HP Data Protector A.06.10
コンセプトガイド

製品番号： B6960-96057
初版： 2008年11月

ご注意

本書で取り扱っているコンピュータ ソフトウェアは秘密情報であり、 その保有、使用、または複製には、Hewlett-Packard Companyから使用許諾を得る必要があります。 米国政府の連邦調達規則であるFAR 12.211および12.212の規定に従って、コマーシャル コンピュータ ソフトウェア、コンピュータ ソフトウェア ドキュメンテーションおよびコマーシャル アイテムのテクニカル データ（Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items）は、ベンダが提供する標準使用許諾規定に基づいて米国政府に使用許諾が付与されます。

本書に記載されている内容は事前の通知なしに変更されることがあります。 HP製品およびサービスに対する保証は、当該製品およびサービスに付属の明示的保証規定に記載されているものに限られます。ここに記載の何ものも、追加保証を構成すると解釈されるものではありません。 本書の内容につきましては万全を期しておりますが、本書の技術的あるいは校正上の誤り、省略に対しては責任を負いかねますのでご了承ください。

Printed in the US

目次

図目次

表目次

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	出版年月	製品
B6960-99080	2003年5月	Data Protector リリース A.05.10
B6960-99105	2004年10月	Data Protector リリース A.05.50
B6960-96026	2006年8月	Data Protector リリース A.06.00
B6960-96057	2008年11月	Data Protector リリース A.06.10

本書について

このガイドでは、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、このマニュアルをお読みください。

対象読者

このガイドは、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。 必要な詳細レベルによって、Data Protectorのオンライン ヘルプとともにこのマニュアルも使用することができます。

ドキュメント セット

その他のドキュメントおよびオンライン ヘルプでは、関連情報が提供されます。

ガイド

Data Protectorのガイドは、印刷された形式あるいはPDF形式で利用できます。PDFファイルは、Data Protectorのセットアップ時に、Windowsの場合はEnglish documentation and Help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。 インストールすると、このガイドはWindowsの場合は*Data_Protector_home*\docsディレクトリ、UNIXの場合は/opt/omni/doc/C/ディレクトリに保存されます。

これらの資料は、HP Business Support CenterのWebサイトの[Manuals]ページから入手できます。

http://www.hp.com/support/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。手順を中心に説明しているオンライン ヘルプとあわせてお読みください。
- 『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 リカバリのプランニング、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』
  このマニュアルでは、さまざまなデータベースやアプリケーションをバックアップ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。 このマニュアルは、バックアップ管理者やオペレータを対象としています。4種類のガイドがあります。
  - 『HP Data Protector Microsoft アプリケーション用インテグレーションガイド： SQL Server、SharePoint Portal Server、Exchange Server、および Volume Shadow Copy Service』
    このガイドでは、Microsoft Exchange Server、Microsoft SQL Server、Volume Shadow Copy Service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、SAP R3、SAP DB/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 integration guide for IBM applications： Informix, DB2, and Lotus Notes/Domino』
    このガイドでは、Informix Server、IBM DB2、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 integration guide for VMware Virtual Infrastructure, Sybase, Network Node Manager, and Network Data Management Protocol Server』
    このガイドでは、VMware Virtual Infrastructure、Sybase、Network Node Manager、および Network Data Management Protocol Server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 integration guide for HP Service Information Portal』
  このガイドでは、HP Service Information Portalに対応するData Protector統合ソフトウェアのインストール、構成、使用方法について説明します。 これはバックアップ管理者用です。 ここでは、アプリケーションを使用して Data Protector サービスを管理する方法について説明しています。
- 『HP Data Protector integration guide for HP Reporter』
  このマニュアルでは、HP Reporter に対応する Data Protector 統合ソフトウェアのインストール、構成、使用方法について説明します。これはバックアップ管理者用です。 Data Protector のサービス管理にアプリケーションを使用する方法について説明します。
- 『HP Data Protector integration guide for HP Operations Manager for UNIX』
  このガイドでは、UNIX 版の HP Operations Manager software 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 software 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 Performance Manager and HP Performance Agent』
  このマニュアルでは、Windows 版、HP-UX 版、Solaris 版、Linux 版のHP Performance Manager (PM) および HP Performance Agent (PA) 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 zero downtime backup administrator's guide』および『HP Data Protector zero downtime backup integration guide』とあわせてお読みください。
- 『HP Data Protector zero downtime backup administrator's guide』
  このガイドでは、HP StorageWorks Virtual Array、HP StorageWorks Enterprise Virtual Array、EMC Symmetrix Remote Data FacilityおよびTimeFinder、HP StorageWorks Disk Array XPに対応するData Protector統合ソフトウェアのインストール、構成、使用方法について説明します。 このマニュアルは、バックアップ管理者やオペレータを対象としています。ファイルシステムやディスク イメージのゼロ ダウンタイム バックアップ、インスタント リカバリ、および復元についても説明します。
- 『HP Data Protector zero downtime backup integration guide』
  このガイドでは、Oracle、SAP R/3、Microsoft Exchange Server 2000/2003、およびMicrosoft SQL Server 2000データベースのゼロ ダウンタイム バックアップ、インスタント リカバリ、および標準復元を行うための、Data Protectorの構成方法および使用法について説明します。また、Microsoft Volume Shadow Copy Serviceを使用してバックアップ、および復元を実行するためのData Protectorの構成方法および使用方法についても説明します。
- HP Data Protector MPE/iX system user guide
  このマニュアルでは、MPE/iXクライアントの構成方法、およびMPE/iXデータのバックアップおよび復元方法を説明します。
- HP Data Protector『Media Operations user guide』
  このガイドでは、オフライン ストレージ メディアのトラッキングと管理について説明します。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 product announcements 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 A.06.10の新機能について説明しています。また、サポートされている構成(デバイス、プラットフォームおよびオンライン データベースの統合ソフトウェア、SAN、ZDB)、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。 サポートされている構成の更新バージョンは、http://www.hp.com/support/manualsにあります。

- 『HP Data Protector product announcements ソフトウェアノートおよびリファレンス for integrations to HP Operations Manager, HP Reporter, HP Performance Manager, HP Performance Agent, and HP Service Information Portal』
  このガイドは、記載されている統合ソフトウェアに対して同様の役割を果たします。
- 『HP Data Protector Media Operations Product Announcements, Software Notes, and references』
  このガイドは、Media Operationsに対して同様の役割を果たします。

オンライン ヘルプ

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

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

- ***Windows の場合***:ZipファイルDP_help.zipを解凍し、DP_help.chmを開きます。
- ***UNIX 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でオンライン 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

以下の表は、ドキュメントマップに使用されている略称の説明です。 ガイドのタイトルには、すべて先頭に「"HP Data Protector"」が付きます。

略称	ガイド
CLI	コマンド行インタフェース リファレンス
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
Help	オンライン ヘルプ
IG-IBM	IBMアプリケーション用インテグレーションガイド
IG-MS	Microsoftアプリケーション用インテグレーションガイド
IG-O/S	インテグレーション ガイド — Oracle、SAP R/3、SAP DB/MaxDB
IG-OMU	インテグレーション ガイド — HP Operations Manager software、UNIX
IG-OMW	インテグレーション ガイド — HP Operations Manager software、Windows
IG-PM/PA	インテグレーション ガイド — Performance ManagerおよびHP Performance Agent
IG-Report	インテグレーションガイド — HP Reporter
IG-SIP	インテグレーションガイド — HP Service Information Portal
IG-Var	インテグレーションガイド — VMware、Sybase、Network Node Manager、およびNDMP Server
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 RN	Media Operations Product Announcements, Software Notes, and References
MO UG	Media Operations User Guide
MPE/iX	MPE/iX System User Guide
PA	製品に関するお知らせ、ソフトウェア使用上の注意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 Administrator's Guide
ZDB Concept	ゼロダウンタイム バックアップ コンセプトガイド
ZDB IG	ZDB Integration Guide

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。黒く塗りつぶされたセルの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			MO			MPE/iX	CLI
								MS	O/S	IBM	Var	SIP	Report	OMU	OMW	Concept	Admin	IG	GS	User	PA		
バックアップ	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	
障害復旧	X		X			X																	
インストール / アップグレード	X	X		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		
新機能	X						X																
プランニング方法	X		X									X				X							
手順 / 作業	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		
復元	X	X	X					X	X	X	X						X	X				X	
サポート一覧							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					

統合

以下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。

統合	ガイド
HP Operations Manager software for UNIX/for Windows	IG-OMU、IG-OMW
HP Performance Manager	IG-PM/PA
HP Performance Agent	IG-PM/PA
HP Reporter	IG-R
HP Service Information Portal	IG-SIP
HP StorageWorks Disk Array XP	すべてのZDB
HP StorageWorks Enterprise Virtual Array (EVA)	すべてのZDB
HP StorageWorks Virtual Array (VA)	すべてのZDB
IBM DB2 UDB	IG-IBM
Informix	IG-IBM
Lotus Notes/Domino	IG-IBM
Media Operations	MO User
MPE/iX System	MPE/iX
Microsoft Exchange Server	IG-MS、ZDB IG
Microsoft Exchange Single Mailbox	IG-MS
Microsoft SQL Server	IG-MS、ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	IG-MS、ZDB IG
NDMP Server	IG-Var
Network Node Manager (NNM)	IG-Var
Oracle	IG-O/S
Oracle ZDB	ZDB IG
SAP DB	IG-O/S
SAP R/3	IG-O/S、ZDB IG
Sybase	IG-Var
Symmetrix (EMC)	すべてのZDB
VMware	IG-Var

表記上の規則および記号

表 2 表記上の規則

表記	要素
ミディアム ブルーのテキスト： 表 2 (26 ページ)	クロスリファレンス リンクおよびEメール アドレス
青色の下線付き語句： http://www.hp.com	Webサイト アドレス
斜体 テキスト	テキストの強調
固定スペース テキスト	▪ ファイルおよびディレクトリの名前 ▪ システム出力 ▪ コード ▪ コマンド、その引数、および引数の値
固定スペース、斜体 テキスト	▪ コード変数 ▪ コマンド変数
テキスト	強調された固定スペースのテキスト

△ **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、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、オンライン ヘルプを参照してください。

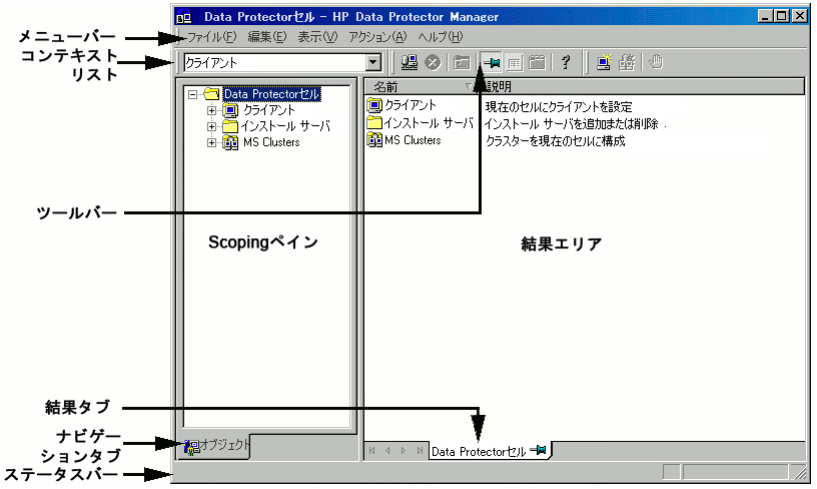

図 1 Data Protectorグラフィカル ユーザー インタフェース

一般情報

Data Protectorの概要については、以下のWebサイトでご覧いただけます。
http://www.hp.com/go/dataprotector.

HPテクニカル サポート

この製品のテクニカルサポートについては、次のHPサポートのWebサイトに記載されています。

http://www.hp.com/support

HPにお問い合わせになる前に、次の情報を収集してください。

- 製品のモデル名とモデル番号
- テクニカル サポートの登録番号（該当する場合）
- 製品シリアル番号
- エラー メッセージ

- オペレーティング システムの種類とリビジョン レベル
- 質問の詳細

製品サービスへの登録

下記のSubscriber's Choice for BusinessのWebサイトに製品を登録することをお勧めします。

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

登録を済ませると、製品のアップグレード、ドライバの新しいバージョン、ファームウェア アップデートなどの製品リソースに関する通知を電子メールで受け取ることができます。

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://www.hp.com/service_locator
- http://www.hp.com/support/manuals
- http://www.hp.com/support/downloads

ご意見、ご感想

HPでは、お客様からのフィードバックを歓迎いたします。

製品ドキュメントについてのご意見、ご感想は、次のアドレスに電子メールでご送信ください。 DP.DocFeedback@hp.com.ご送信いただいた内容は、HPに帰属します。

1 バックアップとData Protector

この章の内容

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

この章の構成は以下のとおりです。

Data Protectorについて

HP 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。 さらに中心となる1つのシステムから、複数のバックアップ環境を管理することも可能です。 また、Data Protectorにはコマンド行インタフェースも用意されているので、スクリプトを使用してData Protectorを管理することもできます。
- **優れたバックアップ性能**
  Data Protectorを使用すると、数百ものバックアップ デバイスに同時にバックアップすることができます。 また、大容量ライブラリ内のハイエンド デバイスもサポートされます。 さらに、ローカル バックアップ、ネットワーク バックアップ、オンライン バックアップ、ディスク イメージ バックアップ、合成バックアップ、オブジェクト ミラーリングを伴うバックアップ、並列データ ストリームの組み込みサポートなど、多様なバックアップがサポートされるため、ユーザー要件に最適なバックアップを実行できます。
- **データセキュリティ**
  データのセキュリティを強化するため、Data Protectorではバックアップを暗号化して、他から保護します。Data Protectorには、ソフトウェアベースとドライブベースの2つの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とWindowsのCell Managerからは、サポート対象のクライアント プラットフォームのすべて(UNIX、Windows、およびNovell NetWare)を制御できます。 Data Protector ユーザー インタフェースを使用すると、各サポート対象プラットフォーム上のすべてのData Protector機能にアクセスできます。
- **混合環境におけるインストールの容易性**
  Installation Server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Installation Server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Installation Server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。 Installation Server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 product announcements 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。
  - クラスタとの統合によりフェイルセーフ オペレーションを確実に実行し、仮想ノードのバックアップにも対応。 サポート対象クラスタの一覧は、

『HP Data Protector product announcements 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。

- クラスタ上でData Protector Cell Manager自体の実行が可能。
- 一般に使用されている、すべてのオンライン データベースのアプリケーション プログラミング インタフェース(API)をサポート。
- EMC Symmetrix、HP StorageWorks Disk Array XP、HP StorageWorks Virtual Array、HP StorageWorks Enterprise Virtual Arrayなどの、高度な高可用性ソリューションとの統合が可能。
- WindowsおよびUNIXの各プラットフォーム上で、さまざまなディザスタ 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。

- **復元の容易性**
  Data Protectorでは、どのシステムのどのファイルが、どのメディア上に保存されているかをトラッキングするための内部データベースが用意されています。 システム上の任意の部分を復元する場合、目的のファイルやディレクトリを簡単に一覧することができます。 その結果、復元するデータにすばやく簡単にアクセスできます。
- **自動または無人処理**
  Data Protectorでは、内部データベースを使用して、Data Protectorメディアに関する情報と、それぞれのメディア上に保存されているデータに関する情報を管理しています。Data Protectorには高度なメディア管理機能が備わっています。 例えば、あるバックアップ データをいつまで復元可能な状態で保持する必要があるかといった点や、どのメディアがバックアップ用として(再)利用可能かといった点をトラッキングしています。
  また、大容量ライブラリをサポートしているため、数日間あるいは数週間にわたって、オペレータが介入しない状態で処理を継続することも可能です(自動メディア交換)。 さらに、Data Protectorでは、新しいディスクがシステムに接続された場合、自動的にそのディスクを検出して(ディスク ディスカバリ)、バックアップすることもできます。 この機能を使用すると、バックアップ構成情報を手動で調整する必要がなくなります。
- **サービス管理**
  Data Protectorは、バックアップ管理と復元管理のためのソリューションとしては初めてサービス管理機能をサポートしました。 Application Response Management (ARM)、およびData Source Integration (DSI)の統合により、システムの管理および設計に必要なデータが提供されるため、サービスレベル管理(SLM)およびサービスレベル契約(SLA)の概念が強力にサポートされます。
  このDSIの統合により、スクリプトおよび構成ファイルのセットが提供されるため、ユーザーはData Protectorのレポート機能を使用して、レポートの仕様を追加する場合の指定方法を調べることができます。
- **モニタリング、レポート、および通知機能**
  Webを使用する優れたレポート機能および通知機能が用意されているため、バックアップ状態のチェックや、活動中のバックアップ動作のモニタリング、レポートのカスタマイズなどを簡単に実行できます。 レポートは、Data Protector

GUIを使用して作成したり、UNIXまたはWindowsを実行しているシステム上でomnirptコマンドを使用して生成したりすることもできます。 さらに、Javaベースのオンライン生成Webレポートを使用することもできます。
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。バックアップ セッションの情報は、監査ログ ファイルに記録されます。

- **オンライン データベース アプリケーションとの統合**
  Data Protectorは、Microsoft Exchange Server、Microsoft SQL Server、Oracle、Informix Server、SAP R/3、Lotus Notes/Domino Server、IBM DB2 UDB、Sybaseのデータベース オブジェクト、およびVMware Virtual Infrastructure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 product announcements 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://www.hp.com/support/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。 作成したコピーは、オリジナル データの破壊や破損に備えて保管しておきます。

バックアップを最も抽象化すると、図 2（32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。

ダイレクト バックアップ

ダイレクト バックアップとは、データを移動するための専用のバックアップ サーバを使用せずに、SAN環境でディスクからテープにデータを直接送信するバックアップ方法です。

ファイルシステムに依存しないデータ解決機能の使用は、サポート対象のディスク アレイやブリッジに組み込まれている業界標準のXCOPY 機能と完全に統合されているため、データ ムーバ装置を別途用意する必要はありません。

Data Protectorアーキテクチャ

Data Protectorでは、 **セル**(図 5 (35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。

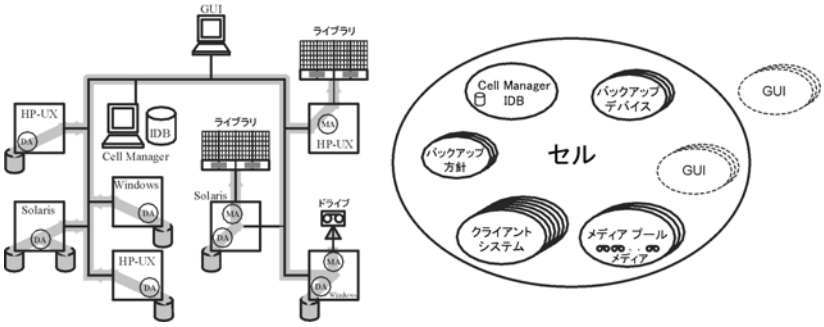

図 5 Data Protectorセル（物理的な構成図と論理的な構成図）

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 product announcements 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。
- Session Manager を実行します。このSession Managerは、バックアップ セッションや復元セッションの開始および停止を行うほか、セッションに関する情報をIDBに書き込む働きをします。

バックアップ対象システム

[クライアントシステム] ファイル システムのバックアップ元となるクライアント システムには、Data Protectorの Disk Agent (DA)をインストールする必要があります。Disk AgentはBackup Agentとも呼ばれます。 また、オンライン データベース統合をバックアップするには、Application Agentをインストールしてください。 以降の説明では、両方のエージェントを指して、Disk Agentと呼んでいます。 Disk Agentは、システム上のディスクからデータを読み取ってMedia Agentに渡したり、Media Agentから受け取ったデータをディスクに書き込んだりする働きをします。 また、Disk AgentをCell Manager上にもインストールすることで、Cell Manager上のデータや、Data Protectorの構成情報、IDBなどのバックアップも可能になります。

バックアップ デバイスを接続したシステム

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

ユーザー インタフェースをインストールしたシステム

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

Installation Server

Installation Serverでは、 特定アーキテクチャ用のData Protectorソフトウェア パッケージのレポジトリが保持されています。 デフォルトでは、Cell Managerが同時にInstallation Serverになります。 混在環境では、少なくとも2台のInstallation Server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

図 6（37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。

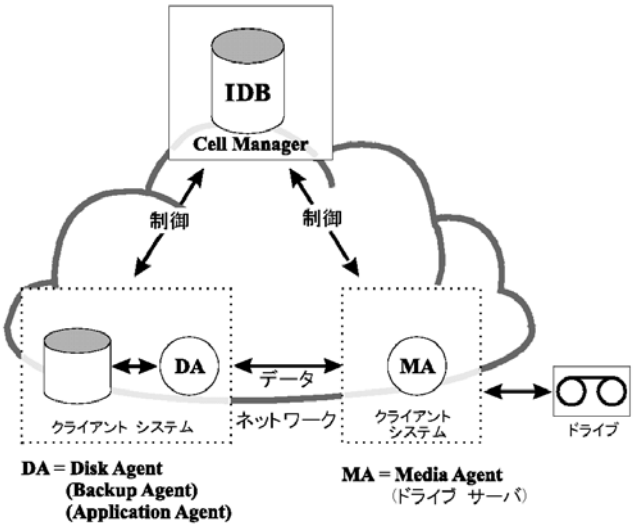

図 6 バックアップ処理および復元処理

バックアップ セッション

バックアップ セッションとは

図 7 (38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。

復元の仕組み

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

図 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、図 7（38ページ）に示したよりも複雑なものになります。 通常は複数のDisk Agentによって複数のディスクから並列にデータが読み取られ、1つまたは複数のMedia Agentにそのデータが渡されます。 複雑なバックアップ セッションの詳細は、第7章（207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

図 8（38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。

復元の仕組み

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

図 8 復元セッション

通常の復元セッションは、図 8（38ページ）に示したよりも複雑なものになります。復元セッションの詳細は、第7章（207ページ）を参照してください。

企業環境

企業環境とは

図 9（39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

このマニュアル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。

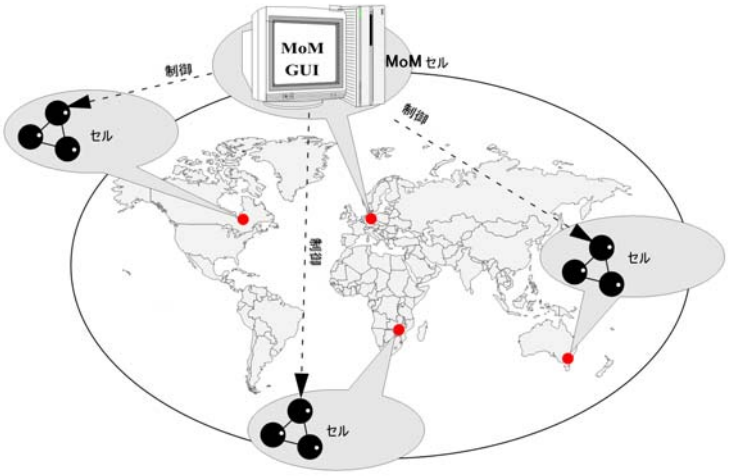

図 9 世界規模のData Protector企業環境

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 （40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

環境構築時の注意点については、第2章 (51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。

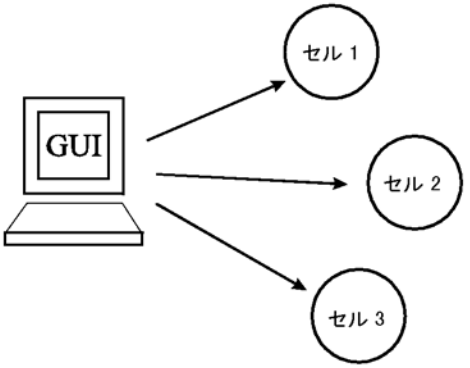

図 10 複数セルを一元管理

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(図 10 (40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。

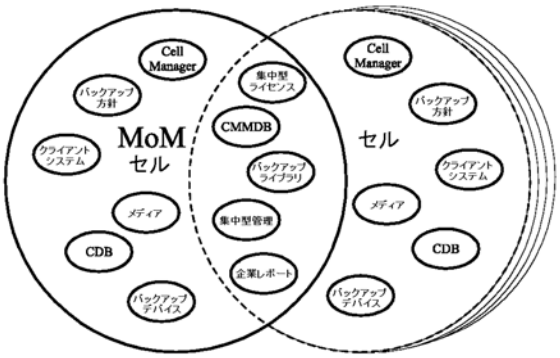

図 11 Manager-of-Managers環境

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。
- **CMMDB (Centralized Media Management Database: 集中型メディア管理データベース)**
  CMMDBを使うと、1つのMoM環境に含まれる複数のセル間で、デバイスとメディアを共有できます。 つまり、CMMDBを使っているあるセル内のデバイスに、同じCMMDBを使っている別のセルからアクセスできます。 CMMDBを使う場合は、このデータベースをMoMセル内に配置しなければなりません。 またMoMセルとその他のData Protectorセルとの間に、信頼性の高いネットワーク接続が必要になります。 CMMDBは、メディア管理データベースを一元管理するための任意選択の機能である点に注意してください。
- **ライブラリの共有**
  CMMDBを使用すると、1つの環境内の複数セル間で、ハイエンド デバイスを共有できます。 そのため、例えばあるセルから、別のセル内のシステムに接続された複数デバイスを制御できるロボティクスを使用することも可能です。 Disk AgentからMedia Agentへのデータ パスも、セルの境界に制約されません。
- **企業レポート**
  Data ProtectorのManager-of-Managersを使用すると、セル単位のレポートだけでなく、全社レベルのレポートも生成できます。

メディア管理

Data Protectorには強力なメディア管理機能が備わっており、次に示すような方法で、それぞれの環境内にある多数のメディアを簡単に効率よく管理できます。

メディア管理機能

- 個々のメディアは、**メディア プール**と呼ばれる論理グループにまとめることができます。 そのため各メディアを個別に取り扱うのではなく、大容量のメディア セットとしてまとめて管理できます。
- Data Protectorでは、個々のメディアと、そのメディアの状態がすべてトラッキングされています(データ保護の有効期限、バックアップ時にそのメディアを使用できるかどうか、各メディアにバックアップされている情報に関するカタログ情報など)。
- 完全な自動処理が可能です。 Data Protectorでは、ライブラリ デバイス内に十分なメディアを用意しておくと、メディア管理機能により、オペレータによる介入操作を必要とせずにバックアップ セッションを自動実行できます。
- メディアの自動交換方針を設定しておくと、バックアップ用のメディア交換を手動で行う必要がなくなります。
- バーコードを使用する大容量のライブラリ デバイスおよびサイロ デバイスで使われるバーコードの認識およびサポートが可能です。
- 大容量ライブラリ デバイスおよびサイロ デバイス内に存在する、Data Protectorが使用する全メディアに対する認識、トラッキング、ブラウズ、および操作が可能です。
- メディアに関する情報を中央で一元管理し、複数のData Protectorセル間でこの情報を共有できます。
- メディアのデータの追加コピーを対話的または自動的に作成します。
- 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。

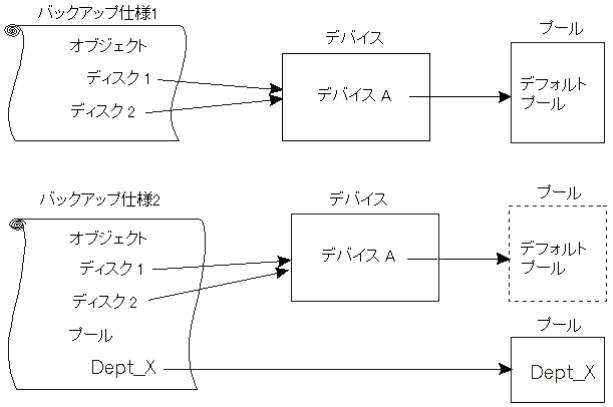

図 12 バックアップ仕様、デバイス、およびメディア プールの関連

図 12（43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、バックアップ仕様内でこのメディア プールを変更することも可能です。 例えば上図のバックアップ仕様2は、デフォルト プールではなくDept_Xプールを参照しています。

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

ユーザー インターフェース

Data Protectorでは、Windows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、コマンド行インタフェースは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。 図 13（44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。

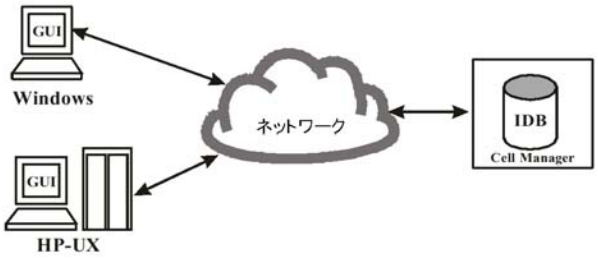

図 13 Data Protectorユーザー インターフェースの使用

ヒント：

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

Data Protector GUI

図 14（45ページ）に示すオリジナルのData Protector GUIおよび図 15（45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 トピックと呼ばれる包括的なオンライン ヘルプ システムおよびヘルプ ナビゲータと呼ばれる、状況依存のヘルプが用意されています。

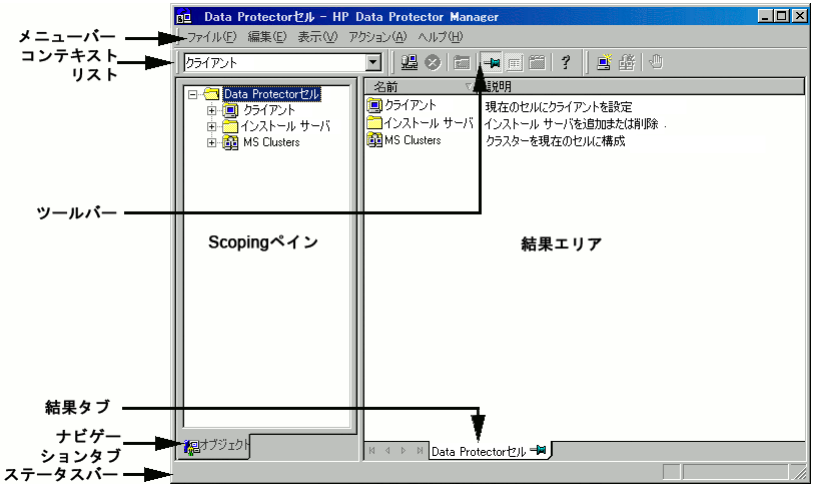

図 14 オリジナルのData Protector GUI

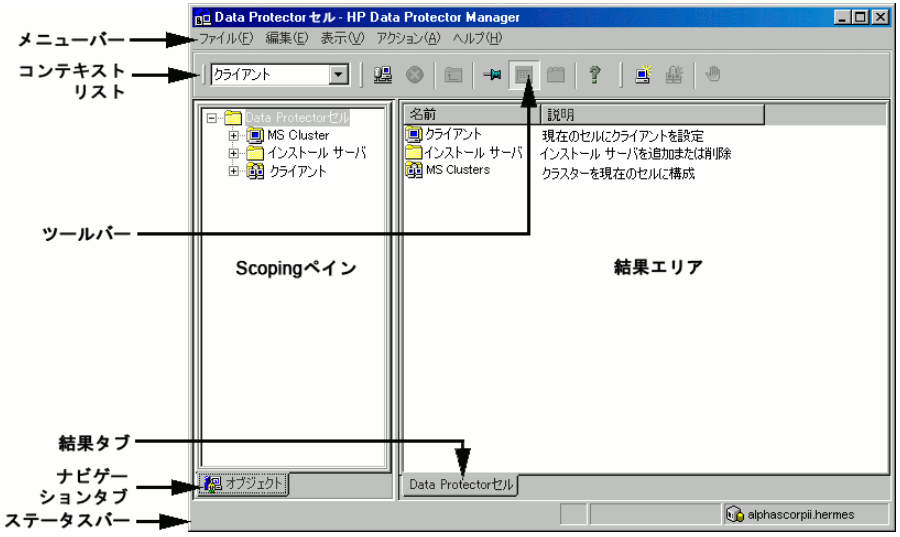

図 15 Data Protector Java GUI

Data Protector Java GUI

Data Protector Java GUIは、クライアントサーバ アーキテクチャを使用したJavaベースのグラフィカル ユーザー インタフェースです。 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 ServerとJava GUI Clientの2つのコンポーネントで構成されています。 図 16（46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。

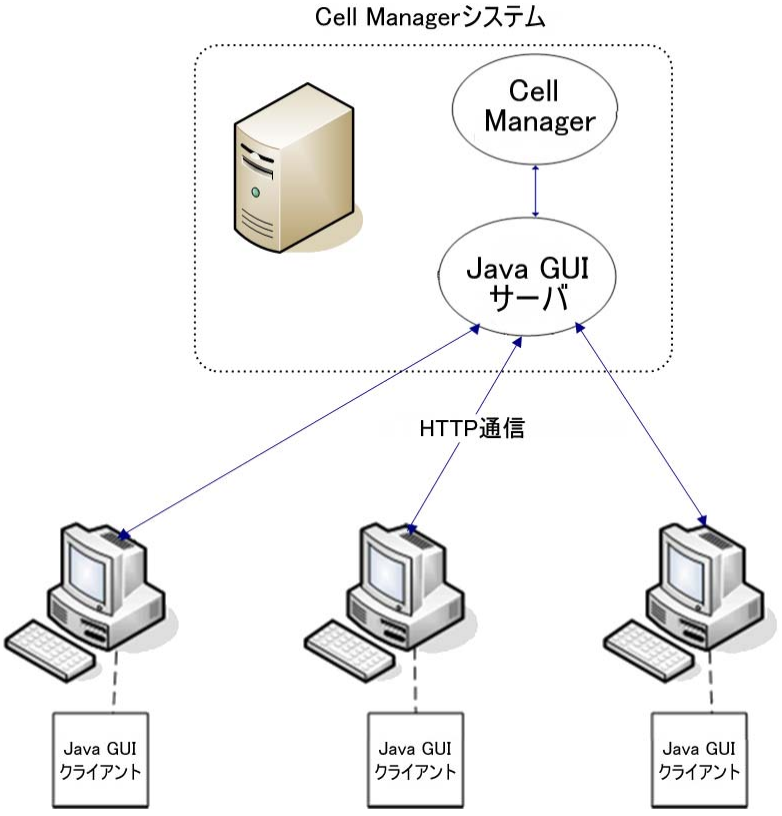

図 16 Data Protector Java GUIのアーキテクチャ

Java GUI Server は、Data Protector Cell Managerシステムにインストールします。Java GUI Serverは、Java GUI Clientからの要求を受け取って処理し、応答をJava GUI Clientに戻します。 通信は、ポート5556でHypertext Transfer Protocol (HTTP)を通して行われます。

Java GUI Client 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 Serverに接続しなければ動作しません。

Java GUIの利点

Data Protector Java GUIには、オリジナルのData Protector GUIに対して以下の利点があります。

- 移植性
  Data Protector Java GUIアーキテクチャでは、Java Runtime Environment (JRE)をサポートするすべてのプラットフォームにJava GUI Clientをインストールできます。
- ファイアウォールの構成が簡単
  Java GUI Clientはポート5556を使用してJava GUI Serverに接続します。 1つのポートしか開く必要がないので、ファイアウォール環境にJava GUIを簡単に構成できます。 Java GUI ClientとJava GUI Serverは、ファイアウォールとも相性の良いHTTPで通信します。
  詳細については、http://www.hp.com/support/manualsに示すData Protectorサポート一覧を参照してください。
- 優れたローカライズと各国語対応
  1つのインストール パッケージですべてのロケールに対応します。 Java GUIはテキストのサイズに合わせてコントロールの大きさが自動的に変わるので、いずれのロケールにも適した表示が可能です。
- 円滑な動作
  Java GUI Serverは現在のコンテキストのデータのみを転送するため、Java GUI ServerとJava GUI Client間のネットワーク トラフィックが軽減されます。作業が妨害されないため、Java GUI Serverがバックグラウンドで要求を処理中であっても別のコンテキストで作業できます。

オリジナルのData Protector GUIとの相違点

使用されている基盤技術が異なるため、2つのGUIの表示や細かい機能については相違点が複数あります。 これらの相違点は、Data Protectorの機能には大きな影響を与えません。

たとえば、**[クライアント]**コンテキストでクライアントのプロパティの**[保護]**タブを表示した場合、使用するGUIに応じてネットワーク参照の動作が異なります。

- オリジナルのData Protector GUI (Windowsシステムのみ)には、GUIクライアントの近くのコンピュータが表示されます。
- Data Protector Java GUIでは、近くのコンピュータにはCell Managerが表示され、GUIクライアントは表示されません。 参照は、Windows Cell Managerでのみ使用可能です。 ただし、WindowsシステムとUNIXシステムのどちらでGUIを実行しても、違いはありません。

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、必ずしも以下のすべての手順を実行する必要はありません。

1. ネットワーク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。
3. Data Protectorセルの構成について、以下のような点を決定します。
   - Cell Managerとなるシステム
   - ユーザー インタフェースをインストールするシステム
   - バックアップ方法(ローカル バックアップまたはネットワーク バックアップ)
   - バックアップ デバイスおよびライブラリを制御するシステム
   - 接続の種類(LANまたはSAN、あるいはその両方)
4. 決定したセットアップ方法に合わせて、必要なData Protectorライセンスを購入します。 ライセンスを購入すると、インストールに必要なパスワードを入手できます。

   別のやり方として、一時パスワードを使用してData Protectorを操作することも可能です。 ただし、このパスワードはインストール後60日間のみ有効です。 詳細は、『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. セキュリティ面を検討します。
   - セキュリティ上、注意すべき点を分析します。 『HP 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。
   - データをメディアに暗号化フォーマットで書き込むことにより、セキュリティを強化します。
6. バックアップ構造を決定します。
   - どのようなメディア プールを定義し、どのように使用するか。
   - どのデバイスをどのように使用するか?
   - 各バックアップデータのコピーはそれぞれいくつ必要か。
   - いくつのバックアップ仕様を作成し、どのようにグループ化するか。
   - 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。
   - バックアップの失敗への対処
   - 復元処理の実行
   - バックアップ データのコピーとメディアのボールティング
   - ディザスタリカバリの準備
   - IDBの保守

2 バックアップ方針の策定

この章の内容

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

この章の構成は以下のとおりです。

バックアップ方針の策定

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

バックアップ方針の策定とは

バックアップ方針の策定手順は、以下のとおりです。

1. データのバックアップ頻度や、バックアップ データを別のメディア セットに追加コピーする必要があるかどうかなど、バックアップに関する要件と制約事項を明らかにします。
2. ネットワークやバックアップ デバイスにおける定常データ転送速度など、バックアップ ソリューションに影響を与える要因を明らかにします。 これらの要因は、Data Protectorの構成方法や実行するバックアップの種類(ネットワーク経由のバックアップやダイレクト バックアップなど)の選択に影響する可能性があります。 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. バックアップ方針を構築する準備として、実行するバックアップの構想と、その実装方法を明らかにします。

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、このマニュアルの以降の部分では、バックアップ ソリューションの構築に役立つ重要な情報および注意点について説明しています。

バックアップ方針における要件の明確化

バックアップ方針の目的と制約事項を明らかにするため、以下の点を検討してください。

- 各自の**組織におけるバックアップと復元の方針**
  組織によっては、データの保管および保存に関する方針が既に確立されていることがあります。 新たに構築するバックアップ方針は、こうした方針に従ったものでなければなりません。
- バックアップするデータのタイプ
  ネットワーク内に存在するすべてのデータ タイプをリストアップします(ユーザー ファイル、システム ファイル、Webサーバ、大容量リレーショナル データベースなど)。
- 復旧までに許される最大ダウンタイム
  どれくらいのダウンタイムが許されるかは、バックアップ用のネットワーク基盤および装置に必要な予算に大きく影響します。 そのため各データ タイプについて、復旧までのダウンタイムが最大どれくらいまで許されるか、つまりバックアップ データから復元するまでの間、どれくらいの時間そのデータを使用できなくても構わないかを明らかにしておきます。 例えば、ユーザー ファイルは2日以内に復元できればよいが、大容量データベース内のビジネス データは2時間以内に復旧しなければならない、といった状況が考えられます。
  復旧までの時間は、主として、メディアにアクセスするための時間と、ディスク上に実際にデータを復元するための時間に分かれます。 完全なシステム復旧を行う場合は、より多くの手順が必要となるため、さらに多くの時間がかかります。 詳細については、「ディザスタ リカバリ」 (120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。 例えば、ユーザー ファイルは3週間だけ保管

すればよいが、従業員に関する情報は5年間保管するのが妥当である、といったことが考えられます。

- バックアップ データを保存したメディアの保管方法
  安全な外部の保管場所(ボールト)を使用するのであれば、各タイプのデータ毎に、そのデータを保存したメディアをどれくらいの期間、ボールトに保管するべきかを検討しておきます。 例えば、ユーザー ファイルをボールトに保存する必要はないが、発注情報は5年間保管しておき、2年後には各メディアを検証しなければならないといったことが考えられます。
- バックアップ時にデータを書き込むメディア セットの総数
  重要なデータは、バックアップ時に複数のメディア セットに書き込むことを検討してください。 これによりバックアップのフォールト トレランスが向上し、複数の場所に分けてのボールティングも可能になります。 ただし、オブジェクト ミラーリングを行うと、バックアップにかかる時間はそれだけ長くなります。
- バックアップするデータの総量
  各データ タイプごとに、データ総量を見積もっておきます。 データ総量は、バックアップに要する時間に大きく影響します。 またデータ総量の見積もりは、バックアップに必要なデバイスおよびメディアを選択するうえでも重要です。
- データ総量の将来における増加率
  各データ タイプごとに、将来におけるデータ増加率を見積もります。 データ増加率を見積もっておくと、将来も有効に機能するバックアップ ソリューションを構築できます。 例えば、100人の従業員を新たに採用する計画がある場合には、ユーザー データとクライアント システム データの総量もそれだけ増加するはずです。
- バックアップに要する時間
  それぞれのバックアップ処理に要する時間を見積もります。 この値は、データの利用可能時間に直接影響を与えます。 例えば、ユーザー ファイルについては、そのユーザーが使用していないときには、いつでもバックアップを実行できますが、トランザクション データベースについては、バックアップ可能な時間帯が数時間程度しかないことが予想されます。
  またバックアップに要する時間は、実行するバックアップのタイプ、つまりフル バックアップを実行するか、増分バックアップを実行するかによっても異なります。 詳細については、「フル バックアップと増分バックアップ」 (84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。
  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、第11章 (245ページ) およびディスクステージング (110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。
  さらに、大量のデータをバックアップする必要があり、バックアップに使用できる時間も限られている場合は、ダイレクト バックアップの使用も検討して

ください。 ダイレクト バックアップを使用するとSANの速度を活用し、ネットワーク トラフィックを減少させ、バックアップ サーバーがボトルネックとなるのを回避できます。

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

バックアップ方針に影響する各種の要因

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

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

バックアップ方針を構築する準備

バックアップ方針を構築するには、以下の点を明らかにする必要があります。

- 各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。
  - ライブラリ デバイスをFibre Channelブリッジ経由でSANに接続して、ダイレクト バックアップを実行できるようにシステムを構成することを検討してください。 これは、ネットワークによってバックアップ速度が遅くなる場合のソリューションです。
- 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

バックアップ方針の策定において最も重要な決定事項の1つが、単一セル環境または複数セル環境のどちらを選択するのかという点です。 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。 例えば管理対象が複数のグループに分かれているような環境では、データ セキュリティ上の理由により、これらのグループを1つのセル内にはまとめたくない可能性があります。 一方、複数セルに分割した場合の問題点としては、単一セルの場合に比べて管理作業が煩雑になり、場合によっては各セルごとに専用の管理者を設ける必要があるといった点が挙げられます。
- セルのサイズ
  Data Protectorセルのサイズは、バックアップ性能およびセルの管理能力に影響を与えます。 Data Protectorセルの推奨最大サイズは、100クライアント システムです。 200を超えるクライアント システムを含むセルは管理しにくくなります。
- ネットワーク上の問題
  最大の性能を得るためには、同一セル内のすべてのクライアント システムを、同一LAN上に配置する必要があります。 その他、ネットワーク構成などに関する詳細は、以下の項を参照してください。
- 地理的な配置
  バックアップ対象となるクライアント システムが地理的に分散している場合、それらのシステムを1つのセル内で管理するのは難しく、また、クライアント システム間のネットワーク接続に関して問題が発生する可能性があります。 さらに、データのセキュリティ面にも注意しなければなりません。
- 時間帯
  1つのセル内が、複数の時間帯に分かれてはいけません。
- データのセキュリティ
  Data Protectorのセキュリティは、セル レベルで提供されます。 また、Data Protectorにおける管理業務は、必ず単一セル単位で行われます。 例えば、メディア、バックアップ デバイス、バックアップ データなどは、必ず1つのセルに所属します。 ただしData Protectorでは、複数のセル間でデバイスを共有した

り、別のセルにメディアを移動したりすることも可能なため、個々のメディアに対する物理的なアクセス権は適切なユーザーのみに与えるようにしてください。

- 混合環境
  Data Protectorでは、多数のプラットフォームからなるクライアント システムを1つのセルにバックアップすることができます。 ただし場合によっては、各クライアント システムを、プラットフォームごとに個別のセルにまとめた方が便利なこともあります。 つまり、1つのセル内にはWindowsクライアント システムのみを、もう1つのセル内にはUNIXクライアント システムのみを配置するといった方法です。 特に、UNIX環境とWindows環境で、それぞれ個別の管理者とバックアップ方針を設定する場合には、この方法をお勧めします。
- 部門とサイト
  各部門またはサイトごとに、それぞれ個別のセルを設定することも可能です。 例えば、経理部門、IT部門、製造部門別に、それぞれ専用のセルを設定できます。 Data Protectorを使用すると、このように環境内を複数セルに分割した場合であっても、これらのセル間で共通のバックアップ方針を簡単に構成できます。

クライアント システムのインストールと保守

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

Installation Serverと Cell Manager

Data Protectorセルの中心となるシステムは Cell Managerです。中央のある一点から、各クライアント システムにData Protectorコンポーネントを簡単に配布(プッシュ)するには、Data Protectorソフトウェア レポジトリを持ったシステムが必要になります。 このシステムをData Protector Installation Serverと呼びます。デフォルトでは、Cell Managerが同時にInstallation Serverにもなります。

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

ソフトウェアのインストールを実際に開始する前に、まずInstallation Server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Installation Serverは、CDから直接インストールします。 Cell ManagerとInstallation Server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。 このマニュアルで説明する注意点に基づいて、セル内に加えるクライアント システムと、Cell Managerシステムを決定してください。 インストール時には、すべてのクライアント システムに対してrootアクセス権が必要です。 また重要な前提条件として、クリーンな形でノード名を解決したセットアップを行っておき、クライアント システム同士が、完全修飾されたノード名を使用して互いにアクセスできるようにしておく必要があります。

Windows環境でのセルの作成

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

Windowsドメイン

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

Data ProtectorセルとWindowsドメインの対応付け

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

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

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

Windowsワークグループ

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

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

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」 (58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考慮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。 詳細については、「環境内を複数セルに分割する」 (39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

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

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

性能に関する概要と計画上の注意点

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

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

インフラストラクチャ

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

ネットワーク バックアップとローカル バックアップ

ネットワークおよびサーバ経由でデータを送信する場合は、新たなオーバーヘッドが生じるため、ネットワーク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。

ネットワークのデータ ストリーム

ディスク→送信元システムのメモリ→ネットワーク→送信先システムのメモリ→デバイス

ローカルのデータ ストリーム

ディスク→メモリ→デバイス

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

ネットワーク バックアップまたはサーバ バックアップとダイレクト バックアップ

ネットワークおよびサーバ経由でデータを送信する場合は、新たなオーバーヘッドが生じるため、ネットワークやサーバによっても性能が左右されます。Data Protectorでは次のような場合にデータストリームを別に処理します。

ネットワークのデータ ストリーム

ディスク→送信元システムのメモリ→ネットワーク→送信先システムのメモリ→デバイス

ダイレクト データ ストリーム

ディスク→デバイス

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

デバイス

デバイスの性能

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。
- 複数のXCOPYエンジンを使用して、オブジェクト(ディスクまたはファイル)を複数の(テープ)デバイスに直接バックアップできる場合。
- クライアント システム間で複数の専用ネットワーク リンクを使用できる場合。例えば、system_Aにバックアップ対象のオブジェクト(ディスク)が6個あり、system_Bに高速テープ デバイスが3台ある場合は、system_Aとsystem_Bとの間で3つのネットワーク リンクをバックアップ専用にします。
- 負荷調整
  これはData Protectorの機能であり、どのオブジェクト(ディスク)をどのデバイスにバックアップするかがData Protectorによって動的に決定されます。 特に、動的環境において多数のファイルシステムをバックアップする場合は、この機能をオンに設定してください。 詳細については、「負荷調整の仕組み」 (146ページ) をご覧ください。
  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」（147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**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、『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

セル

セッションの開始

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

特定のCell Managerからのアクセス

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

実行前および実行後スクリプトの制限

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

Data Protectorのユーザー アカウント

Data Protectorユーザー アカウント

Data Protectorの機能を使用するためには、管理作業を行う場合であっても、個人的なデータを復元するだけの場合であっても、必ずData Protectorのユーザー アカウン

トを取得しておかなければなりません。 このユーザー アカウントは、Data Protectorおよびバックアップ データに対する不正アクセスの防止に役立っています。

ユーザー アカウントの設定者

ユーザー アカウントは管理者が作成し、作成時にはユーザーのログイン名、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。

詳細については、第4章 (173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、例えば、[end user]グループのメンバーには、個人データをローカル システム上に復元する権限のみを与え、一方[operators]グループのメンバーには、バックアップの開始およびモニタリングを行う権限を与えるが、バックアップの作成は許可しない、といった設定が可能です。

詳細については、第4章 (173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。

詳細については、第4章 (173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。 オーナーとは、そのバックアップを構成し、バックアップ セッションを開始(あるいはスケジュール設定)したユーザーを指します。 バックアップ オーナーの詳細については、「誰がバックアップ セッションを所有するのか」 (72ページ) 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、AES 256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のキー保存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）を使用するエンコード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

Backup Session Manager (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。

図 17 (70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。

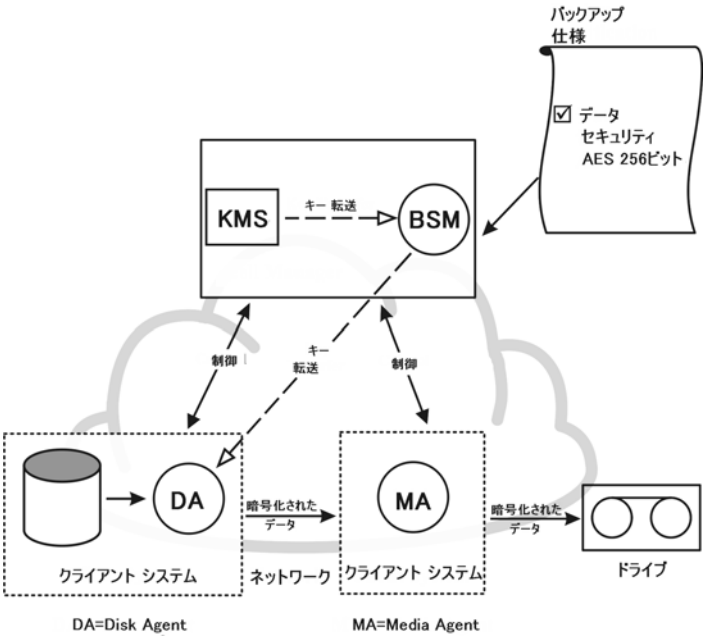

図 17 AES 256ビット暗号化を指定したバックアップ セッション

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、宛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）。

図 18（71ページ）では、[Drive based encryption]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。

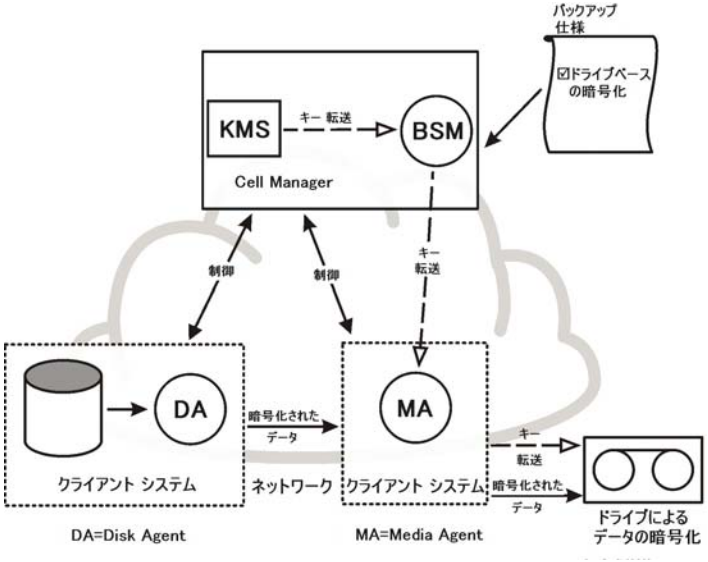

図 18 ドライブベースの暗号化を指定したバックアップ セッション

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。

誰がバックアップ セッションを所有するのか

バックアップ所有権とは

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

バックアップを開始できるユーザー

各ユーザーは、自分が作成したバックアップ仕様しか実行できません。 そのため、バックアップ管理者がバックアップ仕様を作成した場合には、他のユーザーはこのバックアップ仕様に基づくバックアップを開始することができません。 バックアップ オーナーの変更方法については、オンライン ヘルプで「所有権」をキーワードに指定して確認してください。 バックアップ オーナーを変更すると、新しいオーナーは、実際には所有していないデータへのアクセスや復元も可能になる点に注意してください。

バックアップ所有権と復元

バックアップ所有権は、データの復元時にも影響します。 [プライベート]/[パブリック]オプションが[プライベート]に設定されている場合には、そのメディア セット内に保存されているデータは、メディア セットのオーナーまたは管理者しか見ることができません。

クラスタリング

クラスタの概念

クラスタとは

クラスタとは、 ネットワーク上では単一のシステムとして認識される、複数のコンピュータから構成されるグループを指します。 クラスタ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ではクラスタ化を実現するために、 Windows Server用のMicrosoft Cluster Server、 HP-UX用のMC/Service Guard、 Solaris用のVeritas Cluster、および Novell NetWare Cluster Servicesとの統合が可能です。 サポートされているクラスターの一覧は、『HP Data Protector product announcements 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。

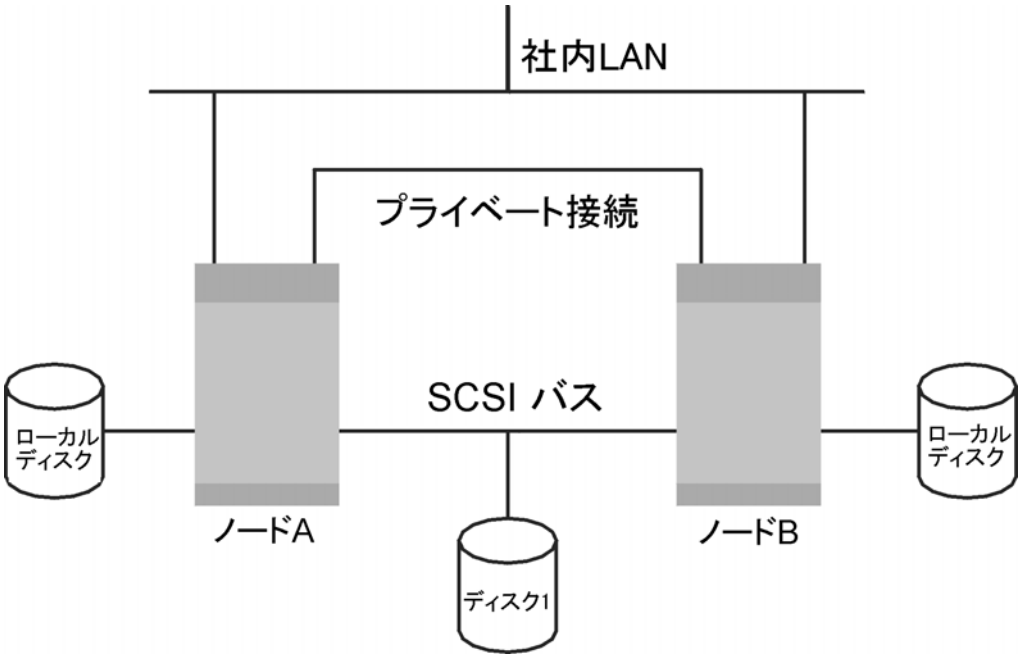

図 19 代表的なクラスタ

構成要素

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

クラスタノード

クラスタノード クラスタを構成するコンピュータは、クラスタ ノードと呼ばれます。 クラスタノードは、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、クラスタの実行に必要なクラスタ固有のデータも格納されています。 MSCSクラスタ内では、共有ディスクはある一時点では1つのクラスタ ノード上でしか使用できません。

クラスタネットワーク

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

パッケージまたはグループとは

パッケージ(MC/SGまたはVeritas Clusterの場合)、またはグループ(MSCSの場合)とは、特定の**クラスタ対応**アプリケーションの実行に必要なリソースの集まりを指します。 各クラスタ対応アプリケーションでは、それぞれの重要なリソースを宣言します。 各グループまたはパッケージ内では、以下のリソースが定義されていなければなりません。

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

仮想サーバとは

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

フェイルオーバーとは

それぞれのパッケージまたはグループには、通常の場合に実行される「優先」ノードが設定されています。 このようなノードを **一次ノード**と呼びます。 パッケージまたはグループは、別のクラスタ ノード(いずれかの**二次ノード**)に移動させることができます。 パッケージまたはグループを一次クラスタ ノードから二次クラスタ ノードに移すことを **フェイルオーバー**、またはスイッチオーバーと呼びます。 二次ノードは、一次ノードで障害が発生した場合にパッケージまたはグループを引き継ぎます。 フェイルオーバーは、以下に示すような原因により発生します。

- 一次ノード上でソフトウェア障害が発生した場合
- 一次ノード上でハードウェア障害が発生した場合
- 一次ノード上での保守作業を目的として、管理者が意図的に所有権を移した場合

クラスタ環境では、複数の二次ノードを設定できますが、一次ノードは1つしか設定できません。

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

Data Protector Cell Managerの高可用性の実現

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

バックアップの自動再開

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

フェイルオーバー時の負荷調整

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

クラスタのサポート

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

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

注記：

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

- Data Protectorクライアントがクラスタ内にインストールされていること。 このような場合、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 でフェイルオーバーが発生した場合のバックアップ セッションの動作を指定するオプションの詳細については、オンライン ヘルプでキーワード「クラスター」から「バックアップ仕様オプション」を指定して確認してください。

