HP OpenView Storage Data Protector
管理者ガイド

第 8 版

B6960-99106

2004 年 10 月

Release A.05.50

ご注意

1. 本書に記載した内容は、予告なしに変更することがあります。

2. 当社は、本書に関して特定目的の市場性と適合性に対する保証を含む一切の保証をいたしかねます。

3. 当社は、本書の記載事項の誤り、またはマテリアルの提供、性能、使用により発生した損害については責任を負いかねますのでご了承ください。

4. 本製品パッケージとして提供した本書、CD-ROM などの媒体は本製品用だけにお使いください。プログラムをコピーする場合はバックアップ用だけにしてください。プログラムをそのままの形で、あるいは変更を加えて第三者に販売することは固く禁じられています。

Restricted Rights Legend

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph(c)(1)(ii) of the Rights In Technical Data and Computer Software clause in DFARS 52.22707013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commerical Computer Software Restricted rights clause at FAR 52.227-19 for other agencies.

Hewlett-Packard Company
United States of America

UNIX® は、The Open Group の登録商標です。

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

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

Java™ は Sun Microsystems, Inc. の米国における商標です。

ARM® は ARM Limited の登録商標です。

目次

目次

目次

目次

目次

目次

目次

目次

目次

目次

目次

目次

目次

13.Data Protector 環境のカスタマイズ

目次

14.トラブルシューティング

目次

目次

目次

目次

目次

出版履歴

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

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

表 0-1 **出版履歴**

部品番号	出版年月	製品
B6960-99057	2002 年 11 月	Data Protector リリース A.05.00
B6960-99078	2003 年 7 月	Data Protector リリース A.05.10
B6960-99106	2004 年 10 月	Data Protector リリース A.05.50

このマニュアルで使用する表記法

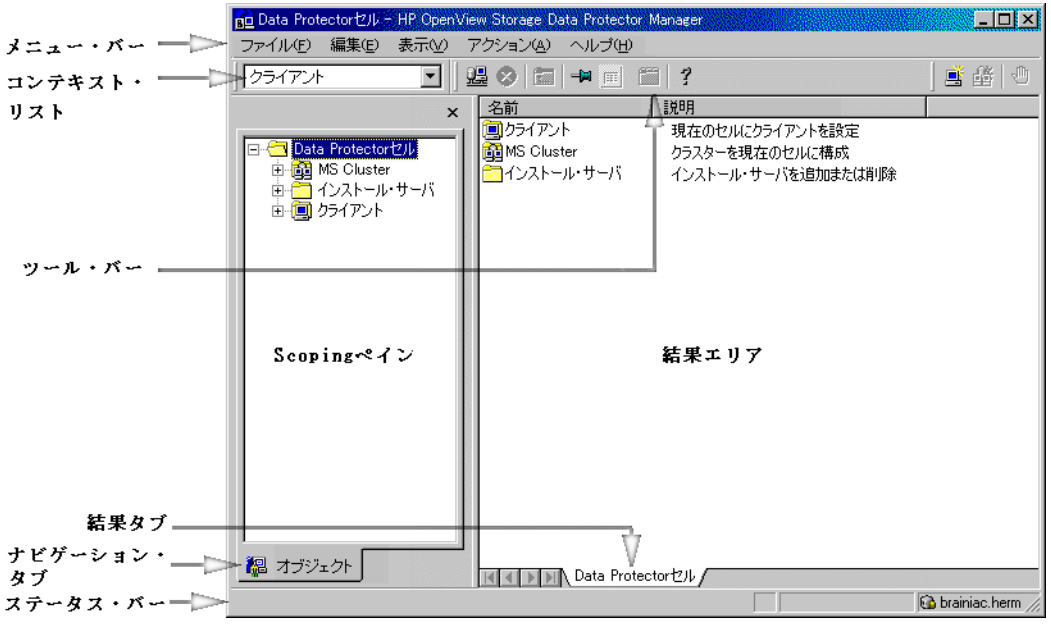
このマニュアルでは、以下の表記法を使用します。

表 2

表記	意味	例
斜体	コマンド入力時にユーザーが指定する変数	プロンプトで以下を入力します。 `rlogin` *your_name* (ユーザーのログイン名を入力する)
太字	新しい用語、強調するテキスト	Data Protector **Cell Manager** は ...
Computer	画面に表示されるテキストや項目	[Enter] を押してください。
	コマンド名	`grep` コマンドを使用します ..
	ファイルやディレクトリの名前	`/usr/bin/X11`
	プロセスの名前	`Data Protector Inet` が実行されているか確かめてください。
[ ]	ウィンドウ / ダイアログ・ボックスの名前	[バックアップ・オプション] ダイアログ・ボックスで ...
	キーボードのキー	[**Return**] を押します。
Computer Bold	ユーザーが入力するテキスト	プロンプトで以下を入力します。 **ls -l**

Data Protector は異なるプラットフォーム間 (Windows と UNIX) で使用可能なグラフィカル・ユーザー・インタフェースを備えています。

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



当社へのお問い合わせについて

概要

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

http://www.hp.com/go/dataprotector(英語版)

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

テクニカル・サポート

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

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

http://www.hp.com/support

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

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

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

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

ドキュメントに関するご意見

ドキュメントに関するお客様のご意見を基に、お客様のご要望を理解し、ご要望に沿ったドキュメントの開発に努めていきたいと思っております。

ドキュメントに関するご意見は、当社の以下のドキュメント専用サイトへお送りください。

http://ovweb.external.hp.com/lpe/doc_serv/ (英語版)

http://welcome.hp.com/country/jp/ja/contact_us.html (日本語版)

トレーニング情報

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

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

http://www.jpn.hp.com/education (日本)

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

Data Protector のドキュメント

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

マニュアル

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

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

このマニュアルでは、Data Protector の概念と Data Protector の動作に関する詳しい説明が記載されています。このマニュアルは、タスク・ベースで書かれている『HP OpenView Storage Data Protector 管理者ガイド』との併用を前提として書かれています。

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

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

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

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

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

このマニュアルでは、さまざまなデータベースをバックアップ / 復元するための Data Protector の構成 / 使用方法を説明しています。このマニュアルには以下の 4 種類のバージョンが提供されています。

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

  このマニュアルでは、Microsoft Exchange Server 2000/2003、Microsoft Exchange Server 5.x、Microsoft SQL Server 7/2000、および Volume Shadow Copy Service の各 Microsoft アプリケーションと Data Protector との統合について説明しています。

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

  このマニュアルでは、Oracle、SAP R/3、SAP DB と Data Protector との統合について説明しています。

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

  このマニュアルでは、Informix、IBM DB2、および Lotus Notes/Domino の各 IBM アプリケーションと Data Protector との統合について説明しています。

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

  このマニュアルでは、Sybase、Network Node Manager、および Network Data Management Protocol と Data Protector との統合について説明しています。

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

このマニュアルでは、HP OpenView Service Information Portal、HP OpenView Service Desk、および HP OpenView Reporter に対応した 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ています。このマニュアルはバックアップ管理者を対象とし、上記の OpenView アプリケーションを使用して Data Protector のサービス管理を行う方法を説明します。

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

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

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

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

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

このマニュアルでは、Data Protector ゼロ ・ダウンタイム・バックアップおよびインスタント・リカバリの概念を説明し、Data Protector がゼロ・ダウンタイム・バックアップ環境で動作するしくみに関する背景知識を提供しています。このマニュアルは、タスク・ベースで書かれている『HP OpenView Storage Data Protector ゼロ ダウンタイム バックアップ 管理者ガイド』および『 HP OpenView Storage Data Protector ゼロ ダウンタイム バックアップ インテグレーション ガイド』との併用を前提として書かれています。

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

このマニュアルでは、Data Protector と HP StorageWorks Virtual Array、HP StorageWorks Enterprise Virtual Array、EMC Symmetrix Remote Data Facility and TimeFinder、および HP StorageWorks Disk Array XPT を統合して使用する方法を説明しています。このマニュアルはバックアップ管理者またはオペレータを対象とし、ゼロ・ダウンタイム・バックアップ、インスタント・リカバリ、およびファイルシステムとディスク・イメージの復旧について解説しています。

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

このマニュアルでは、Oracle、SAP R/3、Microsoft Exchange Server 2000/2003、および Microsoft SQL Server 2000 の各データベースに関して、ゼロ・ダウンタイム・バックアップ、インスタント・リカバリ、および標準的な復旧を行うための、Data Protector の構成および使用方法を説明して

います。またこのマニュアルでは、Microsoft Volume Shadow Copy Service を使用したバックアップおよび復元を行う際の Data Protector の構成および使用方法についても説明しています。

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

このマニュアルでは、MPE/iX クライアントのインストールと構成方法、および MPE/iX データのバックアップと復元方法について説明します。

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

このマニュアルでは、オフライン・ストレージ・メディアのトラッキングと管理に関する情報を説明しています。このマニュアルは、システムの保守とバックアップを担当するネットワーク管理者を対象とし、日常的なメディア操作とレポートの作成を行いながらアプリケーションをインストールおよび構成する作業を記載しています。

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

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

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・ヘルプを備えています。

本書について

『HP OpenView Storage Data Protector 管理者ガイド』は、ネットワーク・バックアップ製品である Data Protector の構成と使用方法を説明します。Data Protector の構成を開始する前に、Data Protector を正しくインストールすることが必要です。

注記

本書では、Data Protector 機能について、特定 Data Protector ライセンス要件に関する情報を記載していません。一部の Data Protector 機能では、専用の Data Protector ライセンスが必要になる場合があります。ライセンスに関する情報については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

対象読者

本書は、ネットワーク上のシステムの保守とバックアップを担当するネットワーク管理者を対象として書かれています。

Data Protector の概念に関する情報は、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。Data Protector の基本的な情報やモデルについて十分理解するために一読されることをお勧めします。

本章の構成

本書は、以下の章で構成されています。

第 11 章 「Data Protector 内部データベースの管理」(487 ページ)

第 12 章 「障害復旧」(545 ページ)

第 13 章 「Data Protector 環境のカスタマイズ」(643 ページ)

第 14 章 「トラブルシューティング」(677 ページ)

第 15 章 「他のアプリケーションとの統合」(767 ページ)

付録 A 「詳細情報」(A-1 ページ)

付録 B 「スタンドアロン・ファイル・デバイスとファイル ジュークボックス デバイス」(B-1 ページ)

用語集 本書で使用する用語の定義

1 Data Protector について

本章の概略

本章では、Data Protector の動作の概要について、以下の 3 項目を説明します。

Data Protector セル環境

Data Protector **セル**とは、**Cell Manager**、**クライアント**、**バックアップ・デバイス**がネットワークを通じて接続されている環境を指します。Cell Manager には、中心となる Data Protector 制御用ソフトウェアがインストールされており、セルの管理やバックアップ / 復元操作の制御などにおいて中心的役割を果たします。バックアップ対象のシステムをセルに追加し、Data Protector クライアントとして設定します。Data Protector がこのクライアントのデータのバックアップを実行した場合には、データはバックアップ・デバイス内の（磁気テープやハードディスクなどの）メディアに保存されます。

Data Protector 内部データベース (IDB) には、バックアップされたファイルのトラッキング情報が保存され、システム全体または単一ファイルのどちらについても、容易にブラウズしたり復元することができます。

Cell Manager はセルの中心となる管理センターであり、IDB を保持しています。また、コア Data Protector ソフトウェアや Session Manager を実行します。Session Manager は、バックアップ・セッションや復元セッションを開始 / 終了したり、IDB にセッション情報を書き込みます。

任意のセル環境にあるいずれのシステムでも Data Protector **クライアント**として設定できます。本来、クライアントとは、バックアップされるシステム、またはバックアップ・データが保存されているバックアップ・デバイスに接続されているシステム、またはその両方を指します。クライアントの役割は、Disk Agent または Media Agent のどちらがインストールされているかにより決まります。

Data Protector を使用したバックアップの対象となるクライアントには、**Disk Agent** がインストールされている必要があります。Data Protector は、ディスクへのアクセスを制御します。Disk Agent により、クライアント・システムの情報のバックアップ、または復元が可能となります。

バックアップ・デバイスが接続されているクライアント・システムには、**Media Agent** がインストールされている必要があります。これはバックアップ・デバイスへのアクセスを制御するソフトウェアです。Media Agent は、バックアップ・デバイス上のメディアへのデータの読み書きを制御します。

バックアップ・デバイスは、記録メディアへのバックアップ・データの記録、または記録メディアからの復元データの収集を、実際に行います。

DAT テープやハードディスクなど、データが記録される物体を、バックアップ・**メディア**と呼びます。

注記

上記の用語や Data Protector の動作原理の詳細については、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

バックアップ・セッションの流れ

バックアップ・セッションは、ユーザー・インタフェースを通じて要求があった時点、またはバックアップ・スケジュールが設定されている時刻になった時点で開始されます。バックアップ・セッションでは、Data Protector は、バックアップが要求されているファイルシステムとディスクを指定されたメディアへバックアップします。

1. Cell Manager は、要求のあったセッションの種類 (バックアップ) を決定して、対応する Session Manager を起動します。
2. Session Manager はバックアップ仕様を読み込み、バックアップが必要なデータと使用するデバイスを決定します。
3. Session Manager は、使用対象となる各メディア・ドライブの Media Agent と、データを読み取る各ディスクの Disk Agent を起動します。
4. [モニター] ウィンドウが表示されます。このウィンドウを使って、ユーザーはマウント要求に応答したり、バックアップ・セッションの進行状況を表示したりできます。
5. Disk Agent は Media Agent へデータ送信を開始します。
6. 複数の Disk Agent が使用されている場合、各 Disk Agent は Media Agent へ同時にデータを送信し、Media Agent は受信したデータをメディアに保存します。
7. データの各ブロックがメディアへ書き込まれると、Media Agent はバックアップされているデータに関する情報を Session Manager に送信します。Session Manager はこの情報を使って、IDB 内のバックアップ済みファイルのカタログを更新します。

復元セッションの流れ

復元セッションは、復元が要求された時点で開始されます。復元セッションでは、Data Protector は、要求されたファイルとディスクをメディアから復元します。

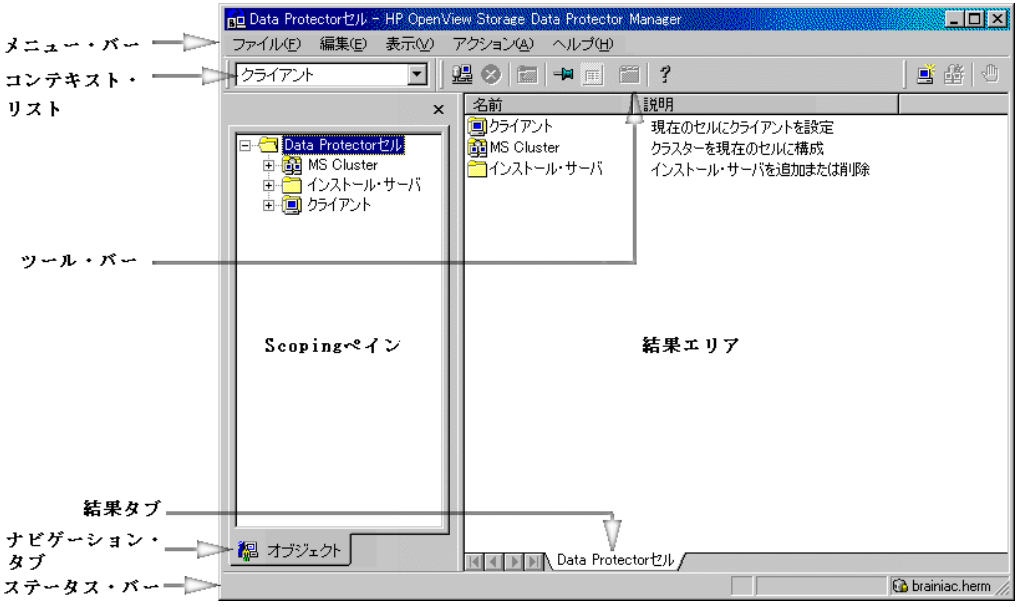
1. ユーザーは、復元するファイルシステムと復元方法を Data Protector ユーザー・インタフェースを使って指定します。
2. Cell Manager は、要求のあったセッションの種類 (復元) を決定して、対応する Session Manager を起動します。
3. Session Manager は、復元するファイルシステムまたはディレクトリ、使用するデバイス、指定されている復元オプションを決定します。
4. Session Manager は、対応する Disk Agent と Media Agent を起動します。たとえば、使用するメディア (テープ) ・ドライブの Media Agent を起動し、データの復元先となるディスクの Disk Agent を起動します。
5. [モニター] ウィンドウが表示されます。このウィンドウを使って、ユーザーはマウント要求に応答したり、復元セッションの進行状況を表示したりできます。
6. Media Agent は Disk Agent へデータ送信を開始します。
7. Session Manager は、IDB を更新し、Disk Agent はデータをディスクへ書き込みます。

Data Protector ユーザー・インタフェースの使用

Data Protector ユーザー・インタフェースは、Windows と UNIX の各プラットフォーム上で使用できます。ユーザー・インタフェースには、Data Protector グラフィカル・ユーザー・インタフェース (GUI) とコマンド行インタフェース (CLI) があります。

Data Protector ユーザー・インタフェースを使うと、Data Protector のすべてのタスクを実行できます。

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



グラフィカル・ユーザー・インタフェース

Data Protector グラフィカル・ユーザー・インタフェース (GUI) は、ボタンやテキスト・ボックスなど Windows の機能を備えており、快適な操作性を提供します。また、ドロップダウン・リスト (表示されている場合) を使えば、設定する内容をリストから選択することができ、キーボード入力は不要です。さらに、オンライン・ヘルプ・システムを使って、各ウィンドウやタスクの情報を表示することもできます。

ユーザー権限に応じて、ユーザーは GUI を使用して、Data Protector のすべての機能、または特定のコンテキストにアクセスできます。

ユーザー権限の詳細については、「Data Protector ユーザー権限」(137 ページ) を参照してください。

Data Protector コンテキストの詳細については、「コンテキスト・リスト」(9 ページ) を参照してください。

国際化とローカリゼーションに関する設定の詳細については、「GUI 内でのファイル名エンコードの設定」(652 ページ) を参照してください。

Windows プラットフォームでの GUI の起動

Windows プラットフォームで Data Protector GUI を起動するには、以下のいずれかの手順を実行します。

- Windows デスクトップの［スタート］をクリックします。［HP OpenView Storage Data Protector］プログラム・グループから［Data Protector Manager］をクリックすると、Data Protector のすべての機能を使用できる GUI が起動します。
- `manager` コマンドを使用すると、Data Protector のすべての機能を使用できる GUI が起動します。

  このコマンドにコンテキスト固有オプションを指定して実行することにより、1 つまたは複数の Data Protector コンテキストを起動できます。次にコマンドの例を示します。
  `manager -backup -restore`
  Data Protector の［バックアップ］および［復元］コンテキストが起動されます。

  接続先の Cell Manager を指定するには、以下のコマンドを使用します。
  `manager -server <Cell Manager_name>`

  上記コマンドの詳細については、`omnigui` の man ページを参照してください。

UNIX プラットフォームでの GUI の起動

Data Protector GUI がサポートされていない UNIX Cell Manager に、Data Protector GUI を使用してアクセスするには、まず `omniusers` コマンドを使用して、その Cell Manager にリモート・アクセスするユーザーのアカウントを作成します。次に、Data Protector GUI がインストールされている任意のシステム上でこのユーザー・アカウントを使用して GUI を起動し、Cell Manager に接続してください。詳細については、`omniusers` の man ページを参照してください。ユーザー・インタフェースがサポートされているオペレーティング・システムのバージョン / リリースは、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』に記載されています。サポートされている言語や非 ASCII 文字を含むファイル名の使用方法については、『HP OpenView Storage Data Protector 管理者ガイド』を参照してください。

Data Protector GUI がサポートされているその他の UNIX システム上では、以下のコマンドを使用できます。

`xomni`	Data Protector のすべての機能を使用できる GUI を起動します。
`xomniadmin`	クライアント、ユーザー、レポート、IDB の管理 (構成) に使用する GUI を起動します。
`xomnibackup`	バックアップに使用する GUI を起動します。
`xomnicellmon`	MoM セルのモニターに使用する GUI を起動します。
`xomnicopy`	コピーに使用する GUI を起動します。
`xomnimm`	メディアとデバイスの管理に使用する GUI を起動します。
`xomnimonitor`	単一セルのモニターに使用する GUI を起動します。
`xomnirestore`	復元に使用する GUI を起動します。
`xomniinstrec`	インスタント・リカバリ用 GUI を起動します。この GUI を起動するには特別なライセンスが必要です。インスタント・リカバリ機能の詳細については、『HP OpenView Storage Data Protector ゼロ ダウンタイム バックアップ 管理者ガイド』と『HP OpenView Storage Data Protector ゼロ ダウンタイム バックアップ コンセプト ガイド』を、また Data Protector ライセンスの詳細については『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

xomnimom Manager-of-Managers GUI を起動します。

上記コマンドの詳細については、omnigui の man ページを参照してください。

Data Protector GUI からの印刷

Data Protector では、GUI から印刷を行えます。印刷できるのは、セッション・メッセージ、レポート、イベント・ログ、その他様々なリスト（構成済みのクライアントやデバイスのリストなど）です。通常、結果エリアにリスト表示されたものやオンライン・ヘルプのトピックは、すべて印刷できます。ただし、［プロパティ］を印刷することはできません。その代わりに、Data Protector のレポート機能を使用して、バックアップ環境に関する様々なレポートを構成できます。レポートの詳細については、「Data Protector レポート」（417 ページ）を参照してください。

必要条件

あらかじめシステム上でプリンタを構成しておく必要があります。

HP-UX 上で［印刷］をクリックすると、定義済みのプリンタが選択できます。正しいプリンタ・ドライバがインストールされていない場合、印刷は行えません。その場合は、PS プリンタを選択して［ファイルへ出力］オプションを指定します。その後、UNIX 端末から lp コマンドを使用して、生成されたファイルを PS プリンタに送信します。

Windows の場合では、［プリンタの選択］ウィンドウに表示されるプリンタは、システムで構成済みで印刷可能なプリンタです。

印刷の詳細な手順については、オンライン・ヘルプの索引キーワード「GUI からの印刷」を参照してください。

Data Protector GUI の構成要素

Data Protector GUI の各要素については、図 1-1 (6 ページ) を参照してください。

コンテキスト・リスト

コンテキスト・リストは、ドロップダウン・メニューで表示されます。以下に説明する管理作業コンテキストから選択することができます。

クライアント	現在の Data Protector セル内のすべてのクライアント・システムの制御。セル内の任意のクライアントを追加、削除、モニターできます。
ユーザー	ユーザー、ユーザー・グループ、ユーザー権限の追加 / 削除。

デバイス / メディア	デバイスやメディアの保守およびデータを保存しているメディアへのアクセスの管理。
バックアップ	バックアップするデータ、バックアップ先、バックアップ方法の管理。
コピー	コピーするデータ、コピー先、コピー方法の管理。
モニター	実行中のセッションのモニター。
復元	復元するデータ、復元先、復元方法の管理。
インスタント・リカバリ	スプリット・ミラー・インスタント・リカバリ・プロセスの管理。この GUI を起動するには特別なライセンスが必要です。インスタント・リカバリの機能詳細については、『*HP OpenView Storage Data Protector HP SureStore Disk Array XP Integration Guide*』を、また Data Protector ライセンスの詳細については『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。
レポート	セルの構成、バックアップ仕様、メディアとメディア・プールに関する情報や、特定のセッションやオブジェクトに関する情報の取得。
内部データベース	IDB の保存容量、データベース・オブジェクト、セッションに関する情報の取得。

Scoping ペイン

Scoping ペインには項目の一覧が表示され、そこから項目を選択することによりウィンドウを表示できます。Scoping ペインで項目を選択すると、選択した項目に関する情報が**結果エリア**に表示されます。

結果エリア

Scoping ペインで項目を選択すると、選択した項目に関する情報が**結果エリア**に表示されます。Scoping ペインでクライアントをクリックした場合、結果エリアには、セル内の全クライアントのリストが表示されます。

ナビゲーション・タブ

Scoping ペインのいちばん下に**ナビゲーション・タブ**が表示されます。これらのタブを使って、Scoping ペインの 2 つの項目リスト画面（**オブジェクト**と**タスク**）を切り替えることができます。ただし、どの Scoping ペインにも項目が 2 つとも表示されるわけではありません。

タブ名	Scoping ペインの表示内容
オブジェクト	データが階層構造で表示されます（Windows エクスプローラに表示されるディレクトリ・ツリーと同様）。たとえば、［デバイス / メディア］コンテキストを選択すると、Data Protector を使って構成されたデバイスとメディアのリストが Scoping ペインに表示されます。
タスク	実行可能なタスクの一覧。タスクをクリックすると、ウィザードが表示されます。ウィザードの指示に従って操作を行うことにより、タスク全体を実行することができます（ファイルのバックアップなど）。

結果タブ

結果タブ上の名前は、Scoping ペインで現在選択されている項目の名前に対応します。ツールバー上のピンのアイコンをクリックすると、現在のビューが「ピン留め」され、後から参照できるように維持されます。たとえば、GUI から他の情報を参照した後でも、「ピン留め」されたタブを選択すれば、前のビューに簡単に戻ることができます。

1 つまたは複数の結果タブを削除するには、タブ内の領域を右クリックして、［タブの削除］または［他のタブを削除］を選択します。

コマンド行インタフェース

コマンド行インタフェース (CLI) は、コマンドとオプションに関する UNIX の標準形式に準拠しており、コマンド行インタフェースからは Data Protector の全機能を使用できます。スクリプトの中でこれらのコマンドを使用することにより、頻繁に実行するタスクのスピードアップを図ることができます。

`omniintro` の man ページには、サポートされているすべての Data Protector コマンドや、UNIX および Windows プラットフォームでのコマンドの違いが記載されています。

「Data Protector のコマンド」(A-7 ページ) も参照してください。

Data Protector オンライン情報源

Data Protector に関する情報は、本ガイドとオンライン・ヘルプ・システムで得ることができます。本ガイドには、Data Protector ネットワークのプランニングと管理に必要な情報や、一般的な作業に関する説明が記載されています。オンライン・ヘルプにより、実行可能なすべての作業を実行するのに必要な情報が提供されます。

以下に示す Data Protector オンライン情報源が使用可能です。

ヘルプ・トピック	タスクの実行方法や参照情報に関するオンライン・ヘルプ。目次やインデックス、検索機能を使ってトピックを選択できます。
ヘルプ・ナビゲータ	コンテキスト依存のヘルプで、現在作業中のタスクの詳しい内容を表示します。
オンライン・ドキュメント	PDF 形式のオンライン・マニュアル (Adobe Acrobat Reader を使用)。
Data Protector Web サイト	Web ブラウザを起動し、Data Protector の Web ページを表示します。Data Protector の詳しい内容が記載されています。
オンライン・サポート	Web ブラウザで、HP OpenView 対話型オンライン・サポート・サービスのページを開きます。
情報	Data Protector のバージョン、著作権情報、ライセンス情報を表示します。

オンライン情報源を表示するには、［ヘルプ］ドロップダウン・メニュー、または Data Protector の各ウィンドウにある［ヘルプ］ボタンを使用します。

ヘルプ・テキスト内には、関連情報や定義へのハイパーリンク（相互参照）があります。ハイパーリンクが付いている単語や語句をクリックすると、新しいトピックに「ジャンプ」できます。ハイパーリンクされた単語や語句には下線が付くか、本文とは別の色で表示されます。

ヘルプ・ナビゲータの起動と使用方法

ヘルプ・ナビゲータはコンテキスト依存のオンライン・ヘルプで、現在の GUI パネルやタスクについての情報を得るために使用します。

GUI が Windows 上で実行されている場合、ヘルプ・ナビゲータはダイナミックになります。ヘルプ・ナビゲータを起動すると、ウィザードで次のページへ進んだり、Data Protector ユーザー・インタフェースの別の画面を表示した場合にヘルプの内容が自動的に変わります。

ヘルプ・ナビゲータを起動するには、以下のいずれかを行います。

- [F1] キーを押します。
- ヘルプ・メニューの [ヘルプ・ナビゲータ] をクリックします。
- ボタン・バーの [ヘルプ・ナビゲータ] アイコン (? マーク) をクリックします。

オンライン・マニュアルの使用

Data Protector では PDF 形式のオンライン・マニュアルが提供されます。このマニュアルは Adobe Acrobat Reader を使って表示します。インストールしたオンライン・マニュアルは、Cell Manager システムの *<Data_Protector_home>*¥Docs ディレクトリ (Windows の場合)、または /opt/omni/doc/ja ディレクトリ (HP-UX または Solaris の場合) に格納されます。

Microsoft 管理コンソール (MMC) の使用

Windows システムでは、Data Protector GUI を Microsoft 管理コンソールと統合することが可能です。

Microsoft 管理コンソール (MMC) は、共通のインタフェース環境内での管理ツールの管理 / 実行に使用できるグラフィカル・ユーザー・インタフェース (GUI) です。この管理コンソールに、既にインストール済みのソフトウェア、ハードウェア、ネットワーク管理アプリケーションを追加することができます。**管理コンソールに追加できる主要なツールをスナップ・イン**と呼びます。

Data Protector のスナップ・インは、**OB2_Snap** と呼ばれ、Data Protector と MMC の基本的な統合を行います。OB2_Snap を使用して、Data Protector のホームページや Data Protector Web/Java レポートを表示できます。また、MMC から Windows 上の Data Protector GUI を起動することもできます。

OB2_Snap を MMC に追加するには、以下の手順に従ってください。

1. MMCソフトウェアを http://www.microsoft.com/downloads/search.aspx?displaylang=ja からダウンロードします。
2. Windows のデスクトップで、[スタート] をクリックし、[ファイル名を指定して実行] を選択します。
3. [名前] テキスト・ボックスに `mmc` と入力し、[`Microsoft` 管理コンソール] ウィンドウを開きます。
4. [ファイル] メニューから [スナップインの追加と削除 `...`] を選択します。[スナップインの追加と削除 `...`] ウィンドウの [スタンドアロン] プロパティ・ページの [追加 `...`] をクリックします。
5. [スタンドアロン スナップインの追加] ウィンドウで、[HP OpenView Storage Data Protector] 選択し、[追加] をクリックします。[閉じる] をクリックしてウインドウを終了し、[`OK`] をクリックして [`Microsoft` 管理コンソール] ウィンドウに戻ります。

   [コンソール ルート] に [HP OpenView Storage Data Protector] という項目が表示されます。MMC にアプリケーションを追加したら、ファイルを *<Console_Name>*`.msc` という名前で保存します。

Data Protector 設定作業の概要

Data Protector の構成は容易に行えますが、より高度なプランニングにより、環境を構成して、最適な状態でバックアップを実行することができます。本項では、バックアップ環境を設定するための全体的な作業の概要を説明します。

環境の規模や複雑さによっては、以下の手順をすべて実行する必要はない場合があります。

1. ネットワークと組織構造を分析して、バックアップする必要があるシステムを決定します。詳細については、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。
2. バックアップ対象となる特殊なアプリケーションやデータベースがあるかチェックします (Microsoft Exchange、Microsoft SQL、Oracle、SAP R/3 など)。Data Protector では、このような製品向けの統合ソフトウェアを提供しています。

   統合ソフトウェアの構成方法については、『HP OpenView Storage Data Protector インテグレーション・ガイド』も参照してください。
3. Data Protector セルの構成について、以下のような点を決定します。
   - Cell Manager として使用するシステム
   - ユーザー・インタフェースをインストールするシステム
   - バックアップの種類 (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・デバイスや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. セットアップに必要な Data Protector ライセンスを購入します。このライセンスにより、インストールに必要なパスワードを入手できます。

   または、一時パスワードを使って Data Protector を動作させることもできます。ただし、このパスワードの有効期間はインストール後 60 日間しかありません。詳細は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。
5. セキュリティ面を検討します。

- セキュリティ上注意すべき点を分析します。詳細は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。
- ユーザー・グループをどのように構成するか検討します。

6. バックアップの内容を決めます。
   - メディア・プールの種類と使用方法
   - デバイスの種類と使用方法
   - 各バックアップのコピーの数
   - バックアップ仕様の数と分類方法
7. Data Protector Cell Manager およびインスト ール・ サーバをインスト ールします。次に、Data ProtectorGUI を使用して Data Protector エージェント を他のシステムに配布します。詳しい手順については、『 HP OpenView Storage Data Protector インスト ールおよびライセンス・ ガイド 』を参照してください。
8. バックアップ・デバイスを構成します。第 2 章「バックアップ・デバイスの 構成と使用」(17 ページ) を参照してください。
9. メディア・プールを構成し、メディアを準備します。第 5 章「メディアの管理」(151 ページ) を参照してください。
10. バックアップ仕様を構成します。IDB 用のバックアップ仕様も必要です。第 6 章「バックアップ」(207 ページ) を参照してください。
11. 必要に応じてレポートを構成します。第 9 章「モニター、レポート、通知、およびイベント・ログ」(407 ページ) を参照してください。
12. 障害復旧に対する準備をします。第 12 章「障害復旧」(545 ページ) を参照してください。
13. 以下の作業について十分理解します。
    - バックアップが失敗した場合の対処方法
    - 復元の実行
    - バックアップ・データの複製とメディアのボールティング
    - 障害復旧のテスト
    - IDB の保守

2 バックアップ・デバイスの構成と使用

本章の概略

本章では、以下の項目について説明します。

「デバイスの同時処理数、セグメントおよびブロック・サイズ」（101 ページ)

「デバイス性能の調整」（106 ページ)

注記

バックアップ・デバイス (テープ・ドライブなど) では、専用の Data Protector ライセンスが必要になる場合があります。詳細は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

バックアップ・デバイスの構成

バックアップ・デバイスを準備するには、デバイスをシステムに接続し、関連付けられているデバイスファイル (SCSI アドレス) のどれを使用するかを確認します。デバイスの構成手順は以下のとおりです。

1. バックアップ・デバイスをコンピュータ・システムに接続します。接続方法については、デバイスに付属のマニュアルを参照してください。
2. 必ず、以下の手順を行ってください。

UNIX システムの場合

UNIX システムに接続されているデバイスのデバイスファイル名を作成または検索します。詳しい手順については、オンライン・ヘルプの索引キーワード「デバイスファイル名の作成」または「デバイスファイル名の確認」を参照してください。詳細は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』の「付録 B」を参照してください。

Windows システムの場合

SCSI アドレスを設定し、Windows システムに接続されているデバイスで使用するドライバをロードします。

テープ・ドライブに関して、Windows のネイティブ・テープ・ドライバの処置は以下のいずれかを選択できます。

- アンロードする。(推奨)
- ロードしたままにする。

  デバイスファイル名は、Windows ネイティブ・テープ・ドライバがどのテープ・ドライブで使用されているかによって決まります。

SCSI アドレスの取得方法は、オンライン・ヘルプの索引キーワード「SCSI アドレスの作成」を参照してください。詳細は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』の「付録 B」を参照してください。

Windows ロボティクス・ドライバ

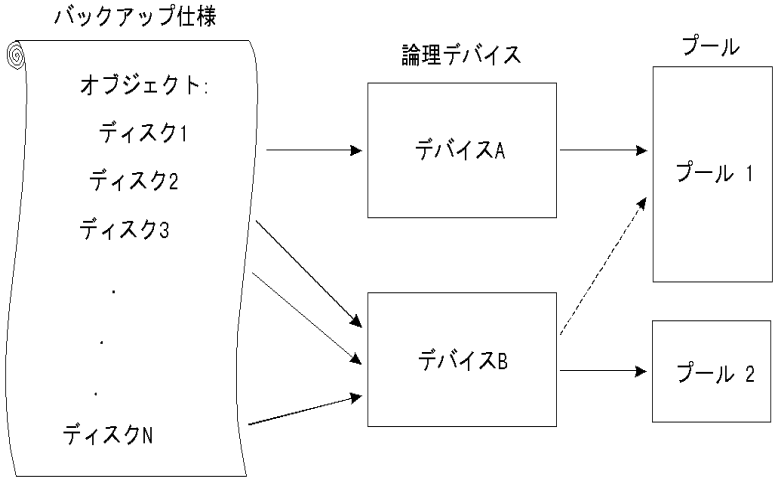
Windows では、Data Protector を使ってロボティクス・デバイスを構成する前に、Removable Storage Service または Windows メディア・チェンジャー (ロボティクス) ドライバを無効にしてください。詳しい手順については、オンライン・ヘルプの索引キーワード「ロボティクス・ドライバ」を参照してください。詳細は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』の「付録 B」を参照してください。

3. システムをブートし、システムにデバイスを認識させます。
4. 以降の項の説明に従って、デバイスを Data Protector で使用できるように構成します。
5. バックアップに使用するメディアを準備します。メディアのフォーマット方法は、「メディアのフォーマット」(164 ページ) を参照してください。

   各デバイスに対してはデフォルトのメディア・プールが使用されるので、メディア・プールを新規作成する必要はありません。メディア・プールを新規作成する場合は、「メディア・プールの作成」(157 ページ) を参照してください。

   図 2-1 (22 ページ) に、バックアップ仕様、デバイス、メディア・プールの相互関係を示します。デバイスはバックアップ仕様内で参照されます。一方、各デバイスはデフォルトのメディア・プールにリンクしています。このデフォルトのメディア・プールはバックアップ仕様で変更できます。

図 2-1　バックアップ仕様、デバイス、メディア・プールの相互関係



スタンドアロン・デバイスの構成

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、単体ドライブで同時に 1 つのメディアに対してのみ読み書きを行うような単純なバックアップ・デバイスを指し、小規模なバックアップに使用します。メディアがいっぱいになった場合、オペレータは手動で新しいメディアと取り替えてバックアップを続行する必要があります。したがって、スタンドアロン・デバイスは、無人で実行する大規模なバックアップには適していません。

Data Protector では、スタンドアロン・バックアップ・デバイスで使用するメディアを容易に構成 / 管理できます。

スタンドアロン・デバイスの構成方法

「バックアップ・デバイスの構成」(20 ページ) の説明に従って、構成するデバイスの準備が完了したら、スタンドアロン・デバイスを構成して、このデバイスを Data Protector で使用できるようにします。［デバイス / メディア］コンテキストで［デバイス］を右クリックして、[デバイスの追加] をクリックします。[デバイスの追加] ウィザードで、デバイスの種類として [スタンドアロン] を指定します。詳細は、図 2-2 を参照してください。

詳しい手順と例については、オンライン・ヘルプの索引キーワード「スタンドアロン・デバイスの構成」を参照してください。

Data Protector は、特定のバックアップ・デバイスをサポートしています。サポートされるデバイスと対応するメディアの種類の詳しいリストについては、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

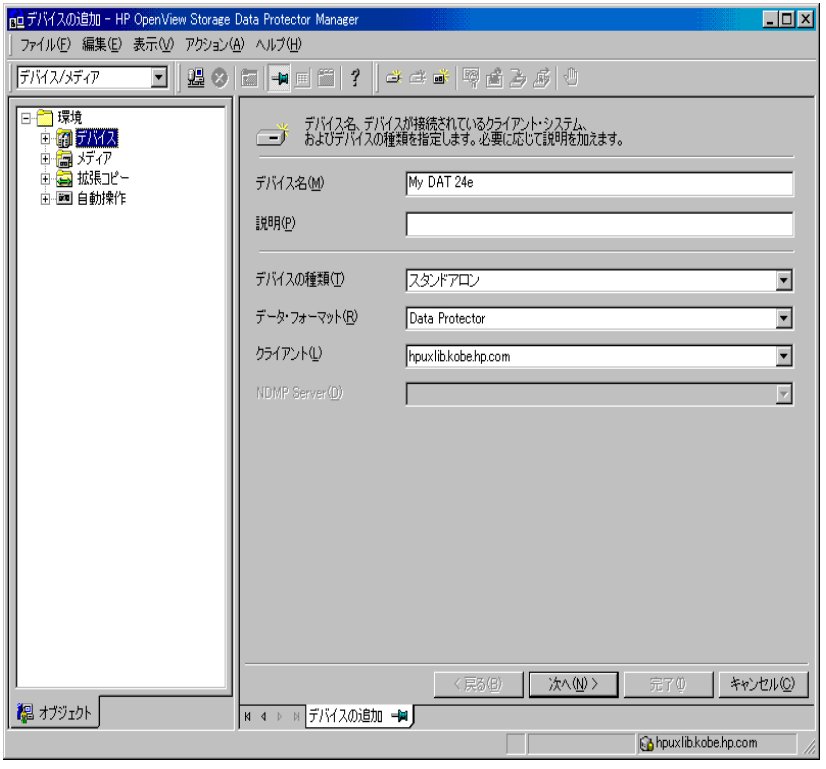
使用したいデバイスが、サポート対象のリストにない場合は、「新しいデバイスのサポート」(51 ページ) を参照してください。

ヒント

最も頻繁に使用するデバイスを Data Protector が自動的に構成するよう設定できます。ユーザーは、バックアップ・セッションに使用するメディアを準備することが必要ですが、その後は、Data Protector がデバイスの名前、ポリシー、メディアの種類、メディアのポリシー、デバイスの SCSI アド

レスまたはデバイスファイルを自動的に決定します。詳しい手順については、オンライン・ヘルプの索引キーワード「バックアップ・デバイスの自動構成」を参照してください。

図 2-2 **デバイスの種類とデバイス名の指定**



デバイス・チェーンの構成

Data Protector を使用して、同じ種類のスタンドアロン・デバイスを**デバイス・チェーン**に構成することができます。あるデバイス内のメディアがいっぱいになった場合、バックアップは、デバイス・チェーン内の次のデバイスにあるメディア上で自動的に続行されます。デバイス・チェーンを使用できる Media Agent は 1 つだけです。つまり、デバイス・チェーンは 1 つのシステム上にしか接続できません。

デバイス・チェーンの構成方法は、スタンドアロン・デバイスの構成方法と同じですが、複数の SCSI アドレス (Windows の場合) またはデバイスファイル名 (UNIX の場合) を入力する点が異なります。

注記

デバイスを追加する順番によって、Data Protector がデバイスを使用する順番が決まります。

デバイス・チェーン内のすべてのメディアがいっぱいになった場合、Data Protector はマウント要求を発行します。この場合、オペレータは**最初のデバイス**内にあるメディアを新しいメディアと交換して、新しいメディアをフォーマットした後、マウント要求の確認を行うことが必要です。Data Protector は、認識可能なメディアで、書込み保護が設定されていないものであればすぐに使用できます。また、Data Protector は中身が空のメディアも使用できるので、ユーザーがそのメディアをフォーマットする必要はありません。

ライブラリ・デバイスの構成

ライブラリ・デバイスとは

SCSI ライブラリ・デバイスは大容量バックアップ・デバイスで、オートローダとも呼ばれます。このデバイスのレポジトリには多数のメディア・カートリッジが含まれており、複数のドライブを収容できるので一度に複数のメディアを扱うことができます。また大部分のライブラリ・デバイスは、ドライブの自動クリーニングを構成できるので、ドライブが汚れた場合は、Data Protector によって自動的にクリーニングが行われます。詳細は、「ドライブのクリーニング」(87 ページ) を参照してください。

ライブラリ・デバイスには、デバイス内の各ドライブ用の SCSI ID と、ライブラリ・ロボティクス機構用の SCSI ID があります。この機構は、メディアをスロットからドライブへ、またドライブからスロットへ移動させるものです。たとえば、4 台のドライブを持つライブラリは 5 つの SCSI ID を持っています。このうち 4 つはドライブ用、1 つはロボティクス機構用です。

スロット番号

デバイスのレポジトリ内の各スロットには 1 つのメディアを入れます。Data Protector は各スロットに対して 1 から順に番号を割り当てます。ユーザーはライブラリを管理する際に、スロット番号を使ってスロットを参照します。たとえば、48 個のレポジトリ・スロットを持つライブラリのスロット番号は、1、2、3、4、5、6...47、48 となります。

ドライブのインデックス

ドライブのインデックスにより、ライブラリ内のドライブの機械的位置を識別します。詳細は、図 2-3 を参照してください。

インデックス番号はロボット制御に必要となります。ロボットはインデックス番号だけを認識し、ドライブの SCSI アドレスは認識しません。ドライブ・インデックスは (1 から始まる) 連続する整数で、このドライブの SCSI アドレスと関連付ける必要があります。たとえば、4 台のドライブを持つライブラリの場合、ドライブ・インデックスは 1、2、3、4 となります。

ライブラリ内のドライブが 1 台だけの場合は、ドライブ・インデックスは 1 となります。

ドライブの SCSI アドレス

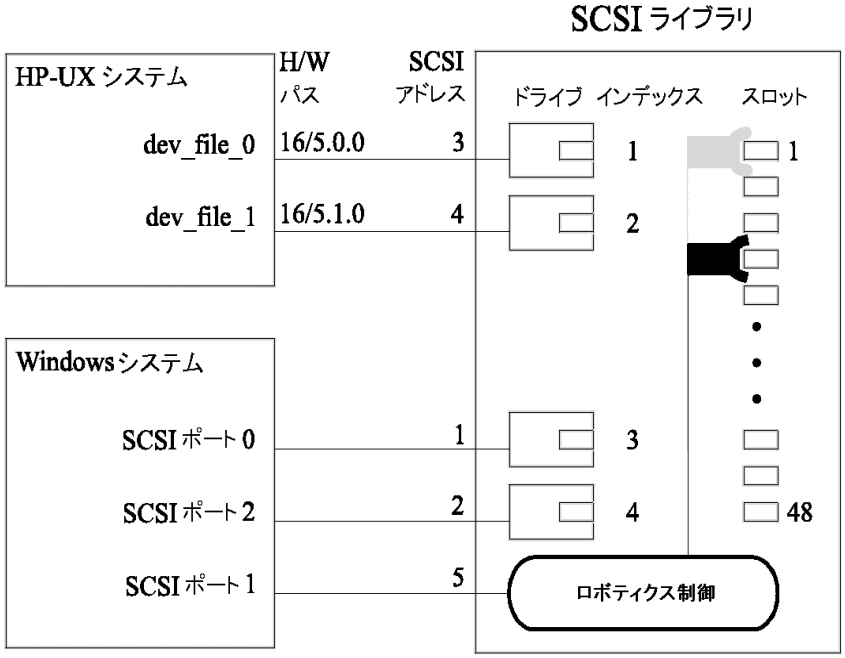
ドライブのインデックスは、SCSI アドレスと一対一で対応させる必要があります。つまり、次のようなペアを構成する必要があります。

SCSI アドレス A - インデックス 1
SCSI アドレス B - インデックス 2、など。

注記

Data Protector で使用するすべてのドライブを構成する必要はありません。全ドライブに対して 1 つのメディア・プールを構成したり、各ドライブに対して個別のメディア・プールを構成することができます。デバイスを構成する場合はデフォルトのメディア・プールを使用することをお勧めします。

図 2-3　SCSI アドレスに対するドライブ・インデックスのマッピング



ライブラリ・デバイスの構成方法

「バックアップ・デバイスの構成」(20 ページ) の説明に従って、構成するデバイスの準備が完了したら、ライブラリ・デバイスとドライブを構成します。どちらも、[デバイスの追加] ウィザードの指示に従って構成できます。詳しい手順と例については、オンライン・ヘルプの索引キーワード「構成ー SCSI ライブラリ」を参照してください。

ヒント

ライブラリ・デバイスを Data Protector が自動的に構成するよう設定することもできます。ユーザーは、バックアップ・セッションに使用するメディアを準備することが必要ですが、その後は、Data Protector がデバイスの名前、ポリシー、メディアの種類、メディアのポリシー、デバイスの SCSI アドレスを自動的に決定し、ドライブとスロットの構成も行います。詳しい手順については、オンライン・ヘルプの索引キーワード「バックアップ・デバイスの自動構成」を参照してください。

デバイス構成を検証するには、作成したドライブを右クリックして、[メディアのスキャン] を選択します。デバイスが正しく構成されていれば、Data Protector はスロット内のメディアのロード、読み取り、アンロードを行うことができます。

次に行う手順

Data Protector で使用するすべてのバックアップ・デバイスの構成が完了したら、以下を行います。

- 上記で構成したデバイスで使用するメディアをメディア・プールに追加します。詳細は、「メディア・プールへのメディアの追加」(162 ページ) を参照してください。
- クリーニング・テープを構成する場合は、「ドライブのクリーニング」(87 ページ) を参照してください。
- お使いのデバイスがバーコードを使用している場合は、「バーコードのサポートを可能にする」(93 ページ) を参照してください。
- データのバックアップを構成します。詳細は、第 6 章「バックアップ」(207 ページ) を参照してください。

複数システムによるライブラリの構成

Data Protector では、ライブラリを構成して、Media Agent(General Media Agent または NDMP Media Agent) が動作している別のシステムからデータを受信するように構成できます。この場合でも、ライブラリ・ロボティクス制御は、General Media Agent または NDMP Media Agent がインストールされた 1 台のシステムが行います。これにより、データをネットワーク経由で移動させる代わりにローカル・バックアップを実行できるので、ハイエンド環境での性能が向上します。

必要条件

- ライブラリ内のドライブと共に使用する各クライアント・システムには、Data Protector Media Agent(General Media Agent または NDMP Media Agent) のコンポーネントをインストールしておく必要があります。
- バックアップ・デバイスを Data Protector で使用できるように構成する前に、バックアップ・デバイスをシステムに接続し、デバイスファイル (SCSI アドレス) が存在することを確認しておく必要があります。

複数ドライブのサポートの詳細は、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

複数システムによるライブラリの構成方法

「ライブラリ・デバイスの構成」(26 ページ) の手順に従って、ライブラリを構成します。ライブラリ内のドライブの構成を要求するメッセージが表示された場合は、各ドライブに使用するクライアント・システムを指定します。詳しい手順については、オンライン・ヘルプの索引キーワード「複数システム用のライブラリの構成」を参照してください。

ヒント

デバイス構成を検証するには、ライブラリから目的の範囲のスロットを選択して、[アクション] メニューの [スキャン] をクリックします。デバイスが正しく構成されている場合は、Data Protector はメディアをロードして読み取り、スロットへ再びアンロードすることができます。

次に行う手順

Data Protector で使用するすべてのバックアップ・デバイスの構成が完了したら、以下を行います。

- 上記で構成したデバイスで使用するメディアをメディア・プールに追加します。「メディア・プールへのメディアの追加」(162 ページ) を参照してください。
- クリーニング・テープを構成する場合は、「ドライブのクリーニング」(87 ページ) を参照してください。
- お使いのデバイスがバーコードを使用している場合は、「バーコードのサポートを可能にする」(93 ページ) を参照してください。
- バックアップを構成します。第 6 章「バックアップ」(207 ページ) を参照してください。

マガジン・デバイスの構成

マガジン・デバイスとは

マガジン・デバイスとは、多数のメディアを**マガジン**と呼ばれる 1 つのユニットにまとめたものです。マガジンを使うことにより、個々のメディアを多数使用するよりも容易に大容量のデータを処理できます。

Data Protector では、メディアの管理作業をマガジン上でまとめて行ったり、単一のメディア上で行うことができます。

必要条件

[マガジンのサポート] オプション・セットを使って、メディア・プールを少なくとも 1 つ構成します。「メディア・プールへのメディアの追加」(162 ページ) を参照してください。

マガジン・デバイスの構成方法

マガジンはライブラリとして構成することが必要です。[デバイスの追加] ウィザードで、デバイスの種類として [SCSI ライブラリ] を選択します。マガジンが所属するメディア・プールでは、[マガジンのサポート] オプションを選択しておく必要があります。詳しい手順については、オンライン・ヘルプの索引キーワード「構成ー SCSI ライブラリ」を参照してください。

ヒント

お使いのデバイスを Data Protector が自動的に構成するよう設定できます。ユーザーは、バックアップ・セッションに使用するメディアを準備することが必要ですが、その後は、Data Protector がデバイスの名前、ポリシー、メディアの種類、メディアのポリシー、デバイスの SCSI アドレスを自動的に決定し、ドライブとスロットの構成も行います。詳しい手順については、オンライン・ヘルプの索引キーワード「バックアップ・デバイスの自動構成」を参照してください。

デバイス構成を検証するには、作成したドライブを右クリックして、[スキャン] を選択します。デバイスが正しく構成されていれば、Data Protector はスロット内のメディアのロード、読み取り、アンロードを行うことができます。

次に行う手順

Data Protector で使用するすべてのバックアップ・デバイスの構成が完了したら、以下を行います。

- クリーニング・テープを構成する場合は、「ドライブのクリーニング」(87 ページ) を参照してください。
- お使いのデバイスがバーコードを使用している場合は、「バーコードのサポートを可能にする」(93 ページ) を参照してください。
- データのバックアップを構成します。詳細は、第 6 章「バックアップ」(207 ページ) を参照してください。

スタッカー・デバイスの構成

スタッカー・デバイスとは

スタッカーとは、1 台のドライブが接続された単一デバイスで、メディアへは 1 つずつ順にしかアクセスできません。複数のスタッカー・デバイスの使用は、小規模なライブラリをひとつだけ使用するよりも、人手によるメディア管理が多く必要となります。Data Protector は、バックアップ用スタッカー・デバイスで使用するメディアを容易に構成 / 管理する機能を備えています。

スタッカー・デバイスの構成方法

スタッカー・デバイスを作成するには、[デバイスの追加] ウィザードで、デバイスの種類として [スタッカー] を選択します。詳しい手順については、オンライン・ヘルプの索引キーワード「構成ースタッカー・デバイス」を参照してください。

スタッカー・デバイスのメディア管理

スタッカー・デバイスでは、スキャン、検証、またはフォーマットの各操作は個々のメディア上で別々に実行する必要があります。これらの操作を行う際に、各メディアが自動的にロードされるように、[操作後メディアを取出し] オプションを使用してください (最初のメディアだけ手動でロードする必要があります)。スタッカー・マガジン内のすべてのテープが使用されたら、手動でマガジンを取り外し、次のマガジンを挿入します。

スタッカーでは、メディアが順にロードされるので、メディア割り当てポリシーとしては [Loose] が適しています。[Strict] ポリシーを設定すると、メディアを使用順にロードしなければなりません。

例

1. 1 番目のメディアを手動でロードします。
2. [操作後メディアを取出し] オプションを設定した状態で) フォーマット / 検証 / スキャンを実行します -- (2 番目のテープが自動的にロードされます)。
3. すべてのテープに対してステップ 2 を繰り返します。
4. スタッカー・マガジン内のすべてのテープが使用されたら、手動でマガジンを取り外し、次のマガジンを挿入します。

注記

メディアが正しくロードされていない場合、Data Protector はセッションを中止します。

スタッカー・デバイスを使ったバックアップと復元

最初のメディアだけは手動でロードする必要があります。テープがデータで満杯になると、このテープが取り出され、2 番目のテープが自動的にロードされます。スタッカー・マガジン内のすべてのテープが使用されたら、このマガジンを手動で取り外し、次のマガジンを挿入します。新しく挿入したマガジンについても、最初のテープは手動でドライブに挿入する必要があります。

注記

メディアが挿入されていない場合でも、バックアップ・セッションまたは復元セッションは中止されませんが、代わりにマウント要求が発行されます。タイムアウト期間内にスタッカー・マガジンの交換が行われなかった場合でも、セッション全体は中止されません。

ADIC/GRAU DAS ライブラリと STK ACS ライブラリの構成

本章では、ADIC/GRAU または STK ACS ライブラリの物理的な構成が完了していると想定して説明します。構成が完了していない場合は、ADIC/GRAU または STK ACS ライブラリに付属のマニュアルを参照して、ライブラリを構成してください。サポートされているソフトウェア・バージョンのリストは、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

注記

ADIC/GRAU と STK の機能では、専用の Data Protector ライセンスが必要になる場合があります。詳細は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

バックアップ対象のデータ量が膨大なため、データの保存に大量のメディアを必要とする複雑な環境では通常、Data Protector と ADIC/GRAU DAS または STK ACS との統合が必要です。ADIC/GRAU ライブラリと STK ACS ライブラリは、大量のメディアを管理できるだけでなく、Data Protector 以外の複数のアプリケーションが使用するメディアの管理も可能です。

Data Protector は、ADIC/GRAU DAS および STK ACS ライブラリ・システムをフル・サポートしています。これらのライブラリは複数のアプリケーションが使用するメディアを管理するため、ユーザーは、Data Protector で使用するメディア、トラッキング対象のメディア、Data Protector で使用するドライブを構成することが必要です。図 2-4 (36 ページ) と図 2-5 (36 ページ) では、2 つのライブラリがそれぞれ Data Protector と統合された状態を示します。

図 2-4 **Data Protector と ADIC/GRAU DAS ライブラリ**

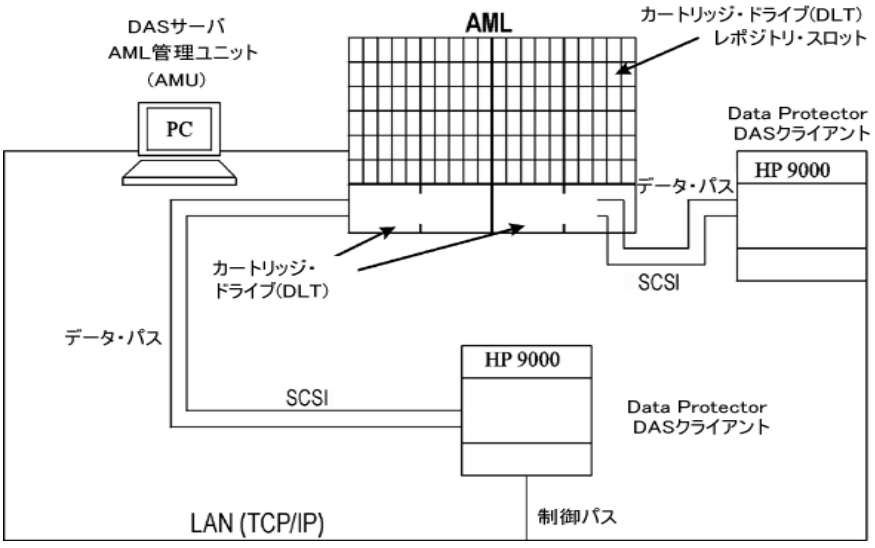
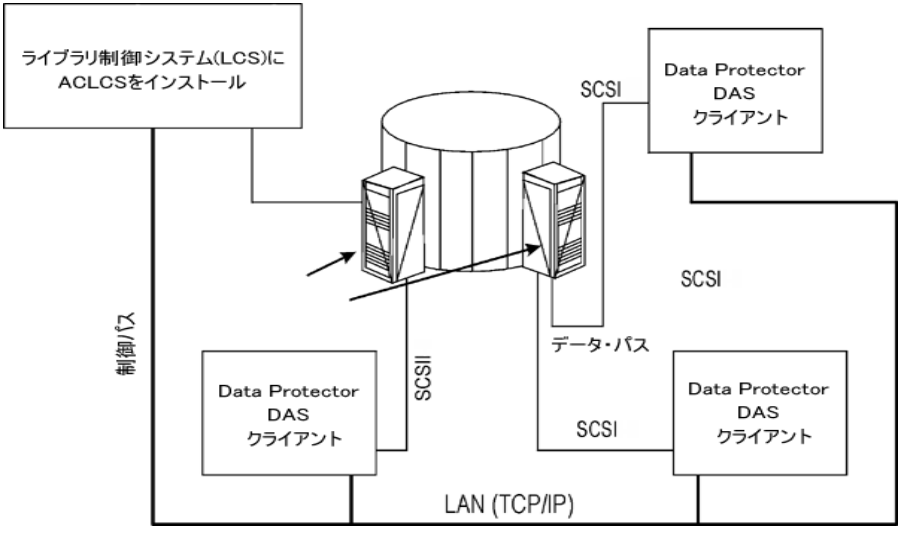


図 2-5 **Data Protector と StorageTek ACS ライブラリ**



構成の基本的概念

GRAU/ADIC DAS または STK ACS ライブラリ・サーバ経由でライブラリ・ロボティクスにアクセスするクライアントと、ドライブにアクセスするクライアントには、Data Protector Media Agent ソフトウェア (General Media Agent または NDMP Media Agent) をインストールする必要があります。

メディア管理の基本的概念

ADIC/GRAU DAS および STK ACS ライブラリ・デバイスでは、メディアは、ボリューム・シリアル番号 (VOLSER) によって識別されます。バーコードと同様の働きをする VOLSER によって、各メディアは使用期限が切れるまで一意に識別されます。

ライブラリ内のメディアを使用できるアプリケーションは Data Protector 以外にも多数あります。したがって、どのアプリケーションがどのメディアを使用しているかを把握して、メディアが上書きされないよう注意が必要です。

ADIC/GRAU または ACS ライブラリを Data Protector とだけ併用し、Data Protector を使ってライブラリ全体を管理することが理想的です。ただし、別のアプリケーションでこれらのライブラリを使用している場合、Data Protector と別のアプリケーションに対して割り当てるメディアのサブセットが重複しないよう注意が必要です。また、Data Protector はスクラッチ・プールを使用しませんが、独自のメディア割当てポリシーを持っていることにも注意してください。これは、特定のメディアが Data Protector に割り当てられた (Data Protector メディア・プールに追加された) 場合に、このメディアは、使用期限が切れるか、Data Protector メディア・プールから取り出されるまで、Data Protector の管理対象となることを意味します。

重要

Data Protector では各種類のメディアにそれぞれ独自のライブラリを指定する必要があります。ADIC/GRAU または STK ACS システムでは、物理的に種類の異なる、さまざまなメディアを使用できますが、Data Protector は、メディアが 1 種類のライブラリしか認識できません。したがって、DAS システムではメディアの各種類ごとに、Data Protector の**論理**ライブラリを作成する必要があります。「ADIC/GRAU DAS または STK ACS ライブラリで使用される Data Protector 照会操作」（39 ページ) も参照してください。

メディアの実際の物理的な位置は、Data Protector ではなく DAS サーバ (ADIC/GRAU ライブラリ内) または ACS サーバ (STK ACS ライブラリ内) によって管理されます。DAS サーバまたは ACS サーバは、VOLSER を使ってメディアの位置をトラッキングします。メディアがレポジトリ内を移動した場合、そのメディアは毎回同じ物理スロットに割り当てられるわけではありません。したがって、メディアを扱う際は、スロット番号ではなくバーコード (VOLSER) に基づいて区別してください。

Data Protector では、デバイスのレポジトリ内にあるメディアについては、メディアの位置が**「常駐」**と表示され、デバイスのレポジトリ外にあるメディアについては、**「非常駐」**と表示されます。

注記

Data Protector は、認識可能な形式のデータが含まれているメディアは上書きしません。ただし、テープ上の Data Protector データが、同じメディアを使用する別のアプリケーションによって上書きされないという保証はありません。したがって、Data Protector が使用するメディアを別のアプリケーションが使用しないように、また別のアプリケーションが使用するメディアを Data Protector が使用しないように注意することをお勧めします。「ADIC/GRAU DAS または STK ACS ライブラリで使用される Data Protector 照会操作」(39 ページ) も参照してください。

メディアの トラッキング

Data Protector は、Data Protector メディアと非 Data Protector メディアの両方をトラッキングします。認識可能な形式のメディアについては、Data Protector はその形式をメディアの種類として表示します (**「tar」**など)。認識不可能な形式のメディアについては、Data Protector はそのメディアの種類として**「無関連」**と表示します。

メディア・ラベルの 付与

Data Protector は、使用する各メディアに対して一意のメディア・ラベルとメディア ID を付与します。 メディア・ラベルとメディア ID は IDB に保管され、メディアの管理に使用されます。メディア ID は Data Protector によって割り当てられます。 メディア・ラベルとは、ユーザーが定義する説明とメディアのバーコード (VOLSER) を組み合わせたものです。

ユーザーは、自分でもラベルを変更したりバーコード番号をラベルから除外することができますが、このような作業はあまりお勧めしません。一度手を加えてしまうと、ユーザーは実際のバーコードとメディアに割り当てたメディア・ラベルを手動でトラッキングしなければならなくなります。

他の形式のフォーマット

Data Protector がメディアの別のデータ形式または別のアプリケーションが使用したメディアを認識した場合、[強制] オプションを選択しない限り、メディアはフォーマットされません。Data Protector は、以下のデータ形式およびアプリケーションが使用したメディアを認識します。tar、cpio、Fbackup、FileSys、Ansi、OmniStorage。

ドライブ・クリーニングのサポート

ADIC/GRAU DAS および STK ACS ライブラリには、ライブラリ内のドライブがある一定の回数使用された後、ドライブを自動的にクリーニングする機能があります。ただし、このライブラリ内蔵クリーニング機能によりセッションが中断され、失敗する原因となるため、この機能の使用はお勧めできません。ライブラリのクリーニング機能を使用する場合は、Data Protector セッションが実行されていないことを確かめることが必要です。

ドライブの詳しいクリーニング方法については、「ドライブのクリーニング」(87 ページ) を参照してください。

ADIC/GRAU DAS または STK ACS ライブラリで使用される Data Protector 照会操作

Data Protector 照会操作の詳細は、「デバイス内のメディアのスキャン」(187 ページ) を参照してください。

Data Protector 照会操作が開始されると、DAS または ACS ライブラリ・サーバ上に構成されているすべてのメディアに対して照会が行われます。この照会は、複数の ADIC/GRAU DAS または STK ACS の**論理**ライブラリに属すものとして構成されているメディアに対しても行われます。

また、Data Protector 照会操作では、Data Protector 以外のアプリケーションで使用されるように構成された DAS または ACS ライブラリ・サーバ上に構成されているメディアに対しても照会を行います。この結果、Data Protector によって照会操作が開始されると、照会操作の開始された ADIC/GRAU DAS または STK ACS の**論理**ライブラリ以外のライブラリに属しているメディアは、照会操作の開始された ADIC/GRAU DAS または STK ACS の**論理**ライブラリに移動されます。

したがって、ADIC/GRAU DAS または STK ACS ライブラリで Data Protector 照会操作を使用することはお勧めできません。Data Protector 照会操作を使用して IDB を同期化する代わりに、Data Protector の VOLSER 追加操作を使用して、VOLSER を手動で追加することをお勧めします。

注記

ここで説明した内容は、論理ライブラリが Data Protector ではなく ADIC/GRAU DAS ユーティリティを使用して構成されている ADIC/GRAU DAS ライブラリには適用されません。多数の論理ライブラリが ADIC/GRAU DAS ユーティリティを使用して構成されている場合、これらのライブラリでは Data Protector 照会操作を安全に使用できます。

VOLSER を手動で追加する方法については、「手動による VOLSER の追加」(202 ページ) を参照してください。

メディア管理のヒント

GRAU DAS または STK ACS デバイスで Data Protector を使用する際は、以下のヒントを参考にしてください。

- 各種類のメディアにメディア・プールを少なくとも 1 つずつ構成します。たとえば、4mm タイプに 1 つ、3480 タイプに 1 つといった具合です。環境によっては、各部門ごとのメディア・プールなど、複数のメディア・プールを作成できます。メディア・プールのプランニング方法については、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。
- メディアを操作する際は、Data Protector コマンドを使用します。ADIC/GRAU DAS または STK ACS コマンドを使ってメディアを手動で操作した場合、Data Protector はメディアの位置や情報の変更を追跡できなくなります。
- Data Protector を使ってライブラリ全体を管理します。これにより、1 箇所からの管理が可能になり、ライブラリ内の Data Protector メディアと非 Data Protector メディアの両方をトラッキングできます。
- Data Protector とその他のアプリケーションが同じメディア・セットを使用しないようにしてください。

インストール

Data Protector で使用するために ADIC/GRAU または STK ACS ライブラリを準備する方法については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』の「Media Agent をインストールして ADIC/GRAU ライブラリまたは StorageTek ライブラリを使用する」を参照してください。さらに以下の項に示す手順を続けて実行します。

構成

Data Protector で ADIC/GRAU または STK ACS ライブラリを構成するには、以下の手順を実行します。

1. [HP OpenView Storage Data Protector Manager] で [デバイス / メディア] コンテキストを選択します。Scoping ペインで [デバイス] を右クリックした後、[デバイスの追加] をクリックします。
2. 必要に応じて、[マルチパス・デバイス] オプションを選択します。
3. デバイスの [デバイス名] と [説明] を入力します。
4. [デバイスの種類] ドロップダウン・リストで、[GRAU DAS ライブラリ] または [StorageTek ACS ライブラリ] を選択します。

   [マルチパス・デバイス] オプションを選択しなかった場合は、ADIC/GRAU または STK ACS のロボティクスにアクセスする Media Agent クライアントの名前を選択します。
5. 必要に応じて、[管理コンソールの URL] テキスト・ボックスに、ライブラリ管理コンソールの正しい URL を入力します。これによって、Data Protector GUI から直接 Web ブラウザを開いて、管理コンソールのインタフェースをロードできるようになります。

   [次へ] をクリックします。
6. ADIC/GRAU ライブラリを構成している場合は、[DAS サーバ] テキスト・ボックスに DAS サーバのホスト名を入力します。

   STK ACS ライブラリを構成している場合は、[ACSLM ホスト名] テキスト・ボックスに ACS ライブラリ・サーバのホスト名を入力します。

   マルチパス デバイスについては、クライアント名を選択して [追加] をクリックすることにより、構成されているパスの一覧にこのパスを追加します。

7. [ビジー・ドライブの処理] ドロップダウンリストで、いずれかのアクションを選択します。

   [次へ] をクリックします。

8. ADIC/GRAU ライブラリを構成している場合は、ライブラリのインポート / エクスポート領域を指定します。

   STK ACS ライブラリを構成している場合は、ライブラリの CAP を指定します。

   [次へ] をクリックします。

9. [メディアの種類] ドロップダウンリストでライブラリのメディアの種類を選択します。

   [完了] をクリックして、次に [はい] をクリックしてライブラリのドライブを構成します。

10. [デバイス名] テキスト・ボックスにドライブ名を入力します。

    [説明] テキスト・ボックスにドライブに関する説明を入力します。

    必要に応じて、[マルチパス・デバイス] オプションを選択します。

    [マルチパス・デバイス] オプションを選択しなかった場合は、ADIC/GRAU または STK ACS のロボティクスにアクセスする Media Agent クライアントの名前を選択します。

    [次へ] をクリックします。

11. [データのドライブ] ドロップダウンリストにデバイスのSCSIアドレスを入力します。

    マルチパス デバイスについては、ADIC/GRAU または STK ACS のロボティクスにアクセスする Media Agent クライアントの名前を選択して [追加] をクリックすることにより、構成されているパスの一覧にこのパスを追加します。

    変更された SCSI アドレスを自動検出できるように、[変更された SCSI アドレスの自動検出] を選択します。

    『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』の説明に従って、[ドライブ名] テキスト・ボックスに、Media Agent のインストール中に取得した ADIC/GRAU のドライブ名または STK ACS のドライブ ID を入力します。

[次へ] をクリックします。

12. [デフォルトのメディア・プール] ドロップダウンリストからメディア・プールを選択します。これが、構成しているデバイスのデフォルトのメディア・プールになります。

    必要に応じて [拡張オプション] ダイアログを表示して、[同時処理数] やその他の設定値を変更します。

    必要な場合は、[その他] タブの下にある [ロック名を使用] オプションを選択し、ロック名を指定します。このオプションの詳細は、「デバイスのロック」(99 ページ) を参照してください。

    [完了] をクリックします。

Data Protector で使用する各種類のメディア用にライブラリを作成します。

混合メディア用ライブラリの構成

混合メディア用ライブラリには、複数の種類のメディアが含まれています (DLT および光磁気ディスクなど)。このライブラリでは、(メディアの種類に関係なく) 同じロボティクスを使用してスロットとドライブ間ですべてのメディアを移動させます。

このライブラリ機能を使用するには、複数の (サブ) ライブラリを構成する必要があります (例 : 1 つのメディアの種類につきライブラリ定義を 1 つ作成する)。

この機能の利点をフルに活用するには、以下の手順を行うことが必要です。

- 1 つのメディアの種類につき、少なくとも 1 つのメディア・プールを構成します (またはデフォルトのプールを使用します)。
- 1 つのメディアの種類につき、ライブラリ・ロボティクスを 1 回構成します。対象となるメディアの種類に関するスロット範囲についても構成します。各ライブラリ・ロボティクス定義に対するロボティクス制御 (SCSI パス (Windows) またはデバイスファイル (UNIX)) が同一ホスト上に存在し、かつ、それらが同じであることを確認してください。
- メディアの種類ごとにすべてのドライブを構成し、それらを関連するライブラリ・ロボティクスとメディア・プールにリンクさせます。メディアの種類に関係なく、各物理デバイスに対して必ず一意のドライブ・インデックスを指定してください。

SAN 環境における物理デバイスへの複数のパスの構成

マルチパス・デバイスとは、1 つの物理デバイスに複数のパスを構成して、1 つの論理デバイスとして使用するデバイスを指します。このとき指定されるパスは、クライアント名と SCSI アドレス (UNIX の場合はデバイスファイル名) の組み合わせになります。

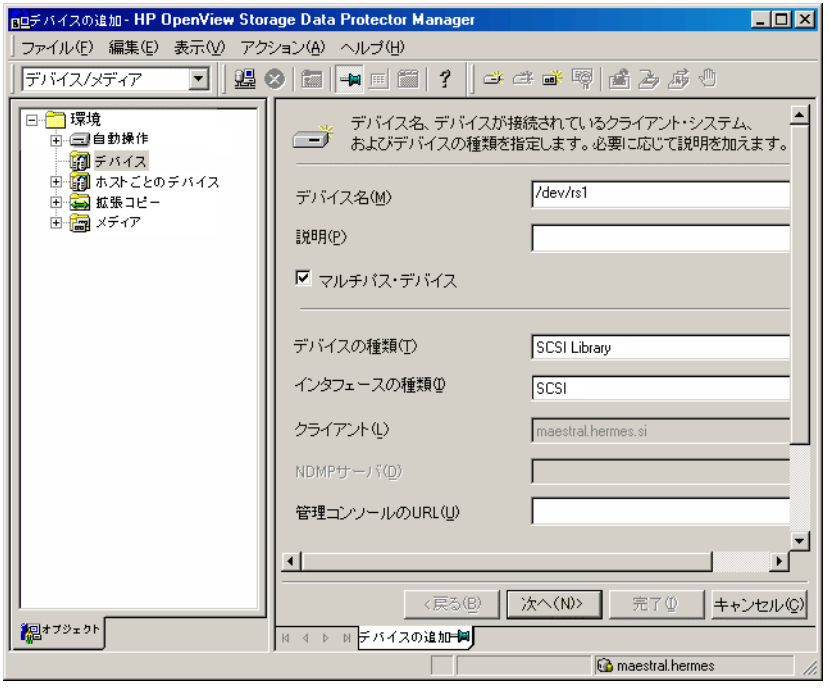
マルチパスの概念の詳細は、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

手動構成

1 つの物理デバイスに対して複数のパスを使えるようにするには、デバイス構成ウィザードを使用してデバイスを手動で構成します。

マルチパス・デバイスの構成方法については、オンライン・ヘルプの索引キーワード「構成 - 複数パス」を参照してください。

図 2-6 マルチパス・デバイスの有効化



自動構成

マルチパス・デバイスは、手動での構成以外にも、デバイスの自動構成や sanconf コマンドを使用することによって自動的に構成できます。

- デバイスの自動構成ウィザードのデフォルト動作では、複数のクライアントに接続されているすべての物理デバイスは、マルチパス・デバイスとして構成されます。詳細については、オンライン・ヘルプの索引キーワード「構成 - 複数パス」を参照してください。
- sanconf コマンドコマンドを、オプションなしまたは -no_multipath オプションを指定して実行した場合は、マルチパス・デバイスは**構成されません。**その場合、パスごとに個別の論理デバイスが構成されます。同一物理デバイスに対するすべてのパスを含むマルチパス・デバイスを構成するには、sanconf コマンドに -multipath オプションを指定して実行してください。

詳細は、「sanconf コマンドを使用した SAN 環境におけるライブラリの自動構成」（72 ページ) と、sanconf の man ページを参照してください。

制限事項

以下の制限事項が適用されます。

- NDMP デバイスとジュークボックス・ライブラリに対して、複数のパスはサポートされていません。
- デバイス・チェーンはマルチパス・デバイスに対してサポートされていません。
- マルチパス・デバイスを構成すると、libtab ファイルは無効になります。

ダイレクト・バックアップ用のデバイスの構成

本項では、ダイレクト・バックアップ環境で使用するバックアップ・デバイスの構成手順を説明します。ダイレクト・バックアップの概念の詳細は、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

ダイレクト・バックアップは、SAN 環境における Data Protector のバックアップ・ソリューションです。SAN 環境の一般的情報については、「SAN 環境内の共有デバイス」(54 ページ) を参照してください。ダイレクト・バックアップ用のデバイス構成手順は、上記の項で説明されている構成手順とは違うことに注意してください。ダイレクト・バックアップ用のデバイス構成手順は、本項で説明します。

ダイレクト・バックアップ環境は、以下の要素で構成されています。

- SAN ネットワーク
- 内部または外部ファイバー・チャネル・ブリッジ (FC ブリッジ)
- FC ブリッジに接続されたバックアップ・デバイス (スタンドアロンまたは SCSI ライブラリ)
- 物理 XCopy エンジン (FC ブリッジ内に存在)
- ポイント・イン・タイムでのデータの安定性を保証するディスク・アレイ (HP StorageWorks Disk Array XP)
- ディスク・アレイのオリジナル・ディスクに接続されたアプリケーション・システム
- ディスク・アレイのミラー・ディスクに接続され、SCSI ライブラリ・ロボティクスおよび SCSI ライブラリ / スタンドアロン・デバイス・ドライブを制御するバックアップ・システム

内部 FC ブリッジはバックアップ・デバイスに組み込まれているのに対し、外付け FC ブリッジは SAN 上に設置します。

ダイレクト・バックアップ環境で使用するバックアップ・デバイスは、バックアップ・デバイスに接続されている、または組み込まれている FC ブリッジのワールド・ワイド名 (WWN)、および SAN で使用されるデバイスと同様のデバイス (スタンドアロン・デバイス) またはドライブ (SCSI

ライブラリ) の論理ユニット番号 (LUN) で識別されます。SCSI ライブラリを使用する場合、そのロボティクスを FC ブリッジに接続する必要はありません。

バックアップ・デバイスの自動検出

XCopy エンジンは、バックアップ・デバイスまたはドライブが接続されている FC ブリッジ（外付け FC ブリッジ）、または内部ブリッジに装備されていなければなりません。ダイレクト・バックアップ機能で使用されるバックアップ・デバイスは、ダイレクト・バックアップ・セッションが開始されるたびに自動検出されます。自動検出を使用する場合でも、WWN パラメータと LUN パラメータはデバイス構成時に手入力する必要があり、LUN が変わるたびに LUN を再構成しなければなりません。

XCopy エンジン

ダイレクト・バックアップ環境では、複数の物理 XCopy エンジンを使用できます。各物理 XCopy エンジンを元に、複数の論理 XCopy エンジンを構成して割り当てられます。ダイレクト・バックアップ・セッションで使用する論理 XCopy エンジンは、ダイレクト・バックアップ仕様で指定します。これはダイレクト・バックアップ・セッションで使用するバックアップ・デバイスを選択し、それに論理 XCopy エンジンを割り当てることで指定できます。バックアップ仕様で指定した論理 XCopy エンジンの元となる物理 XCopy エンジンは、バックアップ仕様で指定したバックアップ・システムで実際に構成されていなければなりません。

Data Protector ダイレクト・バックアップでサポートされているバックアップ・デバイスの種類を次に示します。

- スタンドアロン・デバイス
- SCSI ライブラリ

構成手順

本項で説明するバックアップ・デバイスの構成を行う前に、次に示すオンライン・ヘルプの索引キーワードを参照して、必要な手順を実行してください。

- オンライン・ヘルプの索引キーワード「準備－バックアップ・デバイス」
- オンライン・ヘルプの索引キーワード「構成－ダイレクト・バックアップ環境」

ダイレクト・バックアップ用のバックアップ・デバイスの構成は、次の手順で行います。

1. スタンドアロン・デバイスまたは SCSI ライブラリの構成
2. XCopy エンジンの構成
3. libtab ファイルの構成 (ダイレクト・ライブラリ・アクセスを使用する場合)

スタンドアロン・デバイスの構成

ダイレクト・バックアップ用のスタンドアロン・デバイスの構成方法の詳細は、オンライン・ヘルプの索引キーワード「構成－ダイレクト・バックアップ用スタンドアロン・デバイス」を参照してください。

SCSI ライブラリの構成

ダイレクト・バックアップ用の SCSI ライブラリの構成方法については、オンライン・ヘルプの索引キーワード「ダイレクト・バックアップ用 SCSI ライブラリの構成」を参照してください。

XCopy エンジンの構成

ダイレクト・バックアップ用の XCopy エンジンの構成方法については、オンライン・ヘルプの索引キーワード「ダイレクト・バックアップ用 XCopy エンジンの構成」を参照してください。

libtab ファイルの構成

libtab ファイルの構成は、ダイレクト・ライブラリ・アクセスを使用する場合のみ必要です。

libtab ファイルの構成方法については、「libtab ファイルの手動構成」（66 ページ) を参照してください。

新しいデバイスのサポート

『HP OpenView Storage Data Protector ソフトウェア リリース ノート』でサポート対象として記載されていないデバイスを使用する場合は、scsitab ファイル用の最新ソフトウェア・パッケージを次の HP OpenView Web サイトからダウンロードしてください。

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

重要

scsitab ファイルの修正はサポートされていません。

scsitab ソフトウェア・パッケージをダウンロードしたら、付属のインストール手順にしたがってください。

scsitab ファイルは、デバイスが接続されているシステムの以下の場所にあります。

- *<Data_Protector_home>*¥scsitab (Windows プラットフォームの場合)
- /opt/omni/scsitab (HP-UX および Solaris プラットフォームの場合)
- /usr/omni/scsitab (上記以外の UNIX プラットフォームの場合)

デバイスの構成中にエラーが出る場合には、当社サポート担当にご連絡いただき、デバイスのサポート予定時期についてお尋ねください。

ライブラリ内で複数の種類のドライブを使用する

DLT 4000/7000/8000 など、同一ライブラリ内で同じテクノロジーを使用した複数の種類のドライブ (DDS 製品の場合も同様) を使用すると、すべてのメディアが同一フォーマットかどうか確かではない状態でいずれかのドライブでメディアを使用した場合に問題が発生するおそれがあります。

たとえば、DLT 4000 は、DLT 8000 (最も高密度) を使って書き込まれたテープを (復元時に) 読み取ることができません。圧縮されたメディアと圧縮されていないメディアには互換性がありません。

このような問題を回避するには、すべてのメディアを同一密度に設定するか、またはメディア・プールを分けてください。以降の項で、これらの解決法について説明します。

同一密度に設定

この方法では、すべてのメディアに対して共通のフォーマットを使用するため、どのドライブでもすべてのメディアを互換使用できます。

Windows システム上で使用するデバイスの場合、特定の書き込み密度の使用に関する情報については、ドライブに付属のマニュアルを参照してください。

UNIX システムの場合、ドライブに密度を設定するには、関連するデバイスファイル名を選択して、デバイス定義でそのファイル名を使用します。密度は同じ値に設定することが必要です。たとえば、ドライブ DLT 4000 と DLT 7000 の場合、DLT 4000 ドライブの密度を設定します。

使用するデバイスのブロック・サイズ設定が同じであることを確かめてください。メディアのフォーマット時に、デバイス定義内のこの設定がすでに使用されているはずです。

フリー・プールは、必要に応じて使用できます。

復元時は、任意のメディアを任意のドライブで使用できます。

HP-UX では、デバイスファイル名の作成時にドライブの密度を設定できます。詳細は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』の付録 B「HP-UX 上のデバイスファイルの作成」を参照してください。

個別のメディア・プールを設定 (UNIX および Windows)

この方法では、あるドライブのグループが使用するメディアと、別のドライブのグループが使用するメディアを区別します。これにより、ドライブとメディアを最適な状態で使用できます。

Windows および UNIX システムでは、ドライブ・グループ別にメディア・プールを構成できるので、ドライブが複数種類あれば、密度も複数の設定ができます。たとえば、DLT4000 プールと DLT8000 プールを作成できます。

メディアのフォーマット時に、デバイス定義内で関連する設定を使用する必要があります。たとえば、高密度 DLT 8000 用のプール内のメディアは、DLT 8000 を使って、高密度の設定でフォーマットすることが必要です。

このような個別設定のプールでは、フリー・プールの概念を使用できません。フリー・プールは、デバイスに設定されている別のプールに属するメディアを正しく識別できないため、このようなメディアは「外部」メディアとみなされます。フリー・プールの概念を適用できるとしても、単一のプール (たとえば DLT8000 プール) だけでしか使用できず、しかもこの場合、同種類 (DLT) のメディアへの書き込みが互換性のない方法で行われます。

あるプールに属するメディアは、関連するデバイスでしか使用できないため、復元時には注意が必要です。

新しいメディア・プールを構成する場合は、オンライン・ヘルプの索引キーワード「メディア・プールの構成」を参照してください。

ドライブに対するメディア・プールの設定を変更するには、ドライブのプロパティを変更します。詳しい手順については、オンライン・ヘルプの索引キーワード「変更 - メディア・プール」を参照してください。

SAN 環境内の共有デバイス

本項では、Storage Area Networks (SAN) の基本概念を説明します。概念の詳細は、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

ここでは、以下の概念と構成手順について説明します。

- Data Protector によってライブラリが排他的に使用される場合のデバイスのロック機構
- Data Protector ユーザー・インタフェースを使ったライブラリ・ロボティクスとドライブの構成方法
- ライブラリ・ロボティクスとドライブのロック
- ライブラリへの直接アクセスと間接アクセス

SAN とは

Storage Area Network (SAN) は、データ記憶専用のネットワークであり、高速のファイバー・チャネル技術に基づいています。専用のネットワークによってデータ記憶処理が行われるため、アプリケーション・サーバの負荷が軽減されます。Data Protector でも、この技術がサポートされており、SAN 経由で接続された記憶デバイスを複数のホストの間で共有できるようになっています。これによって複数のシステムを複数のデバイスに接続することができます。これは、同じ物理デバイスを複数回定義することで可能になります。たとえば、デバイスへのアクセスが必要なすべてのシステムごとに 1 回定義します。

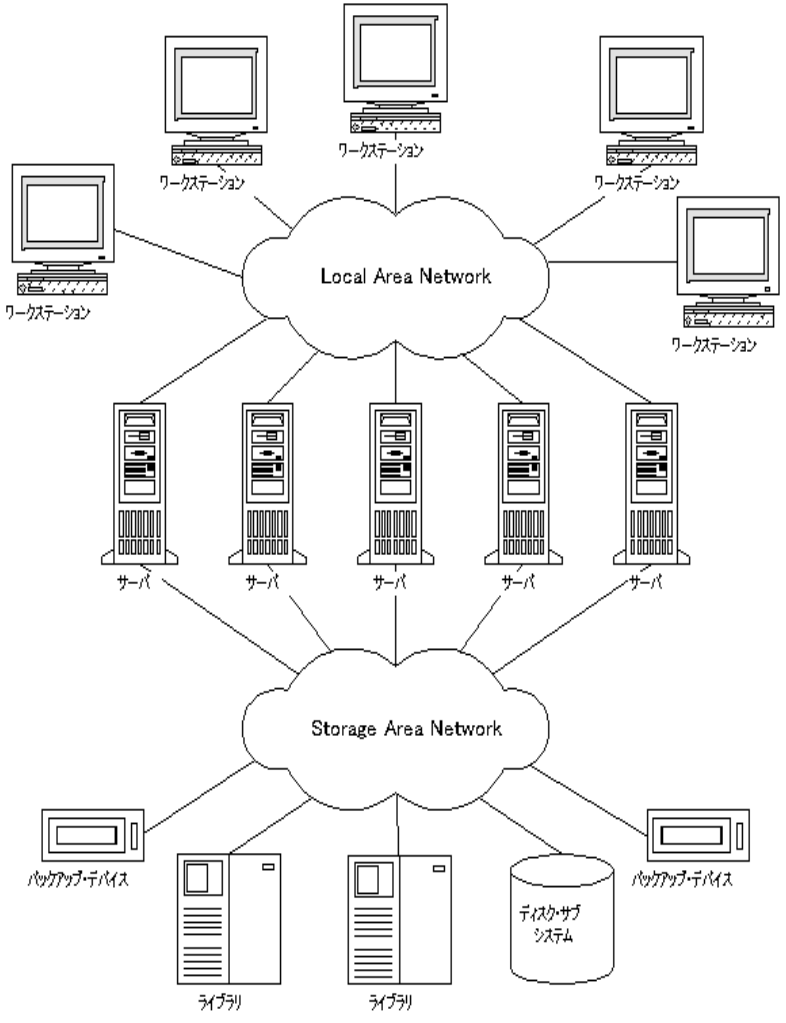
主要な概念

SAN 環境内で Data Protector を使用する際に考慮が必要な主要概念を以下に示します。

- 各システムはそれぞれ (疑似) ローカル・デバイスを持つことができます。ただし、これらのデバイスは通常、複数のシステム間で共有されます。これは、個々のドライブと、ライブラリ内のロボティクスのどちらにも該当します。
- 複数のシステムが同じデバイスに同時にデータを書き込まないように注意する必要があります。デバイスへのアクセスは、すべてのシステム間で同期をとる必要があります。このためには、ロック機構を使用します。

- AN は、複数のシステムによるライブラリ・ロボティクスの管理に優れています。ロボティクスに送られる様々な要求が、関連するすべてのシステム間で同期されていれば、ロボティクスを直接管理することが可能です。

図 2-7　　SAN 内での複数システムと複数デバイスの接続



LIP を伴う FC-AL SAN の使用

FC-AL(Fibre Channel Arbitrated Loop) 内のテープ・デバイスを使用すると、バックアップ・セッションを中止するような異常が発生することがあります。これは、新しい FC リンクの接続 / 切断時、および FC-AL に接続されているシステムの再起動時には、FC-AL によって必ず LIP(Loop Initialization Protocol) が実行されるからです。この FC-AL の再初期化により、実行中のバックアップが中止されます。このように中止されたジョブは、再開させる必要があります。

FC-AL ループ上で LIP が実行される時は、アクティブな I/O プロセスを伴うユーティリティで I/O エラーが発生します。バックアップ・ユーティリティが共有テープを使おうとすると、I/O エラーが発生し、現在のバックアップ・セッションは失敗します。動作中のテープが巻き戻され、アンロードされて、バックアップ・セッションが中止されます。

この問題を回避するには、次の注意事項を守ってください。

- バックアップ・セッションの実行中に、FC-AL へのデバイスの追加または削除をしてはいけません。
- バックアップ・セッションの実行中に、FC コンポーネントに触れてはいけません。静電荷により LIP が起きる可能性があります。
- `discovery` (Windows の場合)、または `ioscan` (HP-UX システムの場合) を使用してはいけません。これらを実行すると LIP が発生します。

Data Protector が専用で使用するデバイスのロック

Data Protector だけが任意のドライブを使用していて、他のアプリケーションは使用していない場合でも、そのドライブを複数のシステムで共用する必要性があれば、デバイス・ロック機構を使用することが必要です。

また、Data Protector だけが複数システムから任意のロボティクス制御を使っていて、他のアプリケーションは使用していない場合でも、Data Protector はロボティクス制御を内部処理します (ただし、そのロボティクスを制御する必要性のあるすべてのシステムと同じセル内にある場合)。このような場合、デバイスに対するアクセスの同期化はすべて Data Protector の内部制御機能によって管理されます。

複数のアプリケーションが使用するデバイスのロック

Data Protector と少なくとも 1 つの Data Protector 以外のアプリケーションが同じデバイスを複数のシステムから使用する場合、すべてのアプリケーションで同じ (一般的な) デバイス・ロック機構を使う必要があります。この機構は、複数のアプリケーション間で機能しなければなりません。このモードは、現在 Data Protector ではサポートされていません。このような必要が生じた場合、すべてのデバイスに対し、一時点においては 1 つのアプリケーションからの排他的アクセスしか受け付けないように、運用ルールで保証する必要があります。

ライブラリへの直接アクセスの概念

直接ライブラリ・アクセスの場合、どのシステムからでも直接ライブラリ・ロボティクスに制御コマンドが送信されます。そのため、どのシステムも他のシステムに依存することなく機能することができます。

ライブラリへ直接アクセスを行い、複数のシステムが同じライブラリにコマンドを送信する場合、コマンドが送信される順序について調整されるようにする必要があります。したがって、Data Protector では、どのライブラリの定義も、ライブラリ・ロボティクスを制御しているホストとデフォルトで関連付けられています。他のホストからメディアを移動するよう要求があった場合、Data Protector は、まずライブラリ定義で指定されたシステムにアクセスし、メディアの移動を行います。そのシステムが利用できない場合は、`libtab` ファイルが設定されていれば、ローカル・ホストから直接ライブラリ・ロボティクスにアクセスします。この動作はすべて、Data Protector 内部で透過的に行われます。

ライブラリへの間接アクセスの概念

間接ライブラリ・アクセスの場合、Data Protector によって開始されたロボティクス制御コマンドを送信するシステムは、1 つだけです (デフォルトのロボティクス制御システム)。ロボティクス機能を要求するその他のシステムは要求をロボティクス制御システムに転送し、そこから実際にコマンドがロボティクスに送信されます。これはデフォルトの設定で、Data Protector からの要求すべてに対し、Data Protector の内部で透過的に行われます。

構成の概要

本項では、システムの構成に必要な手順の概要を説明します。取り上げる項目は以下のとおりです。

- 構成の目的

  本項では、構成対象となる混在 SAN 環境を指定します。

- 構成方法

  本項では、UNIX、Windows、混在 SAN 環境に対して実行が必要な構成方法の概要を説明します。

- デバイスの自動構成

  本項では、SAN 環境に固有のデバイス自動構成について、概要を説明します。

- ロボティクスの手動構成

  本項では、ライブラリ・ロボティクスを SAN 環境で使用するよう手動で構成する方法を説明します。

- デバイスの手動構成

  本項では、ドライブの構成に必要な手順を説明します。また、どのような場合にロック名と直接アクセスを使用する必要があるかについても説明します。

- 手動による `libtab` ファイルの構成

  本項では、`libtab` ファイルの目的と使用方法を説明します。`libtab` ファイルの例も示します。

- `sanconf` コマンドによる構成の簡略化

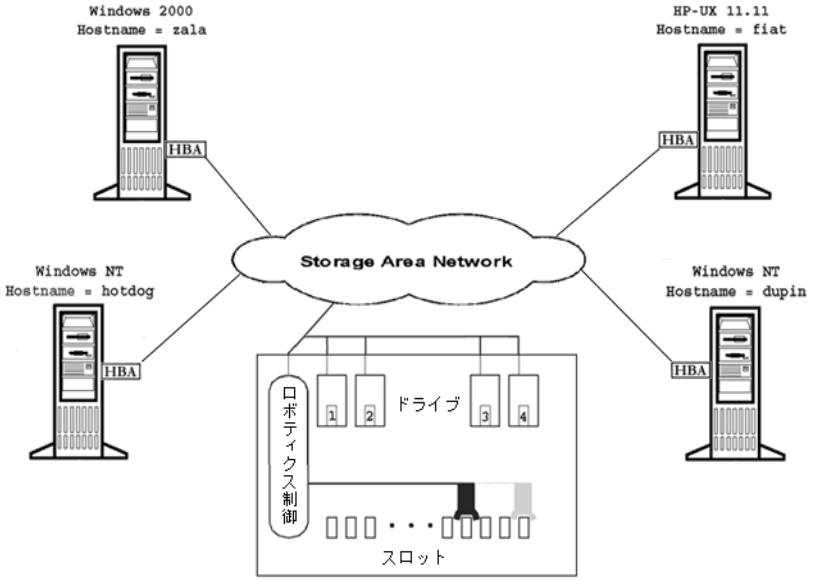
  本項では、SAN 環境におけるライブラリの構成作業を簡略化する `sanconf` コマンドについて説明します。

構成の目的

SAN 環境には、1 つのライブラリを使用する 1 つのホストから、複数のライブラリを使用する複数のホストまで、様々な環境があります。また、その複数のホストが、複数のオペレーティング・システム・プラットフォーム上で実行されている場合もあります。以下の例では、SAN 環境は以下のシステムで構成されています。

- Windows XP システム 2 台 (Windows XP システム dupin は、ライブラリ・ロボティクスを制御するデフォルトのホストとして使用されています)
- Windows 2000 システム 1 台
- HP-UX 11.11 システム 1 台
- ブリッジ 1 台
- スイッチ 1 台
- HP LTO Ultrium ドライブ 4 台と 40 スロットを備えたライブラリ 1 つ

図 2-8　　SAN 環境の構成



ライブラリは、ドライブに直接アクセス可能な複数のシステムに接続されているため、ホストから使用したい数のドライブを各ホスト上で構成する必要があります。この場合は、4 台の物理ドライブすべてが各ホストから使用されることになります。

Data Protector から見た場合の目標は以下のとおりです。

- ライブラリ・ロボティクスを共有する予定の各ホスト上で、各ホスト用のライブラリ・ロボティクス定義を作成します。ロボティクスを制御するホストが 1 台だけの場合は、デフォルトのロボティクス制御ホストに対するライブラリ定義のみを作成します。
- ライブラリ内の同じ (テープ) ドライブを共有する予定の各ホスト上で、以下を行います。
  - 使用するデバイスごとにデバイスの定義を作成します。
  - 別のホストでも (物理) デバイスを使用する場合は (共有デバイス)、ロック名を使用します。
  - 必要に応じて、直接アクセスの機能を使用したい場合は直接アクセスを選択します。使用する場合には、`libtab` ファイルがそのホスト上で設定されていることを確認してください。

構成方法

SAN 構成で使用するプラットフォームによって、3 つの種類構成方法があります。

- Data Protector の自動構成機能を使用することで、GUI を使用して SAN 環境内のデバイスを構成できます。デバイスの自動構成機能は、Windows、HP-UX、Solaris、Linux、Novell NetWare、Tru64、AIX オペレーティング・システム上で使用可能です。 詳細は、「デバイスの自動構成」(60 ページ) を参照してください。
- `sanconf` コマンドを使用することで、コマンド行を使用して SAN 環境内のデバイスを自動構成できます。詳細は、「sanconf コマンドを使用した構成」(61 ページ) を参照してください。
- お使いの環境に、デバイスの自動構成をサポートしていないシステムがある場合は、手動構成を行います。詳細は、「ライブラリの手動構成」(62 ページ) を参照してください。

デバイスの自動構成

Data Protector の自動構成機能により、SAN 環境内の複数ホストのデバイスやライブラリを自動構成できます。

制限事項

自動構成機能は、SAN 環境内の以下のデバイスの構成には使用できません。

- 混合メディア用ライブラリ

- DAS または ACSLS ライブラリ
- NDMP デバイス

Data Protector は、お使いの環境に接続されているバックアップ・デバイスを検出します。また Data Protector はスロット数、メディアの種類、ライブラリに含まれるドライブを識別します。次に、Data Protector は論理名、ロック名、メディアの種類、デバイス・ファイルまたはデバイスの SCSI アドレス、ドライブとスロットの構成を行います。

自動構成手順では、どのホスト上にどのライブラリやデバイスを構成するかを選択できます。複数のホストが 1 台のライブラリのテープ・ドライブを使用している場合、このライブラリは各ホストに表示され、複数のホストがテープ・デバイスを共有でき、1 台のホスト (制御ホスト) がロボティクスを制御します。

注記

新しいホストを SAN 環境に導入したときに、すでに構成済みのライブラリとデバイスは自動更新されません。

既存のライブラリを新しいホスト上で使用するには、このライブラリをいったん削除して、同じ名前の新しいライブラリを新しいホスト上で自動構成してください。

既存のライブラリにデバイスを追加するには、ライブラリをいったん削除して、新しいホスト上に同じ名前のライブラリと新しいドライブを自動構成するか、ライブラリにドライブを手動で追加します。手動構成の手順については、オンライン・ヘルプの索引キーワード「構成 - SAN 環境内のデバイス」を参照してください。

Removable Storage サービスの実行中にライブラリを自動構成すると、ドライブとロボティクス (エクスチェンジャ) が適切に組み合わされません。

自動構成の詳しい手順については、オンライン・ヘルプの索引キーワード「バックアップ・デバイスの自動構成」を参照してください。

sanconf コマンドを使用した構成

sanconf コマンドを使用して、SAN 環境内のデバイスを自動構成できます。

sanconf コマンドによって以下の動作が実行されます。

- デフォルトのロボティクス制御ホストを構成します。

- ホストのリストを提供するだけで、すべてのホスト上のデバイス (テープ・ドライブ) を構成できます。これにはロック名の構成も含まれます。

sanconf コマンドの使用方法の詳細は、「sanconf コマンドを使用した SAN 環境におけるライブラリの自動構成」(72 ページ) と、sanconf の man ページを参照してください。

ライブラリの手動構成

まず、任意のホスト上でライブラリ・ロボティクス制御を構成する必要がありますが、このホストがデフォルトのロボティクス制御システムの役割を果たします。また、このホストはメディアの移動を管理するために使用されます。他のホストから出されるメディアの移動要求に依存しません。

これは、複数のホストがメディアの移動を同時に要求した場合に発生するロボティクス内での競合を防ぐことを目的としています。このホストで障害が発生し、直接アクセスが有効な場合に限り、ロボティクスは、メディアの移動を要求したローカル・ホストによって制御されます。

必要条件

SAN 環境で Data Protector デバイスを構成する前に、共有ライブラリとデータをやりとりする必要のある各ホスト上に Media Agent をインストールしておくことが必要です。Media Agent のインストール方法の詳細は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

ライブラリ・ロボティクスの構成

ライブラリ自体の作成方法については、「ライブラリ・デバイスの構成」(26 ページ) またはオンライン・ヘルプの索引キーワード「構成 - SAN 環境内のデバイス」を参照してください。

ロボティクス制御については、SAN 内の任意のホストを使用できます。ここでは例として、システム dupin.company.com を使用することにします。ライブラリ・ロボティクスは、このホストが使用不可能で直接アクセスが有効な場合を除き、このホストによって制御されます。詳細は、「直接アクセスを 可能にする」(65 ページ) を参照してください。

クラスター内でのライブラリ・ロボティクスの構成

ロボティクス制御をクラスターが管理するようにしたい場合は、以下のことを確認することが必要です。

- ロボティクス制御が各クラスター・ノード上に存在すること
- ライブラリ・ロボティクス構成で仮想クラスター名が使用されていること

- mksf コマンドまたは libtab ファイルを使用して、共通のロボティクスおよびデバイスファイル名がインストールされていること。libtab ファイルの構成方法については、「libtab ファイルの手動構成」(66 ページ) を参照してください。

ライブラリ・ロボティクスの構成後、ドライブを作成します。

デバイス (ドライブ) の手動構成

デバイスを使用する各ホスト上で、デバイス (テープ・ドライブ) を構成する必要があります。

複数のホストが同じデバイスを同時に使用することを避けるには、ロック名を使用します。必要に応じて、「直接アクセス」モードを選択できます。

ドライブの構成

以下のドライブ命名規則に従うと便利です。理由は以降で明らかになります。

```
LibraryLogicalName_DriveIndex_Hostname
```

(例 : SAN_LIB_2_computer_1)

ドライブの命名規則には、バックアップ仕様作成時の利点が示されています。あるホスト上でバックアップを構成する際は、そのホスト上に構成されているドライブを使用することが唯一の必要条件です。これは、そのドライブ名にホスト名が含まれているためです。

表 2-1 ドライブに対するデバイスのロック

環境条件	必要なアクション
ドライブを使用するのは 1 台のシステムと Data Protector のみである	ロックは不要なため、フィールドは空白にしておきます (例 : [ロック名] = 空白)。
ドライブを使用するシステムが複数あるが (SAN)、このドライブにアクセスするアプリケーションは Data Protector だけである	デバイスのロックを使用します (ロック名を定義します)。詳細は、「デバイスのロック」(99 ページ) を参照してください。

表 2-1 ドライブに対するデバイスのロック

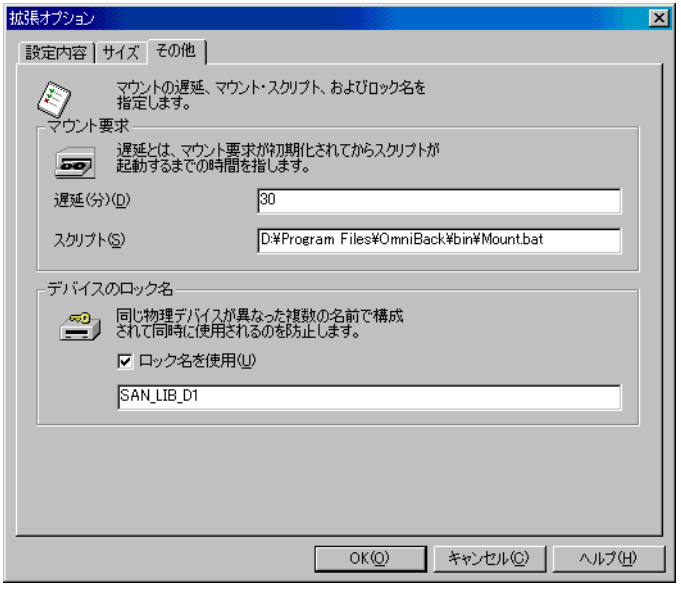
環境条件	必要なアクション
複数のシステムとアプリケーションがドライブを使用する (Data Protector だけではない)	デバイスのロックを使用します (ロック名を定義します)。また運用ルールで、すべてのデバイスに対し、一時点においては 1 つのアプリケーションからの排他的なアクセスしか行われないようにする必要があります。

ロック名の定義

SAN 環境ではロック名を使用することが必要です。これは、複数のシステムがデバイスへ同時にアクセスすることによる衝突を防ぐためです。ロック名には以下の命名規則を使用することをお勧めします。

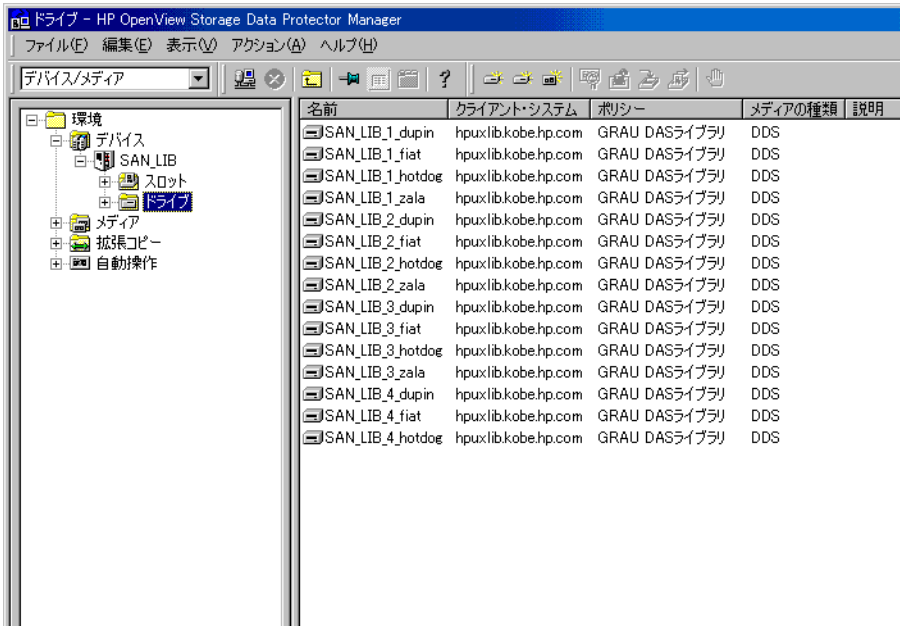
`LibraryLogicalName_DdriveIndex` (例 : `SAN_LIB_D1.`)

図 2-9 拡張オプションを設定する



ドライブにロック名を設定した場合、その物理ドライブに対しては別ホストのデバイス定義でも同じロック名を使用する必要があります。

図 2-10　ロック名を使ったデバイス定義のまとめ



直接アクセスを可能にする

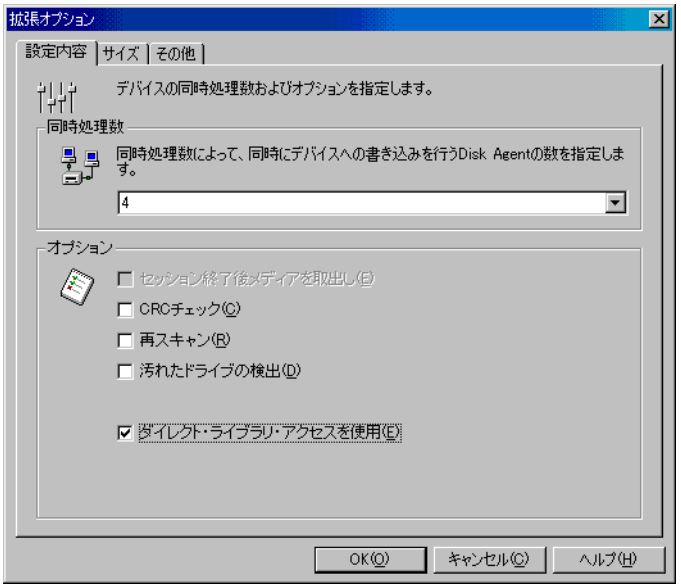
直接アクセス機構では必ず、メディアの移動にはデフォルトのロボティクス制御ホストを最初に使用しますが、このホストで障害が発生した場合、Data Protector は直接アクセスを使用します (使用可能に設定されている場合)。

直接アクセスを可能にするには、[ダイレクト・ライブラリ・アクセスを使用] オプションを選択して (図 2-11 (66 ページ) を参照)、直接アクセスを使用するすべてのホスト上で `libtab` ファイルを構成します。

注記

マルチパス・デバイスに対する直接アクセスを可能にした場合は、構成されているパスの順序にかかわらず、ローカル・パス (あて先クライアント上のパス) が最初に使用されます。

図 2-11 直接アクセスを選択する



libtab ファイルの手動構成

libtab ファイルの目的は、ライブラリ・ロボティクス制御アクセスをマッピングして、「直接アクセスを要求するシステム」上でも機能するようにすることです。これは、このようなシステム上では、ローカル制御パスがデフォルトのライブラリ・ロボティクス制御システム上で使用されるものと異なる可能性があるためです。

注記

マルチパス・デバイスを構成している場合、libtab ファイルの機能は使用できません。

libtab ファイルは、次のようなクライアント・ホストごとにひとつずつ作成する必要があります。すなわち、ライブラリ・ロボティクスへの「直接アクセス」を必要としていて、しかもデフォルトのライブラリ・ロボティクス制御システムとして構成されたシステムとは異なる Windows システムおよび UNIX システムのクライアント・ホストが対象です。

直接アクセスを要求する各システム上に、テキスト・ファイルを以下の書式で作成します。

<FullyQualifiedHostname> <DeviceFile | SCSIPath> <DeviceName>

- *<FullyQualifiedHostname>* とは、ライブラリ・ロボティクス用の直接アクセス制御を要求しているクライアント・ホストの名前です。このホストがクラスターの一部である場合、ノード名を使用します。
- *<DeviceFile | SCSIPath>* とは、このクライアント・ホスト上のライブラリ・ロボティクス・ドライバへの制御パスです。
- *<DeviceName>* とは、このクライアント・ホスト上で使用されるデバイス定義の名前です。

デバイスに直接アクセスを要求する場合は、デバイスごとに 1 行使用する必要があります。

libtab ファイルは以下のディレクトリにあります。

- *<Data_Protector_home>*¥libtab (Windows システムの場合)
- /opt/omni/.libtab (HP-UX および Solaris システムの場合)
- /usr/omni/.libtab (上記以外の UNIX システムの場合)

サンプル・ファイルは、関連するすべてのシステムに当てはまります。定義は行で区切り、空白行は無視されます。デフォルトのライブラリ・ロボティクスはホスト dupin.company.com で定義されているため、このシステムには libtab ファイルは必要ありません。

ヒント

関連するすべてのシステムの定義を含む libtab ファイルが 1 つだけであり、このファイルが、関連するすべてのシステムに配布される可能性もあります。この場合、特定のシステムがライブラリ・ロボティクスへの「直接アクセス」を必要とした場合、他のシステムの定義は無視され、該当するシステムの定義だけが使用されます。

zala 上の libtab ファイルの例

ホスト zala.company.com (Windows) 上の libtab ファイルの例

```
zala.company.com  scsi:2:0:2:0  SAN_LIB_1_zala
zala.company.com  scsi:2:0:2:0  SAN_LIB_2_zala
```

```
zala.company.com  scsi:2:0:2:0  SAN_LIB_3_zala
zala.company.com  scsi:2:0:2:0  SAN_LIB_4_zala
```

oda 上の libtab ファイルの例

ホスト oda.company.com (HP-UX) 上の libtab ファイルの例

```
oda.company.com  /dev/spt/lib  SAN_LIB_1_computer_2
oda.company.com  /dev/spt/lib  SAN_LIB_2_computer_2
oda.company.com  /dev/spt/lib  SAN_LIB_3_computer_2
oda.company.com  /dev/spt/lib  SAN_LIB_4_computer_2
```

donat 上の libtab ファイルの例

ホスト donat.company.com (Solaris) 上の libtab ファイルの例

```
donat.company.com /dev/rsst6 SAN_LIB_1_sample
donat.company.com /dev/rsst6 SAN_LIB_2_sample
donat.company.com /dev/rsst6 SAN_LIB_3_sample
donat.company.com /dev/rsst6 SAN_LIB_4_sample
```

注記

ホストがクラスターの一部である場合、<FullyQualifiedHostname> には仮想ホスト名を指定し、<DeviceFile | SCSIPath> はローカル・ノードを参照することが必要です。

共有デバイスと MC/ServiceGuard

Data Protector を MC/ServiceGuard と併用してクラスター化を行っている場合、SAN 環境内でも両者を併用することは可能です。クラスター化は、ネットワークの名前、ディスク、テープなどのリソースをノード間で共有することにより実現されるので、ファイバー・チャネルと SAN は、ストレージ・デバイスの共有に適しています。

本項では、必要なデバイスファイルの作成方法、仮想ホストの構成方法、拘束および非拘束ドライブの構成方法、SAN 環境内で統合ソフトウェアを使用するための Data Protector GUI を使った構成方法について説明します。

構成の基本概念

クラスター内のノードは、SAN に接続されたデバイスを共有することにより、クラスター内で実行されているアプリケーションを LAN に依存しないでバックアップできます。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ので、クラスター内のどのノード上でも随時実行できます。このようなアプリケーションに対して、LAN に依存しないローカル・バックアップを実行するには、実際のノード名ではなく仮想ホスト名を指定した論理デバイスを構成する必要があります。

1 つの物理デバイスについて、必要な数だけ論理デバイスを構成できますが、このときすべてのデバイスに対して同じロック名を使用しなければなりません。

複数のシステム間でデバイスを共有するには、そのデバイスをローカルで使用する各システムに対して、1 つの論理デバイスを構成します。

詳しくは、以下のドキュメントを参照してください。

- B3935-90015『MC/ServiceGuard バージョン A.11.05 リリースノート』
- B3936-90026 『MC/ServiceGuard の管理』第 6 版

ドライブの構成

非拘束ドライブ

パッケージがどちらのホスト上で実行されているかに応じて、どちらのホストからもアクセス可能にする必要があるドライブは、仮想ホストに基づいて構成してください。

表 2-2 非拘束ドライブの構成方法

ホスト名	node_Appl
デバイスの制御パス	/dev/rmt/st3m
ロック名	Libl_Drive_1

拘束ドライブ

ドライブは、拘束ホスト名とローカル・デバイスファイルを使った標準的な方法で使用することもできます (ローカルな HP-UX デバイスファイルを使用可能)。ローカル・ドライブはノード上で構成することが必要です。例 :

表 2-3 拘束ドライブの構成方法

ホスト名	Host_A

表 2-3 **拘束ドライブの構成方法**

デバイスの制御パス	/dev/rmt/0m
ロック名	Lib1_Drive_1

非拘束ドライブと拘束ドライブに関する上記 2 つの例では、デバイスが /dev/rmt/0m と /dev/rmt/st3m で識別されることを示しています。どちらのデバイスファイルも同じ物理デバイスを参照するので、ロック名 (Lib1_Drive_1) は同じです。

変更された SCSI アドレスの自動検出

SAN 環境では、SCSI アドレス (UNIX ではデバイス・ファイル) が動的に変更されるために、バックアップ・セッションが失敗することがあります。Data Protector では、SAN デバイスのシリアル番号を内部保存しておいて、デバイスが使用されるたびにシリアル番号をチェックすることができます。デバイスのアドレスが IDB に保存されたアドレスと一致しない場合、デバイスパスの検出プロセスが開始されます。新しいパスが見つかったら、IDB が更新されます。

制限事項

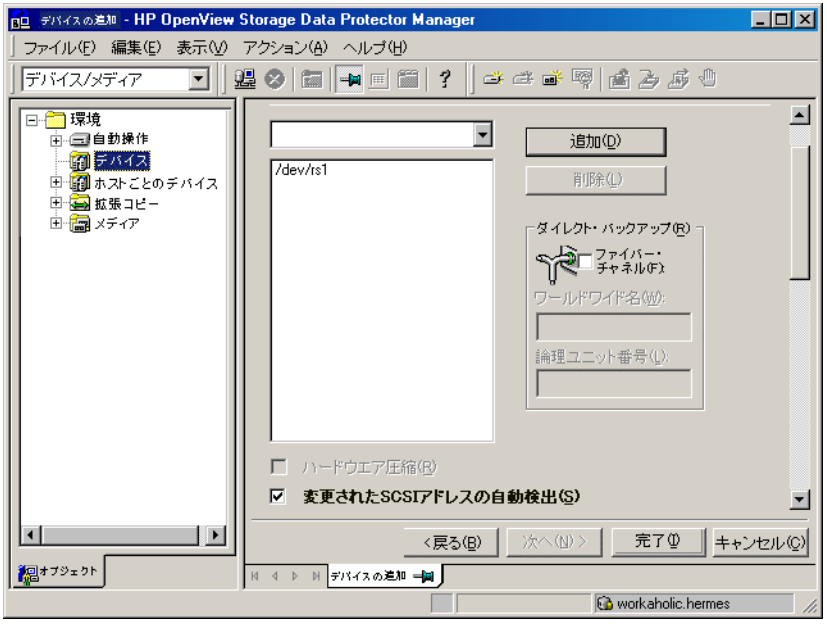
- 変更された SCSI アドレスの自動検出は、スタンドアロン・デバイスのチェーンとして構成されたデバイスには使用できません。
- デバイスがシリアル番号を持っていない場合は、変更された SCSI アドレスの自動検出機能は使用しないでください。

変更された SCSI アドレスの自動検出を使用可能にするには、[デバイスの追加] ウィザードの 2 番目の手順か、デバイスの [コントロール] プロパティのページで、[変更された SCSI アドレスの自動検出] を選択します。詳細は、図 2-12 を参照してください。

注記

デバイスを再構成するには、デバイスのシリアル番号を削除します。シリアル番号を削除しなかった場合、Data Protector は古いシリアル番号を検索します。

図 2-12 変更された SCSI デバイスの自動検出



sanconf コマンドを使用した SAN 環境におけるライブラリの自動構成

sanconf コマンドは、SAN 環境でのライブラリの構成を容易にするユーティリティです。このコマンドは、複数のクライアントからドライブに関する情報を収集して、それらを 1 つのライブラリに構成することによって、SAN 環境内のライブラリを自動構成します。

sanconf コマンドは、Data Protector Cell Manager または Data Protector クライアント上で実行できます。このコマンドは、Windows の場合は *<Data_Protector_home>*¥bin ディレクトリ、HP-UX および Solaris クライアントの場合は /opt/omni/lbin ディレクトリに存在します。

sanconf コマンドを使用すると以下の作業を実行できます。

- 指定された Data Protector クライアントをスキャンして、SAN 環境内のクライアントに接続されたドライブとロボティクス・コントローラの SCSI アドレスに関する情報を収集します。詳細は、「クライアント上でのデバイス情報の収集」(74 ページ) を参照してください。
- Data Protector クライアントのスキャンによって収集した情報を使用して、指定されたクライアントの既存のライブラリ設定やドライブ設定を作成または変更します。詳細は、「ライブラリ・デバイスの構成」(75 ページ) を参照してください。
- 指定されたクライアントのドライブをライブラリから削除します。詳細は、「構成の削除」(82 ページ) を参照してください。

sanconf セッションはすべて、*<Data_Protector_home>*¥log¥sanconf.log(Windows の場合) または /var/opt/omni/log/sanconf.log(HP-UX および Solaris システムの場合) に記録されます。このログ・ファイルはトラブルシューティングに使用されます。

制限事項と推奨事項

本項では、sanconf コマンドに特有の制限事項と推奨事項について説明します。

制限事項

sanconf コマンドの制限事項は以下のとおりです。

- sanconf は以下のプラットフォーム上で使用できます。
  - Windows
  - HP-UX
  - Solaris
- sanconf は、以下のプラットフォームで実行されているクライアントに接続されたデバイスを検出して構成することができます。
  - Windows
  - HP-UX
  - Solaris
  - Linux
  - Novell NetWare
  - Tru64
  - AIX
- sanconf によってサポートされているライブラリの完全なリストについては、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』または http://www.openview.hp.com/products/datapro/spec_0001.html に表示されている「Support Matrices」を参照してください。
- sanconf がサポートして**いない**機能は以下のとおりです。
  - ドライブスロットへのスペアドライブの配置。
  - ドライブの種類の混合 (たとえば、DLT、9840、LTO ドライブの組み合わせなど)。
  - sanconf の実行されている Data Protector セル以外にあるクライアントの構成。
  - 現在使用不可能なクライアントの構成。使用不可能なクライアントの構成ができるのは、クライアントのスキャンによって収集された情報を格納した構成ファイルを使用してライブラリの構成が実行されている場合のみです。

推奨事項

対象とする各デバイスについて、1 つのシステム上にドライバを 1 つだけ構成することをお勧めします。

クライアント上でのデバイス情報の収集

sanconf -list[_devices] コマンドを実行することによって、SAN 環境内のクライアントに接続されたドライブとロボティクス・コントローラの SCSI アドレスに関する情報を取得できます。sanconf は指定された Data Protector クライアントをスキャンして情報を収集し、その情報を Cell Manager のメディア管理データベースにアップロードします。構成およびスキャンデータに関する情報は、**構成ファイル**にも保存できます。この構成ファイルは、ライブラリの構成時に使用します。

クライアントのデバイス情報を収集するための構文は、以下のとおりです。

構文

```
sanconf -list[_devices][<ListFileName>]
        [-hosts <host_1> [<host_2>... ] |
        -hostsfile <HostsFileName>]
```

コマンドが実行されると、クライアントのスキャン状況を示すメッセージが画面に表示されます。スキャンが完了すると、サマリーが表示されます。

<ListFileName> が指定されると、構成情報とスキャン情報が構成ファイル内に格納されます。構成ファイルは、-configure オプションによって使用できます。このオプションの詳細については、「ライブラリ・デバイスの構成」(75 ページ) を参照してください。

sanconf コマンドにはスキャン対象のクライアントのリストが必要です。このリストは、-hosts または -hostsfile オプションを使用することで指定できます。上記のどちらのオプションも指定されなかった場合、現在のセル内のすべてのクライアントがスキャンされます。

-hosts オプションが指定された場合は、リストされたすべてのクライアントがスキャンされます。-hostsfile オプションが指定された場合は、<HostsFileName> ファイル内にリストされたすべてのクライアントがスキャンされます。<HostsFileName> は、スキャン対象のクライアントのリストを格納する ASCII ファイルでなくてはなりません。各クライアントはすべて別々の行で指定する必要があります。構成ファイルにスキャン情報を保存する前に、クライアントリスト内ですべてのクライアントを指定するようにお勧めします。

注記

構成するすべてのクライアント (ロボティクスを表示できるものとドライブを表示できるもの) をスキャンする必要があります。

例

以下の例では、「host01」、「host02」、「host03」という 3 つのホスト上でデバイスをスキャンしています。

```
sanconf -list_devices -hosts host01 host02 host03

=================== SUMMARY REPORT ===================
LIBRARY="HP:C7200-8000" serial="ABC0000123"
        on hosts: host01 host02 host03
        DRIVE: index=1; name="QUANTUM:DLT8000";
serial="A0B1C3D4E5"
        DRIVE: index=2; name="QUANTUM:DLT8000";
serial="F6G7H8I9J0"
======================================================
```

ライブラリ・デバイスの構成

ライブラリ・デバイスは sanconf -configure コマンドを使用して構成します。

テープ・ライブラリを構成するための構文は以下のとおりです。

構文

```
sanconf -configure [<ListFileName>]
       -library <LibrarySerialNumber> <LibraryName>
        [<RoboticControlHostName>]
        [<DeviceTypeNumber> | ".<DeviceTypeExtension>"]
        [-hosts <host_1> [<host_2> ] | -hostsfile
    <HostsFileName>]
        [-drive_template <DriveTemplateFileName>]
        [-library_template <LibraryTemplateFileName>]
        [-[no_]multipath]]
```

<ListFileName> パラメータが指定されていない場合は、sanconf コマンドによって現在のセル内にあるすべてのクライアントがスキャンされます。このパラメータが指定されると、sanconf はクライアントのすべての情報

が構成ファイル内にすでに存在しているものと想定するため、スキャンは実行されません。クライアントがスキャンされない場合、このホストに接続されているドライブの存在しない状態でライブラリが構成されます。

デフォルトの状態、または no_multipath オプションを指定した状態で sanconf コマンドを実行した場合は、パスごとに個別の論理デバイスが構成されます。-multipath オプションを指定して sanconf コマンドを実行した場合は、同一物理デバイスに対するすべてのパスが 1 つのマルチパス・デバイスとして構成されます。

ライブラリ・デバイスの初期構成

ライブラリ・デバイスを最初に構成するときには、-configure オプションを使用して sanconf コマンドを実行する必要があります。sanconf によって、指定されたすべてのクライアント上で devbra が起動します。devbra は、デバイスに対して物理ライブラリとドライブの構成情報を照会します。まず -list[_devices] <ListFileName> オプションを使用してクライアントの情報を保存して、次に、-configure <ListFileName> を使用してライブラリとドライブを構成することをお勧めします。

<ListFileName> パラメータが使用されると、sanconf コマンドは構成ファイルを読み込むだけになります。この場合、クライアントのスキャンは実行されません。

-library パラメータが使用されると、sanconf コマンドはシステム内に 1 つの論理ライブラリを作成し、指定されたすべてのクライアント上にすべてのデバイスを作成します。-list_devices オプションを使用すると、ライブラリのシリアル番号が取得できます。

例

以下の例では、sanconf コマンドが指定されたクライアントをスキャンし、「SAN_STORE」という名前の論理ライブラリを作成しています。このライブラリでは、ロボティクスが「host33」というクライアント上で構成され、この論理ライブラリ用のドライブが「host01」、「host02」、「host03」という 3 つのクライアント上で構成されます。

```
sanconf -configure -library MPC0100013 SAN_STORE host33
       -hosts host01 host02 host03
```

例

以下の例では、sanconf コマンドがまず、指定されたクライアント「host01」、「host02」、「host03」、「host33」の構成情報について SAN 環境をスキャンしています。次に、この情報を mySAN.cfg ファイルに保存しています。

```
sanconf -list_devices mySAN.cfg
        -hosts host01 host02 host03 host33

sanconf -configure mySAN.cfg -library MPC0100013 SAN_STORE
        host33 -hosts host01 host02 host03
```

2 つ目のコマンドは mySAN.cfg ファイルに保存された情報を使用して、「SAN_STORE」という名前の論理ライブラリを作成しています。このライブラリでは、ロボティクスが「host33」というクライアント上で構成され、そのライブラリ用のドライブが「host01」、「host02」、「host03」という 3 つのクライアント上で構成されます。

<RoboticControlHostName> パラメータを指定した場合、ライブラリのロボティクスは、そのクライアント上で制御されるように構成されます。*<RoboticControlHostName>* パラメータを指定しなかった場合は、Cell Manager がロボティクス制御ホストとして使用されます。

<DeviceTypeNumber> パラメータまたは ".<DeviceTypeExtension>" パラメータが使用されると、このパラメータで指定された種類のドライブがライブラリ内で構成されます。サポートされているドライブの種類とそのパラメータについては、表 2-4 (77 ページ) を参照してください。これらのパラメータのどちらも指定されない場合は、デフォルトで DLT タイプのドライブが使用されます。ライブラリ内のドライブが指定された種類と異なる場合は、エラーがレポートされます。<DeviceTypeNumber> パラメータは、<RoboticControlHostName> パラメータを指定しなくても実行することができます。

表 2-4　デバイスの種類の番号と対応する拡張子

デバイスの種類の番号	デバイスの種類に対応する拡張子
1	.DDS
2	.QIC
3	.EXA
4	.AIT

表 2-4 デバイスの種類の番号と対応する拡張子

デバイスの種類の番号	デバイスの種類に対応する拡張子
5	.3480
6	.RDSK
7	.REGFILE
8	.9840
9	.TAPE
10	.DLT
11	.D3
12	.3590
13	.LTO
14	.SDLT
15	.VXA
16	.DTF
17	.9940
18	.SAIT
19	.3592

指定されたクライアントだけにドライブを構成するには、-hosts オプションか -hostsfile オプションのどちらかと一緒に -configure オプションを使用します。どちらのオプションも指定されなかった場合、ドライブはセル内のすべてのクライアントで構成されます。-hosts オプションが指定された場合は、リストされたすべてのクライアントでドライブが構成されます。-hostsfile オプションが指定された場合は、<HostsFileName> ファイル内にリストされたすべてのクライアントでドライブが構成されます。<HostsFileName> は、ライブラリのドライブを構成するすべてのクライアントを格納する ASCII ファイルでなくてはなりません。各クライアントはすべて別々の行で指定する必要があります。

マルチパス・デバイスを構成するには、<HostsFileName> ファイルの先頭に次の内容を追加します。

```
<OPTIONS>
-multipath
</OPTIONS>
```

マルチパス・デバイスの場合は、リストまたはファイル内に指定した順番によって、使用されるパスの順番が決まります。たとえば、-hosts Client2 Client1 Client3 と指定すると、Client2 を含んでいるパスが最初に使用されます。

例

sanconf コマンドを使用して、ライブラリの構成時に特定のドライブタイプを指定するには、以下のコマンドを実行します。

```
sanconf -configure -library MPC0100013 SAN_STORE host33
        ".9840" -hosts host01 host02
```

このコマンドでは SA_STORE という名前のライブラリが作成され、クライアント host33 でロボティクスが構成され、クライアント「host01」および「host02」で STK ドライブが構成されます。各ドライブの名前は以下のようになります。

```
SAN_STORE_1_host01

SAN_STORE_1_host02

SAN_STORE_2_host01

SAN_STORE_2_host02

...
```

-drive_template <DriveTemplateFileName> オプションを使用すると、ライブラリ内の構成済みのすべてのドライブのデフォルト構成を変更できます。各パラメータは、ASCII ファイル内に別々の行で指定する必要があります。ドライブのテンプレートは以下のパラメータをサポートしています。

VERIFY	このパラメータは、Data Protector GUI の［CRC チェック］オプションに対応しています。
CLEANME	このパラメータは、Data Protector GUI の［汚れたドライブの検出］オプションに対応しています。
RESCAN	このパラメータは、Data Protector GUI の［再スキャン］オプションに対応しています。

また、-library_template <LibraryTemplateFileName> オプションを使用してライブラリのデフォルト構成を変更することもできます。各パラメータは、ASCII ファイル内に別々の行で指定する必要があります。ライブラリのテンプレートは以下のパラメータをサポートしています。

BARCODEREADER	このパラメータは、Data Protector GUI の [バーコード・リーダーのサポート] オプションに対応しています。
BUSYDRIVETOSLOT	このパラメータは、Data Protector GUI の [ビジー・ドライブの処理]、[メディアの取出し] オプションに対応しています。
BUSYDRIVETOMAILSLOT	このパラメータは、Data Protector GUI で指定される [ビジー・ドライブの処理]、[メール・スロットへのメディアの取出し] オプションに対応しています。

重要

ライブラリのデフォルト構成が変更できるのは、最初の構成のときだけです。ライブラリの構成後に、sanconf コマンドを使用してライブラリの構成を変更することはできません。

例

以下の例では、sanconf コマンドが、セル内のすべてのクライアントをスキャンして、次に、host33 というクライアントでロボティクスの構成された SAN_STORE という名前の論理ライブラリを作成しています。このライブラリとドライブは、DriveTemplate.txt および LibraryTemplate.txt という 2 つのファイル内で指定されたパラメータによっても構成されます。

```
sanconf -configure -library MPC0100013 SAN_STORE host33
       -drive_template DriveTemplate.txt
       -library_template LibraryTemplate.txt
```

ライブラリ・デバイスの再構成

既存のライブラリを再構成するには、-configure オプションを使用します。sanconf コマンドは、すでにドライブが構成済みのクライアントを除いて、最初の構成のときと同じ方法で使用できます。構成失敗時に備えて、まず構成ファイルに構成情報を保存することをお勧めします。また、混乱なく最初の構成を復元できるように、別のファイル名を使用することをお勧めします。sanconf は、ライブラリの再構成時にカスタム設定を再使用します。

マルチパスでないライブラリをマルチパス ライブラリとして再構成すると、そのライブラリはマルチパス ライブラリに変更されて、ライブラリ制御ホストが最初のパスとして使用されるようになります。非マルチパス ドライブは変更も削除もされず、代わりに新しいマルチパス ドライブが作成されます。マルチパス ドライブだけが更新の対象になります。

マルチパス ライブラリを非マルチパス・ライブラリとして再構成すると、そのライブラリは非マルチパス ライブラリに変更されて、1 つのパスだけが作成されます。マルチパス ライブラリに含まれていたマルチパス ドライブは変更されず、代わりに新しいドライブが作成されます。非マルチパス ドライブだけが更新の対象になります。

スイッチによって SCSI アドレスが変更されたときの再構成

たとえばスイッチの再起動後に SCSI アドレスが変更された場合などに、既存の論理ライブラリを再構成したり変更することができます。sanconf コマンドは、最初の構成で使用したのと同じパラメータによって実行できます。以下に例を示します。

例 1

シリアル番号が「MPC0100013」で、デバイスがホスト「host01」、「host02」、「host03」上にあり、ロボティクス制御ホストは「host33」である、「SAN_STORE」という名前のライブラリ・デバイスを SCSI アドレスの変更後に再構成するには、以下のコマンドを実行します。

```
sanconf -configure -library MPC0100013 SAN_STORE host33
       -hosts host01 host02 host03
```

例 2

同様の状況にある同じライブラリ・デバイスを、構成ファイル「mySAN.cfg」を使用して再構成するには、以下のコマンドを実行します。

```
sanconf -list_devices mySAN.cfg
       -hosts host01 host02 host03 host33
```

```
sanconf -configure mySAN.cfg -library MPC0100013 SAN_STORE
       host33 -hosts host01 host02 host03
```

新しいクライアントが追加されたときの再構成

sanconf コマンドは、指定されたクライアントの既存のライブラリにドライブを追加することができます。新しいクライアントはすべて、構成データをまずスキャンしてから、既存のデータベース内に構成することをお勧めします。

例 1

セルに新しいクライアント「host04」および「host05」が追加された場合、-hosts オプションを使用して、シリアル番号が「MPC0100013」である「SAN_STORE」という名前のライブラリ・デバイスを再構成するには、以下のコマンドを実行します。

```
sanconf -configure -library MPC0100013 SAN_STORE host33
       -hosts host04 host05
```

例 2

同じライブラリ・デバイスを、構成ファイル「myNewHostsSAN.cfg」を使用して再構成するには、以下のコマンドを実行します。

```
sanconf -list_devices myNewHostsSAN.cfg -hosts host04 host05
```

```
sanconf -configure myNewHostsSAN.cfg -library MPC0100013
       SAN_STORE host33 -hosts host04 host05
```

例 3 - マルチパス

同じライブラリをマルチパス ライブラリとして再構成するには、以下のコマンドを実行します。

```
sanconf -configure -library MPC0100013 SAN_STORE host33
       -hosts host04 host05 -multipath
```

構成の削除

ライブラリ・デバイスからのドライブの削除

-remove_drives オプションを付加して sanconf コマンドを実行すると、指定したクライアントのライブラリ内に存在する構成済みのドライブを削除できます。マルチパス ドライブとして構成されていたドライブは削除されません。

構成の削除には以下の構文が使用されます。

構文

```
sanconf -remove_drives <LibraryName>
        [-hosts <host_1> [<host_2>... ] |
        -hostsfile <HostsFileName>]
```

注記

この操作のための再スキャンは必要ありません。

例

クライアント「host04」および「host05」上に構成されている「SAN_STORE」という名前のライブラリ内のすべてのドライブを削除するには、以下のコマンドを実行します。

```
sanconf -remove_drives SAN_STORE -hosts host04 host05
```

ライブラリ・デバイスからのパスの削除

ライブラリ・デバイスからパスを削除するには、-remove hosts オプションを付加して sanconf コマンドを実行します。

構成の削除には以下の構文が使用されます。

構文

```
sanconf -remove_hosts <LibraryName>
        [-hosts <host_1> [<host_2>... ] |
        -hostsfile <HostsFileName>]
         [-[no_]multipath]
```

注記

この操作のための再スキャンは必要ありません。

指定したホストを含んでいるすべてのパスが削除されます。ただし、指定したホストがライブラリのすべてのパスに含まれている場合は、ライブラリ・パスの削除は行われず、代わりに警告メッセージが表示されます。

このコマンドは以下の 3 つのモードで実行できます。

- **マルチパス** デバイスのパスのみを削除するには、-multipath オプションを付加します。
- **非マルチパス** デバイスのパスのみを削除するには、-no_multipath オプションを付加します。

- マルチパス・デバイス**および**非マルチパス・デバイスのパスを**両方とも**削除するには、-no_multipath オプションと -multipath オプションのどちらも**指定せずに**コマンドを実行します。

例 - マルチパス

クライアント「host04」および「host05」上に構成された「SAN_STORE」という名前のマルチパス ライブラリからすべてのパスを削除するには、以下のコマンドを実行します。

```
sanconf -remove_hosts SAN_STORE -hosts host04 host05
-multipath
```

例

クライアント「host02」および「host03」上に構成された「SAN_STORE1」という名前の非マルチパス ライブラリからすべてのパスを削除するには、以下のコマンドを実行します。

```
sanconf -remove_hosts SAN_STORE1 -hosts host02 host03
-no_multipath
```

ライブラリ・デバイス全体の削除

構成ユーティリティとしての sanconf コマンドは、IDB からライブラリ全体を削除するオプションを提供していません。このアクションを実行するには、以下のオプションを使用して omniupload コマンドを実行します。

```
omniupload -remove_library <LibraryName>
```

omniupload コマンドの詳細は、omniupload の man ページを参照してください。

sanconf コマンドに関連する omnirc ファイル変数

sanconf コマンドは次の omnirc ファイル変数を使用します。

OB2SANCONFSCSITIMEOUT=s

デフォルト値 : 20 秒

この変数は、sanconf 関連操作のタイムアウト値を設定するもので、Windows システムで使用されます。
sanconf コマンドの実行前に、このコマンドの影響を受けるすべてのクライアントにこの変数を設定する必要があります。

omnirc ファイルの位置と使用方法については、「omnirc オプションの使用」(647 ページ) を参照してください。

ドライブの命名規則

sanconf コマンドによって作成されるドライブはすべて sanconf によって自動的に命名されます。

重要

再構成が正常に動作しなくなるため、ドライブの名前は手動で変更しないでください。

ドライブの命名規則は、デバイスがマルチパス モードで構成されているかどうかによって、以下のいずれかの形になります。

- **非マルチパス**デバイスの場合 :

  `libname_index_host`

  `libname_index_busindex_host`

  busindex 番号は、ドライブに対するパスが複数ある場合にのみ使用します。

- **マルチパス**デバイスの場合 :

  `libname_index`

例

物理ライブラリ内のポジション 2 に存在し、クライアント「host01」にドライブのある「SAN_STORE」という名前のライブラリの場合は、以下のドライブ名を使用します。

```
SAN_STORE_2_host01
```

デュアル HBA 環境の場合、バス番号も追加されます。ライブラリ内でインデックス 2 を持ち SCSI アダプタのバス 4 に表示されるクライアント「host01」に別のドライブが配置されている場合は、以下のように命名されます。

```
SAN_STORE_2_4_host01
```

例 - マルチパス

物理ライブラリ内のポジション 2 に存在し、クライアント「host01」にドライブのある「SAN_STORE」という名前のライブラリの場合は、以下のドライブ名を使用します。

```
SAN_STORE_2
```

デュアル HBA 環境の場合、バス番号は追加されません。ライブラリ内でインデックス 2 を持ち SCSI アダプタのバス 4 に表示されるクライアント「host01」に別のドライブが配置されている場合は、新しいパスだけが追加されます。

ドライブロック機構

SAN 環境での構成が正常に完了したら、1 つの物理ドライブを表す複数の論理ドライブが作成された状態になります。Data Protector は、同一の物理ドライブにマッピングされた複数の論理ドライブで同時にバックアップが開始されるのを防ぐロック機構を備えています。この機構で重要な役割を果たすのは**ロック名**です。

ロック名は、1 つの物理ドライブを表すすべての論理ドライブによって使用されます。sanconf コマンドは、構成対象のドライブのロック名を自動的に作成します。ロック名はドライブのベンダー ID 文字列、製品 ID 文字列、製品シリアル番号によって構成されています。

例

ベンダー ID が「HP」、製品 ID が「DLT8000」、シリアル番号が「A1B2C3D4E5」である HP DLT 8000 ドライブには、以下のロック名が自動構成されます。

```
HP:DLT8000:A1B2C3D4E5
```

sanconf コマンドによって作成されたロック名は変更しないでください。手動で作成され、sanconf によって構成された物理ドライブを表している他のすべての論理ドライブも、sanconf によって作成されたロック名を使用する必要があります。

ドライブのクリーニング

汚れたドライブをクリーニングするには、以下の方法があります。

- ライブラリ内蔵クリーニング機構

  テープ・ライブラリの中には、ドライブがヘッド・クリーニングを要求した場合にドライブを自動的にクリーニングする機能を備えたものがあります。ライブラリが汚れたドライブを検出した場合、クリーニング・テープを自動的にロードします。この動作は Data Protector には通知されません。クリーニング動作により、アクティブなセッションが中断されるので、セッションが失敗する原因となります。

  このようなハードウェア側が管理するクリーニング手順は、Data Protector と互換性がないためお勧めできません。この手順の代わりに、Data Protector が管理するドライブの自動クリーニング機能を使用してください。

- Data Protector が管理するドライブの自動クリーニング機能

  Data Protector は、クリーニング・テープを使用するデバイスのほとんどに対して自動クリーニング機能を行うことができます。SCSI ライブラリやマガジン・デバイスの場合は、クリーニング・テープを入れるスロットを定義できます。汚れたドライブからクリーニング要求が送信されると、Data Protector はクリーニング・テープを使ってドライブのクリーニングを行います。

  この方法を使用すれば、汚れたドライブによってセッションが失敗するのを防ぐことができます。ただし、バックアップに適したメディアがドライブに挿入され使用可能であることが条件です。詳細は、「ドライブの自動クリーニングの構成」(89 ページ) を参照してください。

- 手動によるクリーニング

  ドライブの自動クリーニングが構成されていない場合、汚れたドライブを手動でクリーニングする必要があります。Data Protector が汚れたドライブを検出した場合、セッション・モニター・ウィンドウにクリーニング要求が表示されます。その場合は、クリーニング・テープをドライブに手動で挿入する必要があります。

ヘッドのクリーニングには少量の研磨剤付きテープが入った特殊なテープ・クリーニング用カートリッジを使用します。この特殊テープ・カートリッジをロードすると、ドライブはカートリッジを認識して、ヘッド・クリーニングを開始します。

制限事項

- Data Protector では、クリーニング・テープ格納用の特殊なスロットに入っているクリーニング・テープを使ってクリーニングを行うためのベンダー固有の診断用 SCSI コマンドをサポートしていません。この特殊スロットへは、通常の SCSI コマンドを使ってアクセスできないため、Data Protector が管理する自動ドライブ・クリーニング機能と併用できません。クリーニング・テープを格納するための標準スロットを構成してください。
- クリーニング・テープの検出方法や使用方法は、Media Agent が実行されているシステムのプラットフォームによって異なります。詳細は、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。
- Data Protector が管理する自動ドライブ・クリーニング機能を構成する場合は、別の種類のデバイス管理アプリケーションを使用してはいけません。このようなアプリケーションの使用により、予期せぬ結果を招く場合があります。これは、デバイスの種類とメーカにもよりますが、「cleanme」要求が読み込まれると同時に消去されることが原因です。
- 共有クリーニング・テープを使用した、論理ライブラリの自動クリーニングはサポートされていません。各論理ライブラリ用に、専用のクリーニング・テープを構成することが必要です。

自動クリーニングの条件

ライブラリのバーコード・サポートの有無に関わらず、ドライブの自動クリーニングがサポートされています。

自動クリーニングを行うには、以下の条件を満たすことが必要です。

- バーコードをサポートしていないライブラリでは、クリーニング・テープ用スロットが Data Protector のデバイス定義で構成済みであり、スロットにクリーニング・テープ・カートリッジが挿入されていること。クリーニング・テープ用スロットは、他のライブラリ・スロットと共に構成する必要があります。
- バーコードがサポートされているライブラリでは、クリーニング・テープに、"CLN" プレフィックスが付いたバーコード・ラベルが付いていること。また、バーコード・サポートを使用可能にしておくことが必要です。詳細は、「バーコードのサポートを可能にする」(93 ページ) を参照

してください。

- [汚れたドライブの検出] オプションが有効になっていること。

ドライブのクリーニングが必要であるという通知を Data Protector が受け取ると、クリーニング・テープが自動的にロードされ、ドライブのクリーニングが行われた後、セッションが再開されます。

クリーニング作業はすべて以下のログ・ファイルに記録されます。

- Windows の場合 :
  `<Data_Protector_home>¥log¥server¥cleaning.log`
- UNIX の場合 : `/var/opt/omni/server/log/cleaning.log`

ドライブの自動クリーニングの構成

ドライブの自動クリーニング機能を構成するには、以下の 2 つの手順を行います。

1. 汚れたドライブの検出機能を使用可能にします。これは、すべてのデバイスの種類 (スタンドアロンとライブラリ) に対して行うことが必要です。これにより、Data Protector はドライブによって発行されるイベントを認識できます。
2. ライブラリ・デバイスまたはマガジン・デバイス内でのクリーニング・テープ用のスロットを構成します。

汚れたドライブの検出を可能にする

汚れたドライブの検出機能を使用可能にするには、目的のドライブの [設定] プロパティ・ページで [汚れたドライブの検出] 拡張オプションを選択します。詳しい手順については、オンライン・ヘルプの索引キーワード「ドライブ・クリーニングの構成」を参照してください。

クリーニング・テープ用スロットの構成

SCSI ライブラリ内でクリーニング・テープ用スロットを構成するには、このデバイスの [レポジトリ] プロパティ・ページで [クリーニング] オプションをクリックし、ドロップダウン・リストで既存のスロットを選択します。バーコード・リーダーのサポートが有効化されているライブラリでは、クリーニング・スロットは構成できない点に注意してください。詳しい手順については、オンライン・ヘルプの索引キーワード「ドライブ・クリーニングの構成」を参照してください。

ドライブ・クリーニング構成のテスト

ドライブのクリーニングが正しく構成されたかどうかは、以下の手順に従ってテストします。

準備

1. ドライブに対応する Media Agent がインストールされているシステムにログオンします。
2. Data Protector の tmp ディレクトリに移動します。
   - HP-UX および Solaris システムの場合 : /var/opt/omni/tmp/
   - その他の UNIX システムの場合 : /usr/omni/tmp/
   - Windows システムの場合 : *<Data_Protector_home>*¥tmp¥
   - Novell NetWare システムの場合 : ¥usr¥omni¥tmp¥
3. simtab (Windowsシステムの場合)または.simtab (UNIXシステムの場合) という名前の ASCII ファイルを作成します。このファイルの作成時には、以下を考慮します。
   - フィールド区切り文字は、1 文字の ASCII 文字（タブまたは空白）である必要があります。
   - 論理デバイス名は、引用符で囲んだり、空白を含めてはいけません ("test drive" など)。

   simtab または .simtab ファイルの内容は、以下のようになります。

   CLEANME *<file_name>* *<drive_name>*

   ここで、*<file_name>* には汚れたドライブのシミュレートに使用するファイルの名前を指定し、*<drive_name>* にはテスト対象のドライブの名前を指定します。

複数のドライブをテストする場合は、それらに対応する複数のエントリを追加できます。ファイル名の前にディレクトリを追加しないでください。

構成のテスト

以下の手順に従って、構成をテストします。

1. 汚れたドライブのシミュレートに使用する空のファイルを Data Protector の tmp ディレクトリ内に作成します。ファイル simtab または .simtab で定義したのと同じファイル名を使用してください。
2. テスト対象のドライブを使用してバックアップを開始します。

Data Protector は選択されたドライブが汚れているものとみなして動作し、クリーニングを実行します。

指定したドライブでの汚れたドライブのシミュレーション動作を中止するには、シミュレーションに使用されているファイルを削除します。

ビジー・ドライブの処理

Data Protector では通常、ドライブにはメディアが入っていないとみなすため、復元またはバックアップが現在実行中でない限り、ドライブにメディアを入れたままにしないでください。ただし、いくつかの理由によりメディアがドライブに入ったままになる場合があります (別のアプリケーションで使用したメディアを取り出していない場合、またはデータをテープに書き込むシステム (Media Agent) がバックアップ中に異常終了した場合など)。このドライブを次回のバックアップで使用する場合は、このような状況に対応することが必要となります。Data Protector は、数通りの方法でこの状況に自動的に対処します。対処方法は、ライブラリ・オプション [ビジー・ドライブの処理] を使って構成できます。

以下のオプションを使用できます。

[中止] バックアップは中止されます (デフォルト)。

[取出し] ドライブからメディアが取り出され、空のスロットに置かれます。

[メール・スロットへのメディアの取出し]
ドライブからメディアが取り出され、ライブラリのメール・スロット (CAP) に置かれます。

バックアップを自動的に続行したい場合は、**[取出し]** を選択します。テープは不明なスロットに移動するので、次回のバックアップ実行前にライブラリのスキャンが行われます。

バーコードのサポートを可能にする

SCSI ライブラリ・デバイスがバーコードを使ってメディアを使用する場合、Data Protector は、以下のサポート機能により、バーコードを使用できます。

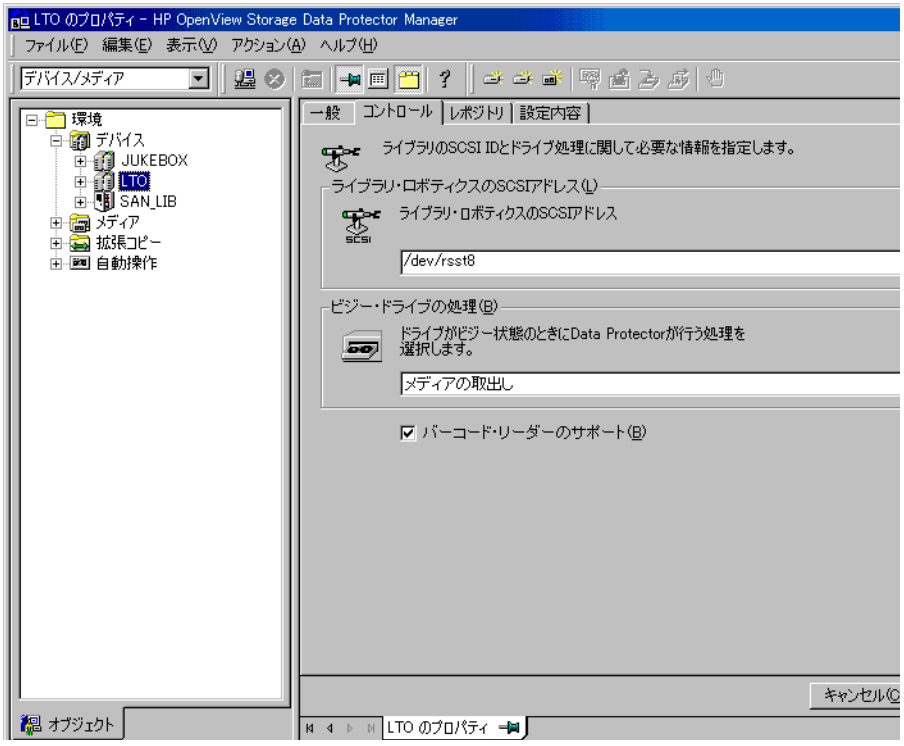
- CLN という接頭辞の付いたクリーニング・テープの認識。
- メディアをバーコードで参照。バーコードは、IDB 内の Data Protector メディア・ラベルに追加されます。メディアの初期化中に、必要に応じてバーコードをメディア・ラベルとして使用して、テープ上のメディア・ヘッダに書き込むこともできます。
- メディアのバーコードを使用した、ライブラリのレポジトリのスロット内にあるメディアのクィック・スキャン。この場合、バーコード機能を使わずにレポジトリをスキャンするよりはるかに高速でスキャンできます。[アクション] メニューで [バーコードのスキャン] をクリックして、メディアのライブラリのレポジトリをスキャンします。

デバイスの [コントロール] プロパティ・ページで [バーコード・リーダーのサポート] オプションを選択して、バーコードのサポートを使用可能にします。[初期化時にメディア・ラベルとしてバーコードを使用] を選択した場合、このライブラリを使用してメディアを初期化するときに、[バーコードを使用] オプションがデフォルトで有効になります。詳細は、図 2-13 (94 ページ) を参照してください。詳しい手順については、オンライン・ヘルプの索引キーワード「バーコード・リーダー・サポートのアクティブ化」を参照してください。

注記

セル内のすべてのバーコードは、メディアの種類または複数のライブラリの有無に関係なく一意でなければなりません。

図 2-13 バーコード・リーダー・サポートを可能にする



バックアップ・デバイスの無効化

バックアップ・デバイスの無効化は、デバイスが損傷したときや保守作業を実施するときに役立つ機能です。

バックアップ・デバイスを無効化すると、それ以降のバックアップ・セッションでは、そのデバイスが使用されなくなります。バックアップ仕様のデバイス・リストに含まれている別の利用可能なデバイスが代わりに使用されます (ただし、負荷調整が選択されている場合)。無効化したデバイスと同じロック名を使用しているデバイスは、すべて無効化されます。

特定のデバイスを保守する必要が生じたときは、他のデバイスをバックアップに使用したり、バックアップ用に構成したりすることができるので、そのデバイスが原因でバックアップが失敗するのを防止できます。

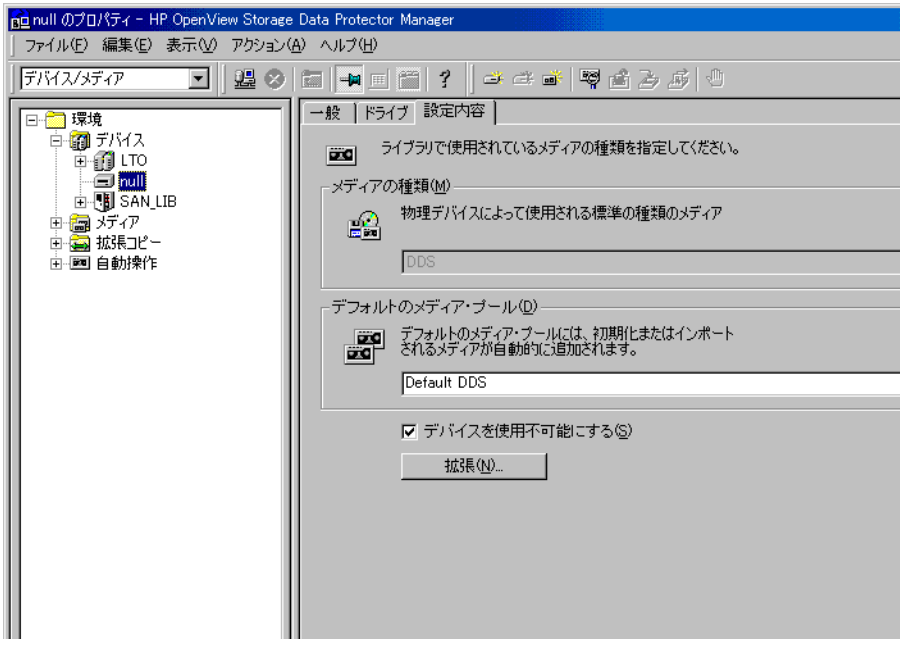
デバイスを無効化する方法

デバイスまたはドライブの [設定内容] プロパティ・ページで [デバイスを使用不可能にする] オプションを選択して、バックアップ・デバイスを無効化します。詳細は、図 2-14 を参照してください。詳しい手順については、オンライン・ヘルプの索引キーワード「バックアップ・デバイスの無効化」を参照してください。

デバイスを再起動する方法

そのデバイスをバックアップに利用できるようにするには、[デバイスを使用不可能にする] オプションをオフにする必要があります。

図 2-14 デバイスを無効化する



バックアップ・デバイスの削除

バックアップまたは復元に使用しているデバイスの使用を中止するには、Data Protector 構成からバックアップ・デバイスを削除します。この場合、このデバイスを使用していたすべてのバックアップ仕様からこのデバイスを削除したことを確かめてください。削除していない場合、バックアップまたは復元は正常に実行されません。

ヒント

バックアップ・デバイスを今後 Data Protector で使用しない場合は、Media Agent ソフトウェアをシステムから削除しても構いません。この操作は [クライアント] コンテキストから実行できます。

バックアップ・デバイスの削除方法

バックアップ・デバイスを削除するには、[デバイス / メディア] コンテキストを使用します。詳しい手順については、オンライン・ヘルプの索引キーワード「バックアップ・デバイスの削除」を参照してください。

バックアップ・デバイスの名前の変更

バックアップ・デバイスの名前を変更すると、バックアップまたは復元時にそのデバイスを新しい名前で指定できるようになります。

重要

デバイス名を変更したときは、そのデバイスを使用していたすべてのバックアップ仕様から古いデバイス名を削除する必要があります。古いデバイス名が残されていると、存在しないデバイスを参照することになるので、バックアップ・セッションまたは復元セッションが失敗します。

バックアップ・デバイスの名前を変更する方法

バックアップ・デバイスの名前は、デバイスの［一般］プロパティ・ページで変更します。詳しい手順については、オンライン・ヘルプの索引キーワード「バックアップ・デバイスの名前変更」を参照してください。

デバイスのロック

内部ロック

バックアップ・デバイスの内部ロックにより、2 つの Data Protector セッションが同時に同じ物理デバイスからアクセスされるのを防止できます。たとえば、1 つのバックアップ・セッションがあるデバイスを使用している場合、それ以外のすべてのバックアップ / 復元セッションがこのデバイスを使用するには、使用可能になるまで待機しなければなりません。バックアップまたは復元セッションが開始されたとき、Data Protector はそのセッションで使用されるデバイス、ドライブ、スロットをロックします。

メディアの操作を実行するメディア・セッション (初期化、スキャン、検証、コピー、またはインポートなど) も、デバイスをロックします。そのセッションの実行中は、他の操作がそのデバイスをロックしたり使用したりすることはできません。メディア・セッションがロックを取得できない場合、そのメディア操作は正常に実行されないため、ユーザーは後で同じ操作を再試行する必要があります。

マウント要求が発行された場合のロック

バックアップまたは復元セッションにおけるマウント要求中は、メディア管理操作 (新しいメディアのフォーマットなど) のためにデバイスを使用できます。

マウント要求が確認されると、バックアップまたは復元セッションはデバイスを再度ロックし、セッションを継続します。

Data Protector でのロック

1 つの物理デバイスを複数のデバイス名で構成するだけで、このデバイスに複数のデバイス特性を指定できます。

内部ロックは物理デバイスではなく論理デバイスに対して行われるため、あるバックアップ仕様でデバイス名を 1 つ指定し、他のバックアップ仕様で同じ物理デバイスを別のデバイス名で指定した場合、デバイスの競合が発生する可能性があります。バックアップ・スケジュールにもよりますが、これにより、Data Protector が複数のバックアップ・セッションで同時に同じ物理デバイスを使用する可能性があります。また、2 つのデバイス名を 2 種類の操作 (バックアップと復元、バックアップとスキャンなど) で使用した場合も、このような状況が発生する場合があります。

デバイスの競合を避けるため、どちらのデバイス構成でも仮想ロック名を指定できます。Data Protector はこのロック名を使ってデバイスが使用可能かどうかをチェックするので、競合を防止できます。

デバイスのロック

実際には同一の物理デバイスを指す 2 つの Data Protector バックアップ・デバイスを構成している場合、2 つの論理デバイスに対して拡張オプションで [ロック名] を指定することをお勧めします。[ロック名] は、Data Protector がバックアップ・セッションや復元セッションを開始する前に、デバイスをロックするために認識する名前です。論理デバイスは 2 つとも同じロック名にする必要があります。[ロック名] の使用例は、「SAN 環境内の共有デバイス」(54 ページ) を参照してください。

デバイスをロックする方法

バックアップ・デバイスをロックするには、デバイスの [設定内容] プロパティ・ページで [ロック名を使用] 拡張オプションを選択して、適切なロック名を入力します。詳しい手順については、オンライン・ヘルプの索引キーワード「バックアップ・デバイスのロック」を参照してください。

デバイスの同時処理数、セグメントおよびブロック・サイズ

ストリーミング

最大のデバイス性能を得るには、ストリーミングが維持されることが必要です。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。また、デバイス・ストリーミングは、ネットワーク負荷、1 回の動作でバックアップ・デバイスに書き込まれるデータのブロック・サイズなど他の要因にも依存します。

デバイスの同時処理数、セグメント・サイズおよびブロック・サイズの詳細は、『HP OpenView Storage Data Protector コンセプト・ガイド』第 3 章「メディア管理とデバイス」を参照してください。

同時処理数の変更

Data Protector では、デバイスの種類ごとに起動される Disk Agent のデフォルト数が設定されています。Media Agent へデータを同時に送信する Disk Agent の数を増やすことにより、デバイス・ストリーミングの性能が向上します。

目的のデバイスの [拡張オプション] ダイアログ・ボックスで、[同時処理数] を、各 Media Agent へデータを送信する Disk Agent の最大数に設定します。図 2-15 (102 ページ) を参照してください。詳しい手順については、オンライン・ヘルプの索引キーワード「同時処理数」を参照してください。

同時処理数もバックアップ仕様で設定できます。バックアップ仕様で設定した同時処理数は、デバイス定義で設定された同時処理数より優先的に使用されます。図 2-16 (103 ページ) を参照してください。詳しい手順については、オンライン・ヘルプの索引キーワード「同時処理数」を参照してください。

図 2-15 [拡張オプション] ダイアログ・ボックス : [同時処理数]

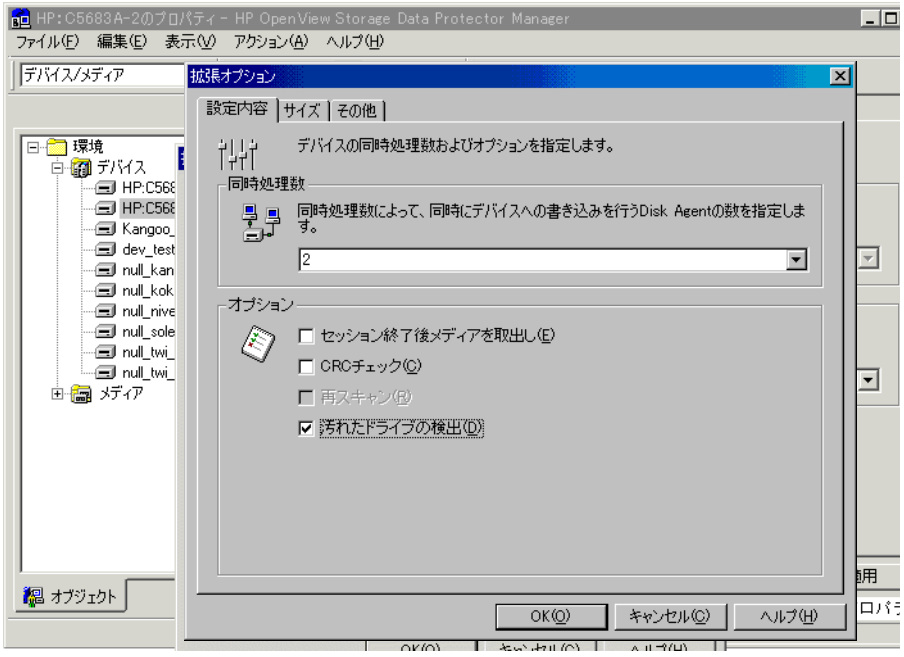
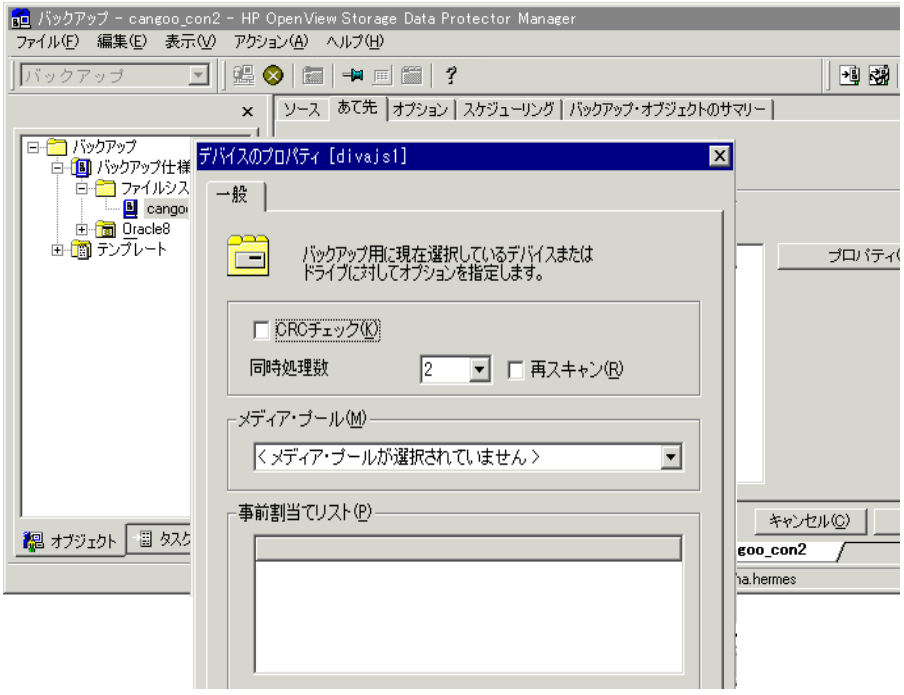


図 2-16 [デバイスのプロパティ] ダイアログ・ボックス : [同時処理数]



セグメント・サイズの変更

セグメント・サイズは、Data Protector がデータをメディアに書き込む際に使用するデータ領域のサイズに関連があります。各デバイスのセグメント・サイズはユーザーが構成できます。セグメント・サイズが小さいほど、メディアの中で使用されるスペースが大きくなることに注意してください。これは、各セグメントがファイル・マークを持っており、このファイル・マークがメディア上のスペースを占めるためです。ただし、ファイル・マークが多数あると、Media Agent が復元対象のデータを含むセグメントをより迅速に見つけることができるので、復元速度が向上します。

最適なセグメント・サイズは、デバイスで使用するメディアの種類やバックアップ対象となるデータの種類により異なります。テープ当たりの平均セグメント数は 50 です。デフォルトのセグメント・サイズは、テープの元の容量を 50 で割ることにより求められます。カタログ・サイズの最大値は、どのメディアについても 12 MB に制限されています。

最初の上限値に達すると、Data Protector はセグメントを完了します。容量の小さいファイルを多数バックアップした場合、メディア・カタログの上限値により早く達するので、セグメント・サイズは小さくなります。

セグメント・サイズは、目的のデバイスの [拡張オプション] ダイアログ・ボックスで変更できます。詳しい手順については、オンライン・ヘルプの索引キーワード「セグメント・サイズ」を参照してください。

バッファ数の変更

Data Protector Media Agent と Disk Agent は、データ転送時にメモリ・バッファを使用します。メモリは、バッファ領域数に分割されます。1 ～ 32 までの値を指定できます。

各バッファ領域は、8 個の Disk Agent バッファで構成され、各 Disk Agent バッファのサイズは、このデバイスに構成されているブロック・サイズと同じです。デバイスのデフォルトのブロック・サイズは 64 KB です。

バッファ数を変更するには、選択したデバイスの [拡張オプション] プロパティを変更します。詳しい手順については、オンライン・ヘルプの索引キーワード「Disk Agent のバッファ数」を参照してください。

ブロック・サイズ

デバイスがデータを受信すると、デバイスの種類 (DDS、DLT) に固有のブロック・サイズを使ってデータを処理します。

注記

各バックアップ・デバイス (ドライブ) には、ブロック・サイズが設定されています。復元は、ブロック・サイズに合わせて行われます。

Data Protector のブロック・サイズを変更する前に

Data Protector は、異なる種類のデバイスに対して、デフォルトのブロック・サイズを使用します。このブロック・サイズは、Data Protector で作成されたすべてのデバイスやさまざまなプラットフォーム上で動作する Media Agent に適用されます。

デバイスのブロック・サイズは、メディアのヘッダに書き込まれるので、Data Protector はどのサイズを使用すればよいか認識できます。デバイスのブロック・サイズがメディアのブロック・サイズと違う場合は、エラーが発生します。

Data Protector の GUI で、デバイスのブロック・サイズを変更できます。ただし、ブロック・サイズを変更する前に、ホスト・アダプタのサポートしているブロック・サイズを確認する必要があります。

以前の SCSI カード (Adaptec 2940 など) の最小ブロック・サイズは 56KB でした。現在、新しい SCSI カードで主に使用されている最小ブロック・サイズは 64KB です。

Windows Media Agent クライアントのレジストリを変更することで、そのクライアントの最大ブロック・サイズを大きくすることができます。ブロック・サイズの変更方法については、「Windows Media Agent 上のブロック・サイズの変更」(A-52 ページ) にある例を参照してください。

SCSI カードのブロック・サイズを変更する前に、SCSI カードのドキュメントを参照するか、ベンダーのサポート窓口に連絡してください

Data Protector でのブロック・サイズの変更

ブロック・サイズは、目的のデバイスの [拡張オプション] ダイアログ・ボックスで設定できます。詳しい手順については、オンライン・ヘルプの索引キーワード「ブロック・サイズ」を参照してください。

デバイス性能の調整

ブロック・サイズ

すべての論理デバイスについて、データを処理する単位 (**ブロック・サイズ**) を構成することが可能です。各デバイスにはそれぞれ異なるデフォルトのブロック・サイズが設定されており、この値を使用する方が安全 (セッションが正常に終了する可能性が高い) ですが、最適な性能は得られないことがあります。ブロック・サイズを調整すると、Data Protector セッションの性能を向上できます。

最適なブロック・サイズは、以下に示す環境要件によって異なります。

- ハードウェア (デバイス、ブリッジ、スイッチなど)
- ファームウェア
- ソフトウェア (オペレーティング・システム、ドライバ、ファイアウォールなど)

最適な結果を得るには、始めに最新のドライバやファームウェアをインストールして環境を最適化したり、ネットワークを最適化したりしておくことをお勧めします。

最適なブロック・サイズの求め方

最適なブロック・サイズを調べるには、ブロック・サイズの値を変更しながら通常の Data Protector 操作 (バックアップ、復元、コピーなど) を実行して、性能を測定します。

ただし、デバイスのブロック・サイズを変更すると、以前のブロック・サイズで作成したバックアップ・データは、そのデバイスでは復元できなくなることに注意してください。そのため、以前に作成したメディア上のデータも復元できるように、元の論理デバイスとメディア・プールはそのまま残しておき、テスト用にブロック・サイズを変えた新しい論理デバイスとメディア・プールを作成するようにしてください。

制限事項

デフォルトのブロック・サイズを変更する前に、以下の制限事項を確認しておいてください。

- 障害復旧 : EADR/OBDR のオフライン復旧 (「Windows システムの拡張自動障害復旧」(572 ページ) および「Windows システムのワンボタン障害復旧」(583 ページ) を参照) を実行するには、デフォルトの 64KB のブロック・サイズでデータをバックアップする必要があります。
- ライブラリ : 同一ライブラリ内に同種のテクノロジを使用する複数種類

