

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

出版年月 : 2006 年 7 月



Manufacturing Part Number : B6960-96027

リリース **A.06.00**

© Copyright 2006 Hewlett-Packard Development Company, L.P.

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直接損害、間接損害、特別損害、付随的損害または結果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。

本書には著作権によって保護される内容が含まれています。本書の内容の一部または全部を著作者の許諾なしに複製、改変、および翻訳することは、著作権法下での許可事項を除き、禁止されています。

All rights are reserved.

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 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices.

©Copyright 2006 Hewlett-Packard Development Company, L.P.

Trademark Notices.

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。

その他一般に各会社名、各製品名は各社の商号、商標または登録商標です。

1. インストール手順の概要

この章の内容	2
インストール手順の概要	3
インストールの概念	6
Data Protector のインストール DVD-ROM	8
Cell Manager システムの選択	11
Data Protector ユーザー インタフェース システムの選択	13
Data Protector グラフィカル ユーザー インタフェース	14

2. ネットワークへの Data Protector のインストール

この章の内容	18
Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール	19
UNIX 用 Cell Manager のインストール	20
Windows 用 Cell Manager のインストール	29
インストール サーバのインストール	37
Data Protector クライアントのインストール	46
Data Protector クライアントのリモート インストール	50
Data Protector コンポーネント	59
Windows 用クライアントのインストール	63
HP-UX クライアントのインストール	68
Solaris 用クライアントのインストール	72
Linux クライアントのインストール	79
AIX クライアントのインストール	85
Siemens Sinix クライアントのインストール	87
Tru64 クライアントのインストール	89
SCO クライアントのインストール	91
ADIC/GRAU ライブラリ用または StorageTek ライブラリ用の Media Agent のインストール	93
Novell NetWare クライアントのローカル インストール	102
OpenVMS クライアントのローカル インストール	108
MPE/iX クライアントのインストール	115
UNIX クライアントのローカル インストール	119
Data Protector 統合クライアントのインストール	124
ローカル インストール	126
リモート インストール	126
クラスター対応統合ソフトウェアのインストール	127
Microsoft Exchange Server クライアント	127
MS SQL クライアント	128
Sybase クライアント	128

目次

Informix Server クライアント	128
SAP R/3 クライアント	129
SAP DB クライアント	129
Oracle クライアント	129
DB2 クライアント	131
NNM クライアント	131
NDMP クライアント	131
MS Volume Shadow Copy クライアント	132
Lotus Notes/Domino Server クライアント	132
EMC Symmetrix 用統合ソフトウェア	132
HP StorageWorks XP 用統合ソフトウェア	136
HP StorageWorks Virtual Array 用統合ソフトウェア	143
HP StorageWorks Enterprise Virtual Array 用統合ソフトウェア	149
各国語版 Data Protector ユーザー インタフェースのインストール	156
Windows システムへの各国語版 Data Protector ユーザー インタフェースの インストール	156
UNIX システムへの各国語版 Data Protector ユーザー インタフェースの インストール	158
トラブルシューティング	159
Data Protector シングルサーバ版のインストール	161
Windows 用 SSE の制限	161
HP-UX および Solaris 用の SSE の制限事項	162
Data ProtectorWeb Reporting のインストール	163
MC/ServiceGuard への Data Protector のインストール	165
クラスタ対応 Cell Manager のインストール	165
クラスタ対応クライアントのインストール	166
Data Protector の Microsoft Cluster Server へのインストール	167
クラスタ対応 Cell Manager のインストール	167
クラスタ対応クライアントのインストール	175
Veritas Cluster への Data Protector クライアントのインストール	178
クライアントのインストール	178
Novell NetWare Cluster への Data Protector クライアントのインストール	179
クライアントのインストール	179

3. インストールの保守

この章の内容	184
セルへのクライアントのインポート	185
セルへのインストール サーバのインポート	187
セルへのクラスタ対応クライアントのインポート	188

Microsoft Cluster Server	188
その他のクラスタ	189
セルからのクライアントのエクスポート	192
保護について	195
保護レイヤー	195
クライアントの保護	198
ホスト名厳密チェック	205
Start Backup Specification ユーザー権限	207
バックアップ仕様の内容の隠蔽	208
ホスト信頼	208
保護イベントのモニター	209
インストールされている Data Protector パッチの確認	211
GUI を使用した Data Protector パッチの確認	211
CLI を使用した Data Protector パッチの確認	212
Data Protector ソフトウェアのアンインストール	213
Data Protector クライアントのアンインストール	214
Cell Manager とインストール サーバのアンインストール	215
UNIX 上の Data Protector ソフトウェアの手動削除	224
Data Protector ソフトウェア コンポーネントの変更	226

4. Data Protector A.06.00 へのアップグレード

この章の内容	232
アップグレードの概要	233
アップグレードの手順	234
IDB でのファイル名変換の必要性	235
Data Protector A.05.x からのアップグレード	237
UNIX 用 Cell Manager とインストール サーバのアップグレード	237
Windows Cell Manager とインストール サーバのアップグレード	243
構成の変更のチェック	247
クライアントのアップグレード	249
MoM 環境でのアップグレード	260
IDB 内でのファイル名の変更	262
Windows Cell Manager での IDB 変換	267
UNIX Cell Manager での IDB 変換	270
シングルサーバ版からのアップグレード	271
旧バージョンの SSE から Data Protector A.06.00 SSE へのアップグレード	271
Data Protector A.06.00 SSE から Data Protector A.06.00 へのアップグレード	271
Windows NT から Windows のより新しいバージョンへのアップグレード	274

目次

Solaris 7/8 から Solaris 9 へのアップグレード	275
HP-UX 11.x から HP-UX 11.23 への移行	276
MoM 固有の手順	279
インストール サーバ固有の手順	280
32 ビット Windows から 64 ビット Windows への移行	281
MoM 固有の手順	283
インストール サーバ固有の手順	284
MC/ServiceGuard 上で構成されている Cell Manager のアップグレード	285
Microsoft Cluster Server 上で構成されている Cell Manager のアップグレード	289
5. Data Protector のライセンス	
この章の内容	294
概要	295
ライセンス チェック機能とレポート機能	296
Cell Manager 関連ライセンス	296
エンティティ ベース使用権	297
キャパシティ ベース使用権	297
キャパシティ ベース使用権の例	301
必要に応じたライセンス レポートの作成	305
購入可能なライセンス	306
パスワードについて	307
Data Protector のパスワード	308
HP OpenView AutoPass ユーティリティを使用した恒久パスワードの取得と インストール	309
恒久パスワードの取得とインストールのためのその他の方法	311
パスワードの検証	313
インストール済みライセンスの数を調べる	314
他の Cell Manager システムへのライセンスの移動	314
集中ライセンス	316
Data Protector Order Tool	317
6. インストールのトラブルシューティング	
この章の内容	320
Windows 用 Cell Manager インストール時の名前解決に関する問題	321
Data Protector セル内の DNS 接続の確認	322
omnicheck コマンドの使用	322
Windows 上での Data Protector のインストールとアップグレード	325
Windows クライアントのリモート インストールに関する問題	326
Solaris 上での Data Protector Cell Manager のインストールに関する問題の	

トラブルシューティング	327
UNIX クライアントのインストールに関する問題のトラブルシューティング	328
Data Protector クライアントのインストール結果の確認	330
アップグレードのトラブルシューティング	331
手作業でのアップグレード手順	332
ログファイルの使用	333
ローカル インストール	333
リモート インストール	334
Data Protector ログ ファイル	334
インストール実行トレースの作成	336

A. 付録 A

Data Protector A.06.00 の製品構成とライセンス	A-2
スターター パック	A-4
ドライブとライブラリの使用権	A-5
機能拡張	A-8
シングルサーバ版 (SSE)	A-17
Data Protector A.06.00 へのライセンス移行	A-19
ライセンス概要図	A-20
Data Protector ライセンス フォーム	A-25

B. 付録 B

この付録の内容	B-2
ネイティブ ツールを使用した、HP-UX、Solaris、および Linux システムへの インストール	B-3
swinstall を使用した HP-UX システムへの Cell Manager のインストール	B-3
pkgadd を使用した Solaris システムへの Cell Manager のインストール	B-5
rpm を使用した Linux システムへの Cell Manager のインストール	B-6
HP-UX システムへのインストール サーバのインストール	B-8
pkgadd を使用した Solaris システムへのインストール サーバのインストール	B-8
rpm を使用した Linux システムへのインストール サーバのインストール	B-12
クライアントのインストール	B-15
ネイティブ ツールを使用した HP-UX システムと Solaris システムでの アップグレード	B-16
swinstall を使用した HP-UX システムでの Data Protector のアップグレード	B-16
pkgadd を使用した Solaris システムでの Data Protector のアップグレード	B-17
Windows システム上の TCP/IP プロトコルのセットアップ	B-19
Windows への TCP/IP プロトコルのインストールと構成	B-20
TCP/IP 設定をチェックする	B-24

目次

Cell Manager 名の変更	B-26
デフォルトのポート番号の変更	B-28
NIS サーバの準備	B-30
Windows でのテープ ドライバおよびロボティクス ドライバの使用	B-32
Windows 上でのデバイス ファイル (SCSI アドレス) の作成	B-35
HP-UX 上の SCSI ロボティクス構成	B-37
HP-UX 上のデバイス ファイルの作成	B-42
SCSI コントローラのパラメータの設定	B-45
HP-UX 上の未使用の SCSI アドレスの取得	B-46
Solaris システム上の未使用の SCSI ターゲット ID の取得	B-48
Solaris システム上でのデバイスおよびドライバ構成の更新	B-49
構成ファイルの更新	B-49
デバイス ファイルの作成とチェック	B-52
Windows システム上の未使用の SCSI ターゲット ID の取得	B-54
HP StorageWorks 330fx ライブラリ上の SCSI ID の設定	B-55
バックアップ デバイスの接続	B-56
HP StorageWorks 24 スタンドアロン デバイスの接続	B-60
HP StorageWorks DAT オートローダーの接続	B-61
HP StorageWorks DLT ライブラリ 28/48 スロットの接続	B-63
Seagate Viper 200 LTO Ultrium テープ ドライブの接続	B-68
Novell NetWare 上にインストールした General Media Agent のチェック	B-71
記憶デバイスの識別	B-71
General Media Agent の起動テスト	B-71
HPUMA.NLM および HPDEVBRA.NLM の起動テスト	B-74
Veritas Volume Manager がインストールされた Microsoft Cluster への Data Protector のインストール	B-76
Data Protector A.06.00 での構成ファイル パスの変更	B-77
UNIX での構成ファイル	B-77
Windows での構成ファイル	B-78
Data Protector A.06.00 にアップグレードした後のコマンド行ツールの変更	B-80

C. 付録 C

インストールメディアとして CD-ROM を使用	C-2
Data Protector のインストール CD-ROM	C-2
CD-ROM から Data Protector をインストールする場合の追加手順	C-5
CD-ROM から Data Protector をアップグレードする場合の追加手順	C-9

用語集

出版履歴

マニュアルの出版の日付と部品番号は、そのマニュアルの最新の版数を示しています。出版の日付は、最新版ができるたびに更新します。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更新します。

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もな行われます。お手元のマニュアルが最新のものか否かは、当社の営業担当または購入された販売会社にお問い合わせください。詳細については、HP の営業担当にお問い合わせください。

表 1 出版履歴

部品番号	出版年月	製品
B6960-99079	2003 年 6 月	Data Protector リリース A.05.10
B6960-99107	2004 年 10 月	Data Protector リリース A.05.50
B6960-96027	2006 年 7 月	Data Protector リリース A.06.00

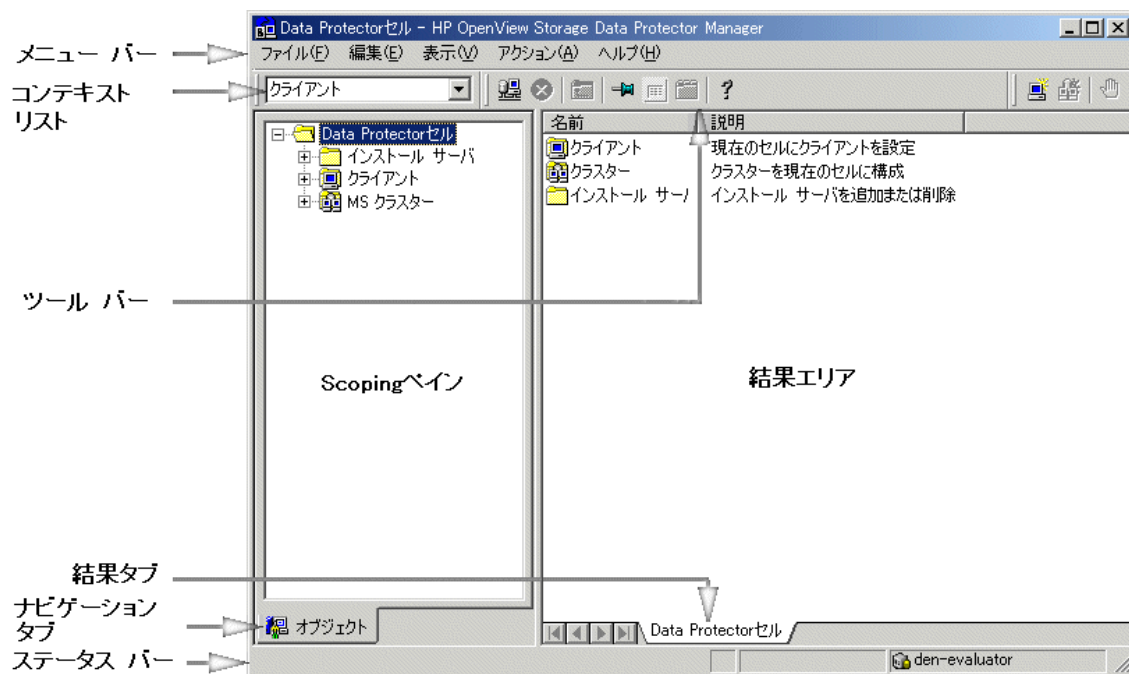
表記法

表 2

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

Data Protector では、クロスプラットフォーム (Windows と UNIX) のグラフィカル ユーザー インタフェースを提供します。Data Protector のグラフィカル ユーザー インタフェースについては、オンラインヘルプを参照してください。

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



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://www.itrc.hp.com>

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://www.itrc.hp.com>

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。

storagedocs.feedback@hp.com

トレーニング情報

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

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

<http://www.hp.com/jp/education> (日本)

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

Data Protector のドキュメント

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

マニュアル

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

<http://www.hp.com/support/manuals> (英語版)

<http://www.hp.com/jp/manual/> (日本語版)

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

このマニュアルでは、Data Protector のコンセプトを解説するとともに、Data Protector の動作原理を詳細に説明しています。手順を中心に説明しているオンライン ヘルプとあわせてお読みください。

『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 トラブルシューティング ガイド』

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

『HP OpenView Storage Data Protector 障害復旧 ガイド』

このマニュアルでは、障害復旧の計画、準備、テスト、および実行方法について説明します。

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

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

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

このマニュアルでは、Microsoft アプリケーション (Microsoft Exchange Server 2000/2003、Microsoft SQL Server 7/2000/2005、および Volume Shadow Copy Service) に対応する Data Protector の統合ソフトウェアについて説明します。

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

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

- 『HP OpenView Storage Data Protector Integration Guide for IBM Applications: Informix, DB2, and Lotus Notes/Domino』

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

- 『HP OpenView Storage Data Protector Integration Guide for Sybase, Network Node Manager, and Network Data Management Protocol』

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

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

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

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

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

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

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

マニュアルには、以下の 2 つのバージョンがあります。

- OVO 7.1x、7.2x 用
- OVO 7.5 用

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

このマニュアルでは、Data Protector ゼロ ダウンタイム バックアップとインスタント リカバリのコンセプトについて解説するとともに、ゼロ ダウンタイム バックアップ環境における Data Protector の動作原理を詳細に説明します。手順を中心に説明している『HP OpenView Storage Data Protector Zero Downtime Backup Administrator's Guide』および『HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide』とあわせてお読みください。

『HP OpenView Storage Data Protector Zero Downtime Backup Administrator's Guide』

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

『HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide』

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

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

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

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

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

『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』

このマニュアルでは、HP OpenView Storage Data Protector A.06.00 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.hp.com/support/manuals> (英語)

この他に 4 冊の『Product Announcements ソフトウェア ノート およびリファレンス』があり、以下の内容を説明しています。

- OVO UNIX の統合
- OVO 7.1x/7.2x Windows の統合
- OVO 7.5 Windows の統合
- Media Operations

オンライン ヘルプ

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

ドキュメントマップ

略称

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

略称	マニュアル
CLI	Command Line Interface Reference Guide
Concepts	コンセプト ガイド
DR	障害復旧 ガイド
GS	スタートアップ ガイド
Help	オンライン ヘルプ
IG-IBM	Integration Guide—IBM Applications
IG-MS	インテグレーション ガイド —Microsoft アプリケーション
IG-O/S	インテグレーション ガイド —Oracle、SAP R/3、SAP DB/MaxDB
IG-OV	Integration Guide—HP OpenView Service Information Portal/OpenView Reporter
IG-OVOU	Integration Guide—HP OpenView Operations, UNIX
IG-OVOW	Integration Guide—HP OpenView Operations 7.1x, 7.2x, Windows
IG-OVOW	Integration Guide—HP OpenView Operations 7.5, Windows
IG-Var	Integration Guide—Sybase, Network Node Manager, NDMP and VMware
Install	インストールおよびライセンス ガイド
MO GS	Media Operations Getting Started Guide

略称	マニュアル
MO RN	Media Operations Product Announcements, Software Notes, and References
MO UG	Media Operations User Guide
MPE/iX	MPE/iX System User Guide
PA	Product Announcements ソフトウェア ノート およびリファレンス
Trouble	トラブルシューティング ガイド
ZDB Admin	ZDB Administrator's Guide
ZDB Concept	ゼロ ダウンタイム バックアップ コンセプト ガイド
ZDB IG	ZDB Integration Guide

マップ

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

	Help	GS	Concepts	Install	Trouble	DR	PA	インテグレーションガイド						ZDB			MO			MPE/iX	CLI		
								MS	O/S	IBM	Var	OV	OVOU	OVOW	Concept	Admin	IG	GS	User			PA	
バックアップ	X	X	X					X	X	X	X				X	X	X					X	
CLI																							X
コンセプト/テクニック	X		X					X	X	X	X	X	X	X	X	X						X	
障害復旧	X		X			X																	
インストール/ アップグレード	X	X		X			X					X	X	X				X	X			X	
インスタント リカバリ	X		X												X	X	X						
ライセンス	X			X			X												X				
制限事項	X				X		X	X	X	X			X			X					X		
新機能	X						X														X		
計画方針	X		X							X			X										

	Help	GS	Concepts	Install	Trouble	DR	PA	インテグレーションガイド						ZDB			MO			MPE/iX	CLI			
								MS	O/S	IBM	Var	OV	OVOU	OVOW	Concept	Admin	IG	GS	User			PA		
手順/タスク	X			X	X	X		X	X	X	X	X	X	X	X	X		X	X					
推奨事項			X				X							X							X			
必要条件				X			X	X	X	X	X			X				X	X	X				
復元	X	X	X					X	X	X	X				X	X						X		
サポートマトリクス							X																	
サポートされる構成														X										
トラブルシューティング	X			X	X			X	X	X	X	X			X	X								

統合

以下の統合に関する詳細については、該当するマニュアルを参照してください。

統合ソフトウェア	マニュアル
HP OpenView Operations (OVO)	IG-OVOU、 IG-OVOW
HP OpenView Reporter (OVR)	IG-OV
HP OpenView Reporter Light	IG-OVOW
HP OpenView Service Information Portal (OVSIP)	IG-OV
HP StorageWorks Disk Array XP	すべての ZDB
HP StorageWorks Enterprise Virtual Array (EVA)	すべての ZDB
HP StorageWorks Virtual Array (VA)	すべての ZDB
IBM DB2 UDB	IG-IBM
Informix	IG-IBM
Lotus Notes/Domino	IG-IBM
Media Operations	MO User
MPE/iX System	MPE/iX
Microsoft Exchange Servers	IG-MS、ZDB IG

統合ソフトウェア	マニュアル
Microsoft Exchange Single Mailbox	IG-MS
Microsoft SQL Servers	IG-MS、 ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	IG-MS、 ZDB IG
NDMP Server	IG-Var
Network Node Manager (NNM)	IG-Var
Oracle	IG-O/S
Oracle ZDB	ZDB IG
SAP DB	IG-O/S
SAP R/3	IG-O/S、 ZDB IG
Sybase	IG-Var
Symmetrix (EMC)	すべての ZDB
VMware	IG-Var

このマニュアルについて

『HP OpenView Storage Data Protector インストールおよびライセンス ガイド』は、Data Protector ネットワーク製品のインストール、インストール手順の開始前の前提条件、アップグレード方法およびライセンシングについて説明したものです。

対象読者

このマニュアルは、システムのインストールおよび保守を担当する管理者と、バックアップ環境の計画、インストール、および管理を担当するバックアップ管理者を対象にしています。

Data Protector の概念については、『HP OpenView Storage Data Protector コンセプト ガイド』で説明しています。このマニュアルに目を通し、Data Protector の基礎知識と基準について十分に理解を深めていただくことをお勧めします。

この章の構成

このマニュアルは、以下の章で構成されています。

第 1 章	1 ページの「インストール手順の概要」
第 2 章	17 ページの「ネットワークへの Data Protector のインストール」
第 3 章	183 ページの「インストールの保守」
第 4 章	231 ページの「Data Protector A.06.00 へのアップグレード」
第 5 章	293 ページの「Data Protector のライセンス」
第 6 章	319 ページの「インストールのトラブルシューティング」
付録 A	A-1 ページの「付録 A」
付録 B	B-1 ページの「付録 B」
付録 C	C-1 ページの「付録 C」
用語集	このマニュアルで使用する用語の定義

1 インストール手順の概要

この章の内容

この章では、Data Protector のインストール手順の概要とインストールの概念について説明します。また、Data Protector Cell Manager と Data Protector ユーザー インタフェースの概要も示します。

インストール手順の概要

Data Protector バックアップ環境は、同じタイムゾーンに所属し同じ LAN/SAN 上に存在する、共通のバックアップ方針が適用される複数のシステムで構成されます。このネットワーク環境を Data Protector **セル**と呼びます。典型的なセルは、Cell Manager、インストール サーバ、クライアント、およびバックアップ デバイスで構成されます。

Cell Manager とは、セルを集中的に制御するメイン システムです。このシステムでは、Data Protector 内部データベース (IDB) が保持され、Data Protector のコア ソフトウェアおよび Session Manager が実行されます。

IDB には、バックアップしたファイルに関する情報とセルの構成に関する情報が記録されます。

インストール サーバ (IS) とは、クライアントのリモート インストールに必要な Data Protector ソフトウェア レポジトリを保持するコンピュータまたは Cell Manager コンポーネントです。Data Protector のこの機能を使用すると、ソフトウェアのインストール (特にリモート クライアントのインストール) が非常に容易になります。

セルは、1 つの Cell Manager と通常多数のクライアントで構成されます。コンピュータ システムに Data Protector ソフトウェア コンポーネントのいずれかをインストールすれば、そのシステムは Data Protector **クライアント**として機能するようになります。各システムにどのクライアント コンポーネントをインストールするかは、バックアップ環境内でそのシステムに与える役割によって異なります。Data Protector コンポーネントは、1 つのシステムにローカル インストールすることも、多数のシステムにインストール サーバから配布することも可能です。

Data Protector 機能にアクセスするには**ユーザー インタフェース** コンポーネントが必要であり、すべての構成作業と管理作業はこのユーザー インタフェースを介して行います。ユーザー インタフェース コンポーネントは、バックアップ管理に使用するすべてのシステムにインストールしてください。Data Protector は、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)

バックアップが必要なディスクを含むクライアント システムには、Data Protector **Disk Agent** コンポーネントをインストールする必要があります。Disk Agent は、クライアント ディスク上のデータをバックアップおよび復元するのに必要なコンポーネントです。

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** コンポーネントをインストールする必要があります。このコンポーネントは、バックアップ デバイスおよびバックアップ メディアを管理します。Data Protector Media Agent には、**General Media Agent** と **NDMP Media Agent** の 2 種類があります。NDMP Media Agent は、NDMP サーバのバックアップ

インストール手順の概要

インストール手順の概要

を制御するクライアント システム (NDMP 専用ドライブを制御するクライアント システム) でのみ必要です。これ以外のシステムの場合は、2 種類の **Media Agent** のうち、どちらを使用しても構いません。

Data Protector をネットワークにインストールする前に、以下の項目を決定しておく必要があります。

- ✓ どのシステムに **Cell Manager** をインストールするか。サポート対象のオペレーティング システムとそのバージョンについては、『*HP OpenView Storage Data Protector Product Announcements* ソフトウェア ノート および リファレンス』を参照してください。

1 つのセル内で **Cell Manager** として機能できるコンピュータは 1 つだけです。**Cell Manager** をインストールしなければ、**Data Protector** は実行できません。

- ✓ どのシステムからユーザー インタフェースを使用して **Data Protector** の機能を使用するか。これらのシステムには、ユーザー インタフェースをインストールする必要があります。
- ✓ どのシステムをバックアップするか。これらのシステムには、ファイルシステムをバックアップするための **Disk Agent** コンポーネントをインストールする必要があります。オンライン データベース用統合ソフトウェアを利用する場合は、それぞれのアプリケーションに対応した **Application Agent** コンポーネントをインストールする必要があります。
- ✓ どのシステムにバックアップ デバイスを接続するか。これらのシステムには、**Media Agent** コンポーネントをインストールする必要があります。
- ✓ どのシステムに **Data Protector** のインストール サーバをインストールするか。ソフトウェアのリモート インストールに使用するインストール サーバ (IS) には、UNIX クライアント用と Windows クライアント用の 2 種類があります。プラットフォームに合わせてインストールしてください。

インストール サーバとして使用するコンピュータは、**Cell Manager** やユーザー インタフェースがインストールされているシステムとは無関係に選択できます。**Cell Manager** とインストール サーバを同一システム上にインストールすることも (両方が同じプラットフォーム用の場合)、異なるシステム上にインストールすることも可能です。

1 つのインストール サーバを複数の **Data Protector** セル間で共有することもできます。

注記

Windows 用インストール サーバは、Windows システム上にインストールする必要があります。UNIX 用インストール サーバは、HP-UX、Solaris、または Linux システム上にインストールする必要があります。サポート対象のオペレーティング システムのバージョンについては、『*HP OpenView Storage Data Protector Product Announcements* ソフトウェア ノート および リファレンス』を参照してください。

重要

Solaris システムに Data Protector Cell Manager、インストール サーバまたはクライアントをインストールするときは、`/usr/omni` ディレクトリのすべてのファイルを別のディレクトリに保存してください。これは、Data Protector のインストール時には、`/usr/omni` ディレクトリのすべてのファイルが削除されるからです。

