HP Data Protector 7.00
コンセプトガイド

HP 部品番号: N/A
2012 年 8 月
第 2 版

目次

出版履歴

次の版が発行されるまでの間に、間違いの訂正や製品マニュアルの変更を反映したアップデート版が発行されることもあります。アップデート版や新しい版を確実に入手するためには、対応する製品のサポートサービスにご登録ください。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

製品番号	ガイド版	製品
B6960-96035	2008 年 11 月	Data Protector リリース A.06.10
B6960-90151	2009 年 9 月	Data Protector リリース A.06.11
N/A	2011 年 3 月	Data Protector リリース 6.20
N/A	2012 年 3 月	Data Protector リリース 7.00
N/A	2012 年 7 月	Data Protector リリース 7.00。次のいずれかのパッチバンドルで提供: DPWINBDL_00701、DPUXBDL_00701、DPLNXBDL_00701

本書について

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

対象読者

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

ドキュメントセット

その他のガイドおよびヘルプには、関連情報が記載されています。

ガイド

Data Protector のガイドは、電子的な 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 の場合は英語のドキュメント（ガイド、ヘルプ）コンポーネントを、UNIX の場合は `OB2-DOCS` コンポーネントを、それぞれ選択してインストールします。ガイドのインストール後の保存先ディレクトリは、*`Data_Protector_home`*`\docs`(Windows) または `/opt/omni/doc/C`(UNIX) です。

これらの資料は、HP サポート Web サイトの [Manuals] ページから入手できます。

http://support.openview.hp.com/selfsolve/manuals

[Storage] セクションの **[Storage Software]** をクリックし、ご使用の製品を選択してください。

- 『HP Data Protector コンセプトガイド』

  このガイドでは、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。これは、タスクごとのヘルプとともに使用するように作成されています。

- 『HP Data Protector インストールおよびライセンスガイド』

  このガイドでは、Data Protector ソフトウェアのインストール方法をオペレーティングシステムおよび環境のアーキテクチャごとに説明しています。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 Data Protector トラブルシューティングガイド』

  このガイドでは、Data Protector の使用中に起こりうる問題に対するトラブルシューティングの方法について説明します。

- 『HP Data Protector ディザスタリカバリガイド』

  このガイドでは、ディザスタリカバリの計画、準備、テスト、および実行の方法について説明します。

- 『HP Data Protector インテグレーションガイド』

  このガイドでは、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および復元するための、Data Protector の構成方法および使用法を説明します。このガイドは、バックアップ管理者やオペレータを対象としています。6 種類のガイドがあります。

  - 『HP 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、SharePoint Server、Exchange Server』

    このガイドでは、Microsoft SQL Server、Microsoft SharePoint Server、Microsoft Exchange Server といった Microsoft アプリケーションに対応する Data Protector の統合ソフトウェアについて説明します。

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

  このガイドでは、Oracle Server、SAP R/3、SAP MaxDB 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 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』

  このガイドでは、Informix Server、IBM DB2 UDB、Lotus Notes/Domino Server といった IBM アプリケーションに対応する Data Protector の統合ソフトウェアについて説明します。

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

  このガイドでは、Sybase Server、HP Network Node Manager、Network Data Management Protocol Server に対応する HP の統合ソフトウェアについて説明します。

- 『HP Data Protector インテグレーションガイド - 仮想環境』

  このガイドでは、Data Protector と仮想環境 (VMware 仮想インフラストラクチャ、VMware vSphere、VMware vCloud Director、Microsoft Hyper-V、および Citrix XenServer) との統合について説明します。

- 『HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service』

  このガイドでは、Data Protector と Microsoft ボリュームシャドウコピーサービスの統合について説明します。また、ドキュメントアプリケーションライターの詳細についても説明します。

- 『HP Data Protector Integration Guide for HP Operations Manager for UNIX』

  このガイドでは、UNIX 版の HP Operations Manager と HP Service Navigator を使用して、Data Protector 環境の健全性と性能を監視および管理する方法について説明します。

- 『HP Data Protector Integration Guide for HP Operations Manager for Windows』

  このガイドでは、Windows 版の HP Operations Manager を使用して、Data Protector 環境の健全性と性能を監視および管理する方法について説明します。

- 『HP Data Protector ゼロダウンタイムバックアップコンセプトガイド』

  このガイドでは、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 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 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』とあわせてお読みください。

- 『HP Data Protector ゼロダウンタイムバックアップ管理者ガイド』

  このガイドでは、HP P4000 SAN ソリューション、HP P6000 EVA ディスクアレイファミリ、HP P9000 XP ディスクアレイファミリ、HP P10000 Storage Systems、EMC Symmetrix Remote Data Facility および TimeFinder に対応する Data Protector 統合ソフトウェアの構成方法および使用方法を説明します。このガイドは、バックアップ管理者やオペレータを対象としています。ファイルシステムと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 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』

  このガイドでは、Oracle Server、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server の各データベースに対して、そ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、標準復元を実行するための Data Protector の構成方法および使用方法について説明します。

- 『HP Data Protector Granular Recovery Extension User Guide for Microsoft Exchange Server』

  このガイドでは、Microsoft Exchange Server 2010 環境用の Granular Recovery Extension を構成し使用する方法について説明します。Microsoft Exchange Server 用の Data Protector Granular Recovery Extension のグラフィカルユーザーインタフェースは、Microsoft 管理コンソールに組み込まれます。このガイドは、Microsoft Exchange Server 管理者および Data Protector バックアップ管理者を対象としています。

- 『HP Data Protector Granular Recovery Extension ユーザーガイド - Microsoft SharePoint Server』

  このガイドでは、Microsoft SharePoint Server 用に Data Protector Granular Recovery Extension を構成し使用する方法について説明します。Data Protector Granular Recovery Extension は Microsoft SharePoint Server のサーバーの全体管理に組み込まれ、個々のアイテムをリカバリできるようになります。このガイドは、Microsoft SharePoint Server 管理者および Data Protector バックアップ管理者を対象としています。

- 『HP Data Protector Granular Recovery Extension User Guide for VMware vSphere』

  このガイドでは、VMware vSphere 用 Data Protector Granular Recovery Extension の構成方法および使用方法について説明します。Data Protector Granular Recovery Extension は VMware vCenter Server に組み込まれ、個々のアイテムをリカバリできるようになります。このガイドは、VMware vCenter Server ユーザーおよび Data Protector バックアップ管理者を対象としています。

- 『HP Data Protector Media Operations User Guide』

  このガイドは、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に、オフラインストレージメディアの追跡と管理に関する情報を提供します。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 Data Protector 製品案内、ソフトウェアノートおよびリファレンス』

  このガイドでは、HP Data Protector 7.00 の新機能について説明しています。また、インストール要件、必要なパッチ、制限事項、報告されている問題とその回避方法などの情報も記載されています。

- 『HP Data Protector Product Announcements, Software Notes, and References for Integrations to HP Operations Manager』

  このガイドは、HP Operations Manager 統合ソフトウェアに対して同様の機能を果たします。

- 『HP Data Protector Media Operations Product Announcements, Software Notes, and References』

  このマニュアルは、Media Operations に対して同様の機能を果たします。

- 『HP Data Protector Command Line Interface Reference』

  このガイドでは、Data Protector コマンドラインインタフェース、コマンドオプション、使用方法を、基本コマンドラインの例とともに説明しています。

ヘルプ

Data Protector は、Windows および UNIX の各プラットフォーム用にヘルプトピックとコンテキスト依存ヘルプ (F1 キー) を備えています。

Data Protector をインストールしていない場合でも、任意のインストール DVD-ROM の最上位ディレクトリからヘルプにアクセスできます。

Windows システムの場合: `DP_help.chm` を開きます。

UNIX システムの場合: 圧縮された tar ファイル `DP_help.tar.gz` をアンパックし、`DP_help.htm` 経由でヘルプシステムにアクセスします。

ドキュメントマップ

略称

次の表は、ドキュメントマップで使用される略称の説明です。ドキュメント項目のタイトルには、すべて先頭に「HP Data Protector」が付きます。

略称	ドキュメント項目
CLI	Command Line Interface Reference
Concepts	コンセプトガイド
DR	ディザスタリカバリガイド
GS	スタートガイド
GRE-Exchange	Granular Recovery Extension User Guide for Microsoft Exchange Server
GRE-SPS	Granular Recovery Extension ユーザーガイド - Microsoft SharePoint Server
GRE-VMware	Granular Recovery Extension User Guide for VMware vSphere
Help	ヘルプ
IG-IBM	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
IG-MS	インテグレーションガイド - Microsoft アプリケーション: SQL Server、SharePoint Server、Exchange Server
IG-O/S	インテグレーションガイド - Oracle、SAP
IG-OMU	Integration Guide for HP Operations Manager for UNIX
IG-OMW	Integration Guide for HP Operations Manager for Windows
IG-Var	インテグレーションガイド - Sybase、Network Node Manager、Network Data Management Protocol Server
IG-VirtEnv	インテグレーションガイド - 仮想環境
IG-VSS	Integration Guide for Microsoft Volume Shadow Copy Service
Install	インストールおよびライセンスガイド
MO-GS	Media Operations Getting Started Guide
MO-PA	Media Operations Product Announcements, Software Notes, and References
MO-UG	Media Operations User Guide
PA	製品案内、ソフトウェアノートおよびリファレンス
Trouble	トラブルシューティングガイド
ZDB-Admin	ZDB 管理者ガイド
ZDB-Concept	ZDB コンセプトガイド
ZDB-IG	ZDB インテグレーションガイド

対応表

以下の表は、各種情報がどのドキュメントに記載されているかを示したものです。セルが塗りつぶされているドキュメントを最初に参照してください。

	Help	GS	Concepts	Install	Trouble	DR	PA	インテグレーションガイド								ZDB			GRE			MO			
								MS	O/S	IBM	Var	VSS	VirtEnv	OMU	OMW	Concept	Admin	IG	Exchange	SPS	VMware	GS	UG	PA	CLI
バックアップ	X	X	X					X	X	X	X	X	X			X	X	X							
CLI																									X
概念/ 手法	X		X					X	X	X	X	X	X	X	X	X	X	X	X	X	X				
ディザスタリカバリ	X		X			X																			
インストール/ アップグレード	X	X		X			X							X	X							X	X		
インスタントリカバリ	X		X													X	X	X							
ライセンス	X			X			X																X		
制限事項	X				X		X	X	X	X	X	X	X					X						X	
新機能	X						X																	X	
プラニング方法	X		X													X									
手順/ 作業	X			X	X	X		X	X	X	X	X	X	X	X		X	X	X	X	X		X		
推奨事項			X				X									X								X	
必要条件				X			X	X	X	X	X	X	X	X	X							X	X	X	
復元	X	X	X					X	X	X	X	X	X				X	X	X	X	X				
サポートされる 構成																X									
トラブルシューティング	X			X	X			X	X	X	X	X	X	X	X		X	X	X	X	X				

統合ソフトウェア

以下のソフトウェアアプリケーションとの統合に関する詳細については、該当するガイドを参照してください。

ソフトウェアアプリケーション	ガイド
HP Network Node Manager(NNM)	IG-Var
HP Operations Manager	IG-OMU、IG-OMW
IBM DB2 UDB	IG-IBM
Informix Server	IG-IBM
Lotus Notes/Domino Server	IG-IBM
Media Operations	MO-UG
Microsoft Exchange Server	IG-MS、ZDB IG、GRE-Exchange
Microsoft Hyper-V	IG-VirtEnv
Microsoft SharePoint Server	IG-MS、ZDB-IG、GRE-SPS
Microsoft SQL Server	IG-MS、ZDB-IG
Microsoft ボリュームシャドウコピーサービス (VSS)	IG-VSS
ネットワークデータ管理プロトコル (NDMP) サーバー	IG-Var
Oracle Server	IG-O/S、ZDB-IG
SAP MaxDB	IG-O/S
SAP R/3	IG-O/S、ZDB-IG

ソフトウェアアプリケーション	ガイド
Sybase Server	IG-Var
VMware vSphere	IG-VirtEnv、GRE-VMware
VMware vCloud Director	IG-VirtEnv

以下のディスクアレイシステムファミリとの統合に関する詳細については、該当するガイドを参照してください。

ディスクアレイファミリ	ガイド
EMC Symmetrix	すべての ZDB
HP P4000 SAN ソリューション	ZDB-Concept、ZDB-Admin、IG-VSS
HP P6000 EVA ディスクアレイファミリ	すべての ZDB、IG-VSS
HP P9000 XP ディスクアレイファミリ	すべての ZDB、IG-VSS
HP P10000 Storage Systems	ZDB-Concept、ZDB-Admin、IG-VSS

表記上の規則および記号

表 2 表記上の規則

規則	要素
青色のテキスト: 「表記上の規則」 (15 ページ)	クロスリファレンスリンクおよび電子メールアドレス
青色の下線付きテキスト: http://www.hp.com	Web サイトアドレス
太字テキスト	• 押すキー • ボックスなど GUI 要素に入力するテキスト • メニュー、リストアイテム、ボタン、タブ、およびチェックボックスなどクリックまたは選択する GUI 要素
斜体テキスト	テキスト強調
等幅テキスト	• ファイルおよびディレクトリ名 • システム出力 • コード • コマンド、引数、および引数の値
等幅、斜体テキスト	• コード変数 • コマンド変数
等幅、太字テキスト	強調された等幅テキスト

△ **注意:** 指示に従わなかった場合、機器設備またはデータに対して、損害をもたらす可能性があることを示します。

重要: 詳細情報または特定の手順を示します。

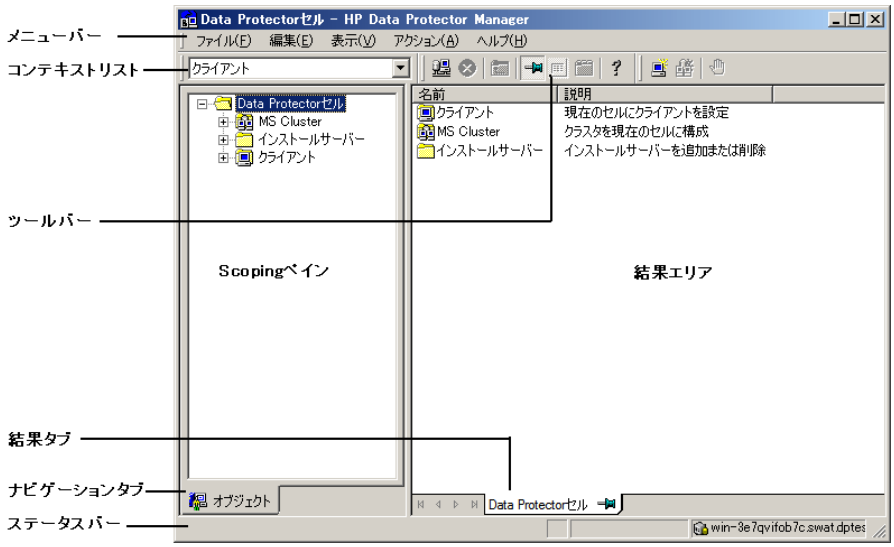
注記: 補足情報を示します。

ヒント: 役に立つ情報やショートカットを示します。

Data Protector グラフィカルユーザーインタフェース

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。オリジナルの Data Protector GUI(Windows のみ) または Data Protector Java GUI を使用できます。Data Protector グラフィカルユーザーインタフェースに関する詳細は、『HP Data Protector ヘルプ』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



一般情報

Data Protector に関する一般的な情報は、http://www.hp.com/go/dataprotector にあります。

HP テクニカルサポート

各国のテクニカルサポート情報については、以下のアドレスの HP サポート Web サイトを参照してください。

http://www.hp.com/support

HP に問い合わせる前に、以下の情報を集めておいてください。

- 製品のモデル名とモデル番号
- 技術サポートの登録番号 (ある場合)
- 製品のシリアル番号
- エラーメッセージ
- オペレーティングシステムのタイプとリビジョンレベル
- 詳細な質問内容

メールニュース配信サービス

ご使用の製品を以下のアドレスのメールニュース配信登録 Web サイトで登録することをお勧めします。

http://www.hp.com/go/e-updates

登録すると、製品の強化機能内容、ドライバの新バージョン、ファームウェアのアップデートなどの製品リソースに関する通知が電子メールで届きます。

HP Web サイト

その他の情報については、次の HP Web サイトを参照してください。

- http://www.hp.com
- http://www.hp.com/go/software
- http://support.openview.hp.com/selfsolve/manuals
- http://www.hp.com/support/downloads

1 バックアップと Data Protector

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。

Data Protector について

HP 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、事実上どのような構成でも実装することが可能です。さらに、Data Protector では、合成バックアップやディスクステージングなどの、バックアップ分野の高度な概念を利用することができます。

- **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。複数のバックアップ環境を単一のシステムから管理することも可能です。また、Data Protector にはコマンドラインインタフェース (CLI) も用意されているので、スクリプトを使用して Data Protector を管理することもできます。

- **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ます。さらに、ローカルバックアップ、ネットワークバックアップ、オンラインバックアップ、ディスクイメージバックアップ、合成バックアップ、オブジェクトミラーリングを伴うバックアップ、並列データストリームの組み込みサポートなど、多様なバックアップがサポートされるため、ユーザー要件に最適なバックアップを実行できます。

- **データの安全性**

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

- **混合環境のサポート**

  Data Protector は異機種環境をサポートしており、大部分の機能は UNIX プラットフォームと Windows プラットフォームで共通です。UNIX および Windows Cell Manager では、サポート対象のクライアントプラットフォームをすべて制御できます。Data Protector ユーザーインタ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。サポートされるプラットフォームの一覧は、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

- **混合環境におけるインストールの容易性**

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

- **高可用性のサポート**

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

  - クラスターとの統合によりフェイルセーフオペレーションを確実に実行し、仮想ノードのバックアップにも対応。サポート対象クラスターの一覧は、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。
  - クラスター上で Data Protector Cell Manager 自体の実行が可能。
  - 一般に使用されている、すべてのオンラインデータベースのアプリケーションプログラミングインタフェース (API) をサポート。
  - EMC Symmetrix、HP P6000 EVA ディスクアレイファミリ、HP P9000 XP ディスクアレイファミリ、HP P4000 SAN ソリューションなどの高度な高可用性ソリューションとの統合が可能。
  - Windows および UNIX の各プラットフォーム上で、さまざまなディザスタリカバリ機能を提供。
  - バックアップの実行中および実行後にバックアップデータを複製するためのメソッドを提供。この機能により、バックアップのフォールトトレランスの強化やデータの二重化が容易になります。

- **バックアップオブジェクト操作**

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

- **復元の容易性**

  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。たとえば、あるバックアップデータをいつまで復元可能な状態で保持する必要があるかといった点や、どのメディアがバックアップ用として (再) 利用可能かといった点をトラッキングしています。

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

- **サービス管理**

  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。

- **監視、レポート、および通知機能**

  Web を使用する幅広い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、UINX または Windows を実行しているシステム上で Data Protector GUI または Data Protector CLI を使用して生成でき、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。

  レポートは、特定の時間に生成されるようにスケジュール設定することもできれば、事前定義のイベント (バックアップセッションの終了やマウント要求など) に関連付けて設定することもできます。

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

- **オンラインアプリケーションとの統合**

  Data Protector は、Microsoft Exchange Server、Microsoft SQL Server、Microsoft SharePoint Server、Oracle、Informix Server、SAP R/3、SAP MaxDB、Lotus Notes/Domino Server、IBM DB2 UDB、Sybase のデータベースオブジェクト、VMware Virtual Infrastructure オブジェクト、および Hyper-V オブジェクトに対するオンラインバックアップ機能を備えています。個々のオペレーティングシステムでサポートされているバージョンの一覧は、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

- **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 Data Protector のホームページでご確認ください。http://support.openview.hp.com/selfsolve/manuals

バックアップと復元の概要

この項では、バックアップと復元についてそれぞれの基礎的な概念を説明します。

バックアップとは

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

バックアップをわかりやすく抽象化すると、「バックアッププロセス」 (21 ページ) のような形になります。

図 2 バックアッププロセス

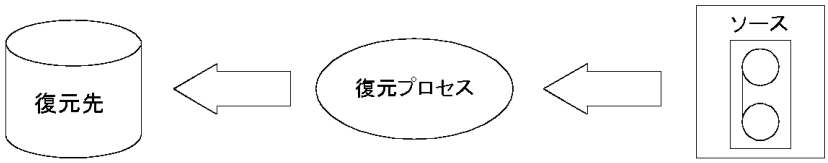
通常**ソース**となるのは、ファイル、ディレクトリ、データベース、アプリケーションなど、ディスク上のデータです。作成したバックアップをディザスタリカバリ用として使用する場合は、一貫性のある形でバックアップデータを作成することが大切です。

バックアップアプリケーションとは、バックアップ先に実際にデータをコピーするソフトウェアのことです。また**バックアップ先**とは、テープドライブのような、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 3 復元プロセス

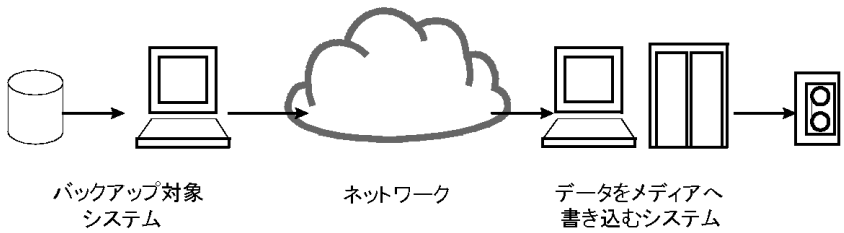


復元プロセスの**ソース**はバックアップコピーです。また復元アプリケーションとは、復元先に実際にデータを書き込むソフトウェアのことです。**復元先**は通常、オリジナルデータの書き込み先となるディスクです。

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 4 ネットワークバックアップ



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

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

  これにより、コスト削減を目的として、ローカルバックアップ (大容量データを格納したシステム用) とネットワークバックアップの両方を実行することが可能となります。

- 任意のネットワークパスに、バックアップデータフローを経路指定できること。
- データ量またはネットワークトラフィックが原因で LAN 転送の効率が悪い場合は、バックアップデータの転送経路を LAN から SAN に変更できること。
- 任意のシステムからバックアップ活動を管理できること。
- IT 管理の枠組みに統合できること。
- さまざまなタイプのバックアップ対象システムをサポートできること。

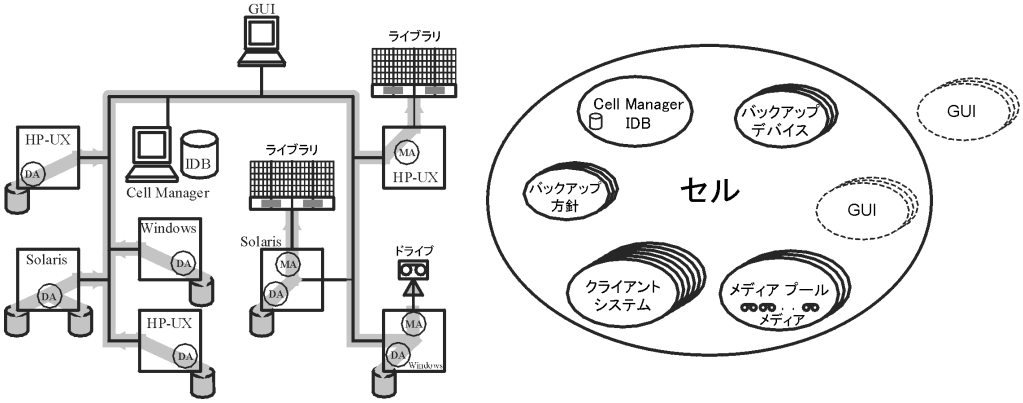
Data Protector アーキテクチャ

Data Protector では、**セル** (「Data Protector セル (物理的な構成図と論理的な構成図)」 (22 ページ) 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 5 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 システムは、UNIX および Windows の各オペレーティングシステム上で実行できます。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 Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

Cell Manager

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

バックアップ対象のシステム

クライアントシステム には、Data Protector Disk Agent (DA) をインストールしておく必要があります (DA は、**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が接続されているシステム

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、**ドライブサーバー**とも呼ばれます。バックアップデバイスは、Cell Manager だけでなく、どのシステムにでも接続できます。Media Agent は、デバイス内のメディアからデータを読み取って Disk Agent に渡したり、Disk Agent から受け取ったデータをメディアに書き込んだりする働きをします。

ユーザーインタ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、たとえば 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。

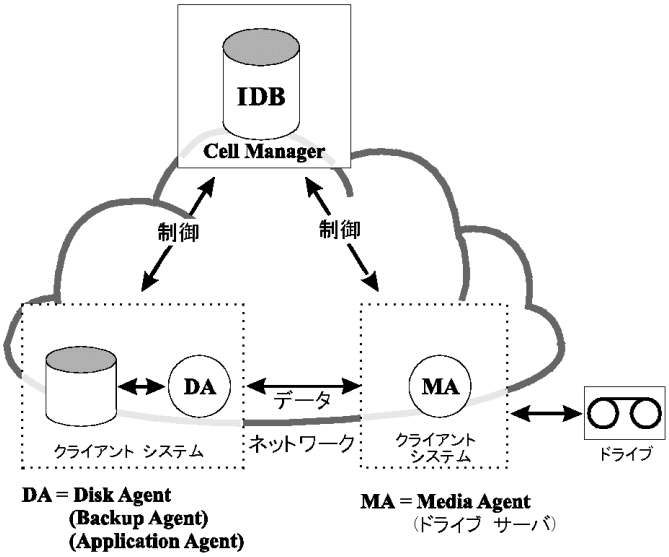
インストールサーバー

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

セル内の処理

「バックアップ処理および復元処理」 (24 ページ) に示すとおり、バックアップセッションおよび復元セッションは、Data Protector Cell Manager により制御され、これらのセッション内でバックアップおよび復元に必要なすべての処理が実行されます。

図 6 バックアップ処理および復元処理



バックアップセッション

バックアップセッションとは

「バックアップセッション」 (24 ページ) に示すバックアップセッションとは、記憶メディア上にデータのコピーを作成するプロセスを指します。バックアップセッションは、オペレータが 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。

説明

バックアップの実行時には、バックアップセッションマネージャープロセスが、Media Agent と Disk Agent をそれぞれ 1 つまたは複数開始して、セッションを制御し、生成されたメッセージを IDB に書き込みます。データは Disk Agent によって読み取られた後、Media Agent に渡されてメディア内に保存されます。

図 7 バックアップセッション

通常のバックアップセッションは、「バックアップセッション」 (24 ページ) よりも複雑になります。通常は複数の Disk Agent によって複数のディスクから並列にデータが読み取られ、1 つまたは複数の Media Agent にそのデータが渡されます。複雑なバックアップセッションの詳細は、「Data Protector が機能する仕組み」 (153 ページ) を参照してください。

復元セッション

復元セッションとは

「復元セッション」 (25 ページ) 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。

説明

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

図 8 復元セッション

通常の復元セッションは、「復元セッション」 (25 ページ) よりも複雑になります。復元セッションの詳細は、「Data Protector が機能する仕組み」 (153 ページ) を参照してください。

企業環境

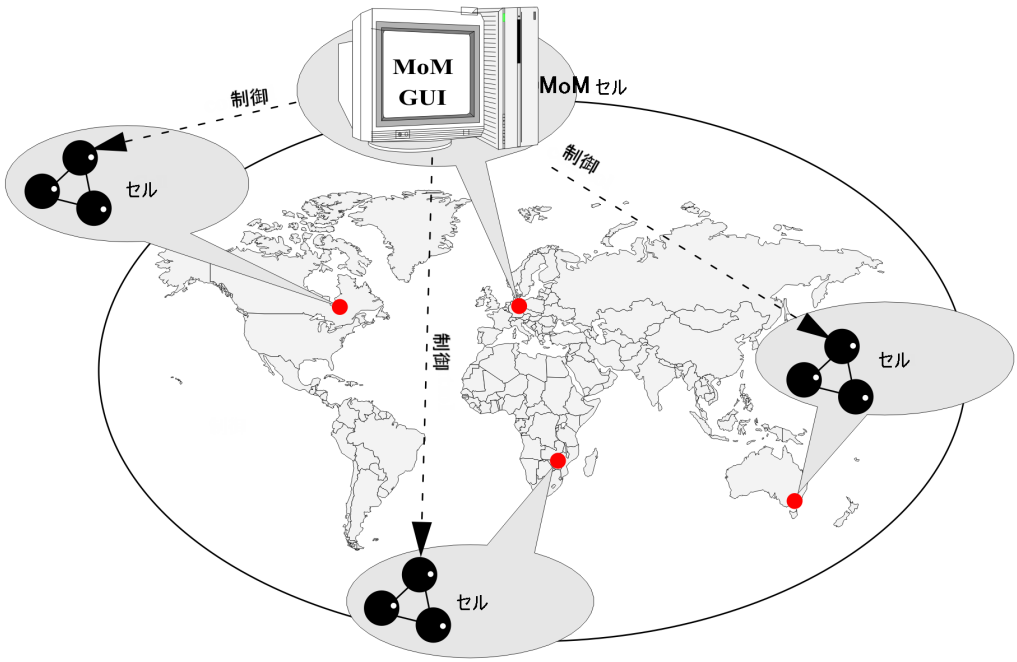
企業環境とは

「世界規模の Data Protector 企業環境」 (26 ページ) に示すように、一般に企業のネットワーク環境は、さまざまなベンダー製品を含む多数のシステムで構成されており、各種オペレーティングシステムが使用されています。また、これらのシステムが、時間帯の異なるさまざまな地域に配置されていることもあります。これらのシステムは、さまざまな通信速度の LAN または WAN ネットワークによって相互に接続されています。

導入が必要となる場合

このガイドで説明するソリューションは、地理的に離れている複数のサイトに共通の**バックアップ方針**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 9 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、「MoM」 (27 ページ) を参照してください。

環境内を複数セルに分割する

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

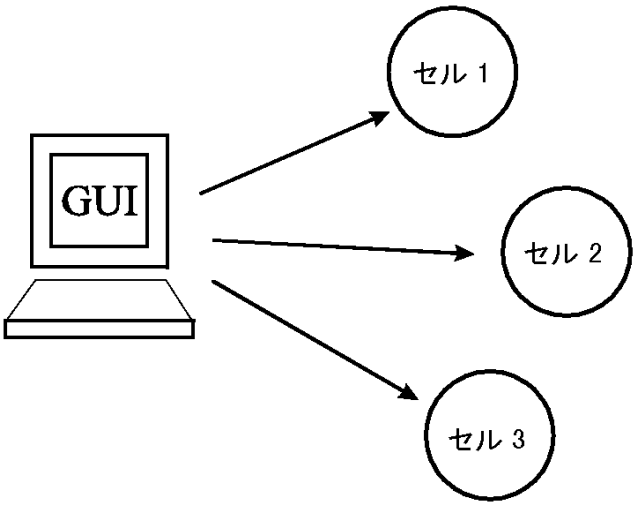
分割が必要となる場合

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

環境計画時の留意事項の一覧は、「バックアップ戦略の計画」 (34 ページ) 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 10 複数セルを一元管理

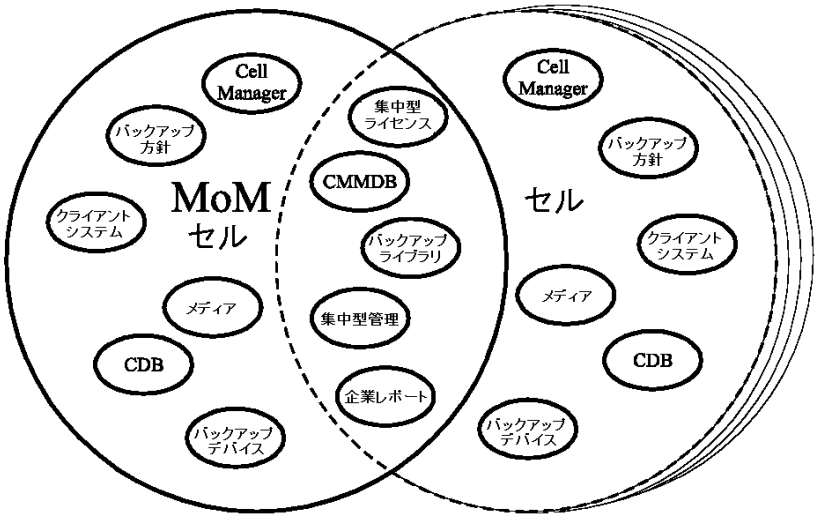


MoM

Data Protector には、複数セルに分かれた大規模環境を管理するために、Manager-of-Managers (MoM) と呼ばれる機能が用意されています。この MoM 機能を使用すると、複数のセルを MoM 環境と呼ばれる 1 つの大きな単位にまとめて、一元管理することができます (「複数セルを一元管理」 (27 ページ) 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 11 Manager-of-Managers 環境



Manager-of-Managers は、以下の機能を提供します。

- **集中型のライセンスレポジトリ**

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

- **メディア集中管理データベース (CMMDB)**

  CMMDB 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、たとえばあるセルから、別のセル内のシステムに接続された複数デバイスを制御できるロボティクスを使用することも可能です。Disk Agent から Media Agent へのデータパスも、セルの境界に制約されません。

- **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または自動的に作成できます。
- メディアボールティング (安全な場所でのメディアの保管機能) がサポートされています。

メディアプールとは

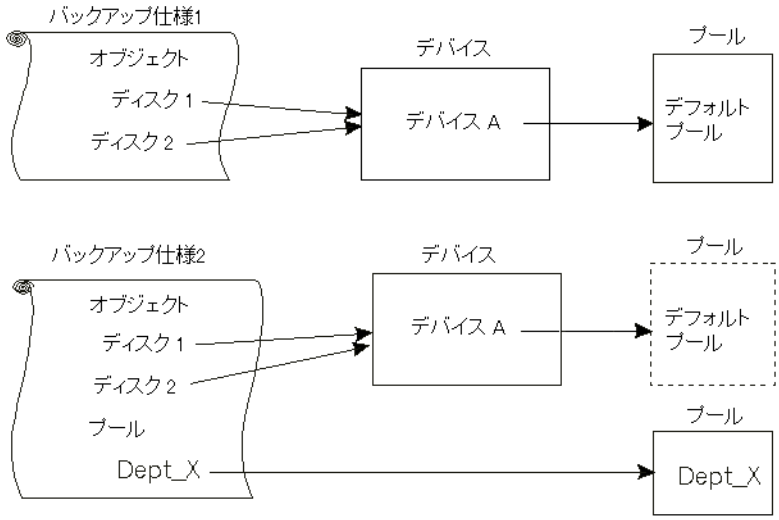
Data Protector では、多数のメディアを管理するためにメディアプールを使用します。メディアプールとは、使用方針 (プロパティ) が共通であり、かつ物理タイプが**同じ**であるメディアの論理的な集まりのことです。メディアの使用方針は、メディア上に保存されているデータに応じて決定します。メディアプールの構造やサイズに加え、プール内に保存するデータのタイプは、ユーザーが自由に設定できます。

デバイス構成時には、デフォルトのメディアプールが指定されます。バックアップ仕様の中でメディアプールを指定しなければ、このデフォルトのメディアプールが使用されます。

バックアップデバイス

Data Protector では各デバイスを、デフォルトプールなどの使用プロパティが個々に定義された物理デバイスとして、定義およびモデリングします。このようなデバイス概念の使用や、バックアップ仕様などにより、Data Protector ではデバイスとその使用方針を容易にかつ柔軟に構成することができます。バックアップデバイスの定義は、Data Protector メディア管理データベース内に保存されています。

図 12 バックアップ仕様、デバイス、およびメディアプールの関連



「バックアップ仕様、デバイス、およびメディアプールの関連」(29 ページ) は、バックアップ仕様、デバイス、およびメディアプールの関連を示したものです。各デバイスは、バックアップ仕様の中で指定されています。各デバイスはメディアプールにリンクされており、バックアップ仕様でこのメディアプールを変更することも可能です。たとえば上図のバックアップ仕様 2 は、デフォルトプールではなく `Dept_X` プールを参照しています。

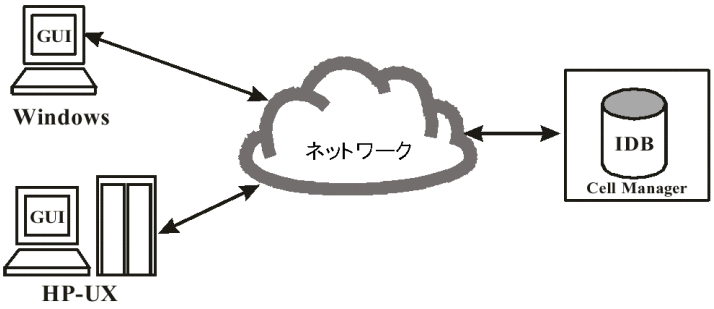
Data Protector は、多種多様なデバイスをサポートしています。詳細については、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

ユーザーインタフェース

Data Protector では、Windows や UNIX のプラットフォーム上で Data Protector GUI を使用して、すべての構成作業および管理作業を簡単に利用できます。オリジナルの Data Protector GUI (Windows) または Data Protector Java GUI (Windows および UNIX) を使用できます。同じコンピュータで両方のユーザーインタフェースを同時に実行できます。また、コマンドラインインタフェース (CLI) は UNIX と Windows のいずれのプラットフォームでも使用できます。

Data Protector のアーキテクチャ上、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。ユーザーインタフェースは、Cell Manager システムから使用する必要はありません。デスクトップシステム上にインストールすることができます。「Data Protector ユーザーインタフェースの使用」(30 ページ) に示すように、このユーザーインタフェースがサポートされているプラットフォームであれば、Cell Manager を使って、Data Protector セルを特に意識することなく管理できます。

図 13 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 ProtectorGUI

「オリジナルの Data Protector GUI」 (30 ページ) に示すオリジナルの Data Protector GUI および「Data Protector Java GUI」 (31 ページ) に示す Data Protector Java GUI はいずれも、以下の機能を備えた使い易い強力なユーザー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 Server、Microsoft Exchange Server、SAP R/3、Oracle8 などや、UNIX 環境で実行される SAP R/3、Oracle8、Informix Server などのオンラインデータベースアプリケーションのバックアップを簡単に構成して管理できます。
- ヘルプトピックや状況依存ヘルプを含む包括的なヘルプシステムが用意されています。

図 14 オリジナルの Data Protector GUI

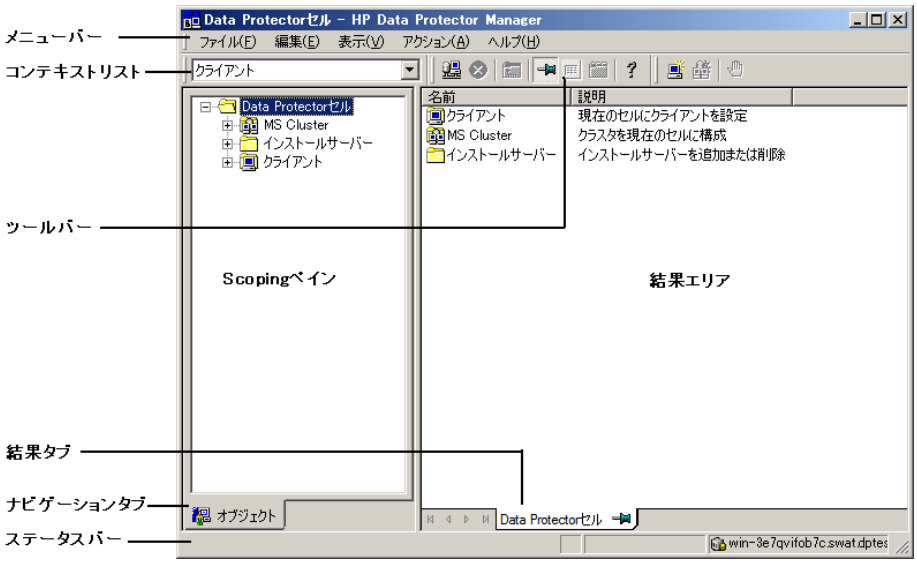
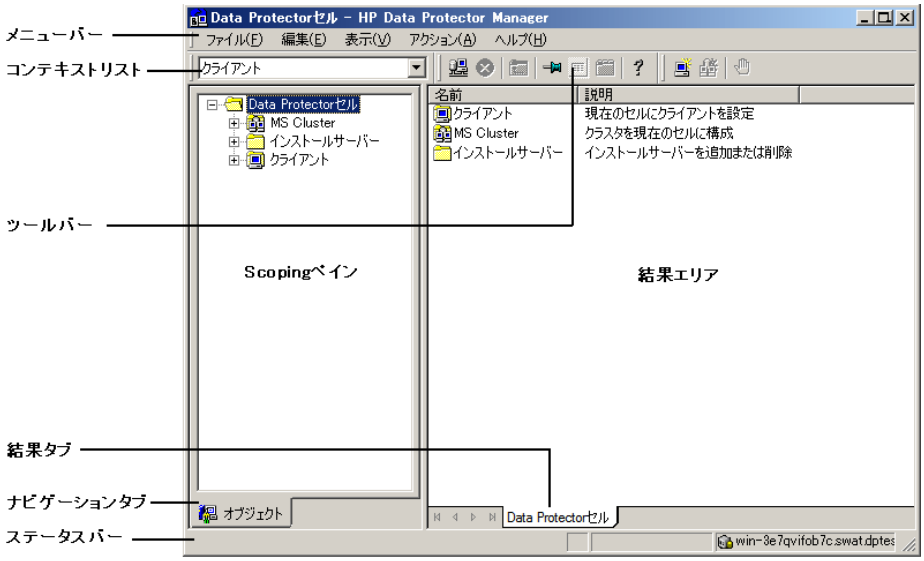


図 15 Data Protector Java GUI

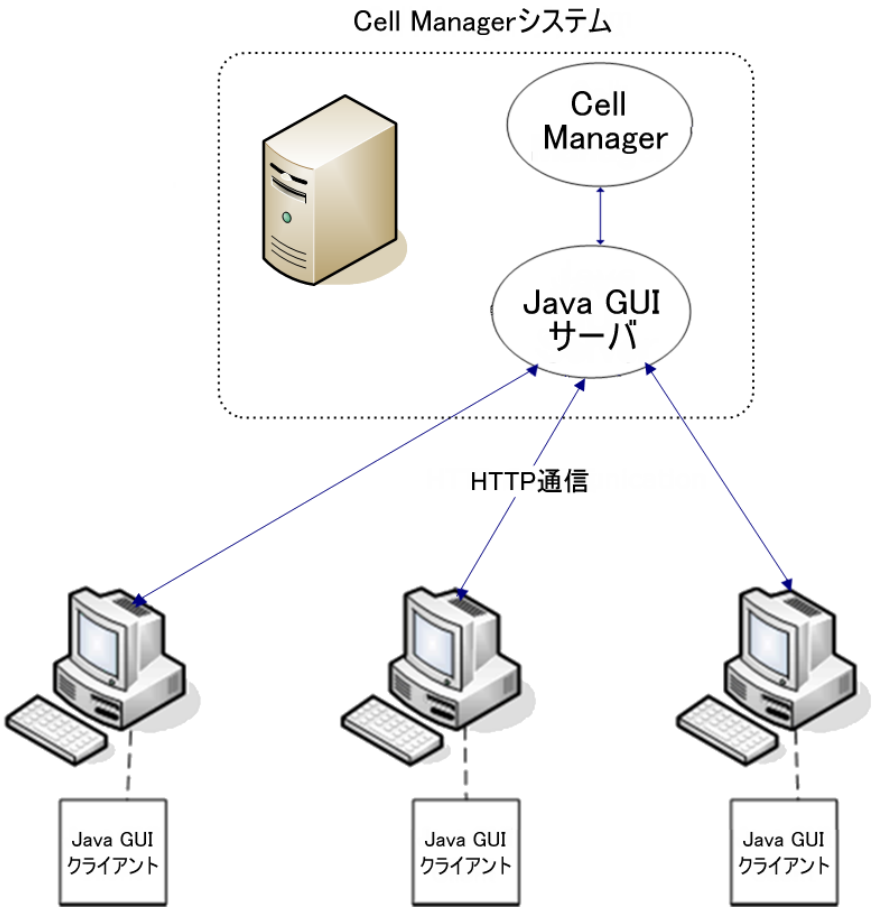


Data Protector Java GUI

Data Protector Java GUI は Java ベースのグラフィカルユーザーインタフェースで、クライアントサーバーアーキテクチャに対応します。オリジナルの Data Protector GUI と同じ概観のインタフェースでバックアップ管理を実行できます。

Java GUI は、Java GUI サーバーと Java GUI クライアントの 2 つのコンポーネントで構成されています。「Data Protector Java GUI のアーキテクチャ」 (32 ページ) では、これらのコンポーネントの関係を表しています。

