessions in a timeframe)] ->[バックアップ・セッションのリスト (List of Backup Sessions)] でレポートを構成します。
- *NoOfFilesPerDir*
  1 つのディレクトリあたりの平均ファイル数。ほとんどの場合、通常 10 が適当です。5 未満の値は使用しないでください。
- *IncrRatio*
  増分バックアップとフル・バックアップでバックアップされるデータ量 (またはファイル数) の比率。例えば値が 0.05 の場合、平均的な増分バックアップでは 5% のファイルがバックアップされることを意味します。
- *NoOfObjects*
  バックアップ・オブジェクト (マウント・ポイント / ドライブ) 数。

Data Protector の設定と入力パラメータ

計算で使用する Data Protector の設定には、データ保護、カタログ保護、ロギング・レベル、フル・バックアップや増分バックアップのスケジュール、デバイスの同時処理数、セグメント・サイズなどがあります。

これらの設定の中には式で使用するのが困難なものがあるため、以下の補助的な入力パラメータが必要です。

- *NoOfFullsDP*
  データ保護期間中に実行されるフル・バックアップの回数。例えば、週に 1 度フル・バックアップを行いデータ保護が 1 年の場合は、この値は 52 です。保護期間が [無期限 (Permanent)] の場合は、保護期間が 1 年に設定されているものとして計算します。
- *NoOfIncrementalsDP*
  データ保護期間中に実行される増分バックアップの回数。
- *NoOfFullsCP*
  カタログ保護期間中に実行されるフル・バックアップの回数。
- *NoOfIncrementalsCP*
  カタログ保護期間中に実行される増分バックアップの回数。
- *LogLevelFactor*
  ロギング・レベルが [すべてログに記録 (Log All)] または [ファイル・レベルまでログに記録 (Log Files)] の場合、この要素の値は 1 になります。ロギング・レベルが [ディレクトリ・レベルまでログに記録 (Log Directories)] の場合は 1/*FilesPerDir*、[なし (None)] の場合は 0 になります。*FilesPerDir* を正確に見積もるには、ディレクトリあたりに少なくとも 5 つのファイルが必要です。
- *DeviceConcurrency*
  1 つのデバイスに対して同時に書き込みを行える Disk Agent 数。
- *SegmentSize*
  使用中のデータ・セグメント・サイズ。例えば、デフォルトの DLT セグメント・サイズは 2GB です。

MMDB のサイズ

通常 MMDB のサイズは小さく、増大する速度も緩やかです。メディアの数が万単位でない限り、MMDB の大きさは 30MB を超えないと思っていてよいでしょう。

多数のメディアを使用すると、IDB のメモリ消費量が大きくなり、バックアップに失敗する可能性があります。次の計算式を使用すると、HP-UX 上でのメモリ消費量を計算できます。

$$RDSSize = 2048KB + n \times (0.7KB \times m + 1.5KB \times a)$$

n には並列セッション数または RPC スレッド数の最小値 (velocis.ini 内に設定、デフォルト値は 3)、m には選択したプール内のメディア数、a には IDB 内のメディア数をそれぞれ代入します。

平均的なサイズは以下のとおりです。

- *0.7 KB* - IDB 内のメディア・レコードのサイズ (プールごと)
- *1.5 KB* - バイナリ・ファイル内のメディア・レコードのサイズ (全メディア)
- *2048 KB* - RDS の初期サイズ

上の式を使用すると、RDS のメモリ消費量の概算値を見積もることができます。ただし HP-UX 上では、解放されたメモリがシステムに返されないため、ピーク時の RDS メモリ・サイズは反映されていません。大きいサイズの連続したメモリを割り当てる必要があった場合、メモリ管理ではメモリを断片化せずに、通常は大きいかたまりのままメモリを返します。そのため、メモリ内の小さい領域は空いていても使用されないため、メモリ・サイズが増大します。メモリ・サイズが最大許容値 (930MB) に到達したら、再割り当ては失敗します。

次の式は、メモリ使用量が最大許容値の 50%(465MB) になるよう計算する場合の例を示したものです。ここではすべてのメディアが同一プール内にあるものと想定しています。

$$
\begin{aligned}
&465MB = 2048KB + 3 \times (0.7KB \times m + 1.5KB \times a), a = m \\
&465MB = 2048KB + 3 \times (0.7KB \times m + 1.5KB \times m) \\
&465MB = 2048KB + 3 \times 0.7KB \times m + 3 \times 1.5KB \times m \\
&465MB - 2048KB = m \times (3 \times 0.7KB + 3 \times 1.5KB) \\
&465MB - 2048KB = m \times (2.1KB + 4.5KB) \\
&465MB - 2048KB = m \times 6.6KB \\
&m = (465MB - 2048KB)/(6.6KB) \\
&m = 71835media
\end{aligned}
$$

CDB (オブジェクトと位置) のサイズ

式

ファイル名を除くと CDB のサイズは小さく、増大する速度も緩やかです。以下に式を示します。

$$CDB(obj + pos) = BASE + (NoOfMpos \times MPOS) + [NoOfObjVer \times OBJVER]$$

BASE はサイズ定数です。20MB より大きな値は設定できません。

NoOfMpos は、メディア位置レコード数です。メディア位置レコードはメディア上に書かれたデータ・セグメントごとに存在します。

$$NoOfMpos = \frac{NoOfBackupsDP \times AmountOfData}{SegmentSize} \times DeviceConcurrency$$

MPOS と *OBJVER* は、サイズの定数です。*MPOS* は 124 バイトです。*OBJVER* は 384 バイトです。

NoOfObjVer は、バックアップしたオブジェクトとコピーしたオブジェクトのバージョンの数です。これは以下の式で計算します。

$$NoOfObjVer = NoOfObj \times (NoOfFullsDP + NoOfIncrementalsDP)$$

NoOfObj は、バックアップ仕様内のオブジェクトと、そのコピーまたはミラーの合計数です。

NoOfFullsDP は、データ保護期間中に実行されるフル・バックアップの回数です。

NoOfIncrementalsDP は、データ保護期間中に実行される増分バックアップの回数です。

CDB (ファイル名) のサイズ

式

IDB のファイル名数を算出する式は以下のとおりです。

$$CDB(Fnames) = NoOfFiles \times FNAME \times LogLevelFactor \times CumulativeGrowthFactor$$

FNAME は定数で、ファイル名レコードの平均的なサイズを表します。*FNAME* は 75 バイトです。

つまりバックアップとバックアップの間に作成、削除されるファイル数の見積もりが一番困難です。予測は困難ですが、重要な影響を与える要素です。このため、*CumulativeGrowthFactor* を使用して IDB の現在のファイル数と 1 年後のファイル名の数の比率を示します。この値が 1 であれば、1 年間新しいファイルは作成されていないことを意味します。10 の場合は 1 ファイルに対して 9 つのファイルが追加されることを意味します。一般的にこの値は 1.5(ファイルの増加が少ない場合) ～ 4 の間になります。

例

ファイル数が 10,000,000 で、ロギング・レベルが [すべてログに記録 (Log All)](*LogLevelFactor* が 1)、*CumulativeGrowthFactor* が 2、*FNAME* が 75 バイトの場合、ファイル名部分のサイズは約 1 GB になると見積もることができます。

DCBF のサイズ

式

DCBF のサイズを算出する式は以下のとおりです。

$$DCBF = NoOfFiles \times NoOfBackupsCP \times FVER \times LogLevelFactor$$

NoOfBackupsCP はカタログ保護期間中に実行されるバックアップ・セッションの回数で、以下の方法で計算します。

$$NoOfBackupsCP = NoOfFullsCP + (NoOfIncrementalsCP \times IncrRatio)$$

ロギング・レベルが [ファイル・レベルまでログに記録 (Log Files)] の場合、*FVER* は 10 バイト、[すべてログに記録 (Log All)] または [ディレクトリ・レベルまでログに記録 (Log Directories)] の場合は 30 バイトです。

SMBF のサイズ

SMBF のサイズは小さく、増大する速度も緩やかなため、IDB のサイズやサイズの増大に重要な影響を与えません。サイズの見積もりは、バックアップ仕様内の 1 つのバックアップ・オブジェクトと各オブジェクト・ミラー、およびオブジェクト・コピー仕様内の 1 つのオブジェクト・コピーが、それぞれ SMBF で 10 ～ 100KB を占めるものとして計算します。

6　サービス管理

本章の内容

サービス管理、レポート、およびモニタリング機能は、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。本章では、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、HP OpenView 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。

この章の構成は以下のとおりです。

概要

企業の IT (情報技術) 部門では、サービス・レベルの目標値を設定して、その目標値に対する達成率を測定したり、将来的なサービス拡充の必要性を実証したりするために、サービス管理ツール、テクニック、手法等を使用するケースが増えています。

IT 部門ではデータ喪失の危険にも備えなければならないため、データのバックアップと復元は、IT 部門によるサービスの提供と管理に欠かせない非常に重要な要素です。企業のデータは、ユーザー・エラーからウィルスその他の不正なデータ・アクセスやデータ変更に至るまでのさまざまな脅威や、ときに発生する記憶装置自体の故障などの危険に常にさらされています。ビジネスに不可欠なデータを失うと、企業はダウンタイム 1 時間あたりに数千から数百万ドル単位の損失をこうむる恐れがあります。

バックアップの最中には各種のサービスにアクセスできなくなったり、応答速度が低下したりすることがあるため、ユーザーからは不満が生じることもあります。しかしバックアップを行っておかなければ、サービスの可用性や適時性の継続に問題が生じ、重大な危険へと発展する恐れがあります。

ただし、すべてのデータが危険にさらされているとはいえ、すべてのデータに同じレベルの復元性が必要なわけではありません。そのため IT 部門では費用対効果も考慮して、ビジネスに不可欠なデータには重要度の低いデータよりも高レベルの保護を設定するといった手法をとらなければなりません。

サービス管理の測定機能やレポート機能は、IT 部門の管理者が、組織に提供するサービスの価値を証明したり、競争力に優れた原価構造を保持したりするうえで非常に有益なツールです。サービス・プロバイダでは SLA (サービス・レベル・アグリーメント) を使用して、可用性や性能の目標値を大まかに設定し、プロバイダと顧客間の契約上の目標値を文書化します。

SLA への準拠を実証するには、モニタリングを常時行い、目標値に到達しているかどうかを示すレポートを定期的に作成する必要があります。Data Protector にはバックアップや復元操作に関する文書を作成するための、モニタリング、通知、およびレポート用のツールが備わっており、インストール後すぐに使用できます。また他の OpenView サービス管理製品と統合すると、サービス・ビュー、サービス性能データ、およびその他の機能を 1 つのコンソールから統合管理できるようになるため、全体的な IT サービスの提供状態について、より的確で詳細な情報を得ることができます。

Data Protector からは、バックアップ処理およびデータ復元処理を効率よくモニタリングしたり、設計したりするのに役立つ重要なデータが、IT サービス・マネージャとともに提供されます。これらのデータは、サービス・アグリーメントを遂行するうえで欠かせない、サービスの可

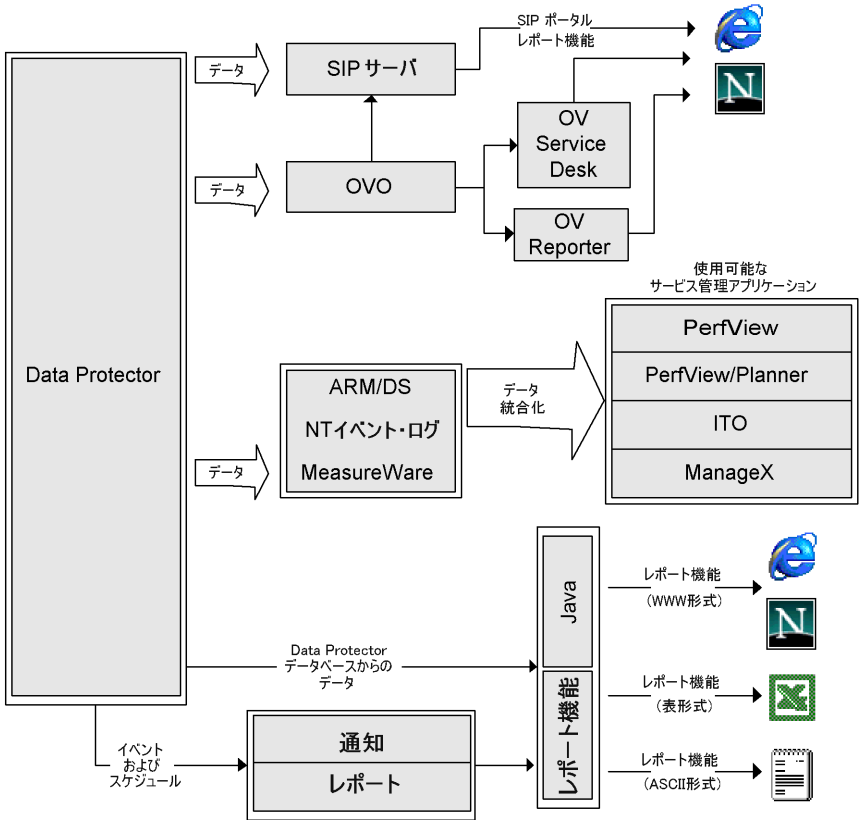
用性や復旧に対する設計作業に役立ちます。さらに Data Protector から提供される情報は、真の IT 財務管理の実現に必要な、コスト管理およびチャージバック・モデルの実装にも使用できます。

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、ManageX、OpenView Performance Agent (以前の MeasureWare Agent)、OpenView Reporter、OpenView Service Desk、および OpenView Service Information Portal などの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 のサービス管理機能は、(インストール後すぐに使用できる) ネイティブな機能と、アプリケーション統合機能という 2 つのカテゴリに分けることができます。各カテゴリの詳細については、本章の後半で詳しく説明します。

図 6-1　　サービス管理における情報の流れ



ネイティブな Data Protector 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

- Data Protector では、Application Response Measurement バージョン 2.0 API (ARM 2.0 API) を使用して、主要な処理にかかった時間を、処理したデータ量とともにトラッキングして、記録することができます。このデータの蓄積には、HP OpenView Performance Agent (OVPA) を使用します。
- 実行中のセッションをモニタリング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報を受け取って、これをさまざまな方法 (電子メール、SNMP、Windows 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 と HP OpenView Operations を統合すると、OVO コンソール上で Data Protector からの警告を受けとって、対応するアクションを自動的に実行させることができます。
- 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。
- HP OpenView ManageX と統合すると、Data Protector の主要かつ重大なイベントを、ManageX オペレータ・コンソールに自動的に転送できます。バックアップ環境で発生した障害に対する処理の自動実行を設定することも可能です。
- Data Protector に組み込まれている Java ベースのオンライン・レポート機能を使用すると、ネットワーク環境内の任意の地点から (遠隔地からでも)、オンライン・レポート機能を実行できます。この場合、使用するローカル・システム上にユーザー・インタフェースがインストールされている必要はなく、Web ブラウザさえあれば、この機能を使用できます。

Application Response Measurement バージョン 2.0 (ARM 2.0 API)

ARM とは

ARM API は、分散環境における終端間のトランザクション応答時間を測定するための、新たに登場した標準化インタフェースです。ARM API を使用するアプリケーション・プログラム (および、特定のトランザクションに関連してユーザーが提供する情報) は、HP OpenView Performance Agent (OVPA) などの、ARM に準拠したシステム管理およびモニタリング・ツールで応答時間を調べるためのソースとなります。OVPA では、後から分析やレポート作成に使用できるように、ARM トランザクション情報をリポジトリ内にログとして蓄積できます。また、バックアップ処理などの特定トランザクションが、事前定義したしきい値を超えても終了しないような場合に、リアルタイムな警告 (または「警報」) を発することも可能です。リアルタイムな警報が発せられた場合には、さまざまなアクションを実行するように、事前設定しておくことができ、例えば HP OpenView Operations などの中央の操作コンソールに情報を送ったり、システム・オペレータのポケットベルを呼び出したり、または問題を解決するための自動アクションを試みたりすることが可能です。

表 6-1 ARM 機能

トランザクションの種類 (ARM 1.0)	ARM に新しく追加されたログ・データ (ARM 2.0)	使用目的
バックアップ仕様セッションに要した時間	処理されたデータ量 (MB 単位)	可用性と復旧の計画。チャージバック
オブジェクト・バックアップ・セッションに要した時間	処理されたデータ量 (MB 単位)	可用性と復旧の計画。チャージバック
復元セッションに要した時間	復旧されたデータ量 (MB 単位)	可用性および復旧に対する計画
IDB のチェックに要した時間	IDB のサイズ (MB 単位)	Data Protector アーキテクチャの管理
IDB の削除に要した時間	削除後の IDB のサイズおよび削除レコード数	Data Protector アーキテクチャの管理

Data Protector には ARM が既に組み込まれているため、ARM API をサポートする OVPA などのアプリケーションと簡単に統合できます。Windows プラットフォームでは、この作業は完全に自動化されています。OVPA がすでに存在するシステム上に Data Protector をインストールするか、またはその逆の場合、トランザクション・データがただちに OVPA および HP OpenView Performance Manager (OVPM) に表示されるようになります。また HP-UX の場合にも、必要となるのは、OVPA ライブラリから Data Protector ディレクトリへのリンクを作成する作業だけです。詳細は、『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。

OVPA と Data Protector 間のインタフェースとして、DSI (Data Source Integration) を使用することも可能です。トランザクションのトラッキングに使用するアプリケーションが ARM 2.0 に準拠していない場合には、この方法が有効です。ARM 1.0 では、バックアップ・セッションの実行に要した時間など、時間に関連するデータしかログに記録できません。DSI を使用すると、コマンド行から取得できる任意のデータについても、OVPA などのツールでレポートを作成できるようになります。そのため、高度にカスタマイズされたレポートの作成が可能です。

HP OpenView Operations との統合

Data Protector OVO 統合ソフトウェアの機能

Data Protector は、HP OpenView Operations (OVO) との統合が可能です。OVO を使用すると、オペレータはある 1 点から、ネットワーク全体やさまざまなアプリケーションをモニタリングおよび管理できるようになるため、大規模なネットワーク環境の管理が容易になります。Data Protector を OVO 環境に統合すると、ネットワーク管理者は、バックアップ中に発生したあらゆる問題点をただちに検出し、表示された情報に対応できるようになります。Data Protector メッセージは、OVO メッセージ・ウィンドウ内に表示できます。

ManageX との統合

Data Protector ManageX 統合ソフトウェアの機能

Data Protector と ManageX との統合は、Windows プラットフォーム上でのみ可能です。この場合、以下のような機能が提供されます。

- Data Protector は、バックアップ、復元、またはその他の処理中に発生したすべての主要かつ重大なメッセージを、Windows のイベント・ログに書き込むため、ManageX でこれらのイベント・ログを使用したり、オペレータが対応できるように ManageX コンソールに転送したりすることが可能です。
- サービス・モニタリング機能

ManageX では、すべての Data Protector サービス、つまり Cell Manager 上で実行されているサービスだけでなく、Data Protector クライアント・システム上で実行されているサービスもモニタリングできます。いずれかのサービスで問題が発生した場合は、ManageX からオペレータにただちに警告が発せられます。また、失敗したサービスの再開を自動的に試みるよう、ManageX を構成することも可能です。

ManageX 3.5 以降ではこれらの方針が既に組み込まれています。それぞれの ManageX 方針を各 Data Protector システムに配布するだけで、これらの統合機能を利用できます。

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 のチェックおよび保守の機構や SNMP トラップの構成に関する詳細は、『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。

モニター

Data Protector モニターは、Data Protector ユーザー・インタフェースの一部であり、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モニタリング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モニタリングすることも可能です。モニターのユーザー・インタフェースからは、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・インタフェースから、複数のセルで実行中のセッションを同時にモニタリングできます。

レポートと通知

Data Protector にはさまざま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 Cell Manager の管理にこれらの機能を使用してきました。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。例えば、保護されていないシステムに関する情報を示す host_not_conf レポートや、スケジューリングされている全バックアップの一覧を示す dl_sched レポート、メディア・インベントリ・レポートである media_list レポートなど。
- 稼働率関連レポート。例えば、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、現在バックアップに使われていない (使用可能な) デバイスの一覧を示す dev_unused レポートなど。
- 問題関連レポート。例えば、失敗したバックアップに関連する情報を示す backup_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)。

- 事前構成された約 30 種のレポートが用意されており、例えば、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 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。

レポートと通知の例

- 毎朝 7:00 に、24 時間以内に実行されたバックアップ・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 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 OpenView 管理アプリケーションで SLA への適合を示すレポート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 OpenView 管理アプリケーションに Data Protector SPI (スマート・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。詳細は 3.1 の例を参照してください。

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。HP OpenView Operations や OpenView Reporter との統合も、SNMP トラップ・ベースの実装の一例です。

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**レポート、通知、イベント・ログ**のユーザー権限を持つ Data Protector ユーザーに限られています。イベント・ログ内のすべてのイベントをブラウズしたり削除できます。

Data Protector ログ・ファイル

HP OpenView Operations などのサービス管理アプリケーションの中には、特定のログ・エントリに関していつ、どのログ・ファイルをモニターするか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。OVO ではこれを *ログ・ファイルのカプセル化*と呼びます。

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・ファイルの詳細は、『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。ログ・ファイルに関する書式化の仕様は用意されていないことに注意してください。

Windows アプリケーション・ログ

ManageX などサービス管理アプリケーションの中には、Windows のアプリケーション・ログをモニターできるものがあります。

すべての Data Protector メッセージや Data Protector サービス (停止している場合) に関するメッセージを Windows アプリケーション・ログに自動転送するには、Data Protector グローバル・オプション・ファイルの `EventLogMessages` 変数を `1` に設定します。Data Protector グローバル・オプション・ファイルの詳細は、『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。

Java ベースのオンライン・レポート

Data Protector が提供する Java ベースのオンライン・レポート機能を使用すると、Data Protector のすべての組み込みレポートの構成、実行、および印刷作業をその場で対話形式に実行できます。レポート処理が開始されると、Data Protector Java レポート機能は Cell Manager に直接アクセスして、最新のデータを取得します。この Java アプレットは Web サーバを介して使用するか、直接アクセスできるようにクライアント・マシンにコピーするか、またはローカル・マシン上で使用してください。

この機能は、サポートされている Web ブラウザさえあれば使用できるため、使用するシステム上に Data Protector GUI がインストールされていなくても構いません。

Java レポート機能を使用すると、レポートにオンライン・アクセスできるだけでなく、新しいレポートをスケジュールに追加したり、レポートのパラメータを変更したりするなど、レポート体系に対する構成作業も可能になります。

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 のセルフチェックおよび保守機能では、次のような処理が可能です。

- 「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

提供される機能の一覧は、『*HP OpenView Storage Data Protector 管理者ガイド*』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 セル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、モニタリング、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、単一の Cell Manager の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 の詳細は、『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。

Data Protector が提供するデータの使用

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。

データの用途

- 指定した時間枠を超えても処理が終了しないバックアップ・セッションまたは復元セッションに対するリアルタイムな警告が可能です (OVPA を使用)。
- 環境内の主要なシステムのバックアップ処理にかかった時間をグラフ化して、処理時間の傾向を分析できます (OVPM を使用)。
- IDB サイズの増大を予想することにより、データベース・サイズが限界値に達する時期を推測できます (OVPM Planner を使用)。
- バックアップ・オペレータ、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、HP OpenView Network Node Manager などのネットワーク管理ソフトウェアに送信できます (Data Protector 組み込み通知エンジンの SNMP トラップ送信機能を使用)。

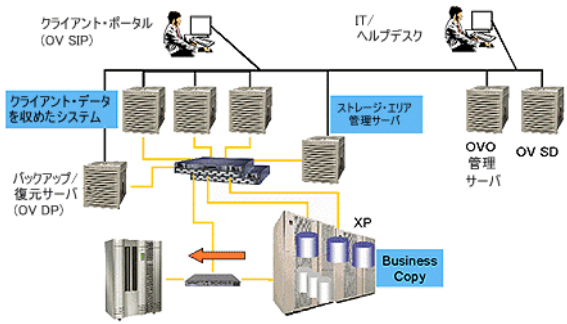
サービス管理の統合

以下の Data Protector 統合ソフトウェアをインストールすると、サービス管理機能がさらに向上し、さまざまなサービス管理機能を一元的に操作できるようになります。

主要な機能

- 標準および独自のレポート形式の使用
- Data Protector 用の「トラブル・チケット」インタフェースの使用
- 明確で整合性のある適切なサービス・レベルの促進
- Web インタフェースを介した Data Protector 情報の使用
- データのグラフィカルな表示

図 6-2　クライアント・ポータルを介してサービス管理にアクセスする IT サービス・プロバイダ環境の例



Data Protector-OVO-OVR の統合

Data Protector と HP OpenView Operations (OVO) との統合環境に、HP OpenView Reporter 3.0 (英語版) を追加すると、機能をさらに拡張できます。Reporter を追加すると、サービス・プロバイダは中央管理ポイントとしての OVO コンソールから、レポートを生成できるようになります。Reporter と統合すると、以下の分野について、さまざまな新しい種類のレポートを作成できます。

- バックアップ・セッション・レポート

- 管理レポート
- メディア・プール・レポート
- 性能

IT サービス・プロバイダは、これらのレポート機能を使用して、SLA への適合を顧客に実証できます。例えば、「Data Protector Transaction Performance」レポートには、IT の SLA パラメータの 1 つであるサービス性能メトリクスが示されます。

図 6-3 Data Protector-OVR の統合例

hp OpenView | data protector

hp OpenView data protector Transaction Performance

This report was prepared: 3/26/02, 10:51:16 AM
This report shows transaction time for backup session, restore session, backup of a specific object, internal database purge and internal database check during the report interval of **3/19/02 10:00:00AM to 3/25/02 10:00:00PM**.

This report shows the systems where each Application Response Measurement (ARM) transaction has been executed
Completed = the number of transactions completed successfully.
Aborted = the number of transactions that have been aborted instead of completed.
Response = the average time (seconds) to complete a successful transaction.

HP OpenView Data Protector Management System: ovdmux17.cup.hp.com

Backup of Specific Object Transcations

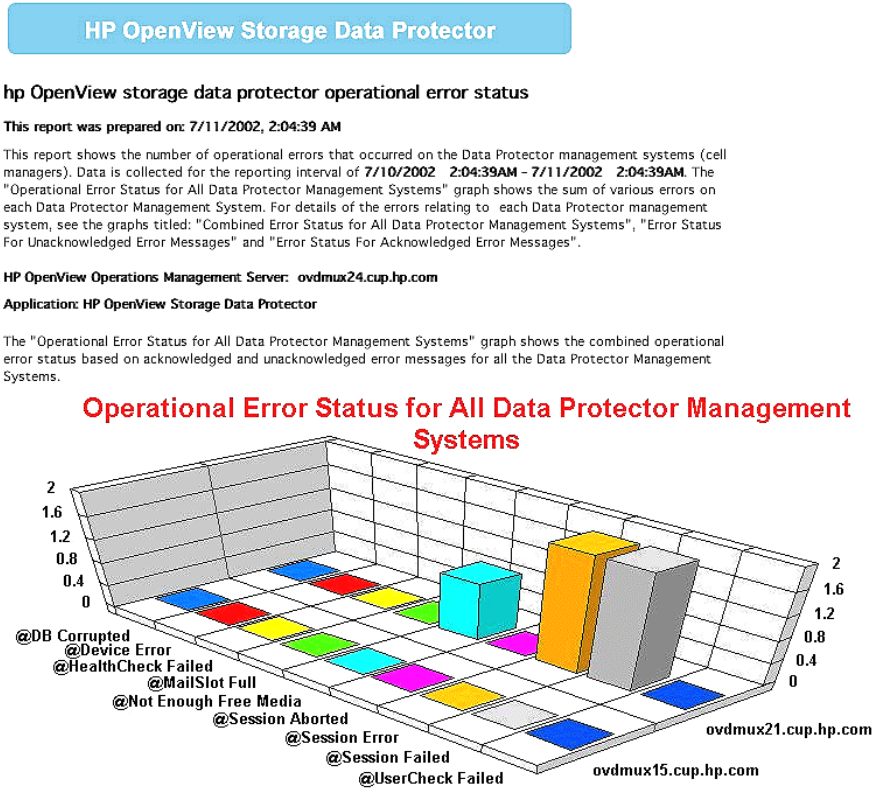
Object Name	Completed	Aborted	Response
02 ovdmux17.cup.hp.com:/ // /	3	0	159.66
02 ovdmux17.cup.hp.com:/opt // /opt	30	0	44.46
02 ovdmux17.cup.hp.com:/usr // /usr	1	0	100.97
02 ovdmux17.cup.hp.com:/var // /var	19	0	42.51
03 ovdmux17.cup.hp.com:/ // [Database]: ovdmux17.cup.hp.c	10	0	10.46
	63	0	44.86

Backup Session Transcations

Backup Specification	Completed	Aborted	Response
	21	0	146.55
back1	1	0	
backHigh	1	0	
backLow	1	0	
backTop	1	0	
ClearCase NT Server	1	0	1,340.95
DP Cell Manager	7	0	216.55
Sysback-ii	6	0	628.83
SystemBackup	5	0	33.08
	44	0	6

さらに SLA への適合を示すレポートに加えて、IT サービス・プロバイダでは Data Protector 環境の処理に関する月次レポートも作成できます。例えば、「Data Protector Operational Error Status」レポートは、「問題のある」データを集計したもので、IT サービス・プロバイダにおける処理計画の策定に役立ちます。

図 6-4　Operational Error Status レポート

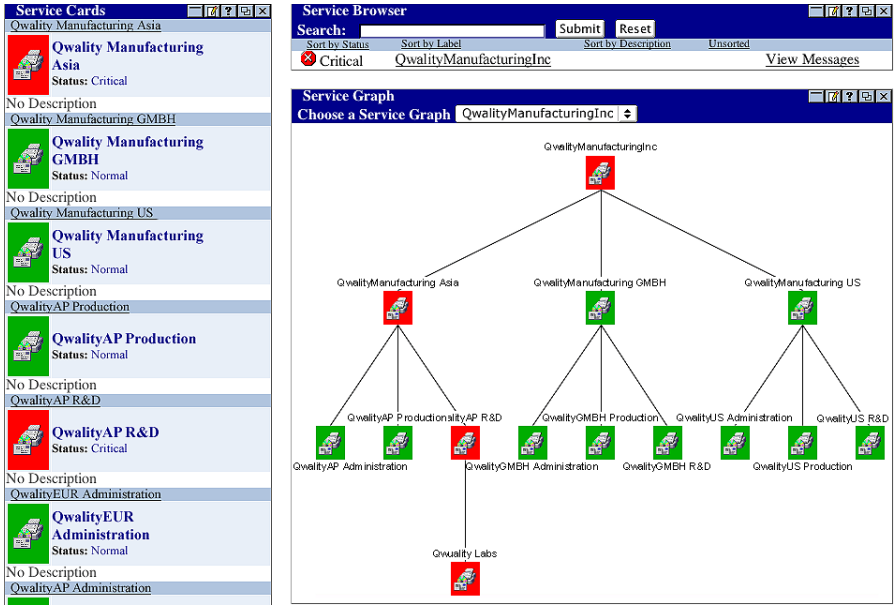


Data Protector-OVO-SIP の統合

SIP を使用すると、提供しているサービスの内容をわかりやすく表示できます。SIP では、サービス・プロバイダの全般的なインフラストラクチャのビューを示すのではなく、各顧客に関する情報を抽出し、その顧客環境に関するステータスやビジネス情報を表示することができます。

SIP と統合すると、外部委託されたデータ保護処理の状況を各顧客に示すことができます。この統合では、ストレージ・ネットワークをグラフィカルに表示するために、OVO コンポーネントが使われます。

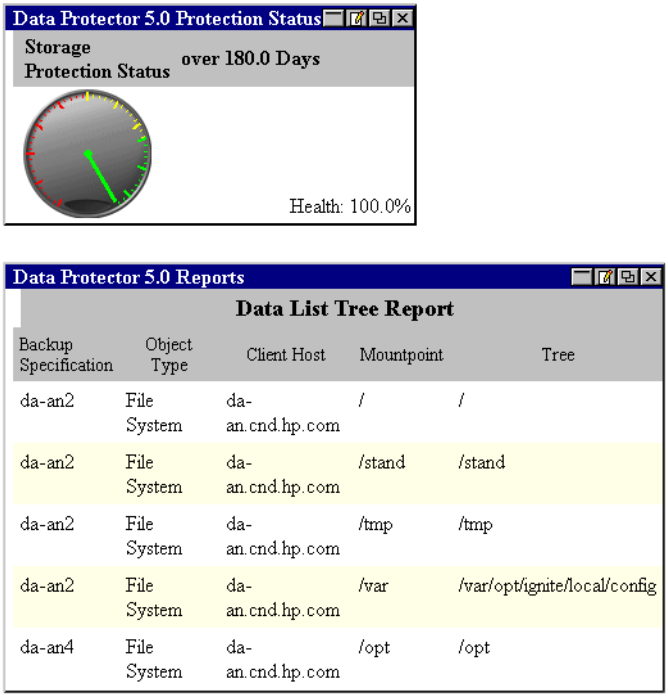
図 6-5　Data Protector-OVO-SIP の統合例



Data Protector-SIP の統合

この統合では SIP を使用して、Data Protector 情報を Web ベースのインタフェースを介して提供することもできます。OVO がインストールされている必要はありません。情報は表およびゲージの形で提供されます。

図 6-6　　Direct SIP の統合例



Data Protector と HP OpenView Service Desk の統合

Service Desk はヘルプ・デスク用のソリューションです。IT サポート部門は Service Desk を統合することにより、構成、ヘルプ・デスク、緊急事態への対処、問題の解決、変更管理プロセスなどを、一連のワークフローとして運用できるようになります。Service Desk は、IT トラブルシューティング・プロセスの自動化や標準化に役立ちます。また Service Desk は SLA の内容を記憶し、サポート・サービスがそれに準拠しているかどうかをモニタリングすることができます。

Data Protector と統合することにより、Service Desk は、メディアの追加や失敗したバックアップの再開といったバックアップに関連する問題の解決に要した時間を (オペレータの介入なしに) モニタリングできるため、Data Protector のモニタリング機能や測定機能をさらに強化できます。

Service Desk はサービス・ヘルプ・デスクのワークフローを管理し、サービスの品質レベルを測定し、SLA への適合を実証するレポートを生成できます。Data Protector A.05.50 と Service Desk を統合することにより、サポート・スタッフは Data Protector データにアクセスしてタイムリーな応答を行い、重要なデータ保護サービスに影響が及ぶ前に操作上の問題を解決できるようになります。

7 Data Protector が機能する仕組み

本章の内容

本章では、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。

この章の構成は以下のとおりです。

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。

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。
CRS	CRS (Cell Request Server) プロセス (サービス) は、Data Protector の 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開されます。
MMD	MMD (Media Management Daemon) プロセス (サービス) は、Data Protector の 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。
RDS	RDS (Raima Database Server) プロセス (サービス) は、Data Protector の Cell Manager 上で実行され、IDB の管理を担当しています。このプロセスは Data Protector を Cell Manager 上にインストールした時点で開始されます。

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、『*HP OpenView Storage Data Protector 管理者ガイド*』またはオンライン・ヘルプを参照してください。

バックアップ・セッション

本項では、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。

バックアップ・セッションとは

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

スケジュール形式のバックアップ・セッションは、指定された時間になると、Data Protector スケジューラにより自動的に開始されます。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

対話形式のバックアップ・セッションは、Data Protector ユーザー・インタフェースを使ってオペレータが直接開始します。この場合は Data Protector モニターがただちに開始されて、バックアップ・セッションの進捗状況をモニタリングできます。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。モニタリングをやめるには、ユーザー・インタフェースをセッションから切り離します。セッション自体は、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、238 ページの図 7-1 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 (ダイレクト・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。

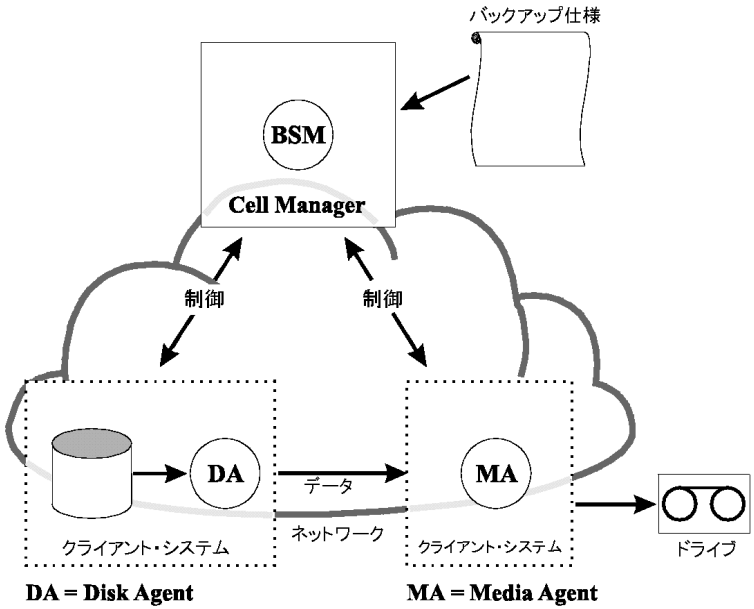
バックアップ・セッションが開始されると、以下の処理が実行されます。

1. BSM (Backup Session Manager) 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接続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。

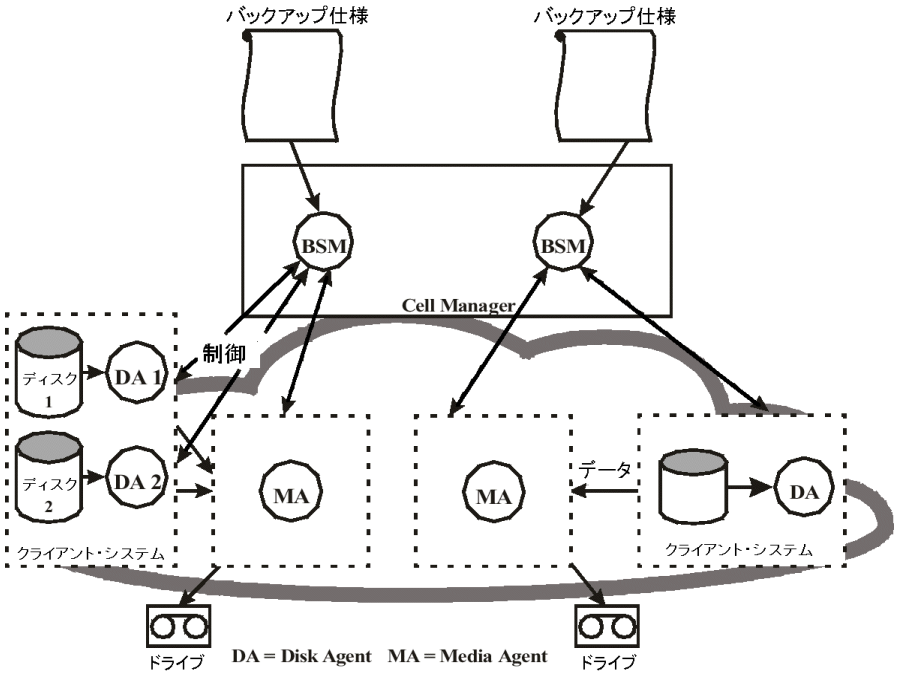
図 7-1　　バックアップ・セッションにおける情報の流れ (1)



同時に実行できるセッションの数

図 7-2 に示すように、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、Cell Manager の構成や、プロセッサの速度、メイン・メモリの容量、ディスク・スペースなど、セル内のリソースによって制限されます。同時実行できるバックアップ・セッションの最大数は変更可能です。

図 7-2　バックアップ・セッションにおける情報の流れ－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。また、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・オペレータなどが自分で記述する必要があります。

バックアップ・セッションにおける待ち行列の使用

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。セッションは、必要最小限のリソースが使用できるようになるまで、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、セッションは中止されます。タイムアウトまでの時間は、グローバル・オプション SmWaitForDevice を使って設定できます。

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、グローバル・オプション・ファイルを編集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リングされた場合には、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

マウント要求とは

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方針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。

詳細は、142 ページの「バックアップ・セッション中にデータをメディアに追加」と 141 ページの「バックアップ用メディアの選択」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に電子メールで送信することができます。オペレータ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、221 ページの「レポートと通知」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・ディスカバリとは

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かなければなりません。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。

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

オブジェクト・コピー・セッションとは、バックアップ・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・セッションでは、選択したバックアップ・オブジェクトがオリジナルのメディアからコピー先メディアにコピーされます。

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、バックアップの終了直後に開始することも可能です。スケジュール方式のオブジェクト・コピー・セッションは、Data Protector スケジューラで指定した時刻に開始されます。一方、バックアップ後のオブジェクト・コピー・セッションは、指定したバックアップ・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

対話形式のバックアップ・セッションは、Data Protector ユーザー・インタフェースを使ってオペレータが直接開始します。この場合は Data Protector モニターがただちに開始されて、バックアップ・セッションの進行状況をモニタリングできます。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。モニタリングをやめるには、ユーザー・インタフェースをセッションから切り離します。セッション自体は、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・セッション中の処理内容

オブジェクト・コピー・セッションにおける情報の流れは、244 ページの図 7-3 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 (Copy Session Manager) 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 が Media Agent をロックします。すべての読み取り用 Media Agent と、必要最小限の書き込み用 Media Agent のロックが完了するまで、セッションは待ち行列に入れられます。タイムアウトまでの時間はバックアップの場合と同じです。タイムアウトになってもリソースをまだ使用できない場合、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。バックアップ方針に従って各 Media Agent に、コピー元メディアとコピー先メディアがそれぞれ割り振られます。
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ければ、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します。

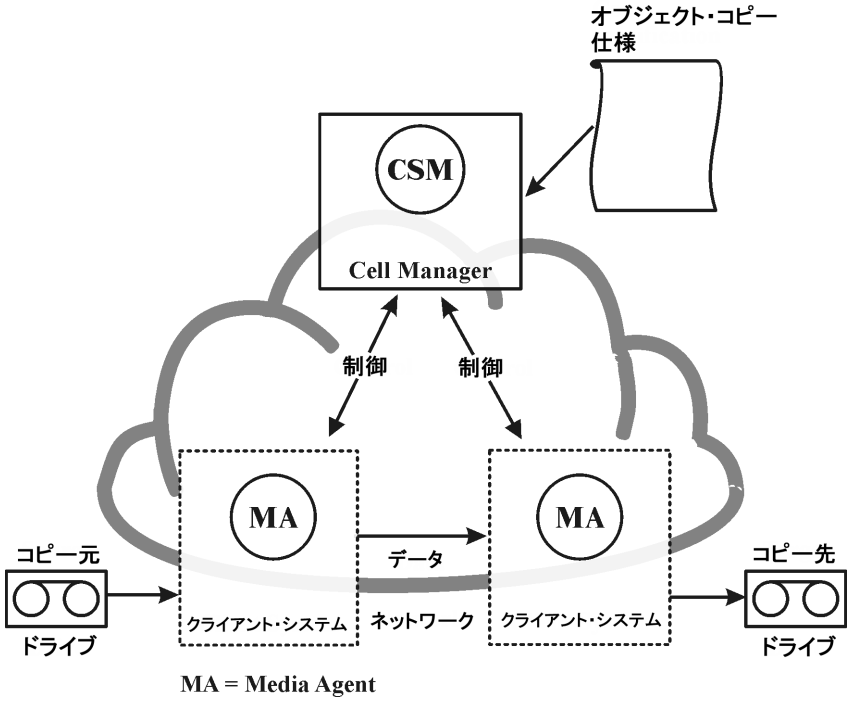
   - コピー元デバイスとブロック・サイズが同じデバイスは、ブロック・サイズが異なるデバイスよりも優先的に、コピー先デバイスとして選択されます。
   - ローカルに接続されているデバイスは、ネットワークに接続されているデバイスよりも優先的に選択されます。
6. コピー先メディアを担当する Media Agent が、コピー元メディアを担当する Media Agent からの接続を受け入れ、コピー先メディアへのオブジェクト・コピーの書き込みを開始します。