Data Protector セル内における各システムの役割を決定したら、インストール作業を行います。一般的な手順は以下のとおりです。

1. インストールの前提条件が満たされていることをチェックします。
2. Data Protector Cell Manager をインストールします。
3. インストール サーバおよびユーザー インターフェースをインストールします。
4. クライアントシステムをリモートにインストールするか (推奨)、または DVD-ROM からローカルにインストールします。

注記

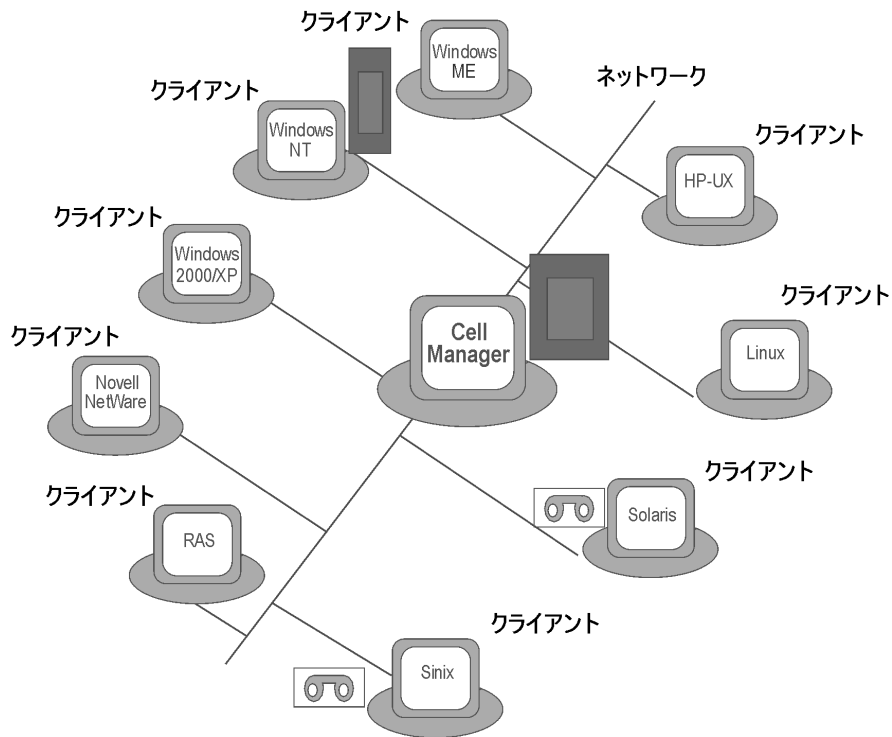
インストール サーバをすでにインストールしてある Windows システムには、Data Protector クライアントをリモートでインストールすることはできません。同一システム上にインストール サーバとクライアント コンポーネントをインストールする場合は、Data Protector の Windows 用インストール DVD-ROM を使用して、クライアントをローカルにインストールする必要があります。この場合は、[Component Selection] ウィンドウで、必要なクライアント コンポーネントとインストール サーバ コンポーネントを選択してください。

インストール手順の概要

インストール手順の概要

また、Windows Me/XP Home Edition、MPE、Novell NetWare の各クライアントシステムについても、リモート インストールを行えません。この場合もローカルインストールが必要です。

図 1-1 Data Protector セル



インストールの概念

Data Protector Cell Manager、ユーザー インタフェース、およびインストール サーバ (UNIX または Windows の各プラットフォーム別に最低 1 つ必要) をインストールしたら、リモート インストールをサポートするオペレーティング システム上で実行されているクライアントに、Data Protector ソフトウェアを配布できるようになります。詳細は 8 ページの図 1-2 を参照してください。

リモート インストールを実行するときは、必ず GUI を使用してインストール サーバにアクセスします。通常ユーザー インタフェース コンポーネントは、Cell Manager 上にインストールされています(ただし、このインストールは必須ではありません)。一般的には、ユーザー インタフェースは、さまざまな場所から Cell Manager にアクセスできるように、複数のコンピュータにインストールします。

Windows Me/XP HE 以外の Windows システムには、Windows 用のインストール サーバからクライアント ソフトウェアを配布できます。

Windows Me/XP HE クライアント システムは、Data Protector の Windows 用インストール DVD-ROM からローカルにインストールする必要があります。

Data Protector は Novell NetWare クライアントもサポートしていますが、クライアントをリモートインストールすることはできません。インストールは、Novell ネットワークに接続されている Windows システムから実行してください。

UNIX 用のインストール サーバ(サポート対象のプラットフォームの一覧は、『*HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス*』を参照)からは、HP-UX、Solaris、Sinix、Linux、AIX、およびその他のサポート対象 UNIX オペレーティングシステム上に、クライアント ソフトウェアをリモートでインストールできます。

インストール先のシステムがリモート インストールをサポートしていない UNIX オペレーティングシステムである場合や、UNIX 用のインストール サーバをインストールしていない場合は、Data Protector の UNIX 用インストール DVD-ROM を使用して、UNIX クライアントをローカルにインストールできます。

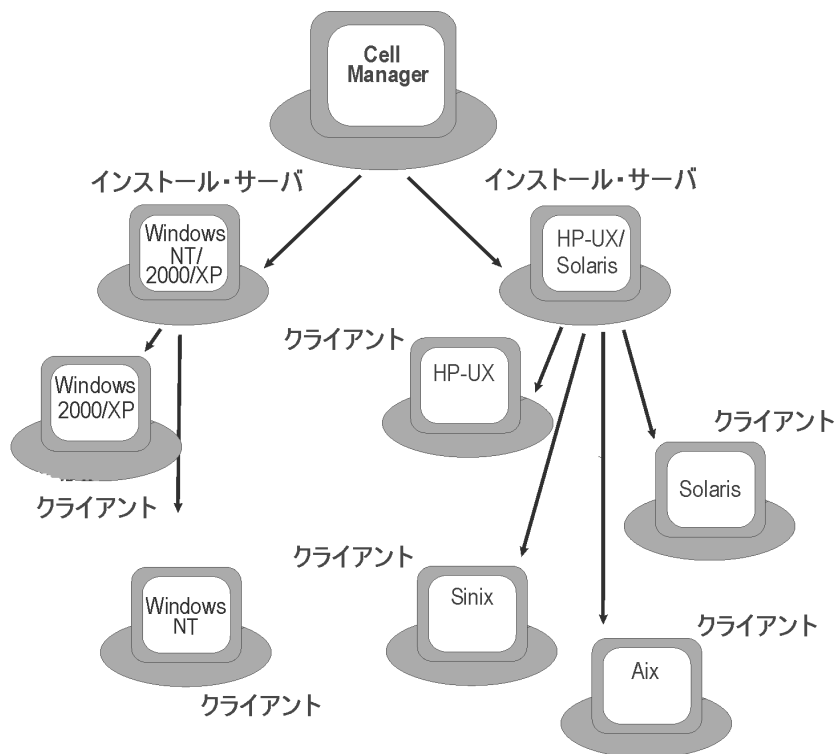
ただし、一部の OS 環境については、リモート インストールしか実行できない場合があります。

さまざまな Data Protector クライアントのそれぞれのインストール方法の詳細は、46 ページの「Data Protector クライアントのインストール」を参照してください。

インストール手順の概要 インストール手順の概要

UNIX クライアントのローカル インストールの手順は、119 ページの「UNIX クライアントのローカル インストール」を参照してください。

図 1-2 Data Protector インストールの概念



Data Protector のインストール DVD-ROM

Data Protector は、さまざまなプロセッサアーキテクチャ上でさまざまなオペレーティングシステムをサポートします。これらのプラットフォームのすべてに対応するには、2種類のDVD-ROMを用意する必要があります。それぞれのDVD-ROMに収録されているコンポーネントの詳細は、9ページの「Data Protector のDVD-ROMの一覧」を参照してください。

注記

Data Protector は DVD-ROM からインストールすることをお勧めします。
DVD-ROM の代わりに CD-ROM を使用する場合は、「付録 C」(C-1 ページ) を参照してください。参照先には、インストール手順の違いと、CD-ROM の一覧が示されています。

表 1-1 Data Protector の DVD-ROM の一覧

DVD 番号	DVD-ROM のタイトル	内容
1	Data Protector Starter Pack for Windows オープンファイル・バックアップ使用権、メディア操作、および Netware、MPE、OpenVMS クライアント用エージェントを含みます。	<ul style="list-style-type: none">Windows 32 ビット /64 ビット (AMD64/Intel EM64T) システム上の Windows 用 Cell Manager とインストールサーバAutoPass^aPDF 形式のマニュアル (英語版: DOCS ディレクトリ、日本語版: DOCS/JPN ディレクトリ)Windows IA64 クライアントNovell NetWare クライアントOpenVMS クライアント (Alpha システムと IA64 システム)MPE クライアントオープンファイル マネージャ インストール パッケージWindows プラットフォーム用の製品デモ製品情報メディア操作のインストール パッケージ

表 1-1 Data Protector の DVD-ROM の一覧 (続き)

DVD 番号	DVD-ROM のタイトル	内容
2	Data Protector Starter Pack for HP-UX, Solaris, and Linux HP-UX、Solaris、および Linux クライアント用エージェントを含みます。	<ul style="list-style-type: none">• HP-UX (PA-RISC、IA64)、Solaris、および Linux 用の Cell Manager とインストール サーバ• その他の UNIX システムのクライアント• AutoPass^b• PDF 形式のマニュアル (英語版 : DOCS ディレクトリ、日本語版 : DOCS/JPN ディレクトリ)• OpenView 統合ソフトウェア パッケージ

- a. Windows x64 オペレーティング システム上では AutoPass は使用できません。
- b. Linux 上では AutoPass は使用できません。

Cell Manager システムの選択

Cell Manager は、Data Protector セルのメイン システムとなります。Cell Manager には以下の機能があります。

- セルを集中管理します。
- IDB (バックアップセッション、復元セッション、およびメディア管理セッションに関する情報を格納するファイル) を維持します。
- Data Protector のコア ソフトウェアを実行します。
- Session Manager を実行します。Session Manager は、バックアップセッションおよび復元セッションの開始と停止を制御し、セッション情報を IDB に書き込みます。

お使いの環境のどのシステムを Cell Manager として使用するかを決定する際には、以下の点に留意してください。

✓ サポート対象プラットフォーム

Cell Manager は、Windows、HP-UX、または Solaris の各プラットフォーム上にインストールできます。サポート対象のプラットフォームのバージョンとリリースの詳細は、『*HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス*』を参照してください。

✓ Cell Manager システムの信頼性

Cell Manager 上では IDB が保持されており、Cell Manager が停止するとバックアップや復元を実行できなくなるため、お使いの環境で特に信頼性の高いシステムを選択してください。

✓ データベースのサイズ増加と必要なディスク スペース

Cell Manager には、Data Protector の内部データベース (IDB) が格納されています。IDB には、バックアップされたデータとそのメディア、セッション メッセージ、およびデバイスに関する情報が含まれています。IDB のサイズは、環境によって、非常に大きくなる場合があります。たとえば、バックアップの大半がファイルシステムのバックアップである場合、IDB の概算サイズは、通常、バックアップされるデータが占有しているディスク スペースの 2% です。IDB のサイズを算出するには、Data Protector のインストール メディアに収録されている IDB_capacity_planning.xls の表を使用できます。

データベース サイズの見積もりとサイズ増加の管理については、オンライン ヘルプの索引キーワード「IDB のサイズ増加とパフォーマンス」で表示される内容を参照してください。

インストール手順の概要

Cell Manager システムの選択

IDB に必要なディスク スペースの詳細は、『*HP OpenView Storage Data Protector Product Announcements* ソフトウェア ノート およびリファレンス』を参照してください。

注記 必ずしも、Cell Manager をグラフィカル ユーザー インタフェース システムとして使用する必要はありません。たとえば、UNIX 用の Cell Manager を使用する環境で、Windows クライアントにインストールしたユーザー インタフェース コンポーネントを使用することも可能です。

この次に行う作業

Cell Manager として使用するシステムが満たすべき条件を確認します。19 ページの「Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール」を参照してください。

Data Protector ユーザー インタフェース システムの選択

Data Protector は、Windows、HP-UX、および Solaris プラットフォーム用のグラフィカル 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) を備えています。このユーザー インタフェースは、Data Protector ソフトウェア コンポーネントとしてインストールされます。

セルの制御用に選択したシステムは、ネットワーク管理者またはバックアップ オペレータが使用することになります。

ただし大規模なコンピュータ環境では、複数のシステム上でユーザー インタフェースを使用できる方が便利です。また、混在環境では、プラットフォームの異なる複数のシステム上にユーザー インタフェースを配置するのが理想的です。

たとえば、ネットワーク上にさまざまな種類の UNIX システムが存在し、少なくとも 1 台の Solaris または HP-UX システムにユーザー インタフェースをインストールしてある場合は、X サーバを実行しているその他の UNIX システムにそのユーザー インタフェースの表示内容をエクスポートできます。しかし、パフォーマンスの観点から、Data Protector セルの制御に使用されるすべてのシステムに、Data Protector GUI をインストールすることをお勧めします。

バックアップ対象の Windows システムが多数配備されているオフィスエリアでは、そのエリアにある Windows システムからバックアップおよび復元操作をローカルに実行できる方が便利です。このような場合は、ユーザー インタフェース コンポーネントを Windows システム上にインストールしてください。さらに付け加えると、Windows 上の Data Protector GUI では、異種混合環境をより簡単に管理できます。これは、ローカル設定の変更が不要だからです。

Data Protector GUI がサポートされていない UNIX プラットフォームに Cell Manager が配置されている場合、そのプラットフォームで Data Protector GUI の機能を使用するには、まず `omniusers` コマンドを使用して Cell Manager 上にリモート ユーザー アカウントを作成します。次に、作成したユーザー アカウントを使用して、Data Protector GUI がインストールされている別のシステムでこの GUI を起動し、Cell Manager に接続します。詳細は、`omniusers` コマンドのマニュアル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とリリースの詳細は、『*HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス*』を参照してください。ローカル言語のサポートとファイル名における非 ASCII 文字の使用については、オンライン ヘルプの索引キーワード「言語設定、カスタマイズ」で表示される内容を参照してください。

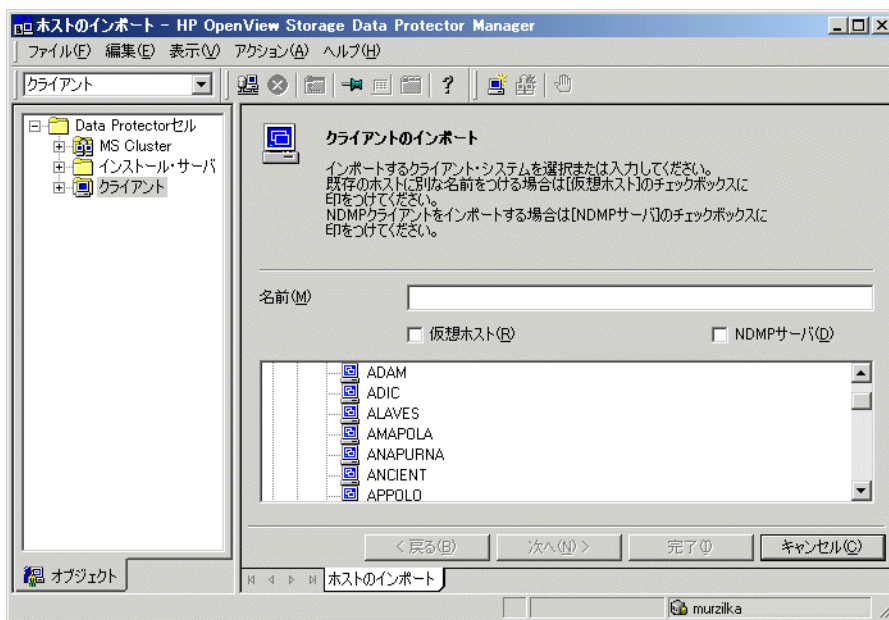
セル内のシステムにユーザー インタフェースをインストールすれば、そのシステムから Cell Manager にリモート アクセスできます。もちろん、Cell Manager 上でグラフィカル ユーザー インタフェース システムを必ずしも使用する必要はありません。

Data Protector グラフィカル ユーザー インタフェース

Data Protector GUI は強力なツールであり、これを使うと Data Protector の機能に簡単にアクセスできます。メインウィンドウには、[クライアント]、[ユーザー]、[デバイス / メディア]、[バックアップ]、[復元]、[コピーと集約]、[レポート]、[モニター]、[インスタント リカバリ]、[内部データベース]などのさまざまなコンテキストが用意されており、これらに関連する作業をすべて実行できるようになっています。

たとえば、[クライアント]コンテキストでは、クライアントをリモート インストール (追加) できます。ここで対象となるすべてのシステムを指定し、インストールのパスおよびオプションを定義すると、指定したインストール サーバシステムに情報が送信されます。クライアント上でのセットアッププログラムの実行中には、そのクライアントへのインストールに関連するメッセージだけがモニター ウィンドウに表示されます。

図 1-3 Data Protector グラフィカル ユーザー インタフェース



本書の前書きにある図 1 も参照してください。この図には Data Protector GUI の主な領域が示されています。

注記

UNIX では、Data Protector GUI を実行する前に、この GUI を実行するシステム上で詳細なローカル設定を行う必要があります。これによって、GUI の文字エンコード方式を切り替えて、正しいエンコード方式を選択することにより、ファイル名やセッション メッセージ内の非 ASCII 文字を適切に表示できるようになります。詳細はオンライン ヘルプの索引キーワード「設定、UNIX の GUI のローカル」で表示される内容を参照してください。

インストール手順の概要

Data Protector ユーザー インタフェース システムの選択

2 ネットワークへの Data Protector のインストール

この章の内容

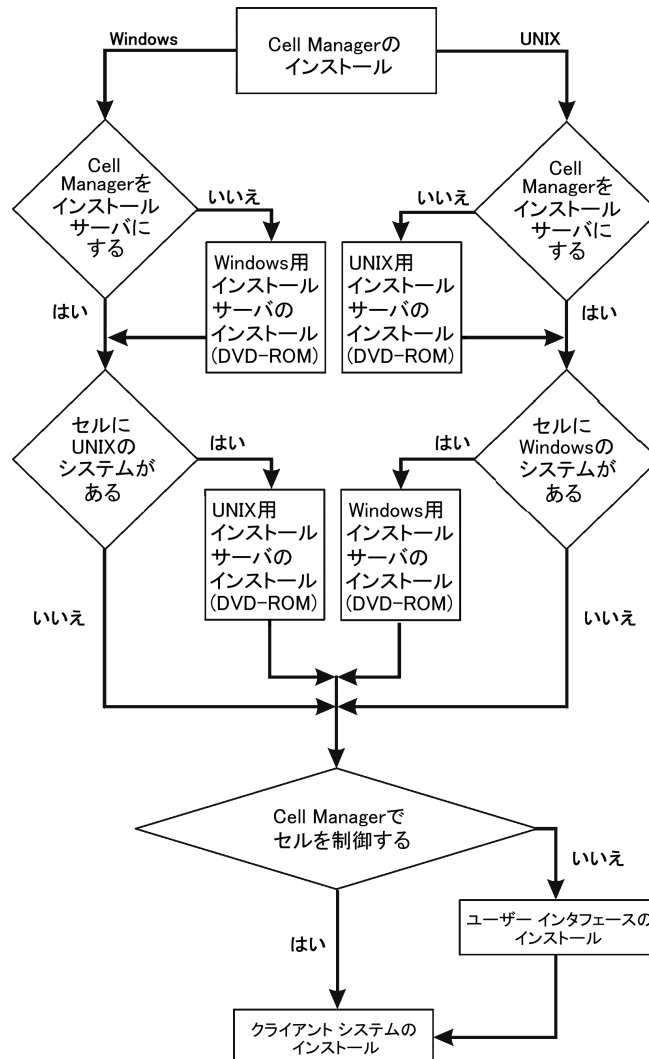
この章では、以下の各作業について詳細な手順を示します。

- Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール。詳細は 19 ページの「Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール」を参照してください。
- Data Protector クライアントのインストール。詳細は 46 ページの「Data Protector クライアントのインストール」を参照してください。
- 各国語版 Data Protector ユーザー インタフェースのインストール。詳細は 156 ページの「各国語版 Data Protector ユーザー インタフェースのインストール」を参照してください。
- Data Protector シングルサーバ版のインストール。詳細は 161 ページの「Data Protector シングルサーバ版のインストール」を参照してください。
- Data Protector Web Reporting のインストール。詳細は 163 ページの「Data Protector Web Reporting のインストール」を参照してください。
- MC/ServiceGuard への Data Protector のインストール。詳細は 165 ページの「MC/ServiceGuard への Data Protector のインストール」を参照してください。
- Microsoft Cluster Server への Data Protector のインストール。詳細は 167 ページの「Data Protector の Microsoft Cluster Server へのインストール」を参照してください。
- Veritas Cluster への Data Protector クライアントのインストール。詳細は 178 ページの「Veritas Cluster への Data Protector クライアントのインストール」を参照してください。
- Novell NetWare Cluster への Data Protector クライアントのインストール。詳細は 179 ページの「Novell NetWare Cluster への Data Protector クライアントのインストール」を参照してください。

Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール

インストール手順は、図 2-1 を参照してください。

図 2-1 インストール手順



Cell Manager とインストール サーバを同一システム上にインストールする場合は、この作業を 1 つにまとめて実施できます。

重要 Data Protector セル内の構成情報やセッション情報に関するファイルはすべて、Cell Manager 上に保存されます。これらの情報を後から別のシステムに移動するのは困難です。そのため、適正に管理されている安定した環境内の信頼性の高いシステムを、Cell Manager として選択してください。

注記 この章では、DVD-ROM インストール メディアを使用している場合を想定して、Cell Manager およびインストール サーバのインストール手順と、クライアントのローカル インストール手順を説明しています。CD-ROM メディアを使用している場合は、C-1 ページの「付録 C」を参照してください。参照先には、インストール手順の違いと、CD-ROM の一覧が示されています。

UNIX 用 Cell Manager のインストール

この項では、UNIX 用 Cell Manager のインストール手順について、順を追って詳しく説明します。Windows 用 Cell Manager のみをインストールする場合は、29 ページの「Windows 用 Cell Manager のインストール」を参照してください。

前提条件

- Cell Manager として機能させる HP-UX、Solaris、または Linux システムは、以下の条件を満たしていなければなりません。
 - ✓ Data Protector ソフトウェアをインストールするのに十分な大きさの空きディスク スペースがあること。詳細は『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス』を参照してください。ディスク容量の不足については、リンク ディレクトリにインストールすることで解決できますが、最初に 24 ページの「HP-UX、Solaris、および Linux にインストールされるディレクトリの構造」および 27 ページの「Cell Manager のインストール用に割り当てるディスク スペースを増やす」を必ずお読みください。
 - ✓ IDBを作成するのに十分な大きさの空きディスク スペース (バックアップ対象データの約 2%) があること。詳細は『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス』を参照してください。現在の IDB の仕様では、

ネットワークへの Data Protector のインストール Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール

データベースのサイズが大きくなった場合に、必要に応じてデータベースのバイナリファイルを再配置できます。詳細は、オンライン ヘルプの索引キーワード「IDB, サイズの計算」で表示される内容を参照してください。

- ✓ ロング ファイル名がサポートされていること。使用しているファイルシステムでロング ファイル名がサポートされているかどうかを調べる場合は、`getconf NAME_MAX <directory>` コマンドを使用します。
 - ✓ `inetd` デーモンが実行されていること。
 - ✓ ポート番号 5555 (デフォルト) が利用可能であること。このポート番号がすでに使用されている場合は、B-28 ページの「デフォルトのポート番号の変更」を参照してください。
 - ✓ TCP/IP プロトコルがインストールされており、実行されていること。このプロトコルを使って、ホスト名を解決できること。
 - ✓ DVD-ROM ドライブにアクセスできること。
 - ✓ NIS サーバを使用する場合は、Cell Manager を認識するように構成されていること。詳細は B-30 ページの「NIS サーバの準備」を参照してください。
 - ✓ `ksh` シェルがインストールされていること。
- すべてのターゲット システムに対する `root` パーミッションが必要です。

注記 Linux 上では GUI はサポートされていません。ただし、`omniusers` コマンドを使用して、新しい Cell Manager 上にリモート ユーザー アカウントを作成することは可能です。これにより、Data Protector GUI をインストールした任意のシステム上でこのユーザー アカウントを使って GUI を起動し、新しい Cell Manager に接続できます。詳細は `omniusers` のマンページを参照してください。

クラスタ対応 Cell Manager

クラスタ対応 Cell Manager をインストールする場合は、前述の説明以外にも必要となる前提条件および手順があります。165 ページの「クラスタ対応 Cell Manager のインストール」を参照してください。

注記 マルチ セル環境 (MoM) では、すべての Cell Manager に同じバージョンの Data Protector をインストールする必要があります。

カーネル パラメータの設定

HP-UX では、カーネルパラメータ `maxdsiz`(最大データセグメントサイズ) を 134217728 バイト (128 MB) 以上に、また、カーネルパラメータ `semnu`(セマフォ取り消し構造体の数) を 256 以上に、それぞれ設定することをお勧めします。パラメータを変更したときは、カーネルを再コンパイルし、マシンを再起動してください。

Solaris では、`/etc/system` のカーネルパラメータ `shmsys:shminfo_shmmax`(最大共有メモリセグメントサイズ [SHMMAX]) を、67108864 バイト (64 MB) 以上に設定することをお勧めします。パラメータを変更したときは、この変更を確定し、マシンを再起動してください。

インストール手順

ヒント Cell Manager とインストール サーバを同じシステム上にインストールする場合は、`omnisetup.sh -CM -IS` コマンドを使用して、この作業をワンステップで実行できます。

`omnisetup.sh` コマンドの説明については、DVD-ROM の `<Mount_point>/LOCAL_INSTALL` ディレクトリにある README ファイルか、DVD-ROM の `<Mount_point>/DOCS/C/MAN` ディレクトリにある『HP OpenView Storage Data Protector Command Line Interface Reference』を参照してください。

HP-UX システム、Solaris システム、または Linux システムに UNIX 用 Cell Manager をインストールするには、以下の手順に従ってください。

1. UNIX インストール DVD-ROM をドライブに挿入し、マウントポイントにマウントします。

例：

```
mkdir /dvdrom
mount /dev/dsk/c0t0d0 /dvdrom
```

必要であれば、Data Protector をディスク上のデポからインストールすることもできます。その場合は、以下の手順に従ってください。

- インストールファイルが格納されている `DP_DEPOT` ディレクトリ、`AUTOPASS` ディレクトリ、および `LOCAL_INSTALL` をローカルディスクにコピーするには、以下のコマンドを実行します。

```
mkdir <directory>
cp -r /dvdrom/<platform_dir>/DP_DEPOT <directory>
cp -r /dvdrom/<platform_dir>/AUTOPASS <directory>
cp -r /dvdrom/<platform_dir>/LOCAL_INSTALL <directory>
```