図 16 Data Protector Java GUI のアーキテクチャ



Java GUI サーバー は、Data Protector Cell Manager システムにインストールします。Java GUI サーバーは、Java GUI クライアントからの要求を受け取って処理し、応答を Java GUI クライアントに戻します。

Java GUI クライアント にはユーザーインタフェース関連の機能のみが搭載されており、Java GUI サーバーに接続しなければ動作しません。

Data Protector のセットアップ作業の概要

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

1. ネットワーク構造と編成構造を分析します。どのシステムのバックアップが必要であるかを判断します。
2. Microsoft Exchange、Oracle、IBM DB2 UDB、SAP R/3 など、バックアップする必要がある特別なアプリケーションおよびデータベースがあるかどうかを確認します。Data Protector には、これらの製品に特化した統合機能が備わっています。詳細については、『HP Data Protector インテグレーションガイド』を参照してください。
3. Data Protector セルの構成について、以下のような点を決定します。
   - Cell Manager となるシステム
   - ユーザーインタ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。この結果、インストールに必要なパスワードを取得できます。

   別のやり方として、一時パスワードを使用して Data Protector を操作することも可能です。ただし、このパスワードはインストール後 60 日間のみ有効です。詳細は、『HP 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. セキュリティ面について考慮します。
   - セキュリティ留意事項を分析します。『HP 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。
   - どのユーザーグループを構成する必要があるかを考慮します。
   - 暗号化形式のメディアにデータを書き込んでセキュリティを強化します。
   - 暗号制御通信を有効にして、不正なアクセスの防止に役立ちます。
6. バックアップの構造について決定します。
   - どのようなメディアプールを定義し、どのように使用するか。
   - どのデバイスをどのように使用するか。
   - 各バックアップデータのコピーはそれぞれいくつ必要か。
   - いくつのバックアップ仕様を作成し、どのようにグループ化するか。
   - ディスクへのバックアップを計画している場合、合成バックアップやディスクステージングなどのアドバンストバックアップ戦略を検討する。
7. Data Protector 環境をインストールして構成します。
   - Data Protector Cell Manager システムをインストールし、Data Protector のユーザーインタ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。
   - 失敗したバックアップの処理
   - 復元処理の実行
   - バックアップデータのコピーとメディアのボールティング
   - ディザスタリカバリの準備
   - IDB の保守

2 バックアップ戦略の計画

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

バックアップ戦略の計画

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

バックアップ戦略の計画とは

バックアップ戦略の計画手順は、以下のとおりです。

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

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

バックアップ戦略における要件の明確化

バックアップ戦略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戦略は、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 サーバー、大容量リレーショナルデータベースなど)。

- 復旧までに許される最大ダウンタイム

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

  復旧までの時間は、主として、メディアにアクセスするための時間と、ディスク上に実際にデータを復元するための時間に分かれます。完全なシステム復旧を行う場合は、より多

くの手順が必要となるため、さらに多くの時間がかかります。詳細は、「ディザスタリカバリ」 (94 ページ) を参照してください。

- 各タイプのデータの保管期間

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

- バックアップデータを保存したメディアの保管方法

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

- バックアップ時にデータを書き込むメディアセットの総数

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

- バックアップするデータの総量

  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。たとえば、100 人の従業員を新たに採用する計画がある場合には、ユーザー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。たとえば、ユーザーファイルについては、そのユーザーが使用していないときには、いつでもバックアップを実行できますが、トランザクションデータベースについては、バックアップ可能な時間帯が数時間程度しかないことが予想されます。

  またバックアップに要する時間は、実行するバックアップのタイプ、つまりフルバックアップを実行するか、増分バックアップを実行するかによっても異なります。詳細は、「フルバックアップ、増分バックアップ、合成バックアップ」 (59 ページ) 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。詳細は、『HP Data Protector インテグレーションガイド』を参照してください。

  ディスクにバックアップする場合は、合成バックアップとディスクステージングを活用することができます。これらの高度なバックアップ戦略により、バックアップに要する時間を大幅に短縮できます。詳細については、「合成バックアップ」 (63 ページ) および 「ディスクステージング」 (84 ページ) を参照してください。

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

- バックアップを実行する頻度

  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。たとえば、ユーザーの作業ファイルは 1 日に 1 回バックアップし、システムデータは週に 1 回だけバックアップし、一部のデータベーストランザクションについては 1 日に 2 回バックアップするといった方法が考えられます。

バックアップ戦略に影響する各種の要因

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

- 各企業におけるバックアップおよび保存に対する方針と要件
- 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

バックアップ戦略を構築する準備

バックアップ戦略を構築するには、以下の点を明らかにする必要があります。

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

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

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

  企業データの種類をリストアップし、バックアップ仕様の中でこれらのデータをどのように組み合わせるかを、バックアップが可能な時間枠も考慮して検討します。企業データは、企業のビジネスデータ、企業のリソースデータ、プロジェクトデータ、個人データなどに分類でき、データの種類別に個別の要件が存在します。
- バックアップ方針の実装
  - 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てください。これは、ネットワーク負荷、デバイス負荷、バックアップ可能な時間枠などに関する問題を軽減するために、クライアント (バックアップ仕様) ごとに日を変えてフルバックアップを実行するやり方です。

- メディア上のデータとバックアップ関連情報の保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が新しいデータで上書きされないように、一定期間保護するかどうかを検討します。この保護策はデータ保護と呼ばれ、セッションベースで実行されます。

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

- デバイスの構成

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

  バックアップするデータ量が多い場合は、以下の点を検討してください。

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

- メディア管理

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

  各バックアップ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

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

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

単一セルと複数セル

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

- バックアップ管理上の問題

  複数セルを使用すると、個々のセル内で、より柔軟な形で管理作業を実行できます。この場合、各セル内では、それぞれ完全に独立した方針でメディアやデバイスを管理できます。たとえば管理対象が複数のグループに分かれているような環境では、データセキュリティ上の理由により、これらのグループを 1 つのセル内にはまとめたくない可能性があり

ます。一方、複数セルに分割した場合の問題点としては、単一セルの場合に比べて管理作業が煩雑になり、場合によっては各セル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。推奨サイズを超えるセルがあると、そのセルの管理が煩雑になってしまいます。Data Protector クライアントからセルを編成して管理を効率化する方法については、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

- ネットワーク上の問題

  最大の性能を得るためには、同一セル内のすべてのクライアントシステムを、同一 LAN 上に配置する必要があります。ネットワーク構成などのその他のネットワークに関する詳細は、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。たとえば、メディア、バックアップデバイス、バックアップデータなどは、必ず 1 つのセルに所属します。ただし Data Protector では、複数のセル間でデバイスを共有したり、別のセルにメディアを移動したりすることも可能なため、個々のメディアに対する物理的なアクセス権は適切なユーザーのみに与えるようにしてください。

- 混合環境

  Data Protector では、多数のプラットフォームからなるクライアントシステムを 1 つのセルにバックアップすることができます。ただし場合によっては、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。たとえば、経理部門、IT 部門、製造部門別に、それぞれ専用のセルを設定できます。Data Protector を使用すると、このように環境内を複数セルに分割した場合であっても、これらのセル間で共通の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ーと Cell Manager

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

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

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

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

Windows 環境でのセルの作成

Windows では 2 種類の構成方法が存在するため (ドメインまたはワークグループ)、これらのシステムの管理者に対してはさまざまなレベルのサポートが用意されており、この点が、主としてインストール時における Data Protector のセットアップ方法に多少の影響を与える可能性があります。また重要な前提条件として、クリーンな形でノード名を解決したセットアップを行っておき、クライアントシステム同士が、完全修飾されたノード名を使用して互いにアクセスできるようにしておく必要があります。

Windows ドメイン

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

Data Protector セルと Windows ドメインの対応付け

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

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

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

Windows ワークグループ

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

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

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

混合環境でのセルの作成

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

地理的に離れているセル

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

地理的に離れているセルに関する注意点

地理的に離れたセルを構成する場合は、以下の点に注意する必要があります。

- WAN を介してデータを送信しないこと

  バックアップ対象クライアントシステムと使用するデバイスは、ローカルな形で構成しなければなりません。

- 各セルを、MoM 環境内に構成すること

  地理的に離れたセルを中央で一元管理するには、それらのセルを MoM 環境内に構成する必要があります。

- ユーザー構成を考慮すること

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

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

MoM 環境

MoM 環境では、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] を使用して、接続が切れた場合でも自動的に再確立されるようにしておきます。

性能に関する概要と計画上の注意点

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

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

インフラストラクチャ

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

ネットワークおよびサーバー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、ネットワークによっても性能が左右されます。Data Protector は、次の場合にデータストリームを別に処理します。

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

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

デバイス

デバイスの性能

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

データ転送速度は、ハードウェア圧縮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。

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

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

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

デバイス以外の高性能ハードウェア

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。

高度なパフォーマンス構成

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

ゼロダウンタイムバックアップの詳細については、『HP Data Protector ゼロダウンタイムバックアップコンセプトガイド』を参照してください。

ハードウェアを並行して使用する

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

並行使用が有効な場合

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

- 負荷調整

  これは Data Protector の機能であり、どのオブジェクト (ディスク) をどのデバイスにバックアップするかが Data Protector によって動的に決定されます。特に、動的環境において多数のファイルシステムをバックアップする場合は、この機能をオンに設定してください。詳細は、「負荷調整の仕組み」 (98 ページ) を参照してください。

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

バックアップと復元の構成

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

ソフトウェア圧縮

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

デフォルトでは、ソフトウェア圧縮は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する場合は、ハードウェア圧縮を無効化してください。両方の方法でデータを圧縮しようとすると、データのサイズが大きくなってしまいます。

ハードウェア圧縮

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

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

フルバックアップと増分バックアップ

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

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

ディスクイメージバックアップとファイルシステムバックアップ

従来は、ファイルシステムをバックアップするよりも、ディスクイメージ (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、「デバイスストリーミングと同時処理数」 (99 ページ) を参照してください。

ディスク性能

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

ただしオペレーティングシステムによっては、アクセスしたデータをいったん**キャッシュメモリー**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。

Windows システムでの Disk Agent の性能

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

SAN 性能

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

オンラインデータベースアプリケーションの性能

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

Data Protector とさまざまなアプリケーションとの統合や、バックアップ性能を向上させるテクニックについては、各『HP 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
- データの暗号化
- 暗号制御通信

セル

セッションの開始

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

特定の Cell Manager からのアクセス

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

実行前および実行後スクリプトの制限

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

Data Protector の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イン名、そのユーザーがログインに使用できるシステム、および所属する Data Protector ユーザーグループのメンバーシップを指定します。このメンバーシップにより、所属するユーザーの権限が決められます。

アカウントチェックのタイミング

ユーザー権限のチェックは、ユーザーが Data Protector ユーザーインタ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、「ユーザーとユーザーグループ」 (134 ページ) を参照してください。

Data Protector ユーザーグループ

ユーザーグループとは

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

ユーザーグループが必要な理由

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

詳細は、「ユーザーとユーザーグループ」 (134 ページ) 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。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。あるデータをバックアップおよび復元することは、本質的にはそのデータのコピーを作成するのと同じことです。

詳細は、「ユーザーとユーザーグループ」 (134 ページ) を参照してください。

バックアップデータの表示

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

他のユーザーからデータを隠す

バックアップの構成時には、そのデータを誰でも復元できるようにするか (public)、またはバックアップデータのオーナーしか復元できないようにするか (private) を指定できます。バックアップ オーナーの詳細については、「バックアップ所有権とは」 (47 ページ) を参照してください。

バックアップ所有権とは

誰がバックアップセッションを所有するのか

各バックアップセッションとその中でバックアップされたすべてのデータはオーナーに割り当てられます。このオーナーは、対話型のバックアップを開始するユーザー、CRS プロセスを実行しているアカウント、またはバックアップ仕様オプションでオーナーとして指定されるユーザーです。バックアップオーナーの指定方法については、『HP Data Protector ヘルプ』の索引「所有権」を参照してください。

バックアップ所有権と復元

バックアップ所有権は、データを参照および復元するユーザーの能力に影響します。オブジェクトがパブリックに設定されていない場合、そのメディアセット内に保存されているデータは、メディアセットのオーナーまたは管理者しか見ることができません。プライベートオブジェクトを参照および復元する権限は、**admin** 以外のグループにも与えることができます。プライベートオブジェクトの参照および復元が可能なユーザーについては、『HP Data Protector ヘルプ』の索引「所有権」を参照してください。

データの暗号化

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

Data Protector ソフトウェアの暗号化機能は **AES 256 ビット暗号化**といい、256 ビットの長さのランダムなキーを使用する AES-CTR (Advanced Encryption Standard in Counter Mode) の暗号化アルゴリズムを基盤としています。同一のキー が暗号化と複合化の両方に使用されます。データはネットワークを介して転送される前およびメディアに書き込まれる前に、AES256 ビット暗号化機能によって暗号化されます。

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

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

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

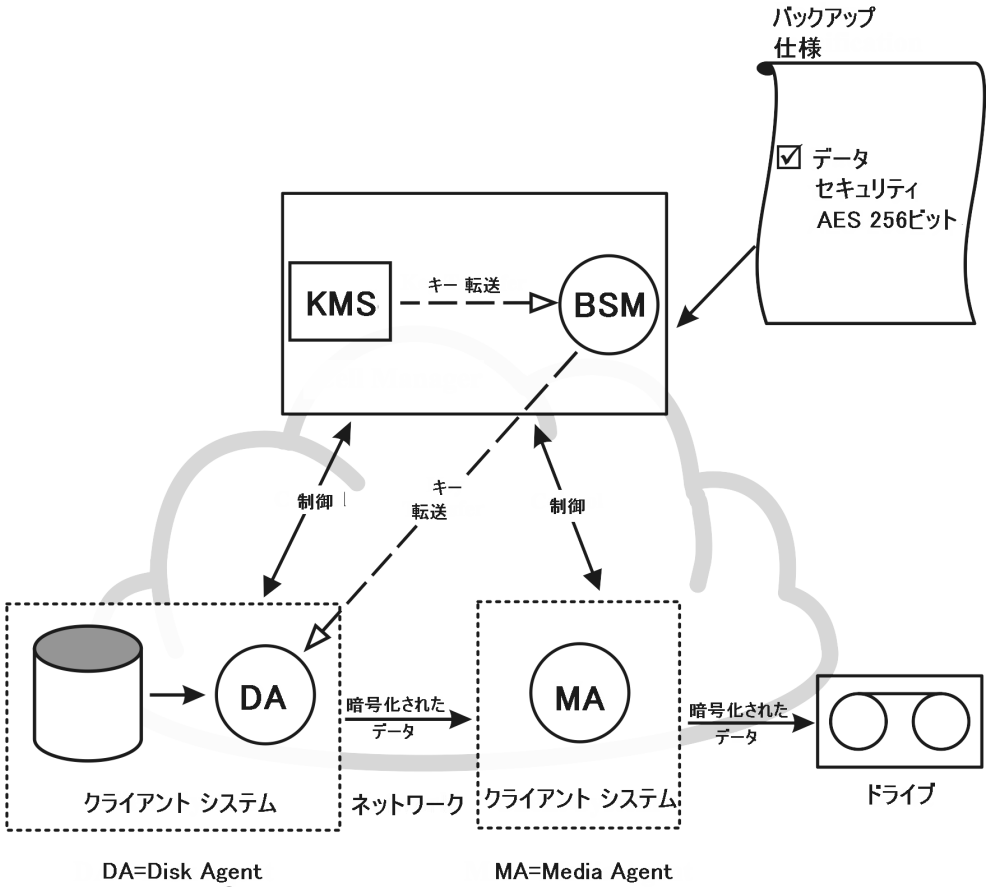
また、Data Protector では暗号化機能のほかに、この目的で使用できる組み込み型のアルゴリズム (キーなし) を使用する暗号化機能も備えています。

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

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

「AES 256 ビット暗号化を指定したバックアップセッション」 (49 ページ) では、[**AES 256-bit**] 暗号化オプションが選択されていて暗号化が行われるバックアップセッションの際の、基本的なやり取りを表しています。

図 17 AES 256 ビット暗号化を指定したバックアップセッション



Data Protector でのドライブベースの暗号化機能の仕組み

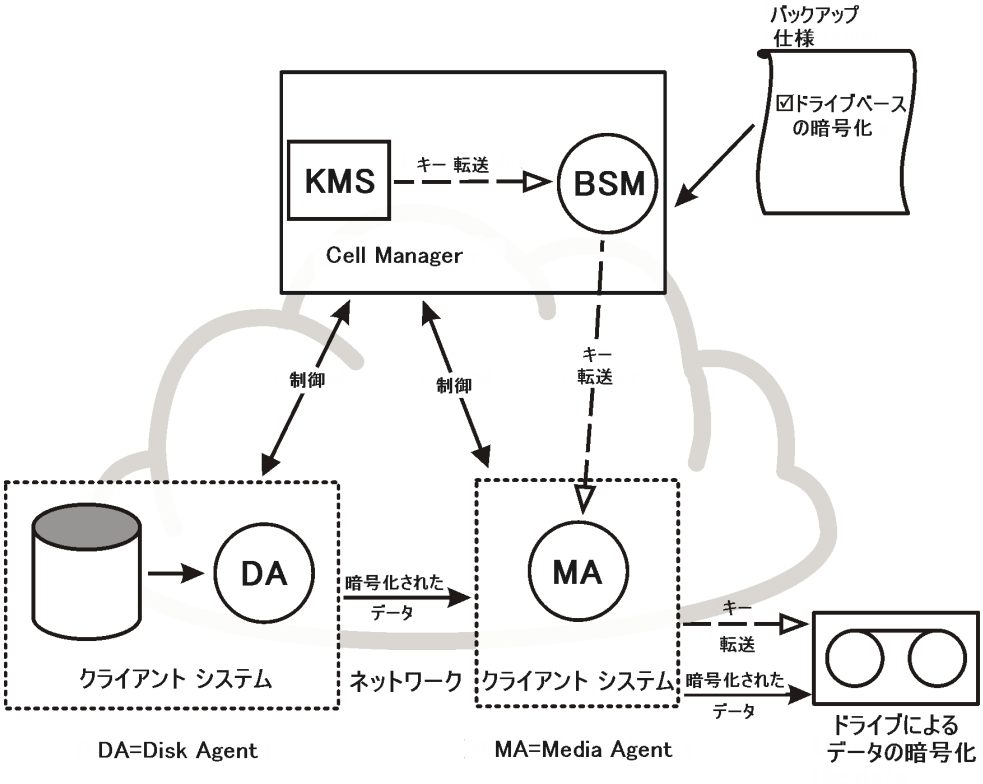
BSM で [**Drive based encryption**] オプションが選択されているバックアップ仕様を読み込み、KMS にアクティブな暗号化キーを要求します。キーが Media Agent (MA) に転送されます。ここで暗号化のためにドライブが構成され、ドライブに暗号化キーが設定されます。ドライブによってメディアに書き込まれるデータとメタデータの両方が暗号化されます。

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

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

「AES 256 ビット暗号化とドライブベース暗号化が指定されたバックアップセッション」(50 ページ) は、[**AES 256** ビット] 暗号化オプションと [ドライブベースの暗号化] オプションを選択した場合の暗号化されたバックアップセッション時における基本的なやり取りを示します。

図 18 AES 256 ビット暗号化とドライブベース暗号化が指定されたバックアップセッション



暗号化されたバックアップからの復元

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

暗号制御通信

不正なアクセスを防止する、Data Protector の暗号制御通信は、ネットワーク経由の通信にセキュリティを提供する暗号プロトコルの Secure Socket Layer (SSL) に基づいています。SSL は、ネットワーク通信のセグメントを暗号化し、既存の Data Protector 通信プロトコルをカプセル化します。

Data Protector セル内の制御通信は、Disk Agent(および統合用ソフトウェア) から Media Agent へのデータ転送とその逆方向のデータ転送を除く、Data Protector プロセス間のすべての通信です。Data Protector では、エクスポートグレード SSLv3 アルゴリズムを使用して、非対称暗号化の場合は最大 512 ビット鍵で、対称暗号化の場合は最大 64 ビット鍵で制御通信を暗号化します。SSL では、暗号化された通信を確立するための証明書が必要なため、Data Protector は、インストールまたはアップグレード時にデフォルトの証明書を提供しています。

Data Protector の暗号制御通信の仕組み

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、そ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。暗号化はクライアントごとに有効になります。つまり、暗号化は、選択されたクライアントとのすべての制御通信について有効または無効のどちらかになります。

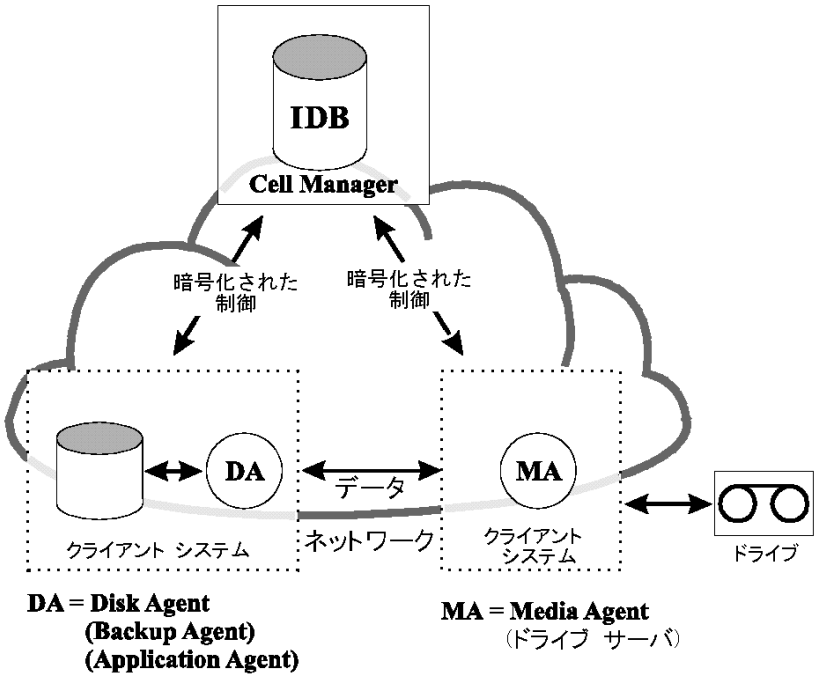
暗号化は、まず Cell Manager で有効にしてから、セル内のクライアントで有効にする必要があります。暗号化した通信を行わないクライアントは Cell Manager の例外リストに記述します。すると、そのクライアントの通信を非暗号化モードで行うことができます。Data Protector プロセスは接続を受け入れる前に、ローカル構成 (暗号化の有効/無効、使用する証明書など) をチェックします。SSL 接続は、ローカル構成の暗号化パラメータを使って確立されます。

Data Protector プロセスは、バックアップセッション中に、ローカル構成の暗号化パラメータを読み込みます。バックアップセッションマネージャー (BSM) は、Media Agent (MA) および

Disk Agent (DA) との SSL 接続を確立し、通常の Data Protector 接続プロトコルが続きます。次に、MA へのデータ接続が DA によって確立されます。データバックアップは、その後に続きます。

「暗号制御通信」 (51 ページ) に、暗号制御通信が有効な場合の、Data Protector セル内での基本的な通信のやり取りを示します。

図 19 暗号制御通信



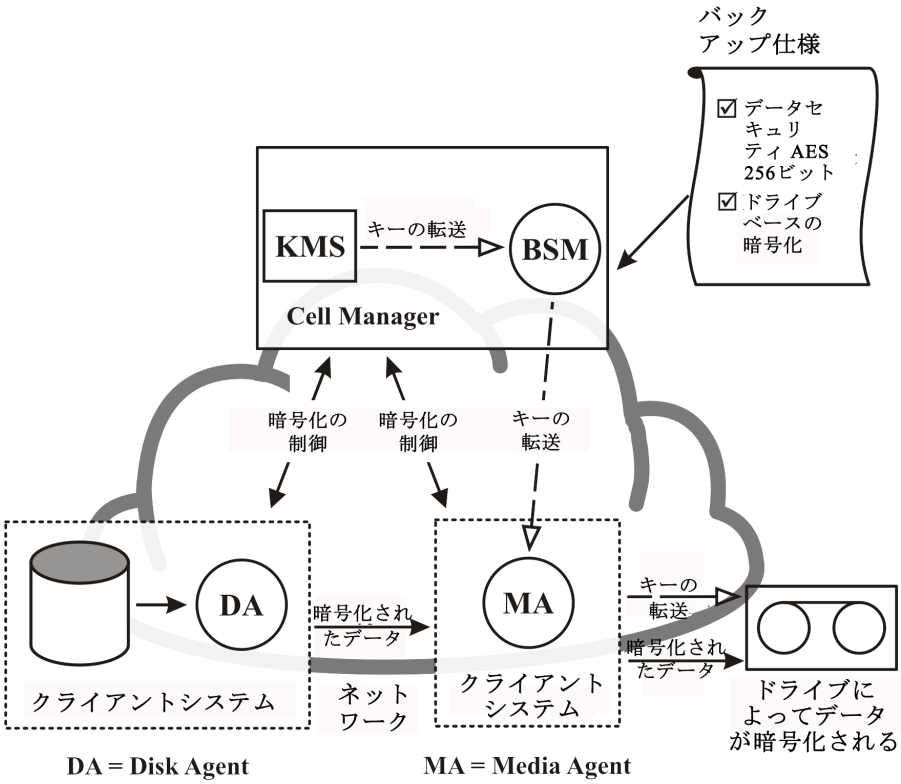
データの暗号化と暗号制御通信

データの暗号化と暗号制御通信を組み合わせることで、システムのセキュリティレベルを容易に最大化することができます。

- データをネットワーク上で転送してメディアに書き込む前に、ソフトウェア (AES 256 ビット) 暗号化によってデータを暗号化します。
- バックアップのハードウェア (ドライブベース) 暗号化によって、メディアへの保存/移動時のデータへの不正アクセスを防ぎます。
- 暗号制御通信によって、セル内のクライアント間にセキュアな通信が提供されます。

「暗号制御通信とデータの暗号化」 (52 ページ) に、**[AES 256** ビット**]** 暗号化オプションと **[**ドライブベースの暗号化**]** オプションが選択され、暗号制御通信が有効な場合の、暗号化されたバックアップセッション時における Data Protector セル内での基本的なやり取りを示します。

図 20 暗号制御通信とデータの暗号化



クラスターリング

クラスターの概念

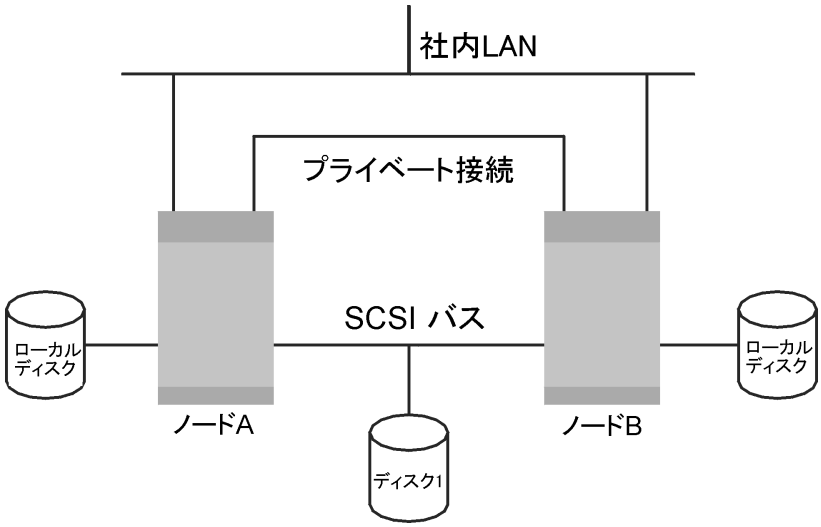
クラスターとは

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

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

Data Protector ではクラスター化を実現するために、 Windows Server 用の Microsoft Cluster Server および HP-UX 用の MC/Service Guard と統合します。サポート対象クラスターの一覧は、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

図 21 代表的なクラスター



構成要素

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

クラスターノード

クラスターノード クラスターを構成するコンピュータは、クラスターノードと呼ばれます。クラスターノードは、1 つまたは複数の共有ディスクに物理的に接続されています。

共有ディスク

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

クラスターネットワーク

クラスターネットワークは、すべてのクラスターノードを接続するプライベートネットワークです。このネットワークにより、**クラスターのハートビート**と呼ばれる内部的なクラスターデータが転送されます。ハートビートとはタイムスタンプ付きのデータパケットで、すべてのクラスターノードに配布されます。各クラスターノードでは、このパケットを比較することによりどのクラスターノードが現在稼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**クラスター対応**アプリケーションの実行に必要なリソースの集まりを指します。各クラスター対応アプリケーションでは、それぞれの重要なリソースを宣言します。各グループまたはパッケージ内では、以下のリソースが定義されていなければなりません。

- 共有ディスクボリューム (MSCS、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

- クラスター対応アプリケーションサービス

仮想サーバーとは

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

フェイルオーバーとは

それぞれのパッケージまたはグループには、通常の場合に実行される「優先」ノードが設定されています。このようなノードを**一次ノード**と呼びます。パッケージまたはグループは、別のクラスターノード (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ーノードから二次クラスターノードに移すことを**フェイルオーバー**、またはスイッチオーバーと呼びます。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

クラスター環境では、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ー対応の Data Protector Cell Manager には、非クラスター対応バージョンに比べて、以下に挙げる多くの利点があります。

Data Protector Cell Manager の高可用性の実現

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

バックアップの自動再開

バックアップ手順を定義するための Data Protector バックアップ仕様は、Data Protector Cell Manager でのフェイルオーバーの発生時に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。

フェイルオーバー時の負荷調整

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

クラスターのサポート

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

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

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

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

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

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

Data Protector Cell Manager のフェイルオーバーの発生時のバックアップセッションの動作オプションの詳細については、『HP Data Protector ヘルプ』の索引「クラスター、バックアップ仕様オプション」を参照してください。

クラスター環境の例

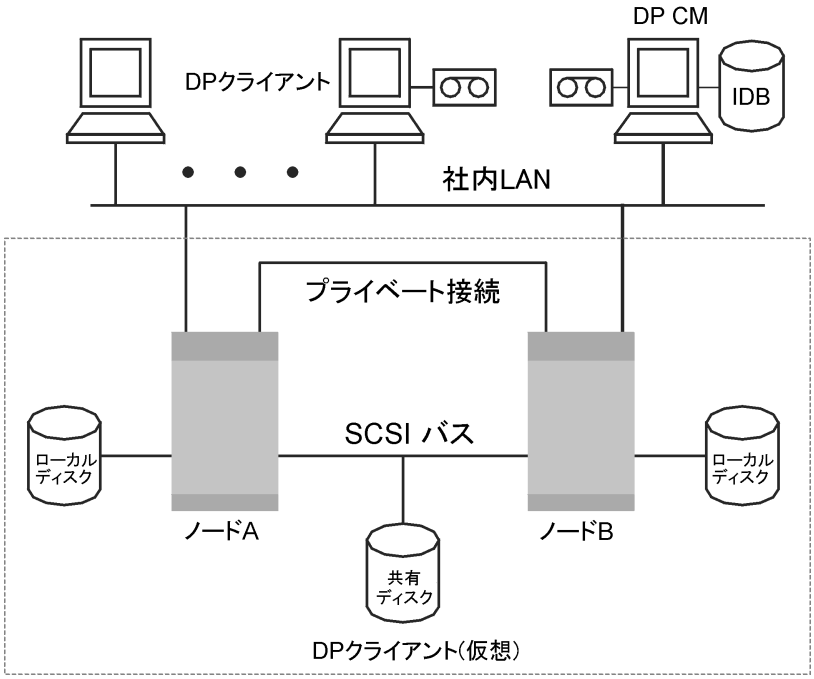
この項では、3 つのクラスター構成例を示します。

Cell Manager がクラスター外部にインストールされている構成

下図の環境には以下のような特徴があります。

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

図 22 Cell Manager がクラスター外部にインストールされている構成



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

- 物理ノード A
- 物理ノード B
- 仮想サーバー

仮想サーバーのバックアップ

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

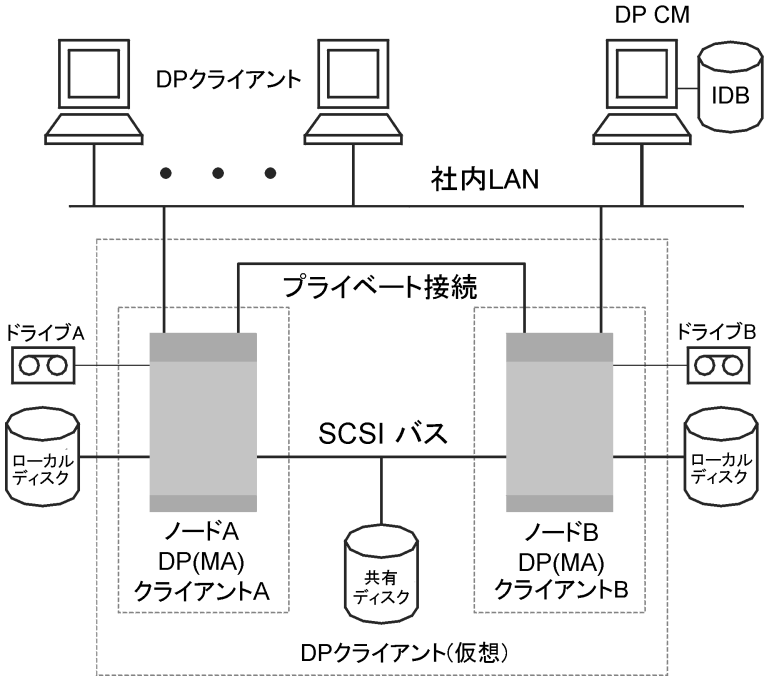
これらのオプションの定義方法については、『HP Data Protector ヘルプ』の索引「クラスター、バックアップ仕様オプション」を参照してください。

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

下図の環境には以下のような特徴があります。

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

図 23 Cell Manager がクラスター外部にインストールされ、デバイスがクラスターノードに接続されている構成



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

- 物理ノード A
- 物理ノード B
- 仮想サーバー

仮想サーバーのバックアップ

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

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

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

下図の環境には以下のような特徴があります。

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

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

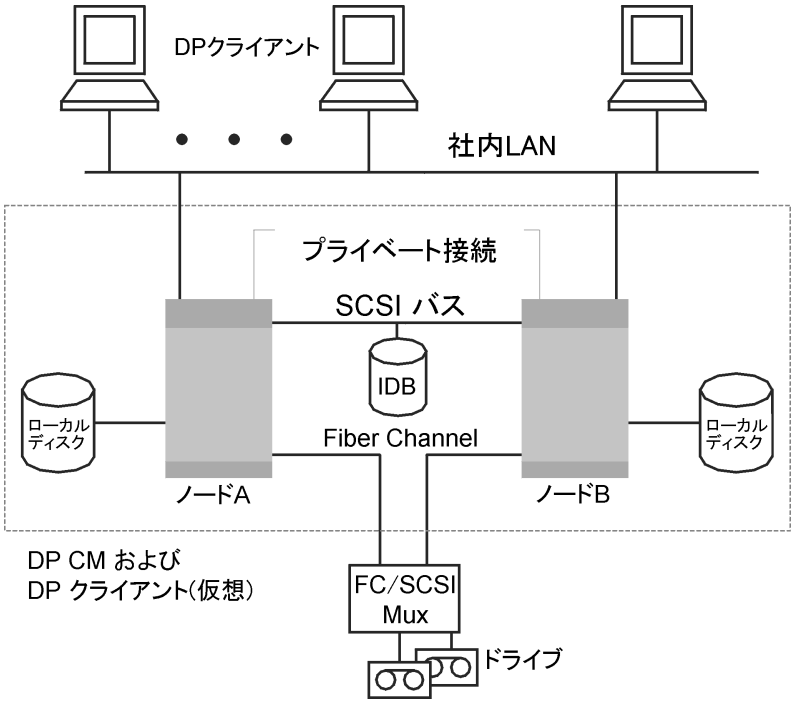
  - Data Protector Cell Manager をアプリケーションと同じノード上で実行するよう構成します (通常の動作時およびフェイルオーバー時共)。つまり、Data Protector クラスターの重要なリソースは、アプリケーションクラスターの重要なリソースと同じパッケージ (MC/ServiceGuard の場合) またはグループ (Microsoft Cluster Server の場合) 内に定義します。

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

図 24 Cell Manager がクラスター内部にインストールされ、デバイスがクラスターノードに接続されている構成



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

- 物理ノード A
- 物理ノード B
- 仮想サーバー

仮想サーバーのバックアップ

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

注記: クラスターでは、共有テープに SCSI バスを使用できません。Media Agent についても高可用性を実現するには、デバイスとのインタフェースに 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` を使用します 。管理者は、フェイルオーバー発生時に実行すべき処理内容を、Cell Manager を使用して、以下のように定義できます。

  - バックアップシステムに引き継がれたアプリケーションに比べて、バックアップ処理の重要度が低い場合には、Data Protector により実行中のバックアップセッションを中止できます。
  - より重要なバックアップを行っていた場合や、あと少しで処理が終了するような場合には、Data Protector はセッションを継続します。

また、Data Protector クラスターの Cell Manager/クライアントを、EMC Symmetrix 環境または HP P9000 XP ディスクアレイファミリ環境と統合すると、非常に可用性の高いバックアップ環境を構築できます。詳細は、『HP 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、増分バックアップ、合成バックアップ

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

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

表 3 フルバックアップと増分バックアップの比較

	フルバックアップ	増分バックアップ
リソース	増分バックアップより完了までの時間が長く、必要とするメディア容量が大きい	前回のバックアップ以降の変更部分のみをバックアップするため、必要な時間とメディア容量が少なくて済みます。
デバイスの操作	単一ドライブのスタンドアロンデバイスを使用する場合は、バックアップデータの量が 1 つのメディアのサイズを上回っていると、手動でメディアを交換する必要が生じます。	バックアップに追加メディアが必要となることは少ない
復元	シンプルで速い復元が可能	必要となるメディア数が多いため、復元にかかる時間が長い
IDB への影響	IDB 内に占めるスペースが大きい	IDB に書き込む情報の量がフルバックアップほど多くありません。

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

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

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

フルバックアップ

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

合成バックアップ

合成バックアップは、通常のフルバックアップを実行する必要のない高度なバックアップソリューションです。代わりに、増分バックアップが実行され、続いてそれがフルバックアップとマージされると、新規合成フルバックアップとなります。詳細は、「合成バックアップ」(63 ページ) を参照してください。

増分バックアップ

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

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

従来の増分バックアップ

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

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

拡張増分バックアップ

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

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

拡張増分バックアップの使用は、合成バックアップの前提条件となります。

Change Log Provider を使用した拡張増分バックアップ

拡張増分バックアップや従来の増分バックアップは、Windows NTFS Change Log Provider を使用して実行できます。Change Log Provider では、時間を要するファイルツリー検索ではな

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

増分バックアップの種類

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

増分
: 単純な増分バックアップは、「増分バックアップ」 (61 ページ) に示すとおり、まだ保護期限が切れていない最後のバックアップ (フルバックアップ、またはいずれかのレベルの増分バックアップ) をベースとして行われます。

増分 1～9
: **複数レベル増分バックアップ**は、「複数レベル増分バックアップ」 (61 ページ) 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。たとえば増分 1 バックアップを実行すると、前回のフルバックアップ時より後に更新された、すべてのデータが保存されます。また、増分 5 バックアップを実行すると、前回の増分 4 バックアップより後に更新されたすべてのデータが保存されます (増分 4 バックアップが存在する場合)。増分 1～9 バックアップでは、既存の増分バックアップは参照**されません**。

図 25 増分バックアップ

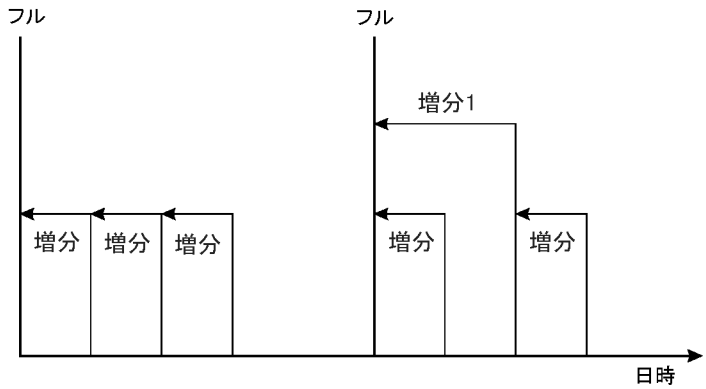
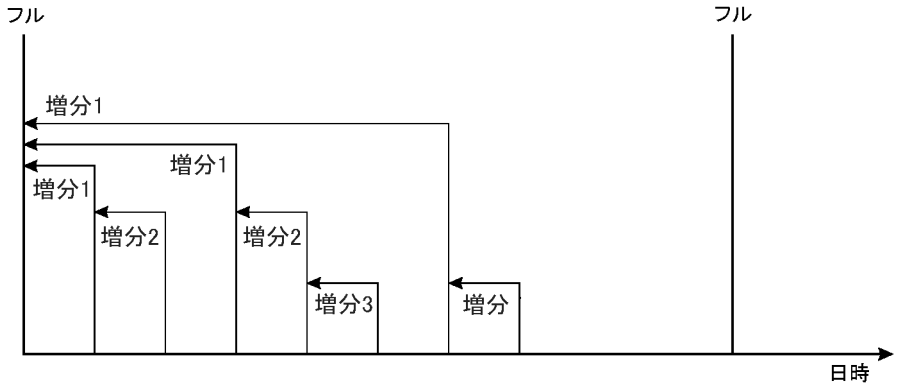


図 26 複数レベル増分バックアップ



「バックアップ実行時の相対的参照関係」 (62 ページ) に、さまざまなバックアップタイプの実行時の相対的な参照関係を示します。詳細な説明については、表の下のテキストを参照してください。

表 4 バックアップ実行時の相対的参照関係

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

「バックアップ実行時の相対的参照関係」 (62 ページ) の見方

- 「バックアップ実行時の相対的参照関係」 (62 ページ) の各行は互いに関係性はなく、異なる状況を示します。
- バックアップの経過時間は、右から左に増加します。したがって左端が一番古く、右端が最新のバックアップになります。
- フルと増分 X は、同じ所有者の保護期限内のオブジェクトを表します。保護されていない既存の増分 X は復元に使用できますが、それより後のバックアップ実行時の参照には考慮されません。

例

- 2 行目では、フルで保護期間内のバックアップが実行され、増分 2 が実行中です。増分 1 がないため、バックアップは増分 1 として実行されます。
- 5 行目では、フルバックアップが実行され、増分 1 と他の増分が実行中です。Data Protector では、現在 1 つ前の増分に対して実行中のバックアップ、つまり増分 1 に対する参照を設定します。
- 8 行目では増分 3 が増分 2 として実行され、11 行目では増分 3 が増分 1 として実行されます。

バックアップ世代

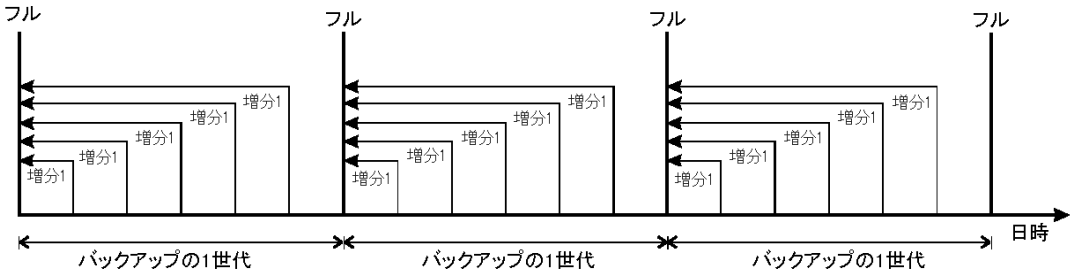
Data Protector では、日付/時刻ベースの保護モデルが採用されています。定期的にバックアップを行っている場合は、世代ベースのバックアップモデルと、この日時ベースのバックアップモデルを簡単に対応付けることができます。

バックアップ世代とは

「バックアップ世代」 (63 ページ) に示すように、バックアップ世代は、1 つのフルバックアップと、そのフルバックアップをベースとするすべての増分バックアップで構成されています。次のフルバックアップが実行されると、新しいバックアップ世代が作成されます。

バックアップ世代は、フルバージョンのバックアップデータがいくつあるかを把握するのに役立ちます。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 27 バックアップ世代



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

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

適切なプール使用方法を設定しておくと、保護期間が切れたメディアを自動交換させることもできます。詳細は、「メディア交換方針の実装」 (125 ページ) を参照してください。