クラスタ環境の例

この項では、3つのクラスタ構成例を示します。

Cell Manager がクラスタ外部にインストールされている構成

下図の環境には以下のような特徴があります。

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

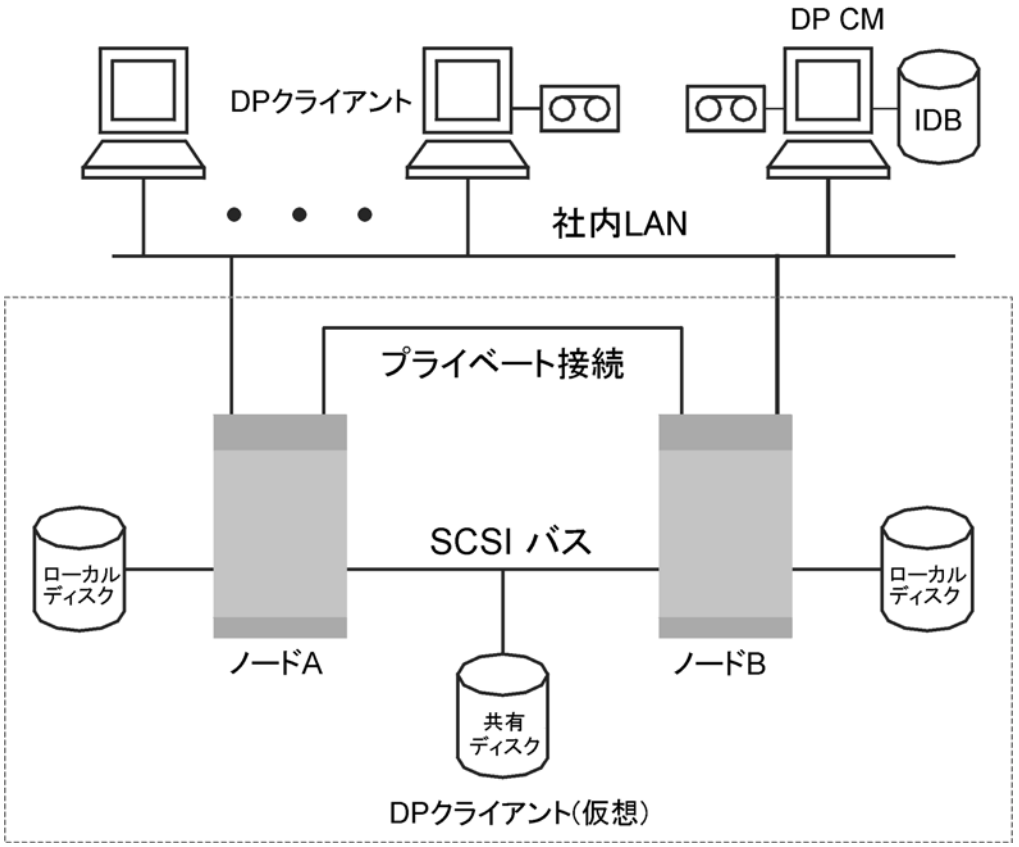

図 20 Cell Manager がクラスタ外部にインストールされている構成

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

- 物理ノードA
- 物理ノードB
- 仮想サーバー

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、オンライン ヘルプでキーワード「クラスター」から「バックアップ仕様オプション」を指定して確認してください。

以下に、この構成で予想されるバックアップ動作を示します。

表 3 バックアップ動作

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

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

下図の環境には以下のような特徴があります。

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

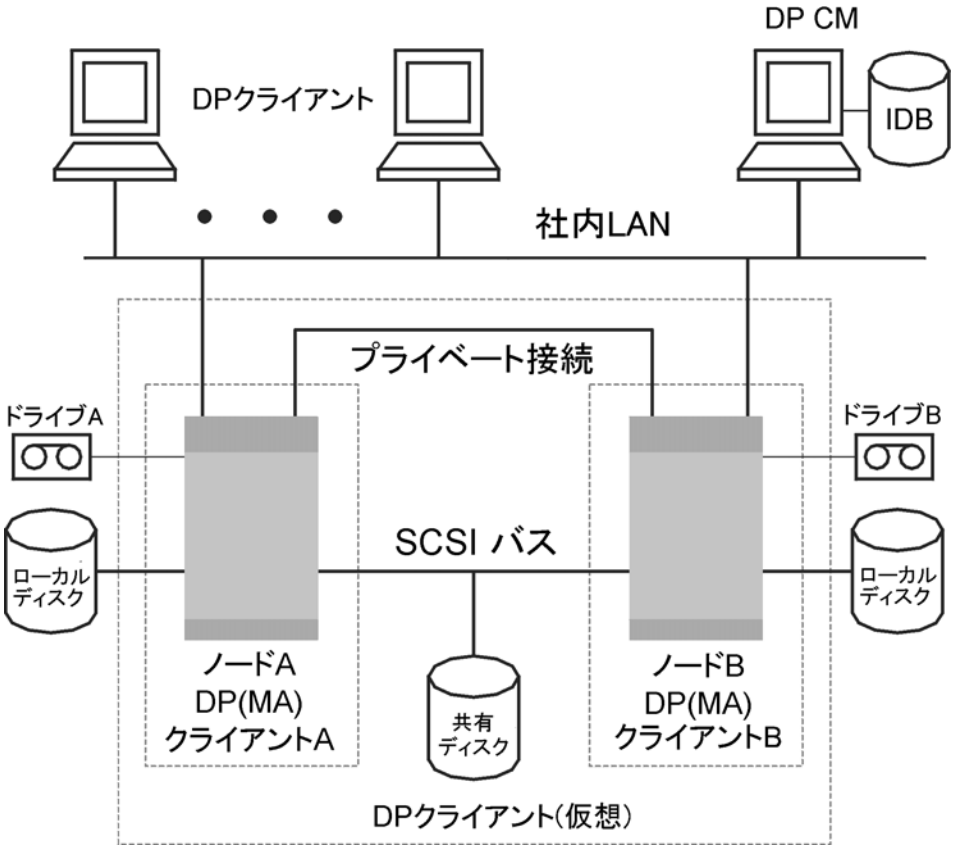

図 21 Cell Manager がクラスタ外部にインストールされ、デバイスがクラスタ ノードに接続されている構成

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

- 物理ノードA
- 物理ノードB
- 仮想サーバー

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

以下に、この構成で予想されるバックアップ動作を示します。

表 4 バックアップ動作

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

重要：

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

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

下図の環境には以下のような特徴があります。

- Cell Managerは、クラスタの内部にインストールされています。 Data Protectorアプリケーション用統合機能については、このような構成の場合、Data Protectorとアプリケーションを以下のいずれかの方法で構成できます。
  - Data Protector Cell Managerをアプリケーションと同じノード上で実行するよう構成します(通常の動作時およびフェイルオーバー時共)。 つまり、

Data Protectorクラスタの重要なリソースは、アプリケーション クラスタの重要なリソースと同じパッケージ(MC/ServiceGuardの場合)またはグループ(Microsoft Cluster Serverの場合)内に定義します。

重要：

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

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

- バックアップ デバイスは、クラスタの共有Fibre Channelバスに、FC/SCSI MUXを介して接続されています。

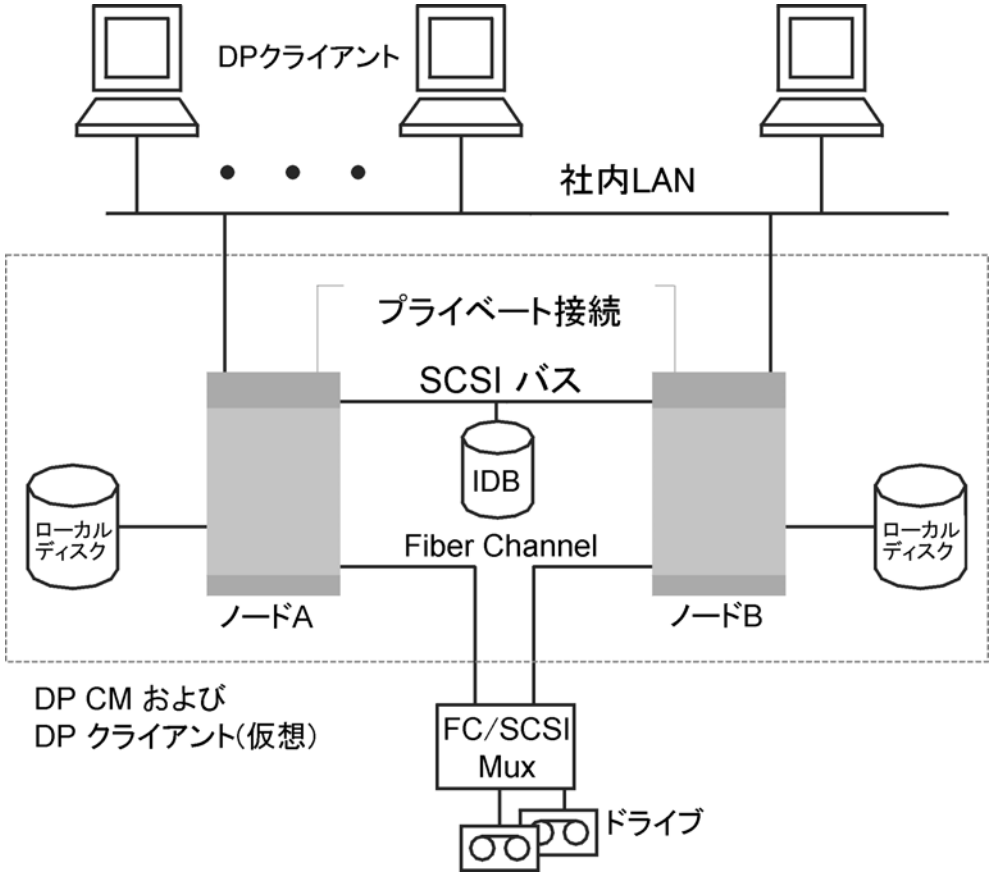

図 22 Cell Manager がクラスタ内部にインストールされ、デバイスがクラスタ ノードに接続されている構成

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

- 物理ノードA
- 物理ノードB
- 仮想サーバー

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、セッションを継続できます。

以下に、この構成で予想されるバックアップ動作を示します。

表 5 バックアップ動作

条件	結果	
バックアップ開始前にフェイルオーバーが発生	バックアップ成功	
バックアップ中に、アプリケーションとCell Managerのフェイルオーバーが発生した場合(Cell Managerとアプリケーションは同じノード上で実行)。	**ファイルシステム/ディスク イメージのバックアップ**バックアップ セッションが失敗します。 このセッションでバックアップが完了しているオブジェクトは復元に使用できます。失敗したオブジェクト(実行中および保留中)については、セッションが自動的に再開されて再度バックアップされます。	**重要** セッションを再開するには、適切なData Protectorオプションを選択することが必要です。 Cell Managerのフェイルオーバー発生時に実行可能な各種Data Protectorアクショ

条件	結果	
	アプリケーションのバックアップ バックアップ セッションが失敗します。 セッションは自動的に再開されます。	ンを定義する方法については、オンライン ヘルプでキーワード「クラスター」から「バックアップの管理」を指定して確認してください。
バックアップ中に、アプリケーションのフェイルオーバーが発生したが、Cell Manager自体のフェイルオーバーは発生していない場合(Cell Managerはアプリケーションとは別のノード上で実行)。	**ファイルシステム/ディスク イメージのバックアップ**ファイルシステムがインストールされているノードがフェイルオーバーすると、バックアップ セッションが失敗します。 このセッションでバックアップが完了しているオブジェクトは復元に使用できますが、失敗したオブジェクト(実行中および保留中)については、セッションを手動で再開してもう一度バックアップする必要があります。	
	アプリケーションのバックアップバックアップ セッションが失敗します。 セッションを手動で再開する必要があります。	

重要：

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

またData ProtectorクラスタのCell Manager/クライアントを、EMC Symmetrix環境またはHP StorageWorks Disk Array XP環境と統合すると、非常に可用性の高いバックアップ環境を構築できます。 詳細については、『HP Data Protector zero downtime backup administrator's guide』を参照してください。

フル バックアップと増分バックアップ

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

フル バックアップを実行すると、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方針に及ぼす影響について説明します。

表 6 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。 例えばSybaseでは、この種のバックアップはトランザクション バックアップと呼ばれ、最後のバックアップ以降に変更されたトランザクション ログのみがバックアップされます。

増分バックアップの概念は、ロギング レベルの概念とは無関係である点に注意してください。 ロギング レベルとは、IDBに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用統合機能を使用すると、さらにさまざまな種類のバックアップが可能になります(ダイレクト バックアップ、スプリット ミラー バックアップ、スナップショット バックアップ、データ ムーバ バックアップなど)。詳細は、『HP Data Protector インテグレーションガイド』を参照してください。

フルバックアップ

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

合成バックアップ

合成バックアップは、通常のフル バックアップを実行する必要のない高度なバックアップ ソリューションです。 代わりに、増分バックアップが実行され、続いてそれがフル バックアップとマージされると、新規合成フル バックアップとなります。 詳細については、第11章 (245ページ) をご覧ください。

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。

Windows NTFS Change Log Providerを使用する場合も、拡張増分バックアップを実行することができます。 Change Log Providerでは、時間を要するファイル ツリー検索ではなく、変更ファイルのリスト取得のためにWindows Change Journalに問い合わせます。 Change Journal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、図 23 (87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、図 24 (88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。 例えば増分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*。

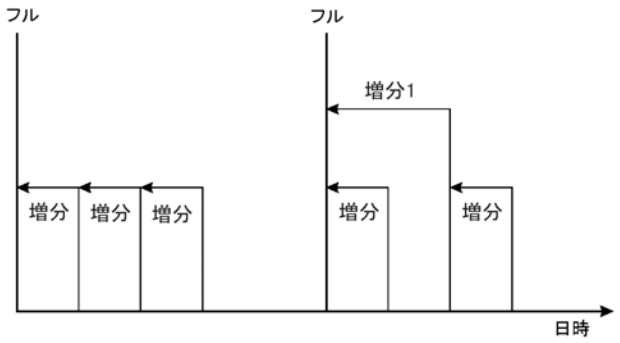

図 23 増分バックアップ

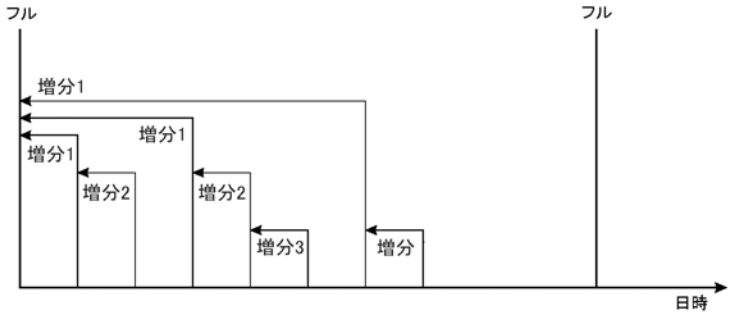

図 24 複数レベル増分バックアップ

表 7 (88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 7 バックアップ実行時の相対的参照関係

1	Full（挿入中）	<----	増分1						
2	Full（挿入中）	<----	<----	<----	増分2				
3	Full（挿入中）	<----	増分1	<----	増分2				
4	Full（挿入中）	<----	増分						
5	Full（挿入中）	<----	増分1	<----	増分				
6	Full（挿入中）	<----	増分1	<----	増分2	<----	増分		
7	Full（挿入中）	<----	増分1	<----	増分	<----	増分		
8	Full（挿入中）	<----	増分1	<----	増分3				
9	Full（挿入中）	<----	増分1	<----	増分2	<----	増分3		
10	Full（挿入中）	<----	<----	<----	増分2	<----	増分3		
11	Full（挿入中）	<----	<----	<----	<----	<----	増分3		

表 7（88ページ）の見方

- 表 7（88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。

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。

図 25（90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**(Appendable on Incrementals Only)]オプションを使うと、フル バックアップと、同じバックアップ仕様内の増分バックアップが同一のメディア セット内に保存されます。

増分バックアップ概念の別の共通な用途については、図 26（90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。

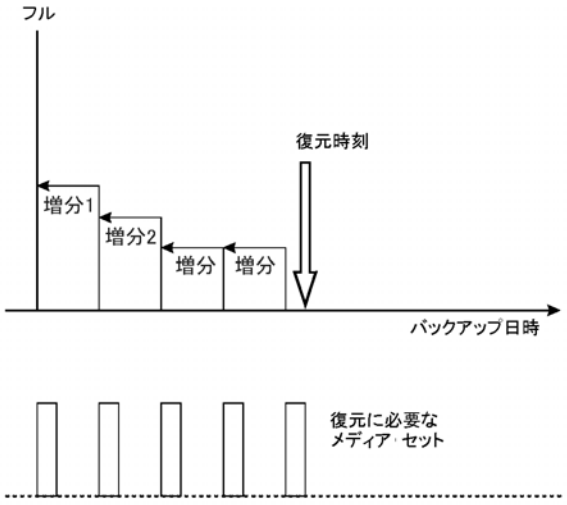

図 25 簡易および複数レベルの増分バックアップからの復元時に必要となるメディア

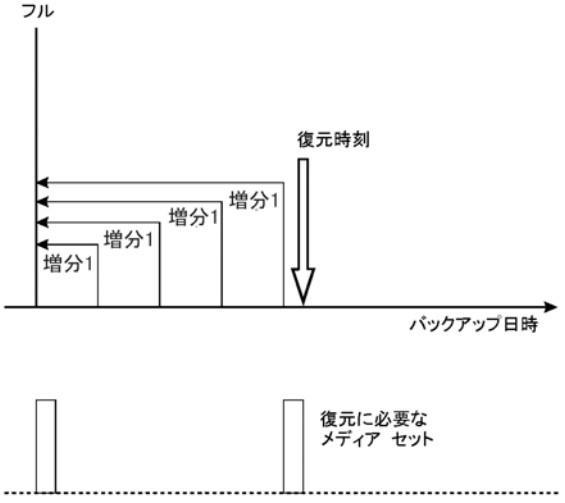

図 26 複数レベルの増分バックアップからの復元時に必要となるメディア

復元に必要なフル バックアップと増分バックアップが、必要時にすべて揃っているようにするには、データ保護を適切に設定しなければならない点に注意してください。 データ保護が適切に設定されていないと、復元チェーンが切れる可能性があります。 詳細については、付録 B (319ページ) を参照してください。

バックアップ データおよびバックアップ データに関する情報の保存

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

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

Data Protector内部データベース

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

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

データ保護

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。 詳細はオンライン ヘルプでキーワード「データ保護」を指定して確認してください。

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

カタログ保護(Catalog protection)

カタログ保護とは

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

保護期間は、絶対日付または相対日付のどちらでも指定できます。

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

カタログ保護の設定がIDB サイズの増大と性能に及ぼす影響の詳細については、「IDBの主要な調整可能パラメータとしてのカタログ保護」 (190ページ) を参照してください。

Data Protectorで採用されている保護モデルは、バックアップ世代に対応付けることができます。 詳細については、付録 B (319ページ) 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」 (188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。

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。

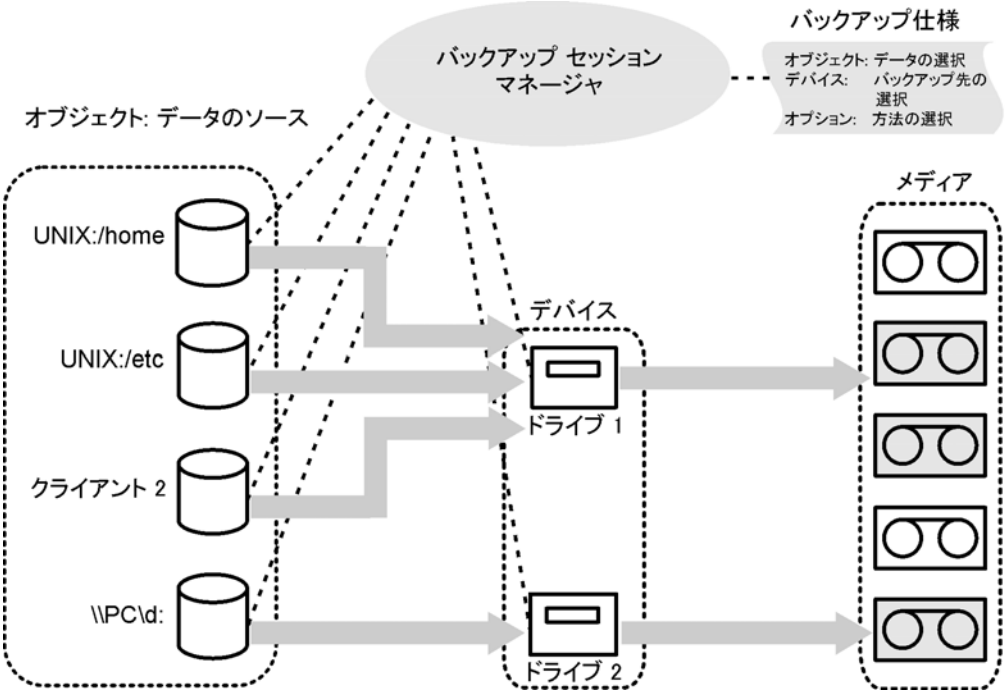

図 27 バックアップセッション

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。 詳細は、「ディスク ディスカバリ バックアップ」 (213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ています。

- クライアント名: バックアップ オブジェクトが存在するData Protectorクライアントのホスト名です。
- マウントポイント: バックアップ オブジェクトの存在するクライアント上のディレクトリ構造内で、そのバックアップ オブジェクトへアクセスするためのポイントです(Windows上のドライブまたはUNIX上のマウント ポイント)。

- 説明： 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。 例えば、バックアップ オブジェクトの説明を変更すると、そのオブジェクトは新しいバックアップ オブジェクトであるとみなされて、増分バックアップではなくフル バックアップが自動的に実行されます。

バックアップ オプションの例

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

- IDBに記録するログ情報のレベル
  Data Protectorでは、ファイルやディレクトリについてどの程度の詳細情報をIDBに記録するかを4つのレベルから選択できます。
  - [すべてログに記録(Log All)] すべてろぐにきろく(Log All)
  - [ファイル レベルまでログに記録(Log Files)] ふぁいる れべるまでろぐにきろく(Log Files)
  - [ディレクトリ レベルまでログに記録(Log Directories)] でぃれくとり れべるまでろぐにきろく(Log Directories)
  - [記録しない(No Log)] きろくしない(No Log)

  保存する詳細情報のレベルを変更すると、復元時にData Protectorのユーザーインタフェースを使ってファイルをブラウズする機能が影響を受けることに注意してください。 ロギング レベルの詳細については、「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」 (188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。 詳細については、「負荷調整の仕組み」 (146ページ) をご覧ください。
  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」 (211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

A 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、第7章 (207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。

詳細については、「オブジェクト ミラーの作成」 (112ページ) をご覧ください。

メディア セット

メディア セットとは

カラーマネージメントを行うには、オペレーティング システムからの場合もアプリケーションからの場合も 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。 (表 6 (85ページ) を参照)。

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。 詳細は、「フル バックアップの時差実行」 (99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。

個々のバックアップおよび定期的にスケジュールされるバックアップでは、**[バックアップの種類]** (フルか増分か)、**[ネットワーク負荷]**、**[バックアップ保護]**のオプションを指定できます。 また、スプリット ミラー バックアップまたはスナップショット バックアップで、ディスクへのZDBまたはディスク+テープへのZDB (インスタント リカバリに対応) を実行する場合は、**スプリット ミラー/スナップショット バックアップ** オプションを指定します。 スプリット ミラー バックアップおよびスナップショット バックアップについては、バックアップの種類は無視されて、必ずフル バックアップが実行されます。

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

バックアップセッション

バックアップ セッションが開始されると、Data Protectorでは、デバイスなどの必要なリソースの割り当てを試みます。 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 バックアップと増分バックアップ」 (84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」 (91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」 (99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 8 時差実行方式

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

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 を参照してください。

例1

図 28（100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。

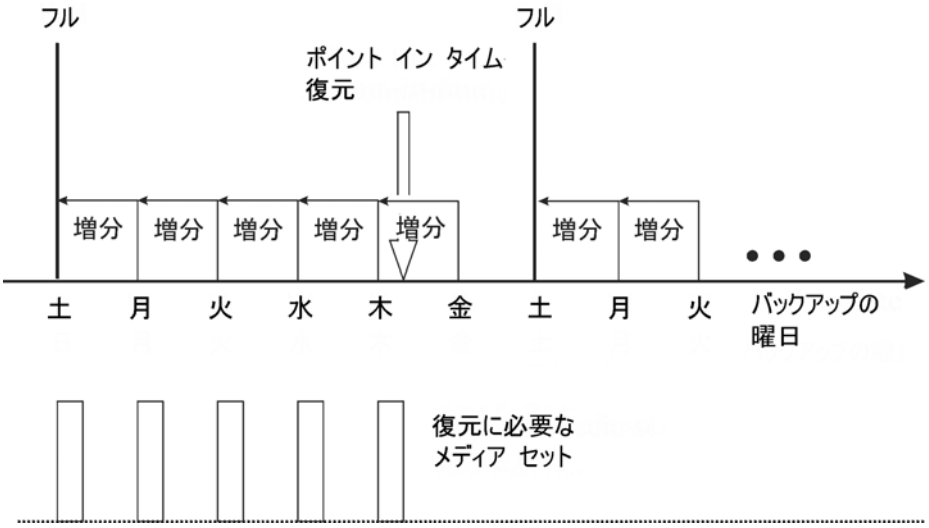

図 28 フル バックアップと1日1回の簡易増分バックアップを実行

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、例えば木曜日のバックアップからファイルを復元するような場合には、フル バックアップと木曜日までの増分バックアップが必要になるため、合計5つのメディア セットが必要です。 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

図 29（101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。

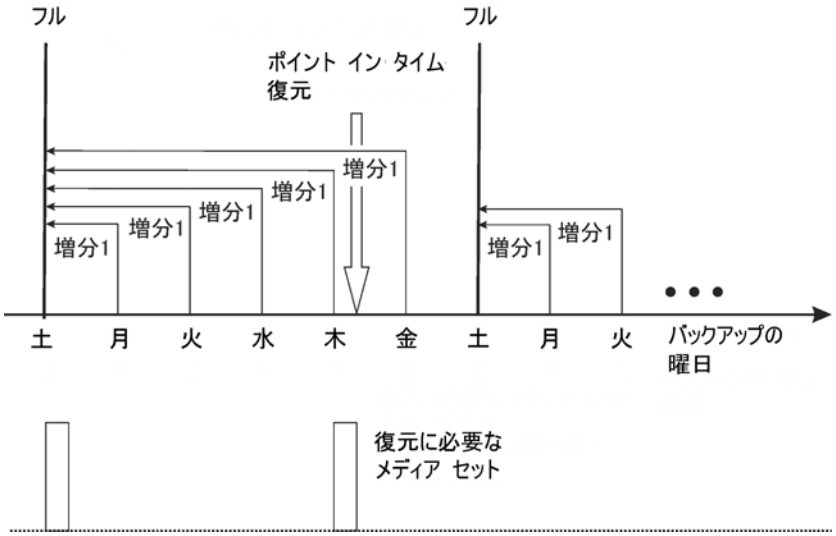

図 29 フルバックアップと1日1回のレベル1増分バックアップ

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、例えば木曜日のバックアップからファイルを復元するには、フル バックアップと木曜日の増分バックアップしか必要ないため、合計2つのメディア セットのみが必要となります。 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。 例えば、以下に示すスケジュール設定方針を設定できます。

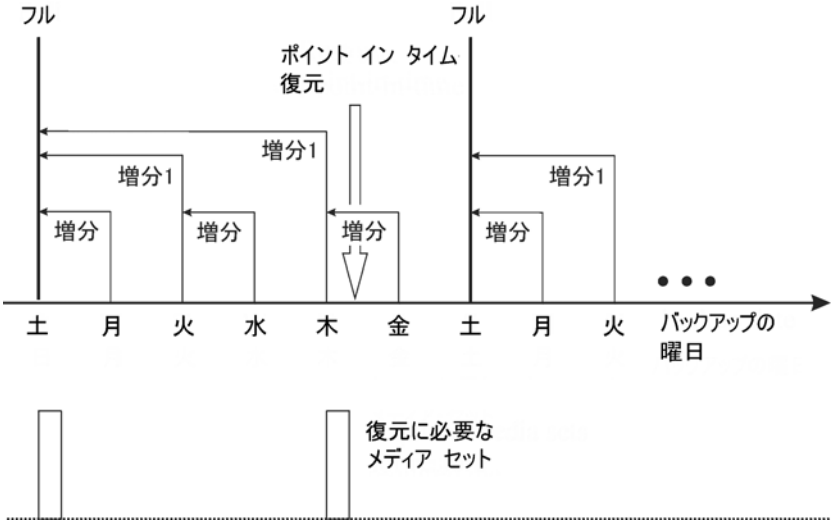

図 30 フルバックアップと2通りの増分バックアップ

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(ディファレンシャル)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、例えば木曜日のバックアップからファイルを復元するには、フル バックアップと2番目の増分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。 詳細は、「メディア交換方針の実装」 (134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。 詳細については、「大容量ライブラリ」 (152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では、バックアップ データの複製方法として、オブジェクト コピー、オブジェクト ミラー、メディア コピーが用意されています。 これらの機能の主な特徴に関して、表 9（104ページ）にまとめます。

表 9 Data Protectorのデータ複製メソッド

	オブジェクト コピー	オブジェクト ミラー	メディア コピー	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 セッションで作成される異なるオブジェクト バージョンの任意の組み合わせ	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	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	あり	あり	なし [2]	いいえ [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	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 コピーの作成

オブジェクトコピーとは

Data Protectorには、選択したオブジェクト バージョンを特定のメディア セットにコピーするための、オブジェクト コピー機能が用意されています。 この機能を使用すると、コピー元として、1つまたは複数のバックアップ セッションまたは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。

図 31（106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。

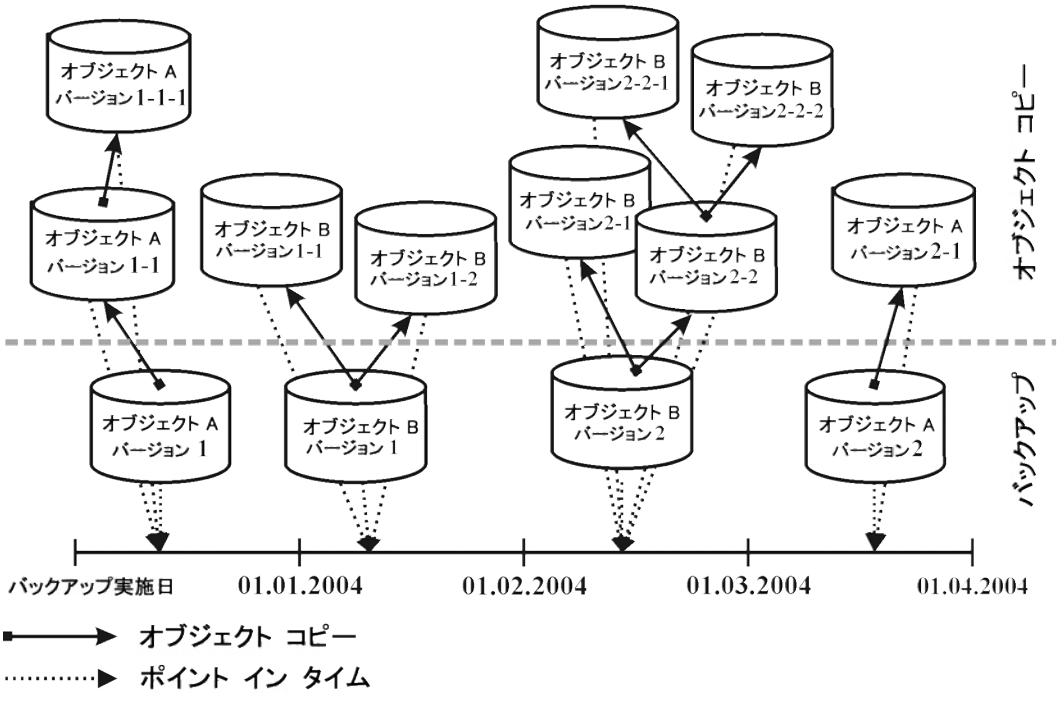

図 31 オブジェクト コピーの概念

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のオブジェクトコピー 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。 自動オブジェクトコピー仕様に従って選択された、特定のセッションで書き込まれた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 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。

オブジェクト コピー仕様内にコピー元デバイスを指定しなければ、デフォルトのデバイスが使用されます。 デフォルトでは、オブジェクトの書き込みに使用されたデバイスがソースデバイスとして使用されます。 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同じブロック サイズのデバイスが、ブロック サイズが異なるデバイスよりも優先的に選択されます。
- 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」 (118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

以下のような目的で、バックアップデータの追加コピーを作成します。

- ボールティング
  バックアップ オブジェクトのコピーを作成し、それらを複数の場所に保管できます。
- メディアの解放
  メディア上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 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」 (142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

お客様 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。 (図 32 (109ページ) を参照)。

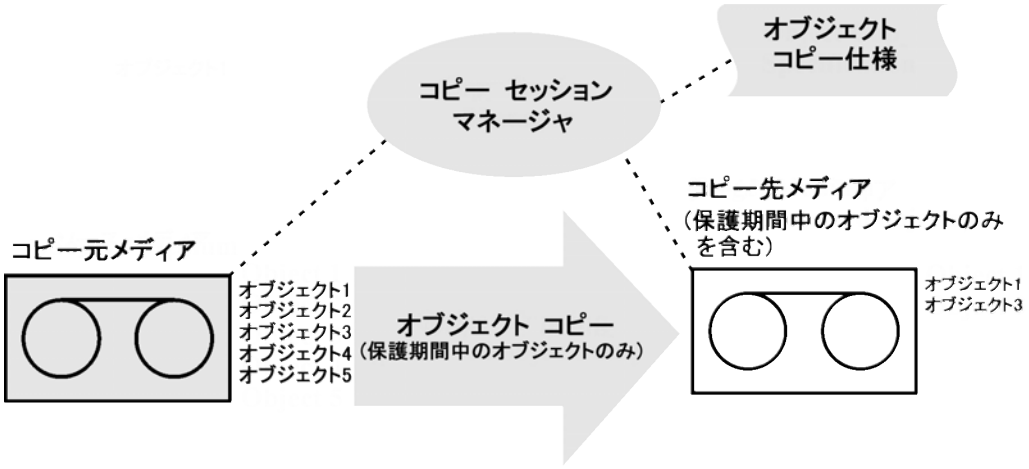

図 32 メディアの解放

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。 (図 33 (110ページ) を参照)。

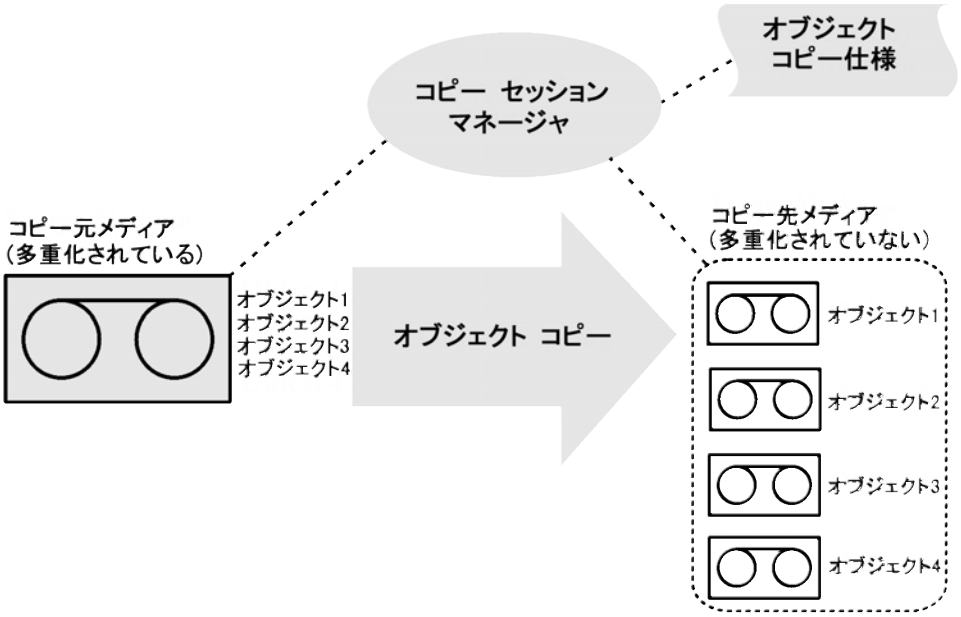

図 33 メディアの多重化(データの断片化)の解消

復元チェーンの統合

お客様 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。 例えば、あるオブジェクトをファイル デバイスからLTOデバイスに、またはDLTデバイスからLTOデバイスにコピーできます。

ディスクステージング

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

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。 （図 34（111ページ）を参照）。

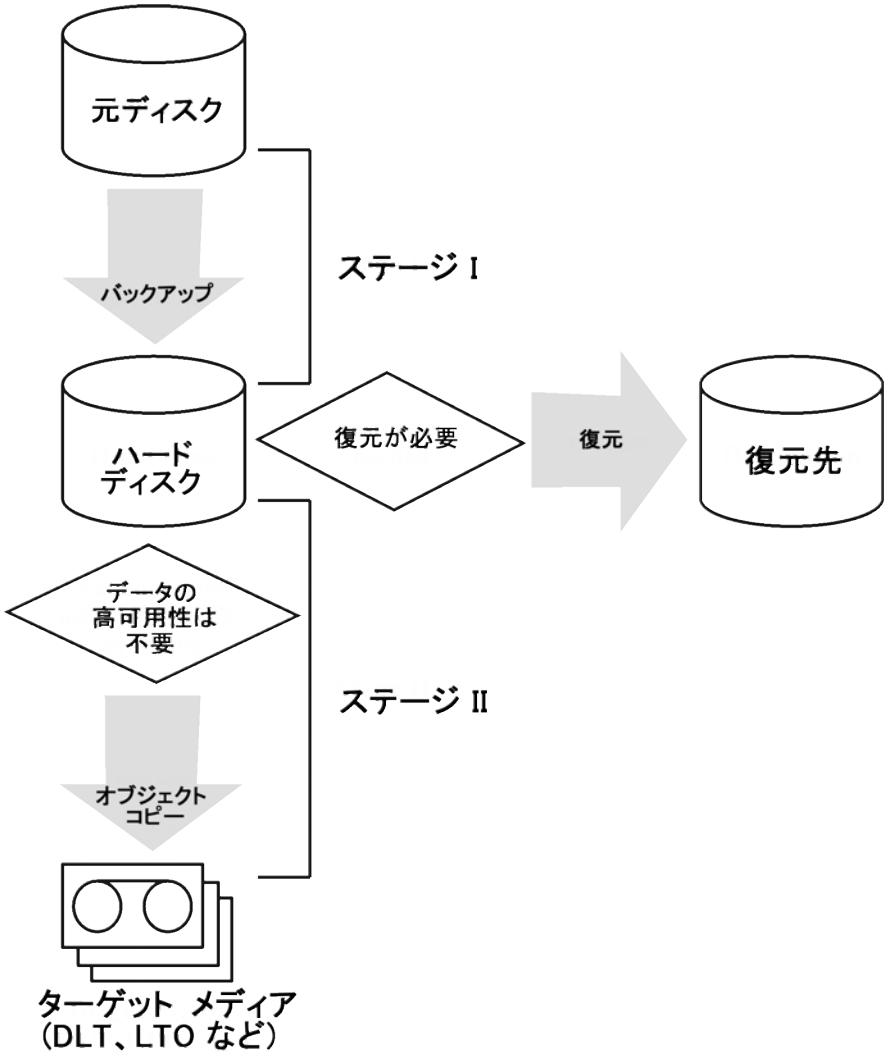

図 34 ディスクステージングの概念

ディスクステージングを使用すると、サイズの小さい多数のオブジェクトをテープに頻繁にバックアップする必要もなくなります。 そのようなバックアップでは、メディアをいちいちロードおよびアンロードしなければならないため、作業に手間がかかりま

す。 ディスクステージングを使用すると、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。

オブジェクト ミラーの作成

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。 （図 35（113ページ）を参照）。

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

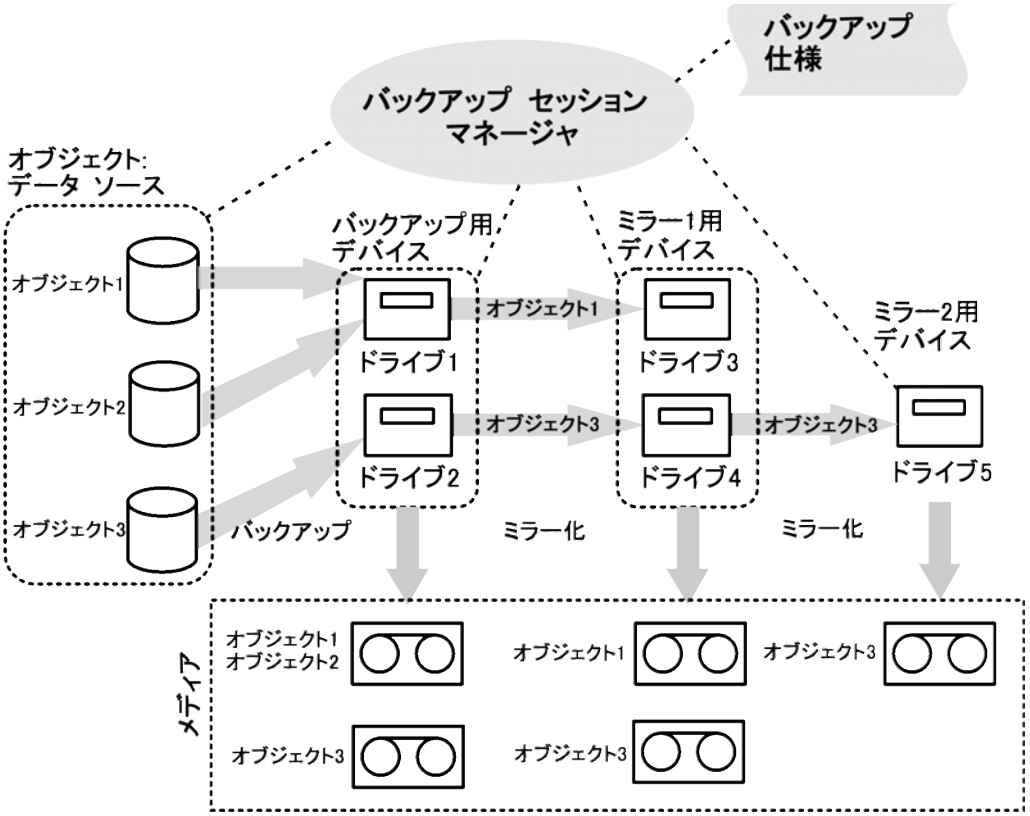

図 35 オブジェクト ミラーの作成

デバイスの選択

オブジェクト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、それらが選択されます。
- 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」 (116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(non appendable)マークが付けられて、新しいバックアップ データは追加できなくなります。 これは元のメディアの内容がそのコピーと異ならないようにするためです。 同様にコピーにも追加不可能マークが付けられます。 コピーに対するデフォルトの保護設定は、 元のメディアと同じになります。

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

自動メディア コピー

自動メディア コピーとは

自動メディア コピーとは、バックアップ データが格納されたメディアのコピーを自動作成するプロセスを指します。 この機能はライブラリ デバイスとともに使用します。

Data Protectorには2種類の自動メディア コピー機能が用意されています。 1つはバックアップ後のメディア コピー、もう1つはスケジュール方式のメディア コピーです。

バックアップ後のメディア コピー

バックアップ後の メディア コピーは、バックアップ セッションの終了後に開始されます。 この場合は、特定のセッション内で使用されたメディアがコピーされます。

スケジュール方式のメディア コピー

予定済み 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 コピーには独自の調整機構が備わっています。 Data Protectorはできるだけ多くのデバイスを使用し、また可能であればローカル デバイスを使用することにより、使用可能なデバイスを最大限有効に活用しようとします。

自動メディア コピー機能は、マウント要求やクリーニング要求には対応できません。マウント要求が発行された場合は、その要求に関係するメディア ペアに対する処理は打ち切られますが、セッションは続行されます。

使用例については、「自動メディア コピーの例」 (320ページ) 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、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 コピーの、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。

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 コピーの詳細は、オンライン ヘルプの索引キーワード「スマート メディア コピー」およびVLSのドキュメントを参照してください。

データの復元

データ復元方針は、各企業の全体的なバックアップ方針における本質的なポイントとなります。 以下の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。 詳細については、「フル バックアップと増分バックアップ」 (84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。 詳細については、第3章 (125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。 詳細については、「性能に関する概要と計画上の注意点」 (60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)。 詳細については、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。
- 並列復元の使用。 データのバックアップ方法によっては、単一の読み取り操作で、複数のオブジェクトを同時に復元できます。 詳細は、「並行復元」 (215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。 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」 (188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 セットはData Protectorにより自動的に選択されます。 メディア位置の優先順位を設定しておくと、このメディア セットの自動選択をある程度まで制御できます。 統合オブジェクトを復元する場合を除き、復元に使用するメディア セットを手動で選択することも可能です。

メディア セットの選択アルゴリズム

デフォルトでは、可用性と品質に最も優れたメディア セットが自動的に選択されます。 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 セットは避けられます。 オブジェクトの完了ステータス、可用性、および特定のメディア 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

宛先 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

デフォルトでは、選択したデータはバックアップ時に使用したのと同じデバイスを使って復元されます。 また、同じ種類の異なるデバイスを使ってデータを復元することもできます。 さらに、選択したデバイスが無効または使用中の場合など、デバイスを使用できない場合の処理を指定することもできます。

- 元のデバイスの選択：
  Data Protectorはデバイスが使用可能になるまで待機します。 これは、Data ProtectorのSAP DB/MaxDB用統合ソフトウェア、IBM UDB DB2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。

- デバイスの自動選択(デフォルト):
  Data Protectorは、使用できないデバイスがあれば、互換性のある使用可能なデバイスに自動的に交換します。 互換性のあるデバイスは、構成時にデバイスのサブタイプを同じ名前にすることで定義できます。 デバイスのサブタイプは、同じライブラリにあり、同じメディアの種類を持つデバイス(ドライブ)のみに同じ名前が与えられます。 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。

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(例えば復元処理の請求には必ず電子メールを使い、オペレータが目的のファイルを見つけてエンド ユーザーのシステム上に復元するために必要となる情報を、すべてこのメール内に記入する、など)。 またエンド ユーザーに、ファイルが復元されたことを知らせる方法も、取り決めておく必要があります。

復元する権限をエンド ユーザーにも付与

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

この方針が適している場合

この方針は、以下の場合に適用します。

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

必要な作業

この方針を実施するには、以下の作業が必要になります。

- Data Protectorのend usersユーザー グループに、自分自身のデータを復元できるエンド ユーザーを追加します。 セキュリティ面を強化するために、これらのユーザーがData Protectorへのアクセスに使用できるシステムを制限することも可能です。
- 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、さまざまなディザスタ リカバリの概念について簡単に説明します。 詳細なディザスタ リカバリの概念、計画、準備、および手順については、HP Data Protector ディザスタリカバリガイドで説明します。

コンピュータ障害とは、 人的エラー、ハードウェアまたはソフトウェアの障害、自然災害などにより、コンピュータ システムがブート不可能な状態になるイベントを指します。 通常このような状況が発生した場合は、システムのブート パーティションやシステム パーティションが使用不能になっているため、標準的な復元作業を開始する前に、まず環境を復旧しなければなりません。 このためには、ブート パーティションの

再作成や再フォーマット、環境を定義するすべての構成情報を含めたオペレーティングシステムの再構築などを実行する必要があります。 *最初にこの作業を完了しておかなければ、その他のユーザ データを復旧できません。*

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。 クラッシュしたシステムとは異なり、ターゲット システムの場合は、障害が発生したハードウェアはすべて交換されています。

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. 今から **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. 今から 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。 つまり、ASR はData Protectorディスク、ネットワーク、テープ、およびファイル システムへのアクセスを行うアクティブなDR OSをインストールするData Protectorの drstart.exeコマンドを実行可能にします。
- 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、クラッシュしたシステム上のディスク(またはディスクが物理的に損傷している場合は交換用のディスク)を、ホスティング システムに一時的に接続します。 復元後、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 クライアントおよびCell Manager向けの高度に自動化されたData Protector復旧方法であり、ユーザーの介入は最小限で済みます。 システムはOBDRテープからブートされ、自動的に復旧されます。

個々のオペレーティング システムでサポートされるディザスタ リカバリの手法のリストについては、『HP Data Protector product announcements ソフトウェアノートおよびリファレンス』のサポート一覧か以下のWebサイトを参照してください。

http://www.hp.com/support/manuals

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、他社製品のディザスタ 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 システムを一からインストールし直します。

2. アプリケーションを再インストールします。
3. アプリケーション データを復元します。

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

他社製ツールを使った復旧(Windowsの場合)

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

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

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

一方Data Protectorは、複数のプラットフォームにまたがる包括的で強力な企業向けソリューションであり、バックアップや復元の機能を持ち、クラスタ化にも対応しているため、高速かつ効率的にディザスタ 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 メディア管理とデバイス

この章の内容

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

この章の構成は以下のとおりです。

メディア管理

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)。
- メディアの自動交換方針を設定でき、テープを手動で交換する必要がありません。
- 特定のバックアップに使用するメディアとデバイスを明示的に定義できます。
- デバイスの種類(スタンドアロン デバイス、マガジン デバイス、ライブラリ デバイス、大容量のサイロ デバイスなど)に合わせて、それぞれに最適な形でメディアを管理できます。
- 完全な自動処理が可能です。 ライブラリ デバイス内に十分な数のメディアを用意しておけば、メディア管理機能により、何週間にもわたってオペレータによるメディア交換の必要なしにバックアップを実行できます。
- バーコードに対応した大容量ライブラリやサイロ デバイスに対して、バーコードの認識とサポートが可能です。
- Data Protectorのメディア フォーマットやその他の一般的なテープ フォーマットを自動認識できます。
- Data Protectorでは、Data Protectorで初期化(フォーマット)した空のメディアにのみ書き込みを行います。 バックアップ時に、他のフォーマットのテープに上書きすることはないため、他のアプリケーションが使っているメディアに偶発的にデータを上書きする危険はありません。
- ライブラリ デバイスおよびサイロ デバイス内で、Data Protectorが使用しているすべてのメディアを認識、トラッキング、ブラウズ、および操作でき、これらのメディアを他のアプリケーションが使用しているメディアと区別できます。
- 使用中のメディアに関する情報を中央で一元管理し、複数のData Protectorセル間でこの情報を共有できます。
- メディア ボールティング(安全な場所でのメディアの保管機能)がサポートされています。
- メディアのデータの追加コピーを対話的または自動的に作成します。

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。

   詳細については、「バックアップ開始前のメディア管理」 (136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。

   詳細については、「バックアップ セッション中のメディア管理」 (137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。

   ボールティングの詳細は、「バックアップ セッション後のメディア管理」 (142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(Poor)マークが付加され、Data Protectorでは使用されなくなります。

   詳細は、「メディア状態の計算」 (141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。 例えば一つのメディア プール内にDLTメディアとDAT/DDSメディアを混在させることはできません。

メディアが現在どこに存在するかは、プールとの対応付けには関係ありません。 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メディアがあるかどうかは問題ではありません。 セルからリサイクルまたは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(Appendable)
  このオプションを設定すると、バックアップ セッションの実行時に、プール内のメディアの空きスペースにデータが書き込まれます。

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

- [増分のみ追加可能(Appendable on Incrementals Only)]
  バックアップ セッション時には、増分バックアップが実行された場合に限り、メディアにデータが書き込まれます。 そのため、メディア内に十分なスペースが残っている場合には、フル バックアップと増分バックアップがすべて同一のメディア上に保存されるようになります。
- メディア割り当てポリシー
  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が、バックアップ仕様内でこのプールを変更することも可能です。

その他のメディア プールのプロパティの詳細は、オンライン ヘルプでキーワード「メディア プール」から「プロパティ」を指定して確認してください。

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」 (179ページ) を参照してください。

メディア プールの使用方法

カラーマネージメントを行うには、オペレーティング システムからの場合もアプリケーションからの場合も 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。例えば、以下のような基準でプールを定義できます。

- システム プラットフォームごと(UNIXシステム用、Windows 2000システム用、Windows XP用に、それぞれ個別のプールを設定するなど) 。
- システムごと(各システムごとに個別のプールを設定するなど)。
- 組織構造ごと(部門Aの全システム用に1つのプールを設定し、部門Bの全システム用にもう1つ別のプールを設定するなど)。
- システムのカテゴリごと(大容量データベースを実行するシステムや、基幹業務を実行するシステムなどについて、それぞれ個別のプールを設定するなど)。
- バックアップの種類ごと(すべてのフル バックアップ用に1つのプールを設定し、すべての増分バックアップ用にもう1つ別のプールを設定するなど)。
- 上記の条件の組み合わせ。 その他。

メディア プールの概念を簡単に理解するには、これらのプールをバックアップ データの保存先と考え、またデバイスは、バックアップ データとメディア プール間の転送メカニズムであると考えてください。

あるシステム カテゴリと目的のプールとを対応付けるには、対象となるシステムを同一のバックアップ仕様内ですべてリストアップし、使用するプールを指定します。 オブジェクト データがメディア上にどのように保存されるかは、デバイス、プール、およびバックアップ仕様の定義時に指定したオプションに基づいて決定されます。

このように、同一タイプのバックアップに使用するメディアを1つのメディア プール内にまとめておくと、グループ レベルで共通のメディア取り扱い方針を適用できるため、各メディアを個別に管理する必要がなくなります。 プール内の全メディアは1つのセットとしてトラッキングされ、同一のメディア割り当て方針が適用されます。

デフォルト メディア プール

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

フリー プール

あるメディア プールに割り当てたメディアの容量が不足した場合、同じ種類であっても他のプールにあるメディアを代用することはできません。 他のプールのメディアを使用すると、不要なマウント要求が発生してオペレータによる操作が必要になります。 この問題を解決するにはすべてのメディアを1つのプールに配置するシングル プール モデルを使用します。 この方法ではフリー メディアを共有できますが、メディア プールを使用する第1の利点(メディア管理の利便性、重要度に基づくデータの分類など)を活用できなくなります。 この問題点をカバーするためにフリー プールを使用します。

フリープールとは

フリー プールは、同じ種類のメディア(DLTなど)で構成される補助ソースで、通常のプール内にあるすべてのフリー メディアが不足した場合に使用します。 メディア(フリー メディア)不足に起因するバックアップの失敗を防止するのに役立ちます。

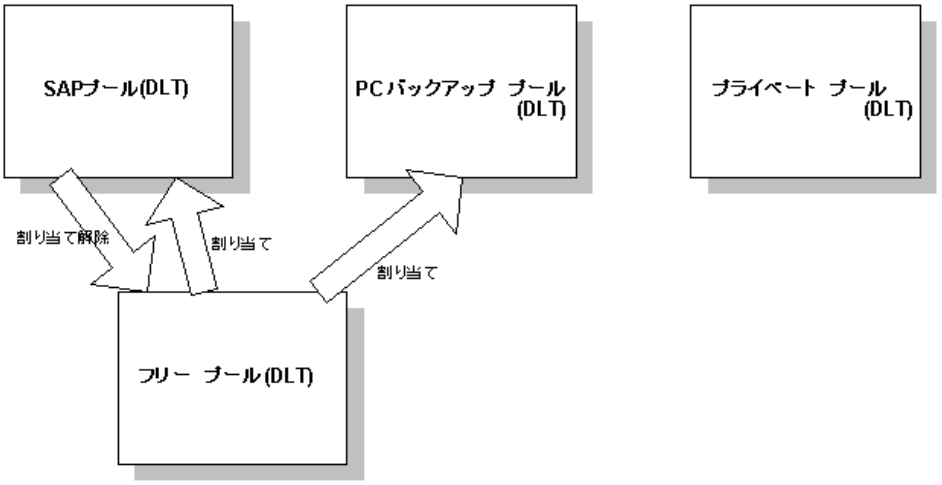

図 36 フリー プール

フリー プールを使用するタイミング

メディアは、以下の2つのイベント時に通常のプールとフリー プールの間で移動されます(図 36 (130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。 図 36 (130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。

図 36 (130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(例えば無期限に変更)すると、メディアがフリー プール内にあってもバックアップ用に割り当てられません。
- フリー プール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 プールについての詳細は、Data Protectorのオンライン ヘルプで「フリー プール」をキーワードに指定して確認してください。

メディア プールの使用例

バックアップ環境を選択する上で考慮可能な構成例を以下に示します。

例1

図 37（132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。

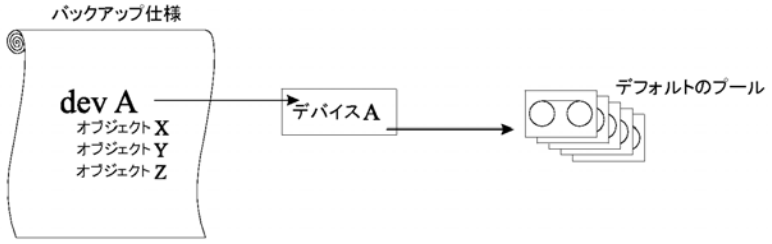

図 37 単一デバイス/単一メディア プールの単純な対応付け

例2

大容量ライブラリ デバイス内には、多数の物理ドライブが装備され、さまざまな部門やアプリケーションで使われる多数のメディアが格納されています。 この場合、図 38（133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」（152ページ）を参照してください。

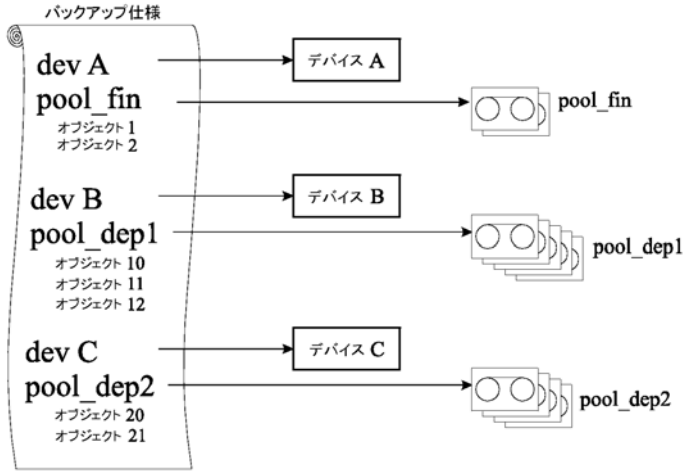

図 38 大容量ライブラリを使用する場合のメディア プール構成例

例3

図 39（133ページ）は、複数のデバイスから、同一メディア プール内のメディアに、データを同時にバックアップする場合の例を示したものです。 どのプールを使用するかにかかわらず、複数のデバイスを並列に使用すると、性能は向上します。