ネットワークへの Data Protector のインストール Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール

ここで、<platform_dir>には、以下のいずれかの値を指定します。

hpux_ia	IA-64 システム上の HP-UX 11.23
hpux_pa	PA-RISC システム上の HP-UX
linux_x86_64	AMD64/Intel EM64T 上の Linux システム
solaris	Solaris システム

- DVD-ROM 全体をローカルディスクにコピーする場合は、以下のコマンドを実行します。

```
cp -r /dvdrom <dvd_image_dir>
```

2. omnisetup.sh コマンドを実行します。

このコマンドを DVD-ROM から実行するには、コマンドを以下のように入力します。

```
cd /dvdrom/LOCAL_INSTALL  
./omnisetup.sh -CM
```

ディスクからインストールを開始するには、以下の手順に従ってください。

- DP_DEPOT ディレクトリ、AUTOPASS ディレクトリ、および LOCAL_INSTALL ディレクトリを、ローカルディスク上の <directory> ディレクトリにコピーした場合は、以下のコマンドを実行します。

```
cd <directory>/LOCAL_INSTALL  
./omnisetup.sh -source <directory> -CM
```

- DVD-ROM 全体を <dvd_image_dir> にコピーした場合は、-CM パラメータ付きで omnisetup.sh コマンドを実行します。

```
cd <dvd_image_dir>/LOCAL_INSTALL  
./omnisetup.sh -CM
```

3. **HP-UX および Solaris の場合**、omnisetup.sh コマンドを実行するとプロンプトが表示され、購入済みライセンスのパスワードを HP Password Delivery Center の Web サーバからインターネットを介して直接ダウンロードしてインストールする場合は、HP OpenView AutoPass ユーティリティをインストールまたはアップグレードするよう指示されます。AutoPass ユーティリティに関する詳細は 309 ページの「HP OpenView AutoPass ユーティリティを使用した恒久パスワードの取得とインストール」を参照してください。AutoPass はできるだけインストールすることをお勧めします。

AutoPass を MC/ServiceGuard にインストールする場合は、すべてのノードにインストールする必要があります。

ネットワークへの Data Protector のインストール

Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール

プロンプトが表示されたら、**[Return]** キーを押して AutoPass をインストールまたはアップグレードします。AutoPass をインストールまたはアップグレードしない場合は、**n** と入力します。

Linux には、HP OpenView AutoPass はインストールされません。

注記

Solaris 9 または Solaris 10 上で Cell Manager をインストールまたはアップグレードした場合は、インストールやアップグレードの完了後にインストール サーバを使用して Cell Manager 上に Disk Agent をリモート インストールすることができます。これにより、汎用の Solaris Disk Agent が Solaris 9 Disk Agent または Solaris 10 Disk Agent に置き換えられます。詳細は、50 ページの「Data Protector クライアントのリモート インストール」を参照するか、または ob2install のマンページを参照してください。

UNIX 用のインストール サーバを Cell Manager 上にインストールする場合は、この段階でインストールしてください。必要な手順の詳細は、37 ページの「UNIX 用のインストール サーバのインストール」を参照してください。

HP-UX、Solaris、および Linux にインストールされるディレクトリの構造

Data Protector のコア ソフトウェアは /opt/omni/bin ディレクトリにインストールされ、UNIX 用のインストール サーバは /opt/omni/databases/vendor ディレクトリにインストールされます。以下の一覧は Data Protector のサブディレクトリとその内容を示したものです。

重要

Data Protector は、たとえば次のようなリンク ディレクトリにインストールすることができます。

```
/opt/omni/ -> /<prefix>/opt/omni/
```

```
/var/opt/omni/ -> /<prefix>/var/opt/omni/
```

```
/etc/opt/omni/ -> /<prefix>/etc/opt/omni/
```

このようにする場合は、インストール前にリンクを作成しておき、インストール先ディレクトリが存在することを確認しておかなければなりません。

詳細は 27 ページの「Cell Manager のインストール用に割り当てるディスク スペースを増やす」を参照してください。

/opt/omni/bin	すべてのコマンド
---------------	----------

/opt/omni/gui	GUI 項目
---------------	--------

ネットワークへの Data Protector のインストール Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール

/opt/omni/gui/help	オンライン ヘルプ ファイル
/opt/omni/lbin	Data Protector 内部コマンド
/opt/omni/sbin	スーパーユーザー用コマンド
/opt/omni/sbin/install	インストール用スクリプト
/etc/opt/omni	構成情報
/opt/omni/lib	圧縮、データ暗号化、デバイス処理のための共有ライブラリ
/opt/omni/doc/C	オンラインドキュメント (オプション)
/var/opt/omni/log および /var/opt/omni/server/log	ログ ファイル
/opt/omni/lib/nls/C	メッセージ カタログ ファイル
/opt/omni/lib/man	マンページ
/var/opt/omni/tmp	一時ファイル
/var/opt/omni/server/db40	IDB ファイル (オンライン ヘルプの索引キーワード「IDB, ディレクトリの位置」で表示される内容を参照)

自動での起動とシャットダウンの構成

Data Protector のインストール時には、システムの再起動時にすべての Data Protector プロセスが自動的にシャットダウンおよび起動されるように構成されます。この構成の一部は、オペレーティング システムによって異なります。

以下のファイルが自動的に構成されます。

HP-UX の場合:

/sbin/init.d/omni	起動処理およびシャットダウン処理を実行するスクリプト。
/sbin/rc1.d/K162omni	Data Protector をシャットダウンする /sbin/init.d/omni スクリプトへのリンク。
/sbin/rc2.d/S838omni	Data Protector を起動する /sbin/init.d/omni スクリプトへのリンク。
/etc/rc.config.d/omni	omni 変数が格納されます。この変数は、以下のいずれかの値をとります。 omni=1 システムの再ブート時に Data Protector の自動停止および自動起動を行います。デフォルトでは、この値が適用されます。

ネットワークへの Data Protector のインストール

Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール

omni=0 システムの再ブート時に Data Protector の自動停止および自動起動を行いません。

Solaris の場合:

/etc/init.d/omni 起動処理およびシャットダウン処理を実行するスクリプト。
/etc/rc1.d/K09omni Data Protector をシャットダウンする /etc/init.d/omni スクリプトへのリンク。
/etc/rc2.d/S97omni Data Protector を起動する /etc/init.d/omni スクリプトへのリンク。

Linux の場合:

/etc/init.d/omni 起動処理およびシャットダウン処理を実行するスクリプト。
/etc/rc<init_level>.d/K10omni Data Protector をシャットダウンする /etc/init.d/omni スクリプトへのリンク。
<init_level> は 1 および 6 です。
/etc/rc<init_level>.d/S90omni Data Protector を起動する /etc/init.d/omni スクリプトへのリンク。
<init_level> は 2、3、4、5 です。

インストール中には、Cell Manager システムのシステム ファイルのうち、以下のファイルが修正されます。

HP-UX の場合:

/etc/services Data Protector のサービス用ポート番号がファイルに追加されます。
/opt/omni/lbin/crs Data Protector CRS サービスが追加されます。

インストールが完了すると、以下のプロセスが UNIX 用 Cell Manager 上で動作するようになります。

/opt/omni/lbin/crs システムに Cell Manager ソフトウェアをインストールすると、Cell Manager システム上で Data Protector Cell Request Server (CRS) サービスが実行されます。CRS は、セル内のバックアップ セッションおよび復元セッションの開始および制御に使用されます。

ネットワークへの Data Protector のインストール Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール

<code>/opt/omni/lbin/rds</code>	システムに Cell Manager ソフトウェアをインストールすると、Cell Manager システム上で Data Protector Raima Database Server (RDS) サービスが実行されます。RDS は、IDB の管理に使用されます。
<code>/opt/omni/lbin/mmd</code>	システムに Cell Manager ソフトウェアをインストールすると、Cell Manager 上で Data Protector Media Management Daemon (MMD) サービスが実行されます。MMD は、デバイスおよびメディアの管理操作に使用されます。

環境変数の設定

先に説明した UNIX 用 Cell Manager のインストール時には、Data Protector のユーザー インタフェースもインストールされます。

ユーザー インタフェース (グラフィカル ユーザー インタフェースまたはコマンド行インタフェース) を使用する場合は、事前に次の内容を環境変数に追加してください。

`/opt/omni/bin`、`/opt/omni/lbin`、および、`/opt/omni/sbin` を、`PATH` 変数に追加します。

`/opt/omni/lib/man` を `MANPATH` 変数に追加します。

`/opt/omni/lib` および `/opt/omni/lib/arm` を `LD_LIBRARY_PATH` 変数に追加します。

さらに、グラフィカル ユーザー インタフェースを使用する前に、`DISPLAY` 変数とロケール設定が正しく設定されていることも確認してください。

注記

複数プラットフォームにわたるバックアップや復元を Data Protector ユーザー インタフェースを使用して実行する予定がある場合は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス』を参照して制限事項を確認してください。また、Data Protector GUI の言語設定のカスタマイズ方法については、オンラインヘルプの索引キーワード「言語設定、カスタマイズ」で表示される内容を参照してください。

Cell Manager のインストール用に割り当てるディスクスペースを増やす

UNIX 用 Cell Manager をインストールする場合は、特に、`/opt` ディレクトリと、データベースの保存先となる `/var` ディレクトリに、十分な空きディスクスペース (バックアップ対象データの約 2%) が必要です。必要となるディスクスペースの詳細は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス』を参照してください。ディス

ク スペースが足りない場合はリンク ディレクトリを使用することも可能ですが、その場合はインストール前にリンクを作成しておき、インストール先ディレクトリが存在することを確認しておかなければなりません。以下に手順例を示します。

- マウントされたディスク、/data_protector に十分な空きスペースのある場合は、/opt/omni 用に以下のリンクを作成します。

```
mkdir /data_protector/opt_omni
```

```
ln -s /data_protector/opt_omni /opt/omni
```

リンクさせるその他のディレクトリについても、同様の操作を繰り返します (/var/opt/omni や /etc/opt/omni など)。

- HP-UX 上で**、ファイルシステムは存在するが現在マウントが解除されている場合は、以下のようにしてマウントします。なお、ここでは、/dev/vgspare/lvol2 をマウントするものとします。

```
mkdir /opt/omni
```

```
mount /dev/vgspare/lvol2 /opt/omni
```

- Solaris 上で**、ファイルシステムは存在するが現在マウントが解除されている場合は、以下のようにしてマウントします。なお、ここでは、/dev/dsk/c0t0d0s0 をマウントするものとします。

```
mkdir /opt/omni
```

```
mount /dev/dsk/c0t0d0s0 /opt/omni
```

この次に行う作業

この時点で、Cell Manager がインストールされている必要があります。さらに、同じシステム上にインストールするよう選択した場合は、UNIX 用のインストール サーバもインストールされていなければなりません。この後、以下の作業を行います。

- UNIX 用のインストール サーバを同一システム上にインストールしなかった場合は、37 ページの「UNIX 用のインストール サーバのインストール」を参照してください。
- ソフトウェアを Windows クライアントにリモート インストールしたい場合は、Windows 用のインストール サーバをインストールします。詳細は 41 ページの「Windows 用のインストール サーバのインストール」を参照してください。
- ソフトウェアをクライアントに配布します。詳細は 46 ページの「Data Protector クライアントのインストール」を参照してください。

Windows 用 Cell Manager のインストール

前提条件

Cell Manager システムとして使用する Windows システムは、以下の条件を満たしている必要があります。

- ✓ サポート対象の Windows オペレーティング システムがインストールされていること。Cell Manager でサポートされているオペレーティングシステムの詳細は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。
- ✓ Microsoft Internet Explorer 5.0 以上がインストールされていること。
- ✓ Data Protector Cell Manager ソフトウェアをインストールするのに十分な容量の空きディスクスペースがあること。詳細は『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。
- ✓ IDB を作成するのに十分な容量の空きディスク スペース (バックアップ対象データの約2%) があること。詳細は『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。
- ✓ ポート番号 5555 (デフォルト) が利用可能であること。このポート番号がすでに使用されている場合は、B-28 ページの「デフォルトのポート番号の変更」を参照してください。
- ✓ Cell Manager のインストール先のシステムには、静的な IP アドレスが必要です。DHCP クライアントとして構成されているシステムの場合は、IP アドレスが動的に割り当てられるため、システム用の恒久 DNS エントリを割り当ててシステムを再構成するか、または、DHCP サーバを構成して、このシステムに予約された静的 IP アドレスが使用されるようにする必要があります。後者の場合は、IP アドレスがシステムの MAC アドレスにバインドされます。
- ✓ Microsoft 社の TCP/IP プロトコルがインストールされており、実行されていること。このプロトコルを使って、ホスト名を解決できること。コンピュータの名前とホスト名は同じでなければなりません。TCP/IP プロトコルのインストールおよび構成については、B-19 ページの「Windows システム上の TCP/IP プロトコルのセットアップ」を参照してください。
- ✓ DVD-ROM ドライブにアクセスできること。

Microsoft ターミナルサービスクライアント

- ✓ Microsoft ターミナルサービスクライアントを介して Windows 上に Data Protector をインストールする場合は、Data Protector のインストール先システムで、[ターミナルサーバーモード] が [リモート管理] に設定されていることを確認してください。

ネットワークへの Data Protector のインストール

Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール

1. Windows の [コントロールパネル] で [管理ツール] をクリックし、次に [ターミナルサービス構成] をクリックします。
2. [ターミナルサービス構成] ダイアログ ボックスで、[サーバー設定] をクリックします。ターミナル サービス サーバがリモート管理モードで実行中であることを確認してください。

推奨事項

Data Protector A.06.00 のインストールを開始するにあたって、Microsoft Installer (MSI) 2.0 がインストールされていることを確認してください。MSI のバージョンが古い場合は、Data Protector セットアップ プログラムにより、自動的にバージョン 2.0 にアップグレードされます。この場合、Data Protector では、アップグレードの最後の段階で、MSI がアップグレードされたことが通知されます。MSI がアップグレードされた場合は、システムを再起動することを強く推奨します。

Data Protector A.06.00 をインストールする前に、MSI をバージョン 2.0 にアップグレードすることをお勧めします。

クラスタ対応 Cell Manager

クラスタ対応 Cell Manager をインストールする場合は、前述の説明以外にも必要となる前提条件および手順があります。167 ページの「クラスタ対応 Cell Manager のインストール」を参照してください。

インストール手順

Windows システムに新規でインストールするには、以下の手順に従ってください。

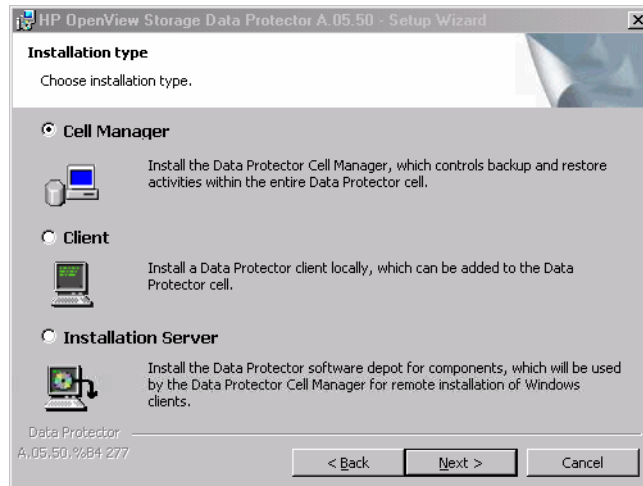
1. Windows 用インストール DVD-ROM をドライブに挿入し、以下のコマンドを実行します。
32 ビット システムの場合: %Windows_other%\i386\setup.exe
64 ビット システムの場合: %Windows_other%\x8664\setup.exe
Data Protector セットアップ用ウィザードが表示されます。
2. セットアップ用ウィザードの指示に従って操作を行い、ライセンス契約を十分にお読みください。記載内容に同意する場合は、[Next] をクリックして次に進みます。

ネットワークへの Data Protector のインストール

Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール

3. [Installation Type] ページで、[Cell Manager] を選択します。[Next] をクリックすると、選択した Data Protector Cell Manager ソフトウェアがインストールされます。

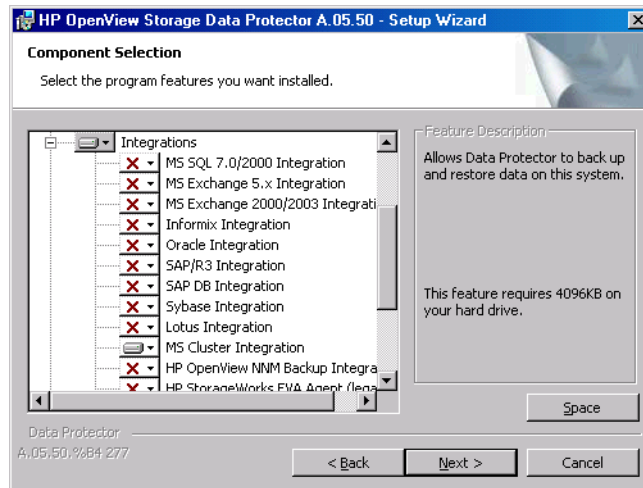
図 2-2 **インストールの種類を選択**



4. Data Protector サービスを実行するアカウントの、ユーザー名とパスワードを入力します。
[Next] をクリックして次に進みます。
5. Data Protector をデフォルト フォルダにインストールする場合には、[Next] をクリックします。
デフォルト以外のフォルダにインストールする場合には、[Change] をクリックし、
[Change Current Destination Folder] ウィンドウを開いて、新しいパスを入力します。

- [Component Selection] ページで、インストールするコンポーネントを選択します。Data Protector コンポーネントのリストと説明は、59 ページの「Data Protector コンポーネント」を参照してください。

図 2-3 ソフトウェア コンポーネントの選択



[Disk Agent]、[General Media Agent]、[User Interface]、および [インストールサーバ] は、デフォルトで選択されています。[Next] をクリックします。

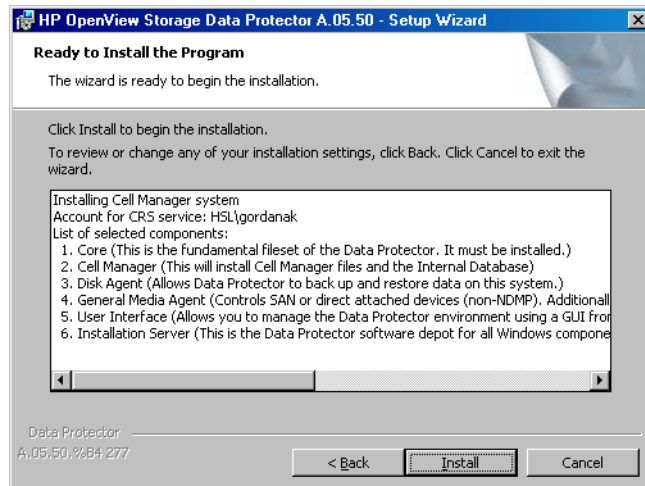
- Windows XP SP2、Windows 2003 SP1 の場合:** Data Protector によってシステムにファイアウォールが検出されると、[Windows Firewall configuration] ページが表示されます。Data Protector のセットアッププログラムによって、必要なすべての Data Protector 実行可能ファイルが登録されます。デフォルトでは、[Initially, enable newly registered Data Protector binaries to open ports as needed] オプションが選択されています。この時点で、Data Protector によってポートがオープンされないようにするには、オプションを選択解除します。ただし、Data Protector を適切に機能させるには、実行可能ファイルを有効にする必要があります。

[Next] をクリックします。

ネットワークへの Data Protector のインストール Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール

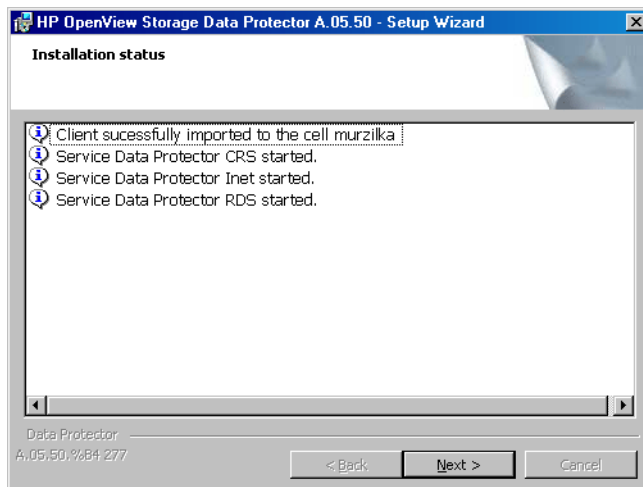
8. コンポーネントのサマリー リストが表示されます。選択したコンポーネントのインストールを開始するには、[Install] をクリックします。インストールには数分かかる場合があります。

図 2-4 コンポーネントのサマリー リスト



9. [Installation status] ページが表示されます。[Next] をクリックします。

図 2-5 **[Installation Status] ページ**



10. *Windows x64* 以外のオペレーティングシステムでは、購入済みライセンスのパスワードを HP Password Delivery Center の Web サーバからインターネットを介して直接ダウンロードしてインストールする場合は、セットアップ用ウィザードに従って、HP OpenView AutoPass ユーティリティをインストールまたはアップグレードします。詳細は 309 ページの「HP OpenView AutoPass ユーティリティを使用した恒久パスワードの取得とインストール」を参照してください。

デフォルトでは、[Start AutoPass installation] オプション、または [Upgrade AutoPass installation] オプションが選択されています。HP OpenView AutoPass ユーティリティをインストールすることをお勧めします。AutoPass をインストールまたはアップグレードしない場合は、オプションを選択解除します。

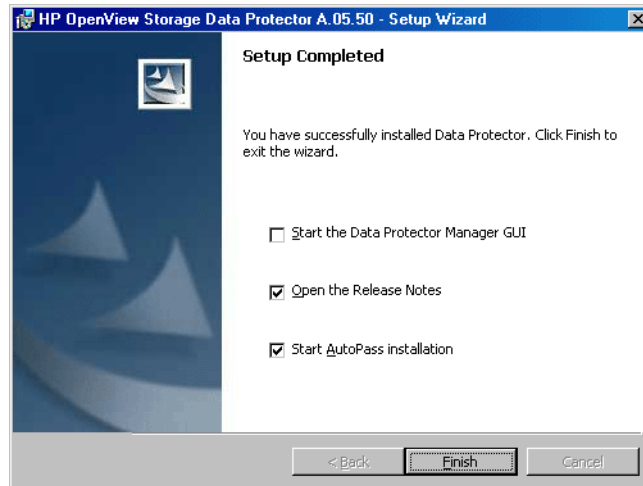
Windows x64 オペレーティングシステムには、AutoPass はインストールされません。

セットアップ後すぐに Data Protector を起動するには、[Start the Data Protector Manager] を選択します。

ネットワークへの Data Protector のインストール Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール

『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を表示するには、[Open the Product Announcements] を選択します。

図 2-6 AutoPass をインストール対象として選択する場合



[Finish] をクリックします。

インストール完了後

セットアップが完了すると、Cell Manager ファイルは <Data_Protector_home>%bin ディレクトリにインストールされ、Windows 用のソフトウェア デポは <Data_Protector_home>%Depot ディレクトリにインストールされています。

インストールが完了すると、以下のプロセスが Cell Manager システム上で動作するようになります (これらのファイルは、<Data_Protector_home>%bin ディレクトリに格納されています)。

crs.exe

システムに Cell Manager ソフトウェアをインストールすると、Cell Manager システム上で Data Protector Cell Request Server (CRS) サービスが実行されます。CRS は、セル内のバックアップセッションおよび復元セッションの開始および制御に使用されます。

ネットワークへの Data Protector のインストール

Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール

rds.exe	システムに Cell Manager ソフトウェアをインストールすると、Cell Manager システム上で Data Protector Raima Database Server (RDS) サービスが実行されます。RDS は、IDB の管理に使用されます。
OmniInet.exe	ネットワーク上の他のシステムの Data Protector サービスとの通信を可能にする Data Protector 常駐サービスです。Data Protector Inet サービスは、Data Protector セル内のすべてのシステム上で実行することが必要です。

注記 複数プラットフォームにわたるバックアップや復元を Data Protector ユーザー インタフェースを使用して実行しよう計画している場合は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照して制限事項を確認してください。

ヒント Data Protector GUI で適切なエンコーディングが使用できない場合は、ファイル名を正しく表示するために、コード ページ変換テーブルを追加でインストールすることが可能です。手順の詳細は、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。

トラブルシューティング

セットアップを正常に完了できない場合は、**セットアップ**自体がチェックする必要条件を検証し、その条件が満たされていなかった場合にエラーの原因となる項目を調べてください。詳細は 29 ページの「前提条件」を参照してください。

セットアップがチェックする必要条件を以下に示します。

- ✓ Service Pack のバージョンが正しいこと。
- ✓ NSLookup を実行して、Data Protector がホスト名を解決できることが確認されていること。
- ✓ ディスク スペースが十分にあること。
- ✓ 管理権限が正しく構成されていること。

この次に行う作業

この時点で、Cell Manager がインストールされている必要があります。さらに、同じシステム上にインストールするよう選択した場合は、Windows 用のインストール サーバもインストールされていなければなりません。この後、以下の作業を行います。

ネットワークへの Data Protector のインストール Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール

1. オペレーティング システムが混在するバックアップ環境の場合は、UNIX 用のインストール サーバをインストールします。詳細は 37 ページの「インストール サーバのインストール」を参照してください。なお、UNIX 用のインストール サーバが不要な場合は、この作業は省略できます。
2. ソフトウェアをクライアントに配布します。詳細は 46 ページの「Data Protector クライアントのインストール」を参照してください。

インストール サーバのインストール

インストール サーバは、Cell Manager システム上にインストールすることも、LAN を介して Cell Manager と接続されているサポート対象システム上にインストールすることも可能です。インストール サーバでサポートされているオペレーティング システムの詳細は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。

Cell Manager とは別のシステム上にインストール サーバを配置する場合は、該当するソフトウェア デポをローカルにインストールしてください。この項では、手順の詳細を説明します。

UNIX 用のインストール サーバのインストール

UNIX の場合の前提条件

インストール サーバシステムとして使用する UNIX システムは、以下の条件を満たしている必要があります。

- ✓ HP-UX、Solaris、Linux のいずれかのオペレーティング システムがインストールされていること。インストール サーバでサポートされているオペレーティング システムの詳細は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。
- ✓ inetd デーモンが実行されていること。
- ✓ ポート番号 5555 (デフォルト) が利用可能であること。このポート番号がすでに使用されている場合は、B-28 ページの「デフォルトのポート番号の変更」を参照してください。
- ✓ TCP/IP プロトコルがインストールされており、実行されていること。このプロトコルを使って、ホスト名を解決できること。
- ✓ 完全な Data Protector ソフトウェア デポを作成するのに十分な空きディスク スペースがあること。詳細は『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。

- ✓ DVD-ROM ドライブがあること。
- ✓ Data Protector セル内の Cell Manager は、バージョン A.06.00 であること。