合成バックアップ

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

概要

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

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

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

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

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

合成バックアップの利点

合成バックアップには、次のような利点があります。

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

Data Protector の合成バックアップの仕組み

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

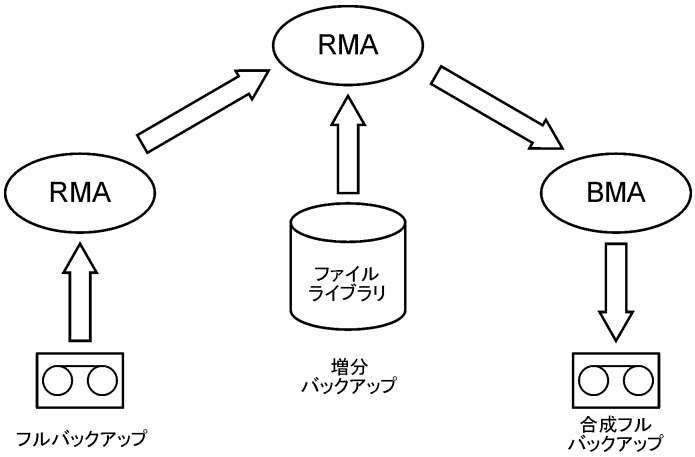
合成バックアップを有効にするには、拡張増分バックアップを使用する必要があります。拡張増分バックアップは、フルバックアップおよび増分バックアップを実行する前にオンにしておく必要があります。

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

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

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

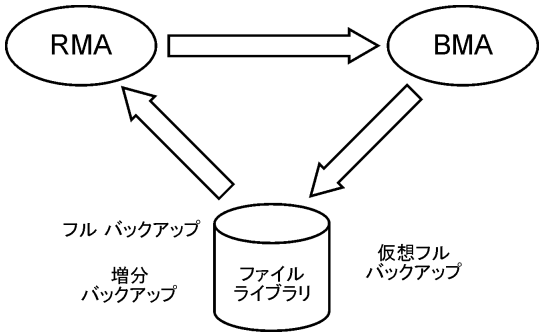
図 28 合成バックアップ



「合成バックアップ」 (64 ページ) は、合成フルバックアップが作成される様子を示しています。Restore Media Agent(RMA) によって、バックアップメディア (テープまたはディスク) からフルバックアップが読み取られます。そのデータは別の RMA に送られ、その RMA がファイルライブラリから増分バックアップを読み取り、データを集約します。次に、集約されたデータは Backup Media Agent(BMA) に送られ、合成フルバックアップがバックアップメディア (テープまたはディスク) に書き込まれます。

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

図 29 仮想フルバックアップ



「仮想フルバックアップ」 (65 ページ) は、仮想フルバックアップが作成される様子を示しています。このタイプのバックアップの場合、配布ファイルメディア形式を使用する 1 つのファイルライブラリ内にすべてのバックアップが存在します。Restore Media Agent(RMA) は、フルバックアップと増分バックアップに関する情報を読み取り、仮想フルバックアップ用のデータを生成します。生成されたデータは Backup Media Agent(BMA) に送られ、そこで仮想フルバックアップがファイルライブラリ内に作成されます。

合成バックアップとメディアスペースの使用量

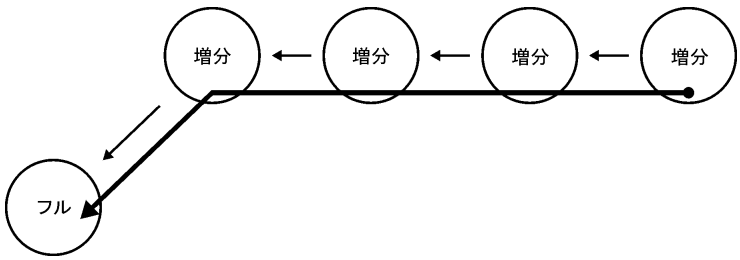
合成バックアップを頻繁に実行し、ソースを保持しておく場合、バックアップメディア上のスペース使用量は一般にかなり大きくなります。ただし、仮想フルバックアップを実行すると、バックアップメディア上のスペース使用量を最小限に抑えることができます。

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

復元と合成バックアップ

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

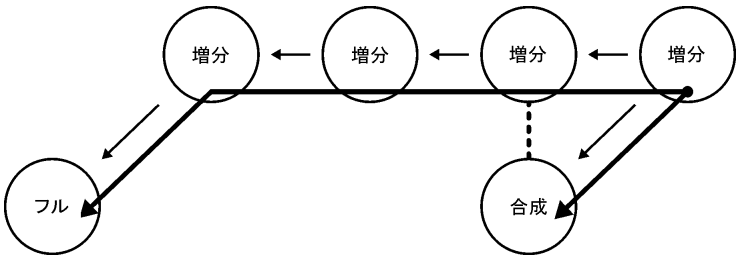
図 30 フルバックアップと増分バックアップ



「フルバックアップと増分バックアップ」 (65 ページ) では、従来のバックアップが実行されています。可能な限り最新の状態に復元するためには、フルバックアップと 4 つ増分バックアップがすべて必要になります。復元チェーンは 5 つの要素で構成されており、これらの要素は異なるメディアに存在することがよくあります。

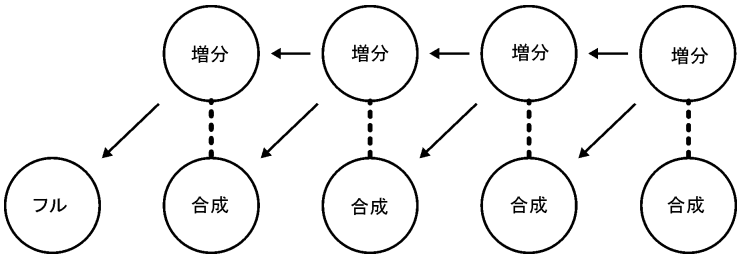
このような復元では、それぞれの増分バックアップを読み取る必要があるため、非常に多くの時間を要する場合があります。テープデバイスを使用している場合は、複数のメディアのロードとアンロードの時間や、復元するオブジェクトバージョンを検索する時間を要します。

図 31 合成バックアップ



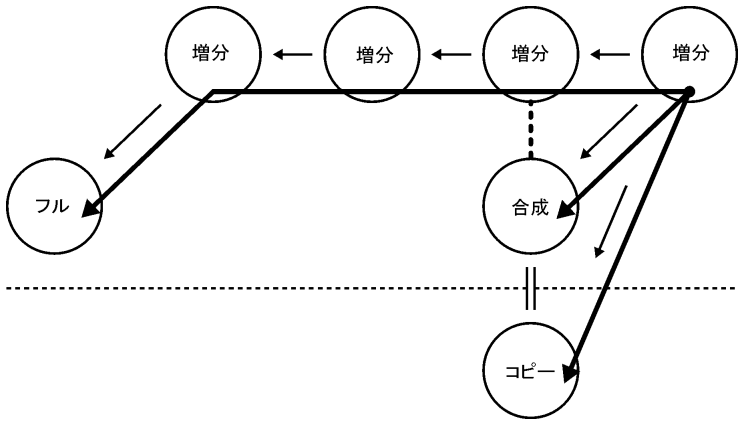
「合成バックアップ」 (66 ページ) には合成フルバックアップが存在しており、復元用にデフォルトで使用されます。復元チェーンは、2 つの要素 (合成フルバックアップとそれ以降の増分バックアップ) のみで構成されます。復元は、合成フルバックアップがない場合に比べて大幅に単純かつ高速になります。この図では、想定される両方の復元チェーンを示しています。

図 32 通常の合成バックアップ



「通常の合成バックアップ」 (66 ページ) は、それぞれの増分バックアップ後に合成バックアップが実行された状況を示しています。この方式では、可能な限り最新の状態またはバックアップされた任意の時点に、最も単純かつ高速に復元できます。復元に必要な要素は 1 つのみ (希望する時点の合成フルバックアップのみ) です。

図 33 合成バックアップとオブジェクトコピー



「合成バックアップとオブジェクトコピー」 (66 ページ) では、合成バックアップが、実行された後でコピーされています。これにより、安全性が強化されます。図に示している 3 つの復

元チェーンのいずれを使用した場合でも、可能な限り最新の状態に復元することができます。デフォルトでは、Data Protector によって最適な復元チェーンが選択され、それには、通常、合成フルバックアップまたはそのコピーが含まれます。メディアが失われた場合や、メディアエラーなどの場合には、別の復元チェーンが使用されます。

合成バックアップからの復元に対するデータ保護期間の影響

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

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

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

復元時の注意点

最新のデータを復元するには、前回のフルバックアップが格納されたメディアと、それ以降に実行された増分バックアップが格納されたメディアが必要です。そのため、増分バックアップの回数が多ければ多いほど、必要となるメディアの数も増加します。スタンドアロンデバイスを使用している場合には、この点が問題となって、復元処理に時間がかかってしまいます。

「簡易および複数レベルの増分バックアップからの復元時に必要となるメディア」 (68 ページ) に示す簡易バックアップおよび複数レベルの増分バックアップを実行した場合、フルバックアップとそれ以降に作成された増分バックアップの、合計 5 つの**メディアセット**にアクセスする必要があります。この場合、メディア上で必要とされるスペースは少なくなりますが、復元作業は複雑になります。必要となる一連のメディアセットは、**復元チェーン**とも呼ばれます。

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

増分バックアップ概念の別の共通な用途については、「複数レベルの増分バックアップからの復元時に必要となるメディア」 (68 ページ) に示されています。ここでは、メディアに必要な容量は若干大きくなります。この方法では、特定の時点までの復元処理を行うのに、2 つのメディアセットしか必要ありません。またこの復元方法の場合には、復元する状態の時刻を変更しない限り、以前に作成された増分 1 メディアセットに依存する必要がない点に注目してください。

図 34 簡易および複数レベルの増分バックアップからの復元時に必要となるメディア

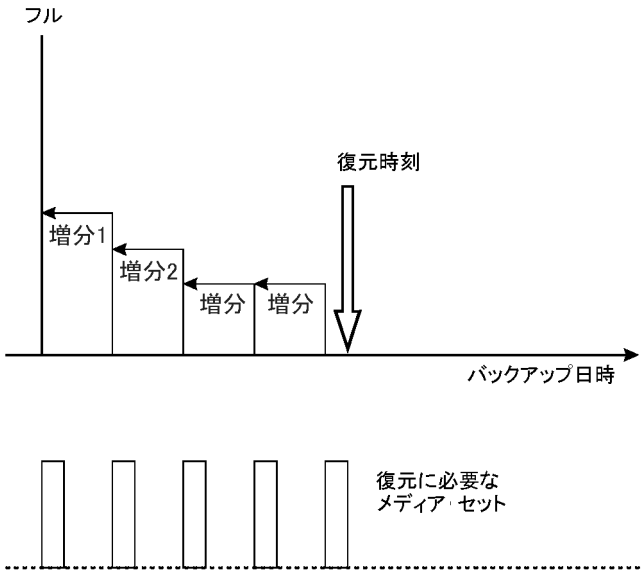
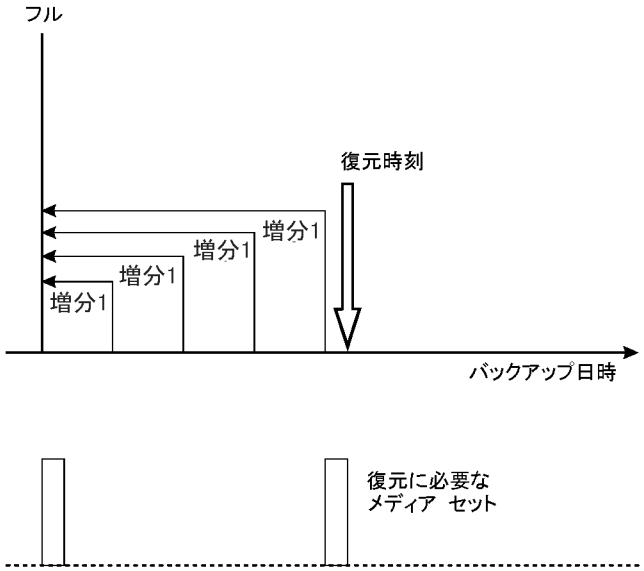


図 35 複数レベルの増分バックアップからの復元時に必要となるメディア



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

バックアップデータおよびバックアップデータに関する情報の保存

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

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

Data Protector 内部データベース

復元の性能を考えるうえで、復元作業に必要なメディアをいかにすばやく見つけられるかも重要なポイントになります。メディアに関する情報は、デフォルトでは IDB に保存され、復元の

性能を向上するとともに、復元するファイルやディレクトリを簡単にブラウズできるようになっています。ただし、すべてのバックアップにおけるすべてのファイル名を IDB に長期間保存すると、IDB のサイズがあまりにも大きくなってしまう可能性があります。

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

データ保護

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 Data Protector ヘルプ』の索引キーワード「データ保護」を参照してください。

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

カタログ保護

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] 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 サイズの増大とパフォーマンスに及ぼす影響の詳細については、『HP Data Protector ヘルプ』を参照してください。

ロギングレベル

ロギングレベルとは

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、「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」 (144 ページ) 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

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。

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

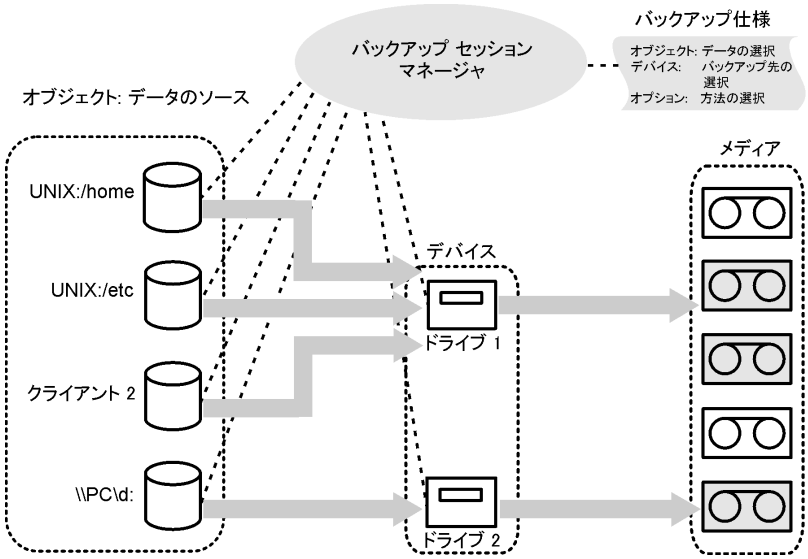
データのバックアップ

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 36 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。また、メディアプールも指定できます。メディアプールが指定されなかった場合、デフォルトメディアプールが使用されます。バックアップ仕様では、 1 つのディスクをスタンドアロンの DDS ドライブにバックアップするといった単純な設定もできれば、40 台の大規模サーバーを、8 台のドライブを搭載したサイロテープライブラリにバックアップするといった複雑な設定も可能です。

バックアップ設定の作成

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。Data Protector には、ほとんどの場合に適合するデフォルトの動作が用意されています。Data Protector バックアップオプションを使用すると、バックアップ動作をカスタマイズできます。

Data Protector では、対象となるクライアントに接続されているすべてのディスクをバックアップ時に検出して、バックアップすることも可能です。「ディスクディスカバリバックアップ」(157 ページ) 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ます。

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

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

バックアップオプションの例

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

- IDB に記録するログ情報のレベル

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

  - [すべてログに記録]
  - [ファイルレベルまでログに記録]
  - [ディレクトリレベルまでログに記録]
  - [ログなし]

  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、「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」(144 ページ) を参照してください。

- 自動負荷調整

  指定リストに基づくデバイスの動的割り当て。 詳細は、「負荷調整の仕組み」(98 ページ) を参照してください。

Data Protector により、どのオブジェクト (ディスク) をどのデバイスでバックアップするかが動的に決定されます。

- 実行前スクリプトと実行後スクリプト

  一貫性のあるバックアップを作成するための、クライアント側での準備作業に使用。詳細は、「実行前コマンドと実行後コマンド」 (156 ページ) を参照してください。

- データセキュリティ

  データに適用するセキュリティのレベル。

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

  - なし
  - AES 256 ビット
  - 暗号化

  暗号化の詳細については、「データの暗号化」 (48 ページ) 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、「Data Protector が機能する仕組み」 (153 ページ) 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、「オブジェクトのミラーリング」 (86 ページ) 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。データを復元するときには、復元元となるメディアがわかっている必要があります。Data Protector ではこの情報をカタログデータベースに保存しています。

バックアップの種類とバックアップのスケジュール設定

スケジュール設定方針では、バックアップの開始時点と種類(フルか増分か)が定義されます。フルバックアップおよび増分バックアップの違いを考慮してください。「フルバックアップと増分バックアップの比較」(59 ページ)を参照してください。

スケジュールバックアップを構成するときには、フルバックアップと増分バックアップを組み合わせることができます。たとえば、日曜日にフルバックアップを実行し、平日に毎日増分バックアップを行うことができます。大量データのバックアップを行いながらも、フルバックアップの大量データによるピークを避けるためには、時差を用いたアプローチを採用します。「フルバックアップの時差実行」(75 ページ)を参照してください。

スケジュール設定、バックアップ構成、およびセッション

バックアップ構成

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

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

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

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

バックアップ性能の最適化

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

スケジュール設定のヒントとテクニック

バックアップ世代、データ保護、およびカタログ保護の概念については、「フルバックアップ、増分バックアップ、合成バックアップ」(59 ページ)および「バックアップデータおよびバックアップデータに関する情報の保存」(68 ページ)の各項目を参照してください。

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

バックアップに適した時間帯

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

またフルバックアップは、クライアントごと(バックアップ仕様ごと)に、日を変えて実行する方がよい場合もあります。詳細については「フルバックアップの時差実行」(75 ページ)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 5 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

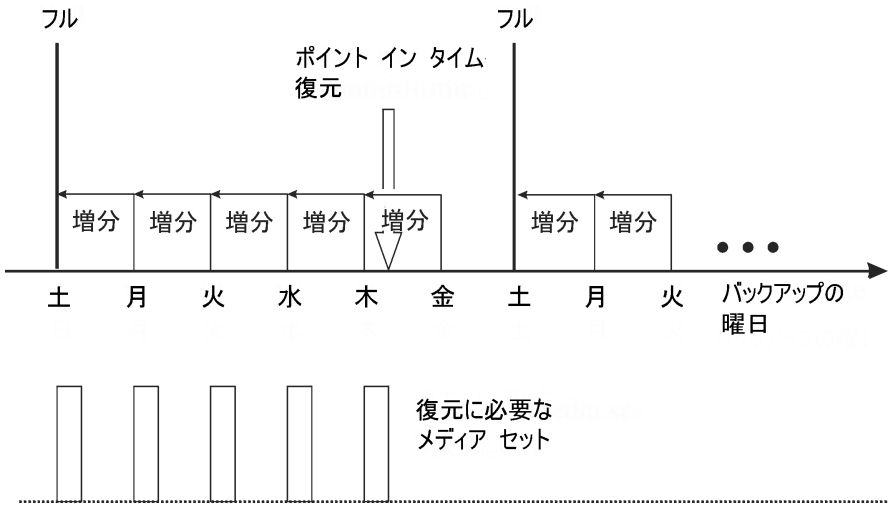
スケジュール設定方針と、フルバックアップおよび増分バックアップをどのように組み合わせるかは、対象となるデータの復元処理にかかる時間に大きく影響します。以下に 3 つの例を使って、この点を説明します。

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、「バックアップ用メディアの選択」(128 ページ)を参照してください。

例 1

「フルバックアップと 1 日 1 回の簡易増分バックアップを実行」(75 ページ)は、フルバックアップと簡易増分バックアップに基づくスケジュール設定方針を示したものです。

図 37 フルバックアップと 1 日 1 回の簡易増分バックアップを実行

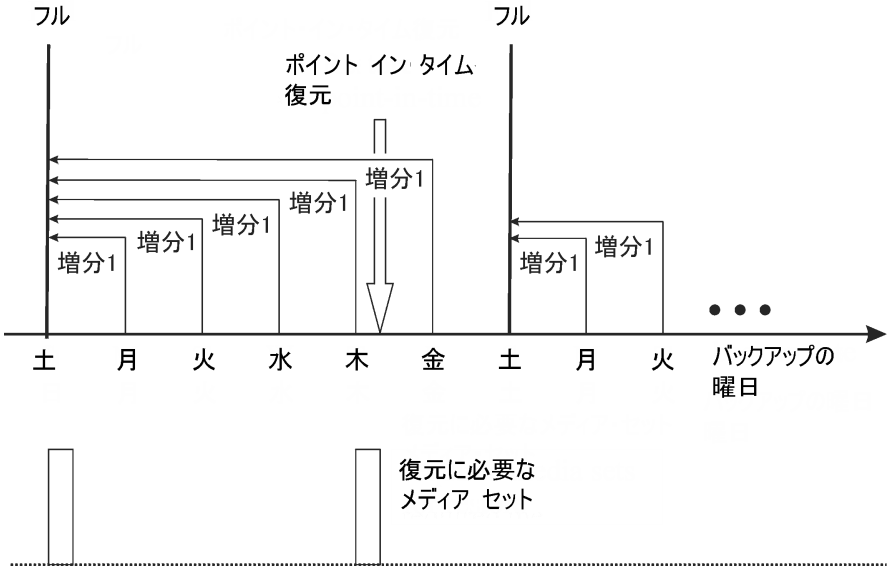


このスケジュールポリシーでは、前日以降の変更だけをバックアップするので、バックアップに必要になるメディア容量と時間が節減されます。ただし、たとえば木曜日のバックアップからファイルを復元するような場合には、フルバックアップと木曜日までの増分バックアップが必要になるため、合計 5 つのメディアセットが必要です。このため、復元の手順が複雑になり、時間がかかります。

例 2

「フルバックアップと 1 日 1 回のレベル 1 増分バックアップ」 (76 ページ) は、フルバックアップとレベル 1 増分バックアップに基づくスケジュール設定方針を示したものです。

図 38 フルバックアップと 1 日 1 回のレベル 1 増分バックアップ

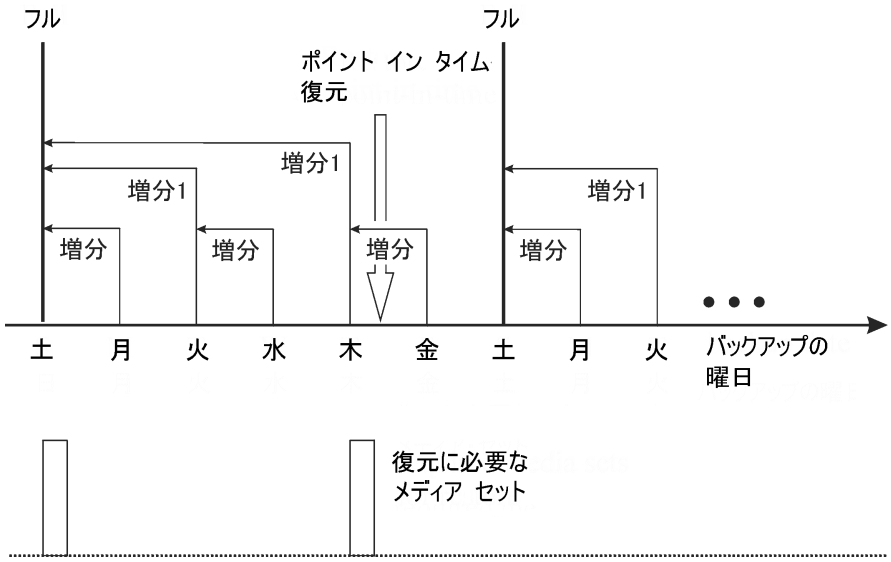


この方針では、毎日、前回のフルバックアップ以降に更新されたデータがバックアップされるため、バックアップに必要なメディアスペースと時間は多少増加します。ただし、たとえば木曜日のバックアップからファイルを復元するには、フルバックアップと木曜日の増分バックアップしか必要ないため、合計 2 つのメディアセットのみが必要となります。これにより、復元が大幅に簡略化され、時間も大きく短縮されます。

例 3

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

図 39 フルバックアップと 2 通りの増分バックアップ



このポリシーでは、週末には変更が多くないという事実を考慮します。データのバックアップに簡易増分バックアップと増分 1(差分) バックアップを組み合わせることで、バックアップのパフォーマンスを最適化しています。この場合、たとえば木曜日のバックアップからファイルを復元するには、フルバックアップと 2 番目の増分 1 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。

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

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

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

- 復元処理の容易性は、どの程度重要か。

  フルバックアップおよび増分バックアップのスケジュール方法によっては、最新バージョンのファイルを復元するときに、フルバックアップが格納されたメディアと増分バックアップが格納されたメディアの両方が必要になります。この場合、自動ライブラリデバイ

スを持っていなければ、復元処理に時間がかかったり、手動によるメディア交換が必要になる可能性があります。

- バックアップするデータの量はどの程度か。

  フルバックアップは増分バックアップよりも時間がかかります。また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。「メディア交換方針の実装」(125 ページ) を参照してください。ここでは、対象ライブラリ内に十分な数のメディアを用意しておくことにより、バックアップ時に手動でメディア交換を行わずに済ませる方法について説明しています。

- どのようにマウントプロンプトに対応するか

  ライブラリを使用するかどうかを決定します。ライブラリを使用すると、自動処理が可能となります。これは、Data Protector から、すべてのメディア、または大部分のメディアに対するアクセスが可能となり、メディアを手動で処理する必要がほとんどなくなるためです。データ量が非常に多く、1 台のライブラリでは対処しきれない場合は、ライブラリの追加も検討する必要があります。詳細は、「大容量ライブラリ」(103 ページ) 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。

  大量データをバックアップする必要があり、バックアップウィンドウに問題が表示される場合、ディスクベースデバイスへのバックアップと、合成バックアップやディスクステージングなどのアドバンストバックアップ戦略を検討してください。

- バックアップ対象の実行中のアプリケーションに対して、どのように準備するか。多くのアプリケーションでは、ファイルが開かれたままですので、バックアップの実行により、整合性のないバックアップが生成されます。実行前スクリプトおよび実行後スクリプトを使用して、アプリケーションの状態とバックアップ処理とを同期させることにより、この状況を防止できます。

バックアップデータの複製

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

Data Protector には、バックアップされたデータの複製方法 (オブジェクトコピー、オブジェクトミラー、メディアコピー) が用意されています。これらの機能の主な特徴に関して、「Data Protector のデータ複製メソッド」 (79 ページ) にまとめます。

表 6 Data Protector のデータ複製メソッド

	オブジェクトコピー	複製	オブジェクトミラー	メディアコピー	スマートメディアコピー
複製の対象	1 つまたは複数のバックアップ、オブジェクトコピー、オブジェクト集約セッションで作成される複数のオブジェクトバージョンの組み合せ	バックアップセッション、オブジェクトコピーセッション、オブジェクト集約セッションのオブジェクトセット	バックアップセッションのオブジェクトセット	メディア全体	メディア全体
複製のタイミング	バックアップ終了後の任意のタイミング	バックアップ終了後の任意のタイミング	バックアップ時	バックアップ終了後の任意のタイミング	バックアップ終了後の任意のタイミング
ソースメディアとターゲットメディアのメディアの種類	同じでなくてよい	同じ種類の B2D デバイスのみに複製可能	同じでなくてよい	同じであることが必要	ディスクベースのストレージをテープベースのストレージと組み合わせるので異なる
ソースメディアとターゲットメディアのサイズ	同じでなくてよい	ターゲットデバイスには、複製データ用の十分な空きスペースが必要	同じでなくてよい	同じであることが必要	同じであることが必要[1]
ターゲットメディアを追加可能かどうか	可	該当なし	可	不可[2]	不可[3]
作成される内容	選択したオブジェクトバージョンを含むメディア	ターゲット B2D デバイス上に格納された同一のコピー	選択したオブジェクトバージョンを含むメディア	ソースメディアと同じメディア	ソースメディアと同じメディア

[1] ソースメディアはディスクアレイ上の仮想テープにあり、ターゲットメディアは VLS に接続された物理テープライブラリにあります。

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

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

オブジェクトのコピー

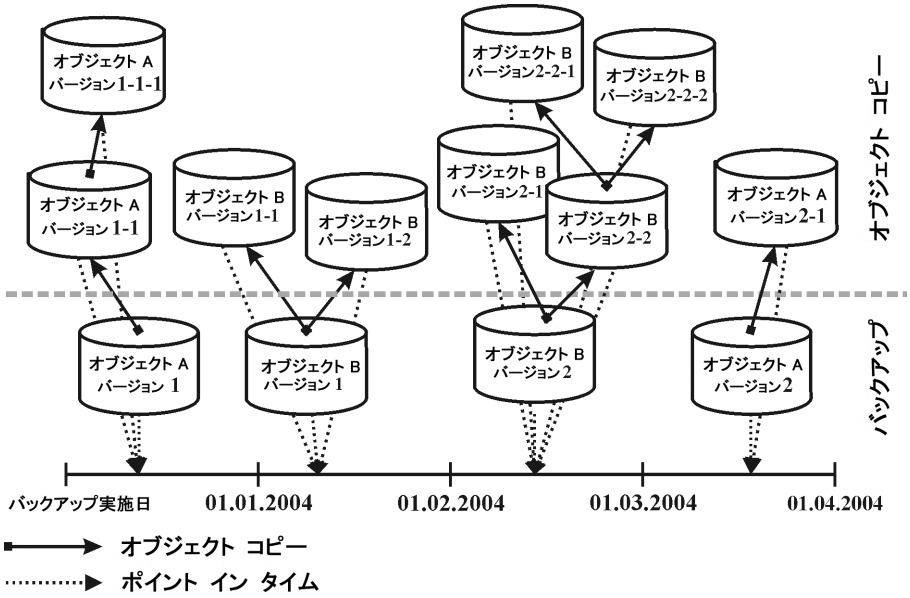
オブジェクトコピーとは

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。1 つまたは複数のバックアップ、オブジェクトコピー、オブジェクト集約セッションで作成される複数のオブジェクトバージョンを選択できます。オブジェクトコピーセッションでは、コピー元メディアから読み取られたデータが転送されて、コピー先メディアに書き込まれます。

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

「オブジェクトコピーの概念」 (80 ページ) 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 40 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 には、**ポストバックアップのオブジェクトコピー**および**スケジュール方式のオブジェクトコピー**の 2 種類の自動オブジェクトコピー機能が用意されています。

ポストバックアップのオブジェクトコピー

ポストバックアップ/ポストコピー/ポスト集約のオブジェクトコピー。これは、ポストバックアップのオブジェクトコピーのサブセットです。自動オブジェクトコピー仕様で指定したセッションの終了後に開始されます。この場合は、その特定のバックアップセッションで作成された自動オブジェクトコピー仕様に従って、選択されているオブジェクトがコピーされます。

スケジュール済みのオブジェクトコピー

スケジュール済みのオブジェクトコピーはユーザーが指定した時刻に開始されます。さまざまなセッションからのオブジェクトを、スケジュールされた 1 つのオブジェクトコピーセッションにおいてコピーできます。

デバイスの選択

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

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

ソースデバイスの選択

デフォルトで、Data Protector は、デバイス構成内のデバイスポリシー設定に従って、オブジェクトコピー用のソースデバイスを自動的に選択します。これにより、使用可能なリソースの利

用を最適化できます。元のデバイスを使用する場合に自動デバイス選択を無効にすることも、特定のデバイスを選択することも可能です。

- デバイスの自動選択 (デフォルト):

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

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

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

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

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

- 元のデバイスの選択:

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

あて先デバイスの選択

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

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

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

コピー元のメディアセットの選択

コピー対象のオブジェクトバージョンが、Data Protector のデータ複製方法で作成された複数のメディアセットに存在する場合、そのメディアセットはコピー元として使用できます。メディア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。

メディアを選択するプロセス全体は、復元と同じです。詳細については、「メディアセットの選択」 (91 ページ) を参照してください。

オブジェクトコピーセッションの性能

オブジェクトコピーの性能は、デバイスのブロックサイズや接続方法などの要因に影響されます。オブジェクトコピーセッションで使われる各デバイスのブロックサイズが異なっていると、セッション中にデータの再パッケージ化が必要になるため、時間とリソースが余分に消費されます。また、ネットワークを介してデータを転送すると、新たなネットワーク負荷が発生

し、処理時間もそれだけ長くなります。これらの要因による影響は、処理の負荷調整を行うことで最小限に抑えることができます。

オブジェクトコピーを使う理由

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

- ボールティング

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

- メディアの解放

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

- メディアのデマルチプレックス

  オブジェクトをコピーして、インタリーブされたデータを削減できます。

- 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

  異なる種類のメディアにバックアップをコピーできます。

- 拡張バックアップの概念のサポート

  ディスクステージングなどのバックアップ概念を使用できます。

ボールティング

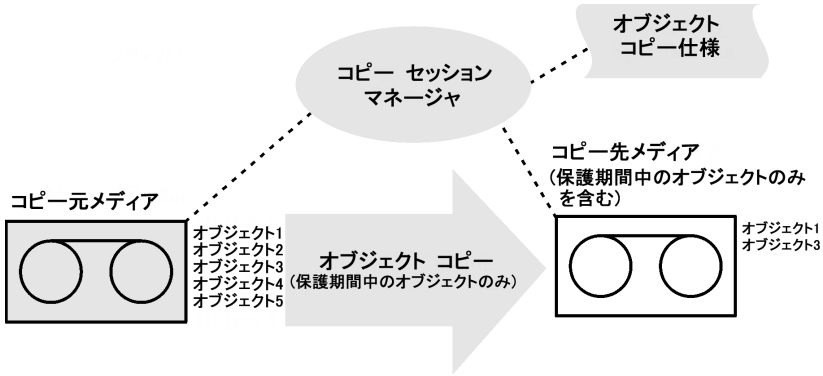
ボールティングはメディアを安全な場所に保管するプロセスを指します。この保管場所はボールトと呼ばれ、この中にメディアが一定期間保管されます。詳細については、「ボールティング」 (131 ページ) を参照してください。

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。「メディアの解放 」 (83 ページ) を参照してください。

図 41 メディアの解放

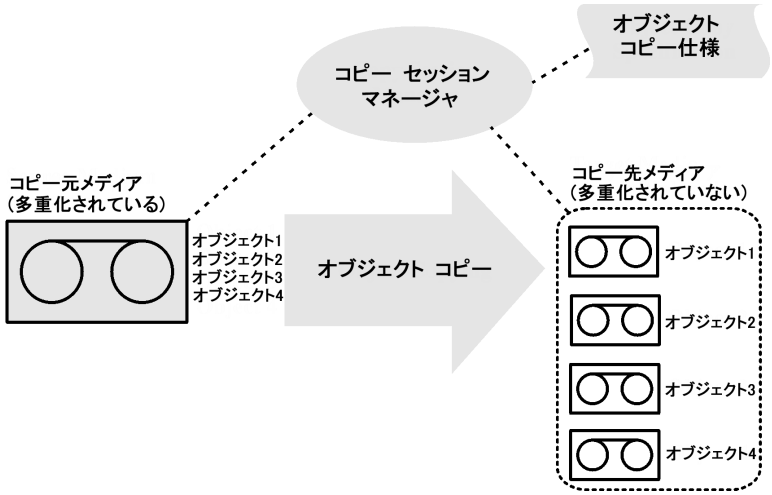


メディアのデマルチプレックス

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

Data Protector には、メディアの多重化を解消するための機能が用意されています。この機能を使うと、多重化されているメディア上の各オブジェクトを、指定した複数のメディアにコピーできます。「メディアの多重化 (データの断片化) の解消」 (83 ページ) を参照してください。

図 42 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使用すると、複数のメディアをロードしたり、必要なオブジェクトバージョンをシークしたりする必要がないため、すばやく、効率的に復元を実行できます。

別の種類のメディアへの移動

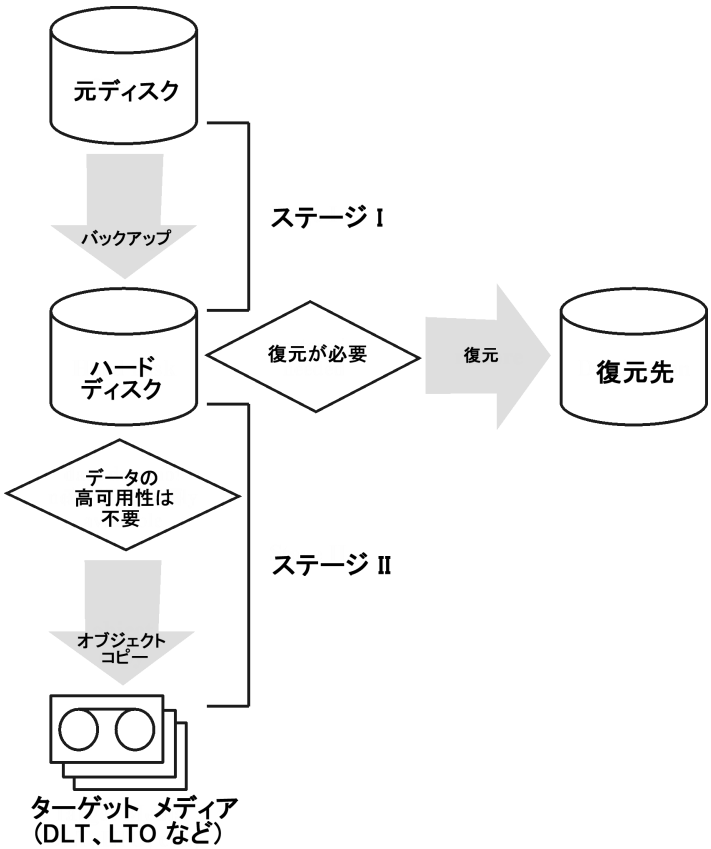
バックアップしたデータを 別の種類のメディアへ移動できます。たとえば、あるオブジェクトをファイル デバイスから LTO デバイスに、または DLT デバイスから LTO デバイスにコピーできます。

ディスクステージング

ディスクステージングとは、 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。

バックアップステージは、ある種類のメディアにデータをバックアップし、その後、そのデータを別の種類のメディアに移動するという操作で構成されています。最初の段階では、高性能でアクセスも容易ではあるが容量に限りがあるメディア (システム ディスクなど) にデータをバックアップします。通常バックアップしたデータは、復元に使用される可能性が最も高いバックアップ後の一定期間のみ、アクセスが容易なこれらのメディア上に保管しておきます。一定の期間が経過した後、データは、オブジェクトコピー機能を使って、パフォーマンスと可用性は低いが大容量の保存用メディアに移動されます。「ディスクステージングの概念」(84 ページ) を参照してください。

図 43 ディスクステージングの概念



この手順は、自動処理として実行可能です。

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

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

めにテープコピーを残して、コピーを削除できます。それまでは、テープコピーにより、ディスクコピーが破損した場合のセキュリティを確保できます。

ディスクステージングを使用すると、サイズの小さい多数のオブジェクトをテープに頻繁にバックアップする必要もなくなります。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を使用すると、バックアップ時間を短縮でき、メディアの劣化を防止できます。

複製

複製とは

Data Protector の複製機能は、複製に対応した 2 つのディスクへのバックアップ (B2D) デバイス間でオブジェクトを複製する機能であり、Media Agent によるデータ転送は行われません。

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

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

複製セッションの開始

複製セッションは、対話式に開始する方法と、自動的に開始するように指定する方法があります。Data Protector での自動複製には、**ポストバックアップ複製**と**スケジュール方式の複製**という 2 つの種類があります。

ポストバックアップ複製

ポストバックアップ複製には、ポストバックアップ、ポストコピー、ポスト集約の複製が含まれます。この複製は、自動複製仕様で指定したセッションの終了後に開始され、そのセッションで書き込まれた自動複製仕様に従って選択されたオブジェクトが複製されます。

スケジュール方式の複製

スケジュール方式の複製 はユーザーが指定した時刻に開始されます。1 つのスケジュール方式の複製セッションで複数のセッションを複製できます。

デバイスの選択

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

複製を使用する理由

複製は、ボールティングなど、オブジェクトコピーを行うさまざまな用途 (ただしメディア操作を除きます) で使用されます。「オブジェクトコピーを使う理由」 (82 ページ) も参照してください。

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

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

オブジェクトのミラーリング

オブジェクトのミラーリングとは

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。

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

オブジェクトのミラーリングの利点

オブジェクトミラー機能は、以下の目的に役立ちます。

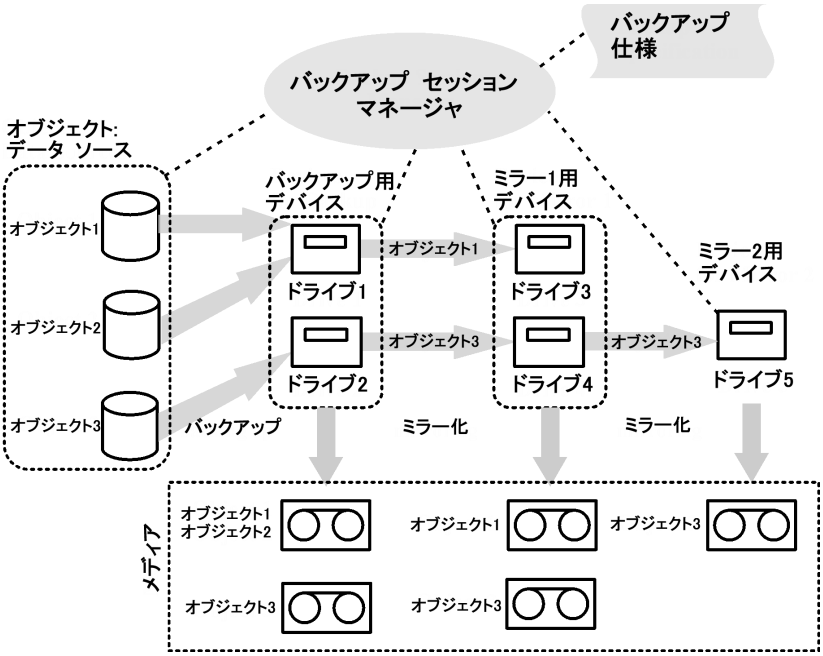
- 複数のコピーが存在するため、バックアップデータの可用性が向上します。
- バックアップデータをリモートサイトにミラー化できるため、複数の場所へのボールティングが容易になります。
- 同じデータが複数のメディアに書き込まれるため、バックアップのフォールトトレランスが強化されます。1 つのメディアで障害が発生しても、他のミラーの作成には影響しません。

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。「オブジェクトミラーのミラーリング」 (87 ページ) を参照してください。

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

図 44 オブジェクトミラーのミラーリング



デバイスの選択

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

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

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

バックアップ性能

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

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

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

メディアのコピー

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、「自動メディアコピー」 (89 ページ) 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。メディアの自動コピーセッションの開始時には、メディアの自動コピー仕様内で指定したパラメータに基づいて、メディアのリスト (ソースメディア) が自動的に作成されます。各ソースメディアでは、データのコピー先となるターゲットメディアが選択されます。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機能には独自の負荷調整機能が備えられています。Data Protector はできるだけ多くのデバイスを使用し、また可能であればローカルデバイスを使用することにより、使用可能なデバイスを最大限有効に活用しようとします。

自動メディアコピー機能は、マウント要求やクリーニング要求には対応できません。マウント要求が発行された場合は、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、『HP Data Protector ヘルプ』を参照してください。

VLS を使用したスマートメディアコピー

スマートメディアコピーとは

スマートメディアコピーでは、データは、まず、仮想ライブラリシステム (VLS) に構成された仮想テープライブラリ (VTL) にバックアップされます。次に、バックアップが含まれる仮想テープのコピーが、自動移行と呼ばれるプロセスで、VLS に接続された物理ライブラリに作成されます。Data Protector でコピープロセスが開始され、その後 VLS によって実行されます。データは、スマートコピーで物理ライブラリに転送され、これによって、Data Protector では、ソースメディアとターゲットメディアが区別され、メディア管理が可能になります。スマートコピーメディアは Data Protector フォーマットに従っているため、互換性のあるすべてのテープドライブに挿入でき、Data Protector で読み取られます。スマートコピーを行うと、VLS の仮想テープにあるソースメディアと、VLS に接続されている物理テープライブラリにあるターゲットメディア (スマートコピー) の、2 つの同等のメディアのセットになります。これらのいずれのコピーも復元に使用できるため、セキュリティが向上しバックアップされたデータの可用性が高まります。スマート メディアのコピーは、長期保存やボールティングなどの目的でも保持できます。

Data Protector には 2 種類のスマートメディアコピー機能が用意されています。それは、自動スマートメディアコピーと、対話形式のスマートメディアコピーです。

自動スマートメディアコピー

以下の種類の スマートメディアコピーを作成することができます。

- ポストバックアップのスマートメディアコピーで、バックアップセッションの完了後に行われ、特定のセッションで使用されるメディアがコピーされます。
- スケジュール形式のスマートメディアコピーで、特定の時刻または定期的な間隔で実行されます。