詳細については、「デバイス リストと負荷調整」（145ページ）を参照してください。

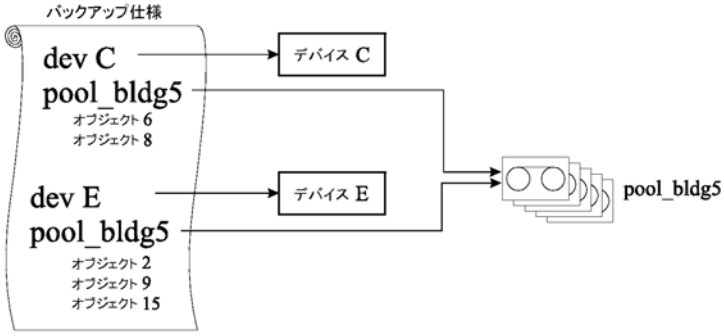

図 39 複数デバイスと単一メディア プールの対応付け

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。

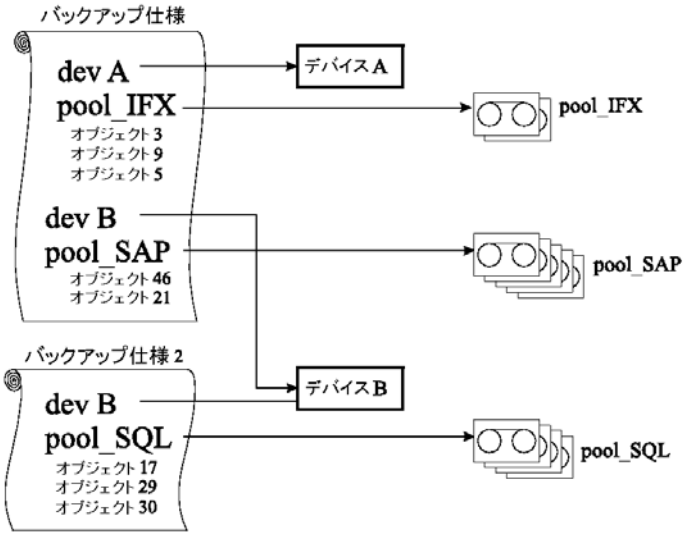

図 40 複数デバイスと複数メディア プールの対応付け

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

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

自動メディア交換と自動メディア操作

- 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方針と使用オプションに基づいて、メディア プールから自動的にメディアが選択されます。 必要に応じて、自動選択機能を無効にし、手動でメディアを選択することも可能です。
- Data Protectorで構成したメディアについては、Data Protectorユーザー インタフェースを使用して、メディア位置のトラッキングおよび表示が可能です。
- Data Protectorでは、メディアの上書き回数と使用年数がトラッキングされており、メディアの状態が常に把握されています。
- Data Protectorにはセキュリティ機構が備わっているため、保護されたデータが入っているメディアが、Data Protectorにより偶発的に上書きされる危険はありません。

メディア交換に必要なメディアの数

必要なメディア数の見積もり

次の点を検討すると、フル メディア交換で必要になるメディアの総数を見積もることができます。

- 各メディアの容量について、完全に使い切るようにするのか、またはメディアによっては追記不可能として一部分しか使わないようにするのかを決定します。
- バックアップ対象となるシステムと、バックアップ データの保存に必要なメディア スペースを明らかにします。 この作業には、バックアップ プレビューが役立ちます。
- 2つのフル バックアップ間で実行する増分バックアップの回数など、バックアップの頻度を決定します。
- 1つのバックアップ世代で必要となるメディアの量を明らかにします。 1つのバックアップ世代の中には、1つのフル バックアップと、次回のフル バックアップまでの間に実行される一連の増分バックアップがすべて含まれます。 複数のデバイスを使用する場合は、ハードウェア圧縮の使用も検討してください。
- メディアの保護期間を決定します。
- 何世代分のバックアップを保持するかを決定します。 この数を超えれば、一番初めに作成したバックアップ世代を上書きします。

以上の点を明らかにすると、フル メディア交換で必要となるメディアの総量を見積ることができます。 メディア量については、さらに以下の点を考慮する必要があります。

- ディレクトリおよびファイル情報用として、メディア上のデータの約10％分のオーバーヘッドがメディアに追加されます。 この情報はバックアップのプレビュー サイズに計算済みです。
- メディアの最大使用期限が切れたら、メディアを交換しなければなりません。
- バックアップするデータ量の増加も予測する必要があります。

バックアップ開始前のメディア管理

バックアップ用にメディアを使用するためには、まずそのメディアをData Protectorで使用できるように初期化(フォーマット)しなければなりません。 メディアの初期化(フォーマット)は、手動で行っておくこともできれば、バックアップ用にメディアが選択された時点で、Data Protectorにより自動的に初期化(フォーマット)されるように設定しておくことも可能です。 詳細は、「バックアップ用メディアの選択 」 (138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)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。 詳細については、「バックアップ用メディアの選択 」 (138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。 例えば、メディア上に新しいバックアップ情報を書き込もうとした場合、メディア管理システムにより、メディア上の既存データの保護期限が切れているかどうかがチェックされます。 ユーザー定義のラベルは、メディアを識別するために使用します。

[位置(Location)]フィールド

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

各メディアの[位置(Location)]フィールドは、オペレータが自由に変更できます。 このフィールドを使用すると、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」 (118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、以下の項も参照してください。

- 「フル バックアップと増分バックアップ」 (64ページ)
- 「メディア プール」 (127ページ)

バックアップ用メディアの選択

Data Protectorでは、メディア割り当て方針に基づいて、バックアップ用メディアが自動的に選択されます。 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。

メディア割り当て方針

バックアップ用メディアの選択方法は、 メディア割り当て方針に基づいて決定されます。 方針に[Loose]と指定した場合は、新しいメディアや空のメディアも含めて、適切な任意のメディアが使用されるようになります。 一方[Strict]と指定した場合には、メディアの使用状況を均一化するために、事前に定義された順番でメディアがロードされなければなりません。 さらに事前割り当てリストを使用することも可能です。

事前割り当てメディア

Data Protectorでは、事前割り当てリストを使用して、メディア プール内のどのメディアをバックアップに使用するかを明示的に指定できます。 このリストは、メディア割り当て方針の[Strict]と組み合わせて使用してください。 この場合、メディアは指定された順番どおりに使用されます。 この順番どおりにメディアが見つからなければ、Data Protectorによりマウント要求が発行されます。

メディア状態

バックアップ用メディアの選択時には、各メディアの状態も考慮されます。 例えば、状態が[良好(Good)]のメディアは、状態が[普通(Fair)]のメディアよりも優先的に使用されます。 詳細については、「メディア状態の計算」 (141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、メディア使用方針で設定します。

メディア使用方針

選択できるメディアの使用方針は、以下のとおりです。

[追加可能(Appendable)]	バックアップ セッション時には、まず初めに、前回のバックアップ セッションで最後に使用されたメディア上に残っているスペースにデータが書き込まれます。 このセッションで2本目以降に使われるメディアについては、テープの先頭からデータが書き込まれるため、保護期限が切れているテープまたは新しいテープのみが使用されます。 この方針を選ぶとメディア スペースを節約できますが、1つのメディア内に複数のメディア セットのデータが含まれる可能性があるため、ボールティング作業は多少複雑になります。
[追加不可能(Non Appendable)]	バックアップ セッション時には、使用可能な最初のバックアップ用メディアの先頭から、データが書き込まれます。 各メディアには単一セッションからのデータのみが格納されるため、ボールティング作業が容易になります。
[増分のみ追加可能(Appendable on Incrementals Only)]	バックアップ セッション時には、増分バックアップが実行された場合に限り、メディアにデータが書き込まれます。 そのため、メディア内に十分なスペースが残っている場合には、フル バックアップと増分バックアップがすべて同一のメディア上に保存されるようになります。

オブジェクトのメディアへの分散

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

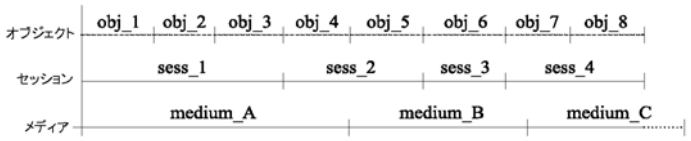

図 41 1つのメディア上に複数セッションの複数オブジェクトを格納（順次書き込み）

図 41 (139ページ) では、メディア使用方針に[追加可能(Appendable)]を指定した状態で、4つのセッションにわたって、8つの順次書き込みを実行しています。 データは、4つのセッションにわたって書き込まれますが、1度に書き込まれるオブジェクトは1つだけになります。 3つのメディアは、同一のメディア プールに所属しています。 *medium_A*と*medium_B*はすでに一杯になっていますが、*medium_C*にはまだ多少のスペースが残っています。

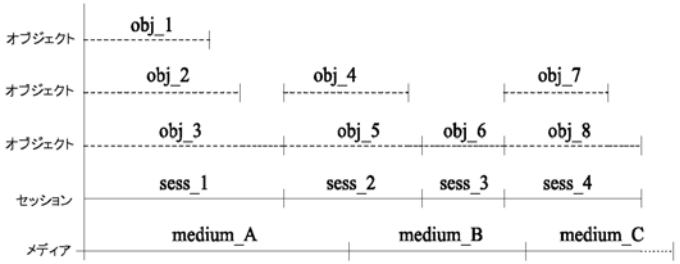

図 42 1つのメディア上に複数セッションの複数オブジェクトを格納（並列書き込み）

図 42（140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*および*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。 メディア使用方針は、[追加可能(Appendable)]に設定されています。

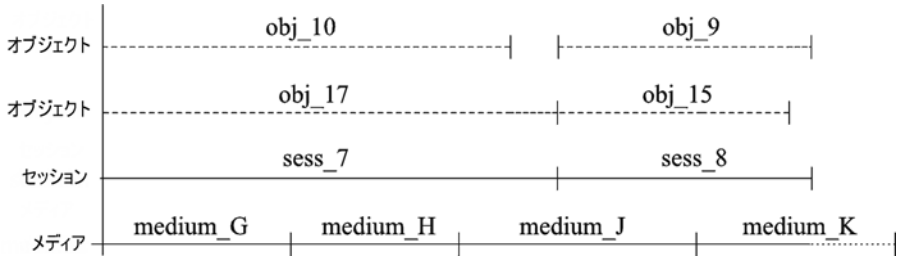

図 43 1セッションあたり複数のメディアを使用し、1つのオブジェクトを複数のメディアに格納

図 43（140ページ）の例では、2つのセッションで4つのオブジェクトをバックアップしており、バックアップ オブジェクトの最初のペアは*sess_7*で、2番目のペアは*sess_8*で、それぞれ同時に書き込まれます。 この場合、1つのオブジェクトが、複数のメディアにまたがって書き込まれる可能性があることに注目してください。 メディア使用方針は、[追加可能(Appendable)]に設定されています。

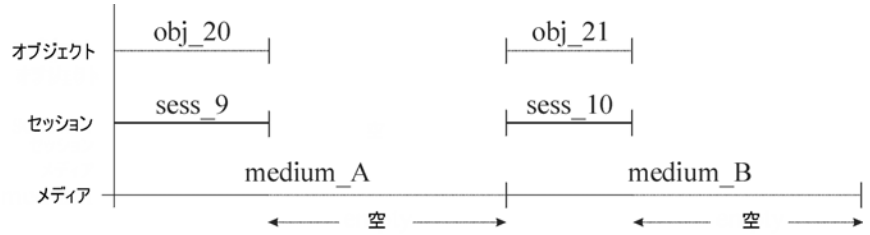

図 44 各オブジェクトを個別のメディアに格納

図 44 (141ページ) の例では、オブジェクトごとに1つのバックアップ仕様を作成し、メディア使用方針には[追加不可能(Non Appendable)]を指定しています。 この方法では、メディアの消費量が多くなります。 この方法で、メディア使用方針を[増分のみ追加可能 (Appendable on Incrementals Only)]に変更すると、同一オブジェクトの増分バックアップのみが同じメディア上に保存されるようになります。

フル バックアップと増分バックアップに対する方針が、復元性能とメディア使用量に与える影響は、「フル バックアップと増分バックアップ」 (64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。 詳細については、「オブジェクト ミラーの作成」 (112ページ) をご覧ください。

メディア状態の計算

メディアの状態要素

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

メディアは、良好(Good)、普通(Fair)、不良(Poor)の3つの状態になる可能性があります。

各メディアについて以下を使用し、状態を計算します。

- 上書き回数
  メディアの使用回数は、そのメディアが上書きされた回数として定義されます。メディアの上書き回数が指定されたしきい値を超えると、不良(Poor)マークが付加されます。
- メディアの使用期間

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

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

バックアップ セッション後のメディア管理

データをメディア上に保存した後は、そのメディアおよびメディア上のデータを、適切に保護しなければなりません。 以下の点に注意してください。

- 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。 データ保護とカタログ保護は、「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」 (91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。
  詳細は、「バックアップ データの複製」 (104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**(media location)]を調べると、メディアが保管されている物理的位置を確認できます。
- 指定した期間内に使われたバックアップ メディアに関するレポートを作成できます。
- 指定したメディアをバックアップ中に使用したバックアップ仕様に関するレポートを作成できます。
- 指定した位置に保管されており、かつ指定した期間内にデータ保護期限が切れるメディアに関するレポートを作成できます。

- 復元に必要なメディアの一覧と、そのメディアが保管されている物理的位置を表示できます。
- 一定の基準に基づいて、メディア ビューに表示するメディアをフィルタリングできます。

ボールティングの実施

ボールティングの実施方法は、各企業のバックアップ戦略と、データおよびメディアに対する取り扱い方針によって異なります。 一般的な実施手順は、以下のようになります。

1. バックアップ仕様を構成するときに、適切なデータ保護期間とカタログ保護期間を設定します。
2. Data Protector内でボールトを構成します。 これは基本的には、そのメディアを保管するボールトの名前を指定するだけの作業です(Vault_1など)。
3. ボールト内のメディアに対する適切な保守方針を設定します。
4. 必要に応じてボールティング用にバックアップしたデータの追加コピーを作成します。 バックアップ時にオブジェクト ミラー機能を使うか、バックアップ後にオブジェクト コピーまたはメディア コピー機能を使います。
5. ボールトに移すメディアを選択し、そのメディアを取り出して、ボールトに格納します。
6. ボールトに格納されているメディアのうち、保護期限が切れたものを取り出して、ライブラリ内に戻します。

ボールティングの例

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」 (91ページ) を参照してください。.

デバイス

Data Protectorは、市販されているさまざまなデバイスをサポートしています。 サポート対象デバイスの最新情報は、『HP Data Protector product announcements 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。

Data Protectorでのデバイスの使用

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

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

ライブラリ管理コンソールのサポート

現在使われているテープ ライブラリの多くは、リモート システムからライブラリを構成、管理、監視するための管理コンソールを備えています。 リモートから実行できる作業の範囲は、各ライブラリに実装されている管理コンソールによって異なります。 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、『HP Data Protector product announcements 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。

重要：

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

TapeAlert

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

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

デバイス リストと負荷調整

複数のバックアップ デバイスの使用

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

デバイス使用率の平均化

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

負荷調整の使用に適している場合

以下の場合は、負荷調整を使用してください。

- 多数のオブジェクトをバックアップする場合。
- 複数のドライブを持つライブラリ(オートチェンジャ)デバイスを使用する場合。
- オブジェクトがどのメディアにバックアップされるかを知る必要がない場合。
- 高性能なネットワーク接続がある場合。
- バックアップの頑健性を高めたい場合。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(Concurrency)には通常1を指定すれば十分です。

デバイスストリーミングの構成方法

デバイス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。 例えば標準的なDDSデバイスの場合であれば、2つのDisk Agentにより、ストリーミングの維持に十分なデータをデバイスに送信できます。 また、ライブラリ デバイス内に複数のドライブがあり、各ドライブが個別のMedia Agentで制御される場合には、それぞれのドライブごとに個別に同時処理数を設定できます。

性能の向上

バックアップの同時処理数を適切に設定すると、 バックアップ性能が向上します。例えば4つのドライブを持つライブラリ デバイスがあり、各ドライブは個別のMedia Agentで制御されているとします。 このとき、個々のMedia Agentがそれぞれ2つ

のDisk Agentから同時にデータを受け取ると、8つのディスク上のデータを同時にバックアップできます。

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

関連情報は、「バックアップ セッション」（208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 セグメントから構成されています。 ヘッダ情報は、ブロック サイズと同じ長さのヘッダ セグメントに格納されます。 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メモリに格納され、次にメディア内のカタログ セグメントと、IDBに書き込まれます。 図 45（149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。

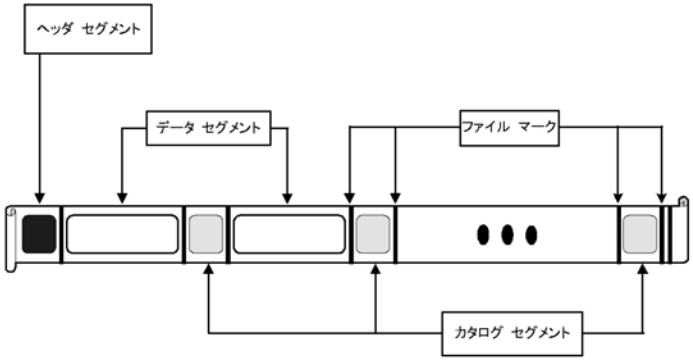

図 45 データ フォーマット

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。 例えば、DLTメディアのデフォルトのセグメント サイズは150MBです。

Block size

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

注記：

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 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。

- メモリの不足
  Media Agentが必要とする共有メモリのサイズは、次のように計算できます。
  DAの同時処理数*バッファ数*ブロックサイズ
  例えばバッファ数を8から4に減らすと、メモリ消費量は約50%削減されますが、性能にも影響が及びます。
- ストリーミング
  利用可能なネットワーク帯域幅がバックアップ中に大きく変動する場合は、デバイスのストリーミングを維持するために、Media Agentが十分な書き込み用データを確保できることが特に重要になります。 このような場合は、バッファ数を増やしてください。

デバイス ロックとロック名

デバイス名

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

物理デバイスの衝突

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

衝突の防止

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。

たとえば図 46（151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。

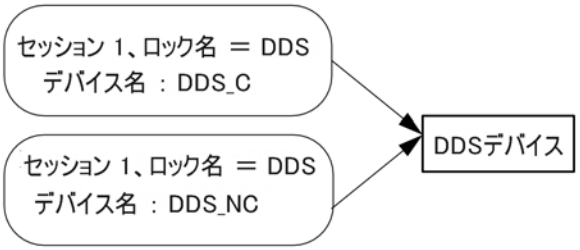

図 46 デバイス ロックとデバイス名

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 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。 サポート対象のデバイスの一覧は、『HP Data Protector product announcements 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。

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。 例えば、4つのドライブを備えたライブラリの場合には5つのSCSI IDが必要になります(ドライブ用に4つ、ロボティクス用に1つ)。

Data Protectorは、 HP StorageWorksライブラリ、StorageTek/ACSLS、ADIC/GRAU AMLなどのサイロ ライブラリもサポートしています。 サポート対象のデバイスの一覧は、『HP Data Protector product announcements 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。

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。 詳細は、「メディア交換方針の実装」(134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。 例えば4つのドライブを持つライブラリであれば、そのうち2つのドライブのみをData Protectorで使用するというように設定します。

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

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

挿入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。

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

バーコード サポート

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

バーコードの利点

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

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

ヒント：

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

クリーニング テープのサポート

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

- SCSIライブラリでは、クリーニング テープを格納するスロットを定義できます。
- バーコード リーダーを備えたデバイスで、クリーニング テープのバーコードの先頭をCLNとしておくと、Data Protectorによりクリーニング テープが自動的に認識されます。
- クリーニング テープが用意されていないデバイスで、ドライブの汚れが検出された場合は、セッション モニター ウィンドウ上にクリーニング要求が表示されます。 この場合は、オペレータが手動でデバイスをクリーニングしなければなりません。
  ドライブが汚れていると、メディア上にデータを正しく書き込めず、バックアップが失敗する可能性があるため、ドライブをクリーニングするまではバックアップを続行できないようになっています。

複数システムによるライブラリの共有

ライブラリの共有とは

デバイス共有機能を利用して、物理ライブラリ内の各ドライブを、個別のシステムに接続することも可能です。 こ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。

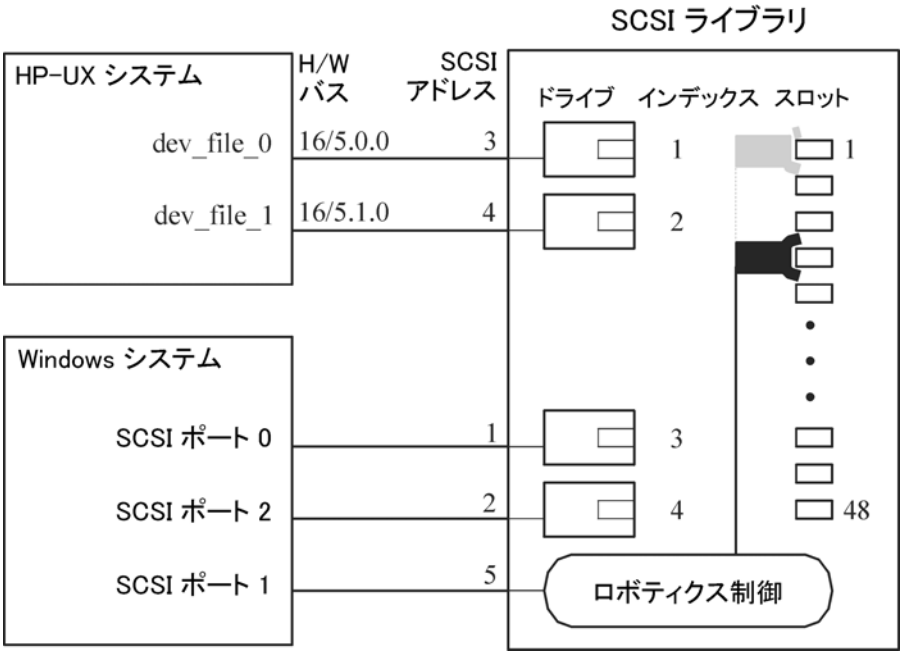

図 47 ドライブを複数のシステムに接続

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

表 10 (157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 10 ドライブ制御に必要なData Protector Media Agent

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

ロボティクス制御

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

表 11 (158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 11 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

図 48（159ページ）から図 50（161ページ）までの図は、ライブラリのドライブを共有する構成と、そのような構成でのData Protector Media Agentの分散に関する例を示しています。

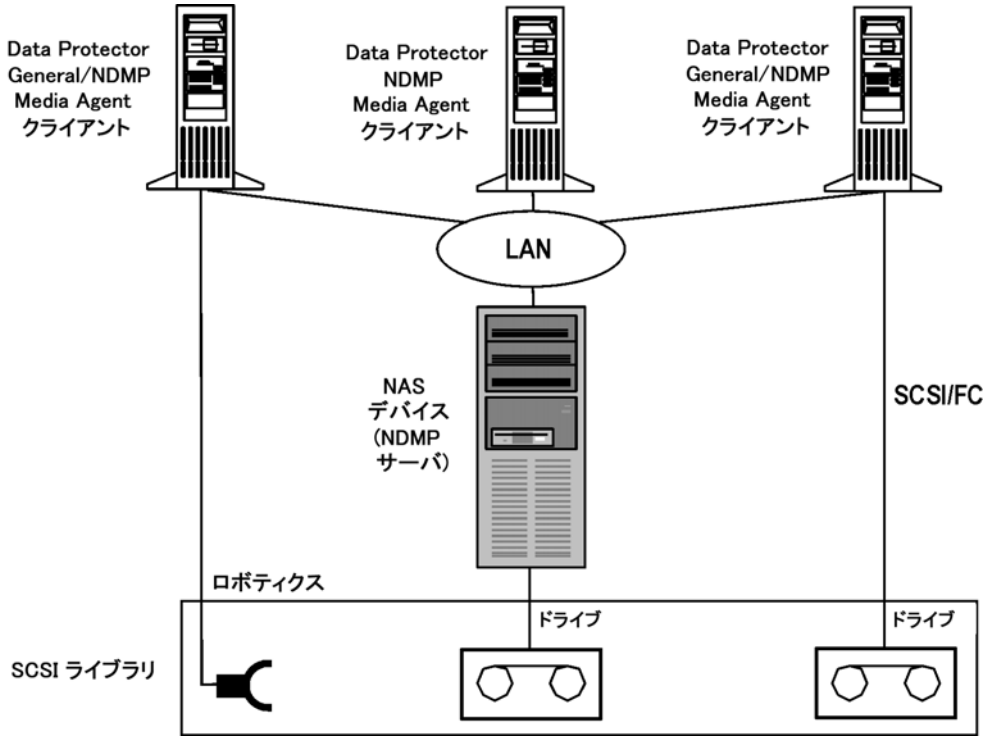

図 48 SCSIライブラリの共有(ロボティクスをData Protectorクライアント システムに接続)

図 48 (159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。

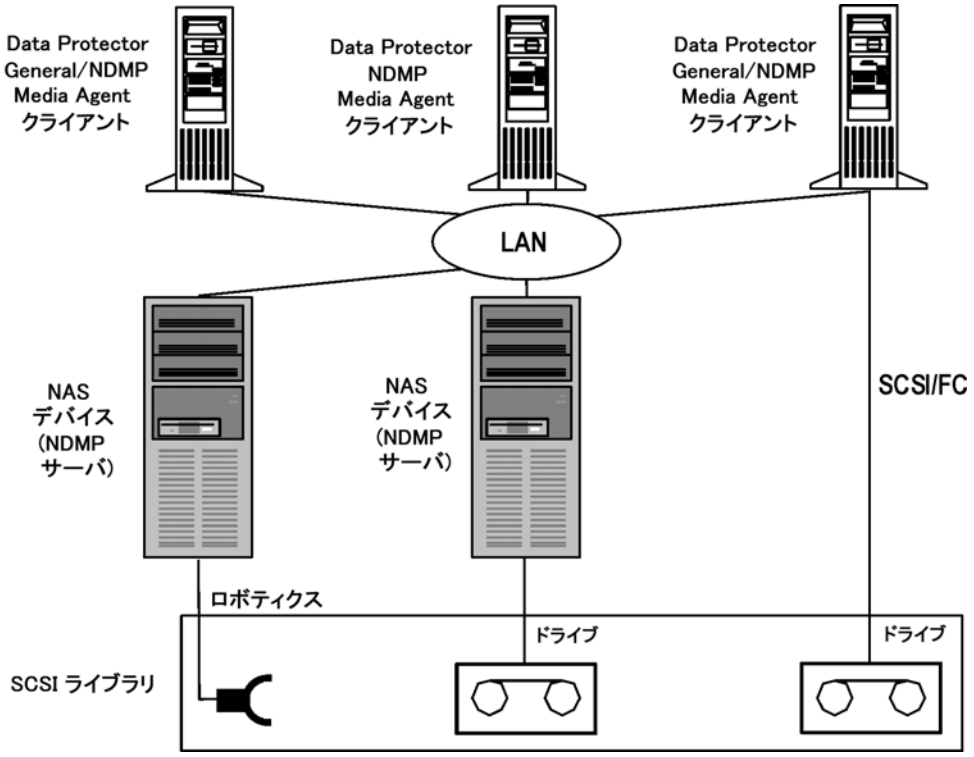

図 49 SCSIライブラリの共有(ロボティクスをNDMPサーバに接続)

図 49（160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サーバに接続され、General Media AgentまたはNDMP Media Agentのインストールされた Data Protectorクライアント システム上に構成されています。 このクライアント上のGeneral Media AgentまたはNDMP Media Agentは、SCSIロボティクス制御プロトコルを使用します。 ロボティクスを接続したNDMPサーバに、さらに1つ以上のドライブを接続することも可能です。

重要：

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

ライブラリ内のNDMP専用ドライブは、NDMP Media Agentがインストールされた Data Protectorクライアント システム上に構成されています。 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。

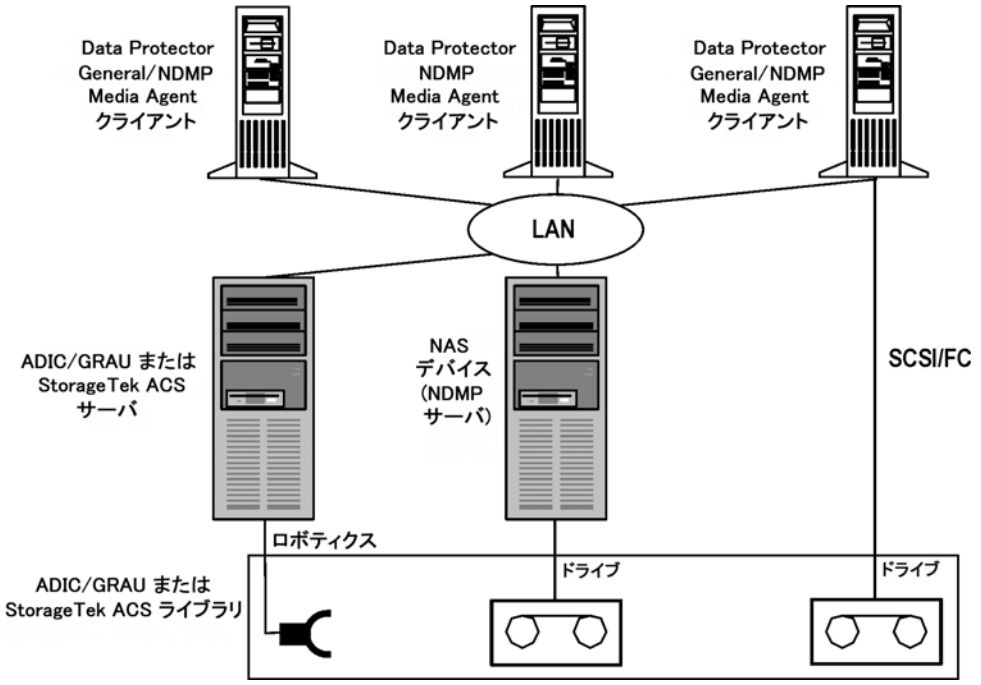

図 50 ADIC/GRAUライブラリまたはStorageTek ACSライブラリの共有

図 50 (161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(またはStorageTek ACSサーバ)に接続され、General Media AgentまたはNDMP Media Agentのインストールされ たData Protectorクライアント システム上に構成されています。 このクライアント上のGeneral Media AgentまたはNDMP Media Agentは、ADIC/GRAUロボティクス制御プロトコルを使用します。 ADIC/GRAUサーバやStorageTek ACSサーバに、さらに1つ以上のドライブを接続することも可能です。

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

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

Data ProtectorとStorage Area Network

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

Storage Area Network

図 51 (163ページ) に示すStorage Area Network (SAN)は、ネットワークを介した記憶管理の新しい方式であり、記憶装置専用のネットワークを使用して、記憶管理とサーバ管理を切り離すことができます。

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

SANの概念を導入すると、複数のデータ記憶デバイスおよびサーバ間での情報交換が可能になります。 サーバは、任意のデバイス上のデータを直接取得でき、従来型のLANを介したデータ転送の必要はありません。 SANは、サーバ、バックアップ デバイス、ディスク アレイ、およびその他のノードから構成され、これらがすべて高速なネットワーク接続(通常はFibre Channel)で接続されています。 この専用の高速ネットワークにより、従来型のLANは記憶装置の処理から解放されます。

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

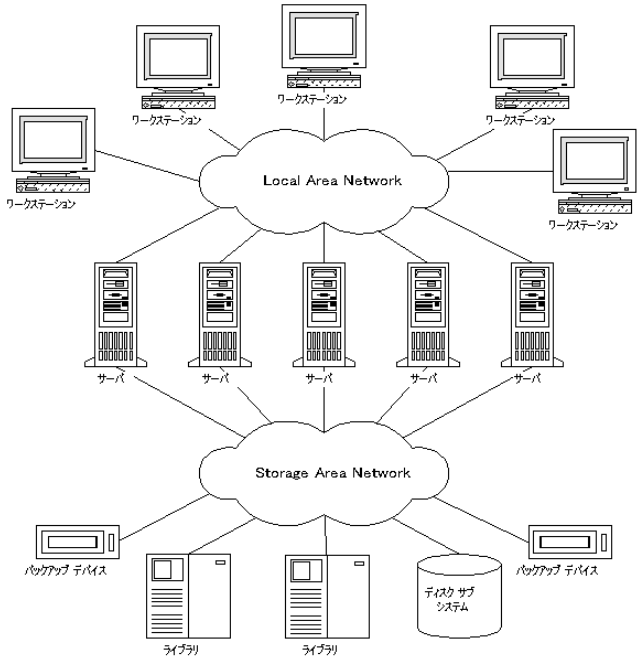

図 51 ストレージ エリア ネットワーク (storage area network)

ファイバ 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。 光ケーブルまたは銅線ケーブルを使って、大容量データ ファイルを最大4.25GB/秒で双方向送信でき、30kmの範囲にあるサイト間を接続できます。 Fibre Channelは情報の格納、転送、および取り出しに関して、現時点における最も信頼性が高く高性能のソリューションです。

Fibre Channelは、ノード間を次の3種類の物理トポロジー(およびそのバリエーション)で接続できます。

- ポイント トゥ ポイント
- ループ
- スイッチ式

ポイント トゥ ポイント、ループ、およびスイッチ式の Fibre Channelトポロジーは、それぞれの環境における接続や将来的な要件に合わせて適宜組み合わせることも可能です。

サポート対象構成の詳細については、『HP Data Protector product announcements ソフトウェアノートおよびリファレンス』またはhttp://www.hp.com/support/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、一般的にはサーバとバックアップ デバイスを接続することができます。 この方法では、性能の向上と長距離間のノードの接続という基本的な利点が得られます。

ループ トポロジー

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

LIP

A LIP (Loop Initialization Primitive)プロトコルはさまざまな場合に起動されますが、最も一般的なのは新しいデバイスが導入された場合です。 新しいデバイスには、すでにループに属していたデバイスに電源を入れたものや、アクティブなデバイスでスイッチ ポートを移動したものもあります。 LIPが起動されると、テープのバックアップ処理など、SAN上の進行中のプロセスが予期せず中断される場合があります。 これによってSCSIブリッジとノード(SCSIデバイス)間のSCSI接続がリセットされます。 詳細は、図 52 (165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。

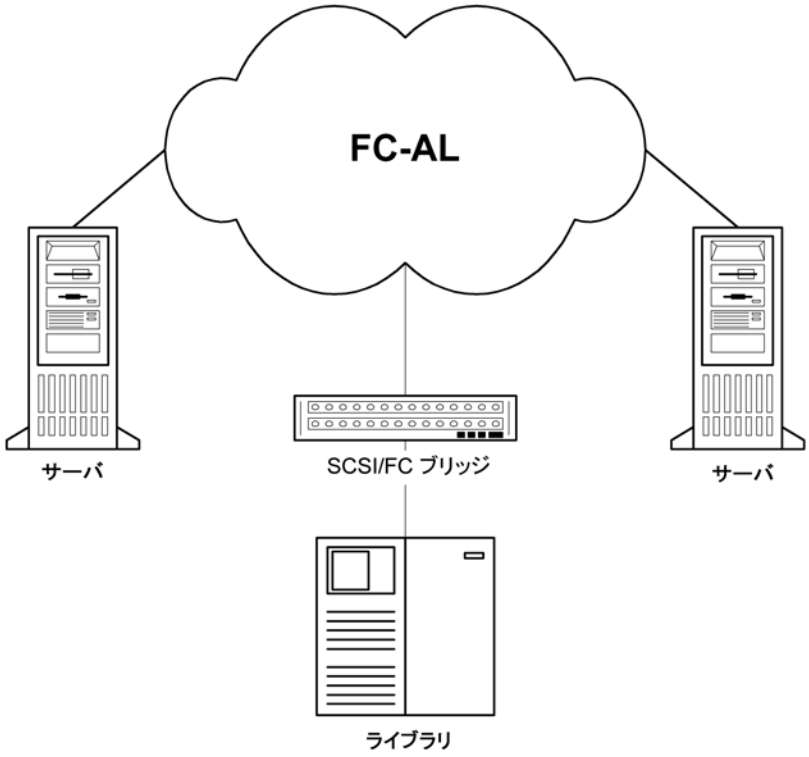

図 52 Loop Initializationプロトコル

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。

例えば、あるデバイスがclient1上では、/dev/rs1および/dev/rs2として、client2上では/dev/r1s1として、またclient3上ではscsi1:0:1:1として構成されています。 このため、client1:/dev/rs1、client1:/dev/rs2、client2:/dev/r1s1、およびclient3:scsi1:0:1:1という4つの異なるパスを通してデバイスにアクセスすることができま す。 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。

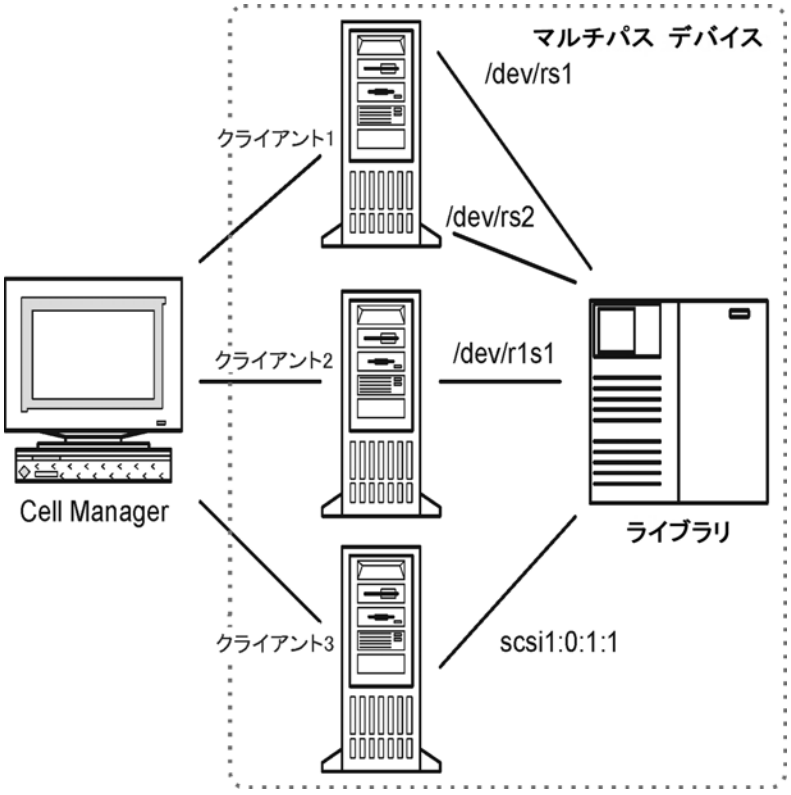

図 53 マルチパスの構成例

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。 図 54（169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 StorageWorks DLTマルチドライブ ライブラリに接続されています。 クライアント システムcastorがロボティクスと最初のドライブを制御しており、クライアント システムpolluxが2番目のドライブを制御しています。 pollux上のData Protector Media Agentがロボティクスを制御するには、castor上で実行されているプロセスと通信する必要があります。 このData Protectorのライブラリ共有機能は、ライブラリやドライブのホスト名が異なっている場合に自動的に使用されます。

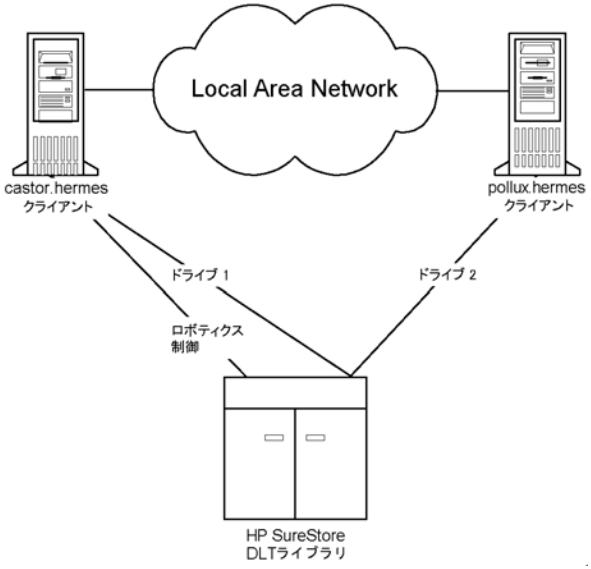

図 54 間接ライブラリ アクセス

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、再構成の必要もありません。 ロボティクスは複数のクライアント システムから制御できます。

図 55（170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 StorageWorks DLTマルチドライブ ライブラリを示したものです。 これらのクライアント システムは、ライブラリと両方のドライブにアクセスできます。 ライブラリとの通信にはSCSIプロトコルが使われています。

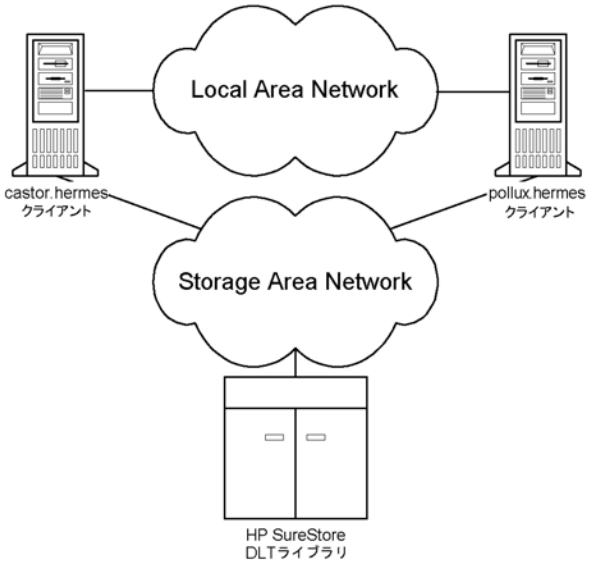

図 55 直接ライブラリ アクセス

クラスタ内のデバイス共有

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

クラスタ対応アプリケーションは仮想ホスト上で実行されるため、その時々でクラスタ内の任意のノード上で実行されている可能性があります。 そのため、これらのアプリケーションをローカル バックアップするには、実際のノード名ではなく仮想ホスト名を指定してデバイスを構成する必要があります。 各物理デバイスに対するデバイス構成

を必要に応じて複数定義し、デバイス ロック機構にはロック名を使用してください。 詳細は、「デバイスのロック」（168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、クラスタ内の実ノード上に構成されるデバイスです。 これらのドライブは、共有されていないディスクを持つシステムのバックアップに使用できます。 ただし、クラスタ対応アプリケーショは、クラスタ内の任意のノードで実行される可能性があるため、これらのアプリケーションのバックアップには静的ドライブは使用できません。

浮動ドライブ

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。クラスタ対応アプリケーションをバックアップする場合は、この浮動ドライブを構成してくださ い。 浮動ドライブを使うと、クラスタ対応アプリケーションが現在どのノード上で実行されていても、Data Protectorはそのノード上で確実にMedia Agentを開始できます。

4 ユーザーとユーザー グループ

この章の内容

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

この章の構成は以下のとおりです。

Data Protectorユーザーに対するセキュリティの強化

Data Protectorには優れたセキュリティ機能が備わっており、権限のないユーザーによるデータのバックアップや復元を防止しています。 Data Protector Data Protectorのセキュリティ機能を使用すると、権限のないユーザーからデータを隠したり、データを暗号化したり、各ユーザーを作業内容に基づいてグループ化したりすることが可能になります。

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、例えばバックアップ オペレータがバックアップを構成したような場合には、そのバックアップ オペレータまたはシステム管理者しかそのデータをブラウズしたり復元したりすることができません。 他のユーザーもこのデータを見ることができるようにするには、Data Protectorの

[**パブリック**]オプションを使用します。 詳細については Data Protector のオンライン 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モニター、バックアップの構成、ファイルの復元など)を持つユーザー グループにまとめられます。

事前定義されたユーザー グループ

バックアップ構成を簡略化するために、Data ProtectorではData Protector機能にアクセスするための特定の権限を持つ事前定義されたユーザー グループを用意しています。 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。

ヒント：

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

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

[Admin]ユーザー グループのデフォルトのメンバー

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

- UNIX Cell Managerシステム上のUNIX rootユーザー
- Windows Cell Managerシステムに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。 詳細については、Data Protector のオンライン ヘルプでキーワード「ユーザー グループ」から「admin」を指定して確認してください。

事前定義されたユーザー グループの使用

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

表 12 Data Protectorの事前定義されたユーザー グループ

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

注記：

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

Data Protectorユーザー権限

Data Protectorユーザーには、各自が所属するユーザー グループのData Protectorユーザー権限が与えられます。 例えば、[Admin]ユーザー グループのすべてのメンバーには、Data Protector [Admin]ユーザー グループの権限が与えられます。

UNIX Cell Manager上で実行されているData Protector内のWindowsドメインからユーザーを構成する場合は、構成時にドメイン名またはワイルドカード グループ "*" を指定する必要があります。

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

5 Data Protector内部データベース

この章の内容

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

この章の構成は以下のとおりです。

IDBについて

Data Protector内部データベース(IDB)とは

IDBはCell Manager上に置かれる埋め込みデータベースです。 バックアップ対象のデータとバックアップ データの格納先メディアのほか、バックアップ、復元、コピー、オブジェクト集約、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

メッセージ送信に IDBを使用する3つの主な理由を以下に示します。

- 復元が高速で便利。IDBに保存されている情報によって復元に必要なメディアを迅速に検出できるため、復元を高速に行うことができます。 また復元対象のファイルやディレクトリをブラウズすることもできます。
- バックアップ管理が可能。IDBに保存されている情報によって、どのようにバックアップが行われたかを確認できます。 Data Protectorのレポート機能を使用して、さまざまなレポートを作成することも可能です。
- メディア管理が可能。Data Protectorでは、IDBに保存されている情報によって、バックアップ セッションやコピー セッション、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。

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の管理者はIDBについてよく理解し、必要に応じて、IDBに保存する情報とその期間を熟考する必要があります。 復元にかかる時間や機能と、IDBのサイズとサイズの増大との間のバランスを取ることは、管理者の役目になります。このニーズのバランスを取るために、Data Protectorでは重要な次の2つのパラメータを用意しています。 **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」 (186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。

詳細は、「国際化」 (328ページ) を参照してください。

Manager-of-Managers環境のIDB

Manager-of-Managers (MoM)環境では、 メディア集中管理データベース(CMMDB)を使用できます。CMMDB を使用すると、複数のセル間でデバイスやメディアを共有できます。 MoM機能の詳細は、「企業環境」 (38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)
- CDB(カタログ データベース)。ファイル名とその他のCDBレコードの部分に分割
- DCBF (詳細カタログ バイナリ ファイル)
- SMBF (セッション メッセージ バイナリ ファイル)
- SIBF (NDMP統合用のサーバレス統合バイナリ ファイル)

以上のIDBの構成要素は、それぞれ特定のData Protector情報(レコード)を保存しており、IDBのサイズやサイズの増大にさまざまな点で影響を与えます。 各構成要素はCell Manager上の別々のディレクトリに配置されています。 図 56 (180ページ) を参照してください。

データベースの強度に関する注意点やIDBディレクトリの再配置によるデータベース強度の最適化に関する推奨事項については、オンライン ヘルプでキーワード「IDBの堅牢性」を指定して確認してください。

基礎となる技術

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

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

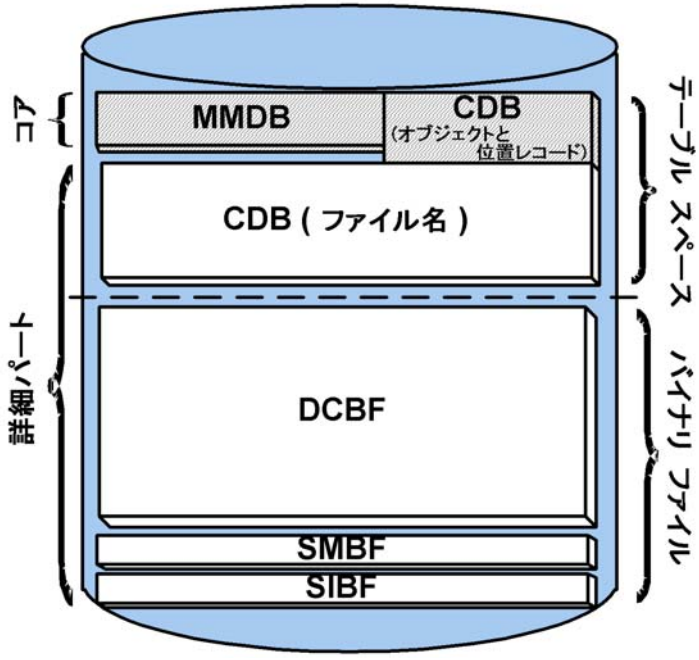

図 56 IDBの構成要素

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。 スペースの消費は、30MBの範囲内です。 詳細は、「IDBサイズの見積もり 」 (192ページ) を参照してください。

MMDBの場所

MMDBは以下のディレクトリにあります。

- Windows Server 2008の場合：
  Data_Protector_program_data\db40\datafiles\mmdb
- その他のWindowsシステムの場合：
  Data_Protector_home\db40\datafiles\mmdb
- UNIXシステムの場合：/var/opt/omni/server/db40/datafiles/mmdb

カタログ データベース(CDB)

CDBレコード

カタログ データベースでは、以下に関する情報を保存しています。

- バックアップ、復元、コピー、オブジェクト集約、メディア管理の各セッションに関する情報。 これは、Data Protectorのモニター ウィンドウに送信される情報のコピーです。
- バックアップされたオブジェクトとそのバージョン、およびオブジェクト コピーに関する情報。
- バックアップ オブジェクトのメディア上の位置に関する情報。 Data Protectorは、各バックアップ オブジェクトについて、バックアップに使用するメディアやデータ セグメントの情報を保存します。 オブジェクト コピーやオブジェクト ミラーについても同様に情報を保存します。
- バックアップ ファイルのパス名(ファイル名)とクライアント システム名に関する情報。 ファイル名は1つのクライアント システムごとに1度だけ保存されます。バックアップとバックアップの間に作成されたファイル名はCDBに追加されます。

ファイル名のサイズとサイズの増大

CDBで最も大きな容量を占め、またサイズの増大が速いのはファイル名の部分です。通常、データベース全体の20%をこの情報が占めています。 ファイル名部分の増大速度はバックアップ環境の増大速度や変動には比例しますが、バックアップ回数には比例しません。

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

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

CDB（オブジェクトと位置レコード)のサイズとサイズの増大

ファイル名以外の部分のCDBレコードがIDBで占める割合はそれほど大きくありません。 中規模のバックアップ環境では100MB程度になります。 詳細は、「IDBサイズの見積もり 」 (192ページ) を参照してください。

CDBの場所

CDBは以下のディレクトリにあります。

- Windows Server 2008の場合：*Data_Protector_program_data*\db40\datafiles\cdb
- その他のWindowsシステムの場合：*Data_Protector_home*\db40\datafiles\cdb
- UNIXシステムの場合：/var/opt/omni/server/db40/datafiles/cdb

詳細カタログ バイナリ ファイル(DCBF)

DCBFの情報

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

[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**(Log All)]オプションを使用してファイルシステムのバックアップを行うのが一般的な環境では、DCBFはIDBで最も大きな割合を占めます(通常80%)。DCBFのサイズを計算する場合は、 *dcbf_file_in_bytes*は、約*num_of_files_on_tape x 30_bytes*です。 実際に何をどのくらいの期間IDBに保存するかは、ロギング レベルとカタログ保護で指定できます。「IDBの増大と性能：主要な調整可能パラメータ」 (187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¥ 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16 GB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。

DCBFの場所

デフォルトでは、DCBFは以下のディレクトリにあります。

- Windows Server 2008の場合：*Data_Protector_program_data*\db40\dcbf
- その他のWindowsシステムの場合：*Data_Protector_home*\db40\dcbf
- UNIXシステムの場合：/var/opt/omni/server/db40/dcbf

Cell Managerのディスク スペースを考慮して、必要であればDCディレクトリを再配置します。 DCディレクトリを複数作成して、これらを別々のディスクに配置することができます。 メディア/DCバイナリ ファイル数がかなりの数(数千)に増加した場合、またはスペースが不足している場合のみDCディレクトリを複数作成してください。 詳細は、オンライン ヘルプでキーワード「DCディレクトリ」を指定して確認してください。

セッション メッセージ バイナリ ファイル(SMBF)

SMBFレコード

セッション メッセージ バイナリ ファイルには、バックアップ、コピー、復元、メディア管理の各セッション中に生成されたセッション メッセージが保存されます。 1つのセッションにつき1つのバイナリ ファイルが作成されます。 ファイルは年毎や月毎に分類されます。

SMBFのサイズとサイズの増大

SMBFのサイズは以下の要素によって決定されます。

- 実行されたセッション数(1セッションにつきバイナリ ファイルが1つ作成されるため)。
- セッション内のメッセージ数。 セッション メッセージの容量は、Windowsの場合約200バイト、UNIXシステムの場合約130バイトです。 [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、オンライン ヘルプを参照してください。

SMBFの場所

SMBFは以下のディレクトリにあります。

- Windows Server 2008の場合: *Data_Protector_program_data*\db40\msg
- その他のWindowsシステムの場合: *Data_Protector_home*\db40\msg
- UNIXシステムの場合: /var/opt/omni/server/db40/msg

SessionMessageDirグローバル オプションを編集してディレクトリの場所を変更することもできます。 Data Protectorのグローバル オプション ファイルの詳細は、『HP 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。

サーバレス統合バイナリ ファイル(SIBF)

SIBFレコード

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

SIBFのサイズとサイズの増大

SIBFのサイズはそれほど大きくなりません。 詳細は、「IDBサイズの見積もり 」 (192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3KB使用されます。

SIBFの場所

SIBFは以下のディレクトリにあります。

- Windows Server 2008の場合：*Data_Protector_program_data*\db40\meta
- その他のWindowsシステムの場合：*Data_Protector_home*\db40\meta
- UNIXシステムの場合：/var/opt/omni/server/db40/meta

IDBの操作

バックアップ時

バックアップ セッションが開始されると、IDBにセッション レコードが作成されます。また、そのセッションのオブジェクトごと、およびオブジェクト ミラーごとにオブジェクト バージョン レコードが作成されます。 これらのレコードはすべてCDBに保存され、いくつかの属性が与えられます。 バックアップ中にBackup Session Managerがメディアを更新します。 すべてのメディア レコードはMMDBに保存され、方針に従ってバックアップに割り当てられます。

データ セグメントがテープに書き込まれ、次にカタログ セグメントに書き込まれると、このデータ セグメントの一部である各オブジェクト バージョンに対して、 メディア位置レコードがCDBに保存されます。 また、カタログが DC (詳細カタログ)バイナリ ファイルに保存されます。 Data Protectorメディア1つにつき、1つのDCバイナリ ファイルが保持されます。 DCバイナリ ファイル名は、*MediumID_TimeStamp*.datとなります。 バックアップ中にメディアが上書きされると、古いDCバイナリ ファイルが削除されて新しいDCバイナリ ファイルが生成されます。

バックアップ中に生成されたセッション メッセージは、いずれも、 セッション メッセージ バイナリ ファイル(SMBF部分)に保存されます。

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

復元時

復元構成時にData ProtectorはCDB部分とDCBF部分で一連の照会を行い、ユーザーがバックアップ データがある仮想ファイルシステムをブラウズできるようにします。 このブラウズのための照会には2つの手順が含まれています。 最初の手順では、オブジェクト(ファイルシステムまたは論理ドライブ)を選択します。 オブジェクトのバックアップ バージョンやコピーが複数ある場合は、この手順に多少時間がかかります。 これは今後のブラウズに必要なルックアップ キャッシュを作成するためにData ProtectorがDCBFをスキャンするためです。 2番目の手順では、ディレクトリをブラウズします。

特定のファイル バージョンを選択すると、Data Protectorは必要なメディアを決定し、選択したファイルが使用するメディア位置レコードを検出します。 これらのメディアはMedia Agentから読み込まれ、選択したファイルを復元するDisk Agentに詳細が送信されます。

オブジェクト コピー時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のセッション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」（184ページ）および「復元時」（184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、以下が 削除されます。

- エクスポートしたメディアのすべてのメディア位置レコードがCDBから削除されます。
- その他のメディアに位置レコードがないすべてのオブジェクトとオブジェクト コピーがCDB部分から削除されます。
- 30日以上経過した不要なセッション(メディアが上書き、またはエクスポートされたセッション)が削除されます(この日数を変更するには、グローバル オプション ファイルのKeepSession変数を使用します)。 また、このようなセッションのセッション メッセージも削除されます。
- MMDB部分からメディア レコードが削除され、そのメディアのDCバイナリ ファイルがDCBFから削除されます。

詳細カタログの削除

メディアから詳細カタログを削除すると、対応するDCバイナリ ファイルが削除されます。 メディア上のすべてのオブジェクト バージョンとオブジェクト コピーのカタログ保護を削除しても同じ結果が得られます(DCバイナリ ファイルに対して次に行う日常の保守作業でバイナリ ファイルが削除されます)。 その他のレコードはいずれもCDBとMMDBに保持され、これらのメディアから復元を行えます(ただしブラウズはできません)。

ファイル名の削除

ファイルが関連のメディアにバックアップされているかどうかはDCバイナリ ファイルで知ることができますが、ファイル名は実際にはCDBに保存されます。 少なくとも1つのDCバイナリ ファイル内でバックアップ済みとしてマークされているファイル名は「使用中」とみなされます。 時間が経つと、実際には使用されていないファイル名が増加します。 このようなファイル名を削除するために、Data Protectorはすべてのバイナリ 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、オンライン ヘルプでキーワード「IDB」から「復旧」を指定して確認してください。

IDBの増大と性能

IDBを適切に構成、保守するには、IDBの増大や性能に影響する重要な要素や主要な調整可能パラメータを理解する必要があります。 このパラメータは必要に応じて適用できるのでIDBの増大や性能を効果的に調整できます。