   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. 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。

図 7-3　　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の使用

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。セッションは、必要最小限のリソースが使用できるようになるまで、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、セッションは中止されます。タイムアウトまでの時間は、グローバル・オプション SmWaitForDevice を使って設定できます。

オブジェクト・コピー・セッションにおけるマウント要求

マウント要求とは

オブジェクト・コピー・セッション中に、オブジェクト・コピーに必要なコピー元またはコピー先のメディアが使用不能であると、マウント要求が発行されます。

マウント要求への対応

マウント要求に応答するには、要求されたメディアをセットしてから、処理を続行するよう指示します。要求されたコピー元メディアのコピーが存在する場合は、オリジナルのメディアの代わりにコピーを使用することも可能です。

復元セッション

以下では、復元セッションの開始方法、復元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。

復元セッションとは

復元セッションでは、(通常はテープ・メディア上の) バックアップ・コピーからディスク上に、データがコピーされます。

復元セッションは、対話形式で開始します。オペレータは、復元する対象を Data Protector に伝えて必要なメディアを選択させ、必要なオプションを指定して、復元処理を開始します。オペレータおよび他のユーザーはセッションの進捗状況をモニタリングできます。

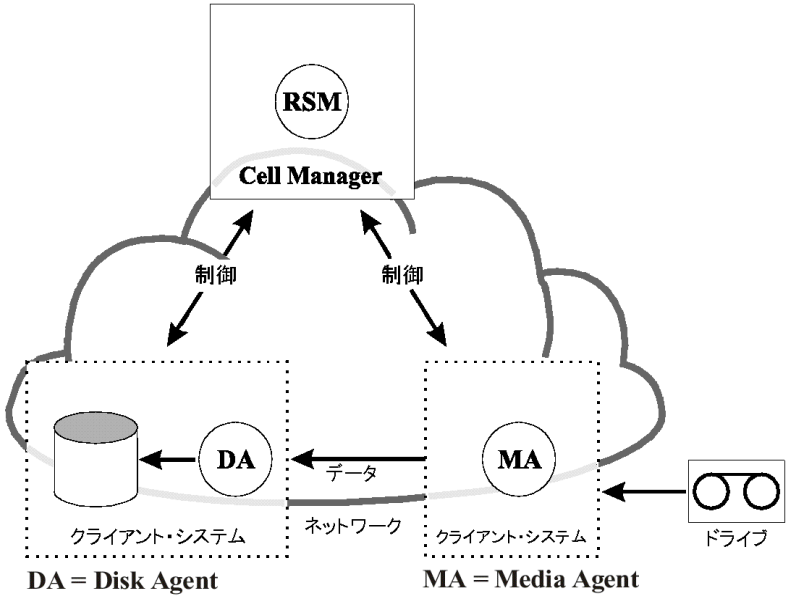
復元セッションにおけるデータ・フローとプロセス

復元セッション中の処理内容

図 7-4 に示すように、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. RSM (Restore Session Manager) 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、復元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、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、復元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、復元に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。ドライブが並列に使用される場合には、ドライブごとに個々の Media Agent が開始されます。
4. RSM により、並行して復元されるディスクごとに、個々の Disk Agent (DA) が開始されます。実際に開始される Disk Agent の数は、復元対象に選択したオブジェクトの数に基づいて決められます。詳細は、248 ページの「並行復元」を参照してください。
5. メディア上のデータが、Media Agent により読み取られて Disk Agent に送信されて、ディスク上に書き込まれます。RSM は、セッションの進捗状況をモニタリングしており、必要に応じて新しい Disk Agent および Media Agent を開始します。
6. 復元セッションが終了したら、RSM によりセッションが閉じられます。

図 7-4　　復元セッションにおける情報の流れ



同時に実行できる復元セッションの数

セル内では同時に複数の復元セッションを実行できます。いくつのセッションを実行できるかは、Cell Manager や、システムとそのシステムに接続されているデバイスなど、セル内のリソースによって制限されます。

復元セッションの待ち行列

タイムアウト

復元セッションが開始されると、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みられます。いずれかのリソースが使用できない場合には、セッションは待ち行列に入れられます。待ち行列に入れられたセッションについては、一定時間が経過するまでリソースの再割り当てが試みられます。この時間がタイムアウトです。タイムアウトまでの時間はユーザーが変更できます。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

マウント要求とは

復元セッション中に、復元に必要なメディアがデバイス内で見つからない場合には、Data Protector からマウント要求が発行されます。Data Protector では、マウント要求が発行された場合の動作を、あらかじめ設定しておくことも可能です。

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、復元処理を続行するよう Data Protector に指示します。

並行復元

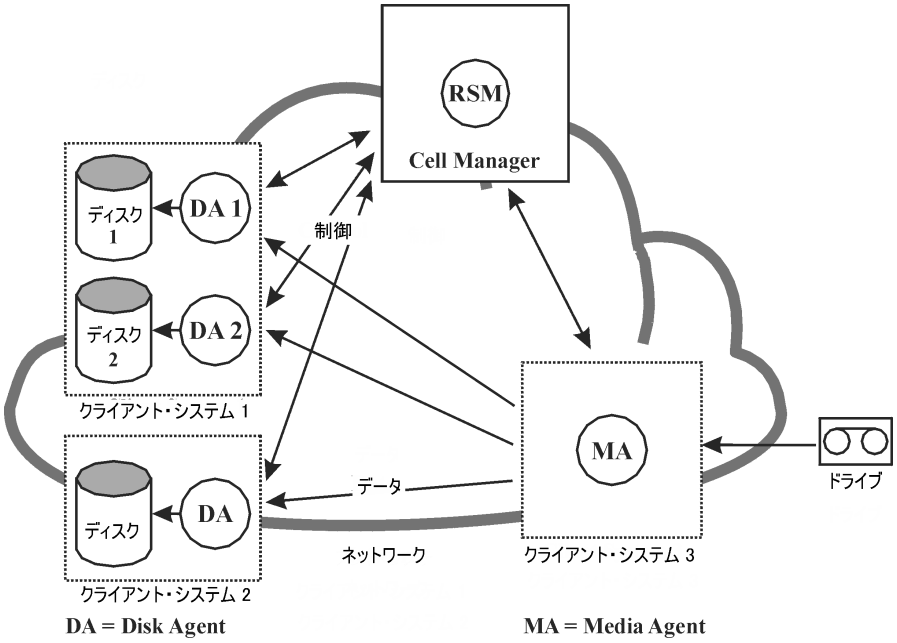
並行復元とは

並行復元を実行すると、複数のオブジェクトから送られたデータがメディアから同時に読み取られ、まとめて復元されます。同一メディアから複数のオブジェクトを復元できる場合には、並行復元を実行することで、復元処理の性能を大きく向上できます。詳細は、図 7-5 を参照してください。

標準的な復元処理との違い

多くの場合、メディア上には、複数の Disk Agent から送られたデータが多重化された形で格納されています。詳細は、143 ページの「1 つのメディア上に複数セッションの複数オブジェクトを格納 （並列書き込み）」を参照してください。標準的な復元処理では、多重化されたデータがメディアから読み取られ、選択されたオブジェクトに該当する部分のみが集められて使用されることになります。この場合、次のオブジェクトを復元するには、いったんメディアを巻き戻してから、そのオブジェクトに該当する部分をあらためて読み取っていかなければなりません (両方のオブジェクトが、同一メディア上に多重化された形で書き込まれている場合)。

図 7-5　並行復元セッションにおける情報の流れ



並行復元処理の場合は、多重化されたデータの中から、復元対象に指定されている個々のオブジェクトに該当する部分がすべて読み取られ、各データが対応する Disk Agent に送られていきます。そのため、メディアからデータを読み取るときの性能が向上します。選択したオブジェクトを物理的に分かれているディスク上に復元する場合には、性能はさらに向上します。この場合は、複数のディスク上にデータが同時にコピーされます。

複数の単一ファイルの高速復元

Data Protector では、オブジェクトを不連続に復元することにより復元の性能を向上させます。ファイルまたはツリーの間に少なくとも 1 つのセグメントがある場合、Data Protector は特定のファイルまたはツリーを復元した後、メディア上の復元対象となる次のファイルまたはツリーに直接移動して復元を続行します。

1 つの復元オブジェクト内で複数の Disk Agent を起動できるので、Data Protector がメディアをスキャンするよりもはるかに高速でメディア内に存在する複数の単一ファイルを復元できます。

メディア管理セッション

メディア管理セッションとは

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 内に格納されます。

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中の処理内容

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. MSM (Media Session Manager) 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、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・インタフェースに送られます。このとき、セッションも IDB 内に格納されます。
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。

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。

8　データベース・アプリケーションとの統合

本章の内容

本章では Data Protector と、Microsoft Exchange Server、Oracle Server、IBM DB2 UDB、Informix OnLine Server などのデータベース・アプリケーションとの統合について簡単に説明します。

この章の構成は以下のとおりです。

サポートされている統合機能の一覧については、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』を参照してください。

データベース操作の概要

ユーザーの観点からすると、**データベース**とは、情報を一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**内に格納されています。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与えられています。データはテーブル内の各行に格納されます。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 (マネージャ) ・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 Online では **db スペース**、Sybase では**セグメント**と呼ばれています。

図 8-1　　リレーショナル・データベース

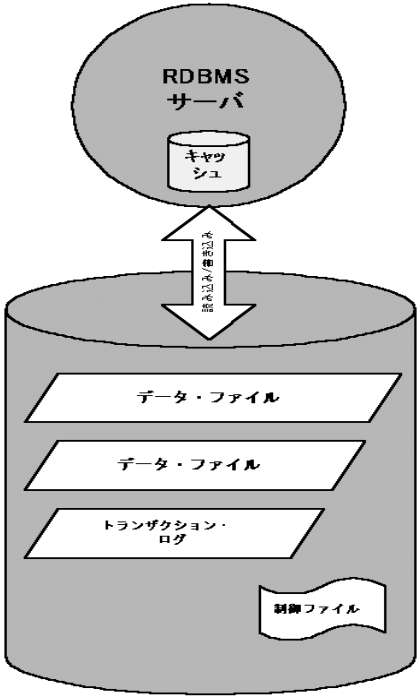


図 8-1 は典型的なリレーショナル・データベースと、その内部にある以下の構造を示したものです。

データ・ファイルは、データベース内のすべてのデータが格納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、例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。これらの制御データが保存された制御ファイルは、データベースの操作に欠かせません。

データベース・サーバ・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格納されます。

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。例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 つのプログラムをそれぞれ用意します。
- データベースに所属するすべてのデータ・ファイルを含めたファイルシステム・**バックアップ仕様**を構成します。次に、**実行前コマンド**としてデータベース停止プログラムを、**実行後コマンド**としてデータベース開始プログラムを指定します。

この方法は理解するのも構成するのも比較的容易ですが、*バックアップ中はデータベースにアクセスできない*という大きな問題点があります。これはほとんどのビジネス環境で容認できない重大な欠点です。

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フェースを用意しています。これらのインタフェースを使うと、バックアップ中または復元中もサーバ・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フェースを使って、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。サポートされる統合機能の詳細は、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』を参照してください。

バックアップ・インタフェースの主要目的は、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。

図 8-2　　Data Protector とデータベースの統合

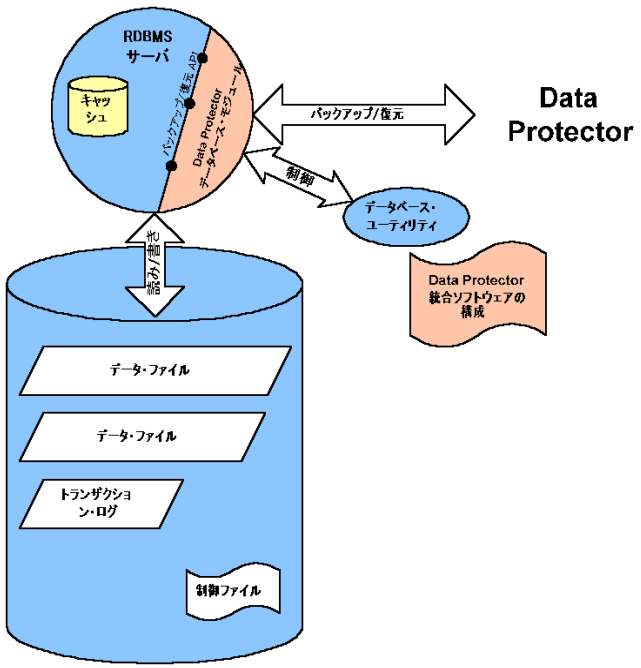


図 8-2 は、リレーショナル・データベースと Data Protector の統合方法を示したものです。Data Protector からは、データベース・サーバにリンクされる**データベース・ライブラリ**が提供されます。データベース・サーバは Data Protector に対してデータを送信したり、データを要求したりします。データベース・ユーティリティは、バックアップ処理や復元処理の開始に使用されます。

以下に、Data Protector の統合機能を使っ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・インタフェースを使って、バックアップ仕様を準備します。

データベースと Data Protector 統合ソフトウェアを使うと、データベースを常に**オンライン**状態に保てるだけでなく、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がなく、データ・ファイルを同一のディスク上に置く必要もありません。
- 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だけ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。

9 ダイレクト・バックアップ

本章の内容

この章ではダイレクト・バックアップの概念と、ダイレクト・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 でサポートされるダイレクト・バックアップ構成についても紹介しています。

この章の構成は以下のとおりです。

概要

バックアップ・ソリューションに対するストレージ業界からの要求は年々厳しさを増しており、アプリケーションのダウンタイムとシステム負荷を可能な限り抑えながら、バックアップ処理を高速化することが求められています。またデータ量も増え続けており、過去 20 年間にわたって 1.5 年ごとに 2 倍の分量になり、さらに増加の速度を増しています。

またアプリケーションやサービスは、ほぼ終日にわたりオンライン状態を保ち、最大の性能を発揮することが求められています。そのためバックアップが可能な時間帯は限られています。またバックアップ処理等に伴う性能の低下が許されなくなってきています。

これらに加えて、相当な出費を伴う専用の装置を必要としないバックアップ・ソリューションへの要求も高まっています。

こうした各方面からの要求に応えて新たに開発されたのが、ダイレクト (「サーバレス」) バックアップ技術です。

ミッション・クリティカルな Oracle 環境を管理する企業やサービス・プロバイダにとって、Data Protector のダイレクト・バックアップ機能は、HP のネットワーク・バックアップ・ソリューション・ファミリーに、他の処理への影響が少ないサーバレス・バックアップ機能を追加する優れた機能拡張となります。

ダイレクト・バックアップでは、ディスクからテープにデータを直接移動することにより、HP のゼロ・ダウンタイム・バックアップ (ZDB) ソリューションのメリットを高めることができ、またバックアップ・サーバの負荷を大幅に軽減できるため、場合によってはバックアップ・サーバをなくすことも可能です。

また、他の処理に影響を及ぼすソフトウェアベースのスナップショットではなく、ハードウェアベースのミラー化技術を採用しているため、実稼動データベース・サーバに対する影響も最小限に抑えられています。

さらにダイレクト・バックアップ・ソリューションは、HP StorageWorks テープ・ライブラリ (および外付けの Fiber Channel SCSI ブリッジ) に組み込まれている業界標準の XCopy (ANSI T10 SCP-2 拡張コピー仕様) コマンドと完全に統合されているため、専用の「データ・ムーバ」装置を用意する必要もありません。

注記 HP OpenView Storage Data Protector A.05.50 のダイレクト・バックアップでサポートされるアプリケーション、オペレーティング・システム、およびデバイスの詳細は、269 ページの「サポートされる構成」を参照してください。

ダイレクト・バックアップ

ダイレクト・バックアップとは、どのような処理を意味するのでしょうか。このバックアップ・ソリューションは「サーバレス」で実行されます。つまり、データを移動するための専用のバックアップ・サーバは必要なく、またデータが LAN を介して転送されることもありません。バックアップされるデータは、クライアント・システムからテープ・デバイスに*直接*送信され、バックアップ・サーバを経由しません。

ダイレクト・バックアップでは、アプリケーション・データ・ファイルと制御ファイル、およびディスク・イメージ (raw ディスク・ボリュームまたは raw 論理ボリュームのいずれも可能) をバックアップすることができます。

ダイレクト・バックアップでは、既存のスプリット・ミラーおよび SAN (Storage Area Network) 技術を使用して、以下の処理が実行されます。

- アプリケーションにできる限り影響を与えずに、アプリケーション・データにアクセスします。アプリケーションを実行しているサーバは最小限しか使用されず、アプリケーションのダウンタイムは、ほとんどまたは全くありません。
- ネットワーク・トラフィックや LAN 速度に起因するボトルネックに影響されることなくデータを移動できます。

ダイレクト / サーバレス・バックアップをサポートするために、Data Protector では対象のファイルシステムを解析し、SAN を介してデータを送信するための新たな技術も採用しています。XCopy 標準をベースにしたこの新しい技術により、サーバを介することなく対象のシステムからテープ・デバイスにデータを送信することが可能になります。XCopy の概要については、265 ページの「XCopy について」を参照してください。

このディスクからテープへの (SAN を経由した) 直接的なデータ・パスにより、設備投資を減らすとともに、既存設備の使用率を高めることができます。

バックアップの種類

ダイレクト・バックアップでは、アプリケーション・データ・ファイルと制御ファイル、およびディスク・イメージ (raw ディスク・ボリュームまたは raw 論理ボリュームのいずれも可能) をバックアップすることができます。

ダイレクト・バックアップの利点

データ・ムーバは SAN ブリッジ内に存在し、対象システムを解釈するための技術は汎用 Media Agent に組み込まれているため、ダイレクト・バックアップを使用する場合は、廉価な管理サーバを使用してバックアップを実施でき、またブロック識別を実行するための複数のサーバを購入する必要もありません。

さらに、ダイレクト・バックアップはハードウェア機能を活用して稼動時間を増大し、また復元時間を短縮するためのインスタント・リカバリにも対応できるように設計されています。

ダイレクト・バックアップの対象は、特定のファイルシステムや論理ボリューム・マネージャ (LVM) に限定されません。

ダイレクト・バックアップは、さまざまな面でバックアップ・ソリューションの機能を拡張します。例えばダイレクト・バックアップを使用すると、次のことが可能になります。

- 最新の XCopy 機能を活用してバックアップにかかる時間を短縮できます。
- 既存のハードウェア・ミラー化機能およびスナップショット機能を活用して、稼動時間を最大化できます。
- Data Protector の業界をリードする優れたインスタント・リカバリ機能を使用して、復旧にかかる時間を短縮できます。
- XCopy ホスト・デバイスは、CPU リソースおよびメモリ・リソースをほとんど必要としません。

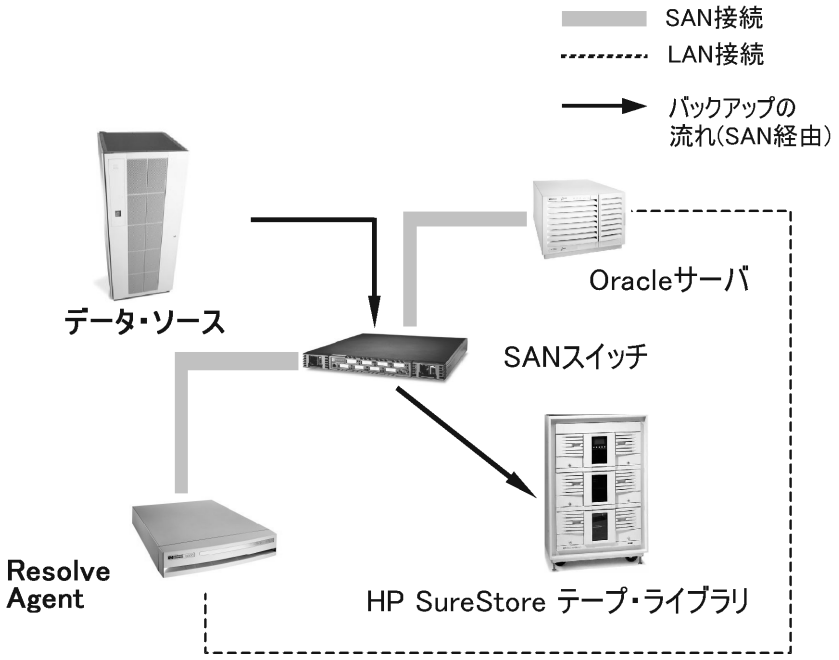
ダイレクト・バックアップの仕組み

Data Protector のその他のバックアップ方法と同様に、バックアップをいつどのように実行するかは、バックアップ仕様を作成して制御します。

- アプリケーションを実行しているサーバ上の汎用 Media Agent によりアプリケーションを休止します。
- アプリケーションを実行しているサーバおよびバックアップ・ホスト上のスプリット・ミラー・エージェントにより、ミラーを分割します。
- バックアップ・ホスト上の汎用 Media Agent により、以下の処理を実行します。
  - 対象システム上のディスクを解析します。
  - 解析した情報を計算します。
  - XCopy を呼び出します。
- XCopy はこれに応じて対象データを取得し、ブリッジを介してこのデータをテープ・デバイスに送信します。

図 9-1 は、基本的なダイレクト・バックアップ構成を示したものです。この構成では、独立したバックアップ・ホスト上に Resolve Agent が存在しています。ただし、データはこのホストを経由して転送されるわけではありません。

図 9-1　　ダイレクト・バックアップのアーキテクチャ



環境

この項ではダイレクト・バックアップ環境に関して、接続する必要があるデバイスと、それらのデバイスをどこに接続すればよいかについて説明します。また必要なエージェントと、そのインストール先についても説明します。

サポートされるプラットフォーム、テープ・ドライブ、およびライブラリの詳細は、269 ページの「サポートされる構成」を参照してください。

ダイレクト・バックアップを実行する場合、アプリケーションを実行しているサーバ以外の場所に汎用 Media Agent を配置することが求められます。また、アプリケーションを実行しているサーバまたはその他のホスト上に Resolve Media Agent が存在し、XCopy エンジンにアクセスできなければなりません。Resolve Agent の配置については、269 ページの「サポートされる構成」を参照してください。

ダイレクト・バックアップの要件は以下のとおりです。

- ディスク・アレイ、XCopy エンジン、アプリケーションを実行しているサーバ、およびテープ・ドライブまたはライブラリが SAN に接続されていること。
- Resolveホストおよびアプリケーションを実行しているサーバがLANに接続されていること。
- HP StorageWorks Disk Array XP (XP) が BC (Business Copy) として、ミラーとともに構成されていること。また、そのミラーに十分なディスク・スペースが割り当てられていること。
- XCopy エンジン、および Data Protector General Media Agent を実行しているホストの両方から、コピー元デバイス (ディスク) とコピー先デバイス (テープ) にアクセスできるように、SAN が適切に構成されていること。つまり LUN マスキングと SAN ゾーニングが、次のように構成されていなければなりません。
  - General Media Agent ホストから XCopy エンジンにアクセスできること。
  - General Media Agent ホストからコピー先のテープ・ドライブまたはライブラリにアクセスできること。
  - SureStoreE Agent (SSEA) ホストからコピー元ディスクにアクセスできること。
  - XCopy エンジンからコピー元ディスクにアクセスできること。
  - XCopy エンジンからテープ・ドライブまたはライブラリにアクセスできること。

Resolve プログラムについて

Resolve プログラムとは、さまざまな種類のファイルシステム固有のディスク・レイアウトを理解するための、Data Protector 独自のコンポーネントです。Data Protector のダイレクト・バックアップでは、Resolve を使用することにより、さまざまなオペレーティング・システム上で書き込まれたデータを、各オペレーティング・システムが実行されているサーバをそれぞれ用意することなしにバックアップできます。

Resolve はディスク上の raw 情報を確認し、ディスク上のファイルシステムを解釈するのに適した方法を選択します。なお、Resolve はデータ自体を読むのではなく、ディスク上の配置に関する情報のみを読み取る点に注意してください。その後 Resolve は、XCopy エンジンに直接入力するのに適した情報を返します。

XCopy について

XCopy は NCITS (National Committee for Information Technology) 標準に準拠しており、別のコンピュータ / サーバを介すことなく、2 台のデバイスが相互に通信することを可能にします。

XCopy では一連の SCSI コマンドが指定されます。このコマンドが XCopy エンジンに渡されることにより、あるデバイスから別のデバイスにデータを転送することが可能になります。その際、データの転送にコンピュータやサーバを必要としません。データは、XCopy を介して、コピー元デバイス (ブロックまたはストリーム、つまりディスクまたはテープ) からコピー先デバイス (ブロックまたはストリーム) に送られます。

XCopy はストリーム (テープ) デバイスがセットアップされ、データの読み書きが可能な状態になっていることを前提としています。つまりドライブがオンライン状態になっており、ドライブ内にテープがセットされ、読み書きの開始位置にテープが位置付けられている必要があります。XCopy 機能を使用することにより、制御サーバは、コピー元デバイスのデータをメモリ内に読み込んでコピー先デバイスにその情報を書き込む作業から解放されます。XCopy 機能を使用する場合、サーバ側では、XCopy コマンドを XCopy エンジンに渡し、その結果が返ってくるのを待つだけで済みます。

XCopy と Resolve

Resolve が登場する以前は、XCopy から返される情報を受け取るには、その情報と一致するファイルシステムを持つサーバが必要でした。また適合するサーバが存在する場合であっても、情報が返される前にオペレーティング・システムにより実際の物理セクタがそのオペレーティング・システムの論理ビューに変換されている可能性があるため、この情報を利用するのは困難でした。Resolve の登場により、複数のファイルシステムをサポートするための複数のサーバを用意する必要がなくなり、またファイルシステム固有の情報フォーマットにより生じる問題点も解消されました。

ダイレクト・バックアップ処理の流れ

ダイレクト・バックアップ処理の流れは以下のとおりです。ここに示すのはダイレクト・バックアップの開始から終了までの基本手順です。

- バックアップ仕様を読み取ります。
- バックアップ対象を決定します。
- アプリケーションを休止します。
- ミラーを分割します。
- アプリケーションを再開します。
- ブロックを解析します。
- データを移動します (XCopy エンジン)。
- ミラーを再接続して再同期化します。

データ・ファイルのバックアップ段階

バックアップ対象のオリジナル・データ・ファイルは、後から復元処理に使用できる形に最終的にコピーされるまでに、複数の段階を経てバックアップされます。通常、ダイレクト・バックアップ処理は以下の手順で実行されます。

1. データ・ファイルの整合性を確保します (アプリケーションを休止します)。
2. メタデータ (ファイル属性) を読み取り、ファイルをオブジェクトにグループ化します。
3. データファイルの安定性を確保します (特定の時点におけるデータの安定性を確保するために、スプリット・ミラー技術を使用します)。
4. データ・ファイルを一連のディスク・ブロックに対応付けます (Resolve 技術を使用)。
5. ディスク・ブロックをテープに移動します (XCopy 技術を使用)。

通常、各段階は 1 つの Data Protector エージェントで管理されます。エージェントは BSM (Backup Session Manager) により生成されます。エージェントで内部的に処理できないエラーはすべて BSM を介してユーザーに通知され、内部データベースに記録されます。また、BMA (Backup Media Agent) により、カタログ・セグメントと、データ・セグメントとカタログ・セグメント間の区切り (ファイル・マーク) が書き込まれます。

復元

ダイレクト・バックアップで保存したデータは、以下のいずれかの方法で復元できます。

- HP StorageWorks XP ディスク・アレイを使用しており、インスタント・リカバリ機能を実行できる場合は、この機能を使ってデータを復元できます。インスタント・リカバリの詳細は、『*HP OpenView Storage Data Protector ゼロ ダウンタイム バックアップ 管理者ガイド*』を参照してください。
- ダイレクト・バックアップを使用して保存した情報の復元には、通常の Data Protector ネットワーク復元機能も使用できます。

いずれの場合も、アプリケーションを実行しているサーバがこの復元の際に発生する負荷に対応できることを確認しておいてください。バックアップ中はデータがサーバを経由しないため、バックアップ時にはこの点を考慮する必要はありません。一方、復元時にはデータ処理がサーバに影響を及ぼします。

要件とサポート

この項では、ダイレクト・バックアップを適切に実行するための要件と、ダイレクト・バックアップでサポートされるファイルシステムおよびアプリケーションについて説明します。

- Data Protector Cell Manager (サポート対象のいずれかのオペレーティング・システム上で実行されていること)
- HP-UX 11.11 上で実行されている Resolve Agent
- HP-UX 11.11 上で実行されているアプリケーションのサポート
- HP-UX 11.11 上の HP LVM のサポート
- XCopy ホスト、コピー元ディスク、コピー先デバイス、および XCopy エンジンが同一の SAN ゾーン内に存在すること
- ファイルシステムのサポート :
  - Veritas の VxFS 3.1、3.3
- アプリケーションのサポート :
  - Oracle 9.i
- Raw ボリュームのサポート
- アプリケーションの動作環境として ServiceGuard をサポート
- 標準的な Data Protector 復元インタフェースを介した復元
- XP 用のインスタント・リカバリ機能のサポート
- ブリッジ内の XCopy エンジン

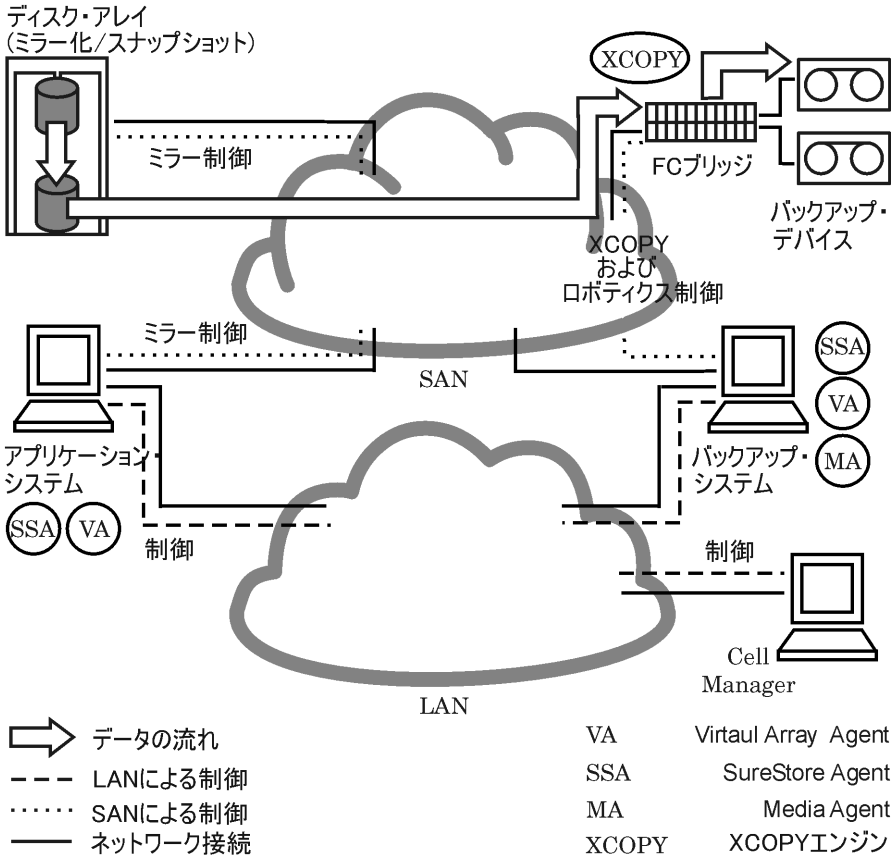
サポートされる構成

3 台のホスト : CM、アプリケーション、Resolve

このソリューションでは 3 台のホストを使用します。Cell Manager、Resolve Agent、およびアプリケーション用に各 1 台ずつです。この構成は 3 台のマシンを必要としますが、Resolve ホストは低価格なホストで十分であり、このようにマシンを分けることでリソース負荷を分散し、アプリケーションの性能に影響が及ぶのを回避できます。

この構成の Cell Manager ホストでは、Data Protector でサポートされているどのオペレーティング・システムが実行されていてもかまいません。アプリケーション・ホストと Resolve Agent ホストでは、HP-UX 11.11 が実行されていなければなりません。

図 9-2　3 台のホストによる基本的な構成



2 台のホスト : Cell Manager/Resolve Agent とアプリケーション

このソリューションでは 2 台のホストを使用します。1 台は Cell Manager と Resolve Agent 用、もう 1 台はアプリケーション用です。この構成では 2 台のマシンが必要ですが、このようにマシンを分けることでリソース負荷を分散し、アプリケーションの性能に影響が及ぶのを回避できます。さらに、Cell Manager と Resolve Agent を実行するマシンについては、最低限の処理能力しか必要ありません。

この構成では、両方のホスト上で HP-UX 11.11 が実行されていなければならない点に注意してください。

基本的な構成 : 1 台のホスト

このソリューションでは 1 台のホストのみを使用し、そのホスト上に Cell Manager、アプリケーション、および Resolve Agent をすべてインストールします。この場合は 3 つのコンポーネントがすべて同一の物理マシン上で実行されるため、これらのコンポーネント間でリソース (I/O チャネル、CPU、メモリなど) が共有されます。この構成では、最小限の設備を揃えるだけでダイレクト・バックアップを実行できます。ただしリソースが共有されるため、Cell Manager や汎用 Media Agent の実行により、アプリケーション・データベースの性能に影響が生じる可能性があります (XCopy 処理による負荷はごくわずかで無視できるレベルです)。

この構成では、ホスト上で HP-UX 11.11 が実行されていなければならない点に注意してください。

10 ディスク・バックアップ

本章の内容

この章では、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。

この章の構成は以下のとおりです。

概要

業界では、データのバックアップと復元をさらに高速化するための方法が求められています。また、日常の企業アプリケーションの実行が妨げられないように、データのバックアップと復元に必要な時間を最小限まで減らすことが、ますます重要となってきています。

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。

ディスクベースの記憶メディアは、近年ますます低価格化が進んでいます。またそれと同時に、ディスクの大容量化も進行しています。そのため、低コストで高性能なシングル・ディスクおよびディスク・アレイによるデータの保存が、実現可能になってきました。

ディスク・バックアップ (ディスクツーディスク バックアップ) は、次第にその役割を大きくしています。従来は、コストと効率の両面で障害復旧要件を満たす最適な記憶装置として、バックアップや復元には一般にテープ記憶装置が使われてきました。近年、従来のテープ記憶装置によるバックアップ・ソリューションに加えて、より高速なディスクベースのバックアップ・ソリューションを採用する企業が増え始めています。この手法を導入すると、より高速なデータのバックアップや復元が可能になります。

ディスク・バックアップの利点

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、実際には特定ディレクトリ内の特定ファイルです。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れば、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。

- 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。例えば、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 がサポートする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。ファイル・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。

スロット数 X 2TB

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。ファイル・ライブラリ・デバイスの機能の詳細は、『*HP OpenView Storage Data Protector 管理者ガイド*』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。

構成

ディスク・デバイスのプロパティは、デバイスの初期セットアップ時だけでなく、その後のデバイス使用中にも変更できます。プロパティをどの程度まで変更できるかは、個々のデバイスによって異なります。

ディスク・デバイスへのバックアップ

ディスクベース・デバイスにバックアップするには、Data Protector の通常のバックアップ仕様を作成します。

11 スプリット・ミラーの概念

本章の内容

この章では、スプリット・ミラー・バックアップの概念と、当社がサポートしている構成について説明します。

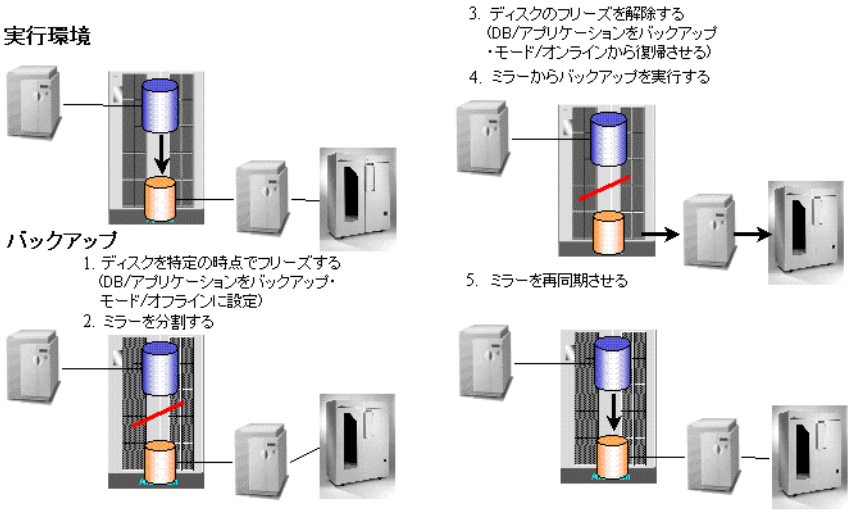
この章の構成は以下のとおりです。

概要

記憶装置の構成が高可用性を持つにつれて、バックアップ概念に新たな要求が発生してきました。高可用性構成では、単一または複数のミラー構造がさまざまな組み合わせで使用されています。

通常、このような構成では、1 つの**複製**(ミラー・コピー) を使用してバックアップ処理を行う一方で、アプリケーションの実行には**ソース ボリューム**を引き続き使用する、といった方法が採られます。詳細については、図 11-1 を参照してください。

図 11-1　　スプリット・ミラー・バックアップの概念



通常、複製処理における**ターゲット・ボリューム**は個々のクライアントに接続し、このクライアントにはローカル・バックアップ用のテープ・デバイスを接続します。一般的に HP StorageWorks Disk Array XP や EMC Symmetrix などのハードウェア・ミラー技術を使って複製を作成します。たとえば、次のようなソフトウェアを使用します。

- HP StorageWorks ContinuousAccess XP
- HP StorageWorks BusinessCopy XP

アプリケーションの可用性は、ディスク上のデータの整合性をとるために必要な数秒から数分間の時間を除くと、ほぼ永久に保持されます。この時間にディスクの整合性がとられ、実際のミラー分割も行われます。データは、復元後にアプリケーションが使用できるように整合性を保つ必要があります。通常は、バックアップ時に複製は作成されませんが、この時点ではすでに作成

されており、アプリケーションの可用性を実現するために同期がとられています。バックアップおよび複製の再同期処理は、別のハードウェア上で並行して行われるため、アプリケーションの性能に影響が及ぶことはありません。

ほとんどの場合、アプリケーション・クライアントとバックアップ・クライアントは別であるため、バックアップ・ミラーを分割する前にクライアント上のすべてのキャッシュ情報 (データベース・キャッシュ、ファイルシステム・キャッシュ) を一括してディスクに書き込むことが重要です。これを行うには、以下のオプションのいずれかを使用します。

- データベースをバックアップ・モードにする。
- データベースをオフラインにする。
- マウント・ポイントをアンマウントする。

複製の整合性を保つためには、これらを分割*前に*行う必要があります。ただし、データベースがファイルシステムまたは raw ディスク上で実行されている場合は、データの書き込み先がファイルシステムのキャッシュではなくディスクであることをデータベースが確認するため、ファイルシステムまたは raw ディスクをアンマウントする必要はありません。

オンライン・データベース・バックアップについては、複製を単独で復元することはできません。アプリケーション・クライアントからのアーカイブ・ログ・ファイルも必要となります。アーカイブ・ログのバックアップは分割の直後に開始できます。このときデータベースはバックアップ・モードから復帰します。

1 つの複製を、HP StorageWorks Contiunous Aceess XP の技術と組み合わせて使用してバックアップを行う場合、バックアップ中の記憶装置の高可用性が失われます。ミラーを追加すると記憶装置の高可用性が保たれ、同じバックアップ方法を使用できます。

バックアップ・クライアント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・クライアントの中心的なバックアップ・クライアントとして使用することができます。この場合、バックアップ・クライアントをアプリケーション・クライアントと同じオペレーティング・システム上で実行する必要があります。これにより、各オペレーティング・システム固有の方法でミラー化されたリソースにアクセスできます。

バックアップ・クライアントによるバックアップの時間は適度な長さでなければなりません。論理的にはバックアップの実行に 24 時間近く要する可能性がありますが、復元に要する時間も考慮する必要があるため、バックアップ・クライアントによるバックアップ時間は、2 ～ 4 時間とすることをお勧めします。また、復元はアプリケーション・クライアントを通じて行うことをお勧めします。

このアプローチでは、バックアップ・クライアントを通して大量のデータ転送や、複製へのアクセスが頻繁に行われます。バックアップ・クライアントとアプリケーション・クライアント間の LAN 接続はバックアップにかかわる調整にのみ使用されます。各クライアント上では、分割の自動化を実現するためのプロセスが実行されています。

インスタント・リカバリ

Data Protector のインスタント・リカバリでは、スプリット・ミラー技術を活用して、データを即時に復元できるようにしています。このソリューションは、スプリット・ミラー技術を採用している HP StorageWorks Disk Array XP 用統合ソフトウェアと同様に、ゼロ・ダウンタイム・バックアップ (ZDB) のソリューションをベースにしています。

スプリット・ミラー・バックアップ・セッション中は、バックアップ・メディア (テープ) へのデータの移動には、元のデータの複製が使用されます。バックアップ完了後、複製を破棄して、次回のバックアップ・セッションに備えてディスク・ペアを再同期により作成することができます。または、インスタント・リカバリに備えて、複製をそのまま残すこともできます。つまり、複数の複製を同時に作成できます。例えば、HP StorageWorks Disk Array XP では、同時に最大 3 個の複製を保持でき、(カスケード接続を行った場合) それぞれの複製が他の 2 個のコピーを所有できます。

インスタント・リカバリ時には、指定された複製 (インスタント・リカバリに備えてそのまま残しておいたもの) のデータと、アプリケーション・クライアントのソース ボリュームとの同期がとられ、バックアップ・メディアからの復元は行われません。

Data Protector では、最初の 3 個の複製しか使用しません。これは、セカンダリ・ミラーは再同期を高速で実行できないため、復元時間を最小化するうえで致命的となるためです。インスタント・リカバリを実行できるのは、HP StorageWorks BusinessCopy XP 構成 (ローカル・ミラー (デュアル・ホスト) とローカル・ミラー (シングル・ホスト) の 2 通りの構成) を使用する場合だけです。

テープへの ZDB とディスク + テープへの ZDB

テープへの ZDB バックアップおよびディスク + テープへの ZDB バックアップのセッション中は、アプリケーション・データの複製が、別のバックアップ・システムに接続したテープ・デバイスへ連続的に流されます。この処理には Data Protector の Disk Agent と汎用 Media Agent が使用され、アプリケーション・システムへの影響は最小限に抑えられます。バックアップの終了後、複製は以下のいずれかの処理がなされます。

- 廃棄 - テープへの ZDB の場合
- 保持 (インスタント・リカバリに使用可能) - ディスク + テープへの ZDB の場合

ディスクへの ZDB

ディスクへの ZDB バックアップ・セッション中は、複製からバックアップ・メディア (テープ) への移動に、オリジナルのデータは使用されません。最大 3 個の複製は、オフライン・データ処理やインスタント・リカバリなどのさまざまな目的に使用できます。ただしインスタント・リカ