対話形式のスマートメディアコピー

対話形式の スマートメディアコピーでは、バックアップされたデータを含むメディアのコピーが作成され、必要に応じて任意の時点で開始できます。

バックアップ後に行われる処理

バックアップデータが物理テープに移動された後では、Data Protector の復元で使用できます。ただし、復元先のライブラリは Data Protector では表示されないため、復元はこのライブラリからは直接実行できませんが、Data Protector で制御される任意のテープドライブまたはライブラリから実行できます。

VLS スマートコピーの詳細については『HP Data Protector ヘルプ』の索引キーワード「スマートメディアコピー」と VLS マニュアルを参照してください。

バックアップメディアとバックアップオブジェクトの検証

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

メディアの検証とは

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

- アーカイブのためにメディアをコピーし、そのコピーをボールト内に格納する前にその有効性をチェックしたい場合。

- バックアップメディアが満杯になり、長期保管用のストレージに送信する前に、メディア内のすべてのオブジェクトをチェックしたい場合。

メディアの検証作業

メディアの検証を実行すると、以下が実行されます。

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

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

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

オブジェクト検証とは

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

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

以下の場合、オブジェクト検証を使用できます。

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

オブジェクト検証作業

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

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

さらに、以下に対して検証を実行できます。

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

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

データの復元

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

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

この項では、Data Protector を使った復元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。詳細は、「フルバックアップ、増分バックアップ、合成バックアップ」 (59 ページ) 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、「デバイスとメディアの管理」 (97 ページ) 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。詳細は、「性能に関する概要と計画上の注意点」 (41 ページ) 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)。詳細は、各自の環境に適した『HP Data Protector インテグレーションガイド』を参照してください。
- 並行復元の使用。データのバックアップ方法によっては、単一の読み取り操作で、複数のオブジェクトを同時に復元できます。「並行復元」 (159 ページ) を参照してください。
- 復元するデータを選択する際の速度と容易さは、バックアップに使用したログレベル設定とカタログ保護期間により異なります。「IDB の主要な調整可能パラメータとしてのロギングレベル」 (144 ページ) 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が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。たとえば、Data Protector では、損失メディアまたは劣化メディアがあるメディアセットは避けます。オブジェクトの完了ステータス、可用性、特定のメディアセットで使用されるデバイスのロー

カル性などが考慮されます。ライブラリ内に格納されたメディアセットは、スタンドアロンデバイス内のメディアセットよりも先に使用されます。

復元チェーンの選択

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

メディア位置の優先順位

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

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

デバイスの選択

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

- デバイスの自動選択 (デフォルト):

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

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

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

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

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

- 元のデバイスの選択:

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

復元する権限をオペレータにのみ付与

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ディザスタリカバリを実行する権限が与えられます。

この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 (たとえば復元処理の請求には必ず電子メールを使い、オペレータ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。
- Data Protector のユーザーインタフェースを、エンドユーザが使用しているシステムにインストールします。Data Protector ではユーザー権限を自動的に確認して、復元機能のみを許可します。

- エンドユーザーシステムのバックアップ構成時に、Data Protector の **public** オプションをオンにして、エンドユーザーがバックアップデータを使用できるようにしておく必要があります。

ディザスタリカバリ

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

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

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

障害の発生は常に重大な問題ですが、以下の要因は状況をさらに深刻化します。

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

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

ディザスタリカバリプロセスは 4 つのフェーズに分けられます。

1. ディザスタリカバリを成功させるには、それ以前に**フェーズ 0**(計画および準備フェーズ)を実行しておくことが重要です。

△ **注意:** 障害に備えてあらかじめ準備作業を行っていない場合は、障害が発生しても復旧作業を正しく実行することはできません。

2. **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。
3. 環境を定義するすべての構成情報を含めたオペレーティングシステムと 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。
4. フェーズ 2 までの作業が完了して初めて、アプリケーションデータやユーザーデータの復元 (**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。

ディザスタリカバリの方法

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

- 手動によるディザスタリカバリ

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

- 自動ディザスタリカバリ

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

- ディスクデリバリーによるディザスタリカバリ

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

- 拡張自動ディザスタリカバリ (EADR)

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

- ワンボタンディザスタリカバリ (OBDR) とは、Windows クライアントと Cell Manager 用に完全に自動化された Data Protector 復旧方法で、ユーザーが介在する手間は最小限に抑えられています。システムは OBDR テープからブートされ、自動的に復旧されます。

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

その他のディザスタリカバリの方法

この項では、Data Protector を使ったディザスタリカバリの概念と、サードパーティー製品のディザスタリカバリの概念を比較します。ここでは、Data Protector 以外の復旧方法について簡単に紹介します。主な復旧方法としては、以下の 2 つが挙げられます。

オペレーティングシステムのベンダーが提供する復旧方法

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

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

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

サードパーティー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 (サードパーティー製ツールを使用)。
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、クラスター化にも対応しているため、高速かつ効率的にディザスタリカバリを実行できます。Data Protector には、大規模な組織のシステム管理を支援するための、集中管理や復元を容易にする機能、高可用性のサポート、モニタリング、レポート、通知などの機能が備わっています。

3 デバイスとメディアの管理

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

デバイス

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

デバイスの種類

デバイスは、次の種類に分類されます。

- テープデバイス:
  - スタンドアロンデバイス「スタンドアロンデバイス」 (102 ページ) を参照してください。
  - 小規模なマガジンデバイス「小規模なマガジンデバイス」 (102 ページ) を参照してください。
  - 大容量ライブラリ「大容量ライブラリ」 (103 ページ) を参照してください。
- ディスクベースのデバイス。「ディスクバックアップ」 (109 ページ) 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 (たとえばハードウェアデータ圧縮を使用するものと、使用しないものなど)。

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

ライブラリ管理コンソールのサポート

現在使われているテープライブラリの多くは、リモートシステムからライブラリを構成、管理、監視するための管理コンソールを備えています。リモート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。これらの管理コンソールは、Data Protector には依存しません。

Data Protector は、ライブラリ管理コンソールのインタ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、『http://support.openview.hp.com/selfsolve/manuals 』を参照してください。

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

TapeAlert

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

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

デバイスリストと負荷調整

複数のバックアップデバイスの使用

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

デバイス使用率の平均化

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

負荷調整の使用に適している場合

以下の場合は、負荷調整を使用してください。

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

負荷調整の使用に適さない場合

以下の場合は、負荷調整を使用しないでください。

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

デバイスチェーン

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

負荷調整の仕組み

たとえば 100 個のオブジェクトを 4 台のデバイスにバックアップする場合、同時処理数を 3 に設定し、負荷調整パラメータ `MIN` と `MAX` をどちらも 2 に設定したとします。少なくとも 2 台のデバイスが使用可能な場合はセッションが開始し、3 オブジェクトずつ、それぞれ最初

に使用できるこの 2 デバイスに並列してバックアップされます。残りの 94 個のオブジェクトは保留となり、その時点では特定のデバイスに割り当てられません。

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

デバイスストリーミングと同時処理数

デバイスストリーミングとは

デバイスの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。バックアップインフラストラクチャでネットワークを多用する場合は、そのことにも注意が必要です。ローカルバックアップの場合は、ディスクとデバイスが同一システムに接続されているため、ディスクの処理速度が速くても、同時処理数には通常 1 を指定すれば十分です。

デバイスストリーミングの構成方法

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

Disk Agent の同時処理数

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。Data Protector では、ほとんどの場合に適用できるデフォルトの数を設定しています。たとえば標準的な DDS デバイスの場合であれば、2 つの Disk Agent により、ストリーミングの維持に十分なデータをデバイスに送信できます。また、ライブラリデバイス内に複数のドライブがあり、各ドライブが個別の Media Agent で制御される場合には、それぞれのドライブごとに個別に同時処理数を設定できます。

性能の向上

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

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

関連情報については、「バックアップセッション」 (153 ページ) を参照してください。

多重データストリーム

Data Protector では、ディスクの一部を複数のデバイスに同時にバックアップできます。この機能は非常に大容量で高速のディスクを比較的遅いデバイスへバックアップする場合に役立ちます。複数の Disk Agent が同じディスクから並列にデータを読み取り、複数の Media Agent

に送信します。これによってバックアップ速度が向上しますが、以下のことを考慮する必要があります。

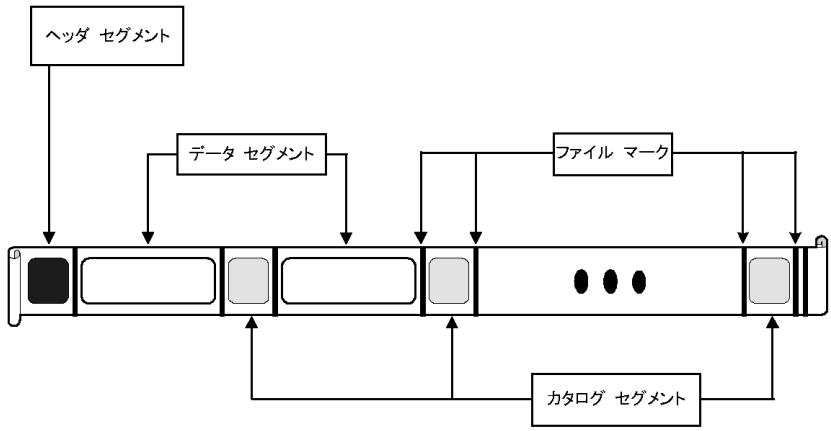
1 つのマウントポイントが複数の Disk Agent を通してバックアップされた場合、データは複数のオブジェクトに格納されます。マウントポイント全体を復元するには、1 つのバックアップ仕様でマウントポイントの要素をすべて定義した後、セッション全体を復元します。

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 つのヘッダーセグメントから構成されています。ヘッダー情報は、ブロックサイズと同じ長さのヘッダーセグメントに格納されます。データは、データセグメント内のデータブロックに格納されます。各データセグメントに関する情報は、対応するカタログセグメントに格納されます。このカタログ情報は最初に Media Agent メモリーに格納され、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。「データフォーマット」(100 ページ)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 45 データフォーマット



セグメントサイズ (MB 単位) は、データセグメントの最大サイズです。小サイズのファイルを多数バックアップする場合、実際のセグメントサイズはカタログセグメントの最大サイズに制限されることがあります。セグメントサイズはデバイスごとにユーザーが構成できます。セグメントサイズは復元速度に影響を与えます。セグメントサイズが小さくなればなるほど、メディア上のスペースは少なくなります。これはセグメントごとのファイルマークがメディアスペースを消費するためです。ただし、ファイルマークの数が多いと、Media Agent が目的のデータが含まれているセグメントをすばやく見つけ出せるため、復元速度は向上します。最適なセグメントサイズは、デバイスで使用されるメディアの種類やバックアップデータの種類によって異なります。たとえば、DLT メディアのデフォルトのセグメントサイズは 150MB です。

ブロックサイズ

セグメントは全ユニットに対してではなく、ブロックと呼ばれる小さなサブユニットに対して指定します。デバイスのハードウェアでは、デバイスの種類ごとに固有のブロックサイズの単位でデータを処理します。Data Protector では、デバイスに送信するブロックサイズを調整できます。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。

ブロックサイズを大きくすると、パフォーマンスが向上することがあります。ただし、ブロックサイズの変更は、テープをフォーマットする**前**に実行しておかなければなりません。たとえ

ば、デフォルトのブロックサイズを使ってすでにデータが書き込まれているテープに、別のブロックサイズのデータを追加することはできません。

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

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

Disk Agent 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ーバッファを使用します。このメモリーは、複数のバッファ領域に分割されています。総数はデバイスの同時処理数に依存しますが、Disk Agent ごとにバッファ領域が 1 つずつあります。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。

- メモリーの不足

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

  DA の同時処理数 * バッファ数 * ブロックサイズ

  たとえばバッファ数を 8 から 4 に減らすと、メモリー消費量は約 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。たとえば、1 つのスタンドアロン DDS デバイスを、圧縮デバイスとして定義し、さらに名前を変えて非圧縮デバイスとしても定義することができます。ただし、このような定義の仕方はお勧めできません。

物理デバイスの衝突

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

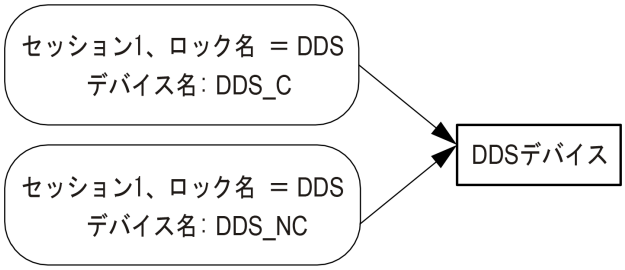
衝突の防止

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

たとえば「デバイスロックとデバイス名」(102 ページ)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 46 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く必要があります。Data Protector では、ほとんどのスタンドアロンデバイスを検出し、自動的に設定することができます。

バックアップ中に、デバイス内のメディアが一杯になると、Data Protector からマウント要求が発行されます。バックアップを続行するには、オペレータ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。

スタッカーデバイス

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

小規模なマガジンデバイス

マガジンデバイスとは

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

Data Protector とマガジンデバイス

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

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

汚れたドライブのクリーニング

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

大容量ライブラリ

ライブラリデバイスとは

ライブラリデバイスは、自動化されたデバイスであり、オートローダ、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。たとえば、4 つのドライブを備えたライブラリの場合には 5 つの SCSI ID が必要になります (ドライブ用に 4 つ、ロボティクス用に 1 つ)。

Data Protector は、 HP ライブラリ、StorageTek/ACSLS、ADIC/GRAU AML などのサイロライブラリもサポートしています。サポート対象デバイスの一覧は、『http://support.openview.hp.com/selfsolve/manuals 』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、ブランク (新しい) メディアや、Data Protector のメディアまたは Data Protector 以外のメディアを含めることもできます。Data Protector では、スロット内のメディアを確認して、メディアの情報をライブラリビューに表示します。この機能では、Data Protector で使われているメディアだけでなく、すべてのメディアのチェックが可能です。

ライブラリのサイズ

必要なライブラリのサイズは、以下のように見積ります。

- メディアを複数の場所に分散させる必要があるか、または 1 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。「メディア交換方針の実装」 (125 ページ) を参照してください。

他のアプリケーションとのライブラリの共有

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

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

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

特に 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。

挿入および取り出しメールスロット

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

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

詳細は、ご使用のデバイスのマニュアルを参照してください。

バーコードサポート

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

バーコードの利点

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

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

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

クリーニングテープのサポート

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。

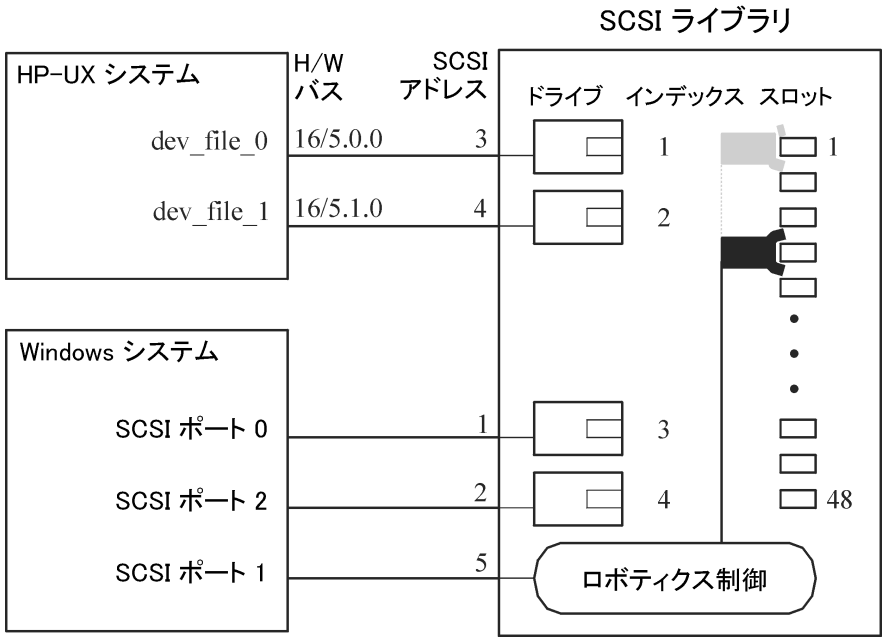
  ドライブが汚れていると、メディア上にデータを正しく書き込めず、バックアップが失敗する可能性があるため、ドライブをクリーニングするまではバックアップを続行できないようになっています。

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。これらのシステムでは、ライブラリへのローカルバックアップを実行できます。この結果、バックアップのパフォーマンスは非常に向上し、ネットワークトラフィックは軽減されます。この機能を使用するには、ライブラリ内の各ドライブを、個別の SCSI-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。

図 47 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 サーバーのバックアップを制御するクライアントシステム (NDMP 専用ドライブ向けに構成されたクライアントシステム) 上にのみ必要です。その他のケースでは、2 種類ある Data Protector Media Agent のどちらを使用しても構いません。

「ドライブ制御に必要な Data Protector Media Agent」 (106 ページ) 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 7 ドライブ制御に必要な Data Protector Media Agent

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

ロボティクス制御

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

「ロボティクス制御に必要な Data Protector Media Agent」 (107 ページ) 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。

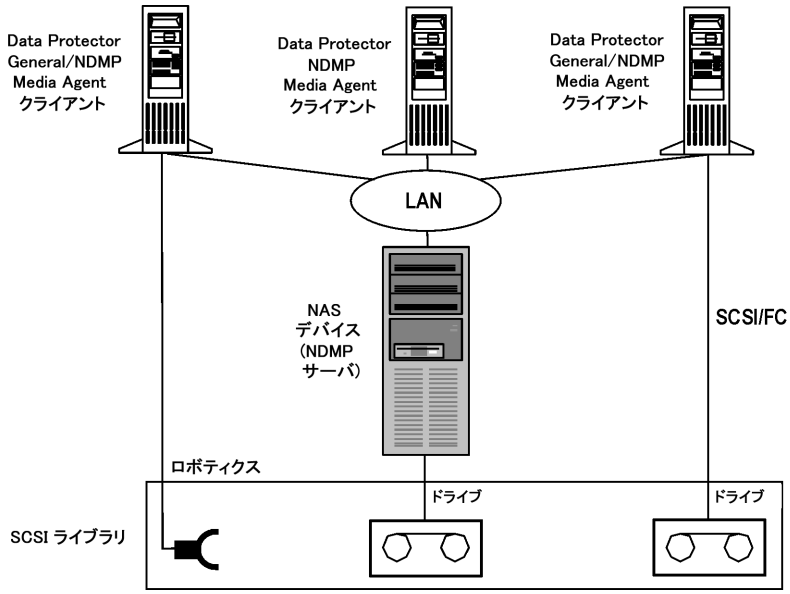
表 8 ロボティクス制御に必要な Data Protector Media Agent

	ロボティクス制御プロトコル			
	ADIC/GRAU	**StorageTek ACS**	**SCSI**	**NDMP**
ドライブ制御プロトコル (NDMP 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

「SCSI ライブラリの共有 (ロボティクスを Data Protector クライアントシステムに接続)」(107 ページ) から「ADIC/GRAU ライブラリまたは StorageTek ACS ライブラリの共有」(109 ページ) 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 48 SCSI ライブラリの共有 (ロボティクスを Data Protector クライアントシステムに接続)

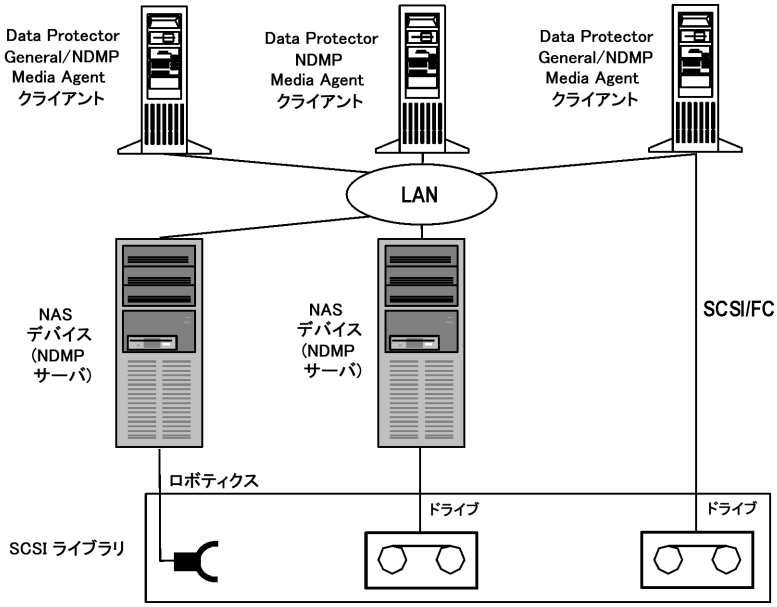


「SCSI ライブラリの共有 (ロボティクスを Data Protector クライアントシステムに接続)」(107 ページ) に示す SCSI ライブラリのロボティクスは、General Media Agent または NDMP Media Agent のインストールされた Data Protector クライアントシステムに接続され、そのクライアントシステム上に構成されています。このクライアント上の General Media Agent または NDMP Media Agent は、SCSI ロボティクス制御プロトコルを使用します。ロボティクスを接続した Data Protector ク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。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。

図 49 SCSI ライブラリの共有 (ロボティクスを NDMP サーバーに接続)



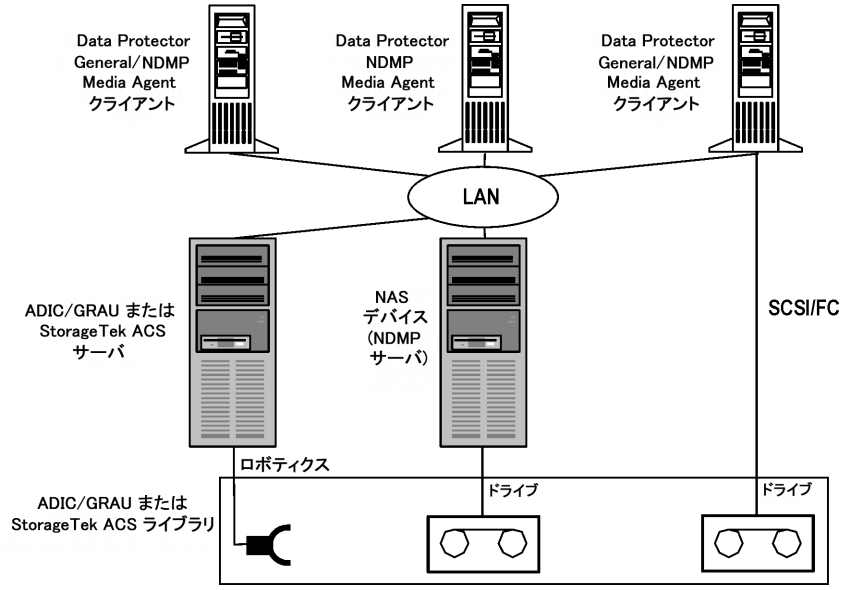
「SCSI ライブラリの共有 (ロボティクスを NDMP サーバーに接続)」 (108 ページ) に示す SCSI ライブラリでは、ライブラリのロボティクスが NDMP サーバーに接続され、General Media Agent または NDMP Media Agent のインストールされた Data Protector クライアントシステム上に構成されています。このクライアント上の General Media Agent または NDMP Media Agent は、SCSI ロボティクス制御プロトコルを使用します。ロボティクスを接続した NDMP サーバーに、さらに 1 つ以上のドライブを接続することも可能です。

重要: ロボティクスを接続した NDMP サーバーに NDMP 専用ドライブも接続する場合は、ロボティクスと NDMP 専用ドライブを担当する Data Protector クライアントシステムに、必ず NDMP Media Agent をインストールしなければなりません。これは、NDMP 専用ドライブの制御に、NDMP ドライブ制御プロトコルが使用されるためです。

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

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

図 50 ADIC/GRAU ライブラリまたは StorageTek ACS ライブラリの共有



「ADIC/GRAU ライブラリまたは StorageTek ACS ライブラリの共有」 (109 ページ) に示す ADIC/GRAU ライブラリ (または StorageTek ACS ライブラリ) では、ライブラリのロボティクスが ADIC/GRAU サーバー (または StorageTek ACS サーバー) に接続され、General Media Agent または NDMP Media Agent のインストールされた Data Protector クライアントシステム上に構成されています。このクライアント上の General Media Agent または NDMP Media Agent は、ADIC/GRAU ロボティクス制御プロトコルを使用します。ADIC/GRAU サーバーや StorageTek ACS サーバーに、さらに 1 つ以上のドライブを接続することも可能です。

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

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

ディスクバックアップ

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

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

ディスク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ると、上記の制限事項を解消できます。短期間のバックアップソリューションとしては、ディスクベースのデバイスだけで十分です。一方、長期にわたるバックアップソリューションが必要な場合は、ディスクベースのデバイスに保存したデータを定期的にテープに移すことで、ディスクスペースを解放するという手法が有効です。このプロセスを、**ディスクステージング**と呼びます。

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

Data Protector のディスクベースのデバイス

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

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

スタンドアロンファイルデバイス

スタンドアロンファイルデバイスは、ディスクベースのバックアップデバイスのうち最も単純なものです。1 つのスロットで構成されており、このスロットにデータをバックアップできます。このデバイスのプロパティは、いったん構成すると変更できません。最大容量は 2TB です

(このデバイスが動作するオペレーティングシステムで、このファイルサイズがサポートされていることが前提となります)。

ファイルジュークボックスデバイス

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

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

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。さらに、合成バックアップのようなアドバンストバックアップ戦略を用いることもできます。

ファイルライブラリデバイスの機能の詳細は、『HP Data Protector ヘルプ』の索引「ファイルライブラリデバイス」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。

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

Data Protector と Storage Area Network

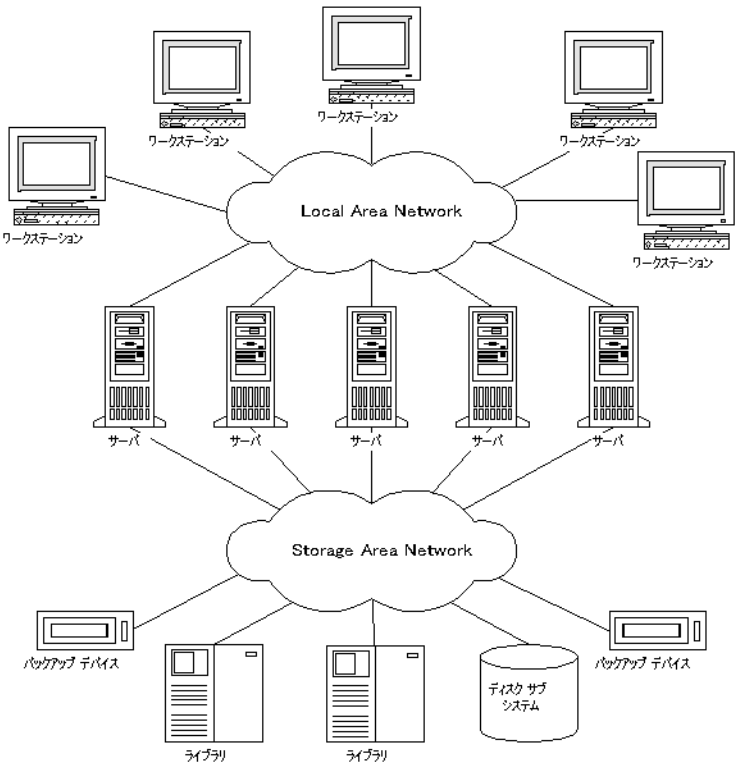
企業内のどこにどのような形でデータを保存するかは、ビジネスに重大な影響を及ぼす可能性があります。ほとんどの企業にとって、情報はますます必要不可欠なものとなりつつあります。今日ではテラバイト単位のデータに、ユーザーがネットワークを介してアクセスできなければなりません。Data Protector は SAN (Storage Area Network) ベースの Fibre Channel テクノロジを実装しており、新たなデータ記憶ソリューションの提供が可能です。

Storage Area Network

Storage Area Network (SAN) では、すべてのネットワークリソース間で **any-to-any** の接続が可能となるため、複数のクライアントシステム間でデバイスを共有でき、デバイスの可用性だけでなくデータ トラフィックの性能も向上します。

SAN の概念を導入すると、複数のデータ記憶デバイスおよびサーバー間での情報交換が可能になります。サーバーは、任意のデバイス上のデータを直接取得でき、従来型の LAN を介したデータ転送の必要はありません。SAN は、サーバー、バックアップデバイス、ディスクアレイ、およびその他のノードから構成され、これらがすべて高速なネットワーク接続 (通常は 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。

図 51 Storage Area Network



ファイバーチャネル

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。この標準では、光ケーブルまたは銅線ケーブルを使用して、大容量データファイルの双方向送信が可能です。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。

サポートされる構成の一覧について、http://support.openview.hp.com/selfsolve/manuals 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、一般的にはサーバーとバックアップデバイスを接続することができます。この方法では、性能の向上と長距離間のノードの接続という基本的な利点が得られます。

ループトポロジー

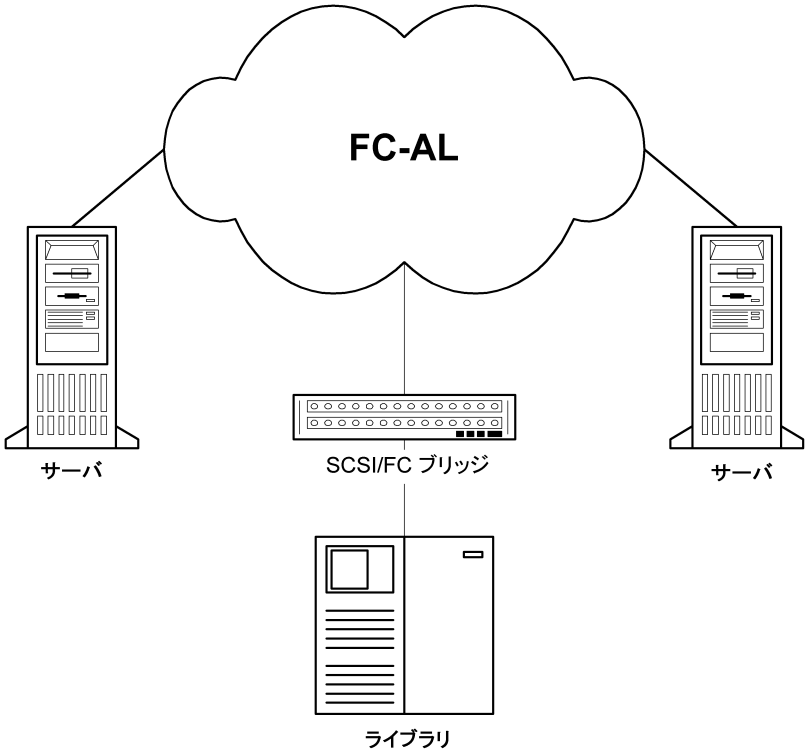
ループトポロジーは、FC-AL (Fibre Channel Arbitrated Loop) 標準をベースにしています 。ノードとなるのはサーバー、バックアップデバイス、ハブ、スイッチなどです。ループ内のすべてのノードは、そのループ内の任意のノードと通信でき、すべてのノードが同一の帯域幅を共有します。FC-AL ループの実装には、通常 FC-AL ハブと自動ポートバイパスが使用されます。自動ポートバイパスを使うと、ループへのノードのホットプラグが可能になります。

LIP

LIP (Loop Initialization Primitive) 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。「Loop Initialization プロトコル」 (114 ページ) を参照してください。

バックアップや復元中に SCSI バスがリセットされると、書き込みエラーとして記録されます。Data Protector では、書き込みエラーが発生したときにはすべての操作を中止します。バックアップを実行していた場合は、(メディアにすでにバックアップされている情報をコピーした後) メディアを再フォーマットしてバックアップを再開することをお勧めします。

図 52 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。このためには、ロックメカニズムを使用します。

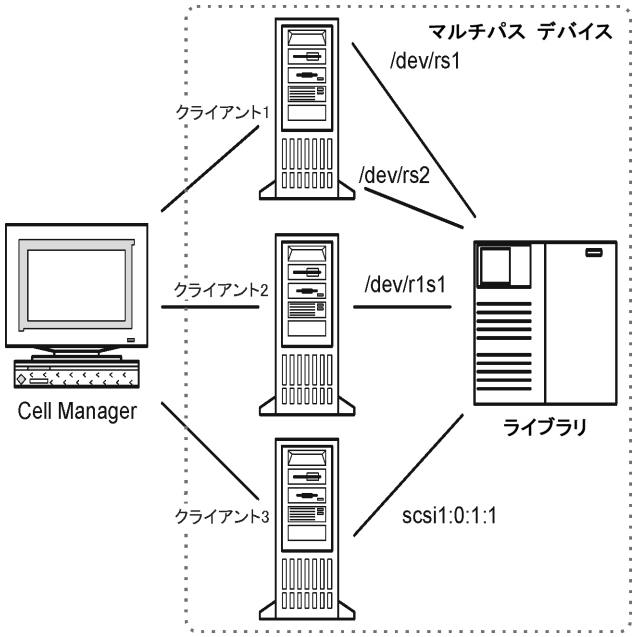
SAN テクノロジでは、複数のシステムからライブラリのロボティクスデバイスを制御するための、非常に優れた方法が用意されています。そのため、1 つのシステムからのみロボティクスを制御できるようにも (従来の方法)、またはライブラリを使用する個々のシステムからロボティクスに直接アクセスできるようにも構成できます (関連するすべてのシステム間でロボティクスへの要求を同期化できることが前提)。

物理デバイスに対する複数パスの構成

通常、SAN 環境のデバイスは複数のクライアントに接続されているため、複数のパス (クライアント名と SCSI アドレス (UNIX 上ではデバイスファイル) の組み合わせ) からアクセスが可能です。Data Protector では、これらのパスのいずれかを使用できます。同一物理デバイスに対するすべてのパスをまとめて、1 つの論理デバイスとして構成することも可能です。これを、**マルチパスデバイス**と呼びます。

たとえば、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。マルチパスデバイスには、このテープデバイスへの 4 つのパスすべてが含まれています。

図 53 マルチパスの構成例



複数のパスを使う理由

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。この問題を回避するには、複数の論理デバイスを、ロック名を使用して単一の物理デバイスとして構成する必要がありました。このようにして、複数のシステムから単一の物デバイスへのアクセスの構成にロック名を使用する場合は、各システムですべてのデバイスを構成する必要がありました。たとえば、単一のデバイスに接続されているクライアントが 10 個あった場合は、同じロック名のデバイスを 10 個構成する必要がありました。Data Protector の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によってシステムの復元性が向上します。Data Protector では最初に定義されたパスの使用を試みます。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。リストされているパスがすべて利用不可能だった場合にのみ、セッションは中断されます。

パスの選択

バックアップセッション中は、バックアップ仕様で優先クライアントが選択されている場合を除き、構成時に定義された順序でデバイスパスが選択されます。その場合は、選択されている優先クライアントが最初に使用されます。

復元セッションでは、次の順序でデバイスパスが選択されます。

1. **すべて**のオブジェクトを同じターゲットクライアントに復元する場合は、オブジェクトが復元されるクライアント上のパス
2. バックアップに使用されたパス
3. その他の利用可能なパス

直接ライブラリアクセスが有効な場合は、構成されている順序に関係なく、最初にローカルパス (あて先クライアント上のパス) がライブラリ制御に使用されます。

以前のバージョンとの互換性

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。

デバイスのロック

デバイスロック機構は、Data Protector のみが複数のシステムから渡されたデータやコマンドを使ってデバイスを操作する場合だけでなく、複数のアプリケーションが同一デバイスを使用する場合にも対処できなければなりません。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

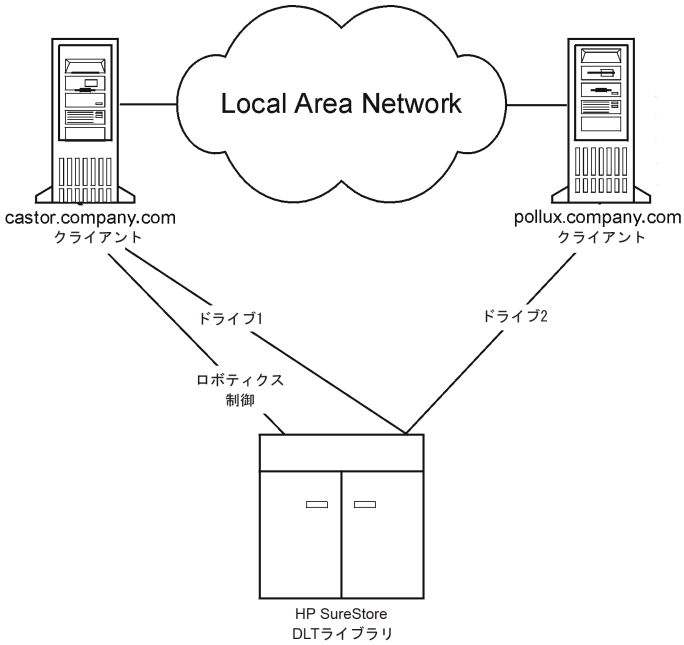
SCSI ライブラリデバイスでの Data Protector の構成時には、クライアントシステムがライブラリロボティクスにアクセス可能な方法として、間接ライブラリアクセスと直接ライブラリアクセスの 2 つの方法があります。

間接ライブラリアクセス

この構成は SAN を導入する場合も、従来型の SCSI による直接接続環境でも使用できます。この構成では各システムは、ライブラリロボティクスへの直接アクセス権を持つクライアントシステムに要求を転送することにより、ライブラリロボティクスへのアクセスが可能になりま

す。この方法は間接ライブラリアクセスと呼ばれます。「間接ライブラリアクセス」(117 ページ) の例では、2 台のクライアントシステムが、1 台の HP 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 54 間接ライブラリアクセス



この構成では、ロボティクスを制御するクライアントシステム (この例の場合は `castor`) で障害が発生すると、共有ライブラリを使用できなくなる点に注意してください。

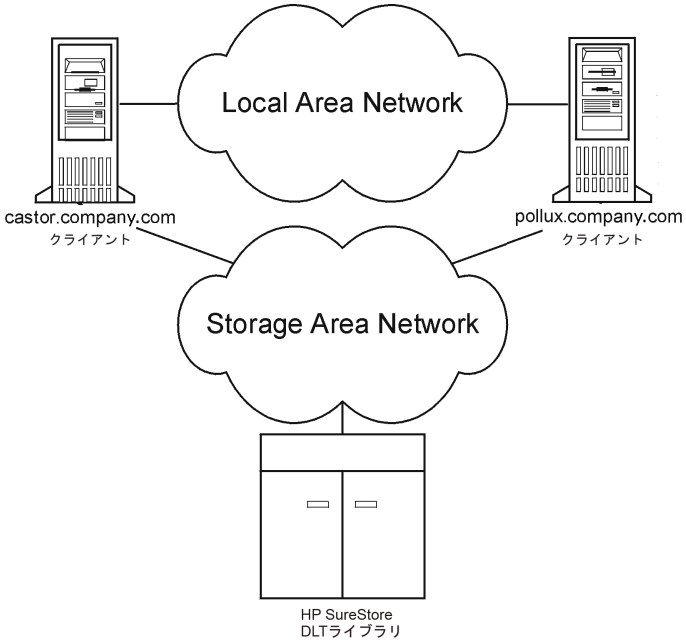
直接ライブラリアクセス

SAN の概念を導入する場合は、SCSI ライブラリとともに Data Protector を構成するときに、個々のクライアントシステムからライブラリロボティクスとドライブに直接アクセスできるように構成できます。この方法は直接ライブラリアクセスと呼ばれます。

この場合は、ロボティクスに対する単一の「制御クライアントシステム」は存在しません。そのため、ロボティクスを制御するシステムで障害が発生しても、他のシステムでは問題なくライブラリを使用できます。再構成の必要はありません。ロボティクスは複数のクライアントシステムから制御できます。

「直接ライブラリアクセス」(118 ページ) 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 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 55 直接ライブラリアクセス



クラスター内のデバイス共有

SAN の概念と組み合わされることが多いクラスター化は、ノード間でのネットワークリソース (ネットワーク名、ディスク、テープデバイスなど) の共有を基盤に構築されます。

クラスター対応アプリケーションは仮想ホスト上で実行されるため、その時々でクラスター内の任意のノード上で実行されている可能性があります。そのため、これらのアプリケーションをローカルバックアップするには、実際のノード名ではなく仮想ホスト名を指定してデバイスを構成する必要があります。各物理デバイスに対するデバイス構成を必要に応じて複数定義し、デバイスロック機構にはロック名を使用してください。詳細については、「デバイスのロック」 (116 ページ) を参照してください。

静的ドライブ

静的ドライブとは、クラスター内の実ノード上に構成されるデバイスです。これらのドライブは、共有されていないディスクを持つシステムのバックアップに使用できます。ただし、クラスター対応アプリケーショは、クラスター内の任意のノードで実行される可能性があるため、これらのアプリケーションのバックアップには静的ドライブは使用できません。

浮動ドライブ

浮動ドライブは、仮想システム名を使用して、仮想ホストに構成するデバイスです。クラスター対応アプリケーションをバックアップする場合は、この浮動ドライブを構成してください。浮動ドライブを使うと、クラスター対応アプリケーションが現在どのノード上で実行されていても、Data Protector はそのノード上で確実に Media Agent を開始できます。

メディア管理

エンタープライズ環境で大量のメディアを管理する場合に、深刻な問題が生じることがあります。Data Protector のメディア管理機能を使用すると、 柔軟かつ効率的にバックアップデータをメディアに割り当てることができます。これは、メディアの自動での割り当て方法や厳密な割り当て方法を定義することにより、さまざまに実現できます。

メディア管理機能

Data Protector は以下に示すようなメディア管理機能を備えており、大量のメディアを簡単に効率よく管理できます。

- メディアをメディアプールと呼ぶ論理グループに分けることにより、個々のメディアを意識せずに大量のメディアをグループとして一括管理できます。
- Data Protector では個々のメディアと、そのメディアの状態がすべてトラッキングされています (データ保護の有効期限、バックアップ時にそのメディアを使用できるかどうか、各メディアにバックアップされている情報に関するカタログ情報など)。
- メディアへの物理的なアクセスを行わずに、Data Protector Cell Manager から別の Data Protector Cell Manager にメディア関連のカタログデータをすべて転送できます。
- メディアの自動交換方針を設定でき、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。
- メディア上のデータの追加コピーを対話式または自動的に作成できます。

この章では、上記の機能をさらに詳しく説明します。

メディアのライフサイクル

一般的なメディアのライフサイクルは、以下の各段階から構成されます。

1. バックアップに使用するための準備をします。

   準備には、 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、「バックアップ開始前のメディア管理」 (126 ページ) 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、「バックアップセッション中のメディア管理」 (127 ページ) を参照してください。

3. データストレージのメディアを安全な場所 (ボールト) に長期間保管します。Data Protector のデータ複製方法のいずれかを使って、ボールティング用にバックアップしたデータのコピーを作成することができます。

   詳細は、「バックアップセッション後のメディア管理」 (131 ページ) を参照してください。
4. メディア上のデータが不要になったら、新しいバックアップに再使用できるように、メディアをリサイクルします。
5. メディアを廃棄します。

   使用期限が切れたメディアには不良マークが付加され、Data Protector では使用されなくなります。

   「メディア状態の計算」 (130 ページ) 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。たとえば一つのメディアプール内に DLT メディアと DAT/DDS メディアを混在させることはできません。

メディアが現在どこに存在するかは、プールとの対応付けには関係ありません。メディアがドライブ、ライブラリのリポジトリスロット、ボールト、またはその他の場所にあるかどうかは問題ではありません。リサイクルされ、セルからエクスポートされるまで、常にそのプールに属します。

複数のデバイスで、同一プールに所属するメディアを共有することも可能です。

メディアプールのプロパティの例

プールのプロパティ例を以下に示します:

- 追加可能

  このオプションを設定すると、バックアップセッションの実行時に、プール内のメディアの空きスペースにデータが書き込まれます。

  このオプションが選択されていない場合は、各メディア内には同一セッションのデータのみが格納されます。

- 増分のみ追加可能

  バックアップセッション時には、増分バックアップが実行された場合に限り、メディアにデータが書き込まれます。そのため、メディア内に十分なスペースが残っている場合には、フルバックアップと増分バックアップがすべて同一のメディア上に保存されるようになります。

- メディア割り当てポリシー

  バックアップ用メディアの選択方法については、厳密さが異なるいくつかの設定レベルが用意されています。厳密な設定では、使用するメディアが Data Protector により指定され、緩やかな設定では、Data Protector は新しい (空の) メディアも含め、使用可能な任意のメディアを使用します。