のドライブがある場合は、これらのドライブのブロック・サイズを統一する必要があります。

- SCSI アダプタ : 選択したブロック・サイズが、そのデバイスの接続先ホストの SCSI アダプタでサポートされていることを確認してください。
- オブジェクトコピー機能 : コピー先デバイスのブロック・サイズは、コピー元デバイスのブロック・サイズと同じかそれより大きくなければなりません。
- ミラー : デバイスのブロック・サイズがミラー・チェーン内で漸減してはいけません。ミラー 1 の書き込みに使用されるデバイスのブロック・サイズは、バックアップに使用されるデバイスと同じかそれより大きくなければならず、同様に、ミラー 2 の書き込みに使用されるデバイスのブロック・サイズは、ミラー 1 の書き込みに使用されるデバイスと同じかそれより大きくなければなりません。これ以降も同様です。
- その他の制限事項については、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

Data Protector でのブロック・ サイズの変更

ブロック・サイズは、目的のデバイスの [拡張オプション] ダイアログ・ボックスで設定できます。詳しい手順については、オンライン・ヘルプの索引キーワード「ブロック・サイズ」を参照してください。

3 ディスクベースのデバイスの構成と使用

本章の概略

本章では、以下の項目について説明します。

注記

バックアップ・デバイスでは、専用の Data Protector ライセンスが必要になる場合があります。詳細は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

概要

Data Protector では、ディスクによるバックアップや復元を行うように設計されたデバイスを選択できます。これらのデバイスは、データをテープではなくディスクにバックアップするよう設計されているため、ディスクベースのデバイスと呼ばれています。これらのデバイスには、さまざまな機能や用途のものがあります。具体的には以下のとおりです。

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・デバイスは最も単純なディスクベースのデバイスです。このデバイスは手動で構成します。いったん作成したデバイスのプロパティを変更することはできません。スタンドアロン・ファイル・デバイスに保存できるデータの推奨最大容量は 2TB です。このデバイスを使用するうえで一番問題となるのは、いったん作成したデバイスを使用中に再構成できない点です。スタンドアロン・ファイル・デバイスの詳細は「スタンドアロン・ファイル・デバイスとファイル ジュークボックス デバイス」(B-1 ページ) を参照してください。

ファイル ジュークボックス

ファイル ジュークボックス デバイスは、論理的にはテープスタックと同じものです。このデバイスに含まれているスロットのサイズは、デバイスの最初の構成時にユーザーによって定義されます。ジュークボックス デバイスは手動で構成します。ファイル ジュークボックスのプロパティは、使用中に変更できます。ファイル ジュークボックス デバイスで推奨されるデータの最大記憶容量は、このデバイスを実行しているオペレーティング・システムがファイルシステムに保存できるデータ容量によってのみ制限されます。ファイル ジュークボックス デバイスの詳細は「スタンドアロン・ファイル・デバイスとファイル ジュークボックス デバイス」(B-1 ページ) を参照してください。

ファイル・ライブラリ・デバイス

ファイル・ライブラリ・デバイスは最も高度なディスクベースのデバイスです。このデバイスは、大量のデータを無人でバックアップおよび復元するために設計されたものです。ファイル・ライブラリ・デバイスは、Data Protector の GUI でウィザードを使用して自動構成されます。ファイル ジュークボックスの場合と同様に、ファイル・ライブラリ・デバイスで推

奨される最大記憶容量は、このデバイスを実行しているオペレーティング・システムがファイルシステムに保存できるデータ容量によってのみ制限されます。

推奨される使用方法

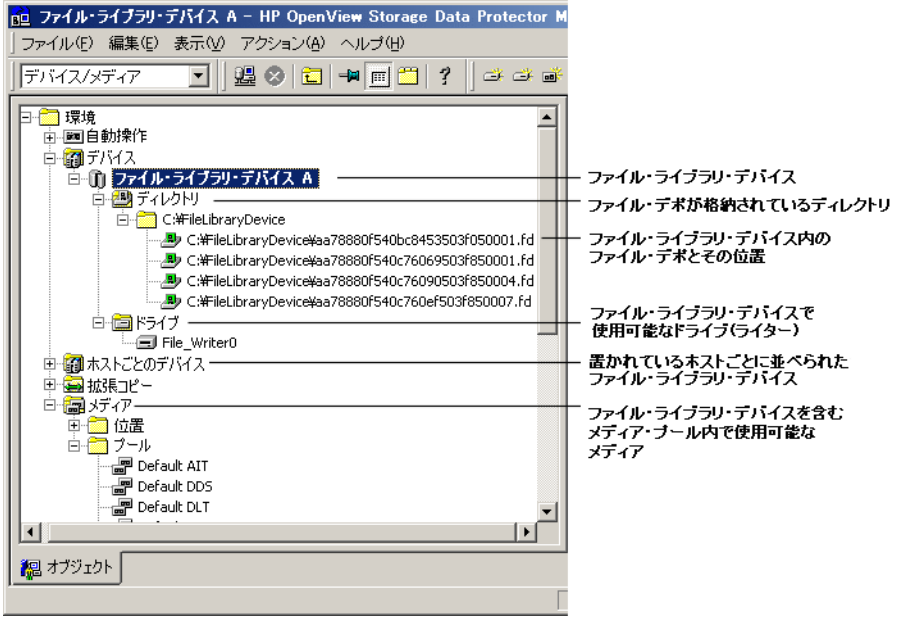
ここに示した 3 つのディスクベースのデバイスのうち、無人バックアップ用のデバイスとしてはファイル・ライブラリ・デバイスの使用をお勧めします。スタンドアロン・ファイル・デバイスは、本来、少量のデータ保存用に開発されたデバイスです。そのため、ごく単純な機能しかありません。ファイル ジュークボックス デバイスは、スタンドアロン・ファイル・デバイスの後に開発されたデバイスで、多少は高度な機能を持っていますが、ファイル・ライブラリ・デバイスに比べると柔軟性に欠けています。スタンドアロン・ファイル・デバイスとファイル ジュークボックス デバイスの構成および使用方法については、「スタンドアロン・ファイル・デバイスとファイル ジュークボックス デバイス」(B-1 ページ) を参照してください。ファイル・ライブラリ・デバイスの機能については、本章の以降の項で説明します。

ファイル・ライブラリ・デバイスの機能について

ファイル・ライブラリ・デバイスのディレクトリ構造

ファイル・ライブラリの構築は、ファイルを格納したディレクトリによってファイルシステムを構築するのと類似しています。ディレクトリは、ファイル・ライブラリ・デバイスを最初に構成するときに、ユーザー自身が作成します。ファイルは**ファイル・デポ**と呼ばれます。次の図はファイル・ライブラリのディレクトリ構造を示したものです。

図 3-1　ファイル・ライブラリ・デバイスのディレクトリ構造



ファイル・デポとは　ファイル・デポとはファイル・ライブラリの構成要素の 1 つで、データの保存先となる場所です。ファイル・ライブラリ・デバイスへのバックアップまたはコピーが実行されると、その都度ファイル・デポが自動的に作成されます。

注記

本章では、コピー・セッションとバックアップ・セッションを合わせて「バックアップ」と呼んでいます。これらの処理が行われると、データがデバイスに保存されます。

ファイル・デポの作成

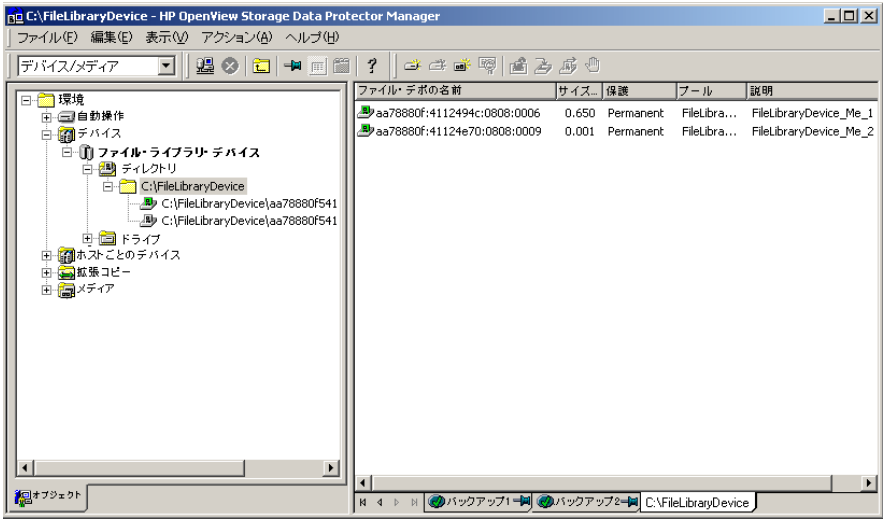
ファイル・ライブラリ・デバイスへの最初のバックアップが開始されると、Data Protector により、デバイス内にファイル・デポが自動的に作成されます。このデバイスを使用するデータ・バックアップ・セッションごとに、1 つのファイル・デポが作成されます。バックアップするデータの容量がデフォルトの最大ファイル・デポ・サイズを超える場合は、1 つのバックアップ・セッションに対して複数のファイル・デポが作成されます。

ファイル・デポの名前

各ファイル・デポには、システムにより自動生成される一意の識別子が名前として付けられます。

ファイル・デポには Data Protector によりメディア識別子も追加されます。この識別子により、ファイル・デポはメディア・プール内のメディアとして識別されます。メディアに追加されたこの識別子は、復元時に特定のバックアップ・セッションを識別するのに役立ちます。識別子は、結果エリアの [説明] フィールド、およびファイル・デポのプロパティで確認できます。ファイル・デポのプロパティを表示する方法については、オンライン・ヘルプの索引キーワード「設定 - ファイル・ライブラリ・デバイスのプロパティ」を参照してください。

図 3-2 **複数のファイル・デポ**



注記

ファイル・デポがリサイクルされた場合、ファイル・デポのアイコンは GUI に表示されたままですが、ファイル・デポの名前は GUI から消失してしまう可能性があります。詳細は、本項の「削除とリサイクル」(131 ページ) を参照してください。

ファイル・デポのサイズ

ファイル・デポのサイズは、ファイル・ライブラリ・デバイスを最初に作成するときに定義します。このプロセスでは、ファイル・デポの最大サイズをはじめとして、デバイスのサイズに関するすべてのプロパティを指定します。ファイル・デポのサイズに関するプロパティは、1 度入力するだけで各ファイル・デポに対してグローバルに適用されます。同一セッション内でバックアップされるデータ容量が最初に指定したファイル・デポのサイズより大きい場合、Data Protector は、ファイル・ライブラリ・デバイスに割り当てられたディスク容量を使い切ってしまうまで、自動的にファイル・デポの数を増やしていきます。

Windows 上でのファイル・デポ / スロットの最大推奨サイズは 50GB です。ただし、Windows 上では最大 600GB のファイル・デポを使用して、ファイル・ライブラリ・デバイスのテストが行われています。Unix 上でのファイル・デポの最大推奨サイズは 2TB です。

ファイル・デポの使用容量

Data Protector は、デバイスが使用できるディスク容量がなくなってしまうまで、ファイル・デポを自動作成します。ファイル・ライブラリ・デバイス用に空けておくべきディスク容量は、デバイスを最初に設定するときにデバイスのプロパティで定義します。ファイル・デポのプロパティの設定方法については、「ファイル・ライブラリ・デバイスのプロパティの設定」(120 ページ) を参照してください。

ディスクフルの処理

ファイル・ライブラリ・デバイスが使用できるディスク容量の合計がユーザーの指定したレベルを下回った場合、イベント・ログに通知が表示されます。

バックアップに使用できるディスク容量が不足している場合は、スペース情報メッセージが表示されます。ディスク容量が不足した場合の対処方法については、「ファイル・ライブラリ・デバイスのディスクに空きスペースがない」(734 ページ) を参照してください。

ファイル・ライブラリ・デバイスの内容の表示

ファイル・ライブラリ・デバイスの内容は、以下の 2 つの観点から表示できます。

- デバイス
- メディア

[デバイス] 表示

[デバイス] 表示を使用すると、データベース内に登録されているすべてのデバイスの一覧を表示できます。この表示を使用して、ファイル・ライブラリ・デバイスで実行可能なすべての操作を実行できます。ファイル・ライブラリ・デバイスを作成および構成する場合は、この表示方法を使用します。[デバイス] 表示で実行できる操作の種類については、「ファイル・ライブラリの [デバイス] 表示」(123 ページ) を参照してください。

[メディア] 表示

[メディア] 表示には、特定のメディア・プールに割り当てられたすべてのメディアの一覧が表示されます。メディア・プールとは、バックアップに使用できる同じ種類のすべてのメディアの集合です。メディア・プールの詳細は、本ガイドの第 5 章「メディアの管理」(151 ページ) を参照してください。[メディア] 表示でファイル・ライブラリ・デバイスに対して実行できる操作の種類については、「ファイル・ライブラリの [メディア] 表示」(126 ページ) を参照してください。

ファイル・ライブラリ・デバイスの作成および構成

ファイル・ライブラリ・デバイスの構成では、デバイスにとって不可欠な特性を定義します。デバイスの作成および構成は、Data Protector の GUI でウィザードを使用して実行されます。

ファイル・ライブラリ・デバイスの構成

ファイル・ライブラリ・デバイスの構成作業では、以下の手順を行います。

1. ファイル・ライブラリ・デバイスで使用するディスク上に、1 つまたは複数のディレクトリを作成します。
2. Data Protector の GUI でウィザードを使用して、デバイスのプロパティを定義します。

デバイスが作成され、デバイスに対してバックアップが実行されたら、デバイス内にファイル・デポが作成されます。バックアップされたデータはここに格納されます。

ファイル ライブラリ・デバイスのプロパティ

ファイル・ライブラリ・デバイスのプロパティは、デバイスの作成後、いつでも変更できます。ファイル・ライブラリ・デバイスのプロパティの設定および変更については、「ファイル・ライブラリ・デバイスのプロパティの設定」(120 ページ) を参照してください。

[メディア・プール]

デバイス仕様で別途指定されない限り、新しいファイル・ライブラリ・デバイスに対しては、それぞれ新しいメディア・プールが作成されます。メディア・プールの詳細は、本ガイドの第 5 章「メディアの管理」(151 ページ) を参照してください。

ファイル ライブラリ・デバイスの最大サイズ

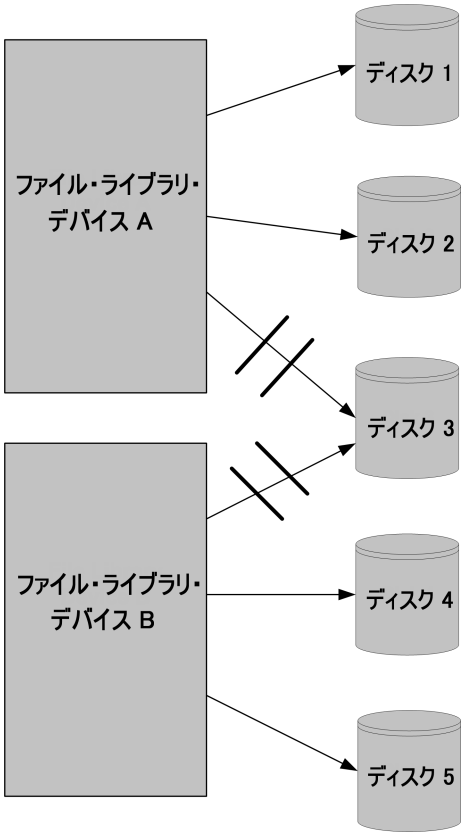
ファイル・ライブラリ・デバイスは複数のファイル・デポから構成されるため、ファイル・ライブラリ・デバイスの最大サイズは、ファイルシステムの最大サイズと同じ大きさになります。特定のオペレーティング・システムが管理できるファイルの最大サイズについては、各オペレーティング・システムのマニュアルで確認してください。

ディスクあたりのデバイス数

ファイル・ライブラリ・デバイス内には 1 つまたは複数のディレクトリを作成できます。ただし、1 つのファイルシステム上には 1 つのディレクトリしか配置できません。

ファイル・デポがさまざまなディスク上に配置されている環境では、2 つの異なるファイル・ライブラリ・デバイスのファイル・デポを、同一ディスク上に共存させないようにしてください。両者のプロパティが異なっている場合に、Data Protector 内で競合が発生してしまうことがあるからです。競合状態の例としては、1 つのファイル・ライブラリ・デバイスのプロパティではファイル・デポのためのディスクの残容量が 20MB に指定されているのに、他のファイル・ライブラリ・デバイスのプロパティではファイル・デポが存在するためのディスクの残容量が 10MB に指定されている場合があげられます。

図 3-3　ファイル・デポのプロパティの競合



ファイル・ライブラリ・デバイス ウィザードを使用したファイル・ライブラリ・デバイスの作成

ファイル・ライブラリ・デバイスは、Data Protector GUI のファイル・ライブラリ・デバイス ・ウィザードを使用して作成できます。

必要条件

ファイル・ライブラリ・デバイスを作成するには、以下の必要条件を満たす必要があります。

- ファイル・ライブラリ・デバイスの配置先となるディスクが、ファイル・ライブラリ・デバイスが存在するファイルシステム内に表示されていること。
- ファイル・ライブラリ・デバイスの内容が作成されるディレクトリが、ファイル・ライブラリ・デバイスが配置されるディスク上に存在していること。
- Windows ファイルシステム上にファイル・ライブラリを作成する場合は、デバイスを作成する前に圧縮オプションをオフにすること。

ファイル・ライブラリ用のディレクトリの作成方法

ファイル・ライブラリ・デバイスを作成するには、デバイスを配置しようとする内部ディスクまたは外部ディスクのどちらかにディレクトリを作成する必要があります (例 : `C:¥FileLibrary`)。

ファイル・ライブラリは、ネットワーク・ドライブまたは UNIX 上の NFS マウント・ファイルシステムに配置することも可能です。バックアップを実行するためには、Media Agent ホスト上の Data Protector Inet プロセスがドライブへの書き込みを行えなければなりません。Inet プロセスのプロパティを設定する方法については、オンライン・ヘルプを参照してください。

ファイル・ライブラリ・デバイスは、Media Agent に対してローカルなディスク上に配置することをお勧めします。この条件が満たされない場合、ファイル・ライブラリ・デバイスのパフォーマンスが低下する可能性があります。

注意

ファイル・ライブラリ用に作成されたディレクトリをディスクから削除しないことが重要です。これを削除してしまうと、ファイル・ライブラリ・デバイス内のデータが失われてしまいます。

デバイス特性の定義方法

Data Protector を起動して、[デバイス / メディア] コンテキストを選択します。[デバイス] を右クリックし、[デバイスの追加] をクリックします。新しいファイル・ライブラリ・デバイスの追加方法については、オンライン・ヘルプの索引キーワード「構成 - ファイル・ライブラリ・デバイス」を参照してください。

デバイスのプロパティの定義方法

ファイル・ライブラリ・デバイスの構成過程で、デバイスのサイズに関するプロパティを設定できます。詳細は、「ファイル・ライブラリ・デバイスのプロパティの設定」(120 ページ) を参照してください。

次に行う手順

作成直後のファイル・ライブラリ内には、ファイル・デポはありません。ファイル・ライブラリ・デバイスへのバックアップが実行されると、必要に応じてデバイス内にファイル・デポが作成されます。

ファイル・ライブラリ・デバイスのプロパティの設定

ファイル・ライブラリ・デバイスのプロパティは、デバイスの作成時に設定されます。これらのプロパティはデバイスの使用中にいつでも変更できます。

定義されるプロパティ

ファイル・ライブラリ・デバイスには以下の 2 種類のプロパティを設定できます。

- デバイスのプロパティ
- メディア・プールのプロパティ

デバイスのプロパティ

デバイスのプロパティでは、すべてのデバイス特性が決定されます。デバイスのプロパティには、デバイス名、そのデバイスの存在するホスト、そのデバイスの割り当てられたメディア・プールなどが含まれます。メディアの種類は [ファイル] となっており、この値は変更できません。デバイスのプロパティを表示する方法については、オンライン・ヘルプの索引キーワード「設定 - ファイル・ライブラリ・デバイスのプロパティ」を参照してください。

デバイスのプロパティでは、デバイスが機能するために必要な空きディスク容量も指定できます。デバイス・プロパティの指定には、[プロパティ] ダイアログを使用します。[プロパティ] ダイアログは、[デバイスのプロパティ] ペインからアクセスできます。

[プロパティ] ダイアログ

[ファイル・ライブラリ・デバイス] ウィザードの [プロパティ] ダイアログを使用すると、ファイル・ライブラリ・デバイスのサイズに関するプロパティを指定できます。

[プロパティ] ダイアログに指定したデバイス・プロパティは、プロパティの変更後にファイル・ライブラリ・デバイス内に新規作成されるファイル・デポに適用されます。デバイス・プロパティの変更前に作成されていたファイル・デポのプロパティは変更されません。

図 3-4　[プロパティ] ダイアログ

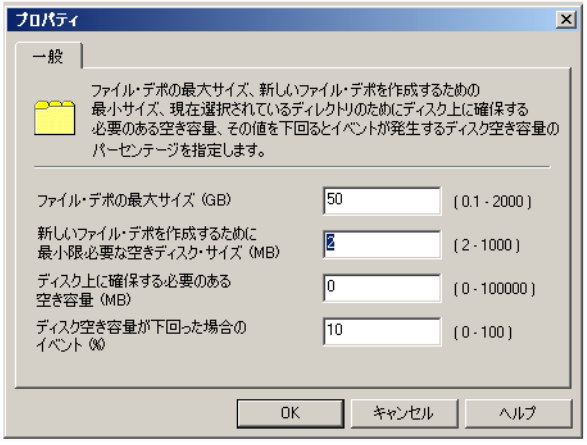


表 3-1　[プロパティ] ダイアログで設定できる値

フィールド名	デフォルト値	最小値	最大値
ファイル・デポの最大サイズ (GB)	50	0.1	2TB-1MB
新しいファイル・デポを作成するために最小限必要な空きディスク・サイズ (MB)	2	2	1000
ディスク上に確保する必要のある空き容量 (MB)	0	0	105 (100000)

表 3-1 **[プロパティ] ダイアログで設定できる値**

フィールド名	デフォルト値	最小値	最大値
ディスク空き容量が下回った場合のイベント (%)	10	0	100

プロパティの計算方法

Data Protector では、以下の例に示すようにファイル・ライブラリ・デバイスのプロパティを計算します。

ディスクのプロパティ

ディレクトリ サイズ合計 = 100GB

使用済みディレクトリ容量 = 20 GB

ファイル・ライブラリ・デバイスのプロパティ

ディスク空き容量の設定 = 30GB

書き込み可能な容量の計算

使用可能な容量からディスク空き容量を減算 80 GB - 30 GB = 50 GB

書き込み可能な容量 = 50GB

Data Protector は、ファイル・デポを使用する前に上記の計算を実行します。容量が不足している場合、Data Protector はユーザーにメッセージを通知します。この容量チェックは、各バックアップ・セッションの開始時に行われます。ディスク容量が不足した場合の対処方法については、「ファイル・ライブラリ・デバイスのディスクに空きスペースがない」(734 ページ) を参照してください。

ファイル・ライブラリ・デバイスの変更

ファイル・ライブラリ・デバイスの作成後、Data Protector では、一定範囲内でデバイス構成のチェックおよび変更ができるようになっています。

ファイル・ライブラリの [デバイス] 表示

ファイル・ライブラリ・デバイスの [デバイス] 表示を使用すると、デバイスとデバイス内のファイル・デポの動作およびプロパティを変更できます。

[デバイス] 表示へのアクセス

[デバイス] 表示にアクセスするには以下の手順を実行します。

1. Data Protector を起動して、コンテキスト・リストで［デバイス / メディア］を選択します。
2. ［ デバイス ］を展開し、目的のデバイスをクリックします。
3. デバイス内のディレクトリまたはドライブを表示するには、目的の項目をクリックします。
4. デバイスのリストから、関係するファイル・ライブラリ・デバイスの名前を選択します。

アクセス可能な項目

［ デバイス ］表示でアクセスできる GUI 項目は以下のとおりです。

- ディレクトリ
- ドライブ

ディレクトリ

[ディレクトリ] 項目には、ファイル・ライブラリ・デバイス内のディレクトリが一覧表示されます。ディレクトリに格納されているファイル・ライブラリのデポにはここからアクセスできます。

ドライブ

ファイル・ライブラリの [ドライブ] 項目には、ファイル・ライブラリ・デバイスへの書き込みを行うドライブが表示されます。ドライブとは、バックアップ・デバイスにデータを渡す「ライター」の働きをするものです。

ドライブに対する操作の実行

[デバイス] 表示の [ドライブ] 部分を使用して、ファイル・ライブラリの存在するドライブに対する操作を実行できます。各メニュー項目については本項で説明します。

スキャン

[ドライブのスキャン] によって、ファイル・ライブラリ内のファイル・デポに関する IDB 内の情報が更新されます。いずれかのファイル・デポを別の場所に移動した場合は、このオプションを使用してください。

注記

ドライブのスキャンは、デバイス内にファイル・デポが存在する場合、つまりそのデバイスへのバックアップが既に行われている場合にのみ実行可能です。

削除

[削除] オプションを使用すると、IDB からドライブを削除できます。ただし、ドライブを持たないファイル・ライブラリ・デバイスは使用できません。すべてのドライブを削除した場合、バックアップや復元にそのデバイスを使用するためには、新しいドライブを作成する必要があります。

プロパティ

[プロパティ] オプションを使うと、ドライブの一般的なプロパティを表示できます。ここにはドライブを使用しているデバイスの名前、デバイスの種類、ドライブの存在するホスト名などが含まれます。また、デバイスに対するライター (ドライブ) のプロパティのチェックや変更も可能で、たとえば、巡回冗長チェック、データのブロック・サイズとセグメント・サイズ、マウント要求がドライブに到着してから書き込みが開始されるまでの遅延時間、ドライブのロック名などを設定できます。

ファイル・ライブラリ・デバイスに対する操作の実行

[デバイス] 表示内でファイル・ライブラリ・デバイスを右クリックするとポップアップ メニューが表示され、デバイスの削除やデバイス・プロパティの表示などの操作を実行できます。各メニュー項目については本項で説明します。

削除

[削除] オプションを使用すると、IDB からファイル・ライブラリを削除できます。ただし削除が実行できるのは、デバイスに保護されたデータが含まれていない場合のみです。詳しい手順については、「削除とリサイクル」(131 ページ) またはオンライン・ヘルプの索引キーワード「削除 - ファイル・ライブラリ・デバイス」を参照してください。

プロパティ

[プロパティ] オプションを使うと、デバイス構成を表示して変更できます。このオプションを使用して、デバイスの名前を変更したり、デバイス内の各ディレクトリのサイズに関するプロパティを変更したり、IDB からディレクトリを削除したりできます。ファイル・デポ (ディレクトリ) のサイズに関するプロパティを変更する方法については、「ファイル・ライブラリ・デバイスのプロパティの設定」（120 ページ) を参照してください。

[デバイス] 表示でのファイル・デポに対する操作の実行

ファイル・ライブラリ内のファイル・デポを右クリックするとポップアップ メニューが表示され、ファイル・デポに対するスキャン、フォーマット、インポート、エクスポート、リサイクルなどの操作、カタログのインポート、ファイル・デポのプロパティの表示などを実行できます。

スキャン

Data Protector では、各ファイル・デポ上で診断を実行するためのスキャン機能を提供しています。ファイル・デポを選択してスキャンを実行すると、Data Protector によって、デポの絶対パス、デポ内に保存されたメディアの種類、および IDB 内のデポのラベルに関する情報が提供されます。

注記

バックアップに一度も使われていないファイル・ライブラリ・デバイスについては、デバイス内のファイル・デポをスキャンすることはできません。

フォーマット

ファイル・デポをフォーマットすると、ファイル・デポに関する情報が Data Protector IDB に保存されて、Data Protector でそのファイル・デポを使用できるようになります。IDB には、メディア ID、説明、および位置に関する情報が記録されます。ファイル・デポのフォーマット時には、ファイル・デポを所属させるプールも指定してください。

通常、ファイル・デポは作成時にフォーマットされるため、ファイル・デポのフォーマットを特に実行する必要はありません。別のデバイスのメディアをファイル・ライブラリにインポートし、その特性 (ブロック・サイズなど) を変更するような場合には、メディアのフォーマットが必要になります。

インポート

ファイル・ライブラリからいったんエクスポートしたファイル・デポをインポートすることも可能です。インポートできるのは、ファイル・ライブラリ・デバイスにかつて所属しており、過去にエクスポートされたファイル・デポに限られます。

エクスポート

ファイル・デポのエクスポートは、IDB からデポの内容を削除するために使用されます。このユーティリティは、デポの削除の一部として使用されます。ファイル・デポの削除方法の詳細は、オンライン・ヘルプの索引キーワード「ファイル・デポのリサイクル」を参照してください。

リサイクル

ファイル・デポをリサイクルすると、そのファイル・デポに対するデータ保護は [なし] に設定されます。ファイル・ライブラリ・デバイスに対してバックアップが次に実行されるときに、この領域はバックアップ・データによって上書きされます。ファイル・デポのリサイクル方法の詳細は、オンライン・ヘルプの索引キーワード「ファイル・デポのリサイクル」を参照してください。

カタログのインポート

ファイル・デポのカタログ保護期限が切れると、復元に使用できる項目を Data Protector GUI 上で調べることができなくなります。IDB からカタログをインポートすると、これらの項目を再び GUI 上で見られるようになります。

カタログのインポートは、ファイル・デポに対するログ・レベルが低く設定されており、このレベルを [すべてログに記録] に引き上げたい場合にも使用できます。カタログのインポート機能を使用すると、より高いログ・レベルを再設定できます。

プロパティ

[プロパティ] オプションを使用すると、各ファイル・デポに関するすべての情報を表示できます。ファイル・デポのプロパティは変更することも可能です。プロパティの変更方法の詳細は、「ファイル・ライブラリ・デバイスのプロパティの設定」(120 ページ) またはオンライン・ヘルプの索引キーワード「設定 - ファイル・ライブラリ・デバイスのプロパティ」を参照してください。

ファイル・ライブラリの [メディア] 表示

[メディア] 表示を使用すると、メディア・プールからの視点でデバイスの内容を変更できます。メディア・プールとは、同じ種類のバックアップ用メディアの集まりです。各ファイル・ライブラリ・デバイスに対しては、それぞれ新しいメディア・プールが作成されます。メディア・プールの命名規則は、`<LibraryName>_MediaPool` になります。

メディア・プールの設定

メディア・プールの設定は変更できます。Data Protector におけるメディア管理の詳細は、第 5 章「メディアの管理」(151 ページ) を参照してください。

[メディア] 表示を使用すると、特定のメディア・プールに所属するメディアや、デバイス内の個々のファイル・デポに対してさまざまな操作を実行できます。

[メディア] 表示へのアクセス

[メディア] 表示にアクセスするには以下の手順を実行します。

1. Data Protector を起動して、コンテキスト・リストで［デバイス / メディア］を選択します。
2. [メディア] をクリックします。
3. [プール] をクリックします。
4. ファイル・ライブラリ内の目的のメディア・プールの名前をダブルクリックします。

ファイル・ライブラリ・デバイスが使用するメディア・プールに対する操作

本項では、ファイル・ライブラリが所属するメディア・プールを操作するための各メニュー項目について説明します。

フォーマット

メディア・プール内の特定のメディアを選択してフォーマットできます。メディアをフォーマットすると、そのメディアに関する情報が Data Protector IDB に保存されます。

注記

ファイル・ライブラリ・デバイスへの最初のバックアップを実行するまでは、そのデバイスをフォーマットすることはできません。これは、最初のバックアップが実行されるまでは、ファイル・ライブラリ・デバイス内にファイル・デポが作成されておらず、また、ファイル・デポを手動で作成することもできないためです。バックアップ中に作成されるファイル・デポは、メディアに相当します。ファイル・ライブラリ・デバイス用のメディア・プールのメディア割り当てポリシーによっては、新しくフォーマットされたメディアは自動的に削除されます。

メディアをフォーマットするときは、デバイスが存在しているファイルシステムで許可されているサイズより大きい値にフォーマットしないでください。たとえば、Windows FAT ファイルシステムを使用している場合は、ファイルのサイズは 4GB までに制約されます。

インポート

メディアをメディア・プールにインポートすると、現在のメディア・プールにメディアがインポートされます。

通常このオプションは、過去にファイル・デポをエクスポートした場合にのみ使用します。これは、デバイスの削除に先立ってエクスポートしたファイル・デポを、再びインポートするための機能です。ファイル・ライブラリ・デバイスの削除方法の詳細は、「削除とリサイクル」(131 ページ)またはオンライン・ヘルプの索引キーワード「削除 - ファイル・ライブラリ・デバイス」を参照してください。

注記

別のホスト上にあるファイル・ライブラリからのメディアのインポートは、ジュークボックス デバイスについてのみ可能です。詳しい手順については、オンライン・ヘルプの索引キーワード「ファイル・ライブラリ・メディア - 別のホストへのインポート」を参照してください。

削除

[削除] オプションを使用すると、メディア・プール全体を削除できます。ただし削除ができるのは、そのメディア・プールと関連付けられているファイル・ライブラリ・デバイス内に保護されたデータが含まれていない場合に限られます。ファイル・ライブラリ・デバイス内のデータの保護レベルを変更する方法については、オンライン・ヘルプの索引キーワード「削除 - ファイル・ライブラリ・デバイス」を参照してください。

メディアの選択

[メディアの選択] オプションは、メディアの内容を別の場所にコピーするために使用します。このオプションを使用するには、コピー元のメディアとコピー先のメディアが同じ種類でなければなりません。ファイル・ライブラリ・デバイスの場合であれば、デバイスが存在するディスクから別のディスクにデータコピーするときにのみ、[メディアの選択] オプションを使用できます。

プロパティ

[プロパティ] オプションを使うと、メディア・プールに関する情報を表示できます。この中には、そのメディア・プールを使用するファイル・ライブラリ、プール内で使われている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できるとみなされる期間、メディアへの最大上書き回数などの情報が含まれます。[プロパティ] オプションを使用して、メディア・プールのプロパティを変更することも可能です。詳細は、オンライン・ヘルプの索引キーワード「メディア・プールのプロパティ」を参照してください。

[メディア] 表示内での操作

本項では、[メディア] 表示内でメディア (この場合はファイル・デポ) に対して実行できるメニュー項目について説明します。

エクスポート

ファイル・デポをエクスポートすると、ファイル・デポに関する情報が IDB から削除され、Data Protector はそのファイル・デポの存在を認識しなくなります。ただしデポの情報はまだ残っているので、後で必要に応じてインポートして、ファイル・デポを回復することができます。エクスポートは、ファイル・ライブラリ・デバイスを削除するための前段階として実行されます。この作業の詳細は、「[デバイス] 表示でのファイル・デポに対する操作の実行」(125 ページ) またはオンライン・ヘルプの索引キーワード「削除 - ファイル・ライブラリ・デバイス」を参照してください。

位置の変更

[位置の変更] オプションを使うと、メディアの現在位置に関する情報を挿入できます。この情報は Data Protector では使われません。これは、ユーザー向けの参考情報です。

リサイクル

メディアをリサイクルすると、メディア内に保持されているデータの保護レベルが「なし」に変更されます。これによって、メディアが使用しているディスク上の領域が、次のバックアップ時には再使用されるようになります。メディアのリサイクルは、ファイル・ライブラリ・デバイスの削除処理の一部として行われます。詳細については、本章の「削除とリサイクル」(131 ページ)、またはオンライン・ヘルプの索引キーワード「削除 - ファイル・ライブラリ・デバイス」を参照してください。

プールへの移動

このオプションを使うと、同じ種類のメディアを含むメディア・プール間でメディアを移動できます。バックアップを再編成して、各プールの目的を再設定したい場合は、このオプションが必要になります。

コピー

ファイル・デポの内容を別のメディアにコピーすることも可能です。アーカイブの目的でデータを別の場所にコピーしたり、復元に使用するためのコピーを作成したりする場合は、このオプションが役立ちます。このオプションを使用するには、コピー元のメディアとコピー先のメディアが同じ種類である必要があります。ファイル・ライブラリ・デバイスの場合は、コピー元メディアの種類がディスクになるため、コピー先メディアもディスクでなければなりません。

検証

メディアをまだ復元に使用できるかどうかを調べるには、ファイル・デポの検証機能が役立ちます。検証では、ファイル・デポの品質がさまざまな面 (すべての識別情報など) からチェックされます。また、すべての情報ブロックが読み込まれ、ファイル・デポが最初に作成されたときに巡回冗長チェックが使用されたかどうかチェックされます。

カタログのインポート

このオプションは、ファイル・デポの作成時に生成されたカタログ・データの保護期限が切れている場合に使用します。カタログをインポートすると、メディアから IDB にカタログ・データが再インポートされます。復元時にメディアの一覧をブラウズするには、このカタログ・データが必要です。

メディアの選択

この機能は、メディア・プールにあるメディアの全リストをブラウズせずに、特定のメディア (ここではファイル・デポ) を検索して選択するために使用されます。

プロパティ

[プロパティ] オプションを使うと、メディア・プール内のメディアのプロパティを表示できます。このオプションでは、メディアの名前、IDB 内でのメディア ID、割り当て先のメディア・プールの名前、メディア内に保存されたオブジェクトの一覧、メディアの使用頻度に関する詳細情報といったメディアに関する情報が提供されます。[プロパティ] オプションを使ってメディアの説明を変更したり、バックアップ時のメディア・プール内のメディアの使用順序を指定したりすることも可能です。

注記

デフォルトでは、ファイル・ライブラリ・デバイス用のメディア・プールのメディア割り当てポリシーは、[追加不可能] に設定されています。つまりデフォルトではバックアップを開始する前に、ファイル・ライブラリ・デバイスにより、デバイス内に保護されていないデータがないかチェックされるため、バックアップ用メディアの事前割り当てを行うことはできません。デバイス内に保護されていないデータがあると、デバイスへの書き込みが開始される前に、まずそのデータが削除されます。ただし、メディアの事前割り当てポリシーを [追加可能] に設定すると、このポリシーが機能するようになります。メディア割り当てポリシーの変更方法については、オンライン・ヘルプの索引キーワード「メディアの事前割当て」を参照してください。

削除とリサイクル

ファイル・デポまたはファイル・ライブラリ・デバイス全体をリサイクルして削除すると、ディスク・スペースを解放できます。

リサイクル

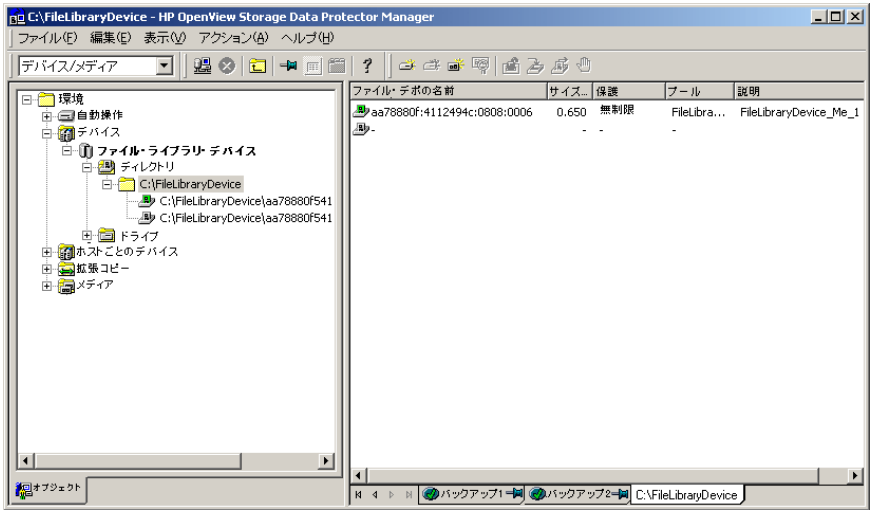
ファイル・ライブラリ・デバイスに割り当てられた領域を再使用したい場合は、個々のファイル・デポ、またはファイル・ライブラリ内のすべてのファイル・デポをリサイクルします。これによって、リサイクル対象のファイル・デポが使用していたディスク上の領域が解放されて、次のバックアップ時に再使用されるようになります。保護されていないファイル・デポを削除して新しいファイル・デポを作成しても同じことです。

エクスポート

[エクスポート] オプションを使うと、Data Protector IDB 内の項目を削除できます。このオプションは、対象となる項目にデータ保護が設定されていない場合にのみ使用できます。そのため、[エクスポート] オプションを使用するには、最初にその項目をリサイクルする必要があります。

ファイル・デポをエクスポートすると、Data Protector GUI では、以下のようにファイル・デポのアイコンだけが表示され、名前は消失した状態になります。

図 3-5 **エクスポートしたファイル・デポのラベル**



エクスポートしたファイル・デポのアイコンを削除することも可能です。GUI 上の一覧からアイコンを削除しても、ファイル・デポが IDB から物理的に削除されるわけではありません。ファイル・ライブラリ・デバイスのアイコンを削除する方法の詳細については、オンライン・ヘルプの索引キーワード「削除 - ファイル・ライブラリ・デバイス」を参照してください。

削除

削除は 3 つの段階に分けて行われます。最初に、削除対象の項目からデータ保護を削除します。これをリサイクル・プロセスと呼びます。次に、[エクスポート] オプションを使用して、対象の項目を Data Protector IDB からエクスポートします。最後に削除処理を実行します。これらのオプションは、特定の項目に対してのみ、またはファイル・ライブラリ全体に対して使用できます。

ファイル・ライブラリの削除は、デバイス内に保護されたデータが含まれていない場合にのみ実行できます。ファイル・ライブラリ・デバイスの内容はファイル・デポに格納されています。ファイル・ライブラリ・デバイス全体を削除するには、最初に各ファイル・デポのデータ保護レベルを変更してから、それぞれのファイル・デポをエクスポートする必要があります。この作業が終了して初めて、デバイスの削除が可能になります。

ファイル・ライブラリ・デバイスの削除方法の詳細については、オンライン・ヘルプの索引キーワード「削除 - ファイル・ライブラリ・デバイス」を参照してください。

ファイル・ライブラリ・デバイスの–コマンド行インタフェースのオプション

ファイル・ライブラリ・デバイスをコマンド行インタフェース (CLI) から操作するために、以下の 2 種類のユーティリティが用意されています。

- `omniupload`
- `omnidownload`

`omniupload` はファイル・ライブラリ・デバイスの作成に、`omnidownload` はデバイスの削除に使用します。これらのコマンドの使用方法については、`omniupload` と `omnidownload` の man ページをそれぞれ参照してください。

4 ユーザーとユーザー・グループの構成

本章の概略

本章ではユーザー・グループと各ユーザーを構成する方法を説明します。本章では、以下の項目について説明します。

Data Protector ユーザー権限

Data Protector ユーザーには、所属しているユーザー・グループごとにユーザー権限が付与されます。たとえば、「Admin」ユーザー・グループに属するすべてのユーザーは、Data Protector Admin ユーザー・グループの権限を持っています。

HP-UX または Solaris プラットフォームの Cell Manager 上で実行中の Data Protector セルで Windows のユーザーを構成する場合、ドメイン名またはワイルドカード・グループ "*" を使って構成する必要があります。

以下に Data Protector ユーザー権限を示します。

[クライアントの構成] ユーザーに、クライアント・システム上への Data Protector ソフトウェアのインストールおよびアップデートを許可します。

[ユーザーの構成] ユーザーに、ユーザーとユーザー・グループの追加、削除、変更を許可します。これは強力な権限であることに注意してください。

[デバイスの構成] ユーザーに、デバイスの作成、削除、変更、名称変更を許可します。論理デバイスへのマウント要求スクリプトの追加も許可されます。

[メディアの構成] ユーザーに、メディア・プールとプール内のメディアの管理や、ライブラリ内のメディアの操作 (メディアの挿入や取出し) を許可します。

[レポートと通知] ユーザーに、Data Protector レポートの作成を許可します。Web レポート機能を使用するには、Admin ユーザー・グループのアプレット・ドメインに Java ユーザーの権限も必要です。

[バックアップ開始] ユーザーに、自分のデータのバックアップ、および自分のセッションのモニターと中止を許可します。

[バックアップ仕様を開始]
ユーザーにバックアップ仕様を使ったバックアップの実行を許可して、バックアップ仕様にリストされている任意のオブジェクトのバックアップ、および既存のバックアップを変更できるようにします。

[バックアップ仕様を保存]
ユーザーに、バックアップ仕様の作成、スケジュール設定、変更、保存を許可します。

[ルート・ユーザーとしてバックアップ]
ユーザーに、UNIX クライアント上で root ユーザーの権限を使用して任意のオブジェクトをバックアップすることを許可します。このユーザー権限は UNIX クライアントに対してのみ有効です。この権限は Novell NetWare クライアント上でバックアップを実行する際に必要です。

[セッションの所有権を切り替え]
ユーザーに、バックアップ仕様のオーナーの指定を許可します。バックアップはこのオーナーの下で開始されます。デフォルトでは、バックアップを開始したユーザーがオーナーとなります。スケジュール設定したバックアップは、UNIX Cell Manager 上では root として、Windows システム上では Cell Manager アカウントで開始されます。このユーザー権限は [バックアップ仕様を開始] が有効な場合に適用されます。詳細は、「所有権 : 誰が復元を実行できるか」（300 ページ) を参照してください。

モニター
ユーザーに、セル内のすべてのアクティブなセッションに関する情報の表示を許可します。また IDB にアクセスして過去のセッションを表示する許可も与えます。

[中止] ユーザーに、セル内のすべてのアクティブなセッションの中止を許可します。

[マウント要求] ユーザーに、セル内のすべてのアクティブなセッションのマウント要求に応答することを許可します。

[復元の開始] ユーザーに、自分のデータの復元、および自分の復元セッションのモニターと中止を許可します。このユーザー権限を持つユーザーは、Cell Manager 上に自分のオブジェクトとパブリック・オブジェクトを表示できます。

[別のクライアントへ復元] オブジェクトがバックアップされたシステム以外のシステムへオブジェクトを復元することを許可します。

[別のユーザーから復元] ユーザーに、別のユーザーが所有するオブジェクトの復元を許可します。これは UNIX クライアントに対してのみ有効です。

[ルートユーザーで復元] ユーザーに、UNIX の root ユーザー権限を使用したオブジェクトの復元を許可します。これは強力なユーザー権限で、システムのセキュリティに影響を与える可能性があることに注意してください。この権限は Novell NetWare クライアント上で復元を実行する際に必要です。

[プライベート・オブジェクトを表示] ユーザーに、プライベート・オブジェクトとしてバックアップされたオブジェクトの表示と復元を許可します。

定義済みの Data Protector ユーザー・グループ

デフォルトのユーザー・グループ （Admin、Operator、User）を以下に示します。

ユーザー権限	Admin	Operator	User
[クライアントの構成]	有		
[ユーザーの構成]	有		
[デバイスの構成]	有		
[メディアの構成]	有	有	
[レポートと通知]	有		
[バックアップ開始]	有	有	
[バックアップ仕様を開始]	有	有	
[バックアップ仕様を保存]	有		
[ルート・ユーザーとしてバックアップ]	有		
[セッションの所有権を切り 替え]	有	有	
モニター	有	有	
[中止]	有	有	
[マウント要求]	有	有	
[復元の開始]	有	有	有
[別のクライアントへ復元]	有		
[別のユーザーから復元]	有	有	
[ルートユーザーで復元]	有		
[プライベート・オブジェクトを表示]	有	有	

ヒント

各ユーザー・グループの正確なユーザー権限を確認するには、グループを選択して、右クリックしてメニューを開き、［プロパティ］を選択します。

Cell Manager で設定したユーザー権限により、Data Protector Cell Manager GUI や、Cell Manager に接続しているコンピュータの GUI コンテキストが使用できるかどうかが決まります。たとえば、ユーザー権限として [復元の開始] だけが設定されている場合は、ユーザー・インタフェース・コンポーネントをインストールした際に使用できるコンテキストは [復元] だけになります。

重要

Data Protector ユーザーの構成は、セル全体のセキュリティに重大な影響を及ぼします。セキュリティに関する考慮事項については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

インストール直後は、Admin グループを除いてデフォルトのユーザー・グループにはユーザーが全く指定されていません。Data Protector は、Admin グループに以下のユーザーを追加します。

- `root:sys` (HP-UX または Solaris の場合)
- インストール時に入力した Cell Manager アカウント（Windows の場合）
- `java` ユーザー (Web レポートを使用可能にするユーザー)

1 つの環境内でユーザーを種類別に特定するグループを定義して、それぞれに最小限必要な権限を割り当てるようお勧めします。

重要

Admin の権限は非常に強力です。Data Protector の Admin ユーザー・グループのユーザーは、セル全体に対してシステム管理者としての権限を持ちます。

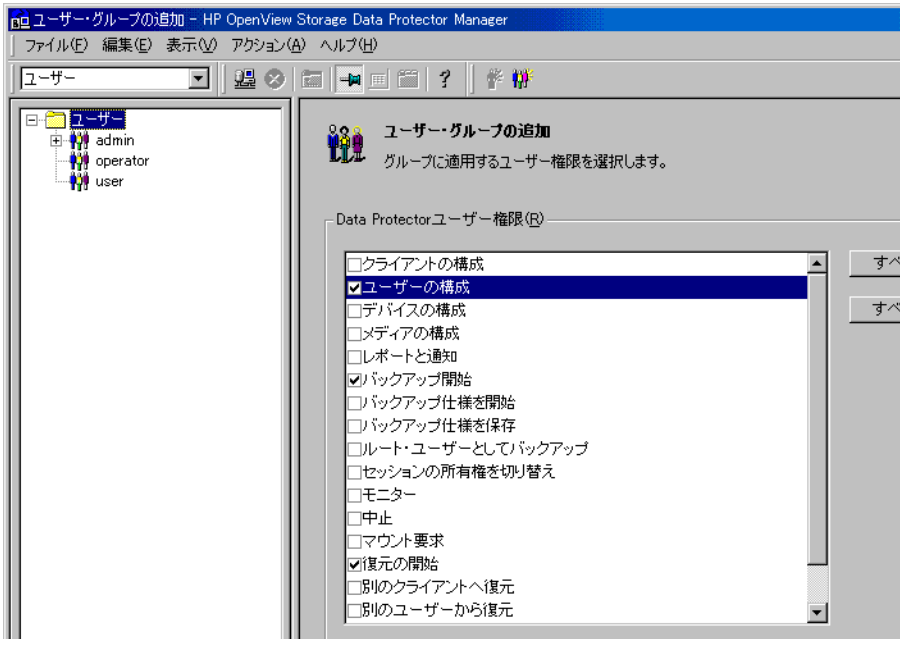
ユーザー・グループの追加または削除

デフォルトの Data Protector ユーザー・グループでほとんどの要件は満たしています。しかし、セキュリティ上の理由から、1 つの環境内でユーザーを種類別に特定するグループを定義して、それぞれに最小限必要な権限を割り当てるようお勧めします。セキュリティに関する考慮事項については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

ユーザー・グループの追加

1. ［Data Protector Manager］で［ユーザー］コンテキストを選択します。
2. Scoping ペインで［ユーザー］を右クリックして、［ユーザー・グループの追加］をクリックします。［ユーザー・グループの追加］ウィザードが表示されます。
3. ウィザードの指示に従って操作を行います。詳細は、[F1] キーを押してください。

図 4-1 新規ユーザー・グループの追加



ユーザー・グループの削除

1. ［Data Protector Manager］で［ユーザー］コンテキストを選択します。
2. Scoping ペインで、［ユーザー］を展開して、ユーザー・グループを表示します。
3. 削除するユーザー・グループを右クリックして［削除］をクリックします。
4. 操作を確認します。

ユーザーの追加または削除

製品のインストール後、以下のユーザーが Admin ユーザー・グループに構成されます。

- UNIX の root ユーザー (UNIX システムの場合)
- Windows の administrator ユーザー（Windows の場合）
- インストールを実行したユーザー

新規ユーザーを Data Protector のユーザー・グループに追加すると、ユーザーにそのグループの権限が付与されます。ユーザー権限の詳細については、「Data Protector ユーザー権限」（137 ページ) を参照してください。

注記

クライアント・システムで Data Protector GUI の使用を開始する前に、そのシステムのユーザーを Cell Manager 上の対応する Data Protector ユーザー・グループに追加してください。

UNIX または Windows のどちらの環境でもユーザーを構成できます。

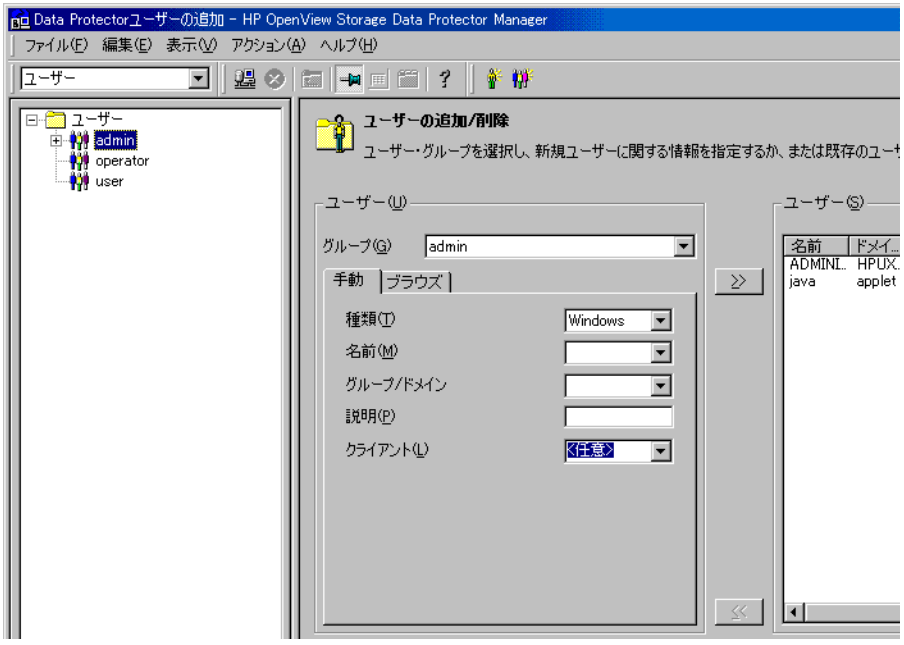
UNIX ユーザーは、ログイン名、UNIX のユーザー・グループ、およびログオンに使用されるシステムによって定義します。ワイルドカード (*) を使用できます。

Windows ユーザーは、ログオン名、Windows のユーザー・グループ (ドメイン)、およびログオンに使用されるシステムによって定義します。ワイルドカード (*) を使用できます。

以下の手順に従って、ユーザーを追加します。

1. ［Data Protector Manager］で［ユーザー］コンテキストを選択します。
2. Scoping ペインで［ユーザー］を展開します。
3. ユーザーを追加したいグループ、またはユーザーを削除したいグループを右クリックした後、［ユーザーの追加 / 削除］をクリックしてウィザードを起動します。

図 4-2　新規ユーザーの追加



詳細は、[F1] キーを押してください。

ユーザーの変更

既存ユーザーのプロパティを変更したり、ユーザーをグループ間で移動できます。

注記

個々のユーザーについてユーザー権限を変更することはできませんが、ユーザー・グループ全体の権限であれば変更できます。

ユーザーのプロパティの変更

ユーザーのプロパティを変更するには、以下の手順を行います。

1. ［Data Protector Manager］で［ユーザー］コンテキストを選択します。
2. Scoping ペインで［ユーザー］を展開して、目的のユーザーが所属するグループをクリックします。
3. 目的のユーザーを右クリックした後、［プロパティ］をクリックしてユーザーのプロパティを表示します。

   詳細は、[F1] キーを押してください。

ユーザーの別のユーザー・グループへの移動

個々のユーザーのユーザー権限を変更するには、ユーザーを別のユーザー・グループに移動します。

1. ［Data Protector Manager］で［ユーザー］コンテキストを選択します。
2. Scoping ペインで［ユーザー］を展開して、目的のユーザーが所属するグループをクリックします。
3. 結果エリアでユーザーをクリックして［移動］をクリックします。

   詳細は、［ヘルプ ］をクリックしてください。

ユーザー・グループの権限の変更

ユーザーは、所属しているユーザー・グループの権限を持っています。したがって、ユーザー・グループのユーザー権限を変更すると、そのグループに属するすべてのユーザーの権限が変更されます。ユーザー・グループの権限は変更可能です。ユーザー・グループの権限を変更すると、そのグループに属する各ユーザーの権限が変更されます。ただし、Admin ユーザー・グループの権限は変更できません。

注記

グループ内の各ユーザーのプロパティを変更することもできます。たとえば、ユーザーが所属するドメイン、ユーザーの実名、ユーザーが所属するユーザー・グループなどです。

ユーザー・グループの権限、つまりグループ内の各ユーザーの権限の変更方法を以下に示します。

1. ［Data Protector Manager］で［ユーザー］コンテキストを選択します。
2. 権限を変更するユーザー・グループをブラウズして選択します。

注記

ユーザーが所属していないグループを選択すると、このグループのプロパティが結果エリアに表示されます。また、すでにユーザーが所属しているグループを選択すると、グループに属するユーザーのリストが結果エリアに表示されます。また、ユーザー・グループ内の各ユーザーのプロパティも変更できます。この場合は、プロパティを変更したいユーザーをクリックします。

3. 選択したユーザー・グループを右クリックして［プロパティ］をクリックします。ユーザー・グループのプロパティが結果エリアに表示されます。
4. ［ユーザー権限］タブをクリックして、このグループに対して設定可能な権限のリストを表示します。

   詳細は、[F1] キーを押してください。

ユーザー構成の例

本項では、代表的なユーザー構成の例を説明します。

ユーザーが自分のファイルを復元できるようにする

この復元ポリシーでは、すべてのユーザーまたは選択されたユーザーが自分のデータを復元できます。これによって十分なセキュリティが確保され、バックアップ・オペレータが頻繁に復元を行う必要がなくなります。

どのような場合にこのポリシーを使用するか

- ユーザーが復元処理に関する十分な知識を持っている場合。基本的なバックアップの概念と復元操作について、何らかの方法でユーザーをトレーニング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いて、最新のバックアップのメディアが全部そのデバイスにある場合。デフォルトでは、Data Protector の User グループのユーザーには必要なメディアのマウント要求の処理は許可されていません。マウント要求が発行された場合、ユーザーはバックアップ・オペレータを通じてマウント要求に応答しなければなりません。

必要な準備作業

1. Data Protector の `users` ユーザー・グループにユーザーを追加して、自分のデータを復元する許可を与えます。セキュリティを強化するには、ユーザーが Data Protector へアクセスする際に使用できるシステムを限定します。
2. ユーザーが使用しているシステムに Data Protector ユーザー・インタフェースをインストールします。Data Protector は自動的にユーザー権限をチェックし、復元機能だけを許可します。
3. ユーザーのシステムのバックアップを構成する際に、バックアップをパブリックに設定してユーザー側で表示できるようにします。

ユーザーが自分のシステムをバックアップできるよう設定する

Data Protector は、バックアップを構成するユーザー権限とすでに構成を完了したバックアップを実行するユーザー権限を区別します。

ユーザーが自分のシステムのバックアップを実行する権限を作成するには、以下の手順を行います。

1. 新規ユーザー・グループを作成するか、または既存のグループを変更して、[バックアップ開始] のユーザー権限を与えます。
2. ユーザーをこのユーザー・グループに追加して、自分のバックアップを構成する許可を与えます。
3. バックアップ構成のオーナーを変更して、ユーザーがバックアップを開始できるようにします。図 4-1 (143 ページ) を参照してください。

5 メディアの管理

本章の概略

本章では、メディアの管理方法に関する以下の情報について詳しく説明します。

Data Protector におけるメディア管理の概要

Data Protector には、大量のメディアを容易に効率よく管理するために、次のような機能があります。

注記

Data Protector は、メディアへのデータ書き込み時に、さまざまな種類のメディア・フォーマットを認識 / 使用します。制限事項については、「異なる種類のメディア・フォーマットの使用」(205 ページ) を参照してください。

- 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 は、データ保護期限切れ期日、バックアップ用メディアの有無、各メディアにバックアップされている内容など、全メディアと各メディアのステータスを常にトラッキングしています。
- すべての操作は完全に自動化されています。ライブラリ・デバイス内に Data Protector が管理しているメディアが十分にあれば、メディア管理機能によってバックアップが自動的に行われるので、手作業によるメディアの交換などは必要ありません。
- メディアのローテーションはポリシーに従って自動的に行われるので、ユーザーによる操作は必要ありません。
- 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。
- スタンドアロン、マガジン、ライブラリ・デバイス、サイロ・デバイスなど、各デバイスに最も適した方法でメディアが管理されます。
- Data Protector メディアおよびその他の代表的なテープ・フォーマットの自動認識が可能です。
- バーコードをサポートしている大規模ライブラリおよびサイロ・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。
- ライブラリやサイロなどの大容量デバイスに保管され、Data Protector が使用するメディアを認識し、状態をトラッキングして内容を表示できます。

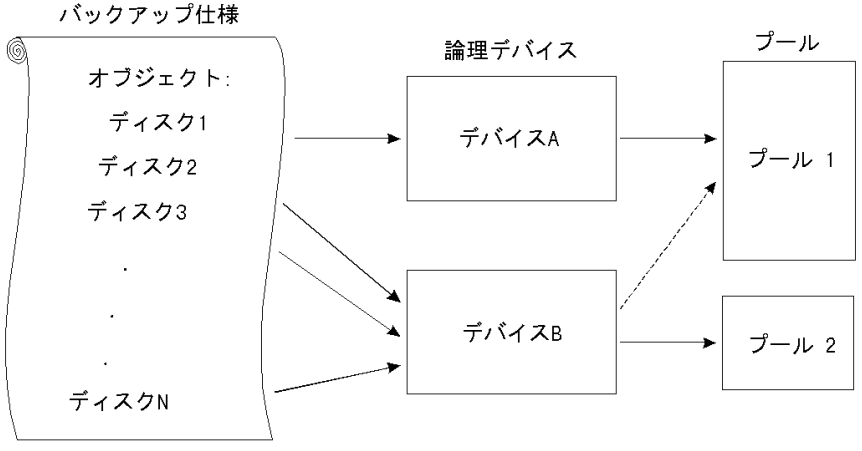
- メディアに関する情報を中央に保管し、複数の Data Protector セルとの間でその情報を共有できます。
- **メディアのボールティング (アーカイビング、オフサイトのストレージ)** に対応しています。
- メディア上に保存されているデータの追加コピーを、自動的にまたは対話形式で作成できます。

使用メディアの情報は、IDB に保管されます。

メディア管理の詳細については、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

図 5-1 に、コンポーネント、バックアップ仕様、デバイス、メディア・プールの相互関係を示します。プールはバックアップ・セッション中に使用されます。デフォルトのプールはデバイス定義に含まれていますが、バックアップ仕様で別のプールを指定できます。

図 5-1　メディア・プールと他のコンポーネントとの関係



メディアのライフ・サイクル

一般にメディアのライフ・サイクルは、以下のステップで構成されています。

1. バックアップ用のメディアを準備します。この作業には、Data Protector で使用するメディアのフォーマットとメディアのメディア・プールへの割り当てが含まれます。メディア・プールは、これらのメディアをトラッキングするために用いられます。準備作業の詳細は、以下の各項を参照してください。

   「メディア・プールの作成」(157 ページ).

   「メディア・プールへのメディアの追加」(162 ページ).

2. メディアへのバックアップを行います。この作業には、バックアップに使用するメディアの選択、メディア状態要素のチェック (上書き回数など)、メディアへの新規バックアップの追加、メディアへのデータの上書きが含まれます。
3. メディアを安全な場所にボールティングします。

   Data Protector が提供するいずれかの複製方法を使用すると、バックアップ・データのボールティング用コピーを作成できます。
4. 保存されているデータが必要なくなったら、そのメディアをリサイクルします。リサイクルされたメディアは再使用できるようになります。
5. メディアには、使用期限があります。期限 (最大使用基準) が終了したメディアには、「不良」というマークが付き、Data Protector ではそれ以上使用されません。詳しくは、「メディアの状態に影響する要素」(191 ページ) を参照してください。

以下の各項では、これらの作業の内容について詳しく説明します。

メディア・プールの作成

メディア・プールとは

メディア・プールとは、バックアップに使用する同じ種類のメディア (DLT など) の内、同じ使用ポリシーとプロパティを持つものの集まりを指します。たとえば、定期バックアップ用のメディア・プール、アーカイビング用のメディア・プール、各部門ごとのメディア・プールなど、目的に応じて複数のメディア・プールを作成できます。

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) のソースとして補助的に使用できるプールで、通常のプール内のフリー・メディアがすべて使用できない場合に使われます。これによって、メディアが使用できないことによるバックアップの失敗を回避できます。

通常のプールとフリー・プールの間でメディアが移動されるのは、以下のどちらかの場合です。

- 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動されます。
- 割り当て解除時。メディアは通常のプールからフリー・プールに移動されます。GUI で、割り当て解除を自動的に行うかどうかを指定できます。

保護メディア (割り当て済み、使用中) は、特定の通常のプール (SAP プールなど) に所属していますが、Data Protector のフリー・メディアは、自動的にフリー・プールに移動させることができます。このフリー・プールは、後でバックアップを行う際に、必要に応じてフリー・メディアを特定の通常のプールに割り当てるのに使用されます。

メディア・プールの詳細は、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

デフォルトのメディア・プール

Data Protector には、メディアの種類ごとにデフォルトのメディア・プール (Default_DDS など) があり、Data Protector を最初に構成する際にこれらのデフォルトをそのまま使用することができます。

メディア・プールを作成せずにデフォルトのメディア・プールを使用する場合は、「メディア・プールへのメディアの追加」(162 ページ) へ進んでください。

メディア・プールの作成方法

新しいメディア・プールの作成は、[デバイス / メディア] コンテキストで [メディア・プールの追加] ウィザードを使って行います。詳しい手順については、オンライン・ヘルプの索引キーワード「メディア・プールの追加」を参照してください。

次に行う手順

次のステップでは、バックアップに使用するメディアをメディア・プールへ追加します。手順については、「メディア・プールへのメディアの追加」(162 ページ) を参照してください。

メディア・プールのプロパティ

本項では、メディア・プールのプロパティについて説明します。プロパティは、メディア・プールを構成する際に指定します。ただしプロパティの中には、後で設定を変更できるものもあります。

[プール名]

メディア・プールを識別するための名前です。スペースを含む半角 32 文字までの名前を指定できます。他のメディア・プールと区別しやすいように、部署名などメディア・プールの内容を端的に示す名前を付けるとよいでしょう。

[説明]

メディア・プールを識別しやすくするためのものであり、必ずしも入力する必要はありません。任意の文字を半角 80 文字分まで説明として入力できます。

[メディアの種類]

構成に応じて使用できるメディアの種類のリストが表示されます。

サポートされているメディアの種類に関する最新のリストは、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』の「サポート一覧」を参照してください。

メディアの種類を選択すると、選択したメディア上でメディア・プールに使用できるスペースを Data Protector が計算します。計算は選択されたメディアの種類に基づいて行われます。

[メディア割り当てポリシー]

メディア割り当てポリシーは、メディアの摩耗状態が均等になるように、メディア・プール内でのメディアのアクセス順序を決定するものです。

Data Protector でのバックアップ用の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」(176 ページ) を参照してください。

[Strict] 特定のメディアを要求するよう Data Protector に指示します。メディアはフォーマット済みであることが必要です。このポリシーを使用する場合、Data Protector はメディアをフォーマットしません。ライブラリ内やメディアの使用状況ポリシーが優先される場合でも、非 Data Protector メディアを誤って上書きすることを避けるために、ライブラリ・デバイスにはこの割り当てポリシーを使用することをお勧めします。

[Loose] プール内にある、**「不良」**なメディア、または保護されたメディア以外の適切なメディアならどれでも受け入れるよう Data Protector に指示します。このオプションは、[フォーマットされていないメディアを先に割り当てる] オプションと併用します。

`InitOnLoosePolicy` が 1 に設定されている場合 (デフォルトでは 0)、Data Protector が認識できないメディア (新しいメディア) は自動的にフォーマットされます。このポリシーは、Data Protector が選択できるメディアの数を最大にするため、無人バックアップを実行する場合に適しています。

[フォーマットされていないメディアを先に割り当てる]

`[Loose]` ポリシーを一部変更したオプションです。このポリシーを選択すると、ライブラリ内に使用可能な保護されていない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。Data Protector がライブラリを使用する唯一のアプリケーションで、すべてのメディアを均等に使用したい場合は、このポリシーの使用をお勧めします。

[フリー・プールを使用]

通常のプールに加え、フリー・プール内の使用可能なメディアも検索するよう Data Protector に指示します。このオプションは、デフォルトではオフになっています。

詳細は、「バックアップ用メディアの選択」(176 ページ) を参照してください。

フリー・プールの詳細は、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

[メディア使用法ポリシー] メディア使用法ポリシーは、前回のバックアップに使用したメディアに新しいバックアップを追加するかどうかを決定します。

[追加可能] バックアップ・セッションは、前回のバックアップ・セッションで使用した最後のメディアに残っているスペースにデータを書き込みます。バックアップ・セッションで必要な後続のテープについては、テープの先頭からデータが書き込まれるので、書き込み保護されていないテープまたは新しいテープしか使用できません。データは任意のバックアップ仕様からその他のバックアップ仕様に追加できます。メディアを追加するとスペースを節約できますが、1 つのメディアに複数のバックアップ・セッションからのデータが保存される可能性があるため、復元時の操作が複雑になります。

[追加不可能] バックアップ・セッションは、バックアップに使用可能な先頭のメディアの先頭からデータを書き込みます。

[増分のみ追加可能] 増分バックアップを行う場合にのみ、バックアップ・セッションで最初に使用されたメディアにデータが追加されます。プール内に追加可能なメディアが複数ある場合は、書き込みが一番旧いメディアが最初に使用されます。同じバックアップ・セッション中に、さらにメディアが必要になった場合は、保護されたバックアップを含まない空のメディアを使用する必要があります。このメディア使用法ポリシーを使用すると、1 つのフル・バックアップといくつかの増分バックアップを含むメディアが生成されます。

注記

追加機能を使用する場合で、バックアップに複数のメディアが必要な場合、前回のセッションのバックアップ・データを含めることができるのは、最初に使用するメディアだけです。その後、Data Protector は空のメディアまたは保護されていないメディアのみを使用します。

詳細は、「メディアへのバックアップの追加」(173 ページ) および「バックアップ用メディアの選択」(176 ページ) を参照してください。

[マガジンのサポート] [マガジンのサポート] を指定すると、マガジンとして構成されているメディアを使用できます。ただしこれらのメディアと使用するバックアップ・デバイスは、HP 12000e などマガジンをサポートしているものに限られます。

このオプションは、新しくメディア・プールを構成するときに使用します。

詳細は、以下の各項を参照してください。

- マガジン・デバイスの構成方法については、「マガジン・デバイスの構成」(31 ページ) を参照してください。
- マガジン全体、またはマガジン内の単一メディアをフォーマットする方法については、「メディアのフォーマット」(164 ページ) を参照してください。
- マガジン全体、または単一メディアのインポート方法については、「メディアのインポート」(169 ページ) を参照してください。

[メディア状態要素] [メディア状態要素] は、メディアの状態を定義することにより、そのメディアのバックアップ用メディアとしての信頼性を決定します。プールがフリー・プール・オプションを使用する場合、フリー・プールのメディア状態要素が継承されます。Data Protector は**メディア状態要素**をもとに使用中のメディアの状態を算出します。メディア状態要素には 2 つの選択項目があります。

メディアの有効期限
このオプションを選択すると、メディアの使用時間を基準として状態が判定されます。ここで、使用時間とは、メディアをフォーマットした時点から経過した月数を意味します。しきい値である月数より旧くなると、「不良」なメディアとして判断されます。デフォルトのしきい値は 36 か月です。

最大上書き数
メディアの使用状況は、そのメディアの先頭から上書きされた回数として定義されます。しきい値である上書き回数を超えると、「不良」なメディアとして判断されます。デフォルトのしきい値は 250 回です (ただし、DDS テープの場合は 100 回)。

メディア状態要素の計算方法については、「メディア状態算出法の変更」(192 ページ) を参照してください。

メディア・プールへのメディアの追加

メディア・プールを作成したら、バックアップに使用するメディアをそのメディア・プールに追加します。

未使用メディアの追加方法

未使用メディアをメディア・プールに追加する場合は、「メディアのフォーマット」(164 ページ) を参照してください。メディア・プールに設定しているメディア割当てポリシーが [Loose] の場合は、別途メディアをフォーマットする必要はありません。InitOnLoosePolicy が 1 に設定されている場合 (デフォルトでは 0)、メディアはバックアップ・セッションで使用される前にフォーマットされます。詳しくは、「[メディア使用法 ポリシー]」(159 ページ) を参照してください。

使用済みメディアの追加方法

すでに使用されている Data Protector メディアを上書きせずにメディア・プールにインポートする場合は、「メディアのインポート」(169 ページ) を参照してください。

すでに使用されている非 Data Protector メディアをメディア・プールに追加する場合は、再フォーマットする必要があります。「メディアのフォーマット」(164 ページ) を参照してください。

他のアプリケーションで使用したメディアの取り扱いについては、「他のデータ・フォーマットの認識」(167 ページ) を参照してください。

メディア・ラベルの付与

Data Protector は、使用する各メディアに対して一意のメディア・ラベルとメディア ID を付与します。メディア・ラベルとメディア ID は IDB に保管され、メディアの管理に使用されます。メディア ID は Data Protector によって割り当てられます。メディア・ラベルとは、ユーザーが定義する説明とメディアのバーコードを組み合わせたものです (メディアにバーコードが付与されており、[バーコード・リーダーのサポート] オプションが有効に設定されている場合)。バーコードはメディアの説明の接頭辞として表示されます。たとえば、メディア・ラベル [CW8279]Default DLT_1 は、説明が Default DLT_1 でバーコードが CW8279 のメディアを示します。メディアの初期化中に、必要に応じてバーコードをメディア・ラベルとしてテープ上のメディア・ヘッダに書き込むこともできます。

Data Protector GUI では、メディア・ラベルごとにメディアを分類できます。結果エリアの [メディア・ラベル] フィールドをクリックして実行します。

次に行う手順

メディア・プールへのメディアの追加が完了したら、バックアップするデータを選択できます。詳しい手順については、第 6 章「バックアップ」(207 ページ) を参照してください。

メディアのフォーマット

メディアのフォーマットとは

メディアのフォーマットとは、メディアに関する情報 (メディア ID、説明、位置) を IDB に保存し、メディア自体 (ヘッダ) にも書き込むことによって、そのメディアを Data Protector で使用できる状態にすることです。メディアをフォーマットするときに、そのメディアが所属するメディア・プールも指定します。

フォーマットのタイミング

メディアは、バックアップに使用する前にフォーマットすることが必要です。バックアップの前にメディアをフォーマットせず、メディア・プールのメディア割当てポリシーが [Loose] に設定されていて、グローバル変数 InitOnLoosePolicy が 1 に設定されている場合 (デフォルトは 0) は、そのメディアをバックアップに使用すると、Data Protector は自動的にメディアをフォーマットします。その場合、メディア・ラベルはデフォルトの値になります。ただし、ライブラリのプロパティで [初期化時にメディア・ラベルとしてバーコードを使用] が選択されている場合は、バーコードが書き込まれます。

非 Data Protector メディアは、バックアップの前にフォーマットすることが必要です。

Data Protector 以外のフォーマットの認識

Data Protector はメディアがすでに使用中の場合、共通のメディア・フォーマットを認識します。詳細は、「他のデータ・フォーマットの認識」(167 ページ) を参照してください。

埋め込みブロックを使用したフォーマット

メディアのヘッダ・サイズを拡張して圧縮できないデータ (埋め込みブロック) を埋め込むことができます。これはメディアのコピーを作成する時に有効です。埋め込みブロックはターゲット・メディアにはコピーされません。このため、ターゲット・メディアがソース・メディアよりも先にテープの終わりに到達するのを防ぎます。

オブジェクトコピー機能を使用してバックアップ・データをコピーする場合、データを埋め込む必要はありません。

テープへの埋め込み機能は、デフォルトでは無効になっています。有効にするには、バックアップ・デバイスが接続されているシステム上の omnirc ファイルの OB2BLKPADDING_n 変数を設定してください。詳細は、「omnirc オプションの使用」(647 ページ) を参照してください。

メディアのフォーマット方法

メディアをフォーマットするには、対象のデバイス、メディア・プールまたはライブラリ・スロットを [デバイス / メディア] コンテキストでブラウズして右クリックし、[フォーマット] をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「メディアのフォーマット」を参照してください。

ライブラリ・デバイスを使用する場合は、[Ctrl] キーを使って複数のスロットを選択し、複数のメディアを同時にフォーマットできます。メディアの初期化中に、必要に応じてバーコードをメディア・ラベルとして使用してメディア・ヘッダに書き込むこともできます。詳しい手順については、オンライン・ヘルプの索引キーワード「フォーマット - ライブラリ・デバイス内のメディア」を参照してください。

ヒント

Data Protector 以外のアプリケーションが使用するメディアをフォーマットする場合は、[強制] オプションを使用します。ただし、Data Protector により保護されているメディアについては、このオプションを使用しても再フォーマットされません。この場合は、先に保護を解除する必要があります。詳しくは、「メディアのリサイクル」(180 ページ) を参照してください。

注記

[メディアのサイズ] オプションを選択する場合は、[デフォルト] または [指定 (MB)] を選択します。[デフォルト] を選択した場合、実際のメディア・サイズではなく、Data Protector によって予測されたメディア・サイズが表示されます。メディア全体のサイズは、メディアが圧縮されていないことを前提に設定されます。デバイスがハードウェア圧縮されていると、メディア上のスペースが倍になる場合があります。実際のメディア・サイズはメディアがいっぱいになった時点で表示されます。

次に行う手順

メディアのフォーマットが完了したら、メディアを使用してバックアップを実行できます。バックアップの構成方法については、第 6 章「バックアップ」(207 ページ) を参照してください。

マガジン内のメディアのフォーマット

マガジンをサポートしているデバイスを使用する場合は、マガジン内のすべてのメディアまたは単一メディアをフォーマットできます。

マガジン全体のフォーマット方法

マガジン全体をフォーマットするには、デバイスに使用しているメディア・プールをブラウズして右クリックし、[マガジンのフォーマット] をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「マガジン内のメディアのフォーマット」を参照してください。

マガジン内の単一メディアのフォーマット方法

マガジン内の単一メディアをフォーマットするには、デバイスに使用しているメディア・プールをブラウズして右クリックし、[フォーマット] をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「マガジン内の単一メディアのフォーマット」を参照してください。

ヒント

Data Protector 以外のアプリケーションが使用するメディアをフォーマットする場合は、[強制] オプションを使用します。ただし、Data Protector により保護されているメディアについては、このオプションを使用しても再フォーマットされません。この場合は、先に保護を解除する必要があります。詳しくは、「メディアのリサイクル」(180 ページ) を参照してください。

次に行う手順

メディアのフォーマットが完了したら、メディアを使用してバックアップを実行できます。バックアップの構成方法については、第 6 章「バックアップ」(207 ページ) を参照してください。

他のデータ・フォーマットの認識

フォーマットの認識

すでにメディアに書き込まれているデータが誤って上書きされないように、Data Protector はさまざまなテープ・フォーマットを認識します。

表 5-1 Data Protector メディア・フォーマットのカテゴリ

メディア・フォーマット	Data Protector の動作
不明または新規	[Loose] ポリシー : グローバル変数 InitOnLoosePolicy が 1 に設定されている場合、フォーマットされてバックアップに使用されます。 [Strict] ポリシー : バックアップには使用されません。
メディアは圧縮オプションを使って書き込まれ、現在は圧縮オプションを使用していない	
メディアは圧縮オプションを使わずに書き込まれ、現在は圧縮オプションを使用	
Data Protector 以外 (別のセルのメディア)	インポートされるか [強制] オプションを使用してフォーマットされない限り、バックアップには使用されません。
tar、cpio、OmniStorage、OmniBack I 、ANSI ラベル、ファイルシステム	[強制] オプションを使用してフォーマットされない限り、バックアップには使用されません。
Data Protector で保護されていないメディア	バックアップに使用されます。
Data Protector で保護されているメディア	バックアップの追加に使用されます。

注記

メディア・タイプの識別は使用されるプラットフォームに依存するため、Data Protector のみを使用してその他のメディア・タイプを識別しないようにしてください。

注記

ハードウェア圧縮機能を使って書き込まれたメディアから、ハードウェア圧縮機能をサポートしていないデバイスを使ってデータを読み込もうとした場合、Data Protector はメディアを認識せず、データを読み込むことはできません。このため、このメディアは不明または新規として処理されます。

メディアのインポート

メディアのインポートにより、Data Protector がすでに使用していたメディアがメディア・プールに追加されますが、このときメディア上のデータが失われることはありません。Data Protector が使用していたメディアは Data Protector によってフォーマットされており、Data Protector セルからエクスポートされたメディアです。

メディアをインポートすると、メディア上のバックアップ・データに関する詳細情報が IDB に書き込まれます。したがって復元時に、データベースに記録された情報をブラウズできます。

Data Protector セル間でメディアを移動する際にメディアのインポートを使用します。

フリー・プール内のメディアではこの操作を実行できません。

注記

オブジェクトやメディアのサイズなどの属性情報は、インポート時に再構築されません。したがって、インポートされたオブジェクトのサイズは 0KB と表示されます。

使用するデバイスやメディアにもよりますが、インポートには非常に長い時間がかかることに注意してください。

重要

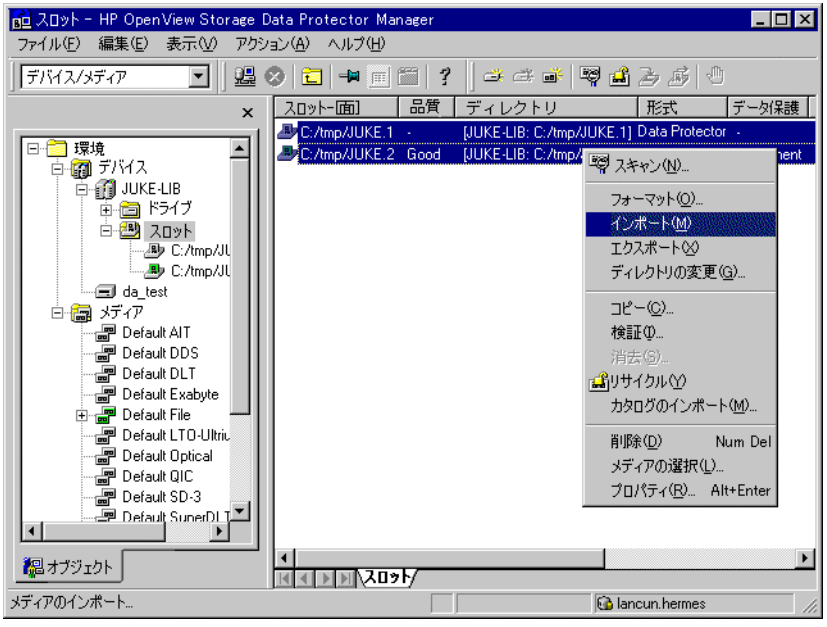
1 回のバックアップ・セッションで使用したメディアは、すべて一度にインポートしてください。一部のメディアだけを読み込んでも、残りのメディアに記録されているバックアップ・データは復元されません。

メディアのインポート方法

メディアをインポートするには、対象のデバイス、メディア・プールまたはライブラリ・スロットを [デバイス / メディア] コンテキストでブラウズして右クリックし、[インポート] をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「メディアのインポート」を参照してください。

ライブラリ・デバイスを使用する場合は、[Ctrl] キーを使って複数のスロットを選択し、複数のメディアを同時にインポートできます。詳細は、図 5-2 を参照してください。詳しい手順については、オンライン・ヘルプの索引キーワード「インポート - ライブラリ・デバイス内のメディア」を参照してください。

図 5-2　　複数のメディアのインポート



メディアからのカタログのインポート

メディアからカタログをインポートすると、ファイル・バージョンに関する詳細情報が IDB に書き込まれ、復元対象のファイルとディレクトリをブラウズできるようになります。

特定のオブジェクトのカタログ保護期限が切れていてファイルやディレクトリをブラウズできない場合は、[カタログのインポート] を使用してカタログをインポートしてください。

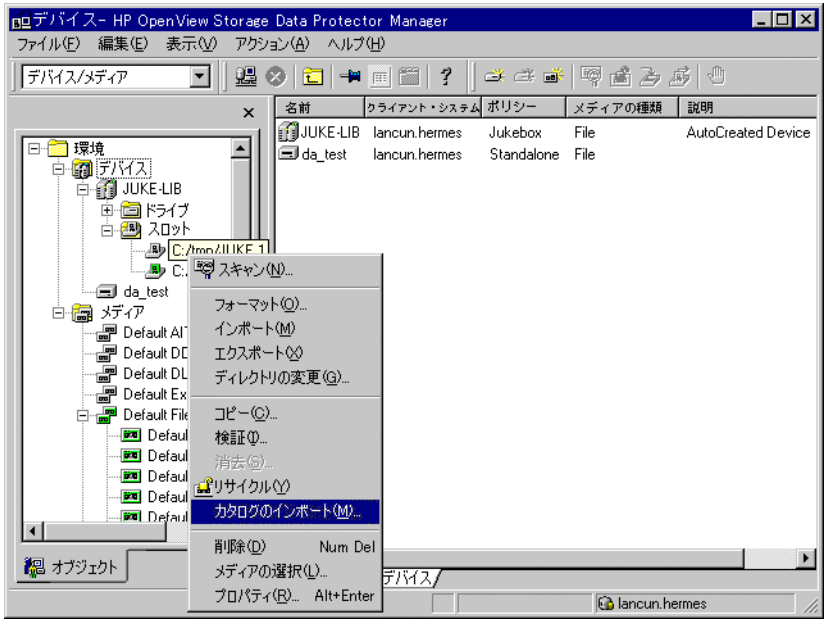
フリー・プール内のメディアではこの操作を実行できません。

メディアからのカタログのインポート方法

メディアからカタログをインポートするには、対象のデバイス、メディア・プールまたはライブラリ・スロットを [デバイス / メディア] コンテキストでブラウズして右クリックし、[カタログのインポート] をクリックします。詳細は、図 5-3 を参照してください。詳しい手順については、オンライン・ヘルプの索引キーワード「メディアからのカタログのインポート」を参照してください。

図 5-3

カタログのインポート



マガジン・デバイス内のメディアのインポート

マガジンをサポートしているデバイスを使用する場合は、すべてのメディアまたは単一メディアをマガジンにインポートできます。

必要条件

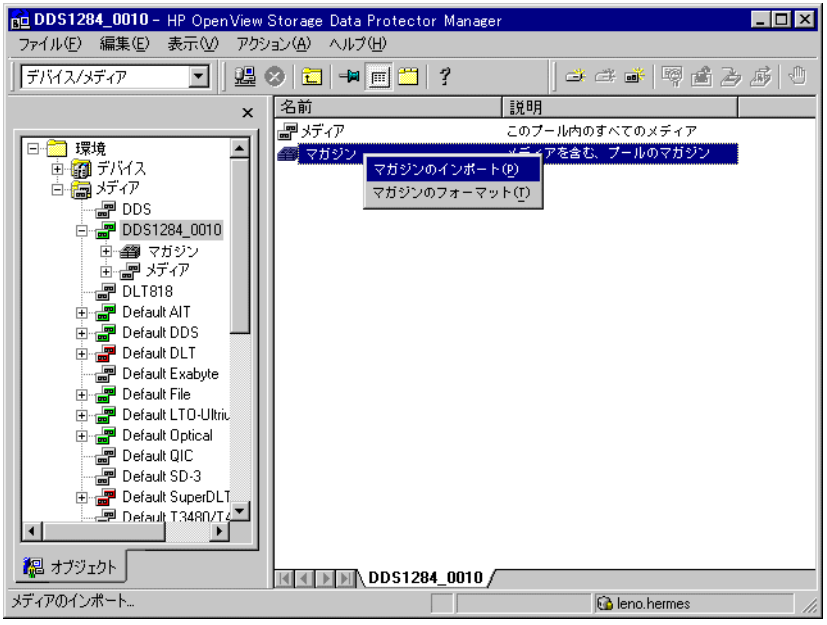
マガジン・デバイスのメディア・プールは必ず、[マガジンのサポート] オプションを使用可能に設定して構成することが必要です。

すべてのメディアをインポートするには

マガジン・デバイス内のすべてのメディアをインポートするには、[デバイス / メディア] コンテキストでそのデバイス用に使用しているメディア・プールを展開し、[マガジン] を右クリックして [マガジンのインポート]

をクリックします。詳細は、図 5-4 を参照してください。詳しい手順については、オンライン・ヘルプの索引キーワード「マガジン内のメディアのインポート」を参照してください。

図 5-4 **マガジンのインポート**



単一メディアのマガジンへのインポート方法

マガジン・デバイスに単一メディアをインポートするには、[デバイス / メディア] コンテキストでそのデバイス用に使用しているメディア・プールを展開し、対象のマガジンを選択して [メディア] を右クリックして [インポート] をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「マガジン内の単一メディアのインポート」を参照してください。

次に行う手順

メディアのインポートが完了したら、メディアを使用してバックアップを実行できます。バックアップの構成方法については、第 6 章「バックアップ」(207 ページ) を参照してください。

メディアへのバックアップの追加

Data Protector では、すでにバックアップが保存されているメディアに対して新しいバックアップを追加できます。この方法を使用するとメディアのスペースを節約できます。

制限事項

Travan デバイス内で使用しているメディアにはバックアップを追加できません。

[追加可能] メディア使用法ポリシーは、メディア・プールの構成時に選択できます。追加可能なメディアには現在保護中のオブジェクトが含まれており、メディア状態が良好であることと、メディアがいっぱいでないことが必要です。

複数のデバイスを使って負荷調整を行う場合は、[追加可能] ポリシーはデバイスごとに適用されます。つまり、それぞれのデバイスが追加可能メディア (使用可能な場合) をバックアップ・セッションの最初のメディアとして使用します。ひとつのメディアに対して複数のバックアップ・セッションがデータを追加する場合でも、これらのセッションがすべて同じバックアップ仕様を使用する必要はありません。

追加可能メディア使用法ポリシーには、以下の 2 つがあります。

- **[追加可能]:** バックアップ・セッションで最初に使用するメディアとして、以前のバックアップ・セッションで使用したメディアの残りのスペースを使用します。プール内に追加可能なメディアが複数ある場合は、使用時期が最も旧いメディアが最初に使用されます。同じバックアップ・セッション中に、さらにメディアが必要になった場合は、保護されたバックアップを含まない空のメディアを使用する必要があります。このメディア使用法ポリシーを使用すると、メディア上にバックアップの種類 (フル・バックアップまたは増分バックアップ) を任意の順で保存することができます。
- **[増分のみ追加可能]:** 増分バックアップを行う場合にのみ、バックアップ・セッションで最初に使用されたメディアにデータが追加されます。プール内に追加可能なメディアが複数ある場合は、使用時期が最も旧いメディアが最初に使用されます。同じバックアップ・セッション中に、さらにメディアが必要になった場合は、保護されたバックアップを含まない空のメディアを使用する必要があります。このメディア使用法ポリシーを使用すると、1 つのフル・バックアップといくつかの増分バックアップを含むメディアが生成されます。

ヒント

あるクライアントに関するフル・バックアップと増分バックアップだけが保存されたテープを作成したい場合は、Data Protector を以下のように構成します。

- [増分のみ追加可能] メディア使用法ポリシーを設定して、クライアントごとに 1 つのプールを構成する。
- バックアップ仕様内の各クライアントに個別のプールを関連付ける、またはクライアントごとに個別のバックアップ仕様を作成する。

この方法により、復元チェーンを含むメディアが作成されます。場合によっては増分バックアップのみが保存されたメディアが作成されることに注意してください。

[追加可能] など、メディア使用法ポリシーのオプションの説明については、「[メディア使用法 ポリシー]」(159 ページ) を参照してください。

メディア使用法ポリシーがバックアップ用メディアの選択に与える影響については、「バックアップ用メディアの選択」(176 ページ) を参照してください。

設定を変更する場合は、メディア・プールのプロパティをオープンします。

バックアップ用メディアの事前割当てリストの使用

メディア・プール内のメディアをバックアップに使用する順序を指定できます。この順序を指定したものが、事前割当てリストです。事前割当てリストは、バックアップを構成する際に指定します。事前割当てリストの目的は、バックアップ・セッションに使用されるメディアを正確に管理することです。各バックアップの前に、事前割当てリストを使用可能なメディアと一致させる必要があります。

メディアの事前割当ては、オブジェクトコピーの実行時にも使用できます。

メディア・プールの割当てポリシーに応じて、Data Protector の動作は 2 つに分かれます。

- 事前割当てリストを [Strict] メディア割当てポリシーと併用する場合、Data Protector はバックアップデバイス内のメディアが事前割当てリストで指定されている順番で使用可能であるとみなします。メディアが使用できない場合、Data Protector はマウント要求を発行します。事前割当てリストに記載されているメディアを SCSI エクスチェンジャにロードした場合、Data Protector はメディアを指定された順序で自動的に使用します。
- 事前割当てリストを [Loose] メディア割当てポリシーと併用する場合、事前割当てリスト内のメディアが最初に使用されます。このメディアが使用可能でない場合は、ライブラリ内にある適切なメディアのいずれかが使用されます。

バックアップ用メディアの事前割当て

バックアップ用メディアの事前割当て方法については、オンライン・ヘルプの索引キーワード「メディアの事前割当て」を参照してください。

バックアップ用メディアの選択

Data Protector のメディア管理機能では、バックアップに最も適したメディアが自動的に選択されます。本項では、バックアップ用メディアの選択に影響を与えるさまざまな要素について説明します。

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は、**メディア割り当て**ポリシーにより設定できます。たとえばメディア割り当てポリシーを [Loose] に設定すると、プール内の適切なメディアならどれでもバックアップに使用することができますが、[Strict] に設定すると、特定のメディアはあらかじめ決められた順序でしか使用できません。

詳しくは、「[メディア割り当てポリシー]」(158 ページ) を参照してください。

メディアの事前割り当て

メディア・プール内のメディアをバックアップに使用する順序を指定できます。この順序を指定したものが、事前割当てリストです。詳細は、「バックアップ用メディアの事前割当てリストの使用」(175 ページ) を参照してください。

メディアの状態

バックアップ用にどのメディアが選択されるかは、メディアの状態によっても変わります。たとえば、状態が「普通」のメディアよりは、状態が「良好」のメディアが先に選択されます。状態が「不良」のメディアはバックアップには使用されません。

注意

「普通」と表示されているメディアは、そのメディア上に保護が設定されたオブジェクトがない場合に限り使用されます。このようなオブジェクトがある場合は、マウント要求が発行され、バックアップが完了する前にデータが失われる可能性があります。

詳しくは、「メディアの状態に影響する要素」(191 ページ) を参照してください。

メディア使用法ポリシー

バックアップ用のメディアの選択には、メディア使用法ポリシーも関連しています。詳細は、「[メディア使用法 ポリシー]」(159 ページ) および「メディアへのバックアップの追加」(173 ページ) を参照してください。

メディアの選択

本項では、Data Protector がバックアップに使用するメディアの選択に使用する基準について説明します。

状態が「不良」のメディアはバックアップには使用されません。状態が「普通」のメディアは、使用可能な「良好」のメディアがない場合に限り使用されます。状態が「良好」のメディアが使用できる場合はそれが使用されます。

メディアは常に、指定されたプールおよびフリー・プール (オプション) から最初に選択されます。

表 5-2 バックアップ用メディアの選択方法

割り当てポリシー	[フォーマットされていないメディアを先に割り当てる]	Data Protector の選択順序
[Loose]	オフ	1. 事前割当てリスト (指定されている場合) 2. [追加可能] (使用ポリシーの設定に基づく) 3. 保護が設定されていない Data Protector メディア 4. 未フォーマットのメディア 5. 状態が「普通」のメディア
[Loose]	オン	1. 事前割当てリスト (指定されている場合) 2. [追加可能] (使用ポリシーの設定に基づく) 3. 未フォーマットのメディア 4. 保護が設定されていない Data Protector メディア 5. 状態が「普通」のメディア

表 5-2 バックアップ用メディアの選択方法

割り当てポリシー	[フォーマットされていないメディアを先に割り当てる]	Data Protector の選択順序
[Strict]	(使用不可)	1. 事前割当てリスト (指定されている場合) 2. [追加可能] (使用ポリシーの設定に基づく) 3. 保護が設定されていない Data Protector メディア 4. 状態が「普通」のメディア

メディアのデータ保護設定

Data Protector は、使用されているすべてのメディアのデータを常にトラッキングしています。バックアップを構成する際に、指定した期間だけ、新たなバックアップによってデータが上書きされないよう保護できます。この場合の保護はセッション単位で設定できます。複数のセッションのデータが同一メディア上にある場合、保護期間が最も長いものがこのメディアの保護期間となります。詳細は、「データ保護 : メディア上にデータを保存する期間を指定する」(293 ページ) を参照してください。

メディアのデータ保護を解除すると、そのメディアをリサイクルすることができます。詳しくは、「メディアのリサイクル」(180 ページ) を参照してください。

メディアのリサイクル

Data Protector は、使用されているすべてのメディアのデータを常にトラッキングしています。バックアップを構成する際に、指定した期間だけ、新たなバックアップによってデータが上書きされないよう保護できます。詳細は、第 6 章「バックアップ」(207 ページ) を参照してください。

すべてのメディアには、複数のバックアップ・セッションによるデータが保管されている可能性があることに留意してください。各セッションには、複数のバックアップ・オブジェクト (ファイルシステム) からのデータが含まれている可能性があります。

メディアをリサイクルすると、メディア上に保存されているすべてのバックアップ・データに対する保護が削除され、次回のバックアップ時にデータを上書きできます。メディアをリサイクルしても、単にデータの保護が削除されるだけで、メディア上のデータが実際に削除されるわけではありません。フリー・プール内のメディアにはこのオプションを使用できません。

特定のセッションまたは任意のオブジェクトのデータ保護設定を変更する方法については、第 11 章「Data Protector 内部データベースの管理」(487 ページ) を参照してください。

メディアのリサイクル方法

[デバイス / メディア] コンテキストでメディアをブラウズして右クリックし、[リサイクル] をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「メディアのリサイクル」を参照してください。

別のプールへのメディアの移動

Data Protector では、メディアの種類が同じであれば、プール間でメディアを移動できます。

バックアップを再編成して、各プールの目的を再設定したい場合は、このようなメディアの移動が必要になります。この機能は、使用したいメディアが、別のメディア・プールのデフォルトのデバイス内にある場合にも役立ちます。

別のプールへのメディアの移動方法

[デバイス / メディア] コンテキストでメディアをブラウズして右クリックし、[プールへ移動] をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「メディアの移動」を参照してください。

フリー・プールを使用する場合のメディアの移動

フリー・プールの使用時にメディアが移動されるのは、以下のどちらかの場合です。

- バックアップ用のメディアを選択 (割り当て) する場合。フリー・プールから通常のプールにメディアが移動されます。
- メディアの保護期限が切れた場合。通常のプールからフリー・プールにメディアが移動されます。

この動作は選択されているフリー・プール・オプションによって異なります。

詳細は、「メディア・プールの作成」(157 ページ) を参照してください。

Data Protector 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とは

メディアをエクスポート (削除) すると、メディアに関する情報とメディアに保存されている内容が IDB から削除され、Data Protector ではメディアが認識されなくなります。ただしこれは、メディアそのものからメディアに関する情報と保存データが削除されるのではありません。メディアをいったんエクスポートしても、そのメディアを再度インポートして、メディアに関する情報とメディアに保存されているデータを IDB に読み込むことができます。手順については、「メディアのインポート」(169 ページ)を参照してください。

どのような場合にメディアをエクスポートするか

メディアを別のセルへ移動する場合は、現在のセルからメディアをエクスポートして、移動先のセルにインポートすることが必要です。

保護されたデータを含むメディアは、エクスポート (削除) できません。この場合は、まずメディアをリサイクルする必要があります。手順については、「メディアのリサイクル」(180 ページ) を参照してください。

ヒント

バックアップ・セッションからすべてのメディアをエクスポートしてください。バックアップ・セッションが複数のメディアにまたがっている場合は、それらのメディアをすべて移動しなければ、データを復元できなくなります。これは、Data Protector がメディア上にデータが存在していることを認識していても、実際にはそのメディアを使用できないためです。

メディアのエクスポート方法

[デバイス / メディア] コンテキストでメディアをブラウズして右クリックし、[エクスポート] をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「メディアのエクスポート」を参照してください。

次に行う手順

メディアを別のプールへ追加するか、別のセルへ移動する場合は、「メディア・プールへのメディアの追加」(162 ページ) を参照してください。

メディアを別のセルにインポートする場合は、「メディアのインポート」(169 ページ) を参照してください。

メディアの位置変更

位置とは

メディアの位置とは、メディアが物理的に存在する場所を指します。1 つのオブジェクト・バージョンが複数のメディア・セット上に存在する場合は、メディアの位置を指定することにより、復元に使用されるメディア・セットの選択順位をある程度制御することも可能です。

メディアの位置は、メディアをフォーマットする際に入力します。位置に関する初期情報はメディアと IDB に書き込まれます。

メディアを別の場所 (例 : オフサイトの保管場所、4 番キャビネットの 3 番ボックスなど) へ移動した場合は、位置情報を変更する必要があります。変更後の位置情報は IDB だけに書き込まれます。

Data Protector では、あらかじめ位置リストを作成しておくことで、ボールティングやアーカイビング (オフサイトの保管) の作業の手間を省くことができます。詳しくは、「メディアのボールティング」(199 ページ) を参照してください。

注記

位置を変更しても、メディアそのものの位置が変わるわけではなく、IDB 内でメディアの位置情報が書き換えられるだけです。

したがって、いったんエクスポートしたメディアを再びインポートした場合でも、データベース内の位置情報は、インポートしたメディアに記録されている位置情報に書き換えられます。

ヒント

複数のメディアの位置を同時に変更することができます。これは、ボールティングやアーカイビングを行う場合に便利です。「メディアのボールティング」(199 ページ) を参照してください。

メディアの位置の変更方法

メディアの [一般] プロパティ・ページでメディアの位置を変更します。詳しい手順については、オンライン・ヘルプの索引キーワード「メディアの位置の変更」を参照してください。

メディア位置の優先順位の設定方法

［デバイス / メディア］コンテキストで、［メディア］を展開して［位置］を選択し、適切な位置をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「設定 - メディアの位置の優先順位」を参照してください。

メディアの説明の変更

説明とは

メディアの説明とは、メディアを区別しやすくするためのものです。説明は、新しいメディアをフォーマットするときに定義できます。説明に関する初期情報はメディアと IDB に書き込まれます。

バックアップ中、自動フォーマット時に説明が書き込まれても、後でより適切な説明に書き換えることができます。変更後の説明情報は IDB だけに書き込まれます。

注記

メディアの説明を変更しても、IDB に保存されている説明が書き換えられるだけで、メディアそのものに記録されている説明は**変更されません**。

したがって、更新していないメディアをいったんエクスポートして再びインポートした場合、IDB 内の説明はメディアに記録されている説明に書き換えられます。

メディア・ラベル

メディア・ラベルとは、ユーザーが定義する説明とメディアのバーコードを組み合わせたものです (メディアにバーコードが付与されており、[バーコード・リーダーのサポート] オプションが有効に設定されている場合)。たとえば、メディア・ラベル `[CW8279]Default DLT_1` は、説明が Default DLT_1 でバーコードが CW8279 のメディアを示します。メディアの説明が変更されると、メディア・ラベルの説明部分も変更されます。ただし、バーコード部分は変更されません。

メディアの説明の変更方法

メディアの [一般] プロパティ・ページでメディアの説明を変更します。詳しい手順については、オンライン・ヘルプの索引キーワード「メディアの説明の変更」を参照してください。

メディア上のデータの検証

データの検証とは

メディアの検証を行うと、そのメディア上のデータが有効であるかどうかが分かります。メディアの検証を行うことにより、IDB 内のメディアに関する情報 (メディアの状態など) が更新されます。

Data Protector により実行される処理は、以下のとおりです。

- Data Protectorヘッダのメディアに関する情報のチェック (メディアのID、説明、位置)
- メディア上の全ブロックの読み込みと検証
- [CRCチェック](巡回冗長検査) オプションを使用してメディアへの書込みを行った場合は、Data Protector は CRC を再計算して、メディアに保存されているものと比較します。

  CRC オプションを使用しないで検証を行い、検証が正常終了した場合は、メディア上のすべてのデータが読み込まれたことを意味します。メディアの読み取りエラーは発生しなかったため、テープのハードウェア・ステータスは最低限の受け入れ可能なレベルにあるといえます。このレベルのチェックでは、検証が完全であるとみなすことはできません。

  また、CRC オプションを使用した場合は、各ブロック内のバックアップ・データの整合性が保たれます。このレベルのチェックを行うと高い信頼性が得られます。

注記

使用するバックアップ・デバイスとメディアによっては、検証に時間がかかる場合があります。

検証のタイミング

バックアップ中にエラーがレポートされた場合、メディアを検証してそのバックアップが使用可能かどうかチェックできます。

メディア上のデータの検証方法

［デバイス / メディア］コンテキストでメディアをブラウズして右クリックし、［ 検証 ］をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「メディアの検証」を参照してください。

デバイス内のメディアのスキャン

メディアのスキャンとは

デバイスをスキャンすると、デバイスまたはライブラリ内のメディアに関して IDB に保存されている情報を更新できます。

- スタンドアロン・デバイスの場合は、ドライブ内の単一メディアをスキャンします。
- ライブラリ・デバイスでは、選択したスロット内のメディアがスキャンの対象になります。
- ADIC/GRAU DAS または STK ACS ライブラリを使用する場合は、ADIC/GRAU DAS または STK ACSLM Server に対して照会が行われ、サーバから返された情報と IDB 内の情報との同期が取られます。

重要

ADIC/GRAU DAS または STK ACS ライブラリで、複数の**論理**ライブラリが同じ物理ライブラリに対して構成されている場合、DAS Server または STK ACSLM Server への照会操作はお勧めできません。この場合は VOLSER を手動で追加してください。詳細は、「ADIC/GRAU DAS または STK ACS ライブラリで使用される Data Protector 照会操作」（39 ページ) を参照してください。VOLSER を手動で追加する方法については、「手動による VOLSER の追加」（202 ページ) を参照してください。

ただし、ADIC/GRAU DAS ライブラリで、論理ライブラリが Data Protector ではなく ADIC/GRAU DAS ユーティリティを使用して構成されている場合は、Data Protector 照会操作を安全に使用できます。

制限事項

ADIC/GRAU ライブラリをレポジトリ内で構成するときに 3970 を超える VOLSER が使用されていると、VOLSER のスキャンが正しく実行されない可能性があります。この問題の対応策として、複数の ADIC/GRAU 論理ライブラリを構成して、大きなレポジトリから小さな複数のレポジトリにスロットを分割します。

どのような場合にデバイスをスキャンするか

デバイスのスキャンが必要になるのは、Data Protector のコマンドを使用せずに手動でメディアの位置を変更した場合 (メディアを挿入したり取り出したりした場合) です。コマンドを使用せずに手動でメディアの位置を変更すると、Data Protector がメディアの実際の位置をトラッキングできなくなり、IDB 内でメディア位置の情報に不整合が発生します。

スキャンを実行すると、選択したすべてのスロットからドライブにメディアがロードされ、メディアのフォーマットがチェックされ、メディアのヘッダ情報が表示された後、IDB 内のレポジトリに関する情報が更新されます。

注記

選択したスロットの数によっては、スキャンに非常に時間がかかる場合があります。これは、Data Protector が各スロットからメディアをドライブへロードして、メディアの情報が記載されているヘッダを読み込む時間が必要なためです。

デバイス内のメディアのスキャン方法

デバイス内のメディアをスキャンするには、デバイスを選択し、[アクション] メニューから [スキャン] をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「バックアップ・デバイスのスキャン」を参照してください。

ライブラリ・デバイスを使用する場合、同時に複数のメディアをスキャンできます。ただし、使用できるドライブは 1 つだけです。詳しい手順については、オンライン・ヘルプの索引キーワード「ライブラリ・デバイス内のドライブのスキャン」を参照してください。

バーコードのスキャン

バーコードをサポートしているライブラリをスキャンするには、[バーコードのスキャン] オプションを使用します。この場合 Data Protector は、メディア上のバーコードだけをチェックして IDB 内の情報を更新します。

ADIC/GRAU DAS Server と STK ACSLM Server の照会

サーバから GRAU DAS または STK ACS ライブラリ内のレポジトリに関する情報を取得する場合は、DAS Server または ACSLM Server へ照会を行うことができます。照会操作により、DAS Server または ACSLM Server データベースの照会が行われ、現在レポジトリ内にあるメディアと IDB の情報との同期が取られます。

この機能は、GRAU DAS または STK ACS コマンドを使ってメディアを管理している場合は特に便利です。この場合、Data Protector はライブラリのレポジトリ内にあるメディアの最新ステータスを認識せず、IDB との間に

不整合が生じるためです。詳しい手順については、オンライン・ヘルプの索引キーワード「ADIC/GRAU DAS ホストおよび StorageTek ACSLM ホストを照会する」を参照してください。

重要

ADIC/GRAU DAS または STK ACS ライブラリで、複数の**論理**ライブラリが同じ物理ライブラリに対して構成されている場合、DAS Server または STK ACSLM Server への照会操作はお勧めできません。この場合は VOLSER を手動で追加してください。詳細は、「ADIC/GRAU DAS または STK ACS ライブラリで使用される Data Protector 照会操作」（39 ページ) を参照してください。VOLSER を手動で追加する方法については、「手動による VOLSER の追加」（202 ページ) を参照してください。

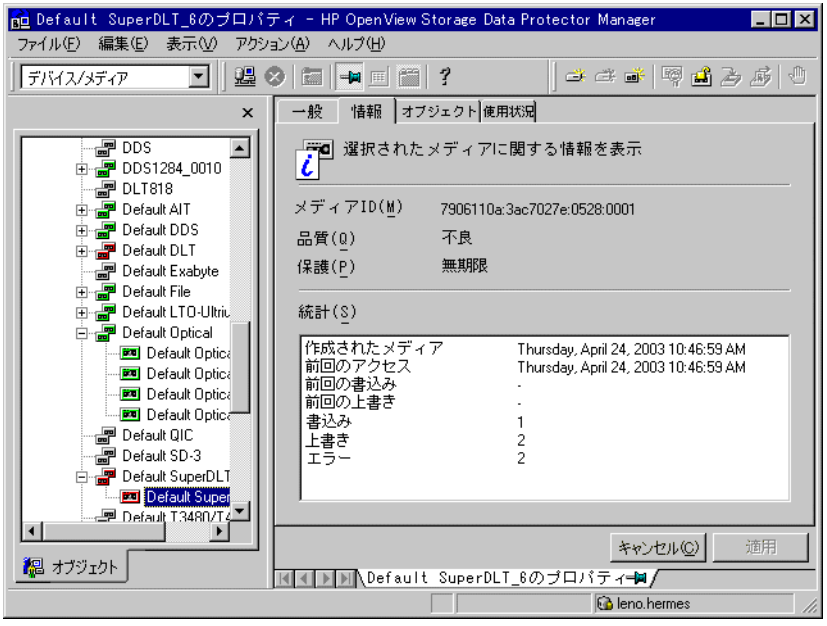
ただし、ADIC/GRAU DAS ライブラリで、論理ライブラリが Data Protector ではなく ADIC/GRAU DAS ユーティリティを使用して構成されている場合は、Data Protector 照会操作を安全に使用できます。

メディアの状態チェック

Data Protector では、メディアの使用状況と状態に関する情報を表示できます。メディアの状態は、メディアへの書き込みやメディアに記録されている情報の読み出しに影響を与えます。つまりメディアの状態を知ることによって、交換が必要であるかどうかを判断することができます。メディアの交換時期については、「メディアの状態に影響する要素」(191 ページ) を参照してください。

メディアの品質 (状態) に関する情報を表示するには、メディアの [情報] プロパティ・ページを使用します。詳細は、図 5-5 を参照してください。

図 5-5 **メディアの情報**



バックアップ・メディアの選択

メディアの状態はバックアップに使用するメディアの選択にも影響を与えます。メディアの状態が「良好」のメディアは、「普通」のメディアよりも優先して選択されます。「不良」のメディアは選択されません。詳細は、「バックアップ用メディアの選択」(176 ページ) を参照してください。

メディアの状態に影響する要素

Data Protector では、**メディア状態要素をもとに使用中のメディアの状態を算出します。**また、メディア・プールの状態は、プールに含まれているメディアの状態によって決まります。たとえば、プール内のいずれかのメディアが「不良」になると、メディア・プール全体が「不良」になります。「不良」のメディアをプールから削除すると、プールの状態は「普通」または「良好」になります。

メディア・プールの状態は、バックアップ用メディア・プールとしての信頼性を示します。たとえば、旧いメディアや摩耗したメディアへのバックアップでは、読み取り / 書き込みエラーが発生する確率が高くなります。

[メディア状態要素] [メディア状態要素] には 2 つの選択項目があります。

メディアの有効期限
このオプションを選択すると、メディアの使用時間を基準として状態が判定されます。ここで、使用時間とは、メディアをフォーマットした時点から経過した月数を意味します。しきい値である月数より旧くなると、「不良」なメディアとして判断されます。デフォルトのしきい値は 36 か月です。

最大上書き数
メディアの使用状況は、そのメディアの先頭から上書きされた回数として定義されます。しきい値である上書き回数を超えると、「不良」なメディアとして判断されます。デフォルトのしきい値は 250 回です (ただし、DDS テープの場合は 100 回)。

デバイス・エラーとメディアの状態
バックアップ中にデバイス・エラーが発生すると、そのデバイスでバックアップに使用していたメディアの状態は「不良」と判断されます。これにより、メディアの不良でエラーが発生した場合は、将来同じエラーが発生するのを防ぐことができます。

ドライブが汚れていたためにエラーが発生した可能性がある場合は、ドライブのクリーニングを行い、メディアの状態を検証して元に戻します。

プール内に「不良」のメディアがないかを調べることをお勧めします。[検証] を選択すると、各メディアの状態に関する情報を収集できます。単にメディアをリサイクルすることはお勧めできません。

メディアとメディア・プールのステータス
メディアまたはメディア・プールのステータスは、メディア状態要素によって、次の 3 種類に分類されます。

[良好] 使用年数または使用状況がしきい値の 80% 以下。

[普通] 使用年数または使用状況がしきい値の 81 ～ 100%。

[不良] 使用年数または使用状況がしきい値の 100% 以上、またはこのメディアで読込み / 書込みエラーが発生した場合。

メディア状態要素の変更については、以下の説明を参照してください。

メディア状態算出法の変更

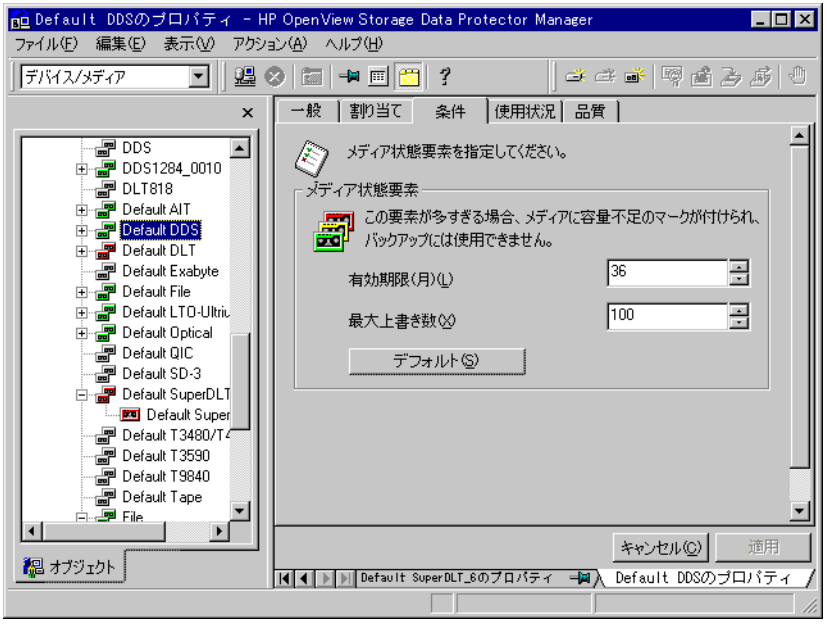
メディア・プールにメディアを追加するときに、メディア状態の算出に使用するメディア状態要素を設定することができます。

重要

Data Protector がメディアの状態を正確に算出できるようにするため、メディアをメディア・プールに追加する場合は新しいメディアを使用してください。

メディア状態要素は、メディア・プールの [条件] プロパティ・ページを使って変更します。状態要素はメディア・プール全体に適用されます。

図 5-6　メディアの [条件] プロパティ・ページ



メディアの検索と選択

この機能は、全メディアのリストをブラウズせずに、特定のメディアだけを指定して検索する場合に使用します。

メディアの選択は、ボールティングを行う場合に便利です。たとえば、14日以上経過しているメディアをすべて選択して、ボールティングすることも可能です。詳細は、「メディアのボールティング」（199 ページ) を参照してください。

メディアの検索および選択方法

［デバイス / メディア］コンテキストでメディア・プールまたはライブラリ・デバイスをブラウズして右クリックし、[メディアの選択] をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「メディアの検索」を参照してください。

デバイスへのメディアの挿入

Data Protector では、ライブラリ・デバイスへメディアを挿入する物理的な操作を行えます。使用するスロットは選択できます。メディアの挿入 / 取出しは、メディアが所属するメディア・プールには影響を与えません。

重要

デバイス内のメディアを取り扱う際は Data Protector を使用することをお勧めします。これにより、IDB 内のメディアに関する情報が最新の状態に維持されるためです。デバイス側の制御機能を使ってメディアを手動で挿入した場合、IDB 内の情報の整合性が保てなくなるため、デバイスをスキャンしてこの情報を更新する必要があります。手順については、「デバイス内のメディアのスキャン」(187 ページ) を参照してください。

ヒント

複数のメディアをデバイスに一度に挿入できます。以下に手順を示します。

デバイスへのメディアの挿入方法

1. [Data Protector Manager] で [デバイス / メディア] コンテキストを選択します。
2. Scoping ペインで [デバイス] をクリックします。構成済みのデバイスのリストが結果エリアに表示されます。
3. 構成済みデバイスのリストから、ライブラリの名前をクリックして展開すると、[ドライブ] と [スロット] という項目が表示されます。
4. [スロット] をクリックしてスロットのリストを表示します。
5. メディアを挿入するスロット (複数可) を右クリックして、[メディアの挿入] をクリックします。

   セッションが開始され、必要に応じてさらにメディアをデバイスに挿入するよう指示するプロンプトが表示されます。

次に行う手順

メディアをメディア・プールに追加するには、「メディア・プールへのメディアの追加」(162 ページ) を参照してください。

デバイスからのメディアの取出し

Data Protector では、デバイスからメディアを取り出す物理的な操作を行えます。ライブラリ・デバイスの場合は、メディアは指定されたスロットへ移動されます。使用するスロットは選択できます。

重要

デバイス内のメディアを取り扱う際は Data Protector を使用することをお勧めします。これにより、IDB 内のメディアに関する情報が最新の状態に維持されるためです。デバイス側の制御機能を使ってメディアを手動で取り出した場合、IDB 内の情報の整合性が保てなくなるため、デバイスをスキャンしてこの情報を更新する必要があります。手順については、「デバイス内のメディアのスキャン」（187 ページ) を参照してください。

メディアの一括取り出し

複数のメディアをライブラリから一度に取り出すことができます。Data Protector は、メール・スロットがいっぱいになると、メール・スロットからメディアを取り出すように指示します。これによって、選択した以外のメディア用にスペースが解放されます。

事前定義に基づいたメディアの取り出し

操作によっては、セッション終了時のメディアの自動取出しが可能です。たとえば、メディアをコピーする際に、セッション終了後にメディアを自動的に取り出すかどうかを指定できます。

メール・スロットがいっぱいでメディアを取り出せない場合、Data Protector はメール・スロットに空きができるか、または事前定義された制限時間が経過するまで操作を再試行します。再試行中、ロボティクスは他のセッションにアクセスできます。

取り出し実行中は、他のセッションは取り出すよう指定されたメディアを使用できません。

制限事項

Novell NetWare では、一括取り出しはサポートされていません。

メディアの取り出し方法

[デバイス / メディア] コンテキストで、メディア / スロット (複数選択可) を右クリックし、[取出し] をクリックしてメディアを取り出します。詳しい手順については、オンライン・ヘルプの索引キーワード「メディアの取り出し」を参照してください。

ヒント

メディアの取り出しはスケジュール設定できます。詳細は、「スケジュールに基づいたメディアの取り出し」(197 ページ) を参照してください。

次に行う手順

メディアをボールティングする場合は、「メディアのボールティング」(199 ページ) を参照してください。

スケジュールに基づいたメディアの取り出し

Data Protector では、レポート機能を使って特定のメディアを取り出すスケジュールを設定できます。スケジュール設定されたメディアの取り出しは、外部スクリプトによる送信を使って作成された特定のレポートに関連付けられています。この方法によって、ユーザーの定義した外部スクリプトにレポートを送信できます。このスクリプトがレポートを解析し、メディアの取り出しを実行します (`omnimm -eject` コマンドを使用)。

必要条件

取り出しを実行するには、Cell Manager 上でプログラムまたはスクリプトを作成することが必要です。また、Cell Manager に適切なインタプリタがインストールされていることも必要です。この例では、Perl スクリプトを使用しています。

概要

レポートを作成し、そのレポートをスクリプトへの入力として送信するために、レポート・グループを設定して、スケジュールを設定できます。このようなレポート・グループは、レポート・パラメータを指定することにより ([メディアのリスト] など)、取り出し対象のメディアをリストし、取り出し対象のメディアのみがレポートに含まれるように設定する必要があります。(設定したスケジュールに基づいて、または [セッションの完了] 通知などの通知にトリガされて) レポート・グループが起動されると、Data Protector はレポートの結果をスクリプトへの入力として送信し、スクリプトを起動します。スクリプトはレポートを解析し、Data Protector の `omnimm` CLI コマンドを使って指定されたメディアを取り出します。

[メールスロットがいっぱいです] 通知

取り出し操作を続行するためにメール・スロットからメディアを取り出す必要がある場合には、デフォルトではイベント・ログ・ビューアに通知されます。このような状況は、取り出すメディアの数がライブラリの空のメール・スロットよりも多い場合に発生します。Data Protector による通知の詳細は、第 9 章「モニター、レポート、通知、およびイベント・ログ」(407 ページ) を参照してください。

デフォルトで設定された時間を過ぎてもメディアがメール・スロットから取り出されておらず、取り出す対象のメディアが残っている場合は、omnimm コマンドは実行を中止します。デフォルトの時間は、omnirc ファイルで変更できます。詳細は、「omnirc オプションの使用」（647 ページ) を参照してください。

メディアの取り出しスケジュールの構成例は、「メディア取り出しのスケジュール例」(A-15 ページ) を参照してください。

メディアのボールティング

ボールティングとは

ボールティングとは、重要なデータが記録されているメディアを安全な場所に移動して、そこで一定期間保管しておく処理を指します。メディアを保管しておく安全な場所は、しばしば**ボールト**と呼ばれます。またボールティングは、オフサイト・ストレージとも呼ばれます。

ボールティングと Data Protector

Data Protector は、以下のようにさまざまなレベルでボールティングをサポートしています。

- データ保護およびカタログ保護のポリシーが設定可能。
- ライブラリ内のメディアの選択と取出しをサポート。
- メディアの物理的な保管場所を示すメディア位置の機能。
- 指定した期間内にバックアップに使われたメディアを示すレポート。
- バックアップ時に、指定したメディアをどのバックアップ仕様が使用したかを示すレポート。
- 指定した場所で保管され、特定の時期にデータ保護が期限切れになるメディアを示すレポート。
- 復元が必要なメディアとその位置を示すリストの表示。
- メディア・リストからの指定した基準と一致するメディアの抽出 (メディアへの書込み時刻、または保護期限切れのメディアなど) が可能。

ボールティングの実装

ボールティングをどのように実装するかは、データとメディアに対するバックアップのストラテジーとポリシーにより異なります。一般的には、次のような作業が含まれます。

1. データのバックアップを構成するときに、データ保護とカタログ保護のポリシーを指定します。

   バックアップ仕様では、バックアップ中に同一データのコピーを複数作成するかどうかを指定できます。「バックアップの構成」(210 ページ) を参照してください。

2. Data Protector でボールトを構成します。実際の作業としては、メディアのボールティングに使用するボールトの名前 (Vault_1 など) を指定します。「ボールトの構成」(200 ページ) を参照してください。

3. バックアップの終了後、ボールティングのためにバックアップ・データのコピーを追加で作成できます。

   特定のバックアップ・オブジェクトをコピーするには、オブジェクトコピー機能を使用します。「オブジェクトコピーの構成」(347 ページ) を参照してください。メディアの完全なコピーを作成するには、メディアコピー機能を使用します。「メディアのコピー」(356 ページ) を参照してください。

4. ボールトに保管するメディアを選択し、そのメディアの位置を変更してメディアを取り出し、ボールトに保管します。
5. ボールトから取り出すメディア (データ保護期限切れのメディアなど) を選択します。[メディアのリスト] レポートで、このようなメディアのリストを取得できます。このレポートの作成方法は、「個別レポートの実行」(441 ページ) を参照してください。
6. メディアをライブラリに挿入してスキャンし、位置フィールドを変更します。
7. ボールトに保管されているメディアに応じて適切な保守方針を決定します。

ボールトの構成

Data Protector では、頻繁に使用するボールトの位置をあらかじめリストに定義しておくことができます。これにより、メディアをボールトへ移動するときに位置を入力する手間が省けます。

[デバイス / メディア] コンテキストで、[編集] メニューから [位置] をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「保管場所リストの構成」を参照してください。

メディアのボールトへの移動

各社の方針に応じて、オリジナルのメディアをボールトに直接移動することも、バックアップ・データのコピーを作成し、そのコピーをボールトに移動することも可能です。

メディアは、以下の手順でボールトへ移動します。

1. 移動するメディアを選択して、メディアの位置を変更します。「メディアの位置変更」(183 ページ) を参照してください。

2. メディアをデバイスから取り出し、ボールトへ移動します。「デバイスからのメディアの取出し」(196 ページ) を参照してください。

ボールトに保管されているメディアからの復元

ボールトからのメディアの復元は、他のメディアからの復元と同じです。データ保護とカタログ保護のポリシーの定義によって、追加ステップが必要になる場合もあります。

1. 復元に必要なメディアを確認します。
2. ボールトに保管されていたメディアをライブラリに挿入して、メディアをスキャンします。
3. メディアに対するカタログ保護がまだ有効な場合は、Data Protector のユーザー・インタフェースを使用して復元するデータを選択することにより、データが復元されます。

   メディアに対するカタログ保護が期限切れの場合は、バックアップされているデータの詳細な情報が Data Protector にはない可能性があります。この場合は、復元対象のファイルまたはディレクトリを手動で選択して復元するか、[メディアのリスト] 機能を使用して復元できます。

ヒント

カタログ保護が期限切れになったメディアからファイルやディレクトリの詳細な情報を再度読み込むには、詳細なカタログ・データの読み込みを指定して、メディアをいったんエクスポートしてもう一度インポートします。このようにすると、Data Protector のユーザー・インタフェースでファイルやディレクトリをブラウズできるようになります。

手動による VOLSER の追加

ADIC/GRAU DAS または STK ACS ライブラリを使用している場合、Data Protector で構成されたライブラリに照会操作を行う代わりに、VOLSER を手動で追加することができます。ADIC/GRAU DAS または STK ACS ライブラリへの照会操作については、「デバイス内のメディアのスキャン」（187 ページ) を参照してください。

ADIC/GRAU DAS および STK ACS ライブラリで、複数の**論理**ライブラリが同じ物理ライブラリに対して構成されている場合は、Data Protector で構成されたライブラリに VOLSER を手動で追加することをお勧めします。ただし、ADIC/GRAU DAS ライブラリで、論理ライブラリが Data Protector ではなく ADIC/GRAU DAS ユーティリティを使用して構成されている場合は、Data Protector 照会操作を安全に使用できるので、VOLSER を手動で追加する必要はありません。詳細は、「ADIC/GRAU DAS または STK ACS ライブラリで使用される Data Protector 照会操作」（39 ページ) を参照してください。

詳しい手順については、オンライン・ヘルプの索引キーワード「追加 - VOLSER を手動で」を参照してください。

スロットまたは VOLSER の削除

Data Protector は、ライブラリによって使用されるスロットとメディア・プール内のメディアを完全にサポートしています。スロットを削除することで、Data Protector がレポジトリ内のスロットを使用したり、アクセスするのを防止できます。スロットに関する情報は IDB から削除されます。

この操作は、GRAU DAS ライブラリ内の VOLSER には影響しません。特定のメディアが IDB から削除されるだけです。したがって、Data Protector はこれらのメディアの存在を認識していないので、使用することもありません。

スロットまたは VOLSER の削除の詳しい手順については、オンライン・ヘルプの索引キーワード「スロット」を参照してください。

書き込み禁止メディアの検出

Data Protector は、書込み禁止スイッチがオンに設定されていて機械的に保護されているメディアを検出し、処理することができます。

注記

Data Protector では書き込み禁止メディアを使用しないことをお勧めします。

下記の操作で、書き込み禁止メディアの検出 / 処理が行われます。

- 読み取り専用の操作 (リスト表示、スキャン、検証など)

  読み取り専用の操作は、書き込み禁止メディアを検出しても警告なしで続行します。

- 書き込み操作 (初期化、消去、バックアップなど)

  書き込み操作では、書き込み禁止メディアを検出すると、セッションを中止するか、または書き込み禁止メディアをスキップして処理を続行します。バックアップ・セッションでは、書き込み禁止メディアは使用不可能なメディアとして処理され、メディア割り当てポリシーに従って処理が続行されます。割り当てポリシーが `[Strict]` の場合は、マウント要求が発行されます。割り当てポリシーが `[Loose]` の場合は、そのメディアはスキップされます。

書き込み禁止メディアの検出、およびメディアの書き込み禁止状態への変更は、すべて `media.log` ファイルに記録されます。

異なる種類のメディア・フォーマットの使用

Data Protector は、メディアへのデータ書き込み時に、2 種類のメディア・フォーマットを認識 / 使用します。

- Data Protector (Data Protector が直接制御するバックアップ・デバイス用)
- NDMP (NDMP サーバに接続されているバックアップ・デバイス用)

2 種類のフォーマットは、それぞれ異なる Data Protector Media Agent コンポーネントを使用してバックアップ・デバイスと通信します。

制限事項

異なる種類のメディア・フォーマットを使用するときは、以下の制限事項に留意してください。

- バックアップ・デバイスと異なる種類のフォーマットで書き込みが行われたメディアは、そのバックアップ・デバイスでは空のメディアまたは無関係なメディアとして認識されます。
- 1 つのメディアに、異なる種類のフォーマットでオブジェクトをバックアップすることはできません。
- 同一システム上に、複数の異なる Data Protector Media Agent コンポーネントをインストールすることはできません。
- フォーマットの種類が異なるメディアに対しては、別々のメディア・プールを使用することを、強くお勧めします。

メディア管理ウィンドウの表示の変更

メディア管理ウィンドウでメディアに関してどのような情報を表示するかをカスタマイズできます。これにより、常に必要な情報だけを表示することができます。

以下の手順に従って、表示をカスタマイズします。

1. 以下に示すグローバル・オプション・ファイルを開きます。

   UNIX Cell Manager の場合

   `/etc/opt/omni/server/options/global`

   Windows Cell Manager の場合

   <Data_Protector_home>¥Config¥server¥Options¥global

2. 対応するトークン文字列を指定することで、ライブラリまたはメディア管理ウィンドウに表示される属性をカスタマイズします。

6 バックアップ

本章の概略

本章では、データのバックアップ方法について説明します。また、Data Protector の拡張機能についても説明します。

データベース・アプリケーション (Oracle、SAP R/3、MS Exchange、MS SQL、Informix、IBM DB2 UDB、Sybase など) のバックアップ方法の詳細は、『HP OpenView Storage Data Protector インテグレーション・ガイド』を参照してください。

Data Protector 内部データベース (IDB) の詳しいバックアップ方法については、「データベース・バックアップを構成する」(505 ページ) を参照してください。

Data Protector 管理用アプリケーションのインストールと構成方法については、第 15 章「他のアプリケーションとの統合」(767 ページ) を参照してください。

注記

バックアップ・デバイス (テープ・ドライブなど) では、専用の Data Protector ライセンスが必要になる場合があります。詳細は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

バックアップの構成

バックアップとは、システム・データのコピーをバックアップ・メディア上に作成するプロセスです。このコピーは、オリジナルのデータが破損した場合に備えて保管されます。

必要条件

- バックアップの対象となる各システム上に Disk Agent がインストールされている必要があります。ただし、NFS (UNIX) またはネットワーク共有のバックアップ (Windows) でバックアップするシステムの場合は、Disk Agent は不要です。
- Data Protector セル内に少なくとも 1 つのバックアップ・デバイスを構成する必要があります。
- バックアップに使用するメディアを準備しておく必要があります。
- バックアップを実行するための適切なユーザー権限が必要です。

バックアップの構成 バックアップの構成作業では、以下の手順を行います。

1. バックアップの対象を選択する - Disk Agent クライアント上のデータ・ソース
2. バックアップ先を選択する - Media Agent クライアントに接続されたバックアップ・デバイス
3. 追加で作成するバックアップコピーの数と使用するバックアップ・デバイスを選択する - オブジェクトミラー機能
4. バックアップ方法を選択する - バックアップ・オプション
5. 必要に応じて無人バックアップをスケジュールできます。

バックアップ仕様の作成時に、上記オプションを指定します。詳細は、「バックアップ仕様の作成」(212 ページ) を参照してください。

Data Protector は、バックアップ仕様に基づいて、指定された時刻にバックアップ・セッションを開始します。1 つのディスク・ボリュームからバックアップ対象として選択するすべての項目 (論理ディスクまたはマウント・ポイント) を含むバックアップ単位を**バックアップ・オブジェクト**といいます。項目としては、任意の数のファイル、ディレクトリ、あるいはディスクまたはマウント・ポイント全体を選択することができます。バック

アップ・オブジェクトは、それが存在するクライアントとマウント・ポイント、説明、およびオブジェクト・タイプ (ファイルシステムや Oracle など) によって一意に定義されます。

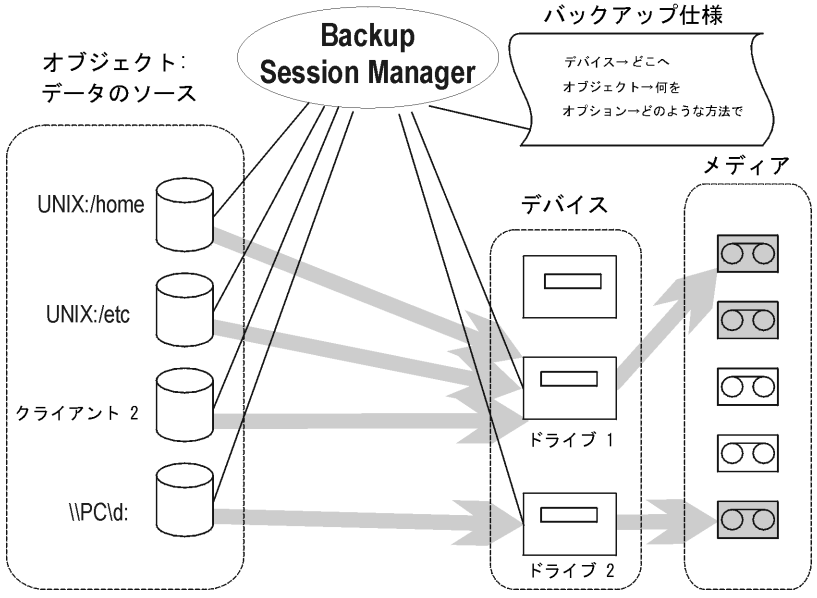
バックアップ・セッション中、Data Protector はオブジェクトを読み取って、ネットワーク経由でデータを転送し、デバイス内のメディアに書き込みます。

バックアップ仕様では使用するデバイスと、必要に応じてメディア・プールを定義します。特定のメディア・プールが指定されていない場合、デフォルトのメディア・プール (デバイス仕様の一部) が使用されます。

バックアップ仕様では、スタンドアロン DDS ドライブの 1 つのドライブをバックアップするような単純な定義から、40 台の大規模なサーバを 8 つのドライブを使用したテープ・ライブラリにバックアップするような複雑な定義が可能です。

バックアップ・セッションはバックアップ仕様に基づいており、対話方式で起動できます。バックアップ・セッション中、Data Protector はバックアップ・オブジェクトを読み取って、ネットワーク経由でデータを転送し、デバイス内のメディアに書き込みます。

図 6-1 バックアップ・セッション



バックアップ仕様の作成

バックアップ仕様は、Data Protector ユーザー・インタフェースを使って構成できます。バックアップ仕様では、バックアップ対象となるクライアント・システム、ドライブ、ディレクトリ、ファイル、使用するデバイスまたはドライブ、追加のバックアップコピー (ミラー) の数、仕様内のすべてのオブジェクトに適用するバックアップ・オプション、バックアップを実行する日時を定義します。

既存の仕様をコピーしてその内容を変更すれば、様々なバックアップ仕様を作成できます。

Data Protector では大抵のケースに対応可能な複数のデフォルト・オプションを提供しています。これをカスタマイズするには、Data Protector バックアップ・オプションを使用してください。

バックアップ・セッションを実行する際は、以下のキー・ポイントに注意してください。

キー・ポイント

- バックアップの種類 (フルまたは増分) はバックアップ・セッション全体を通して同じものが使用されます。グループ内のすべてのデータは同じバックアップ種類によってバックアップされます。
- 1 つのバックアップ・オブジェクトを複数のバックアップ仕様に追加できます。このため、用途別に (フル・バックアップ用、増分バックアップ用、部門別バックアップ用、アーカイブ・バックアップ用など) それぞれバックアップ仕様を設定できます。各オブジェクトには、説明用テキストを指定できます。この説明に基づいて同じファイルシステムからの複数のバックアップを区別するため、説明を慎重に選択することが必要です。
- オブジェクトまたはクライアントは、メディアとバックアップの管理方法が同じ場合、またはメディアを 1 つのボールトに保存する場合、1 つのバックアップ仕様にまとめることができます。
- 多数のバックアップ仕様が作成されている、または作成が計画されている場合、それらのバックアップ仕様をグループに分類することが必要です。グループを共通のオプション設定 (バックアップ方法) に基づいて分類しておけば、バックアップ・テンプレートを効率よく適用することができます。
- Data Protector GUI が表示するバックアップ仕様の数には制限があります。バックアップ仕様の数は各パラメータ (名前、グループ、所有権情報、バックアップ仕様が負荷調整されているかどうか) のサイズによって決まります。このサイズは 80KB を超えることはできません。

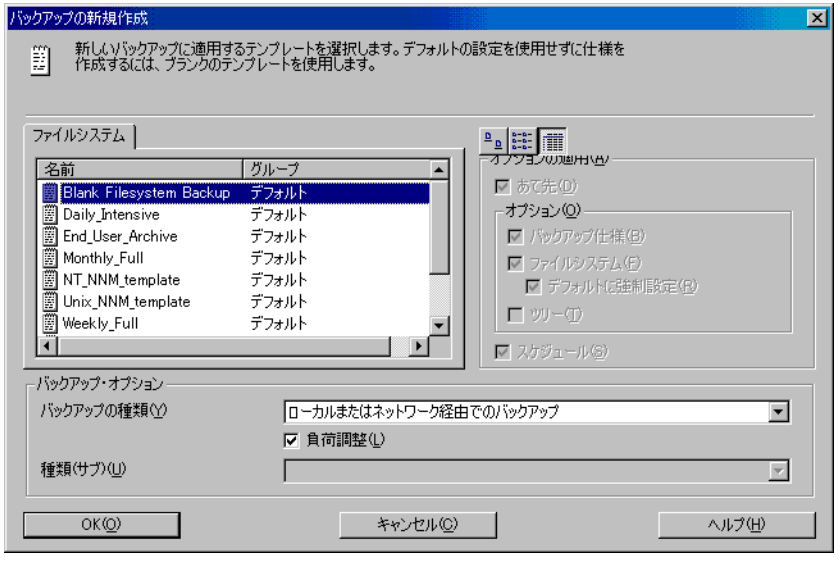
バックアップ仕様の作成例

以下の例では、ファイルシステム向けのバックアップ仕様の作成方法と、対話型バックアップの開始方法を示します。

1. [HP OpenView Storage Data Protector Manager] ウィンドウで [バックアップ] コンテキストを選択します。
2. Scoping ペインで [バックアップ] を展開した後、[バックアップ仕様] をダブルクリックします。
3. 結果エリアで [ファイルシステム] を右クリックして [バックアップの追加] をクリックします。[バックアップの新規作成] ダイアログ・ボックスが表示されます。

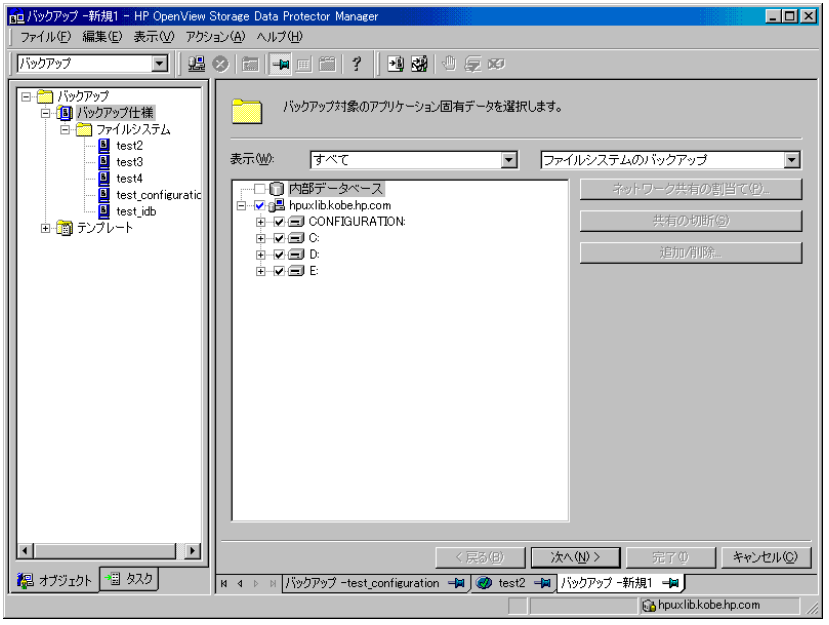
4. [バックアップの新規作成] ダイアログ・ボックスで、[Blank Filesystem Backup] テンプレートを選択して [OK] をクリックすると、[バックアップ] ウィザードが表示されます。図 6-2 (214 ページ) を参照してください。

図 6-2　[バックアップの新規作成] ダイアログ・ボックス



5. バックアップの対象を選択します。バックアップ対象として選択されたデータ・ソースを図 6-3 (215 ページ) に示します。[次へ] をクリックして次の手順に進みます。

図 6-3 [バックアップ] ウィザードの [ソース] ページ



UNIX システムの GUI では Windows システムのブラウズはサポートされていません。したがって、UNIX の GUI を使用したバックアップ・オブジェクトの表示用にサポートされているのは [ファイルシステムのバックアップ] オプションだけです。[ネットワーク共有のバックアップ] は、Windows の共有ディスクをバックアップするための Windows 固有のオプションなので、Windows の GUI でしか使用できません。

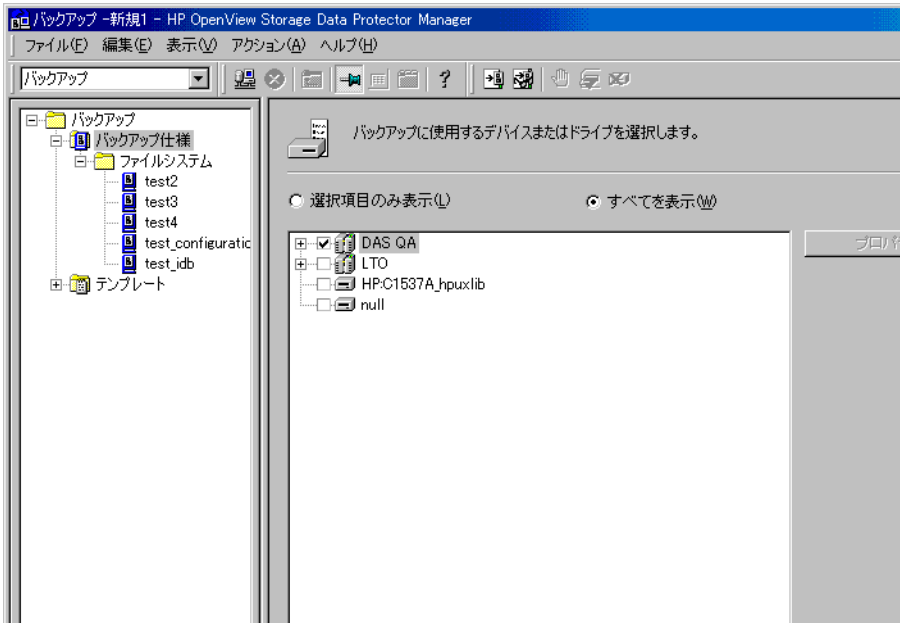
6. データのバックアップに使用するデバイスを選択します。図 6-4 (216 ページ) を参照してください。

   バックアップ・セッションの実行中に、バックアップの追加コピー (ミラー) を作成するかどうかを指定することもできます。必要なミラーの数を指定するには、[ミラーの追加] ボタンおよび [ミラーの削除] ボタンをクリックします。バックアップおよび各ミラー用のデバイスを個別に選択します。

   オブジェクトミラー機能の詳細は「オブジェクトミラー」(354 ページ) を参照してください。

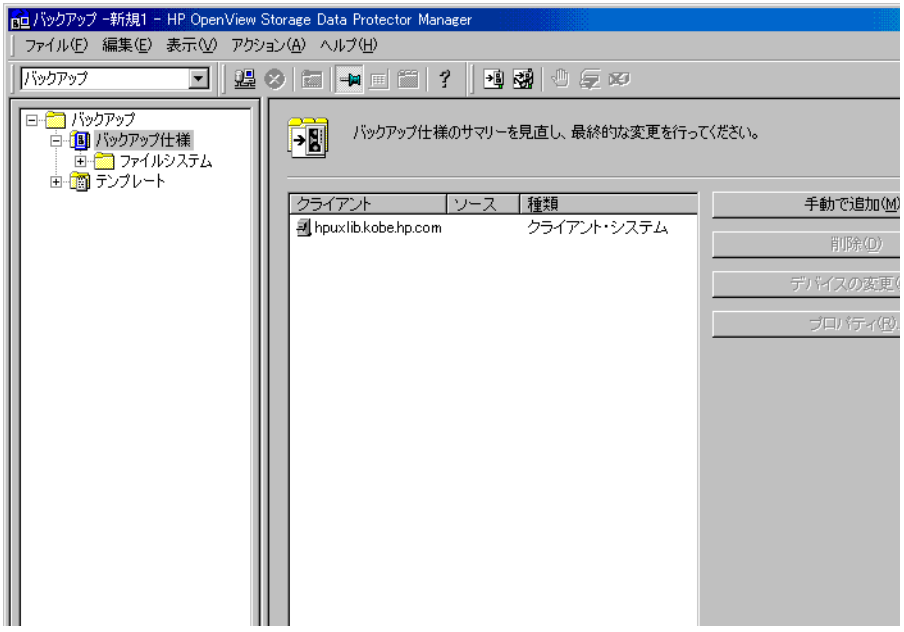
   [次へ] をクリックして次の手順に進みます。

図 6-4 [バックアップ] ウィザードの [デバイス] ページ



7. バックアップ・オプションを選択します。詳細は、「バックアップ・オプションの使用」(290 ページ) を参照してください。[次へ] をクリックします。
8. [スケジュール] ページでは、バックアップをスケジュールできます。詳しくは、「無人バックアップのスケジュール」(269 ページ) を参照してください。[次へ] をクリックします。
9. [バックアップ・オブジェクトのサマリー] ページでは、バックアップ・オプションを確認できます。図 6-5 (217 ページ) を参照してください。[次へ] をクリックします。

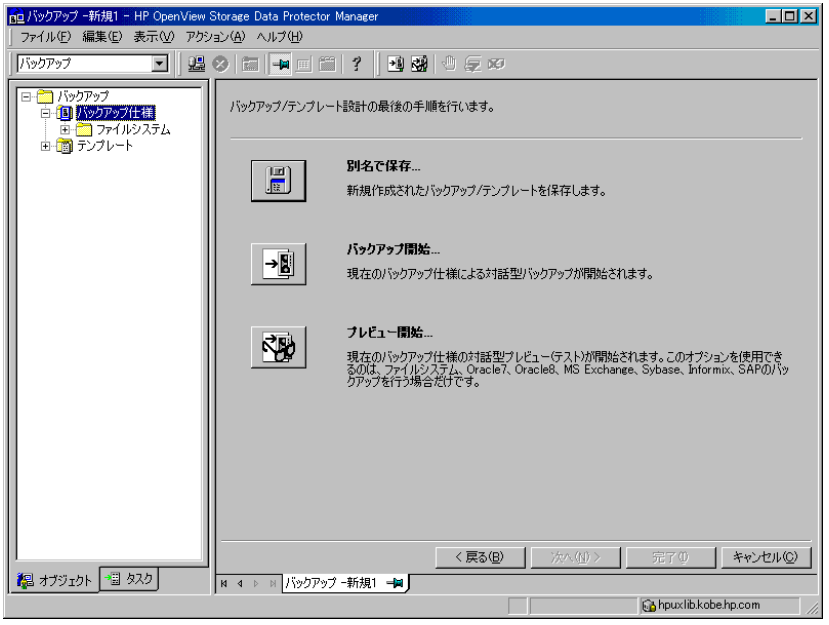
図 6-5 [バックアップ・オブジェクトのサマリー] ページ



10. [バックアップ] ウィザードの最終ページでは、バックアップ仕様の保存、対話型バックアップの開始、またはバックアップのプレビューを行うことができます。図 6-6 (218 ページ) を参照してください。

    バックアップ仕様を保存して、後でスケジュールを設定したり仕様を変更できるようにしておくことをお勧めします。

図 6-6 **[バックアップ] ウィザードの最終ページ**



11. [バックアップ開始] をクリックして、バックアップを対話形式で実行します。[バックアップ開始] ダイアログ・ボックスが表示されます。

注記

バックアップ中に、バックアップを続行するためメディアの追加を要求するメッセージが表示される場合があります。これはマウント要求と呼ばれます。詳細は、「マウント要求への応答」(412 ページ) を参照してください。

UNIX システムのバックアップ

UNIX システムをバックアップするには、対象となる各 UNIX システム上に Disk Agent をインストールします。または、ネットワーク・ファイルシステム (NFS) を使って、Disk Agent がインストールされていないシステムからデータをバックアップすることもできます。

詳細は、「NFS を使ったディスクのバックアップ」（223 ページ) を参照してください。

Disk Agent のインストール方法については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』またはオンライン・ヘルプを参照してください。

サポートされているプラットフォームの全リストと既知の制限事項については、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

UNIX ファイルシステムのバックアップ

制限事項

バックアップできるファイルの最大サイズは、オペレーティング・システムとファイルシステムの制限によって決まります。ファイルサイズの制限事項については、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

Data Protector では、ディレクトリ構造、通常のファイル、および特殊なファイルをバックアップします。特殊なファイルには、キャラクタ・デバイスファイル、ブロック・デバイスファイル、UNIX ドメイン・ソケット、FIFO ファイル、HP-UX のネットワーク・ファイル、XENIX の名前付きファイルがあります。

ソフトリンクとマウント・ポイントは上記に含まれず、これらはそれぞれソフトリンク、通常の空白のディレクトリとしてバックアップされます。

同じファイルを参照する複数のハードリンクがある場合は、参照先ファイルが 1 回だけバックアップされます。この動作を変更するには、「Data Protector バックアップ・オプションのリスト」（302 ページ) で説明されているとおり、[POSIX ハードリンクをファイルとしてバックアップ] オプションを設定します。

どのプラットフォームでも、基本の ACL(ファイル権限属性) や時間属性がファイルと一緒にバックアップされます。ただし、プラットフォームによっては拡張 ACL のサポートが制限されています。詳細については、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。各ファイルへの最終アクセス時刻は、ファイルの内容を読み取る前に保存され、ファイルのバックアップ後に元の値に戻されます。この動作を変更するには、「バックアップ・オプションの使用」(290 ページ) で説明している [アクセス時刻属性を保存しない] オプションを設定します。

Data Protector は、増分バックアップという優れた機構を備えています。Data Protector Disk Agent は、どのファイルが変更されたかを判別するため、各ファイルの前回変更日時を調べます。この方法では、移動されたファイルは検出されません。ファイルを移動しても、ファイルの変更日時は変わらないためです。

注記

バックアップ・セッション時に、バックアップ対象の各ファイルはオープンされ、読み取りが行われます。したがって、バックアップ後ファイルのアクセス時刻は変更されます。[アクセス時刻属性を保存しない] バックアップ・オプションが設定されていない場合、アクセス時刻属性は元の値に設定されます。このオプションのデフォルト値はオフです。このオプションが設定されている場合、UNIX クライアント上で移動されたファイルは増分バックアップの対象となります。これは、移動ファイルの検出が `inode` 変更時刻に基づいて行われるためです。

特定のファイルまたはディレクトリの選択

各ファイルシステムでは、特定のディレクトリ・ツリーだけをバックアップすることができます。各ディレクトリ・ツリーに対しては以下を実行できます。

- サブツリーまたはファイルを除外する
- 特定のワイルドカード指定に一致するファイルだけをバックアップする
- 特定のワイルドカード指定に一致するファイルだけを除外する

ファイルの中には、データベース・アプリケーションなどによって常時使用されているものもあります。これらのファイルを通常のファイルシステム・バックアップから除外して、特殊な方法でバックアップする必要があります。このことは、IDB 自体にもあてはまります。

つまり、UNIX Cell Manager 上の IDB ディレクトリ /var/opt/omni/server/db40 および /etc/opt/omni を標準ファイルシステム・バックアップから除外して、データの整合性を維持する必要があります。

IDB のバックアップ方法の詳細は、「データベース・バックアップを構成する」(505 ページ) を参照してください。

一時ディレクトリも除外する必要があります。

UNIX ファイルのバックアップ方法

UNIX ファイルをバックアップするには、「バックアップ仕様の作成例」(213 ページ) に示す手順を実行します。

バックアップ・オプションの使用および設定方法については、「バックアップ・オプションの使用」(290 ページ) を参照してください。

ディスク・ディスカバリによるクライアントのバックアップ

ディスクはどのようにして検出されるか

ディスク・ディスカバリを使ってクライアント・バックアップを指定した場合、Data Protector はバックアップ時に、まずクライアントにアクセスして、そのシステムに接続されているディスク上のすべてのファイルシステムを検出します。マウント・コマンドを使用すると、マウントされているディスクしか検出されません。次に、Data Protector は、検出した各ファイルシステムを通常のファイルシステムとしてバックアップします (ただし、NFS、CD にマウントされたファイルシステム、取り外し可能なボリュームを除く)。各ファイルシステム・オブジェクトの説明用テキストが生成され、ファイルシステムのマウント・ポイントがクライアント・バックアップの説明に追加されます。

どのような場合にディスク・ディスカバリを使用するか

以下の状況では、この種類のバックアップを実行することをお勧めします。

- マウント / アンマウントを頻繁に行う、比較的容量の小さいディスクを持つワークステーションをバックアップする場合
- マウントされているファイルシステムの数に関係なく、マウント・ポイントの下にあるデータを 1 つのディレクトリにバックアップする場合 (例 : /home/data - ここでは、/home/data/disk1 と /home/data/newdisk/disk2 のマウント / アンマウントをそれぞれ頻繁に独立して行うことができます。)

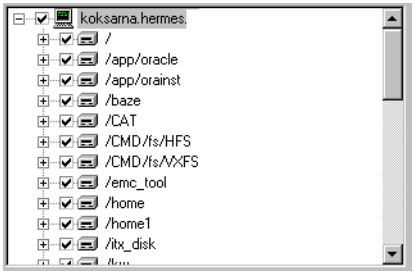
クライアントをデータ・ソースとして指定することにより、ディスク・ディスカバリを使用できます。後で別のディスクをマウントすると、そのディスクもバックアップの対象となります。

ファイルシステム・バックアップでは、新しく追加されたディスクまたはマウントされているファイルシステムがバックアップ仕様で指定されていない場合、その都度指定する必要があるのに対し、ディスク・ディスカバリを使用すれば、指定する必要はありません。

ディスク・ディスカバリによるバックアップを定義するバックアップ仕様を作成するには、「バックアップ仕様の作成例」(213 ページ) に示す手順を行います。

[バックアップ] ウィザードの [ソース] プロパティ・ページを表示して、クライアント・システムの横にあるチェックボックスをクリックします。これにより、図 6-7 に示すとおり、クライアント・システム全体がバックアップ対象として選択されます。

図 6-7　クライアント・システム全体をバックアップ対象として選択する



注記

クライアントのすべてのドライブを選択するという操作と、クライアント・システム名の横のチェックボックスをクリックするという操作は全く別のものです。後者はディスク・ディスカバリによるバックアップを行うための手順です。

クライアントのバックアップを実行すると、ルート (/)・マウント・ポイントに所属するすべてのファイルとディレクトリが自動的にバックアップされます。したがって、バックアップ仕様からルートを除外することはできません。ルートを除外したい場合は、ファイルシステムのバックアップを実行してください。

構成済みのバックアップの種類を調べるには、[バックアップ・オブジェクトのサマリー] プロパティ・ページを表示します。ディスク・ディスカバリによるバックアップが構成されている場合は、[オブジェクトの種類] ラベルに [クライアント・システム] と表示され、ドライブのみが選択されている場合は、[ファイルシステム] と表示されます。

バックアップ仕様の設定方法については、「バックアップ・オプションの使用」(290 ページ) を参照してください。

NFS を使ったディスクのバックアップ

NFS とは

NFS(ネットワーク・ファイルシステム) とは UNIX 上で配信されるファイルシステム・プロトコルの 1 つで、コンピュータがネットワーク上のファイルに対して、ローカル・ディスク上のファイルと同様にアクセスできるようにします。

どのような場合に NFS バックアップを使用するか

NFS のバックアップは、以下のいずれかの状況で使用します。

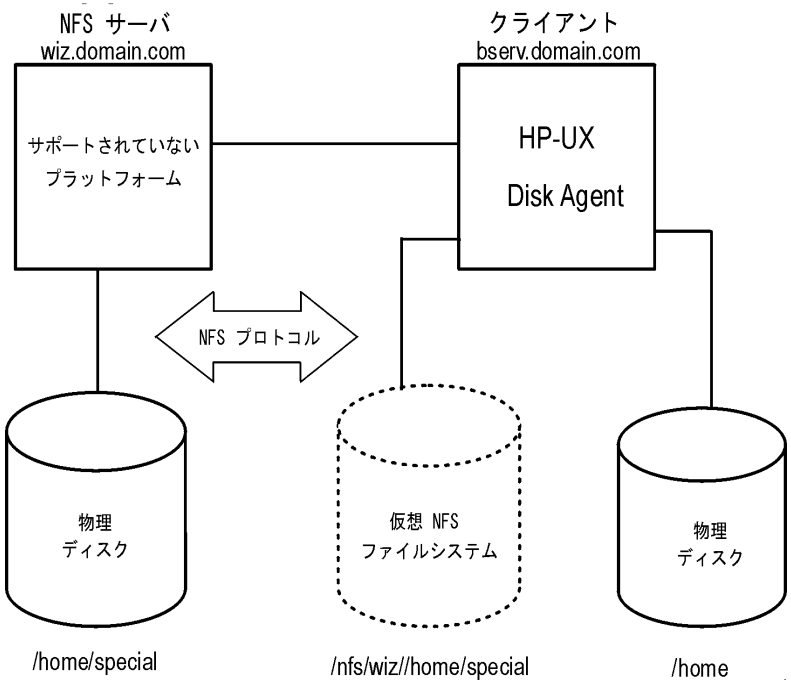
- バックアップ対象のシステムが Data Protector セルの一部でないか、Disk Agent がインストールされていない場合
- Data Protector でサポートされていないシステム・プラットフォームをバックアップする場合

例

図 6-8 に代表的な構成を示します。例では、システム `wiz` からファイルシステム `/home/special` をバックアップするとします。このシステムは Data Protector セルの一部でなく、Data Protector ソフトウェアはインストールされていません。ただし、上記のファイルシステムは、クライアント Data Protector client `bserv` 上に `/nfs/wiz/home/special` としてマウントされています。

このファイルシステムを NFS を使ってバックアップするには、`bserv` 上の他のファイルシステムをバックアップする場合と同じ手順を使用する必要があります。ただし、マウント・ポイントとして `/nfs/wiz/home/special` を手動で入力する点だけが異なります。ブラウズするとローカル・ファイルシステムだけが表示されます。

図 6-8 **NFS 環境**



制限事項

- NFS を使用できるのは、HP-UX クライアント上および Solaris 上でファイルをバックアップする場合だけです。ソフト・リンク、またはキャラクタ・ファイルとデバイスファイルはバックアップできません。
- ACL(アクセス制御リスト) 属性は維持されません。NFS ではリモート・ファイルに対する ACL をサポートしていません。各種システム・コール、ライブラリ・コール、およびコマンドの動作は、個々の手動エントリとして指定します。省略可能なエントリを指定したファイルをネットワーク経由で転送したり、リモート・ファイルを操作すると、省略可能なエントリが予期せず削除されることがあります。

注記

マウントされている NFS ファイルシステムに対して root 権限を持つことをお勧めします。

NFS を使ってファイルシステムをバックアップするには、[バックアップ] ウィザードの [バックアップ・オブジェクトのサマリー] ページが表示される時点まで「バックアップ仕様の作成例」(213 ページ) に示す手順を行います。それ以降は、以下の手順を行います。

1. [バックアップ・オブジェクトのサマリー] ページで [手動で追加] をクリックします。
2. [UNIX ファイルシステム] ボタンをクリックした後、[次へ] をクリックします。
3. [一般的な選択項目] ページでクライアントを選択し、[マウント・ポイント] テキスト・ボックスにマウント・ポイントを手動で追加します。詳細はオンライン・ヘルプを参照してください。

UNIX ディスクをディスク・イメージ・オブジェクトとしてバックアップする

ディスク・イメージ・バックアップとは

ディスク・イメージ・バックアップとは、ディスク、ディスク・パーティション、または論理ボリュームを、データ・ソースに保存されているファイルやディレクトリ構造をトラッキングせずに高速バックアップしたものを指します。Data Protector はディスク・イメージ構造を文字レベルで保存します。

どのような場合にディスク・イメージ・バックアップを使用するか

ディスク・イメージ・バックアップは、以下のいずれかの状況で使用します。

- 容量の小さいファイルが多数あり、高速バックアップが必要な場合。
- 障害復旧用またはソフトウェアのメジャー・アップデートを行う前などにディスクのフル・バックアップが必要な場合。
- 2 つのディスク間を直接接続できない場合に、一方のディスクへファイルシステムを複製する場合。この場合、2 つのディスクは同一でなければなりません。

raw ディスク・セクションの場所

HP-UX および Solaris システムでは通常、raw ディスク・セクションは /dev/rdsk ディレクトリにあります。HP-UX では、raw 論理ボリュームは、/dev/vg< *番号* > にあります。新しい論理ボリュームの最初の文字は、r でなければなりません (例 : /dev/vg01/rlvol1)。

重要

ディスク・イメージ・バックアップを行う前にはディスクを一旦アンマウントして、後でもう一度マウントしてください。これを行うため、実行前 / 実行後コマンドを使用できます。「実行前 / 実行後コマンドの例 (UNIX の場合)」(A-21 ページ) を参照してください。

ディスク・イメージ・オブジェクトをバックアップするには、[バックアップ] ウィザードの [バックアップ・オブジェクトのサマリー] ページが表示される時点まで「バックアップ仕様の作成例」(213 ページ) に示す手順を行います。それ以降は、以下の手順を行います。

1. [バックアップ・オブジェクトのサマリー] ページで [手動で追加] をクリックします。
2. [ディスク・イメージ・オブジェクト] ボタンをクリックした後、[次へ] をクリックします。
3. [一般的な選択項目] ページでクライアントを選択し、[マウント・ポイント] テキスト・ボックスにマウント・ポイントを手動で追加します。詳細はオンライン・ヘルプを参照してください。

Windows システムのバックアップ

必要条件

Data Protector セル内の Windows コンピュータ上に Disk Agent が少なくとも 1 つインストールされていることが必要です。このコンピュータが Disk Agent クライアントとなります。

Disk Agent クライアント上にないファイルでも、これらのファイルが Disk Agent クライアントとディスクを共有している場合はバックアップできます。バックアップ対象のすべての Windows システムに Disk Agent をインストールすることをお勧めします。

詳細は、「Windows 共有ディスクのバックアップ」（246 ページ) を参照してください。

Disk Agent のインストール方法については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』またはオンライン・ヘルプを参照してください。

サポートされているシステムのプラットフォームの全リストについては、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

制限事項

- VSS ファイルシステムのバックアップを実行するには、システムに最低 1 つの NTFS ファイルシステムが必要です。

ファイルシステム (論理ディスク・ドライブ) のバックアップ

バックアップ・オブジェクトの選択

[バックアップ] ウィザードでバックアップの対象とするファイル、ディレクトリ、または論理ディスク・ドライブを選択します。

詳細は、「バックアップ仕様の作成例」（213 ページ) および「バックアップ・オプションの使用」（290 ページ) を参照してください。

バックアップの対象

ディスク・ドライブのファイルシステム・バックアップでは、選択されたディスク・ドライブ上のディレクトリ構造とファイルの内容が読み込まれます。また、ファイル内のデータと共に以下のデータもバックアップされます。

- Unicode のフル・ファイル名

- FAT16、FAT32、VFAT、NTFS 属性

  各ファイルのバックアップ後、ファイルのアーカイブ属性はクリアされます。この動作を変更するには、バックアップ仕様の［拡張］ファイルシステム・オプションの［アーカイブ属性を使用しない］オプションを設定します。詳細はオンライン・ヘルプを参照してください。

- NTFS の代替データ・ストリーム
- NTFS セキュリティ・データ
- ディレクトリの共有情報

  ネットワーク上でディレクトリが共有されている場合、デフォルトで共有情報がバックアップされます。復元時に、デフォルトで共有情報が復元され、復元後にネットワーク上でディレクトリが共有されます。この動作を変更するには、ファイルシステム・オプション・ウィンドウで、［ディレクトリ共有情報のバックアップ］オプションをオフにします。

バックアップの対象とならないもの

バックアップ仕様では、バックアップから除外またはスキップするファイルを指定できます。これらのファイルのリストは、**プライベート除外リスト**とも呼ばれます。

ファイルやディレクトリの詳しい除外方法については、「オブジェクト・オプション」(306 ページ) とオンライン・ヘルプを参照してください。

Data Protector は、デフォルトではプライベート除外リストの内容に加えて、以下を除外します。

- Windows クライアントまたは Cell Manager バックアップから *<Data_Protector_home>*¥log と *<Data_Protector_home>*¥tmp ディレクトリを除外
- Windows Cell Manager バックアップから *<Data_Protector_home>*¥db40 ディレクトリを除外

  たとえば、*<Data_Protector_home>*¥db40 ディレクトリは、バックアップ仕様で選択されていても、Cell Manager バックアップから除外されます。これは、*<Data_Protector_home>*¥db40 ディレクトリには IDB が含まれており、このディレクトリを特殊な方法でバックアップしてデータの整合性を維持する必要があるためです。詳細は、「データベース・バックアップを構成する」(505 ページ) を参照してください。

スキップされるファイルは Pagefile.sys システム・ファイルです。バックアップを開始する前に、Data Protector は、除外するファイルとスキップするファイルのリストを以下のレジストリ・キーから読み込みます。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Hewlett-Packard¥OpenView
¥¥OmniBack II¥Agents¥FileSystem¥Exclude
```

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Hewlett-Packard¥OpenView
¥¥OmniBack II¥Agents¥FileSystem¥Skip
```

NTFS 3.x ファイルシステムの特長

NTFS 3.x ファイルシステムで新たに採用されたファイル属性と概念の概要を以下に示します。

- NTFS 3.x ファイルシステムでは、**再解析ポイント**をサポートしています。**ボリューム・マウント・ポイント**、**Single Instance Storage (SIS)**、**ディレクトリ接続**は再解析ポイントの概念に基づいています。詳細は、「用語集」を参照してください。
- NTFS 3.x ファイルシステムは、ディスク・スペースの割り当て量を効率的に低減する手段として**疎ファイル**をサポートしています。

- NTFS 3.x ファイルシステムでは、**オブジェクト ID** をサポートしています。これらは Data Protector によって、代替データ・ストリームと共にバックアップされます。
- NTFS 3.x ファイルシステムに固有の機能には、独自のデータ・レコードを維持するシステム・サービスによって制御されるものがあります。これらのデータ構造は、CONFIGURATION の一部としてバックアップされます。

  詳細は、「CONFIGURATION のバックアップ」（233 ページ) および「Windows サービスのバックアップ」（239 ページ) を参照してください。
- Microsoft 暗号化 NTFS 3.x ファイルは､暗号化された状態でバックアップと復元が行われますが、ファイルの内容は、復号化した時点でしか正しく表示されません。関連する制限事項の詳細は、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

VSSファイルシステムのバックアップ

Volume Shadow Copy サービス (VSS) は Windows Server 2003 オペレーティング・システム上に実装されています。このサービスにより、これまでにない Windows ファイルシステムのバックアップが可能となり、従来のアクティブなボリュームのバックアップに比べてデータの完全性レベルが若干向上します。

シャドー・コピー作成の準備をするため、すべての I/O 動作が VSS 機構により停止されます。シャドー・コピーが作成されると、Data Protector は通常のバックアップ手順を開始しますが、ソース・ボリュームは新たに作成されたシャドー・コピーに置き換えられます。シャドー・コピーの作成が失敗した場合、バックアップ仕様で［フォールバックを許可］オプションが指定されていれば、Data Protector は通常のファイルシステム・バックアップを続行します。

VSS ファイルシステム・バックアップ中のデータの整合性は、VSS ファイルシステム以外のバックアップに比べて向上します。VSS により、ボリュームのシャドー・コピー・バックアップや、正確なポイント・イン・タイムでのファイル (すべてのオープン中のファイルを含む) のコピーの作成が可能となります。この方法では、バックアップ中に変更されたファイルも適切にコピーされます。

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の実行中にコンピュータのバックアップが可能です。したがって、アプリケーションはバックアップ中もボリュームへのデータ書き込みを続行できます。
- オープン中のファイルもシャドー・コピー・ボリューム上ではクローズしているとみなされてシャドー・コピーが作成されるため、オープン中のファイルに対するバックアップ処理がスキップされません。
- ユーザーをロックアウトすることなく、いつでもバックアップを実行できます。
- バックアップを実行しても、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、あるいはまったく影響ありません。

VSS ファイルシステム・バックアップ関連のオプションについては、「バックアップ・オプションの使用」（290 ページ）を参照してください。VSS の概念の詳細は、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

再解析ポイント

NTFS 3.x ディレクトリまたはファイルに再解析ポイントを含めることができます。このポイントは通常、別のディレクトリからあるデータを参照することにより、その内容がそこに存在するかのように動作します。

Data Protector が再解析ポイントを検出した場合、デフォルトでは、再解析ポイント ID の先はバックアップされません。これは、再解析ポイント自体のバックアップとも呼ばれます。このことは、バックアップの構成方法に影響を与えます。

- ディスク・デリバリーによるバックアップを構成している場合、すべてのデータは一度にバックアップされます。
- 再解析ポイントが格納されているファイルシステムまたはドライブをバックアップする場合は、再解析ポイントのリンク先のデータも必ずバックアップしてください。たとえば、Windows で**ディレクトリ接続**に使用されている再解析ポイントは無視されるので、接続点を個別にバックアップする必要があります。SIS 再解析ポイントの場合は例外です。

  Single Instance Storage (SIS) サービスは、ディスク上のファイルを定期的にチェックします。同一ファイルが検出された場合、それらを再解析ポイントと置き換え、データを共通レポジトリに保存します。これにより、使用されるディスク・スペースが節約されます。

再解析ポイントにより、論理ボリュームをディスク・ドライブとしてマウントできます。Data Protector では、マウントされたボリュームは通常のドライブと同様に扱われるので、バックアップ対象として選択可能なオブジェクトとして表示されます。

疎ファイル

疎ファイルには、圧縮ファイルなどとは対照的にゼロ・データ・セットが多数含まれています。バックアップ時に、Data Protector はゼロの部分を自動的にスキップするため、バックアップ・デバイス上のメディア・スペースはゼロ以外の部分にしか割り当てられません。

