HP Data Protector A.06.11

コンセプトガイド

製品番号: B6960-99121
初版: 2009年9月

ご注意

© Copyright 1999, 2009 Hewlett-Packard Development Company, L.P.

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。

インテル®、Itanium®、Pentium®、Intel Inside®、およびIntel Insideロゴは、米国およびその他の国におけるIntel Corporationまたはその子会社の商標または登録商標です。

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

AdobeおよびAcrobatは、Adobe Systems Incorporatedの商標です。

Javaは、米国におけるSun Microsystems, Inc.の商標です。

Oracle®は、Oracle Corporation (Redwood City, California)の米国における登録商標です。

UNIX®は、The Open Groupの登録商標です。

Printed in the US

目次

図一覧

表一覧

出版履歴

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

表 1 出版履歴

製品番号	ガイド版	製品
B6960-90059	2002年8月	Data Protector リリース A.05.00
B6960-90080	2003年5月	Data Protector リリース A.05.10
B6960-90105	2004年10月	Data Protector リリース A.05.50
B6960-96001	2006年8月	Data Protector リリース A.06.00
B6960-96035	2008年11月	Data Protector リリース A.06.10
B6960-99121	2009年9月	Data Protector リリース A.06.11

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 & 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、障害復旧のプランニング、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.06.11の新機能について説明しています。また、インストールの必要条件、必要なパッチ、および制限事項に関する情報に加えて、既知の問題と回避策についても提供します。

- 『*HP Data Protector product announcements ソフトウェアノートおよびリファレンス 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。

- 『*HP Data Protector command line interface reference*』

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

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-ROM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***: 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	障害復旧ガイド
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 - Informix、DB2、Lotus Notes/Domino
IG-MS	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, and Volume Shadow Copy Service
IG-O/S	インテグレーションガイド - Oracle、SAP
IG-OMU	インテグレーションガイド - HP Operations Manager、UNIX
IG-OMW	インテグレーションガイド - HP Operations Manager、Windows
IG-PM/PA	インテグレーションガイド - HP Performance Manager およびHP Performance Agent

略称	ガイド
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 Virtual Infrastructure、Sybase、Network Node Manager、Network Data Management Protocol 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	ZDB 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				
								MS	O/S	IBM	Var	SIP	Report	OMU	OMW	Concept	Admin	IG	GS	User	PA	MPE/iX	CLI
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 for UNIX/for Windows	IG-OMU、IG-OMW
HP Performance Manager	IG-PM/PA
HP Performance Agent	IG-PM/PA

統合	ガイド
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

統合	ガイド
Sybase	IG-Var
EMC Symmetrix	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

規則	要素
青色のテキスト:表2(31ページ)	クロスリファレンスリンクおよび電子メールアドレス
青色の下線付きテキスト:http://www.hp.com	Webサイトアドレス
*斜体*テキスト	テキスト強調
等幅テキスト	• ファイルおよびディレクトリ名 • システム出力 • コード • コマンド、引数、および引数の値
等幅、*斜体*テキスト	• コード変数 • コマンド変数
等幅、太字テキスト	強調された等幅テキスト

△ **注意:**

指示に従わなかった場合、機器設備またはデータに対し、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 ProtectorGUIまたはData ProtectorJava 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。

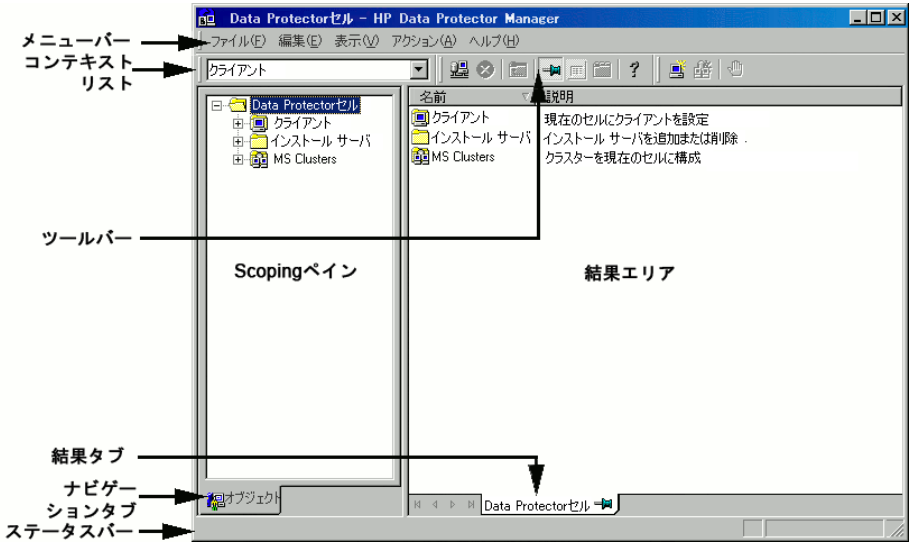


図 1 Data Protectorグラフィカルユーザーインタフェース

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/support/manuals
- http://h20230.www2.hp.com/selfsolve/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。

- **バックアップ オブジェクト操作**

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

- **復元の容易性**

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

- **自動または無人処理**

  Data Protectorでは、内部データベースを使用して、Data Protectorメディアに関する情報と、それぞれのメディア上に保存されているデータに関する情報を管理しています。Data Protectorには高度なメディア管理機能が備わっています。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（39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。

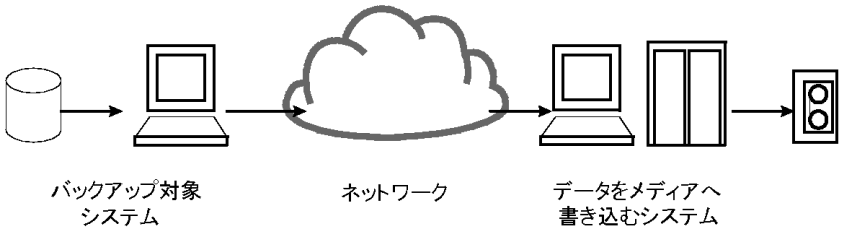


図 4 ネットワーク バックアップ

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(42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。

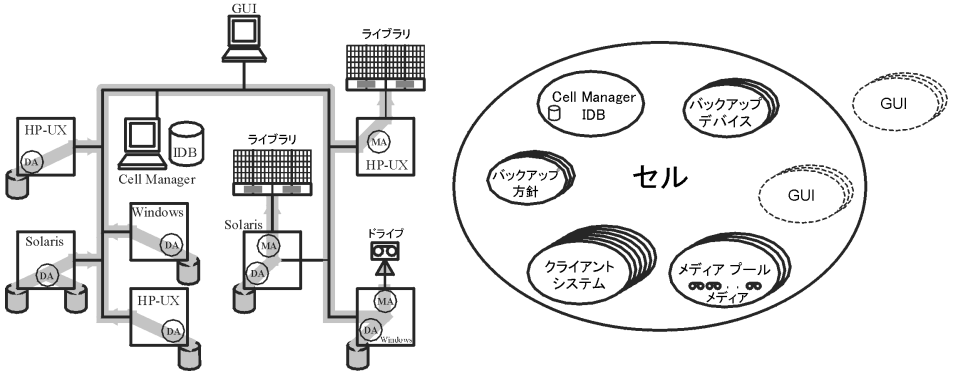


図 5 Data Protectorセル (物理的な構成図と論理的な構成図)

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 (44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。

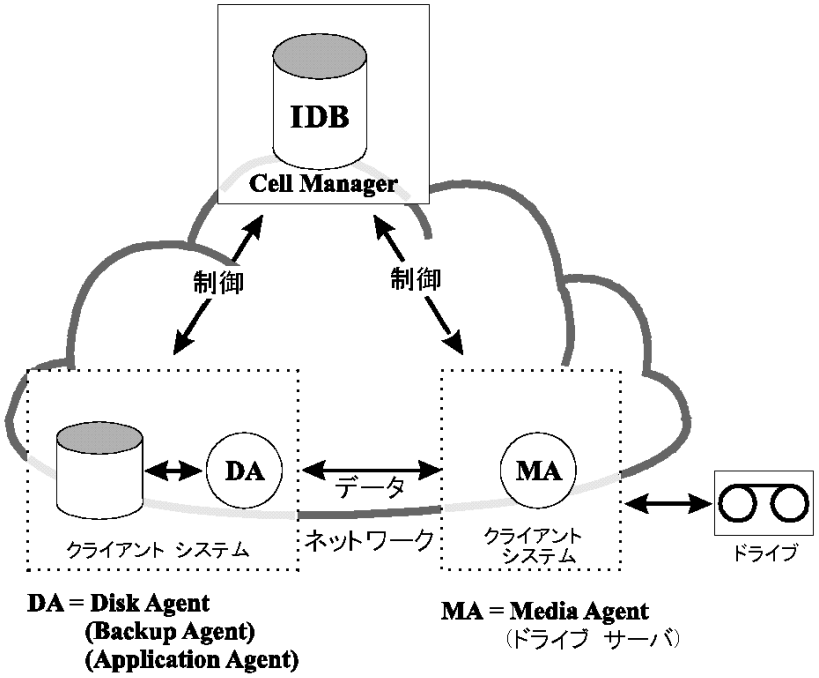


図 6 バックアップ処理および復元処理

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 (45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(45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(229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(45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(45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(229ページ)を参照してください。

企業環境

企業環境とは

図9(46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。

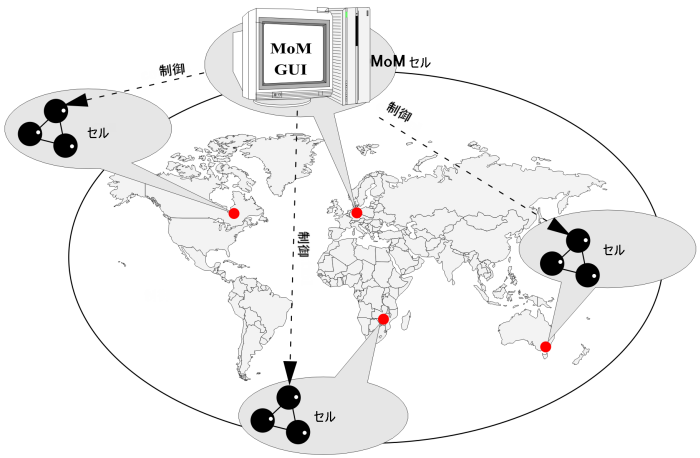


図 9 世界規模のData Protector企業環境

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(47ページ)を参照してください。

環境内を複数セルに分割する

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

分割が必要となる場合

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

環境計画時の留意事項の一覧は、第2章(59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。

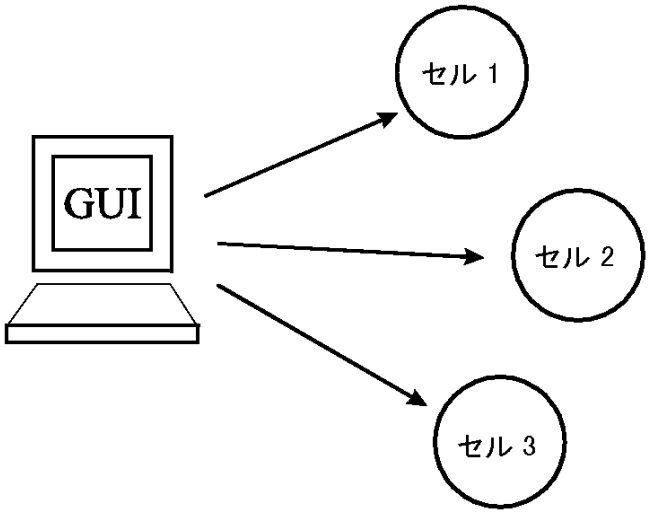


図 10 複数セルを一元管理

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(47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。

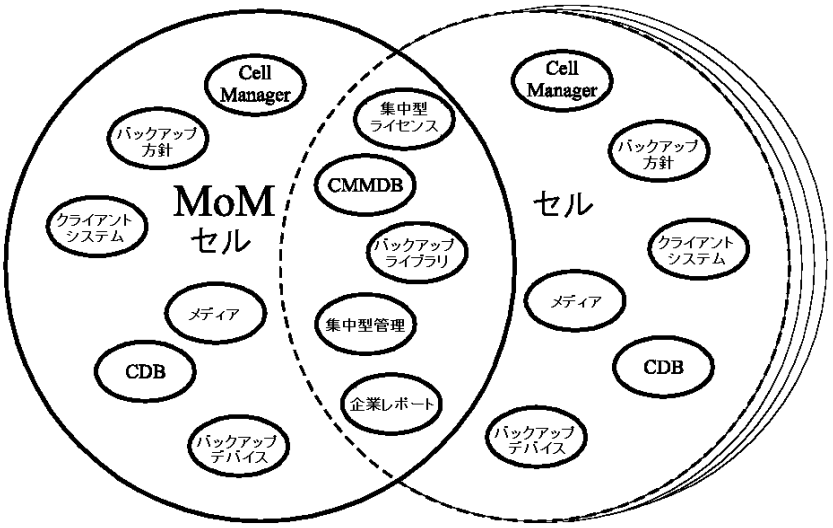


図 11 Manager-of-Managers環境

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。

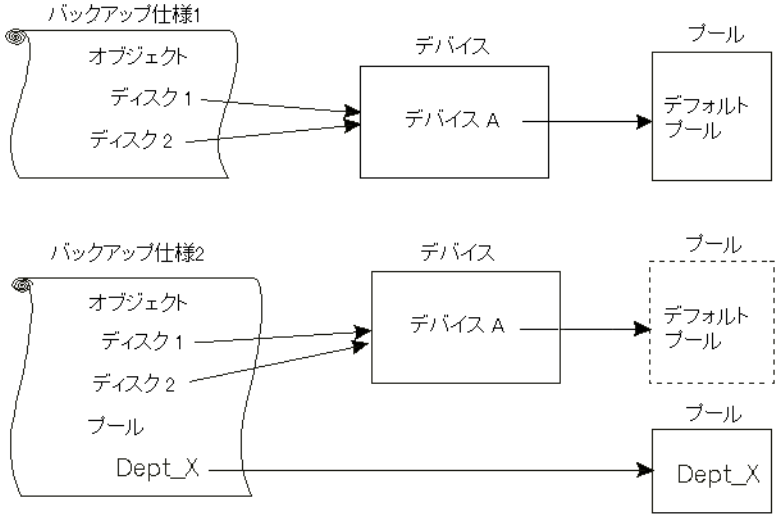


図 12 バックアップ仕様、デバイス、およびメディア プールの関連

図12(50ページ)は、バックアップ仕様、デバイス、およびメディア プールの関連を示したものです。各デバイスは、バックアップ仕様の中で指定されています。各デバイスはメディア プールにリンクされており、バックアップ仕様でこのメディア プールを変更することも可能です。例えば上図のバックアップ仕様2は、デフォルト プールではなくDept_Xプールを参照しています。

Data Protectorは、多種多様なデバイスをサポートしています。詳細は、『*HP 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(51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。

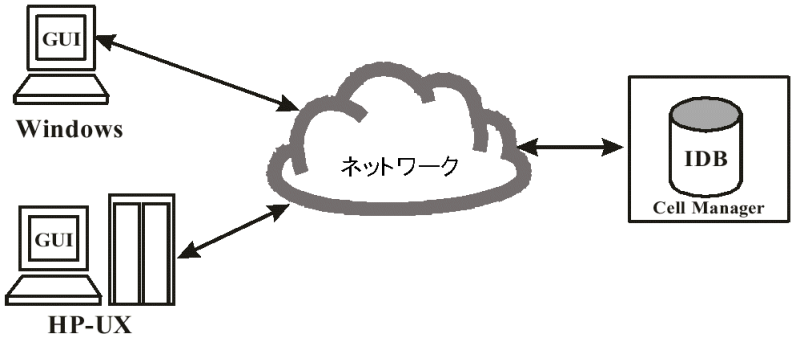


図 13 Data Protectorユーザー インターフェースの使用

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(53ページ)に示すオリジナルのData Protector GUIおよび図15(53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。

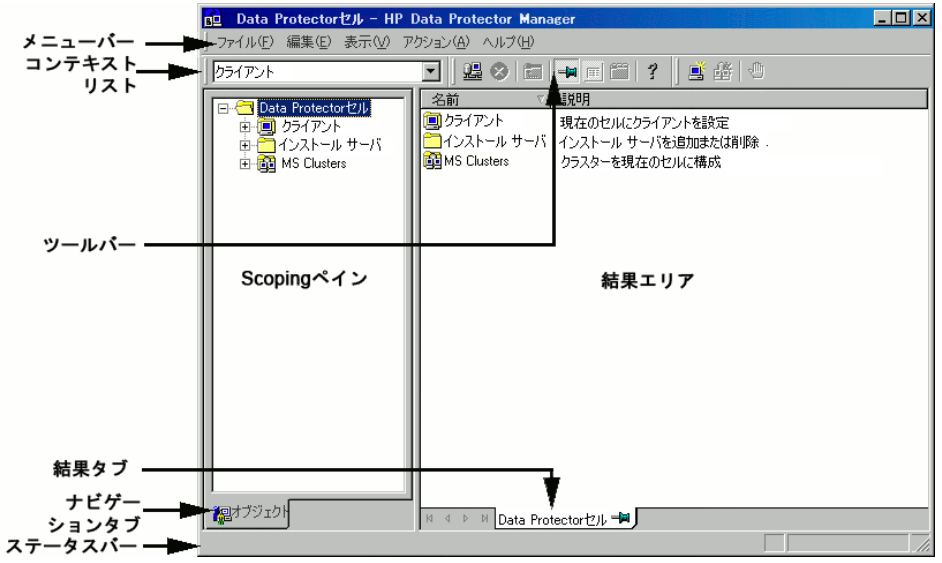


図 14 オリジナルのData Protector GUI

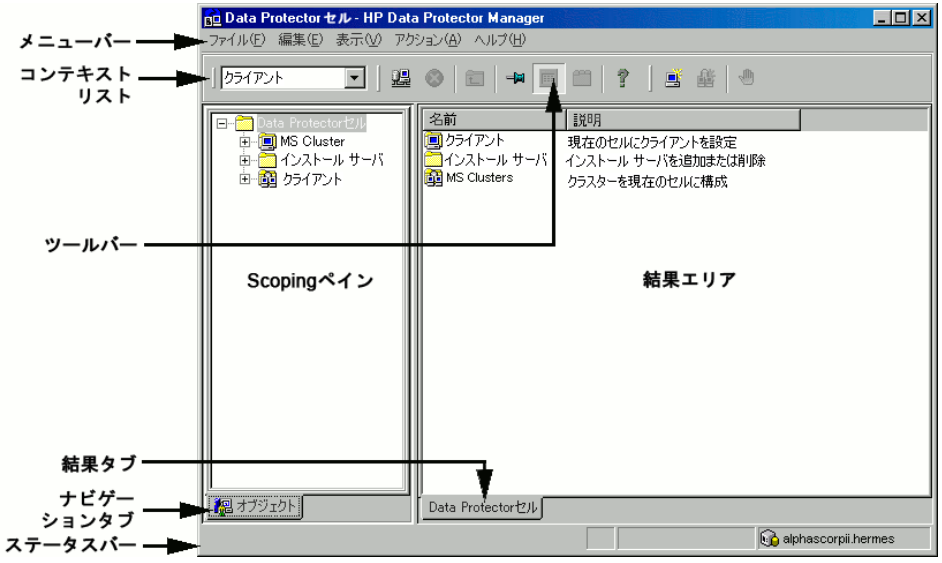


図 15 Data Protector Java GUI

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（54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。

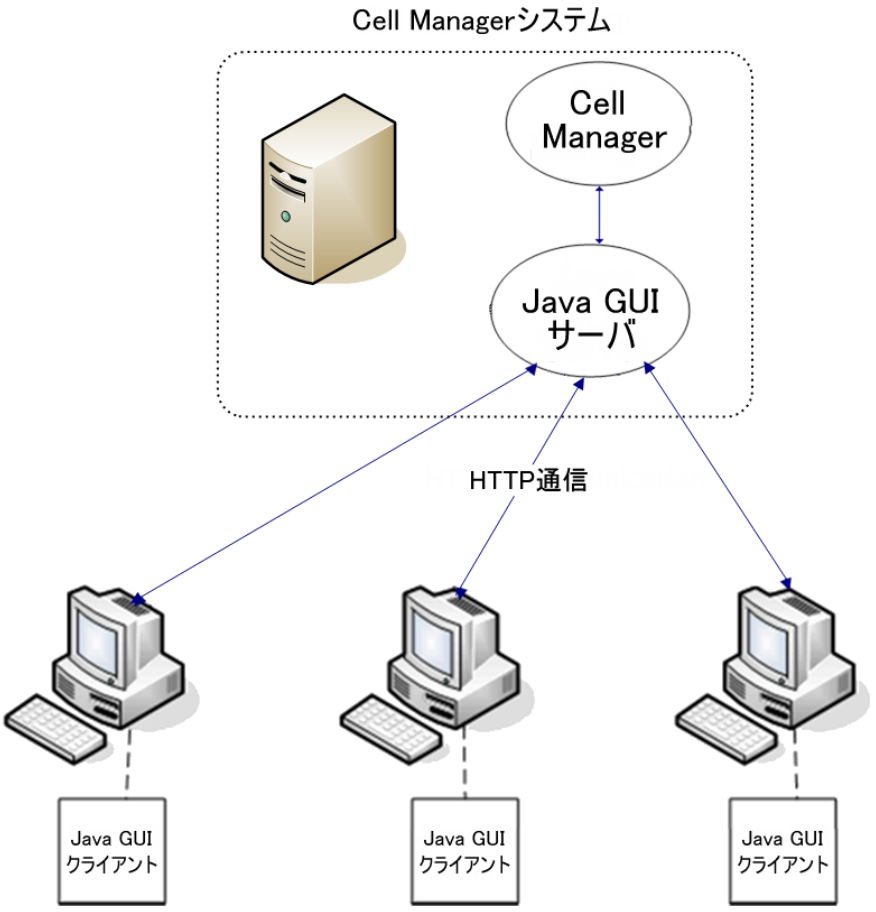


図 16 Data Protector Java GUIのアーキテクチャ

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、クラスター化、および障害復旧方法についても紹介します。

この章の構成は以下のとおりです。

バックアップ方針の策定

Data Protectorの構成および管理は容易ですが、多数の異なるクライアントシステムを使用する大規模な環境で、大容量のデータをバックアップするような場合には、事前に適

切な設計を行っておくことが大切になります。設計段階を確実に行っておくことで、以降の構成作業が容易になります。

バックアップ方針の策定とは

バックアップ方針の策定手順は、以下のとおりです。

1. データのバックアップ頻度や、バックアップデータを別のメディアセットに追加コピーする必要があるかどうかなど、バックアップに関する要件と制約事項を明らかにします。
2. ネットワークやバックアップデバイスにおける定常データ転送速度など、バックアップソリューションに影響を与える要因を明らかにします。これらの要因は、Data Protectorの構成方法や実行するバックアップの種類(ネットワーク経由のバックアップやダイレクトバックアップなど)の選択に影響する可能性があります。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サーバー、大容量リレーショナルデータベースなど)。

- 復旧までに許される最大ダウンタイム

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

タベース内のビジネスデータは2時間以内に復旧しなければならない、といった状況が考えられます。

復旧までの時間は、主として、メディアにアクセスするための時間と、ディスク上に実際にデータを復元するための時間に分かれます。完全なシステム復旧を行う場合は、より多くの手順が必要となるため、さらに多くの時間がかかります。詳細は、「障害復旧」(137ページ)を参照してください。

- 各タイプのデータの保管期間

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

- バックアップデータを保存したメディアの保管方法

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

- バックアップ時にデータを書き込むメディアセットの総数

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

- バックアップするデータの総量

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

- データ総量の将来における増加率

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

- バックアップに要する時間

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

  またバックアップに要する時間は、実行するバックアップのタイプ、つまりフルバックアップを実行するか、増分バックアップを実行するかによっても異なります。詳細は、

「フルバックアップと増分バックアップ」(94ページ)を参照してください。さらにData Protectorでは、一般に使われている大部分のオンラインデータベースアプリケーションに対してバックアップを実行することもできます。詳細は、『*HP Data Protector インテグレーションガイド*』を参照してください。

ディスクにバックアップする場合は、合成バックアップとディスクステージングを活用することができます。これらの高度なバックアップ戦略により、バックアップに要する時間を大幅に短縮できます。詳細については、第11章(273ページ)およびディスクステージング(124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。たとえば、ユーザーの作業ファイルは1日に1回バックアップし、システムデータは週に1回だけバックアップし、一部のデータベーストランザクションについては1日に2回バックアップするといった方法が考えられます。

バックアップ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。たとえば管理対象が複数のグループに分かれているような環境では、デー

タセキュリティ上の理由により、これらのグループを1つのセル内にはまとめたくない可能性があります。一方、複数セルに分割した場合の問題点としては、単一セルの場合に比べて管理作業が煩雑になり、場合によっては各セルごとに専用の管理者を設ける必要があるといった点が挙げられます。

- セルのサイズ

  Data Protectorセルのサイズは、バックアップ性能およびセルの管理能力に影響を与えます。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。ネットワーク構成などのその他のネットワークに関する詳細は、以下の項を参照してください。

- 地理的な配置

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

- 時間帯

  1つのセル内が、複数の時間帯に分かれてはいけません。

- データのセキュリティ

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

- 混合環境

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

- 部門とサイト

  各部門またはサイトごとに、それぞれ個別のセルを設定することも可能です。たとえば、経理部門、IT部門、製造部門別に、それぞれ専用のセルを設定できます。Data

Protectorを使用すると、このように環境内を複数セルに分割した場合であっても、これらのセル間で共通のバックアップ方針を簡単に構成できます。

クライアントシステムのインストールと保守

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

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、削除などにかかる時間を大幅に短縮できることです。

ソフトウェアのインストールを実際に開始する前に、まず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。たとえばソフトウェアを配布するには、そのソフトウェアをインストールするすべてのシステムに、個々にログオンしなければなりません。つまり、ワークグループ環境で100台のシステムにインストールするためには、ログオン作業を100回繰り返す必要があります。このような場合には、ドメイン環境を選択する方が、インストール作業だけでなく、Data Protectorに関連しないその他の管理作業もかなり容易になるはずです。

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

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

混合環境でのセルの作成

混合環境では、「UNIX環境でのセルの作成」(67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。詳細は、「環境内を複数セルに分割する」(46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

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

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

性能に関する概要と計画上の注意点

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

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

インフラストラクチャ

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

ネットワークバックアップとローカルバックアップ

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

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

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

ネットワークバックアップまたはサーバー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ー経由でデータを送信する場合は、新たなオーバーヘッドが生じるため、ネットワークやサーバー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。たとえば、system_Aにバックアップ対象のオブジェクト(ディスク)が6個あり、system_Bに高速テープデバイスが3台ある場合は、system_Aとsystem_Bとの間で3つのネットワークリンクをバックアップ専用にします。
- 負荷調整

  これはData Protectorの機能であり、どのオブジェクト(ディスク)をどのデバイスにバックアップするかがData Protectorによって動的に決定されます。特に、動的環境において多数のファイルシステムをバックアップする場合は、この機能をオンに設定してください。詳細については、「負荷調整の仕組み」(164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ーから元のデータを受信し、受信したデータを圧縮モードでメディアに書き込みます。ハードウェ

ア圧縮を使うと、テープに書き込まれるデータのサイズが小さくなり、テープドライブがデータを受信する速度が向上します。

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

フルバックアップと増分バックアップ

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

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

ディスクイメージバックアップとファイルシステムバックアップ

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

メディアへのオブジェクトの配布

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

- 1つのオブジェクト(ディスク)を1つのメディアに格納。

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

  一方、ネットワークバックアップを行う場合にこの方法を使用すると、ネットワークが原因で性能が制限されるため、デバイス ストリームを維持できない可能性があります。

- 多数のオブジェクトを複数のメディアに格納。1つのメディアには複数のオブジェクトが保存されるが、1つのオブジェクトは必ず1つのデバイスで処理されます。

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

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

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

デバイスストリーミングとバックアップの同時処理数の詳細については、「デバイスストリーミングと同時処理数」(165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(たとえば整合性のとれたバックアップを作成するために、アプリケーションを終了させるなど)。

Data Protectorのユーザーアカウント

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

ユーザーアカウントの設定者

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

アカウントチェックのタイミング

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

詳細は、第4章(191ページ)を参照してください。

Data Protectorユーザーグループ

ユーザーグループとは

新しいユーザーアカウントの作成時には、そのユーザーが所属するユーザーグループも指定されます。個々のユーザーグループに対しては、それぞれ複数のData Protector

ユーザー権限が与えられています。グループのメンバーとなったユーザーは、そのグループのユーザー権限が与えられます。

ユーザーグループが必要な理由

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

詳細は、第4章(191ページ)を参照してください。

Data Protectorユーザー権限

ユーザー権限とは

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

ユーザー権限が必要な理由

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

詳細は、第4章(191ページ)を参照してください。

バックアップデータの表示

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

他のユーザーからデータを隠す

バックアップの構成時には、そのデータを誰でも復元できるようにするか(public)、またはバックアップデータのオーナーしか復元できないようにするか(private)を指定できます。

バックアップ オーナーの詳細については、「バックアップ所有権とは」(81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のキーストアファイルに一元的に保存され、KMSによって管理されます。

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

また、Data Protectorでは暗号化機能のほかに、この目的で使用できる組み込み型のアルゴリズム(キーなし)を使用する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(80ページ)では、[**AES 256-bit**]暗号化オプションが選択されていて暗号化が行われるバックアップセッションの際の、基本的なやり取りを表しています。

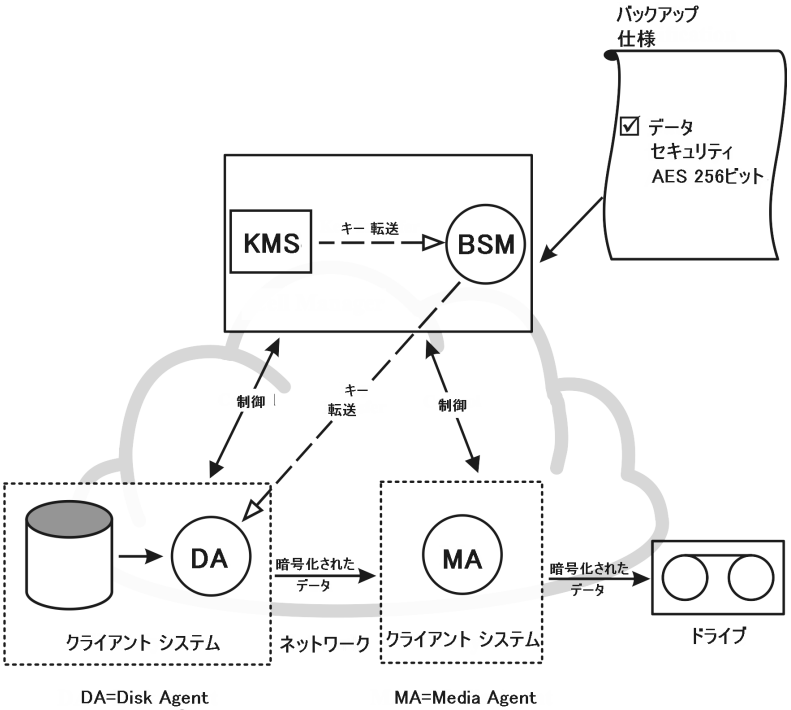


図 17 AES 256ビット暗号化を指定したバックアップセッション

Data Protectorでのドライブベースの暗号化機能の仕組み

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

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

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

図18 (81ページ)は、[**AES 256ビット**]暗号化オプションと[**ドライブベースの暗号化**]オプションを選択した場合の暗号化されたバックアップセッション時における基本的なやり取りを示します。

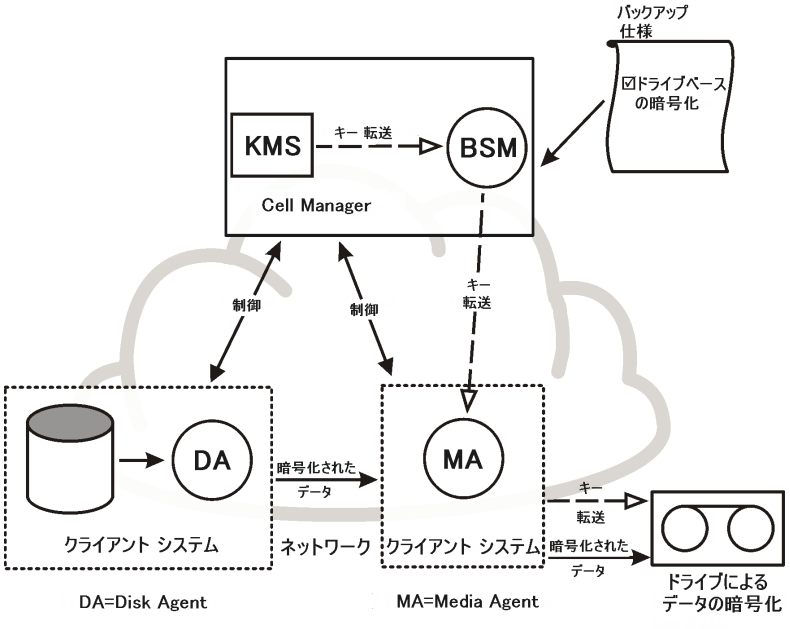


図 18 AES 256ビット暗号化とドライブベース暗号化が指定されたバックアップセッション

暗号化されたバックアップからの復元

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

バックアップ所有権とは

誰がバックアップセッションを所有するのか

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

バックアップ所有権と復元

バックアップ所有権は、データを参照および復元するユーザーの能力に影響します。オブジェクトがパブリックに設定されていない場合、そのメディアセット内に保存されているデータは、メディアセットのオーナーまたは管理者しか見ることができません。プライベー

トオブジェクトを参照および復元する権限は、*admin*以外のグループにも与えることができます。プライベートオブジェクトの参照および復元が可能なユーザーについては、オンラインヘルプの索引「所有権」を参照してください。

クラスタリング

クラスターの概念

クラスターとは

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

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

Data Protectorではクラスター化を実現するために、Windows Server用のMicrosoft Cluster Server、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。サポート対象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。

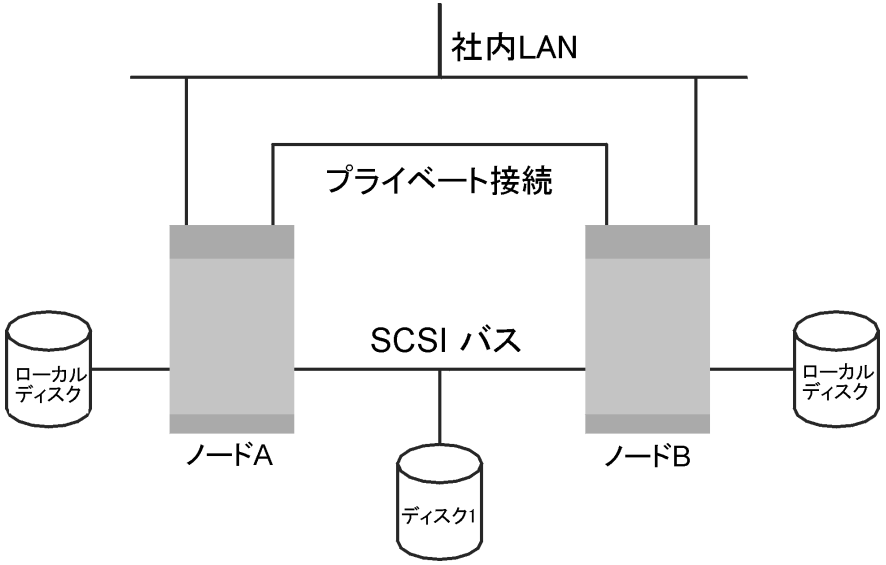


図 19 代表的なクラスター

構成要素

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

クラスターノード

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

共有ディスク

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

クラスターネットワーク

クラスターネットワークは、すべてのクラスターノードを接続するプライベートネットワークです。このネットワークにより、**クラスターのハートビート**と呼ばれる内部的なクラスターデータが転送されます。ハートビートとはタイムスタンプ付きのデータパケットで、すべてのクラ

スターノードに配布されます。各クラスターノードでは、このパケットを比較することによりどのクラスターノードが現在稼動中であるかを判断します。これにより、**パッケージ**(MC/SGまたはVeritas Clusterの場合)または**グループ**(MSCSの場合)の適切な所有権を決定できます。

パッケージまたはグループとは

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

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

仮想サーバーとは

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

フェイルオーバーとは

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

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

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

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

Data Protector Cell Managerの高可用性の実現

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

バックアップの自動再開

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

フェイルオーバー時の負荷調整

Data Protector以外のアプリケーションがフェイルオーバーを実行した場合に、バックアップセッションを中止する特殊なコマンド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。基準の定義方法については、オンラインヘルプの索引「クラスター、バックアップの管理」を参照してください。

クラスターのサポート

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

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

注記:

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

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

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

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

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

クラスター環境の例

この項では、3つのクラスター構成例を示します。

Cell Manager がクラスター外部にインストールされている構成

下図の環境には以下のような特徴があります。

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

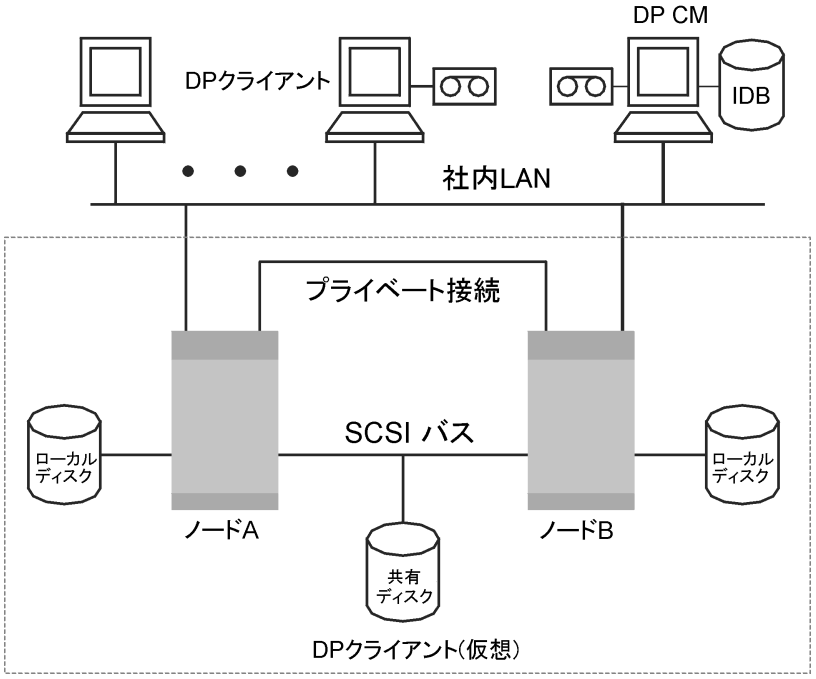


図 20 Cell Manager がクラスター外部にインストールされている構成

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

- 物理ノードA
- 物理ノードB
- 仮想サーバー

仮想サーバーのバックアップ

バックアップ仕様で仮想サーバーを選択した場合のバックアップセッションでは、パッケージまたはグループが現在どの物理ノードで稼動している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、オンラインヘルプの索引「クラスター、バックアップ仕様オプション」を参照してください。