重要

Data Protector をリンク ディレクトリにインストールするには、たとえば次のような手順を実行します。

```
/opt/omni/ -> /<prefix>/opt/omni/  
/etc/opt/omni/ -> /<prefix>/etc/opt/omni/  
/var/opt/omni/ -> /<prefix>/var/opt/omni/
```

このようにする場合は、インストール前にリンクを作成しておき、インストール先ディレクトリが存在することを確認しておかなければなりません。

注記

ネットワーク上のデバイスからソフトウェアをインストールする場合は、まず、インストール対象のコンピュータにソース ディレクトリをマウントします。

インストール手順

UNIX 用のインストール サーバを HP-UX システム、Solaris システム、または Linux システムにインストールするには、以下の手順に従ってください。

1. UNIX インストール DVD-ROM をドライブに挿入し、マウント ポイントにマウントします。

例：

```
mkdir /dvdrom  
mount /dev/dsk/c0t0d0 /dvdrom
```

必要であれば、Data Protector をディスク上のデポからインストールすることもできます。その場合は、以下の手順に従ってください。

- インストール ファイルが格納されている DP_DEPOT ディレクトリ、AUTOPASS ディレクトリ、および LOCAL_INSTALL をローカル ディスクにコピーするには、以下のコマンドを実行します。

```
mkdir <directory>  
cp -r /dvdrom/<platform_dir>/DP_DEPOT <directory>  
cp -r /dvdrom/<platform_dir>/AUTOPASS <directory>  
cp -r /dvdrom/LOCAL_INSTALL <directory>
```

ここで、<platform_dir>には、以下のいずれかの値を指定します。

ネットワークへの Data Protector のインストール Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール

hpux_ia	IA-64 システム上の HP-UX 11.23
hpux_pa	PA-RISC システム上の HP-UX
linux_x86_64	AMD64/Intel EM64T 上の Linux システム
solaris	Solaris システム

- DVD-ROM 全体をローカル ディスクにコピーする場合は、以下のコマンドを実行します。

```
cp -r /dvdrom <dvd_image_dir>
```

2. omnisetup.sh コマンドを実行します。

このコマンドを DVD-ROM から実行するには、コマンドを以下のように入力します。

```
cd /dvdrom/LOCAL_INSTALL  
./omnisetup.sh -IS
```

ディスクからインストールを開始するには、以下の手順に従ってください。

- DP_DEPOT ディレクトリ、AUTOPASS ディレクトリ、および LOCAL_INSTALL ディレクトリを、ローカル ディスク上の <directory> ディレクトリにコピーした場合は、以下のコマンドを実行します。

```
cd <directory>/LOCAL_INSTALL  
./omnisetup.sh -source <directory> -IS
```

- DVD-ROM 全体を <dvd_image_dir> にコピーした場合は、-IS パラメータ付きで omnisetup.sh コマンドを実行します。

```
cd <dvd_image_dir>/LOCAL_INSTALL  
./omnisetup.sh -IS
```

omnisetup.sh コマンドの説明については、DVD-ROM の <Mount_point>/ ディレクトリにある README ファイルか、DVD-ROM の <Mount_point>/DOCS/C/MAN ディレクトリにある『HP OpenView Storage Data Protector Command Line Interface Reference』を参照してください。

インストールが終了すると、UNIX 用のソフトウェア デポは、/opt/omni/databases/vendor ディレクトリにインストールされます。

omnisetup.sh コマンドを実行すると、インストール サーバのすべてのパッケージがインストールされます。パッケージの一部のみをインストールする場合は、swinstall コマンド (HP-UX の場合)、pkgadd コマンド (Solaris の場合)、または rpm コマンド (Linux の場合) を使用する必要があります。詳細は、B-3 ページの付録 B 「ネイティブ ツールを使用した、HP-UX、Solaris、および Linux システムへのインストール」を参照してください。

重要

ネットワーク上に UNIX 用のインストール サーバをインストールしない場合は、UNIX インストール DVD-ROM を使用して、すべての UNIX クライアントをローカルにインストールしなければなりません。

注記

ユーザー インタフェース コンポーネント (グラフィカル ユーザー インタフェースまたはコマンド行インタフェース) を使用する場合は、事前に環境変数を更新する必要があります。詳細は 27 ページの「環境変数の設定」を参照してください。

複数プラットフォームにわたるバックアップや復元を Data Protector ユーザー インタフェースを使用して実行するよう計画している場合は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照して制限事項を確認してください。

この次に行う作業

この時点で、UNIX 用のインストール サーバがネットワーク上にすでにインストールされていない必要があります。準備が整ったら、以下の作業を実施します。

1. インストール サーバを Cell Manager とは別のシステムにインストールした場合は、そのシステムを Data Protector セルに追加 (インポート) する必要があります。詳細については、187 ページの「セルへのインストール サーバのインポート」を参照してください。

注記

インストール サーバをインポートすると、Cell Manager 上の `/etc/opt/omni/server/cell/installation_servers` ファイルが更新されて、インストールしたプッシュ パッケージが反映されます。CLI からこのファイルを使用して、使用可能なプッシュ パッケージを確認できます。このファイルを最新状態に保つために、プッシュ パッケージをインストールまたは削除したときは、インストール サーバのエクスポートと再インポートを必ず実行してください。これは、インストール サーバを Cell Manager と同じシステムにインストールしてある場合も同様です。

2. Data Protector セルに Windows システムが含まれている場合は、Windows 用のインストール サーバをインストールする必要があります。詳細は 41 ページの「Windows 用のインストール サーバのインストール」を参照してください。

ネットワークへの Data Protector のインストール Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール

3. ソフトウェアをクライアントに配布します。詳細は 46 ページの「Data Protector クライアントのインストール」を参照してください。

Windows 用のインストール サーバのインストール

前提条件

インストール サーバ システムとして使用する Windows システムは、以下の条件を満たしている必要があります。

- ✓ サポート対象の Windows オペレーティング システムがインストールされていること。インストール サーバでサポートされているオペレーティング システムの詳細は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。
- ✓ Microsoft Internet Explorer 5.0 以上がインストールされていること。
- ✓ 完全な Data Protector ソフトウェア デポを作成するのに十分な空きディスク スペースがあること。詳細は『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。
- ✓ DVD-ROM ドライブにアクセスできること。
- ✓ Microsoft 社の TCP/IP プロトコルがインストールされており、実行されていること。このプロトコルを使って、ホスト名を解決できること。コンピュータの名前とホスト名は同じでなければなりません。TCP/IP プロトコルのインストールおよび構成については、B-19 ページの「Windows システム上の TCP/IP プロトコルのセットアップ」を参照してください。

制限事項

Windows オペレーティング システムのセキュリティ規制により、インストール サーバを使用してクライアントをリモートにインストールできるのは、同ドメイン内に限られます。

推奨事項

Data Protector A.06.00 のインストールを開始するにあたって、Microsoft Installer (MSI) 2.0 がインストールされていることを確認してください。MSI のバージョンが古い場合は、Data Protector セットアップ プログラムにより、自動的にバージョン 2.0 にアップグレードされます。この場合、Data Protector によって、アップグレードの最後の段階で MSI がアップグレードされたことが通知されます。MSI がアップグレードされた場合は、システムを再起動することを強く推奨します。個々の Windows オペレーティング システムに対する MSI 2.0 の前提条件については、Microsoft Support にお問い合わせください。

Data Protector A.06.00 をインストールする前に、MSI をバージョン 2.0 にアップグレードすることをお勧めします。

重要 Windows 用のインストール サーバをネットワーク上にインストールしない場合は、すべての Windows クライアントを、DVD-ROM を使ってローカルにインストールしなければなりません。

注記 インストール サーバをすでにインストールしてある Windows システムには、Data Protector クライアントをリモートでインストールすることはできません。同一システム上にインストール サーバとクライアント コンポーネントをインストールする場合は、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。この場合はインストール手順の中で、必要なクライアント コンポーネントとインストール サーバ コンポーネントをすべて選択してください。詳細は 63 ページの「Windows 用クライアントのインストール」を参照してください。

インストール手順

Windows 用のインストール サーバをインストールするには、以下の手順に従ってください。

1. Windows 用インストール DVD-ROM をドライブに挿入し、以下のコマンドを実行します。

32 ビット システムの場合: %Windows_other%i386%setup.exe

64 ビット システムの場合: %Windows_other%x8664%setup.exe

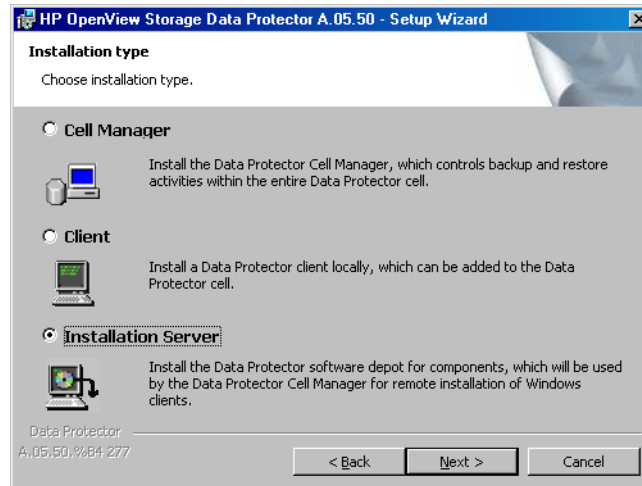
Data Protector セットアップ用ウィザードが表示されます。

2. セットアップ用ウィザードの指示に従って操作を行い、ライセンス契約を十分にお読みください。記載内容に同意する場合は、[Next] をクリックして次に進みます。

ネットワークへの Data Protector のインストール Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール

3. [Installation Type] ページで、[インストール サーバ] を選択します。[Next] をクリックすると、選択した Data Protector ソフトウェア デポがインストールされます。

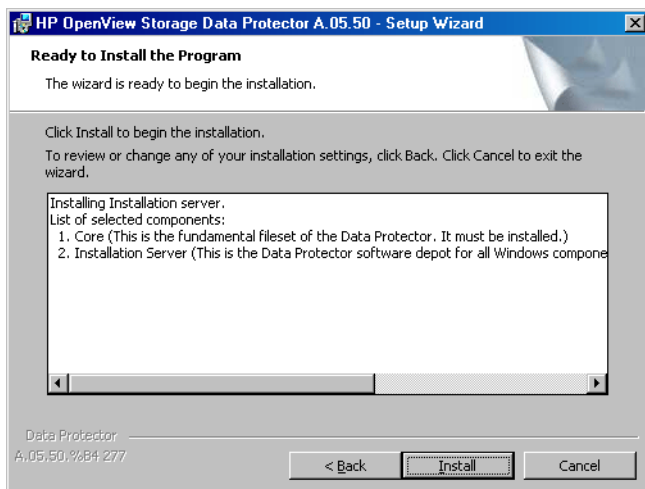
図 2-7 インストールの種類を選択



4. Data Protector をデフォルト フォルダにインストールする場合には、[Next] をクリックします。
デフォルト以外のフォルダにインストールする場合には、[Change] をクリックし、[Change Current Destination Folder] ウィンドウを開いて、新しいパスを入力します。
5. **Windows XP SP2、Windows 2003 SP1 の場合**:Data Protector によってシステムにファイアウォールが検出されると、[Windows Firewall configuration] ページが表示されます。Data Protector のセットアッププログラムによって、必要なすべての Data Protector 実行可能ファイルが登録されます。デフォルトでは、[Initially, enable newly registered Data Protector binaries to open ports as needed] オプションが選択されています。この時点で、Data Protector によってポートがオープンされないようにするには、オプションを選択解除します。ただし、Data Protector を適切に機能させるには、実行可能ファイルを有効にする必要があります。
[Next] をクリックします。

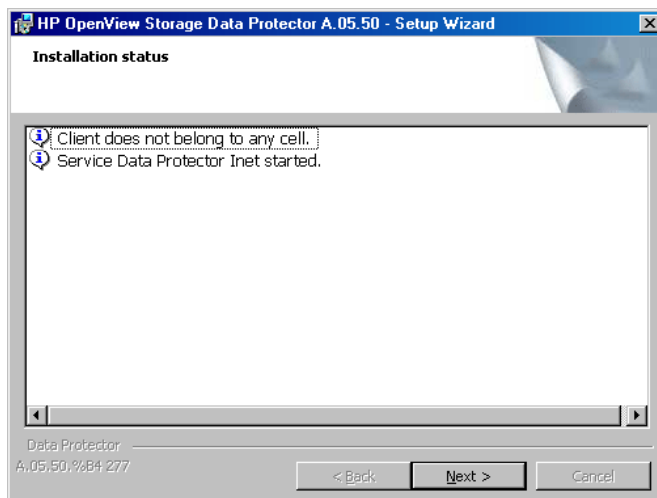
- コンポーネントのサマリー リストが表示されます。選択したコンポーネントのインストールを開始するには、[Install] をクリックします。インストールには数分かかる場合があります。

図 2-8 コンポーネント選択サマリー ページ



- [Installation status] ページが表示されます。[Next] をクリックします。

図 2-9 [Installation Status] ページ



ネットワークへの Data Protector のインストール Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール

- 『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を表示するには、[Open the Product Announcements] を選択します。

[Finish] をクリックします。

インストールが終了したら、ソフトウェアはデフォルトで <Data_Protector_home>\Depot ディレクトリに保存されます。このディレクトリは共有ディレクトリで、ネットワーク上の他のコンピュータからアクセスできます。

この次に行う作業

この時点で、Windows 用のインストールサーバがネットワーク上にインストールされていなければなりません。準備が整ったら、以下の作業を実施します。

- (Cell Manager とは別のシステムに) 独立した形でインストールサーバをセットアップした場合は、このシステムを Data Protector セルに手作業で追加 (インポート) しなければなりません。詳細は 187 ページの「セルへのインストールサーバのインポート」を参照してください。
- オペレーティングシステムが混在するバックアップ環境の場合は、HP-UX システム、Solaris システム、または Linux システム上に、UNIX 用のインストールサーバをインストールします。詳細は 37 ページの「UNIX 用のインストールサーバのインストール」を参照してください。
- ソフトウェアをクライアントに配布します。詳細は 46 ページの「Data Protector クライアントのインストール」を参照してください。

Data Protector クライアントのインストール

Data Protector クライアントは、インストール サーバを使って配布することによりリモートでインストールでき、また、インストール DVD-ROM からローカルにインストールすることもできます。

Data Protector インストール DVD-ROM の一覧については、8 ページの「Data Protector のインストール DVD-ROM」を参照してください。

Data Protector クライアントをインストールして Data Protector セル内にインポートした後は、インストール結果を確認し、不正アクセスからクライアントを保護することを強くお勧めします。クライアントのインストール結果を確認する手順は、330 ページの「Data Protector クライアントのインストール結果の確認」を参照してください。セキュリティ保護の詳細は、195 ページの「保護について」を参照してください。

表 2-1 は、Data Protector クライアント システムの一覧と詳細説明の参照先を示したものです。

表 2-1 Data Protector クライアント システムのインストール

クライアント システム	インストール方法と参照先
Windows	リモートおよびローカル インストール。63 ページの「Windows 用クライアントのインストール」を参照。
HP-UX	リモートおよびローカル インストール。68 ページの「HP-UX クライアントのインストール」を参照。
AIX	リモートおよびローカル インストール。85 ページの「AIX クライアントのインストール」を参照。
Solaris	リモートおよびローカル インストール。72 ページの「Solaris 用クライアントのインストール」を参照。
Tru64	リモートおよびローカル インストール。89 ページの「Tru64 クライアントのインストール」を参照。

表 2-1 Data Protector クライアント システムの
インストール (続き)

クライアント システム	インストール方法と参照先
Siemens Sinix	リモートおよびローカル インストール。87 ページの「Siemens Sinix クライアントのインストール」を参照。
SCO	リモートおよびローカル インストール。91 ページの「SCO クライアントのインストール」を参照。
Linux	リモートおよびローカル インストール。79 ページの「Linux クライアントのインストール」を参照。
DAS クライアント	リモートおよびローカル インストール。93 ページの「ADIC/GRAU ライブラリ用または StorageTek ライブラリ用の Media Agent のインストール」を参照。
ACS クライアント	リモートおよびローカル インストール。93 ページの「ADIC/GRAU ライブラリ用または StorageTek ライブラリ用の Media Agent のインストール」を参照。
Novell NetWare	ローカル インストール。102 ページの「Novell NetWare クライアントのローカル インストール」を参照。
OpenVMS	ローカル インストール。108 ページの「OpenVMS クライアントのローカル インストール」を参照。
MPE/iX	ローカル インストール。115 ページの「MPE/iX クライアントのインストール」を参照。
その他の UNIX クライアント	ローカル インストール。119 ページの「UNIX クライアントのローカル インストール」を参照。

ネットワークへの Data Protector のインストール Data Protector クライアントのインストール

統合ソフトウェア

Data Protector 統合ソフトウェアは、Data Protector を使ってデータベース アプリケーションのバックアップを可能にするソフトウェア コンポーネントです。これらのコンポーネントを統合ソフトウェアと呼びます。MS Exchange Server データベースのバックアップには MS Exchange 2000/2003 Integration コンポーネントを使用し、Oracle データベースのバックアップには Oracle Integration コンポーネントを使用するというように、適切な統合ソフトウェアを選択すれば、データベース アプリケーションを実行するシステムを Windows クライアント システムおよび UNIX クライアント システムと同じ方法でインストールできます。詳細は本章の表 2-2 を参照してください。

表 2-2 統合ソフトウェアのインストール

アプリケーション	参照先
Microsoft Exchange Server	詳細は、127 ページの「Microsoft Exchange Server クライアント」を参照してください。
Microsoft SQL Server	詳細は、128 ページの「MS SQL クライアント」を参照してください。
Sybase	詳細は、128 ページの「Sybase クライアント」を参照してください。
Informix Server	詳細は、128 ページの「Informix Server クライアント」を参照してください。
SAP R/3	詳細は、129 ページの「SAP R/3 クライアント」を参照してください。
SAP DB	詳細は、129 ページの「SAP DB クライアント」を参照してください。
Oracle	詳細は、129 ページの「Oracle クライアント」を参照してください。
IBM DB2 UDB	詳細は、131 ページの「DB2 クライアント」を参照してください。
NNM	詳細は、131 ページの「NNM クライアント」を参照してください。
NDMP	詳細は、131 ページの「NDMP クライアント」を参照してください。

表 2-2 統合ソフトウェアのインストール (続き

アプリケーション	参照先
Microsoft Volume Shadow Copy	詳細は、132 ページの「MS Volume Shadow Copy クライアント」を参照してください。
Lotus Domino Server	詳細は、132 ページの「Lotus Notes/Domino Server クライアント」を参照してください。
EMC Symmetrix	詳細は、132 ページの「EMC Symmetrix 用統合ソフトウェア」を参照してください。
HP StorageWorks XP	詳細は、136 ページの「HP StorageWorks XP 用統合ソフトウェア」を参照してください。
HP StorageWorks Virtual Array	詳細は、143 ページの「HP StorageWorks Virtual Array 用統合ソフトウェア」を参照してください。
HP StorageWorks Enterprise Virtual Array	詳細は、149 ページの「HP StorageWorks Enterprise Virtual Array 用統合ソフトウェア」を参照してください。

表 2-3 その他の対象システム

インストール	参照先
ローカライズされたユーザー インタフェース	詳細は、156 ページの「各国語版 Data Protector ユーザー インタフェースのインストール」を参照してください。
Web Reporting	詳細は、163 ページの「Data Protector Web Reporting のインストール」を参照してください。
MC/ServiceGuard	詳細は、165 ページの「MC/ServiceGuard への Data Protector のインストール」を参照してください。

表 2-3 その他の対象システム (続き)

インストール	参照先
Microsoft Cluster Server	詳細は、167 ページの「Data Protector の Microsoft Cluster Server へのインストール」を参照してください。
Veritas Cluster Server	詳細は、178 ページの「Veritas Cluster への Data Protector クライアントのインストール」を参照してください。
Novell NetWare Cluster	詳細は、179 ページの「Novell NetWare Cluster への Data Protector クライアントのインストール」を参照してください。

Data Protector クライアントのリモート インストール

この項では、インストール サーバを使って Data Protector ソフトウェアをクライアントに配布する手順 (リモート インストールまたはアップグレード手順) を説明します。

前提条件

- インストールの前提条件および推奨事項については、対象となるクライアント システムに応じたインストール手順の説明をお読みください。説明は、46 ページの表 2-1 および 48 ページの表 2-2 に示すとおりです。
- サポートされているプラットフォームと Data Protector コンポーネント、およびディスク スペース要件は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。
- この手順を開始する前に、Cell Manager およびインストール サーバをネットワークにインストールしておく必要があります。

注記

Windows 用のインストール サーバは、ネットワーク上の他のコンピュータからアクセスできるように、共有ディレクトリに格納する必要があります。

Data Protector ユーザー インタフェースを使って、ソフトウェア コンポーネントをクライアントに配布します。プラットフォームが異なるクライアントへのインストールも可能です。

- セキュア シェル インストールを使用するには、クライアントおよびインストール サーバ上に OpenSSH をインストールしてセットアップする必要があります。秘密キーが暗号化されている場合は、インストール サーバ上に keychain をインストールしてセットアップします。詳細な手順は、56 ページの「セキュア シェルによるリモート インストール」を参照してください。

注記

別の Data Protector セル内のクライアントにソフトウェアを配布することはできません。ただし独立したインストール サーバがある場合は、そのインストール サーバを複数のセルにインポートすることも可能です。こうすることで、各セルの Cell Manager に接続された GUI を順番に使用することにより、それぞれのセル内にソフトウェアを配布できます。

セルへのクライアントの追加

Data Protector セルにまだ含まれていないクライアントに Data Protector ソフトウェアを配布するには、以下の手順に従ってください。

1. Data Protector グラフィカル ユーザー インタフェースを起動します。
 - Windows の場合: [スタート] -> [プログラム] -> [HP OpenView Storage Data Protector] -> [Data Protector Manager] を選択します。
 - HP-UX または Solaris の場合: コマンド行に /opt/omni/bin/xomni と入力します。

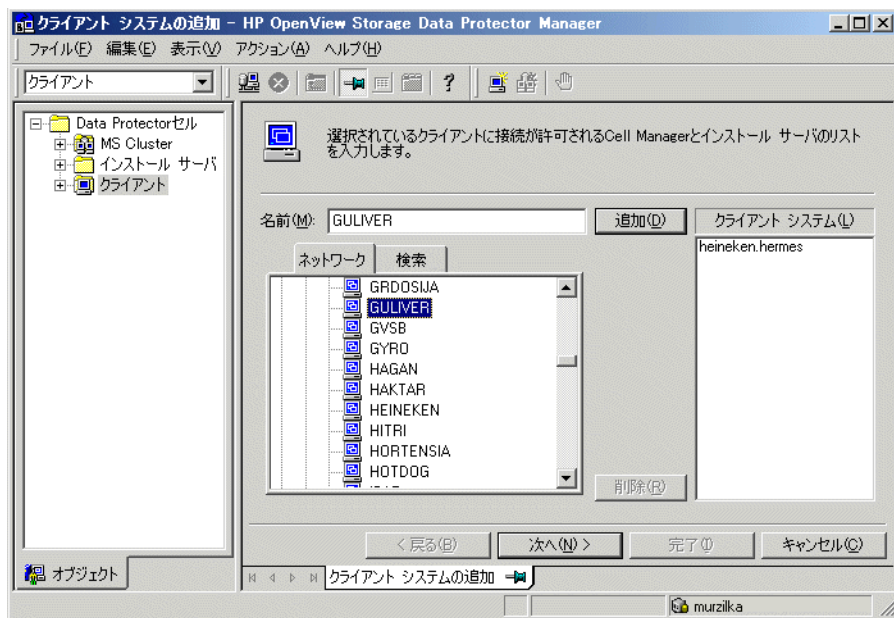
Data Protector グラフィカル ユーザー インタフェースの詳細は、オンライン ヘルプを参照してください。

2. [Data Protector Manager] で、[クライアント] コンテキストを選択します。
3. Scoping ペインの [クライアント] をマウスの右ボタンでクリックし、[クライアントの追加] を選択します。
4. 複数のインストール サーバが構成されている場合は、インストールするクライアントのプラットフォーム (UNIX または Windows) と、クライアントのインストールに使用するインストール サーバを選択します。[次へ] をクリックします。

ネットワークへの Data Protector のインストール Data Protector クライアントのインストール

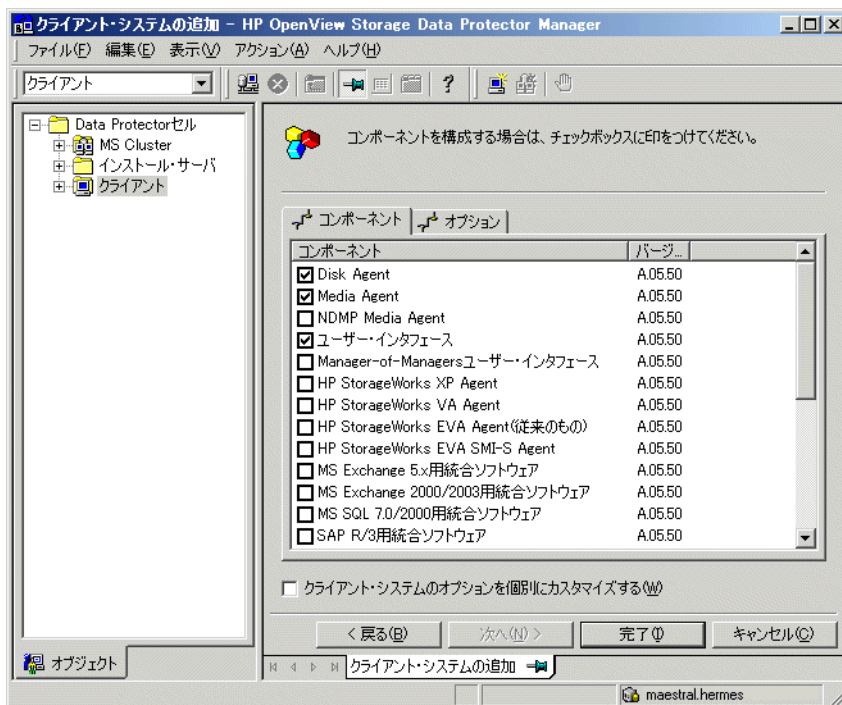
- 図 2-10 に示すように、インストールするクライアントを指定します。クライアントの名前を直接入力できるほか、Windows GUI を使用している場合はクライアントを検索することもできます。[次へ] をクリックします。

図 2-10 クライアントの選択



6. 図 2-11 に示すように、インストールする Data Protector コンポーネントを選択します。なお、Media Agent は 1 種類しか選択できません。詳細は 59 ページの「Data Protector コンポーネント」を参照してください。