IDBの増大や性能に影響を与える重要な要素

IDBの増大や性能に影響を与える重要な要素を以下に示します。

- ロギング レベルの設定。バックアップ時にIDBに書き込まれる詳細情報の量は、ロギング レベルの設定によって決まります。 詳細度を高めるようにロギング レベルを変更すると、IDBへの影響が増大します。 詳細については、「IDBの増大と性能：主要な調整可能パラメータ」（187ページ）を参照してください。
- カタログ保護の設定。バックアップ データに関する情報がIDBに保管される期間は、カタログ保護の設定によって決まります。 カタログ保護の期間を長くすると、IDBへの影響が増大します。 詳細については、「IDBの増大と性能：主要な調整可能パラメータ」（187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、および各ファイルのそれぞれのバージョンをトラッキングしています。 IDBへの影響は、バックアップの種類によって異なります。 バックアップの種類については、「フル バックアップと増分バックアップ」（64ページ）を参照してください。
- バックアップの数
  バックアップを頻繁に行えば行うほど、IDBに保存される情報量は増加します。
- ファイルシステムの変動 バックアップとバックアップの間に作成または削除されるファイル数は、IDBのファイル名部分の増大に重大な影響を与えます。 [システム処理能力のレポート(Report on System Dynamics)]でシステム変動に関する情報が取得できます。 ファイルシステムの変動に起因するIDBの増大を回避するには、[ディレクトリ レベルまでログに記録(Log Directories)]ロギング レベルを使います。
- バックアップ環境の増大 セル内でバックアップされているシステムの数はIDBの増大に影響を与えます。 このため、バックアップ環境の増大についての計画を立ててください。
- ファイル名に使用されるエンコード方式(UNIXのみ) ファイル名のエンコード方式によって、ファイル名の各文字がIDB内に占めるサイズは1～3バイトと異なります。 例えば、Shift-JIS形式のファイル名の場合に各文字がIDB内で最大3バイトを占めるのに対し、純粋なASCII形式のファイル名の場合は1バイトしか必要ありません。 このようにUNIX上では、文字のエンコード方式がIDBのファイル名部分の増大に影響を及ぼします。 なおWindows上では、すべての文字がIDB内で2バイトを占めます。
- オブジェクト コピーおよびオブジェクト ミラーの数。作成するオブジェクト コピーやオブジェクト ミラーの数が増えると、IDBに保存される情報はそれだけ多くなります。 オブジェクト コピーおよびオブジェクト ミラーについては、ファイル名情報を除き、バックアップ オブジェクトの場合と同様の情報がIDBに保存されます。

IDBの増大と性能：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、図57（188ページ）に示します。

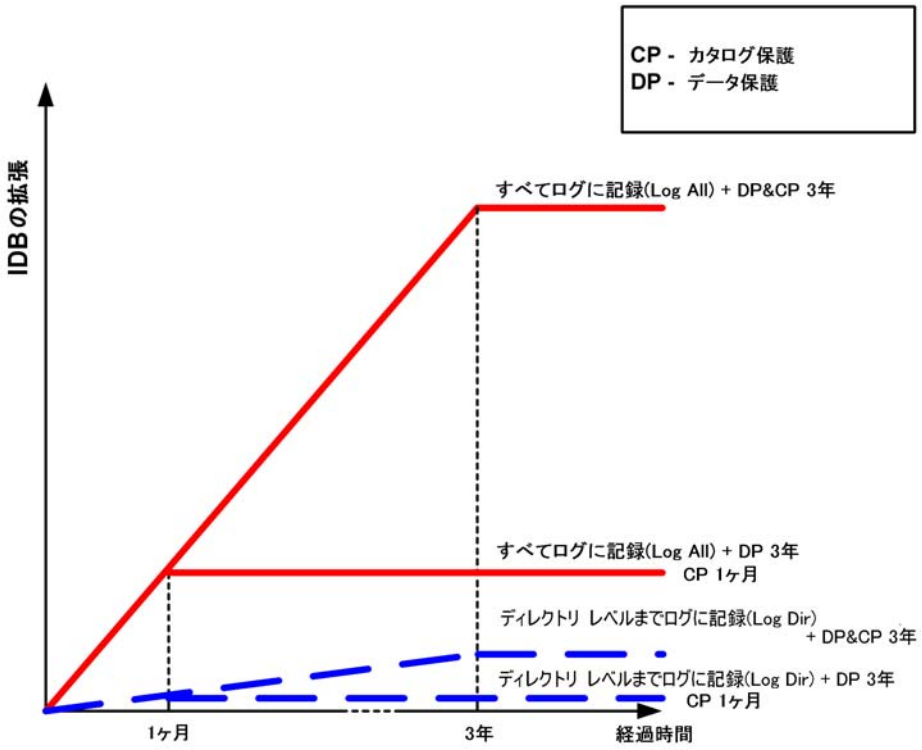

図 57 ロギング レベルとカタログ保護がIDBの増大に与える影響

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(Log All)] すべてろぐにきろく(Log All)	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(Log Files)] ふぁいる れべるまでろぐにきろく(Log Files)	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(Log Directories)] でぃれくとり れべるまでろぐにきろく(Log Directories)	バックアップ ディレクトリに関するすべての詳細情報(名称、バージョン、属性)を記録します。 これは、バックアップ ファイルおよびバックアップ ディレクトリに関する全詳細情報の約10%に相当します。
[記録しない(No Log)] きろくしない(No Log)	バックアップ ファイルおよびディレクトリに関する情報をIDBに記録しません。

設定によって、IDBの増大、バックアップ速度、および復元データの表示の容易度に影響が生じます。

性能への影響

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

ロギングレベルと復元時のブラウズ

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。 [ログなし(No Log)]オプションが設定されている場合は、参照できません。 [ディレクトリ レベルまでログに記録(Log Directories)]オプションが設定されている場合は、ディレクトリの参照は可能です。 [ファイル レベルまでログに記録(Log Files)]オプションが設定されている場合、全体の参照は可能ですが、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(Log All)]、[ディレクトリ レベルまでログに記録(Log Directories)]、[ファイル レベルまでログに記録(Log Files)]オプションが設定されている場合、復元速度はほぼ同じです。

[ログなし(No Log)]オプションを設定すると、単一ファイルを復元する場合に処理速度が低下する可能性があります。 これは、復元するファイルを見つけるために、Data Protectorがオブジェクトの先頭からすべてのデータを読み取る必要があるためです。

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

IDBの主要な調整可能パラメータとしてのカタログ保護

カタログ保護とは

カタログ保護は、IDBでのバックアップ データに関する情報の保管期間を決定します。 バックアップ データの実際のメディア上の保管期間を決定するデータ保護とは異なります。 カタログ保護を設定しなくてもデータは復元できますが、Data Protector GUIでのブラウズができなくなります。

カタログ保護の概念は、最新の保存データが最も重要かつアクセス頻度も最大であるという事実に基づいています。 古いファイルは頻繁に検索されないため、新しいファイルよりも検索に時間がかかります。

期限切れのカタログ保護

カタログ保護期限が過ぎても、情報はすぐにIDBからは削除されません。Data Protectorは一日に一度自動的に削除作業を実行します。 IDB内の情報はメディア単位でまとめられているため、メディアの全オブジェクトのカタログ保護期限が終了した時に完全に削除されます。

性能への影響

カタログ保護の設定は、バックアップの性能には影響を与えません。

カタログ保護と復元

カタログ保護期限が過ぎたデータは[ログなし(No Log)]オプションを使用してバックアップしたデータと同様に復元されます。 「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」（188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、[ログなし(No Log)]オプションが設定されている場合は例外です(この場合、カタログ保護を設定しても設定は適用されません)。

カタログ保護を[無期限(Permanent)]に設定している場合、メディアをエクスポートまたは削除しない限りIDBの情報は削除されません。 この場合、セル内のファイル数が変わらなくても、IDBのサイズはデータ保護期限が切れるまで直線的に増加します。

例えば、データ保護期間が1年で、メディアをリサイクルする場合、1年を過ぎるとIDBはそれほど拡張しなくなります。 新しいカタログとOBDBから削除されたカタログの容量はほぼ同じです。 カタログ保護を4週間に設定した場合、4週間を過ぎるとIDBはそれほど拡張しなくなります。 このため、カタログ保護を[無制限(Permanent)]に設定した場合のIDBの大きさはこの場合の13倍になります。

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

同一セル内で異なるロギング レベルを使用

1つのセルが、複数のシステム(毎日多数のファイルを生成するメール(または同種の)サーバ、少数のファイルにあらゆる情報を保存するデータベース サーバ、ユーザーのワークステーションなど)で構成されていることはよくあることです。 これらのシステムはそれぞれの変動の仕方がかなり異なるため、すべてに適合する1つの設定を決定することは非常に困難です。 このため、以下に示すロギング レベル設定で複数のバックアップ仕様を作成することをお勧めします。

- メール サーバには、[ディレクトリ レベルまでログに記録(Log Directories)]オプションを使用します。
- データベース サーバには独自の復元方針があるため、ログは必要ありません。 このため、[ログなし(No Log)]オプションを使用します。
- ワークステーションには、異なるバージョンのファイルを検索および復元できるように[すべてログに記録(Log All)]または[ファイル レベルまでログに記録(Log Files)]オプションを使用します。 [ディレクトリ レベルまでログに記録(Log Directories)]または[ログなし(No Log)]オプションを設定したバックアップでは、メディアから比較的短時間でカタログをインポートでき、選択したオブジェクトをブラウズできます。 メディアからのカタログのインポート方法についての詳細は、オンライン ヘルプでキーワード「インポート」から「メディアからのカタログ」を指定して確認してください。

オブジェクト コピーに異なるロギング レベルを設定

バックアップ対象のオブジェクトと、そのオブジェクトのコピーやミラーでは、ロギングレベルは同じでも、異なっていてもかまいません。 オブジェクト コピーのロギング レベルは、バックアップ方針に応じて、ソース オブジェクトのロギング レベルよりも詳細度が高いレベルや低いレベルに設定できます。

例えば、バックアップ セッションで正常にバックアップされたことを確実にするためにだけオブジェクト ミラーを作成するような場合であれば、オブジェクト ミラーには[ログなし(No Log)]オプションを指定するだけで十分です。 バックアップの性能を向上させたい場合は、バックアップ対象のオブジェクトに[ログなし(No Log)]オプションを指定しておき、後から行われるオブジェクト コピー セッションでそのオブジェクトに[すべてログに記録(Log All)]オプションを指定することもできます。

小規模のセルでの設定

セル内のファイル数が少なく将来もファイル数が増加しない(1,000,000未満)場合で、セル内のシステムが通常の業務を実行している場合は、常にData Protectorのデフォルトの[すべてログに記録(Log All)]オプションを使用できます。 ただしこの場合、IDBの増大に注意し、適切なカタログ保護レベルを設定することが必要です。

大規模のセルでの設定

ファイル数が数千万に増加した場合や毎日万単位でファイルが生成される場合に[すべてログに記録(Log All)]オプションを使用すると、比較的短期間でバックアップ速度やIDBの増大の問題が生じます。 この場合、以下の方法があります。

- ロギング レベルを使用可能な一番低いレベルに設定します。 [ファイル レベルまでログに記録(Log Files)]オプションを使用するとIDBのサイズを3分の1まで減らすことができ、[ディレクトリ レベルまでログに記録(Log Directories)]オプションを使用すると、約10分の1にまで減らせます。 ただし、これはセル内のファイルシステムの性質に左右されます。
- カタログ保護を最小値に設定します。
- セルを2つに分割します。 最終的なソリューションとしては、別のIDBを導入して、システムの半分をもう一方のIDBに転送する方法があります。

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

IDBサイズの見積もり

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

IDBのサイズを見積もるには、Internal Database Capacity Planning Toolを使用します。 このツールは以下のディレクトリにあります。

- UNIX Cell Manager場合:
  /opt/omni/doc/C/IDB_capacity_planning.xls
- Windows Cell Managerの場合:
  Data_Protector_home\docs\IDB_capacity_planning.xls

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

6 サービス管理

この章の内容

サービス管理、レポート、およびモニタリング機能は、管理者がバックアップ環境を効率よく管理するのに役立ちます。 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。

この章の構成は以下のとおりです。

概要

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

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

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

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

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

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

Data Protectorからは、バックアップ処理およびデータ復元処理を効率よくモニタリングしたり、設計したりするのに役立つ重要なデータが、ITサービス マネージャとともに提供されます。 これらのデータは、サービス アグリーメントを遂行するうえで欠かせない、サービスの可用性や復旧に対する設計作業に役立ちます。 さらにData Protectorから提供される情報は、真のIT財務管理の実現に必要な、コスト管理およびチャージバック モデルの実装にも使用できます。

Data Protectorとサービス管理

Data Protectorはサービス管理機能をサポートしており、 Operations Manager Windows、Performance Agent (以前のMeasureWare Agent)、Reporter、および Service Information Portalなどのサービス管理アプリケーションとの統合が可能です。

Data Protectorのサービス管理は、ネイティブ(即時使用)およびアプリケーション統合の2つに分かれます。 各カテゴリの詳細については、この章の後半で詳しく説明します。

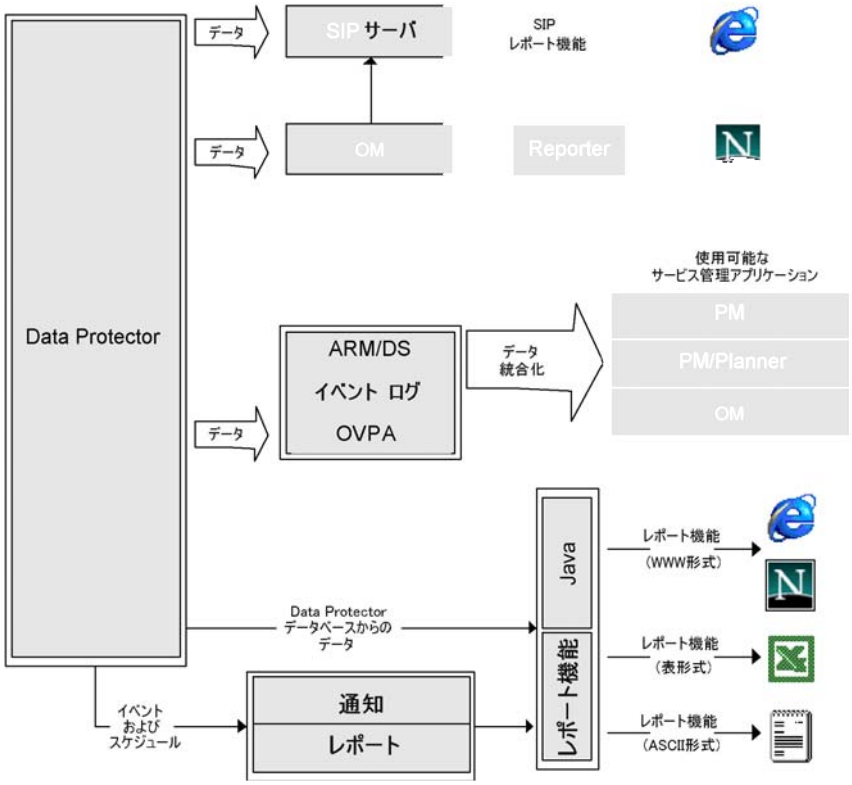

図 58 サービス管理における情報の流れ

ネイティブなData Protector機能

ここで説明する機能は、Data Protectorに組み込まれており、インストール後すぐに使用できます。

主要な機能

- Data Protectorでは、Application Response Measurementバージョン2.0 API (ARM 2.0 API)を使用して、主要な処理にかかった時間を、処理したデータ量とともにトラッキングして、記録することができます。 Application Response Measurementバージョン2.0 API (ARM 2.0 API)。 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モニタリングする機能が組み込まれているため、バックアップ環境内で発生した出来事にただちに対応できます。

- Data Protectorに組み込まれている通知およびレポート用エンジンを使用すると、さまざまな形式(ASCII、HTML、スプレッドシート互換形式など)で作成された要約レポートや即時警報を受け取って、 これをさまざまな方法(電子メール、SNMP、Windows上でのみ可能なブロードキャスト、ファイルへの書き込み、外部コマンドへの送信など)で配布できます。 Data Protectorの組み込み通知エンジンでは、SNMPを介して警報を送信できるため、SNMPトラップを受け取ることができるアプリケーションであれば、事実上どのアプリケーションとも統合することが可能です。
- Data Protector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Data Protectorからの警告を受けとって、対応するアクションを自動的に実行させることができます。
- Data Protectorでは、主要かつ重大なイベントをWindowsのイベント ログに送ることができるため、これを利用してさまざまな興味深い統合機能を開発できます。
- HP Operations Manager Windows (OMW)と統合すると、Data Protectorの主要かつ重大なイベントを、OMWオペレータ コンソールに自動的に転送できます。 バックアップ環境で発生した障害に対する処理の自動実行を設定することも可能です。
- Data Protectorに組み込まれているJavaベースのオンライン レポート機能を使用すると、ネットワーク環境内の任意の地点から(遠隔地からでも)、オンライン レポート機能を実行できます。 この場合、使用するローカル システム上にユーザー インタフェースがインストールされている必要はなく、Webブラウザさえあれば、この機能を使用できます。

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

ARMとは

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

表 13 ARM機能

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

Data ProtectorにはARMが既に組み込まれているため、ARM APIをサポートする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、またはその逆の場合、トランザクション データがただちにPAおよびHP Performance Manager (PM)に表示されるようになります。 またHP-UXの場合にも、必要となるのは、PAライブラリからData Protectorディレクトリへのリンクを作成する作業のみです。 詳細は、オンライン ヘルプでキーワード「ARM統合ソフトウェア」から「インストール」を指定して確認してください。

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

HP Operations Manager ソフトウェアとの統合

Data Protector 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モニタリングおよび管理できるようになるため、大規模なネットワーク環境の管理が容易になります。 Data Protectorを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。

Data Protector Operations Manager Windowsの機能

Data Protector Operations Manager on Windows (OMW)により、以下の機能が提供されます。

- 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。 Operations Manager 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 モニタリング機能
  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モニタリングできます。 いずれかのサービスで問題が発生した場合は、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トラップの構成に関する詳細は、オンライン ヘルプでキーワード「SNMP, レポートの送信方法」を指定して確認してください。

モニター

Data Protectorモニターは、Data Protectorユーザー インタフェースの一部であり、現在実行中のバックアップ、復元、およびメディア管理の各セッションのモニタリングや修正処置の実行に使用します。 モニター内にはセル内のすべてのセッションが表示され、これらのセッションに関する詳細メッセージと現在の状態をチェックできます。 複数セル環境では、他のセルにあるシステム上で実行中のセッションをモニタリングすることも可能です。 モニターのユーザー インタフェースからは、バックアップや復元、メディア管理の各セッションを中止したり、「マウント」要求に応答したりすることができます。

Manager-of-Managers機能を使用する場合は、1つのユーザー インタフェースから、複数のセルで実行中のセッションを同時にモニタリングできます。

レポートと通知

Data Protector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。例えば、保護されていないシステムに関する情報を示すhost_not_confレポートや、スケジューリングされているバックアップ、オブジェクト コピー、オブジェクト集約のすべての一覧を示すdl_schedレポート、メディア インベントリ レポートであるmedia_listレポートなど。
- 稼動率関連レポート。例えば、Data Protectorライセンスの使用状況を示すライセンス レポートや、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dev_unusedレポートなど。
- 問題関連レポート。例えば、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backup_statisticsレポートなど。 管理者は、失敗したジョブとその原因を示す電子メール レポートを、毎時、毎日、または週1回のペースで受け取ることができます。

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

- 事前構成された多数のレポートが用意されており、例えば、指定した時間帯に実行されたセッションに関するレポート、IDBレポート、デバイス使用状況レポートなどを作成できます。
- これらのレポートはパラメータを指定してカスタマイズすることもできます(対象となる時間帯、バックアップ、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サーバ上にHTMLファイル形式で書き込んで、他のユーザーもこの情報を利用できるようにします。

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

イベント ロギングと通知

Data Protectorのイベント ログは、Data Protector関連の通知すべてを管理する中央レポジトリです。 Data Protectorの組み込み通知エンジンは、ログ エントリに基づいて、警報の送信やData Protectorレポート機構の開始などを実行します。 イベント ログは、Data Protectorや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 (スマート プラグイン)経由で情報を提供することにより、予防処置や修正処置を実施することも可能です。詳細は3.1の例を参照してください。

Data Protectorの組み込み通知エンジンは、SNMPを介して警報を送信できるため、SNMPトラップを受け取ることができるアプリケーションであれば、事実上どのアプリケーションとも統合することが可能です。 Operations ManagerやReporterとの統合も、SNMPトラップ ベースの実装の一例です。

イベント ログへのアクセスはData Protectorの[**管理者**]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。 **イベント ログ**内のすべてのイベントをブラウズしたり削除できます。

Data Protectorログファイル

HP Operations Managerソフトウェアなどのサービス管理アプリケーションの中には、特定のログ エントリに関していつ、どのログ ファイルをモニターするかを指定できるものがあります。 特定のエントリがファイル内で検出された場合、動作を指定できます。 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』を参照してください。 ログ ファイルに関する書式化の仕様は用意されていないことに注意してください。

Windowsアプリケーション ログ

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

すべてのData ProtectorメッセージやData Protectorサービス(停止している場合)に関するメッセージをWindowsアプリケーション ログに自動転送するには、Data Protector

グローバル オプション ファイルのEventLogMessages変数を1に設定します。 Data Protectorグローバル オプション ファイルの詳細は、『HP 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、オンライン ヘルプでキーワード「Data Protector"が実行するチェック」を指定して確認してください。

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、モニタリング、ステータス レポートの作成などの作業を実施できます。 MoMを使用すると、多数のData Protector Cell Managerを、単一のCell Managerの場合と同じように簡単に管理できます。 またITサービス プロバイダは、スタッフを増員することなしに、より大規模なクライアント環境を管理することが可能になります。 MoMの詳細は、オンライン ヘルプでキーワード「MoM環境」を指定して確認してください。

Data Protectorが提供するデータの使用

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

データの用途

- 指定した時間枠を超えても処理が終了しないバックアップ セッションまたは復元セッションに対するリアルタイムな警告が可能です(PAを使用)。
- 環境内の主要なシステムのバックアップ処理にかかった時間をグラフ化して、処理時間の傾向を分析できます(PMを使用)。
- IDBサイズの増大を予想することにより、データベース サイズが限界値に達する時期を推測できます(PM Plannerを使用)。
- バックアップ オペレータ、エンド ユーザー、管理者などに、電子メール形式でレポートを定期的に送信できます(Data Protector組み込みレポート機能の電子メール送信機能を使用)。
- バックアップ レポートがWebサーバに書き込まれ、各ユーザーが必要に応じて使用できるようになります(Data Protector組み込みレポート機能のHTMLレポート作成機能を使用)。
- Data Protectorの主要かつ重大なイベントを、HP Network Node Managerなどのネットワーク管理ソフトウェアに送信できます(Data Protector組み込み通知エンジンのSNMPトラップ送信機能を使用)。

サービス管理の統合

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

主要な機能

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

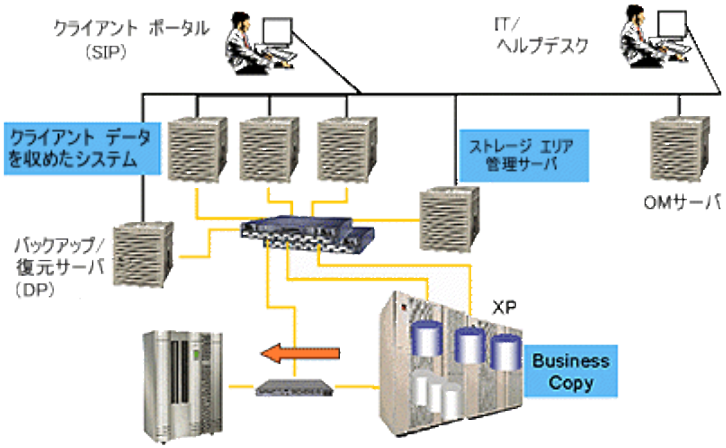

図 59 クライアント ポータルを介してサービス管理にアクセスするITサービス プロバイダ環境の例

Data Protector OM-Rの統合

Data ProtectorとHP Operations Manager software (OM)との統合環境に、HP Reporter 3.7または3.8(英語版)を追加すると、機能をさらに拡張できます。 Reporterを追加すると、サービス プロバイダは中央管理ポイントとしてのOMコンソールから、レポートを生成できるようになります。 Reporterと統合すると、以下の分野について、さまざまな新しい種類のレポートを作成できます。

- バックアップ セッション レポート
- 管理レポート
- メディア プール レポート
- パフォーマンス

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

hp OpenView | data protector

hp OpenView data protector Transaction Performance

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

This report shows the systems where each Application Response Measurement (ARM) transaction has been executed

Completed = the number of transactions completed successfully.

Aborted = the number of transactions that have been aborted instead of completed.

Response = the average time (seconds) to complete a successful transaction.

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

Backup of Specific Object Transcations

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

Backup Session Transcations

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

図 60 Data Protector Reporterの例

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

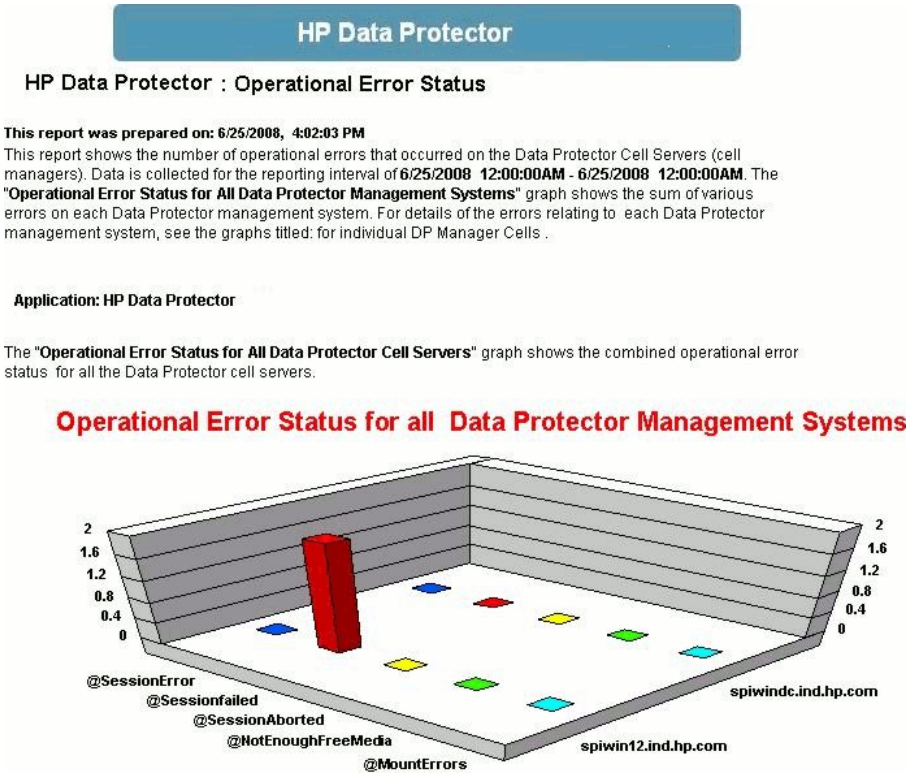

図 61 Operational Error Statusレポート

Data Protector OM SIP

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

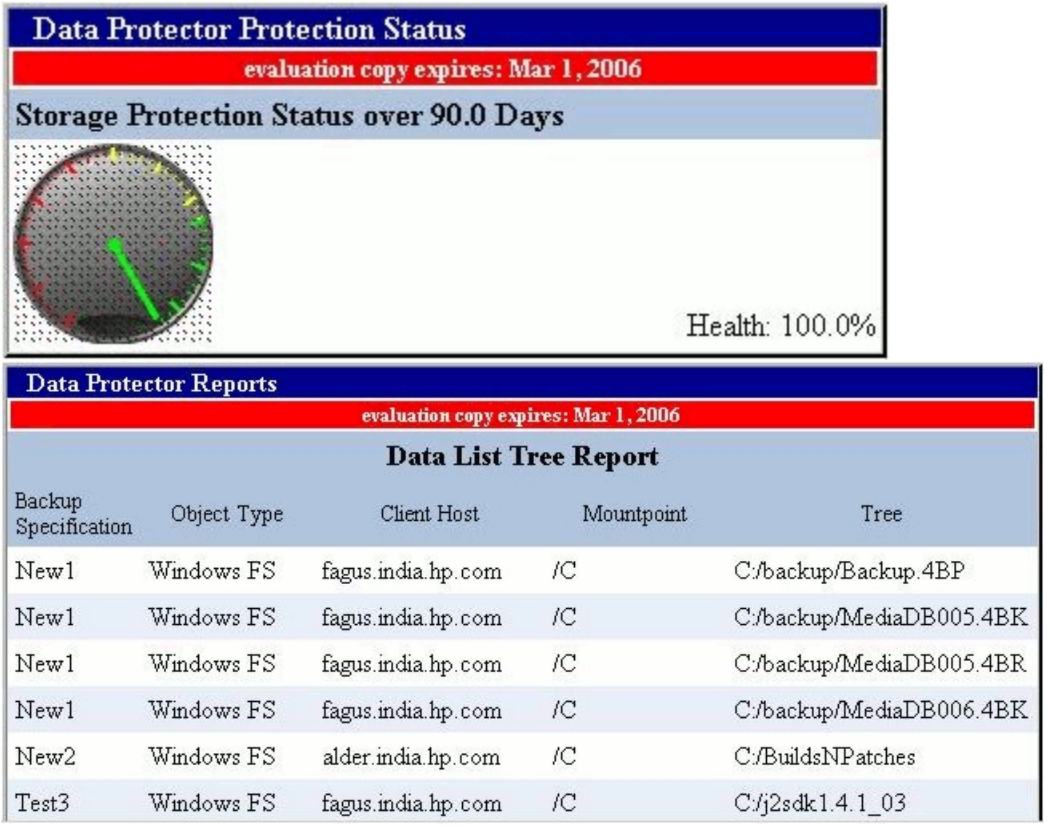

図 62 Direct SIPの統合例

7 Data Protectorが機能する仕組み

この章の内容

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。

この章の構成は以下のとおりです。

Data Protectorのプロセス(サービス)

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

Inet	Data Protector Inetサービスは、Data Protectorセル内の個々のWindowsシステム上で実行されます。 Inetは、セル内のシステム間の通信と、バックアップおよび復元に必要なその他のプロセスの開始を担当しています。 Data Protector Inetサービスは、Data Protectorをシステム上にインストールした時点で開始されます。 UNIXシステム上では、システムのinetデーモン(INETD)により、Data ProtectorのInetプロセスが開始されます。
CRS	CRS (Cell Request Server)プロセス(サービス)は、Data ProtectorのCell Manager上で実行されます。 CRSは、バックアップ セッションおよび復元セッションの開始および制御を担当しています。 このサービスは、Data ProtectorをCell

	Managerシステム上にインストールした時点で開始され、システムが再起動されるたびに再開されます。
MMD	MMD (Media Management Daemon)プロセス(サービス)は、Data ProtectorのCell Manager上で実行され、メディア管理およびデバイス操作を担当しています。 このプロセスは、Cell Request Serverプロセス(サービス)により開始されます。
RDS	RDS (Raima Database Server)プロセス(サービス)は、Data ProtectorのCell Manager上で実行され、IDBの管理を担当しています。 このプロセスは、Data ProtectorをCell Managerにインストールしたときに開始されます。
UIProxy	Java GUI Server(UIProxyサービス)はData Protector Cell Managerで実行されます。 Java GUI Serverでは、Java GUI Client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、オンライン ヘルプを参照してください。

バックアップ セッション

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

A 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、図 63 (210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(ダイレクト バックアップなど)におけるデータ フローやプロセスについては、関連する章を参照してください。

バックアップ セッションが開始されると、以下の処理が実行されます。

1. カラーマネージメントを行うには、オペレーティング システムからの場合もアプリケーションからの場合も BSM (Backup Session Manager)プロセスが、Cell Managerシステム上で開始されて、バックアップ セッションを制御します。 このプロセスにより、バックアップ仕様内に指定されているバックアップ対象、オプション、バックアップ用メディアとデバイスなどの情報が読み取られます。
2. BSMにより、IDBがオープンされて、生成されるメッセージのほか、バックアップデータに関する詳細や、使用するデバイスやメディアに関する情報など、バックアップ セッションに関する情報がデータベース内に書き込まれます。
3. BSMにより、バックアップ用デバイスが接続されているシステム上で、Media Agent (MA)が起動されます。 ドライブが並列に使用される場合は、ドライブごとに個々のMedia Agentが開始されます。 同一セル内で開始できるMedia Agentの数は、セルの構成と購入しているライセンスの数とによって制約されます。

   オブジェクト ミラーの作成を伴うバックアップ セッションの場合は、BSMにより、ミラー作成用のMedia Agentも開始されます。
4. BSMにより、並行してバックアップされるディスクごとに、個々のDisk Agent (DA)が起動されます。 実際に起動されるDisk Agentの数は、バックアップ仕様に構成されたDisk Agentの同時実行数に基づいて決められます。 これは、デバイス ストリーミングを維持するために、同時に開始できるDisk Agentの数を示すものであり、これらのDisk Agentから1つのMedia Agentにデータが並行して送られます。
5. Disk Agentによりディスク上のデータが読み取られてMedia Agentに送信され、このMedia Agentによりメディアに書き込まれます。

   オブジェクト ミラーの作成を伴うバックアップ セッションでは、ミラー オブジェクトの書き込みに使用される各Media Agentが、デイジーチェーン方式で連結されます。 個々のMedia Agentは受け取ったデータをメディアに書き込み、処理が終わると、チェーン内の次のMedia Agentにデータを渡します。

6. セッションの進捗状況はBSMによりモニタリングされており、必要に応じて新しいDisk AgentやMedia Agentが開始されます。
7. バックアップ セッションが終了したら、BSMによりセッションが閉じられます。

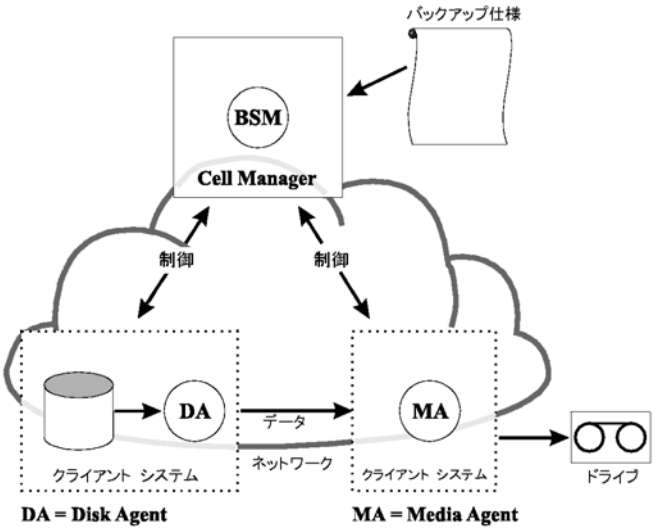

図 63 バックアップ セッションにおける情報の流れ(1)

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。

図 64（211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。

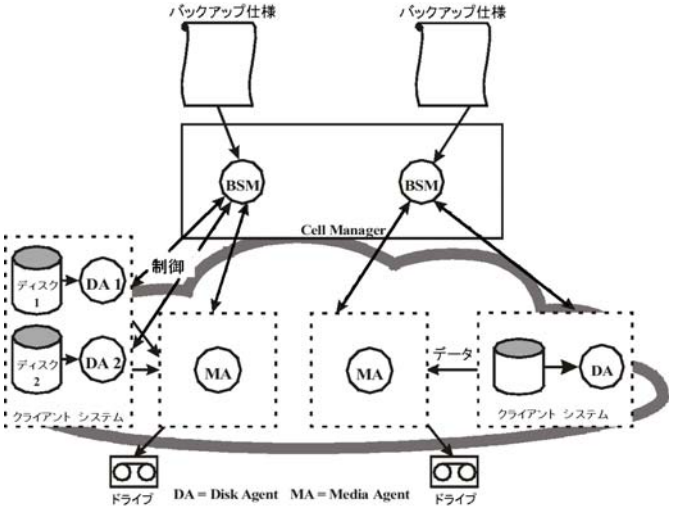

図 64 バックアップ セッションにおける情報の流れ – 複数のセッション

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。 タイムアウト時間は、[SmWaitForDevice]グローバル オプションを使用して設定できます。

負荷の最適化

Cell Managerの負荷を最適化するために、Data Protectorは、デフォルトでは、最大5つのバックアップ セッションを同時に開始できるようになっています。 このデフォルトの値は、グローバル オプション ファイルを編集することにより変更可能です。 これ以上のセッションが同時にスケジューリングされた場合には、処理できないセッションは待ち行列に入れられて、他のセッションの終了後に開始されます。

バックアップ セッションにおけるマウント要求

マウント要求とは

バックアップ セッション中に新しいバックアップ用メディアが必要になり、そのメディアが使用可能でない場合には、Data Protectorからマウント要求が発行されます。

Data Protectorは、次のいずれかの場合にマウント要求を発行します。

マウント要求の発行

- バックアップ メディア上のスペースが不足したが、使用可能な新しいメディアがない場合。
- Data Protectorのメディア割り当て方針により特定のメディアが要求されたが、そのメディアがデバイス内にない場合。
- バックアップに使用するメディアの順番が事前割り当てリスト内に指定されているが、この順番でメディアを使用できない場合。

詳細については、「バックアップ セッション中にデータをメディアに追加」（138ページ）および「バックアップ用メディアの選択 」（138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。 詳細については、「レポートと通知」（198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

図 65 (214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. Restore Session Manager (RSM)プロセスは、Cell Managerシステム上で開始されます。 このプロセスによって、復元セッションが制御されます。

2. RSMによってIDBがオープンされ、復元に必要なメディアの情報が読み取られ、復元セッションの情報(生成されるメッセージなど)がIDBに書き込まれます。
3. RSMにより、復元に使用するデバイスがあるシステム上で、Media Agent (MA)が起動されます。 並行して使用される各ドライブで、新たにMedia Agentが起動されます。
4. 並行して復元される各ディスクに対して、RSMによりDisk Agent (DA)が起動されます。 起動されるDisk Agentの実際の数は、復元を選択したオブジェクトに依存します。 詳細については、「並行復元」 (215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。

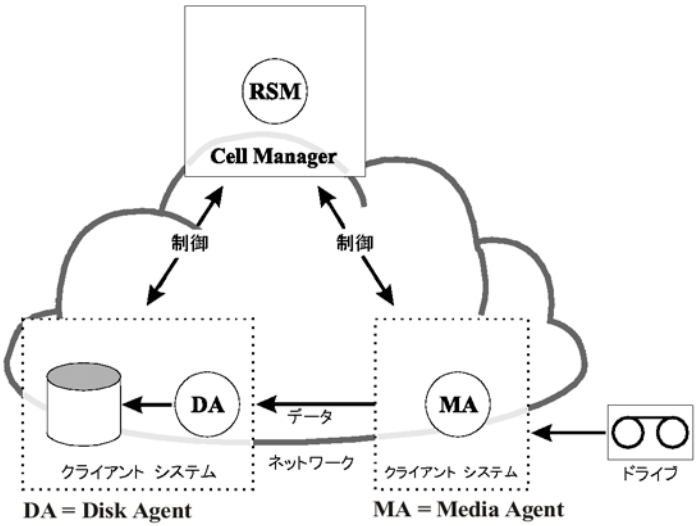

図 65 復元セッションの情報フロー

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。 詳細については、図 66 (216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。 詳細は、図 41 (139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。

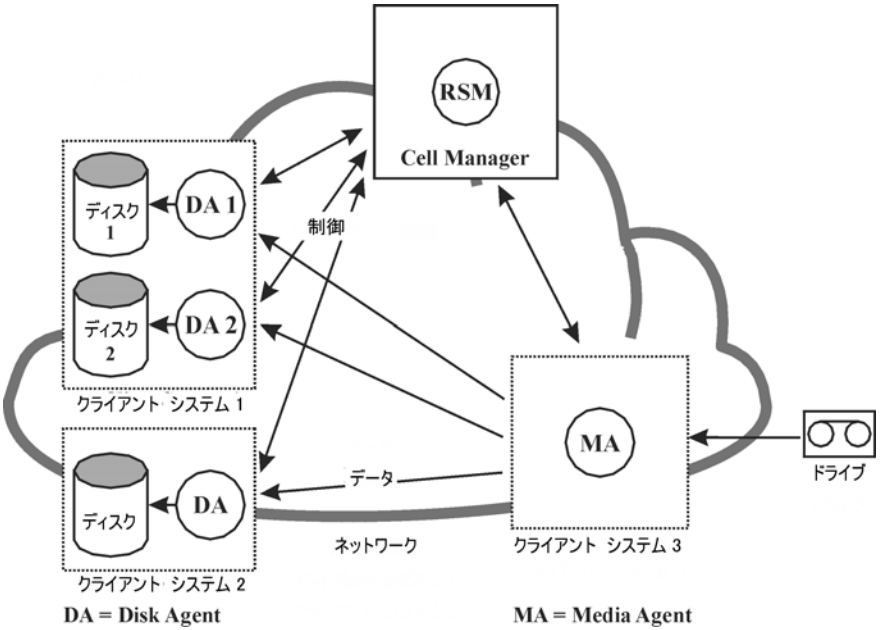

図 66 並行復元セッションのフロー

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。

オブジェクト コピー セッション

ここでは、オブジェクト コピー セッションの開始方法、セッション中の処理内容、および関連するプロセスとサービスについて説明します。

オブジェクト コピー セッションとは

オブジェクト コピー セッションとは、バックアップ データの追加コピーを別のメディア セット上に作成するプロセスです。 オブジェクトコピーセッション中に、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。

自動および対話形式のオブジェクト コピー セッション

自動オブジェクト コピー セッション

自動オブジェクト コピー セッションは、スケジュールを設定して開始することも、バックアップの終了直後に開始することも可能です。 スケジュール方式のオブジェクト コピー セッションは、Data Protectorスケジューラで指定した時刻に開始されます。 一方、バックアップ後のオブジェクト コピー セッションは、指定した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参照できます。 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、図 67 (219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 (Copy and Consolidation Session Manager)プロセスが、Cell Managerシステム上で開始されます。 このプロセスは、オブジェクト コピー仕様に指定されたコピー対象、オプション、使用するメディアとデバイスなどの情報を読み取ります。またこのプロセスは、オブジェクト コピー セッション全体を制御します。
2. CSMがIDBをオープンし、コピーに必要なメディアの情報を読み取り、オブジェクト コピー セッションの情報(生成されるメッセージなど)をIDBに書き込みます。
3. CSM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. オブジェクト コピー セッションが終了したら、CSMによりセッションが閉じられます。

同時に実行できるセッションの数

セル内では同時に複数のオブジェクト コピー セッションを実行できます。 同時に実行できるセッションの数は、Cell Managerや、デバイスを接続しているシステムなど、セル内のリソースによって制限されます。

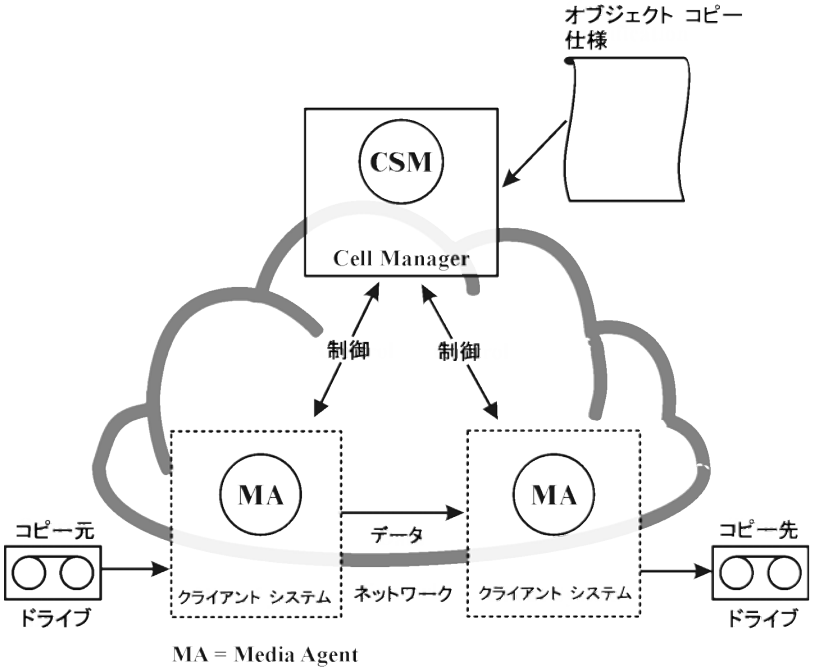

図 67 オブジェクト コピー セッションにおける情報の流れ

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。 タイムアウト時間は、[SmWaitForDevice]グローバル オプションを使用して設定できます。

オブジェクト コピー セッションにおけるマウント要求

マウント要求とは

オブジェクト コピー セッションのマウント要求は、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。

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。

詳細については、第11章 (245ページ) をご覧ください。

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参照できます。 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 (Copy and Consolidation Session Manager)プロセスが、Cell Managerシステム上で開始されます。 このプロセスにより、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。

   宛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 サイズを持つ宛先デバイスが、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、宛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。 タイムアウト時間は、[SmWaitForDevice]グローバル オプションを使用して設定できます。

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。

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. The Media Session Manager (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 データベース アプリケーションとの統合

この章の内容

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

この章の構成は以下のとおりです。

サポートされている統合機能の一覧については、『HP Data Protector product announcements 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。

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(マネージャ)プロセスにより管理されて、データの整合性と一貫性が保たれます。

リレーショナル形式の構造またはオブジェクト指向の構造のいずれを使用する場合も、データベース内のデータは**ファイル**に保存されます。. 内部的には、これらのデータベース構造によりデータからファイルへの論理マッピングが提供され、データ型の異なるデータは個別に保存できます。 これらの論理領域は、Oracleでは**表領域**、Informix Serverでは**dbスペース**、Sybaseでは**セグメント**と呼ばれています。

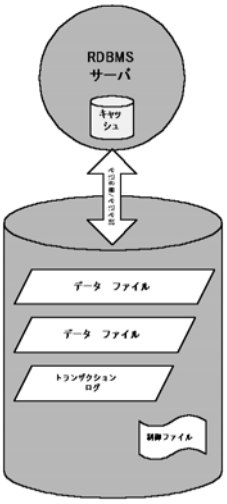

図 68 リレーショナル データベース

図 68（226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、例えば、データベースの名前、データベースに所属するデータ ファイルやログ ファイルの名前と場所、データベース作成時のタイム スタンプなどが保存されています。 この制御データは、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 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 サーバは、接続ユーザーへの迅速な応答や性能の向上を図るために、複数のコンポーネントで構成されています。 例えばデータの中には、内部キャッシュ メモリや一時的なログ ファイルに保存されているものもあります。 これらのデータは、**チェックポイント**でディスクに一括して書き込まれます。

データベース内のデータはバックアップ中にも変更される可能性があるため、データベース ファイルの有効なファイルシステム バックアップを作成するには、データベース サーバを特殊モードまたはオフライン状態にしなければなりません。 データに整合性がなければ、データベース ファイルをバックアップしても意味がありません。

次に、データベースまたはアプリケーションのファイルシステム バックアップを構成する手順を示します。

- 対象となるすべてのデータ ファイルを確認します。
- データベースを停止および開始するための2つのプログラムをそれぞれ用意します。
- データベースに所属するすべてのデータ ファイルを含めたファイルシステム**バックアップ仕様**を構成します。 次に、**実行前コマンド**としてデータベース停止プログラムを、 **実行後コマンド**としてデータベース開始プログラムを指定します。

この方法は、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 アプリケーションをオンライン状態のままにでき、ユーザーの利用が引き続き可能になります。 Data Protectorを始めとするバックアップ製品では、これらのアプリケーション固有のインタフェースを使って、データベース アプリケーションの論理ユニットのバックアップや復元を実行できます。 バックアップAPIの機能はデータベース ベンダーによって異なります。Data Protectorの統合機能は、主要なデータベースおよびアプリケーションで利用可能です。 サポートされる統合機能の詳細は、『HP Data Protector product announcements 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。

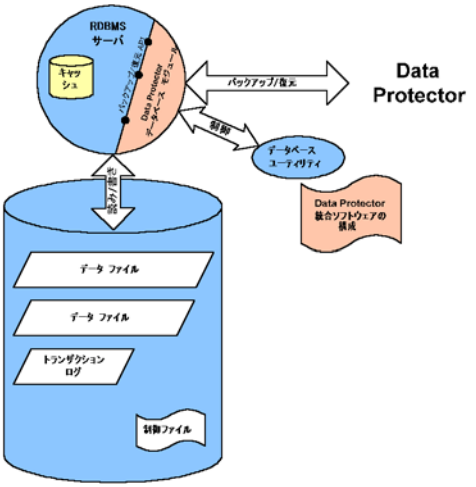

図 69 Data Protectorとデータベースの統合

図 69 (228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 サーバにリンクされる**データベース ライブラリ**が提供されます。 データベース サーバは、Data Protectorに対してデータを送信したり、データを要求したりします。 データベース ユーティリティは、バックアップ処理や復元処理の開始に使用されます。

以下に、Data Protectorの統合機能を使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。

9 ダイレクト バックアップ

この章の内容

この章ではダイレクト バックアップの概念と、ダイレクト バックアップを支える技術について説明します。 また、Data Protectorでサポートされるダイレクト バックアップ構成についても紹介しています。

この章の構成は以下のとおりです。

概要

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

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

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

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

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

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

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

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

注記：

HP Data Protector A.06.10のダイレクト バックアップでサポートされるアプリケーション、オペレーティング システム、およびデバイスの詳細は、「サポートされている構成」 (238ページ) を参照してください。

ダイレクト バックアップ

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

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

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

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

ダイレクト/サーバレス バックアップをサポートするために、Data Protectorでは、対象のファイルシステムを解析し、SANを介してデータを送信するための新たな技術も採用しています。 XCopy標準をベースにしたこの新しい技術により、サーバを介することなく対象のシステムからテープ デバイスにデータを送信することが可能になります。 XCopyの簡単な説明については、「XCopyについて」 (235ページ) を参照してください。

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

バックアップの種類

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

ダイレクト バックアップの利点

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

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

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

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

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

ダイレクト バックアップの仕組み

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

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

図 70（234ページ）は、基本的なダイレクト バックアップ構成を示したものです。 この構成では、独立したバックアップ ホスト上にResolve Agentが存在しています。 ただし、データはこのホストを経由して転送されるわけではありません。

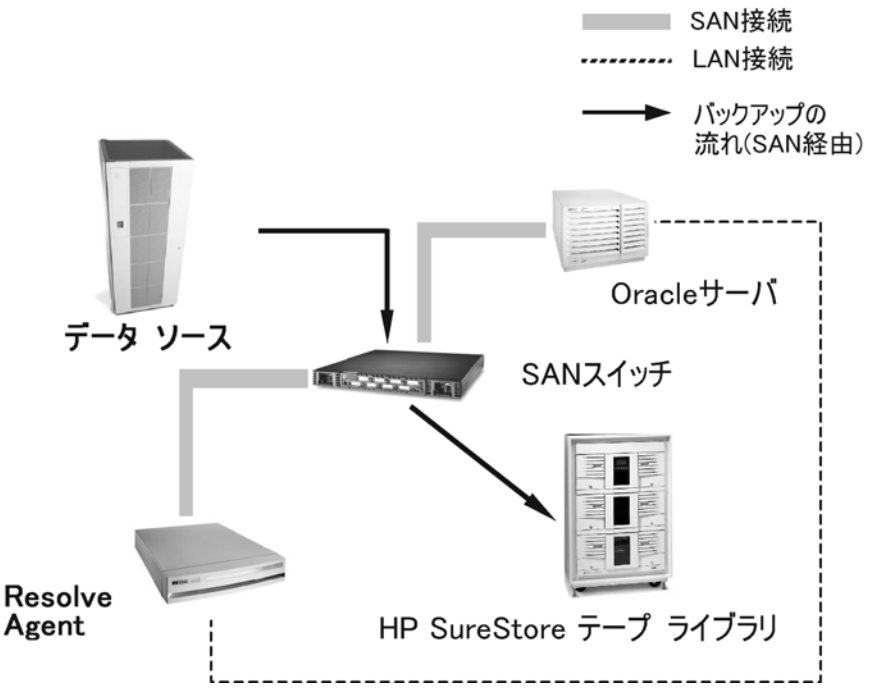

図 70 ダイレクト バックアップのアーキテクチャ

[環境]

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

サポートされるプラットフォーム、テープ ドライブ、およびライブラリの詳細は、「サポートされている構成」（238ページ）を参照してください。

ダイレクト バックアップを実行する場合、アプリケーションを実行しているサーバ以外の場所に汎用Media Agentを配置することが求められます。 また、アプリケーションを実行しているサーバまたはその他のホスト上にResolve Media Agentが存在し、XCopyエンジンにアクセスできる必要があります。 Resolve Agentの配置については、「サポートされている構成」（238ページ）を参照してください。

ダイレクト バックアップの要件は以下のとおりです。

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

Resolveプログラムについて

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

Resolveはディスク上のraw情報を確認し、ディスク上のファイルシステムを解釈するのに適した方法を選択します。 Resolveはデータそのものは読み込まないことに注意してください。 ディスクの場所に関連する情報のみを読み込みます。 その後Resolveは、XCopyエンジンに直接入力するのに適した情報を返します。

XCopyについて

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

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

XCopyはストリーム(テープ)デバイスがセットアップされ、データの読み書きが可能な状態になっていることを前提としています。 つまりドライブがオンライン状態になってお

り、ドライブ内にテープがセットされ、読み書きの開始位置にテープが位置付けられている必要があります。 XCopy機能を使用することにより、制御サーバは、コピー元デバイスのデータをメモリ内に読み込んでコピー先デバイスにその情報を書き込む作業から解放されます。 XCopy機能を使用する場合、サーバ側では、XCopyコマンドをXCopyエンジンに渡し、その結果が返ってくるのを待つだけで済みます。

XCopyとResolve

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

ダイレクト バックアップ処理の流れ

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

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

データ ファイルのバックアップ段階

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

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

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

復元

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

- HP StorageWorks XPディスク アレイを使用しており、インスタント リカバリ機能を実行できる場合は、この機能を使ってデータを復元できます。 インスタント リカバリの使用に関する説明については、『HP Data Protector zero downtime backup administrator's guide』を参照してください。
- ダイレクト バックアップを使用して保存した情報の復元には、通常のData Protectorネットワーク復元機能も使用できます。

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

要件とサポート

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

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

サポートされている構成

3台のホスト： CM、アプリケーション、Resolve

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

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

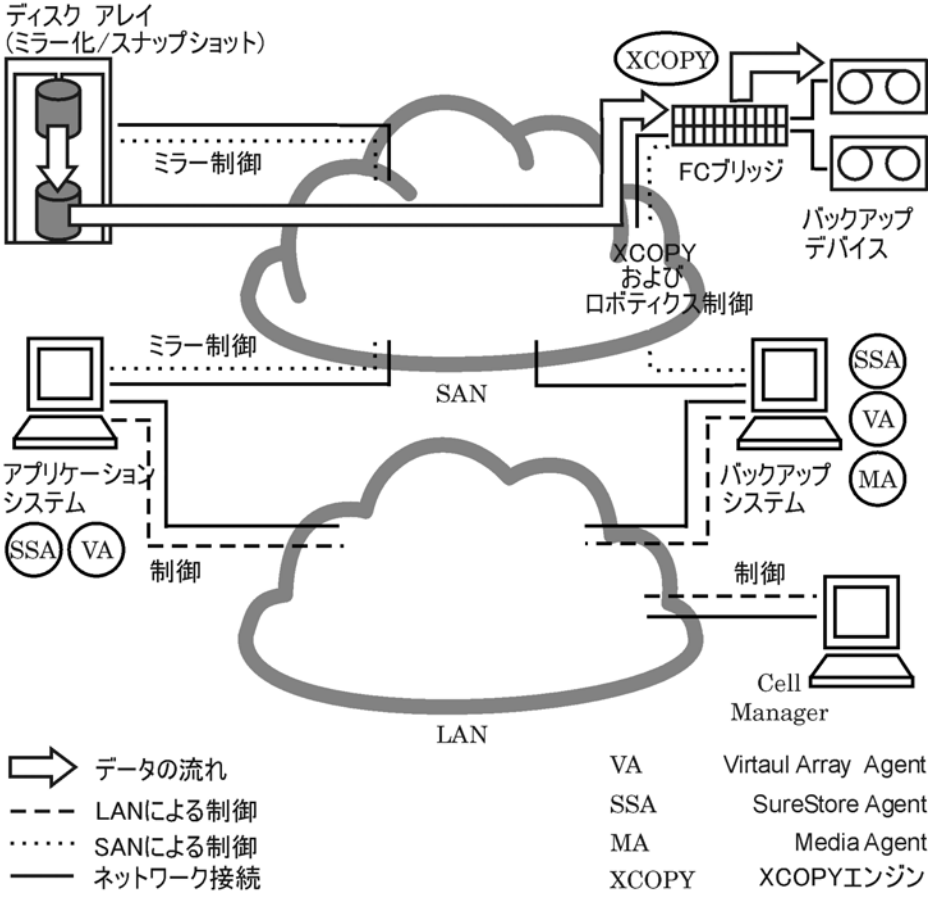

図 71 3台のホストによる基本的な構成

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

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

この構成では、両方のホスト上でHP-UX 11.11が実行されている必要がある点に注意してください。

基本的な構成：1台のホスト

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

この構成では、ホスト上でHP-UX 11.11が実行されている必要がある点に注意してください。

10 ディスク バックアップ

この章の内容

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

この章の構成は以下のとおりです。

概要

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

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

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

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

ディスク バックアップの利点

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

- 多くのアプリケーションとデータベースでは、基幹業務データを含むファイルが、継続的に数多く生成または変更されます。 こうした状況下でデータを完全に復元できるようにするためには、関連するファイルを頻繁にバックアップしなければなりません。
  通常、このような環境では、テープ デバイスでデータ ストリームを絶え間なく受信することがないため、テープ デバイスをスタート/ストップモードで動作させる必要があります。 そのため、テープ デバイスにより、関連ファイルへのアクセスが制限される可能性があります。 また、バックアップ デバイスの耐用年限も大幅に短縮されてしまいます。
  代わりにディスクベースのデバイスにバックアップするようにすると、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。 例えば、復元を迅速かつ簡単に行えるように、バックアップデータをディスクベースのデバイスに24時間保管しておくことができます。
- 装置の特性により、ディスクベースのデバイスはテープよりも速やかに使用を開始できます。 ディスクベースのデバイスを使用するときには、テープのマウントとアンマウントのような操作を行う必要がありません。 またディスクベースのデバイスではテープ ドライブのような初期化時間が不要なため、特に少量のデータをバックアップまたは復元する場合に、その違いを実感できます。 少量のバックアップや復元ではメディアのロードとアンロードにかかる時間の割合が大きくなりますが、ディスクベースのデバイスを使用すると、このロードとアンロードが不要になります。 ディスクベースのデバイスを使用する利点は、増分バックアップからの復元を実行するときに、いっそう明らかになります。
- テープの障害やマウントの失敗といったメディアに関するトラブルを最小限に抑えられます。 ディスク障害からデータを保護するために、RAIDディスク構成を導入することも可能です。
- テープを取り扱う必要がないため、オーバーヘッドコストが削減されます。