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

下図の環境には以下のような特徴があります。

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

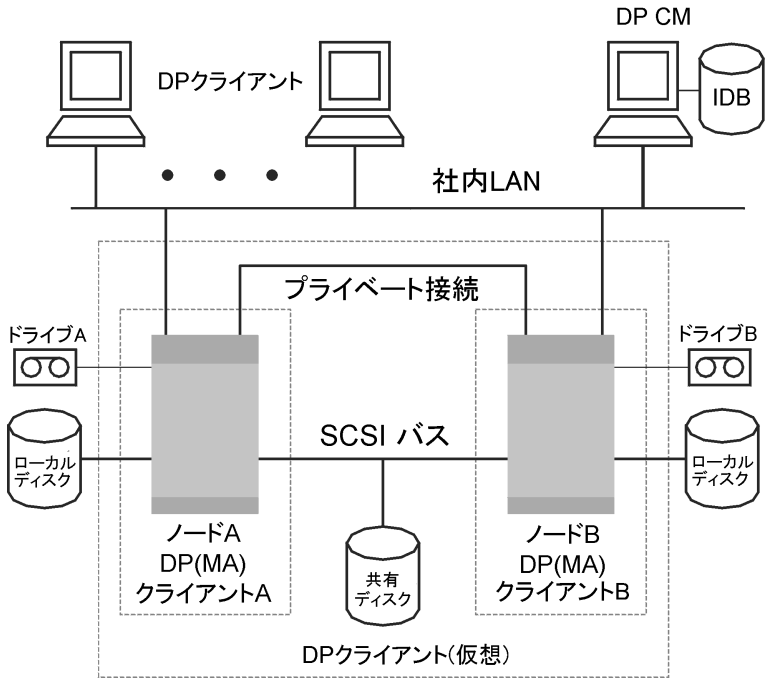


図 21 Cell Manager がクラスター外部にインストールされ、デバイスがクラスターノードに接続されている構成

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

- 物理ノードA
- 物理ノードB
- 仮想サーバー

仮想サーバーのバックアップ

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

注記:

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

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

下図の環境には以下のような特徴があります。

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

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

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

重要:

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

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

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

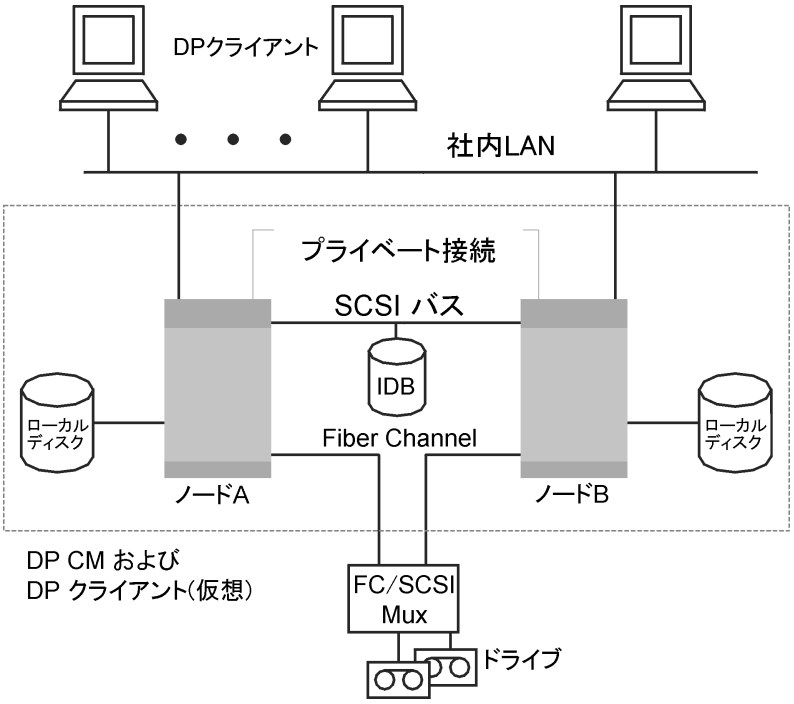


図 22 Cell Managerがクラスター内部にインストールされ、デバイスがクラスターノードに接続されている構成

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

- 物理ノードA
- 物理ノードB
- 仮想サーバー

仮想サーバーのバックアップ

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

注記:

クラスターでは、共有テープにSCSIバスを使用できません。Media Agentについても高可用性を実現するには、デバイスとのインタフェースにFibre Channelテクノロジを使用してください。この構成では、デバイスそのものは高可用性構成にはなっていません。

この構成では、以下の機能が提供されます。

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

  Data Protectorでは、Cell Managerのフェイルオーバーが発生した場合にバックアップを再開するよう、バックアップ仕様を構成できます。再開に関するパラメータを定義するには、Data ProtectorのGUIを使用します。

- フェイルオーバー発生時のシステム負荷を制御できます。

  高度な制御機能により、フェイルオーバー発生時におけるData Protectorの動作を定義することも可能です。この処理には、専用のomniclusを使用します。管理者は、フェイルオーバー発生時に実行すべき処理内容を、Cell Managerを使用して、以下のように定義できます。

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

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

<table>
<tr><th>条件</th><th colspan="2">結果</th></tr>
<tr><td rowspan="2">バックアップ中に、アプリケーションとCell Managerのフェイルオーバーが発生した場合(Cell Managerとアプリケーションは同じノード上で実行)。</td><td>ファイルシステム/ディスクイメージのバックアップバックアップセッションが失敗します。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。</td><td rowspan="2">重要
セッションを再開するには、適切なData Protectorオプションを選択することが必要です。Cell Managerのフェイルオーバーが発生したときの考えられるすべてのData Protectorアクションの定義の詳細については、オンラインヘルプの索引「クラスター、バックアップの管理」を参照してください。</td></tr>
<tr><td>アプリケーションのバックアップバックアップセッションが失敗します。セッションは自動的に再開されます。</td></tr>
<tr><td rowspan="2">バックアップ中に、アプリケーションのフェイルオーバーが発生したが、Cell Manager自体のフェイルオーバーは発生していない場合(Cell Managerはアプリケーションとは別のノード上で実行)。</td><td colspan="2">ファイルシステム/ディスクイメージのバックアップファイルシステムがインストールされているノードがフェイルオーバーすると、バックアップセッションが失敗します。このセッションでバックアップが完了しているオブジェクトは復元に使用できますが、失敗したオブジェクト(実行中および保留中)については、セッションを手動で再開してもう一度バックアップする必要があります。</td></tr>
<tr><td colspan="2">アプリケーションのバックアップバックアップセッションが失敗します。セッションを手動で再開する必要があります。</td></tr>
</table>

重要:

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

またData Protectorクラスターの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。たとえばSybaseでは、この種のバックアップはトランザクションバックアップと呼ばれ、最後のバックアップ以降に変更されたトランザクションログのみがバックアップされます。

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

注記:

Data Protectorのアプリケーション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*』を個別に参照してください。

フルバックアップ

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

合成バックアップ

合成バックアップは、通常のフルバックアップを実行する必要のない高度なバックアップソリューションです。代わりに、増分バックアップが実行され、続いてそれがフルバックアップとマージされると、新規合成フルバックアップとなります。詳細については、第11章(273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(98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(98ページ)に示すとおり、まだ保護期限が切れていない、1つ下のレベルの前回の複数レベル増分バックアップをベースとして行われます。たとえば増分1バックアップを実行すると、前回のフルバックアップ時より後に更新された、すべてのデータが保存されます。 また、増分5バックアップを実行すると、前回の増分4バックアップより後に更新されたすべてのデータが保存されます(増分4バックアップが存在する場合)。増分1～9バックアップでは、既存の増分バックアップは参照されません。

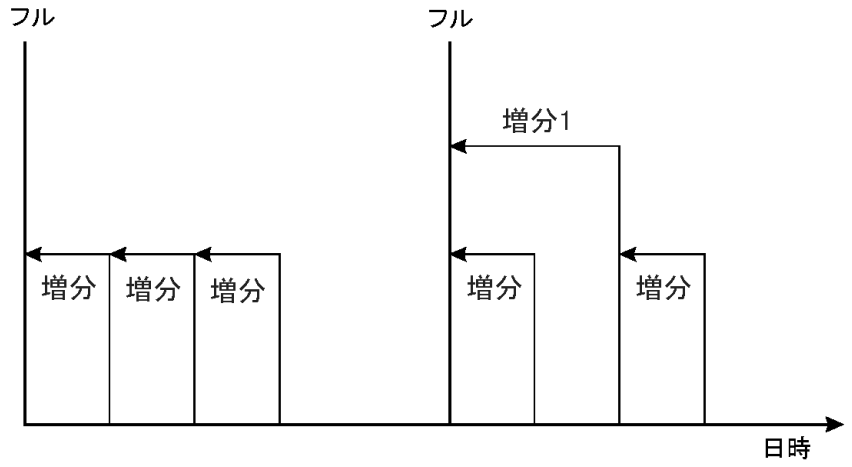


図 23 増分バックアップ

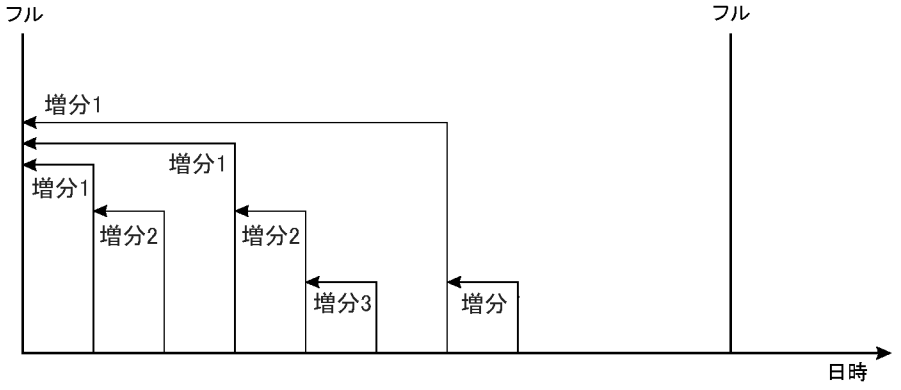


図 24 複数レベル増分バックアップ

表7 (98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(98ページ)の見方

- 表7(98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（101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（102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。

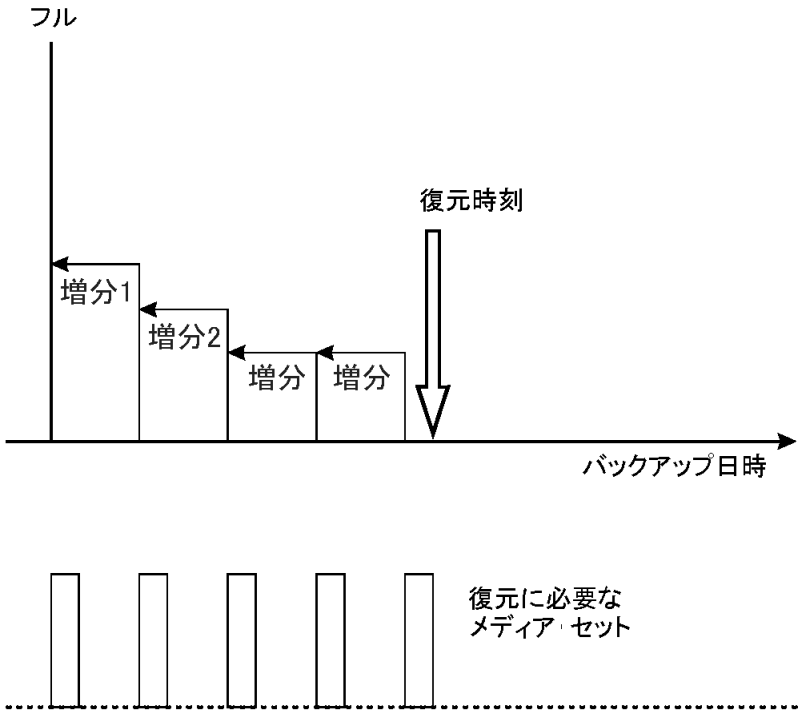


図 25 簡易および複数レベルの増分バックアップからの復元時に必要となるメディア

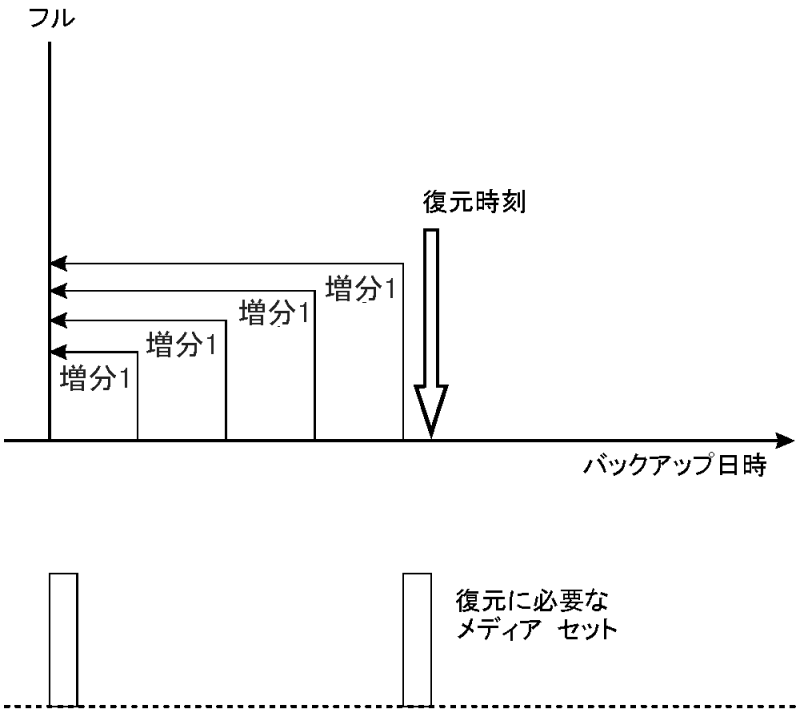


図 26 複数レベルの増分バックアップからの復元時に必要となるメディア

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。詳細は、付録B(349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。たとえば、バックアップ後4週間は簡単かつ高速に復元処理を行えるようにカタログ保護期間を4週間に設定しておきます。それ以降、データ保護の有効期限が切れるまでの1年間程度は、多少手間はかかるにしても、復元処理自体の実行は可能になります。このように工夫することで、IDB上のスペースを削減できます。

データ保護

データ保護とは

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

Data Protectorでは、さまざまな場所でデータ保護の設定を行うことができます。詳細は、オンラインヘルプの索引「データ保護」を参照してください。

バックアップの構成時に、バックアップオプション[**データ保護**(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」(211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(349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」(209ページ)を参照してください。

復元するファイルのブラウズ

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

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

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

ファイルのブラウズとすばやい復元が可能な場合

ファイルをすばやく復元するためには、メディア上に保護されたデータが存在し、かつバックアップデータに関するカタログ情報がデータベース内に存在していなければなりません。カタログ情報がある場合は、Data Protectorユーザーインタフェースを使用して、復元するファイルのブラウズや選択、復元処理の開始などを実行できるため、Data Protector

により、バックアップメディアに格納されているデータをすばやく見つけ出すことができます。

ファイルのブラウズはできないが復元は可能な場合

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

新しいデータによるバックアップファイルの上書き

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

ヒント:

データ保護の有効期限には、そのデータを本当に保存しておく必要がある期間を指定してください(1年など)。

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

セルからのメディアのエクスポート

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

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

データのバックアップ

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

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

バックアップ仕様では、これらの項目をすべて指定できます。

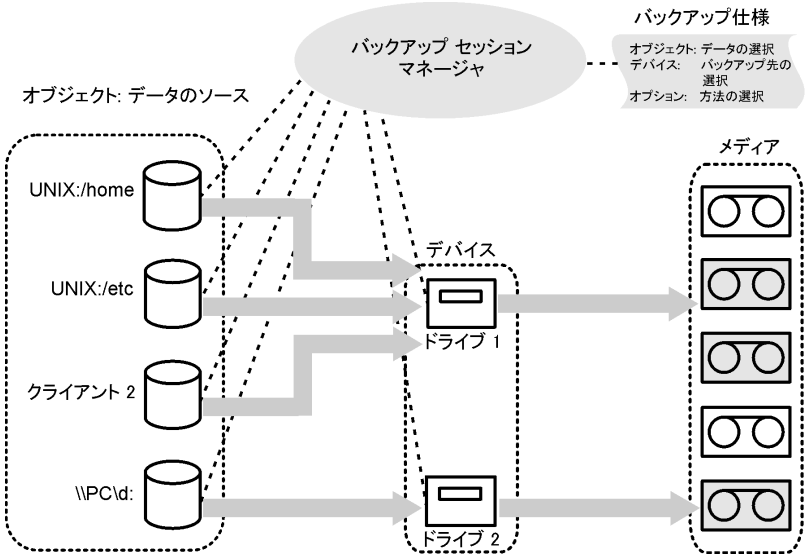


図 27 バックアップセッション

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。Aバックアップ仕様では、1つ

のディスクをスタンドアロンのDDSドライブにバックアップするといった単純な設定もできれば、40台の大規模サーバーを、8台のドライブを搭載したサイロテープライブラリにバックアップするといった複雑な設定も可能です。

バックアップ設定の作成

バックアップ仕様とは

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

バックアップ仕様の作成方法

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

Data Protectorでは、対象となるクライアントに接続されているすべてのディスクをバックアップ時に検出して、バックアップすることも可能です。(「ディスクディスカバリバックアップ」(236ページ)を参照)。

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

バックアップオプションの例

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

- IDBに記録するログ情報のレベル

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

  - [すべてログに記録(Log All)]
  - [ファイルレベルまでログに記録(Log Files)]
  - [ディレクトリレベルまでログに記録(Log Directories)]
  - [記録しない(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」(209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」(164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」(234ページ)を参照してください。

- データセキュリティ

  データに適用するセキュリティのレベル。

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

  - なし

- AES 256-ビット
- エンコード

暗号化の詳細については、「「データの暗号化」(79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(229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」(126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(95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。(「フルバックアップの時差実行」(112ページ)を参照)。

スケジュール設定、バックアップ構成、およびセッション

バックアップ構成

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

単独で、または定期的に実行されるようにスケジュールされたバックアップでは、[**バックアップの種類**](フルまたは増分)、[**ネットワーク負荷**]、[**バックアップ保護**]の各オプションを指定できます。また、スプリットミラーバックアップまたはスナップショットバックアップで、ディスクへのZDBまたはディスク+テープへのZDB(インスタントリカバリに対応)を実行する場合は、**スプリットミラー/スナップショットバックアップ** オプションを指定します。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」(94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」(102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」(112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（113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。

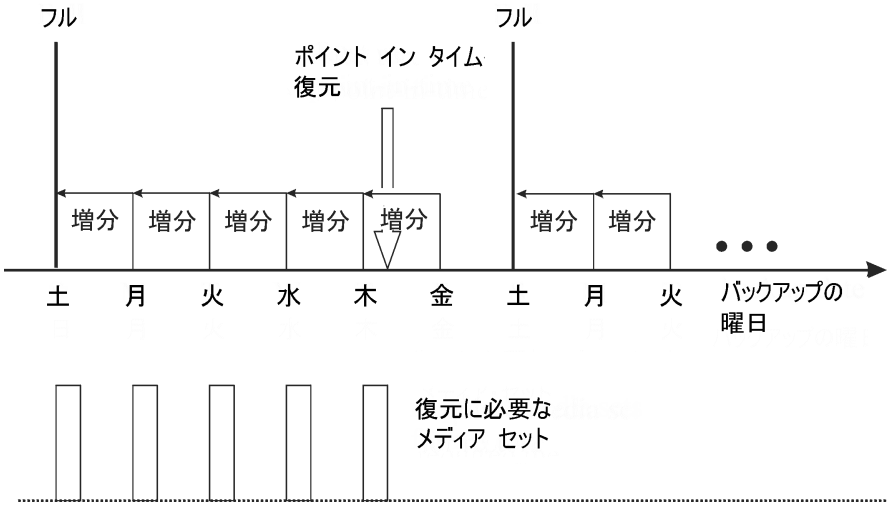


図 28 フルバックアップと1日1回の簡易増分バックアップを実行

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、たとえば木曜日のバックアップからファイルを復元するような場合には、フルバックアップと木曜日までの増分バックアップが必要になるため、合計5つのメディアセットが必要です。このため、復元の手順が複雑になり、時間がかかります。

例2

図29 (114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。

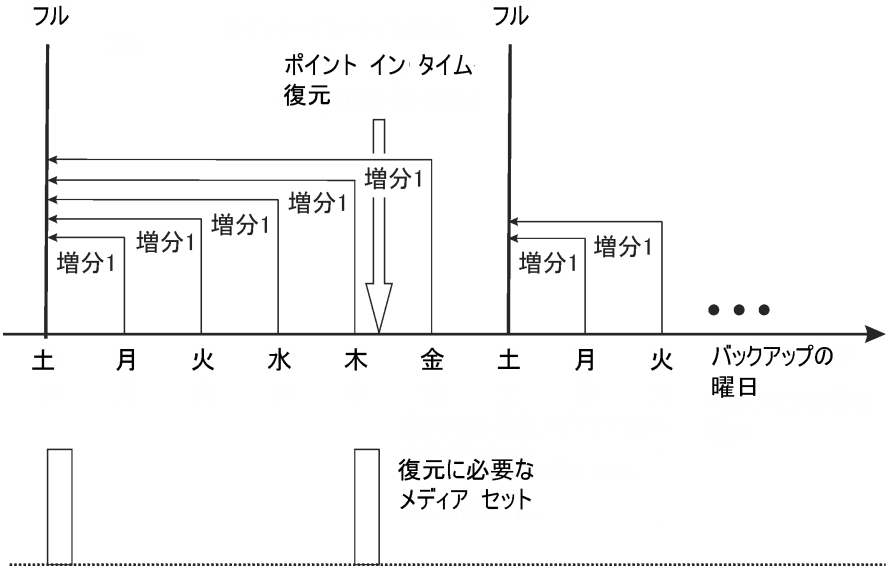


図 29 フルバックアップと1日1回のレベル1増分バックアップ

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、たとえば木曜日のバックアップからファイルを復元するには、フルバックアップと木曜日の増分バックアップしか必要ないため、合計2つのメディアセットのみが必要となります。これにより、復元が大幅に簡略化され、時間も大きく短縮されます。

例3

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

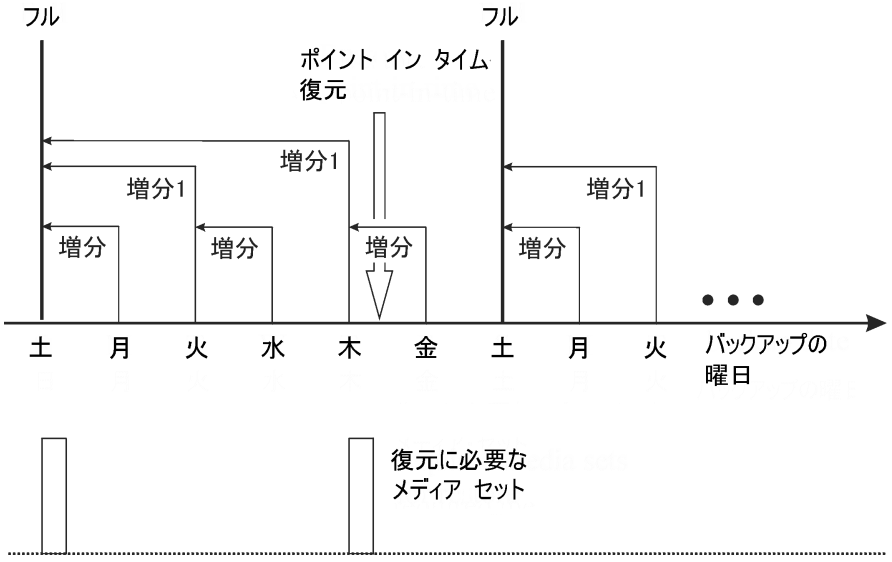


図 30 フルバックアップと2通りの増分バックアップ

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、たとえば木曜日のバックアップからファイルを復元するには、フルバックアップと2番目の増分1バックアップの合計2つのメディアセットのみを用意すればよいことになります。

自動または無人処理

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

無人バックアップの注意点

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

- システム使用率とユーザー活動が最小になるのはいつか。

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

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

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

- 復元処理の容易性は、どの程度重要か。

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

- バックアップするデータの量はどの程度か。

  フルバックアップは増分バックアップよりも時間がかかります。また一般にバックアップ処理は、限られた時間枠内で実行する必要があります。

- どれくらいの量のメディアが必要か。

  メディア交換方針を決定します。(「メディア交換方針の実装」(151ページ)を参照)。ここでは、対象ライブラリ内に十分な数のメディアを用意しておくことにより、バックアップ時に手動でメディア交換を行わずに済ませる方法について説明しています。

- どのようにマウントプロンプトに対応するか

  ライブラリを使用するかどうかを決定します。ライブラリを使用すると、自動処理が可能となります。これは、Data Protectorから、すべてのメディア、または大部分のメディアに対するアクセスが可能となり、メディアを手動で処理する必要がほとんどなくなるためです。データ量が非常に多く、1台のライブラリでは対処しきれない場合は、ライブラリの追加も検討する必要があります。詳細は、「大容量ライブラリ」(171ページ)を参照してください。

- デバイスが使用できない場合の対応をどうするか。

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

- すべてのデータのバックアップにはどれくらいの時間が必要か。

  バックアップ作業は、ネットワークの使用率が低く、ユーザーがシステムを使用しない時間帯に実行しなければなりません。 そのため、バックアップのスケジュール設定を

適切に行って、バックアップによるネットワーク負荷を分散させ、バックアップセッションの効率を最大化することが大切になります。場合によっては、時差実行方式の採用も検討してください。

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

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

バックアップデータの複製

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

Data Protectorには、バックアップされたデータの複製方法(オブジェクトコピー、オブジェクトミラー、メディアコピー)が用意されています。これらの機能の主な特徴に関して、表9 (117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、オブジェクトコピー、オブジェクト集約セッションで作成される複数のオブジェクトバージョンの組み合せ	バックアップセッション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

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

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

図31(119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。

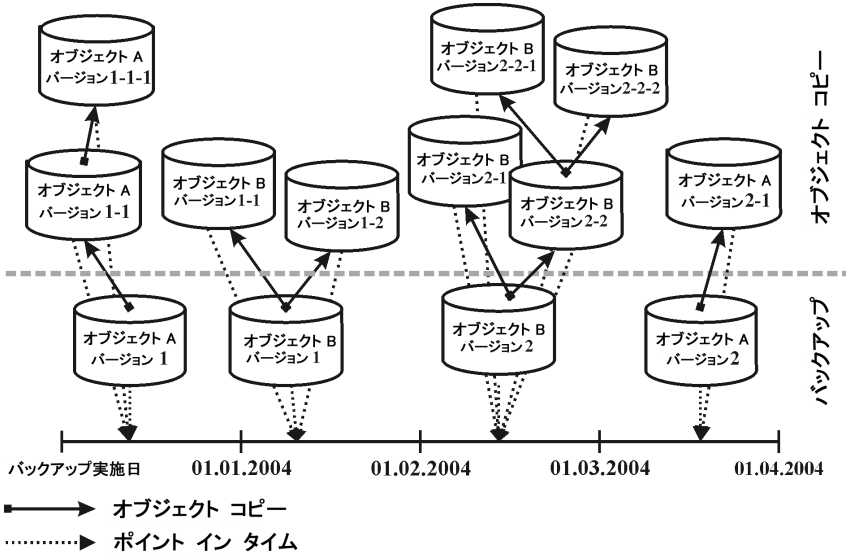


図 31 オブジェクトコピーの概念

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

スケジュール済みのオブジェクトコピー

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

デバイスの選択

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

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

ソースデバイスの選択

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

- デバイスの自動選択(デフォルト):

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

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

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

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

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

- 元のデバイスの選択:

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

あて先デバイスの選択

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

- コピー元デバイスと同じブロックサイズのデバイスが、ブロックサイズが異なるデバイスよりも優先的に選択されます。
- 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」(133ページ)を参照してください。

オブジェクトコピーセッションの性能

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

オブジェクトコピーを使う理由

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

- ボールティング

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

- メディアの解放

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

- メディアのデマルチプレックス

  オブジェクトをコピーして、インタリーブされたデータを削減できます。

- 復元チェーンの統合

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

- 別の種類のメディアへの移動

  異なる種類のメディアにバックアップをコピーできます。

- 拡張バックアップの概念のサポート

  ディスクステージングなどのバックアップ概念を使用できます。

ボールティング

ボールティング 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。詳細は、「ボールティング」(160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(123ページ)を参照)。

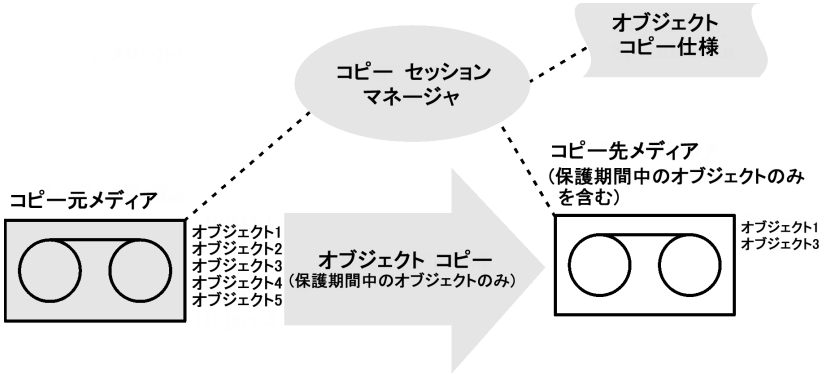


図 32 メディアの解放

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(124ページ)を参照)。

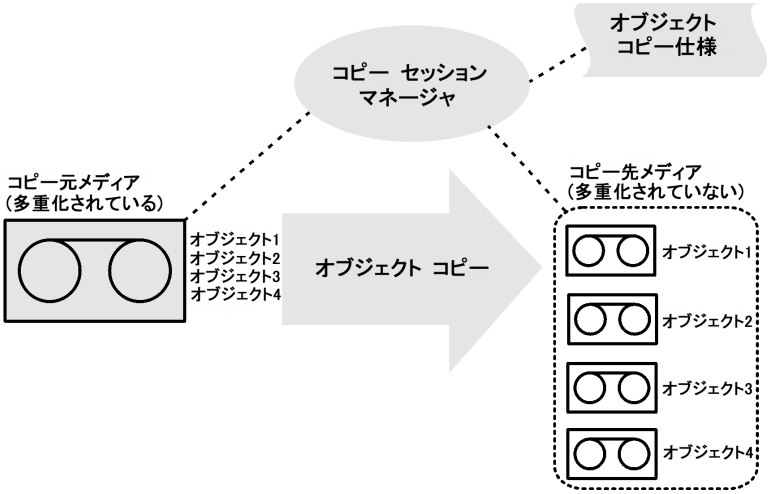


図 33 メディアの多重化(データの断片化)の解消

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

ディスクステージング

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

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

マンスと可用性は低いが大容量の保存用メディアに移動されます。(図34(125ページ)を参照)。

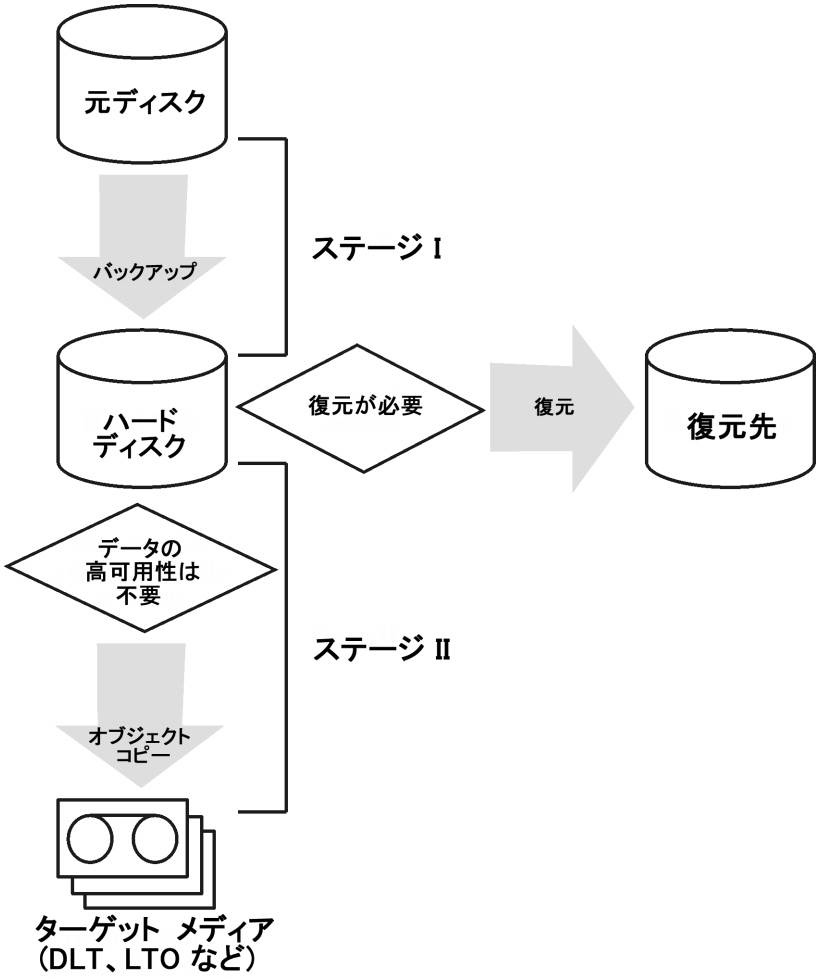


図 34 ディスクステージングの概念

この手順は、自動処理として実行可能です。

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

- 初期バックアップは、ファイルライブラリを使用するディスクに対して実行します。データとカタログの保護は、45日間の全体要件に設定します。

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

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

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(127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。

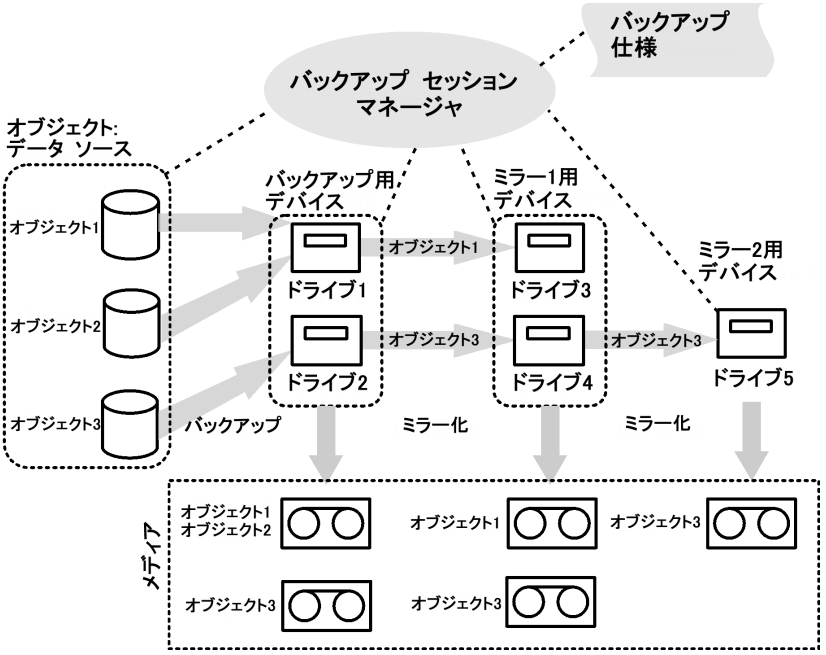


図 35 オブジェクトミラーの作成

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」(130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機能には独自の負荷調整機能が備えられています。Data Protectorはできるだけ多くのデバイスを使用し、また可能であればローカル デバイスを使用することにより、使用可能なデバイスを最大限有効に活用しようとします。

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

使用例については、「自動メディア コピーの例」(350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2種類のスマートメディアコピー機能が用意されています。それは、自動スマートメディアコピーと、対話形式のスマートメディアコピーです。

自動スマートメディアコピー

以下の種類の スマートメディアコピーを作成することができます。

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

対話形式のスマートメディアコピー

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

バックアップ後に行われる処理

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

VLS スマートコピーの詳細については、オンラインヘルプの索引「スマートメディアコピー」とVLSマニュアルを参照してください。

バックアップメディアとバックアップオブジェクトの検証

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

メディアの検証とは

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

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

メディアの検証作業

メディアの検証を実行すると、以下が実行されます。

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

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

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

オブジェクト検証とは

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

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

以下の場合、オブジェクト検証を使用できます。

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

オブジェクト検証作業

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

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

さらに、以下に対して検証を実行できます。

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

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

データの復元

データ復元方針は、各企業の全体的なバックアップ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。詳細は、「フルバックアップと増分バックアップ」(94ページ)を参照してください。
- バックアップに使用したメディアとデバイス。詳細は、第3章(141ページ)を参照してください。
- ネットワークおよびシステムの速度。詳細は、「性能に関する概要と計画上の注意点」(69ページ)を参照してください。
- 復元するアプリケーションの種類(Oracleデータベースファイルなど)。詳細は、各自の環境に適した『*HP Data Protector インテグレーションガイド*』を参照してください。
- 並列復元の使用。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。(「並行復元」(239ページ)を参照)。
- 復元するデータを選択する際の速度と容易さは、バックアップに使用したログレベル設定とカタログ保護期間により異なります。(「IDBの主要な調整可能パラメータとしてのロギングレベル」(209ページ)を参照)。

メディアセットの選択

復元するオブジェクトバージョンが複数のメディアセット上にある場合は、それらがData Protectorのいずれかの複製メソッドで作成されている限り、どのメディアセットを使って復

元処理を行っても構いません。デフォルトでは、使用するメディアセットが自動的に選択されます。メディア位置の優先順位を設定しておくと、このメディアセットの自動選択をある程度まで制御できます。統合オブジェクトを復元する場合を除き、復元に使用するメディアセットを手動で選択することも可能です。

メディアセットの選択アルゴリズム

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

復元チェーンの選択

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

メディア位置の優先順位

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

- デバイスの自動選択(デフォルト):

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

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

使用できないようにするには、グローバル変数AutomaticDeviceSelectionOrderを変更します。

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

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

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

- 元のデバイスの選択:

  Data Protectorは、復元に元のデバイスを使用し、そのデバイスが使用できない場合には待機します。これは、Data ProtectorのSAP DB/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。

復元する権限をオペレータにのみ付与

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

この方針が適している場合

この方針は、以下の場合に適用します。

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

必要な作業

この方針を実施するには、以下の作業が必要になります。

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

  その他のユーザーグループに、新たなユーザー(自分のシステムを復元できるユーザーなど)を追加する必要はありません。

- インストール時に、エンドユーザーのシステム上に、Data Protectorユーザーインタフェースをインストールしないよう注意します。Disk Agentをインストールして、Data Protectorでこれらのシステムをバックアップできるようにします。
- 復元要求に対する対処方針を決定しておきます。この中では、エンドユーザーがファイル復元を要求する場合の手順も明確にしておく必要があります(たとえば復元処理の請求には必ず電子メールを使い、オペレータが目的のファイルを見つけてエンドユーザーのシステム上に復元するために必要となる情報を、すべてこのメール内に記入する、など)。またエンドユーザーに、ファイルが復元されたことを知らせる方法も、取り決めておく必要があります。

復元する権限をエンドユーザーにも付与

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

この方針が適している場合

この方針は、以下の場合に適用します。

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

必要な作業

この方針を実施するには、以下の作業が必要になります。

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

障害復旧

この項では、さまざまな障害復旧の概念について簡単に説明します。詳細な障害復旧の概念、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の障害復旧は、このシステムを元のシステム構成に戻すことを目的としています。影響を受けたシステムとは異なり、ターゲットシステムの場合は、障害が発生したハードウェアはすべて交換されています。

障害の発生は常に重大な問題ですが、以下の要因は状況をさらに深刻化します。

- システムをできる限り迅速かつ効率的にオンライン状態に戻す必要がある。
- 障害復旧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。

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

障害復旧プロセスは4つのフェーズに分けられます。

1. 障害復旧を成功させるには、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。

障害復旧の方法

Data Protectorは、以下の障害復旧の手法をサポートしています。

- 手動による障害復旧

  これは基本的で非常に柔軟な障害復旧の手法です。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。

- 自動障害復旧

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

- ディスクデリバリーによる障害復旧

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

- 拡張自動障害復旧(EADR)

  拡張自動障害復旧(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、障害復旧 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。

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

個々のオペレーティングシステムでサポートされる障害復旧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

その他の障害復旧の方法

この項では、Data Protectorを使った障害復旧の概念と、他社製品の障害復旧の概念を比較します。ここでは、Data Protector以外の復旧方法について簡単に紹介します。主な復旧方法としては、以下の2つが挙げられます。

オペレーティングシステムのベンダーが提供する復旧方法

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

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

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

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、クラスター化にも対応しているため、高速かつ効率的に障害復旧を実行できます。Data Protectorには、大規模な組織のシステム管理を支援するための、集中管理や復元を容易にする機能、高可用性のサポート、モニタリング、レポート、通知などの機能が備わっています。

3 メディア管理とデバイス

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

   詳細は、「バックアップ開始前のメディア管理」(153ページ)を参照してください。

2. メディアをバックアップに使用します。

   ここでは、バックアップ用メディアの選択基準やメディア状態のチェック方法、新しいバックアップデータをメディアに追加する方法、メディア上のデータを上書きするタイミングなどを定義する必要があります。

   詳細は、「バックアップセッション中のメディア管理」(155ページ)を参照してください。

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

   詳細は、「バックアップセッション後のメディア管理」(159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。

   (「メディア状態の計算」(159ページ)を参照)。

メディアプール

Data Protectorのメディアプールでは大量のメディアをまとめて管理できるため、管理者の負担が大幅に軽減されます。

メディアプールとは

メディアプールとは、使用パターンとメディアプロパティが共通のメディアの論理的なセット(グループ)のことです。プール内のメディアは物理タイプも同一でなければなりません。たとえば一つのメディアプール内にDLTメディアとDAT/DDSメディアを混在させることはできません。

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

複数のデバイスで、同一プールに所属するメディアを共有することも可能です。

メディアプールのプロパティの例

プールのプロパティ例を以下に示します。:

- 追加可能(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プロパティの詳細については、オンラインヘルプの索引「メディアプール、プロパティ」を参照してください。

メディアプールとdcbfディレクトリ

Data Protectorでは、メディアプールに対してターゲットのdcbfディレクトリを設定できます。ターゲットdcbfディレクトリを指定すると、メディアプールのすべてのメディア情報が指定されたディレクトリに保存されます。

IDBのDCBF部分とdcbfディレクトリの詳細は、「IDBのアーキテクチャ」(197ページ)を参照してください。

メディアプールの使用方法

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

- システムプラットフォームごと(UNIXシステム用、Windows 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。

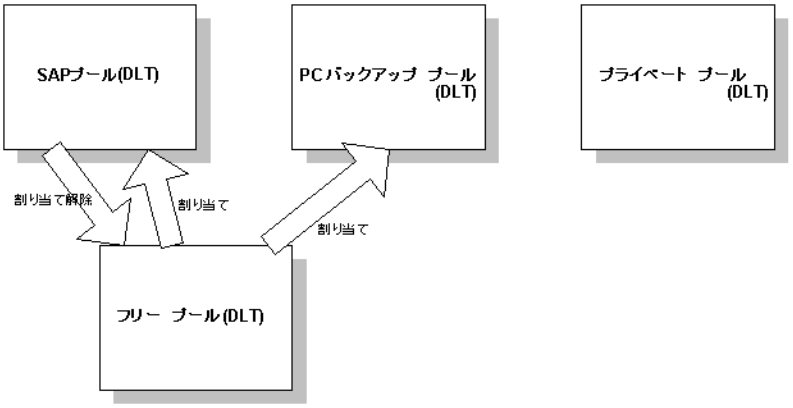


図 36 フリープール

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(146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(146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(146ページ)のプライベートプールなど、通常のプールの中にはメディアをフリープールと共有しないように構成できるプールもあります。

フリープールの利点

フリープールには、以下の利点があります。

- プール間でフリーメディアを共有できます。
  すべてのフリー(保護されていない空の)メディアをフリープールにまとめて、フリープールの使用をサポートするすべてのメディアプール間で共有できます。
- バックアップ時のオペレータの手動での作業を軽減します。
  すべてのフリーメディアが共有されている場合、マウント要求の必要性が低くなります。

フリープールのプロパティ

フリープールには、以下のような特徴があります。

- フリープールを使用するよう構成すると、フリープールを手動でまたは自動的に作成できます。通常のプールにリンクされているフリープールや空でないフリープールは削除できません。
- 通常のプールと異なり、割り当て方針オプションがありません。
- Data Protectorメディアのみ(不明のメディアまたは空のメディアを含まない)で構成されます。

メディア品質の計算

メディアの品質ではプール間の平均値が計算されます。メディア状態要素はフリープールに対してのみ構成可能で、フリープールを使用するすべてのプールによって継承されます。

フリープールの制限

フリープールには、以下の制限があります。

- 各プールごとに異なる状態要素は選択できません。その代わりにフリープールを使用するすべてのプールは、このフリープールに構成された状態要素を使用できます。
- メディアを手動で移動すること(保護メディアをフリープールへ移動したり、自動的に割り当て解除されるように構成されている、非保護メディアを通常のプールへ移動すること)はできません。
- フリープール内のメディアに対してインポート、コピー、リサイクルなどの操作は実行できません。
- マガジンをサポートするプールでフリープールは使用できません。
- フリープール使用時に、プール内に一時的な不整合が生じる場合があります(通常のプール内の非保護メディアが割り当て解除プロセスを待機しているなど)。
- メディアの保護期限が切れた後に保護期間を変更(たとえば無期限に変更)すると、メディアがフリープール内にあってもバックアップ用に割り当てられません。

- フリープールから割り当てられた場合は、異なるデータ形式タイプを持つメディアを使用でき、自動的に再フォーマットされます。たとえばNDMPメディアは、通常のメディアに再フォーマットされます。

フリープールの詳細については、Data Protectorのオンラインヘルプの索引「フリープール、特性」を参照してください。

メディアプールの使用例

バックアップ環境を選択する上で考慮可能な構成例を以下に示します。

例1

図37（148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。

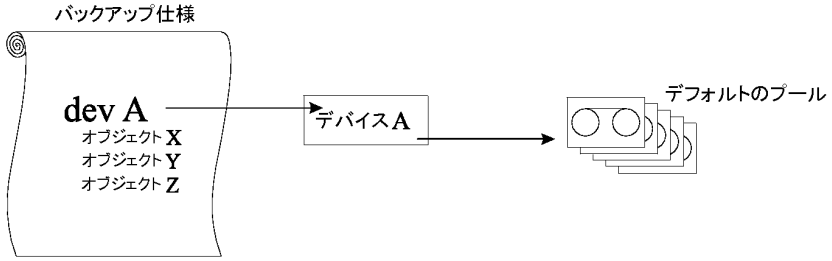


図 37 単一デバイス/単一メディアプールの単純な対応付け

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（149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」（171ページ）を参照してください。

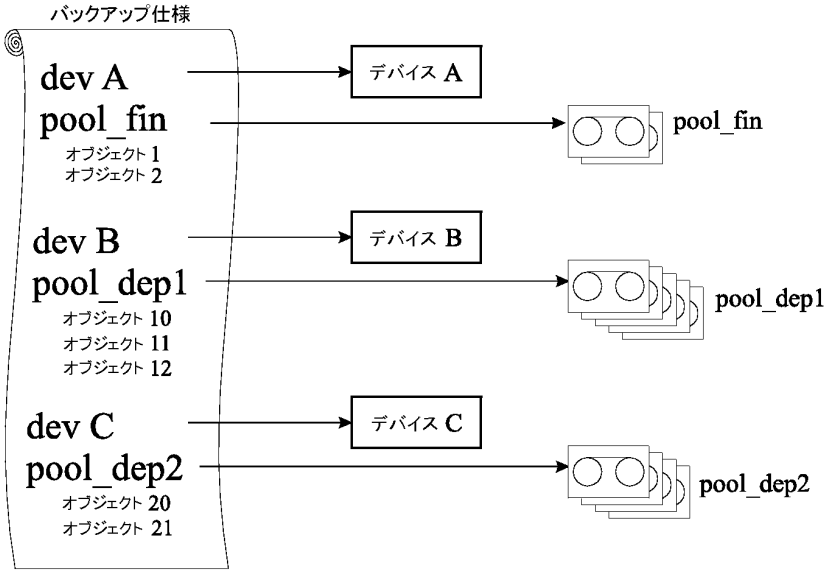


図 38 大容量ライブラリを使用する場合のメディアプール構成例

例3

図39(150ページ)は、複数のデバイスから、同一メディアプール内のメディアに、データを同時にバックアップする場合の例を示したものです。どのプールを使用するかにかかわらず、複数のデバイスを並列に使用すると、性能は向上します。

詳細は、「デバイスリストと負荷調整」(163ページ)を参照してください。

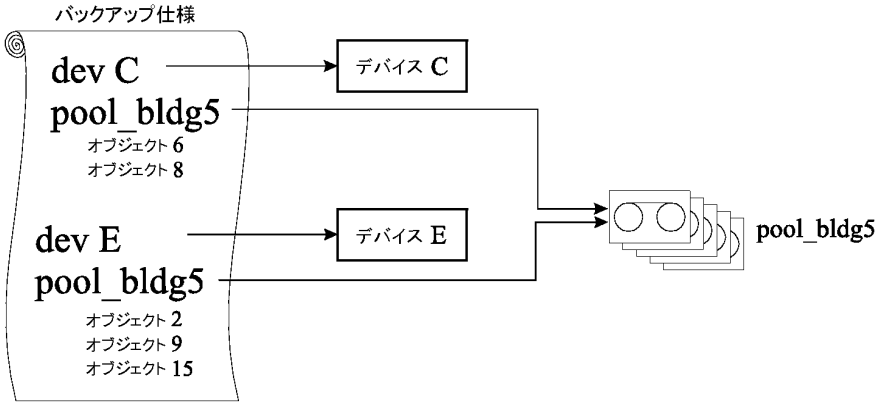


図 39 複数デバイスと単一メディアプールの対応付け

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。

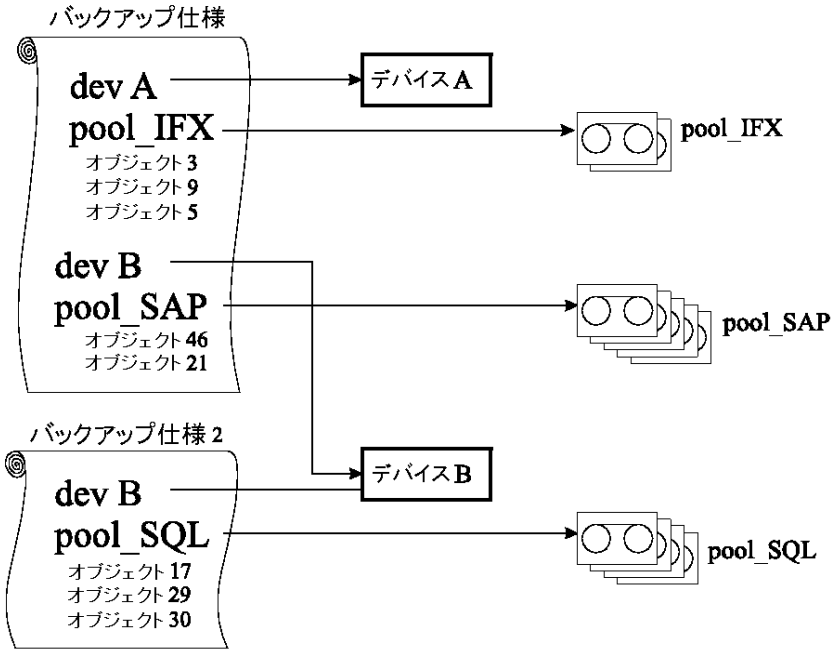


図 40 複数デバイスと複数メディアプールの対応付け

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

自動メディア交換と自動メディア操作

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

- メディアはメディアプールにグループ化されるため、単独のメディアを管理する必要はなくなります。Data Protectorでは、メディアプール内の各メディアを自動的に追跡および管理します。
- バックアップされるデータがどのメディアに書き込まれるかを決める必要はありません。それは、Data Protectorによって行われます。管理者は、メディアプールにバックアップを行います。
- Data Protectorでは、指定したメディア割り当て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。「バックアップ用メディアの選択 」(155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。詳細は、「バックアップ用メディアの選択 」(155ページ)を参照してください。

Data Protectorメディアのラベリング

Data Protectorで使われるメディアのラベリング

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

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

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

メディアラベルを変更すると、メディア自体ではなく、IDB内のメディアラベルが変更されます。そのため、書き換えていないメディアをいったんエクスポートしてからインポートし直すと、IDB内のメディアラベルがメディア上のメディアラベルで置き換えられます。テープ上のメディアラベルは、メディアを再初期化(フォーマット)しない限り変更できません。

ラベルの使用目的

これらのラベルは、そのメディアがData Protectorメディアであることを示します。バックアップ時または復元時にメディアがロードされると、そのメディアのメディアIDが自動的にチェックされます。メディア管理システムでは、個々のメディアに関する情報を保持しており、そのメディアに対して要求された動作を実行してもよいかどうかが判断されます。たとえば、メディア上に新しいバックアップ情報を書き込もうとした場合、メディア管理システムにより、メディア上の既存データの保護期限が切れているかどうかがチェックされます。ユーザー定義のラベルは、メディアを識別するために使用します。

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

各メディアの[位置(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」(133ページ)を参照してください。

バックアップセッション中のメディア管理

バックアップ中の処理内容

バックアップセッション中には、Data Protectorにより、バックアップ用メディアが自動的に選択され、どのデータがどのメディアに保存されたかもトラッキングされています。このように、どのデータがどのメディアにバックアップされたかをオペレータが正確に把握する必要はなく、メディア管理が容易になります。同一セッション内でバックアップされたバックアップオブジェクトは、メディアセットと呼ばれます。

以下では、次の項目について説明します。

- Data Protectorによる、バックアップ用メディアの選択方法
- フルバックアップおよび増分バックアップの、メディアへの追加方法
- メディア状態の計算方法

関連情報については、以下の項を参照してください。

- 「フルバックアップと増分バックアップ」(73ページ)
- 「メディアプール」(143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。たとえば、状態が[良好(Good)]のメディアは、状態が[普通(Fair)]のメディアよりも優先的に使用されます。詳細は、「メディア状態の計算」(159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。

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。

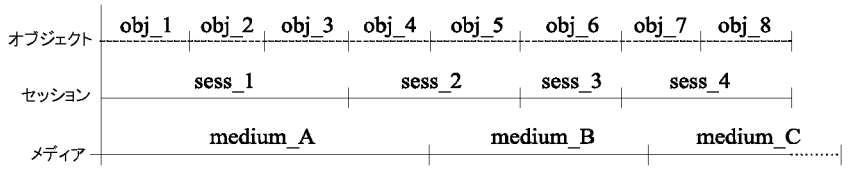


図 41 1つのメディア上に複数セッションの複数オブジェクトを格納（順次書き込み）

図41（157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。

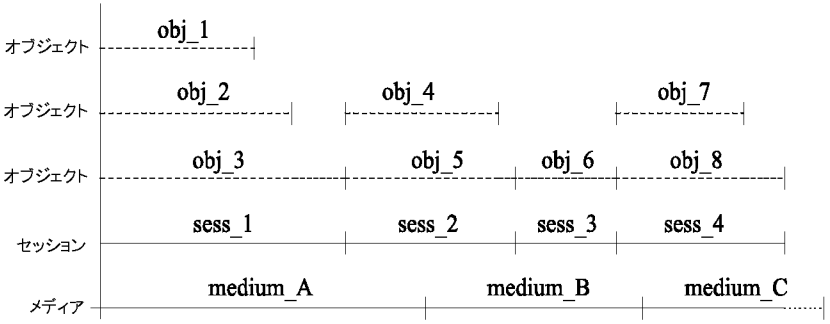


図 42 1つのメディア上に複数セッションの複数オブジェクトを格納（並列書き込み）

図42（157ページ）の例では、4つのセッションで、並列処理を有効にして同時書き込みを可能にした状態で、8つのオブジェクトを書き込んでいます。この場合、*obj_1*、*obj_2*、*obj_3*は*sess_1*で同時にバックアップされ、*obj_4*と*obj_5*は*sess_2*で同時にバックアップされました。*obj_1*は*system_A*の、*obj_2*は*system_B*の情報である場合もあれば、これらのオブジェクトが同一システム上の個別のディスク上の情報である場合も考えられます。メディア使用方針は、[追加可能(Appendable)]に設定されています。

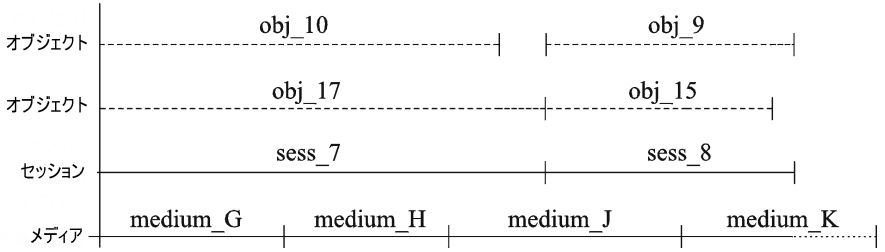


図 43 1セッションあたり複数のメディアを使用し、1つのオブジェクトを複数のメディアに格納

図43 (158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。

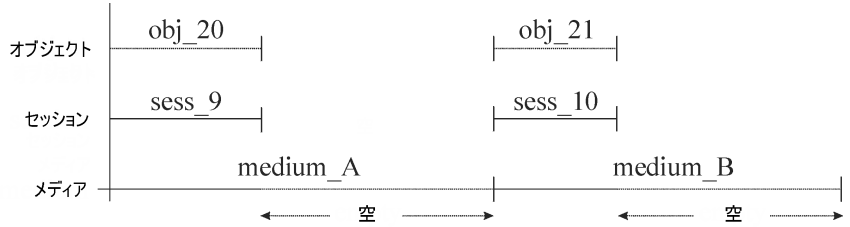


図 44 各オブジェクトを個別のメディアに格納

図44 (158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に与える影響の詳細は、「フルバックアップと増分バックアップ」(73ページ) を参照してください。

バックアップ時の複数メディアセットへのデータ書き込み

Data Protectorのオブジェクトミラー機能を使用すると、バックアップセッション中に、一部またはすべてのオブジェクトを、複数のメディアセットに同時に書き込むことができます。詳細は、「オブジェクトミラーの作成」(126ページ) を参照してください。

メディア状態の計算

メディアの状態要素

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。たとえば、メディアプール内のある1つのメディアの状態が不良(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。

メディアには、良好(Good)、普通(Fair)、不良(Poor)の3つの状態があります。

各メディアについて以下を使用し、状態を計算します。

- 上書き回数

  メディアの使用回数は、そのメディアが上書きされた回数として定義されます。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。たとえばバックアップ中にデバイス障害が発生した場合は、そのデバイスでバックアップに使われていたメディアには、不良(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。データおよびカタログ保護の詳細については、「バックアップデータおよびバックアップデータに関する情報の保存」(102ページ)を参照してください。

- 物理的損傷からメディアを保護する。

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

- バックアップデータのコピーを作成し、そのコピーを安全な場所に保管する。

「バックアップデータの複製」(117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に設定されていることを意味します。データ保護期間は5年に設定します。カタログ保護期間は1年に設定します。こうすることで、1年間はデータのブラウズや復元を簡単に実行でき、さらにデータそのものの復元は5年間可能になります。フルバックアップで作成されたメディアについてはコピーを作成し、保管場所に格納しておきます。バックアップ後1年が経過したメディアについては、Data Protectorのデータベースから、そのメディア上のデータに関する詳細情報が自動的に削除されます。これにより、新しい情報を保存するためのスペースがデータベース内に確保されます。

保管場所内のメディアを使った復元処理

保管場所内のメディアからデータを復元する方法は、一般のメディアからの復元方法と変わりません。データ保護とカタログ保護の方針によっては、以下に示す以外の手順が必要になることもあります。

1. 保管場所からメディアを取り出して、デバイスに挿入します。
2. メディアのカタログ保護がまだ有効な場合には、Data Protectorユーザーインタフェースを使用して復元対象を選択することにより、簡単にデータを復元できます。

   メディアのカタログ保護期限が切れている場合には、そのメディア上のバックアップデータに関する詳細情報はData Protector内には保存されていません。その場合は、復元するファイルまたはディレクトリを手動で指定する必要があります。予備のディスクにオブジェクト全体を復元し、復元されたファイルシステム内で目的のファイルやディレクトリを検索することも可能です。

ヒント:

カタログ保護期限がいったん切れた後に、メディア上にバックアップされているファイルおよびディレクトリに関する詳細情報をData Protectorに再度読み込むには、メディアをいったんエクスポートしてから、インポートし直します。次に、メディア上の詳細なカタログデータを読み取るよう指示します。こうすると、Data Protectorユーザーインタフェースを使用したファイルやディレクトリの選択が、再び可能になります。

データ保護方針およびカタログ保護方針が復元処理に与える影響の詳細については、「バックアップデータおよびバックアップデータに関する情報の保存」(102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については、http://www.hp.com/support/manualsを参照してください。

Data Protectorでのデバイスの使用

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

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

ライブラリ管理コンソールのサポート

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

Data Protectorは、ライブラリ管理コンソールのインタフェースに簡単にアクセスするための機能を備えています。管理コンソールのURL(Webアドレス)は、ライブラリの構成時また

は再構成時に指定できます。GUIでこの作業用のメニューを選択すると、Webブラウザが起動され、ブラウザ内にコンソール インタフェースが自動的に表示されます。

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

重要:

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

TapeAlert

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

性能の向上

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

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

関連情報については、「バックアップセッション」(230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(167ページ)に示すように、個々のセグメントはファイルマークによって分割されます。

注記:

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

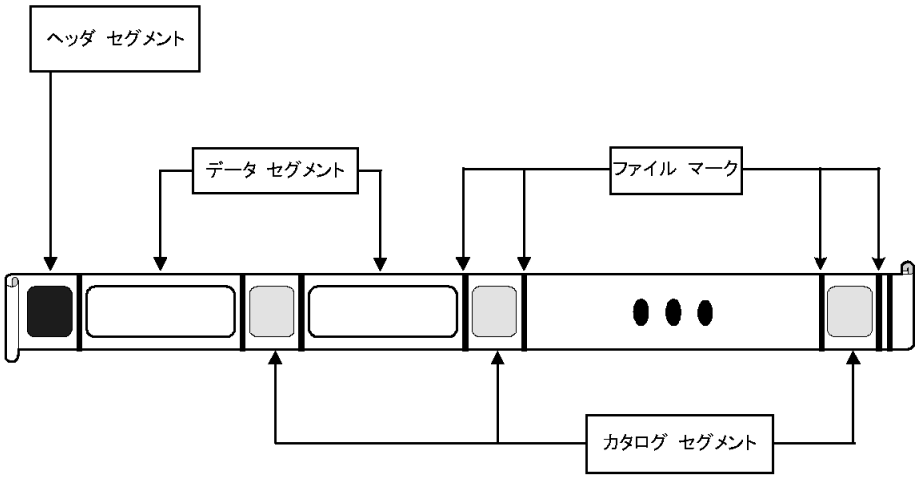


図 45 データフォーマット

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

ブロックサイズ

セグメントは全ユニットに対してではなく、ブロックと呼ばれる小さなサブユニットに対して指定します。デバイスのハードウェアでは、デバイスの種類ごとに固有のブロックサイズの単位でデータを処理します。Data Protectorでは、デバイスに送信するブロックサイズを調整できます。すべてのデバイスのデフォルトブロックサイズ値は64KBです。

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

注記:

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

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

物理デバイスの衝突

バックアップに使用するデバイスを指定するときに、あるバックアップ仕様内で1つのデバイス名を指定し、別のバックアップ仕様内で同じ物理デバイスの別名を指定していること

があります。このような場合、バックアップのスケジュール方法によっては、複数のバックアップセッションで同時に同一の物理デバイスを使おうとして、デバイスの衝突が発生する可能性があります。

衝突の防止

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

たとえば図46（169ページ）では、あるDDSデバイスをDDS_Cという名前の圧縮デバイスとして構成し、さらにDDS_NCという名前の非圧縮デバイスとしても構成しています。この場合、両方のデバイス構成内に、DDSという同一のロック名を指定しておきます。

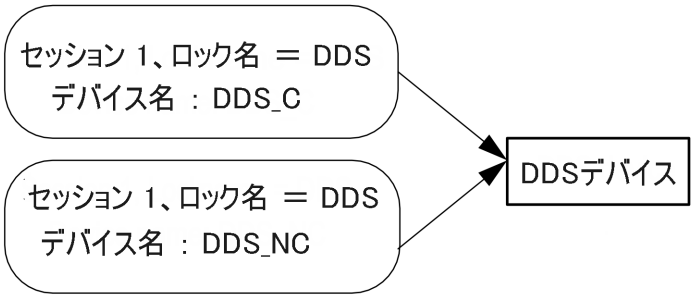


図 46 デバイスロックとデバイス名

スタンドアロンデバイス

スタンドアロンデバイスとは

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

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

Data Protectorとスタンドアロンデバイス

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

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

デバイスチェーンとは

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

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

スタッカーデバイス

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

小規模なマガジンデバイス

マガジンデバイスとは

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

Data Protectorとマガジンデバイス

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

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

汚れたドライブのクリーニング

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

大容量ライブラリ

ライブラリデバイスとは

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

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

Data Protectorは、HP 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。サポート対象デバイスの一覧は、http://www.hp.com/support/manualsを参照してください。

メディアの操作

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

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

ライブラリの構成

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

ライブラリのサイズ

必要なライブラリのサイズは、以下のように見積ります。

- メディアを複数の場所に分散させる必要があるか、または1箇所に集中して管理するかを決定します。

- 必要なメディアの数を見積ります。「メディア交換方針の実装」(151ページ)を参照してください。

他のアプリケーションとのライブラリの共有

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

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

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

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

挿入および取り出しメールスロット

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

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

詳細は、ご使用のデバイスのマニュアルを参照してください。

バーコードサポート

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

バーコードの利点

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

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

ヒント:

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

クリーニングテープのサポート

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

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

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

複数システムによるライブラリの共有

ライブラリの共有とは

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

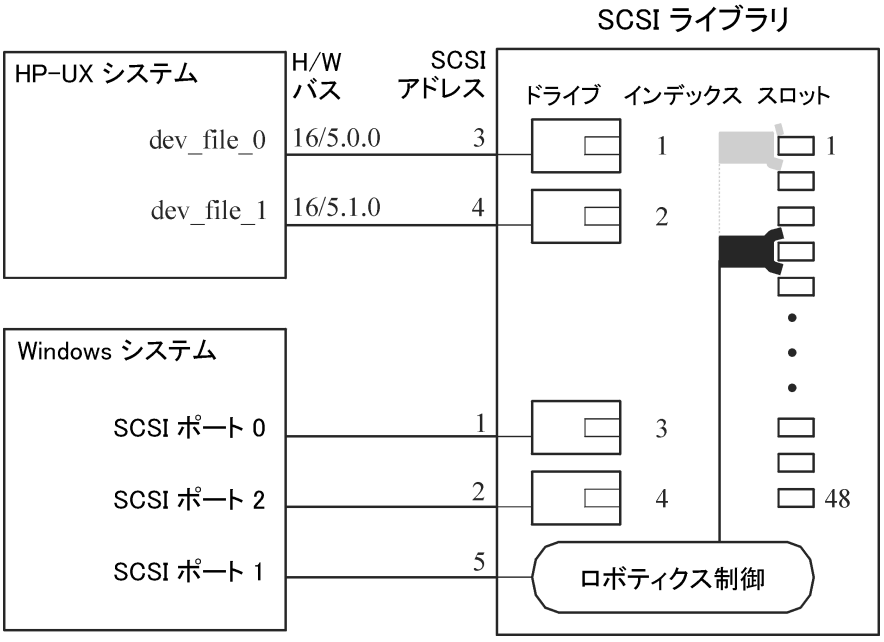


図 47 ドライブを複数のシステムに接続

制御プロトコルとData Protector Media Agent

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

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

- SCSI–SCSIまたはFibre Channel接続ドライブ向け

このプロトコルは、汎用Media AgentとNDMP Media Agentの両方に実装されています。

- NDMP—NDMP専用ドライブ向け
  このプロトコルはNDMP Media Agentにのみ実装されています。

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

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

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

ドライブ制御

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

表10(175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(176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(177ページ)から図50(179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。

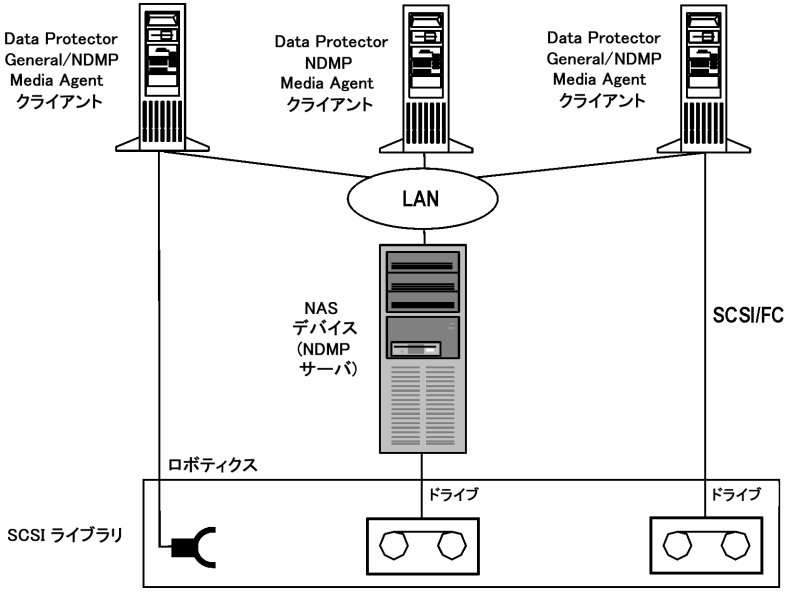


図 48 SCSIライブラリの共有(ロボティクスをData Protectorクライアントシステムに接続)

図48(177ページ)に示すSCSIライブラリのロボティクスは、General Media AgentまたはNDMP Media Agentのインストールされ たData Protectorクライアントシステムに接続され、そのクライアントシステム上に構成されています。このクライアント上のGeneral Media AgentまたはNDMP Media Agentは、SCSIロボティクス制御プロトコルを使用します。ロボティクスを接続したData Protectorクライアントシステムに、さらに1つ以上のドライブを接続することも可能です。

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

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

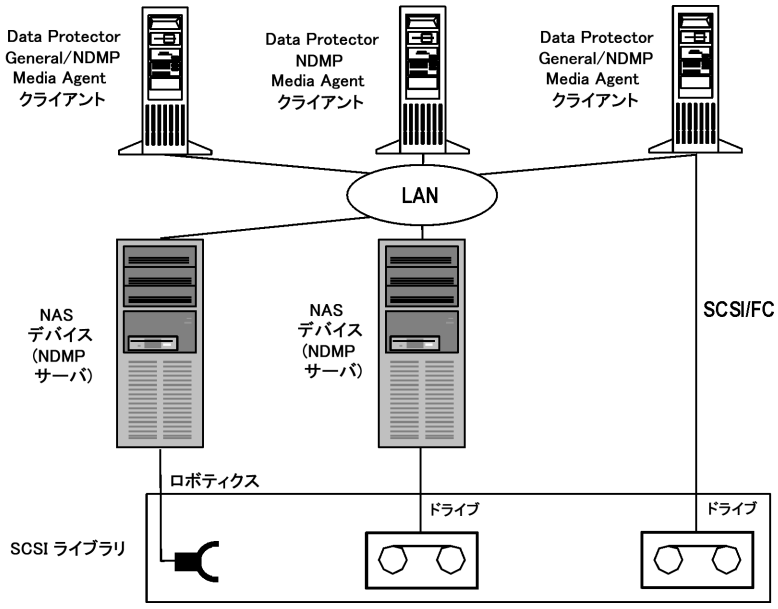


図 49 SCSIライブラリの共有(ロボティクスをNDMPサーバーに接続)

図49(178ページ)に示すSCSIライブラリでは、ライブラリのロボティクスがNDMPサーバーに接続され、General Media AgentまたはNDMP Media Agentのインストールされた Data Protectorクライアントシステム上に構成されています。このクライアント上のGeneral Media AgentまたはNDMP Media Agentは、SCSIロボティクス制御プロトコルを使用します。ロボティクスを接続したNDMPサーバーに、さらに1つ以上のドライブを接続することも可能です。

重要:

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

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

ライブラリ内のもう1つのドライブは、General Media AgentまたはNDMP Media Agentのインストールされた Data Protectorクライアントシステムに接続され、このクライアントシステム

上に構成されています。クライアント上のGeneral Media AgentまたはNDMP Media Agentは、SCSIドライブ制御プロトコルを使用します。

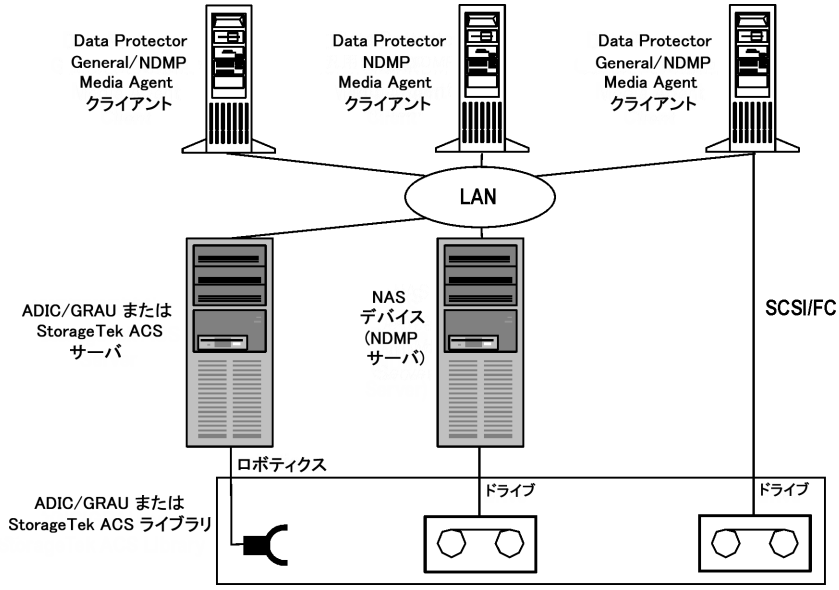


図 50 ADIC/GRAUライブラリまたはStorageTek ACSライブラリの共有

図50 (179ページ) に示すADIC/GRAUライブラリ(またはStorageTek ACSライブラリ)では、ライブラリのロボティクスがADIC/GRAUサーバー(またはStorageTek ACSサーバー)に接続され、General Media AgentまたはNDMP Media Agentのインストールされた Data Protectorクライアントシステム上に構成されています。このクライアント上のGeneral Media AgentまたはNDMP Media Agentは、ADIC/GRAUロボティクス制御プロトコルを使用します。ADIC/GRAUサーバーやStorageTek ACSサーバーに、さらに1つ以上のドライブを接続することも可能です。

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

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

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

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。

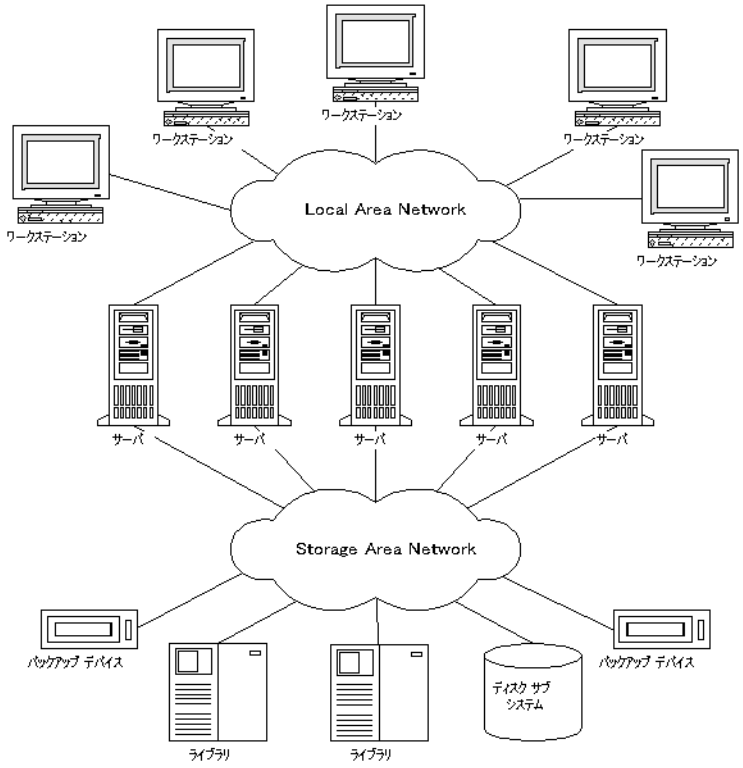


図 51 ストレージエリアネットワーク（storage area network）

ファイバチャンネル

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。

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

ループトポロジー

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

LIP

LIP (Loop Initialization Primitive)プロトコルはさまざまな場合に起動されますが、最も一般的なのは新しいデバイスが導入された場合です。新しいデバイスには、すでにループに属していたデバイスに電源を入れたものや、アクティブなデバイスでスイッチポートを移動したものもあります。LIPが起動されると、テープのバックアップ処理など、SAN上の進行中のプロセスが予期せず中断される場合があります。これによってSCSIブリッジとノード(SCSIデバイス)間のSCSI接続がリセットされます。図52 (183ページ)を参照してください。