各デバイスにはデフォルトプールが設定されています。バックアップ仕様内でこのプールを変更することも可能です。

その他のメディアプールプロパティの詳細については、『HP Data Protector ヘルプ』の索引「メディアプール、プロパティ」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、「IDB のアーキテクチャ」 (137 ページ) を参照してください。

メディアプールの使用方法

メディアプールの大部分はユーザーが自由に設定できます。たとえば、以下のような基準でプールを定義できます。

- システムプラットフォームごと (UNIX システム用、Windows Vista システム用、Windows 7 用に、それぞれ個別のプールを設定するなど)。
- システムごと (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ポリシーが適用されます。

デフォルトのメディアプール

Data Protector では、さまざまなメディアタイプ別に、デフォルトのメディアプールが用意されています。これらのデフォルトメディアプールを使用すると、独自のメディアプールを作成しなくても、簡単にバックアップを実行できます。ただし、大規模な環境で、効率よくバックアップを管理するためには、目的に応じたメディアプールを作成する必要があります。バックアップの実行時には、使用するメディアプールを指定できます。

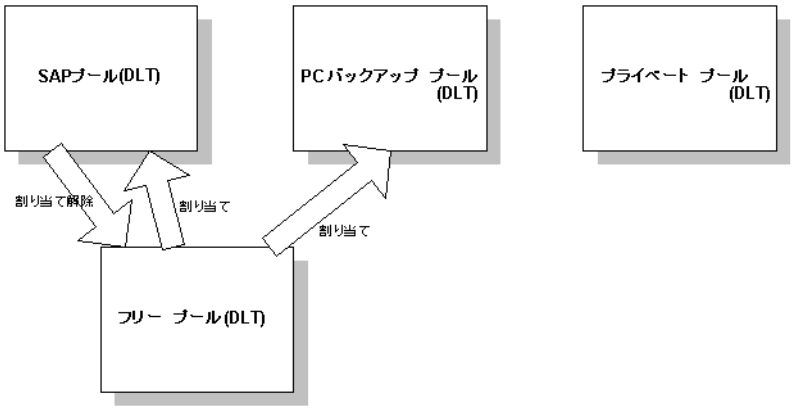
フリープール

あるメディアプールに割り当てたメディアの容量が不足した場合、同じ種類であっても他のプールにあるメディアを代用することはできません。他のプールのメディアを使用すると、不要なマウント要求が発生してオペレータ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 56 フリープール



フリープールを使用するタイミング

メディアは、以下の 2 つのイベント時に通常のプールとフリープールの間で移動されます (「フリープール」 (122 ページ) を参照してください)。

- 割り当て時。メディアはフリープールから通常のプールに移されます。
- 割り当て解除時。メディアは通常のプールからフリープールに移されます。割り当て解除を自動で行うかどうかは、GUI で指定できます。「フリープール」 (122 ページ) の PC バックアッププールの例では、メディアは自動的には割り当て解除されません。

保護 (割り当て済み、または使用中) メディアは特定の通常プール (SAP プールなど) に所属しますが、Data Protector のフリーメディアはフリープールに (自動的に) 移動できます。このフリープールは、後に、このフリープールを使用するように構成されたすべてのプールに対して、フリーメディアを割り当てる際に使用されます。

「フリープール」 (122 ページ) 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、フリープールを手動でまたは自動的に作成できます。通常のプールにリンクされているフリープールや空でないフリープールは削除できません。
- 通常のプールと異なり、割り当て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。

- 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、このフリープールに構成された状態要素を使用できます。
- メディアを手動で移動すること (保護メディアをフリープールへ移動したり、自動的に割り当て解除されるように構成されている、非保護メディアを通常のプールへ移動すること) はできません。
- フリープール内のメディアに対してインポート、コピー、リサイクルなどの操作は実行できません。
- マガジンをサポートするプールでフリープールは使用できません。
- フリープール使用時に、プール内に一時的な不整合が生じる場合があります (通常のプール内の非保護メディアが割り当て解除プロセスを待機しているなど)。
- メディアの保護期限が切れた後に保護期間を変更 (たとえば無期限に変更) すると、メディアがフリープール内にあってもバックアップ用に割り当てられません。
- フリープールから割り当てられた場合は、異なるデータ形式タイプを持つメディアを使用でき、自動的に再フォーマットされます。たとえば NDMP メディアは、通常のメディアに再フォーマットされます。

フリープールの詳細は、『HP Data Protector ヘルプ』の索引「フリープール、特性」を参照してください。

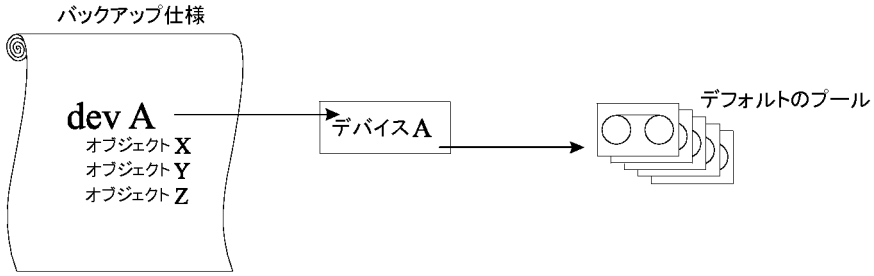
メディアプールの使用例

バックアップ環境を選択する上で検討の対象となる可能性のある構成例を以下に示します。

例 1

「単一デバイス/単一メディアプールの単純な対応付け」(123 ページ) に示すモデルでは、すべてのオブジェクトが同一のメディアプールにバックアップされます。このバックアップ仕様ではプールを指定していないため、デバイス定義で指定されているデフォルトのプールが使われます。

図 57 単一デバイス/単一メディアプールの単純な対応付け



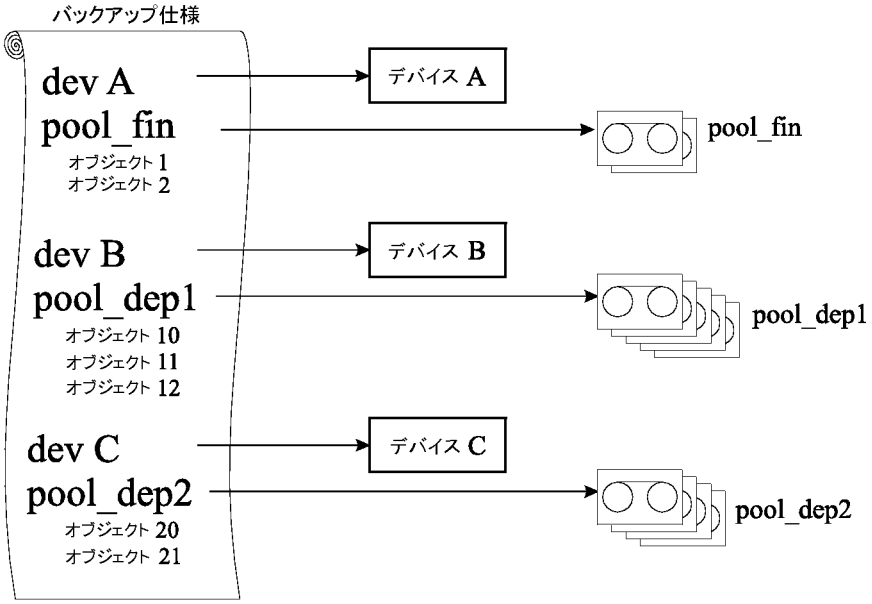
例 2

大容量ライブラリデバイス内には、多数の物理ドライブが装備され、さまざまな部門やアプリケーションで使われる多数のメディアが格納されています。この場合、「大容量ライブラリを使用する場合のメディアプール構成例」(124 ページ) に示すように、各部門別のメディアプールを構成して、ライブラリ内のドライブのうち、どのドライブを実際のデータ転送に使用するかを指定できます。図の中でバックアップ仕様からメディアプールに伸びている矢印は、バックアップ仕様の中でそのメディアプールを指定していることを示します。バックアップ仕様の

中でメディアプールを指定していない場合は、デバイス定義で指定されているデフォルトプールが使用されます。

メディアプールと大容量ライブラリデバイスとの関連については、「大容量ライブラリ」(103 ページ)を参照してください。

図 58 大容量ライブラリを使用する場合のメディアプール構成例

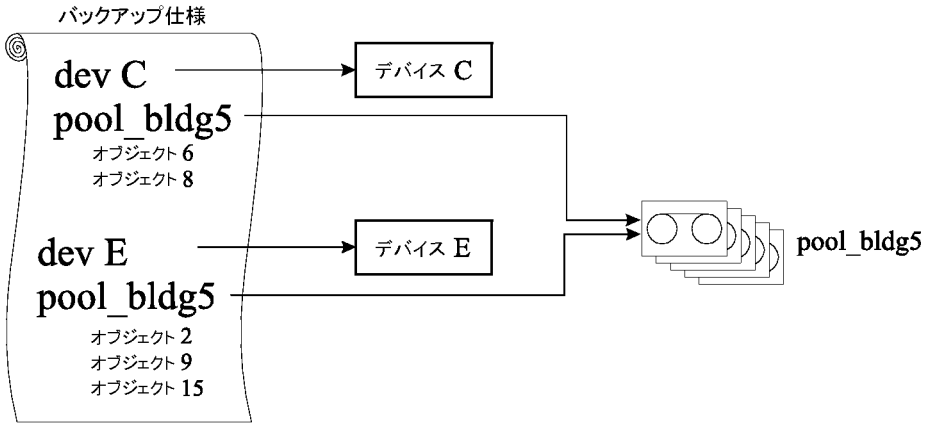


例 3

「複数デバイスと単一メディアプールの対応付け」(124 ページ)は、複数のデバイスから、同一メディアプール内のメディアに、データを同時にバックアップする場合の例を示したものです。どのプールを使用するかにかかわらず、複数のデバイスを並列に使用すると、性能は向上します。

詳細は、「デバイスリストと負荷調整」(98 ページ)を参照してください。

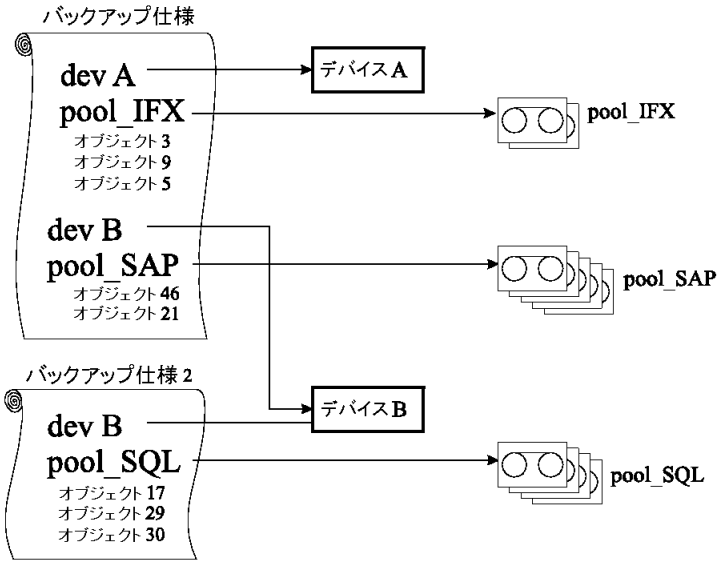
図 59 複数デバイスと単一メディアプールの対応付け



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 60 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。

メディア交換方針と Data Protector

自動メディア交換と自動メディア操作

Data Protector では、メディア交換およびメディア操作が 以下のように自動化されています。

- メディアはメディアプールにグループ化されるため、単独のメディアを管理する必要はなくなります。Data Protector では、メディアプール内の各メディアを自動的に追跡および管理します。
- バックアップされるデータがどのメディアに書き込まれるかを決める必要はありません。それは、Data Protector によって行われます。管理者は、メディアプールにバックアップを行います。
- Data Protector では、指定したメディア割り当てポリシーと使用オプションに基づいて、メディアプールから自動的にメディアが選択されます。必要に応じて、自動選択機能を無効にし、手動でメディアを選択することも可能です。

- Data Protector で構成したメディアについては、Data Protector ユーザーインタ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。「バックアップ用メディアの選択」 (128 ページ) 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 (メディアヘッダー) にも書き込まれます。メディアを初期化 (フォーマット) するときには、そのメディアが所属するメディアプールも指定する必要があります。

設定したプール方針によっては、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、「バックアップ用メディアの選択」 (128 ページ) を参照してください。

Data Protector メディアのラベリング

Data Protector で使われるメディアのラベリング

Data Protector で使用するメディアを追加するために、メディアを初期化 (フォーマット) するときには、このメディアを後から識別できるように、メディアラベルを付加しなければなりません。デバイスにバーコードリーダーが装備されている場合は、メディアラベルの先頭にバーコードがメディアの説明として自動的に表示されます。このバーコードは、IDB 内で管理されている各メディアに対する一意の識別子となります。メディアを初期化する際に、バーコードをメディアラベルとして使用することも可能です。

また、各メディアに対しては、Data Protector によって、そのメディアを一意に識別するメディア ID が自動的に割り当てられます。

ANSI X3.27他のシステムでも識別用のラベルがテープに書き込まれます。Data Protector では、これらのラベルと一緒に他の情報をメディアのヘッダーと IDB に書き込みます。

メディアラベルを変更すると、メディア自体ではなく、IDB 内のメデ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。たとえば、メディア上に新しいバックアップ情報を書き込もうとした場合、メディア管理システムにより、メディア上の既存データの保護期限が切れているかどうかがチェックされます。ユーザー定義のラベルは、メディアを識別するために使用します。

位置フィールド

バックアップメディアは通常さまざまな場所に保管されています。たとえば、バックアップメディアは復元時にすぐに使用できるように社内に置いておき、バックアップデータのコピーを保管したメディアは安全性を考慮して社外に保管するといったケースが考えられます。

各メディアの位置フィールドは、オペレータが自由に変更できます。このフィールドを使用すると、メディアの場所を追跡することができます。意味のある位置フィールドの例は、ライブラリ、社外、vault_1 などです。

複数のメディアセットに存在するオブジェクトバージョンを復元する場合には、メディアの位置を設定する方法が便利です。メディアの位置の優先順位を設定することができます。この優先順位は復元に使われるメディアセットの選択に影響します。復元用のメディアセット選択の詳細は、「メディアセットの選択」 (91 ページ) 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」 (43 ページ)
- 「メディアプール」 (120 ページ)

バックアップ用メディアの選択

Data Protector では、メディア割り当てポリシーに基づいて、バックアップ用メディアが自動的に選択されます。これによって、メディア管理およびメディア処理が簡素化されます。バックアップオペレータは、手動でバックアップ用メディアを管理する必要はありません。

メディア割り当てポリシー

バックアップ用メディアの選択方法は、 メディア割り当てポリシーに基づいて決定されます。方針に [緩和] 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 [厳格] 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、メディア割り当てポリシーの [厳格] と組み合わせて使用してください。この場合、メディアは指定された順番どおりに使用されます。この順番どおりにメディアが見つからなければ、Data Protector によりマウント要求が発行されます。

メディアの状態

バックアップ用メディアの選択時には、各メディアの状態も考慮されます。たとえば、状態が [良好] のメディアは、状態が [普通] のメディアよりも優先的に使用されます。詳細は、「メディア状態の計算」 (130 ページ) 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、メディアの使用法で設定します。

メディアの使用法

選択できるメディアの使用法は、以下のとおりです。

追加可能

バックアップセッション時には、まず初めに、前回のバックアップセッションで最後に使用されたメディア上に残っているスペースにデータが書き込まれます。このセッションで 2 本目以降に使われるメディアについては、テープの先頭からデータが書き込まれるため、保護期限が切れているテープまたは新しいテープのみが使用されます。この方針を選ぶとメディアスペースを節約できますが、1 つのメディア内に複数のメディアセットのデータが含まれる可能性があるため、ボールティング作業は多少複雑になります。

追加不可能

バックアップセッション時には、使用可能な最初のバックアップ用メディアの先頭から、データが書き込まれます。各メディアには単一セッションからのデータのみが格納されています。このため、ボールティング作業が容易になります。

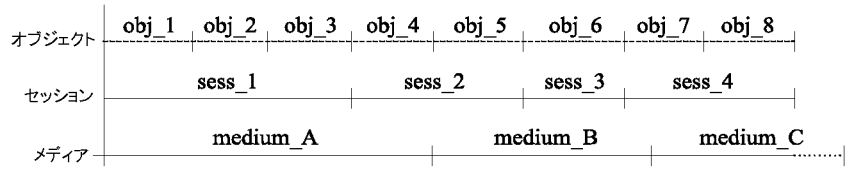
増分のみ追加可能

バックアップセッション時には、増分バックアップが実行された場合に限り、メディアにデータが書き込まれます。そのため、メディア内に十分なスペースが残っている場合には、フルバックアップと増分バックアップがすべて同一のメディア上に保存されるようになります。

オブジェクトのメディアへの分散

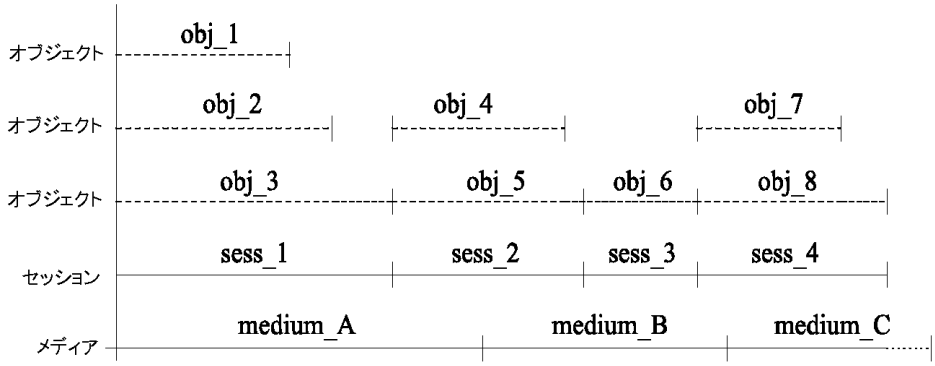
以下の図は、複数のオブジェクトを複数のメディア上に保存する場合の例を示したものです。

図 61 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)



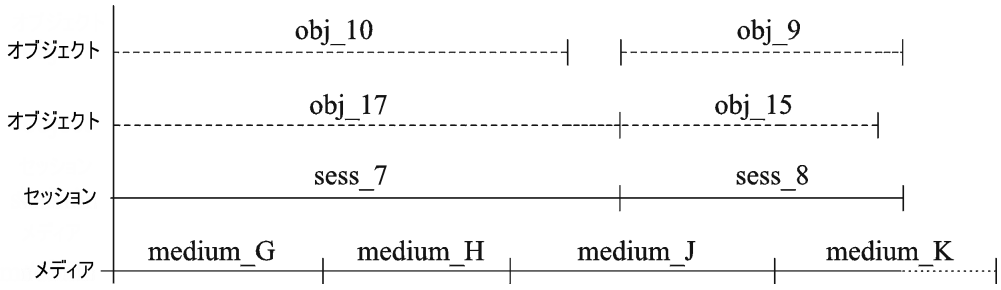
「1 つのメディア上に複数セッションの複数オブジェクトを格納 (順次書き込み)」 (129 ページ)では、メディアの使用法に [追加可能] を指定した状態で、4 つのセッションにわたって、8 つの順次書き込みを実行しています。データは、4 つのセッションにわたって書き込まれますが、1 度に書き込まれるオブジェクトは 1 つだけになります。3 つのメディアは、同一のメディアプールに所属しています。**medium_A** と **medium_B** はすでに一杯になっていますが、**medium_C** にはまだ多少のスペースが残っています。

図 62 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)



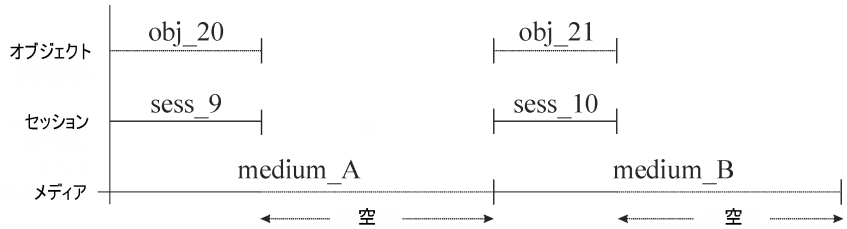
「1 つのメディア上に複数セッションの複数オブジェクトを格納 (並列書き込み)」 (129 ページ)の例では、4 つのセッションで、並列処理を有効にして同時書き込みを可能にした状態で、8 つのオブジェクトを書き込んでいます。この場合、**obj_1**、**obj_2**、**obj_3** は **sess_1** で同時にバックアップされ、**obj_4** と **obj_5** は **sess_2** で同時にバックアップされました。**obj_1** は **system_A** の、**obj_2** は **system_B** の情報である場合もあれば、これらのオブジェクトが同一システム上の個別のディスク上の情報である場合も考えられます。メディアの使用法は、[追加可能] に設定されています。

図 63 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



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

図 64 各オブジェクトを個別のメディアに格納



「各オブジェクトを個別のメディアに格納」(130 ページ)の例では、オブジェクトごとに 1 つのバックｓアップ仕様を作成し、メディアの使用法には [追加不可能] を指定しています。この方法では、メディアの消費量が多くなります。この方法で、メディアの使用法を [増分のみ追加可能] に変更すると、同一オブジェクトの増分バックアップのみが同じメディア上に保存されるようになります。

フルバックアップと増分バックアップに対する方針が、復元性能とメディア使用に与える影響の詳細は、「フルバックアップと増分バックアップ」(43 ページ)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、「オブジェクトのミラーリング」(86 ページ)を参照してください。

メディア状態の計算

メディア状態要素

Data Protector では、**メディア状態要素**を使用して、使用中のメディアの状態を計算します。プール全体の状態は、プール内の最も状態の悪いプールによって決まります。たとえば、メディアプール内のある 1 つのメディアの状態が不良になると、プールの状態も直ちに不良になります。そのメディアをプールから取り除くと、プールの状態は普通または良好に戻ります。

メディアには、良好、普通、不良の 3 つの状態があります。

各メディアについて以下を使用し、状態を計算します。

- 上書き回数

  メディアの使用回数は、そのメディアが上書きされた回数として定義されます。ここで、使用回数とは、メディアに対してこれまでに行われた上書きの回数を意味します。上書き回数のしきい値を超過したメディアは、[不良] 状態と見なされます。

- メディアの使用期間

  メディアの使用期間は、メディアのフォーマットつまり初期化以降の経過月数として計算されます。メディアの使用期間が指定された月数を超えると、不良マークが付加されます。

- デバイスエラー

  なんらかのデバイスエラーが発生すると、メディアに不良マークが付加されます。たとえばバックアップ中にデバイス障害が発生した場合は、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。以下の点に注意してください。

- メディアの上書きを防止する。

  データ保護期間はバックアップの構成時に指定しますが、バックアップ以降にも変更可能です。データおよびカタログ保護の詳細については、「バックアップデータおよびバックアップデータに関する情報の保存」 (68 ページ) を参照してください。

- 物理的損傷からメディアを保護する。

  永久に保存するデータが書き込まれているメディアは、安全な場所に保管することをお勧めします。

- バックアップデータのコピーを作成し、そのコピーを安全な場所に保管する。

  「バックアップデータの複製」 (78 ページ) 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] 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

お客様のここで、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。

これは、Data Protector が 1 週間に一度のフルバックアップと、毎日の増分バックアップを行うように設定されていることを意味します。データ保護期間は 5 年に設定します。カタログ保護期間は 1 年に設定します。こうすることで、1 年間はデータのブラウズや復元を簡単に実行でき、さらにデータそのものの復元は 5 年間可能になります。フルバックアップで作成されたメディアについてはコピーを作成し、保管場所に格納しておきます。バックアップ後 1 年が経過したメディアについては、Data Protector のデータベースから、そのメディア上のデータに関する詳細情報が自動的に削除されます。これにより、新しい情報を保存するためのスペースがデータベース内に確保されます。

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の詳細については、「バックアップデータおよびバックアップデータに関する情報の保存」 (68 ページ) を参照してください。

4 ユーザーとユーザーグループ

この章では、Data Protector のセキュリティ、ユーザー、ユーザーグループ、およびユーザー権限について説明します。

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 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。

この項ではデータのバックアップや復元、バックアップセッションの進捗状況のモニタリングに Data Protector を使用する場合の、セキュリティ関連問題について説明します。

バックアップデータへのアクセス権

データのバックアップを行い、そのデータを復元することは本質的にデータのコピーと同じことです。このため、データへのアクセスをアクセス権のあるユーザーのみに制限することが重要です。

Data Protector には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。他のユーザーに対しては、データがバックアップされているという事実さえも知らされません。そのため、たとえばバックアップオペレータ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] オプションを使用します。その手順については、『HP Data Protector ヘルプ』を参照してください。

ユーザーとユーザーグループ

Data Protector を使用するには、特定の権限を付与された Data Protector ユーザーとして Data Protector 構成に追加されている必要があります。ただし、あるユーザーが使用しているシステムをバックアップするために、そのユーザーを構成に追加する必要は必ずしもないことに注意してください。

ユーザーは、特定のユーザー権限 (セル内のセッションの監視、バックアップの構成、ファイルの復元など) を持つユーザーグループにまとめられます。

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。デフォルトで admin、operator、end-user という 3 つのユーザーグループが用意されています。たとえば、管理ユーザーグループのメンバーのみが、Data Protector のすべての機能にアクセスできます。オペレータは、デフォルトでバックアップの開始およびモニタリングを行うことができます。詳細は、『HP Data Protector ヘルプ』の索引キーワード「ユーザーグループ」で表示される内容を参照してください。

ヒント: 小規模な環境では、1 人のユーザーですべてのバックアップ関連作業を実行できます。このユーザーは、Data Protector の [Admin] ユーザーグループに所属しなければなりません。この場合は、その他のユーザーを Data Protector 構成内に追加する必要はありません。

ユーザーグループのカスタマイズ

環境に応じて、どのデフォルトの Data Protector ユーザーグループを使用するのか、または変更して使用するのか、新しいユーザーグループを作成するのかを決定します。

[Admin] ユーザーグループのデフォルトのメンバー

以下のユーザーは、インストール時に、Data Protector の [Admin] ユーザーグループに自動的に追加されます。

- UNIX Cell Manager システム上の UNIX root ユーザー
- Windows Cell Manager システムに 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。詳細は、『HP Data Protector ヘルプ』の索引キーワード「ユーザーグループ、admin」で表示される内容を参照してください。

Data Protector ユーザー権限

Data Protector ユーザーには、各自が所属するユーザーグループの Data Protector ユーザー権限が与えられます。

UNIX 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。

さらに、セルの特定のシステムへのユーザーアクションを制限することで、Data Protector のユーザーグループに用意されているユーザーセキュリティレイヤを補うこともできます。

各ユーザーグループに与えられる Data Protector ユーザー権限の詳細については、『HP Data Protector ヘルプ』を参照してください。

5 Data Protector 内部データベース

この章では Data Protector 内部データベース (IDB) のアーキテクチャ、使用方法、および操作方法について説明します。データベースの各部やレコード、データベースの増大や性能の推奨管理方法、データベースサイズの計算式について説明します。これらはデータベースを効果的に構成、保守するために必要な情報です。

IDB について

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とバックアップデータの格納先メディアのほか、バックアップ、復元、オブジェクトコピー、オブジェクト集約、オブジェクト検証、およびメディア管理の各セッションの結果や、構成済みのデバイスとライブラリなどに関する情報を保持します。

IDB を使う理由

IDB に保存された情報を利用することで、以下のことが可能になります。

- 復元が高速で便利。IDB に保存されている情報によって復元に必要なメディアを迅速に検出できるため、復元を高速に行うことができます。また復元対象のファイルやディレクトリをブラウズすることもできます。
- バックアップ管理が可能。IDB に保存されている情報によって、どのようにバックアップが行われたかを確認できます。Data Protector のレポート機能を使用して、さまざまなレポートを作成することも可能です。
- メディア管理が可能。IDB に保存されている情報によって、バックアップセッション、オブジェクトコピーセッション、およびオブジェクト集約セッション中のメディアの割り当て、メディア属性のトラッキング、異なるメディアプールに属するメディアのグループ化、テープライブラリ内のメディア位置のトラッキングなどを行えます。
- 暗号化/復号化管理。IDB に保存されている情報によって、暗号化されたバックアップまたはオブジェクトコピーセッション用に暗号化キーを割り当て、暗号化されたバックアップオブジェクトの復元に必要な復号キーを提供できます。

IDB のサイズ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。したがって、Data Protector 管理者は、IDB について十分理解し、必要に応じて、どの情報をどのくらいの期間にわたって IDB に維持するかを決定する必要があります。復元時間および機能性の側面と IDB のサイズと増加の側面のバランスを取るのは、管理者の役目です。Data Protector には、このニーズのバランスを取る際に役立つ**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。「IDB の増大と性能」 (142 ページ) 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_program_data*\db40(Windows Server 2008 の場合)、または*Data_Protector_home*\db40(その他の Windows システムの場合) の各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。

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、「企業環境」 (25 ページ) 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)
- ファイル名とその他の CDB レコードの 2 つの部分に分割された CDB(カタログデータベース)
- DCBF(詳細カタログバイナリファイル)
- SMBF(セッションメッセージバイナリファイル)
- SIBF (NDMP 統合用のサーバーレス統合バイナリファイル)
- 暗号化キーストア

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。「IDB の構成要素」 (138 ページ) を参照してください。

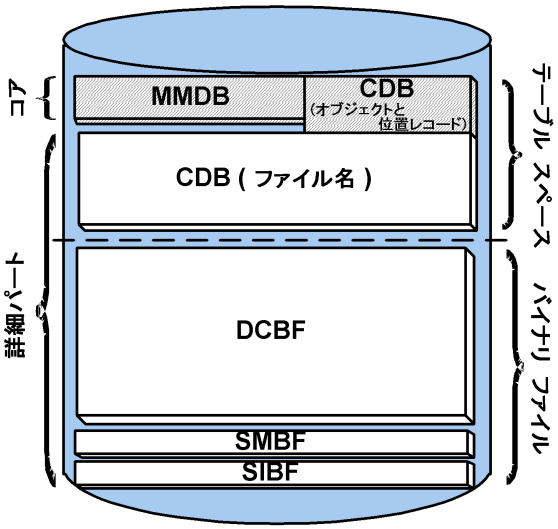
堅牢性についての注意事項と、IDB ディレクトリを再配置して堅牢性を最適化することについての推奨事項については、『HP Data Protector ヘルプ』の索引「IDB の堅牢性」を参照してください。

基礎となる技術

MMDB と CDB の各部分は、表領域を含む組込みデータベースを使って実装されています。この組込みデータベースは RDS データベースサーバー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。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 65 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 の大部分は、_Data Protector メディアに関する情報が占めるのが普通です。詳細については、「IDB サイズの見積もり」(147 ページ)を参照してください。

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、オブジェクトコピー、オブジェクト集約、オブジェクト検証、およびメディア管理の各セッションに関する情報。これは、Data Protector のモニターウィンドウに送信される情報のコピーです。
- バックアップされたオブジェクトとそのバージョン、およびオブジェクトコピーに関する情報。暗号化されたオブジェクトバージョンの場合、キー ID(KeyID-StoreID) も格納されます。
- バックアップ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 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 2GB 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。詳細については、「IDB サイズの見積もり」 (147 ページ) を参照してください。

詳細カタログバイナリファイル (DCBF)

DCBF 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。

[一つ] 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] 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%)。「IDB の増大と性能:主要な調整可能パラメータ」 (143 ページ) を参照してください。

デフォルトでは、DC ディレクトリ (`db40¥`は 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 16GB 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 50 のディレクトリを作成することができます。詳細は、『HP Data Protector ヘルプ』の索引キーワード「DC ディレクトリ」を参照してください。

セッションメッセージバイナリファイル (SMBF)

SMBF レコード

セッションメッセージバイナリファイルには、Data Protector セッション中に生成されたセッションメッセージが保存されます。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。[レポートレベル：] オプションを指定すると、バックアップ中、復元中、およびメディア管理中に表示されるメセージ数を変更できます。これによって IDB に保存されるメッセージ数も変わります。詳細は、『HP Data Protector ヘルプ』を参照してください。

サーバーレス統合バイナリファイル (SIBF)

SIBF レコード

サーバー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。これらのデータは、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。詳細については、「IDB サイズの見積もり」(147 ページ)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 3 kB 使用されます。詳細は、『HP Data Protector ヘルプ』を参照してください。

暗号化キーストアとカタログファイル

暗号化されたバックアップ中に手動または自動で作成されたすべてのキーは、キーストアに保存されます。キーは、オブジェクトコピー、オブジェクト検証、および復元の各セッションにも使用できます。ハードウェア暗号化の場合、これらのキーはオブジェクト集約セッションにも使用できます。

ソフトウェア暗号化の場合、キー ID(各キー ID は keyID と StoreID で構成される) は、暗号化されたオブジェクトバージョンにマップされます。このマッピングは、カタログデータベースに保存されています。メディア内の複数のオブジェクトに、それぞれ別のソフトウェア暗号化キーを設定できます。

ハードウェア暗号化の場合、キー ID がメディア ID にマップされ、これらのマッピングはカタログファイルに保存されます。このファイルには、暗号化されたメディアを別のセルにエクスポートできるようにするために必要な情報が含まれます。詳細は、『HP Data Protector ヘルプ』の索引キーワード「暗号化」で表示される内容を参照してください。

IDB の操作

バックアップ時

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。バックアップに対してソフトウェア暗号化が要求された場合、関係するエンティティ (ホスト) の有効な暗号化キーが、キーストアから取得され、バックアップに使用されます。キー ID(KeyID-StoreID) は、オブジェクトバージョンにリンクされ、CDB レコードに含められます。ホストと KeyID-StoreID とのマッピングは、キーストア内のカタログにも格納されます。

バックアップ中にバックアップセッションマネージャーがメディアを更新します。すべてのメディア レコードは MMDB に保存され、方針に従ってバックアップに割り当てられます。関係するメディアがハードウェア暗号化を要求したドライブ内にある場合、まず、エンティティ (メディア) の有効な暗号化キーがキーストアから取得されます。メディアと KeyID-StoreID とのマッピングは、キーストア内のカタログに記録され、メディアにも書き込まれます。

データセグメントがテープに書き込まれ、次にカタログセグメントに書き込まれると、このデータセグメントの一部である各オブジェクトバージョンに対して、メディア位置レコードが CDB に保存されます。また、カタログが DC (詳細カタログ) バイナリファイルに保存されます。Data Protector メディア 1 つにつき、1 つの DC バイナリファイルが保持されます。DC バイナリファイル名は、*MediumID_TimeStamp*.dat 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。関係するメディアに対してハードウェア暗号化が行われた場合、Media Agent は最初にキー ID(KeyID-StoreID) を検出し、Key Management Server (KMS) によってキーストアから取得されるキーを要求します。

関係するバックアップに対してソフトウェア暗号化が使用された場合、Disk Agent は暗号化されたデータを取得したときに、検出された KeyID-StoreID を KMS に送信し、キーストアから取得される関連する復号キーを要求します。

オブジェクトコピー時またはオブジェクト集約時

オブジェクトコピーセッションまたはオブジェクト集約セッション中では、バックアップと復元セッション中と同じ処理が実行されます。基本的には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またはオブジェクト集約セッションで行われることと、バックアップと復元で行われることは同じです。詳細は、「バックアップ時」(140 ページ) および「復元時」(141 ページ) を参照してください。ソフトウェア暗号化を使用するオブジェクト集約はサポートされていないため、これは当てはまりません。

オブジェクトの検証時

オブジェクト検証セッション中では、復元セッションと同じデータベース処理が実行されます。基本的には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、オブジェクトの検証を実行するホスト Disk Agent に送信されます。IDB 操作という点では、オブジェクト検証セッションで行われることと、復元セッションで行われることは同じです。検証セッション中に生成されるすべてのセッションメッセージは、セッションメッセージのバイナリファイルに保存されます。詳細は、「復元時」(141 ページ) を参照してください。

メディアのエクスポート

メディアをエクスポートすると、暗号化された情報が含まれる場合、関連するキーが Cell Manager 上でキーストアから `.csv` ファイルにエクスポートされます。このファイルは、別のセルでメディアを正常にインポートするために必要です。

削除されたアイテム

さらに、複数のアイテムが削除されます。

- エクスポートしたメディアのすべてのメディア位置レコードが CDB から削除されます。
- その他のメディアに位置レコードがないすべてのオブジェクトとオブジェクトコピーが CDB 部分から削除されます。
- 30 日を超える古いセッション (メディアが上書きまたはエクスポートされているセッション) が削除されます。また、このようなセッションのセッションメッセージも削除されます。

- MMDB 部分からメディアレコードが削除され、そのメディアの DC バイナリファイルが DCBF から削除されます。

詳細カタログの削除

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

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 Data Protector ヘルプ』の索引キーワード「IDB、復旧」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。

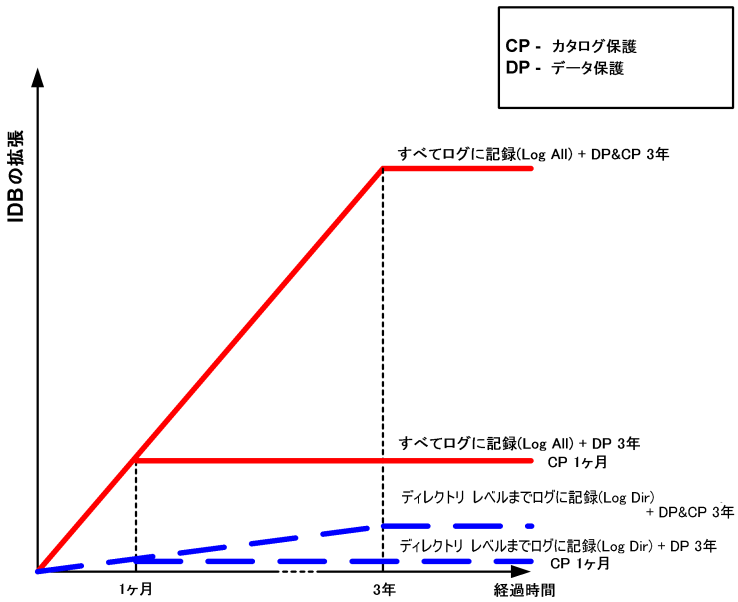
- ロギングレベルの設定。ロギングレベルでは、バックアップ時に IDB に書き込まれる詳細データ量を定義します。詳細度を高めるようにロギングレベルを変更すると、IDB への影響が増大します。詳細については、「IDB の増大と性能:主要な調整可能パラメータ」(143 ページ) を参照してください。
- カタログ保護の設定。カタログ保護は、IDB でのバックアップデータに関する情報の保管期間を決定します。カタログ保護の期間を長くすると、IDB への影響が増大します。詳細については、「IDB の増大と性能:主要な調整可能パラメータ」(143 ページ) を参照してください。
- バックアップファイル数。Data Protector では、各ファイルおよびファイルの各バージョンを記録します。IDB への影響は、バックアップの種類によって異なります。バックアップの種類については、「フルバックアップと増分バックアップ」(43 ページ) を参照してください。
- バックアップの数バックアップ

  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] 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] 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。たとえば、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とオブジェクトミラーの数。作成するオブジェクトコピーおよびオブジェクトミラーの数が多いほど、IDB に格納される情報量が増えます。オブジェクトコピー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: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、「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」(144 ページ) に示します。

図 66 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。

すべてログに記録	バックアップされるファイルやディレクトリに関するすべての詳細情報 (名称、バージョン、属性) を記録します。
ファイルレベルまでログに記録	バックアップされるファイルやディレクトリに関するすべての詳細情報 (名称とバージョン) を記録します。これは、バックアップファイルおよびバックアップディレクトリに関する全詳細情報の約 30% に相当します。
ディレクトリレベルまでログに記録	バックアップディレクトリに関するすべての詳細情報 (名称、バージョン、属性) を記録します。これは、バックアップファイルおよびバックアップディレクトリに関する全詳細情報の約 10% に相当します。
ログなし	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。

パフォーマンスへの影響

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時のブラウズ

保存される情報のレベルを変更すると、復元時に Data Protector GUI を使用してブラウズできるファイルも変わります。[記録しない] オプションを設定すると、ブラウズが不可能になり、[ディレクトリレベルまでログに記録] オプションを設定すると、ディレクトリのブラウズが可能になり、[ファイルレベルまでログに記録] オプションを設定すると、完全ブラウズが可能になりますがファイル属性 (サイズ、作成日付、変更日付など) は表示されません。

データの復元は、ロギングレベルの設定とは関係なく、いつでも行えます。データ:

- 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]、[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] 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。

[記録しない] 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。

パフォーマンスへの影響

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 [記録しない] オプションを使用してバックアップしたデータと同様に復元されます。「IDB の主要な調整可能パラメータとしてのロギングレベル」(144 ページ) を参照してください。

ロギングレベルとカタログ保護の推奨使用方法

カタログ保護の常用

常に適切なレベルのカタログ保護を設定してください。ただし、[記録しない] 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。たとえば、データ保護期間が 1 年で、メディアをリサイクルする場合、1 年を過ぎると IDB はそれほど拡張しなくなります。新しいカタログと OBDB から削除されたカタログの容量はほぼ同じです。カタログ保護を 4 週間に設定した場合、4 週間を過ぎると IDB はそれほど拡張しなくなります。このため、カタログ保護を 1 年に設定した場合の IDB の大きさはこの場合の 13 倍になります。

少なくとも最新のフルバックアップがカタログ保護に含まれるように設定することをお勧めします。たとえば、フルバックアップのカタログ保護を 8 週間に設定して、増分バックアップを 1 週間に設定します。

同一セル内で異なるロギングレベルを使用

1 つのセルが、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) サーバー、少数のファイルにあらゆる情報を保存するデータベースサーバー、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 サーバーには、[ディレクトリレベルまでログに記録] オプションを使用します。
- データベースサーバー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、[記録しない] オプションを使用します。
- ワークステーションまたはファイルサーバーには、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] または [ファイルレベルまでログに記録] 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] または [記録しない] オプションを設定したバックアップでは、メディアから比較的短時間でカタログをインポートでき、選択したオブジェクトをブラウズできます。メディアからのカタログのインポートについては、『HP Data Protector ヘルプ』の索引「インポート、メディアからカタログを」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。

たとえば、バックアップセッションで正常にバックアップされたことを確実にするためにだけオブジェクトミラーを作成するような場合であれば、オブジェクトミラーには [記録しない] 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 [記録しない] 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] 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] 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] 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] 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] 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] 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

IDB のサイズを見積もるには、Internal Database Capacity Planning Tool を使用します。このツールは、英語のドキュメント（ガイド、ヘルプ）コンポーネントの一部としてインストールされます。

6 サービス管理

サービス管理、レポート、および監視機能は、管理者がバックアップ環境を効率よく管理するのに役立ちます。この章では、サービス管理機能の概念について説明するとともに、Data Protector をスタンドアロンな形で使用する場合に得られる利点と、HP サービス管理製品と統合した場合に得られる利点について、それぞれ説明します。

Data Protector とサービス管理

Data Protector はサービス管理機能をサポートしており、HP Operations Manager for Windows システム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 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 API (ARM 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 Performance Agent (PA) を使用します。
- 実行中のセッションを監視する機能が組み込まれているため、バックアップ環境内で発生した出来事にただちに対応できます。
- Data Protector に組み込まれている通知およびレポート用エンジンを使用すると、さまざまな形式 (ASCII、HTML、スプレッドシート互換形式など) で作成された要約レポートや即時警報を受け取って、これをさまざまな方法 (電子メール、SNMP、Windows システム上でのみ可能なブロードキャスト、ファイルへの書き込み、外部コマンドへの送信など) で配布できます。Data Protector の組み込み通知エンジンでは、SNMP を介して警報を送信できるため、SNMP トラップを受け取ることができるアプリケーションであれば、事実上どのアプリケーションとも統合することが可能です。
- Data Protector バックアップセッション監査では、Data Protector のセル全体で長期にわたって実行されたすべてのバックアップタスクに関する情報が保存され、監査および管理のため必要に応じて、統合的かつ印刷可能な形式でこの情報が提供されます。
- Data Protector を HP Operations Manager ソフトウェアと統合して使用すると、OM コンソール上で HP 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 Operations Manager for Windows システム (OMW) と統合すると、 Data Protector の主要かつ重大なイベントを、OMW 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。

ARM 準拠のシステム管理および監視ツールとの統合

ARM とは

Application Response Measurement (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は、HP Performance Agent (PA) などの、ARM に準拠したシ

ステム管理および監視ツールで応答時間の情報 (および、特定のトランザクションに関連するユーザー情報) を提供します 。

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 PA 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。PA 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、Data Protector がすでに存在するシステム上に PA をインストールすると、トランザクションデータがただちに PA および HP Performance Manager (PM) に表示されるようになります。HP-UX の場合は、Data Protector ディレクトリから ARM ディレクトリへのリンクを作成する必要があります。