UNIX と Window s の疎ファイルには互換性がありません。

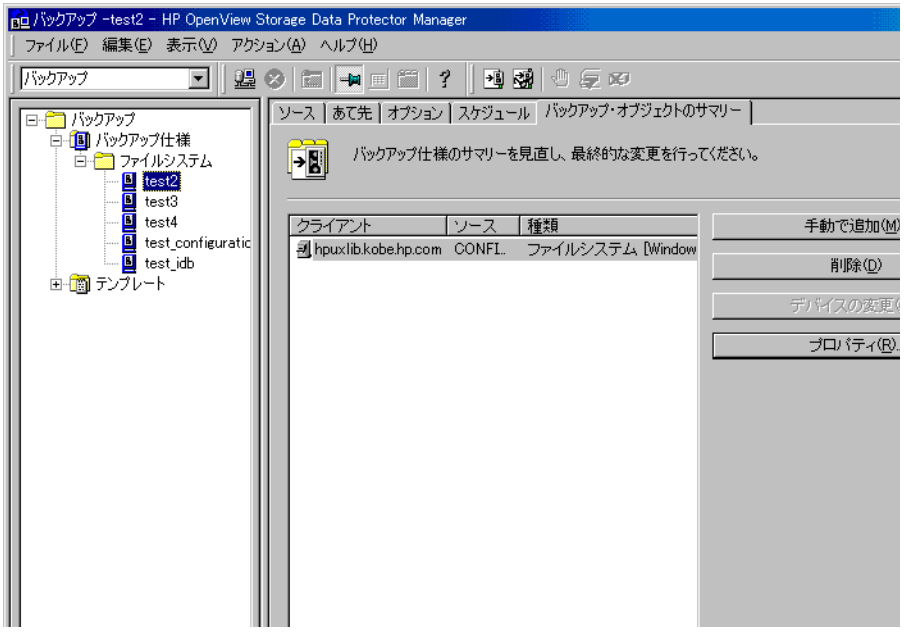
複数の Disk Agents の手動による定義

複数の Disk Agents (DA) を通じて 1 つのマウント・ポイントをバックアップする場合、[手動で追加] 機能を使って各オブジェクトを個別に指定する必要があります。各オブジェクトに新しい説明を追加し、[手動で追加] ウィザードの `[-trees]/[-exclude]` オプションを使って、オブジェクトのパスを指定します。詳細は、図 6-9 を参照してください。

また、以下の事項を検討してください。

- データ領域の分割を手動で定義することが必要です。このとき、同一データを複数の領域に重複して指定しないよう注意してください。
- 複数の DA が同じマウント・ポイントに同時にアクセスしていて、このマウント・ポイントが 1 つのディスクとして定義されている場合、ディスクからデータを取り込む性能が低下します。ディスク・アレイを使用すれば、性能の低下を避けることができます。

図 6-9 **[手動で追加] 機能を使ったオブジェクトの指定**



詳しい手順については、オンライン・ヘルプの索引キーワード「同時処理数」を参照してください。

CONFIGURATION のバックアップ

Data Protector の CONFIGURATION オブジェクトは、Windows オペレーティング・システムが持つデータ構造では、論理ドライブ (C: または D: など) がバックアップ対象として選択された場合、ファイルシステム・バックアップの一部として扱われません。

Windows の CONFIGURATION

CONFIGURATION は、以下のオブジェクトで構成されています。

- EventLog
- Profiles
- Registry
- SystemRecoveryData
- EISA Utility Partition

- WINS、DHCP(Windows TCP/IP プロトコル・サーバの場合)
- QuotaInformation、RemovableStorageManagementDatabase、FileReplicationService
- **System State(システム状態)** サービス

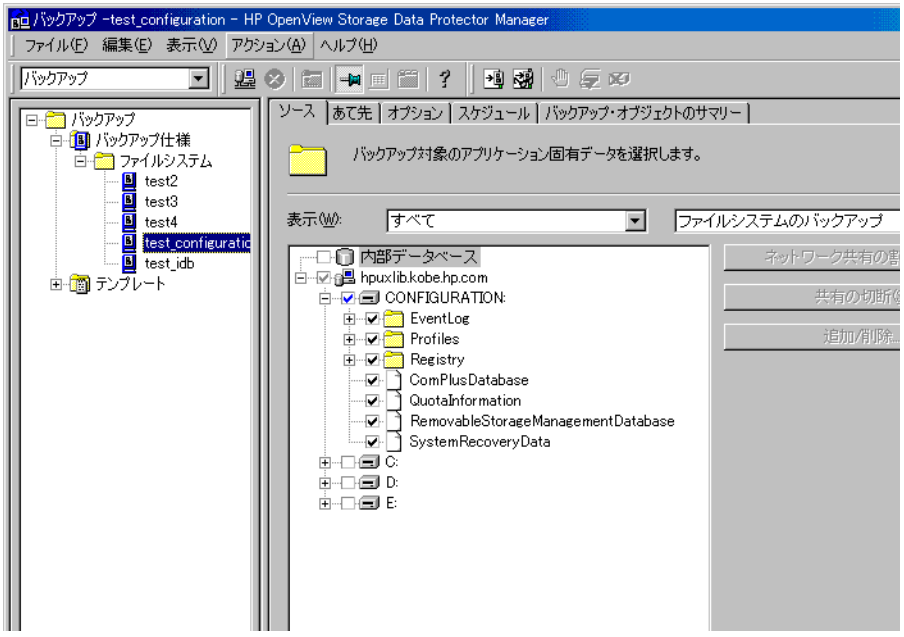
  「Windows のシステム状態のバックアップ」(235 ページ) を参照してください。
- DNSServerDatabase

  「WINS、DHCP、DNS サーバのバックアップ」(238 ページ) を参照してください。
- SysVol

  SysVol は、ドメインのパブリック・ファイルのサーバ・コピーを保存する共有ディレクトリで、ドメイン内のすべてのドメイン・コントローラ間で複製されます。
- IIS

  Microsoft Internet Information Server は、ネットワーク用ファイル / アプリケーション・サーバで、複数のプロトコルをサポートしています。IIS は、主に Hypertext Markup Language (HTML) ページ内の情報を Hypertext Transport Protocol (HTTP) を使って送信します。

図 6-10 Windows の CONFIGURATION



CONFIGURATION は、Microsoft Windows の各バージョンによって異なります。

CONFIGURATION のバックアップ

システム上では 1 度に 1 つの CONFIGURATION のバックアップしか実行できません。[バックアップ] ウィザードでクライアントを展開して、CONFIGURATION を選択します。

「バックアップ仕様の作成例」（213 ページ)、および図 6-10 を参照してください。

Windows のシステム状態のバックアップ

Windows のシステム状態は、Windows のさまざまな面に関連するいくつかの要素で構成されています。これらは、各 Windows バックアップ・オブジェクトの下に構成されています。Windows のシステム状態には、以下の構成要素が含まれます。

- Registry と ComPlusDatabase

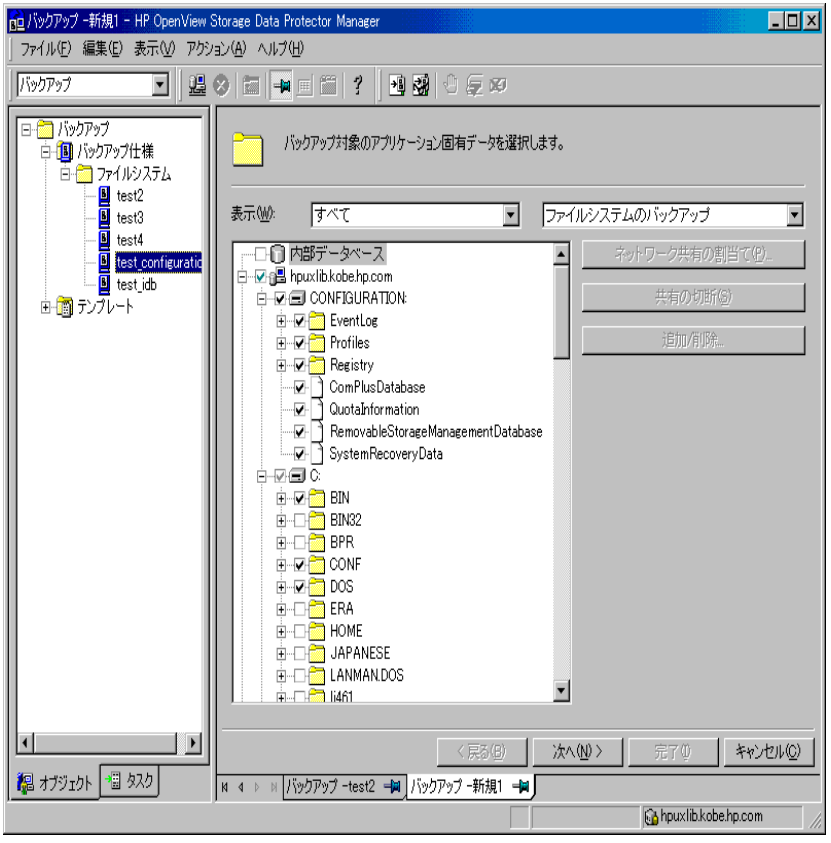
- 以下のブート・ファイル：Ntldr.exe、Ntdetect.com、boot.ini
- System Volume Information ディレクトリ。このディレクトリには、System File Protection (SFP) サービスがアクセスするデータが保存されています。

サービスのインストールと構成が行われている場合は、Windows Server システムのシステム状態データには以下も含まれます。

- ActiveDirectoryService
- CertificateServer
- TerminalServiceDatabase

バックアップ手順の詳細は、「バックアップ仕様の作成例」（213 ページ) を参照してください。図 6-11 に、[バックアップ] ウィザードでシステム状態を選択する方法を示します。

図 6-11 Windows のシステム状態

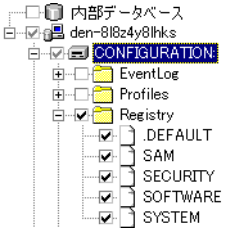


Windows レジストリのバックアップ

データベース・レポジトリに格納される情報には、レジストリと呼ばれる Windows のシステム構成が含まれます。Windows のレジストリは、システム動作に重要な役割を果たすもので、定期的にバックアップすることが必要です。

レジストリは、CONFIGURATION の一部としてバックアップすることも、図 6-12 に示すとおり Registry フォルダを選択して個別にバックアップすることもできます。

図 6-12 **Windows レジストリのバックアップ**



WINS、DHCP、DNS サーバのバックアップ

WINS、DHCP、DNS サーバ

TCP/IP ネットワークでは、Windows サーバ上で以下のサービスを構成して実行することができます。

- **WINS サーバ**

  Windows Internet Name Service とも呼ばれ、NetBIOS 名を TCP/IP ネットワーク上で使用される IP アドレスに登録したり解決するデータベース・サービスです。このデータベースは動的に複製されます。

  このデータベースをバックアップするには、[バックアップ] ウィザードで [WINS] を選択します。

- **DHCP サーバ**

  Dynamic Host Configuration Protocol (DHCP) クライアントに対して、IP アドレスの動的割り当てやネットワーク構成を行うサービスです。

  このデータベースをバックアップするには、[バックアップ] ウィザードで [DHCP] を選択します。

- **DNS サーバ**

  Domain Name System サーバ上で実行され、独自のデータベースを持つサービスです。DNS サーバは、DNS 名要求に対する応答、照会、更新を行います。

  このデータベースをバックアップするには、[バックアップ] ウィザードで [DNSServerDatabase] を選択します。

Windows サービスのバックアップ

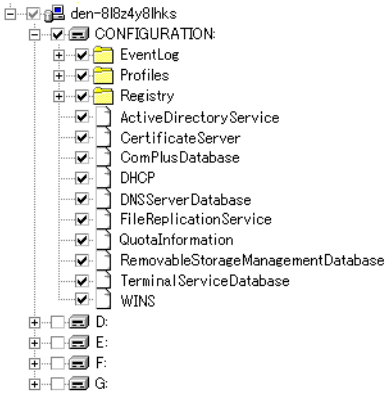
Windows サービスのバックアップとは、各サービスが使用するデータ構造のバックアップを指します。データベースはファイルにエクスポート (ダンプ) された後、バックアップされます。Windows サービスは、[バックアップ] ウィザードで CONFIGURATION が選択されている場合は必ずバックアップされます。

注記

Data Protector が検出して [バックアップ] ウィザードに選択可能項目として表示するサービスは、現在稼動中のサービスだけです。バックアップ時に稼動していないサービスがあると、対応するバックアップ・オブジェクトはバックアップされません。詳しくは、「失敗したバックアップの管理」(335 ページ) を参照してください。

あるサービスをバックアップするには、CONFIGURATION バックアップ・オブジェクトの下にある、目的のサービスのフォルダを選択します。

図 6-13 Windows サービスのバックアップ



手順の詳細は、「バックアップ仕様の作成例」(213 ページ) を参照してください。

Data Protector では、以下の Windows サービスの検出とバックアップを行えます。

- COM+ Event System

加入している COM+ コンポーネントにイベントを自動配布するサービスです。このデータベースをバックアップするには、[バックアップ] ウィザードで [ComPlusDatabase] を選択します。

- Removable Storage(取り外し可能記憶デバイス)

  取り外し可能なメディア、ドライブ、ライブラリを管理するサービスです。このデータベースをバックアップするには、[バックアップ] ウィザードで [RemovableStorageManagementDatabase] を選択します。

重要

Removable Storage データベースはバックアップできますが、このサービスは Data Protector メディア管理には使用できません。Data Protector でデバイスを構成する前に、ロボティクスのメディア・チェンジャで使用するロボティクス用ネイティブ・ドライバを使用不可能に設定しておく必要があります。

詳細は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

- Active Directory サービス

  Active Directory サービスは、Windows サーバのディレクトリ・サービスで、ネットワークを通じてデータ構造を管理できます。たとえば、Active Directory サービスでは、ユーザー・アカウント、パスワード、電話番号、プロファイル、インストールされているサービスに関する情報が保存されます。このサービスにより、ディレクトリのデータを保存したり、このデータをネットワーク・ユーザーや管理者が使用できるようにすることができます。

  ローカル・システムに保存されている Active Directory のデータ構造をバックアップするには、[バックアップ] ウィザードで [ActiveDirectoryService] を選択します。

- Terminal Service

  マルチ・セッション環境を利用可能にするサービスで、サーバ上で実行されている Windows の仮想デスクトップ・セッションや Windows ベースのプログラムへのクライアント・システムのアクセスを可能にします。

このデータベースをバックアップするには、[バックアップ] ウィザードで [TerminalServiceDatabase] を選択します。

- Certificate サービス

  公開鍵方式に基づく暗号化技術に採用されている認証情報の発行、取り消し、管理を行うサービスです。このデータベースをバックアップするには、[バックアップ] ウィザードで [CertificateServer] を選択します。

  Active Directory を使って、認証取り消しリスト (CLR) などを発行する場合は、Active Directory サービスと Certificate サービス共にバックアップしてください。

- Remote Storage Service

  Remote Storage Service (RSS) を使用すると、頻繁にアクセスされないファイルをローカルからリモート記憶装置へ自動的に移動できます。リモートに移動したファイルがオープンされた場合、そのファイルは自動的に呼び戻されます。RSS データベースはシステム状態データの一部ですが、手動でバックアップします。詳細は、「Remote Storage Service データベースのバックアップ」（242 ページ) を参照してください。

- System File Protection サービス

  System File Protection (SFP) サービスは、コンピュータの再起動後、保護されているすべてのシステム・ファイルのバージョンのスキャンと検証を行うサービスです SFP サービスは、保護されているファイルが上書きされたことを検出した場合、このファイルの正しいバージョンを検索して、検出した不適切なファイルと置き換えます。Data Protector を使うと、保護されているファイルを上書きせずにバックアップして復元できます。保護されているファイルをバックアップするには、ファイルシステムの標準バックアップ手順の [使用中のファイルを移動] オプションを使用します。

- DNS、DHCP、WINS

  「WINS、DHCP、DNS サーバのバックアップ」（238 ページ) を参照してください。

DFS のバックアップ

Data Protector では、Windows の DFS (分散ファイルシステム) を以下のいずれかの項目の一部としてバックアップします。

- Windows のレジストリ - DFS がスタンドアロン・モードで構成されている場合。
- Windows Active Directory - DFS がドメイン・モードで構成されている場合。

Remote Storage Service データベースのバックアップ

Data Protector では、ファイルシステムの標準バックアップ手順を使って Remote Storage Server (RSS) データベースをバックアップできます。RSS データベースはオフラインでバックアップすることが必要です。Remote Storage Service の終了と再起動は、実行前 / 実行後スクリプトを使って実行することも、バックアップの前後に手動で行うこともできます。以下のコマンドを使用します。

```
net stop/start "Remote Storage Engine"

net stop/start "Remote Storage File"
```

RSS データベースは以下のディレクトリにあります。

```
<%SystemRoot%>¥System32¥RemoteStorage

<%SystemRoot%>¥System32¥NtmsData
```

Windows ユーザー・プロファイル、イベント・ログ、ユーザー・ディスク・クォータのバックアップ

ユーザー・プロファイル

ユーザー・プロファイルには、ユーザー構成に関する情報が格納されています。この情報には、プロファイル・コンポーネント (デスクトップ設定、画面の表示色、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、ユーザー・プロファイルが読み込まれ、ユーザー・プロファイルに応じて Windows 環境が設定されます。

ユーザー・プロファイル・データは、¥Documents and Settings ディレクトリに存在します。

上記のディレクトリには、システム上で構成されているすべてのユーザー・プロファイルが格納されており、Data Protector によってバックアップされます。システムが複数ユーザー向けに構成されている場合、定義されている各ユーザーごとに個別のユーザー・プロファイルが設定されます。たとえば、All Users には、定義されているすべてのユーザーに共通のプ

ロファイル・コンポーネントが格納され、Default User には、新規作成されたユーザーに割り当てられたプロファイル・コンポーネントが格納されます。

Data Protector は、以下のレジストリ・キーからプロファイルの位置を読み取ります。

HKEY_USERS¥.DEFAULT¥Software¥Microsoft¥Windows¥¥

CurrentVersion¥Explorer¥Shell Folders

上記のディレクトリには、共通プロファイル・コンポーネントに関する情報が格納されています。

HKEY_USERS¥.DEFAULT¥Software¥Microsoft¥Windows¥¥

CurrentVersion¥Explorer¥User Shell Folders

注記

CONFIGURATION と Windows システムのパーティション全体を 1 つのファイルシステムとしてバックアップした場合 Profiles は、2 回バックアップされます (つまり、1 回はファイルシステム・バックアップとして、もう 1 回は CONFIGURATION の一部としてバックアップされます)。この状況を避けるには、プロファイル・データをファイルシステム・バックアップから除外します (データがあるディレクトリについては上記を参照してください)。

「システム・ディスクのバックアップ時の警告」(335 ページ) も参照してください。

イベント・ログ

イベント・ログとは、イベント (サービスの起動 / 停止、ユーザーのログオン / ログオフ) に関する情報を Windows が保存するファイルです。

ユーザー・ディスク・クォータ

ユーザー・ディスク・クォータにより、拡張トラッキング機構が使用可能となり、Windows 上のディスク・スペース使用量を制御できます。

Data Protector は、システム全体と構成されているすべてのユーザーに対するユーザー・ディスク・クォータを一度にバックアップします。

[バックアップ] ウィザードで CONFIGURATION が選択されていれば、イベント・ログ、ユーザー・プロファイル、ユーザー・ディスク・クォータは常にバックアップされます。

手順の詳細は、図 6-10「Windows の CONFIGURATION」、および「バックアップ仕様の作成例」(213 ページ) を参照してください。

ディスク・ディスカバリによる Windows クライアントのバックアップ

クライアントをデータ・ソースとして指定することにより、ディスク・ディスカバリを使用できます。後で別のディスクを追加した場合でも、追加したディスクはバックアップの対象となります。

ディスクはどのようにして検出されるか

ディスク・ディスカバリを使ってクライアント・バックアップを指定した場合、Data Protector は、まずクライアントにアクセスして、そのクライアントの物理ディスクに属しているすべての論理ディスク・ドライブを検出します (ただし、CD と取り外し可能なドライブを除く)。次に、Data Protector は CONFIGURATION フォルダと検出した論理ドライブを通常のファイルシステムとしてバックアップします。これらのファイルシステム・オブジェクトの説明用テキストは、ドライブを示す文字を角括弧で囲んで [クライアント・バックアップ] の説明に追加することで生成されます。

どのような場合にディスク・ディスカバリを使用するか

この種類のバックアップは、以下の状況で使用することをお勧めします。

- 比較的容量の小さいディスクを持つバックアップ・システムをバックアップする場合
- 障害復旧に備えてシステム全体をバックアップする場合
- システムに接続されているディスクの数がさまざまな場合

ディスク・ディスカバリを使ってクライアント・バックアップを行う場合、特定のディレクトリ・ツリーだけを選択することはできません。これは、単一の論理ドライブのバックアップを示すことになるためです。ただし、バックアップから任意のディレクトリを除外することはできます。

バックアップの実行方法

Windows クライアントのバックアップを実行するには、「バックアップ仕様の作成例」(213 ページ) の説明に従ってバックアップ仕様を作成する必要があります。

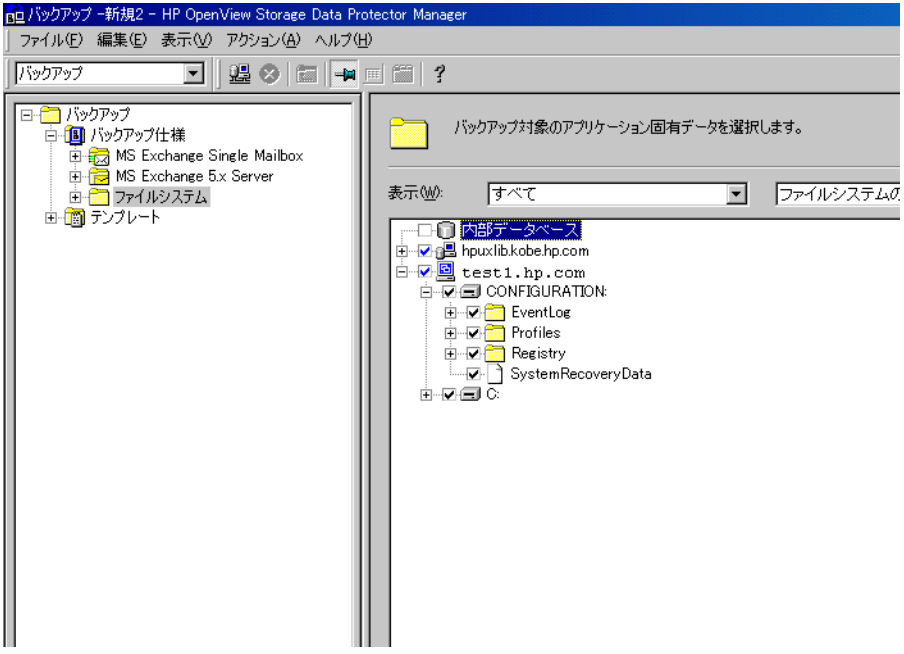
[バックアップ] ウィザードの [ソース] プロパティ・ページで、クライアント名の横にあるチェックボックスをクリックして、ディスク・ディスカバリ機能を有効にします。以降はウィザードの指示に従って操作を行います。

注記

クライアントのすべてのドライブを選択するという操作と、クライアント・システム名の横のチェックボックスをクリックするという操作は全く別のものです。後者はディスク・ディスカバリによるバックアップを行うための手順です。

構成済みのバックアップの種類を調べるには、[バックアップ・オブジェクトのサマリー] プロパティ・ページを表示します。ディスク・ディスカバリによるバックアップが構成されている場合は、[オブジェクトの種類] ラベルに [クライアント・システム] と表示され、ディスクのみが選択されている場合は、[ファイルシステム] と表示されます。

図 6-14 **クライアントの選択**



バックアップ仕様の使用および設定方法については、「バックアップ・オプションの使用」(290 ページ) を参照してください。

Windows 共有ディスクのバックアップ

Data Protector では、Windows 共有ディスク上のデータをバックアップできます。この場合、通常の Disk Agent クライアントを使用することが必要です。このクライアントを使うと、共有ディスクを通じて他のリモート・システムをバックアップできます。次に、バックアップ仕様を構成できます。

注記

共有ディスクを使ったバックアップは、この方法以外にバックアップできないシステムをバックアップするための対応策です。したがって、このバックアップ方法をメインのバックアップ方法として使用しないことをお勧めします。

どのような場合に共有ディスクのバックアップを使用するか

共有ディスクのバックアップは、以下のいずれかの状況で使用します。

- リモート・システムが Data Protector セルの一部でなく、かつシステムに Data Protector Disk Agent がインストールされていない場合
- Data Protector が直接サポートしていないプラットフォーム (Windows 3.11 など) をバックアップする場合

ヒント

ネットワーク負荷を軽減するため、Disk Agent クライアントと Media Agent クライアントは同一クライアントにします。そうでない場合は、データはネットワーク上で 2 度転送されます。

1 台の Windows クライアントを使って、共有ディスクまたは他のリモート・システムに関するバックアップや復元を管理できます。一度に多数のバックアップ・セッションを開始すると、バックアップ性能が低下する可能性があります。これは、バックアップ対象となる各ディスクにつき 1 つの Disk Agent が起動されるためです。このような場合は、Disk Agent クライアントを追加構成して、バックアップ速度を上げる必要があります。

制限事項

VSS 機能を使用してネットワーク共有ボリューム上にデータを格納しているライターのバックアップはサポートされていません。

必要条件

- Windows の GUI を使用します。UNIX システムの GUI では Windows システムのブラウズはサポートされていないからです。

- 共有ドライブは、[バックアップ] ウィザードを使って割り当てることが必要です。

重要

Disk Agent クライアントには、共有ディスクにアクセス可能なユーザー・アカウントを使って Inet サービスを構成しておくことが必要です。このアカウントはシステム・アカウントではなく、ユーザー・アカウントでなければなりません。適切なログオン・アカウントの使用方法については、「Data Protector Inet サービスに対するユーザー・アカウントの設定」(248 ページ) を参照してください。

Inet サービスにユーザー・アカウントを設定した後は、ローカル・システム上にあるディスクと同様に共有ディスクをバックアップすることができます。

Windows 共有ディスクのバックアップ方法

1. [Data Protector Manager] で [バックアップ] コンテキストを選択します。
2. [バックアップ] を展開した後、[バックアップ仕様] をダブルクリックします。
3. [ファイルシステム] を右クリックし、[バックアップの追加] をクリックします。
4. [バックアップの新規作成] ダイアログ・ボックスで、利用可能なテンプレートのいずれかを選択し、[OK] をクリックしてウィザードを起動します。
5. ウィザードの最初のページのドロップダウン・リストで [ネットワーク共有のバックアップ] を選択します。
6. [ネットワーク共有の割当て] をクリックします。[ネットワーク共有のブラウズ] ダイアログ・ボックスが表示されます。
7. [クライアント・システム] ドロップダウン・リストで、リモート・システムのバックアップに使用する Disk Agent がインストールされているクライアントを選択します。
8. 共有ディスクを選択します。選択した共有ディスクが [共有名] テキスト・ボックスに表示されます。

9. 必要な情報を入力します。詳細はオンライン・ヘルプを参照してください。

注記

ネットワーク上でディレクトリが共有されている場合、デフォルトで共有情報がバックアップされます。復元時に、デフォルトで共有情報が復元され、復元後にネットワーク上でディレクトリが共有されます。この動作を変更するには、[ファイルシステム・オプション] ウィンドウで、[ディレクトリ共有情報のバックアップ] オプションをオフにします。

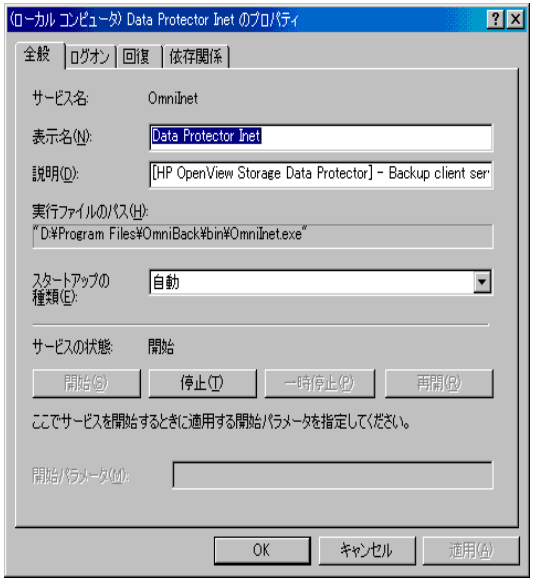
Data Protector Inet サービスに対するユーザー・アカウントの設定

Data Protector Inet サービスがリモート・コンピュータに属するディスクにアクセスする際に使用するユーザー・アカウントを変更する方法を以下に示します。このアカウントには、ローカル・クライアントとリモート共有ディスクの両方にアクセスするための権限が設定されていなければなりません。また、このアカウントはシステム・アカウントではなくユーザー・アカウントであることが必要です。

以下の手順に従って、Windows Disk Agent クライアント上でユーザー・アカウントを変更します。

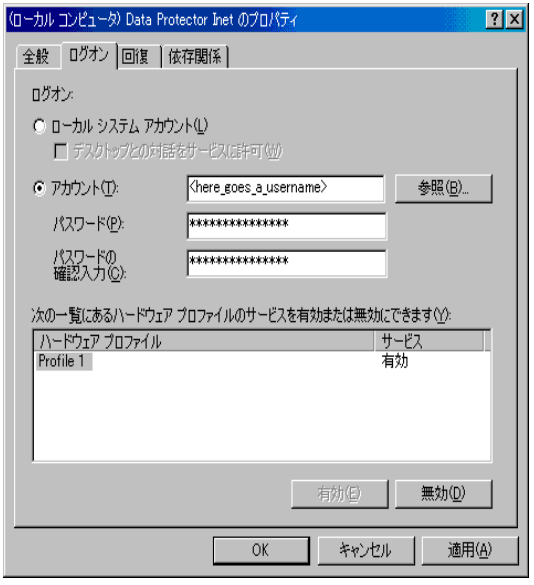
1. [コントロール パネル] ウィンドウで [管理ツール] をクリックし、[サービス] をダブルクリックします。
2. サービス・リストを下へスクロールして [Data Protector Inet] を選択します。
3. [全般] プロパティ・ページで [停止] をクリックします。[ログオン] タブを選択します。

図 6-15 Windows の Inet 用 [全般] プロパティ・ページ



4. [ログオン] で、[アカウント] ボタンを選択します。
5. バックアップ対象の共有ディスクにアクセスするための正しい権限を持つアカウントを入力するか、リストをブラウズして選択します。
6. パスワードを入力し、確認のためもう一度パスワードを入力します。

図 6-16 **Windows の Inet 用ログオン・オプション**



7. [適用] をクリックして変更内容を適用した後、[全般] プロパティ・ページの [開始] ボタンをクリックしてサービスを再開します。

Windows ディスクをディスク・イメージ・オブジェクトとしてバックアップする

ディスク・イメージ・バックアップ とは

ディスク・イメージ・バックアップとは、ディスク、ディスク・パーティション、または論理ボリュームを、データ・ソースに保存されているファイルやディレクトリ構造をトラッキングせずに高速バックアップしたものを指します。

どのような場合にディスク・イメージ・バックアップを使用するか

ディスク・イメージ・バックアップは、以下の状況で使用します。

- 容量の小さいファイルが多数あり、高速バックアップが必要な場合。
- 障害復旧用またはソフトウェアのメジャー・アップデートを行う前などにディスクのフル・バックアップが必要な場合。

- 2 つのディスク間を直接接続できない場合に、一方のディスクへファイルシステムを複製する場合。この場合、2 つのディスクは同一でなければなりません。

ディスク・イメージ・セクションの指定方法

ディスク・イメージ・セクションの指定方法は 2 通りあります。ゼロ・ダウンタイム・バックアップ (スナップショットまたはスプリット・ミラー) の場合は、2 番目の方法を使用する必要があります。

- ¥¥.¥<*drive_letter*> (例 : ¥¥.¥E:)
- ¥¥.¥PHYSICALDRIVE#

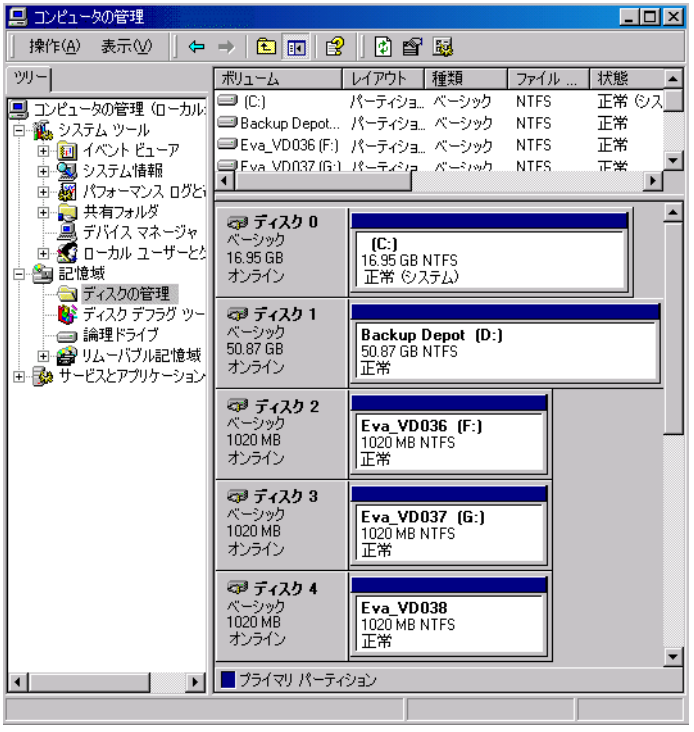
  上記で、# はバックアップするディスクの現在の番号を示します。

  例 : ¥¥.¥PHYSICALDRIVE3

ディスク番号 (物理ドライブ番号) の場所

Windows システムでディスクの現在の番号 (およびドライブ文字) を確認するには、[コントロールパネル]、[管理ツール]、[コンピュータの管理]、[記憶域]、[ディスクの管理] を順にクリックします。

図 6-17 **Windows システム上のディスク番号 (物理ドライブ番号)**



注記

システムが再起動されると、ディスク番号が変わる可能性があります。

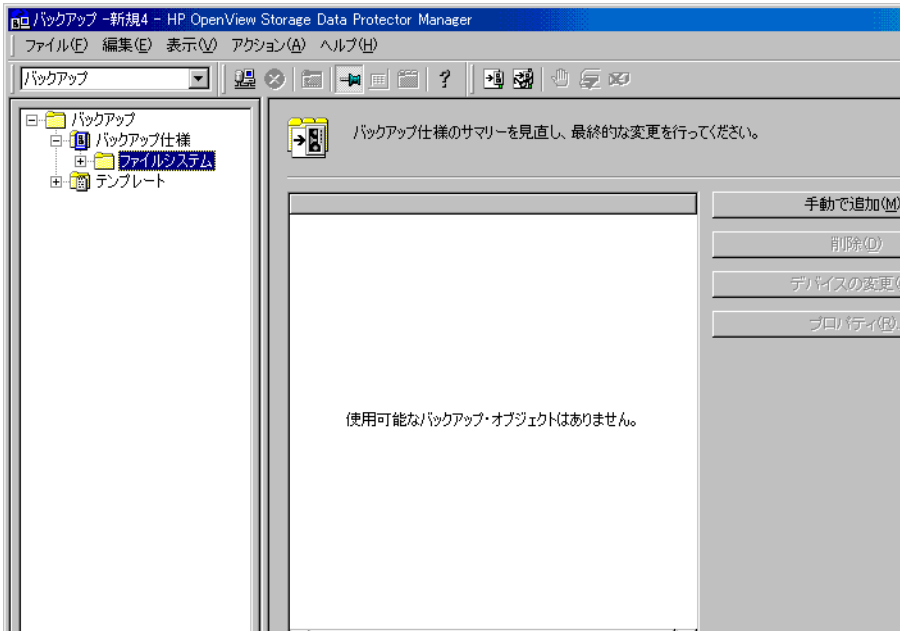
制限事項

ターゲット・システム上のファイルがオープンされていると、Data Protector はそのファイルをロックできないので、ディスク・イメージをバックアップできません。

ディスク・イメージ・バックアップの実行方法

ディスク・イメージ・バックアップを実行するには、[バックアップ・オブジェクトのサマリー] ページの [手動で追加] 機能を使用します。詳しい手順については、オンライン・ヘルプの索引キーワード「バックアップ、ディスク・イメージ」を参照してください。

図 6-18 [手動で追加 ...] 機能



Novell NetWare システムのバックアップ

本項では、Novell NetWare ファイルシステムと NDS/eDirectory のバックアップ方法を説明します。

Novell NetWare ファイルシステム (ボリューム) のバックアップ

必要条件

Novell NetWare システムのデータをバックアップするには、Novell NetWare システムに Novell NetWare Disk Agent をインストールします。インストール手順については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

Novell NetWare システムに接続されたバックアップ・デバイスを Data Protector で使用するには、Novell NetWare システムに General Media Agent をインストールします。インストール手順については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

Novell NetWare システムのバックアップ方法

Novell NetWare ファイルシステムをバックアップするには、以下の手順を行います。

1. [HP OpenView Storage Data Protector Manager] で [バックアップ] コンテキストを選択します。
2. [バックアップ] を展開した後、[バックアップ仕様] を右クリックし、[バックアップの追加] をクリックします。
3. [バックアップの新規作成] ダイアログ・ボックスで、利用可能なテンプレートのいずれかを選択し、[OK] をクリックしてウィザードを起動します。
4. ドロップダウン・リストで [ファイルシステムのバックアップ] を選択します。
5. データをバックアップするクライアントを展開します。
6. バックアップ・オブジェクトを選択します。ウィザードの指示に従って、バックアップ・デバイスを選択します。

7. ウィザードの次のページで、[ファイルシステム・オプション]の [拡張] ボタンをクリックして、[ファイルシステム・オプション] ダイアログ・ボックスを表示します。[NetWare オプション] タブをクリックして、バックアップ・オプションを設定します。各オプションの詳細は、「オブジェクト・オプション」(306 ページ) を参照してください。
8. ウィザードの指示に従って操作を行い、バックアップの保存や開始を行います。

バックアップの対象 ディレクトリ構造とファイル、および以下のファイルシステム情報がバックアップされます。

- DOS、Mac、NFS、Long の 4 つのネーム・スペース情報
- トラスティ情報
- 継承された権限マスク
- ファイルおよびディレクトリの属性
- 時間属性 (作成日時、変更日時、最終アクセス日時、最終変更日時、最終アーカイブ日時)
- オーナー
- 所有側のネーム・スペース
- 検索モード
- ボリュームまたはディレクトリ空間の制限。ボリュームの制限をバックアップするには、ボリューム・オブジェクト全体のバックアップを選択します。

サーバ固有の情報は、CONFIGURATION マウント・ポイントの一部として個別にバックアップされます。

ファイルのバックアップが完了するたびに、ファイルのアーカイブ・フラグがクリアされ、アーカイブ時間が設定されます。

バックアップの対象とならないもの Data Protector では、[読み取り禁止] オプションが設定されているファイルで、共有アクセス用にオープンされているものはバックアップできません。アプリケーションが特定のファイルを特定の回数だけ使用した後でそのファイルを解放するように動作している場合は、[再試行回数] オプションを設定すると、ファイルがバックアップされる確率が高くなります。

- キュー・ディレクトリ内のシステム・ファイルはバックアップされませ

ん。

- NDS/eDirectory に所属しているファイルは、すべてスキップされます。NDS/eDirectory は、ファイルシステムとは別にバックアップできます。
- 拡張属性 (NetWare 追加属性としてインストール可能な属性) は、バックアップされません。

制限事項

NetWare では以下のオプションは使用できません。

- ［バックアップ時にファイルをロック］、［圧縮 ］、［アクセス時刻属性を保存しない］の各バックアップ・オプション
- `omit_deleted_files` 復元オプション

Novell Storage Management Services (SMS) の制限により、NetWare 5.1 でバックアップ可能なファイルの最大サイズは 4GB です。他の Novell NetWare システムのファイル・サイズに制限はありません。

Novell NetWare システム上でユーザーによるバックアップの実行を許可する場合は、ユーザーに［ ルート・ユーザーとしてバックアップ ］ユーザー権限が必要です。ユーザー権限の変更方法の詳細は、第 4 章「ユーザーとユーザー・グループの 構成」(135 ページ) を参照してください。

Data Protector は、増分バックアップ・セッション時には**移動されたファイル**をバックアップできません。

Data Protector Disk Agent は、どのファイルが変更されたかを判別するため、各ファイルの前回変更日時を調べます。この方法では、移動されたファイルは検出されません。ファイルを移動しても、ファイルの変更日時は変わらないからです。

増分バックアップの詳細は、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

特定のファイルまたはディレクトリの選択

各ファイルシステムでは、特定のディレクトリ・ツリーだけをバックアップすることができます。各ディレクトリ・ツリーに対して以下を実行できます。

- サブツリーまたはファイルを除外する
- 特定のワイルドカード指定に一致するファイルだけをバックアップする
- 特定のワイルドカード指定に一致するファイルだけを除外する

CONFIGURATION のバックアップ

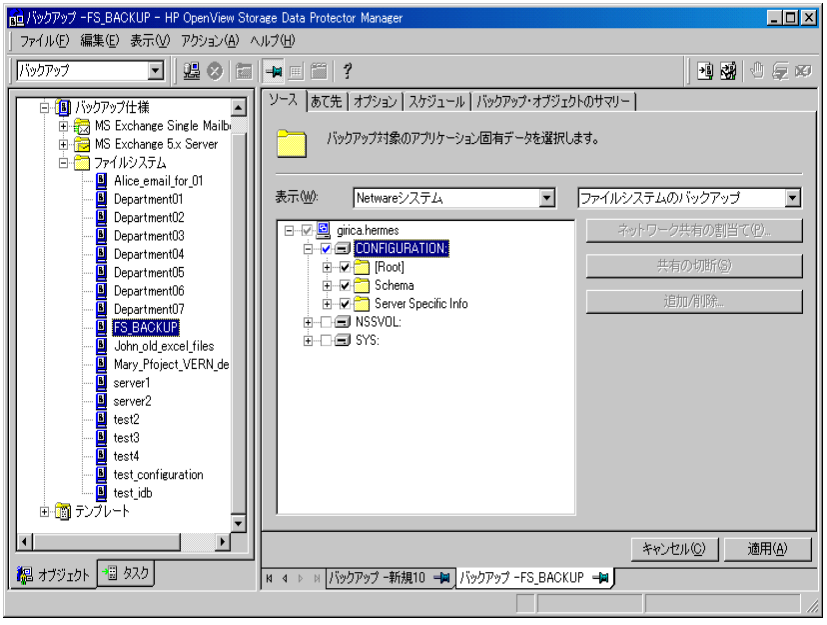
Data Protector では、CONFIGURATION と呼ばれる特殊なデータ構造をバックアップできます。CONFIGURATION は、図 6-19 に示すとおり、以下のコンポーネントで構成されています (NetWare 5.x および 6.x の場合)。

CONFIGURATION のコンポーネント

- サーバ固有の情報
- スキーマ
- Root

CONFIGURATION オブジェクト全体またはその一部をバックアップするには、「Novell NetWare システムのバックアップ方法」(254 ページ) の手順に従って操作を行い、[バックアップ] ウィザードの [ソース] ページで適切な項目を選択します。

図 6-19 NetWare 5.x Configuration のバックアップ



ディスク・ディスカバリによるクライアントのバックアップ

NetWare 上のディスク (ボリューム) の検出は、UNIX または Windows システムの場合と同様に行えます。

ディスクはどのようにして検出されるか

ディスク・ディスカバリを使ってクライアント・バックアップを指定した場合、Data Protector は、まずクライアントにアクセスして、そのクライアントに属しているすべてのボリュームを検出します。次に、Data Protector は CONFIGURATION 項目と検出したボリュームを通常のファイルシステムとしてバックアップします。各ファイルシステム・オブジェクトの説明用テキストは、ドライブを示す文字を角括弧で囲んで [クライアント・バックアップ] の説明に追加することにより生成されます。

ディスク・ディスカバリを使ってクライアント・バックアップを行う場合、特定のディレクトリ・ツリーだけを選択することはできません。これは、単一ボリュームのバックアップを示すことになるためです。ただし、バックアップから任意のディレクトリを除外することはできます。

NetWare クライアント・バックアップの実行方法

1. [Data Protector Manager] で [バックアップ] コンテキストを選択します。
2. [バックアップ] を展開した後、[バックアップ仕様] をダブルクリックします。
3. 結果エリアで [ファイルシステム] を右クリックして [バックアップの追加] をクリックします。
4. [バックアップの新規作成] ダイアログ・ボックスで、使用可能なテンプレートをいずれか 1 つ選択します。
5. [OK] をクリックして、[バックアップ] ウィザードを起動します。
6. クライアントの横のチェックボックスをクリックします。これにより、図 6-14 に示すとおり、バックアップ対象としてクライアント・システム全体が選択されます。

バックアップ仕様の使用および設定方法については、「バックアップ・オプションの使用」(290 ページ) を参照してください。

NDS/eDirectory のバックアップ

Data Protector は、Novell NetWare Storage Management Services (SMS) を使って NDS/eDirectory をバックアップします。Data Protector は、すべての拡張子を NDS/eDirectory スキーマにバックアップ / 復元します。

注記

NDS/eDirectory データベースの増分バックアップを行うことはできません。NDS/eDirectory データベースについては常にフル・バックアップが実行されます。

NDS/eDirectory を正しくバックアップするには、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』の手順に従っており、以下を行っていることを確認してください。

- `TSANDS.NLM` をロードしていること
- `HPLOGIN.NLM` をロードしており、Data Protector にアクセス情報が提供されていること

NDS/eDirectory のバックアップ

NDS/eDirectory のバックアップは、UNIX または Windows ファイルシステムの場合と同様の手順で行いますが、マウント・ポイントを `CONFIGURATION` にする点が異なります。

NDS/eDirectory オブジェクトをバックアップ仕様に追加する

Data Protector は、NDS/eDirectory の一部だけをバックアップする高度な機能を備えています。ただし、NDS の一部をバックアップから除外する理由を理解していない場合は、NDS 全体をバックアップすることをお勧めします。

NDS/eDirectory ツリーの各オブジェクトにはそれぞれ完全修飾名があります。たとえば、コンテナ・オブジェクトの `O=HSL` 内にあるリーフ・オブジェクト `CN=Admin` は、以下に示すとおり SMS(`TSANDS.NLM`) が認識できる完全修飾名を持っています。

```
.CN=Admin.O=HSL.[Root]
```

Data Protector は、この完全修飾名を使って以下のとおり NDS/eDirectory のツリー構造を構築します。

- 完全修飾名を逆順にします。

- ドット記号(.)の区切り文字をスラッシュ記号(/)の区切り文字に置き換えます。

たとえば、以下の完全修飾名

```
.CN=Admin.O=HSL.[Root]
```

に対応する置換名を Data Protector が使用し、以下のとおりスラッシュを使用することにより、Windows で使用できます。

```
/[Root]/O=HSL/CN=Admin
```

この命名規則を除いて、Data Protector バックアップ仕様構文は、Novell NetWare または UNIX ファイルシステム・オブジェクトの場合と同じです。

注記

NDS/eDirectory オブジェクト (コンテナ・オブジェクトとリーフ・オブジェクト) はディレクトリとして表示され、バックアップされます。これらのオブジェクトを、[スキップ] オプションを使って除外したり、[オンリー] オプションを使ってバックアップできます。Data Protector は、[Root] オブジェクトを非格納オブジェクトとして表示するため、[Root] オブジェクトは除外できません。

マウント・ポイント構成ファイル TSANDS.CFG

NDS/eDirectory データを最大限に保護するには、ディレクトリ全体のバックアップを実行して、[Root] オブジェクトから分岐するツリー内の NDS/eDirectory スキーマとすべてのコンテナをバックアップすることが必要です。とはいえ、[Root] オブジェクト以外のコンテナから NDS/eDirectory のバックアップを開始したい場合があり、しかもユーザーはバックアップを開始するコンテナのコンテキストがあるところまでブラウズするための十分な権限を持っていない場合があります。

NDS/eDirectory ツリーの一部だけを容易にバックアップするため、Novell 社はテキスト形式のファイル `SYS:SYSTEM¥TSA¥TSANDS.CFG` を提供して、バックアップを開始するコンテナの名前を指定できるようにしました。このファイルは、`TSANDS.NLM` をロードしたサーバ上にあります。

NDS/eDirectory バックアップを HSL コンテナから開始するには、以下の行を含むファイル `TSANDS.CFG` を作成します。

```
.O=HSL.[Root]
```

これにより、バックアップ構成に対して別のマウント・ポイントが使用可能になります。

OpenVMS システムのバックアップ

本項では、OpenVMS ファイルシステムのバックアップ方法を説明します。

OpenVMS ファイルシステムのバックアップ

必要条件

OpenVMS システム上のデータをバックアップするには、OpenVMS システムに OpenVMS Disk Agent をインストールします。インストール手順については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

OpenVMS システムに接続されたバックアップ・デバイスを Data Protector で使用するには、OpenVMS システムに General Media Agent をインストールします。インストール手順については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

OpenVMS システムのバックアップ方法

OpenVMS ファイルシステムをバックアップするには、以下の手順を行います。

1. [HP OpenView Storage Data Protector Manager] で [バックアップ] コンテキストを選択します。
2. [バックアップ] を展開した後、[バックアップ仕様] を右クリックし、[バックアップの追加] をクリックします。
3. [バックアップの新規作成] ダイアログ・ボックスで、利用可能なテンプレートのいずれかを選択し、[OK] をクリックしてウィザードを起動します。
4. ドロップダウン・リストで [ファイルシステムのバックアップ] を選択します。
5. データをバックアップするクライアントを展開します。
6. バックアップ・オブジェクトを選択します。ウィザードの指示に従って、バックアップ・デバイスを選択します。
7. バックアップ・オプションを選択します。詳細は、「バックアップ・オプションの使用」(290 ページ) を参照してください。

8. ウィザードの指示に従って操作を行い、バックアップの保存や開始を行います。

バックアップの対象

ディレクトリ構造とファイル、および以下のファイルシステム情報がバックアップされます。

- ファイルおよびディレクトリの属性
- ACL(アクセス制御リスト)

ファイルは、マウントされた FILES-11 ODS-2 または ODS-5 ボリュームからのみバックアップできます。

制限事項

- GUI に入力して CLI に渡すファイル仕様は、UNIX 形式の構文でなければなりません

  ```
  /disk/directory1/directory2/filename.ext.n
  ```

  — 文字列の先頭にスラッシュ (/) を付け、その後にディスク、ディレクトリ、ファイル名をスラッシュで区切って続けます。

  — ディスク名の後にコロン (:) を付けてはいけません。

  — バージョン番号の前には、セミコロン (;) の代わりにピリオド (.) を使用します。

  — OpenVMS ファイル用のファイル仕様では、大文字と小文字が区別されます。

  例 :

  OpenVMS のファイル仕様が以下の場合

  ```
  $1$DGA100:[USERS.DOE]LOGIN.COM;1
  ```

  以下の形式で指定する必要があります。

  ```
  /$1$DGA100/Users/Doe/Login.Com.1
  ```

- 暗黙のバージョン番号はありません。バージョン番号は、常に明示的に指定する必要があります。バックアップ対象として選択されたファイル・バージョンのみがバックアップされます。ファイルのすべてのバージョンをバックアップしたい場合は、GUI ウィンドウでそれらをすべて選択するか、CLI で `Only (-only)` オプションを使用してバージョン番号にワイルド・カードを使用して以下に示すとおりファイル仕様を指定します。

/DKA1/dir1/filename.txt.*

- バックアップの際に［アクセス時刻属性を保存しない］（-touch）オプションが有効になっている場合、ODS-5 ディスク上では最終アクセス日時が現在の日時で更新されます。ODS-2 ディスク上ではこのオプションは機能せず、すべての日時は変更されません。
- OpenVMS 上では、raw ディスクのバックアップはできません。「BACKUP/PHYSICAL」に相当するものはありません。
- OpenVMS 上では、[POSIX ハードリンクをファイルとしてバックアップ］（-hlink）、［ソフトウェア圧縮］（-compress）、［暗号化］（-encode）オプションは使用できません。

  複数のディレクトリ・エントリを持つファイルは、一次パス名を使用して一度だけバックアップされます。二次パス・エントリは、ソフト・リンクとして保存されます。復元の際、これらのパス・エントリも復元されます。

  「BACKUP/IMAGE」に相当するものはサポートされていません。OpenVMS システム・ディスクの復元コピーをブート可能にするには、OpenVMS WRITEBOOT ユーティリティを使用して、復元ディスクにブート・ブロックを書き込む必要があります。
- バックアップ中のファイルは、［バックアップ時にファイルをロック］（-lock）オプションの設定にかかわらず、常にロックされます。-lock オプションを有効にすると、書き込み用にオープンされているファイルはバックアップされません。また、-lock オプションを無効にすると、オープン中のファイルもすべてバックアップされます。
- 実行前 / 実行後コマンドの格納されているデフォルトのデバイスとディレクトリは、/omni$root/bin です。実行前 / 実行後コマンドを別の場所に置く場合は、ファイル仕様にデバイスとディレクトリ・パスを UNIX 形式で記述する必要があります。例 : /SYS$MANAGER/DP_SAVE1.COM
- Skip（-skip）または Only（-only）フィルタでワイルドカード文字を指定する場合、複数の文字を表す場合は「*」を、1 文字を表す場合は「?」を使用してください。

ダイレクト・バックアップ環境でのバックアップ

本項では、ダイレクト・バックアップ環境で使用するバックアップ仕様の構成手順を説明します。ダイレクト・バックアップの概念の詳細は、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

必要条件

- アプリケーションおよびバックアップ・システムは、使用されているディスク・アレイに応じて、スプリット・ミラーまたはスナップショット・バックアップ用に構成されていることが必要です。詳細は、『HP OpenView Storage Data Protector ゼロ ダウンタイム バックアップ 管理者ガイド』を参照[1] してください。
- アプリケーション・システム上の Oracle9i サーバをバックアップする場合は、使用されているディスク・アレイに応じて、アプリケーション・システムが Oracle9i スプリット・ミラーまたはスナップショット・バックアップ用に構成されていることが必要です。詳細は、『HP OpenView Storage Data Protector ゼロ ダウンタイム バックアップ インテグレーション ガイド』を参照してください。
- XCopy エンジンは、バックアップ元 (バックアップ・システムに接続されたミラー・ディスク) およびバックアップ先 (ファイバー・チャネル・ブリッジに接続されたバックアップ・デバイス) と同じ SAN 領域内で構成されていることが必要です。言い換えると、XCopy エンジンはバックアップ・システムに接続されたミラー・ディスクおよびファイバー・チャネル・ブリッジに接続されたバックアップ・デバイス双方へ、SAN を経由してアクセスできなければなりません。
- バックアップ対象のすべてのシステム (アプリケーション・システム) に、HP StorageWorks Disk Array XP エージェントがインストールされていることが必要です。詳細は、HP OpenView Storage Data Protector インストールおよびライセンス・ガイドを参照してください。
- バックアップ・デバイスを制御するすべてのシステム (バックアップ・システム) に、General Media Agent および HP StorageWorks Disk Array XP エージェントがインストールされていることが必要です。詳細は、HP OpenView Storage Data Protector インストールおよびライセンス・ガイドを参照してください。

1.

- Data Protector セル内に、最低 1 つのバックアップ・デバイスがダイレクト・バックアップ用に構成されていることが必要です。詳細は、「ダイレクト・バックアップ用のデバイスの構成」(48 ページ) を参照してください。
- バックアップ用メディアを準備することが必要です。詳細は、第 5 章「メディアの管理」(151 ページ) を参照してください。
- バックアップを実行するための適切なユーザー権限が必要です。詳細は、第 4 章「ユーザーとユーザー・グループの 構成」(135 ページ) を参照してください。

制限事項

- ダイレクト・バックアップ環境内のシステムは、HP-UX 11.11 であることが必要です。
- [負荷調整] オプションの [最小] および [最大] オプションは、ダイレクト・バックアップでは無視されます。負荷調整を使用する場合、バックアップ仕様で選択したすべてのデバイスが負荷調整の対象となります。したがって、デバイスの使用順序を決める機能を使って、選択したデバイスの使用順序を設定することはできません。
- バックアップ・オブジェクトに対する実行前 / 実行後オプションは、raw 論理ボリュームのダイレクト・バックアップには使用できません。Oracle9i のダイレクト・バックアップには使用できます。
- バックアップ・デバイスは、XCopy エンジンのある外付け FC ブリッジに接続されているか、または XCopy エンジンのある FC ブリッジが内蔵されていることが必要です。
- raw パーティション (raw ディスクまたは raw 論理ボリューム) にインストールされた Oracle データベースのバックアップと復元はサポートされていません。
- ストライプ論理ボリュームのバックアップと復元はサポートされていません。
- [CRC チェック] オプションは、ダイレクト・バックアップでは無視されます。
- Disk Agent の [同時処理数] オプションは、ダイレクト・バックアップでは無視されます。
- [ブロック・サイズ] オプションは、FC ブリッジに依存します。

- [セグメント・サイズ] および [Disk Agent バッファ] オプションは、ダイレクト・バックアップでは無視されます。
- オブジェクト・コピーおよびオブジェクト・ミラーはダイレクト・バックアップではサポートされていません。

インスタント・リカバリ

インスタント・リカバリがサポートされているのは次の場合です。

- 制御ファイルとオンラインの REDO ログが、同じ論理ボリューム上にデータ・ファイルとして存在していないこと。
- データベース全体のバックアップが実行されていること。つまり、バックアップ時に Oracle9i Server インスタンスに属するすべてのデータ・ファイルが選択されている必要があります。

復元

ダイレクト・バックアップ環境でバックアップしたデータの復元について、以下に示します

- Data Protector の raw ディスクまたは Oracle の復元手順に続いて、バックアップ・メディアから LAN 経由で直接アプリケーション・システムに復元できます。「ディスク・イメージの復元」(368 ページ)(raw ディスクの復元)、または『HP OpenView Storage Data Protector インテグレーション・ガイド』(Oracle の復元) を参照してください。
- Data Protector のインスタント・リカバリ機能を使用して復元できます。詳細は、『HP OpenView Storage Data Protector ゼロ ダウンタイム バックアップ 管理者ガイド』を参照してください。

バックアップ仕様の構成手順

ダイレクト・バックアップ仕様は、次のオブジェクトに対して構成できます。

- raw ディスク
- Oracle9i データベース (オンライン)
- Oracle9i データベース (オフライン)

raw ディスクのバックアップ

raw ディスクのダイレクト・バックアップ用のバックアップ仕様の構成方法については、オンライン・ヘルプの索引キーワード「ダイレクト・バックアップ仕様の構成」を参照してください。

Oracle9i(オンラインおよびオフライン) のバックアップ

Oracle9i(オンラインおよびオフライン) のダイレクト・バックアップ用のバックアップ仕様の構成方法については、オンライン・ヘルプの索引キーワード「ダイレクト・バックアップ仕様の構成」を参照してください。

CLI を使用したダイレクト・バックアップの開始

ダイレクト・バックアップ仕様を構成したら、GUI(前述) または CUI(以下で説明) を使用してバックアップ・セッションを開始します。

- raw ディスクの場合

  ```
  omnib -datalist <Name>
  ```

- Oracle9i(オンラインおよびオフライン) の場合

  ```
  omnib -oracle8_list <Name>
  ```

ここで、*<Name>* はダイレクト・バックアップ仕様の名前を示します。

無人バックアップのスケジュール

Data Protector では、システムのバックアップ・スケジュールを指定した時間に行うよう設定することにより、無人バックアップを構成できます。

構成とスケジュールの設定ポリシーは、バックアップの効率と性能に大きな影響を与えます。

キー・ポイント

- スケジュール作業を容易にするため、Data Protector はクライアントを分類するためのバックアップ仕様を提供しています。1 つのバックアップ仕様に構成されているすべてのクライアントは、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。
- 無人バックアップを円滑に行うため、メディアとデバイスを必ず十分に用意しておいてください。実行中のセッションのモニター方法や、マウント要求に対する電子メールまたはその他の通知手段の設定方法については、第 9 章「モニター、レポート、通知、およびイベント・ログ」(407 ページ) を参照してください。
- スケジュールされたバックアップが開始されると、Data Protector は必要なすべてのリソース (ライセンス、デバイス、IDB へのアクセス権など) を割り当てようとします。必要なリソースの内いずれかが使用不可能な場合、このセッションには待機中を示すマークが付き、同時に、Data Protector は、タイムアウトになるまで、待機中セッションに必要なリソースを毎分ごとに 1 回見つけようとします。

  Data Protector がリソースを見つけると、待ち行列に入っているセッションの内いずれかが開始されます。セッションが開始される順番は画面の表示順とは異なります。
- Cell Manager の過負荷を防止するため、同時に開始できるバックアップ・セッションの最大数は 5 個です。同時に開始するよう設定されているセッション数が 5 個を超える場合、超過分のセッションは待ち行列に入れられます。
- 個々のバックアップまたは定期的バックアップのそれぞれに対して、［バックアップの種類］(フルまたは増分)、［ネットワーク負荷］および［バックアップ保護］オプションを指定できます。スプリット・ミラーまたはスナップショットのバックアップにおいて、ZDB ディスクまたは ZDB ディスク / テープ・バックアップ (インスタント・リカバリが

有効) を行う場合は、［スプリット・ミラー / スナップショットのバックアップ］オプションを指定します。スプリット・ミラーおよびスナップショット・バックアップでは、バックアップの種類は無視されます (フル・バックアップに設定されます)。

- 各バックアップ仕様は、異なるオプションを指定して複数回スケジュールできます。1 つのバックアップ仕様に対して、ZDB ディスクおよび ZDB ディスク / テープ・バックアップの両方をスケジュールできます。また個々のバックアップまたは定期的にスケジュールされたバックアップのそれぞれに対して、異なるデータ保護期間を指定できます。
- データがメディア上に保存される期間 (データ保護) と IDB に保存される期間 (カタログ保護) は、データ保護とカタログ保護の設定値によって決まります。詳細は、「データ保護 : メディア上にデータを保存する期間を指定する」（293 ページ) および「カタログ保護 : データベース上にログ情報が保存される期間」（295 ページ) を参照してください。
- バックアップ・テンプレートを適用すると、テンプレートのスケジュール設定値によって、バックアップ仕様のスケジュール設定値が無効になります。テンプレートの適用後も、バックアップ仕様を変更して、別のスケジュールを設定できます。

注記

バックアップは最高 1 年先までスケジュールできます。ただし定期的バックアップでは、期限の上限は定義されていません。

スケジュール衝突の処理

定期的バックアップをスケジュールする際、選択したバックアップ開始時間が、同じバックアップ仕様内の別のスケジュールされたバックアップによって、すでに使用されている場合があります。この場合、Data Protector からスケジュールの衝突が発生していることを示すプロンプトが出力され、続行するかどうかを尋ねるプロンプトが表示されます。［はい］をクリックすると、設定可能な (まだ使用されていない) 日時に新しいスケジュールが設定されます。［いいえ］をクリックすると、新しいスケジュールは廃棄されます。

スケジュール・ポリシーのプランニング

以下の疑問に対する回答については、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

- 自分の環境に対するスケジュール・ポリシーについてどのようなプランを立てるか

- 設定したスケジュール・ポリシーにデータの量がどのような影響を与えるか
- バックアップにはどれぐらいの時間を要するか
- バックアップにはどれぐらいのメディアが必要か
- 障害復旧に備えてどのようなプランを立てるか

指定した日時にバックアップを開始する

Data Protector では、無人バックアップを開始する日時を指定できます。通常、指定した日時にバックアップを実行するのは、定期的なバックアップに例外を構成したい場合です。たとえば、特定のイベントの前にデータをバックアップできます。

指定した日時のバックアップを構成する方法

指定した日時のバックアップを構成するには、新たなバックアップ仕様を作成するか、既存のバックアップ仕様を変更します。詳しい手順については、オンライン・ヘルプの索引キーワード「指定した日時のバックアップのスケジュール」を参照してください。

定期的バックアップの開始

定期的バックアップは、指定した日以降一定の期間ごとに行われます。たとえば、定期的バックアップを構成することにより、フル・バックアップを日曜日の午前 3 時に行い、以降は 2 日に一度フル・バックアップが繰り返し行われるよう設定できます。2 回目のフル・バックアップが実行されるのは、火曜日の午前 3 時となります。定期的バックアップにより、通常スケジュールのバックアップに対するバックアップ構成を容易に行えます。

Data Protector は、構成を容易に行うための定義済みバックアップ・スケジュールを備えています。

定義済みバックアップ・スケジュール

定義済みバックアップ仕様を使って、構成作業を容易に行えます。スケジュールは後で変更できます。スケジュールの種類には、以下の各項で説明するものがあります。

毎日 (集中的)

Data Protector は、深夜にフル・バックアップ、毎日 12:00(正午) と 18:00 に 2 回の増分バックアップを実行します。この種類のバックアップは、データベース・トランザクション・サーバなど、バックアップを頻繁に実行する必要がある環境での使用を目的としています。

毎日 (フル)

Data Protector は毎日 21:00 にフル・バックアップを実行します。この種類のバックアップは、単一のワークステーションまたはサーバでの使用を目的としています。

毎週 (フル)

Data Protector は毎週金曜日にフル・バックアップ、月曜日から金曜日まで毎日 21:00 に増分 1 バックアップを実行します。この種類のバックアップは、小規模な環境での使用を目的としています。

隔週 (フル)

Data Protector は隔週金曜日にフル・バックアップを実行します。さらに、このバックアップの間、毎週月曜日から木曜日まで 21:00 に増分 1 バックアップを実行します。

毎月 (フル)

Data Protector は毎月 1 日にフル・バックアップ、毎週増分 1 バックアップ、1 日おきに増分バックアップを実行します。この種類のバックアップは、比較的データのやりとりの少ない環境での使用を目的としています。

定義済みスケジュールの使用方法

定義済みスケジュールを使用してバックアップを構成するには、新たなバックアップ仕様を作成するか、既存のバックアップ仕様を変更します。詳しい手順については、オンライン・ヘルプの索引キーワード「定期的バックアップのスケジュール」を参照してください。

繰り返しバックアップの構成

設定済みのスケジュールに日時を指定してバックアップが実行されるように、バックアップ・スケジュールを設定できます。たとえば、フル・バックアップが今後 6 か月間毎週金曜日 21:00 に実行されるようスケジュールできます。

繰り返しバックアップの構成方法

繰り返しバックアップを構成するには、新たなバックアップ仕様を作成するか、既存のバックアップ仕様を変更します。詳しい手順については、オンライン・ヘルプの索引キーワード「定期的バックアップのスケジュール」を参照してください。

バックアップ・スケジュールの編集

スケジュールのクリア

設定済みのスケジュールを削除するには、[スケジュール] プロパティ・ページの [リセット] をクリックします。

スケジュールをクリアした場合、今年度中に指定されているモードのすべてのスケジュール設定値がクリアされます。

クリアしたスケジュールを元に戻す

クリアしたスケジュールを元に戻すには、[スケジュール] プロパティ・ページの [元に戻す] をクリックします。

開始日を変更する

開始日を変更するには、指定した日時にバックアップを開始する手順を行います。「指定した日時にバックアップを開始する」(271 ページ) を参照してください。

スケジュールを無効にする

バックアップ・スケジュールを無効にするには、[スケジュール] プロパティ・ページで [スケジュールを使用不可能にする] オプションを選択します。これにより、このオプションの選択を解除するまで、バックアップは実行されなくなります。

バックアップ・スケジュールを無効化しても、現在実行中のバックアップ・セッションは影響されません。

休日のバックアップを省略する

Data Protector は、デフォルトでは休日にバックアップを実行します。

休日にはバックアップを実行しないようにするには、[バックアップ] ウィザードの [スケジュール] ページで [休日] オプションをオンに設定します。休日とは、`Holidays` ファイルに定義した日、またはカレンダー上に赤色でマークされている日を指します。

重要

一般には、休日にバックアップをスキップすることはお勧めできません。

定義済み以外の休日を設定するには、Cell Manager 上の Holidays ファイルを編集します。このファイルは以下のディレクトリにあります。

- UNIX Cell Manager の場合 : /etc/opt/omni/server/Holidays
- Windows Cell Manager の場合 : *<Data_Protector_home>*¥Config¥server¥holidays

Holidays ファイル内のエントリを追加または編集するときは、以下の点に注意してください。

- 各行の最初の数字は、その年の累積日数を示しています。この値は Data Protector により無視されますが、0 ～ 366 の値を設定しなければなりません。0 を設定することにより、この数字が後続の日付と対応していないことを示すことも可能です。
- 日付は Mmm d の形で指定し、Mmm 部分が月を表す 3 文字の略語、d 部分が月内の日付です (Jan 1 など)。各自のロケールとは関係なく、月名は英語で指定する必要があります。
- 休日の説明はオプションであり、現在のところ Data Protector では使われていません。

ファイルの先頭に指定する年にかかわらず、ファイル内に指定された休日は**常にそのままの形**で使用されるため、年によって日付が変わる休日は手動で変更しなければなりません。Holidays オプションをスケジューラとして使用しない場合は、Holidays ファイル内のエントリを削除またはコメントアウトしておくことにより、有効期限が切れたり、各国や各企業の要件に合わせてカスタマイズされていない Holidays ファイルが誤って使用された場合のトラブルを回避できます。

スケジュール・ポリシーをどのように構成するかによって、バックアップの効率と性能が大きな影響を受けます。たとえば、January 1 が休日として登録されている場合、Data Protector はこの日にバックアップを実行しません。フル・バックアップを 1 月 1 日、増分バックアップを 1 月 2 日に設定している場合、Data Protector は 1 月 1 日にフル・バックアップを実行しませんが、1 月 2 日には増分バックアップを実行します。ただしこの場合、増分バックアップは前回のフル・バックアップに基づいて行われます。

バックアップのスケジュール時のバックアップ・オプションの構成

バックアップをスケジュールする際、さらにオプションを設定できます。これらのオプションはスケジュールされたバックアップのみに有効で、対話形式で開始されたバックアップには無効です。[バックアップのスケジュール] ダイアログで指定されたデータ保護は、バックアップ仕様内で別に定義されている保護設定よりも優先して適用されます。

バックアップのスケジュール時のオプション指定方法

バックアップのスケジュール時のオプションを指定するには、新たなバックアップ仕様を作成するか、既存のバックアップ仕様を変更します。詳しい手順については、オンライン・ヘルプの索引キーワード「バックアップのスケジュール時のオプション指定」を参照してください。

複数のバックアップを連続して実行する

1 つのバックアップが終了した後に、別のバックアップを起動できます。たとえば、ファイルシステムのバックアップ終了後に Oracle データベースのバックアップを起動できます。詳しい手順については、オンライン・ヘルプの索引キーワード「複数のバックアップの連続実行」を参照してください。

UNIX システムでの実行前 / 実行後スクリプトの詳細については、「実行前 / 実行後コマンドの例 (UNIX の場合)」(A-21 ページ) を参照してください。

バックアップの種類の選択 フルまたは増分

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により、バックアップに要する時間とメディアを節約できます。たとえば、前回の第 1 レベルの増分バックアップに基づいて第 2 レベルの増分バックアップを行い、さらにこの増分バックアップに基づいて第 3 レベルのバックアップを行うことができます。

バックアップの種類 (フルまたは増分) はバックアップ仕様全体に適用され、ファイルシステム・オブジェクトのみに適用されます。

ゼロ・ダウンタイム・バックアップ・セッション (スナップショットまたはスプリット・ミラー) では、バックアップの種類は無視され、「フル」に設定されます。

フル・バックアップと増分バックアップを組み合わせて使用する場合は、バックアップ・オブジェクトが以下について完全に一致していることを確認してください。

- クライアント名
- ドライブ / マウント・ポイント
- 説明

  説明は、バックアップ仕様全体または特定のオブジェクトに対して設定できます。詳しくは、「バックアップ仕様オプション」(302 ページ) と「オブジェクト・オプション」(306 ページ) を参照してください。

- オーナー

  バックアップ所有権は、バックアップ仕様全体に対して設定できます。詳細は、「所有権 : 誰が復元を実行できるか」(300 ページ) を参照してください。

バックアップの種類

- フル・バックアップ

  フル・バックアップは、以前に同じオブジェクトがバックアップされていた場合でも、すべてのオブジェクトをバックアップします。オブジェクトを初めてバックアップする場合は必ずフル・バックアップが行われます。2 回目以降は、オーナーが同じで、保護が設定されたフル・バックアップがバックアップ時に使用可能でない場合に、フル・バックアップが行われます。

- 増分バックアップ

  この種類のバックアップは、前回の保護されたバックアップ・チェーン (フル・バックアップまたは増分バックアップのどちらでも可) に基づいて行われます。増分バックアップでは、前回の保護されたバックアップ以降変更されたファイルだけがバックアップされます。前回のバックアップが増分バックアップ (**増分**、**増分 1**、**増分 2**...) の場合でも、以降の増分バックアップでは、前回のバックアップ以降に変更されたファイルだけがバックアップされます。

- 増分 1 バックアップ

  この種類のバックアップは、オーナーが同じで最新の保護されたフル・バックアップを参照します。したがって、前回までの増分バックアップに基づくものでもありません。最新の保護されたフル・バックアップ以降に変更されたすべてのファイルがバックアップの対象となります。

- 増分 2 バックアップ

  この種類のバックアップは、フル・バックアップ後に増分 1 バックアップが実行されていない場合には、最新の保護されたフル・バックアップを参照します。複数の増分 1 バックアップがある場合は、最新のものを参照します。基準となるバックアップ以降変更されたすべてのファイルがバックアップされます。

- 増分 1-9 バックアップ

  上記の説明は増分レベルの概念を示しており、増分 9 までこの説明が適用されます。

さまざまな種類のバックアップに対して実行されるバックアップの相対関係を表 6-1 に示します。表の見方の説明は、表の後を参照してください。

表 6-1　実行されるバックアップの相対関係

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

表 6-1 **実行されるバックアップの相対関係**

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

表 6-1 の見方

- 表 6-1 の各行は他の行とは独立しており、異なった状況を示しています。
- バックアップの実行日は右から左に向かって古くなっているので、左が最も古く、右が最新です。
- フルと増分 X は、オーナーが同じで現時点でも保護が設定されているオブジェクトを示します。保護されていない増分 X は復元には使用できますが、後続のバックアップの対象とはみなされません。

例 :

- 2 行目は、保護が設定されたフル・バックアップと増分 2 バックアップが実行されたことを示しています。増分 1 バックアップがないので、バックアップは増分 1 バックアップとして実行されます。
- 5 行目は、フル・バックアップ、増分 1 バックアップ、さらに増分バックアップが実行されたことを示しています。Data Protector は、現在実行中のバックアップの参照元を前回の増分バックアップ (つまり増分 1) としてバックアップを実行します。
- 8 行目では、増分 3 バックアップが増分 2 バックアップとして実行され、11 行目では、増分 3 バックアップが増分 1 バックアップとして実行されます。

バックアップの種類の選択方法

対話型バックアップを実行する場合は、バックアップの種類を選択するプロンプトが表示されます。バックアップをスケジュールする際は、[バックアップのスケジュール] ダイアログでバックアップの種類を指定します。たとえば、同じバックアップ仕様を実行するスケジュール (土曜日にフル・バックアップ、毎営業日に増分 1 バックアップを実行するスケジュール) を容易に作成できます。

バックアップの種類と復元プロセス

フル・バックアップは復元を容易かつ効率的に行えますが、多数のメディアが必要となり、これらにバックアップ・データ全体の複数のバージョンが保存されることに注意してください。このため、バックアップの実行に必要な時間は非常に長くなります。増分バックアップでは、必要なメディアの量は少なく済みますが、復元アルゴリズムが複雑になります。以下の 2 つの例を比較してみます。

1. フル → 増分 → 増分 → 増分 → 増分 （→時間）

   この例では、バックアップに要する時間は短くなり、メディアに必要なスペースも少なくなります。ただし、前回の増分バックアップの状態に復元する場合は、復元プロセスはより複雑になり、多数のメディアへのアクセスが必要となるため、復元に必要な時間もより長くなります。

2. フル → 増分 1 → 増分 1 → 増分 1 → 増分 1 （→時間）

   この例では、例 1 に比べてバックアップ時間が長くかかり、メディアに必要なスペースも多少多くなります。ただし、復元プロセスは簡単で、アクセスが必要なメディアの数も少なく、復元時間も例 1 に比べて短くなります。

バックアップ・テンプレートの使用

概要

Data Protector のバックアップ・テンプレートは、バックアップ構成を容易に行うための強力なツールです。テンプレートには、バックアップ仕様向けにオプション・セットが明確に指定されており、バックアップ仕様を作成、編集する際の基礎としてこのテンプレートを使用できます。Data Protector では、テンプレートに用意されている一連のオプションを適用できます。

テンプレートの使用方法は 2 通りあります。

- バックアップ仕様の新規作成に使用できます。
- 既存のバックアップ仕様に適用して、このバックアップ仕様を変更できます。

バックアップ・テンプレートは、バックアップ仕様と同様に作成、編集できます。ただしバックアップ・テンプレートでは、オブジェクトとバックアップ・アプリケーションの構成は選択されません。

Data Protector のデフォルトのバックアップ・テンプレート

Data Protector には、ファイルシステムまたはアプリケーション・バックアップを構成するためのデフォルト・テンプレートが、さまざまなデータの種類 (ファイルシステム、Oracle/SAP など) に応じて用意されています。テンプレートには代表的な設定値が指定されており、この値を基にバックアップ仕様を作成できます。

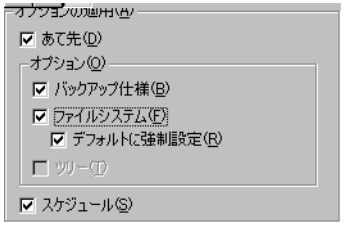
ブランクのバックアップ・テンプレート

ブランクのバックアップ・テンプレート (`Blank Filesystem Backup`、`Blank Informix Backup` など) では、オブジェクトまたはデバイスは選択されていません。バックアップ仕様オプションとオブジェクト・オプションでは、Data Protector のデフォルト値が指定されていますが、バックアップ・スケジュールはありません。[負荷調整] オプションを個別に選択することにより、バックアップ用に選択したデバイスの使用状況を Data Protector で自動調整できます。

テンプレートで提供されるオプション

バックアップ仕様の作成または編集にバックアップ・テンプレートを使用する場合は、テンプレートで提供されるオプションを選択することも選択解除することもできます。

図 6-20　テンプレートで提供されるオプション



[あて先]　テンプレートで指定されているバックアップ・デバイスの設定をバックアップ仕様に適用します。

[バックアップ仕様] テンプレートで指定されているバックアップ仕様オプションをバックアップ仕様に適用します。

[ファイルシステム] テンプレートで指定されているファイルシステム・オプションをバックアップ仕様のすべてのファイルシステム・オブジェクトに適用します。

[デフォルトに強制設定] テンプレートで指定されているファイルシステム・オブジェクト・オプションをバックアップ仕様のすべてのファイルシステム・オブジェクトに適用します。これらのオプションは [バックアップ・オブジェクトのサマリー] ページにあります。

[ツリー]　テンプレートで指定されているツリー・オプションをバックアップ仕様に適用します。

[スケジュール] テンプレートで指定されているスケジュール設定値をバックアップ仕様に適用します。

テンプレートのオプションを適用した後も、バックアップ仕様を編集して任意の設定値を変更できます。

上記オプションの詳細は、「バックアップ・オプションの使用」(290 ページ) を参照してください。

[負荷調整]　データをデバイスにどのように分散させるかを指示します。

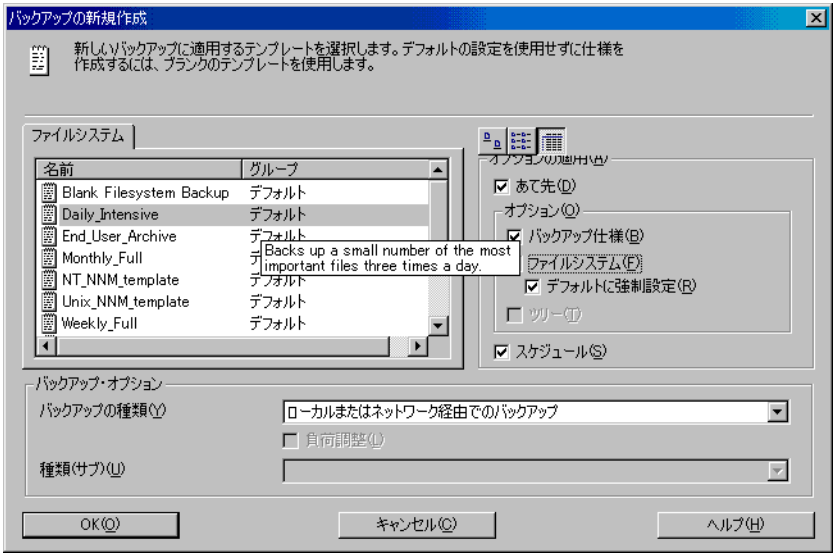
[負荷調整] オプションの詳細は、「負荷調整 : バックアップ・デバイスの使用状況を調整する」(297 ページ)を参照してください。

バックアップ仕様の新規作成時にバックアップ・テンプレートを使用する

バックアップ仕様を新規作成する際、Data Protector では、バックアップ・テンプレートを使用できます。このテンプレートは、デフォルトのテンプレートまたはユーザーが作成したテンプレートです。適切なテンプレートを選択するか、または必要に応じて一部のオプション・グループを選択 / 選択解除して、[バックアップ] ウィザードの操作を続行します。

定義済み設定値を使わずにバックアップ仕様を作成するには、`Blank Filesystem Backup` を選択します。

図 6-21 バックアップ仕様の新規作成時にバックアップ・テンプレートを使用する



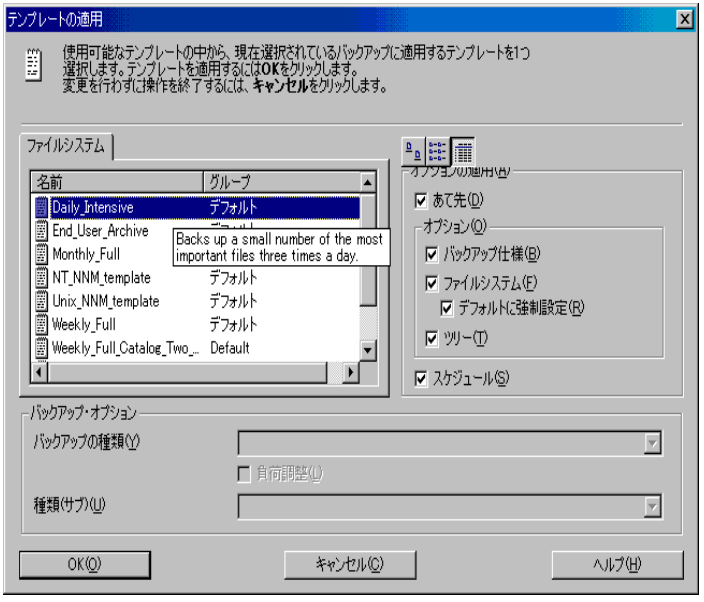
バックアップ・テンプレートの適用

Data Protector では、保存したバックアップ仕様にバックアップ・テンプレートを適用できます。バックアップ仕様にテンプレートを適用する際、どのオプション・グループを適用するかを選択できます。詳細は、「テンプレートで提供されるオプション」(281 ページ) を参照してください。

オプション・グループを適用することにより、このグループに含まれるすべての関連オプションが、テンプレートで指定された状態に設定されます。

テンプレートをバックアップ仕様に適用するには、バックアップ仕様を右クリックして、[テンプレートの適用] をクリックします。[テンプレートの適用] ダイアログ・ボックスで目的のオプションを適用します。詳しい手順については、オンライン・ヘルプの索引キーワード「バックアップ・テンプレートの適用」を参照してください。

図 6-22 [テンプレートの適用] ダイアログ・ボックス



統合ソフトウェア用バックアップ仕様

統合ソフトウェア用バックアップ仕様にテンプレートを適用するには、そのバックアップ仕様を結果エリアで開いてはいけません。バックアップ仕様をクリックして開き、このバックアップ仕様にテンプレートを適用しようとしても、[テンプレートの適用] オプションは使用できません。

重要

[デフォルトに強制設定] オプションを選択すると、[バックアップ・オブジェクトのサマリー] ページでオプションを変更したバックアップ仕様のすべてのファイルシステム・オブジェクトに対して、テンプレートで指定されているファイルシステム・オプションが適用されます。

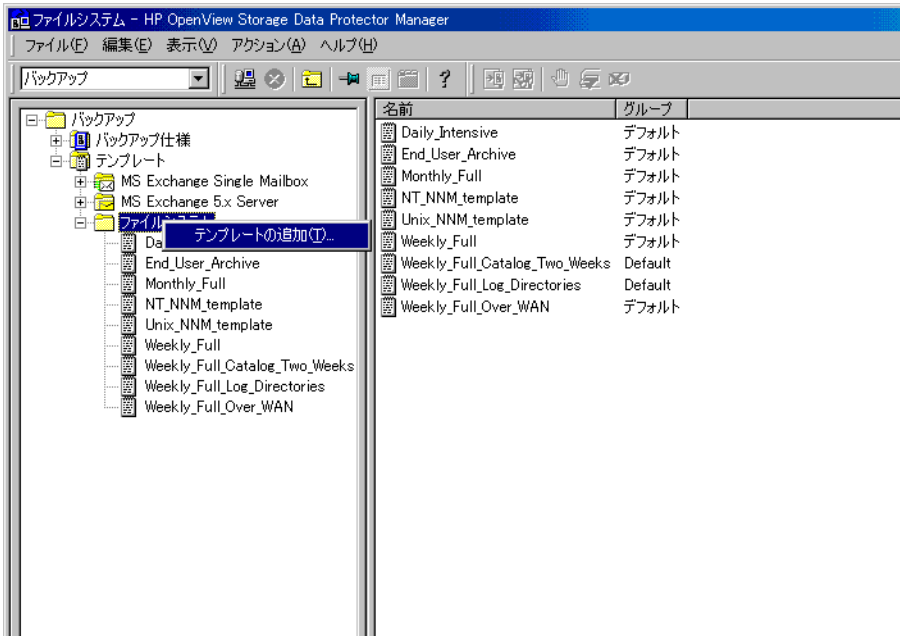
テンプレートを新規作成する

テンプレートを新規作成して、作成したテンプレートを使ってバックアップ仕様を作成したり変更できます。

テンプレートを新規作成するには、[バックアップ] コンテキストを使用します。詳しい手順については、オンライン・ヘルプの索引キーワード「バックアップ・テンプレートの作成」を参照してください。

個々のオプションの詳細は、「バックアップ・オプションの使用」(290 ページ) を参照してください。

図 6-23　テンプレートを新規作成する



既存のテンプレートを修正する

Data Protector のデフォルトのテンプレートは、ユーザーが作成したテンプレートと同様修正できます。

既存のテンプレートを修正するには、修正するテンプレートのプロパティを開きます。詳しい手順については、オンライン・ヘルプの索引キーワード「バックアップ・テンプレートの変更」を参照してください。

個々のオプションの詳細は、「バックアップ・オプションの使用」(290 ページ) を参照してください。

小規模な繰り返しバックアップの処理

多数の小さいオブジェクトを繰り返しバックアップする必要がある場合、バックアップ・セッションを何度も実行しなければなりません。この場合、メディアはバックアップ・セッションのたびに、ドライブ内にロードされアンロードされます。このような方法でバックアップを行っていては、時間がかかるだけでなくメディアも劣化してしまいます。メディアをもっと経済的に使用して時間を節約するには、ファイル・ライブラリ・デバイスを作成し、これを使用して小規模な繰り返しバックアップを、テープ上ではなくディスク上で実行します。その後、オブジェクトコピー機能を使用して、データをディスクからテープ・メディアに移動させます。

この方法を使用すれば、メディアがロードおよびアンロードされるのはオブジェクトコピー セッション中に 1 度だけになるので、バックアップの速度が上がり、メディアも経済的に使用できます。

多数の小さいオブジェクトを何度もバックアップするには、以下のタスクを実行します。

1. ファイル・ライブラリ・デバイスを構成します。各ライターのブロック・サイズは、第 2 ステージで使用するデバイスのブロック・サイズに合わせてください。「ファイル・ライブラリ・デバイスの作成および構成」(117 ページ) を参照してください。
2. 小さいオブジェクトすべてに対するバックアップ仕様を作成します。バックアップの最初の手順で作成したファイル・ライブラリを使用します。詳細は、「バックアップの構成」(210 ページ) を参照してください。
3. バックアップを実行またはスケジュール設定します。
4. オブジェクトコピー機能を使用して、バックアップ・データをテープに移動させます。この目的で構成されたオブジェクトコピー仕様の例については、オンライン・ヘルプの索引キーワード「ディスク・ステージング」を参照してください。

バックアップ仕様の分類

Data Protector では、バックアップ仕様を複数のグループに分類できます。分類の目的は、複数のバックアップ仕様を分かりやすく整理することです。

以下に、**「企業 X」**のバックアップ仕様を以下の 3 種類のグループに分類する例を示します。

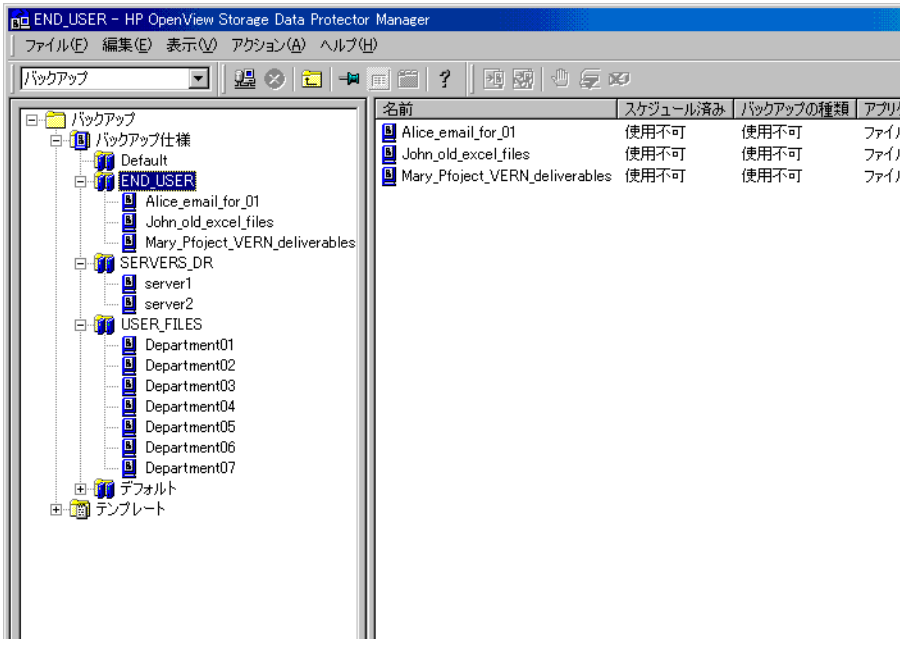
- **USER_FILES**: このグループには、10 部門単位で全ユーザーのフル・バックアップを週に一度実行するバックアップ仕様が入ります。これが、基幹バックアップとなります。
- **SERVERS_DR**: このグループには、会社のサーバの障害復旧に備えるためのバックアップ仕様が入ります。新しいサーバをインストールするか、既存サーバをアップグレードするたびに、新しいバックアップ仕様が作成され、このグループに追加されます。
- **END_USER**: このグループは、エンド・ユーザーの要求で作成するバックアップ仕様の保存に使用します。たとえば、あるエンド・ユーザーがディスク・スペースに空きを作るため、まずハードディスクのアーカイブを作成しなければならない場合などです。

図 6-24 (288 ページ) を参照してください。

この構成ではバックアップ仕様の数が 50 にものぼる場合があり、一度に表示した場合、管理しにくくなります。バックアップ仕様を分かりやすくグループに分類しておけば、それぞれのバックアップ仕様の検索や管理を容易に行えます。これにより、共通のオプション設定をテンプレートからグループ全体に適用できます。

たとえば、グループ内のすべてのバックアップ仕様に対してデバイスのリストを変更したい場合、テンプレートのデバイス設定を選択して変更することができます。

図 6-24 バックアップ仕様グループの例



グループの表示方法と作成方法

以下に、使用可能なバックアップ・グループを表示する方法と新しいグループを作成する方法を示します。

1. [Data Protector Manager] で [バックアップ] コンテキストを選択します。
2. [表示] メニューで [グループ別] をクリックします。[バックアップ仕様] に使用可能なバックアップ・グループのリストが表示されます。グループをクリックすると、そのグループに含まれるバックアップ仕様が表示されます。
3. [バックアップ仕様] 項目を右クリックし、[グループの追加] をクリックします。[新しいグループの追加] ダイアログ・ボックスが表示されます。
4. [名前] テキスト・ボックスに新しいグループの名前を入力した後、[OK] をクリックします。[バックアップ仕様] に、新しいグループが表示されます。

バックアップ仕様をグループに保存する方法

バックアップ仕様を保存する際、このバックアップ仕様はバックアップ仕様のグループへも追加されます。グループ名を指定しなかった場合、バックアップ仕様は [デフォルト] グループに追加されます。

グループの削除方法

グループを削除するには、まずグループを空にする必要があります。グループを空にするための 1 つの方法は、バックアップ仕様を他のグループに移動させることです。詳細はオンライン・ヘルプを参照してください。

バックアップ・オプションの使用

Data Protector は総合的なバックアップ・オプションを備えており、バックアップを微調整できます。すべてのオプションにはデフォルト値があり、大部分の場合にはこの値が適しています。

利用できるバックアップ・オプションは、バックアップの対象となるデータのタイプによって異なります。たとえば、ファイルシステム・バックアップとディスク・イメージ・バックアップとでは、利用できるオプションの組み合わせが異なります。Exchange や SQL などで使用するための共通オプションおよびアプリケーション固有オプションについては、『HP OpenView Storage Data Protector インテグレーション・ガイド』を参照してください。

また、一部のプラットフォームおよび統合ソフトウェアでは、ユーザー定義変数を使うと、変数の名前と値を指定して、柔軟性に富んだ操作を行えます (MPE プラットフォームのバックアップなど)。

バックアップ・オプションは以下のように分類できます。

- バックアップ仕様全体に対して設定するバックアップ仕様オプション (**[所有権]**、**[実行前コマンド]**、**[実行後コマンド]** オプション)
- さまざまなバックアップ・オブジェクト (ファイルシステムまたはディスク・イメージ) のバックアップ方法を指定するオブジェクト・オプション。

  オブジェクト・オプションは 2 つのレベルに設定できることを理解しておくことが必要です。第一に、バックアップ仕様内のすべてのファイルシステムとすべてのディスク・イメージ・オブジェクトに対して個別に**デフォルトのオブジェクト・オプション**を設定できます。第二に、**各オブジェクトに対して**個別にオブジェクト・オプションを設定できます。デフォルト値はこの設定値によって無効にされます。たとえば、CPU 速度が遅いクライアントを除くすべてのクライアントからのデータを圧縮するには、ファイルシステム・オプションの設定時に [ソフトウェア圧縮] を ON に設定し、次に、CPU 速度の遅いクライアントを選択して、このクライアントの [ソフトウェア圧縮] を OFF に設定します。
- バックアップ・デバイスの動作を定義するデバイス・オプション。デバイス・オプションを設定しなかった場合は、デバイスの定義から値が読み込まれます。

- スケジュール・オプションでは、個々のバックアップまたはスケジュールされた定期的バックアップに対して、バックアップの種類、ネットワーク負荷、およびデータ保護を定義します。スプリット・ミラーまたはスナップショットのバックアップにおいて、ZDB ディスクまたは ZDB ディスク / テープ・バックアップ (インスタント・リカバリが有効) を行う場合は、［スプリット・ミラー / スナップショットのバックアップ］オプションも指定します。

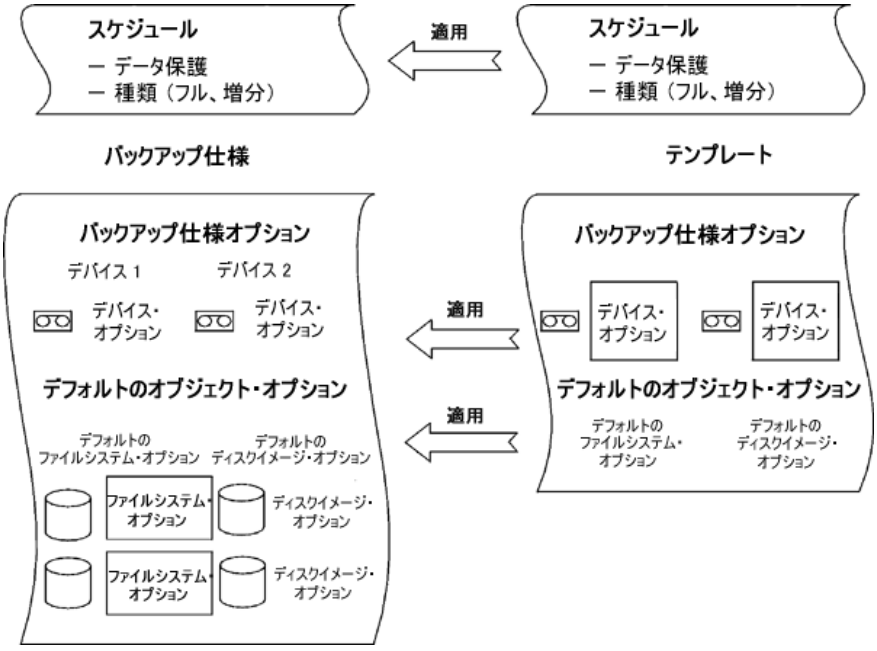
  スプリット・ミラーおよびスナップショット・バックアップでは、バックアップの種類は無視されます (フル・バックアップに設定されます)。［ バックアップのスケジュール ］ダイアログで指定されたデータ保護は、バックアップ仕様内で別に定義されている保護設定よりも優先して適用されます。

図 6-25 にオプションの動作状況を示します。バックアップ・テンプレートを使用することにより、多数のバックアップ仕様に同じオプション・グループを適用できます。テンプレートを適用すると、適用されたテンプレートに応じてバックアップ仕様が変更されます。後でテンプレートを変更した場合は、テンプレートをもう一度適用して、変更内容を有効にする必要があります。

ユーザーは、スケジュール、デバイス、およびオブジェクト・オプションやプライベート除外リストを選択して適用できます。

バックアップ・テンプレートの詳細は、「バックアップ・テンプレートの使用」（280 ページ) も参照してください。

図 6-25 バックアップ・オプション



最も頻繁に使用されるバックアップ・オプション

本項では、バックアップ方針に従って頻繁に変更される可能性の高い以下のオプションについて説明します。

- 「データ保護 : メディア上にデータを保存する期間を指定する」(293 ページ)
- 「カタログ保護 : データベース上にログ情報が保存される期間」(295 ページ)
- 「ロギング : データベースに保存されているデータの詳細を変更する」(296 ページ)
- 「負荷調整 : バックアップ・デバイスの使用状況を調整する」(297 ページ)
- 「所有権 : 誰が復元を実行できるか」(300 ページ)

データ保護 : メディア上にデータを保存する期間を指定する

データ保護ポリシーの構成は、データの安全性を確保して環境を円滑に管理する上で非常に重要な作業です。データ保護ポリシーの詳しい定義方法については、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

ユーザーは、自社のデータ保護ポリシーに基づいて、バックアップしたデータをメディアに保存しておく期間を指定する必要があります。たとえば、3 週間経過したデータは期限切れのデータとして、次回のバックアップ時に上書きできます。

[保護] オプションは、バックアップ操作とオブジェクトコピー操作に対して指定できます。

制限事項

オペレーティング・システムの制限により、保護期限として指定できるのは 2038 年 1 月 18 日までです。

データ保護は複数の場所で指定できます。対話形式でバックアップを実行するか、保存済みのバックアップ仕様を起動するか、バックアップをスケジュールするかによって、さまざまな組み合わせを使用できます。デフォルトは [無期限] です。

- 対話型バックアップ

  対話型バックアップの構成時には、バックアップ全体に対するデフォルトのデータ保護を変更できます。図 6-26 (294 ページ) を参照してください。さらに、個々のバックアップ・オブジェクトに対して異なるデータ保護を設定できます。バックアップ・オブジェクトに対して指定されたデータ保護が、デフォルトのデータ保護に優先して適用されます。図 6-27 (295 ページ) を参照してください。

- 保存済みバックアップ仕様によるバックアップ

  GUI を使用して保存済みバックアップ仕様を起動する場合は、上記で説明した対話型バックアップと同様のデータ保護が適用されます。

  CLI を使用して保存済みバックアップ仕様を起動する場合もデータ保護を指定できます。この指定は、バックアップ仕様内のデータ保護設定より優先されます。

- スケジュールされたバックアップ

個々のバックアップまたはスケジュールされた定期的バックアップに対して、異なるデータ保護を指定できます。[バックアップのスケジュール] ダイアログで指定されたデータ保護は、バックアップ仕様内で別に定義されている保護設定よりも優先して適用されます。データ保護をデフォルトのままにした場合、上記で説明した対話型バックアップと同様のデータ保護が適用されます。

データ保護の設定方法は、オンライン・ヘルプの索引キーワード「データ保護の設定」を参照してください。

注記

既存のバックアップ仕様にバックアップ・テンプレートを適用して［ファイルシステム］および / または［スケジュール］オプションを選択した場合、テンプレートの保護設定がバックアップ仕様各部に対する従来のデータ保護設定を上書きします。詳細は、「テンプレートで提供されるオプション」(281 ページ) を参照してください。

図 6-26　バックアップ・オプション : 保護

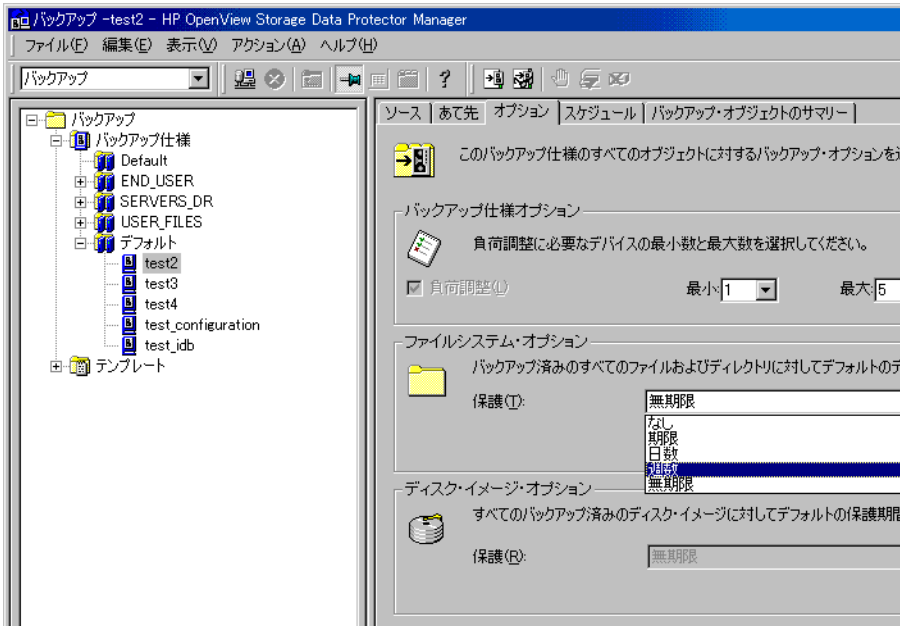
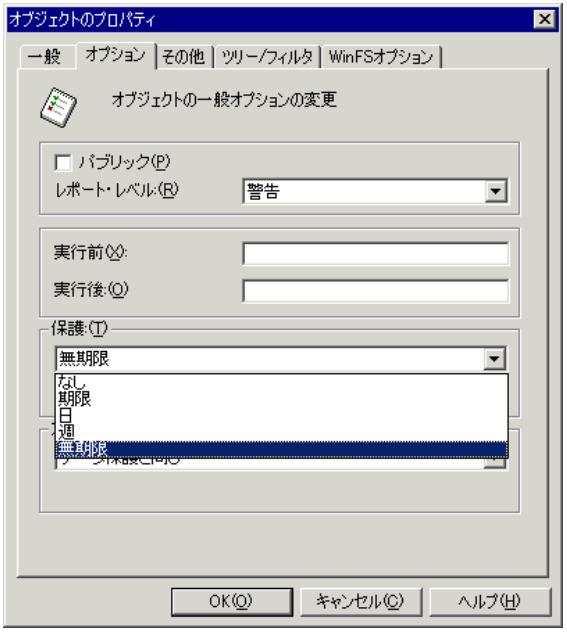


図 6-27 バックアップ・オブジェクトのプロパティ - オプション：保護



カタログ保護：データベース上にログ情報が保存される期間

メディア上でのデータ保護期間を制御する［データ保護］オプションの他に、［カタログ保護］オプションを設定することにより、バックアップされたファイルとディレクトリに関する情報を IDB に保存する期間を制御できます。[カタログ保護] オプションと [データ保護] オプションは個別に設定できます。ログ・レベルが［ログなし］に設定されている場合、カタログ保護は無効になります。

［カタログ保護］オプションは、バックアップ操作とオブジェクトコピー操作に対して指定できます。

カタログ保護のデフォルト値は［データ保護と同じ］です。これは、メディアが復元用に使用可能な限り、ファイルまたはディレクトリをブラウズしたり選択できることを意味します。

注記

データ保護期限が切れると、カタログ保護は取り消されます。つまり、データ保護が終了して、メディアが上書きされる際に、オブジェクトのカタログは、カタログ保護の設定の有無に関係なく削除されます。

カタログ保護期限が切れた場合でも、復元は可能です。ただし、ファイル名を手動で指定する必要があります。

カタログ保護は、ログ・レベルと共に、IDB の拡張性に大きな影響を与えることに注意してください。したがって、実際の環境に適したカタログ保護ポリシーを定義することが非常に重要です。カタログ保護と、推奨される使用方法については、『HP OpenView Storage Data Protector コンセプト・ガイド』の「IDB」の項を参照してください。

制限事項

オペレーティング・システムの制限により、保護期限として指定できるのは 2038 年 1 月 18 日までです。

ロギング : データベースに保存されているデータの詳細を変更する

ログ・レベルにより、バックアップ・セッション中に IDB に書き込まれるファイルとディレクトリの詳細情報の量が決まります。データの復元は、バックアップ・セッション中に使用されるログ・レベルに関係なく可能です。

ログ・レベルは、バックアップ操作とオブジェクトコピー操作に対して指定できます。

Data Protector には、以下の 4 つのログ・レベルがあります。

表 6-2

[すべてログに記録]	デフォルトのログ・レベルです。バックアップしたファイルとディレクトリに関するすべての詳細情報 (名前、バージョン、属性) が IDB に記録されます。ユーザーは、復元前にディレクトリとファイルをブラウズしてファイルの属性を確認できます。 また Data Protector は、特定のファイルまたはディレクトリを復元する際に、テープ上の位置を素早く特定できます。

表 6-2

ログ・ファイル	このログ・レベルを選択した場合は、バックアップしたファイルとディレクトリに関する詳細情報 (名前、バージョン) が IDB に記録されます。ユーザーは、復元前にディレクトリとファイルをブラウズできます。また Data Protector は、特定のファイルまたはディレクトリを復元する際に、テープ上の位置を素早く特定できます。すべてのファイル詳細 (ファイル属性) がデータベースに記録されるわけではないので、保存される情報が占めるスペースはそれほど大きくありません。
[ディレクトリ・レベルまでログに記録]	このログ・レベルを選択した場合は、バックアップしたディレクトリに関するすべての詳細情報 (名前、バージョン、属性) が IDB に記録されます。ユーザーが復元前にブラウズできるのはディレクトリのみです。ただし、テープ上ではファイルが実際に属するディレクトリの近くに位置しているため、Data Protector は復元時に際して素早く位置を特定できます。このオプションは、ニュースやメール・システムなど、自動生成ファイルが多いファイルシステムに適しています。
[ログなし]	このログ・レベルを選択した場合は、バックアップしたファイルとディレクトリに関する情報は IDB に記録されません。復元前にファイルやディレクトリを検索したりブラウズすることはできません。

ログ・レベルの設定によって、IDB のサイズ増加、バックアップの速度、復元対象データのブラウズのしやすさが影響を受けます。

最も適切なログ・レベル設定を決定するには、設定によりどのような結果になるかを理解することが重要です。推奨されるログ・レベルや使用方法の詳細については、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

負荷調整 : バックアップ・デバイスの使用状況を調整する

負荷調整とは

デフォルトでは、Data Protector はバックアップ用に指定されているバックアップ・デバイスの使用状況を自動的に調整します。これは負荷調整とも呼ばれ、この機能により、デバイスの使用状況を均等にすることができま

す。[負荷調整] オプションを使ってバックアップを実行する場合、Data Protector は負荷調整バックアップ仕様で指定された順にデバイスを使用します。

注記

[負荷調整] オプションを使用不可能に設定した場合、バックアップ仕様で各オブジェクトのバックアップに使用するバックアップ・デバイスを選択しなければなりません。デバイスが使用不可能になった場合、このデバイスにバックアップする予定のオブジェクトは保存されません。

負荷調整の詳細については、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

どのような場合に負荷調整を使用するか

[負荷調整] オプションは、多数のオブジェクトを複数の使用可能なデバイスにバックアップして、Data Protector によって常にすべてのデバイスが使用されるようにしておきたい場合に使用することをお勧めします。デバイスが使用不可能になることによるバックアップへの影響を最小限に抑えるには、この [負荷調整] オプションを使用してください。デバイスが使用不可能になる理由には、以下のようなものがあります。

- バックアップ時に異常終了した
- バックアップ中に停止した
- 別のセッションによって使用中である
- 起動できない

どのような場合に負荷調整を使用しないか

以下の場合は、[負荷調整] オプションの選択を解除することをお勧めします。

- バックアップするオブジェクトの数が少ない場合
- オブジェクトを単純なデバイス (DDS など) でバックアップする場合
- オブジェクトをバックアップするデバイスを手動で選択する場合
- どのメディアにオブジェクトがバックアップされるかを知りたい場合

パラメータはどのように使用されるか

[負荷調整] オプションには最小と最大の 2 つのパラメータがあります。

最小は、バックアップ仕様のデバイス・リストの中から、セッションを起動するために使用可能でなくてはならないバックアップ・デバイスの最小数を指定するパラメータです。使用可能なデバイスとは、別のバックアップ・セッションによって使用されておらず、十分なライセンスがあることを意味します。

最大は、バックアップ仕様で定義されているデバイスの数に関係なく、同時に使用できるデバイスの最大数を指定するオプションです。残りのデバイスは必要に応じて使用されます。

たとえば、バックアップ仕様で 4 つのデバイスが指定されており、最小と最大を共に 2 に設定しているとします。この場合、まずバックアップ・セッションは、これら 4 つの内 2 つのデバイスが使用できるようになるまで待ち行列に入ります。ただし、この 2 つのいずれかで障害が発生した場合は、予備の 2 つのデバイスの内 1 つが使用されます。

オブジェクトをどのようにして使用可能なデバイスに割り当てるか

デバイスのリストから 1 番目のデバイスが起動されます。デバイスに対して選択されるオブジェクトの数は、[同時処理数] で定義されています。次に、2 番目のデバイスが起動され、リスト内のオブジェクトがなくなるか、実行されるデバイスの数が最大になるまで、オブジェクトが選択されます。

バックアップ対象のオブジェクトは、以下の条件に基づいて割り当てられます。

- バックアップ・デバイスに接続されているクライアント上にあるオブジェクトの優先順位が最も高くなります。
- クライアント当たりの Disk Agent 数ができるだけ少なくなるようにオブジェクトが選択されます。

オブジェクトをデバイスに割り当てるときに、オブジェクトのサイズは考慮されません。

デバイスが使用不可能になった場合、以下の状況が発生します。

- 障害発生前にデバイスにバックアップされていたすべてのオブジェクトは、実際にバックアップされています。
- 障害発生時にデバイスにバックアップ中であったオブジェクトのバックアップは中止されます。
- そのデバイスでのバックアップ待ちであったすべてのオブジェクトは、バックアップ仕様で指定されているその他の使用可能なデバイスにバックアップされます (ただし、指定されている最大数のデバイスが使用さ

れていない場合)。

例

たとえば、100 個のオブジェクトのバックアップを、デバイス数 4、同時処理数 3、負荷調整の最小および最大パラメータを共に 2 で構成したとします。少なくとも 2 台のデバイスが使用可能であればバックアップ・セッションが開始され、使用可能なデバイスの最初の 2 台でそれぞれ 3 つのオブジェクトのバックアップが並行して行われます。残りの 94 個のオブジェクトはバックアップ待ちとなり、その時点ではデバイスへの割り当ては行われません。

あるオブジェクトのバックアップが終了した時には、同時にバックアップしているオブジェクト数が 3 未満のデバイスにバックアップ待ちの次のオブジェクトが割り当てられ、そのオブジェクトのバックアップが開始されます。負荷調整により、バックアップ待ちのオブジェクトがある間は、2 台のデバイスが並行して動作します。バックアップ中のデバイスのうち 1 台が故障した場合には、予備のデバイスの内の 1 台が使用されます。故障したデバイスで実行中だったオブジェクトのバックアップは異常終了し、バックアップ待ちの次の 3 つのオブジェクトが新しいデバイスに割り当てられます。つまり、1 台のデバイスが故障した場合には、バックアップ・セッションを継続できる他のデバイスがあれば、最高 3 つのオブジェクトのバックアップが異常終了するということです。

テンプレートからデバイス・オプションを適用する際は、以下の規則に留意してください。

- テンプレート内で [負荷調整] オプションを選択していない場合、バックアップ仕様ではデバイス・オプションは使用されません。
- テンプレートとバックアップ仕様の両方で [負荷調整] オプションが選択されていれば、デバイス・オプションが適用されます。
- ［負荷調整］オプションがテンプレートだけで選択されている場合は、デバイス・オプションはバックアップ仕様にデバイスが指定されていない場合に限り適用されます。

失敗したバックアップの詳細は、「失敗したバックアップの管理」（335 ページ) を参照してください。

所有権 : 誰が復元を実行できるか

バックアップ・セッション・オーナーとは

対話型バックアップを開始するユーザーをセッション・オーナーといいます。ユーザーが既存のバックアップ仕様を変更しないで使用した場合、バックアップ・セッションは対話型とはみなされません。

ユーザーがバックアップ仕様を変更してバックアップを開始した場合、以下の条件が当てはまらない限りこのユーザーがオーナーとなります。

- ユーザーが [セッションの所有者を切り替え] ユーザー権限を持っている場合。
- 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。この場合は、バックアップ仕様で指定したユーザーがバックアップ・セッション・オーナーになります。

UNIX Cell Manager でバックアップがスケジュールされている場合は、上記の条件に当てはまらなければ、セッション・オーナーは `root:sys` になります。

Windows Cell Manager 上でスケジュールされたバックアップの場合は、上記の条件に当てはまらない限り、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。

誰がプライベート・オブジェクトを復元できるか

以下のユーザーはプライベート・オブジェクトを復元できます。

- `Admin` ユーザー・グループおよび `Operator` ユーザー・グループのメンバー。
- [復元の開始] ユーザー権限を持っているバックアップ・セッション・オーナー。他のユーザー権限 ([別のクライアントへ復元] など) も必要になる場合があります。
- [プライベート・オブジェクトを表示] ユーザー権限を持っているユーザー。

なぜバックアップ・オーナーを変更するか

バックアップ・オーナーを変更した方がよい場合もあります。たとえば、管理者がバックアップ仕様の構成とスケジュールを行い、オペレータがそのバックアップ仕様の実行を許可されている (ただし、バックアップ仕様の変更や保存はできない) と想定します。すべてのオブジェクトに対して [プライベート] バックアップ・オプションが設定されている場合、オペレータは何も復元できません。ただし、バックアップの管理や、正常に実行されなかったセッションの再開は行うことができます。

オーナーを変更できるのは、保存済みのバックアップ仕様の場合だけです。バックアップ構成を変更した後、保存しなければ、対話型バックアップとみなされるのでオーナーは変更されません。このため、意図していない種類のバックアップを作成してしまう可能性があります。たとえば、フル・

バックアップのオーナーではないユーザーが増分バックアップを対話型で起動すると、増分バックアップではなく別のフル・バックアップが作成されることになります。

Data Protector バックアップ・オプションのリスト

本項では、3 セットのバックアップ・オプションについて説明します。各セットのオプションはアルファベット順に記載されています。

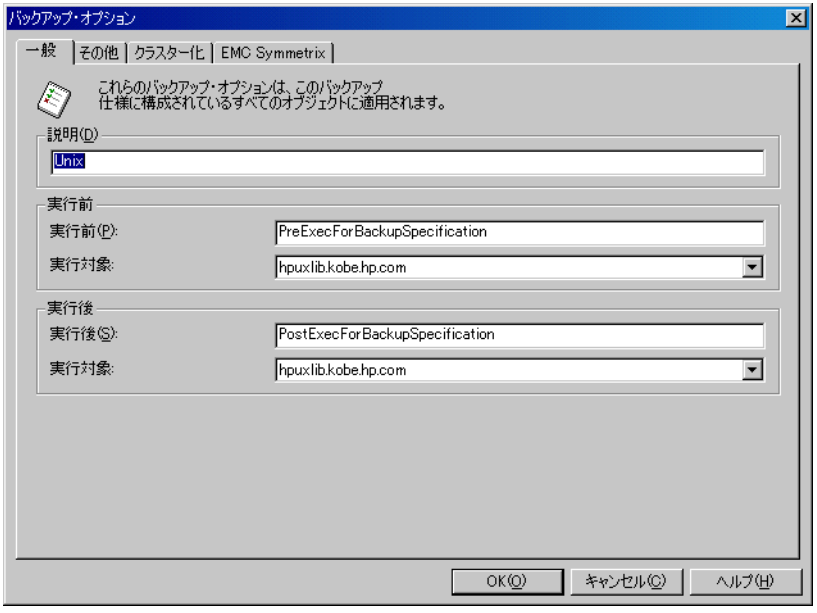
バックアップ仕様オプション

バックアップ仕様にオプションを設定する

1. オプションを設定するバックアップ仕様を選択します。
2. [オプション] タブをクリックします。
3. [バックアップ仕様オプション] で [拡張] をクリックします。[バックアップ・オプション] ウィンドウが表示されます。
4. [一般] および [クラスター化] でオプションをそれぞれ選択します、[EMC Synmetrix] タブと [HP StorageWorks XP] タブは、それぞれ EMC デバイスと Storageworks デバイスが接続されて構成されている場合に限り表示されます。

   MC/Service Guard または Microsoft Cluster Server のインストールと構成が行われていない場合、[クラスター化] は無視してください。
5. 設定内容を確認して [バックアップ・オプション] ウィンドウを終了するには、[OK] をクリックします。詳細はオンライン・ヘルプを参照してください。

図 6-28 バックアップ仕様オプション - [一般]



使用可能なバックアップ仕様オプション

説明

ユーザーはバックアップ仕様オプションの目的や内容を説明するテキストを入力できます。このテキストはバックアップ・セッションに全く影響を与えません。

[負荷調整]

このオプションは、[バックアップの新規作成] ダイアログ・ボックスで、デフォルトで有効に設定されています。ここでこのオプションを無効にしても、後から [バックアップ] タブを開いて、バックアップ仕様の [あて先] プロパティ・ページで設定できます。

このオプションを設定した場合、Data Protector は、使用可能なデバイスにバックアップ・オブジェクトを動的に割り当てます。これは、デバイスが均等に使用され、いずれかのデバイスで障害が発生しても、他の使用可能なデバイスでバックアップが続行されることを意味します。

このオプションを設定しなかった場合、バックアップ・オブジェクトはオブジェクトに割り当てられているデバイスに、指定された順序でバックアップされます。

デフォルトは ON です。

詳しくは、「負荷調整 : バックアップ・デバイスの使用状況を調整する」（297 ページ) を参照してください。

[所有権]

バックアップ仕様でオーナーが指定されていない場合、対話型バックアップを開始したユーザーがセッション・オーナーとなります。それ以外の場合は、以下のようになります。

- UNIX Cell Manager の場合は root
- Windows Cell Manager の場合は、インストール時に指定したユーザー

デフォルトの設定では指定されていません。

詳しくは、「所有権 : 誰が復元を実行できるか」（300 ページ) を参照してください。

セッション・オーナーを変更するには、以下の手順を行います。

1. [HP OpenView Storage Data Protector Manager] で [バックアップ] コンテキストを選択します。
2. [バックアップ仕様] をダブルクリックした後、変更するバックアップ仕様を右クリックします。
3. [プロパティ]、[オプション] の順に選択し、[バックアップ仕様オプション] で [拡張] を選択します。[一般] タブを選択します。
4. 必要に応じてセッションの所有権を変更します。Windows システムでは大文字を使用してください。

注記

ユーザーの構成時に指定した情報をそのまま指定してください。

[実行前]

このフィールドで指定されたコマンドは、オブジェクトのバックアップ前に、指定されたクライアント上で実行されます。クライアントが定義されていない場合は、コマンドは Cell Manager 上で実行されます。

Windows における実行前コマンドの指定の詳細は、「Windows システムでの実行前 / 実行後コマンド」（321 ページ) を参照してください。

UNIX における実行前コマンドの指定の詳細は、「UNIX システムでの実行前 / 実行後コマンド」（328 ページ) を参照してください。

UNIX 上でのサンプル・スクリプトについては、「実行前 / 実行後コマンドの例 (UNIX の場合)」(A-21 ページ) を参照してください。

デフォルトの設定では指定されていません。

[実行後]

このフィールドで指定されたコマンドは、すべてのオブジェクトのバックアップが完了した後に、指定されたクライアント上で実行されます。クライアントが定義されていない場合は、コマンドは Cell Manager 上で実行されます。

Windows における実行後コマンドの指定の詳細は、「Windows システムでの実行前 / 実行後コマンド」（321 ページ) を参照してください。

UNIX における実行前コマンドの指定の詳細は、「UNIX システムでの実行前 / 実行後コマンド」（328 ページ) を参照してください。

UNIX 上でのサンプル・スクリプトについては、「実行前 / 実行後コマンドの例 (UNIX の場合)」(A-21 ページ) を参照してください。

デフォルトの設定では指定されていません。

[切断された接続の再接続]

このオプションをオンに設定すると、ネットワークで短期間のエラーが発生した場合でも、Data Protector が以下を再接続します。

- Backup Session Manager と Disk Agent または Media Agent(コントロール接続)
- バックアップ中は Disk Agent と Media Agent、オブジェクトミラーが有効な場合は Media Agent(データ接続)

このオプションをオフに設定した場合は、セッションは中止されます。

この設定は、Disk Agent または Media Agent が Cell Manager が接続されている LAN とは別の LAN に接続されている場合などに役立ちます。この 2 つの LAN の間の接続の信頼性が低下した場合に (WAN 接続)、Data Protector はデフォルトで 600 秒間再接続を試みます。この秒数は、omnirc 変数である OB2RECONNECT_RETRY を使って設定できます。

デフォルトは OFF です。

オブジェクト・オプション

ファイルシステム・オプションの設定

1. バックアップ仕様を選択して、[オプション] プロパティ・ページをクリックし、[ファイルシステム・オプション] で [拡張] をクリックします。
2. [オプション]、[その他]、[WinFS オプション] または [NetWare オプション] から希望のオプションを選択します。

注記

[オプション] タブで実行前 / 実行後コマンド名を指定する場合、コマンドに対してフルパスを指定する必要がある場合とない場合があります。

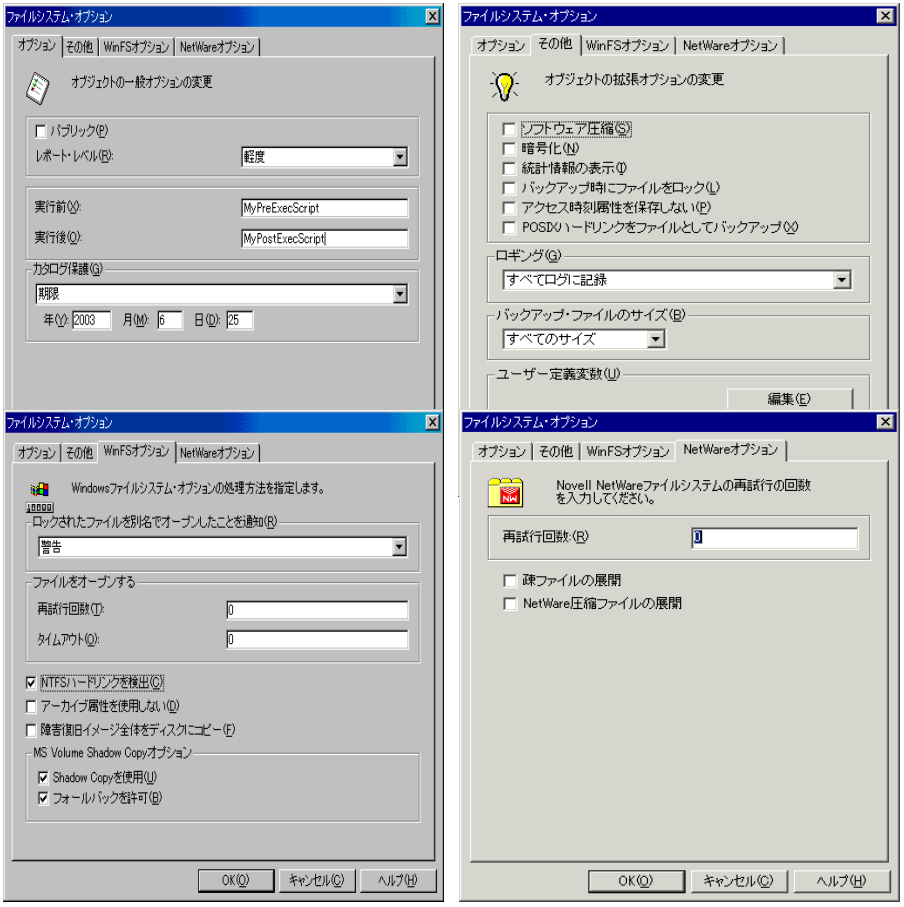
Windows における実行前コマンドの指定の詳細は、「Windows システムでの実行前 / 実行後コマンド」(321 ページ) を参照してください。

UNIX における実行前コマンドの指定の詳細は、「UNIX システムでの実行前 / 実行後コマンド」(328 ページ) を参照してください。

3. このダイアログ・ボックスを確認して終了するには、[OK] をクリックします。

   各オプション固有の情報については、オンライン・ヘルプを参照してください。

図 6-29 **ファイルシステム・オプション**



ディスク・イメージ・オプションの設定

1. バックアップ仕様を選択します。
2. [オプション] プロパティ・ページを選択します。
3. [ディスク・イメージ・オプション] で [拡張] をクリックします。

4. [オプション] または [その他] タブをクリックして、希望のオプションを選択します。各オプションの説明は、ダイアログ・ボックス内で [ヘルプ] をクリックすると表示されます。

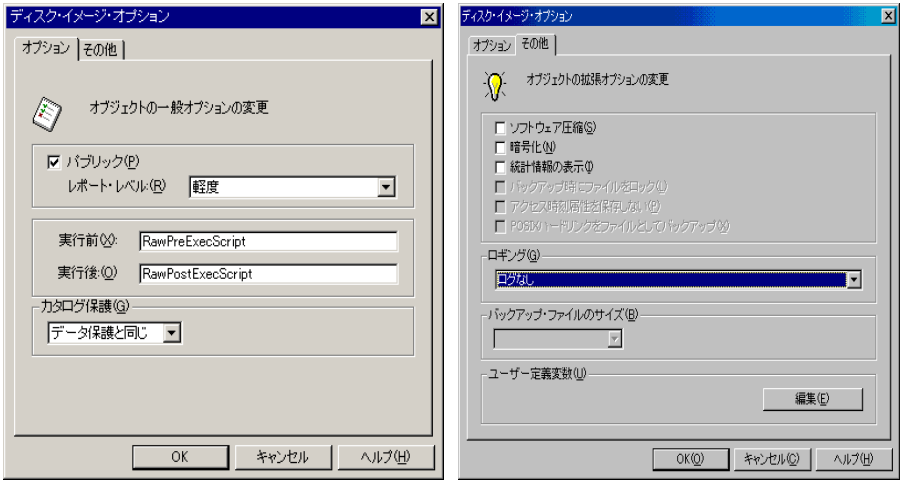
注記

[オプション] タブで実行前 / 実行後コマンド名を指定する場合、コマンドに対してフルパスを指定する必要がある場合とない場合があります。

Windows における実行前コマンドの指定の詳細は、「Windows システムでの実行前 / 実行後コマンド」(321 ページ) を参照してください。

UNIX における実行前コマンドの指定の詳細は、「UNIX システムでの実行前 / 実行後コマンド」(328 ページ) を参照してください。

図 6-30 ディスク・イメージ・オプション



5. このダイアログ・ボックスを確認して終了するには、[OK] をクリックします。

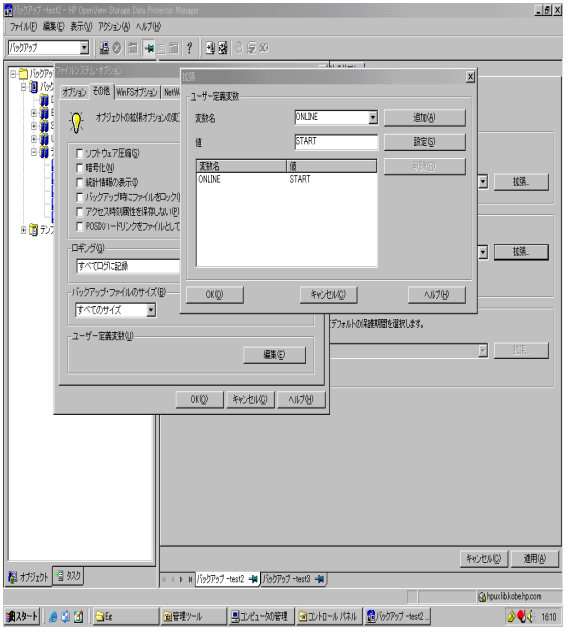
オブジェクト固有オプションの設定

1. オプションを設定するバックアップ仕様を選択します。
2. [バックアップ・オブジェクトのサマリー] プロパティ・ページを選択します。

3. バックアップ・オブジェクトを右クリックして、[プロパティ] を選択します。[オブジェクトのプロパティ] ウィンドウの内容は、選択したバックアップ・オブジェクトの種類によって異なります。オブジェクトの種類には、UNIX ファイルシステム、Windows ファイルシステム、UNIX ディスク・イメージがあります。

   Windows ファイルシステム用の [オブジェクト・プロパティ] ウィンドウは、[一般]、[オプション]、[その他]、[ツリー / フィルタ]、[WinFS オプション] の各タブで構成されます。[オプション]、[その他]、[WinFS オプション] の内容を図 6-29、[一般] と [ツリー / フィルタ] の内容を図 6-31 に示します。

図 6-31　オブジェクトのプロパティ - [一般] と [ツリー / フィルタ]

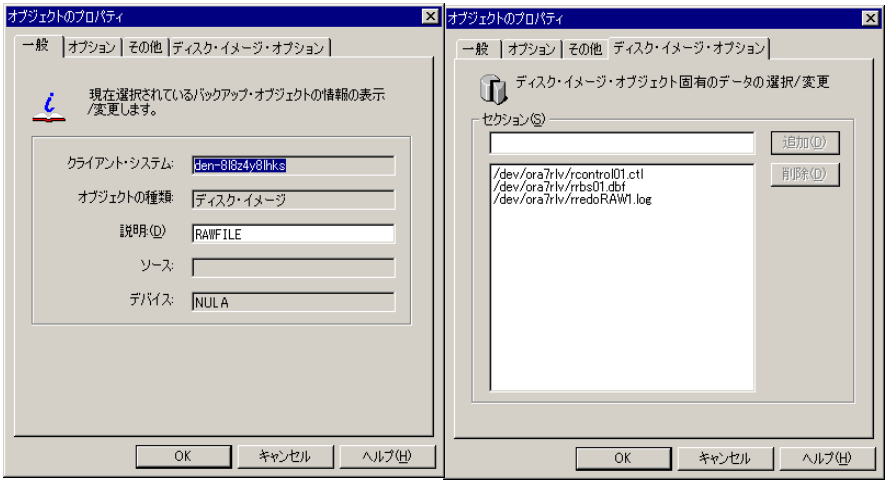


   UNIX ファイルシステム用の [オブジェクト・プロパティ] ウィンドウは、[一般]、[オプション]、[その他]、[ツリー / フィルタ] の各タブで構成されます。[オプション] と [その他] の内容を図 6-29、

[一般] と [ツリー / フィルタ] の内容を図 6-31 に示します。ただし、[オブジェクトの種類] にはファイルシステム [UNIX] と表示されます。

ディスク・イメージ・オブジェクト用の [オブジェクトのプロパティ] ウィンドウは、[一般]、[オプション]、[その他]、[ディスク・イメージ・オプション] の各タブで構成されます。バックアップ仕様に関する [オプション] と [その他] の内容を図 6-30、[一般] と [ディスク・イメージ・オプション] の内容を図 6-32 に示します。

図 6-32　オブジェクトのプロパティ - [一般] と [ディスク・イメージ・オプション]



4. オプションを設定した後、[OK] をクリックして、選択内容を確認します。各オプションの詳細については、以下を参照してください。

設定可能なオブジェクト・オプション

[フォールバックを許可] (Windows 固有オプション)

[Shadow Copy を使用] オプションが指定されており、VSS ファイルシステム・バックアップを実行中のシステムでシャドー・コピーの作成が失敗した場合、デフォルトではバックアップも失敗します。ただし、[フォールバックを許可] オプションを指定することで

バックアッの失敗を回避できます。この場合、バックアップは VSS バックアップではないバックアップとして続行されます。

[バックアップ・ファイルのサイズ]

このオプションを使って、バックアップ・ファイルのサイズを指定します。バックアップ・ファイルのサイズは、[すべてのサイズ](デフォルト)、[～以上 (単位 : KB)]、[～以下 (単位 : KB)]、[範囲 (単位 : KB)] のいずれかで指定できます。

[POSIX ハードリンクをファイルとしてバックアップ]

このオプションは UNIX ファイルシステムの場合のみ有効です。

ハード・リンクとは、物理ファイルの場所を実際に示すディレクトリのエントリです。このオプションを設定しなかった場合、Data Protector はディレクトリ・ツリーを 2 回スキャンします。1 回目のスキャン時に、同じファイルを示すすべてのハード・リンクのテーブルが作成されます。2 回目のスキャン時に、1 つのハード・リンクだけがそのファイル内容と共にバックアップされ、他のすべてのハード・リンクはハード・リンクとしてバックアップされます。また Data Protector は、1 回目のスキャンでバックアップのサイズを予測することもできます。

このオプションを設定した場合、Data Protector は各ハード・リンクのファイル内容全体をバックアップします。Data Protector はファイルシステム・ツリーを 1 回だけスキャンするため、バックアップ・プロセスの速度が非常に速くなります。

ディレクトリ内にハード・リンクがない場合は、このオプションを使用してください。このオプションがオンの場合、Data Protector はバックアップのサイズを予測したり、バックアップが完了した割合 (%) を表示できません。

デフォルトは OFF です。

[カタログ保護]

[カタログ保護] のデフォルト値は **[データ保護と同じ]** です。この値を変更するには、**[なし]**、**[期限]**、**[日数]**、**[週数]** のいずれかの値を指定します。

詳細は、「カタログ保護 : データベース上にログ情報が保存される期間」(295 ページ) を参照してください。

[アクセス時刻属性を保存しない]

このオプションを設定しない場合は、アクセス時刻属性は前回のバックアップ時のまま変更されません。各ファイルがバックアップされた後、この属性は元の値にリセットされます。このオプションを設定した場合は、アクセス時刻の値はバックアップ時の時刻に設定されます。

「UNIX システムのバックアップ」(219 ページ) も参照してください。

デフォルトは OFF です。

このオプションは、Novell NetWare ではサポートされていません。

[アーカイブ属性を使用しない](Windows 固有オプション)

Data Protector はバックアップ後 (ファイルの読み取り完了後) アーカイブ属性をクリアします。別のアプリケーションでこの属性を使用する場合は、このオプションをオンに設定しておくことが必要です。

デフォルトは OFF です。

[NTFS ハードリンクを検出] (Windows 固有オプション)

このオプションは [POSIX ハードリンクをファイルとしてバックアップする] オプションと同様ですが、NTFS に対してのみ有効であり、デフォルト値がオフである点が異なります。これは、ハード・リンクが通常ファイルとしてバックアップされることを意味します。デフォルトはオフです。これは、NTFS ハード・リンクが使用される頻度が低く、このオプションを設定すると、バックアップ性能が低下するためです。

[暗号化]

オープン・システムとパブリック・ネットワーキングを利用する大規模な企業では、データ・セキュリティが重要な課題となります。Data Protector では、ファイルと raw ディスク・イメージのデータをコード化してそれらを読み取り不可能にすることができます。データは、ネットワークを介して転送される前とメディアに書き込まれる前にコード化されます。Data Protector では、ある特定の内蔵アルゴリズムを使ってコード化を行います。

デフォルトは OFF です。

[バックアップ時にファイルをロック]

このオプションをオンに設定した場合、バックアップ中のファイルがロックされるため、ファイルがバックアップ中に変更されるのを防止できます。強制ロック機能が使用されます。

デフォルトは OFF です。

このオプションは、Novell NetWare ではサポートされていません。

[ロギング]

デフォルトのログ・レベルは **[すべてログに記録]** です。この設定は、**[ログなし]**、**[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]** のいずれかに変更できます。

各ログ・レベルの詳細は、「ロギング : データベースに保存されているデータの詳細を変更する」(296 ページ) を参照してください。

[再試行回数] (Novell Netware 固有オプション)

このオプションでは、Data Protector がファイルのバックアップを試行する回数を定義します。この回数以内にバックアップを実行できなかった場合、Data Protector はエラー・メッセージを表示します。ファイルを開いた後に解放するアプリケーションをお使いの場合は、このオプションを使用することにより、ファイルがバックアップされる確率を高くすることができます。

デフォルト値は 1 です。

[ファイルをオープンする] (Windows 固有オプション)

このオプションは、オープンしている Windows ファイルが見つかった場合に Data Protector が何を行うかを制御します。**[再試行回数]** を指定しておくと、オープンされているファイルまたはビジー・ファイルのバックアップが、Data Protector により指定した回数だけ試行されます。**[タイムアウト]** では、オープンされているファイルまたはビジー・ファイルのバックアップを Data Protector が再試行するまでの待機時間 (単位 : 秒) を指定できます。

[保護] (データ保護)

このオプションでは、バックアップするデータに保護期間を設定できます。これにより、指定した期間中にバックアップ・メディアが上書きされるのを防止できます。[保護] の値には、**[なし]**、**[期限]**、**[日数]**、**[週数]**、**[無期限]** があります

デフォルトは **[無期限]** です。

[パブリック]/[プライベート]

このオプションを使うと、バックアップしたデータを復元するためのアクセス権を設定できます。**[プライベート]** オプションを使ってファイルシステムをバックアップした場合、このファイルシステムを復元できるのは、バックアップしたユーザーまたは Data Protector `Admin` グループに所属するユーザーに限られます。

このオプションを **[パブリック]** に設定すると、[復元の開始] ユーザー権限を持つユーザーなら誰でもデータを復元できます。

デフォルトは **[プライベート]** です。

[レポート・レベル]

このオプションは、バックアップ・セッション中にオブジェクトに関して通知されるエラーのレベルを定義します。レベルを設定することにより、設定したレベルとそれ以上のレベルに相当するエラーが通知されます。設定可能なレポート・レベルは、**[警告]**、**[軽度]**、**[重度]**、**[致命的]** の 4 段階です。

たとえば、[軽度] に設定すると、**「軽度」**、**「重度」**、**「致命的」** レベルのエラーのみが [メッセージ] フィールドに表示されます。**[正常]** レベルのメッセージは、常に [メッセージ] フィールドに表示されます。デフォルトは **[警告]** です。

注記

IDB に保存されるメッセージの数は、1 つのバックアップ・システム当たり最大 3000 個です。

[ロックされたファイルを別名でオープンしたことを通知] (Windows 固有オプション)

このオプションは、Data Protector がバックアップを試行した時点でオープンされていてロックされているファイルのレポート・レベルを設定します。Data Protector は、**[レポート・レベル]** の設定に応じて、ファイルをレポートします。デフォルトは **[警告]** です。

[ソフトウェア圧縮]

Data Protector では、Disk Agent のデータを圧縮して、圧縮したデータを Media Agent へ転送できます。この機能はソフトウェア圧縮とも呼ばれます。[オブジェクトのプロパティ] ウィンドウの [その他] プロパティ・ページで [[ソフトウェア圧縮] を選択して、ソフトウェア圧縮を使用可能に設定します。これにより、ネットワーク上でやりとりされるデータの量が減り、必要なメディアの数が削減されるため、バックアップ性能全体が向上します。データの種類にもよりますが、データ圧縮率は 30 ～ 70% で、Lempel-Ziv 4.3 圧縮アルゴリズムを使用しています。このアルゴリズムは UNIX の標準 `compress` ユーティリティと完全な互換性があります。このオプションを使用している場合、モニターに表示される圧縮の状況 (圧縮完了率を % で表示) が正確でないことがあるので注意してください。

デフォルトは `OFF` です。

このオプションは、Novell NetWare ではサポートされていません。ただし、以前のバージョンの Data Protector でこのオプションを使用して圧縮したファイルを展開することは可能です。

注記

現在使用されているバックアップ・デバイスの大部分は、内蔵ハードウェア圧縮機能を備えており、ユーザーは、デバイス構成手順でデバイスファイルまたは SCSI アドレスを作成する際にこの機能を設定できます。ソフトウェア圧縮機能とハードウェア圧縮機能を同時に使用しないでください。データ圧縮を二重に行うと性能が低下し、良好な圧縮結果が得られないためです。ハードウェア圧縮の設定方法の詳細は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

HP Ultrium LTO デバイスでは、自動ハードウェア圧縮機能を使用不可能に設定できません。Data Protector を使って HP Ultrium LTO ドライブを構成する場合は、デフォルトのソフトウェア圧縮設定を保持しないように設定します。

[NetWare 圧縮ファイルの展開] (Novell Netware 固有オプション)

Data Protector のデフォルト動作では、Novell NetWare の圧縮ファイルは圧縮形式でバックアップされます。この方式では、バックアップ処理が高速化される反面、Novell NetWare の圧縮ファイルを圧縮されていない Novell NetWare ボリュームには復元できなくなります。そこで、[NetWare 圧縮ファイルの展開] オプションをオンにすると、Novell NetWare の圧縮ファイルを展開した上でバックアップすることができます。この方法でバックアップを行うと、圧縮されていない Novell NetWare ボリュームにファイルを復元できるようになります。

[Shadow Copy を使用] (Windows 固有オプション)

Windows Sever 2003 システム上でファイルシステム・バックアップを実行する場合、Data Protector はポイント・イン・タイム・バックアップを調整するため、MS Volume Shadow Copy サービス (VSS) を使用します。VSS により、ボリュームのシャドー・コピー・バックアップや、正確なポイント・イン・タイムでのファイル (すべてのオープン中のファイルを含む) のコピーの作成が可

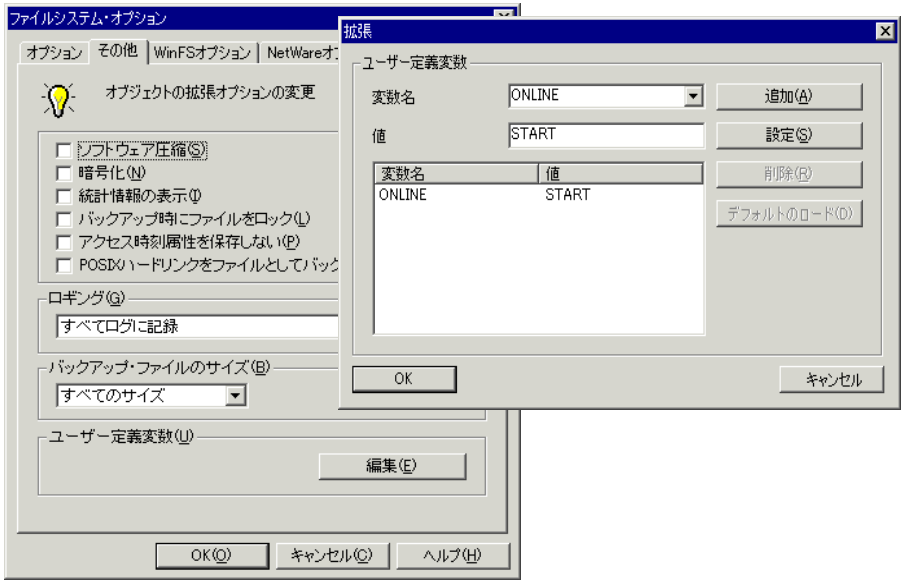
能となります。これは、VSS 機構が、保留中の I/O 動作をすべて停止し、シャドー・コピー・ボリュームの作成中に受け取る書き込み要求を保留にすることを意味します。この方法では、シャドーコピー作成中に、ファイルシステム上のすべてのファイルが閉じられ、ロックが解除されます。

ユーザー定義のバックアップ変数を設定する

一部のプラットフォームおよび Data Protector との統合ソフトウェアでは、ユーザー定義のバックアップ変数 (変数名と値) を設定することで、より柔軟な操作が可能になることがあります。詳しい手順については、オンライン・ヘルプの索引キーワード「ユーザー定義のバックアップ変数を設定する」を参照してください。

Data Protector で構成可能な変数とその値のリストは変更される場合があり、Data Protector パッチに付属しています。

図 6-33 [ユーザー定義変数]



デバイスのバックアップ・オプション

使用する各バックアップ・デバイスに対して、オプションをリストから選択できます。[CRC チェック]、[同時処理数]、[メディア・プール] は、デバイスの構成時に設定されるデフォルト値を使用するので、設定値は不要です。[事前割当てリスト] は、メディア・プールの設定値と共に設定されます。

設定可能なデバイス・バックアップ・オプション

[CRC チェック]

このオプションを設定すると、Data Protector はバックアップ実行時に CRC(巡回冗長検査) を計算します。CRC チェックは拡張チェックサム機能で、ユーザーは後で検証オプションを使ってデータがメディアに正しく書き込まれたかどうかを確認できます。

このオプションは、バックアップ操作とオブジェクトコピー操作に対して指定できます。

デフォルトは OFF です。

[同時処理数]

このオプションにより、1 台のバックアップ・デバイスに複数の Disk Agent が書き込みを行うことができます。これにより、Data Protector は Disk Agent が送信するよりも速くデータを受信できる場合に、デバイスのストリーミングを維持できます。同時処理数の最大値は 32 です。

Data Protector では、サポートされているすべてのデバイスに対してデフォルト値が設定されています。

このオプションは、バックアップ操作とオブジェクトコピー操作に対して指定できます。

[メディア・プール]

このオプションは、バックアップに使用するメディアのメディア・プールを選択します。オプションを定義しなかった場合は、デバイス仕様に含まれているデフォルトのプールが使用されます。

このオプションは、バックアップ操作とオブジェクトコピー操作に対して指定できます。

[事前割当てリスト]

事前割当てリストとは、バックアップに使用するメディア・プール内のメディアのサブセットで、メディアを使用する順番を指定します。バックアップ・デバイスで**事前割当てリスト**と `Strict` メディア割当てポリシーを使用する場合、Data Protector はデバイス内のメディアの順番が、**事前割当てリスト**で指定されている順番に対応しているとみなします。メディアをこの順番で使用できない場合、Data Protector はマウント要求を発行します。このリストにメディアが全く指定されていない場合は、Data Protector の割当て手順を使って、メディアが割り当てられます。

このオプションは、バックアップ操作とオブジェクトコピー操作に対して指定できます。

[優先度の高いマルチパス・ホストを使用]

このオプションは、マルチパス デバイスに対してのみ使用できます。優先されるホストを設定するには、このオプションを選択して、ドロップダウン・リストからホストを選択します。バックアップ・セッション時に、Data Protector は、事前定義された順番に関係なくこのホストを最初に使用しようとします。

実行前 / 実行後コマンド

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、別の作業が必要な場合があります。たとえば、バックアップするファイル数の確認、一部のトランザクション処理の中止、データベースのシャットダウンなどです。のような作業は、実行前 / 実行後コマンドを使って実行します。Data Protector では実行前 / 実行後コマンドを提供していません。必要に応じて、その作業を実行する実行可能ファイルをユーザーが記述する必要があります。

重要

実行前 / 実行後コマンドの使用は危険性を孕んでいます。未承認ユーザーによる不正な侵入を招いてしまう可能性が非常に高いからです。セキュリティに関する考慮事項については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

バックアップ用の実行前 / 実行後コマンドは以下の 2 段階で構成します。

バックアップ仕様

実行前コマンドはバックアップ・セッションの開始前に実行され、実行後コマンドはバックアップ・セッションの終了時に実行されます。これらのコマンドをバックアップ仕様全体に対するバックアップ・オプションとして指定します。セッションの実行前 / 実行後コマンドはデフォルトでは Cell Manager 上で実行されますが、別のシステムを選択することもできます。

特定のバックアップ・オブジェクト

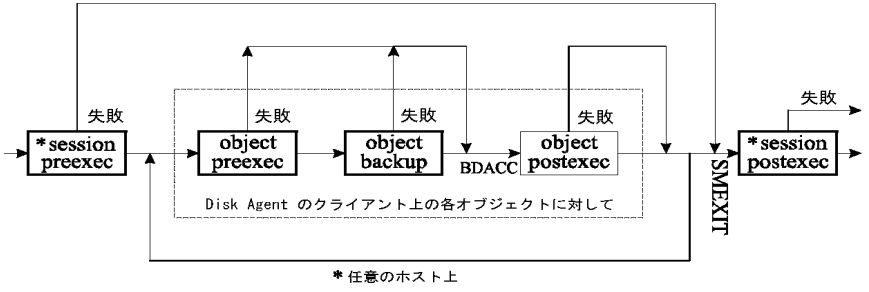
特定のバックアップ・オブジェクトに対する実行前コマンドは、オブジェクトのバックアップ前に実行されます。また、特定のバックアップ・オブジェクトに対する実行後コマンドは、オブジェクトのバックアップ後に実行されます。これらのコマンドを、すべてのオブジェクト、または個々のオブジェクトに適用されるバックアップ・オプションとして指定します。オブジェクトに対する実

行前 / 実行後コマンドは、このオブジェクトをバックアップする Disk Agent が実行されているシステム上で実行されます。

実行前 / 実行後コマンドは以下の順序で実行されます。

1. バックアップ仕様全体に対する実行前コマンドが起動して完了します。
2. バックアップ仕様内の各オブジェクトに対して、以下が行われます。
   a. 実行前コマンドが起動して完了します。
   b. 各オブジェクトのバックアップが行われます。
   c. バックアップ仕様内の各オブジェクトに対する実行後コマンドが起動して完了します。
3. バックアップ仕様全体に対する実行後コマンドが起動して完了します。

図 6-34　実行前 / 実行後コマンドの制御フロー



Windows システムでの実行前 / 実行後コマンド

本項では、Windows Cell Manager およびクライアントで実行前 / 実行後コマンドを実行する方法を説明します。

コマンドの記述方法　実行前 / 実行後コマンドは、実行可能ファイルまたはバッチファイルとして記述します。Windows システム上で実行前 / 実行後コマンドに使用できる拡張子は、.bat、.exe、および .cmd のみである点に注意してください。サポート対象外の拡張子 (.vbs など) を持つ実行前 / 実行後コマンドを実行するには、そのスクリプトを開始するバッチ・ファイル (.bat) を作成し

ます。このバッチ・ファイルを実行前 / 実行後コマンドとして実行するよう Data Protector を構成すると、このファイルにより、サポート対象外の拡張子を持つスクリプトが開始されます。

バッチファイル内で実行するすべてのコマンドの終了コードは、正常は 0、失敗時は 1 以上でなければなりません。

次項で説明する実行のガイドラインに従ってください。

バックアップ仕様に対する実行前 / 実行後コマンド

バックアップ・セッションに対する実行前 / 実行後コマンドは、バックアップ・セッションの前後にそれぞれ起動されます。これらのコマンドは通常 Cell Manager 上で実行されますが、別のシステムを選択することもできます。

コマンドの格納場所

実行前 / 実行後スクリプトは、Cell Manager 上で実行される場合は CRS によって起動され、リモートで実行される場合には Inet サービス・アカウント (デフォルトでは、ローカル・システム・アカウント) で起動されます。

Cell Manager 上では、スクリプトがどのディレクトリにあっても構いません。Cell Manager 以外のシステム上では、スクリプトは *<Data_Protector_home>*¥bin ディレクトリに存在しなければなりません。

<Data_Protector_home>¥bin ディレクトリにあるスクリプトはファイル名だけ指定すればよく、それ以外のスクリプトはフルパス名を指定する必要があります。

ファイル名またはパス名の指定方法

バックアップ仕様で [オプション] タブをクリックします。[バックアップ仕様オプション] で [拡張] をクリックします。［実行前］および / または［実行後］テキスト・ボックスにファイル名またはパス名を入力します。

フルパス名を入力する場合、ディレクトリ名が 8 文字を超えるときは、パス名を引用符で囲むか、8.3 形式の DOS 互換形式で入力してください。

重要

パス名の指定に引用符 ("") を使用する場合は、円記号と引用符を組み合わせて (¥") 使用しないでください。パス名の最後に円記号を付ける必要がある場合は、円記号を二重にして使用します (¥¥)。

環境変数

バックアップ・セッションの開始時に Data Protector によって以下の環境変数が設定されます。この環境変数を使用できるのは、Cell Manager のバックアップ仕様に対する実行前 / 実行後スクリプト内に限られます。

DATALIST バックアップ仕様の名前

MODE バックアップ動作の種類 (フル、増分、増分 1、増分 2 など)。

OWNER セッションのオーナー

この変数の内容は以下に示すとおりデータベースの形式と同じです (大文字と小文字が区別されます)。
UNIX の場合 - *< ユーザー >.< グループ >@< ホスト名 >*、
Windows の場合 - *< ドメイン >¥< ユーザー >@< ホスト名 >*

PREVIEW プレビューの実行中は 1 に、バックアップの実行中は 0(ゼロ) に設定されます。コマンドを変更して、バックアップ中にだけ実行され、プレビュー中には実行されないようにする場合に、この変数を使用します。デフォルトでは、実行前コマンドまたは実行後コマンドはプレビューに対して実行されません。これを有効にするにはグローバル・オプション `ExecScriptOnPreview` を設定します。

RESTARTED 現在のセッションが、再起動されたバックアップ・セッションである場合は 1 に設定されます。そうでない場合は 0 に設定されます。実行後コマンドはこの変数を使って、**SMEXIT** = 0 の場合にさらに再起動が行われるのを防止します。

SESSIONID 完了したセッションの識別に使用する変数で、データベースに記録されます。この変数を使ってセッションのプレビューはできません (この場合は SESSIONKEY を使用します)。

SESSIONKEY 実行中のセッションの識別に使用します。たとえば、問題が発生した場合、バックアップ・セッションの開始前にこの変数を使ってセッションを中止できます。

SMEXIT Session Manager の終了コードで、omnib コマンドの終了コードと同じです。この変数を使用できるのは実行後コマンドだけです。エージェントとは、Disk Agent、Media Agent、Application Agent、または Symmetrix Agent などを指します。

表 6-3 SMEXIT の値

値	説明
0	ファイルはすべて正常にバックアップされました。
10	エージェントはすべて正常に実行されましたが、ファイルの中に一部保存されていないものがあります。
11	1 つまたは複数のエージェントで問題が発生したか、またはデータベース・エラーが発生しました。
12	どのエージェントも動作を完了しませんでした。Data Protector によってセッションが中止されました。
13	ユーザーによってセッションが中止されました。

キー・ポイント

- バックアップ仕様に対する実行前 / 実行後コマンドは実行可能ファイルまたはバッチファイルでなければなりません。Windows の場合、ファイル名の拡張子を指定する必要があります。
- 実行前/実行後コマンドはCell Manager上のどのディレクトリにあっても構いません。または、*<Data_Protector_home>*¥bin ディレクトリ内で Disk Agent の実行されている他のどのシステム上にあっても構いません。*<Data_Protector_home>*¥bin 以外のディレクトリにある場合には、フルパス名の指定が必要です。
- 実行前/実行後コマンドはWindowsのパイプ機構を使って実行されます。実行前 / 実行後関数内で起動されたすべてのプロセスは、以降の処理が実行される前に完了していなければなりません。
- 実行前 / 実行後コマンドは、正常終了後すぐに負でない値を返さなければなりません。
- 実行前コマンドが正常終了しなかった場合 (ゼロ未満の値を返した場合)、バックアップ・セッションのステータスは「失敗」となり、セッションは中止されます。実行後コマンドは実行されません。

- 実行後コマンドが正常終了しなかった場合 (ゼロ未満の値を返した場合)、バックアップ・セッションのステータスは「完了 / エラー」となります。
- 実行後コマンドはセッションが中止されない限り常に実行されます。実行前コマンドは実行されないか、設定されません。
  OB2FORCEPOSTEXEC omnirc 変数が設定された場合、実行後コマンドは常に実行されます。
- バックアップ仕様に対する実行前 / 実行後コマンドは、デフォルトではバックアップのプレビュー中は実行されません。この動作は、グローバル・オプション・ファイルの変数 ExecScriptOnPreview によって定義されます。これらの値の変更方法は、「グローバル・オプション・ファイル」(645 ページ) を参照してください。
- 実行前 / 実行後コマンドは、DOS プロンプトから入力されるコマンドと同様に処理されます。したがって、パイプ (|) やリダイレクト記号 (> や <) などの特殊文字は使用できません。
- 実行前 / 実行後コマンドの実行中はバックアップ・セッションを中止できません。
- 実行前 / 実行後コマンドはバックグラウンド・モードで実行されます。したがって、ユーザーによる対話型操作が必要なコマンドは使用しないでください。
- 実行前 / 実行後コマンドの標準出力は、メッセージとして IDB に書き込まれ、Data Protector GUI のモニター画面に表示されます。
- Cell Manager 上でセッションの実行前 / 実行後コマンドを無効にするには、グローバル・オプション SmDisableScript を 1 に設定します。
- クライアント上でリモート・セッションの実行前 / 実行後コマンドを無効にするには、目的のクライアントの omnirc ファイルに OB2REXECOFF=1 を追加します。
- クライアントに保護を設定するには、どの Cell Manager にクライアントへのアクセスを許可するかを指定します。アクセスが許可された Cell Manager だけが、そのクライアント上で実行前 / 実行後コマンドを実行できます。クライアントへの保護の設定方法については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

特定のバックアップ・オブジェクトに対する実行前 / 実行後コマンド

オブジェクトに対する実行前 / 実行後コマンドはそれぞれ、オブジェクトのバックアップ前後に実行されます。これらのコマンドを、バックアップ仕様内のすべてのオブジェクト、または個々のオブジェクトに対して指定できます。Oracle などの統合ソフトウェアをバックアップする場合、データベースは 1 つのオブジェクトとして扱われるので、コマンドはデータベース・バックアップの前後に実行されます。これらのコマンドは Disk Agent が実行されているシステム上で実行されます。

コマンドの格納場所

バックアップ・オブジェクトに対する実行前 / 実行後スクリプトは、Data Protector Inet サービス・アカウント (デフォルトでは、ローカル・システム・アカウント) で起動されます。

Disk Agent が実行されているシステム上では、バックアップ・オブジェクトに対する実行前 / 実行後スクリプトはどのディレクトリにあっても構いません。ただし、クライアント・バックアップに対する実行スクリプトは、*<Data_Protector_home>*¥bin ディレクトリに置かなくてはなりません。スクリプトが *<Data_Protector_home>*¥bin ディレクトリにある場合はファイル名だけ指定すればよく、それ以外の場合はフルパス名を指定する必要があります。

ファイル名またはパス名の指定方法

実行前 / 実行後コマンドをバックアップ仕様内のすべてのオブジェクトに適用するには、バックアップ仕様の［オプション］タブをクリックします。[ファイルシステム・オプション](ディスク・イメージ・バックアップ用の保存済みバックアップ仕様では [ディスク・イメージ・オプション]) の [拡張] をクリックします。

実行前 / 実行後コマンドを個々のオブジェクトのみに適用するには、バックアップ仕様の［バックアップ・オブジェクトのサマリー］タブをクリックします。オブジェクトを右クリックして、[プロパティ] をクリックします。[オブジェクトのプロパティ] ダイアログ・ボックスで [オプション] タブをクリックします。

実行前 / 実行後コマンドを統合ソフトウェア・オブジェクトに適用するには、バックアップ仕様の［オプション］タブをクリックします。[アプリケーション固有オプション] の [拡張] をクリックします。

実行前および / または実行後テキスト・ボックスにファイル名またはパス名を入力します。

フルパス名を入力する場合、ディレクトリ名が 8 文字を超えるときは、パス名を引用符で囲むか、8.3 形式の DOS 互換形式で入力してください。

環境変数

BDACC

Disk Agent は終了コードを環境変数 **BDACC** に設定します (0(ゼロ) は正常終了)。この変数は実行後コマンド内でチェックできるので、実行後コマンドを Disk Agent の正常終了時に合わせて実行できます。

注記

ホスト・バックアップを実行する場合、実行前スクリプトは、あるシステムに対する 1 回目のファイルシステム・バックアップが行われる前に 1 回起動されます。また、実行後スクリプトはバックアップ後に起動されます。この場合、**BDACC** 変数は、単独のファイルシステム・オブジェクトに関連するものであり、クライアント全体に関連するものではないため、エクスポートできません。

キー・ポイント

- バックアップ・オブジェクトに対する実行前 / 実行後コマンドは実行可能ファイルまたはバッチファイルでなければなりません。Windows の場合、ファイル名の拡張子を指定する必要があります。
- Disk Agent が実行されているシステム上では、実行前 / 実行後コマンドはどのディレクトリにあっても構いません (クライアント・バックアップに対するものを除く)。*<Data_Protector_home>*¥bin 以外のディレクトリにある場合には、フルパス名の指定が必要です。
- 実行前コマンドが正常終了しなかった場合 (ゼロ以外の値を返した場合)、そのオブジェクトのバックアップは中止されます。オブジェクトのステータスは「中止」に設定され、バックアップ用 Disk Agent は処理を中止しますが、実行後コマンドは実行されます (実行後コマンドが環境変数 BDACC に依存している場合を除く)。オブジェクトのバックアップは作成されません。
- 実行後コマンドが正常終了しなかった場合 (ゼロ以外の値を返した場合)、バックアップ・オブジェクトのステータスは「中止」に設定されます。ただし、オブジェクトのバックアップは作成されるため、データを復元できます。

- 実行前 / 実行後コマンドは、DOS プロンプトから入力されるコマンドと同様に処理されます。したがって、パイプ (|) やリダイレクト記号 (> や <) などの特殊文字は使用できません。
- 実行前 / 実行後コマンドの実行中はバックアップ・セッションを中止できません。
- 実行前 / 実行後コマンドはバックグラウンド・モードで実行されます。したがって、ユーザーによる対話型操作が必要なコマンドは使用しないでください。
- 実行前 / 実行後コマンドの標準出力は、メッセージとして IDB に書き込まれ、Data Protector GUI のモニター画面に表示されます。
- デフォルトでは、実行前 / 実行後スクリプトは最低 15 分おきに何らかの出力を送信しなければなりません。そうしないと、このスクリプトを待機中のセッションは中止されます。このタイムアウト期間を変更するには、グローバル・オプション・ファイルの変数 `ScriptOutputTimeout` を変更します。
- タイムアウト機能を備えています。指定されたタイムアウト (単位:秒) 以内にメッセージが受信されない場合は、セッションが中止されます。
- 実行前 / 実行後スクリプトを無効にするには、クライアントの `omnirc` ファイルに `OB2OEXECOFF=1` という行を追加します。
- クライアントに保護を設定するには、どの Cell Manager にクライアントへのアクセスを許可するかを指定します。アクセスが許可された Cell Manager だけが、そのクライアント上で実行前 / 実行後コマンドを実行できます。クライアントへの保護の設定方法については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

UNIX システムでの実行前 / 実行後コマンド

本項では、UNIX 上での Cell Manager およびクライアントで実行前 / 実行後コマンドを実行する方法を説明します。

コマンドの記述方法 実行前 / 実行後コマンドは、シェル・スクリプトとして記述します。

「実行前 / 実行後コマンドの例 (UNIX の場合)」(A-21 ページ) を参照してください。

バックアップ仕様に対する実行前 / 実行後コマンド

バックアップ・セッションに対する実行前 / 実行後コマンドは、バックアップ・セッションの前後にそれぞれ起動されます。これらのコマンドは通常 Cell Manager 上で実行されますが、別のシステムを選択することもできます。

コマンドの格納場所

UNIX システムでは、バックアップ仕様に対する実行前 / 実行後コマンドはバックアップ・セッションのオーナーにより起動されます。ただし、オーナーが [ルート・ユーザーとしてバックアップ] 権限を持っている場合は root で起動されます。

Cell Manager 上では、バックアップ仕様に対する実行前 / 実行後コマンドはどのディレクトリにあっても構いません。

リモートの UNIX クライアント上では、バックアップ仕様に対する実行前 / 実行後コマンドは以下の場所に置くことが必要です。

- Solaris 7/8/9、HP-UX: `/opt/omni/lbin`
- Solaris 2.6、上記以外の UNIX システム : `/usr/omni/bin`

`/opt/omni/lbin` または `/usr/omni/bin` ディレクトリにあるコマンドはファイル名だけ指定すればよく、それ以外のコマンドはフルパス名を指定する必要があります。

ファイル名またはパス名の指定方法

コマンドの指定方法の詳細は、オンライン・ヘルプの索引キーワード「バックアップ仕様に対する実行前 / 実行後コマンド」を参照してください。

環境変数

バックアップ・セッションの開始時に以下の環境変数がエクスポートされます。この環境変数は、任意のホストのバックアップ仕様セッションに対する実行前 / 実行後スクリプト内で使用できます。

DATALIST バックアップ仕様の名前

MODE バックアップ動作の種類 (フル、増分、増分 1 など)。

OWNER セッションのオーナー

この変数の内容は以下に示すとおりデータベースの形式と同じです (大文字と小文字が区別されます)。
UNIX の場合 - *< ユーザー >.< グループ >@< ホスト名 >*、
Windows の場合 - *< ドメイン >¥< ユーザー >@< ホスト名 >*

PREVIEW プレビューの実行中は 1 に、バックアップの実行中は 0(ゼロ) に設定されます。コマンドを変更して、バックアップ中にだけ実行され、プレビュー中には実行されないようにする場合に、この変数を使用します。デフォルトでは、実行前コマンドおよび実行後コマンドはプレビューに対して実行されません。これを有効にするにはグローバル・オプション `ExecScriptOnPreview` を使用します。

RESTARTED 現在のセッションが、再起動されたバックアップ・セッションである場合は 1 に設定されます。そうでない場合は 0 に設定されます。実行後コマンドはこの変数を使って、**SMEXIT** = 0 の場合にさらに再起動が行われるのを防止します。

SESSIONID 完了したセッションの識別に使用する変数で、データベースに記録されます。この変数を使ってセッションのプレビューはできません (この場合は SESSIONKEY を使用します)。

SESSIONKEY 実行中のセッションの識別に使用します。たとえば、問題が発生した場合、バックアップ・セッションの開始前にこの変数を使ってセッションを中止できます。

SMEXIT Session Manager の終了コードで、`omnib` コマンドの終了コードと同じです。この変数を使用できるのは実行後コマンドだけです。エージェントとは、Disk Agent、Media Agent、Application Agent、または Symmetrix Agent などを指します。SMEXIT 値の詳細は、表 (324 ページ) を参照してください。

キー・ポイント

ローカル・ホストまたはリモート・ホストのバックアップ仕様に対する実行前 / 実行後コマンドを構成する前に、以下の項目を確認してください。

- 実行前コマンドが正常終了しなかった場合 (ゼロ以外の値を返した場合)、セッションのバックアップ・ステータスは「失敗」となり、セッションは中止されます。実行後コマンドは実行されません。
- 実行後コマンドが正常終了しなかった場合 (ゼロ以外の値を返した場合)、セッションのバックアップ・ステータスは「完了 / エラー」となります。

- 実行後コマンドはセッションが中止されない限り常に実行されます。実行前コマンドは実行されないか、設定されません。
  OB2FORCEPOSTEXEC omnirc 変数が設定された場合、実行後コマンドは常に実行されます。
- バックアップ仕様に対する実行前 / 実行後コマンドは、デフォルトではバックアップのプレビュー中は実行されません。この動作は、グローバル・オプション・ファイルの変数 ExecScriptOnPreview によって定義されます。詳細は、「グローバル・オプション・ファイル」(645 ページ) を参照してください。
- 実行前 / 実行後コマンドの実行中はバックアップ・セッションを中止できません。
- 実行前 / 実行後コマンドはバックグラウンド・モードで実行されます。したがって、ユーザーによる対話型操作が必要な実行前 / 実行後コマンドは使用しないでください。
- デフォルトでは、実行前 / 実行後スクリプトは最低 15 分おきに何らかの出力を送信しなければなりません。そうしないと、このスクリプトを待機中のセッションは中止されます。このタイムアウト期間を変更するには、グローバル・オプション・ファイルの変数 ScriptOutputTimeout を変更します。
- タイムアウト機能を備えています。指定されたタイムアウト (単位:秒) 以内にメッセージが受信されない場合は、セッションが中止されます。
- ホスト上に実行可能スクリプトがない場合、またはスクリプトのパスが間違っている場合は、スクリプトの実行に失敗し、セッションが中止されたことを示すエラー・メッセージが表示されます。
- コマンドが標準出力にテキストを書き込んだ場合、このテキストは Session Manager に送信され、データベースに書き込まれます。標準エラーは /dev/null へリダイレクトされます。このエラーを標準出力にリダイレクトすることにより、エラー・メッセージをデータベースに記録できます。

注記

実行前 / 実行後スクリプトが新しいプロセスへ分岐する前にすべてのファイル記述子を閉じなかった場合、スクリプトがハングするおそれがあります。これはバックグラウンドで実行されている新しいプロセス (データベース・サーバ・プロセス dbstart など) がハングした場合に発生します。こ

の場合、ユーザーは detach コマンドを使用できます。detach コマンドのソース・プログラムは detach.c ファイルにあります。このコマンドは正式にはサポートされていません。例 :

```
/opt/omni/lbin/utilns/detach pre_script [arguments...]
```

- Cell Manager 上でセッションの実行前 / 実行後コマンドを無効にするには、グローバル・オプション SmDisableScript を 1 に設定します。
- クライアント上でリモート・セッションの実行前 / 実行後コマンドを無効にするには、目的のクライアントの omnirc ファイルに OB2REXECOFF=1 を追加します。
- クライアントに保護を設定するには、どの Cell Manager にクライアントへのアクセスを許可するかを指定します。アクセスが許可された Cell Manager だけが、そのクライアント上で実行前 / 実行後コマンドを実行できます。クライアントへの保護の設定方法については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

特定のバックアップ・オブジェクトに対する実行前 / 実行後コマンド

オブジェクトに対する実行前 / 実行後コマンドはそれぞれ、オブジェクトのバックアップ前後に実行されます。これらのコマンドを、バックアップ仕様内のすべてのオブジェクト、または個々のオブジェクトに対して指定できます。Oracle などの統合ソフトウェアをバックアップする場合、データベースは 1 つのオブジェクトとして扱われるので、コマンドはデータベース・バックアップの前後に実行されます。これらのコマンドは Disk Agent が実行されているシステム上で実行されます。

コマンドの格納場所 UNIX システムでは、バックアップ・オブジェクトに対する実行前 / 実行後コマンドはバックアップ・セッションのオーナーにより起動されます。ただし、オーナーが [ルート・ユーザーとしてバックアップ] 権限を持っている場合は root で起動されます。

Disk Agent が実行されているシステム上では、バックアップ・オブジェクトに対する実行前 / 実行後コマンドはどのディレクトリにあっても構いません。ただし、クライアント・バックアップに対しては、/opt/omni/lbin ディレクトリ (HP-UX の場合)、または /usr/omni/bin ディレクトリ (その他の UNIX システムの場合) になけ

ればなりません。コマンドが /opt/omni/lbin または /usr/omni/bin ディレクトリにある場合はファイル名だけ指定すればよく、それ以外の場合はフルパス名を指定する必要があります。

ファイル名またはパス名の指定方法

コマンドの指定方法の詳細は、オンライン・ヘルプの索引キーワード「バックアップ・オブジェクトに対する実行前 / 実行後コマンド」を参照してください。

環境変数

バックアップ・セッションの開始時に以下の環境変数がエクスポートされます。この環境変数は、Disk Agent の実行されているシステム上のオブジェクトに対する実行前 / 実行後スクリプト内で使用できます。