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

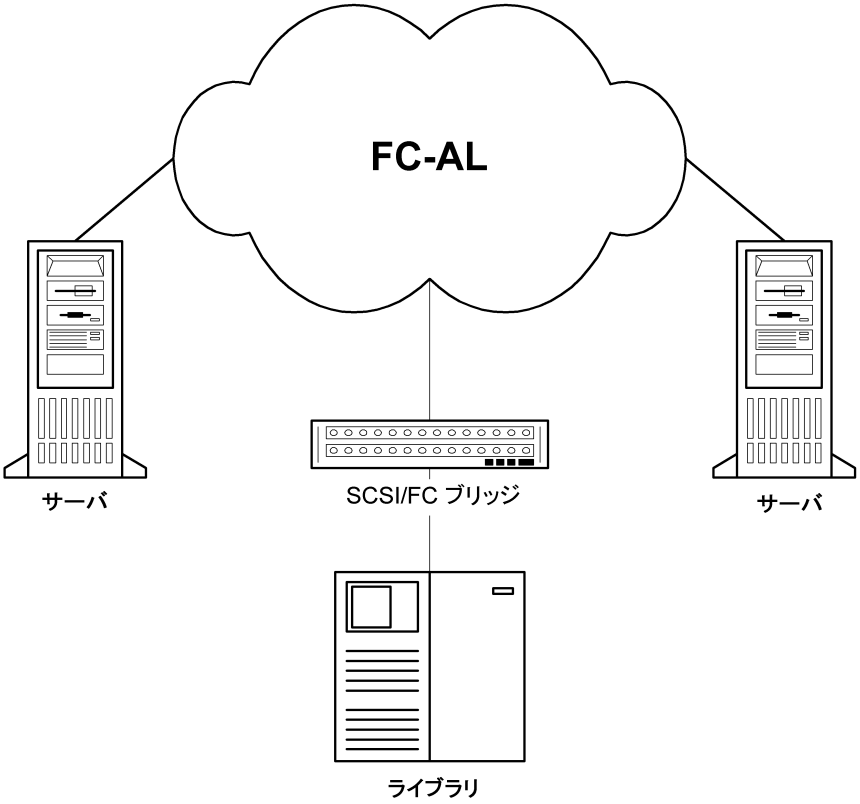


図 52 Loop Initializationプロトコル

スイッチ式トポロジー

スイッチ式トポロジーでは、スイッチに接続されたすべてのノード間でany-to-anyの接続が可能となります。Fibre Channelプロトコルには自動構成および自動管理機能があるため、スイッチは簡単にインストールして使用できます。スイッチは、接続されている装置(ノード、FC-ALハブ、その他のFCスイッチなど)を自動的に検出し、それに合わせて自分自身を構成できます。スイッチは、接続されているノードにスケーリングされた帯域幅を提供します。スイッチ式トポロジーでは、ノードの真のホットプラグ機能が実現されます。

注記:

ホットプラグとは、リセットや通信の再確立などのプロトコル機能を指します。ホットプラグの最中は進行中のデータ転送は中断されますが、テープデバイスなどの一部のデバイスではこの動作に対応できない点に注意が必要です。ノードをループに接続したり、ループから切り離したりすると、バックアップ処理や復元処理が中断されて、処理が失敗する可能性があります。そのため、ループへのノードの接続や切り離しは、関連するハードウェアを使用したバックアップ処理や復元処理が行われていない時間帯にのみ実行してください。

SANにおけるデバイスの共有

Data ProtectorはSANの概念をサポートしており、SAN環境のバックアップデバイスを複数のシステム間で共有できます。つまり同一の物理デバイスに対して複数のシステムからのアクセスが可能です。そのため個々のデバイスに対するローカルバックアップを任意のシステムから実行できます。データはSANを介して転送され、バックアップに従来型のLANの帯域幅は必要ありません。そのためこの種のバックアップは、「LANフリー」なバックアップとも呼ばれます。また、通常SANベースのFibre Channelテクノロジの処理速度はLANテクノロジよりもはるかに優れているため、バックアップの性能も大幅に向上します。

ただし、複数のコンピュータシステムが、同一デバイスに同時にデータを書き込まないようにするための、なんらかの機構が必要になります。特に複数のアプリケーションが同一デバイスを使用する場合は問題がより複雑になります。こうした問題を解決するには、関連するすべてのシステム間で、デバイスへのアクセスを同期化する必要があります。このためには、ロックメカニズムを使用します。

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

物理デバイスに対する複数パスの構成

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

たとえば、あるデバイスがclient1上では、/dev/rs1および/dev/rs2として、client2上では/dev/r1s1として、またclient3上ではscsi1:0:1:1として構成されています。このため、

client1:/dev/rs1、client1:/dev/rs2、client2:/dev/r1s1、およびclient3:scsi1:0:1:1という4つの異なるパスを通してデバイスにアクセスすることができます。マルチパスデバイスには、このテープデバイスへの4つのパスすべてが含まれています。

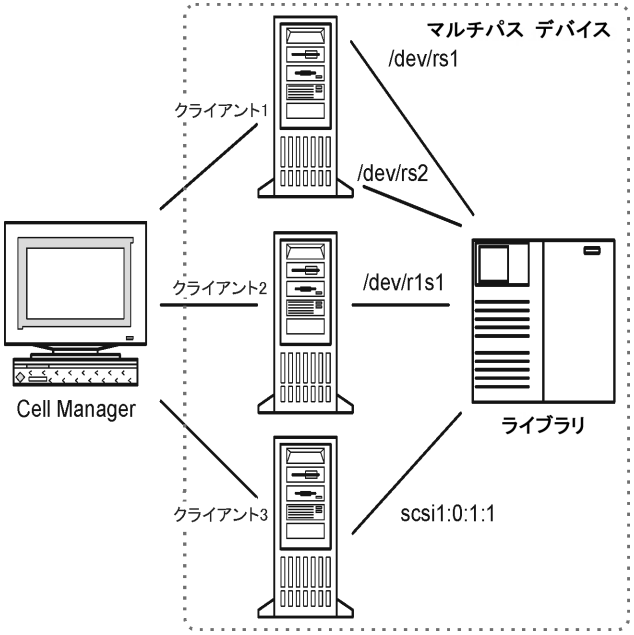


図 53 マルチパスの構成例

複数のパスを使う理由

Data Protectorの従来のバージョンでは、1つのクライアントからのみデバイスにアクセスできました。この問題を回避するには、複数の論理デバイスを、ロック名を使用して単一の物理デバイスとして構成する必要がありました。このようにして、複数のシステムから単一の物デバイスへのアクセスの構成にロック名を使用する場合は、各システムですべてのデバイスを構成する必要がありました。たとえば、単一のデバイスに接続されているクライアントが10個あった場合は、同じロック名のデバイスを10個構成する必要がありました。Data Protectorの現在のバージョンでは、すべてのパスを単一のマルチパスデバイスとして構成することにより構成を簡便化することができます。

マルチパスデバイスによってシステムの復元性が向上します。Data Protectorでは最初に定義されたパスの使用を試みます。1つのクライアントのすべてのパスにアクセスできない場合は、次のクライアントのパスを使って試行します。リストされているパスがすべて利用不可能だった場合にのみ、セッションは中断されます。

パスの選択

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

復元セッションでは、次の順序でデバイスパスが選択されます。

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

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

以前のバージョンとの互換性

従来のバージョンのData Protectorで構成されたデバイスはアップグレード時に再構成されず、変更を行わずに以前のリリースのData Protectorと同じように使うことができます。ただし、新しいマルチパス機能を使用するためには、それらのデバイスをマルチパスデバイスとして再構成する必要があります。

デバイスのロック

デバイスロック機構は、Data Protectorのみが複数のシステムから渡されたデータやコマンドを使ってデバイスを操作する場合だけでなく、複数のアプリケーションが同一デバイスを使用する場合にも対処できなければなりません。ロック機構の目的は、複数のシステム間で共有されるデバイスが、ある一時点では単一のシステムとのみ通信できるようにすることにあります。

複数アプリケーション間のデバイスロック

Data Protectorと少なくとも1つの別のアプリケーションが、複数のシステムで同一デバイスを共有するためには、各アプリケーションが同一(共通)のデバイスロック機構を使用する必要があります。このロック機構は、複数のアプリケーションにわたって機能するものでなければなりません。Data Protectorは、現時点ではこのモードをサポートしていません。そのためこのような形でデバイスを共有する必要がある場合は、運用規則を設けることにより、ある一時点では1つのアプリケーションのみがすべてのデバイスに排他的にアクセスできるようにしてください。

Data Protectorのデバイスロック機構

あるドライブを使用するアプリケーションはData Protectorのみであるが、複数のシステムでそのドライブを使用する可能性がある場合は、デバイスロック機構を使用する必要があります。

また、あるロボティクス制御を、Data Protectorのみが複数のシステムで使用する場合は、ライブラリ制御とそれを使用するすべてのシステムが同一セル内にある場合に限り、Data Protectorで内部的に処理することができます。このような場合は、そのデバイスへのアクセスの同期はすべて、Data Protectorにより内部的に制御されます。

間接ライブラリアクセスと直接ライブラリアクセス

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

間接ライブラリアクセス

この構成はSANを導入する場合も、従来型のSCSIによる直接接続環境でも使用できます。この構成では各システムは、ライブラリロボティクスへの直接アクセス権を持つクライアントシステムに要求を転送することにより、ライブラリロボティクスへのアクセスが可能になります。この方法は間接ライブラリアクセスと呼ばれます。図54（188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。

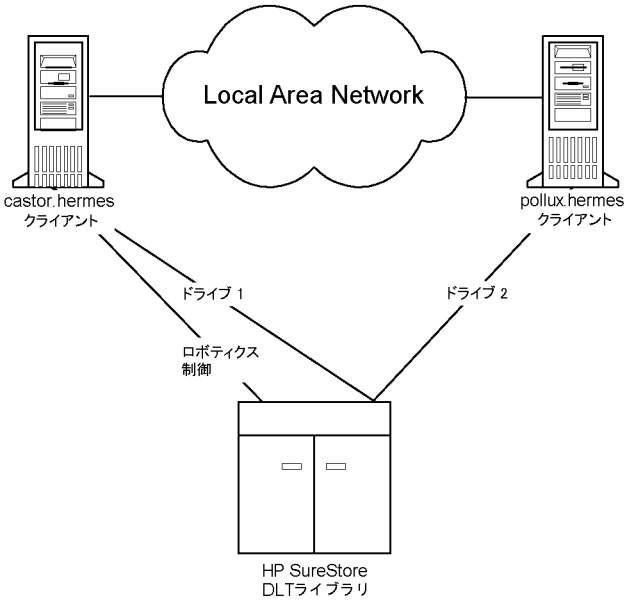


図 54 間接ライブラリアクセス

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(189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。

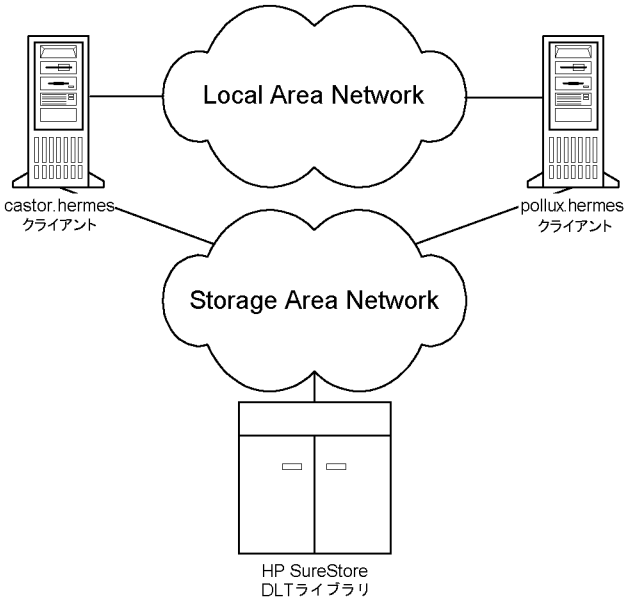


図 55 直接ライブラリアクセス

クラスター内のデバイス共有

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

クラスター対応アプリケーションは仮想ホスト上で実行されるため、その時々でクラスター内の任意のノード上で実行されている可能性があります。そのため、これらのアプリケーションをローカルバックアップするには、実際のノード名ではなく仮想ホスト名を指定してデバイスを構成する必要があります。各物理デバイスに対するデバイス構成を必要に応じて複数定義し、デバイスロック機構にはロック名を使用してください。詳細は、「デバイスのロック」(186ページ)を参照してください。

静的ドライブ

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

浮動ドライブ

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

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。詳細は、オンライン ヘルプの索引「ユーザー グループ、admin」を参照してください。

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、オブジェクトコピー、オブジェクト集約、オブジェクト検証、およびメディア管理の各セッションの結果や、構成済みのデバイスとライブラリなどに関する情報を保持します。

IDBを使う理由

IDBに保存された情報を利用することで、以下のことが可能になります。

- 復元が高速で便利。IDBに保存されている情報によって復元に必要なメディアを迅速に検出できるため、復元を高速に行うことができます。また復元対象のファイルやディレクトリをブラウズすることもできます。

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

IDBのサイズおよびサイズの増大に関する注意点

IDBは非常に大きくなる場合があります。IDBのサイズの変動はバックアップ性能やCell Managerシステムに大きく影響します。したがって、Data Protector管理者は、IDBを理解し、必要に応じて、IDB内に保持する情報と保持期間を決定する必要があります。復元時間と機能と、IDBのサイズとサイズの増大との間でバランスを維持するのは、管理者の作業です。Data Protectorには、このバランスを取るのに役立つ主要な2つのパラメータが用意されています。**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」(208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」(358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」(46ページ)を参照してください。

IDBのアーキテクチャ

IDBの構成要素を以下に示します。

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

以上のIDBの構成要素は、それぞれ特定のData Protector情報(レコード)を保存しており、IDBのサイズやサイズの増大にさまざまな点で影響を与えます。各構成要素はCell Manager上の別々のディレクトリに配置されています。(図56(199ページ)を参照)。

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

基礎となる技術

MMDBとCDBの各部分は、表領域を含む組込みデータベースを使って実装されています。この組込みデータベースはRDSデータベースサーバープロセスが制御しています。MMDBやCDBへの変更はすべてトランザクションログを使って更新されます。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。

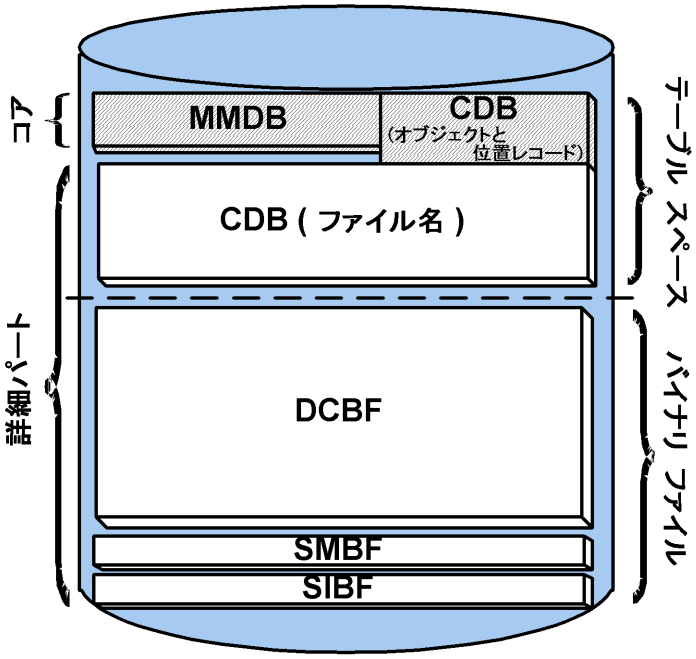


図 56 IDBの構成要素

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。詳細については、「IDBサイズの見積もり 」(213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、オブジェクトコピー、オブジェクト集約、オブジェクト検証、およびメディア管理の各セッションに関する情報。これは、Data Protectorのモニターウィンドウに送信される情報のコピーです。
- バックアップされたオブジェクトとそのバージョン、およびオブジェクトコピーに関する情報。暗号化されたオブジェクトバージョンの場合、キーID(KeyID-StoreID)も格納されます。
- バックアップオブジェクトのメディア上の位置に関する情報。Data Protectorは、各バックアップオブジェクトについて、バックアップに使用するメディアやデータセグメントの情報を保存します。オブジェクトコピーやオブジェクトミラーについても同様に情報を保存します。
- バックアップファイルのパス名(ファイル名)とクライアントシステム名に関する情報。ファイル名は1つのクライアントシステムごとに1度だけ保存されます。バックアップとバックアップの間に作成されたファイル名はCDBに追加されます。

ファイル名のサイズとサイズの増大

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

ファイルまたはディレクトリは、HP-UX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」(213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」(209ページ)を参照してください。

デフォルトでは、DCディレクトリ(db40¥ はDCバイナリファイル用に構成されます。このディレクトリのデフォルトの最大サイズは16GBです。DCディレクトリを複数作成してCell Manager上の別のディスクに配置し、IDBサイズを拡張することができます。1つのセルに対して最大50のディレクトリを作成することができます。

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、オンラインヘルプの索引「DCディレクトリ」を参照してください。

セッションメッセージバイナリファイル(SMBF)

SMBFレコード

セッションメッセージバイナリファイルには、Data Protectorセッション中に生成されたセッションメッセージが保存されます。1つのセッションにつき1つのバイナリファイルが作成されます。ファイルは年毎や月毎に分類されます。

SMBFのサイズとサイズの増大

SMBFのサイズは以下の要素によって決定されます。

- 実行されたセッション数(1セッションにつきバイナリファイルが1つ作成されるため)。
- セッション内のメッセージ数。セッション メッセージの容量は、Windowsの場合約200バイト、UNIXシステムの場合約130バイトです。[レポートレベル:]オプションを指定すると、バックアップ中、復元中、およびメディア管理中に表示されるメセージ数を変更できます。これによってIDBに保存されるメッセージ数も変わります。詳細は、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。

サーバーレス統合バイナリファイル(SIBF)

SIBFレコード

サーバーレス統合バイナリファイルには、NDMPの加工されていない復元データが保存されます。このデータは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」(213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

暗号化キーストアとカタログファイル

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

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

ハードウェア暗号化の場合、キーIDがメディアIDにマップされ、これらのマッピングはカタログファイルに保存されます。このファイルには、暗号化されたメディアを別のセルにエクスポートできるようにするために必要な情報が含まれます。

キーストアの位置

キーストア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¥keystore
- その他のWindowsシステムの場合:*Data_Protector_home*¥db40¥keystore
- UNIXシステムの場合:/var/opt/omni/server/db40/keystore

カタログファイルの位置

カタログファイルは、以下のディレクトリに格納されています。

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

IDBの操作

バックアップ時

バックアップセッションが開始されると、IDBにセッションレコードが作成されます。また、そのセッションのオブジェクトごと、およびオブジェクトミラーごとにオブジェクトバージョンレコードが作成されます。これらのレコードはすべてCDBに保存され、いくつかの属性が与えられます。バックアップに対してソフトウェア暗号化が要求された場合、関係するエンティティ(ホスト)の有効な暗号化キーが、キーストアから取得され、バックアップに使用されます。キーID(KeyID-StoreID)は、オブジェクトバージョンにリンクされ、CDBレコードに含められます。ホストとKeyID-StoreIDとのマッピングは、キーストア内のカタログにも格納されます。

バックアップ中に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。関係するメディアがハードウェア暗号化を要求したドライブ内にある場合、まず、エンティティ(メディア)の有効な暗号化キーがキーストアから取得されます。メディアとKeyID-StoreIDとのマッピングは、キーストア内のカタログに記録され、メディアにも書き込まれます。

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

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

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

復元時

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

特定のファイルバージョンを選択すると、Data Protectorは必要なメディアを決定し、選択したファイルが使用するメディア位置レコードを検出します。これらのメディアはMedia Agentから読み込まれ、選択したファイルを復元するDisk Agentに詳細が送信されます。関係するメディアに対してハードウェア暗号化が行われた場合、Media Agentは最初にキーID(KeyID-StoreID)を検出し、Key Management Server (KMS)によってキーストアから取得されるキーを要求します。

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

オブジェクトコピー時またはオブジェクト集約時

オブジェクトコピーセッションまたはオブジェクト集約セッション中では、バックアップと復元セッション中と同じ処理が実行されます。基本的には復元時と同様にコピー元メディアからデータが読み込まれ、バックアップ時と同様にコピー先メディアにそのデータが書き込まれます。IDBの操作という点では、オブジェクトコピーセッションまたはオブジェクト集約セッションで行われることと、バックアップと復元で行われることは同じです。詳細は、「バックアップ時」(204ページ)および「復元時」(205ページ)を参照してください。ソフトウェア暗号化を使用するオブジェクト集約はサポートされていないため、これは当てはまりません。

オブジェクトの検証時

オブジェクト検証セッション中では、復元セッションと同じデータベース処理が実行されます。基本的には復元時と同様にコピー元メディアからデータが読み込まれ、オブジェクトの検証を実行するホストディスクエージェントに送信されます。IDB操作という点では、オブジェクト検証セッションで行われることと、復元セッションで行われることは同じです。検証セッション中に生成されるすべてのセッションメッセージは、セッションメッセージのバイナリファイルに保存されます。詳細は、「復元時」(205ページ) を参照してください。

メディアのエクスポート

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

さらに、複数のアイテムが削除されます。

キーエクスポートディレクトリの位置

暗号化キーエクスポートディレクトリの位置を以下に示します。

- Windows Server 2008の場合: *Data_Protector_program_data*¥Config¥Server¥export¥keys
- その他のWindowsシステムの場合:*Data_Protector_home*¥Config¥Server¥export¥keys
- UNIXシステムの場合:/var/opt/omni/server/export/keys

削除されたアイテム

以下のアイテムが削除されます。

- エクスポートしたメディアのすべてのメディア位置レコードがCDBから削除されます。
- その他のメディアに位置レコードがないすべてのオブジェクトとオブジェクトコピーがCDB部分から削除されます。
- 30日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、オンラインヘルプの索引「IDB, recovery」(IDB、復旧)を参照してください。

IDBの増大と性能

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

IDBの増大や性能に影響を与える重要な要素

IDBの増大や性能に影響を与える重要な要素を以下に示します。

- ロギングレベルの設定ロギングレベルでは、バックアップ時にIDBに書き込まれる詳細データ量を定義します。詳細度を高めるようにロギングレベルを変更すると、IDBへの影響が増大します。詳細については、「IDBの増大と性能: 主要な調整可能パラメータ」(209ページ)を参照してください。
- カタログ保護の設定カタログ保護は、IDBでのバックアップデータに関する情報の保管期間を決定します。カタログ保護の期間を長くすると、IDBへの影響が増大します。詳細については、「IDBの増大と性能: 主要な調整可能パラメータ」(209ページ)を参照してください。
- バックアップファイル数。Data Protectorでは、各ファイルおよびファイルの各バージョンを記録します。IDBへの影響は、バックアップの種類によって異なります。バックアップの種類については、「フルバックアップと増分バックアップ」(73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。たとえば、Shift-JIS形式のファイル名の場合に各文字がIDB内で最大3バイトを占めるのに対し、純粋なASCII形式のファイル名の場合は1バイトしか必要ありません。このようにUNIX上では、文字のエンコード方式がIDBのファイル名部分の増大に影響を及ぼします。なおWindows上では、すべての文字がIDB内で2バイトを占めます。

- オブジェクトコピーとオブジェクトミラーの数。作成するオブジェクトコピーおよびオブジェクトミラーの数が多いほど、IDBに格納される情報量が増えます。オブジェクトコピーおよびオブジェクトミラーについては、ファイル名情報を除き、バックアップオブジェクトの場合と同様の情報がIDBに保存されます。

IDBの増大と性能: 主要な調整可能パラメータ

ロギングレベルとカタログ保護は、IDBの増大と性能を左右する要素のうちの主なものです。これらの要素がIDBに与える影響は、設定によって異なります。ロギングレベルの設定とカタログ保護の設定によって影響がどのように変動するかを、図57 (209ページ)に示します。

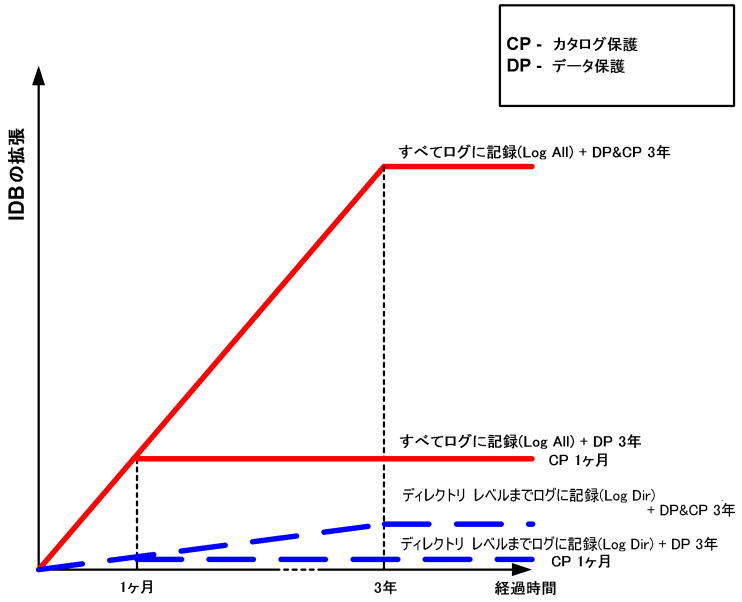


図 57 ロギングレベルとカタログ保護がIDBの増大に与える影響

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

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

パフォーマンスへの影響

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

ロギングレベルと復元時のブラウズ

保存される情報のレベルを変更すると、復元時にData Protector GUIを使用してブラウズできるファイルも変わります。[ログなし(No Log)]オプションを設定すると、ブラウズが不可能になり、[ディレクトリレベルまでログに記録(Log Directories)]オプションを設定すると、ディレクトリのブラウズが可能になり、[ファイルレベルまでログに記録(Log Files)]オプションを設定すると、完全ブラウズが可能になりますがファイル属性(サイズ、作成日付、変更日付など)は表示されません。

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

- 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。

パフォーマンスへの影響

カタログ保護の設定は、バックアップの性能には影響を与えません。

カタログ保護と復元

カタログ保護期限が過ぎたデータは[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」(209ページ)を参照)。

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

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

同一セル内で異なるロギングレベルを使用

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

- メール サーバーには、[ディレクトリレベルまでログに記録(Log Directories)]オプションを使用します。
- データベースサーバーには独自の復元方針があるため、ログは必要ありません。このため、[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またはファイルサーバーには、異なるバージョンのファイルを検索および復元できるように[すべてログに記録(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については、オンラインヘルプの索引「インポート、メディアからカタログを」を参照してください。

オブジェクトコピーに異なるロギングレベルを設定

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

たとえば、バックアップセッションで正常にバックアップされたことを確実にするためにだけオブジェクトミラーを作成するような場合であれば、オブジェクトミラーには[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バックアップを実行する場合、IDBのサイズが2GBを超える可能性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、English Documentation & Helpコンポーネントの一部としてインストールされます。ツールはインストール時に以下の場所に置かれます。

- ***UNIXシステムの場合***:

  /opt/omni/doc/C/IDB_capacity_planning.xls

- ***UNIXシステムの場合***:

  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。

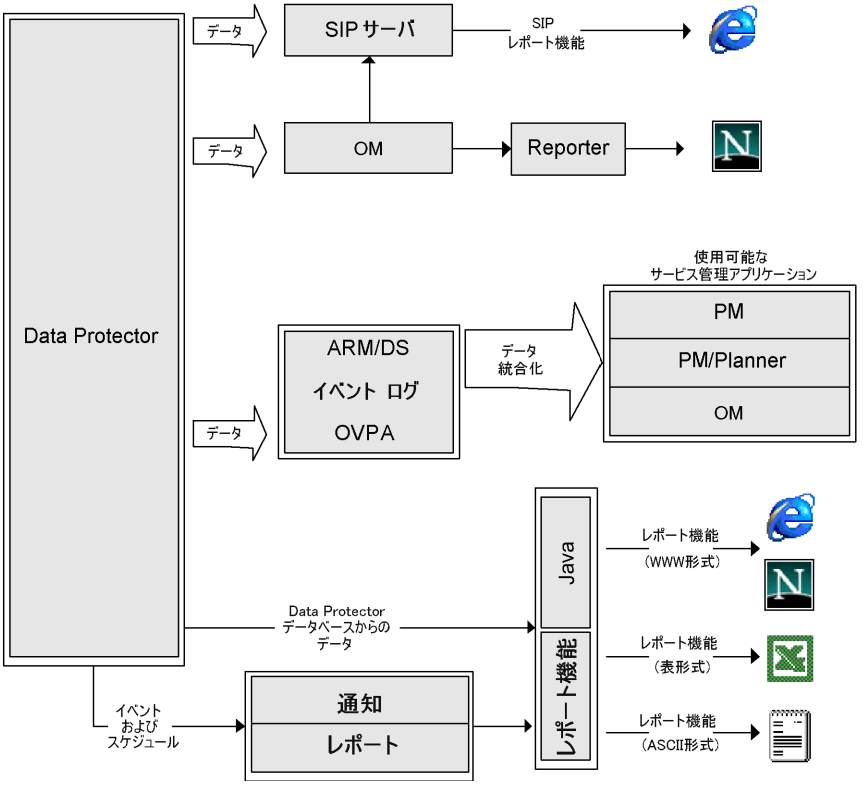


図 58 サービス管理における情報の流れ

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、たとえば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、オンラインヘルプの索引「ARM統合ソフトウェア、インストール」を参照してください。

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トラップの構成の詳細については、オンラインヘルプの索引「SNMP、レポートの送信方法」を参照してください。

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。たとえば、保護されていないシステムに関する情報を示す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。たとえば、Data Protectorライセンスの使用状況を示すライセンス レポートや、バックアップ、オブジェクトコピー、またはオブジェクト集約に現在使われていないために使用可能なデバイスの一覧を示すdev_unusedレポートなど。
- 問題関連レポート。たとえば、バックアップ、コピー、および集約に失敗したセッションに関連する情報を示す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、たとえば、指定した時間帯に実行されたセッションに関するレポート、IDBレポート、デバイス使用状況レポートなどを作成できます。
- これらのレポートはパラメータを指定してカスタマイズすることもできます(対象となる時間帯、バックアップ、コピー、および集約の仕様、バックアップ グループなど)。
- さまざまな出力形式を選択できます(ASCII、HTML、スプレッドシート互換形式など)。
- これらのレポートに対して、Data Protectorの組み込みスケジューラを使ったスケジューリングも可能です。
- 何らかのイベントに基づいて、これらのレポート送信を開始することも可能です(デバイス障害、マウント要求、セッションの終了時など)。

- さまざまな配布方法の中から、レポートを受け取る方法を選択できます(電子メール、SNMP、Windowsでのみ可能なブロードキャスト、ファイルへの書き込み、外部コマンドへの送信など)。

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

以下にいくつかの例を示します。

レポートと通知の例

- 毎朝7:00に、24時間以内に実行されたバックアップ、コピー、および集約の各セッションに関するレポートを作成し、これをASCII形式の電子メールの形でバックアップ管理者のメールボックスに送信します。さらに同じレポートを、Webサーバー上にHTMLファイル形式で書き込んで、他のユーザーもこの情報を利用できるようにします。
- デバイス障害やマウント要求が発生した場合は、ブロードキャストメッセージをただちにバックアップ管理者のWindowsワークステーションに送信し、さらに外部コマンドを開始して、バックアップ管理者のポケットベルを呼び出します。
- バックアップセッションの終了時には、バックアップされたシステムを所有しているエンドユーザーに、バックアップ状態を示すレポートを、ASCII形式の電子メールで送信します。

イベントロギングと通知

Data Protectorのイベントログは、Data Protector関連の通知すべてを管理する中央レポジトリです。Data Protectorの組み込み通知エンジンは、ログエントリに基づいて、警報の送信やData Protectorレポート機構の開始などを実行します。イベントログは、Data ProtectorやHPソフトウェア管理アプリケーションでSLAへの適合を示すレポートを生成するための情報ソースとなります。さらにレポート機能に加えて、ログエントリからHPソフトウェア管理アプリケーションにData Protector SPI(SMARTプラグイン)経由で情報を提供することにより、予防処置や修正処置を実施することも可能です。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サーバーを介して使用するか、直接アクセスできるようにクライアントマシンにコピーするか、またはローカルマシン上で使用してください。この機能の使用には、サポートされているWebブラウザのみが必要です。Data Protector GUIをシステムにインストールする必要はありません。Javaレポート機能を使用すると、レポートにオンラインアクセスできるだけでなく、新しいレポートをスケジュールに追加したり、レポートのパラメータを変更したりするなど、レポート体系に対する構成作業も可能になります。

Data Protectorのチェックおよび保守の機構

Data Protectorには日常のセルフチェックや保守のための、さまざまな自動化された機構が備わっており、処理の信頼性や予測可能性の向上に役立っています。Data Protector’のセルフチェックや保守の処理には次のものがあります。

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

詳細は、オンラインヘルプの索引「Data Protector”が実行するチェック」を参照してください。

中央管理、分散環境

Data ProtectorのMoM機能を使用すると、管理者は複数のData Protector Cell Managerから構成される企業環境を一元管理することができます。MoMシステム管理者は、単一のコンソールから、企業全体にわたる構成、メディア管理、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、オンラインヘルプの索引「MoM環境」を参照してください。

Data Protectorが提供するデータの使用

データの用途

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

- 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サーバーに書き込まれ、各ユーザーが必要に応じて使用できるようになります(Data Protector組み込みレポート機能のHTMLレポート作成機能を使用)。

- Data Protectorの主要かつ重大なイベントを、HP Network Node Managerなどのネットワーク管理ソフトウェアに送信できます(Data Protector組み込み通知エンジンのSNMPトラップ送信機能を使用)。

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

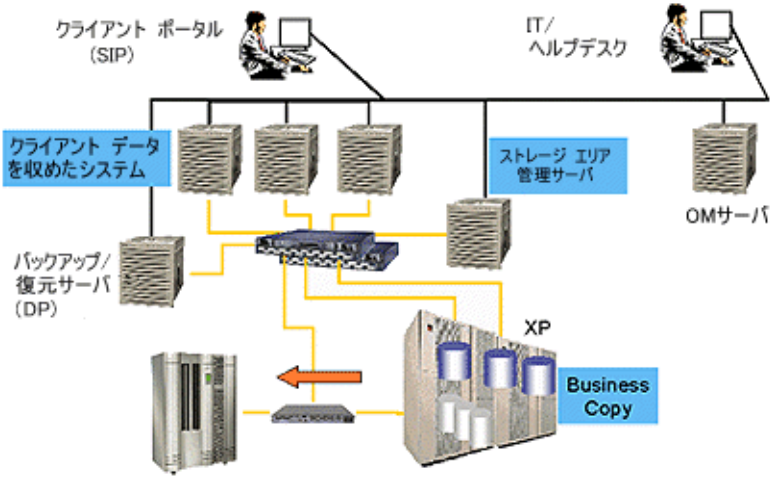


図 59 クライアントポータルを介してサービス管理にアクセスするITサービスプロバイダ環境の例

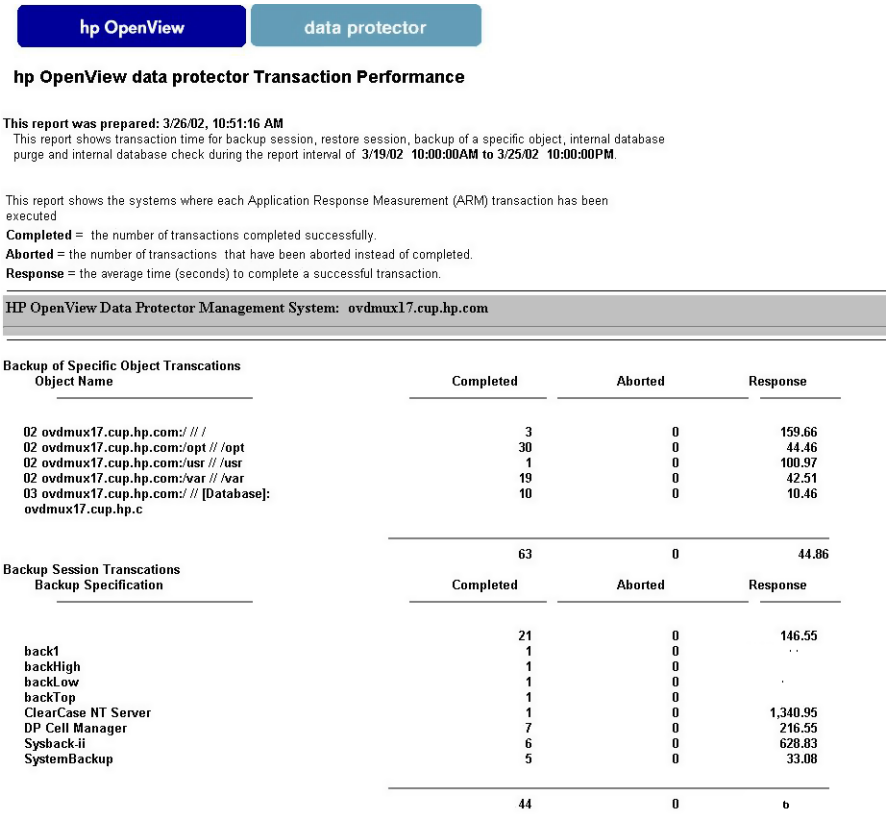
Data Protector OM-Rの統合

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。たとえば、「“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。たとえば、「“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。