詳細は、『HP Data Protector ヘルプ』の索引キーワード「ARM 統合ソフトウェア、インストール」を参照してください。

HP Operations Manager ソフトウェアとの統合

HP OM 統合ソフトウェアの機能

Data Protector は、HP Operations Manager ソフトウェア (OM) と統合されます。OM を使用すると、オペレータは、ネットワーク全体やさまざまなアプリケーションを一元的に監視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 OM 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、OM メッセージウィンドウ内に表示できます。

HP Operations Manager for Windows システムの機能

HP Operations Manager for Windows システム (OMW) には、以下の機能があります。

- Data Protector では、バックアップ中、復元中、または他の操作中に発生するすべての主なメッセージと重要なメッセージが、Windows のイベントログに書き込まれます。HP Operations Manager for Windows (OMW) では、オペレータが対処できるよう、これらのイベントが使用され、OMW コンソールに転送されます。
- サービス監視機能

  OMW 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監視できます。いずれかのサービスで問題が発生した場合は、OMW 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、OMW を構成することも可能です。

SNMP トラップ

SNMP トラップの使用により、Data Protector のイベント発生時、または Data Protector のチェックおよび保守の機構の結果として SNMP トラップが送信されたときに、サービス管理アプリケーションが SNMP トラップメッセージを受信および処理できるようになります。Data Protector の SNMP トラップの構成の詳細については、『HP Data Protector ヘルプ』の索引「SNMP、レポートの送信方法」を参照してください。

Data Protector モニター

Data Protector モニターは、Data Protector ユーザーインタ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監視や修正処置の実行に使用します。モニター内にはセル内のすべてのセッションが表示され、これらのセッションに関する詳細メッセージと現在の状態をチェックできます。複数セル環境では、他のセルにあるシステム上で実行中のセッションを監視することも可能です。モニターのユーザーインタフェースからは、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監視できます。

レポートと通知

Data Protector のレポート機能では、バックアップ環境の管理と計画にとって、強力でカスタマイズ可能な柔軟性のあるツールを提供しています。Data Protector には豊富なレポート機能が組み込まれており、システム管理者は従来からこれらの機能に立脚して Cell Manager を管理してきました。これらのレポート機能は、IT サービスプロバイダが、SLA に定義されたデータ保護レベルを達成していることを実証する際にも役立ちます。サービスレベル管理に特に関係が深い組み込みのレポート機能は、以下のとおりです。

- インベントリ/ステータス関連レポート。たとえば、保護されていないシステムに関する情報を示す **Data Protector 向けに構成されていないクライアント**レポート、スケジューリングされているバックアップ、オブジェクトコピー、オブジェクト集約をすべて覧表示する**セッション仕様スケジュール**レポート、メディア インベントリ レポートである**プールのリスト**レポートなど。
- 稼動率関連レポート。たとえば、Data Protector ライセンスの使用状況を示す**ライセンス**レポートや、バックアップ、オブジェクトコピー、またはオブジェクト集約に現在使われていないために使用可能なデバイスの一覧を示す **Data Protector が使用していない構成済みデバイス**レポートなど。
- 問題関連レポート。たとえば、バックアップ、コピー、および集約に失敗したセッションに関連する情報を示す **Session Statistics** レポートなど。管理者は、失敗したジョブとその原因を示す電子メールレポートを、毎時、毎日、または週 1 回のペースで受け取ることができます。

Cell Manager に従来から組み込まれているこれらのレポート機能と通知機能を利用すると、以下のような処理も可能です (これらの機能は従来のバージョンより大幅に機能拡張されています)。

- 事前構成された多数のレポートが用意されており、たとえば、指定した時間帯に実行されたセッションに関するレポート、IDB レポート、デバイス使用状況レポートなどを作成できます。
- これらのレポートはパラメータを指定してカスタマイズすることもできます (対象となる時間帯、バックアップ、コピー、および集約の仕様、バックアップ グループなど)。
- さまざまな出力形式を選択できます (ASCII、HTML、スプレッドシート互換形式など)。
- これらのレポートに対して、Data Protector の組み込みスケジューラを使ったスケジューリングも可能です。
- 何らかのイベントに基づいて、これらのレポート送信を開始することも可能です (デバイス障害、マウント要求、セッションの終了時など)。
- さまざまな配布方法の中から、レポートを受け取る方法を選択できます (電子メール、SNMP、Windows システムでのみ可能なブロードキャスト、ファイルへの書き込み、外部コマンドへの送信など)。

これらの出力形式、配布方法、スケジュール方法、開始方法などの大部分は、自由に組み合わせられます。

以下にいくつかの例を示します。

レポートと通知の例

- 毎朝 7:00 に、24 時間以内に実行されたバックアップ、コピー、および集約の各セッションに関するレポートを作成し、これを ASCII 形式の電子メールの形でバックアップ管理者のメールボックスに送信します。さらに同じレポートを、Web サーバー上に HTML ファイル形式で書き込んで、他のユーザーもこの情報を利用できるようにします。

- デバイス障害やマウント要求が発生した場合は、ブロードキャストメッセージをただちにバックアップ管理者の Windows ワークステーションに送信し、さらに外部コマンドを開始して、バックアップ管理者のポケットベルを呼び出します。
- バックアップセッションの終了時には、バックアップされたシステムを所有しているエンドユーザーに、バックアップ状態を示すレポートを、ASCII 形式の電子メールで送信します。

イベントロギングと通知

Data Protector のイベントログは、Data Protector 関連の通知すべてを管理する中央レポジトリです。Data Protector イベントログに記録されるイベントは、プロセスまたはユーザのどちらかによってトリガされたイベントです。Data Protector の組み込み通知エンジンは、ログエントリに基づいて、警報の送信や Data Protector レポート機構の開始などを実行します。イベントログは、Data Protector や HP ソフトウェア管理アプリケーションで SLA への適合を示すレポートを生成するための情報ソースとなります。さらにレポート機能に加えて、ログエントリから HP ソフトウェア管理アプリケーションに Data Protector SPI(SMART プラグイン) 経由で情報を提供することにより、予防処置や修正処置を実施することも可能です。

Data Protector の組み込み通知エンジンは、SNMP を介して警報を送信できるため、SNMP トラップを受け取ることができるアプリケーションであれば、事実上どのアプリケーションとも統合することが可能です。HP Operations Manager との統合は、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 [レポートと通知] のユーザー権限を持つ Data Protector ユーザーに限られています。Data Protector イベントログ内のすべてのイベントは、イベントログビューアを使用して表示または削除できます。

Data Protector ログファイル

サービス管理アプリケーションの中には、HP Operations Manager ソフトウェアのように、特定のログエントリに関して、モニターするログファイルと時間を指定できるものがあります。特定のエントリがファイル内で検出された場合、動作を指定できます。OM 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 Data Protector トラブルシューティングガイド』と『HP Data Protector ヘルプ』を参照してください。

Windows アプリケーションログ

サービス管理アプリケーションの中には、HP Operations Manager for Windows システム (OMW) のように、Windows 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。

Data Protector メッセージと Data Protector サービスに関連するメッセージ (停止している場合) をすべて Windows アプリケーションログに自動転送する方法は、『HP Data Protector トラブルシューティングガイド』を参照してください。

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 サーバー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。この機能の使用には、サポートされている Web ブラウザのみが必要です。Data Protector GUI をシステムにインストールする必要はありません。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 のセルフチェックや保守の処理には次のものがあります。

- 「空きメディア不足」のチェック
- 「Data Protector ライセンス期限」のチェック

詳細は、『HP Data Protector ヘルプ』の索引「Data Protector が実行するチェック」を参照してください。

中央管理、分散環境

Data Protector の MoM 機能を使用すると、管理者は複数の Data Protector Cell Manager から構成される企業環境を一元管理することができます。MoM システム管理者は、単一のコンソールから、企業全体にわたる構成、メディア管理、監視、ステータスレポートの作成などの作業を実施できます。MoM を使用すると、多数の Data Protector Cell Manager を、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 Data Protector ヘルプ』の索引「MoM 環境」を参照してください。

Data Protector が提供するデータの使用

データの用途

Data Protector が提供するデータは、以下に示すような形で使用できます。

- バックアップオペレータ、エンドユーザー、管理者などに、電子メール形式でレポートを定期的に送信できます (Data Protector 組み込みレポート機能の電子メール送信機能を使用)。
- バックアップレポートが Web サーバーに書き込まれ、各ユーザーが必要に応じて使用できるようになります (Data Protector 組み込みレポート機能の HTML レポート作成機能を使用)。
- Data Protector の主要かつ重大なイベントを、HP 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)。

7 Data Protector が機能する仕組み

この章では、Data Protector が機能する仕組みについて説明します。ここでは、Data Protector のプロセス (UNIX の場合) とサービス (Windows の場合)、バックアップセッションと復元セッション、およびメディア管理セッションについて、順に説明していきます。

Data Protector のプロセス (サービス)

Data Protector では複数のプロセス (UNIX の場合) とサービス (Windows の場合) がバックグラウンドで実行されており、これらのプロセス (サービス) により、バックアップセッションおよび復元セッションの実行が可能になります。また、必要な通信パスの確立、バックアップセッションおよび復元セッションの起動、Disk Agent および Media Agent の起動、バックアップされたデータに関する情報の保存、メディア管理などの各種機能が実行されます。

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 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。
KMS	KMS(Key Management Server) プロセス (サービス) は、Cell Manager 上で動作し、Data Protector の暗号化機能のためのキー管理を提供します。このプロセスは、Data Protector を Cell Manager にインストールしたときに開始されます。
MMD	MMD (Media Management Daemon) プロセス (サービス) は、Data Protector Cell Manager 上で実行され、メディア管理およびデバイス操作を担当しています。このプロセスは、Cell Request Server プロセス (サービス) により開始されます。
RDS	RDS (Raima Database Server) プロセス (サービス) は、Data Protector 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 にインストールしたときに開始されます。
UIProxy	Java GUI サーバー (`UIProxy` サービス) は Data Protector Cell Manager で実行されます。Java GUI サーバーでは、Java GUI クライアントと Cell Manager との間の通信を行います。また、ビジネスロジック操作を実行し、重要な情報のみをクライアントに送信する必要があります。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。

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 Data Protector ヘルプ』を参照してください。

バックアップセッション

この項では、バックアップセッションの開始方法、バックアップセッション中の処理内容、および関連するプロセスとサービスについて説明します。

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用し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。なお、複数のユーザーが同じバックアップセッションをモニターできます。ユーザーインタフェースをセッションから切断して、モニターを停止することもできます。セッションは、その後、バックグラウンドで継続されます。

バックアップセッションにおけるデータフローとプロセス

バックアップセッション中の処理内容

バックアップセッションにおける情報の流れは、「バックアップセッションにおける情報の流れ (1)」 (155 ページ) に示すような形になります。これは標準的なネットワークバックアップを実行する場合のデータフローやプロセスです。その他のバックアップ方法 (スプリットミラーバックアップなど) におけるデータフローやプロセスについては、関連する章を参照してください。

バックアップセッションが開始されると、以下の処理が実行されます。

1. BSM(バックアップセッションマネージャー) プロセスが、Cell Manager システム上で開始されて、バックアップセッションを制御します。このプロセスにより、バックアップ仕様内に指定されているバックアップ対象、オプション、バックアップ用メディアとデバイスなどの情報が読み取られます。
2. BSM により、IDB がオープンされて、生成されるメッセージのほか、バックアップデータに関する詳細や、使用するデバイスやメディアに関する情報など、バックアップセッションに関する情報がデータベース内に書き込まれます。
3. BSM により、バックアップ用デバイスが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。

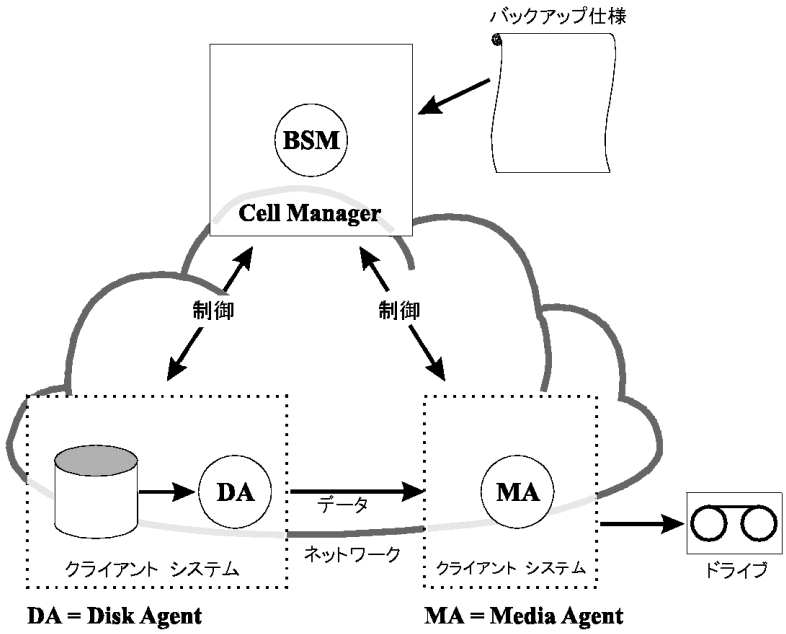
   オブジェクトミラーの作成を伴うバックアップセッションの場合は、BSM により、ミラー作成用の Media Agent も開始されます。
4. BSM により、並行してバックアップされるディスクごとに、個々の Disk Agent(DA) が起動されます。実際に起動される Disk Agent の数は、バックアップ仕様に構成された Disk Agent の同時実行数に基づいて決められます。これは、デバイスストリーミングを維持するために、同時に開始できる Disk Agent の数を示すものであり、これらの Disk Agent から 1 つの Media Agent にデータが並行して送られます。
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 67 バックアップセッションにおける情報の流れ (1)

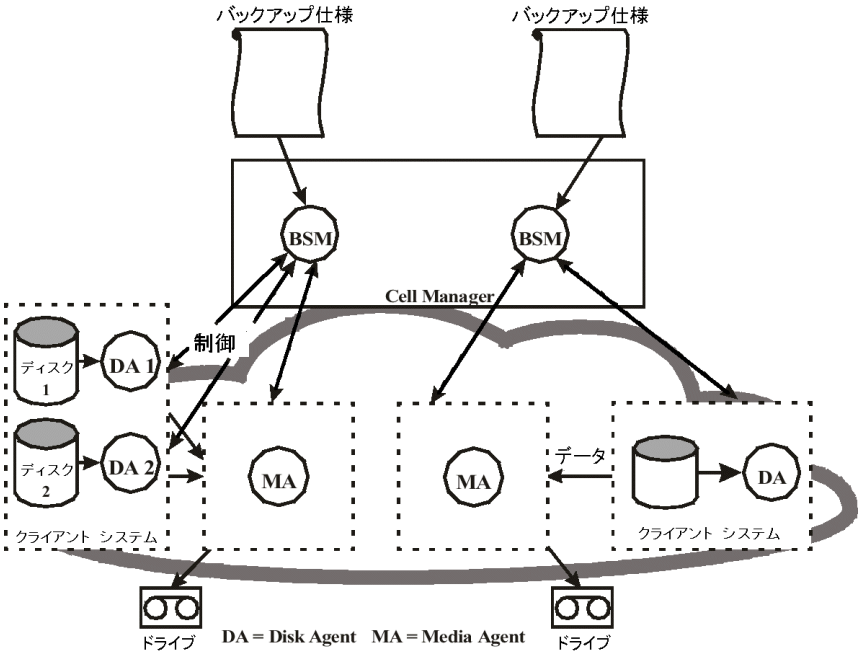


同時に実行できるセッションの数

セル内では同時に複数のバックアップセッションを実行できます。同時に実行できるセッションの数は、デバイスの可用性や Cell Manager の構成 (たとえば、プロセッサの速度、メインメモリーの容量など)、セル内のリソースによって制限されます。Data Protector のプロセスがシステムの能力を超えないよう、同時実行できるバックアップセッションの最大数は制限されます。この最大数は変更可能です。

「バックアップセッションにおける情報の流れ－複数のセッション」(156 ページ)は、同時実行されている複数のセッションを示しています。

図 68 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。いずれかのリソースが使用できるようになるまで、セッションは待ち行列に入れられます。タイムアウトになってもリソースがまだ使用できない場合は、そのセッションは中止されます。

負荷の最適化

Cell Manager の負荷を最適化するために、Data Protector は、デフォルトでは、最大 5 つのバックアップセッションを同時に開始できるようになっています。このデフォルトの値は、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ポリシーにより特定のメディアが要求されたが、そのメディアがデバイス内にない場合。
- バックアップに使用するメディアの順番が事前割り当てリスト内に指定されているが、この順番でメディアを使用できない場合。

詳細については、「バックアップセッション中にデータをメディアに追加」(128 ページ) および「バックアップ用メディアの選択」(128 ページ) 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、「レポートと通知」(150 ページ) 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く必要があります。この場合、指定されたオブジェクトのみがバックアップ対象となります。そのため、システムに新しいディスクを追加したり、別のオブジェクトをバックアップしたりする場合には、バックアップ仕様を手動で変更して、これらの新しいオブジェクトを追加する必要があります。ディスクディスカバリバックアップと標準的なバックアップのどちらを使用するかは、バックアップの構成時に選択できます。

復元セッション

この項では、復元セッションの開始方法、復元セッションの処理内容、および関連するプロセスとサービスについて説明します。

復元セッションとは

復元セッションでは、バックアップコピー(通常はテープメディア)からディスクへデータが戻されます。

復元セッションは対話形式で起動されます。Data Protector で何を復元するかを指定すると、Data Protector によって必要なメディアが判断され、いくつかのオプションが選択されて、復元が開始されます。ユーザーはセッションの進行状況をモニターできます。

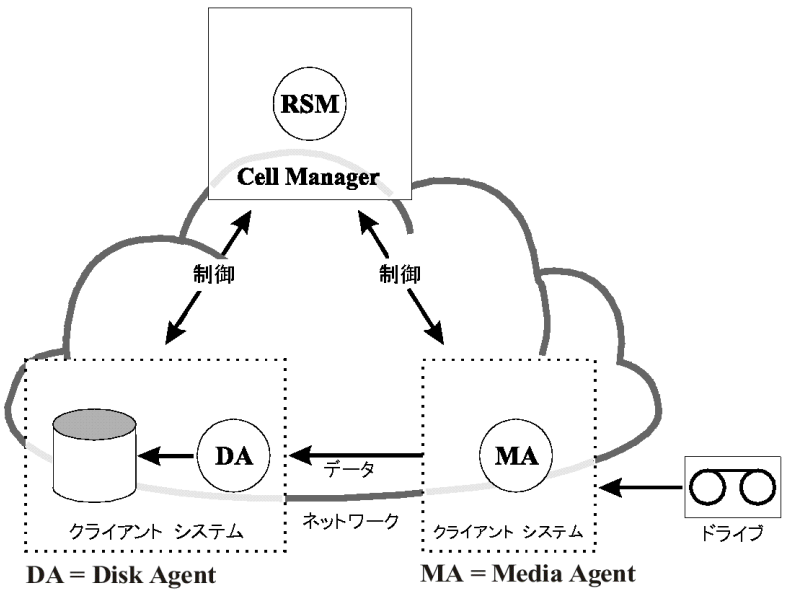
復元セッションにおけるデータフローとプロセス

復元セッション中の処理内容

「復元セッションの情報フロー」(158 ページ)のように復元セッションが開始されると、以下の処理が実行されます。

1. 復元セッションマネージャー (RSM) プロセスは、Cell Manager システム上で開始されます。このプロセスによって、復元セッションが制御されます。
2. RSM によって IDB がオープンされ、復元に必要なメディアの情報が読み取られ、復元セッションの情報 (生成されるメッセージなど) が IDB に書き込まれます。
3. RSM により、復元に使用するデバイスがあるシステム上で、Media Agent (MA) が起動されます。並行して使用される各ドライブで、新たに Media Agent が起動されます。
4. 並行して復元される各ディスクに対して、RSM により Disk Agent (DA) が起動されます。起動される Disk Agent の実際の数は、復元を選択したオブジェクトに依存します。詳細は、「並行復元」(159 ページ) を参照してください。
5. Media Agent によりメディアからデータが読み取られ、ディスクにデータが書き込まれる Disk Agent に対して、そのデータが送信されます。RSM により、セッションの進行状況がモニターされ、必要に応じて新規の Disk Agent や Media Agent が起動されます。
6. 復元セッションが完了すると、RSM によりセッションがクローズされます。

図 69 復元セッションの情報フロー



同時に実行できる復元セッションの数

セル内では、多数の復元セッションを同時に実行できます。実行可能な数は、Cell Manager とデバイスを接続したシステム数などの、セル内のリソースによって制限されます。

復元セッションにおける待ち行列

タイムアウト

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

復元セッションにおけるマウント要求

マウント要求とは

マウント要求は、復元セッションで復元に必要なメディアがデバイス内で使用可能でない場合に出されます。Data Protector では、マウント要求が発生したときに実行する処理を構成することができます。

マウント要求への対応

マウント要求に対応するには、要求されたメディアまたはメディアのコピーをセットし、Data Protector に復元処理を実行するよう指示します。

並行復元

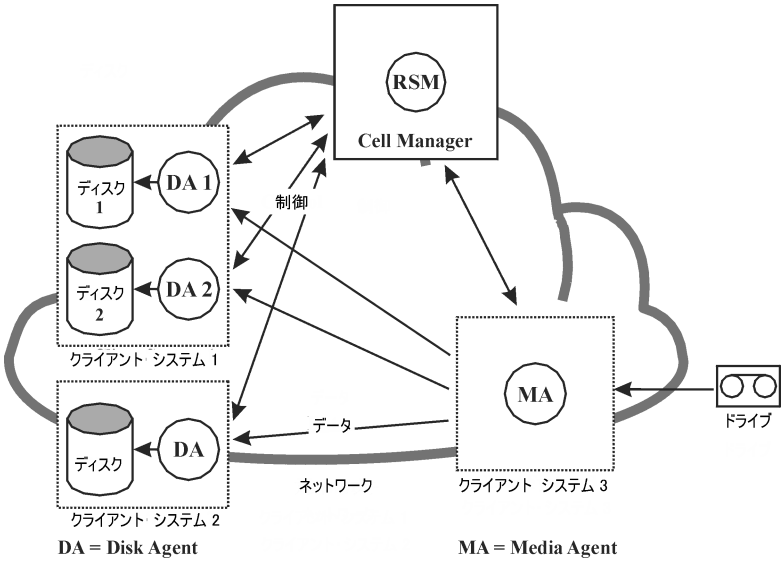
並行復元とは

並行復元では、複数オブジェクトのインタリーブデータがメディアから単一パスで同時に読み取られ、復元されます。並行復元により、同一メディアから複数オブジェクトを復元する際のパフォーマンスが大幅に改善されます。詳細は、「並行復元セッションのフロー」(160 ページ) を参照してください。

標準的な復元との比較

複数の Disk Agent からのデータは (ほとんどの場合)、多重化されメディア上に保存されます。「1 つのメディア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)」(129 ページ) を参照してください。標準的な復元の場合、Data Protector によってメディアから多重化されたデータが読み取られ、選択されたオブジェクトで必要な部分だけがアセンブルされます。次のオブジェクトが復元される際には、両オブジェクトが同じメディア上にあり、多重化を使用して書き込まれると想定して、Data Protector でメディアを巻き戻し、次のオブジェクトの部分を読み取る必要があります。

図 70 並行復元セッションのフロー



並行復元では、Data Protector によって、選択されたすべてのオブジェクトの多重化データが読み取られ、直ちに全オブジェクトに必要な部分がアセンブルされて、正しい Disk Agent に正しいデータが送信されます。これにより、メディアからの読み取りパフォーマンスが向上します。選択されたオブジェクトが異なる物理ディスクに書き込まれる場合には、パフォーマンスがさらに向上します。この場合、データは同時に複数のディスクにコピーされます。

高速な複数の単一ファイル復元

Data Protector では、復元パフォーマンスを向上させるために不連続のオブジェクト復元が使用されます。あるファイルかツリーが復元された後、少なくとも 1 セグメントがファイル間またはツリー間にある場合、Data Protector の位置は、メディア上の次のファイルまたは次のツリーに、直接、移動されます。

個々の復元オブジェクト内では、複数の Disk Agent を起動することができます。この方法により、メディア中のさまざまな場所に存在する複数の単一ファイルの復元処理は、Data Protector がメディア内をトラバースするよりはるかに高速になります。

復元セッションの再開

ネットワークの問題などによって正常に完了しなかった復元セッションは、Data Protector 再開セッション機能を使用して再開できます。失敗したセッションを再開すると、Data Protector は、失敗したセッションが中止したところから新規セッションで復元を続行します。

オブジェクトコピーセッション

ここでは、オブジェクトコピーセッションの開始方法、セッション中の処理内容、および関連するプロセスとサービスについて説明します。

オブジェクトコピーセッションとは

オブジェクトコピーセッションとは、バックアップ、コピー、または集約されたデータの追加コピーを別のメディアセット上に作成するプロセスです。オブジェクトコピーセッション中に、選択されたバックアップ、コピー、または集約オブジェクトがソースからターゲットメディアへコピーされます。

自動および対話形式のオブジェクトコピーセッション

自動オブジェクトコピーセッション

自動オブジェクトコピーセッションは、スケジュールを設定して開始することも、バックアップ、オブジェクトコピー、またはオブジェクト集約の直後に開始することも可能です。スケジュール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、ポストバックアップ、ポストコピー、またはポスト集約オブジェクトコピーセッションは、指定したセッションの終了後に開始されます。自動オブジェクトコピーセッションの進行状況は、Data Protector モニターで確認できます。

対話形式のオブジェクトコピーセッション

対話形式のオブジェクトコピーセッションは、Data Protector ユーザーインタフェースを使用してオペレータが直接開始します。Data Protector モニターがすぐに起動され、セッションの進行状況を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。ユーザーインタフェースをセッションから切断して、モニターを停止することもできます。セッションは、その後、バックグラウンドで継続されます。

オブジェクトコピーセッションにおけるデータフローとプロセス

オブジェクトコピーセッション中の処理内容

オブジェクトコピーセッションにおける情報の流れは、「オブジェクトコピーセッションにおける情報の流れ」(164 ページ)に示すような形になります。オブジェクトコピーセッションが開始されると、以下の処理が実行されます。

1. CSM(コピーおよび集約セッションマネージャー) プロセスが、Cell Manager システム上で開始されます。このプロセスは、オブジェクトコピー仕様に指定されたコピー対象、オプション、使用するメディアとデバイスなどの情報を読み取ります。またこのプロセスは、オブジェクトコピーセッション全体を制御します。
2. CSM が IDB をオープンし、コピーに必要なメディアの情報を読み取り、オブジェクトコピーセッションの情報 (生成されるメッセージなど) を IDB に書き込みます。
3. CSM により、デバイスがロックされます。セッションは、すべての読み取り Media Agent と必要な最小限の書き込み Media Agent がロックされるまで、バックアップと同じタイムアウトの時間を使用して待ち行列に入れられます。タイムアウトになってもリソースがまだ使用できない場合は、そのセッションは中止されます。
4. CSM により、コピー用デバイスが構成されているシステム上で Media Agent が開始されます。Media Agent は、バックアップ方針に従って割り当てられたソースメディアとターゲットメディアをロードします。
5. Media Agent がコピー元メディアからデータを読み取り、コピー先メディアを担当する Media Agent に接続します。

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

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

   コピー元デバイスのブロックサイズがコピー先デバイスのブロックサイズよりも小さい場合は、オブジェクトコピーセッションのこの段階でブロックの再パッケージ化が行われます。

7. 正常にコピーされたすべてのオブジェクトに対して、CSM は、コピーセッションに指定されたオプションに従って IDB 保護エントリを更新します。

   セッションにリサイクルオプションが指定されている場合、リサイクルを可能にするために失敗したソースオブジェクトの保護も更新されます。

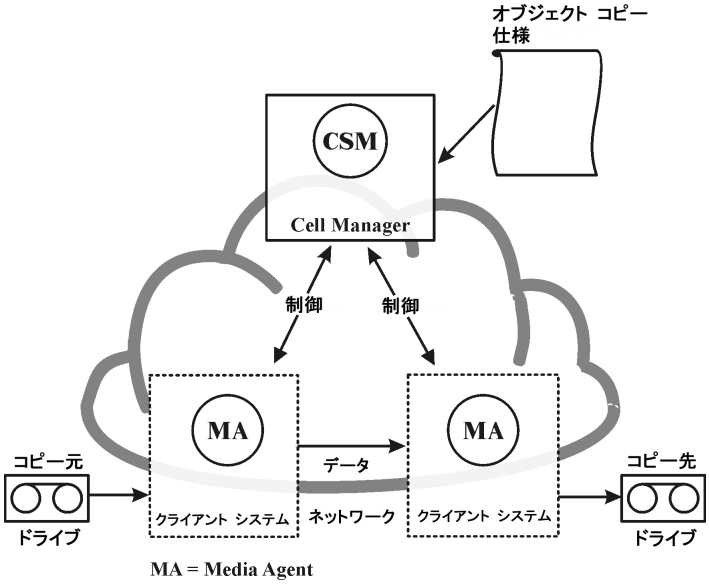
8. オブジェクトコピーセッションが終了したら、CSM によりセッションが閉じられます。

同時に実行できるセッションの数

セル内では同時に複数のオブジェクトコピーセッションを実行できます。同時に実行できるセッションの数は、Cell Manager や、デバイスを接続しているシステムなど、セル内のリソースによって制限されます。

ただし、同じオブジェクトコピー仕様から 2 つ以上のオブジェクトコピー セッションを並行して実行することはできません。

図 71 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。いずれかのリソースが使用できるようになるまで、セッションは待ち行列に入れられます。タイムアウトになってもリソースがまだ使用できない場合は、そのセッションは中止されます。

オブジェクトコピーセッションにおけるマウント要求

マウント要求とは

オブジェクトコピーセッションのマウント要求は、オブジェクトコピー処理に必要なソースまたはターゲットのメディアが使用可能でない場合に行われます。

マウント要求への対応

マウント要求に対しては、必要なメディアをセットして、マウント要求を確認し、応答します。要求されたソースメディアにコピーメディアがある場合は、オリジナルメディアの代わりにコピーをセットすることも可能です。

複製セッション

この項では、複製セッションの開始方法、複製セッションの処理内容、および関連するプロセスとサービスについて説明します。

複製セッションとは

複製セッションとは、複製に対応したディスクへのバックアップ (B2D) デバイス上に、バックアップデータ、コピーデータ、集約データの追加コピーを作成するプロセスです。複製セッションでは、バックアップオブジェクト、コピーオブジェクト、集約オブジェクトをソースデバイスで選択するとターゲットデバイスに直接複製され、Media Agent クライアントを経由した転送は行われません。さらに、データは重複排除後にネットワーク転送されるので、ネットワーク負荷も軽減されます。

自動の複製セッションと対話型の複製セッション

自動複製セッション

自動複製セッションは、スケジュールを設定して開始することも、バックアップ、オブジェクトコピー、またはオブジェクト集約の直後に開始することも可能です。スケジュールした複製セッションは、Data Protector スケジューラを使って、指定した時刻に開始されます。一方、ポストバックアップ、ポストコピー、またはポスト集約の複製セッションは、指定したセッションの終了後に開始されます。自動複製セッションの進捗は、Data Protector モニターで確認できます。

対話型の複製セッション

対話式複製セッションは、Data Protector ユーザーインタフェースから直接開始します。Data Protector モニターがすぐに起動され、セッションの進行状況をモニタリングできます。1 つの複製セッションを複数のユーザーがモニターできます。ユーザーインタフェースをセッションから切断して、モニターを停止することもできます。セッションは、その後、バックグラウンドで継続されます。

複製セッションにおけるデータフローとプロセス

複製セッション中の処理内容

複製セッションにおける情報の流れは、「オブジェクトコピーセッションにおける情報の流れ」(164 ページ)に示すような形になります。複製セッションが開始されると、以下の処理が実行されます。

1. CSM(コピーおよび集約セッションマネージャー) プロセスが、Cell Manager システム上で開始されます。このプロセスは、コピー仕様 (および有効な複製オプション) を読み取り、複製の対象、使用するオプション、使用するデバイスを特定します。またこのプロセスは、複製セッションの制御も行います。
2. CSM が IDB を開き、複製に必要なデバイスの情報を読み取り、複製セッションの情報 (生成されるメッセージなど) を IDB に書き込みます。
3. CSM により、デバイスがロックされます。タイムアウトになってもリソースがまだ使用できない場合は、そのセッションは中止されます。
4. CSM は、複製対象として構成されているデバイス間で複製プロセスを開始します。
5. CSM は、正常に複製されたすべてのオブジェクトについて、複製セッションで指定されたオプションに従って IDB 保護エントリを更新します。

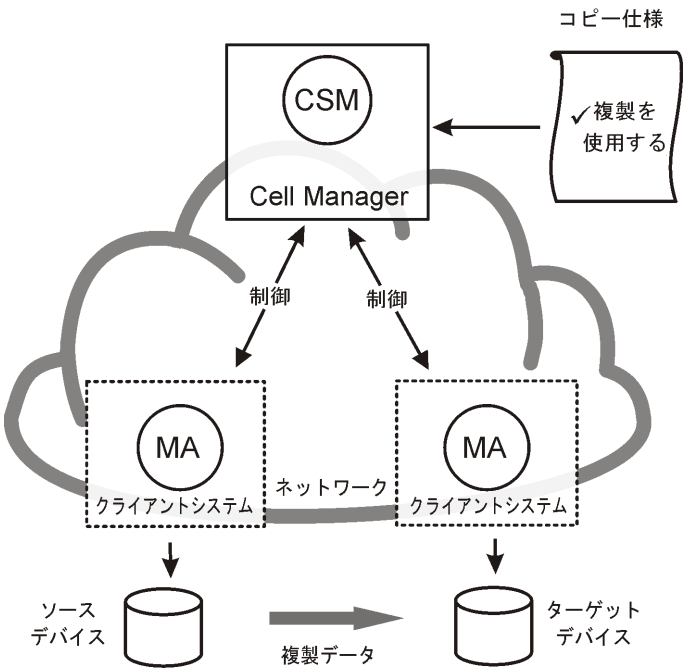
   セッションにリサイクルオプションが指定されている場合、リサイクルを可能にするために失敗したソースオブジェクトの保護も更新されます。
6. 複製セッションが終了したら、CSM によってセッションが閉じられます。

同時に実行できるセッションの数

セル内では、多数の複製セッションを同時に実行できます。同時に実行できるセッションの数は、Cell Manager や、デバイスを接続しているシステムなど、セル内のリソースによって制限されます。

ただし、同じ複製仕様から 2 つ以上の複製セッションを並行して実行することはできません。また、対話型の複製セッションを 2 つ以上並行して実行することもできません。

図 72 複製セッションの情報フロー



複製セッションにおける待ち行列

タイムアウト

複製セッションが開始されると、Data Protector は、必要な全リソースの割り当てを試みます。いずれかのリソースが使用できるようになるまで、セッションは待ち行列に入れられます。タイムアウトになってもリソースがまだ使用できない場合は、そのセッションは中止されます。

オブジェクト集約セッション

この項では、オブジェクト集約セッションの開始方法、セッション中の処理内容、および関連するプロセスとサービスについて説明します。

オブジェクト集約セッションとは

オブジェクト集約セッションとは、フルバックアップと少なくとも 1 つの増分バックアップで構成されるバックアップオブジェクトの復元チェーンを、そのオブジェクトのために新規に集約されるバージョンにマージするプロセスです。オブジェクト集約セッションでは、Data Protector によってソースメディアのバックアップデータが読み取られ、データがマージされ、集約されたバージョンがターゲットメディアへ書き込まれます。

詳細は、「合成バックアップ」 (63 ページ) を参照してください。

自動および対話形式のオブジェクト集約セッション

自動オブジェクト集約セッション

自動オブジェクト集約セッションは、スケジュールするか、または、バックアップ直後に開始させることができます。スケジュールしたオブジェクト集約セッションは、Data Protector スケジューラで指定された時間に起動されます。ポストバックアップオブジェクト集約セッションは、指定されたバックアップセッションの終了後に起動されます。自動オブジェクト集約セッションの進行状況は、Data Protector モニターで参照できます。

対話形式のオブジェクト集約セッション

対話形式のオブジェクト集約セッションは、Data Protector ユーザーインタフェースから直接起動されます。Data Protector モニターがすぐに起動され、セッションの進行状況をモニタリングできます。複数のユーザーが、同じオブジェクト集約セッションをモニターできます。ユーザーインタフェースをセッションから切断して、モニターを停止することもできます。セッションは、その後、バックグラウンドで継続されます。

オブジェクト集約セッションにおけるデータフローとプロセス

オブジェクト集約セッションが開始されると、以下の処理が実行されます。

1. CSM(コピーおよび集約セッションマネージャー) プロセスが、Cell Manager システム上で開始されます。このプロセスにより、集約するオブジェクトや使用するオプション、メディア、およびデバイスに関するオブジェクト集約仕様が読み取られます。これにより、オブジェクト集約セッションが制御されます。
2. CSM により IDB がオープンされて、復元に必要なメディアに関する情報が読み取られるほか、オブジェクト集約セッションに関する情報 (生成されるメッセージなど) が IDB に書き込まれます。
3. CSM により、デバイスがロックされます。セッションは、すべての読み取り Media Agent と必要な最小限の書き込み Media Agent がロックされるまで、バックアップと同じタイムアウトの時間を使用して待ち行列に入れられます。タイムアウトになってもリソースがまだ使用できない場合は、そのセッションは中止されます。
4. CSM により、セッションで使用されるデバイスがあるシステム上の Media Agent が起動されます。Media Agent は、バックアップ方針に従って割り当てられたソースメディアとターゲットメディアをロードします。

   あて先デバイスがオブジェクトに対して指定されていない場合は、ユーザーが以下に記載順の優先順位に従ってオブジェクト集約仕様で選択した中から、Data Protector によって自動的に選択されます。

   - ソースデバイスと同じブロックサイズを持つあて先デバイスが、異なるブロックサイズのものより先に選択される
   - ネットワーク接続デバイスより、ローカル接続デバイスが先に選択される
5. 1 つの Media Agent が、フルオブジェクトバージョンを読み込みます。この Media Agent は、増分オブジェクトバージョンを読み込む別の Media Agent にデータを送信します。この 2 つ目の Media Agent が実際の統合を行い、ターゲットメディアにデータを書き込む Media Agent にデータを送信します。

   フルバックアップと増分バックアップが同じファイルライブラリにある場合、同じ Media Agent がすべてのバックアップを読み込んでこれらを統合します。

   ソースデバイスのブロックサイズが、あて先デバイスのブロックサイズよりも小さい場合は、ブロックが再パッケージされます。
6. オブジェクト集約セッションが終了したら、CSM によりセッションが閉じられます。

同時に実行できるセッションの数

セル内では同時に複数のオブジェクト集約セッションを実行できます。オブジェクト集約セッションは、バックアップセッションと同じように扱われ、最大数も同じ要因で制限されます。

オブジェクト集約セッションにおける待ち行列

タイムアウト

オブジェクト集約セッションが開始されると、Data Protector により、必要なすべてのリソースの割り当てが試行されます。いずれかのリソースが使用できるようになるまで、セッションは待ち行列に入れられます。タイムアウトになってもリソースがまだ使用できない場合は、そのセッションは中止されます。

オブジェクト集約セッションにおけるマウント要求

マウント要求とは

オブジェクト集約セッションのマウント要求は、オブジェクト集約処理に必要なソースまたはターゲットのメディアが使用可能でない場合に行われます。

マウント要求への対応

マウント要求に対しては、必要なメディアをセットして、マウント要求を確認し、応答します。要求されたソースメディアにコピーメディアがある場合は、オリジナルメディアの代わりにコピーをセットすることも可能です。

オブジェクト検証セッション

この項では、オブジェクト検証セッションの開始方法、セッション中の処理内容、および関連するプロセスとサービスについて説明します。

オブジェクト検証セッションとは

オブジェクト検証セッションは、指定したオブジェクトに割り当てられたメディアセグメントを検証するプロセスで、ヘッダーセグメント内の情報を確認し、フォーマットを検証するためにデータセグメント内のデータブロックを読み取ります。オリジナルのバックアップ中に巡回冗長検査 (CRC) が実行された場合、CRC の再計算およびオリジナルとの比較も行われます。

Data Protector は、バックアップのソースであったホスト上でオブジェクトの検証を実行し、復元パス内の Data Protector コンポーネントの効率的な検証、別のホスト上にある別の保存場所への復元能力の検証、または関係する Media Agent のあるホスト上で直接、データのみの検証を行うことができます。

自動および対話型オブジェクト検証セッション

自動オブジェクト検証セッション

自動オブジェクト検証セッションは、Data Protector スケジューラを使用して指定した時間に実行するか、あるいは指定したバックアップ、オブジェクトコピー、またはオブジェクト集約セッションの完了直後にバックアップ後のオブジェクト検証セッションとして実行するよう指定できます。Data Protector モニターでこのようなセッションの進行状況をモニタリングできます。

対話型オブジェクト検証セッション

対話型オブジェクト検証セッションは、Data Protector のユーザーインタフェースから直接開始できます。Data Protector モニターがすぐに起動され、セッションの進行状況をモニタリングできます。複数のユーザーが同一のオブジェクト検証セッションをモニタリングすることも可能です。ユーザーインタフェースを使って他の操作を実行し、必要に応じてセッションをバックグラウンドで続行させることができます。

オブジェクト検証セッションにおけるデータフローとプロセス

オブジェクト検証セッション中の処理内容

オブジェクト検証セッションを開始する場合、基本のプロセスフローは以下のようになります。

1. Restore Session Manager (RSM) プロセスは、Cell Manager システム上で開始され、以下のいずれかによってトリガされます。
   - スケジュール設定されたセッションの場合、Data Protector のスケジューラ
   - バックアップ後のセッションの場合、End of Session イベント
   - 対話形式のセッションの場合、GUI または CLI からのユーザー

   このプロセスにより、検証セッションが制御されます。
2. RSM により IDB がオープンされて、検証するオブジェクトに関する情報が読み取られるほか、検証セッションに関する情報 (生成されるメッセージなど) が IDB に書き込まれます。
3. RSM により、オブジェクトの検証に関係するソースシステム上で Media Agent (MA) が起動されます。並行して使用される各ドライブで、新たに Media Agent が起動されます。
4. あて先ホスト上の Disk Agents (DA) によりデータ検証が実行され、これにより並行して使用される各あて先ディスクに対して RSM により Disk Agent が起動されます。起動される Disk Agent の実際の数は、検証を選択したオブジェクトに依存します。このプロセスは、復元の場合と同様です。詳細は、228 ページの「並行復元」を参照してください。
5. Media Agent はメディアからオブジェクトデータを読み取り、オブジェクトの検証を実行する Disk Agent に送信します。RSM により、セッションの進行状況がモニターされ、必要に応じて新規の Disk Agent や Media Agent が起動されます。
6. オブジェクト検証セッションが完了すると、RSM によりセッションがクローズされます。

オブジェクト検証を使用するプロセスフローのバリエーション

オブジェクト検証プロセスでは、復元のためにデータが要求されたポイントから、データがあて先ホストに到達したポイントまでの復元処理がエミュレートされます。そのポイントを超えると、検証プロセスによるデータの書き込みは行われず、アプリケーション統合オブジェクトの場合、アプリケーション統合とのやり取りは行われません。

メディア管理セッション

メディア管理セッションとは

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 内に保存されます。

Data Protector モニターとメディア管理セッション

メディア管理セッションは、モニターウィンドウを使ってモニタリングできます。Data Protector GUI を閉じると、セッションはバックグラウンドで実行されます。

メディア管理セッションにおけるデータフロー

メディア管理セッション中の処理内容

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. メディアセッションマネージャー (MSM) プロセスは、Cell Manager システム上で開始されます。このプロセスにより、メディアセッションが制御されます。

2. MSM により、メディア管理セッションで使用するデバイスが接続されているシステム上で、Media Agent(MA) が開始されます。
3. 要求した処理が Media Agent により実行され、生成されたメッセージが、進捗状況のモニタリングに使用する Data Protector ユーザーインタフェースに送られます。このとき、セッションも IDB 内に保存されます。
4. セッションが終了したら、MSM によりセッションが閉じられます。