バリは、HP StorageWorks BusinessCopy XP 構成が使用されている場合のみ実行可能です。ディスクへの ZDB セッションで作成したオブジェクトを復元するには、インスタント・リカバリ機能を使用する必要があります。

複製セットのローテーション

複製は同時に複数存在できます。HP StorageWorks Disk Array XP では、同時に最大 3 個の複製を保持でき、(カスケード接続を行った場合) それぞれの複製が 2 個の追加コピーを所有できます。ただし Data Protector では、バックアップおよびインスタント・リカバリの目的に、最初の 3 個の複製 (**ファースト・レベル・ミラー**または **MU**) のディスクしか使用できません。追加の 6 個のコピー (カスケード接続ミラー) はサポートされていません。

ファースト・レベル・ミラーで構成したソース ボリューム (LDEV) に対して ZDB バックアップ仕様を構成する場合、またはそのようなソース ボリュームに復元する場合、Data Protector を使って**複製セット**を定義することができ、その複製セットから現在のセッションに対して複製が 1 つ選択されます。

バックアップ・クライアントとクラスタ

バックアップ・クライアントは、アプリケーション・クライアント用のフェイルオーバー・サーバとしては使用しないでください。アプリケーション・サービスとバックアップ・サービスは、別々のクラスタ上に置くことをお勧めします。

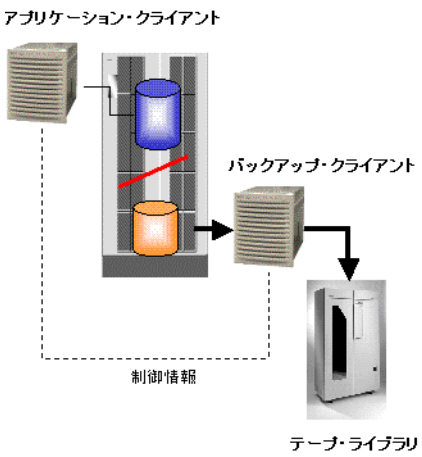
サポートされる構成

ローカル・ミラー (デュアル・ホスト)

このソリューションでは、Business Copy XP などのローカル・ミラー機能を使用します。2 つのディスクが同じディスク・アレイ上に存在します。つまり、RAID システムの I/O インフラストラクチャをアプリケーション・クライアント (またはホスト) とバックアップ・クライアント間で共有しています。

アプリケーション・クライアントとバックアップ・クライアントは物理的には個別のシステムであるため、それぞれ各自の処理 (相互干渉しないバックアップ) には独自のリソース (I/O チャンネル、CPU、メモリなど) を使用できます。このため、バックアップ性能はデータベース性能に影響を与えません。

図 11-2　ローカル・ミラー (デュアル・ホスト、最高性能時でダウンタイムがゼロのバックアップ)



利点

- OracleやSAPに対して真のオンライン・バックアップを実行できる
- バックアップ中にアプリケーション/データベースの性能に影響を与えない
- 業務上重要なアプリケーションの動作可能時間を最大にする
- オンライン・バックアップから迅速に復旧できる
  - バックアップ・モードの時間が短いため、生成されるアーカイブ・ログの量が少ない
- 完全統合ソリューションの自動化
  - Oracle RMANとの統合
  - SAP brbackupとの統合

Data Protector のスプリット・ミラー・バックアップの統合により、ミラー状態の自動処理やアプリケーション (SAP R/3、Oracle など) との密接な統合が可能になり、データの整合性およびアプリケーション / データベース対応バックアップが確実に実行されます。アプリケーション / データベースがバックアップが行われていることを認識している場合に限り、安全な操作が保証されます。この場合、アプリケーション固有のツール (sapdba など) を使用して復元が行えま

す。バックアップがアプリケーションに与える影響は、ミラーの分割に必要な時間と、分割可能な整合性のあるモードにデータベースを切り替えて元のモードに戻すための時間との合計にまで削減されます。

この構成によって非常に大規模なデータベースのオフライン・バックアップを短時間で実行でき、また少しのアーカイブ・ログ・ファイルしか作成しないオンライン・バックアップも行えます。これはデータベースのバックアップ・モード時間を最小限に抑えることができるためです。

アーカイブ・ログの数が少なければ、データベースの復旧プロセスを高速化できるだけでなく、アーカイブ・ログ全体に必要な容量を抑えることができます。オンライン・データベースを復元したら、データベースを整合性のある状態に戻す必要があります。バックアップ中に生成されたすべてのアーカイブ・ログを適用することが必要です。スプリット・ミラー・バックアップでは、分割時に作成されたアーカイブ・ログ・ファイルだけが適用されます。

ローカル・ミラー (シングル・ホスト)

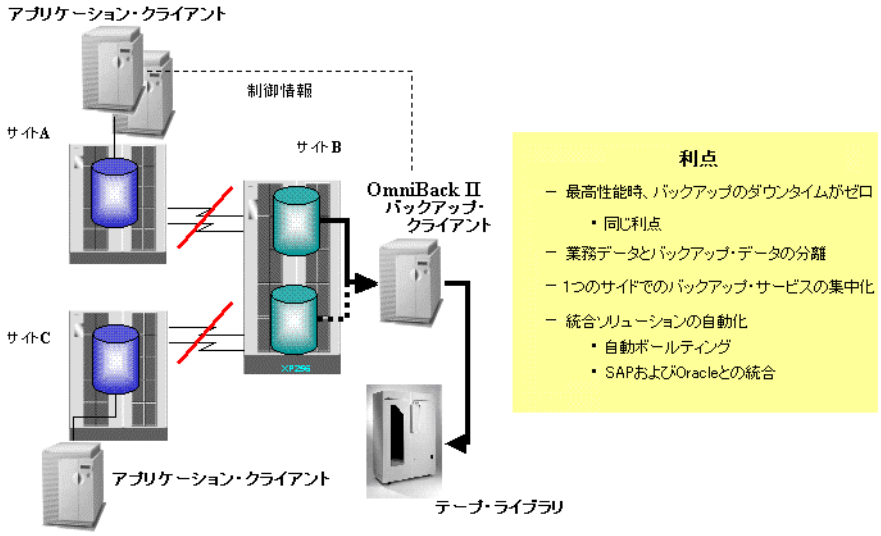
バックアップ専用のサーバを使用できない場合は、1 つのクライアント (またはホスト) で両方の機能 (アプリケーションとバックアップ) を実行します。例えば、メール用アプリケーションをオフラインでバックアップすることにより、アプリケーションのダウンタイムを数時間から数分にまで削減できます。

この種類の構成では**ディスク・イメージ** (raw ディスク) ・バックアップと**ファイルシステム**・バックアップのみをサポートしています。Oracle や SAP R/3 などのデータベースやアプリケーションのバックアップはサポートしていません。これは、バックアップ・サーバにデータベースをマウントする必要があり、すでにデータベースがマウントされている同じサーバにはデータベースをマウントできないためです。

リモート・ミラー

Continuous Access XP のようなリモート・ミラー技術を使用することにより、バックアップ・プロセスおよびアプリケーション・プロセスがさまざまな場所で異なるディスク・アレイ・リソースを利用できるようになり、前述の構成がさらに拡張されます。

図 11-3　スプリット・ミラー (リモート・ミラー) (LAN を経由しないリモート・バックアップとデータの高可用性)



リモート・ミラーでは物理的に独立したサイトにデータを転送します。データは、このサイトでローカルに使用可能なテープにバックアップされます。これによって実稼働データとバックアップ・データを分離できるため、火災等の災害により実稼働環境とバックアップ環境が同時に破損する危険性がなくなります。

バックアップ中のミラーとの同期をとるためにはネットワーク・リソースは必要ありません。データはネットワークを通じて転送されませんが、Cell Manager とそのクライアントとの間の通信は必要です。

このソリューションは、複数の実稼働サイト (この場合 A と C) からのアプリケーション・データを中心地または中核のディスク・アレイにミラーリングすることによって、バックアップ・サービスを集中化することができます。この場合、バックアップ・サービス (サーバおよびテープ・ライブラリ) に投資することによって高可用性を備えたリモート・ミラー構成と統合できます。

リモート・サイトは、バックアップ時に 2 つのサイト間のリンクが切断されるため (また 2 つのディスクの同期がとられないため)、バックアップ時は自動障害復旧サイトとしては使用できません。これは、サイト A で障害が発生した場合、一定期間 (データをテープへストリームするために必要な時間) 通常行っているようにサイト B が自動的に作業を引き継げないことを意味しま

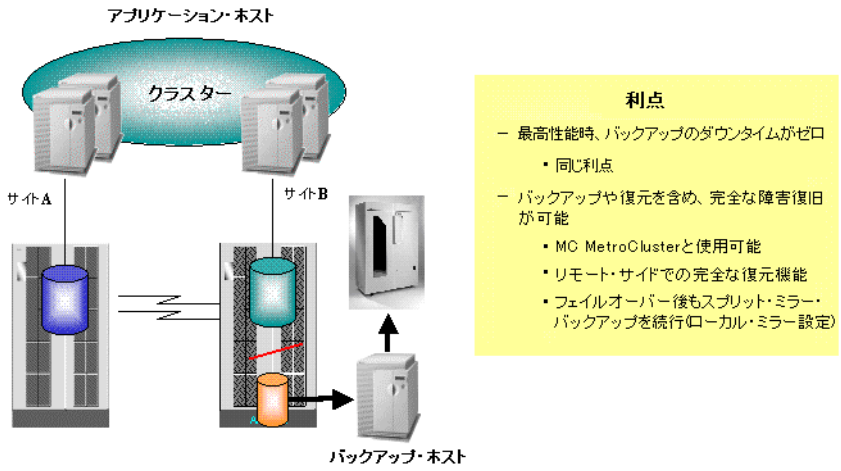
す。これはローカル・ミラーリングにも当てはまることですが、リモート・ソリューションに対しては特に重要です。これは、ハードウェア・ミラー概念を使用したリモートの障害復旧サイトという概念が業界で広く受け入れられているためです。

ローカル・ミラーとリモート・ミラーの組み合わせ

常時使用可能な障害復旧サイト (MetroCluster などによって提供される) が必要な場合、ダウンタイムのないバックアップ・ソリューションに加え、リモート・ミラーとローカル・ミラーを組み合わせて使用できます。

このソリューションによってリモート・サイトでの復旧ソリューションとスプリット・ミラーの両方の利点を完全に享受することができます。この例では、リモート・ミラーはバックアップの目的でローカル・リンク・スプリットだけを使って常に維持されるので、クラスタは継続的にリモート・サイト (サイト B) へフェイルオーバーできます。

図 11-4　ローカル / リモート・ミラーを組み合わせて使用 (障害復旧統合バックアップ [サービスの高可用性 (HP-UX のみ)])



フェイルオーバー機能をバックアップ操作と分離させるには、バックアップ・クライアントがクラスタの外部にある別のクライアントである必要があります。MetroCluster ソリューションを実行する場合、クラスタ調停クライアントをバックアップ・クライアントとして使用できます。

その他の構成

この他にも特定の利点を提供したり、特定のユーザーのニーズを満たすようなスプリット・ミラー構成が多数あります。ただし、それぞれの構成には固有の動作パターンがあり、バックアップおよび復旧を保証するには機能を制御するために特定の要件が課されます。サポートされている構成を管理、把握しておくことが重要です。

当社ではここで示したすべての構成をサポートしています。サポートされる構成の最新情報は以下の URL を参照してください。http://www.openview.hp.com/products/datapro/spec_0001.html

ここで紹介されていない構成でデータをバックアップする場合、その構成がサポートされないという意味ではありません。最寄りの当社営業担当または相談窓口に、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。

12 スナップショットの概念

本章の内容

この章ではスナップショット・バックアップの概念と、当社がサポートする構成について説明します。

この章の構成は以下のとおりです。

概要

急増する高可用性記憶装置構成への要望に応えて、ダウンタイムをゼロに抑えたバックアップ (ZDB: Zero Downtime Backup) を行うための新しい技術が開発されました。記憶装置の仮想化技術の進歩により、従来のスプリット・ミラー技術に代わる新たな手法が可能になりました。

Data Protector の ZDB ソリューションでは、さまざまなディスク・アレイ技術と最新のスナップショット技術を組み合わせて、ディスク・アレイ上に保存されているアプリケーション・データやデータベース・データのスナップショットを作成できます。作成したスナップショットは、特定の時点におけるオリジナル・データのコピーとしてディスク・アレイ上に保存しておき**インスタント・リカバリ**に使用することもできれば、バックアップ・システム上のテープへの ZDB のセッションに使用することもできます。関連するプロセスはアプリケーション・サーバに最小限の影響しか及ぼさず、効率のよい ZDB ソリューションが提供されます。

記憶装置の仮想化

「記憶装置の仮想化」とは、記憶装置の論理的な表現と、実際の物理的な記憶装置コンポーネントを切り離す技術を指します。具体的にはディスク・アレイ内に存在する物理ディスク・プールから、論理ボリュームを作成することを意味します。論理ボリュームはプール境界を越えることはできませんが、ディスク・アレイ内の複数の物理ディスクにまたがることは可能です。論理ボリュームは 1 つまたは複数のホスト・システムから使用できます。論理ボリュームに対して、物理ディスク上の割り当て位置を厳密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により割り当てを制御することは可能です。

RAID

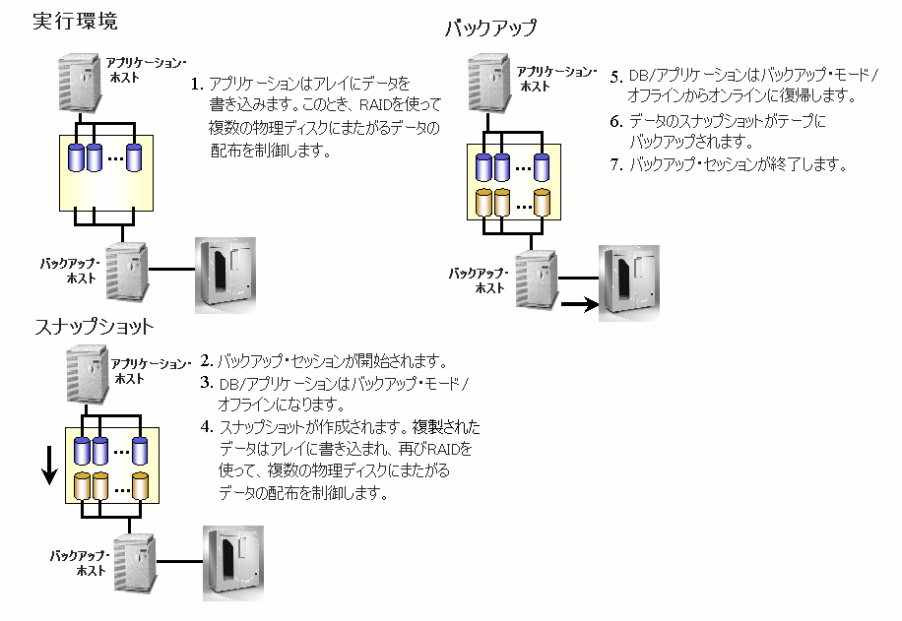
RAID (Redundant Array of Inexpensive Disks) 技術は、ディスク・アレイ内の複数の物理ディスク上にデータをどのように配布するかを制御するのに用いられます。RAID にはいくつかのレベルがあり、それぞれにデータの冗長性、データ・セキュリティ、速度、アクセス時間などのレベルが異なります。例えば、RAID0 ではデータの二重化は行われず、RAID1 ではすべてのデータが二重化され、RAID5 ではパリティによるデータ保護が提供されます。

Data Protector のスナップショット統合機能は、HP StorageWorks Virtual Array、HP StorageWorks Enterprise Virtual Array などの、スナップショット技術を使用するディスク・アレイで動作する設計となっています。

スナップショットの概念

スナップショット技術を使用する基本的なセットアップでは、単一のディスク・アレイがそれぞれ独立したアプリケーション・システムとバックアップ・システムの両方に接続されています。このようなディスク・アレイはアプリケーション・システムとバックアップ・システムの両方から記憶装置として使用でき、論理ボリュームはどちらのシステムにもマウント可能です。このような構成では、アプリケーション・システムは通常動作中に、自身のデータをディスク・アレイ内の論理ボリュームに保存します。アプリケーション・システム・データを格納している論理ボリュームは Data Protector のスナップショット統合機能で使用され、**ソース ボリューム**とも呼ばれます。スナップショット・バックアップを実行すると、ソース ボリューム上にあるアプリケーション・データが複製されて、同じディスク・アレイ上の別の論理ボリュームに書き込まれます。この論理ボリュームは**ターゲット・ボリューム**と呼ばれます。複製されたデータはスナップショット・データとも呼ばれ、これは特定のファイルシステムまたはボリュームのほぼ瞬間的なある特定時点におけるコピーです。このようにして作成されたターゲット・ボリュームのセットは**複製**と呼ばれます。スナップショット・データの複製の作成が終了すれば、その後は一次データを変更してもバックアップ処理に影響が及ぶことはありません。

図 12-1　　スナップショット・バックアップ



バックアップ・クライアントは、テープ・デバイスが接続された Data Protector クライアントとして設定し、ローカル・バックアップを実行できるようにします。

バックアップ・セッションが開始されると、バックアップ・クライアントではバックアップ・プロセスの準備が行われる一方、アプリケーション・クライアントはバックアップ・モードに入り、アプリケーション・データのスナップショットが作成されます。

バックアップ・クライアントの準備が完了し、スナップショット・データの複製が作成されると、アプリケーションは通常の動作に戻ります。

アプリケーション・クライアントがバックアップ・モードになっている間 (アプリケーションによっては短時間停止する場合もあります)、アプリケーションの可用性に対する影響は最小限に抑えられます。

テープへの ZDB を指定した場合は、バックアップ・クライアント上のテープ・メディアにスナップショット・データがストリームされます。テープ・メディアのストリーミング中も、アプリケーション・クライアントは影響を受けることなく動作できます。

(ほとんどの場合) アプリケーション・クライアントとバックアップ・クライアントは別個のため、スナップショットが作成される前に、アプリケーション・クライアント上でキャッシュに入れられたすべての情報 (データベース・キャッシュ、ファイルシステム・キャッシュ) をアレイに出力しておくことが非常に重要になります。これを行うには、以下のオプションのいずれかを使用します。

- データベースをバックアップ・モードにする。
- データベースをオフラインにする。
- マウント・ポイントをアンマウントする。

オンライン・データベース・バックアップの場合、復元を行うにはスナップショット・データだけでは不十分です。アプリケーション・クライアントからのアーカイブ・ログ・ファイルも必要となります。Data Protector の標準的なバックアップ手順によるアーカイブ・ログ・ファイルのバックアップは、スナップショットが作成された直後に開始できます。このときデータベースはバックアップ・モードから復帰します。

アプリケーション・データのスナップショット・データの作成には、次に示すような仮想ディスク・アレイ技術が使用されます。

- HP StorageWorks Business Copy Virtual Array
- HP StorageWorks Enterprise Virtual Array

スナップショット・バックアップの種類

Data Protector のスナップショット統合機能では、次の種類のスナップショット・バックアップが可能です。

- テープへの ZDB

- ディスクへの ZDB
- ディスク + テープへの ZDB

テープへの ZDB とディスク + テープへの ZDB

テープへの ZDB およびディスク + テープへの ZDB のセッション中は、アプリケーション・データの特定時点におけるスナップショット・データが、別のバックアップ・システムに接続されたテープ・デバイスにストリームされます。この処理には Data Protector の Disk Agent と General Media Agent が使用され、アプリケーション・システムへの影響は最小限に抑えられます。バックアップの終了後、スナップショット・データは次のように処理されます。

- 廃棄 - テープへの ZDB の場合
- 保持 (インスタント・リカバリに使用可能) - ディスク + テープへの ZDB の場合

ディスクへの ZDB

ディスクへの ZDB のセッション中は、テープへの ZDB やディスク + テープへの ZDB と同様の標準的なスナップショット技術が使用されますが、スナップショット・データはスナップショット・コピーからバックアップ・メディア (テープ・デバイス) にストリームされることはなく、ディスク・アレイ上に保持されます。このスナップショット・データはインスタント・リカバリに使用できます。スナップショット・データの作成が終了したら、セッションは事実上終了します。

インスタント・リカバリ

スナップショット・バックアップ・セッションでは、データのスナップショット・コピーを複数生成して、ディスク・アレイ上に保持できます。個々の特定時点におけるコピーはそれぞれ専用の複製に保存されます。保持されているスナップショット・コピー・データは、オフラインのデータ処理やインスタント・リカバリなどのさまざまな目的に使用できます。インスタント・リカバリ機能による復元が可能なのは、ディスクへの ZDB およびディスク + テープへの ZDB のセッション中に生成された特定時点におけるコピーのみです。

インスタント・リカバリ機能を使用すると、選択した複製内にある特定時点におけるコピーがディスク・アレイ内に復元され、スナップショット・データが生成された時点の状態に戻されます。このプロセスではデータをテープ・メディアから復元する必要がないため、復元時間が大幅に短縮されます。

アプリケーションのアーカイブ・ログ・ファイルはスナップショット・バックアップに含まれていないため、アーカイブ・ログを復元して適用するには、当該ファイルをテープ・メディアから復元する必要があります。

複製セットと複製セットのローテーション

ディスク・アレイ上に同時に保持できる複製の最大数は、使用するディスク・アレイによって異なります。同一のバックアップ仕様に基づいてディスク・アレイ上に保存されている複数の複製は、そのバックアップ仕様に対する**複製セット**を形成します。この複製セットは、特定のバックアップ仕様に基づいてディスク・アレイ上に保存される複製の最大数によって定義されます。スナップショット・バックアップ・セッション中に、保持できる最大複製数に到達した場合は、複製セット内で最も古い複製のスナップショット・データが上書きされます。最大数にまだ達していなければ、新たな複製が作成されます。これらの動作を指して**複製セットのローテーション**と呼びます。

スナップショットの種類

Data Protector のスナップショット・バックアップ・セッション中に作成できるスナップショットの種類は、使用するディスク・アレイによって異なります。Data Protector のスナップショット統合機能では、次の種類のスナップショットが使用されます。

- ディスク・スペースの事前割り当てありのコピーオンライト・スナップショット
- ディスク・スペースの事前割り当てなしのコピーオンライト・スナップショット
- スナップクローン

ディスク・スペースの事前割り当てありのスナップショット

ディスク・スペースの事前割り当てありのコピーオンライト・スナップショットを作成するには、ソース ボリュームと同じディスク容量の事前割り当てが必要です。ただし実際に必要になるまでは、予約されたスペースにデータが書き込まれることはありません。ソース ボリューム上のデータが変更されたら、ターゲット・ボリューム上のスナップショット・データも元のデータに合わせて更新されます。

このスナップショット技術では、絶えず変化し続ける元のデータのうち、特定時点における状態からの変更内容のみがキャッシュに入れられます。ディスク・スペースの事前割り当てありのコピーオンライト・スナップショットはそれぞれソース ボリュームに依存しているため、ソース ボリューム上のデータが失われた場合は、対応するスナップショットは役に立たなくなります。

ディスク・スペースの事前割り当てなしのスナップショット

ディスク・スペースの事前割り当てなしのコピーオンライト・スナップショットも元のデータの特定時点におけるコピーですが、ディスク容量の事前割り当ては必要ありません。ディスク・スペースは必要に応じて動的に割り当てられます。ソース ボリューム上のデータが変更されると、ディスク・アレイ内の空きスペースを使ってスナップショットが作成されます。ディスク・スペースの事前割り当てなしのコピーオンライト・スナップショットは、短期間のみ保持するス

ナップショットに適しています。スナップショット・データのサイズは動的に拡張し続けるため、定期的に削除しなければ、最終的には記憶域の容量を使い切ってしまう点に注意してください。

ディスク・スペースの事前割り当てなしのコピーオンライト・スナップショットの最大の利点は、ディスク・スペースの事前割り当てありのコピーオンライト・スナップショットに比べて、コストを大幅に削減できる点です。スナップショットを定期的に削除すると、標準的なスナップショット技術を使用する場合に比べて、複製スペースに必要な追加の記憶容量はかなり少なくて済みます。

このスナップショット技術では、絶えず変化し続ける元のデータのうち、特定時点における状態からの変更内容のみがキャッシュに入れられます。ディスク・スペースの事前割り当てなしのコピーオンライト・スナップショットはそれぞれソース ボリュームに依存しているため、ソース ボリューム上のデータが失われた場合は、対応するスナップショットは役に立たなくなります。

スナップクローン

スナップクローンの作成時には、最初にディスク・スペースの事前割り当てありのコピーオンライト・スナップショットと同様の処理が行われ、その後クローン化プロセスが実行されます。クローン化プロセスでは、ソース ボリューム上の全データがターゲット・ボリュームにコピーされます。スナップクローンを作成しておくと、複製データに迅速にアクセスできるようになります。クローン化プロセス自体はディスク・アレイの待ち時間を利用して、バックグラウンドで実行されます。クローン化プロセスが終了したら、特定時点におけるソース ボリュームの状態をそのまま反映したフル・データ・コピーであるスナップクローンが完成しています。そのため、ソース ボリューム上のデータが失われても、スナップクローンを作成した時点の状態にいつでも復帰できます。

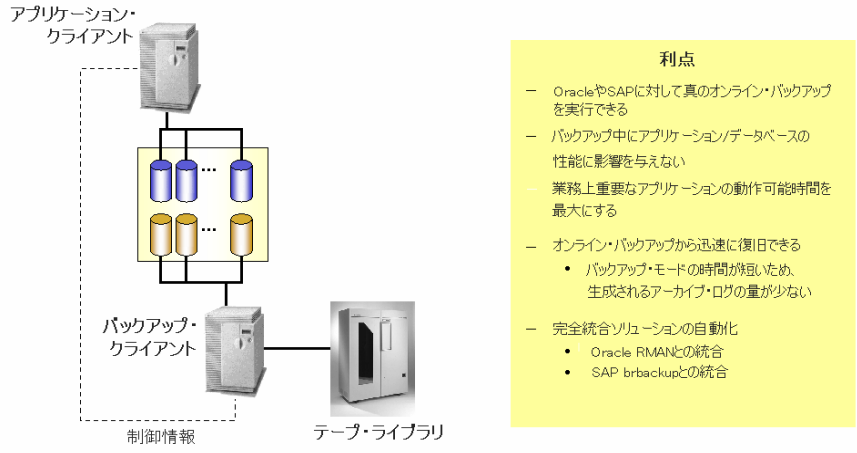
サポートされる構成

基本的な構成 : 単一のディスク・アレイ (デュアル・ホスト)

両方のホストが同じディスク・アレイに接続されるため、RAID システムの I/O インフラストラクチャはアプリケーション・クライアントとバックアップ・クライアントの間で共有されます。

アプリケーション・クライアントとバックアップ・クライアントは物理的には個別のシステムであるため、それぞれ各自の処理 (相互干渉しないバックアップ) には独自のリソース (I/O チャンネル、CPU、メモリなど) を使用できます。そのためバックアップ処理がデータベースの性能に与える影響は最小限で済みます。

図 12-2　単一のディスク・アレイ (デュアル・ホスト) (最高性能、ダウンタイムがゼロのバックアップ)



Data Protector のスナップショット統合機能では、ディスク・アレイ状態への自動対応のほか、アプリケーション (SAP R/3、Oracle、Microsoft SQL や Exchange Server など) との緊密な統合が可能であるため、データの整合性や、アプリケーション / データベースに対応したバックアップの実行が保証されます。アプリケーション / データベースがバックアップが行われていることを認識している場合に限り、安全な操作が保証されます。この場合、アプリケーション固有のツール (sapdba など) を使用して復元が行えます。バックアップがアプリケーションに与える影響は、以下の手順を実行する時間にまで削減されます。

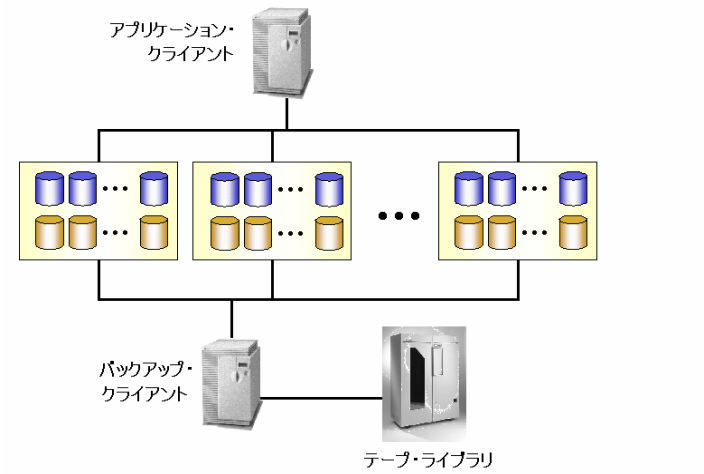
1. スナップショットの実行が可能な、整合性のある状態にデータベースを戻す。
2. アプリケーション・データのスナップショットを実行する。
3. データベースを通常の動作モードに戻す。

この構成では非常に大規模なデータベースのオフライン・バックアップを短時間で実行でき、また少しのアーカイブ・ログ・ファイルしか作成しないオンライン・バックアップも行えます。これはデータベースのバックアップ・モード時間を最小限に抑えることができるためです。

アーカイブ・ログの数が少なければ、データベースの復旧プロセスを高速化できるだけでなく、アーカイブ・ログ全体の必要な容量を抑えることができます。オンライン・データベースを復元したら、データベースを整合性のある状態に戻す必要があります。バックアップ中に生成されたすべてのアーカイブ・ログを適用することが必要です。スナップショット・バックアップでは、スナップショット中に作成されたアーカイブ・ログ・ファイルだけが適用されます。

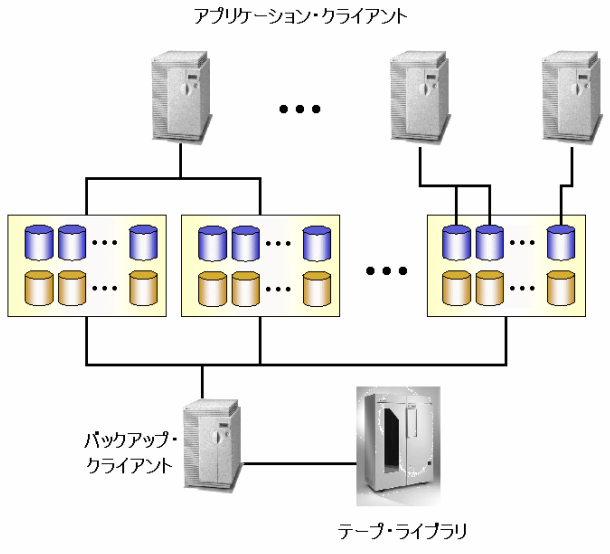
サポートされるその他の構成

図 12-3　　複数のディスク・アレイ (デュアル・ホスト)



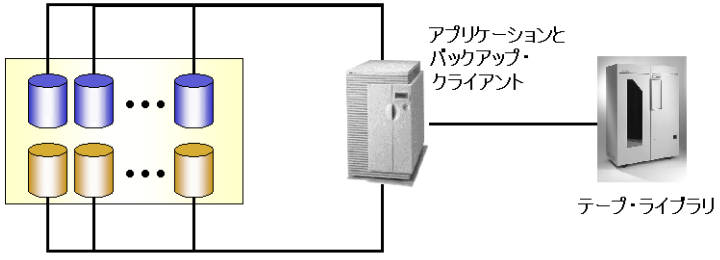
このソリューションでは、2 つのホストを複数のディスク・アレイに接続します。RAID システムの I/O インフラストラクチャは、アプリケーション・クライアントとバックアップ・クライアントの間で共有されます。

図 12-4　　複数のアプリケーション・ホスト (シングル・バックアップ・ホスト)



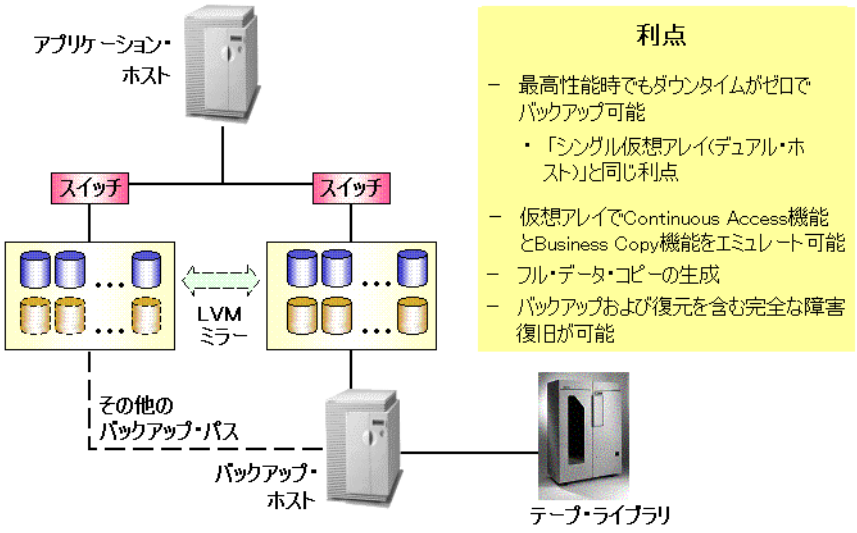
このソリューションでは、複数のアプリケーション・ホストを 1 つまたは複数のディスク・アレイに接続できます。接続先の仮想アレイは 1 台のバックアップ専用ホストに接続します。RAID システムの I/O インフラストラクチャは、アプリケーション・クライアントとバックアップ・クライアントの間で共有されます。

図 12-5　　ディスク・アレイ (シングル・ホスト)



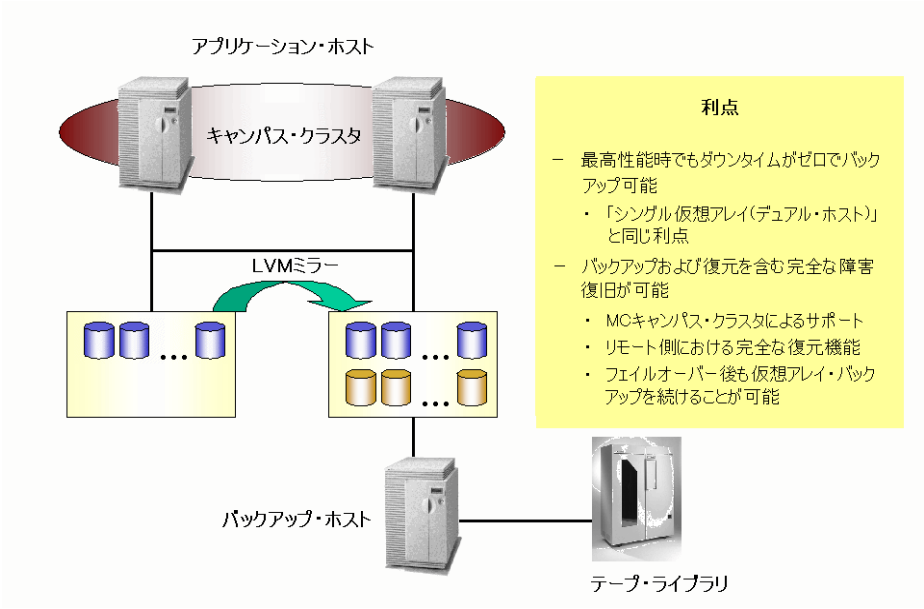
専用のバックアップ・サーバが使用可能でない場合は、アプリケーションとバックアップのどちらの機能も同一クライアント (またはホスト) 上で実行できます。例えば、メール用アプリケーションをオフラインでバックアップすることにより、アプリケーションのダウンタイムを数時間から数分にまで削減できます。

図 12-6　　LVM ミラー (HP StorageWorks Virtual Array のみ)



前述したサポート対象構成では、HP StorageWorks Virtual Array 統合ソフトウェアの Business Copy 機能のみが使用可能です。ただし LVM ミラーを使用すると、異なる仮想アレイ間にデータのスナップショット・コピーを作成し、両方の仮想アレイに同時に書き込むことが可能になります。これにより、HP StorageWorks Disk Array XP で使用可能な Continuous Access 機能と Business Copy 機能をエミュレートできます。

図 12-7　　LVM ミラーを使用するキャンパス・クラスタ (HP StorageWorks Virtual Array のみ)



この構成では、標準的なクラスタ・フェイルオーバー機能に加えて、Continuous Access 機能と Business Copy 機能をエミュレートできます。ミッション・クリティカルなアプリケーションについては、しばしばこの構成が必要となります。

バックアップ・クライアントとクラスタ

バックアップ・クライアントは、アプリケーション・クライアント用のフェイルオーバー・サーバとしては使用しないでください。アプリケーション・サービスとバックアップ・サービスは、別々のクラスタ上に置くことをお勧めします。

その他の構成

この他にも特定の利点を提供したり、特定のユーザーのニーズを満たすようなディスク・アレイ構成が多数あります。ただし、それぞれの構成には固有の動作パターンがあり、バックアップおよび復旧を保証するには機能を制御するために特定の要件が課されます。サポートされている構成を管理、把握しておくことが重要です。

当社ではここに示す構成のみサポートしています。サポートされる構成の最新情報は以下の URL を参照してください。http://www.openview.hp.com/products/datapro/spec_0001.html

ここで紹介されていない構成でデータをバックアップする場合、その構成がサポートされないという意味ではありません。最寄りの当社営業担当または相談窓口に、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。

13 Microsoft Volume Shadow Copy サービス

本章の内容

この章では、Microsoft Volume Shadow Copy サービス (VSS) の概念と、バックアップ処理および復元処理におけるこの機能の役割について説明します。また、この機能を使用する場合のバックアップ処理および復元処理の流れについても簡単に説明します。

この章の構成は以下のとおりです。

統合の詳細については、『*HP OpenView Storage Data Protector インテグレーション ガイド*』を参照してください。ファイルシステムのバックアップと復元の詳細については、『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。

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法では、バックアップする個々のアプリケーションに対応した個別のインタフェースを、バックアップ・アプリケーション側で用意する必要があります。

市販されているアプリケーションは日々その数を増しています。これらのさまざまなアプリケーション固有の機能に対処しなければならないため、バックアップや復元、記憶などの処理はより難しくなってきています。こうした問題に対する有効な解決策として登場したのが、バックアップや復元に関わる要素間に調整役を導入するやり方です。

VSS

Volume Shadow Copy サービス (VSS) は、Microsoft 社により 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・コピーの提供元 (プロバイダ)、およびオペレーティング・システムのカーネルと連携して、ボリュームのシャドウ・コピーおよびシャドウ・コピー・セットの管理機能を実現しています。

Volume Shadow Copy サービスとは、統合された通信インタフェースを提供することにより、個々のアプリケーション固有の機能とは無関係に各アプリケーションのバックアップおよび復元を調整しようというものです。この方法を採用すると、バックアップ・アプリケーション側で個々のバックアップ対象アプリケーションを個別に操作する必要がなくなります。ただしこの方法を使えるのは、VSS 仕様に準拠しているバックアップ・アプリケーションに限られます。

シャドウ・コピーとは

シャドウ・コピーとは、元の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。ボリューム・シャドウ・コピー技術を使用すると、元のボリュームの特定時点におけるコピーを作成できます。データのバックアップには、元のボリュームではなくこのシャドウ・コピーが使われます。バックアップ中に元のボリュームに変更が加えられても、ボリュームのシャドウ・コピーは整合性のある状態に保たれます。

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。

ライターとは

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 (例えば MS 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・プロバイダとは

シャドウ・コピー・プロバイダとは、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・プロバイダはソフトウェア (システム・プロバイダや 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・プロバイダである MS Software Shadow Copy Provider はソフトウェア機構であり、Windows Server 2003 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・プロバイダが使用されるようにします。いずれのプロバイダでもシャドウ・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

Volume Shadow Copy 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・プロバイダ間の調整を可能にします。

図 13-1 と図 13-2 は、従来のバックアップ・モデルと VSS を調整役に使用するモデルとの違いを示したものです。

図 13-1 従来のバックアップ・モデルに関係する要素

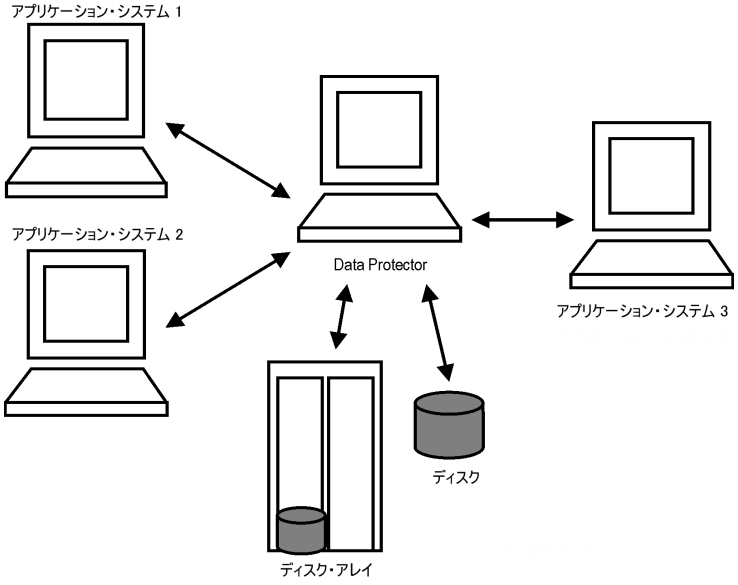
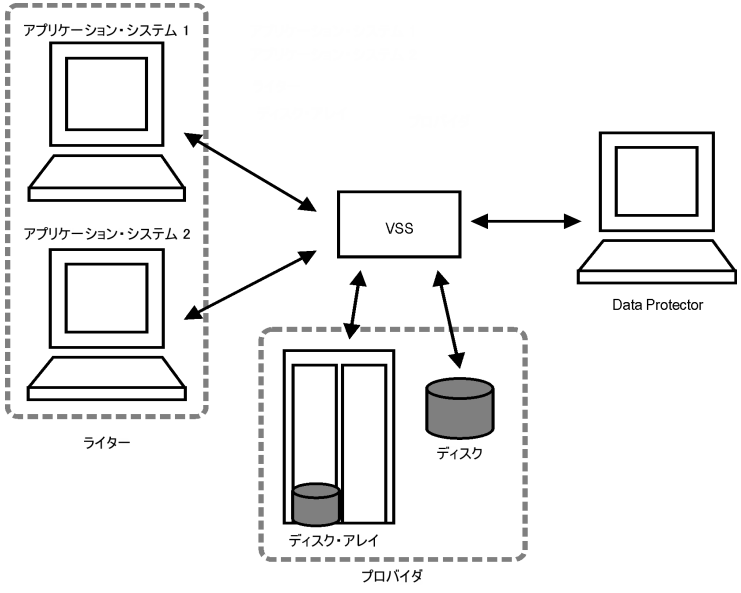


図 13-2 VSS バックアップ・モデルに関係する要素



従来のモデルでは、バックアップ・アプリケーションはバックアップ対象アプリケーションと個別のインタフェースで交信する必要があります。一方 VSS モデルの場合は、バックアップ・アプリケーションは VSS とのみ交信し、バックアップ処理全体は VSS により調整されます。

VSS の利点

Volume Shadow Copy サービスを使用する利点は以下のとおりです。

- 統合されたバックアップ・インタフェースがすべてのライターに提供されます。
- 統合されたバックアップ・インタフェースがすべてのシャドウ・コピー・プロバイダに提供されます。
- データの整合性はライターによりアプリケーション・レベルで提供されます。バックアップ・アプリケーションによる介入は必要はありません。