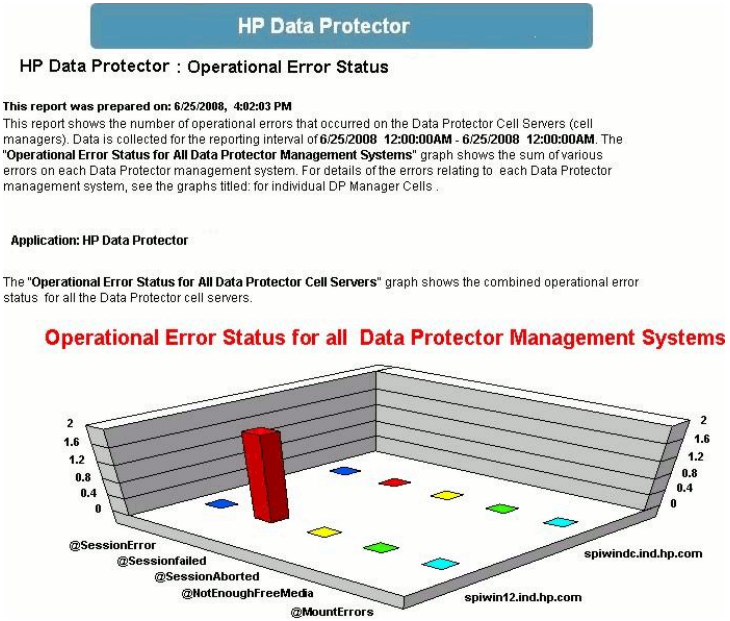
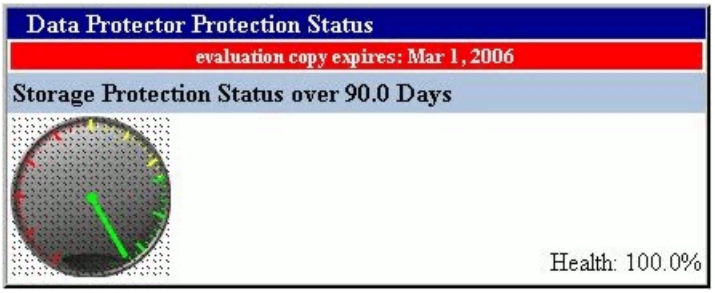


図 61 Operational Error Statusレポート

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。



Data Protector Reports

evaluation copy expires: Mar 1, 2006

Data List Tree Report

Backup Specification	Object Type	Client Host	Mountpoint	Tree
New1	Windows FS	fagus.india.hp.com	/C	C:/backup/Backup.4BP
New1	Windows FS	fagus.india.hp.com	/C	C:/backup/MediaDB005.4BK
New1	Windows FS	fagus.india.hp.com	/C	C:/backup/MediaDB005.4BR
New1	Windows FS	fagus.india.hp.com	/C	C:/backup/MediaDB006.4BK
New2	Windows FS	alder.india.hp.com	/C	C:/BuildsNPatches
Test3	Windows FS	fagus.india.hp.com	/C	C:/j2sdk1.4.1_03

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。
KMS	KMS(Key Management Server)プロセス(サービス)は、Cell Manager上で動作し、Data Protectorの暗号化機能のためのキー管理を提供します。このプロセスは、Data ProtectorをCell Managerにインストールしたときに開始されます。
MMD	MMD (Media Management Daemon)プロセス(サービス)は、Data Protector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(233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。

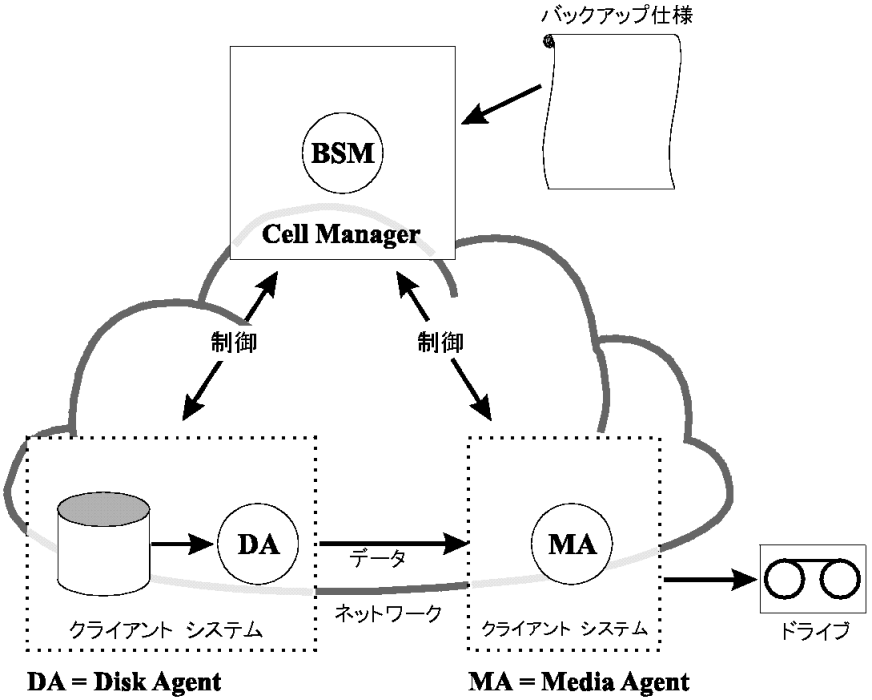


図 63 バックアップセッションにおける情報の流れ(1)

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(234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。

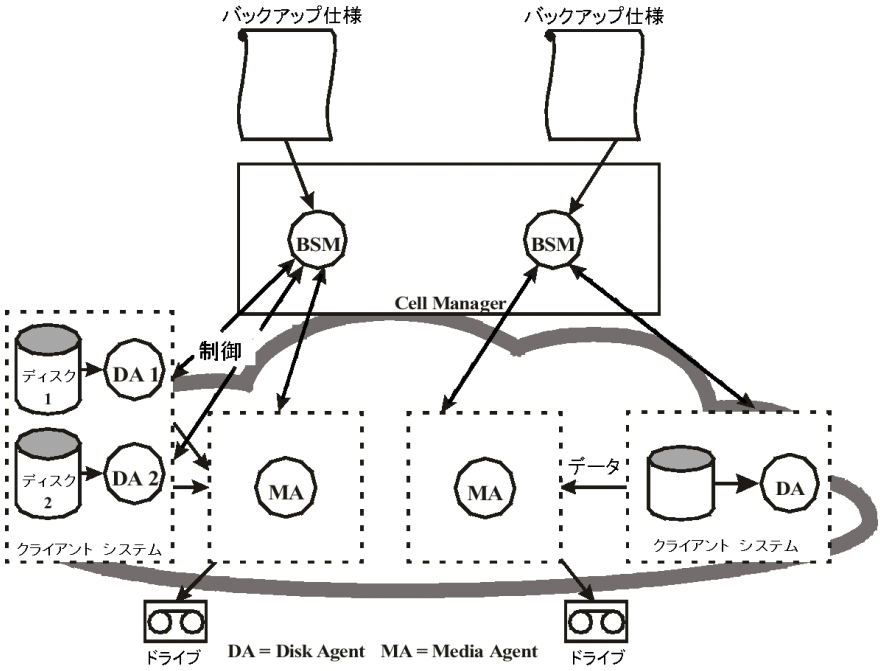


図 64 バックアップセッションにおける情報の流れ－複数のセッション

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」(156ページ)および「バックアップ用メディアの選択 」(155ページ)を参照してください。

マウント要求への対応

マウント要求に対応するには、要求されたメディアをセットし、バックアップ処理を続行するようData Protectorに指示します。

Data Protectorでは、マウント要求が発行された場合の動作を、次のような形で事前に設定できます。

オペレータに通知を送付

Data Protectorの通知機能を使って、マウント要求に関する情報をオペレータに電子メールで送信することができます。オペレータはこの情報に基づいて、必要なメディアを手動でロードしたり、セッションを停止したりするなど、何らかの適切な操作を行います。詳細は、「レポートと通知」(221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(238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。詳細は、「並行復元」(239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。

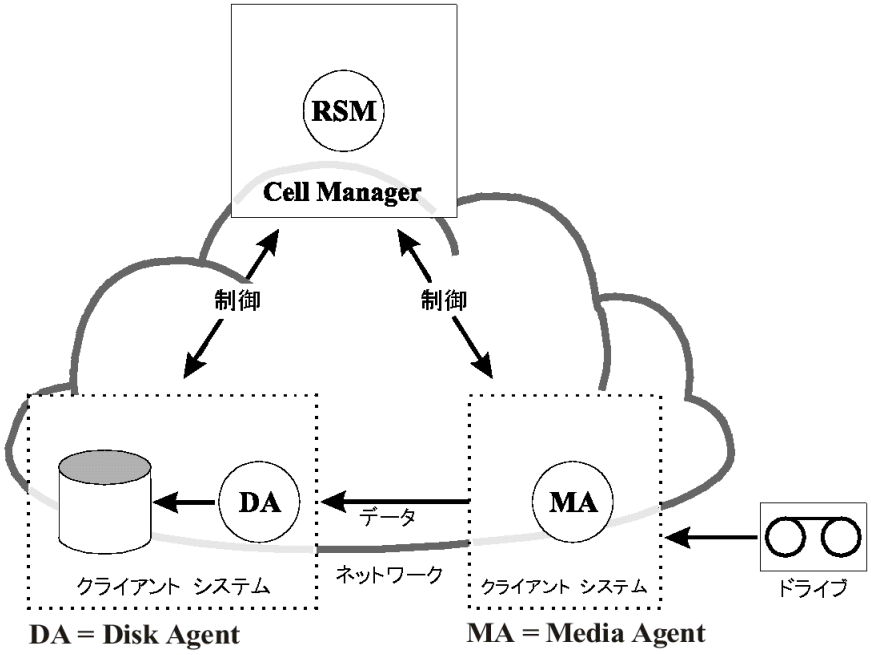


図 65 復元セッションの情報フロー

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。詳細は、図66（240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。（図41（157ページ）を参照）。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。

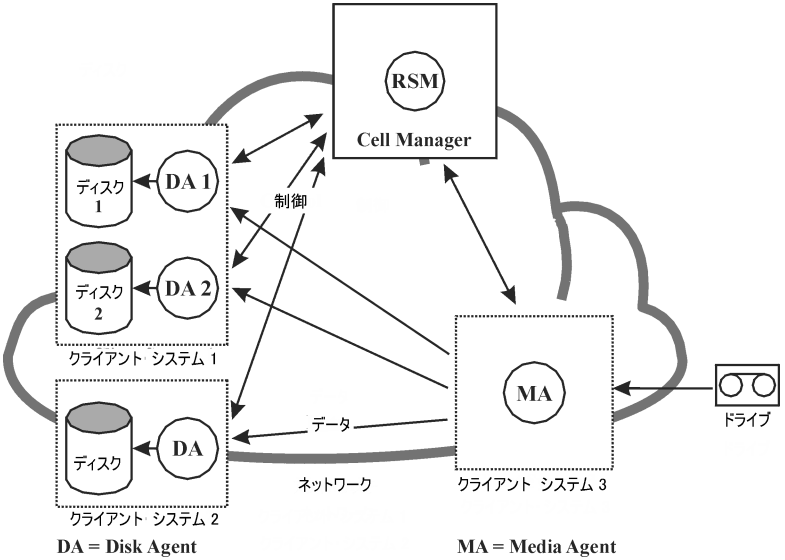


図 66 並行復元セッションのフロー

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。

復元セッションの再開

ネットワークの問題などによって正常に完了しなかった復元セッションは、Data Protector再開セッション機能を使用して再開できます。失敗したセッションを再開すると、Data

Protectorは、失敗したセッションが中止したところから新規セッションで復元を続行します。

オブジェクトコピーセッション

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

オブジェクトコピーセッションとは

オブジェクトコピーセッションとは、バックアップ、コピー、または集約されたデータの追加コピーを別のメディアセット上に作成するプロセスです。オブジェクトコピーセッション中に、選択されたバックアップ、コピー、または集約オブジェクトがソースからターゲットメディアへコピーされます。

自動および対話形式のオブジェクトコピーセッション

自動オブジェクトコピーセッション

自動オブジェクトコピーセッションは、スケジュールを設定して開始することも、バックアップ、オブジェクトコピー、またはオブジェクト集約の直後に開始することも可能です。スケジュール方式のオブジェクトコピーセッションは、Data Protectorスケジューラで指定した時刻に開始されます。一方、ポストバックアップ、ポストコピー、またはポスト集約オブジェクトコピーセッションは、指定したセッションの終了後に開始されます。自動オブジェクトコピーセッションの進行状況は、Data Protectorモニターで確認できます。

対話形式のオブジェクトコピーセッション

対話形式のオブジェクトコピーセッションは、Data Protectorユーザーインタフェースを使用してオペレータが直接開始します。Data Protectorモニターがすぐに起動され、セッションの進行状況を参照できます。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（243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. 正常にコピーされたすべてのオブジェクトに対して、CSMは、コピーセッションに指定されたオプションに従ってIDB保護エントリを更新します。

   セッションにリサイクルオプションが指定されている場合、リサイクルを可能にするために失敗したソースオブジェクトの保護も更新されます。
8. オブジェクトコピーセッションが終了したら、CSMによりセッションが閉じられます。

同時に実行できるセッションの数

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

ただし、同じオブジェクトコピー仕様から2つ以上のオブジェクトコピー セッションを並行して実行することはできません。

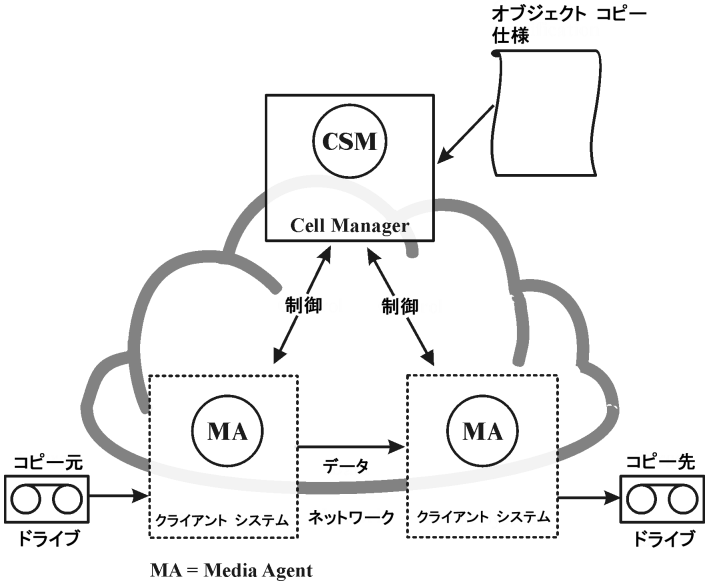


図 67 オブジェクトコピーセッションにおける情報の流れ

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 (273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。

   あて先デバイスがオブジェクトに対して指定されていない場合は、ユーザーが以下に記載順の優先順位に従ってオブジェクト集約仕様で選択した中から、Data Protectorによって自動的に選択されます。

   - ソースデバイスと同じブロックサイズを持つあて先デバイスが、異なるブロックサイズのものより先に選択される
   - ネットワーク接続デバイスより、ローカル接続デバイスが先に選択される

5. 1つのMedia Agentが、フルオブジェクトバージョンを読み込みます。このMedia Agentは、増分オブジェクトバージョンを読み込む別のMedia Agentにデータを送信します。この2つ目のMedia Agentが実際の統合を行い、ターゲットメディアにデータを書き込むMedia Agentにデータを送信します。

   フルバックアップと増分バックアップが同じファイルライブラリにある場合、同じMedia Agentがすべてのバックアップを読み込んでこれらを統合します。

   ソースデバイスのブロックサイズが、あて先デバイスのブロックサイズよりも小さい場合は、ブロックが再パッケージされます。

6. オブジェクト集約セッションが終了したら、CSMによりセッションが閉じられます。

同時に実行できるセッションの数

セル内では同時に複数のオブジェクト集約セッションを実行できます。オブジェクト集約セッションは、バックアップセッションと同じように扱われ、最大数も同じ要因で制限されます。

オブジェクト集約セッションにおける待ち行列

タイムアウト

オブジェクト集約セッションが開始されると、Data Protectorにより、必要なすべてのリソースの割り当てが試行されます。いずれかのリソースが使用できるようになるまで、セッションは待ち行列に入れられます。タイムアウトになってもリソースがまだ使用できない場合は、そのセッションは中止されます。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。

オブジェクト検証セッション

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

オブジェクト検証セッションとは

オブジェクト検証セッションは、指定したオブジェクトに割り当てられたメディアセグメントを検証するプロセスで、ヘッダーセグメント内の情報を確認し、フォーマットを検証するためにデータセグメント内のデータブロックを読み取ります。オリジナルのバックアップ中に巡回冗長検査(CRC)が実行された場合、CRCの再計算およびオリジナルとの比較も行われます。

Data Protectorは、バックアップのソースであったホスト上でオブジェクトの検証を実行し、復元パス内のData Protectorコンポーネントの効率的な検証、別のホスト上にある別の保存場所への復元能力の検証、または関係するメディアエージェントのあるホスト上で直接、データのみの検証を行うことができます。

自動および対話型オブジェクト検証セッション

自動オブジェクト検証セッション

自動オブジェクト検証セッションは、Data Protectorスケジューラを使用して指定した時間に実行するか、あるいは指定したバックアップ、オブジェクトコピー、またはオブジェクト集約セッションの完了直後にバックアップ後のオブジェクト検証セッションとして実行するよう指定できます。Data Protectorモニターでこのようなセッションの進行状況をモニタリングできます。

対話型オブジェクト検証セッション

対話型オブジェクト検証セッションは、Data Protectorのユーザーインタフェースから直接開始できます。Data Protectorモニターがすぐに起動され、セッションの進行状況をモニタリングできます。複数のユーザーが同一のオブジェクト検証セッションをモニタリングすることも可能です。ユーザーインタフェースを使って他の操作を実行し、必要に応じてセッションをバックグラウンドで続行させることができます。

オブジェクト検証セッションにおけるデータフローとプロセス

オブジェクト検証セッション中の処理内容

オブジェクト検証セッションを開始する場合、基本のプロセスフローは以下のようになります。

1. Restore Session Manager (RSM)プロセスは、Cell Managerシステム上で開始され、以下のいずれかによってトリガされます。
   - スケジュール設定されたセッションの場合、Data Protectorのスケジューラ
   - バックアップ後のセッションの場合、End of Sessionイベント
   - 対話形式のセッションの場合、GUIまたはCLIからのユーザー

   このプロセスにより、検証セッションが制御されます。
2. RSMによりIDBがオープンされて、検証するオブジェクトに関する情報が読み取られるほか、検証セッションに関する情報(生成されるメッセージなど)がIDBに書き込まれます。
3. RSMにより、オブジェクトの検証に関係するソースシステム上でMedia Agent (MA)が起動されます。並行して使用される各ドライブで、新たにMedia Agentが起動されます。
4. あて先ホスト上のDisk Agents (DA)によりデータ検証が実行され、これにより並行して使用される各あて先ディスクに対してRSMによりDisk Agentが起動されます。起動されるDisk Agentの実際の数は、検証を選択したオブジェクトに依存します。このプロセスは、復元の場合と同様です。詳細は、「並列復元」???を参照してください。
5. Media Agentはメディアからオブジェクトデータを読み取り、オブジェクトの検証を実行するDisk Agentに送信します。RSMにより、セッションの進行状況がモニターされ、必要に応じて新規のDisk AgentやMedia Agentが起動されます。
6. オブジェクト検証セッションが完了すると、RSMによりセッションがクローズされます。

オブジェクト検証を使用するプロセスフローのバリエーション

オブジェクト検証プロセスでは、復元のためにデータが要求されたポイントから、データがあて先ホストに到達したポイントまでの復元処理がエミュレートされます。そのポイントを超えると、検証プロセスによるデータの書き込みは行われず、アプリケーション統合オブジェクトの場合、アプリケーション統合とのやり取りは行われません。

メディア管理セッション

メディア管理セッションとは

メディア管理セッションは、メディアの初期化、内容のスキャン、メディア上のデータの検証、メディアのコピーなど、メディアに対する特定の操作を行う場合に実行されます。

IDBへのログの記録

生成されたメッセージなど、メディア管理セッションに関する情報が、IDB内に保存されます。

Data Protectorモニターとメディア管理セッション

メディア管理セッションは、モニターウィンドウを使ってモニタリングできます。Data Protector GUIを閉じると、セッションはバックグラウンドで実行されます。

メディア管理セッションにおけるデータフロー

メディア管理セッション中の処理内容

メディア管理セッションが開始されると、以下の処理が実行されます。

1. 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、http://www.hp.com/support/manuals を参照してください。

データベース操作の概要

ユーザーから見ると、**データベース**は、情報を1つに集めたものです。データベース内のデータは、**テーブル**内に保存されています。.リレーショナルテーブルは複数の列で構成され、各テーブルにはそれぞれ名前がつけられています。データはテーブル内の各行に保存されます。テーブルは相互に関連付けることができ、データベースという形で実際の関連付けが行われます。データはこのように**リレーショナル形式**で保存することも、抽象データ型やメソッドのような**オブジェクト指向**の構造として保存することもできます。また、オブジェクトを他のオブジェクトと関連付けたり、オブジェクト内に他のオブジェクトを包含することも可能です。データベースは通常サーバー(マネージャ)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。

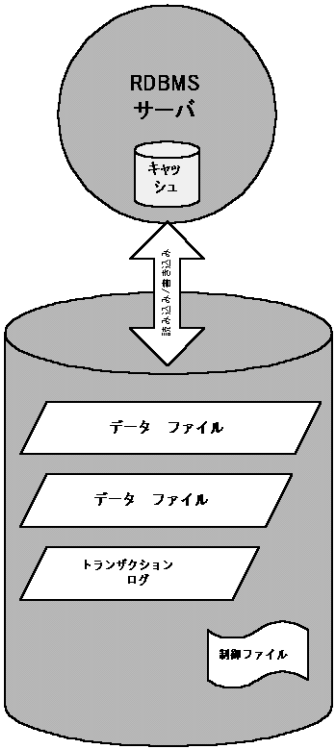


図 68 リレーショナルデータベース

図68 (252ページ) は、典型的なリレーショナルデータベースと、その内部にある以下の構造を示したものです。

データファイルは、データベース内のすべてのデータが保存される物理ファイルです。データファイルはランダムに変更され、非常に大容量になる可能性があります。物理ファイルの内部は、複数のページに分割されています。

トランザクションログには、すべてのデータベーストランザクションが処理を続行する前に、最初にそれらのトランザクションが保存されます。なんらかの障害により変更データをデータファイルに永久に書き込めなくなった場合も、このログファイルから変更情報を取得できます。復旧処理を行う場合は、必ず次の2つの作業が必要になります。1つ目はトランザクションをメインデータベースに適用する作業で、**ロールフォワード**と呼ばれます。2つ目はコミットされていないトランザクションを削除する作業で、**ロールバック**と呼ばれます。

制御ファイル には、データベースの物理構造、たとえば、データベースの名前、データベースに所属するデータファイルやログファイルの名前と場所、データベース作成時のタイムスタンプなどが保存されています。この制御データは、制御ファイルに保存されます。これらのファイルは、データベースの操作に非常に重要です。

データベースサーバープロセスの**キャッシュ**内には、データファイルの中の使用頻度の高いページが保存されます。

以下に、標準的なトランザクション処理手順を示します。

1. 最初に、トランザクションがトランザクションログに記録されます。
2. 次に、トランザクションにより要求された変更内容が、キャッシュ内のページに適用されます。
3. 変更されたページは、ディスク上のデータファイルに随時一括して書き込まれます。

データベースおよびアプリケーションのファイルシステムバックアップ

オンライン状態のデータベースは絶えず変更されています。またデータベースサーバーは、接続ユーザーへの迅速な応答や性能の向上を図るために、複数のコンポーネントで構成されています。たとえばデータの中には、内部キャッシュメモリや一時的なログファイルに保存されているものもあります。これらのデータは、**チェックポイント**でディスクに一括して書き込まれます。

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

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

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

この方法は、比較的理解と構成が容易ですが、主な欠点が1つあります。*それは、バックアップ中にデータベースにアクセスできないことです。* これは、ほとんどのビジネス環境で、受け入れられることではありません。

データベースおよびアプリケーションのオンラインバックアップ

バックアップ中にもデータベースを停止せずに済むように、各データベースベンダーでは、データベースを一時的に特殊モードにしてデータをテープに保存できるようにするためのインタフェースを用意しています。これらのインタフェースを使用すると、バックアップ中または復元中もサーバーアプリケーションをオンライン状態のままにでき、ユーザーの利用が引き続き可能になります。Data Protectorを始めとするバックアップ製品では、これらのアプリケーション固有のインタフェースを使って、データベースアプリケーションの論理ユニットのバックアップや復元を実行できます。バックアップAPIの機能はデータベースベンダーによって異なります。Data Protectorの統合機能は、主要なデータベースおよびアプリケーションで利用可能です。サポートされている統合機能一覧については、『*HP Data Protector 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。

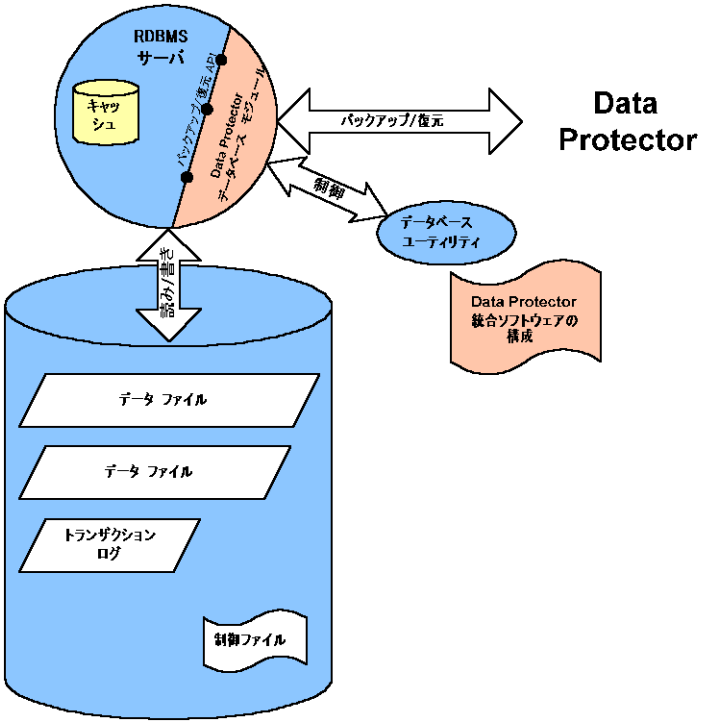


図 69 Data Protectorとデータベースの統合

図69 (255ページ) は、リレーショナルデータベースとData Protectorの統合方法を示したものです。Data Protectorでは、データベースサーバーにリンクされる**データベースライブラリ**が提供されます。データベースサーバーは、Data Protectorに対してデータを送信したり、データを要求したりします。データベースユーティリティは、バックアップ処理や復元処理の開始に使用されます。

以下に、Data Protectorの統合機能を使用してデータベースをバックアップするための典型的な構成手順を示します。

1. データベース/アプリケーション固有のエージェントを、データベースシステムにインストールします。
2. データベースごとに、Data Protectorの統合ソフトウェアを構成します。Data Protectorでデータベースを処理するために必要なデータは、データベースシステムの構成ファイルまたはレジストリエントリに保存されます。通常、この情報には、パス名や、ユーザーの名前とパスワードが含まれます。
3. Data Protectorのユーザーインタフェースを使用して、バックアップ仕様を準備します。

データベースとData Protector統合ソフトウェアを使用すると、データベースを常に**オンライン**状態に保てるだけでなく、以下の利点もあります。

- データファイルの場所を指定する必要はありません。これらは、異なるディスク上に置くことができます。
- データベースの論理構造をブラウズできます。データベース中のあるサブセットのみを選択することも可能です。
- アプリケーション側でバックアップ操作を感知して、どの部分がバックアップされたかを追跡できます。
- 複数モードによるバックアップが可能です。**フル** バックアップのほかにも、(ブロックレベルの)**増分**バックアップやトランザクションログのみのバックアップも選択できます。
- 複数のモードによる復元が可能です。またデータファイルの復元後に、データベースにより自動的にトランザクションログを復元し、構成内容に従ってそれらのトランザクションをデータベースに適用することもできます。

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.06.11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」(264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」(262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（260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。

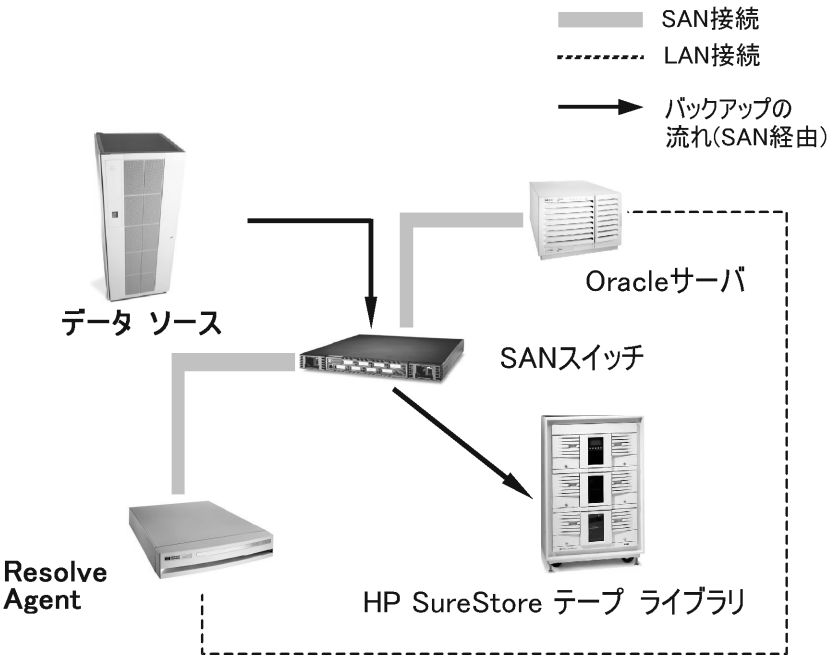


図 70 ダイレクト バックアップのアーキテクチャ

[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」（264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」(264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。

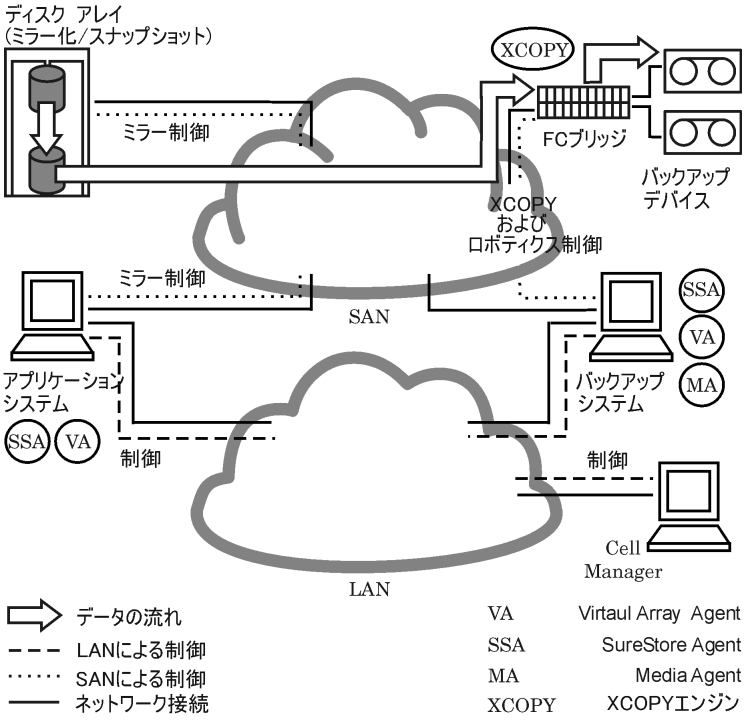


図 71 3台のホストによる基本的な構成

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 ヘルプの索引「ファイル ライブラリ デバイス」を参照してください。

データ フォーマット

ディスクベース デバイス用のデータ フォーマットは、テープ用のデータ フォーマットに基づいています。Data Protectorでは、ディスクベースのデバイスにバックアップ データを書き込む前に、そのデータをテープ用のフォーマットに変換します。

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

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。

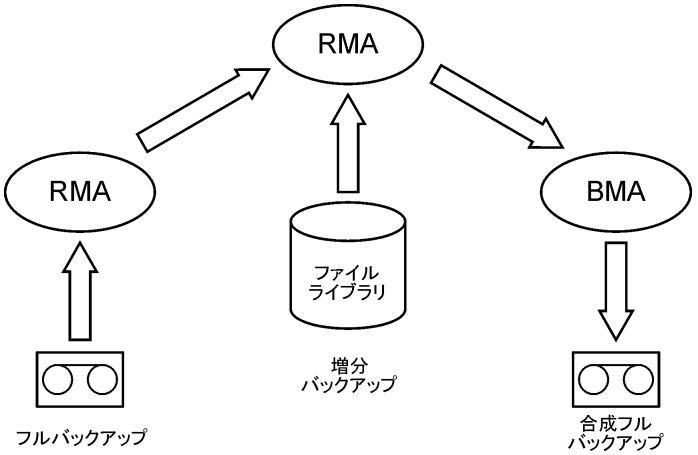


図 72 合成バックアップ

図72 (275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。

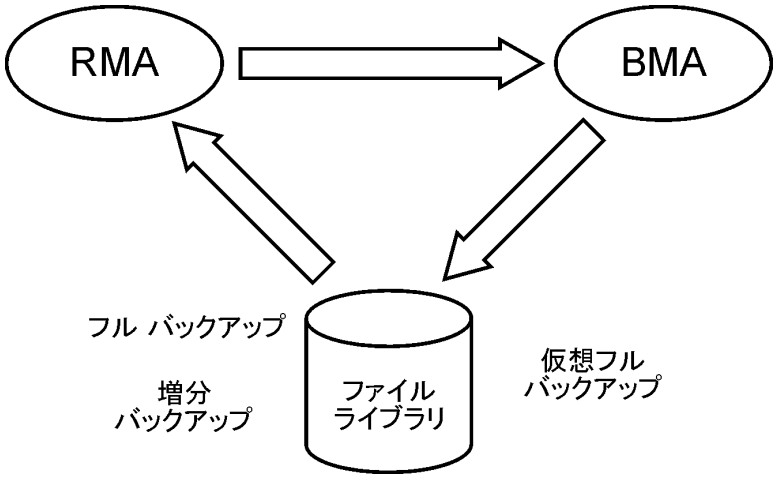


図 73 仮想フル バックアップ

図73 (276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。

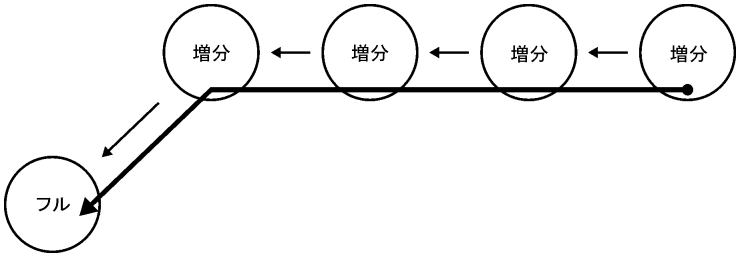


図 74 フル バックアップと増分バックアップ

図74(277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。

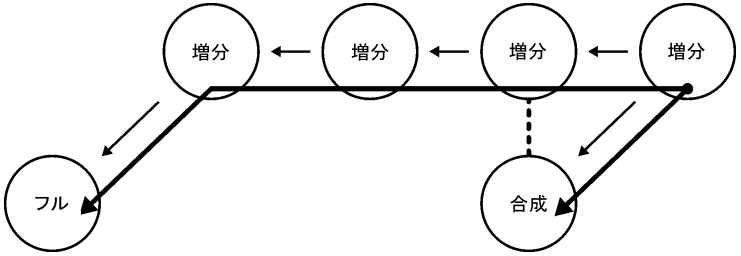


図 75 合成バックアップ

図75(277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。

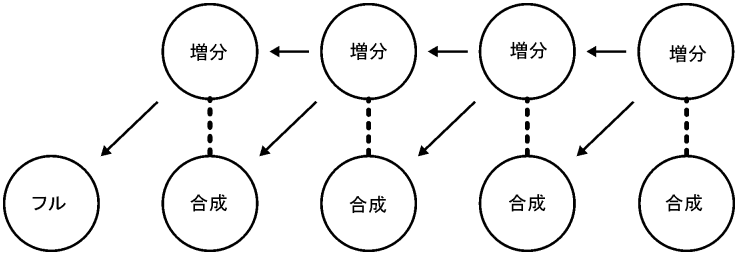


図 76 通常の合成バックアップ

図76 (278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。

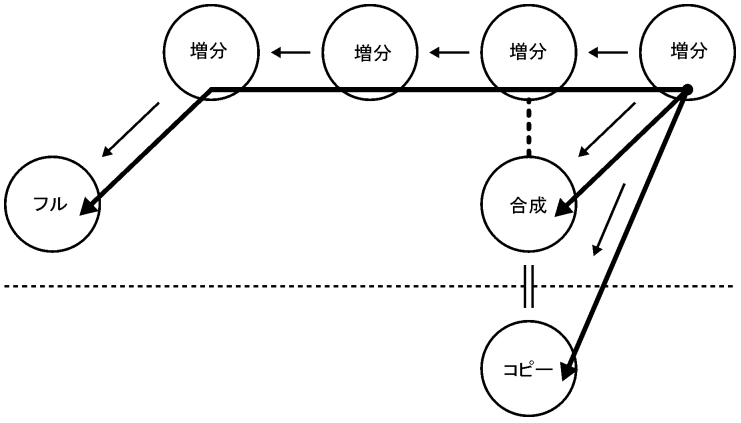


図 77 合成バックアップとオブジェクト コピー

図77 (278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。(図78(282ページ)を参照)。

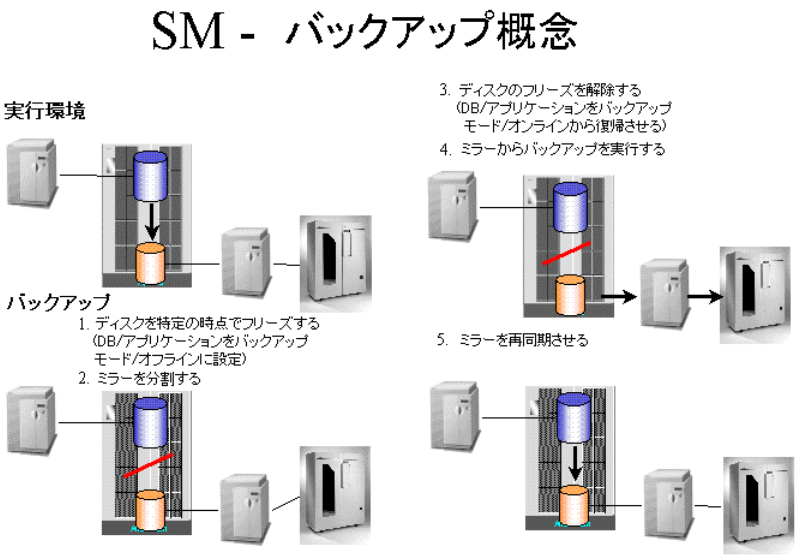


図 78 スプリット ミラー バックアップの概念

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

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。

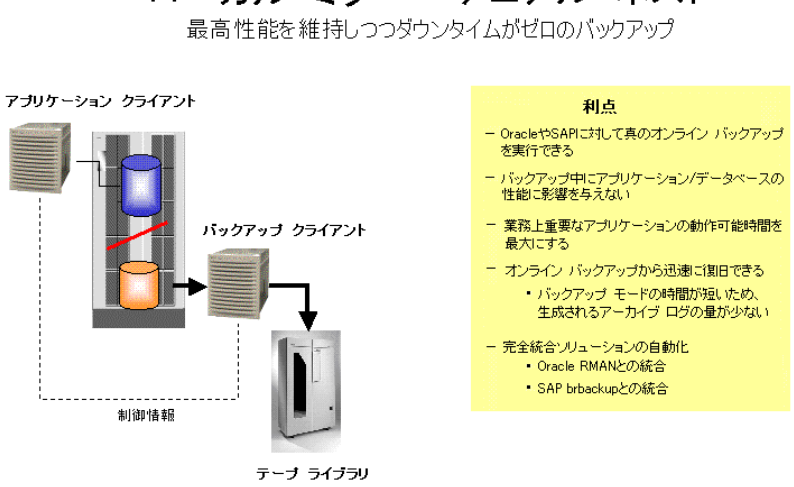


図 79 ローカル ミラー(デュアル ホスト、最高性能時でダウンタイムがゼロのバックアップ)