- ディスクベースの記憶スペースは、テープベースの記憶装置に比べても、総じて低価格化が進んでいます。

Data Protector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、オンライン ヘルプでキーワード「ファイル ライブラリ デバイス」を指定して確認してください。

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。

設定

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

ディスク デバイスへのバックアップ

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

11 合成バックアップ

この章の内容

この章では、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。

この章の構成は以下のとおりです。

概要

データ量の増加とバックアップ ウィンドウの縮小に伴い、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、それだけ復元に必要な時間が増えるため、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、そのパフォーマンスの高さや容量の大きさ、価格が比較的安いなどの理由から一般的になりつつありますが、それに伴って新たな要望が出てきています。 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性能を持ちながら、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。 これは何度でも繰り返すことができ、フル バックアップを再度実行する必要はありません。

復元スピードの点では、合成フル バックアップは従来のフル バックアップと同じです。 復元チェーンが1つの要素のみで構成されるため、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 バックアップより後に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 オブジェクトの合成がデバイス 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 バックアップからの復元と同程度に高速です。 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には、複数のメディアのマウントとアンマウントや、オブジェクトのバージョンの検索も、必要がなくなります。

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回数の増分バックアップを新規の合成フル バックアップにマージできます。

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の使用が必須です。 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、拡張増分バックアップをオンにする必要があります。

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、作成されます。 合成フル バックアップは、ディスクまたはテープ デバイスへの再書き込みが可能です。

フルおよび増分のすべてのバックアップを配布ファイル メディア形式を使用する同じファイル ライブラリに書き込む場合は、 **仮想フル バックアップ**と呼ばれる、さらに効率の良い合成バックアップを使用できます。 仮想フル バックアップでは、データがコピーされるのではなく、ポインタが使用されてデータが集約されます。 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。

以下の各図は、合成バックアップと仮想フル バックアップの概念を示したものです。合成フル バックアップまたは仮想フル バックアップが、フル バックアップと任意回数の増分バックアップからどのように作成されるのかを示します。

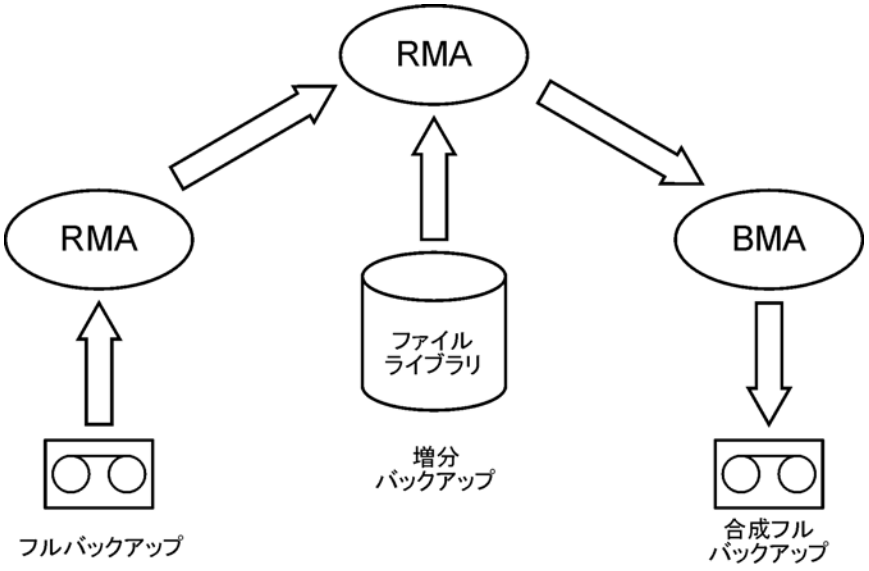

図 72 合成バックアップ

図 72 (247ページ) は、合成フル バックアップがどのように作成されるのかを示しています。 Restore Media Agent (RMA)によって、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)から読み取られます。 データは別のRMAに送られ、そこでファイル ライブラリから増分バックアップが読み取られて、データが集約されます。そして、集約されたデータがBackup Media Agent (BMA)に送られ、合成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。

これ以降は、通常、合成フル バックアップがそれより後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、または必要な間隔ごとに、何度でも繰り返すことができます。

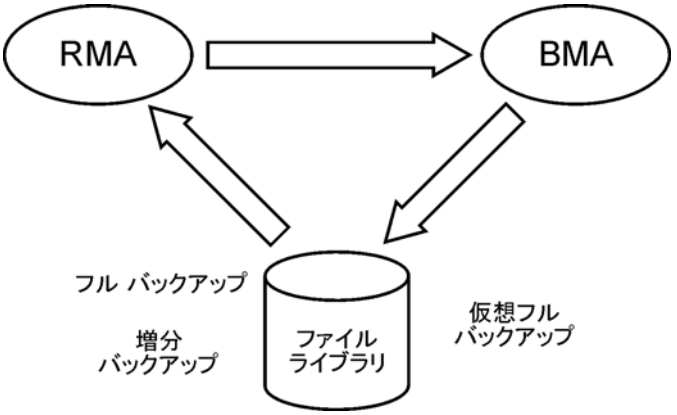

図 73 仮想フル バックアップ

図 73 (248ページ) は、仮想フル バックアップがどのように作成されるのかを示しています。 仮想フル バックアップでは、すべてのバックアップが配布ファイル メディア形式を使用する単一のファイル ライブラリに存在します。 Restore Media Agent (RMA)によって、フル バックアップと増分バックアップに関する情報が読み取られ、仮想フル バックアップ用のデータが生成されます。 生成されたデータは Backup Media Agent (BMA)に送られ、BMAによって仮想フル バックアップがファイル ライブラリに作成されます。

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と、通常はバックアップ メディア上でのスペース使用量が膨大になります。 仮想フル バックアップを実行すると、バックアップ メディア上で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されるファイルのサイズに大きく依存します。 使用されているブロック サイズよりもバックアップされるファイルのサイズが大きいほど、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大きくなります。 これに対し、ファイルがブロック サイズよりも小さい場合には、大きな効果はありません。

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に相当するとみなすことができます。 以下の各図は、データを可能な限り最新の状態に復元する必要がある場合を想定したさまざまな状況を示しています。 どの例でも、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が、 合成バックアップの使用方法が異なります。

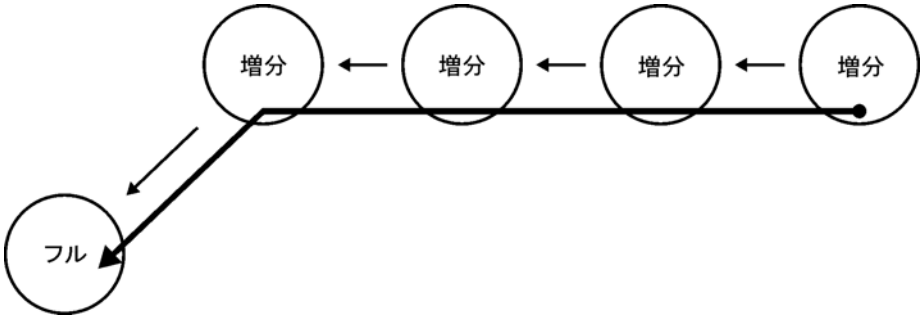

図 74 フル バックアップと増分バックアップ

図 74 (249ページ) は、従来のバックアップを実行した場合です。 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つすべての増分バックアップが必要になります。 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場合があります。

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可能性があります。 テープ デバイスを使用している場合には、複数のメディアのマウントとアンマウントの時間や、復元するオブジェクトのバージョンを検索するための時間を要します。

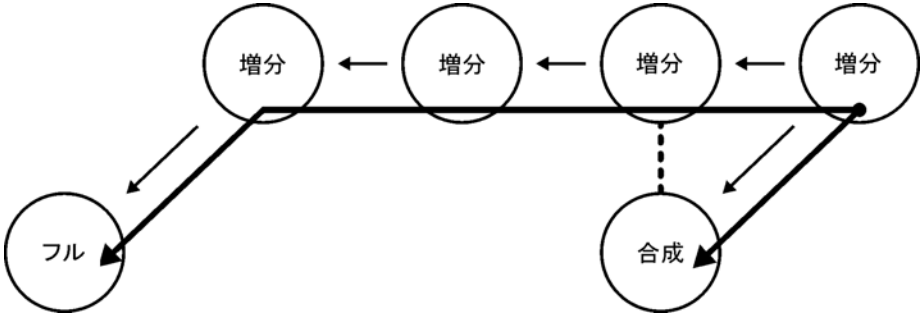

図 75 合成バックアップ

図 75 (249ページ) では、復元用にデフォルトで使用される合成フル バックアップが存在します。 復元チェーンは、合成フル バックアップとそれより後の増分バックアップの2つの要素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簡単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。

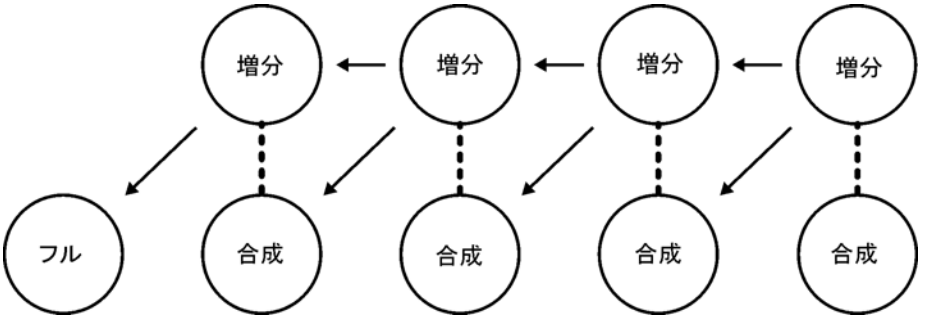

図 76 通常の合成バックアップ

図 76 (250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る状況を示しています。 この方式では、最も簡単かつ高速に、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、復元することが可能になります。 復元に必要な要素は1つのみ、つまり必要となる時点の合成フル バックアップのみです。

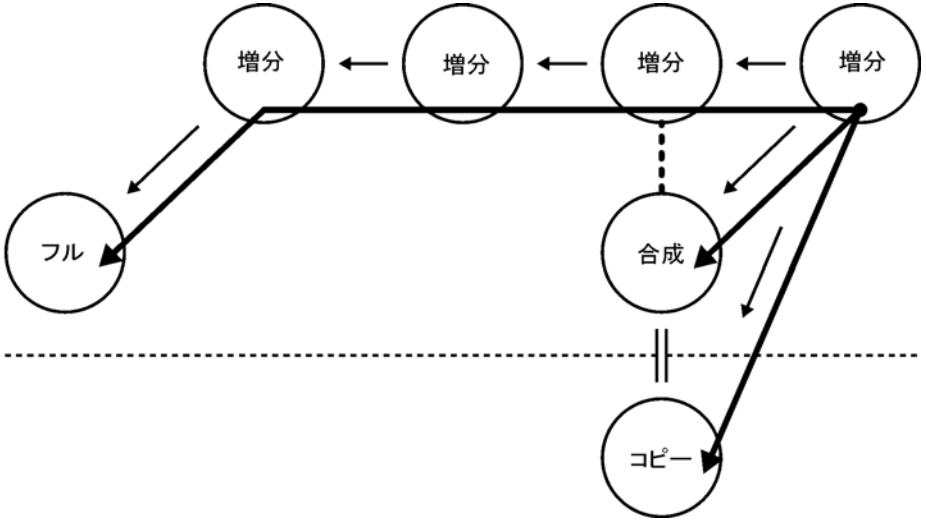

図 77 合成バックアップとオブジェクト コピー

図 77 (250ページ) は、合成バックアップ後にコピーが実行された場合を示しています。 これにより、安全性が強化されます。 図に示している3つの異なる復元チェーンのいずれを使用しても、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、これには、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、代替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ても、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、復元にはバックアップ チェーンでの最新の合成フル バックアップが使用されます。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、保護がすでに切れていてオブジェクトがIDBから削除されているかどうかが影響を及ぼすことはありません。

より安全性を高めるため、データ保護期間は[無期限(Permanent)]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。

12 スプリット ミラーの概念

この章の内容

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

この章の構成は以下のとおりです。

概要

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

通常、このような構成では、 1つの**複製**(ミラー コピー)を使用してバックアップ処理を行う一方で、 アプリケーションの実行には**ソース ボリューム**を引き続き使用する、といった方法が採られます。 詳細については、図 78 (254ページ) を参照してください。

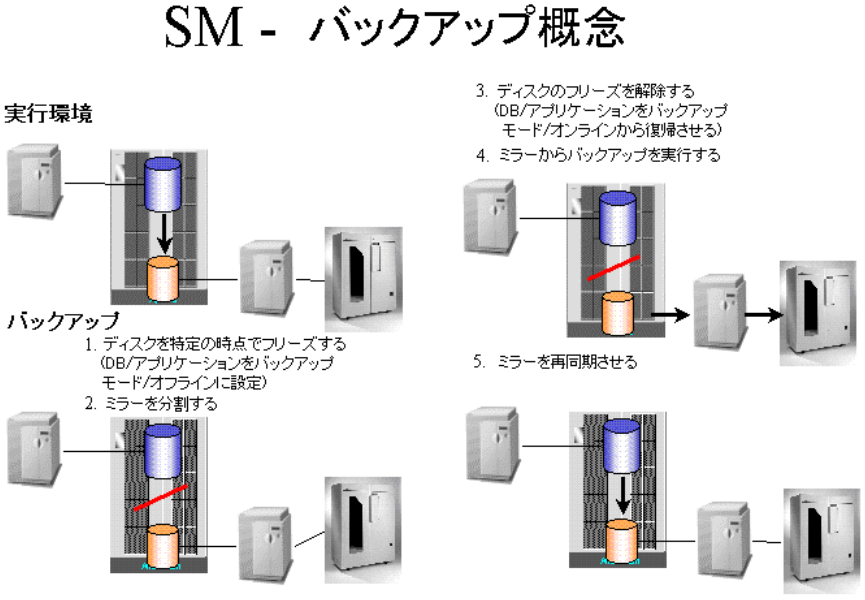

図 78 スプリット ミラー バックアップの概念

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

- HP StorageWorks ContinuousAccess XP
- HP StorageWorks BusinessCopy XP

アプリケーションの可用性は、ディスク上のデータの整合性をとるために必要な数秒から数分間の時間を除くと、ほぼ永久に保持されます。 この時間にディスクの整合性がとられ、実際のミラー分割も行われます。 データは、復元後にアプリケーションが使用できるように整合性を保つ必要があります。 通常は、バックアップ時に複製は作成されませんが、この時点ではすでに作成されており、アプリケーションの可用性を実現するために同期がとられています。 バックアップおよび複製の再同期処理は、別のハードウェア上で並行して行われるため、アプリケーションの性能に影響が及ぶことはありません。

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

- データベースをバックアップ モードにする。

- データベースをオフラインにする。
- マウント ポイントをアンマウントする。

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

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

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

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

バックアップ クライアントによるバックアップの時間は適度な長さである必要があります。 しかし、理論上は、バックアップの実行にほぼ24時間必要である可能性があり、復元時間も考慮する必要があります。 したがって、2 ~ 4時間でバックアップを実行できるバックアップ クライアントを用意することをお勧めします。 また、復元はアプリケーション クライアントを通じて行うことをお勧めします。

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

インスタント リカバリ

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

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

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

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

テープへのZDBとディスク+テープへのZDB

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

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

ディスクへのZDB でぃすくへのZDB

ディスクへのZDBバックアップ セッション中は、複製からバックアップ メディア(テープ)への移動に、オリジナルのデータは使用されません。 オフライン データ処理やインスタント リカバリなどのさまざまな用途に3つまでの複製を使用できます。 ただし、インスタント リカバリに複製を使用できるのは、HP StorageWorks BusinessCopy XP構成が使用されている場合のみです。 ディスクへのZDBセッションで作成したオブジェクトを復元するには、インスタント リカバリ機能を使用する必要があります。

複製セットのローテーション

つまり、複数の複製を同時に作成できます。 HP StorageWorks Disk Array XPでは同時に最大3個の複製を保持でき、カスケード接続を行った場合は、それぞれの複製が2個の追加コピーを所有できます。ただしData Protectorでは、バックアップおよびインスタント リカバリ用としては、最初の3個の複製(**ファースト レベル ミラー**または**MU**)のディスクしか使用できません。 6個の追加コピー(カスケード ミラー)はサポートされていません。ファースト レベル ミラーで構成したソース ボリューム(LDEV)に対してZDBバックアップ仕様を構成する場合、またはそのようなソース ボリュームに復元する場合、Data Protectorを使って複製セットを定義することができ、 その**複製セット**から現在のセッションに対して複製が1つ選択されます。

バックアップ クライアントとクラスタ

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

サポートされている構成

ローカル ミラー(デュアル ホスト)

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

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

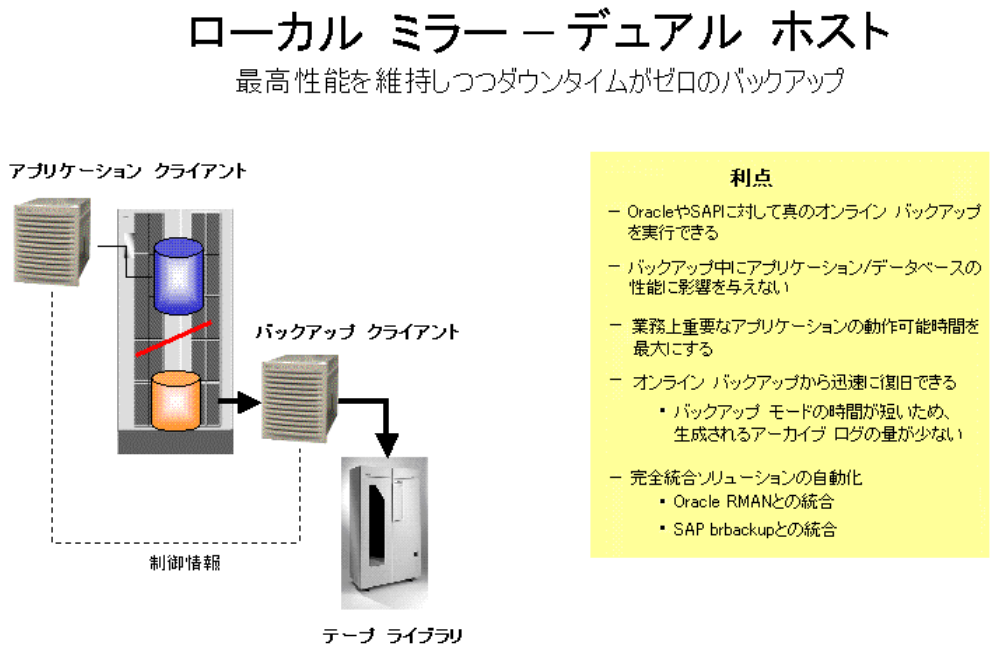

図 79 ローカル ミラー(デュアル ホスト、最高性能時でダウンタイムがゼロのバックアップ)

Data Protectorのスプリット ミラー バックアップの統合により、ミラー状態の自動処理やアプリケーション(SAP R/3、Oracleなど)との密接な統合が可能になり、データの整

合性およびアプリケーション/データベース対応バックアップが確実に実行されます。 アプリケーション/データベースによって、バックアップが行われていることが認識されている場合に限り、安全な操作が保証されます。 この場合、アプリケーション固有のツールを使用して復元が行えます。 バックアップがアプリケーションに与える影響は、ミラーの分割に必要な時間と、分割可能な整合性のあるモードにデータベースを切り替えて元のモードに戻すための時間との合計にまで削減されます。

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

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

ローカル ミラー(シングル ホスト)

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

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

リモート ミラー

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

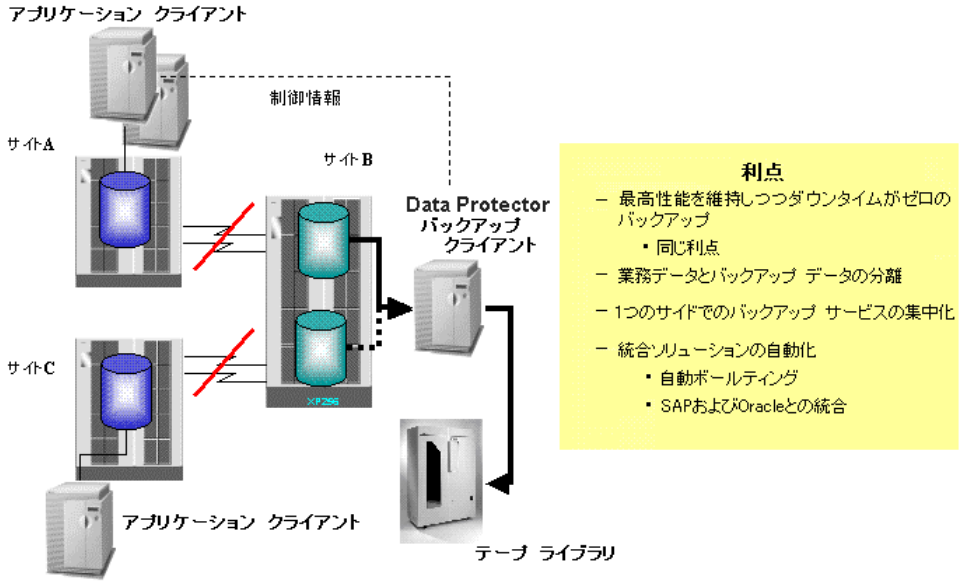

図 80 スプリット ミラー – リモート ミラー(LAN を経由しないリモート バックアップとデータの高可用性)

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

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

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

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

グにも当てはまることですが、リモート ソリューションに対しては特に重要です。 これは、ハードウェア ミラー概念を使用したリモートのディザスタ リカバリ サイトという概念が業界で広く受け入れられているためです。

ローカル ミラーとリモート ミラーの組み合わせ

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

このソリューションによってリモート サイトでの復旧ソリューションとスプリット ミラーの両方の利点を完全に享受することができます。 この例では、バックアップの目的でローカル リンク スプリットでのみ、リモート ミラーが継続的に管理されます。 これによって、クラスタがリモート サイト(サイトB)に継続的にフェイルオーバーする機能が提供されます。

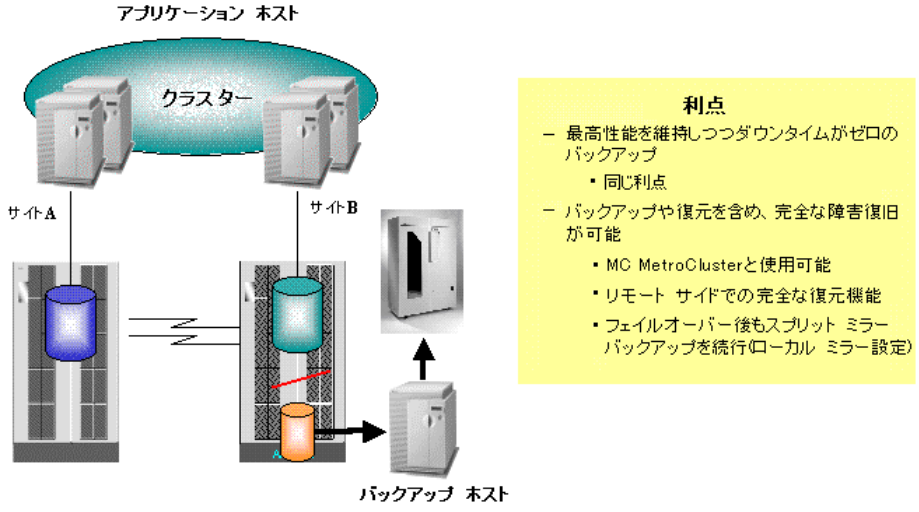

図 81 ローカル ミラーとリモート ミラーを組み合わせて使用(ディザスタ リカバリ統合バックアップ[サービスの高可用性 – HP-UXのみ)])

フェイルオーバー機能をバックアップ操作と分離させるには、バックアップ クライアントがクラスタの外部にある別のクライアントである必要があります。 MetroCluster

ソリューションを実行する場合、クラスタ調停クライアントをバックアップ クライアントとして使用できます。

その他の構成

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

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

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

13 スナップショットの概念

この章の内容

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

この章の構成は以下のとおりです。

概要

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

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

ストレージの仮想化

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

RAID

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

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

スナップショットの概念

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

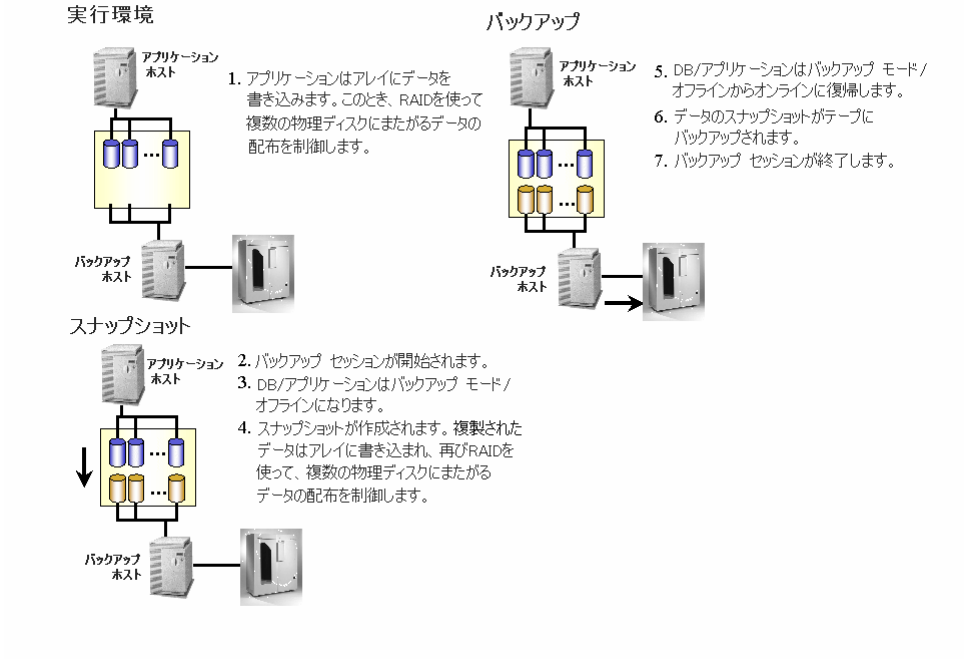

図 82 スナップショット バックアップ

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

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

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

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

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

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

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

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

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

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

スナップショット バックアップの種類

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

- テープへのZDB てーぷへのZDB
- ディスクへのZDB でぃすくへのZDB
- ディスク/テープへの ZDB

テープへのZDBとディスク+テープへのZDB

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

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

ディスクへのZDB でぃすくへのZDB

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

インスタント リカバリ

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

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

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

複製セットと複製セットのローテーション

ディスク アレイ上に同時に保持できる複製の最大数は、使用するディスク アレイによって異なります。 同一のバックアップ仕様に基づいてディスク アレイ上に保存されている複数の複製は、そのバックアップ仕様に対する**複製セット**を形成します。 この複製セットは、特定のバックアップ仕様に基づいてディスク アレイ上に保存される複製の最大数によって定義されます。 スナップショットのバックアップ セッションの際には、この番号に到達すると、複製セットの中の最も古い複製にあるスナップショット データが上書きされます。 番号に到達するまでは、新しい複製が作成されます。これら2つの動作は、**複製セットのローテーション**と呼びます。

スナップショットの種類

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

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

ディスク スペースの事前割り当てありのスナップショット

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

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

ディスク スペースの事前割り当てなしのスナップショット

ディスク スペースの事前割り当てなしのコピーオンライト スナップショットも元のデータの特定時点におけるコピーですが、ディスク容量の事前割り当ては必要ありません。ディスク スペースは必要に応じて動的に割り当てられます。 ソース ボリューム上のデータが変更されると、ディスク アレイ内の空きスペースを使ってスナップショットが作成されます。 ディスク スペースの事前割り当てなしのコピーオンライト スナップショットは、短期間のみ保持するスナップショットに適しています。 スナップショットデータのサイズは動的に拡張し続けるため、定期的に削除しなければ、最終的には記憶域の容量を使い切ってしまう点に注意してください。

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

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

スナップクローン

スナップクローンの作成時には、最初にディスク スペースの事前割り当てありのコピーオンライト スナップショットと同様の処理が行われ、その後クローン化プロセスが実行されます。 クローン化プロセスでは、ソース ボリューム上の全データがターゲット ボリュームにコピーされます。 スナップクローンを作成しておくと、複製データに迅速にアクセスできるようになります。 クローン化プロセス自体はディスク アレイの待ち時間を利用して、バックグラウンドで実行されます。 クローン化プロセスの完了時には、スナップクローンは、ソース ボリュームの特定時点の状態を表すフル データ コピーになります。 ソース ボリューム上のデータが損失した場合、スナップクローンを戻すことができます。

サポートされている構成

基本的な構成：単一のディスク アレイ(デュアル ホスト)

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

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

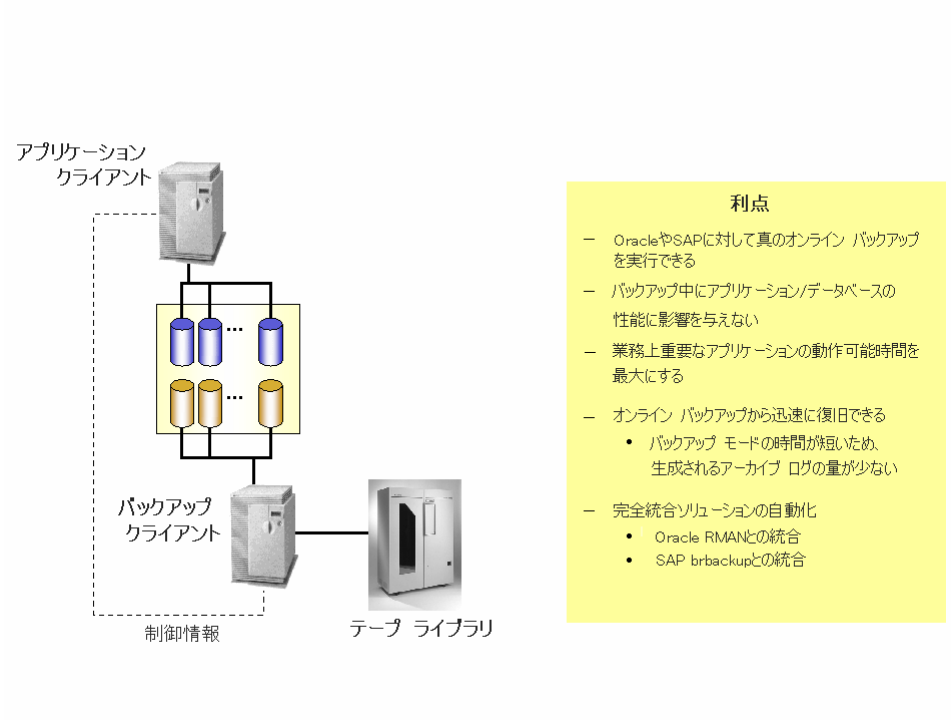

図 83 単一のディスク アレイ – デュアル ホスト(最高性能、ゼロ ダウンタイム バックアップ)

Data Protectorのスナップショット統合機能では、ディスク アレイ状態への自動対応のほか、アプリケーション(SAP R/3、Oracle、Microsoft SQLやExchange Serverなど)との緊密な統合が可能であるため、データの整合性や、アプリケーション/データベースに対応したバックアップの実行が保証されます。 アプリケーション/データベースがバックアップが行われていることを認識している場合に限り、安全な操作が保証されます。

この場合、アプリケーション固有のツールを使用して復元が行えます。 バックアップがアプリケーションに与える影響は、以下の手順を実行する時間にまで削減されます。

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

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

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

サポートされるその他の構成

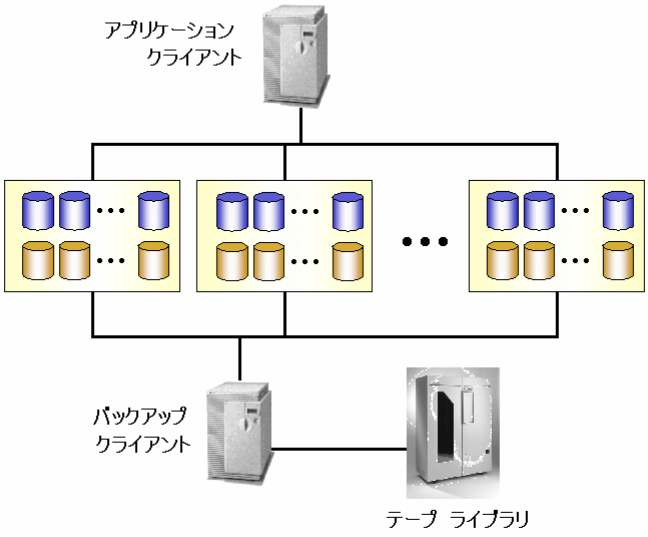

図 84 複数のディスク アレイ – デュアル ホスト

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

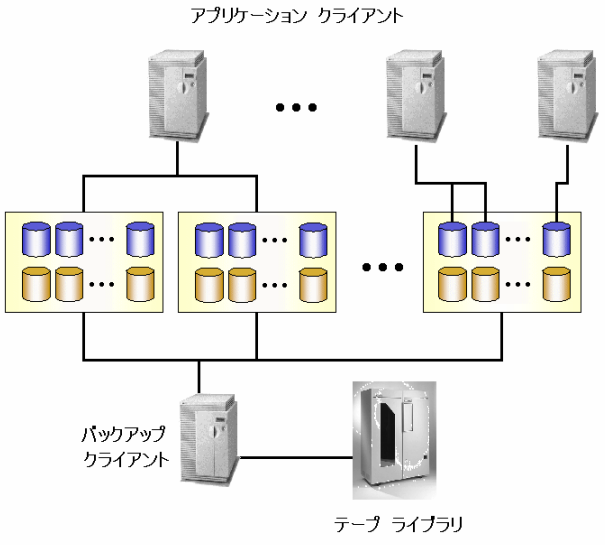

図 85 複数のアプリケーション ホスト – シングル バックアップ ホスト

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

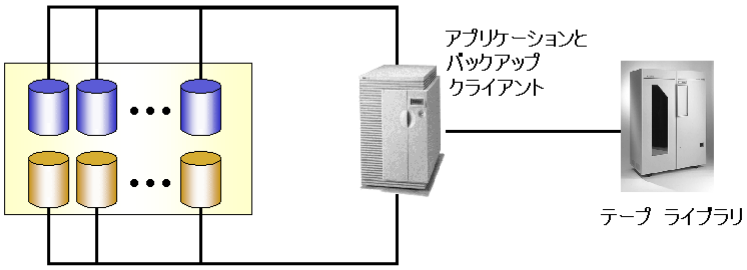

図 86 ディスク アレイ – シングル ホスト

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

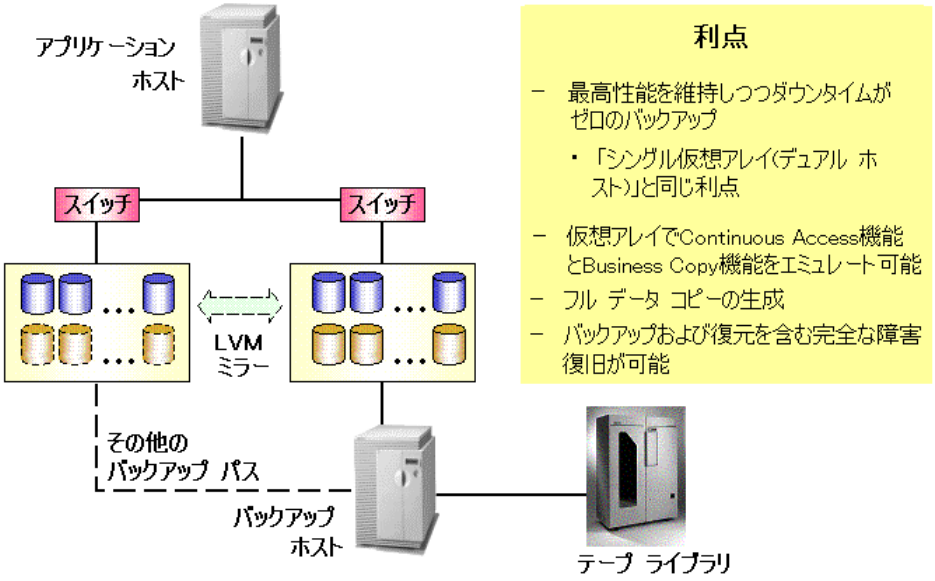

図 87 LVMミラー – HP StorageWorks Virtual Array のみ

前述したサポート対象構成では、HP StorageWorks Virtual Array統合ソフトウェアのBusiness Copy機能のみが使用可能です。 ただし、LVMミラーを使用すると、異なる仮想アレイ間にデータのスナップショット コピーを作成し、両方の仮想アレイに同時に書き込むことが可能になります。 これにより、HP StorageWorks Disk Array XPで使用可能なContinuous Access機能とBusiness Copy機能をエミュレートできます。

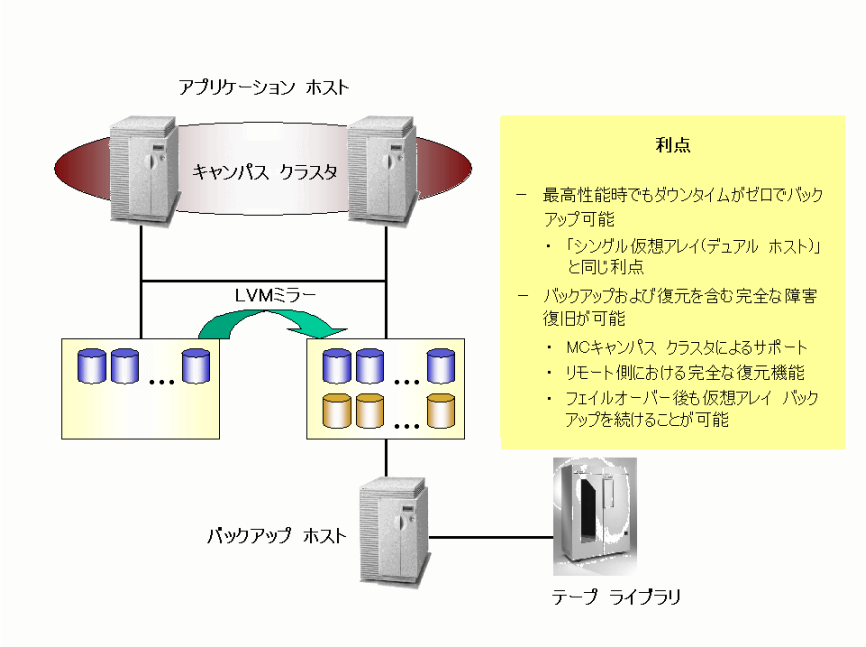

図 88 LVMミラーを使用するキャンパス クラスタ – HP StorageWorks Virtual Array のみ

この構成では、標準的なクラスタ フェイルオーバー機能に加えて、Continuous Access機能とBusiness Copy機能をエミュレートできます。 ミッション クリティカルなアプリケーションについては、しばしばこの構成が必要となります。

バックアップ クライアントとクラスタ

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

その他の構成

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

当社ではここに示す構成のみサポートしています。 サポートされる構成の最新情報は以下のURLを参照してください。 http://www.hp.com/support/manuals.

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

14 Microsoft Volume Shadow Copyサービス

この章の内容

この章では、Microsoft Volume Shadow Copyサービス(VSS)の概念と、バックアップ処理および復元処理におけるこの機能の役割について説明します。 また、この機能を使用する場合のバックアップ処理および復元処理の流れについても簡単に説明します。

この章の構成は以下のとおりです。

統合の詳細については、『HP Data Protector インテグレーションガイド』を参照してください。 ファイルシステムのバックアップと復元の詳細については、Data Protectorのオンライン ヘルプを参照してください。

概要

従来のバックアップ処理は、バックアップ アプリケーション(バックアップを開始および実行するアプリケーション)とバックアップ対象アプリケーションが直接交信しながら実行されます。 このバックアップ方式では、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。

市販されているアプリケーションは日々その数を増しています。 アプリケーション固有の機能を扱いながらバックアップ、復元、および保存の各処理を行うのには困難が伴います。 こうした問題に対する有効な解決策として登場したのが、バックアップや復元に関わる要素間に調整役を導入するやり方です。

VSS

Volume Shadow Copyサービス (VSS)は、Microsoft社によりWindowsオペレーティング システム上に採用されたソフトウェア サービスです。 このサービスは、バックアップ アプリケーション、バックアップ対象アプリケーション、シャドウ コピー 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。

Volume Shadow Copyサービスとは、統合された通信インタフェースを提供することにより、個々のアプリケーション固有の機能とは無関係に各アプリケーションのバックアップおよび復元を調整しようというものです。 このアプローチにより、バックアップ アプリケーションがバックアップ対象の各アプリケーションを個別に処理する必要がなくなります。 ただしこの方法を使えるのは、VSS仕様に準拠しているバックアップ アプリケーションに限られます。

シャドウ コピーとは

シャドウ コピー とは、元のボリュームの特定時点における複製であるボリュームを指します。 ボリュームシャドウコピー技術を使用すると、元のボリュームの特定時点におけるコピーを作成できます。 データのバックアップには、元のボリュームではなくこのシャドウ コピーが使われます。 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(例えばMS SQL Server用のMSDE ライターなど)またはシステム サービス(システム ライターやレジストリ ライターなど)です。 ライターはシャドウ コピーの同期プロセスにおいて、データの整合性を保証する働きをします。

シャドウ コピー プロバイダとは

シャドウ コピー プロバイダ とは、ボリューム シャドウ コピーの作成および提供に関わる処理を実行するなんらかの実体を指します。 シャドウ コピー プロバイダはシャドウ コピー データの所有者であり、シャドウ コピーを公開する働きをします。 シャドウ コピー プロバイダはソフトウェア(システム プロバイダやMS Software Shadow Copy Providerなど)の場合もあれば、ハードウェア(ローカル ディスクやディスク アレイ)の場合もあります。

ハードウェア プロバイダの例としてはディスク アレイが挙げられます。 ディスク アレイには特定時点におけるディスク状態を提供するための独自のハードウェア機構が備わっています。 ソフトウェア プロバイダは物理ディスクを操作し、ソフトウェア機構を使用して特定時点におけるディスク状態を提供します。 システム プロバイダであるMS Software Shadow Copy Providerはソフトウェア機構であり、Windows Server 2003オペレーティング システムに組み込まれています。

VSSではシャドウ コピーの作成時に、まずすべてのハードウェア プロバイダが優先して使用され、その後はじめてソフトウェア プロバイダが使用されるようにします。 いず

れのプロバイダでもシャドウ コピーを作成できなければ、VSSはシャドウ コピーの作成に(常に使用可能な) MS Software Shadow Copy Providerを使用します。

Data ProtectorとVSS

Volume Shadow Copyサービスはバックアップおよび復元時の、バックアップ アプリケーション、ライター、およびシャドウ コピー プロバイダ間の調整を可能にします。

図 89 (279ページ) と図 90 (280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。

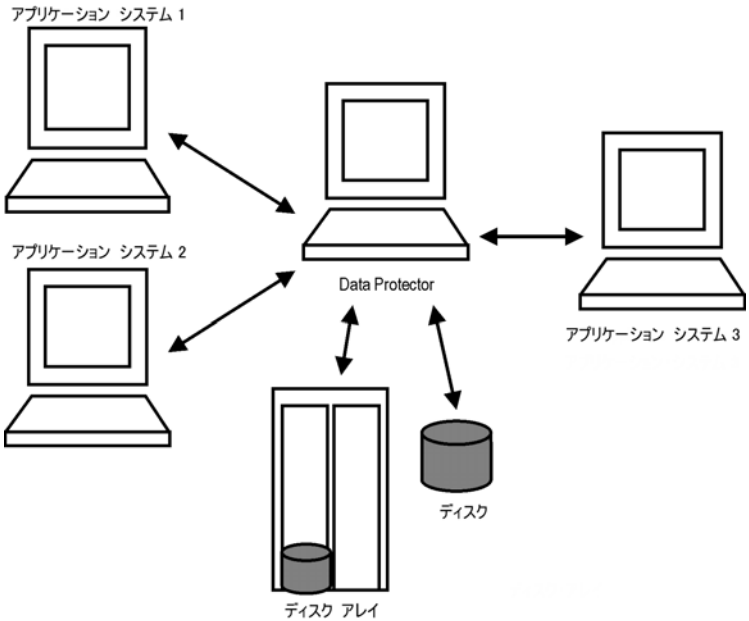

図 89 従来のバックアップ モデル

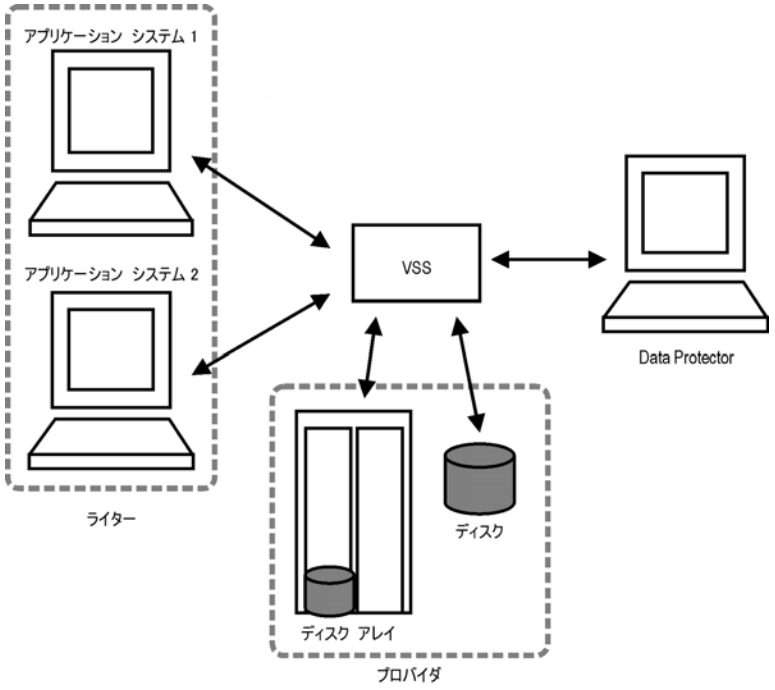

図 90 VSSバックアップ モデルに関係する要素

従来のモデルでは、バックアップ アプリケーションはバックアップ対象アプリケーションと個別のインタフェースで交信する必要があります。 一方VSSモデルの場合は、バックアップ アプリケーションはVSSとのみ交信し、バックアップ処理全体はVSSにより調整されます。

VSSの利点

Volume Shadow Copyサービスを使用する利点は以下のとおりです。

- 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 Volume Shadow Copyサービスを次の2つのレベルでサポートしています。

- Microsoft Volume Shadow Copyサービスと統合すると、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対応でない場合は、シャドウ コピーが作成されます。 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 14 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Volume Shadow Copyの統合

Data ProtectorとMicrosoft Volume Shadow Copyサービスを統合すると、VSS対応ライターを完全にサポートできるようになります。 このサポートには、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。 統合の詳細については、『HP Data Protector インテグレーションガイド』を参照してください。

VSSバックアップ

VSS対応ライターのバックアップでは、データの整合性はライター レベルで提供され、バックアップ アプリケーションには依存しません。Data Protectorでは、バックアップの対象を選択する際に、ライターから提供された要件に従います。

VSS対応ライターのバックアップ時には、Data Protectorが個々のライターと個別に交信することはなく、交信はVSSインタフェースを介して行われます。 Data ProtectorはVSS統合エージェントを使用してVolume Shadow Copyサービスと接続し、このサービスによりバックアップ処理が調整されます。 VSSからData Protectorに対して、整合性のあるバックアップと復元の実行に必要となる、ライターに関連するメタデータが提供されます。Data Protectorでこのデータが確認され、バックアップするボリュームが識別されます。その後、Data ProtectorからVSSに対して、指定したボリュームのシャドウ コピーを作成するよう要求します。

注記：

ライター メタデータ ドキュメント(WMD)とは、各ライターから提供されるメタデータです。 ライターはメタデータを使用して自身を識別し、バックアップの対象とデータの復元方法をバックアップ アプリケーションに指示します。したがって、Data Protectorでは、バックアップの対象とするボリュームと復元方法を選択する際に、ライターから指示される要件に従います。

Volume Shadow Copyサービスはライターとプロバイダを同期させる働きをします。バックアップ シャドウ コピーの作成が終了したら、VSSはこの情報をData Protectorに伝えます。 これを受けてData Protectorはシャドウ コピー ボリューム上のデータをメディアにバックアップし、作業が終了したらシャドウ コピーを解放してもよいことをVSSに通知します。

VSSの復元

VSSの統合復元とは、Volume Shadow Copyサービスとライターを使用してバップアップされたデータを復元することを意味します。 復元処理中は、Volume Shadow Copyサービスにより、Data Protectorとライター間の交信が調整されます。

VSS対応ライターの復元時には、Data Protectorは、最初に関連するすべてのメタデータを復元することにより、使用するバックアップ コンポーネントと復元方法を決定します。 次にVolume Shadow Copyサービスに接続し、復元処理の開始を宣言します。 復元中はVSSによりライターのアクティビティが調整されます。 Data Protectorによるデータの復元が成功したら、VSSからライターに復元処理の完了が通知されます。 これを受けてライターは復元されたデータへのアクセスと、自身の内部処理を開始できます。

VSSファイルシステムのバックアップと復元

アプリケーションの中にはVolume Shadow Copyサービスに対応していないものもあります。 このようなアプリケーションの場合は、シャドウ コピーの作成時にデータの整合性が保証されません。 VSSではこれらのアプリケーションのアクティビティを調整して、整合性のあるバックアップを実行することはできません。

ただしこの場合も、VSS機能によるメリットがまったくないわけではありません。 バックアップ アプリケーションとシャドウ コピー プロバイダの連携により、データ整合性レベルは向上します。 Microsoftではこのようなデータ整合性状態を「クラッシュ時整合データ」と呼んでいます。 シャドウ コピー ボリュームの準備中には、VSSにより、保留中のすべてのI/O操作がコミットされ、新たな書き込み要求は保留されます。 このようにしてシャドウ コピーの作成中はファイルシステム上のすべてのファイルが閉じられ、ロックは解除されます。

Microsoft Volume Shadow Copyを使用すると、バックアップ対象アプリケーションの関与なしにボリューム シャドウ コピーを作成できます。 この場合シャドウ コピー ボリュームの作成とバックアップは、Data Protectorにより実行されます。 このやり方は、VSSに対応していないアプリケーションに使用できます。

重要：

VSSに対応していないアプリケーションをバックアップする場合は、アプリケーション側から見たデータ整合性は保証されません。 データの整合性は、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 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。 例えばVSSファイルシステムバックアップでは、排他的に開かれているデータベースや、オペレータやシステム アクティビティにより開かれているファイルもバックアップされます。 このようにして、バックアップ中に変更が加えられたファイルも適正にコピーされます。

VSSファイルシステム バックアップの利点は以下のとおりです。

- アプリケーションやサービスを実行したままでコンピュータをバックアップできます。 バックアップの実行中もアプリケーションはボリュームへのデータ書き込みを継続できます。
- 開いているファイルもバックアップ中にスキップされません。 これはシャドウコピーの作成時に、これらのファイルがシャドウ コピー ボリューム上では閉じた状態になるためです。
- ユーザを締め出すことなくバックアップをいつでも実行できます。
- バックアップ 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バックアップはWindows Server 2003上に、追加のWindowsファイルシステムバックアップ機能として実装されています。 データ整合性のレベルは、従来の方法によるアクティブ ボリュームのバックアップに比べて多少向上しています。 Windowsファイルシステムのバックアップと復元の詳細については、オンライン ヘルプを参照してください。

VSSファイルシステム バックアップでは、アプリケーションがVSSに対応していないため、データ整合性の向上にアプリケーションが関与することは事実上できません。ただしこの場合も、Data Protectorとプロバイダは連携してボリューム シャドウ コピーの作成にあたります。 VSSファイルシステム バックアップを使用すると、バックアップ中のシステムI/O動作の有無に関わりなく、特定時点におけるデータ状態をバックアップすることが可能になります。

バックアップ仕様に指定されたボリュームのバックアップをData Protectorが要求すると、VSSにより、保留中のすべてのI/O操作がコミットされ、新たな書き込み要求は保留されて、シャドウ コピー ボリュームの準備が行われます。

シャドウ コピーの作成が終了したら、Data Protectorによる通常のバックアップ手順が開始されます。 ただしコピー元ボリュームは新たに作成されたシャドウ コピーで

置き換えられます。 シャドウ コピーの作成に失敗した場合は、Data Protectorで通常のファイルシステム バックアップを続行します(バックアップ仕様内でこの動作が指定されている場合)。

このように、ファイルが開かれていたりサービスが実行中であっても、コンピュータのバックアップが可能です。 この種のバックアップではファイルがスキップされることはありません。 VSSを使用するとシャドウ コピーの作成中も、実ボリューム上で実行中のサービスやアプリケーションが中断されることはありません。 バックアップが終了するとシャドウ コピーは削除されます。

VSSファイルシステム バックアップを使用してバックアップしたデータは、通常と同様の手順で復元できます。

A バックアップシナリオ

この付録の内容

この付録では、 XYZ社およびABC社という2つの企業のバックアップ シナリオを紹介します。 これらの企業では、自社のデータ記憶システムの強化を計画しています。 以下では、まず各企業の現在のバックアップ ソリューションとその問題点を説明します。 次にこれらの問題点を改善し、両社の将来のデータ量の増加にも対応できる新たなソリューションを提案していきます。

留意事項

どちらの企業の場合も、バックアップ戦略の策定時には、以下の点を考慮する必要があります。

- 各社にとってのシステム可用性(およびバックアップ)の重要度
  - 災害に備えてバックアップ データを遠隔地に保存する必要はあるか。
  - どの程度のビジネス継続運用性が求められるのか。 すべての重要なシステムの復旧および復元計画も検討する必要があります。
  - バックアップ データのセキュリティ対策
    構内への不法侵入に対する防御策の必要性を意味します。 関連するすべてのデータを不正アクセスから保護するための、物理的なアクセス防止策と電子的なパスワードによる保護策を含みます。
- バックアップするデータの種類
  企業データは、企業のビジネス データ、企業のリソース データ、プロジェクト データ、個人データなどに分類でき、データの種類別に個別の要件が存在します。
- バックアップおよび復元の性能
  - ネットワークおよびシステムのトポロジー
    どのシステムがどのネットワーク リンクを使用でき、転送速度はどの程度かを明らかにします。
  - バックアップ可能な時間枠
    各システムについてバックアップが可能な時間枠を明らかにします。
  - ローカル バックアップかネットワーク バックアップか
    バックアップ デバイスをどのシステムに接続し、どのシステムをローカルな形でバックアップし、どのシステムをネットワーク経由でバックアップするのかを決定します。
- バックアップ方針の実装
  - バックアップの実行方法とバックアップ オプションの選択

フル バックアップと増分バックアップの頻度を決定します。 また使用するバックアップ オプションを選択し、バックアップ メディアを遠隔地に保存してバックアップ データを永続的に保護するかどうかを決定します。

- バックアップ仕様作成時の各システムのグループ化方法
  バックアップ仕様をどのようにグループ化すればよいかを検討します。 部門、データの種類、バックアップの頻度などに基づく分類が考えられます。
- バックアップのスケジュール方法
  時差実行方式の採用を検討してください。これは、ネットワーク負荷、デバイス負荷、バックアップ可能な時間枠などに関する問題を軽減するために、クライアント(バックアップ仕様)ごとに日を変えてフル バックアップを実行するやり方です。
- メディア上のデータおよびバックアップ関連情報の保護期間
  以前のバックアップ データが新しいデータで上書きされないように、一定期間保護するかどうかを検討します。
  Data Protectorのカタログ データベース内にバックアップ関連情報を保存しておく期間を決定します。

- デバイスの構成
  バックアップに使用するデバイスと、デバイスを接続するシステムを決定します。 データ量が最も多いシステムにバックアップ デバイスを接続すると、多くのデータをネットワークを介さずにローカルにバックアップできるため、バックアップ速度が向上します。
  バックアップするデータ量が多い場合は、ライブラリ デバイスの使用も検討してください。
- メディア管理
  使用するメディアの種類、メディアをメディア プールにグループ化する方法、およびメディア上にオブジェクトを配置する方法を決定します。
- ボールティング
  メディアを安全な場所に一定期間保管するかどうかを決定します。
- バックアップ管理者とオペレータ
  バックアップ システム ユーザーに付与する管理権限や操作権限を決定します。

XYZ社のバックアップ

XYZ社は次のようなサービスを提供する翻訳会社です。

- 翻訳、ローカライズ、言語編集、および校正
- 翻訳ドキュメントの検証
- 同時通訳および逐次通訳
- DTP (デスクトップ パブリッシング)とグラフィック デザイン
- 会議用通訳機器のレンタル

XYZ社は現在年に20 ~ 25%の割合で成長を続けています。 同社の現在のバックアップ ソリューションでは、この成長率に対応できません。 またバックアップ テープを手動で取り扱っているため、バックアップの作業負荷が非常に高くなっています。

[環境]