Data Protector は Microsoft Volume Shadow Copy サービスを次の 2 つのレベルでサポートしています。

- Microsoft Volume Shadow Copy サービスと統合すると、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に提供されます。アプリケーションが VSS 対応でない場合もシャドウ・コピーは作成されますが、アプリケーション・レベルでのシャドウ・コピー・データの整合性は保証されません。ただしこの場合も、非 VSS ファイルシステム・バックアップに比べると、整合性は向上しています。

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。

表 13-1 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。

表 13-1 VSS を使用する利点 (続き)

	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
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。	整合状態の破損 (電源障害の発生時と同等のレベル)。	なし (本質的に)

Data Protector と Volume Shadow Copy の統合

Data Protector と Microsoft Volume Shadow Copy 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。この中には VSS 対応ライターの自動検出、バックアップ、復元などの機能も含まれます。統合の詳細については、『*HP OpenView Storage Data Protector インテグレーション ガイド*』を参照してください。

VSS バックアップ

VSS 対応ライターのバックアップでは、データの整合性はライター・レベルで提供され、バックアップ・アプリケーションには依存していません。Data Protector はライターからの要求に従って、バックアップ対象を選択します。

VSS 対応ライターのバックアップ時には、Data Protector が個々のライターと個別に交信することはなく、交信は VSS インタフェースを介して行われます。Data Protector は VSS 統合エージェントを使用して Volume Shadow Copy サービスと接続し、このサービスによりバックアップ処理が調整されます。VSS は Data Protector に、整合性のあるバックアップおよび復元の実行に必要なライター関連のメタデータを提供します。Data Protector はこのデータを調べて、バックアップすべきボリュームを特定します。次に Data Protector から VSS に、特定ボリュームのシャドウ・コピーを作成するよう指示が出されます。

注記

ライター・メタデータ・ドキュメント (WMD) とは、各ライターから提供されるメタデータです。各ライターはこのメタデータによって自身の識別情報を明らかにし、バックアップすべき対象とデータの復元方法をバックアップ・アプリケーションに指示します。このようにして、Data Protector はライターからの要求に従って、バックアップすべきボリュームと復元方法を選択します。

Volume Shadow Copy サービスはライターとプロバイダを同期させる働きをします。バックアップ・シャドウ・コピーの作成が終了したら、VSS はこの情報を Data Protector に伝えます。これを受けて Data Protector はシャドウ・コピー・ボリューム上のデータをメディアにバックアップし、作業が終了したらシャドウ・コピーを解放してもよいことを VSS に通知します。

VSS 復元

VSS 統合復元とは、Volume Shadow Copy サービスとライターの連携によりバックアップされたデータの復元を指します。復元処理中は Volume Shadow Copy サービスにより、Data Protector とライター間の交信が調整されます。

VSS 対応ライターの復元時には、Data Protector は最初に関連するすべてのメタデータを復元することにより、使用するバックアップ・コンポーネントと復元方法を決定します。次に Volume Shadow Copy サービスに接続し、復元処理の開始を宣言します。復元中は VSS によりライターのアクティビティが調整されます。Data Protector によるデータの復元が成功したら、VSS からライターに復元処理の完了が通知されます。これを受けてライターは復元されたデータへのアクセスと、自身の内部処理を開始できます。

VSS ファイルシステムのバックアップと復元

アプリケーションの中には Volume Shadow Copy 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。

ただしこの場合も、VSS 機能によるメリットがまったくないわけではありません。バックアップ・アプリケーションとシャドウ・コピー・プロバイダの連携により、データ整合性レベルは向上します。Microsoft ではこのようなデータ整合性状態を「クラッシュ時整合データ」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 Volume Shadow Copy 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。データ整合性のレベルは、電源障害が発生したような場合と同等です。アプリケーションがシャドウ・コピーの作成に主体的に関与していない場合は、Data Protector 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・バックアップ時のデータ整合性は、非 VSS ファイルシステム・バックアップに比べて優れています。VSS を使用すると、ボリュームのシャドウ・コピー・バックアップ、つまりすべての開いているファイルも含めた特定時点におけるファイルのコピーを生成できます。例えば VSS ファイルシステム・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されます。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・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。

バックアップと復元

VSS バックアップは Windows Server 2003 上に、追加の Windows ファイルシステム・バックアップ機能として実装されています。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ます。Windows ファイルシステムのバックアップと復元の詳細については、『*HP OpenView Storage Data Protector 管理者ガイド*』を参照してください。

VSS ファイルシステム・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 ファイルシステム・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。ただしコピー元ボリュームは新たに作成されたシャドウ・コピーで置き換えられます。シャドウ・コピーの作成に失敗した場合は、通常のファイルシステム・バックアップを続行することも可能です (バックアップ仕様内でこの動作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。

A バックアップ・シナリオ

本章の内容

この付録では、XYZ 社および ABC 社という 2 つの企業のバックアップ・シナリオを紹介します。これらの企業では、自社のデータ記憶システムの強化を計画しています。以下では、まず各企業の現在のバックアップ・ソリューションとその問題点を説明します。次にこれらの問題点を改善し、両社の将来のデータ量の増加にも対応できる新たなソリューションを提案していきます。

考慮すべき点

どちらの企業の場合も、バックアップ戦略の策定時には以下の点を考慮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。
  - どの程度のビジネス継続運用性が求められるのか。すべての重要な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。
- バックアップおよび復元の性能
  - ネットワークおよびシステムのトポロジー

    どのシステムがどのネットワーク・リンクを使用でき、転送速度はどの程度かを明らかにします。
  - バックアップ可能な時間枠

    各システムについてバックアップが可能な時間枠を明らかにします。
  - ローカル・バックアップかネットワーク・バックアップか

    バックアップ・デバイスをどのシステムに接続し、どのシステムをローカルな形でバックアップし、どのシステムをネットワーク経由でバックアップするのかを決定します。

- バックアップ方針の実装
  - — 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・メディアを遠隔地に保存してバックアップ・データを永続的に保護するかどうかを決定します。
  - — バックアップ仕様作成時の各システムのグループ化方法

    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およびバックアップ関連情報の保護期間

    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。

    Data Protector のカタログ・データベース内にバックアップ関連情報を保存しておく期間を決定します。
- デバイスの構成

  バックアップに使用するデバイスと、デバイスを接続するシステムを決定します。データ量が最も多い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、ライブラリ・デバイスの使用も検討してください。
- 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。
- ボールティング

  メディアを安全な場所に一定期間保管するかどうかを決定します。
- バックアップ管理者とオペレータ

  バックアップ・システム・ユーザーに付与する管理権限や操作権限を決定します。

XYZ 社のバックアップ

XYZ 社は次のようなサービスを提供する翻訳会社です。

- 翻訳、ローカライズ、言語編集、および校正
- 翻訳ドキュメントの検証
- 同時通訳および逐次通訳
- DTP (デスクトップ・パブリッシング) とグラフィック・デザイン
- 会議用通訳機器のレンタル

XYZ 社は現在年に 20 ～ 25% の割合で成長を続けています。同社の現在のバックアップ・ソリューションでは、この成長率に対応できません。またバックアップ・テープを手動で取り扱っているため、バックアップの作業負荷が非常に高くなっています。

バックアップ環境

ここでは、XYZ 社の現在のハードウェア環境およびソフトウェア環境と、実装されているデータ記憶方針について説明します。

XYZ 社は以下の 3 つの部門に分かれており、各部門は企業のネットワーク・バックボーンに接続されています。

- 英語部門
- その他言語部門
- 管理部門

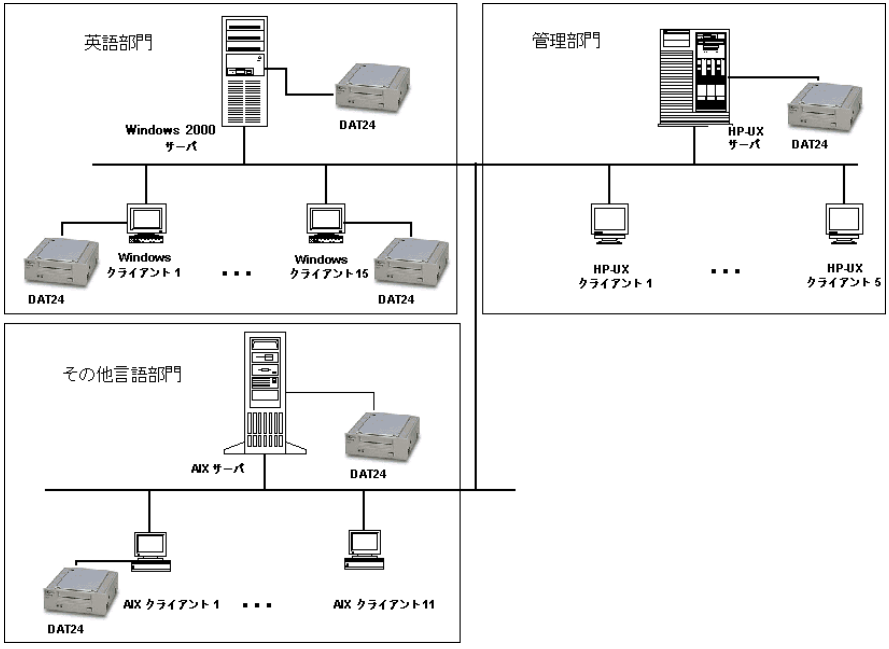
XYZ 社の現在のハードウェア環境とソフトウェア環境は 323 ページの表 A-1 に、また現在のバックアップ・トポロジーは 323 ページの図 A-1 に示すとおりです。

表 A-1　XYZ 社のハードウェア環境とソフトウェア環境

部門	サーバ数	クライアント数	現在のデータ量	将来的なデータ量 (5 年後)	現在のデバイス
英語	Windows 2000 1 台	Windows 15 台	35 GB	107 GB	HP StorageWorks DAT24 オートローダ 3 台
その他言語	AIX 1 台	UX 11 台	22 GB	67 GB	HP StorageWorks DAT24 オートローダ 2 台
管理	HP-UX 1 台	UX 5 台	10 GB	31 GB	HP StorageWorks DAT24 オートローダ 1 台

323 ページの図 A-1 は、XYZ 社のバックアップ環境を示したものです。

図 A-1　XYZ 社の現在のバックアップ・トポロジー



XYZ 社では現在 3 台のサーバを使用しており、データ量は合計で約 67GB に上ります。英語部門では、毎日の終業時に従業員がデータをそれぞれのサーバに手動でコピーしています。英語部門のデータ量の約 1/3 (12GB) は、この部門に属しているある 1 台の Windows 2000 クライアントのデータです。

その他言語部門のクライアントは、ネットワーク・ファイルシステムを介してバックアップされ、管理部門のクライアントはネットワーク共有を介してバックアップされています。その他言語部門の従業員は、土曜日も働いています。

現在のソリューションの問題点

現在のバックアップ・ソリューションでは、XYZ 社の成長の速さに対応できず、バックアップの作業負荷も非常に高くなっています。また現在のバックアップ・プロセスのままでは、バックアップ管理の統合や、全社レベルでのバックアップ・アーキテクチャの構築は不可能です。個々のバックアップ・サーバは個別に管理されており、バックアップを一元管理することはできません。次に、現在のバックアップ・ソリューションの問題点を示します。

- バックアップ・ソリューションが自動化されていません。
  - 従業員が手動でデータを定期的にコピーする必要があるため、ミスが生じる危険性が常にあります。
  - 複数のバックアップ・ユーティリティが使われているため、トレーニング・コストが高くつきます。
- その他言語部門と管理部門では多少は高度なソリューションが使われていますが、ここでも別の問題が発生しています。まずこれらの部門では、ネットワークの使用状況がバックアップの性能に大きく影響します。さらに、すべてのデータがバックアップされるわけではありません。その他言語部門ではネットワーク・ファイルシステム共有ファイルのみ、管理部門ではネットワーク共有ファイルのみがバックアップ対象となっています。
- 3 つの部門で使われている 3 台のバックアップ・サーバがそれぞれ独立しているため、以下に示すような重要な作業を一元的に制御および管理することができません。
  - デバイスの構成
  - メディア管理
  - バックアップ構成
  - スケジュール設定
  - モニタリング
  - 復元操作

- 各バックアップ・サーバが個別に管理されているため、一元的なレポートを作成できません。
- 現在のソリューションには、障害復旧機能がありません。これはますます重要性を増している問題点です。大きな障害が発生すると、企業は重要なビジネス・データを失う危険性があります。

バックアップ戦略の要件

要件

320 ページの「考慮すべき点」に示す項目を検討すると、XYZ 社のバックアップ・ソリューションについて以下の要件が明らかになります。

- バックアップ方針
  - 週 1 回フル・バックアップを実行し、12 時間以内に処理を終了しなければなりません。
  - 毎営業日には業務の最後に増分バックアップを実行し、この処理は 8 時間以内に終了しなければなりません。
  - 永続的なデータ保護期間を設定します。
  - バックアップ・メディアは遠隔地に保管します。
- バックアップ

  すべてのバックアップ操作について、現在よりもオペレータの介入を減らす必要があります。
- 復元
  - 最近作成したバックアップ・データは、簡単かつ迅速に復元できなければなりません。バックアップから 3 週間が経過するまでは、復元するデータをブラウズできるようにしておきます。
  - ボールトに保管してあるバックアップ・データも、2 日以内に復元できなければなりません。
- ネットワーク接続

  バックアップ・サーバと各部門は、100TX Ethernet LAN で接続します。
- データ量の増加予測

  今後 5 年間のデータ増加率は、年 20 ～ 25% 程度と予測されます。

- ソフトウェア

  バックアップ・サーバは、サポートされているオペレーティング・システム上で実行する必要があります。Cell Manager でサポートされているオペレーティング・システムの一覧は、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』を参照してください。

- 障害対策

  バックアップに使用したメディアは、ファイルを復元する場合に備えて、そのまま現場に保管しておきます。20 日が経過したら、企業サイトでの災害の発生に備えるとともに、新たなバックアップ・データの保管場所を空けるためにも、外部の保管場所に移送します。

ソリューション案

現在のバックアップ・ソリューションでは、バックアップの性能と全社レベルの管理の両面で限界があるため、XYZ 社の経営目的に合わせてバックアップのアーキテクチャと戦略を再設計する必要があります。以下では、まずソリューション案の概要を説明し、次にこのソリューションの詳細を紹介していきます。これは XYZ 社のデータ管理に対する唯一のソリューションではなく、1 つの提案にすぎない点に注意してください。

ソリューションの概要

すべてのクライアントとサーバを単一の Data Protector セル内に構成し、英語部門の Windows 2000 Server を Cell Manager 兼 Windows システム用のインストール・サーバとして使用します。UNIX システム用のインストール・サーバには、管理部門の HP-UX バックアップ・サーバを使用します。またバックアップ・デバイスには、HP StorageWorks DLT 4115w Library 1 台と、既存の HP StorageWorks DAT24 オートローダのうちの 2 台を使用します。

この構成で、今後 5 年間における年 20 ～ 25%というデータ増加率に十分に対応できます。また、これまで使われてきたデバイスを使用することは、障害復旧の面で付加的な利点があります。英語部門のデータ量の約 1/3 (12GB) を保持する Windows 2000 クライアントは、HP StorageWorks DAT24 オートローダにローカルな形でバックアップできるようにします。このバックアップ・ソリューション案では、以下の主要目的が達成されています。

- バックアップの性能が向上します。
- 最小限の手間でメディアを管理できます。
- 簡潔かつ効率的な障害復旧が可能です。
- 一元的なバックアップ・レポートを作成できます。
- 大部分のバックアップ操作が自動化されます。

このソリューションにおけるこれらの機能はすべて、次に示すハードウェアと組み合わせることで達成されます。

表 A-2 提案されるバックアップ環境

部門	現在のデータ量	将来的なデータ量 (5 年後)	デバイス	
英語 *	35 GB	107 GB	HP DLT 4115 Library	HP StorageWorks DAT24 オートローダ 2 台
その他言語	22 GB	67 GB		
管理	10 GB	31 GB		
* 現時点では、12GB のデータをローカルにバックアップするために、1 台の HP StorageWorks DAT24 オートローダが使用されます。もう 1 台の HP StorageWorks DAT24 オートローダは、IDB と構成ファイルのバックアップに使用されます。この部門の残りのデータは、HP StorageWorks DLT 4115 Library にリモートでバックアップされます。				

残り 4 台の HP StorageWorks DAT24 オートローダは別の R&D システムで使われており、この構成には含まれません。

この企業バックアップ・ソリューション向けに提案されるソフトウェア・コンポーネントには、HP OpenView Storage Data Protector A.05.50 も含まれます。

ソリューション案の詳細

以下に、このソリューション案の詳細について説明します。

- セルの構成

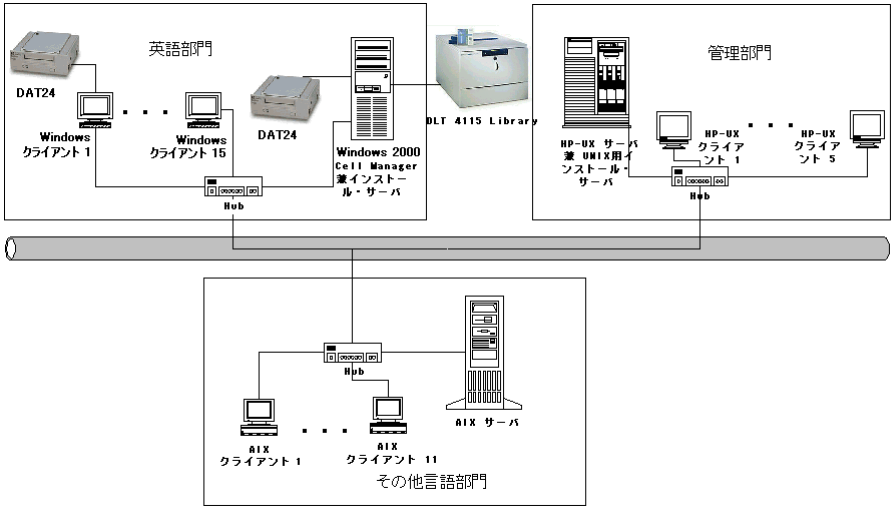
  すべてのクライアントとサーバは、単一の Data Protector セル内に構成します。Data Protector Cell Manager は、英語部門の Windows 2000 Server 上で実行します。

  最大の性能を引き出すには、セル内のすべてのシステムを同一 LAN 上に配置する必要があります。Cell Manager は、同時に Windows 用のインストール・サーバとしても使用します。UNIX 用のインストール・サーバには、管理部門の HP-UX バックアップ・サーバを使用してください。HP StorageWorks DLT 4115w Library は、IDB と構成ファイルをバックアップするための HP StorageWorks DAT24 オートローダ 1 台とともに、Cell Manager に

接続します。英語部門のデータ量の約 1/3 (12GB) を保持する Windows 2000 クライアントは、HP StorageWorks DAT24 オートローダにローカルな形でバックアップできるようにします。

ここで提案したバックアップ環境は、328 ページの図 A-2 に示すとおりです。

図 A-2　　XYZ 社のバックアップ・トポロジー案



Cell Manager では、CDB (Catalog Database、カタログ・データベース) が保守されます。これにより現在のデータベース上に、バックアップされたファイルやディレクトリに関する詳細情報が最低 20 日間保存されます。

IDB サイズの見積もり

IDB の 1 年間のサイズ変化の見積もりには、Internal Database Capacity Planning Tool を使用しています。このツールは Data Protector のその他のオンライン・マニュアルと同じディレクトリにあります。329 ページの図 A-3 に示す入力パラメータでは、環境内のファイル数 (2,000,000)、拡張係数 (1.2)、データ保護期間 (52 週間)、カタログ保護期間 (3 週間)、1 週間に行うフル・バックアップの回数 (1 回)、1 週間に行う増分バックアップの回数 (5 回) を指定しています。

図 A-3　　入力パラメータ

Environment description			
	Files:	2	million
	Files per directory:	10	
	Data volume:	200	GB
	Growth factor:	1.20	
	Device performance:	10.00	MB/second
	Medium capacity:	70.00	GB
	Objects:	50	
	Change per incr-bkup	5.00%	
Backup parameters			
	Device concurrency:	2	
	Data segment size:	2,048.00	MB
	Log level:	All	
	Data protection:	52	Weeks
	Catalog protection:	3	Weeks
	Full backups/week:	1	
	Incr backups/week:	5	
Cell Manager parameters			
	Insertion speed:	12	million/hour

329 ページの図 A-4 に結果を示します。データベースは 1 年間で約 419.75MB まで増加すると予測されます。

図 A-4　　結果

Results/calculation			
	Avg. file size:	123.36	KB
	Files/segement:	16,931.38	
	Catalog size:	1.03	MB
	K devices:	40	
	K performance:	1445.647059	GB/hour
	K duration:	0.14	hour
	Protected media:	278.5714286	
Space estimation			
MMDB:		30.00	MB
CDB:	Fnames:	153.00	MB
	Overs:	5.71	MB
	Mpos:	1.54	MB
DCBF:		229.50	MB
SMBF:		2.86	MB
Total:		419.75	MB

- ハードウェア
  - ネットワーク

最大の性能を引き出すには、すべてのシステムを同一の 100TX ネットワーク上に配置する必要があります。このネットワークは、10MB/s (36GB/h) のデータ転送速度を維持できます。

— バックアップ・デバイス

バックアップ・デバイスには 1 台の HP StorageWorks DLT 4115w Library と、2 台の HP StorageWorks DAT24 オートローダを使用します。

HP StorageWorks DLT 4115w Library を使う理由

HP StorageWorks DLT 4115w Library には、1 つの DLT4000 ドライブと 15 個のスロットがあります。このライブラリは圧縮状態で合計 600GB の記憶容量を持ち、データを圧縮した状態で 3MB/s (10.5GB/h) のデータ転送速度を維持できます。以下の説明ではこの転送速度を前提としています。現時点では、HP StorageWorks DLT 4115w Library にフル・バックアップする必要があるデータの総容量は、単一のフル・バックアップまたは時差実行方式のいずれを使用する場合も、約 55GB になります。増分バックアップのサイズをフル・バックアップの約 5% と見積もると、1 つのバックアップ世代、つまり 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がライブラリに占める容量は (55+55*5%*5)GB、つまり **68.75GB** になります。5 年後には、この値は約 210GB にまで増加すると予測されます。XYZ 社のバックアップ方針では 2 つのバックアップ世代を保管する必要があるため、210*2GB (420GB) のライブラリ領域が必要になります。そのため、600GB の記憶容量を持つ HP StorageWorks DLT 4115w Library で十分に対応できます。

HP StorageWorks DAT24 オートローダを使う理由

HP StorageWorks DAT24 オートローダには、24GB のデータ・カートリッジが 6 個あります。圧縮状態で合計 144GB の記憶容量を持ち、データを圧縮した状態で最大 2MB/s (7GB/h) のデータ転送速度を維持できます。以下の説明ではこの転送速度を前提としています。現時点では、前述した英語部門の Windows 2000 クライアントに接続された HP StorageWorks DAT24 オートローダに 1 回のフル・バックアップで保存する必要があるデータの総容量は 12GB になります。増分バックアップのサイズをフル・バックアップの約 5% と見積もると、1 つのバックアップ世代、つまり 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のサイズは (12+12*5%*5) GB、つまり **15GB** になります。5 年後には、この値は約 45GB にまで増加すると予測されます。XYZ 社のバックアップ方針

では 2 つのバックアップ世代を保管する必要があるため、45*2GB (**90GB**) のライブラリ領域が必要になります。そのため、144GB の記憶容量を持つ HP StorageWorks DAT24 オートローダで十分に対応できます。

フル・バックアップに要する時間

12GB のデータを持つ英語部門の Windows 2000 クライアントは、HP StorageWorks DAT24 オートローダにローカルな形でバックアップされます。このデバイスは 2MB/s、つまり約 7GB/h のデータ転送速度を維持できます。そのため、この Windows 2000 クライアントのフル・バックアップには、約 **2 時間**かかると計算できます。データ増加率を年 20 ～ 25% と予測すると、このクライアントの 5 年後のデータ量は約 36GB になり、フル・バックアップには約 **6 時間**を要するようになると予測されます。

Data Protector カタログ・データベースのサイズは約 0.4GB です。カタログ・データベースは HP StorageWorks DAT24 オートローダにローカルな形でバックアップされ、このオートローダは 2MB/s、つまり 7GB/h のデータ転送速度を維持できます。Data Protector では、デフォルトで、データベースのバックアップの前にそのデータベースの整合性がチェックされます。0.4GB のデータベースの整合性チェックは 30 分以内に終了し、データベースのバックアップ自体は数分程度で終了します。そのため IDB の整合性チェックと、データベースおよび構成ファイルのバックアップは、**1 時間**以内に終了すると計算できます。

カタログ・データベースのサイズは、5 年後には約 1.2GB になると予測されます。1.2GB のデータベースの整合性チェックは 1 時間以内に終了し、バックアップ自体は 30 分以内に終了します。そのため、5 年後の IDB の整合性チェックと、データベースおよび構成ファイルのバックアップは、**2 時間**以内に終了すると予測できます。

システム内のその他のデータは現時点で約 55GB の容量があり、HP StorageWorks DLT 4115w Library にリモートでバックアップされます。このライブラリは 3MB/s、つまり 10.5GB/h のデータ転送速度を維持できます。これらのデータの大部分は、100TX ネットワークを介して転送されますが、このネットワークは 10MB/s、つまり 36GB/h のデータ転送速度を維持できるため、ネットワークがボトルネックになることはなりません。そのため、これらのデータをすべてバックアップするには、約 **5 ～ 7 時間**かかると計算できます。現時点では許容限度の 12 時間以内に終了するため問題ありませんが、5 年後にはデータ量が約 170GB になると予測され、バックアップに 15 ～ 21 時間もかかることになってしまいます。

この問題を解決するには、時差実行方式を採用します。例えば英語部門のフル・バックアップは金曜日の 20:00 に開始し、その他言語部門のフル・バックアップは土曜日の 20:00 に、また管理部門のフル・バックアップは日曜日の 20:00 に開始するというようにスケジュールを設定します。

表 A-3 時差実行方式

	月	火	水	木	金	土	日
英語	増分 1	増分 1	増分 1	増分 1	フル	増分 1	
その他言語	増分 1	増分 1	増分 1	増分 1	増分 1	フル	
管理	増分 1	増分 1	増分 1	増分 1	増分 1		フル

現時点および 5 年後の、これらのフル・バックアップのサイズとバックアップにかかる時間は、332 ページの表 A-4 に示すとおりです。

表 A-4 HP DLT 4115 Library へのリモートのフル・バックアップ

部門	現在のデータ量 / バックアップ時間	将来的なデータ量 / バックアップ時間
英語	23 GB / 3 H	70 GB / 7 H
その他言語	22 GB / 3 H	67 GB / 7 H
管理	10 GB / 1 H	31 GB / 3 H

増分バックアップのサイズをフル・バックアップの約 5% とすると、5 年後に、最大の部門である英語部門のリモートのフル・バックアップと、他の 2 つの部門の増分バックアップをすべて実行するには、7+5%(7+3) 時間かかります。つまり 8 時間以内に処理を終了できます。そのため、5 年後も、許容限度の 12 時間以内に処理を終了できるとわかります。

- メディア・プール

  追跡や制御を容易にするために、個々のメディアはメディア・プールと呼ばれるグループにまとめられます。ここでは、メディアを、メディアの種類 (DLT と DDS) ごとのプールにまとめます。

  — デフォルト DDS

  このプールはすべての DDS メディア用に使用します。

  — デフォルト DLT

このプールはすべての DLT メディア用に使用します。

— DB_Pool

このプールは IDB と構成ファイル用に使用します。データベースはセキュリティ上の理由により、2 つのメディアにバックアップする必要があります。

- バックアップ仕様

各部門用と、IDB および構成ファイル用に、以下の 5 つのバックアップ仕様を構成します。

— ENG1_BS

英語部門内の、ローカルにバックアップする必要がある Windows 2000 クライアント用のバックアップ仕様です。このバックアップ仕様では、例えば、毎週金曜日に Data Protector によってフル・バックアップが実行されるようにスケジュールを設定し、さらに金曜と日曜を除く毎日 20:00 にレベル 1 増分バックアップが実行されるように設定します。

レベル 1 増分バックアップを使う理由

最新のデータを復元する場合に、2 つのメディア・セット、つまり最新のフル・バックアップと、復元時点よりも前に作成された最新のレベル 1 増分バックアップの 2 つのみになります。そのため復元処理が簡単になり、処理時間も大幅に短縮されます。

— ENG2_BS

英語部門のデータのうち、HP StorageWorks DLT 4115w Library にリモートでバックアップするデータ用のバックアップ仕様です。このバックアップ仕様では、例えば、毎週金曜日に Data Protector によってフル・バックアップが実行されるようにスケジュールを設定し、さらに日曜を除く毎日 20:00 にレベル 1 増分バックアップが実行されるように設定します。

— OTH_BS

その他言語部門のデータのうち、HP StorageWorks DLT 4115w Library にリモートでバックアップするデータ用のバックアップ仕様です。このバックアップ仕様では、例えば、毎週土曜日の 20:00 に Data Protector によってフル・バックアップが実行されるようにスケジュールを設定し、さらに日曜を除く毎日 20:00 にレベル 1 増分バックアップが実行されるように設定します。

— ADM_BS

管理部門のデータのうち、HP StorageWorks DLT 4115w Library にリモートでバックアップするデータ用のバックアップ仕様です。このバックアップ仕様では、例えば、毎週日曜日の 20:00 にフル・バックアップが Data Protector によって実行されるようにスケジュールを設定し、さらに土曜日を除く毎日 20:00 にレベル 1 増分バックアップが実行されるように設定します。

— DB_BS

IDB と構成ファイル用のバックアップ仕様です。このバックアップ仕様では、例えば、毎日 4:00 にフル・バックアップが Data Protector によって実行されるようにスケジュールを設定します。この時刻には、他のフル・バックアップや増分バックアップは終了しており、Cell Manager とその他クライアント・システム間での CPU リソースの共有に関する問題も発生しないはずです。データベースについては、2 つのコピーを作成する必要があります。

バックアップ・オプション

デフォルトの Data Protector バックアップ・オプションを使用します。以下のオプションを以下に示すように設定します。

— [カタログ保護 (Catalog Protection)]

[カタログ保護 (Catalog Protection)] オプションでは、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に関する情報、データベースに保存されているメッセージなどを、Data Protector カタログ・データベース内に保存しておく期間を設定します。カタログ保護期間が切れると、Data Protector GUI を使ったファイルやディレクトリのブラウズはできなくなります。カタログ保護期間は 20 日に設定します。

— [データ保護 (Data Protection)]

[データ保護 (Data Protection)] オプションでは、各メディアの再使用を許可するまでの期間を設定します。メディア上のデータを誤って上書きしないように、データ保護期間は [無期限 (Permanent)] に設定します。

— [同時処理数 (Concurrency)]

このオプションは 5 に設定して、最大 5 つの Disk Agent が HP StorageWorks DLT 4115w Library に同時にデータを書き込めるようにします。これにより、バックアップの性能が向上します。

— [メディア・プール (Media Pool)]

IDB については、適切なバックアップ・メディアが含まれている DB_Pool を選択します。その他のオブジェクトについては、デフォルトのメディア・プールを使用します。

復元オプション

デフォルトの Data Protector 復元オプションを使用します。以下のオプションを以下に示すように設定します。

— [復元されたデータをリスト (List Restored Files)]

このオプションはオンに設定して、復元されたファイルとディレクトリのパス名の一覧が作成されるようにします。復元するファイルの数が非常に多い場合は、このオプションにより処理速度が低下することがあります。

— [統計情報の表示 (Display Statistical Information)]

このオプションはオンに設定して、復元セッションに関する詳細な統計情報が表示されるようにします。統計情報には、復元されたファイルとディレクトリの数や、復元されたデータ量などが含まれます。

- レポートと通知

電子メール通知をセットアップしておき、すべてのバックアップ仕様に関するマウント要求、データベース容量の不足、デバイス・エラー、セッション終了イベントなどがバックアップ管理者に送信されるようにします。電子メールまたはブロードキャスト通知を使って、エンド・ユーザーに自分のシステムのバックアップが成功したかどうかを知らせることも可能です。

また、すべてのユーザーがバックアップ状態を簡単にチェックできるように、企業のイントラネット上にクライアント・バックアップ情報を以下に示すようにセットアップします。

1. [クライアントのバックアップをレポート (Client Backup Report)] を使って、各クライアントごとにレポート・グループを構成します。レポートは HTML 形式でログ・ファイルに記録してください。
2. レポート・グループのスケジュールを設定します。
3. ログ・ファイルを企業のイントラネット・ページにリンクします。

- ボールティング

ボールティングとは、メディアを安全な場所に一定期間保管するプロセスを指します。

メディアは毎週 1 回保管場所 (ボールト) に移送され、HP StorageWorks DLT 4115w Library と HP StorageWorks DAT24 オートローダ内には新しいメディアがセットされます。メディアを実際にボールトに移送する作業を除き、すべての処理はソフトウェアにより実行されます。例えば、データベースの照会も内部的に自動実行されるため、排出するメディアを管理者が自分で探す必要はありません。

その後メディアはボールトから警備会社に再び移送されます。この作業は毎月 1 回実行されます。Data Protector からは、警備会社に移送する必要があるメディアの一覧レポートが提供されます。

ボールトに移送したメディアについても、引き続き保管場所を追跡する必要があります。この情報は、警備会社に移されたメディアからデータを復元するような場合に重要になります。Data Protector では、ボールティングに関する以下のタスクを実行できます。

- 指定された場所に保管されており、指定された日時にデータ保護期間が切れるバックアップ・メディアの一覧レポートを生成できます。
- 指定された期間内に作成されたバックアップ・メディアの一覧レポートを生成できます。
- 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の一覧を表示できます。
- 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。
- なんらかの基準に基づいて (保護期間が切れたメディアなど)、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。

- 復元

  - 照会による復元

    照会による復元要求は、管理者に送られます。要求されたファイルが 20 日以内にバックアップされている場合は、管理者は復元タスクの [照会による復元 (Restore by Query)] を使って、なんらかの基準に基づいて復元するファイルやディレクトリを選択できます。次に管理者は、ディスク上のファイルやディレクトリをメディアに保管されているバージョンで上書きするために、[上書き (Overwrite)] オプションを選択します。

  - ファイルシステム全体の復元

    ファイルシステム全体の復元要求も、管理者に送られます。要求されたファイルが 20 日以内にバックアップされている場合は、管理者は復元するオブジェクトを選択できます。ファイルシステム全体の復元では、[復元先を指定して復元 (Restore Into)] オプションが使われます。

    [復元先を指定して復元 (Restore Into)] オプションを選択すると、オブジェクトは正確なディレクトリ構造を保ったままで選択したディレクトリに復元されます。Windows または UNIX のユーティリティを使うと、復元したオブジェクトとバックアップ・オブジェクトを比較できます。

  - ボールトからの復元

ボールトに保管されている、例えば 3 年前のデータを復元する場合は、まず要求を管理者に送ります。これを受けて管理者は以下の処理を実行します。

1. 復元に必要なメディアを特定します。
2. メディアをボールトから搬入し、HP StorageWorks DLT 4115w Library またはその他のデバイスに挿入してスキャンします。
3. そのメディアが IDB 内になければ、[メディアからリスト (List From Media)] オプションを使って復元するオブジェクトを選択します。
4. 復元処理を実行します。

ABC 社のバックアップ

ABC 社は成長著しいソフトウェア・エンジニアリング企業であり、南アフリカのケープタウンに本部を置いています。ABC 社はさまざまな国のビジネス・パートナーからソフトウェアを受注しており、複数のサイトにまたがるプロジェクト・チームと、それに対応したインフラストラクチャを構築して、広範囲にわたるソフトウェア・エンジニアリング・プロジェクトをシームレスに実行できるようにしています。ABC 社は年 30 ～ 40%の割合で成長を続けてきましたが、次の 5 年間では 15 ～ 20%程度に落ち着くと予測されています。

バックアップ環境

ここでは、ABC 社の現在のハードウェア環境およびソフトウェア環境と、実装されているデータ記憶方針について説明します。

ABC 社のオフィスは 3 つの場所に分かれています。それぞれのオフィスの主要なハードウェア構成は、338 ページの表 A-5 に示すとおりです。

表 A-5 バックアップ環境の構成内容

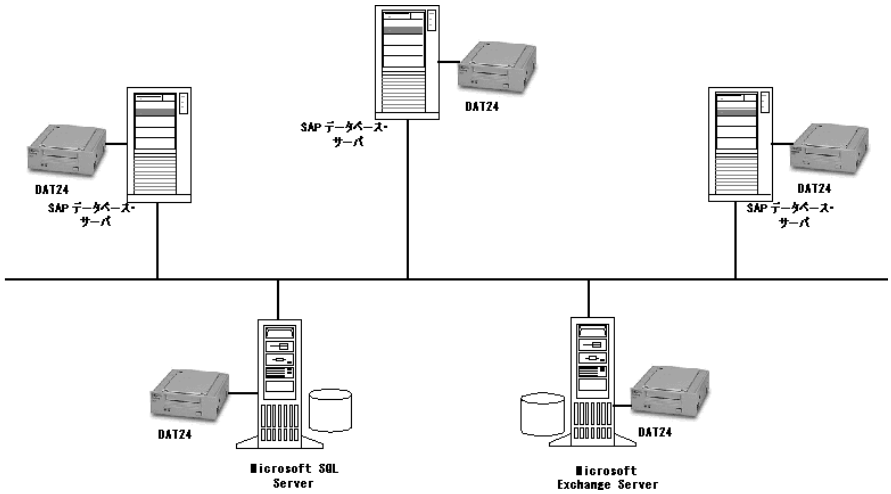
場所	Win サーバ数	Win クライアント数	UX サーバ数	UX クライアント数	現在のデータ量	将来的なデータ量 (5 年後)	現在のデバイス
ABC ケープタウン	7	55	11	40	100	250	DAT24* 5 台
ABC プレトリア	5	39	5	32	22	55	DAT24* 1 台
ABC ダーバン	3	21	6	59	16	40	DAT24* 1 台
* HP StorageWorks DAT24 オートローダ							

ABC ケープタウンにある 3 つの部門では、データの保存に Microsoft SQL データベースを使っています。また企業全体のメール・サービスには、Microsoft Exchange Server が使われています。現時点ではこれらのデータベースには、それぞれ 11GB および 15GB のデータが保存されており、2 台の HP StorageWorks DAT24 オートローダを使ってバックアップされています。

ABC ケープタウンのシステム・アーキテクチャには、Oracle データベースを使用する SAP R/3 システムが含まれており、3 台の HP T600 サーバが SAP データベース・サーバとして使われています。また ABC ケープタウンでは、販売と流通、経理、および製造の各業務グループ別に構

成された、複数の K260 SAP アプリケーション・サーバが使われています。これらのアプリケーション・サーバは高可用性構成にはなっていません。ABC ケープタウンの現在のバックアップ環境は、339 ページの表 A-5 に示すとおりです。

図 A-5　　ABC ケープタウンの現在のバックアップ・トポロジー



現在のところ、ABC ケープタウンの SAP データベース・サーバは、SAP BRBACKUP ユーティリティと BRARCHIVE ユーティリティを使って、3 台の HP StorageWorks DAT24 オートローダにバックアップされています。データは 1 日 1 回、従業員が手動でそれぞれのサーバにコピーしています。またバックアップ管理者は、Microsoft Exchange Server と Microsoft SQL データベースをそれぞれ個別に HP StorageWorks DAT24 オートローダにバックアップしています。

ABC ダーバンと ABC プレトリアでも同一のシステムが使われていますが、これらのサイトでは SAP システムは使われていません。従業員は各自のデータをそれぞれのサーバにコピーします。データは HP StorageWorks DAT24 オートローダに 1 日 1 回バックアップされます。

ABC プレトリアのサーバのうちの 2 台には、それぞれ 500,000 個以上のファイルが格納されています。

バックアップ・メディアには、部門名、サーバ名、およびそのメディアを使ったバックアップの最初と最後の日付が示されています。四半期の終わりには、メディアは外部の保管場所に移されて一元的に管理されます。

現在のソリューションの問題点

現在のバックアップ・ソリューションには、以下の問題点があります。

- SAP データベース・サーバに対するオンライン・バックアップ・ソリューションがありません。
- バックアップ・ソリューションが一元管理されていません。
- バックアップ操作が完全には自動化されていません。
- メディア管理にかなりのオペレータの介入が必要になります。
- 障害復旧が複雑です。
- バックアップ処理が、バックアップに許される時間枠内に終了しません。
- 現在のバックアップ・ソリューションでは、ABC 社の成長率に対応できません。
- バックアップに関する重要イベントについての報告や通知の機能がありません。

バックアップ戦略の要件

ABC 社のバックアップ戦略の要件を明らかにするには、まず 320 ページの「考慮すべき点」の項目を検討する必要があります。

要件

以下に、ABC 社のバックアップ戦略の要件について説明します。

- バックアップと復元に関する企業ポリシー

  データの記録や保存に関するこの企業のポリシーに従って、週単位のバックアップは **12 時間**以内に終了しなければならず、毎日の増分バックアップまたは差分バックアップは、**8 時間**以内に終了しなければなりません。
- 復旧までに許される最大ダウンタイム

復旧までに許されるダウンタイムは、バックアップに必要なネットワーク基盤や機器を整備するための予算に大きく影響します。以下の表は復旧までに許されるダウンタイム、つまりバックアップ・データからデータを復元するまでの間、どれくらいの期間であればデータを利用できなくても許されるかを、データの種類別に示したものです。

表 A-6　復旧までに許される最大ダウンタイム

データの種類	最大ダウンタイム
企業のビジネス・データ	6 時間
企業のリソース・データ	6 時間
プロジェクト・データ	1 日
個人データ	2 日

復旧までに要する時間は、主としてメディアへのアクセスと、データを実際にディスクに復元する作業に費やされます。

- 各種データの保管期間

  341 ページの表 A-7 は、各種データの保管期間を示したものです。データの保管期間は、必要となるバックアップ・メディアの数に直接影響します。

表 A-7　データの保管期間

データの種類	最大データ保管期間
企業のビジネス・データ	5 年
企業のリソース・データ	5 年
プロジェクト・データ	5 年
個人データ	3 か月

- バックアップ・データを格納したメディアの保管および保守の方法

  メディアはコンピュータ室内のテープ・ライブラリに保管します。企業のバックアップ・システムの対象となるデータは、いずれも、週 1 回フル・バックアップを作成し、毎日増分バックアップを作成する必要があります。データは警備会社に保管します。

- バックアップする必要があるデータ量

現時点でバックアップする必要があるデータ量は、342 ページの表 A-8 に示すとおりです。

表 A-8　バックアップする必要があるデータ量

場所	データ量 (GB)
ABC ケープタウン	100
ABC プレトリア	22
ABC ダーバン	16

将来的なデータ量の増加への対応

ABC 社の今後の成長率は年 15 ～ 20% 程度と予測され、バックアップが必要なデータ量もこれに応じて増加していくと考えられます。データ量の増加は、バックアップに要する時間やバックアップに必要なデバイスの数だけでなく、IDB のサイズにも影響を及ぼします。

表 A-9　5 年後にバックアップする必要があるデータ量

場所	データ量 (GB)
ABC ケープタウン	250
ABC プレトリア	55
ABC ダーバン	40

- データのバックアップ頻度

  データはそれぞれの種類ごとに、金曜、土曜、日曜のいずれかに毎週 1 回フル・バックアップを作成します。またレベル 1 増分バックアップは、平日に必ず実行します。ただし、例えばフル・バックアップを金曜日に作成するデータについては、金曜を除く平日と土曜日に、対応するレベル 1 増分バックアップを実行します。