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。

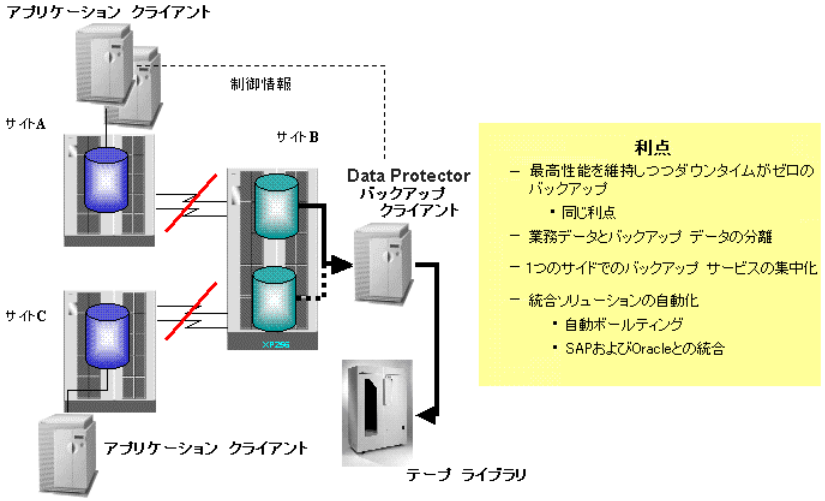


図 80 スプリット ミラー – リモート ミラー(LAN を経由しないリモート バックアップとデータの高可用性)

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。

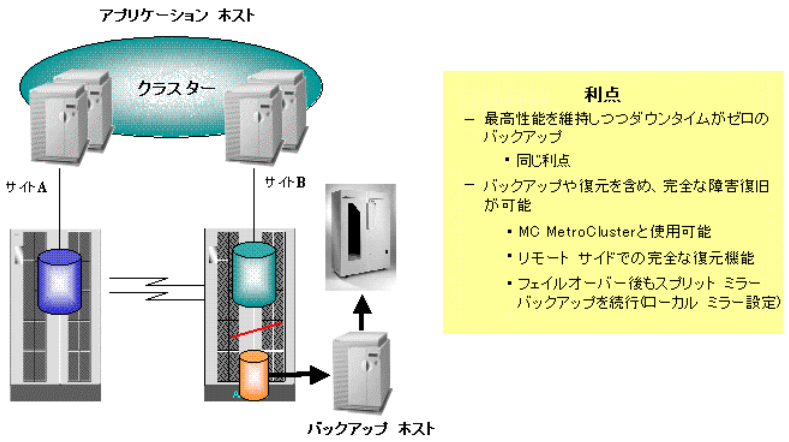


図 81 ローカル ミラーとリモート ミラーを組み合わせて使用(ディザスタ リカバリ統合バックアップ[サービスの高可用性 – HP-UXのみ])

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ー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。たとえば、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。

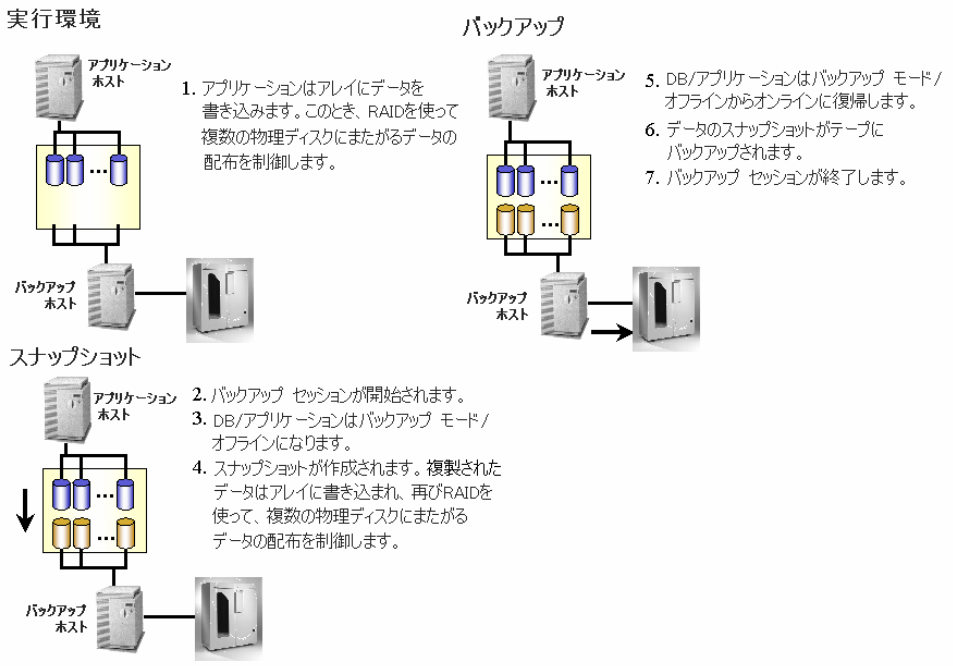


図 82 スナップショットバックアップ

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
- ディスクへのZDB
- ディスク/テープへの ZDB

テープへのZDBとディスク+テープへのZDB

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

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

ディスクへのZDB

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

インスタントリカバリ

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

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

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

複製セットと複製セットのローテーション

ディスクアレイ上に同時に保持できる複製の最大数は、使用するディスクアレイによって異なります。同一のバックアップ仕様に基づいてディスクアレイ上に保存されている複数の複製は、そのバックアップ仕様に対する**複製セット**を形成します。この複製セットは、特定のバックアップ仕様に基づいてディスクアレイ上に保存される複製の最大数によって定義されます。スナップショット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**と呼ばれます。

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、いつでもスナップクローンに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。

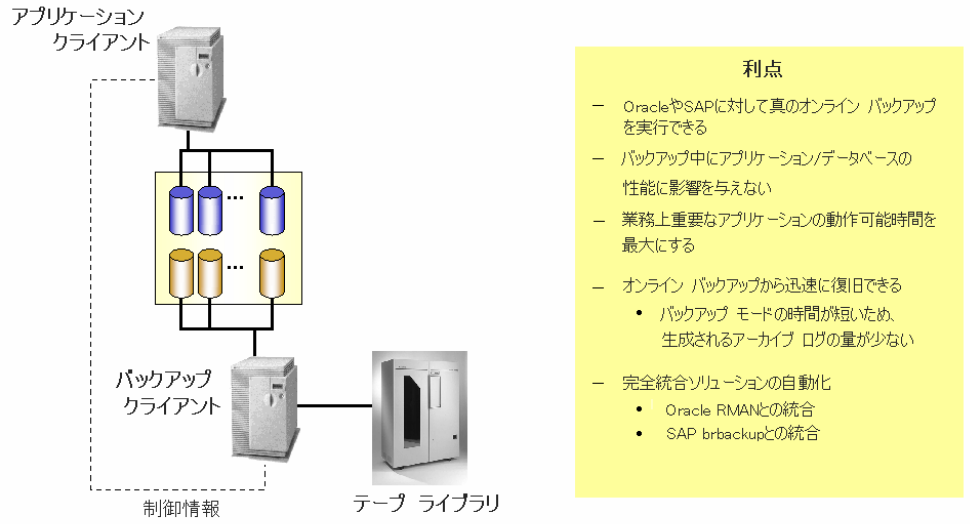


図 83 単一のディスクアレイ – デュアルホスト(最高性能、ゼロダウンタイムバックアップ)

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

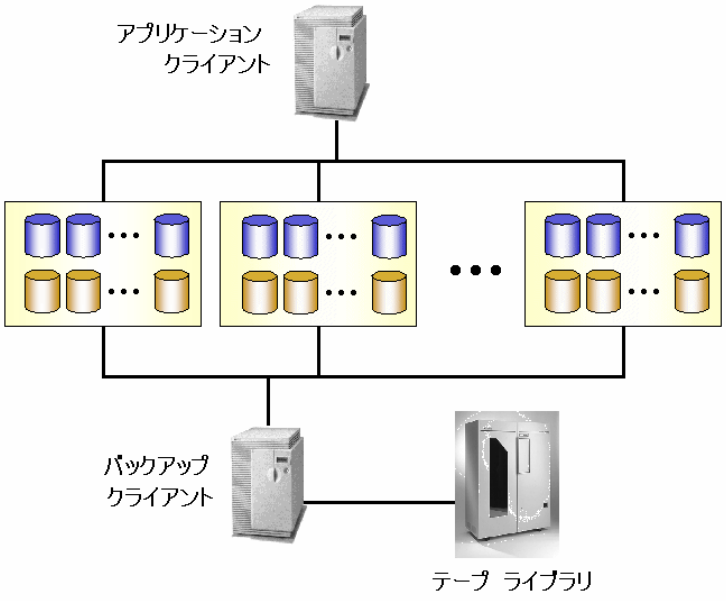


図 84 複数のディスクアレイ – デュアルホスト

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。

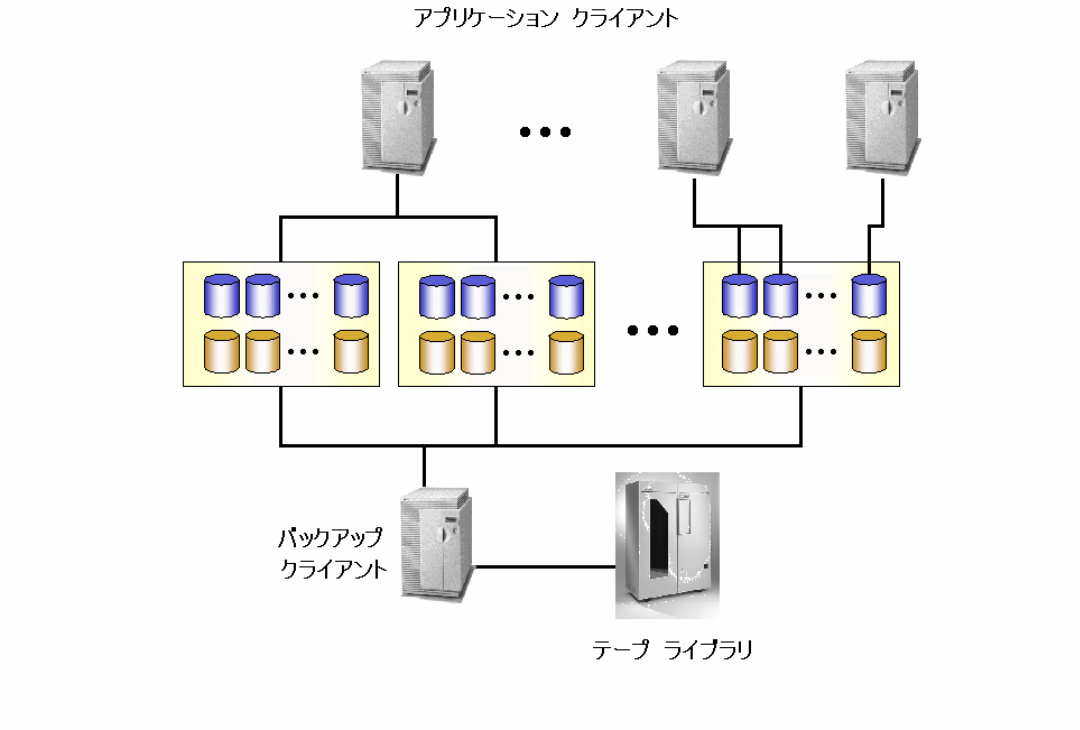


図 85 複数のアプリケーションホスト – シングルバックアップホスト

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。

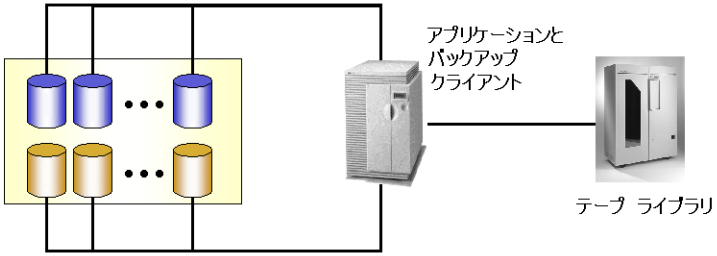


図 86 ディスクアレイ – シングルホスト

専用のバックアップサーバー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。たとえば、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。

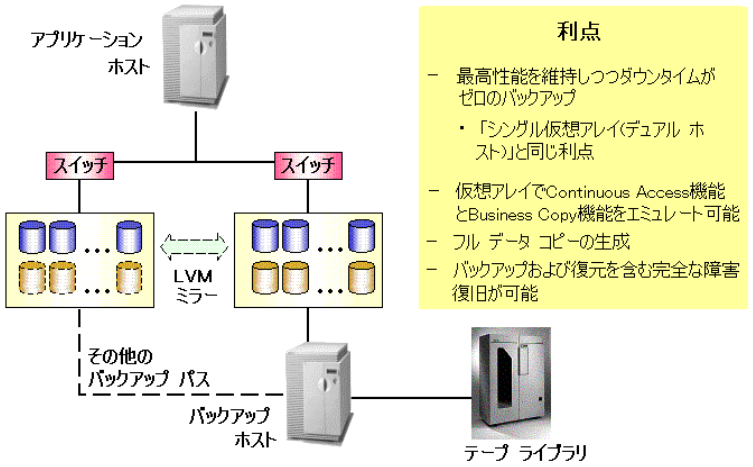


図 87 LVMミラー – HP StorageWorks Virtual Array のみ

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。

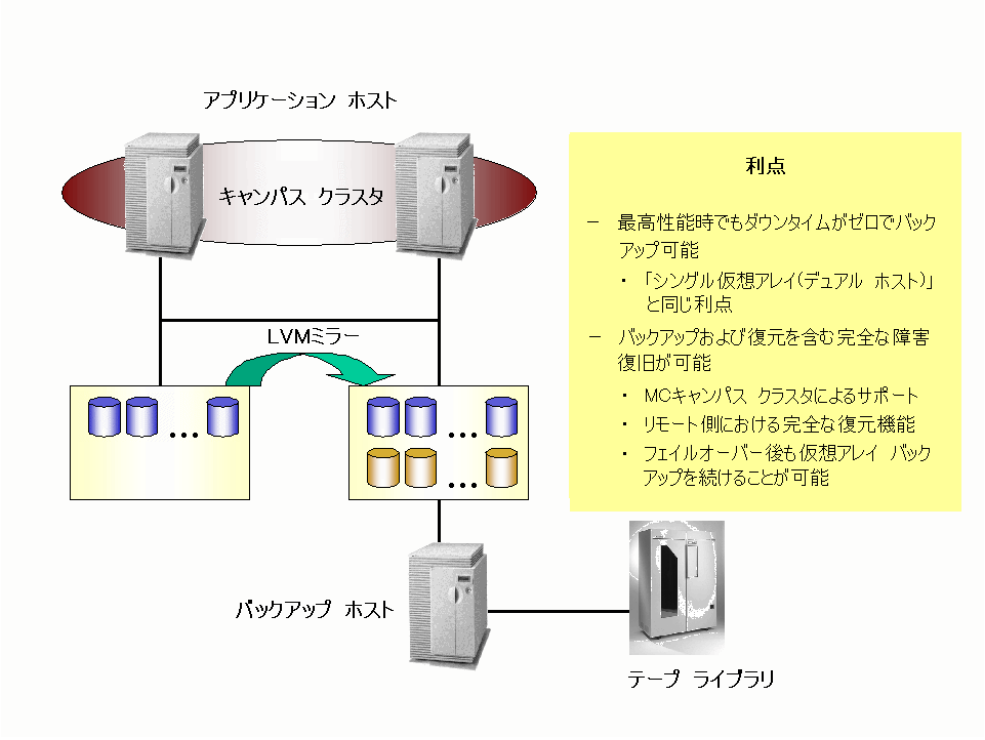


図 88 LVMミラーを使用するキャンパスクラスタ – HP StorageWorks Virtual Arrayのみ

この構成では、標準的なクラスター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ー

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ー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、別々のクラスター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については、以下の最新のサポート一覧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 (308ページ)と図90 (308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。

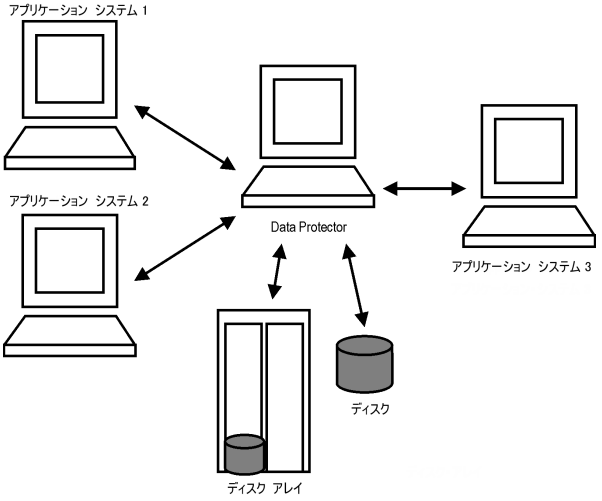


図 89 従来のバックアップ モデル

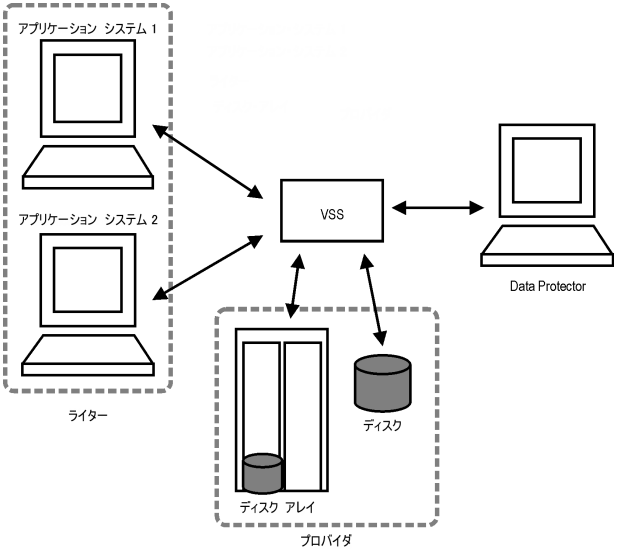


図 90 VSSバックアップ モデルに関係する要素

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「クラッシュ時整合状態」と呼んでいます。シャドウ コピー ボリュームの準備中には、VSSにより、保留中のすべてのI/O操作がコミットされ、新たな書き込み要求は保留されます。このようにしてシャドウ コピーの作成中はファイルシステム上のすべてのファイルが閉じられ、ロックは解除されます。

Microsoft 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。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(315ページ)に、また現在のバックアップ トポロジーは図91(316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

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
管理者	1 HP-UX	UX 5台	10GB	31GB	HP StorageWorks DAT24オートローダ 1台

図91 (316ページ)は、XYZ社のバックアップ環境を示したものです。

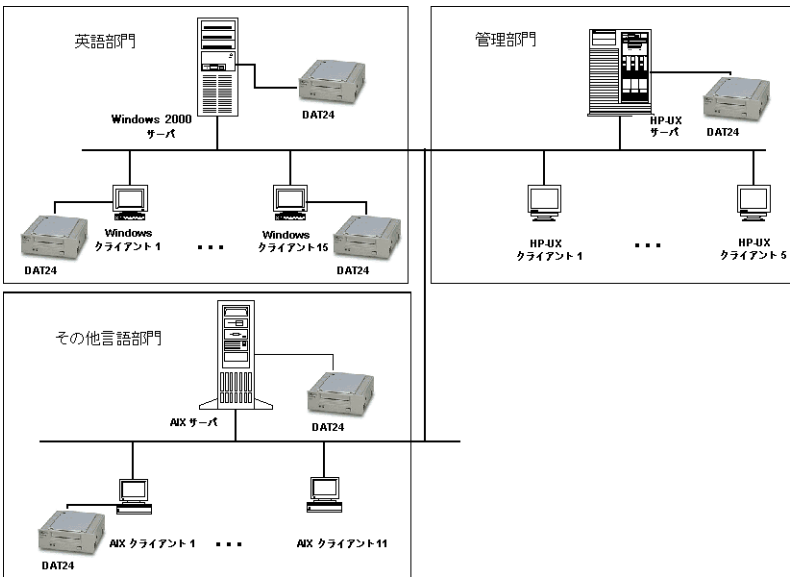


図 91 XYZ社の現在のバックアップ トポロジー

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」(313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。

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.06.11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 (320ページ)に示すとおりです。

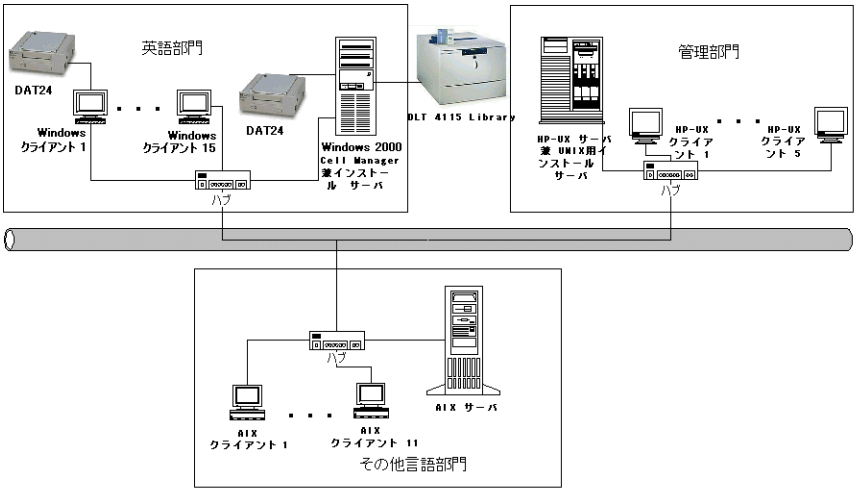


図 92 XYZ社のバックアップ トポロジー案

- 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 (321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(322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 (324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（329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（330ページ）に示すとおりです。

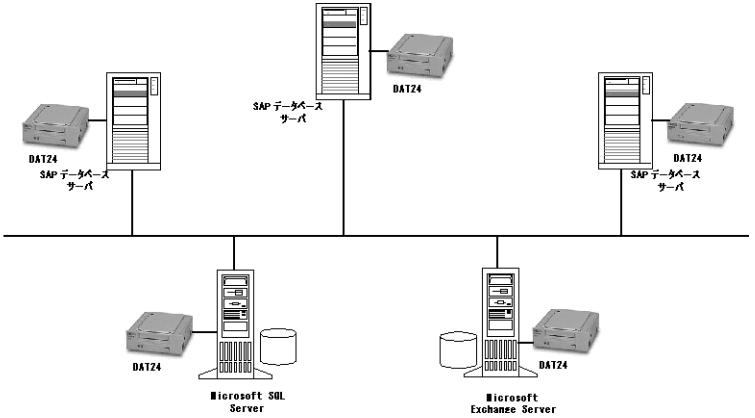


図 95 ABCケープタウンの現在のバックアップ トポロジー

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」(313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(332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(332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(330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(334ページ)に、この構成を示します。

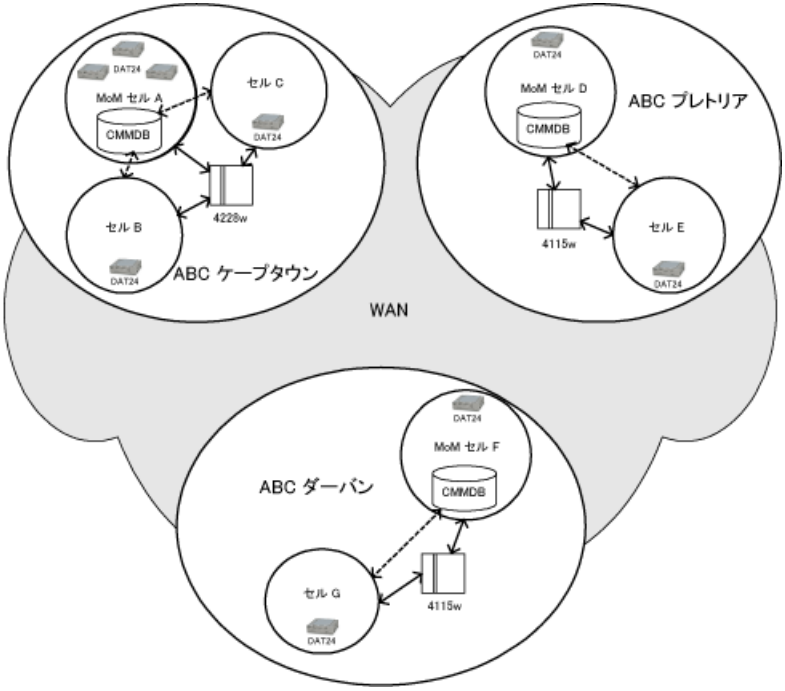


図 96 ABC社のバックアップ環境

これらの7つのセル内のCell ManagerとManager-of-Managers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(335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

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
	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Manager-of-Managers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（337ページ）に示すとおりです。

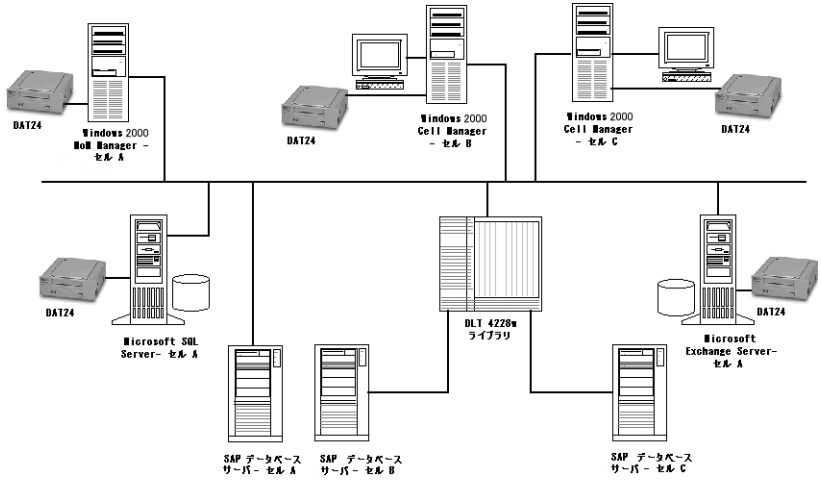


図 97 ABCケープタウンのバックアップ環境

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 (338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(339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 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。これらのデータベースはセルA、D、FのManager-of-Managers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。

- 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(343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(344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(344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 (344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

[名前]	セル	説明	バックアップ曜日	Time
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)]

  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(350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)。

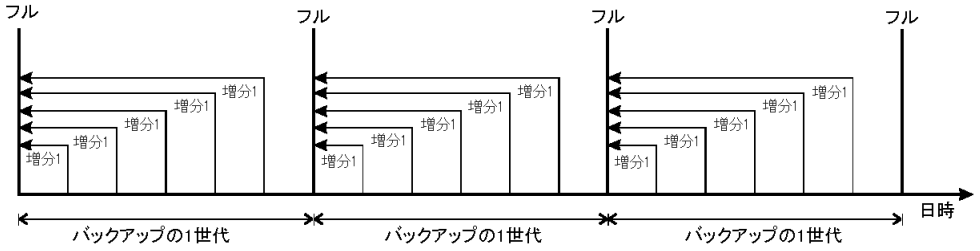


図 100 バックアップ世代

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。詳細は、「メディア交換方針の実装」(151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 (353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。

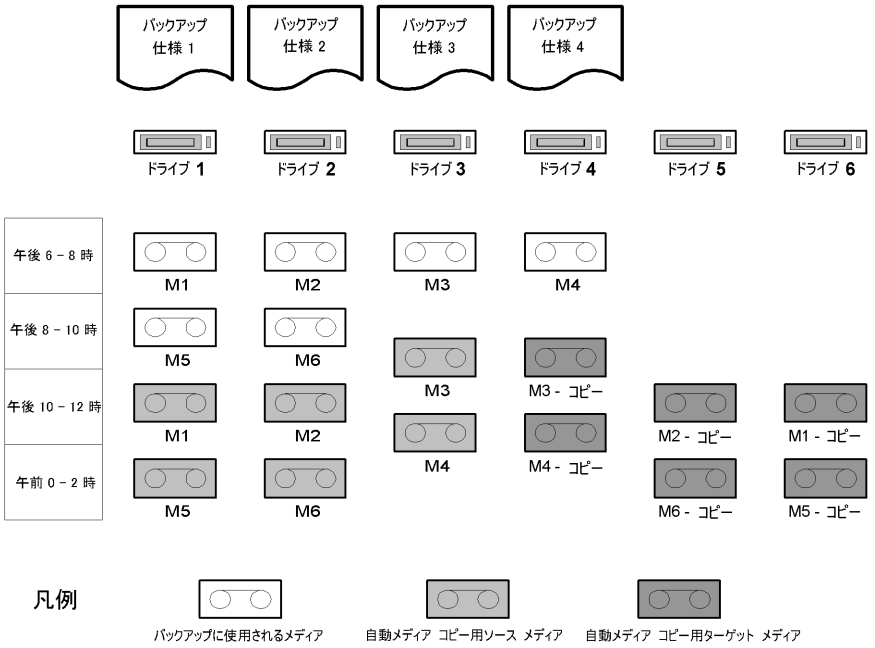


図 101 [増分1]バックアップとメディアの自動コピー

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（355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。

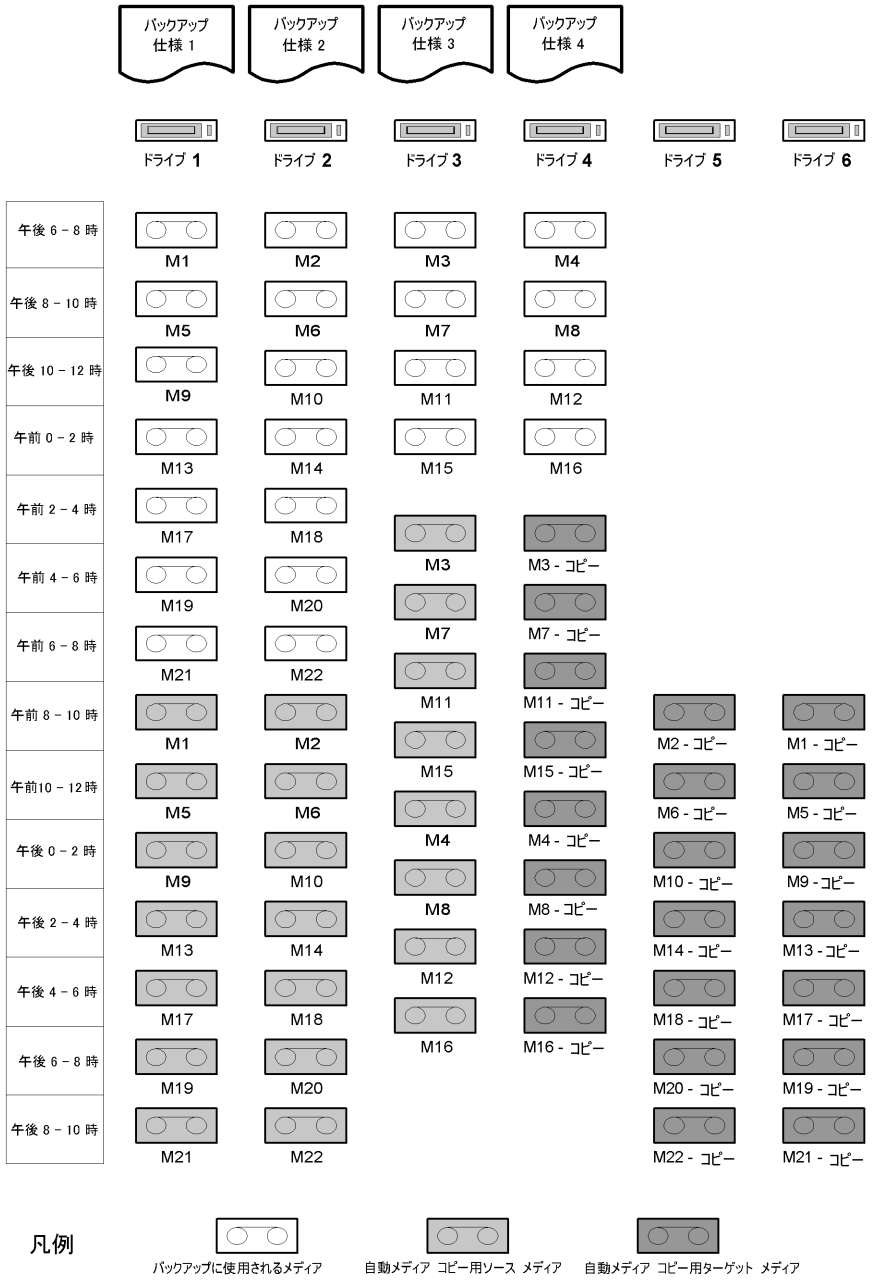


図 102 フルバックアップとメディアの自動コピー

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(356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。

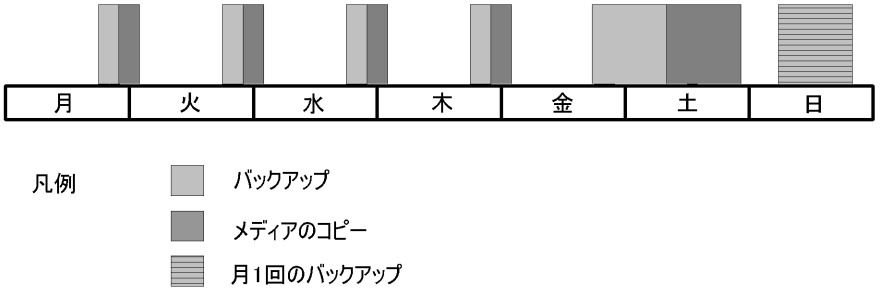


図 103 バックアップセッションとメディアの自動コピーセッションの概要

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 (357ページ)は、フル データベース 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。

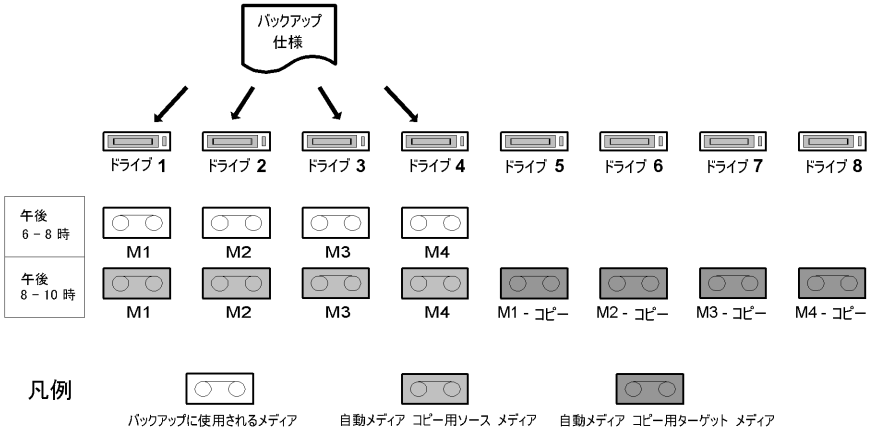


図 104 データベースのフル バックアップと自動メディア コピー

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 (358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。

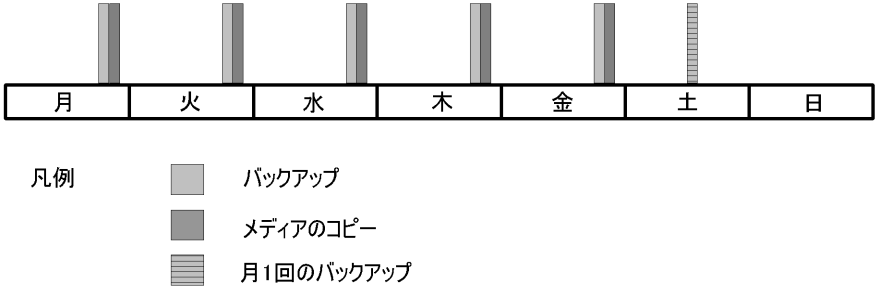


図 105 バックアップセッションとメディアの自動コピーセッションの概要

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」(359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 ヘルプの索引「国際化」を参照してください。

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

アクセス権限
「ユーザー権限」を参照。

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 Protector256ビット長のランダムキーを使用するAES-CTR(Advanced Encryption Standard in Counter Mode)暗号化アルゴリズムを基にしたソフトウェア暗号化。暗号化と復号化の両方で同じキーが使用されます。データはネットワークを介して転送される前およびメディアに書き込まれる前に、AES256ビット暗号化機能によって暗号化されます。

AML
*(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。

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。

アーカイブREDOログ
*(Oracle固有の用語)*オフラインREDOログとも呼びます。Oracleデータベースが ARCHIVELOGモードで動作している場合、各オンラインREDOログが最大サイズまで書き込まれると、アーカイブ先に

コピーされます。このコピーをアーカイブREDOログと呼びます。各データベースに対してアーカイブREDOログを作成するかどうかを指定するには、以下の2つのモードのいずれかを指定します。