BDACC

Disk Agent は終了コードを環境変数 BDACC に設定します (0(ゼロ) は正常終了)。この変数は実行後スクリプト内でチェックできるので、実行後コマンドを Disk Agent の正常終了時に合わせて実行できます。

注記

ホスト・バックアップを実行する場合、実行前スクリプトは、あるシステムに対する 1 回目のファイルシステム・バックアップが行われる前に 1 回起動されます。また、実行後スクリプトはバックアップ後に起動されます。この場合、BDACC 変数は、単独のファイルシステム・オブジェクトに関連するものであり、クライアント全体に関連するものではないため、エクスポートできません。

キー・ポイント

実行前 / 実行後コマンドを構成する前に、以下のキー・ポイントを確認してください。

- オブジェクトに対する実行前 / 実行後コマンドは、バックアップのプレビュー中も実行できます。したがって、最初にバックアップをプレビューした後で実行前 / 実行後コマンドを追加したり、スクリプトで環境変数 PREVIEW をチェックしたりします。
- オブジェクトに対する実行前コマンドが正常終了しなかった場合 (0 以外の値を返した場合)、このオブジェクトのバックアップ・ステータスは「中止」に設定され、バックアップ用の Disk Agent は処理を中止しますが、実行後コマンドは実行されます (実行後コマンドが環境変数 BDACC に依存している場合を除く)。オブジェクトのバックアップは作成されません。

- 実行後コマンドが正常終了しなかった場合 (ゼロ以外の値を返した場合)、オブジェクトのバックアップ・ステータスは「中止」に設定されます。ただし、オブジェクトのバックアップは作成されるため、データを復元できます。
- デフォルトでは、実行前 / 実行後コマンドは最低 120 分おきに何らかの出力を Disk Agent に送信しなければなりません。そうしないと、オブジェクトのバックアップは中止されます。このタイムアウト期間を変更するには、グローバル・オプション・ファイルの変数 `SmDaIdleTimeout` を変更します。
- 実行前 / 実行後コマンドは、シェル・プロンプトから入力されるコマンドと同様に処理されます。パイプ (|) やリダイレクト記号 (> や <) などの特殊文字は使用できません。
- 実行前 / 実行後コマンドの実行中はバックアップ・セッションを中止できません。
- 実行前 / 実行後コマンドはバックグラウンド・モードで実行されます。したがって、ユーザーによる対話型操作が必要な実行前 / 実行後コマンドは使用しないでください。
- コマンドが標準出力にテキストを書き込んだ場合、このテキストは Disk Agent が受信し、Session Manager に送信され、データベースに書き込まれます。標準エラーは `/dev/null` へリダイレクトされます。このエラーを標準出力にリダイレクトすることにより、エラー・メッセージをデータベースに記録できます。
- オブジェクトに対する実行前 / 実行後コマンドは、Disk Agent が実行されているクライアント上に置く必要があります。
- 実行前 / 実行後コマンドは実行可能ファイルでなければなりません。また、このコマンドのフルパス名を指定しなければなりません。
- 実行前 / 実行後スクリプトを無効にするには、クライアントの `omnirc` ファイルに `OB2OEXECOFF=1` という行を追加します。
- クライアントに保護を設定するには、どの Cell Manager にクライアントへのアクセスを許可するかを指定します。アクセスが許可された Cell Manager だけが、そのクライアント上で実行前 / 実行後コマンドを実行できます。クライアントへの保護の設定方法については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

失敗したバックアップの管理

バックアップ時に、一部のシステムは、シャットダウンしたり、ネットワークの問題が発生したり、または同様の問題が発生したために使用不可能になる場合があります。この結果、一部のシステムのバックアップが完了しません。

設定の通知

Data Protector では、通知を構成することにより、バックアップ・セッション中に発生する予期しないイベント (マウント要求またはデバイス・エラーなど) をユーザーに通知できます。ユーザーは、要望に最も適した通知方法を選択できます (電子メール、ブロードキャスト・メッセージを Windows の画面に表示するなど)。

詳細については、第 9 章「モニター、レポート、通知、およびイベント・ログ」(407 ページ) を参照してください。

失敗したバックアップのチェック

バックアップを管理する上で最も重要なポイントの 1 つは、バックアップ・ステータスの定期的なチェックです。Data Protector は総合的なレポート機能を備えており、バックアップ・ステータスに関するレポートを表示できます。レポート機能の詳細は、「セッションのモニター」(409 ページ) を参照してください。

システム・ディスクのバックアップ時の警告

Windows システム上でシステム・ディスクをバックアップする際、Data Protector により警告が表示されます。この警告が表示される理由は、システム・ディスク上の特定のファイルが常に使用中であり、Disk Agent をはじめ、どのアプリケーションからもこのファイルを開くことができないためです。これらのファイルの内容は、`CONFIGURATION` の一部としてのみバックアップできます。

ファイルシステムのバックアップ時にこれらのファイルへのアクセスが行われた場合 (システム・ディスク全体をバックアップする場合など)、Data Protector はこれらのファイルのオープンに失敗するため、このことが警告 (またはバックアップ・オプションによってはエラー) として通知されます。「バックアップ・オプションの使用」(290 ページ) を参照してください。

この動作は、ファイルシステム・バックアップの観点からは正しい動作ですが、管理機能上の問題となる可能性があります。これは、常に大量の警告が通知され、他のファイルで発生している障害を見落とすおそれがあるためです。

これら特定のファイルをバックアップできるのは、CONFIGURATION バックアップを実行した場合だけです。このことを念頭に置いて、ファイルシステム・バックアップから上記ファイルを除外することにより、この警告が表示されないようにすることができます。

例として、稼動中の Windows システム上で開くことができないファイルの一覧を以下に示します (Windows ソフトウェアが C: ドライブにインストールされている場合)。

```
<%SystemRoot%>¥system32¥config¥default

<%SystemRoot%>¥system32¥config¥default.LOG

<%SystemRoot%>¥system32¥config¥SAM

<%SystemRoot%>¥system32¥config¥SAM.LOG

<%SystemRoot%>¥system32¥config¥SECURITY

<%SystemRoot%>¥system32¥config¥SECURITY.LOG

<%SystemRoot%>¥system32¥config¥software

<%SystemRoot%>¥system32¥config¥software.LOG

<%SystemRoot%>¥system32¥config¥system

<%SystemRoot%>¥system32¥config¥SYSTEM.ALT
```

ログオンした各ユーザー側では、以下のファイルも開くことができません。

```
<%SystemRoot%>¥Profiles¥<user>¥NTUSER.DAT

<%SystemRoot%>¥Profiles¥<user>¥ntuser.dat.LOG
```

重要

システム・ディスクのファイルシステム・バックアップを実行する場合、上記のファイルはバックアップされません。上記ファイルを除外することで解決できるのは、セッション・レポートの管理上の問題だけです。上記ファイルの内容をバックアップするには、CONFIGURATION バックアップを実行してください。

休止中のシステム・ディスクをバックアップする場合 (デュアル・ブート・システムの場合など)、上記のファイルは、現在稼動中の CONFIGURATION には含まれません。したがって、上記のファイルはファイルシステム・バックアップとしてバックアップ可能なため、除外しないようにしてください。

バックアップの失敗を防止する

Data Protector はバックアップの確実性を高める機能を備えており、バックアップが失敗する可能性を低減することができます。

オブジェクトのバックアップが開始できなかった場合、Data Protector はバックアップ・セッションの最後にもう一度このオブジェクトのバックアップを試行します。それでもバックアップに失敗した場合は、オブジェクトはバックアップされず、オブジェクトとセッションのステータスは「失敗」となります。再度バックアップするようスケジュールされている場合は、バックアップが繰り返し実行されます。これにより一部のオブジェクトのバックアップが正常に実行された場合は、セッションのステータスは「完了 / 失敗」となります。

バックアップ・スケジュールが設定された時点で起動および実行されていないクライアントは、他のオブジェクトのバックアップが完了した後、バックアップの再試行が行われます。最初にバックアップに失敗したオブジェクトの再試行が実行されるまで、バックアップ・セッションは 30 秒間中断されます。この待機時間を変更するには、グローバル・オプション WaitBeforeRetry を使用します。グローバル・オプションの変更方法の詳細は、「グローバル・オプション・ファイル」(645 ページ) を参照してください。

重要

バックアップが頻繁に行われないようにスケジュールしている場合は、データの最新バックアップが存在しない期間が発生する可能性があります。

注記

Data Protector は常にデータのフル・バックアップを必要とします。保護されたフル・バックアップに使用可能なものがない場合は、次回に増分バックアップがスケジュールされていても、フル・バックアップが実行されます。これを避けるには、バックアップをスケジュールする前に、バックアップに失敗したシステムに対して対話型のフル・バックアップを実行してください。

フル・バックアップおよび増分バックアップの動作の詳細は、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

[切断された接続の再接続] バックアップ・オプションを設定すると、Data Protector はバックアップ・セッション中にネットワークで短期間のエラーが発生した場合に以下を再接続します。

- Backup Session Manager と Disk Agent または Media Agent(コントロール接続)
- バックアップ中の Disk Agent と Media Agent(データ接続)

(この状況は信頼性の低い LAN ネットワークで頻繁に発生します。) このタイムアウト値は、`OB2RECONNECT_RETRY` `omnirc` 変数を使って定義できます。`omnirc` ファイルの使用方法については、「omnirc オプションの使用」(647 ページ) を参照してください。

Wake ONLAN サポートを使用可能にする

リモート操作による電源投入 (**Wake ONLAN**) が可能なマシンをお使いの場合は、Data Protector の Wake ONLAN サポートを使用できます。Backup Session Manager が、Wake ONLAN サポートを使用するよう構成されているクライアントへの接続に失敗した場合、Backup Session Manager は Wake ONLAN プロトコルに従ってウェイク・アップ要求を送信し、クライアントへの再接続を試みます。これにより、デスクトップ・システムの節電機能をフルに活用でき、節電機能によりバックアップ・プロセスが妨害されるのを防止できます。

注記

Wake ONLAN 対応 LAN インタフェース (HP NightDIRECTOR シリーズなど) を備えたコンピュータでは、Wake ONLAN サポートを使用可能に設定できます。Wake ONLAN (WOL) オプションは、BIOS の設定時に使用できます。

Windows クライアントに Disk Agent をインストールして、このクライアントをセルに追加した場合、このクライアントの MAC アドレスが自動的に検索されます。また、Wake ONLAN (WOL) オプションを使用可能にしたセクションで MAC アドレスを手動で変更できます。以下を参照してください。

Windows クライアントで Wake ONLAN サポートを使用可能に設定するには、以下の手順を行います。

1. ［Data Protector Manager］で［クライアント］コンテキストを選択します。
2. Scoping ペインで、WOL オプションを使用可能にしたいクライアントを右クリックした後、[プロパティ] をクリックします。
3. [拡張] タブをクリックします。
4. [マジック・パケット] セクションを選択して、[マジック・パケットを使用可能にする] チェックボックスを選択した後、[適用] をクリックします。

失敗したバックアップの再開

Data Protector では、バックアップが正常に実行されなかったオブジェクトのバックアップだけを容易に再開できます。以下の手順を行います。

1. ［Data Protector Manager］で［内部データベース］コンテキストを選択します。
2. ［内部データベース］で、［セッション］を展開します。
3. 結果エリアで目的のバックアップを検索します。

   各カラムの一番上にあるボタンを使ってセッションの順番を並べ替えることができます。
4. 正常に実行されなかったセッションを右クリックした後、[失敗したオブジェクトの再開] を選択します。

   ダイアログ・ボックスにセッションの再開を確認するメッセージが表示されます。[はい] をクリックします。

7 データのコピー

本章の概略

本章では、バックアップ中またはバックアップ後にバックアップ・データを複製できるようにする Data Protector の機能について説明します。本章は以下の項で構成されています。

概要

バックアップ・データを複製することによって、多くの利点がもたらされます。セキュリティや可用性を強化するために、または運用上の理由から、データをコピーできます。

Data Protector では、オブジェクトコピー、オブジェクトミラー、およびメディア・コピーといった方法でバックアップ・データを複製できます。本章ではこれらの方法について説明します。各複製方法の比較については、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

複製方法は組み合わせて使用することもできます。たとえば、オブジェクトミラーによって作成されたデータからオブジェクトコピーまたはメディア・コピーを作成することができます。あるいは、オブジェクトコピーを格納したメディア全体をコピーすることもできます。

オブジェクトのコピー

オブジェクトコピーとは

Data Protector のオブジェクトコピー機能では、選択したオブジェクト・バージョンを特定のメディア・セットにコピーできます。1 つまたは複数のバックアップ・セッションからオブジェクト・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、Data Protector がソース・メディアからバックアップ・データを読み込み、そのデータを転送して、ターゲット・メディアに書き込みます。

オブジェクトコピー セッションを実行すると、指定したオブジェクト・バージョンのコピーを格納したメディア・セットが出来上がります。

オブジェクトコピー機能の特性は、以下のとおりです。

- セッションの起動

  オブジェクトコピー セッションは、対話型で起動するか、自動で起動することができます。

- メディアの選択

  ソース・メディアとして、バックアップを格納したオリジナルのメディア・セット、オブジェクトコピーを格納したメディア・セット、またはメディア・コピーであるメディア・セットを使用できます。

  ただし、オブジェクトコピー セッションの起動後はメディア・セットを選択できません。マウントを要求された場合は、Data Protector から要求された特定のメディアか、それと同一のコピー (メディア・コピー機能によって作成) を指定する必要があります。

- メディアの種類

  異なる種類のメディアにオブジェクトをコピーできます。また、コピー先のデバイスのブロック・サイズがソース・デバイスのブロック・サイズを上回ることもできます。

- メディアのポリシー

  バックアップまたはオブジェクトコピーがすでに格納されているメディアに、データを追加することができます。

オブジェクトコピーを使用する理由

バックアップ・データの追加コピーは、以下に示す複数の目的で作成されます。

- ボールティング

  バックアップ・オブジェクトのコピーを複数作成して、さまざまな場所に保管することができます。

- メディアの解放

  メディア上の保護されたオブジェクト・バージョンのみを保存するには、これらのオブジェクト・バージョンをコピーしてから、上書きできるようにメディアを解放します。

- メディアの集約

  オブジェクトのコピーによってデータのインターリーブを避けることができます。

- 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。

- 他のメディアの種類への移行

  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。

- 高度な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。

オブジェクトコピーの使用

オブジェクトコピー機能の必要条件と制限事項は、以下のとおりです。

必要条件

- オブジェクトコピー セッションに関わるすべてのシステムに、Media Agent をインストールする必要があります。
- Data Protector セル内に少なくとも 2 つのバックアップ・デバイスを構成する必要があります。
- オブジェクトコピー セッションに使用するメディアを準備しておく必要があります。
- オブジェクトコピー セッションを実行するための適切なユーザー権限

が必要です。

制限事項

- ZDB バックアップ、ダイレクト・バックアップ、NDMP バックアップ機能を使用してバックアップしたオブジェクトはコピーできません。
- 1 つのオブジェクトコピー セッションにおいて、1 つのオブジェクト・バージョンに対して複数のコピーを作成することはできません。
- コピー先のデバイスには、ソース・デバイスと同じかそれよりも大きいブロック・サイズが必要です。
- 同一のオブジェクトコピー セッションでは、ソース・メディア (オブジェクトのコピー元) とターゲット・メディア (オブジェクトのコピー先) に同じメディアは使用できません。
- オブジェクトのコピー中は、コピー元のメディアを復元に使用することはできません。
- オブジェクトコピー セッションでは、エージェント間の再接続機能は使用できません。
- SAP DB、DB2、または SQL 統合ソフトウェア・オブジェクトを非マルチプレックス化することはできません。

オブジェクトコピー機能の使用方法

まず、オブジェクトコピーの仕様を作成します。この仕様のなかで、コピー対象のオブジェクト、使用するメディアとデバイス、セッションのオプション、メディアの位置の優先順位を選択します。メディアの位置の優先順位は、同じオブジェクトが複数のメディア・セットに存在する場合の、Data Protector によるメディアの選択方法に影響を与えます。

重要

統合ソフトウェア・オブジェクトは、相互に依存している可能性があります。このような統合ソフトウェア・オブジェクトをコピーするときは、コピー対象として、同じバックアップ ID を持つオブジェクトをすべて選択してください。データベースの復元に必要なすべてのオブジェクトをコピーしなければ、コピーからの復元は不可能です。

オブジェクトのコピー元のメディアは**ソース・メディア**と呼ばれ、オブジェクトのコピー先のメディアは**ターゲット・メディア**と呼ばれています。ソース・メディアとターゲット・メディアは、メディアの種類が異なる場合もあります。

デバイスの選択

ソース・メディアとターゲット・メディアによって使用されるデバイスは分ける必要があります。コピー先の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・サイズを上回ることができます。ただし、パフォーマンスへの影響を避けるために、デバイスは同じブロック・サイズに設定し、すべてを同じシステムか SAN 環境に接続するようにお勧めします。

重要

SAP DB、DB2、または Microsoft SQL Server 統合ソフトウェア・オブジェクトのコピーに必要なデバイスの最小数は、バックアップに使用したデバイスの数と同じになります。これらのオブジェクトのバックアップとコピーでは、デバイスの同時処理数に同じ値を設定しなければなりません。

オブジェクトコピーはデフォルトで負荷調整されています。Data Protector は、できる限り多くのデバイスを使用することでデバイスの利用を最適化します。

使用するソース・デバイスがオブジェクトコピーの仕様で指定されていない場合、Data Protector はデフォルトのデバイスを使用します。デフォルトでは、オブジェクトの書き込みに使用されたデバイスがソース・デバイスとして使用されます。コピー先デバイスがオブジェクトごとに指定されていない場合、Data Protector が、オブジェクトコピーの仕様で選択されているデバイスの中から、最適なデバイスを自動的に選択します。

デバイスはセッションの開始時にロックされます。セッション開始後にデバイスをロックすることはできないため、セッションの開始時に使用不可能なデバイスは、そのセッションでは使用できません。メディアのエラーが発生した場合、エラーの発生したデバイスはそのコピーセッション内では使用されなくなります。

処理の結果

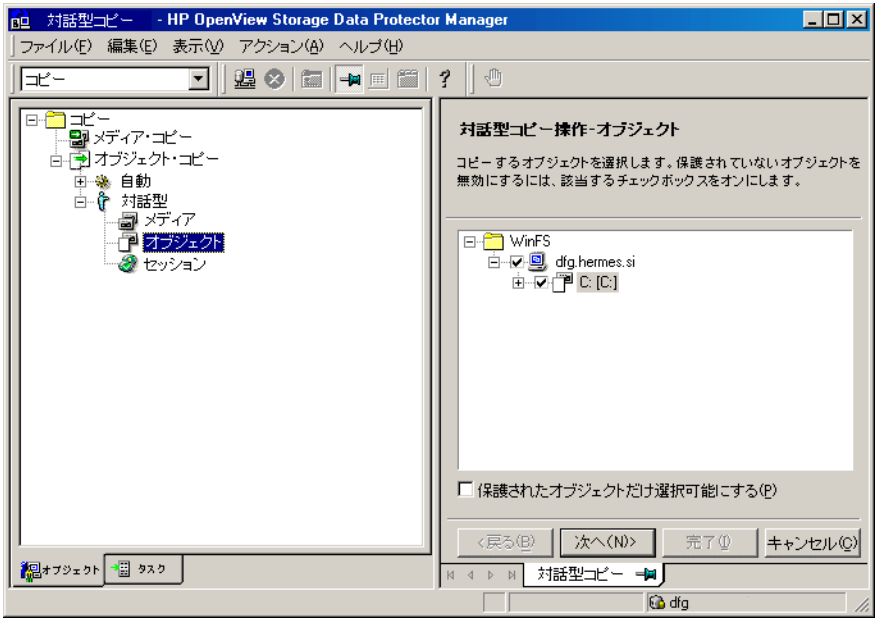
オブジェクトコピー セッションが正しく完了したら、選択したバックアップ・オブジェクトの追加コピーが別のメディア・セット上に出来上がります。

オブジェクトコピーの構成

オブジェクトコピー セッションは、オブジェクトコピーの仕様に基づいて実行されます。オブジェクトコピーの仕様を構成するには、以下の手順を行います。

1. セッションの種類を選択します。対話型または自動 (ポスト・バックアップまたはスケジュール設定) のどちらかです。
2. コピー対象を選択します。
3. コピーに使用するデバイスを選択します。
4. コピー方法 (セッションのオプション) を選択します。

図 7-1　対話型コピーでのオブジェクトの選択



対話型のオブジェクトコピー

対話型のオブジェクトコピー セッションは、対話型のオブジェクトコピーの仕様を使用して開始されます。対話型のオブジェクトコピーの仕様は保存できません。オブジェクトコピー セッションを開始できるだけです。

[コピー] コンテキストで [コピー] を展開し、さらに [対話型] を展開して、[メディア]、[オブジェクト]、または [セッション] をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「対話型オブジェクト・コピー」を参照してください。

自動オブジェクトコピー

Data Protector には、2 種類の自動オブジェクトコピー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」**と**「スケジュールされたオブジェクトコピー」**です。

自動オブジェクトコピーの仕様では、コピーされるオブジェクト・バージョンに関する 1 つまたは複数の選択基準を指定できます。

- バックアップ仕様 - 特定のバックアップ仕様によってバックアップされるオブジェクト・バージョンのみをコピーする場合。
- データ保護 - データ保護されたオブジェクト・バージョンのみをコピーする場合。
- 既存のコピーの数 - 指定された数を上回る正常なコピーが存在しないオブジェクト・バージョンのみをコピーする場合。
- ライブラリ - 指定されたライブラリ内のメディアに位置するオブジェクト・バージョンのみをコピーする場合。
- 時間枠 (スケジュールされたオブジェクトコピー仕様のみ) - 指定された期間内にバックアップされたオブジェクト・バージョンのみをコピーする場合。

ポスト・バックアップのオブジェクトコピー

ポスト・バックアップのオブジェクトコピーは、自動オブジェクトコピーの仕様で指定されたバックアップ・セッション完了後に実行されます。この機能では、特定のバックアップ・セッションでバックアップされたオブジェクトを、自動オブジェクトコピーの仕様に基づいて選択してコピーします。

[コピー] コンテキストで [コピー] を展開し、さらに [自動] を展開して、[ポスト・バックアップ] を右クリックして、[追加] をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「ポスト • バックアップのオブジェクト • コピー」を参照してください。

スケジュールされたオブジェクトコピー

スケジュールされたオブジェクトコピーは、ユーザーの定義した時間に実行されます。複数のバックアップ・セッションでバックアップされたオブジェクトを、1 つのスケジュールされたオブジェクトコピー・セッション内でコピーできます。

スケジュールされたオブジェクトコピーを構成して、特定の日時にコピーを実行したり、定期的にコピーを実行できます。スケジュールのリセットや、有効 / 無効を切り替えることも可能です。また、休日のオブジェクトコピーを有効または無効にすることもできます。

[コピー] コンテキストで [コピー] を展開し、さらに [自動] を展開して、[スケジュール済み] を右クリックして、[追加] をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「スケジュールされたオブジェクト・コピー」を参照してください。

オブジェクトコピー・オプション

オブジェクトコピーの仕様では、オブジェクトコピーに対するデータ保護、カタログ保護、ログ・レベルを指定できます。同等のオプションはバックアップに対しても使用されます。これらのオプションの詳細は、「最も頻繁に使用されるバックアップ・オプション」(292 ページ) を参照してください。

ユーザーのポリシーによって、バックアップされたオブジェクトとそのコピーに指定されるオプションの値を同じにしたり別々にすることができます。たとえば、バックアップ性能を向上させるためにバックアップ・オブジェクトに対しては [ログなし] を指定し、次に続くオブジェクトコピーセッションでは、同じオブジェクトに対して [すべてログに記録] を指定することができます。

バックアップされたオブジェクトとまったく同じコピーを作成するには、オブジェクトコピーに対して同じログ・レベルを指定します。オブジェクトコピーのログ・レベルを [ログなし] よりも高く設定すると、IDB のサイズに影響するので注意が必要です。これらのオプションが IDB のサイズに与える影響については、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

重要

ZDB からディスク / テープへのバックアップ・セッションで作成したオブジェクトをコピーする場合は、[コピーが正常に実行された後でデータとカタログ保護をリサイクル] オプションは選択しないでください。このオプションを選択すると、メディアが上書きされた時点で、GUI からこのバックアップ・データを使ったインスタント・リカバリを実行することはできなくなります。

コピー元のメディア・セットを選択する

コピーしたいオブジェクト・バージョンが、Data Protector のいずれかのデータ複製方法を使用して、複数のメディア・セット上に作成されている場合は、どのメディア・セットをコピー元に使用しても構いません。デフォルトでは、コピー元となるメディア・セットは自動的に選択されます。メディア・セットの選択をユーザーが設定するには、メディアの位置の優先順位を指定します。

全体的なメディア選択手順は、復元処理の場合と同じです。詳細は、「復元元のメディア・セットを選択する」(404 ページ) を参照してください。[オブジェクト] または [セッション] から、対話形式でオブジェクトコピーを実行する場合は、コピー元のメディア・セットを手動で選択することも可能です。自動オブジェクトコピーの構成時にメディアを選択することはできません。通常、オブジェクトのバックアップは、これより後で実行されるためです。

オブジェクトコピーの完了ステータス

オブジェクトが配置されているすべてのメディアのログが IDB 内に記録されている場合は、ステータスが [完了] または [完了 / エラー] となっているオブジェクトをコピーできます。コピー操作が正常に完了したら、コピーされたオブジェクトのステータスは、対応するバックアップ・オブジェクトのステータスと同じになります。

バックアップ・セッションが失敗した場合は、ポスト・バックアップのオブジェクトコピー セッションは開始されません。バックアップ・セッションは中止されたが、一部のオブジェクトは既に作成されている場合には、作成済みのオブジェクトが、ポスト・バックアップのオブジェクトコピー セッションでコピーされます。これはデフォルトの動作です。セッションが中止された場合は、コピーを行わないようにするには、グローバル変数 [CopyStartPostBackupOnAbortedSession] を 0 に設定してください。

オブジェクトコピー セッションを中止したり、その他の原因でセッションが失敗した場合、セッションのステータスは [失敗] になります。ステータスが [失敗] になったオブジェクトコピーは、2 度とコピーできません。データ保護とカタログ保護が [なし] に設定されるからです。

オブジェクトコピーに基づくタスク

オブジェクトコピー機能を使用すると、以下のタスクも実行できます。

ボールティング

ボールティングとは、メディアを「ボールト」と呼ばれる安全な場所に保存するプロセスのことです。 メディアはボールト内で一定期間保管されます。詳細は、「メディアのボールティング」(199 ページ) を参照してください。

復元作業用にバックアップ・データのコピーを保管しておくことをお勧めします。追加でコピーを取得するには、必要に応じて、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・コピーの各機能を使用できます。

オブジェクトコピー機能を使ってボールティング用のコピーを作成する方法については、オンライン・ヘルプの索引キーワード「オブジェクトのコピー - ボールティング用」を参照してください。

メディアの解放

保護されたバックアップだけを保持し、保護されていないバックアップは上書きすることによって、メディアのスペースの消費を最小限に抑えることができます。1 つのメディア内に保護されたものと保護されていないものが混在する可能性があるので、保護されたオブジェクトを新しいメディア・セットにコピーして、上書き用のメディアはそのままにしておくことができます。

メディアを解放する方法については、オンライン・ヘルプの索引キーワード「メディアの解放」を参照してください。

メディアの集約

多重化されているメディアには、複数のオブジェクトのインタリーブされたデータが含まれます。このようなメディアは、デバイスの同時処理数が 2 以上のバックアップ・セッションから作成されます。多重化されたメディアを使用すると、バックアップのプライバシーが損なわれたり、復元に時間がかかったりすることがあります。

Data Protector には、メディアを集約する機能が備わっています。多重化されているメディアのオブジェクトは、ユーザーの指定する複数のメディアにコピーされます。

メディアを集約する方法については、オンライン・ヘルプの索引キーワード「メディアの集約」を参照してください。

復元チェーンの統合

1 つのオブジェクト・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・セットにコピーすることができます。このメディア・セットを使用すれば、複数のメディアをロードして必要なオブジェクト・バージョンを探す必要がなくなるため、復元が高速で簡単になります。

復元チェーンを統合する方法については、オンライン・ヘルプの索引キーワード「復元チェーンの統合」を参照してください。

他のメディアの種類への移行

バックアップ・データを他のメディアの種類に移行できます。たとえば、オブジェクトをファイル・デバイスから LTO デバイスにコピーしたり、DLT デバイスから LTO デバイスにコピーできます。

他のメディアの種類に移行する方法については、オンライン・ヘルプの索引キーワード「他のメディアの種類への移行」を参照してください。

ディスク・ステージング

オブジェクトコピー機能は、ディスク・ステージングを実現するためにも使用できます。ディスク・ステージングの概念については、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

ディスク・ステージングは、この目的のために明示的に構成されたオブジェクトコピー仕様を使用して実行します。ディスク・ステージングの具体例については、オンライン・ヘルプの索引キーワード「ディスク・ステージング」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

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・セッション時に同じデータを複数のメディア・セットに同時に書き込むことができます。バックアップ・オブジェクトの全体または一部を、1 つまたは多数のメディア・セットにミラーリングできます。

オブジェクトミラーの利点

オブジェクトミラー機能を使用することで以下の目的が達成されます。

- 複数のコピーを存在させることで、利用可能なバックアップ・データが増加します。
- バックアップ・データをリモート・サイトにミラーリングすることができるので、複数サイトへのボールティングが簡単になります。
- 同じデータを複数のメディアに書き込むことができるので、バックアップのフォールト・トレランスが向上します。メディア上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使用

オブジェクトミラー機能の制限事項は以下のとおりです。

制限事項

- ZDB バックアップ、ダイレクト・バックアップ、NDMP バックアップ機能を使用してバックアップしたオブジェクトはミラーリングできません。
- 単一のセッションで 1 つのオブジェクトを同じデバイスに複数回ミラーリングすることはできません。
- デバイスのブロック・サイズがミラー・チェーン内で減少してはいけません。具体的には以下のとおりです。
  - ミラー 1 の書き込みに使用されるデバイスには、バックアップに使用されるデバイスと同じかそれよりも大きいブロック・サイズが必要です。
  - ミラー 2 の書き込みに使用されるデバイスには、ミラー 1 の書き込みに使用されるデバイスと同じかそれよりも大きいブロック・サイズが必要です。以下同じように続きます。

オブジェクトミラーの使用方法

オブジェクトミラーは、バックアップ仕様の構成時に指定します。バックアップ仕様の構成方法については、「バックアップ仕様の作成」(212 ページ) を参照してください。

バックアップ仕様で、ミラーリングするオブジェクトを選択して、次にミラーの数を指定します。5 つより多くのミラーを指定するには、グローバル・オプション・ファイル内の `MaxNumberOfMirrors` 変数の値を大きくします。

デバイスの選択

バックアップおよび各ミラー用のデバイスを個別に指定します。パフォーマンスへの影響を避けるために、デバイスは同じブロック・サイズに設定し、すべてを同じシステムか SAN 環境に接続するようにお勧めします。

重要

SAP DB、DB2、または Microsoft SQL Server 統合ソフトウェア・オブジェクトのミラーに必要なデバイスの最小数は、バックアップに使用したデバイスの数と同じになります。

オブジェクトミラーを伴うバックアップ・セッションが開始されたら、ユーザーがバックアップ仕様で指定したものの中から、Data Protector がデバイスを選択します。

オブジェクトミラーはデフォルトで負荷調整されています。Data Protector は、できる限り多くのデバイスを使用することでデバイスの利用を最適化します。コマンド行からオブジェクトミラー操作を実行する場合、負荷調整はできません。

処理の結果

オブジェクトミラーを伴うバックアップ・セッションが正常に完了したら、バックアップ・オブジェクトを格納したメディア・セットが 1 つと、ミラーオブジェクトを格納した追加のメディア・セットが作成されます。これらのメディア・セット上にあるミラーオブジェクトは、オブジェクトコピーとして処理されます。

メディアのコピー

メディア・コピーとは

Data Protector のメディア・コピー機能では、バックアップの実行後にメディアをコピーできます。メディア・コピーは、バックアップを格納したメディアとまったく同じコピーを作成するプロセスです。この機能を使用すると、アーカイブまたはボールティングのためにメディアを複製できます。

メディアをコピーしたら、オリジナルのメディアかコピーのどちらかをオフサイトのボールトに移動させ、もう一方のメディア・セットを復元作業用に使用できます。Data Protector でのボールティングの構成方法については、「メディアのボールティング」(199 ページ) を参照してください。

Data Protector では、メディア・コピーを手動で開始することも自動で行うこともできます。詳細は、「自動メディア・コピー (Automated Media Copy)」(358 ページ) を参照してください。

メディアのコピー方法

[デバイス / メディア] コンテキストでメディアをブラウズして右クリックし、[コピー] をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「コピー - メディア」を参照してください。

ソース・メディア用と**ターゲット・メディア**用に、同じ種類のメディアがそれぞれ 1 つずつ必要です。ここで、ソース・メディアとはデータのコピー元のメディアを意味し、ターゲット・メディアとはデータのコピー先のメディアを意味します。

ターゲット・メディアに保存したデータの保護期間を指定して、その期間内の上書きを禁止できます。デフォルトの保護期間は、オリジナルのデータと同じです。その他のオプションとして、[無期限] および [期限](指定日まで保護) があります。メディアは、メディア上で一番長く保護が設定されているオブジェクトの保護期間が終了するまで保護されます。

1 回のコピー・セッションでは 1 つのメディアしかコピーされないため、各メディアのコピーは個別に開始する必要があります。フリー・プール内のメディアおよび NDMP メディアについては、コピー操作を実行できません。

処理の結果

メディア・コピーの結果、同じメディアが 2 セット (オリジナルとコピー) 作成されます。このうちどちらかを復元に使用できます。

ソース・メディアがコピーされたら、Data Protector はこのメディアを「追加不可能」としてマークし、新しいバックアップが追加されないようにします。(オリジナルとコピーが食い違わないようにするためです。) コピーの方も「追加不可能」としてマークされます。

1 つのオリジナル・メディアに対して複数のコピーを作成できます。ただし、コピーのコピーを作成することはできません (これは第 2 世代コピーと呼ばれます)。

注記

メディアのコピーを行う際、ソース・メディアよりも先にターゲット・メディアがテープの最後に到達することがあります。これは、ソース・メディアがストリーミング・モードで書き込まれており、ビジー状態のシステム上や負荷の高いネットワークを通じてコピーを作成した場合に起こる可能性があります (テープが停止 / 再スタートした場所に空白スペースが作成されます)。メディアのフォーマット時にテープへの埋め込みブロックを有効にすることで、これを防止できます。「メディアのフォーマット」(164 ページ) を参照してください。

コピーの移動

通常、コピーしたメディアは安全な場所に保管します。詳細は、「メディアのボールティング」(199 ページ) および「デバイスからのメディアの取出し」(196 ページ) を参照してください。

コピーのエクスポート

メディアをエクスポートすると、そのメディアに関する情報がすべて IDB から削除されます。オリジナルのメディアをエクスポートしても、1 つまたは複数のメディアのコピーが存在している場合、コピーのいずれかがオリジナルとなります。

いったんエクスポートしたコピーをインポートしようとして、オリジナルのメディアが IDB にない場合は、[強制] オプションを使用してこのメディアをインポートする必要があります。手順については、「メディアのインポート」(169 ページ) を参照してください。

コピーからの復元

Data Protector は、デフォルトではオリジナルのメディア・セットからデータを復元します。しかし、オリジナルのメディア・セットが使用できず、コピーが使用可能な場合は、そのコピーを復元に使用します。

復元時にオリジナルとコピーのどちらもデバイスにない場合、Data Protector はマウント要求を発行して、オリジナルとコピーの両方を復元に必要なメディアとして表示するので、どちらかを復元に使用します。

スタンドアロンのデバイスを使用して復元を実行する場合は、オリジナルではなくコピーからの復元を選択することもできます。コピーから復元するには、復元に使用するデバイスにコピーを挿入するか、コピーが挿入されているデバイスを復元用に選択します。ただし、ライブラリ・デバイスを使用して復元を実行する場合に、オリジナルがそのライブラリ内に存在する際は、Data Protector はオリジナルを復元に使用します。

メディアのアーカイブからデータを復元する方法については、「メディアのボールティング」（199 ページ）を参照してください。

自動メディア・コピー (Automated Media Copy)

自動メディア・コピー (Automated Media Copy) とは

自動メディア・コピーとは、バックアップが保存されているメディアのコピーを自動的に作成するプロセスです。

Data Protector には、2 種類の自動メディア・コピーが用意されています。**「ポスト・バックアップのメディア・コピー」**と**「スケジュールされたメディア・コピー」**です。

ポスト・バックアップのメディア・コピー

ポスト・バックアップのメディア・コピーは、バックアップ・セッション完了後に実行され、そのセッションで使用されたすべてのメディアをコピーします。

［デバイス / メディア］コンテキストで［自動操作］を右クリックして、［ポスト・バックアップのメディア操作を追加］をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「ポスト・バックアップのメディア・コピー」を参照してください。

スケジュールされたメディア・コピー

スケジュールされたメディア・コピーは、ユーザーの定義した時間に実行されます。複数のバックアップ仕様で使用されたメディアを、1 つのセッションでコピーできます。自動メディア・コピーの仕様を作成して、コピーするメディアを定義します。

［デバイス / メディア］コンテキストで［自動操作］を右クリックして、［スケジュール・メディア操作の追加］をクリックします。詳しい手順については、オンライン・ヘルプの索引キーワード「スケジュールされたメディア・コピー」を参照してください。

スケジュールされたメディア・コピーを構成して、特定の日時にコピーを実行したり、定期的にコピーを実行できます。スケジュールのリセットや、有効 / 無効を切り替えることも可能です。また、休日のメディアの自動コ

ピーを有効または無効にすることもできます。詳しい手順については、オンライン・ヘルプの索引キーワード「メディアの自動コピー」を参照してください。

制限事項

- メディアの自動コピーにスタンドアロン・デバイスは使用できません。ライブラリ・デバイスのみ使用可能です。
- ソース・メディアとターゲット・メディアは同じ種類でなければなりません。
- NDMP メディアのコピーはできません。

メディアの自動コピーはどのように行われるか

まず、自動メディア・コピーの仕様を作成します。自動メディア・コピー・セッションの開始時に、Data Protector は自動メディア・コピー仕様で指定されたパラメータに基づいて、**ソース・メディア**として参照されるメディアのリストを作成します。各ソース・メディアに対して、データのコピー先となる**ターゲット・メディア**が選択されます。ターゲット・メディアは、ソース・メディアと同じメディア・プール、フリー・プール、またはライブラリ内の空きメディアのいずれかから選択されます。

デバイスの選択と使用

各ソース・メディアに対して、Data Protector は自動メディア・コピー仕様で指定されたデバイスの中から 1 組 (2 台) のデバイスを選択します。自動メディア・コピー機能は、独自の負荷調整機能を備えています。Data Protector は、できる限り多くのデバイスを使用し、またローカル・デバイスが使用可能な場合はそれらを選択することで、デバイスの利用を最適化しようとします。

デバイスはセッションの開始時にロックされます。セッション開始後にデバイスをロックすることはできないため、セッションの開始時に使用不可能なデバイスは、そのセッションでは使用できません。セッション全体が正常終了するには、メディアの種類ごとに最低 2 台のデバイスが使用可能でなければなりません。セッションに必要な最低数のデバイスをロックできない場合、セッションは失敗します。

複数のパスが構成されたデバイスでは、ローカル・パスが優先されます。ローカル・パスが使用できない場合、使用可能なパスがあらかじめ決められた順序で使用されます。

メディアのエラーが発生した場合、エラーの発生したデバイスはその自動メディア・コピー・セッション内では使用されなくなります。ただし、使用可能なデバイスが他に存在しない場合は再使用されます。

コピーのあて先となるプール

ターゲット・メディアのあて先となるプールは、ソース・メディアにより決まります。つまり、コピーされたメディアは、オリジナルのメディアと同じプールに入れられます。

コピーのデータ保護

コピーの保護期間はデフォルトでは、オリジナルの保護期間と同じです。自動メディア・コピー仕様を作成または変更する際、デフォルト以外の保護期間を設定できます。

マウント要求と「cleanme」要求の処理

自動メディア・コピー機能は、マウント要求や「cleanme」要求を処理しません。マウント要求を受け取った場合、処理中のメディアに対する操作は中止されますが、セッションは続行されます。自動メディア・コピー・セッション完了後、コピーされなかったメディアを手動でコピーできます。

使用例については、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

8 復元

本章の概略

本章では、復元方法について説明します。特定のデータを復元したり、復元オプションを使用して必要に応じた復元を行うことができます。

「データの復元」(363 ページ)

「UNIX システムの復元」(371 ページ)

「Windows システムの復元」(372 ページ)

「Novell Netware ファイルシステムの復元」(384 ページ)

「OpenVMS ファイルシステムの復元」(388 ページ)

「復元オプション」(391 ページ)

「復元のテクニック」(397 ページ)

データベース・アプリケーション (Oracle、SAP R/3、MS Exchange、MS SQL、Informix、IBM DB2 UDB、Sybase など) の復元方法の詳細は、『HP OpenView Storage Data Protector インテグレーション・ガイド』を参照してください。

IDB の復元方法の詳細は、第 11 章「Data Protector 内部データベースの管理」(487 ページ) および「IDB を復旧する」(527 ページ) を参照してください。

データの復元

復元とは、ディスク上にあるバックアップ・コピーから元のデータを再作成するプロセスです。このプロセスは準備段階とデータを実際に復元する段階で構成されます。さらに必要に応じて復元後に適切な処理を施すことによりデータを利用可能な状態にします。

Data Protector の内部データベース (IDB) には、どのシステムからバックアップしたどのファイルがどのメディアに保存されているか、といった情報が記録されています。この IDB により、復元対象のデータにすばやく、効率的にアクセスできます。

Data Protector は、以下の特別な復元機能を備えています。

- 様々なレベル (セッション、クライアント、オブジェクト、ディレクトリ、特定のファイル、特定のファイル・バージョンなど) での復元機能
- バックアップ元と異なる場所を復元先に指定するためのオプション
- 複数のプラットフォームにまたがる復元
- セッション、クライアント、セル内にある複数のオブジェクトの並行復元
- 復元に使用するメディア・セットの自動または手動による選択

これらの機能の指定方法と利用可能なオプションはプラットフォームによって異なります。

標準復元手順

必要条件

復元を実行するには、適切なユーザー権限が必要です。ユーザー権限は、ユーザー・グループに応じて定義されています。

復元を行うために必要な作業

標準復元手順として、以下を実行する必要があります。

- 復元対象のデータの選択
- 必要なメディアの確認
- 復元セッションの開始

その他の設定

その他の設定はバックアップの実行段階ですでに定義されていますが、変更も可能です。事前に定義されている設定を変更するには、以下を指定します。

- 復元対象データのバックアップ・バージョン
- データの復元先
- 復元元のデバイス
- 既存のファイルと重複するファイルの処理
- 復元オプション ([復元時にファイルをロック] など)
- 同じオブジェクト・バージョンを格納したメディアが複数ある場合の、位置による選択優先順位
- 同じオブジェクト・バージョンを格納したメディア・セットが複数ある場合の、手動でのメディア・セットの選択

標準復元作業の詳しい手順については、オンライン・ヘルプの索引キーワード「標準復元手順」を参照してください。

復元対象データの選択

Data Protector の [復元] コンテキストでは、以下の 2 つの方法で復元対象のオブジェクトをブラウズできます。

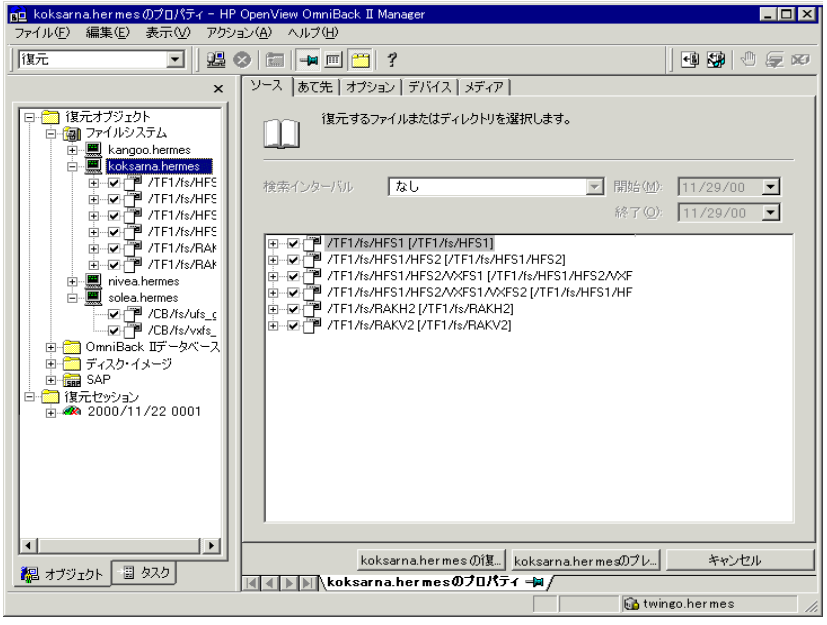
- [復元オブジェクト] では、バックアップ・オブジェクトの一覧を表示します。オブジェクトは、セル内のクライアント・システムごとやデータの種類 (ファイルシステム、ディスク・イメージ、内部データベースなど) ごとに分類されます。
- [復元セッション] では、ファイルシステム・セッションの一覧を表示します。各セッション内でバックアップされたすべてのオブジェクトも併せて表示します。表示対象のセッションを前年、前月、先週からのみに指定することもできます。デフォルトでは、すべてのファイルシステム・セッションが表示されます。特定のバックアップ・セッションからオンライン・データベース用統合ソフトウェアを復元することはできません。

復元対象には 1 つのオブジェクトを選択することも、複数のオブジェクトを選択することもできます。復元オブジェクトが 1 つの場合は単一復元を、複数の場合は並行復元を実行します。並行復元の詳細は、「複数ファイルの並行復元」(399 ページ) を参照してください。

[検索インターバル] を指定して、特定の時間間隔にバックアップされたオブジェクトのみをブラウズすることもできます。

Data Protector には [照会ごとに復元] 機能があります。この機能では、まずファイルやディレクトリを検索し、復元対象を特定した上で復元を実行します。詳細は、「照会ごとに復元する」(401 ページ) を参照してください。

図 8-1 復元対象データの選択



バックアップ・バージョンの選択

復元対象データを選択する際には、デフォルトでは最新のバックアップのバージョンが選択されています。つまり、最後に実行されたバックアップ・セッションで保存されたディレクトリやファイルのみが復元用に選択されます。同じツリー構造にあるディレクトリやファイルで、同じバックアップ・セッションでバックアップされなかったものはグレー表示されます。

別のバックアップ・セッションのデータを復元したい場合は、復元したいディレクトリやファイルをブラウズして選択し、右クリックで [バージョンの復元] を選択します。

[バージョン] タブで [...] をクリックすると、バックアップ・バージョンの詳細情報が表示されます。[...] ボタンは、属性を記録するログ・レベルでバックアップを実行した場合のみ使用できます。

ファイルの重複の処理

復元の [説明] プロパティ・ページでは、現在ディスク上にあるファイルとバックアップ・ファイルのバージョン間でファイルが重複する場合にどのような処理を行うかを指定できます。[ファイル重複時の処理] には、[最新ファイルを保存]、[上書きしない]、[上書きする] の 3 つのオプションがあります。上記オプションの詳細は、「復元オプション」(391 ページ) を参照してください。

復元先の指定

Data Protector のデフォルト設定では、データのバックアップ元のクライアントとディレクトリがデータの復元先になります。これらのデフォルト設定を変更するには、[あて先] プロパティ・ページでデータの復元先を指定します。

- 適切なユーザー権限がある場合、別のクライアントを復元先に指定できます。
- 別のディレクトリを復元先に指定できます。

これらの設定はオブジェクトごとに指定できます。

また、Data Protector では [別名で復元 / 復元先 ...] オプションで、1 つのバックアップ・オブジェクトのファイルやディレクトリに対して個別の復元先を指定できます。これらの設定は、オブジェクトまたはファイルごとに指定できます。

復元先の指定方法については、「別のパスにファイルを復元する」(397 ページ) を参照してください。

復元オプションの設定

復元の [オプション] プロパティ・ページで復元オプションを設定します。使用可能なオプションは、復元するデータの種類によって異なります。たとえば、ファイルシステムの復元とディスク・イメージの復元とでは、利用できるオプションの組み合わせが異なります。復元オプションの詳細は、「復元オプション」(391 ページ) を参照してください。

別のデバイスを使った復元

デフォルトでは、バックアップで使用したデバイスが復元に使用されます。ただし、同じ Data Protector セル内に構成されたデバイスであればどのデバイスからでもデータを復元できます。新しいデバイスを指定するには、復元の [デバイス] プロパティ・ページの [変更] ボタンをクリックします。新しいデバイスはこのセッションのみで使用されます。

注記

一部のデータベース統合ソフトウェアの場合、[デフォルトとして保存] ボタンをクリックすることによって、変更したデバイスを (統合ソフトウェアの種類に関わらず) **すべて**の Data Protector 統合ソフトウェアの復元セッションのデフォルトの復元デバイスとして設定できます。

必要なメディアの検出

データが保存されているメディアのリストを入手するには、復元対象データを選択して [メディア] プロパティ・ページに移動します。

復元に必要なメディアは、[復元セッションの開始] ダイアログ・ボックスで、[必要なメディア] ボタンをクリックして表示することもできます。このダイアログ・ボックスは、復元の開始時に表示されます。

同じオブジェクト・バージョンが複数のメディア・セット上にある場合は、メディア位置の優先順位を設定することにより、復元に使用するメディア・セットの選択をある程度制御できます。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。詳細は、「復元元のメディア・セットを選択する」(404 ページ) を参照してください。

復元のプレビューと開始

復元を開始する前に、メディアが適切にロードされていることを確認してください。適切にロードされていないと、メディアが検出されません。

復元の [ソース] プロパティ・ページで選択したオブジェクトを復元する場合、[開始] をクリックして復元プロセスを開始するか、[プレビュー] をクリックしてプレビュー画面を表示します。

Scoping ペインで選択したオブジェクトを復元する場合は、[アクション] メニューから [復元のプレビュー] をクリックして復元プロセスをプレビューするか、[復元開始] をクリックして実際に復元を開始します。

復元の中止

復元セッションを中止すると、復元が停止します。セッションを中止する前に処理が完了していたデータは、指定の場所に復元されます。

復元セッションを中止するには、[アクション] メニューの [中止] を選択します。

復元セッションは、Data Protector の [モニター] コンテキストでも中止できます。

ディスク・イメージの復元

ディスク・イメージの復元では、ディスク・イメージのバックアップがセクタごとに復元されます。Data Protector は、特定の時刻に (ディスク・イメージとして) バックアップされたディスク全体のイメージを復元しますこの方法を使用すると、非常に高速に復元が実行されます。この方法は、Wondows と UNIX のシステムで使用できます。

必要条件

ディスク・イメージの復元を実行するには、以下の必要条件を満たす必要があります。

- ディスクが、ディスク・イメージ・バックアップを使用してバックアップされている。
- ディスク・イメージをバックアップ元とは異なるディスクに復元する場合、復元先のディスク・サイズがバックアップ元と同じ、または大きい。
- UNIX システムの場合、ディスク・イメージの復元を行う前にディスクをアンマウントし、後でマウントし直す。

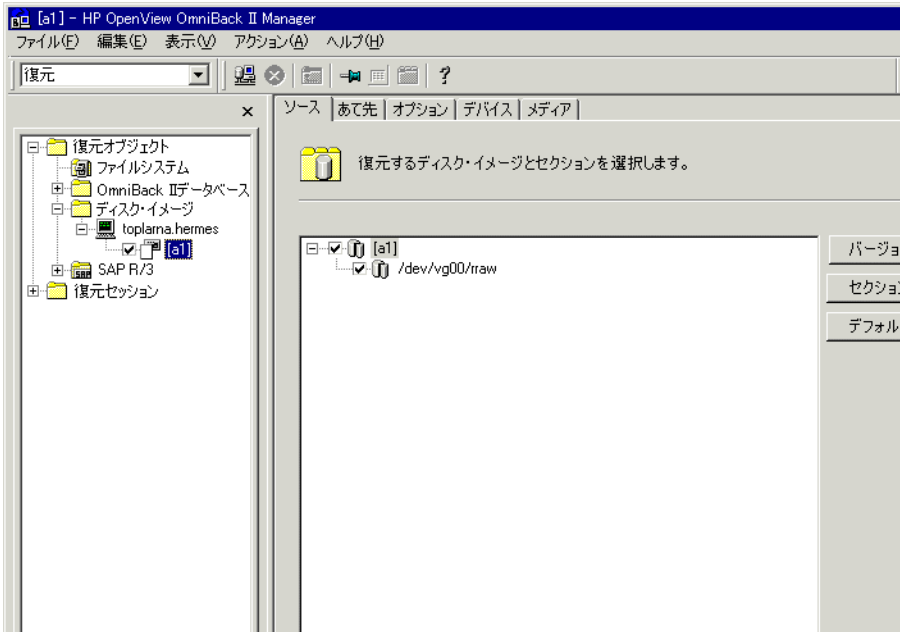
制限事項

Windows システムの場合、使用中のファイルまたはセクションがあるとディスク・イメージの復元は失敗します。

手順

ディスク・イメージ・バックアップを復元する場合、図 8-2 (369 ページ) のように [復元] コンテキストでディスク・イメージ・オブジェクトを展開し、標準復元手順を実行します。詳細は、「標準復元手順」(363 ページ) を参照してください。

図 8-2 ディスク・イメージ・オブジェクト



共有ディスクへのデータの復元

Data Protector を使用すると、データのバックアップ元でない Windows 共有ディスクにも UNIX および Windows のデータを復元できます。Data Protector のユーザー・アカウントと Inet サービスには、リモート・コンピュータへアクセスするための権限と Disk Agent クライアント上での権限が必要です。適切なログオン・アカウントの使用方法については、「Data Protector Inet サービスに対するユーザー・アカウントの設定」(248 ページ)を参照してください。

以下のような場合に、UNIX または Windows のファイルシステムを Windows の共有ディスクに復元します

- システムが Data Protector のセルの一部ではなく、Data Protector DiskAgent がインストールされていない場合。
- Data Protector で直接サポートされていないプラットフォーム (Windows for Workgroups や Windows 3.1 システムなど) に復元する場合。
- データを複数のシステムから利用できるようにする場合。

注記

バックアップ元とは異なるファイルシステム (UNIX から Windows へ) にデータを復元する場合、ファイルシステム固有の属性が失われることがあります。

共有ディスクへの復元方法

復元の [あて先] プロパティ・ページでは、データの新しい復元先としてターゲット・クライアントと Windows 共有ディスクを指定できます。詳しい手順については、オンライン・ヘルプの索引キーワード「共有ディスク、復元」を参照してください。

UNIX システムの復元

どのデータが復元されるか

バックアップ元にファイルを復元する場合、Data Protector はファイル属性も含めてファイルを復元します。

UNIX の ACL(アクセス制御リスト) などのシステム固有データは、ファイルシステムとオペレーティング・システムがバックアップ元と同じ種類の場合にのみ復元されます。

通常の UNIX ファイルの復元

UNIX のファイルおよびディレクトリを復元するには、標準復元手順を使用します。詳細は、「標準復元手順」(363 ページ) を参照してください。

VxFS の復元

一時ディレクトリにバックアップされた VxFS データを復元する場合は、[別名で復元] オプションを使って希望の場所にデータを復元します。[別名で復元] オプションの使用方法については、「別のパスにファイルを復元する」(397 ページ) を参照してください。

OmniStorage バックアップの復元

OmniStorage 制御ファイルシステム (MFS) へのバックアップ・データの復元とは別に、Data Protector A.05.50 には、HP-UX 11.x 上で通常のファイルシステムの復元を行うことで OmniBack II または Data Protector でバックアップした OmniStorage ファイルシステムのデータを復元する機能があります。この場合、OmniStorage の移行属性 (移行ポリシーなど) は失われます。

OmniStorage ファイルは HP-UX のどのファイルシステムにも復元できますが、VxFS 固有のファイル属性を保持するためには、復元先のシステムを VxFS3 またはそれ以降のレイアウトを持つ JFS とすることをお勧めします。

ディスク・イメージの復元

詳細は、「ディスク・イメージの復元」(368 ページ) を参照してください。

共有ディスクへの復元

詳細は、「共有ディスクへのデータの復元」(370 ページ) を参照してください。

Windows システムの復元

どのデータが復元されるか

Windows のファイルシステムを復元する場合、Data Protector はファイルおよびディレクトリ内のデータと、ファイルおよびディレクトリに関する Windows 固有の情報を復元します。

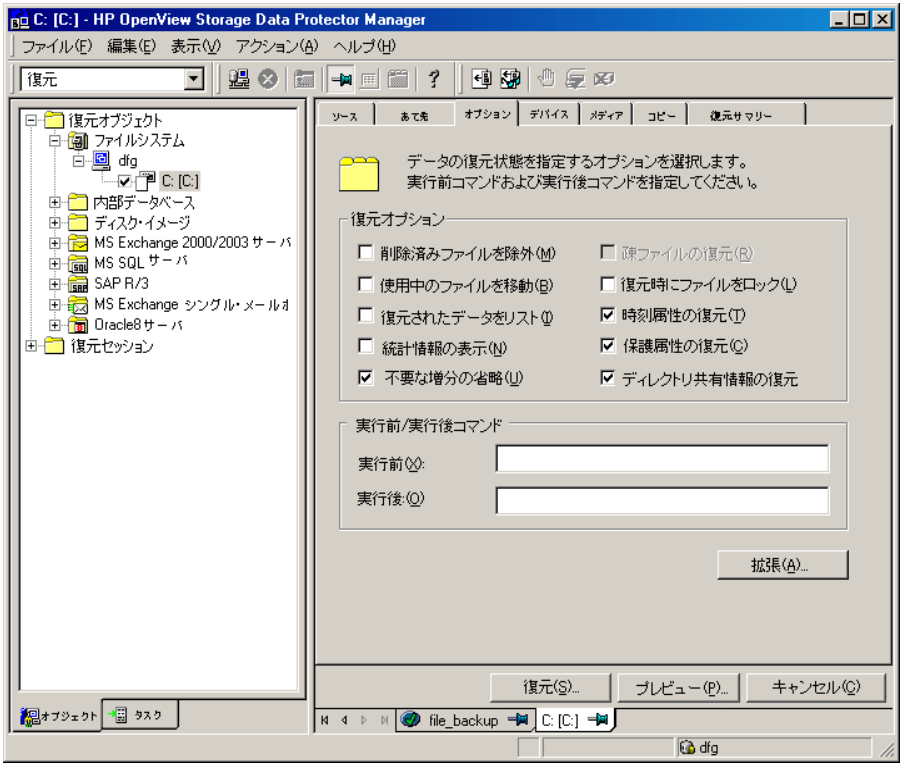
バックアップを実行したファイルシステムと異なるファイルシステムに復元を行う場合は、ファイルシステムの復元に関する制限事項を考慮してください。「ファイルシステムの制限事項」(374 ページ) を参照してください。

以下の Windows 固有の情報が復元されます。

- Unicode のフル・ファイル名
- FAT16、FAT32、VFAT、NTFS 属性
- ディレクトリの共有情報

  バックアップ時にネットワーク上でディレクトリが共有されている場合、バックアップ・メディアに共有情報が保存されます。デフォルトでは復元後にネットワーク上でディレクトリが共有されます (同じ共有名を持つ共有ディレクトリがすでに存在する場合を除きます)。復元中のディレクトリの共有情報を復元しないようにするには、[ディレクトリ共有情報の復元] オプションをオフにします。

図 8-3 **ディレクトリの共有情報の復元**



Windows ディレクトリの共有情報は、Data Protector A.05.50 の Disk Agent またはそれ以降を使用しないと Windows に復元できません。この要件を満たしていない場合でもディレクトリは復元されますが、Disk Agent がディレクトリの共有情報を無視します。

注記

ディレクトリの共有情報の復元には、ファイル重複の処理に関するオプションも適用されます。たとえば、[上書きしない] オプションが復元に対して使用された場合、ディスク上に存在するディレクトリの共有情報は保持されます。ファイル重複の処理のオプションが復元に及ぼす影響については、「復元オプション」(391 ページ) を参照してください。

- NTFS の代替データ・ストリーム

たとえば、Windows 2000 上のオブジェクト ID は、代替データ・ストリーム・セットとしてバックアップされます。

- NTFS セキュリティ・データ

NTFS 3.x を使用している Windows システムには、さらに以下が適用されます。

- NTFS 3.x ファイルシステムは、再解析ポイントをサポートしています。

  ボリューム・マウント・ポイント、Single Instance Storage (SIS)、ディレクトリ接続は、再解析ポイントの概念に基づいています。これらの再解析ポイントは、他のファイルシステム・オブジェクトと同様に選択できます。

- NTFS ファイルシステムでは、ディスク・スペースを節約する効果的な手段として疎ファイルをサポートしています。

  これらのファイルは、ディスク・スペース節約のため疎ファイルとしてバックアップされます。疎ファイルは、NTFS 3.x ファイルシステムに対してのみ疎ファイルとしてバックアップおよび復元されます。

- NTFS ファイルシステムに固有の機能には、独自のデータ・レコードを維持するシステム・サービスによって制御されるものがあります。これらのデータ構造は、CONFIGURATION の一部としてバックアップされます。

- 暗号化ファイル

ファイルシステムの制限事項

バックアップを行ったファイルシステムとは別のファイルシステムを復元先として選択できます。ただし、この機能を使用するには、制限事項を考慮する必要があります。表 8-1 (374 ページ) を参照してください。

表 8-1 Windows ファイルシステムの復元に関する制限事項

	復元先					
復元元	FAT32	FAT16	CDFS	UDF	NTFS 3.0b	NTFS 3.1c
FAT32	FC	FC	適用なし	適用なし	FC	FC
FAT16	FC	FC	適用なし	適用なし	FC	FC

表 8-1　Windows ファイルシステムの復元に関する制限事項

CDFS	FC	FC	適用なし	適用なし	FC	FC
UDF	FC	FC	適用なし	適用なし	FC	FC
NTFS 3.0b	*	*	適用なし	適用なし	FC	FC
NTFS 3.1c	*	*	適用なし	適用なし	FC	FC

表の見方

b　NTFS 5.0 とも呼ばれます。Windows 2000 で使用されています。

c　NTFS 5.1 とも呼ばれます。Windows XP/Server 2003 で使用されています。

FC　完全な互換性有り (ファイル属性が完全に保持されます)。

*****　再解析ポイント、疎ファイル、および暗号化されたファイルは復元されません。ファイルの復元時にセキュリティ情報と代替データ・ストリームが失われます。

表 8-1 に示したように、NTFS 3.x ファイルシステム・オブジェクトは NTFS 3.x ファイルシステムに対してのみ完全に復元できます。異なるファイルシステムや古いバージョンのファイルシステムに復元すると、ファイルシステム固有の属性と代替データ・ストリームが失われます。

- Windows の再解析ポイント (ディレクトリ接続やボリュームのマウント・ポイントなど) は、NTFS 3.x ファイルシステムのみに復元されます。UNIX の再解析ポイントは NTFS 3.x ファイルシステムには復元できません。

注記

SIS 再解析ポイントを含む NTFS 3.x ファイルシステムを復元する場合、ディスク・スペースがいっぱいになる可能性があります。この状況は、元のファイルが複数のファイルに復元され、使用可能なスペース以上のスペースを占める場合に発生します。

- 疎ファイルは、NTFS 3.x ファイルシステムのみに疎ファイルとして復元されます。
- Data Protector を使ってユーザー・ディスク・クォータの復元はできません。
- NTFS 3.x 以外のファイルシステムへ疎ファイルを復元しようとした場合、Data Protector は警告を出力します。NTFS 3.x ファイルシステム以外のファイルシステムに復元された疎ファイルには、ゼロ・セクションは含まれません。
- Microsoft暗号化NTFS 3.xファイルはNTFS 3.xファイルシステムにしか復元できません。これは、他のファイルシステムのドライバでは復号化できないためです。

通常の Windows ファイルとディレクトリの復元

Windows のファイルおよびディレクトリを復元するには、標準復元手順を使用します。詳細は、「標準復元手順」（363 ページ) を参照してください。

共有ディスクの復元

共有ディスクとしてバックアップされたオブジェクトは、そのオブジェクトをバックアップした Disk Agent クライアントと関連付けられます。環境に変更がない場合は、ローカルの Windows ファイルシステムを復元するのと同様に共有ディスクを復元できます。デフォルトでは、共有ディスクのバックアップに使用した Disk Agent クライアントを使って、元のディレクトリへのデータの復元が実行されます。

共有ディスクを復元する Disk Agent クライアントの選択方法と構成方法については、「Windows 共有ディスクのバックアップ」（246 ページ) を参照してください。

UNIX または Windows ファイルシステムの共有ディスクへの復元方法については、「共有ディスクへのデータの復元」（370 ページ) を参照してください。

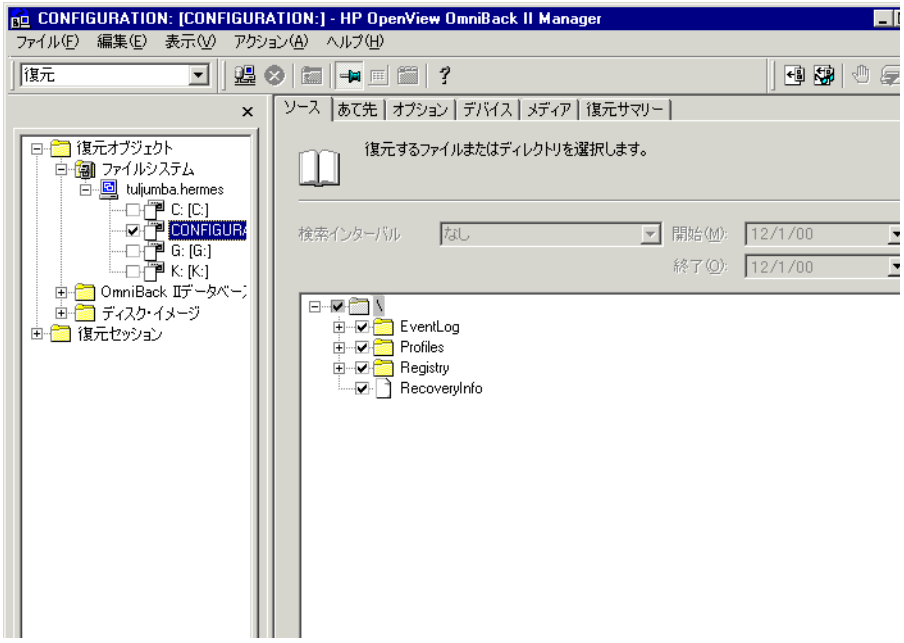
ディスク・イメージの復元

詳細は、「ディスク・イメージの復元」（368 ページ) を参照してください。

Windows の CONFIGURATION の復元

Windows の CONFIGURATION を復元するには、CONFIGURATION オブジェクトを選択して標準復元手順を実行します。図 8-4 を参照してください。

図 8-4　Windows の CONFIGURATION の復元



必要条件

CONFIGURATION はシステムの動作に影響を与えるデータ構造で構成されています。そのため、このような復元に対応したシステムを準備する必要があります。必要条件は、CONFIGURATION の内容や Windows の OS バージョンによって変わります。詳細は、「CONFIGURATION のバックアップ」（233 ページ）を参照してください。要約を以下に示します。

- 現在使用中のユーザー・プロファイルを復元することはできません。この場合、ログイン・アカウントを変えるか、関連するサービスを停止する必要があります。

  詳細は、「Windows のユーザー・プロファイルおよびイベント・ログの復元」（382 ページ）を参照してください。

- Active Directory を復元するには、システムを Active Directory 復元モードで起動する必要があります。

  詳細は、「Windows サービスの復元」（380 ページ）を参照してください。

CONFIGURATION 全体を復元した場合は、システムを再起動して、復元されたデータを［レジストリ］に読み込んでください。詳細は、「Windows レジストリの復元」（379 ページ) を参照してください。

SysVol の復元

SysVol ディレクトリの復元は、以下の 3 種類のモードのいずれかを使って実行できます。

- ［権限なし ］モード

  ドメイン内で少なくとも 1 つの使用可能なドメイン・コントローラが動作している場合、ファイルは元の位置に復元されます。復元されたデータは他のドメイン・コントローラへは配布されません。

- ［権限付き ］モード

  クリティカルな SysVol データをローカル・ドメイン・コントローラから削除し、他のドメイン・コントローラでも同様の削除を実行する場合は、権限付きモードで復元します。

- ［プライマリ ］モード

  ドメイン内のすべてのドメイン・コントローラが失われ、バックアップからドメイン・コントローラを再構築したい場合は、ユーザーがプライマリ・ファイルを復元することが FRS へ通知され、ファイルは元の位置へ復元されます。

Windows のシステム状態の復元

必要条件

Active Directory を使用する場合、Active Directory は常にシステム状態の一部であるため、Active Directory 復元モードでシステムを起動する必要があります。

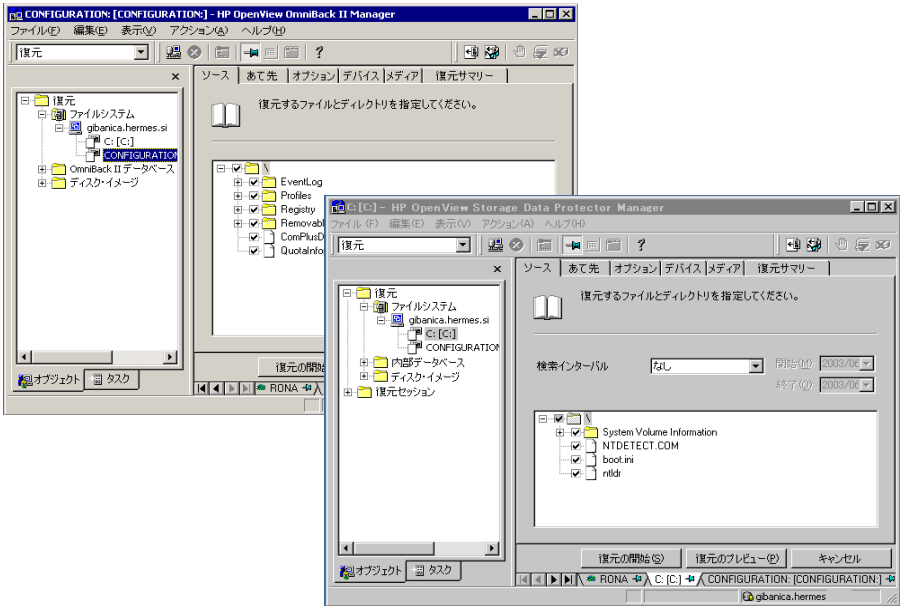
Active Directory モードの詳細は、「Windows サービスの復元」（380 ページ) を参照してください。

システム状態を復元するには、復元ウィザードで以下のオブジェクトを選択します。

1. CONFIGURATIONに所属しているシステム状態オブジェクト。これらのオブジェクトの一覧は、「Windows のシステム状態のバックアップ」（235 ページ) を参照してください。

2. SystemVolumeInformation のフォルダとブート・ファイル。この 2 つは、システム・ドライブにあります。

図 8-5 **システム状態の項目の選択**



注記

Data Protector から見たシステム状態データは、通常のファイルシステム・オブジェクトと CONFIGURATION オブジェクトで構成されています。[バックアップ] ウィザードでオブジェクトを選択する場合とは異なり、復元対象の各オブジェクトは [復元] ウィザードで個別に選択します。

復元セッションが完了したら、システムを再起動します。

Windows レジストリの復元

Windows レジストリを復元するには、[CONFIGURATION] を展開し、[Registry] のみを選択します。

復元セッションが完了したら、システムを再起動します。

注記

Windows レジストリ全体を復元対象として選択した場合、レジストリ・キーの中には復元されないものや、復元中に特殊な方法で処理されるものがあります。これは、これらのキーが OS で使用されているために起こります。これらのキーは以下のディレクトリの [レジストリ] キーに存在します。

¥HKEY_LOCAL_MACHINE¥SYSTEM¥CurentControlSet¥Control¥BackupRestore¥KeysNotToRestore

Windows サービスの復元

Windows サービスを復元するには、[CONFIGURATION] を展開して復元対象のサービスを選択します。

必要条件

Windows サービスに含まれる以下の情報を [CONFIGURATION] で選択できます。

- COMPlusDatabase
- FileReplicationService
- RemovableStorageManagementDatabase
- ActiveDirectoryService
- TerminalServiceDatabase
- CertificateServer
- DHCP、WINS、および DNSServerDatabase

これらの用語の詳細な説明は、「用語集」を参照してください。

各 Windows サービスの復元に関する固有の情報を以下に示します

Active Directory の復元

Active Directory サービスを復元する場合、[ディレクトリ サービス復元モード] 起動オプションを使ってシステムを再起動してください。

[ディレクトリ サービス復元モード] でシステムが起動すると、ドメイン・ユーザー・アカウントは使用できなくなります。Data Protector Inet と crs サービス (Cell Manager 用) を構成して、ローカル・ユーザー・アカウント

を使ってログオンし、サービスを再起動します。詳細は、「Data Protector Inet サービスに対するユーザー・アカウントの設定」(248 ページ) を参照してください。

Active Directory を選択し、[Windows 固有のオプション] で [プライマリ]、[権限なし]、[権限付き] のいずれかを選択することで複製モードを設定します。これらのオプションの詳細は、「Active Directory 固有のオプション」(395 ページ) を参照してください。

注記

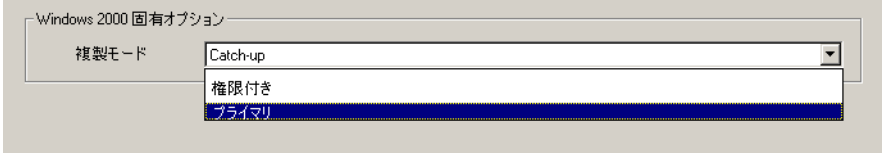
[権限付き] モードで復元を実行するには、復元セッション完了後に ntdsutil.exe も実行する必要があります。たとえば、代表的な [権限付き] モードの復元では、コマンド・プロンプトで ntdsutil、authoritative restore、restore database の順に入力します。その後、サーバを起動して、複製が実行されるのを待ちます。

ヒント

Active Directory を [権限付き] モードで復元するのに必要な追加作業を実行するために、実行後コマンドを作成することもできます。たとえば、ディレクトリ全体を [権限付き] モードで復元するには、以下のコマンドを使用します。

```
ntdsutil "popups off" "authoritative restore" "restore
database" quit quit
```

図 8-6 Active Directory の復元モード



Certificate サービスの復元

Certificate Server サービスはオフラインで復元します。復元を開始する前にサービスを終了する必要があります。使用可能な複製モードは［権限付き］だけです。

復元セッションが完了したら、システムを再起動します。

Remote Storage Service の復元

RSS データベースはシステム状態データの一部ですが、手動で復元します。RSS データベースはオフラインで復元することが必要です。Remote Storage Service の終了と再起動は、実行前 / 実行後スクリプトを使って実行することも、復元の前後に手動で行うこともできます。

復元対象として以下のディレクトリを選択します。

- `<%SystemRoot%>¥System32¥RemoteStorage`
- `<%SystemRoot%>¥System32¥NtmsData`

DFS の復元

Data Protector では、Windows の DFS(分散ファイルシステム) の構成を以下のいずれかの項目の一部として復元します。

- Windows のレジストリ - DFS がスタンドアロン・モードで構成されている場合。
- Windows Active Directory - DFS がドメイン・モードで構成されている場合。

Windows のユーザー・プロファイルおよびイベント・ログの復元

Windows のユーザー・プロファイルやイベント・ログを復元するには、`[CONFIGURATION]` オブジェクトを展開して復元対象を選択します。

ユーザー・プロファイル

Data Protector はアクセス中のファイルは復元しません。このため、まずシステムからログオフし、復元するプロファイルのあるユーザー・アカウントで実行されているサービスをすべて停止する必要があります。

復元セッションは、別のシステムから開始したり、また別のユーザーとして復元対象のシステムにログオンして開始できます。

削除されたユーザー・プロファイル

ユーザー・プロファイルを復元できるのは、ユーザー・プロファイルの位置がシステムで定義されている場合だけです。既存のユーザー・プロファイルや削除されたプロファイルの個々のファイルでも、システムのプロファイル内に存在していれば復元可能です。システムのプロファイル内にファイルがない場合は、復元を開始する前にファイルを再作成する必要があります。それ以降は、以下の手順を行います。

1. 復元するプロファイルのユーザーとしてログオンし、デフォルトのユーザー・プロファイルを作成します。
2. 復元したファイルがマージされないように、復元セッションを実行する前に、新規作成したプロファイル内のファイルを削除できます。
3. ログオフして、別のユーザーとしてログオンするか別のシステムを使って復元セッションを開始します。

システムは、ユーザーに別の名前を割り当てる可能性があります。この場合は、[別名で復元] オプションを使って、新しく割り当てられた位置にファイルを復元してください。

復元が完了したら、システムを再起動します。

ユーザー・ディスク・クォータ

Data Protector を使ってユーザー・ディスク・クォータの復元はできません。バックアップされた情報は、Microsoft 社のユーティリティを使って復元できます。

Windows TCP/IP サービスの復元

WINS、DHCP、DNS サーバ

Microsoft TCP/IP プロトコルを実行し、**WINS サーバ**、**DHCP サーバ**または**DNS サーバ**として構成されている Windows サーバでは、ネットワーク通信の管理サービスを復元できます。

Windows TCP/IP サービスを復元するには、[CONFIGURATION] を展開して [WNS]、[DHCP] または [DNSServerDatabase] を選択します。

復元開始前に、これらのサービスはそれぞれ自動的に終了します。

復元が完了したら、システムを再起動します。

Novell Netware ファイルシステムの復元

Novell NetWare ファイルシステムを復元するには、標準復元手順を使用します。詳細は、「標準復元手順」(363 ページ) を参照してください。

ネーム・スペース情報とボリューム・スペース制限の復元

ボリューム・スペース制限のみを復元する場合は、[あて先] ページで [ボリューム・スペース制限のみ復元] オプションを指定します。復元対象のオブジェクトとして必ずボリュームを選択します。

Data Protector では、通常のファイルシステム復元セッションの際に Novell Netware ボリュームのネーム・スペース情報が完全に復元されます。DOS、Mac、NFS、OS/2 のネーム・スペース情報は、ファイル / ディレクトリごとに復元されます。

ファイルまたはディレクトリを復元する際には、以下の点に注意してください。

- バックアップされたネーム・スペース情報が正常に復元されるのは、データを復元するボリュームに同じネーム・スペースがインストールされている場合だけです。
- DOS のネーム・スペースは、インストール済みの Novell Netware の各ボリュームに存在しているので、常に復元されます。
- Mac の resource fork は、Mac のネーム・スペースがインストールされているボリュームだけに復元されます。
- NDS/eDirectory オブジェクトの存在に依存する固有のネーム・スペース情報 (NFS ネーム・スペース内のユーザーやグループ ID など)。
- Queue オブジェクトの復元後は、ディレクトリ `SYS:SYSTEM` 内に待ち行列ディレクトリを適切な名前 (*<queue_ID>*`.qdr`) を付けて手動で作成する必要があります。適切なユーティリティ (`NWADMIN.EXE` または `SYSCON.EXE`) を使って、NDS/eDirectory から *<queue_ID>*.qdr を読み込みます。
- Novell NetWare 5.1 上の NSS ボリュームでは、4GB までのファイルをサポートします。他の Novell NetWare システムのファイル・サイズに制限はありません。

- Novell NetWareファイルは非NetWareプラットフォームには復元できません。

ファイルの所有権とトラスティの復元

Data Protector は、所有権およびトラスティ情報をファイル / ディレクトリごとに復元します。ファイルやディレクトリの所有権とトラスティは、適切なオブジェクトが NDS/eDirectory データベースに存在していれば正しく復元されます。

復元時には、[Trustee のみ復元] を選択し、[復元] コンテキストの [あて先] ページで適切な [Trustee の衝突処理] オプションを選択します。

NetWare の CONFIGURATION の復元

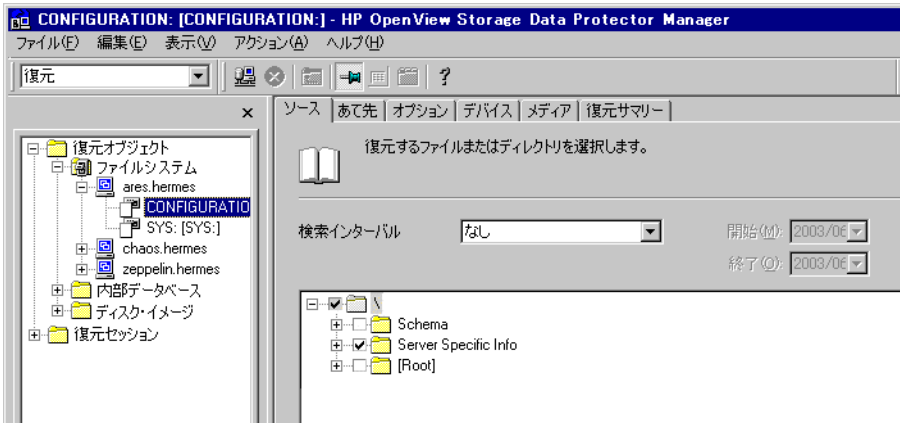
Data Protector では、CONFIGURATION と呼ばれる特殊なデータ構造を復元できます。CONFIGURATION は以下で構成されています。

CONFIGURATION のコンポーネント

- サーバ固有の情報
- スキーマ
- Root

CONFIGURATION のコンポーネントを復元するには、[CONFIGURATION] オブジェクトを選択して標準復元手順を実行します。詳細は、図 8-7 を参照してください。

図 8-7 NetWare の構成の復元



Novell NDS/eDirectory の復元

必要条件

NDS/eDirectory データベースを正しく復元するための必要条件は、バックアップの場合の必要条件と同じです。Data Protector では Novell NetWare ファイルシステムのデータと同じ方法で、NDS/eDirectory オブジェクトを復元できます。ただし、以下の場合は例外です。

- 他のNovell NetWareボリュームに復元できないNDS/eDirectoryオブジェクトの場合。
- コンテナ・オブジェクトおよびリーフ・オブジェクトは、Data Protector ではディレクトリとして扱われます。これらを他のコンテナ・オブジェクト内に復元したり、他のコンテナ・オブジェクトとして復元することはできません。

NDS/eDirectory を復元しても、現在の NDS/eDirectory ツリーのパーティションや複製の状態に影響はありません。NDS/eDirectory 情報を復元する際に、パーティションや複製がある場合は、それらをすべて利用して復元が行われます。復元時にパーティション情報がなければ、ツリー構造全体が 1 つのパーティションに復元されます。

注記

Data Protector では NDS/eDirectory のパーティションや複製に関する情報を復元できません。パーティションや複製は手動で再構築する必要があります。

Novell NDS/eDirectory の復元では、現在ディスク上にあるファイルのバージョンとバックアップ・ファイルのバージョンが重複する場合にどのような処理を行うかを指定できます。[ファイル重複時の処理] には、[最新ファイルを保存]、[上書きしない]、[上書きする] の 3 つのオプションがあります。上記オプションの詳細は、「復元オプション」(391 ページ) を参照してください。

NDS/eDirectory スキーマと NDS/eDirectory オブジェクトの復元

Data Protector では、単一の NDS/eDirectory オブジェクトの復元が可能です。Data Protector 復元セッションでは、以下を行うことができます。

- ［-trees］オプション : NDS/eDirectory のツリーを復元
- [-exclude] オプション : NDS/eDirectory のサブツリーを除外
- [-skip] オプション : 復元時に NDS/eDirectory オブジェクトをスキップ
- [-overwrite] オプション : 既存の NDS/eDirectory オブジェクトに上書き

トラブルシューティング

NDS/eDirectory の復元セッションが正常終了しても、一部のオブジェクトが正しく復元されず「不明」となる場合があります。この現象は、バックアップ・セッション後に NDS/eDirectory から NDS/eDirectory コンテナ・オブジェクトが削除された場合に発生します。この問題を解決するには、-overwrite オプションを使用して、このオブジェクトを再度復元してください。

OpenVMS ファイルシステムの復元

OpenVMS ファイルシステムを復元するには、標準復元手順を使用します。詳細は、「標準復元手順」（363 ページ) を参照してください。

どのデータが復元されるか

ディレクトリ構造とファイル、および以下のファイルシステム情報が復元されます。

- ディレクトリとファイルの属性
- 使用可能であれば、ACL(アクセス制御リスト)(以下の制限事項を参照)
- 二次ファイル・エントリ

  複数のディレクトリ・エントリを持つファイルは、一次パス名を使用して一度だけバックアップされます。二次パス・エントリは、ソフト・リンクとして保存されます。復元の際、これらの予備のパス・エントリも復元されます。詳細は、「バックアップ仕様の構成手順」（267 ページ) の「制限事項」を参照してください。

ファイルは、マウントされた FILES-11 ODS-2 または ODS-5 ボリュームにのみ復元できます。

制限事項

- 他のオペレーティング・システム・プラットフォーム上に保存されたファイルとディレクトリについては、すべてのファイル属性が復元されるわけではなく、また ACL は復元されません。

  復元中に作成されたディレクトリで、保存されていなかったディレクトリの属性は、－ no_protection オプションで無効にされない限り、そのディレクトリに最初に復元されたファイルの属性と同じになります。

- GUI に入力して CLI に渡すファイル仕様は、UNIX 形式の構文でなければなりません

  ```
  /disk/directory1/directory2/filename.ext.n
  ```

  — 文字列の先頭にスラッシュ (/) を付け、その後にディスク、ディレクトリ、ファイル名をスラッシュで区切って続けます。

  — ディスク名の後にコロン (:) を付けてはいけません。

— バージョン番号の前には、セミコロン (;) の代わりにピリオド (.) を使用します。

— OpenVMS ファイル用のファイル仕様では、大文字と小文字が区別されます。

例 :

OpenVMS のファイル仕様が以下の場合

```
$1$DGA100:[USERS.DOE]LOGIN.COM;1
```

以下の形式で指定する必要があります。

```
/$1$DGA100/Users/Doe/Login.Com.1
```

- 暗黙のバージョン番号はありません。バージョン番号は、常に明示的に指定する必要があります。復元対象として選択されたファイル・バージョンのみがバックアップされます。ファイルのすべてのバージョンをバックアップしたい場合は、GUI ウィンドウでそれらをすべて選択するか、CLI で Only (-only) オプションを使用してバージョン番号にワイルド・カードを使用して以下に示すとおりファイル仕様を指定します。

  ```
  /DKA1/dir1/filename.txt.*
  ```

- 元の位置以外に復元すると、ディスク・デバイスと開始ディレクトリのみが変更されます。元のディレクトリ・パスが復元先として指定したパスに追加されて、新しい復元先ディレクトリとなります。
- 復元の際に［時刻属性の復元］(-notouch) オプションが無効になっている場合、ODS-5 ディスク上では最終アクセス日時が現在の日時で更新されます。ODS-2 ディスク上では、元の日時が設定されます。
- ソフト・リンクとして保存されたファイルは、「DCL SET FILE/ENTER」コマンドに相当するオプションを使用して復元します。この場合データは復元されません。入力されたソフト・リンクは、そのファイルが保存された時点の一次パス / ファイル名を示しています。一次パス / ファイル名が存在しないか、復元されなかった場合、ソフト・リンクは作成できません。

  OpenVMS システム・ディスクの復元コピーをブート可能にするには、OpenVMS WRITEBOOT ユーティリティを使用して、ディスクの復元後にブート・ブロックを書き込む必要があります。
- OpenVMS 上では、［使用中のファイルを移動］(-move) および［疎ファイルの復元］(-sparse) オプションは使用できません。

- OpenVMS システム上の ODS-5 ディスクからバックアップされたファイルで、拡張ファイルシステム名 (大文字 / 小文字の組み合わせ、Unicode 文字など) を持つものは、ODS-2 ディスクに復元できません。
- 復元中のファイルは、[復元時にファイルをロック] (-lock) オプションの設定にかかわらず、常にロックされます。
- 実行前 / 実行後コマンドの格納されているデフォルトのデバイスとディレクトリは、/omni$root/bin です。実行前 / 実行後コマンドを別の場所に置く場合は、ファイル仕様にデバイスとディレクトリ・パスを UNIX 形式で記述する必要があります。例 :
  /SYS$MANAGER/DP_SAVE1.COM
- [保護属性の復元] (-no_protection) オプションをオフにした場合、ファイルはデフォルトのオーナー、保護属性、ACL で作成されます。
- Skip (-skip) または Only (-only) フィルタでワイルドカード文字を指定する場合、複数の文字を表す場合は「*」を、1 文字を表す場合は「?」を使用してください。

復元オプション

Data Protector は総合的な復元オプションを備えており、復元を微調整できます。すべてのオプションにはデフォルト値があり、ほとんどの場合はこの値が適しています。

復元オプションは復元するデータによって異なります。たとえば、ファイルシステムの復元オプションは、ディスク・イメージの復元オプションとは異なります。

復元オプションのリスト

オブジェクトに対して設定可能な復元オプションのリストを以下に示します。これらのオプションは、バックアップ済みのオブジェクトから復元されるすべてのデータに対して適用されます。

一般的な復元オプション

[ターゲット・クライアント]

デフォルトでは、データのバックアップを行ったクライアントがデータの復元先になります。ドロップダウン・リストからセル内の別のシステムを選択すると、選択したクライアント・システム上で Disk Agent が起動され、データはそのシステムに復元されます。 別のクライアント・システムへの復元を行うには、[別のクライアントへ復元] ユーザー権限が必要です。

[削除済みファイルを除外]

フル・バックアップと増分バックアップの間に削除されたファイルを除外します。このオプションにより、前回の増分バックアップ実行時のディスクまたはディレクトリの状態が再現されます。このオプションは、増分バックアップ実行後に作成されたファイルには適用されません。このオプションは、デフォルトではオフになっています。

注意

フル・バックアップと増分バックアップの間に、削除されたファイルと同名のファイルを作成した場合は、新規作成したファイルも削除されます。

フル・バックアップと増分バックアップの間にファイルが元の位置から削除された場合は、[別名で復元] 機能を使用すると、(復元先の) 新しい位置にあるファイルも削除されます。また、ファイルの修正時刻は前回の増分バックアップ時刻よりも古くなります。

[削除済みファイルを除外] オプションが正しく動作するには、Cell Manager とクライアントの時刻の同期が取れている必要があります。

[使用中のファイルを移動]

このオプションは、ディスク上のファイルを復元時に置き換える際に、アプリケーションがそのファイルを使用している場合に有効です。このオプションは、[最新ファイルを保存] または [上書きする] オプションと併用します。このオプションは、デフォルトではオフになっています。

UNIX システムの場合、Data Protector は使用中のファイル名を *filename* から #*filename* に変更します (ファイル名の前に # マークを追加します)。アプリケーションは、使用中のファイルをクローズするまでそのまま使用します。その後は、復元されたファイルが使用されます。

Windows システムの場合、ファイルは *filename.001* として復元されます。すべてのアプリケーションは古いファイルをそのまま使用します。システムの再起動時に、古いファイルは復元されたファイルで置き換えられます。

[復元されたデータをリスト]

このオプションをオンにすると、Data Protector は、ファイル名とディレクトリ名を [モニター] ウィンドウに復元対象のオブジェクトとして表示します。このオプションは、デフォルトではオフになっています。

[統計情報の表示]

このオプションをオンにすると、Data Protector は復元対象の各オブジェクトの統計情報 (サイズや性能など) をレポートします。この情報は [モニター] ウィンドウに表示されます。このオプションは、デフォルトではオフになっています。

[不要な増分の省略]

このオプションを指定すると、特定オブジェクトの各ファイルの復元時にメディア内で再配置が行われます。Media Agent は特定項目を復元し、それを次の要求項目の隣に再配置して復元を継続します。これにより、複数の単一ファイル復元時のパフォーマンスが向上します。複数の Disk Agent がオブジェクトごとに起動される場合があることに注意してください。空のディレクトリを復元する場合は、このオプションをオフにしてください。このオプションは、デフォルトではオンになっています。

[疎ファイルの復元]

疎ファイルを元の圧縮形式で復元します。疎ファイルを元の形式で復元しない場合は、余分なディスク・スペースを消費する可能性があるため、このオプションは重要です。このオプションは、デフォルトではオフになっています。

このオプションは UNIX の疎ファイルに対してのみ適用されます。Windows の疎ファイルは常に疎ファイルとして復元されます。

[復元時にファイルをロック]

復元中のファイルへのアクセスが拒否されます。このオプションは、デフォルトではオフになっています。

[時間属性の復元]

各復元ファイルの時刻属性を保持します。このオプションをオフにすると、Data Protector は、復元されるオブジェクトの時刻属性を現在の日時に設定します。このオプションは、デフォルトではオンになっています。

[保護属性の復元]

各復元ファイルの元の保護属性を保持します。このオプションをオフにすると、Data Protector は現在の復元セッションの保護属性を適用します。このオプションは、デフォルトではオンになっています。

Windows システムでは、このオプションはファイル属性のみに適用されます。セキュリティ情報は、このオプションがオフに設定されている場合でも常に復元されます。

実行前 / 実行後コマンド

実行前 / 実行後コマンドの全般的な情報については、「実行前 / 実行後コマンド」(320 ページ) を参照してください。UNIX におけるこれらのコマンドの例は、「実行前 / 実行後コマンドの例 (UNIX の場合)」(A-21 ページ) を参照してください。実行前 / 実行後コマンドは、復元セッション全体の前後ではなく、各オブジェクトの復元の前後に実行されることに注意してください。

[実行前] 各オブジェクトの復元開始前に実行するコマンドを入力できます。Data Protector が復元を続行するには、このコマンドが正常終了しなければなりません。[実行前] コマンドは、Disk Agent が実行されているクライアント・システム上で実行されます。コマンドの指定方法については、オンライン・ヘルプを参照してください。

[実行後] 各オブジェクトの復元完了後に実行するコマンドを入力できます。[実行後] コマンドは、Disk Agent が実行されているクライアント・システム上で実行されます。コマンドの指定方法については、オンライン・ヘルプを参照してください。

[ファイル重複時の処理] オプション

[最新ファイルを保存] このオプションを選択すると、ファイルの最新バージョンが保存されます。ディスク上のファイルがバックアップ・ファイルのバージョンよりも新しい場合、ファイルは復元されません。ディスク上のファイルがバックアップ・ファイルのバージョンよりも古い場合は、バックアップされている新しいバージョンのファイルで上書きされます。このオプションは、デフォルトではオンになっています。

[上書きしない] このオプションを選択すると、ディスク上のファイルが保持されます。つまり、バックアップされている他のバージョンのファイルで上書きされません。ディスク上にないファイルだけがバックアップから復元されます。このオプションは、デフォルトではオフになっています。

[上書きする] このオプションを選択すると、ディスク上のファイルはバックアップされているファイルで置き換えられます。このオプションは、デフォルトではオフになっています。

Active Directory 固有のオプション

[権限付き] Active Directory データベースは、復元後は**更新されません**。復元先の既存のデータは復元データで上書きされます。[権限付き] モードで復元を実行するには、復元セッションの完了後に、コマンド・プロンプトから `ntdsutil.exe` を実行する必要があります。

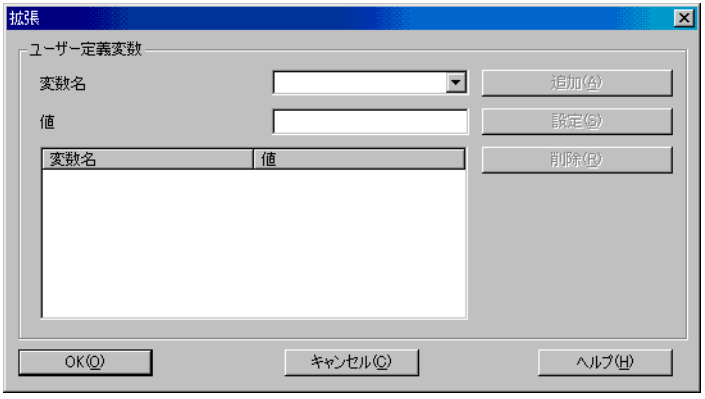
[権限なし] ［権限なし］複製モードは、デフォルトのオプションです。Active Directory のデータベースは、標準のレプリケーション (複製) テクニックを使って復元した後に更新されます。

[プライマリ] ［プライマリ］複製モードにより、ディレクトリ・サービスをオンラインで保持できます。このモードは、`FileReplicationService` を Active Directory サービスと併せて復元する際に使用します。複製した共有に対応するすべてのレプリケーション・パートナーが失われた場合に、このオプションを使用します。Certificate Server と Active Directory Server の場合、［プライマリ］は［権限付き］と同じ結果が得られます。

ユーザー定義の復元変数

プラットフォームおよび Data Protector との統合環境によっては、変数 (変数名と値) を設定することで、より柔軟な操作が可能になります。詳しい手順については、オンライン・ヘルプの索引キーワード「ユーザー定義の復元変数を設定する」を参照してください。

図 8-8 ユーザー定義の復元変数



復元のテクニック

以下の復元テクニックは、UNIX と Windows のどちらのプラットフォームでも使用できます。

別のパスにファイルを復元する

Data Protector のデフォルト設定では、データのバックアップ元のクライアントとディレクトリがデータの復元先になります。ただし、別のクライアント・システムやディレクトリにデータを復元することもできます。それぞれのファイルおよびディレクトリに、異なるパスや名前を指定できます。

オブジェクトに別の復元先を指定する

復元の [あて先] ページで、復元対象として選択したオブジェクトに対し、異なる復元先を指定できます。

- 適切なユーザー権限がある場合、[ターゲット・クライアント] ドロップダウン・リストでクライアント・システムを選択することにより、別のクライアント・システムに復元できます。デフォルトでは、Data Protector は同じディレクトリ構造を使用してオブジェクトを復元します。たとえば、システム A の `C:¥temp` ディレクトリからオブジェクトをバックアップした場合、データはシステム B の `C:¥temp` ディレクトリに復元されます
- 別のディレクトリを復元先に指定するには、[新しいディレクトリに復元] オプションを選択し、テキスト・ボックスに新しいパスを入力するか、またはブラウズして選択します。元のパスは、新しいパスの後ろに追加されます。たとえば、`C:¥sound¥songs` ディレクトリからバックアップしたデータに対し、新しいパスとして `¥users¥bing` を入力した場合、データは `C:¥users¥bing¥sound¥songs` ディレクトリに復元されます。

詳しい手順については、オンライン・ヘルプの索引キーワード「復元先オプション」を参照してください。

個々のファイルに個別の復元先を指定する

[別名で復元 / 復元先 ...] オプションで指定したディレクトリは、[あて先] プロパティ・ページで指定されたデフォルトのディレクトリよりも優先して適用されます。

復元の [ソース] プロパティ・ページの [別名で復元 / 復元先 . . .] オプションを使用すると、個々のファイルやディレクトリを個別のパスや名前で復元できます。

この機能は、初めて選択するツリー・ノード (ディレクトリ) や、選択済みのツリー・ノードとは階層的に依存関係にないツリー・ノードに対して使用できます。選択したツリー・ノードは青いチェック・マークで示され、依存するツリー・ノードは黒いチェック・マークで示されます。

[復元先を指定して復元] オプションは、元のパスを [位置] で入力した新しいパスの後ろに追加します。たとえば、colors.mp3 ファイルを C:¥sound¥songs ディレクトリからバックアップし、新しいパスとして ¥users¥bing を入力した場合、ファイルは C:¥users¥bing¥sound¥songs ディレクトリに復元されます。

[別名で復元] オプションは、元のパスを [位置] で入力したパスに置き換えます。復元先のパスには、新しいディレクトリまたは既存のディレクトリを指定できます。復元時に、ファイル名やディレクトリ名を変更できます。たとえば、colors.mp3 ファイルを C:¥sound¥songs ディレクトリからバックアップし、新しいパスとして ¥users¥bing¥colors.mp3 を入力した場合、ファイルは C:¥users¥bing ディレクトリに復元されます。

注意

以下の場合、[上書きする] オプションが有効に設定されているデータが削除される危険があることに注意してください。

- 既存のファイル / ディレクトリ名を指定して復元した場合
- ファイルまたはディレクトリ名を指定しないで既存のパスを指定した場合

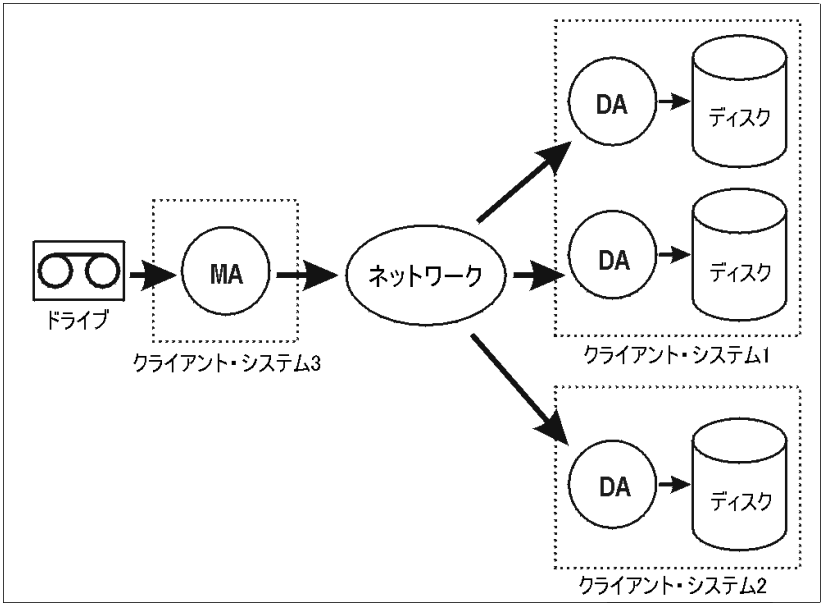
たとえば、[位置] テキスト・ボックスに、colors.mp3 ファイルの復元先として新しいパス ¥users¥bing を入力して、ファイル名を入力しなかった場合、colors.mp3 ファイルは bing という名前で復元されます。この場合、bing という元のディレクトリは削除され、復元されたファイルに置き換わります。

複数ファイルの並行復元

並行復元とは

並行復元では、複数ファイルを複数ディスクに同時に復元できます。この場合、バックアップ時に 2 以上の同時処理数を設定して同じデバイスにディスクをバックアップしたとみなされます。これにより、復元速度が向上します。並行復元は、並行バックアップ (バックアップ時に複数のディスクからファイルを 1 つのデバイスに同時にバックアップする) を補完する動作です。

図 8-9　複数ファイルの並行復元



この図は、1 つのメディアからファイルを並行して復元する例を示しています。各オブジェクトはそれぞれ別の DA を使用しています。

並行復元の実行方法

異なるディスクに復元するデータを選択し、復元を開始します。実行する復元の種類 (並行復元または単一復元) を尋ねるメッセージが表示されます。並行復元を選択すると、複数の Data Protector Disk Agent が並行して実行されます。詳細は、「復元対象データの選択」(364 ページ) を参照してください。

IDB 内に存在しないファイルを表示する

Data Protector では、データに関する情報が IDB 内に存在しない場合も、バックアップ・メディアから直接データを表示したり復元することができます。

どのような場合にメディアから復元を行うか

以下の場合に、この方法で復元を行います。

- バックアップ済みのデータやメディアに関する情報を IDB から削除した場合。
- カタログ保護期限が切れた場合。データおよびカタログ保護の詳細は、「最も頻繁に使用されるバックアップ・オプション」(292 ページ) を参照してください。
- メディアが別の Data Protector セルにあるため、このセルの IDB で認識されない場合。この場合、まずメディアをインポートする必要があります。

必要条件

Cell Manager に大量のメモリが必要です。必要なメモリ容量は次の式で算出できます。*number_of_files* × 200 バイト

制限事項

- メディアから、データベース・アプリケーション・オブジェクトをリストすることはできません。
- 複数のメディアにまたがるファイルは復元できません。ファイルの復元に必要なすべてのメディアをまずインポートした後、[内部データベースのリスト] オプションを使ってファイルを復元できます。

メディアからの復元方法

データをメディアから復元するには、[復元] コンテキストの [アクション] メニューで [メディアのリスト] をクリックし、[メディアから復元] ウィザードに従って操作を進めます 詳しい手順については、オンライン・ヘルプの索引キーワード「メディアからデータを直接復元する」を参照してください。

使用中のファイルを復元する

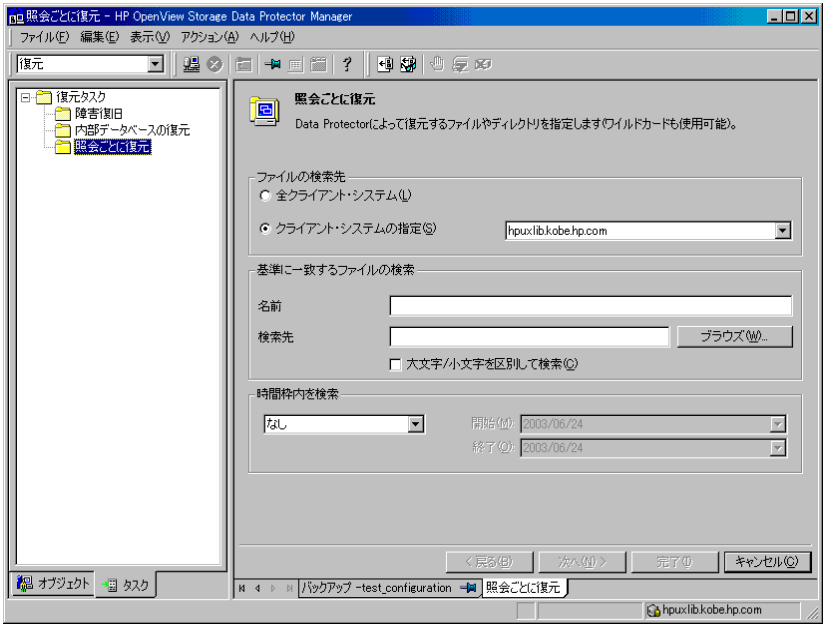
Data Protector では、他のアプリケーション (データベースやワードプロセッサのドキュメントなど) で使用中 (オープン中) のファイルをバックアップしたり復元できます。

Data Protector では、復元対象のファイルが使用中の場合の動作を、復元オプションを使って指定できます。**［復元時にファイルをロック］**と**［使用中のファイルを移動］**の 2 つのオプションがあります。詳細は、「復元オプション」（391 ページ）を参照してください。

照会ごとに復元する

復元対象のファイルの絶対パスが不明な場合でも、そのファイルのバックアップ時のログ・レベルが［ファイル・レベルまでログに記録］または［すべてログに記録］に設定されていれば、IDB 内でファイルを検索することができます。少なくとも名前の一部がわかっていれば、［照会ごとに復元］タスクを使用してファイルまたはディレクトリを検索できます。

図 8-10　照会ごとに復元



照会ごとの復元方法　Data Protector Manager の［復元］コンテキストから、［照会ごとに復元］タスクを選択します。［タスク］ナビゲーション・タブを使用します。図 8-10 を参照してください。詳しい手順については、オンライン・ヘルプの索引キーワード「照会ごとに復元」を参照してください。

[照会ごとに復元] 機能を使用して非 ASCII 文字を含むファイル名を指定するときは、純粋な Windows 環境で操作している場合を除き、非 ASCII 文字をワイルドカードに置き換えてください。

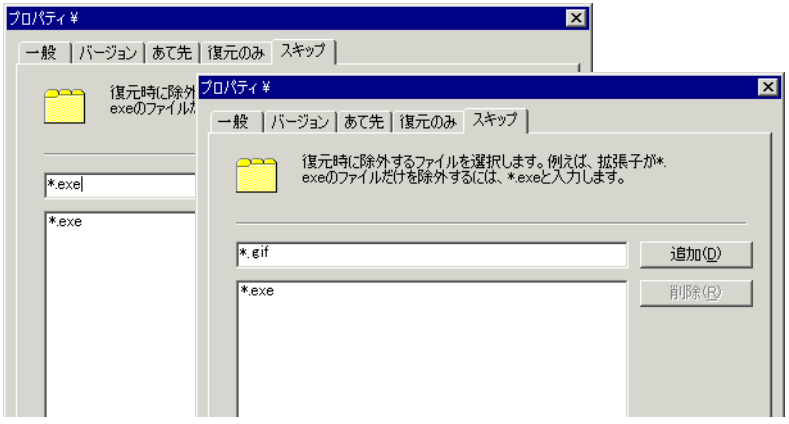
復元対象から除外するファイルの指定

Data Protector では、特定のファイルを復元対象から除外できます。ワイルドカード (* または ?) を使用して、指定した基準と一致するファイルを除外します。たとえば、*.exe と入力した場合、ファイル名が .exe で終わるファイルが復元対象から除外されます。

復元対象から除外するファイルの指定方法

復元の [ソース] プロパティ・ページで、復元対象のツリー・ノードを選択し、右クリックをしてプロパティを開きます。[スキップ] プロパティ・ページで、除外するファイルの基準を指定します。詳しい手順については、オンライン・ヘルプの索引キーワード「復元対象から除外するファイルを指定する」を参照してください。

図 8-11 復元対象から除外するファイルの指定



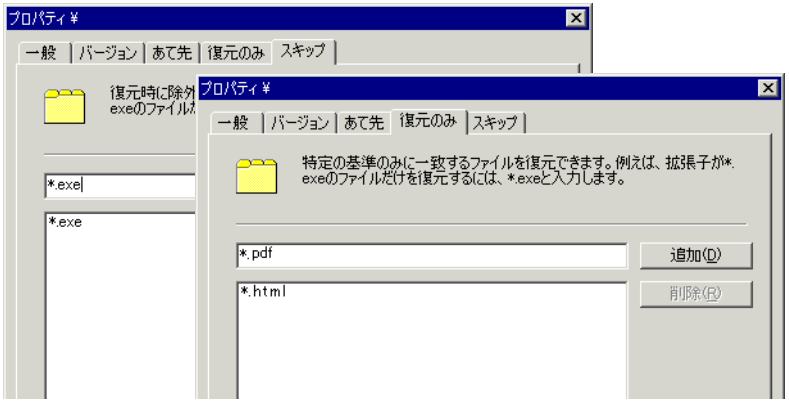
条件に一致するファイルだけを復元対象として選択する

Data Protector では、特定のファイルだけを復元できます。ワイルドカード (* または ?) を使用して、指定した基準と一致するファイルのみを復元します。たとえば、*.exe と入力した場合、ファイル名が .exe で終わるファイルのみを復元します。

復元対象ファイルの条件の指定方法

復元の [ソース] プロパティ・ページで、復元対象のツリー・ノードを選択し、右クリックをしてプロパティを開きます。[復元のみ] プロパティ・ページで、復元対象ファイルの一致基準を指定します。詳しい手順については、オンライン・ヘルプの索引キーワード「条件に一致するファイルだけを復元対象として選択する」を参照してください。

図 8-12　復元対象ファイルの条件の指定



ファイルやディレクトリを手作業で復元する

ファイルまたはディレクトリをブラウズできなくなった場合、ファイルやディレクトリを手作業で復元する必要があります。データのカタログ保護期限が切れた場合や、[ログなし] オプションを使ってバックアップを行った場合に必要になります。

必要条件

ファイルまたはディレクトリを手作業で追加するには、ファイルまたはディレクトリの正確なパスと名前を指定する必要があります。ファイル名とパス名は大文字と小文字が区別されます。

ファイルやディレクトリの手作業での追加方法

復元の [復元サマリー] ページで、ファイルまたはディレクトリの正確なパスと名前を入力し、[追加] をクリックします 詳しい手順については、オンライン・ヘルプの索引キーワード「ファイルまたはディレクトリの手作業での復元」を参照してください。

復元元のメディア・セットを選択する

復元したいオブジェクト・バージョンが複数のメディア・セットに存在している場合、それらが Data Protector のデータ複製方法のいずれかを使用して作成されたものであれば、どのメディア・セットを使用して復元しても構いません。デフォルトでは、コピー元となるメディア・セットは自動的に選択されます。メディア・セットの選択をユーザーが設定するには、メディアの位置の優先順位を指定します。

注記

メディア位置の優先順位を使用するためには、各メディアの位置を指定しておく必要があります。この操作は個々のメディアまたは複数のメディアに対して実行できます。

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できます (統合ソフトウェア・オブジェクトの復元を除く)。復元に必要なメディアが使用不可能である場合、マウント要求が発行されます。詳しい手順については、オンライン・ヘルプの索引キーワード「検索 - 復元対象のメディア」を参照してください。

注記

メディア・コピー機能を使って作成したコピーは、データ復元時に [メディア] タブ内の必要なメディアの一覧に表示されず、位置優先順位の対象にもなりません。これらのコピーは、オリジナルのメディア (コピー元のメディア) が存在しないか使用できない場合にのみ使われます。

メディアの位置の優先順位

メディア・セットの選択をユーザーが制御するには、メディア位置の優先順位を設定します。メディア・セットの選択アルゴリズムに合致するメディア・セットが複数ある場合は、位置の優先順位が高いメディア・セットが使用されます (優先順位は [1] が最高で、[なし] が最低です)。選択アルゴリズムの詳細については、*HP OpenView Storage Data Protector コンセプト・ガイド*を参照してください。

メディアの位置の優先順位は 2 つのレベルで指定します。

- グローバルに設定する場合は［デバイス / メディア］コンテキストを使用します。グローバルに設定された優先順位は復元セッション全体に適用されますが、復元セッション・レベルで設定された優先順位によって上書きされます。図 8-13 (405 ページ) を参照してください。

詳しい手順については、オンライン・ヘルプの索引キーワード「設定 - メディアの位置の優先順位」を参照してください。

- [復元] コンテキストでは、特定の復元セッションに対するメディアの優先順位を設定できます。ここで設定された優先順位は、グローバル・レベルで設定された優先順位を上書きします。図 8-14 (406 ページ) を参照してください。

  詳しい手順については、オンライン・ヘルプの索引キーワード「検索 - 復元対象のメディア」を参照してください。

図 8-13　メディアの位置の優先順位をグローバルに設定

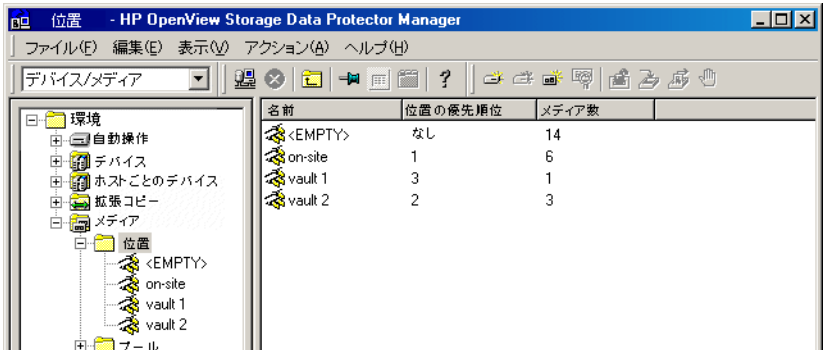
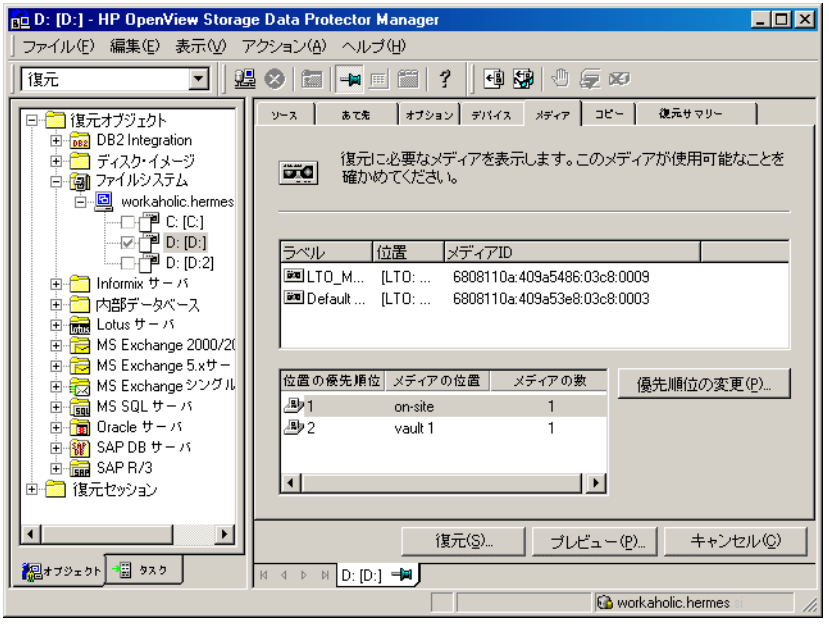


図 8-14　メディアの位置の優先順位を復元セッションごとに設定



9 モニター、レポート、通知、およびイベント・ログ

本章の概略

本章は以下の各項で構成されています。

Manager-of-Managers 機能を使用して、複数のセルを同時にモニターできます。詳しくは、第 10 章「Manager-of-Managers 環境」(463 ページ) を参照してください。

Data Protector のユーザー・インタフェースへのアクセス権がない場合でも、Web ブラウザを使ってレポートを表示したり通知を設定できます。この方法の詳細は、「Web レポートおよび Web 通知の構成」(457 ページ) を参照してください。

セッションのモニター

Data Protector では、実行中のセッションを管理したり、マウント要求に応答できます。セッションのステータスや種類、オーナー、セッション ID、セッションの開始時刻、および対応するバックアップ仕様の名前を確認できます。

対話型バックアップ / 復元 / メディア管理セッションを実行すると、[モニター] ウィンドウが開いて、使用されているオブジェクトやバックアップ・デバイス、セッション中に生成されるメッセージが表示されます。ユーザー・インタフェースを終了しても、セッションは続行されます。

バックアップ・セッションまたは復元セッションの進行中に通知されるメッセージのレベルを変更するには、バックアップ仕様の構成時または復元セッションの開始時に [レポート・レベル] オプションを変更します。

注記

Data Protector のモニター機能にアクセスできるのは、Admin グループに所属する Data Protector ユーザーと [モニター] ユーザー権限を付与された Data Protector ユーザーだけです。

現在のセッションのモニター

現在実行中のセッションは、Data Protector GUI の [モニター] コンテキストで確認できます。

注記

現在実行中のセッションは、実行前スクリプトの完了後に [モニター] コンテキストに表示されます。

更新間隔

現在実行中のセッション一覧は、設定されている更新間隔 (デフォルトでは 5 秒) で自動更新され、新しいセッションがあれば表示されます。デフォルトの更新間隔を変更するには、Data Protector GUI で以下の手順を実行してください。

1. [ファイル] メニューの [選択値] をクリックします。

[選択値] ダイアログ・ボックスが表示されます。

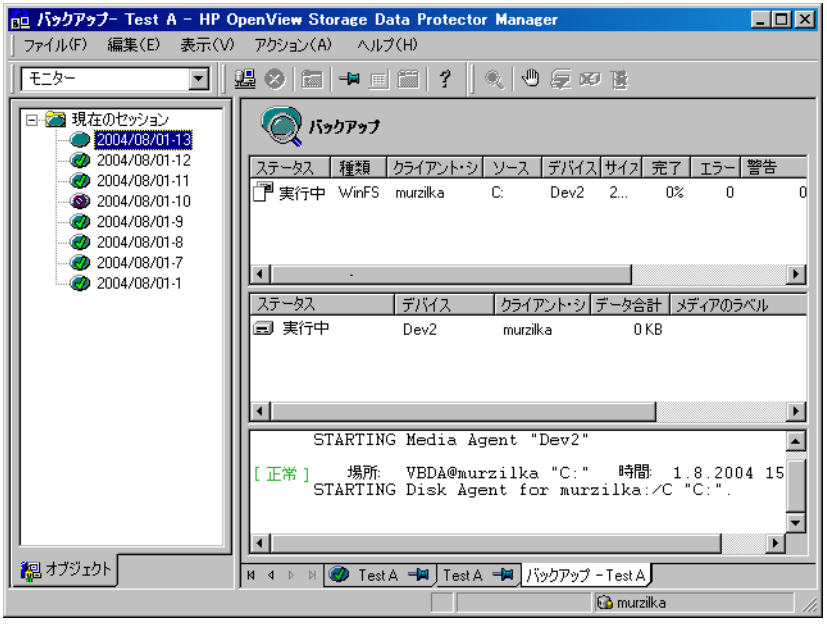
2. [モニター] タブをクリックします。
3. Cell Manager と Manager-of-Managers (MoM) の更新間隔を秒単位で指定します。

現在実行中のセッションをモニターするには、Data Protector GUI で以下の手順を実行します。

1. コンテキスト・リストで [モニター] をクリックします。

   現在実行中のすべてのセッションが結果エリアに一覧表示されます。
2. モニターするセッションをダブルクリックします。図 9-1 (410 ページ) を参照してください。

図 9-1 **現在のセッションのモニター**



セッションのクリア 完了または中止されたすべてのセッションを [モニター] コンテキストの結果エリアから削除するには、以下の手順を実行します。

1. Scoping ペインで [現在のセッション] をクリックします。

2. [アクション] メニューの [セッションをクリア] を選択します。または、ツールバー上の [セッションをクリア] アイコンをクリックします。

完了または中止された特定のセッションを現在実行中のセッション一覧から削除するには、そのセッションを右クリックし、[リストから削除] を選択します。

注記

Data Protector GUI を再起動すると、完了または中止されたすべてのセッションが、[モニター] コンテキストの結果エリアから自動的に削除されます。

完了または中止されたセッションの詳細については、「過去のセッションの表示」を参照してください。

過去のセッションの表示

過去のセッションをモニターするには、Data Protector GUI で以下の手順を実行します。

1. コンテキスト・リストで [内部データベース] をクリックします。

MoM

Manager-of-Managers を実行している場合は、コンテキスト・リストで [モニター] を選択し、目的の Cell Manager を選択します。[ツール] メニューの [データベース管理 . . .] を選択すると、新しい Data Protector GUI が開き、[内部データベース] コンテキストが選択された状態になっています。

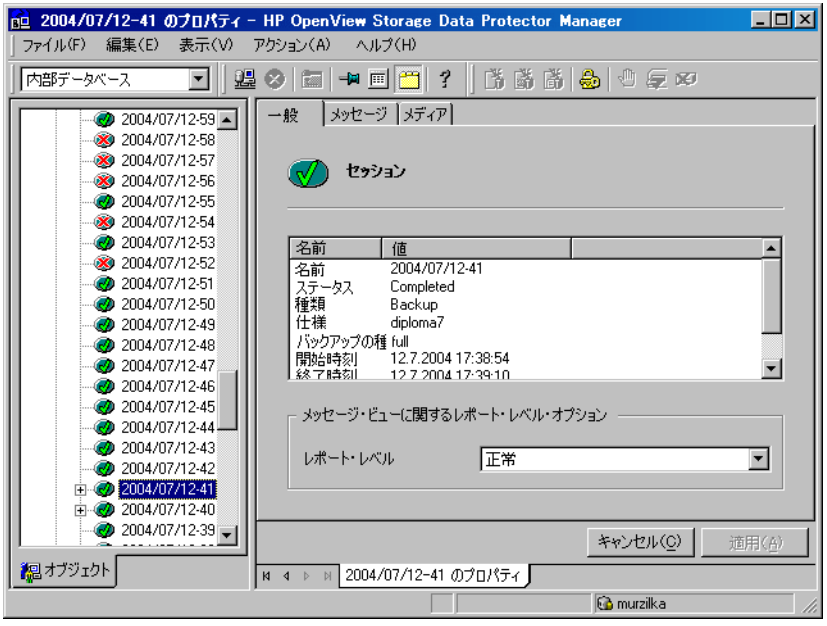
2. Scoping ペインで、[セッション] を展開すると、IDB に保存されているすべてのセッションが表示されます。

   セッションは日付順に表示されます。各セッションには、YY/MM/DD 形式の日付と固有の番号から構成されるセッション ID が付加されています。

3. 特定のセッションの詳細情報を見るには、そのセッションを右クリックし、[プロパティ] を選択します。

4. セッションの一般情報、セッション・メッセージ、セッションで使われたメディアに関する情報を見るには、それぞれ [一般] タブ、[メッセージ] タブ、[メディア] タブをクリックします。図 9-2 (412 ページ) を参照してください。

図 9-2　完了したセッションの表示



マウント要求への応答

Data Protector は、以下の場合にマウント要求を発行します。

- 現在使用しているメディアの使用限度に達し、Data Protector が空のメディアを必要としている場合。
- メールスロットが開いている場合。この場合はメールスロットを閉じてください。

マウント要求への応答では、必要なメディアがデバイス内にロードされていることを確認します。セッションをモニター中にマウント要求に応答する場合は、以下の手順を行ってください。

1. コンテキスト・リストで [モニター] をクリックします。
2. 必要なメディアをデバイスに挿入します。ライブラリ・デバイスがある場合には、マウント要求で要求されたスロットを使う必要はありません。
3. 結果エリアで、ステータスが [マウント要求] になっているデバイスをダブルクリックして、セッションに関する情報を表示します。
4. ステータスが [マウント要求] になっているデバイスを選択します。
5. [アクション] メニューで、[マウント要求の確認] をクリックします。セッションとデバイスのステータスが [実行中] に変わります。

ヒント

ステータスが [マウント要求] になっているデバイスを右クリックして [マウント要求の確認] を選択することもできます。

失敗したバックアップの再開

バックアップ中に、システムのシャットダウンやネットワークの問題などによりシステムが使用不可能となる場合があります。この場合、システムによっては、バックアップされなかったり、一部だけがバックアップされる (つまりバックアップされないオブジェクトが残る) ことがあります。

本項では、失敗したバックアップ・セッションを再開するための詳しい手順を説明します。失敗したバックアップの詳しい管理方法については、「失敗したバックアップの管理」(335 ページ) を参照してください。

バックアップ仕様が保存されていないことが原因で失敗したセッションは再開できません。

関連する問題を解決してから失敗したセッションを再開してください。以下の手順を行います。

1. ［Data Protector Manager］で［内部データベース］コンテキストを選択します。

   Manager-of-Managers を実行している場合は、コンテキスト・リストで [クライアント] を選択し、[エンタープライズ・クライアント] を展開します。バックアップが失敗した Cell Manager を選択し、[ツール] メニューの [データベース管理 . . .] を選択します。

2. 新しい Data Protector ウィンドウが開き、[内部データベース] コンテキストが表示されます。[内部データベース] で [セッション] を選択して画面を展開します。
3. 結果エリアで目的のバックアップを検索します。

   各カラムの一番上にあるボタンを使ってセッションの順番を並べ替えることができます。
4. 失敗したセッションを右クリックした後、[失敗したオブジェクトの再開] を選択します。
5. [はい] をクリックして処理を実行します。

実行中のセッションの中止

バックアップや復元、メディア管理操作を停止したい場合は、セッションを中止します。セッションを中止する前にバックアップまたは復元が完了していたデータのバックアップ・コピーまたは復元データだけが保存されることになります。

1. コンテキスト・リストで、[モニター] をクリックします。現在のセッションの進行状況とステータスが結果エリアに表示されます。

   Manager-of-Managers を実行している場合は、Scoping ペインで [エンタープライズ・モニター] を展開し、モニター対象の Cell Manager を選択します。現在のセッションの進行状況とステータスが結果エリアに表示されます。
2. 列見出しをクリックすると、セッションの順番を並べ替えることができます。
3. 中止したいセッションを右クリックし、[中止] を選択します。

バックアップ用に選択したディスクのサイズをチェックしているときにバックアップ・セッションを中止しようとした場合は、サイズのチェック (treewalk) が完了した時点でバックアップが中止されます。

ヒント

バックアップ、復元、メディア管理セッションを対話形式で起動した場合は、Data Protector の [バックアップ]、[復元]、[デバイス / メディア] コンテキストからそれぞれセッションを中止することもできます。

表示されるメッセージの数の変更

バックアップ・オプションや復元オプションを変更することにより、バックアップ・セッションや復元セッションについて通知されるメッセージのレベルを変更できます。

表示されるメッセージに影響を与えるバックアップ・オプションについては、「バックアップ・オプションの使用」(290 ページ) を参照してください。

表示されるメッセージに影響を与える復元オプションについては、「復元オプション」(391 ページ) を参照してください。

複数セルの同時モニター

Manager-of-Managers 機能を使用して、複数のセルを同時にモニターできます。

詳しくは、第 10 章「Manager-of-Managers 環境」(463 ページ) を参照してください。

Data Protector レポート

レポートとは

Data Protector のレポートによって、バックアップ環境に関する各種の情報が得られます。たとえば、前回のバックアップのステータス、ネットワーク内のシステムに関するバックアップ構成の有無、デバイスのステータスなどをチェックできます。

Data Protector のレポートは、バックアップ環境の管理とプランニングに使用する強力なツールで、柔軟性に富んだカスタマイズ可能なツールです。

レポートおよびレポート・グループは、Data Protector GUI または、Java 対応の任意の Web ブラウザを使って構成できます。

注記

Data Protector のレポート機能にアクセスできるのは、Admin グループに所属する Data Protector ユーザー、およびレポート、通知、イベント・ログのユーザー権限を付与された Data Protector ユーザーだけです。

必要条件

CRS サービスを実行している Data Protector ユーザーを削除してはいけません。このユーザーは、インストール時にデフォルトで構成されます。Windows Cell Manager の場合、このユーザーのアカウントでインストールが実行されます。UNIX Cell Manager 場合、このユーザーが Cell Manager の root ユーザーとなります。

レポート・グループ

複数のレポートを 1 つのレポート・グループにまとめることにより、それらのレポートのスケジュール設定、対話形式での開始、通知によるトリガが可能になります。

レポートの開始

レポートを開始するには、Data Protector GUI、Data Protector コマンド行インタフェース、Data Protector Web レポート・インタフェース、Data Protector スケジューラ、通知イベントまたは Data Protector コマンド行インタフェース・コマンドを含む実行後スクリプトのいずれかを使います。

複数セルのレポート

レポート機能は、Manager-of-Managers 機能を使用している場合の複数セル構成でも使用できます。

レポート・パラメータ

レポートは、省略可能な入力パラメータ (省略可能な選択項目) を構成することによってカスタマイズできます。一部の入力パラメータは、複数の項目を選択することができます。

レポート構成時に、省略可能な入力パラメータ (省略可能な選択項目) が 1 つも指定されていない場合は、デフォルト値が適用されます。デフォルト値は、オブジェクトの場合は < *すべて* >、時間枠の場合は < *時間制限なし* > です。

レポートまたはレポート・グループを構成するには、以下を指定する必要があります。

- レポートの名前
- レポートの種類
- 送信方法
- 受信者
- 形式

その他の入力パラメータ (選択項目) は、レポートの種類によって異なります。

レポートの形式

レポートはさまざまな形式で出力できます。必要に応じて、入力パラメータ (選択項目) を表示することもできます。詳しくは、「レポートの形式」(431 ページ) を参照してください。

レポートの送信方法

レポートは、さまざまな方法で送信できます。「レポートの送信方法」(433 ページ) を参照してください。

レポートの種類

Data Protector が作成するさまざまな種類のレポートを表 9-1 に示します。

表 9-1

バックアップ仕様	バックアップ・オブジェクトの平均サイズ、バックアップのスケジュール、バックアップが構成されていないファイルシステムなど、バックアップに関する情報を提供します。
構成	Data Protector セル、バックアップ用に構成されていないデバイス、バックアップ用に構成されていないシステムなどの構成に関する情報を提供します。
IDB	IDB のサイズや IDB 削除セッションの結果に関する情報を提供します。
プールとメディア	メディア・プールおよび使用されたメディアに関する情報を提供します。
時間枠内のセッション	特定の期間内に実行されたバックアップ・セッションに関する情報を提供します。
単一セッション	特定のセッションの詳細情報を提供します。

バックアップ仕様に関するレポート

以下の表に、バックアップ仕様に関するレポートについて示します。バックアップ仕様に関するレポートでは、バックアップ・オブジェクトの平均サイズ、バックアップのスケジュール、バックアップ用に構成されていないファイルシステムなど、バックアップに関する情報を提供します。

サポートされている形式については、「レポートの形式」(431 ページ) を参照してください。

表 9-2 バックアップ仕様に関するレポート

レポートと omnirpt オプション	説明	必須選択項目	省略可能な選択	サポートされている形式
[バックアップ仕様のツリー] dl_trees	指定したバックアップ仕様に含まれているツリーをすべて示します。ドライブ名とツリー名も示します。	なし	• バックアップ仕様 • バックアップ仕様のグループ	すべての形式
[バックアップを持たないオブジェクト] obj_nobackup	バックアップ仕様に含まれているオブジェクトのうち、有効なバックアップ (バックアップが正常に完了したものや、保護期限が切れていないもの) を持たないオブジェクトをすべて示します。[a]	なし	• バックアップ仕様 • バックアップ仕様のグループ • 日数[b]	すべての形式
[オブジェクトの最新バックアップ] obj_lastbackup	指定したバックアップ仕様のそれぞれについて、すべてのオブジェクトと、前回のフル・バックアップと前回の増分バックアップの日時を示します。	なし	• バックアップ仕様 • バックアップ仕様のグループ • 日数[b]	すべての形式
[オブジェクトの平均サイズ] obj_avesize	指定したバックアップ仕様に含まれているオブジェクトの平均サイズを表示します。これは、オブジェクトのフル・バックアップと増分バックアップのサイズです。	なし	• バックアップ仕様 • バックアップ仕様のグループ • 日数[b]	すべての形式

表 9-2　バックアップ仕様に関するレポート

レポートと omnirpt オプション	説明	必須選択項目	省略可能な選択	サポートされている形式
[構成済みでないファイルシステム] fs_not_conf	指定したバックアップ仕様のいずれにおいても構成されていないディスク (ファイルシステム) をすべて示します。	なし	• バックアップ仕様 • バックアップ仕様のグループ	すべての形式
[バックアップ仕様情報] dl_info	指定したすべてのバックアップ仕様に関して、バックアップ仕様名、種類、グループ、オーナー、実行前 / 実行後コマンドを表示します。	なし	• バックアップ仕様 • バックアップ仕様のグループ	すべての形式
[バックアップ仕様スケジュール] dl_sched	指定したバックアップ仕様のそれぞれについて、次回のバックアップ日時を示します。	なし	• バックアップ仕様 • バックアップ仕様のグループ	すべての形式

a. 統合ソフトウェア用のバックアップ仕様には適用されません。
b. レポート開始時点から過去にさかのぼった日数

構成に関するレポート

以下の表に、構成に関するレポートについて示します。構成に関するレポートでは、Data Protector セル、デバイス、バックアップ用に構成されていないシステムなどの構成に関する情報を提供します。サポートされている形式については、「レポートの形式」(431 ページ) を参照してください。

表 9-3 構成に関するレポート

レポートと omnirpt オプション	説明	必須選択項目	省略可能な選択	サポートされている形式
[セル情報] cell_info	Data Protector セルに関する情報 (クライアント数、バックアップ仕様、メディア管理サーバ、ライセンス・サーバ) を示します。	なし	なし	すべての形式
[Data Protector が使用していない構成済みクライアント] hosts_unused	構成済みのクライアントのうち、バックアップに使用されておらず、デバイスが構成されていないクライアントをすべて示します。	なし	なし	すべての形式
[Data Protector が使用していない構成済みデバイス] dev_unused	構成済みのデバイスのうち、バックアップに使用されていないデバイスを示します。	なし	なし	すべての形式
[スケジュールのチェック] lookup_sched	指定した日数内に開始するようにスケジュール設定されているバックアップ仕様を示します。	日数	なし	すべての形式
[Data Protector 向けに構成されていないクライアント] hosts_not_conf	選択したドメイン内のクライアントの内、現在のセルの要素ではないものを示します。	ネットワークの範囲	なし	すべての形式

表 9-3 構成に関するレポート

レポートと omnirpt オプション	説明	必須選択項目	省略可能な選択	サポートされている形式
[ライセンス付与] ライセンス管理	すべてのライセンスとライセンス総数および使用可能なライセンス数を示します。	なし	なし	すべての形式
[クライアントのバックアップの構成 (クライアントのバックアップ・オブジェクト)] host	指定したクライアントに関して、未構成のファイルシステム、すべてのオブジェクト、有効なバックアップが存在するオブジェクトとそのバックアップ日時および平均サイズなどの情報を示します。	ホスト名	なし	すべての形式

IDB に関するレポート

以下の表に、IDB に関するレポートについて示します。IDB に関するレポートは、IDB のサイズと IDB 削除セッションの結果に関する情報を提供します。サポートされている形式については、「レポートの形式」(431 ページ) を参照してください。

表 9-4 IDB のレポート

レポートと omnirpt オプション	説明	必須選択項目	省略可能な選択	サポートされている形式
[IDB サイズ] db_size	メディア管理データベース、カタログ・データベース、データベース拡張ファイル、統計値 (DC バイナリ・ファイル、SMBF、SIBF)、ディスク・スペース不足のデータベースを表形式で表示します。	なし	なし	すべての形式

表 9-4 IDB のレポート

レポートと omnirpt オプション	説明	必須選択項目	省略可能な選択	サポートされている形式
[IDB の削除] db_purge	すべての削除セッションとセッションに関する情報 (開始時刻、終了時刻、継続期間、休止時間、ファイル名レコードの数、読み取ったデータ量 (MB 単位)) を示します。	なし	なし	すべての形式
[削除プレビュー] db_purge_preview	データベース内のファイル名の総数 (1000 単位)、データベース内の古くなったファイル名の推定数 (1000 単位)、データベース削除の推定期間 (秒単位) を示します。	なし	なし	すべての形式

表 9-4 IDB のレポート

レポートと omnirpt オプション	説明	必須選択項目	省略可能な選択	サポートされている形式
[システム処理能力] db_system	セル内の各 Data Protector クライアントごとに、IDB 内のファイル名の数 (1000 単位)、IDB 内のアクティブなファイル名の数 (1000 単位)、IDB 内のファイル名の増加率 (1 日あたりの新規ファイル名の数)、IDB 内で 1 日あたりに削除されたファイル名の数、1 年あたりのアクティブ増加率、およびダイナミック・インジケータ (medium/high/low/critical) を示します。 IDB 内のバックアップ済みファイルのうち、IDB 内のファイル・バージョンに関連付けられていないファイルは、アクティブでないファイル名とみなされます。1 年あたりのアクティブ増加率の計算方法には、以下の 2 通りの方法があります。 Data Protector データベース削除セッションが Data Protector データベースに記録されていない場合は、過去 11 日の増加率に基づいて 1 年あたりのアクティブ増加率が計算され、1 年あたりの推定増加率として示されます。 Data Protector データベース削除セッションが Data Protector データベースに記録されている場合は、最後の Data Protector データベース削除セッション以降の期間に基づいて 1 年あたりのアクティブ増加率が計算され、1 年あたりの推定増加率として示されます。	なし	なし	すべての形式

プールとメディアに関するレポート

以下の表に、プールとメディアに関するレポートについて示します。プールとメディアに関するレポートは、メディア・プールと使用されているメディアに関する情報を提供します。サポートされている形式については、「レポートの形式」(431 ページ) を参照してください。

表 9-5 プールとメディアに関するレポート

レポートと omnirpt オプション	説明	必須選択項目	省略可能な選択	サポートされている形式
[メディアの拡張リスト] media_list_extended	指定した検索条件に一致するすべてのメディアを表示します。メディアごとに、メディア ID、メディア・ラベル、メディアの位置、メディアの状態、メディア保護、使用中スペースと総スペース (MB 単位)、メディアが前回アクセスされた日時、メディア・プール、メディアの種類、およびバックアップ時にそのメディアを使用したバックアップ仕様を示します。	なし	• 説明 • 位置 • プール名 • メディアの種類 (DDS や DLT など) • 条件 • 保護期限 1 • 時間枠 2 • ライブラリ・デバイス	すべての形式
[プールのリスト] pool_list	指定した検索条件に一致するすべてのプールを表示します。プールごとに、プール名、説明、メディアの種類、メディアの総数、保護データが格納されている満量状態 / 追加可能メディアの数、保護データが格納されていないフリー・メディアの数、[不良]/[普通]/[良好] の各状態のメディアの数を示します。	なし	• プール名 • 位置 • メディアの種類 (DDS、DLT など) • ライブラリ・デバイス • 時間枠 2	すべての形式

表 9-5 プールとメディアに関するレポート

レポートと omnirpt オプション	説明	必須選択項目	省略可能な選択	サポートされている形式
[メディア統計] media_statistics	検索条件に一致するメディアに関する統計情報を表示します。メディア数、スクラッチ・メディアの数、[保護]/[良好]/[普通]/[不良] の各状態のメディアの数、追加可能メディアの数、メディア上の総スペース / 使用中スペース / 空きスペースを示します。	なし	• 説明 • 位置 • プール名 • メディアの種類 (DDS や DLT など) • ステータス • 保護期限 1 • 時間枠 2 • ライブラリ・デバイス	すべての形式
[メディアのリスト] media_list	指定した検索条件に一致するすべてのメディアを表示します。メディアごとに、メディア ID、メディア・ラベル、メディアの位置、メディアの状態、メディア保護、使用中スペースと総スペース (MB 単位)、メディアが前回アクセスされた日時、メディア・プール、およびメディアの種類を示します。	なし	• 説明 • 位置 • プール名 • メディアの種類 (DDS や DLT など) • 条件 • 保護期限 1 • 時間枠 2 • ライブラリ・デバイス	すべての形式

1. 以下の選択肢があります。

[設定しない]/[非保護]/[保護] ([保護] の場合は、以下のサブオプションがあります)。

レポート時点からデータ保護期限が切れるまでの残りの日数、または日数指定なし。

2. メディアをバックアップに使用した時間枠。

相対時間 : 最初のパラメータには時間枠の始点 (レポート開始時点から過去にさかのぼった時間数) を指定し、2 番目のパラメータには時間枠の終点 (始点からの時間数) を指定します。

絶対時間 : 最初のパラメータには時間枠の始点 (日付) を指定し、2 番目のパラメータには時間枠の終点 (日付) を指定します。

時間枠内のセッションに関するレポート

以下の表に、Data Protector の時間枠内のセッションに関するレポートについて示します。時間枠内のセッションに関するレポートは、特定の時刻に実行されたバックアップ・セッションに関する情報を提供します。サポートされている形式については、「レポートの形式」(431 ページ) を参照してください。

表 9-6 時間枠内のセッションに関するレポート

レポートと omnirpt オプション	説明	必須選択項目	省略可能な選択	サポートされている形式
[バックアップ・セッションのリスト] list_sessions	指定した時間枠内のすべてのセッションを表示します。	時間枠 1	• バックアップ仕様 • バックアップ仕様のグループ	すべての形式
[セッション・フロー] session_flow	検索条件に一致するバックアップ・セッションのフロー・チャートです。指定した時間枠に対応する各セッションの継続期間をグラフィック表示します。	時間枠 1	• バックアップ仕様 • バックアップ仕様のグループ	HTML

表 9-6 時間枠内のセッションに関するレポート

レポートと omnirpt オプション	説明	必須選択項目	省略可能な選択	サポートされている形式
[デバイス・フロー] device_flow	検索条件に一致するバックアップ・セッションのフロー・チャートです。指定した時間枠に対応する各セッションの継続期間をグラフィック表示します。	時間枠 1	• バックアップ仕様 • バックアップ仕様のグループ	HTML
[使用メディア] used_media	指定した時間枠内のバックアップ・セッションで使用されたメディアを統計情報とともに表示します。	時間枠 1	• バックアップ仕様 • バックアップ仕様のグループ	すべての形式
[クライアント統計] host_statistics	検索条件に一致するクライアントのリストです。クライアントと、各クライアントのバックアップ・ステータス統計情報を表示します。	時間枠 1	• バックアップ仕様 • バックアップ仕様のグループ • ホスト名	すべての形式
[バックアップ統計情報] backup_statistics	選択した時間枠内のバックアップ・ステータスに関する統計情報を表示します。	時間枠 1	• バックアップ仕様 • バックアップ仕様のグループ	すべての形式
[バックアップ・エラー] backup_errors	バックアップ中に出力されたメッセージを表示します。メッセージはクライアント別に分類されます。	時間枠 1	• バックアップ仕様 • バックアップ仕様のグループ • ホスト名 • メッセージ・レベル	すべての形式

表 9-6 時間枠内のセッションに関するレポート

レポートと omnirpt オプション	説明	必須選択項目	省略可能な選択	サポートされている形式
[使用メディアの拡張レポート] used_media_extended	選択したセッションで使用されたすべてのメディアに関する拡張情報を示します。	時間枠 1	• バックアップ仕様 • バックアップ仕様のグループ	すべての形式

1. メディアをバックアップに使用した時間枠。

相対時間 : 最初のパラメータには時間枠の始点 (レポート開始時点から過去にさかのぼった時間数) を指定し、2 番目のパラメータには時間枠の終点 (始点からの時間数) を指定します。

絶対時間 : 最初のパラメータには時間枠の始点 (日付) を指定し、2 番目のパラメータには時間枠の終点 (日付) を指定します。

単一セッションに関するレポート

以下の表に、Data Protector の単一セッションに関するレポートについて示します。「レポートの形式」(431 ページ) を参照してください。

表 9-7 単一セッションに関するレポート

レポートと omnirpt オプション	説明	必須選択項目	省略可能な選択	サポートされている形式
単一セッション single_session	単一の Data Protector バックアップ・セッションの関連情報をすべて表示します。	セッション ID	メッセージ・レベル	すべての形式
[セッション・オブジェクト] session_objects	選択したセッションに含まれるすべてのバックアップ・オブジェクトを統計情報とともに表示します。	セッション ID	なし	すべての形式

表 9-7 単一セッションに関するレポート

レポートと omnirpt オプション	説明	必須選択項目	省略可能な選択	サポートされている形式
[クライアント当たりのセッション] session_hosts	選択したセッションに含まれる各クライアントに関する情報を示します。[複数のレポートを作成] オプションを使うと、このレポートを複数のレポートに分割してクライアントごとに 1 つずつ作成できます。	セッション ID	メッセージ・レベル	すべての形式
[セッション・デバイス] session_devices	選択したセッションで使用されたすべてのデバイスに関する情報を示します。	セッション ID	なし	すべての形式
[セッション・メディア] session_media	選択したセッションで使用されたすべてのメディアに関する情報を示します。	セッション ID	なし	すべての形式

レポートの形式

Data Protector のレポートはさまざまな形式で作成できます。

レポートを個別に表示する場合は Data Protector Manager に表示されるので、レポート形式を選択する必要はありません。

レポートをレポート・グループにまとめて、特定のイベントの発生時に送信したり、スケジュールを設定したりする場合は、各レポートの形式や受信者を指定する必要があります。

選択可能なレポート形式は、以下のとおりです。

ASCII　テキスト形式でレポートを生成します。

HTML　HTML 形式でレポートを生成します。Web ブラウザを使用して表示する場合に便利です。たとえば、イントラネット上のリンクをクリックし、レポートを表示することによって、システムがバックアップされたかどうかをチェックできます。

重要

Windows Cell Manager 上から電子メールで HTML レポートを送信した場合、そのレポートがどのように表示されるかは、そのメールを開くメール・クライアントに依存します。多くのメール・クライアントは、レポートを ASCII テキスト形式で表示します。レポートを正しく HTML 形式で表示させるには、Web ブラウザで表示してください。

ショート	最も重要な情報だけを短く要約したレポートをテキスト形式で生成します。ブロードキャスト・メッセージに適しています。
タブ	フィールドをタブで区切った形式のレポートを生成します。

ヒント

タブ形式は、レポートを別のアプリケーション (Microsoft Excel など) やスクリプトにインポートして、詳しく分析する場合に適しています。

以下のコマンドを実行すると、過去 24 時間以内に使用されたメディアのリストが Microsoft Excel の表形式で生成されます。

```
omnirpt -report used_media -timeframe 24 24 -log
used_media.xls -tab
```

レポートの送信方法

レポートの送信方法

レポートは、以下に示すさまざまな方法で送信できます。

- 電子メールによる送信
- ブロードキャスト・メッセージによる送信
- SNMP による送信
- 外部スクリプトによる送信
- ログ・ファイルによる送信

以下の項では、各送信方法について詳しく説明します。

電子メールによる送信

電子メール送信機能を使用すると、レポートの出力結果を電子メールで送受信できます。

制限事項

オペレーティング・システムの制限により、異なるロケールを使用する UNIX システム間でローカライズされた電子メール通知 / レポートが送受信された場合、通知 / レポート内の国際文字が正しく表示されない場合があります。

Windows 上で HTML 電子メール・レポートがどのように表示されるかは、電子メール・クライアントの設定に依存します。多くの電子メール・クライアントは、レポートを ASCII テキストで表示します。レポートを正しく HTML 形式で表示させるには、Web ブラウザで表示してください。

Windows における必要条件

Windows システムからレポートの出力結果を電子メールで送信するには、メール・プロファイルがなければなりません。既存のプロファイルを使用するか、Data Protector という名前の新しいメール・プロファイルを作成してください。

既存のメール・プロファイルを使用するには、Data Protector `omnirc` ファイルに次の行を追加してください。

`OB2_MAPIPROFILE=<existing_MAPI_profile_name>`

`omnirc` ファイルの詳細は、「omnirc オプションの使用」（647 ページ) を参照してください。

Data Protector メール・プロファイルの作成

Microsoft Outlook 2002 がインストールされた Windows 2000 システム上で Data Protector という名前の新しいメール・プロファイルを作成するには、以下の手順を実行します。

1. Windowsの [コントロール パネル] の [メール] アイコンをダブルクリックします。

   [メール設定 - Outlook] ダイアログ・ボックスが表示されます。

2. [プロファイル] をクリックします。

   [メール] ダイアログ・ボックスが表示されます。

3. [追加] をクリックします。

   [新しいプロファイル] ダイアログ・ボックスが表示されます。

4. [プロファイル名] テキスト・ボックスに Data Protector と入力し、[OK] をクリックすると、[電子メール・アカウント・ウィザード] が起動されます。

5. [新しい電子メール アカウントの追加] を選択して [次へ] をクリックします。

6. [サーバーの種類] ページで、[Microsoft Exchange Server] を選択し、[次へ] をクリックします。

7. [Exchange Server の設定] ページで、ローカルの Microsoft Exchange Server システムの名前とユーザー名を入力し、[次へ] をクリックします。

8. [完了] をクリックしてウィザードを終了します。

   [メール] ダイアログ・ボックスに、システムに設定されている他のプロファイルとともに Data Protector プロファイルが表示されます。

UNIX システムの場合、特別な構成は必要ありません。

ブロードキャスト・メッセージによる送信

ブロードキャスト・メッセージによる送信では、ブロードキャスト・メッセージ (レポートの出力結果を含む) を指定したシステムに送信します。

ブロードキャスト・メッセージを Windows システムへ送信するには、送信先のシステムを指定する必要があります。ブロードキャスト・メッセージの長さには制限があるため、[ショート] 形式を使用することをお勧めします。レポートの文字数の上限は 1000 文字です。

ログ・ファイルによる送信

ログ・ファイルによる送信では、ログ・ファイル (レポートの出力結果を含む) を指定したファイルに出力します。

ログ・ファイルは、Cell Manager システムへ送信されます。レポートの送信先となるファイルの名前を指定してください。同じ名前のファイルが存在する場合は、既存のファイルが上書きされます。

SNMP による送信

SNMP による送信では、レポートの出力結果を SNMP トラップとして送信することができます。この SNMP トラップは、SNMP トラップをサポートしているアプリケーションで処理することができます。

注記

UNIX Cell Manager では、通知で構成されたシステムに対して SNMP トラップが送信されます。

Windows Cell Manager では、Windows の SNMP トラップの構成で設定されているシステムに SNMP トラップが送信されます。

Windows

以下の手順に従って、Windows の SNMP トラップを構成します。

1. *<Data_Protector_home>*¥binディレクトリからomnisnmp.exeコマンドを実行します。
   システム・レジストリの次の場所に適切な Data Protector エントリが作成されます。
   CurrentControlSet¥Services¥SNMP¥Parameters¥ExtensionAgents
2. Cell Manager 上で [設定] をクリックした後、[ネットワークとダイヤルアップの接続] をクリックします。
3. [高度] メニューの [オプション ネットワーク コンポーネント] を選択

してウィザードを起動します。

4. ウィザードで [管理と監視] ツールを選択し、[次へ] をクリックします。
5. ウィザードの指示に従って、管理ツールと監視ツールをインストールします。
6. [コントロール パネル]、[管理ツール]、[サービス] を順に開きます。
7. [SNMP Service] を右クリックして、[プロパティ] を選択します。
   a. [トラップ] タブを選択します。[コミュニティ名] テキスト・ボックスに public と入力し、[トラップ送信先] テキスト・ボックスに VPO Management Server のホスト名を入力します。
   b. [セキュリティ] タブを選択します。[認証コミュニティ名] の下で public コミュニティ (デフォルト値) を選択し、[編集] をクリックして [コミュニティ権限] を READ CREATE に設定します。
   c. 設定を確認します。
8. omnisnmp を起動します。

外部スクリプトによる送信

外部スクリプトによる送信では、レポートの出力をユーザー独自のスクリプトで処理できます。スクリプトは、出力を標準入力 (STDIN) として受け取ります。スクリプトの処理に推奨される形式はタブ形式です。

スクリプトが Cell Manager システムにある場合は、/opt/omni/lbin ディレクトリ (UNIX システムの場合) または *<Data_Protector_home>*¥bin ディレクトリ (Windows システムの場合) に置く必要があります。この場合スクリプト名のみを指定し、パス全体を指定する必要はありません。

Windows システム上で外部スクリプトに使用できる拡張子は、.bat、.exe、および .cmd のみである点に注意してください。サポート対象外の拡張子 (.vbs など) を持つ外部スクリプトを実行するには、そのスクリプトを開始するバッチ・ファイル (.bat) を作成します。このバッチ・ファイルを外部スクリプトとして実行するよう Data Protector を構成すると、このファイルにより、サポート対象外の拡張子を持つスクリプトが開始されます。

ヒント

指定したメディアの取り出しをスケジュールに基づいて実行する場合にも、この送信方法を使用できます。詳しくは、「スケジュールに基づいたメディアの取り出し」(197 ページ) を参照してください。

Data Protector GUI を使用したレポートの構成

本項では、Data Protector GUI を使って Data Protector レポートを構成する方法について説明します。

注記

レポートの出力に入力パラメータ (選択項目) を表示するには、[レポート] ウィザードで [レポートに選択条件を表示] オプションを選択します。ただしこのオプションは、必須、省略可能ともに入力パラメータ (選択項目) がないレポートでは使用できません。レポートの出力には、デフォルト値が変更された必須パラメータと省略可能パラメータのみが表示されます。

レポート・グループの構成とレポートの追加

レポート・グループ

Data Protector レポートは、個別に (対話形式で) 実行することも、レポート・グループにまとめて、レポート・グループとして開始することもできます。個々のレポートを構成済みのレポート・グループに追加できます。

Data Protector GUI では、レポート・グループで以下を行えます。

- すべてのレポートを同時に (対話形式で) 開始する。
- グループが特定の時間にレポートを開始するようにスケジュールを設定する。
- 通知の際にグループを起動する。

例

以下にレポートの利用例を示します。

- バックアップ・オペレータが、前日の夜間に行われたバックアップのステータスに関する電子メールを受け取る必要がある。
- 特定の部署の管理者が、管轄のシステムのバックアップに関するブロードキャスト・メッセージを受け取る必要がある。
- データをタブで区切ったフル・レポートをログ・ファイルとして送信し、バックアップ統計を記録するアプリケーションで使用する。

管理者はレポート・グループを構成して、上記のそれぞれの要求に対して個別のレポートを追加します。このレポート・グループが早朝に実行されるようスケジュールを設定すると、受信者全員が仕事を開始する前にレポートを受け取れます。

注記

[マウント要求] レポートと [デバイス・エラー] レポートは、対話型レポートとしては使用できず、レポート・グループでのみ使用できます。

以下の手順に従って、レポート・グループを構成します。

1. [Data Protector Manager] で、[レポート] コンテキストを選択します。
2. Scoping ペインの下の [オブジェクト] タブをクリックして、[オブジェクト] を表示します。
3. [レポート] を右クリックして、[レポート・グループの追加] を選択します。[レポート・グループの追加] ウィザードが表示されます。

   ウィザードの指示に従ってください。手順は以下のとおりです。

   a. レポート・グループに名前を付けます。

   b. 必要な場合は、グループの開始時刻のスケジュールを設定します。スケジューラの使用方法の詳細については、「無人バックアップのスケジュール」(269 ページ) を参照してください。

   c. グループ用のレポートを選択して構成します。各レポートごとに、レポート送信時に使用する形式、各レポートの受信者、送信方法を構成します。レポートの種類の詳細については、「レポートの形式」(431 ページ) を参照してください。送信手段の詳細については、「Data Protector 通知」(445 ページ) を参照してください。

重要

Windows Cell Manager 上から電子メールで HTML レポートを送信した場合、そのレポートがどのように表示されるかは、そのメールを開くメール・クライアントに依存します。多くのメール・クライアントは、レポートを ASCII テキスト形式で表示します。レポートを正しく HTML 形式で表示させるには、Web ブラウザで表示してください。

注記

通知によってレポート・グループをトリガするには、まずレポート・グループを構成し、レポート・グループによる送信を行う通知を構成します。

4. レポート・グループが作成され、Scoping ペインに表示されます。
5. グループに複数のレポートを追加するには、グループを右クリックして、[レポートの追加] を選択します。

Data Protector GUI を使用したレポートおよびレポート・グループの実行

Data Protector のレポートは、個別に実行することも、レポート・グループとしてまとめて実行することもできます。

個別レポートの実行

各レポートを個別に実行するには、以下の手順を行います。

1. [Data Protector Manager] で、[レポート] コンテキストを選択します。
2. Scoping ペインの下の [タスク] タブをクリックして、[タスク]コンテキストを選択します。表示されたレポートをブラウズして、目的のレポートを選択します。
3. [レポート] ウィザードに従って、レポートを構成して実行します。

レポート・グループの実行

構成済みのレポート・グループを実行するには、以下の手順を行います。

1. [Data Protector Manager] で、[レポート] コンテキストを選択します。
2. Scoping ペインで、レポート・グループのリストをブラウズし、目的のレポート・グループを右クリックして、[開始] をクリックします。
3. [はい] をクリックして処理を実行します。

コマンド行インタフェースを使用したレポートおよびレポート・グループの実行

Data Protector のレポートは、コマンド行インタフェースを使って作成できます。コマンド行インタフェースを使って、使用中の別の構成スクリプトに Data Protector のレポートを挿入できます。また、コマンド行インタフェースから、個別のレポート作成、レポート・グループの実行、レポート形式や送信方法の定義を行えます。

レポートを作成するには omnirpt コマンドを使用します。このコマンドの詳細については omnirpt の man ページを参照してください。

omnirpt の使用例を以下に示します。

```
omnirpt -rptgroup <ReportGroup>
```

<ReportGroup> という名前のレポート・グループを実行します。

注記

Data Protector コマンド行インタフェースを使ってレポート・グループを実行する前に、まず Data Protector GUI または Web レポート・インタフェースを使ってレポート・グループを構成する必要があります。

```
omnirpt -report host -host <Hostname> -html
```

<HostName> で指定したシステムのクライアント・バックアップ・レポートが HTML 形式で作成されます。

重要

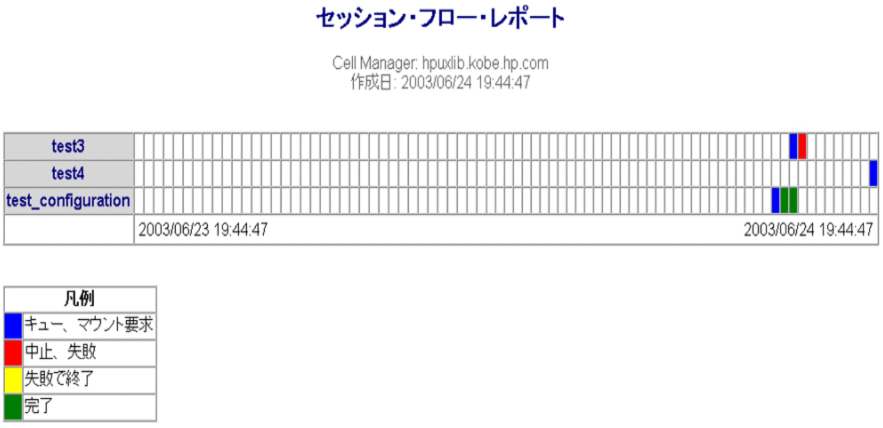
Windows Cell Manager 上から電子メールで HTML レポートを送信した場合、そのレポートがどのように表示されるかは、そのメールを開くメール・クライアントに依存します。多くのメール・クライアントは、レポートを ASCII テキスト形式で表示します。レポートを正しく HTML 形式で表示させるには、Web ブラウザで表示してください。

例 1

以下のコマンドにより、過去 24 時間以内のセッション・フロー・レポートが作成され、図 9-3 (443 ページ) に示すとおり HTML 形式のファイルに記録されます。

```
omnirpt -report session_flow -timeframe 24 24 -log
session_flow.html -html
```

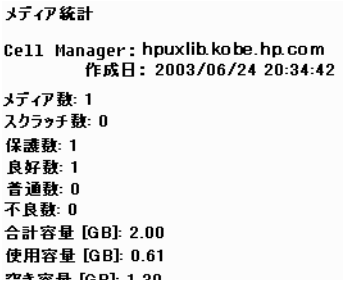
図 9-3 **セッション・フロー・レポート**



例 2 以下のコマンドにより、[不良] 状態にあるメディアのメディア統計レポートが作成され、図 9-4 (443 ページ) に示すとおり ASCII 形式のファイルに記録されます。

```
omnirpt -report media_statistics -status poor -log
media_statistics.txt -ascii
```

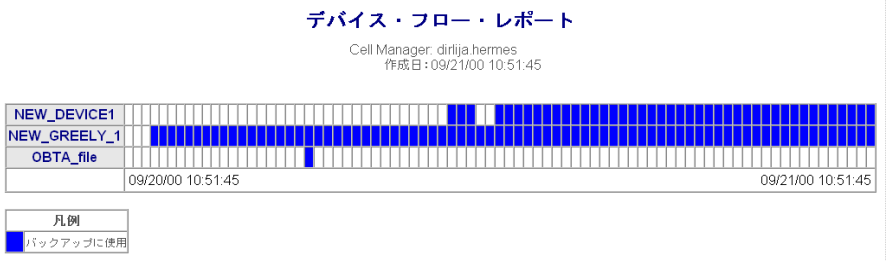
図 9-4 **メディア統計レポート**



例 3 以下のコマンドにより、過去 24 時間以内のデバイス・フロー・レポートが作成され、図 9-5 (444 ページ) に示すとおり HTML 形式の電子メールで送信されます。

```
omnirpt -report device_flow -timeframe 24 24 -email
ulmo@outersea.ea -html
```

図 9-5 デバイス・フロー・レポート



Data Protector 通知

通知とは

Data Protector の通知機能を使用すると、特定のイベントの発生時に通知を受信できます。たとえば、バックアップ・セッション完了時に、セッションのステータスに関する電子メールを受信できます。

通知の際にレポートがトリガされるよう設定できます。Data Protector のレポートに関する詳細は、「Data Protector レポート」（417 ページ) を参照してください。

注記

Data Protector の通知機能にアクセスできるのは、Admin グループに所属する Data Protector ユーザー、およびレポート、通知、イベント・ログのユーザー権限を付与された Data Protector ユーザーだけです。Data Protector のユーザーとユーザー・グループの詳細は、「ユーザーとユーザー・グループの 構成」（135 ページ) を参照してください。

通知の構成

通知は、Data Protector のユーザー・インタフェースまたは Java 対応の任意の Web ブラウザで構成できます。

通知は、入力パラメータを構成することによってカスタマイズできます。

どの通知にも共通する入力パラメータを以下に示します。

- [名前] - 通知の名前。
- [メッセージ・レベル] - デフォルト値は通知の種類によって異なります。各通知のデフォルト値を下表に示します。
- [送信方法] - デフォルト値は Data Protector イベント・ログ。

通知の種類

通知は、以下の 2 種類に大別できます。

- イベントの発生時にトリガされる通知 :
  - [警告]
  - [バックアップ・エラー]

— デバイス・エラー

— [セッションの最後]

— [IDB の破損]

— [メールスロット満量]

— マウント要求

- Data Protectorのチェック/保守機構によりスケジュール設定および開始される通知 :

— [健全性チェックの失敗]

— [IDB の削除必要]

— [IDB のスペース不足]

— [IDB テーブル・スペースのスペース不足]

— [ライセンス警告]

— [ライセンス期限切れ]

— [フリー・メディア不足]

— [予期しないイベント]

— [ユーザー・チェックの失敗]

Data Protector のチェックと保守機構の詳細は、「Data Protector のチェック / 保守機構」（757 ページ) を参照してください。

表 9-8 Data Protector 通知

名前	省略可能な入力パラメータ	デフォルトのメッセージ・レベルおよび省略可能な入力パラメータのデフォルト値	表示されるメッセージ
[IDB の破損]	なし	• [致命的]	内部データベースの *<DB_part>* 部分に損傷が見つかりました *<error_message>*。

表 9-8 Data Protector 通知

名前	省略可能な入力パラメータ	デフォルトのメッセージ・レベルおよび省略可能な入力パラメータのデフォルト値	表示されるメッセージ
[バックアップ・エラー]	[シングル・メッセージ・レベル] (< 任意 >、[警告]、[軽度]、[重度]、[致命的]、[正常]) — 指定したレベル以上の Data Protector メッセージだけがこの通知をトリガします。	• [重度] • [重度]	バックアップ仕様 *<backup_spec>* のバックアップ・セッション *<session_ID>* にエラーがあります : *<number_of_errors>*
[予期しないイベント]	[イベント数] (この通知をトリガする Data Protector イベント・ログ内のイベント数のしきい値)	• [警告] • 20	昨日 *<Number of Events>* 個の予期しないイベントが発生したため、Data Protector イベント・ログが増大しました。
[健全性チェックの失敗]	なし	[致命的]	健全性チェック・メッセージ : *<healthcheck_command>* が失敗しました。HealthCheck.log ファイルを確認してください。
[ユーザー・チェックの失敗]	[コマンド・パス]	• [重度] • なし	ユーザー・チェックが失敗しました。終了コード : *<error_code>*:*<error_description>*
[セッションの最後]	• [データリスト] • [セッション・ステータス]	• [警告] • [すべて] • [完了しましたが、エラーが発生しています]	バックアップ仕様 *<Datalist>* のセッション *<session_ID>* が包括的なステータス *<Session Status>* で終了しました。
デバイス・エラー	[デバイス]	• [致命的] • < *任意* >	デバイス *<Device>* にエラーが発生しました。

表 9-8 Data Protector 通知

名前	省略可能な入力パラメータ	デフォルトのメッセージ・レベルおよび省略可能な入力パラメータのデフォルト値	表示されるメッセージ
[IDB のスペース不足]	• [filenames.dat の最大サイズ] (MB) • [内部データベース用に使用可能なディスク・スペース] (MB) • [DCBF のサイズ制限] (MB)	• [重度] • 250 MB • 50 MB • 250 MB	内部データベースのスペースが不足しています。
[IDB テーブル・スペースのスペース不足]	[テーブルスペース使用率のしきい値] (%)	• [重度] • 85%	テーブルスペース *<Tablespace_name>* が不足しています。
[IDB の削除必要]	• [最終削除日からの日数] (単位 : 日) • [ファイル名数の推定値] (単位 :100 万) • [推定削除時刻] (単位 : 分) • [ファイル名数] (単位 :100 万)	• [警告] • 180 日 • 600 万 • 120 分 • 1 億	内部データベースに対して、ファイル名の削除を実行する必要があります
[マウント要求]	[デバイス]	• [警告] • *< 任意 >*	デバイス *<Device>* に対するマウント要求

表 9-8 Data Protector 通知

名前	省略可能な入力パラメータ	デフォルトのメッセージ・レベルおよび省略可能な入力パラメータのデフォルト値	表示されるメッセージ
[フリー・メディア不足]	• [メディア・プール] • [フリー・メディア数] (この通知をトリガするフリー・メディアの最小数のしきい値)	• [警告] • < *任意* > • 2	メディア・プール *<Media Pool>* には *<number_of_media>* フリー・メディアしかありません。
[メールスロット満量]	• [デバイス]	• [警告] • < *任意* >	ライブラリ *<Device>* のすべてのメールスロットがいっぱいです。直ちにメディアを取り出してください。
[ライセンス警告]	なし	• [警告]	*<name of the license>* というカテゴリのライセンスを *<n>* 個購入する必要があります。詳細は、`omnicc -check_licenses -detail` を実行して確認してください。
[ライセンス期限切れ]	[ライセンスの有効期限]	• [警告] • 10	最初に取得したライセンスはあと *<License expires in days>* 日で期限切れになります。
[警告]	なし	• [警告]	警告 : *<Alarm_message>*

通知に関する説明

[警告] [警告] 通知は、Data Protector の内部の状態によってトリガされた Data Protector の重要なメッセージを表示します。

[IDB の削除必要] デフォルトでは、Data Protector はチェック / 保守機構の一環として 1 日 1 回 IDB の削除が必要かどうかをチェックし、以下の条件が成立した場合に通知をトリガします。

- セル内のいずれかの Data Protector クライアントで、前回 IDB からファイル名を削除した時点からの経過日数が *<最終削除日からの日数>* 入力パラメータ (単位 : 日) の値を超過し、なおかつ以下の内少なくとも 1 つの条件が成立した場合。
  - 削除の対象となるファイル名レコードの数が *<ファイル名数の推定値>* 入力パラメータ (単位 :100 万) の値より大きい。
  - 削除を完了するまでに *<推定削除時刻>* 秒以上の時間が必要と推測される。
- IDB内のファイル名の数が *<ファイル名数>* 入力パラメータ (単位:100万) の値を超えている場合。

Data Protector のチェックと保守機構の詳細は、「Data Protector のチェック / 保守機構」（757 ページ) を参照してください。

[IDB のスペース不足] デフォルトでは、Data Protector は 1 日 1 回 IDB のスペースが不足していないかをチェックし、CDB 拡張ファイル用に割り当てられたスペースが不足したり、IDB が所属するディスクのディスク・スペースが不足したり、またはすべての DC ディレクトリ用に割り当てられたスペースが不足する場合に通知をトリガします。つまり、以下のいずれかの条件が成立した場合に通知がトリガされます。

- **すべての**CDB拡張ファイルの最大サイズ (全CDB拡張ファイルの最大サイズの合計) とすべての CDB 拡張ファイルの現在のサイズの差が、*<filenames.dat の最大サイズ (単位 :MB)>* 入力パラメータの設定値未満になった場合。
- IDB が所属する**任意の**ディスクで、使用可能なディスク・スペースが *<内部データベース用に使用可能なディスク・スペース (単位 :MB)>* 入力パラメータの設定値未満になった場合。
- **すべての**DCディレクトリの最大サイズとすべてのDCディレクトリの現在のサイズの差が、*<DCBF のサイズ制限 (単位 :MB)>* 入力パラメータの設定値未満になった場合。

Data Protector のチェックと保守機構の詳細は、「Data Protector のチェック / 保守機構」（757 ページ) を参照してください。

[IDB テーブル・スペースのスペース不足] デフォルトでは、Data Protector はチェック / 保守機構の一環として 1 日 1 回 IDB のテーブルスペースが不足してないかをチェックし、いずれかのテーブルスペースに割り当てられ

たスペースが不足している場合に通知をトリガします。デフォルトでは、割り当てられたスペースの 85% が使用されたときにこの通知をトリガします。

[健全性チェックの失敗] Data Protector はチェック / 保守機構の一環として、デフォルトでは 1 日 1 回健全性のチェックを行います。健全性のチェックでは、omnihealthcheck コマンドが起動され、omnihealthcheck コマンドが失敗した場合に通知がトリガされます。omnihealthcheck コマンドの詳細については、omnihealthcheck の man ページを参照してください。omnihealthcheck コマンドは、以下についてチェックします。

- Data Protector サービス (rds、crs、mmd、omnitrig、および OmniInet) がアクティブになっているか。
- メディア管理データベースの整合性が維持されているかどうか。
- IDBのバックアップが1つ以上存在するか。終了コードが0以外の場合は、失敗したチェックがあるということを示します。

このコマンドの終了コードが 0 (OK) になるのは、上の 3 つのチェックがすべて正しく終了している場合だけです (つまり、すべてのチェックの終了コードが 0 になった場合)。終了コードが 0 以外の場合は、チェックに失敗したことを意味します。終了コードの詳細については、omnihealthcheckman ページを参照してください。