ここでは、XYZ社の現在のハードウェア環境およびソフトウェア環境と、実装されているデータ記憶方針について説明します。

XYZ社は以下の3つの部門に分かれており、各部門は企業のネットワーク バックボーンに接続されています。

- 英語部門
- その他言語部門
- 管理部門

XYZ社の現在のハードウェア環境とソフトウェア環境は表 15（287ページ）に、また現在のバックアップ トポロジーは図 91（288ページ）に示すとおりです。

表 15 XYZ社のハードウェア環境とソフトウェア環境

部門	サーバ数	クライアント数	現在のデータ量	将来的なデータ量(5年後)	現在のデバイス
日本語	Windows 2000 1台	Windows 15台	35GB	107GB	HP StorageWorks DAT24オートローダ3台
その他言語	AIX 1台	UX 11台	22GB	67GB	HP StorageWorks DAT24オートローダ2台
管理者	1 HP-UX	UX 5台	10GB	31GB	HP StorageWorks DAT24オートローダ1台

図 91（288ページ）は、XYZ社のバックアップ環境を示したものです。

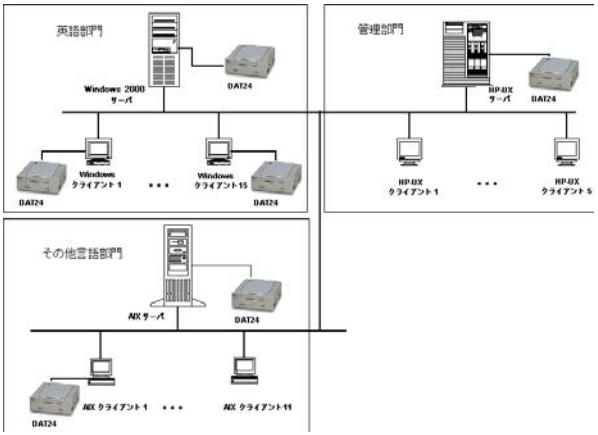

図 91 XYZ社の現在のバックアップ トポロジー

XYZ社では現在3台のサーバを使用しており、データ量は合計で約67GBに上ります。英語部門では、毎日の終業時に従業員がデータをそれぞれのサーバに手動でコピーしています。 英語部門のデータ量の約1/3 (12GB)は、この部門に属しているある1台のWindows 2000クライアントのデータです。

その他言語部門のクライアントは、ネットワーク ファイルシステムを介してバックアップされ、管理部門のクライアントはネットワーク共有を介してバックアップされています。 その他言語部門の従業員は、土曜日も働いています。

現在のソリューションの問題点

同社の現在のバックアップ ソリューションでは、XYZ社の成長率に対応できません。実際のバックアップ プロセスには、非常に労力を要します。 また現在のバックアップ プロセスのままでは、バックアップ管理の統合や、全社レベルでのバックアップ アーキテクチャの構築は不可能です。 各バックアップ サーバは個別に管理されます。 一元的なバックアップ管理の機能はありません。 次に、現在のバックアップ ソリューションの問題点を示します。

- バックアップ ソリューションが自動化されていません。
  - 従業員が手動でデータを定期的にコピーする必要があるため、ミスが生じる危険性が常にあります。
  - 複数のバックアップ ユーティリティが使われているため、トレーニング コストが高くつきます。
- その他言語部門と管理部門では多少は高度なソリューションが使われていますが、ここでも別の問題が発生しています。 まずこれらの部門では、ネットワークの使用状況がバックアップの性能に大きく影響します。 さらに、すべてのデータがバックアップされるわけではありません。 その他言語部門ではネットワーク ファイルシステム共有ファイルのみ、管理部門ではネットワーク共有ファイルのみがバックアップ対象となっています。

- 3つの部門で使われている3台のバックアップ サーバがそれぞれ独立しているため、以下に示すような重要な作業を一元的に制御および管理することができません。
  - デバイスの構成
  - メディア管理
  - バックアップ構成
  - スケジュール設定
  - 監視
  - 復元操作
- 各バックアップ サーバが個別に管理されているため、一元的なレポートを作成できません。
- 現在のソリューションには、ディザスタ リカバリ機能がありません。 これはますます重要性を増している問題点です。 大きな障害が発生すると、企業は重要なビジネス データを失う危険性があります。

バックアップ方針の要件

要件

「留意事項」 (285ページ) に示す項目を検討すると、XYZ社のバックアップ ソリューションについて以下の要件が明らかになります。

- バックアップ方針
  - 週1回フル バックアップを実行し、12時間以内に処理を終了しなければなりません。
  - 毎営業日には業務の最後に増分バックアップを実行し、この処理は8時間以内に終了しなければなりません。
  - 永続的なデータ保護期間を設定します。
  - バックアップ メディアは遠隔地に保管します。
- バックアップ
  すべてのバックアップ操作について、現在よりもオペレータの介入を減らす必要があります。
- 復元
  - 最近作成したバックアップ データは、簡単かつ迅速に復元できなければなりません。 バックアップから3週間が経過するまでは、復元するデータをブラウズできるようにしておきます。
  - ボールトに保管してあるバックアップ データも、2日以内に復元できなければなりません。
- ネットワーク接続
  バックアップ サーバと各部門は、100TX Ethernet LANで接続します。
- データ量の増加予測
  今後5年間のデータ増加率は、年20 ~ 25%程度と予測されます。

- ソフトウェア
  バックアップ サーバは、サポートされているオペレーティング システム上で実行する必要があります。 Cell Managerでサポートされているオペレーティング システムの詳細は、『HP Data Protector product announcements 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。
- 障害対策
  バックアップに使用したメディアは、ファイルを復元する場合に備えて、そのまま現場に保管しておきます。 20日が経過したら、企業サイトでの災害の発生に備えるとともに、新たなバックアップ データの保管場所を空けるためにも、外部の保管場所に移送します。

提案ソリューション

現在のバックアップ ソリューションでは、バックアップの性能と全社レベルの管理の両面で限界があるため、XYZ社の経営目的に合わせてバックアップのアーキテクチャと戦略を再設計する必要があります。 以下では、まずソリューション案の概要を説明し、次にこのソリューションの詳細を紹介していきます。 これはXYZ社のデータ管理に対する唯一のソリューションではなく、1つの提案にすぎない点に注意してください。

提案内容概要

すべてのクライアントとサーバを単一のData Protectorセル内に構成し、英語部門のWindows 2000 ServerをCell Manager兼Windowsシステム用のInstallation Serverとして使用します。 UNIXシステム用のInstallation Serverには、管理部門のHP-UXバックアップ サーバを使用します。 またバックアップ デバイスには、HP StorageWorks DLT 4115w Library 1台と、既存のHP StorageWorks DAT24オートローダのうちの2台を使用します。 この構成で、今後5年間における年20～25%というデータ増加率に十分に対応できます。 また、これまで使われてきたデバイスを使用することは、ディザスタ リカバリの面で付加的な利点があります。 英語部門のデータ量の約1/3(12GB)を保持するWindows 2000クライアントは、HP StorageWorks DAT24オートローダにローカルな形でバックアップできるようにします。 このバックアップ ソリューション案では、以下の主要目的が達成されています。

- バックアップの性能が向上します。
- 最小限の手間でメディアを管理できます。
- 簡潔かつ効率的なディザスタ リカバリが可能です。
- 一元的なバックアップ レポートを作成できます。
- 大部分のバックアップ操作が自動化されます。

このソリューションにおけるこれらの機能はすべて、次に示すハードウェアと組み合わせることで達成されます。

表 16 提案されるバックアップ環境

部門	現在のデータ量	将来的なデータ量 (5年後)	デバイス	
英語*	35 GB	107 GB	HP DLT 4115 Library	HP StorageWorks DAT24オートローダ2台
その他言語	22GB	67GB		
管理者	10 GB	31 GB		
* 現時点では、12GBのデータをローカルにバックアップするために、1台のHP StorageWorks DAT24オートローダが使用されます。 もう1台のHP StorageWorks DAT24オートローダは、IDBと構成ファイルのバックアップに使用されます。 この部門の残りのデータは、HP StorageWorks DLT 4115 Libraryにリモートでバックアップされます。				

残り4台のHP StorageWorks DAT24オートローダは別のR&Dシステムで使われており、この構成には含まれません。

この企業バックアップ ソリューション向けに提案されるソフトウェア コンポーネントには、HP Data Protector A.06.10も含まれます。

ソリューション案の詳細

以下に、このソリューション案の詳細について説明します。

- セルの構成
  すべてのクライアントとサーバは、単一のData Protectorセル内に構成します。 Data Protector Cell Managerは、英語部門のWindows 2000 Server上で実行します。
  最大の性能を引き出すには、セル内のすべてのシステムを同一LAN上に配置する必要があります。 Cell Managerは、同時にWindows用のInstallation Serverとしても使用します。 UNIX用のInstallation Serverには、管理部門のHP-UXバックアップ サーバを使用してください。 HP StorageWorks DLT 4115w Libraryは、IDBと構成ファイルをバックアップするためのHP StorageWorks DAT24オートローダ1台とともに、Cell Managerに接続します。 英語部門のデータ量の約1/3 (12GB)を保持するWindows 2000クライアントは、HP StorageWorks DAT24オートローダにローカルな形でバックアップできるようにします。
  ここで提案したバックアップ環境は、図 92 (292ページ) に示すとおりです。

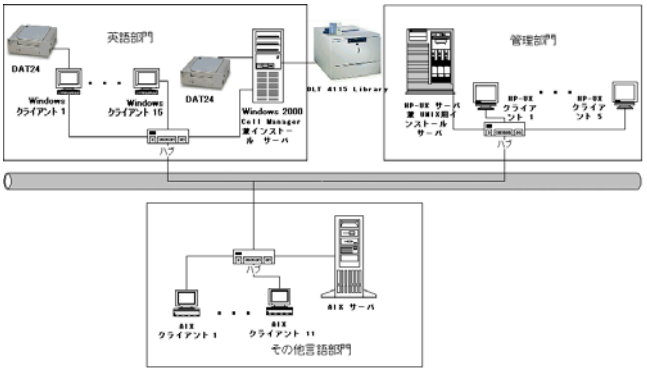

図 92 XYZ社のバックアップ トポロジー案

- Cell Managerでは、CDB (Catalog Database、カタログ データベース)が保守されます。 これにより現在のデータベース上に、バックアップされたファイルやディレクトリに関する詳細情報が最低20日間保存されます。

IDBサイズの見積もり

IDBの1年間のサイズ変化の見積もりには、Internal Database Capacity Planning Toolを使用しています。 このツールはData Protectorのその他のオンライン マニュアルと同じディレクトリにあります。 図 93 (293ページ) に示す入力パラメータでは、環境内のファイル数(2,000,000)、拡張係数(1.2)、データ保護期間(52週間)、カタログ保護期間(3週間)、1週間に行うフル バックアップの回数(1回)、1週間に行う増分バックアップの回数(5回)を指定しています。

Environment description			
	Files:	2	million
	Files per directory:	10	
	Data volume:	200	GB
	Growth factor:	1.20	
	Device performance:	10.00	MB/second
	Medium capacity:	70.00	GB
	Objects:	50	
	Change per incr-bkup	5.00%	
Backup parameters			
	Device concurrency:	2	
	Data segment size:	2,048.00	MB
	Log level:	All	
	Data protection:	52	Weeks
	Catalog protection:	3	Weeks
	Full backups/week:	1	
	Incr backups/week:	5	
Cell Manager parameters			
	Insertion speed:	12	million/hour

図 93 入力パラメータ

図 94（294ページ）に結果を示します。 データベースは1年間で約419.75MBまで増加すると予測されます。

Results/calculation			
	Avg. file size:	123.36	KB
	Files/segement:	16,931.38	
	Catalog size:	1.03	MB
	K devices:	40	
	K performance:	1445.647059	GB/hour
	K duration:	0.14	hour
	Protected media:	278.5714286	

Space estimation			
MMDB:		30.00	MB
CDB:	Fnames:	153.00	MB
	Overs:	5.71	MB
	Mpos:	1.54	MB
DCBF:		229.50	MB
SMBF:		2.86	MB
Total:		419.75	MB

図 94 結果

- ハードウェア
  - [ネットワーク]
    最大の性能を引き出すには、すべてのシステムを同一の100TXネットワーク上に配置する必要があります。 このネットワークは、10MB/s (36GB/h)のデータ転送速度を維持できます。
  - バックアップ デバイス
    バックアップ デバイスには1台のHP StorageWorks DLT 4115w Libraryと、2台のHP StorageWorks DAT24オートローダを使用します。
    HP StorageWorks DLT 4115w Libraryを使う理由
    HP StorageWorks DLT 4115w Libraryには、1つのDLT4000ドライブと15個のスロットがあります。 このライブラリは圧縮状態で合計600GBの記憶容量を持ち、データを圧縮した状態で3MB/s (10.5GB/h)のデータ転送速度を維持できます。 以下の説明ではこの転送速度を前提としています。 現時点では、HP StorageWorks DLT 4115w Libraryにフル バックアップする必要があるデータの総容量は、単一のフル バックアップまたは時差実行方式のいずれを使用する場合も、約55GBになります。 増分バックアップのサイズをフル バックアップの約5%と見積もると、1つのバックアップ世代、つまり1つのフル バックアップとそのフル バックアップをベースとするすべての増分バックアップがライブラリに占める容量は(55+55*5%*5)GB、つまり**68.75GB**になります。 5年後には、この値は約210GBにまで増加すると予測されます。 XYZ社のバックアップ方針では、2つのバックアップ世代を保持しておく必要があります。 したがって、210*2 GB (420 GB)のライブラリ領域がストレージに必要になります。 そのため、600GBの記憶容量を持つHP StorageWorks DLT 4115w Libraryで十分に対応できます。
    HP StorageWorks DAT24オートローダを使う理由
    HP StorageWorks DAT24オートローダには、24GBのデータ カートリッジが6個あります。 圧縮状態で合計144GBの記憶容量を持ち、データを圧

縮した状態で最大2MB/s (7GB/h)のデータ転送速度を維持できます。 以下の説明ではこの転送速度を前提としています。 現時点では、前述した英語部門のWindows 2000クライアントに接続されたHP StorageWorks DAT24オートローダに1回のフル バックアップで保存する必要があるデータの総容量は12GBになります。 増分バックアップのサイズをフル バックアップの約5%と見積もると、 1つのバックアップ世代、つまり1つのフル バックアップとそのフル バックアップをベースとするすべての増分バックアップのサイズは(12+12*5%*5) GB、つまり**15GB**になります。 5年後には、この値は約45GBにまで増加すると予測されます。 XYZ社のバックアップ方針では、2のバックアップ世代を保持しておく必要があります。 したがって、45*2 GB (**90 GB**)のライブラリ領域がストレージに必要になります。 そのため、144GBの記憶容量を持つHP StorageWorks DAT24オートローダで十分に対応できます。

フル バックアップに要する時間

12GBのデータを持つ英語部門のWindows 2000クライアントは、HP StorageWorks DAT24オートローダにローカルな形でバックアップされます。 このデバイスは2MB/s、つまり約7GB/hのデータ転送速度を維持できます。 そのため、このWindows 2000クライアントのフル バックアップには、約**2時間**かかると計算できます。 データ量は1年間で20 ~ 25%増加するため、このクライアントでは、5年後には約36 GBのデータが保存されていると予想されます。 このデータは約**6時間**でバックアップされます。

Data Protectorカタログ データベースのサイズは約0.4GBです。 これはHP StorageWorks DAT24オートローダにローカルな形でバックアップされます。このデバイスは2 MB/s、つまり7 GB/hのデータ転送速度を維持できます。Data Protectorでは、デフォルトでデータベースをバックアップする前にデータベースの整合性を確認します。 0.4GBのデータベースの整合性チェックは30分以内に終了し、データベースのバックアップ自体は数分程度で終了します。 そのため、IDBの整合性チェックと、データベースおよび構成ファイルのバックアップは、**1時間**以内に終了すると計算できます。

カタログ データベースのサイズは、5年後には約1.2GBになると予測されます。 1.2GBのデータベースの整合性チェックは1時間以内に終了し、バックアップ自体は30分以内に終了します。 そのため、IDBの整合性チェックと、データベースおよび構成ファイルのバックアップは、**2時間**以内に終了すると計算できます。

システム上の他のすべてのデータは現時点で約55GBあり、HP StorageWorks DLT 4115w Libraryにリモートの形でバックアップされます。このデバイスは3 MB/s、つまり10.5 GB/hのデータ転送速度を維持します。このデータの大部分は、100TXネットワーク経由で転送されます。このネットワークは10 MB/s、つまり36 GB/hのデータ転送速度を維持できます。 これらのデータの大部分は、100TXネットワークを介して転送されますが、このネットワークは10MB/s、つまり36GB/hのデータ転送速度を維持できるため、ネットワークがボトルネックになることはなりません。 そのため、これらのデータをすべてバックアップするには、約**5 ~ 7時間**かかると計算できます。 現時点では許容限度の12時間以内に終了するため問題ありませんが、5年後にはデータ量が約170GBになると予測され、バックアップに15 ~ 21時間もかかることになってしまいます。

この問題を解決するには、時差実行方式を採用します。 例えば英語部門のフル バックアップは金曜日の20:00に開始し、その他言語部門のフル バックアップは土曜日の20:00に、また管理部門のフル バックアップは日曜日の20:00に開始するというようにスケジュールを設定します。

表 17 時差実行方式

	月	火	水	木	金	土	Sun
日本語	増分1	増分1	増分1	増分1	Full（挿入中）	増分1	
その他言語	増分1	増分1	増分1	増分1	増分1	Full（挿入中）	
管理者	増分1	増分1	増分1	増分1	増分1		Full（挿入中）

現時点および5年後の、これらのフル バックアップのサイズとバックアップにかかる時間は、表 18 (296ページ)に示すとおりです。

表 18 HP DLT 4115 Libraryへのリモートのフル バックアップ

部門	現在のデータ量/バックアップ時間	将来的なデータ量/バックアップ時間
日本語	23 GB / 3 H	70 GB / 7 H
その他言語	22 GB / 3 H	67 GB / 7 H
管理者	10 GB / 1 H	31 GB / 3 H

増分バックアップのサイズをフル バックアップの約5%とすると、5年後に、最大の部門である英語部門のリモートのフル バックアップと、他の2つの部門の増分バックアップをすべて実行するには、7+5% (7+3)時間かかります。 つまり8時間以内に処理を終了できます。 そのため、5年後も、許容限度の12時間以内に処理を終了できるとわかります。

- Media Pools（メディア プール）
  追跡や制御を容易にするために、個々のメディアはメディア プールと呼ばれるグループにまとめられます。 ここでは、メディアを、メディアの種類(DLTとDDS)ごとのプールにまとめます。
  - デフォルトDDS
    このプールはすべてのDDSメディア用に使用します。
  - デフォルトDLT
    このプールはすべてのDLTメディア用に使用します。
  - DB_Pool
    このプールはIDBと構成ファイル用に使用します。 データベースは、セキュリティ上の理由により、2つのメディアにバックアップする必要があります。

- [バックアップ仕様の使用法に関するレポート]
  各部門用と、IDBおよび構成ファイル用に、以下の5つのバックアップ仕様を構成します。
  - ENG1_BS
    英語部門内の、ローカルにバックアップする必要があるWindows 2000クライアント用のバックアップ仕様です。 このバックアップ仕様では、例えば、毎週金曜日にData Protectorによってフル バックアップが実行されるようにスケジュールを設定し、さらに金曜と日曜を除く毎日20:00にレベル1増分バックアップが実行されるように設定します。

レベル1増分バックアップを使う理由

最新のデータを復元する場合に、2つのメディア セット、つまり最新のフル バックアップと、復元時点よりも前に作成された最新のレベル1増分バックアップの2つのみになります。 そのため復元処理が簡単になり、処理時間も大幅に短縮されます。

  - ENG2_BS
    英語部門のデータのうち、HP StorageWorks DLT 4115w Libraryにリモートでバックアップするデータ用のバックアップ仕様です。 このバックアップ仕様では、例えば、毎週金曜日にData Protectorによってフル バックアップが実行されるようにスケジュールを設定し、さらに日曜を除く毎日20:00にレベル1増分バックアップが実行されるように設定します。
  - OTH_BS
    その他言語部門のデータのうち、HP StorageWorks DLT 4115w Libraryにリモートでバックアップするデータ用のバックアップ仕様です。 このバックアップ仕様では、例えば、毎週土曜日の20:00にData Protectorによってフル バックアップが実行されるようにスケジュールを設定し、さらに日曜を除く毎日20:00にレベル1増分バックアップが実行されるように設定します。
  - ADM_BS
    管理部門のデータのうち、HP StorageWorks DLT 4115w Libraryにリモートでバックアップするデータ用のバックアップ仕様です。 このバックアップ仕様では、例えば、毎週日曜日の20:00にフル バックアップがData Protectorによって実行されるようにスケジュールを設定し、さらに土曜日を除く毎日20:00にレベル1増分バックアップが実行されるように設定します。
  - DB_BS
    IDBと構成ファイル用のバックアップ仕様です。 このバックアップ仕様では、例えば、毎日4:00にフル バックアップがData Protectorによって実行されるようにスケジュールを設定します。このときには、他のフル バックアップや増分バックアップは完了していて、Cell Managerと他のクライアントシステムとの間でCPUリソースの共有に関する問題が生じないようにします。 データベースについては、2つのコピーを作成する必要があります。

[バックアップオプション]

- デフォルトのData Protectorバックアップ オプションを使用します。 以下のオプションを以下に示すように設定します。

- カタログ保護(Catalog Protection)
  [カタログ保護(Catalog Protection)]オプションでは、バックアップ バージョンに関する情報、バックアップされたファイルやディレクトリの数に関する情報、データベースに保存されているメッセージなどを、Data Protectorカタログ データベース内に保存しておく期間を設定します。 カタログ保護期間が切れると、Data Protector GUIを使ったファイルやディレクトリのブラウズはできなくなります。 カタログ保護期間は20日に設定します。
- データ保護
  [データ保護(Data Protection)]オプションでは、各メディアの再使用を許可するまでの期間を設定します。 メディア上のデータを誤って上書きしないように、データ保護期間は[無期限(Permanent)]に設定します。
- 同時処理数
  このオプションは5に設定して、最大5つのDisk AgentがHP StorageWorks DLT 4115w Libraryに同時にデータを書き込めるようにします。 これにより、バックアップの性能が向上します。
- [Media Pool]
  IDBについては、適切なバックアップ メディアが含まれているDB_Poolを選択します。 その他のオブジェクトについては、デフォルトのメディア プールを使用します。

リストアのオプション

- デフォルトのData Protector復元オプションを使用します。 以下のオプションを以下に示すように設定します。
  - [復元されたデータをリスト(List Restored Files)]
    このオプションはオンに設定して、復元されたファイルとディレクトリのパス名の一覧が作成されるようにします。 復元するファイルの数が非常に多い場合は、このオプションにより処理速度が低下することがあります。
  - [統計情報の表示(Display Statistical Information)]
    このオプションはオンに設定して、復元セッションに関する詳細な統計情報が表示されるようにします。統計情報には、復元されたファイルとディレクトリの数や、復元されたデータ量などが含まれます。
- レポートと通知
  電子メール通知をセットアップしておき、すべてのバックアップ仕様に関するマウント要求、データベース容量の不足、デバイス エラー、セッション終了イベントなどがバックアップ管理者に送信されるようにします。 電子メールまたはブロードキャスト通知を使って、エンド ユーザーに自分のシステムのバックアップが成功したかどうかを知らせることも可能です。
  また、すべてのユーザーがバックアップ状態を簡単にチェックできるように、企業のイントラネット上にクライアント バックアップ情報を以下に示すようにセットアップします。
  1. [クライアントのバックアップをレポート(Client Backup Report)]を使って、各クライアントごとにレポート グループを構成します。 レポートはHTML形式でログ ファイルに記録してください。
  2. レポート グループのスケジュールを設定します。

3. ログ ファイルを企業のイントラネット ページにリンクします。

- ボールティング
  ボールティングとは、メディアを安全な場所に一定期間保管するプロセスを指します。
  メディアは毎週1回保管場所(ボールト)に移送され、HP StorageWorks DLT 4115w LibraryとHP StorageWorks DAT24オートローダ内には新しいメディアがセットされます。 メディアを実際にボールトに移送する作業を除き、すべての処理はソフトウェアにより実行されます。 例えば、データベースの照会も内部的に自動実行されるため、排出するメディアを管理者が自分で探す必要はありません。
  その後メディアはボールトから警備会社に再び移送されます。 これは1か月に1度行います。Data Protectorからは、警備会社に移送する必要があるメディアの一覧レポートが提供されます。
  ボールトに移送したメディアについても、引き続き保管場所を追跡する必要があります。 この情報は、警備会社に移されたメディアからデータを復元するような場合に重要になります。Data Protectorでは、次のボールティング処理を実行できます。
  - 指定された場所に保管されており、指定された日時にデータ保護期間が切れるバックアップ メディアの一覧レポートを生成できます。
  - 指定された期間内に作成されたバックアップ メディアの一覧レポートを生成できます。
  - 指定したメディアをバックアップ中に使用したバックアップ仕様の一覧を表示できます。
  - 復元に必要なメディアの一覧と、そのメディアが保管されている物理的位置を表示できます。
  - なんらかの基準に基づいて(保護期間が切れたメディアなど)、メディア ビューに表示するメディアをフィルタリングできます。
- 復元
  - 照会ごとに復元
    照会による復元要求は、管理者に送られます。 要求されたファイルが20日以内にバックアップされている場合は、管理者は復元タスクの[照会による復元(Restore by Query)]を使って、なんらかの基準に基づいて復元するファイルやディレクトリを選択できます。 次に管理者は、ディスク上のファイルやディレクトリをメディアに保管されているバージョンで上書きするために、[上書き(Overwrite)]オプションを選択します。
  - ファイルシステム全体の復元
    ファイルシステム全体の復元要求も、管理者に送られます。 要求されたファイルが20日以内にバックアップされている場合は、管理者は復元するオブジェクトを選択できます。 ファイルシステム全体の復元では、[復元先を指定して復元(Restore Into)]オプションが使われます。
    [復元先を指定して復元(Restore Into)]オプションを選択すると、オブジェクトは正確なディレクトリ構造を保ったままで選択したディレクトリに復元されます。 WindowsまたはUNIXのユーティリティを使うと、復元したオブジェクトとバックアップ オブジェクトを比較できます。

- ボールトからの復元
  ボールトに保管されている、例えば3年前のデータを復元する場合は、まず要求を管理者に送ります。これを受けて管理者は以下の処理を実行します。
  1. 復元に必要なメディアを特定します。
  2. メディアをボールトから搬入し、HP StorageWorks DLT 4115w Libraryまたはその他のデバイスに挿入してスキャンします。
  3. そのメディアがIDB内になければ、[メディアからリスト(List From Media)]オプションを使って復元するオブジェクトを選択します。
  4. 復元処理を実行します。.

ABC社のバックアップ

ABC社は成長著しいソフトウェア エンジニアリング企業であり、南アフリカのケープタウンに本部を置いています。 ABC社はさまざまな国のビジネス パートナーからソフトウェアを受注しており、複数のサイトにまたがるプロジェクト チームと、それに対応したインフラストラクチャを構築して、広範囲にわたるソフトウェア エンジニアリング プロジェクトをシームレスに実行できるようにしています。 ABC社は年に30 ~ 40%の割合で成長を続けています。 成長率は、次の5年間で、15 ~ 20%に減速すると予想されています。

[環境]

ここでは、ABC社の現在のハードウェア環境およびソフトウェア環境と、実装されているデータ記憶方針について説明します。

ABC社のオフィスは3つの場所に分かれています。 それぞれのオフィスの主要なハードウェア構成は、表 19 (300ページ)に示すとおりです。

表 19 バックアップ環境の構成内容

場所	Win サーバ数	Winクライアント数	UXサーバ数	UXクライアント数	現在のデータ量	将来的なデータ量(5年後)	現在のデバイス
ABC ケープタウン	7	55	11	40	100	250	DAT24* 5台
ABCプレトリア	5	39	5	32	22	55	DAT24* 1台
ABC ダーバン	3	21	6	59	16	40	DAT24* 1台
* HP StorageWorks DAT24オートローダ							

ABCケープタウンにある3つの部門では、データの保存にMicrosoft SQLデータベースを使っています。 また企業全体のメール サービスには、Microsoft Exchange Serverが使われています。 現時点ではこれらのデータベースには、それぞれ11GBおよび15GBのデータが保存されており、2台のHP StorageWorks DAT24オートローダを使ってバックアップされています。

ABCケープタウンのシステム アーキテクチャには、Oracleデータベースを使用したSAP R/3システムが含まれています。 3台のHP T600サーバが、SAPデータベースサーバとして使用されています。 またABCケープタウンでは、販売と流通、経理、および製造の各業務グループ別に構成された、複数のK260 SAPアプリケーションサーバが使われています。 これらのアプリケーション サーバは高可用性構成にはなっていません。 ABCケープタウンの現在のバックアップ環境は、図 95 (301ページ)に示すとおりです。

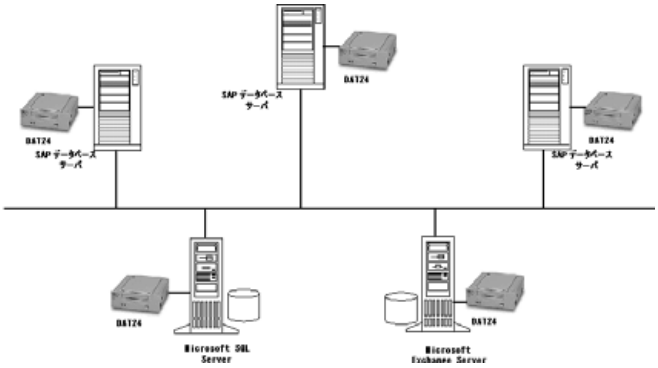

図 95 ABCケープタウンの現在のバックアップ トポロジー

現在のところ、ABCケープタウンのSAPデータベース サーバは、SAP BRBACKUPユーティリティとBRARCHIVEユーティリティを使って、3台のHP StorageWorks DAT24オートローダにバックアップされています。 データは1日1回、従業員が手動でそれぞれのサーバにコピーしています。 またバックアップ管理者は、Microsoft Exchange ServerとMicrosoft SQLデータベースをそれぞれ個別にHP StorageWorks DAT24オートローダにバックアップしています。

ABCダーバンとABCプレトリアでも同一のシステムが使われていますが、これらのサイトではSAPシステムは使われていません。 従業員は各自のデータをそれぞれのサーバにコピーします。 データはHP StorageWorks DAT24オートローダに1日1回バックアップされます。

ABCプレトリアのサーバのうちの2台には、それぞれ500 000個以上のファイルが保存されています。

バックアップ メディアには、部門名、サーバ名、およびそのメディアを使ったバックアップの最初と最後の日付が示されています。 四半期の終わりには、メディアは外部の保管場所に移されて一元的に管理されます。

現在のソリューションの問題点

現在のバックアップ ソリューションには、以下の問題点があります。

- SAPデータベース サーバに対するオンライン バックアップ ソリューションがありません。
- バックアップ ソリューションが一元管理されていません。
- バックアップ操作が完全には自動化されていません。
- メディア管理にかなりのオペレータの介入が必要になります。
- ディザスタ リカバリが複雑です。
- バックアップ処理が、バックアップに許される時間枠内に終了しません。
- 現在のバックアップ ソリューションでは、ABC社の成長率に対応できません。
- バックアップに関する重要イベントについての報告や通知の機能がありません。

バックアップ方針の要件

ABC社のバックアップ方針の要件を明らかにするには、まず「留意事項」 (285ページ) の項目を検討する必要があります。

要件

以下に、ABC社のバックアップ戦略の要件について説明します。

- バックアップと復元に関する企業ポリシー
  データの記録や保存に関するこの企業のポリシーに従って、週単位のバックアップは**12時間**以内に終了しなければならず、毎日の増分バックアップは、**8時間**以内に終了しなければなりません。
- 復旧までに許される最大ダウンタイム
  復旧までに許されるダウンタイムは、バックアップに必要なネットワーク基盤や機器を整備するための予算に大きく影響します。 以下の表は復旧までに許されるダウンタイム、つまりバックアップ データからデータを復元するまでの間、どれくらいの期間であればデータを利用できなくても許されるかを、データの種類別に示したものです。

  表 20 復旧までに許される最大ダウンタイム

データの種類	最大ダウンタイム
企業のビジネス データ	6時間
企業のリソース データ	6時間
プロジェクト データ	1日
個人データ	2 日

  復旧までに要する時間は、主としてメディアへのアクセスと、データを実際にディスクに復元する作業に費やされます。
- 各種データの保管期間
  表 21 (303ページ) には、データの保管期間が示されています。 データの保管期間は、必要となるバックアップ メディアの数に直接影響します。

表 21 データの保管期間

データの種類	最大データ保管期間
企業のビジネス データ	5年
企業のリソース データ	5年
プロジェクト データ	5年
個人データ	3か月

- バックアップ データを格納したメディアの保管および保守の方法
  メディアはコンピュータ室内のテープ ライブラリに保管します。 企業のバックアップ システムの対象となるデータは、いずれも、週1回フル バックアップを作成し、毎日増分バックアップを作成する必要があります。 データは警備会社に保管します。
- バックアップする必要があるデータ量
  現時点でバックアップする必要があるデータ量は、表 22 (303ページ)に示すとおりです。

表 22 バックアップする必要があるデータ量

場所	データ量(GB)
ABCケープタウン	100
ABCプレトリア	22
ABCダーバン	16

将来的なデータ量の増加への対応
ABC社は年に15 ~ 20%の割合で成長を続けると予測されています。 バックアップするデータ容量も、それに従って増大すると考えられています。 データ量の増加は、バックアップに要する時間やバックアップに必要なデバイスの数だけでなく、IDBのサイズにも影響を及ぼします。

表 23 5年後にバックアップする必要があるデータ量

場所	データ量(GB)
ABCケープタウン	250
ABCプレトリア	55
ABCダーバン	40

- データのバックアップ頻度
  データはそれぞれの種類ごとに、金曜、土曜、日曜のいずれかに毎週1回フル バックアップを作成します。 またレベル1増分バックアップは、平日に必ず実行します。 ただし、フル バックアップを金曜日に実行する場合、金曜を除く平日と土曜日に、対応するレベル1増分バックアップを実行します。

提案ソリューション

現在のソリューションの問題点（301ページ）に示した現在のバックアップ ソリューションの問題点を解決するために、ABC社ではデータ記憶システムの再設計を検討しています。

提案内容概要

ABCケープタウンの3つの部門は、いずれも同一のManager-of-Managers (MoM)セル内に構成します。 さらにABCダーバンとABCプレトリアについても個別のMoMセルを構成し、各MoMセル内にはそれぞれ2つのData Protectorセルを含めます。

セルAをABCケープタウン環境のMoMセルとして構成します。 同様に、セルDをABCプレトリア環境のMoMセルとして構成し、セルFをABCダーバン環境のMoMセルとして構成します。 図 96（304ページ）に、この構成を示します。

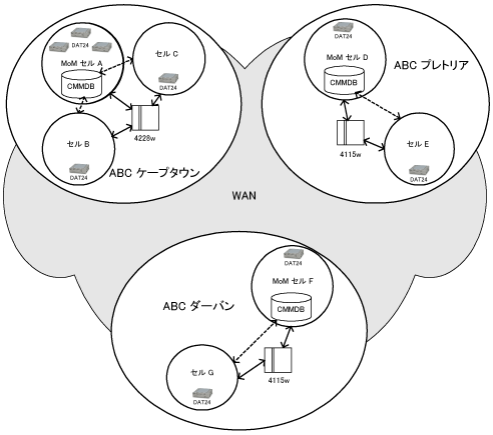

図 96 ABC社のバックアップ環境

これらの7つのセル内のCell ManagerとMoM Managerは、いずれもWindowsシステムでなければなりません。 メディア集中管理データベース(CMMDB)は各MoM環境のいずれか1つのセル内にのみ構成し、カタログ データベースは7つのセルのすべてに構成します。 メディア集中管理データベースを使うと、同じMoM環境に所属するセル間でライブラリを共有できます。

ABC社の3箇所にあるオフィスでは、それぞれ専用のライブラリを使用します。 ABCケープタウン環境では、HP StorageWorks DLT 4228w Libraryを使用します。 またABCプレトリア環境とABCダーバン環境では、HP StorageWorks DLT 4115w Libraryを使用します。

ABCケープタウンのMoM環境に含まれる3つのセルには、SAPデータベース サーバがそれぞれ1台ずつあります。 これらのSAPデータベース サーバは、1台のHP StorageWorks DLT 4228w Libraryを共有します。 またMicrosoft SQLデータベース

とMicrosoft Exchangeデータベースは、HP StorageWorks DAT24オートローダにローカルな形でバックアップされます。

ABCプレトリアのMoM環境内の2つのセルでも、同一のメディア集中管理データベースを共有します。 このデータベースはセルDのMoM Manager上に構成して、2つのセル間でHP StorageWorks DLT 4115w Libraryを共有できるようにします。

ABCダーバンのMoM環境内の2つのセルでも、同一のメディア集中管理データベースを共有します。 このデータベースはセルFのMoM Manager上に構成して、2つのセル間でHP StorageWorks DLT 4115w Libraryを共有できるようにします。

以下に、このソリューション案の詳細について説明します。

ソリューション案の詳細

- セルの構成
  各部門を7つのセルに分けて構成します。ABCケープタウンに3つ、ABCプレトリアとABCダーバンにそれぞれ2つずつです。

7つのセルに分割する理由

- ABC社の各部門は地理的に離れているため、単一のセルで管理するのは困難です。 さらに、システム間のネットワーク接続に伴う問題が発生する可能性もあります。 構成は部門の数と一致していますが、これはセキュリティの観点からも重要な意味を持っています。 各セル内には、それぞれ30～50台のクライアント システムを含めることが推奨されます。 ただしこの数は、各クライアント システムが所有するファイルやディレクトリの数などの条件に大きく依存します。

次に、3つの環境をそれぞれManager-of-Managers環境として構成します。MoMを使うと単一のポイントから、効率よく、透過的かつ一元的に複数のセルを管理できます。 MoMを構成したら、 それぞれのMoM環境でメディア集中管理データベース(CMMDB)を構成します。

CMMDBを使う理由

- メディア集中管理データベース(CMMDB)を使用すると、同じMoM環境内のすべてのセルでデバイスやメディアを共有できるようになります。 そのためABC社の3つのMoM環境でも、それぞれの環境に所属するすべてのセル内のクライアント システムで、1つのライブラリを共有できます。ABC社の全データを単一の大容量ライブラリに保存する方法は合理的ではありません。 この方法では、バックアップ時にWANを介して大量のデータを転送しなければなりません。

カタログ データベースは、7つのセルのそれぞれに必要です。 セル内のシステム構成は、表 24 (306ページ) に示すとおりです。

表 24 ABC社のセル構成

MoM環境	セル	Windows サーバ数	Windows クライアント数	UNIX サーバ数	UNIXクライアント数	SAP数
ABCケープタウン	A*	3	24	2	7	1
	B	2	11	5	21	1
	C	2	20	4	12	1
ABCプレトリア	D*	4	33			
	E	1	6	5	32	
ABCダーバン	F*	2	10	4	30	
	p	1	11	2	29	
SAP数とは、SAPデータベース サーバの数を意味します。						
* はMoMセルを表します。						

これらの7つのセル内のCell ManagerとMoM Managerは、いずれもWindowsシステムでなければなりません。

Windowsシステムを選ぶ理由

- Windowsシステムでは標準でUnicode形式がサポートされているため、他のシステムに比べて、ファイル名に使われている各国の文字を正しく取り扱うための構成が容易です。

ABCケープタウン環境では、セルAをManager-of-Managersセルとして構成し、残りのセルをこのMoM環境にインポートします。 MoMセルAにメディア集中管理データベースを構成すると、セルBとセルCでも同一ライブラリを共有できるようになります。 ABCケープタウン環境では、1台のHP StorageWorks DLT 4228w Libraryを共有します。 このライブラリは圧縮形式で1.1TBのデータを保存できるため、今後5年間に予測されるデータ増加率に十分に対応できます。 ABCケープタウンの3つのセルには、それぞれに1つのSAPデータベース サーバが必要です。 これらのSAPデータベース サーバは、1台のHP StorageWorks DLT 4228w Libraryを共有します。 またMicrosoft SQLデータベースとMicrosoft Exchangeデータベースは、既存のHP StorageWorks DAT24オートローダにローカルな形でバックアップされます。 またこの環境内の各セルでは、それぞれに個別のカタログ データベースが必要です。 ケープタウン環境の構成は、図 97 (307ページ)に示すとおりです。

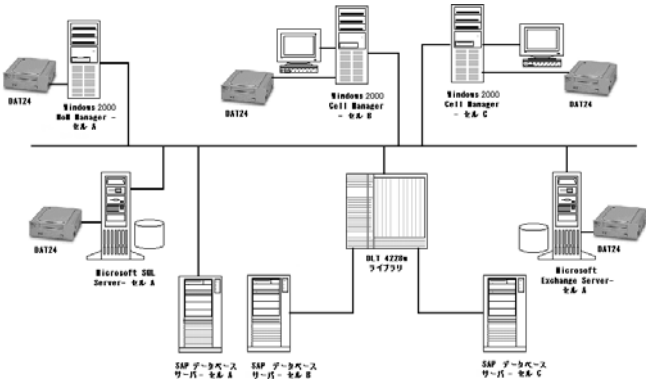

図 97 ABCケープタウンのバックアップ環境

ABCプレトリアのMoM環境内の2つのセルでも、メディア集中管理データベースを共有する必要があります。 このデータベースはセルDのMoM Manager上に構成します。CMMDBを使用する目的は、セル間でHP StorageWorks DLT 4115w Libraryを共有できるようにすることです。 またこの環境内の各セルでは、それぞれに個別のカタログ データベースが必要です。
同様にABCダーバンのMoM環境内の2つのセルでも、メディア集中管理データベースを共有する必要があります。 このデータベースは、セルFのMoM Manager上に構成します。 ダーバン環境内の各セルでも、それぞれ個別のカタログ データベースが必要です。
ABCプレトリア環境およびABCダーバン環境では、HP StorageWorks DLT 4115w Libraryを使用します。 このライブラリは圧縮形式で600GBのデータを格納できるため、これらの環境で今後5年間に予測されるデータ増加率に十分に対応できます。

IDBサイズの見積もり

セルF内のIDBの1年間のサイズ変化の見積もりには、Internal Database Capacity Planning Toolを使用しています。 このツールは次の場所にあります。

- HP-UXおよびSolaris Cell Managerの場合： /opt/omni/doc/C/IDB_capacity_planning.xls
- Windows Cell Managerの場合： *Data_Protector_home*\docs\IDB_capacity_planning.xls

図 98 (308ページ) に示す入力パラメータでは、環境内のファイル数(2,000,000)、拡張係数(1.2)、データ保護期間(260週間)、カタログ保護期間(3週間)、1週間に行うフル バックアップの回数(1回)、1週間に行う増分バックアップの回数(5回)を指定しています。

Environment description			
	Files:	2	**million**
	Files per directory:	10	
	Data volume:	16	**GB**
	Growth factor:	1.20	
	Device performance:	10.00	**MB/second**
	Medium capacity:	70.00	**GB**
	Objects:	100	
	Change per incr-bkup	10.00%	
Backup parameters			
	Device concurrency:	2	
	Data segment size:	2,048.00	**MB**
	Log level:	All	
	Data protection:	260	**Weeks**
	Catalog protection:	3	**Weeks**
	Full backups/week:	1	
	Incr backups/week:	5	
Cell Manager parameters			
	Insertion speed:	12	**million/hour**

図 98 入力パラメータ

図 99（309ページ）に結果を示します。 データベースは1年間で約667.47MBまで増加すると予測されます。

Results/calculation			
	Avg. file size:	7.29	KB
	Files/segement:	269,057.37	
	Catalog size:	16.42	MB
	K devices:	2	
	K performance:	85.48173913	GB/hour
	K duration:	0.19	hour
	Protected media:	133.7142857	

Space estimation			
MMDB:		30.00	MB
CDB:	Fnames:	207.00	MB
	Overs:	57.13	MB
	Mpos:	0.74	MB
DCBF:		372.60	MB
SMBF:		5.72	MB
Total:		667.47	MB

図 99 結果

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

- ハードウェア
  - [ネットワーク]
    性能を最大限に引き出すには、同じオフィス内のすべてのシステムを同一LAN上に配置する必要があります。 それぞれのオフィス内のシステム同士は100TXネットワークで接続し、3つのオフィス内の各セル同士はWANで接続します。 100TXネットワークは、10MB/s (36GB/h)のデータ転送速度を維持できます。
  - バックアップ デバイス
    バックアップ デバイスには、ABCケープタウン用にHP StorageWorks DLT 4228w Libraryを1台、ABCプレトリアとABCダーバン用にHP StorageWorks DLT 4115w Libraryを2台、すべてのセル内のIDBと構成ファイルをバックアップするためにHP StorageWorks DAT24オートローダを7台、およびABCケープタウンのMicrosoft SQLデータベースとMicrosoft Exchangeデータベースをバックアップするためにに HP StorageWorks DAT24オートローダを2台使用します。 Microsoft Exchange ServerとMicrosoft SQL Serverの現時点でのデータ容量はそれぞれ15GBと11GBであり、それ以外のデータ(100GB −15GB − 11GB = 74GB)は、3台のSAPデータベース サーバにバックアップされます。

HP StorageWorks DLT 4228w Libraryを使う理由

- HP StorageWorks DLT 4228w Libraryには、2つのDLT4000ドライブと28個のスロットがあります。 このライブラリは圧縮状態で合計1.1TBの記憶容量を持ち、データを圧縮した状態で最大6MB/s (2 x 3MB/s)、つまり21GB/hのデータ転送速度を維持できます。 以下の説明ではこの

転送速度を前提としています。 現時点では、HP StorageWorks DLT 4228w Libraryにフル バックアップする必要があるデータの総容量は、単一のフル バックアップまたは時差実行方式のいずれを使用する場合も、約74GBになります。 増分バックアップのサイズをフル バックアップの約5%と見積もると、1つのバックアップ世代、つまり1つのフル バックアップとそのフル バックアップをベースとするすべての増分バックアップがライブラリに占める容量は、(74+74*5%*5) GB、つまり**92.5GB**になります。 5年後には、この値は約230GBにまで増加すると予測されます。 ABC社のバックアップ方針では、3つのバックアップ世代を保持しておく必要があります。 したがって、230*3 GB (690 GB)のライブラリ領域がストレージに必要になります。 そのため、1.1TBの記憶容量を持つHP StorageWorks DLT 4228w Libraryで十分に対応できます。

ABCケープタウンのライブラリは、このオフィスの3つのセル間で共有されます。 またABCプレトリア環境のライブラリはセルDとセルEで、ABCダーバン環境のライブラリはセルFとセルGでそれぞれ共有されます。 このように構成する場合は、3つのMoM環境のそれぞれで、Data Protectorメディア集中管理データベースを使用する必要があります。 このデータベースはセルA、D、FのMoM Manager上にそれぞれ構成します。

HP StorageWorks DLT 4115w Libraryを使う理由

- HP StorageWorks DLT 4115w Libraryには、1つのDLT4000ドライブと15個のスロットがあります。 このライブラリは圧縮状態で合計600GBの記憶容量を持ち、データを圧縮した状態で3MB/s (10.5GB/h)のデータ転送速度を維持できます。 以下の説明ではこの転送速度を前提としています。 現時点では、ABCプレトリアでHP StorageWorks DLT 4115w Libraryにフル バックアップする必要があるデータの総容量は、単一のフル バックアップまたは時差実行方式のいずれを使用する場合も、約22GBになります。 増分バックアップのサイズをフル バックアップの約5%と見積もると、1つのバックアップ世代、つまり1つのフル バックアップとそのフル バックアップをベースとするすべての増分バックアップがライブラリに占める容量は(22+22*5%*5) GB、つまり**27.5GB**になります。 5年後には、この値は約68.75GBにまで増加すると予測されます。社のバックアップ方針では、3つのバックアップ世代を保持しておく必要があります。 したがって、68.75*3 GB (206.25 GB)のライブラリ領域がストレージに必要になります。 そのため、600GBの記憶容量を持つHP StorageWorks DLT 4115w Libraryで十分に対応できます。

ABCケープタウンのMicrosoft Exchange ServerとMicrosoft SQL Server、および3つのMoM環境内の7つのCell Managerのバックアップには、HP StorageWorks DAT24オートローダが使われます。

HP StorageWorks DAT24オートローダを使う理由

- HP StorageWorks DAT24オートローダには、24GBのデータ カートリッジが6個あります。 圧縮状態で合計144GBの記憶容量を持ち、データを圧縮した状態で最大2MB/s (7GB/h)のデータ転送速度を維持できます。以下の説明ではこの転送速度を前提としています。 現時点では、前

述したABCケープタウンのMicrosoft Exchange Serverに接続されたHP StorageWorks DAT24オートローダにバックアップする必要があるデータの総容量は15GBになります。 増分バックアップのサイズをフル バックアップの約5%と見積もると、 1つのバックアップ世代、つまり1つのフル バックアップとそのフル バックアップをベースとするすべての増分バックアップのサイズは(15+15*5%*5) GB、つまり**18.75GB**になります。 5年後には、この値は約47GBにまで増加すると予測されます。 ABC社のバックアップ方針では、2つのバックアップ世代を保持しておく必要があります。 したがって、47*2 GB (**94 GB**)のライブラリ領域がストレージに必要になります。 そのため、144GBの記憶容量を持つHP StorageWorks DAT24オートローダで十分に対応できます。

フル バックアップに要する時間

ABCケープタウンの3つのセル内にあるSAPデータベース サーバには、HP StorageWorks DLT 4228w Libraryにバックアップする必要があるデータが合計74GBあります。 このライブラリには2つのドライブがあり、6MB/s (2 x 3MB/s)、つまり21GB/hのデータ転送速度を維持できます。 そのためこのライブラリにデータをバックアップするには、**最大約5時間**かかることになります。 5年後のデータ量は185GBになり、バックアップ時間は**9 ~ 10時間**になると予測されるため、5年後も、許容限度の12時間以内に処理を終了できるとわかります。
ABCプレトリアのセルDとセルEでは、1台のHP StorageWorks DLT 4115w Libraryを共有します。 このライブラリには1つのドライブがあり、3MB/s、つまり10.5GB/hのデータ転送速度を維持できます。 これらのセルでバックアップする必要があるデータ量は全体で約22GBあり、約**2 ~ 3時間**でバックアップできます。 5年後のデータ量は55GBになり、バックアップ時間は**5 ~ 7時間**になると予測されるため、5年後も、許容限度の12時間以内に処理を終了できます。
同様に、ABCダーバンのセルFとセルGのデータ量は約16GBあり、**最大約2時間**でバックアップできます。 5年後のデータ量は40GBになり、バックアップ時間は**約4時間**になると予測されるため、5年後も、許容限度の12時間以内に処理を終了できます。
ABCプレトリアのData Protectorカタログ データベースは最大で1.3GBであり、事前にデータベースの整合性の確認を行わない場合は数分でバックアップできます。Data Protectorでは、データベースをバックアップする前にデフォルトで整合性を確認します。 確認に要する時間は、1.3 GBのデータベースで1時間未満です。 したがって、ABCプレトリアのIDBおよび構成ファイルは、**2時間**未満でバックアップされると考えられます。

- Media Pools (メディア プール)
  追跡や制御を容易にするために、個々のメディアはメディア プールと呼ばれるグループにまとめられます。 メディア プールを使うと多数のメディアを効率よく管理できるため、バックアップ管理者の負担が軽減されます。 ここでは、企業の組織構造やシステム カテゴリに基づいて、以下のメディア プールを定義します。

表 25 ABC社のメディア プールの使用

メディア プール名	場所	[Description]
CT_SAP_Pool	ケープタウン	SAPデータベース サーバ
CT_SQL_Pool	ケープタウン	Microsoft SQL Server
CT_Exchange_Pool	ケープタウン	Microsoft Exchange Server
CT_DB_Pool	ケープタウン	IDB
P_DLT_Pool	プレトリア	HP StorageWorks DLT 4115w Library
P_DAT_Pool	プレトリア	HP StorageWorks DAT24オートローダ
P_DB_Pool	プレトリア	IDB
D_DLT_Pool	ダーバン	HP StorageWorks DLT 4115w Library
D_DAT_Pool	ダーバン	HP StorageWorks DAT24オートローダ
D_DB_Pool	ダーバン	IDB

- [バックアップ仕様の使用法に関するレポート]
  バックアップ仕様は以下のように構成します。
  - DB_A...G
    7つのIDBと構成ファイル用のバックアップ仕様です。 このバックアップ仕様では、例えば、週1回フル バックアップがData Protectorによって実行されるようにスケジュールを設定し、さらに日曜を除く毎日03.00にレベル1増分バックアップが実行されるように設定します。

差分(増分1)バックアップを使う理由

- 最新のデータを復元する場合に、2つのメディア セット、つまり最新のフル バックアップと、復元時点よりも前に作成された最新のレベル1増分バックアップの2つのみになります。 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。 単純な増分バックアップを使用する場合は、より多くのメディア セットが必要になるため、復元処理が複雑になり処理時間も長くなります。

IDBと構成ファイルについては、セキュリティ上の理由により、2つのコピーを作成します。

- SAP_A...C
  セルA、B、C内のSAPデータベース サーバ用のバックアップ仕様です。 ネットワーク負荷、デバイス負荷、およびバックアップ可能な時間枠に関する問題を回避するために、表 26 (313ページ) に示す時差実行方式を使用します。

表 26 ABCケープタウンにおける時差実行方式

	月	火	水	木	金	土	Sun
セルA	増分1	増分1	増分1	増分1	Full（挿入中）	増分1	
セルB	増分1	増分1	増分1	増分1	増分1	Full（挿入中）	
セルC	増分1	増分1	増分1	増分1	増分1		Full（挿入中）

- SERVERS_A...G
  ディザスタ リカバリに備えるための、企業のサーバ用のバックアップ仕様です。 新しいサーバをインストールしたとき、または既存のサーバをアップグレードしたときは、このバックアップ仕様も更新しなければなりません。 このバックアップ仕様では、例えば、表 27（314ページ）に示すような形でData Protectorによってフル バックアップが実行されるようにスケジュールを設定し、さらに平日には毎日レベル1増分バックアップが実行されるように設定します。
- USERS_D...G
  ユーザー データ用のバックアップ仕様です。 これは、ABCプレトリアおよびABCダーバンで作成される主要なバックアップ データです。 このバックアップ仕様では、表 27（314ページ）に示すような形でData Protectorによってフル バックアップが実行されるようにスケジュールを設定します。 例えば、毎週金曜日にフル バックアップが、また平日には毎日レベル1増分バックアップが実行されるように設定します。 ただし、フル バックアップを金曜日に実行する場合、金曜を除く平日と土曜日に、対応するレベル1増分バックアップを実行します。

表 27（314ページ）は、バックアップ仕様の構成の詳細を示したものです。

表 27 ABC社のバックアップ仕様の構成

[名前]	セル	説明	バックアップ曜日	Time
DB_A	A	IDB	土曜日	03:00
DB_B	B	IDB	土曜日	03:00
DB_C	C	IDB	土曜日	03:00
SQL_A	A	Microsoft SQLデータベース	金曜日	20:00
EXCHANGE_A	A	Microsoft Exchangeデータベース	金曜日	20:00
SAP_A	A	SAPデータベース サーバ	金曜日	20:00
SAP_B	B	SAPデータベース サーバ	土曜日	20:00
SAP_C	C	SAPデータベース サーバ	日曜日	20:00
SERVERS_A	A	サーバ	金曜日	23:00
SERVERS_B	B	サーバ	土曜日	23:00
SERVERS_C	C	サーバ	日曜日	23:00
DB_D	D	IDB	土曜日	03:00
DB_E	E	IDB	土曜日	03:00
SERVERS_D	D	サーバ	金曜日	23:00
SERVERS_E	E	サーバ	土曜日	23:00
USERS_D	D	ユーザー データ	土曜日	0:00
USERS_E	E	ユーザー データ	日曜日	0:00
DB_F	F	IDB	土曜日	03:00
DB_G	G	IDB	土曜日	03:00
SERVERS_F	F	IDB	金曜日	23:00
SERVERS_G	G	サーバ	土曜日	23:00
USERS_F	F	ユーザー データ	土曜日	0:00
USERS_G	G	ユーザー データ	日曜日	0:00

[バックアップオプション]

デフォルトのData Protectorバックアップ オプションを使用します。 以下のオプションを以下に示すように設定します。

- [ディレクトリ レベルまでログに記録(Log Directories)] でぃれくとり れべるまでろぐにきろく(Log Directories)
  このファイルシステム バックアップ オプションを使うと、ディレクトリに関する詳細情報のみがカタログ データベースに保存されます。 このオプションを選択した場合は、復元時に検索機能を使用できず、ディレクトリのブラウズのみが可能になります。 セルDにそれぞれ50万以上のファイルがある2台のサーバをバックアップするには、このオプションを使用します。このオプションを使用しないと、Data Protectorカタログ データベースのサイズが大幅に増加します。
- 保護
  バックアップ後3週間は、データに簡単にアクセスできなければなりません。 フル バックアップは週1回しか実行しないため、カタログ保護は27日(3週間*7日+6日=27日)と設定します。
  Exchange_A以外のバックアップ仕様については、データ保護期間を5年と設定します。 Exchange_Aは個人メール用のバックアップ仕様です。 このバックアップ仕様については、データ保護期間を3か月と設定します。
- 同時処理数
  このオプションは5に設定して、最大5つのDisk Agentがライブラリに同時にデータを書き込めるようにします。 これにより、バックアップの性能が向上します。
- [Media Pool]
  バックアップに使う適切なメディア プールとメディアを選択します。

- レポートと通知
  電子メール通知をセットアップしておき、すべてのバックアップ仕様に関するマウント要求、データベース容量の不足、デバイス エラー、セッション終了イベントなどがバックアップ管理者に送信されるようにします。 電子メールまたはブロードキャスト通知を使って、エンド ユーザーに自分のシステムのバックアップが成功したかどうかを知らせることも可能です。
  また、すべてのユーザーがバックアップ状態を簡単にチェックできるように、自社のホーム ページ上にクライアント バックアップ情報を以下に示すようにセットアップします。
  1. [クライアントのバックアップをレポート(Client Backup Report)]を使って、各クライアントごとにレポート グループを構成します。 レポートはHTML形式でログ ファイルに記録してください。
  2. レポート グループのスケジュールを設定します。
  3. ログ ファイルを自社のホーム ページにリンクします。
- ボールティング
  ボールティングとは、メディアを安全な場所に一定期間保管するプロセスを指します。

メディアは毎週1回保管場所(ボールト)に移送され、HP StorageWorks DLT 4228w Library、HP StorageWorks DLT 4115w Library、およびHP StorageWorks DAT24オートローダには新しいメディアがセットされます。 メディアを実際にボールトに移送する作業を除き、すべての処理はソフトウェアにより実行されます。 例えば、データベースの照会も内部的に自動実行されるため、排出するメディアを管理者が自分で探す必要はありません。
ボールトに移送したメディアについても、引き続き保管場所を追跡する必要があります。 この情報は、ボールトに移されたメディアからデータを復元するような場合に重要になります。Data Protectorでは、次のボールティング処理を実行できます。

- 指定された場所に保管されており、指定された日時にデータ保護期間が切れるバックアップ メディアの一覧レポートを生成できます。
- 指定された期間内に作成されたバックアップ メディアの一覧レポートを生成できます。
- 指定したメディアをバックアップ中に使用したバックアップ仕様の一覧を表示できます。
- 復元に必要なメディアの一覧と、そのメディアが保管されている物理的位置を表示できます。
- なんらかの基準に基づいて(保護期間が切れたメディアなど)、メディア ビューに表示するメディアをフィルタリングできます。

- 復元
  - 照会ごとに復元
    照会による復元要求は、管理者に送られます。 要求されたファイルが3週間以内にバックアップされている場合は、管理者は復元タスクの[照会による復元(Restore by Query)]を使って、なんらかの基準に基づいて復元するファイルやディレクトリを選択できます。 次に管理者は、ディスク上のファイルやディレクトリをメディアに保管されているバージョンで上書きするために、[上書き(Overwrite)]オプションを選択します。
  - ファイルシステム全体の復元
    ファイルシステム全体の復元要求も、管理者に送られます。 要求されたファイルが3週間以内にバックアップされている場合は、管理者は復元するオブジェクトを選択できます。 ファイルシステム全体の復元では[復元先を指定して復元(Restore Into)]オプションが使われます。
    [復元先を指定して復元(Restore Into)]オプションを選択すると、オブジェクトは正確なディレクトリ構造を保ったままで選択したディレクトリに復元されます。 WindowsまたはUNIXのユーティリティを使うと、復元したオブジェクトとバックアップ オブジェクトを比較できます。
  - ボールトからの復元
    ボールトに保管されている、例えば3年前のデータを復元する場合は、まず要求を管理者に送ります。これを受けて管理者は以下の処理を実行します。
    1. 復元に必要なメディアを特定します。
    2. メディアをボールトから搬入し、HP StorageWorks DLT 4228w Library、HP StorageWorks DLT 4115w Library、またはその他のデバイスに挿入してスキャンします。

3. そのメディアがData Protectorのカタログ データベース内になければ、[メディアからリスト(List From Media)]オプションを使って復元するオブジェクトを選択します。
4. 復元処理を実行します。.