図 2-11 コンポーネントの選択



デフォルトのユーザー アカウントとインストール先ディレクトリ (Windows のみ) を変更する場合は、[オプション] をクリックします。

複数のクライアントを選択した後、クライアントごとに異なるコンポーネントをインストールするには、[クライアント システムのオプションを個別にカスタマイズする] をクリックし、[次へ] をクリックします。その後、インストール対象のコンポーネントをクライアントごとに個別に選択します。

[完了] をクリックしてインストールを開始します。

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

7. インストール中にメッセージが表示されたら、目的のクライアントシステムにアクセスするために必要なデータ (ユーザー名、パスワード、および Windows の場合はドメイン) を入力し、[OK] をクリックします。

Data Protector ソフトウェアをインストールしたシステムは、Data Protector セルに追加され、Data Protector クライアントとして動作するようになります。

注記 クライアントシステム上で Data Protector GUI を起動する前に、そのシステムを使用するユーザーを適切な Data Protector ユーザーグループに追加しておいてください。ユーザーグループへの追加手順と選択可能なユーザー権限の詳細は、オンラインヘルプを参照してください。

トラブルシューティング

リモートインストール中に失敗したインストール手順がある場合は、リモートインストールの終了後に GUI 上で [アクション] と [失敗したクライアントを再開] をクリックすると、失敗したインストール手順を再実行できます。それでもインストールが失敗する場合は、319 ページの「インストールのトラブルシューティング」を参照してください。

クライアントへのコンポーネントの追加

既存のクライアントおよび Cell Manager 上に追加の Data Protector ソフトウェアコンポーネントをリモートインストールまたはローカルインストールすることができます。ローカルインストールについては、226 ページの「Data Protector ソフトウェアコンポーネントの変更」を参照してください。

MC/ServiceGuard クライアント

MC/ServiceGuard クラスタ環境では、コンポーネントの追加先のノードがアクティブになっていることを確認してください。

前提条件

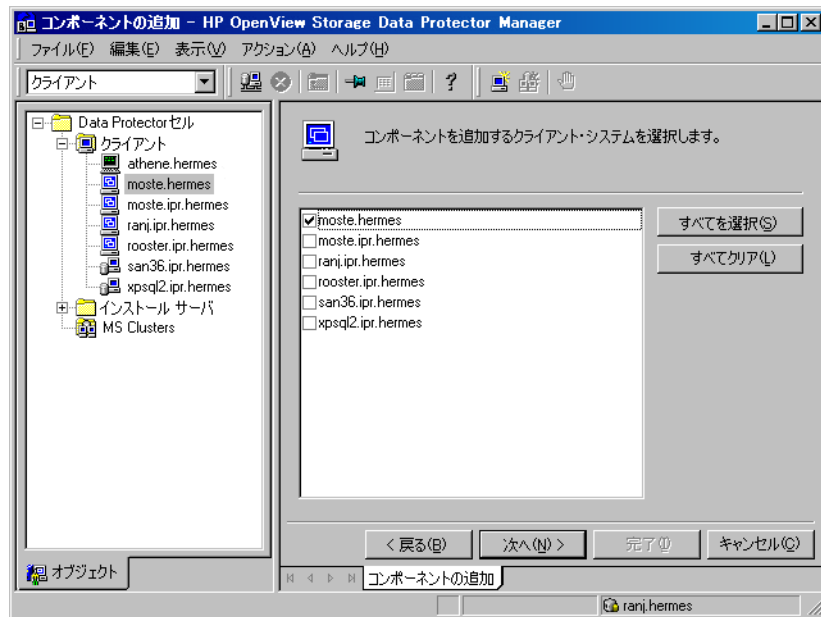
対応するインストールサーバが利用可能であること。

Data Protector セル内のクライアントに Data Protector ソフトウェアを配布するには、以下の手順に従ってください。

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 ペインの [クライアント] を展開し、クライアントを右クリックした後、[コンポーネントの追加] を選択します。
3. 複数のインストール サーバが構成されている場合は、コンポーネントをインストールするクライアントのプラットフォーム (UNIX または Windows) と、コンポーネントのインストールに使用するインストール サーバを選択します。[次へ] をクリックします。
4. 図 2-12 に示すように、インストールするコンポーネントを選択します。[次へ] をクリックします。

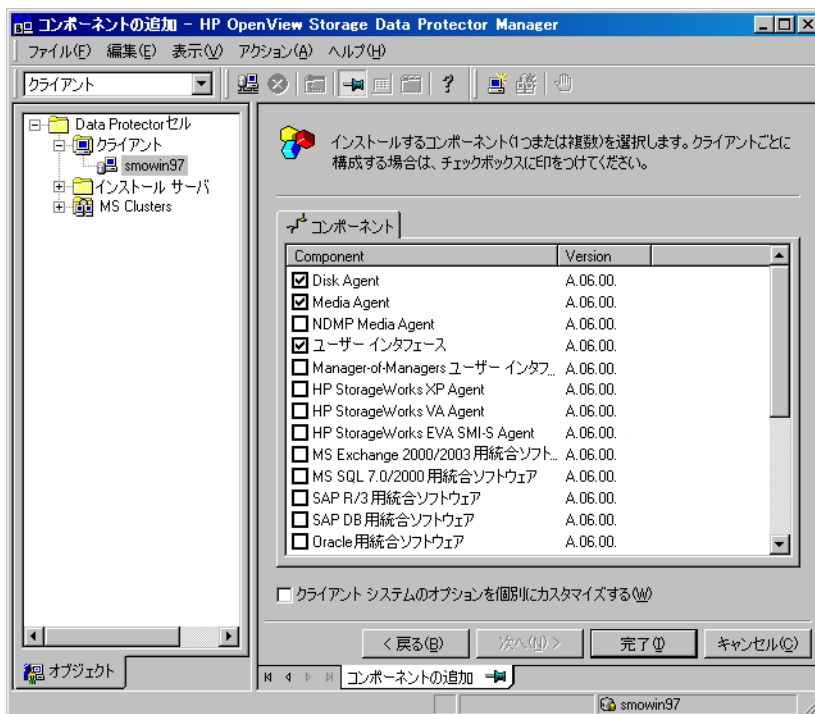
図 2-12 クライアントの選択



ネットワークへの Data Protector のインストール Data Protector クライアントのインストール

5. 図 2-13 に示すように、インストールする Data Protector コンポーネントを選択します。なお、Media Agent は 1 種類しか選択できません。詳細は 59 ページの「Data Protector コンポーネント」を参照してください。

図 2-13 コンポーネントの選択



複数のクライアントを選択した後、クライアントごとに異なるコンポーネントをインストールするには、[クライアント システムのオプションを個別にカスタマイズする]をクリックし、[次へ]をクリックします。その後、コンポーネントをクライアントごとに個別に選択します。

[完了] をクリックしてインストールを開始します。

セキュア シェルによるリモート インストール

セキュア シェル インストールでは、安全な方法で Data Protector コンポーネントがインストールされるため、クライアントとインストール サーバのセキュリティ保護に役立ちます。以下の処理により、高度な保護が実現されます。

- 公開 - 秘密キー ペア メカニズムによって保護された方法で、クライアントにアクセスするインストール サーバのユーザーを認証します。
- インストール パッケージを暗号化してからネットワーク上で転送します。

注記 セキュア シェル インストールは、UNIX プラットフォームでのみサポートされています。

セキュア シェル インストールを使用するには、以下の手順に従って、クライアントおよびインストール サーバ上に OpenSSH をインストールしてセットアップする必要があります。

OpenSSH のセットアップ

OpenSSH は、セキュア シェル プロトコルのオープン ソース実装です。OpenSSH をセットアップするには、以下の手順に従ってください。

1. openssh をシステム上にまだインストールしていない場合、<http://www.openssh.org> からダウンロードし、Data Protector クライアントとインストール サーバの両方にインストールします。HP-UX では、代わりに HP-UX Secure Shell を使用できます。

注記 セキュア シェル インストールのデフォルトのインストール先は、/opt/ssh になります。

2. インストール サーバ上で、ssh-keygen を実行して公開キー ペアを生成します。公開キーはクライアントに転送しますが、秘密キーはインストール サーバ上に維持します。暗号化された (パスフレーズで保護された) 秘密キーを使用する場合は、インストール サーバ上に keychain をセットアップする必要がある点に注意してください。詳細は 58 ページを参照してください。

ssh-keygen の詳細については、<http://www.openbsd.org/cgi-bin/man.cgi?query=ssh-keygen&sektion=1> を参照してください。

3. クライアント上では、\$HOME/.ssh ディレクトリに authorized_keys という名前で公開キーを保存します。

注記 通常、\$HOME/.ssh は、root ユーザーのホーム ディレクトリです。

SSH プロトコルのバージョン (SSH1 または SSH2) を設定するには、以下のファイルを開いて、protocol パラメータの設定を変更します。

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

- a. インストール サーバの場合:

```
<ssh_install_directory>/ssh/etc/ssh_config
```

このファイルは、ssh コマンドにより使用されます。

- b. クライアントの場合:

```
<ssh_install_directory>/ssh/etc/sshd_config
```

このコマンドは、ssh デーモン (sshd) により使用されます。

なお、上記の 2 つのファイルは同期させる必要があります。

注記 SSH プロトコルのデフォルトバージョンは、SSH2 です。

4. クライアント上で、以下のコマンドを実行して ssh デーモンを起動します。

```
<ssh_install_directory>/ssh/sbin/sshd
```

5. 以下のコマンドを実行して、インストールサーバ上の \$HOME/.ssh/known_hosts にある既知のホストのリストにクライアントを追加します。

```
ssh root@<client_host>
```

なお、<client_host> は、次の例のような完全修飾 DNS 名でなければなりません。

```
ssh root@client1.company.com
```

6. インストールサーバ上で、omnirc 変数 OB2_SSH_ENABLED を 1 に設定します。omnirc 変数の詳細は、『HP OpenView Storage Data Protector トラブルシューティングガイド』を参照してください。

keychain のセットアップ

keychain は、パスフレーズを手動で入力しなくても秘密キーを復号化できるようにするツールです。このツールは、秘密キーが暗号化されている場合にのみ必要です。keychain をセットアップするには以下の手順に従ってください。

1. keychain を <http://www.gentoo.org/proj/en/keychain/index.xml> からインストールサーバにダウンロードします。
2. \$HOME/.profile ファイルに以下の 2 行を追加します。

HP-UX、Solaris の場合:

```
<keychain_install_directory>/keychain-<keychain_version>/keychain  
$HOME/.ssh/<private_key>
```

```
. $HOME/.keychain/'hostname'-sh
```

Linux の場合:

```
/usr/bin/keychain $HOME/.ssh/<private_key>
```

```
. $HOME/.keychain/'hostname'-sh
```

3. インストール サーバ上で、omnirc 変数 OB2_ENCRYPT_PVT_KEY を 1 に設定します。omnirc 変数の詳細は、『HP OpenView Storage Data Protector トラブルシューティング ガイド』を参照してください。

この次に行う作業

OpenSSH と keychain のセットアップが終了したら、GUI を使用するか (51 ページの手順を参照)、CLI から ob2install コマンドを実行することにより、クライアントをセルに追加します。CLI コマンドとそのパラメータについては、『HP OpenView Storage Data Protector Command Line Interface Reference』を参照してください。

注記 コマンドの実行に失敗するためセキュア シェル インストールを実行できない場合は、警告が表示されます。ただし、Data Protector の標準リモート インストール方法によりインストールは続行されます。

Data Protector コンポーネント

サポートされているプラットフォームに関する最新情報は、HP OpenView Storage Data Protector ホーム ページ (<http://www.hp.com/support/manuals>) を参照してください。

選択可能な Data Protector コンポーネントとその説明を以下に示します。

ユーザー インタフェース

ユーザー インタフェース コンポーネントは、Data Protector グラフィカル ユーザー インタフェースとコマンド行インタフェースで構成されます。Data Protector Cell Manager にアクセスするには、このコンポーネントが必要です。セルの管理用システムには、このコンポーネントを必ずインストールしなければなりません。

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

注記 複数プラットフォームにわたるバックアップや復元を Data Protector ユーザー インタフェースを使用して実行するよう計画している場合は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照して制限事項を確認してください。

Manager-of-Managers (MoM)

ユーザー インタフェース

Manager-of-Managers (MoM) ユーザー インタフェース コンポーネントは、Data Protector グラフィカル ユーザー インタフェースとコマンド行インタフェースで構成されます。Data Protector の Manager-of-Managers 機能にアクセスしてマルチセル環境を管理するには、このコンポーネントが必要です。

Disk Agent

Disk Agent コンポーネントは、Data Protector によるバックアップの対象となるディスクを持つクライアントにインストールする必要があります。

General Media Agent

General Media Agent は、Data Protector で管理するバックアップ デバイスに接続されているクライアントか、Data Protector で管理するライブラリ ロボティクスにアクセス可能なクライアントにインストールする必要があります。

自動障害復旧モジュール

障害復旧の準備を自動実行するには、自動障害復旧で復旧したいクライアント、および拡張障害復旧用の DR CD ISO イメージを準備するシステムに、自動障害復旧モジュール コンポーネントをインストールする必要があります。

SAP R/3 用統合ソフトウェア

SAP R/3 用統合ソフトウェア コンポーネントは、Data Protector によるバックアップの対象となる SAP R/3 データベースがあるクライアントにインストールする必要があります。

SAP DB 用統合ソフトウェア

SAP DB 用統合ソフトウェア コンポーネントは、Data Protector によるバックアップの対象となる SAP DB データベースがあるクライアントにインストールする必要があります。

Oracle 用統合ソフトウェア

Oracle 用統合ソフトウェア コンポーネントは、Data Protector によるバックアップの対象となる Oracle データベースがあるクライアントにインストールする必要があります。

DB2 用統合ソフトウェア	DB2 用統合ソフトウェア コンポーネントは、Data Protector によるバックアップの対象となる DB2 Server があるクライアントすべてにインストールする必要があります。
Sybase 用統合ソフトウェア	Sybase 用統合ソフトウェア コンポーネントは、Data Protector によるバックアップの対象となる Sybase データベースがあるクライアントにインストールする必要があります。
Informix 用統合ソフトウェア	Informix 用統合ソフトウェア コンポーネントは、Data Protector によるバックアップの対象となる Informix Server データベースがあるクライアントにインストールする必要があります。
MS Exchange 2000/2003 用統合ソフトウェア	MS Exchange 2000/2003 用統合ソフトウェア コンポーネントは、Data Protector によるバックアップの対象となる Microsoft Exchange Server データベースがあるクライアントにインストールする必要があります。
MS SQL 7.0/2000 用統合ソフトウェア	SQL 7.0/2000 用統合ソフトウェア コンポーネントは、Data Protector によるバックアップの対象となる MS SQL データベースがあるシステムにインストールする必要があります。
MS Volume Shadow Copy 用統合ソフトウェア	MS Volume Shadow Copy 用統合ソフトウェア コンポーネントは、Volume Shadow Copy サービスによるバックアップを実行する Windows Server 2003 システムにインストールする必要があります。
EMC Symmetrix Agent	EMC Symmetrix Agent コンポーネントは、EMC Symmetrix を Data Protector と統合する場合に、アプリケーションシステムとバックアップシステムにインストールする必要があります。
HP StorageWorks XP Agent	HPStorageWorks XP Agent コンポーネントは、HP StorageWorksXP を Data Protector と統合する場合に、アプリケーションシステムとバックアップシステムにインストールする必要があります。

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

HP StorageWorks VA Agent	HPStorageWorks VA Agent コンポーネントは、HP StorageWorksVirtual Array を Data Protector と統合する場合に、アプリケーション システムとバックアップ システムにインストールする必要があります。
HP StorageWorks EVA SMI-S Agent	HP StorageWorks EVA SMI-S Agent コンポーネントは、HP StorageWorks Enterprise Virtual Array を Data Protector と統合する場合に、アプリケーション システムとバックアップ システムにインストールする必要があります。
Cluster Server	Cluster Server 用コンポーネントは、Data Protector のクラスター対応クライアントすべてにインストールする必要があります。
HP OpenView NNM バックアップ用統合ソフトウェア	NNM 用統合ソフトウェア コンポーネントは、セル内で Data Protector によるバックアップの対象となる NNM データベースがあるすべてのクライアントにインストールする必要があります。
NDMP Media Agent	NDMP Media Agent コンポーネントは、NDMP サーバを介して NDMP 専用ドライブにデータをバックアップしているすべてのクライアントにインストールする必要があります。
Lotus 用統合ソフトウェア	Lotus 用統合ソフトウェア コンポーネントは、セル内で Data Protector によるバックアップの対象となる Lotus Notes/Domino Server データベースがあるすべてのクライアントにインストールする必要があります。
フランス語のサポート	フランス語のサポート コンポーネントは、Data Protector ユーザー インタフェースをフランス語で使用するクライアントにインストールする必要があります。
日本語のサポート	日本語のサポート コンポーネントは、Data Protector ユーザー インタフェースを日本語で使用するクライアントにインストールする必要があります。

注記

General Media Agent と NDMP Media Agent を同じクライアントにインストールすることはできません。

Windows 用クライアントのインストール

各 Windows オペレーティング システムでサポートされているプラットフォームとコンポーネントの詳細は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。

前提条件

Windows クライアントをインストールするには、Administrator のアカウントが必要です。Data Protector クライアント システムとして使用する Windows システムは、以下の条件を満たしている必要があります。

- ✓ Microsoft Internet Explorer 5.0 以上がインストールされていること。
- ✓ Data Protector クライアント ソフトウェアをインストールするのに十分な容量の空きディスクスペースがあること。詳細は『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。
- ✓ ポート番号 5555 (デフォルト) が利用可能であること。
- ✓ Microsoft 社の TCP/IP プロトコルがインストールされており、実行されていること。このプロトコルを使って、ホスト名を解決できること。コンピュータの名前とホスト名は同じでなければなりません。TCP/IP プロトコルのインストールおよび構成については、B-19 ページの「Windows システム上の TCP/IP プロトコルのセットアップ」を参照してください。

制限事項

- Windows オペレーティング システムのセキュリティ規制により、インストール サーバを使用してクライアントをリモートにインストールできるのは、同一ドメイン内に限られます。
- Windows Me/XP HE では、Data Protector クライアントはローカルにのみインストールできます。

推奨事項

Data Protector A.06.00 のインストールを開始するにあたって、各 Windows クライアント上に Microsoft Installer (MSI) 2.0 がインストールされていることを確認してください。MSI のバージョンが古い場合は、Data Protector セットアップ プログラムにより、自動的にバージョン 2.0 にアップグレードされます。この場合、Data Protector によって、アップグレードの最後の段階で MSI がアップグレードされたことが通知されます。MSI がアップグレードされた場合は、システムを再起動することを強く推奨します。個々の Windows オペレーティング システムに対する Microsoft Installer 2.0 の前提条件については、Microsoft Support にお問い合わせください。

ネットワークへの Data Protector のインストール Data Protector クライアントのインストール

MSI の古いバージョンで Data Protector のインストールを開始した場合は、Data Protector セットアッププログラムにより、自動的にバージョン 2.0 にアップグレードされます。ただし、アップグレードを有効にするには、システムを再ブートする必要があります。システムの再ブートが完了したら、インストールを初めからやり直してください。

自動障害復旧モジュール

障害復旧の準備を自動実行するには、自動障害復旧で復旧したいクライアント、および拡張障害復旧用の DR CD ISO イメージを準備するシステムに、自動障害復旧コンポーネントをインストールする必要があります。

クラスタ対応クライアント

クラスタ対応クライアントをインストールする場合は、上記以外にも必要となる前提条件があります。175 ページの「クラスタ対応クライアントのインストール」を参照してください。

インストール手順を開始する前に、どのコンポーネントをクライアントシステムにインストールするかを決定しておいてください。Data Protector ソフトウェア コンポーネントのリストと説明は、59 ページの「Data Protector コンポーネント」を参照してください。

ローカル インストール

Windows クライアントは、Windows インストール DVD-ROM からローカルにインストールすることができます。以下の手順に従ってください。

1. DVD-ROM をドライブに挿入し、以下のコマンドを実行します。

32 ビット プロセッサの場合: %Windows_other%i386%setup.exe

AMD-64/Intel EM64T プロセッサの場合: %Windows_other%x8664%setup.exe

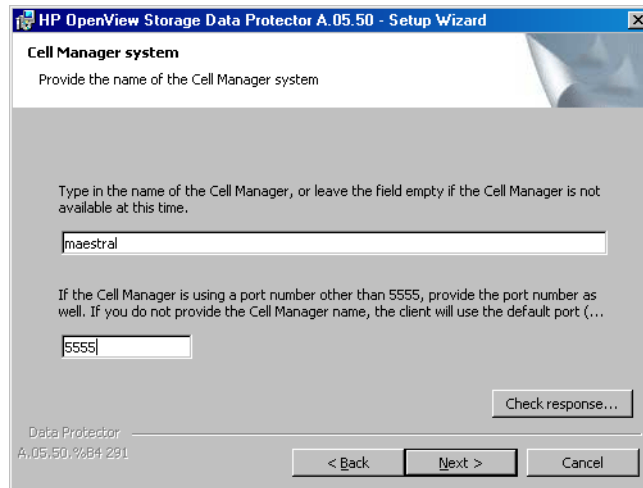
Itanium プロセッサの場合: %Windows_other%ia64%setup.exe

2. [Installatoin Type] ページで、[Client] を選択します。Itanium クライアントの場合は、自動的にタイプが選択されます。
3. Cell Manager の名前を入力します。詳細は図 2-14 を参照してください。

Cell Manager でデフォルト ポート番号 5555 以外の番号を使用する場合は、ポート番号を変更します。[Check response...] をクリックすると、Cell Manager がアクティブかどうかと、選択したポート番号が使用されているかどうかをテストできます。

[Next] をクリックします。

図 2-14 Cell Manager の選択



4. Data Protector をデフォルト フォルダにインストールする場合には、[Next] をクリックします。

デフォルト以外のフォルダにインストールする場合には、[Change] をクリックし、[Change Current Destination Folder] ページを開いて、パスを入力します。

5. インストール対象の Data Protector コンポーネントを選択します。

その他の Data Protector コンポーネントの詳細は、59 ページの「Data Protector コンポーネント」を参照してください。

[Next] をクリックします。

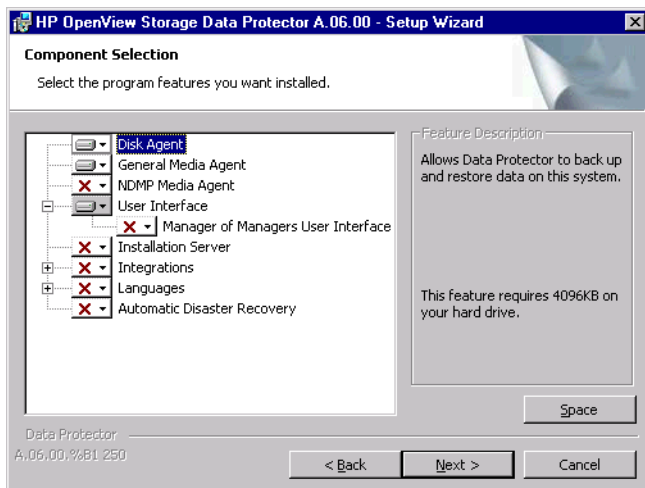
6. **Windows XP SP2、Windows 2003 SP1 の場合**:Data Protector によってシステムにファイアウォールが検出されると、[Windows Firewall configuration] ページが表示されます。Data Protector のセットアッププログラムによって、必要なすべての Data Protector 実行可能ファイルが登録されます。デフォルトでは、[Initially, enable newly registered Data Protector binaries to open ports as needed] オプションが選択されています。この時点で、Data Protector によってポートがオープンされないようにするには、オプションを選択解除します。ただし、Data Protector を適切に機能させるには、実行可能ファイルを有効にする必要があります。

ネットワークへの Data Protector のインストール Data Protector クライアントのインストール

[Next] をクリックします。

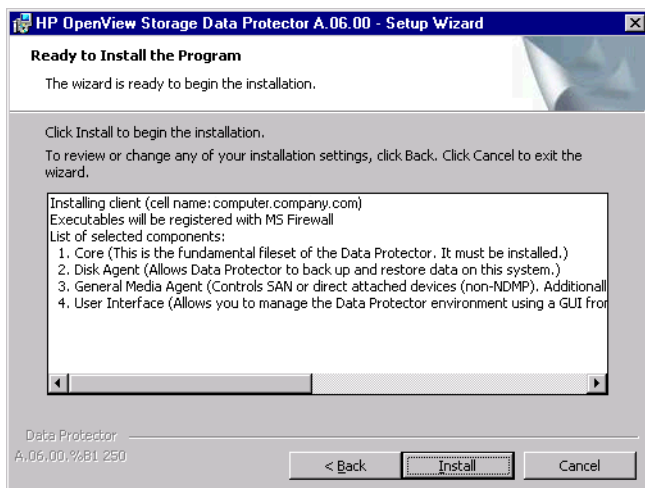
7. 選択したコンポーネントのサマリー ページが表示されます。 [Install] をクリックして、選択したコンポーネントをインストールします。

図 2-15 コンポーネント選択サマリー ページ



8. [Installation status] ページが表示されます。 [Next] をクリックします。

図 2-16 インストールのサマリー ページ



9. セットアップ後すぐに Data Protector を起動するには、[Start Data Protector Manager GUI] を選択します。

『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス』を表示するには、[Open the Product Announcements] を選択します。

[Finish] をクリックします。

Windows システムへのバックアップ デバイスの接続

Media Agent コンポーネントのインストール後は、バックアップ デバイスを Windows システムに接続できます。以下の手順に従ってください。

1. 利用可能な SCSI アドレスを確認し、接続するバックアップ デバイスのドライブおよび制御デバイス (ロボティクス) に割り当てる SCSI アドレスを決定します (なお Windows 上では、SCSI アドレスのことを *SCSI ターゲット ID* と呼びます)。詳細は B-54 ページの「Windows システム上の未使用の SCSI ターゲット ID の取得」を参照してください。
2. まだ使用されていない SCSI **ターゲット ID** を、ドライブおよび制御デバイス (ロボティクス) に割り当てます。デバイスの種類にもよりますが、通常はターゲット ID をデバイス上のスイッチで設定できます。詳細は、使用するデバイスのマニュアルを参照してください。サポート対象デバイスの詳細は、<http://www.hp.com/support/manuals> も参照してください。
3. コンピュータの電源を切り、バックアップ デバイスを本体に接続します。
4. デバイスとコンピュータの電源を順に投入し、ブート処理が完了するまで待ちます。
5. 新しいバックアップ デバイスがシステムによって正しく認識されていることを確認します。
<Data_Protector_home>%bin ディレクトリから devbra -dev コマンドを実行してください。

画面に表示されたリストに新しいデバイスが含まれていることを確認します。devbra -dev コマンドの出力例を以下に示します。

- 使用しているデバイスのテープドライバがロードされている場合。

```
HP:C1533A
tape3:0:4:0
DDS
...
```

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

1 行目はデバイスの仕様を表し、2 行目はデバイス ファイル名を示します。

この例の場合、ドライブ インスタンス番号 3 の HP DDS テープ デバイスが SCSI バス 0 に接続されており、SCSI ターゲット ID 4 および LUN 番号 0 が割り当てられています。