ソリューション案

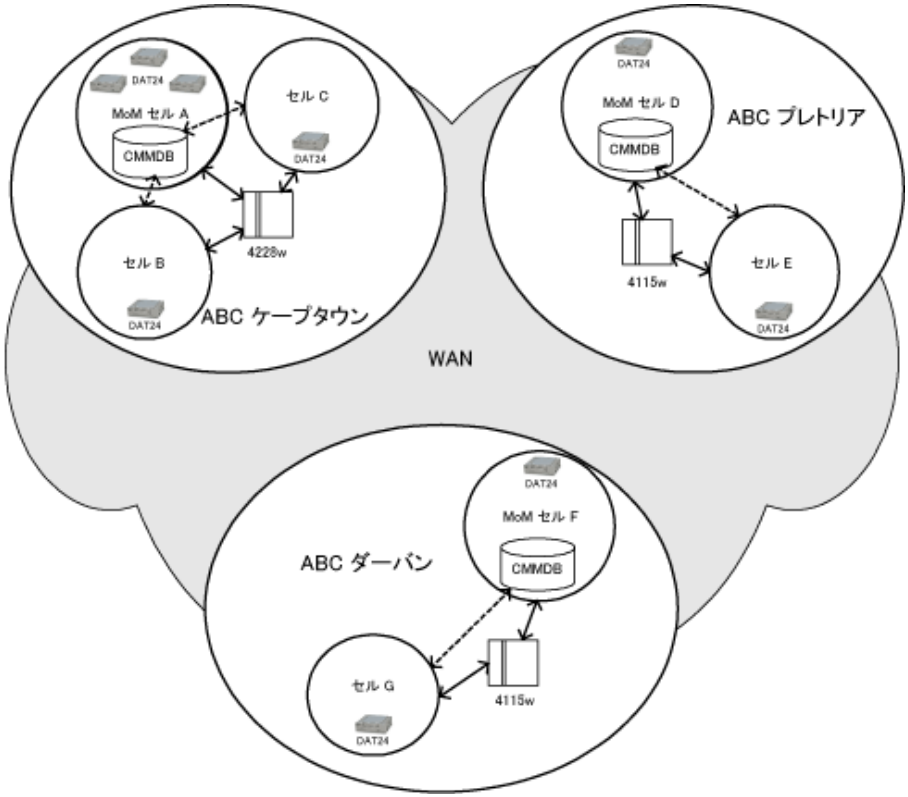
340 ページの「現在のソリューションの問題点」に示した現在のバックアップ・ソリューションの問題点を解決するために、ABC 社ではデータ記憶システムの再設計を検討しています。

ソリューションの概要

ABC ケープタウンの 3 つの部門は、いずれも同一の Manager-of-Managers (MoM) セル内に構成します。さらに ABC ダーバンと ABC プレトリアについても個別の MoM セルを構成し、各 MoM セル内にはそれぞれ 2 つの Data Protector セルを含めます。

セル A を ABC ケープタウン環境の MoM セルとして構成します。同様に、セル D を ABC プレトリア環境の MoM セルとして構成し、セル F を ABC ダーバン環境の MoM セルとして構成します。343 ページの図 A-6 にこの構成を示します。

図 A-6　　ABC 社のバックアップ環境



これらの 7 つのセル内の Cell Manager と MoM Manager は、いずれも Windows システムでなければなりません。メディア集中管理データベース (CMMDB) は各 MoM 環境のいずれか 1 つのセル内にのみ構成し、カタログ・データベースは 7 つのセルのすべてに構成します。メディア集中管理データベースを使うと、同じ MoM 環境に所属するセル間でライブラリを共有できます。

ABC 社の 3 箇所にあるオフィスでは、それぞれ専用のライブラリを使用します。ABC ケープタウン環境では、HP StorageWorks DLT 4228w Library を使用します。また ABC プレトリア環境と ABC ダーバン環境では、HP StorageWorks DLT 4115w Library を使用します。

ABC ケープタウンの MoM 環境に含まれる 3 つのセルには、SAP データベース・サーバがそれぞれ 1 台ずつあります。これらの SAP データベース・サーバでは、1 台の HP StorageWorks DLT 4228w Library を共有します。また Microsoft SQL データベースと Microsoft Exchange データベースは、HP StorageWorks DAT24 オートローダにローカルな形でバックアップされます。

ABC プレトリアの MoM 環境内の 2 つのセルでも、同一のメディア集中管理データベースを共有します。このデータベースはセル D の MoM Manager 上に構成して、2 つのセル間で HP StorageWorks DLT 4115w Library を共有できるようにします。

ABC ダーバンの MoM 環境内の 2 つのセルでも、同一のメディア集中管理データベースを共有します。このデータベースはセル F の MoM Manager 上に構成して、2 つのセル間で HP StorageWorks DLT 4115w Library を共有できるようにします。

以下に、このソリューション案の詳細について説明します。

ソリューション案の詳細

- セルの構成

  各部門を 7 つのセルに分けて構成します。ABC ケープタウンに 3 つ、ABC プレトリアと ABC ダーバンにそれぞれ 2 つずつです。

  #### 7 つのセルに分割する理由

  — ABC 社の各部門は地理的に離れているため、単一のセルで管理するのは困難です。さらに、システム間のネットワーク接続に伴う問題が発生する可能性もあります。構成は部門の数と一致していますが、これはセキュリティの観点からも重要な意味を持っています。各セル内には、それぞれ 30 ～ 50 台のクライアント・システムを含めることが推奨されます。ただしこの数は、各クライアント・システムが所有するファイルやディレクトリの数などの条件に大きく依存します。

次に、3 つの環境をそれぞれ Manager-of-Managers 環境として構成します。MoM を使うと単一のポイントから、効率よく、透過的かつ一元的に複数のセルを管理できます。MoM を構成したら、それぞれの MoM 環境でメディア集中管理データベース (CMMDB) を構成します。

CMMDB を使う理由

— メディア集中管理データベース (CMMDB) を使用すると、同じ MoM 環境内のすべてのセルでデバイスやメディアを共有できるようになります。そのため ABC 社の 3 つの MoM 環境でも、それぞれの環境に所属するすべてのセル内のクライアント・システムで、1 つのライブラリを共有できます。ABC 社の全データを単一の大容量ライブラリに格納するやり方は合理的ではありません。この方法では、バックアップ時に WAN を介して大量のデータを転送しなければなりません。

カタログ・データベースは、7 つのセルのそれぞれに必要です。セル内のシステム構成は、345 ページの表 A-10 に示すとおりです。

表 A-10　ABC 社のセル構成

MoM 環境	セル	Windows サーバ数	Windows クライアント数	UNIX サーバ数	UNIX クライアント数	SAP 数
ABC ケープタウン	A*	3	24	2	7	1
	B	2	11	5	21	1
	C	2	20	4	12	1
ABC プレトリア	D*	4	33			
	E	1	6	5	32	
ABC ダーバン	F*	2	10	4	30	
	G	1	11	2	29	
SAP 数とは、SAP データベース・サーバの数を意味します。						
* は MoM セルを表します。						

これらの 7 つのセル内の Cell Manager と MoM Manager は、いずれも Windows システムでなければなりません。

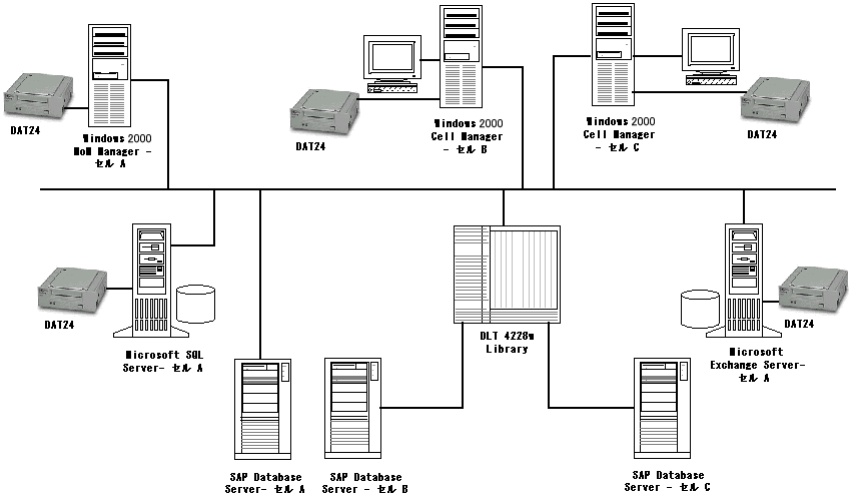
Windows システムを選ぶ理由

— Windows システムでは標準で Unicode 形式がサポートされているため、他のシステムに比べて、ファイル名に使われている各国の文字を正しく取り扱うための構成が容易です。

ABC ケープタウン環境では、セル A を Manager-of-Managers セルとして構成し、残りのセルをこの MoM 環境にインポートします。MoM セル A にメディア集中管理データベースを構成すると、セル B とセル C でも同一ライブラリを共有できるようになります。ABC ケープタウン環境では、1 台の HP StorageWorks DLT 4228w Library を共有します。このライブラリは圧縮形式で 1.1TB のデータを格納できるため、今後 5 年間に予測されるデータ増加率に十分に対応できます。

ABC ケープタウンの 3 つのセルには、それぞれに 1 つの SAP データベース・サーバが必要です。これらの SAP データベース・サーバは、1 台の HP StorageWorks DLT 4228w Library を共有します。また Microsoft SQL データベースと Microsoft Exchange データベースは、既存の HP StorageWorks DAT24 オートローダにローカルな形でバックアップされます。またこの環境内の各セルでは、それぞれに個別のカタログ・データベースが必要です。ケープタウン環境の構成は、346 ページの図 A-7 に示すとおりです。

図 A-7　　ABC ケープタウンのバックアップ環境



ABC プレトリアの MoM 環境内の 2 つのセルでも、メディア集中管理データベースを共有する必要があります。このデータベースは、セル D の MoM Manager 上に構成します。CMMDB を使用すると、2 つのセル間で HP StorageWorks DLT 4115w Library を共有できるようになります。またこの環境内の各セルでは、それぞれに個別のカタログ・データベースが必要です。

同様に ABC ダーバンの MoM 環境内の 2 つのセルでも、メディア集中管理データベースを共有する必要があります。このデータベースは、セル F の MoM Manager 上に構成します。ダーバン環境内の各セルでも、それぞれ個別のカタログ・データベースが必要です。

ABC プレトリア環境および ABC ダーバン環境では、HP StorageWorks DLT 4115w Library を使用します。このライブラリは圧縮形式で 600GB のデータを格納できるため、これらの環境で今後 5 年間に予測されるデータ増加率に十分に対応できます。

IDB サイズの見積もり

セル F 内の IDB の 1 年間のサイズ変化の見積もりには、Internal Database Capacity Planning Tool を使用しています。このツールは次の場所にあります。

— HP-UX および Solaris Cell Manager の場合 :
`/opt/omni/doc/C/IDB_capacity_planning.xls`

— Windows Cell Manager の場合 :
`<Data_Protector_home>¥docs¥IDB_capacity_planning.xls`

348 ページの図 A-8 に示す入力パラメータでは、環境内のファイル数 (2,000,000)、拡張係数 (1.2)、データ保護期間 (260 週間)、カタログ保護期間 (3 週間)、1 週間に行うフル・バックアップの回数 (1 回)、1 週間に行う増分バックアップの回数 (5 回) を指定しています。

図 A-8　　入力パラメータ

Environment description			
	Files:	2	million
	Files per directory:	10	
	Data volume:	16	GB
	Growth factor:	1.20	
	Device performance:	10.00	MB/second
	Medium capacity:	70.00	GB
	Objects:	100	
	Change per incr-bkup	10.00%	
Backup parameters			
	Device concurrency:	2	
	Data segment size:	2,048.00	MB
	Log level:	All	
	Data protection:	260	Weeks
	Catalog protection:	3	Weeks
	Full backups/week:	1	
	Incr backups/week:	5	
Cell Manager parameters			
	Insertion speed:	12	million/hour

348 ページの図 A-9 に結果を示します。データベースは 1 年間で約 667.47MB まで増加すると予測されます。

図 A-9　　結果

Results/calculation			
	Avg. file size:	7.29	KB
	Files/segement:	269,057.37	
	Catalog size:	16.42	MB
	K devices:	2	
	K performance:	85.48173913	GB/hour
	K duration:	0.19	hour
	Protected media:	133.7142857	
Space estimation			
MMDB:		30.00	MB
CDB:	Fnames:	207.00	MB
	Overs:	57.13	MB
	Mpos:	0.74	MB
DCBF:		372.60	MB
SMBF:		5.72	MB
Total:		667.47	MB

Internal Database Capacity Planning Tool を使うと、オンライン・データベース (Oracle、SAP R/3) を使用する環境内での IDB サイズを見積もることもできます。

- ハードウェア

  — ネットワーク

  性能を最大限に引き出すには、同じオフィス内のすべてのシステムを同一 LAN 上に配置する必要があります。それぞれのオフィス内のシステム同士は 100TX ネットワークで接続し、3 つのオフィス内の各セル同士は WAN で接続します。100TX ネットワークは、10MB/s (36GB/h) のデータ転送速度を維持できます。

  — バックアップ・デバイス

  バックアップ・デバイスには、ABC ケープタウン用に HP StorageWorks DLT 4228w Library を 1 台、ABC プレトリアと ABC ダーバン用に HP StorageWorks DLT 4115w Library を 2 台、すべてのセル内の IDB と構成ファイルをバックアップするために HP StorageWorks DAT24 オートローダを 7 台、および ABC ケープタウンの Microsoft SQL データベースと Microsoft Exchange データベースをバックアップするために HP StorageWorks DAT24 オートローダを 2 台使用します。Microsoft Exchange Server と Microsoft SQL Server の現時点でのデータ容量はそれぞれ 15GB と 11GB であり、それ以外のデータ (100GB -15GB - 11GB = 74GB) は、3 台の SAP データベース・サーバにバックアップされます。

HP StorageWorks DLT 4228w Library を使う理由

HP StorageWorks DLT 4228w Library には、2 つの DLT4000 ドライブと 28 個のスロットがあります。このライブラリは圧縮状態で合計 1.1TB の記憶容量を持ち、データを圧縮した状態で最大 6MB/s (2 x 3MB/s)、つまり 21GB/h のデータ転送速度を維持できます。以下の説明ではこの転送速度を前提としています。現時点では、HP StorageWorks DLT 4228w Library にフル・バックアップする必要があるデータの総容量は、単一のフル・バックアップまたは時差実行方式のいずれを使用する場合も、約 74GB になります。増分バックアップのサイズをフル・バックアップの約 5% と見積もると、1 つのバックアップ世代、つまり 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がライブラリに占める容量は、(74+74*5%*5)GB、つまり **92.5GB** になります。5 年後には、この値は約 230GB にまで増加すると予測されます。ABC 社のバックアップ方針では 3 つのバックアップ世代を保管する必要があるため、230*3GB (690GB) のライブラリ領域が必要になります。そのため、1.1TB の記憶容量を持つ HP StorageWorks DLT 4228w Library で十分に対応できます。

ABC ケープタウンのライブラリは、このオフィスの 3 つのセル間で共有されます。また ABC プレトリア環境のライブラリはセル D とセル E で、ABC ダーバン環境のライブラリはセル F とセル G でそれぞれ共有されます。このように構成する場合は、3 つの MoM 環境のそれぞれで、Data Protector メディア集中管理データベースを使用する必要があります。このデータベースはセル A、D、F の MoM Manager 上にそれぞれ構成します。

HP StorageWorks DLT 4115w Library を使う理由

HP StorageWorks DLT 4115w Library には、1 つの DLT4000 ドライブと 15 個のスロットがあります。このライブラリは圧縮状態で合計 600GB の記憶容量を持ち、データを圧縮した状態で 3MB/s (10.5GB/h) のデータ転送速度を維持できます。以下の説明ではこの転送速度を前提としています。現時点では、ABC プレトリアで HP StorageWorks DLT 4115w Library にフル・バックアップする必要があるデータの総容量は、単一のフル・バックアップまたは時差実行方式のいずれを使用する場合も、約 22GB になります。増分バックアップのサイズをフル・バックアップの約 5% と見積もると、1 つのバックアップ世代、つまり 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がライブラリに占める容量は (22+22*5%*5)GB、つまり **27.5GB** になります。5 年後には、この値は約 68.75GB にまで増加すると予測されます。ABC 社のバックアップ方針では 3 つのバックアップ世代を保管する必要があるため、68.75*3GB (206.25GB) のライブラリ領域が必要になります。そのため、600GB の記憶容量を持つ HP StorageWorks DLT 4115w Library で十分に対応できます。

ABC ケープタウンの Microsoft Exchange Server と Microsoft SQL Server、および 3 つの MoM 環境内の 7 つの Cell Manager のバックアップには、HP StorageWorks DAT24 オートローダが使われます。

HP StorageWorks DAT24 オートローダを使う理由

HP StorageWorks DAT24 オートローダには、24GB のデータ・カートリッジが 6 個あります。圧縮状態で合計 144GB の記憶容量を持ち、データを圧縮した状態で最大 2MB/s (7GB/h) のデータ転送速度を維持できます。以下の説明ではこの転送速度を前提としています。現時点では、前述した ABC ケープタウンの Microsoft Exchange Server に接続された HP StorageWorks DAT24 オートローダにバックアップする必要があるデータの総容量は 15GB になります。増分バックアップのサイズをフル・バックアップの約 5% と見積もると、1 つのバックアップ世代、つまり 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のサイズは (15+15*5%*5)GB、つまり **18.75GB** になります。5 年後には、この値は約 47GB にまで増加すると予測されます。ABC 社のバックアップ方針

では 2 つのバックアップ世代を保管する必要があるため、47*2GB (**94GB**) のライブラリ領域が必要になります。そのため、144GB の記憶容量を持つ HP StorageWorks DAT24 オートローダで十分に対応できます。

フル・バックアップに要する時間

ABC ケープタウンの 3 つのセル内にある SAP データベース・サーバには、HP StorageWorks DLT 4228w Library にバックアップする必要があるデータが合計 74GB あります。このライブラリには 2 つのドライブがあり、6MB/s (2 x 3MB/s)、つまり 21GB/h のデータ転送速度を維持できます。そのためこのライブラリにデータをバックアップするには、**最大約 5 時間**かかることになります。5 年後のデータ量は 185GB になり、バックアップ時間は **9 ～ 10 時間**になると予測されるため、5 年後も、許容限度の 12 時間以内に処理を終了できるとわかります。

ABC プレトリアのセル D とセル E では、1 台の HP StorageWorks DLT 4115w Library を共有します。このライブラリには 1 つのドライブがあり、3MB/s、つまり 10.5GB/h のデータ転送速度を維持できます。これらのセルでバックアップする必要があるデータ量は全体で約 22GB あり、約 **2 ～ 3 時間**でバックアップできます。5 年後のデータ量は 55GB になり、バックアップ時間は **5 ～ 7 時間**になると予測されるため、5 年後も、許容限度の 12 時間以内に処理を終了できます。

同様に、ABC ダーバンのセル F とセル G のデータ量は約 16GB あり、**最大約 2 時間**でバックアップできます。5 年後のデータ量は 40GB になり、バックアップ時間は**約 4 時間**になると予測されるため、5 年後も、許容限度の 12 時間以内に処理を終了できます。

ABC プレトリアにある 1.3GB の容量を持つ最大の Data Protector カタログ・データベースは、データベースの整合性の事前チェックを省略した場合は、数分程度でバックアップされます。Data Protector では、デフォルトで、バックアップ前にデータベースの整合性がチェックされます。1.3GB のデータベースをチェックするには 1 時間近くかかるため、事前チェックを行うと、ABC プレトリアの IDB と構成ファイルのバックアップには **2 時間**近くかかることになります。

- メディア・プール

  追跡や制御を容易にするために、個々のメディアはメディア・プールと呼ばれるグループにまとめられます。メディア・プールを使うと多数のメディアを効率よく管理できるため、バックアップ管理者の負担が軽減されます。ここでは、企業の組織構造やシステム・カテゴリに基づいて、以下のメディア・プールを定義します。

表 A-11 ABC 社のメディア・プール

メディア・プール名	場所	説明
CT_SAP_Pool	ケープタウン	SAP データベース・サーバ
CT_SQL_Pool	ケープタウン	Microsoft SQL Server
CT_Exchange_Pool	ケープタウン	Microsoft Exchange Server
CT_DB_Pool	ケープタウン	IDB
P_DLT_Pool	プレトリア	HP StorageWorks DLT 4115w Library
P_DAT_Pool	プレトリア	HP StorageWorks DAT24 オートローダ
P_DB_Pool	プレトリア	IDB
D_DLT_Pool	ダーバン	HP StorageWorks DLT 4115w Library
D_DAT_Pool	ダーバン	HP StorageWorks DAT24 オートローダ
D_DB_Pool	ダーバン	IDB

- バックアップ仕様

  バックアップ仕様は以下のように構成します。

  — DB_A...G

  7 つの IDB と構成ファイル用のバックアップ仕様です。このバックアップ仕様では、例えば、週 1 回フル・バックアップが Data Protector によって実行されるようにスケジュールを設定し、さらに日曜を除く毎日 03.00 にレベル 1 増分バックアップが実行されるように設定します。

レベル 1 増分バックアップを使う理由

最新のデータを復元する場合に、2 つのメディア・セット、つまり最新のフル・バックアップと、復元時点よりも前に作成された最新のレベル 1 増分バックアップの 2 つのみになります。そのため復元処理が簡単になり、処理時間も大幅に短縮されます。差分バックアップを使用する場合は、より多くのメディア・セットが必要になるため、復元処理が複雑になり処理時間も長くなります。

IDB と構成ファイルについては、セキュリティ上の理由により、2 つのコピーを作成します。

— SAP_A...C

セル A、B、C 内の SAP データベース・サーバ用のバックアップ仕様です。ネットワーク負荷、デバイス負荷、およびバックアップ可能な時間枠に関する問題を回避するために、353 ページの表 A-12 に示す時差実行方式を使用します。

表 A-12 ABC ケープタウンにおける時差実行方式

	月	火	水	木	金	土	日
セル A	増分 1	増分 1	増分 1	増分 1	フル	増分 1	
セル B	増分 1	増分 1	増分 1	増分 1	増分 1	フル	
セル C	増分 1	増分 1	増分 1	増分 1	増分 1		フル

— SERVERS_A...G

障害復旧に備えるための、企業のサーバ用のバックアップ仕様です。新しいサーバをインストールしたとき、または既存のサーバをアップグレードしたときは、このバックアップ仕様も更新しなければなりません。このバックアップ仕様では、例えば、354 ページの表 A-13 に示すような形で Data Protector によってフル・バックアップが実行されるようにスケジュールを設定し、さらに平日には毎日レベル 1 増分バックアップが実行されるように設定します。

— USERS_D...G

ユーザー・データ用のバックアップ仕様です。これは、ABC プレトリアおよび ABC ダーバンで作成される主要なバックアップ・データです。このバックアップ仕様では、354 ページの表 A-13 に示すような形で Data Protector によってフル・バックアップが実行されるようにスケジュールを設定します。例えば、毎週金曜日にフル・バックアップが、また平日には毎日レベル 1 増分バックアップが実行されるように設定します。ただし、フル・バックアップを金曜日に実行する場合、金曜を除く平日と土曜日に、対応するレベル 1 増分バックアップを実行します。

354 ページの表 A-13 は、バックアップ仕様の構成の詳細を示したものです。

表 A-13　ABC 社のバックアップ仕様の構成

仕様名	セル	説明	バックアップ曜日	バックアップ時刻
DB_A	A	IDB	土曜日	03:00
DB_B	B	IDB	土曜日	03:00
DB_C	C	IDB	土曜日	03:00
SQL_A	A	Microsoft SQL データベース	金曜日	20:00
EXCHANGE_A	A	Microsoft Exchange データベース	金曜日	20:00
SAP_A	A	SAP データベース・サーバ	金曜日	20:00
SAP_B	B	SAP データベース・サーバ	土曜日	20:00
SAP_C	C	SAP データベース・サーバ	日曜日	20:00
SERVERS_A	A	サーバ	金曜日	23:00
SERVERS_B	B	サーバ	土曜日	23:00
SERVERS_C	C	サーバ	日曜日	23:00
DB_D	D	IDB	土曜日	03:00
DB_E	E	IDB	土曜日	03:00
SERVERS_D	D	サーバ	金曜日	23:00
SERVERS_E	E	サーバ	土曜日	23:00
USERS_D	D	ユーザー・データ	土曜日	0:00
USERS_E	E	ユーザー・データ	日曜日	0:00
DB_F	F	IDB	土曜日	03:00

表 A-13 ABC 社のバックアップ仕様の構成 (続き)

仕様名	セル	説明	バックアップ曜日	バックアップ時刻
DB_G	G	IDB	土曜日	03:00
SERVERS_F	F	IDB	金曜日	23:00
SERVERS_G	G	サーバ	土曜日	23:00
USERS_F	F	ユーザー・データ	土曜日	0:00
USERS_G	G	ユーザー・データ	日曜日	0:00

バックアップ・オプション

デフォルトの Data Protector バックアップ・オプションを使用します。以下のオプションを以下に示すように設定します。

— [ディレクトリのレベルで記録 (Log Directories)]

このファイルシステム・バックアップ・オプションを使うと、ディレクトリに関する詳細情報のみがカタログ・データベースに保存されます。このオプションを選択した場合は、復元時に検索機能を使用できず、ディレクトリのブラウズのみが可能になります。セル D 内の 500,000 個以上のファイルを持つ 2 台のサーバをバックアップするときは、このオプションを使用します。このオプションを使用しないと、Data Protector カタログ・データベースのサイズが非常に大きくなってしまいます。

— [保護 (Protection)]

バックアップ後 3 週間は、データに簡単にアクセスできなければなりません。フル・バックアップは週 1 回しか実行しないため、カタログ保護は 27 日 (3 週間 *7 日 +6 日 =27 日) と設定します。

Exchange_A 以外のバックアップ仕様については、データ保護期間を 5 年と設定します。Exchange_A は個人メール用のバックアップ仕様です。このバックアップ仕様については、データ保護期間を 3 か月と設定します。

— [同時処理数 (Concurrency)]

このオプションは 5 に設定して、最大 5 つの Disk Agent がライブラリに同時にデータを書き込めるようにします。これにより、バックアップの性能が向上します。

— [メディア・プール (Media Pool)]

バックアップに使う適切なメディア・プールとメディアを選択します。

- レポートと通知

  電子メール通知をセットアップしておき、すべてのバックアップ仕様に関するマウント要求、データベース容量の不足、デバイス・エラー、セッション終了イベントなどがバックアップ管理者に送信されるようにします。電子メールまたはブロードキャスト通知を使って、エンド・ユーザーに自分のシステムのバックアップが成功したかどうかを知らせることも可能です。

  また、すべてのユーザーがバックアップ状態を簡単にチェックできるように、自社のホーム・ページ上にクライアント・バックアップ情報を以下に示すようにセットアップします。

  1. [クライアントのバックアップをレポート (Client Backup Report)] を使って、各クライアントごとにレポート・グループを構成します。レポートは HTML 形式でログ・ファイルに記録してください。
  2. レポート・グループのスケジュールを設定します。
  3. ログ・ファイルを自社のホーム・ページにリンクします。

- ボールティング

  ボールティングとは、メディアを安全な場所に一定期間保管するプロセスを指します。

  メディアは毎週 1 回保管場所 (ボールト) に移送され、HP StorageWorks DLT 4228w Library、HP StorageWorks DLT 4115w Library、および HP StorageWorks DAT24 オートローダには新しいメディアがセットされます。メディアを実際にボールトに移送する作業を除き、すべての処理はソフトウェアにより実行されます。例えば、データベースの照会も内部的に自動実行されるため、排出するメディアを管理者が自分で探す必要はありません。

  ボールトに移送したメディアについても、引き続き保管場所を追跡する必要があります。この情報は、ボールト内のメディアからデータを復元するような場合に重要になります。Data Protector では、ボールティングに関する以下のタスクを実行できます。

  — 指定された場所に保管されており、指定された日時にデータ保護期間が切れるバックアップ・メディアの一覧レポートを生成できます。

  — 指定された期間内に作成されたバックアップ・メディアの一覧レポートを生成できます。

  — 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の一覧を表示できます。

  — 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。

  — なんらかの基準に基づいて (保護期間が切れたメディアなど)、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。

- 復元

  — 照会による復元

  照会による復元要求は、管理者に送られます。要求されたファイルが 3 週間以内にバックアップされている場合は、管理者は復元タスクの [照会による復元 (Restore by Query)] を使って、なんらかの基準に基づいて復元するファイルやディレクトリを選択できます。次に管理者は、ディスク上のファイルやディレクトリをメディアに保管されているバージョンで上書きするために、[上書き (Overwrite)] オプションを選択します。

  — ファイルシステム全体の復元

  ファイルシステム全体の復元要求も、管理者に送られます。要求されたファイルが 3 週間以内にバックアップされている場合は、管理者は復元するオブジェクトを選択できます。ファイルシステム全体の復元では [復元先を指定して復元 (Restore Into)] オプションが使われます。

  [復元先を指定して復元 (Restore Into)] オプションを選択すると、オブジェクトは正確なディレクトリ構造を保ったままで選択したディレクトリに復元されます。Windows または UNIX のユーティリティを使うと、復元したオブジェクトとバックアップ・オブジェクトを比較できます。

  — ボールトからの復元

  ボールトに保管されている、例えば 3 年前のデータを復元する場合は、まず要求を管理者に送ります。これを受けて管理者は以下の処理を実行します。

  1. 復元に必要なメディアを特定します。
  2. メディアをボールトから搬入し、HP StorageWorks DLT 4228w Library、HP StorageWorks DLT 4115w Library、またはその他のデバイスに挿入してスキャンします。
  3. そのメディアが Data Protector のカタログ・データベース内になければ、[メディアからリスト (List From Media)] オプションを使って復元するオブジェクトを選択します。
  4. 復元処理を実行します。

B その他の情報

本章の内容

この付録では、バックアップ世代、自動メディア・コピー (Automated Media Copy) の例、国際化に関する情報など、Data Protector の概念に関する追加情報について説明します。

バックアップ世代

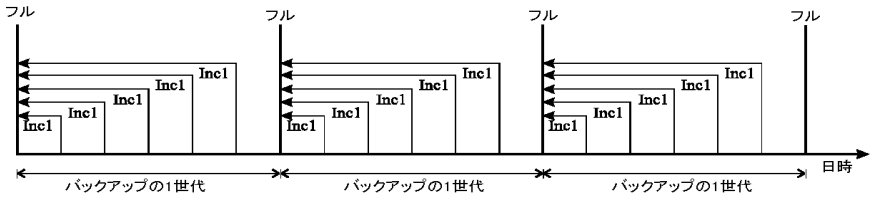
Data Protector では、日付 / 時刻ベースの保護モデルが採用されています。定期的にバックアップを行っている場合は、世代ベースのバックアップ・モデルと、この日時ベースのバックアップ・モデルを簡単に対応付けることができます。

バックアップ世代とは

361 ページの図 B-1 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。ポイント・イン・タイム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)。

図 B-1　　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。

例えば、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。詳細は、136 ページの「メディア交換方針の実装」を参照してください。

自動メディア・コピーの例

バックアップが終了したら、自動メディア・コピー (Automated Media Copy) 機能を使用してメディアをコピーし、元のメディアまたはそのコピーを外部の保管場所に移すこともできます。メディア・コピー機能はデバイスの空き状況に応じて、バックアップ後に自動実行することも、スケジュール形式で実行することも可能です。

ただし以下の点に注意してください。

- 最初にすべてのバックアップを実行してからメディアをコピーすることをお勧めします。
- メディアのコピー中は、コピー元のメディアを復元に使用できません。
- メディア全体のコピーのみ可能であり、特定オブジェクトだけをコピーすることはできません。
- コピーが終了したら、元のメディアとそのコピーには追加不可能 (Non Appendable) マークが付加されます。このマークが付加されたメディアには新しいバックアップ・データを追加できなくなります。
- メディア・コピーをスケジュール設定する場合は、設定した時刻に必要なデバイスおよびメディアが使用可能でなければなりません。使用できなければコピー処理は中止されます。

例 1: ファイルシステム・バックアップの自動メディア・コピー

ここで取り上げる企業では 2 つのセルを持つ MoM 環境を所有しており、各セル内にはそれぞれ 150 台のコンピュータ・システム (サーバおよびワークステーション) が含まれています。各システムの平均データ量は 10GB であるため、バックアップが必要な総データ量は 3000GB になります。

これらのデータについて毎日 1 回 Incr1 バックアップを実行し、週に 1 回フル・バックアップを実行し、さらに長期保存目的で月に 1 回フル・バックアップを実行するものとします。バックアップは営業時間外に実行しなければならないため、開始時刻は午後 5 時以降でなければならず、翌日の午前 8 時までに終了していなければなりません。また週末にも実行可能です。

さらにバックアップ・メディアのコピーも作成します。このコピーは復元時に使用できるように社内に保管しておき、また安全性を考慮して元のバックアップ・メディアは外部の保管場所に移送するものとします。メディアのコピーはバックアップの終了後に実行する必要があります。この作業には自動メディア・コピー機能を使用します。

作業には 6 台の LTO ドライブを搭載した HP StorageWorks 6/60 Tape Library および LTO Ultrium 1 メディアを使用します。これまでの経験から判断して、データ転送速度は 80GB/h、各メディアの平均容量は 153GB になると予測されます。

メディア・コピーの終了後は、コピー元メディアとコピー先メディアの両方が追加不可能 (Non Appendable) になります。この点を考えると、バックアップに使用するメディアの数は最小限に抑えることが望まれます。空のメディアを使って作業を開始し、各メディアの最大容量まで使い切るようにしてください。このためには各バックアップ仕様に 1 つのデバイスのみを割り当てるようにします。こうしておくと、現在のメディアが一杯になってはじめて新しいメディアが使用されます。ただし、複数のメディアに書き込む場合に比べてバックアップ時間は長くなる点に注意してください。

ここでは 4 つのバックアップ仕様を作成することにします。メディア・スペースを節約するため、使用するメディアの数が最小限で済むような形で、データを複数のバックアップ仕様に分割します。それぞれのバックアップでは 1 つのデバイスしか使用されません。

バックアップが終了したら自動メディア・コピーが実行されます。この処理には空いているすべてのデバイスを使用できます。つまりコピー元メディア用に 3 つのデバイスを、コピー先メディア用に 3 つのデバイスをそれぞれ使用します。

メディアのコピーには、バックアップとほぼ同じ時間がかかると予想されます。

Incr1 バックアップ

バックアップの構成

Incr1 バックアップは月曜から木曜までの毎日午後 6 時に実行するようスケジュール設定します。データ保護期間は 4 週間に設定します。毎日のデータ変更量は全体の 30% であるため、バックアップが必要なデータ量は 900GB になると予測されます。このデータを次のように複数のバックアップ仕様に分割します。

- BackupSpec1 (ドライブ 1) -300 GB
- BackupSpec2 (ドライブ 2) -300 GB
- BackupSpec3 (ドライブ 3) -150 GB
- BackupSpec4 (ドライブ 4) -150 GB

BackupSpec1 と BackupSpec2 にはそれぞれ 2 つのメディアが必要で、バックアップには約 4 時間かかります。BackupSpec3 と BackupSpec4 にはそれぞれ 1 つのメディアが必要で、バックアップには約 2 時間かかります。

自動メディア・コピーの構成

バックアップが終了したら、そのバックアップに対応する自動メディア・コピーが開始されます。コピーが必要なメディアの数は 6 個で、この処理にはライブラリ内のすべてのドライブを、ドライブが空き次第使用できます。

BackupSpec1 および BackupSpec2 で使用するメディアのコピーには、バックアップ後メディア・コピー機能を使用できます。これは 2 つのドライブ (ドライブ 5 と 6) が空いているため、デバイスが使用可能かどうかを考慮する必要がないためです。

BackupSpec1 用のバックアップ後メディア・コピーを構成します。コピー元デバイスにはドライブ 1 を、コピー先デバイスにはドライブ 6 を指定してください。データ保護は元のデータと同様に設定し、メディアの位置も指定します (Shelf 1 など)。

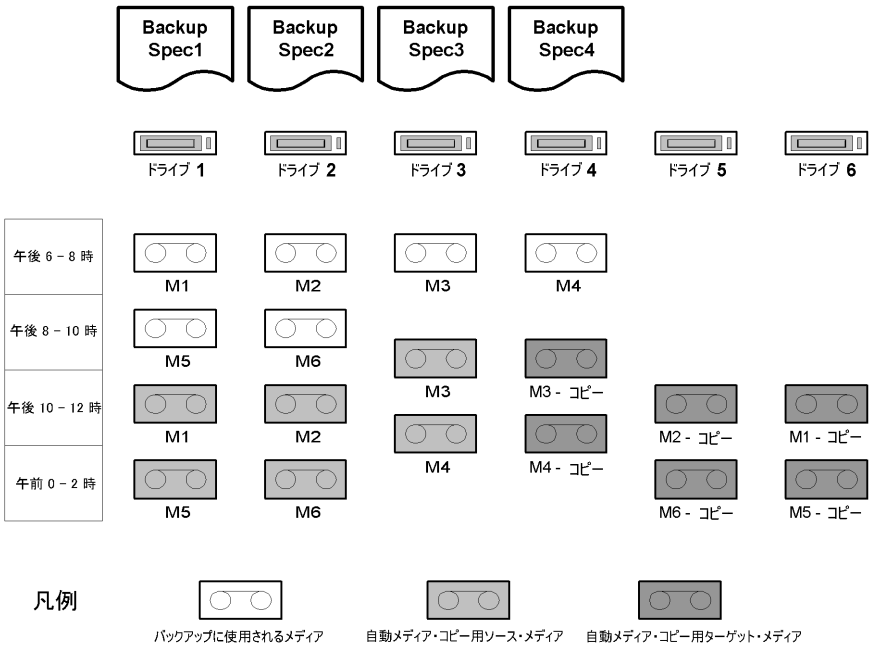
同様に、BackupSpec2 用のバックアップ後メディア・コピーを構成します。コピー元デバイスにはドライブ 2 を、コピー先デバイスにはドライブ 5 を指定してください。データ保護は元のデータと同様に設定し、メディアの位置も指定します。

BackupSpec3 と BackupSpec4 で使用するメディアのコピーには、スケジュール形式のメディア・コピー機能を使用します。これは、コピー処理にドライブ 3 とドライブ 4 を使用するため、両方のバックアップが終了するまで待つ必要があるためです。メディア・コピーがスケジュール設定されている時刻にこれらのデバイスが使用不能であると、処理は失敗する点に注意してください。そのため、バックアップと同じデバイスを使用してスケジュール形式の自動メディア・コピーを実行する場合は、バックアップの終了予定時刻よりも少し後の時間を指定するようにしてください。

ここではバックアップ終了予定時刻の 1 時間後にメディア・コピーが開始されるようにスケジュールを設定します。メディア・コピーの対象には BackupSpec3 と BackupSpec4 を選択し、コピー元デバイスにはドライブ 3 を、コピー先デバイスにはドライブ 4 を指定します。データ保護は元のデータと同様に設定し、メディアの位置も指定します。

366 ページの図 B-2 は、Incr1 バックアップと自動メディア・コピーを図で表したものです。

図 B-2　　Incr1 バックアップと自動メディア・コピー



フル・バックアップ

バックアップの構成

週 1 回のフル・バックアップは金曜日の午後 6 時に開始するようスケジュール設定します。データ保護期間は 8 週間に設定します。バックアップが必要なデータ量は 3000GB です。このデータを次のように複数のバックアップ仕様に分割します。

- BackupSpec1 (ドライブ 1) -1000 GB
- BackupSpec2 (ドライブ 2) -1000 GB
- BackupSpec3 (ドライブ 3) -500 GB
- BackupSpec4 (ドライブ 4) -500 GB

BackupSpec1 と BackupSpec2 にはそれぞれ 7 つのメディアが必要で、BackupSpec3 と BackupSpec4 にはそれぞれ 4 つのメディアが必要です。バックアップには約 14 時間かかります。

自動メディア・コピーの構成

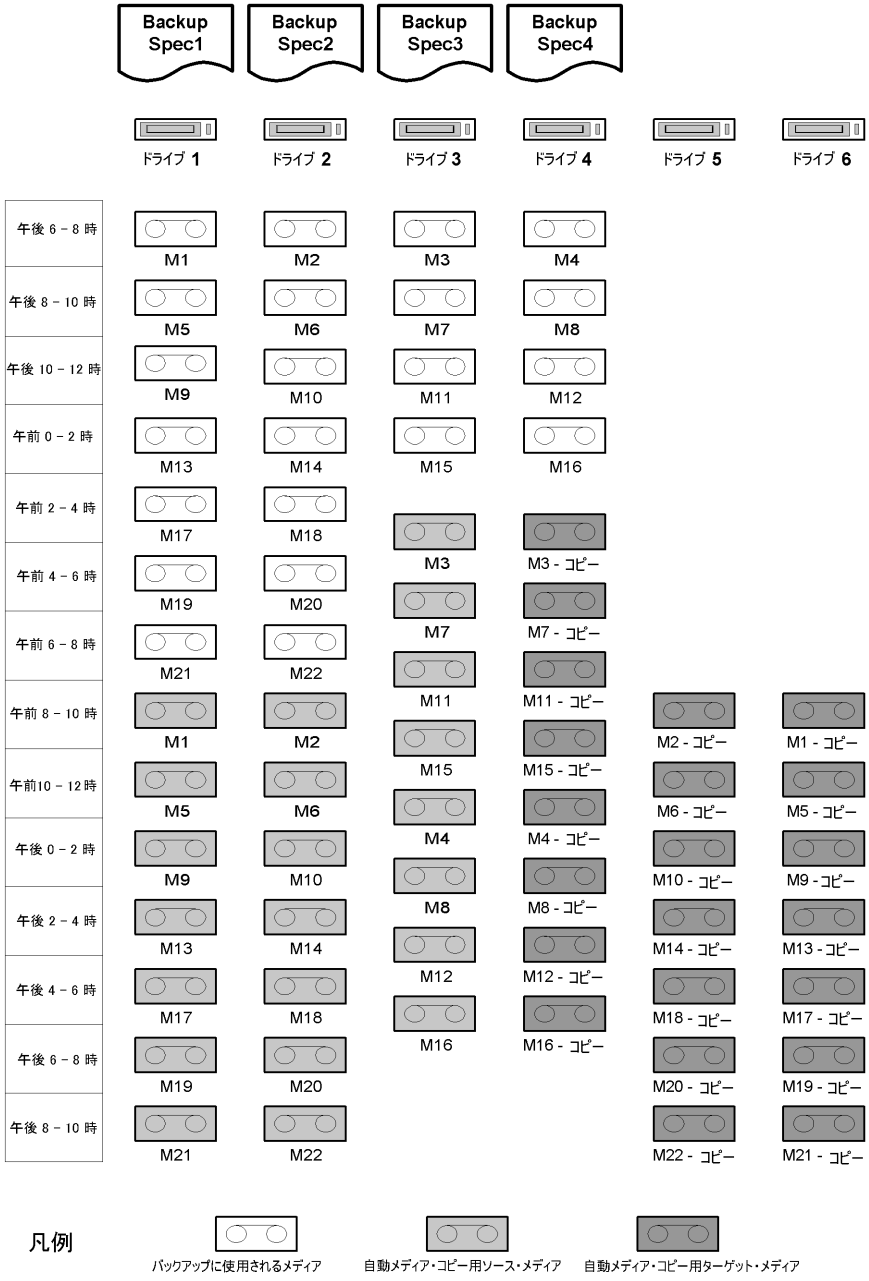
バックアップが終了したら、そのバックアップに対応する自動メディア・コピーが開始されます。コピーが必要なメディアの数は 22 個で、すべてのデバイスが空き次第使用されます。