実行できるセッションの数

セル内では同時に複数のメディア管理セッションを実行できます。ただし、これらのセッションが同一のリソース (デバイスやメディアなど) を使用しない場合に限ります。

8 アプリケーションとの統合

この章では、Data Protector とデータベースアプリケーションとの統合について簡単に説明します。

データベースアプリケーションとの統合

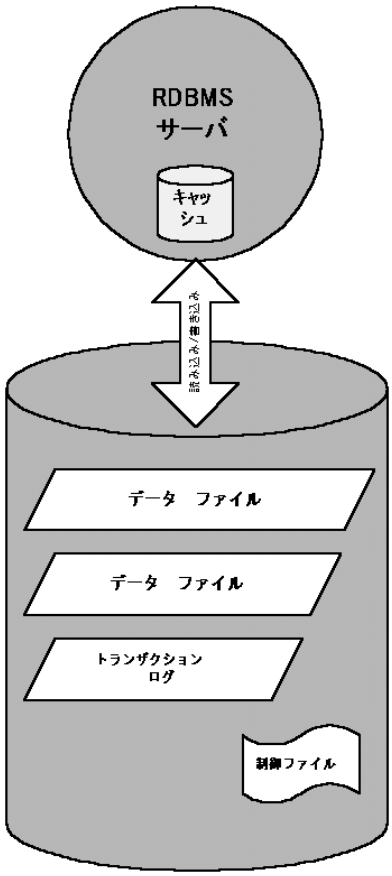
この項では、Data Protector とデータベースアプリケーションとの統合について簡単に説明します。サポートされるアプリケーションの詳細なリストは、最新のサポート一覧 (http://support.openview.hp.com/selfsolve/manuals) を参照してください。

データベース操作の概要

ユーザーから見ると、**データベース**は、情報を 1 つに集めたものです。データベース内のデータは、**テーブル**内に保存されています。リレーショナルテーブルは複数の列で構成され、各テーブルにはそれぞれ名前がつけられています。データはテーブル内の各行に保存されます。テーブルは相互に関連付けることができ、データベースという形で実際の関連付けが行われます。データはこのように**リレーショナル形式**で保存することも、抽象データ型やメソッドのような**オブジェクト指向**の構造として保存することもできます。また、オブジェクトを他のオブジェクトと関連付けたり、オブジェクト内に他のオブジェクトを包含することも可能です。データベースは通常サーバー (マネージャー) プロセスにより管理されて、データの整合性と一貫性が保たれます。

リレーショナル形式の構造またはオブジェクト指向の構造のいずれを使用する場合も、データベース内のデータは**ファイル**に保存されます。内部的には、これらのデータベース構造によりデータからファイルへの論理マッピングが提供され、データ型の異なるデータは個別に保存できます。これらの論理領域は、Oracle では**表領域**、Informix Server では **dbspace**、Sybase では**セグメント**など、さまざまな名前で呼ばれています。

図 73 リレーショナルデータベース



「リレーショナルデータベース」(169 ページ)は、典型的なリレーショナルデータベースと、その内部にある以下の構造を示したものです。

データファイルは、データベース内のすべてのデータが保存される物理ファイルです。データファイルはランダムに変更され、非常に大容量になる可能性があります。物理ファイルの内部は、複数のページに分割されています。

トランザクションログには、すべてのデータベーストランザクションが処理を続行する前に、最初にそれらのトランザクションが保存されます。なんらかの障害により変更データをデータファイルに永久に書き込めなくなった場合も、このログファイルから変更情報を取得できます。復旧処理を行う場合は、必ず次の 2 つの作業が必要になります。1 つ目はトランザクションをメインデータベースに適用する作業で、**ロールフォワード**と呼ばれます。2 つ目はコミットされていないトランザクションを削除する作業で、**ロールバック**と呼ばれます。

制御ファイル には、データベースの物理構造、たとえば、データベースの名前、データベースに所属するデータファイルやログファイルの名前と場所、データベース作成時のタイムスタンプなどが保存されています。この制御データは、制御ファイルに保存されます。これらのファイルは、データベースの操作に非常に重要です。

データベースサーバープロセスの**キャッシュ**内には、データファイルの中の使用頻度の高いページが保存されます。

以下に、標準的なトランザクション処理手順を示します。

1. 最初に、トランザクションがトランザクションログに記録されます。
2. 次に、トランザクションにより要求された変更内容が、キャッシュ内のページに適用されます。
3. 変更されたページは、ディスク上のデータファイルに随時一括して書き込まれます。

データベースおよびアプリケーションのファイルシステムバックアップ

オンライン状態のデータベースは絶えず変更されています。またデータベースサーバーは、接続ユーザーへの迅速な応答や性能の向上を図るために、複数のコンポーネントで構成されています。たとえばデータの中には、内部キャッシュメモリーや一時的なログファイルに保存されているものもあります。これらのデータは、**チェックポイント**でディスクに一括して書き込まれます。

データベース内のデータはバックアップ中にも変更される可能性があるため、データベースファイルの有効なファイルシステムバックアップを作成するには、データベースサーバーを特殊モードまたはオフライン状態にしなければなりません。データに整合性がなければ、データベースファイルをバックアップしても意味がありません。

次に、データベースまたはアプリケーションのファイルシステムバックアップを構成する手順を示します。

- 対象となるすべてのデータファイルを確認します。
- データベースを停止および開始するための 2 つの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、比較的理解と構成が容易ですが、主な欠点が 1 つあります。**それは、バックアップ中にデータベースにアクセスできないことです。**これは、ほとんどのビジネス環境で、受け入れられることではありません。

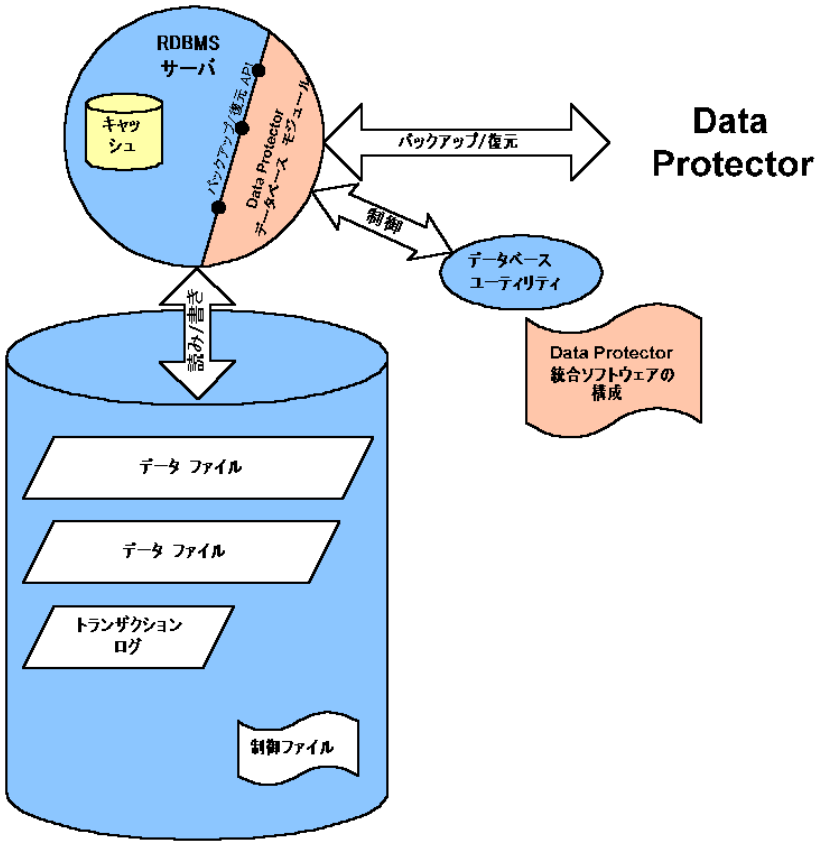
データベースおよびアプリケーションのオンラインバックアップ

バックアップ中にもデータベースを停止せずに済むように、各データベースベンダーでは、データベースを一時的に特殊モードにしてデータをテープに保存できるようにするためのインタ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用すると、バックアップ中または復元中もサーバーアプリケーションをオンライン状態のままにでき、ユーザーの利用が引き続

き可能になります。Data Protector を始めとするバックアップ製品では、これらのアプリケーション固有のインタフェースを使って、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。サポートされている統合機能一覧については、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

バックアップインタ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 74 Data Protector とデータベースの統合



「Data Protector とデータベースの統合」(171 ページ)は、リレーショナルデータベースと Data Protector の統合方法を示したものです。Data Protector では、データベースサーバーにリンクされる**データベースライブラリ**が提供されます。データベースサーバーは、Data Protector に対してデータを送信したり、データを要求したりします。データベースユーティリティは、バックアップ処理や復元処理の開始に使用されます。

以下に、Data Protector の統合機能を使用してデータベースをバックアップするための典型的な構成手順を示します。

1. データベース/アプリケーション固有のエージェントを、データベースシステムにインストールします。
2. データベースごとに、Data Protector の統合ソフトウェアを構成します。Data Protector でデータベースを処理するために必要なデータは、データベースシステムの構成ファイルまたはレジストリエントリに保存されます。通常、この情報には、パス名や、ユーザーの名前とパスワードが含まれます。
3. Data Protector のユーザーインタフェースを使用して、バックアップ仕様を準備します。

データベースと Data Protector 統合ソフトウェアを使用すると、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はありません。これらは、異なるディスク上に置くことができます。
- データベースの論理構造をブラウズできます。データベース中のあるサブセットのみを選択することも可能です。
- アプリケーション側でバックアップ操作を感知して、どの部分がバックアップされたかを追跡できます。
- 複数モードによるバックアップが可能です。**フル**バックアップのほかにも、(ブロックレベルの) **増分**バックアップやトランザクションログのみのバックアップも選択できます。
- 複数のモードによる復元が可能です。またデータファイルの復元後に、データベースにより自動的にトランザクションログを復元し、構成内容に従ってそれらのトランザクションをデータベースに適用することもできます。

仮想環境との統合

この項では、Data Protector と仮想環境との統合について簡単に説明します。サポートされる環境の詳細なリストは、最新のサポート一覧 (http://support.openview.hp.com/selfsolve/manuals) を参照してください。

詳細は、『HP Data Protector インテグレーションガイド - 仮想環境』を参照してください。

仮想マシンのファイルシステムのオフラインバックアップ

仮想マシンは、オンライン中は絶えず変化しているため、ファイルシステムのバックアップを開始する前に、仮想マシンを特別なモードにするか、場合によってはシャットダウンする必要があります。

仮想マシンに属するディスク上のファイルは、整合性がある状態になっていることが必要です。そうでなければ、その仮想マシンに対して作成されたバックアップイメージは役に立ちません。

仮想マシンのファイルシステムバックアップを構成するには、すべての仮想マシンファイルを特定し、仮想マシンのシャットダウンと起動を行う 2 つのプログラムを作成し、すべての仮想マシンファイルが含まれるファイルシステムバックアップ仕様を作成し、シャットダウンプログラムを実行前コマンドとして指定し、起動プログラムを実行後コマンドとして指定する必要があります。

これは、比較的簡単で明瞭な方法ですが、バックアップ中に仮想マシンをアクティブに使用できないという、大きな欠点があります。

仮想マシンのオンラインバックアップ

Data Protector では、仮想環境に用意されている特定のインタフェースを使用して、仮想マシンの稼動中に仮想マシンのバックアップを実行します (オンラインバックアップ)。仮想環境によっては、仮想マシン内のアプリケーションを整合性のある状態に移してからバックアップを開始できます。

データベースとの Data Protector 統合ソフトウェアを使用すると、仮想マシンが常にオンライン状態に保たれるという重要な利点に加えて、以下の利点もあります。

- データファイルの場所を指定する必要はありません。
- 仮想環境側でバックアップ操作を認識し、どの部分がバックアップされたかを追跡できます。
- 複数モードによるバックアップが可能です。
- 複数モードによる復元が可能です。

Microsoft ボリュームシャドウコピーサービス

概要

従来のバックアップ処理は、バックアップアプリケーション (バックアップを開始および実行するアプリケーション) とバックアップ対象アプリケーションが直接交信しながら実行されます。このバックアップ方式では、バックアップアプリケーションがバックアップ対象のアプリケーションのそれぞれに対応した個別のインタフェースを使用する必要があります。アプリケーション固有の実装の数を減らす効果的な方法の 1 つが、バックアップおよび復元プロセスに関連する要素間を調整する機能を導入する方法です。

VSS

ボリュームシャドウコピーサービス (VSS) は、Microsoft 社により Microsoft Windows オペレーティングシステム上に採用されたソフトウェアサービスです。このサービスは、バックアップアプリケーション、バックアップ対象アプリケーション、シャドウコピープロバイダ、およびオペレーティングシステムと連携して、ボリュームシャドウコピーおよびシャドウコピーセットの管理を実現します。

VSS は、任意のアプリケーションのバックアップと復元を、そのアプリケーションの機能に関係なく取りまとめる、統一通信インタフェースを提供します。バックアップアプリケーションは、VSS 仕様に準拠しているアプリケーションであれば、バックアップ対象のアプリケーションを個々に処理する必要はありません。

シャドウコピーとは

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。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。オリジナルボリュームはバックアップ処理中も更新が可能ですが、ボリュームのシャドウコピーは同じ内容に維持されます。

シャドウコピーは基本的にはスナップショットバックアップであり、バックアップの最中もアプリケーションやユーザーはボリュームにデータを書き込むことができます。バックアップ処理には、元のボリュームのシャドウコピー内のデータが使用されます。

シャドウコピーセットとは、同じタイミングで作成されたシャドウコピーの集合を指します。

ライターとは

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 (たとえば 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 以降の Windows オペレーティングシステムに組み込まれています。

VSS ではシャドウコピーの作成時に、まずすべてのハードウェアプロバイダ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

ボリュームシャドウコピーサービスはバックアップおよび復元時の、バックアップアプリケーション、ライター、およびシャドウコピープロバイダ間の調整を可能にします。

「従来のバックアップモデルに関係する要素」(174 ページ) と「VSS バックアップモデルに関係する要素」(174 ページ) 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 75 従来のバックアップモデルに関係する要素

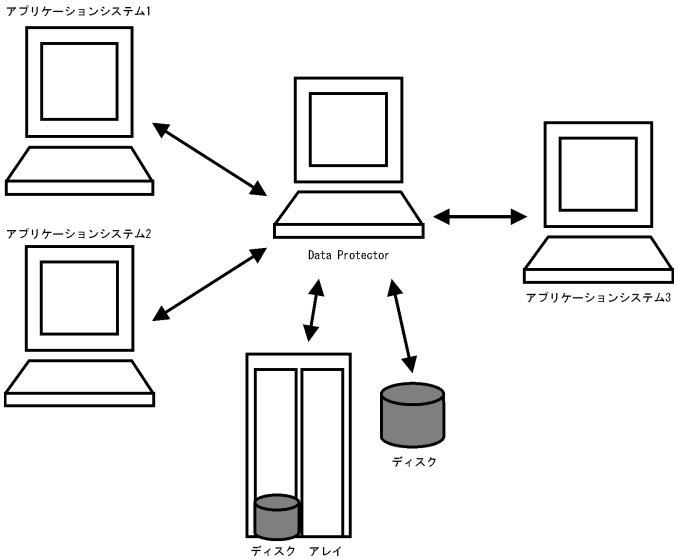
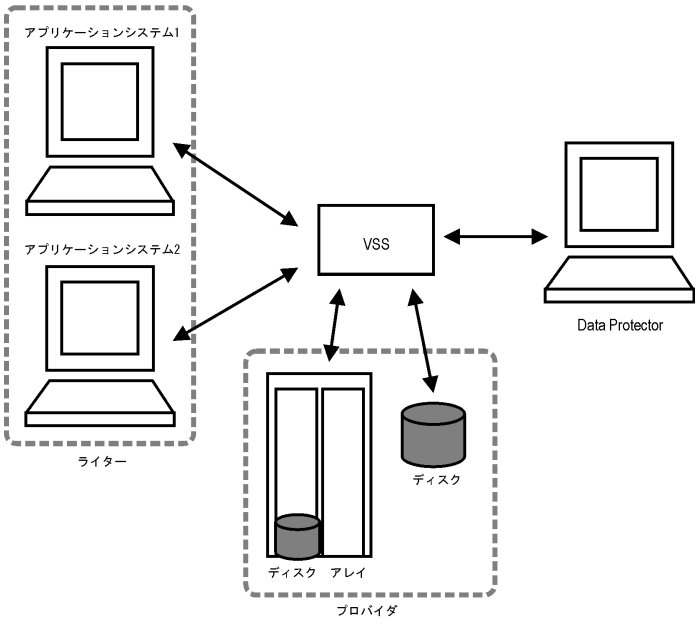


図 76 VSS バックアップモデルに関係する要素



VSS の利点

ボリュームシャドウコピーサービスを使用する利点は以下のとおりです。

- すべてのライターに対して共通のバックアップインタフェース。

- すべてのシャドウコピープロバイダに対して共通のバックアップインタフェース。
- ライターがアプリケーションレベルでデータの整合性を提供できる。バックアップアプリケーションからの介入が不要。

Data Protector は、Microsoft ボリュームシャドウコピーサービスを次の 2 つのレベルでサポートしています。

- Microsoft ボリュームシャドウコピーサービスと統合すると、Data Protector で ZDB およびインスタントリカバリ機能を含む VSS 対応ライターのシャドウコピーバックアップおよび復元が可能になります。
- Disk Agent 機能を使った VSS ファイルシステムバックアップが可能です。

Data Protector の VSS 統合機能では、VSS 対応のライターについてのみ、整合性のあるシャドウコピーバックアップが保証されます。この場合の整合性はライター側で提供されます。アプリケーションが VSS に対応していない場合、シャドウコピーデータの整合性はアプリケーションレベルでは保証されませんが、非 VSS のファイルシステムのバックアップに比べて向上しています。

次の表は、Data Protector の VSS 統合バックアップ、VSS ファイルシステムバックアップ、および非 VSS ファイルシステムバックアップの違いを簡単にまとめたものです。

表 9 VSS を使用する利点

	Data Protector VSS 統合バックアップ	VSS ファイルシステムバックアップ	非 VSS ファイルシステムバックアップ
開いているファイル	開いているファイルはありません。	開いているファイルはありません。	ファイルが開いていると、バックアップが失敗する可能性があります。
ロックされているファイル	ロックされているファイルはありません。	ロックされているファイルはありません。	ロックされているファイルは、バックアップ時にスキップされます。
データの整合性	ライターにより提供されます。	整合性の破綻 (電源障害の場合など)。	なし (本質的に)

Data Protector とボリュームシャドウコピーの統合

Data Protector と Microsoft ボリュームシャドウコピーサービスを統合すると、VSS 対応ライターを完全にサポートできるようになります。このサポートには、VSS 対応ライターの自動検出やバックアップ/復元機能が含まれます。統合ソフトウェアの主な目的は、アプリケーションデータのバックアップです。

統合の詳細については、『HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service』を参照してください。

VSS ファイルシステムとディスクイメージのバックアップと復元

アプリケーションの中にはボリュームシャドウコピーサービスに対応していないものもあります。このようなアプリケーションの場合は、シャドウコピーの作成時にデータの整合性が保証されません。VSS ではこれらのアプリケーションのアクティビティを調整して、整合性のあるバックアップを実行することはできません。ただし、ファイルシステムバックアップよりも優れたデータ整合性を実現できます。Microsoft ではこのようなデータ整合性状態を「クラッシュ時整合状態」と呼んでいます。シャドウコピー ボリュームの準備中には、VSS により、保留中のすべての I/O 操作がコミットされ、新たな書き込み要求は保留されます。このようにしてシャドウコピーの作成中はファイルシステム上のすべてのファイルが閉じられ、ロックは解除されます。

Microsoft ボリュームシャドウコピーを使用すると、バックアップ対象アプリケーションの関与なしにボリュームシャドウコピーを作成できます。この場合シャドウコピー ボリュームの作成

とバックアップは、Data Protector により実行されます。このやり方は、VSS に対応していないアプリケーションに使用できます。

重要: VSS に対応していないアプリケーションをバックアップする場合は、アプリケーション側から見たデータ整合性は保証されません。データの整合性は、電源障害の場合と同じです。Data Protector では、アプリケーションがシャドウコピーの作成に積極的に関与していない場合は、データの整合性を保証できません。

VSS ファイルシステムとディスクイメージバックアップのデータの整合性は、非 VSS ファイルシステムのバックアップよりも向上しています。VSS では、ボリュームのシャドウコピーバックアップを作成できます。シャドウコピーバックアップは、ファイルの正確なポイントインタイムコピーです。開いているファイルもすべて含まれます。たとえば VSS ファイルシステムまたはディスクイメージバックアップでは、排他的に開かれているデータベースや、オペレータやシステムアクティビティにより開かれているファイルもバックアップの対象になります。このようにして、バックアップ中に変更が加えられたファイルも適正にコピーされます。

VSS ファイルシステムおよびディスクイメージバックアップの利点は以下のとおりです。

- アプリケーションやサービスを実行したままでコンピュータをバックアップできます。バックアップの実行中もアプリケーションはボリュームへのデータ書き込みを継続できます。
- 開いているファイルもバックアップ中にスキップされません。これはシャドウコピーの作成時に、これらのファイルがシャドウコピーボリューム上では閉じた状態になるためです。
- ユーザーを締め出すことなくバックアップをいつでも実行できます。
- バックアッププロセス中でも、アプリケーションシステムのパフォーマンスにはほとんど影響はありません。

バックアップと復元

VSS ファイルシステムおよびディスクイメージバックアップは、Windows Server 2003 以降のすべての Windows オペレーティングシステムで、追加のバックアップ機能として実装されています。VSS ファイルシステムバックアップを有効にするには、WinFS のオプションとして指定してください。ディスクイメージバックアップの実行中、VSS ライターがデフォルトで使用されます。データ整合性のレベルは、従来の方法によるアクティブボリュームのバックアップに比べて多少向上しています。Windows ファイルシステムとディスクイメージのバックアップと復元の詳細については、『HP Data Protector ヘルプ』を参照してください。

VSS ファイルシステムおよびディスクイメージバックアップでは、アプリケーションが VSS に対応していないため、データ整合性の向上にアプリケーションが関与することは事実上できません。ただしこの場合も、Data Protector とプロバイダは連携してボリュームシャドウコピーの作成にあたります。VSS バックアップを使用すると、バックアップ中のシステム I/O 動作の有無に関わりなく、特定時点におけるデータ状態をバックアップすることが可能になります。

バックアップ仕様に指定されたボリュームのバックアップを Data Protector が要求すると、VSS により、保留中のすべての I/O 操作がコミットされ、新たな書き込み要求は保留されて、シャドウコピーボリュームの準備が行われます。

シャドウコピーの作成が終了したら、Data Protector による通常のバックアップ手順が開始されます。ただし、バックアップ中はソースボリュームではなく新たに作成されたシャドウコピーが使用されます。シャドウコピーの作成に失敗した場合は、Data Protector は従来の方法によるバックアップを行います (ただし、バックアップ仕様でフォールバックが指定されている場合)。

このように、ファイルが開かれていたりサービスが実行中であっても、コンピュータのバックアップが可能です。この種のバックアップではファイルがスキップされることはありません。VSS を使用するとシャドウコピーの作成中も、実ボリューム上で実行中のサービスやアプリケーションが中断されることはありません。バックアップが終了するとシャドウコピーは削除されます。

VSS ファイルシステムバックアップを使用してバックアップしたデータは、通常と同様の手順で復元できます。

Windows Vista、Windows 7、Windows 2008 Server の各システムでは、EADR および OBDR に対応している場合、VSS ディスクイメージバックアップを使用した論理ボリュームのバックアップが可能です。指定可能なのは論理ボリュームのみです。シャドウコピーを作成できないという点から、IDB と構成オブジェクト、NTFS フォルダとしてマウント済みまたはマウントされていないボリュームは、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てください。

注記: VSS ディスクイメージバックアップのカスタマイズには、`omnirc` 変数を使用します。

9 ゼロダウンタイムバックアップとインスタントリカバリ

この章では、ゼロダウンタイムバックアップとインスタントリカバリの基本的な概念を紹介します。概念の詳しい説明は、『HP Data Protector ゼロダウンタイムバックアップコンセプトガイド』を参照してください。

データベースアプリケーションなど、大量のデータを操作するアプリケーションには、従来のデータバックアップ方法は適していません。データベースをオフラインにする必要がある場合や、アプリケーションで対応している場合には、そのデータがテープへストリーミングされている間に「ホットバックアップモード」になります。最初のケースでは、アプリケーションの操作が大幅に中断される可能性があります。2 番目のケースでは、多くのトランザクションログが生成され、アプリケーションシステムに余分な負荷がかけられる可能性があります。

ゼロダウンタイムバックアップ (ZDB) およびインスタントリカバリ (IR) には、従来のバックアップ方法や復元方法と比べて 2 つの大きな利点があります。

- セッション中にアプリケーションシステムで発生するダウンタイムや影響を最小限に抑えることができる
- 復元にかかる時間を短縮できる

ディスクアレイとストレージの仮想化技術

RAID 技術を使用する大容量ディスクアレイには、膨大な量のデータを含む大規模なアプリケーションデータベースを格納できます。ストレージの 仮想化では、ディスクアレイは多くの仮想ディスクに分割されます。仮想ディスクはディスクアレイ内で簡単にコピーでき、ディスクアレイ技術および空きストレージ容量によっては多数回コピーできることがあります。これによりコピーしたデータに対して操作を行うことが可能になり、オリジナルデータをリスクから解放できます。特に、高可用性が求められるミッションクリティカルな分野において、アプリケーションに対する効率的なバックアップソリューションが可能になります。

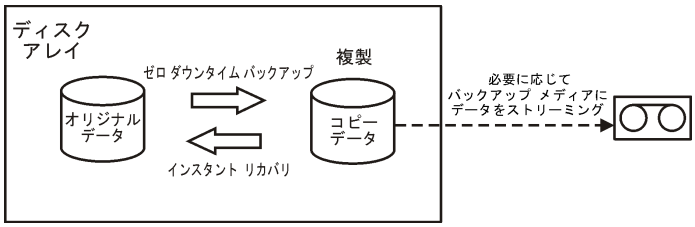
ゼロダウンタイムバックアップ

ゼロダウンタイムバックアップは、ディスクアレイ技術を使用して、バックアッププロセスが原因で発生するサービスの中断を最小限に抑えます。一般的に、データのコピーまたは**複製**は、ディスクアレイ上で作成または管理されます。これは非常に高速に行われるため、アプリケーションシステムへ及ぼす影響は最小限に抑えられます。複製は、それ自体がバックアップになることが可能であるほか、アプリケーションによるソースデータベースの使用をそれ以上妨げずにバックアップメディアにストリーミングすることができます。

複製は、バックアップ対象データの正確なコピーの場合もあれば、仮想コピーの場合もあります。これは、複製の作成に使用されるハードウェアおよびソフトウェアによって異なります。

ZDB では、**複製** (この場合は、複製を作成または保持するプロセスを指す) が、アプリケーションの中断を最小化するうえで重要な要因になります。

図 77 ゼロダウンタイムバックアップとインスタントリカバリの概念



複製の作成

複製プロセスでは、ある瞬間のアプリケーションデータまたはファイルシステムデータの複製が作成されます。

複製されるオリジナルデータオブジェクトを含むボリュームは、**ソースボリューム**と呼ばれます。これらは、同数の**ターゲットボリューム**に複製されます。複製プロセスが完了したときに、ターゲットボリュームのデータによって複製が構築されます。

Data Protector では、基本的な複製方法として次の 2 つの方法を使用します。

- **スプリットミラー**

  ミラーはソースデータの動的な複製で、ソースデータとの同期がとられます。ソースに対するすべての変更が自動的にミラーにも適用されます。

  複製を作成するために、ミラーは一時的にソースから分割されます。データはミラーからバックアップされ、次にミラーではソースとの再同期がとられます。

- **スナップショット**

  スナップショット複製は、特定の時点でデータのコピーを行うことによって作成されます。スナップショットはソースボリュームから独立しているフル コピーか、ソースボリュームに依存している仮想コピーになります。

ZDB の種類

作成された複製は、バックアップメディアへのバックアップが可能です。この複製は、それが作成されたアレイに接続されている**バックアップシステム**にマウントされます。ZDB の利点を最大限に生かすには、分離したシステムにする必要があります。ZDB には、次の 3 つの形式があります。

- **テープへの ZDB**
  1. 複製内のデータは、選択したバックアップの種類 (Full、Incr、Incr1～9) に従ってテープにストリーミングされます。
  2. ストリーミングが完了したら、複製は破棄してかまいません。

  データは、Data Protector の**標準的な**技術を使用してテープから復元できます。

- **ディスクへの ZDB**

  複製は、ディスクアレイに保持され、バックアップとして使用されます。

  インスタントリカバリを使用してデータを復元することで、完全な複製を復元できます。「インスタントリカバリ」 (179 ページ) を参照してください。

- **ディスク + テープへの ZDB**
  1. 複製内のデータは、選択したテープバックアップの種類 (Full、Incr、Incr1～9) に従ってテープにストリーミングされます。
  2. 複製はディスクアレイ上に保持されます。

  これは次の 2 通りの方法でデータを復元できるため、柔軟性の高い方法と言えます。

  - Data Protector を使用してバックアップメディアから復元する標準的な方法 (バックアップオブジェクトを個別に復元可能)
  - インスタントリカバリを使用して、複製から直接、完全な複製を復元する方法

データのインスタントリカバリと復元

インスタントリカバリ

インスタントリカバリでは、データの復元先のディスクアレイに複製が存在する必要があります。アプリケーションシステムとバックアップシステムが無効化されるほか、複製の内容が元

の場所に直接復元されるか、ソースボリュームの内容の代わりに複製の内容がシステムのアクセス先として設定されます。インスタントリカバリはディスクアレイ内部で実行されるので、通常は非常に高速に実行されます。

インスタントリカバリが完了すると、関連するデータベースやファイルシステムのセクションは複製が作成された時点の状態に戻り、アプリケーションシステムも再び使用可能になります。

関連するアプリケーションまたはデータベースにより、これが必要なすべてのものになります。一部の場合、別にバックアップされ、アーカイブされたトランザクションログファイルの適用など、完全な復元には追加の処理が必要な場合もあります。

その他の復元方法

バックアップメディアにバックアップされたデータは、 **標準的な Data Protector の復元**処理を使用して復元できます。

ただし、特定のディスクアレイファミリでは、先にバックアップメディアからデータを復元して複製を更新し、その後、複製の内容を元の場所に復元することができます。これは、**スプリットミラー復元**と呼ばれます。複製の内容を元の場所に復元することは、インスタントリカバリと類似したプロセスです。この段階でのみアプリケーション操作を中断する必要があり、アプリケーションへの影響が最小限に抑えられます。

用語集

A

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。

AES 256 ビット暗号化
256 ビット長のランダムキーを使用する AES-CTR(Advanced Encryption Standard in Counter Mode) 暗号化アルゴリズムを基にした Data Protector ソフトウェア暗号化。暗号化と復号化の両方で同じキーが使用されます。データはネットワークを介して転送される前およびメディアに書き込まれる前に、AES256 ビット暗号化機能によって暗号化されます。

AML
(ADIC/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。

AMU
(ADIC/GRAU 固有の用語) Archive Management Unit(アーカイブ管理単位) の略。

Application Agent
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。

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オリジナル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_program_data*\Config\Server\dr\asr ディレクトリ (Windows Server 2008 の場合)、*Data_Protector_home*\Config\Server\dr\asr ディレクトリ (その他の Windows システムの場合)、または/etc/opt/omni/server/dr/asr ディレクトリ (UNIX システムの場合) に保存されます。障害が発生すると、ASR アーカイブファイルは複数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。

B

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 Protectorbackint 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 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。

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。
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、またはすべての表領域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。
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。
BRBACKUP および BRARCHIVE も参照。

BSM Data Protector バックアップセッションマネージャー (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。

C

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 Catalog Database(カタログデータベース) の略。CDB は IDB の一部で、バックアップ、復元、オブジェクトコピー、オブジェクト集約、オブジェクト検証、メディア管理の各セッションに関する情報が格納されます。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、クラスター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。各セルには Cell Manager システムが 1 つあります。

Certificate Server Windows Certificate Server をインストールして構成すると、クライアントに証明書を提供することができます。証明書サーバーは、エンタープライズ用の証明書を発行および管理するためのカスタマイズ可能なサービスを提供します。これらのサービスでは、公開キーベースの暗号化技術で使用されている証明書の発行、取り消し、および管理が可能です。

Change Log Provider **(Windows 固有の用語)** ファイルシステム上のどのオブジェクトが作成、変更、または削除されたかを判断するために照会できるモジュール。

CMMDB 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 Manager-of-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+ クラス登録データベース **(Windows 固有の用語)**COM+ クラス登録データベースと Windows レジストリには、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 VLS **(VLS 固有の用語)**LAN 経由で VLS を構成、管理、モニターするのに使用する Web ブラウザベースの GUI。
仮想ライブラリシステム (VLS) も参照。

CRS
Data Protector Cell Manager 上で実行され、バックアップと復元セッションを開始、制御する、Cell Request Server のプロセス (サービス)。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。Windows システムでは、CRS 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。UNIX システムでは、CRS はアカウントルートで実行されます。

CSM
Data Protector コピーおよび集約セッションマネージャー (Copy and Consolidation Session Manager) の略。このプロセスは、オブジェクトコピーセッションとオブジェクト集約セッションを制御し、Cell Manager システム上で動作します。

D

Data_Protector_home
Data Protector のプログラムファイルを含むディレクトリへの参照 (Windows Vista、Windows 7、および Windows Server 2008 の場合)、または Data Protector のプログラムファイルおよびデータファイルを含むディレクトリへの参照 (他の Windows オペレーティングシステムの場合)。デフォルトのパスは、`%ProgramFiles%\OmniBack` ですが、パスはインストール時に Data Protector セットアップウィザードで変更できます。
Data_Protector_program_data も参照。

Data_Protector_program_data
Windows Vista、Windows 7、および Windows Server 2008 上の Data Protector データファイルを含むディレクトリへの参照。デフォルトのパスは、`%ProgramData%\OmniBack` ですが、パスはインストール時に Data Protector セットアップウィザードで変更できます。
Data_Protector_home も参照。

Dbobject
(Informix Server 固有の用語) Informix Server 物理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
IDB の詳細カタログバイナリファイル (DCBF) 部には、ファイルのバージョンと属性に関する情報が格納されます。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。バックアップに使用される Data Protector メディアごとに 1 つの DC バイナリファイルが作成されます。サイズの最大値は、ファイルシステムの設定による制限を受けます。

DC ディレクトリ
詳細カタログ (DC) ディレクトリには、詳細カタログバイナリファイル (DCBF) が含まれており、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` と呼ばれ、*`Data_Protector_program_data`*`\db40` ディレクトリ (Windows Server 2008 の場合)、*`Data_Protector_home`*`\db40` ディレクトリ (その他の Windows システムの場合)、または `/var/opt/omni/server/db40` ディレクトリ (UNIX システムの場合) の Cell Manager に置かれます。他の DC ディレクトリを作成し、独自に指定した場所を使用することができます。1 つのセルでサポートされる DC ディレクトリは 50 個までです。DC ディレクトリのデフォルト最大サイズは 16GB です。

DHCP サーバー
Dynamic Host Configuration Protocol(DHCP) を通じて、DHCP クライアントに IP アドレスの動的割り当て機能とネットワーク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。オブジェクト検証セッション中に、Disk Agent は Media Agent からデータを取得し、確認処理を実行しますが、データはディスクには書き込まれません。

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ーに直接アクセスすることを防ぐことができます。

DNS サーバー
DNS クライアント/サーバーモデルでは、DNS サーバー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 サーバーは、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 OS
ディザスタリカバリを実行するオペレーティングシステム環境。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 ディザスタリカバリを実行する前に、DR OS をディスクにインストールするかメモリにロードして、構成しておく必要があります。DR OS には、一時 DR OS とアクティブ DR OS があります。一時 DR OS は、他のオペレーティングシステムの復元用ホスト環境として排他的に使用されます。このホスト環境には、ターゲットとなるオペレーティングシステムの構成データも置かれます。ターゲットシステムを元のシステム構成に復元し終えた後、一時 DR OS は削除されます。アクティブ DR OS は、Data Protector ディザスタリカバリ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。

DR イメージ
一時ディザスタリカバリ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。

E

EMC Symmetrix Agent
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。

Event Log(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。イベントは Cell Manager で記録され、*Data_Protector_program_data*\log\server\Ob2EventLog.txt (Windows Server 2008 の場合)、*Data_Protector_home*\log\server\Ob2EventLog.txt (その他の Windows システムの場合)、/var/opt/omni/server/log/Ob2EventLog.txt (UNIX システムの場合) に書き込まれます。このイベントログにアクセスできるのは、Data Protector の Admin ユーザーグループに所属しているユーザーか、Data Protector の「レポートと通知」ユーザー権限が付与されているユーザーのみです。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。

Exchange Replication Service
(Microsoft Exchange Server 固有の用語) ローカル連続レプリケーション (LCR) か、クラスター連続レプリケーション (CCR) テクノロジのいずれかを使用して複製されたストレージグループを表す Microsoft Exchange Server のサービス。
クラスター連続レプリケーションおよびローカル連続レプリケーション も参照。

F

FC ブリッジ
ファイバーチャネルブリッジ を参照。

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。

G

GUI
Data Protector には、構成、管理、および操作に関するあらゆるタスクに簡単にアクセスできる、グラフィカルユーザーインタフェースが用意されています。Windows 用のオリジナルの Data Protector GUI の他に、Data Protector には、さまざまなプラットフォームで実行できる、外観も操作も変わらない Java ベースの GUI も用意されています。

H

Holidays ファイル
休日に関する情報を格納するファイル。このファイルは、*Data_Protector_program_data*\Config\Server\holidays ディレクトリ (Windows Server 2008 の場合)、*Data_Protector_home*\Config\Server\holidays ディレクトリ (その他の Windows システムの場合)、または /etc/opt/omni/server/Holidays ディレクトリ (UNIX システムの場合) の Cell Manager の Holidays ファイルを編集することで、各種の休日を設定できます。

HP Business Copy (BC) P6000 EVA
(HP P6000 EVA ディスクアレイファミリ固有の用語) ローカル複製ソフトウェアソリューションの 1 つで、P6000 EVA ファームウェアのスナップショット機能およびクローン機能を使用して、ソースボリュームの特定時点のコピー (複製) を作成できます。
複製、ソースボリューム、スナップショット、および HP Continuous Access + Business Copy (CA+BC) P6000 EVA も参照。

HP Business Copy (BC) P9000 XP

(HP P9000 XP ディスクアレイファミリ固有の用語) HP P9000 XP ディスクアレイファミリ構成の 1 つで、データ複製やバックアップなどのさまざまな目的のために LDEV の内部コピーの作成および保守を可能にします。これらのコピー (セカンダリボリューム:S-VOL) は、プライマリボリューム (P-VOL) から分離して、別のシステムに接続することができます。Data Protector ゼロダウンタイムバックアップを目的とする場合、アプリケーションシステムで P-VOL を使用可能にし、S-VOL セットのいずれかをバックアップシステムで使用可能にする必要があります。
LDEV、HP Continuous Access (CA) P9000 XP、メインコントロールユニット、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。

HP Command View (CV) EVA

(HP P6000 EVA ディスクアレイファミリ固有の用語) P6000 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ショットやスナップクローン、ミラークローンの作成などに使用されます。HP Command View EVA ソフトウェアは HP ストレージ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 P6000 EVA SMI-S Agent および HP SMI-S P6000 EVA アレイプロバイダ も参照。

HP Continuous Access + Business Copy (CA+BC) P6000 EVA

(HP P6000 EVA ディスクアレイファミリ固有の用語) HP P6000 EVA ディスクアレイファミリ構成の 1 つで、リモート P6000 EVA 上にソースボリュームのコピー (複製) を作成および保守し、このリモートアレイでローカル複製を行うときにソースとしてこのコピーを使用できます。
HP Business Copy (BC) P6000 EVA、複製、およびソースボリューム も参照。

HP Continuous Access (CA) P9000 XP

(HP P9000 XP ディスクアレイファミリ固有の用語) HP P9000 XP ディスクアレイファミリ構成の 1 つで、データ複製やバックアップ、ディザスタリカバリなどのために LDEV のリモートコピーの作成および保守を可能にします。HP CA P9000 XP を使用するには、メイン (プライマリ) ディスクアレイユニットとリモート (セカンダリ) ディスクアレイユニットが必要です。メインディスクアレイユニットはアプリケーションシステムに接続され、オリジナルのデータを格納しているプライマリボリューム (P-VOL) を格納します。リモートディスクアレイはバックアップシステムに接続され、セカンダリボリューム (S-VOL) を格納します。
HP Business Copy (BC) P9000 XP、メインコントロールユニット、および LDEV も参照。

HP Operations Manager

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 HP Operations Manager。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、Windows、HP-UX、Solaris および Linux 上の HP Operations Manager 管理サーバー用の SMART Plug-In として実装されています。以前のバージョンの HP Operations Manager は、IT/Operations、Operations Center、Vantage Point Operations、および OpenView Operations と呼ばれていました。

HP Operations Manager 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 Operations Manager に追加するだけですぐに使えます。HP Operations Manager 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 Operations Manager 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 P6000 EVA SMI-S Agent

HP P6000 EVA ディスクアレイファミリ統合に必要なすべてのタスクを実行する Data Protector のソフトウェアモジュール。P6000 EVA SMI-S Agent を使用すると、受信した要求と HP CV EVA 間のやり取りを制御する HP SMI-S P6000 EVA アレイプロバイダを通じてアレイを制御できます。
HP Command View (CV) EVA および HP SMI-S P6000 EVA アレイプロバイダ も参照。

HP P9000 XP Agent

Data Protector HP P9000 XP ディスクアレイファミリ統合に必要なすべてのタスクを実行する Data Protector コンポーネント。P9000 XP アレイストレージシステムとの通信に RAID Manager ライブラリを使用します。
RAID Manager ライブラリ も参照。

HP SMI-S P6000 EVA アレイプロバイダ

HP P6000 EVA ディスクアレイファミリを制御するために使用するインタフェース。SMI-S P6000 EVA アレイプロバイダは HP 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 HP Command View EVA 間のゲートウェイとして機能します。Data Protector HP P6000 EVA ディスクアレイファミリ統合を使用すると、SMI-S P6000 EVA アレイプロバイダは P6000 EVA SMI-S Agent からの標準化された要求を受け入れ、HP Command View EVA と通信して情報の取得またはメソッドの起動を行って、標準化された応答を返します。
HP P6000 EVA SMI-S Agent および HP Command View (CV) EVA も参照。

I

ICDA **(EMC Symmetrix 固有の用語)**EMC の 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 チャンネル、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 の内部データベース。IDB 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たか、バックアップ、復元などのセッションがどのように実行されたか、どのデバイス、ライブラリ、ディスクアレイが構成されているかなどに関する情報が格納されます。

IDB 復旧ファイル IDB バックアップ、メディア、バックアップ用デバイスに関する情報を含む IDB ファイル (obrindex.dat)。この情報により、IDB の復旧を大幅に簡素化できます。IDB トランザクションログと共にこのファイルを他の IDB ディレクトリとは別の物理ディスクに移動し、さらにこのファイルのコピーを作成することをお勧めします。

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。

Informix Server **(Informix Server 固有の用語)**Informix Dynamic Server のことです。

Informix Server 用の CMD スクリプト **(Informix Server 固有の用語)**Informix Server データベースの構成時に INFORMIXDIR 内に作成される Windows CMD スクリプト。環境変数を Informix Server にエクスポートするコマンド一式が含まれています。

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。

J

Java GUI クライアント Java GUI クライアントは Java GUI コンポーネントの 1 つで、ユーザーインタフェース関連の機能 (Cell Manager グラフィカルユーザーインタフェースおよび Manager-of-Managers(MoM) のグラフィカルユーザーインタフェース) のみで構成されており、機能するためには Java GUI サーバーと接続する必要があります。

Java GUI サーバー Java GUI コンポーネントの 1 つ。Data Protector Cell Manager システムにインストールされています。Java GUI サーバーは、Java GUI クライアントからの要求を受け取って処理し、応答を Java GUI クライアントに戻します。通信には、HTTP (Hypertext Transfer Protocol) とポート 5556 を使用します。

K

keychain パスフレーズを手動で入力しなくても秘密キーを復号化できるようにするツールです。セキュアシェルを使用してリモートインストールを実行する場合、このツールをインストールサーバーにインストールして構成する必要があります。

KMS キー管理サーバー (KMS) は Data Protector の暗号化機能のためのキー管理を提供する、Cell Manager で実行する集中サービス。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。

L

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。

LDEV **(HP P9000 XP ディスクアレイファミリ固有の用語)** HP P9000 XP ディスクアレイファミリのディスクアレイの物理ディスクの論理パーティション。LDEV は、このようなディスクアレイのスプリットミラー機能やスナップショット機能を使用して複製可能なエンティティです。HP Business Copy (BC) P9000 XP、HP Continuous Access (CA) P9000 XP、および複製 も参照。

LISTENER.ORA **(Oracle 固有の用語)**Oracle の構成ファイルの 1 つ。サーバー上の 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 Server UNIX 固有の用語)**ON-Bar に用意されているスクリプトの 1 つで、Informix Server で logfull イベント警告が発行された際に、論理ログファイルのバックアップを開始するために使用できます。Informix Server 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、Informix 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ー) 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。

M

make_net_recovery `make_net_recovery` は、Ignite-UX のコマンドの 1 つ。Ignite-UX サーバーまたはその他の指定システム上にネットワーク経由で復旧アーカイブを作成できます。ターゲットシステムは、Ignite-UX の `make_boot_tape` コマンドで作成したブート可能なテープからブートするか、または Ignite-UX サーバーから直接ブートした後、サブネットを通じて復旧することができます。Ignite-UX サーバーからの直接ブートは、Ignite-UX の `bootsys` コマンドで自動的に行うか、またはブートコンソールから対話的に指定して行うことができます。

make_tape_recovery `make_tape_recovery` は、Ignite-UX のコマンドの 1 つ。システムに応じてカスタマイズしたブート可能テープ (インストールテープ) を作成できます。ターゲットシステムにバックアップデバイスを直接接続し、ブート可能な復旧テープからターゲットシステムをブートすることにより、無人ディザスタリカバリを実行できます。アーカイブ作成時とクライアント復旧時は、バックアップデバイスをクライアントにローカル接続しておく必要があります。

Manager-of-Managers (MoM)
MoM を参照。

MAPI **(Microsoft Exchange Server 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。

MCU メインコントロールユニット (MCU) を参照。

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。復元またはオブジェクト検証セッション中、Media Agent はバックアップメディア上のデータを探して、処理するために Disk Agent に送信します。復元セッションの場合、続いて Disk Agent はデータをディスクに書き込みます。Media Agent は、ライブラリのロボティクス制御も管理します。

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/サーバー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 分散型"クライアント/サーバー"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 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。

Microsoft ボリュームシャドウコピーサービス (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、複製およびライター も参照。

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。集中管理用セルの管理システムが、MoM(Manager-of-Managers) です。他のセルは MoM クライアントと呼ばれます。MoM を介して、複数のセルを一元的に構成および管理することができます。

MSM Data Protector メディアセッションマネージャー (Media Session Manager) 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。

O

obdrindex.dat IDB 復旧ファイル を参照。

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、ディザスタリカバリ用のブートデバイスとしても使用可能です。

ON-Bar **(Informix Server 固有の用語)**Informix Server のためのバックアップと復元のシステム。ON-Bar により、Informix 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` コマンド
- 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。

ONCONFIG **(Informix Server 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、Informix Server が*INFORMIXDIR*`\etc`(Windows の場合)、または*INFORMIXDIR*`/etc/`(UNIX の場合) ディレクトリの `ONCONFIG` ファイルにある構成値を使います。

Oracle Data Guard **(Oracle 固有の用語)**Oracle Data Guard は Oracle の主要なディザスタリカバリソリューションです。プロダクション (一次) データベースのリアルタイムコピーであるスタンバイデータベースを最大 9 個まで保持することにより、破損、データ障害、人為ミス、および災害からの保護を提供します。プロダクション (一次) データベースに障害が発生すると、フェイルオーバーによりスタンバイデータベースの 1 つを新しい一次データベースにすることができます。また、プロダクション処理を現在の一次データベースからスタンバイデータベースに迅速に切り替えたり、元に戻したりできるため、保守作業のための計画ダウンタイムを縮小することができます。

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。

- この場合、*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。各ユーザー名はパスワードと関連付けられており、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する必要があります。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* には、Oracle パスワードファイル (orapwd) 内に指定したのと同じパスワードを指定しなければなりません。パスワードは、データベースを管理するユーザーの認証に使用されます。
- *service* には、ターゲットデータベースのための SQL*Net サーバープロセスの識別に使用される名前を指定します。

P

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拡張自動ディザスタリカバリ (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 に保存されます。保存場所は、*Data_Protector_program_data*\Config\Server\dr\p1s ディレクトリ (Windows Server 2008 の場合)、*Data_Protector_home*\Config\Server\dr\p1s ディレクトリ (その他の Windows システムの場合)、/etc/opt/omni/server/dr/p1s ディレクトリ (UNIX システムの場合) です。ファイル名は以下のとおりです。recovery.p1s.