- 使用しているデバイスのテープ ドライバがロードされていない場合。

```
HP:C1533A  
  
scsi1:0:4:0  
  
DDS  
  
...
```

1 行目はデバイスの仕様を表し、2 行目はデバイス ファイル名を示します。

この例の場合、HP DDS テープ デバイスが SCSI バス 0 上の SCSI ポート 1 に接続されており、テープ ドライブに SCSI ターゲット ID 4 および LUN 番号 0 が割り当てられています。

デバイスのネイティブ テープ ドライバをロードまたはアンロードする方法は、B-32 ページの「Windows でのテープ ドライバおよびロボティクス ドライバの使用」を参照してください。デバイス ファイル名の作成方法は、B-35 ページの「Windows 上でのデバイス ファイル (SCSI アドレス) の作成」を参照してください。

この次に行う作業

クライアント コンポーネントをインストールし、バックアップ デバイスを接続したら、バックアップ デバイスおよびメディア プールを構成します。構成作業の詳細は、オンライン ヘルプの索引キーワード「構成, バックアップ デバイス」で表示される内容を参照してください。

HP-UX クライアントのインストール

HP-UX クライアントは、HP-UX 用インストール DVD-ROM を使ってローカルにインストールすることも、UNIX 用のインストール サーバを使ってリモートでインストールすることもできます。

インストール手順を開始する前に、どのコンポーネントをクライアント システムにインストールするかを決定しておいてください。Data Protector ソフトウェア コンポーネントのリストと説明は、59 ページの「Data Protector コンポーネント」を参照してください。

前提条件

- システム要件、ディスクスペース要件、サポートされているプラットフォーム、プロセッサと Data Protector コンポーネントについては、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。
- この時点で、Cell Manager および UNIX 用のインストール サーバをネットワーク上にインストールしておく必要があります。まだインストールしていない場合は、19 ページの「Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール」の説明にしたがってインストールしてください。
- HP-UX クライアントをインストールするには、*root* ユーザーによるアクセスか、または *root* 権限付きのアカウントが必要です。

ローカル インストール

お使いの環境に UNIX 用のインストール サーバがない場合は、UNIX 用のインストール DVD-ROM を使用して、ローカル インストールを行う必要があります。詳細は 119 ページの「UNIX クライアントのローカル インストール」を参照してください。

ローカル インストール後には、クライアント システムをセルに手作業でインポートする必要があります。詳細は、185 ページの「セルへのクライアントのインポート」を参照してください。

リモート インストール

UNIX クライアント ソフトウェアは、Data Protector グラフィカル ユーザー インタフェースを使って UNIX 用のインストール サーバからリモートにインストールできます。ソフトウェアのリモート インストール手順は、50 ページの「Data Protector クライアントのリモート インストール」を参照してください。

リモート インストールが終了すると、クライアント システムは自動的に Data Protector セルのメンバーになります。

クライアントに Media Agent をインストールしたら、バックアップ デバイスをシステムに物理的に接続しなければなりません。また、デバイスの種類に応じた適切なデバイスドライバがカーネルに組み込まれているかどうかを確認するため、バックアップの実行前にカーネルの構成をチェックしておかなければなりません。

クラスタ対応クライアント

クラスタ対応クライアントをインストールする場合は、上記以外にも必要となる前提条件があります。166 ページの「クラスタ対応クライアントのインストール」を参照してください。

ネットワークへの Data Protector のインストール Data Protector クライアントのインストール

HP-UX のカーネル構成のチェック

HP System Administration Manager (SAM) ユーティリティを使って、HP-UX 11.x 上のカーネルの構成をチェックおよびビルドするには、以下の手順に従ってください。なお、カーネルを手作業でビルドする手順は、B-37 ページの「HP-UX 上の SCSI ロボティクス構成」を参照してください。

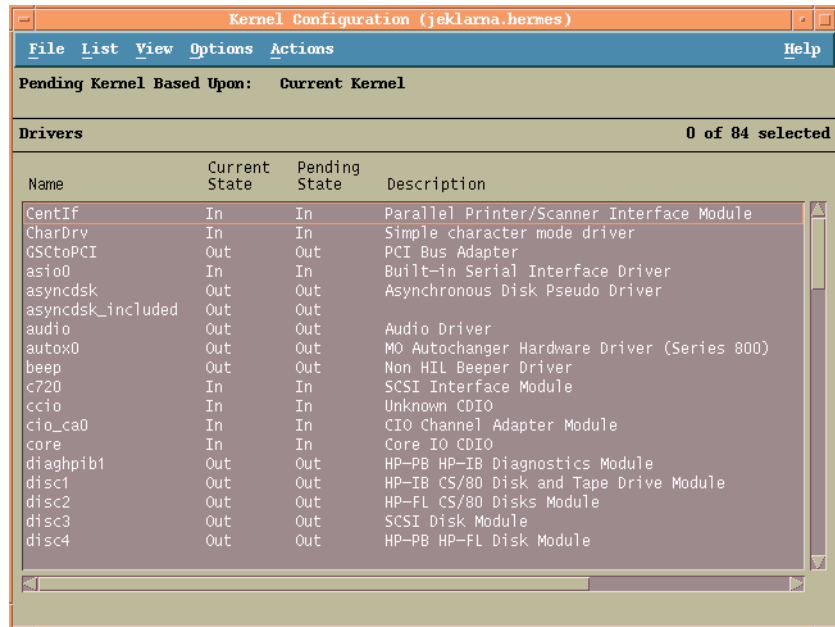
HP System Administration Manager (SAM) ユーティリティを使ってカーネルをビルドするには、以下の手順に従ってください。

1. root ユーザーとしてログインし、端末を開いて sam と入力します。
2. [System Administration Manager] ウィンドウで [Kernel Configuration] と [Drivers] を順にダブルクリックします。
3. [Kernel Configuration] ウィンドウで、以下の条件が満たされていることを確認します。
 - ✓ 使用するデバイスのドライバがインストール済みドライバのリストに含まれていること。図 2-17 を参照してください。目的のドライバがリストに含まれていない場合は、/usr/sbin/swinstall ユーティリティを使ってインストールする必要があります。以下に例を示します。
 - テープ デバイスにはテープ デバイスドライバが必要です。システムにテープ デバイスを接続する場合は、適切なテープ デバイスドライバがインストールされていることを確認してください。たとえば stape ドライバは DLT や LTO などの汎用的な SCSI テープドライブで使用され、tape2 ドライバは DDS デバイスで使用されます。

HP-UX 11.00 システムに Quantum DLT 4000 を接続している場合は、stape ドライバではなく tape2 の使用をお勧めします。
 - テープ ライブラリ デバイスのロボティクスを制御するには、使用するハードウェアに応じて、SCSI パススルードライバ (sctl または spt) か、オートチェンジャロボティクスドライバ (schgr) が必要です。

詳細は B-37 ページの「HP-UX 上の SCSI ロボティクス構成」を参照してください。

図 2-17 [Kernel Configuration] ウィンドウ



✓ Current State 列でドライバのステータスが In に設定されていることを確認します。ステータスが Out に設定されている場合は、以下の操作を行ってください。

- リスト内のドライバを選択します。[Actions] をクリックして [Add Driver to Kernel] を選択します。Pending State 列のステータスが In に変化したことを確認します。

これを、Current State 列が Out に設定されている各ドライバに対して繰り返します。

- [Actions] をクリックして [Create a New Kernel] を選択し、変更内容を確定します。これにより、Pending Kernel のラベルが Current Kernel に変化します。ただし、システムを再起動する必要があります。

必要なドライバをカーネルに組み込んだら、以下の手順に従って、バックアップ デバイスをコンピュータに接続してください。

ネットワークへの Data Protector のインストール Data Protector クライアントのインストール

HP-UX システムへのバックアップ デバイスの接続

1. ドライブおよび制御デバイス (ロボティクス) に割り当てる SCSI アドレスを決定します。システム コマンドの `/usr/sbin/ioscan -f` を使います。

詳細は B-46 ページの「HP-UX 上の未使用の SCSI アドレスの取得」を参照してください。

2. デバイスの SCSI アドレスを設定します。デバイスの種類にもよりますが、通常は SCSI アドレスをデバイス上のスイッチで設定できます。詳細は、使用するデバイスのマニュアルを参照してください。

サポート対象デバイスの詳細は、<http://www.hp.com/support/manuals> を参照してください。

3. デバイスをコンピュータに接続し、デバイスとコンピュータの電源を順に投入します。ブート処理が完了するまで待ちます。通常、デバイス ファイルは、ブート処理中に生成されます。
4. 新しいバックアップ デバイスがシステムによって正しく認識されていることを確認します。`ioscan` ユーティリティを以下のコマンドで実行してください。

```
/usr/sbin/ioscan -fn
```

このコマンドを実行すると、接続されている各バックアップ デバイスに対するデバイス ファイルのリストが表示されます。デバイス ファイルがブート時に自動生成されない場合は、手作業でデバイス ファイルを作成する必要があります。詳細は B-42 ページの「HP-UX 上のデバイス ファイルの作成」を参照してください。

インストールを完了し、バックアップ デバイスをシステムに適切に接続したら、バックアップ デバイスやメディア プールなど、Data Protector の運用に必要な要素を構成します。詳細は、オンライン ヘルプの索引キーワード「構成、バックアップ デバイス」で表示される内容を参照してください。

Solaris 用クライアントのインストール

Solaris クライアントは、UNIX 用インストール DVD-ROM を使ってローカルにインストールすることも、UNIX 用のインストール サーバを使ってリモート インストールすることもできます。

インストール手順を開始する前に、どのコンポーネントをクライアント システムにインストールするかを決定しておいてください。Data Protector ソフトウェア コンポーネントのリストと説明は、59 ページの「Data Protector コンポーネント」を参照してください。

前提条件

- システム要件、ディスク スペース要件、サポートされているプラットフォームと Data Protector コンポーネントについては、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。
- この時点で、Cell Manager および UNIX 用のインストール サーバをネットワーク上にインストールしておく必要があります。詳細は 19 ページの「Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール」を参照してください。
- Solaris クライアントをインストールするには、*root* ユーザーによるアクセスか、または *root* 権限付きのアカウントが必要です。

ローカル インストール

お使いの環境に UNIX 用のインストール サーバがない場合は、UNIX 用のインストール DVD-ROM を使用して、ローカル インストールを行う必要があります。詳細は 119 ページの「UNIX クライアントのローカル インストール」を参照してください。

リモート インストール

UNIX クライアント ソフトウェアは、Data Protector グラフィカル ユーザー インタフェースを使って UNIX 用のインストール サーバからリモートにインストールできます。ソフトウェアのリモート インストール手順は、50 ページの「Data Protector クライアントのリモート インストール」を参照してください。

注記

ユーザー インタフェース コンポーネント (グラフィカル ユーザー インタフェースとコマンド行インタフェースが含まれる) を使用する場合は、事前に環境変数を更新する必要があります。詳細は 27 ページの「環境変数の設定」を参照してください。

Solaris 2.6 クライアントにユーザー インタフェースをインストールした場合、コマンド行インタフェースのみを使用できます。

クライアント コンポーネントのインストールが完了したターゲット システムは、自動的に Data Protector セルに追加されます。

重要

Data Protector は、たとえば次のようなリンク ディレクトリにインストールすることができます。

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

```
/opt/omni/ -> /<prefix>/opt/omni/  
/etc/opt/omni/ -> /<prefix>/etc/opt/omni/  
/var/opt/omni/ -> /<prefix>/var/opt/omni/
```

このようにする場合は、インストール前にリンクを作成しておき、インストール先ディレクトリが存在することを確認しておかなければなりません。

クラスタ対応クライアント

クラスタ対応クライアントをインストールする場合は、上記以外にも必要となる前提条件があります。178 ページの「クライアントのインストール」を参照してください。

インストール後の構成作業

構成ファイル

クライアントシステムに Media Agent コンポーネントをインストールした後は、使用するデバイスの種類に応じて、構成ファイル (/kernel/drv/st.conf) の内容をチェックする必要があります。

- Exabyte デバイス (8 mm) を使用する場合は、/kernel/drv/st.conf ファイルの内容を変更する必要はありません。
- HP DAT デバイス (4 mm) を使用する場合は、/kernel/drv/st.conf ファイルに以下の行を追加してください。

```
tape-config-list =  
"HP      HP35470A", "HP DDS 4mm DAT", "HP-data1",  
"HP      HP35480A", "HP DDS-DC 4mm DAT", "HP-data1",  
"HP      C1533A", "HP DDS2 4mm DAT", "HP-data2",  
"HP      C1537A", "HP DDS3 4mm DAT", "HP-data3",  
"HP      C1553A", "HP DDS2 4mm DATloader", "HP-data2",  
"HP      C1557A", "HP DDS3 4mm DATloader", "HP-data3";  
HP-data1 = 1,0x34,0,0x8019,3,0x00,0x13,0x03,2;  
HP-data2 = 1,0x34,0,0x8239,4,0x0,0x13,0x24,0x3,3;  
HP-data3 = 1,0x34,0,0x8239,4,0x0,0x13,0x24,0x3,3;
```

重要

これらの HP データ エントリは、HP のサポートで通常推奨しているデフォルト エントリとは異なっています。これらの行は必ず上に示したとおり記述してください。記述に誤りがあると、そのドライブを Data Protector で使用できなくなります。

- DLT、DLT1、SuperDLT、LTO1、LTO2、および STK9840 デバイスを使用する場合は、
/kernel/drv/st.conf ファイルに以下の行を追加してください。

```
tape-config-list=  
  
"HP      Ultrium 1-SCSI", "HP Ultrium 1-SCSI", "LTO-data",  
"HP      Ultrium 2-SCSI", "HP_LTO",      "HP-LTO2",  
"DEC DLT2000", "Digital DLT2000",      "DLT2k-data",  
"Quantum DLT4000", "Quantum DLT4000", "DLT4k-data",  
"QUANTUM DLT7000", "Quantum DLT7000", "DLT7k-data",  
"QUANTUM DLT8000", "Quantum DLT8000",      "DLT8k-data",  
"HP C9264CB-VS80", "HP DLT vs80 DLTloader", "HP_data1"  
"QUANTUM SuperDLT1", "QUANTUM SuperDLT", "SDLT-data",  
"TANDBERGSuperDLT1", "TANDBERG SuperDLT", "SDL-data",  
"STK      9840", "STK 9840",      "CLASS_9840";  
  
DLT2k-data = 1,0x38,0,0x8639,4,0x17,0x18,0x80,0x81,3;  
DLT4k-data = 1,0x38,0,0x8639,4,0x17,0x18,0x80,0x81,3;  
DLT7k-data = 1,0x38,0,0x8639,4,0x82,0x83,0x84,0x85,3;  
DLT8k-data = 1,0x77,0,0x1D639,4,0x84,0x85,0x88,0x89,3;  
HP_data1 = 1,0x3a,0,0x8639,4,0x40,0x86,0x87,0x7f,0;  
LTO-data = 1,0x7a,0,0x1d679,4,0x00,0x00,0x00,0x40,3;  
HP-LTO2 = 1,0x7a,0,0xd639,4,0x00,0x00,0x00,0x42,3;  
SDLT-data = 1,0x79,0,0x8639,4,0x90,0x91,0x90,0x91,3;  
CLASS_9840 = 1,0x78,0,0x1d679,1,0x00,0;
```

- HP StorageWorks 12000e (48AL) オートローダー (HP C1553A) を使用する場合は、
/kernel/drv/st.conf ファイル内の HP データ エントリに加えて、以下のエントリを追加
してください。

```
name="st" class="scsi"  
target=<ID> lun=0;  
name="st" class="scsi"  
target=<ID> lun=1;
```

<ID>の箇所にオートローダーの SCSI アドレスを指定し、オートローダーのオプション番号
スイッチを 5 に設定します (このスイッチは、デバイスの背面パネルにあります)。さらに、
デバイスの DIP スイッチの設定を 11111001 に変更します (これらのスイッチは、オート
ローダーの底面から操作できます)。

注記

HP StorageWorks 12000e ライブラリには、ピッカー デバイス専用の SCSI ID はあ
りませんが、同じ SCSI ID からデータドライブアクセス コマンドとピッカー コ
マンドの両方を受け付けるようになっていました。ただし、データドライブアクセ
ス コマンドは SCSI lun=0 にリダイレクトし、ピッカー コマンドは SCSI lun=1 に
リダイレクトする必要があります。

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

他のすべてのデバイスについて、`st.conf` ファイルに必要なエントリがあるかどうか、`st.conf.template` テンプレート ファイル (`/opt/omni/spt` にあります) をチェックします。これは単なるテンプレート ファイルであり、`st.conf` ファイルの代用となるものではありません。

- Solaris 上で SCSI パススルードライバとともに SCSI エクスチェンジャ デバイスを使用する場合は、SCSI パススルードライバをまず最初にインストールしてから、SCSI デバイスをインストールする必要があります。

SCSI パススルードライバをインストールするには、以下の手順に従ってください。

1. `sst` モジュールを `/usr/kernel/drv/sparcv9` ディレクトリにコピーし、構成ファイル `sst.conf` を `/usr/kernel/drv` ディレクトリにコピーします。以下のコマンドを実行してください。

32 ビット版 Solaris の場合:

```
$cp /opt/omni/spt/sst /usr/kernel/drv/sst
$cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
```

64 ビット版 Solaris の場合:

```
$cp /opt/omni/spt/sst.64bit /usr/kernel/drv/sparcv9
/sst
$cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
```

2. `/etc/devlink.tab` ファイルに以下の行を追加します。

重要	<code>/etc/devlink.tab</code> ファイルの編集には、スペース文字を使用しないでください。タブ文字のみを使用してください。
-----------	--

```
“type=ddi_pseudo;name=sst;minor=character rsst¥A1”
```

この行を追加すると、`devlinks(1M)` によって、`/dev/rsstX` (`X` は SCSI ターゲット番号) 形式の名前のデバイスへのリンクが生成されます。

3. 以下のコマンドを入力して、システムにドライバをインストールします。

```
add_drv sst
```

4. ここまでの段階で、SCSI デバイスをインストールする準備は完了です。インストールを開始する前に、各ドライブおよびエクスチェンジャ デバイスのロボティクス (ピッカー) に正しい SCSI アドレスを割り当てておく必要があります。選択するアドレスは、システム上の他のデバイスに使用されていないものでなければなりません。

SCSI 構成をチェックするには、最初に以下のコマンドを入力してシステムをシャットダウンします。

```
shutdown -i0
```

次に ok プロンプトから probe-scsi-all コマンドを実行して、割り当て済みのアドレスをチェックします。

```
ok probe-scsi-all
```

チェックが完了したら、以下のコマンドでシステムを再起動します。

```
ok boot -r
```

SCSI デバイスをインストールするには、以下の手順に従ってください。

- a. /kernel/drv/st.conf を編集し、割り当てた SCSI ポートを使用するようにデバイスのドライブ パラメータを構成します。詳細は、デバイスのマニュアルを参照してください。

なお、ここでは、SCSI ポート 5 を SCSI ドライブに割り当て、SCSI ポート 4 を ADIC SCSI 制御デバイス (ピッカー) に割り当てて、ADIC-VLS DLT デバイスをセットアップする場合を想定しています。

例 :

```
tape-config-list = "DEC      DLT2000", "ADIC DLTDlib", "ADIC2000-data";  
ADIC2000-data = 1,0x38,0,0x8639,4,0x17,0x18,0x80,0x81,3;name="st" class=  
"scsi"  
target=5 lun=0;  
name="st" class= "scsi"  
target=4 lun=0;
```

上の例に示したデータを /kernel/drv/st.conf ファイルに追加します。

- b. /usr/kernel/drv/sst.conf ファイルを編集して、割り当てた SCSI ポート 4 を使用するように ADIC SCSI 制御デバイスをセットアップします。ADIC ドライブに関して以下のデータを /usr/kernel/drv/sst.conf ファイルに追加します。

```
name="sst" class= "scsi"  
target=4 lun=0;
```

/kernel/drv/st.conf ファイルおよび /usr/kernel/drv/sst.conf ファイルを変更し終えたら、システムにバックアップ デバイスを接続する準備が完了したことになります。

Solaris システムへのバックアップ デバイスの接続

Solaris システムにバックアップ デバイスを接続するには、以下の手順に従ってください。

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

1. reconfigure ファイルを作成します。

```
touch /reconfigure
```

2. 次に、`$shutdown -i0` コマンドを入力してシステムをシャットダウンし、コンピュータの電源を切ってから、デバイスを SCSI バスに物理的に接続します。選択した SCSI アドレスが他のデバイスに使用されていないことをチェックしてください。

サポート対象デバイスの詳細は、<http://www.hp.com/support/manuals> を参照してください。

注記

Data Protector は、Solaris システム上ではクリーニング テープを自動認識しません。StorageWorks 12000e (48AL) デバイスで使用されているクリーニング テープを Data Protector が検出して挿入した場合は、テープドライバは、未定義の状態となり、システムの再ブートが必要になります。Data Protector がクリーニング テープのロード要求を出した場合は、手作業でロードしてください。

3. コンピュータの電源を投入し、ブート処理の途中で Stop-A キーを押して、ブート処理を中断させます。ok プロンプトにコマンドを `probe-scsi-all` と入力して、新しいデバイスが正しく認識されているかどうかを確認します。

```
ok > probe-scsi-all
```

次に

```
ok > go
```

と入力して操作を続行します。

4. この時点で、デバイスが正しく動作していることを確認します。ドライブのデバイス ファイルは `/dev/rmt` ディレクトリに格納する必要があり、SCSI 制御デバイス (ピッカー) のデバイス ファイルは `/dev` ディレクトリに格納する必要があります。

注記

Solaris システム上では (特に 64 ビット版 Solaris の場合は)、SCSI 制御デバイス (ピッカー) へのリンクが自動的に生成されないことがあります。この場合はシンボリック リンクを作成してください。以下に例を示します。

```
ln -s /devices/pci@1f,4000/scsi@3,1/sst@4,1:character  
/dev/rsst4
```

デバイスの動作は、Data Protector の uma ユーティリティで確認できます。前に例示した SCSI エクスチェンジャ デバイス (SCSI ポート 4 を使用) のピッカーの動作をチェックするには、以下のように入力します。

```
echo "inq" | /opt/omni/sbin/uma -ioctl /dev/rsst4
```

ピッカーは、SCSI-2 デバイス ライブラリとして動作しなければなりません。ライブラリは、強制的に初期化することでチェックできます。以下のコマンドを入力してください。

```
echo "init" | /opt/omni/sbin/uma -ioctl /dev/rsst4
```

Berkeley スタイルのデバイス ファイルを必ず使用してください。この例の場合、エクスチェンジャドライブには、/dev/rmt/0h ではなく /dev/rmt/0hb を使用し、SCSI 制御デバイス (ピッカー) には /dev/rsst4 を使用する必要があります。

この次に行う作業

インストールを完了し、バックアップ デバイスを Solaris クライアントに適切に接続したら、バックアップ デバイスやメディア プールなど、運用に必要な要素を構成します。詳細は、オンライン ヘルプの索引キーワード「構成, バックアップ デバイス」で表示される内容を参照してください。

Linux クライアントのインストール

Linux クライアント システムは、UNIX 用インストール DVD-ROM を使ってローカルにインストールすることも、UNIX 用のインストール サーバを使ってリモート インストールすることもできます。

インストール手順を開始する前に、どのコンポーネントをクライアント システムにインストールするかを決定しておいてください。Data Protector ソフトウェア コンポーネントのリストと説明は、59 ページの「Data Protector コンポーネント」を参照してください。

前提条件

- システム要件、ディスク スペース要件、サポートされているプラットフォームと Data Protector コンポーネントについては、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。
- この時点で、Cell Manager および UNIX 用のインストール サーバをネットワーク上にインストールしておく必要があります。詳細は 19 ページの「Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール」を参照してください。

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

- rpm ユーティリティをインストールして、セットアップしておく必要があります。その他のパッケージングシステム (deb など) はサポートされていません。

注記 Linux 上では GUI はサポートされていません。ただし、omniusers コマンドを使用して、新しい Cell Manager 上にリモート ユーザー アカウントを作成することは可能です。これにより、Data Protector GUI をインストールした任意のシステム上でこのユーザー アカウントを使って GUI を起動し、新しい Cell Manager に接続できます。詳細は omniusers のマンページを参照してください。

注記 Data Protector はデフォルトでポート番号 5555 を使用します。そのため、このポート番号が他のプログラムで使われていないことを確認する必要があります。一部の Linux バージョンでは、このポート番号が別の目的で使われています。

ポート番号 5555 がすでに使われている場合は、Data Protector で使えるようにこのポート番号を空けるか、あるいは、デフォルトのポート番号を未使用の番号に変更してください。詳細は B-28 ページの「デフォルトのポート番号の変更」を参照してください。

HP ServiceGuard クラスタ

HP ServiceGuard クラスタの場合は、Data Protector エージェント (Disk Agent、Media Agent) を、共有ディスク上ではなく、各クラスタ ノード (ローカル ディスク) 上に個別にインストールしなければなりません。

インストールが終了したら、*仮想ホスト* (アプリケーション パッケージ) をクライアントとしてセルにインポートする必要があります。そのため、アプリケーション パッケージ (Oracle など) はクラスタ上で、クラスタの *仮想 IP* を使って実行されていなければなりません。クライアントをインポートする前に、cmviewcl -v コマンドを使用して、この点をチェックしてください。

ローカル インストール

お使いの環境に UNIX 用のインストール サーバがない場合は、UNIX 用のインストール DVD-ROM を使用して、ローカル インストールを行う必要があります。詳細は 119 ページの「UNIX クライアントのローカル インストール」を参照してください。

リモート インストール

Linux クライアント システムは、UNIX 用のインストール サーバから Linux システムに Data Protector コンポーネントを配布することにより、リモートでインストールできます。この操作には、Data Protector グラフィカル ユーザー インタフェースを使用します。ソフトウェア配布手順の詳細は、50 ページの「Data Protector クライアントのリモート インストール」を参照してください。

クライアント コンポーネントのインストールが完了したターゲット システムは、自動的に Data Protector セルに追加されます。

トラブルシューティング

Linux クライアント システムへのリモート インストール中に問題が発生した場合は、root アカウントに、exec サービスまたは shell サービスを使ってシステムにアクセスする権限があるかどうかを確認します。以下の手順に従ってください。

1. /etc/xinetd.conf ファイルを開き、exec サービスおよび shell サービスに対する定義を探して、これらのサービス定義に以下の行を追加します。

```
server_args = -h
```

例：

```
service shell
{
socket_type = stream
protocol = tcp
wait = no
user = root
server = /usr/sbin/in.rshd
server_args = -L -h
}

service exec
{
socket_type = stream
protocol = tcp
wait = no
user = root
server = /usr/sbin/in.rexecd
server_args = -h
}
```