B 詳細情報

この付録の内容

この付録では、バックアップ世代、自動メディア コピー(Automated Media Copy)の例、国際化に関する情報など、Data Protectorの概念に関する追加情報について説明します。

バックアップ世代

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

バックアップ世代とは

図 100 (319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)。

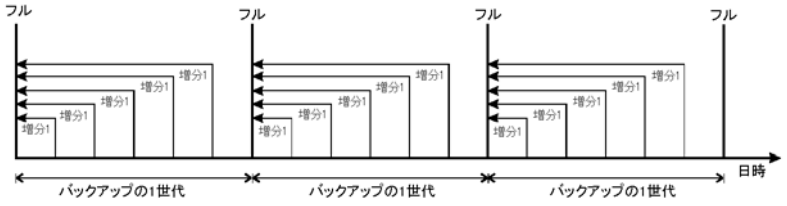

図 100 バックアップ世代

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

例えば、週1回のフル バックアップと1日1回の増分バックアップを実行する場合に、3つのバックアップ世代を保管するには、データ保護期間を7*3+6=27日と設定します。

1つのバックアップ世代は、1つのフル バックアップと、その次のフル バックアップまでに実行されるすべての増分バックアップで構成されます。 式に含まれる6という数値は、4番目のバックアップ世代が作成されるまでに、3番目のバックアップ世代に属する増分バックアップが実行される回数を表しています。

適切なプール使用方法を設定しておくと、保護期間が切れたメディアを自動交換させることもできます。 詳細については、「メディア交換方針の実装」 (134ページ）を参照してください。

自動メディア コピーの例

バックアップが終了したら、自動メディア コピー(Automated Media Copy)機能を使用してメディアをコピーし、元のメディアまたはそのコピーを外部の保管場所に移すこともできます。 メディア コピー機能はデバイスの空き状況に応じて、バックアップ後に自動実行することも、スケジュール形式で実行することも可能です。

ただし以下の点に注意してください。

- 最初にすべてのバックアップを実行してからメディアをコピーすることをお勧めします。
- メディアのコピー中は、コピー元のメディアを復元に使用できません。
- メディア全体のコピーのみ可能であり、特定オブジェクトだけをコピーすることはできません。
- コピーが終了したら、元のメディアとそのコピーには追加不可能(Non Appendable)マークが付加されます。このマークが付加されたメディアには新しいバックアップ データを追加できなくなります。
- メディア コピーをスケジュール設定する場合は、設定した時刻に必要なデバイスおよびメディアが使用可能でなければなりません。使用できなければコピー処理は中止されます。

例1: ファイルシステム バックアップの自動メディア コピー

ここで取り上げる企業では2つのセルを持つMoM環境を所有しており、各セル内にはそれぞれ150台のコンピュータ システム(サーバおよびワークステーション)が含まれています。 各システムの平均データ量は10GBであるため、バックアップが必要な総データ量は3000GBになります。

これらのデータについて毎日1回増分1バックアップを実行し、週に1回フル バックアップを実行し、さらに長期保存目的で月に1回フル バックアップを実行するものとします。 このバックアップは、会社の営業時間外に実行しなければなりません。 つまり、午後5時以降にバックアップを開始し、翌日の午前8時までにバックアップを完了させる必要があります。 また、週末にバックアップを実行することもできます。

さらにバックアップ メディアのコピーも作成します。 このコピーは復元時に使用できるように社内に保管しておき、また安全性を考慮して元のバックアップ メディアは外部の保管場所に移送するものとします。 メディアのコピーはバックアップの終了後に実行する必要があります。 この作業には自動メディア コピー機能を使用します。

作業には6台のLTOドライブを搭載したHP StorageWorks 6/60 Tape LibraryおよびLTO Ultrium 1メディアを使用します。 これまでの経験から判断して、データ転送速度は80GB/h、各メディアの平均容量は153GBになると予測されます。

メディア コピーの終了後は、コピー元メディアとコピー先メディアの両方が追加不可能(Non Appendable)になります。 この点を考えると、バックアップに使用するメディアの数は最小限に抑えることが望まれます。 空のメディアを使って作業を開始し、各メディアの最大容量まで使い切るようにしてください。 このためには各バックアップ仕様に1つのデバイスのみを割り当てるようにします。 こうしておくと、現在のメディアが一杯になってはじめて新しいメディアが使用されます。 ただし、複数のメディアに書き込む場合に比べてバックアップ時間は長くなる点に注意してください。

ここでは4つのバックアップ仕様を作成することにします。 メディア スペースを節約するため、使用するメディアの数が最小限で済むような形で、データを複数のバックアップ仕様に分割します。 それぞれのバックアップでは1つのデバイスしか使用されません。

バックアップが終了したら自動メディア コピーが実行されます。 この処理には空いているすべてのデバイスを使用できます。 デバイスがビジー状態になっているときの概要を以下の図に示します。

メディアのコピーには、バックアップとほぼ同じ時間がかかると予想されます。

[増分1]バックアップ

バックアップの構成

増分1バックアップは月曜から木曜までの毎日午後6時に実行するようスケジュール設定します。 データ保護期間は4週間に設定します。 毎日のデータ変更量は全体の30%であるため、バックアップが必要なデータ量は900GBになると予測されます。 このデータを次のように複数のバックアップ仕様に分割します。

- BackupSpec1（ドライブ1）–300 GB
- BackupSpec2（ドライブ2）–300 GB
- BackupSpec3（ドライブ3）–150 GB
- BackupSpec4（ドライブ4）–150 GB

BackupSpec1とBackupSpec2にはそれぞれ2つのメディアが必要で、バックアップには約4時間かかります。 BackupSpec3とBackupSpec4にはそれぞれ1つのメディアが必要で、バックアップには約2時間かかります。

自動メディア コピーの構成

バックアップが終了したら、そのバックアップに対応する自動メディア コピーが開始されます。 コピーが必要なメディアの数は6個で、この処理にはライブラリ内のすべてのドライブを、ドライブが空き次第使用できます。

BackupSpec1およびBackupSpec2で使用するメディアのコピーには、バックアップ後メディア コピー機能を使用できます。これは2つのドライブ(ドライブ5と6)が空いているため、デバイスが使用可能かどうかを考慮する必要がないためです。

BackupSpec1用のバックアップ後メディア コピーを構成します。 コピー元デバイスにはドライブ1を、コピー先デバイスにはドライブ6を指定してください。 データ保護は元のデータと同様に設定し、メディアの位置も指定します(Shelf 1など)。

同様に、BackupSpec2用のバックアップ後メディア コピーを構成します。 コピー元デバイスにはドライブ2を、コピー先デバイスにはドライブ5を指定してください。 データ保護は元のデータと同様に設定し、メディアの位置も指定します。

BackupSpec3とBackupSpec4で使用するメディアのコピーには、スケジュール形式のメディア コピー機能を使用します。 これは、コピー処理にドライブ3とドライブ4を使用するため、両方のバックアップが終了するまで待つ必要があるためです。 メディア コピーがスケジュール設定されている時刻にこれらのデバイスが使用不能であると、処理は失敗する点に注意してください。 そのため、バックアップと同じデバイスを使用してスケジュール形式の自動メディア コピーを実行する場合は、バックアップの終了予定時刻よりも少し後の時間を指定するようにしてください。

ここではバックアップ終了予定時刻の1時間後にメディア コピーが開始されるようにスケジュールを設定します。 メディア コピーの対象にはBackupSpec3とBackupSpec4を選択し、コピー元デバイスにはドライブ3を、コピー先デバイスにはドライブ4を指定します。 データ保護は元のデータと同様に設定し、メディアの位置も指定します。

図 101（323ページ）は、増分1バックアップと自動メディア コピーを図で表したものです。

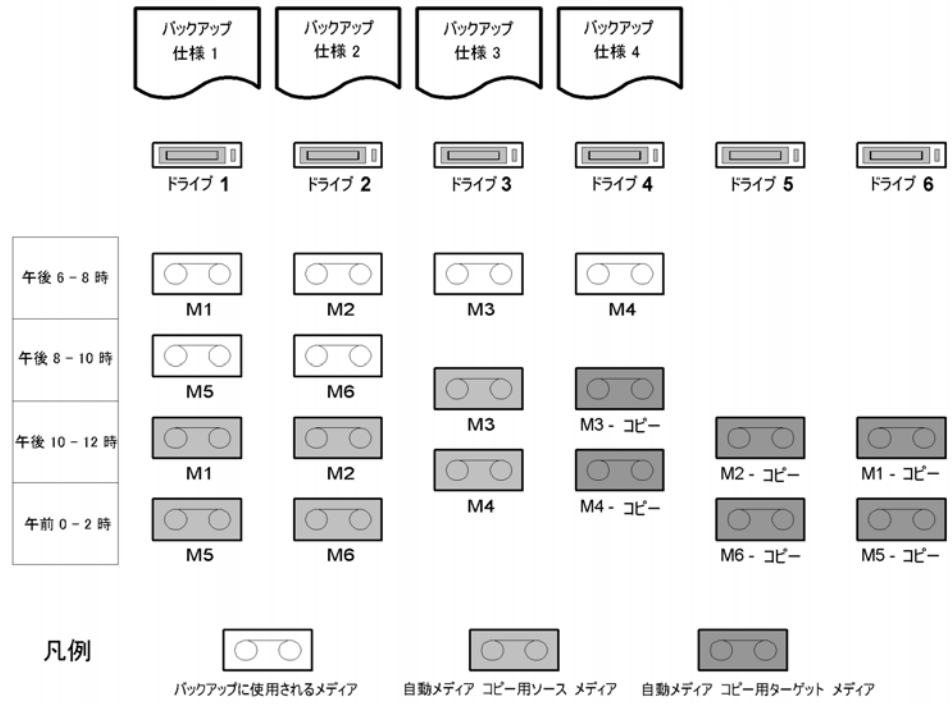

図 101 [増分1]バックアップとメディアの自動コピー

フルバックアップ

バックアップの構成

週1回のフル バックアップは金曜日の午後6時に開始するようスケジュール設定します。 データ保護期間は8週間に設定します。 バックアップするデータの量は3000 GBです。 このデータを次のように複数のバックアップ仕様に分割します。

- BackupSpec1（ドライブ1）–1000 GB
- BackupSpec2（ドライブ2）–1000 GB
- BackupSpec3（ドライブ3）–500 GB
- BackupSpec4（ドライブ4）–500 GB

BackupSpec1とBackupSpec2にはそれぞれ7つのメディアが必要で、BackupSpec3とBackupSpec4にはそれぞれ4つのメディアが必要です。 バックアップには約14時間かかります。

自動メディア コピーの構成

バックアップが終了したら、そのバックアップに対応する自動メディア コピーが開始されます。 コピーが必要なメディアの数は22個で、すべてのデバイスが空き次第使用されます。

ここでも、BackupSpec1とBackupSpec2で使用したメディアのコピーにはバックアップ後メディア コピーを使用し、BackupSpec3とBackupSpec4で使用したメディアのコピーにはスケジュール形式のメディア コピーを使用するよう構成します。

デバイスおよびデータ保護は、増分1バックアップのコピー時と同様に設定します。スケジュール形式のメディア コピーは、バックアップ終了予定時刻の1時間後に開始されます。

図 102（325ページ）は、フル バックアップと自動メディア コピーを図で表したものです。

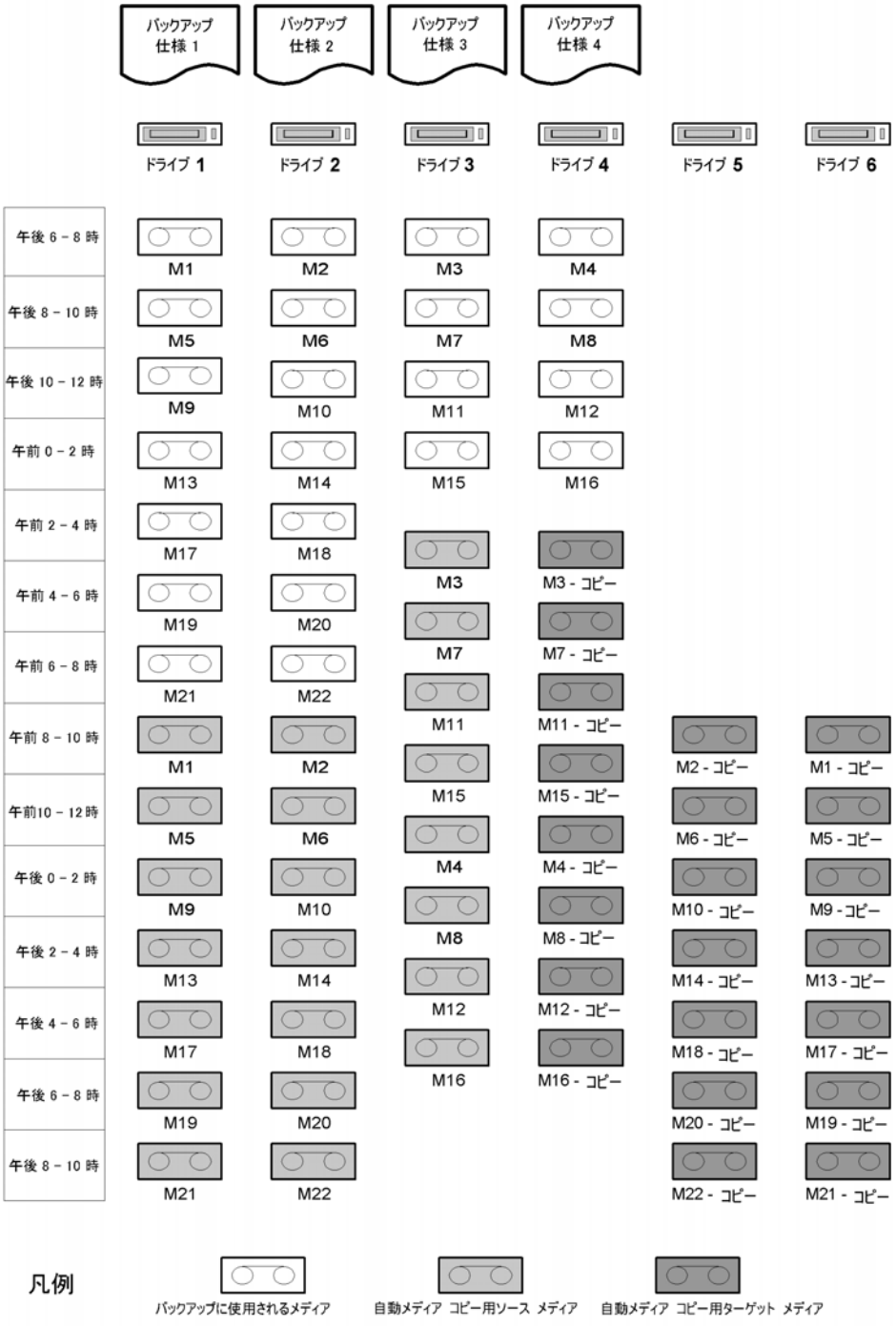

図 102 フルバックアップとメディアの自動コピー

月1回のフル バックアップは日曜日の午前6時に開始するようスケジュール設定します。このバックアップは長期保存が目的であるため、通常コピーは作成しません。

図 103（326ページ）はデバイス使用率が高い時間帯の概要を示したものです。 このグラフは使用率の概要を示したものであり、一部のバックアップ セッションおよびコピー セッションの部分的な重複は無視しています。

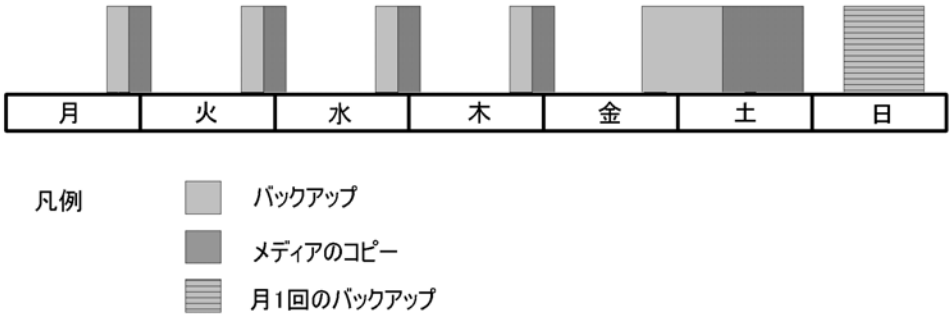

図 103 バックアップセッションとメディアの自動コピーセッションの概要

例2：Oralceデータベース バックアップの自動メディア コピー

ここで取り上げる企業では、500GBのサイズのOracleデータベースを使用しています。このデータベースは、毎日のフル バックアップが必要です。 このバックアップは、会社の営業時間外に実行しなければなりません。 つまり、午後5時以降にバックアップを開始し、翌日の午前8時までにバックアップを完了させる必要があります。 また、週末にバックアップを実行することもできます。

バックアップ メディアのコピーには自動メディア コピー機能を使用し、作成したコピーは復元時に使用できるように社内に保管しておきます。 また安全性を考慮して元のバックアップ メディアは外部の保管場所に移送します。 メディアのコピーは、バックアップ終了後に実行しなければなりません。 この作業にはバックアップ後メディア コピー機能を使用します。

作業には10台のLTOドライブを搭載したHP StorageWorks 10/700 Tape LibraryおよびLTO Ultrium 1メディアを使用します。 これまでの経験から判断して、データ転送速度は80GB/h、各メディアの平均容量は153GBになると予測されます。

メディア コピーが終了したらバックアップに使われたメディアとそのコピーは追加不可能(Non Appendable)になるため、テープ スペースは最大容量まで使い切ることが望まれます。 その一方、バックアップはできるだけ短時間で終了する必要があります。 ここでは4台のデバイスを使用してバックアップを実行します。 空のメディアを使って作業を開始し、各メディアの最大容量まで使い切るようにしてください。

バックアップが終了したら自動メディア コピーが開始されます。 コピーが必要なメディアの数は4個であるため、処理には8台のデバイスが必要です。 つまり、ソースメディアとターゲットメディアのそれぞれにデバイスを4つずつ使用できます。

メディアのコピーには、バックアップとほぼ同じ時間がかかると予想されます。

フルバックアップ

バックアップの構成

毎日のフル バックアップは月曜から金曜までの毎日午後6時に実行するようスケジュール設定します。 データ保護期間は4週間に設定します。 バックアップするデータの量は500 GBです。 ドライブ1、ドライブ2、ドライブ3、ドライブ4の4つのドライブを使用し、4つのメディアにデータをバックアップしています。バックアップの所要時間は約2時間です。

自動メディア コピーの構成

ここでは十分な数のデバイスを使用できるため、バックアップ後メディア コピー機能を使用します。 コピー元デバイスにはドライブ1、2、3、4を、コピー先デバイスにはドライブ5、6、7、8を指定します。 データ保護は元のデータと同様に設定し、メディアの位置も指定します。

図 104 (327ページ) は、データベースのフル バックアップと自動メディア コピーを図で表したものです。

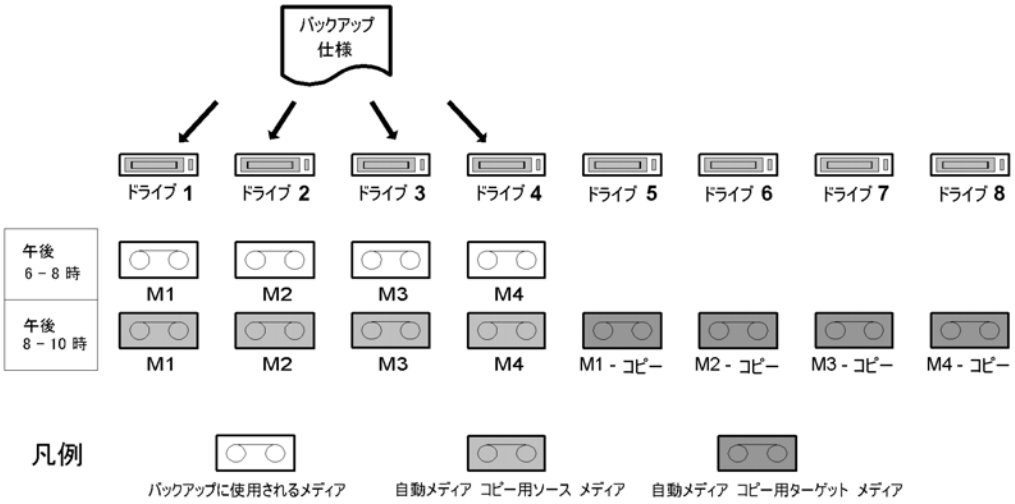

図 104 データベースのフル バックアップと自動メディア コピー

月1回のフル バックアップは土曜日の午後12時に開始するようスケジュール設定します。 このバックアップは長期保存が目的であるため、通常コピーは作成しません。

図 105 (328ページ) はデバイス使用率が高い時間帯の概要を示したものです。

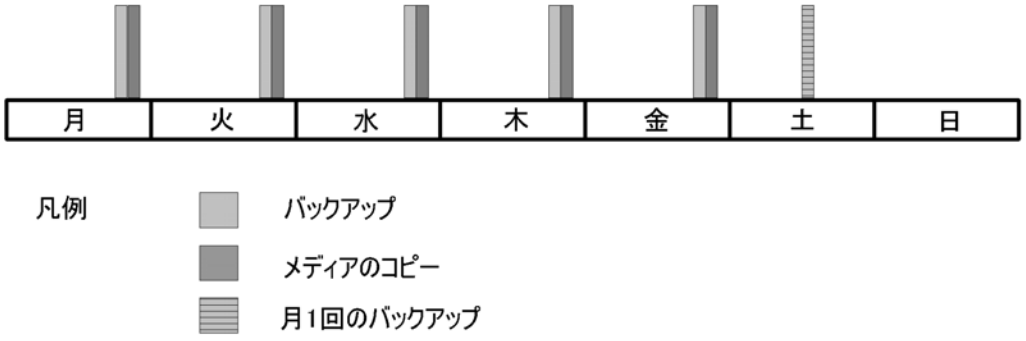

図 105 バックアップセッションとメディアの自動コピーセッションの概要

国際化

国際化とはソフトウェア製品の設計および実装方法で、これにより、製品をユーザーの母国語を使ってユーザーのロケール設定(通貨、時刻、日付、数字、その他の形式)に合わせて動作させることができます。 国際化によって、ユーザーの母国語によるテキスト データの入力、表示が可能になります。 一方、ソフトウェアの開発技法としての国際化とは、単一のソース コードを持つ、単一のバイナリ ソフトウェアをもって、複数の言語環境への個別ローカライズを可能とすることです。 言語ごとのローカライズ作業は、バイナリとは別個のテキスト部分を翻訳することにより行います。 したがって、国際化とは、ローカライズを可能にするプロセスです。Data Protectorは、ユーザー インタフェース用に複数の言語が用意されている国際化された製品です。

ローカライズ

ローカライズとは、製品またはサービスを特定の言語や文化に適応させるプロセスです。 このプロセスは、ローカライズ済みの画面やオンライン ヘルプ、エラー メッセージ、マニュアルなどの提供に関することです。

Data Protectorでは実際のメッセージ文字列を送信する代わりに、文字列IDをエージェントからCell Managerへ送信します。 Cell Managerによってその文字列はGUIに転送され、メッセージが適切な言語形式で表示されます。 ファイル名やディレクトリ名はインデックスにより表示されるわけでないことに注意してください。 ファイル名やディレクトリ名はテキスト文字列として転送され、GUIにテキスト文字列として表示されます。 この方法については「ファイル名の取り扱い」 (329ページ)の項で説明します。

Data Protectorはさまざまな言語にローカライズされています。 ローカライズ対応言語に関する詳細は、『HP Data Protector product announcements ソフトウェアノートおよびリファレンス』を参照いただくか、製品の購入元または最寄りの当社営業所にお問い合わせください。

ファイル名の取り扱い

異機種混在環境(1つのセルに異なるオペレーティング システムがあり、異なるローカル設定が行われている環境)でのファイル名の取り扱いは、大きな課題です。Data Protectorでは、ファイル名が作成されたときにそのシステム上で有効であったさまざまなローカル設定(言語、領域、文字セットなど)に応じてファイル名を処理します。 そのため、あるロケール設定の下でバックアップしたファイルを、別のロケール設定の下で表示または復元するには、ファイル名を正しく表示するための特殊なセットアップが必要になります。

背景

各種のプラットフォームを提供するベンダー各社はサポートする言語セットを独自に選択してきており、キャラクタセット表記や 文字のエンコード規格(ISO 8859-1、Shift-JIS、EUC、Code Page 932、UNICODEなど)の採用も各社ごとに行われています。 これらのエンコード規格は互いに衝突する可能性があります。 例えば2つのエンコード規格で、同じ値がそれぞれ*異なる*文字に割り当てられていたり、異なる値が*同じ*文字に割り当てられていたりするケースが考えられます。 いったん作成されたファイル名について、使用されたコード セットを知る方法はありません。 そのため異なるエンコード規格が使われているシステム間でファイル名を受け渡した場合、ファイル名がGUI上に正しく表示されない可能性があります。

異種プラットフォーム間でデータを受け渡しても、すべてのプラットフォームで同じキャラクタセットが使われているか、すべての国の文字に対応しているUNICODEの実装(Windows上ではUTF-16、その他のプラットフォーム上ではUTF-xx)が使われている場合には、問題は起こりません。

残念ながら、UNIXシステム上ではUNICODEの実装(UTF-xx)はまだ標準ではサポートされていません。 アプリケーションのコンポーネントは、Windows XP Professional、Windows 2000、HP-UX、Solaris、AIXなど、プラットフォームが異なるさまざまなシステム上に配布されている可能性があります。 これらすべてのプラットフォーム上にあるデータをバックアップおよびリストアする必要があります。言語やキャラクタセットに対する業界標準の欠如を、Data Protectorで完全に補うことはできませんが、ユーザーへの影響をできる限り少なくすることは可能です。

例

異機種環境の場合、構成によってはファイル名をGUIに正常に表示できないことがあります。 例えば、Data Protectorでは、Disk Agentを実行しているHP-UX上のファイルをバックアップしてWindows上のData Protector GUIで表示することができますが、このとき、 両方のプラットフォームで同一のコード セットが使用されていなければ、ファイル名を正常に表示できないことがあります。 これは、種類が異なるキャラクタセットでは、ある1つの値がお互いに異なる意味を持っており、別の文字として表示される可能性があるためです。

UNIX上での非互換例

Data Protectorがインストールされていないsolarisシステムの同一ファイルシステム上で、3人のユーザーがそれぞれASCII以外の異なるキャラクタセットを使用してファイルを作成したとします。 これらのユーザーが自分の作成したファイル、および他のユーザーが作成したファイルをlsコマンドで表示した場合、以下のことが起こります。

- 自分の作成したファイル名は正常に表示される。
- 他のユーザーが作成したファイル名は正常に表示されない。 これらのファイル名は、別のシステムではさらに違う形式で表示される場合があります。

正常に表示されなかったファイル名は、lsコマンドを実行するときに使用されたコードセットとは異なるコード セットで作成されています。 また、これらのファイル名には、ファイル作成時に使用されたコード セットを示す「タグ」が付与されていません。 この例のような現象は、固有のファイルシステム ビューア(ターミナル ウィンドウのlsなど)を使用しているシステムで起こります。

バックアップ時のファイル名の取り扱い

Data ProtectorではDisk Agent (バックアップ対象の各クライアント上で実行)を使用してファイル名を読み取り、元のコピーをメディアに保存します。 バックアップのlog filenameオプションが選択されている場合は、ファイル名は「内部」コードセットに変換され、IDBに記録されます。

ファイル名のブラウズ

Data Protectorでは、GUIを使用して、復元するファイルを選択できます。 そのためには、GUIが実行されているシステムで、IDBにファイル名を表示します。Data Protectorでは、GUIにあらゆるファイル名を表示するために、複数のエンコードを用意しています。 ある特定の文字暗号化方式が選択されると、Data Protectorでは、それを使用して、ファイル名の文字が表示されます。

ファイル名を正しく表示するためには、ファイルが作成されたシステム上で設定されていた文字エンコード方式を選択する必要があります。 エンコード方式が異なっていると、Data Protector GUI内にファイル名が正しく表示されません。

バックアップが作成されたプラットフォームと同じプラットフォーム上にファイルを復元すると、正しい名前で復元されます。

各種の構成におけるファイル名のブラウズに関する制約事項については、オンラインヘルプで「国際化」をキーワードに指定して確認してください。

復元時のファイル名の取り扱い

通常、ファイルは、バックアップに使用したプラットフォーム上に復元します。 復元プロセスは、次のようになります。

- GUI上で復元するファイルを選択します。
- 指定したデータがData Protectorによりテープ内で検索されて、データが復元されます。

- 元のファイル名(テープ内に保存されていたオリジナル コピー)が復元されます。

用語集

ACSLS

(StorageTek固有の用語) Automated Cartridge System Library Server の略語。 ACS (Automated Cartridge System: 自動カートリッジ システム) を管理するソフトウェア。

Active Directory

(Windows固有の用語) Windowsネットワークで使用されるディレクトリ サービス。ネットワーク上のリソースに関する情報を格納し、ユーザーやアプリケーションからアクセスできるように維持します。このディレクトリ サービスでは、サービスが実際に稼動している物理システムの違いに関係なく、リソースに対する名前や説明の付加、検索、アクセス、および管理を一貫した方法で実行できます。

AES 256ビット暗号化

Data Protectorソフトウェアの暗号化方式で、256ビット長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にしています。暗号化にも復号化にも同じキーを使用します。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、AES 256ビット暗号化方式によって暗号化されます。

AML

*(EMASS/GRAU固有の用語)*Automated Mixed-Media library (自動混合メディア ライブラリ) の略。

ASRセット

フロッピー ディスク上に保存されたファイルのコレクション。交換用ディスクの適切な再構成(ディスク パーティション化と論理ボリュームの構成)およびフル クライアント バックアップでバックアップされた元のシステム構成とユーザー データの自動復旧に必要となります。これらのファイルは、バックアップ メディア上に保存されると共に、Cell Manager上の*Data_Protector_home*\Config\Server\dr\asr ディレクトリ (Windows用Cell Managerの場合) または /etc/opt/omni/server/dr/asr/ディレクトリ (UNIX用Cell Managerの場合) に保存されます。ASRアーカイブ ファイルは、障害発生後に複数のフロッピー ディスクに展開されます。32ビット版のWindows XP/.NETでは3枚のフロッピー ディスクに展開され、64ビット版のWindows XP/.NETの場合は4枚のフロッピー ディスクに展開されます。これらのフロッピー ディスクは、ASRの実行時に必要となります。

Automatic Storage Management

(Oracle固有の用語) 自動ストレージ管理は、Oracle 10g/11gによって統合された、Oracleデータベース ファイルを管理するファイルシステムおよびボリュームのマネージャ機能です。データとディスクの管理の複雑さを解消するとともに、ストライプ化とミラー化によってパフォーマンスの最適化も行います。

BACKINT

*(SAP R/3固有の用語)*SAP R/3 バックアップ プログラムが、オープン インタフェースへの呼び出しを通じてData Protector backintインタフェース ソフトウェアを呼び出し、Data Protectorソフトウェアと通信できるようにします。バックアップ時および復元時には、SAP R/3 プログラムがData Protector backintインタフェースを通じてコマンドを発行します。

BC

(EMC Symmetrix固有の用語) Business Continuanceの略。BCは、EMC Symmetrix標準デバイスのインスタント コピーに対するアクセスおよび管理を可能にするプロセスです。
「BCV 。」を参照。

BC

(HP StorageWorks Disk Array XP固有の用語) Business Copy XPの略。 BCを使うと、HP StorageWorks Disk Array XP LDEVの内部コピーをデータ バックアップやデータ複製などの目的で維持できます。これらのコピー（セカンダリ ボリュームまたはS-VOL）は、プライマリ ボリューム（P-VOL）から分離して、バックアップや開発などの用途に応じた別のシステムに接続することができます。バックアップ目的の場合、P-VOLをアプリケーション システムに接続し、S-VOLミラー セットのいずれかをバックアップ システムに接続する必要があります。
「HP StorageWorks Disk Array XP LDEV 、CA 、Main Control Unit 、アプリケーション システム 、およびバックアップ システム 。」を参照。

BC EVA

(HP StorageWorks EVA固有の用語) Business Copy EVAは、ローカル複製ソフトウェア ソリューションです。EVAファームウェアのスナップショット機能とクローン機能を使用して、ソース ボリュームのポイントインタイム 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CA+BC EVA 。」を参照。

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 。」を参照。

BC VA

(HP StorageWorks Virtual Array固有の用語) Business Copy VAを使用すると、同じ仮想アレイ内で、データ バックアップ用またはデータ複製用のHP StorageWorks Virtual Array LUNの内部コピーを管理することができます。コピー(子またはBusiness Copy LUN)は、バックアップやデータ解析、開発など様々な目的に使用できます。バックアップ目的で使用されるときは、元(親)のLUNはアプリケーション システムに接続され、Business Copy(子) LUNはバックアップ システムに接続されます。
「HP StorageWorks Virtual Array LUN 、アプリケーション システム 、およびバックアップ システム 」を参照。

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 」を参照。

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 ファイルをアーカイブできます。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 。」を参照。

BRBACKUP

(SAP R/3固有の用語) SAP R/3 バックアップ ツールの1つ。制御ファイル、個々のデータ ファイル、またはすべてのテーブルスペースをオンラインでもオフラインでもバックアップできます。 また、必要に応じて、オンラインREDOログ ファイルをバックアップすることもできます。
「BRARCHIVE 、および BRRESTORE 。」を参照。

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 。」を参照。

BSM

Data Protector Backup Session Managerの略。バックアップ セッションを制御します。このプロセスは、常にCell Manager システム上で稼動します。

CA

(HP StorageWorks Disk Array XP固有の用語) Continuous Access XPの略。CAでは、データ複製、バックアップ、およびディザスタ リカバリなどの目的でHP StorageWorks Disk Array XP LDEVのリモート コピーを作成および維持できます。CAを使用するには、メイン(プライマリ)ディスク アレイとリモート(セカンダリ)ディスク アレイが必要です。オリジナルのデータを格納し、アプリケーション システムに接続されているCAプライマリ ボリューム(P-VOL)がメイン ディスク アレイに格納されます。リモート ディスク アレイには、バックアップ システムに接続されているCAセカンダリ ボリューム(S-VOL)が格納されます。
「BC *(HP StorageWorks Disk Array XP固有の用語)*、Main Control Unit 、およびHP StorageWorks Disk Array XP LDEV 。」を参照。

CA+BC EVA

(HP StorageWorks EVA固有の用語) Continuous Access (CA) EVAとBusiness Copy (BC) EVAを併用すると、リモートEVA上にソース ボリュームのコピー(複製)を作成して保持でき、その後、これらのコピーをそのリモート アレイ上でローカル複製のソースとして使用できます。
「BC EVA 、複製 、およびソース ボリューム 」を参照。

CAP

(StorageTek固有の用語) Cartridge Access Portの略。ライブラリのドア パネルに組み込まれたポートです。メディアの出し入れに使用されます。

CDB カタログ データベース (Catalog Database) の略。

カタログ データベース (Catalog Database) の略。CDBは、IDBのうち、バックアップ、オブジェクト コピー、復元、メディア管理セッションおよびバックアップしたデータに関する情報を格納する部分。選択したロギング レベルによっては、ファイル名とファイル バージョンも格納されます。CDBは、常にセルに対してローカルとなります。
「MMDB 」を参照。

CDFファイル

(UNIX固有の用語) Context Dependent File（コンテキスト依存ファイル）の略。CDFファイルは、同じパス名でグループ化された複数のファイルからなるファイルです。通常、プロセスのコンテキストに基づいて、これらのファイルのいずれかがシステムによって選択されます。このメカニズムにより、クラスタ内のすべてホストから同じパス名を使って、マシンに依存する実行可能ファイル、システム データ、およびデバイス ファイルを正しく動作させることができます。

Cell Manager

セル内のメイン システム。Data Protectorの運用に不可欠なソフトウェアがインストールされ、すべてのバックアップおよび復元作業がここから管理されます。管理タスク用のGUIは、異なるシステムにインストールできます。各セルにはCell Managerシステムが1つあります。

Change Journal

(Windows固有の用語) 各変更のレコードがローカルNTFSボリューム上のファイルおよびディレクトリに発生するたびに、それが記録されるWindowsのファイル システムの機能。

Change Log Provider

(Windows固有の用語) 作成、変更、または削除されたファイル システム上のオブジェクトを特定するために問い合わせることができるモジュール。

Cluster Continuous Replication

(Microsoft Exchange Server固有の用語) Cluster continuous replication (CCR)は、クラスタ管理およびフェイルオーバーの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）を作成および管理する、高可用ソリューションです。ストレージ グループは、別のサーバに複製されます。CCRでは、使用しているExchangeバックエンド サーバの単一障害ポイントが削除されます。CCRコピーの配置により、アクティブ ノード上の負荷が低減しているExchange Serverのパッシブ ノード上では、VSSを使用してバックアップを実行することができます。
数秒でCCRコピーに切り替えることができるため、CCRコピーはディザスタ リカバリに使用されます。複製ストレージ グループは、Exchange Replication Serviceと呼ばれるExchangeライタの新しいインスタンスとして表され、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。
「Exchange Replication Service およびLocal Continuous Replication 。」を参照。

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MoM Manager上に置く必要があります。MoMセルとその他のData Protectorセルの間には、できるだけ信頼性の高いネットワーク接続を用意してください。
「MoM 。」を参照。

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

「CMMDB 」を参照。

COM+登録データベース

*(Windows固有の用語)*COM+登録データベースとWindowsレジストリには、COM+アプリケーションの属性、クラスの属性、およびコンピュータ レベルの属性が格納されます。これにより、これらの属性間の整合性を確保でき、これらの属性を共通の方法で操作できます。

Command View (CV) EVA

(HP StorageWorks EVA固有の用語) HP StorageWorks EVA ストレージ システムを構成、管理、モニターするためのユーザー インタフェース。さまざまなストレージ管理作業を行うために使用されます。たとえば、仮想ディスクファミリの作成、ストレージ システム ハードウェアの管理、仮想ディスクのスナップクローンやスナップショットの作成などに使用されます。Command View EVA ソフトウェアは HP Storage マネジメント アプライアンス上で動作し、Web ブラウザからアクセスできます。
「HP StorageWorks EVA SMI-S Agent およびHP StorageWorks SMI-S EVAプロバイダ 。」を参照。

CRS

Data Protector Cell Manager上で実行される、Cell Request Serverのプロセス(サービス)。バックアップ セッションと復元セッションの開始および制御を行います。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。Windowsシステムでは、CRSは、インストール時に指定したユーザー アカウントで実行されます。UNIXシステムでは、rootアカウントで実行されます。

CSM

Data Protectorコピーおよび集約セッション マネージャ(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。

Data Replication (DR)グループ

(HP StorageWorks EVA固有の用語) EVA仮想ディスクの論理グループ。共通の性質を持ち、同じCA 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 」を参照。

Data_Protector_home

Data_Protector_home Windows Vista および Windows Server 2008 では、Data Protector のプログラム ファイルを含むディレクトリ。その他の Windows オペレーティング システムでは、Data Protector のData Protectorおよびデータ ファイルを含むディレクトリ。デフォルトのパス

は *%ProgramFiles%*\OmniBack ですが、インストール時に Data Protector セットアップ ウィザードでパスを変更できます。
「Data_Protector_program_data .」を参照。

Data_Protector_program_data

Data_Protector_program_data Windows Vista および Windows Server 2008 では、Data Protector のデータ ファイルを含むディレクトリ。デフォルトのパスは *%ProgramData%*\OmniBack ですが、インストール時に Data Protector セットアップ ウィザードでパスを変更できます。
「Data_Protector_home .」を参照。

Dbobject

(Informix Server固有の用語) Informix Serverの物理データベース 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

DCBF (Detail Catalog Binary Files: 詳細カタログ バイナリ ファイル) ディレクトリは、IDBの一部です。IDBの約80%を占有します。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) が含まれています。DCBFファイルの中には、ファイル バージョンについての情報が保管されています。これは、IDBのDCBF部分を表し、IDB全体の約80%の容量を占めます。デフォルトの DC ディレクトリは、dcbf ディレクトリと呼ばれ、Cell Manager の以下のディレクトリに配置されています。*Data_Protector_program_data*\db40 (Windows Server 2008 の場合)、*Data_Protector_home*\db40 (その他の Windows システムの場合)、または /var/opt/omni/server/db40 (UNIX システムの場合)。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10個までです。DCディレクトリのデフォルト最大サイズは16 GBです。

DHCPサーバ

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。

Disk Agentの同時処理数

1つのMedia Agentに対して同時にデータを送信できるDisk Agentの数。

DMZ

DMZ (Demilitarized Zone)は、企業のプライベート ネットワーク(イントラネット)と外部のパブリック ネットワーク(インターネット)の間に「中立地帯」として挿入されたネットワークです。DMZにより、外部のユーザーが企業のイントラネット内のサーバに直接アクセスすることを防ぐことができます。

DNSサーバ

DNSクライアント サーバ モデルでは、DNSサーバにインターネット全体で名前解決を行うのに必要なDNSデータベースに含まれている情報の一部を保持します。DNSサーバは、このデータベースを使用して名前解決を要求するクライアントに対してコンピュータ名を提供します。

DR OS

ディザスタ リカバリ オペレーティング システムとは、ディザスタ リカバリを実行するためのオペレーティング システム環境です。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 ProtectorData Protectorディザスタ リカバリを実行する前に、DR OSをインストールおよび構成しておく必要があります。DR OSは、Data Protector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。

EMC Symmetrix Agent (SYMA) ***(EMC Symmetrix固有の用語)***

「Symmetrix Agent (SYMA) 。」を参照。

Event Log (Data Protector Event Log)

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___BC_BRIEF_PRODUCT_NAME___イベント ログに送信されます。このイベント ログにアクセスできるData Protectorユーザーは、Adminユーザー グループに所属しているか、または「レポートと通知」のユーザー権限が付与されているData Protectorユーザーのみです。イベント ログ内のイベントは、すべてブラウズしたり削除することができます。

Exchange Replication Service

(Microsoft Exchange Server固有の用語) Local Continuous Replication (LCR) テクノロジまたはCluster Continuous Replication (CCR) テクノロジ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サービス。「Cluster Continuous Replication およびLocal Continuous Replication 。」を参照。

FCブリッジ

「Fibre Channelブリッジ 。」を参照。

Fibre Channelブリッジ

Fibre Channelブリッジ(マルチプレクサ)は、RAIDアレイ、ソリッド ステート ディスク(SSD)、テープ ライブラリなどの既存のパラレルSCSIデバイスをFibre Channel環境に移行できるようにします。ブリッジ(マルチプレクサ)の片側にはFibre Channelインタフェースがあり、その反対側にはパラレルSCSIポートがあります。このブリッジ(マルチプレクサ)を通じて、SCSIパケットをFibre ChannelとパラレルSCSIデバイスの間で移動することができます。

fnames.dat

IDBのfnames.dat ファイルには、バックアップしたファイルの名前に関する情報が格納されます。一般に、ファイル名が保存されている場合、それらのファイルはIDBの20%を占めます。

GUI

Data Protectorには、グラフィカル ユーザー インタフェース (GUI) が用意されており、すべての構成タスク、管理タスク、および処理タスクに容易にアクセスできます。Windows 上で実行される Data Protector の GUI には、Data Protectorオリジナル以外にも、操作感の変わらない Java ベースの GUI があり、多数のプラットフォームで実行されます。

hard recovery

(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。

Holidaysファイル

休日に関する情報を格納するファイル。Cell Manager の以下のディレクトリにあるこのファイルを編集して、休日の設定を変更できます。*Data_Protector_program_data*\Config\Server\holidays (Windows Server 2008 の場合)、 *Data_Protector_home*\Config\Server\holidays (その他の Windows システムの場合)、または /etc/opt/omni/server/Holidays (UNIX システムの場合)。

HP ITO

「OM 。」を参照。

HP OM

「OM。」を参照。

HP OpC

「OM 。」を参照。

HP Operation Manager SMART Plug-In (SPI)

ドメイン管理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ソフトウェアに追加するだけですぐに使えます。 Through theHP OpenView SMART Plug-Inとして実装されるData Protector用統合ソフトウェアを使用して、ユーザーはHP Operations Managerソフトウェア (OM) 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 StorageWorks Disk Array XP LDEV

HP StorageWorks Disk Array XPの物理ディスクの論理パーティション。LDEVは、Continuous Access XP (CA)構成およびBusiness Copy XP (BC)構成で複製することができるエンティティで、スタンドアロンのエンティティとしても使用できます。「BC 、CA *(HP StorageWorks Disk Array XP固有の用語)*、および複製 。」を参照。

HP StorageWorks EVA SMI-S Agent

Data Protectorのソフトウェア モジュール。HP StorageWorks Enterprise Virtual Array用統合ソフトウェアに必要なタスクをすべて実行します。EVA SMI-S Agentを使用すると、受信した要求とCV EVA間のやり取りを制御するHP StorageWorks SMI-S EVA プロバイダを通じてアレイを制御できます。「Command View (CV) EVA およびHP StorageWorks SMI-S EVAプロバイダ 。」を参照。

HP StorageWorks SMI-S EVAプロバイダ

HP StorageWorks Enterprise Virtual Arrayを制御するために使用されるインタフェース。SMI-S EVAプロバイダはHP OpenView ストレージ マネジメント アプライアンス システム上で個別のサービスとして動作し、受信した要求とCommand View EVA間のゲートウェイとして機能します。Data Protector HP StorageWorks EVA用統合ソフトウェアでは、SMI-S EVAプロバイダはEVA SMI-S Agentから標準化された要求を受け入れ、Command View EVAとやり取りして情報または方法を呼び出し、標準化された応答を返します。「HP StorageWorks EVA SMI-S Agent およびCommand View (CV) EVA 。」を参照。

HP StorageWorks Virtual Array LUN

HP StorageWorks Virtual Array内の物理ディスクの論理パーティション。LUNはHP StorageWorks Business Copy VA 構成で複製することができるエンティティで、スタンドアロンのエンティティとしても使用できます。「BC VA および複製 。」を参照。

HP VPO

「OM 。」を参照。

IAPへのバックアップ

HP Integrated Archiving Platform (IAP) アプライアンスへのData Protectorベースのバックアップ。各データ チャンク固有のコンテンツ アドレスを作成することによって、IAPの機能の利点を生かし、ブロック (またはチャンク) レベルで保存された

データの冗長性が低減されます。変更されたチャンクのみ、ネットワーク経由で転送され、保存場所に追加されます。

ICDA

(EMC Symmetrix固有の用語) MC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チャネル、内部キャッシュ メモリ、および通常マイクロコードと呼ばれる制御/診断ソフトウェアを備えたディスク アレイ デバイスです。

IDB

Data Protector内部データベースは、Cell Manager上に維持される埋込み型データベースです。どのデータがどのメディアにバックアップされるか、バックアップ セッションと復元セッションがどのように実行されるか、さらに、どのデバイス上やライブラリ上に構成されているかについての情報が格納されます。

IDB回復ファイル

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) 。この情報を使うと、IDBの復旧を大幅に効率化できます。ファイルをIDBトランザクション ログとともに、ほかのIDBディレクトリから別の物理ディスク上に移し、さらに、そのファイルのコピーを作成します。

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。

IP アドレス

IP(インターネット プロトコル)アドレスは、ネットワーク上のシステムを一意に識別するアドレスで、数字で表されます。IPアドレスは、ピリオド(ドット)で区切られた4組の数字からなります。

ISQL

(Sybase固有の用語) Sybaseのユーティリティの1つ。Sybase SQL Serverに対してシステム管理作業を実行できます。

ITO

「OM 。」を参照。

Java GUI クライアント

Java GUI コンポーネントの1つ。ユーザー インタフェース関連の機能のみを含みます。動作するためは、Java GUI サーバに接続する必要があります。

Java GUI サーバ
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 クライアントからの要求を受け取ると、それを処理し、要求があったクライアントに応答を返します。通信は、HTTPプロトコル（ポート 5556）により行います。

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は、インストール サーバにインストールして構成する必要があります。

KMS
KMS キー マネジメント サービス (KMS) は、Cell Manager 上で稼動してData Protectorの暗号化機能のためのキー マネジメントを行う集中化されたサービスです。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。

LBO
(EMC Symmetrix固有の用語) Logical Backup Object（論理バックアップ オブジェクト）の略。LBOは、EMC Symmetrix/Fastrax環境内で保存/取得されるデータ オブジェクトです。LBOはEMC Symmetrixによって1つのエンティティとして保存/取得され、部分的には復元できません。

LISTENER.ORA
*(Oracle固有の用語)*Oracleの構成ファイルの1つ。サーバ上の1つまたは複数のTNS リスナを定義します。

Local Continuous Replication
(Microsoft Exchange Server固有の用語) Local continuous replication (LCR) は、ストレージ グループの精密なコピー (LCRコピー) を作成および管理する単一サーバ ソリューションです。LCRコピーは、オリジナル ストレージ グループと同じサーバ上にあります。LCRコピーが作成される際、変更伝播（ログ リレー）テクノロジを介して最新の状態に保たれます。LCRの複製機能では、複製されていないログは削除されないことが保証されます。この動作は、ログのコピーよりかなり後に複製を行う場合、ログを削除するモードでバックアップを実行しても、実際には領域を解放しない可能性があることを意味します。
数秒でLCRコピーに切り替えることができるため、LCRコピーはディザスタ リカバリに使用されます。LCRコピーがバックアップに使用され、オリジナル データとは異なるディスク上にある場合、本稼働データベースへのI/O負荷は最小限に抑制されます。
複製ストレージ グループは、Exchange Replication Service と呼ばれるExchangeライタの新しいインスタンスとして表され、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。
「Cluster Continuous Replication およびExchange Replication Service 。」を参照。

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)は、HP-UXシステム上で物理ディスク スペースを構造化し、論理ボリュームにマッピングするためのサブシステムです。LVMシステムは、複数のボリューム グループで構成されます。各ボリューム グループには、複数のボリュームが含まれます。

Main Control Unit (MCU)

(HP StorageWorks Disk Array XP固有の用語) CA構成およびBC構成用のプライマリ ボリュームを含み、マスター デバイスとしての役割を果たすHP StorageWorks XPディスク アレイ。「 BC (HP StorageWorks Disk Array XP固有の用語)、CA *(HP StorageWorks Disk Array XP固有の用語)*、およびHP StorageWorks Disk Array XP LDEV 。」を参照。

make_net_recovery

make_net_recoveryは Ignite-UX のコマンドで、Ignite-UX サーバまたは他の指定システム上に、ネットワークを経由して復旧アーカイブを作成するツールです。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 のコマンドで、ブート可能な復旧（インストール）テープを作成するツールです。この復旧テープはご利用のシステムにカスタマイズされており、バックアップ デバイスをターゲット システムに直接接続して、ターゲット システムをこのブート可能な復旧テープからブートすることで、無人のディザスタ リカバリが可能となります。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	**「Main Control Unit (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。バックアップ セッション中、Media AgentはDisk Agentからデータを受信し、デバイスに送信します。データを受信したデバイスはメディアに書き込みます。Media Agentは、ライブラリのロボティクス制御も管理します。
Microsoft Exchange Server	多様な通信システムへの透過的接続を提供するクライアント/サーバ型のメッセージング/ワークグループ システム。電子メール システムの他、個人とグループのスケジュール、オンライン フォーム、ワークフロー自動化ツールなどをユーザーに提供します。また、開発者に対しては、情報共有およびメッセージング サービス用のカスタム アプリケーション開発プラットフォームを提供します。
Microsoft SQL Server	分散型クライアント サーバ コンピューティングのニーズを満たすように設計されたデータベース管理システム。
Microsoft Volume Shadow Copy Service (VSS)	VSS対応アプリケーションのバックアップと復元をそのアプリケーションの機能に関係なく統合管理する統一通信インタフェースを提供するソフトウェア サービスです。このサービスは、バックアップ アプリケーション、ライター、シャドウ コピー プロバイダ、およびオペレーティング システム カーネルと連携して、ボリューム シャドウ コピーおよびシャドウ コピー セットの管理を実現します。 「シャドウ コピー 、シャドウ コピー プロバイダ 、複製 、およびライタ 。」を参照。
Microsoft管理コンソール (MMC)	*(Windows固有の用語)* Windows環境における管理モデル。シンプルで一貫した統合型管理ユーザー インタフェースを提供します。同じGUIを通じて、さまざまなMMC対応アプリケーションを管理できます。
MMD	Media Management Daemon (メディア管理デーモン)の略。MMDプロセス (サービス) は、Data Protector Cell Manager上で稼動し、メディア管理操作およびデバイス操作を制御します。このプロセスは、Data ProtectorをCell Managerにインストールしたときに開始されます。

MMDB

Media Management Database（メディア管理データベース）の略。MMDBは、IDBの一部です。セル内で構成されているメディア、メディア プール、デバイス、ライブラリ、ライブラリ デバイス、スロットに関する情報と、バックアップに使用されているData Protectorメディアに関する情報を格納します。エンタープライズ バックアップ環境では、データベースをすべてのセル間で共有できます。
「CMMDB 、CDB 。」を参照。

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 Media Session Manager（メディア セッション マネージャ）の略。MSMは、Cell Manager上で稼動し、メディア セッション（メディアのコピーなど）を制御します。

MU番号

(HP StorageWorks Disk Array XP固有の用語) ミラー ユニット番号。ファーストレベルミラーを示すために使う整数(0、1または2)です。
「ファースト レベル ミラー 。」を参照。

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。

OM

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、UNIX用HP Operations Managerソフトウェアの略称。Data Protectorには、この管理製品用の統合ソフトウェアが用意されています。この統合ソフトウェアは、HP-UX、Solaris、およびLinux上のOM管理サーバ用のSMART Plug-Inとして実装されています。以前のバージョンのOMは、IT/Operation、Operations Center、および Vantage Point Operationsと呼ばれていました。
「マージ 。」を参照。

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。

OpC

「OM 。」を参照。

OpenSSH

さまざまな認証方式と暗号化方式を採用することにより、リモート マシンへの安全なアクセスを提供するネットワーク接続ツールのセット。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、Installation Serverとクライアントにこれをインストールして構成する必要があります。

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) ログイン情報の書式は、*user_name*/*password*@*service*です。

- *user_name*は、Oracle Serverおよびその他のユーザーに対して公開されるユーザー名です。各ユーザーがOracleターゲット データベースに接続するには、ユーザー名とパスワードの両方を入力しなければなりません。ここでは、

OracleのSYSDBA権限またはSYSOPER権限が付与されているユーザーを指定する必要があります。

- *password*は、Oracle パスワード ファイル（orapwd）に指定されているパスワードに一致する必要があります。これは、データベース管理を行うユーザーの認証に使用されるファイルです。
- *service*は、ターゲット データベースのSQL*Net サーバ プロセスを識別する名前です。

P1Sファイル

P1Sファイルには、システムにインストールされているすべてのディスクを高度な自動ディザスタ 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recovery.p1sというファイル名で保存されます。保存場所は、*Data_Protector_home*\Config\Server\dr\p1sディレクトリ（Windows用Cell Managerの場合）または/etc/opt/omni/server/dr/p1sディレクトリ（UNIX用Cell Managerの場合）です。 .