- ARCHIVELOG – 満杯になったオンラインREDOログファイルは、再利用される前にアーカイブされます。そのため、インスタンスやディスクにエラーが発生した場合に、データベースを復旧することができます。「ホット」バックアップを実行できるのは、データベースがこのモードで稼動しているときだけです。
- NOARCHIVELOG – オンラインREDOログファイルは、いっぱいになってもアーカイブされません。

「オンラインREDOログも参照。」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。

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ASRアーカイブファイルとしてディレクトリ *Data_Protector_program_data*¥Config¥Server¥dr¥asr(Windows Server 2008の場合)、*Data_Protector_home*¥Config¥Server¥dr¥asr(他のWindowsシステム)、または/etc/opt/omni/server/dr/asr/(UNIXシステムの場合)に保存されます。障害発生後、ASRアーカイブファイルは、ASRを実行する必要があるフロッピーディスクに展開されます。

監査ログ

監査情報が保存されるデータファイル。

監査レポート

監査ログファイルの保存されたデータから作成される、ユーザーが判読可能な形式の監査情報出力。

監査情報

セル全体に対し、ユーザーが定義した拡張期間にわたって実施された、全バックアップセッションに関するデータ。

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。

自動ストレージ管理

*(Oracle固有の用語)*自動ストレージ管理は、Oracleデータベースファイルを管理するOracle 10g/11g統合型ファイルシステムおよびボリュームマネージャです。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。

自動移行

*(VLS固有の用語)*データのバックアップをまずVLSの仮想テープに作成し、それを物理テープ(1つの仮想テープが1つの物理テープをエミュレート)に移行する操作を、中間バックアップアプリケーションを使用せずに実行する機能。
「仮想ライブラリシステム(VLS)と仮想テープも参照。」を参照。

BACKINT

*(SAP R/3固有の用語)*SAP R/3バックアッププログラムが、オープンインタフェースへの呼び出しを通じてData Protector backintインタフェースソフトウェアを呼び出し、Data Protectorソフトウェアと通信できるようにします。バックアップ時および復元時には、SAP R/3プログラムがData Protectorbackintインタフェースを通じてコマンドを発行します。

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ID

統合ソフトウェアオブジェクトの識別子で、統合ソフトウェアオブジェクトのバックアップのセッションIDと一致します。バックアップIDは、オブジェクトのコピー、エクスポート、またはインポート時に保存されます。

バックアップオブジェクト

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ています。

- 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ー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ー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ー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ー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ー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ー「Bar」

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。

バックアップセッション

データのコピーを記憶メディア上に作成するプロセス。バックアップ仕様に処理内容を指定することも、対話式に操作を行うこと(対話式セッション)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。

「バックアップ仕様、増分バックアップ、およびフル バックアップも参照。」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、およびバックアップを行いたい日時とともに指定したリスト。オブジェクトとなるのは、ディスクやボリューム全体、またはその一部、たとえばファイル、ディレクトリ、Windowsレジストリなどです。インクルードリストおよびエクスクルードリストを使用して、ファイルを選択することもできます。

バックアップシステム

*(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。

バックアップの種類

「増分バックアップ、ディファレンシャルバックアップ、トランザクションバックアップ、フルバックアップおよびデルタバックアップ」を参照。

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。データチャンクごとに固有のコンテンツアドレスを作成して、保存データの冗長性をブロック(またはチャンク)レベルで排除するというIAP機能を活用します。変更されたチャンクのみがネットワーク上を転送され、ストアに追加されます。

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]を選択すると、バックアップ/テンプレートで利用できるデータの種類に基づいたビューが表示されます。(デフォルト)
[グループ別]を選択すると、バックアップ仕様/テンプレートの所属先のグループに基づいたビューが表示されます。
[名前別]を選択すると、バックアップ仕様/テンプレートの名前に基づいたビューが表示されます。
[Manager別](MoMの実行時のみ有効)を選択すると、バックアップ仕様/テンプレートの所属先のCell Managerに基づいたビューが表示されます。

BC

*(EMC Symmetrix固有の用語)*Business Continuanceの略。BCは、EMC Symmetrix標準デバイスのインスタントコピーに対するアクセスおよび管理を可能にするプロセスです。
「BCVも参照。」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も参照。」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も参照。」を参照。

BCプロセス

*(EMC Symmetrix固有の用語)*保護されたストレージ環境のソリューション。特別に構成されたEMC Symmetrixデバイスを、EMC Symmetrix標準デバイス上でデータを保護するために、ミラーとして、つまりBusiness Continuance Volumesとして規定します。
「BCVも参照。」を参照。

BC VA

*(HP StorageWorks Virtual Array固有の用語)*Business Copy VAの略。BCを使うと、HP StorageWorks Virtual Array LUNの内部コピーを同じ仮想アレイに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。コピー(子またはBusiness Copy LUN)は、バックアップやデータ解析、開発などさまざまな目的に使用できます。バックアップ目的で使用されるときは、元(親)のLUNはアプリケーションシステムに接続され、Business Copy(子)LUNはバックアップシステムに接続されます。
「HP StorageWorks Virtual Array LUN、アプリケーションシステム、およびバックアップシステムも参照。」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も参照。」を参照。

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。

ブートボリューム/ディスク/パーティション

ブートプロセスの開始に必要なファイルが入っているボリューム/ディスク/パーティション。Microsoftの用語では、オペレーティングシステムファイルが入っているボリューム/ディスク/パーティションをブートボリューム/ブートディスク/ブートパーティションと呼んでいます。

BRARCHIVE

*(SAP R/3固有の用語)*SAP R/3バックアップツールの1つ。アーカイブREDOログファイルをバックアップできます。BRARCHIVEでは、アーカイブプロセスのすべてのログとプロファイルも保存されます。

「BRBACKUPおよびBRRESTOREも参照。」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、またはすべての表領域をオンラインでもオフラインでもバックアップできます。また、必要に応じて、オンラインREDOログファイルをバックアップすることもできます。

「BRARCHIVEおよびBRRESTOREも参照。」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、表領域、バックアップ全体、REDOログファイルのログシーケンス番号、またはバックアップのセッションIDを指定することができます。

「BRBACKUPおよびBRARCHIVEも参照。」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、および障害

復旧などの目的でHP StorageWorks Disk Array XP LDEVのリモートコピーを作成および維持できます。CAを使用するには、メイン(プライマリ)ディスクアレイとリモート(セカンダリ)ディスクアレイが必要です。オリジナルのデータを格納し、アプリケーションシステムに接続されているCAプライマリボリューム(P-VOL)が、メインディスクアレイに格納されます。リモートディスクアレイには、バックアップシステムに接続されているCAセカンダリボリューム(S-VOL)が格納されます。
「BC (*HP StorageWorks Disk Array XP固有の用語*)、Main Control UnitおよびHP StorageWorks Disk Array XP LDEVも参照。」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も参照。」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。

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。

CDB

カタログデータベース(Catalog Database)の略。CDBは、IDBのうち、バックアップ、復元、オブジェクトコピー、オブジェクト集約、オブジェクト検証、およびメディア管理セッションに関する情報を格納する部分。選択したロギングレベルによっては、ファイル名とファイルバージョンも格納されます。CDBは、常にセルに対してローカルとなります。
「MMDBも参照。」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、クラスター内のすべてホストから同じパス名を使って、マシンに依存する実行可能ファイル、システムデータ、およびデバイスファイルを正しく動作させることができます。

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。集中管理によるバックアップおよび復元のポリシーやタスクの管理が可能です。

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。

集中型ライセンス

Data Protectorでは、複数のセルからなるエンタープライズ環境全体にわたってライセンスの集中管理を構成できます。すべてのData Protectorライセンスは、エンタープライズCell Managerシステム上にインストールされます。ライセンスは、実際のニーズに応じてエンタープライズCell Managerシステムから特定のセルに割り当てることができます。
「MoMも参照。」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。」を参照。

Change Journal

*(Windows固有の用語)*ローカルNTFSボリューム上のファイルやディレクトリへの変更が発生するたび、それに関するレコードをログに記録するWindowsファイルシステム機能。

Change Log Provider

*(Windows固有の用語)*ファイルシステム上のどのオブジェクトが作成、変更、または削除されたかを判断するために照会できるモジュール。

チャンネル

*(Oracle固有の用語)*Oracle Recovery Managerリソース割り当て。チャンネルが割り当てられるごとに、新しいOracleプロセスが開始され、そのプロセスを通じてバックアップ、復元、および復旧が行われます。割り当てられるチャンネルの種類によって、使用するメディアの種類が決まります。

- diskタイプ
- sbt_tapeタイプ

OracleがData Protectorと統合されており、指定されたチャンネルの種類がsbt_tapeタイプの場合は、上記のサーバー プロセスがData

Protectorに対してバックアップの読み取りとデータファイルの書き込みを試行します。

チャンク

*(IAP固有の用語)*データをブロック(チャンク)に分割する処理。各チャンクには固有のコンテンツアドレスが割り振られます。このアドレスは、特定のチャンクがIAPアプライアンスにバックアップ済みかどうかを判断するのに使用されます。データの重複が検出された場合(2つのアドレスが一致している、つまりIAPに保存済みの他のデータチャンクとアドレスが同じ)、そのようなデータはバックアップされません。これにより、データの冗長性が排除され、最適なデータ保存が実現されます。
「IAPへのバックアップ」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データベースおよび Lotus Domino Serverデータベースモードの1つ。このモードでは、トランザクションログファイルのコンテンツは、対応するデータがデータベースにコミットされると、定期的に上書きされます。循環ログにより、ディスク記憶領域の要件が軽減されます。

クライアントバックアップ

Data Protectorクライアントにマウントされているすべてのファイルシステムのバックアップ。
実際にバックアップされる対象は、バックアップ仕様でユーザーが選択したオブジェクトによって決まります。

- クライアントシステム名の横にあるチェックボックスを選択する場合、Client Systemタイプが作成されます。その結果、バックアップ時にData Protectorは選択されたクライアントにマウントされているすべてのボリュームを最初に検出してから、それらをバックアップします。Windowsクライアントの場合、CONFIGURATIONもバックアップされます。
- クライアントシステムにマウントされているすべてのボリュームを別々に選択する場合、Filesystemタイプの個別バックアップオブジェクトがボリュームごとに作成されます。その結果、バックアップ時に、選択されたボリュームのみがバックアップされます。バックアップ仕様が作成された後にクライアントにマウントされた可能性があるボリュームは、バックアップされません。

クライアントまたはクライアントシステム

セル内でData Protectorの機能を使用できるように構成された任意のシステム。

クラスター対応アプリケーション

クラスタアプリケーションプログラミングインタフェースをサポートしているアプリケーション。クラスター対応アプリケーションごとに、クリ

ティカルリソースが宣言されます。これらのリソースには、ディスクボリューム(Microsoft Cluster Serverの場合)、ボリュームグループ(MC/ServiceGuardの場合)、アプリケーションサービス、IP名およびIPアドレスなどがあります。

クラスター連続レプリケーション

*(Microsoft Exchange Server固有の用語)*クラスター連続レプリケーション(CCR)はクラスター管理とフェイルオーバーオプションを使用して、ストレージグループの完全なコピー(CCRコピー)を作成および維持する高可用性ソリューションです。ストレージグループは個別のサーバーに複製されます。CCRはExchangeバックエンドサーバーで発生した単発箇所の障害を取り除きます。CCRコピーが存在するパッシブExchange ServerノードでVSSを使用してバックアップを実行すれば、アクティブノードの負荷が軽減されます。CCRコピーへの切り替えは数秒で完了するため、CCRコピーは障害復旧に使用されます。複製されたストレージグループは、Exchangeライターの新しいインスタンス(Exchange Replication Service)として表示され、元のストレージグループと同様にVSSを使用してバックアップできます。
「Exchange Replication ServiceおよびローカルCCRも参照。」を参照。

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。

CMMDB

Data ProtectorのCMMDB(Centralized Media Management Database: メディア集中管理データベース)は、MoMセル内で、複数セルのMMDBをマージすることにより生成されます。この機能を使用することで、MoM環境内の複数のセルの間でハイエンドデバイスやメディアを共有することが可能になります。いずれかのセルからロボティクスを使用して、他のセルに接続されているデバイスを制御することもできます。CMMDBはManager-of-Manager上に置く必要があります。MoMセルとその他のData Protectorセルの間には、できるだけ信頼性の高いネットワーク接続を用意してください。
「MoMも参照。」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。

コマンドラインインタフェース(CLI)
CLIには、DOSコマンドやUNIXコマンドと同じようにシェルスクリプト内で使用でできるコマンドが用意されています。これらを使用して、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。

Command View (CV) EVA
*(HP StorageWorks EVA固有の用語)*HP StorageWorksEVA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プロバイダも参照。」を参照。

Command View VLS
*(VLS固有の用語)*LAN経由でVLSを構成、管理、モニターするのに使用するWebブラウザベースのGUI。
「仮想ライブラリシステム(VLS)」を参照。

同時処理数
「Disk Agentの同時処理数を参照。」を参照。

制御ファイル
*(OracleおよびSAP R/3固有の用語)*データベースの物理構造を指定するエントリが記述されたOracleデータファイル。復旧に使用するデータベース情報の整合性を確保できます。

コピーセット
*(HP StorageWorksEVA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も参照。」を参照。

CRS
Data Protector Cell Manager上で実行され、バックアップと復元セッションを開始、制御する、Cell Request Serverのプロセス(サービス)。このサービスは、Data ProtectorがCell Manager上にインストールされるとすぐに開始されます。Windowsシステムでは、CRSはインストール時に使用したユーザーアカウントで実行されます。UNIXシステムでは、CRSはアカウントルートで実行されます。

CSM
Data Protectorコピーおよび集約セッションマネージャ(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。

データファイル

*(OracleおよびSAP R/3固有の用語)*Oracleによって作成される物理ファイル。表や索引などのデータ構造を格納します。データファイルは、1つのOracleデータベースにのみ所属できます。

データ保護

メディア上のバックアップデータを保護する期間を定義します。この期間中は、データが上書きされません。保護期限が切れると、それ以降のバックアップセッションでメディアを再利用できるようになります。
「カタログ保護も参照。」を参照。

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。

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のプログラムファイルと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、パスはインストール時にData Protectorセットアップウィザードで変更できます。
「Data_Protector_program_data.」を参照。

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、パスはインストール時にData Protectorセットアップウィザードで変更できます。
「Data_Protector_home.」を参照。

データベースライブラリ

Data Protectorのルーチンのセット。Oracle Serverのようなオンラインデータベース統合ソフトウェアのサーバーとData Protectorの間でのデータ転送を可能にします。

データベース並列処理

十分な台数のデバイスが利用可能であり、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。

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。
「コピーセットも参照。」を参照。

データベースサーバー

大規模なデータベース(SAP R/3データベースやMicrosoft SQLデータベースなど)が置かれているコンピュータ。サーバー上のデータベースへは、クライアントからアクセスできます。

Dbobject

*(Informix Server固有の用語)*Informix Server物理データベースオブジェクト。blobspace、dbspace、または論理ログファイルなどがそれにあたります。

DCディレクトリ

詳細カタログ(DC)ディレクトリには、詳細カタログバイナリファイル(DCBF)が含まれており、そのファイルの中にはファイルバージョンについての情報が保管されています。これは、IDBのDCBF部分を表し、IDB全体の約80%の容量を占めます。デフォルトのDCディレクトリはdcbfと呼ばれ、Data_Protector_program_data¥db40ディレクトリ(Windows Server 2008の場合)、*Data_Protector_home*¥db40ディレクトリ(その他のWindowsシステムの場合)、または/var/opt/omni/server/db40ディレクトリ(UNIXシステム)のCell Managerに置かれます。他のDCディレクトリを作成し、独自に指定した場所を使用することができます。1つのセルでサポートされるDCディレクトリは50個までです。DCディレクトリのデフォルト最大サイズは16GBです。

DCBF

DCBF(Detail Catalog Binary Files: 詳細カタログバイナリファイル)ディレクトリは、IDBの一部です。IDBの約80%を占めるファイルバージョンと属性に関する情報を格納します。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。

デルタバックアップ

差分バックアップ(delta backup)では、前回の各種バックアップ以降にデータベースに対して加えられたすべての変更がバックアップされます。
「バックアップの種類も参照。」を参照。

デバイス

ドライブまたはより複雑な装置(ライブラリなど)を格納する物理装置。

デバイスチェーン

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成ります。デバイスチェーンに含まれるデバイスのメディアで空き容量がなくなると、自動的に次のデバイスのメディアに切り替えて、バックアップを継続します。

デバイスグループ

*(EMC Symmetrix固有の用語)*複数のEMC Synnetrixデバイスを表す論理ユニット。デバイスは1つのデバイスグループにしか所属できません。デバイスグループのデバイスは、すべて同じEMC Symmetrix装置に取り付けられている必要があります。デバイスグループにより、利用可能なEMC Symmetrixデバイスのサブセットを指定し、使用することができます。

デバイスストリーミング

デバイスがメディアへ十分な量のデータを継続して送信できる場合、デバイスはストリーミングを行います。そうでない場合は、デバイスはテープを止めてデータが到着するのを待ち、テープを少し巻き戻した後、テープへの書込みを再開します。言い換えると、テープにデータを書き込む速度が、コンピュータシステムがデバイスへデータを送信する速度以下の場合、デバイスはストリーミングを行います。ストリーミングは、スペースの使用効率とデバイスのパフォーマンスを大幅に向上します。

DHCPサーバー

Dynamic Host Configuration Protocol(DHCP)を通じて、DHCPクライアントにIPアドレスの動的割り当て機能とネットワークの動的構成機能を提供するシステム。

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。このバックアップを実行するには、増分1バックアップを指定します。
「増分バックアップも参照。」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だけを記録するデータベースバックアップ。
「バックアップの種類も参照。」を参照。

ディファレンシャルデータベースバックアップ

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。

直接バックアップ

SCSI Extended Copy (Xcopy)コマンドを使用してディスクからテープ(または他の2次ストレージ)へのデータの直接移動を効率化する、SANベースのバックアップソリューション。ダイレクトバックアップは、SAN環境内のシステムへのバックアップI/O負荷を軽減します。ディスクからテープ(または他の2次ストレージ)へのデータの直接移動をSCSI Extended Copy (XCopy)コマンドで効率化します。このコマンドは、ブリッジ、スイッチ、テープライブラリ、ディスクサブシステムなど、インフラストラクチャの各要素でサポートされています。
「XCopyエンジンも参照。」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。

障害復旧

クライアントのメインシステムディスクを(フル)バックアップの実行時に近い状態に復元するためのプロセスです。

障害復旧オペレーティングシステム(DR OS)
「DR OS」を参照。

Disk Agent
クライアントのバックアップと復元を実行するためにクライアントシステム上にインストールする必要があるコンポーネントの1つ。Disk Agentは、ディスクに対するデータの読み書きを制御します。バックアップ セッション中には、Disk Agentがディスクからデータを読み取って、Media Agentに送信してデータをデバイスに移動させます。復元セッション中には、Disk AgentがMedia Agentからデータを受信して、ディスクに書き込みます。オブジェクト検証セッション中に、Disk AgentはMedia Agentからデータを取得し、確認処理を実行しますが、データはディスクには書き込まれません。

Disk Agentの同時処理数
1つのMedia Agentに対して同時にデータを送信できるDisk Agentの数。

ディスクグループ
*(Veritas Volume Manager固有の用語)*VxVMシステムのデータストレージの基本ユニット。ディスクグループは、1つまたは複数の物理ボリュームから作成できます。同じシステム上に複数のディスクグループを置くことができます。

ディスクイメージ(rawディスク)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ため、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。

ディスクステージング
データをいくつかの段階に分けてバックアップする処理。これにより、バックアップと復元のパフォーマンスが向上し、バックアップデータの格納費用が節減され、データの可用性と復元時のアクセス性が向上します。バックアップステージは、最初に1種類のメディア(たとえば、ディスク)にデータをバックアップし、その後データを異なる種類のメディア(たとえば、テープ)にコピーすることから構成されます。

配布ファイルメディア形式

ファイルライブラリで利用できるメディア形式。仮想フルバックアップと呼ばれる容量効率のいい合成バックアップをサポートしています。この形式を使用することは、仮想フルバックアップにおける前提条件です。
「仮想フルバックアップも参照。」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。

DMZ

DMZ (Demilitarized Zone)は、企業のプライベートネットワーク(イントラネット)と外部のパブリックネットワーク(インターネット)の間に「中立地帯」として挿入されたネットワークです。DMZにより、外部のユーザーが企業のイントラネット内のサーバーに直接アクセスすることを防ぐことができます。

DNSサーバー

DNSクライアントサーバーモデルでは、DNSサーバーにインターネット全体で名前解決を行うのに必要なDNSデータベースに含まれている情報の一部を保持します。DNSサーバーは、このデータベースを使用して名前解決を要求するクライアントに対してコンピュータ名を提供します。

ドメインコントローラ

ユーザーのセキュリティを保護し、別のサーバーグループ内のパスワードを検証するネットワーク内のサーバー。

DRイメージ

一時障害復旧オペレーティングシステム(DR OS)のインストールおよび構成に必要なデータ。

DR OS

障害復旧を実行するオペレーティングシステム環境。Data Protectorに対して基本的な実行時環境(ディスク、ネットワーク、テープ、およびファイルシステムへのアクセス)を提供します。Data Protector障害復旧を実行する前に、DR OSをディスクにインストールするかメモリにロードして、構成しておく必要があります。DR OSには、一時DR OSとアクティブDR OSがあります。一時DR OSは、他のオペレーティングシステムの復元用ホスト環境として排他的に使用されます。このホスト環境には、ターゲットとなるオペレーティングシステムの構成データも置かれます。ターゲットシステムを元のシステム構成に復元し終えた後、一時DR OSは削除されます。アクティブDR OSは、Data Protector障害復旧プロセスのホストとして機能するだけでなく、復元後のシステムの一部にもなります。その場合、DR OSの構成データは元の構成データに置き換わります。

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。

ドライブベース暗号化

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。バックアップの実行中、ドライブではメディアに書き込まれるデータとメタデータの両方が暗号化されます。

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。

動的(ダイナミック)クライアント

「ディスクディカバリによるクライアントバックアップ」を参照。

EMC Symmetrix Agent (SYMA)
(EMC Symmetrix 固有の用語)

「Symmetrix Agent (SYMA)」を参照。

緊急ブートファイル

*(Informix Server固有の用語)*Informix Server構成ファイルixbar.*server_id*。このファイルは、*INFORMIXDIR*/etcディレクトリ(Windowsの場合)、または*INFORMIXDIR*¥etcディレクトリ(UNIXの場合)に置かれています。*INFORMIXDIR*はInformix Serverのホームディレクトリ、*server_id*はSERVERNUM構成パラメータの値です。緊急ブートファイルの各行は、1つのバックアップオブジェクトに対応します。

暗号化キー

Data Protector暗号化アルゴリズムで使用されるランダムに生成された256ビットの数値。これを使用して、AES 256ビットソフトウェア暗号化またはドライブベースの暗号化が指定されたバックアップ中に情報を暗号化します。これに続く情報の復号化では、同じキーが使用されます。Data Protectorセルの暗号化キーは、Cell Manager上の中央キーストアに保存されます。

暗号化キー KeyID-StoreID

Data Protector Key Management Serverで使用される結合識別子。これを使用して、Data Protectorで使用される暗号化キーを識別および管理します。KeyIDは、キーストア内のキーを識別します。StoreIDは、Cell Manager上のキーストアを識別します。Data Protectorを暗号化機能付きの旧バージョンからアップグレードした場合、同じCell Manager上で使用されるStoreIDが複数存在する可能性があります。

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。

エンタープライズバックアップ環境

複数のセルをグループ化して、1つのセルから集中管理することができます。エンタープライズバックアップ環境には、複数のData Protectorセル内のすべてのクライアントが含まれます。これらのセルは、Manager of Managers (MoM)のコンセプトにより集中管理用のセルから管理されます。
「MoMも参照。」を参照。

イベントログ(Data Protectorイベントログ)

イベントログには、Data Protector関連のすべての通知が書き込まれます。デフォルトの送信方法では、すべての通知がイベントログに送信されます。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ユーザーだけです。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。

イベントログ

(Windows固有の用語)サービスの開始または停止、ユーザーのログオンとログオフなど、Windowsがすべてのイベントを記録したファイル。 Data Protectorは、Windowsイベントログをwindows構成バックアップの一部としてバックアップできます。

Exchange Replication Service

*(Microsoft Exchange Server固有の用語)*ローカル連続レプリケーション(LCR)か、クラスター連続レプリケーション(CCR)テクノロジのいずれかを使用して複製されたストレージグループを表すMicrosoft Exchange Serverのサービス。
「クラスター連続レプリケーションおよびローカル連続レプリケーション.」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。

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。

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。

フェイルオーバー
あるクラスターノードから別のクラスターノードに最も重要なクラスターデータ(Windowsの場合はグループ、UNIXの場合はパッケージ)を転送すること。フェイルオーバーは、主に、プライマリノードのソフトウェア/ハードウェア障害発生時や保守時に発生します。

フェイルオーバー
*(HP 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.も参照。」を参照。

FCブリッジ
「Fibre Channelブリッジ」を参照。

Fibre Channel
Fibre Channelは、高速のコンピュータ相互接続に関するANSI標準です。光ケーブルまたは銅線ケーブルを使って、大容量データファイルを高速で双方向送信でき、数km離れたサイト間を接続できます。ファイバチャンネルは、ノード間を3種類の物理トポロジー(ポイントトゥポイント、ループ、スイッチ式)で接続できます。

Fibre Channelブリッジ
Fibre Channelブリッジ(マルチプレクサ)は、RAIDアレイ、ソリッドステートディスク(SSD)、テープライブラリなどの既存のパラレルSCSIデバイスをファイバーチャネル環境に移行できるようにします。ブリッジ(マルチプレクサ)の片側にはFibre Channelインタフェースがあり、その反対側にはパラレルSCSIポートがあります。このブリッジ(マルチプレクサ)を通じて、SCSIパケットをFibre Channelとパラレル SCSIデバイスの間で移動することができます。

ファイルデポ
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。

ファイル複製サービス(FRS)
Windowsサービスの1つ。ドメインコントローラのストアログオンスクリプトとグループポリシーを複製します。また、分散ファイルシステム(DFS)共有をシステム間で複製したり、任意のサーバーから複製作業を実行することもできます。

ファイルツリーウォーク

*(Windows固有の用語)*どのオブジェクトが作成、変更、または削除されたかを判断するためにファイルシステムを巡回する処理。

ファイルバージョン

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番号も参照。」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、バックアップと復旧に関係するファイル(リカバリファイル)の集中管理ストレージ領域として機能する、Oracle 10g/11gによって管理されるディレクトリ、ファイルシステム、または自動ストレージ管理のディスクグループです。
「リカバリファイルも参照。」を参照。

fnames.dat

IDBのfnames.datファイルには、バックアップしたファイルの名前に関する情報が格納されます。一般に、ファイル名が保存されている場合、それらのファイルはIDBの20%を占めます。

初期化

メディアをData Protectorで使用できるように初期化するプロセス。メディア上の既存データはすべて消去されます。メディアに関する情報(メディアID、説明、場所)は、IDBおよび該当するメディア(メディアヘッダ)に保存されます。Data Protectorのメディアは、保護の期限が切れるか、またはメディアの保護が解除されるかメディアがリサイクルされるまで、フォーマットされません。

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。

フルバックアップ

フルバックアップでは、最近変更されたかどうかに関係なく、選択されたオブジェクトをすべてバックアップします。
「バックアップの種類も参照。」を参照。

フルデータベースバックアップ

最後に(フルまたは増分)バックアップした後に変更されたデータだけではなく、データベース内のすべてのデータのバックアップ。フルデータベースバックアップは、他のバックアップに依存しません。

フルメール

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。
「増分ZDBも参照。」を参照。

グローバルオプションファイル

Data Protectorをカスタマイズするためのファイル。このファイルでは、Data Protectorのさまざまな設定(特に、タイムアウトや制限)を定義でき、その内容はData Protectorセル全体に適用されます。このファイルは、Data_Protector_program_data¥Config¥Server¥Optionsディレクトリ(Windows Server 2008の場合)、*Data_Protector_home*¥Config¥Server¥Optionsディレクトリ(その他のWindowsシステム)、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)のCell Managerに置かれています。

グループ

(*Microsoft Cluster Server固有の用語*)特定のクラスター対応アプリケーションを実行するために必要なリソース(ディスクボリューム、アプリケーションサービス、IP名およびIPアドレスなど)の集合。

GUI

Data Protectorには、構成、管理、および操作に関するあらゆるタスクに簡単にアクセスできる、グラフィカルユーザーインタフェースが用意されています。Windows用のオリジナルのData Protector GUIの他に、Data Protectorには、さまざまなプラットフォームで実行できる、外観も操作も変わらないJavaベースのGUIも用意されています。

ハード復旧

(*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。

ハートビート

特定のクラスターノードの動作ステータスに関する情報を伝達するタイムスタンプ付きのクラスターデータセット。このデータセット(パケット)は、すべてのクラスターノードに配布されます。

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。

Holidaysファイル

休日に関する情報を格納するファイル。このファイルは、Data_Protector_program_data¥Config¥Server¥holidaysディレクトリ(Windows Server 2008の場合)、*Data_Protector_home*¥Config¥Server¥holidaysディレクトリ(その他のWindowsシステムの場合)、または/etc/opt/omni/server/Holidaysディレクトリ(UNIXシステムの場合)のCell ManagerのHolidaysファイルを編集することで、各種の休日を設定できます。

ホストシステム

ホストシステムとは、ディスクデリバリーによる障害復旧に使用される、Disk Agentがインストールされた動作中のData Protectorクライアントです。

HP Operations Manager

ネットワーク内の多数のシステムとアプリケーションの運用管理を強力な機能でサポートする HP Operations Manager。Data Protectorには、この管理製品を使用するための統合ソフトウェアが用意されています。この統合ソフトウェアは、Windows、HP-UX、SolarisおよびLinux上のHP Operations Manager管理サーバー用のSMART Plug-Inとして実装されています。以前のバージョンのHP Operations Managerは、IT/Operation、Operations Center、およびVantage Point Operations、OpenView Operationsと呼ばれていました。

HP Operations Manager SMART Plug-In (SPI)

ドメイン監視機能を強化する完全に統合されたソリューションで、HP Operations Managerに追加するだけですぐに使えます。HP Operations Manager SMART Plug-Inとして実装されるData Protector用統合ソフトウェアを使用して、ユーザーはHP Operations Managerの拡張機能として任意の数のData Protector Cell Managerを監視できます。

HP 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)*、および複製も参照。」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プロバイダも参照。」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ストレージマネジメントアプライアンスシステム上で個別のサービスとして動作し、受信した要求とCommand View EVA間のゲートウェイとして機能します。Data Protector HP StorageWorks EVA用統合ソフトウェアでは、SMI-S EVAプロバイダはEVA SMI-S Agentから標準化された要求を受け入れ、Command View EVAとやり取りして情報または方法を呼び出し、標準化された応答を返します。
「HP StorageWorks EVA SMI-S AgentおよびCommand View (CV) EVAも参照。」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および複製も参照。」を参照。

ICDA

*(EMC Symmetrix固有の用語)*EMCのSymmetrixの統合キャッシュディスクアレイ(ICDA)は、複数の物理ディスク、複数のFWD SCSIチャンネル、内部キャッシュメモリ、およびマイクロコードと呼ばれる制御/診断ソフトウェアを備えたディスクアレイデバイスです。

IDB

Data Protector内部データベースは、Cell Manager上に保持される埋込み型データベースです。どのデータがバックアップされるか、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どのデバイスやライブラリ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バックアップおよびバックアップ用のメディアとデバイスに関する情報を格納するIDBファイル(obrindex.dat)です。この情報により、IDBの復旧を大幅に簡素化できます。IDBトランザクションログと共にこのファイルを他のIDBディレクトリとは別の物理ディスクに移動し、さらにこのファイルのコピーを作成することをお勧めします。

メディアのインポート

メディアに書き込まれているバックアップセッションデータをすべて再読み込みして、IDBに取り込むプロセス。これにより、メディア上のデータにすばやく、簡単にアクセスできるようになります。
「メディアのエクスポートも参照。」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も参照。」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も参照。」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。

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。

差分同期(再同期)

*(EMC Symmetrix固有の用語)*BCVまたはSRDF制御操作。BCV制御操作では、差分同期(Incremental Establish)により、BCVデバイスが増分的に同期化され、EMC Symmetrixミラー化メディアとして機能します。EMC Symmetrixデバイスは、事前にペアにしておく必要があります。SRDF制御操作では、差分同期(Incremental Establish)により、ターゲットデバイス(R2)が増分的に同期化され、EMC Symmetrixミラー化メディアとして機能します。EMC Symmetrixデバイスは、事前にペアにしておく必要があります。

差分リストア

*(EMC Symmetrix固有の用語)*BCVまたはSRDF制御操作。BCV制御操作では、差分リストアにより、BCVデバイスがペア内の2番目に利用可能な標準デバイスのミラーとして再割り当てされます。これに対し、標準デバイスの更新時には、オリジナルのペアの分割中にBCVデバイスに書き込まれたデータだけが反映され、分割中に標準デバイスに書き込まれたデータはBCVミラーからのデータで上書きされます。SRDF制御操作では、差分リストアにより、ターゲットデバイス(R2)がペア内の2番目に利用可能なソースデバイス(R1)のミラーとして再割り当てされます。これに対し、ソースデバイス(R1)の更新時には、オリジナルのペアの分割中にターゲットデバイス(R2)に書き込まれたデータだけが反映され、分割中にソースデバイス(R1)に書き込まれたデータはターゲットミラー(R2)からのデータで上書きされます。

増分ZDB

ファイルシステムZDBからテープへ、またはZDBからディスク+テープへのセッション。前回の保護されたフルバックアップまたは増分バックアップからの変更のみがテープにストリーミングされます。「フルZDBも参照。」を参照。

Inet

Data Protectorセル内の各UNIXシステムで動作するプロセスまたはWindowsシステム上で動作するサービス。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。

Information Store

*(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。

Informix Server

*(Informix Server固有の用語)*Informix Dynamic Serverのことです。

初期化

「フォーマット」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台はUNIXシステム用で、1台はWindowsシステム用です。

インスタントリカバリ

*(ZDB固有の用語)*ディスクへのZDBセッションまたはディスク+テープへのZDBセッションで作成された複製を使用して、ソースボリュームの内容を複製が作成された時点の状態に復元するプロセスです。これにより、テープからの復元を行う必要がなくなります。関連するアプリケーションやデータベースによってはインスタントリカバリだけで十分な場合もあれば、完全に復旧するためにトランザクションログファイルを適用するなどその他にも手順が必要な場合もあります。
「複製、ゼロダウンタイムバックアップ(ZDB)、ディスクへのZDB、およびディスク/テープへのZDBも参照。」を参照。

統合オブジェクト

OracleまたはSAP DBなどの統合ソフトウェアのバックアップオブジェクト。

Internet Information Services (IIS)

*(Windows固有の用語)*Microsoft Internet Information Servicesは、ネットワーク用ファイル/アプリケーションサーバーで、複数のプロトコルをサポートしています。IISでは、主に、HTTP(Hypertext Transport Protocol)によりHTML(Hypertext Markup Language)ページとして情報が転送されます。

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。

Java GUIクライアント

Java GUIクライアントはJava GUIコンポーネントの1つで、UI関連のインタフェースのみで構成されており、機能するためにはJava GUIサーバーとの通信が必要です。

Java GUIサーバー

Java GUIコンポーネントの1つ。Data Protector Cell Managerシステムにインストールされています。Java GUIサーバーは、Java GUIクライアントからの要求を受け取って処理し、応答をJava GUIクライアントに戻します。通信は、ポート5556でHypertext Transfer Protocol (HTTP)を通して行われます。

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成るデバイス。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。

キーチェーン

秘密キーを復号化する際、手動でパスフレーズを入力する手間を省くツール。セキュアシェルを使用してリモートインストールを実行する場合、このツールをインストールサーバーにインストールして構成する必要があります。

Key Management Service

*(Microsoft Exchange Server固有の用語)*拡張セキュリティのための暗号化機能を提供するMicrosoft Exchange Serverのサービス。
「インフォメーションストアおよびサイト複製サービスも参照。」を参照。

KMS

キー管理サーバー(KMS)はData Protectorの暗号化機能のためのキー管理を提供する、Cell Managerで実行する集中サービス。このサービスは、Data ProtectorがCell Manager上にインストールされるとすぐに開始されます。

キーストア

すべての暗号化キーはCell Managerのキーストアに集中的に格納され、キー管理サーバー(KMS)により管理されます。

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。

ライブラリ

オートチェンジャー、ジュークボックス、オートローダー、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。

無人操作(lights-out operationまたはunattended operation)

オペレータの介在なしで、通常の営業時間外に実行されるバックアップ操作または復元操作。オペレータが手動で操作することなく、バックアップアプリケーションやサービスのマウント要求などが自動的に処理されます。

LISTENER.ORA

*(Oracle固有の用語)*Oracleの構成ファイルの1つ。サーバー上の1つまたは複数のTNSリスナを定義します。

負荷調整

デフォルトでは、デバイスが均等に使用されるように、バックアップ用に選択されたデバイスの負荷(使用率)が自動的に調整されます。負荷調整では、各デバイスに書き込まれるオブジェクトの個数を調整することで、使用率を最適化します。負荷調整はバックアップ時に自動的に実行されるので、データが実際にどのようにバックアップされるかを管理する必要はありません。使用するデバイスを指定する必要があるだけです。負荷調整機能を使用しない場合は、バックアップ仕様に各オブジェクトに使用するデバイスを選択できます。Data Protectorは、指定した順にデバイスにアクセスします。

ローカル復旧とリモート復旧

リモート復旧は、SRDファイルで指定されているMedia Agentホストがすべてアクセス可能な場合にのみ実行されます。いずれかのホ

ストがアクセス不能になっていると、障害復旧プロセスがローカルモードにフェイルオーバーされます。これは、ターゲットシステムにローカルに接続しているデバイスが検索されることを意味します。デバイスが1台しか見つからない場合は、そのデバイスが自動的に使用されます。複数のデバイスが見つかった場合は、デバイスが選択できるプロンプトが表示され、ユーザーが選択したデバイスが復元に使用されます。

ローカル連続レプリケーション

*(Microsoft Exchange Server固有の用語)*ローカル連続レプリケーション(LCR)はストレージグループの完全コピー(LCRコピー)を作成および維持するシングルサーバーソリューション。LCRコピーは元のストレージグループと同じサーバーに配置されます。LCRコピーが作成されると、変更伝播(ログリプレイ)テクノロジで最新に保たれます。LCRの複製機能では未複製のログが削除されません。この動作の影響により、ログを削除するモードでバックアップを実行しても、コピー中のログと複製に十分な余裕がある場合、実際にはディスクの空き容量が解放されない場合があります。
LCRコピーへの切り替えは数秒で完了するため、LCRコピーは障害復旧に使用されます。元のデータとは異なるディスクに存在するLCRコピーをバックアップに使用すると、プロダクションデータベースの入出力の負荷が最小になります。
複製されたストレージグループは、Exchangeライターの新しいインスタンス(Exchange Replication Service)として表示され、通常のストレージグループのようにVSSを使用してバックアップできます。
「クラスター連続レプリケーションおよびExchange Replication Serviceも参照。」を参照。