注記

一部の Linux ディストリビューションでは、これらのサービスが /etc/xinetd.d ディレクトリ内の個別のファイル内に構成されていることがあります。この場合は、適切なファイル (/etc/xinetd.d/rexec および /etc/xinetd.d/rsh) を探して、上記の変更を行ってください。

2. HUP シグナルを使用して、inetd プロセスを停止します。

```
kill -HUP $(ps ax|grep inet|grep -v grep|cut -c1-6)
```

3. ~root/.rhosts ファイルを作成し、ファイル内にエントリ <my_installation_server> root を定義します。

これで、インストール サーバからの管理アクセスが可能になります。

Data Protector のインストールが終了したら、このエントリを -root/.rhosts ファイルから削除し、-h フラグを /etc/xinetd.conf ファイル (Red Hat Enterprise Linux の場合は /etc/inetd.conf ファイル) から削除してもかまいません。その後、手順 2 の kill コマンドを繰り返します。

詳細は、rexecd(8)、rexec(3)、rshd(8)、rsh(1)、pam(8) のマンページを参照してください。問題が発生した場合は、119 ページの「UNIX クライアントのローカル インストール」を参照してください。

カーネル構成

以下の手順は、カーネル構成のチェックおよびビルドの方法を説明したものです。

1. root ユーザーとしてログインし、/usr/src/linux ディレクトリから make menuconfig コマンドを実行します。
2. [SCSI Support] を選択し、[Enter] キーを押します。次に、オプション [SCSI support]、[SCSI tape support]、[SCSI generic support] を選択し、必要に応じて [Probe all LUNS on each SCSI device] も選択します。

これらの項目がカーネルにすでに含まれている場合は、変更を保存せずに終了し、バックアップ デバイスをシステムに接続する作業に進みます。83 ページの「Linux システムへのバックアップ デバイスの接続」を参照してください。

3. 構成を変更した場合は、変更内容を保存して以下の手順を実行します。

- a. make dep コマンドを実行します。

このコマンドにより、カーネル ソース内に依存ツリーが作成されます。作成される依存関係は、カーネル構成時に選択したオプションに影響されます。

- b. `make clean` コマンドを実行して、以前のカーネルビルド時に作成されていた不要なファイルを消去します。
 - c. `make bzImage` コマンドを実行します。このコマンドが終了したら、次に `make modules` コマンドを実行します。
4. Intel ベースシステムの `/boot` ディレクトリにカーネルをインストールするには、新しい `bzImage` を `/boot` ディレクトリに、次のようにコピーします。

- a. 次のコマンドを実行します。
`cp /usr/src/linux/arch/i386/boot/bzImage/boot/newkernel`
- b. `make modules_install` コマンドを実行して、モジュールを `/lib/modules` ディレクトリにインストールします。
- c. `/etc/lilo.conf` ファイルを開いて、次のエントリを追加します。

```
image = /boot/newkernel  
  
label = new  
  
read-only
```

- d. `/sbin/lilo` コマンドを実行して LILO を更新します。

次の再起動時に、LILO 内のカーネル「new」を選択して新しいカーネルをロードします。新しいカーネルを使ってみて問題が生じなければ、カーネル「new」を `lilo.conf` ファイル内の先頭に移動して、このカーネルが毎回デフォルトで起動するようにしてください。

カーネルと SCSI 構成の詳細については、カーネルソースディレクトリ `/usr/src/linux/Documentation/` 内を参照してください。

Linux システムへのバックアップ デバイスの接続

Linux クライアントに Media Agent コンポーネントをインストールした後は、以下の手順に従って、システムにバックアップ デバイスを接続してください。

1. `cat /proc/scsi/scsi` コマンドを実行して、ドライブおよび制御デバイス (ロボティクス) 用に使用可能な SCSI アドレスを調べます。
2. デバイスの SCSI アドレスを設定します。デバイスの種類にもよりますが、通常 SCSI アドレスはデバイス上のスイッチで設定できます。詳細は、使用するデバイスのマニュアルを参照してください。

サポート対象デバイスの詳細は、<http://www.hp.com/support/manuals> を参照してください。

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

3. デバイスをコンピュータに接続し、デバイスとコンピュータの電源を順に投入して、ブート処理が完了するまで待ちます。ブート処理中にデバイス ファイルが生成されます。(RedHat Linux の場合は、コンピュータに新しいデバイスを接続すると、ブート処理中にアプリケーション Kudzu が起動されます。任意のキーを押してアプリケーションを開始し、[Configure] ボタンをクリックしてください。)
4. 新しいバックアップ デバイスをシステムが正しく認識しているかどうかを検証するため、`cat /proc/scsi/scsi` を実行し、次に、`dmesg |grep scsi` を実行します。接続されている個々のバックアップ デバイスについて、デバイス ファイルが一覧表示されます。

例

ロボティクスの場合は、`dmesg |grep scsi` コマンドの出力は次のようになります。

```
Detected scsi generic sg2 at scsi2, channel 0, id 4, lun 0, type 8
```

ドライブの場合は次のようになります。

```
Detected scsi tape st0 at scsi2, channel 0, id 5, lun 0
```

5. デバイス ファイルは `/dev` ディレクトリ内に生成されます。次のコマンドを実行して、デバイス ファイルへのリンクが作成されていることを確認します。

```
ll /dev | grep <device_file>
```

例：

```
ll /dev | grep sg2
```

このコマンドの出力は次のようになります。

```
lrwxrwxrwx 1 root root 3 Nov 27 2001 sg2 -> sgc
```

`/dev/sg2` はデバイス ファイル `/dev/sgc` へのリンクです。これは、Data Protector で使用されるデバイス ファイルが、ロボティクス用は `/dev/sgc`、デバイス用は `/dev/st0` であることを意味しています。ロボティクス用のデバイス ファイル名は、`sga`、`sgb`、`sgc`、... `sgh`、ドライブ用のデバイス ファイル名は、`st0`、`st1`、... `st7` のようになります。

この次に行う作業

インストールを完了し、バックアップ デバイスを Linux クライアント システムに適切に接続したら、バックアップ デバイスやメディア プールなど、運用に必要な要素を構成します。詳細は、オンライン ヘルプの索引キーワード「構成、バックアップ デバイス」で表示される内容を参照してください。

AIX クライアントのインストール

AIX クライアントは、UNIX 用インストール DVD-ROM を使ってローカルにインストールすることも、UNIX 用のインストール サーバを使ってリモート インストールすることもできます。

インストール手順を開始する前に、どのコンポーネントをクライアント システムにインストールするかを決定しておいてください。Data Protector ソフトウェア コンポーネントのリストと説明は、59 ページの「Data Protector コンポーネント」を参照してください。

前提条件

- システム要件、ディスク スペース要件、サポートされているプラットフォームと Data Protector コンポーネントについては、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。
- この時点で、Cell Manager および UNIX 用のインストール サーバをネットワーク上にインストールしておく必要があります。詳細は 19 ページの「Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール」を参照してください。

重要

AIX システムに Disk Agent コンポーネントをインストールする前に、ポート マッパーが動作していることを確認する必要があります。/etc/rc.tcpip ファイルを開き、ポートマッパーを起動する行が以下のように記述されていることを確認してください。

```
start /usr/sbin/portmap "$src_running"
```

srcmstr デーモンが実行されている場合は、src_running フラグは 1 に設定されます。srcmstr デーモンは、System Resource Controller (SRC) です。srcmstr デーモンは、サブシステムの生成と管理、サブシステム ステータスに関するショート リクエストの処理、サブシステムへのリクエストの送信、エラー通知の処理を行います。

ローカル インストール

お使いの環境に UNIX 用のインストール サーバがない場合は、UNIX 用のインストール DVD-ROM を使用して、ローカル インストールを行う必要があります。詳細は 119 ページの「UNIX クライアントのローカル インストール」を参照してください。

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

リモート インストール

AIX クライアント ソフトウェアは、Data Protector グラフィカル ユーザー インタフェースを使って UNIX 用のインストール サーバからリモートにインストールできます。ソフトウェアのリモート インストール手順は、50 ページの「Data Protector クライアントのリモート インストール」を参照してください。

クライアント コンポーネントのインストールが完了したターゲット システムは、自動的に Data Protector セルに追加されます。

AIX クライアントへのバックアップ デバイスの接続

AIX クライアントに Media Agent をインストールした後は、以下の作業を実行してください。

1. コンピュータをシャットダウンし、バックアップ デバイスを SCSI バスに接続します。バックアップ デバイスに使用する SCSI アドレスが、他のデバイスに使用されていないことを確認してください。
サポート対象デバイスの詳細は、<http://www.hp.com/support/manuals> を参照してください。
2. コンピュータの電源を投入し、ブート処理が完了するまで待ちます。AIX システム管理ツールの `smit` を起動し、新しいバックアップ デバイスがシステムによって正しく認識されていることを確認します。

重要 `smit` を使って、デバイスのデフォルト ブロック サイズを 0 (可変長ブロック) に変更してください。

3. `/dev` ディレクトリから適切なデバイス ファイルを選択し、Data Protector バックアップ デバイスを構成します。

重要 非巻き戻し型のデバイス ファイルのみを使用してください。たとえば、`/dev/rmt0` ではなく、`/dev/rmt0.1` を選択してください。

この次に行う作業

インストールを完了し、バックアップ デバイスを AIX システムに適切に接続したら、バックアップ デバイスやメディア プールなど、Data Protector の運用に必要な要素を構成します。詳細は、オンライン ヘルプの索引キーワード「構成、バックアップ デバイス」で表示される内容を参照してください。

Siemens Sinix クライアントのインストール

Siemens Sinix クライアントは、UNIX 用インストール DVD-ROM を使ってローカルにインストールすることも、UNIX 用のインストール サーバを使ってリモート インストールすることもできます。

インストール手順を開始する前に、どのコンポーネントをクライアント システムにインストールするかを決定しておいてください。Data Protector ソフトウェア コンポーネントのリストと説明は、59 ページの「Data Protector コンポーネント」を参照してください。

前提条件

- システム要件、ディスク スペース要件、サポートされているプラットフォームと Data Protector コンポーネントについては、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。
- この時点で、Cell Manager および UNIX 用のインストール サーバをネットワーク上にインストールしておく必要があります。詳細は 19 ページの「Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール」を参照してください。

ローカル インストール

お使いの環境に UNIX 用のインストール サーバがない場合は、UNIX 用のインストール DVD-ROM を使用して、ローカル インストールを行う必要があります。詳細は 119 ページの「UNIX クライアントのローカル インストール」を参照してください。

リモート インストール

Sinix クライアント ソフトウェアは、Data Protector グラフィカル ユーザー インタフェースを使って UNIX 用のインストール サーバからリモートにインストールできます。ソフトウェアのリモート インストール手順は、50 ページの「Data Protector クライアントのリモート インストール」を参照してください。

クライアント コンポーネントのインストールが完了したターゲット システムは、自動的に Data Protector セルに追加されます。

Siemens Sinix システムへのバックアップ デバイスの接続

Siemens Sinix クライアント システムに Media Agent コンポーネントをインストールした後は、以下の手順に従って、システムにバックアップ デバイスを接続してください。

1. コンピュータをシャットダウンし、バックアップ デバイスを SCSI バスに接続します。

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

サポートされているデバイスの詳細は、<http://www.hp.com/support/manuals> を参照してください。また、デバイスに付属するドキュメントも参照してください。

バックアップ デバイス用に選択した SCSI アドレスが、他のデバイスに使用されていないことを確認します。

2. コンピュータの電源を投入し、ブート処理が完了するまで待ちます。
3. /dev ディレクトリから、適切なデバイス ファイルを選択します。

デバイスのリストを表示するには、`autoconf -l` コマンドを使います。このコマンドの出力に報告されたテープ デバイス名 (`ios0/stape006` など) に基づいて、Data Protector で使用できる専用のデバイス ファイル名 (`/dev/ios0/rstape006nv` など) を特定します。

注記

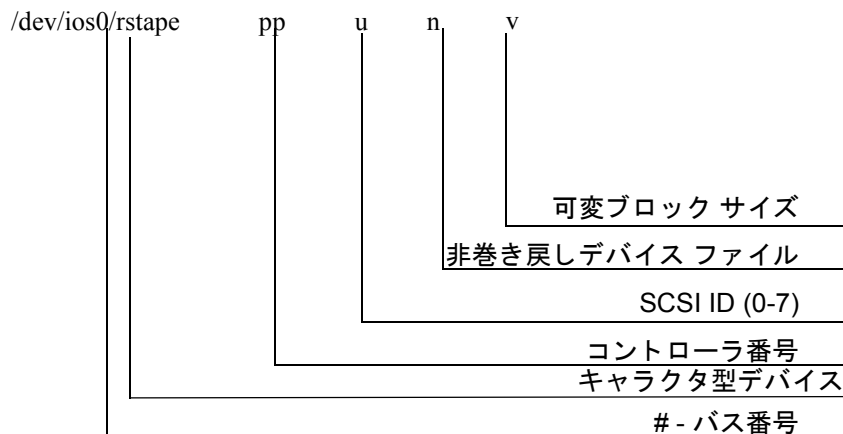
専用のデバイス ファイルは /dev ディレクトリに格納されていますので、デバイス名の前に /dev パスを付けてください。

Data Protector ではキャラクタ デバイスだけを使用できます。このため、`stape006` の直前に文字 `r` を付けて使用します。

Data Protector でテープ デバイスを処理できるのは、そのデバイスが非巻き戻しデバイスとしてオープンされており、かつブロック サイズが可変に設定されている場合です。したがって、文字 `n` および `v` を末尾に付加する必要があります。

図 2-18 では、デバイス ファイル /dev/ios0/rstape006nv を例に、デバイス ファイル名について説明しています。

図 2-18 デバイス ファイル名の形式 :



この次に行う作業

インストールを完了し、バックアップ デバイスを Siemens Sinix クライアント システムに適切に接続したら、バックアップ デバイスやメディア プールなど、運用に必要な要素を構成します。詳細は、オンライン ヘルプの索引キーワード「構成, バックアップ デバイス」で表示される内容を参照してください。

Tru64 クライアントのインストール

Tru64 クライアントは、UNIX 用インストール DVD-ROM を使ってローカルにインストールすることも、UNIX 用のインストール サーバを使ってリモート インストールすることもできます。

インストール手順を開始する前に、どのコンポーネントをクライアント システムにインストールするかを決定しておいてください。Data Protector ソフトウェア コンポーネントのリストと説明は、59 ページの「Data Protector コンポーネント」を参照してください。

前提条件

- システム要件、ディスク スペース要件、サポートされているプラットフォームと Data Protector コンポーネントについては、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

- この時点で、Cell Manager および UNIX 用のインストール サーバをネットワーク上にインストールしておく必要があります。詳細は 19 ページの「Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール」を参照してください。

ローカル インストール

お使いの環境に UNIX 用のインストール サーバがない場合は、UNIX 用のインストール DVD-ROM を使用して、ローカル インストールを行う必要があります。詳細は 119 ページの「UNIX クライアントのローカル インストール」を参照してください。

リモート インストール

Tru64 クライアント ソフトウェアは、Data Protector グラフィカル ユーザー インタフェースを使って UNIX 用のインストール サーバからリモートにインストールできます。ソフトウェアのリモート インストール手順は、50 ページの「Data Protector クライアントのリモート インストール」を参照してください。

クライアント コンポーネントのインストールが完了したターゲット システムは、自動的に Data Protector セルに追加されます。

Tru64 クラスタ

すべてのターゲット システムに、root ユーザーのパーミッションが必要です。

Data Protector は、Tru64 クラスタの共有ディスクにローカルまたはリモートにインストールする必要があります。インストールを実行するには、クラスタ ノードのいずれかを使用します。

インストール後、クラスタ仮想ホスト名および個々のノードを Data Protector セルにインポートする必要があります。詳細な手順については、188 ページの「セルへのクラスタ対応クライアントのインポート」を参照してください。

Tru64 クライアントへのバックアップ デバイスの接続

Tru64 クライアントに Media Agent をインストールした後は、以下の作業を実施してください。

1. コンピュータをシャットダウンし、バックアップ デバイスを SCSI バスに接続します。

注記 バックアップ デバイスをハードディスク ドライブと同じ SCSI バスに接続することは、お勧めしません。

バックアップ デバイス用に選択した SCSI アドレスが、他のデバイスに使用されていないことを確認します。

サポート対象デバイスの詳細は、<http://www.hp.com/support/manuals> を参照してください。

2. コンピュータの電源を投入し、ブート処理が完了するまで待ちます。新しいバックアップ デバイスがシステムによって正しく認識されていることを確認します。

この次に行う作業

インストールを完了し、バックアップ デバイスを Tru64 システムに適切に接続したら、バックアップ デバイスやメディア プールなど、Data Protector の運用に必要な要素を構成します。詳細は、オンライン ヘルプの索引キーワード「構成、バックアップ デバイス」で表示される内容を参照してください。

SCO クライアントのインストール

SCO クライアントは、UNIX 用インストール DVD-ROM を使ってローカルにインストールすることも、UNIX 用のインストール サーバを使ってリモート インストールすることもできます。

なお、UnixWare では、リモート インストールができません。

インストール手順を開始する前に、どのコンポーネントをクライアント システムにインストールするかを決定しておいてください。Data Protector ソフトウェア コンポーネントのリストと説明は、59 ページの「Data Protector コンポーネント」を参照してください。

前提条件

- システム要件、ディスク スペース要件、サポートされているプラットフォームと Data Protector コンポーネントについては、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。
- この時点で、Cell Manager および UNIX 用のインストール サーバをネットワーク上にインストールしておく必要があります。詳細は 19 ページの「Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール」を参照してください。

ローカル インストール

お使いの環境に UNIX 用のインストール サーバがない場合は、UNIX 用のインストール DVD-ROM を使用して、ローカル インストールを行う必要があります。詳細は 119 ページの「UNIX クライアントのローカル インストール」を参照してください。

ネットワークへの Data Protector のインストール Data Protector クライアントのインストール

リモート インストール

SCO クライアント ソフトウェアは、Data Protector グラフィカル ユーザー インタフェースを使って UNIX 用のインストール サーバからリモートにインストールできます。ソフトウェアのリモート インストール手順は、50 ページの「Data Protector クライアントのリモート インストール」を参照してください。

クライアント コンポーネントのインストールが完了したターゲット システムは、自動的に Data Protector セルに追加されます。

SCO システムへのバックアップ デバイスの接続

SCO クライアント システムに Media Agent コンポーネントをインストールした後は、以下の手順に従って、システムにバックアップ デバイスを接続してください。

1. /etc/conf/cf.d/m SCSI ファイルをチェックして、利用可能な SCSI アドレスを調べます。このファイルには、現在接続されている SCSI デバイスのリストが示されます。
サポートされているデバイスの詳細は、<http://www.hp.com/support/manuals> を参照してください。また、デバイスに付属するドキュメントも参照してください。
2. コンピュータをシャットダウンし、バックアップ デバイスを SCSI バスに接続します。
3. コンピュータを再起動します。
4. `mkdev tape` コマンドを使用してデバイスを構成します。テープドライブ デバイスのリストから Generic SCSI-1 / SCSI-2 tape drive を選択します。

注記 UNIT ID は、`mkdev tape` コマンドの実行時に表示されます。デバイス ファイル名を認識するには、この ID が必要となります。

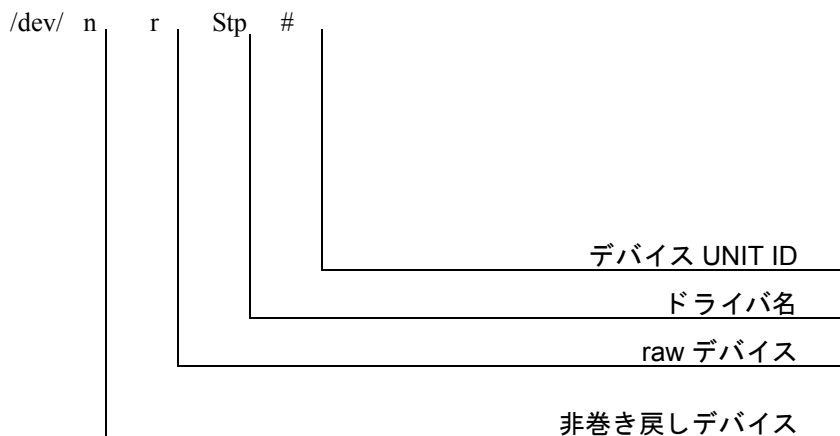
5. デバイスを構成し、システムを再起動した後、/etc/conf/cf.d/m SCSI ファイルをチェックし、デバイスが正しく接続されていることを確認します。
6. /dev ディレクトリから、適切なデバイス ファイル名を選択します。

名前の末尾にデバイスの UNIT ID を付けます。UNIT ID を # とすると、nrStp# のように指定してください。デバイスの UNIT ID は、手順 4 で定義されています。図 2-19 では、デバイス ファイル /dev/nrStp# を例に、デバイス ファイル名について説明しています。

注意

可変長ブロックサイズの非巻き戻しデバイス ファイルのみを使用してください。
tape -s getblk /dev/nrStp# コマンドを使って、可変長ブロックサイズを確認してください。可変長ブロックサイズの値は、0 でなければなりません。ブロックサイズが 0 に設定されていない場合は、tape -a 0 setblk /dev/nrStp# コマンドを実行します。

図 2-19 **デバイス ファイル名の形式 :**



この次に行う作業

インストールを完了し、バックアップ デバイスを SCO クライアント システムに適切に接続したら、バックアップ デバイスやメディア プールなど、運用に必要な要素を構成します。詳細は、オンライン ヘルプの索引キーワード「構成、バックアップ デバイス」で表示される内容を参照してください。

ADIC/GRAU ライブラリ用または StorageTek ライブラリ用の Media Agent のインストール

Data Protector には、ADIC/GRAU ライブラリまたは StorageTek ACS ライブラリを Data Protector のバックアップ デバイスとして構成するための専用の ADIC/GRAU ライブラリ方針と StorageTek ACS ライブラリ方針が用意されています。ADIC/GRAU ライブラリ内または StorageTek ライブラリ内のドライブに物理的に接続されるすべてのシステムに、Data Protector Media Agent (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。また、マルチホス

ネットワークへの Data Protector のインストール Data Protector クライアントのインストール

ト構成の場合は、ADIC/GRAU ライブラリまたは StorageTek ライブラリのロボティクスを制御するシステムにも、Data Protector Media Agent をインストールする必要があります。なお、マルチホスト構成とは、ライブラリとドライブが互いに別のコンピュータに接続される構成を意味しません。

ADIC/GRAU ライブラリでは、Media Agent ソフトウェアがインストールされ、GRAU/ADIC DAS Server を介してライブラリ ロボティクスにアクセスする各システムは、**DAS クライアント**と呼ばれます。STK ACS 用統合ソフトウェアでは、Media Agent ソフトウェアがインストールされ、STK ACS Server を介してライブラリ ロボティクスにアクセスする各システムは、**ACS クライアント**と呼ばれます。

注記 StorageTek ライブラリ内で使用するドライブおよびスロットの数によっては、特殊なライセンスが必要になります。詳細は 293 ページの第 5 章「Data Protector のライセンス」を参照してください。

ライブラリ ドライブの接続

Media Agent ソフトウェアのインストール先のシステムにライブラリ ドライブを物理的に接続します。

サポート対象の ADIC/GRAU ライブラリまたは STK ライブラリの詳細は、<http://www.hp.com/support/manuals> を参照してください。

バックアップ デバイスをシステムに物理的に接続する方法は、68 ページの「HP-UX クライアントのインストール」を参照してください。また、ADIC/GRAU ライブラリまたは StorageTek ライブラリのマニュアルも参照してください。

バックアップ デバイスをサポート対象の Windows システムに物理的に接続する方法は、63 ページの「Windows 用クライアントのインストール」を参照してください。また、ADIC/GRAU ライブラリまたは StorageTek ライブラリの手動マニュアルも参照してください。

ADIC/GRAU ライブラリを使用する Data Protector クライアントの準備作業

Media Agent ソフトウェアをインストールする前に、以下の手順で ADIC/GRAU ライブラリを構成してください。

1. DASサーバがOS/2をベースに稼動している場合は、Data ProtectorのADIC/GRAUバックアップ デバイスを構成する前に、DAS サーバ コンピュータ上の C:¥DAS¥ETC¥CONFIG ファイルを作成または更新してください。このファイルには、すべての DAS クライアントを定義する必要があります。Data Protector の場合は、ライブラリ ロボティクスを制御することが可能な各 Data Protector クライアントをファイルに定義する必要があります。

各 DAS クライアントは、たとえば DP_C1 のように、スペースを含まない一意のクライアント名で定義されています。C:¥DAS¥ETC¥CONFIG ファイルには、たとえば、以下のようなリストを記述します。

```
client client_name = DP_C1,  
#      hostname = AMU,"client1"  
      ip_address = 19.18.17.15,  
      requests = complete,  
      options = (avc,dismount),  
      volumes = ((ALL)),  
      drives = ((ALL)),  
      inserts = ((ALL)),  
      ejects = ((ALL)),  
      scratchpools = ((ALL))
```

2. ADIC/GRAU DAS ライブラリ ロボティクスへのアクセスを必要とする Data Protector Media Agent がインストールされた各 Data Protector クライアント上で、omnirc ファイル (Windows の場合は <Data_Protector_home>¥omnirc ファイル、HP-UX および Solaris の場合は /opt/omni/.omnirc ファイル、AIX の場合は /usr/omni/omnirc ファイル) を開いて以下の変数を設定します。

DAS_CLIENT DAS サーバ上に定義される一意な GRAU クライアント名です。たとえば、クライアント名が「DP_C1」であれば、omnirc ファイル内のこれに該当する行は、DAS_CLIENT=DP_C1 となります。

DAS_SERVER DAS サーバ名です。

3. ADIC/GRAU ライブラリ スロットの割り当て方針には、静的な割り当てと動的な割り当ての 2 種類があるため、現在、そのどちらの方針が適用されているかを確認する必要があります。割り当て方針の種類をチェックする方法は、『AMU Reference Manual』を参照してください。

静的割り当て方針では各 volser ごとにスロットがあらかじめ指定されていますが、動的割り当て方針ではスロットがランダムに割り当てられます。静的方針の場合は、以下のような Data Protector の構成作業が必要です。

静的割り当て方針が設定されている場合は、ライブラリのロボティクスを制御するシステムに、以下の omnirc 変数を追加する必要があります。

```
OB2_ACIEJECTTOTAL = 0
```

注記 これは、HP-UX および Windows に当てはまります。

ADIC/GRAU ライブラリの構成に関して、さらに詳しい情報が必要な場合は、最寄りの ADIC/GRAU サポートに問い合わせるか、ADIC/GRAU のマニュアルなどを参照してください。

ADIC/GRAU ライブラリ用の Media Agent のインストール

前提条件

Media Agent をインストールするシステムは、以下の条件を満たしている必要があります。

- ✓ ADIC/GRAU ライブラリが構成済みで、実行されていること。ADIC/GRAU ライブラリのマニュアルを参照してください。
- ✓ Data Protector のインストールと構成が完了していること。本章の 19 ページの「Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール」を参照してください。
- ✓ DAS サーバが実行されていること。