[ユーザー・チェックの失敗] デフォルトでは、Data Protector は 1 日 1 回ユーザー・チェックを行います。ユーザー・チェックでは、*<script/command pathname>* 入力パラメータとして指定されているスクリプトまたはコマンドが実行されます。HP-UX の場合は /opt/omni/lbin ディレクトリ、Windows の場合はアプリケーション・システムの *<Data_Protector_home>*¥bin ディレクトリでスクリプト / コマンドを作成して、ここにファイル名を入力します。スクリプト / コマンドが 0 以外の値を返して終了した場合に通知がトリガされます。

[ユーザー・チェックの失敗] 通知の詳細については、「[ユーザー・チェックの失敗] 通知」(758 ページ) を参照してください。

[セッションの起動] この通知は、< *データリスト* > 入力パラメータに指定されたバックアップ仕様の Data Protector セッションが、< *セッション・ステータス* > 入力パラメータに指定されたステータスで開始した場合にトリ

ガされます。デフォルト値は [バックアップ仕様 *<Datalist>*、バックアップ・グループ *<BackupGroup>* のセッション *<Session_ID>* が開始されました。] です。

[セッションの完了] この通知は、*< データリスト >* 入力パラメータに指定されたバックアップ仕様の Data Protector セッションが、*< セッション・ステータス >* 入力パラメータに指定されたステータスで終了した場合にトリガされます。デフォルト値は [完了しましたが、エラーが発生しています。] です。

通知の送信方法

通知は、以下に示すさまざまな方法で送信できます。

- 電子メールによる送信
- ブロードキャスト・メッセージによる送信
- SNMP による送信
- 外部スクリプトによる送信
- ログ・ファイルによる送信
- レポート・グループによる送信
- Data Protector イベント・ログによる送信

注記

デフォルトでは、すべての通知が Data Protector イベント・ログに送信されるように構成されています。他の送信方法でも通知を送信したい場合は、通知の構成を追加する必要があります。

電子メールによる送信

指定したイベントの発生時に、希望する情報を電子メールで受信できます。

Windows における必要条件

Windows システムから電子メール通知を送信するには、メール・プロファイルがなければなりません。既存のプロファイルを使用するか、Data Protector という名前の新しいメール・プロファイルを作成してください。

既存のメール・プロファイルを使用するには、Data Protector `omnirc` ファイルに次の行を追加してください。

OB2_MAPIPROFILE=*<existing_MAPI_profile_name>*

omnirc ファイルの詳細は、「omnirc オプションの使用」（647 ページ）を参照してください。

Data Protector メール・プロファイルの作成

Microsoft Outlook 2002 がインストールされた Windows 2000 システム上で Data Protector という名前の新しいメール・プロファイルを作成するには、以下の手順を実行します。

1. Windowsの [コントロール パネル] の [メール] アイコンをダブルクリックします。

   [メール設定 － Outlook] ダイアログ・ボックスが表示されます。

2. [プロファイル] をクリックします。

   [メール] ダイアログ・ボックスが表示されます。

3. [追加] をクリックします。

   [新しいプロファイル] ダイアログ・ボックスが表示されます。

4. [プロファイル名] テキスト・ボックスに Data Protector と入力し、[OK] をクリックすると、[電子メール・アカウント・ウィザード] が起動されます。

5. [新しい電子メール アカウントの追加] を選択して [次へ] をクリックします。

6. [サーバーの種類] ページで、[Microsoft Exchange Server] を選択し、[次へ] をクリックします。

7. [Exchange Server の設定] ページで、ローカルの Microsoft Exchange Server システムの名前とユーザー名を入力し、[次へ] をクリックします。

8. [完了] をクリックしてウィザードを終了します。

   [メール] ダイアログ・ボックスに、システムに設定されている他のプロファイルとともに Data Protector プロファイルが表示されます。

UNIX システムの場合、特別な構成は必要ありません。

ブロードキャスト・メッセージによる送信

ブロードキャスト・メッセージによる通知では、指定したイベントが発生した時にシステムにブロードキャスト・メッセージを送信できます。

ブロードキャスト・メッセージを Windows システムへ送信するには、送信先のシステムを指定する必要があります。ブロードキャスト・メッセージの長さには制限があるため、[ショート] 形式を使用することをお勧めします。レポートの文字数の上限は 1000 文字です。

ログ・ファイルによる送信

指定したイベントの発生時に、希望する情報をログ・ファイルとして送信できます。

ログ・ファイルは、Cell Manager システムへ送信されます。レポートの送信先となるファイルの名前を指定してください。

SNMP による送信

指定したイベントの発生時に、希望する情報を SNMP トラップとして送信できます。この SNMP トラップは、SNMP トラップをサポートしているアプリケーションで処理することができます。

注記

UNIX Cell Manager では、通知で構成されたシステムに対して SNMP トラップが送信されます。

Windows Cell Manager では、Windows の SNMP トラップの構成で設定されているシステムに SNMP トラップが送信されます。

Windows

以下の手順に従って、Windows の SNMP トラップを構成します。

1. Cell Manager 上で [設定] を開いた後、[ネットワークとダイヤルアップの接続] を開きます。
2. [高度] メニューの [オプション ネットワーク コンポーネント] を選択してウィザードを起動します。
3. ウィザードで [管理と監視] ツールを選択し、[次へ] をクリックします。
4. ウィザードの指示に従って、管理ツールと監視ツールをインストールします。
5. [コントロール パネル]、[管理ツール]、[サービス] を開きます。
6. [SNMP Service] を右クリックして、[プロパティ] を選択します。

a. [トラップ] タブを選択します。[コミュニティ名] テキスト・ボックスに public と入力し、[トラップ送信先] テキスト・ボックスに VPO Management Server のホスト名を入力します。

b. [セキュリティ] タブを選択します。[認証コミュニティ名] の下で public コミュニティ (デフォルト値) を選択し、[編集] をクリックして [コミュニティ権限] を READ CREATE に設定します。

c. 設定を確認します。

7. omnisnmp を起動します。

外部スクリプトによる送信

レポートの出力をユーザー独自のスクリプトで処理できます。スクリプトは、出力を標準入力 (STDIN) として受け取ります。スクリプトの処理に推奨される形式はタブ形式です。

スクリプトが Cell Manager 上にある場合は、/opt/omni/lbin ディレクトリ (HP-UX または Solaris システムの場合) または *<Data_Protector_home>*¥bin ディレクトリ (Windows システムの場合) に置く必要があります。この場合スクリプト名のみを指定し、パス全体を指定する必要はありません。

Windows システム上で外部スクリプトに使用できる拡張子は、.bat、.exe、および .cmd のみである点に注意してください。サポート対象外の拡張子 (.vbs など) を持つ外部スクリプトを実行するには、そのスクリプトを開始するバッチ・ファイル (.bat) を作成します。このバッチ・ファイルを外部スクリプトとして実行するよう Data Protector を構成すると、このファイルにより、サポート対象外の拡張子を持つスクリプトが開始されます。

ヒント

指定したメディアの取り出しをスケジュールに基づいて実行する場合にも、この送信方法を使用できます。詳しくは、「スケジュールに基づいたメディアの取り出し」(197 ページ) を参照してください。

レポート・グループによる送信

レポート・グループによる通知では、指定したイベントの発生時にレポート・グループを開始します。レポート・グループの詳細については、「Data Protector GUI を使用したレポートの構成」（438 ページ）を参照してください。

Data Protector イベント・ログによる送信

デフォルトでは、すべての通知が Data Protector イベント・ログに送信されます。Data Protector イベント・ログにアクセスできるユーザーは、Admin グループに所属している Data Protector ユーザーか、またはレポート、通知、およびイベント・ログ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。Data Protector イベント・ログに書き込まれているイベントは、いずれも表示と削除が可能です。詳しくは、「Data Protector イベント・ログ」（461 ページ）を参照してください。

通知の構成

以下の手順に従って、通知を構成します。

1. [Data Protector Manager] で、[レポート] コンテキストを選択します。
2. Scoping ペインの下の [オブジェクト] タブをクリックして、[オブジェクト] を表示します。
3. [通知] を右クリックして、[通知の追加] を選択します。[通知の追加] ウィザードが表示されます。ウィザードの指示に従ってください。

ヒント

通知によってレポート・グループをトリガするには、レポート・グループを構成し、レポート・グループによる送信を行うよう通知を構成します。

4. 通知が作成され、Scoping ペインに表示されます。

Web レポートおよび Web 通知の構成

Web ブラウザを使って Data Protector レポートおよび通知を表示できます。

Web レポート / 通知インタフェースを使用すると、ネットワーク上のすべてのシステムから Data Protector レポート / 通知を表示、構成、開始できます。Web レポート / 通知インタフェースを使用することによって、さまざまな方法や形式で送信されたレポートや通知を構成できるようになります。

Data Protector GUI からアクセスできるすべてのレポート / 通知機能へは、Data Protector Web レポート / 通知からもアクセスできます。制限事項については以下を参照してください。

Cell Manager のインストール時には、java という名前の Web レポート・ユーザーが自動的に作成されます。デフォルトでは、パスワードなしで Data Protector Web レポート / 通知機能を使用できます。Data Protector Web ユーザーのパスワードを構成すると、Web レポート / 通知機能へのアクセスを制限できます。

必要条件

- システムに Java VM(バージョン 1.1 以降) がインストールされており、Web ブラウザで有効になっている必要があります。

制限事項

Data Protector Web レポート / 通知インタフェースの制限事項は以下のとおりです。

- サポートされているブラウザは、Netscape Navigator 4.7.x、Netscape 7.x、サービス・パック 1 以降が適用された Microsoft Internet Explorer 5.0 です。
- Web レポート / 通知インタフェースでは、保存済みのレポートを編集、表示、または削除できません。
- Web レポート / 通知インタフェースでは、レポート・グループを起動できません。
- Webレポート/通知インタフェースに複数の入力パラメータ(選択項目)を**入力する**場合、スペースが含まれている各パラメータ (選択項目) を必ず二重引用符で囲む必要があります。

以下の手順に従って、Data Protector Web レポートおよび通知を使用します。

1. システムで Web サーバを構成して実行します。Data Protector は一般的なすべての Web サーバに対応しています。
2. Data Protector Java プログラムを Web サーバにコピーします。コピー先のシステムは Data Protector クライアントでなくても構いません。手順は以下の項で説明します。
3. 必要な場合は、パスワードを構成して Web レポートへのアクセスを制限します。手順は以下の項で説明します。

Web サーバに Data Protector Java プログラムをコピーする

すべてのシステムのブラウザから Data Protector の Web レポート / 通知インタフェースへのアクセスを可能にするには、Data Protector の Java レポート・プログラムを Web サーバにコピーする必要があります。

Data Protector ユーザー・インタフェースがインストールされたシステムから、以下のディレクトリとそのサブディレクトリをすべてコピーします。

- Windows の場合 : `<Data_Protector_home>¥java`
- UNIX の場合 : `/opt/omni/java`

コピーした `java` フォルダから `¥bin¥WebReporting.html` (Windows システムの場合)、または `/bin/webreporting.html` ファイル (UNIX システムの場合) にアクセスして、Data Protector レポートをブラウザに表示します。このファイルを完全な URL 形式で記述し、Web レポートのユーザーが使用できるようにします。たとえば、イントラネット・サイトからこのファイルへのリンクを設定します。

Web レポートへのアクセスを制限する

Cell Manager のインストール時には、`java` という名前の Web レポート / 通知ユーザーが自動的に作成されます。デフォルトでは、パスワードなしで Data Protector Web レポート / 通知機能を使用できます。Data Protector Web ユーザーのパスワードを構成すると、Web レポート / 通知機能へのアクセスを制限できます。Web レポート / 通知を使用するすべてのユーザーは、Web 上で Data Protector のレポートを表示する際にこのパスワードを入力する必要があります。

Data Protector Web レポート / 通知インタフェースに対するパスワードを変更するには、以下の手順を行います。

1. ［Data Protector Manager］で［ユーザー］コンテキストを選択します。
2. ［アクション］、[Web ユーザー・パスワードの設定］の順に選択します。パスワードを変更するためのダイアログ・ボックスが表示されます。

   パスワードを設定すると、Web レポート / 通知インタフェースを使用するすべてのユーザーは、Web 上で Data Protector のレポートをブラウズする際にパスワードの入力が必要になります。

レポートを作成する

Data Protector の Web レポート / 通知インタフェースを使ってレポートを作成するには、このインタフェースにアクセスする必要があります。実際の手順は構成によって異なりますが、Cell Manager へのログオン後、さまざまな種類のレポートを作成できます。レポートの種類の詳細は、「Data Protector レポート」（417 ページ) を参照してください。

レポートを表示するには、レポートをクリックして必要な情報を入力します。

表示されたレポートは、印刷したり保存できます。レポートを保存する際に、既存または新規のレポート・グループへ追加することもできます。詳細については、次項を参照してください。

通知の構成

Data Protector の Web レポート / 通知インタフェースを使って通知を構成するには、このインタフェースにアクセスする必要があります。実際の手順は構成によって異なりますが、Cell Manager へのログオン後、さまざまな種類の通知を構成できます。通知の詳細は、「Data Protector 通知」（445 ページ) を参照してください。

通知を構成するには、［通知］を選択して［通知の追加］をクリックします。必要な情報を入力して通知を保存します。

レポート・グループを構成する

レポート・グループ

レポート・グループの詳細については、「レポート・グループの構成とレポートの追加」（438 ページ) を参照してください。

Web レポート / 通知インタフェースでレポートを保存する際に、新規のレポート・グループを作成できます。

1. 作成するレポートを選択します。
2. 必要な情報を入力します。
3. レポートが表示されたら、[保存] をクリックします。レポート名と、レポートの追加先のレポート・グループ (新規または既存) を入力します。

Data Protector イベント・ログ

Data Protector イベント・ログにより、Data Protector の操作中に発生した特定のイベントを集中管理できます。イベントは、*<Data_Protector_home>*¥log¥server¥Ob2EventLog.txt ファイル (Windows Cell Manager の場合) または /var/opt/omni/server/log/Ob2EventLog.txt ファイル (UNIX Cell Manager の場合) に記録されます。Data Protector イベント・ログは、Data Protector GUI を使って表示でき、問題発生時のトラブルシューティングに役立てることができます。

イベントは通知機能によって記録されます。通知の詳細については、「Data Protector 通知」（445 ページ) を参照してください。

注記

Data Protector イベント・ログ機能にアクセスできるのは、Admin グループに所属する Data Protector ユーザー、およびレポート、通知、イベント・ログのユーザー権限を付与された Data Protector ユーザーだけです。

イベント・ログ

イベント・ログ・ビューアにアクセスするには、Data Protector GUI の [レポート] コンテキストを選択して [レポート] を展開します。[イベント・ログ] を選択してイベントを表示します。

注記

Data Protector イベント・ログは自動的には更新されません。新しいメッセージを表示したい場合は、[F5] キーを押して更新してください。

イベント・ログ・ビューアの表示内容を削除する

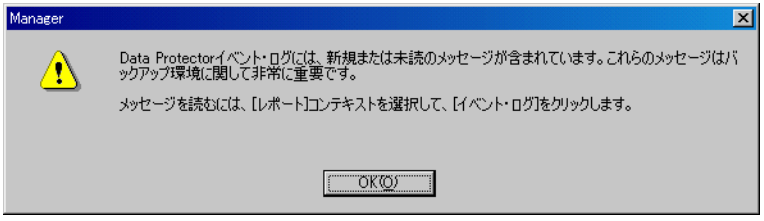
[イベント・ログ] を右クリックして [イベント・ログを空にする] を選択します。[イベント・ログ] 内のすべてのエントリが削除されます。

注記

イベント・ログ・ビューアの表示内容を削除しても、*<Data_Protector_home>*¥log¥server¥Ob2EventLog.txt ファイル（Windows Cell Manager の場合）、または /var/opt/omni/server/log/Ob2EventLog.txt ファイル（UNIX Cell Manager の場合）は削除されません。

Data Protector GUI を起動したとき、Data Protector イベント・ログに新しい通知が書き込まれている場合は、次のメッセージが表示されます。

図 9-6 イベント・ログのメッセージ



10 Manager-of-Managers 環境

本章の概略

本章では、Data Protector Manager-of-Managers の構成方法と使用方法について説明します。Data Protector Manager-of-Managers はエンタープライズ・バックアップ環境の管理に使用します。本章は以下の各項で構成されています。

注記

MoM には、専用の Data Protector ライセンスが必要です。詳しくは、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

Manager-of-Managers

Data Protector の Manager-of-Managers (MoM) を使用して、管理者は複数の Data Protector セル (MoM クライアントとも呼ばれます) で構成される大規模な環境を 1 箇所から集中管理できます。エンタープライズ環境の詳細は、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

注記

各 MoM クライアントと MoM Manager は、同一バージョンの Data Protector を実行することが必要です。

Data Protector MoM では、エンタープライズの規模の拡大に伴ってバックアップ環境を柔軟に拡張できます。MoM は以下の機能を備えています。

全タスクの集中管理

エンタープライズ環境の構成、管理、制御を 1 箇所から行えます。つまり、環境全体に対するバックアップの構成、メディア管理、復元、モニター、ステータスのレポートなどを行えます。

メディア集中管理データベース

必要に応じて、環境内のすべてのセルは、中央の共通データベースを共有することによりエンタープライズ内のデバイスやメディアを管理できます。メディア集中管理データベース (CMMDB) を使用すると、セル間でハイエンド・デバイスを共有できます。これは、あるセル内の CMMDB を使用する任意のデバイスが、CMMDB を使用するすべてのセルにアクセスできることを意味します。

ライセンス集中管理

Data Protector では MoM 環境全体に対してライセンス集中管理を構成できます。これにより、すべての Data Protector ライセンスを MoM Manager システムにインストールして保持し、必要に応じて特定のセルに割り当てることができます。

Manager-of-Managers の構成

MoM 環境を構成するには、以下の手順を行います。

1. MoM Manager を設定する。「MoM Manager の設定」(467 ページ) を参照してください。
2. Data Protector セルを MoM 環境にインポートする。「セルのインポート」(468 ページ) を参照してください。
3. 環境内のすべてのセルの admin ユーザー・グループに Data Protector ユーザー (MoM 管理者) を作成する。「MoM 管理者の追加」(468 ページ) を参照してください。
4. Data Protector サービスを再起動する。「Data Protector サービスの再起動」(469 ページ) を参照してください。

必要に応じて、以下の構成も行えます。

- メディア集中管理データベースを構成する。「メディア集中管理データベースの構成」(473 ページ) を参照してください。
- ライセンス集中管理を構成する。「ライセンス集中管理」(477 ページ) を参照してください。
- MoM 構成を配布する。「MoM 構成の配布」(483 ページ) を参照してください。

必要条件

以下のガイドラインに従って、MoM Manager として構成するシステムを選択します。

- MoM Manager システムの信頼性が高いこと
- ソフトウェアがインストールされた Data Protector Cell Manager システムであること。Data Protector Cell Manager システムの構成方法の詳細は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

MoM セルと、MoM クライアント・セルになると予想されるすべてのセルに必要なライセンスをインストールします。

MoM Manager の設定

エンタープライズ環境を設定するには、Cell Manager の 1 つを Manager-of-Managers として構成します。

1. [Data Protector Manager] のコンテキスト・リストから [クライアント] をクリックします。
2. [アクション] メニューで、[CM を Manager-of-Managers サーバとして構成] をクリックします。
3. Data Protector サービスを終了して再起動します。「Data Protector サービスの再起動」（469 ページ) を参照してください。
4. MoM の GUI (グラフィカル・ユーザー・インタフェース) を実行します。
   - Windows プラットフォームの場合は、以下のいずれかを実行してください。
     - Windows タスクバーの［スタート］をクリックし、［HP OpenView Storage Data Protector］プログラム・グループの［Manager-of-Managers］をクリックして、Data Protector のすべての機能を使用できる MoM GUI を起動します。
     - mom コマンドを使用して、Data Protector のすべての機能を使用できる GUI を起動します。

       このコマンドにコンテキスト固有オプションを指定して実行することにより、1 つまたは複数の Data Protector コンテキストを起動できます。次にコマンドの例を示します。

       ```
       mom -backup -restore
       ```

       Data Protector の [モニター] コンテキストに加えて、［バックアップ］および［復元］コンテキストが起動されます。

       接続先の Cell Manager を指定するには、以下のコマンドを使用します。`mom -server <Cell Manager_name>`
   - UNIX の場合 : `/opt/omni/bin/xomnimom` コマンドを実行して、すべての Data Protector コンテキストが有効化された状態の Data Protector Manager-of-Managers GUI を起動します ([内部データベース] コンテキストと [デバイス / メディア] コンテキストは除く)。コンテキスト・オプションを付加してコマンドを実行すると、指定した Data Protector コンテキストだけが起動されます。

上記コマンドの詳細については、omnigui の man ページを参照してください。

セルのインポート

MoM Manager を構成したら、Data Protector セルを MoM 環境に追加 (インポート) します。Data Protector セルを MoM 環境に追加するには、以下の手順を行います。

1. [Data Protector Manager-of-Managers] のコンテキスト・リストから [クライアント] をクリックします。
2. [エンタープライズ・クライアント] を右クリックし、[Cell Manager のインポート] をクリックします。

重要

Cell Manager を MoM にエンタープライズ・クライアントとしてインポートするには、その Cell Manager 上の admin ユーザーグループに所属するユーザーでなければなりません。そうでない場合、インポートは失敗します。

3. インポートしたい Cell Manager を入力またはブラウズして選択し、[完了] をクリックします。これで、選択した Cell Manager が MoM 環境の一部となります。

注記

クラスターにインストールされた Cell Manager を MoM セルに追加する場合は、必ず**仮想サーバ名**を入力してください。

MoM 管理者の追加

MoM 管理者は、エンタープライズ環境内のすべてのセルで管理作業を実行できます。

管理用のユーザーは、MoM 環境内のすべての Cell Manager の admin ユーザーグループに所属している必要があります。たとえば、*MoM_Admin* というユーザーなどです。このユーザーが MoM 管理者となります。

1. Data Protector Manager を使用して、MoM 環境内の各 Cell Manager に Admin ユーザーグループのメンバーとして接続します（[ユーザーの構

成] ユーザー権限が必要です)。

2. MoM管理者となるユーザーをData ProtectorのAdminユーザーグループに追加します。

ユーザーの追加方法は、「ユーザーの追加または削除」(144 ページ) を参照してください。

Data Protector サービスの再起動

MoM 環境の構成が完了すると、Data Protector サービスの再起動を要求するメッセージが表示されます。

Windows Service Control Manager を使って Cell Manager 上のサービスの起動と終了を行った場合は、現在と前回のデータベース・ログのコピーだけが保存されます。omnisv -stop および omnisv -start コマンドを使用すれば、これまでのデータベース・ログがすべて保存されます。

1. 以下のコマンドを入力して、すべての Data Protector サービスを終了します。
   - Windows の場合 : *<Data_Protector_home>*¥bin¥omnisv -stop
   - UNIX の場合 : /opt/omni/sbin/omnisv -stop

注記

omnisv コマンドは、クラスター環境ではサポートされていません。

MC/ServiceGuard

Cell Manager が MC/SG 上に構成されている場合は、以下のコマンドを使用して Data Protector パッケージを停止します。

cmhaltpkg *<pkg_name>* 。ここで、*<pkg_name>* は Data Protector クラスターパッケージの名前を示します。

このコマンドによって Data Protector パッケージは停止され、Data Protector 共有ボリューム・グループがアンマウントされます。

Microsoft Cluster Server

Cell Manager が Microsoft Cluster Server 上に構成されている場合は、アクティブなノード上でクラスター・アドミニストレータユーティリティを使用して、OBVS_VELOCIS クラスター・グループをオフラインにします。

2. 以下のコマンドを入力して、すべての Data Protector サービスを再起動します。
   - Windowsの場合: `<Data_Protector_home>¥bin¥omnisv -start`
   - UNIX の場合 : `/opt/omni/sbin/omnisv -start`

MC/ServiceGuard

Cell Manager が MC/SG 上に構成されている場合は、以下のコマンドを使用して Data Protector パッケージを再起動します。

```
cmrunpkg -n <node_name> <pkg_name>
```

Microsoft Cluster Server

Cell Manager が MSCS 上に構成されている場合は、クラスター・アドミニストレータユーティリティを使用して、OBVS_VELOCIS と OBVS_MCRS クラスター・グループをオンラインにします。

メディア集中管理データベース (CMMDB)

IDB は、バックアップ / 復元 / メディア管理セッション、デバイスやメディアなどに関する情報を保持する埋め込みデータベースです。IDB は、Cell Manager 上にある 5 つのパートから構成されています。

- MMDB - メディア管理データベース
- CDB - カタログ・データベース
- DCBF - 詳細カタログ・バイナリ・ファイル
- SMBF - セッション・メッセージ・バイナリ・ファイル
- SIBF - サーバレス統合バイナリ・ファイル

一般的なセル指向の環境では、すべてのパートが Cell Manager システム上に配置され、そのセルのデバイスやメディア、バックアップに関する情報が保存されます。セキュリティ上の理由により、別の Data Protector セルからこのデータにアクセスしてデータを使用することはできません。したがって、このセルで使用されるメディアやデバイスは、別のセルに移動しない限り、別のセルからのアクセスや使用はできません。

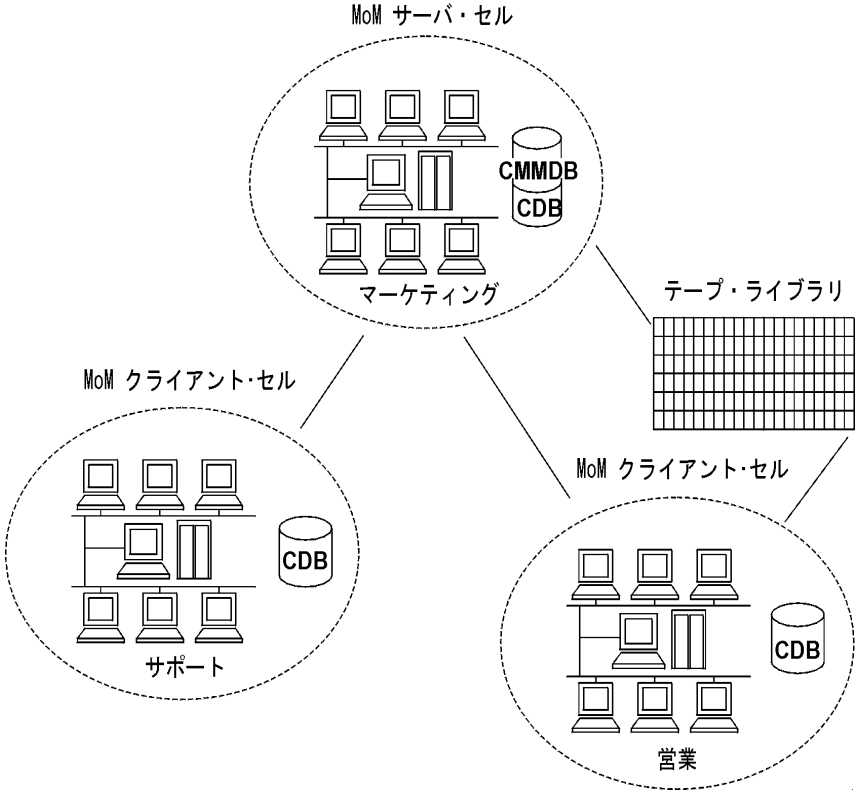
ハイエンド・バックアップ・デバイスが含まれる大規模な複数セルの環境では、デバイスやメディアを複数のセル間で共有したい場合があります。これを実現するには、すべてのセルに対して 1 つの中央 MMDB データベースを設定し、個々のセルに対しては個別の CDB を設定します。これにより、複数セル構造によるセキュリティ機能を維持しながら、デバイスやメディアを共有できます。

CMMDB を使用すると、あるメディアを使用してバックアップを最初に実行した Data Protector セルがそのメディアのオーナーとなります。メディアのオーナーはメディア・ビューに表示されます。メディアの保護期間中は、オーナーのセルからのバックアップだけがそのメディアに追加されます。したがって、複数のセルが同時にあるメディアのオーナーになることはできません。保護期限が終了したメディアは、再び他のセルからも使用できるようになります。

注記

エンタープライズ環境内のどこからバックアップする場合でも、バックアップを実行するセルが CMMDB にアクセスできなければバックアップを実行できません。たとえば、セルと MoM セルの間でネットワーク障害が発生した場合などがこれに該当します。

図 10-1　メディア集中管理データベース



メディア集中管理データベースの構成

メディア集中管理データベース (CMMDB) の設定は必須ではありません。CMMDB を設定しなくても、Data Protector は複数セル環境で動作しますが、各セルに独自の OBDB が存在する状態になります。この機能についての詳細は、「メディア集中管理データベース (CMMDB)」(471 ページ) を参照してください。

本項では、複数セルの環境全体に対してメディア集中管理データベースを構成する方法を説明します。必要であれば、構成プロセス中にローカルのメディア管理データベースを中央の CMMDB にマージすることができます。CMMDB とローカルの MMDB のどちらを使用するかを各セルに対して指定できます。

重要

CMMDB は、ライセンス設定に大きな影響を及ぼします。MMDB をローカルからリモートへ変更すると、直ちにライブラリやデバイスに関連するすべてのライセンスが MoM Manager から取得され (有効になり)、クライアントのセルから削除可能になります。

CMMDB を使用する場合、MoM Manager システム上に置く必要はありません。CMMDB は、MoM 環境内のいずれの Cell Manager 上に置いても構いません。CMMDB を置く Cell Manager は、以下のディレクトリにある `mmdb_server` ファイルで指定します。

- Windows の場合 : `<Data_Protector_home>¥Config¥server¥cell`
- UNIX の場合 : `/etc/opt/omni/server/cell`

保護が設定されているデータが保存されている各メディアには、現在どのセルがそのデータを所有しているかを示す情報があります。保護期限が終了すると、任意のセルがこのメディアを再度使用できます。たとえば、あるセルでテープを初期化した場合、テープ上に保護されているデータがなければ他のセルがこのテープを使用できます。ライブラリにロードされたテープがまだ初期化されていない場合、メディア割当てポリシーが `[Loose]` に設定されており、他のテープが使用不可能な場合は、任意のセルがこのテープを初期化できます。

メディア割当て規則は、共有されているテープにも同様に適用されます。ただし、追加可能なメディアが、それを所有しているセルによってのみ追加可能である場合を除きます。

MoM では、CMMDB に一度に追加できるセルは 1 つだけです。

必要条件

- すべてのセルの Data Protector Cell Manager に、同じバージョンの Data Protector がインストールされて実行されている必要があります。
- 複数セル環境へ追加するどのセル上でも、バックアップ、復元、メディア管理が行われていないことを確かめてください。

CMMDB の構成方法

MoM 環境で CMMDB を構成するには、以下の 2 つの手順を実行する必要があります。

1. MoM Manager で CMMDB を構成する。「MoM Manager での CMMDB の構成」（474 ページ) を参照してください。
2. クライアント・セルで CMMDB を構成する。「クライアント・セルでの CMMDB の構成」（475 ページ) を参照してください。

注記

CMMDB を構成して使用を開始した後で、ローカルの MMDB に分割することはできません。古い MMDB を復元することはお勧めできません。この場合は、MMDB を新規作成することをお勧めします。

MoM Manager での CMMDB の構成

MoM Manager にログオンして、以下の手順を実行します。

1. 安全性を考慮して、以下のディレクトリを一時ディレクトリにコピーします。
   - Windows の場合 : *<Data_Protector_home>*¥db40¥datafiles¥mmdb
   - UNIX の場合 : /var/opt/omni/server/db40/datafiles/mmdb
2. 以下のコマンドを実行して、ローカルの MMDB を CMMDB にマージします。

- Windows の場合 : *<Data_Protector_home>*¥bin¥omnidbutil -mergemmdb *<Cell_Server_Hostname>*
- UNIX の場合 : /opt/omni/sbin/omnidbutil -mergemmdb *<Cell_Server_Hostname>*

ヒント

新しいセルを構成している場合 (かつデバイスやメディアをまだ構成していない場合) は、データベースをマージする必要はありません。デバイスやメディアをすでに構成したセルだけが CMMDB へのマージ対象となります。

3. 以下のコマンドを実行して、ローカルの CDB を同期させます。
   - Windows の場合 : *<Data_Protector_home>*¥bin¥omnidbutil -cdbsync *<Cell_Server_Hostname>*
   - UNIX の場合 : /opt/omni/sbin/omnidbutil -cdbsync *<Cell_Server_Hostname>*
4. MoM Manager 上で、(ユーザーインタフェースを使用して) メディア・プールとデバイスの複製名を編集します。複製名には、元の名前に "_N" が追加されています。N は番号を示します。デフォルト・プールが 2 つのセル上にある場合は、必ずこの状況が発生します。この場合は、これらのデバイスを使用するバックアップ仕様を手動で変更して、新しいデバイス名を使用することが必要です。メディア・プールの説明に、そのプールがどのセルのものかを記述しておくと良いでしょう。

CMMDB に追加するすべてのクライアント・セルに対して、上記のステップ 2 ～ 4 を繰り返し行います。

クライアント・セルでの CMMDB の構成

各 MoM クライアント・セル上で、以下を行います。

1. クライアントセルの Cell Manager に Administrator ユーザーグループのメンバーとしてログオンします。
2. MMDB サーバの名前 (完全修飾名) を含むファイルを作成します。

- Windows の場合 :
  <Data_Protector_home>¥Config¥server¥cell¥mmdb_server
  ファイルを UNICODE 形式で保存します。
- UNIX の場合 : /etc/opt/omni/server/cell/mmdb_server

3. Data Protector サービスを終了して再起動します。「Data Protector サービスの再起動」(469 ページ) を参照してください。
4. 以下のコマンドを実行して構成ファイルを更新します。
   - Windows の場合 : *<Data_Protector_home>*¥bin¥omnicc -update_mom_server
   - UNIX の場合 : /opt/omni/bin/omnicc -update_mom_server

ライセンス集中管理

ライセンス集中管理の設定は必須ではありません。各 Cell Manager には個別のライセンスをインストールできます。ライセンス集中管理を使用しない場合、ライセンスの使用はインストールされたセルに限定され、すべてのライセンス管理作業はローカルで行う必要があります。

注記

MoM セル内でクラスターを構成している場合は、必ずクラスター・クライアントに仮想ホスト名を付けて識別してください。

ライセンス集中管理を使用する理由

Data Protector では MoM 環境全体に対してライセンス集中管理を構成できます。これにより、すべてのライセンスを MoM Manager システムにインストールして保持し、必要に応じて特定のセルに割り当てることができます。

ライセンス集中管理を行うことにより、ラインセンス管理が容易になります。MoM 環境内のすべてのセルのライセンス管理作業は MoM 管理者が行います。管理作業にはライセンスの配布や移動も含まれます。

ライセンスを Cell Manager にローカルにインストールした場合、*HP Password Delivery Center* の許可を得ずにセル間を移動させることはできません。ライセンスの移動方法については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

ライセンス集中管理の設定

必要条件

既存の Data Protector セルを MoM 環境に統合する場合は、既存の Cell Manager から新しい MoM Manager へライセンスを移動するよう *HP Password Delivery Center* にライセンスの移動要求を送付する必要があります。

ライセンス集中管理の構成

1. MoM Manager にログオンして `licdistrib.dat` ファイルを作成します。
   - Windows の場合 : *<Data_Protector_home>*¥Config¥server¥cell¥licdistrib.dat
   - UNIX の場合 : /etc/opt/omni/server/cell/licdistrib.dat

2. MoM 環境内の各クライアント Cell Manager にログオンして、MoM Manager の名前を含む lic_server ファイルを作成します。

   Windows の場合 :
   <Data_Protector_home>¥Config¥server¥cell¥lic_server

   UNIX の場合 : /etc/opt/omni/server/cell/lic_server

3. 変更を行なった各 Cell Manager で、Data Protector サービスを終了して再起動します。「Data Protector サービスの再起動」（469 ページ) を参照してください。

4. [Data Protector Manager-of-Managers] のコンテキスト・リストから [クライアント] をクリックします。

5. Scoping ペインで、ライセンス情報を変更したい Cell Manager を右クリックした後、[ライセンス付与の構成] をクリックしてウィザードを起動します。選択した Cell Manager で使用可能なライセンスの種類と数が表示されます。

   [使用中] 列には、その Cell Manager に割り当てられているライセンス数が表示されます。この列に表示されている数を増やすと、それに対応して使用可能なライセンス数が減ります。逆に、この列に表示されている数を減らすと、使用可能なライセンス数が増えます。

   [使用中] 列には、エンタープライズ全体で使用可能なライセンス数が表示されます。これはエンタープライズ環境内のいずれのセルにも使用されていないライセンスの数です。

   [合計] の列には、エンタープライズ全体で使用中のライセンスおよび使用可能なライセンスの合計数が表示されます。

6. [リモート] オプションをクリックしてライセンス設定をローカルからリモートに変更します。**[使用可能]** 列が **[割り当て済]** に変更することに注意してください。

7. ライセンス構成を変更します。変更作業中に使用できるのは[割り当て済] 列だけであることに注意してください。

ライセンスのリリース

特定の種類のライセンスの割り当てを解除して使用可能なライセンス数を増やすには、**[割り当て済]** 列で対応するライセンス数を減らします。

ライセンスの割り当て

特定の種類のライセンスを割り当てるには、**[割り当て済]** 列をダブルクリックして、対応するライセンス数を増やします。

8. [完了] をクリックして構成を適用します。
9. ライセンスの集中管理を設定するすべての Cell Manager に対して、上記のステップを繰り返し行います。

注記

Data Protector は 1 時間ごとに MoM Manager に接続してライセンス構成をチェックします。ライセンス付与のステータスは 72 時間保存されます。通信に問題がある場合、72 時間を経過するとローカル・ライセンスが使用されます。

MoM 環境でのライセンスの移動

ライセンス集中管理を構成していない場合、*HP Password Delivery Center* の許可を得ずに別のセルにライセンスを移動させることはできません。しかし、ライセンス集中管理が構成されており、MoM 管理者が必要に応じてライセンスを割り当てるように構成されている MoM 環境内では、ライセンスを移動できます。

以下の例では、あるセルのクライアントが別のセルに移動されています。これは、ライセンスの移動に必要なことです。

再編成前のエンタープライズ環境

Aztec と Mayan という 2 つの Cell Manager がエンタープライズ環境内にあり、ライセンス集中管理が構成されているとします。Aztec は 1 つの Cell Manager for UNIX - Single Drive ライセンスを持つ HP-UX Cell Manager です。このセルには、NDMP Server Backup Extension ライセンスが必要な NDMP サーバも接続されています。Mayan も 1 つの Cell Manager for UNIX - Single Drive ライセンスを持つ HP-UX Cell Manager です。

エンタープライズ環境の再編成

Aztec セルを再編成する必要があります。大部分のクライアントと NDMP サーバを Mayan セルに移動します。移動により、Mayan では NDMP Server Backup Extension ライセンスが必要になります。以下の手順に従って、ライセンスを移動します。

1. [Data Protector `Manager-of-Managers`] のコンテキスト・リストから [クライアント] をクリックします。
2. Aztec Cell Manager を右クリックし、[ライセンス付与の構成] をクリックします。Aztec Cell Manager で使用可能なライセンスの種類と数が表示されます。NDMP Server Backup Extension ライセンスを削除します。
3. [完了] をクリックして構成を適用します。
4. Mayan Cell Manager を右クリックし、[ライセンス付与の構成] をクリックします。NDMP Server Backup Extension ライセンスを追加します。
5. [完了] をクリックして構成を適用します。

再編成後のエンタープライズ環境

Aztec Cell Manager には Cell Manager for UNIX - Single Drive ライセンスが 1 つ、Mayan Cell Manager には Cell Manager for UNIX - Single Drive ライセンスと NDMP サーバ用の NDMP Server Backup Extension ライセンスが 1 つずつあることになります。

Data Protector のライセンス付与のポリシーの詳細については、『*HP OpenView Storage Data Protector インストールおよびライセンス・ガイド*』を参照してください。

ライセンス集中管理の非アクティブ化

ライセンス集中管理を非アクティブ化し、ライセンス設定をローカルに戻すことができます。

非アクティブ化の手順

1. [Data Protector Manager-of-Managers] のコンテキスト・リストから [クライアント] をクリックします。
2. Scoping ペインで、ライセンス集中管理を非アクティブ化したい Cell Manager を右クリックした後、[ライセンス付与の構成] をクリックしてウィザードを起動します。選択した Cell Manager で使用可能なライセンスの種類と数が表示されます。
3. [ローカル] オプションをクリックしてライセンス設定をリモートからローカルに変更します。
4. [完了] をクリックして構成を適用します。
5. ライセンス集中管理を非アクティブ化するすべての Cell Manager に対して、上記のステップを繰り返し行います。
6. MoM Manager にログオンして、以下のディレクトリをマウントします。
   - Windows の場合 : `<Data_Protector_home>¥Config¥server¥cell`
   - UNIX の場合 : `/etc/opt/omni/server/cell`
7. `licdistrib.dat` のファイル名を `licdistrib.old` などに変更します。

変更した内容は、変更を行った MoM Manager や各 Cell Manager 上の Data Protector サービスを終了して再起動するまで有効になりません。「Data Protector サービスの再起動」（469 ページ) を参照してください。

MoM 環境で行う作業

Manager-of-Managers インタフェースを使用すると、エンタープライズ・バックアップ環境の構成、管理、制御を 1 箇所から行えます。

MoM ユーザー・インタフェースでは、セルのインポートやエクスポート、セル間でのクライアントの移動、環境内の他のセルへの MoM 構成の配布が可能です。

MoM Manager では、その他の作業もローカル管理者として行う場合と同様に実行できます。通常の手順に従って、バックアップや復元の構成、特定のセルに対するデバイスやメディアの管理、Data Protector ユーザーやユーザー・グループの構成、クライアントの追加、実行中のセッションやバックアップ環境のステータスのモニター、レポートや通知の構成を行えます。

Data Protector セルのインポートおよびエクスポート

MoM 環境にセルをインポートすると、MoM Manager を使ってセルを集中管理できます。セルをエクスポートすると、エンタープライズ環境からそのセルが削除されます。

注記

クラスター・クライアントは、MoM Manager に対する識別名として仮想サーバ名を使用します。MoM 環境内でクラスターをインポートまたはエクスポートする場合は、仮想サーバ名以外は使用しないでください。

Cell Manager のインポート

1. [Data Protector Manager-of-Managers] のコンテキスト・リストから [クライアント] をクリックします。
2. [エンタープライズ・クライアント] を右クリックし、[Cell Manager のインポート] をクリックします。
3. インポートする Cell Manager を選択して [完了] をクリックします。

Cell Manager のエクスポート

1. [Data Protector Manager-of-Managers] のコンテキスト・リストから [クライアント] をクリックします。
2. Scoping ペインでエクスポートする Cell Manager を右クリックし、[Cell Manager のエクスポート] をクリックします。

3. 選択内容を確定します。

セル間でのクライアント・システムの移動

Data Protector では、セル間でシステムを移動することができます。この作業中に Data Protector は以下のことを行います。

- 移動対象のシステムがバックアップ仕様で構成されているかどうかを確認し、構成されている場合は、移動先のセルでこのシステムのバックアップを再構成する手順を示します。
- 対象のシステムにデバイスが構成されているかどうかを確認し、構成されたデバイスがあれば別のシステムに移動する手順を示します。
- 対象のシステムのデバイスでメディアが使用されているかどうかを確認し、使用中のメディアがあればそれを移動する手順を示します。

クライアントの移動

1. [Data Protector Manager-of-Managers] のコンテキスト・リストから [クライアント] をクリックします。
2. 移動対象のシステムが所属している Cell Manager を展開します。
3. 対象のクライアント・システムを右クリックし、[クライアント・システムを別のセルへ移動] をクリックしてウィザードを開きます。
4. 移動先の Cell Manager を選択し、[完了] をクリックしてクライアントを移動します。

MoM 構成の配布

Data Protector では、MoM 環境のすべての Cell Manager 上で、共通のユーザー・クラス仕様、holidays ファイルの設定値、グローバル・オプション・ファイルの設定値を作成したり、ボールティングを行えます。

MoM 構成の配布方法

以下の手順に従って、MoM 構成を配布します。

1. [Data Protector Manager-of-Managers] のコンテキスト・リストから [クライアント] を選択します。[エンタープライズ・クライアント] を右クリックし、[構成を配布] をクリックします。
2. [構成を配布] ダイアログ・ボックスで、配布する構成の種類と、配布先の Cell Manager を選択します。
3. [完了] をクリックして構成を配布します。

ユーザーの構成

単一の Cell Manager の場合と同様に、MoM 環境にユーザーやユーザー・グループを追加できます。追加を実行すると、すべての Cell Manager が新しいユーザーに更新されます。ユーザーとユーザグループの詳細は、第 4 章「ユーザーとユーザー・グループの 構成」(135 ページ) を参照してください。

Data Protector ユーザーまたはユーザーグループの構成は、以下の手順で行います。

1. [Data Protector Manager-of-Managers] のコンテキスト・リストから [ユーザー] をクリックします。
2. ユーザーを追加する Cell Manager を選択します。
3. [編集] メニューの [追加] をクリックし、新しいユーザーを追加する場合は [ユーザー] を、ユーザー・グループを追加する場合は [ユーザー・グループ] を選択します。
4. 必要な情報を入力して [完了] をクリックします。

特定のセルのデバイスとメディアの管理

デバイスとメディアを、エンタープライズ環境内の特定のデバイスやメディアに対して構成できます。以下の手順で行います。

1. [Data Protector Manager-of-Managers] のコンテキスト・リストから [クライアント] をクリックします。
2. 管理対象となるデバイスまたはメディアを含むセルを選択します。
3. [ツール] メニューで、[デバイスとメディアの管理] をクリックします。[デバイス / メディア] コンテキストで、ローカル管理者と同様の手順でデバイスとメディアを構成します。

エンタープライズ環境でのデータの復元、モニター、レポート

エンタープライズ環境では、単一セル環境の場合と同様にデータを復元できます。

適切なソースからデータを選択して、第 8 章「復元」(361 ページ) に記載された手順で復元を行います。

Data Protector では、エンタープライズ環境の任意のセルに関して、現在実行中、または以前に実行されたセッションをモニターできます。また、Web レポートを使用している場合は、Scoping ペインの MULTICELL を使ってエンタープライズ環境全体に関するレポートを作成できます。

エンタープライズ環境における上記の機能の使用方法については、第 9 章「モニター、レポート、通知、およびイベント・ログ」(407 ページ) を参照してください。

11 Data Protector 内部データベースの管理

本章の概略

本章では、Data Protector 内部データベース (IDB) と、データベースの管理に関する作業について説明します。本章は以下の項で構成されています。

内部データベースについて

Data Protector 内部データベース (IDB) とは

Data Protector 内部データベース (IDB) は Cell Manager 上に置かれる埋め込みデータベースです。バックアップ対象のデータ、バックアップ・データの格納先メディア、バックアップ / 復元 / コピー / メディア管理セッションの結果、構成済みのデータベースとライブラリなどに関する情報を保持します。

IDB を使用する理由

IDB を使用する主な理由は以下の 3 つです。

- 復元手順の高速化と効率化

  IDB に格納された情報により復元対象のファイルとディレクトリをブラウズできます。復元に必要なメディアをすばやく検索できるので、復元をすばやく実行できます。

- バックアップ管理

  IDB に格納された情報によりバックアップ・セッションの結果を確認できます。

- メディア管理

  IDB に格納された情報により、バックアップ・セッションやコピー・セッション中のメディアの割り当て、メディア管理操作やメディア属性の追跡が可能になります。また、メディアを異なるメディア・プールにグループ化したり、テープ・ライブラリ内のメディアの収納場所を追跡することもできます。

IDB の管理方法

Data Protector のバックアップ環境を設定する重要な手順の 1 つは IDB の構成です。「IDB の構成」(494 ページ) の説明に従って IDB を構成すると、IDB の保守作業の実施が必要になったときに通知されるようになります。

IDB に対する保守作業、およびその実施が必要になる場合については 「IDB の保守」(510 ページ) を参照してください。

エラー・メッセージが表示された場合は、「IDB のトラブルシューティング」(745 ページ) と「IDB を復旧する」(527 ページ) 参照してください。

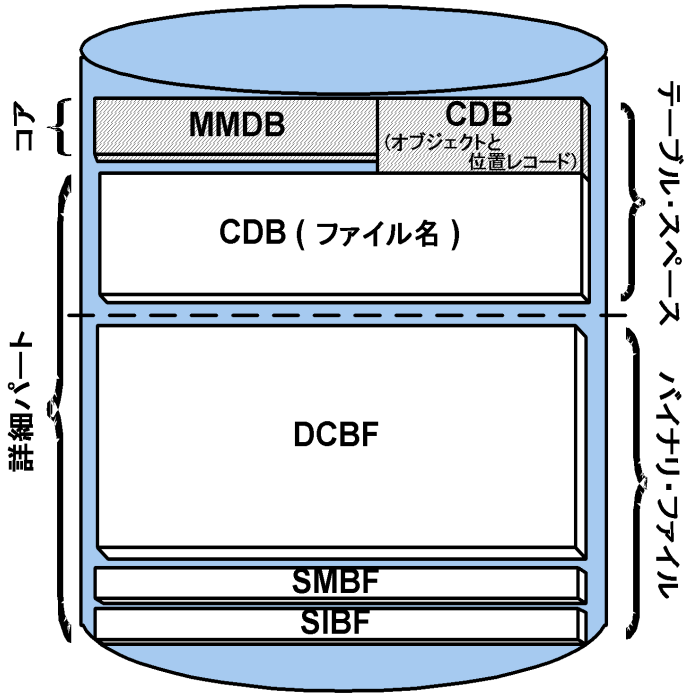
IDB の制限事項については、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

IDB のアーキテクチャ

IDB は、以下のパートで構成されます。

- MMDB (メディア管理データベース)
- CDB (カタログ・データベース)
- DCBF (詳細カタログ・バイナリ・ファイル)
- SMBF (セッション・メッセージ・バイナリ・ファイル)
- SIBF (サーバレス統合バイナリ・ファイル)

図 11-1 IDB のアーキテクチャ



IDB の各パートは、特定の Data Protector 情報 (レコード) を格納し、IDB のサイズと増加にさまざまな影響を与えます。各パートは、Cell Manager 上の個別のディレクトリに置かれます。

MMDB　メディア管理データベースには、以下の項目に関する情報が格納されます。

- 構成済みのデバイス、ライブラリ、ライブラリ・ドライブ、およびスロット
- Data Protector メディア
- 構成済みのメディア・プールとメディア・マガジン

CDB　カタログ・データベースには、以下の項目に関する情報が格納されます。

- バックアップ、復元、コピー、メディア管理セッション。これは Data Protector のモニター・ウィンドウに送られる情報のコピーです。
- バックアップ・オブジェクトとそれらのバージョン、オブジェクト・コピー。
- バックアップしたファイルのパス名 (ファイル名) とクライアント・システム名。ファイル名は、クライアント・システムごとに 1 回だけ記録されます。バックアップ後、次回のバックアップまでの間に作成されたファイル名は、CDB に追加されます。
- バックアップしたオブジェクトのメディア上の位置。バックアップしたオブジェクトごとに、バックアップに使用したメディアとデータ・セグメントに関する情報が格納されます。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です。

DCBF

詳細カタログ・バイナリ・ファイル・パートには、ファイル・バージョン情報が格納されます。これは、バックアップしたファイルに関する情報 (ファイル・サイズ、変更日時、属性 / 保護など) です。

バックアップに使用した各 Data Protector メディアにつき、DC (詳細カタログ) バイナリ・ファイルが 1 つずつ作成されます。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、新しいバイナリ・ファイルが作成されます。

SMBF

セッション・メッセージ・バイナリ・ファイル・パートには、バックアップ / 復元 / コピー / メディア管理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ます。セッションごとに 1 つのバイナリ・ファイルが作成されます。バイナリ・ファイルは、年と月に基づいて分類されます。

SIBF

サーバレス統合バイナリ・ファイル・パートには、NDMP の raw 復元データが格納されます。このデータは、NDMP オブジェクトの復元に必要です。

MMDB パートと CDB パートは、テーブルスペースからなる埋め込みデータベースで実装されています。このデータベースは、rds データベース・サーバ・プロセスによって制御されます。MMDB と CDB に対する変更は、すべてトランザクション・ログを使用して更新されます。CDB (オブジェクトと位置) と MMDB が、IDB のコア・パートとなります。

IDB の DCBF パート、SMBF パート、および SIBF パートは、バイナリ・ファイルで構成されます。更新は、トランザクションなしで直接行われます。

Manager-of-Managers (MoM) 環境では、MMDB をセントラル・システムに移動することで、集中メディア管理データベース (CMMDB) を構築できます。

IDB の各パートのさらに詳しい情報については、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

IDB の構成

IDB を構成することにより、以下の項目が管理しやすくなります。

- IDB のサイズと利用可能なディスク・スペース
- IDB ディレクトリの位置
- トランザクション・ログの使用状況
- IDB の破損 / 障害時に必要な IDB のバックアップ
- IDB のレポートと通知の構成

IDB は、構成後、保守が必要なことを通知された場合にのみ保守を行います。

一般的な手順

IDB を構成するための一般的な手順は以下のとおりです。

1. 今後の必要性を考えてディスク・スペースを割り当てます。
   詳細は、「今後の使用を考えてディスク・スペースを割り当てる」（494 ページ) を参照してください。
2. IDB 復旧の準備をします。
   詳細は、「IDB 復旧の準備」（496 ページ) を参照してください。
3. IDB について適切なレポートと通知を設定します。
   詳細は、「データベースのレポートと通知を構成する」（507 ページ) を参照してください。

今後の使用を考えてディスク・スペースを割り当てる

時間の経過に伴い、Cell Manager 上のディスク・スペースのかなりの部分を IDB が占める可能性があります。IDB 用のディスク・スペース割り当ては、今後の必要性を十分に見据えて計画しておく必要があります。

必要条件

- ファイル数、ファイルの変動率、環境規模の拡張など、IDB のサイズ増加に影響を及ぼす主な要因について理解しておく必要があります。詳細は『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

- 環境要件と利用可能なディスク・スペースに応じて、ログ・レベルとカタログ保護に関するポリシーを設定する必要があります。これらの情報の取得方法、およびログ・レベルの推奨される使用方法、カタログ保護の設定については、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。
- 今後の IDB のサイズ (今後 IDB で必要となるディスク・スペース) を見積もる必要があります。IDB サイズの見積もりについては、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

ディスク・スペースの必要量

IDB に必要となるディスク・スペースは、バックアップの定義や実行に使用するさまざまな構成条件とポリシーによって異なります。

ここでは、3 か月後に IDB で約 900MB のディスク・スペースが必要になり、それ以降のサイズ増加がごくわずかにとどまる環境の例を簡略化して示します。

- バックアップ対象となるシステムは 100 台 (10,000 ファイル / システム、メール・サーバなし)。
- 総データ量は 350GB。
- 代表的な変動率 (1 か月あたりの新ファイル 3%) でのファイルシステム・バックアップ。
- 毎週 1 回のフル・バックアップと 4 回の増分バックアップを計画。
- 復元前にファイル名を簡単にブラウズできるように、ログ・レベルを [すべてログに記録] に設定。これはディスク・スペースを最も消費するログ・オプションです。
- カタログ保護は、フル・バックアップに対しては 3 か月、増分バックアップに対しては 2 週間に設定。

構成規模が大きい場合や、IDB 内のカタログの保護期間が長い場合は、IDB 用スペースが 20GB 以上必要になる可能性があることに注意してください。

Cell Manager 上にある、Database Capacity Planning Tool を使うと、詳細な見積もりが可能です。このツールのパスは、以下のとおりです。

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

事前に計画しておくべきこと

IDB のサイズは、通常、特に使用開始直後 (カタログの維持期限に達するまでの間) 急速に増加します。その後の IDB サイズ増加率は、1 か月あたりの新規ファイル数の割合が高いシステムの変動率や、環境規模の拡大 (バックアップ対象のシステムの追加) などの要因によって決まります。

様々な IDB サイズ増加要因を理解しておくことが重要です。

- IDB のファイル名パートのサイズは、セル内のファイル名の総数に比例します (データ量やバックアップ数には比例しません)。一部のメール・サーバや自動生成ファイル数の多いシステムを例外として、一般に、ファイル名パートのサイズ増加率は、あまり高くありません。
- IDB のファイル・バージョン・パートのサイズは、バックアップおよびオブジェクト・コピーの回数、セル内のファイル数、およびカタログ保護の期間に比例して増加します。
- IDB トランザクション・ログ・ファイルを使用する場合は、ディスク・スペースの必要量が増えます。この場合のサイズは、単純には予測できません。バックアップ対象の新しいファイル名の数や、IDB のバックアップ後、次回のバックアップまでの間の総体的なバックアップ・アクティビティ (スケジュール済みバックアップが主体の場合は、週数) が主なサイズ増加要因となります。

IDB 復旧の準備

いつでも IDB を復旧できるようにするためには、事前の準備が必要です。IDB の復旧により、IDB 内に格納されている情報が復元されます。IDB の復旧は、Cell Manager がクラッシュした場合のバックアップ・データの復元には不可欠です。

IDB 復旧の準備手順は以下のとおりです。

- 堅牢性強化のための推奨事項を考慮します。「堅牢性に関する考慮事項」(497 ページ) を参照してください。
- ディレクトリの位置を変更します。「IDB ディレクトリ」(497 ページ) を参照してください。
- トランザクション・ログを有効にします。「トランザクション・ログを有効化する」(503 ページ) を参照してください。
- IDB バックアップを構成し、定期的にバックアップします。
  詳細は、「データベース・バックアップを構成する」(505 ページ) を参照してください。

堅牢性に関する考慮事項

本項では、IDB の堅牢性と信頼性を強化するために考慮すべきポイントと推奨事項について、概要を説明します。

- CDB(オブジェクトと位置) および MMDB を含む IDB のコア・パートは、Data Protector の運用に不可欠です。
- バックアップと復元など、Data Protector の基本操作は、IDB の DCBF パートと SMBF パートが存在しなくても実行可能です。ただし、これらが存在しない場合は、復元対象のファイル名をブラウズできず、またセッション・メッセージが失われます。
- IDB 回復ファイルと IDB トランザクション・ログが失われた場合、通常の操作には支障をきたしませんが、IDB の復元が非常に困難になり、前回の IDB バックアップ以降に生成された IDB データを再生できなくなります。この場合は、使用したメディアの再インポートが必要になります。

堅牢性強化のための推奨事項

- IDB 回復ファイルとトランザクション・ログは必ず、IDB のコア・パートとは別の物理ディスクに置きます。

  これは、物理ディスク A がクラッシュした場合に、IDB をすばやく、かつ簡単に復元できるようにすることを目的としています。さらに、これにより、前回の IDB バックアップ以降に発生したトランザクションの再生も可能になります。図 11-2 を参照してください。
- DCBF、SMBF、および SIBF の各パートも IDB のコア・パートとは別のディスクに置くことをお勧めしますが、さほど重要ではありません。これらを別のディスクに置くと、ディスク A に対する負荷が大幅に減り、IDB のスペース管理が容易になります。これらのファイルは通常、IDB の大部分を占めるためです。

ヒント

これらの推奨事項に従って堅牢性を強化することで性能も向上し、Cell Manager システム上でより多くのバックアップ作業を行えるようになります。

IDB ディレクトリ

IDB は Cell Manager 上にあります。一部の IDB ディレクトリを別の場所に移動して、スペース管理を向上させることができます。

制限事項

- IDB ファイルは、ローカルに接続されているディスク上にのみ置くことができます。NFS や共有ディスクは使用できません。
- IDB をクラスターの中にインストールする場合は、クラスター・グループ (Microsoft Cluster Server) またはクラスター・パッケージ (MC/ServiceGuard) 内のディスク上にインストールする必要があります。

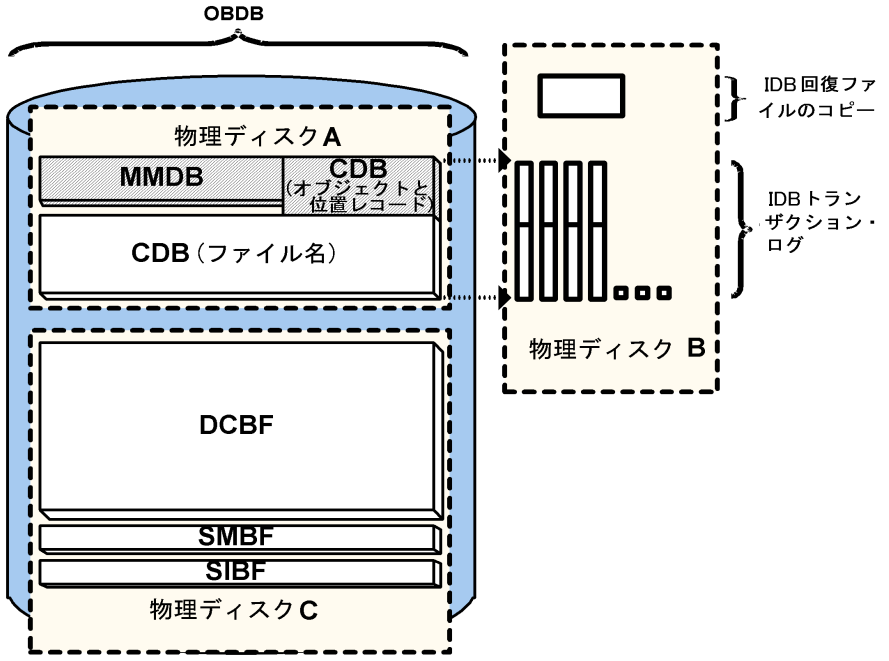
表 11-1 Windows システム上の IDB ディレクトリの位置

IDB	Windows システム上の位置
テーブルスペース (CDB と MMDB)	*<Data_Protector_home>*¥db40¥datafiles
バイナリ・ファイル (DCBF、SMBF、SIBF)	• *<Data_Protector_home>*¥db40¥dcbf • *<Data_Protector_home>*¥db40¥msg • *<Data_Protector_home>*¥db40¥meta
トランザクション・ログ	*<Data_Protector_home>*¥db40¥logfiles¥syslog
IDB 回復ファイル	*<Data_Protector_home>*¥db40¥logfiles¥rlog

表 11-2 UNIX システム上の IDB ディレクトリの位置

IDB	UNIX システム上の位置
テーブルスペース (CDB と MMDB)	/var/opt/omni/server/db40/datafiles
バイナリ・ファイル (DCBF、SMBF、SIBF)	• /var/opt/omni/server/db40/dcbf • /var/opt/omni/server/db40/msg • /var/opt/omni/server/db40/meta
トランザクション・ログ	/var/opt/omni/server/db40/logfiles/syslog
IDB 回復ファイル	/var/opt/omni/server/db40/logfiles/rlog

図 11-2 IDB ディレクトリの推奨位置



IDB ディレクトリの位置を変更する

以下に示す IDB のどのディレクトリの位置も変更できます。

- IDB の CDB パート (オブジェクト、位置、ファイル名) と MMDB パートを含む `datafiles` ディレクトリ
- トランザクション・ログと IDB 回復ファイルを含む `logfiles` ディレクトリ
- IDB の DCBF パートを含む `dcbf` ディレクトリ
- IDB の SMBF パートを含む `msg` ディレクトリ
- IDB の SIBF パートを含む `meta` ディレクトリ

Data Protector ユーザー・インタフェースを使用して) dcbf ディレクトリ、および (グローバル・オプション・ファイルを使用して) msg と meta ディレクトリのディレクトリ・パスを変更することもできます。

注記

UNIX 上で、シンボリック・リンクを使ってディレクトリの位置を変更することも可能ですが、/var/opt/omni/server/db40/datafiles ディレクトリの下層ではリンクを使用できません。

IDB ディレクトリの位置を変更するには、以下の手順を行います。

1. すべてのバックアップ・セッションと Data Protector アクティビティを終了し、omnisv -stop コマンドを実行して、Data Protector サービスを終了します。
   - Windows の場合 : *<Data_Protector_home>*¥bin¥omnisv -stop
   - UNIX の場合 : /opt/omni/sbin/omnisv -stop

   IDB が MC/ServiceGuard 上にインストールされている場合は、アクティブなノード上で cmhaltpkg *<pkg_name>* コマンドを実行し、Data Protector パッケージを終了します。ここで、*<pkg_name>* は Data Protector クラスター・パッケージの名前を示します。
2. 移動したい *<IDB_dir>* ディレクトリの名前を、*<IDB_dir>*.save に変更します。たとえば、トランザクション・ログと IDB 回復ファイルの位置を変更するには、*<Data_Protector_home>*¥db40¥logfiles を *<Data_Protector_home>*¥db40¥logfiles.save (Windows の場合) に、/var/opt/omni/server/db40/logfiles を /var/opt/omni/server/db40/logfiles.save (UNIX の場合) に名前を変更します。
3. 同じ相対パスを持つ空のディレクトリを新規作成します。たとえば *<Data_Protector_home>*¥db40¥logfiles (Windows の場合) または /var/opt/omni/server/db40/logfiles (UNIX の場合) などです。
4. Windows の場合、新しいディスクを追加するか、または *<Data_Protector_home>*¥db40¥*<IDB_dir>* として NTFS フォルダに新しいボリュームをマウントします。たとえば、*<Data_Protector_home>*¥db40¥logfiles としてマウントします。

UNIX の場合、新しいディスクを追加するか、または新しい論理ボリュームを作成し、/var/opt/omni/server/db40/*<IDB_dir>* としてマウントします。たとえば、/var/opt/omni/server/db40/logfiles としてマウントします。

5. 新しいディスクまたはボリューム上の*<IDB_dir>*に*<IDB_dir>*.saveの内容をコピーします。
6. omnisv -start コマンドを実行して Data Protector サービスを起動します。
   - Windowsの場合: *<Data_Protector_home>*¥bin¥omnisv -start
   - UNIX の場合 : /opt/omni/sbin/omnisv -start

   IDB が MC/ServiceGuard 上にインストールされている場合、アクティブなノード上で cmrunpkg *<pkg_name>* コマンドを実行し、Data Protector パッケージを起動します。

IDB 回復ファイルの追加コピーを作成する

IDB 回復ファイルの追加コピーを作成することにより、IDB の復旧のための重要なデータが失われるのを防ぐことができます。

以下の手順に従って、IDB 回復ファイルのコピーを作成します。

1. すべてのバックアップ・セッションと Data Protector アクティビティを終了し、omnisv -stop コマンドを実行して、Data Protector サービスを終了します。
   - Windows の場合 : *<Data_Protector_home>*¥bin¥omnisv -stop
   - UNIX の場合 : /opt/omni/sbin/omnisv -stop

   IDB が MC/ServiceGuard 上にインストールされている場合は、アクティブなノード上で cmhaltpkg *<pkg_name>* コマンドを実行し、Data Protector パッケージを終了します。ここで、*<pkg_name>* は Data Protector クラスター・パッケージの名前を示します。

   IDB が Microsoft Cluster Server にインストールされている場合は、アクティブなノード上でクラスター・アドミニストレータユーティリティを使用して、OBVS_VELOCIS クラスター・グループをオフラインにし、Inet サービスを停止します。

2. RecoveryIndexDir 変数の値を設定してグローバル・オプション・ファイルを編集します。つまり、Data Protector が IDB 回復ファイル obrindex.dat のコピーを作成するディレクトリを指定します。このとき、別の物理ディスクを指定することをお勧めします。
3. omnisv -start コマンド (UNIX では /opt/omni/sbin ディレクトリにあります) を実行して Data Protector サービスを起動します。
   - Windows の場合: *<Data_Protector_home>*¥bin¥omnisv -start
   - UNIX の場合 : /opt/omni/sbin/omnisv -start

   IDB が MC/ServiceGuard 上にインストールされている場合、アクティブなノード上で cmrunpkg *<pkg_name>* コマンドを実行し、Data Protector パッケージを起動します。

   IDB が Microsoft Cluster Server にインストールされている場合は、クラスター・アドミニストレータユーティリティを使用して、OBVS_VELOCIS と OBVS_MCRS クラスター・グループをオンラインにし、Inet サービスを起動します。

DC ディレクトリを作成または位置変更する

DC ディレクトリの作成

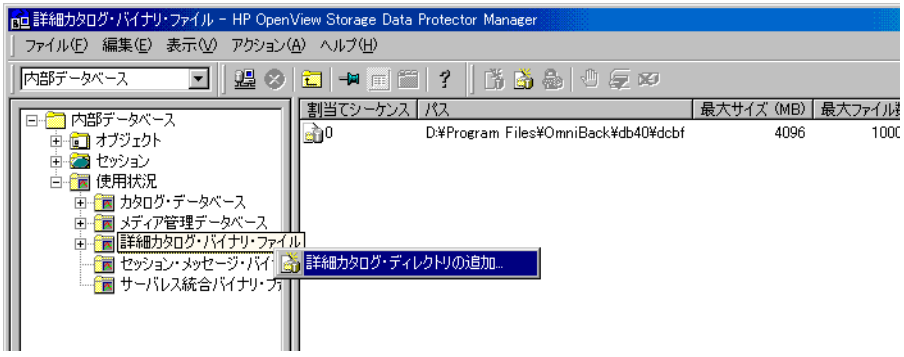
[Data Protector Manager] の [内部データベース] コンテキストを使用して、DC ディレクトリを作成します。図 11-3 を参照してください。詳しい手順については、オンライン・ヘルプの索引キーワード「DC ディレクトリの作成」を参照してください。

DC ディレクトリの位置変更

DC ディレクトリの位置を変更するには、以下の手順を行います。

1. Data Protector ユーザー・インタフェースを使って、新しい場所に新しい DC ディレクトリを作成します。図 11-3 を参照してください。
2. 新しい DC ディレクトリが正しく作成されており、ディスク・スペースが十分にあることを確認します。
3. DC バイナリ・ファイルをソース DC ディレクトリから新しい DC ディレクトリに移動します。
4. omnidbutil -remap_dcdir コマンドを実行して、DC バイナリ・ファイルのパス名を更新します。
5. 古いDCディレクトリを構成済みDCディレクトリのリストから削除します。

図 11-3 DC ディレクトリの作成



トランザクション・ログを有効化する

IDB の MMDB パートと CDB パートで使用するトランザクション・ログは、以下のディレクトリに作成されます。

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

トランザクション・ログは、デフォルトでは無効になっています。トランザクション・ログを有効にすると、最新の IDB バックアップから次の IDB バックアップまでトランザクション・ログが保持されます。トランザクション・ログ・ファイルのサイズが 2MB に達すると、新しいファイルが作成されます。IDB バックアップを実行すると、現在アクティブになっている以外の既存のトランザクション・ログがすべて削除され、新しいトランザクション・ログの作成が開始されます。

トランザクション・ログを有効にする理由

ガイド式自動回復機能を使うと、ログを再生することで、IDB を簡単に復元できます。この機能を使うには、前回の IDB バックアップ以降に作成されたログ・ファイルを利用可能にする必要があります。

ディスク・スペースに関する考慮事項

トランザクション・ログに使用されるディスク・スペースは、2 回の IDB バックアップの間に作成されたバックアップの量によって異なります。ファイル名がすでに IDB に格納されていれば、この量はかなり少なくなり、多くの場合 100MB の予約スペースだけで十分です。新しいファイル名をバックアップした場合は、ディスク・スペースの使用量が非常に大きく

なります (ファイル名ごとに約 200 バイト)。環境全体の最初のフル・バックアップを実行した**後で** (つまり、すべてのファイル名が IDB に格納された時点で) トランザクション・ログを有効にすることをお勧めします。

トランザクション・ログを有効にする方法

トランザクション・ログを有効にするには、以下の手順を行います。

1. すべてのバックアップ・セッションと Data Protector アクティビティを終了し、`omnisv -stop` コマンドを実行して、Data Protector サービスを終了します。
   - Windows の場合 : `<Data_Protector_home>¥bin¥omnisv -stop`
   - UNIX の場合 : `/opt/omni/sbin/omnisv -stop`
2. 以下のディレクトリのディスク・スペースが十分にあることを確認します。
   - Windows の場合 : `<Data_Protector_home>¥db40¥logfiles¥syslog`
   - UNIX の場合 : `/var/opt/omni/server/db40/logfiles/syslog`
3. `velocis.ini` ファイルを編集し、Archiving パラメータの値を 1 に設定します。
   - Windows の場合 : `<Data_Protector_home>¥db40¥datafiles¥catalog¥velocis.ini`
   - UNIX の場合 : `/var/opt/omni/server/db40/datafiles/catalog/velocis.ini`
4. `omnisv -start` コマンドを使って Data Protector サービスを起動します。
   - Windows の場合 : `<Data_Protector_home>¥bin¥omnisv -start`
   - UNIX の場合 : `/opt/omni/sbin/omnisv -start`

データベース・バックアップを構成する

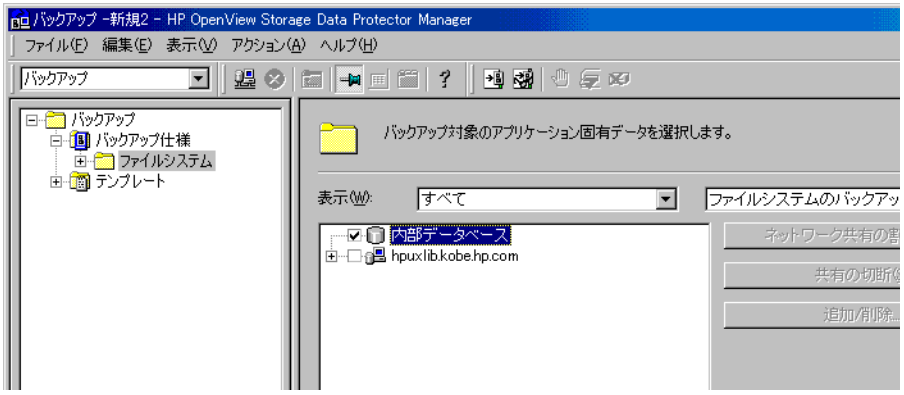
IDB の構成では、IDB 自体のバックアップを構成することが非常に重要です。IDB バックアップを定期的に実行するように構成すれば、障害発生時の復旧のための最も重要な準備作業が完了したことになります。Cell Manager がクラッシュした場合、他のバックアップ・データを復元するには、IDB の復旧が必須です。

IDB バックアップの構成方法

他の標準バックアップの場合と同じように、IDB バックアップを構成します。バックアップ対象オブジェクトとして［内部データベース］を選択し、IDB バックアップ仕様の [バックアップ・オブジェクトのサマリー] ページでオブジェクト・オプションを指定します。詳しい手順については、Data Protector オンライン・ヘルプの索引キーワード「IDB バックアップの構成」を参照してください。

図 11-4

内部データベース・オブジェクトを選択する



推奨される IDB バックアップの構成

IDB バックアップの構成時には、以下をお勧めします。

- IDB 用のバックアップ仕様を別に用意します。これにより、スケジュールの設定が容易になり、ディスク・クラッシュ時の復元も簡単になります。IDB 用のバックアップ仕様を作成するには、標準バックアップ手順に従い、バックアップ対象オブジェクトとして［内部データベース］を選択します。
- IDBバックアップを1日1回実行するスケジュールを設定します。これによりほぼ最新の IDB バックアップを常に保持できます。

- 特定のデバイス上で、通常のバックアップに使用するものとは別のメディアのメディア・プールで IDB バックアップを実行します。IDB バックアップにどのメディアを使用するかを明確にしておきます。[セッションで使用されるメディアのレポート] を構成しておくと、バックアップに使用するメディアに関する情報が通知されます。これにより、復元手順が大幅に効率化されます。可能な限り、Cell Manager にローカルに接続されたデバイスを使用してください。「Data Protector レポート」(417 ページ) を参照してください。
- データ保護とカタログ保護の期間は、数日間だけに設定します。これらのオプションは、少なくとも最新とその前の 2 つの IDB バックアップ・バージョンが保護されるように設定してください。
- [内部データベースのチェック] オプションは、常に有効にしておきます (デフォルトは有効)。図 11-5 を参照してください。
- 以前の IDB バックアップを新しいバックアップで上書きしないようにします。複数のコピーを保存しておくことをお勧めします。

IDB バックアップ時の動作

IDB のバックアップ時に、Data Protector は以下を実行します。

- IDB の整合性をチェックします。これにより、破損した IDB がバックアップされたり復元されるのを防止します。このチェックを実行させるには、[内部データベースのチェック] オプションを有効にする必要があります (デフォルトは有効)。

  データベースのサイズが 10GB で、`fnames.dat` ファイルのサイズが 1GB の場合、このチェック処理には約 1 時間半かかります。
- IDB 使用中はオンラインで IDB をバックアップします。したがって、IDB のバックアップ中に他のバックアップ・セッションや復元セッションを実行できます。ただし、可能であれば、他のバックアップや復元アクティビティを実行している時は IDB のバックアップは行わないようにしてください。
- デバイスのデータ、バックアップ仕様、スケジュールなど、Data Protector の構成データをすべてバックアップします。これにより、障害発生時の復旧手順が簡単になります。

注記

一度に実行できる IDB バックアップは 1 つだけです。

バックアップ前の自動チェックを無効にする

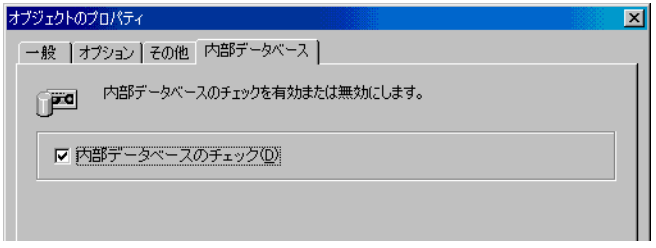
デフォルトでは、IDB のバックアップ前にデータベースの整合性が自動チェックされます。整合性の自動チェックは、有効 / 無効を切り替えることができます。ただし、IDB の自動チェックを有効にしておくことを強くお勧めします。

Cell Manager の使用率が高く、IDB のチェックに要する時間が問題になる場合は、[内部データベースのチェック] オプションを無効にすることが必要になります。この場合、以下の指針に従ってください。

- 自動チェックを行っても問題にならない時間帯に IDB バックアップが実行されるように、IDB チェック・オプションを有効にしてスケジュールを設定します。
- 毎日の IDB バックアップが、IDB チェック・オプションを無効にした状態で実行されるようにスケジュールを設定します。
- 少なくとも、最新のチェック済み IDB バックアップを保持するようにします。

詳しい手順については、オンライン・ヘルプの索引キーワード「IDB の自動チェックの無効化」を参照してください。

図 11-5 **[内部データベースのチェック] オプション (デフォルトは有効)**



データベースのレポートと通知を構成する

IDB のレポートと通知を構成して、IDB の削除、IDB サイズの拡張など、IDB に対する保守作業の実施が必要になったときに通知されるようにします。

IDB のレポート

以下は IDB レポートの一覧です。

[IDB の削除プレビュー・レポート]	クライアントあたりのファイル名数、クライアントあたりの古くなったファイル名の推定数、クライアントあたりのファイル名削除セッションの推定時間の情報を表示します。
[システム処理能力のレポート]	特定のクライアントにおけるファイル名の増加状況に関する情報を通知します。
[IDB の削除レポート]	IDB から削除されたファイル名を表示します。
[IDB サイズ・レポート]	IDB の各パートのサイズを表示します。

その他の Data Protector レポートについても考慮が必要です。たとえば、1 つのセッションリスト中の詳細情報を示すレポートなどです。詳細は「Data Protector レポート」(417 ページ) を参照してください。

IDB 通知

以下は IDB 通知の一覧です。

[IDB のスペース不足]	IDB のスペースが不足している場合に通知します。
[IDB テーブル・スペースのスペース不足]	IDB のテーブルスペースが不足している場合に通知します。
[IDB の削除必要]	ファイル名を IDB から削除する必要がある場合に通知します。
[IDB の破損]	IDB に何らかの破損が検出された場合に通知します。

各レポートと通知に関する詳細については、「レポートの種類」(419 ページ) を参照してください。

IDB のレポートと通知の構成手順

[Data Protector Manager] の [レポート] コンテキストを使用して、IDB レポートと通知を構成します。詳しい手順については、オンライン・ヘルプの索引キーワード「IDB レポートの構成」と「IDB 通知の構成」を参照してください。

次に行う手順

IDB レポートと通知を構成し終えたら、IDB 構成の最後の手順を完了したことになります。何らかの IDB 保守作業が必要になった場合は、Data Protector によって通知されます。引き続き環境を設定してください。

IDB の保守

IDB の構成後、下記の場合は、IDB の保守作業を実施する必要があります。

- IDB のスペースが不足している場合

  IDB 用のスペースを追加するか、IDB に書き込まれるデータ量を減らす必要があります。[IDB のスペース不足] または [IDB テーブル・スペースのスペース不足] により、スペース不足が通知されます (この機能を事前に構成している場合)。

- IDB ファイル・バージョンの削除が必要な場合

  削除の単位はメディア全体になります。つまり、メディア上のすべてのオブジェクト・バージョンのカタログ保護が切れてから、ファイル・バージョン・レコードが削除されます。次に、関連するメディアのバイナリ・ファイル（詳細カタログを含む）が削除されます。これにより、多数のファイル・バージョンが短時間で削除されます。これは毎日自動的に実行されます。古くなったセッションとメッセージも自動的に削除されます。

- IDB ファイル名の削除が必要な場合

  ファイル名の削除を実行する必要があります。1 日に 10 万個のファイルが古くなる環境なら、年 1 回の作業が必要です。ファイル名の削除が必要になると、そのことが自動的に通知されます。ファイル名の削除は、ホストを選択して実行できます。この処理は排他的に実行する必要があるので、バックアップと同時に実行することはできません。削除処理は Data Protector の以前のバージョンよりも時間がかかります。

- クライアント・システムの変動率が高いか、致命的なレベルに達している場合

  これは、時間経過に伴い新しいファイル名または変更されたファイル名が多くなっていることを意味します。ファイル名が IDB にロギングされている場合には、IDB に影響を及ぼします。[システム処理能力のレポート] により、クライアント・システムの変動率が通知されます (このレポートが事前に構成されている場合)。

- IDB を別の Cell Manager に移動したい場合
- IDB のサイズをチェックしたい場合

[IDB サイズのレポート] により、IDB サイズについての情報が示されます。

- IDB が正しく動作しないため (破損の可能性がある)、その整合性をチェックしたい場合

  [IDB の破損] 通知により、IDB の破損についての情報が示されます。

どの場合にどの保守作業を実行できるかについては、表 11-3 を参照してください。

表 11-3 IDB 保守作業

状況	実行可能なタスク	参照
IDB のスペースが不足している場合	• IDB サイズを拡大する • IDB ファイル名を削除する • IDB サイズの増加を軽減する • IDB の現在のサイズを縮小する	• 「IDB のサイズを拡大する」(517 ページ) • 「古くなったファイル名を削除する」(517 ページ) • 「IDB のサイズの増加を軽減する」(513 ページ) • 「IDB のサイズを縮小する」(514 ページ)
古くなったファイル名が IDB に含まれている場合	• IDB ファイル名を削除する	• 「古くなったファイル名を削除する」(517 ページ)
クライアント・システムの変動率が高いか、致命的なレベルに達している場合	• IDB サイズの増加を軽減する • IDB サイズを拡大する	• 「IDB のサイズの増加を軽減する」(513 ページ) • 「IDB のサイズを拡大する」(517 ページ)
IDB のサイズをチェックしたい場合	• IDB サイズをチェックする	• 「IDB のサイズをチェックする」(520 ページ)
IDB が正しく動作しない (破損の可能性がある) 場合	• IDB の整合性をチェックする	• 「IDB の整合性をチェックする」(521 ページ)
IDB を別の Cell Manager に移動したい場合	• 同一プラットフォーム上の別の Cell Manager に IDB を移動する	• 「別の Cell Manager にデータベースを移動する」(522 ページ)

IDB のサイズの増加を軽減する

IDB のサイズ増加を抑えるには、バックアップ仕様やオブジェクト・コピー仕様のログ・レベルとカタログ保護の設定を低くします。これにより、IDB の現在のサイズは変わりませんが、今後のサイズ増加を抑えることができます。

バックアップの復元時にカタログ保護期間が切れていた場合、ブラウズ機能は利用できません。

カタログ保護期間を短縮する場合は、（カタログ保護期間を超えるバックアップの）復元時にブラウズ機能が使用できなくなることに注意してください。

IDB のサイズ増加と性能に影響する主な要因と調整可能なパラメータ、および推奨される使用例については、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

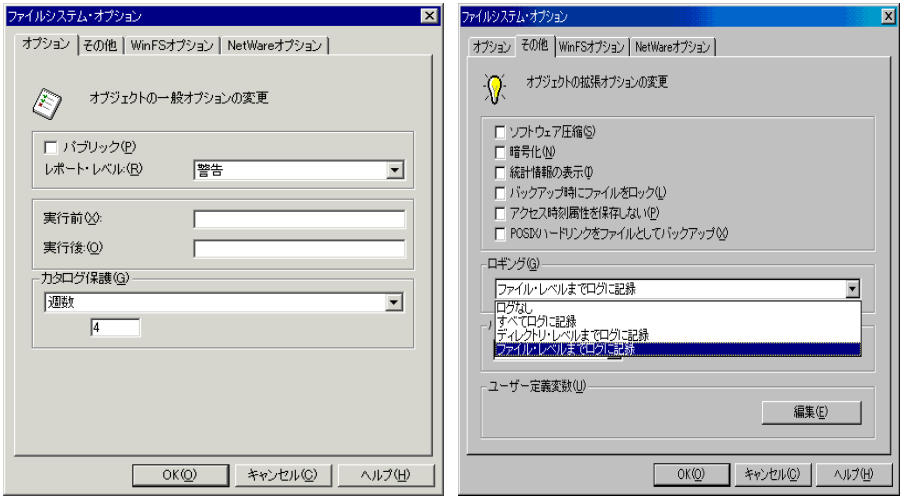
IDB のサイズ増加の軽減方法

［Data Protector Manager］で［Data Protector バックアップ］コンテキストを使用して、ログ・レベルとカタログ保護の設定を変更して、バックアップ仕様を修正します。図 11-6 を参照してください。詳しい手順については、オンライン・ヘルプの索引キーワード「IDB のサイズ増加を抑える」を参照してください。

バックアップ仕様のログ・レベル設定を低くすると、IDB に保存されるデータ (ファイル / ディレクトリ) の量が減ります。ログ・レベルは、高いものから順に［すべてログに記録］ -> ［ファイル・レベルまでログに記録］ -> ［ディレクトリ・レベルまでログに記録］ -> ［ログなし］です。

カタログ保護期間を短縮すると、IDB に保存されている復元時ブラウズ用の情報に対する保護期間のみが短縮されます。メディア上の情報は影響されません。

図 11-6 バックアップのログ・レベルとカタログ保護の設定を変更する



IDB のサイズを縮小する

IDB のサイズは、カタログ保護の設定を変更することで縮小できます。このとき、バックアップ・セッションまたはオブジェクト・コピー・セッション全体 (セッション内のすべてのオブジェクト) を対象とすることも、特定のオブジェクトだけを対象とすることもできます。

カタログ保護期間を短縮する場合は、(カタログ保護期間を超えるバックアップの) 復元時にブラウズ機能が使用できなくなることに注意してください。

この操作は、IDB の今後のサイズ増加には影響しません。

変更内容が適用されるタイミング

変更内容は、以下のタイミングで適用されます。

- メディア上のすべてのオブジェクトからカタログ保護が削除されたとき。
- 古くなったデータが1日1回(デフォルトでは正午) Data Protectorによって自動的に削除されるとき。この時刻は、グローバル・オプション・ファイルの `DailyMaintenanceTime` 変数で、24 時間表記を使って指定できます。「グローバル・オプション・ファイル」(645 ページ) を参照してください。

削除をすぐに開始するには、omnidbutil -purge -dcbf コマンドを実行します。IDB から古くなった他の項目を削除する方法については、omnidbutil の man ページを参照してください。

カタログ保護設定を変更すると、IDB 内の保護設定だけが変更されます。メディア上の情報は影響されません。したがってメディアをいったんエクスポートして再びインポートすると、メディアに保存されているカタログ保護設定がもう一度 Data Protector に読み込まれます。

IDB のサイズの縮小方法

［Data Protector Manager］で［内部データベース］コンテキストを使用して、カタログ保護の設定を変更します。図 11-7 および図 11-8 を参照してください。詳しい手順については、オンライン・ヘルプの索引キーワード「IDB の現在のサイズを縮小する」を参照してください。

図 11-7 セッションのカタログ保護を変更する

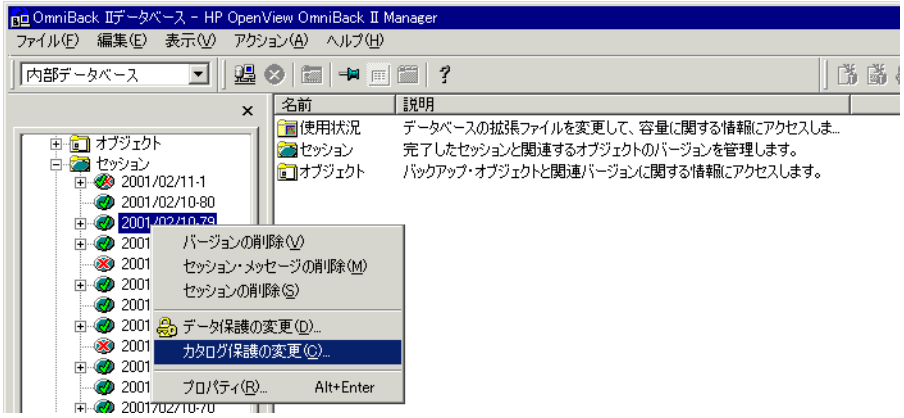
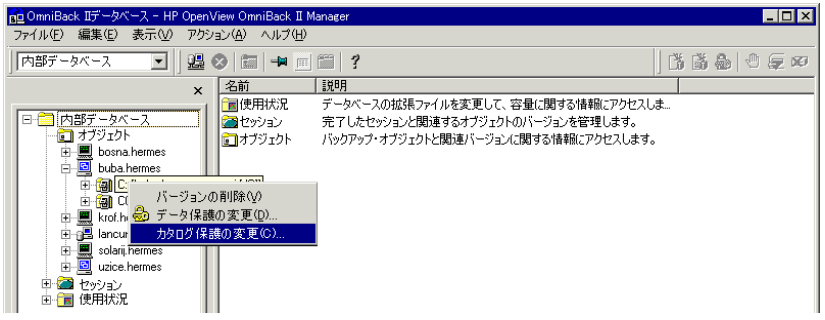


図 11-8 オブジェクトのカタログ保護を変更する



古くなったファイル名を削除する

Data Protector では、削除プロセス中に、IDB 内の古くなったファイル名を自動的に検出して削除します。これによりスペースが解放され、新しい情報を格納できます。古くなったファイル名とは、IDB 内に対応するファイル・バージョンが存在しなくなったファイル名を意味します。

削除に関する詳細な情報は、[IDB の削除プレビュー・レポート] と [IDB 削除レポート] を使用して取得できます。「データベースのレポートと通知を構成する」(507 ページ) を参照してください。

古くなった IDB ファイル名の削除方法

Cell Manager 上で他のバックアップ・セッションが実行されていない状態で IDB を削除します。以下のコマンドを実行してください。

```
omnidbutil -purge -filenames
```

次のコマンドを実行すると、削除対象を 1 つまたは複数の特定のクライアントに絞り込むことができます。

```
omnidbutil -purge -filenames <host_1 ... host_n>
```

Data Protector では、古くなったファイル名が 100 万個未満のクライアント上でのファイル名の削除は行われません。これらのクライアント上でもファイル名を削除するには、-force サブコマンドを使用します。

IDB のサイズを拡大する

以下の場合は、IDB のサイズを拡張する必要があります。

- ファイル名のスペースが消費されており、新しい fnames.dat ファイルが必要、または他のテーブルスペースの拡張が必要な場合
- IDB の詳細パート (ファイル・バージョンと属性) 用のディスク・スペースを増やす必要がある場合

IDB のサイズは、以下の 2 つのうちいずれかの方法で拡張できます。

- 新しい DC(詳細カタログ) ディレクトリを作成し、可能な場合は、それを別のディスク上に配置する。
- fnames.dat ファイルを新たに作成して追加する。
- 他のテーブルスペースを拡張する。

新しい DC ディレクトリを作成する

[Data Protector Manager] の [内部データベース] コンテキストを使用して、DC ディレクトリを作成します。図 11-3 (503 ページ) を参照してください。詳しい手順については、オンライン・ヘルプの索引キーワード「DC ディレクトリの作成」を参照してください。

新しい fnames.dat ファイルを作成する

fnames.dat ファイルとは

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。通常、これらのファイルは IDB の約 20%を占めます。fnames.dat ファイルのデフォルト・サイズは 2GB、最大サイズは 32GB です

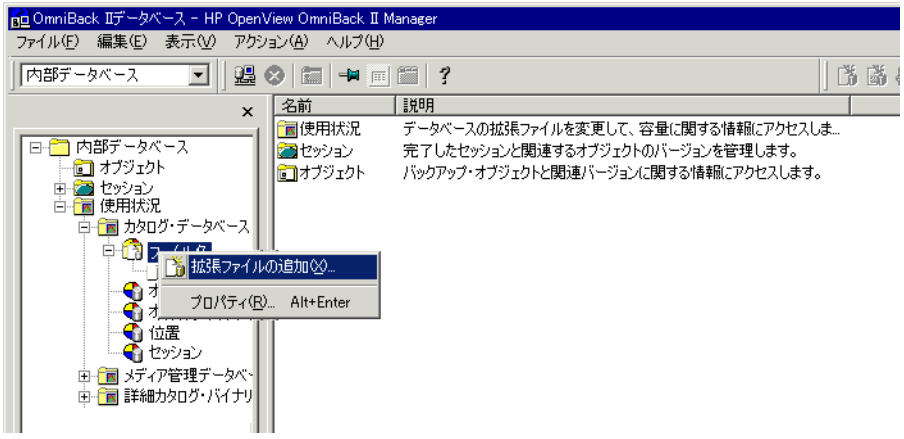
fnames.dat ファイルの作成方法

[Data Protector Manager] の [内部データベース] コンテキストを使用して、新しい fnames.dat ファイルを追加します。図 11-9 を参照してください。詳しい手順については、オンライン・ヘルプの索引キーワード「fnames.dat ファイルの作成」を参照してください。

Windows Cell Manager では、拡張ファイルは IDB と同じ論理ディスク上に作成することをお勧めします。

IDB 拡張ファイルは、IDB バックアップの一部としてバックアップされ、IDB 復旧を使用して復元されます。

図 11-9 新しい fnames.dat ファイルの作成



他のテーブルスペースを拡張する

デフォルトでは、特定のテーブルスペースに割り当てられたスペースの 85% が使用されると、[IDB テーブル・スペースのスペース不足] が通知されます。特定のテーブルスペースを拡張する方法については、オンライン・ヘルプの索引キーワード「IDB サイズの拡張」を参照してください。

IDB のサイズをチェックする

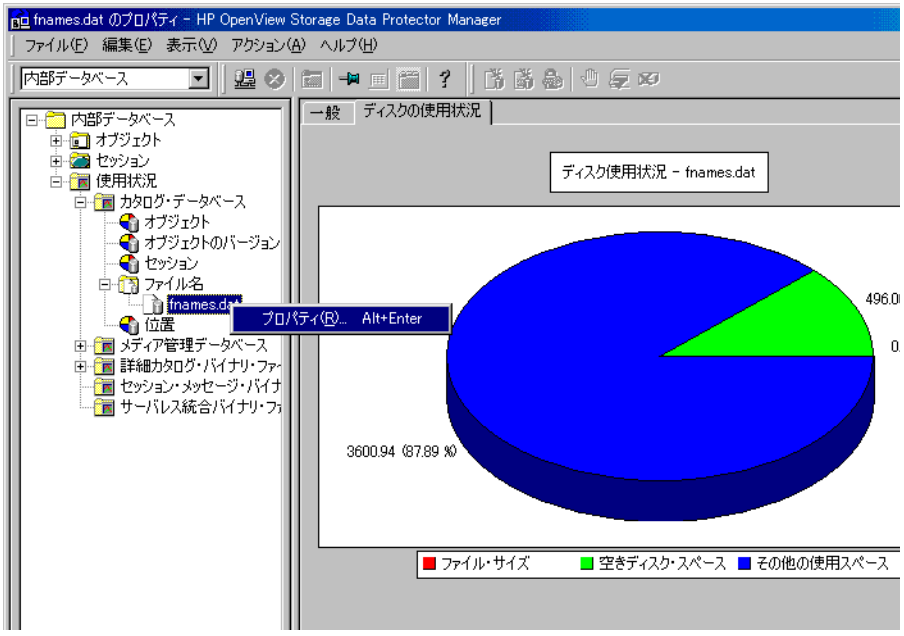
IDB の現在のサイズは、Data Protector GUI を使ってチェックできます。

また、[IDB・サイズのレポート] や、[IDB のスペース不足] および [IDB テーブル・スペースのスペース不足] 通知により、IDB のサイズが通知されます (これらを事前に構成しておいた場合)。

IDB のサイズのチェック方法

[Data Protector Manager] の [内部データベース] コンテキストを使用して、IDB の各パート (CDB、MMDB、DCBF、SMBF、SIBF) のサイズをチェックします。図 11-10 を参照してください。詳しい手順については、オンライン・ヘルプの索引キーワード「IDB サイズのチェック」を参照してください。

図 11-10 fnames.dat ファイル (CDB パート) のサイズをチェック



IDB の整合性をチェックする

Data Protector のデフォルトでは、IDB のバックアップ前に IDB の整合性がチェックされます。これは、障害発生時に IDB とバックアップ・データを復旧する上で非常に重要です。

さらに、以下の IDB チェックを手動で実行することも可能です。

IDB のコア・部分のチェック	ファイル名情報を含まないメディア管理データベース (MMDB) パートとカタログ・データベース (CDB) パートをチェックします。中規模の IDB の場合、約 5 〜 10 分かかります。チェックするには、`omnidbcheck -core` コマンドを実行します。
ファイル名チェック	ファイル名に関する IDB 情報をチェックします。中規模の IDB の場合、約 1 時間かかります。チェックするには、`omnidbcheck -filename` コマンドを実行します。
DCBF 部分の簡易チェック	DC バイナリ・ファイルの有無とそのサイズをチェックします。中規模の IDB の場合、約 10 〜 30 秒かかります。チェックするには、`omnidbcheck -bf` コマンドを実行します。
DCBF 部分の完全チェック	メディア位置と DC バイナリ・ファイルの整合性をチェックします。DCBF パートの 1GB ごとに約 10 分かかります。チェックするには、`omnidbcheck -dc` コマンドを実行します。
SMBF 部分のチェック	セッション・メッセージ・バイナリ・ファイルの有無をチェックします。チェックするには、`omnidbcheck -smbf` コマンドを実行します。
SIBF 部分のチェック	オブジェクト・バージョンとサーバレス統合バイナリ・ファイル (SIBF) の整合性をチェックします。SIBF パートの 1GB ごとに約 10 分かかります。チェックするには、`omnidbcheck -sibf` コマンドを実行します。
クイック・チェック	コア・パート (MMDB と CDB)、ファイル名、および DCBF パートをチェックします。中規模の IDB の場合、約 2 時間半かかります。チェックするには、`omnidbcheck -quick` コマンドを実行します。

拡張チェック　コア・パート (MMDB と CDB)、ファイル名、DCBF パート、および DC パートをチェックします。チェックするには、`omnidbcheck - extended` コマンドを実行します。

IDB の使用中に問題が生じた場合、トラブルシューティングに関する項「IDB のトラブルシューティング」(745 ページ) と「IDB を復旧する」(527 ページ) を参照してください。

別の Cell Manager にデータベースを移動する

IDB は、同じオペレーティング・システム上で動作する別の Cell Manager に移動できます。以下の手順を行います。

1. ソース・システムとターゲット・システムの両方で `omnisv -stop` コマンドを実行し、すべての Data Protector サービスを終了します。

   - Windows の場合 : `<Data_Protector_home>¥bin¥omnisv -stop`
   - UNIX の場合 : `/opt/omni/sbin/omnisv -stop`

   IDB が MC/ServiceGuard 上にインストールされている場合は、アクティブなノード上で `cmhaltpkg <pkg_name>` コマンドを実行し、Data Protector パッケージを終了します。ここで、*<pkg_name>* は Data Protector クラスター・パッケージの名前を示します。

   IDB が Microsoft Cluster Server にインストールされている場合は、アクティブなノード上でクラスター・アドミニストレータユーティリティを使用して、`OBVS_VELOCIS` クラスター・グループをオフラインにし、`Inet` サービスを停止します。

2. 以下の IDB ファイルをターゲット・システムにコピーします。

   - テーブルスペースは、同じ相対パス名にコピーします。

     Windows の場合 : `<Data_Protector_home>¥db40¥datafiles` → `<Data_Protector_home>¥db40¥datafiles`

     UNIX の場合 : `/var/opt/omni/server/db40/datafiles` → `/var/opt/omni/server/db40/datafiles`

- 拡張ファイルは、ソース・システム上の拡張ファイルと同じフル・パス名にコピーします。このファイルのリストを入手するには、omnidbutil -extendinfo コマンドを使用します。
- SMBF ファイルは、同じ相対パス名にコピーします。

  Windows の場合 : *<Data_Protector_home>*¥db40¥msg → *<Data_Protector_home>*¥db40¥msg

  UNIX の場合 : /var/opt/omni/server/db40/msg → /var/opt/omni/server/db40/msg
- SIBF ファイルは、同じ相対パス名にコピーします。

  Windows の場合 : *<Data_Protector_home>*¥db40¥meta → *<Data_Protector_home>*¥db40¥meta

  UNIX の場合 : /var/opt/omni/server/db40/meta → /var/opt/omni/server/db40/meta
- DC ディレクトリは、同じ場所にも、異なる場所にもコピーできます。DC ディレクトリのリストは、omnidbutil -list_dcdir コマンドで取得できます。

3. ターゲット・システム上で omnisv -start コマンドを使って、Data Protector サービスを起動します。
   - Windows の場合: *<Data_Protector_home>*¥bin¥omnisv -start
   - UNIX の場合 : /opt/omni/sbin/omnisv -start

   IDB が MC/ServiceGuard 上にインストールされている場合、アクティブなノード上で cmrunpkg *<pkg_name>* コマンドを実行し、Data Protector パッケージを起動します。

   IDB が Microsoft Cluster Server にインストールされている場合は、クラスター・アドミニストレータユーティリティを使用して、OBVS_VELOCIS と OBVS_MCRS クラスター・グループをオンラインにし、Inet サービスを起動します。
4. omnidbutil -change_cell_name コマンドを実行します。
5. ターゲット・システム上の DC ディレクトリの位置を変更します。
6. omnidbutil -remap_dcdir コマンドを実行し、DC ディレクトリの新しい位置を Data Protector に認識させます。

IDB の復元

標準的な手順で IDB をバックアップした場合は、本項で説明する方法で IDB を復元できます。

障害発生時の IDB 復元処理の詳細は、「IDB を復旧する」（527 ページ) を参照してください。

IDB の復元は、以下の 2 段階で構成されます。

1. IDB を一時ディレクトリに復元します。

重要

このステップは、復元時にも IDB は使用中であるため必要となります。IDB を元のディレクトリに復元しようとすると、IDB が破損してしまいます。

2. IDB を元のディレクトリに移動します。

この処理を行う前に、十分なディスク・スペースがあることを確認してください。

IDB を一時ディレクトリに復元する

IDB ファイルを一時ディレクトリに復元するには、以下の手順で行います。

1. ［Data Protector Manager］ で［復元］コンテキストを選択します。
2. ［内部データベース］項目を展開します。
3. IDB をバックアップするクライアント・システムを展開し、データベース・オブジェクトをクリックして［ソース］プロパティ・ページを表示します。
4. ［ソース］プロパティ・ページで復元したい IDB ディレクトリを選択します。デフォルトでは最新のバックアップ・バージョンが復元用に選択されます。別のバージョンを復元したい場合は、選択したディレクトリを右クリックして、［バックアップ・バージョン］をクリックします。［バックアップ・バージョン］ドロップダウン・リストから復元したいバックアップ・バージョンを選択して［OK］をクリックします。

5. [あて先] プロパティ・ページで [新しいディレクトリに復元] オプションを選択し、IDB ファイルの一時ディレクトリを選択します (例 : temp ディレクトリ)。

注記

ここで、*<Data_Protector_home>* ディレクトリを選択しないでください。これは IDB のオリジナル・ディレクトリです。

別のシステムに復元したい場合は、新しい Cell Manager の名前を指定します。

6. [復元] をクリックします。

IDB を元のディレクトリに移動する

IDB を一時ディレクトリに復元したら、IDB ディレクトリを元のディレクトリに移動します。以下の手順を行います。

UNIX Cell Manager の場合

1. 実行中のすべての Data Protector セッションを停止して、Data Protector GUI を閉じます。これにより IDB へのアクセスを防止します。
2. 以下のコマンドを実行して、すべての Data Protector プロセスを停止します。

   ```
   /opt/omni/sbin/omnisv -stop
   ```

3. 既存の IDB ディレクトリを移動します。

   `/var/opt/omni/server/db40` および `/etc/opt/omni/server`

   これにより、新旧のファイルが混ざるのを防止します。

4. IDB ディレクトリを、一時ディレクトリから元のディレクトリにコピーします。

   `/var/opt/omni/server` および `/etc/opt/omni/server`

   拡張ファイルが別のディレクトリにある場合は、それらも必ず元のディスクの元のディレクトリにコピーしてください。

5. 以下のコマンドを実行して、すべての Data Protector プロセスを再起動します。

   ```
   /opt/omni/sbin/omnisv -start
   ```

注記

既存の Cell Manager を IA-64 ベースの HP-UX 11.23 システムに移行する作業の一部として、IDB を元の場所に移動する場合は、Data Protector サービスを再起動する必要はありません。

Windows Cell Manager の場合

1. 実行中のすべての Data Protector セッションを停止して、Data Protector GUI を閉じます。これにより IDB へのアクセスを防止します。
2. 以下のコマンドを実行して、すべての Data Protector サービスを停止します。

   ```
   <Data_Protector_home>¥bin¥omnisv -stop
   ```

3. 既存の IDB ディレクトリ (db40 および config) を *<Data_Protector_home>* ディレクトリから移動します。これにより、新旧のファイルが混ざるのを防止します。
4. IDB ディレクトリを、一時ディレクトリから元のディレクトリ *<Data_Protector_home>* にコピーします。

   拡張ファイルが別のディレクトリにある場合は、それらも必ず元のディスクの元のディレクトリにコピーしてください。
5. 以下のコマンドを実行して、すべての Data Protector サービスを再起動します。

   ```
   <Data_Protector_home>¥bin¥omnisv -start
   ```

ヒント

復元後、IDB の整合性をチェックできます。詳細は「IDB の整合性をチェックする」(521 ページ) を参照してください。

IDB を復旧する

復旧が必要になる場合

一部またはすべての IDB ファイルが使用不可能になった場合や破損した場合は、IDB の復旧が必要になります。

IDB の問題には 3 つのレベルがあり、それぞれの修復方法があります。

- ファイルシステムがマウントされていないことやネームサービスの障害など、OS の構成に原因があって IDB に発生した問題に対しては、トラブルシューティングを行います。トラブルシューティングに関する項「IDB のトラブルシューティング」(745 ページ) を参照してください。
- IDB のうち、コア以外のパート (バイナリ・ファイルやファイル名パート) に問題がある場合は、それらを除外または削除します。このように処置できるのは、IDB の破損レベルが [軽度] または [重度] の場合 (つまり、IDB のコア・パートが破損していない場合) だけです。
- 完全回復を実行します。この作業は、IDB の復元と、前回の IDB バックアップからの IDB の更新で構成されます。IDB の破損レベルが [致命的] の場合 (コア・パートが破損している場合) には、必ずこの処置を行います。

完全回復

完全回復は、以下の 2 段階で構成されます。

1. IDB を復元して、IDB を最後の (利用可能な) 整合状態に戻します。
2. IDB を最後の整合状態から IDB が動作していた最後の時点の状態まで更新します。

復元の手順は、問題が発生する前に IDB 復旧にどの程度まで備えていたか (IDB 回復ファイル、IDB バックアップ、オリジナルのデバイス、およびトランザクション・ログが利用可能かどうか) によって異なります。これらがすべて利用可能であれば、ガイド式自動回復機能を使って IDB を簡単に復旧できます。

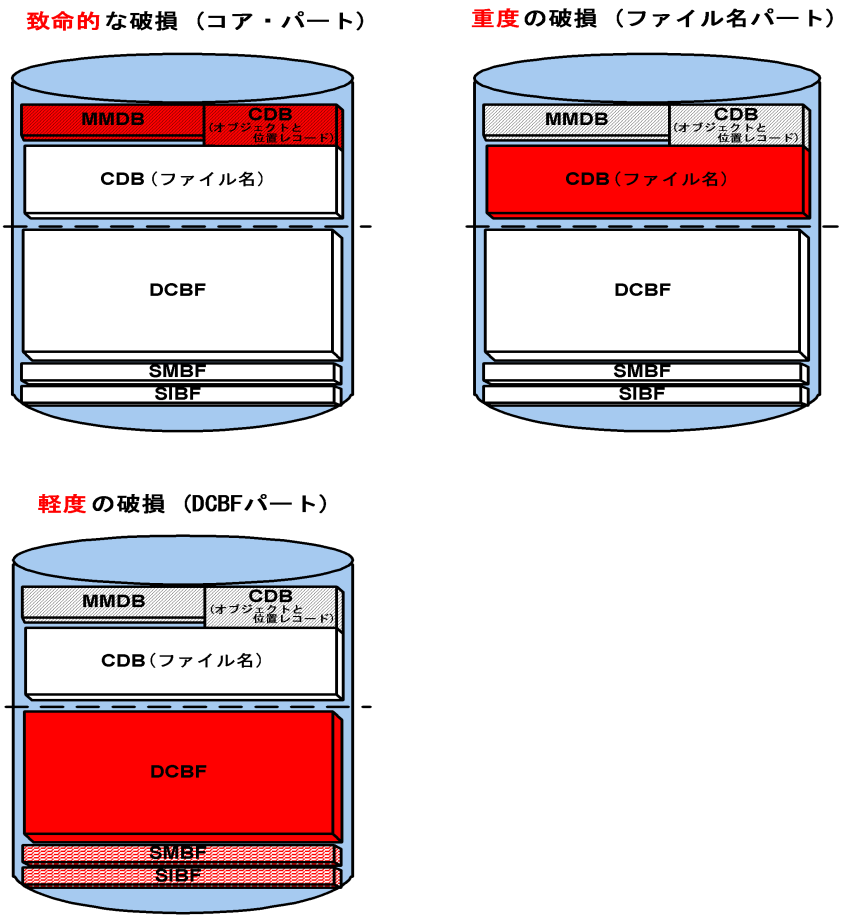
データベースの破損レベルを特定する

IDB 破損レベル

IDB には、[致命的]、[重度]、[軽度] の 3 つの破損レベルがあります。IDB のどのパートで破損が発生したかに応じて、レベルが決まります。

IDB 整合性チェックを実行すると、IDB のどのパートが破損しているかを確認できます。IDB の復旧手順は、破損レベルによって異なります。

図 11-11 **IDB 破損レベル**



破損レベルの特定

方法 `omnidbcheck -extended` コマンドを使って、IDB の破損レベルを特定します。

注記

上記のコマンドで拡張チェックを行うと数時間を要することがあります。システム・ダウンタイムが長くなるのを避けるには、omnidbcheck コマンドの実行対象を制限できます。たとえば omnidbcheck -core を実行することで、IDB のコア・パートが破損しているかどうかを確認できます。

破損のレベルを特定したら、レベルに対応する方法で復旧を実行します。「IDB 復旧方法の概要」(529 ページ) を参照してください。

IDB 復旧方法の概要

IDB の復旧には複数の方法があります。破損のレベルや必要条件によって、また、IDB 回復ファイル、オリジナルのデバイス、およびトランザクション・ログがそれぞれ利用可能かどうかによって、復旧手順に違いがあります。

最も効率的な完全回復

IDB 全体が失われたか、またはコア・パートが破損している場合、IDB の破損レベルは [致命的] です。IDB 回復ファイル、および IDB バックアップに使用したオリジナル・デバイスが利用できる場合は、ガイド式自動回復 (IDB 復元とログ再生) を実行することができます。「ガイド式自動回復を実行する」(534 ページ) を参照してください。そうでない場合は、「その他の復旧方法」(530 ページ) に示す方法のいずれかを実行してください。

ガイド式自動回復では、指示に従って、IDB の復元とトランザクション・ログの再生を行えます。トランザクション・ログが利用できない場合でも、最後のバックアップ以降に使用されたメディアをすべてインポートすれば IDB を更新できます。

破損した IDB のパートの除外 (削除)

破損レベルが [重度] または [軽度] の場合 (コア・パートが破損していない場合) は、IDB 全体を復旧する代わりに、IDB のうち、失われた、または破損したパートを除外 (削除) することもできます。

ファイル名テーブルスペースが破損している場合、IDB の破損レベルは [重度] です。「ファイル名パートの [重度] レベルのデータベース破損に対処する」(532 ページ) を参照してください。

DC バイナリ・ファイルが失われた、または破損している場合、IDB の破損レベルは [軽度] です。「DCBF パートの [軽度] レベルのデータベース破損に対処する」(531 ページ) を参照してください。

その他の復旧方法

ここでは、特定の状況に適用する復旧手順を示します。IDB 全体を復旧したいが、何らかの理由でガイド式自動回復機能を実行できない場合には、これらの手順で対処できます。復旧手順は、IDB の復元と更新で構成されます。

表 11-4 IDB の復元

現在の状況	備考	復旧手順
IDB 回復ファイルは利用できるが、IDB のバックアップに使用したオリジナルのデバイスが変更されている。	この方法は、基本的にガイド式自動回復と同じですが、ガイド内容が少なく手順が複雑になっており時間もかかります。	「IDB 回復ファイルと新しいデバイスを使って IDB を復旧する」(536 ページ).
IDB 回復ファイルが利用できない。	この方法は、基本的にガイド式自動回復と同じですが、ガイド内容が少なく手順が複雑になっており時間もかかります。	「IDB 回復ファイルを使わずに IDB を復旧する」(537 ページ).
特定の IDB バックアップ (最新ではないバックアップ) から IDB を復旧したい。	この方法では、IDB が最新の状態に復元されません。	「特定の IDB セッションから IDB を復旧する」(539 ページ).
別のディスク・レイアウトに復旧したい。	この方法は、IDB トランザクション・ログ、IDB 回復ファイル、および `media.log` ファイルが失われた場合に Data Protector 構成から行う障害復旧と同じです。ガイド式自動回復よりも手順が複雑な上、IDB は最新の状態に復元されません。	「IDB を別のディスク・レイアウトに復元する」(540 ページ).

トランザクション・ログが利用できる場合、表 11-4 の復旧手順に従って、IDB トランザクション・ログを再生します。「IDB トランザクション・ログを再生する」(541 ページ) を参照してください。

トランザクション・ログが利用できない場合でも、メディアをインポートすると、IDB を更新できます。「メディアをインポートして IDB を更新する」(543 ページ) を参照してください。

DCBF パートの [軽度] レベルのデータベース破損に対処する

IDB に重度 [軽度] の破損が検出された場合は、一部の DC バイナリ・ファイルが失われている、または破損していることを意味します。したがって、IDB 全体を復旧する必要はありません。バイナリ・ファイルは、メディアからカタログをインポートすることで簡単に再作成できます。破損の種類に応じた復旧手順を選択してください。

DC バイナリ・ファイルが失われた場合の復旧

DC バイナリ・ファイルは、メディアごとに 1 つずつ作成されます。一部の DC バイナリ・ファイルが失われている場合は、一部のメディアのメディア位置が、存在しないファイルを参照しています。この場合、そのファイルに関連するファイルシステムをブラウズすると、エラー・メッセージが表示されます。以下の手順を行います。

1. `omnidbcheck -bf` コマンドの出力から、失われたバイナリ・ファイルのメディア ID を特定します。また、`omnimm -media_info` *<Medium>* コマンドを実行すると、その他のメディア属性 (メディア・ラベルやメディア・プールなど) を確認できます。
2. `omnidbutil -fixmpos` コマンドを実行して、メディア位置 (mpos) とバイナリ・ファイル間の整合性を確立します。
3. メディアからカタログをインポートしてバイナリ・ファイルを再作成します。「メディアからのカタログのインポート」(170 ページ) を参照してください。

DC バイナリ・ファイル破損時の復旧

一部の DC バイナリ・ファイルが破損している場合は、それらの DC バイナリ・ファイルをいったん削除してから再作成することで対処できます。ファイルを削除すると、一部のメディア位置が存在しないバイナリ・ファイルを参照することになるため、そのファイルに関連するファイルシステムのブラウズ時にエラー・メッセージが表示されますが、それ以外の影響はありません。以下の手順を行います。

1. omnidbcheck -dc コマンドの出力から、破損した DC バイナリ・ファイルのメディア ID を特定します。また、omnimm -media_info *<Medium>* コマンドを実行すると、その他のメディア属性 (メディア・ラベルやメディア・プールなど) を確認できます。
2. 上記で特定したメディアの DC バイナリ・ファイルを特定します。DC バイナリ・ファイル名は、*<Medium>*_*<TimeStamp>*.dat の形式をとります。なお、*<Medium>* に含まれるコロン (:) は下線 (_) に置き換わります。
3. 破損した DC バイナリ・ファイルを削除します。
4. omnidbutil -fixmpos コマンドを実行して、メディア位置 (mpos) とバイナリ・ファイル間の整合性を確立します。
5. メディアからカタログをインポートしてバイナリ・ファイルを再作成します。「メディアからのカタログのインポート」(170 ページ) を参照してください。

ファイル名パートの [重度] レベルのデータベース破損に対処する

重大度が [重度] の破損が検出された場合は、ファイル名テーブルスペースが破損しています。この場合は、IDB 全体を復旧する代わりに詳細カタログ (ファイル名と DC バイナリ・ファイル) を削除することで対処できます。

この手順は短時間で完了し、IDB が詳細カタログなしの状態で復元されます (すべてのバックアップの作成時に [ログなし] オプションが指定されていた場合と同じ結果になります)。この IDB は、ブラウジングできない (バックアップ・データの情報はメディアから読み込む必要があります) ことを除いて、バックアップ、復元、メディア管理操作はすべて可能です。

この復旧方法は、すべての詳細カタログが失われることになるので、以下の場合だけに使用してください。

- 以降のバックアップで作成されたカタログが十分良好な場合
- 利用可能な IDB バックアップが存在しない場合

復旧手順

それ以降は、以下の手順を行います。

1. 以下のコマンドを実行します。

```
omnidbutil -writedb -no_detail -cdb <Directory> -mmdb
<Directory>
```

上記のコマンドを実行すると、詳細カタログを除いた IDB が ASCII ファイルに書き込まれます。

2. 以下のコマンドを実行します。

```
omnidbutil -readdb -cdb <Directory> -mmdb <Directory>
```

上記のコマンドを実行すると、ASCII ファイルから IDB が読み込まれます。

この処理が完了するまでに、約 5 ～ 20 分かかります。

詳細カタログの削除後、すべての DC バイナリ・ファイルを削除できますが、DC ディレクトリは登録されたままになります。以降のバックアップでは、DC バイナリ・ファイルにファイル・バージョンが保存されます。

IDB 復旧の準備

- 障害発生時前と同じサイズのディスクを、IDB バックアップ時と同じディレクトリ (Windows の場合は、ドライブも同じ) にマウントします。これを確実に行えない場合は、IDB を別のディスク / ボリューム・レイアウトに復元する手順に従ってください。`omnidbrestore` コマンドの `-preview` オプションを使うと、ファイルの復元先を事前に確認できます。
- Cell Manager 上およびデバイス (なるべく IDB バックアップに使用したもの) が接続されているシステム上に Data Protector がインストールされていることを確認します。
- 可能であれば、既存の `media.log` ファイルを安全な場所に保存しておきます。このファイルには、前回の IDB バックアップ以降に使用されたメディアに関する情報が含まれています。トランザクション・ログが利用できない場合は、このファイルが IDB の更新に大きく役立ちます。
- IDB が MC/ServiceGuard 上にインストールされている場合は、復旧を実行する前に、アクティブなノード上で次のコマンドを実行する必要があります。

  1. `cmhaltpkg <pkg_name>` 。ここで、*<pkg_name>* は Data Protector クラスターパッケージの名前を示します。

このコマンドによって Data Protector パッケージは停止され、Data Protector 共有ボリューム・グループがアンマウントされます。

2. `vgchange -a e /dev/<vg_name>`。ここで、*<vg_name>* は Data Protector 共有ボリューム・グループの名前を示します。

   このコマンドにより、Data Protector 共有ボリューム・グループが使用可能になります。システム上のボリューム・グループを表示するには次のコマンドを実行します。`ll /dev/*/group`

3. `mount /dev/<vg_name>/<lv_name>/<MountPoint>`。ここで、*<MountPoint>* は Data Protector 共有ボリューム・グループのマウント・ポイント名を示します。

   このコマンドにより、Data Protector 共有ボリューム・グループがマウントされます。

ガイド式自動回復が完了したら、アクティブなノード上で `cmrunpkg <pkg_name>` コマンドを実行し、Data Protector パッケージを起動します。

- IDB が Microsoft Cluster Server にインストールされている場合は、復旧を実行する前に、アクティブなノード上でクラスター・アドミニストレータユーティリティを使用して、`OBVS_VELOCIS` クラスター・グループをオフラインにし、`Inet` サービスを停止します。

  復旧が完了したら、クラスター・アドミニストレータユーティリティを使用して、`OBVS_VELOCIS` と `OBVS_MCRS` クラスター・グループをオンラインにし、`Inet` サービスを起動します。

ガイド式自動回復を実行する

IDB を復旧する最も便利な方法は、ガイド式自動回復機能を使う方法です。IDB 回復ファイル、IDB バックアップ作成時のオリジナル・デバイス、IDB バックアップ・メディアがすべて利用可能であれば、ガイド式自動回復機能を使用できます。

この方法では、指示に従って、IDB の復元、および最後の IDB バックアップ以降のトランザクション・ログの再生を行えます。トランザクション・ログが利用できない場合でも、メディアをインポートすれば最後の IDB バックアップから IDB を更新できます。

トランザクションを再生すると、IDB のコア・パートが更新されます。ただし、バイナリ・ファイルは更新されないので、バイナリ・ファイルの変更内容は失われます。

最後の IDB バックアップから IDB 破損までの間に実行されたバックアップについては、以下の項目が利用できなくなります。

- セッション・メッセージ
- ファイル・バージョンのブラウズ (オブジェクト全体の復元は可能です)。バックアップに使用したメディアに対してカタログのインポートを実行すると、変更内容を復旧できます。
- SIBF の更新内容。バックアップに使用したメディアをエクスポートおよびインポートすると、変更内容を復旧できます。

必要条件

詳細は、「IDB 復旧の準備」(533 ページ) を参照してください。

クラスター

クラスターにインストールされている IDB の復元を行う場合には、特別な手順が必要となります。「IDB 復旧の準備」(533 ページ) を参照してください。

復旧手順

IDB を復旧するには、`omnidbrestore -autorecover` コマンドを実行します。

このコマンドによって IDB 回復ファイルが読み込まれます。IDB バックアップが回復ファイルに記録されている場合は、サービスが終了し、IDB の元の位置への復元が開始されます。オプションはすべて、IDB 回復ファイルからのデータを使用して自動的に生成されます。

復元が完了したら、トランザクション・ログが再生可能かどうか `omnidbrestore` コマンドでチェックします。ログが利用できる場合、ログの再生を確認するよう求められます。この手順をキャンセルした場合、またはトランザクション・ログが利用できない場合は、以下の方法で前回の IDB バックアップから IDB を更新する手順が表示されます。

- メディアのインポート
- トランザクション・ログを検索し、後で再生する

ログを再生するか、またはメディアをインポートして IDB を更新し終えたら、IDB 全体が正常に復旧されます。

IDB 回復ファイルと新しいデバイスを使って IDB を復旧する

IDB 回復ファイル (obrindex.dat) が利用できる場合で、IDB バックアップ作成時に使用されたオリジナル・デバイスが復旧に使用するデバイスと異なるとき、またはメディアが異なるスロットに格納されているときは、この手順に従って IDB を復旧します。

必要条件

詳細は、「IDB 復旧の準備」(533 ページ) を参照してください。

クラスター

クラスターにインストールされている IDB の復元を行う場合には、特別な手順が必要となります。「IDB 復旧の準備」(533 ページ) を参照してください。

復旧手順

1. 以下のコマンドを、復元ジョブ・オプションを付けて実行し、テキスト・ファイルを作成します。

   ```
   omnidbrestore -logview -autorecover -skiprestore -save
   C:¥TEMP¥restjob.txt
   ```

重要

コマンドで -logview を指定すると、セッション ID の隣に、最初のトランザクション・ログが表示されます。復元したいセッションの最初のトランザクション・ログを記録しておいてください。復元の後、IDB を更新するために必要です。たとえば、2001/02/09-2 セッションを復元するには、2001/02/09-2 AAAAAAH という出力から、最初のトランザクション・ログ AAAAAAH を覚えておく必要があります。

作成した restjob.txt ファイルには、オリジナルのデバイスに関する情報と、IDB バックアップ時にメディアが格納されていたスロットに関する情報が含まれています。

たとえば、IDB バックアップが SCSI アドレス scsi0:0:0:0 の DDS ドライブ上で行われた場合、以下のようなファイルが作成されます。

```
-name LDEV
-policy 1
-type 1
-dev scsi0:0:0:0
-mahost goedl.hermes
-maid 0100007f:3a486bd7:0410:0001
```

```
-position 3:0
-daid 977824764
```

2. restjob.txt ファイルを変更し、現在のデバイス、またはメディアが現在格納されているスロットを指定します。

   たとえば、DDS ドライブの SCSI アドレスが、バックアップ時には scsi0:0:0:0 で、復元時には scsi0:0:1:0 になっている場合、restjob.txt ファイルをそのように変更する必要があります。

   ```
   -name LDEV
   -policy 1
   -type 1
   -dev scsi0:0:1:0
   -mahost cm.dom.com
   -maid 0100007f:3a486bd7:0410:0001
   -position 3:0
   -daid 977824764
   ```

3. omnidbrestore -read C:¥TEMP¥restjob.txtコマンドで復元を実行します。

このコマンドでは、指示に従って、IDB の復元、および最後の IDB バックアップ以降のトランザクション・ログの再生を行えます。

トランザクション・ログが利用できない場合でも、最後のバックアップ以降に使用されたメディアをすべてインポートすれば IDB を更新できます。「メディアをインポートして IDB を更新する」(543 ページ) 参照してください。

IDB 回復ファイルを使わずに IDB を復旧する

IDB 回復ファイル (obrindex.dat) が利用できない場合、この手順に従って IDB を復旧します。

必要条件

詳細は、「IDB 復旧の準備」(533 ページ) を参照してください。

クラスター

クラスターにインストールされている IDB の復元を行う場合には、特別な手順が必要となります。「IDB 復旧の準備」(533 ページ) を参照してください。

復旧手順

1. [Data Protector Manager] を使ってデバイスを構成します。
2. 最新の IDB バックアップが含まれているメディアを見つけます。
3. メディアをデバイスに挿入し、以下のコマンドを使ってメディアの内容を表示します。

   ```
   omnimlist -dev <LogicalDevice>
   ```

   IDB 復元に必要な情報は、復元するバックアップ・セッションのメディア ID と Disk Agent ID です。
4. 以下のコマンドを使って、デバイス構成に関する情報を表示します。

   ```
   omnidownload -dev <LogicalDevice>
   ```

   IDB 復元に必要な情報は、以下のとおりです。

   - Mahost (Media Agent ホスト)
   - ポリシー (番号)

     ポリシー番号を指定します。スタンドアロン・デバイスの場合は 1、スタッカー・デバイスの場合は 3、SCSI ライブラリの場合は 10、ジュークボックス・デバイスの場合は 5 です。
   - メディアの種類 (番号)

     メディアの種類の番号を指定します。DDS は 1 、ExaByte は 3 、DLT は 10、ファイルは 7 です。
   - SCSI アドレス
   - ロボティクスの SCSI アドレス (エクスチェンジャ・ライブラリ・デバイスを使用する場合のみ必要)
5. 取得した情報を使用して omnidbrestore コマンドを実行します。

   ```
   omnidbrestore -policy <log. device policy> -type <log.
   device_type> [-ioctl <RoboticsDevice>] -dev <PhysicalDevice>
   -mahost <DeviceHostname> -maid <mediumID> -daid <DAID>
   ```

   次の例では、メディア ID として 0100007f:3a486bd7:0410:0001 を指定し、Disk Agent ID として 977824764 を指定してバックアップ・セッションから IDB を復元します。このバックアップは、DLT メディアのスタンドアロン・デバイスを使用して実行されたものです。このデバイスは、cm.dot.com というシステムに接続されており、SCSI アドレスは scsi0:1:2:0 です。

```
omnidbrestore -policy 1 -type 10 -dev scsi0:1:2:0 -mahost
cm.dom.com -maid 0100007f:3a486bd7:0410:0001 -daid  977824764
```

このコマンドでは、指示に従って、IDB の復元、および最後の IDB バックアップ以降のトランザクション・ログの再生を行えます。

トランザクション・ログが利用できない場合でも、最後のバックアップ以降に使用されたメディアをすべてインポートすれば IDB を更新できます。「メディアをインポートして IDB を更新する」（543 ページ) 参照してください。

特定の IDB セッションから IDB を復旧する

IDB 回復ファイル (obrindex.dat) が利用できる場合、最新のバックアップ以外のバックアップを使用して IDB を復旧するには、この手順に従います。

必要条件

詳細は、「IDB 復旧の準備」（533 ページ) を参照してください。

クラスター

クラスターにインストールされている IDB の復元を行う場合には、特別な手順が必要となります。「IDB 復旧の準備」（533 ページ) を参照してください。

復旧手順

1. 以下のコマンドを使って、すべてのバックアップをチェックします。

   ```
   omnidbrestore -autorecover -logview -skiprestore
   ```

2. どのバックアップ・セッションのデータを復元するかを選択し、`omnidbrestore -autorecover -session <sessionID>` コマンドを実行して復元を実行します。

   たとえば、バックアップ・セッション 2000/12/26-1 からデータを復元することを選択し、IDB バックアップに使用されたオリジナル・デバイスが存在する場合は、以下を実行します。

   ```
   omnidbrestore -autorecover -session 2000/12/26-1
   ```

   このコマンドでは、指示に従って、IDB の復元、および最後の IDB バックアップ以降のトランザクション・ログの再生を行えます。トランザクション・ログが利用できない場合でも、最後のバックアップ以降に使用されたメディアをすべてインポートすれば IDB を更新できます。「メディアをインポートして IDB を更新する」（543 ページ) 参照してください。

3. クラスター・アドミニストレータユーティリティを使用して、OBVS_VELOCIS と OBVS_MCRS クラスター・グループをオンラインにし、Inet サービスを起動します。
4. omnidbutil -fixmpos コマンドを実行します。

IDB を別のディスク・レイアウトに復元する

障害発生前とは別のサイズのディスク、およびバックアップ時とは別のディレクトリに、IDB を復元することができます。

必要条件

詳細は、「IDB 復旧の準備」(533 ページ) を参照してください。

さらに、IDB を別のディスク・レイアウトに復旧する前に、以下の必要条件を満たしていることが必要です。

クラスター

クラスターにインストールされている IDB の復元を行う場合には、特別な手順が必要となります。「IDB 復旧の準備」(533 ページ) を参照してください。

- IDB バックアップが含まれているメディアをインポートします。

復旧手順

必要条件が満たされたら、以下の手順に従って IDB を復旧します。

1. [Data Protector Manager] で、[内部データベース] バックアップ・オブジェクトをブラウズし、復元対象として選択します。「復元対象データの選択」(364 ページ) を参照してください。
2. db40/datafiles ディレクトリについては、[別名で復元 / 復元先 ...] オプションを使って、デフォルトとは別の復元先を指定します。「別のパスにファイルを復元する」(397 ページ) を参照してください。
   詳細カタログとセッション・メッセージ・バイナリ・ファイルを別の場所に復元したい場合も、[別名で復元 / 復元先 ...] オプションを使います。
3. IDB の復元を開始します。「復元のプレビューと開始」(367 ページ) を参照してください。
4. db40/datafiles ディレクトリを元の位置に戻し、omnisv -start コマンドで Data Protector サービスを起動します。
   - Windows の場合 : *<Data_Protector_home>*¥bin¥omnisv -start
   - UNIX の場合 : /opt/omni/sbin/omnisv -start

IDB が MC/ServiceGuard 上にインストールされている場合は、アクティブなノード上で cmrunpkg *<pkg_name>* コマンドを実行し、Data Protector パッケージを起動します。ここで、*<pkg_name>* は Data Protector クラスター・パッケージの名前を示します。

IDB が Microsoft Cluster Server にインストールされている場合は、クラスター・アドミニストレータユーティリティを使用して、OBVS_VELOCIS と OBVS_MCRS クラスター・グループをオンラインにし、Inet サービスを起動します。

5. 詳細カタログとセッション・メッセージ・バイナリ・ファイルを別の場所に復元した場合は、以下の手順を行う必要があります。

   a. 新しい DC ディレクトリを作成し、古い DC ディレクトリを削除します。「DC ディレクトリの作成」(502 ページ) を参照してください。

   b. omnidbutil -remap_dcdir コマンドを実行して、DC バイナリ・ファイルのパス名を更新します。

6. omnidbcheck コマンドを実行して、すべてのファイルが元の位置に戻っていることを確認します。

次に行う手順

IDB の復元後、media.log ファイルが利用可能であれば、メディアをインポートして IDB を更新する必要があります。「メディアをインポートして IDB を更新する」(543 ページ) を参照してください。

IDB トランザクション・ログを再生する

mnidbrestore -autorecover コマンドが正常に実行された場合、トランザクション・ログはすでに再生されています。トランザクション・ログの再生をもう一度行う必要がある場合、または以前に再生を延期していた場合にのみ、この手順を行うようにしてください。

IDB の復元が完了した後にトランザクション・ログを再生すると、IDB がクラッシュ直前と同じ状態に復旧されます。ただし、バイナリ・ファイルは更新されないので、バイナリ・ファイルの変更内容は失われます。

最後の IDB バックアップから IDB 破損までの間に実行されたバックアップについては、以下の項目が利用できなくなります。

- セッション・メッセージ。
- ファイル・バージョンのブラウズ (オブジェクト全体の復元は可能です

)。バックアップに使用したメディアに対してカタログのインポートを実行すると、変更内容を復旧できます。

- SIBF の更新内容。バックアップに使用したメディアをエクスポートおよびインポートすると、変更内容を復旧できます。

制限事項

トランザクション・ログを再生できるのは、トランザクション・ログのアーカイブが有効になっている場合だけです。つまり、`velocis.ini` ファイル内で Archiving パラメータが 1 に設定されていなければなりません。

必要条件

- トランザクション・ログが利用可能である必要があります。トランザクション・ログの詳細については、「IDB 復旧の準備」(496 ページ) を参照してください。トランザクション・ログが利用可能かどうかを検証するには、`/db40/logfiles/syslog` ディレクトリをリストします。

  トランザクション・ログが利用できない場合は、「メディアをインポートして IDB を更新する」(543 ページ) を参照してください。

- IDB が MC/ServiceGuard 上にインストールされている場合は、以下の手順で `omnidbrestore` コマンドを実行する前に、アクティブなノード上で `cmhaltpkg <pkg_name>` コマンドを実行し、Data Protector パッケージを終了します。以下の手順で `omnidbcheck` コマンドを実行する前に、アクティブなノード上で `cmrunpkg <pkg_name>` コマンドを実行し、Data Protector パッケージを起動します。ここで、*<pkg_name>* は Data Protector クラスター・パッケージの名前を示します。

- IDB が Microsoft Cluster Server にインストールされている場合は、以下の手順で `omnidbrestore` コマンドを実行する前に、アクティブなノード上でクラスター・アドミニストレータユーティリティを使用して、`OBVS_VELOCIS` クラスター・グループをオフラインにし、`Inet` サービスを停止します。以下の手順で `omnidbcheck` コマンドを実行する前に、クラスター・アドミニストレータユーティリティを使用して、`OBVS_VELOCIS` と `OBVS_MCRS` クラスター・グループをオンラインにし、`Inet` サービスを起動します。

トランザクション・ログの再生方法

それ以降は、以下の手順を行います。

1. 次のコマンドを実行して、トランザクション・ログを再生します。

   ```
   omnidbrestore -replay_only -firstlog
   <FirstTransactionLog>
   ```

ここで、*<first_trans_log>* は、IDB バックアップの開始後に最初に作成されたトランザクション・ログを指します。

`omnidbrestore -autorecover` の出力の末尾には、トランザクション・ログを再生するためのコマンドが最初のトランザクション・ログ名を含めて正確に表示されます。

たとえば、以下のようなコマンドが表示されます。

```
omnidbrestore -replay_only -firstlog AAAAAC
```

ここで、`AAAAAC` の位置には、IDB バックアップの開始後に最初に作成されたトランザクション・ログの名前が示されます。

2. `omnidbcheck` コマンドを実行します。

以上で、復旧が完了します。

メディアをインポートして IDB を更新する

IDB 復旧を正常に完了するには、IDB 復元後に IDB の変更内容を更新する必要があります。

トランザクション・ログが利用できない場合は、前回の IDB バックアップ以降に使用されたすべてのメディアをインポートして、変更内容を更新します。この操作は、IDB 復元の完了後に 1 回実行します。

トランザクション・ログが利用できるかどうかを確認したり、トランザクション・ログを使用して変更内容を更新するには、「IDB トランザクション・ログを再生する」(541 ページ) を参照してください。

メディアをインポートして変更内容を更新するには、以下の手順に従ってください。

1. `omnisv -start` コマンドを使って Data Protector プロセスとサービスを起動します。
   - Windows の場合 : *<Data_Protector_home>*¥bin¥omnisv -start
   - UNIX の場合 : /opt/omni/sbin/omnisv -start
2. 以下のコマンドを使用して、セッション・カウンタを 200 に進めます。

   ```
   omnidbutil -set_session_counter 200
   ```

   必要であれば、ここでバックアップを開始できます。

3. 前回の IDB バックアップが含まれているメディアをエクスポートおよびインポートします。これにより、前回の IDB バックアップに関する整合性のある情報が作成されます。
4. 前回のバックアップ以降、IDB 復旧までに使用されたメディアをインポート (すでに IDB 内にある場合はエクスポート) します。メディアのリストについては、`/var/opt/omni/server/log/media.log` ファイル (UNIX の場合)、または *<Data_Protector_home>*`¥log¥server¥media.log` ファイル (Windows の場合) を参照してください。
5. `omnidbcheck` コマンドを実行します。

IDB 全体が正常に復旧されます。

注記

CMMDB またはリモート MMDB が含まれている IDB を別のディスク・レイアウトに復旧する場合は、IDB の更新後に `omnidbutil -cdbsync` コマンドを実行する必要があります。

12 障害復旧

本章の概略

本章では、Windows、UNIX クライアントや Cell Manager 上での障害復旧の概要を説明します。以下の項目について説明します。

はじめに

本項では、障害復旧の章で使用される基本用語について説明します。使用可能な障害復旧方法の概要と概念、および各オペレーティング・システムで使用可能な障害復旧方法の一覧表は『HP OpenView Storage Data Protector コンセプト・ガイド』の障害復旧の項を参照してください。

特定のオペレーティング・システムでサポートされている障害復旧方法のリストは、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』のサポート・マトリクスを参照してください。

コンピュータ障害とは

コンピュータ障害とは、人的ミス、ハードウェア障害、ウィルス、自然災害などにより、コンピュータ・システムがブート不可能な状態になるイベントを指します。このような場合には、システムのブート・パーティションまたはシステム・パーティションが使用できなくなり、標準的な復元操作を行う前に環境の復旧が必要となります。この復旧作業には、ブート・パーティションの再作成、再フォーマット、環境を定義するすべての構成情報を使ったオペレーティング・システムの回復が含まれます。**他のユーザー・データを回復するには、この作業を完了しておく必要があります。**

オリジナル・システムとは

オリジナル・システムとは、システムでコンピュータ障害が発生する前に Data Protector によってバックアップされたシステム構成を指します。

ターゲット・システムとは

ターゲット・システムとは、コンピュータ障害発生後のシステムを指します。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いるため、Data Protector 障害復旧は、このシステムをオリジナル・システムの構成に復元することを目的としています。クラッシュしたシステムとターゲット・システムの違いは、ターゲット・システムは故障したハードウェアが交換されていることです。

ブート・ディスク / パーティション / ボリュームおよびシステム・ディスク / パーティション / ボリュームとは

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

注記

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

ホスティング・システムとは

ホスティング・システムとは、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。

補助ディスクとは

補助ディスクとは、ネットワーク機能を備えた最低限の OS と、Data Protector Disk Agent がインストールされたブート可能ディスクです。このディスクは持ち運び可能で、UNIX クライアントのディスク・デリバリーによる障害復旧のフェーズ 1 で、ターゲット・システムをブートするのに使用されます。

障害復旧オペレーティング・システム (DR OS) とは

障害復旧オペレーティング・システムとは、障害復旧プロセスが実行されているオペレーティング・システム環境であり、Data Protector に基本的ランタイム環境 (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) を提供します。Data Protector 障害復旧を行うには、障害復旧オペレーティング・システムのインストールと構成が行われている必要があります。

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、別のオペレーティング・システムをターゲット・オペレーティング・システム構成データと共に復元するホスト環境としてだけ使用され、ターゲット・システムがオリジナル構成に復旧した後は削除されます。**アクティブ DR OS** は、Data Protector 障害復旧処理に使用されるだけでなく、自身の構成データをオリジナル・システムの構成データと置き換えて、復元されたシステムの一部となります。

クリティカル・ボリュームとは

クリティカル・ボリュームとは、システム・ファイルと Data Protector ファイルのブートに必要なボリュームを指します。オペレーティング・システムの種類に関係なく、以下のボリュームがクリティカル・ボリュームとなります。

- ブート・ボリューム
- システム・ボリューム

- Data Protector 実行可能ファイル
- IDB (Cell Manager のみ)

注記

IDB が上記のいずれとも違うボリュームにある場合は、IDB のあるボリュームもクリティカル・ボリュームとなります。

Windows システムでは、上記のクリティカル・ボリュームとは別に、CONFIGURATION もクリティカル・ボリュームの一部となっています。サービスは、CONFIGURATION バックアップの一部としてバックアップされます。

CONFIGURATION に含まれる一部の項目は、システム、ブート、Data Protector、IDB ボリュームとは異なるボリュームにある場合があります。この場合、以下のボリュームもクリティカル・ボリュームの一部となります。

- ユーザー・プロファイル・ボリューム
- Windows Server 上の Certificate Server データベース・ボリューム
- Windows Server のドメイン・コントローラ上のアクティブ・ディレクトリ・サービス・ボリューム
- Microsoft Cluster Server の定数ボリューム

オンライン復旧とは

オンライン復旧は、Cell Manager がアクセス可能な場合に行います。この場合、Data Protector のほとんどの機能 (Cell Manager によるセッションの実行、セッションの IDB への記録、GUI を使った復元作業の進行状況の監視など) が使用可能です。

オフライン復旧とは

オフライン復旧は、Cell Manager がアクセスできない場合に行います (ネットワークや Cell Manager の障害、オンライン復旧が失敗した場合など)。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うことに注意してください。

ローカル / リモート復旧とは

リモート復旧は、SRD ファイルで指定された Media Agent ホストがすべて使用可能な場合に行います。1 台でも使用できない場合は、障害復旧プロセスはローカル・モードに切り替わります。つまり、ターゲット・システムはローカルに接続されたデバイスを探します。デバイスが 1 台しか見つか

らない場合は、そのデバイスが使用されます。デバイスが 2 台以上見つかった場合、Data Protector は使用するデバイスを画面に表示してユーザーに選択させます。オフライン OBDR は常にローカルで行うことに注意してください。

障害は常に重大な問題ですが、以下の要因により状況はさらに悪化するおそれがあります。

- システムをできるだけ迅速かつ効率的にオンライン状態に復帰させなければならない。
- 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。
- 復旧作業に配置可能な人員が基礎的な知識しか持っていない可能性がある。

障害復旧は、実行に先立って、広範囲にわたるプランニングと準備を必要とする非常に複雑な作業です。したがって、障害に備えたり、障害から回復するためには、十分に整備された段階的な復旧プロセスを完備しておくことが必要です。

復旧プロセス

障害復旧プロセスには次の 4 つのフェーズがあります。**フェーズ 0** は、障害復旧を成功させるために必要な準備作業です。**フェーズ 1** で、DR OS のインストールと構成を行います。通常はブート・パーティションの再作成と再フォーマットも行います。これは、システムのブートもしくはシステム・パーティションは常に使用可能とは限らず、通常の復元操作を行う前に環境の復旧が必要な場合があるためです。**フェーズ 2** では、Data Protector を含むオペレーティング・システム環境を定義するすべての構成情報を以前と同じように復旧します。このステップが無事完了し場合のみ、アプリケーションとユーザー・データの復元が可能となります (**フェーズ 3**)。迅速で効率的な復元のためには、明確なプロセスを確実に実行することが必要です。

障害復旧の準備

本項で説明する手順に従って障害復旧に対する準備作業を行い、迅速で効率的に復元が実行できるようにしてください。準備作業はどの障害復旧方法でも変わりませんが、詳細な障害復旧プランの作成、整合性と関連性を兼ね備えたバックアップの実行、SRD ファイルの更新 (Windows の場合) は必ず行います。

本項では、すべての障害復旧方法に共通する一般的な準備手順を説明します。それぞれの障害復旧方法について、独自の追加手順が必要です。追加手順については対応する項を参照してください。

プランニング

綿密な障害復旧プランの作成は、障害復旧の手順が円滑に実行されるかどうかに大きく影響します。様々なシステムが混在する大規模な環境で障害復旧を行うには、以下の手順で行います。

1. **プラン**

   計画は IT 管理者が作成し、以下の事項が含まれている必要があります。

   - 復旧が必要なシステム、復旧の時間および度合いの決定。重要なシステムは、ネットワークが正しく機能するために必要なすべてのシステム（DNS サーバ、ドメイン・コントローラ、ゲートウェイなど）、Cell Manager および Media Agent クライアントです。
   - 復旧方法の決定 (必要な準備に影響します)。
   - 復旧に必要な情報の取得方法の決定。この情報には、IDB が含まれているメディア、更新された SRD ファイルの位置、Cell Manager バックアップ・メディアの位置とラベルなどがあります。
   - 復旧プロセスの指針となる、段階を追った詳細なチェックリストの作成。
   - 復旧が実際にうまくいくことを確認するテスト・プランの作成と実行。

2. **復旧の準備**

   使用する復旧方法により、準備には以下のような作業が含まれます。

UNIX システムの場合 :

- 補助ディスクなどのツールの作成。補助ディスクには、最低限のオペレーティング・システム、ネットワーク機能、Data Protector Disk Agent をインストールします。
- データ記憶構造などクライアント固有の準備データ収集を行う、実行前スクリプトの作成。

Windows の場合 :

- **システム復旧データ (SRD)** の更新と安全な場所への保存。セキュリティ上の理由から、SRD ファイルへのアクセスは制限する必要があります。

すべてのシステム :

- 定期的で整合性のとれたバックアップの実行。

3. **復旧手順の実行**

   テスト済みの手順とチェックリストに従い、クラッシュしたシステムを復旧します。

整合性と関連性を兼ね備えたバックアップ

障害が発生した場合、ターゲット・システムを最新の有効なバックアップ時点の状態に戻さなければなりません。また、システムが最新の有効なバックアップ直前と同様に機能するようにする必要もあります。

注記

UNIX システムでは、様々な理由から、デーモンやプロセスの一部はシステムのブート直後に開始します (HP-UX の実行レベル 2 におけるライセンス・サーバなど)。このような初期プロセスは、実行中にデータをメモリに読み込んだり、ファイルに「ダーティ・フラグ」を書き込む可能性があります。また、標準的な動作段階 (標準実行レベル 4) で行われたバックアップでは、適切なアプリケーションが正常に起動しません。この例で言えば、ライセンス・サーバがこのような疑似復旧後に起動された場合、ライセンス・サーバはデータが不整合であると認識し、サービスを予定どおりに実行できません。

Windows では、システムの実行中は多くのシステム・ファイルがシステムによりロックされているため、これらを置き換えることはできません。たとえば、現在使用中のユーザー・プロファイルは復元できません。この場合、ログイン・アカウントを変えるか、関連するサービスを停止する必要があります。

バックアップ実行時にシステム上でどのプロセスが起動しているかによって異なりますが、アプリケーションに対するデータの整合性は維持されない可能性があります。したがって、復旧後、再起動や実行に関する問題が発生します。

整合性と関連性を兼ね備えたバックアップの作成方法

- 最も適切な方法として、関連するパーティションをオフラインに設定してバックアップする方法がありますが、通常はこの方法は実行できません。
- バックアップ時のシステム上の動作状況を調べます。バックアップ実行中に稼動できるのは、オペレーティング・システム関連のプロセスと、オンラインでバックアップされるデータベース・サービスのみです。
- UNIX の低水準アプリケーションや Windows のバックグラウンド・レベル・アプリケーションに固有のサービスは実行できません。

整合性と関連性を兼ね備えたバックアップに何を含めるべきかは、使用する予定の障害復旧方法や他のシステム仕様（Microsoft Cluster の障害復旧など）に依存します。特定の障害復旧方法に関連する項を参照してください。

システム復旧データ (SRD) の更新と編集

SRD とは

システム復旧データ (SRD) とは、Windows ターゲット・システムの構成と復元に必要な情報が収められた、UNICODE 形式のテキスト・ファイルです。SRD ファイルは、Windows クライアント上で `CONFIGURATION` バックアップが実行された時に作成され、`<Data_Protector_home>¥Config¥server¥dr¥srd` (Windows Cell Manager の場合)、または `/etc/opt/omni/server/dr/srd/` (UNIX Cell Manager の場合) に保存されます。

重要

IDB が使用できない場合、オブジェクトとメディアの情報は SRD ファイルだけに保存されます。

Cell Manager 上の SRD ファイルの名前は、このファイルが作成されたコンピュータのホスト名と同じです (computer.company.com など)。

CONFIGURATION バックアップの後、SRD には、DR OS のインストールに必要なシステム情報だけが保存されます。障害復旧を実行するには、バックアップ・オブジェクトとそのオブジェクトが格納されたメディアに関する情報を SRD に追加する必要があります。SRD は Windows クライアントでしか更新できません。更新された SRD ファイルの名前は、recovery.srd です。

SRD の更新方法

SRD ファイルの更新には、以下の 3 種類の方法を使用できます。

- [SRD ファイルの更新] ウィザード
- omnisrdupdate コマンド (スタンドアロン・ユーティリティとしてとして使用)
- omnisrdupdate コマンド (バックアップ・セッションの実行後スクリプトとして使用)

[SRD ファイルの更新] ウィザードの使用

[SRD ファイルの更新] ウィザードを使って SRD ファイルを更新するには、以下の手順を行います。

1. [Data Protector Manager] で [復元] コンテキストを選択し、[タスク] ナビゲーション・タブをクリックします。
2. [タスク] ナビゲーション・タブの Scoping ペインで、[障害復旧] を選択します。
3. 結果エリアで [SRD ファイルの更新] オプション・ボタンを選択し、クライアントを選択した後、[次へ] をクリックします。
4. 各クリティカル・オブジェクトごとにオブジェクトのバージョンを選択して、[次へ] をクリックします。
5. 更新した SRD ファイルの保存先ディレクトリを入力して、[完了] をクリックします。

重要

SRD ファイルは Cell Manager システムに保存されるため、Cell Manager に障害が発生した場合は、このファイルにアクセスできなくなります。したがって、Cell Manager の SRD ファイルのコピーを別途作成しておくことが必要です。

障害復旧に備えた準備の一環として、更新された SRD ファイルは、Cell Manager だけでなく、セキュリティが確保されている複数の保管先に置いてください。「準備」（559 ページ) を参照してください。

omnisrdupdate コマンドの使用

SRD ファイルは、omnisrdupdate コマンドをスタンドアロン・コマンドとして使用して更新することもできます。omnisrdupdate コマンドは *<Data_Protector_home>*¥bin ディレクトリにあります。

あるセッションに所属するバックアップ・オブジェクト情報が保存されている既存の SRD ファイルを更新するには、Omnisrdupdate で session_ID を指定する必要があります。omnisrdupdate は、渡された session_ID の値に対応するバックアップ・オブジェクトの情報が格納されている SRD ファイルを更新します。更新された SRD ファイルは、Cell Manager 上に保存されます。

この手順は、(SRD ファイルで指定されている) すべての重要なバックアップ・オブジェクトが、指定されたセッション内で実際にバックアップされた場合に限り、正常に実行されます。どのオブジェクトが SRD 更新対象のクリティカル・オブジェクトとされているかを調べるには、テキスト・エディタを使って SRD ファイルを開き、オブジェクトに関する部分 (section objects) を参照します。この部分に、SRD 更新対象のクリティカル・オブジェクトがすべてリストされています。データベースは “/” で示されています。

SRD ファイルのオブジェクトに関する部分は以下のようになります。

```
-section objects
-objcount 3
-object /C -objtype 6 -objpurpose 283
-endobject /C
-object / -objtype 3 -objpurpose 32
-endobject /
-object /CONFIGURATION -objtype 6 -objpurpose 4
-endobject /CONFIGURATION
-endsection objects
```

上記の例の場合、クリティカル・オブジェクトは、/C、/ (データベース)、/CONFIGURATION の 3 つです。

ヒント

セッション ID を取得するには、omnidb コマンドを -session オプションを付けて実行します。最新のセッション ID を取得する場合は、コマンド・プロンプトから omnidb -session -latest と入力してください。

更新済みの SRD ファイルは、障害に備えて安全な場所に保存しておくことが必要です。更新済み SRD ファイルの保存場所を指定するには、omnisrdupdate コマンドに -location オプションを付けて実行します。-location パラメータは複数指定できます (書き込み権限を持っているネットワーク共有を含む)。パラメータで指定した各保存場所に、更新済み SRD ファイルのコピーが保存されます。「準備」(559 ページ) を参照してください。

Cell Manager 上の SRD ファイルをどのホスト名で更新するかを指定するには、omnisrdupdate コマンドで -host オプションを使用します。ホスト名を指定しなかった場合は、ローカル・ホストとみなされます。Cell Manager 上の SRD ファイルは更新されません。

例

ホスト名が computer.company.com というクライアントの 2002/05/02-5 セッションに属するバックアップ・オブジェクト情報で SRD ファイルを更新して、更新済みの SRD ファイルのコピーをフロッピー・ディスクとホスト名が computer2 というコンピュータの SRDfiles 共有ディスクに保存するには、以下のコマンドを実行してください。

```
omnisrdupdate -session 2002/05/02-5 -host
computer.company.com -location a: -location
¥¥computer2¥SRDfiles
```

共有ディスクに対して書き込み権限があることを確認してください。

実行後スクリプトの使用

SRD を更新するもう 1 つの方法は、バックアップの実行後スクリプトとして omnisrdupdate コマンドを使用します。この方法を使用するには、既存のバックアップ仕様を変更するか、新しいバックアップ仕様を作成することが必要です。以下の手順に従ってバックアップ仕様を変更することにより、バックアップ・セッション終了時に、バックアップされたオブジェクトに関する情報を使って SRD ファイルが更新されます。

1. [バックアップ] コンテキストで [バックアップ仕様] → [ファイルシステム] の順に展開します。

2. 変更したいバックアップ仕様を選択します (選択するバックアップ仕様には、SRD ファイルでクリティカルとマークされているバックアップ・オブジェクトがすべて含まれていることが必要です。そうでない場合は、更新は正常に実行されません。このため、ディスク・ディスカバリを使ったクライアント・バックアップを実行することをお勧めします)。選択後、結果エリアで [オプション] をクリックします。
3. [バックアップ仕様オプション] の下の [拡張] ボタンをクリックします。
4. [実行後] テキスト・ボックスに `omnisrdupdate.exe` と入力します。
5. この実行後スクリプトを実行するクライアントを [実行対象] ドロップダウン・リストで選択し、[OK] を選択して確認します。選択するクライアントは、[ソース] ページでバックアップ対象としてマークされているクライアントでなければなりません。

`omnisrdupdate` コマンドを実行後ユーティリティとして実行すると、セッション ID が環境から自動的に取得されるので、ユーザーがセッション ID を指定する必要はありません。

その他すべてのオプションは、スタンドアロン・ユーティリティ (`-location` <*path*>,`-host` <*name*>) の場合と同様に指定できます。

SRD ファイルの編集

障害復旧を実行する時点で、SRD ファイルに保存されているバックアップ・デバイスまたはメディアに関する情報が古くなっている場合もあります。その場合は、障害復旧を実行する前に SRD ファイルを編集して、関連する情報を正しい情報に置き換えてください。「編集後の SRD ファイルを使用した復旧」(612 ページ) を参照してください。

重要

セキュリティ上の理由から、SRD ファイルへのアクセスは制限する必要があります。

Windows システムの半自動障害復旧

本項では、Windows システム上での半自動障害復旧の準備と実行方法について説明します。サポート対象のオペレーティング・システムは、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

半自動障害復旧は基本的な復旧方法で、以下の手順で構成されます。

1. Windows システムの元の位置へのインストール。この作業には、Windows のインストールに必要なブート・パーティション / システム・パーティションの作成やフォーマットも含まれます。
2. クラッシュ前と同じ状態になるよう、その他のパーティションの作成 / フォーマット (元のドライブ文字の割り当ても含む)。
3. 一時的に Data Protector をインストールし、システムのクリティカル・ボリュームの復元を開始する Data Protector `drstart.exe` コマンドの実行。
4. システムのブート。
5. ベンダー固有のパーティションの復旧 (障害発生前に存在していた場合)。

注記

Data Protector クライアントと Data Protector Cell Manager では、復旧に必要な準備手順と復旧手順は異なります。相違点は本章の中で明記されています。

Windows については、障害復旧の実行を決定する前に、システムを別の方法で復旧できる可能性があることに注意してください。システムをセーフ・モード、または復旧フロッピー・ディスクからブートして、問題解決を試みてください。もう 1 つの方法は、最後に正常動作していた構成で起動することです。

必要条件

- パーティションのサイズは、障害が発生したディスクのパーティション・サイズと同じかそれより大きくなければなりません。これにより、障害が発生したディスクに保存されていた情報を新しいディスクに復元できます。また、ファイルシステムの形式 (FAT、NTFS) と、ボリュームの圧縮属性も一致していることが必要です。
- ターゲット・システムのハードウェア構成は、障害発生前の状態と同じでなければなりません。これには、SCSI の BIOS 設定 (セクタの再マッピング) も含まれます。

制限事項

- Internet Information Server(IIS) データベース、ターミナル・サービス・データベース、Certificate Server データベースは、フェーズ 2 で自動的には復元されません。これらをターゲット・システムに復元するには、通常の Data Protector 復元手順を実行してください。

準備

障害復旧が正しく実行されるよう準備するには、一般的な準備に関する手順と、特定の障害復旧方法を使用するための要件に関連する手順を実行することが必要です。迅速かつ効率的に障害復旧を実行するには、事前の準備が必要です。Cell Manager と Microsoft Cluster Server の障害復旧準備にも十分な注意が必要です。

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。

本項で挙げられている手順を完了する前に、すべての障害復旧方法に共通する一般的な準備手順として「障害復旧の準備」(551 ページ) も参照してください。障害から迅速かつ効率的に復旧するため、以下の項目を考慮した上で適切な環境を準備してください。、

1. システムを CD-ROM から起動するには、ブート可能な Windows インストール用 CD-ROM が必要です。ブート可能な CD-ROM がない場合は、ディスクからコンピュータを起動する標準的手順を実行してください。

2. 復旧対象のシステムに適したドライバがあることを確認します。Windows のセットアップ中、ネットワーク、HBA、SCSI ドライバなど、いくつかのドライバをインストールする必要があります。
3. クラッシュしたシステムを復旧するには、障害発生前のシステムに関する以下の情報が必要です (SRD ファイルにも保存されています)。
   - 障害発生前に DHCP が使用されていなかった場合 ― TCP/IP のプロパティ (IP アドレス、デフォルトのゲートウェイ、サブネット・マスク、DNS の順序)
   - クライアントのプロパティ (ホスト名)
4. 以下の条件が当てはまることを確認します。
   - 正常に実行されたクライアントのフル・バックアップがあること。「ファイルシステム (論理ディスク・ドライブ) のバックアップ」(227 ページ) および「CONFIGURATION のバックアップ」(233 ページ) を参照してください。
   - 正常に実行されたバックアップ・セッションに含まれるバックアップ・オブジェクトに関する情報を使って更新された SRD ファイルが必要です。「システム復旧データ (SRD) の更新と編集」(553 ページ) を参照してください。
   - Cell Manager を復旧する場合は、正常に実行された Cell Manager の IDB バックアップが必要です。IDB バックアップの実行方法の詳細は、「IDB 復旧の準備」(496 ページ) を参照してください。
   - Microsoft Cluster Server のための整合性のあるバックアップには、(同じバックアップ・セッションに) 以下のものが含まれている必要があります。
     - すべてのノード
     - 管理仮想サーバ (管理者が定義)
     - Cell Manager 仮想サーバと IDB(Data Protector がクラスター対応アプリケーションとして構成されている場合)

     詳細については、「Microsoft Cluster Server の復元に固有の手順」(603 ページ) を参照してください。

- ブート・パーティションのあるディスクには、Data Protector 障害復旧ユーティリティのインストール (15 MB) とアクティブ DR OS インストールに必要な空きディスク・スペースが必要です。また、元のシステムの復元に必要な空きディスク・スペースも別途必要です。

5. 32 ビット版 Windows クライアントまたは Cell Manager の場合、次の内容を 3 枚のフロッピー・ディスク（**drsetup ディスク**）にコピーします。*<Data_Protector_home>*¥Depot¥DRSetup、または Data Protector インストール用メディアの ¥i386¥tools¥DRSetup。64 ビット版 Windows システムの場合、次の内容を 4 枚のフロッピー・ディスクにコピーします。*<Data_Protector_home>*¥Depot¥DRSetup64 または Data Protector インストール用メディアの ¥i386¥tools¥DRSetup64。障害が発生した場合、クラッシュしたクライアントの更新済み SRD ファイルを 1 枚目のフロッピー・ディスク (ディスク 1) に保存します。どの Windows システムの場合でも、1 つのサイトにつき必要な drsetup ディスクは 1 セットだけです。ただし、1 枚目のフロッピー・ディスク上にある、クラッシュしたクライアントの更新された SRD ファイルは必ずコピーしておいてください。SRD ファイルが複数ある場合は、適切なバージョンを選ぶように Data Protector が尋ねてきます。
6. ディスク・パーティションを障害発生前の初期状態に再構成するため、各パーティションごとに以下の情報を記録しておきます (この情報は復旧プロセスで必要になります)。

   - パーティションの長さと順序
   - パーティションに割り当てられるドライブ文字
   - パーティションのファイルシステムの種類

   この情報は、SRD ファイルに保存されています。SRD ファイルの diskinfo セクションで -type オプションを使用すると、特定のパーティションのファイルシステムの種類が分かります。

表 12-1 SRD ファイルからファイルシステムの種類を知る方法

種類を示す番号	ファイルシステム
1	Fat12
4、6	Fat32
5、15	拡張パーティション
7	NTFS
11、12	Fat32
18	EISA
66	LDM パーティション

次ページの表に、障害復旧の準備例を示します。表のデータは特定のシステムのものであり、それ以外のシステムでは使用できないことに注意してください。半自動障害復旧の準備に使用できる空のテンプレートについては、「Windows での手動による障害復旧準備用テンプレート」(A-50 ページ)を参照してください。

表 12-2　半自動障害復旧準備用テンプレートの例

クライアントのプロパティ	コンピュータ名	ANDES
	ホスト名	andes.company.com
ドライバ		hpn.sys、hpncin.dll
Windows Service Pack		Windows SP3
TCP/IP のプロパティ	IP アドレス	3.55.61.61
	デフォルト・ゲートウェイ	10.17.250.250
	サブネット・マスク	255.255.0.0
	DNS の順序	11.17.3.108, 11.17.100.100
メディア・ラベル / バーコード番号		"andes - disaster recovery" / [000577]

表 12-2 半自動障害復旧準備用テンプレートの例

パーティション情報と順序	第 1 ディスクのラベル	
	第 1 パーティションの長さ	31 MB
	第 1 ドライブの文字	
	第 1 ファイルシステム	EISA
	第 2 ディスクのラベル	BOOT
	第 2 パーティションの長さ	1419 MB
	第 2 ドライブの文字	C:
	第 2 ファイルシステム	NTFS/HPFS
	第 3 ディスクのラベル	
	第 3 パーティションの長さ	
	第 3 ドライブの文字	
	第 3 ファイルシステム	

復旧

以下の手順に従って、半自動障害復旧を使って Windows システムを復旧します。高度な復旧作業 (Cell Manager または IIS の復旧など) を行おうとしている場合は、「高度な復旧作業」（603 ページ) も参照してください。

1. CD-ROM から Windows システムをインストールし、必要に応じてドライバをインストールします。Windows オペレーティング・システムは、障害前と同じパーティションにインストールする必要があります。システムのインストール中に Internet Information Server（IIS）をインストールしないでください。詳しくは、「Internet Information Server (IIS) の復元に固有の手順」（610 ページ) を参照してください。

重要

Windows の無人セットアップを使用して Windows がインストールされている場合、復旧時に Windows のインストールに使用したスクリプトと同じものを使用して、`<$SystemRoot$>` フォルダと `¥Documents and Settings` フォルダが同じ場所にインストールされるようにします。

2. [Windows Partition Setup] 画面が表示されたら、以下の手順に従います。

   - クラッシュ前のシステム上にベンダー固有のパーティション（EISA Utility Partition など）があった場合は、SRD ファイルから収集した EISA 情報に基づいて、ダミーの FAT パーティションを作成し (クラッシュにより失われた場合)、フォーマットします。EUP はあとから、ダミー・パーティションによって保持されているスペースに復旧されます。ダミー・パーティションの作成後すぐに、ブート・パーティションを作成およびフォーマットしてください。この方法については、「準備」（559 ページ) を参照してください。
   - クラッシュ前のシステム上に EUP がなかった場合は、クラッシュ前の状態になるようブート・パーティションを作成し (クラッシュにより失われた場合)、フォーマットします。この方法については、「準備」（559 ページ) を参照してください。

   Windows を元の位置 (つまり、障害発生前の元のシステムとドライブ文字およびディレクトリが同じ位置) にインストールします。この情報は、SRD ファイルに保存されています。

注記

インストール時には、障害発生前に Windows ドメインが置かれていた場所にシステムを追加せずに、ワークグループに追加してください。

3. TCP/IP プロトコルをインストールします。障害発生前に DHCP を使用していなかった場合は、TCP/IP を障害発生前の状態に設定します。このとき設定する情報は、クラッシュしたクライアントのホスト名、IP アドレス、デフォルト・ゲートウェイ、サブネット・マスク、DNS サーバです。[このコンピュータのプライマリ DNS サフィックス] フィールドにはドメイン名を入力します。

警告

デフォルトでは、Windows のセットアップ時に Dynamic Host Configuration Protocol (DHCP) がインストールされます。

4. [Administrators] グループに障害復旧用の一時的なアカウントを作成します。「ユーザーの追加または削除」(144 ページ) を参照してください。このアカウントは、障害前のシステムには存在しなかったものを作成し、あとの手順で削除します。
5. ログオフした後、新規作成したアカウントを使用してシステムにログインします。
6. 障害発生後にバックアップ・デバイスを変更したなどの理由で SRD ファイルの情報が最新のものでなく、オフライン復旧を実行しようとしている場合は、この手順を続行する前に SRD ファイルを変更してください。「編集後の SRD ファイルを使用した復旧」(612 ページ) を参照してください。
7. *<Data_Protector_home>*¥Depot¥drsetup¥Disk1 (Windows Cell Manager) または ¥i386¥tools¥drsetup¥Disk1 (Data Protector インストール用メディア) のいずれかのディレクトリから drstart.exe コマンドを実行します。
   drsetup ディスクが用意されている場合は (「準備」(559 ページ) を参照)drstart.exe コマンドを実行することもできます。
8. Drstart.exe はまず、現在の作業ディレクトリ、フロッピー・ディスク、CD ドライブをスキャンして、障害復旧用セットアップ・ファイル (Dr1.cab と omnicab.ini) の位置を調べます。必要なファイルが見つかった場合は、drstart ユーティリティは障害復旧用ファイルを *<%SystemRoot%>¥system32¥OB2DR* ディレクトリにインストールします。Drstart.exe がファイルを見つけられない場合は、[DR Installation Source] テキストボックスにパスを入力するか、ブラウズしてファイルを選択します。
9. recovery.srd ファイルが dr1.cab および omnicab.ini ファイルと同じディレクトリに保存されている場合は、drstart.exe により recovery.srd ファイルが *<%SystemRoot%>*¥system32¥OB2DR¥bin ディレクトリにコピーされ、omnidr ユーティリティが自動的に起動されます。そうでない場合は、SRD ファイル (recovery.srd) の位置を [SRD Path] フィールド

に入力するかブラウズして選択して、[次へ] をクリックします。

フロッピー・ディスクに SRD ファイルが複数ある場合は、適切な適切なバージョンを選ぶように Data Protector が尋ねてきます。

omnidr が正常終了した後、システムを正しくブートするのに必要なすべてのクリティカル・オブジェクトが復元されます。

10. コンピュータを再起動し、ログオンして、復元されたアプリケーションが実行されているか検証します。
11. Cell Manager を復旧する場合は、「固有の復元手順」(600 ページ) に記載されている手順を行います。
12. Data Protector を使って、ユーザー・データとアプリケーション・データを復元します。

一時 DR OS は、以下の場合を除いて、最初のログイン後に削除されます。

- Disaster Recovery Wizard が DR のインストールとバックアップ・メディア上の SRD ファイルを発見した後の 10 秒間のポーズの間に、ユーザーがウィザードを中断して [デバッグを使用] (Use Debugs) オプションを選択した場合。
- omnidr コマンドを、no_reset または debug オプションをつけて手動で起動した場合。
- 障害復旧が失敗した場合。

Windows クライアントのディスク・デリバリーによる障害復旧

ディスク・デリバリーによる障害復旧を実行するには、現在稼働中の Data Protector クライアント (Data Protector 障害復旧ホスト) を使って、新しいディスクをこのクライアントに接続した状態で作成します。管理者は、ディスクのフォーマットおよびパーティションの構成が正しく行われるよう、障害発生前に十分なデータを収集する必要があります。ただし Data Protector により CONFIGURATION バックアップの対象として関連情報が自動的に保存されます。

復旧対象となるパーティションを以下に示します。

- ブート・パーティション
- システム・パーティション
- Data Protector を含むパーティション

その他のパーティションは、通常の Data Protector 復旧手順を使って復旧できます。

サポート対象のオペレーティング・システムは、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

ヒント

この方法は、ホットスワップ・ハードディスク・ドライブと共に使用すると非常に便利です。システムの電源を切らずに稼動させたまま、ハードディスク・ドライブをシステムから外して、新しいハードディスク・ドライブを接続できるためです。

必要条件

- パーティションのサイズは、障害が発生したディスクのパーティション・サイズと同じかそれより大きくなければなりません。これにより、障害が発生したディスクに保存されていた情報を新しいディスクに復元できます。また、ファイルシステムの形式 (FAT、NTFS) が一致していることが必要です。

- ディスクを作成したシステムと、ディスクを使用するシステムは同じセクタ・マッピング / アドレッシング (SCSI BIOS は使用可能 / 不可能のどちらに設定されているか、EIDE で両システムは必ず同じアドレッシング・モードを使用すること、LBA、ECHS、CHS の各設定など）を使用しなければなりません。

制限事項

- ディスク・デリバリーによる障害復旧は、Microsoft Cluster Server ではサポートされていません。
- RAID はサポートされていません。これには、ソフトウェア RAID（フォールト・トレラント・ボリュームおよびダイナミック・ディスク）も含まれます。
- Internet Information Server(IIS) データベース、ターミナル・サービス・データベース、Certificate Server データベースは、フェーズ 2 で自動的には復元されません。これらをターゲット・システムに復元するには、通常の Data Protector 復元手順を実行してください。

準備

障害復旧の準備としていくつかの手順を実行します。本項で挙げられている手順を完了する前に、障害復旧方法に共通する一般的な準備手順として「障害復旧の準備」（551 ページ) も参照してください。