ここでも、BackupSpec1 と BackupSpec2 で使用したメディアのコピーにはバックアップ後メディア・コピーを使用し、BackupSpec3 と BackupSpec4 で使用したメディアのコピーにはスケジュール形式のメディア・コピーを使用するよう構成します。

デバイスおよびデータ保護は、Incr1 バックアップのコピー時と同様に設定します。スケジュール形式のメディア・コピーは、バックアップ終了予定時刻の 1 時間後に開始されます。

368 ページの図 B-3 は、フル・バックアップと自動メディア・コピーを図で表したものです。

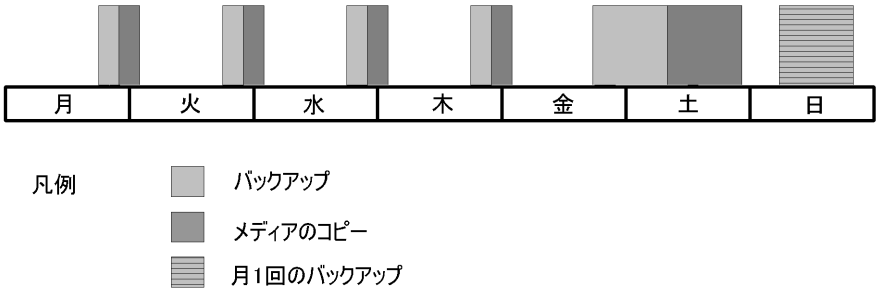
図 B-3　フル・バックアップと自動メディア・コピー



月 1 回のフル・バックアップは日曜日の午前 6 時に開始するようスケジュール設定します。このバックアップは長期保存が目的であるため、通常コピーは作成しません。

369 ページの図 B-4 はデバイス使用率が高い時間帯の概要を示したものです。このグラフは使用率の概要を示したものであり、一部のバックアップ・セッションおよびコピー・セッションの部分的な重複は無視しています。

図 B-4　バックアップ・セッションおよび自動メディア・コピー・セッションの概要



例 2: Oralce データベース・バックアップの自動メディア・コピー

ここで取り上げる企業では、500GB のサイズの Oracle データベースを使用しています。このデータベースは、毎日のフル・バックアップが必要です。バックアップは営業時間外に実行しなければならないため、開始時刻は午後 5 時以降でなければならず、翌日の午前 8 時までに終了していなければなりません。また週末にも実行可能です。

バックアップ・メディアのコピーには自動メディア・コピー機能を使用し、作成したコピーは復元時に使用できるように社内に保管しておきます。また安全性を考慮して元のバックアップ・メディアは外部の保管場所に移送します。メディアのコピーは、バックアップ終了後に実行しなければなりません。この作業にはバックアップ後メディア・コピー機能を使用します。

作業には 10 台の LTO ドライブを搭載した HP StorageWorks 10/700 Tape Library および LTO Ultrium 1 メディアを使用します。これまでの経験から判断して、データ転送速度は 80GB/h、各メディアの平均容量は 153GB になると予測されます。

メディア・コピーが終了したらバックアップに使われたメディアとそのコピーは追加不可能 (Non Appendable) になるため、テープ・スペースは最大容量まで使い切ることが望まれます。その一方、バックアップはできるだけ短時間で終了する必要があります。ここでは 4 台のデバイスを使用してバックアップを実行します。空のメディアを使って作業を開始し、各メディアの最大容量まで使い切るようにしてください。

バックアップが終了したら自動メディア・コピーが開始されます。コピーが必要なメディアの数は 4 個であるため、処理には 8 台のデバイスが必要です。つまりコピー元メディア用に 4 つのデバイスを、コピー先メディア用に 4 つのデバイスをそれぞれ使用します。

メディアのコピーには、バックアップとほぼ同じ時間がかかると予想されます。

フル・バックアップ

バックアップの構成

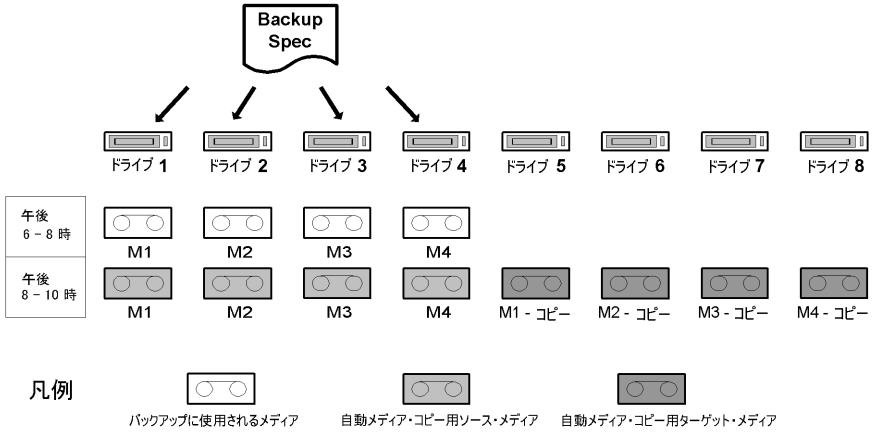
毎日のフル・バックアップは月曜から金曜までの毎日午後 6 時に実行するようスケジュール設定します。データ保護期間は 4 週間に設定します。バックアップが必要なデータ量は 500GB です。処理にはドライブ 1、ドライブ 2、ドライブ 3、ドライブ 4 を使用します。このバックアップには 4 つのメディアが必要で、処理には約 2 時間かかります。

自動メディア・コピーの構成

ここでは十分な数のデバイスを使用できるため、バックアップ後メディア・コピー機能を使用します。コピー元デバイスにはドライブ 1、2、3、4 を、コピー先デバイスにはドライブ 5、6、7、8 を指定します。データ保護は元のデータと同様に設定し、メディアの位置も指定します。

371 ページの図 B-5 は、データベースのフル・バックアップと自動メディア・コピーを図で表したものです。

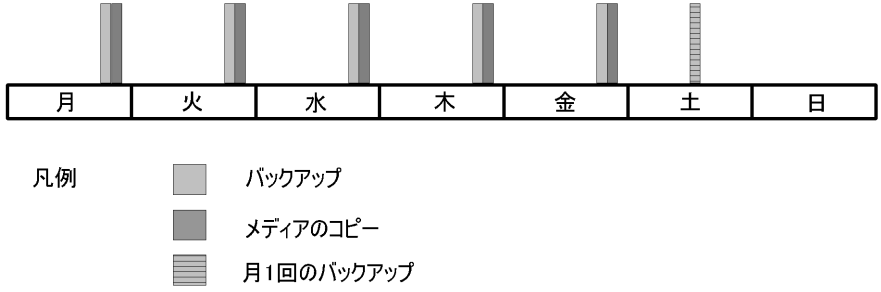
図 B-5　　データベースのフル・バックアップと自動メディア・コピー



月 1 回のフル・バックアップは土曜日の午後 12 時に開始するようスケジュール設定します。このバックアップは長期保存が目的であるため、通常コピーは作成しません。

371 ページの図 B-6 はデバイス使用率が高い時間帯の概要を示したものです。

図 B-6　　バックアップ・セッションおよび自動メディア・コピー・セッションの概要



国際化

国際化とはソフトウェア製品の設計および実装方法で、これにより、製品をユーザーの母国語を使ってユーザーのロケール設定 (通貨、時刻、日付、数字、その他の形式) に合わせて動作させることができます。国際化によって、ユーザーの母国語によるテキスト・データの入力、表示が可能になります。一方、ソフトウェアの開発技法としての国際化とは、単一のソース・コードを持つ、単一のバイナリ・ソフトウェアをもって、複数の言語環境への個別ローカライズを可能とすることです。言語ごとのローカライズ作業は、バイナリとは別個のテキスト部分を翻訳することにより行います。したがって、国際化はローカライズを可能にするプロセスと言えます。Data Protector は国際化対応製品で、複数の言語のユーザー・インタフェースを提供しています。

ローカライズ

ローカライズとは、製品またはサービスを特定の言語や文化に適応させるプロセスです。このプロセスは、ローカライズ済みの画面やオンライン・ヘルプ、エラー・メッセージ、マニュアルなどの提供に関することです。

Data Protector では実際のメッセージ文字列を送信する代わりに、文字列 ID をエージェントから Cell Manager へ送信します。Cell Manager によってその文字列は GUI に転送され、メッセージが適切な言語形式で表示されます。ファイル名やディレクトリ名はインデックスにより表示されるわけでないことに注意してください。ファイル名やディレクトリ名はテキスト文字列として転送され、GUI にテキスト文字列として表示されます。この方法については 372 ページの「ファイル名の取り扱い」の項で説明します。

Data Protector はさまざまな言語にローカライズされています。ローカライズ対応言語に関する詳細は、『*HP OpenView Storage Data Protector ソフトウェア リリース ノート*』を参照いただくか、製品の購入元または最寄りの当社営業所にお問い合わせください。

ファイル名の取り扱い

異機種環境 (セル内に複数の異なるオペレーティング・システムが存在し、それぞれロケール設定が異なっている環境) でのファイル名の取り扱いはかなりの難題です。Data Protector では、ファイル名は、そのファイル名が作成されたときにシステム上で有効となっていた個別のロケール設定 (言語、地域、キャラクタセットなど) に基づいて取り扱われます。そのため、あるロケール設定の下でバックアップしたファイルを、別のロケール設定の下で表示または復元するには、ファイル名を正しく表示するための特殊なセットアップが必要になります。

背景

各種のプラットフォームを提供するベンダー各社はサポートする言語セットを独自に選択してきており、キャラクタセット表記や文字のエンコード規格 (ISO 8859-1、Shift-JIS、EUC、Code Page 932、UNICODE など) の採用も各社ごとに行われています。これらのエンコード規格は互いに衝突する可能性があります。例えば 2 つのエンコード規格で、同じ値がそれぞれ*異*なる文字に割り当てられていたり、異なる値が*同じ*文字に割り当てられていたりするケースが考えられます。いったん作成されたファイル名について、使用されたコード・セットを知る方法はありません。そのため異なるエンコード規格が使われているシステム間でファイル名を受け渡した場合、ファイル名が GUI 上に正しく表示されない可能性があります。

異種プラットフォーム間でデータを受け渡しても、すべてのプラットフォームで同じキャラクタセットが使われているか、すべての国の文字に対応している UNICODE の実装 (Windows 上では UTF-16、その他のプラットフォーム上では UTF-xx) が使われている場合には、問題は起こりません。

残念ながら、UNIX システム上では UNICODE の実装 (UTF-xx) はまだ標準ではサポートされていません。アプリケーションのコンポーネントは、Windows XP Professional、Windows 2000、HP-UX、Solaris、AIX など、プラットフォームが異なるさまざまなシステム上に配布されている可能性があります。こうした各種プラットフォーム上のデータについてもバックアップや復元が必要です。言語やキャラクタセットに対する業界標準の欠如を、Data Protector で完全に補うことはできませんが、ユーザーへの影響をできる限り少なくすることは可能です。

例

異機種環境の場合、構成によってはファイル名を GUI に正常に表示できないことがあります。例えば、Data Protector では、Disk Agent を実行している HP-UX 上のファイルをバックアップして Windows 上の Data Protector GUI で表示することができますが、このとき、両方のプラットフォームで同一のコード・セットが使用されていなければ、ファイル名を正常に表示できないことがあります。これは、種類が異なるキャラクタセットでは、ある 1 つの値がお互いに異なる意味を持っており、別の文字として表示される可能性があるためです。

UNIX 上での非互換例

Data Protector がインストールされていない Solaris システムの同一ファイルシステム上で、3 人のユーザーがそれぞれ ASCII 以外の異なるキャラクタセットを使用してファイルを作成したとします。これらのユーザーが自分の作成したファイル、および他のユーザーが作成したファイルを `ls` コマンドで表示した場合、以下のことが起こります。

- 自分の作成したファイル名は正常に表示される。
- 他のユーザーが作成したファイル名は正常に表示されない。これらのファイル名は、別のシステムではさらに違う形式で表示される場合があります。

正常に表示されなかったファイル名は、ls コマンドを実行するときに使用されたコード・セットとは異なるコード・セットで作成されています。また、これらのファイル名には、ファイル作成時に使用されたコード・セットを示す「タグ」が付与されていません。この例のような現象は、固有のファイルシステム・ビューア (ターミナル・ウィンドウの ls など) を使用しているシステムで起こります。

バックアップ時のファイル名の取り扱い

Data Protector では Disk Agent (バックアップ対象の各クライアント上で実行) を使用してファイル名を読み取り、元のコピーをメディアに保存します。バックアップの log filename オプションが選択されている場合は、ファイル名は「内部」コード・セットに変換され、IDB に記録されます。

ファイル名のブラウズ

Data Protector では GUI を使用して、復元するファイルを選択できます。この場合、GUI を実行しているシステム上で、IDB に記録されているファイル名を閲覧することになります。Data Protector では、GUI に表示されるすべてのファイル名についてエンコード方式が選択できるようになっており、ファイル名内の各文字は、選択した文字エンコード方式に従って表示されます。

ファイル名を正しく表示するためには、ファイルが作成されたシステム上で設定されていた文字エンコード方式を選択する必要があります。エンコード方式が異なっていると、Data Protector GUI 内にファイル名が正しく表示されません。

バックアップが作成されたプラットフォームと同じプラットフォーム上にファイルを復元すると、正しい名前で復元されます。

各種の構成におけるファイル名のブラウズに関する制約事項については、オンライン・ヘルプで「**国際化**」をキーワードに指定して確認してください。

復元時のファイル名の取り扱い

通常、ファイルは、バックアップに使用したプラットフォーム上に復元します。復元プロセスは、次のようになります。

- GUI 上で復元するファイルを選択します。
- 指定したデータが Data Protector によりテープ内で検索されて、データが復元されます。
- 元のファイル名 (テープ内に保存されていたオリジナル・コピー) が復元されます。

用語集

ACSLS
(StorageTek 固有の用語)
Automated Cartridge System Library Server の略語。ACS (Automated Cartridge System: 自動カートリッジ システム) を管理するソフトウェア。

Active Directory
(Windows 固有の用語)
Windows ネットワークで使用されるディレクトリ サービス。ネットワーク上のリソースに関する情報を格納し、ユーザーやアプリケーションからアクセスできるように維持します。このディレクトリ サービスでは、サービスが実際に稼動している物理システムの違いに関係なく、リソースに対する名前や説明の付加、検索、アクセス、および管理を一貫した方法で実行できます。

AML
(EMASS/GRAU 固有の用語)
Automated Mixed-Media library (自動混合メディア ライブラリ) の略。

ASR セット
フロッピー ディスク上に保存されたファイルのコレクション。交換用ディスクの適切な再構成 (ディスク パーティション化と論理ボリュームの構成) およびフル クライアント バックアップでバックアップされた元のシステム構成とユーザー データの自動復旧に必要となります。
これらのファイルは、バックアップ メディア上に保存されると共に、Cell Manager 上の *<Data_Protector_home>*¥Config¥Server¥dr¥asr ディレクトリ (Windows 用 Cell Manager の場合) または /etc/opt/omni/server/dr/asr/ ディレクトリ (UNIX 用 Cell Manager の場合) に保存されます。ASR アーカイブ ファイルは、障害発生後に複数のフロッピー ディスクに展開されます。32 ビット版の Windows XP/.NET では 3 枚のフロッピー ディスクに展開され、64 ビット版の Windows XP/.NET の場合は 4 枚のフロッピー ディスクに展開されます。これらのフロッピー ディスクは、ASR の実行時に必要となります。

BACKINT
(SAP R/3 固有の用語)
SAP R/3 バックアップ プログラムが、オープン インタフェースへの呼び出しを通じて Data Protector backint インタフェース ソフトウェアを呼び出し、Data Protector ソフトウェアと通信できるようにします。バックアップ時および復元時には、SAP R/3 プログラムが Data Protector backint インタフェースを通じてコマンドを発行します。

BC
(EMC Symmetrix 固有の用語)
Business Continuance の略。BC は、EMC Symmetrix 標準デバイスのインスタント コピーに対するアクセスおよび管理を可能にするプロセスです。
BCV *も参照。*

BC
(HP StorageWorks Disk Array XP 固有の用語)
Business Copy XP の略。BC を使うと、HP StorageWorks Disk Array XP LDEV の内部コピーをデータ バックアップやデータ複製などの目的で維持できます。これらのコピー (セカンダリ ボリュームまたは S-VOL) は、プライマリ ボリューム (P-VOL) から分離して、バックアップや開発などの用途に応じた別のシステムに接続することができます。バックアップ目的の場合、P-VOL をアプリケーション システムに接続し、S-VOL ミラー セットのいずれかをバックアップ システムに接続する必要があります。
HP StorageWorks Disk Array XP LDEV、

CA、**Main Control Unit**、**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**も*参照。*

BC Process

(EMC Symmetrix 固有の用語)
保護されたストレージ環境のソリューション。特別に構成された EMC Symmetrix デバイスを、EMC Symmetrix 標準デバイス上でデータを保護するために、ミラーとして、つまり Business Continuance Volumes として規定します。
BCV *も参照。*

BCV

(EMC Symmetrix 固有の用語)
Business Continuance Volumes の略。BCV デバイスは ICDA 内であらかじめ構成された専用の SLD です。ビジネスの継続運用を可能にするために使用されます。BCV デバイスには、これらのデバイスによりミラー化される SLD のアドレスとは異なる、個別の SCSI アドレスが割り当てられます。BCV デバイスは、保護を必要とする一次 EMC Symmetrix SLD の分割可能なミラーとして使用されます。
BC および **BC Process** *も参照。*

BC VA

(HP StorageWorks Virtual Array 固有の用語)
BC は Business Copy の略。Business Copy VA により、HP StorageWorks Virtual Array LUN の内部コピーをデータ バックアップやデータ複写の目的で同じ仮想アレイ内に保持することができます。コピー (子または Business Copy LUN) は、バックアップやデータ解析、開発など様々な目的に使用できます。バックアップ目的で使用されるときは、元 (親) の LUN はアプリケーション システムに接続され、Business Copy (子) LUN はバックアップ システムに接続されます。

HP StorageWorks Virtual Array LUN、**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**も*参照。*

BRARCHIVE

(SAP R/3 固有の用語)
SAP R/3 バックアップ ツールの 1 つ。アーカイブ REDO ログ ファイルをバックアップできます。BRARCHIVE では、アーカイブ プロセスのすべてのログとプロファイルも保存されます。
SAPDBA、**BRBACKUP** および **BRRESTORE** *も参照。*

BRBACKUP

(SAP R/3 固有の用語)
SAP R/3 バックアップ ツールの 1 つ。制御ファイル、個々のデータ ファイル、またはすべてのテーブルスペースをオンラインでもオフラインでもバックアップできます。また、必要に応じて、オンライン REDO ログ ファイルをバックアップすることもできます。
SAPDBA、**BRARCHIVE** および **BRRESTORE** *も参照。*

BRRESTORE

(SAP R/3 固有の用語)
SAP R/3 のツール。以下の種類のファイルを復元するために使います。

- BRBACKUP で保存されたデータベース データ ファイル、制御ファイル、オンライン REDO ログ ファイル
- BRARCHIVE でアーカイブされた REDO ログ ファイル
- BRBACKUP で保存された非データベース ファイル

ファイル、テーブル スペース、バックアップ全体、REDO ログ ファイルのログ シーケンス番号、またはバックアップのセッション ID を指定することができます。
SAPDBA、**BRBACKUP** および **BRARCHIVE** *も参照。*

BSM
Data Protector Backup Session Manager の略。バックアップ セッションを制御します。このプロセスは、常に Cell Manager システム上で稼動します。

CA
(HP StorageWorks Disk Array XP 固有の用語)
Continuous Access XP の略。CA では、データ複製、バックアップ、および障害復旧などの目的で HP StorageWorks Disk Array XP LDEV のリモート コピーを作成および維持できます。CA を使用するには、メイン (プライマリ) ディスク アレイとリモート (セカンダリ) ディスク アレイが必要です。オリジナルのデータを格納し、アプリケーション システムに接続されている CA プライマリ ボリューム (P-VOL) がメイン ディスク アレイに格納されます。リモート ディスク アレイには、バックアップ システムに接続されている CA セカンダリ ボリューム (S-VOL) が格納されます。
BC *(HP StorageWorks Disk Array XP 固有の用語)*、**Main Control Unit** および **HP StorageWorks Disk Array XP LDEV** *も参照。*

CAP
(StorageTek 固有の用語)
Cartridge Access Port の略。ライブラリのドア パネルに組み込まれたポートです。メディアの出し入れに使用されます。

CDB
カタログ データベース (Catalog Database) の略。CDB は、IDB のうち、バックアップ、オブジェクト コピー、復元、メディア管理セッションおよびバックアップしたデータに関する情報を格納する部分。選択したロギング レベルによっては、ファイル名とファイル バージョンも格納されます。CDB は、常にセルに対してローカルとなります。
MMDB *も参照。*

CDF ファイル
(UNIX 固有の用語)
Context Dependent File (コンテキスト依存ファイル) の略。CDF ファイルは、同じパス名でグループ化された複数のファイルからなるファイルです。通常、プロセスのコンテキストに基づいて、これらのファイルのいずれかがシステムによって選択されます。このメカニズムにより、クラスタ内のすべてホストから同じパス名を使って、マシンに依存する実行可能ファイル、システム データ、およびデバイス ファイルを正しく動作させることができます。

Cell Manager
セル内のメイン システム。Data Protector の運用に不可欠なソフトウェアがインストールされ、すべてのバックアップおよび復元作業がここから管理されます。管理タスク用の GUI は、異なるシステムにインストールできます。各セルは、1 つの Cell Manager システムによって管理されます。

CMD Script for OnLine Server
(Informix 固有の用語)
Informix OnLine Server の構成時に INFORMIXDIR 内に作成される Windows CMD スクリプト。環境変数を OnLine Server にエクスポートするコマンド一式が含まれています。

CMMDB

COM+ 登録データベース

Data Protector の CMMDB (Centralized Media Management Database: メディア集中管理データベース) は、MoM セル内で、複数セルの MMDB をマージすることにより生成されます。この機能を使用することで、MoM 環境内の複数のセルの間でハイエンド デバイスやメディアを共有することが可能になります。いずれかのセルからロボティクスを使用して、他のセルに接続されているデバイスを制御することもできます。
CMMDB は MoM Manager 上に置く必要があります。MoM セルとその他の Data Protector セルの間には、できるだけ信頼性の高いネットワーク接続を用意してください。
MoM *も参照。*

COM+ 登録データベース

(Windows 固有の用語)
COM+ 登録データベースと Windows レジストリには、COM+ アプリケーションの属性、クラスの属性、およびコンピュータ レベルの属性が格納されます。これにより、これらの属性間の整合性を確保でき、これらの属性を共通の方法で操作できます。

Command View (CV) EVA

(HP StorageWorks EVA 固有の用語)
HP StorageWorks EVA ストレージ システムを構成、管理、モニターするためのユーザー インタフェース。さまざまなストレージ管理作業を行うために使用されます。たとえば、仮想ディスクファミリの作成、ストレージ システム ハードウェアの管理、仮想ディスクのスナップクローンやスナップショットの作成などに使用されます。Command View EVA ソフトウェアは HP OpenView Storage マネジメント アプライアンス上で動作し、Web ブラウザからアクセスできます。
HP StorageWorks EVA Agent (従来のもの) および **HP StorageWorks EVA SMI-S Agent** *も参照。*

CRS

Data Protector Cell Manager 上で実行される、Cell Request Server のプロセス (サービス)。バックアップ セッションと復元セッションを開始および制御します。このサービスは、Data Protector が Cell Manager 上にインストールされるとすぐに開始されます。CRS は、UNIX システムでは root アカウントで実行されます。Windows では、いかなるアカウントでも実行できます。デフォルトでは、インストール時に使用したユーザー アカウントで実行されます。

CSM

Data Protector コピー セッション マネージャの略。このプロセスは、オブジェクト コピー セッションを制御し、Cell Manager システム上で動作します。

Data Protector イベント ログ

イベント ログには、Data Protector 関連のすべての通知が書き込まれます。デフォルトの送信方法では、すべての通知がイベント ログに送信されます。イベント ログにアクセスできる Data Protector ユーザーは、admin ユーザー グループに所属しているか、または「**レポートと通知**」のユーザー権限が付与されている Data Protector ユーザーだけです。イベント ログに書き込まれているイベントは、いずれも表示と削除が可能です。

Data Protector ユーザー アカウント

Data Protector およびバックアップ データに対する無許可のアクセスを制限するために、Data Protector ユーザーとして許可を受けたユーザーにしか Data Protector を使用できないようになっています。Data Protector 管理者がこのアカウントを作成するときには、ユーザー ログオン名、ユーザーのログオン元として有効なシステム、および Data Protector ユーザー グループのメンバーシップを指定します。ユーザーが Data Protector

のユーザー インタフェースを起動するか、または特定のタスクを実行するときには、このアカウントが必ずチェックされます。

Dbobject

(Informix 固有の用語)
Informix の物理的なデータベース オブジェクト。blobspace、dbspace、または論理ログ ファイルなどがそれにあたります。

DCBF

DCBF (Detail Catalog Binary Files: 詳細カタログ バイナリ ファイル) ディレクトリは、IDB の一部です。IDB の約 80% を占めるファイル バージョンと属性に関する情報を格納します。デフォルトでは、DCBF は 1 つの DC ディレクトリからなり、その最大サイズは 2GB です。新たに DC ディレクトリを作成して追加することもできます。

DC ディレクトリ

詳細カタログ (DC) ディレクトリは、詳細カタログ バイナリ ファイル (DCBF) で構成されており、そのファイルの中にはファイル バージョンについての情報が保管されています。これは、IDB の DCBF 部分を表し、IDB 全体の約 80% の容量を占めます。デフォルトの DC ディレクトリは、`dcbf` ディレクトリと呼ばれ、*`<Data_Protector_home>`*`¥db40` ディレクトリ (Windows 用 Cell Manager の場合) または `/var/opt/omni/server/db40` ディレクトリ (UNIX 用 Cell Manager の場合) に配置されています。他の DC ディレクトリを作成して、適切な場所に置くことができます。1 つのセルでサポートされる DC ディレクトリは 10 個までです。DC ディレクトリのデフォルト最大サイズは 2GB です。

DHCP サーバ

Dynamic Host Configuration Protocol (DHCP) を通じて、IP アドレスおよび関連情報の動的構成機能を提供するシステム。

Disk Agent

クライアントのバックアップと復元を実行するためにクライアント システム上にインストールする必要があるコンポーネントの 1 つ。Disk Agent は、ディスクに対するデータの読み書きを制御します。バックアップ セッション中には、Disk Agent がディスクからデータを読み取って、Media Agent に送信してデータをデバイスに移動させます。復元セッション中には、Disk Agent が Media Agent からデータを受信して、ディスクに書き込みます。

Disk Agent の同時処理数

1 つの Media Agent に対して同時にデータを送信できる Disk Agent の数。

DMZ

DMZ (Demilitarized Zone) は、企業のプライベート ネットワーク (イントラネット) と外部のパブリック ネットワーク (インターネット) の間に「中立地帯」として挿入されたネットワークです。DMZ により、外部のユーザーが企業のイントラネット内のサーバに直接アクセスすることを防ぐことができます。

DNS サーバ

DNS クライアント サーバ モデルでは、DNS サーバにインターネット全体で名前解決を行うのに必要な DNS データベースに含まれている情報の一部を保持します。DNS サーバは、このデータベースを使用して名前解決を要求するクライアントに対してコンピュータ名を提供します。

DR イメージ

一時障害復旧オペレーティング システム (DR OS) のインストールおよび構成に必要なデータ。

DR OS
障害復旧オペレーティング システムとは、障害復旧を実行するためのオペレーティング システム環境です。Data Protector に対して基本的な実行時環境 (ディスク、ネットワーク、テープ、およびファイルシステムへのアクセス) を提供します。Data Protector 障害復旧を実行する前に、DR OS をインストールおよび構成しておく必要があります。DR OS は、Data Protector 障害復旧プロセスのホストとして機能するだけでなく、復元後のシステムの一部にもなります。その場合、DR OS の構成データは元の構成データに置き換わります。

EMC Symmetrix Agent (SYMA)
(EMC Symmetrix 固有の用語)
Symmetrix Agent (SYMA) を参照。

EMC Symmetrix Application Programming Interface (SYMAPI)
(EMC Symmetrix 固有の用語)
Symmetrix Application Programming Interface (SYMAPI) を参照。

EMC Symmetrix CLI Database File
(EMC Symmetrix 固有の用語)
Symmetrix CLI Database File を参照。

EMC Symmetrix Command-Line Interface (SYMCLI)
(EMC Symmetrix 固有の用語)
Symmetrix Command-Line Interface (SYMCLI) を参照。

FC ブリッジ
Fibre Channel ブリッジ *を参照。*

Fibre Channel
Fibre Channel は、高速のコンピュータ相互接続に関する ANSI 標準です。光ケーブルまたは銅線ケーブルを使って、大容量データ ファイルを高速で双方向送信でき、数 km 離れたサイト間を接続できます。
Fibre Channel は、ノード間を 3 種類の物理トポロジー (ポイント トゥ ポイント、ループ、スイッチ式) で接続できます。

Fibre Channel ブリッジ
Fibre Channel ブリッジ (マルチプレクサ) は、RAID アレイ、ソリッド ステート ディスク (SSD)、テープ ライブラリなどの既存のパラレル SCSI デバイスを Fibre Channel 環境に移行できるようにします。ブリッジ (マルチプレクサ) の片側には Fibre Channel インタフェースがあり、その反対側にはパラレル SCSI ポートがあります。このブリッジ (マルチプレクサ) を通じて、SCSI パケットを Fibre Channel とパラレル SCSI デバイスの間で移動することができます。

fnames.dat
IDB の fnames.dat ファイルには、バックアップしたファイルの名前に関する情報が格納されます。一般に、ファイル名が保存されている場合、それらのファイルは IDB の 20% を占めます。

GUI
Data Protector には、各種プラットフォーム (HP-UX、Solaris、Windows) に対応したグラフィカル ユーザー インタフェース (GUI) が用意されており、すべての構成タスク、管理タスクおよび処理タスクに容易にアクセスできます。

Holidays ファイル
休日に関する情報を格納するファイル。このファイルを通じて、休日の設定を変更できます。Holidays ファイルのパスは、`/etc/opt/omni/server/Holidays` (UNIX 用 Cell Manager の場合) または `<Data_Protector_home>¥Config¥Server¥holidays` (Windows 用 Cell Manager の場合) です。

HP ITO
OVO *を参照。*

HP OpC
OVO *を参照。*

HP OpenView SMART Plug-In (SPI)
ドメイン監視機能を強化する完全に統合されたソリューションで、HP OpenView Operations に追加するだけですぐに使えます。HP OpenView SMART Plug-In として実装される Data Protector 用統合ソフトウェアを使用して、ユーザーは HP OpenView Operations (OVO) の拡張機能として任意の数の Data Protector Cell Manager を監視できます。

HP OVO
OVO *を参照。*

HP StorageWorks Disk Array XP LDEV
HP StorageWorks Disk Array XP の物理ディスクの論理パーティション。LDEV は、Continuous Access XP (CA) 構成および Business Copy XP (BC) 構成で複製することができるエンティティで、スタンドアロンのエンティティとしても使用できます。
BC *(HP StorageWorks Disk Array XP 固有の用語)*、**CA** *(HP StorageWorks Disk Array XP 固有の用語)*、および**複製** *も参照。*

HP StorageWorks EVA Agent (従来のもの)
Data Protector のソフトウェア モジュール。Command View (CV) EVA ソフトウェア v3.1 以前と、EVA VCS ファームウェア v3.01x 以前がインストールされた HP StorageWorks EVA 上で稼動する HP StorageWorks Enterprise Virtual Array 統合ソフトウェアに必要なすべてのタスクを実行します。
Command View (CV) EVA および **HP StorageWorks EVA SMI-S Agent** *も参照。*

HP StorageWorks EVA SMI-S Agent
Data Protector のソフトウェア モジュール。Command View (CV) EVA ソフトウェアの v3.2 以降がインストールされた HP StorageWorks EVA 上で稼動する HP StorageWorks Enterprise Virtual Array 統合ソフトウェアに必要なタスクをすべて実行します。EVA SMI-S Agent を使用すると、受信した要求と CV EVA 間のやり取りを制御する HP StorageWorks SMI-S EVA プロバイダを通じてアレイを制御できます。
Command View (CV) EVA、**HP StorageWorks SMI-S EVA プロバイダ**、および **HP StorageWorks EVA Agent (従来のもの)** *も参照。*

HP StorageWorks SMI-S EVA プロバイダ
HP StorageWorks Enterprise Virtual Array を制御するために使用されるインタフェース。SMI-S EVA プロバイダは HP OpenView ストレージ マネジメント アプライアンス システム上で個別のサービスとして動作し、受信した要求と Command View EVA 間のゲートウェイとして機能します。Data Protector HP StorageWorks EVA 用統合ソフトウェアでは、SMI-S EVA プロバイダは EVA SMI-S Agent から標準化された要求を受け入れ、Command View EVA とやり取りして情報または方法を呼び出し、標準化された応答を返します。
HP StorageWorks EVA SMI-S Agent および **Command View (CV) EVA** *も参照。*

HP StorageWorks Virtual Array LUN
HP StorageWorks Virtual Array 内の物理ディスクの論理パーティション。LUN は HP StorageWorks Business Copy VA 構成で複製することができるエンティティで、スタンドアロンのエンティティとしても使用できます。
BC VA および**複製** *も参照。*

HP VPO

OVO *を参照。*

ICDA

(EMC Symmetrix 固有の用語)
EMC's Symmetrix の統合キャッシュ ディスク アレイ (ICDA) は、複数の物理ディスク、複数の FWD SCSI チャネル、内部キャッシュ メモリ、およびマイクロコードと呼ばれる制御 / 診断ソフトウェアを備えたディスク アレイ デバイスです。

IDB

Data Protector 内部データベースは、Cell Manager 上に維持される埋込み型データベースです。どのデータがどのメディアにバックアップされるか、バックアップ セッションと復元セッションがどのように実行されるか、さらに、どのデバイスとライブラリが構成されているかについての情報が格納されます。

Inet

Data Protector セル内の各 UNIX システムまたは Windows システム上で動作するプロセス。このプロセスは、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起動を受け持ちます。システムに Data Protector をインストールすると、Inet サービスが即座に起動されます。Inet プロセスは、inetd デーモンにより開始されます。

Internet Information Server (IIS)

(Windows 固有の用語)
Microsoft Internet Information Server は、ネットワーク用ファイル / アプリケーション サーバで、複数のプロトコルをサポートしています。IIS では、主に、HTTP (Hypertext Transport Protocol) により HTML (Hypertext Markup Language) ページとして情報が転送されます。

IP アドレス

IP (インターネット プロトコル) アドレスは、ネットワーク上のシステムを一意に識別するアドレスで、数字で表されます。IP アドレスは、ピリオド (ドット) で区切られた 4 組の数字からなります。

ISQL

(Sybase 固有の用語)
Sybase のユーティリティの 1 つ。Sybase SQL Server に対してシステム管理作業を実行できます。

ITO

OVO *を参照。*

LBO

(EMC Symmetrix 固有の用語)
Logical Backup Object (論理バックアップ オブジェクト) の略。LBO は、EMC Symmetrix/Fastrax 環境内で保存 / 取得されるデータ オブジェクトです。LBO は EMC Symmetrix によって 1 つのエンティティとして保存 / 取得され、部分的には復元できません。

LISTENER.ORA

(Oracle 固有の用語)
Oracle の構成ファイルの 1 つ。サーバ上の 1 つまたは複数の TNS リスナを定義します。

log_full シェル スクリプト

(Informix UNIX 固有の用語)
ON-Bar に用意されているスクリプトの 1 つ。OnLine Server が log-full イベント警告を発行したときに論理ログ ファイルのバックアップを開始できます。Informix の ALARMPROGRAM 構成パラメータは、デフォルトで、`<INFORMIXDIR>/etc/log_full.sh` に設定されます。ここで、`<INFORMIXDIR>` は、OnLine Server ホーム ディレクトリです。論理ログ ファイルを継続的にバックアップした

くない場合は、ALARMPROGRAM 構成パラメータを *<INFORMIXDIR>*/etc/no_log.sh に設定してください。

Lotus C API
(Lotus Domino Server 固有の用語)
Lotus Domino Server と Data Protector などのバックアップ ソリューションの間でバックアップ情報および復元情報を交換するためのインタフェース。

LVM
LVM (Logical Volume Manager: 論理ボリューム マネージャ) は、HP-UX システム上で物理ディスク スペースを構造化し、論理ボリュームにマッピングするためのサブシステムです。LVM システムは、複数のボリューム グループで構成されます。各ボリューム グループには、複数のボリュームが含まれます。

Main Control Unit (MCU)
(HP StorageWorks Disk Array XP 固有の用語)
Continuous Access 構成用のプライマリ ボリュームを含み、マスター デバイスとしての役割を果たす HP StorageWorks XP ディスク アレイ。
BC*(HP StorageWorks Disk Array XP 固有の用語)*、**CA** *(HP StorageWorks Disk Array XP 固有の用語)* および **HP StorageWorks Disk Array XP LDEV** *も参照。*

Manager-of-Managers (MoM)
エンタープライズ Cell Manager *を参照。*

MAPI
(MS Exchange 固有の用語)
MAPI (Messaging Application Programming Interface) は、アプリケーションおよびメッセージング クライアントがメッセージング システムおよび情報システムと対話するためのプログラミング インタフェースです。

Media Agent
デバイスに対する読み込み / 書き込みを制御するプロセス。制御対象のデバイスはテープなどのメディアに対して読み込み / 書き込みを行います。バックアップ セッション中、Media Agent は Disk Agent からデータを受信し、デバイスに送信します。データを受信したデバイスはメディアに書き込みます。Media Agent は、ライブラリのロボティクス制御も管理します。

MFS
Migrating Filesystem の略。MFS は、HP-UX 11.00 において、移行能力を持つ標準的な JFS ファイルシステムを実現します。MFS は、標準ファイルシステム インタフェース (DMAPI) 経由でアクセスでき、通常の HP-UX ファイルシステムと同様にディレクトリにマウントされます。MFS では、スーパーブロック、i ノード情報、および " 拡張属性 " 情報のみがハードディスク上に永続的に保持され、これらが移動されることはありません。
VBFS *も参照。*

Microsoft Exchange Server
多様な通信システムへの透過的接続を提供するクライアント / サーバ型のメッセージング / ワークグループ システム。電子メール システムの他、個人とグループのスケジュール、オンライン フォーム、ワークフロー自動化ツールなどをユーザーに提供します。また、開発者に対しては、情報共有およびメッセージング サービス用のカスタム アプリケーション開発プラットフォームを提供します。

Microsoft SQL Server 7.0/2000
分散型クライアント / サーバ コンピューティングのニーズを満たすように設計されたデータベース管理システム。

Microsoft Volume Shadow Copy Service (VSS)
VSS 対応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統合管理する統一通信インタフェースを提供するソフトウェア 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、ライター、シャドウ コピー プロバイダ、およびオペレーティング システム カーネルと連携して、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。
シャドウ コピー、シャドウ コピー プロバイダ、ライター *も参照。*

Microsoft 管理コンソール (MMC)
(Windows 固有の用語)
Windows 環境における管理モデル。シンプルで一貫した統合型管理ユーザー インタフェースを提供します。同じ GUI を通じて、さまざまな MMC 対応アプリケーションを管理できます。

MMD
Media Management Daemon (メディア管理デーモン) の略。MMD プロセス (サービス) は、Data Protector Cell Manager 上で稼動し、メディア管理操作およびデバイス操作を制御します。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。

MMDB
Media Management Database (メディア管理データベース) の略。MMDB は、IDB の一部です。セル内で構成されているメディア、メディア プール、デバイス、ライブラリ、ライブラリ デバイス、スロットに関する情報と、バックアップに使用されている Data Protector メディアに関する情報を格納します。エンタープライズ バックアップ環境では、データベースをすべてのセル間で共有できます。
CMMDB および **CDB** *も参照。*

MoM
複数のセルをグループ化して、1 つのセルから集中管理することができます。集中管理用のセルが MoM (Manager-of-Managers) です。MoM を通じて、複数のセルを一元的に構成および管理できます。

MSM
Media Session Manager (メディア セッション マネージャ) の略。MSM は、Cell Manager 上で稼動し、メディア セッション (メディアのコピーなど) を制御します。

MU 番号
(HP StorageWorks Disk Array XP 固有の用語)
MU 番号は、Mirror Unit Number (ミラー ユニット番号) の略語。ファースト レベル ミラーを示すために使う整数 (0、1 または 2) です。
ファースト レベル ミラー *も参照。*

obdrindex.dat
IDB バックアップおよびバックアップ用のメディアとデバイスに関する情報を格納する IDB ファイルです。この情報を使うと、IDB の復旧を大幅に効率化できます。ファイルを IDB トランザクション ログとともに、ほかの IDB ディレクトリから別の物理ディスク上に移し、さらに、そのファイルのコピーを作成し、適切な場所に保存します。

OBDR 対応デバイス
ブート可能ディスクを装填した CD-ROM ドライブをエミュレートできるデバイス。バックアップ デバイスとしてだけでなく、障害復旧用のブート デバイスとしても使用可能です。

OmniStorage
透過的な移行を可能にするソフトウェア。使用頻度の高いデータをハード ディスク上に残したまま使用頻度の低いデータを光磁気ライブラリに移動します。HP OmniStorage は、HP-UX システム上で動作します。

ON-Bar
(Informix 固有の用語)
OnLine Server のためのバックアップと復元のシステム。ON-Bar により、OnLine Server データのコピーを作成し、後でそのデータを復元することが可能になります。ON-Bar のバックアップと復元のシステムには、以下のコンポーネントが含まれます。

- onbar ユーティリティ
- バックアップ ソリューションとしての Data Protector
- XBSA インタフェース
- ON-Bar カタログ テーブル。これは、dbobject をバックアップし、複数のバックアップを通して dbobject のインスタンスをトラッキングするために使われます。

onbar ユーティリティ
(Informix 固有の用語)
Informix ユーティリティの 1 つ。バックアップ要求および復元要求を OnLine Server との間でやり取りします。このユーティリティでは、XBSA を使用して制御データを交換し、Data Protector と連携してデータのバックアップと復元を行います。

ONCONFIG
(Informix 固有の用語)
アクティブな ONCONFIG 構成ファイルの名前を指定する環境変数。ONCONFIG 環境変数が存在しない場合、OnLine が *<INFORMIXDIR>*¥etc¥onconfig (HP-UX の場合)、または *<INFORMIXDIR>*/etc/onconfig (Windows の場合) のファイルにある構成値を使います。

OnLine Server
(Informix 固有の用語)
INFORMIX-OnLine Dynamic Server を指します。

OpC
OVO ***を参照。***

ORACLE_SID
(Oracle 固有の用語)
Oracle Server インスタンスの一意な名前。別の Oracle Server に切り替えるには、目的の *<ORACLE_SID>* を指定します。*<ORACLE_SID>* は、TNSNAMES.ORA ファイル内の接続記述子の CONNECT DATA 部分と LISTENER.ORA ファイル内の TNS リスナの定義に含まれています。