RAID

Redundant Array of Inexpensive Disksの略。

RAID Manager XP

(HP StorageWorks Disk Array XP固有の用語) RAID Manager XPアプリケーションでは、CAおよびBC アプリケーションのステータスをレポートおよび制御する多数のコマンド リストが提供されます。これらのコマンドは、RAID Managerインスタンスを通じて、StorageWorks Disk Array XP Disk Control Unitと通信します。このインスタンスは、コマンドを一連の低レベルSCSIコマンドに変換します。

RAID Manager ライブラリ

(HP StorageWorks Disk Array XP固有の用語) Solarisシステム上のData Protectorでは、RAID Manager ライブラリを内部的に使用して、HP StorageWorks Disk Array XPの構成データ、ステータス データ、およびパフォーマンス データにアクセスします。さらに、一連の低レベル SCSI コマンドに変換される関数呼び出しを通じて、HP StorageWorks Disk Array XPの主要な機能にアクセスします。

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。

RDBMS

Relational Database Management System（リレーショナル データベース管理システム）の略。

RDF1/RDF2

*(EMC Symmetrix固有の用語)*SRDF デバイス グループの一種。RDF グループには RDF デバイスだけを割り当てることができます。RDF1 グループ タイプにはソース デバイス（R1）

が格納され、RDF2 グループ タイプにはターゲット デバイス（R2）が格納されます。

RDS

Raima Database Serverの略。RDS（サービス）は、Data ProtectorのCell Manager上で稼動し、IDBを管理します。このプロセスは、Data ProtectorをCell Managerにインストールしたときに開始されます。

Recovery Manager（RMAN）

*(Oracle固有の用語)*Oracleコマンド行インタフェース。これにより、Oracle Serverプロセスに接続されているデータベースをバックアップ、復元、および復旧するための指示がOracle Serverプロセスに出されます。RMANでは、バックアップについての情報を格納するために、リカバリ カタログまたは制御ファイルのいずれかが使用されます。この情報は、後の復元セッションで使うことができます。

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 リカバリ実行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。

Remote Control Unit（RCU）

(HP StorageWorks Disk Array XP固有の用語) Remote Control Unit（RCU）は、CA構成の中でMCU（Main Contol Unit）のスレーブとしての役割を果たします。双方向の構成の中では、RCUはMCUとしての役割を果たします。

RMAN *(Oracle固有の用語)*

「Recovery Manager 。」を参照。

RSM

Data Protector Restore Session Managerの略。復元セッションを制御します。このプロセスは、常にCell Managerシステム上で稼動します。

RSM

*(Windows固有の用語)*Removable Storage Managerの略。RSMは、アプリケーション、ロボティクス チェンジャ、およびメディア ライブラリの間の通信を効率化するメディア管理サービスを提供します。これにより、複数のアプリケーションがローカル ロボティクス メディア ライブラリとテープまたはディスクドライブを共有でき、リムーバブル メディアを管理できます。

SIBF

サーバレス統合バイナリ ファイル (SIBF) は、IDBのうち、NDMPのrawメタデータが格納される部分です。これらのデータは、NDMP オブジェクトの復元に必要です。

SMB

「スプリット ミラー バックアップ 。」を参照。

SMBF

セッション メッセージ バイナリ ファイル(SMBF)は、IDBのうち、バックアップ、復元、オブジェクト コピー、オブジェクト集約、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。セッションごとに1つのバイナリファイルが作成されます。バイナリ ファイルは、年と月に基づいて分類されます。

sqlhostsファイル

(Informix 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保存されています。

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SLDのリアルタイム 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

SRD (System Recovery Data：システム復旧データ) ファイルには、障害発生時にオペレーティング システムをインストールおよび構成するために必要なシステム情報が含まれています。SRDファイルはASCIIファイルで、CONFIGURATIONバックアップがWindowsクライアント上で実行されCell Managerに保存される時に生成されます。

SSE Agent

(HP StorageWorks Disk Array XP固有の用語) スプリット ミラー バックアップの統合に必要なタスクをすべて実行するData Protectorソフトウェア モジュール。RAID Manager XP ユーティリティ (HP-UXシステムおよびWindowsシステムの場合) またはRAID Manager ライブラリ (Solarisシステムの場合) を使い、HP StorageWorks Disk Array XPの保管システムと通信します。

sst.confファイル

/usr/kernel/drv/sst.confファイルは、マルチドライブ ライブラリ デバイスが接続されているData Protector Sun Solarisクライアントのそれぞれにインストールされていなければならないファイルです。このファイルには、クライアントに接続されている各ライブラリ デバイスのロボット機構のSCSIアドレス エントリが記述されてなければなりません。

st.confファイル

/kernel/drv/st.conf ファイルは、バックアップ デバイスが接続されているData Protector Solarisクライアントのそれぞれに

インストールされていなければならないファイルです。このファイルには、クライアントに接続されている各バックアップ ドライブのデバイス情報とSCSIアドレスが記述されていなければなりません。シングルドライブ デバイスについては単一のSCSIエントリが必要で、マルチドライブ ライブラリ デバイスについては複数のSCSIエントリが必要です。

StorageTek ACS ライブラリ *(StorageTek固有の用語)* ACS (Automated Cartridge System) は、1つのライブラリ管理ユニット (LMU) と、このユニットに接続された1 ~ 24個のライブラリ記憶域モジュール (LSM) からなるライブラリ システム (サイロ) です。

Sybase Backup Server API *(Sybase固有の用語)*Sybase SQL ServerとData Protectorなどのバックアップ ソリューションの間でのバックアップ情報および復旧情報交換用に開発された業界標準インタフェース。

Sybase SQL Server *(Sybase固有の用語)* Sybaseの「クライアント サーバ」アーキテクチャ内のサーバ。Sybase SQL Serverは、複数のデータベースと複数のユーザーを管理し、ディスク上のデータの実位置を追跡します。さらに、物理データ ストレージ域に対する論理データ記述のマッピングを維持し、メモリ内のデータ キャッシュとプロシージャ キャッシュを維持します。

Symmetrix Agent (SYMA) *(EMC Symmetrix固有の用語)*EMC Symmetrix 環境でのバックアップ操作と復元操作を可能にするData Protectorソフトウェア モジュール。

System Backup to Tape *(Oracle固有の用語)*Oracleがバックアップ要求または復元要求を発行したときに正しいバックアップ デバイスをロード、ラベリング、およびアンロードするために必要なアクションを処理するOracle インタフェース。

SysVol *(Windows固有の用語)* ドメインのパブリック ファイルのサーバ コピーを保存する共有ディレクトリで、ドメイン内のすべてのドメイン コントローラ間で複製されます。

TimeFinder *(EMC Symmetrix固有の用語)*単一または複数のEMC Symmetrix 論理デバイス (SLD) のインスタント コピーを作成するBusiness Continuationプロセス。インスタント コピーは、BCVと呼ばれる専用の事前構成SLD上に作成され、システムに対する別個のプロセスを経由してアクセスできます。

TLU Tape Library Unit (テープ ライブラリ ユニット) の略。

TNSNAMES.ORA *(OracleおよびSAP R/3固有の用語)* サービス名にマッピングされた接続記述子が保存されているネットワーク構成ファイル。このファイルは、1か所で集中的に管理してすべてのクライアントで使用することも、また、ローカルに管理して各クライアントで個別に使用することもできます。

TSANDS.CFG ファイル

(Novell NetWare固有の用語) バックアップを開始するコンテナの名前を指定するファイル。このファイルはテキスト ファイルで、TSANDS.NLMがロードされるサーバのSYS:SYSTEM\TSAディレクトリにあります。

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クライアントとCell Manager間の通信を行います。また、ビジネス ロジック処理を実行し、重要な情報のみをクライアントに送信します。このサービスは、Data ProtectorがCell Manager上にインストールされるとすぐに開始されます。

VMware 管理クライアント

(VMware用統合統合ソフトウェア固有の用語) Data Protectorを使用してVMware Virtual Infrastructureと通信するクライアント。VirtualCenter Server システム（VirtualCenter 環境）または ESX Server システム（スタンドアロンの ESX Server 環境）が考えられます。

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。

Volume Shadow Copy Service

「Microsoft Volume Shadow Copy Service 。」を参照。

VPO

「OM 。」を参照。

VSS

「Microsoft Volume Shadow Copy Service 。」を参照。

VSS準拠のモード

(HP StorageWorks Disk Array XP VSSプロバイダ固有の用語) 2つのXP VSSハードウェア プロバイダのうちの1つの操作モード。XPプロバイダがVSS準拠モードである場合、ソース ボリューム（P-VOL）および複製（S-VOL）は、バックアップ後に単方向のペアリングされない状態になります。したがって、ローテーションされる複製（1つのP-VOLごとのS-VOL）の最大数には、制限がありません。このような構成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です。「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 。」を参照。

VxFS

Veritas Journal Filesystemの略。

VxVM（Veritas Volume Manager）

Veritas Volume Managerは、Solarisプラットフォーム上でディスク スペースを管理するためのシステムです。VxVMシステムは、論理ディスク グループに編成された1つまたは複数の物理ボリュームの任意のグループからなります。

Wake ONLAN 節電モードで動作しているシステムを同じLAN上の他のシステムからのリモート操作により電源投入するためのサポート。

Webレポート Data Protectorの機能の1つ。バックアップ ステータス、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 CONFIGURATION バックアップ Data Protectorでは、Windows CONFIGURATION（構成データ）をバックアップできます。Windowsレジストリ、ユーザー プロファイル、イベント ログ、WINSサーバ データおよびDHCPサーバ データ（システム上で構成されている場合）を1回の操作でバックアップできます。

Windowsレジストリ オペレーティング システムやインストールされたアプリケーションの構成情報を保存するため、Windowsにより使用される集中化されたデータベース。

WINSサーバ Windowsネットワークのコンピュータ名をIPアドレスに解決するWindows Internet Name Serviceソフトウェアを実行しているシステム。 Data Protectorでは、WINSサーバ データをWindowsの構成データの一部としてバックアップできます。

XBSAインタフェース *(Informix 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。

XCopyエンジン *(ダイレクト バックアップ固有の用語)* SCSI-3のコピー コマンド。SCSIソース アドレスを持つストレージ デバイスからSCSIあて先アドレスを持つバックアップ デバイスにデータをコピーし、ダイレクト バックアップを可能にします。XCopyでは、ソース デバイスからデータをブロック（ディスクの場合）またはストリーム（テープの場合）としてあて先デバイスにコピーします。これにより、データをストレージ デバイスから読み込んであて先デバイスに書き込むまでの一連の処理が、制御サーバをバイパスして行われます。
「ダイレクト バックアップ 。」を参照。

ZDB **「ゼロ ダウンタイム バックアップ (ZDB) 。」を参照。**

ZDBデータベース *(ZDB固有の用語)*ソース ボリューム、複製およびセキュリティ情報などのZDB関連情報を格納するIDBの一部。ZDBデータベースはZDB、インスタント リカバリ、スプリット ミラー復元に使用されます。
「ゼロ ダウンタイム バックアップ (ZDB) 。」を参照。

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。

アーカイブREDOログ

(Oracle固有の用語) オフラインREDOログとも呼ばれます。OracleデータベースがARCHIVELOGモードで動作している場合、各オンラインREDOログが最大サイズまで書き込まれると、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 」を参照。

アクセス権限

「ユーザー権限 。」を参照。

アプリケーション エージェント

クライアント上でオンライン データベース統合ソフトウェアを復元およびバックアップするために必要なコンポーネント。「Disk Agent 。」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 。」を参照。

イベント ログ

(Windows固有の用語) イベント ログ (Windows固有の用語) サービスの開始および停止、ユーザーのログインおよびログオフなど、Windows のすべてのイベントが記録されるファイル。 Data Protector では、Windowsの構成バックアップの一部として、Windows Event Logをバックアップすることができます。

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 。」を参照。

Installation Server
特定のアーキテクチャ用のData Protectorソフトウェア パッケージのレポジトリを保持するコンピュータ システム。Installation Server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Installation Serverが必要です。1台がUNIXシステム用、もう1台が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 ストアでは、メールボックス ストアとパブリック フォルダ ストアの2種類のストアが管理されます。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 。」を参照。

上書き
復元中のファイル名競合を解決するモードの1つ。既存のファイルの方が新しくても、すべてのファイルがバックアップから復元されます。
「マージ 。」を参照。

エクスチェンジャ
SCSIエクスチェンジャとも呼ばれます。
「ライブラリ 。」を参照。

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 。」を参照。

オートチェンジャー
「ライブラリ 。」を参照。

オートローダ
「ライブラリ 。」を参照。

オブジェクト
「バックアップ オブジェクト 。」を参照。

オブジェクト コピー
特定のオブジェクト バージョンのコピー。オブジェクト コピー セッション中またはオブジェクト ミラーのバックアップ セッション中に作成されます。

オブジェクト コピー セッション

異なるメディア セット上にバックアップされたデータの追加のコピーを作成するプロセス。オブジェクト コピー セッション中に、選択されたバックアップ オブジェクトがソースからターゲット メディアへコピーされます。

オブジェクト 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。

オブジェクトのコピー

選択されたオブジェクト バージョンを特定のメディア セットにコピーするプロセス。1つまたは複数のバックアップ セッションからコピーするオブジェクトを選択できます。

オブジェクトのミラーリング

バックアップ セッション中に、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

フル バックアップと1回以上の増分バックアップから成るバックアップ オブジェクトの復元チェーンを、新しい集約バージョンのオブジェクトにマージするプロセス。

オフライン バックアップ

実行中はアプリケーション データベースがアプリケーションから使用できなくなるバックアップ。

- 単純なバックアップ方法の場合 (ZDBではない)、データベースはバックアップ中 (数分から数時間) に通常オフライン状態となり、バックアップ システムからは使用できますが、アプリケーションから使用できません。たとえばテープへのバックアップの場合、テープへのデータ ストリーミングが終わるまでの間となります。
- ZDBの方法を使うと、データベースはオフライン状態になりますが、所要時間はデータ複製プロセス中のわずか数秒間です。残りのバックアップ プロセスでは、データベースは通常の稼動を再開できます。

「ゼロ ダウンタイム バックアップ (ZDB) およびオンライン バックアップ 。」を参照。

オフラインREDOログ

「アーカイブREDOログ 。」を参照。

オフライン復旧

オフライン復旧は、ネットワーク障害などによりCell Managerにアクセスできない場合に行われます。オフライン復旧には、スタンドアロン デバイスとSCSIライブラリ デバイスだけを使用できます。Cell Managerの復旧は、常にオフラインで行われます。

オリジナル 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 バックアップ

データベース アプリケーションを利用可能な状態に維持したまま行われるバックアップ。データベースは、バックアップ アプリケーションが元のデータ オブジェクトにアクセスする必要がある間、特別なバックアップ モードで稼動します。この期間中、データベースは完全に機能しますが、パフォーマンスに多少影響が出たり、ログ ファイルのサイズが急速に増大したりする場合もあります。

- 単純なバックアップ方法の場合（ZDBではない）、バックアップ中（数分から数時間）は、常にバックアップ モードである必要があります。たとえばテープへのバックアップの場合、テープへのデータ ストリーミングが終わるまでの間となります。
- ZDBの方法を使うと、バックアップ モードである必要がある時間はデータ複製プロセス中のわずか数秒間です。残りのバックアップ プロセスでは、データベースは通常の稼動を再開できます。

場合によっては、データベースを整合性を保って復元するために、トランザクション ログもバックアップする必要があります。「ゼロ ダウンタイム バックアップ(ZDB) 、およびオフライン バックアップ 。」を参照。

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 。」を参照。

階層ストレージ管理(HSM)

使用頻度の低いデータを低コストの光磁気プラッタに移動することで、コストの高いハード ディスク記憶域を有効利用するための仕組み。移動したデータが必要になった場合は、ハード ディスク記憶域に自動的に戻されます。これにより、ハード ディスクからの高速読み取りと光磁気プラッタの低コスト性のバランスが維持されます。

拡張可能ストレージ エンジン (ESE)

(Microsoft Exchange Server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。

仮想コントローラ ソフトウェア (VCS)

(HP StorageWorks EVA固有の用語) HSVコントローラを介したCommand View EVAとの通信など、記憶システムの処理すべてを管理するファームウェア。
「Command View (CV) EVA 。」を参照。

仮想サーバ

仮想マシンとは、ネットワークIP名およびIPアドレスでドメイン内に定義されるクラスタ環境を意味します。このアドレスは、クラスタ ソフトウェアによってキャッシュされ、仮想サーバ リソースを現在実行しているクラスタ ノードにマッピングされます。こうして、特定の仮想サーバに対するすべての要求が特定のクラスタ ノードにキャッシュされます。

仮想ディスク

(HP StorageWorks EVA固有の用語) HP StorageWorks Enterprise Virtual Arrayストレージ プールから割り当てられたストレージのユニット。仮想ディスクは、HP StorageWorks Enterprise Virtual Arrayのスナップショット機能により複製されるエンティティです。
「ソース ボリューム およびターゲット ボリューム 。」を参照。

仮想テープ

(VLS固有の用語) テープに保存するのと同様に、データをディスク ドライブにバックアップするアーカイブ ストレージ テクノロジ。仮想テープ システムの利点には、バックアップおよび復元のスピードが向上すること、運用コストが低いことなどがあります。
「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 。」を参照。

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) 。」を参照。

仮想デバイス インタフェース

(Microsoft SQL Server固有の用語) 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

効率の良い合成バックアップのタイプ。コピーされる代わりに、ポインタの使用によってデータが集約されます。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、およびその結果生成される仮想フル バックアップ)を、配布ファイル メディア形式を使用する単一のファイル ライブラリに書き込む場合に実行します。

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 。」を参照。

監査情報 Data Protectorセル全体でユーザーによって定義された拡張期間に実行された、各バックアップ 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ているデータから作成された、ユーザーが読み取り可能な形式の監査情報。

監査ログ 監査データが保存されているデータ ファイル。

キー ストア 暗号化キーはすべてCell Managerのキー ストアに集中して保存され、Key Management Server (KMS)によって管理されます。

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 。」を参照。

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)* *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) にある、Informix Serverの構成ファイル ixbar.*server_id*。*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。

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。

クライアント バックアップ
クライアント上にマウントされている状態のすべてのファイルシステムのバックアップ。ただし、バックアップ仕様の作成後にクライアントにマウントされたファイルシステムは、自動検出されません。

クラスタ対応アプリケーション
クラスタ アプリケーション プログラミング インタフェースをサポートしているアプリケーション。クラスタ対応アプリケーションごとに、クリティカル リソースが宣言されます。これらのリソースには、ディスク ボリューム(Microsoft Cluster Serverの場合)、ボリューム グループ(MC/ServiceGuardの場合)、アプリケーション サービス、IP名、およびIPアドレスなどがあります。

グループ
(Microsoft Cluster Server固有の用語) 特定のクラスタ対応アプリケーションを実行するために必要なリソース（ディスクボリューム、アプリケーション サービス、IP名およびIPアドレスなど）の集合。

グローバル オプション ファイル
Data Protectorをカスタマイズするためのファイル。このファイルでは、Data Protectorのさまざまな設定（特に、タイムアウトや制限）を定義でき、その内容はData Protectorセル全体に適用されます。ファイルは、Cell Managerの*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Solarisシステムの場合)に配置されています。

検証
指定したメディア上のData Protectorデータが読み取り可能かどうかをチェックする機能。また、CRC（巡回冗長検査）オプションをオンにして実行したバックアップに対しては、各ブロック内の整合性もチェックできます。

合成バックアップ
合成フル バックアップを生成するバックアップ ソリューション。データに関しては従来のフル バックアップと同等ですが、プロダクション サーバまたはネットワークに負荷がかかりません。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回数の増分バックアップから作成されます。

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を新しい合成フル バージョンのオブジェクトにマージする、オブジェクト集約処理の結果として生成されます。合成フル バックアップは、復元速度の点では、従来のフル バックアップと同等です。

コピー セット
(HP StorageWorks EVA固有の用語) ローカルEVA上にあるソース ボリュームとリモート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CA+BC EVA 」を参照。

コマンド ビュー VLS

(VLS固有の用語) LANを介してVLSを構成、管理、監視するために使用されるWebブラウザ ベースのGUI。
「仮想ライブラリ システム (VLS) 。」を参照。

コマンド行インタフェース (CLI)

CLIには、DOSコマンドやUNIXコマンドと同じようにシェル スクリプト内で使用でできるコマンドが用意されています。これらを使用して、Data Protectorの構成、バックアップ、復元、および管理の各タスクを実行することができます。

再解析ポイント

(Windows固有の用語) 任意のディレクトリまたはファイルに関連付けることができるシステム制御属性。再解析属性の値は、ユーザー制御データをとることができます。このデータの形式は、データを保存したアプリケーションによって認識され、データの解釈用にインストールされており、該当ファイルを処理するファイルシステム フィルタによっても認識されます。ファイルシステムは、再解析ポイント付きのファイルを検出すると、そのデータ形式に関連付けられているファイルシステム フィルタを検索します。

再同期モード

(HP StorageWorks Disk Array XP VSSプロバイダ固有の用語) One of two XP VSS hardware provider operation modes.XPプロバイダが再同期モードである場合、ソース ボリューム (P-VOL) および複製(S-VOL) は、バックアップ後に一時停止されたミラー関係になります。ローテーションされる複製 (1つのP-VOLごとのS-VOL) の最大数は、MU範囲が0 ~ 2または0、1、2の場合、3つになります。このような構成のバックアップからの復元は、S-VOLのP-VOLとの再同期によってのみ可能です。
「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) 、MU番号 、および複製セット ローテーション 。」を参照。

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によって、Microsoft Exchange Server 5.5との互換性を持つMicrosoft Exchange Server 2000/2003のサービスです。
「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 。」を参照。

差分同期(再同期)

(EMC Symmetrix固有の用語) BCVまたはSRDFの制御操作。BCV制御操作では、Incremental Establish(増分的確立)により、BCVデバイスが増分的に同期化され、EMC Symmetrixミラー化メディアとして機能します。EMC Symmetrixデバイスは、事前にペアにしておく必要があります。SRDF制御操作では、Incremental Establish(増分的確立)により、ターゲット デ

バイス(R2)が増分的に同期化され、EMC Symmetrixミラー化メディアとして機能します。EMC Symmetrixデバイスは、事前にペアにしておく必要があります。

差分バックアップ (delta backup)

差分バックアップ(delta backup)では、前回の各種バックアップ以降にデータベースに対して加えられたすべての変更がバックアップされます。
「バックアップの種類 。」を参照。

差分リストア

(EMC Symmetrix固有の用語) BCVまたはSRDFの制御操作。BCV制御操作では、差分リストアにより、BCVデバイスがペア内の2番目に利用可能な標準デバイスのミラーとして再割り当てされます。これに対し、標準デバイスの更新時には、オリジナルのペアの分割中にBCVデバイスに書き込まれたデータだけが反映され、分割中に標準デバイスに書き込まれたデータはBCVミラーからのデータで上書きされます。SRDF制御操作では、差分リストアにより、ターゲット デバイス(R2)がペア内の2番目に利用可能なソース デバイス(R1)のミラーとして再割り当てされます。これに対し、ソース デバイス(R1)の更新時には、オリジナルのペアの分割中にターゲット デバイス(R2)に書き込まれたデータだけが反映され、分割中にソース デバイス(R1)に書き込まれたデータはターゲット ミラー(R2)からのデータで上書きされます。

システム データベース

(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 ボリューム/ディスク/パーティション

オペレーティング システム ファイルが格納されているボリューム/ディスク/パーティション。ただし、Microsoftの用語では、ブート プロセスの開始に必要なファイルが入っているボリューム/ディスク/パーティションをシステム ボリューム/ディスク/パーティションと呼んでいます。

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 (証明書サーバの場合) が含まれます。サーバがドメイン コントローラの場合は、Active DirectoryサービスとSYSVOLディレクトリもシステム状態データに含まれます。サーバ上でクラスタ サービスが実行されている場合は、リソース レジストリ チェックポイントと、最新のクラスタ データベース情報を格納するクォーラム リソース回復ログもシステム状態データに含まれます。

事前割当てリスト メディア プール内のメディアのサブセットをバックアップに使用する順に指定したリスト。

実行後 オブジェクトのバックアップ後、またはセッション全体の完了後にコマンドまたはスクリプトを実行するバックアップ オプション。実行後コマンドは、Data Protectorで事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows上で動作する実行可能ファイルまたはバッチファイル、UNIX上で動作するシェル スクリプトなどを使用できます。
「実行前 。」を参照。

実行前 オブジェクトのバックアップ前、またはセッション全体の開始前にコマンドまたはスクリプトを実行するバックアップ オプション。実行前コマンドおよび実行後コマンドは、Data Protectorで事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows上で動作する実行可能ファイルまたはバッチファイル、UNIX上で動作するシェル スクリプトなどを使用できます。
「実行後 。」を参照。

実行前/実行後コマンド 実行前コマンドおよび実行後コマンドは、バックアップ セッションまたは復元セッションの前後に付加的な処理を実行する実行可能ファイルまたはスクリプトです。実行前コマンドおよび実行後コマンドは、Data Protectorで事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows上で動作する実行可能ファイルまたはバッチファイル、UNIX上で動作するシェル スクリプトなどを使用できます。

自動移行 *(VLS固有の用語)* 最初にVLS仮想テープに対してデータ バックアップを行い、次にバックアップ アプリケーションを使用することなく物理テープ (1つの物理テープをエミュレートする1つの仮想テープ) に移行することができる機能。
「仮想ライブラリ システム (VLS) および仮想テープ 。」を参照。

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。バックアップ中に元のボリュームに変更が加えられても、ボリュームのシャドウ コピーは整合性のある状態に保たれます。
「Microsoft Volume Shadow Copy Service および複製 。」を参照。

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 。」を参照。

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、ソフトウェアで実装することも (システム プロバイダなど)、ハードウェア (ローカル ディスクやディスク アレイ) で実装することもできます。
「シャドウ コピー 。」を参照。

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 。」を参照。

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 モードおよびLotus Domino Serverデータベース モードで、該当するデータがデータベースにコミットされた後、トランザクション ログ ファイルの内容が定期的に上書きされる形式のログです。循環ログにより、ディスク記憶領域の消費が低減できます。

初期化

「フォーマット 。」を参照。

所有権

バックアップの所有権は、どのユーザーがバックアップからデータを復元できるかを決定します。あるユーザーが対話型バックアップを開始すると、そのユーザーはセッション オーナーになります。ユーザーが既存のバックアップ仕様を修正せずにそのまま起動した場合、そのバックアップ セッションは対話型とみなされません。この場合、バックアップ仕様内でバックアップ オーナーが指定されていれば、その指定が継承されます。バックアップ仕様内でバックアップ オーナーが指定されていなければ、バックアップを開始したユーザーがセッション オーナーになります。スケジュールされたバックアップについては、デフォルトで、UNIX Cell Managerのセッション所有者はroot.sys@*Cell Manager*、Windows Cell Managerのセッション所有者はCell Managerのインストール中に指定されたユーザーです。所有権は変更可能なので、特定のユーザーをセッション オーナーにすることができます。

シングル インスタンス機能

(IAP固有の用語) オブジェクト全体およびチャンク レベルの両方で、データの冗長性を認識するプロセス。各データ チャンクのストロング ハッシュ関数が計算され、作成中の複製の保存を試行するか決める際に必要となる、固有のコンテンツ アドレスとして使用されます。
「IAPへのバックアップ 。」を参照。

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。

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セカンダリ ボリューム (S-VOL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 プロセスで管理します。

ストレージ ボリューム

(ZDB固有の用語) ストレージ ボリュームは、オペレーティング システムまたはボリューム管理システム、ファイル システム、または他のオブジェクトが存在可能なその他のエンティティに提供可能なオブジェクトを表します（たとえば仮想化技法)。ボリューム管理システム、ファイル システムはこの記憶域に構築されます。これらは通常、ディスク アレイなどの記憶システム内に作成または存在します。

スナップショット

(HP StorageWorks VAおよびHP StorageWorks EVA固有の用語) スナップショット作成技法を使用して作成された複製の形式。使用するアレイ/技法に応じて、特徴の異なるさまざまな種類のスナップショットが使用できます。スナップショッ

トで作成された複製は動的なもので、スナップショットの種類や作成時間によって、ソース ボリュームの内容に依存する仮想コピーか、独立した正確な複製（クローン）かのいずれかになります。
「複製 およびスナップショット作成 。」を参照。

スナップショット バックアップ *(HP StorageWorks VA およびHP StorageWorks EVA固有の用語)*

「テープへのZDB 、ディスクへのZDB 、およびディスク+テープへのZDB 。」を参照。

スナップショット作成

(HP StorageWorks VAおよびHP StorageWorks EVA固有の用語) 複製を作成する技法で、ストレージ仮想化技法を使用して、ソース ボリュームのコピーが作成されます。 複製はある一時点で作成されたものとみなされ、事前構成することなく、即座に使用できます。ただし、通常は複製作成後もコピープロセスはバックグラウンドで継続されます。
「スナップショット 。」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。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その例です。スパースファイルの処理を復元中に有効にしておかないと、スパースファイルを復元できなくなる可能性があります。

スプリット ミラー

*(EMC SymmetrixおよびHP StorageWorks Disk Array XP固有の用語)*スプリット ミラー技法を使用して作成した複製。複製により、ソース ボリュームの内容について独立した正確な複製（クローン）が作成されます。
「複製 およびスプリット ミラー作成 。」を参照。

スプリット ミラー バックアップ *(EMC Symmetrix固有の用語)*

「テープへのZDB 。」を参照。

スプリット ミラー バックアップ *(HP StorageWorks Disk Array XP固有の用語)*

「テープへのZDB 、ディスクへのZDB 、およびディスク+テープへのZDB 。」を参照。

スプリット ミラーの作成

*(EMC SymmetrixおよびHP StorageWorks Disk Array XP固有の用語)*事前構成したターゲット ボリュームのセット（ミラー）を、ソース ボリュームの内容の複製が必要になるまでソース ボリュームのセットと同期化し続ける複製技法。その後、同期を停止（ミラーを分割）すると、分割時点での

ソース ボリュームのスプリット ミラー複製はターゲット ボリュームに残ります。
「スプリット ミラー 。」を参照。

スプリット ミラー復元

*(EMC SymmetrixおよびHP StorageWorks Disk Array XP固有の用語)*テープへのZDBセッションまたはディスク+テープへのZDBセッションでバックアップされたデータをテープ メディアからスプリット ミラー複製へ復元し、その後ソース ボリュームに同期させるプロセス。この方法では、完全なセッションを復元することも個々のバックアップ オブジェクトを復元することも可能です。
「テープへのZDB 、ディスク+テープへのZDB 、および複製 。」を参照。

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 ライブラリに作成されたバックアップ データのコピー。スマート コピーのプロセスのよって、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。
「仮想ライブラリ システム (VLS) 。」を参照。

スマート コピープール

(VLS固有の用語) 指定したソース仮想ライブラリのスマート コピー ターゲットとして使用可能なコピー先ライブラリ スロットが定義されたプール。
「仮想ライブラリ システム (VLS) およびスマート コピー 。」を参照。

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1式のレジスタ値からなります。同じプロセス内で複数のスレッドを同時に実行できます。

スロット

ライブラリ内の機械的位置。各スロットがメディア (DLTテープなど) を1つずつ格納します。Data Protector では、各スロットを番号で参照します。メディアを読み取るときには、ロボット機構がメディアをスロットからドライブに移動します。

制御ファイル

(OracleおよびSAP R/3固有の用語) データベースの物理構造を指定するエントリが含まれるOracleデータ ファイル。復旧に使用するデータベース情報の整合性を確保できます。

セカンダリ ボリューム (S-VOL)

(HP StorageWorks Disk Array XP固有の用語) セカンダリ ボリューム (S-VOL) は、他のLDEV (P-VOL)のセカンダリなCAミラーおよびBCミラーとして動作するXP LDEVです。CAの場合、S-VOLをMetroCluster構成内のフェイルオーバー デバイスとして使うことができます。S-VOLには、P-VOLによって使用されるアドレスとは異なる、個別のSCSIアドレスが割り当てられます。

「プライマリ ボリューム (P-VOL) およびMain Control Unit (MCU) 。」を参照。

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 キー

実行前スクリプトおよび実行後スクリプト用の環境変数。プレビュー セッションを含めたData Protectorセッションを一意に識別します。セッション キーはデータベースに記録されず、CLIコマンドのomnimnt、，omnistat、およびomniabortコマンド。

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、またはメディア管理セッションの識別子で、セッションを実行した日付と一意の番号から構成されます。

セル

1台のCell Managerに管理されているシステムの集合。セルには、一般に、同じLANに接続されたサイトや組織エンティティ上のシステムが含まれます。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。

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 。」を参照。

増分1メールボックス バックアップ

増分1メールボックス バックアップでは、前回のフル バックアップ以降にメールボックスに対して行われた変更をすべてバックアップします。

増分ZDB

保護されている最後のフル バックアップまたは増分バックアップより後に変更された部分のみをバックアップする、ファイルシステムのテープへのZDBセッションまたはディスク+テープへのZDBセッション。
「フルZDB 。」を参照。

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 。」を参照。

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 。」を参照。

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) 。」を参照。

ソース ボリューム

(ZDB固有の用語) 複製されたデータを含むストレージ ボリューム。

ターゲット システム

(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) ソース デバイス (R1) との SRDF操作に参加するEMC Symmetrixデバイス。リモート EMC Symmetrix ユニット内に置かれます。ローカル EMC Symmetrix ユニット内でソース デバイス (R1) とペアになり、ミラー化ペアから、すべての書き込みデータを受け取ります。このデバイスは、通常のI/O操作ではユーザー アプリケーションからアクセスされません。R2 デバイスは、RDF2 グループ タイプに割り当てる必要があります。
「ソース デバイス (R1) 。」を参照。

ターゲット ボリューム

(ZDB固有の用語) データの複製先のストレージ ボリューム。

ターミナル サービス

(Windows固有の用語) Windowsのターミナル サービスは、サーバ上で実行されている仮想Windowsデスクトップ セッションとWindowsベースのプログラムにクライアントからアクセスできるマルチセッション環境を提供します。

ダイレクト バックアップ

SCSI Extended Copy (Xcopy)コマンドを使用してディスクからテープ(または他の2次ストレージ)へのデータの直接移動を効率化する、SANベースのバックアップ ソリューション。ダイレクト バックアップは、SAN環境内のシステムへのバックアップI/O負荷を軽減します。ディスクからテープ(または他の2次ストレージ)へのデータの直接移動をSCSI Extended Copy (XCopy)コマンドで効率化します。このコマンドは、ブリッジ、スイッチ、テープ ライブラリ、ディスク サブシステムなど、インフラストラクチャの各要素でサポートされています。
「XCopyエンジン 。」を参照。

チャネル

(Oracle固有の用語) Oracle Recovery Managerのリソース割り当て。チャネルが割り当てられるごとに、新しいOracleプロセスが開始され、そのプロセスを通じてバックアップ、復元、および復旧が行われます。割り当てられるチャンネルの種類によって、使用するメディアの種類が決まります。

- diskタイプ
- SBT_TAPEタイプ

OracleがData Protectorと統合されており、指定されたチャネルの種類が SBT_TAPEタイプの場合は、上記のサーバ プロセスがData Protectorに対してバックアップの読み取りとデータ ファイルの書き込みを試行します。

チャンク化

(IAP固有の用語) データをブロック (チャンク) に分割するプロセスで、各チャンクでは固有のコンテンツ アドレスが取得されます。次に、このアドレスは、特定のチャンクがIAPアプライアンスにすでにバックアップされたかどうかを特定するために使用されます。重複データが特定された場合 (2つのアドレスが同じ、つまり、取得したアドレスがIAPにすでに保存されているデータ チャンクのアドレスと同じ場合)、バックアップされません。この方法では、データの冗長性が低減され最適なデータ保存が達成されます。
「IAPへのバックアップ 。」を参照。

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。

ディスク イメージ (rawディスク) のバックアップ

ディスク イメージのバックアップでは、ファイルがビットマップ イメージとしてバックアップされるので、高速バックアップが実現します。ディスク イメージ(rawディスク)バックアップでは、ディスク上のファイルおよびディレクトリの構造はバックアップされませんが、ディスク イメージ構造がバイト レベルで保存されます。ディスク イメージ バックアップは、ディスク全体か、またはディスク上の特定のセクションを対象にして実行できます。

ディスク クォータ コンピュータ システム上のすべてのユーザーまたはユーザーのサブセットに対してディスク スペースの消費を管理するためのコンセプト。このコンセプトは、いくつかのオペレーティング システム プラットフォームで採用されています。

ディスク グループ *(Veritas Volume Manager固有の用語)* VxVMシステムにあるデータ 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 複数のフェーズでデータをバックアップするプロセス。これにより、バックアップと復元のパフォーマンスが改善し、バックアップ データの保存コストが低減し、復元に対するデータの可用性とアクセス性が向上します。バックアップ ステージは、最初に1種類のメディア(たとえば、ディスク)にデータをバックアップし、その後データを異なる種類のメディア(たとえば、テープ)にコピーすることから構成されます。

ディスク+テープへのZDB *(ZDB固有の用語)* ゼロ ダウンタイム バックアップの1つの形式。ディスクへのZDBと同様に、作成された複製が特定の時点でのソース ボリュームのバックアップとしてディスク アレイに保持されます。ただし、テープへのZDBと同様、複製データはバックアップ メディアにもストリーミングされます。このバックアップ方法を使用した場合、同じセッションでバックアップしたデータは、インスタント リカバリ、Data Protector標準のテープからの復元を使用して復元できます。スプリット ミラー アレイではスプリット ミラー復元が可能です。
「ゼロ ダウンタイム バックアップ (ZDB) 、ディスクへのZDB 、テープへのZDB 、インスタント リカバリ 、複製 、および複製セット ローテーション 。」を参照。

ディスクへのZDB *(ZDB固有の用語)* ゼロ ダウンタイム バックアップの1つの形式。作成された複製が、特定の時点でのソース ボリュームのバックアップとしてディスク アレイに保持されます。同じバックアップ仕様を使って別の時点で作成された複数の複製を、複製セットに保持することができます。テープにZDBした複製はインスタント リカバリ プロセスで復元できます。
「ゼロ ダウンタイム バックアップ (ZDB) 、テープへのZDB 、ディスク+テープへのZDB 、インスタント リカバリ 、および複製セット ローテーション 。」を参照。

ディスク検出 ディスク検出では、クライアントのバックアップ中にディスクを検出します。このときData Protectorが探索（検出）するのは、クライアント上に存在するディスクで、バックアップの構成時にシステム上に存在しなかったディスクも検出の対象に含まれます。検出されたディスクがバックアップされます。これにより、ディスクのマウントとマウント解除が頻繁に繰り返される動的な構成にも対応できます。ディスクが展開されると、それぞれのディスクがマスター クライアント オブジェクト

のオプションをすべて継承します。実行前コマンドと実行後コマンドは、1回しか指定されていなくても、オブジェクトごとに繰り返し起動されることになります。

ディスク検出によるクライアントのバックアップ
クライアントにマウントされているすべてのファイルシステムのバックアップ。バックアップの開始時に、Data Protectorがクライアント上のディスクを自動検出します。ディスク検出によるクライアント バックアップでは、バックアップ構成が単純化され、ディスクのマウント/アンマウントが頻繁に行われるシステムに対するバックアップ効率が向上されます。

ディファレンシャル 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 タイプを実行するには、増分1バックアップ タイプを指定します。
「インクリメンタル バックアップ 。」を参照。

ディファレンシャル 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のみ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 。」を参照。

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が保存されます。データファイルは、1つのOracleデータベースにのみ所属できます。

データベース サーバ
大規模なデータベース(SAP R/3 データベースやMicrosoft SQLデータベースなど)が置かれているコンピュータ。サーバ上のデータベースへは、クライアントからアクセスできます。

データベース ライブラリ
Data Protectorのルーチンのセット。Oracle Serverのようなオンライン データベース統合ソフトウェアのサーバとData Protectorの間でのデータ転送を可能にします。

データベースの並列処理(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 」を参照。

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。スプリット ミラー アレイでは、スプリット ミラー復元も使用することができます。
「ゼロ ダウンタイム バックアップ (ZDB) 、ディスクへのZDB 、インスタント リカバリ 、ディスク+テープへのZDB 、および複製 。」を参照。

テーブルスペース (表領域、表スペース)

データベース構造の一部。各データベースは論理的に1つまたは複数の表スペースに分割されます。各表スペースには、データ ファイルまたは raw ボリュームが排他的に関連付けられます。

デバイス

ドライブまたはより複雑な装置（ライブラリなど）を格納する物理装置。

デバイス グループ

(EMC Symmetrix固有の用語) 複数のEMC Symmetrixデバイスを表す論理ユニット。デバイスは1つのデバイス グループにしか所属できません。デバイス グループのデバイスは、すべて同じ EMC Symmetrix装置に取り付けられている必要があります。デバイス グループにより、利用可能な EMC Symmetrix デバイスのサブセットを指定し、使用することができます。

デバイス ストリーミング

デバイスがメディアへ十分な量のデータを継続して送信できる場合、デバイスはストリーミングを行います。そうでない場合は、デバイスはテープを止めてデータが到着するのを待ち、テープを少し巻き戻した後、テープへの書込みを再開します。言い換えると、テープにデータを書き込む速度が、コンピュータ システムがデバイスへデータを送信する速度以下の場合、デバイスはストリーミングを行います。ストリーミングは、スペースの使用効率とデバイスのパフォーマンスを大幅に向上します。

デバイス チェーン

デバイス チェーンは、シーケンシャルに使用するように構成された複数のスタンドアロン デバイスからなります。デバイス チェーンに含まれるデバイスのメディアで空き容量がなくなると、自動的に次のデバイスのメディアに切り替えて、バックアップを継続します。

統合ソフトウェア オブジェクト

OracleまたはSAP DBなどのData Protector統合ソフトウェアのバックアップ オブジェクト。

同時処理数

「Disk Agentの同時処理数 」を参照。

動的（ダイナミック）クライアント

「ディスク検出によるクライアント バックアップ 。」を参照。

ドメイン コントローラ

ユーザーのセキュリティを保護し、別のサーバ グループ内のパスワードを検証するネットワーク内のサーバ。

ドライブ

コンピュータ システムからデータを受け取って、磁気メディア(テープなど) に書き込む物理装置。データをメディアから読み取って、コンピュータ システムに送信することもできます。

ドライブのインデックス

ライブラリ デバイス内のドライブの機械的な位置を識別するための数字。ロボット機構によるドライブ アクセスは、この数に基づいて制御されます。

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方式では、ドライブの暗号化機能を使用します。バックアップの実行時に、メディアに書き込まれるデータとメタ データの両方がドライブによって暗号化されます。

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元できます。

トランザクション ログ ファイル
データベースを変更するトランザクションを記録するファイル。データベースが破損した場合にフォールト トレランスを提供します。

トランスポータブル スナップショット
(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 Volume Shadow Copy Service (VSS) 。」を参照。

ハートビート
特定のクラスタ ノードの動作ステータスに関する情報を伝達するタイム スタンプ付きのクラスタ データ セット。このデータセット(パケット)は、すべてのクラスタ ノードに配布されます。

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 タイ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 。」を参照。

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 システムのターゲット ボリュームに接続しているシステム。典型的なバックアップ システムは、バックアップ デバイスに接続され、複製内のデータのバックアップを実行します。
「アプリケーション システム 、ターゲット ボリューム 、および複製 。」を参照。

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（対話式セッション）こともできます。1つのバックアップ仕様の中で複数のクライアントが構成されている場合、すべてのクライアントが同じバックアップの種類（フルまたは増分）を使って、1回のバックアップ セッションで同時にバックアップされます。バックアップ セッションの結果、1式のメディア にバックアップ データが書き込まれます。これらのメディアは、バックアップ セットまたはメディア セットとも呼ばれます。
「および バックアップ仕様、 増分バックアップ、およびフルバックアップ 。」を参照。

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 ビュー
Data Protectorでは、バックアップ仕様のビューを切り替えることができます。
[種類別]（デフォルト）を選択すると、バックアップ/テンプレートで利用できるデータの種類に基づいたビューが表示されます。
[グループ別]を選択すると、バックアップ仕様/テンプレートの所属先のグループに基づいたビューが表示されます。
[名前別]を選択すると、バックアップ仕様/テンプレートの名前に基づいたビューが表示されます。
[Manager別]（MoMの実行時のみ有効）を選択すると、バックアップ仕様/テンプレートの所属先のCell Managerに基づいたビューが表示されます。

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。

バックアップの種類
「増分バックアップ 、差分バックアップ (differential backup) 、トランザクション バックアップ 、フル バックアップ 、および差分バックアップ 。」を参照。

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。

バックアップ仕様
バックアップ対象オブジェクトを、使用するデバイスまたはドライブのセット、仕様内のすべてのオブジェクトに対するバックアップ オプション、バックアップを行う日時とともに指定したリスト。オブジェクトとなるのは、ディスクやボリューム全体、またはその一部、たとえばファイル、ディレクトリ、Windowsレジストリなどです。インクルード リストおよびエクスクルード リストを使用して、ファイルを選択することもできます。

パッケージ
(MC/ServiceGuardおよびVeritas Cluster固有の用語) 特定のクラスタ対応アプリケーションを実行するために必要なリソース（ボリューム グループ、アプリケーション サービス、IP名およびIPアドレスなど）の集合。

パブリック フォルダ ストア

(Microsoft Exchange Server固有の用語) インフォメーション ストアのうち、パブリック フォルダ内に情報を維持する部分。パブリック フォルダ ストアは、バイナリ リッチテキスト.edbファイルと、ストリーミング ネイティブ インターネット コンテンツを格納する.stmファイルから構成されます。

パブリック/プライベート バックアップ データ

バックアップを構成する際は、バックアップ データをパブリックまたはプライベートのいずれにするかを選択できます。

- パブリック データ – すべてのData Protectorユーザーに対してアクセスと復元が許可されます。
- プライベート データ – バックアップの所有者および管理者に対してのみ表示と復元が許可されます。

未介在操作

「無人操作 。」を参照。

ファースト レベル ミラー

(HP StorageWorks Disk Array XP固有の用語) HP StorageWorks Disk Array XPでは、プライマリ ボリュームのミラー コピーを最大3つまで作成することができ、このコピー1つにつきさらに2つのコピーを作成できます。最初の3つのミラー コピーはファースト レベル ミラーと呼ばれます。「プライマリ ボリューム およびMU番号 。」を参照。

ファイバ 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。光ケーブルまたは銅線ケーブルを使って、大容量データ ファイルを高速で双方向送信でき、数km離れたサイト間を接続できます。Fibre Channelは、ノード間を3種類の物理トポロジー(ポイント トゥ ポイント式、ループ式、スイッチ式)で接続できます。

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) 作成、変更、または削除されたオブジェクトを特定するために、ファイルシステムをたどる処理。

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 ライブラリ デバイス

複数のメディアからなるライブラリをエミュレートするディスク上に存在するデバイス。ファイル デポと呼ばれる複数のファイルが格納されます。

ファイルシステム
ハード ディスク上に一定の形式で保存されたファイルの集まり。 ファイルシステムは、ファイル属性とファイルの内容がバックアップ メディアに保存されるようにバックアップされます。

ファイル複製サービス(FRS)
Windowsサービスの1つ。ドメイン コントローラのストア ログオン スクリプトとグループ ポリシーを複製します。また、分散ファイルシステム(DFS)共有をシステム間で複製したり、任意のサーバから複製作業を実行することもできます。

ブート ボリューム/ディスク/パーティション
ブート プロセスの開始に必要なファイルが入っているボリューム/ディスク/パーティション。ただし、Microsoftの用語では、オペレーティング システム ファイルが格納されているボリューム/ディスク/パーティションをブート ボリューム/ディスク/パーティションと呼んでいます。

ブール演算子
オンライン ヘルプ システムの全文検索には、AND、OR、NOT、NEAR の各ブール演算子を使用できます。複数の検索条件をブール演算子で組み合わせて指定することで、検索対象をより正確に絞り込むことができます。複数単語の検索に演算子を指定しなければ、ANDを指定したものとみなされます。たとえば、「manual disaster recovery」という検索条件は、「manual AND disaster AND recovery」と同じ結果になります。

フェイルオーバー
あるクラスタ 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 StorageWorks EVA固有の用語) CA+BC EVA構成におけるソースとあて先の役割を逆にする操作。
「CA+BC EVA 。」を参照。

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上（メディア ヘッダ）に保存されます。保護データがある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では、指定された順序でデバイスにアクセスします。

復元セッション

バックアップ メディアからクライアントシステムにデータをコピーするプロセス。

復元チェーン

バックアップ オブジェクトをある時点まで復元するのに必要なすべてのバックアップ。復元チェーンは、オブジェクトのフル バックアップと任意の数の関連する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/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、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。基本オペレーティング システムでは、バックアップ オブジェクトが含まれている完全な物理ディスクが複製されます。しかし、UNIXでボリュームマネージャを使用するときは、バックアップ オブジェクト（論理ボリューム）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でパーティションが使用されている場合、選択されたパーティションが含まれている物理ボリュームが複製されます。
「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 。」を参照。

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 。」を参照。

複製セット ローテーション

(ZDB固有の用語) 通常のバックアップ作成のために継続的に複製セットを使用すること。複製セットの使用を必要とする同一のバックアップ仕様が実行されるたびに、新規の複製がセットの最大数になるまで作成され、セットに追加されます。その後、セット内の最も古い複製は置き換えられ、セット内の複製の最大数が維持されます。
「複製 および複製セット 。」を参照。

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 StorageWorks Disk Array XP固有の用語) CA構成およびBC構成用のプライマリ ボリュームとしての役割を果たす標準のHP StorageWorks Disk Array XP LDEV。P-VOLはMCU内に配置されています。

「セカンダリ ボリューム (S-VOL) およびMain Control Unit (MCU) 。」を参照。

フラッシュ リカバリ領域

(Oracle固有の用語) フラッシュ リカバリ領域は、Oracle 10g/11gで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のディスク グループです。バックアップと復旧に関するファイル(リカバリ ファイル)の中央格納領域として機能します。
「リカバリ ファイル 。」を参照。

フリー プール

フリー プールは、メディア プール内のすべてのメディアが使用中になっている場合にメディアのソースとして補助的に使用できるプールです。ただし、メディア プールでフリー プールを使用するには、明示的にフリー プールを使用するように構成する必要があります。

フル データベース バックアップ

最後に（フルまたは増分）バックアップした後に変更されたデータだけではなく、データベース内のすべてのデータのバックアップ。フル データベース バックアップは、他のバックアップに依存しません。

フル バックアップ

フル バックアップでは、最近変更されたかどうかに関係なく、選択されたオブジェクトをすべてバックアップします。
「バックアップの種類 。」を参照。

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。

フルZDB

前回のバックアップから変更がない場合でも選択されたすべてのオブジェクトをテープにストリーミングする、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。
「インクリメンタルZDB 。」を参照。

分散ファイルシステム (DFS)

複数のファイル共有を単一の名前空間に接続するサービス。対象となるファイル共有は、同じコンピュータに置かれていても、異なるコンピュータに置かれていてもかまいません。DFSは、リソースの保存場所の違いに関係なくクライアントがリソースにアクセスできるようにします。

ペア ステータス

(HP StorageWorks Disk Array XP固有の用語) ミラー化されたディスクのペアは、そのペア上で実行されるアクションによって、さまざまなステータス値を持ちます。最も重要なステータス値は以下の3つです。

- コピー – ミラー化されたペアは、現在再同期中。データは一方のディスクからもう一方のディスクに転送されます。2つのディスクのデータは同じではありません。

- ペア – ミラー化されたペアは、完全に同期されており、両方のディスク（プライマリ ボリュームとミラー ボリューム）は全く同じデータを持ちます。
- 中断 – ミラー化されたディスク間のリンクは中断されています。両方のディスクが別々にアクセスされ、更新されています。ただし、ミラー関係はまだ保持されており、このペアはディスク全体を転送することなく、再同期することができます。

並行復元

1つの Media Agentからデータを受信するDisk Agentを複数実行して、バックアップ データを複数のディスクに同時に（並行して）復元すること。並行復元を行うには、複数のディスクまたは論理ボリュームに置かれているデータを選択し、同時処理数を2以上に設定してバックアップを開始し、異なるオブジェクトのデータを同じデバイスに送信する必要があります。並行復元中には、復元対象として選択した複数のオブジェクトがメディアから同時に読み取られるので、パフォーマンスが向上します。

並列処理

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。

保護

「データ保護 およびカタログ保護 。」を参照。

ホスティング 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。

ホスト バックアップ

「ディスク検出によるクライアント バックアップ 。」を参照。

ボリューム グループ

LVMシステムにおけるデータ ストレージ単位。ボリューム グループは、1つまたは複数の物理ボリュームから作成できます。同じシステム上に複数のボリューム グループを置くことができます。

ボリューム マウント ポイント

(Windows固有の用語) ボリューム上の空のディレクトリを他のボリュームのマウントに使用できるように構成したもの。ボリューム マウント ポイントは、ターゲット ボリュームへのゲートウェイとして機能します。ボリュームがマウントされていれば、ユーザーやアプリケーションがそのボリューム上のデータをフル（マージ）ファイルシステム パスで参照できます（両方のボリュームが一体化されている場合）。

マージ

復元中のファイル名競合を解決するモードの1つ。復元するファイルと同じ名前のファイルが復元先に存在する場合、変更日時の新しい方が維持されます。既存のファイルと名前が重複しないファイルは、常に復元されます。

「上書き 。」を参照。

マウント ポイント ディレクトリ構造内において、ディスクまたは論理ボリュームにアクセスするためのアクセス ポイント（/optやd:など）。UNIXでは、bdfコマンドまたはdfコマンドを使ってマウント ポイントを表示できます。

マウント要求 マウント要求時には、デバイスにメディアを挿入するように促す画面が表示されます。必要なメディアを挿入して確認することでマウント要求に応答すると、セッションが続行されます。

マジック パケット **「Wake ONLAN 。」を参照。**

マルチドライブ サーバ 単一システム上でMedia Agentを無制限に使用できるライセンス。このライセンスは、Cell ManagerのIP アドレスにバインドされており、新しいバージョンでは廃止されました。

ミラー ローテーション *(HP StorageWorks Disk Array XP固有の用語)* **「複製セット ローテーション 。」を参照。**

ミラー *(EMC SymmetrixおよびHP StorageWorks Disk Array XP固有の用語)* **「ターゲット ボリューム 。」を参照。**

無人操作 または**未介在操作** 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。

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 セット バックアップ セッションでは、メディア セットと呼ばれるメディアのグループにデータをバックアップします。メディ

アの使用法によっては、複数のセッションで同じメディアを共有できます。

メディア プール 同じ種類のメディア(DDS)などのセット。グループとして追跡されます。フォーマットしたメディアは、メディア プールに割り当てられます。

メディア ラベル メディアに割り当てられるユーザー定義の識別子。

メディアID Data Protectorがメディアに割り当てる一意な識別子。

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 。」を参照。

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 。」を参照。

メディアのポールティング 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。ポールティング手順は、会社のバックアップ戦略やデータ保護/信頼性ポリシーに依存します。

メディアの割り当て方針 メディアをバックアップに使用する順序を決定します。[Strict] メディア割り当てポリシーでは、特定のメディアに限定されます。[Loose] ポリシーでは、任意の適切なメディアを使用できます。[フォーマットされていないメディアを先に割り当てる] ポリシーでは、ライブラリ内に利用可能な非保護メディアがある場合でも、不明なメディアが優先されます。

メディアの使用法 ここでは、メディアの使用法として、以下のオプションのいずれかを選択します。メディアの使用法は、[追加可能]、[追加不可能]、[増分のみ追加可能]のいずれかに設定できます。

メディアの位置 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。

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 アカウントを持つユーザーのみ、Data Protectorを使用できなる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) 管理者が特権レベルの昇格を許可するまで、アプリケーション ソフトウェアの実行権限を標準ユーザーに限定するWindows Vista および Windows Server 2008 のセキュリティ コンポーネント。

ユーザー グループ 各Data Protectorユーザーは、ユーザー グループのメンバーです。各ユーザー グループには1式のユーザー権限があり、それらの権限がユーザー グループ内のすべてのユーザーに付与されます。ユーザー権限を関連付けるユーザー グループの数は、必要に応じて定義できます。ユーザー グループの例は、Admin、Operator、Userなどです。

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、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を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。

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。

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。

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archived logバックアップ セット
- データ ファイルのコピー
- アーカイブ REDO ログ
- ストアド スクリプト

リカバリ カタログ データベース

(Oracle固有の用語) リカバリ カタログ スキーマを格納するOracleデータベース。リカバリ カタログはターゲット データベースに保存しないでください。

リカバリ カタログ データベースへのログイン情報

(Oracle固有の用語) リカバリ カタログ データベース (Oracle) へのログイン情報の形式は *<user_name>*/*<password>*@*<service>*で、ユーザー名、パスワード、サービス名の説明は、Oracleターゲット データベースへのOracle SQL*Net V2ログイン情報と同じです。ただし、この場合の*service*はOracleターゲット データベースではなく、リカバリ カタログ データベースに対するサービス名となります。
ここで指定するOracleユーザーは、Oracleのリカバリ カタログのオーナー(所有者)でなければならないことに注意してください。

リカバリ ファイル

(Oracle固有の用語) リカバリ ファイルは、フラッシュ リカバリ領域に置かれるOracle 10g/11g固有のファイルです。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 。」を参照。

リサイクル

メディア上のすべてのバックアップ データのデータ保護を解除して、以降のバックアップで上書きできるようにするプロセス。同じセッションに所属しているデータのうち、他のメディアに置かれているデータも保護解除されます。リサイクルを行っても、メディア上のデータ自体は変更されません。

リムーバブル記憶域の管理データベース

(Windows固有の用語) Windowsサービスの1つ。リムーバブル メディア (テープやディスクなど) と記憶デバイス (ライブラリ) の管理に使用されます。リムーバブル記憶域により、複数のアプリケーションが同じメディア リソースを共有できます。

ローカル復旧とリモート復旧

リモート復旧は、SRDファイルで指定されているMedia Agentホストがすべてアクセス可能な場合にのみ実行されます。いずれかのホストがアクセス不能になっていると、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[ログなし]の4つのロギング レベルがあります。ロギング レベルの設定によって、IDBのサイズ増加、バックアップ速度、復元対象データのブラウズしやすさが影響を受けます。

ログイン ID

(Microsoft SQL Server固有の用語) Microsoft SQL Server上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。

論理ログ ファイル 論理ログ ファイルは、変更されたデータがディスクにフラッシュされる前に書き込まれるファイルです。オンライン データベース バックアップの場合に使用されます。障害発生時には、これらの論理ログ ファイルを使用することで、コミット済みのトランザクションをすべてロールフォワードするとともに、コミットされていないトランザクションをロールバックすることができます。

ワイルドカード文字 1文字または複数文字を表すために使用できるキーボード文字。たとえば、通常、アスタリスク (*) は1文字以上の文字を表し、疑問符 (?) は1文字を示します。ワイルドカード文字は、名前により複数のファイルを指定するための手段としてオペレーティング システムで頻繁に使用されます。

索引

E

F

G

H

I

J

K

L

M

N

O

R

S

T

か

き

く

け

こ

さ

せ

そ

た

ち

つ

へ

ほ

ま

む

め

も

や

ゆ

よ

ら

り

る

れ

ろ