重要

障害復旧の準備は、障害が発生する**前に**行っておく必要があります。

障害から迅速かつ効率的に復旧するには、以下が必要です。

- 最新かつ有効な、復旧対象のクライアントのフル・バックアップ
- クラッシュしたディスクと交換する新しいハードディスク
- Data Protector ホスト・システムは、クラッシュしたクライアントとオペレーティング・システムが同じで、新しいディスクの接続に必要なハードウェア I/O パスも一致していることが必要です。

ディスク・パーティションをクラッシュ前の初期状態に再構成するため、各パーティションごとに以下の情報を記録しておきます (この情報は復旧プロセスで必要になります)。

- パーティションの長さと順序
- パーティションに割り当てられるドライブ文字
- パーティションのファイルシステムの種類

表 12-2 (563 ページ) に、ディスク・デリバリーによる障害復旧の準備の例を示します。障害復旧の準備に使用できる空のテンプレートについては、「Windows での手動による障害復旧準備用テンプレート」(A-50 ページ) を参照してください。

復旧

本項では、ディスク・デリバリーによる障害復旧方法を使って Windows クライアントを復旧する手順を説明します。「高度な復旧作業」（603 ページ) も参照してください。

Windows 上でのディスク・デリバリーによる障害復旧では、Data Protector 障害復旧ホスト（DR ホスト）を使って、クラッシュしたディスクの最新の有効なフル・バックアップを、クライアントに接続されている新しいハード・ディスクに復元します。次に、障害が発生したシステムのクラッシュしたディスクを新しいハードディスクと交換します。

ディスク・デリバリーによる障害復旧手順

実際のディスク・デリバリーによる障害復旧は以下の手順で構成されています。

1. DR ホストに新しいディスクを接続します。
2. DR ホストを再起動して、新しいディスクを認識させます。
3. 障害復旧ホストの Data Protector GUI を使って、[復元] コンテキストに切り替え、[タスク] タブをクリックします。Scoping ペインで［障害復旧］を選択して、ドロップダウン・リストからクライアントを選択し、結果エリアで [ディスクのデリバリーによる障害復旧] を選択します。
4. 各クリティカル・オブジェクトごとに、復元対象のオブジェクト・バージョンを選択して、[次へ] をクリックします。
5. パーティションをまだ作成していない場合は、ディスク・アドミニストレータを使って新しいディスクのパーティションを作成します。このとき、ディスク・デリバリーによる障害復旧の準備作業の一環として収集したパーティション情報を使用します。

6. パーティションを作成する際には、フルバックアップが実行される前と同じ順序でパーティションを割り当てる必要があります。これにより、復元後のドライブ文字の再割り当てが円滑に行われるので、`boot.ini` ファイルに設定されているシステム・パーティションへのパスが不適切になることによって起こるシステム再起動時の障害を防止できます。

重要

Windows のマウント・ポイントにドライブ文字を割り当てます。この場合、各マウント・ポイントごとにドライブ文字を割り当てることができるよう、十分な未使用のドライブ文字が必要となります。

7. 元のドライブ文字を右クリックして、必要なドライブ文字の割り当てをすべて行います。ホスト・システムと元のシステムのドライブ文字が異なる可能性があるために、この作業が必要となります。
8. [完了] を選択します。
9. 新しいディスクを DR ホストから取り外して、ターゲット・システムに接続します。
10. ターゲット・システムの電源を入れます。
11. 通常の Data Protector 復元手順で、ユーザー・データとアプリケーション・データを復元します。これでクライアントの復旧は完了です。

ディスク・デリバリーは、マルチ・ブート・システムのディスクの内 1 つがクラッシュした場合にも有効な障害復旧方法です。この場合、ユーザーは少なくとも 1 つの構成をブートできるためです。

注記

Data Protector はボリューム圧縮フラグを復元しません。バックアップ時に圧縮されていたファイルはすべて圧縮されて復元されますが、新規ファイルを圧縮ファイルとして作成したい場合は、手動でボリューム圧縮フラグをセットする必要があります。

Windows システムの拡張自動障害復旧

拡張自動障害復旧 (EADR) 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 の復旧方法で、ユーザーが介在する手間は最小限に抑えられています。サポート対象のオペレーティング・システムについては、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

Windows プラットフォーム用の EADR 手順では、環境に関連するすべてのデータがバックアップ時に自動収集されます。CONFIGURATION バックアップの際に、一時 DR OS のセットアップと構成に必要なデータが、セル内のバックアップ対象の各クライアントごとに 1 つの大きな **DR OS イメージファイル**にパックされ、バックアップ・テープに (オプションで Cell Manager にも) 保存されます。

イメージファイルに加え、ディスクの適切なフォーマットとパーティション作成に必要なフェーズ 1 開始情報 (**P1S** ファイルに保存) が Cell Manager に保存されます。障害が発生した場合、EADR ウィザードで、DR OS イメージをバックアップ・メディア (フル・バックアップ時に Cell Manager に保存されていない場合) から復元し、それを**障害復旧 CD ISO イメージ**に変換します。CD ISO イメージは、CD 書き込みツールで CD に保存して、ターゲット・システムのブートに使用します。

次に Data Protector は、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作成を自動的に行い、最後にオリジナル・システムをバックアップ時と同じ状態に復旧します。

重要

ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行して新しい DR CD を作成します。これは、IP アドレスや DNS サーバの変更など、ネットワーク構成が変更された場合も同じです。

復旧対象となるボリュームを以下に示します。

- ブート・パーティション
- システム・パーティション

- Data Protector を含むパーティション

その他のパーティションは、通常の Data Protector 復旧手順を使って復旧できます。

以降の項では、Windows クライアントの拡張自動障害復旧に関する制限事項、準備および復旧方法を説明します。「高度な復旧作業」（603 ページ) も参照してください。

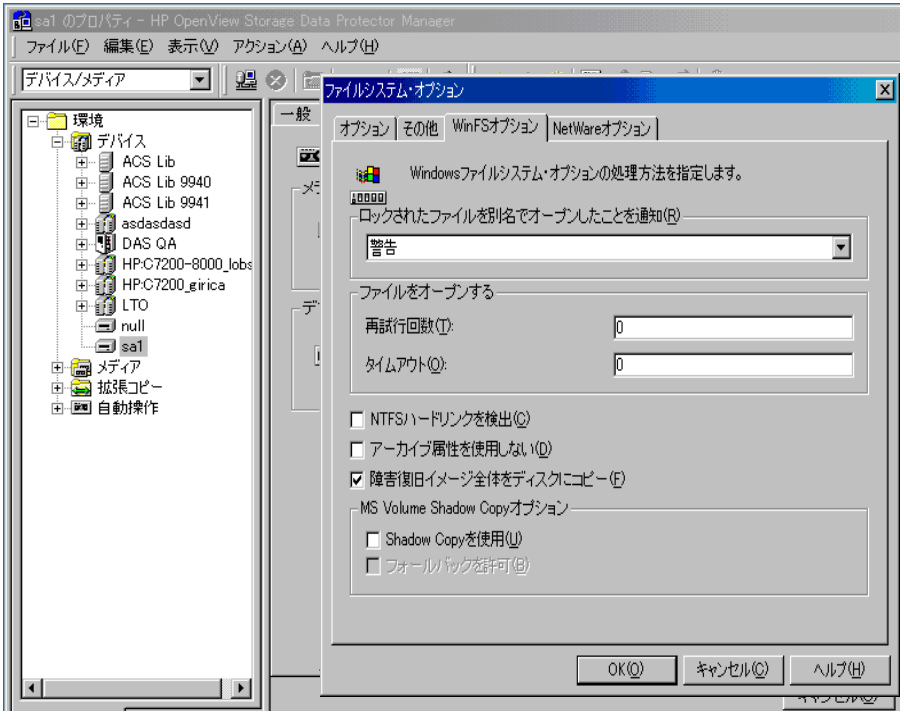
障害復旧方法を選択する前に、以下の必要条件と制限事項をよくお読みください。

必要条件

- Data Protector 自動障害復旧コンポーネントが、この方法で復旧したいクライアントと、DR CD ISO イメージを作成するシステムにインストールされている必要があります。『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。
- ターゲット・システムのハードウェア構成は、障害発生前の状態と同じでなければなりません。これには、SCSI の BIOS 設定 (セクタの再マッピング) も含まれます。
- 交換ディスクは、同じバスの同じホスト・バス・アダプタに接続されている必要があります。
- ブート・パーティションは 100MB より大きい必要があります。そうでない場合、障害復旧は失敗します。
- バックアップ時には、ブート・パーティションに別途 200MB の空きスペースが必要です。この空きスペースがない場合、障害復旧は失敗します。元のパーティションで［ドライブの圧縮］を行っている場合には、400 MB の空きスペースが必要となります。
- ブートに必要なドライバは、すべて `<%SystemRoot%>` フォルダにインストールされている必要があります。
- ネットワーク機能が付いたセーフモード、またはディレクトリ・サービス復元モード (ドメイン・コントローラのみ) でシステムをブートする場合は、ネットワークが使用可能でなければなりません。ただし、システムのバックアップは通常のブート・プロセスの後に実行する必要があります。

- システムの BIOS は、El-Torito 標準で定義されているブート可能 CD をサポートしている必要があります。また INT13h 機能の XXh により、LBA アドレッシングを使用しているハードディスク・ドライブへの読み書きが可能である必要があります。BIOS のオプションは、システムのユーザー・マニュアル、またはブート前にシステム設定を調査することでチェックできます。
- オフライン復元を計画している場合は、クライアント・バックアップ時のデバイスへの書き込みにはデフォルトのブロック・サイズ 64KB を使用してください。障害復旧を実行する際に Windows で使用できるブロック・サイズはこのデフォルトのサイズだけです。デフォルトのブロック・サイズ 64KB が設定されているかどうかを確かめるには、[プロパティ] ボックスの [拡張 . . .] を選択します。図 12-1 を参照してください。

図 12-1　デフォルトのブロック・サイズの確認



制限事項

ディスクとパーティションの構成

- ダイナミック・ディスクはサポートされていません (Windows NT からのミラー・セットのアップグレードも含む)。
- 新しいディスクのサイズは、クラッシュしたディスクのサイズ以上である必要があります。元のディスクのサイズよりも大きい場合、余った分に対しては割り当てが行われません。
- 拡張自動障害復旧でサポートされているベンダー固有のパーティションは、0x12 タイプ (EISA を含む) と 0xFE タイプのみです。

その他

- Microsoft のブート・ローダを使用していないマルチブート・システムはサポートされていません。
- Internet Information Server(IIS)、ターミナル・サービス・データベース、Certificate Server データベースは、フェーズ 2 で自動的には復元されません。これらをターゲット・システムに復元するには、通常の Data Protector 復元手順を実行してください。

準備

本項で挙げられている手順を完了する前に、すべての障害復旧方法に共通する一般的な準備手順として「障害復旧の準備」(551 ページ) も参照してください。さらに、「高度な復旧作業」(603 ページ) も参照してください。

重要

障害復旧の準備は、障害が発生する**前に**行っておく必要があります。

必要条件

- フル・クライアント・バックアップを実行します（CONFIGURATION も含む)。「ファイルシステム (論理ディスク・ドライブ) のバックアップ」(227 ページ) および「CONFIGURATION のバックアップ」(233 ページ) を参照してください。

Microsoft Cluster Server

- Microsoft Cluster Server のための整合性のあるバックアップには、(同じバックアップ・セッションに）以下のものが含まれている必要があります。

  — すべてのノード

— 管理仮想サーバ (管理者が定義)

— Cell Manager仮想サーバとIDB(Data Protectorがクラスター対応アプリケーションとして構成されている場合)

詳細については、「Microsoft Cluster Server の復元に固有の手順」（603 ページ) を参照してください。

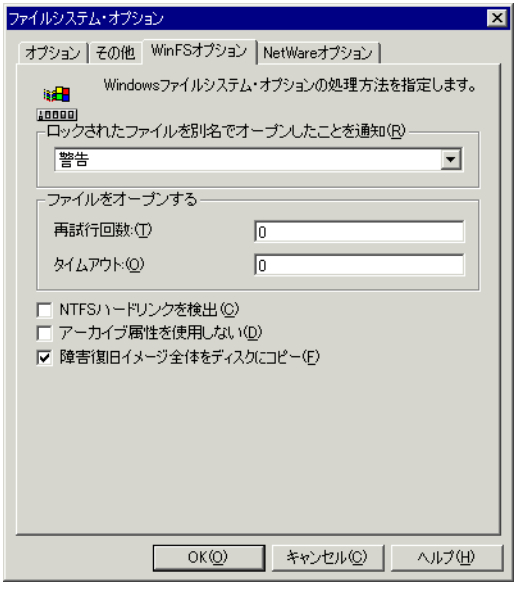
バックアップ実行後に、MSCS 内の全ノードの P1S ファイルをマージします。これにより、各ノードの P1S ファイルには共有クラスター・ボリューム構成の情報が格納されます。詳しくは「EADR 用に全ノードの P1S ファイルをマージ」（607 ページ) を参照してください。

DR イメージファイル

一時 DR OS のセットアップと構成に必要なデータ (**DR イメージ**) は、フル・クライアント・バックアアップ時に 1 つの大きなファイルにパックされ、バックアップ・テープ、さらにオプションで Cell Manager にも保存されます。Cell Manager にも、バックアップ仕様にあるクライアントすべての障害復旧イメージを保存したい場合は、以下の手順を実行してください。

1. コンテキスト・リストで [バックアップ] を選択します。
2. Scopingペインで [バックアップ仕様] → [ファイルシステム] の順に展開します。
3. フル・クライアント・バックアップに使用するバックアップ仕様を選択します (まだ作成していない場合は作成します)。
4. 結果エリアで [オプション] をクリックします。
5. [ファイルシステム・オプション] で [拡張] をクリックします。
6. [WinFS オプション] をクリックし、[障害復旧イメージ全体をディスクにコピー] チェックボックスにチェックを付けます。

図 12-2 WinFS オプション・タブ



バックアップ仕様内の特定クライアントの DR イメージファイルだけをコピーする場合は、以下の手順を実行します。

1. コンテキスト・リストで [バックアップ] を選択します。
2. Scopingペインで [バックアップ仕様] → [ファイルシステム] の順に展開します。
3. フル・クライアント・バックアップに使用するバックアップ仕様を選択します。まだ作成していない場合は「バックアップ仕様の作成」(212 ページ) に記述されている手順で作成します。
4. 結果エリアで [バックアップ・オブジェクトのサマリー] をクリックします。
5. Cell Manager に DR イメージファイルを保存したいクライアントを選択して、[プロパティ] をクリックします。
6. [WinFS オプション] をクリックし、[障害復旧イメージ全体をディスクにコピー] を選択します。

障害復旧 CD を Cell Manager 上で作成する場合、障害復旧イメージ全体を Cell Manager に保存するのが便利です。そうすれば DR イメージはハードディスクから読み込まれ、バックアップ・メディアから読み込む場合よりもはるかに速く作業が進みます。DR イメージはデフォルトでは、*<Data_Protector_home>*¥Config¥server¥dr¥p1s (Windows Cell Manager の場合)、または /etc/opt/omni/server/dr/p1s (UNIX Cell Manager の場合) に *<client name>*.img という名前で保存されます。デフォルトのディレクトリを変更するには、グローバル・オプション・ファイルで新たなグローバル変数 EADRImagePath = *<valid_path>* (EADRImagePath = /home/images または EADRImagePath = c:¥temp など) を指定します。詳細は、「グローバル・オプション・ファイル」(645 ページ) を参照してください。

ヒント

宛先ディレクトリに十分な空きディスク・スペースがでない場合には、他のボリュームへのリンクを作成するか（UNIX の場合）、マウント・ポイントを作成します（Windows の場合）。

DRecoveryKB.cfg ファイル

このファイルの目的は、特定のブート関連ハードウェアまたはアプリケーション構成を持つシステム用に、ドライバ（および他の必要ファイル）を DR OS に含めるための柔軟な方法を提供することです。デフォルトの DRecoveryKB.cfg ファイルには、業界標準のハードウェア構成に必要なすべてのファイルがすでに含まれています。

デフォルトの DRecoveryKB.cfg ファイルを使用したテスト・プランを作成し実行します。DR OS が正常にブートしない、またはネットワークにアクセスできない場合は、ファイルを変更する必要があります。「DRecoveryKB.cfg ファイルの編集」(611 ページ) を参照してください。

フェーズ 1 開始ファイル (P1S)

DR イメージファイルに加え、フル・バックアップ時には**フェーズ 1 開始ファイル (P1S)** が作成されます。このファイルは、バックアップ・メディア、および Cell Manager の *<Data_Protector_home>*¥Config¥server¥dr¥p1s ディレクトリ (Windows Cell Manager)、または /etc/opt/omni/server/dr/p1s ディレクトリ (UNIX Cell Manager) に保存されます。ファイル名はホスト名と同じです (たとえば computer.company.com など)。これは Unicode UTF-8 でエンコードされたファイルで、システムにインストールされているすべてのディスクのフォーマット / パーティション作成方法に関する情報が含ま

れています。これに対して更新済みの SRD ファイルには、システム情報、およびバックアップ・オブジェクトと対応するメディアに関するデータのみが含まれています。

障害が発生した場合、障害復旧インストールの際に EADR ウィザードを使用して、DR イメージ、SRD ファイル、P1S ファイルを**障害復旧 CD ISO イメージ**としてマージできます。このイメージは ISO9660 フォーマットをサポートしている CD 書き込みツールで CD に保存できます。この**障害復旧 CD** は、自動障害復旧を実行する際に使用します。

重要

Cell Manager 用の障害復旧 CD を事前に用意しておく必要があります。

Microsoft Cluster のノード用の障害復旧 CD を作成する場合には、特別な手順が必要になります。「Microsoft Cluster Server の復元に固有の手順」（603 ページ) を参照してください。

重要

セキュリティ上の理由から、バックアップ・メディア、DR イメージ、SRD ファイル、障害復旧 CD へのアクセスを制限しておくことをお勧めします。

DR CD ISO イメージの作成

DR CD ISO イメージを作成するには、以下の手順を行います。

1. コンテキスト・リストで [復元] を選択します。
2. Scoping ペインで [タスク] ナビゲーション・タブをクリックし、[障害復旧] を選択します
3. 結果エリアのドロップダウン・リストから、復旧対象のクライアントを選択します。
4. [拡張自動障害復旧] 、[次へ] の順にクリックします。
5. 各クリティカル・オブジェクトごとに、適切なオブジェクト・バージョンを選択します。

   [次へ] をクリックします。
6. Cell Manager に DR イメージファイルが保存されている場合は保存ディレクトリを指定します。それ以外の場合は、[バックアップからの復元] をクリックします。[次へ] をクリックします。

7. ISO CD イメージ (recovery.iso) の保存先ディレクトリを選択して [完了] をクリックすると、ISO CD イメージが作成されます。

注意

新しい ISO CD イメージを、すでに recovery.iso があるディレクトリへ保存した場合は、既存の ISO CD イメージは新しいイメージで上書きされます。このとき警告メッセージは表示されません。

8. 障害復旧 ISO CD イメージを、ISO9660 フォーマットをサポートしている CD 書き込みツールを使用して CD に保存します。

重要

ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行して新しい DR CD を作成します。これは、IP アドレスや DNS サーバの変更など、ネットワーク構成が変更された場合も同じです。

復旧

クラッシュしたシステム上でシステムの障害復旧を正しく実行するには、以下が必要です。

- クラッシュしたディスクと交換する新しいハードディスク
- 復旧対象のクライアントの正常なフル・バックアップ
- Data Protector 障害復旧 CD

Windows クライアントの拡張自動障害復旧

Windows クライアントの拡張自動障害復旧を実行する手順を以下に示します。

1. 元のシステムを障害復旧 CD からブートします。
2. Press 以下のメッセージが表示されたときに F12 キーを押します。
   <HOSTNAME> の復旧を開始するには、[F12] キーを押してください。
3. 復旧範囲を選択して、Enter キーを押します。復旧範囲は 5 種類あります。
   - 再起動 (Reboot): 障害復旧は実行されず、コンピュータが再起動されます。

- デフォルト復旧 (Default Recovery): クリティカル・ボリュームが復旧されます。他のすべてのディスクはパーティション作成やフォーマットが行われず、フェーズ 3 に備えた状態になります。
- 最小復旧 (Minimal Recovery): システム・ディスクとブート・ディスクのみが復旧されます（EADR と OBDR のみで使用可能)。
- 共有ボリュームを含む完全復旧 (Full with Shared Volumes): MSCS でのみ使用可能です。このオプションは、MSCS 内のすべてのノードがクラッシュして、最初のノードに対する拡張自動障害復旧を実行する場合に使用します。復元セット内のすべてのボリューム (バックアップ時にバックアップ対象のノードによりロックされていたクラスター共有ボリュームを含む) が復元されます。

  1 つでも稼動中のノードがあって MSCS サービスが実行されている場合、共有ボリュームは復元されません。これは、稼動中のノードにより共有ボリュームがロックされるためです。この場合はデフォルト復旧を使用してください。

4. 復旧範囲を選択すると、Data Protector は、ハードディスクに対して直接 DR OS のセットアップを開始します。この処理の進行状況はモニター可能です。DR OS のセットアップが完了するとシステムは再起動します。
5. 「<HOSTNAME> の復旧を開始するには、F12 キーを押してください。」というプロンプトの表示で 10 秒間待つと、システムは CD ではなくハードディスクから起動します。
6. 障害発生後にバックアップ・デバイスを変更したなどの理由で SRD ファイルの情報が最新のものでなく、オフライン復旧を実行しようとしている場合は、この手順を続行する前に SRD ファイルを変更してください。「編集後の SRD ファイルを使用した復旧」（612 ページ) を参照してください。
7. Data Protector は次に、選択された復旧範囲内で障害発生前の記憶データ構造を再構築し、すべてのクリティカル・ボリュームを復元します。一時 DR OS は、以下の場合を除いて、最初のログイン後に削除されます。

   - 最小復旧が選択された場合。
   - Disaster Recovery Wizard が DR のインストールとバックアップ・メディア上の SRD ファイルを発見した後の 10 秒間のポーズの間に、ユーザーがウィザードを中断して [デバッグを使用] (Use Debugs) オプションを選択した場合。

- omnidr コマンドを、no_reset または debug オプションをつけて手動で起動した場合。
- 障害復旧が失敗した場合。

8. Cell Manager の復旧、または高度な復旧作業を行おうとしている場合は、特別な手順が必要となります。詳しくは、「高度な復旧作業」(603 ページ) を参照してください。
9. 通常の Data Protector 復元手順を使用して、ユーザー・データとアプリケーション・データを復元します。

注記

Data Protector はボリューム圧縮フラグを復元しません。バックアップ時に圧縮されていたファイルはすべて圧縮されて復元されますが、新規ファイルを圧縮ファイルとして作成したい場合は、手動でボリューム圧縮フラグをセットする必要があります。

Windows システムのワンボタン障害復旧

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。サポート対象のオペレーティング・システムは、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

OBDR では、環境に関連するすべてのデータがバックアップ時に自動収集されます。バックアップの際に、一時 DR OS のセットアップと構成に必要なデータが、1 つの大きな OBDR イメージファイルにパックされ、バックアップ・テープに保存されます。障害が発生した場合には、OBDR デバイス (CD-ROM をエミュレートできるバックアップ・デバイス) を使用して、OBDR イメージファイルと障害復旧情報を含むテープからターゲット・システムを直接ブートします。

Data Protector は次に、障害復旧オペレーティング・システム (DR OS) のインストールと構成、ディスクのフォーマットとパーティション作成を自動的に行い、最後に元のオペレーティング・システムをバックアップ時と同じ状態に復元します。

重要

ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行します。これは、IP アドレスや DNS サーバの変更など、ネットワーク構成が変更された場合も同じです。

復旧対象となるパーティションを以下に示します。

- ブート・パーティション
- システム・パーティション
- Data Protector を含むパーティション

その他のパーティションは、通常の Data Protector 復旧手順を使って復旧できます。

以下の項で、Windows システム上でのワンボタン障害復旧に関する必要条件、制限事項、準備、および復旧について説明します。「高度な復旧作業」(603 ページ) も参照してください。

必要条件

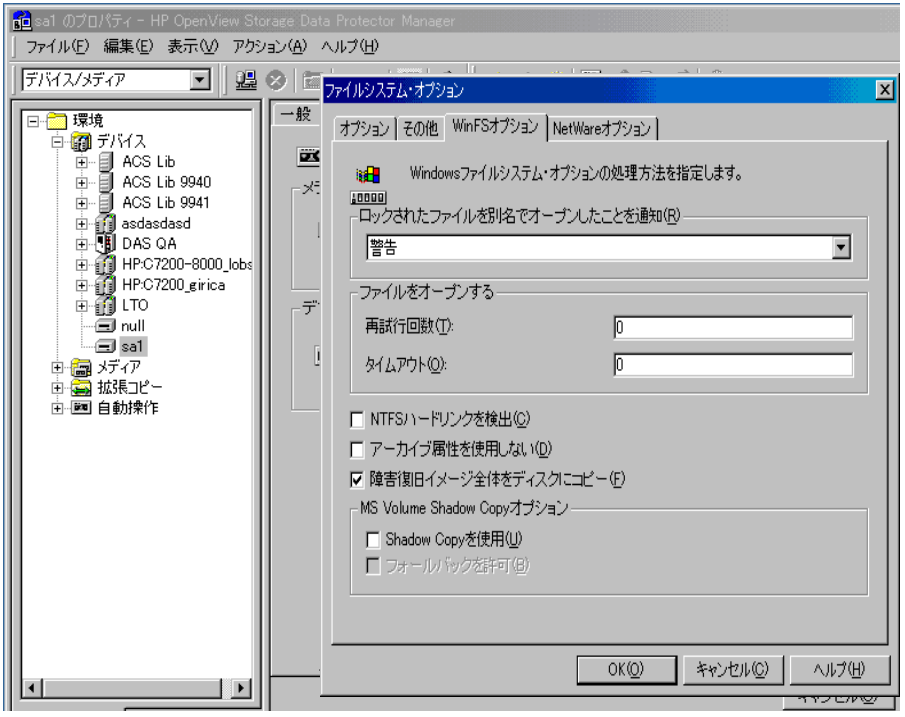
- Data Protector 自動障害復旧コンポーネントとユーザー・インタフェース・コンポーネントが、この方法で復旧するシステムにインストールされている必要があります。『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。
- OBDR を実行できるコンピュータ構成であることが必要です。システムの BIOS は、El-Torito 標準で定義されているブート可能 CD をサポートしている必要があります。また INT13h 機能の XXh により、LBA アドレッシングを使用しているハードディスク・ドライブへの読み書きが可能である必要があります。OBDR デバイスが CD-ROM をエミュレートする場合には、同じ標準に準拠していなければなりません。BIOS のオプションは、システムのユーザー・マニュアル、またはブート前にシステム設定を調査することでチェックできます。

  サポートされているシステム、デバイスおよびメディアに関する詳細については、以下の Web ページにある HP StorageWorks のテープとハードウェアの互換性一覧表を参照してください。

  http://www.openview.hp.com/products/datapro/spec_0001.html. 『HP OpenView Storage Data Protector ソフトウェア リリース ノート』も参照してください。
- ターゲット・システムのハードウェア構成は、障害発生前の状態と同じでなければなりません。これには、SCSI の BIOS 設定 (セクタの再マッピング) も含まれます。
- 交換ディスクは、同じバスの同じホスト・バス・アダプタに接続されている必要があります。
- バックアップ時には、ブート・パーティションに別途 200MB の空きスペースが必要です。この空きスペースがない場合、障害復旧は失敗します。元のパーティションで［ドライブの圧縮］を行っている場合には、400 MB の空きスペースが必要となります。
- ブートに必要なドライバは、すべて `<%SystemRoot%>` フォルダにインストールされている必要があります。
- ネットワーク機能が付いたセーフモード、またはディレクトリ・サービス復元モード (ドメイン・コントローラのみ) でシステムをブートする場合は、ネットワークが使用可能でなければなりません。ただし、システムのバックアップは通常のブート・プロセスの後に実行する必要があります。

- メディアの使用ポリシーが [追加不可能] でメディア割当てポリシーが [Loose] のメディア・プールを OBDR 対応のデバイスに対して作成する必要があります。障害復旧には、このようなプールのメディアしか使用できません。
- オフライン復元を計画している場合は、クライアント・バックアップ時のデバイスへの書き込みにはデフォルトのブロック・サイズ 64KB を使用してください。障害復旧を実行する際に Windows で使用できるブロック・サイズはこのデフォルトのサイズだけです。デフォルトのブロック・サイズ 64KB が設定されているかどうかを確かめるには、[プロパティ] ボックスの [拡張 . . .] を選択します。図 12-3 を参照してください。

図 12-3　デフォルトのブロック・サイズの確認



制限事項

全般

- Microsoft のブート・ローダを使用していないマルチブート・システムはサポートされていません。
- Internet Information Server(IIS) データベース、ターミナル・サービス・データベース、Certificate Server データベースは、フェーズ 2 で自動的には復元されません。これらをターゲット・システムに復元するには、通常の Data Protector 復元手順を実行してください。
- ワンボタン障害復旧のバックアップ・セッションは、同じ OBDE デバイス上では 1 度に 1 つのクライアントまたは Cell Manager に対してしか実行できません。バックアップ・セッションは、ローカルに接続された 1 台の OBDR 対応デバイス上で行う必要があります。

ディスクとパーティションの構成

- ダイナミック・ディスクはサポートされていません (Windows NT からのミラー・セットのアップグレードも含む)。
- 新しいディスクのサイズは、クラッシュしたディスクのサイズ以上である必要があります。元のディスクのサイズよりも大きい場合、余った分に対しては割り当てが行われません。
- OBDR でサポートされているベンダー固有のパーティションは、0x12 タイプ (EISA を含む) と 0xFE タイプのみです。

準備

本項で挙げられている手順を完了する前に、すべての障害復旧方法に共通する一般的な準備手順として「障害復旧の準備」(551 ページ) も参照してください。さらに、「高度な復旧作業」(603 ページ) も参照してください。

重要

障害復旧の準備は、障害が発生する**前に**行っておく必要があります。

DDS または LTO メディア用のメディア・プールを作成します。使用ポリシーは [追加不可能](テープ上のバックアップであることを確実にするため)、メディア割当てポリシーは [Loose](テープは OBDR バックアップ時にフォーマットされるため) です。また、このメディア・プールを OBDR

デバイス用のデフォルト・メディア・プールとして選択する必要があります。詳細については、「メディア・プールの作成」(157 ページ) を参照してください。このプールのメディアのみが、OBDR で使用できます。

Microsoft Cluster Server

Microsoft Cluster Server のための整合性のあるバックアップには、(同じバックアップ・セッションに) 以下のものが含まれている必要があります。

- すべてのノード
- 管理仮想サーバ (管理者が定義)
- Cell Manager 仮想サーバと IDB(Data Protector がクラスター対応アプリケーションとして構成されている場合)

詳細については、「Microsoft Cluster Server の復元に固有の手順」(603 ページ) を参照してください。

OBDR で MSCS 内の全共有ディスク・ボリュームの自動復元を可能にするには、ボリュームをすべて OBDR ブート・テープの準備作業に使用するノードに一時的に移動します。そうすることで、OBDR バックアップ中に共有ディスク・ボリュームが他のノードによりロックされることはなくなります。バックアップ時に他のノードによりロックされている共有ディスク・ボリュームのディスクをフェーズ 1 で構成するために必要な情報を収集するのは不可能です。

OBDR バックアップ

OBDR を使用して復旧を実行したいシステム上で OBDR バックアップをローカルに実行するには、以下の手順を実行します。

1. コンテキスト・リストで [バックアップ] を選択します。
2. Scoping ペインで [タスク] ナビゲーション・タブをクリックし、[ワンボタン障害復旧ウィザード] を選択します。
3. 結果エリアのドロップダウン・リストから OBDR バックアップの対象となるクライアントを選択して、[次へ] をクリックします。
4. クリティカル・オブジェクトはすでにすべて選択された状態になっていて (Cell Manager OBDR バックアップの場合は IDB も含む)、選択を解除することはできません。復旧手順の中で、Data Protector はシステムからパーティションをすべて削除してしまうため、他のパーティションを復旧後も使用する場合、手動で選択します。[次へ] をクリックします。
5. バックアップに使用するローカル接続の OBDR ドライブを選択して [次へ] をクリックします。

6. バックアップ・オプションの選択 詳細は、「バックアップ・オプションの使用」(290 ページ) を参照してください。
7. [次へ] をクリックして、[スケジューラ] ページを表示します。ここでは、バックアップの実行スケジュールを設定できます。詳しくは、「無人バックアップのスケジュール」(269 ページ) を参照してください。
8. [次へ] をクリックして、[バックアップ・オブジェクトのサマリー] ページを表示します。ここでは、バックアップ・オプションが表示されます。このページには、バックアップ・オプションが表示されます。

注記

[サマリー] ページでは、それまでに選択したバックアップ・デバイスやバックアップ仕様の順序を変更することができません（順序を入れ替える機能はありません）。OBDR に必要ではないバックアップ・オブジェクトのみ削除可能であり、一般的なオブジェクトのプロパティのみ表示できます。

ただし、バックアップ・オブジェクトの説明は変更できます。

9. [バックアップ] ウィザードの最終ページでは、バックアップ仕様の保存、対話型バックアップの開始、またはバックアップのプレビューを行うことができます。

   バックアップ仕様を保存して、後でスケジュールを設定したり仕様を変更できるようにしておくことをお勧めします。

OBDR のバックアップ仕様の変更

バックアップ仕様を一度保存すると、編集が可能になります。バックアップ仕様を右クリックして、[プロパティ] を選択します。変更したバックアップ仕様を、通常の Data Protector バックアップ仕様として扱うか、または OBDR バックアップ仕様として扱うかを尋ねられますので、OBDR バックアップ仕様として保存します (オリジナルのワンボタン障害復旧フォーマットで保存されます)。標準バックアップ仕様として保存した場合は、OBDR には使用できません。

10. [バックアップ開始] をクリックして、バックアップを対話形式で実行します。[バックアップ開始] ダイアログ・ボックスが表示されます。[OK] をクリックしてバックアップを開始します。

一時 DR OS のインストールと構成に必要な情報がすべて含まれているシステム用ブート可能イメージはテープの先頭に書き込まれ、これによりテープからのブートが可能となります。

重要

ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行してブート可能なバックアップ・メディアを作成します。これは、IP アドレスや DNS サーバの変更など、ネットワーク構成が変更された場合も同じです。

DRecoveryKB.cfg ファイル

このファイルの目的は、特定のブート関連ハードウェアまたはアプリケーション構成を持つシステム用に、ドライバ（および他の必要ファイル）を DR OS に含めるための柔軟な方法を提供することです。デフォルトの `DRecoveryKB.cfg` ファイルには、業界標準のハードウェア構成に必要なすべてのファイルがすでに含まれています。

デフォルトの `DRecoveryKB.cfg` ファイルを使用したテスト・プランを作成し実行します。DR OS が正常にブートしない、またはネットワークにアクセスできない場合は、ファイルを変更する必要があります。「DRecoveryKB.cfg ファイルの編集」（611 ページ) を参照してください。

注意

セキュリティ上の理由から、バックアップ・メディアへのアクセスを制限することをお勧めします。

復旧

クラッシュしたシステム上でシステムの障害復旧を正しく実行するには、以下が必要です。

- クラッシュしたディスクと交換する新しいハードディスク (必要な場合)。
- 復旧対象クライアントのクリティカル・オブジェクトがすべて含まれたブート可能なバックアップ・メディア。
- ターゲット・システムにローカル接続された OBDR デバイス。

OBDR の手順

Windows システムのワンボタン障害復旧の詳細な手順を以下に示します。

1. イメージファイルとバックアップ・データを含むテープを OBDR デバイスに挿入します。

2. ターゲット・システムをシャットダウンして、テープ・デバイスの電源を落とします。
3. ターゲット・システムの電源を入れ、初期化中にテープ・デバイスの取出しボタンを押して、テープ・デバイスの電源を入れます。詳しくはデバイス付属のドキュメントを参照してください。
4. 表示される画面で復旧範囲を選択して Enter を押します。復旧範囲は 5 種類あります。
   - 再起動 (Reboot): 障害復旧は実行されず、コンピュータが再起動されます。
   - デフォルト復旧 (Default Recovery): クリティカル・ボリュームが復旧されます。他のすべてのディスクはパーティション作成やフォーマットが行われず空のままで、フェーズ 3 に備えた状態になります。
   - 最小復旧 (Minimal Recovery): システム・ディスクとブート・ディスクのみが復旧されます（EADR と OBDR のみで使用可能)。
   - 共有ボリュームを含む完全復旧 (Full with Shared Volumes): MSCS でのみ使用可能です。このオプションは、MSCS 内のすべてのノードがクラッシュして、最初のノードに対するワンボタン障害復旧を実行する場合に使用します。復元セット内のすべてのボリューム (バックアップ時にバックアップ対象のノードによりロックされていたクラスター共有ボリュームを含む) が復元されます。

ヒント

MSCS 内の全共有ディスク・ボリュームの自動復元を可能にするには、ボリュームをすべて OBDR ブート・テープの準備作業に使用するノードに一時的に移動します。バックアップ時に他のノードによりロックされている共有ディスク・ボリュームのディスクをフェーズ 1 で構成するために必要な情報を収集するのは不可能なことです。

1 つでも稼動中のノードがあって MSCS サービスが実行されている場合、共有ボリュームは復元されません。稼動中のノードが共有ボリュームをロックしているためです。この場合はデフォルト復旧を使用してください。

5. 復旧範囲を選択すると、Data Protector は、ハードディスクに対して直接 DR OS のセットアップを開始します。この処理の進行状況はモニター可能です。DR OS のセットアップが完了するとシステムは再起動します。
6. 障害発生後にバックアップ・デバイスを変更したなどの理由で SRD ファイルの情報が最新のものでなく、オフライン復旧を実行しようとしている場合は、この手順を続行する前に SRD ファイルを変更してください。「編集後の SRD ファイルを使用した復旧」(612 ページ) を参照してください。
7. 次に Data Protector は、従来の記憶データ構造を再構築し、すべてのクリティカル・ボリュームを復元します。一時 DR OS は、以下の場合を除いて、最初のログイン時に削除されます。
   - 最小復旧が選択された場合。
   - Disaster Recovery Wizard が DR のインストールとバックアップ・メディア上の SRD ファイルを発見した後の 10 秒間のポーズの間に、ユーザーがウィザードを中断して [デバッグを使用] (`Use Debugs`) オプションを選択した場合。
   - `omnidr` コマンドを、`no_reset` または `debug` オプションをつけて手動で起動した場合。
   - 障害復旧が失敗した場合。
8. Cell Manager の復旧、または高度な復旧作業を行おうとしている場合は、特別な手順が必要となります。詳しくは、「高度な復旧作業」(603 ページ) を参照してください。
9. 通常の Data Protector 復元手順を使用して、ユーザー・データとアプリケーション・データを復元します。

注記

Data Protector はボリューム圧縮フラグを復元しません。バックアップ時に圧縮されていたファイルはすべて圧縮されて復元されますが、新しく作成するファイルも圧縮ファイルとして作成したい場合は、手動でボリューム圧縮フラグをセットする必要があります。

自動システム復旧

自動システム復旧（ASR）とは、障害発生時に Windows システム上でディスクを元の状態に再構成（または、新しいディスクが元のディスクより大きい場合はパーティションのサイズ変更）する自動システムです。これには、ディスクのパーティション作成とボリュームの構成（ファイルのフォーマット、ドライブ文字の割り当て、ボリューム・マウントポイント、ボリューム特性）が含まれます。このように ASR は Data Protector の `drstart.exe` コマンドにより、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。

Data Protector は次に、ターゲット・システムを元のシステム構成に復旧し、最後にユーザー・データを復元します。

サポート対象のオペレーティング・システムは、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

重要

ハードウェアやソフトウェア、または構成が変更された場合や、ASR ディスクをアップデートする場合には、その都度クライアントのフル・バックアップを行う必要があります。これは、IP アドレスや DNS サーバの変更など、ネットワーク構成が変更された場合も同じです。

重要

Cell Manager 用の ASR セットは、前もって作成しておく必要があります。これは、障害発生後には ASR アーカイブ・ファイルを取得できないためです。他のシステム用の ASR セットは障害発生時に Cell Manager を使用して作成できます。

復旧対象となるパーティションを以下に示します。

- ブート・パーティション
- システム・パーティション
- Data Protector を含むパーティション

その他のパーティションは、通常の Data Protector 復旧手順を使って復旧できます。

以下の項で、Windows システム上での自動システム復旧に関する必要条件、制限事項、準備、および復旧について説明します。「高度な復旧作業」（603 ページ）も参照してください。

必要条件

- Data Protector の自動システム復旧コンポーネントが、ASR で復旧するシステム上にインストールされている必要があります。『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。
- オンライン ASR を可能にするには、ネットワーク上に DHCP が構成されている必要があります。

ハードウェア構成

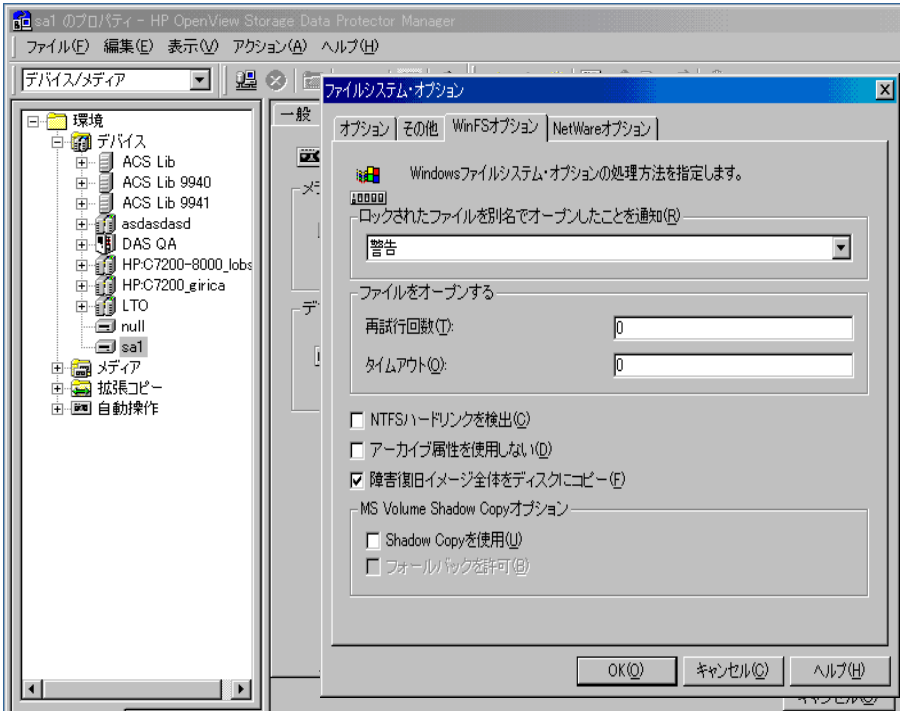
- ターゲット・システムのハードウェア構成は、元のシステムのハードウェア構成と同じでなければなりません。ただし、ハードディスク・ドライブ、ビデオ・カード、ネットワーク・インタフェース・カードは除きます。ネットワーク・カードまたはビデオ・カードを交換した場合は、それらを手動で構成する必要があります。
- フロッピー・ディスク・ドライブがインストールされている必要があります。
- フロッピー・ドライブと CD ドライブが、IDE または SCSI コントローラに接続されている必要があります。USB や PCMCIA デバイスなどの外部デバイスはサポートされていません。

ハードディスク・ドライブ

- クリティカル・ボリュームがある物理ディスクの数が、ターゲット・システムと元のシステムで同じでなければなりません。
- 交換ディスクは、同じバスの同じホスト・バス・アダプタに接続されている必要があります。
- ターゲット・システムの各交換ディスクの記憶容量は、元のシステムの対応するディスクの記憶容量以上である必要があります。さらに、交換ディスクのジオメトリも交換前のディスクと同じである必要があります。
- ターゲット・システムのすべてのディスクは、512 バイト / セクタでなければなりません。

- ASR で使用されるすべてのディスクがシステムからアクセスできる必要があります（ハードウェア RAID が構成されている、SCSI ディスクが適切にターミネートされている、など）。
- オフライン復元を計画している場合は、クライアント・バックアップ時のデバイスへの書き込みにはデフォルトのブロック・サイズ 64KB を使用してください。障害復旧を実行する際に Windows で使用できるブロック・サイズはこのデフォルトのサイズだけです。デフォルトのブロック・サイズ 64KB が設定されているかどうかを確かめるには、[プロパティ] ボックスの [拡張 . . .] を選択します。図 12-4 を参照してください。

図 12-4　デフォルトのブロック・サイズの確認



制限事項

- Windows XP Home Edition は ASR をサポートしていません。

- Microsoft のブート・ローダを使用していないマルチブート・システムはサポートされていません。
- Internet Information Server(IIS) データベース、Terminal Service データベース、Certificate Server データベースは、フェーズ 2 で自動的には復元されません。
- これらをターゲット・システムに復元するには、通常の Data Protector 復元手順を実行してください。ベンダー固有のパーティションに格納されていたデータは、ASR では自動的に復元されません。ASR 時にパーティションは再作成されますが、データはベンダー固有の手順で復元する必要があります。ただし、EISA ユーティリティ・パーティションに格納されていたデータは、Data Protector の通常の復元手順で復元できます。
- OS のインストール時に Windows によりインストール可能な（ドライバは別途不要）ローカル・バックアップ・デバイスのみがサポートされています。

準備

本項で挙げられている手順を完了する前に、すべての障害復旧方法に共通する一般的な準備手順として「障害復旧の準備」（551 ページ) も参照してください。さらに、障害復旧の準備に関して「高度な復旧作業」（603 ページ) を参照してください。

重要

障害復旧の準備は、障害が発生する**前に**行っておく必要があります。

必要条件

- 自動システム復旧を正常に行うためには、フル・クライアント・バックアップ (CONFIGURATION も含む) が必要です。「ファイルシステム (論理ディスク・ドライブ) のバックアップ」（227 ページ) および「CONFIGURATION のバックアップ」（233 ページ) を参照してください。

  Microsoft Cluster Server のための整合性のあるバックアップには、（同じバックアップ・セッションに）以下のものが含まれている必要があります。

  — すべてのノード

— 管理仮想サーバ (管理者が定義)

— Cell Manager仮想サーバとIDB(Data Protectorがクラスター対応アプリケーションとして構成されている場合)

詳細については、「Microsoft Cluster Server の復元に固有の手順」（603 ページ) を参照してください。

フル・クライアント・バックアップの実行後、ASR セットを作成する必要があります。ASR セットは 3 枚または 4 枚のフロッピー・ディスクに格納されたファイルの集まりで、交換ディスクの適切な再構成（ディスクのパーティションと論理ボリュームの構成）、および元のシステムの構成とフル・クライアント・バックアップでバックアップされたユーザー・データの自動復旧に必要なものです。これらのファイルは、バックアップ・メディア上だけでなく、ASR アーカイブ・ファイルとして Cell Manager 上の次の場所にも格納されます。
<Data_Protector_home>¥Config¥server¥dr¥asr (Windows の場合) または /etc/opt/omni/server/dr/asr/ (UNIX の場合)。ASR アーカイブ・ファイルは、障害発生後、32 ビット版 Windows システムでは 3 枚、64 ビット版 Windows システムでは 4 枚のフロッピー・ディスクに取り出されされます。ASR を実行するにはこれらのフロッピー・ディスクが必要です。

注記

Cell Manager 用の ASR セットは、前もって作成しておく必要があります。これは、障害後には ASR アーカイブ・ファイルを取得できないためです。

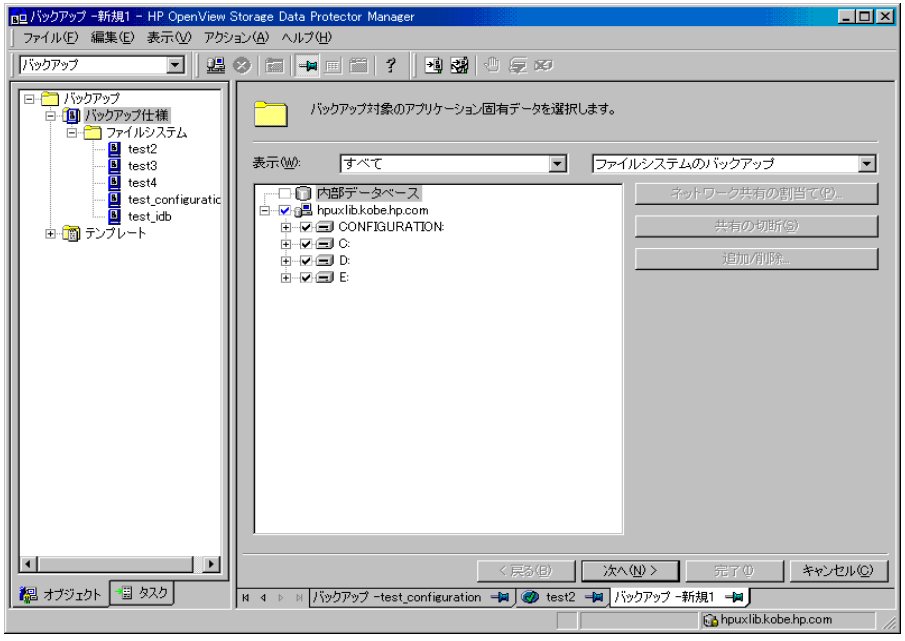
ASR セットの作成

ASR セットを作成するには、以下の手順を実行します。

1. フル・クライアント・バックアップを実行します。
2. フロッピー・ディスクをフロッピー・ディスク・ドライブに挿入します。
3. [HP OpenView Storage Data Protector Manager] で [復元] コンテキストを選択します。
4. Scoping ペインで [タスク] ナビゲーション・タブをクリックし、[障害復旧] を選択します
5. 結果エリアのドロップダウン・リストから、ASR セットを作成するクライアントを選択します。

6. ［自動システム・リカバリ・セットの作成］をクリックし、［次へ］をクリックします。

図 12-5



Data Protector が Cell Manager から ASR アーカイブ・ファイルを取得します。Cell Manager に保存されていない場合は、障害復旧ウィザードによりバックアップ・メディアから復旧するようメッセージが表示されます。

7. 各クリティカル・オブジェクトごとに、適切なオブジェクト・バージョンを選択して、［次へ］をクリックします。
8. フル・クライアント・バックアップ時に作成された ASR アーカイブ・ファイルが、Cell Manager からダウンロードされます。取得された ASR アーカイブ・ファイルの保存先を選択し、［DR インストールをコピー］チェック・ボックスを選択して、DR インストール・ファイルを同じ場所にコピーします。ASR を実行するにはこれらのファイルをフロッピー・ディスク（ASR セット）に保存する必要があるため、フロッピー・ドライブを保存先に指定することをお勧めします。

Data Protector は、32 ビット版 Windows システム用には 3 枚、64 ビット版 Windows システム用には 4 枚をディスクを作成します。Cell Manager 用の ASR セットは事前に作成しておく必要がありますが、他のシステム用の ASR ディスクは障害発生時に Cell Manager を使用して作成できます。

ASR セットの作成後、ハードウェアやソフトウェア、構成の変更があった場合には、その都度 1 枚目のディスクのみをアップデートする必要があります。これは、IP アドレスや DNS サーバの変更など、ネットワーク構成が変更された場合も同じです。ASR セットの 1 枚目のディスクをアップデートするには、最初からすべての手順を再度実行しますが、[DR インストールをコピー] チェック・ボックスを選択する必要はありません。このオプションを選択すると、アップデートには不要な DR インストール・ファイルが（選択した保存先に）コピーされます。

重要

セキュリティ上の理由から、ASR ディスクへのアクセスを制限することをお勧めします。

ローカル・デバイス

ローカル接続されたデバイスを ASR 用に使用する場合は、そのデバイスがサポートされているか確認してください。以下の手順で確認します。

1. コマンド・プロンプトから `devbra -dev` を実行します（ディレクトリは *<Data_Protector_home>*¥bin）。
2. `scsitab` ファイル（ディレクトリは *<Data_Protector_home>*）の名前を変更して、コマンド・プロンプトから `devbra -dev` を実行します。
3. `devbra -dev`コマンドの2つの出力を比較します。2つのファイルが同じであれば、ASR でそのデバイスを使用することができます。そうでない場合は、`scsitab` ファイルを ASR ディスクの 1 枚目にコピーします。`scsitab` ファイルをコピーする必要があるのは、最初に ASR セットを作成する時のみです。ASR セットのアップデートだけを行う場合には、コピーする必要はありません。詳細は、「新しいデバイスのサポート」(51 ページ) を参照してください。
4. `scsitab` ファイルの名前を元に戻します。

復旧

クラッシュしたシステムのシステムの障害復旧を正常に実行するには、以下が必要です。

- クラッシュしたディスクと交換する新しいハードディスク
- 復旧対象のクライアントの正常なフル・バックアップ
- アップデート済みの ASR セット
- Windows インストール・メディア

ASR の手順

ASR を実行する手順を以下に示します。

1. Windows インストール・メディアからシステムを起動します。
2. OS のセットアップ時に F2 キーを押して、ASR モードに入ります。
3. 障害発生後にバックアップ・デバイスを変更したなどの理由で ASR ディスク上の SRD ファイルの情報が最新のものでなく、オフライン復旧を実行しようとしている場合は、この手順を続行する前に SRD ファイルを変更してください。「編集後の SRD ファイルを使用した復旧」（612 ページ) を参照してください。
4. ASR セットの 1 枚目の（アップデート済みの）ディスクをドライブに挿入します。
5. 再起動後、障害復旧ウィザードが起動され、[DR Installation Source] と [SRD Path] の入力を求めてきます。DR インストール・ファイルと SRD ファイルは、両方とも ASR セットの 1 枚目のディスクにあります（a:¥)。
6. プロンプトが表示されたらフロッピー・ディスクを交換します。

   ASR セットの情報に基づいて、元の記憶データ構造装置の構成が自動的に再構築され、すべてのクリティカルなデータが自動的に復元されます。
7. プロンプトが表示されたらシステムを再起動し、Windows インストール・メディアと ASR ディスクを取り出します。
8. 通常の Data Protector 復元手順を使用して、ユーザー・データとアプリケーション・データを復元します。

固有の復元手順

本項では、Windows Cell Manager の復元に必要な、特別な手順を説明します。

IDB の整合性をとる (すべての方法)

本項に記載の手順は、一般的な障害復旧手順の実行後のみ使用します。

IDB の整合性をとるには、最新のバックアップがあるメディアをインポートして、バックアップされたオブジェクトの情報をデータベースにインポートします。これを行うには以下の手順を実行してください。

1. 復元対象として残っているパーティションのバックアップが保存されたメディア (1 つまたは複数) を Data Protector GUI を使ってリサイクルして、IDB へメディアをインポートできるようにします。インポート方法の詳細については、「メディアのリサイクル」を参照してください。
   メディアが Data Protector によってロックされているためにリサイクルできない場合があります。このような場合は、Data Protector プロセスを中止して、以下のコマンドを実行して ¥tmp ディレクトリを削除します。
   ```
   <Data_Protector_home>¥bin¥omnisv -stop
   del <Data_Protector_home>¥tmp¥*.*
   <Data_Protector_home>¥bin¥omnisv -start
   ```
2. 復元対象として残っているパーティションのバックアップが保存されたメディア (1 つまたは複数) を Data Protector GUI を使ってエクスポートします。エクスポート方法の詳細については、「Data Protector からのメディアのエクスポート」参照してください。
3. 復元対象として残っているパーティションのバックアップが保存されたメディア (1 つまたは複数) を Data Protector GUI を使ってインポートします。インポート方法の詳細については、「メディアのインポート」を参照してください。

拡張自動障害復旧に固有の手順

拡張自動障害復旧を使用して、Windows Cell Manager を復元する場合には、フェーズ 0 で 2 つの特別な手順が必要です。

- Cell Manager 用の障害復旧 CD を事前に用意しておく必要があります。

重要

ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行して新しい DR CD を作成します。これは、IP アドレスや DNS サーバの変更など、ネットワーク構成が変更された場合も同じです。

- 障害復旧の準備作業の一環として、Cell Manager の更新済みの SRD ファイルを、Cell Manager 以外の場所にも保存しておく必要があります。なぜなら、SRD ファイルは Data Protector で唯一、オブジェクトとメディアに関する情報が保存されているファイルだからです。SRD ファイルを Cell Manager だけにしか保存していないと、Cell Manager に障害が発生した場合に利用できなくなります。「準備」(559 ページ) を参照してください。

重要

バックアップ・メディア、DR イメージ、SRD ファイル、障害復旧 CD へのアクセスを制限しておくことをお勧めします。

ワンボタン障害復旧に固有の手順

Cell Manager がクラッシュした場合には IDB が使用できないため、OBDR のブート可能メディアの位置を知っている必要があります。

重要

ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度 OBDR バックアップを実行して新しいブート可能メディアを作成します。これは、IP アドレスや DNS サーバの変更など、ネットワーク構成が変更された場合も同じです。

重要

バックアップ・メディアへのアクセスを制限することをお勧めします。

自動システム復旧に固有の手順

自動システム復旧（ASR）を使用して Windows Cell Manager を復旧する場合には、フェーズ 0 で別途手順が必要です。

- Cell Manager 用の ASR ディスクを事前に用意しておく必要があります。

重要

ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行して ASR ディスクを更新します。これは、IP アドレスや DNS サーバの変更など、ネットワーク構成が変更された場合も同じです。

重要

バックアップ・メディアと ASR ディスクへのアクセスを制限することをお勧めします。

高度な復旧作業

本項では、Microsoft Cluster Server や Internet Information Server の復元など、高度な復旧作業を行う場合に必要な手順について説明します。

Microsoft Cluster Server の復元に固有の手順

本項では、Microsoft Cluster Server(MSCS) の障害復旧を行う場合に必要な手順について説明します。概念と一般的情報については、『HP OpenView Storage Data Protector コンセプト・ガイド』のクラスター化関連の項を参照してください。また、『HP OpenView Storage Data Protector 管理者ガイド』の「クラスターと Data Protector との統合」（769 ページ) も参照してください。

ご使用のクラスター環境に適した障害復旧方法を選択し、障害復旧プランに取り入れます。使用する障害復旧方法を決定する前に、各方法の制限事項と必要条件を検討します。テストプランを作成してテストを行います。

考えられる状況

MSCS の障害復旧では、考えられる状況が 2 つあります。

- 最低 1 台のノードが稼動している場合
- クラスター内のすべてのノードで障害が発生している場合

重要

MSCS の復旧は、「ディスク・デリバリーによる障害復旧」以外の方法で行えます。使用する障害復旧方法に関する固有の制限や必要条件は、MSCS の障害復旧にも当てはまります。サポート対象のオペレーティング・システムについては、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

MSCS を復旧するには、障害復旧の必要条件 (整合性のある最新のバックアップ、更新済みの SRD ファイル、不良ハードウェアの交換など) がすべて満たされていなければなりません。

MSCS のための整合性のあるバックアップには、（同じバックアップ・セッションに）以下のものが含まれている必要があります。

- すべてのノード
- 管理仮想サーバ (管理者が定義)
- Cell Manager 仮想サーバと IDB(Data Protector がクラスター対応アプリケーションとして構成されている場合)

二次ノードの障害復旧

これは MSCS の障害復旧についての基本的な状況です。障害復旧に関する他の必要条件に加えて、以下の条件も満たされている必要があります。

- 最低 1 台のクラスター・ノードが正常に機能していること
- そのノード上でクラスター・サービスが実行されていること
- すべての物理ディスク資源がオンラインであること (つまり、クラスターによって所有されていること)
- 通常のクラスター機能がすべて使用可能であること (クラスター管理グループがオンラインであること)
- Cell Manager がオンラインであること

この場合、クラスター・ノードの障害復旧は Data Protector クライアントの障害復旧と同じです。二次ノードの復元に使用する特定の障害復旧方法の手順に従ってください。

注記

ローカル・ディスクのみが復元されます。復旧作業中でも共有ディスクはすべてオンラインであり、稼動中のノードにより所有 / ロックされているためです。

二次ノードは、復旧完了後にブートを行うと、クラスターに参加します。

MSCS データベースの復元は、すべてのノードの復旧が完了し、それらがクラスターに参加したあとに実行できます。そうすることによって、すべてのノードが共同作用することを確実にします。MSCS データベースは、Windows の CONFIGURATION に含まれています。「Windows の CONFIGURATION の復元」(376 ページ) を参照してください。

一次ノードの障害復旧

この場合、MSCS 内のすべてのノードが使用不能で、クラスター・サービスは実行されていません。

障害復旧に関する他の必要条件に加えて、以下の条件も満たされている必要があります。

- 一次ノードはクォーラム ディスクへの書き込みが可能である必要があります (クォーラム ディスクはロックされていてはいけません)。
- Cell Manager を復旧する場合、一次ノードはすべての IDB ボリュームへの書き込みが可能である必要があります。
- すべての物理ディスク資源がオンラインになるまで、他のノードはすべてシャットダウンしておく必要があります。

この場合、一次ノードの復元の際にはクォーラム ディスクを最初に復元します。Cell Manager がクラスターにインストールされている場合には、IDB の復元も必要です。必要に応じて、MSCS データベースを復元することもできます。一次ノードの復元が完了したら、残りの全ノードの復元が可能となります。

注記

MSCS サービスは、すべてのハードディスクの MBR に書き込まれているハードディスク署名を使用して物理ディスクを識別しています。共有クラスター・ディスクを交換した場合、障害復旧のフェーズ 1 でこのディスク署名が変わることになります。その結果、クラスター・サービスは交換されたディスクを有効なクラスター資源として認識せず、その資源に依存するクラスター・グループは正常に動作しません。詳しくは、「Windows でのハード・ディスク署名の復元」(608 ページ) を参照してください。

一次ノードの復元は、以下の手順で行います。

1. 一次ノード (クォーラム ディスクも含む) の障害復旧を行います。
   - 半自動障害復旧の場合 : クォーラム ディスク上のすべてのユーザー・データとアプリケーション・データは、`drstart` コマンド (`-full_clus` オプション付き) で自動的に復元されます。
   - 拡張自動障害復旧およびワンボタン障害復旧の場合 : 復旧範囲を尋ねられたときに、共有ボリュームを含む完全復旧を選択してクォーラム ディスクを復元します

- 自動システム復旧の場合: 自動システム復旧の場合: クォーラム ディスク上のすべてのユーザー・データとアプリケーション・データは、自動的に復元されます。

ヒント

OBDR で、MSCS 内の全共有ディスク・ボリュームの自動復元を可能にするには、ボリュームをすべて OBDR ブート・テープの準備作業に使用するノードに一時的に移動します。他のノードによりロックされている共有ディスク・ボリュームのディスクをフェーズ 1 で構成するために必要な情報を収集するのは不可能です。

2. コンピュータを再起動します。
3. クラスター・データベースを復元します。MSCS データベースは、Windows の CONFIGURATION に含まれています。「Windows の CONFIGURATION の復元」（376 ページ) を参照してください。

注記

MSCS データベースを復元するには、MSCS サービスが実行中である必要があります。したがって、障害復旧のフェーズ 2 では自動的に復元されません。しかし、クラスター・データベースはフェーズ 2 の最後に通常の Data Protector 復元手順で復元できます。

4. Cell Manager を復元している場合は、IDB の整合性を取ります。「IDB の整合性をとる (すべての方法)」（600 ページ) を参照してください。
5. 定数ボリュームと IDB ボリュームが復元されます。他のすべてのボリュームは影響を受けず、破損していなければ復元された一次ノードにより所有されます。

   他のボリュームが破損していた場合は、以下を行う必要があります。

   a. クラスター・サービスとクラスター・ディスク・ドライバを使用不可にします (MSDN Q176970 に記述されているとおりに行う必要があります)。
   b. システムを再起動します。
   c. 従来の記憶データ構造を再構築します。
   d. クラスター・サービスとクラスター・ディスク・ドライバを使用可

能にします。

e. システムを再起動します。

f. ユーザー・データとアプリケーション・データを復元します。

6. 残りのノードを復元します。「二次ノードの障害復旧」(604 ページ) を参照してください。

EADR 用に全ノードの P1S ファイルをマージ

EADR を行うには、バックアップ実行後に特別な手順が必要です。バックアップ時に他のノードによりロックされている共有ディスク・ボリュームのディスクをフェーズ 1 で構成するために必要な情報を収集するのは不可能です。すべての共有ディスク・ボリュームを復元するにはこの情報が必要です。クラスター内の全ノードの P1S ファイルに共有クラスター・ボリューム情報を含めるには、以下のいずれかを実行します。

- フル・クライアント・バックアップ実行後、クラスター内の全ノードの P1S ファイルに含まれる共有クラスター・ボリューム情報をマージする。これにより、各ノードの P1S ファイルには共有クラスター・ボリューム構成の情報が格納されます。
- すべての共有クラスター・ボリュームを一時的にバックアップ対象のノードに移動する。こうすれば、すべての共有クラスター・ボリュームに関する必要情報が収集されます。この場合、一次ノードにできるのはこのノードだけです。

マージ

全ノードの P1S ファイルをマージするには、*<Data_Protector_home>*¥bin¥drim¥bin から mmerge.cmd コマンドを実行します。

```
mmerge p1sA_path ... p1sX_path
```

ここで、p1sA は MSCS 内の最初のノードの P1S ファイルへのフルパスであり、p1sX は最後のノードの P1S ファイルへのフルパスです。マージ後の P1S ファイルは元の P1S ファイルと同じディレクトリに保存され、ファイル名には .merged が追加されます (例 : computer.company.com.merged)。元のファイルの他のディレクトリに移動した後、マージ後の P1S ファイルの名前を元の名前に変更します (.merged 拡張子を削除する)。

UNIX Cell Manager

`mmerge.cmd` コマンドは、Data Protector 自動障害復旧モジュールがインストールされた Windows システムでのみ動作します。UNIX Cell Manager を使用している場合は、P1S ファイルを自動障害復旧モジュールがインストールされた Windows クライアントにコピーして、ファイルをマージします。マージ後の P1S ファイルの名前を元の名前に変更し、Cell Manager にコピーします。

例

2 台のノードがある MSCS の P1S ファイルをマージする例 : `mmerge <Data_Protector_home>¥Config¥server¥dr¥p1s¥node1.company.com <Data_Protector_home>¥Config¥server¥dr¥p1s¥node2.company.com`。パス名に空白が含まれている場合には、Windows ではパス名を引用符で囲む必要があります。マージ後のファイルは、`node1.company.com.merged` と `node2.company.com.merged` です。これらのファイルの名前を元の名前に変更します (まず元の P1S ファイルの名前を変更する必要があります）: node1.company.com および node2.company.com。

Windows でのハード・ディスク署名の復元

MSCS サービスは、すべてのハードディスクの MBR に書き込まれているハードディスク署名を使用しています。共有クラスター・ディスクを交換した場合、障害復旧のフェーズ 1 でこのディスク署名が変わることになります。その結果、クラスター・サービスは交換されたディスクを有効なクラスター資源として認識せず、その資源に依存するクラスター・グループは正常に動作しません。最低 1 台のノードが稼動中でその資源を所有している限り、共有クラスター資源は運用可能であるため、これはアクティブなノードを復元する場合のみ当てはまります。また、EADR/OBDR ではクリティカル・ディスクの元のディスク署名が自動的に復旧されるため、この問題は EADR と OBDR のクリティカル・ディスクには当てはまりません。クリティカル・ディスク以外のディスクを交換した場合は、そのハード・ディスク署名を復元する必要があります。

最も重要な共有ディスクはクラスターのクォーラム・リソースです。これを交換した場合は元のディスク署名を復元する必要があり、そうしないとクラスター・サービスは開始しません。

フェーズ 2 において、MSDS データベースはシステム・ボリュームの `¥TEMP¥ClusterDatabase` に復元されます。フェーズ 1 でハード・ディスク署名が変わっているためクォーラム・リソースが識別されず、システムを再起動してもクラスター・サービスは実行されません。これは、

(*<Data_Protector_home>*¥bin¥utilns にある)clubar ユーティリティを実行することで解決できます。これは元のハードディスク署名を復元するユーティリティです。clubar が正常終了すると、クラスター・サービスが自動的に開始されます。

例

コマンド・プロンプトで clubar r c:¥temp¥ClusterDatabase force q: と入力して、MSCS データベースを c:¥temp¥ClusterDatabase から復元します。

clubar の使用法と構文の詳細は、*<Data_Protector_home>*¥bin¥utilns にある clubar.txt テキスト・ファイルを参照してください。

Cell Manager 上の Data Protector 共有ディスクがクォーラム ディスクと異なる場合は、これも復元する必要があります。Data Protector 共有ディスクと他のアプリケーション・ディスクの署名を復元するには、Windows 2000 リソース・キットに含まれている dumpcfg.exe ユーティリティを使用します。dumpcfg.exe の使用法の詳細は、dumpcfg /? を実行するか、Windows 2000 リソース・キットのマニュアルを参照してください。Windows 2000 におけるハードディスク署名に関する問題については、MSDN Q280425 を参照してください。

元のハードディスク署名は SRD ファイルから取得できます。SRD ファイル内の署名には、番号の後に volume というキーワードが付いています。

例

```
-volume 5666415943 -number 0 -letter C -offslow 32256
-offshigh 0 -lenlow 320430592 -lenhigh 2 -fttype 4 -ftgroup
0 -ftmember 0

-volume 3927615943 -number 0 -letter Q -offslow 320495104
-offshigh 2 -lenlow 1339236864 -lenhigh 0 -fttype 4 -ftgroup
0 -ftmember 0
```

-volume の後の数字がハードディスク署名です。この例では、SRD ファイルにはローカル・ハードディスク (ドライブ文字 C) とクォーラム ディスク (ドライブ文字 Q) に関する情報が保存されています。クォーラム ディスクの署名は、バックアップ時にアクティブであったのノードの SRD ファイルにだけ保存されています。これは、アクティブなノードがクォーラム ディスクをロックしており、他のノードはクォーラム ディスクにアクセスできないためです。したがって、常にクラスター全体のバックアップを取ることをお勧めします。これは、フェーズ 1 で共有ディスク・ボリュームのディスクを構成するのに十分な情報を得るにはすべての SRD ファイルを揃

える必要があり、これにはクラスター内の全ノードの SRD ファイルが必要なためです。SRD ファイルに保存されているハードディスク署名は 10 進数で表示されていることに注意してください。これに対して、dumpcfg コマンドでは 16 進数を指定する必要があります。

Internet Information Server (IIS) の復元に固有の手順

Internet Information Server (IIS) は、障害復旧ではサポートされていません。IIS の半自動障害復旧を行うには、(通常の半自動障害復旧の手順に加えて) 以下の手順を実行してください。

1. システムのクリーン・インストール中に IIS をインストールしないでください。
2. IIS Admin Service が実行されている場合は、それを停止またはアンインストールします。
3. drstart コマンドを実行します。
4. IIS データベースがプレーン・ファイルとして、デフォルトの IIS ディレクトリ (%SystemRoot%¥system32¥inetsrv) に復元されます (ファイル名は DisasterRecovery)。
5. ブートが正常に終了したら、標準の Data Protector 復元手順、または IIS バックアップ / 復元スナップ・インを使用して、IIS データベースを復元します。この処理は長時間かかることに注意してください。

トラブルシューティング

1. IIS に依存するサービス (SMTP、NNTP など) のいずれかが自動的に起動されない場合は、手動での起動を試みてください。
2. 手動でも起動できない場合は、IIS Admin Service を停止して、%SystemRoot%¥system32¥inetsrv¥MetaBase.bin ファイルを overwrite オプションを使用して復元してください。

注記

%SystemRoot%¥system32¥inetsrv は IIS サービスのデフォルトのディレクトリです。IIS サービスを別のディレクトリにインストールした場合は、MetaBase.bin ファイルの復元先としてそのディレクトリを指定してください。

3. IIS Admin Service と、それに依存するサービスをすべて起動します。

DRecoveryKB.cfg ファイルの編集

ドライバの中には、正常に動作するために必要な機能が複数のファイルに分かれているものがあります。それらが DRecoveryKB.cfg ファイルに逐次列挙されていなければ、Data Protector は DR イメージ・ファイルの作成中にすべてのドライバ・ファイルを特定できません。この場合、それらのファイルは障害復旧操作システムに含まれず、その結果、DR OS の起動後に一部のドライバやサービスが動作しなくなります。

The DRecoveryKB.cfg ファイルは *<Data_Protector_home>*¥bin¥drim¥bin ディレクトリにあり、*%SystemRoot%* ディレクトリにあるドライバ・ファイルの位置に関する情報を含んでいます。テスト・プランの実行時に、OS が起動した後、必要なサービスがすべて実行中で、必要なドライバがすべて動作することを確認してください。

これらのドライバをバックアップする場合は、依存ファイルの情報を DRecoveryKB.cfg ファイルに適切な形式で追加します。この形式についての指示は、DRecoveryKB.cfg ファイルの最初に記述されています。

このファイルを編集する最も簡単な方法は、既存の行をコピー、ペーストして適切な情報に書き換えることです。パスの区切り文字が / （スラッシュ）であることに注意してください。パス名が引用符で囲まれている場合以外、空白は無視されます。したがって、エントリを複数行にまたがって記述することもできます。また、# （シャープ）記号で始まり行末で終わるコメント行も追加できます。

ファイルの編集が終了したら、元の場所に保存します。次に、追加したファイルを DR イメージに含めるために、「準備」（575 ページ）の記述に従ってフル・クライアント・バックアップを再度実行します。

システムのハードウェアやアプリケーションの構成は様々であるため、すべての構成に対して「出来合い」の解決法を提供することはできません。そのため、自らの責任でこのファイルを変更して、ドライバや他のファイルを含めてください。

このファイルへのあらゆる変更はユーザーの責任であり、Hewlett-Packard のサポート対象外となります。

警告

DRecoveryKB.cfg ファイルの編集後に復旧が正常動作するかを確認するため、テスト・プランを作成して実行する必要があります。

編集後の SRD ファイルを使用した復旧

SRD ファイルの編集

障害復旧を実行する時点で、SRD ファイルに保存されているバックアップ・デバイスまたはメディアに関する情報が古くなっている場合もあります。オンライン復旧を実行する場合には、必要な情報が Cell Manager の IDB に保存されているため、これは問題となりません。しかしオフライン復旧を行う場合には、IDB の保存されている情報にアクセスできません。

たとえば、障害が Cell Manager だけでなく、それに接続されたバックアップ・デバイスでも発生した場合、障害発生後にそのバックアップ・デバイスを別のバックアップ・デバイスに交換すると、更新された SRD ファイル (`recovery.srd`) に保存されているバックアップ・デバイスに関する情報は正しくなくなり、復旧は失敗します。この場合は、更新された SRD ファイルを障害復旧のフェーズ 2 を実行する前に編集して、復旧が正常終了するように不正な情報を更新します。

SRD ファイルを修正するには、テキスト・エディタでこのファイルを開いて変更された情報を更新します。

ヒント

`devbra -dev` コマンドを使用すると、デバイス構成情報を表示できます。

たとえば、復旧しようとしているコンピュータのクライアント名が変更されている場合は、`-host` オプションの値を書き換えます。以下に示す項目についても情報の修正が可能です。

- Cell Manager クライアント名 (`-cm`)
- Media Agent クライアント (`-mahost`)
- 論理デバイスまたはドライブ (ライブラリ) の名前 (`-dev`)
- デバイスの種類 (`-devtype`)

-devtype オプションに指定できる値については、「ライブラリ・デバイスの初期構成」（76 ページ) を参照してください。

- デバイスの SCSI アドレス (-devaddr)
- デバイスのポリシー (-devpolicy)

  ポリシーには、1(スタンドアロン)、3(スタッカー)、5(ジュークボックス)、6(外部制御)、8(Grau DAS エクスチェンジャ・ライブラリ)、9(STK サイロ・メディア・ライブラリ)、10(SCSI-II ライブラリ) のいずれかを定義します。
- ロボティクスの SCSI アドレス (-devioctl)
- ライブラリ・スロット (-physloc)
- 論理ライブラリ名 (-storname)

ファイルを編集し終わったら、元の場所に Unicode 形式で保存してください。

MA クライアントの変更例

old_mahost.company.com クライアントに接続されたバックアップ・デバイスを使用して、障害復旧バックアップを実行した場合を考えてみましょう。障害復旧時には、このバックアップ・デバイスが new_mahost.company.com クライアントに同じ SCSI アドレスで接続されていたとします。この場合、障害復旧を適切に実行するには、障害復旧のフェーズ 2 を開始する前に、(更新された)SRD ファイル内の -mahost old_mahost.company.com 文字列を -mahost new_mahost.company.com に変更する必要があります。

新しい MA クライアント上でバックアップ・デバイスの SCSI アドレスが変更されている場合は、更新された SRD ファイル内の -devaddr オプションの値を適切に変更してください。

バックアップ・デバイスと MA クライアントの変更例

バックアップ時とは異なるデバイスを使用して障害復旧を実行するには (MA クライアントは同じものを使用)、更新された SRD ファイル内の以下のオプションの値を変更します。-dev、-devaddr、-devtype、-devpolicy、および -devioctl。復元にライブラリ・デバイスを使用する場合は、SRD ファイル内の以下のオプションの値も変更してください。-physloc および -storname。

たとえば、障害復旧の目的で、HP StorageWorks Ultrium スタンドアロン・デバイスを使用してバックアップを実行した場合を考えてみましょう。デバイス名は Ultrium_dagnja で、MA ホスト dagnja(Windows) に接続され

ています。ただし障害復旧時には、HP StorageWorks Ultrium ロボティクス・ライブラリを使用するものとします。このライブラリの論理ライブラリ名は Autoldr_kerala で、ドライブ Ultrium_kerala が MA クライアント kerala(Linux) に接続されています。

最初に kerala 上で devbra -dev コマンドを実行して、構成されているデバイスとその構成情報の一覧を確認しておきます。この情報は、更新された SRD ファイル内の以下のオプション値を変更するために必要です。

```
-dev "Ultrium_dagnja" -devaddr Tape4:1:0:1C -devtype 13
-devpolicy 1 -mahost dagnja.company.com
```

次に例を示します。

```
-dev "Ultrium_kerala" -devaddr /dev/nst0 -devtype 13
-devpolicy 10 -devioctl /dev/sg1 -physloc "     2 -1"
-storname "AutoLdr_kerala" -mahost kerala.company.com
```

編集後の SED ファイルを障害復旧に使用する手順は、それぞれの障害復旧方法により異なります。詳細は個々の障害復旧方法に関する項を参照してください。

重要

セキュリティ上の理由から、SRD ファイルへのアクセスは制限する必要があります。

AMDR/ASR

通常の AMDR/ASR 復旧手順を実行する前に、以下を実行します。

1. 最初の drsetup / ASR ディスクにある recovery.srd ファイルをテキスト・エディタで開き、必要な変更を行います。
2. Unicode 形式で元の場所に保存します。

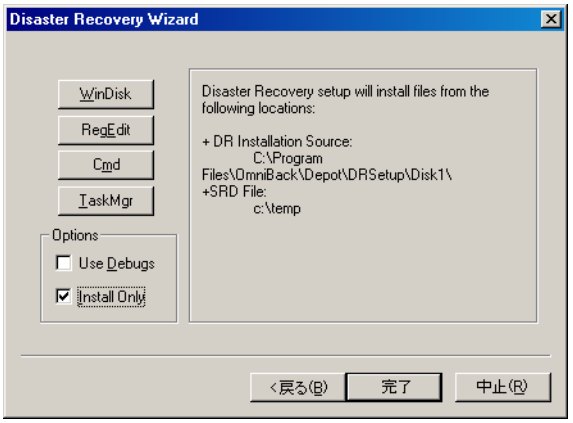
EADR/OBDR

通常の EADR/OBDR 復旧手順を実行する前に、以下を実行します。

1. 障害復旧ウィザードが表示されたら、カウントダウン中にいずれかのキーを押してウィザードを停止し、Install only オプションを選択して、[完了] をクリックします。このオプションを選択すると、対象の

システムに一時オペレーティング・システムのみがインストールされて、障害復旧のフェーズ 1 を完了できます。Install only を選択した場合、障害復旧のフェーズ 2 は自動的には開始されません。

図 12-6　障害復旧ウィザードの［Install only］オプション



2. Windows タスク・マネージャを実行します（alt+ctrl+del キーを押し、タスク・マネージャを選択）。
3. ［ファイル］をクリックし、［新しいタスクの実行］を選択します。notepad c:¥DRSYS¥System32¥OB2DR¥bin¥recovery.srd と入力して Enter を押すと、ノートパッドで SRD ファイルが開きます。
4. SRD ファイルを編集します。編集方法の詳細は、「システム復旧データ (SRD) の更新と編集」（553 ページ) を参照してください。
5. SRD ファイルを編集して保存したら、c:¥DRSYS¥System32¥OB2DR¥bin ディレクトリから以下のコマンドを実行します。

   ```
   omnidr -drimini c:¥$DRIM$.OB2¥OBRecovery.ini
   ```

6. 通常の EADR/OBDR 復旧手順における次の手順に進みます。

HP-UX クライアントの手動による障害復旧

本項では、HP-UX クライアントの障害復旧手順を説明します。

この手順は Ignite-UX 製品をベースにしています。これは主に HP-UX システムのインストールと構成作業用に開発されたアプリケーションで、(システム管理用の強力なインタフェースに加え) システム障害に対する準備と復旧のための機能を備えています。

Ignite-UX はターゲット・クライアントの障害復旧に特化しているため、障害復旧のフェーズ 3 でユーザー・データとアプリケーション・データを復元するには Data Protector を使用する必要があります。

本項では、Ignite-UX のすべての機能を説明できません。詳しくは『Ignite-UX 管理ガイド』を参照してください。

概念

Ignite-UX で、障害に対する準備と障害の復旧を行うには 2 つの方法があります。

- カスタム・インストール・メディアを使用する (ゴールドイメージ)
- システム復旧ツールを使用する (**make_tape_recovery**、**make_net_recovery**)

ゴールドイメージを使用する方法は、ハードウェア構成と OS リリースが基本的に同じシステムが多い IT 環境に適しています。一方、システム復旧ツールを使用する方法は、お使いの個々のシステムに合わせた復旧アーカイブの作成をサポートしています。

どちらの方法でも、DDS テープや CD などのブート可能インストール・メディアの作成が可能です。これらのメディアを使用して、システム管理者は障害が発生したクライアントのシステム・コンソールから直接、ローカルに障害復旧を行うことができます。

さらに、どちらの方法でも、故障したクライアントに適切なゴールドイメージまたは事前に作成した「復旧アーカイブ」を割り当てることにより、クライアントのネットワークを利用して復旧を実行できます。この場合、クライアントは Ignite サーバから直接ブートし、割り当てられたデポからインストールを実行します。このデポはネットワークの NFS 共有にある必要があります。

サポートされている場合は、Ignite-UX GUI を使用してください。

カスタム・インストール・メディアの使用

概要

大規模な IT 環境では、それを構成する多くのシステムが同じハードウェアやソフトウェアをベースにしている場合が多いものです。あるインストール済みのシステムの完全なスナップショットを他のシステムのインストールに使用すれば、OS やアプリケーションのインストールやパッチ適用の手間が大幅に軽減されます。Ignite-UX には、ゴールドイメージなどを別のシステムに割り当てる前に、ネットワークやファイルシステムの設定パラメータを変更したり、Data Protector などのソフトウェアをイメージへ追加したりする機能 (Ignite-UX の `make_config` コマンド) があります。そこで、この機能を使用してシステムの障害復旧を行うことができます。

「ゴールドイメージ」の作成

ゴールドイメージの作成手順

以下に、ターゲット・クライアント・システムのゴールドイメージの作成手順を示します。クライアント・システムは、ゴールドイメージをネットワークの NFS を介して共有します。この例では、Data Protector クライアントはすでにクライアント・システムにインストールされており、特別な構成手順を行わなくても「ゴールドイメージ」に含まれることになります。

1. `/opt/ignite/data/scripts/make_sys_image` ファイルを、Ignite-UX サーバからクライアント・システムの一時ディレクトリにコピーします。
2. 次のコマンドをクライアント・システム上で実行し、クライアントの圧縮イメージを別のシステム上に作成します : `make_sys_image -d <directory of the archive> -n <name of the archive>.gz -s <IP address of the target system>`
   引数は以下のとおりです。
   directory of the archiveアーカイブのディレクトリ
   name of the archiveアーカイブ名
   IP address of the target systemターゲット・システムの IP アドレス

   このコマンドにより、GZIP で圧縮されたファイル・デポが `-d` と `-s` オプションで指定したシステムの指定ディレクトリに作成されます。

HP-UX クライアントが、ターゲット・システムへのパスワードなしのアクセス権を与えられていることを確認してください (ターゲット・システムの .rhosts ファイルにクライアント・システムのエントリがあること)。アクセス権がないと、コマンドは失敗します。

3. ターゲット・ディレクトリをターゲット・システムの /etc/exports ディレクトリに追加し、このディレクトリをターゲット・サーバにエクスポートします (exportfs -av)
4. Ignite-UX サーバの構成で、アーカイブ・テンプレート・ファイル core.cfg を archive_<name>.cfg にコピーします。
   cp /opt/ignite/data/examples/core.cfg /var/opt/ignite/data/<OS_Release>/archive_<name>.cfg

   例

   cp /opt/ignite/data/examples/core.cfg /var/opt/ignite/data/Rel_B.11.11/archive_HPUX11_11_DP50_CL.cfg
5. コピーした構成ファイルの以下のパラメータを確認して変更します。
   - sw_source セクション :

     load_order = 0

     source_format = archive

     source_type="NET"

     # change_media=FALSE

     post_load_script = "/opt/ignite/data/scripts/os_arch_post_l"

     post_config_script = "/opt/ignite/data/scripts/os_arch_post_c"

     nfs_source = "<IP Target System>:<Full Path>”
   - 対応する OS archive セクション :

     archive_path = "<archive_name>.gz
6. archive_impact コマンドをイメージファイルに対して実行して「impacts」エントリの値を決定し、出力を構成ファイル /opt/ignite/lbin/archive_impact -t -g <archive_name>.gzの同じ「OS archive」セクションにコピーします。

   例

   /opt/ignite/lbin/archive_impact -t -g /image/archive_HPUX11_11_DP50_CL.gz

```
impacts = "/" 506Kb
impacts = "/.root" 32Kb
impacts = "/dev" 12Kb
impacts = "/etc" 26275Kb
impacts = "/opt" 827022Kb
impacts = "/sbin" 35124Kb
impacts = "/stand" 1116Kb
impacts = "/tcadm" 1Kb
impacts = "/usr" 729579Kb
impacts = "/var" 254639Kb
```

7. Ignite-UX に新しく作成したデポを認識させるには、cfg エントリを /var/opt/ignite/INDEX ファイルに以下のレイアウトで追加します。

```
cfg "<This_configuration_name>" {
description "<Description of this configuration>"
"/opt/ignite/data/<OS>/config"
"/var/opt/ignite/data/<OS>/ archive_<name>.cfg
}
```

例

```
cfg "HPUX11_11_DP50_Client" {
description "HPUX 11.i OS incl Patches and DP50 Client"
"/opt/ignite/data/Rel_B.11.11/config"

"/var/opt/ignite/data/Rel_B.11.11/archive_HPUX11_11_DP50_CL.cfg
"
}
```

8. ブートするクライアント用に予約してある 1 つまたは複数の IP アドレスが、/etc/opt/ignite/instl_boottab ファイルで構成されていることを確認してください。IP アドレスの数は同時にブートするクライアントの数と同じです。

上記の手順を完了すると、HP-UX クライアントのゴールドイメージ (固有のハードウェアおよびソフトウェア構成を含む) が作成されます。このイメージは、同様の構成のシステムを復旧するために使用することができます。

ハードウェアおよびソフトウェア構成が異なるシステムすべてに対して、ゴールドイメージの作成手順を繰り返します。

注記

Ignite-UX を使用して、作成したゴールドイメージからブート可能なテープや CD を作成することができます。詳しくは、『Ignite-UX 管理ガイド』を参照してください。

復旧

ゴールドイメージ使用した復旧

ネットワークの NFS 共有上にあるゴールドイメージを適用して HP-UX クライアントを復旧するには、以下の手順を実行してください。

- クライアント・システムでの手順

  1. 障害が発生したハードウェアを交換します。
  2. HP-UX クライアントを Ignite-UX サーバからブートします。
     `boot lan.<IP-address Ignite-UX server>install`
  3. `Welcome to Ignite-UX` 画面が表示されたら `Install HP-UX` を選択します。
  4. UI オプション画面で [`Remote graphical interface running on the Ignite-UX server`] を選択します。
  5. ネットワーク構成ダイアログに応答します。
  6. 以上で、Ignite-UX サーバによるリモート制御インストールに対するクライアント・システムの準備は完了です。

- Ignite-UX サーバでの作業

  7. Ignite-UX GUI の [`client`] アイコンを右クリックし、[`Install Client`] → [`New Install`] を選択します。
  8. インストールするゴールドイメージを選択し、設定 (ネットワーク、ファイルシステム、タイムゾーンなど) をチェックして、[`Go!`] ボ

タンをクリックします。

9. [client] アイコンを右クリックして [Client Status...] を選択すると、インストールの進行状況が確認できます。
10. インストールが完了したら、通常の Data Protector 復元手順でユーザー・データとアプリケーション・データの復元を行います。

システム復旧ツールの使用

概要

Ignite-UX にバンドルされているシステム復旧ツールにより、ディスク障害の復旧を迅速かつ容易に行うことができます。システム復旧ツールの復旧アーカイブには HP-UX の必須ディレクトリのみが含まれます。しかし、復旧をより迅速に行うために、他のファイルやディレクトリ (追加のボリューム・グループもしくは Data Protector のファイルおよびディレクトリなど) をアーカイブに含めることも可能です。

make_tape_recovery は、ブート可能な復旧 (インストール）テープを作成するツールです。この復旧テープはご利用のシステムにカスタマイズされており、バックアップ・デバイスをターゲット・システムに直接接続して、ターゲット・システムをこのブート可能な復旧テープからブートすることで、無人の障害復旧が可能となります。アーカイブ作成時とクライアント復旧時は、バックアップ・デバイスをクライアントにローカル接続しておく必要があります。

make_net_recovery は、ネットワーク上の Ignite-UX サーバまたは他の指定システム上に、復旧アーカイブを作成するツールです。ターゲット・システムは、Ignite-UX の make_boot_tape コマンドで作成したブート可能なテープからブートするか、または Ignite-UX サーバから直接ブートした後、サブネットを通じて復旧することができます。Ignite-UX サーバからの直接ブートは、Ignite-UX の bootsys コマンドで自動的に行うか、またはブート・コンソールから対話的に指定して行うことができます。

復旧アーカイブの作成

HP-UX 用の復旧アーカイブを作成する最も簡単な方法は、Ignite-UX サーバ上で Ignite-UX GUI を使用することです。GUI コマンドはすべて、コマンド行からも実行できます。詳しくは『Ignite-UX 管理ガイド』を参照してください。

必要条件

システム障害に対する準備を行う前に、Ignite-UX ファイルセットをクライアントにインストールして、Ignite-UX サーバとクライアントが通信できるようにする必要があります。

Ignite-UX のバージョンが、Ignite-UX サーバとクライアントで同じになるようにします。すべてを整合性のとれた状態にする最も簡単な方法は、Ignite-UX を Ignite-UX サーバ上に構築されたデポからインストールすることです。このデポを構築するには、Ignite-UX サーバで以下のコマンドを実行します。

```
pkg_rec_depot -f
```

これにより、Ignite-UX のデポが `/var/opt/ignite/depots/recovery_cmds` ディレクトリに作成されます。クライアントで `swinstall` コマンドにより Ignite-UX をインストールする際に、このディレクトリをソース・ディレクトリとして指定します。

クライアントに Ignite-UX をインストールしたら、Ignite-UX サーバの GUI で、`make_net_recovery` または `make_tape_recovery` を使用して復旧アーカイブを作成します。

make_tape_recovery を使用したアーカイブの作成

`make_tape_recovery` を使用してアーカイブを作成するには、以下の手順を実行します。

1. バックアップ・デバイスが HP-UX クライアントに接続されていることを確認してください。
2. 以下のコマンドを実行して Ignite-UX GUI を起動します。
   `/opt/ignite/bin/ignite &`
3. `[client]` アイコンを右クリックして、`[Create Tape Recovery Archive]` を選択します。
4. HP-UX クライアントに複数のデバイスが接続されている場合には、デープ・デバイスを選択します。
5. アーカイブに含めるボリューム・グループを選択します。
6. テープ作成プロセスが開始されます。クライアント・アイコンを右クリック後 `[Client Status]` を選択して、ステータスと Ignite-UX サーバ上のログ・ファイルを確認します。

注記

Ignite-UX では、すべての DDS がどの DDS ドライブでも確実に使用できるように、90m の DDS1 バックアップ・テープの使用を推奨しています。

make_net_recovery を使用したアーカイブの作成

make_net_recovery を使用した復旧アーカイブの作成手順は、make_tape_recovery の場合とほとんど同じです。この方法の利点は、復旧アーカイブがデフォルトで Ignite-UX サーバ上に保存されるため、ローカルに接続するデバイスが不要である点です。

1. 以下のコマンドを実行して Ignite-UX GUI を起動します。
   `/opt/ignite/bin/ignite &`
2. [client] アイコンを右クリックして、[Create Network Recovery Archive] を選択します。
3. 保存先のシステムとディレクトリを選択します。圧縮されたアーカイブが保存できるだけの容量があることを確認してください。
4. アーカイブに含めるボリューム・グループを選択します。
5. アーカイブ作成プロセスが開始されます。クライアント・アイコンを右クリック後 [Client Status] を選択して、ステータスと Ignite-UX サーバ上のログ・ファイルを確認します。

注記

Ignite-UX では、ブート可能なアーカイブ・テープを圧縮アーカイブ・ファイルから作成することができます。『Ignite-UX 管理ガイド』の「ネットワーク経由でのリカバリアーカイブの作成」を参照してください。

復旧

バックアップ・テープからの復旧

make_tape_recovery で作成したブート可能なテープを使用してシステムの障害復旧を行うには、以下の手順で行います。

1. 障害が発生したハードウェアを交換します。
2. クラッシュした HP-UX クライアントにテープ・デバイスがローカル接続されており、復元したいアーカイブが保存されたメディアがそのデバイスに挿入されていることを確認してください。

3. 用意した復旧テープからブートします。そのためには、boot admin メニューで SEARCH と入力して、使用可能なすべてのブート・デバイスのリストを出力します。使用するテープ・デバイスを決定し、次のブート・コマンドを入力します : boot *<hardware path>* または boot P<number>
4. 復旧プロセスが自動的に開始されます。
5. インストールが正常に完了したら、通常の Data Protector 復元手順でユーザー・データとアプリケーション・データの復元を行います。

ネットワークからの復旧

HP-UX クライアントの障害復旧をネットワーク経由で行うには、ゴールドイメージによる復旧手順に従います。インストールしたいアーカイブが選択されていることを確認します。

- クライアントでの手順

  1. 障害が発生したハードウェアを交換します。
  2. HP-UX クライアントを Ignite-UX サーバからブートします。boot lan.*<IP-address Ignite-UX server>* install
  3. [Welcome to Ignite-UX] 画面で [Install HP-UX] を選択します。
  4. UIオプション画面で [Remote graphical interface running on the Ignite-UX server] を選択します。
  5. ネットワーク構成ダイアログに応答します。
  6. 以上で、Ignite-UX サーバからのリモート制御インストールに対するクライアント・システムの準備は完了です。

- Ignite-UX サーバでの作業

  7. Ignite-UX GUI の [client] アイコンをクリックし、[Install Client] → [New Install] を選択します。
  8. [Configurations] で、インストールする [Recovery Archive] を選択して設定 (ネットワーク、ファイルシステム、タイムゾーンなど) を確認し、[Go!] をクリックします。
  9. [client] アイコンを右クリックして [Client Status...] を選択すると、インストールの進行状況が確認できます。
  10. インストールが正常に完了したら、通常の Data Protector 復元手順で

ユーザー・データとアプリケーション・データの復元を行います。

UNIX クライアントのディスク・デリバリーによる障害復旧

UNIX クライアントのディスク・デリバリーによる障害復旧を実行するには、最低限の OS と Data Protector Disk Agent が含まれているブート可能なディスクを、クラッシュしたシステムに接続します。管理者は、ディスクのフォーマットおよびパーティションの構成が正しく行われるよう、障害発生前に十分なデータを収集する必要があります。

サポート対象のオペレーティング・システムは、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

制限事項

- ここでは、クラスター環境の復旧については説明しません。クラスター環境の構成によっては、特別な手順や環境の変更が必要です。
- RAID はサポートされていません。
- ターゲット・システムと同じハードウェア・クラスのシステム上に、補助ディスクを用意する必要があります。

準備

障害復旧の準備作業は、いくつかの段階に分けて実行します (バックアップ仕様の情報の収集、ディスクの準備、バックアップ仕様 (実行前コマンド) の準備、バックアップの実行など)。クライアントの障害復旧を実行する前に、これらの準備手順をすべて行うことが必要です。

情報の収集

本項では、復旧作業を正しく実行するため、バックアップ時に各ターゲット・システムに対して実行する必要のある項目を示します。これらの情報を実行前コマンドの一部として収集する場合は、これらのファイルのあるディレクトリを障害復旧プランに明記して、障害発生時にこの情報を見つけやすくしておくことが必要です。また、バージョン管理 (バックアップごとの「補助情報」を集めたもの) についても考慮が必要です。

- バックアップ対象のシステムがアプリケーション・プロセスを低実行レベルで実行している場合は、復旧後のエラーを避けるため、**「最小限の動作」**状態 (修正 **"init 1" 実行レベル**) を確立して、シングル・ユー

ザー・モードに入ることが必要です（「整合性と関連性を兼ね備えたバックアップ」（552 ページ) を参照してください)。詳細は、お使いのオペレーティング・システムのマニュアルを参照してください。

HP-UX の例

1. 抹消リンクを /sbin/rc1.d から /sbin/rc0.d へ移動して、ブート・セクションに対する変更内容を補足します。抹消リンクには基本サービスが含まれており、上記の作業を行わなかった場合、実行レベル 1 に移行することによってこのサービスは中断されます。このサービスはバックアップに必要です。「障害復旧 : 抹消リンクの移動 (HP-UX 11.x)」(A-26 ページ) を参照してください。
2. システムで rpcd を構成します (ファイル /etc/rc.config.d/dce で変数 RPCD=1 を構成します)。

   これにより、システムが最小限の動作状態で実行する準備ができました。この状態の特徴を以下に示します。

   — init-1 の実行レベル (ファイルシステム : マウント済み、ホスト名 : 設定済み、日付および時刻 : 設定済み、syncer: 実行中)

   — ネットワークが稼動している必要があります。

   — 以下のプロセスも実行されます。inetd、rpcd、swagentd

Solaris の例

1. rpc 抹消リンクを /etc/rc1.d から /etc/rc0.d へ移動して、ブート・セクションに対する変更内容を補足します。抹消リンクには基本サービスが含まれており、上記の作業を行わなかった場合、実行レベル 1 に移行することによってこのサービスは中断されます。このサービスはバックアップに必要です。
2. rpcbind が、システム上で構成されていることを確認します。

   これにより、システムが最小限の動作状態で実行する準備ができました。この状態の特徴を以下に示します。

   — Init 1

   — ネットワークが稼動している必要があります。

   — 以下のプロセスも実行されます。inetd、rpcbind

Tru64

1. システムの電源がオフになっている場合は、システムを起動して System Reference Manual（SRM）コンソール（ファームウェア・コンソール）に入ります。

2. SRM コンソールから以下のコマンドを実行して、シングル・ユーザー・モードに入ります。

   — `boot -fl s` で、生成済みの vmunix ファイルを使用して起動します。

   — `boot -fi genvmunix -fl s` で、一般的なカーネルを使用するシングル・ユーザー・モードに入ります。

3. システムがすでに稼動中であれば、以下のコマンドを実行して、現在の実行レベルからシングル・ユーザー・モードに変更します。
   `init s`

AIX

— 操作は必要ありません。補助ディスクの作成に使用する `alt_disk_install` コマンドにより、システムの動作状態を最小限にしなくてもディスク・イメージの整合性が保証されるためです。

補助ディスクの作成

- 補助ディスクを使用して障害復旧を行う場合は、補助ブート・ディスクを準備する必要があります。1 つのサイトとプラットフォームにつき、ブート可能な補助ディスクが 1 台だけ必要です。このディスクには、オペレーティング・システムとネットワーク構成が含まれており、ブート可能であることが必要です。

バックアップ仕様の作成

- 以下を実行する実行前スクリプトを作成します。

  — 環境に関して必要なすべての情報を収集して、収集した情報を障害復旧時に使用可能な場所に保存するスクリプト。このスクリプトは、容易にアクセスできる別のシステムに保存することをお勧めします。収集する情報を以下に示します。

  - 保管場所の物理的および論理的保存構造
  - 現在の論理ボリュームの構造 (HP-UX の場合、`vgcfgbackup` と `vgdisplay -v` を使用)
  - MC/ServiceGuard の構成データ、ディスク・ミラーリング、ストライピング
  - ファイルシステムとマウント・ポイントの概要 (HP-UX の場合、`bdf`、または `/etc/fstab` のコピーを使用)
  - システムのページングスペース情報 （HP-UX の場合、`swapinfo` コマンドの出力を使用）

- I/O構造の概要(HP-UXの場合、`ioscan -fun`と`ioscan -fkn`を使用)
- クライアントのネットワーク設定

— データの非常用コピーもバックアップに保存できます。ただし、これを実行した場合は、実際の復旧を行う前にこの情報を取り出しておく必要があります。

— システムからすべてのユーザーをログアウトさせます。

— アプリケーション・データを個別にバックアップする場合でない限り、データベースのオンライン・バックアップなどを使ってすべてのアプリケーションを停止します。

— システムへのネットワーク・アクセスを制限します。これにより、バックアップの実行中はシステムへのログオンが禁止されます (HP-UX の場合、`inetd.sec` を上書きして、`inetd -c` を使用する)。

— 必要に応じて、システムの動作状態を最小限にします (`sbin/init 1`; wait 60; 実行レベルが 1 になっているかどうかをチェックします)。これは修正 "init 1" 状態です。

- システムの実行レベルを標準にする実行後スクリプトを実行して、アプリケーションの再起動などを行います。
- Data Protector Cell Manager 上のクライアントに対するバックアップ仕様を設定します。バックアップ仕様には、すべてのディスクを指定し (ディスク・ディスカバリを使用)、実行前 / 実行後スクリプトを指定することが必要です。

手順のテスト

- バックアップ手順を実行します。この手順は、定期的に繰り返し実行するか、または少なくともシステム構成に主要な変更があった場合、特に論理ボリューム構造に何らかの変更があった場合 (HP-UX では、LVM) に実行します。

復旧

本項では、バックアップ実行時の状態にシステムを復元する方法を説明します。ディスク・デリバリーによる障害復旧を正しく実行するには、以下が必要です。

- クラッシュしたディスクと交換する新しいハードディスク

- 適切なオペレーティング・システムと Data Protector エージェントを含む補助ディスク
- 復旧対象のクライアントの正常なフル・バックアップ

以下のステップを実行します。

1. 問題のあるディスクを新しいディスク (同等サイズ) と交換します。
2. 補助ディスク (適切なオペレーティング・システムと Data Protector クライアントが含まれているディスク) をシステムに接続して、これをブート・デバイスにします。
3. 補助オペレーティング・システムからブートします。
4. 必要に応じて、論理ボリューム構造を再構築します (HP-UX の場合は、LVM)。ルート以外のボリューム・グループについては、保存されているデータを使用します (HP-UX の場合は、`vgcfgrestore` または SAM を使用)。
5. さらに、復元対象のルート・ボリューム・グループを修復済みディスク上に作成します (HP-UX の場合は、`vgimport` を使用)。このボリューム・グループは、復元プロセス中はルート・ボリューム・グループとはみなされません。これは、補助ディスクから OS を実行しているためです。`vgimport` の詳細は、同コマンドの man ページを参照してください。
6. 新しいディスクをブート可能にします。
7. バックアップ時に二次記憶デバイスに保存したデータから、他のデータ記憶構造 (ミラー、ストライピング、MC/ServiceGuard など) を再構築します。
8. ファイルシステムを作成して、バックアップからのデータの要求に応じてファイルシステムをマウントします。このとき使用するマウント・ポイント名には元の名前に似た名前を使用して、元の名前はそのまま使用しないでください (例 : `/etc` の代わりに `/etc_restore` を使用)。
9. マウント・ポイントにある復元対象のファイルをすべて削除して、マウント・ポイントを空の状態にします。
10. Data Protector GUI を起動して、Cell Manager との接続を開始します。補助ディスクを使って、システムをセルにインポートします。

11. 復元するバージョンを選択します。まず復元に必要なメディアをすべてリストして、それらが使用可能であることを確認します。[Restore As <*新しいマウント・ポイント名*>] オプションを使って、(今後) システムに対してルート・ボリュームとなるボリュームを含む必要なマウント・ポイントをすべて復元します。バックアップのルート・ボリュームは「修復ディスク」上のルート・ボリュームに復元されます。現在補助ディスク上で実行されている補助オペレーティング・システムには何も復元されません。
12. 復元したシステムをシャットダウンします。
13. 補助ディスクをシステムから取り外します。
14. システムを新しい (または修復された) ディスクからリブートします。

注記

補助ディスクの代わりに、新しいディスクを、Disk Agent がインストールされているクライアント・システムに一時的に接続することもできます。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 Cell Manager の手動による障害復旧

手動による障害復旧は、基本的な障害復旧方法です。この方法には、最初にインストールした時と同様の方法でシステムを再インストールして復旧する他に、Data Protector を使ってオペレーティング・システムを含むすべてのファイルを復元する方法があります。

制限事項

サポート対象のオペレーティング・システムは、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

ここでは、クラスター環境の復旧については説明しません。クラスター環境の構成によっては、特別な手順や環境の変更が必要です。

準備

HP-UX または Solaris クライアントの手動による障害復旧に対する準備と同じ手順を行います (ただし補助ディスクに関する手順を除く)。詳しくは、「準備」(626 ページ) を参照してください。上記の手順とは別に、以下の手順も実行することが必要です。

1. IDB の通常バックアップを行います。このとき、別のバックアップ仕様を使って、Cell Manager 自体のバックアップ完了後にバックアップが実行されるようスケジュール設定することをお勧めします。
2. Cell Manager システム上の指定したデバイスに IDB と構成のバックアップを行います。これにより、管理者はそのデバイス内のメディアに IDB の最新バージョンが含まれていることが分かります。

復旧

以下の手順に従って、UNIX Cell Manager を復元します。

必要条件

ディスク・デリバリーによる障害復旧を正しく実行するには、以下が必要です。

- Cell Manager と IDB のルート・パーティションの最新の有効なバックアップが含まれているメディア

- Cell Manager システムに接続されたデバイス

手順

以下の手順に従って、Cell Manager の復旧を実行します。

1. クラッシュしたディスクを交換します。
2. お使いのオペレーティング・システムのインストール用メディアからシステムをブートします。
3. オペーティング・システムを再インストールします。インストール方法については、お使いのシステムの管理者用マニュアルを参照してください。インストール時に、復旧準備手順 (実行前スクリプト) で収集したデータを使って、保管場所の物理的および論理的保存構造、論理ボリューム構造、ファイルシステムとマウント・ポイント、ネットワーク設定などを再作成して構成します。
4. Cell Manager に Data Protector を再インストールします。
5. データベースの最新バックアップと `/etc/opt/omni` を一時ディレクトリに復元します。これにより、メディアから他のすべてのファイルを容易に復元できます。ただし、データベースは直接復元できないことに注意してください。復元方法については、第 6 章「データの復元」を参照してください。`/opt/omni/sbin/omnisv -stop` コマンドを使用してすべての Data Protector プロセスを終了します。これにより、使用中のファイルがない状態になります。
6. `/etc/opt/omni/` ディレクトリを削除して、一時ディレクトリの `/etc/opt/omni` と置き換えます。これにより、前回の構成が再び作成されます。
7. `/opt/omni/sbin/omnisv -start` コマンドを使って Data Protector プロセスを起動します。
8. Data Protector ユーザー・インタフェースを起動して、すべてのファイルをバックアップから復元します。
9. システムをリブートします。

以上で、Cell Manager が正しく復旧されます。

Windows 上での障害復旧のトラブルシューティング

本項では、Windows システム上での障害復旧実行時に問題が発生した場合に必要な手順を説明します。

一般的なトラブルシューティング

Autodr.log

Autodr.log は *<Data_Protector_home>*¥tmp ディレクトリにあるログ・ファイルで、自動障害復旧（EADR、OBDR、ASR）に関するメッセージが含まれています。エラーが発生した場合は、このファイルを点検してください。Autodr.log には多くのメッセージが記録されていますが、その大半は開発およびサポート用のもので、エラーの発生を示すものは一部だけです。そうしたエラー・メッセージは通常、トレースバックとともにログ・ファイルの最後に記録されています。

autodr.log に記録されるメッセージには 4 つのタイプ / レベルがあります（これらのタイプ / レベルは、Data Protector GUI のバックアップ・セッションの最後に報告されるメッセージの報告レベルとは対応していないことに注意してください）。

- 致命的エラー : 深刻なエラーで、オブジェクトのバックアップは続行不可能であり、中止されます。
- エラー : 致命的である可能性もありますが、いくつかの要因に依存します。

  たとえば、autodr.log に、あるドライバが障害復旧オペレーティング・システムに含まれていないことが記録されていたとします。そのドライバがないことで、復旧後のシステムが動作しない場合もありますが、OS のブート後に重要でないサービスが実行されないだけの場合もあります。これは、どのドライバがバックアップされていなかったかに依存します。
- 警告および情報 : これらはエラー・メッセージではなく、通常は何らかの障害を意味するものではありません。

autodr.log ファイルに記録される最も一般的なメッセージには、次のようなものがあります。

- `filename 'not a pe file'`: このメッセージは、あるファイルがポータブルな実行ファイルでないことを意味します。この警告は何らかの障害を示すものではありません。
- `unsupported location`: Data Protector は、障害復旧オペレーティング・システム（DR OS）に含まれる予定のサービスやドライバに必要なファイルが、*%SystemRoot%* ディレクトリにないことを通知します。

  こうしたドライバは多くの場合、アンチウィルス・ソフトウェアやリモート・コントロール・ソフトウェア（pcAnywhere など）で使用されます。必要なファイルが不足しているサービスやドライバがブート後に動作しない可能性があるため、このメッセージは重要です。障害復旧が正常終了するか失敗するかは、影響を受けるサービスやドライバに左右されます。この問題に対して考えられる解決方法は、不足しているファイルを *%SystemRoot%* ディレクトリにコピーし、Windows レジストリ内のそのパスを変更することです。Windows レジストリを不正に編集すると、システムが深刻なダメージを受ける可能性があることに注意してください。

障害復旧後のシステムへのログオン時の問題

問題

システム復旧後、以下のエラー・メッセージが表示される場合があります。

“`The system cannot log you on to this domain, because the system's computer account in its primary domain is missing or the password on that account is incorrect.`”（このドメインにログオンできません。プライマリ・ドメイン内にシステム・コンピュータのアカウントがないか、このアカウントに対するパスワードが不適切なためです。

この種類のメッセージは、通常以下のいずれかの理由により表示されます。

- 障害復旧プロセス (フル・バックアップを含む) を正常に実行するためのすべての情報を収集した後、Windows を再インストールして、要求を満たしていないドメインにシステムを (再度) 追加した。
- 障害復旧プロセス (フル・バックアップを含む) を正常に実行するためのすべての情報を収集した後、要求を満たしていないドメインからシステムを削除して、同じドメインまたはその他のドメインにシステムを (再度) 追加した。

解決方法

このような場合、Windows は、障害復旧時に復元される情報とは互換性のない新しいシステム保護情報を生成します。この場合の解決方法を以下に示します。

1. 管理者アカウントを使って、ローカルでシステムにログオンします。
2. [コントロール パネル] ウィンドウで [ネットワーク] をクリックし、[識別] タブを使って、このシステムを現在のドメインから一時的なワークグループ (TEMP など) へ移します。この後、システムを削除したドメインにこのシステムを再度追加します。この作業には、ドメイン管理者用パスワードが必要です。
3. コンピュータを再び適切なドメインに入れた後、[ネットワーク] ウィンドウで [OK] をクリックします。この時点で Windows システムの再起動が必要となります。
4. 障害復旧プロセスを使ってこの新しい状態を更新するには、もう一度必要な手順 (システム・データの収集、バックアップ) をすべて実行することが必要です。詳しくは、「障害復旧の準備」の項を参照してください。

コピーからの障害復旧

問題

メディア・コピーまたはオブジェクト・コピーから障害復旧を実行することはできません。

Data Protector はデフォルトで、オリジナル・メディア・セットを使用して障害復旧を行います。したがって、Data Protector GUI にはコピー・オブジェクトのバージョンは表示されません。

解決方法

オリジナル・メディア・セットが使用できないまたは損傷した場合に、メディア・コピーまたはオブジェクト・コピーから障害復旧を実行するには、以下の手順を実行します。

- オブジェクト・コピー : オリジナル・メディア・セット内のすべてのメディアを IDB からエクスポートした後、SRD ファイルを再生成します。その後、Data Protector の障害復旧ウィザードでは、最初に使用可能なオリジナル・メディア・セットのコピーが表示されます。

  詳しくは、「Data Protector からのメディアのエクスポート」(182 ページ) と「システム復旧データ (SRD) の更新と編集」(553 ページ) を参照してください。

- メディア・コピー：SRD ファイル内のオリジナル・メディアのメディア ID をメディア・コピーのメディア ID に書き換えます。その後、Data Protector の障害復旧ウィザードでは、最初に使用可能なオリジナル・メディア・セットのコピーが表示されます。

  詳細は、「システム復旧データ (SRD) の更新と編集」（553 ページ) を参照してください。

半自動障害復旧のトラブルシューティング

問題

drstart が “Can not Copy <filename>” というエラーを出力した場合

このエラーは、drstart ユーティリティが指定されたファイルをコピーできなかった場合に出力されます。1 つの原因として、ファイルがシステムによってロックされていたことが考えられます。たとえば、drstart が omniinet.exe をコピーできない場合は、おそらく Inet サービスがすでに実行中であると思われます。これは通常では考えられない状況で、クリーン・インストールの後では起きないはずです。

解決方法

残りのファイルのコピーを続けるか確認するダイアログ・ボックスが表示されます。[はい] をクリックすると、drstart はロックされたファイルをスキップして他のファイルのコピーを続行します。ファイルがシステムによりロックされている場合には、障害復旧に必要なプロセスがすでに実行中でありそのファイルはコピーする必要がないため、これで問題は解決されます。

[中止] ボタンをクリックして drstart ユーティリティをクローズすることもできます。

ディスク・デリバリーによる障害復旧のトラブルシューティング

問題

「ディスクのデリバリー用に選択されたドライブの物理的位置が見つかりません !」

ディスク・デリバリーによる障害復旧を行う場合、以下のエラーが表示される可能性があります。「ディスクのデリバリー用に選択されたドライブの物理的位置が見つかりません !」。オブジェクトを復元するには、新しい

ディスク上にパーティションを作成する際、これまでに使用されていないドライブ文字を選択しておく方法もあります。さらにすぐれた解決策を以下に示します。

解決方法

障害復旧プロセスは、オブジェクトの復元前にディスク情報をチェックします。内部関数は、ディスク・アドミニストレータによって作成されたレジストリ値 Information を読み取ります。ディスク・アドミニストレータを何度か起動すると、Information は破損し (更新中にフォーマットが変更されるため)、このような場合、解析プログラムは正常に動作しません。このとき、HKEY_LOCAL_MACHINE¥SYSTEM¥DISK Information キーを削除してディスク・アドミニストレータを再起動すると、この関数は正常に動作します。

問題

「No Operating System Found」

解決方法

障害復旧実行後、Windows システムのブート時に、"No Operating System Found" というメッセージが表示され、システムが正常に起動しない場合は、パーティション情報が格納されているファイル boot.ini にパーティション情報があるかどうかを確認してください。詳しくは、「復旧」(570 ページ) の項のステップ 4 を参照してください。

問題

Media Agent クライアントのディスク・デリバリーによる障害復旧

ディスク・デリバリーによる障害復旧を実行する場合、Data Protector はまず、バックアップ・デバイスが接続されていた元のクライアント (Media Agnet クライアント) に接続し、同じデバイスを使って復元を実行しようとします。ただし、バックアップを実行した Media Agent クライアントがクラッシュし、そのクライアントに対してディスク・デリバリーによる障害復旧を実行した場合、Data Protector はこのクライアントに接続できず、オフラインによる復元を実行して、復元用のローカル・デバイスを検索します。ローカル・デバイスが接続されていない場合は、その旨と障害復旧の中止を通知するメッセージが表示されます。

解決方法

これを回避する方法には以下の 2 通りがあります。

- メディアを別のメディア・プールへ移動します。これにより、メディアを新しいデバイスに割り当てることができます。その後、ディスク・デリバリーによる障害復旧を続行します。

- 2 番目の方法では、障害発生前の準備段階の作業が必要です。セル内に Media Agent クライアントが 2 つある場合、障害発生前に第一の Media Agent クライアントを第二の Media Agent クライアント (およびその逆) にバックアップして、Media Agent クライアントのディスク・デリバリーによる障害復旧実行時の問題を回避することができます。

拡張自動障害復旧およびワンボタン障害復旧のトラブルシューティング

問題

「自動障害復旧情報が収集できない」

EADE または OBDR を実行中に、次のエラーが出力される場合があります。「致命的でないエラーが自動障害復旧データの収集中に検出されました。自動障害復旧ログを確認してください。」

解決方法

- すべての記憶装置が正しく構成されているか確認します。デバイス・マネージャがデバイスを不明なデバイスと表示している場合は、EADR または OBDR を実行する前に、正しいデバイス・ドライバをインストールする必要があります。システムに接続されている記憶装置が正しく構成されていない場合には、`autodr.log` (場所は *<Data_Protector_home>*¥tmp) に次と同様のエントリが記録されます。

  ```
  DRIM_WIN_ERROR 13 SetupDiGetDeviceRegistryProperty
  ```

- 使用可能なレジストリ・スペースが十分にある必要があります。レジストリの最大サイズを、少なくとも現在のレジストリ・サイズの 2 倍に設定することをお勧めします。使用可能なレジストリ・スペースが十分にない場合、`autodr.log` に次と同様のエントリが記録されます。

  ```
  ERROR registry  'Exception while saving registry'
  ...
  WindowsError: [Errno 1450] Insufficient system resources
  exist to complete the requested service.
  ```

この問題が継続する場合は、Data Protector 自動障害復旧モジュールをアンインストールして (手動およびディスク・デリバリーによる障害復旧は可能)、当社サポート担当に連絡してください。

問題

「致命的ではないエラーが検出された」

EADE または OBDR を実行中に、次のエラーが出力される場合があります。「致命的でないエラーが自動障害復旧データの収集中に検出されました。自動障害復旧ログを確認してください。」

自動障害復旧モジュール実行中に致命的でないエラーが検出された場合は、そのバックアップがまだ障害復旧に使用できる可能性が高いことを示します。致命的でないエラーの原因は `autodr.log` に記録されています (ディレクトリは *<Data_Protector_home>*¥tmp)。

解決方法

- `<%SystemRoot%>` フォルダにないサービスやドライバ (ウィルス・スキャナなど) が検出された。`Autodr.log` には、次と同様のエラー・メッセージが記録されます。

  ```
  ERROR safeboot  'unsupported location' 'intercheck support 06' 2
  u'¥¥??¥¥D:¥¥Program Files¥¥Sophos SWEEP for NT¥¥icntst06.sys'.
  ```

  このエラー・メッセージが表示されても、障害復旧の正常動作には影響しないため、無視して構いません。

問題

復旧中にブランク画面が表示された

Windows がセーフモードで起動された場合、一部のシステム構成ではビデオ・ディスプレイが正常動作しない場合があります。このエラーは Data Protector には無関係であり、Windows だけがインストールされている場合でも発生します。

解決方法

障害復旧中に画面がブランクになっても復旧が失敗したわけではありません。障害復旧の進行状況は Cell Manager 上でモニターできます。または別のクライアントから `ping` と `telnet 5555` コマンド (または他の適切なコマンド) を使ってターゲット・システムが応答するかを確認できます。他に復旧が処理中かどうかを示すものには、デバイスが動作中か、あるいはハード・ディスクのランプが点滅しているか、などがあります。

ターゲット・システムが `ping` と `telnet 5555` コマンドに応答しても、ハード・ディスクのランプが点滅しておらずデバイスが動作していない場合は、自動ログオンに失敗した可能性があります。Enter キーを押して、パスワードがない管理者用アカウントでログオンしてください。

システムの復旧が終われば、画面はバックアップ時と同じように表示されるようになります。

問題 **復旧中にネットワークが使用できなくなった**

解決方法 スイッチ、ケーブルなどに問題がないか確認します。他に考えられるのは DNS サーバ (バックアップ時の構成と同じ) が復元時にオフラインになっていることです。DR OS の構成はバックアップ時と同じであるため、ネットワークが使用できません。この場合はオフライン復元を行い、復旧後に DNS の設定を変更します。またフェーズ 2 の開始前にレジストリ (HKey_Local_Machine¥SYSTEM¥CurrentControlSet¥Services¥Tcpip¥Parameters) を変更することもできます。この場合は変更を有効にするために、フェーズ 2 実行前に再起動が必要です。フェーズ 2 完了後、フェーズ 3 を開始する前に設定を修正します。

注意 レジストリを誤って編集すると、障害復旧が正常動作しなくなる場合があります。

問題 **自動ログオンが正常動作しない**

解決方法 自動ログオンが正常動作せず、パスワードがない管理者用アカウントを使って手動でログオンしなくてはならない場合があります。

問題 **EADR 中にコンピュータがフリーズした**

解決方法 CD が読み込み可能か確認します。CD-RW を何回も再使用してはいけません。

問題 **MSCS の EADR 用 CD ISO イメージを作成できない**

解決方法 CD ISO イメージを作成できるようにするためには、クォーラム ディスクのバックアップを行う必要があります。

13 Data Protector 環境のカスタマイズ

本章の概略

本章では、ユーザーの要求に適合するよう Data Protector をカスタマイズする方法を説明します。本章は以下の項で構成されています。

重要

Data Protector の制限事項や推奨事項に関する特定の情報については、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。Data Protector セルに対するセキュリティの設定方法の詳細については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

グローバル・オプション・ファイル

グローバル・オプションは Data Protector セル全体に影響を及ぼし、タイムアウトや各種制限など Data Protector のさまざまな特性を設定するオプションです。グローバル・オプションはすべてグローバル・オプション・ファイルに記述されており、このファイルを編集して Data Protector をカスタマイズできます。ファイルは以下のディレクトリにあります。
`/etc/opt/omni/server/options` (UNIX Cell Manager の場合)、
`<Data_Protector_home>``¥Config¥server¥options` (Windows Cell Manager の場合)。ファイル名は、`global` です。

グローバル・オプションの使用方法

各オプションにシャープ記号 (#) を付けてコメントにし、この記号に続けてオプションの内容を記述することができます。本書に記述されていないオプションについては、このファイルを参照します。

グローバル・オプションを使用するには、目的のオプション名がある行のコメントを解除して、適切な値を設定します。コメントを解除するには、単にシャープ記号 (#) を削除します。

注記

大部分のユーザーは、Data Protector を操作する際にグローバル・オプションを変更する必要はありません。

最も頻繁に使用される変数

最も頻繁に使用されるグローバル変数を以下に示します。各オプションの詳細については、グローバル・オプション・ファイルを参照してください。

- `MediaView`: [メディア] コンテキストに表示されるフィールドとその順番を変更します。
- `MaxBSessions`: 同時処理バックアップ数のデフォルトの上限値 5 を変更します。
- `InitOnLoosePolicy`: メディア・ポリシーが `[Loose]` の場合に Data Protector が空のテープまたは認識されないテープを自動的に初期化するようにします。

- MaxMAperSM: バックアップ・セッションごとのデバイス同時処理数のデフォルト上限値を増加させます (デバイス同時処理数の上限は 32)。
- DCDirAllocation: 新しい詳細カタログのバイナリ・ファイルの格納先となる dcbf ディレクトリを選択する際に使用するアルゴリズムを決定します。使用可能なアルゴリズムには 3 種類 (fill in sequence (デフォルト)、balance size、balance number) あります。
- DailyMaintenanceTime: 日常保守作業を開始する時刻を 24 時間表記で指定します。デフォルトでは、12:00(正午) に設定されています。日常保守作業のリストは、「Data Protector のチェック / 保守機構」(757 ページ) を参照してください。
- DailyCheckTime: 日常チェックを開始する時刻を24時間表記で指定します。デフォルトでは、午後 12:30 に設定されています。日常チェックを実行しない場合は、無効にすることもできます。日常チェック作業のリストは、「Data Protector のチェック / 保守機構」(757 ページ) を参照してください。

omnirc オプションの使用

omnirc オプションは、トラブルシューティングを行ったり、他の設定値を無効にする際に非常に役立ち、Data Protector クライアントの動作のみに適用されます。動作環境によって要求されない限り、上級ユーザーでもこの変数を使用してはいけません。Disk Agent や Media Agent はこれらのオプションの値を使用します。

これらのオプションは以下のディレクトリにあります。

位置

- /opt/omni/.omnirc (HP-UX および Solaris プラットフォームの場合)
- usr/omni/.omnirc (上記以外の UNIX クライアント)
- *<Data_Protector_home>*¥omnirc (Windows クライアント)
- sys:¥usr¥omni¥omnirc (Novell NetWare クライアント)

omnirc オプションの使用方法

Data Protector をインストールすると、omnirc ファイル用のテンプレートが提供されます (ファイル名はプラットフォームによって異なりますが、.omnirc.TMPL または omnirc.TMPL のどちらかになります)。このファイルはアクティブな状態にはなっていません。アクティブな omnirc ファイルを作成するには、テンプレート・ファイルを omnirc (または .omnirc) にコピーして編集します。オプションを使用するには、このオプション名がある行のコメントを解除 (シャープ記号 (#) を削除) して、必要に応じて値を編集します。

- (ファイルをコピーするかエディタを使用して) omnirc ファイルを作成する際に、omnirc ファイルの権限を確認してください。UNIX の場合、権限はユーザーの umask の設定値に応じて自動的に設定されるため、一部のプロセスでファイルを読み取れない設定になる場合があります。

  権限を手動で 644 に設定します。

- omnirc ファイルを変更した場合は、omnirc ファイルを変更した Data Protector クライアント上の Data Protector サービス / デーモンを再起動する必要があります。UNIX の crs デーモンは必ず再起動してください。また、Windows の Data Protector CRS サービスと Inet サービスを再起動することをお勧めします。特に Windows については、エントリを追加または変更した場合や、エントリを削除 (またはファイル名を変更) しただけの場合、再起動は必要ありません。

最も頻繁に使用される変数

最も頻繁に使用される omnirc 変数を以下に示します。

- **OB2BLKPADDING_n:** 初期化の際にメディアに書き込まれる空のブロック数を指定します。
- **OB2DEVSLEEP:** デバイスのロード中、再試行後次の再試行が行われるまでのスリープ時間を変更します。
- **OB2ENCODE:** バックアップ仕様でバックアップ・オプションがどのように設定されているかに関係なく、ユーザーが常にデータのコード化をオンにできるようにします。
- **OB2OEXECOFF:** 特定のクライアントに対するバックアップ仕様で定義されている任意のオブジェクトの実行前 / 実行後スクリプトを禁止または使用不可能に設定できます。
- **OB2INCRDIFFTIME** と **OB2CHECKCHANGETIME:**

  OB2CHECKCHANGETIME と **OB2INCRDIFFTIME** 変数は、UNIX クライアントに対してのみ有効です。増分バックアップ中、Disk Agent は最後のバックアップ以後どのファイルが変更されたかを判別するため、各ファイルの「前回変更日時」属性と「前回 i ノード変更日時」属性を調べます。しかし、「前回変更日時」属性は［アクセス時刻属性を保存しない］バックアップ・オプションが有効で、［バックアップ時にファイルをロック］バックアップ・オプションが無効の場合にのみ評価されます。この変数により、増分バックアップでいつ「前回 i ノード変更日時」を使用するかについてより細かな制御が行えます。

  OB2INCRDIFFTIME 変数は、増分バックアップに対する「前回 i ノード変更日時」をチェックした後に強制される「増分待ち」期間 (単位 : 分) を指定します。Session Manager から受信する参照時刻 (前回のバックアップ時刻) に指定した期間が加算され、それを「前回 i ノード変更日時」と比較することで、バックアップを行う時刻に到達したかが判断されます。この変数は、**OB2CHECKCHANGETIME** 変数が 2 に設定されている場合のみ有効です。
- **OB2RECONNECT_ACK:** Data Protector が Ack メッセージを待つ時間を定義します (デフォルトは 1200 秒)。つまり、`OB2RECONNECT_ACK` で定義された時間 (単位 : 秒) 以内にエージェントが Ack メッセージを受け取らなかった場合は、ソケット接続は無効とみなされます。
- **OB2RECONNECT_RETRY:** 以下のいずれかの間の接続が切断した場合に、Data Protector が再接続を試みるまでの待ち時間を定義します。

— Disk Agent と Media Agent（バックアップ中）

— バックアップ Session Manager と Disk Agent または Media Agent

デフォルトは 600 秒です。バックアップ中に、バックアップ Session Manager と Disk Agen/Media Agent 間、または Disk Agent と Media Agent 間の LAN/WAN 回線が、OB2RECONNECT_RETRY で指定した秒数以上ダウンしてはいけません。

- **OB2REXECOFF:** 特定のクライアントに対する任意のリモート・セッションの実行前 / 実行後スクリプトを使用不可能に設定できます。
- **OB2SHMEM_IPCGLOBAL:** このオプションは、Disk Agent と Media Agent の両方がインストールされている HP-UX 11.X クライアントで、バックアップ中に以下のエラーが発生した場合に備えて 1 に設定しておくことが必要です。

  共有メモリ （%1!s!） の割り当て / 取り付けができません。（IPC は共有メモリ・セグメントを割り当てることができません。

  システム・エラー： [13] 権限が拒否されました。 中止しています。
- **OB2VXDIRECT:** 拡張 VxFS ファイルシステムの直接読み取り (キャッシュなし) と性能の向上を可能にします。
- **OB2PORTRANGE:** Data Protector がリスン・ポートを動的に割り当てる際に使用するポート番号の範囲を限定するオプションです。通常このオプションは、ファイアウォール越しのセル管理を可能にする場合に設定します。ファイアウォールは別途構成する必要があり、このオプションで指定したポート範囲は Inet リスン・ポートに影響を与えないことに注意してください。

例

```
OB2PORTRANGE=40000-40199
```

上記により、ポート範囲が 40000 ～ 40199 に設定されます。

- **OB2PORTRANGESPEC:** すべてのバイナリに対するポート番号の範囲を指定するオプションです。これにより、ポート番号の範囲をより細かく制御でき、範囲を狭くすることができます。ファイアウォールは別途構成する必要があり、このオプションで指定したポート範囲は Inet リスン・ポートに影響を与えないことに注意してください。

  構成例については、「ファイアウォールのサポート」（657 ページ) を参照してください。

Data Protector GUI 用の言語の選択

Data Protector は、複数の言語にローカライズされています。ローカライズされた言語カタログ (Data Protector GUI およびメッセージ) に合わせて国際文字を正しく表示するためには、いくつかの必要条件が満たされている必要があります。

Data Protector GUI 用に選択した言語は、Data Protector GUI 内に示されるセッション・メッセージやファイル名内の国際文字の表示にも影響を及ぼします。

選択可能なローカライズ言語カタログは、Data Protector のインストール時に選択した言語によって異なります。ローカライズされた言語カタログをインストールしていなければ、既存の GUI クライアントに Data Protector の言語カタログを追加インストールすることも可能です。詳しい手順については、オンライン・ヘルプの索引キーワード「Data Protector のコンポーネント、追加」を参照してください。

Data Protector 用にインストールされている言語を調べるには、以下の手順を実行してください。

1. コンテキスト・リストで [クライアント] をクリックします。
2. Scoping ペインで、[クライアント] を展開して、インストールされているクライアントの一覧を表示します。
3. GUI クライアントをクリックし、インストールされているコンポーネントを結果エリアで確認します。

英語版のローカライズ・カタログは必ずインストールされます。これは、Data Protector GUI のデフォルト言語です。

必要条件

以下の必要条件が満たされている必要があります。

- 必要な言語サポートが Data Protector GUI クライアント上にインストールされていること。
- Windows システムの場合は、ローカライズされた Data Protector GUI は、適切にローカライズされた Windows オペレーティング・システム上で実行しなければなりません。たとえば、Data Protector GUI の日本語サポートは、日本語版の Windows 上でしか正しく動作できません。

- UNIX システムの場合は、ファイル名のエンコードに使用するロケール内でデスクトップ環境を開始しなければなりません。たとえば SJIS 環境の場合であれば、SJIS ロケール内でデスクトップを開始します。

上記の必要条件が満たされていると、Data Protector GUI は、オペレーティング・システム上に設定されているロケールに対応した言語で開始されます。たとえば Windows システム上で、Windows コントロール・パネルの [地域と言語のオプション] でフランス語ロケールを設定している場合には、Data Protector GUI の言語として (可能であれば) フランス語の言語カタログが使用されます。

GUI 内でのファイル名エンコードの設定

Data Protector GUI でファイル名やセッション・メッセージの国際文字を正しく表示させるには、特定の設定と構成が必要です。背景となる情報は、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

必要条件

GUI システムで国際文字を正しく表示させるには、以下の必要条件が満たされている必要があります。

- Data Protector A.05.50 にアップグレードする場合には、IDB 内のファイル名が変換されていること。詳細は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』をご覧ください。
- 選択した文字セットに対して適切なロケール（UNIX の場合）とフォントが、Data Protector GUI システムにインストールされていること。たとえば、欧州システム上の Windows GUI で日本語を表示させるには、日本語フォントをインストールします。
- Data Protector GUI がインストールされた UNIX システム上では、GUI を開始する**前に**適切なロケールを設定してください。「UNIX 上の Data Protector GUI での国際文字の適切な表示」（653 ページ) を参照してください。

Windows システムや UNIX システム上の GUI で国際文字を正しく表示するには、ファイルを作成したシステムで使用されていた文字エンコードを選択してください。

制限事項

正しい文字エンコードを選択しても、以下の制限事項が適用されます。

- GUI で正しい文字エンコードを選択しても、一部の文字が正しく表示されない場合があります。その理由は、Windows と UNIX オペレーティング・システムにはコード・ページの実装に細かな違いがあるためです。したがって、クライアントが構成されたときと異なるプラットフォームで Data Protector GUI が実行されている場合には、一部の文字が正しくマッピングされません。ただし、最悪の場合でも正しく表示されないのは数文字だけであり、バックアップや復旧には影響ありません。
- 残念ながら、UNIX 上の Data Protector GUI では、あるロケールの下で作成された GUI 項目の名前（バックアップ・デバイスやバックアップ仕様など）が、異なるロケールでは正しく表示されない場合があります。

GUI 項目の名前が正しく表示されていなくても、その項目を使用することは可能です。たとえば、非 ASCII 文字を使用してバックアップ・デバイスを構成し、名前をつけた場合、ASCII 文字だけを使用するロケールで GUI を実行するとデバイス名は正しく表示されません。しかし、GUI でデバイス名が正しく表示されていなくても、そのデバイスを使用してバックアップや復旧を実行することができます。

UNIX 上の Data Protector GUI での国際文字の適切な表示

UNIX Data Protector GUI システムでは、GUI におけるエンコードの切り替えを可能にし、国際文字を正しく表示させるために、Data Protector GUI を起動する前に（セル構成を考慮して）適切なロケールを設定する必要があります。

ロケールの設定は、システム上でのファイルの表示やエンコードだけでなく、インストールされているどの言語カタログが Data Protector GUI で使用されるかにも影響します。ファイルシステム・ブラウザでバックアップするファイルを選択するときや、IDB ブラウザで復元するファイルを選択するとき、セッション・メッセージ内などで、特定のファイル名関連設定が使用されます。

エンコードについては、通常次のいずれかの方法を選択します。

- UTF-8 ベースのロケールを使用。この場合は、Data Protector GUI を再起動することなしに、ファイル名のエンコードを動的に切り替えられます。
- 任意のロケールを使用。この場合は、選択したロケールを使用してファイル名が正しく表示されます。

ロケールは以下のように設定することをお勧めします。

- セル内のすべてのクライアントのロケール設定が同じである場合は、UNIX 上の Data Protector GUI でも同じロケール設定を使用します。
- 異機種環境（1 つのセル内に、異なるロケール設定を持つ複数のオペレーティング・システムがある場合）における UNIX システム上の Data Protector GUI では、Data Protector GUI を起動する**前に**、UTF-8 エンコードを使用するロケールを設定する必要があります。
- 異機種環境において、Data Protector GUI 内でエンコードが適切に行われない場合は、適切なロケールを設定してから GUI を再起動してください。

システムにインストールされているすべてのロケールをリストするには、次のコマンドを実行します。`locale -a`

ロケールはオペレーティング・システムのインストール中にインストールしますが、オペレーティング・システムのインストールが完了した後でもロケールをインストールできます。詳細な手順は、オペレーティング・システムのマニュアルを参照してください。

ロケールを設定するには、次のコマンドを実行します。

```
export LANG=<locale>
```

ロケールをリストして、UTF-8 エンコードを使用するロケール名をコピー、ペーストすることができます。ロケールの設定が成功したかどうかは、新しい端末を開いて適切な文字が使用できるかを確認します。

例

以下に、UNIX 上で UTF-8 エンコードを使用するロケールを設定し、そのロケールで GUI を実行する例を示します。

```
export LANG=C.utf8
xomni&
```

これにより、UNIX 上の Data Protector GUI で文字エンコードの切り替えができるようになります。

Data Protector GUI でのデフォルト文字コードの変更

Data Protector GUI 内でのデフォルトの文字エンコードは、以下のロケールに合わせて設定されます。

- UNIX システムの場合 : デスクトップ環境が開始されたロケール。
- Windows の場合 : Windows コントロールパネルの [地域と言語のオプション] で設定されたロケール。

(アップグレード後の)IDB 変換が完了すれば、使用されている文字エンコードに関係なくすべてのファイルのバックアップと復元が可能です。ファイル名やセッション・メッセージの国際文字を正しく表示させるには、Data Protector GUI で適切なエンコードを選択する必要があります。Data Protector GUI では、デフォルトで一部の文字コードが使用可能になっていますが、適切なロケール / 文字コードがシステムにインストールされていれば、デフォルト文字コードを他の文字コードで置き換えることもできます。

Windows GUI

Windows GUI でデフォルト文字エンコードを他の文字エンコードに置き換えるには、以下の手順を実行してください。

1. Windows の [コントロール パネル] で、[地域と言語のオプション] をクリックします。
2. [詳細設定] タブをクリックします。［コードページ変換テーブル］で、Data Protector GUI に追加したい文字エンコードをブラウズし、そのコードを覚えます。

   追加したい文字エンコードに対するコードページがインストールされていない場合は、次の手順に進む前にインストールします。
3. Windows のレジストリ・エディタを開き、次のキーをブラウズします。
   `¥HKEY_LOCAL_MACHINE¥SOFTWARE¥Hewlett-Packard¥OpenView¥OmnibackII¥Gui¥Core`
4. デフォルト文字エンコードは、各レジストリ文字列の下に `REG_KEY_CP<number>` という名前でリストされています。置き換えるレジストリ文字列をダブルクリックします。たとえば、Shift-JIS を他の文字エンコードで置き換える場合は、`REG_KEY_CP5` レジストリ文字列をダブルクリックします。
5. 文字エンコードのコードを [値のデータ] フィールドに入力します。このコードは、Windows の［コードページ変換テーブル］内のコードと一致している必要があります（手順 2 参照）。たとえば、Data Protector GUI に ANSI/OEM 韓国文字コードを追加するには、`949` と入力します。
6. 対応する `REG_KEY_NAME_CP<number>` レジストリ文字列をダブルクリックし、[値のデータ] フィールドを編集します。Data Protector GUI のエンコード・リストに表示させたいとおりに、文字エンコードの名前を入力します。

   たとえば、手順 4 で `REG_KEY_CP5` レジストリ文字列を変更した場合は、`REG_KEY_NAME_CP5` レジストリ文字列を変更して文字エンコードの名前を変更します。
7. Data Protector GUI を再起動して変更を有効にします。

UNIX GUI

UNIX GUI でデフォルト文字エンコードを他の文字エンコードに置き換えるには、以下の手順を実行してください。

1. 端末を開き、次のプログラムを実行します。`/opt/omni/bin/xregedit`

2. 次のキーをブラウズします。
   ¥HKEY_LOCAL_MACHINE¥SOFTWARE¥Hewlett-Packard¥OpenView¥OmnibackII¥Gui¥Core

   このキーは、Data Protector GUI でエンコードの切り替えを最初に有効にしたとき（すなわち、UTF-8 エンコードを使用するロケールを設定して Data Protector GUI を起動したとき）に作成されます。

3. デフォルト文字エンコードは、各レジストリ文字列の下に REG_KEY_LC<*number*> という名前でリストされています。置き換えるレジストリ文字列をダブルクリックします。たとえば、Shift-JIS を他の文字エンコードで置き換える場合は、REG_KEY_LC5 レジストリ文字列をダブルクリックします。

4. 文字エンコードのコードを [値のデータ] フィールドに入力します。このコードは、/usr/lib/nls/iconv/config.iconv ファイル内のコードと一致している必要があります。たとえば、Data Protector GUI にアラビア文字エンコードを追加するには、cp864 と入力します。

   システムには適切なロケールがインストールされている必要があります。

5. 対応する REG_KEY_NAME_CP<*number*>レジストリ文字列をダブルクリックし、[値のデータ] フィールドを編集します。Data Protector GUI のエンコード・リストに表示させたいとおりに、文字エンコードの名前を入力します。

   たとえば、手順 4 で REG_KEY_LC5 レジストリ文字列を変更した場合は、REG_KEY_NAME_CP5 レジストリ文字列を変更して文字エンコードの名前を変更します。

6. Data Protector GUI を再起動して変更を有効にします。

ファイアウォールのサポート

本項では、Data Protector プロセスがファイルウォールを越えて通信する環境での Data Protector の構成方法を説明します。

Data Protector の通信

Data Protector プロセスは TCP/IP 接続を使って通信を行います。すべての Data Protector システムは、デフォルトでポート 5555 の接続を受け付けます。さらに、一部のプロセスは動的にポートを割り当て、そのポートへの他の Data Protector プロセスからの接続を受け付けます。

Data Protector プロセスがファイアウォールを越えて通信できるようにするために、Data Protector では動的に割り当てられるポート番号の範囲を限定できます。ポートの範囲はシステムごとに定義されます。特定のシステムで、Data Protector プロセスすべてのポート範囲を定義することもでき、また特定の Data Protector エージェントのポート範囲だけを定義することもできます。

構成の仕組み

ポート割り当ての動作は、2 つの omnirc 変数 (OB2PORTRANGE と OB2PORTRANGESPEC) で構成できます。デフォルトでは両方の変数とも設定されておらず、ポートはオペレーティング・システムによって動的に割り当てられます。

ポート番号の範囲の制限

Data Protector プロセスすべてに適用

omnirc ファイルの OB2PORTRANGE 変数で、あるシステム上の Data Protector プロセスすべてのポート範囲を制限できます。

```
OB2PORTRANGE=<start_port>-<end_port>
```

Data Protector プロセスはこの範囲からポートを選択し、動的に割り当てて使用します。"start_port" から始まるポート範囲内で最初に使用可能なポートから割り当てられます。指定された範囲で使用可能なポートがない場合はポート割り当てが失敗し、要求された操作は実行されません。ポート使用の詳細は表 13-1 (659 ページ) を参照してください。

注記

OB2PORTRANGE 変数は動的割り当てポートに対してのみ適用されます。デフォルトの Data Protector ポート番号 5555 の使用には影響しません。

Data Protector プロセスのポート範囲定義は、Data Protector のポート使用を制限します。他のアプリケーションがこの範囲からポートを割り当てるのを妨げるものではありません。

特定の Data Protector エージェントに適用

多くの場合、すべての Data Protector エージェントがファイアウォールを越えて通信する必要はありません。たとえば、特定の 1 つのエージェントをファイアウォールの外側に、他のすべてのコンポーネントをファイアウォールの内側にインストールできます。このような環境では、特定エージェントのポート範囲だけを制限するのが有効です。これによりポート範囲をより狭くすることができ、ファイアウォールを越えてポートをオープンする必要性が少なくなります。

特定のエージェントが実行されているシステムでポート範囲を制限するには、omnirc ファイルの OB2PORTRANGESPEC 変数を使用します。

```
OB2PORTRANGESPEC=<AGENT>:<start_port>-<end_port>;...
```

すべてのエージェントはポート範囲が制限されていないか OB2PORTRANGESPEC をチェックします。エージェントに対する範囲が定義されていれば、動的割り当てポートはすべてこの範囲から選択されます。"start_port" から始まるポート範囲内で最初に使用可能なポートから使用されます。指定された範囲で使用可能なポートがない場合はポート割り当てが失敗し、要求された操作は実行されません。必要なポート範囲の計算方法は、「ファイアウォール環境での Data Protector 構成例」（664 ページ) を参照してください。

下表に、OB2PORTRANGESPEC 変数で使用できる Data Protector エージェント識別子を示します。動的割り当てリスン・ポートを使用していないエージェント・プロセスはこの表にないことに注意してください。

表 13-1 エージェント識別子

Data Protector コンポーネント	エージェント識別子	説明	ポート使用
Cell Manager	BSM	バックアップ・セッション・マネージャ	同時実行中の BSM ごとに 1 ポート
	RSM	復元セッション・マネージャ	同時実行中の RSM ごとに 1 ポート
	DBSM	データベース・セッション・マネージャ	同時実行中の DBSM ごとに 1 ポート
	xSM	ワイルドカードに一致するすべてのセッション・マネージャ	1[a] 同時実行中のセッション・マネージャごとに +1 ポート
	MMD	メディア管理デーモン	1 ポート
	CRS	セル要求サーバ・サービス	1 ポート
Media Agent	BMA-NET	バックアップ Media Agent[b]	同時実行中の Media Agent ごとに 1 ポート
	RMA-NET	復元 Media Agent[b]	同時実行中の Media Agent ごとに 1 ポート
	xMA-NET	ワイルドカードに一致するすべての Media Agent[b]	同時実行中の Media Agent ごとに 1 ポート

a. この追加ポートは、データベース操作時 (ファイル名削除やデータベースのアップグレードなど) に必要となります。

b. BMA と RMA は、メイン・プロセスと NetIO プロセスという 2 つのプロセスをフォークします。リスン・ポートは BMA-NET / RMA-NET プロセスにより割り当てられます。

注記

OB2PORTRANGESPEC 変数は動的割り当てポートに対してのみ適用されます。デフォルトの Data Protector ポート番号 5555 の使用には影響しません。

特定の Data Protector エージェントのポート範囲定義は、そのエージェントのポート使用を制限します。他のプロセス (アプリケーションや Data Protector エージェント) がこの範囲からポートを割り当てるのを妨げるものではありません。

2 つの変数の同時使用

OB2PORTRANGESPEC と OB2PORTRANGE を同時に設定した場合、OB2PORTRANGESPEC が OB2PORTRANGE の設定を上書きします。

以下に例を示します。

```
OB2PORTRANGESPEC=BMA-NET:18000-18009
```

```
OB2PORTRANGE=22000-22499
```

上記の設定では、Media Agent が使用するポート番号は 18000 ～ 18009 に制限され、他のすべての Data Protector プロセスは 22000 ～ 22499 の範囲のポート番号を使用することになります。

両方の変数を使用することで、特定のエージェントが専用のポート範囲だけを使用するように設定すると共に (OB2PORTRANGESPEC)、他の Data Protector プロセスがこの範囲のポート番号を使用するのを禁止できます。

Data Protector におけるポートの使用法

以下の項では、それぞれの Data Protector コンポーネントに必要なポートについて記述した 2 つの表を示します。表 13-2 は、それぞれの Data Protector コンポーネントを分類し、他のコンポーネントからの接続先となるコンポーネントを示しています。これがファイアウォール規則の送信先仕様を定義します。表 13-3 は同じコンポーネントのリストですが、他コンポーネントへの接続元となるコンポーネントを示しています。これがファイアウォール規則の送信元ポートを決定します。

以下の表は、すべての Data Protector コンポーネントのリストです。最初の 2 列はプロセス識別子とそのリスン・ポート、最後の 2 列が接続元となれるすべてのプロセスです。

表 13-2

リスンしているコンポーネント		接続するコンポーネント	
プロセス	**ポート**	**プロセス**	**送信元ポート**
Cell Manager			
Inet	5555	Application Agent	適用なし[a]
		GUI/CLI	適用なし[a]
CRS	動的	Application Agent	適用なし[a]
		GUI/CLI	適用なし[a]
MMD	動的	xSM	適用なし[a]
		CLI (CM から)	適用なし[a]
xSM	動的	GUI/CLI	適用なし[a]
		xMA[b]	適用なし[a]
		xDA[b]	適用なし[a]
		Application Agent	適用なし[a]
Disk Agent			
Inet	5555	xSM	適用なし[a]
xDA	接続を受け付けない		
Media Agent			
Inet	5555	xSM	適用なし[a]
xMA	接続を受け付けない		
xMA-NET	動的	xDA	適用なし[a]
		Application Agent	適用なし[a]
アプリケーション・ホスト			
Inet	5555	xSM	適用なし[a]

表 13-2

リスンしているコンポーネント		接続するコンポーネント	
プロセス	ポート	プロセス	送信元ポート
Application Agent	接続を受け付けない		

a. 接続の送信元ポートは常にオペレーティング・システムによって割り当てられ、特定の範囲に限定できません。
b. 再接続機能が有効になっているバックアップ・セッションのみ。Disk Agent と Media Agent は既存の TCP 接続を使用して Cell Manager と通信します。この列の接続は元のセッションが切断された後にだけ確立されます。

ファイアウォールの構成規則を記述する際、最初の列のプロセスが 2 列目で定義されているポートへの 3 列目のプロセスからの新しい TCP 接続 (SYN ビットがセットされている) を受け付けられるようにする必要があります。

さらに、1 列目のプロセスは、3 列目のプロセスへ既存の TCP 接続上で応答 (SYN ビットがセットされていない) を返せることも必要です。

たとえば、Media Agent システム上の `Inet` プロセスは、Cell Manager からの新しい TCP 接続をポート 5555 で受付可能である必要があります。また Media Agent は既存の TCP 接続を使って Cell Manager に応答できることも必要です。Media Agent が TCP 接続をオープンできる必要はありません。

以下の表は、すべての Data Protector コンポーネントのリストです。最初の 2 列は接続元となれるプロセスであり、最後の 2 列はプロセス識別子とそのリスン・ポートです。接続を開始しないプロセスはリストされていません (`Inet` など)。

表 13-3

接続するコンポーネント		リスンしているコンポーネント	
プロセス	ポート	プロセス	ポート
Cell Manager			
xSM	適用なし[a]	xMA[b]	5555
	適用なし[a]	xDA[b]	5555
	適用なし[a]	Application Agent[b]	5555
	適用なし[a]	MMD[c]	動的
ユーザー・インターフェース			
GUI/CLI	適用なし[a]	CM 上の `Inet`	5555
	適用なし[a]	CRS	動的
	適用なし[a]	BSM	動的
	適用なし[a]	RSM	動的
	適用なし[a]	MSM	動的
	適用なし[a]	DBSM	動的
CLI (Cell Manager のみ)	適用なし[a]	MMD	動的
Disk Agent			
xDA	適用なし[a]	xMA-NET	動的
	適用なし[a]	xSM[d]	動的
Media Agent			
xMA	適用なし	xSM[d]	動的
	適用なし[a]	UMA[b, e]	5555
Application Agent			

表 13-3

接続するコンポーネント		リスンしているコンポーネント	
プロセス	ポート	プロセス	ポート
Application Agent	適用なし [a]	CM 上の Inet	5555
	適用なし [a]	CRS	動的
	適用なし [a]	RSM	動的
	適用なし [a]	BSM	動的
	適用なし [a]	xMA-NET	動的

a. 接続の送信元ポートは常にオペレーティング・システムによって割り当てられ、特定の範囲に限定できません。
b. より正確には、ポート 5555 への接続を受け付けるのは Inet プロセスであり、その後、要求されたエージェント・プロセスが起動されます。このエージェント・プロセスが接続を継承します。
c. Manager-of-Managers (MoM) 環境において、CMMDB が実行中のシステム上の MMD に対してのみ適用されます。
d. 再接続機能が有効になっているバックアップ・セッションのみ。
e. Utility Media Agent (UMA) への接続は、複数のシステム間で 1 つのライブラリを共有するときのみ必要となります。

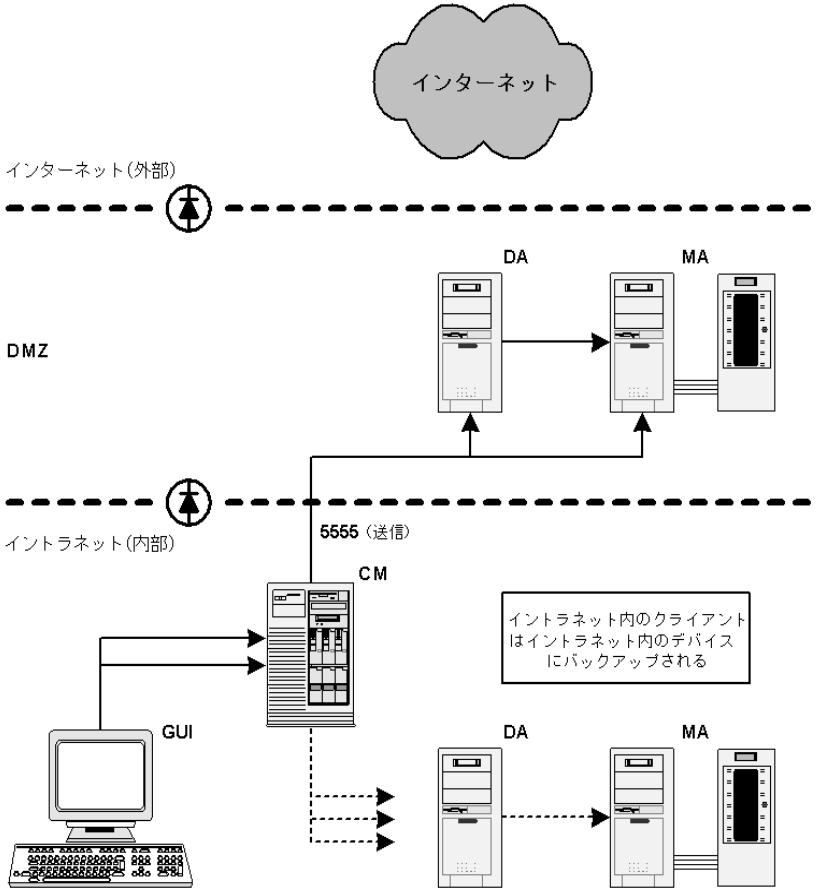
ファイアウォール環境での Data Protector 構成例

以下の項では、4 つの異なるファイアウォール環境での Data Protector の構成例を示します。

例 1: Disk Agent と Media Agent がファイアウォールの外側にインストールされおり、他のコンポーネントはファイアウォールの内側にインストールされている場合。

Cell Manager と GUI をイントラネット内に配置して、Disk Agent と Media Agent を非武装地帯 (DMZ) 内に配置するバックアップ環境を構成します。

図 13-1　　構成図



以下の 2 つの事項が、この構成のポート範囲の設定を決定します。

1. ファイアウォールを越えて通信する必要があるプロセスを特定するため、表 13-2 の Disk Agent と Media Agent を参照します。すると Disk Agent と Media Agent は、Session Manager からのポート 5555 への接続を受け付ける必要があることがわかります。したがってファイアウォールの規則は以下のようになります。
   - CM システムから DA システムのポート 5555 への接続を許可する。
   - CM システムから MA システムのポート 5555 への接続を許可する。

またこの表は、Media Agent が Disk Agent からの接続を受け付ける必要があることも示しています。しかしこの 2 つのエージェント間の通信はファイアウォール越しではないので、この通信に対してファイアウォールの規則を定義する必要はありません。

2. 表 13-3 の Disk Agent と Media Agent も参照します。

   この表は、2 つのエージェントとも Session Manager に接続する可能性があること、および Media Agent は Utility Media Agent(UMA) に接続する可能性があることを示しています。ただし、この接続が発生するのは、共有テープ・ライブラリが使用される場合か、[切断された接続の再接続] オプションが有効な場合だけです。このオプションに詳細は「バックアップ仕様オプション」(302 ページ) を参照してください。

ポート範囲の設定

ファイアウォールを通る接続はすべて固定のポート番号 5555 に接続するため、この環境では OB2PORTRANGE または OB2PORTRANGESPEC 変数を定義する必要はありません。

制限事項

- クライアントの、ファイアウォール越しのリモート・インストールはサポートされていません。DMZ 内でクライアントをローカルにインストールする必要があります。
- このセルでは、イントラネット内のクライアントと同様、DMZ 内のクライアントもバックアップできます。ただし、クライアントの各グループは、ファイアウォールから見て同じ側にあるクライアント上で構成されているデバイスにバックアップする必要があります。

重要

お使いのファイアウォールが、イントラネットから DMZ への接続を制限していない場合、イントラネット内のクライアントを DMZ 内のクライアント上に構成されているデバイスにバックアップすることもできます。しかし、この場合はバックアップされたデータの安全性が低下するため、この方法はお勧めできません。

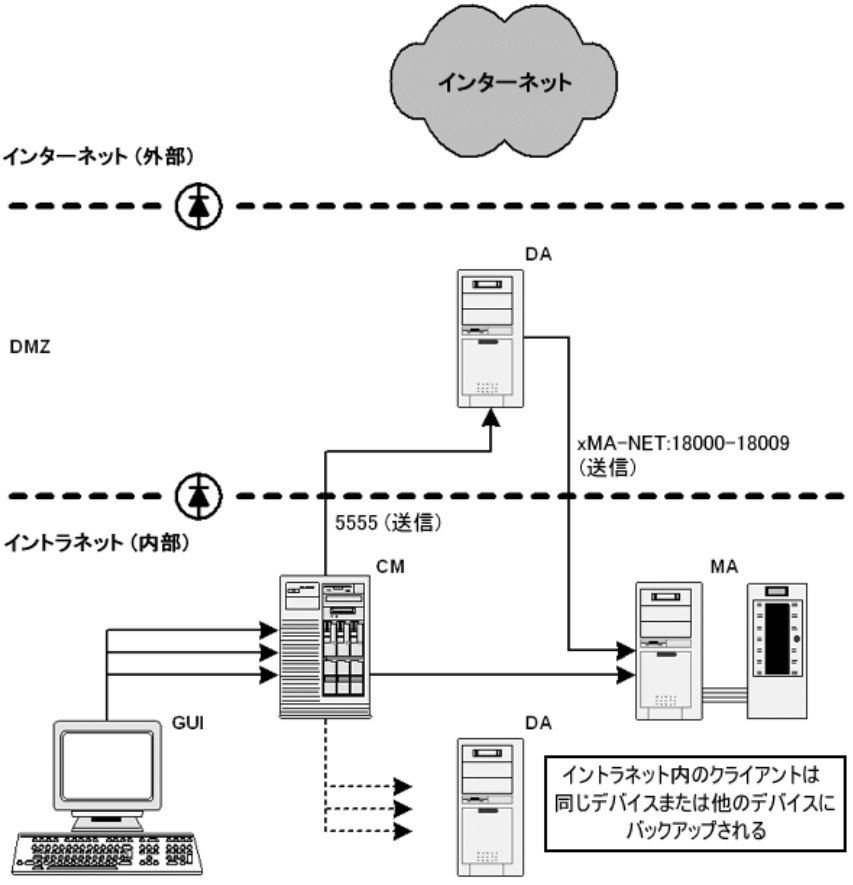
- DMZ 内のデバイスに別のクライアント上のロボティクスが構成されている場合、このクライアントも DMZ 内に存在しなければなりません。
- この設定では、DMZ 内のクライアント上の Application Agent を使用して、データベースまたはアプリケーションのバックアップを行うことはできません。DMZ 内の Application Agent の詳細は、「例 4: Application

Agent と Media Agent がファイアウォールの外側に インストールされており、他のコンポーネントはファイアウォールの内側にインストールされている場合。」(673 ページ) を参照してください。

例 2: Disk Agent がファイアウォールの外側にインストールされおり、他のコンポーネントはファイアウォールの内側にインストールされている場合。

Cell Manager、Media Agent、GUI をイントラネット内に配置し、一部の Disk Agent を DMZ 内に配置するバックアップ環境を構成します。

図 13-2 構成図



以下の 3 つの事項が、この構成のポート範囲の設定を決定します。

1. ファイアウォールを越えて通信する必要があるプロセスを特定するため、表 13-2 の Disk Agent の列を参照します。すると Disk Agent は、Session Manager からのポート 5555 への接続を受け付ける必要があることがわかります。したがってファイアウォールの規則は以下のようになります。

   - CM システムから DA システムのポート 5555 への接続を許可する。

2. 表 13-3 の Disk Agent も参照します。Disk Agent は Media Agent の動的割り

当てポートに接続することがわかります。一般的には Disk Agent と Media Agent 間の通信のためにファイアウォールをオープンすることはしたくないため、Media Agent に割り当てることができるリスン・ポートの範囲を制限する必要があります。

表 13-1 を参照して Media Agent のポート使用を確認します。Media Agent は、実行中の Media Agent ごとに 1 ポートを必要とします。たとえば、接続されているテープ・ドライブが 4 台あるとすれば、4 つの Media Agent が同時に実行される可能性があります。したがって、最低 4 ポートを使用可能にすることが必要です。しかし他のプロセスもこの範囲のポートを割り当てる可能性があるため、MA システム上では 10 ポート程度の範囲を指定する必要があります。

```
OB2PORTRANGESPEC=xMA-NET:18000-18009
```

したがって、Media Agent の通信に関するファイアウォールの規則は以下のようになります。

- DA システムから MA システムのポート 18000～18009 への接続を許可する。

注記

この規則では、DMZ からイントラネットへの通信を許可しており、セキュリティ上のリスクを秘めています。

3. 表 13-3 は、[切断された接続の再接続] オプションが有効になっている場合には、Disk Agent が Session Manager(BSM/RSM) に接続する必要があることも示しています。上記と同様、CM システム上で必要なポート範囲を指定します。

   ```
   OB2PORTRANGESPEC=xSM:20100-20199
   ```

注記

ファイアウォール越しの通信を行う Session Manager だけでなく、すべての Session Manager がこの範囲からポートを割り当てます。

制限事項

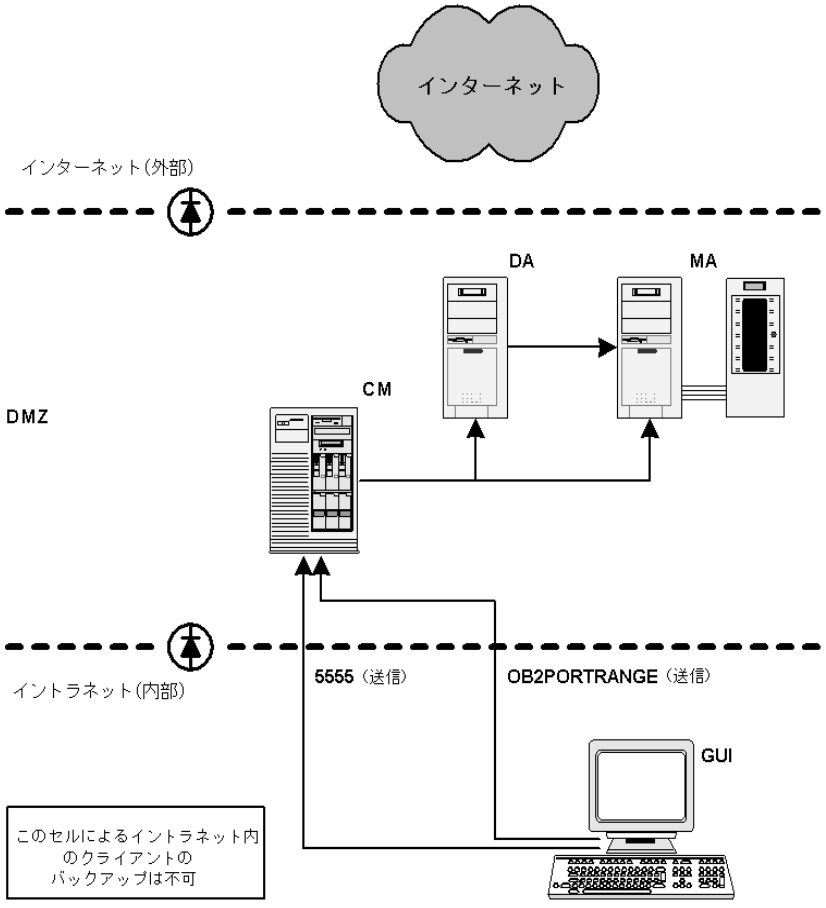
- クライアントの、ファイアウォール越しのリモート・インストールはサポートされていません。DMZ 内でクライアントをローカルにインストールする必要があります。

- この設定では、DMZ 内のクライアント上の Application Agent を使用して、データベースまたはアプリケーションのバックアップを行うことはできません。DMZ 内の Application Agent の詳細は、「例 4: Application Agent と Media Agent がファイアウォールの外側に インストールされており、他のコンポーネントはファイアウォールの内側にインストールされている場合。」(673 ページ) を参照してください。

例 3: GUI がファイアウォールの内側にインストールされおり、他のコンポーネントはファイアウォールの外側にインストールされている場合。

セル全体を DMZ 内に配置して、グラフィカル・ユーザー・インタフェースだけをイントラネット内に配置するバックアップ環境を構成します。

図 13-3　構成図



以下の 3 つの事項が、この構成のポート範囲の設定を決定します。

1. 表 13-2 と表 13-3 は、GUI は接続を受け付けないことを示しています。ただし、Cell Manager 上の以下のプロセスに接続する必要があります。

表 13-4

プロセス	ポート
Inet	5555

表 13-4

プロセス	ポート
CRS	動的
BSM	動的
RSM	動的
MSM	動的
DBSM	動的

したがって、Inet リスン・ポートへの接続に関するファイアウォールの規則は以下のようになります。

- GUI システムから CM システムのポート 5555 への接続を許可する。

2. 表 13-1 は、CRS に必要なのは 1 ポートだけであることを示しています。しかし他のプロセスもこの範囲のポートを割り当てる可能性があるため、CM システム上では 5 ポート程度の範囲を指定する必要があります。このポート範囲の定義は以下のようになります。

   ```
   OB2PORTRANGESPEC=CRS:20000-20004
   ```

   この結果、CRS プロセスへの接続に関するファイアウォールの規則は以下のようになります。

   - GUIシステムからCMシステムのポート20000～20004への接続を許可する。

3. Session Manager については、状況が複雑です。すべての Session Manager は 1 ポートのみ必要とします。しかし、Session Manager(BSM、RSM、MSM、DBSM) の数はバックアップ環境により大きく変わります。最低限必要なポート数は以下の公式で見積もることができます。

   NoOfPorts = NoOfConcurrentSessions + NoOfConnectingGUIs

Cell Manager 上のポート範囲の設定

たとえば、25 のバックアップ・セッションと 5 つの復元セッションが実行中で、2 つの GUI がオープンされている場合、最低 32 ポートが使用可能である必要があります。しかし他のプロセスもこの範囲のポート

を割り当てる可能性があるため、CM システム上では 100 ポート程度の範囲を指定する必要があります。このポート範囲の定義は以下のようになります。

```
OB2PORTRANGESPEC=xSM:20100-20199
```

または

```
OB2PORTRANGESPEC=BSM:20100-20139;RSM:20140-20149;DBSM:20150-20199
```

制限事項

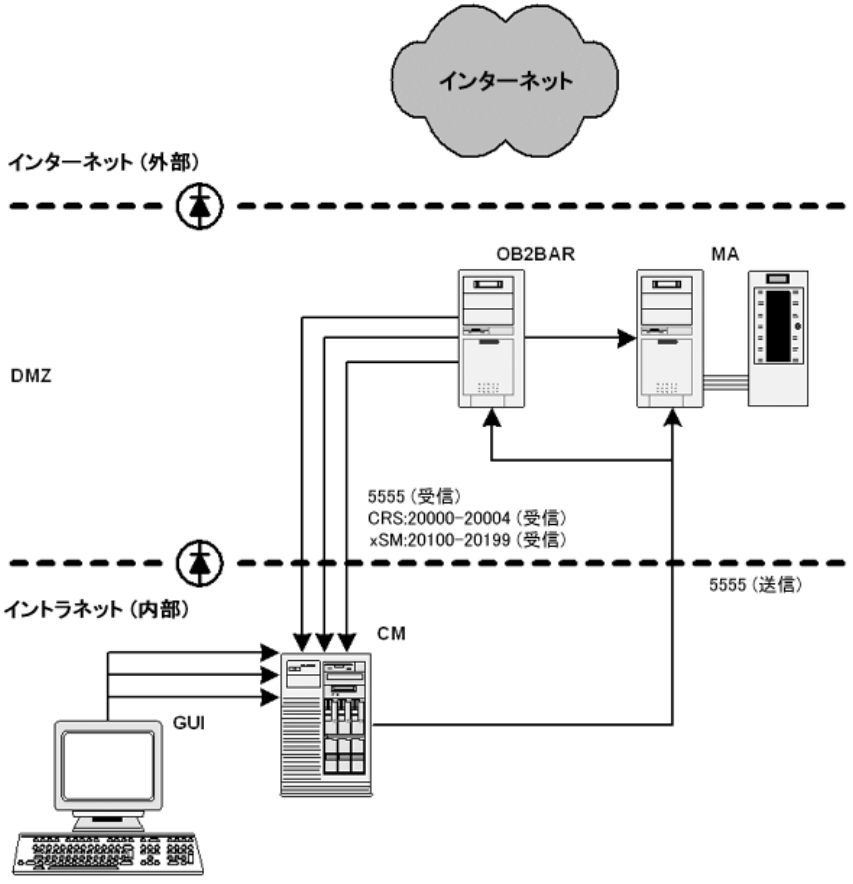
この構成では、リモート・インストールやデータベース / アプリケーションのオンライン・バックアップなど、Data Protector のほとんどの機能が使用可能です。

- メディア集中管理またはライセンス集中管理を使用する場合で、MoM セルがファイアウォールの内側にある場合、このセルを MoM 環境に所属させることはできません。
- バックアップ・クライアントはすべて DMZ 内にある必要があります。GUI クライアントは、DMZ 内の Media Agent でバックアップできません。GUI はイントラネット内の他のセルのメンバーから実行することもできます (両方のセルが同じ `Inet` リスン・ポートを使用している場合)。

例 4: Application Agent と Media Agent がファイアウォールの外側にインストールされており、他のコンポーネントはファイアウォールの内側にインストールされている場合。

Cell Manager と GUI をイントラネット内に配置して、一部の Application Agent(SAP R/3, Oracle など) と Media Agent を DMZ 内に配置するバックアップ環境を構成します。

図 13-4 構成図



以下の 3 つの事項が、この構成のポート範囲の設定を決定します。

1. 表 13-2 は、Application Agent が Cell Manager 上の以下のプロセスに接続することを示しています。

表 13-5

プロセス	ポート
Inet	5555

表 13-5

プロセス	ポート
CRS	動的
RSM	動的
BSM	動的
DBSM	動的
xMA-NET	動的

ここで、Application Agent は Media Agent にも接続しますが、この接続はファイアウォール越しではないため、ポート範囲を定義する必要はありません。

したがって、Inet リスン・ポートへの接続に関するファイアウォールの規則は以下のようになります。

- Application Agent システムから CM システムのポート 5555 への接続を許可する。

注記

この規則では、DMZ からイントラネットへの通信を許可しており、セキュリティ上のリスクを秘めています。

2. 表 13-1 は、CRS に必要なのは 1 ポートだけであることを示しています。しかし他のプロセスもこの範囲のポートを割り当てる可能性があるため、CM システム上では 5 ポート程度の範囲を指定する必要があります。このポート範囲の定義は以下のようになります。

   ```
   OB2PORTRANGESPEC=CRS:20000-20004
   ```

   この結果、CRS プロセスへの接続に関するファイアウォールの規則は以下のようになります。

   - Application Agent システムから CM システムのポート 20000～20004 への接続を許可する。

3. バックアップ Session Manager と復元 Session Manager については、状況が複雑です。各バックアップおよび復元セッションは 1 つの Session Manager により開始され、すべての Session Manager は 1 ポートのみ必