Oracle インスタンス
(Oracle 固有の用語)
1 つまたは複数のシステムにインストールされた個々の Oracle データベース。1 つのコンピュータ システム上で、複数のデータベース インスタンスを同時に稼動させることができます。

Oracle ターゲット データベースへのログイン情報
(Oracle および SAP R/3 固有の用語)
ログイン情報の形式は、<user_name>/<password>@<service> です。

- <user_name> は、Oracle Server およびその他のユーザーに対して公開されるユーザー名です。ユーザー名には必ずパスワードが関連付けられます。各ユーザーが Oracle ターゲット データベースに接続するには、ユーザー名とパスワード

の両方を入力しなければなりません。ここでは、Oracle の SYSDBA 権限または SYSOPER 権限が付与されているユーザーを指定する必要があります。

- <password> は、所有者だけが知っているデータ セキュリティ用の文字列です。パスワードは、オペレーティング システムまたはソフトウェア アプリケーションへの接続時に入力します。パスワードは、Oracle パスワード ファイル (orapwd) に指定されているパスワードに一致する必要があります。これは、データベース管理を行うユーザーの認証に使用されるファイルです。

- <service> は、ターゲット データベースの SQL*Net サーバ プロセスを識別する名前です。

OVO
HP ネットワーク内の多数のシステムとアプリケーションの運用管理を強力な機能でサポートする OpenView Operations for Unix の略称。Data Protector には、この管理製品を使用するための統合ソフトウェアが用意されています。この統合ソフトウェアは、HP-UX および Solaris 上の OVO 管理サーバ用の SMART Plug-In として実装されています。以前のバージョンの OVO は、IT/Operation、Operations Center、および Vantage Point Operations と呼ばれていました。
***マージ*も参照。**

P1S ファイル
P1S ファイルには、システムにインストールされているすべてのディスクを高度な自動障害復旧 (EADR) 中にどのようにフォーマットするかに関する情報が格納されます。このファイルはフル バックアップ中に作成され、バックアップ メディアと Cell Manager に recovery.p1s というファイル名で保存されます。保存場所は、*<Data_Protector_home>*¥Config¥Server¥dr¥p1s ディレクトリ (Windows 用 Cell Manager の場合) または /etc/opt/omni/server/dr/p1s ディレクトリ (UNIX 用 Cell Manager の場合) です。

RAID
Redundant Array of Inexpensive Disks の略。

RAID Manager XP
(HP StorageWorks Disk Array XP 固有の用語)
RAID Manager XP アプリケーションには、CA アプリケーションおよび BC アプリケーションのステータスを報告 / 制御するコマンドが豊富に用意されています。これらのコマンドは、RAID Manager インスタンスを通じて、StorageWorks Disk Array XP Disk Control Unit と通信します。このインスタンスは、コマンドを一連の低レベル SCSI コマンドに変換します。

RAID Manager ライブラリ
(HP StorageWorks Disk Array XP 固有の用語)
Solaris システム上の Data Protector では、RAID Manager ライブラリを内部的に使用して、HP StorageWorks Disk Array XP の構成データ、ステータス データ、およびパフォーマンス データにアクセスします。さらに、一連の低レベル SCSI コマンドに変換される関数呼び出しを通じて、StorageWorks Disk Array XP の主要な機能にアクセスします。

raw ディスクのバックアップ
***ディスク イメージのバックアップ*を参照。**

RCU
(HP StorageWorks 固有の用語)
Remote Control Unit (RCU) は、CA 構成の中で MCU (Main Contol Unit) のスレーブと

しての役割を果たします。双方向の構成の中では、RCU は MCU としての役割を果たします。

RDBMS
Relational Database Management System (リレーショナル データベース管理システム) の略。

RDF1/RDF2
(EMC Symmetrix 固有の用語)
SRDF デバイス グループの一種。RDF グループには RDF デバイスだけを割り当てることができます。RDF1 グループ タイプにはソース デバイス (R1) が格納され、RDF2 グループ タイプにはターゲット デバイス (R2) が格納されます。

RDS
Raima Database Server の略。RDS (サービス) は、Data Protector の Cell Manager 上で稼動し、IDB を管理します。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。

RecoveryInfo
Windows 構成ファイルのバックアップ時、Data Protector は、現在のシステム構成に関する情報 (ディスク レイアウト、ボリューム、およびネットワークの構成に関する情報) を収集します。この情報は、障害復旧時に必要になります。

Recovery Manager (RMAN)
(Oracle 固有の用語)
Oracle コマンド行インタフェース。これにより、Oracle Server プロセスに接続されているデータベースをバックアップ、復元、および復旧するための指示が Oracle Server プロセスに出されます。RMAN では、バックアップについての情報を格納するために、リカバリ カタログまたは制御ファイルのいずれかが使用されます。この情報は、後の復元セッションで使うことができます。

REDO ログ
(Oracle 固有の用語)
各 Oracle データベースには、複数の REDO ログ ファイルがあります。データベース用の REDO ログ ファイルのセットをデータベースの REDO ログと呼びます。Oracle では、REDO ログを使ってデータに対するすべての変更を記録します。

Remote Control Unit
(HP StorageWorks Disk Array XP 固有の用語)
Remote Control Unit (RCU) は、CA 構成の中で MCU (Main Contol Unit) のスレーブとしての役割を果たします。双方向の構成の中では、RCU は MCU としての役割を果たします。

RMAN
(Oracle 固有の用語)
Recovery Manager を参照。

RSM
Data Protector Restore Session Manager の略。復元セッションを制御します。このプロセスは、常に Cell Manager システム上で稼動します。

RSM
(Windows 固有の用語)
Removable Storage Manager の略。RSM は、アプリケーション、ロボティクス チェンジャ、およびメディア ライブラリの間の通信を効率化するメディア管理サービスを提供します。これにより、複数のアプリケーションがローカル ロボティクス メディア ライブラリとテープまたはディスク ドライブを共有でき、リムーバブル メディアを管理できます。

SAPDBA
(SAP R/3 固有の用語)
BRBACKUP ツール、BRARCHIVE ツール、BRRESTORE ツールを統合した SAP R/3 ユーザー インタフェース。

SIBF
サーバレス統合バイナリ ファイル (SIBF) は、IDB のうち、NDMP の raw メタデータが格納される部分です。これらのデータは、NDMP オブジェクトの復元に必要です。

SMB
スプリット ミラー バックアップ *を参照。*

SMBF
セッション メッセージ バイナリ ファイル (SMBF) は、IDB のうち、バックアップ セッション中および復元セッション中に生成されたセッション メッセージが格納される部分です。セッションごとに 1 つのバイナリ ファイルが作成されます。バイナリ ファイルは、年と月に基づいて分類されます。

sqlhosts ファイル
(Informix 固有の用語)
Informix の接続情報ファイル。各データベース サーバの名前の他、ホスト コンピュータ上のクライアントが接続できるエイリアスが格納されます。

SRD ファイル
SRD (System Recovery Data: システム復旧データ) ファイルには、障害発生時にオペレーティング システムをインストールおよび構成するために必要なシステム情報が含まれています。SRD ファイルは ASCII ファイルで、CONFIGURATION バックアップが Windows クライアント上で実行され Cell Manager に保存される時に生成されます。

SRDF
(EMC Symmetrix 固有の用語)
EMC Symmetrix Remote Data Facility の略。SRDF は、異なる位置にある複数の処理環境の間での効率的なリアルタイム データ複製を実現する Business Continuation プロセスです。同じルート コンピュータ環境内だけではなく、互いに遠距離にある環境も対象となります。

SSE Agent
(HP StorageWorks Disk Array XP 固有の用語)
スプリット ミラー バックアップの統合に必要なタスクをすべて実行する Data Protector ソフトウェア モジュール。RAID Manager XP ユーティリティ (HP-UX システムおよび Windows システムの場合) または RAID Manager ライブラリ (Solaris システムの場合) を使い、HP StorageWorks Disk Array XP の保管システムと通信します。

sst.conf ファイル
`/usr/kernel/drv/sst.conf` ファイルは、マルチドライブ ライブラリ デバイスが接続されている Data Protector Sun Solaris クライアントのそれぞれにインストールされていなければならないファイルです。このファイルには、クライアントに接続されている各ライブラリ デバイスのロボット機構の SCSI アドレス エントリが記述されてなければなりません。

st.conf ファイル
`/kernel/drv/st.conf` ファイルは、バックアップ デバイスが接続されている Data Protector Solaris クライアントのそれぞれにインストールされていなければならないファイルです。このファイルには、クライアントに接続されている各バックアップ ドライブのデバイス情報と SCSI アドレスが記述されていなければなりません。シングルドライブ デ

バイスについては単一の SCSI エントリが必要で、マルチドライブ ライブラリ デバイスについては複数の SCSI エントリが必要です。

StorageTek ACS ライブラリ

(StorageTek 固有の用語)

ACS (Automated Cartridge System) は、1 つのライブラリ管理ユニット (LMU) と、このユニットに接続された 1 ～ 24 個のライブラリ記憶域モジュール (LSM) からなるライブラリ システム (サイロ) です。

Sybase Backup Server API

(Sybase 固有の用語)

Sybase SQL Server と Data Protector などのバックアップ ソリューションの間でのバックアップ情報および復旧情報交換用に開発された業界標準インタフェース。

Sybase SQL Server

(Sybase 固有の用語)

Sybase のクライアント / サーバ アーキテクチャにおけるサーバ。Sybase SQL Server は、複数のデータベースと複数のユーザーを管理し、ディスク上のデータの実位置を追跡します。さらに、物理データ ストレージ域に対する論理データ記述のマッピングを維持し、メモリ内のデータ キャッシュとプロシージャ キャッシュを維持します。

Symmetrix Agent (SYMA)

(EMC Symmetrix 固有の用語)

EMC Symmetrix 環境でのバックアップ操作と復元操作を可能にする Data Protector ソフトウェア モジュール。

Symmetrix Application Programming Interface (SYMAPI)

(EMC Symmetrix 固有の用語)

Data Protector クライアントに接続された EMC Symmetrix ユニットとのインタフェースとして使用できる、リンク可能な関数のライブラリ。EMC によって提供されます。

Symmetrix CLI データベース ファイル

(EMC Symmetrix 固有の用語)

EMC Symmetrix ICDA が構成されており SYMCLI がインストールされている各システム上の EMC Symmetrix 構成データを格納する EMC Symmetrix データベース ファイル。

Symmetrix Command-Line Interface (SYMCLI)

(EMC Symmetrix 固有の用語)

特殊な低レベル SCSI コマンドで Symmetrix ユニットからデータを取得するアプリケーション。EMC Symmetrix Application Programming Interface (SYMAPI) を使用しています。SYMCLI では、オープン システム環境で動作しているクライアント上でコマンドを実行することで、クライアントに接続されている EMC Symmetrix ユニットから構成、ステータスおよびパフォーマンスに関するデータを取得できます。

System Backup to Tape

(Oracle 固有の用語)

Oracle がバックアップ要求または復元要求を発行したときに正しいバックアップ デバイスをロード、ラベリング、およびアンロードするために必要なアクションを処理する Oracle インタフェース。

SysVol

(Windows 固有の用語)

ドメインのパブリック ファイルのサーバ コピーを保存する共有ディレクトリで、ドメイン内のすべてのドメイン コントローラ間で複製されます。

TimeFinder
(EMC Symmetrix 固有の用語)
単一または複数の EMC Symmetrix 論理デバイス (SLD) のインスタント コピーを作成する Business Continuation プロセス。インスタント コピーは、BCV と呼ばれる専用の事前構成 SLD 上に作成され、システムに対する別個のプロセスを経由してアクセスできます。

TLU
Tape Library Unit (テープ ライブラリ ユニット) の略。

TNSNAMES.ORA
(Oracle および SAP R/3 固有の用語)
サービス名にマッピングされた接続記述子を格納するネットワーク構成ファイル。このファイルは、1 か所で集中的に管理してすべてのクライアントで使用することも、また、ローカルに管理して各クライアントで個別に使用することもできます。

TSANDS.CFG ファイル
(Novell NetWare 固有の用語)
バックアップを開始するコンテナの名前を指定する**ファイル**。このファイルはテキスト ファイルで、TSANDS.NLM がロードされるサーバの SYS:SYSTEM¥TSA ディレクトリにあります。

VBFS
(OmniStorage 固有の用語)
VBFS (Very Big File System) とは、HP-UX 9.x 上の標準 HP-UX ファイルシステムに対する拡張部分を指します。VBFS は、通常の HP-UX ファイルシステムと同様にディレクトリにマウントされます。VBFS では、スーパーブロック、i ノード情報、および " 拡張属性 " 情報のみがハードディスク上に永続的に保持され、これらが移動されることはありません。
MFS *も参照。*

Virtual Controller Software (VCS)
(HP StorageWorks EVA 固有の用語)
HSV コントローラを介した Command View EVA との通信など、記憶システムの処理すべてを管理するファームウェア。
Command View (CV) EVA *も参照。*

VOLSER
(ADIC および STK 固有の用語)
ボリューム シリアル (VOLume SERial) 番号は、メディア上のラベルで、大容量ライブラリ内の物理テープの識別に使用されます。VOLSER は、ADIC/GRAU デバイスおよび StorageTek デバイス固有の命名規則です。

Volume Shadow Copy サービス
Microsoft Volume Shadow Copy Service *を参照。*

VPO
OVO *を参照。*

VSS
Microsoft Volume Shadow Copy Service *を参照。*

VxFS
Veritas Journal Filesystem の略。

VxVM (Veritas Volume Manager)
Veritas Volume Manager は、Solaris プラットフォーム上でディスク スペースを管理するためのシステムです。VxVM システムは、論理ディスク グループに編成された 1 つまたは複数の物理ボリュームの任意のグループからなります。

Wake ONLAN
節電モードで動作しているシステムを同じ LAN 上の他のシステムからのリモート操作により電源投入するためのサポート。

Web レポート

Data Protector の機能の 1 つ。バックアップ ステータスと Data Protector 構成に関するレポートを Web インタフェース経由で表示できます。

Windows CONFIGURATION バックアップ
Data Protector では、Windows CONFIGURATION (構成データ) をバックアップできます。Windows レジストリ、ユーザー プロファイル、イベント ログ、WINS サーバ データおよび DHCP サーバ データ (システム上で構成されている場合) を 1 回の操作でバックアップできます。

Windows レジストリ
オペレーティング システムやインストールされたアプリケーションの構成情報を保存するため、Windows により使用される集中化されたデータベース。

WINS サーバ
Windows ネットワークのコンピュータ名を IP アドレスに解決する Windows インターネット ネーム サービス ソフトウェアを実行しているシステム。Data Protector では、WINS サーバ データを Windows の構成データの一部としてバックアップできます。

XBSA インタフェース
(Informix 固有の用語)
onbar ユーティリティと Data Protector の間の相互通信には、X/Open Backup Specification Services Programmer's Interface (XBSA) が使用されます。

XCopy エンジン
(ダイレクト バックアップ固有の用語)
SCSI-3 のコピー コマンド。SCSI ソース アドレスを持つストレージ デバイスから SCSI 宛先アドレスを持つバックアップ デバイスにデータをコピーし、ダイレクト バックアップを可能にします。XCopy では、ソース デバイスからデータをブロック (ディスクの場合) またはストリーム (テープの場合) として宛先デバイスにコピーします。これにより、データをストレージ デバイスから読み込んで宛先デバイスに書き込むまでの一連の処理が、制御サーバをバイパスして行われます。
ダイレクト バックアップ も参照。

ZDB
ゼロ ダウンタイム バックアップ (ZDB) を参照。

ZDB データベース
(ZDB 固有の用語)
ソース ボリューム、複製およびセキュリティ情報などの ZDB 関連情報を格納する IDB の一部。ZDB データベースは ZDB、インスタント リカバリ、スプリット ミラー復元に使用されます。
ゼロ ダウンタイム バックアップ (ZDB) も参照。

アーカイブ ロギング
(Lotus Domino Server 固有の用語)
Lotus Domino Server のデータベース モードの 1 つ。トランザクション ログ ファイルがバックアップされて始めて上書きされるモードです。

アーカイブ REDO ログ
(Oracle 固有の用語)
オフライン REDO ログとも呼ばれます。Oracle データベースが ARCHIVELOG モードで動作している場合、各オンライン REDO ログが最大サイズまで書き込まれると、1 つまたは複数のアーカイブ先にコピーされます。このコピーをアーカイブ REDO ログと呼びます。各データベースに対してアーカイブ REDO ログを作成するかどうかを指定するには、以下の 2 つのモードのいずれかを指定します。

- ARCHIVELOG - 満杯になったオンライン REDO ログ ファイルは、再利用される前にアーカイブされます。そのため、インスタンスやディスクにエラーが発生した場合に、データベースを復旧することができます。
  " ホット " バックアップを実行できるのは、データベースがこのモードで稼動しているときだけです。

- NOARCHIVELOG - オンライン REDO ログ ファイルは、満杯になってもアーカイブされません。

オンライン REDO ログ *も参照*。

アクセス権
ユーザー権限 *を参照。*

アプリケーション エージェント
クライアント上でオンライン データベース統合ソフトウェアを復元およびバックアップするために必要なコンポーネント。
Disk Agent *も参照*。

アプリケーション システム
(ZDB 固有の用語)
このシステム上でアプリケーションやデータベースが実行されます。アプリケーションまたはデータベース データは、ソース ボリューム上に格納されています。
バックアップ システムおよび**ソース ボリューム** *も参照。*

イベント ログ
Windows 上で発生したすべてのイベント (サービスの停止 / 開始やユーザーのログオン / ログオフなど) が記録されるファイル。Data Protector では、Windows 構成データ バックアップの一部として Windows イベント ログをバックアップできます。

インスタント リカバリ
(ZDB 固有の用語)
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して、ソース ボリュームの内容を複製が作成された時点の状態に復元するプロセスです。これにより、テープからの復元を行う必要がなくなります。関連するアプリケーションやデータベースによってはインスタント リカバリだけで十分な場合もあれば、完全に復旧するためにトランザクション ログ ファイルを適用するなどその他にも手順が必要な場合もあります。
複製、ゼロ ダウンタイム バックアップ (ZDB)、ディスクへの ZDB、および**ディスク / テープへの ZDB** *も参照。*

インストール サーバ
特定のアーキテクチャ用の Data Protector ソフトウェア パッケージのレポジトリを保持するコンピュータ システム。インストール サーバから Data Protector クライアントのリモート インストールが行われます。混在環境では、UNIX システム用と Windows システム用の 2 台のインストール サーバが最低限必要になります。

インフォメーション ストア
(Microsoft Exchange Server 2000/2003 固有の用語)
記憶域管理を行う Microsoft Exchange Server 2000/2003 のサービス。Microsoft Exchange Server 2000/2003 のインフォメーション ストアは、メールボックス ストアとパブリック フォルダ ストアの 2 種類を管理します。メールボックス ストアは個々のユーザーに属するメールボックスから成ります。パブリック フォルダ ストアには、複数のユーザーで共有するパブリック フォルダおよびメッセージがあります。
キー マネージメント サービスおよび**サイト複製サービス** *も参照。*

インフォメーション ストア
(Microsoft Exchange Server 5.5 固有の用語)
Microsoft Exchange Server 5.5 のデフォルト メッセージ ストア プロバイダ。インフォメーション ストアは、以下から構成されます。

- パブリック インフォメーション ストア
- プライベート インフォメーション ストア
- パーソナル フォルダ ストア
- オフライン インフォメーション ストア

パブリック インフォメーション ストアには、パブリック フォルダおよびメッセージが格納され、これらは複数のユーザー / アプリケーション間で共有できます。複数の Exchange サーバを使用している場合でも、Exchange Server 5.5 組織内のすべてのユーザーが単一のパブリック インフォメーション ストアを共有します。プライベート インフォメーション ストアには、ユーザーまたはアプリケーションに所属するメールボックスが格納されます。メールボックスは、Microsoft Exchange Server 5.5 を実行しているサーバに常駐しています。
ディレクトリ ストア (DS) *も参照。*

上書き
復元中のファイル名競合を解決するモードの 1 つ。既存のファイルの方が新しくても、すべてのファイルがバックアップから復元されます。
マージ *も参照。*

エクスチェンジャ
SCSI エクスチェンジャとも呼ばれます。
ライブラリ *も参照。*

エンタープライズ バックアップ環境
複数のセルをグループ化して、1 つのセルから集中管理することができます。エンタープライズ バックアップ環境には、複数の Data Protector セル内のすべてのクライアントが含まれます。これらのセルは、Manager of Managers (MoM) のコンセプトにより集中管理用のセルから管理されます。
MoM *も参照。*

オートチェンジャー
ライブラリ *を参照。*

オートローダ
ライブラリ *を参照。*

オブジェクト
バックアップ オブジェクト *を参照。*

オブジェクト ID
(Windows 固有の用語)
NTFS 5 ファイルは、オブジェクト ID (OID) を通じてアクセスできます。これにより、システム内でファイルが実際に置かれている場所を意識する必要がなくなります。Data Protector では、OID をファイルの代替ストリームとして扱います。

オブジェクト コピー
特定のオブジェクト バージョンのコピー。オブジェクト コピー セッション中またはオブジェクト ミラーのバックアップ セッション中に作成されます。

オブジェクト コピー セッション
異なるメディア セット上にバックアップされたデータの追加のコピーを作成するプロセス。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 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。

オブジェクトのコピー
選択されたオブジェクト バージョンを特定のメディア セットにコピーするプロセス。1 つまたは複数のバックアップ セッションからコピーするオブジェクトを選択できます。

オブジェクトのミラーリング
バックアップ セッション中に、同一のデータを複数のメディア セットに書き込むプロセス。Data Protector では、すべてまたは一部のバックアップ オブジェクトを 1 つまたは複数のメディア セットにミラーできます。

オブジェクト ミラー
オブジェクトのミラーリングを使用して作成されるバックアップ オブジェクトのコピー。オブジェクトのミラーは通常オブジェクト コピーと呼ばれます。

オフライン REDO ログ
アーカイブ REDO ログ*を参照。*

オフライン バックアップ
実行中はアプリケーション データベースがアプリケーションから使用できなくなるバックアップ。

- 単純なバックアップ方法の場合 (ZDB ではない)、データベースはバックアップ中 (数分から数時間) オフライン状態となり、バックアップ システムからは使用できますが、アプリケーション システムからは使用できません。たとえばテープへのバックアップの場合、テープへのデータ ストリーミングが終わるまでの間となります。

- ZDB の方法を使うと、データベースはオフライン状態になりますが、所要時間はデータ複製プロセス中のわずか数秒間です。残りのバックアップ プロセスでは、データベースは通常の稼動を再開できます。

ゼロ ダウンタイム バックアップ (ZDB) および**オンライン バックアップ***を参照。*

オフライン復旧
オフライン復旧は、ネットワーク障害などにより Cell Manager にアクセスできない場合に行われます。オフライン復旧には、スタンドアロン デバイスと SCSI ライブラリ デバイスだけを使用できます。Cell Manager の復旧は、常にオフラインで行われます。

オンライン REDO ログ
(Oracle 固有の用語)
まだアーカイブされていないが、インスタンスでデータベース アクティビティを記録するために利用できるか、または満杯になっており、アーカイブまたは再使用されるまで待機している REDO ログ。
アーカイブ REDO ログ*も参照。*

オンライン バックアップ
データベース アプリケーションを利用可能な状態に維持したまま行われるバックアップ。データベースは、バックアップ アプリケーションが元のデータ オブジェクトにアクセスする必要がある間、特別なバックアップ モードで稼動します。この期間中、データベースは完全に機能しますが、パフォーマンスに多少影響が出たり、ログ ファイルのサイズが急速に増大したりする場合もあります。

- 単純なバックアップ方法の場合 (ZDB ではない)、バックアップ モードはバックアップ期間全体 (数分から数時間) 必要となります。たとえばテープへのバックアップの場合、テープへのデータ ストリーミングが終わるまでの間となります。

- ZDB の方法を使うと、バックアップ モードに必要な時間はデータ複製プロセス中のわずか数秒間です。残りのバックアップ プロセスでは、データベースは通常の稼動を再開できます。

場合によっては、データベースを整合性を保って復元するために、トランザクション ログもバックアップする必要があります。
ゼロ ダウンタイム バックアップ (ZDB) および**オフライン バックアップ** *も参照。*

階層ストレージ管理 (HSM)
使用頻度の低いデータを低コストの光磁気プラッタに移動することで、コストの高いハード ディスク記憶域を有効利用するための仕組み。移動したデータが必要になった場合は、ハード ディスク記憶域に自動的に戻されます。これにより、ハード ディスクからの高速読み取りと光磁気プラッタの低コスト性のバランスが維持されます。

拡張可能 ストレージ エンジン (ESE)
(Microsoft Exchange Server 2000/2003 固有の用語)
Microsoft Exchange Server 2000/2003 で情報交換用の記憶システムとして使用されているデータベース テクノロジ。

仮想サーバ
仮想マシンとは、ネットワーク IP 名および IP アドレスでドメイン内に定義されるクラスタ環境を意味します。このアドレスは、クラスタ ソフトウェアによってキャッシュされ、仮想サーバ リソースを現在実行しているクラスタ ノードにマッピングされます。こうして、特定の仮想サーバに対するすべての要求が特定のクラスタ ノードにキャッシュされます。

仮想ディスク
(HP StorageWorks EVA 固有の用語)
HP StorageWorks Enterprise Virtual Array のストレージ プールから割り当てられる記憶領域の単位。仮想ディスクは、HP StorageWorks Enterprise Virtual Array のスナップショット機能により複製されるエンティティです。
ソース ボリュームおよび**ターゲット ボリューム** *も参照。*

仮想デバイス インタフェース
(MS SQL Server 7.0/2000 固有の用語)
SQL Server 7.0/2000 のプログラミング インタフェースの 1 つ。大容量のデータベースを高速でバックアップおよび復元できます。

カタログ保護
バックアップ データに関する情報 (ファイル名やファイル バージョンなど) を IDB に維持する期間を定義します。
データ保護 *も参照。*

キー マネージメント サービス
(Microsoft Exchange Server 2000/2003 固有の用語)
セキュリティ強化のための暗号化機能を提供する Microsoft Exchange Server 2000/2003 のサービス。
インフォメーション ストアおよび**サイト複製サービス** *も参照。*

共有ディスク
(Windows 固有の用語)
システム状態データには、レジストリ、COM+ クラス登録データベース、システム起動ファイル、および証明書サービス データベース (証明書サーバの場合) が含まれます。サーバがドメイン コントローラの場合は、Active Directory ディレクトリ サービスと Sysvol ディレクトリもシステム状態データに含まれます。サーバ上でクラスタ サービスが実行されている場合は、リソース レジストリ チェックポイントと、最新のクラスタ データベース情報を格納するクォーラム リソース回復ログもシステム状態データに含まれます。

共有ディスク

あるシステム上に置かれた Windows のディスクをネットワーク上の他のシステムのユーザーが使用できるように構成したもの。共有ディスクを使用しているシステムは、Data Protector Disk Agent がインストールされていなくてもバックアップ可能です。

緊急ブート ファイル
(Informix 固有の用語)
Informix の構成ファイルの 1 つ。ixbar.*<server_id>*(*<server_id>* は SERVERNUM 構成パラメータの値) という名前で *<INFORMIXDIR>*¥etc ディレクトリ (HP-UX の場合) または *<INFORMIXDIR>*/etc ディレクトリ (Windows の場合) に保存されます (*<INFORMIXDIR>* は OnLine Server のホーム ディレクトリ)。緊急ブート ファイルの各行は、1 つのバックアップ オブジェクトに対応します。

クライアント バックアップ
クライアントにマウントされているすべてのファイルシステムのバックアップ。ただし、バックアップ仕様の作成後にクライアントにマウントされたファイルシステムは、自動検出されません。

クライアントまたはクライアント システム
セル内で Data Protector の機能を使用できるように構成された任意のシステム。

クラスタ対応アプリケーション
クラスタ アプリケーション プログラミング インタフェースをサポートしているアプリケーション。クラスタ対応アプリケーションごとに、クリティカル リソースが宣言されます。これらのリソースには、ディスク ボリューム (Microsoft Cluster Server の場合)、ボリューム グループ (MC/ServiceGuard の場合)、アプリケーション サービス、IP 名および IP アドレスなどがあります。

グループ
(Microsoft Cluster Server 固有の用語)
特定のクラスタ対応アプリケーションを実行するために必要なリソース (ディスク ボリューム、アプリケーション サービス、IP 名および IP アドレスなど) の集合。

グローバル オプション ファイル
Data Protector をカスタマイズするためのファイル。このファイルでは、Data Protector のさまざまな設定 (特に、タイムアウトや制限) を定義でき、その内容は Data Protector セル全体に適用されます。このファイルは、HP-UX システムおよび Solaris システムでは /etc/opt/omni/server/options ディレクトリに置かれ、Windows システムでは *<Data_Protector_home>*¥Config¥Server¥Options ディレクトリに置かれます。

検証
指定したメディア上の Data Protector データが読み取り可能かどうかをチェックする機能。また、CRC (巡回冗長検査) オプションをオンにして実行したバックアップに対しては、各ブロック内の整合性もチェックできます。

コマンド行インタフェース (CLI)
CLI には、DOS コマンドや UNIX コマンドと同じようにシェル スクリプト内で使用でできるコマンドが用意されています。これらを通じて、Data Protector の構成、管理、バックアップ / 復元タスクを実行することができます。

再解析ポイント
(Windows 固有の用語)
任意のディレクトリまたはファイルに関連付けることができるシステム制御属性。再解析属性の値は、ユーザー制御データをとることができます。このデータの形式は、データを保存したアプリケーションによって認識され、

データの解釈用にインストールされており、該当ファイルを処理するファイルシステム フィルタによっても認識されます。ファイル システムは、再解析ポイント付きのファイルを検出すると、そのデータ形式に関連付けられているファイルシステム フィルタを検索します。

サイト複製サービス
(Microsoft Exchange Server 2000/2003 固有の用語)
Exchange Server 5.5 ディレクトリ サービスをエミュレートすることで Exchange 5.5 との互換性を確保する Microsoft Exchange Server 2000/2003 サービス。
インフォメーション ストアおよび**キー マネージメント サービス** *も参照。*

差分同期 (再同期)
(EMC Symmetrix 固有の用語)
BCV または SRDF の制御操作の 1 つ。BCV 制御操作では、Incremental Establish (増分的確立) により、BCV デバイスが増分的に同期化され、EMC Symmetrix ミラー化メディアとして機能します。EMC Symmetrix デバイスは、事前にペアにしておく必要があります。
SRDF 制御操作では、Incremental Establish (増分的確立) により、ターゲット デバイス (R2) が増分的に同期化され、EMC Symmetrix ミラー化メディアとして機能します。EMC Symmetrix デバイスは、事前にペアにしておく必要があります。

差分バックアップ (delta backup)
差分バックアップ (delta backup) では、前回の各種バックアップ以降にデータベースに対して加えられたすべての変更がバックアップされます。
バックアップの種類 *も参照。*

差分バックアップ (differential backup)
作成済みで、まだ保護されている Data Protector バックアップ (フルまたは増分) をベースにした増分バックアップ。
増分バックアップ *を参照。*

差分バックアップ (differential backup)
(MS SQL 固有の用語)
前回のフル データベース バックアップ以降にデータベースに対して加えられた変更だけを記録するデータベース バックアップ。
バックアップの種類 *も参照。*

差分リストア
(EMC Symmetrix 固有の用語)
BCV または SRDF の制御操作の 1 つ。
BCV 制御操作では、差分リストアにより、BCV デバイスがペア内の 2 番目に利用可能な標準デバイスのミラーとして再割り当てされます。これに対し、標準デバイスの更新時には、オリジナルのペアの分割中に BCV デバイスに書き込まれたデータだけが反映され、分割中に標準デバイスに書き込まれたデータは BCV ミラーからのデータで上書きされます。
SRDF 制御操作では、差分リストアにより、ターゲット デバイス (R2) がペア内の 2 番目に利用可能なソース デバイス (R1) のミラーとして再割り当てされます。これに対し、ソース デバイス (R1) の更新時には、オリジナルのペアの分割中にターゲット デバイス (R2) に書き込まれたデータだけが反映され、分割中にソース デバイス (R1) に書き込まれたデータはターゲット ミラー (R2) からのデータで上書きされます。

システム ディスク
オペレーティング システム ファイルが入っているディスク。Microsoft の用語では、ブート プロセスの最初の手順に必要なファイルが入っているディスクと定義されています。

システム データベース

システム パーティション

(Sybase 固有の用語)

Sybase SQL Server を新規インストールすると以下の 4 種類のデータベースが生成されます。

- マスター データベース (master)
- 一時データベース (tempdb)
- システム プロシージャ データベース (sybsystemprocs)
- モデル データベース (model)

システム パーティション

オペレーティング システム ファイルが入っているパーティション。Microsoft の用語では、ブート プロセスの最初の手順に必要なファイルが入っているパーティションと定義されています。

システム ボリューム / ディスク / パーティション

オペレーティング システム ファイルが格納されているボリューム / ディスク / パーティション。ただし、Microsoft の用語では、ブート プロセスの開始に必要なファイルが入っているボリューム / ディスク / パーティションをシステム ボリューム / ディスク / パーティションと呼んでいます。

事前割当てリスト

メディア プール内のメディアのサブセットをバックアップに使用する順に指定したリスト。

実行後

オブジェクトのバックアップ後、またはセッション全体の完了後にコマンドまたはスクリプトを実行するバックアップ オプション。実行後コマンドは、Data Protector で事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows 上で動作する実行可能ファイルまたはバッチファイル、UNIX 上で動作するシェル スクリプトなどを使用できます。

実行前コマンド *も参照。*

実行前

オブジェクトのバックアップ前、またはセッション全体の開始前にコマンドまたはスクリプトを実行するバックアップ オプション。実行前コマンドおよび実行後コマンドは、Data Protector で事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows 上で動作する実行可能ファイルまたはバッチファイル、UNIX 上で動作するシェル スクリプトなどを使用できます。

実行後コマンド *も参照。*

実行前 / 実行後コマンド

実行前コマンドおよび実行後コマンドは、バックアップ セッションまたは復元セッションの前後に付加的な処理を実行する実行可能ファイルまたはスクリプトです。実行前コマンドおよび実行後コマンドは、Data Protector で事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows 上で動作する実行可能ファイルまたはバッチファイル、UNIX 上で動作するシェル スクリプトなどを使用できます。

シャドウ コピー

(MS VSS 固有の用語)

特定の時点におけるオリジナル ボリューム (元のボリューム) の複製を表すボリューム。オリジナル ボリュームからではなく、シャドウ コピーからデータがバックアップされます。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。

Microsoft Volume Shadow Copy Service *も参照。*

シャドウ コピー セット

(MS VSS 固有の用語)
同じ時点で作成されたシャドウ コピーのコレクション。
シャドウ コピー*も参照。*

シャドウ コピー プロバイダ
(MS VSS 固有の用語)
ボリューム シャドウ コピーの作成と表現を行うエンティティ。プロバイダは、シャドウ コピー データを所有して、シャドウ コピーを公開します。プロバイダは、ソフトウェアで実装することも (システム プロバイダなど)、ハードウェア (ローカル ディスクやディスク アレイ) で実装することもできます。
シャドウ コピー*も参照。*

ジュークボックス
ライブラリ*を参照。*

ジュークボックス デバイス
光磁気メディアまたはファイル メディアを格納するために使用する、複数のスロットからなるデバイス。ファイル メディアの格納に使用する場合、ジュークボックス デバイスは「ファイル ジュークボックス デバイス」と呼ばれます。

循環ログ
(Microsoft Exchange Server および Lotus Domino Server 固有の用語)
Microsoft Exchange および Lotus Domino Server のデータベース モードの 1 つ。トランザクション ログ ファイルは、対応するデータがデータベースにコミットした後、定期的に上書きされます。循環ログにより、ディスク記憶領域の消費が低減できます。

障害復旧
クライアントのメイン システム ディスクを (フル) バックアップの実行時に近い状態に復元するためのプロセスです。

初期化
フォーマット*を参照。*

所有権
バックアップの所有権は、どのユーザーがバックアップからデータを復元できるかを決定します。あるユーザーが対話型バックアップを開始すると、そのユーザーはセッション オーナーになります。ユーザーが既存のバックアップ仕様を修正せずにそのまま起動した場合、そのバックアップ セッションは対話型とみなされません。この場合、バックアップ仕様内でバックアップ オーナーが指定されていれば、その指定が継承されます。バックアップ仕様内でバックアップ オーナーが指定されていなければ、バックアップを開始したユーザーがセッション オーナーになります。スケジューリングされたバックアップの場合、UNIX 用 Cell Manager では root.sys@<Cell Manager> がデフォルトのセッション オーナーとなり、Windows 用 Cell Manager では、Cell Manager のインストール時に指定されたユーザーがデフォルトのセッション オーナーとなります。所有権は変更可能なので、特定のユーザーをセッション オーナーにすることができます。

スイッチオーバー
フェイルオーバー*を参照。*

スキャン
デバイス内のメディアを識別する機能。これにより、MMDB を、選択した位置 (例えば、ライブラリ内のスロット) に実際に存在するメディアと同期させることができます。

スキャニング
デバイス内のメディアを識別する機能。これにより、MMDB を、選択した位置 (例えば、ライブラリ内のスロット) に実際に存在するメディアと同期させることができます。デバイスに含まれる実際のメディアをスキャンしてチェックすると、第三者が Data Protector

を使用せずにメディアを操作 (挿入または取り出しなど) していないかどうかなどを確認できます。

スケジューラ
自動バックアップの実行タイミングと頻度を制御する機能。スケジュールを設定することで、バックアップの開始を自動化できます。

スタッカー
メディア記憶用の複数のスロットを備えたデバイス。通常は、1 ドライブ構成です。スタッカーは、スタックからシーケンシャルにメディアを選択します。これに対し、ライブラリはレポジトリからメディアをランダムに選択します。

スタンドアロン ファイル デバイス
ファイル デバイスとは、ユーザーがデータのバックアップに指定したディレクトリにあるファイルのことです。

ストレージ グループ
(Microsoft Exchange Server 2000/2003 固有の用語)
同じトランザクション ログ ファイルを共有する複数のデータベース (ストア) のコレクション。Exchange では、各ストレージ グループを個別のサーバ プロセスで管理します。

ストレージ ボリューム
(ZDB 固有の用語)
ストレージ ボリュームは、オペレーティング システムまたはボリューム管理システム、ファイル システム、または他のオブジェクトが存在可能なその他のエンティティに提供可能なオブジェクトを表します (たとえば仮想化技法)。ボリューム管理システム、ファイル システムはこの記憶域に構築されます。これらは通常、ディスク アレイなどの記憶システム内に作成または存在します。

スナップショット
(HP StorageWorks VA および HP StorageWorks EVA 固有の用語)
スナップショット作成技法を使用して作成された複製の形式。使用するアレイ / 技法に応じて、特徴の異なるさまざまな種類のスナップショットが使用できます。スナップショットで作成された複製は動的なもので、スナップショットの種類や作成時間によって、ソース ボリュームの内容に依存する仮想コピーか、独立した正確な複製 (クローン) かのいずれかになります。
複製および**スナップショット作成** *も参照。*

スナップショット作成
(HP StorageWorks VA および HP StorageWorks EVA 固有の用語)
ソース ボリュームのコピー (ストレージ仮想化技法を使用) を作成する複製技法。複製はある一時点で作成されたものと見なされ、事前構成することなく、即座に使用できます。ただし、通常は複製作成後もコピー プロセスはバックグラウンドで継続されます。
スナップショット *も参照。*

スナップショット バックアップ
(HP StorageWorks VA および HP StorageWorks EVA 固有の用語)
テープへの ZDB、**ディスクへの ZDB**、および**ディスク / テープへの ZDB** *を参照。*

スパース ファイル
ブロックが空の部分を含むファイル。一部のデータにゼロが含まれているマトリックス、イメージ アプリケーションで作成したファイル、高速データベースなどの場合にスパース ファイルが生じます。スパース ファイルの処理を復元中に有効にしておかないと、スパース ファイルを復元できなくなる可能性があります。

スプリット ミラー

(EMC Symmetrix および HP StorageWorks Disk Array XP 固有の用語)
スプリット ミラー技法を使用して作成された複製。複製により、ソース ボリュームの内容について独立した正確な複製 (クローン) が作成されます。
複製および**スプリット ミラー バックアップ** *も参照。*

スプリット ミラーの作成
(EMC Symmetrix および HP StorageWorks Disk Array XP 固有の用語)
事前構成したターゲット ボリュームのセット (ミラー) を、ソース ボリュームの内容の複製が必要になるまでソース ボリュームのセットと同期化し続ける複製技法。その後、同期を停止 (ミラーを分割) すると、分割時点でのソース ボリュームのスプリット ミラー複製はターゲット ボリュームに残ります。
スプリット ミラー *も参照。*

スプリット ミラー バックアップ
(EMC Symmetrix 固有の用語)
テープへの ZDB *を参照。*

スプリット ミラー バックアップ
(HP StorageWorks Disk Array XP 固有の用語)
テープへの ZDB、**ディスクへの ZDB**、および**ディスク / テープへの ZDB** *を参照。*

スプリット ミラー復元
(EMC Symmetrix および HP StorageWorks Disk Array XP 固有の用語)
テープへの ZDB セッションまたはディスク / テープへの ZDB セッションでバックアップされたデータをテープ メディアからスプリット ミラー複製へ復元し、その後ソース ボリュームに同期させるプロセス。この方法では、完全なセッションを復元することも個々のバックアップ オブジェクトを復元することも可能です。
テープへの ZDB、**ディスク / テープへの ZDB** および**複製** *も参照。*

スレッド
(MS SQL Server 7.0/2000 固有の用語)
単一のプロセスにのみ所属する実行可能エンティティ。プログラム カウンタ、ユーザー モード スタック、カーネル モード スタック、および 1 式のレジスタ値からなります。同じプロセス内で複数のスレッドを同時に実行できます。

スロット
ライブラリ内の機械的位置。各スロットがメディア (DLT テープなど) を 1 つずつ格納します。Data Protector では、各スロットを番号で参照します。メディアを読み取るときには、ロボット機構がメディアをスロットからドライブに移動します。

制御ファイル
(Oracle および SAP R/3 固有の用語)
データベースの物理構造を指定するエントリが格納される Oracle データ ファイル。復旧に使用するデータベース情報の整合性を確保できます。

セカンダリ ボリューム (S-VOL)
(HP StorageWorks Disk Array XP 固有の用語)
セカンダリ ボリューム (S-VOL) は、他の LDEV (P-VOL) のセカンダリ CA ミラーまたは BC ミラーとしての役割を果たす XP LDEV。CA の場合、S-VOL を MetroCluster 構成内のフェイルオーバー デバイスとして使うことができます。S-VOL には、P-VOL によって使用されるアドレスとは異なる、個別の SCSI アドレスが割り当てられます。
プライマリ ボリューム (P-VOL) *も参照。*

セッション

バックアップ セッション、**メディア管理セッション**および**復元セッション***を参照。*

セッション ID
バックアップ、復元、オブジェクトのコピー、またはメディア管理セッションの識別子で、セッションを実行した日付と一意の番号から構成されます。

セッション キー
実行前スクリプトおよび実行後スクリプト用の環境変数。プレビュー セッションを含めた Data Protector セッションを一意に識別します。セッション キーはデータベースに記録されず、CLI コマンドの omnimnt、omnistat、および omniabort のオプション指定に使用されます。