R

RAID

Redundant Array of Independent Disks の略。

RAID Manager P9000 XP

(HP P9000 XP ディスクアレイファミリ固有の用語) HP P9000 XP ディスクアレイファミリのディスクアレイに対するコマンドラインインタフェースを提供するソフトウェアアプリケーション。P9000 XP アレイストレージシステムのステータスのレポートと制御を行い、ディスクアレイに対する各種操作を実行するための広範なコマンドセットが用意されています。

RAID Manager ライブラリ

(HP P9000 XP ディスクアレイファミリ固有の用語)P9000 XP アレイストレージシステムの構成、ステータス、およびパフォーマンス測定のデータへのアクセスと、ディスクアレイの操作の開始に使用されるソフトウェアライブラリ。このライブラリにより、関数呼び出しが一連の低レベルの SCSI コマンドに変換されます。
HP P9000 XP Agent も参照。

raw ディスクバックアップ

ディスクイメージバックアップ を参照。

RCU

Remote Control Unit(RCU) を参照。

RCU Remote Control Unit (RCU)

(HP P9000 XP ディスクアレイファミリ固有の用語) HP CA P9000 XP または HP CA+BC P9000 XP 構成におけるメインコントロールユニット (MCU) に対するスレーブデバイスとして機能する HP P9000 XP ディスクアレイファミリユニット。双方向の構成の中では、RCU は MCU としての役割も果たします。

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 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。

Recovery Manager (RMAN)

(Oracle 固有の用語) Oracle コマンドラインインタフェース。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。

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、ディザスタリカバリ時に必要になります。

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。

RMAN(Oracle 固有の用語) Recovery Manager を参照。

RSM Data Protector 復元セッションマネージャー (Restore Session Manager) の略。復元セッションおよびオブジェクト検証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。

S

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 サーバー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、復元、オブジェクトコピー、オブジェクト集約、オブジェクト検証、およびメディア管理の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。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。

SMI-S Agent(SMISA) HP P6000 EVA SMI-S Agent を参照。

sqlhosts ファイルまたはレジストリ **(Informix Server 固有の用語)**Informix Server の接続情報ファイル (UNIX) またはレジストリ (Windows)。各データベースサーバーの名前の他、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。

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。

SRD ファイル **(ディザスタリカバリ固有の用語)** Unicode (UTF-16) 形式のテキストファイルで、Windows システムの CONFIGURATION バックアップ中に生成され Cell Manager に格納されます。このファイルには、障害発生時にターゲットシステム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。
ターゲットシステム も参照。

SSE Agent(SSEA) HP P9000 XP Agent を参照。

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 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い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、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、それぞれ必要です。

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ー」アーキテクチャ内のサーバー。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。

SYMA EMC Symmetrix Agent を参照。

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ー 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。

T

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ーの `SYS:SYSTEM\TSA` ディレクトリにあります。

U

UIProxy Java GUI サーバー (`UIProxy` サービス) は Data Protector Cell Manager で実行されます。Java GUI サーバーでは、Java GUI クライアントと Cell Manager との間の通信を行います。また、ビジネスロジック操作を実行し、重要な情報のみをクライアントに送信する必要があります。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。

user_restrictions ファイル 割り当てられているユーザー権限に応じて Data Protector のユーザーグループが使用できる特定のユーザーアクションを、Data Protector セルの特定のシステムでのみ実行されるように制限するファイル。このような制限は、**Admin** および **Operator** 以外の Data Protector のユーザーグループにのみ適用されます。

V

VMware 管理クライアント **(VMware(レガシー) 用統合ソフトウェア固有の用語)**Data Protector で、VMware 仮想インフラストラクチャとの通信に使用されるクライアント。VirtualCenter Server システム (VirtualCenter 環境)、または ESX Server システム (スタンドアロン ESX Server 環境) のどちらかです。

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。

VSS Microsoft ボリュームシャドウコピーサービス (VSS) を参照。

VSS 準拠モード **(HP P9000 XP ディスクアレイファミリ VSS プロバイダ固有の用語)** 2 種類ある P9000 XP アレイ VSS ハードウェアプロバイダの操作モードの 1 つ。P9000 XP アレイプロバイダが VSS 準拠モードであると、ソースボリューム (P-VOL) とその複製 (S-VOL) は、バックアップ後、単純非対状態になります。したがって、ローテーションされる複製数 (P-VOL 当たりの S-VOL

数) に制限はありません。このような構成でのバックアップからの復元は、ディスクの切り替えによってのみ可能となります。
再同期モード、ソースボリューム、プライマリボリューム (P-VOL)、複製、セカンダリボリューム (S-VOL)、および複製セットローテーション も参照。

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。

W

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、オブジェクトコピーステータスおよびオブジェクト集約ステータスと 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 構成のバックアップ
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 サーバーデータおよび DHCP サーバーデータ (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 サーバー
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 サーバーデータを Windows の構成データの一部としてバックアップできます。

X

XBSA インタフェース
(Informix Server 固有の用語)ON-Bar と Data Protector の間の相互通信には、X/Open Backup Services Application Programmer's Interface (XBSA) が使用されます。

Z

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、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、ゼロダウンタイムバックアップ、インスタントリカバリ、スプリットミラー復元の各セッションで使用されます。
ゼロダウンタイムバックアップ (ZDB) も参照。

あ

アーカイブ REDO ログ
(Oracle 固有の用語) オフライン REDO ログとも呼びます。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、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、いっぱい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初めて上書きされるモードです。

アクセス権限
ユーザー権限 を参照。

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。

暗号化 KeyID-StoreID Data Protector Key Management Server が 、Data Protector で使用される暗号化キーの識別と管理に使用する複合識別子です 。`KeyID` は、キーストア内のキーを識別します。`StoreID` は、Cell Manager 上のキーストアを識別します。Data Protector を暗号化機能付きの旧バージョンからアップグレードした場合、同じ Cell Manager 上で使用される `StoreID` が複数存在する可能性があります。

暗号化キー 256 ビットのランダムに生成された数値で、AES 256 ビットソフトウェア暗号化またはドライブベースの暗号化が指定されたバックアップの際に、Data Protector の暗号化アルゴリズムが情報を暗号化するために使用します。これに続く情報の復号化では、同じキーが使用されます。Data Protector セルの暗号化キーは、Cell Manager 上の中央キーストアに保存されます。

暗号制御通信 Data Protector セル内のクライアント間における Data Protector のセキュアな通信は、Secure Socket Layer (SSL) をベースにしており、SSLv3 アルゴリズムを使用して制御通信が暗号化されます。Data Protector セル内の制御通信は、Disk Agent(および統合用ソフトウェア) から Media Agent へのデータ転送とその逆方向のデータ転送を除く、Data Protector プロセス間のすべての通信です。

い

イベントログ **(Windows 固有の用語)** サービスの開始または停止、ユーザーのログオンとログオフなど、Windows がすべてのイベントを記録したファイル。Data Protector は、Windows イベントログを Windows 構成バックアップの一部として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ー 特定のアーキテクチャ用の Data Protector インストール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ーから 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、少なくとも 2 台のインストールサーバーが必要です。1 台は UNIX システム用で、1 台は Windows システム用です。

インターネットインフォメーションサービス (IIS)
(Windows 固有の用語) Microsoft Internet Information Services は、ネットワーク用ファイル/アプリケーションサーバーで、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。

インフォメーションストア **(Microsoft Exchange Server 固有の用語)** ストレージ管理を行う Microsoft Exchange Server のサービス。Microsoft Exchange Server 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という 2 種類のストアを管理します。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。

う

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。

え

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。

お

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)** オブジェクト ID(OID) を使用すると、システムのどこにファイルがあるかにかかわらず、NTFS 5 ファイルにアクセスできます。Data Protector では、ファイルの代替ストリームとして OID を扱います。

オブジェクト検証 Data Protector の観点で見たバックアップオブジェクトのデータ整合性と、それらを必要なあて先に送信する Data Protector の機能を確認する処理です。処理は、バックアップ、オブジェクトコピー、またはオブジェクト集約セッションによって作成されたオブジェクトバージョンを復元する機能に信頼レベルを付与するために使用できます。

オブジェクト検証セッション 指定のバックアップオブジェクトまたはオブジェクトバージョンのデータ整合性と、指定のホストにそれらを送信するための選択済み Data Protector ネットワークコンポーネントの機能を確認するプロセスです。オブジェクト検証セッションは、対話式に実行することも、自動ポストバックアップまたはスケジュール仕様の指定通りに実行することもできます。

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データの追加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。

オブジェクト集約 1 つのフルバックアップと 1 つ以上の増分バックアップで構成されたバックアップオブジェクトの復元チェーンを、新たな集約されたバージョンのオブジェクトとしてマージするプロセス。このプロセスは、合成バックアップの一部です。このプロセスの結果、指定のバックアップオブジェクトの合成フルバックアップが出力されます。

オブジェクト集約セッション 1 つのフルバックアップと 1 つ以上の増分バックアップで構成されたバックアップオブジェクトの復元チェーンを、新たな統合されたバージョンのオブジェクトとしてマージするプロセス。

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バージョンを選択できます。

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、いくつかのメディアセットに同じデータを書き込むプロセス。Data Protector を使用すると、1 つまたは複数のメディアセットに対し、すべてまたは一部のバックアップオブジェクトをミラーリングすることができます。

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。オフラインバックアップセッションでは、一般にデータベースはデータ複製プロセス中に休止状態となり、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。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 も参照。

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。オフライン復旧では、スタンドアロンデバイスおよび SCSI ライブラリデバイスのみが使用可能です。Cell Manager の復旧は、常にオフラインで行われます。

オリジナルシステム 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。

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、データ複製プロセスの間、特別なバックアップモードで稼動します。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。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。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。

オンライン復旧 オンライン復旧は、Cell Manager がアクセス可能な場合に行います。この場合、Data Protector のほとんどの機能 (Cell Manager によるセッションの実行、復元セッションの IDB への記録、GUI を使った復元作業の進行状況の監視など) が使用可能です。

か

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 固有の用語)**Microsoft Exchange Server 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。

拡張増分バックアップ 従来の増分バックアップでは、前回のバックアップより後に変更されたファイルがバックアップされますが、変更検出機能に限界があります。これに対し、拡張増分バックアップでは、名前が変更されたファイルや移動されたファイルのほか、属性が変更されたファイルについても、信頼性のある検出とバックアップが行われます。

確認 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。

仮想コントローラソフトウェア (VCS) **(HP P6000 EVA ディスクアレイファミリ固有の用語)**HSV コントローラを介した HP 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。
HP Command View (CV) EVA も参照。

仮想サーバー 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ー環境の仮想マシンです。アドレスはクラスターソフトウェアによりキャッシュされ、仮想サーバーリソースを現在実行しているクラスターノードにマップされます。こうして、特定の仮想サーバーに対するすべての要求が特定のクラスターノードにキャッシュされます。

仮想ディスク **(HP P6000 EVA ディスクアレイファミリ固有の用語)** HP P6000 EVA ディスクアレイファミリのディスクアレイのストレージプールから割り当てられるストレージユニット。仮想ディスクは、このようなディスクアレイのスナップショット機能を使用して複製可能なエンティティです。
ソースボリュームおよびターゲットボリューム も参照。

仮想テープ **(VLS 固有の用語)** テープに保存された場合と同様にディスクドライブにデータをバックアップするアーカイブ式ストレージテクノロジ。バックアップスピードおよびリカバリスピードの向上、運用コストの削減など仮想テープシステムとしての利点がある。
仮想ライブラリシステム (VLS) および仮想テープライブラリ (VTL) も参照。

仮想テープライブラリ (VTL) **(VLS 固有の用語)** 従来のテープベースのストレージ機能を提供する、エミュレートされるテープライブラリ。

仮想ライブラリシステム (VLS) も参照。

仮想デバイスインタフェース **(Microsoft SQL Server 固有の用語)**Microsoft SQL Server 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。

仮想フルバックアップ コピーするのではなくポインタを使用してデータが統合される、効率の良い合成バックアップ。配布ファイルメディア形式を使用する 1 つのファイルライブラリにすべてのバックアップ (フルバックアップ、増分バックアップ、およびその結果である仮想フルバックアップ) が書き込まれる場合に実行されます。

仮想ライブラリシステム (VLS) 1 つまたは複数の仮想テープライブラリ (VTL) をホストする、ディスクベースのデータストレージデバイス。

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。

監査情報 Data Protector セル全体に対し、ユーザーが定義した拡張期間にわたって実施された、全バックアップセッションに関するデータ。

監査レポート 監査ログファイルに保存されたデータから作成される、ユーザーが判読可能な形式の監査情報出力。

監査ログ 監査情報が保存されるデータファイル。

き

キーストア すべての暗号化キーは、Cell Manager のキーストアに集中的に格納され、キー管理サーバー (KMS) により管理されます。

キーマネージメントサービス **(Microsoft Exchange Server 固有の用語)** 拡張セキュリティのための暗号化機能を提供する Microsoft Exchange Server 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 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 Server 固有の用語)**Informix Server 構成ファイル `ixbar.`*`server_id`*。このファイルは、*`INFORMIXDIR`*`/etc` ディレクトリ (Windows の場合)、または *`INFORMIXDIR`*`\etc` ディレクトリ (UNIX の場合) に置かれています。*`INFORMIXDIR`* は Informix Server のホームディレクトリ、*`server_id`* は `SERVERNUM` 構成パラメータの値です。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。

く

クライアントバックアップ Data Protector クライアントにマウントされているすべてのボリューム (ファイルシステム) のバックアップ。実際に何がバックアップされるかは、バックアップ仕様でどのようにオブジェクトを選択するかによって異なります。

- クライアントシステム名の隣のチェックボックスを選択した場合、[クライアントシステム] の種類の 1 つのバックアップオブジェクトが作成されます。その結果、バックアップ時に Data Protector は選択されたクライアントにマウントされているすべてのボリュームを最初に検出してから、それらをバックアップします。Windows クライアントの場合、`CONFIGURATION` もバックアップされます。
- クライアントシステムにマウントされているすべてのボリュームを別々に選択する場合、`Filesystem` タイプの個別バックアップオブジェクトがボリュームごとに作成されます。その結果、バックアップ時に、選択されたボリュームのみがバックアップされます。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ボリュームは、バックアップされません。

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。

クラスター対応アプリケーション クラスター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。クラスター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。

クラスター連続レプリケーション **(Microsoft Exchange Server 固有の用語)** クラスター連続レプリケーション (CCR) はクラスター管理とフェイルオーバーオプションを使用して、ストレージグループの完全なコピー (CCR コピー) を作成および維持する高可用性ソリューションです。ストレージグループは個別のサーバーに複製されます。CCR は Exchange バックエンドサーバーで発生した単発箇所の障害を取り除きます。CCR コピーが存在するパッシブ Exchange Server ノードで VSS を使用してバックアップを実行すれば、アクティブノードの負荷が軽減されます。

CCR コピーへの切り替えは数秒で完了するため、CCR コピーはディザスタリカバリに使用されます。複製されたストレージグループは、Exchange ライターの新しいインスタンス (Exchange Replication Service) として表示され、元のストレージグループと同様に VSS を使用してバックアップできます。

Exchange Replication Service およびローカル連続レプリケーション も参照。

グループ **(Microsoft Cluster Server 固有の用語)** 特定のクラスター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、*Data_Protector_program_data*\Config\Server\Options ディレクトリ (Windows Server 2008 の場合)、*Data_Protector_home*\Config\Server\Options ディレクトリ (その他の Windows システムの場合)、または /etc/opt/omni/server/options ディレクトリ (HP-UX または Linux システムの場合) の Cell Manager に置かれています。

こ

合成バックアップ データに関しては従来のフルバックアップと同じである合成フルバックアップを、生産サーバーやネットワークに負担をかけずに出力するバックアップソリューション。合成フルバックアップは、前回のフルバックアップと任意の数の増分バックアップを使用して作成されます。

合成フルバックアップ バックアップオブジェクトの復元チェーンが新たな合成フルバージョンのオブジェクトにマージされる、オブジェクト集約処理の結果。合成フルバックアップは、復元速度の面では従来のフルバックアップと同じです。

コピーセット **(HP P6000 EVA ディスクアレイファミリ固有の用語)** ローカル P6000 EVA 上にあるソースボリュームとリモート P6000 EVA 上にあるその複製とのペア。
ソースボリューム、複製、および HP Continuous Access + Business Copy(CA+BC)P6000 EVA も参照。

コマンドデバイス **(HP P9000 XP ディスクアレイファミリ固有の用語)** ディスクアレイ内の専用のボリュームで、管理アプリケーションとディスクアレイのストレージシステムとの間のインタフェースとして機能します。データストレージ用に使用することはできません。操作に対する要求のみを受け付け、ディスクアレイによってその操作が実行されます。

コマンドラインインタフェース (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。

コンテナ **(HP P6000 EVA ディスクアレイファミリ固有の用語)** ディスクアレイ上のスペース。後で標準スナップショット、vsnap、またはスナップクローンとして使用するために事前に割り当てられます。

さ

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。

再同期モード

(HP P9000 XP ディスクアレイファミリ VSS プロバイダ固有の用語) 2 種類ある P9000 XP アレイ VSS ハードウェアプロバイダの操作モードの 1 つ。P9000 XP アレイプロバイダが再同期モードであると、ソースボリューム (P-VOL) とその複製 (S-VOL) は、バックアップ後、中断ミラー関係になります。MU 範囲が 0-2(つまり、0、1、2) の場合、ローテーションされる最大複製数 (P-VOL 当たりの S-VOL 数) は 3 となります。このような構成でのバックアップからの復元は、S-VOL をその P-VOL と再同期することによってのみ可能となります。
VSS 準拠モード、ソースボリューム、プライマリボリューム (P-VOL)、複製、セカンダリボリューム (S-VOL)、ミラーユニット (MU) 番号、および複製セットローテーション も参照。

サイト複製サービス

(Microsoft Exchange Server 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、Microsoft Exchange Server 5.5 と互換性のある Microsoft Exchange Server 2003 のサービス。
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 制御操作。BCV 制御操作では、差分同期 (Incremental Establish) 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、差分同期 (Incremental Establish) 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

前回のフルバックアップより後の変更をバックアップする増分バックアップ。このバックアップを実行するには、増分 1 バックアップを指定します。
増分バックアップ も参照。

差分バックアップ

(Microsoft SQL Server 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 制御操作。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。

し

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/システムディスク/システムパーティションと呼んでいます。

システム状態

(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 (Certificate Server の場合) が含まれます。サーバーがドメインコントローラの場合は、Active Directory 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。サーバーがクラスターサービスを実行している場合、システム状態データにはリソースレジストリチェックポイントとクォーラムリソースリカバリ ログが含まれ、最新のクラスターデータ情報が格納されます。

システムデータベース

(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)

システム復旧データファイル SRD ファイル を参照。

事前割り当てリスト 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 も参照。

実行前コマンドと実行後コマンド 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。

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 も参照。

自動移行 **(VLS 固有の用語)** データのバックアップをまず VLS の仮想テープに作成し、それを物理テープ (1 つの仮想テープが 1 つの物理テープをエミュレート) に移行する操作を、中間バックアップアプリケーションを使用せずに実行する機能。
仮想ライブラリシステム (VLS) と仮想テープ も参照。

自動ストレージ管理 (ASM) **(Oracle 固有の用語)** Oracle に統合されるファイルシステムおよびボリュームマネージャーで、Oracle データベースファイルを管理します。データやディスクの管理が簡単になり、ストライピング機能やミラーリング機能によってパフォーマンスが最適化されます。

シャドウコピー **(Microsoft 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 ボリュームシャドウコピーサービスおよび複製 も参照。

シャドウコピーセット **(Microsoft 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。
シャドウコピーおよび複製セット も参照。

シャドウコピープロバイダ **(Microsoft 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 (システムプロバイダなど) で実装することも、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。

集中型ライセンス 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。

循環ログ **(Microsoft Exchange Server および Lotus Domino Server 固有の用語)** 循環ログは、Microsoft Exchange Server データベースおよび Lotus Domino Server データベースモードの 1 つ。このモードでは、トランザクションログファイルのコンテンツは、対応するデータがデータベースにコミットされると、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要件が軽減されます。

初期化 フォーマット を参照。

所有権

バックアップ所有権は、データを参照および復元するユーザーの能力に影響します。各バックアップセッションとその中でバックアップされたすべてのデータはオーナーに割り当てられます。所有者は、対話型バックアップを開始するユーザー、CRS プロセスを実行するときに使用するアカウント、またはバックアップ仕様オプションで所有者として指定されたユーザーです。

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。

ユーザーがバックアップ仕様を修正して起動すると、以下の条件が成立しない限り、そのユーザーがオーナーになります。

- そのユーザーが [セッションの所有権を切り替え] ユーザー権限を持っている。
- バックアップ仕様内でバックアップセッションオーナーを明示的に定義するには、ユーザー名、グループ名またはドメイン名、およびシステム名を指定します。

UNIXCell Manager 上でスケジュールしたバックアップの場合、上記の条件が成立しない限り、root: sys がセッションオーナーになります。

Windows Cell Manager 上でスケジューリングしたバックアップの場合は、上記の条件が成立していない限り、インストール時に指定されたユーザーがセッションオーナーになります。

オブジェクトのコピーまたは統合を行う場合のオーナーは、コピー仕様や統合仕様で別のオーナーが指定されていない限り、デフォルトでは、その操作を開始するユーザーです。

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 (たとえば、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 固有の用語) 同じログファイルを共有する複数のメールボックスストアとパブリックフォルダストアのコレクション。Exchange Server では、各ストレージグループを個別のサーバー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) ボリューム管理システム、ファイルシステム、他のオブジェクトなどが存在可能なオペレーティングシステムや他のエンティティ (たとえば、仮想化機構など) に提示できるオブジェクト。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 P4000 SAN ソリューション、HP P6000 EVA ディスクアレイファミリ、HP P9000 XP ディスクアレイファミリ、および HP P10000 Storage Systems 固有の用語) 特定の複製方法で作成されたターゲットボリュームの種類の 1 つ。ディスクアレイモデルと選択した複製方法に応じて、特性の異なる、さまざまなスナップショットの種類が使用できます。基本的に、各スナップショットは仮想コピー (ソースボリュームの内容に引き続き依存します)、またはソースボリュームから独立した複製 (クローン) のどちらかです。
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 P4000 SAN ソリューション、HP P6000 EVA ディスクアレイファミリ、HP P9000 XP ディスクアレイファミリ、および HP P10000 Storage Systems 固有の用語) 選択したソースボリュームのコピーをストレージ仮想化技術を使用して作成する複製作成プロセス。スナップショットは、ある特定の時点で作成されたとみなされる複製で、作成後すぐに使用できます。ただし、スナップショットの種類によっては、複製作成後にデータコピープロセスがバックグランドで継続して実行されるものもあります。
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 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。例として、データの一部または大部分にゼロが含まれるマトリクス、イメージアプリケーションからのファイル、高速データベースなどがあります。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 Disk Array および HP P9000 XP ディスクアレイファミリ固有の用語)** 特定の複製方法で作成されたターゲットボリュームの種類の 1 つ。スプリットミラー複製により、ソースボリュームの独立した複製 (クローン) が作成されます。
複製およびスプリットミラーの作成 も参照。

スプリットミラーの作成 **(EMC Symmetrix および HP P9000 XP ディスクアレイファミリ固有の用語)** 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 P9000 XP ディスクアレイファミリ固有の用語) 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 P9000 XP ディスクアレイファミリ固有の用語)** 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、最初にバックアップメディアから複製に、その後に複製からソースボリュームにコピーするプロセス。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。

スマートコピー **(VLS 固有の用語)** 仮想テープから物理テープライブラリへ作成されたバックアップデータのコピー。スマートコピーのプロセスによって、Data Protector ではソースメディアとターゲットメディアを区別できるため、メディア管理が可能になります。
仮想ライブラリシステム (VLS) も参照。

スマートコピープール **(VLS 固有の用語)** 指定されたソース仮想ライブラリに対してどのコピー先ライブラリスロットをスマートコピーターゲットとして使用できるかどうかを定義するプール。
仮想ライブラリシステム (VLS) およびスマートコピー も参照。

スレッド **(Microsoft SQL Server 固有の用語)** 1 つのプロセスのみに属する実行可能なエンティティ。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、およびレジスタ値のセットからなります。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 DLT テープなどのメディアを 1 つずつ格納できます。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。

せ

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記述された 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 P9000 XP ディスクアレイファミリ固有の用語)** HP P9000 XP ディスクアレイファミリのディスクアレイの内部ディスク (LDEV) で、もう 1 つの LDEV であるプライマリボリューム (P-VOL) とペアとなっています。プライマリボリューム (P-VOL) セカンダリボリュームは、P-VOL のミラーとして、また P-VOL のスナップショットストレージに使用されるボリュームとして機能することが可能です。S-VOL は P-VOL に使用される SCSI アドレスとは異なるアドレスに割り当てられます。HP CA P9000 XP 構成では、ミラーとして機能する S-VOL を MetroCluster 構成のフェイルオーバーデバイスとして使用することができます。

プライマリボリューム (P-VOL) およびメインコントロールユニット (MCU) 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、オブジェクトコピー、オブジェクト集約、オブジェクト検証、またはメディア管理の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。Data Protector プレビューセッションを含めた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、`omnimnt`, `omnistat` および `omniabort` コマンド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。セルは、通常、同じ LAN または SAN に接続されている、サイト上または組織エンティティ上のシステムを表します。集中管理によるバックアップおよび復元のポリシーやタスクの管理が可能です。

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。

そ

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 ZDB ファイルシステム ZDB からテープへ、または ZDB からディスク + テープへのセッション。前回の保護されたフルバックアップまたは増分バックアップ以降に変更された内容のみがテープにストリーミングされます。
フル ZDB も参照。

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、復元チェーンの長さを細かく制御できます。
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)** 複製されるデータを含むストレージボリューム。

た

ターゲットシステム **(ディザスタリカバリ固有の用語)** コンピュータの障害が発生した後のシステム。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ディザスタリカバリの目標となります。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)** ターゲットデバイス (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)** 複製されるデータを含む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、サーバー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。

ち

チャンネル **(Oracle 固有の用語)**Oracle Recovery Manager リソース割り当て。チャン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、指定されたチャンネルの種類が sbt_tape タイプの場合は、上記のサーバープロセスが 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。

て

ディザスタリカバリ 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。

ディザスタリカバリオペレーティングシステム
DR OS を参照。

ディザスタリカバリの段階 0 ディザスタリカバリの準備 (ディザスタリカバリを成功させるための必須条件)。

ディザスタリカバリの段階 1 DR OS のインストールと構成 (以前の記憶領域構造の構築)。

ディザスタリカバリの段階 2 オペレーティングシステム (環境を定義する各種の構成情報を含む) と Data Protector の復元。

ディザスタリカバリの段階 3 ユーザーデータとアプリケーションデータの復元。

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プロセス、Data Protector 標準のテープからの復元を使用して復元できます。特定のディスクアレイファミリ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 システムのデータストレージの基本ユニット。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。

ディスクステージング データをいくつかの段階に分けてバックアップする処理。これにより、バックアップと復元のパフォーマンスが向上し、バックアップデータの格納費用が節減され、データの可用性と復元時の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 通信チャン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。

データ複製 (DR) グループ **(HP P6000 EVA ディスクアレイファミリ固有の用語)**HP P6000 EVA ディスクアレイファミリ仮想ディスクの論理グループ。共通の性質を持ち、同じ HP CA P6000 EVA ログを共有していれば、最大 8 組のコピーセットを含めることができます。
コピーセット も参照。

データベースサーバー 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。サーバー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ーと Data Protector の間でのデータ転送を可能にします。

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。

テープなしのバックアップ (ZDB 固有の用語) ディスクへの ZDB を参照。

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。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。特定のディスクアレイファミリでは、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、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 も参照。

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 Synnetrix 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。

デルタバックアップ 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。

と

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。

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、別のサーバー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ー。

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。

ドライブベースの暗号化 Data Protector のドライブベースの暗号化では、ドライブの暗号化機能が使用されます。バックアップの実行中、ドライブではメディアに書き込まれるデータとメタデータの両方が暗号化されます。

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旧できます。

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 **(Microsoft 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 ボリュームシャドウコピーサービス (VSS) も参照。

は

ハートビート 特定のクラスター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ーデータセット。このデータセット (パケット) は、すべてのクラスター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。

配布ファイルメディア形式 ファイルライブラリで利用できるメディア形式。仮想フルバックアップと呼ばれる容量効率のいい合成バックアップをサポートしています。この形式を使用することは、仮想フルバックアップにおける前提条件です。
仮想フルバックアップ も参照。

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います。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/アプリケーション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:ファイルシステムオブジェクトを対象とする場合 — バックアップオブジェクトが存在するクライアント (Windows ではドライブ、UNIX ではマウントポイント) 上のディレクトリ構造におけるアクセスポイント。統合オブジェクトを対象とする場合 — バックアップストリーム ID。バックアップされたデータベース項目/アプリケーション項目を示します。
- 説明:ファイルシステムオブジェクトを対象とする場合 — 同一のクライアント名とマウントポイントを持つオブジェクトを一意に定義します。統合オブジェクトを対象とする場合 — 統合の種類を表示します (例: SAP または Lotus)。
- 種類:バックアップオブジェクトの種類。ファイルシステムオブジェクトを対象とする場合 — ファイルシステムの種類 (例: WinFS)。統合オブジェクトを対象とする場合 — 「Bar」

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とともにディスクアレイに接続されているシステム。ほとんどの場合、バックアップシステムはターゲットボリューム (複製) を作成するためにディスクアレイに接続されるほか、ターゲットボリューム (複製) のマウント処理に使用されます。
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 バックアップ対象のオブジェクトのリストに、使用するデバイスまたはドライブのセット、仕様に含まれているすべてのオブジェクトのバックアップオプション、およびバックアップを実行する曜日や時刻を加えたもの。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。
バックアップ仕様、フルバックアップ、および増分バックアップ 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
復元チェーン を参照。

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。たとえば、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、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デルタバックアップ 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] 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。(デフォルト)

[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) 特定のクラスター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/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。

パブリックフォルダストア
(Microsoft Exchange Server 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の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。

ひ

表領域
データベース構造の一部。各データベースは論理的に 1 つまたは複数の表領域に分割されます。各表領域には、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。

ふ

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。Microsoft の用語では、オペレーティングシステムファイルが入っているボリューム/ディスク/パーティションをブートボリューム/ブートディスク/ブートパーティションと呼んでいます。

ファーストレベルミラー
(HP P9000 XP ディスクアレイファミリ固有の用語) HP P9000 XP ディスクアレイファミリのディスクアレイの内部ディスク (LDEV) のミラーで、このミラーをさらにミラー化し、セカンドレベルのミラーを作成できます。Data Protector ゼロダウンタイムバックアップおよびインスタントリカバリ目的には、ファーストレベルミラーのみを使用できます。
プライマリボリュームおよびミラーユニット (MU) 番号 も参照。

ファイバーチャネル ファイバーチャネルは、高速のコンピュータ相互接続に関する 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。ファイバーチャネルは、ノード間を 3 種類の物理トポロジー (ポイントツーポイント、ループ、スイッチ式) で接続できます。

ファイバーチャネルブリッジ ファイバーチャネルブリッジ (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 デバイスをファイバーチャネル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。

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。

ファイルツリーウォーク **(Windows 固有の用語)** どのオブジェクトが作成、変更、または削除されたかを判断するためにファイルシステムを巡回する処理。

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、任意のサーバーから複製作業を実行することもできます。

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。

フェイルオーバー あるクラスターノードから別のクラスターノードに最も重要なクラスターデータ (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。フェイルオーバーは、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。

フェイルオーバー **(HP P6000 EVA ディスクアレイファミリ固有の用語)** HP Continuous Access + Business Copy (CA+BC) P6000 EVA 構成でソースとあて先の役割を逆にする操作。
HP Continuous Access + Business Copy (CA+BC) P6000 EVA も参照。

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、場所) は、IDB および該当するメディア (メディアヘッダ) に保存されます。Data Protector のメディアは、保護の期限が切れるか、またはメディアの保護が解除されるかメディアがリサイクルされるまで、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、指定した順に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。

復元チェーン 特定の時点までのバックアップオブジェクトの復元に必要なバックアップすべて。復元チェーンは、オブジェクトのフルバックアップ 1 つと、任意の数の増分バックアップで構成されます。

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または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 (スプリットミラーやスナップクローンなど) 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。基本的なオペレーティングシステムの観点からすると、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ーを使用するときは、バックアップオブジェクトを含むボリュームまたはディスクグループ全体が複製されます。Windows でパーティションを使用する場合、選択したパーティションを含む物理ボリューム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。

複製セットのローテーション **(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。

プライマリボリューム (P-VOL) **(HP P9000 XP ディスクアレイファミリ固有の用語)** HP P9000 XP ディスクアレイファミリのディスクアレイの内部ディスク (LDEV) で、これに対して、そのミラー、またはスナップショットストレージに使用されるボリュームのいずれかのセカンダリボリューム (S-VOL) が存在します。HP CA P9000 XP および HP CA+BC P9000 XP 構成では、プライマリボリュームはメインコントロールユニット (MCU) 内に配置されています。
セカンダリボリューム (S-VOL) およびメインコントロールユニット (MCU) も参照。

フラッシュリカバリ領域 **(Oracle 固有の用語)** Oracle によって管理されるディレクトリ、ファイルシステム、または自動ストレージ管理 (ASM) ディスクグループであり、バックアップ、復元、およびデータベース復旧に関係するファイル (リカバリファイル) 用の集中管理ストレージ領域として機能します。
リカバリファイル 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 ZDB 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。前回のバックアップから変更がない場合でも、選択したすべてのオブジェクトがテープにストリーミングされます。
増分 ZDB も参照。

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 P9000 XP ディスクアレイファミリ固有の用語)** HP P9000 XP ディスクアレイファミリのディスクアレイのディスクペア (セカンダリボリュームとそれに対応するプライマリボリューム) の状態。状況によってペアのディスクはさまざまな状態になる可能性があります。Data Protector HP P9000 XP Agent の操作において特に以下の状態が重要となります。

- ペア – セカンダリボリュームがゼロダウンタイムバックアップ用に準備されています。セカンダリボリュームがミラーの場合、完全に同期化されます。セカンダリボリュームがスナップショットストレージ用に使用されるボリュームの場合、空の状態です。

- 中断 – ディスク間のリンクは中断されています。ただし、ペアの関係は維持されたままとなり、後で再度ゼロダウンタイムバックアップを行うためにセカンダリディスクを準備できます。
- コピー – ディスクペアは現在使用中であり、ペア状態に移行中です。セカンダリボリュームがミラーの場合、プライマリボリュームで再同期されています。セカンダリボリュームがスナップショットストレージに使用されるボリュームの場合、その内容はクリアされています。

並行復元 単一の Media Agent からデータを受信する Disk Agent を複数実行して、バックアップされたデータを同時に複数のディスクに (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。

並列処理 1 つの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。

変更ジャーナル **(Windows 固有の用語)** ローカル NTFS ボリューム上のファイルやディレクトリへの変更が発生するたび、それに関するレコードをログに記録する Windows ファイルシステム機能。

ほ

保護 データ保護およびカタログ保護 を参照。

補助ディスク 必要最小限のオペレーティングシステムファイル、ネットワークファイル、および Data Protector Disk Agent がインストールされたブート可能ディスク。ディスクデリバリーで UNIX クライアントを障害から復旧するときのフェーズ 1 では、補助ディスクをターゲットシステムのブートに使用することができます。

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ディザスタリカバリに使用される稼動中の Data Protector クライアント。

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。

ボリュームシャドウコピーサービス Microsoft ボリュームシャドウコピーサービス (VSS) を参照。

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)。

ま

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。

マルチスナップ **(HP P6000 EVA ディスクアレイファミリ固有の用語)** 個々のターゲットボリュームだけでなく、スナップショットを構成するすべてのボリュームでバックアップデータの整合性が取れるように、複数のターゲットボリュームを同時に作成すること。
スナップショット も参照。

み

ミラー (EMC Symmetrix および HP P9000 XP ディスクアレイファミリ固有の用語) ターゲットボリューム を参照。

ミラークローン **(HP P6000 EVA ディスクアレイファミリ固有の用語)** ストレージボリュームの動的な複製です。元のストレージボリュームに加えられた変更は、ローカル複製リンクを介して、ミラークローンに反映されます。元のストレージボリュームとそのミラークローン間の複製は中断できます。各ストレージボリュームについてディスクアレイ上に 1 つのミラークローンを作成できます。

ミラーユニット (MU) 番号 **(HP P9000 XP ディスクアレイファミリ固有の用語)** HP P9000 XP ディスクアレイファミリのディスクアレイ上にある内部ディスク (LDEV) のセカンダリボリューム (S-VOL) を特定する 0 以上の整数。
ファーストレベルミラー も参照。

ミラーローテーション (HP P9000 XP ディスクアレイファミリ固有の用語) 複製セットローテーション を参照。

む

無人操作 夜間処理 を参照。

め

メインコントロールユニット (MCU) **(HP P9000 XP ディスクアレイファミリ固有の用語)** HP CA P9000 XP または HP CA+BC P9000 XP 構成のプライマリボリューム (P-VOL) を含み、マスターデバイスとして機能する HP P9000 XP ディスクアレイファミリのユニット。
HP Business Copy (BC) P9000 XP、HP Continuous Access (CA) P9000 XP、および LDEV も参照。

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 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 メディアの使用法は、既に使用されているメディアに対してバックアップをどのように追加するかを制御します。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。

メディア割り当てポリシー メディアをバックアップに使用する順序を決定します。[厳格] 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。[緩和] 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。

や

夜間処理または無人操作 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。

ゆ

ユーザーアカウント (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。

ユーザーアカウント制御 (UAC) Windows Vista、Windows 7 および Windows Server 2008 のセキュリティコンポーネント。管理者が権限レベルを上げるまで、アプリケーションソフトウェアを標準のユーザー権限に限定します。

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ユーザー権限のセットがあり、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、デフォルトで admin、operator、user という 3 つのユーザーグループが用意されています。

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 の容量管理サポートを使用すると、共有ストレージボリュームに対して、拡張された追跡メカニズムの使用およびディスク容量に対する制御が行えるようになります。Data Protector では、システム全体にわたるユーザーディスク割り当てが、すべてのユーザーに対して一度にバックアップされます。

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。

ら

ライター **(Microsoft 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。

り

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アーカイブログの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でなければならないことに注意してください。

リカバリファイル **(Oracle 固有の用語)** リカバリファイルはフラッシュリカバリ領域に存在する Oracle 固有のファイルで、現在の制御ファイル、オンライン REDO ログ、アーカイブ REDO ログ、フラッシュバックログ、制御ファイル自動バックアップ、データファイルコピー、およびバックアップピースがこれにあたります。
フラッシュリカバリ領域 も参照。

リサイクルまたは保護解除 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。

ろ

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、ディザスタリカバリプロセスがローカルモードにフェイ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に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。

ローカル連続レプリケーション **(Microsoft Exchange Server 固有の用語)** ローカル連続レプリケーション (LCR) はストレージグループの完全コピー (LCR コピー) を作成および維持するシングルサーバー ソリューション。LCR コピーは元のストレージグループと同じサーバーに配置されます。LCR コピーが作成されると、変更伝播 (ログリプレイ) テクノロジで最新に保たれます。LCR の複製機能では未複製のログが削除されません。この動作の影響により、ログを削除するモードでバックアップを実行しても、コピー中のログと複製に十分な余裕がある場合、実際にはディスクの空き容量が解放されない場合があります。

LCR コピーへの切り替えは数秒で完了するため、LCR コピーはディザスタリカバリに使用されます。元のデータとは異なるディスクに存在する LCR コピーをバックアップに使用すると、プロダクションデータベースの入出力の負荷が最小になります。

複製されたストレージグループは、Exchange ライターの新しいインスタンス (Exchange Replication Service) として表示され、通常のストレージグループのように VSS を使用してバックアップできます。

クラスター連続レプリケーションおよび Exchange Replication Service も参照。

ロギングレベル ロギングレベルは、バックアップ、オブジェクトのコピー、またはオブジェクトの集約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 [記録しない] の 4 つのロギングレベルがあります。ロギングレベル設定によって、IDB のサイズ増加、バックアップ速度、および復元データのブラウザのしやすさが影響を受けます。

ログイン ID **(Microsoft SQL Server 固有の用語)**Microsoft SQL Server にログインするためにユーザーが使用する名前。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。

論理演算子 Data Protector 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。たとえば、「マニュアル ディザスタ リカバリ」という検索条件は、「マニュアル AND ディザスタ AND リカバリ」と同じ結果になります。

論理ログファイル 論理ログファイルは、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。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。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。

わ

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。

索引

し

す

せ