要とします。さらに、Application Agent がいくつかの DBSM を起動する可能性もあります。Microsoft Exchange、Microsoft SQL、Lotus NOtes/Domino Server 用統合ソフトウェアでは 1 つの DBSM が起動されます。Oracle、SAP R/3 用統合ソフトウェアでは「同時処理数 +1」の DBSM が起動されます。CM システム上で、Session Manager に対するポート範囲を OB2PORTRANGESPEC 変数に追加する必要があります。

Cell Manager 上のポート範囲の設定

```
OB2PORTRANGESPEC=CRS:20000-20004;xSM:20100-20199
```

この結果、Session Manager への接続に関するファイアウォールの規則は以下のようになります。

- Application Agent システムから CM システムのポート 20100～20199 への接続を許可する。

制限事項

- クライアントの、ファイアウォール越しのリモート・インストールはサポートされていません。DMZ 内でクライアントをローカルにインストールする必要があります。
- このセルでは、イントラネット内のクライアントと同様、DMZ 内のクライアントもバックアップできます。ただし、クライアントの各グループは、ファイアウォールから見て同じ側にあるクライアント上で構成されているデバイスにバックアップする必要があります。

重要

お使いのファイアウォールが、イントラネットから DMZ への接続を制限していない場合、イントラネット内のクライアントを DMZ 内のクライアント上に構成されているデバイスにバックアップすることもできます。しかし、この場合はバックアップされたデータの安全性が低下するため、この方法はお勧めできません。

- DMZ 内のデバイスに別のクライアント上のロボティクスが構成されている場合、このクライアントも DMZ 内に存在しなければなりません。

14 トラブルシューティング

本章の概略

Data Protector で問題が発生した場合は、本章で説明する解決方法に従って、元の状態に復帰させてください。以下の内容について説明します。

「ADIC/GRAU DAS および STK ACS ライブラリの インストールと構成に関するトラブルシューティング」（763 ページ)

「Data Protector が適切に作動しているかチェックする方法」(757 ページ)

Data Protector の性能に関する項目の概要やヒントについては、「性能に関する検討事項」(A-8 ページ) を参照してください。

バックアップ・デバイス (テープ・ドライブなど) では、専用の Data Protector ライセンスが必要になる場合があります。詳細は、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

当社サポート・サービスへご連絡いただく前に

お客様の問題解決を迅速に行うため、HP カスタマー・サポート・サービスに問題をご報告いただく前に、準備を行っていただく必要があります。以下に、お客様にしていただきたい事前作業を示します。

以下のことを確認してください。

- 現在のバージョンの制限事項に触れていないかどうか。Data Protector の制限事項と推奨事項、Data Protector に関連するものとしないものを含めた既知の問題点については、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。
- 問題がサードパーティ製ソフトウェアに関連していないかどうか。サードパーティ製ソフトウェアに関連している場合は、ベンダーのサポート窓口に連絡してください。
- 最新の Data Protector パッチがインストールされているかどうか。パッチは、HP OpenView の Web サイト（http://support.openview.hp.com/patches/patch_index.jsp）から入手できます。OS パッチのリストについては、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。
- 統合バックアップの場合、バックアップ失敗の原因がアプリケーションのダウンではないこと。
- デバッグ・ログまたはリドゥ・ログ・ファイルシステムがオーバーフローしていないこと。
- アプリケーション・データ・ファイルシステムがオーバーフローしていないこと。

発生した問題に関して、以下のデータを収集します。

- セッションの出力を含む問題の説明 (または問題の種類によっては、セッションの出力に相当する出力)。
- Cell Manager および関係するクライアントすべてに対する `omnidlc` コマンドの出力。`omnidlc` コマンドの詳細は「omnidlc コマンド」（691 ページ) を参照してください。

Data Protector ログ・ファイル

Data Protector アプリケーションの使用中に問題が生じた場合、ログ・ファイルの情報を使って問題を調べます。

ログ・ファイルの位置

Data Protector のログ・ファイルは以下のディレクトリにあります。

- Windows の場合 : *<Data_Protector_home>*¥log
- HP-UX および Solaris システムの場合 : /var/opt/omni/log および /var/opt/omni/server/log
- その他の UNIX システムの場合 : /usr/omni/log
- Novell NetWare の場合 : SYS:¥USR¥OMNI¥LOG

ログ・ファイルの形式

ほとんどの Data Protector ログ・ファイルのエントリは以下の形式になっています。

<time_stamp> <process:PID:Thread_ID> <source_file and branch> <Data Protector_version> <log_entry_message>

例 :

```
09/06/00 16:20:04 XOMNI.11561.0 ["/src/lib/ipc/ipc.c
/main/r31_split/10":3414] A.04.10 b325[ipc_receiveDataEx]
buffer 102400 bytes to small to receive data 796226418 bytes
=> ignored
```

ログ・ファイルとその内容

下表に Data Protector ログ・ファイルに記録される情報を示します。

表 14-1 **Data Protector ログ・ファイル**

ログ・ファイル	説明
debug.log	予期しない状況が記録されます。ユーザーにとって役立つものもありますが、主に当社サポート・サービスが使用します。
Ob2EventLog.txt	Data Protector の操作中に発生した Data Protector イベント、およびすべての Data Protector 通知が記録されます。イベント・ログには、Data Protector イベントが一括して保存されます。
inet.log	Data Protector`Inet` サービスに対して発行される要求が記録されます。クライアント上で最近行われた Data Protector の動作をチェックする際に役立ちます。
IS_install.log	リモート・インストールのトレース結果が記録されます。インストール・サーバに保存されます。
media.log	メディアがバックアップ用に使用されたり、初期化またはインポートされるたびに、このファイルに新しいエントリが作成されます。IDB の復旧では、`media.log` を使って、データベースをバックアップしたテープや、前回のバックアップ以降に使用されたメディアを検索できます。
omnisv.log	Data Protector サービスがいつ起動 / 終了されたかに関するデータが記録されます。
purge.log	IDB のバックグラウンドでの削除動作のトレース結果が記録されます。

表 14-1 Data Protector ログ・ファイル

ログ・ファイル	説明
RDS.log	IDB のログが記録されるファイルです。このファイルは Cell Manager 上の以下のディレクトリにあります。 Windows の場合 : *<Data_Protector_home>*¥db40¥datafiles¥catalog UNIX の場合 : /var/opt/omni/server/db40/datafiles/catalog
sanconf.log	sanconf コマンドにより生成されたセッション・レポートが格納されています。
sm.log	バックアップ / 復元セッションで発生したエラー (バックアップ仕様の解析エラーなど) が記録されます。
upgrade.log	アップグレード時に作成されるログ・ファイルで、UCP（アップグレード・コア・パート）および UDP（アップグレード詳細パート）メッセージが記録されます。
OB2_Upgrade.log (UNIX のみ)	アップグレード時に作成されるログ・ファイルで、アップグレード処理のトレース結果が記録されます。
sap.log、oracle8.log、informix.log、sybase.log、db2.log	アプリケーション固有のログ・ファイルで、アプリケーションと Data Protector 間の統合ソフトウェア呼び出しに関するトレース結果が記録されます。これらのファイルはアプリケーション・サーバに保存され、統合ソフトウェアのトラブルシューティングに使用できます。

デバッグ

デバッグの収集が必要となるのは、ユーザーが直面した技術的な問題を当社サポート・サービスが解決するために情報が必要となった場合だけです。Data Protector をデバッグ・モードで実行すると、デバッグ情報が作成され、大量のディスク・スペースを消費します。Data Protector をデバッグ・モードで実行する際にどの詳細レベルを適用するか、またどの環境条件を使用するかについては、当社サポート・サービスにお問い合わせください。

デバッグの最大サイズの制限

循環デバッグ

Data Protector を、循環デバッグと呼ばれる特殊なデバッグ・モードで実行することができます。このモードでは、デバッグ・ファイルのサイズが事前設定されたサイズ（*n*）に達するまで、デバッグ・メッセージが追加されます。事前設定されたサイズに達すると、カウンターがリセットされ、最も旧いデバッグ・メッセージが上書きされます。これにより、最新レコードに影響を与えることなく、トレース・ファイルのサイズを制限できます。

どのような場合に循環デバッグを使用するか

このモードは、セッションの終わり近くで問題が発生する場合、または問題発生後すぐに Data Protector が中止または終了する場合にのみ使用することをお勧めします。

必要なディスク・スペースの推定

循環デバッグを使用する場合、必要なディスク・スペースの推定値は以下のようになります。

- Media Agent クライアント：バックアップまたは復元で実行される Media Agent ごとに、`2*n[kB]`
- Disk Agent クライアント：バックアップまたは復元のマウント・ポイントごとに、`2*n[kB]`
- Cell Manager クライアント：`2*n [kB]`
- 統合ソフトウェア・クライアント：`2*n[kB] *` *並行数*
- Inet および CRS のデバッグでは、それぞれの動作に対して個別にデバッグ・トレースが作成されるため、正確な上限値を計算することはできません。

デバッグの方法

デバッグ・トレースを作成するために Data Protector をデバック・モードで起動するには、いくつかの方法があります。デバッグ・オプションの詳細は、「デバッグ構文」（686 ページ) を参照してください。

重要

Data Protector がデバッグ・モードで実行されている場合、すべての動作についてデバッグ情報が生成されます。たとえば、バックアップ仕様をデバッグ・モードで起動すると、このバックアップ仕様でバックアップされたすべてのクライアントに関するデバッグ情報が Disk Agent によって生成されます。

Data Protector GUI を使ったデバッグ

Data Protector GUI でデバッグ用オプションを設定するには、[ファイル] メニューで、[選択値] をクリックし、続いて [デバッグ] タブをクリックします。デバッグ・オプションを指定して GUI を再起動すると、GUI がデバッグ・モードで再起動されます。

トレース構成ファイルを使用したデバッグ

デバッグ・オプションを設定する別の方法は、トレース構成ファイルを編集することです。構成ファイルは以下の場所にあります。
`/etc/opt/omni/server/options/trace` （UNIX の場合）、または
`<Data_Protector_home>¥Config¥server¥Options¥trace` （Windows の場合）。

OB2OPTS 変数を使用したデバッグ

Data Protector 統合ソフトウェア用のデバッグ・パラメータは、OB2OPTS 環境変数を使用して設定します。OB2OPTS 変数の詳細は、当社サポート担当までご連絡ください。

スケジュール設定されたセッションのデバッグ

スケジュール設定されたセッションをデバッグするには、スケジュール・ファイルを編集します。スケジュール・ファイルは以下の場所にあります。
`/etc/opt/omni/server/schedules` または
`/etc/opt/omni/server/barschedules` （UNIX の場合）、
`<Data_Protector_home>¥Config¥server¥Schedules` または

<Data_Protector_home>¥Config¥server¥BarSchedules （Windows の場合）。デバッグ・パラメータは、ファイルの最初の行に追加してください。

注記

ファイルを編集する前にコピーを作成して、デバッグが不要になった場合に変更を元に戻せるようにしておく必要があります。

スケジュール・ファイル変更の例

```
-debug 1-99 sch.txt
-full
-only 2002
-day 14 -month Dec
-at 22:00
```

デバッグ構文

ほぼすべての Data Protector コマンドは、以下の構文を持つパラメータ -debug を使って起動できます。

-debug 1-99[,C:*<n>*][,T:*<s>*] *<XYZ>* [*<host>*]

上記で

1-99 はデバッグの範囲を示します。デバッグ範囲は、特に指示のない限り、1-99 と指定してください。

C:*<n>* は、デバッグ・ファイルのサイズを *n*KB に制限します。最小値は 4（4KB）で、デフォルト値は 1024（1MB）です。

T:*<s>* は、タイムスタンプの分解能です。デフォルトは 1 で、1000 が分解能 1 ミリ秒、0 がタイムスタンプを使用しないことを意味します。タイムスタンプの分解能と循環デバッグのサイズ制限は、範囲パラメータの一部として指定されます。

<XYZ> は、デバッグの接尾辞です（DBG_01.txt など）。

<host> は、デバッグ・モードが起動されているホスト名のリストです。

注記

一部のプラットフォーム（Novell NetWare、MPE）では、ミリ秒単位の分解能は指定できません。

Data Protector コマンドの実行中にデバッグの対象とするシステムを指定するには、ホスト名のリストを使用します。リストで複数のシステムを指定する場合は半角スペースで区切ります。また、リスト全体を引用符で囲む必要があります。(例 : "host1.company.com host2.company.com")

トレース・ファイル名

デバッグの接尾辞オプションを使って、トレース・ファイルを以下のディレクトリに作成します。

- UNIX システムの場合 : /tmp
- Windows の場合 : *<Data_Protector_home>*¥tmp
- Novell NetWare の場合 : SYS:¥USR¥OMNI¥TMP

ファイル名は以下のようになります。

OB2DBG_*<did>*__*<Program>*_*<Host>*_*<pid>*_*<XYZ>*

上記で

<did>（デバッグ ID）は、デバッグ・パラメータを最初に受け付けたプロセスのプロセス ID です。この ID がデバッグ・セッションの ID として使用されます。後続のプロセスもこの ID を使用します。

*<Program>*はトレース結果の書き込みを行う Data Protectorプログラムのコード名です。

<Host> はトレース・ファイルが作成されるホストの名前です。

<pid> はプロセス ID です。

<XYZ> は -debug パラメータで指定された接尾辞です。

バックアップまたは復元セッションの ID（*<sid>*）が決まると、それがファイル名に付加されます。

OB2DBG_*<did>*_*<sid>*_*<Program>*_*<Host>*_*<pid>*_*<XYZ>*

<sid> を付加するプロセスは、BMA/RMA、xBDA/xRDA、およびセッションにより起動された他のプロセスであり、BSM/RSM 自体によっては付加されません。

注記

セッション ID は、デバッグ・ファイルの識別に役立ちます。他のデバッグ・ファイルも同じセッションに属している場合、それらにも付加する必要があります。

trace.log

`trace.log` ファイルは Cell Manager 上に作成され、デバッグ・ファイルがどこに（どのホストに）作成されたか、どのようなデバッグ接頭辞が使われたかという情報が保存さます。このファイルには、生成されたすべてのファイルのリストが含まれているわけではないことに注意してください。

OB2DBGDIR

トレース・ファイルのデフォルトの位置は、`omnirc` 変数の `OB2DBGDIR` でシステムごとに変更できます。`omnirc` 変数の詳細は、「omnirc オプションの使用」（647 ページ）を参照してください。

UNIX 上の INET デバッグ

UNIX システム上で `Inet` をデバッグするには、`/etc/inetd.conf` ファイルの以下の行

1. `omni stream tcp nowait root /opt/omni/lbin/inet inet -log /var/opt/omni/log/inet.log`

   を以下のように変更します。

   `omni stream tcp nowait root /opt/omni/lbin/inet inet -log /var/opt/omni/log/inet.log -debug 1-140 SSF`

2. ファイルを変更、保存した後、`/etc/inetd -c` コマンドを実行して変更を適用します。

注記

`Inet` デバッグを有効に設定した場合は、すべての統合ソフトウェアによってトレース・ログ・ファイルが生成されます。

Windows 上の INET デバッグ

Windows システム上で Data Protector `Inet` をデバッグするには、Windows Service Control Manager を起動し、Data Protector `Inet` サービスを次の起動パラメータを使って再起動します。

```
-debug 1-140 <POSTFIX>
```

注記

Inet デバッグを有効に設定した場合は、すべての統合ソフトウェアによってトレース・ログ・ファイルが生成されます。

UNIX 上の CRS デバッグ

UNIX システム上で CRS をデバッグするには、以下の手順を行います。

1. `/opt/omni/lbin/crs -shutdown` コマンドを実行して CRS を停止します。
2. `/opt/omni/lbin/crs -debug 1-140 <POSTFIX>` コマンドを実行して、CRS をデバッグ・オプション付きで再起動します。

Windows 上の CRS デバッグ

Windows システム上で Data Protector CRS をデバッグするには、Windows Service Control Manager を起動し、Data Protector CRS サービスを次の起動パラメータを使って再起動します。

```
-debug 1-140 <POSTFIX> <Cell_Manager_name>
```

注記

実行トレース・ファイルの容量は非常に大きくなる可能性があるため、`-debug` オプションを使用する際は注意が必要です。

Microsoft クラスター環境での CRS デバッグ

Data Protector 共有ディレクトリで、*<Data_Protector_home>*¥Config¥server¥options¥Trace ファイルを編集します。以下の行を追加します。

```
ranges=1-99,110-500

postfix=DBG

select=obpkg.rc.aus.hp.com
```

クラスター・アドミニストレータ GUI から、CRS サービス・リソース (OBVS_MCRS) をオフラインにします。

注意

Data Protector パッケージがフェイルオーバーする原因となるため、Windows Service Control Manager から CRS を終了しないでください。

MC/ServiceGuard 環境での CRS デバッグ

MC/ServiceGuard 環境で Data Protector CRS をデバッグするには、以下の手順を実行します。

1. `/etc/opt/omni/server/options/trace` ファイルを開き、コメントを解除して必要なデバッグ・オプションを設定します。ファイルを閉じて保存します。
2. `/opt/omni/lbin/crs -redebug`コマンドを実行してデバッグ収集を開始します。

デバッグ収集を停止するには、`/etc/opt/omni/server/options/trace` ファイルのすべてのデバッグ・オプションを空白に設定してファイルを保存した後、`/opt/omni/lbin/crs -redebug` コマンドを実行します。

HP カスタマー・サポート・サービスに送付するデータの収集

Data Protector は大規模なネットワーク環境で動作するため、HP サポート・サービスが必要とするデータの収集が難しい場合があります。Data Protector には、HP サポート・サービスに送付するログ・ファイル、デバッグ・ファイル、getinfo ファイルの収集やパッキングを行うためのツールが備わっています。

Data Protector のデバッグを有効すると（「デバッグ」（684 ページ) または「HP カスタマー・サポート・サービスに送付するデータ収集の例」（698 ページ) を参照）、Data Protector `omnidlc` コマンドで HP サポート・サービスが必要とするデータを圧縮することができます。このコマンドにより、データは選択したクライアントまたは Cell Manager から Cell Manager または MoM に転送され、自動的にパックされます。

`omnidlc` コマンドで、データを選択して収集することができます。たとえば、あるクライアントのログ・ファイルのみを収集したり、特定の Data Protector セッション中に作成されたデバッグ・ファイルのみを収集したりすることができます。

`omnidlc` コマンドの詳細は、「omnidlc コマンド」（691 ページ) を参照してください。

注記

`omnidlc` コマンドで Data Protector インストール実行トレースを収集することはできません。Data Protector インストール実行トレースの作成・収集方法の詳細は、HP OpenView Storage Data Protector インストールおよびライセンス・ガイドの「インストール実行トレースの作成」を参照してください。

omnidlc コマンド

概要

`omnidlc` コマンドは、Data Protector のデバッグ・ファイル、ログ・ファイル、getinfo ファイルを、Data Protector セル（デフォルトではすべてのクライアント）または MoM 環境（デフォルトではすべての Cell Manager）から収集します。MoM 内の Cell Manager からデータを収集するには、このコマ

ンドを MoM から実行する必要があります。MoM 環境内のクライアントからデータを収集するには、このコマンドを Cell Manager から実行しなければなりません。

データ収集後、以下の処理が可能です。

- Cell Manager または MoM で圧縮やパックができます。
- クライアントから削除できます。
- 収集データに必要なディスク・スペースを表示させることができます。

注記

上記 3 つのうち同時に実行できるのは 1 つだけです。

omnidlc コマンドで、パックまたは圧縮されたファイルをアンパックまたは展開したり、収集データの範囲を限定したりすることもできます。

制限事項

- Data Protector のデフォルト・デバッグ・ディレクトリ以外のディレクトリに作成された**デバッグ**・ファイルを omnidlc コマンドで収集するには、そのファイルを /tmp ディレクトリ（UNIX の場合）、または *<Data_Protector_home>*¥tmp ディレクトリ（Windows の場合）にコピーする必要があります。このコマンドは、Data Protector のデフォルト・デバッグ・ディレクトリ（UNIX では /tmp、Windows では *<Data_Protector_home>*¥tmp）からしか**デバッグ**・ファイルを収集しません。
- 収集ファイル以外のファイルをパッケージに追加するには、omnidlc コマンドを実行する前に、以下のいずれかのディレクトリに目的のファイルをコピーします。dlc/*<client>*/getinfo、dlc/*<client>*/log、または dlc/*<client>*/tmp。追加できるのはファイルだけで、ディレクトリは追加できません。上記のいずれかのディレクトリにファイルをコピーしておかなければ、アンパック・フェーズでパッケージをアンパックすることができません。
- このコマンドは Cell Manager および MoM でのみ使用可能です。
- Data Protector インストール実行トレースの収集には使用できません。
- Cell Manager 以外のシステムに関する Data Protector GUI デバッグ・ファイルは、-hosts オプションを使用した場合のみ収集できます。-hosts オプションの詳しい説明は本項に記載されています。

- クラスター内のデバッグ・ファイルを収集するには、-hosts オプションを使用し、その引数としてクラスター・ノードのホスト名を指定する必要があります。クラスター環境で -hosts オプションが指定されなかった場合、アクティブなノードからデータが収集されます。-hosts オプションの詳しい説明は本項に記載されています。
- MA エージェントが別のクライアント上で UMA プロセスを開始した場合、UMA デバッグ情報は収集されません。この場合は、-hosts オプションまたは -allhosts オプションを使用してください。ただし大規模な環境では、-allhosts オプションの使用はお勧めできません。

構文

以下に、omnidlc コマンドの構文を示します。

```
omnidlc {-session <sessionID> | -did <debugID> | -postfix
string | -no_filter} [-allhosts | -hosts <list>] [-pack
<filename> | -depot [<directory>] | -space | -delete_dbg]
[-no_getinfo] [-no_logs] [-no_debugs] [-no_compress]
[-verbose]

omnidlc -localpack [<filename>]

omnidlc -unpack [<filename>]

omnidlc -uncompress <filename>
```

収集データの範囲限定

収集データの範囲を限定するには、次に示す omnidlc コマンド・オプションを使用します。

```
{-session <sessionID> | -did <debugID> | -postfix string |
-no_filter} [-allhosts | -hosts <list>] [-no_getinfo]
[-no_logs] [-no_debugs]
```

以下の機能を組み合わせて収集データの範囲を制限してください。

- セル内のすべてのシステムからデータを収集します（-allhost オプションを使用）。これはデフォルトの動作です。
- 選択したシステムだけからデータを収集します（-hosts *<list>* オプションを使用）。*<list>* 引数は、クライアントのホスト名（MoM 環境では Cell Manager のホスト名）で、空白で区切ります。
- 収集データから getinfo ファイル、ログ・ファイル、デバッグ・ファイルを除外できます（-no_getinfo、-no_logs、または -no_debugs オプションを使用）。

- 特定のセッションだけからデバッグ・ファイルを収集します（-session *<sessionID>* オプションを使用）。
- 指定したデバッグ ID と一致するデバッグ・ファイルを収集します（-did *<debugID>* オプションを使用）。
- 指定した接尾辞と一致するデバッグ・ファイルを収集します（-postfix *<string>* オプションを使用）。

注記

-did または -session オプションを使用した場合、Cell Manager 以外のクライアントからのデバッグ・ファイル、ログ・ファイル、getinfo ファイルが収集されないことがあります。そのような場合には、-hosts または -allhosts オプションを追加してください。-allhosts オプションを使用するとコマンドの実行に時間がかかることに注意してください。

収集データの範囲を制限しないためには、-no_filter オプションを使用します。このオプションを使用した場合は、-allhosts または -host *<list>* オプションを指定する必要があります。

クライアント上での圧縮

次に、デフォルトでは、収集データは関係するクライアント上で圧縮されます。-no_compress オプションで、クライアント上での圧縮を禁止することもできます。圧縮ファイルには .gz という拡張子が付加されます。圧縮ファイルは、-uncompress *<filename>* オプションで展開できます。

収集データの操作

圧縮済みまたは未圧縮の収集データに対してクライアント上で実行する操作を選択するには、以下の omnidlc コマンド・オプションを使用します。

[-pack *<filename>* | -depot [*<directory>*] | -space | -delete_dbg]

圧縮済みまたは未圧縮の収集データに対しては、以下の操作のうちいずれかを実行できます。

- ネットワーク経由で Cell Manager に送信する（デフォルトの動作）。この場合は以下のような操作が可能です。
  - -pack *<filename>* オプションを使用しない場合、収集データは現在のディレクトリに dlc.pck ファイルとしてパック、保存されます。-pack *<filename>* オプションを使用した場合は、現在のディレクトリに指定したファイル名で（*<filename>* 引数をファイル名

として指定した場合）、または指定したディレクトリに指定したファイル名で（*<filename>* 引数をフルパス名として指定した場合）にパック、保存されます。

パックされたファイルには、関係するクライアントのホスト名、パス、（圧縮された）収集ファイルを含むディレクトリ構造が含まれています。

パックされたファイルは、`-unpack [<filename>]` オプションでアンパックできます。

— 収集データをパックしないまま指定したディレクトリに保存します（`-depot [<directory>]` オプションを使用）。*<directory>* を指定しないと、ファイルは *<Data_Protector_home>*¥tmp¥dlc ディレクトリ（Windows Cell Manager の場合）、または /tmp/dlc ディレクトリ（UNIX Cell Manager の場合）に保存されます。*<directory>* を指定した場合は、収集ファイルは指定したディレクトリ内の dlc ディレクトリに保存されます。

パックまたはアンパックしたファイルのディレクトリは、以下のように生成されます。

```
./dlc/client_1/tmp/debug_files

./dlc/client_1/log/log_files

./dlc/client_1/getinfo/get_info.txt

./dlc/client_2/tmp/debug_files

./dlc/client_2/log/log_files

./dlc/client_2/getinfo/get_info.txt

...
```

- クライアント上で削除する（`-delete_dbg` オプションを使用）。デバッグ・ファイルだけが削除されることに注意してください。getinfo ファイルとログ・ファイルは削除されません。
- データの収集に必要な Cell Manager 上のディスク・スペースを表示する（`-space` オプションを使用）。

データのセグメント化

収集データがネットワーク経由で Cell Manager に送信されるとき、送信ファイルのサイズが 2GB を超えている場合、そのファイルは圧縮前に（圧縮しないことも可能）2GB の断片に分割された後、Cell Manager に送信さ

れます。それぞれの断片のファイル名には、元のファイル名に s001 から s999 までが追加されます。ファイルが圧縮されていない場合、拡張子（.gz）は追加されません。一方、Cell Manager 側では、圧縮済みまたは未圧縮の収集ファイルのサイズがすべて 2GB を超えている場合、収集ファイルは 2GB（元のサイズ）のパッケージにパックされ、ファイル名には s001 から s999 までが追加されます。

その他の操作

- 収集データが Cell Manager に送信された場合、圧縮済みまたは未圧縮の**パックされていない**収集ファイル（-depot [*<directory>*] オプションを使用した場合）は、-localpack [*<filename>*] オプションでパックすることができます。このオプションは、現在のディレクトリ (-depot オプションで生成された dlc ディレクトリを含むディレクトリであること) のディレクトリ構造を *<filename>* 引数で指定したファイルにパックします。*<filename>* 引数を指定しなかった場合は、現在のディレクトリに dlc.pck ファイルが作成されます。

  このオプションは -pack *<filename>* オプションと同様の機能を持ちますが、データが -depot [*<directory>*] オプションを使用して収集された場合のみ使用してください。

- パックされた収集データをアンパックするには、-unpack [*<filename>*] オプションを使用します。*<filename>* 引数を指定しなかった場合は、現在のディレクトリの dlc.pck ファイルがアンパックされます。データは常に現在のディレクトリ内の dlc ディレクトリにアンパックされます。このオプションは、(圧縮済みまたは未圧縮の) 収集データが Cell Manager 上で、-pack *<filename>* オプションまたは -localpack [*<filename>*] オプションのどちらかを使用してパックされた場合に使用してください。

- パックされていない単一の圧縮ファイルを展開するには、-uncompress *<filename>* オプションを使用します。このオプションは、パックされたデータを -unpack [*<filename>*] オプションでアンパックした後で使用してください。

- 詳細出力を有効にするには、-verbose オプションを指定します。デフォルトでは、詳細出力は無効になっています。

例

1. 詳細出力を有効にして、セル内のすべてのデバッグ・ファイル、ログ・ファイル、getinfo ファイルを収集・圧縮し、それらを Cell Manager の現在のディレクトリに“dlc.pck”ファイルとしてパックするには、次のコマンドを実行します。

```
omnidlc -no_filter -allhosts -verbose
```

2. “client1.company.com”および“client2.company.com”というクライアントからログ・ファイルとデバッグ・ファイルのみを Cell Manager の“c:¥depot”ディレクトリに収集し（getinfo ファイルは収集しない）、圧縮もパックも行わないようにするには、次のコマンドを実行します。

   ```
   omnidlc -no_filter -hosts client1.company.com
   client2.company.com -depot c:¥depot -no_getinfo
   -no_compress
   ```

3. “client1.company.com”というクライアントからログ・ファイル、デバッグ・ファイル、getinfo ファイルを収集し、それらを Cell Manager の“c:¥pack¥pack.pck”というファイルに圧縮・パックするには、次のコマンドを実行します。

   ```
   omnidlc -hosts client1.company.com -pack c:¥pack¥pack.pck
   ```

4. “2003/08/27-9”という ID を持つセッションに関するデバッグ・ファイルをすべて削除するには、次のコマンドを実行します。

   ```
   omnidlc -session 2003/08/27-9 -delete_dbg
   ```

5. クライアント“client.company.com”の“2351”というデバッグ ID と持つ未圧縮デバッグ・ファイルに関して、Cell Manager 上で必要なディスク・スペースを表示させるには、次のコマンドを実行します。

   ```
   omnidlc -did 2351 -hosts client.company.com -space
   -no_getinfo -no_logs -no_compress
   ```

6. 現在のディレクトリ (`-depot` オプションで生成された `dlc` ディレクトリを含むディレクトリであること) のディレクトリ構造を、同じディレクトリ内の“dlc.pck”ファイルにパックするには、次のコマンドを実行します。

   ```
   omnidlc -localpack
   ```

7. 現在のディレクトリ内の“dlc”ディレクトリに“dlc.pck”ファイルをアンパックするには、次のコマンドを実行します。

   ```
   omnidlc -unpack
   ```

HP カスタマー・サポート・サービスに送付するデータ収集の例

あるクライアントと Cell Manager に関して、バックアップ・セッション中に発生した問題についてデバッグ・ファイル、ログ・ファイル、getinfo ファイルを収集するには、以下の手順を行います。

1. 以下を行って、エラー環境の規模をできる限り縮小します。
   - 1つまたは少数のファイルやディレクトリだけを含むバックアップ仕様を作成します。
   - 障害が発生している1つのクライアントだけをデバッグの実行対象とします。
2. 情報用のテキスト・ファイルを作成して、以下の情報を入力します。
   - Cell Manager、Media Agent、Disk Agent クライアントのハードウェア識別名 (例： `HP 9000` シリーズ `T-600`、`Vectra XA`)
   - Windows Media Agent クライアント用 SCSI コントローラ名 (例 : `onboard_type/Adaptec xxx/...`)
   - トポロジーの情報 (`omnicellinfo -cell` コマンドの出力から入手可能)
   - `devbra -dev` コマンドの出力 (バックアップ・デバイスに問題がある場合)
3. 発生している技術的問題について当社サポート・サービスに問い合わせた上で、以下の情報を要求します。
   - デバッグ・レベル (“1-99”など。このコマンド・オプションは後で必要になります)
   - デバッグ範囲 (クライアントのみ、Cell Manager のみ、すべてのシステム)
4. すべてのユーザー・インタフェースを終了して、セル内の他のすべてのバックアップ動作を中止します。
5. CRS または Inet デバッグも同時に収集する場合は、Cell Manager 上で CRS および Inet サービスをデバッグ・モードで再起動する必要があります

(「デバッグ」(684 ページ) を参照)。

6. Cell Manager 上で以下のコマンドを実行すると、GUI がデバッグ・モードで起動します。

   - Windows の場合 : `manager -debug 1-140 error_run.txt`
   - UNIX システムの場合 : `xomni -debug 1-140 error_run.txt`

   作成されるトレース・ファイルの名前の接尾辞には、`error_run.txt` の代わりに、ユーザーが希望する名前を定義できます。

7. Data Protector を使って問題を再現します。

8. すべての GUI を終了して、デバッグ・モードを終了します。

   CRS または Inet デバッグも同時に収集した場合は、Cell Manager 上の Data Protector サービスをデバッグ・オプションなしで再起動する必要があります (「デバッグ」(684 ページ) を参照)。

9. Cell Manager 上で次のコマンドを実行します。

   ```
   omnidlc -postfix error_run.txt
   ```

   このコマンドにより、クライアント上のログ・ファイル、getinfo ファイル、デバッグ・ファイルが圧縮され、`error_run.txt` という接尾辞がつけられます。それらはネットワーク経由で Cell Manager に送信され、現在のディレクトリの `dlc.pck` というファイルにパック、保存されます。詳細は「omnidlc コマンド」(691 ページ) を参照してください。

10. パックされたファイル (`dlc.pck`) を当社サポート・サービス宛に電子メールで送付してください。

11. Cell Manager 上で次のコマンドを実行し、クライアント上に作成されたデバッグ・ファイル (`error_run.txt` という接尾辞が付いたファイル) を削除します。

    ```
    omnidlc -postfix error_run.txt -delete_dbg
    ```

トラブルシューティング・メッセージのブラウズ

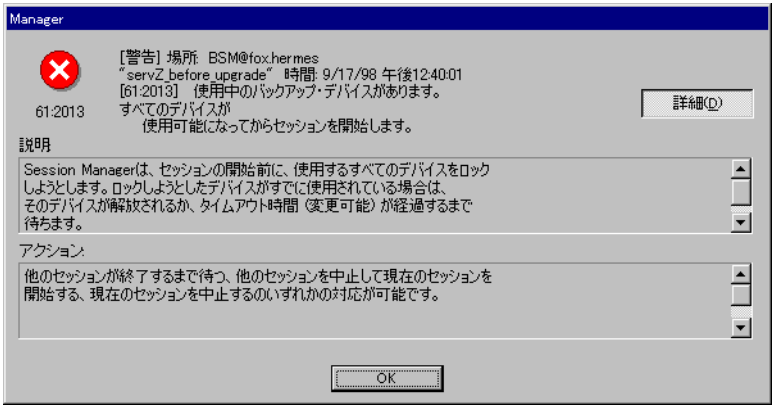
Data Protector は対話型のオンライン・トラブルシューティング・ユーティリティを備えており、それにより問題解決方法を含むエラー・メッセージの詳細情報を得ることができます。

Data Protector のエラー・メッセージが表示された場合、エラー番号はクリッカブル・リンクとして表示されています。エラーの詳細情報を見るにはそのリンクをクリックします。するとエラーに関する広範な情報を含むエラー・メッセージ・ダイアログが表示されます。[詳細] をクリックすると、エラー・メッセージの詳しい説明とエラーを解決または防止するための適切な処置が表示されます。

エラー・メッセージ・ダイアログは、以下で構成されています。

- エラー・メッセージ : 表示されるとおりのエラー・メッセージ
- 説明 : エラー・メッセージの詳しい説明
- 解決方法 : エラーを解決または防止するための処置

図 14-1　エラー・メッセージ・ダイアログの例



オンライン・トラブルシューティングにアクセスできない場合

ユーザー・インタフェースが起動できない場合は、トラブルシューティング・ファイルを使用します。このファイルはテキスト形式のファイルで、Data Protector のすべてのエラー・メッセージが記述されています。各メッセージには以下の情報が含まれています。

- メッセージ : Data Protector で表示されるとおりのエラー・メッセージ
- 説明 : エラー・メッセージの詳しい説明
- 解決方法 : エラーを解決または防止するための処置

トラブルシューティング・ファイルは、Cell Manager がインストールされているディレクトリ内だけにあります。ファイルは以下のディレクトリにあります。

- UNIX の場合 : `/opt/omni/gui/help/C/Trouble.txt`
- Windows の場合 :
  <Data_Protector_home>¥help¥enu¥Trouble.txt

エラー・メッセージの例を以下に示します。

メッセージ :
[12:5] 内部エラー (¥"p¥":num) => プロセスが中止されました。
これは予期しない状況であり、本製品とオペレーティング・システムとを取り巻く環境の組合せが原因と考えられます。

ご購入後のサポート担当までご連絡ください。

説明 :

内部エラーが発生しました。プロセスを回復できませんでした。この状態をレポートした直後に、プロセスが不正に中止しました。

解決方法 :

Data Protector の販売サポート代理店に連絡する前にできるだけ多くの情報を収集してください。

* 製品のバージョンおよびビルド番号を控えてください。
* エラーが発生した際の状況を記録しておいてください。
* セッションの出力をファイル (session.txt など) に保存してくださ

い。
* エラー発生時に関係していたすべてのホスト（VBDA、BMA、BSM などが実行されていたホスト）の *<Data_Protector_home>*/log ディレクトリに保存されているログ・ファイル（*.log）を集めてください。

一般的な問題の説明

Data Protector で問題が発生した場合、以降に示す問題の種類から一番近いものを見つけてください。

- ネットワーキングと通信 (704 ページ)
- サービスの起動 (710 ページ)
- デバイスの使用 (716 ページ)
- バックアップ / 復元セッションの開始 (724 ページ)
- ユーザー・インタフェースの起動 (742 ページ)

Data Protector の機能の中には特定のライセンス要件の制約を受けるものがあります。ライセンス設定の詳細については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

ネットワーキングと通信のトラブルシューティング

本項では、ネットワーキングと通信に関する問題について説明します。

ホスト名の解決に関する問題

ホスト名の解決に関する問題は、Data Protector 環境で最も頻繁に発生する問題です。これは、ホスト A がホスト B と通信できないことを意味します。

以下の表に、Data Protector のコンポーネントと、各コンポーネントが Data Protector 環境内でどのように通信するかを示します。ホスト間の通信とは、表のホスト A がホスト B を完全修飾されたドメイン名 (FQDN) によって解決することを意味します。ホストの解決とは、ホスト A が FQDN を解釈してその IP アドレスを識別することを意味します。

表 14-2 Data Protector 構成要素の名称解決

ホスト A	ホスト B
Disk Agent クライアント・ホスト	Media Agent クライアント・ホスト
Disk Agent クライアント・ホスト	Cell Manager ホスト
Disk Agent クライアント・ホスト	MoM サーバ・ホスト
Media Agent クライアント・ホスト	Disk Agent クライアント・ホスト
Media Agent クライアント・ホスト	Cell Manager ホスト
Media Agent クライアント・ホスト	MoM サーバ・ホスト

表 14-2 **Data Protector 構成要素の名称解決**

ホスト A	ホスト B
Cell Manager ホスト	Media Agent クライアント・ホスト
Cell Manager ホスト	Disk Agent クライアント・ホスト
Cell Manager ホスト	MoM サーバ・ホスト
MoM サーバ・ホスト	Disk Agent クライアント・ホスト
MoM サーバ・ホスト	Media Agent クライアント・ホスト
MoM サーバ・ホスト	Cell Manager ホスト

DNS の名称解決に関する問題

ホスト間の DNS 名称解決をテストするには、omnicheck コマンドを使用します。このコマンドの使用方法は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』の「Data Protector セル内の DNS 接続の確認」の項、および omnicheck の man ページを参照してください。

以下のコマンドを実行します。

```
omnicheck -dns
```

このコマンドは、通常の Data Protector 操作に必要なすべての DNS 接続を確認します。

問題

omnicheck コマンドを実行した結果、以下の応答がありました。

```
<client_1> connects to <client_2>, but connected system
presents itself as <client_3>
```

このメッセージは、*client_1* の hosts ファイルが正しく構成されていないか、*client_2* のホスト名が DNS 名と一致していない場合に出力されます。

omnicheck コマンドを実行した結果、以下の応答がありました。

```
<client_1> failed to connect to <client_2>
```

このメッセージは、*client_1* の hosts ファイルが正しく構成されていないか、*client_2* にアクセスできない（接続されていないなど）場合に出力されます。

解決方法

ネットワーク管理者に問い合わせてください。ユーザーの環境が名称解決の実行に対してどのように構成されているかによって異なりますが、この問題は、お使いの DNS 構成の中で解決するか、または以下のディレクトリにある hosts ファイルを編集するか、どちらかの方法で解決する必要があります。

- Windows の場合 : `<%SystemRoot%>¥System32¥drivers¥etc`
- UNIX の場合 : `/etc`

問題

omnicheck コマンドを実行した結果、以下の応答がありました。

<client_1> cannot connect to *<client_2>*

これは、パケットは送信されたがタイムアウトのため受信されていないことを示します。

解決方法

リモート・ホスト上でネットワークの問題が発生していないかをチェックして解決します。

TCP/IP 設定のチェック

TCP/IP 構成プロセスの重要な作業に、ホスト名解決機構のセットアップがあります。ネットワーク内の各システムは、Cell Manager のアドレスと、Media Agent と物理メディア・デバイスがインストールされたすべてのマシンのアドレスを解決できることが必要です。また Cell Manager は、セル内の全システムの名前を解決できることが必要です。

解決方法

TCP/IP プロトコルのインストール後は、ping と ipconfig ユーティリティを使って、TCP/IP 構成を検証できます。詳しい手順については、オンライン・ヘルプの索引キーワード「チェック、TCP/IP 設定」を参照してください。

HOSTS ファイルの名称解決に関する問題

解決方法

Hosts ファイルの使用時に名称解決に関する問題が発生した場合は、以下を行います。

- Windows の場合 : <%SystemRoot%>¥System32¥drivers¥etc ディレクトリの LMHosts ファイルを編集してください。
- UNIX の場合 : /etc/hosts ファイルを編集してください。

「ピアによって接続がリセットされました。」というメッセージが表示され、クライアントが異常終了する

Windows では、TCP/IP プロトコルのデフォルトの構成パラメータにより接続が切断される場合があります。このような状況が発生する原因として、ネットワークまたはコンピュータへの過大な負荷、ネットワークの信頼性の低さ、異なるオペレーティング・システムの接続などが挙げられます。

このような場合、接続が切断され、以下のエラーが表示されます。

```
[10054] Connection reset by peer.
```

解決方法

TCP/IP プロトコルを構成して、再送数をデフォルトの 5 から 8 に変更します。8 より大きい値を使用することはお勧めできません。これは、値を 1 増やすごとにタイムアウトが倍になるためです。この設定は、Data Protector が使用する接続だけでなく、すべてのネットワーク接続に適用されることに注意してください。

Windows の場合、この変更をまず Cell Manager に適用します。

UNIX Cell Manager を実行しており、上記の手順を行っても問題が解決しない場合は、問題が発生している Windows クライアントすべてに変更を適用します。

1. 以下のレジストリ・キーで、新しい DWORD パラメータ TcpMaxDataRetransmissions を追加して、値を 0x00000008(8) に設定します。

   HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Tcpip¥Parameters

   MaxDataRetries:(DWORD):8

注意

レジストリを誤って編集すると、システムが不安定になり使用できなくなる場合があります。

2. 上記の変更を行った後、システムを再起動してください。

「このクライアントは、どのセルのメンバでもありません。」というメッセージが表示されて、クライアントが異常終了する

クライアントに対して Data Protector 操作を実行したが、そのクライアント上で Cell Manager 情報が見つかりません。次のエラーが表示されて、操作は失敗します。

このクライアントは、どのセルのメンバでもありません。

解決方法

- 問題のクライアントが Data Protector GUI の [クライアント] コンテキストに一覧表示されている場合は、以下の操作を実行します。
  1. [クライアント] コンテキスト内で [クライアント] を展開して問題のクライアントを右クリックし、[削除] を選択します。
  2. [いいえ] をクリックします。
  3. [クライアント] を右クリックし、[クライアントのインポート] を選択します。
  4. クライアント名を入力して [完了] をクリックします。
- 問題のクライアントが Data Protector GUI の [クライアント] コンテキストに一覧表示されていない場合は、以下の操作を実行します。
  1. [クライアント] コンテキスト内で [クライアント] を右クリックし、[クライアントのインポート] を選択します。
  2. クライアント名を入力して [完了] をクリックします。

inet.log ファイルに過剰なログが記録される

問題

クライアントが保護されていない場合に、Cell Manager が MC/ServiceGuard 環境に構成されているか、複数の名前または IP 番号を持っていると、`inet.log` ファイルに次の種類のエントリが大量に記録される可能性があります。

```
A request 0 came from host name.company.com which is not a
cell manager of this client.
```

これは、保護されていないクライアントでは、Cell Manager のプライマリ・ホスト名しか認識できないことが原因です。他のホストからの要求も受け付けられますが、要求は `inet.log` ファイルに記録されます。

解決方法

クライアントと Cell Manager ノードに保護を設定してください。`allow_hosts` ファイルに記述されているホストからの要求は、`inet.log` ファイルに記録されなくなります。その他のホストからの要求は拒否されます。

お使いの環境で、何らかの理由によりこの対応策をとれない場合は、クライアントに保護を設定し、アクセスを許可するシステムの IP アドレス範囲に * を指定してください。この場合、クライアントはすべてのシステム (すべての IP アドレス) からの要求を受け付けるため、実際には保護されていないことになりますが、大量のログが記録される状況は回避できます。

重要

各クライアント上の `allow_hosts` ファイルには、Cell Manager ノードが使用する可能性があるすべてのホスト名を記述しておく必要があります。これにより、フェイルオーバーの発生時にもクライアントへのアクセスが可能になります。

クライアントを誤ってロックアウトしてしまった場合は、そのクライアント上の `allow_hosts` ファイルを手動で編集できます。

Data Protector サービスとデーモンのトラブルシューティング

Data Protector サービスとデーモンは、Cell Manager 上で実行されます。サービスが実行されているかどうかチェックするには、`omnisv -status` コマンドを実行します。

Data Protector サービスが終了しているか、Data Protector ターゲット・クライアント上にインストールされていないと思われる場合、まず名称解決に関する問題が発生していないか確認します。詳細については、「ネットワーキングと通信のトラブルシューティング」（704 ページ）を参照してください。

Data Protector サービスとデーモンに関して発生する可能性がある問題は、以下のように分類できます。

- 「Windows 上での Data Protector サービス起動時の問題」（710 ページ）
- 「Data Protector デーモンの起動に関する問題 (UNIX)」（712 ページ）

Windows 上での Data Protector サービス起動時の問題

サービスを起動するための権限がない

以下のエラー・メッセージが表示されます。

`Could not start the <Service_Name> on <System_Name>.`

`Access is denied.`

解決方法

システム管理者は、管理対象のシステム上でこのユーザーに対してサービスを起動 / 終了 / 変更する権限を設定することが必要です。`<%SystemRoot%>¥system32` ディレクトリの `services.msc` を管理者として実行します。この場合、Shift キーを押しながらこのファイルを右クリックして、ポップアップ・メニューから［別のユーザーとして実行］を選択し、管理者のユーザー名とパスワードを入力します。

変更されたサービス・アカウントのプロパティ

サービス・アカウントにサービスを起動するための権限がない場合、またはサービス・アカウントのプロパティ（パスワードなど）が変更されている場合、以下のエラー・メッセージが表示されます。

Data Protector Inet サービスは次のエラーのため開始できませんでした：

ログオンに失敗したため、サービスを開始できませんでした。

解決方法

1. サービスのパラメータを変更します。Windows コントロール パネルで、[管理ツール] → [サービス] を起動します。
2. 上記を行っても問題が解決しない場合は、システム管理者に連絡して、適切な権限を持つアカウントを設定するよう依頼してください。このアカウントは、[Admin] グループのメンバーである、またはユーザー権限 [サービスとしてログオン] が設定されている必要があります。

指定したサービスが見つからない

サービスが置かれているディレクトリは ImagePath キーに登録されています。実行可能ファイルがこのキーに指定されているディレクトリに存在しない場合は、以下のエラー・メッセージが表示されます。

```
Could not start the <Service_Name> on <System_Name>. The
system can not find the file specified!
```

解決方法

1. Data Protector をアンインストールする前に、Cell Manager 上で、*<Data_Protector_home>*¥db40 と *<Data_Protector_home>*¥Config ディレクトリを安全な場所にコピーします。
2. *<Data_Protector_home>*¥db40 と *<Data_Protector_home>*¥Config ディレクトリを元の場所にコピーします。
3. クライアントまたは Cell Manager のどちらかに現在インストールされている Data Protector をアンインストールし、再度インストールします。

これにより、Data Protector が正しく (クリーンな状態で) インストールされ、すべてのバイナリが適切なディレクトリに配置されます。

CRS サービスを起動すると MMD が異常終了する

Data Protector CRS サービスが起動に失敗すると、mmd.exe により診断ツール **[ワトソン博士]** が起動されます。このツールによりデータベース・ログ・ファイルの破損個所が分かります。

解決方法

1. *<Data_Protector_home>*¥tmpディレクトリにあるmmd.ctxファイルを削除すると問題は解決します。
2. omnisv -start コマンドを使ってサービスを再起動します。

Windows TSE Cell Manager 上で RDS が動作しない

<Data_Protector_home>¥db40¥datafiles¥catalog¥velocis.ini ファイルを変更して、ローカル・トランスポートの代わりに TCP トランスポートを使用します。

TCP Configuration の下の Enabled を yes に設定します。

Data Protector デーモンの起動に関する問題 (UNIX)

UNIX Cell Manager では、以下のデーモンが実行されています。

- Data Protector CRS デーモン : /opt/omni/lbin/crs
- IDB デーモン : /opt/omni/lbin/rds
- Data Protector メディア管理デーモン : /opt/omni/lbin/mmd

Data Protector Inet サービス（/opt/omni/lbin/inet）は、アプリケーションが Data Protector ポート (デフォルトのポートは 5555) へ接続しようとした場合にシステムの inet デーモンによって起動されます。

通常、これらのデーモンはシステムの起動時に自動的に起動します。

Data Protector デーモンの起動 / 終了や、デーモンのステータスの表示を手動で行うには、Cell Manager システムへルート・ユーザーとしてログインします。

デーモンの終了

Data Protector デーモンを終了するには、/opt/omni/sbin ディレクトリで以下のコマンドを実行します。

```
omnisv -stop
```

デーモンの起動

Data Protector デーモンを起動するには、/opt/omni/sbin で以下のコマンドを実行します。

```
omnisv -start
```

デーモンのステータスのチェック

Data Protector デーモンの動作ステータスをチェックするには、/opt/omni/sbin ディレクトリで以下のコマンドを実行します。

```
omnisv -status
```

Data Protector デーモンが起動に失敗する理由として以下が考えられます。

Raima Velocis サーバ・デーモンを起動できなかった

```
/opt/omni/sbin/omnisv -start

Could not start Raima Velocis server daemon.
```

解決方法

詳しくは、/var/opt/omni/server/db40/datafiles/catalog/RDS.log を参照してください。

/var/opt/omni/server/db40 ディレクトリにすべての IDB ファイルがあるか確認してください。
/opt/omni/newconfig/var/opt/omni/server/db40 にあるファイルのリストと、/var/opt/omni/server/db40 にあるファイルのリストとを比較してください。上記のディレクトリがマウントされているか確かめてください。

Raima Velocis サーバ・デーモンが実行されていないように見える

Data Protector コマンドのいずれかが以下のメッセージによって終了した場合、Raima Velocis サーバ・デーモンが実行されていない可能性があります。

```
[12:1166] Velocis デーモンのエラー - このデーモンは実行されていない可能性があります。
```

解決方法

以下のコマンドを使って、データベース・サーバが実際に実行されていないかどうかをチェックします。/opt/omni/sbin/omnisv -status

- データベース・サーバが実行されていない場合は、以下のコマンドを使ってサーバを起動します。/opt/omni/sbin/omnisv -start
- データベース・サーバが実行されている場合は、/var/opt/omni/server/db40 ディレクトリが存在しないか、一部

のファイルが不足しています。これは、上記のディレクトリまたは一部の IDB・ファイルが誤って削除されたことが原因です。IDB を復旧します。詳しくは、「IDB を復旧する」（527 ページ）を参照してください。

Data Protector Cell Manager デーモンを起動できなかった

```
/opt/omni/sbin/omnisv -start
```

```
Could not start the Cell Manager daemon.
```

解決方法

詳細については、`/var/opt/omni/tmp/omni_start.log` を参照してください。

以下の構成ファイルが存在していることを確認します。

- `/etc/opt/omni/server/options/global`
- `/etc/opt/omni/server/options/users/UserList`
- `/etc/opt/omni/server/options/ClassSpec`

Data Protector プロセス

表 14-3 に、実行されるプロセスの種類、場所、時期 (Data Protector の待機中、バックアップ / 復元 / メディア管理セッション実行中) を示します。

表 14-3 実行されるプロセスの種類、時期、および場所

	待機中	バックアップ	復元	メディア管理
Windows Cell Manager	`rds.exe`、`crs.exe`、`omniinet.exe`、`bsm.exe`	`rds.exe`、`mmd.exe`、`omniinet.exe`、`mmd.exe`	`rds.exe`、`omniinet.exe`、`mmd.exe`、`crs.exe`、`rsm.exe`	`rds.exe`、`omniinet.exe`、`mmd.exe`、`crs.exe`、`msm.exe`
UNIX Cell Manager	`rds`、`mmd`、`crs`	`rds`、`mmd`、`crs`、`bsm`	`rds`、`mmd`、`crs`、`rsm`	`rds`、`mmd`、`crs`、`msm`
Windows Disk Agent クライアント	omniinet.exe	`omniinet.exe`、`vbda.exe`	`omniinet.exe`、`vrda.exe`	omniinet.exe
UNIX Disk Agent クライアント		vbda	vrda	

表 14-3 実行されるプロセスの種類、時期、および場所

	待機中	バックアップ	復元	メディア管理
Windows Media Agent クライアント	omniinet.exe	omniinet.exe、bma.exe	omniinet.exe、rma.exe	omniinet.exe、mma.exe
UNIX Media Agent クライアント		bma	rma	mma

デバイスとメディアのトラブルシューティング

本項では、バックアップ・デバイス使用中に発生する以下の問題に対する解決策を説明します。

デバイスの SCSI アドレスに関する問題の詳細については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』の付録 B を参照してください。

Windows 上でエクスチェンジャ制御デバイスにアクセスできない

Data Protector は SCSI ミニポート・ドライバを使って、バックアップ・ドライブとライブラリを制御します。他のデバイスのドライバが同じシステムにロードされている場合、Data Protector はこれらのデバイスを管理できない場合があります。この場合、デバイスの操作 (メディアのフォーマット、またはスキャンなど) を開始した時点で、`Cannot access exchanger control device` というエラー・メッセージが表示されます。

解決方法

この場合は、デバイスがあるシステム上で *<Data_Protector_home>*¥bin¥devbra -dev コマンドを実行して、システム上で構成されているすべての物理デバイスを表示します。SCSI アドレスのいずれかのステータスが CLAIMED の場合、その SCSI アドレスは別のデバイス・ドライバが使用中です。

Windows のロボティクス・ドライバを無効にします。詳しい手順については、オンライン・ヘルプの索引キーワード「ロボティクス・ドライバ」を参照してください。

デバイスのオープンに関する問題

DDS デバイスを使おうとすると、"Cannot open device (not owner)" というエラー・メッセージが表示されます。

解決方法

Media Recognition System (メディア認識システム) と互換性のないメディアを使用していないかチェックしてください。DDS ドライブで使用するメディアは Media Recognition System と互換性がなければなりません。

Windows 上でサポートされていない SCSI HBA/FC HBA の使用

バックアップ・デバイスで、サポートされていない SCSI HBA/FC HBA を使用すると、システム・エラーが発生します。

問題が発生するのは、主に複数の Media Agent が同時に SCSI デバイスにアクセスした場合、またはデバイスのブロック・サイズによって定義されている転送データの長さが SCSI HBA/FC HBA のサポートするデータ長を上回った場合です。

解決方法

この場合は、バックアップ仕様の [拡張バックアップ・オプション] で [ブロック・サイズ] を変更できます。

サポート対象の SCSI HBA/FC HBA については、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

詳しい手順については、オンライン・ヘルプの索引キーワード「[デバイス / メディア] の拡張オプションを設定する」を参照してください。

ライブラリ再構成失敗時の自動復旧

デバイス・リストの変更後、sanconf コマンドで既存のライブラリ構成を変更しようとすると、構成エラーが報告されます。ライブラリ構成は一部しか作成されません。

SAN 環境内のホストのリストを再利用し、sanconf コマンドで再度ホストをスキャンすることで、従来のライブラリ構成を復旧できます。

解決方法

それ以降は、以下の手順を行います。

1. 次のコマンドを実行して、セル内のホストをスキャンします。

   ```
   sanconf -list_devices mySAN.txt -hostsfile hosts.txt
   ```

2. 保存した構成ファイルを使用してライブラリを構成します。次のコマンドを実行してください。

   ```
   sanconf -configure mySAN.txt -library
   <LibrarySerialNumber> <LibraryName>
   [<RoboticControlHostName>] [<DeviceTypeNumber>]
   -hostsfile hosts.txt
   ```

   正常動作していた従来のライブラリ構成が自動的に復旧されます。

その後、sanconf コマンドでライブラリ構成を追加、削除、変更する際に何らかの理由で失敗した場合は、上記の手順を実行すれば正常に動作する構成を復旧することができます。

メディア品質統計

この機能を使って、メディアに関する問題を早い段階で検出します。各メディアがドライブから取り出される前に、Data Protector は SCSI log sense コマンドを発行して、メディアの読み込み / 書き込みに関する統計情報を照会します。この情報は media.log ファイルに書き込まれます。

メディア品質統計機能はデフォルトでは無効になっています。有効にするには、グローバル・オプション・ファイルで、グローバル変数 Ob2TapeStatistics=1 を設定します。

グローバル・オプション・ファイルのパスは以下のとおりです。

- UNIX の場合 : /etc/opt/omni/server/options
- Windowsの場合: *<Data_Protector_home>*¥Config¥server¥Options

書込み操作中にメディア関連のエラーが表示された場合、またはメディアが「不良」とマークされた場合は、media.log ファイルでメディアのエラー統計を確認できます。読み込み操作中にメディア関連のエラーが表示された場合も同じです。

Media.log ファイルには以下のエラー統計が含まれています。

エラー統計	説明
errsubdel=*n*	大幅な遅延後に修正されたエラーの数
errposdel=*n*	ある程度の遅延をもって修正されたエラーの数
total=*n*	再書き込みの合計回数
toterrcorr=*n*	書き込み中に修正・回復されたエラーの合計数
totcorralgproc=*n*	修正アルゴリズムの処理時間の合計
totb=*n*	書き込み処理したバイト数の合計
totuncorrerr=*n*	未修正のエラー（書き込み）の合計数

上記で、*n* はエラーの数を示します。

パラメータの値が -1 の場合は、デバイスがその統計パラメータをサポートしていないことを表します。すべてのパラメータの値が -1 の場合は、テープ品質統計の処理中にエラーが発生したか、またはデバイスがメディア品質統計をサポートしていないことを示します。

テープの統計結果は、[処理したバイト数の合計] にバイト数でレポートされますが、これはすべてのデバイスにあてはまるわけではありません。LTO および DDS デバイスについては、バイトではなく、それぞれデータセットとグループでレポートされます。

例

以下に、media.log ファイルの内容の例をいくつか示します。

- DLT/SDLTデバイスに関するLog sense書き込みレポート ― 処理されたバイト数の合計

```
Media ID from tape= 0fa003bd:3e00dbb4:2310:0001; Medium
Label= DLT10; Logical drive= dlt1; Errors corrected no
delay= 0; Errors corrected delay= 0; Total= 13639; Total
errors corrected= 13639; Total correction algorithm
processed= 0; Total bytes processed= 46774780560; Total
```

```
uncorrected errors= 0
```

46774780560 バイト（圧縮後）のネイティブ・データが処理されました（DLT8000 テープ全体）。

- LTO デバイスに関する Log sense 書き込みレポート ― 処理されたデータセット数の合計

```
Media ID from tape=0fa003bd:3e0057e6:05b7:0001; Medium
Label= ULT2; Logical drive=ultrium1; Errors corrected no
delay= 0; Errors corrected delay= 0; Total= 0;Total errors
corrected= 0; Total correction algorithm processed= 0; Total
bytes processed= 47246; Total uncorrected errors= 0
```

1 つのデータセットのサイズは 404352 バイトです。処理されたバイト数の合計を計算するには、以下の公式を使用します。

```
47246 データセット * 404352 バイト = 19104014592 バイト（テープ全体を圧縮後）
```

- DDS デバイスに関する Log sense 書き込みレポート ― 処理されたグループ数の合計

```
Media ID from tape= 0fa0049f:3df881e9:41f3:0001; Medium
Label= Default DDS_5; Logical drive= DDS; Errors corrected
no delay= -1; Errors corrected delay= -1; Total= -1; Total
errors corrected= 0; Total correction algorithm processed=
154; Total bytes processed= 2244; Total uncorrected errors=
0
```

DDS1/2: 1 グループは 126632 バイトです。
DDS3/4: 1 グループは 384296 バイトです。

処理されたバイト数の合計を計算するには、以下の公式を使用します。

```
2244 グループ * 126632 バイト = 284162208 バイト（圧縮後）（DDS2 上での 359 MB のバックアップ）
```

359 MB のデータがバックアップされ、テープ上に 271 MB のネイティブ・データが書き込まれました。

メディア・ヘッダのサニティ・チェック

Data Protector は、メディアがドライブから取り出される前にメディア・ヘッダのサニティ・チェックを実行して、メディア・ヘッダを検証します。

メディア・ヘッダのサニティ・チェックはデフォルトで有効になっています。グローバル・オプション・ファイル内の、次の行のコメントを解除してグローバル変数を設定できます：`Ob2HeaderCheck=1`

問題

メディア・ヘッダのサニティ・チェックでメディア・ヘッダの整合性エラーが検出された場合は、エラー・メッセージが表示され、メディア上のすべてのオブジェクトに失敗のマークが付けられます。

メディア・ヘッダが破損していた場合、そのメディア上のすべてのオブジェクトに失敗のマークが付けられ、メディアの状態には不良のマークが付けられます。

解決方法

IDB からメディアをエクスポートし、別のメディアを使用して失敗したセッションを再起動します。

Data Protector A.05.50 へのアップグレード後にデバイスを使用できない

問題

Data Protector A.05.50 にアップグレードした後、従来のリリースでは別の種類のデバイスとして構成されていたデバイスが使用できない。たとえば、9840 デバイスとして構成されていた 9940 デバイスを使用できない、あるいは、DLT デバイスとして構成されていた SuperDLT デバイスを使用できない、などです。以下のエラーが発生します。

```
[Critical] From: BMA@ukulele.company.com "SDLT"  時間 :
2/22/2003 5:12:34 PM
[90:43]  /dev/rmt/1m
指定された物理デバイスの種類は無効です。> 中止しています。
```

解決方法

Cell Manager の以下のディレクトリにある mchange コマンドを使用して、手作業でこれらのデバイスを再構成します。

- HP-UX の場合 : `/opt/omni/sbin/utilns/HPUX`
- Solaris の場合 : `/opt/omni/sbin/utilns/SOL`
- Windows の場合 : `<Data_Protector_home>¥bin¥utilns¥NT`

コマンド構文

`mchange -pool PoolName -newtype NewMediaClass`

上記で

PoolName は、現在構成されているデバイスが使用していて再構成が必要なメディア・プールの名前です（Default DLT または Default T9840 など）。

NewMediaClass は、デバイスに対する新しいメディアの種類です。例：9940 デバイスの場合は T9940、SuperDLT デバイスの場合は SuperDLT など。

例

```
mchange -pool "Default DLT" -newtype "SuperDLT"
```

このコマンドは、指定したメディア・プールを使用するすべてのメディア、ドライブ、ライブラリに対するメディアの種類を変更します。変更したい各デバイスに対してこのコマンドを実行した後、再構成したデバイスに関連するメディアを、現在のメディア・プールからそれらのメディアに対応するメディア・プールに移動します。

たとえば、再構成した 9940 デバイスに関連するメディアを Default T9940 メディア・プールに移動し、再構成した SuperDLT デバイスに関連するメディアを Default SuperDLT メディア・プールに移動します。関連する手順は、オンライン・ヘルプを参照してください。

デバイスのシリアル番号に関する問題

問題

問題があるバックアップ・デバイスやロボティクスに対して何らかの操作 (バックアップ、復元、フォーマット、スキャンなど) を実行すると、以下のエラーが表示されます。

デバイス *<DeviceName>* を開くことができませんでした （ シリアル番号が変更されています)。

このエラーは、デバイス・パスが指しているデバイスのシリアル番号が、IDB に保存されている番号と異なっていることを示しています。この状況は、以下の場合に発生します。

- デバイスを正しく構成していない場合(たとえば`omniupload`コマンドの使用時など、またはデバイスファイルの構成が正しくない)。
- 物理デバイスを交換したときに、対応する論理デバイスの更新 (新しいシリアル番号の再ロード) をしなかった場合。
- マルチパス デバイス内のパスを正しく構成していない場合。

解決方法

以下の手順を実行してください。

1. Data Protector GUI で、[デバイス / メディア] コンテキストを選択します。

2. Scopingペインで [デバイス] を展開して問題のデバイスを右クリックし、[プロパティ] をクリックします。
3. 結果エリアで [コントロール] タブをクリックし、[変更された SCSI アドレスの自動検出] オプションを有効にします。
4. [再読み込み] ボタンをクリックして IDB 内のデバイス・シリアル番号を更新します。

その他頻繁に発生する問題

その他頻繁に発生する問題としてハードウェア関連の問題があります。

解決方法

システムとデバイス間の SCSI 通信 (アダプタ、または SCSI ケーブルとケーブル長など) をチェックします。OS で提供されている tar などのコマンドを実行して、システムとドライブが通信していることを検証してください。

バックアップ / 復元セッションのトラブルシューティング

バックアップ / 復元セッションの実行または起動時に発生する可能性がある問題は、以下のように分類できます。

- 「Cell Manager がクラスター内に構成されている場合に、復元に関する問題が発生する」(736 ページ)
- 「MoM Manager のアップグレード後に復元処理が失敗する」(736 ページ)

ファイル名またはセッション・メッセージが GUI で正常に表示されない

Data Protector GUI を使用する場合、非 ASCII 文字を含むファイル名やセッション・メッセージが正常に表示されない場合があります。これは、GUI でファイル名やセッション・メッセージを表示するのに、不正な文字エンコードが使用されているためです。

解決方法

これらのオブジェクトを正しく表示させるには、Data Protector GUI で [表示] メニューから [エンコード] を選択し、適切な符号化文字セットを選択します。

UNIX で GUI のエンコード切替を有効にするには、GUI を起動する前に、ロケールを UTF-8 文字エンコードを使用するロケールに設定してください。

国際化に関する制限事項の表については、オンライン・ヘルプの索引キーワード「国際化」を参照してください。

増分バックアップの代わりにフル・バックアップが実行される

増分バック・アップを指定したにもかかわらずフル・バックアップが実行される場合、以下の理由が考えられます。

前回のフル・バックアップがない

オブジェクトの増分バックアップを実行する前に、フル・バックアップを実行することが必要です。Data Protector は、どのファイルが変更され、増分バックアップに含める必要があるかを比較するベースとしてフル・バックアップを使用します。使用可能な、保護設定されたフル・バックアップがない場合は、フル・バックアップが実行されます。

解決方法

フル・バックアップの保護を設定します。

説明を変更した

バックアップ・オブジェクトは、クライアント、マウント・ポイント、説明によって定義されています。これらの値のいずれかが変更された場合、Data Protector はそのオブジェクトを新しいバックアップ・オブジェクトとみなし、増分バックアップの代わりにフル・バックアップを実行します。

解決方法

フル・バックアップと増分バックアップの両方に同じ説明を使用します。

ツリーを変更した

保護設定されたフル・バックアップが既に存在しているが、増分バックアップとはツリーが異なる。これには 2 つの理由が考えられます。

- 保護設定されたフル・バックアップに関するバックアップ仕様のツリーを変更した。
- 同一のバックアップ・オブジェクトに対して複数のバックアップ仕様を作成しているが、そのバックアップ・オブジェクトに対して異なるツリーを指定している。

解決方法

同一のバックアップ・オブジェクトに対して複数のバックアップ仕様を作成している場合は、そのバックアップ・オブジェクトの（自動生成された）共通説明を変更します。Data Protector はそれらを新しいオブジェクトとみなし、フル・バックアップを実行します。フル・バックアップの実行後は、増分バックアップが可能になります。

バックアップ・オーナーが違う

バックアップをプライベート・バックアップとして実行するよう構成されている場合、バックアップを開始したユーザーがデータのオーナーとなります。たとえば、USER_1 がフル・バックアップを実行した後、USER_2 が増分バックアップを開始しようとすると、増分バックアップではなくフル・バックアップが実行されます。これは、USER_1 のデータがプライベート・バックアップによるデータで、USER_2 が増分バックアップを実行する際のベースとしてこのデータを使用できないためです。

USER_1 がフル・バックアップを実行し、次に USER_2 がオブジェクトコピー セッションを実行してオリジナルをエクスポートまたは上書きした場合にも、同じ問題が発生します。この場合、フル・バックアップ (コピー) のオーナーは USER_2 に変わるため、USER_1 は増分バックアップを実行できなくなります。

解決方法

[バックアップ仕様オプション] の [拡張] でバックアップ・セッションの [所有権] を構成します。バックアップ・オーナーは Admin クラスのユーザーであることが必要です。これにより、バックアップ・セッションを開始したユーザーが誰であっても、このユーザーがすべてのバックアップのオーナーとなります。

予期しないスタンドアロン・デバイスのマウント要求

バックアップ・デバイス内のメディアが使用可能であるにもかかわらず、スタンドアロン・デバイスに対してマウント要求が発行された場合は、以下の状況が考えられます。

デバイス内のメディアが所属するメディア・プールのポリシーが [追加不可能] である

メディアに使用可能なスペースが残っていても、メディア・プールのポリシーが [追加不可能] なため、このメディアは使用されません。

解決方法

メディア・プールのポリシーを [追加可能] に変更して、メディアがいっぱいになるまでバックアップを追加できるようにしてください。

デバイス内のメディアがフォーマットされておらず、使用するメディア・プールのポリシーが [Strict] である

お使いのプールがメディア割当てポリシーとして [Strict] を使用している場合、未フォーマットのメディアはバックアップに使用されません。フォーマットされたメディアが使用できない場合、Data Protector はマウント要求を発行します。

解決方法

未フォーマットのメディアを Data Protector が自動的にフォーマットするようにするには、メディア・プールのポリシーを [Loose] に設定し、グローバル変数 InitOnLoosePolicy を 1 に変更します。

デバイス内のメディアがフォーマットされておらず、使用するメディア・プールのポリシーが [Loose] である

お使いのプールがメディア割当てポリシーとして [Loose] を使用している場合、メディアは自動的にフォーマットされません。

解決方法

未フォーマットのメディアを Data Protector が自動的にフォーマットするようにするには、グローバル変数 InitOnLoosePolicy を 1 に変更します。

デバイス内のメディアはフォーマットされているが、事前割当てリストで指定されているメディアと違っている

デバイス内のメディアはフォーマットされていますが、バックアップ仕様の事前割当てリストで指定されたメディアと違っています。また、指定されているメディア・プールのポリシーが [Strict] になっています。

メディアの事前割当てリストと [Strict] ポリシーを併用している場合は、バックアップの開始時に、事前割当てリストで指定されているメディアがデバイス内で使用可能になっていなければなりません。指定されたメディアが使用不可能な場合、マウント要求が発行されます。

解決方法

事前割当てリストを併用しながら、デバイス内にある使用可能なメディアを使用するには、メディア・プール割当てポリシーを [Loose] に変更します。

予期しないライブラリ・デバイスのマウント要求

ライブラリ内のメディアが使用可能であるにもかかわらず、ライブラリ・デバイスに対してマウント要求が発行された場合は、以下の状況が考えられます。

ライブラリ内のメディアがフォーマットされておらず、バックアップに使用されたメディアのメディア・プールのポリシーが [Strict] である

お使いのプールがメディア割当てポリシーとして [Strict] を使用している場合、未フォーマットのメディアはバックアップに使用されません。フォーマットされたメディアがライブラリ内で使用できない場合、Data Protector はマウント要求を発行します。

解決方法

未フォーマットのメディアを Data Protector で自動的にフォーマットし、ライブラリ内で使用可能にするには、メディア割当てポリシーを [Loose] に設定します。メディア割当てポリシーは、メディア・プールのプロパティで変更できます。

ライブラリ内のメディアはフォーマットされているが、事前割当てリストで指定されているメディアと違っている

ライブラリ内のメディアはフォーマットされていますが、バックアップ仕様の事前割当てリストで指定されたメディアと違っています。また、指定されたメディア・プールのポリシーが [Strict] になっています。

メディアの事前割当てリストと [Strict] ポリシーを併用している場合は、バックアップの開始時に、事前割当てリストで指定されているメディアがデバイス内で使用不可能な場合、マウント要求が発行されます。

解決方法

バックアップの開始時に、事前割当てリストで指定されているメディアがデバイス内で使用可能になっていなければなりません。

事前割当てリストを併用しながら、デバイス内にある他の使用可能なメディアを使うには、メディア・プール割当てポリシーを [Loose] に変更します。

事前割当てリストを使用しないで、デバイス内の使用可能な任意のメディアを使用するには、バックアップ仕様から事前割当てリストを削除します。削除するには、バックアップ仕様のバックアップ・デバイス・オプションを変更します。

予期しないマウントされたファイルシステムの検出

ディスク・イメージの復元時に、復元対象のディスク・イメージはマウントされたファイルシステムであるため復元されないというメッセージが表示されることがあります。

`Object is a mounted filesystem => not restored.`（オブジェクトはマウントされたファイルシステムです。→ 復元不能）

このメッセージは、ディスク・イメージ上のアプリケーションがディスク・イメージ上に何らかのパターンを残している場合に表示されます。このパターンが原因で、ディスク・イメージ上に最終的にマウントされたファイルシステムについて、マウントされているかどうかを検証するシステム・コールが混乱します。このため、システム・コールは、マウントされたファイルシステムがディスク・イメージ上にあると通知します。

解決方法

1. 復元を開始する前に、復元対象のディスク・イメージがある Data Protector クライアント上で、以下のコマンドを入力してディスク・イメージを削除します。

   ```
   prealloc null_file 65536
   ```

   ```
   dd if=null_file of=<device_file>
   ```

   上記で、*<device_file>* は、復元対象のディスク・イメージ用のデバイス・ファイルです。

2. 復元を開始します。

Data Protector スケジュール設定されているセッションを開始できない

スケジュール設定されたセッションが実行されない

スケジュール設定されたセッションを開始するはずの Data Protector システム・アカウントが Cell Manager 上の Admin ユーザー・グループにないため、スケジュール設定されたセッションは実行されません。

このアカウントは、インストール時に Cell Manager 上の Data Protector Admin グループに追加されます。このアカウントが変更されたり、このアカウントに対する権限が削除された場合、またはサービス・アカウントが変更された場合は、スケジュール設定されたセッションは実行されません。

解決方法

Cell Manager 上の Admin ユーザー・グループに Data Protector アカウントを追加します。

セッションが正常に行われず、Data Protector からセッション・ステータスを示すメッセージ「使用可能なライセンスがありません」が表示される

バックアップ・セッションは、Data Protector が使用可能なライセンスをチェックした後に限り開始されます。ライセンスが使用可能でない場合は、バックアップ・セッションは正常に行われず、Data Protector からセッション・ステータスを示すメッセージ「使用可能なライセンスがありません」が表示されます。

解決方法

使用可能なライセンスの情報を取得するには、omnicc -check_licenses -detail コマンドをします。詳細は omnicc のマン・ページを参照してください。

新しいライセンスを請求して、このライセンスを Data Protector システムに適用してください。ライセンスの詳細については、『*HP OpenView Storage Data Protector インストールおよびライセンス・ガイド*』を参照してください。

Data Protector のバックアップ・セッションが開始されない (UNIX の場合のみ)

解決方法

crontab -l コマンドを実行して、omnitrig プログラムが crontab ファイルに含まれているかどうかチェックします。以下の行が表示されない場合、Data Protector によって omnitrig エントリが自動的に追加されます。

```
0,15,30,45 * * * * /opt/omni/sbin/omnitrig
```

ディレクトリ /opt/omni/sbin にある omnisv -stop と omnisv -start コマンドを実行して、Data Protector デーモンの終了と再起動を行います。

Data Protector 対話型セッションを開始できない

バックアップが開始されるたびに、バックアップ・セッションを開始するための権限が必要となり、Data Protector を現在実行しているユーザーについて権限の有無がチェックされます。このユーザーが十分な権限を持っていない場合は、セッションを開始できません。

解決方法

ユーザーのユーザー権限をチェック / 変更します。詳しくは、第 4 章「ユーザーとユーザー・グループの 構成」(135 ページ) を参照してください。

Novell NetWare Server 上でのバックアップ性能が低い

Novell NetWare Server 上でのバックアップ性能が低い場合があります。バックアップが連続して実行されず、断続的に実行されます。これは既知の問題で、システムの TCPIP.NLM が原因です。

解決方法

以下のパラメータを設定します。

- NW5.1/NW6.0 の場合 : SET TCP DELAYED ACKNOWLEDGEMENT = OFF
- NW5.0 の場合 : SET TCP DELAYED ACK = OFF

これにより、他への影響なしにバックアップ性能が向上します。

Data Protector が Novell NetWare クライアント上での並行復元 Media Agent の起動に失敗する

Data Protector の UNIX Session Manager が Novell NetWare クライアント上で復元 Media Agent を並行して起動する場合、"Could not connect to inet" または "Connection reset by peer" などのメッセージを出力して失敗する場合があります。一部の並行復元セッションはエラーを出さずに正常終了して、それ以外の復元セッションが起動すらしない場合があります。

解決方法

この問題の対策として、/etc/opt/omni/server/options/global にある Data Protector グローバル・オプション・ファイル内のグローバル変数 SmMaxAgentStartupRetries を、2 以上に設定します（最大は 50）。この変数は、起動に失敗したエージェントを Session Manager が再起動するリトライ回数の最大値を指定します。Data Protector グローバル・オプション・ファイルの詳細については、「グローバル・オプション・ファイル」（645 ページ）を参照してください。

バックアップの保護期限が終了した

バックアップ・スケジュールの設定時に、フル・バックアップと増分バックアップに同じ保護期間が設定されています。つまり、増分バックアップは対応するフル・バックアップと同じ期間保護されます。このため、増分データが実際に保護されるのは、フル・バックアップの保護期限が終了する時点までとなります。この場合、保護期限が終了したフル・バックアップに基づいて実行された増分バックアップを復元することはできません。

解決方法

この問題を解決するには、増分バックアップの保護期間よりフル・バックアップの保護期間が長くなるように構成します。

このとき、フル・バックアップと増分バックアップの保護期間の差は、フル・バックアップと、次回のフル・バックアップの直前に実行される増分バックアップとの差と同じにしなければなりません。たとえば、増分バックアップを月曜日から金曜日まで実行し、フル・バックアップを土曜日に実行する場合、フル・バックアップの保護期間を増分バックアップの実行期間より長くなるよう最低でも 6 日に設定しなければなりません。これにより、最後に実行される増分バックアップの保護期限が終了するまで、フル・バックアップは保護され、使用可能となります。

アプリケーション・データベース復元のトラブルシューティング

DNS 環境の構成が不適切な場合、データベース・アプリケーションに問題を引き起こす可能性があります。データベースを復元しようとした時に、"Cannot connect to target database" または "Cannot create restore set" などのメッセージによって復元が正常に実行されなかった場合は、以下の問題が発生しています。

システム上でデータベースをバックアップする際、システム上で起動するエージェントはシステム名を *<system.company.com>* という名前でデータベースに記録します。復元セッション・マネージャは、*<system_name.company.com>* という名前で復元しようとしますが、この

システムは *<system_name.company.com>* ではなく、*<system_name>* という名前でしか認識できないため、復元できません。これは、DNS の構成が不適切なために、システム名を完全な文字列に拡張できないことが原因です。また、DNS が Cell Manager 上では構成されているがアプリケーション・クライアント上では構成されていない場合にも、同様の問題が発生します。

解決方法

TCP/IP プロトコルを設定し、DNS を適切に構成します。詳細については、『*HP OpenView Storage Data Protector インストールおよびライセンス・ガイド*』の付録 B を参照してください。

ファイル名に非 ASCII 文字が使用されている場合の問題

プラットフォームが混在した環境では、IDB が新しい内部文字エンコードにまだ変換されていない場合、Data Protector GUI における非 ASCII 文字を含んだファイル名の処理について、いくつかの制限があります。詳細は、HP OpenView Storage Data Protector インストールおよびライセンス・ガイドを参照してください。

解決方法

IDB を新しい内部文字エンコードに変換した後、クライアント上の Disk Agent をアップグレードします。

解決方法

IDB の変換を実施しない場合、バックアップまたは復元できないツリーに関する回避方法は、その上位のツリーを選択することです。この場合、この親ツリーが正常に指定されていることが必要です（その名前が ASCII 文字だけで構成されているなど）。

バックアップに関して、これはより多くのデータがバックアップされることを意味します。しかし、通常はディスク全体または少なくとも大きなツリーがバックアップされることが多いため、これは問題になりません（`/home` または `¥My Documents` など）

復元に関しては、[復元先を指定して別名で復元] または [新しいディレクトリに復元] オプションを使用して、親ツリーを新しいディレクトリに復元することができます。これにより、目的のファイルやディレクトリ以外のオブジェクトを復元することで発生し得る問題を回避できます。

復元に関して自信が持てない場合は、1 つの復元セッションごとに 1 つのツリー / ファイルを復元することをお勧めします。`"Nothing restored"` というメッセージが表示されれば、そのツリーが復元されなかったことがはっきりします。このメッセージが表示される理由は他にもあり、たとえ

ばデフォルトのファイル重複処理（最新ファイルを保存）を使用している場合、このメッセージは、そのファイルがディスク上に既に存在し、上書きされなかったことを示します。[復元先を指定] オプションを使用すると、ファイルは指定したパスに復元されます。数ファイルだけしか復元しない場合は、[復元データをリスト] オプションも使用できます。

国際化に関する制限事項の表については、オンライン・ヘルプの索引キーワード「国際化」を参照してください。

ファイル・ライブラリ・デバイスのディスクに空きスペースがない

ファイル・ライブラリ・デバイスの使用中に、以下のメッセージとともにマウント要求が発行されることがあります。

ファイル・ライブラリ *"File Library Device"* に使用できるディスク・スペースがありません。新しいディスク・スペースをこのライブラリに追加してください。

解決方法

ファイル・ライブラリが存在するディスク上の空きスペースを増やす必要があります。空きディスク・スペースは、以下のいずれかの方法で作成できます。

- ファイルのバックアップ先となるディスク上の空スペースを増やす。
- ファイル・ライブラリ・デバイスが存在するシステムにディスクを追加する。

IDB 変換後、ファイルが不正なファイル名で復元される

IDB 変換を既に実行していても、ファイルが不正なファイル名で復元されます。

解決方法

特定の Data Protector クライアントに関する IDB データが既に変換済みで、ファイル名に非 ASCII 文字が含まれている場合は、復元前にそのクライアント上の Disk Agent をアップグレードしてください。Disk Agent をアップグレードしないと、ファイルは不正なファイル名で復元されます。IDB 変換のステータスは、Data Protector GUI の [モニター] コンテキスト・リストで確認できます。

エラー・メッセージ「接続が拒否されました」が断続的に表示される

次の致命的エラーが表示されて、バックアップ・セッションが中止されます。

システム computer.company.com、ポート 40005 の Media Agent に接続できません（IPC は接続できません。）
システム・エラー：[10061] 接続が拒否されました。）

この問題は、サーバ版でない Windows 上で Media Agent が実行されており、Disk Agent の同時処理数に 5 より大きい値が設定されている場合に発生します。非サーバ版の Windows 上の TCP/IP 実装により、オペレーティング・システムが同時に受け入れられる着信接続は 5 つまでに制限されています。

解決方法

Disk Agent の同時処理数に 5 以下の値を設定してください。

バックアップ処理に頻繁に使用されるシステム (Cell Manager、Media Agent クライアント、Application Agent クライアント、ファイル・サーバなど) には、サーバ版の Windows を使用することをお勧めします。

致命的エラーが表示されて、TruCluster Server サーバ上のバックアップまたは復元が中止される

問題

次のエラー・メッセージが表示されて、バックアップ・セッションまたは復元セッションが中止されます。

("ma/xma/bma.c) 内で内部エラー => プロセスが中止されました。

これは予期しない状況であり、おもにメディアの破損か、この製品とオペレーティング・システムの両方に関係する環境の組み合わせによって発生したと予想されます。

このエラーは、以下のいずれかの状況で発生します。

- バックアップに使用されたバックアップ・デバイスが、クラスターの仮想サーバ上に構成されている。
- バックアップ対象のファイルシステムがクラスターの仮想サーバ上に存在している。

解決方法

TruCluster Server 上に以下の omnirc 変数を設定してください。

- OB2BMANET=1

- OB2RMANET=1
- OB2RDANET=1
- OB2BDANET=1

omnirc ファイルの詳細は、「omnirc オプションの使用」（647 ページ) を参照してください。

Cell Manager がクラスター内に構成されている場合に、復元に関する問題が発生する

問題

クラスター対応の Data Protector Cell Manager で、バックアップ・オプション [すべてのオブジェクトのバックアップを再開] を有効にして、バックアップを実行した場合を考えてみましょう。このバックアップ中にフェイルオーバーが発生し、別のクラスター・ノード上でバックアップ・セッションが再開されて、処理は正常に終了したとします。その後、最新のバックアップからの復元を試みたときに、セッションは正常に終了しているにもかかわらず、次のエラーが表示されることがあります。

正常に完了していないバージョンが選択されています。このようなバックアップを復元すると、一部またはすべてのファイルが正しく復元されない可能性があります。

Cell Manager クラスター・ノード間でシステム時刻の同期がとられていないと、失敗したバックアップのタイムスタンプが、再開されたバックアップのタイムスタンプよりも新しい可能性があります。復元するデータの選択時には、デフォルトで最新のバックアップ・バージョンが選択されるため、この場合は失敗したバックアップからの復元が行われてしまいます。

解決方法

正常に終了した最新のバックアップから復元するには、復元に使用する正しいバックアップ・バージョンを選択してください。このようなエラーを防止するため、ネットワーク上にタイム サーバを構成することをお勧めします。これにより、Cell Manager クラスター・ノード間でシステム時刻の同期が自動的にとられます。

MoM Manager のアップグレード後に復元処理が失敗する

問題

以下のエラー・メッセージが表示されます。「不明な内部エラーです。起動された Session Manager は不正なオプションを受け取りました。」または「Cannot get information from backup host.」

MoM Manager/CMMDB サーバを Data Protector A.05.50 にアップグレードすると、以前の Data Protector クライアントのファイルシステムまたは統合ソフトウェアの**復元**を、Data Protector A.05.50 MoM GUI から実行できなくなります。

解決方法

以前のバージョンの MoM GUI を使用して復元するか、クライアントを Data Protector A.05.50 にアップグレードしてください。

オブジェクトコピー セッションのトラブルシューティング

オブジェクトコピー セッションの実行中に、以下の問題が発生する可能性があります。

コピーされたオブジェクトの数が想定された数より少ない

バックアップ後オブジェクトコピーまたはスケジュールされたオブジェクトコピーの実行時に、実際にコピーされたオブジェクトの数が、選択したフィルタに合致したオブジェクトの数よりも少ないことがあります。

以下のメッセージが表示されます。

指定したフィルタに一致するオブジェクトの数が多すぎます。

解決方法

- オブジェクト・バージョンの選択基準を厳しくする。
- グローバル・オプション・ファイル内の CopyAutomatedMaxObjects 変数の値を大きくして、同一セッション内でコピーされるオブジェクトの最大数を増やす。

選択したライブラリ内の一部のオブジェクトしかコピーされない

バックアップ後オブジェクトコピーまたはスケジュールされたオブジェクトコピーの実行時に、選択したライブラリ内のメディア上にあるオブジェクトの一部がコピーされないことがあります。この問題は、選択したライブラリ内に、そのオブジェクトのメディア・セットの一部しか含まれていないことを示しています。

解決方法

不足しているメディアを選択したライブラリに挿入するか、または、問題のオブジェクトの完全なメディア・セットを含んでいるライブラリを選択してください。

追加のメディアに対するマウント要求が発行される

メディアを始点とする対話型オブジェクトコピー セッションで、特定のメディアを選択したとします。このとき、追加のメディアに対するマウント要求が発行されることがあります。この問題は、そのメディア上に存在するオブジェクトが、ほかのメディアにもまたがっていることを示しています。

解決方法

要求されたメディアをデバイスに挿入して、マウント要求に応答してください。

Data Protector インストールのトラブルシューティング

Data Protector ソフトウェアのインストール時に問題が発生した場合、システムのログ・ファイル (UNIX) または設定ログ・ファイル (Windows) をチェックして、問題を調べます。

システム	ログ・ファイル
UNIX (ローカル・インストール)	/var/adm/sw/swinstall.log /var/adm/sw/swagent.log
UNIX (リモート・インストール)	/var/opt/omni/log/IS_install.log
Windows (ローカル・インストール)	<*System_disk*>:¥<*Temp*>¥OB2_Setup_ui_<*Date*>_<*Time*>.txt
Windows (リモート・インストール)	<*System_disk*>:¥<*Temp*>¥OB2_Setup_exe_<*Date*>_<*Time*>.txt

設定ログ・ファイルが作成されない場合、-debug オプションを付けてインストールを実行します。

Windows クライアントのリモート・インストール時の問題

Data Protector のリモート・インストール機能を使って Windows クライアントを更新する場合、以下のエラーが発生します。

```
Error starting setup process, err=[1326] Logon failure:
unknown user name or bad password.
```

インストール・サーバがインストールされているコンピュータ上の OmniBack II 共有部分にアクセスする権限のないユーザー・アカウントで、リモート・コンピュータ上の Data Protector Inet サービスが実行されていると、この問題が発生します。ほとんどの場合、ローカル・ユーザーに原因があります。

解決方法

Data Protector Inet サービスのユーザー名を、OmniBack II 共有部分へのアクセス権を持つユーザー名に変更します。

Windows Cell Manager インストール時の名称解決の問題

Windows 上に Data Protector Cell Manager をインストールしている最中に、DNS または LMHOSTS ファイルが要求どおりに設定されていないことが、Data Protector によって検出された場合、警告が表示されます。さらに、TCP/IP プロトコルがシステム上にインストールされていない場合、Data Protector によって通知されます。

DNS または LMHOSTS 使用時に名称解決が失敗する

名称解決が失敗した場合、`"error expanding hostname"` メッセージが表示され、インストールは中止されます。

- DNS の使用時に名称解決に関する問題が発生した場合は、現在の DNS 構成について警告メッセージが表示されます。
- LMHOSTS ファイルの使用時に名称解決に関する問題が発生した場合は、LMHOSTS ファイル構成について警告メッセージが表示されます。
- DNS または LMHOSTS のどちらも構成していない場合は、TCP/IP プロパティ・ダイアログで、DNS または LMHOSTS 名称解決を可能にすることを促す警告メッセージが表示されます。

解決方法

DNS または LMHOSTS ファイルの構成をチェックまたはアクティブ化します。詳しくは、「ホスト名の解決に関する問題」（704 ページ）を参照してください。

システム上で TCP/IP プロトコルのインストールと構成が行われていない

システム上で TCP/IP プロトコルのインストールと構成が行われていない場合、インストールは中止されます。

Data Protector はネットワークの通信に TCP/IP プロトコルを使用します。TCP/IP プロトコルは、セル内のすべてのクライアントにインストールおよび構成されている必要があります。

解決方法

TCP/IP 設定をチェックします。詳しい手順については、オンライン・ヘルプの索引キーワード「チェック、TCP/IP 設定」を参照してください。

ユーザー・インタフェースのトラブルシューティング

本項では、Data Protector グラフィカル・ユーザー・インタフェース（GUI）使用中に発生する以下の問題に対する解決策を説明します。

UNIX 上の Data Protector GUI で GUI オブジェクトの名前が正常に表示されない

問題

UNIX 上の Data Protector GUI で、GUI オブジェクト（バックアップ・デバイスやバックアップ仕様など）の名前が正常に表示されません。

GUI オブジェクトがあるロケールの下で作成されている場合、異なるロケールではオブジェクト名が正常に表示されない場合があります。GUI オブジェクトの名前が正しく表示されていなくても、それらの GUI オブジェクトを使用することは可能です。

たとえば、非 ASCII 文字を使用してバックアップ・デバイスを構成し、名前をつけた場合、ASCII 文字だけを使用するロケールで GUI を実行するとデバイス名は正しく表示されません。しかし、GUI でデバイス名が正しく表示されていなくても、そのデバイスを使用してバックアップや復旧を実行することができます。

解決方法

それらのオブジェクトを、UTF-8 エンコードを使用するロケールで作成し直すか、Data Protector GUI が実行されているシステムの従来のロケールをそのまま使用してください（ただしこの場合は、GUI でエンコードを切り替えることはできず、従って Data Protector の国際化機能も使用できません）。

ユーザー・インタフェースの起動に関するトラブルシューティング

Data Protector ユーザー・インタフェースの起動に関する問題が発生する原因は通常、サービスが実行されていない、サービスがインストールされていない、またはネットワーク通信の問題が発生している、のいずれかです。

Cell Manager 上で inet が応答しない

以下のメッセージが表示されます。

Cannot access the system (inet is not responding). The Cell Manager host is not reachable, is not up and running, or has no Data Protector software installed and configured on it. （システムにアクセスできません（inet が応答しません）。Cell Manager ホストがアクセス不能、または起動・稼動していない、または Cell Manager への Data Protector ソフトウェアのインストールと構成が行われていません。

解決方法

システム間の通信に問題がない場合は、telnet を使ってソフトウェアがインストールされているかチェックしてください。

一部のコンポーネントがインストールされていないか、または正しくインストールされていない可能性があります。インストール手順については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』参照してください。

インストールに問題がない場合は、omnisv -status コマンドを実行して、Cell Manager 上でサービスが正常に実行されているかチェックしてください。

Cell Manager にアクセスする権限がない

以下のメッセージが表示されます。

Data Protector 管理者によって、ユーザー権限が Data Protector の機能にアクセスできないように設定されています。

詳細は Data Protector 管理者に問い合わせてください。

解決方法

Data Protector 管理者に、ユーザーとして追加することと、セル内での適切なユーザー権限の付与を要請します。詳しくは、第 4 章「ユーザーとユーザー・グループの 構成」(135 ページ) を参照してください。

Windows または Novell NetWare 上でリモート・システムへの接続が拒否された

telnet <*hostname*> 5555 コマンドを実行した結果、「接続が拒否されました」という応答がありました。

解決方法

Data Protector Inet サービスがリモート・システム上で実行されていない場合は、omnisv -start コマンドを実行して、サービスを起動します。

Data Protector がリモート・システム上にインストールされていない場合、リモート・システム上に Data Protector をインストールします。

IDB のトラブルシューティング

本項では、IDB 使用中の以下の問題に対するトラブルシューティングについて説明します。

バックアップ中にファイル名が IDB に記録されない

Data Protector を使用してバックアップを実行したとき、ファイル名が IDB に記録されません。

解決方法

バックアップ・オプションとして、[ログなし] を選択していないか確認してください。

Windows Cell Manager 上でファイル名が IDB に記録されない原因としては、バックアップ中に IDB 内のファイル名変換が実行中であったことも考えられます。この場合、そのバックアップは [ログなし] オプションで実行されているため、そのセッションのそのクライアントに関しては、IDB に何のデータも書き込まれていません。警告が出ていないか、そのバックアップ・セッションのセッション・メッセージを確認することができます。

ユーザー・インタフェース実行時の問題

IDB が破損している

以下のいずれかのメッセージが表示されることがあります。

- `Database is corrupted.`
- プロセス間通信エラー
- データベース / ファイルをオープンできません。
- エラー - 詳細は不明

解決方法 IDB を復旧します。詳細は、「IDB を復旧する」(527 ページ) を参照してください。

IDB の Session Manager が Cell Manager 上で実行されない

Data Protector が IDB にアクセスまたは使用しようとした時に、IDB の Session Manager が Cell Manager 上で実行されていない場合、「プロセス間通信エラー」メッセージが表示されます。

- Windows Cell Manager の場合、Data Protector プロセス `dbsm.exe` は Windows タスク・マネージャ内のプロセスとして表示されません。
- UNIX Cell Manager の場合、`ps -ef | grep omni` コマンドを使って Data Protector プロセスをリストすると、`/opt/omni/lbin/dbsm` は表示されません。

解決方法 Data Protector GUI を終了し、再起動します。

ライブラリ (実行可能ファイル) が見つからない

Windows Cell Manager の場合、以下のライブラリ・ファイルが *<Data_Protector_home>*¥bin ディレクトリに置かれていなければなりません。

- `libob2ecmn.dll`、`libob2eadm.dll`、`libob2ecdb.dll`、`libob2emmdb.dll`、`_eadm32.dll`、`_erdm32.dll`

UNIX Cell Manager の場合、以下のライブラリ・ファイルが `/opt/omni/lib` ディレクトリに置かれていなければなりません。

- `libob2ecmn.sl`、`libob2eadm.sl`、`libob2ecdb.sl`、`libob2emmdb.sl`、`_eadm.sl`、`_erdm.sl`

RDS サービス / プロセスが起動できない

1 つまたは複数の共有ライブラリ・ファイルが見つからない場合、`omnisv -status` コマンドを実行すると、他のサービス / プロセスがすべて動作しているのに RDS サービス / プロセスだけが動作していないことが通知されます。

解決方法

Data Protector を再インストールし、Cell Manager を再起動します。これにより、共有ライブラリが再インストールされ、RDS サービス / プロセスが再起動されます。

データ・ファイル (ディレクトリ) が見つからない

以下の IDB データ・ファイル (ディレクトリ) が、以下のディレクトリに置かれている必要があります。*<Data_Protector_home>*¥db40 (Windows Cell Manager の場合)、または /var/opt/omni/server/db40 (UNIX Cell Manager の場合)

- datafiles¥catalog
- datafiles¥cdb
- datafiles¥mmdb
- dcbf
- logfiles¥rlog
- logfiles¥syslog
- meta
- msg

1 つまたは複数の IDB データ・ファイルまたはディレクトリが見つからない

Data Protector が IDB にアクセスまたは使用しようとした時に、1 つまたは複数の IDB データ・ファイルまたはディレクトリが見つからない場合、以下のエラーが表示されます。

- データベースのネットワーク通信エラー
- データベース / ファイルをオープンできません。

解決方法

Data Protector を再インストールし、Cell Manager を再起動します。これにより、IDB データ・ファイルとディレクトリが再インストールされます。

一時ディレクトリが見つからない

Cell Manager 上に以下の一時ディレクトリが置かれている必要があります。

- Windows の場合 : *<Data_Protector_home>*¥tmp
- UNIX の場合 : /var/opt/omni/tmp

Data Protector GUI が Cell Manager に接続できない

Data Protector GUI が Cell Manager に接続しようとした時に、Data Protector の一時ディレクトリが見つからない場合、以下のエラー・メッセージが表示されます。

システムにアクセスできません（inet が応答しません）。Cell Manager ホストがアクセス不能、または起動・稼動していない、または Cell Manager への Data Protector ソフトウェアのインストールと構成が行われていません。

解決方法

1. Data Protector GUI を終了します。
2. Cell Manager 上で omnisv -stop コマンドを実行し、Data Protector サービス / プロセスを終了します。
   - Windows の場合 : *<Data_Protector_home>*¥bin¥omnisv -stop
   - UNIX の場合 : /opt/omni/sbin/omnisv -stop
3. Cell Manager 上に一時ディレクトリを手動で作成します。
   - Windows の場合 : *<Data_Protector_home>*¥tmp
   - UNIX の場合 : /var/opt/omni/tmp
4. omnisv -start コマンドを実行してサービス / プロセスを起動します。
   - Windows の場合 : *<Data_Protector_home>*¥bin¥omnisv -start
   - UNIX の場合 : /opt/omni/sbin/omnisv -start

5. Data Protector GUI を再起動します。

バックアップおよびインポート時の問題

IDB のバックアップまたはインポート・セッション中に、BSM または RSM が強制終了する

IDB のバックアップまたはインポート・セッション中に、BSM または RSM が強制終了する場合、以下のエラー・メッセージが表示されます。

```
IPC Read Error System Error: [10054] Connection reset by peer
```

[内部データベース] のコンテキストで、IDB バックアップまたはインポート・セッションのセッション・ステータスが、セッションが実際には実行中でないにもかかわらず、[実行中] と表示されます。

解決方法

1. Data Protector GUI を終了します。
2. `omnidbutil -clear` コマンドを実行し、実際には実行中でないが [実行中] または [失敗] と表示されているすべてのセッションのステータスを、[失敗] に設定します。
3. `omnidbutil -show_locked_devs` コマンドを実行し、Data Protector によってロックされているデバイスやメディアがないか調べます。
4. ロックされたものがある場合は、`omnidbutil -free_locked_devs` コマンドを実行して、ロックを解除します。
5. Data Protector GUI を再起動します。

IDB バックアップまたはインポート・セッション中に、MMD が強制終了する

IDB バックアップまたはインポート・セッション中に、メディア管理デーモン (MMD) が強制終了する場合、以下の 2 つのエラー・メッセージが表示されます。

- `Lost connection to MMD`
- `IPC Read Error System Error: [10054] Connection reset by peer`

以下の方法で、MMD サービス / プロセスが実行中でないか確認します。

- `omnisv -status` コマンドを実行すると、MMD サービス / プロセスが動作していないことが通知されます。
- UNIX の場合、`ps -ef | grep omni` コマンドを使って Data Protector プロセスをリストすると、Data Protector MMD(`/opt/omni/lbin/mmd`) は表示されません。

  Windows の場合、Data Protector MMD プロセス (`mmd.exe`) は Windows タスク・マネージャ内のプロセスとして表示されません。

解決方法

1. Data Protector GUI を終了します。
2. `omnisv -stop` コマンドを実行して Data Protector サービス / プロセスを停止します。
3. `omnisv -start` コマンドを実行して Data Protector サービス/プロセスを起動します。
4. `omnisv -status` コマンドを実行して、サービス / プロセスがすべて実行中かどうかチェックします。

DC バイナリ・ファイルが破損または見つからない

DC バイナリ・ファイルが破損または見つからないと、[復元] コンテキストでバックアップ・オブジェクトをブラウズする時に、エラー・メッセージ「詳細カタログ・バイナリ・ファイルのオープンに失敗しました」が表示されます。

- `omnidbcheck -bf` コマンドを実行すると、1 つまたは複数の DC バイナリ・ファイルが見つからないか、サイズが不適切であることが通知されます。`omnidbcheck -dc` コマンドを実行すると、1 つまたは複数の DC バイナリ・ファイルが破損していることが通知されます。
- Cell Manager 上の *<Data_Protector_home>*`¥log¥debug.log` (Windows システムの場合) または `/var/opt/omni/log/debug.log` (UNIX システムの場合) にある `debug.log` ファイルには、Data Protector が DC バイナリ・ファイルをオープンできないことを示す 1 つまたは複数のエントリが記録されます。

解決方法

メディアからカタログをインポートして、DC バイナリ・ファイルを再作成します。詳細については、「DCBF パートの [軽度] レベルのデータベース破損に対処する」(531 ページ) を参照してください。

性能に関する問題

IDB オブジェクトの数とサイズが大きすぎる

復元対象のオブジェクト・バージョンおよび個々のファイルをブラウズする場合、IDB から情報が読み込まれて表示されるまでに時間がかかることがあります。

解決方法

復元対象のオブジェクト・バージョンをブラウズする時に使用される時間間隔を設定します。この時間間隔は、[復元] コンテキストで復元の対象となる特定のオブジェクト・バージョンを検索する際に変更できます。

復元対象のオブジェクト・バージョンをブラウズする際に**デフォルトの**時間間隔を設定します。

1. Data Protector GUI で [ファイル] メニューをクリックし、続いて [選択値] をクリックします。
2. [復元] タブをクリックします。[検索インターバル] ドロップダウン・リストから検索間隔を選択します。検索間隔を絶対値で設定したい場合は [間隔] を選択し、すべてのオブジェクト・バージョンをリストに表示したい場合は [なし] を選択します。
3. [OK] をクリックして変更内容を適用します。

IDB のスペースが不足している場合

IDB のスペースが不足しています。[IDB のスペース不足] または [IDB テーブル・スペースのスペース不足] 通知が発行されます。

解決方法

IDB のサイズを拡張します。詳細は、「IDB のサイズを拡大する」（517 ページ) を参照してください。.

MMDB と CDB の非同期

MMDB と CDB の非同期は、以下の場合に発生する可能性があります。

- MMDB と CDB に異なる時点で得られた情報が格納されている場合。別々のエクスポート・セッション (`omnidbutil -readdb` コマンド) で作成されたファイルから `omnidbutil -writedb` コマンドで CDB と MMDB をインポートすると、このような差異が生じる可能性があります。

- MoM 環境でローカル CDB と CMMDB の同期が取られていない場合。CMMDB を復元すると、このような問題が発生する可能性があります。

Data Protector は、IDB 内のオブジェクトにメディアが割り当てられていない、またはメディアに対するデータ保護が正しく設定されていない場合に、それを通知します。

解決方法

セルが 1 つの環境の場合 :

- `omnidbutil -cdbsync <Cell_Server_Hostname>` コマンドを実行して、MMDB と CDB の同期を取ります。このコマンドは、`/opt/omni/sbin` ディレクトリ (UNIX Cell Manager の場合) または `<Data_Protector_home>¥bin` ディレクトリ (Windows Cell Manager の場合) にあります。

MoM 環境の場合 :

- `omnidbutil -cdbsync <Cell_Server_Hostname>` コマンドを、CMMDB がインストールされた (MoM の) `/opt/omni/sbin` ディレクトリ (UNIX Cell Manager) または `<Data_Protector_home>¥bin` ディレクトリ (Windows Cell Manager) で実行します。このコマンドは、MoM 環境内の各 Cell Manager に対して実行します。実行時には、対象となる Cell Manager のホスト名を引数として指定します。

IDB における削除処理の性能に関する問題

問題

IDB からファイル・バージョンを削除する処理が極めて遅い。

解決方法

現在の削除セッションに関して、次のメッセージが `<Data_Protector_home>¥log¥server¥purge.log` ファイルに記録されていないか確認します。

```
Multiple passes needed. This will decrease the performance
of the purge session. To improve performance increase the
amount of memory a purge session is allowed to use.
```

ログ・ファイルに上記のメッセージが記録されている場合は、セッションを中止し、グローバル・オプション・ファイル内の `PurgeBufferSize` オプションの値を増やします。グローバル・オプション・ファイルの編集方法に関しては、「グローバル・オプション・ファイル」(645 ページ) を参照してください。その後、削除セッションを再起動します。

HP-UX 上でメモリ割り当て問題により IDB 操作が失敗する

問題

メモリ割り当て問題が原因で、IDB の保守または照会中に、HP-UX 上で RDS サービスが失敗します。

解決方法

以下の手順を実行してください。

1. Cell Manager 上の `omnirc` ファイルに、環境変数 `_M_ARENA_OPTS=1:32` を設定します。詳細は、「omnirc オプションの使用」（647 ページ) を参照してください。
2. Data Protector サービスを再起動します。詳細は、`omnisv` の man ページを参照してください。

レポートと通知に関するトラブルシューティング

Outlook XP または Outlook 98/2000 に最新のセキュリティ・パッチを適用して使用している場合、以下の問題が発生する可能性があります : レポート・グループにレポートを追加するとき、送信方法として電子メールを指定して、レポート・グループを起動しようとすると、GUI がハングする。通知の構成で電子メールによる送信を選択した場合も同じ現象が発生します。この問題の原因は、Outlook が電子メールによる通知を送信する前に、ユーザーによる対話型操作を要求するからです。この機能は Outlook のセキュリティ・ポリシーの一部であるため、無効にできません。問題を解決するには、CLI からレポートを起動してください。

```
omnirpt -report licensing -email <email_address>
```

Outlook による電子メールの送信を許可するかを尋ねる警告メッセージが表示されたら、[はい] をクリックして、通知を受信します。

セキュリティ設定方法の詳細は、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

Data Protector オンライン・ヘルプのトラブルシューティング

Data Protector のオンライン・ヘルプは、ヘルプ・トピックとヘルプ・ナビゲータの 2 つの部分で構成されています。ヘルプ・ナビゲータはコンテキスト依存のヘルプで、Data Protector GUI に表示される画面やオプションの説明が表示されます。一方、ヘルプ・トピックでは概念や手順、例などが表示されます。

ヘルプ・システムは、Data Protector を実行しているプラットフォーム (Windows または UNIX) に依存します。Windows では HTML ヘルプが、UNIX では WebHelp が使用されます。

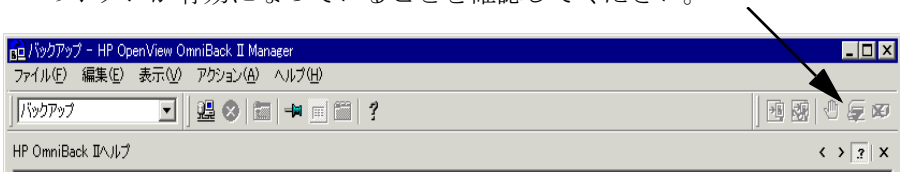
Windows 上でのオンライン・ヘルプのトラブルシューティング

Windows システムでオンライン・ヘルプを使用する場合、ヘルプ・ナビゲータの表示で以下の問題が発生する場合があります。

Data Protector のウィンドウを別のウィンドウに切り替えても、それに合わせて、ヘルプ・ナビゲータの内容が変わらない。

解決方法

1. Microsoft HTML ヘルプモード (デフォルト) を使用している場合、以下のボタンが有効になっていることを確認してください。



2. デフォルトの HTML ブラウザモード (外部 HTML ブラウザでヘルプ・ファイルを表示) を使用している場合、[ファイル] メニューから [選択値] をクリックし、チェック・ボックスに印をつけて [状況依存のヘルプ・ナビゲータを使用可能にする] オプションを有効にします。その後、ヘルプ・ナビゲータを再起動します。

UNIX 上でのオンライン・ヘルプのトラブルシューティング

お使いのブラウザ (HTML ビュアー) が正しく設定されていない場合、オンライン・ヘルプの起動と表示で問題が発生する場合があります。ブラウザを以下のとおり設定してください。

解決方法

1. [ファイル] メニューで [選択値] をクリックします。Netscape Navigator を使用している場合は、ドロップダウン・リストから [Netscape] を選択します。Netscape Navigator 以外を使用している場合は、[カスタム] を選択します。

重要

Data Protector は、オンライン・ヘルプの表示用に Netscape Navigator のみをサポートしています。

2. [設定] をクリックして、[HTML ビューアの設定] ウィンドウを開きます。
3. [実行可能スクリプトまたはバイナリ・ファイルの位置] テキスト・ボックスに、お使いのブラウザがあるディレクトリ (例 : /opt/netscape) を入力します。
4. [ビューアの起動コマンド] テキスト・ボックスに、ブラウザを起動するコマンドを入力します。Netscape Navigator の場合には、netscape $HTML$ と入力します。
5. [既存ビューア・ウィンドウの再使用コマンド] テキスト・ボックスに、各 HTML ファイルを同じウィンドウで開く時に使用するコマンドを入力します。ここに何も入力しない場合、各 HTML ファイルは別のウィンドウで表示されます。Netscape Navigator の場合、このコマンドは、netscape -remote OpenFile($HTML$) です。

Data Protector が適切に作動しているかチェックする方法

以降の項では、Data Protector のチェックと保守機構の概要、およびバックアップ環境で Data Protector が適切に構成されているかどうかを判別するためのチェック項目の概要を説明します。

Data Protector のチェック / 保守機構

Data Protector には独自のチェックと保守機構があり、以下のチェック / 保守作業を毎日行っています。

保守作業

- 古くなった DC バイナリ・ファイル、セッション、関連するメッセージをデフォルトでは毎日 12 時 (正午) に削除します。
- [フリー・プールを使用] と [フリー・メディアをフリー・プールに移動] オプションを設定して、プールにある (保護されていない) フリー・メディアを見つけます。以下のコマンドをデフォルトでは毎日 12 時 (正午) に実行して、見つけたフリー・メディアのフリー・プールへの割り当てを取り消します。

  ```
  omnidbutil -free_pool_update
  ```

  omnidbutil コマンドの詳細については、omnidbutil man ページを参照してください。上記のオプションについての詳細は、第 5 章「メディアの管理」(151 ページ) を参照してください。

チェック

デフォルトでは毎日午後 12 時 30 分に、以下の Data Protector 通知のチェックを開始します。

- [IDB のスペース不足]
- [IDB テーブル・スペースのスペース不足]
- [フリー・メディア不足]
- [健全性チェックの失敗]
- [ユーザー・チェックの失敗]
- [予期しないイベント]

- [ライセンス期限切れ]
- [IDB の削除必要]

ライセンスのチェック

デフォルトでは毎日午後 12 時 30 分に、Data Protector は Data Protector ライセンスをチェックし、ライセンスが見つからない、あるいは期限切れの場合、Data Protector イベント・ログにそれをレポートします。

Data Protector 通知の詳細については、「Data Protector 通知」(445 ページ) を参照してください。トリガされる通知は、デフォルトではすべて Data Protector イベント・ログに送信されます。Data Protector イベント・ログの詳細については、「Data Protector イベント・ログ」(461 ページ) を参照してください。

Data Protector グローバル・オプション・ファイル内の `DailyMaintenanceTime` オプションと `DailyCheckTime` オプションを変更することで、保守作業とチェックについてデフォルトのスケジュール値を変更できます。グローバル・オプションの詳細については、「グローバル・オプション・ファイル」(645 ページ) を参照してください。

[ユーザー・チェックの失敗] 通知

[ユーザー・チェックの失敗] 通知により、バックアップ環境が正常に機能しているかどうかをチェックするタスクを自動化できます。「正常」の定義はバックアップ環境 (バックアップ・ポリシー、ネットワーク構成、使用されているハードウェアなど) により異なることに注意してください。「平均的」バックアップ環境でのチェック項目の概要については、「チェックする項目の概要」(759 ページ) を参照してください。Data Protector 通知の詳細については、「Data Protector 通知」(445 ページ) を参照してください。

[ユーザー・チェックの失敗] 通知により、入力パラメータとしてこの通知に入力されたコマンドまたはスクリプトが実行されます。実行されたコマンドの戻り値、またはスクリプト内の実行されたコマンドの戻り値が 0 (ゼロ) 以外であれば、通知がトリガされます。コマンド / スクリプトは、アプリケーション・システムの `/opt/omni/lbin` ディレクトリ (UNIX システムの場合) または *<Data_Protector_home>*¥`bin` ディレクトリ (Windows システムの場合) に作成する必要があります。 [ユーザー・チェックの失敗] 通知は、トリガされた時に、さまざまな送信方法 (電子メール、ブロー

ドキャスト・メッセージ、SNMP トラップ、ログ・ファイルなど) を使って送信されるように構成できます。またトリガされた時にレポート・グループを開始するように構成することも可能です。

このように、バックアップ環境に応じて指定されたチェックを含むスクリプトを、[ユーザー・チェックの失敗] 通知の中で作成し、構成することができます。Data Protector では、バックアップ環境で問題が発生した場合、保守 / チェック機構を使ってユーザーに通知されます。

構成済み [ユーザー・チェックの失敗] 通知は、デフォルトではすべて、毎日 0 時 (深夜) に開始されるようにスケジュールされています。トリガされた場合は、Data Protector イベント・ログに送信されます。

チェックする項目の概要

Data Protector が適切に作動しているか確認し、問題の発生前にその可能性を特定するため、以降の項で説明する定期的なチェックを実施することをお勧めします。

[ユーザー・チェックの失敗] 通知を使って、これらのチェックを含むスクリプトを作成することで、これらのチェックを自動化できます。一部のチェック (`omnihealthcheck` や `omnitrig -run_checks` コマンドなど) は、Data Protector のチェック / 保守機構によってすでに自動化されています。

Data Protector Cell Manager をチェックする

1. `omnihealthcheck` コマンドを実行して、以下をチェックします。

   - Data Protector サービス (`rds`、`crs`、`mmd`、`omnitrig`、および `OmniInet`) がアクティブになっているか。
   - Data Protector メディア管理データベースの整合性が維持されているか。
   - IDBのバックアップが1つ以上存在するか。終了コードが0以外の場合は、失敗したチェックがあるということを示します。

   このコマンドの終了コードが 0 (OK) になるのは、3 つのチェックがすべて正常に完了した場合 (つまり、すべてのチェックの終了コードが 0 になった場合) だけです。

   終了コードの詳細については、`omnihealthcheck` man ページを参照してください。

2. omnidbcheck -core コマンドを実行し、IDB のコア・パートをチェックします。

   このコマンドの終了コードが 0 (OK) になるのは、チェックが正常に完了した場合だけです。終了コードが 0 以外の場合は、チェックが失敗したことを示します。

   終了コードの詳細については、omnihealthcheck man ページを参照してください。

3. omnidbcheck -critical コマンドを使って、IDB のコア・パートをチェックします。omnidbcheck コマンドの詳細については、omnidbcheck man ページを参照してください。

   このコマンドの終了コードが 0 (OK) になるのは、チェックが正常に完了した場合だけです。終了コードが 0 以外の場合は、チェックが失敗したことを示します。終了コードの詳細については、omnidbcheck man ページを参照してください。

バックアップが正しく構成されているかチェックする

1. 重要なバックアップ仕様についてバックアップのプレビューを実行します。バックアップのプレビューの詳細については、第 6 章「バックアップ」(207 ページ) を参照してください。プレビューが正常に完了した場合、以下のことが確認できます。

   - バックアップ仕様に含まれるすべてのクライアントに、Cell Manager からアクセスできる。
   - すべてのファイルがアクセス可能である。
   - バックアップ対象のデータの量が決定されている。
   - バックアップ・デバイスがすべて正常に構成されている。

2. omnirpt -report dl_sched コマンドを実行して、バックアップ仕様がバックアップ・ポリシーに基づいてスケジュールされているかどうかチェックします。omnirpt コマンドの詳細については、omnirpt man ページを参照してください。このコマンドにより、バックアップ仕様すべてとそのスケジュールがリストされます。

Data Protector のインストールを検証する

Data Protector GUI の [クライアント] コンテキストを使ってインストールを検証し、Data Protector ソフトウェア・コンポーネントが Cell Manager 上またはクライアント上で起動、実行されているかチェックします。Data Protector のインストールの検証方法については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

Data Protector ログ・ファイルを点検する

以下の Data Protector ログ・ファイルを点検し、発生する可能性のある問題を特定します。

- `event.log`
- `debug.log`
- `purge.log`

Data Protector ログ・ファイルの詳細については、「Data Protector ログ・ファイル」(681 ページ) を参照してください。

通知のチェックを実行する

トリガされた Data Protector 通知は、デフォルトではすべて Data Protector イベント・ログに送信されます。また、`omnitrig -run_checks` コマンドを実行して、以下の通知のチェックを開始することもできます。

- [IDB のスペース不足]
- [IDB テーブル・スペースのスペース不足]
- [フリー・メディア不足]
- [健全性チェックの失敗]
- [ユーザー・チェックの失敗]
- [予期しないイベント]
- [ライセンス警告]
- [ライセンス期限切れ]
- [IDB の削除必要]

Data Protector 通知の詳細については、「Data Protector 通知」（445 ページ）を参照してください。Data Protector イベント・ログの詳細については、「Data Protector イベント・ログ」（461 ページ）を参照してください。

他のシステム・リソースをチェックする

以下のオペレーティング・システムのログ・ファイルを点検し、発生する可能性のある問題を特定します。

- UNIX システムの場合 : `/var/adm/syslog/syslog.log`
- Windows の場合 : `Windows` イベント・ビューア、およびセキュリティ、システム、アプリケーション・ログを点検します。

IDB のシステム構成バックアップが定期的に作成されているかチェックする

Data Protector 回復ファイル `obrindex.dat` をチェックし、システムの正常な復旧に必要な IDB と構成ファイルが定期的に作成されていることを確認します。`obrindex.dat` ファイルの詳細については、「IDB 復旧の準備」（496 ページ）を参照してください。

ADIC/GRAU DAS および STK ACS ライブラリのインストールと構成に関するトラブルシューティング

インストール手順

1. GRAU ロボティクス (PC/ ロボット) を制御するシステムに Media Agent をインストールします。
2. ドライブが接続されている PC (PC/ドライブ)に Media Agent をインストールします。
3. `aci.dll`、`winrpc.dll`、`ezrpcw32.dll` をディレクトリ `winnt¥system32` と *<Data_Protector_home>*`¥bin` にコピーします。
4. PC/ ロボット上にディレクトリ `aci` を作成します。
5. 作成したディレクトリに `dasadmin.exe` をコピーします。
6. ディレクトリ `aci` に `portmapper` と `portinst` をコピーします。
7. `portinst` を起動して、`portmapper` をインストールします (PC/ ロボット上のみ)。
8. CM に `mmd` パッチをインストールします。
9. PC を再起動し、Windows の［コントロール パネル］を開きます。[管理ツール]、[サービス] で、`portmapper` と 2 つの rpc サービスが共に実行されているかどうかをチェックします。
10. GRAU ライブラリ内の OS/2 PC へ移動して、`/das/etc/config` ファイルを編集します。

    `cd /das/etc/`

    execute: `"e config"`

    この config ファイル内で、PC/ ロボットの IP アドレスを含む OMNIBACK という名前のクライアントを追加する必要があります。
11. PC/ ロボットから以下のコマンドを実行します。

    `dasadmin listd`

    `dasadmin` all DLT7000 UP *<AMUCLIENT>*

    `dasadmin mount` *<VOLSER>* (次にドライブの `UNLOAD` （取出し）ボタンを押します)。

dasadmin dismount *<VOLSER>*

（または dasadmin dismount -d *<DRIVENAME>*）

ここで、*<AMUCLIENT>* = OMNIBACK

<VOLSER> (例 :001565)

<DRIVENAME> (例 : = DLT7001)

"all" は "allocate" を意味します。

上記のコマンド (DAS Server (OS/2) への通信) が正しく実行されなかった場合、OS/2 PC 上でコマンドをもう一度実行してみてください。dasadmin コマンドは /das/bin/ ディレクトリにあります。

OS/2 PC から上記のコマンドを実行する場合は、以下を使用してください。
<AMUCLIENT> = AMUCLIENT

1. AMUクライアントにログインします。一般的なログイン名を以下に示します。

   ユーザー : Administrator、パスワード : 管理者

   ユーザー : Supervisor、パスワード : supervisor

2. メディアの種類を設定する必要がある場合もあります。

   メディアの種類は以下のとおり設定してください。ACI_MEDIA_TYPE set ACI_MEDIA_TYPE=DECDLT

3. ライブラリを再起動するには、以下の手順を行います。

   OS/2 をシャットダウンして、ロボティクスの電源をオフにします。

   OS/2 を再起動します。OS/2 が起動すると、ロボティクスの使用準備ができていないことを示す AMU ログが表示されます。次にロボティクスの電源をオンにします。

GRAU CAP の構成方法

メディアを移動するには、CAP からスロットへ移動した後、デバイスのロボティクスを使ってドライブへ移動する方法しかありません。このとき import および export コマンドを使用する必要があります。例 :

```
import CAP: I01

import CAP range: I01-I03

export CAP: E01
```

```
export CAP range: E01-E03
```

uma ユーティリティの使用方法

Data Protector の uma ユーティリティを使って GRAU および STK ライブラリ・デバイスを管理するには、以下の構文を使用します。

```
uma -pol 8 -ioctl grauamu
```

```
pol 8 for GRAU
```

```
pol 9 for STK
```

デフォルトのメディアの種類は DLT です。

15 他のアプリケーションとの統合

本章の概略

本章では、以下のアプリケーションと Data Protector との統合に関する詳細を説明します。

上記以外のアプリケーション (Microsoft SQL、Oracle8 など) との統合の詳細については、『HP OpenView Storage Data Protector インテグレーション・ガイド』を参照してください。また、サポートされている統合ソフトウェアのリストについては、本書巻頭の「Data Protector のドキュメント」を参照してください。

注記

一部の機能には、専用の Data Protector ライセンスが必要です。詳しくは、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

クラスターと Data Protector との統合

各オペレーティング・システムでサポートされているクラスター・ソフトウェア、クラスター・サポートのレベル、サポートされている構成については、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

クラスターのサポートと概念の詳細は、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

Data Protector 統合データベース・アプリケーションの詳細については、『HP OpenView Storage Data Protector インテグレーション・ガイド』を参照してください。

クラスターの概念と用語

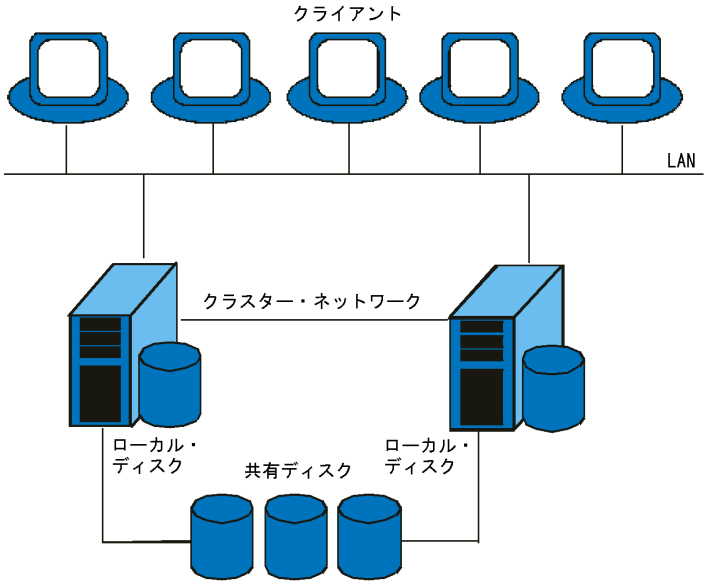
クラスターとは

クラスターとは、ネットワーク上で単一のシステムとして表示される、複数の独立したコンピュータのグループです。このコンピュータのグループは、単一のシステムとして管理され、以下の目的のために設計されています。

- ミッション・クリティカルなアプリケーションやリソースが、可能な限り高い可用性を持つようにする。
- コンポーネントの故障に対する耐性を保つ。
- コンポーネントの追加と取り外しをサポートする。

図 15-1 に代表的なクラスターを示します。

図 15-1 **代表的なクラスター**



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

クラスター・ノード **クラスター・ノード**とは、クラスターを構成するコンピュータのことで、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)、または**共有ボリューム・グループ** (MC/SG)、または**共有プール** (Novell NetWare Cluster) には、ミッション・クリティカルなアプリケーション・データや、クラスターの稼動に必要なクラスター固有のデータが格納されています。MSCS クラスターおよび Novell NetWare クラスターでは、共有ディスク / プールは同時に 1 つのクラスター・ノードでしか使用できません。MC/SG クラスターの場合は、別のノードでも読み取り専用モードでディスクをアクティブにできます。

クラスター・ネットワーク

クラスター・ネットワークとは、すべてのクラスター・ノードが接続されたプライベート・ネットワークで、**クラスターのハートビート**と呼ばれる内部クラスター・データが流れています。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、全クラスター・ノードに配布されます。各クラスター・ノードは、このパケットを比較することによりどのクラスター・ノードが稼働中であるかを判断して、**パッケージ** (MC/SG、Veritas Cluster) または**グループ** (MSCS) の適切な所有者を判断します。

パッケージまたはグループとは

パッケージ (MC/SG、Veritas Cluster)、またはグループ (MSCS) 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合です。各クラスター対応アプリケーションは、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には、以下のリソースが定義されている必要があります。

- 共有ディスク・ボリューム (MSCS)
- 共有ボリューム・グループ (MC/SG、Veritas Cluster)
- 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

仮想サーバとは

ディスク・ボリュームやボリューム・グループは共有物理ディスクを表しています。ネットワーク IP 名とネットワーク 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**を定義するリソースです。仮想サーバの IP 名と IP アドレスはクラスター・ソフトウェアにキャッシュされ、特定のパッケージまたはグループが実行中のクラスター・ノードにマップされます。グループまたはパッケージはノードごとに切り替えることができるので、仮想サーバを時間帯によって異なるマシン上に置くことができます。

フェイルオーバーとは

各パッケージまたはグループには、通常それらが動作する「優先」ノードがあります。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 (二次ノードの 1 つ) に移動できます。パッケージまたはグループを別のクラスター・ノードへ移すことを、**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。フェイルオーバーが発生する原因は、以下のとおり多数あります。

- 一次ノード上でのソフトウェア障害
- 一次ノード上でのハードウェア障害

- 管理者が一次ノードの保守のため意図的に所有権を移動

注記

MSCS 環境では、Cluster Service コンポーネント (データベース・マネージャなど) が中央の共有クラスター・データベースの整合性のとれたイメージを保っています。中央の共有クラスター・データベースにはノード、リソース、グループの状態変化に関する情報が格納されています。クラスター・データベースはクラスターの共有ディスク・ボリューム上に格納されている必要があります。

クラスター対応データベースとアプリケーション

Data Protector は、仮想サーバとしてクラスターにインストールされているクラスター対応アプリケーションとの統合が可能です。統合の際、アプリケーションの仮想サーバ構成を使用します。

クラスター対応のアプリケーションをバックアップする場合は、バックアップ仕様構成時のアプリケーションの仮想クラスター・サーバ名を使用してください。

Microsoft Cluster Server の統合

Data Protector では、高可用性システムのサポート機能の 1 つとして、Microsoft Cluster Server(MSCS) との統合が可能です。各オペレーティング・システムでサポートされているクラスター・ソフトウェア、クラスター・サポートのレベル、サポートされている構成については、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

注記

本項では、Data Protector と Microsoft Cluster Server の統合に固有の情報を記載しています。

クラスターおよび Microsoft Cluster Server の概念について、十分理解していることを前提としています。

詳しくは、以下のマニュアルを参照してください。

- Microsoft Cluster Server オンライン・ドキュメント
- Data Protector のインストール方法については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。
- Data Protector の現在のリリースについての最新情報は、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

ライセンスの設定と Microsoft Cluster Server

Cell Manager のライセンスをご購入の際は、ライセンスは仮想サーバに対応付けられ、Microsoft Cluster Server 内のどの物理ノードで Data Protector Cell Manager を実行するかに関係なく正常に動作することに注意してください。

統合は以下の 2 種類のレベル (Cell Manager またはクライアント) で提供されます。

- Cell Manager を Microsoft Cluster Server 上にインストールして、Data Protector Cell Manager の高可用性を提供します。

- Data Protector クラスター・クライアントは、クラスター環境内のファイルシステムのバックアップとクラスター対応アプリケーションのバックアップをサポートします。

Cell Manager (Microsoft Cluster Server 上の)

Cell Manager を 32 ビット版 Microsoft Cluster Server システムにインストールすると、フェイルオーバー時に Data Protector サービスをあるクラスター・ノードから別のノードに自動的に移行できます。

インストール

クラスター上の Data Protector Cell Manager のインストール方法の詳細については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

セットアップ終了後、Data Protector クラスター・セルには以下のシステムが自動的に追加されます。

- すべてのクラスター・ノード
- すべてのクラスター仮想サーバ

Microsoft Cluster Server 上のクライアント

Data Protector は、完全なクラスター (ローカルおよび共有ディスク) およびクラスター環境で実行されているアプリケーションをバックアップすることができます。

インストール

クラスター対応のアプリケーションをバックアップする場合は、Data Protector クライアント・ソフトウェアをすべてのクラスター・ノードにローカルにインストールする必要があります。クラスター対応クライアントのインストール方法については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

構成

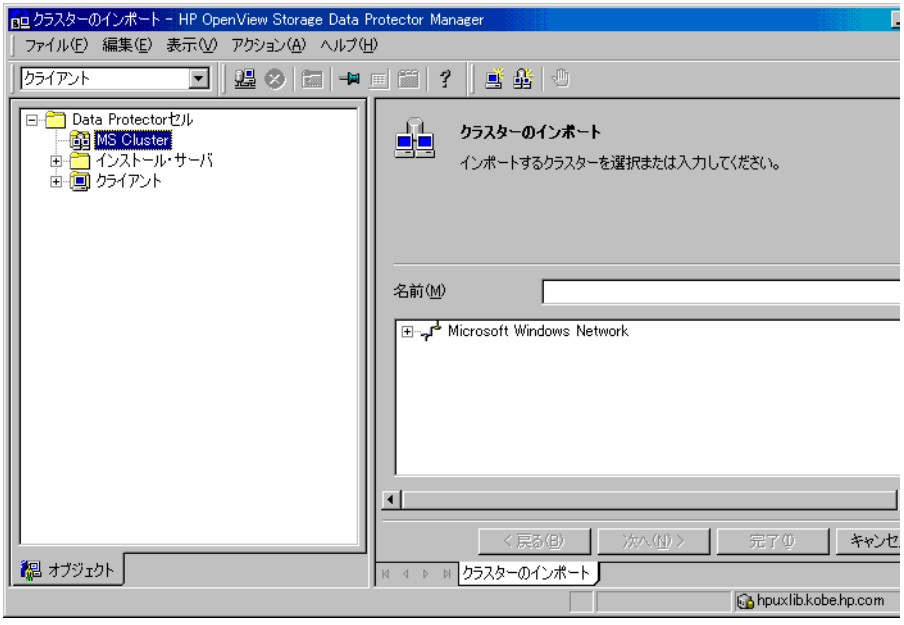
インストール後、クライアントの仮想サーバ・ホスト名を Data Protector セルにインポートする必要があります。この手順は、図 15-2 (775 ページ) および『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

注記

アプリケーションのバックアップをクラスター対応にする場合、つまり仮想サーバを通してバックアップにアクセスしたい場合には、そのアプリケーション用の統合ソフトウェア・モジュールを各アプリケーションの優先所有者 (ノード) 上にインストールする必要があります。この方法を使用した場合に限り、Data Protector 統合エージェントはそのアプリケーションがあるクラスター・ノード上で起動できるようになります。

図 15-2

クラスター仮想サーバのホスト名を Microsoft Cluster Server 上のセルにインポート



クラスター (MSCS) 内のデータのバックアップ

クラスター・ノードのディスク上のデータをバックアップする場合、以下の 2 つを区別する必要があります。

- ローカルのクラスター・ノード・ディスク
- 共有クラスター・ノード・ディスク

Data Protector GUI には、各クラスター・ノードのローカル・ディスクしか表示されません。一方、クラスターの仮想サーバでは、仮想サーバが定義されているグループの共有ディスクのみが表示されます。これにより、共有ディスクに対するバックアップ仕様を作成することを防止できます。このようなバックアップは、あるクラスター・ノード上で共有ディスクが使用不可能になった場合に失敗します。

ローカル・クラスター・ノード・ディスクと共有クラスター・ノード・ディスクを区別するため、Data Protector は MSCS データベースに対して物理クラスター・ディスク・リソースのリストを照会します。専用クラスター・ディスク・リソースとして表示されるクラスター・ディスク（NetRAID 4 ディスク・タイプなど）はすべて、ローカル・クラスター・ノード・ディスクとして扱われます。

しかし、バックアップ仕様の作成時には、バックアップ対象として 3 つまたはそれ以上のシステムが表示されます。

- 一次ノード (ローカル・ディスクのバックアップ時に選択）
- 二次ノード (ローカル・ディスクのバックアップ時に選択）
- 仮想サーバ (共有ディスクのバックアップ時に選択）

ローカル・ディスクのバックアップ

クラスターのローカル・ディスクをバックアップするには、以下の手順を行います。

1. バックアップするローカルディスクがある各クラスター・ノード上に、Data Protector Disk Agent およびクラスター・コンポーネントをインストールし構成します。
2. 特定のクラスター・ノード用のバックアップ仕様を構成し、バックアップするローカル・ディスクを選択します。

共有ディスクのバックアップ

クラスターの共有ディスクをバックアップするには、以下の手順を行います。

1. 各クラスター・ノードに Data Protector クラスター・クライアント・ソフトウェアを (ローカルに) インストールします。インストール手順については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

2. 仮想サーバのホスト名 (Microsoft Cluster Server) を Data Protector セルにインポートします。インストール手順については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。
3. 仮想サーバ用のバックアップ仕様を構成し、バックアップする共有ディスクを選択します。

クラスター対応バックアップの管理

クラスター上の Data Protector Cell Manager では、バックアップ・セッションはクラスター対応となります。Data Protector または他のクラスター対応アプリケーションのフェイルオーバーが発生した場合のバックアップ動作を定義するオプションを設定できます。

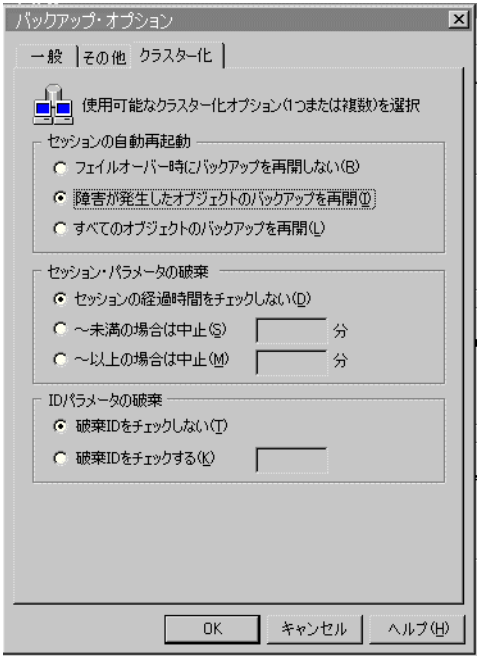
Data Protector のフェイルオーバー

バックアップ中にクラスター対応 Data Protector のフェイルオーバーが発生した場合、実行中および保留中のバックアップ・セッションはすべて失敗します。Data Protector GUI およびバックアップ仕様で、Data Protector フェイルオーバー時のバックアップ・セッションの自動再開を定義するオプションを設定できます。図 15-3 (778 ページ) を参照してください。

障害の発生したセッションの自動再開 バックアップ仕様 (ファイルシステムまたは統合ソフトウェア) を変更して、Cell Manager がフェイルオーバーした場合に、実行中のバックアップ・セッションが自動再開されるようにするには、以下の手順を実行します。

1. [HP OpenView Storage Data Protector Manager] で、[バックアップ] コンテキストに切り替え、[バックアップ仕様] を展開して、変更するバックアップ仕様を選択します。
2. 結果エリアで [オプション] をクリックします。
3. [バックアップ仕様オプション] で、[拡張] をクリックします。
4. [バックアップ・オプション] ウィンドウで、[クラスター化] をクリックし、[セッションの自動起動] オプションを 1 つ選択します。

図 15-3　拡張バックアップ仕様オプション - ［クラスター化］



フェイルオーバー時にバックアップを再開しない

［フェイルオーバー時にバックアップを再開しない］オプションが選択された場合、失敗したセッションは再開されません。これがデフォルトのオプションです。

障害が発生したオブジェクトのバックアップを再開

［障害が発生したオブジェクトのバックアップを再開］オプションは、ファイルシステムのバックアップ仕様に対してのみ有効で、このオプションを指定することにより、ファイルシステム・バックアップ仕様内のバックアップ済みオブジェクトのバックアップは再開されずに、(実行中または保留中に) 障害が発生したオブジェクトのバックアップだけが再開されます。これにより、フェイルオーバーが発生して、一部のバックアップ・オブジェクトのバックアップが完了していない場合のバックアップ時間が最小限に抑えられます。

すべてのオブジェクトのバックアップを再開

[すべてのオブジェクトのバックアップを再開] オプションは、ファイルシステムと統合ソフトウェアのどちらのバックアップ仕様にも有効です。このオプションが選択された場合は、バックアップが完了したオブジェクトも含めて、フェイルオーバー後にセッション全体が再開されます。

Data Protector 以外のアプリケーションのフェイルオーバー

Data Protector クラスター上の Cell Manager は、クラスター環境内のデータ記憶アプリケーションであるため、クラスター内で実行される可能性のある他のアプリケーションを認識する必要があります。Data Protector 以外のノードで他のアプリケーションが実行されており、あるアプリケーションが Data Protector を実行中のノードにフェイルオーバーした場合、このノードに高い負荷がかかることになります。従来、バックアップ操作のみを管理していたノードが、クリティカルなアプリケーションの要求も処理しなければならなくなります。Data Protector では、クリティカル・アプリケーションのデータが保護され、負荷が再度調整されるように、このような状況への対処方法を定義できます。以下の動作を指定できます。

- 実行中のバックアップ・セッションをすべて中止する
- 実行中の特定のバックアップ・セッションを中止する
- 指定した期間、クラスター上の Data Protector Cell Manager を使用不可能にする

実行中のすべてのセッションの中止 バックアップがアプリケーションよりも重要でない場合、Data Protector に実行中のすべてのセッションを自動的に中止させて、アプリケーションがフェイルオーバーした後の負荷を調整するようにします。

このオプションは `omniclus` コマンドで指定します。このコマンドはアプリケーションのフェイルオーバーが発生した時に実行されるスクリプトの一部として使用します。このスクリプトは、事前に作成して、アプリケーション・グループの新しいリソースの種類として定義しておく必要があります

Data Protector 以外のアプリケーションがフェイルオーバーした時に、実行中のすべてのセッションを中止するスクリプトを作成するには、以下の手順を実行します。

1. *<Data_Protector_home>*¥bin ディレクトリで、以下のコマンド行のバッチ・ファイルを作成します。

```
omniclus.exe -clus <Data Protector_virtual_server> -session *
-abortsess
```

注記

* というワイルド・カードは、すべてのセッションを表します。これを特定のバックアップ仕様の名前と置き換えて、その特定のバックアップ・セッションだけを中止することもできます。

2. Windows クラスター・アドミニストレータを開いて、アプリケーション・グループに新しいリソースを追加します。[リソースの種類] で、[一般的なアプリケーション] を選択します。[所有者] でスクリプトを実行するノードを選択します。このノードは Data Protector を実行中のノードとなります。[一般的なアプリケーションのパラメータ] ウィンドウで、バッチ・ファイルのパス名 (例 : c:¥program_files¥omniback¥bin¥clus.bat) と omniclus コマンドのディレクトリを入力します。このコマンドのディレクトリは、*<Data_Protector_home>*¥bin です。

例

サーバ obsv.company.com で実行中のすべてのセッションを中止するには、以下のコマンド行を使用します。

```
omniclus.exe -clus obvs.company.com -session * -abortsess
```

サーバ obsv.company.com 上でバックアップ仕様 backup_1 により実行されているセッションだけを中止するには、以下のコマンド行を使用します。

```
omniclus.exe -clus obvs.company.com -session backup_1
-abortsess
```

論理 ID に応じて実行中のセッションを中止する 実行中の特定のバックアップ・セッションがアプリケーションよりも重要な場合は、Data Protector でセッションを継続することができます。ファイルオーバー後の負荷を調整するため、中止 ID を使って重要なバックアップ・セッション以外はすべて中止します。このオプションは Data Protector GUI およびスクリプトで定義します。

それ以降は、以下の手順を行います。

Data Protector GUI

1. Data Protector GUI で、以下の手順でバックアップ仕様を変更します。
   a. [HP OpenView Storage Data Protector Manager] で、[

バックアップ] コンテキストに切り替え、[バックアップ仕様] を展開して、アプリケーションのフェイルオーバー発生時に中止したくないバックアップ仕様を選択します。

b. 結果エリアで [オプション] をクリックします。

c. [バックアップ仕様オプション] で [拡張] をクリックします。

d. [バックアップ・オプション] ウィンドウで [クラスター化] をクリックします。[破棄 ID をチェックする] を選択して、この仕様を表し、コマンド行で使用されるバックアップ仕様 ID を入力します。

コマンド行

2. バッチ・ファイルで omniclus コマンドを以下のように変更します。

```
omniclus.exe -clus <Data Protector_virtual_server> -session
<backup_specification> -abortsess -abortid
<logical_operator_ID>
```

例

Data Protector GUI で、バックアップ仕様を中止 ID=10 で構成します。以下のコマンド行で、サーバ obsv.company.com 上の、中止 ID が 10 以外のバックアップ・セッションをすべて中止します。

```
omniclus.exe -clus obvs.company.com -session * -abortsess
-abortid != 10
```

セッションの経過時間に応じてセッションを中止する セッションが実行された時間に応じてバックアップ・セッションを中止し、フェイルオーバー後に負荷を調整することができます。実行中の特定のバックアップ・セッションがもうすぐ終了する場合には、そのセッションは継続されます。バックアップ・セッションが始まったばかりで重要でない場合、Data Protector はそのセッションを中止します。このオプションは Data Protector GUI およびスクリプトで指定します。

それ以降は、以下の手順を行います。

Data Protector GUI

1. Data Protector GUI で、以下の手順でバックアップ仕様を変更します。

a. [HP OpenView Storage Data Protector Manager] で、[バックアップ] コンテキストに切り替え、[バックアップ仕様] を展開して、セッションの経過時間に応じて中止したいバックアップ仕様を選択します。

b. 結果エリアで [オプション] をクリックします。

c. [バックアップ仕様オプション] で [拡張] をクリックします。

d. [バックアップ・オプション] ウィンドウで [クラスター化] をクリックします。[～未満の場合は中止] または [～以上の場合は中止] を選択して、この仕様を表す時間 (分）を入力します。フェイルオーバー時に、指定した条件が満たされていればそのセッションは中止されます。

コマンド行

2. バッチ・ファイルで omniclus コマンドを以下のように変更します。

```
omniclus.exe -clus <Data Protector_virtual_server>
-session * -abortsess
```

注記

このコマンドを実行すると、各バックアップ仕様の経過時間がチェックされ、指定された条件を満たしていればそのセッションは中止されます。たとえば、Data Protector GUI で、30 分未満の実行時間のバックアップ仕様を中止するように指定します。フェイルオーバーが発生して omniclus コマンドが起動された場合、実行時間が 30 分未満のセッションは中止され、それ以外のセッションは継続されます。

一時的にバックアップ・セッションを無効にする フェイルオーバー後の負荷を調整するため、Cell Manager を一時的に無効にすることができます。実行中のすべてのセッションは継続されますが、Cell Manager を再度有効にするまでは新しいバックアップを開始できません。スクリプトでのみ指定できます。

コマンド行

バッチ・ファイルで omniclus コマンドを以下のように変更します。

```
omniclus.exe -clus <Data Protector_virtual_server> -inhibit
minutes
```

例

サーバ obvs.company.com 上で新規のバックアップを 20 分間無効にするには、次のコマンド行を使用します。

```
omniclus.exe -clus obvs.company.com -inhibit 20
```

Cell Manager を再度有効にするまで新規のバックアップを無効にするには、以下のコマンド行を使用します。

```
omniclus.exe -clus obvs.company.com -inhibit *
```

バックアップを再度有効にするには、以下のコマンド行を使用します。

```
<Data_Protector_home>¥bin¥omniclus -clus obvs.company.com
-inhibit 0
```

MC/ServiceGuard の統合

Data Protector では、高可用性システムのサポート機能の 1 つとして、HP-UX システム上で Data Protector Cell Manager と MC/ServiceGuard との完全な統合が可能です。サポートされているオペレーティング・システムのバージョン、サポートされている構成、クラスター・サポートのレベルについては、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

注記

本項では、Data Protector および MC/ServiceGuard の統合に固有の情報を記載しています。

クラスターおよび MC/ServiceGuard の概念について、十分理解していることを前提としています。

詳しくは、以下のマニュアルを参照してください。

- MC/ServiceGuard の詳細については、『MC/ServiceGuard の管理』を参照してください。
- Data Protector のインストール方法については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。
- Data Protector の現在のリリースについての最新情報は、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

ライセンスと MC/ServiceGuard

Data Protector Cell Manager のライセンスをご購入の際は、ライセンスは仮想サーバに対応付けられ、パッケージがいずれか 1 つのノードで実行されている限り MC/ServiceGuard クラスター内のどの物理ノードで Data Protector Cell Manager を実行するかに関係なく正常に動作することに注意してください。

Cell Manager（MC/ServiceGuard 上の）

必要条件

- MC/ServiceGuard クラスター環境では、Data Protector Cell Manager は独自のパッケージを持つ必要があります。Data Protector Cell Manager を MC/ServiceGuard 上にインストールする前に、ネットワーク管理者から以下の情報を収集する必要があります。
  - 仮想サーバ名 (クラスター・パッケージ内に指定されているホスト名)
  - パッケージ IP アドレスまたは仮想 IP アドレス

  また、共有ディスク上にボリューム・グループを作成する必要もあります。
- クラスター・ノードとパッケージ IP（仮想 IP）が同じサブネット上にあることを確認してください。
- お使いの環境で DNS を使用している場合、すべてのクラスター・ノードとパッケージの IP アドレスが DNS サーバに登録されていることを確認してください。

インストール

クラスター内のすべてのホストに、UNIX へ Cell Manager をインストールする標準の手順でインストールを行います。この手順は『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』に記述してあります。

重要

GUI を使用して、クラスター・ノード上に他のソフトウェア・コンポーネントを追加する必要がある場合、コンポーネントを追加するノードがアクティブであることを確認してください。

構成

構成時の必要条件

MC/ServiceGuard を使って Data Protector を構成する前に、以下を行っているかチェックしてください。

- 構成を行うには、クラスターがインストールされ実行されていることが必要です。
- 一次Cell Managerと二次Cell Managerをそれぞれどのシステムにするかを決定します。

- 一次 Cell Manager と二次 Cell Manager に決定したシステムに MC/ServiceGuard クラスター・サービスをインストールする必要があります。このとき、推奨パッチを適用し、同じクラスター・メンバーとして構成することが必要です。MC/ServiceGuard のインストールと構成については、『MC/ServiceGuard の管理』を参照してください。
- Data Protector Cell Manager（推奨パッチを含む）、およびクラスター内で使用する他のすべての Data Protector 統合ソフトウェア・コンポーネントを一次ノードと各二次ノードにインストールする必要があります。インストール手順については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

一次 Cell Manager と二次 Cell Manager の構成

本項では、一次 Cell Manager と二次 Cell Manager の構成方法を説明します。

注記

以降の項では、一次 Cell Manager と二次 Cell Manager の構成例を段階的に説明します。例に示されているディレクトリ名やファイル名、番号、他の変数は、環境によって異なります。

一次 Cell Manager の構成

一次 Cell Manager を構成する際、ますボリューム・グループを作成する必要があります。ob2 ディスクをクラスター・ロック・ディスクとして使用している場合は、すでにボリューム・グループを作成済みのはずです。もしまだ作成していない場合は、以下の手順を実行してください。

1. 以下の手順に従って、どちらの Cell Manager へもアクセス可能な共有ディスク上でボリューム・グループ (例 : `/dev/vg_ob2cm`) を作成します。

   a. 新しいボリューム・グループ用のディレクトリを作成します。

   ```
   mkdir /dev/vg_ob2cm
   ```

注記

共有ボリューム・グループには IDB と構成ファイルが格納されます。共有ディスクのサイズを決定する際に、このことに注意してください。

b. システム上の既存のボリューム・グループをすべて表示して、次に使用可能なマイナー番号を確認します。

```
ll /dev/*/group
```

c. このボリューム・グループにグループ・ファイルを作成します。

```
mknod /dev/vg_ob2cm/group c 64 0x010000
```

d. ボリューム・グループ内で使用するディスクを準備します。

```
pvcreate -f /dev/rdsk/c0t1d0
```

```
pvcreate -f /dev/rdsk/c1t2d0
```

e. 新しいボリューム・グループを作成します。

```
vgcreate /dev/vg_ob2cm /dev/dsk/c0t1d0 /dev/dsk/c1t2d0
```

2. 上記のグループに対して論理ボリューム (例 : /dev/vg_ob2cm/lv_ob2cm) を作成した後、以下の手順を行います。

a. 新しい論理ボリュームを作成します。

```
lvcreate -L 100 -n lv_ob2cm /dev/vg_ob2cm
```

上記で、100 という数値は、パーティション・サイズ (MB) を表します。Data Protector ディレクトリ `etc/opt/omni` と `var/opt/omni` がここに配置されます。

b. 論理ボリューム上に、ジャーナル・ファイルシステムを作成します。

```
newfs -F vxfs /dev/vg_ob2cm/rlv_ob2cm
```

注記

新しい論理ボリュームをミラーリングしたい場合は、HP-UX LVM マニュアルで構成手順を参照してください。

3. クラスターのドキュメントに従って、以下の手順でボリューム・グループのプロパティを設定します。

a. ボリューム・グループを通常モードから非アクティブ化します。

```
vgchange -a n /dev/vg_ob2cm
```

b. ボリューム・グループにクラスター用であることを示すマークを付けます。

```
vgchange -c y /dev/vg_ob2cm
```

注記

対象がクラスター・ロック・ディスクで、MC/ServiceGuard の最近のバージョン (11.09 など) を使用している場合は、この手順は自動的に実行されます。

c. ボリューム・グループを排他モードで使用します。

```
vgchange -a e /dev/vg_ob2cm
```

4. 以下の手順に従って、論理ボリュームをディレクトリ (例 : /omni_shared) にマウントします。

a. マウント・ポイント・ディレクトリを作成します。

```
mkdir /omni_shared
```

b. ファイルシステムをマウント・ポイント・ディレクトリにマウントします。

```
mount /dev/vg_ob2cm/lv_ob2cm /omni_shared
```

5. テンプレート・ファイル /etc/opt/omni/sg/sg.conf を編集します。

重要

SHARED_DISK_ROOT 変数に、マウント・ポイント・ディレクトリ名 (例 : SHARED_DISK_ROOT=/omni_shared) が設定されている必要があります。

CS_SERVICE_HOSTNAME 変数に、ネットワークで認識されている仮想 Cell Manager 名が設定されている必要があります。クラスター内の各パッケージは、独自の仮想 IP アドレスと仮想サーバ・ネットワーク名を持つ必要があります (例 : CS_SERVICE_HOSTNAME=ob2cl.company.com)。

6. 一次 Cell Manager を構成します。スクリプトを実行する際は、/etc/opt/omni/ や /var/opt/omni/ ディレクトリ、またはこれらのサブディレクトリにスクリプトを置いていないことを確認してください。また、/etc/opt/omni/ や /var/opt/omni/ にサブディレクトリがマウントされていないことも確認してください。以下のコマンドを実行します。

```
/opt/omni/sbin/install/omniforsg.ksh -primary
```

このスクリプトの実行後は、Data Protector サービスがいったん停止され、後に再起動されることに注意してください。

7. マウント・ポイント・ディレクトリ (Data Protector 共有ディレクトリ) のマウントを解除します。

   ```
   umount /omni_shared
   ```

8. 作成したボリューム・グループを非アクティブ化します。

   ```
   vgchange -a n /dev/vg_ob2cm
   ```

9. 一次 Cell Manager 上に作成したボリューム・グループを以下の手順でエクスポートします。

   a. システム 1(一次 Cell Manager) から、LVM 構成情報をマッピング用ファイル /tmp/lvm_map と共にエクスポートします。

      ```
      vgexport -p -m /tmp/lvm_map /dev/vg_ob2cm
      ```

   b. マッピング用ファイルをシステム 2 (二次 Cell Manager) へ転送します。

      ```
      rcp /tmp/lvm_map second_system:/tmp/lvm_map
      ```

二次 Cell Manager の構成

システム 2 上で二次 Cell Manager を構成するには、以下を実行します。

1. システム 2 上で以下の手順を実行し、インポートするボリューム・グループを設定します。

   a. インポートするボリューム・グループ用のディレクトリを作成します。

      ```
      mkdir /dev/vg_ob2cm
      ```

   b. システム上の既存のボリューム・グループをすべて表示して、次に使用可能なマイナー番号を確認します。

      ```
      ll /dev/*/group
      ```

   c. このボリューム・グループにグループ・ファイルを作成します。

      ```
      mknod /dev/vg_ob2cm/group c 64 0x010000
      ```

   d. ボリューム・グループをマッピング用ファイル /tmp/lvm_map と共にインポートします。

      ```
      vgimport -m /tmp/lvm_map -v /dev/vg_ob2cm
      /dev/dsk/c0t1d0 /dev/dsk/c1t2d0
      ```

2. クラスターのドキュメントに従って、以下の手順でボリューム・グループのプロパティを設定します。

   a. ボリューム・グループにクラスター用であることを示すマークを付けます。

      ```
      vgchange -c y /dev/vg_ob2cm
      ```

注記

対象がクラスター・ロック・ディスクで、MC/ServiceGuard の最近のバージョン (11.09 など) を使用している場合は、この手順は自動的に実行されます。

   b. ボリューム・グループを排他モードで使用します。

      ```
      vgchange -a e /dev/vg_ob2cm
      ```

3. 以下の手順で、論理ボリュームをマウント・ポイント・ディレクトリにマウントします。

   a. 一次 Cell Manager で作成したのと同じマウント・ポイント・ディレクトリを作成します (/omni_shared)。

      ```
      mkdir /omni_shared
      ```

   b. ファイルシステムをマウント・ポイント・ディレクトリにマウントします。

      ```
      mount /dev/vg_ob2cm/lv_ob2cm /omni_shared
      ```

4. 二次 Cell Manager を構成します。

   ```
   /opt/omni/sbin/install/omniforsg.ksh -secondary
   /omni_shared
   ```

5. マウント・ポイント・ディレクトリ (Data Protector 共有ディレクトリ) のマウントを解除します。

   ```
   umount /omni_shared
   ```

6. インポートしたボリューム・グループを非アクティブ化します。

   ```
   vgchange -a n /dev/vg_ob2cm
   ```

パッケージの構成

注記

以降の項では、Data Protector パッケージの構成例を段階的に説明します。例に示されているディレクトリ名やファイル名、番号、他の変数は、環境によって異なります。またこの例では、クラスター構成ファイル名として cluster.conf、Data Protector パッケージ名として ob2cl を使用しています。実際には、ネットワークまたはドメイン管理者から指定された名前に従う必要があります。

このとき、Data Protector デーモンはどちらのクラスター・ノード上でも実行されていないことに注意してください。

必要条件

- 前項で説明したとおり、どちらのクラスター・ノード上にも Data Protector Cell Manager がインストールされ構成されていることが必要です。
- Data Protector クラスター・パッケージを構成する前に、クラスター構成ファイルを作成し編集する必要があります。

Data Protector パッケージの構成

一次 Cell Manager ノード上で、以下の手順を実行します。

1. クラスター構成ファイルにエラーがないかチェックします。

   ```
   cmcheckconf -C /etc/cmcluster/cluster.conf
   ```

   エラーがある場合は修正します。

   エラーがなければ、構成を有効にします。

   ```
   cmapplyconf -C /etc/cmcluster/cluster.conf
   ```

2. クラスターを起動します。

   ```
   cmruncl
   ```

3. ディレクトリ /etc/cmcluster/ の下に、Data Protector パッケージを置くディレクトリを作成します。

   ```
   mkdir /etc/cmcluster/ob2cl
   ```

4. /etc/cmcluster/ob2cl ディレクトリへ移動します。

   ```
   cd /etc/cmcluster/ob2cl
   ```

5. Data Protector パッケージ・ディレクトリにパッケージ構成ファイルを作成します。

   ```
   cmmakepkg -p /etc/cmcluster/ob2cl/ob2cl.conf
   ```

6. Data Protector パッケージ・ディレクトリにパッケージ制御ファイルを作成します。

   ```
   cmmakepkg -s /etc/cmcluster/ob2cl/ob2cl.cntl
   ```

7. Data Protector パッケージ構成ファイル (例 : /etc/cmcluster/ob2cl/ob2cl.conf) の内容を変更します。このファイルの例は、「パッケージ構成ファイルの例」(A-29 ページ) を参照してください。

   このファイルで、以下のフィールドを変更します。

構成ファイルの変更

- PACKAGE_NAME

  PACKAGE_NAME Data Protector クラスター・パッケージ名を入力します。例 :

  ```
  PACKAGE_NAME ob2cl
  ```

- NODE_NAME

  ノード名を入力します。最初に一次（オリジナル）ノード名を、次に二次ノード名（複数あれば複数）を入力します。例 :

  ```
  NODE_NAME partizan
  NODE_NAME lyon
  ```

- RUN_SCRIPT、RUN_SCRIPT_TIMEOUT、HALT_SCRIPT、HALT_SCRIPT_TIMEOUT

  Data Protector パッケージ制御ファイル（スクリプト）の名前を入力し、スクリプト実行のタイムアウト時間を指定します。デフォルトでは、タイムアウトはありません。例 :

  ```
  RUN_SCRIPT /etc/cmcluster/ob2cl/ob2cl.cntl
  RUN_SCRIPT_TIMEOUT NO_TIMEOUT
  HALT_SCRIPT /etc/cmcluster/ob2cl/ob2cl.cntl
  HALT_SCRIPT_TIMEOUT NO_TIMEOUT
  ```

- SERVICE_NAME、SERVICE_FAIL_FAST_ENABLED、SERVICE_HALT_TIMEOUT

サービス情報を入力します。サービス名として任意の名前も設定できますが、この後の制御ファイルでも同じ名前を設定する必要があることに注意してください。例 :

```
SERVICE_NAME omni_sv
SEVICE_FAIL_FAST_ENABLED NO
SERVICE_HALT_TIMEOUT 300
```

- SUBNET

  クラスターのサブネットを入力します。例 :

  ```
  SUBNET 10.17.0.0
  ```

8. Data Protector パッケージ制御ファイル (例 : /etc/cmcluster/ob2cl/ob2cl.cntl) の内容を変更します。このファイルの例は、「パッケージ制御ファイルの例」(A-39 ページ) を参照してください。

   このファイルで、以下のフィールドを変更します。

制御ファイルの変更

- VG [n]

  このパッケージで使用するボリューム・グループを指定します。例 :

  ```
  VG [0] = /dev/vg_ob2cm
  ```

- LV [n], FS [n], FS_MOUNT_OPT [n]

  論理ボリュームとファイルシステムのマウント情報を指定します。

  ```
  LV [0] = /dev/vg_ob2cm/lv_ob2cm
  FS [0] = /omni_shared
  FS_MOUNT_OPT[0]=" "
  ```

- IP、SUBNET

  このパッケージが使用する IP アドレスとサブネット情報を指定します。例 :

  ```
  IP [0] = 10.17.3.230
  SUBNET [0] = 10.17.0.0
  ```

- SERVICE_NAME、SERVICE_CMD、SERVICE_RESTART

  サービス名、コマンド、再起動パラメータを指定します。

重要

このサービス名は構成ファイルで使用したのと同じである必要があります。サービス・コマンド（SERVICE_CMD 変数）は、以下の例で使用されているものである必要があります。

例 :

```
SERVICE_NAME [0] = omni_sv
SERVICE_CMD [0] = "/etc/opt/omni/server/sg/csfailover.ksh
start"
SERVICE_RESTART [0] = "-r 2"
```

フェイルオーバー時に Cell Manager パッケージが確実に再起動されるようにするには、SERVICE_RESTART パラメータを -R (サービスを無期限の回数再起動する ; お勧めしません) または "-r *<number_of_restarts>*" (指定した回数だけサービスを再起動する) に設定します。

9. 以下の手順に従って、Data Protector クラスター・パッケージ・ファイルのチェックと配布を行います。

   a. クラスター内の他のノードにパッケージ制御ファイルをコピーします。

   ```
   remsh system2 "mkdir /etc/cmcluster/ob2cl"
   rcp /etc/cmcluster/ob2cl/ob2cl.cntl
   system2:/etc/cmcluster/ob2cl/ob2cl.cntl
   ```

   b. Data Protector 共有ディスクを、全クラスター・ノード上で (以前作成した) クラスター・ボリューム・グループとして使用できるよう設定します。

   ```
   vgchange -c y /dev/vg_ob2cm
   ```

   c. Data Protector パッケージをチェックします。

   ```
   cmcheckconf -P /etc/cmcluster/ob2cl/ob2cl.conf
   ```

   d. チェックが正常に実行された場合は、Data Protector パッケージを追加します。

   ```
   cmapplyconf -P /etc/cmcluster/ob2cl/ob2cl.conf
   ```

   e. パッケージを起動します。

```
cmrunpkg ob2cl
```

クラスターが構成され、Data Protector Cell Manager パッケージが起動して実行されます。

f. omnicc コマンドなどを使用して、仮想サーバ (クラスター・パッケージ内に指定されたホスト名) を手動でインポートします。

```
omnicc -import_host <virtual_hostname> -virtual
```

g. MC/ServiceGuard 上に Data Protector インストール・サーバもインストールされている場合は (デフォルト)、(omnicc コマンドなどを使用して) インストール・サーバもインポートします。

```
omnicc -import_is <virtual_hostname>
```

h. 二次ノード上で Data Protector GUI を実行するには、Data Protector GUI を起動して、二次ノードの root ユーザーを admin ユーザー・グループに追加する必要があります。詳しくは、「ユーザーの追加または削除」（144 ページ) を参照してください。

MC/ServiceGuard 上のクライアント

Data Protector は、完全なクラスター (ローカルおよび共有ディスク) およびクラスター環境で実行されているアプリケーションをバックアップすることができます。

インストール

クラスター対応のアプリケーションをバックアップする場合は、Data Protector クライアントをすべてのクラスター・ノードにローカルにインストールする必要があります。クラスター対応クライアントのインストール方法については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

構成

アプリケーション仮想サーバ (アプリケーション・クラスター・パッケージ内に指定されたホスト名) をセルにインポートする必要があります。

Cell Manager とアプリケーションが同じクラスターにある場合は、仮想サーバをインポートする前に、Cell Manager パッケージをアプリケーション・ノードに移動する必要があります。その後、以下の手順を行います。

1. Cell Manager パッケージを停止します (例 : ob2cl)。

   ```
   cmhaltpkg ob2cl
   ```

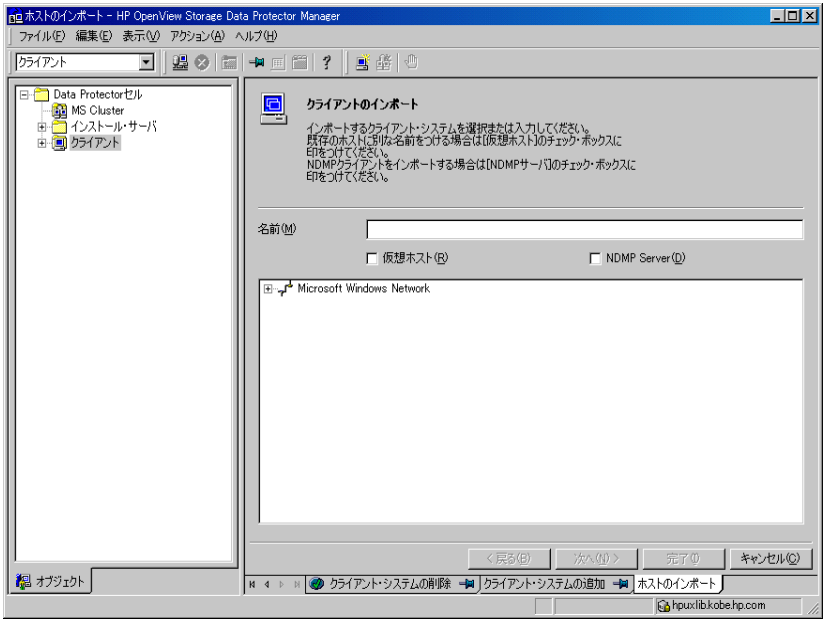
2. Cell Manager パッケージをアプリケーション・ノード上で実行します。

   ```
   cmrunpkg -n <node_name> ob2cl
   ```

注記

Data Protector GUI を使用している場合は、各仮想サーバをクライアントとしてインポートします。詳しくは、図 15-4 (797 ページ) と『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

図 15-4 **アプリケーション・クラスター・パッケージを MC/ServiceGuard 上のセルにインポート**



クラスター内のデータのバックアップ (MC/SG)

本項では、クラスター環境内の特定のデータをバックアップする方法の概要を説明しています。クラスター内のデータの詳しいバックアップ方法については、「クラスター (MSCS) 内のデータのバックアップ」（775 ページ）を参照してください。

注記

仮想サーバのバックアップを行う際、オブジェクトの所有権は、クラスター・パッケージが実行されている特定のホストの所有権と同じになります。したがって、フェイルオーバーが発生した場合は、同じオブジェクトのバックアップの所有者が異なることになります。これを回避するには、バックアップ仕様内でオブジェクトの所有権を仮想サーバに設定してください。

ローカル・ディスクのバックアップ

クラスターのローカル・ディスクをバックアップするには、以下の手順を行います。

1. バックアップするローカル・ディスクがある各クラスター・ノード上に、Data Protector Disk Agent コンポーネントをインストールし構成します。
2. 特定のクラスター・ノード用のバックアップ仕様を物理ノード名を使用して構成し、バックアップするローカル・ディスクを選択します。

共有ディスクのバックアップ

クラスターの共有ディスクをバックアップするには、以下の手順を行います。

1. すべてのクラスター・ノードに Data Protector クラスター・クライアント・ソフトウェアを (ローカルに) インストールして構成します。インストール手順については、『*HP OpenView Storage Data Protector インストールおよびライセンス・ガイド*』を参照してください。
2. 仮想サーバ (クラスター・パッケージ内に指定されたホスト名) を Data Protector セルにインポートします。
3. バックアップ仕様を構成し、仮想サーバを選択します。バックアップする共有ディスクを定義します。

Veritas Cluster の統合

Veritas Cluster 上のクライアント

Data Protector は、Veritas Cluster 環境では、ローカル・ディスクまたは共有ディスクのバックアップのみに使用できます。

Data Protector と Veritas Clusters の組み合わせでは、クラスター対応アプリケーションはサポートされていません。

インストール

Data Protector を各クライアント上にローカルにインストールし、各クライアントをセルにインポートする必要があります。段階的な手順は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

Data Protector を使って Veritas Cluster を構成するには、Data Protector ユーザー・インタフェースが必要です。

詳しくは、以下のドキュメントを参照してください。

- Veritas Cluster のドキュメント
- Data Protector のインストール方法については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。
- Data Protector の現在のリリースについての最新情報は、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

構成

クラスター・ノードのローカル・ディスクをバックアップできるようにするには、各ノードを Data Protector Cell Manager にインポートすることが必要です。

ローカル・ディスクのバックアップ

ディスクがローカルに接続されているシステムをブラウズすると、クラスター内のシステムに対してローカルなディスクが表示されます。

以下の手順に従って、ローカル・ディスクをバックアップします。

1. バックアップ対象のローカル・ディスクのある各システムに、Data Protector Disk Agent をインストールします。
2. クラスター内のローカル・システムのバックアップを構成し、バックアップするローカル・ディスクを定義します。

共有ディスクのバックアップ

前述のとおり、共有ディスクはローカル・ディスクとしてのみバックアップできます。しかし、そのディスクを共有しているいずれのノードからでもバックアップ可能です。

たとえば、2 つのノードで共有しているディスクをバックアップする場合の手順は以下のとおりです。

1. ディスクを共有している各システムに Data Protector Disk Agent をインストールします。
2. 各システム上で、このディスクに対するバックアップ仕様を「ローカル・ディスク」として定義します。
3. 共有ディスクのバックアップをより確実にするには、各バックアップ仕様内で実行後スクリプトを作成します。この実行後スクリプトで、エラーをチェックして、1 台目のシステムでバックアップが失敗した場合は他のシステム上でバックアップを起動するように設定します。

Novell NetWare Cluster 用統合ソフトウェア

Novell NetWare Cluster 上のクライアント

Data Protector は、Novell NetWare Cluster 環境では、ローカル・ディスクまたはクラスター共有プールのバックアップのみに使用できます。

Data Protector を Novell NetWare Cluster で使用する場合、クラスター対応アプリケーションはサポートされません。フェイルオーバーした場合は、バックアップまたは復元セッションを手動で再起動する必要があります。

インストール

Data Protector を各クライアント上にローカルにインストールし、各クライアントをセルにインポートする必要があります。段階的な手順は、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。

Data Protector を使って Novell NetWare Cluster を構成するには、Data Protector ユーザー・インタフェースが必要です。

詳しくは、以下のドキュメントを参照してください。

- Novell NetWare Cluster のドキュメント
- Data Protector のインストール方法については、『HP OpenView Storage Data Protector インストールおよびライセンス・ガイド』を参照してください。
- Data Protector の現在のリリースについての最新情報は、『HP OpenView Storage Data Protector ソフトウェア リリース ノート』を参照してください。

注記

Novell NetWare 仮想サーバ上ではデバイスを追加できません。

構成

クラスター・ノードのローカル・ディスクをバックアップできるようにするには、各ノードを Data Protector セルにインポートすることが必要です。また、クラスター共有プールをバックアップできるようにするには、仮想サーバをセルにインポートする必要があります。

ローカル・ディスクのバックアップ

ディスクがローカルに接続されているシステムをブラウズすると、クラスター内のシステムに対してローカルなディスクが表示されます。

以下の手順に従って、ローカル・ディスクをバックアップします。

1. バックアップ対象のローカル・ディスクのある各システムに、Data Protector Disk Agent をインストールします。
2. クラスター内のローカル・システムのバックアップを構成し、バックアップするローカル・ディスクを定義します。