セル
1 台の Cell Manager に管理されているシステムの集合。セルには、一般に、同じ LAN に接続されたサイトや組織エンティティ上のシステムが含まれます。バックアップおよび復元のポリシーとタスクは、1 か所から集中管理できます。

ゼロ ダウンタイム バックアップ (ZDB)
ディスク アレイにより実現したデータ複製技術を用いて、アプリケーション システムのバックアップ処理の影響を最小限に抑えるバックアップ アプローチ。バックアップされるデータの複製がまず作成されます。その後のすべてのバックアップ処理は、元のデータではなく複製データを使って実行し、アプリケーション システムは通常の処理に復帰します。
ディスクへの ZDB、**テープへの ZDB**、**ディスク / テープへの ZDB**、および**インスタント リカバリ** *も参照。*

増分 1 メールボックス バックアップ
増分 1 メールボックス バックアップでは、前回のフル バックアップ以降にメールボックスに対して行われた変更をすべてバックアップします。

増分バックアップ
前回のバックアップ以降に変更があったファイルだけを選択するバックアップ。増分バックアップには、複数のレベルがあり、前回の増分バックアップ以降に変更されたファイルだけをバックアップできます。
バックアップの種類 *も参照。*

増分バックアップ
(Microsoft Exchange Server 固有の用語)
前回のフル バックアップまたは増分バックアップ以降の変更だけをバックアップする Microsoft Exchange Server データのバックアップ。増分バックアップでは、バックアップ対象はトランザクション ログだけです。
バックアップの種類 *も参照。*

増分メールボックス バックアップ
増分メールボックス バックアップでは、前回の各種バックアップ以降にメールボックスに対して行われた変更をすべてバックアップします。

ソース デバイス (R1)
(EMC Symmetrix 固有の用語)
ターゲット デバイス (R2) との SRDF 操作に参加する EMC Symmetrix デバイス。このデバイスに対するすべての書き込みは、リモート EMC Symmetrix ユニット内のターゲット デバイス (R2) にミラー化されます。R1 デバイスは、RDF1 グループ タイプに割り当てる必要があります。
ターゲット デバイス (R2) *も参照。*

ソース ボリューム
(ZDB 固有の用語)
複製されたデータを含むストレージ ボリューム。

ターゲット システム
(障害復旧固有の用語)
障害が発生したシステム。ターゲット システムは、ブート不能な状態になっていることが多く、そのような状態のシステムを元のシステム構成に戻すことが障害復旧の目標となります。クラッシュしたシステムがそのままターゲット システムになるのではなく、正常に機能していないハードウェアをすべて交換することで、クラッシュしたシステムがターゲット システムになります。

ターゲット データベース
(Oracle 固有の用語)
RMAN では、バックアップまたは復元対象のデータベースがターゲット データベースとなります。

ターゲット デバイス (R2)
(EMC Symmetrix 固有の用語)
ソース デバイス (R1) との SRDF 操作に参加する EMC Symmetrix デバイス。リモート EMC Symmetrix ユニット内に置かれます。ローカル EMC Symmetrix ユニット内でソース デバイス (R1) とペアになり、ミラー化ペアから、すべての書き込みデータを受け取ります。このデバイスは、通常の I/O 操作ではユーザー アプリケーションからアクセスされません。R2 デバイスは、RDF2 グループ タイプに割り当てる必要があります。
ソース デバイス (R1) *も参照。*

ターゲット ボリューム
(ZDB 固有の用語)
データの複製先のストレージ ボリューム。

ターミナル サービス
(Windows 固有の用語)
Windows のターミナル サービスは、サーバ上で実行されている仮想 Windows デスクトップ セッションと Windows ベースのプログラムにクライアントからアクセスできるマルチセッション環境を提供します。

ダイレクト バックアップ
SCSI Extended Copy (Xcopy) コマンドを使用してディスクからテープ (または他の 2 次ストレージ) へのデータの直接移動を効率化する、SAN ベースのバックアップ ソリューション。ダイレクト バックアップは、SAN 環境内のシステムへのバックアップ I/O 負荷を軽減します。ディスクからテープ (または他の 2 次ストレージ) へのデータの直接移動を SCSI Extended Copy (XCopy) コマンドで効率化します。このコマンドは、ブリッジ、スイッチ、テープ ライブラリ、ディスク サブシステムなど、インフラストラクチャの各要素でサポートされています。
XCopy エンジン *も参照。*

チャネル
(Oracle 固有の用語)
Oracle Recovery Manager のリソース割り当て単位。チャネルが割り当てられるごとに、新しい Oracle プロセスが開始され、そのプロセスを通じてバックアップ、復元、および復旧が行われます。割り当てられるチャンネルの種類によって、使用するメディアの種類が決まります。

- DISK タイプ
- SBT_TAPE タイプ

Oracle が Data Protector と統合されており、指定されたチャネルの種類が SBT_TAPE タイプの場合は、上記のサーバ プロセスが Data Protector に対してバックアップの読み取りとデータ ファイルの書き込みを試行します。

ディスク イメージ (raw ディスク) のバックアップ

ディスク イメージのバックアップでは、ファイルがビットマップ イメージとしてバックアップされるので、高速バックアップが実現します。ディスク イメージ (raw ディスク) バックアップでは、ディスク上のファイルおよびディレクトリの構造はバックアップされませんが、ディスク イメージ構造がバイト レベルで保存されます。ディスク イメージ バックアップは、ディスク全体か、またはディスク上の特定のセクションを対象にして実行できます。

ディスク クォータ

コンピュータ システム上のすべてのユーザーまたはユーザーのサブセットに対してディスク スペースの消費を管理するためのコンセプト。このコンセプトは、いくつかのオペレーティング システム プラットフォームで採用されています。

ディスク グループ

(Veritas Volume Manager 固有の用語)

VxVM システムにおけるデータ ストレージの基本単位。ディスク グループは、1 つまたは複数の物理ボリュームから作成できます。同じシステム上に複数のディスク グループを置くことができます。

ディスク検出

ディスク検出では、クライアントのバックアップ中にディスクを検出します。このとき Data Protector が探索 (検出) するのは、クライアント上に存在するディスクで、バックアップの構成時にシステム上に存在しなかったディスクも検出の対象に含まれます。検出されたディスクがバックアップされます。この機能は、構成が頻繁に変更される動的な環境の場合に特に役立ちます。ディスクが展開されると、それぞれのディスクがマスター クライアント オブジェクトのオプションをすべて継承します。実行前コマンドと実行後コマンドは、1 回しか指定されていなくても、オブジェクトごとに繰り返し起動されることになります。

ディスク検出によるクライアントのバックアップ

クライアントにマウントされているすべてのファイルシステムのバックアップ。バックアップの開始時に、Data Protector がクライアント上のディスクを自動検出します。ディスク検出によるクライアント バックアップでは、バックアップ構成が単純化され、ディスクのマウント / アンマウントが頻繁に行われるシステムに対するバックアップ効率が向上されます。

ディスクステージング

複数のフェーズでデータをバックアップするプロセス。これにより、バックアップと復元のパフォーマンスが改善し、バックアップ データの保存コストが低減し、復元に対するデータの可用性とアクセス性が向上します。バックアップ ステージは、最初に 1 種類のメディア (たとえば、ディスク) にデータをバックアップし、その後データを異なる種類のメディア (たとえば、テープ) にコピーすることから構成されます。

ディスク / テープへの ZDB

(ZDB 固有の用語)

ゼロ ダウンタイム バックアップの 1 つの形式。ディスクへの ZDB と同様に、作成された複製が特定の時点でのソース ボリュームのバックアップとしてディスク アレイに保持されます。ただし、テープへの ZDB と同様、複製データはバックアップ メディアにもストリーミングされます。このバックアップ方法を使用した場合、同じセッションでバックアップしたデータは、インスタント リカバリ、Data Protector 標準のテープからの復元を使用して復元できます。スプリット ミラー アレイではスプリット ミラー復元が可能で

す。
ゼロ ダウンタイム バックアップ (ZDB)、ディスクへの ZDB、テープへの ZDB、インスタント リカバリ、複製、および**複製セット ローテーション**も参照。

ディスクへの ZDB
(ZDB 固有の用語)
ゼロ ダウンタイム バックアップの 1 つの形式。作成された複製が、特定の時点でのソース ボリュームのバックアップとしてディスク アレイに保持されます。同じバックアップ仕様を使って別の時点で作成された複数の複製を、複製セットに保持することができます。テープに ZDB した複製はインスタント リカバリ プロセスで復元できます。
ゼロ ダウンタイム バックアップ (ZDB)、テープへの ZDB、ディスク / テープへの ZDB、インスタント リカバリ、および**複製セット ローテーション**も参照。

ディレクトリ ストア (DS)
(Microsoft Exchange 固有の用語)
Microsoft Exchange Server ディレクトリの一部。Microsoft Exchange Server ディレクトリには、メッセージング システムで提供されるサービス、メールボックス、受信者レコード、パブリック フォルダなどをアプリケーションから検索およびアクセスするために Microsoft Exchange アプリケーションが使用するオブジェクトが格納されます。
インフォメーション ストア (MDB) も参照。

ディレクトリ接合
(Windows 固有の用語)
ディレクトリ接合は、Windows の再解析ポイントのコンセプトに基づいています。NTFS 5 ディレクトリ接合では、ディレクトリ / ファイル要求を他の場所にリダイレクトできます。

データ ストリーム
通信チャネルを通じて転送されるデータのシーケンス。

データファイル
(Oracle および SAP R/3 固有の用語)
Oracle によって作成される物理ファイル。表や索引などのデータ構造を格納します。データ ファイルは、1 つの Oracle データベースにのみ所属できます。

データベース サーバ
大規模なデータベース (SAP R/3 データベースや Microsoft SQL データベースなど) が置かれているコンピュータ。サーバ上のデータベースへは、クライアントからアクセスできます。

データベース ライブラリ
Data Protector のルーチンのセット。Oracle Server のようなオンライン データベース統合ソフトウェアのサーバと Data Protector の間でのデータ転送を可能にします。

データベースの差分バックアップ
前回のフル データベース バックアップ以降にデータベースに対して加えられた変更だけを記録するデータベース バックアップ。

データベースの並列処理 (数)
十分な台数のデバイスが利用可能で、並列バックアップを実行できる場合には、複数のデータベースが同時にバックアップされます。

データ保護
メディア上のバックアップ データを保護する期間を定義します。この期間中は、データが上書きされません。保護期限が切れると、それ以降のバックアップ セッションでメディアを再利用できるようになります。
カタログ保護も参照。

テープへの ZDB

テーブルスペース (表領域、表スペース)

(ZDB 固有の用語)

ゼロ ダウンタイム バックアップの 1 つの形式。作成された複製が、バックアップ メディア (通常はテープ) にストリーミングされます。このバックアップ形式ではインスタント リカバリはできませんが、バックアップ終了後にディスク アレイ上に複製を保持する必要がありません。バックアップ データは Data Protector 標準のテープからの復元を使用して復元できます。スプリット ミラー アレイでは、スプリット ミラー復元も使用することができます。

ゼロ ダウンタイム バックアップ (ZDB)、**ディスクへの ZDB**、**インスタント リカバリ**、**ディスク / テープへの ZDB**、および**複製** *も参照。*

テーブルスペース (表領域、表スペース)

データベース構造の一部。各データベースは論理的に 1 つまたは複数の表スペースに分割されます。各表スペースには、データ ファイルまたは raw ボリュームが排他的に関連付けられます。

テープレス バックアップ

(ZDB 固有の用語)

ディスクへの ZDB *を参照。*

デバイス

ドライブまたはより複雑な装置 (ライブラリなど) を格納する物理装置。

デバイス グループ

(EMC Symmetrix 固有の用語)

複数の EMC Symmetrix デバイスを表す論理ユニット。デバイスは 1 つのデバイス グループにしか所属できません。デバイス グループのデバイスは、すべて同じ EMC Symmetrix 装置に取り付けられている必要があります。デバイス グループにより、利用可能な EMC Symmetrix デバイスのサブセットを指定し、使用することができます。

デバイス ストリーミング

デバイスがメディアへ十分な量のデータを継続して送信できる場合、デバイスはストリーミングを行います。そうでない場合は、デバイスはテープを止めてデータが到着するのを待ち、テープを少し巻き戻した後、テープへの書込みを再開します。言い換えると、テープにデータを書き込む速度が、コンピュータ システムがデバイスへデータを送信する速度以下の場合、デバイスはストリーミングを行います。ストリーミングは、スペースの使用効率とデバイスのパフォーマンスを大幅に向上します。

デバイス チェーン

デバイス チェーンは、シーケンシャルに使用するように構成された複数のスタンドアロン デバイスからなります。デバイスチェーンに含まれるデバイスのメディアで空き容量がなくなると、自動的に次のデバイスのメディアに切り替えて、バックアップを継続します。

統合セキュリティ

(MS SQL 固有の用語)

統合セキュリティは、Microsoft SQL Server が Windows の認証メカニズムを使用して、すべての接続に対する Microsoft SQL Server ログインの妥当性をチェックできるようにします。統合セキュリティを使用していれば、すべてのユーザーが同じパスワードで Windows と Microsoft SQL Server の両方にログインできます。すべてのクライアントが信頼関係接続をサポートしている環境では、統合セキュリティを使うことをお勧めします。信頼関係接続とは、Windows Server によって妥当性がチェックされ、Microsoft SQL Server に受け付けられた接続を意味します。信頼関係接続だけが許可されます。

統合ソフトウェア オブジェクト
Oracle または SAP DB などの Data Protector 統合ソフトウェアのバックアップ オブジェクト。

同時処理数
Disk Agent の同時処理数 *を参照。*

動的 (ダイナミック) クライアント
ディスク検出によるクライアント バックアップ *を参照。*

ドメイン コントローラ
ユーザーのセキュリティを保護し、別のサーバ グループ内のパスワードを検証するネットワーク内のサーバ。

ドライブ
コンピュータ システムからデータを受け取って、磁気メディア (テープなど) に書き込む物理装置。データをメディアから読み取って、コンピュータ システムに送信することもできます。

ドライブのインデックス
ライブラリ デバイス内のドライブの機械的な位置を識別するための数字。ロボット機構によるドライブ アクセスは、この数に基づいて制御されます。

トランザクション
一連のアクションを単一の作業単位として扱えるようにするためのメカニズム。データベースでは、トランザクションを通じて、データベースの変更を追跡します。

トランザクション バックアップ
トランザクション バックアップは、一般に、データベースのバックアップよりも必要とするリソースが少ないため、データベースのバックアップよりもより高い頻度で実行できます。トランザクション バックアップを適用することで、データベースを問題発生以前の特定の時点の状態に復旧することができます。

トランザクション バックアップ
(Sybase および SQL 固有の用語)
トランザクション ログをバックアップすること。トランザクション ログには、前回のフル バックアップまたはトランザクション バックアップ以降に発生した変更が記録されます。

トランザクション ログ
(Data Protector 固有の用語)
IDB に対する変更を記録します。IDB 復旧に必要なトランザクション ログ ファイル (前回の IDB バックアップ以降に作成されたトランザクション ログ) が失われることがないように、トランザクション ログのアーカイブを有効化しておく必要があります。

トランザクション ログ テーブル
(Sybase 固有の用語)
データベースに対するすべての変更が自動的に記録されるシステム テーブル。

トランザクション ログ バックアップ
トランザクション ログ バックアップは、一般に、データベースのバックアップよりも必要とするリソースが少ないため、データベースのバックアップよりもより高い頻度で実行できます。トランザクションログ バックアップを用いることにより、データベースを特定の時点の状態に復元できます。

トランザクション ログ ファイル
データベースを変更するトランザクションを記録するファイル。データベースが破損した場合にフォールト トレランスを提供します。

トランスポータブル スナップショット

(MS VSS 固有の用語)
アプリケーション システム上に作成されるシャドウ コピー。このシャドウ コピーは、バックアップを実行するバックアップ システムに提供できます。
Microsoft Volume Shadow Copy Service (VSS) ***も参照。***

ハートビート
特定のクラスタ ノードの動作ステータスに関する情報を伝達するタイム スタンプ付きのクラスタ データ セット。このデータ セット (パケット) は、すべてのクラスタ ノードに配布されます。

ハード リカバリ
(Microsoft Exchange Server 固有の用語)
トランザクション ログ ファイルを使用し、データベース エンジンによる復元後に実行される Microsoft Exchange Server のデータベース復旧。

バックアップ API
Oracle のバックアップ / 復元ユーティリティとバックアップ / 復元メディア管理層の間にある Oracle インタフェース。このインタフェースによってルーチンのセットが定義され、バックアップ メディアのデータの読み書き、バックアップ ファイルの作成や検索、削除が行えるようになります。

バックアップ ID
統合ソフトウェア オブジェクトの識別子で、統合ソフトウェア オブジェクトのバックアップのセッション ID と一致します。バックアップ ID は、オブジェクトのコピー、エクスポート、またはインポート時に保存されます。

バックアップ オーナー
IDB の各バックアップ オブジェクトにはオーナーが定義されてます。デフォルトのオーナーは、バックアップ セッションを開始したユーザーです。

バックアップ オブジェクト
1 つのディスク ボリューム (論理ディスクまたはマウント ポイント) からバックアップされた項目すべてを含むバックアップ単位。バックアップ項目は、任意の数のファイル、ディレクトリ、ディスク全体またはマウント ポイントの場合が考えられます。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 (raw ディスク) 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 オブジェクトが保存される Data Protector クライアントのホスト名
- マウント ポイント : バックアップ オブジェクトが存在するクライアント上のディレクトリ構造 (Windows ではドライブ、UNIX ではマウント ポイント) におけるアクセス 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
- 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 システム
(ZDB 固有の用語)
1 つ以上のアプリケーション システムのターゲット ボリュームに接続しているシステム。典型的なバックアップ システムは、バック

アップ デバイスに接続され、複製内のデータのバックアップを実行します。
アプリケーション システム、**ターゲット ボリューム**および**複製** *も参照。*

バックアップ仕様
バックアップ対象オブジェクトを、使用するデバイスまたはドライブのセット、仕様内のすべてのオブジェクトに対するバックアップ オプション、バックアップを行いたい日時とともに指定したリスト。オブジェクトとなるのは、ディスクやボリューム全体、またはその一部、たとえばファイル、ディレクトリ、Windows レジストリなどです。インクルード リストおよびエクスクルード リストを使用して、ファイルを選択することもできます。

バックアップ世代
1 つのフル バックアップとそれに続く増分バックアップを意味します。次のフル バックアップが行われると、世代が新しくなります。

バックアップ セッション
データのコピーを記憶メディア上に作成するプロセス。バックアップ仕様に処理内容を指定することも、対話式に操作を行うこともできます (対話式セッション)。1 つのバックアップ仕様の中で複数のクライアントが構成されている場合、すべてのクライアントが同じバックアップの種類 (フルまたは増分) を使って、1 回のバックアップ セッションで同時にバックアップされます。バックアップ セッションの結果、1 式のメディア にバックアップ データが書き込まれます。これらのメディアは、バックアップ セットまたはメディア セットとも呼ばれます。
増分バックアップおよび**フル バックアップ** *も参照。*

バックアップ セット
バックアップに関連したすべての統合ソフトウェア オブジェクトのセットです。

バックアップ セット
(Oracle 固有の用語)
RMAN バックアップ コマンドを使用して作成したバックアップファイルの論理グループ。バックアップ セットは、バックアップに関連したすべてのファイルのセットです。これらのファイルはパフォーマンスを向上するため多重化することができます。バックアップ セットにはデータファイルまたはアーカイブ ログのいずれかを含めることができますが、両方同時に使用できません。

バックアップ チェーン
バックアップ チェーンは、フル バックアップと増分バックアップが実行される状況で登場する概念です。実行する増分バックアップのレベル ([増分]、[増分 1]、[増分 2] など) により、前回の増分と今回の増分の間に、単純な (場合によっては多少複雑な) 依存関係が発生します。バックアップ チェーンは、フル バックアップから始まり、目的の時点までに実行された依存関係のある増分バックアップすべてを含みます。

バックアップ デバイス
記憶メディアに対するデータの読み書きが可能な物理デバイスを Data Protector で使用できるように構成したもの。例えば、スタンドアロン DDS/DAT ドライブやライブラリなどをバックアップ デバイスとして使用できます。

バックアップの種類
増分バックアップ、**差分バックアップ (differential backup)**、**トランザクション バックアップ**、**フル バックアップ**および**差分バックアップ (delta backup)** *を参照。*

バックアップ ビュー
Data Protector では、バックアップ仕様のビューを切り替えることができます。[種類別] (デフォルト) を選択すると、バックアップ /

テンプレートで利用できるデータの種類に基づいたビューが表示されます。[グループ別] を選択すると、バックアップ仕様 / テンプレートの所属先のグループに基づいたビューが表示されます。[名前別] を選択すると、バックアップ仕様 / テンプレートの名前に基づいたビューが表示されます。[Manager 別] (MoM の実行時のみ有効) を選択すると、バックアップ仕様 / テンプレートの所属先の Cell Manager に基づいたビューが表示されます。

パッケージ
(MC / ServiceGuard および Veritas Cluster 固有の用語)
特定のクラスタ対応アプリケーションを実行するために必要なリソース (ボリューム グループ、アプリケーション サービス、IP 名および IP アドレスなど) の集合。

パブリック フォルダ ストア
(Microsoft Exchange Server 2000 / 2003 固有の用語)
インフォメーション ストアのうち、パブリック フォルダ内に情報を維持する部分。パブリック フォルダ ストアは、バイナリ リッチ テキスト .edb ファイルと、ストリーミング ネイティブ インターネット コンテンツを格納する .stm ファイルから構成されます。

パブリック / プライベート バックアップ データ
バックアップを構成する際は、バックアップ データをパブリックまたはプライベートのいずれにするかを選択できます。

- パブリック データ ― すべての Data Protector ユーザーに対してアクセスと復元が許可されます。
- プライベート データ ― バックアップの所有者および管理者に対してのみ表示と復元が許可されます。

標準セキュリティ
(MS SQL 固有の用語)
標準セキュリティでは、Microsoft SQL Server のログイン妥当性チェック プロセスをすべての接続に対して使用します。標準セキュリティは、ネットワーク内にさまざまなクライアントが混在しており、一部のクライアントでは信頼関係接続がサポートされていない場合に使用できます。また、以前のバージョンの SQL Server との下位互換性を確保する必要がある場合にも、標準セキュリティを使用できます。
統合セキュリティ *も参照。*

ファースト レベル ミラー
(HP StorageWorks Disk Array XP 固有の用語)
HP StorageWorks Disk Array XP では、プライマリ ボリュームのミラー コピーを最大 3 つまで作成することができ、このコピー 1 つにつきさらに 2 つのコピーを作成できます。最初の 3 つのミラー コピーはファースト レベル ミラーと呼ばれます。
プライマリ ボリュームおよび **MU 番号** *を参照。*

ファイル ジュークボックス デバイス
ファイル メディアを格納するために使用する、複数のスロットからなるディスク上に存在するデバイス。

ファイル デポ
バックアップからファイル ライブラリ デバイスまでのデータを含むファイル。

ファイル バージョン
フル バックアップや増分バックアップでは、ファイルが変更されている場合、同じファイルが複数回バックアップされます。バックアップのロギング レベルとして [すべてログ

に記録] を選択している場合は、ファイル名自体に対応する 1 つのエントリとファイルの各バージョンに対応する個別のエントリが IDB 内に維持されます。

ファイル ライブラリ デバイス
複数のメディアからなるライブラリをエミュレートするディスク上に存在するデバイス。ファイル デポと呼ばれる複数のファイルが格納されます。

ファイルシステム
ハード ディスク上に一定の形式で保存されたファイルの集まり。ファイルシステムは、ファイル属性とファイルの内容がバックアップ メディアに保存されるようにバックアップされます。

ファイル複製サービス (FRS)
Windows サービスの 1 つ。ドメイン コントローラのストア ログオン スクリプトとグループ ポリシーを複製します。また、分散ファイルシステム (DFS) 共有をシステム間で複製したり、任意のサーバから複製作業を実行することもできます。

ブート ボリューム / ディスク / パーティション
ブート プロセスの開始に必要なファイルが入っているボリューム / ディスク / パーティション。ただし、Microsoft の用語では、オペレーティング システム ファイルが格納されているボリューム / ディスク / パーティションをブート ボリューム / ディスク / パーティションと呼んでいます。

ブール演算子
オンライン ヘルプ システムの全文検索には、AND、OR、NOT、NEAR の各ブール演算子を使用できます。複数の検索条件をブール演算子で組み合わせて指定することで、検索対象をより正確に絞り込むことができます。複数単語の検索に演算子を指定しなければ、AND を指定したものとみなされます。例えば、「マニュアル 障害 復旧」という検索条件は、「マニュアル AND 障害 AND 復旧」と同じ結果になります。

フェールオーバー
あるクラスタ ノードから別のクラスタ ノードに最も重要なクラスタ データ (Windows の場合はグループ、UNIX の場合はパッケージ) を転送すること。フェールオーバーは、主に、プライマリ ノードのソフトウェア / ハードウェア障害発生時や保守時に発生します。

フォーマット
メディアを Data Protector で使用できるように初期化するプロセス。メディア上の既存データはすべて消去されます。メディアに関する情報 (メディア ID、説明、および位置) が IDB に保存されるとともに、メディア自体 (メディア ヘッダ) にも書き込まれます。データが保護されている Data Protector メディアは、保護の期限が切れるか、保護解除 / リサイクルされない限り再フォーマットされません。

負荷調整
デフォルトでは、デバイスが均等に使用されるように、バックアップ用に選択されたデバイスの負荷 (使用率) が自動的に調整されます。負荷調整では、各デバイスに書き込まれるオブジェクトの個数を調整することで、使用率を最適化します。負荷調整はバックアップ時に自動的に実行されるので、データが実際にどのようにバックアップされるかを管理する必要はありません。使用するデバイスを指定する必要があるだけです。負荷調整機能を使用しない場合は、バックアップ仕様に各オブジェクトに使用するデバイスを選択できます。Data Protector は指定された順序でデバイスにアクセスします。

復元セッション

バックアップ メディアからクライアントシステムにデータをコピーするプロセス。

複製
(ZDB 固有の用語)
ユーザー指定のバックアップ オブジェクトを含む、特定の時点におけるソース ボリュームのデータのイメージ。イメージは、作成するハードウェア / ソフトウェアによって、物理ディスク レベルでの記憶ブロックの独立した正確な複製 (クローン) になる (スプリット ミラーなど) 場合もあれば、仮想コピーになる (スナップショットなど) 場合もあります。ホストの視点では、標準的な UNIX または Windows システムについて、バックアップ オブジェクトを含む物理ディスク全体が複製されます。しかし、UNIX でボリューム マネージャを使用するときは、バックアップ オブジェクトを含むボリューム / ディスク グループ全体が複製されます。
スナップショット、**スナップショット作成**、**スプリット ミラー**、および**スプリット ミラーの作成***も参照。*

複製セット
(ZDB 固有の用語)
同じバックアップ仕様を使って作成される複製のグループ。
複製および**複製セット ローテーション***も参照。*

複製セット ローテーション
(ZDB 固有の用語)
通常のバックアップ作成のために継続的に複製セットを使用すること。複製セットの使用を必要とする同一のバックアップ仕様が実行されるたびに、新規の複製がセットの最大数になるまで作成され、セットに追加されます。その後、セット内の最も古い複製は置き換えられ、セット内の複製の最大数が維持されます。
複製および**複製セット***も参照。*

物理デバイス
ドライブまたはより複雑な装置 (ライブラリなど) を格納する物理装置。

プライベート インフォメーション ストア
(Microsoft Exchange Server 5.5 固有の用語)
ユーザー メールボックスの中に情報を保存するインフォメーション ストアの一部。1 つのメールボックス ストアは、1 つのバイナリ リッチテキスト .edb ファイルから構成されます。

プライマリ ボリューム (P-VOL)
(HP StorageWorks Disk Array XP 固有の用語)
CA 構成および BC 構成用プライマリ ボリューム (P-VOL) としての役割を果たす複数の標準 HP StorageWorks Disk Array XP LDEV です。P-VOL は MCU 内に配置されています。
セカンダリ ボリューム (S-VOL) *も参照。*

フリー プール
フリー プールは、メディア プール内のすべてのメディアが使用中になっている場合にメディアのソースとして補助的に使用できるプールです。ただし、メディア プールでフリー プールを使用するには、明示的にフリー プールを使用するように構成する必要があります。

フル データベース バックアップ
最後に (フルまたは増分) バックアップした後に変更されたデータだけではなく、データベース内のすべてのデータのバックアップ。フル データベース バックアップは、他のバックアップに依存しません。

フル バックアップ
フル バックアップでは、最近変更されたかどうかに関係なく、選択されたオブジェクトをすべてバックアップします。
バックアップの種類 *も参照。*

フル メールボックス バックアップ
フル メールボックス バックアップでは、メールボックス全体の内容をバックアップします。

分散ファイルシステム (DFS)
複数のファイル共有を単一の名前空間に接続するサービス。対象となるファイル共有は、同じコンピュータに置かれていても、異なるコンピュータに置かれていてもかまいません。DFS は、リソースの保存場所の違いに関係なくクライアントがリソースにアクセスできるようにします。

ペア ステータス
(HP StorageWorks Disk Array XP 固有の用語)
ミラー化されたディスクのペアは、そのペア上で実行されるアクションによって、様々なステータス値を持ちます。最も重要なステータス値は以下の 3 つです。

- コピー - ミラー化されたペアは、現在再同期中。データは一方のディスクからもう一方のディスクに転送されます。2 つのディスクのデータは同じではありません。
- ペア - ミラー化されたペアは、完全に同期されており、両方のディスク (プライマリ ボリュームとミラー ボリューム) は全く同じデータを持ちます。
- 中断 - ミラー化されたディスク間のリンクは中断されています。両方のディスクが別々にアクセスされ、更新されています。ただし、ミラー関係はまだ保持されており、このペアは、ディスク全体を転送することなく、再同期することができます。

並列処理 (数)
オンライン データベースから複数のデータ ストリームを読み取ること。

並行復元
1 つの Media Agent からデータを受信する Disk Agent を複数実行して、バックアップ データを複数のディスクに同時に (並行して) 復元すること。並行復元を行うには、複数のディスクまたは論理ボリュームに置かれているデータを選択し、同時処理数を 2 以上に設定してバックアップを開始し、異なるオブジェクトのデータを同じデバイスに送信する必要があります。並行復元中には、復元対象として選択した複数のオブジェクトがメディアから同時に読み取られるので、パフォーマンスが向上します。

保護
データ保護および**カタログ保護***を参照。*

ホスト システム
Data Protector Disk Agent がインストールされており、ディスク デリバリーによる障害復旧に使用される稼動中の Data Protector クライアント。

ホスト バックアップ
ディスク検出によるクライアント バックアップ*を参照。*

ボリューム グループ
LVM システムにおけるデータ ストレージ単位。ボリューム グループは、1 つまたは複数の物理ボリュームから作成できます。同じシステム上に複数のボリューム グループを置くことができます。

ボリューム マウントポイント
(*Windows 固有の用語*)
ボリューム上の空のディレクトリを他のボリュームのマウントに使用できるように構成したもの。ボリューム マウント ポイントは、ターゲット ボリュームへのゲートウェイとして機能します。ボリュームがマウントされていれば、ユーザーやアプリケーションがその

ボリューム上のデータをフル (マージ) ファイルシステム パスで参照できます (両方のボリュームが一体化されている場合)。

マージ
復元中のファイル名競合を解決するモードの 1 つ。復元するファイルと同じ名前のファイルが復元先に存在する場合、変更日時の新しい方が維持されます。既存のファイルと名前が重複しないファイルは、常に復元されます。
上書き *も参照。*

マウント ポイント
ディレクトリ構造内において、ディスクまたは論理ボリュームにアクセスするためのアクセス ポイント (`/opt` や `d:` など)。UNIX では、`bdf` コマンドまたは `df` コマンドを使ってマウント ポイントを表示できます。

マウント要求
マウント要求時には、デバイスにメディアを挿入するように促す画面が表示されます。必要なメディアを挿入して確認することでマウント要求に応答すると、セッションが続行されます。

マジック パケット
Wake ONLAN を参照。

マルチドライブ サーバ
単一システム上で Media Agent を無制限に使用できるライセンス。このライセンスは、Cell Manager の IP アドレスにバインドされており、新しいバージョンでは廃止されました。

ミラー
(EMC Symmetrix および HP StorageWorks Disk Array XP 固有の用語)
ターゲット ボリューム *を参照。*

ミラー ローテーション
(HP StorageWorks Disk Array XP 固有の用語)
複製セット ローテーション *を参照。*

無人操作 (lights-out operation または unattended operation)
オペレータの介在なしで、通常の営業時間外に実行されるバックアップ操作または復元操作。オペレータが手動で操作することなく、バックアップ アプリケーションやサービスのマウント要求などが自動的に処理されます。

無人操作 (unattended operation)
無人操作 (lights-out operation) *を参照。*

メールボックス
(Microsoft Exchange Server 固有の用語)
電子メールが配信される場所。管理者がユーザーごとに設定します。電子メールの配信場所として複数の個人用フォルダが指定されている場合は、メールボックスから個人用フォルダに電子メールがルーティングされます。

メールボックス ストア
(Microsoft Exchange Server 2000/2003 固有の用語)
インフォメーション ストアのうち、ユーザー メールボックス内の情報を維持する部分。メールボックス ストアは、バイナリ データを格納するリッチテキスト `.edb` ファイルと、ストリーミング ネイティブ インターネット コンテンツを格納する `.stm` ファイルからなります。

メディア ID
Data Protector がメディアに割り当てる一意な識別子。

メディア セット

バックアップ セッションでは、メディア セットと呼ばれるメディアのグループにデータをバックアップします。メディアの使用法によっては、複数のセッションで同じメディアを共有できます。

メディア プール
同じ種類のメディア (DDS) などのセット。グループとして追跡されます。フォーマットしたメディアは、メディア プールに割り当てられます。

メディア ラベル
メディアに割り当てられるユーザー定義の識別子。

メディア管理セッション
初期化、内容のスキャン、メディア上のデータの確認、メディアのコピーなどのアクションをメディアに対して実行するセッション。

メディア集中管理データベース (CMMDB)
CMMDB ***を参照。***

メディア状態要素
使用回数のしきい値と上書きのしきい値。メディアの状態の判定基準となります。

メディアの位置
バックアップ メディアが物理的に収納されている場所を示すユーザー定義の識別子。"building 4" や "off-site storage" のような文字列です。

メディアのインポート
メディアに書き込まれているバックアップ セッション データをすべて再読み込みして、IDB に取り込むプロセス。これにより、メディア上のデータにすばやく、簡単にアクセスできるようになります。
メディアのエクスポートも参照。

メディアのエクスポート
メディアに格納されているすべてのバックアップ セッション情報 (システム、オブジェクト、ファイル名など) を IDB から削除するプロセス。メディア自体に関する情報やメディアとプールの関係に関する情報も IDB から削除されます。メディア上のデータは影響されません。
メディアのインポートも参照。

メディアの種類
メディアの物理的な種類 (DDS や DLT など)。

メディアの状態
メディア状態要素から求められるメディアの品質。テープ メディアの使用頻度が高く、使用時間が長ければ、読み書きエラーの発生率が高くなります。状態が [不良] になったメディアは交換する必要があります。

メディアの使用法
ここでは、メディアの使用法として、以下のオプションのいずれかを選択します。メディアの使用法は、[**追加可能**]、[**追加不可能**]、[**増分のみ追加可能**] のいずれかに設定できます。

メディアのボールティング
メディアを安全な別の場所に収納すること。メディアが復元に必要になった場合や、今後のバックアップにメディアを再使用する場合は、メディアをデータ センターに戻します。ボールティング手順は、会社のバックアップ戦略やデータ保護 / 信頼性ポリシーに依存します。

メディアの割り当て方針
メディアをバックアップに使用する順序を決定します。[Strict] メディア割り当てポリシーでは、特定のメディアに限定されます。[Loose] ポリシーでは、任意の適切なメディアを使用できます。[フォーマットされていないメディアを先に割り当てる] ポリシーでは、

ライブラリ内に利用可能な非保護メディアがある場合でも、不明なメディアが優先されます。

元のシステム
あるシステムに障害が発生する前に Data Protector によってバックアップされたシステム構成データ。

ユーザー アカウント
Data Protector を使用するには、Data Protector のユーザー アカウントが必要です。Data Protector のユーザー アカウントは、Data Protector やバックアップされたデータに対する無断アクセスを制限します。Data Protector 管理者がこのアカウントを作成するときには、ユーザー ログオン名、ユーザーのログオン元として有効なシステム、および Data Protector ユーザー グループのメンバーシップを指定します。ユーザーが Data Protector のユーザー インタフェースを起動するか、または特定のタスクを実行するときには、このアカウントが必ずチェックされます。

ユーザー グループ
各 Data Protector ユーザーは、ユーザー グループのメンバーです。各ユーザー グループには 1 式のユーザー権限があり、それらの権限がユーザー グループ内のすべてのユーザーに付与されます。ユーザー権限を関連付けるユーザー グループの数は、必要に応じて定義できます。Data Protector には、admin、operator、user の 3 つのデフォルト ユーザー グループがあります。

ユーザー権限
特定の Data Protector タスクの実行に必要なパーミッションをユーザー権限またはアクセス権限と呼びます。主なユーザー権限には、バックアップの構成、バックアップ セッションの開始、復元セッションの開始などがあります。ユーザーには、そのユーザーの所属先ユーザー グループに関連付けられているアクセス権限が割り当てられます。

ユーザー ディスク割り当て
NTFS のクォータ管理サポートにより、追跡システムが強化されており、共有ストレージ ボリュームのディスク スペースの使用量を制御できます。Data Protector では、システム全体とすべての構成済みユーザーを対象にユーザー ディスク クォータを同時にバックアップします。

ユーザー プロファイル
(Windows 固有の用語)
ユーザー別に維持される構成情報。この情報には、デスクトップ設定、画面表示色、ネットワーク接続などが含まれます。ユーザーがログオンすると、そのユーザーのプロファイルがロードされ、Windows 環境がそれに応じて設定されます。

ライセンス集中管理
Data Protector では、複数のセルからなるエンタープライズ環境全体にわたってライセンスの集中管理を構成できます。すべての Data Protector ライセンスは、エンタープライズ Cell Manager システム上にインストールされます。ライセンスは、実際のニーズに応じてエンタープライズ Cell Manager システムから特定のセルに割り当てることができます。**MoM** *も参照。*

ライター
(MS VSS 固有の用語)
オリジナル ボリューム上のデータの変更を開始するプロセス。主に、永続的なデータをボリューム上に書き込むアプリケーションまたはシステム サービスがライターとなります。ライターは、シャドウ コピーの同期化プロセスにも参加し、データの整合性を保証します。

ライブラリ
オートチェンジャー、ジュークボックス、オートローダ、またはエクスチェンジャとも呼ばれます。ライブラリには、複数のレポジトリ スロットがあり、それらにメディアが格納されます。各スロットがメディア (DDS/DAT など) を 1 つずつ格納します。スロット / ドライブ間でのメディアの移動は、ロボット機構によって制御され、メディアへのランダム アクセスが可能です。ライブラリには、複数のドライブを格納できます。

リカバリ カタログ
(Oracle 固有の用語)
Recovery Manager が Oracle データベースについての情報を格納するために使用する Oracle の表とビューのセット。この情報は、Recovery Manager が Oracle データベースのバックアップ、復元、および復旧を管理するために使用されます。リカバリ カタログには、以下の情報が含まれます。

- Oracle ターゲット データベースの物理スキーマ
- データ ファイルおよび archivelog バックアップ セット
- データ ファイルのコピー
- アーカイブ REDO ログ
- ストアド スクリプト

リカバリ カタログ データベース
(Oracle 固有の用語)
リカバリ カタログ スキーマを格納する Oracle データベース。リカバリ カタログはターゲット データベースに保存しないでください。

リカバリ カタログ データベースへのログイン情報
(Oracle 固有の用語)
リカバリ カタログ データベース (Oracle) へのログイン情報の形式は <user_name>/<password>@<service> で、ユーザー名、パスワード、サービス名の説明は、Oracle ターゲット データベースへの Oracle SQL*Net V2 ログイン情報と同じです。ただし、この場合の <service> は Oracle ターゲット データベースではなく、リカバリ カタログ データベースに対するサービス名となります。

ここで指定する Oracle ユーザーは、Oracle のリカバリ カタログのオーナー (所有者) でなければならないことに注意してください。

リサイクル
メディア上のすべてのバックアップ データのデータ保護を解除して、以降のバックアップで上書きできるようにするプロセス。同じセッションに所属しているデータのうち、他のメディアに置かれているデータも保護解除されます。リサイクルを行っても、メディア上のデータ自体は変更されません。

リムーバブル記憶域の管理データベース
(Windows 固有の用語)
Windows サービスの 1 つ。リムーバブル メディア (テープやディスクなど) と記憶デバイス (ライブラリ) の管理に使用されます。リムーバブル記憶域により、複数のアプリケーションが同じメディア リソースを共有できます。

ローカル復旧とリモート復旧
リモート復旧は、SRD ファイルで指定されている Media Agent ホストがすべてアクセス可能な場合にのみ実行されます。いずれかのホストがアクセス不能になっていると、障害復旧プロセスがローカル モードにフェールオーバーされます。これは、ターゲット システムにローカル接続しているデバイスが検索されることを意味します。デバイスが 1 台しか見つからない場合は、そのデバイスが自動的に使用されます。複数のデバイスが見つかった

場合は、デバイスが選択できるプロンプトが表示され、ユーザーが選択したデバイスが復元に使用されます。

ロギング レベル

ロギング レベルは、バックアップまたはオブジェクトのコピー時にファイルとディレクトリに関する情報をどの程度まで詳細に IDB に記録するかを示します。バックアップ時のロギング レベルに関係なく、データの復元は常に可能です。Data Protector には、[すべてログに記録]、[ディレクトリ・レベルまでログに記録]、[ファイル・レベルまでログに記録]、および [ログなし] の 4 つのロギング レベルがあります。ロギング レベルの設定によって、IDB のサイズ増加、バックアップ速度、復元対象データのブラウズしやすさが影響を受けます。

ログイン ID

(MS SQL Server 固有の用語)

ユーザーが Microsoft SQL Server にログオンするための名前。Microsoft SQL Server の syslogin システム テーブル内のエントリに対応するログイン ID が有効なログイン ID となります。

ロック名

別のデバイス名を使うことで同じ物理デバイスを違う特性で何度も構成することができます。

そのようなデバイス (デバイス名) が複数同時に使用された場合に重複を防ぐ目的で、デバイス構成をロックするためにロック名が使用されます。ロック名はユーザーが指定する文字列です。同一の物理デバイスを使用するデバイス定義には、すべて同じロック名を使用します。

論理ログ ファイル

論理ログ ファイルは、変更されたデータがディスクにフラッシュされる前に書き込まれるファイルです。オンライン データベース バックアップの場合に使用されます。障害発生時には、これらの論理ログ ファイルを使用することで、コミット済みのトランザクションをすべてロールフォワードするとともに、コミットされていないトランザクションをロールバックすることができます。

ワイルドカード文字

1 文字または複数文字を表すために使用できるキーボード文字。たとえば、通常、アスタリスク (*) は 1 文字以上の文字を表し、疑問符 (?) は 1 文字を示します。ワイルドカード文字は、名前により複数のファイルを指定するための手段としてオペレーティング システムで頻繁に使用されます。

記号

A

B

C

D

索引

き

く

す