ロック名

複数のデバイス名を使うことにより、同じ物理デバイスを異なる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。

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。

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]、[ログなし]の4つのロギングレベルがあります。ロギングレベル設定によって、IDBのサイズ増加、バックアップ速度、および復元データのブラウザのしやすさが影響を受けます。

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。変更されたデータがディスクにフラッシュされる前に書き込まれるファイルです。障害発生時には、これらの論理ログファイルを使用することで、コミット済みのトランザクションをすべてロールフォワードするとともに、コミットされていないトランザクションをロールバックすることができます。

ログインID

*(Microsoft SQL Server固有の用語)*Microsoft SQL Serverにログインするためにユーザーが使用する名前。Microsoft SQL Serverのsysloginシステムテーブル内のエントリに対応するログインIDが有効なログインIDとなります。

Oracleターゲットデータベースへのログイン情報

(OracleおよびSAP R/3固有の用語) ログイン情報の形式は*<user_name>*/*<password>*@*<service>*であり、

- *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*には、Oracleパスワードファイル(orapwd)内に指定したのと同じパスワードを指定しなければなりません。パスワードは、データベースを管理するユーザーの認証に使用されます。
- *service*には、ターゲットデータベースのためのSQL*Netサーバー プロセスの識別に使用される名前を指定します。

リカバリカタログデータベースへのログイン情報

*(Oracle固有の用語)*リカバリカタログデータベース(Oracle)へのログイン情報の形式は*<user_name>*/*<password>*@*<service>*で、ユーザー名、パスワード、サービス名の説明は、Oracleターゲットデータベースへの Oracle SQL*Net V2ログイン情報と同じです。ただし、この場合の*service*はOracleターゲットデータベースではなく、リカバリカタログデータベースに対するサービス名となります。

ここで指定するOracleユーザーは、Oracleのリカバリカタログのオーナーでなければならないことに注意してください。

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。

マジックパケット

「Wake ONLAN」を参照。

メールボックス

*(Microsoft Exchange Server固有の用語)*電子メールが配信される場所。管理者がユーザーごとに設定します。電子メールの配信場所として複数の個人用フォルダが指定されている場合は、メールボックスから個人用フォルダに電子メールがルーティングされます。

メールボックスストア

*(Microsoft Exchange Server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。

Main Control Unit (MCU)

*(HP StorageWorks Disk Array XP固有の用語)*CAと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も参照。」を参照。

Manager-of-Managers (MoM)

「MoM」を参照。

make_net_ recovery

make_net_recoveryは、Ignite-UXのコマンドの1つ。Ignite-UXサーバーまたはその他の指定システム上にネットワーク経由で復旧アーカイブを作成できます。ターゲットシステムは、Ignite-UXのmake_boot_tapeコマンドで作成したブート可能なテープからブートするか、またはIgnite-UXサーバーから直接ブートした後、サブネットを通じて復旧することができます。Ignite-UXサーバーからの直接

ブートは、Ignite-UXのbootsysコマンドで自動的に行うか、またはブートコンソールから対話的に指定して行うことができます。

make_tape_recovery

make_tape_recoveryは、Ignite-UXのコマンドの1つ。システムに応じてカスタマイズしたブート可能テープ(インストールテープ)を作成できます。ターゲットシステムにバックアップデバイスを直接接続し、ブート可能な復旧テープからターゲットシステムをブートすることにより、無人障害復旧を実行できます。アーカイブ作成時とクライアント復旧時は、バックアップデバイスをクライアントにローカル接続しておく必要があります。

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。復元またはオブジェクト検証セッション中、Media Agentはバックアップ メディア上のデータを探して、処理するためにDisk Agentに送信します。復元セッションの場合、続いてDisk Agentはデータをディスクに書き込みます。Media Agentは、ライブラリのロボティクス制御も管理します。

メディア割り当てポリシー

メディアをバックアップに使用する順序を決定します。[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。

メディア状態要素

使用回数のしきい値と上書きのしきい値。メディアの状態の判定基準となります。

メディアID

Data Protectorがメディアに割り当てる一意な識別子。

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。

メディアセット
バックアップセッションでは、メディアセットと呼ばれるメディアのグループにデータをバックアップします。メディアの使用法によっては、複数のセッションで同じメディアを共有できます。

メディアの種類
メディアの物理的な種類(DDSやDLTなど)。

メディアの使用法
メディアの使用法は、すでに使用されているメディアに対してバックアップをどのように追加するかを制御します。メディアの使用法は、[追加可能]、[追加不可能]、[増分のみ追加可能]のいずれかに設定できます。

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。

Microsoft Exchange Server
多様な通信システムへの透過的接続を提供するクライアント/サーバー型のメッセージング/ワークグループシステム。電子メールシステムの他、個人とグループのスケジュール、オンラインフォーム、ワークフロー自動化ツールなどをユーザーに提供します。また、開発者に対しては、情報共有およびメッセージング サービス用のカスタムアプリケーション開発プラットフォームを提供します。

Microsoft管理コンソール(MMC)
*(Windows固有の用語)*Windows環境における管理モデル。シンプルで一貫した統合型管理ユーザーインタフェースを提供します。同じGUIを通じて、さまざまなMMC対応アプリケーションを管理できます。

Microsoft SQL Server
分散型「クライアント/サーバー」コンピューティングのニーズを満たすように設計されたデータベース管理システム。

Microsoft 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、複製およびライターも参照。」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。
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。
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、ライブラリドライブ、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も参照。」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。
mount request	デバイスに特定のメディアを挿入するように促す画面プロンプト。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。

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も参照。」を参照。

マルチドライブサーバー
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。

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、障害復旧用のブートデバイスとしても使用可能です。

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、新規に集約されるバージョンのオブジェクトに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少なくとも1つ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、新規に集約されるバージョンのオブジェクトにマージするプロセス。

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
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。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。

オブジェクトコピー 選択されたオブジェクトバージョンを特定のメディアセットにコピーするプロセス。1つまたは複数のバックアップセッションから、コピーするオブジェクトバージョンを選択できます。

オブジェクト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。

オブジェクト検証 Data Protectorの観点で見たバックアップオブジェクトのデータ整合性と、それらを必要なあて先に送信するData Protectorの機能を確認するプロセス。このプロセスは、バックアップ、オブジェクトコピー、またはオブジェクト集約セッションによって作成されたオブジェクトバージョンを復元する機能に信頼レベルを付与するために使用できます。

オブジェクト検証セッション 指定のバックアップオブジェクトまたはオブジェクトバージョンのデータ整合性と、指定のホストにそれらを送信するための選択済みData Protectorネットワーク コンポーネントの機能を確認するプロセス。オブジェクト検証セッションは、対話式に実行することも、自動ポストバックアップまたはスケジュール仕様の指定通りに実行することもできます。

オフラインバックアップ 実行中はアプリケーションデータベースがアプリケーションから使用できなくなるバックアップ。

- 単純なバックアップ方法の場合(ZDBではない)、データベースはバックアップ中(数分から数時間)オフライン状態となり、バックアップシステムからは使用できますが、アプリケーションシステムからは使用できません。たとえばテープへのバックアップの場合、テープへのデータストリーミングが終わるまでの間となります。
- ZDBの方法を使うと、データベースはオフライン状態になりますが、所要時間はデータ複製プロセス中のわずか数秒間です。残りのバックアッププロセスでは、データベースは通常の稼動を再開できます。

データベースは、データ複製プロセスの間(数秒間)オフライン状態となります。残りのバックアッププロセスでは、データベースは通常の稼動を再開できます。
「ゼロダウンタイムバックアップ(ZDB)およびオンラインバックアップも参照。」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。オフライン復旧では、スタンドアロンデバイスおよびSCSIライブラリデバイスのみが使用可能です。Cell Managerの復旧は、常にオフラインで行われます。

オフラインREDOログ

「アーカイブREDOログ」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。

オンラインバックアップ

データベースアプリケーションを利用可能な状態に維持したまま行われるバックアップ。データベースは、バックアップアプリケーションが元のデータオブジェクトにアクセスする必要がある間、特別なバックアップモードで稼動します。この期間中、データベースは完全に機能しますが、パフォーマンスに多少影響が出たり、ログファイルのサイズが急速に増大したりする場合もあります。

- 単純なバックアップ方法の場合(ZDBではない)、バックアップモードはバックアップ期間全体(数分から数時間)必要となります。たとえばテープへのバックアップの場合、テープへのデータストリーミングが終わるまでの間となります。

- ZDBの方法を使うと、バックアップモードに必要な時間はデータ複製プロセス中のわずか数秒間です。残りのバックアッププロセスでは、データベースは通常の稼動を再開できます。

場合によっては、データベースを整合性を保って復元するために、トランザクションログもバックアップする必要があります。
「ゼロダウンタイムバックアップ(ZDB)およびオフラインバックアップも参照。」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ログも参照。」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の主要な障害復旧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_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。

元のシステム

あるシステムに障害が発生する前にData Protectorによってバックアップされたシステム構成。

上書き

復元中のファイル名競合を解決するモードの1つ。既存のファイルの方が新しくても、すべてのファイルがバックアップから復元されます。
「マージも参照。」を参照。

所有権

バックアップ所有権は、データを参照および復元するユーザーの能力に影響します。各バックアップセッションとその中でバックアップされたすべてのデータはオーナーに割り当てられます。所有者は、対話型バックアップを開始するユーザー、CRSプロセスを実行するときに使用するアカウント、またはバックアップ仕様オプションで所有者として指定されたユーザーです。
ユーザーが既存のバックアップ仕様を修正せずにそのまま起動した場合、そのバックアップセッションは対話型とみなされません。
ユーザーがバックアップ仕様を修正して起動すると、以下の条件が成立しない限り、そのユーザーがオーナーになります。

- そのユーザーが[セッションの所有権を切り替え]ユーザー権限を持っている。
- バックアップ仕様内でバックアップセッションオーナーを明示的に定義するには、ユーザー名、グループ名またはドメイン名、およびシステム名を指定します。

UNIXCell Manager上でスケジュールしたバックアップの場合、上記の条件が成立しない限り、root: sysがセッションオーナーになります。
Windows Cell Manager上でスケジューリングしたバックアップの場合は、上記の条件が成立していない限り、インストール時に指定されたユーザーがセッションオーナーになります。

P1Sファイル

P1Sファイルには、システムにインストールされているすべてのディスクを拡張自動ディザスタリカバリ(EADR)中にどのようにフォーマットするかに関する情報が格納されます。このファイルはフルバックアップ中に作成され、バックアップメディアとCell Managerに recovery.p1sというファイル名で保存されます。 保存場所は、Data_Protector_program_data¥Config¥Se ver¥dr¥p1s ディレクトリ(Windows Server 2008の場合)、Data_Protector_home¥Config¥Server¥dr¥p1sディレクトリ(その他のWindowsシステムの場合)、/etc/opt/omni/server/dr/p1sディレクトリ(UNIXシステムの場合)です。.

パッケージ

*(MC/ServiceGuardVeritas Cluster固有の用語)*特定のクラスター対応アプリケーションを実行するために必要なリソース(ボリュームグループ、アプリケーションサービス、IP名およびIPアドレスなど)の集合。

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。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、両方のディスク(プライマリボリュームとミラー化されたボックス)に同じデータが格納されます。
- 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

単一のMedia Agentからデータを受信するDisk Agentを複数実行して、バックアップされたデータを複数のディスクに同時に(つまり並行して)復元すること。並行復元を行うには、複数のディスクまたは論理ボリュームに置かれているデータを選択し、同時処理数を2以上に設定してバックアップを開始し、異なるオブジェクトのデータを同じデバイスに送信する必要があります。並行復元中には、復元対象として選択した複数のオブジェクトがメディアから同時に読み取られるので、パフォーマンスが向上します。

並列処理

1つのオンラインデータベースから複数のデータストリームを読み取ること。

障害復旧の段階0

障害復旧の準備(障害復旧を成功させるための必須条件)。

障害復旧の段階1

DR OSのインストールと構成(以前の記憶領域構造の構築)。

障害復旧の段階2

オペレーティングシステム(環境を定義する各種の構成情報を含む)とData Protectorの復元。

障害復旧の段階3

ユーザーデータとアプリケーションデータの復元。

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。

実行後

オブジェクトのバックアップ後、またはセッション全体の完了後にコマンドまたはスクリプトを実行するバックアップオプション。実行後コマンドは、Data Protectorで事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。

Windows上で動作する実行可能ファイルまたはバッチファイル、UNIX上で動作するシェルスクリプトなどを使用できます。
「実行前も参照。」を参照。

実行前コマンドおよび実行後コマンド

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。

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。

実行前

オブジェクトのバックアップ前、またはセッション全体の開始前にコマンドまたはスクリプトを実行するバックアップオプション。実行前コマンドおよび実行後コマンドは、Data Protectorで事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows上で動作する実行可能ファイルまたはバッチファイル、UNIX上で動作するシェルスクリプトなどを使用できます。
「実行後も参照。」を参照。

プライマリボリューム(P-VOL)

*(HP StorageWorks Disk Array XP固有の用語)*CAと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HP StorageWorks XP 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)も参照。」を参照。

保護

「データ保護およびカタログ保護」を参照。

パブリックフォルダストア

*(Microsoft Exchange Server固有の用語)*インフォメーションストアのうち、パブリックフォルダ内の情報を維持する部分。パブリックフォルダストアは、バイナリリッチテキスト.edbファイルと、ストリーミングネイティブインターネットコンテンツを格納する.stmファイルから構成されます。

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。

RAID

Redundant Array of Independent Disksの略。

RAIDマネージャライブラリ

*(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。

RAID Manager XP

*(HP StorageWorks Disk Array XP固有の用語)*RAID Manager XPアプリケーションには、CA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ための広範なコマンドリストが用意されています。これらのコマンドは、RAID Managerインスタンスを通じて、StorageWorks Disk Array XP Disk Control Unitと通信します。このインスタンスは、コマンドを一連の低レベルSCSIコマンドに変換します。

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プロセス(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。

リカバリカタログ

*(Oracle固有の用語)*Recovery ManagerがOracleデータベースについての情報を格納するために使用するOracleの表とビューのセット。この情報は、Recovery ManagerがOracleデータベースのバックアップ、復元、および復旧を管理するために使用されます。リカバリカタログには、以下の情報が含まれます。

- Oracleターゲットデータベースの物理スキーマ

- データファイルおよびアーカイブログのバックアップセット
- データファイルのコピー
- アーカイブREDOログ
- ストアドスクリプト

リカバリカタログデータベース

*(Oracle固有の用語)*リカバリカタログスキーマを格納するOracleデータベース。リカバリカタログはターゲットデータベースに保存しないでください。

リカバリファイル

*(Oracle固有の用語)*リカバリファイルはフラッシュリカバリ領域に存在するOracle 10g/11g固有のファイルで、現在の制御ファイル、オンラインREDOログ、アーカイブREDOログ、フラッシュバックログ、制御ファイル自動バックアップ、データファイルコピー、およびバックアップピースがこれにあたります。
「フラッシュリカバリ領域も参照。」を参照。

RecoveryInfo

Windows構成ファイルのバックアップ時、Data Protectorは、現在のシステム構成に関する情報(ディスクレイアウト、ボリューム、およびネットワークの構成に関する情報)を収集します。この情報は、障害復旧時に必要になります。

Recovery Manager (RMAN)

*(Oracle固有の用語)*Oracleコマンド行インタフェース。これにより、Oracle Serverプロセスに接続されているデータベースをバックアップ、復元、および復旧するための指示がOracle Serverプロセスに出されます。RMANでは、バックアップについての情報を格納するために、リカバリカタログまたは制御ファイルのいずれかが使用されます。この情報は、後の復元セッションで使うことができます。

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。

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。

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。

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。

複製

*(ZDB固有の用語)*ユーザー指定のバックアップオブジェクトを含む、特定の時点におけるソースボリュームのデータのイメージ。イメージは、作成するハードウェアまたはソフトウェアによって、物理ディスクレベルでの記憶ブロックの独立した正確な複製(クローン)になる(スプリットミラーやスナップクローンなど)場合もあれば、仮想コピーになる(スナップショットなど)場合もあります。基本的なオペレーティングシステムの観点からすると、バックアップオブジェクトを含む物理ディスク全体が複製されます。しかし、UNIXでボリュームマネージャを使用するときは、バックアップオブジェクトを含むボリュームまたはディスクグループ全体が複製されます。Windowsでパーティションを使用する場合、選択したパーティションを含む物理ボリューム全体が複製されます。
「スナップショット、スナップショット作成、スプリットミラー、およびスプリットミラーの作成も参照。」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も参照。」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も参照。」を参照。

復元チェーン

特定の時点までのバックアップオブジェクトの復元に必要なバックアップすべて。復元チェーンは、オブジェクトのフルバックアップ1つと、任意の数の増分バックアップで構成されます。

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。

再同期モード

*(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操作モードの1つ。XPプロバイダが再同期モードであると、ソースボリューム(P-VOL)とその複製(S-VOL)は、バックアップ後、中断ミラー関係になります。MU範囲が0-2(つまり、0、1、2)の場合、ローテーションされる最大複製数(P-VOL当たりのS-VOL数)は3となります。このような構成でのバックアップからの復元は、S-VOLをそのP-VOLと再同期することによってのみ可能となります。
「VSS準拠モード, ソースボリューム、プライマリボリューム(P-VOL), 複製、セカンダリボリューム(S-VOL), MU番号、および複製セットローテーションも参照。」を参照。

RMAN *(Oracle固有の用語)*

「Recovery Manager」を参照。

RSM

Data Protector Restore Session Managerの略。 復元セッションおよびオブジェクト検証セッションを制御します。このプロセスは、常にCell Managerシステム上で稼動します。

RSM

*(Windows固有の用語)*Removable Storage Managerの略。RSMは、アプリケーション、ロボティクスチェンジャ、およびメディアライブラリの間の通信を効率化するメディア管理サービスを提供します。これにより、複数のアプリケーションがローカルロボティクスメディアライブラリとテープまたはディスクドライブを共有でき、リムーバブルメディアを管理できます。

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。

スケジューラー

自動バックアップの実行タイミングと頻度を制御する機能。スケジュールを設定することで、バックアップの開始を自動化できます。

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、別のLDEV(P-VOL)のセカンダリなCAミラーまたはBCミラーの役割を果たす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)も参照。」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ID

バックアップ、復元、オブジェクトコピー、オブジェクト集約、オブジェクト検証、またはメディア管理セッションの識別子で、セッションを実行した日付と一意の番号から構成されます。

セッションキー

実行前スクリプトおよび実行後スクリプト用の環境変数。Data Protectorプレビューセッションを含めたセッションを一意に識別します。セッションキーはデータベースに記録されず、omnimntomnistat、およびomniabort コマンドのオプション指定に使用されます。

シャドウコピー

*(Microsoft VSS固有の用語)*特定の時点におけるオリジナルボリューム(元のボリューム)の複製を表すボリューム。オリジナルボリュームからではなく、シャドウコピーからデータがバックアップされます。オリジナルボリュームはバックアップ処理中も更新が可能ですが、ボリュームのシャドウコピーは同じ内容に維持されます。
「Microsoft Volume Shadow Copy Serviceおよび複製も参照。」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(システムプロバイダなど)で実装することも、ハードウェア(ローカルディスクやディスクアレイ)で実装することもできます。
「シャドウコピーも参照。」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も参照。」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。

SIBF

サーバーレス統合バイナリファイル(SIBF)は、IDBのうち、NDMPのrawメタデータが格納される部分です。これらのデータは、NDMPオブジェクトの復元に必要です。

単一インスタンス

*(IAP固有の用語)*オブジェクト全体とチャンクレベルの両方でデータの冗長性を認識する処理。この処理では、データチャンクごとに強力なハッシュを計算し、それを重複データを保存しようとしているのかどうかの判断に必要な固有のコンテンツアドレスとして使用します。
「IAPへのバックアップも参照。」を参照。

Site Replication Service

*(Microsoft Exchange Server固有の用語)*Exchange Server 5.5ディレクトリサービスをエミュレートすることで、Microsoft Exchange Server 5.5と互換性のあるMicrosoft Exchange Server 2000/2003のサービス。
「インフォメーションストアおよびキーマネージメントサービスも参照。」を参照。

スロット

ライブラリ内の機械的位置。各スロットがDLTテープなどのメディアを1つずつ格納できます。Data Protectorでは、各スロットを番号で参照します。メディアを読み取るときには、ロボット機構がメディアをスロットからドライブに移動します。

SMB

「スプリットミラーバックアップを参照。」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へ作成されたバックアップデータのコピー。スマートコピーのプロセスによって、Data Protectorではソースメディアとターゲットメディアを区別できるため、メディア管理が可能になります。
「仮想ライブラリシステム(VLS)」を参照。

スマートコピープール

*(VLS固有の用語)*指定されたソース仮想ライブラリに対してどのコピー先ライブラリスロットをスマートコピーターゲットとして使用できるかどうかを定義するプール。
「仮想ライブラリシステム(VLS)およびスマートコピーも参照。」を参照。

SMBF

セッションメッセージバイナリファイル(SMBF)は、IDBのうち、バックアップ、復元、オブジェクトコピー、オブジェクト集約、オブジェクト検証、およびメディア管理のセッション中に生成されたセッションメッ

セージが格納される部分です。1つのセッションにつき1つのバイナリファイルが作成されます。ファイルは年毎や月毎に分類されます。

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。このような複製は動的で、スナップショットの種類と作成からの経過時間によって、仮想コピーにあるか、ソースボリュームの内容に引き続き依存するか、または独立した正確な複製(クローン)になります。
「複製およびスナップショット作成も参照。」を参照。

スナップショットのバックアップ(*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。
「スナップショットも参照。」を参照。

ソースデバイス(R1)

*(EMC Symmetrix固有の用語)*ターゲットデバイス(R2)とのSRDF操作に参加するEMC Symmetrixデバイス。このデバイスに対するすべての書き込みは、リモートEMC Symmetrixユニット内のターゲットデバイス(R2)にミラー化されます。R1デバイスは、RDF1グループタイプに割り当てる必要があります。
「ターゲットデバイス(R2)も参照。」を参照。

ソースボリューム

*(ZDB固有の用語)*複製されるデータを含むストレージボリューム。

スパースファイル

ブロックが空の部分を含むファイル。例として、データの一部または大部分にゼロが含まれるマトリクス、イメージアプリケーションからのファイル、高速データベースなどがあります。スパースファイルの処理を復元中に有効にしておかないと、スパースファイルを復元できなくなる可能性があります。

スプリットミラー

*(EMC Symmetrix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の作成も参照。」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。

スプリットミラー作成

*(EMC SymmetrixおよびHP StorageWorks Disk Array XP固有の用語)*事前構成したターゲットボリュームのセット(ミラー)を、ソースボリュームの内容の複製が必要になるまでソースボリュームのセットと同期化し続ける複製技法。その後、同期を停止(ミラーを分割)すると、分割時点でのソースボリュームのスプリットミラー複製はターゲットボリュームに残ります。
「スプリットミラーも参照。」を参照。

スプリットミラー復元

*(EMC SymmetrixおよびHP StorageWorks Disk Array XP固有の用語)*テープへのZDBセッションまたはディスク+テープへのZDBセッションでバックアップされたデータをテープメディアからスプリットミラー複製へ復元し、その後ソースボリュームに同期させるプロセス。この方法では、完全なセッションを復元することも個々のバックアップオブジェクトを復元することも可能です。
「テープへのZDB、ディスク/テープへのZDBおよび複製も参照。」を参照。

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ーの名前の他、ホストコンピュータ上のクライアントが接続できるエイリアスが格納されます。

SRDファイル

*(障害復旧固有の用語)*Unicode(UTF-16)形式のテキストファイルで、WindowsシステムのCONFIGURATIONバックアップ中に生成されCell Managerに格納されます。これには、障害発生時にターゲットシステム上のオペレーティングシステムをインストールおよび構成するために必要なシステム情報が含まれています。
「ターゲットシステム」を参照。

SRDF

*(EMC Symmetrix固有の用語)*EMC Symmetrix Remote Data Facilityの略。SRDFは、異なる位置にある複数の処理環境の間での効率的なリアルタイムデータ複製を実現するBusiness Continuationプロセスです。同じルートコンピュータ環境内だけではなく、互いに遠距離にある環境も対象となります。

SSE Agent

*(HP StorageWorks Disk Array XP固有の用語)*スプリットミラーバックアップの統合に必要なタスクをすべて実行するData Protectorソフトウェアモジュール。RAID Manager XPユーティリティ(HP-UXシステムおよびWindowsシステムの場合)またはRAID Managerライブラリ(Solarisシステムの場合)を使い、HP StorageWorks Disk Array XPの保管システムと通信します。

sst.confファイル

/usr/kernel/drv/sst.confファイルは、マルチドライブライブラリデバイスが接続されているData Protector Sun Solarisクライアントのそれぞれにインストールされていなければならないファイルです。このファイルには、クライアントに接続されている各ライブラリデバイスのロボット機構のSCSIアドレスエントリが記述されていなければなりません。

st.confファイル

/kernel/drv/st.conf ファイルは、バックアップデバイスが接続されているData Protector Solarisクライアントのそれぞれにインストールされていなければならないファイルです。このファイルには、クライアントに接続されている各バックアップドライブのデバイス情報とSCSIアドレスが記述されていなければなりません。シングルドライブデバイスについては単一のSCSIエントリが、マルチドライブライブラリデバイスについては複数のSCSIエントリが、それぞれ必要です。

スタッカー

メディア記憶用の複数のスロットを備えたデバイス。通常は、1ドライブ構成です。スタッカーは、スタックからシーケンシャルにメディアを選択します。これに対し、ライブラリはレポジトリからメディアをランダムに選択します。

スタンドアロンファイルデバイス

ファイルデバイスとは、ユーザーがデータのバックアップに指定したディレクトリにあるファイルのことです。

ストレージグループ

*(Microsoft Exchange Server固有の用語)*同じログファイルを共有する複数のメールボックスストアとパブリックフォルダストアのコレクション。Exchange Serverでは、各ストレージグループを個別のサーバープロセスで管理します。

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。

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、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(たとえば仮想化機構)。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。

スイッチオーバー

「フェイルオーバー」を参照。

Sybase Backup Server API

*(Sybase固有の用語)*Sybase SQL ServerとData Protectorなどのバックアップソリューションの間でのバックアップ情報および復旧情報交換用に開発された業界標準インタフェース。

Sybase SQL Server

*(Sybase固有の用語)*Sybaseの「クライアントサーバー」アーキテクチャ内のサーバー。Sybase SQL Serverは、複数のデータベースと複数のユーザーを管理し、ディスク上のデータの実位置を追跡します。さらに、物理データストレージ域に対する論理データ記述のマッピングを維持し、メモリ内のデータキャッシュとプロシージャキャッシュを維持します。

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。

合成バックアップ

データに関しては従来のフルバックアップと同じである合成フルバックアップを、生産サーバーやネットワークに負担をかけずに出力するバックアップソリューション。合成フルバックアップは、前回のフルバックアップと任意の数の増分バックアップを使用して作成されます。

合成フルバックアップ

バックアップオブジェクトの復元チェーンが新たな合成フルバージョンのオブジェクトにマージされるオブジェクト集約処理の結果。合成フルバックアップは、復元速度の面では従来のフルバックアップと同じです。

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。

システムデータベース

*(Sybase固有の用語)*Sybase SQL Serverを新規インストールすると、以下の4種類のデータベースが生成されます。

- マスターデータベース(master)
- 一時データベース(tempdb)
- システムプロシージャデータベース(sybsystemprocs)
- モデルデータベース(model)

システム復旧データファイル

「SRDファイル」を参照。

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(証明書サーバーの場合)が含まれます。サーバーがドメインコントローラの場合は、Active DirectoryサービスとSYSVOLディレクトリもシステム状態データに含まれます。サーバーがクラスターサービスを実行している場合、システム状態データにはリソースレジストリチェックポイントとクォーラムリソースリカバリ ログが含まれ、最新のクラスターデータ情報が格納されます。

システムボリューム/ディスク/パーティション

オペレーティングシステムファイルが格納されているボリューム/ディスク/パーティション。ただし、Microsoftの用語では、ブートプロセスの開始に必要なファイルが入っているボリューム/ディスク/パーティションをシステムボリューム/システムディスク/システムパーティションと呼んでいます。

SysVol

*(Windows固有の用語)*ドメインのパブリックファイルのサーバーコピーを保存する共有ディレクトリで、ドメイン内のすべてのドメインコントローラ間で複製されます。

表領域

データベース構造の一部。各データベースは論理的に1つまたは複数の表スペースに分割されます。各表領域には、データファイルまたはrawボリュームが排他的に関連付けられます。

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。

ターゲットデータベース

*(Oracle固有の用語)*RMANでは、バックアップまたは復元対象のデータベースがターゲットデータベースとなります。

ターゲットデバイス(R2)

*(EMC Symmetrix固有の用語)*ソースデバイス(R1)とのSRDF操作に参加するEMC Symmetrixデバイス。リモートEMC Symmetrixユニット内に置かれます。ローカルEMC Symmetrixユニット内でソースデバイス(R1)とペアになり、ミラー化ペアから、すべての書き込みデータを受け取ります。このデバイスは、通常のI/O操作ではユー

ザーアプリケーションからアクセスされません。R2デバイスは、RDF2グループタイプに割り当てる必要があります。
「ソースデバイス(R1)も参照。」を参照。

ターゲットシステム　*(障害復旧固有の用語)*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障害復旧の目標となります。クラッシュしたシステムがそのままターゲットシステムになるのではなく、正常に機能していないハードウェアをすべて交換することで、クラッシュしたシステムがターゲットシステムになります。

ターゲットボリューム　*(ZDB固有の用語)*複製されるデータを含むストレージボリューム。

ターミナルサービス　*(Windows固有の用語)*Windowsのターミナルサービスは、サーバー上で実行されている仮想Windowsデスクトップセッションと Windowsベースのプログラムにクライアントからアクセスできるマルチセッション環境を提供します。

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。

TimeFinder　*(EMC Symmetrix固有の用語)*単一または複数のEMC Symmetrix論理デバイス(SLD)のインスタントコピーを作成するBusiness Continuationプロセス。インスタントコピーは、BCVと呼ばれる専用の事前構成SLD上に作成され、システムに対する別個のプロセスを経由してアクセスできます。

TLU　Tape Library Unit (テープライブラリユニット)の略。

TNSNAMES.ORA　*(OracleおよびSAP R/3固有の用語)*サービス名にマッピングされた接続記述子を格納するネットワーク構成ファイル。このファイルは、1か所で集中的に管理してすべてのクライアントで使用することも、また、ローカルに管理して各クライアントで個別に使用することもできます。

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高い頻度で実行できます。トランザクションログバックアップを用いることにより、データベースを特定の時点の状態に復旧できます。

トランザクションログファイル
データベースを変更するトランザクションを記録するファイル。データベースが破損した場合にフォールトトレランスを提供します。

トランザクションログ
*(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)も参照」を参照。

TSANDS.CFGファイル
*(Novell NetWare固有の用語)*バックアップを開始するコンテナの名前を指定するファイル。このファイルはテキストファイルで、TSANDS.NLMがロードされるサーバーのSYS:SYSTEM¥TSAディレクトリにあります。

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。

無人操作

「lights-out operation」を参照。

ユーザーアカウント (Data Protector ユーザーアカウント)

Data Protectorおよびバックアップデータに対する無許可のアクセスを制限するために、Data Protectorユーザーとして許可を受けたユーザーにしかData Protectorを使用できないようになっています。Data Protector 管理者がこのアカウントを作成するときには、ユーザーログオン名、ユーザーのログオン元として有効なシステム、およびData Protectorユーザーグループのメンバーシップを指定します。ユーザーがData Protectorのユーザーインタフェースを起動するか、または特定のタスクを実行するときには、このアカウントが必ずチェックされます。

User Account Control (UAC)

Windows VistaおよびWindows Server 2008のセキュリティコンポーネント。管理者が権限レベルを上げるまで、アプリケーションソフトウェアを標準のユーザー権限に限定します。

ユーザーディスク割り当て

NTFSの容量管理サポートを使用すると、共有ストレージボリュームに対して、拡張された追跡メカニズムの使用およびディスク容量に対する制御が行えるようになります。Data Protectorでは、システム全体にわたるユーザーディスク割り当てが、すべてのユーザーに対して一度にバックアップされます。

ユーザーグループ

各Data Protectorユーザーは、ユーザーグループのメンバーです。各ユーザーグループには1式のユーザー権限があり、それらの権限がユーザーグループ内のすべてのユーザーに付与されます。ユーザー権限を関連付けるユーザーグループの数は、必要に応じて定義できます。Data Protectorには、デフォルトでAdmin、Operator、Userの3つのユーザーグループが用意されています。

ユーザープロファイル

*(Windows固有の用語)*ユーザー別に保持される構成情報。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。

メディアのボールティング

メディアを安全な別の場所に収納すること。メディアが復元に必要になった場合や、今後のバックアップにメディアを再使用する場合は、メディアをデータセンターに戻します。ボールティング手順は、

会社のバックアップ戦略やデータ保護/信頼性ポリシーに依存します。

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。

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も参照。」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も参照。」を参照。

仮想フルバックアップ

コピーするのではなくポインタを使用してデータが集約される、効率の良い合成バックアップ。配布ファイルメディア形式を使用する1つのファイルライブラリにすべてのバックアップ(フルバックアップ、増分バックアップ、およびその結果である仮想フルバックアップ)が書き込まれる場合に実行されます。

仮想ライブラリシステム (VLS)

1つまたは複数の仮想テープライブラリ(VTL)をホストする、ディスクベースのデータストレージデバイス。

仮想サーバー

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ー環境を意味します。アドレスはクラスターソフトウェアによりキャッシュされ、仮想サーバーリソースを現在実行しているクラスターノードにマップされます。こうして、特定の仮想サーバーに対するすべての要求が特定のクラスターノードにキャッシュされます。

仮想テープ

*(VLS固有の用語)*テープに保存された場合と同様にディスクドライブにデータをバックアップするアーカイブ式ストレージテクノロジ。

バックアップスピードおよびリカバリスピードの向上、運用コストの削減など仮想テープシステムとしての利点がある。
「仮想ライブラリシステム(VLS)および仮想テープライブラリも参照。」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)も参照」を参照。

VMware管理クライアント
*(VMware用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ESX Server環境)のどちらかです。

volser
*(ADICおよびSTK固有の用語)*ボリュームシリアル(VOLume SERial)番号は、メディア上のラベルで、大容量ライブラリ内の物理テープの識別に使用されます。VOLSERは、ADIC/GRAUデバイスおよびStorageTekデバイス固有の命名規則です。

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)。

Volume Shadow Copy Service
「Microsoft Volume Shadow Copy Service.」を参照。

VSS
「Microsoft Volume Shadow Copy Service.」を参照。

VSS準拠モード
*(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操作モードの1つ。XP プロバイダがVSS準拠モードであると、ソースボリューム(P-VOL)とその複製(S-VOL)は、バックアップ後、単純非対状態になります。したがって、ローテーションされる複製数(P-VOL当たりのS-VOL数)

に制限はありません。このような構成でのバックアップからの復元は、ディスクの切り替えによってのみ可能となります。「resyncモード、ソースボリューム、プライマリボリューム(P-VOL)、複製、セカンダリボリューム(S-VOL)、および複製セットローテーションも参照。」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。

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。

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サーバーデータおよびDHCPサーバーデータ(システム上で構成されている場合)を1回の操作でバックアップできます。

Windowsレジストリ

オペレーティングシステムやインストールされたアプリケーションの構成情報を保存するため、Windowsにより使用される集中化されたデータベース。

WINSサーバー

Windowsネットワークのコンピュータ名をIPアドレスに解決するWindowsインターネットネームサービスソフトウェアを実行しているシステム。Data Protectorでは、WINSサーバーデータをWindowsの構成データの一部としてバックアップできます。

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。

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。データは、ソースデバイス(ブロックまたはストリーミング、つまりディスクまたはテープ)からあて先デバイス(ブロックまたはストリーミング)へ、XCopyを介して流れていきます。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、制御サーバーをバイパスして行われます。
「ダイレクトバックアップも参照。」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、セキュリティ情報などのZDB関連情報を格納するIDBの一部。ZDBデータベースはZDB、インスタントリカバリ、スプリットミラー復元に使用されます。
「ゼロダウンタイムバックアップ(ZDB)も参照。」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も参照。」を参照。

ディスク+テープへのZDB

*(ZDB固有の用語)*ゼロダウンタイムバックアップの1つの形式。ディスクへのZDBと同様に、作成された複製が特定の時点でのソースボリュームのバックアップとしてディスクアレイに保持されます。ただし、テープへのZDBと同様、複製データはバックアップメディアにもストリーミングされます。このバックアップ方法を使用した場合、同じセッションでバックアップしたデータは、インスタントリカバリ、Data

Protector標準のテープからの復元を使用して復元できます。スプリットミラーアレイではスプリットミラー復元が可能です。
「ゼロダウンタイムバックアップ(ZDB)、ディスクへのZDB、テープへのZDB、インスタントリカバリ、複製、および複製セットローテーションも参照。」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。作成された複製内のデータが、バックアップメディア(通常はテープ)にストリーミングされます。このバックアップ形式ではインスタントリカバリはできませんが、バックアップ終了後にディスクアレイ上に複製を保持する必要がありません。バックアップデータはData Protector標準のテープからの復元を使用して復元できます。スプリットミラーアレイでは、スプリットミラー復元も使用することができます。
「ゼロダウンタイムバックアップ(ZDB)、ディスクへのZDB、インスタントリカバリ、ディスク/テープへのZDB、および複製も参照。」を参照。

ゼロダウンタイムバックアップ(ZDB)

ディスクアレイにより実現したデータ複製技術を用いて、アプリケーションシステムのバックアップ処理の影響を最小限に抑えるバックアップアプローチ。バックアップされるデータの複製がまず作成されます。その後のすべてのバックアップ処理は、元のデータではなく複製データを使って実行し、アプリケーションシステムは通常の処理に復帰します。
「ディスクへのZDB、テープへのZDB、ディスク/テープへのZDB、およびインスタントリカバリも参照。」を参照。

索引

E

F

G

H

T

U

V

W

あ

い

え

お

か

き

く

け

こ

さ

し

す

せ

と

な

に

ね

の

は

ひ

ふ

へ

ほ

ま

む

め

れ

ろ