共有クラスター・プールのバックアップ

クラスター共有プールのバックアップは、仮想サーバ経由でのみ可能です。バックアップ対象として仮想サーバを選択した場合は、バックアップ可能なプールとしてクラスター共有プールのみが表示されます。

たとえば、2 つのノードで共有しているプールをバックアップする場合の手順は以下のとおりです。

1. プールを共有している各システムに Data Protector Disk Agent をインストールします。
2. クラスター仮想サーバをセルにインポートします。
3. 仮想サーバ上のすべてのプールを含むバックアップ仕様を作成して、バックアップを開始します。

Data Source Integration (DSI)

DSI とは

Data Source Integration (DSI) により、HP OpenView Performance Agent を使ってデータのログへの記録、アラームの定義、データ・ソースから HP OpenView Performance Agent scopeux collector がログに記録した以外のメトリクスへのアクセスが可能です。Data Protector のサンプル用スクリプトと構成ファイルでは、Data Protector のレポート用コマンド行インタフェースを Data Source Integration と併用して、Data Protector 環境やバックアップ / 復元セッションに関するデータを記録する方法を説明しています。

測定可能な内容

DSI 統合を使用して、以下のような数値を測定することができます。

- データベースのサイズ
- メディアの使用状況
- メディアのステータス
- システム数
- システムあたりのデータ量
- フル・バックアップおよび増分バックアップの個数

構成の概要

DSI を使用するには、以下を行うことが必要です。

- どのデータをログに記録するかを確認します。
- Data Protector からデータを照会するためのスクリプトを記述します。
- クラス仕様ファイルを設定します。
- クラス仕様ファイルをコンパイルします。
- ロギング・プロセスを起動します。

Data Protector には、Korn シェル (ksh) スクリプトとクラス仕様ファイルのサンプルが用意されており、デフォルトでは 2 つのメトリクス (セル内のクライアント数と IDB のサイズ) が記録されます。このスクリプトとクラス仕様ファイルは簡単に変更でき、Data Protector から他の情報を収集することも可能です。このスクリプトは、UNIX システム上でサポートされています。

統合の構成

以下の手順に従って、Data Protector DSI 統合を構成します。

1. データを収集するためのスクリプトを記述します。

   まず、ログに記録するデータを選択します。Data Protector のレポート用コマンド omnirpt は、ディレクトリ /opt/omni/bin/ にあります。このコマンドを使って Data Protector 環境に関するさまざまな情報を収集できます。コマンドの詳細については、omnirpt の man ページを参照してください。次に、選択したデータを無限ループで照会し、照会したデータを標準出力に書き込むスクリプトを記述します。

2. クラス仕様ファイルを作成します。

   クラス仕様ファイルでは、ログに記録するデータと記録方法を定義します。Data Protector のクラス仕様ファイルのサンプル obdsi.spec はディレクトリ /etc/opt/omni/server/dsi にあります。クラス仕様ファイルの完全な構文については、DSI のドキュメントを参照してください。

3. クラス仕様ファイルをコンパイルします。

   ディレクトリ /opt/perf/bin にある sdlcomp コマンドを使って、クラス仕様ファイルをコンパイルします。Data Protector のクラス仕様ファイルのサンプルをコンパイルするには、以下のコマンドを実行します。

   ```
   sdlcomp obdsi.spec OmniBack.log OmniBack
   ```

4. perflbd.rc を構成します。

   ファイル perflbd.rc を変更する前に、mwa サービスを終了してください。このサービスを終了するには、以下のコマンドを実行します。

   ```
   /opt/perf/bin/mwa stop
   ```

   上記のコマンドを実行すると、ファイル /var/opt/perf/perflbd.rc を編集できます。Data Protector のメトリクスのサンプルを構成する場合は、ファイルに以下の行を追加します。このとき、必ず 1 行で入力してください。

   ```
   DATASOURCE=OMNIBACKII
   LOGFILE=/etc/opt/omni/server/dsi/OmniBack.log
   ```

5. ロギング・プロセスを起動します。

   dsilog コマンドを使ってデータを収集して出力をパイプに渡すスクリプトを起動します。Data Protector のメトリクスのサンプルの場合は、以下のコマンドを使用します (コマンドは 1 行で入力します)。

   ```
   obdsi.ksh | /opt/perf/bin/dsilog OmniBack.log OMNIBACKII
   ```

Application Response Measurement (ARM) との統合

ARM の統合とは

Data Protector は、分散環境内のトランザクションの応答時間を測定するための新しい基準である Application Response Measurement (ARM) インタフェースをサポートしています。Data Protector によって提供されるデータは、ARM に準拠するシステム管理ツールやモニタリング・ツール (HP OpenView Performance Agent など) で使用できます。これらのツールでは、情報をログに記録して、トレンドの解析、レポート、警告に基づく通知などを行うことができます。収集されたデータは、HP OpenView PerformanceManager またはその他のツールで表示、解析できます。

ARM 統合ソフトウェアのインストール方法

必要なインストール作業は、ARM 2.0 互換の RPM エージェントとライブラリの Cell Manager へのインストールだけです。RPM エージェントとライブラリのインストールは、Data Protector のインストールの前後どちらで行っても構いません。

UNIX Cell Manager の場合は、ダミーのライブラリ `/opt/omni/lib/arm/libarm.sl` (HP-UX の場合)、または `/opt/omni/lib/arm/libarm.so` (Solaris の場合) を適切な ARM ライブラリ (実際に処理を記録する) に交換するか、ライブラリへのリンクを作成する必要があります。リンクを作成することをお勧めします。たとえば、HP OpenView Performance Agent が HP-UX 11.x Cell Manager にある場合は、上記のファイルを `/opt/perf/lib/libarm.sl` ファイルにリンクする必要があります。`/opt/perf/lib/libarm.sl` ファイルは `libarm.0` にリンクされていることに注意してください。

Windows Cell Manager では、ARM 統合の設定に追加して行うべき手順はありません。

測定可能な内容

ARM 統合を使用して、以下のような数値を測定することができます。

- セッションの継続時間
- Disk Agent の読出し時間
- Disk Agent のネットワーク書込み時間
- Media Agent のネットワーク読出し時間

- Media Agent のデータ書込み時間
- Session Manager のデータベースへの書込み時間
- データベースの削除時間

下表に、サポートされている ARM トランザクションを示します。

表 15-1 ARM トランザクション

トランザクション名	追加情報	トランザクションの詳細
BS-*<Backup_specification>*	時間	バックアップ・セッションのバックアップ時間
RS-*<Session_ID>*	時間	復元セッションの復元時間
BO-*<Object_name>*	時間	特定のオブジェクトのバックアップ時間
DP	削除されたレコード数、IDB のサイズ (MB)	IDB の削除時間
DC	IDB サイズ (MB)	IDB のチェック時間

ManageX の統合

ManageX の統合とは

ManageX の統合は、ManageX が実行されている Windows システム上でサポートされています。ManageX を使用して、Data Protector の処理およびバックアップ状態を調べることができます。

サポート内容

ManageX の統合は、以下をサポートしています。

- ユーザーが選択した重大度レベルの Data Protector メッセージを ManageX コンソールに送信する。
- すべての Data Protector サービスが実行されているかを調べ、サービスのいずれかが終了した場合にメッセージを ManageX コンソールに送信する。

統合の構成

ManageX と Data Protector の統合は、以下の手順で行います。

1. Cell Manager で、Data Protector メッセージの転送を有効にします。
   a. グローバル・ファイル・セットで、`EventLogMessages=1` を設定します。詳細については、「グローバル・オプション・ファイル」(645 ページ) を参照してください。
   b. Data Protector サービスを終了して再起動します。
2. ManageX コンソールで受信する Data Protector メッセージの重大度レベルを設定するには、ファイル *<Data_Protector_home>*¥config¥server¥managex¥filter に重大度レベルを追加または削除します。デフォルトでは、このファイルにすべての重大度レベルが記述されています(normal | warning | minor | major | critical)。
3. ManageX コンソールを使用して、ManageX から Data Protector Cell Manager にポリシーを配布します。Data Protector ポリシーは、Backup Application というフォルダにあります。

システム / 管理アプリケーションへのアクセス

本項では、Data Protector のシステム / 管理アプリケーションへのアクセス方法について説明します。

はじめに

Data Protector と HP OpenView を統合することにより、以下のようなシステム / アプリケーション管理用アプリケーションを使って Data Protector プロセスの性能を管理、モニター、測定できるようになります。

- HP OpenView Vantage Point Operations
- HP OpenView DSI
- HP OpenView ManageX

Data Protector では、このようなアプリケーションへアクセスするために以下のような一般的なインタフェースを用意しています。

- SNMP トラップ
- ユーザー・インタフェース (Data Protector GUI、CLI、Web レポート・インタフェース)
- Data Protector ログ・ファイル
- Windows アプリケーション・ログ

Data Protector と統合するアプリケーションによりますが、上記すべての方法、または一部の方法のみが使用可能になります。Data Protector では、これらのアプリケーションを使用して実行できる定義済みレポートや定義済みアクションがあらかじめ用意されています。詳細は、この章の説明を振り返ってください。

Data Protector へのアクセス方法

SNMP トラップ

SNMP トラップを使用することにより、Data Protector でのイベント発生時や Data Protector のチェック / 保守メカニズムによって SNMP トラップが送信された時に、システム / アプリケーション管理用アプリケーションが

SNMP トラップ・メッセージを受信、処理できるようになります。Data Protector のチェックと保守機構の詳細は、「Data Protector のチェック / 保守機構」（757 ページ) を参照してください。

HP-UX と Solaris では、Cell Manager に 2 つの Data Protector ファイルがあり、それらのファイルで Data Protector SNMP トラップの動作を指定できます。

- `/etc/opt/omni/server/snmp/OVdest`

  このファイルでは、Data Protector SNMP トラップを受信するシステムの名前を指定します。このファイルの形式を以下に示します。

  `trap-dest: <hostname1>`

  `trap-dest: <hostname2>`

  `...`

- `/etc/opt/omni/server/snmp/OVfilter`

  このファイルでは、Data Protector SNMP トラップ・メッセージの除外対象 (Data Protector から送信されない) の重大度レベルを指定します。このファイルの形式を以下に示します。

  <message_level>

  <message_level>

  `...`

  < message_level> には、次のいずれかの値を指定します。(`normal | warning | minor | major | critical`)

Windows システムの場合、送信先は Windows SNMP サービスの構成で設定します。

注記

Windows システムの場合、まず SNMP サービスを構成する必要があります。Windows SNMP サービスの構成方法については、「SNMP による送信」（454 ページ) を参照してください。

Data Protector から送信される SNMP トラップは、以下の情報で構成されています。

- **エンタープライズ・イベント ID**

  各イベントには、エンタープライズ・イベント ID(EID) が付与されます。EID はイベントを送信するエンティティの種類を表します。OpenView エンティティが送信するイベントの EID は、".1.3.6.1.4.1.11.2.17.1" です。

- **一般イベント ID**

  各イベントには、一般イベント ID(GID) も付与されます。標準の SNMP トラップの場合、GID は `ovtrapd` に対してどの標準 SNMP トラップが生成されたかを通知します。その他の種類のイベントの場合、GID は **6** になります。これは、イベントをさらに評価するために送信エンティティが特定イベント ID を使用したことを意味します。Data Protector は GID に 6 のみを使用します。

- **特定イベント ID**

  GID が 6 のイベントには、特定イベント ID (SID) も付与されます。SID を使用することにより、エンタープライズはイベント定義のカスタム・セットを独自に定義できます。Data Protector が使用する **59047936** はアプリケーションに対する警告トラップで、HP OpenView トラップ向けの既存の SNMP トラップのサブタイプです。

- **変数**

表 15-2 (810 ページ) に、Data Protector が送信する SNMP トラップの形式と一般的な値を示します。

表 15-2　Data Protector SNMP トラップの形式

MIB ID	意味	例
1.3.6.1.4.1.11.2.17.1.1.0	アプリケーションの種類	1
1.3.6.1.4.1.11.2.17.1.2.0	Cell Manager のホスト名	machine.company.com
1.3.6.1.4.1.11.2.17.1.3.0	トラップ・メッセージの種類	NOTIFICATION、または無し
1.3.6.1.4.1.11.2.17.1.4.0	アプリケーション名	HP Data Protector

表 15-2 Data Protector SNMP トラップの形式

MIB ID	意味	例
1.3.6.1.4.1.11.2.17.1.5.0	メッセージの重大度	致命的
1.3.6.1.4.1.11.2.17.1.6.0	メッセージ	デバイス DLT_1 にエラーが発生しました。
1.3.6.1.4.1.11.2.17.2.7.0	パラメータ・リスト	デバイス名 DLT_1 に対するマウント要求

コマンド行インタフェース、GUI(グラフィカル・ユーザー・インタフェース)、Web レポート・インタフェース

Data Protector CLI では、Data Protector GUI と互換性のある機能が用意されています。Data Protector CLI を使って以下を実行できます。

- Data Protector GUI、サブ GUI の起動。Data Protector のサブ GUI のリストは、「グラフィカル・ユーザー・インタフェース」(6 ページ) を参照してください。
- Data Protector アクション (バックアップ、復元、IDB の削除など) の構成および開始。実行可能な Data Protector アクションのリストは、「Data Protector のコマンド」(A-7 ページ) を参照してください。
- `omnirpt` CLI コマンドを使った Data Protector レポートの構成および開始。レポートの詳細については、「Data Protector レポート」(417 ページ) を参照してください。
- Data Protector レポートを構成、開始するための Java ユーザー・インタフェースの起動。Web レポートの詳細については、「Web レポートおよび Web 通知の構成」(457 ページ) を参照してください。

Data Protector コマンドは、システム / アプリケーション管理用アプリケーションの入力データを提供するスクリプト内で使用できます。

Data Protector ログ・ファイル

システム / アプリケーション管理用アプリケーションの中には HP OpenView Vantage Point Operations のように、特定のログ・エントリに対してモニターを行う時刻やモニター対象のログ・ファイルを指定できるもの

があります。指定しておいたエントリがファイル内で検出された場合の動作を指定できます。VPO ではこれを *ログ・ファイルのカプセル化*と言います。

このようなシステム / アプリケーション管理用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する動作を定義できます。

Data Protector ログ・ファイルの詳細については、「Data Protector ログ・ファイル」(681 ページ) 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。Data Protector ログ・ファイルのエントリの例は、「Data Protector ログ・ファイルの主なエントリ」(A-45 ページ) を参照してください。

Windows アプリケーション・ログ

ManageX などシステム / アプリケーション管理用アプリケーションの中には Windows アプリケーション・ログをモニターできるものがあります。

すべての Data Protector メッセージや Data Protector サービス (終了している場合) 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、「グローバル・オプション・ファイル」(645 ページ) を参照してください。

例

Data Protector プロセスの検証

Data Protector では、`omnisv -status` CLI コマンドを実行して、必要なプロセスが実行中かどうかをチェックできます。

`omnisv -status` コマンドを実行すると、必要な Data Protector プロセスのステータスが通知されます。

omnisv -status

必要な Data Protector プロセスのステータスを取得するには、以下のコマンドを入力します。

```
omnisv -status
```

Data Protector [健全性チェックの失敗] 通知

ユーザーの健全性チェックの通知は、必要なプロセスが実行されていない場合や IDB が実行不可能な場合にのみトリガされ、送信されます。[健全性チェックの失敗] 通知は、デフォルトでは毎日これらを 12 時 (正午) にチェックし、通知を送信する必要がある場合は、Data Protector イベント・ログ (デフォルト) に送信します。Data Protector グローバル・オプション・ファイルの DailyMaintenanceTime パラメータを変更して実行時刻を変更することができます。このとき 24 時間表記を使用します。Data Protector グローバル・オプション・ファイルの詳細は、「グローバル・オプション・ファイル」（645 ページ) を参照してください。通知は、たとえば SNMP トラップとして転送することもできます。

必要な Data Protector プロセスおよび IDB の稼働を毎日決められた時刻にチェックし、実行されていないプロセスや実行不可能なデータベースを SNMP トラップから通知するには、「Data Protector 通知」（445 ページ) の説明に従って[健全性チェックの失敗] 通知を構成してください。

[健全性チェックの失敗] 通知の状況を対話形式でチェックするには、以下のコマンドを入力します。

```
omnihealthcheck
```

omnihealthcheck コマンドの詳細については、omnihealthcheck の man ページを参照してください。

前日の夜間に実行されたバックアップ結果の取得

前日の夜間に実行されたバックアップの結果に関するレポートは、Data Protector レポート機能を使って取得できます。Data Protector レポート機能の詳細は、「Data Protector レポート」（417 ページ) および omnirpt の man ページを参照してください。omnirpt では、30 を超えるレポートそれぞれに異なるオプションを設定して実行することができます。

前日の夜間に実行されたバックアップに関する HTML レポートをファイル report.html に取得するには、以下のコマンドを入力します。

```
omnirpt -report list_sessions -timeframe 24 24 -html -log
report.html
```

A 詳細情報

本付録の概略

この付録では、以下の項目について説明します。

特定の UNIX ファイル・フォーマットのバックアップと復元

この項では、特定の UNIX ファイル・フォーマット (VxFS、Enterprise Filesystem、Context Dependent Filesystem) のバックアップ方法を説明します。

VxFS スナップショット

VxFS とは

VxFS では、別のアプリケーションが使用中のファイルシステムをバックアップできます。これはオンライン・バックアップと呼ばれ、ファイルシステムのスナップショットを作成して、作成されたスナップショットをバックアップするものです。

VxFS ファイルシステムを一時ディレクトリにマウントする際に、ファイルシステムのスナップショットを作成します。このとき、スナップショットの作成対象となるファイルシステムを指定することもできます。

スナップショットとは、VxFS ファイルシステムを一時ディレクトリにマウントする際の特定の時点でのファイルシステムのコピーを指します。

他のファイルシステムについては、VxFS スナップショット機能を使用せずに、単にバックアップを構成するだけで通常のバックアップを実行できます。ただしこの場合、使用中のファイルはバックアップできません。

一時ディレクトリのバックアップを構成します。実際には、このディレクトリがマウント時のファイルシステムのスナップショットへのマウント・ポイントとなります。

バックアップ完了後は、スナップショット・ファイルシステムをアンマウントして、他の用途にも使用できるようにします。

VxFS バックアップの構成方法

VxFS オンライン・バックアップ機能を使用する場合は、以下の手順に従ってバックアップを構成します。

1. VxFS がスナップショットに使用するための空きまたは未使用のパーティションをシステム内に作成する必要があります。作成方法については、システム管理者用マニュアルを参照してください。

バックアップ中のファイルシステムの使用率が高い場合は、スナップショット・ファイルシステムの推奨サイズは、スナップ対象となるファイルシステムの 15% が上限です。ただし通常は、約 5% に設定してください。

スナップ対象のファイルシステム上で変更されるデータの量が使用可能なスペースを超えた場合、Data Protector は、残りのバックアップ対象のすべてのファイルに対して Cannot stat というエラー・メッセージを生成します。この場合は、スナップショット・ファイルシステムをアンマウントして、再度バックアップ手順を実行しなければなりません。

2. スナップショット・ファイルシステムをマウントする一時ディレクトリを作成します。
3. スナップショット・ファイルシステムを一時ディレクトリへマウントとアンマウントを行うシェル・スクリプトを作成します。スクリプトのテンプレートについては、次項の「実行前 / 実行後スクリプトのテンプレート」を参照してください。
4. 一時ディレクトリのバックアップを構成します。マウント用スクリプトは実行前コマンドとして指定し、アンマウント用スクリプトは実行後コマンドとして指定します。

実行前 / 実行後スクリプトのテンプレート

以下に、VxFS ファイルシステムをマウント / アンマウントするための Data Protector 実行前 / 実行後コマンドとして構成できるテンプレートの例を示します。

例 A-1 **実行前スクリプトのテンプレート**

```
# SnapMount.sh
#
# Mounting snapshot filesystem (Pre-exec script)
#
# A script requires 3 parameters:
# 1. # - a block special file of the snapshot FS
# or
# a mount point directory of the snapped FS
# 2. # - a block special file of the snapshot FS
# 3. # - a mount point directory of the snapshot FS
#
# NOTE:
#
```

```
# In case of multiple Disk Agents reading from the same
snapshot
# FS,
# the Pre-exec script should contain a kind of
synchronization
# mechanism for following reasons:
#
# 1) an attempt to mount an already mounted snapshot FS,
# snapping the same FS will cause the Pre-exec script to
fail and
# a DA to abort
#
# 2) an attempt to mount an already mounted snapshot FS,
# snapping some other FS will cause a warning to be
generated,
# script to fail and a DA to abort
#
# 3) a synchronization with the Post-exec script should
be also
# provided because the snapshot FS must not be unmounted
while
# there is other DA reading from the FS.
#


SNAPPED_FS=$1
SNAPSHOT_FS=$2
MOUNT_POINT=$3


mount -F vxfs -e -o snapof=$SNAPPED_FS $SNAPSHOT_FS
$MOUNT_POINT


#
# end SnapMount.sh
#
```

以下に、VxFS ファイルシステムのアンマウントに使用するテンプレートの例を示します。

例 A-2　実行後スクリプトのテンプレート

```
# SnapUnmount.sh
#
# Unmounting snapshot filesystem (Post-exec shell
script)
#
# Script requires 1 parameter:
# - a mount point directory of the snapshot FS
# or
# - a block special file of the snapshot FS
#
# NOTE
# In case of multiple Disk Agents reading from the same
snapshot
# FS, a kind of synchronization mechanism has to be added
for
# the following reasons:
#
# 1} Post-exec script should unmount snapshot FS only if
there
# is no other DA reading from the snapshot FS
#
# Success/failure of the DA can be checked by examining
# the BDACC environment variable
#

MOUNT_POINT=$1

umount -v $MOUNT_POINT


#
# end SnapUnmount.sh
#
```

Data Protector のコマンド

Data Protector がサポートしているコマンドの全リストは、『HP OpenView Storage Data Protector コマンド行インタフェース・リファレンス』（CLIReference.pdf）、または UNIX の omniintro の man ページを参照してください。

『HP OpenView Storage Data Protector コマンド行インタフェース・リファレンス』は、*<Data_Protector_home>*¥docs¥MAN ディレクトリ（Windows の場合）、または /opt/omni/doc/C/ ディレクトリ（UNIX の場合）にあります。

このドキュメントが利用できるのは、ユーザー・インタフェース・コンポーネント（Windows の場合）、または OB2-DOCS コンポーネント（UNIX の場合）がインストールされている場合です。

UNIX の場合、コマンドの詳細については man *<command_name>* を使用してください。

性能に関する検討事項

この項では、バックアップ性能に影響を与える最も一般的な要素について概要を説明します。ただし性能自体については説明しません。変数とその組合せが非常に多数に及ぶため、ユーザーのあらゆる要件や投資レベルに応じた個別のアドバイスを行うことはできません。詳しくは、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

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 / 復元性能に多大な影響を与える要素です。並行データ・パスと処理速度の速い機器を使用することが最も重要なポイントとなります。

ネットワーク・バックアップ / 復元とローカル・バックアップ / 復元での比較

ネットワーク経由でデータを送信するとそれだけオーバーヘッドが加わり、ネットワークが性能に関する検討事項の一要素になります。以下のそれぞれのケースで、Data Protector によるデータ・ストリームの処理は異なります。

ネットワークのデータ・ストリーム

ディスク → メモリ → ネットワーク → メモリ → デバイス

ローカルのデータ・ストリーム

ディスク → メモリ → デバイス

最大限の性能を得るには、大量のデータ・ストリームを処理できるローカル・バックアップ構成を使用することをお勧めします。

デバイス

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

- DDS/DAT デバイスは、モデルによって異なりますが、圧縮を使用しない場合、
  通常 510 KB/ 秒～ 3 MB/ 秒の一定速度でデータの読取り / 書込みを行います。

- DLT デバイスは、モデルによって異なりますが、圧縮を使用しない場合、通常 1.5 MB/ 秒～ 6 MB/ 秒の一定速度でデータの読取り / 書込みを行います。
- LTO デバイスは、モデルによって異なりますが、圧縮を使用しない場合、通常 10 MB/ 秒～ 20 MB/ 秒の一定速度でデータの読取り / 書込みを行います。

上記の速度は、デバイスの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、このことが適用されるのはデバイスのストリーミングが行われている場合に限ります。

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

デバイス以外の高性能ハードウェア

コンピュータ・システム自体、つまりディスクの読取りとデバイスへの書込みは、性能に直接影響を与えます。システムは、ディスクを読み取るか、ソフトウェアによる圧縮 (展開) を行うことにより、バックアップ時にロードされます。

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

ハードウェアを並行して使用する

複数のデータ・パスを並行して使用することは、性能を向上させる上で基本的かつ効率的な方法です。ネットワークのインフラストラクチャもこれに含まれます。この方法は以下の状況で役立ちます。

- 複数の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。

- 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 台ある場合などです。この場合、system_A と system_B 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 がどのファイルシステムをどのデバイスにバックアップするかを動的に決定できる状態を指します。通常は、この機能を使用可能に設定しておくと最良の結果が得られます (特に、動的環境内で多数のファイルシステムをバックアップする場合)。

バックアップと復元の構成

どのようなインフラストラクチャが設定されている場合でも、最大の性能を得るため、それを効率的に使用しなければなりません。Data Protector を使えば、非常に柔軟に環境に対応できます。

デバイスのストリーミング

最大のデバイス性能を得るには、ストリーミングが維持されることが必要です。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。ネットワーク重視のバックアップ・インフラストラクチャでは、これは非常に意義があります。

複数の Disk Agent からのデータを 1 つの Media Agent へ送信して、Media Agent がデータをデバイスへ送信するようバックアップを設定できます。

ブロック・サイズ

デバイスは、デバイスの種類に固有のブロック・サイズを使って、受信したデータを処理します。Data Protector を使って、デバイスへ送信されるブロック・サイズを調整できます。デフォルト値は 64 KB です。

ブロック・サイズを大きくすることにより、性能が向上します。ブロック・サイズの変更は必ず、テープをフォーマットする**前に**行ってください。たとえば、デフォルトのブロック・サイズで書き込まれたテープには、別のブロック・サイズを指定してデータを追加することはできません。

[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。ソフトウェア圧縮によりネットワーク上を流れるデータ量は少なくなりますが、クライアントの CPU リソースが大量に消費されます。

注記

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だけ使用してください。これにより、データが圧縮された後ネットワークへ送信されます。ソフトウェア圧縮を使用した場合は必ず、ハードウェア圧縮を使用不可能にしてください。これは、データの圧縮を二重に行うと、逆にデータのサイズが大きくなるためです。

ハードウェア圧縮

ハードウェア圧縮はデバイスによって実行されます。デバイスは Media Agent クライアントからオリジナル・データを受信し、受信したデータを圧縮モードでテープに書き込みます。ハードウェア圧縮により、テープに書き込まれるデータの量が低減されるので、テープ・ドライブのデータ受信速度が向上します。

デフォルトでは、ハードウェア圧縮は使用可能に設定されています。ハードウェア圧縮を使用可能に設定するには、HP-UX および Solaris ではハードウェア圧縮デバイスファイルを選択し、Windows ではデバイス構成時にハードウェア圧縮オプションを選択します。ハードウェア圧縮を使用するかどうかは、慎重に決定してください。これは、圧縮モードで書き込まれたメディアは、非圧縮モードのデバイスで読み取ることができず、非圧縮モードで書き込まれたメディアは、圧縮モードのデバイスで読み取ることができないためです。

制限事項

HP Ultrium LTO ドライブでは自動的にハードウェア圧縮が行われ、この機能を使用不可能にすることはできません。したがって、HP Ultrium LTO ドライブを構成する際は、ソフトウェア圧縮を使用可能に設定しないようにしてください。

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。このため、フル・バックアップと増分バックアップのプランニングを行う際は、時間とリソースを十分に活用してください。ここで重要な注意点は、必要でない限りすべてのシステムのフル・バックアップを同じ日に実行しなくても構わないということです。詳しくは、『HP OpenView Storage Data Protector コンセプト・ガイド』を参照してください。

イメージ・バックアップ対ファイルシステム・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、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。これは、負荷の高いシステムや、ディスクに分散ファイルが多数含まれている場合には、現在も当てはまります。通常は、ファイルシステム・バックアップを使用することをお勧めします。

メディアへのオブジェクトの配布

オブジェクトの保存先メディアの構成方法には、以下に示すとおりさまざまな方法があります。例 :

- 1 つのオブジェクトを 1 つのメディアに保存する、または
- 複数のオブジェクトを複数のメディアに保存し、各メディアにそれぞれ 1 つのオブジェクトのデータを保存する

状況によっては、バックアップ性能を考慮した場合、保存先メディアが 1 つの方が都合が良い場合もありますが、これは最適な復元構成とはいえません。

したがって、(頻繁に実行される) バックアップを最適な状態で実行できるよう設定すると同時に、復元作業も円滑に行えるよう検討してください。

性能に関するその他のヒント

- パッチ

  性能に関連するパッチが、ネットワークにインストールされていることを確かめてください。

- Media Agent および Disk Agent クライアントとして機能しているコンピュータ上で、IP を以下のとおり設定します。

  ```
  IP is local "<MA_And_DA_Client_name>" == true
  ```

- LAN カード

  FDDI カードを使用している場合、このカードをバス上の上位に移動して、優先順位を上げることができます。ftp を使って MA と DA システム間で大容量ファイルを転送し、転送速度が Data Protector の性能と比べてどの程度違うか調べてみてください。半二重モードで構成されたネットワーク・カードを使用すると性能が低下します。

- 高速デバイスのシミュレーション

  テープ・デバイスへのデータ・フロー速度が遅い、またはデバイスがデータを正しく処理していない可能性がある場合は、Media Agent を使って、システム上で非常に高速なデバイスのシミュレーションを行うことができます。以下に手順を示します。

  1. スタンドアロン・ファイル・デバイスとデバイスファイル /dev/null (UNIX の場合) または nul (Windows の場合) を作成します。
  2. 別のプールを作成して、[Loose] ポリシーを選択します。
  3. InitOnLoosePolicy=1 に設定し、データ保護を [なし] に設定します。このデバイスに対するバックアップを実行して、実際のデバイスへのバックアップと比べてファイル・デバイスへバックアップした場合に性能に違いが見られるかを調べてください。また、ローカルで vbda を実行して、直接ファイルに書き込むこともできます。以下のコマンドを実行します。

     HP-UX および Solaris の場合 :

     ```
     /opt/omni/lbin/vbda -vol /home -trees /home/jdo -
     out /dev/null -profile
     ```

     Windows の場合 :

     ```
     <Data_Protector_home>¥bin¥vbda -vol /C -trees
     "/Program Files/OmniBack/bin" -out nul -profile
     ```

     Novell NetWare の場合 :

     ```
     load sys:usr¥omni¥bin¥hpvbda.nlm -vol /sys -tree
     /usr/omni -out ¥tmp¥test
     ```

- [デバイスの構成]

  必要に応じて、デバイスのブロック・サイズを調整します。

- CRC オプション

  CRC オプションを使用すると、Media Agent クライアントによって実行される CRC の計算のため、性能が影響を受ける可能性があります。

- ロギングとレポート・レベル

  IDB の更新に非常に時間がかかる場合は、[ログなし] に設定することにより、ロギングを使用不可能に設定します。同様に、レポート・レベルを [致命的] に設定することにより、メッセージにフィルタを設定できます。

- Data Protector アプリケーション・クライアント

  アプリケーション・クライアント (Oracle、SAP R/3) の復元セッションに非常に時間がかかる場合は、SmWaitforNewClient の値を小さくします (デフォルトは 5 分)。値をデフォルトより低く設定してください。

メディア取り出しのスケジュール例

夜間のバックアップに使用したすべてのメディアを毎朝 6:00 に取り出すことができます。このような取り出し動作のスケジュールを作成する手順を示します。

レポート・グループのスケジュール設定

1. Data Protector GUI で [レポート] を選択します。
2. Scoping ペインで [レポート] を展開して、[レポート] を右クリックします。[レポート・グループの追加] を選択します。 [レポート・グループの追加] ウィザードが表示されます。
3. ウィザードでレポート・グループに名前を付けて、[次へ] をクリックします。Data Protector スケジューラが表示されます。
4. スケジューラで開始日を選択して [追加] をクリックします。[レポートの配布をスケジュール] ダイアログ・ウィンドウで時間 (時) を指定して、レポートを毎日作成するよう指定します。[OK] をクリックした後、[完了] をクリックします。以上の手順により、レポート・グループのスケジュールが完了します。

   これで、レポートをレポート・グループに追加できるようになります。

レポート・グループにレポートを追加して構成する

1. [レポートの追加] ウィザードで [メディアとメディア・プールに関するレポート] を選択します。
2. [メディアのリスト] を選択して、レポートに名前を付けます。[次へ] をクリックします。
3. メディア・プールや位置に関係なく、**すべての**メディアを取り出すには、すべてのフィールドをデフォルト設定のままにしておきます。[次へ] を 4 回クリックします。
4. [相対時間] を選択し、[開始後経過時間] に 8 を、[継続期間] テキスト・ボックスに 8 をそれぞれ指定します。これにより、レポートの開始時点から起算して最後の 8 時間に行われたバックアップに使用されたメディアのみがレポートにリストされます。[次へ] をクリックします。

5. [形式] テキスト・ボックスで [タブ] を選択し、[送信方法] テキスト・ボックスで [外部] を選択します。[スクリプト] テキスト・ボックスに、スクリプトの名前 (HP-UX および Solaris システムの場合)、またはスクリプトを開始させるコマンドを含んだバッチ・ファイル (Windows システムの場合) の名前を入力します。スクリプトは、次項に記載しています。スクリプト (HP-UX および Solaris システム) または開始用バッチ・ファイル (Windows システム) は、/opt/omni/lbin (HP-UX および Solaris システム) または *<Data_Protector_home>*¥bin (Windows システム) ディレクトリに常駐している必要があります。

   Windows システムの場合、スクリプトを開始させるコマンドを含んだバッチ・ファイルの内容は、以下のとおりです。

   <perl_home>¥perl.exe
   "*<Data_Protector_home>*¥bin¥omnirpt_eject.pl"

6. この受信者を追加するには、[>>] ボタンをクリックします。[完了] をクリックします。

   以上の手順により、レポート・グループのスケジュールの設定と構成が完了します。

指定のディレクトリにスクリプトをコピーする

スクリプトをコピーまたは作成し、omnirpt_eject.pl という名前を付け、/opt/omni/lbin (HP-UX および Solaris システムの場合) または *<Data_Protector_home>*¥bin ディレクトリ (Windows システムの場合) に格納します。

```
#!/usr/contrib/bin/perl

#============================================================
========================

#   FUNCTION    Library_Eject

#

#   ARGUMENTS   param 1 = Library to eject from

#               param 2 = Slots to eject

#

#   DESCRIPTION Function ejects specified slots from
specified library
```

```
#=======================================================
=======================

sub Library_Eject {

    local ($lib,$slots)=@_;

    print "[Normal] Ejecting slot(s) ${slots}from
library ¥"$lib¥"¥n";

   print("[Normal] Executing ¥"${OMNIBIN}omnimm¥" -eject
¥"$lib¥" $slots¥n");

    $report =`"${OMNIBIN}omnimm" -eject ¥"$lib¥" $slots`;

    #print "¥debug>¥n$report¥n<debug¥n";

    if ($report !~/Final report: (¥d+) cartridges out of
(¥d+) successfully ejected¥./) {

        print "[Critical] Eject has
failed!¥n¥nReport:¥n$report¥n";

        return (1);

    }

    print "$report¥n";

    if ($1 ne $2) {

        print "[Warning] Not all media successfully
ejected!¥n";

        return (2);

    }

    print "[Normal] Eject from library ¥"$lib¥"
successfully completed.¥n";

    return (0);

}

#=======================================================
=======================

#   FUNCTION    Eject

#
```

```
#   ARGUMENTS   none
#
#   DESCRIPTION Function for each library in %List call
Library_Eject
#=========================================================
========================
sub Eject {
    local ($lib,$slot,$result);
    while (($lib, $slot) = each(%List)) {
        $result |=&Library_Eject($lib,$slot);
    }
    if ($result) {
        return (1);
    } else {
        print "[Normal] All operations successfully
completed.¥n";
        return (0);
    }
}
#=========================================================
========================
#   FUNCTION    Omnirpt
#
#   ARGUMENTS   none
#
#   DESCRIPTION Function get slots to eject from omnirpt
report
#=========================================================
========================
sub Omnirpt {
```

```
    @lines =<STDIN>;
    for ($i=5;$i<@lines;$i++) {
        @line =split(/¥t/,$lines[$i]);
        if ($line[2] =~/^¥[([¥w:¥-¥s]+):¥s+(¥w+)¥]/) {
            $List{$1}.=$2.'';  # $1= "Library name", $2=
"Slot ID"
        }
    }
    if (!keys(%List)) {
        print "[Warning] No tape(s) to eject.¥n";
        return (1);
    }
    return (0);

}
#-----------------------------------------------------------
-----------------
#                                   MAIN
#-----------------------------------------------------------
-----------------
if ($ENV{"OS"}=~/Windows/) {  # Windows NT
        $OMNIBIN ='c:¥¥program files¥¥omniback¥¥bin¥¥';
    } else {
        local($uname)=`uname -a`;
        chop $uname;
        @uname=split(' ', $uname);
        if ($uname[0]) {
            if ($uname [0] eq 'HP-UX') {
                $OMNIBIN ='/opt/omni/bin/';
```

```
            } else {
                $OMNIBIN ='/usr/omni/bin';
            }
        } else {
            exit (1);
        }
    }

    print "[Normal] Starting eject of media that have
been used in the last 24 hours.¥n";

    exit (0) if (&Omnirpt());
    exit (1) if (&Eject());
```

実行前 / 実行後コマンドの例 (UNIX の場合)

UNIX での実行前 / 実行後コマンドの例を以下に示します。

セッションの実行前コマンドの例 : アプリケーションのシャットダウン

Oracle インスタンスをシャットダウンするスクリプトの例を以下に示します。

```
#!/bin/sh
export ORACLE_HOME=$2
export ORACLE_SQLNET_NAME=$1
if [ -f $ORACLE_HOME/bin/svrmgrl ]; then
$ORACLE_HOME/bin/svrmgrl << EOF
connect sys/manager@$ORACLE_SQLNET_NAME as sysdba
shutdown
EOF
echo "Oracle database ¥"$ORACLE_SID¥" shut down."
exit 0
else
echo "Cannot find Oracle SVRMGRL
($ORACLE_HOME/bin/svrmgrl)."
exit 1
fi
```

ディスク・イメージの実行前コマンドの例: raw ボリューム・バックアップ前にディスクをアンマウントする

```
#!/bin/sh
echo "The disk will be now unmounted!"
umount /disk_with_many_files
if [ $? = 0 ]
then
echo "The disk has been successfully unmounted!"
exit 0
```

```
else
echo "Failed to unmount the disk --> ABORTED!"
exit 1
fi
```

ファイルシステムの実行前コマンドの例：ファイルシステムの使用状況を通知する

```
#!/bin/sh

echo
"================================================="
fuser -cu /var/application_mount_point
echo
"================================================="
exit 0
```

セッションの実行後コマンドの例：アプリケーションの起動

以下に、Oracle データベースを起動する実行後スクリプトの例を示します。

```
#!/bin/sh
export ORACLE_HOME=$2
export ORACLE_SQLNET_NAME=$1
if [ -f $ORACLE_HOME/bin/svrmgrl ]; then
        $ORACLE_HOME/bin/svrmgrl << EOF
connect sys/manager@$ORACLE_SQLNET_NAME as sysdba
startup
EOF
        echo "Oracle database ¥"$ORACLE_SID¥" started."
        exit 0
else
        echo "Cannot find Oracle SVRMGRL
($ORACLE_HOME/bin/svrmgrl)."
```

```
        exit 1
fi
```

ディスク・イメージの実行後コマンドの例: raw ボリューム・バックアップ後にディスクをマウントする

```
#!/bin/sh
if [ $BDACC != 0]
then
echo "Backup could not read the disk!"
echo "Disk will not be automatically mounted!"
fi
echo "The disk will be now mounted!"
mount /dev/vg05/lvol2 /disk_with_many_files
if [ $? = 0 ]
then
echo "Disk successfully mounted!"
exit 0
else
echo "Failed to mount disk!"
exit 1
fi
```

ファイルシステムの実行後コマンドの例: バックアップをログに記録する

```
#!/bin/sh
if  [ ! -f /etc/logfile ]
then
/etc/logfile
fi
echo "Backup finished with code $BDACC on " `date`
>>/etc/logfile
# We do not want a backup to be marked failed even if the
previous
action failed.
```

```
exit 0
```

セッションの実行後コマンドの例：ユーザーに通知する

```
#!/bin/sh
/opt/omni/bin/omnirpt -report single_session -session
$SESSIONID | ¥
 mailx -s "Report for $SESSIONID" $OWNER
```

セッションの実行後コマンドの例：次回のバックアップの開始

```
#!/bin/sh
# First check how the current backup finished
if [ $SMEXIT != 0 -o $SMEXIT != 10 ]
then
echo "Backup not successful --> next backup will not be
started!"
exit 0
fi
if  [ $RESTARTED != 0 ]
then
echo "Restarted backup --> next backup will not be
started!"
exit 0
fi
/opt/omni/bin/omnib -datalist BACKUP_NO_2 -no_mon
exit 0
```

セッションの実行後コマンドの例：失敗したバックアップの再開

```
#!/bin/sh
# First check how the current backup finished
if [ $SMEXIT != 0 -o $SMEXIT != 10 ]
then
echo "Backup not successful --> backup will not be
restarted!"
exit 0
fi
```

```
if  [ $RESTARTED != 0 ]
then
echo "Restarted backup --> backup will not be
restarted!"
exit 0
fi
/opt/omni/bin/omnib -restart $SESSIONID -no_mon
exit 0
```

障害復旧：
抹消リンクの移動 (HP-UX 11.x)

リンクを移動するには、バックアップ対象のシステム上で以下の手順を行います。

```
# The system will go from "run-level" 4 to "run-level 1"

# retaining the inetd, networking, swagentd services up. The
state is called "minimum activity" for backup purposes
(need networking).

# IMPORTANT: ensure the links are present in /sbin/rc1.d
before

# moving and they do have this exact name. You have to
rename them for the rc0.d directory. Put them BELOW the
lowest (original "/sbin/rc0.d/Kxx") "K...-link" in rc0.d

# Move K430dce K500inetd K660net K900swagentd into
../rc0.d BELOW the lowest kill link!!!

echo "may need to be modified for this system"

exit 1

#

cd /sbin/rc1.d

mv K430dce ../rc0.d/K109dce

mv K500inetd ../rc0.d/K110inetd

mv K660net ../rc0.d/K116net

mv K900swagentd ../rc0.d/K120swagentd
```

AIX 上での libaci.o の作成方法

OmniBack II および A.04.10

OmniBack II A.04.10 AIX 上の OmniBack II A.04.10 DAS Agent では、ライブラリ・オブジェクト・モジュール libaci.a を使用します。このモジュールは、同じ名前のライブラリ・アーカイブ・ファイルから作成する必要があります。

1. 以下の手順に従って、オブジェクト・モジュールを作成します。OmniBack II DAS Agent が使用するモジュールのリストを記述したファイル libaci.exp を以下のとおり作成します。

```
#! #! /usr/omni/lib/libaci.a
aci_initialize
aci_qversion
aci_init
d_errno
aci_view
aci_drivestatus
aci_drivestatus2
aci_driveaccess
aci_mount
aci_dismount
aci_qvolsrange
aci_eject_complete
aci_eject
aci_insert
```

2. 以下のコマンドを実行して、オブジェクト・モジュール libaci.o を作成します。

```
ld -L/usr/omni/lib -bM:SRE -e_nostart -lc
-bE:<DAS_PATH>/libaci.exp <DAS_PATH>/libaci.a -o libaci.o
```

   <DAS_PATH> には、ライブラリ・アーカイブ・ファイルの libaci.a ファイルと libaci.exp ファイルがあるディレクトリへのパスを入力します。

3. ライブラリ・オブジェクト・モジュール libaci.o をディレクトリ /usr/omni/lib にコピーして、名前を libaci.a に変更します。

重要

ライブラリ・アーカイブ・ファイルの絶対パスは *<DAS_PATH>*/libaci.a で、DAS Agent が使用するオブジェクト・モジュールの絶対パスは /usr/omni/lib/libaci.a です。

パッケージ構成ファイルの例

この項では、MC/ServiceGuard 環境内で Data Protector Cell Manager パッケージを構成するときのパッケージ構成ファイルの例を示します。

```
**********************************************************************
********

# ****** HIGH AVAILABILITY PACKAGE CONFIGURATION FILE
(template) *******

#
**********************************************************************
********

# ******* Note: This file MUST be edited before it can be used.
********

# * For complete details about package parameters and how to
set them, *

# * consult the MC/ServiceGuard or ServiceGuard OPS Edition
manpages   *

# * or manuals.
*

#
**********************************************************************
********


# Enter a name for this package.  This name will be used to
identify the

# package when viewing or manipulating it.  It must be
different from

# the other configured package names.


PACKAGE_NAME ob2cl



# Enter the failover policy for this package. This policy will
be used
```

```
# to select an adoptive node whenever the package needs to be
started.

# The default policy unless otherwise specified is
CONFIGURED_NODE.

# This policy will select nodes in priority order from the list
of

# NODE_NAME entries specified below.

#

# The alternative policy is MIN_PACKAGE_NODE. This policy will
select

# the node, from the list of NODE_NAME entries below, which is

# running the least number of packages at the time this package
needs

# to start.


FAILOVER_POLICY CONFIGURED_NODE



# Enter the failback policy for this package. This policy will
be used

# to determine what action to take when a package is not
running on

# its primary node and its primary node is capable of running
the

# package. The default policy unless otherwise specified is
MANUAL.

# The MANUAL policy means no attempt will be made to move the
package

# back to its primary node when it is running on an adoptive
node.

#

# The alternative policy is AUTOMATIC. This policy will attempt
to

# move the package back to its primary node whenever the
primary node
```

```
# is capable of running the package.


FAILBACK_POLICY MANUAL



# Enter the names of the nodes configured for this package.
Repeat

# this line as necessary for additional adoptive nodes.

# Order IS relevant.  Put the second Adoptive Node AFTER the
first

# one.

# Example : NODE_NAME  original_node

#           NODE_NAME  adoptive_node


NODE_NAME partizan

NODE_NAME lyon



# Enter the complete path for the run and halt scripts.  In
most cases

# the run script and halt script specified here will be the
same script,

# the package control script generated by the cmmakepkg
command.  This

# control script handles the run(ning) and halt(ing) of the
package.

# If the script has not completed by the specified timeout
value,

# it will be terminated.  The default for each script timeout
is

# NO_TIMEOUT.  Adjust the timeouts as necessary to permit full

# execution of each script.
```

```
# Note: The HALT_SCRIPT_TIMEOUT should be greater than the sum
of
# all SERVICE_HALT_TIMEOUT specified for all services.

RUN_SCRIPT /etc/cmcluster/ob2cl/ob2cl.cntl
RUN_SCRIPT_TIMEOUT NO_TIMEOUT
HALT_SCRIPT /etc/cmcluster/ob2cl/ob2cl.cntl
HALT_SCRIPT_TIMEOUT NO_TIMEOUT



# Enter the SERVICE_NAME, the SERVICE_FAIL_FAST_ENABLED and the
# SERVICE_HALT_TIMEOUT values for this package.  Repeat these
# three lines as necessary for additional service names. All
# service names MUST correspond to the service names used by
# cmrunserv and cmhaltserv commands in the run and halt
scripts.
#
# The value for SERVICE_FAIL_FAST_ENABLED can be either YES or
# NO.  If set to YES, in the event of a service failure, the
# cluster software will halt the node on which the service is
# running.  If SERVICE_FAIL_FAST_ENABLED is not specified, the
# default will be NO.
#
# SERVICE_HALT_TIMEOUT is represented in the number of seconds.
# This timeout is used to determine the length of time (in
# seconds) the cluster software will wait for the service to
# halt before a SIGKILL signal is sent to force the termination
# of the service.  In the event of a service halt, the cluster
# software will first send a SIGTERM signal to terminate the
# service.  If the service does not halt, after waiting for the
```

```
# specified SERVICE_HALT_TIMEOUT, the cluster software will
send

# out the SIGKILL signal to the service to force its
termination.

# This timeout value should be large enough to allow all
cleanup

# processes associated with the service to complete.  If the

# SERVICE_HALT_TIMEOUT is not specified, a zero timeout will be

# assumed, meaning the cluster software will not wait at all

# before sending the SIGKILL signal to halt the service.

#

# Example : SERVICE_NAME                  DB_SERVICE

#           SERVICE_FAIL_FAST_ENABLED     NO

#           SERVICE_HALT_TIMEOUT          300

#

# To configure a service, uncomment the following lines and

# fill in the values for all of the keywords.

#

#SERVICE_NAME                   <service name>

#SERVICE_FAIL_FAST_ENABLED      <YES/NO>

#SERVICE_HALT_TIMEOUT           <number of seconds>


SERVICE_NAME                   omni_sv

SERVICE_FAIL_FAST_ENABLED       NO

SERVICE_HALT_TIMEOUT           300



# Enter the network subnet name that is to be monitored for
this package.

# Repeat this line as necessary for additional subnet names.
If any of
```

```
# the subnets defined goes down, the package will be switched
to another

# node that is configured for this package and has all the
defined subnets

# available.


SUBNET 10.17.0.0



# The keywords RESOURCE_NAME, RESOURCE_POLLING_INTERVAL,

# RESOURCE_START, and RESOURCE_UP_VALUE are used to specify
Package

# Resource Dependencies.  To define a package Resource
Dependency, a

# RESOURCE_NAME line with a fully qualified resource path name,
and

# one or more RESOURCE_UP_VALUE lines are required.  The

# RESOURCE_POLLING_INTERVAL and the RESOURCE_START are
optional.

#

# The RESOURCE_POLLING_INTERVAL indicates how often, in
seconds, the

# resource is to be monitored.  It will be defaulted to 60
seconds if

# RESOURCE_POLLING_INTERVAL is not specified.

#

# The RESOURCE_START option can be set to either AUTOMATIC or
DEFERRED.

# The default setting for RESOURCE_START is AUTOMATIC.  If
AUTOMATIC

# is specified, ServiceGuard will start up resource monitoring
for

# these AUTOMATIC resources automatically when the node starts
up.
```

```
# If DEFERRED is selected, ServiceGuard will not attempt to
start

# resource monitoring for these resources during node start up.
User

# should specify all the DEFERRED resources in the package run
script

# so that these DEFERRED resources will be started up from the
package

# run script during package run time.

#

# RESOURCE_UP_VALUE requires an operator and a value.  This
defines

# the resource 'UP' condition.  The operators are =, !=, <, >,
>=,

# and <=, depending on the type of value.  Values can be string
or

# numeric.  If the type is string, then only = and != are valid

# operators.  If the string contains whitespace, it must be
enclosed

# in quotes.  String values are case sensitive.  For example,

#

# Resource is up when its value is

# --------------------------------

# RESOURCE_UP_VALUE= UP"UP"

# RESOURCE_UP_VALUE!= DOWNAny value except "DOWN"

# RESOURCE_UP_VALUE= "On Course""On Course"

#

# If the type is numeric, then it can specify a threshold, or a
range to

# define a resource up condition.  If it is a threshold, then
any operator

# may be used.  If a range is to be specified, then only > or
>= may be used
```

```
# for the first operator, and only < or <= may be used for the
second operator.

# For example,

# Resource is up when its value is

# --------------------------------

# RESOURCE_UP_VALUE     = 55    (threshold)

# RESOURCE_UP_VALUE     > 5.1greater than 5.1    (threshold)

# RESOURCE_UP_VALUE     > -5 and < 10between -5 and 10
(range)

#

# Note that "and" is required between the lower limit and upper
limit

# when specifying a range.  The upper limit must be greater
than the lower

# limit.  If RESOURCE_UP_VALUE is repeated within a
RESOURCE_NAME block, then

# they are inclusively OR'd together.  Package Resource
Dependencies may be

# defined by repeating the entire RESOURCE_NAME block.

#

# Example : RESOURCE_NAME
/net/interfaces/lan/status/lan0

#     RESOURCE_POLLING_INTERVAL120

#     RESOURCE_STARTAUTOMATIC

#     RESOURCE_UP_VALUE= RUNNING

#     RESOURCE_UP_VALUE= ONLINE

#

#           Means that the value of resource
/net/interfaces/lan/status/lan0

#          will be checked every 120 seconds, and is considered
to

#           be 'up' when its value is "RUNNING" or "ONLINE".

#
```

```
# Uncomment the following lines to specify Package Resource
Dependencies.

#

#RESOURCE_NAME    <Full_path_name>

#RESOURCE_POLLING_INTERVAL  <numeric_seconds>

#RESOURCE_START             <AUTOMATIC/DEFERRED>

#RESOURCE_UP_VALUE    <op> <string_or_numeric> [and <op>
<numeric>]



# The default for PKG_SWITCHING_ENABLED is YES. In the event of
a

# failure, this permits the cluster software to transfer the
package

# to an adoptive node.  Adjust as necessary.


PKG_SWITCHING_ENABLED YES



# The default for NET_SWITCHING_ENABLED is YES.  In the event
of a

# failure, this permits the cluster software to switch LANs
locally

# (transfer to a standby LAN card).  Adjust as necessary.


NET_SWITCHING_ENABLED YES



# The default for NODE_FAIL_FAST_ENABLED is NO.  If set to YES,

# in the event of a failure, the cluster software will halt the
node

# on which the package is running.  Adjust as necessary.
```

```
NODE_FAIL_FAST_ENABLEDNO
```

パッケージ制御ファイルの例

この項では、MC/ServiceGuard 環境内で Data Protector Cell Manager パッケージを構成するときのパッケージ制御ファイルの例を示します。

```
**********************************************************************
********

# *
*

# *       HIGH AVAILABILITY PACKAGE CONTROL SCRIPT (template)
*

# *
*

# *      Note: This file MUST be edited before it can be used.
*

# *
*

#
**********************************************************************
********


# UNCOMMENT the variables as you set them.


# Set PATH to reference the appropriate directories.

PATH=/usr/bin:/usr/sbin:/etc:/bin


# VOLUME GROUP ACTIVATION:

# Specify the method of activation for volume groups.

# Leave the default ("VGCHANGE="vgchange -a e") if you want
volume

# groups activated in exclusive mode. This assumes the volume
groups have

# been initialized with 'vgchange -c y' at the time of
creation.
```

```
#
# Uncomment the first line (VGCHANGE="vgchange -a e -q n"), and
comment
# out the default, if your disks are mirrored on separate
physical paths,
#
# Uncomment the second line (VGCHANGE="vgchange -a e -q n -s"),
and comment
# out the default, if your disks are mirrored on separate
physical paths,
# and you want the mirror resynchronization to occur in
parallel with
# the package startup.
#
# Uncomment the third line (VGCHANGE="vgchange -a y") if you
wish to
# use non-exclusive activation mode. Single node cluster
configurations
# must use non-exclusive activation.
#
# VGCHANGE="vgchange -a e -q n"
# VGCHANGE="vgchange -a e -q n -s"
#VGCHANGE="vgchange -a y"
VGCHANGE="vgchange -a e"# Default


# VOLUME GROUPS
# Specify which volume groups are used by this package.
Uncomment VG[0]=""
# and fill in the name of your first volume group. You must
begin with
# VG[0], and increment the list in sequence.
#
```

```
# For example, if this package uses your volume groups vg01 and
vg02, enter:

#         VG[0]=vg01

#         VG[1]=vg02

#

# The volume group activation method is defined above. The
filesystems

# associated with these volume groups are specified below.

#

VG[0]=/dev/vg_ob2cm


# FILESYSTEMS

# Specify the filesystems which are used by this package.
Uncomment

# LV[0]=""; FS[0]=""; FS_MOUNT_OPT[0]="" and fill in the name
of your first

# logical volume, filesystem and mount option for the file
system. You must

# begin with LV[0], FS[0] and FS_MOUNT_OPT[0] and increment the
list in

# sequence.

#

# For example, if this package uses the file systems pkg1a and
pkg1b,

# which are mounted on the logical volumes lvol1 and lvol2 with
read and

# write options enter:

#          LV[0]=/dev/vg01/lvol1; FS[0]=/pkg1a;
FS_MOUNT_OPT[0]="-o rw"

#          LV[1]=/dev/vg01/lvol2; FS[1]=/pkg1b;
FS_MOUNT_OPT[1]="-o rw"

#

# The filesystems are defined as triplets of entries specifying
the logical
```

```
# volume, the mount point and the mount options for the file
system. Each

# filesystem will be fsck'd prior to being mounted. The
filesystems will be

# mounted in the order specified during package startup and
will be unmounted

# in reverse order during package shutdown. Ensure that volume
groups

# referenced by the logical volume definitions below are
included in

# volume group definitions above.

#

#LV[0]=""; FS[0]=""; FS_MOUNT_OPT[0]=""


LV[0]=/dev/vg_ob2cm/lv_ob2cm

FS[0]=/omni_shared

FS_MOUNT_OPT[0]=""


# FILESYSTEM UNMOUNT COUNT

# Specify the number of unmount attempts for each filesystem
during package

# shutdown.  The default is set to 1.

FS_UMOUNT_COUNT=2


# IP ADDRESSES

# Specify the IP and Subnet address pairs which are used by
this package.

# Uncomment IP[0]="" and SUBNET[0]="" and fill in the name of
your first

# IP and subnet address. You must begin with IP[0] and
SUBNET[0] and

# increment the list in sequence.

#
```

```
# For example, if this package uses an IP of 192.10.25.12 and a
subnet of

# 192.10.25.0 enter:

#          IP[0]=192.10.25.12

#          SUBNET[0]=192.10.25.0 # (netmask=255.255.255.0)

#

# Hint: Run "netstat -i" to see the available subnets in the
Network field.

#

# IP/Subnet address pairs for each IP address you want to add
to a subnet

# interface card.  Must be set in pairs, even for IP addresses
on the same

# subnet.

#

IP[0]=10.17.3.230

SUBNET[0]=10.17.0.0


# SERVICE NAMES AND COMMANDS.

# Specify the service name, command, and restart parameters
which are

# used by this package. Uncomment SERVICE_NAME[0]="",
SERVICE_CMD[0]="",

# SERVICE_RESTART[0]="" and fill in the name of the first
service, command,

# and restart parameters. You must begin with SERVICE_NAME[0],
SERVICE_CMD[0],

# and SERVICE_RESTART[0] and increment the list in sequence.

#

# For example:

#          SERVICE_NAME[0]=pkg1a

#          SERVICE_CMD[0]="/usr/bin/X11/xclock -display
192.10.25.54:0"
```

```
#          SERVICE_RESTART[0]=""  # Will not restart the
service.

#

#          SERVICE_NAME[1]=pkg1b

#          SERVICE_CMD[1]="/usr/bin/X11/xload -display
192.10.25.54:0"

#          SERVICE_RESTART[1]="-r 2"   # Will restart the
service twice.

#

#          SERVICE_NAME[2]=pkg1c

#          SERVICE_CMD[2]="/usr/sbin/ping"

#         SERVICE_RESTART[2]="-r 1" # Will restart the service
an infinite

#                                      number of times.

#

# Note: No environmental variables will be passed to the
command, this

# includes the PATH variable. Absolute path names are required
for the

# service command definition.  Default shell is /usr/bin/sh.

#

SERVICE_NAME[0]=omni_sv

SERVICE_CMD [0] = "/etc/opt/omni/server/sg/csfailover.ksh
start"

SERVICE_RESTART[0]="-r 2"
```

Data Protector ログ・ファイルの主なエントリ

本項では、いくつかの Data Protector ログ・ファイルに記録される主な Data Protector メッセージを示します。ただしここでは、トラブルシューティングに関する詳しい情報は記載していません。Data Protector ログ・ファイルの全リストと、ログ・ファイルの詳しい内容については、「Data Protector ログ・ファイル」(681 ページ) を参照してください。

重要

Data Protector ログ・ファイルのエントリの内容と形式は変更される場合があります。

debug.log

```
02/11/00 12:22:01  OMNIRPT.23856.0
["/src/lib/cmn/obstr.c /main/r31_split/2":212] A.03.10
b325

  StrFromUserSessionId: "-detail": not in correct format


03/01/00 14:19:28  DBSM.21294.0
["PANSRC/db/RCS/cmn_srv.c,v 1.40":229] A.03.10 b325

  DB[1] internal error [9] cannot exclusively open
database, it is already opened


03/01/00 14:21:14  DBSM.21393.0
["PANSRC/db/RCS/cmn_srv.c,v 1.40":272] A.03.10 b325

  CDB cell server "bmw" different than current host
"bmw.hermes"


03/01/00 14:21:43  OMNIB.21471.0 ["/src/cli/omnibackup.c
/main/23":2585] A.03.10 b325

 [Process] CanBackup failed!
```

```
03/02/00 09:36:51  INET.26130.0 ["/src/lib/ipc/ipc.c
/main/r31_split/10":6920] A.03.10 b325

IpcGetPeer: Could not expand ConnectionIP "10.17.6.227"


03/16/00 19:09:42  BSM.13152.0 ["src/db/cdb/cdbwrap.c
/main/84":1538] A.03.10 bPHSS_21234/PHSS_21235

  DB[1] internal error [-2009] The session is
disconnected


05/17/01 12:00:30  OMNIMM.7515.0 ["lib/cmn/obstr.c
/main/17":187] A.04.00.%B3 b335

  StrToUserSessionId: "0": not in correct format


5/14/01 11:08:53 AM  UPGRADE_CFG.357.356
["integ/barutil/upgrade_cfg/upgrade_cfg.c
/main/27":1472] A.04.00.%B3 b335

 [UpgradeSQL] Can not read registry value
HKLM¥Software¥Hewlett-Packard¥OpenView¥OmniBackII¥Agents
¥MS-SQL70¥saUser

[UpgradeSQL] Warning:  2, The system cannot find the
file specified.


5/14/01 11:08:54 AM  UPGRADE_CFG.369.368
["integ/barutil/upgrade_cfg/upgrade_cfg.c /main/27":154]
A.04.00.%B3 b335

[GetConfig] Can not read configuration from Cell Server
"brainiac.hermes" with integration "Oracle" and instance
"_OB2_GLOBAL"

[GetConfig] Error: 1012, [12:1012] Can not access the
file.

システム・エラー : [2] The system cannot find the file
specified.
```

```
5/14/01 12:41:41 PM  OMNIDBUTIL.98.124
["db/vel_cls_spec.c /main/39":103] A.04.00.%B3 b335

  VELOCIS DB ERROR [0] internal error [-2005] Server
unavailable
```

sm.log

```
3/28/00 03:00:01  BSM.23475.0 ["/src/sm/bsm2/brsmutil.c
/main/r31_split/4":630] A.03.50.%B2 b158

Error connecting to database. Code: 1166.


03/27/01 08:17:06  BSM.2709.0 ["sm/bsm2/bsmutil.c
/main/502":3306] A.04.00.%B1 b281

Error opening datalist OMNIBACK-.
```

inet.log

```
5/15/01 12:19:54 AM  INET.119.122 ["inetnt/allow_deny.c
/main/10":524] A.04.00.%B3 b335

A request 3 came from host bmw.hermes which is not a Cell
Manager of this client


[Critical] From: INET@clio.hermes "clio.hermes"  Time:
03/29/01 09:48:29

[70:5]  Cannot execute '/opt/omni/lbin/ob2rman.exe' (No
such file or directory) => aborting
```

media.log

```
02/04/00 06:57:46 0a110210:3861cbbb:742d:0003 "[CBF492]
BMW_DLT_23" [2000/02/04-8] OmniDB


02/04/00 07:02:38 0a110210:3861cbbb:742d:0003 "[CBF492]
BMW_DLT_23" [2000/02/04-9]
```

```
02/04/00 13:38:56 0a110210:389ac85b:3c6e:0001 "[CBF502]
DLT_ARC_8" [INITIALIZATION]


02/29/00 16:04:25 0a110210:38bbdff4:6d85:0026 "NULL_33"
[AUTOINITIALIZATION]


03/02/00 10:03:25 0a110210:385a24bf:410b:0002 "[CW1231]
BMW_DLT_15" [IMPORT]
```

upgrade.log

```
03/15/01 09:15:38

UCP session started.


03/15/01 09:20:55

UCP session finished.

total running time: 317 秒


03/15/01 10:00:09

UDP session started.


03/15/01 10:02:54

Abort request from CLI/GUI on handle 0. Terminating
session


03/15/01 10:03:06

UDP session started.


03/15/01 10:26:47
```

```
Abort request from CLI/GUI on handle 0. Terminating
session

03/15/01 12:40:43

Database check error! Can not proceed with upgrade.

03/15/01 13:24:15

System error

03/15/01 13:24:15

Session was aborted by child ASM, marked error=1026

03/15/01 15:27:22

OmniBack II 3.x database not found.

03/15/01 16:33:19

[12:10904] Open of detail catalog binary file failed.

03/16/01 08:39:31

Internal error: Invalid Ct function argument specified.

03/20/01 10:56:57

[12:1165] Database network communication error.

03/22/01 14:38:21

 [12:10953] Database is in incorrect state. Database
must be empty before critical upgrade can start.
```

Windows での手動による障害復旧準備用テンプレート

次ページに示すテンプレートは、第 12 章「障害復旧」(545 ページ) で説明している Windows での半自動障害復旧に備えてお使いください。

表 A-1

クライアントのプロパティ	コンピュータ名	
	ホスト名	
ドライバ		
Windows Service Pack		
TCP/IP のプロパティ	IP アドレス	
	デフォルト・ゲートウェイ	
	サブネット・マスク	
	DNS の順序	
メディア・ラベル / バーコード番号		
パーティション情報と順序	第 1 ディスクのラベル	
	第 1 パーティションの長さ	
	第 1 ドライブの文字	
	第 1 ファイルシステム	
	第 2 ディスクのラベル	
	第 2 パーティションの長さ	
	第 2 ドライブの文字	
	第 2 ファイルシステム	
	第 3 ディスクのラベル	
	第 3 パーティションの長さ	
	第 3 ドライブの文字	
	第 3 ファイルシステム	

Windows Media Agent 上のブロック・サイズの変更

Windows Media Agent クライアント上でブロック・サイズの最大値を増やす場合は、レジストリを変更する必要があります。レジストリを変更した後、コンピュータを再起動してください。起動時にドライバが MaximumSGList を読み込みます。Windows クラス・ドライバが最大転送サイズの算出に使用する式を以下に示します。

最大サイズ = ((サポートされる scatter/gather element 数 - 1)*4096)

代表的な aic78xx の場合、以下のようになります。

((17-1) * 4096) = 64k

Windows は、レジストリを介してより多くの scatter/gather element をサポートする機構を備えています。regedt32 を起動し、以下のレジストリ・キーで DWORD 値を追加してください。

¥¥HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥aic78xx¥Parameters¥Device0¥MaximumSGList

以下の式を使って MaximumSGList の値を算出します。

$$\text{MaximumSGList} = \left(\frac{\text{BlockSize}}{4096}\right) + 1$$

例

ブロック・サイズが 256k の場合、MaximumSGList の値は以下に示すとおり 65 となります。

MaximumSGList = (265k/4k) + 1 = 64 + 1 = 65

たとえば、システムに 3 つの aic78xx ベースの SCSI チャンネルがある場合は、チャンネルに応じた値（...¥Device0、...¥Device1、または ...¥Device2 など）に変更してください。すべてのアダプタを同時に設定する場合は、...¥Device¥... に MaximumSGList を設定してください。数値参照を省略すると、すべての aic78xx アダプタに対してこの値が設定されます。

B スタンドアロン・ファイル・デバイスとファイルジュークボックス デバイス

本付録の概略

本付録では、Data Protector を使用したバックアップ・ソリューションとして、スタンドアロン・ファイル・デバイスおよびファイル ジュークボックス デバイスを構成および使用する方法を簡単に紹介します。以下の項目について説明します。

「スタンドアロン・ファイル・デバイスとファイル ジュークボックス デバイスの概要」(B-3 ページ)

「推奨される構成」(B-4 ページ)

「スタンドアロン・ファイル・デバイスとファイル ジュークボックス デバイスの構成」(B-7 ページ)

「スタンドアロン・ファイル・デバイスまたはファイル ジュークボックス デバイスを使用したバックアップと復元」(B-9 ページ)

スタンドアロン・ファイル・デバイスとファイル ジュークボックス デバイ

スタンドアロン・ファイル・デバイスとファイル ジュークボックス デバイスの概要

スタンドアロン・ファイル・デバイスとファイル ジュークボックス デバイスは、ディスクへのデータ・バックアップを目的に設計されたデバイスの一種です。この種のデバイスには、以下のようなタイプがあります。

- 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・デバイスとファイル ジュークボックス デバイスは、ファイル・ライブラリ・デバイスよりも構造が単純で、小規模なバックアップに適しています。高度な機能を持つファイル・ライブラリ・デバイスの詳細は、第 3 章「ディスクベースのデバイスの 構成と使用」(109 ページ) を参照してください。

スタンドアロン・ファイル・デバイスには、最大 1GB のデータを保存できます。このデバイスはいったん作成した後で再構成することはできません。

ファイル ジュークボックス デバイスにはより多くのデータを保存できます (最大 1TB)。ファイル ジュークボックス デバイスの場合は、デバイスをいったん作成した後でも、構成の制御や変更が可能です。

どちらのデバイスの場合も、データはディスク上にファイル形式で保存されます。これらのファイルは、テープ・デバイス内のスロットに相当します。スタンドアロン・ファイル・デバイス内には 1 つのスロットしかありません。ファイル ジュークボックス デバイス内には複数のスロットが存在します。

これらのデバイスにバックアップされるデータは、保存前にまずテープ形式に変換されます。

スタンドアロン・ファイル・デバイスとファイル ジュークボックス デバイスの作成および構成には、Data Protector GUI を使用します。

推奨される構成

デバイスの位置

これらのデバイスは、IDB があるディスクとは別のディスク上に作成することをお勧めします。こうすることで、データベース用に十分なディスク・スペースを確保することができます。デバイスと内部データベースを別のディスクに置くことで、性能も向上します。

デバイスと Data Protector 内部データベースを同じディスクに置く場合は、いずれのためにも十分なスペースがあることを確認する必要があります。詳細については、「今後の使用を考えてディスク・スペースを割り当てる」(494 ページ) を参照してください。

ディスク上のデバイス数

同じディスクに対して読み込みまたは書き込みされるデータ・ストリームが複数ある場合、つまり複数の Disk Agent または Media Agent が同じマウント・ポイントを同時にアクセスして、そのマウント・ポイントが 1 つのディスクとして定義されている場合、そのディスクに対する読み込み / 書き込み性能は大きく低下します。

したがって、1 つのディスク上にはスタンドアロン・ファイル・デバイスまたはファイル ジュークボックス デバイスを 1 つだけ作成し、さらに 1 つのデバイスあたり 1 つのドライブだけを作成するようにします。また Data Protector によるバックアップや復元中は、他のアプリケーションが大量のデータをそのディスクに、またはそのディスクから転送しないようにすることをお勧めします。ディスク・アレイを使用すれば、性能の低下を避けることができます。

スロット・サイズ

大量のデータ (1GB 以上) をバックアップする場合は、スタンドアロン・ファイル・デバイスではなく、ファイル ジュークボックス デバイスを使用することをお勧めします。ファイル ジュークボックス デバイスの方が柔軟性に優れており、制御も容易です。

一般に、構成すべきデバイスのサイズはバックアップするデータ量に依存します。ただし、通常スタンドアロン・ファイル・デバイス / スロットのサイズは、Windows の場合は 100MB ～ 50GB に、UNIX の場合は 100MB ～ 2TB に設定することをお勧めします。

たとえば、1TB のデータをバックアップする場合であれば、以下のようなデバイス構成が可能です。

Windows システムの場合 10GB のファイル・スロットを 100 個持つファイル ジュークボックス デバイスを 1 つ

UNIX システムの場合 4GB のファイル・スロットを 250 個持つファイル ジュークボックス デバイスを 1 つ

データ保護は、ファイル ジュークボックス内の各ファイル・スロットに対して設定されるため、この保護を解除することで一つのスロットをリサイクルすることが可能です。したがって、小さなスロットを複数作成すれば柔軟性が増し、より効率的なデータ保護とスペース維持管理が可能になります。

以下のサイズをお勧めします (もちろん、小規模バックアップなど、必要に応じてこの数字を変えることができます)。ライセンス契約への影響については、HP OpenView Storage Data Protector インストールおよびライセンス・ガイドを参照してください。

表 B-1 Windows および UNIX 上で推奨されるスロット・サイズ

使用可能なディスク・スペース	スロットの数	スロット・サイズ (GB)
1TB	100	10
5TB	250	20
10TB	250	40

ブロック・サイズ

スタンドアロン・ファイル・デバイスとファイル ジュークボックス デバイスは効率的な高速デバイスで、テープ・バックアップの代わりに使用されます。このため、これらのデバイスへのデータ書き込みには、テープへの書き込み形式が使用されます。この形式を使用する場合に考慮が必要な主なパラメータは以下のとおりです。

- **ブロック・サイズ**: これはテープ・デバイスの名残です。異なるベンダーのテープ・ドライブは、多くの場合異なるブロック・サイズを使用します。

  通常、スタンドアロン・ファイル・デバイスやファイル ジュークボックス デバイス内の各ドライブでは、同じブロック・サイズを使用してください。そうしないと、あるドライブを使用して書き込まれたスタンドアロン・ファイル・デバイス / スロットが、他のドライブを使用した場合に認識されないことがあります。デフォルトのブロック・サイズは 64KB です。

- セグメント・サイズ : このパラメータには、バックアップ・データを記録するときの、ファイル・マーク間のデータ量を設定します。ファイル・デバイス / スロットのヘッダには、各セグメントのファイル・マーク位置を記録したファイル・マーク・テーブルも書き込まれます。

Windows 上でのスロットの最大推奨サイズは 50GB です。ただし、Windows 上では最大 600GB のスロットを使用して、ファイル ジュークボックス デバイスのテストが行われています。Unix 上でのスロットの最大推奨サイズは 2TB です。

ファイル・デバイス内のブロックやセグメントのサイズを設定する方法の詳細については、オンライン・ヘルプの索引キーワード「拡張オプション , デバイス & メディア」を参照してください。

スタンドアロン・ファイル・デバイスとファイル ジュークボックス デバイスの構成

必要条件

Windows システム上でこれらのデバイスを構成するときは、まず圧縮オプションをオフにしてください。この操作は Windows エクスプローラから実行できます。データのバックアップ先となるディレクトリを右クリックして [プロパティ] を選択し、[属性] の下の [圧縮] を選択解除してください。[圧縮] が選択されていると、Data Protector はそのデバイスへの書き込みができません。

重要

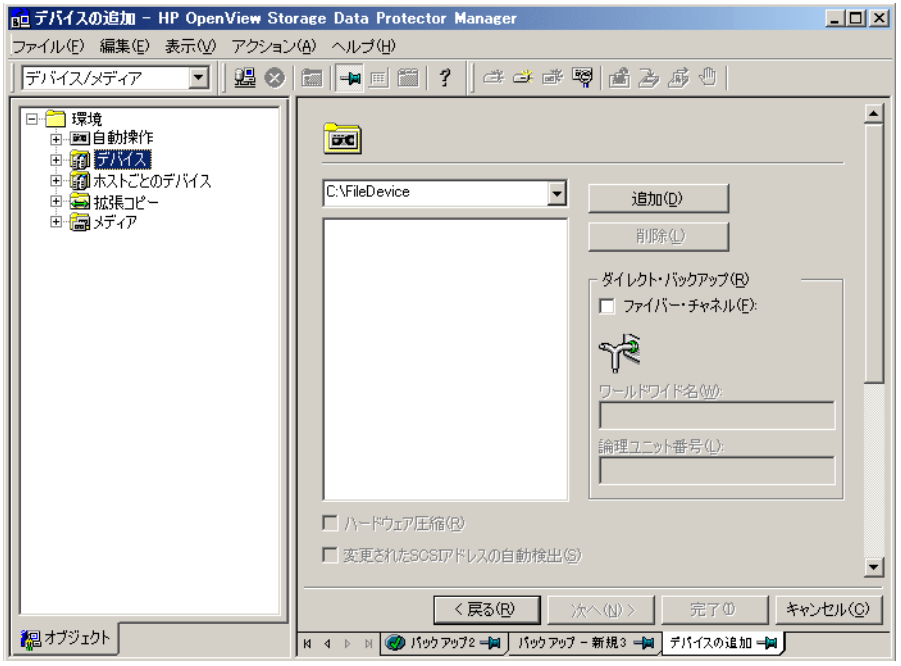
デバイスを構成するときに、既存のデバイス名は使用しないでください。同じ名前を使用すると、既存のデバイスが上書きされてしまいます。

複数のデバイスを構成するときに、同じデバイス名は使用しないでください。同じ名前を使用すると、アクセスされるたびにデバイスが上書きされてしまいます。

デバイスの構成

これらのデバイスを作成するには、[デバイスの追加] ウィザードで、デバイスの種類として [スタンドアロン] または [ジュークボックス] を選択してください。デバイス・アドレスには、デバイスのパス名を指定します (C:¥My_Backup など)。詳細は、図 B-1 を参照してください。構成作業の詳細については、オンライン・ヘルプの索引キーワード「構成 - スタンドアロン・デバイス」または「構成 - ファイル・ジュークボックス・デバイス」を参照してください。

図 B-1 **デバイス・パスの設定**



次の手順

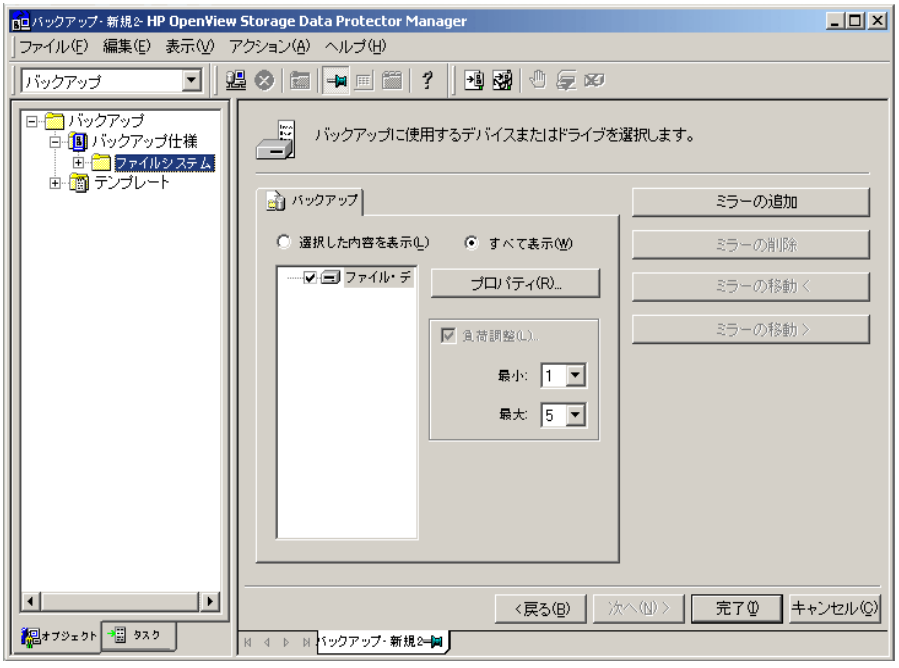
以上で、デバイスを Data Protector で使用するための設定は終了ですが、デバイスはディスク上にまだ存在していません。デバイスをバックアップに使用するためには、最初にデバイスをフォーマットする必要があります。詳細な手順については、オンライン・ヘルプの索引キーワード「フォーマット - ライブラリ・デバイス内のメディア」(ジュークボックス ファイル デバイスの場合)、または「フォーマット - メディア」(スタンドアロン・ファイル・デバイスの場合) を参照してください。

スタンドアロン・ファイル・デバイスまたはファイル ジュークボックス デバイスを使用したバックアップと復元

スタンドアロン・ファイル・デバイスまたはファイル ジュークボックス デバイスへのバックアップ

標準的なバックアップ仕様内で、バックアップ先のデバイスとして、目的のスタンドアロン・ファイル・デバイスを指定します。

図 B-2 **スタンドアロン・ファイル・デバイスまたはファイル ジュークボックス デバイスへのバックアップ**



デバイスが新規作成されたファイル ジュークボックスの場合、Data Protector は最初のファイル・スロットを使用します。バックアップに使用されたことがあるファイル ジュークボックスの場合、Data Protector は前回のバックアップで使用したのと同じファイル・スロットを使用し、そのスロットにデータを書き込みます。スロットがいっぱいになった場合は、次のファイル・スロットを使用してバックアップが継続されます。

このプロセスはすべてのスロットがいっぱいになるまで繰り返されます。その時点で書き込むべきバックアップ・データがまだ残っている場合、Data Protector はリサイクルされているファイル・スロットを探し、検出されればそのスロットを使用してバックアップを継続します。スロットが見つからなければ、マウント要求が発行されます。この場合、バックアップを続行するには、スロットにリサイクル・マークを付加するか新しいファイル・スロットを作成してから、マウント要求に応答する必要があります。

Data Protector は、バックアップを完了するための十分な空きスペースがなく、まだ (GUI により予約スペースなしで作成された) 空きスロットがある場合にもマウント要求を発行します。この場合は、ディスクに空きスペースを作ってからマウント要求に応答する必要があります。その後、Data Protector はバックアップを続行します。

スタンドアロン・ファイル・デバイスとファイル ジュークボックス デバイスの保守

使用中のデバイスに空きスペースがなくなったときには、バックアップを続行するために、以下のいずれかの作業を行う必要があります。

- データをテープに移して、ファイル・デバイスまたはいくつかのファイル・スロットを解放します。
- ファイル ジュークボックス スロットにリサイクル・マークを付けます。
- ファイル ジュークボックスに新しいスロットを追加します。

ファイル・スロットのリサイクル

ファイル・スロットに書き込まれたデータをテープに移動しないでそのファイル・スロットを再利用したい場合 (たとえば、ファイル ジュークボックスを主なバックアップ・デバイスとして使用しており、そのスロットから直接復元したい場合など) は、スロットにリサイクル・マークを付けます。リサイクルされたスロットはバックアップに再利用され、スロッ

ト上のデータは上書きされます。スロットのリサイクル方法の詳細については、オンライン・ヘルプの索引キーワード「ファイル・ジュークボックス・スロットのリサイクル」を参照してください。

重要

この方法を使用した場合、メディア上の既存のデータは上書きされて失われます。

新しいファイル・スロットの追加

ファイル ジュークボックス デバイスのファイル・スロットを追加作成する方法については、オンライン・ヘルプの索引キーワード「追加 - スロット」を参照してください。スロットを使用するには、最初にスロットをフォーマットする必要があります。メディアのフォーマット方法の詳細については、オンライン・ヘルプの索引キーワード「フォーマット - ライブラリ・デバイス内のメディア」を参照してください。

スタンドアロン・ファイル・デバイスまたはファイル ジュークボックス デバイスからの復元

復元時には、復元するオブジェクトを Data Protector GUI 上で選択し、通常どおりの復元処理を開始してください。詳細については、オンライン・ヘルプの索引キーワード「標準復元手順」を参照してください。

Data Protector CLI を使用してこの処理を自動実行するためのスクリプトを作成することも可能です。

ACSLS
(StorageTek 固有の用語)
Automated Cartridge System Library Server の略語。ACS (Automated Cartridge System: 自動カートリッジ システム) を管理するソフトウェア。

Active Directory
(Windows 固有の用語)
Windows ネットワークで使用されるディレクトリ サービス。ネットワーク上のリソースに関する情報を格納し、ユーザーやアプリケーションからアクセスできるように維持します。このディレクトリ サービスでは、サービスが実際に稼動している物理システムの違いに関係なく、リソースに対する名前や説明の付加、検索、アクセス、および管理を一貫した方法で実行できます。

AML
(EMASS/GRAU 固有の用語)
Automated Mixed-Media library (自動混合メディア ライブラリ) の略。

ASR セット
フロッピー ディスク上に保存されたファイルのコレクション。交換用ディスクの適切な再構成 (ディスク パーティション化と論理ボリュームの構成) およびフル クライアント バックアップでバックアップされた元のシステム構成とユーザー データの自動復旧に必要となります。これらのファイルは、バックアップ メディア上に保存されると共に、Cell Manager 上の <*Data_Protector_home*>¥Config¥Server¥dr¥asr ディレクトリ (Windows Cell Manager の場合) または /etc/opt/omni/server/dr/asr/ ディレクトリ (UNIX Cell Manager の場合) に保存されます。ASR アーカイブ ファイルは、障害発生後に複数のフロッピー ディスクに展開されます。32 ビット版の Windows XP/.NET では 3 枚のフロッピー ディスクに展開され、64 ビット版の Windows XP/.NET の場合は 4 枚のフロッピー ディスクに展開されます。これらのフロッピー ディスクは、ASR の実行時に必要となります。

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

ンドを発行します。

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

BC
(HP StorageWorks Disk Array XP 固有の用語)
Business Copy XP の略。BC を使うと、HP StorageWorks Disk Array XP LDEV の内部コピーをデータ バックアップやデータ複製などの目的で維持できます。これらのコピー (セカンダリ ボリュームまたは S-VOL) は、プライマリ ボリューム (P-VOL) から分離して、バックアップや開発などの用途に応じた別のシステムに接続することができます。バックアップ目的の場合、P-VOL をアプリケーション システムに接続し、S-VOL ミラー セットのいずれかをバックアップ システムに接続する必要があります。
HP StorageWorks Disk Array XP LDEV、**CA**、**Main Control Unit**、**アプリケーション システム**、および**バックアップ システム***も参照。*

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

BC VA
(HP StorageWorks Virtual Array 固有の用語)
BC は Business Copy の略。Business Copy VA により、HP StorageWorks Virtual Array LUN の内部コピーをデータ バックアップやデータ複写の目的で同じ仮想アレイ内に保持することができます。コピー (子または Business Copy LUN) は、バックアップやデータ解析、開発など様々な目的に使用できます。バックアップ目的で使用されるときは、元 (親) の LUN はアプリケーション システムに接続され、Business Copy (子) LUN はバックアップ システムに接続されます。
HP StorageWorks Virtual Array LUN、**アプリケーション システム**、および**バックアップ システム***も参照。*

BCV

(EMC Symmetrix 固有の用語)
Business Continuance Volumes の略。BCV デバイスは ICDA 内であらかじめ構成された専用の SLD です。ビジネスの継続運用を可能にするために使用されます。BCV デバイスには、これらのデバイスによりミラー化される SLD のアドレスとは異なる、個別の SCSI アドレスが割り当てられます。BCV デバイスは、保護を必要とする一次 EMC Symmetrix SLD の分割可能なミラーとして使用されます。
BC および **BC Process** *も参照。*

BRARCHIVE

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

BRBACKUP

(SAP R/3 固有の用語)
SAP R/3 バックアップ ツールの 1 つ。制御ファイル、個々のデータ ファイル、またはすべてのテーブル スペースをオンラインでもオフラインでもバックアップできます。また、必要に応じて、オンライン REDO ログ ファイルをバックアップすることもできます。
SAPDBA、**BRARCHIVE** および **BRRESTORE** *も参照。*

BRRESTORE

(SAP R/3 固有の用語)
SAP R/3 のツール。以下の種類のファイルを復元するために使います。

- BRBACKUP で保存されたデータベース データ ファイル、制御ファイル、オンライン REDO ログ ファイル
- BRARCHIVE でアーカイブされた REDO ログ ファイル
- BRBACKUP で保存された非データベース ファイル

ファイル、テーブル スペース、バックアップ全体、REDO ログ ファイルのログ シーケンス番号、またはバックアップのセッション ID を指定することができます。
SAPDBA、**BRBACKUP** および **BRARCHIVE** *も参照。*

BSM

Data Protector Backup Session Manager の略。バックアップ セッションを制御します。このプロセスは、常に Cell Manager システム上で稼動しま

す。

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

CAP
(StorageTek 固有の用語)
Cartridge Access Port の略。ライブラリのドア パネルに組み込まれたポートです。メディアの出し入れに使用されます。

CDB
カタログ データベース (Catalog Database) の略。CDB は、IDB のうち、バックアップ、オブジェクト コピー、復元、メディア管理セッションおよびバックアップしたデータに関する情報を格納する部分。選択したロギング レベルによっては、ファイル名とファイル バージョンも格納されます。CDB は、常にセルに対してローカルとなります。
MMDB *も参照。*

CDF ファイル
(UNIX 固有の用語)
Context Dependent File (コンテキスト依存ファイル) の略。CDF ファイルは、同じパス名でグループ化された複数のファイルからなるファイルです。通常、プロセスのコンテキストに基づいて、これらのファイルのいずれかがシステムによって選択されます。このメカニズムにより、クラスタ内のすべてホストから同じパス名を使って、マシンに依存する実行可能ファイル、システム データ、およびデバイス ファイルを正しく動作させることができます。

Cell Manager
セル内のメイン システム。Data Protector の運用に不可欠なソフトウェアがインストールされ、すべてのバックアップおよび復元作業がここから管理されます。管理タスク用の GUI は、異なるシステムにインストールできます。各セルは、1 つの Cell Manager システムによって管理されます。

CMD Script for OnLine Server
(Informix 固有の用語)
Informix OnLine Server の構成時に INFORMIXDIR 内に作成される Windows CMD スクリプト。環境変数を OnLine Server にエクスポートするコマンド一式が含まれています。

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

COM+ 登録データベース
(Windows 固有の用語)
COM+ 登録データベースと Windows レジストリには、COM+ アプリケーションの属性、クラスの属性、およびコンピュータ レベルの属性が格納されます。これにより、これらの属性間の整合性を確保でき、これらの属性を共通の方法で操作できます。

Command View (CV) EVA
(HP StorageWorks EVA 固有の用語)
HP StorageWorks EVA ストレージ システムを構成、管理、モニターするためのユーザー インタフェース。さまざまなストレージ管理作業を行うために使用されます。たとえば、仮想ディスクファミリの作成、ストレージ システム ハードウェアの管理、仮想ディスクのスナップクローンやスナップショットの作成などに使用されます。Command View EVA ソフトウェアは HP OpenView storage マネジメント アプライアンス上で動作し、Web ブラウザからアクセスできます。

HP StorageWorks EVA Agent (従来のもの) および **HP StorageWorks EVA SMI-S Agent** *も参照。*

CRS

Data Protector Cell Manager 上で実行される、Cell Request Server のプロセス (サービス)。バックアップ セッションと復元セッションを開始および制御します。このサービスは、Data Protector が Cell Manager 上にインストールされるとすぐに開始されます。
CRS は、UNIX システムでは root アカウントで実行されます。Windows では、いかなるアカウントでも実行できます。デフォルトでは、インストール時に使用したユーザー アカウントで実行されます。

CSM

Data Protector コピー セッション マネージャの略。このプロセスは、オブジェクト コピー セッションを制御し、Cell Manager システム上で動作します。

Data Protector イベント ログ

イベント ログには、Data Protector 関連のすべての通知が書き込まれます。デフォルトの送信方法では、すべての通知がイベント ログに送信されます。イベント ログにアクセスできる Data Protector ユーザーは、admin ユーザー グループに所属しているか、または**「レポートと通知」**のユーザー権限が付与されている Data Protector ユーザーだけです。イベント ログに書き込まれているイベントは、いずれも表示と削除が可能です。

Data Protector ユーザー アカウント

Data Protector およびバックアップ データに対する無許可のアクセスを制限するために、Data Protector ユーザーとして許可を受けたユーザーにしか Data Protector を使用できないようになっています。Data Protector 管理者がこのアカウントを作成するときには、ユーザー ログオン名、ユーザーのログオン元として有効なシステム、および Data Protector ユーザー グループのメンバーシップを指定します。ユーザーが Data Protector のユーザー インタフェースを起動するか、または特定のタスクを実行するときには、このアカウントが必ずチェックされます。

Dbobject

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

DCBF

DCBF (Detail Catalog Binary Files: 詳細カタログ バイナリ ファイル) ディレクトリは、IDB の一部です。IDB の約 80% を占めるファイル バージョンと属性に関する情報を格納します。デフォルトでは、DCBF は 1 つの DC ディレクトリからなり、その最大サイズは 2GB です。新たに DC ディレクトリを作成して追加することもできます。

DC ディレクトリ
詳細カタログ (DC) ディレクトリは、詳細カタログ バイナリ ファイル (DCBF) で構成されており、そのファイルの中にはファイル バージョンについての情報が保管されています。これは、IDB の DCBF 部分を表し、IDB 全体の約 80% の容量を占めます。デフォルトの DC ディレクトリは、`dcbf` ディレクトリと呼ばれ、`<Data_Protector_home>¥db40` ディレクトリ (Windows Cell Manager の場合) または `/var/opt/omni/server/db40` ディレクトリ (UNIX Cell Manager の場合) に配置されています。他の DC ディレクトリを作成して、適切な場所に置くことができます。1 つのセルでサポートされる DC ディレクトリは 10 個までです。DC ディレクトリのデフォルト最大サイズは 2GB です。

DHCP サーバ
Dynamic Host Configuration Protocol (DHCP) を通じて、IP アドレスおよび関連情報の動的構成機能を提供するシステム。

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

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

DMZ
DMZ (Demilitarized Zone) は、企業のプライベート ネットワーク (イントラネット) と外部のパブリック ネットワーク (インターネット) の間に「中立地帯」として挿入されたネットワークです。DMZ により、外部のユーザーが企業のイントラネット

内のサーバに直接アクセスすることを防ぐことができます。

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

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

DR OS
障害復旧オペレーティング システムとは、障害復旧を実行するためのオペレーティング システム環境です。Data Protector に対して基本的な実行時環境 (ディスク、ネットワーク、テープ、およびファイルシステムへのアクセス) を提供します。Data Protector 障害復旧を実行する前に、DR OS をインストールおよび構成しておく必要があります。DR OS は、Data Protector 障害復旧プロセスのホストとして機能するだけでなく、復元後のシステムの一部にもなります。その場合、DR OS の構成データは元の構成データに置き換わります。

EMC Symmetrix Agent (SYMA)
(EMC Symmetrix 固有の用語)
Symmetrix Agent (SYMA) を参照。

EMC Symmetrix Application Programming Interface (SYMAPI)
(EMC Symmetrix 固有の用語)
Symmetrix Application Programming Interface (SYMAPI) を参照。

EMC Symmetrix CLI Database File
(EMC Symmetrix 固有の用語)
Symmetrix CLI Database File を参照。

EMC Symmetrix Command-Line Interface (SYMCLI)
(EMC Symmetrix 固有の用語)
Symmetrix Command-Line Interface (SYMCLI) を参照。

FC ブリッジ
Fibre Channel ブリッジ *を参照。*

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

ポイント、ループ、スイッチ式) で接続できます。

Fibre Channel ブリッジ

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

fnames.dat

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

GUI

Data Protector には、各種プラットフォーム (HP-UX、Solaris、Windows) に対応したグラフィカル ユーザー インタフェース (GUI) が用意されており、すべての構成タスク、管理タスクおよび処理タスクに容易にアクセスできます。

Holidays ファイル

休日に関する情報を格納するファイル。このファイルを通じて、休日の設定を変更できます。Holidays ファイルのパスは、`/etc/opt/omni/server/Holidays` (UNIX Cell Manager の場合) または *`<Data_Protector_home>`*`¥Config¥Server¥holidays` (Windows Cell Manager の場合) です。

HP ITO

OVO *を参照。*

HP OpC

OVO *を参照。*

HP OpenView SMART Plug-In (SPI)

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

HP OVO

OVO *を参照。*

HP StorageWorks Disk Array XP LDEV
HP StorageWorks Disk Array XP の物理ディスクの論理パーティション。LDEV は、Continuous Access XP (CA) 構成および Business Copy XP (BC) 構成で複製することができるエンティティで、スタンドアロンのエンティティとしても使用できます。
BC *(HP StorageWorks Disk Array XP 固有の用語)*、**CA** *(HP StorageWorks Disk Array XP 固有の用語)*、および **複製** *も参照。*

HP StorageWorks EVA Agent (従来のもの)
Data Protector のソフトウェア モジュール。Command View (CV) EVA ソフトウェア v3.1 以前と、EVA VCS ファームウェア v3.01x 以前がインストールされた HP StorageWorks EVA 上で稼動する HP StorageWorks Enterprise Virtual Array 統合ソフトウェアに必要なすべてのタスクを実行します。
Command View (CV) EVA および **HP StorageWorks EVA SMI-S Agent** *も参照。*

HP StorageWorks EVA SMI-S Agent
Data Protector のソフトウェア モジュール。Command View (CV) EVA ソフトウェアの v3.2 以降がインストールされた HP StorageWorks EVA 上で稼動する HP StorageWorks Enterprise Virtual Array 統合ソフトウェアに必要なタスクをすべて実行します。EVA SMI-S Agent を使用すると、受信した要求と CV EVA 間のやり取りを制御する HP StorageWorks SMI-S EVA プロバイダを通じてアレイを制御できます。
Command View (CV) EVA、**HP StorageWorks SMI-S EVA プロバイダ**、および **HP StorageWorks EVA Agent (従来のもの)** *も参照。*

HP StorageWorks SMI-S EVA プロバイダ
HP StorageWorks Enterprise Virtual Array を制御するために使用されるインタフェース。SMI-S EVA プロバイダは HP OpenView ストレージ マネジメント アプライアンス システム上で個別のサービスとして動作し、受信した要求と Command View EVA 間のゲートウェイとして機能します。Data Protector HP StorageWorks EVA 用統合ソフトウェアでは、SMI-S EVA プロバイダは EVA SMI-S Agent から標準化された要求を受け入れ、Command View EVA とやり取りして情報または方法を呼び出し、標準化された応答を返します。
HP StorageWorks EVA SMI-S Agent および **Command View (CV) EVA** *も*

参照。

HP StorageWorks Virtual Array LUN
HP StorageWorks Virtual Array 内の物理ディスクの論理パーティション。LUN は HP StorageWorks Business Copy VA 構成で複製することができるエンティティで、スタンドアロンのエンティティとしても使用できます。
BC VA および**複製** *も参照。*

HP VPO
OVO *を参照。*

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

IDB
Data Protector 内部データベースは、Cell Manager 上に維持される埋込み型データベースです。どのデータがどのメディアにバックアップされるか、バックアップ セッションと復元セッションがどのように実行されるか、さらに、どのデバイスとライブラリが構成されているかについての情報が格納されます。

Inet
Data Protector セル内の各 UNIX システムまたは Windows システム上で動作するプロセス。このプロセスは、セル内のシステム間の通信と、バックアップおよび復元に必要なその他のプロセスの起動を受け持ちます。システムに Data Protector をインストールすると、Inet サービスが即座に起動されます。Inet プロセスは、inetd デーモンにより開始されます。

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

IP アドレス
IP (インターネット プロトコル) アドレスは、ネットワーク上のシステムを一意に識別するアドレスで、数字で表されます。IP アドレスは、ピリオド (ドット) で区切られた 4 組の数字からなります。

ISQL

(Sybase 固有の用語)
Sybase のユーティリティの 1 つ。Sybase SQL Server に対してシステム管理作業を実行できます。

ITO
OVO *を参照。*

LBO
(EMC Symmetrix 固有の用語)
Logical Backup Object (論理バックアップ オブジェクト) の略。LBO は、EMC Symmetrix/Fastrax 環境内で保存 / 取得されるデータ オブジェクトです。LBO は EMC Symmetrix によって 1 つのエンティティとして保存 / 取得され、部分的には復元できません。

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

log_full シェル スクリプト
(Informix UNIX 固有の用語)
ON-Bar に用意されているスクリプトの 1 つ。OnLine Server が log-full イベント警告を発行したときに論理ログ ファイルのバックアップを開始できます。Informix の ALARMPROGRAM 構成パラメータは、デフォルトで、
<*INFORMIXDIR*>/etc/log_full.sh
に設定されます。ここで、<*INFORMIXDIR*> は、OnLine Server ホーム ディレクトリです。論理ログ ファイルを継続的にバックアップしたくない場合は、ALARMPROGRAM 構成パラメータを
<*INFORMIXDIR*>/etc/no_log.sh
に設定してください。

Lotus C API
(Lotus Domino Server 固有の用語)
Lotus Domino Server と Data Protector などのバックアップ ソリューションの間でバックアップ情報および復元情報を交換するためのインタフェース。

LVM
LVM (Logical Volume Manager: 論理ボリューム マネージャ) は、HP-UX システム上で物理ディスク スペースを構造化し、論理ボリュームにマッピングするためのサブシステムです。LVM システムは、複数のボリューム グループで構成されます。各ボリューム グループには、複数のボリュームが含まれます。

Main Control Unit (MCU)
(HP StorageWorks Disk Array XP 固有の用語)
Continuous Access 構成用のプライマリ ボリュームを含み、マスター デ

バイスとしての役割を果たす HP StorageWorks XP ディスク アレイ。**BC***(HP StorageWorks Disk Array XP 固有の用語)*、**CA** *(HP StorageWorks Disk Array XP 固有の用語)* および **HP StorageWorks Disk Array XP LDEV** *も参照。*

Manager-of-Managers (MoM)

エンタープライズ Cell Manager *を参照。*

MAPI

(MS Exchange 固有の用語)
MAPI (Messaging Application Programming Interface) は、アプリケーションおよびメッセージング クライアントがメッセージング システムおよび情報システムと対話するためのプログラミング インタフェースです。

Media Agent

デバイスに対する読み込み / 書き込みを制御するプロセス。制御対象のデバイスはテープなどのメディアに対して読み込み / 書き込みを行います。バックアップ セッション中、Media Agent は Disk Agent からデータを受信し、デバイスに送信します。データを受信したデバイスはメディアに書き込みます。Media Agent は、ライブラリのロボティクス制御も管理します。

MFS

Migrating Filesystem の略。MFS は、HP-UX 11.00 において、移行能力を持つ標準的な JFS ファイルシステムを実現します。MFS は、標準ファイルシステム インタフェース (DMAPI) 経由でアクセスでき、通常の HP-UX ファイルシステムと同様にディレクトリにマウントされます。MFS では、スーパーブロック、i ノード情報、および " 拡張属性 " 情報のみがハードディスク上に永続的に保持され、これらが移動されることはありません。**VBFS** *も参照。*

Microsoft Exchange Server

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

Microsoft SQL Server 7.0/2000

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

Microsoft Volume Shadow Copy Service (VSS)
VSS 対応アプリケーションのバックアップと復元をそのアプリケーションの機能に関係なく統合管理する統一通信インタフェースを提供するソフトウェア サービスです。このサービスは、バックアップ アプリケーション、ライター、シャドウ コピー プロバイダ、およびオペレーティング システム カーネルと連携して、ボリューム シャドウ コピーおよびシャドウ コピー セットの管理を実現します。
シャドウ コピー、シャドウ コピー プロバイダ、ライター*も参照。*

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

MMD
Media Management Daemon（メディア管理デーモン）の略。MMD プロセス (サービス) は、Data Protector Cell Manager 上で稼動し、メディア管理操作およびデバイス操作を制御します。このプロセスは、Data Protector を Cell Manager にインストールしたときに開始されます。

MMDB
Media Management Database (メディア管理データベース) の略。MMDB は、IDB の一部です。セル内で構成されているメディア、メディア プール、デバイス、ライブラリ、ライブラリ デバイス、スロットに関する情報と、バックアップに使用されている Data Protector メディアに関する情報を格納します。エンタープライズ バックアップ環境では、データベースをすべてのセル間で共有できます。
CMMDB および **CDB** *も参照。*

MoM
複数のセルをグループ化して、1 つのセルから集中管理することができます。集中管理用のセルが MoM (Manager-of-Managers) です。MoM を通じて、複数のセルを一元的に構成および管理できます。

MSM
Media Session Manager (メディア セッション マネージャ) の略。MSM は、Cell Manager 上で稼動し、メディア セッション (メディアのコピーなど) を制御します。

MU 番号

(*HP StorageWorks Disk Array XP 固有の用語*)
MU 番号は、Mirror Unit Number (ミラー ユニット番号) の略語。ファースト レベル ミラーを示すために使う整数 (0、1 または 2) です。**ファースト レベル ミラー***も参照。*

obdrindex.dat
IDB バックアップおよびバックアップ用のメディアとデバイスに関する情報を格納する IDB ファイルです。この情報を使うと、IDB の復旧を大幅に効率化できますファイルを IDB トランザクション ログとともに、ほかの IDB ディレクトリから別の物理ディスク上に移し、さらに、そのファイルのコピーを作成し、適切な場所に保存します。

OBDR 対応デバイス
ブート可能ディスクを装填した CD-ROM ドライブをエミュレートできるデバイス。バックアップ デバイスとしてだけでなく、障害復旧用のブート デバイスとしても使用可能です。

OmniStorage
透過的な移行を可能にするソフトウェア。使用頻度の高いデータをハード ディスク上に残したまま使用頻度の低いデータを光磁気ライブラリに移動します。HP OmniStorage は、HP-UX システム上で動作します。

ON-Bar
(Informix 固有の用語)
OnLine Server のためのバックアップと復元のシステム。ON-Bar により、OnLine Server データのコピーを作成し、後でそのデータを復元することが可能になります。ON-Bar のバックアップと復元のシステムには、以下のコンポーネントが含まれます。

- onbar ユーティリティ
- バックアップ ソリューションとしての Data Protector
- XBSA インタフェース
- ON-Bar カタログ テーブル。これは、dbobject をバックアップし、複数のバックアップを通して dbobject のインスタンスをトラッキングするために使われます。

onbar ユーティリティ
(Informix 固有の用語)
Informix ユーティリティの 1 つ。バックアップ要求および復元要求を OnLine Server との間でやり取りします。このユーティリティでは、XBSA を使用して制御データを交換し、Data Protector と連携してデータのバックアップと復元を行います。

ONCONFIG
(Informix 固有の用語)
アクティブな ONCONFIG 構成ファイルの名前を指定する環境変数。ONCONFIG 環境変数が存在しない場合、OnLine が <*INFORMIXDIR*>¥etc¥onconfig (HP-UX の場合)、または <*INFORMIXDIR*>/etc/onconfig (Windows の場合) のファイルにある構成値を使います。

OnLine Server
(Informix 固有の用語)
INFORMIX-OnLine Dynamic Server を指します。

OpC
OVO *を参照。*

Oracle インスタンス
(Oracle 固有の用語)
1 つまたは複数のシステムにインストールされた個々の Oracle データベース。1 つのコンピュータ システム上で、複数のデータベース インスタンスを同時に稼動させることができます。

Oracle ターゲット データベースへのログイン情報
(Oracle および SAP R/3 固有の用語)
ログイン情報の形式は、<user_name>/<password>@<service> です。

- <user_name> は、Oracle Server およびその他のユーザーに対して公開されるユーザー名です。ユーザー名には必ずパスワードが関連付けられます。各ユーザーが Oracle ターゲット データベースに接続するには、ユーザー名とパスワードの両方を入力しなければなりません。ここでは、Oracle の SYSDBA 権限または SYSOPER 権限が付与されているユーザーを指定する必要があります。

- <password> は、所有者だけが知っているデータ セキュリティ用の文字列です。パスワードは、オペレーティング システムまたはソフトウェア アプリケーションへの接続時に入力します。パスワードは、Oracle パスワード ファイル (orapwd) に指定されているパスワードに一致する必要があります。これは、データベース管理を行うユーザーの認証に使用されるファイルです。

- <service> は、ターゲット データベースの SQL*Net サーバ プロセスを識別する名前です。

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。

OVO

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

マージも参照。

P1S ファイル

P1S ファイルには、システムにインストールされているすべてのディスクを高度な自動障害復旧 (EADR) 中にどのようにフォーマットするかに関する情報が格納されます。このファイルはフル バックアップ中に作成され、バックアップ メディアと Cell Manager に recovery.p1s というファイル名で保存されます。保存場所は、<*Data_Protector_home*>¥Config¥Server¥dr¥p1sディレクトリ (Windows Cell Manager の場合) または /etc/opt/omni/server/dr/p1s ディレクトリ (UNIX Cell Manager の場合) です。

RAID

Redundant Array of Inexpensive Disks の略。

RAID Manager XP

(HP StorageWorks Disk Array XP 固有の用語)

RAID Manager XP アプリケーションには、CA アプリケーションおよび BC アプリケーションのステータスを報告 / 制御するコマンドが豊富に用意されています。これらのコマンドは、RAID Manager インスタンスを通じて、StorageWorks Disk Array XP Disk Control Unit と通信します。このインスタンスは、コマンドを一連の低レベル SCSI コマンドに変換します。

RAID Manager ライブラリ

(HP StorageWorks Disk Array XP 固有の用語)

Solaris システム上の Data Protector では、RAID Manager ライブラリを内部的に使用して、HP StorageWorks

Disk Array XP の構成データ、ステータス データ、およびパフォーマンス データにアクセスします。さらに、一連の低レベル SCSI コマンドに変換される関数呼び出しを通じて、StorageWorks Disk Array XP の主要な機能にアクセスします。

raw ディスクのバックアップ
ディスク イメージのバックアップ を参照。

RCU
(HP StorageWorks 固有の用語)
Remote Control Unit (RCU) は、CA 構成の中で MCU (Main Contol Unit) のスレーブとしての役割を果たします。双方向の構成の中では、RCU は MCU としての役割を果たします。

RDBMS
Relational Database Management System (リレーショナル データベース管理システム) の略。

RDF1/RDF2
(EMC Symmetrix 固有の用語)
SRDF デバイス グループの一種。RDF グループには RDF デバイスだけを割り当てることができます。RDF1 グループ タイプにはソース デバイス (R1) が格納され、RDF2 グループ タイプにはターゲット デバイス (R2) が格納されます。

RDS
Raima Database Server の略。RDS (サービス) は、Data Protector の Cell Manager 上で稼動し、IDB を管理します。このプロセスは、Data Protector を Cell Manager にインストールしたときに開始されます。

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

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

REDO ログ
(Oracle 固有の用語)
各 Oracle データベースには、複数の REDO ログ ファイルがあります。データベース用の REDO ログ ファイルのセットをデータベースの REDO ログと呼びます。Oracle では、REDO ログを使ってデータに対するすべての変更を記録します。

Remote Control Unit
(HP StorageWorks Disk Array XP 固有の用語)
Remote Control Unit (RCU) は、CA 構成の中で MCU (Main Contol Unit) のスレーブとしての役割を果たします。双方向の構成の中では、RCU は MCU としての役割を果たします。

RMAN
(Oracle 固有の用語)
Recovery Manager を参照。

RSM
Data Protector Restore Session Manager の略。復元セッションを制御します。このプロセスは、常に Cell Manager システム上で稼動します。

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

SAPDBA
(SAP R/3 固有の用語)
BRBACKUP ツール、BRARCHIVE ツール、BRRESTORE ツールを統合した SAP R/3 ユーザー インタフェース。

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

SMB
スプリット ミラー バックアップ *を参照。*

SMBF
セッション メッセージ バイナリ ファイル (SMBF) は、IDB のうち、バックアップ セッション中および復元セッション中に生成されたセッション メッセージが格納される部分です。セッションごとに 1 つのバイナリ ファイルが作成されます。バイナリ ファイルは、年と月に基づいて分類されます。

sqlhosts ファイル
(Informix 固有の用語)
Informix の接続情報ファイル。各データベース サーバの名前の他、ホスト コンピュータ上のクライアントが接続できるエイリアスが格納されます。

SRD ファイル
SRD (System Recovery Data: システム復旧データ) ファイルには、障害発生時にオペレーティング システムをインストールおよび構成するために必要なシステム情報が含まれています。SRD ファイルは ASCII ファイルで、CONFIGURATION バックアップが Windows クライアント上で実行され Cell Manager に保存される時に生成されます。

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

SSE Agent
(HP StorageWorks Disk Array XP 固有の用語)
スプリット ミラー バックアップの統合に必要なタスクをすべて実行する Data Protector ソフトウェア モジュール。RAID Manager XP ユーティリティ (HP-UX システムおよび

Windows システムの場合) または RAID Manager ライブラリ (Solaris システムの場合) を使い、HP StorageWorks Disk Array XP の保管システムと通信します。

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

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

StorageTek ACS ライブラリ
(StorageTek 固有の用語)
ACS (Automated Cartridge System) は、1 つのライブラリ管理ユニット (LMU) と、このユニットに接続された 1 ～ 24 個のライブラリ記憶域モジュール (LSM) からなるライブラリ システム (サイロ) です。

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

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

Symmetrix Agent (SYMA)
(EMC Symmetrix 固有の用語)
EMC Symmetrix 環境でのバックアップ操作と復元操作を可能にする Data

Protector ソフトウェア モジュール。

Symmetrix Application Programming Interface (SYMAPI)
(EMC Symmetrix 固有の用語)
Data Protector クライアントに接続された EMC Symmetrix ユニットとのインタフェースとして使用できる、リンク可能な関数のライブラリ。EMC によって提供されます。

Symmetrix CLI データベース ファイル
(EMC Symmetrix 固有の用語)
EMC Symmetrix ICDA が構成されており SYMCLI がインストールされている各システム上の EMC Symmetrix 構成データを格納する EMC Symmetrix データベース ファイル。

Symmetrix Command-Line Interface (SYMCLI)
(EMC Symmetrix 固有の用語)
特殊な低レベル SCSI コマンドで Symmetrix ユニットからデータを取得するアプリケーション。EMC Symmetrix Application Programming Interface (SYMAPI) を使用しています。SYMCLI では、オープン システム環境で動作しているクライアント上でコマンドを実行することで、クライアントに接続されている EMC Symmetrix ユニットから構成、ステータスおよびパフォーマンスに関するデータを取得できます。

System Backup to Tape
(Oracle 固有の用語)
Oracle がバックアップ要求または復元要求を発行したときに正しいバックアップ デバイスをロード、ラベリング、およびアンロードするために必要なアクションを処理する Oracle インタフェース。

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

TimeFinder
(EMC Symmetrix 固有の用語)
単一または複数の EMC Symmetrix 論理デバイス (SLD) のインスタント コピーを作成する Business Continuation プロセス。インスタント コピーは、BCV と呼ばれる専用の事前構成 SLD 上に作成され、システムに対する別個のプロセスを経由してアクセスできます。

TLU
Tape Library Unit (テープ ライブラリ ユニット) の略。

TNSNAMES.ORA
(Oracle および SAP R/3 固有の用語)
サービス名にマッピングされた接続記述子を格納するネットワーク構成ファイル。このファイルは、1 か所で集中的に管理してすべてのクライアントで使用することも、また、ローカルに管理して各クライアントで個別に使用することもできます。

TSANDS.CFG ファイル
(Novell NetWare 固有の用語)
バックアップを開始するコンテナの名前を指定する**ファイル**。このファイルはテキスト ファイルで、`TSANDS.NLM` がロードされるサーバの `SYS:SYSTEM¥TSA` ディレクトリにあります。

VBFS
(OmniStorage 固有の用語)
VBFS (Very Big File System) とは、HP-UX 9.x 上の標準 HP-UX ファイルシステムに対する拡張部分を指します。VBFS は、通常の HP-UX ファイルシステムと同様にディレクトリにマウントされます。VBFS では、スーパーブロック、i ノード情報、および " 拡張属性 " 情報のみがハードディスク上に永続的に保持され、これらが移動されることはありません。
MFS *も参照。*

Virtual Controller Software (VCS)
(HP StorageWorks EVA 固有の用語)
HSV コントローラを介した Command View EVA との通信など、記憶システムの処理すべてを管理するファームウェア。
Command View (CV) EVA *も参照。*

VOLSER
(ADIC および STK 固有の用語)
ボリューム シリアル (VOLume SERial) 番号は、メディア上のラベルで、大容量ライブラリ内の物理テープの識別に使用されます。VOLSER は、ADIC/GRAU デバイスおよび StorageTek デバイス固有の命名規則です。

Volume Shadow Copy サービス
Microsoft Volume Shadow Copy Service *を参照。*

VPO
OVO *を参照。*

VSS
Microsoft Volume Shadow Copy Service *を参照。*

VxFS
Veritas Journal Filesystem. の略。

VxVM (Veritas Volume Manager)
Veritas Volume Manager は、Solaris プラットフォーム上でディスク スペースを管理するためのシステムです。VxVM システムは、論理ディスク グループに編成された 1 つまたは複数の物理ボリュームの任意のグループからなります。

Wake ONLAN
節電モードで動作しているシステムを同じ LAN 上の他のシステムからのリモート操作により電源投入するためのサポート。

Web レポート
Data Protector の機能の 1 つ。バックアップ ステータスと Data Protector 構成に関するレポートを Web インタフェース経由で表示できます。

Windows CONFIGURATION バックアップ
Data Protector では、Windows CONFIGURATION (構成データ) をバックアップできます。Windows レジストリ、ユーザー プロファイル、イベント ログ、WINS サーバ データおよび DHCP サーバ データ (システム上で構成されている場合) を 1 回の操作でバックアップできます。

Windows レジストリ
オペレーティング システムやインストールされたアプリケーションの構成情報を保存するため、Windows により使用される集中化されたデータベース。

WINS サーバ
Windows ネットワークのコンピュータ名を IP アドレスに解決する Windows インターネット ネーム サービス ソフトウェアを実行しているシステム。Data Protector では、WINS サーバ データを Windows の構成データの一部としてバックアップできます。

XBSA インタフェース
(Informix 固有の用語)
onbar ユーティリティと Data Protector の間の相互通信には、X/Open Backup Specification Services Programmer's Interface (XBSA) が使用されます。

XCopy エンジン
(ダイレクト バックアップ固有の用語)
SCSI-3 のコピー コマンド。SCSI ソース アドレスを持つストレージ デバイスから SCSI 宛先アドレスを持つバックアップ デバイスにデータをコピーし、ダイレクト バックアップを可能にします。XCopy では、ソース デバイスからデータをブロック (ディスクの場合) または

ストリーム (テープの場合) として宛先デバイスにコピーします。これにより、データをストレージ デバイスから読み込んで宛先デバイスに書き込むまでの一連の処理が、制御サーバをバイパスして行われます。
***ダイレクト バックアップ** も参照。*

ZDB
ゼロ ダウンタイム バックアップ (ZDB) *を参照。*

ZDB データベース
(ZDB 固有の用語)
ソース ボリューム、複製およびセキュリティ情報などの ZDB 関連情報を格納する IDB の一部。ZDB データベースは ZDB、インスタント リカバリ、スプリット ミラー復元に使用されます。
ゼロ ダウンタイム バックアップ (ZDB) *も参照。*

アーカイブ ロギング
(Lotus Domino Server 固有の用語)
Lotus Domino Server のデータベース モードの 1 つ。トランザクション ログ ファイルがバックアップされて始めて上書きされるモードです。

アーカイブ REDO ログ
(Oracle 固有の用語)
オフライン REDO ログとも呼ばれます。Oracle データベースが ARCHIVELOG モードで動作している場合、各オンライン REDO ログが最大サイズまで書き込まれると、1 つまたは複数のアーカイブ先にコピーされます。このコピーをアーカイブ REDO ログと呼びます。各データベースに対してアーカイブ REDO ログを作成するかどうかを指定するには、以下の 2 つのモードのいずれかを指定します。

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

- NOARCHIVELOG - オンライン REDO ログ ファイルは、満杯になってもアーカイブされません。

オンライン REDO ログ *も参照*。

アクセス権
ユーザー権限 *を参照。*

アプリケーション エージェント
クライアント上でオンライン データベース統合ソフトウェアを復元およびバックアップするために必要な

コンポーネント。
Disk Agent *も参照*。

アプリケーション システム
(ZDB 固有の用語)
このシステム上でアプリケーションやデータベースが実行されます。アプリケーションまたはデータベース データは、ソース ボリューム上に格納されています。
バックアップ システムおよび**ソース ボリューム** *も参照。*

イベント ログ
Windows 上で発生したすべてのイベント (サービスの停止 / 開始やユーザーのログオン / ログオフなど) が記録されるファイル。Data Protector では、Windows 構成データ バックアップの一部として Windows イベント ログをバックアップできます。

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

インストール サーバ
特定のアーキテクチャ用の Data Protector ソフトウェア パッケージのレポジトリを保持するコンピュータ システム。インストール サーバから Data Protector クライアントのリモート インストールが行われます。混在環境では、UNIX システム用と Windows システム用の 2 台のインストール サーバが最低限必要になります。

インフォメーション ストア
(Microsoft Exchange Server 2000/2003 固有の用語)
記憶域管理を行う Microsoft Exchange Server 2000/2003 のサービス。Microsoft Exchange Server 2000/2003 のインフォメーション ストアは、メールボックス ストアとパブリック フォルダ ストアの 2 種類を管理します。メールボックス ストアは個々のユーザーに属するメールボックスから成ります。パブ

リック フォルダ ストアには、複数のユーザーで共有するパブリック フォルダおよびメッセージがあります。
キー マネージメント サービスおよび**サイト複製サービス** *も参照。*

インフォメーション ストア
(Microsoft Exchange Server 5.5 固有の用語)
Microsoft Exchange Server 5.5 のデフォルト メッセージ ストア プロバイダ。インフォメーション ストアは、以下から構成されます。

- パブリック インフォメーション ストア
- プライベート インフォメーション ストア
- パーソナル フォルダ ストア
- オフライン インフォメーション ストア

パブリック インフォメーション ストアには、パブリック フォルダおよびメッセージが格納され、これらは複数のユーザー / アプリケーション間での共有できます。複数の Exchange サーバを使用している場合でも、Exchange Server 5.5 組織内のすべてのユーザーが単一のパブリック インフォメーション ストアを共有します。プライベート インフォメーション ストアには、ユーザーまたはアプリケーションに所属するメールボックスが格納されます。メールボックスは、Microsoft Exchange Server 5.5 を実行しているサーバに常駐しています。
ディレクトリ ストア (DS) *も参照。*

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

エクスチェンジャ
SCSI エクスチェンジャとも呼ばれます。
ライブラリ *も参照。*

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

オートチェンジャー

ライブラリ *を参照。*

オートローダ
ライブラリ *を参照。*

オブジェクト
バックアップ オブジェクト *を参照。*

オブジェクト ID
(Windows 固有の用語)
NTFS 5 ファイルは、オブジェクト ID (OID) を通じてアクセスできます。これにより、システム内でファイルが実際に置かれている場所を意識する必要がなくなります。Data Protector では、OID をファイルの代替ストリームとして扱います。

オブジェクト コピー
特定のオブジェクト バージョンのコピー。オブジェクト コピー セッション中またはオブジェクト ミラーのバックアップ セッション中に作成されます。

オブジェクト コピー セッション
異なるメディア セット上にバックアップされたデータの追加のコピーを作成するプロセス。オブジェクト コピー セッション中に、選択されたバックアップ オブジェクトがソースからターゲット メディアへコピーされます。

オブジェクト 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。

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

オブジェクトのミラーリング
バックアップ セッション中に、同一のデータを複数のメディア セットに書き込むプロセス。Data Protector では、すべてまたは一部のバックアップ オブジェクトを 1 つまたは複数のメディア セットにミラーできます。

オフライン REDO ログ
アーカイブ REDO ログ *を参照。*

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

- 単純なバックアップ方法の場合 (ZDB ではない)、データベースはバックアップ中 (数分から数時間) オフライン状態となり、バックアップ システムからは使用できますが、アプリケーション システムからは使用できません。たとえばテープへのバックアップの場合、テープへのデータ ストリーミングが終わるまでの間となります。

- ZDB の方法を使うと、データベースはオフライン状態になりますが、所要時間はデータ複製プロセス中のわずか数秒間です。残りのバックアップ プロセスでは、データベースは通常の稼動を再開できます。

ゼロ ダウンタイム バックアップ (ZDB) および**オンライン バックアップ** *を参照。*

オフライン復旧
オフライン復旧は、ネットワーク障害などにより Cell Manager にアクセスできない場合に行われます。オフライン復旧には、スタンドアロン デバイスと SCSI ライブラリ デバイスだけを使用できます。Cell Manager の復旧は、常にオフラインで行われます。

オンライン 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。*

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。*

階層ストレージ管理 (HSM)
使用頻度の低いデータを低コストの光磁気プラッタに移動することで、コストの高いハード ディスク記憶域を有効利用するための仕組み。移動したデータが必要になった場合は、ハード ディスク記憶域に自動的に戻されます。これにより、ハード ディスクからの高速読み取りと光磁気プラッタの低コスト性のバランスが維持されます。

拡張可能 ストレージ エンジン (ESE)
(Microsoft Exchange Server 2000/2003 固有の用語)
Microsoft Exchange Server 2000/2003 で情報交換用の記憶システムとして使用されているデータベース テクノロジ。

仮想サーバ
仮想マシンとは、ネットワーク IP 名および IP アドレスでドメイン内に定義されるクラスタ環境を意味します。このアドレスは、クラスタ ソフトウェアによってキャッシュされ、仮想サーバ リソースを現在実行しているクラスタ ノードにマッピングされます。こうして、特定の仮想サーバに対するすべての要求が特定のクラスタ ノードにキャッシュされます。

仮想ディスク
(HP StorageWorks EVA 固有の用語)
HP StorageWorks Enterprise Virtual Array のストレージ プールから割り当てられる記憶領域の単位。仮想ディスクは、HP StorageWorks Enterprise Virtual Array のスナップショット機能により複製されるエンティティです。
ソース ボリュームおよび**ターゲット ボリューム** *も参照。*

仮想デバイス インタフェース
(MS SQL Server 7.0/2000 固有の用語)
SQL Server 7.0/2000 のプログラミング インタフェースの 1 つ。大容量のデータベースを高速でバックアップおよび復元できます。

カタログ保護
バックアップ データに関する情報 (ファイル名やファイル バージョンなど) を IDB に維持する期間を定義します。
データ保護*も参照。*

キー マネージメント サービス
(Microsoft Exchange Server 2000/2003 固有の用語)
セキュリティ強化のための暗号化機能を提供する Microsoft Exchange Server 2000/2003 のサービス。
インフォメーション ストアおよび**サイト複製サービス***も参照*。

共有ディスク
(Windows 固有の用語)
システム状態データには、レジストリ、COM+ クラス登録データベース、システム起動ファイル、および証明書サービス データベース (証明書サーバの場合) が含まれます。サーバがドメイン コントローラの場合は、Active Directory ディレクトリ サービスと Sysvol ディレクトリもシステム状態データに含まれます。サーバ上でクラスタ サービスが実行されている場合は、リソース レジストリ チェックポイントと、最新のクラスタ データベース情報を格納するクォーラム リソース回復ログもシステム状態データに含まれます。

共有ディスク
あるシステム上に置かれた Windows のディスクをネットワーク上の他のシステムのユーザーが使用できるように構成したもの。共有ディスクを使用しているシステムは、Data Protector Disk Agent がインストールされていなくてもバックアップ可能です。

緊急ブート ファイル
(Informix 固有の用語)
Informix の構成ファイルの 1 つ。`ixbar.`*<server_id>*(*<server_id>* は SERVERNUM 構成パラメータの値) という名前で *<INFORMIXDIR>*`¥etc` ディレクトリ (HP-UX の場合) または *<INFORMIXDIR>*`/etc` ディレクトリ (Windows の場合) に保存されます (*<INFORMIXDIR>* は OnLine Server のホーム ディレクトリ)。緊急ブート ファイルの各行は、1 つのバックアップ オブジェクトに対応します。

クライアントまたはクライアント システム
セル内で Data Protector の機能を使用できるように構成された任意のシステム。

クライアント バックアップ
クライアントにマウントされているすべてのファイルシステムのバックアップ。ただし、バックアップ仕様

の作成後にクライアントにマウントされたファイルシステムは、自動検出されません。

クラスタ対応アプリケーション
クラスタ アプリケーション プログラミング インタフェースをサポートしているアプリケーション。クラスタ対応アプリケーションごとに、クリティカル リソースが宣言されます。これらのリソースには、ディスク ボリューム (Microsoft Cluster Server の場合)、ボリューム グループ (MC/ServiceGuard の場合)、アプリケーション サービス、IP 名および IP アドレスなどがあります。

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

グローバル オプション ファイル
Data Protector をカスタマイズするためのファイル。このファイルでは、Data Protector のさまざまな設定 (特に、タイムアウトや制限) を定義でき、その内容は Data Protector セル全体に適用されます。このファイルは、HP-UX システムおよび Solaris システムでは `/etc/opt/omni/server/options` ディレクトリに置かれ、Windows システムでは *<Data_Protector_home>*`¥Config¥Server¥Options` ディレクトリに置かれます。

検証
指定したメディア上の Data Protector データが読み取り可能かどうかをチェックする機能。また、CRC (巡回冗長検査) オプションをオンにして実行したバックアップに対しては、各ブロック内の整合性もチェックできます。

コマンド行インタフェース (CLI)
CLI には、DOS コマンドや UNIX コマンドと同じようにシェル スクリプト内で使用でできるコマンドが用意されています。これらを通じて、Data Protector の構成、管理、バックアップ / 復元タスクを実行することができます。

再解析ポイント
(Windows 固有の用語)
任意のディレクトリまたはファイルに関連付けることができるシステム制御属性。再解析属性の値は、ユーザー制御データをとることができます。このデータの形式は、データを保存したアプリケーションによって認識され、データの解釈用にインストールされており、該当ファイルを

処理するファイルシステム フィルタによっても認識されます。ファイルシステムは、再解析ポイント付きのファイルを検出すると、そのデータ形式に関連付けられているファイルシステム フィルタを検索します。

サイト複製サービス
(Microsoft Exchange Server 2000/2003 固有の用語)
Exchange Server 5.5 ディレクトリ サービスをエミュレートすることで Exchange 5.5 との互換性を確保する Microsoft Exchange Server 2000/2003 サービス。
インフォメーション ストアおよび**キー マネージメント サービス***も参照。*

差分同期（再同期）
(EMC Symmetrix 固有の用語)
BCV または SRDF の制御操作の 1 つ。BCV 制御操作では、Incremental Establish (増分的確立) により、BCV デバイスが増分的に同期化され、EMC Symmetrix ミラー化メディアとして機能します。EMC Symmetrix デバイスは、事前にペアにしておく必要があります。
SRDF 制御操作では、Incremental Establish (増分的確立) により、ターゲット デバイス (R2) が増分的に同期化され、EMC Symmetrix ミラー化メディアとして機能します。EMC Symmetrix デバイスは、事前にペアにしておく必要があります。

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

差分バックアップ (differential backup)
作成済みで、まだ保護されている Data Protector バックアップ (フルまたは増分) をベースにした増分バックアップ。
***増分バックアップ**を参照。*

差分バックアップ (differential backup)
(MS SQL 固有の用語)
前回のフル データベース バックアップ以降にデータベースに対して加えられた変更だけを記録するデータベース バックアップ。
***バックアップの種類**も参照。*

差分リストア
(EMC Symmetrix 固有の用語)
BCV または SRDF の制御操作の 1 つ。
BCV 制御操作では、差分リストアにより、BCV デバイスがペア内の 2 番目に利用可能な標準デバイスのミ

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

システム ディスク
オペレーティング システム ファイルが入っているディスク。Microsoft の用語では、ブート プロセスの最初の手順に必要なファイルが入っているディスクと定義されています。

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

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

システム パーティション
オペレーティング システム ファイルが入っているパーティション。Microsoft の用語では、ブート プロセスの最初の手順に必要なファイルが入っているパーティションと定義されています。

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

事前割当てリスト
メディア プール内のメディアのサブセットをバックアップに使用する順に指定したリスト。

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

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

実行前 / 実行後コマンド
実行前コマンドおよび実行後コマンドは、バックアップ セッションまたは復元セッションの前後に付加的な処理を実行する実行可能ファイルまたはスクリプトです。実行前コマンドおよび実行後コマンドは、Data Protector で事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows 上で動作する実行可能ファイルまたはバッチファイル、UNIX 上で動作するシェル スクリプトなどを使用できます。

シャドウ コピー
(MS VSS 固有の用語)
特定の時点におけるオリジナル ボリューム (元のボリューム) の複製を表すボリューム。オリジナル ボリュームからではなく、シャドウ コピーからデータがバックアップされます。オリジナル ボリュームはバックアップ処理中も更新が可能ですが、ボリュームのシャドウ コピーは同じ内容に維持されます。
Microsoft Volume Shadow Copy Service *も参照。*

シャドウ コピー セット
(MS VSS 固有の用語)
同じ時点で作成されたシャドウ コピーのコレクション。
シャドウ コピー *も参照。*

シャドウ コピー プロバイダ
(MS VSS 固有の用語)
ボリューム シャドウ コピーの作成と表現を行うエンティティ。プロバ

イダは、シャドウ コピー データを所有して、シャドウ コピーを公開します。プロバイダは、ソフトウェアで実装することも (システム プロバイダなど)、ハードウェア (ローカル ディスクやディスク アレイ) で実装することもできます。
シャドウ コピー*も参照。*

ジュークボックス
ライブラリ*を参照。*

ジュークボックス デバイス
光磁気メディアまたはファイル メディアを格納するために使用する、複数のスロットからなるデバイス。ファイル メディアの格納に使用する場合、ジュークボックス デバイスは「ファイル ジュークボックス デバイス」と呼ばれます。

循環ログ
(Microsoft Exchange Server および Lotus Domino Server 固有の用語)
Microsoft Exchange および Lotus Domino Server のデータベース モードの 1 つ。トランザクション ログ ファイルは、対応するデータがデータベースにコミットした後、定期的に上書きされます。循環ログにより、ディスク記憶領域の消費が低減できます。

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

初期化
フォーマット*を参照。*

所有権
バックアップの所有権は、どのユーザーがバックアップからデータを復元できるかを決定します。あるユーザーが対話型バックアップを開始すると、そのユーザーはセッション オーナーになります。ユーザーが既存のバックアップ仕修正せずにそのまま起動した場合、そのバックアップ セッションは対話型とみなされません。この場合、バックアップ仕様内でバックアップ オーナーが指定されていれば、その指定が継承されます。バックアップ仕様内でバックアップ オーナーが指定されていなければ、バックアップを開始したユーザーがセッション オーナーになります。スケジューリングされたバックアップの場合、UNIX Cell Manager では root.sys@<Cell Manager> がデフォルトのセッション オーナーとなり、Windows Cell Manager では、Cell Manager のインストール時に指定されたユーザーがデフォルトのセッション オーナーとなります。所有権は変更可能なので、特定のユーザーをセッション オーナーにすることができます。

スイッチオーバー
フェイルオーバー*を参照。*

スキャン
デバイス内のメディアを識別する機能。これにより、MMDB を、選択した位置 (例えば、ライブラリ内のスロット) に実際に存在するメディアと同期させることができます。

スキャン
デバイス内のメディアを識別する機能。これにより、MMDB を、選択した位置 (例えば、ライブラリ内のスロット) に実際に存在するメディアと同期させることができます。デバイスに含まれる実際のメディアをスキャンしてチェックすると、第三者が Data Protector を使用せずにメディアを操作（挿入または取り出しなど）していないかどうかなどを確認できます。

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

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

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

ストレージ グループ
(Microsoft Exchange Server 2000/2003 固有の用語)
同じトランザクション ログ ファイルを共有する複数のデータベース (ストア) のコレクション。Exchange では、各ストレージ グループを個別のサーバ プロセスで管理します。

ストレージ ボリューム
(ZDB 固有の用語)
ストレージ ボリュームは、オペレーティング システムまたはボリューム管理システム、ファイル システム、または他のオブジェクトが存在可能なその他のエンティティに提供可能なオブジェクトを表します (たとえば仮想化技法)。ボリューム管理システム、ファイル システムはこの記憶域に構築されます。これらは通常、ディスク アレイなどの記憶システム内に作成または存在します。

スナップショット
(HP StorageWorks VA および HP StorageWorks EVA 固有の用語)
スナップショット作成技法を使用して作成された複製の形式。使用するアレイ / 技法に応じて、特徴の異なるさまざまな種類のスナップショットが使用できます。スナップショットで作成された複製は動的なもので、スナップショットの種類や作成時間によって、ソース ボリュームの内容に依存する仮想コピーか、独立した正確な複製 (クローン) かのいずれかになります。
複製および**スナップショット作成** *も参照。*

スナップショット 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)
ソース ボリュームのコピー (ストレージ仮想化技法を使用) を作成する複製技法。複製はある一時点で作成されたものと見なされ、事前構成することなく、即座に使用できます。ただし、通常は複製作成後もコピー プロセスはバックグラウンドで継続されます。
スナップショット *も参照。*

スパース ファイル
ブロックが空の部分を含むファイル。一部のデータにゼロが含まれているマトリックス、イメージ アプリケーションで作成したファイル、高速データベースなどの場合にスパース ファイルが生じます。スパース ファイルの処理を復元中に有効にしておかないと、スパース ファイルを復元できなくなる可能性があります。

スプリット ミラー
(EMC Symmetrix および HP StorageWorks Disk Array XP 固有の用語)
スプリット ミラー技法を使用して作成された複製。複製により、ソース ボリュームの内容について独立した正確な複製 (クローン) が作成されます。
複製および**スプリット ミラー バックアップ** *も参照。*

スプリット ミラー バックアップ
(EMC Symmetrix 固有の用語)
テープへの ZDB *を参照。*

スプリット ミラー バックアップ
(HP StorageWorks Disk Array XP 固有の用語)
テープへの ZDB、**ディスクへの**

ZDB、および**ディスク / テープへの ZDB** *を参照。*

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

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

スレッド
(MS SQL Server 7.0/2000 固有の用語)
単一のプロセスにのみ所属する実行可能エンティティ。プログラム カウンタ、ユーザー モード スタック、カーネル モード スタック、および 1 式のレジスタ値からなります。同じプロセス内で複数のスレッドを同時に実行できます。

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

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

セカンダリ ボリューム (S-VOL)
(HP StorageWorks Disk Array XP 固有の用語)
セカンダリ ボリューム (S-VOL) は、他の LDEV (P-VOL) のセカンダリ CA ミラーまたは BC ミラーとしての役割を果たす XP LDEV。CA の場

合、S-VOL を MetroCluster 構成内のフェイルオーバー デバイスとして使うことができます。S-VOL には、P-VOL によって使用されるアドレスとは異なる、個別の SCSI アドレスが割り当てられます。
プライマリ ボリューム (P-VOL) *も参照。*

セッション
バックアップ セッション、**メディア管理セッション**および**復元セッション***を参照。*

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

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

セル
1 台の Cell Manager に管理されているシステムの集合。セルには、一般に、同じ LAN に接続されたサイトや組織エンティティ上のシステムが含まれます。バックアップおよび復元のポリシーとタスクは、1 か所から集中管理できます。

ゼロ ダウンタイム バックアップ (ZDB)
ディスク アレイにより実現したデータ複製技術を用いて、アプリケーション システムのバックアップ処理の影響を最小限に抑えるバックアップ アプローチ。バックアップされるデータの複製がまず作成されます。その後のすべてのバックアップ処理は、元のデータではなく複製データを使って実行し、アプリケーション システムは通常の処理に復帰します。
ディスクへの ZDB、**テープへの ZDB**、**ディスク / テープへの ZDB**、および**インスタント リカバリ** *も参照。*

増分 1 メールボックス バックアップ
増分 1 メールボックス バックアップでは、前回のフル バックアップ以降にメールボックスに対して行われた変更をすべてバックアップします。

増分バックアップ
前回のバックアップ以降に変更があったファイルだけを選択するバッ

クアップ。増分バックアップには、複数のレベルがあり、前回の増分バックアップ以降に変更されたファイルだけをバックアップできます。**バックアップの種類***も参照。*

増分バックアップ
(Microsoft Exchange Server 固有の用語)
前回のフル バックアップまたは増分バックアップ以降の変更だけをバックアップする Microsoft Exchange Server データのバックアップ。増分バックアップでは、バックアップ対象はトランザクション ログだけです。
バックアップの種類*も参照。*

増分メールボックス バックアップ
増分メールボックス バックアップでは、前回の各種バックアップ以降にメールボックスに対して行われた変更をすべてバックアップします。

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

ターゲット デバイス (R2) *も参照。*

ソース ボリューム
(ZDB 固有の用語)
複製されたデータを含むストレージ ボリューム。

ターゲット システム
(障害復旧固有の用語)
障害が発生したシステム。ターゲット システムは、ブート不能な状態になっていることが多く、そのような状態のシステムを元のシステム構成に戻すことが障害復旧の目標となります。クラッシュしたシステムがそのままターゲット システムになるのではなく、正常に機能していないハードウェアをすべて交換することで、クラッシュしたシステムがターゲット システムになります。

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

ターゲット デバイス (R2)
(EMC Symmetrix 固有の用語)
ソース デバイス (R1) との SRDF 操作に参加する EMC Symmetrix デバイス。リモート EMC Symmetrix ユニット内に置かれます。ローカル EMC Symmetrix ユニット内でソース

デバイス (R1) とペアになり、ミラー化ペアから、すべての書き込みデータを受け取ります。このデバイスは、通常の I/O 操作ではユーザーアプリケーションからアクセスされません。R2 デバイスは、RDF2 グループ タイプに割り当てる必要があります。
ソース デバイス (R1) *も参照。*

ターゲット ボリューム
(ZDB 固有の用語)
データの複製先のストレージ ボリューム。

ターミナル サービス
(Windows 固有の用語)
Windows のターミナル サービスは、サーバ上で実行されている仮想 Windows デスクトップ セッションと Windows ベースのプログラムにクライアントからアクセスできるマルチセッション環境を提供します。

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

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

- DISK タイプ
- SBT_TAPE タイプ

Oracle が Data Protector と統合されており、指定されたチャネルの種類が SBT_TAPE タイプの場合は、上記のサーバ プロセスが Data Protector に対してバックアップの読み取りとデータ ファイルの書き込みを試行します。

ディスク / テープへの ZDB
(ZDB 固有の用語)

ゼロ ダウンタイム バックアップの 1 つの形式。ディスクへの ZDB と同様に、作成された複製が特定の時点でのソース ボリュームのバックアップとしてディスク アレイに保持されます。ただし、テープへの ZDB と同様、複製データはバックアップ メディアにもストリーミングされます。このバックアップ方法を使用した場合、同じセッションでバックアップしたデータは、インスタント リカバリ、Data Protector 標準のテープからの復元を使用して復元できます。スプリット ミラー アレイではスプリット ミラー復元が可能です。

ゼロ ダウンタイム バックアップ (ZDB)、**ディスクへの ZDB**、**テープへの ZDB**、**インスタント リカバリ**、**複製**、および**複製セット ローテーション** *も参照。*

ディスク イメージ (raw ディスク) のバックアップ

ディスク イメージのバックアップでは、ファイルがビットマップ イメージとしてバックアップされるので、高速バックアップが実現します。ディスク イメージ (raw ディスク) バックアップでは、ディスク上のファイルおよびディレクトリの構造はバックアップされませんが、ディスク イメージ構造がバイト レベルで保存されます。ディスク イメージ バックアップは、ディスク全体か、またはディスク上の特定のセクションを対象にして実行できます。

ディスク クォータ

コンピュータ システム上のすべてのユーザーまたはユーザーのサブセットに対してディスク スペースの消費を管理するためのコンセプト。このコンセプトは、いくつかのオペレーティング システム プラットフォームで採用されています。

ディスク グループ

(Veritas Volume Manager 固有の用語)

VxVM システムにおけるデータ ストレージの基本単位。ディスク グループは、1 つまたは複数の物理ボリュームから作成できます。同じシステム上に複数のディスク グループを置くことができます。

ディスク ステージング

複数のフェーズでデータをバックアップするプロセス。これにより、バックアップと復元のパフォーマンスが改善し、バックアップ データの保存コストが低減し、復元に対するデータの可用性とアクセス性が向上します。バックアップ ステージは、最初に 1 種類のメディア (たとえば、ディスク) にデータをバックアップし、その後データを異なる種類のメディア (たとえば、テープ)

にコピーすることから構成されます。

ディスク検出
ディスク検出では、クライアントのバックアップ中にディスクを検出します。このとき Data Protector が探索 (検出) するのは、クライアント上に存在するディスクで、バックアップの構成時にシステム上に存在なかったディスクも検出の対象に含まれます。検出されたディスクがバックアップされます。この機能は、構成が頻繁に変更される動的な環境の場合に特に役立ちます。ディスクが展開されると、それぞれのディスクがマスター クライアント オブジェクトのオプションをすべて継承します。実行前コマンドと実行後コマンドは、1 回しか指定されていなくても、オブジェクトごとに繰り返し起動されることになります。

ディスク検出によるクライアントのバックアップ
クライアントにマウントされているすべてのファイルシステムのバックアップ。バックアップの開始時に、Data Protector がクライアント上のディスクを自動検出します。ディスク検出によるクライアント バックアップでは、バックアップ構成が単純化され、ディスクのマウント / アンマウントが頻繁に行われるシステムに対するバックアップ効率が向上されます。

ディスクへの ZDB
(ZDB 固有の用語)
ゼロ ダウンタイム バックアップの 1 つの形式。作成された複製が、特定の時点でのソース ボリュームのバックアップとしてディスク アレイに保持されます。同じバックアップ仕様を使って別の時点で作成された複数の複製を、複製セットに保持することができます。テープに ZDB した複製はインスタント リカバリ プロセスで復元できます。
ゼロ ダウンタイム バックアップ (ZDB)、**テープへの ZDB**、**ディスク / テープへの ZDB**、**インスタント リカバリ**、および**複製セット ローテーション** *も参照。*

ディレクトリ ストア (DS)
(Microsoft Exchange 固有の用語)
Microsoft Exchange Server ディレクトリの一部。Microsoft Exchange Server ディレクトリには、メッセージング システムで提供されるサービス、メールボックス、受信者レコード、パブリック フォルダなどをアプリケーションから検索およびアクセスするために Microsoft Exchange アプリケーションが使用するオブジェクトが格納されます。
インフォメーション ストア (MDB) *も参照。*

ディレクトリ接合

(Windows 固有の用語)
ディレクトリ接合は、Windows の再解析ポイントのコンセプトに基づいています。NTFS 5 ディレクトリ接合では、ディレクトリ / ファイル要求を他の場所にリダイレクトできます。

データ ストリーム
通信チャネルを通じて転送されるデータのシーケンス。

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

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

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

データベースの差分バックアップ
前回のフル データベース バックアップ以降にデータベースに対して加えられた変更だけを記録するデータベース バックアップ。

データベースの並列処理 (数)
十分な台数のデバイスが利用可能で、並列バックアップを実行できる場合には、複数のデータベースが同時にバックアップされます。

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

テープへの ZDB
(ZDB 固有の用語)
ゼロ ダウンタイム バックアップの 1 つの形式。作成された複製が、バックアップ メディア (通常はテープ) にストリーミングされます。このバックアップ形式ではインスタント リカバリはできませんが、バックアップ終了後にディスク アレイ上に複製を保持する必要がありません。バックアップ データは Data Protector 標準のテープからの復元を使用して復元できます。スプリット

ミラー アレイでは、スプリット ミラー復元も使用することができます。
ゼロ ダウンタイム バックアップ (ZDB)、**ディスクへの ZDB**、**インスタント リカバリ**、**ディスク / テープへの ZDB**、および**複製** *も参照。*

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

テープレス バックアップ
(ZDB 固有の用語)
ディスクへの ZDB *を参照。*

デバイス
ドライブまたはより複雑な装置 (ライブラリなど) を格納する物理装置。

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

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

デバイス チェーン
デバイス チェーンは、シーケンシャルに使用するように構成された複数のスタンドアロン デバイスからなります。デバイスチェーンに含まれるデバイスのメディアで空き容量がなくなると、自動的に次のデバイスのメディアに切り替えて、バックアップを継続します。

統合セキュリティ
(MS SQL 固有の用語)
統合セキュリティは、Microsoft SQL

Server が Windows の認証メカニズムを使用して、すべての接続に対する Microsoft SQL Server ログインの妥当性をチェックできるようにします。統合セキュリティを使用していれば、すべてのユーザーが同じパスワードで Windows と Microsoft SQL Server の両方にログインできます。すべてのクライアントが信頼関係接続をサポートしている環境では、統合セキュリティを使うことをお勧めします。信頼関係接続とは、Windows Server によって妥当性がチェックされ、Microsoft SQL Server に受け付けられた接続を意味します。信頼関係接続だけが許可されます。

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

同時処理数
Disk Agent の同時処理数*を参照。*

動的 (ダイナミック) クライアント ディスク検出によるクライアント バックアップ*を参照。*

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

ドライブ
コンピュータ システムからデータを受け取って、磁気メディア (テープなど) に書き込む物理装置。データをメディアから読み取って、コンピュータ システムに送信することもできます。

ドライブのインデックス
ライブラリ デバイス内のドライブの機械的な位置を識別するための数字。ロボット機構によるドライブ アクセスは、この数に基づいて制御されます。

トランザクション
一連のアクションを単一の作業単位として扱えるようにするためのメカニズム。データベースでは、トランザクションを通じて、データベースの変更を追跡します。

トランザクション バックアップ
トランザクション バックアップは、一般に、データベースのバックアップよりも必要とするリソースが少ないため、データベースのバックアップよりもより高い頻度で実行できます。トランザクション バックアップを適用することで、データベースを問題発生以前の特定の時点の状態に復旧することができます。

トランザクション バックアップ
(Sybase および SQL 固有の用語)
トランザクション ログをバックアップすること。トランザクション ログには、前回のフル バックアップまたはトランザクション バックアップ以降に発生した変更が記録されます。

トランザクション ログ
(*Data Protector 固有の用語*)
IDB に対する変更を記録します。IDB 復旧に必要なトランザクション ログ ファイル (前回の IDB バックアップ以降に作成されたトランザクション ログ) が失われることがないように、トランザクション ログのアーカイブを有効化しておく必要があります。

トランザクション ログ テーブル
(Sybase 固有の用語)
データベースに対するすべての変更が自動的に記録されるシステム テーブル。

トランザクション ログ バックアップ
トランザクション ログ バックアップは、一般に、データベースのバックアップよりも必要とするリソースが少ないため、データベースのバックアップよりもより高い頻度で実行できます。トランザクションログ バックアップを用いることにより、データベースを特定の時点の状態に復元できます。

トランザクション ログ ファイル
データベースを変更するトランザクションを記録するファイル。データベースが破損した場合にフォールトトレランスを提供します。

トランスポータブル スナップショット
(MS VSS 固有の用語)
アプリケーション システム上に作成されるシャドウ コピー。このシャドウ コピーは、バックアップを実行するバックアップ システムに提供できます。
Microsoft Volume Shadow Copy Service (VSS) ***も参照。***

ハード リカバリ
(Microsoft Exchange Server 固有の用語)
トランザクション ログ ファイルを使用し、データベース エンジンによる復元後に実行される Microsoft Exchange Server のデータベース復旧。

ハートビート
特定のクラスタ ノードの動作ステータスに関する情報を伝達するタイム スタンプ付きのクラスタ データ セット。このデータ セット (パ

ケット) は、すべてのクラスタ ノードに配布されます。

バックアップ オーナー
IDB の各バックアップ オブジェクトにはオーナーが定義されてます。デフォルトのオーナーは、バックアップ セッションを開始したユーザーです。

バックアップ オブジェクト
1 つのディスク ボリューム (論理ディスクまたはマウント ポイント) からバックアップされた項目すべてを含むバックアップ単位。バックアップ項目は、任意の数のファイル、ディレクトリ、ディスク全体またはマウント ポイントの場合が考えられます。また、バックアップ オブジェクトはデータベース エンティティまたはディスク イメージ (raw ディスク) の場合もあります。

バックアップ オブジェクトは以下のように定義されます。

- クライアント名 : バックアップ オブジェクトが保存される Data Protector クライアントのホスト名
- マウント ポイント : バックアップ オブジェクトが存在するクライアント上のディレクトリ構造 (Windows ではドライブ、UNIX ではマウント ポイント) におけるアクセス ポイント
- 説明 : 同一のクライアント名とマウント ポイントを持つバックアップ オブジェクトを一意に定義
- 種類 : バックアップ オブジェクトの種類 (たとえば、ファイル システムや Oracle など)

バックアップ システム
(ZDB 固有の用語)
1 つ以上のアプリケーション システムのターゲット ボリュームに接続しているシステム。典型的なバックアップ システムは、バックアップ デバイスに接続され、複製内のデータのバックアップを実行します。***アプリケーション システム***、***ターゲット ボリューム***および***複製も参照。***

バックアップ セッション
データのコピーを記憶メディア上に作成するプロセス。バックアップ仕様に処理内容を指定することも、対話式に操作を行うこともできます (対話式セッション)。1 つのバックアップ仕様の中で複数のクライアントが構成されている場合、すべてのクライアントが同じバックアップの種類 (フルまたは増

分) を使って、1 回のバックアップ セッションで同時にバックアップされます。バックアップ セッションの結果、1 式のメディア にバックアップ データが書き込まれます。これらのメディアは、バックアップ セットまたはメディア セットとも呼ばれます。
増分バックアップおよび**フル バックアップ** *も参照。*

バックアップ セット
バックアップに関連したすべての統合ソフトウェア オブジェクトのセットです。

バックアップ セット
(Oracle 固有の用語)
RMAN バックアップ コマンドを使用して作成したバックアップファイルの論理グループ。バックアップ セットは、バックアップに関連したすべてのファイルのセットです。これらのファイルはパフォーマンスを向上するため多重化することができます。バックアップ セットにはデータファイルまたはアーカイブ ログのいずれかを含めることができますが、両方同時に使用できません。

バックアップ チェーン
バックアップ チェーンは、フル バックアップと増分バックアップが実行される状況で登場する概念です。実行する増分バックアップのレベル ([増分]、[増分 1]、[増分 2] など) により、前回の増分と今回の増分の間に、単純な (場合によっては多少複雑な) 依存関係が発生します。バックアップ チェーンは、フル バックアップから始まり、目的の時点までに実行された依存関係のある増分バックアップすべてを含みます。

バックアップ デバイス
記憶メディアに対するデータの読み書きが可能な物理デバイスを Data Protector で使用できるように構成したもの。例えば、スタンドアロン DDS/DAT ドライブやライブラリなどをバックアップ デバイスとして使用できます。

バックアップ ビュー
Data Protector では、バックアップ仕様のビューを切り替えることができます。[種類別] (デフォルト) を選択すると、バックアップ / テンプレートで利用できるデータの種類に基づいたビューが表示されます。[グループ別] を選択すると、バックアップ仕様 / テンプレートの所属先のグループに基づいたビューが表示されます。[名前別] を選択すると、バックアップ仕様 / テンプレートの名前に基づいたビューが表示されます。[Manager 別] (MoM の実行時の

み有効) を選択すると、バックアップ仕様 / テンプレートの所属先の Cell Manager に基づいたビューが表示されます。

バックアップ API
Oracle のバックアップ / 復元ユーティリティとバックアップ / 復元メディア管理層の間にある Oracle インタフェース。このインタフェースによってルーチンのセットが定義され、バックアップ メディアのデータの読み書き、バックアップ ファイルの作成や検索、削除が行えるようになります。

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

バックアップ仕様
バックアップ対象オブジェクトを、使用するデバイスまたはドライブのセット、仕様内のすべてのオブジェクトに対するバックアップ オプション、バックアップを行いたい日時とともに指定したリスト。オブジェクトとなるのは、ディスクやボリューム全体、またはその一部、たとえばファイル、ディレクトリ、Windows レジストリなどです。インクルード リストおよびエクスクルード リストを使用して、ファイルを選択することもできます。

バックアップ世代
1 つのフル バックアップとそれに続く増分バックアップを意味します。次のフル バックアップが行われると、世代が新しくなります。

バックアップの種類
増分バックアップ、**差分バックアップ (differential backup)**、**トランザクション バックアップ**、**フル バックアップ**および**差分バックアップ (delta backup)** *を参照。*

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

パブリック フォルダ ストア
(*Microsoft Exchange Server 2000/2003 固有の用語*)
インフォメーション ストアのうち、パブリック フォルダ内に情報を維持する部分。パブリック フォルダ ストアは、バイナリ リッチテキスト .edb ファイルと、ストリーミング ネイティブ インターネット コンテンツを格納する .stm ファイルから構成されます。

パブリック / プライベート バックアップ データ
バックアップを構成する際は、バックアップ データをパブリックまたはプライベートのいずれにするかを選択できます。

- パブリック データ ― すべての Data Protector ユーザーに対してアクセスと復元が許可されます。
- プライベート データ ― バックアップの所有者および管理者に対してのみ表示と復元が許可されます。

標準セキュリティ
(MS SQL 固有の用語)
標準セキュリティでは、Microsoft SQL Server のログイン妥当性チェック プロセスをすべての接続に対して使用します。標準セキュリティは、ネットワーク内にさまざまなクライアントが混在しており、一部のクライアントでは信頼関係接続がサポートされていない場合に使用できます。また、以前のバージョンの SQL Server との下位互換性を確保する必要がある場合にも、標準セキュリティを使用できます。
統合セキュリティ *も参照。*

ファースト レベル ミラー
(*HP StorageWorks Disk Array XP 固有の用語*)
HP StorageWorks Disk Array XP では、プライマリ ボリュームのミラー コピーを最大 3 つまで作成することができ、このコピー 1 つにつきさらに 2 つのコピーを作成できます。最初の 3 つのミラー コピーはファースト レベル ミラーと呼ばれます。
プライマリ ボリュームおよび **MU 番号** *を参照。*

ファイル ジュークボックス デバイス
ファイル メディアを格納するために使用する、複数のスロットからなるディスク上に存在するデバイス

ファイル デポ
バックアップからファイル ライブラリ デバイスまでのデータを含むファイル。

ファイル バージョン

フル バックアップや増分バックアップでは、ファイルが変更されている場合、同じファイルが複数回バックアップされます。バックアップのロギング レベルとして [すべてログに記録] を選択している場合は、ファイル名自体に対応する 1 つのエントリとファイルの各バージョンに対応する個別のエントリが IDB 内に維持されます。

ファイル ライブラリ デバイス
複数のメディアからなるライブラリをエミュレートするディスク上に存在するデバイス。ファイル デポと呼ばれる複数のファイルが格納されます。

ファイルシステム
ハード ディスク上に一定の形式で保存されたファイルの集まり。ファイルシステムは、ファイル属性とファイルの内容がバックアップ メディアに保存されるようにバックアップされます。

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

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

ブール演算子
オンライン ヘルプ システムの全文検索には、AND、OR、NOT、NEAR の各ブール演算子を使用できます。複数の検索条件をブール演算子で組み合わせて指定することで、検索対象をより正確に絞り込むことができます。複数単語の検索に演算子を指定しなければ、AND を指定したものとみなされます。例えば、「マニュアル 障害 復旧」という検索条件は、「マニュアル AND 障害 AND 復旧」と同じ結果になります。

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

保守時に発生します。

フォーマット
メディアを Data Protector で使用できるように初期化するプロセス。メディア上の既存データはすべて消去されます。メディアに関する情報 (メディア ID、説明、および位置) が IDB に保存されるとともに、メディア自体 (メディア ヘッダ) にも書き込まれます。データが保護されている Data Protector メディアは、保護の期限が切れるか、保護解除 / リサイクルされない限り再フォーマットされません。

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

復元セッション
バックアップ メディアからクライアントシステムにデータをコピーするプロセス。

複製
(ZDB 固有の用語)
ユーザー指定のバックアップ オブジェクトを含む、特定の時点におけるソース ボリュームのデータのイメージ。イメージは、作成するハードウェア / ソフトウェアによって、物理ディスク レベルでの記憶ブロックの独立した正確な複製 (クローン) になる (スプリット ミラーなど) 場合もあれば、仮想コピーになる (スナップショットなど) 場合もあります。ホストの視点では、標準的な UNIX または Windows システムについて、バックアップ オブジェクトを含む物理ディスク全体が複製されます。しかし、UNIX でボリューム マネージャを使用するときは、バックアップ オブジェクトを含むボリューム / ディスク グループ全体が複製されます。
スナップショット、**スナップショット作成**、**スプリット ミラー**、および**スプリット ミラーの作成***も参照。*

複製セット
(ZDB 固有の用語)
同じバックアップ仕様を使って作成される複製のグループ。
複製および**複製セット ローテー**

ション *も参照。*

複製セット ローテーション
(ZDB 固有の用語)
通常のバックアップ作成のために継続的に複製セットを使用すること。複製セットの使用を必要とする同一のバックアップ仕様が実行されるたびに、新規の複製がセットの最大数になるまで作成され、セットに追加されます。その後、セット内の最も古い複製は置き換えられ、セット内の複製の最大数が維持されます。
複製および**複製セット** *も参照。*

物理デバイス
ドライブまたはより複雑な装置 (ライブラリなど) を格納する物理装置。

プライベート インフォメーション ストア
(Microsoft Exchange Server 5.5 固有の用語)
ユーザー メールボックスの中に情報を保存するインフォメーション ストアの一部。1 つのメールボックス ストアは、1 つのバイナリ リッチ テキスト .edb ファイルから構成されます。

プライマリ ボリューム (P-VOL)
(HP StorageWorks Disk Array XP 固有の用語)
CA 構成および BC 構成用プライマリ ボリューム (P-VOL) としての役割を果たす複数の標準 HP StorageWorks Disk Array XP LDEV です。P-VOL は MCU 内に配置されています。
セカンダリ ボリューム (S-VOL) *も参照。*

フリー プール
フリー プールは、メディア プール内のすべてのメディアが使用中になっている場合にメディアのソースとして補助的に使用できるプールです。ただし、メディア プールでフリー プールを使用するには、明示的にフリー プールを使用するように構成する必要があります。

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

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

フル メールボックス バックアップ
フル メールボックス バックアップでは、メールボックス全体の内容をバックアップします。

分散ファイルシステム (DFS)
複数のファイル共有を単一の名前空間に接続するサービス。対象となるファイル共有は、同じコンピュータに置かれていても、異なるコンピュータに置かれていてもかまいません。DFS は、リソースの保存場所の違いに関係なくクライアントがリソースにアクセスできるようにします。

ペア ステータス
(HP StorageWorks Disk Array XP 固有の用語)
ミラー化されたディスクのペアは、そのペア上で実行されるアクションによって、様々なステータス値を持ちます。最も重要なステータス値は以下の 3 つです。

- コピー - ミラー化されたペアは、現在再同期中。データは一方のディスクからもう一方のディスクに転送されます。2 つのディスクのデータは同じではありません。
- ペア - ミラー化されたペアは、完全に同期されており、両方のディスク (プライマリ ボリュームとミラー ボリューム) は全く同じデータを持ちます。
- 中断 - ミラー化されたディスク間のリンクは中断されています。両方のディスクが別々にアクセスされ、更新されています。ただし、ミラー関係はまだ保持されており、このペアは、ディスク全体を転送することなく、再同期することができます。

並列処理 (数)
オンライン データベースから複数のデータ ストリームを読み取ること。

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

保護
データ保護および**カタログ保護***を参*

照。

ホスト システム
Data Protector Disk Agent がインストールされており、ディスク デリバリーによる障害復旧に使用される稼動中の Data Protector クライアント。

ホスト バックアップ
ディスク検出によるクライアント バックアップ *を参照。*

ボリューム グループ
LVM システムにおけるデータ ストレージ単位。ボリューム グループは、1 つまたは複数の物理ボリュームから作成できます。同じシステム上に複数のボリューム グループを置くことができます。

ボリューム マウントポイント
(*Windows 固有の用語*)
ボリューム上の空のディレクトリを他のボリュームのマウントに使用できるように構成したもの。ボリューム マウント ポイントは、ターゲット ボリュームへのゲートウェイとして機能します。リュームがマウントされていれば、ユーザーやアプリケーションがそのボリューム上のデータをフル (マージ) ファイルシステム パスで参照できます (両方のボリュームが一体化されている場合)。

マージ
復元中のファイル名競合を解決するモードの 1 つ。復元するファイルと同じ名前のファイルが復元先に存在する場合、変更日時の新しい方が維持されます。既存のファイルと名前が重複しないファイルは、常に復元されます。
上書き *も参照。*

マウント ポイント
ディレクトリ構造内において、ディスクまたは論理ボリュームにアクセスするためのアクセス ポイント (`/opt` や `d:` など)。UNIX では、`bdf` コマンドまたは `df` コマンドを使ってマウント ポイントを表示できます。

マウント要求
マウント要求時には、デバイスにメディアを挿入するように促す画面が表示されます。必要なメディアを挿入して確認することでマウント要求に応答すると、セッションが続行されます。

マジック パケット
Wake ONLAN を参照。

マルチドライブ サーバ
単一システム上で Media Agent を無制限に使用できるライセンス。このライセンスは、Cell Manager の IP アドレスにバインドされており、新し

いバージョンでは廃止されました。

ミラー
(EMC Symmetrix および HP StorageWorks Disk Array XP 固有の用語)
ターゲット ボリューム *を参照。*

ミラー ローテーション
(HP StorageWorks Disk Array XP 固有の用語)
複製セット ローテーション *を参照。*

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

無人操作 (unattended operation)
無人操作 (lights-out operation) *を参照。*

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

メールボックス ストア
(*Microsoft Exchange Server 2000/2003 固有の用語)*
インフォメーション ストアのうち、ユーザー メールボックス内の情報を維持する部分。メールボックス ストアは、バイナリ データを格納するリッチテキスト .edb ファイルと、ストリーミング ネイティブ インターネット コンテンツを格納する .stm ファイルからなります。

メディア ID
Data Protector がメディアに割り当てる一意な識別子。

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

メディア プール
同じ種類のメディア (DDS) などのセット。グループとして追跡されます。フォーマットしたメディアは、メディア プールに割り当てられます。

メディア ラベル
メディアに割り当てられるユーザー定義の識別子。

メディア管理セッション
初期化、内容のスキャン、メディア上のデータの確認、メディアのコピーなどのアクションをメディアに対して実行するセッション。

メディア集中管理データベース (CMMDB)
CMMDB *を参照。*

メディア状態要素
使用回数のしきい値と上書きのしきい値。メディアの状態の判定基準となります。

メディアの位置
バックアップ メディアが物理的に収納されている場所を示すユーザー定義の識別子。"building 4" や "off-site storage" のような文字列です。

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

メディアのエクスポート
メディアに格納されているすべてのバックアップ セッション情報 (システム、オブジェクト、ファイル名など) を IDB から削除するプロセス。メディア自体に関する情報やメディアとプールの関係に関する情報も IDB から削除されます。メディア上のデータは影響されません。
メディアのインポート *も参照。*

メディアの種類
メディアの物理的な種類 (DDS や DLT など)。

メディアの状態
メディア状態要素から求められるメディアの品質。テープ メディアの使用頻度が高く、使用時間が長ければ、読み書きエラーの発生率が高くなります。状態が [不良] になったメディアは交換する必要があります。

メディアの使用法
ここでは、メディアの使用法として、以下のオプションのいずれかを選択します。メディアの使用法は、[**追加可能**]、[**追加不可能**]、[**増分のみ追加可能**] のいずれかに設定できます。

メディアのボールティング
メディアを安全な別の場所に収納すること。メディアが復元に必要になった場合や、今後のバックアップ

にメディアを再使用する場合は、メディアをデータ センターに戻します。ボールティング手順は、会社のバックアップ戦略やデータ保護 / 信頼性ポリシーに依存します。

メディアの割り当て方針
メディアをバックアップに使用する順序を決定します。[Strict] メディア割り当てポリシーでは、特定のメディアに限定されます。[Loose] ポリシーでは、任意の適切なメディアを使用できます。[フォーマットされていないメディアを先に割り当てる] ポリシーでは、ライブラリ内に利用可能な非保護メディアがある場合でも、不明なメディアが優先されます。

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

ユーザー アカウント
Data Protector を使用するには、Data Protector のユーザー アカウントが必要です。Data Protector のユーザー アカウントは、Data Protector やバックアップされたデータに対する無断アクセスを制限します。Data Protector 管理者がこのアカウントを作成するときには、ユーザー ログオン名、ユーザーのログオン元として有効なシステム、および Data Protector ユーザー グループのメンバーシップを指定します。ユーザーが Data Protector のユーザー インタフェースを起動するか、または特定のタスクを実行するときには、このアカウントが必ずチェックされます。

ユーザー グループ
各 Data Protector ユーザーは、ユーザー グループのメンバーです。各ユーザー グループには 1 式のユーザー権限があり、それらの権限がユーザー グループ内のすべてのユーザーに付与されます。ユーザー権限を関連付けるユーザー グループの数は、必要に応じて定義できます。Data Protector には、admin、operator、user の 3 つのデフォルト ユーザー グループがあります。

ユーザー ディスク割り当て
NTFS のクォータ管理サポートにより、追跡システムが強化されており、共有ストレージ ボリュームのディスク スペースの使用量を制御できます。Data Protector では、システム全体とすべての構成済みユーザーを対象にユーザー ディスク クォータを同時にバックアップします。

ユーザー プロファイル
(Windows 固有の用語)
ユーザー別に維持される構成情報。

この情報には、デスクトップ設定、画面表示色、ネットワーク接続などが含まれます。ユーザーがログオンすると、そのユーザーのプロファイルがロードされ、Windows 環境がそれに応じて設定されます。

ユーザー権限
特定の Data Protector タスクの実行に必要なパーミッションをユーザー権限またはアクセス権限と呼びます。主なユーザー権限には、バックアップの構成、バックアップ セッションの開始、復元セッションの開始などがあります。ユーザーには、そのユーザーの所属先ユーザー グループに関連付けられているアクセス権限が割り当てられます。

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

ライター
(MS VSS 固有の用語)
オリジナル ボリューム上のデータの変更を開始するプロセス。主に、永続的なデータをボリューム上に書き込むアプリケーションまたはシステム サービスがライターとなります。ライターは、シャドウ コピーの同期化プロセスにも参加し、データの整合性を保証します。

ライブラリ
オートチェンジャー、ジュークボックス、オートローダ、またはエクスチェンジャとも呼ばれます。ライブラリには、複数のレポジトリ スロットがあり、それらにメディアが格納されます。各スロットがメディア (DDS/DAT など) を 1 つずつ格納します。スロット / ドライブ間でのメディアの移動は、ロボット機構によって制御され、メディアへのランダム アクセスが可能です。ライブラリには、複数のドライブを格納できます。

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

- Oracle ターゲット データベースの物理スキーマ
- データ ファイルおよび archivelog バックアップ セット
- データ ファイルのコピー
- アーカイブ REDO ログ
- ストアド スクリプト

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

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

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

リサイクル
メディア上のすべてのバックアップ データのデータ保護を解除して、以降のバックアップで上書きできるようにするプロセス。同じセッションに所属しているデータのうち、他のメディアに置かれているデータも保護解除されます。リサイクルを行っても、メディア上のデータ自体は変更されません。

リムーバブル記憶域の管理データベース
(Windows 固有の用語)
Windows サービスの 1 つ。リムーバブル メディア (テープやディスクなど) と記憶デバイス (ライブラリ) の管理に使用されます。リムーバブル記憶域により、複数のアプリケーションが同じメディア リソースを共有できます。

ローカル復旧とリモート復旧
リモート復旧は、SRD ファイルで指定されている Media Agent ホストがすべてアクセス可能な場合にのみ実行されます。いずれかのホストがアクセス不能になっていると、障害復旧プロセスがローカル モードにフェールオーバーされます。これ

は、ターゲット システムにローカル接続しているデバイスが検索されることを意味します。デバイスが 1 台しか見つからない場合は、そのデバイスが自動的に使用されます。複数のデバイスが見つかった場合は、デバイスが選択できるプロンプトが表示され、ユーザーが選択したデバイスが復元に使用されます。

ロギング レベル
ロギング レベルは、バックアップまたはオブジェクトのコピー時にファイルとディレクトリに関する情報をどの程度まで詳細に IDB に記録するかを示します。バックアップ時のロギング レベルに関係なく、データの復元は常に可能です。Data Protector には、[すべてログに記録]、[ディレクトリ・レベルまでログに記録]、[ファイル・レベルまでログに記録]、および [ログなし] の 4 つのロギング レベルがあります。ロギング レベルの設定によって、IDB のサイズ増加、バックアップ速度、復元対象データのブラウズしやすさが影響を受けます。

ログイン ID
(MS SQL Server 固有の用語)
ユーザーが Microsoft SQL Server にログオンするための名前。Microsoft SQL Server の syslogin システム テーブル内のエントリに対応するログイン ID が有効なログイン ID となります。

ロック名
別のデバイス名を使うことで同じ物理デバイスを違う特性で何度も構成することができます。

そのようなデバイス (デバイス名) が複数同時に使用された場合に重複を防ぐ目的で、デバイス構成をロックするためにロック名が使用されます。ロック名はユーザーが指定する文字列です。同一の物理デバイスを使用するデバイス定義には、すべて同じロック名を使用します。

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

ワイルドカード文字
1 文字または複数文字を表すために使用できるキーボード文字。たとえば、通常、アスタリスク (*) は 1 文字以上の文字を表し、疑問符 (?) は

1 文字を示します。ワイルドカード文字は、名前により複数のファイルを指定するための手段としてオペレーティング システムで頻繁に使用されます。

す

と