ADIC/GRAU ライブラリを制御するには、DAS クライアント ソフトウェアが必要です。各 DAS クライアントには、DAS クライアント ソフトウェアをインストールする必要があります。Data Protector からメディアおよびデバイスに対して開始されたアクションは、DAS クライアントを介して DAS サーバに送信されます。さらに、ADIC/GRAU ライブラリ内で、ロボティクスの制御と、メディアの移動またはロードを受け持つ部分 (AMU - AML Management Unit) に渡されます。アクションが完了すると、DAS サーバが DAS クライアントに応答を返します。ADIC/GRAU ライブラリのマニュアルを参照してください。

- ✓ Media Agent をインストールする前に、以下の情報を用意しておく必要があります。
 - DAS Server (OS/2 上で実行されるアプリケーション) のホスト名。
 - 対応する DAS 名とともにドライブを示すリスト。取得されたドライブ名は、Data Protector に ADIC/GRAU ドライブを構成する際に使用されます。

ADIC/GRAU システムに対して DAS クライアントがすでに定義されている場合は、以下のいずれかの `dasadmin` コマンドでこのリストを取得できます。

```
dasadmin listd2 <client>
```

```
dasadmin listd <client>
```

ここで、`<client>` は予約済みのドライブを表示する DAS クライアントの名前です。

dasadmin コマンドは、OS/2 ホスト上の C:\DAS\BIN ディレクトリから実行できます。他のシステムにインストールした場合は、DAS クライアント ソフトウェアがインストールされているディレクトリから実行できます。UNIX クライアント システムの場合、通常、このディレクトリは /usr/local/aci/bin システム ディレクトリとなります。

- 利用可能な挿入・取り出しエリア、および、対応するフォーマット仕様のリスト。

OS/2 ホスト上の AMS のグラフィカル構成 (AML Management Software) では、以下の手順で、利用可能な挿入・取り出しエリアのリストを取得できます。

1. [Admin] -> [Configuration] メニューをクリックして、この構成を起動します。
2. [I/O unit] アイコンをダブルクリックして [EIF-Configuration] ウィンドウを開き、[Logical Ranges] フィールドをクリックします。
このテキスト ボックスに、利用可能な挿入・取り出しエリアのリストが表示されます。

注記

1 つの Data Protector ライブラリ デバイスで処理できるメディアの種類は、1 つだけです。
各エリアに所属するメディアの種類をメモしておいてください。この情報は、後で Data Protector ライブラリ用の挿入・取り出しエリアを構成するときに指定する必要があります。

- ドライブに対応する UNIX デバイス ファイルのリスト — Media Agent を UNIX システムにインストールする場合。

この情報を表示するには、システム コマンドの `ioscan -fn` を実行します。

UNIX デバイス ファイルの詳細は、72 ページの「HP-UX システムへのバックアップ デバイスの接続」を参照してください。

- ドライブに対応する SCSI アドレスのリスト — Media Agent を Windows システムにインストールする場合。たとえば、`scsi4:0:1:0` のようなアドレスです。

SCSI アドレスの詳細は、67 ページの「Windows システムへのバックアップ デバイスの接続」を参照してください。

インストール

インストール手順は以下のとおりです。

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

1. Data Protector グラフィカル ユーザー インタフェースとインストール サーバを使って、クライアントに Media Agent コンポーネントを配布します。本章の 50 ページの「Data Protector クライアントのリモート インストール」を参照してください。
2. ADIC/GRAU ライブラリをインストールします。
 - Windows システムでは、以下の操作を行ってください。
 - a. aci.dll, winrpc32.dll, および ezrpc32.dll の各ライブラリを、`<Data_Protector_home>\bin` ディレクトリにコピーします。(これらの 3 つのライブラリは、ADIC/GRAU ライブラリに付属する DAS クライアント ソフトウェアの一部です。インストール メディア、または AMU-PC の `C:\DAS\AMU` ディレクトリに含まれています。)
 - b. この 3 つのファイルは、`<%SystemRoot%\system32` ディレクトリにもコピーしてください。
 - c. Portinst サービスおよび Portmapper service サービスを DAS クライアントにコピーします。(これらは、ADIC/GRAU ライブラリとともに出荷されている DAS クライアント ソフトウェアの要件です。インストール メディアに記載されています。)
 - d. コントロールパネルの [管理ツール] - [サービス] から、portinst を起動して portmapper をインストールします。portmapper サービスを実行するには、DAS クライアントを再起動する必要があります。
 - e. システムを再起動した後、portmapper サービスと rpc サービスがともに実行されているか確認します (コントロールパネルの [管理ツール] - [サービス] で、これらのサービスの状態を確認します)。
 - HP-UX システムの場合は、共有ライブラリ libaci.sl を /opt/omni/lib ディレクトリにコピーします。このディレクトリにアクセスするには、適切なパーミッションが必要です。すべてのユーザー (root とそのユーザー グループ、およびその他 [others]) に対する読み取りパーミッションと実行パーミッションが共有ライブラリに設定されていることを確認してください。libaci.sl 共有ライブラリは、ADIC/GRAU ライブラリに付属する DAS クライアント ソフトウェアの一部です。インストール メディアに含まれています。
 - AIX システムの場合は、共有ライブラリ libaci.o を /usr/omni/lib ディレクトリにコピーします。このディレクトリにアクセスするには、適切なパーミッションが必要です。すべてのユーザー (root とそのユーザー グループ、およびその他 [others]) に対する読み取りパーミッションと実行パーミッションが共有ライブラリに設定されていることを確認してください。libaci.o 共有ライブラリは、ADIC/GRAU ライブラリに付属する DAS クライアント ソフトウェアの一部です。インストール メディアに含まれています。

この時点で、ハードウェアが正しく接続されており、DAS ソフトウェアが適切にインストールされている必要があります。

以下のコマンドを実行して、ライブラリ ドライブがシステムに正しく接続されているかどうかを確認します。

- **Windows の場合:** <Data_Protector_home>%bin%devbra -dev
- **HP-UX の場合:** /opt/omni/lbin/devbra -dev
- **AIX の場合:** /usr/omni/bin/devbra -dev

ライブラリ デバイスが正しく接続されていれば、ライブラリ デバイスおよび対応するデバイス ファイルがリストに表示されます。

この次に行う作業

Media Agent のインストールを完了して、ADIC/GRAU ライブラリをシステムに物理的に接続した後に行うその他の構成作業 (バックアップ デバイスやメディア プールの構成など) は、オンライン ヘルプの索引キーワード「構成, バックアップ デバイス」で表示される内容を参照してください。

StorageTek ライブラリを使用する Data Protector クライアントの準備作業

Media Agent をインストールするシステムは、以下の条件を満たしている必要があります。

- ✓ StorageTek ライブラリが構成済みで、実行されていること。StorageTek ライブラリのマニュアルを参照してください。
- ✓ Data Protector のインストールと構成が完了していること。詳細は 19 ページの「Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール」を参照してください。
- ✓ Media Agent ソフトウェアをインストールする前に、以下の情報を用意しておく必要があります。
 - ACSLS を実行するホストの <ÉzÉXÉgñ°>。
 - Data Protector で使用する ACS ドライブ ID のリスト。取得されたドライブ ID は、Data Protector に StorageTek ドライブを構成する際に使用されます。このリストを表示するには、ACSL S を実行しているホストにログインし、以下のコマンドを実行します。

```
rlogin "ACSL S hostname" -l acssa
```

端末の種類を入力し、コマンド プロンプトが表示されるまで待ちます。ACSSA プロンプトが表示されたら、以下のコマンドを入力します。

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

```
ACSSA> query drive all
```

ACS ドライブのフォーマット仕様は、以下のように定義されていなければなりません。

```
ACS DRIVE: ID:#,#,#,# - (ACS num, LSM num, PANEL, DRIVE)
```

- 利用可能な ACS CAP ID のリストと ACS CAP フォーマットの仕様。このリストを表示するには、ACSLS を実行しているホストにログインし、以下のコマンドを実行します。

```
rlogin "ACSLS hostname" -l acssa
```

端末の種類を入力して、コマンドプロンプトが表示されるまで待ちます。ACSSA プロンプトが表示されたら、次のコマンドを入力します。

```
ACSSA> query cap all
```

ACS CAP のフォーマット仕様は、以下のように定義されていなければなりません。

```
ACS CAP: ID:#,#,# - (ACS num, LSM num, CAP num)
```

- ドライブに対応する UNIX デバイス ファイルのリスト — Media Agent を UNIX システムにインストールする場合。

この情報を表示するには、システム コマンドの `ioscan -fn` を実行します。

UNIX デバイス ファイルの詳細は、72 ページの「HP-UX システムへのバックアップ デバイスの接続」を参照してください。

- ドライブに対応する SCSI アドレスのリスト — Media Agent を Windows システムにインストールする場合。たとえば、`scsi4:0:1:0` のようなアドレスです。

SCSI アドレスの詳細は、67 ページの「Windows システムへのバックアップ デバイスの接続」を参照してください。

- ✓ Data Protector 用に使用されるドライブが、**オンライン**状態であることを確認してください。ドライブが**オンライン**状態でない場合は、ACSLS ホスト上で以下のコマンドを実行してオンラインにします。

```
vary drive <drive_id> online
```

- ✓ Data Protector に使用する CAP が**オンライン**状態になっており、動作モードが**手動**になっていることを確認します。

CAP が**オンライン**状態でない場合は、以下のコマンドを実行してオンラインにします。

```
vary cap <cap_id> online
```

CAP の動作モードが**手動**でない場合は、以下のコマンドを実行して手動モードにします。

```
set cap manual <cap_id>
```

StorageTek ライブラリ用の Media Agent のインストール

インストール手順は以下のとおりです。

1. Data Protector グラフィカル ユーザー インタフェースと UNIX 用インストール サーバを使って、クライアントに Media Agent コンポーネントを配布します。本章の 50 ページの「Data Protector クライアントのリモート インストール」を参照してください。
2. 以下に示すように、各 ACS クライアントで ACS の ssi デーモンを起動します。

- HP-UX と Solaris の ACS クライアントの場合は、以下のコマンドを実行します。

```
/opt/omni/acs/ssi.sh start <ACS_LS_hostname>
```

- Windows ACS クライアントの場合は、LibAttach サービスをインストールします。詳細は、ACS のマニュアルを参照してください。LibAttach サービスの構成時には、必ず適切な ACSLS ホスト名を入力してください。構成が正常に完了すると、LibAttach サービスが自動的に開始されます。それ以降は、システムを再ブートすると、必ずこのサービスが自動的に開始されます。
- AIX ACS クライアントの場合は、以下のコマンドを実行します。

```
/usr/omni/acs/ssi.sh start <ACS_LS_hostname>
```

注記

LibAttach サービスのインストールが完了したら、システムパスに libattach¥bin ディレクトリが自動的に追加されていることを確認します。追加されていない場合は、手作業で追加してください。

LibAttach サービスの詳細は、StorageTek ライブラリのマニュアルを参照してください。

3. 以下のコマンドを実行して、ライブラリ ドライブがシステムに正しく接続されているかどうかをチェックします。
- HP-UX か Solaris の ACS クライアントの場合 : /opt/omni/lbin/devbra -dev
 - Windows ACS クライアントの場合 : <Data_Protector_home>¥bin¥devbra -dev
 - AIX ACS クライアントの場合 : /usr/omni/bin/devbra -dev

ライブラリ ドライブおよび対応するデバイス ファイル /SCSI アドレスのリストが表示されます。

ネットワークへの Data Protector のインストール Data Protector クライアントのインストール

この次に行う作業

Media Agent のインストールを完了して、StorageTek ライブラリをシステムに物理的に接続した後に行うその他の構成作業 (バックアップ デバイスやメディア プールの構成など) は、オンライン ヘルプの索引キーワード「構成、バックアップ デバイス」で表示される内容を参照してください。

Novell NetWare クライアントのローカル インストール

Novell NetWare クライアントのインストールは、Novell ネットワークに接続されているサポート対象の Windows システムから行わなければなりません。

Data Protector Disk Agent および General Media Agent は、Novell NetWare を実行しているシステムにインストールすることができます。Data Protector コンポーネントの詳細は、59 ページの「Data Protector コンポーネント」を参照してください。

サポート対象のデバイスや Novell NetWare プラットフォーム バージョンの詳細、これまでに報告されている問題とその解決策については、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。

前提条件

Novell NetWare プラットフォームに Data Protector をインストールする前に、以下の条件が満たされていることを確認してください。

- ✓ システム要件、ディスク スペース要件、サポートされているプラットフォームと Data Protector コンポーネントについては、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。
- ✓ TCP/IP プロトコルがインストールされており、正しく動作していること。
- ✓ Windows システム上で、以下のサービスのいずれかが実行されていることを確認してください。
 - Novell NetWare 用の Gateway Service。
このサービスは、Windows Server からインストールを行うときに、Windows 上で実行されている必要があります。
 - Windows 用の Novell Client、または NetWare 用の Microsoft Client Service。
このサービスは、Windows ワークステーションからインストールを行うときに、Windows 上で実行されている必要があります。

- ✓ Windows システムから、ターゲットの NetWare サーバ (または適切な NDS/eDirectory ツリー) にログインします。
- ✓ ターゲット NetWare サーバ上での SYS: ボリュームに対して、管理者の権限を持っていることを確認してください。
- ✓ Windows システム上に、利用可能なローカル デバイス名が少なくとも 1 つあることを確認してください。

クラスタ対応クライアント

クラスタ対応クライアントをインストールする場合は、上記以外にも必要となる前提条件があります。179 ページの「クライアントのインストール」を参照してください。

インストール

このインストール手順は、Data Protector の Windows 用 DVD-ROM から実行できます。Novell NetWare のインストールは、インストール サーバからは実行できない点に注意してください。

Novell NetWare サーバに Data Protector をインストールするには、以下の手順に従ってください。

1. Windows システム上でコマンド プロンプトを実行して、現在のパスを DVD-ROM のルート ディレクトリに変更します。
2. インストール スクリプトを実行します。

Data Protector の Novell NetWare クライアントをインストールするには、現在のパスを NetWare ディレクトリに変更し、以下を入力します。

```
NWInstall <target server name> <ALL|DA|MA> <port_number>
```

2 番目のパラメータは、Data Protector Novell Client のどの機能をインストールするかを定義します。

- すべての Data Protector Novell NetWare クライアント機能をインストールするには、ALL と入力します。
- Novell NetWare 用の Data Protector Disk Agent のみインストールする場合は、DA と入力します。
- Novell NetWare 用の Data Protector General Media Agent のみインストールする場合は、MA と入力します。

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

注記

Novell NetWare に Data Protector をインストールする場合、Novell NetWare のバージョンに関わらず、ポート番号は任意に指定できます。番号を指定しなければ、デフォルトのポート番号 5555 が使われます。

Data Protector でサポートされていない Novell NetWare OS のバージョンを使用している場合、インストールは可能ですが警告が表示されます。

インストールを行う段階で、ターゲット サーバにすでに Data Protector ファイルが存在するかどうか確認されます。ファイルがすでに存在する場合、すでにインストールされている Data Protector は、SYS:¥usr¥Omni.old ディレクトリに移されます。

インストールされている NetWare クライアントのバージョンに応じて、サーバ上で OMNIINET.NLM、HPINET.NLM または HPBRAND.NLM が実行されていないか確認します。いずれかが実行されている場合は、Novell NetWare コンソールから以下のコマンドを実行してモジュールをアンロードしてください。

```
UNLOAD HPINET (UNLOAD OMNIINET / UNLOAD HPBRAND)
```

インストールを行うと、自動的に Data Protector のディレクトリ構造が作成され、ターゲットサーバに Data Protector のすべてのファイルがコピーされます。

3. 以下のモジュールがシステムにロードされていることを確認してください。

- NETDB.NLM
- TSAFS.NLM
- TSANDS.NLM

上記のモジュールによって、ローダーは、HPINET.NLM をロードする際に、パブリックシンボルを解決できます。

Novell NetWare 6.x システム上に Novell NetWare Cluster Services が構成されている場合は、NCSSDK.NLM モジュールがロードされていることを確認してください。

4. HPINET.NLM をロードするには、Novell NetWare コンソールで以下のコマンドを入力します。

```
SEARCH ADD SYS:USR¥OMNI¥BIN  
  
LOAD HPINET.NLM
```

注記 デフォルトのポート番号 5555 を使用しない場合は、`-port <port_number>` オプションを追加して LOAD コマンドを実行し、ポート番号を指定します。以下に例を示します。

```
LOAD HPINET.NLM -port <port_number>
```

Novell NetWare のインストールを行うと、Novell NetWare サーバが自動的に Data Protector Cell Manager を認識できるように、AUTOEXEC.NCF ファイルに自動的に上記のコンソールコマンドが追加されます。これにより、HPINET.NLM ファイルが常にロードされ、Novell NetWare サーバがいつでも Data Protector Cell Manager に接続できる状態になります。

注記 インストールが完了したら、AUTOEXEC.NCF ファイルを確認してください。必要なコンソールコマンドが AUTOEXEC.NCF ファイルに追加されていない場合は、手作業で追加してください。

NDS/eDirectory データベースのバックアップと復元を可能にするには、以下の手順を行ってください。

1. NDS/eDirectory のバックアップと復元の実行時に使用するユーザー アカウントを定義します。
2. Novell NetWare コンソールから、HPLOGIN.NLM モジュールをロードします。

```
LOAD HPLOGIN.NLM
```

3. NDS/eDirectory データベースにログインできるように、以下のユーザー情報を HPLOGIN.NLM ファイルに追加します。

- NDS/eDirectory Context:

ユーザー オブジェクトが格納されているコンテナを指定します。コンテナ名は、完全修飾名構文として指定する必要があります。以下に例を示します。

```
OU=SDM.0=HSL
```

- NDS/eDirectory Object Name:

これは、Data Protector Disk Agent が NDS/eDirectory のバックアップ・復元を実行する際に、正規の NDS/eDirectory ユーザーが NDS/eDirectory データベースへのログインに使用するユーザー オブジェクトの共通名です。この正規の NDS ユーザーは、前述のコンテキスト内に記述されている必要があります。以下に例を示します。

```
CN=MarcJ
```

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

たとえば、ユーザーの完全修飾名は .CN=MarcJ.OU=SDM.O=HSL となります。

- NDS/eDirectory Object Password:

正規のユーザー パスワードは、NDS/eDirectory データベースへログインする際、または NDS/eDirectory データベースのバックアップや復元を開始する際に、ユーザー名とともに使用します。

HPLOGIN モジュールに入力されたユーザー情報は暗号化され、SYS:SYSTEM ディレクトリに保存されます。Novell NetWare SMS モジュールのロードにも、パスワードが使用されます。

注記

HPLOGIN モジュールで選択するユーザー アカウントには、NDS/eDirectory データベースのバックアップと復元を実行するためのパーミッションがなければなりません。

NDS/eDirectory ユーザー オブジェクトに対して変更を行った場合 (別のコンテナへの移動、削除、名前の変更、パスワードの変更)、SYS:SYSTEM ディレクトリで暗号化されている情報を HPLOGIN モジュール内で更新する必要があります。

*** InheritNum is only useful for nested lists ***

4. Novell NetWare Storage Management Services (SMS) で NDS/eDirectory をバックアップおよび復元するには、NDS/eDirectory ツリー内の 1 つ以上のサーバ上に SMDR.NLM モジュールおよび TSANDS.NLM モジュールをロードする必要があります。TSANDS.NLM および SMDR.NLM の最新バージョンは、以下の Web ページからダウンロードできます。

<http://support.novell.com/filefinder/>

インストールが完了すると、LOAD TSANDS.NLM 行が AUTOEXEC.NCF ファイルに追加されます。これにより、Novell NetWare サーバは、TSANDS.NLM をすぐに認識できるようになります。Novell NetWare の SMS モジュールの SMDR.NLM は、TSANDS.NLM がロードされるとすぐにロードされます。

注記

インストール後、コンソール コマンドが AUTOEXEC.NCF ファイルに追加されていない場合は、手作業で追加してください。

ヒント

バックアップ プロセス中のネットワーク負荷を最小限にするには、最大の NDS/eDirectory パーティションのレプリカを含むサーバ上にモジュールをロードします。

以上で、NDS/eDirectory のバックアップおよび復元の要件を満たしたことになります。必要となるその他の作業については、オンライン ヘルプの索引キーワード「構成」で表示される内容を参照してください。

Media Agent の構成

この時点で、Data Protector コンポーネントはすべてインストールされています。ただし、インストールの始めの段階で ALL または MA パラメータを選択している場合は、Data Protector General Media Agent が Novell NetWare サーバに接続されているバックアップ デバイスを使用するための追加の構成作業が必要です。

Data Protector では、Adaptec SCSI ホスト アダプタ コントローラとそれに対する .HAM ドライバがサポートされています。Data Protector Media Agent は、.HAM ドライバと直接通信して、SCSI ホスト アダプタにアクセスできます。そのため、SCSI ホスト アダプタ ドライバをインストールしておく必要があります。Adaptec ドライバの最新バージョンは、<http://www.adaptec.com> からダウンロードできます。

STARTUP.NCF ファイルに LOAD コマンドが追加されていれば、サーバが再起動時されるたびにドライバが自動的にロードされます。このコマンドには、ドライバのロケーション、使用可能なオプション、およびスロット番号を指定しなければなりません。使用可能なオプションのリスト、およびスロット番号の算出方法は、Adaptec 社の『Adaptec Driver User's Guide』を参照してください。

例：

サーバが再起動されるたびに AHA-2940 Adaptec ドライバが Novell NetWare 6.x サーバに自動的にロードされるようにするには、STARTUP.NCF ファイルに次の行を追加します。

```
SET RESERVED BUFFERS BELOW 16 MEG=200
```

```
LOAD AHA2940.HAM SLOT=4 lun_enable=03
```

SLOT には、ホスト アダプタ デバイスが格納されているスロット番号を指定します。また、lun_enable は、すべてのターゲット上で特定の LUN (論理ユニット番号) をスキャンするマスクを指定します。

各 LUN をすべての SCSI アドレスに対してスキャンするには、その LUN に対応するビットを 1 に設定します。上の例では lun_enable=03 と指定していますが、この場合、LUN 0 および LUN 1 がすべてのターゲット上でスキャンされます。

ネットワークへの Data Protector のインストール Data Protector クライアントのインストール

注記 lun_enable の指定は、SCSI LUN が 0 より大きいデバイスを使用する場合にのみ必要となります。たとえば、HP StorageWorks Tape 12000e ライブラリ デバイスを構成する場合などです。

ヒント サーバが再起動されるたびに、Novell NetWare サーバに接続されたすべてのデバイスとその LUN を自動的にスキャンするには、AUTOEXEC.NCF ファイルに次の行を追加します。

```
SCAN FOR NEW DEVICES
```

```
SCAN ALL LUNS
```

以上で、General Media Agent の構成が完了します。

この次に行う作業

Novell NetWare プラットフォームに General Media Agent ソフトウェアをインストールした後は、Data Protector General Media Agent のインストール状態をチェックすることをお勧めします。詳細は B-71 ページの「Novell NetWare 上にインストールした General Media Agent のチェック」を参照してください。

インストール状態を確認したら、Novell NetWare クライアントを Data Protector グラフィカル ユーザー インタフェースを使って Data Protector セルにインポートします。追加の構成作業の詳細は、オンライン ヘルプの索引キーワード「Novell NetWare」で表示される内容を参照してください。

OpenVMS クライアントのローカル インストール

OpenVMS クライアントのインストール手順は、サポート対象の OpenVMS システム上でローカルに実行する必要があります。リモート インストールはサポートされていません。

Data Protector Disk Agent、General Media Agent、ユーザー インタフェース (コマンド行インタフェースのみ) は、OpenVMS 7.3-1/IA64 8.2 が稼働中のシステムにインストールすることができます。さらに、Oracle 用統合ソフトウェア コンポーネントは、OpenVMS 7.3-1 以上が稼働中のシステムにインストールできます。Data Protector コンポーネントの詳細は、59 ページの「Data Protector コンポーネント」を参照してください。

サポート対象のデバイスや OpenVMS プラットフォーム バージョンの詳細、これまでに報告されている問題とその解決策については、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス』を参照してください。

前提条件

OpenVMS プラットフォームに Data Protector クライアントをインストールする前に、以下の条件が満たされていることを確認してください。

- ✓ TCP/IP トランスポート プロトコルがインストールおよび実行されていること。
- ✓ `SY$MANAGER:UTC$TIME_SETUP.COM` コマンドで、システムの TIMEZONE が設定されていること。
- ✓ OpenVMS システムの SYSTEM アカウントにログインしていること。適切なパーミッションが必要であることに注意してください。
- ✓ OpenVMS クライアント インストール パッケージが含まれた Data Protector インストール DVD-ROM にアクセスできること。

インストール

このインストール手順は、Data Protector の Windows 用インストール DVD-ROM から実行できます。OpenVMS のインストールは、インストール サーバからは実行できない点に注意してください。

OpenVMS システムに Data Protector クライアントをインストールするには、以下の手順に従ってください。

1. PCSI インストール ファイルがすでにある場合は、手順 2 に進みます。PCSI インストール ファイルを探す必要がある場合は、インストール CD をマウントし、CD の OpenVMS ディレクトリにある `DPVMSKIT.EXE` プログラムを実行します。PCSI インストール ファイルが、デフォルト ディレクトリか指定した場所にコピーされます。

2. 次のコマンドを実行します。

```
$ PRODUCT INSTALL DP /SOURCE=device:[directory]
```

`device:[directory]` は、.PCSI インストール ファイルがある場所です。

3. プロンプトに YES と応答して、キットのバージョンを確認します。

```
The following product has been selected:  
HP AXPVMS DP A06.00-xx Layered Product  
Do you want to continue? [YES]
```

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

4. インストールするソフトウェア コンポーネントを選択します。デフォルトでは、Disk Agent、General Media Agent、およびユーザー インタフェースがインストールされます。Oracle 用統合ソフトウェア (Alpha システムの場合のみ) はデフォルトではインストールされない点に注意してください。各コンポーネントを個別に選択することもできます。

選択した製品がインストールされるほか、ソフトウェアの依存関係を満たすために必要な製品もインストールされます。これらの製品に関するオプションを選択するように促すプロンプトが表示されます。

例：

```
HP AXPVMS DP A6.00-xx: HP AXPVMS Data Protector V6.00
```

```
Copyright 2006 Hewlett-Packard Development Company, L.P.
```

```
Do you want the defaults for all options? [YES] NO
```

```
Do you wish to install a disk agent for this client node? [YES] YES
```

```
Do you wish to install a media agent for this client node? [YES] YES
```

```
Do you wish to install the command language interface (CLI)? [YES] YES
```

```
Do you want to review the options? [NO] YES
```

```
HP AXPVMS DP A6.00-xx: HP OpenVMS Alpha Data Protector V6.00 [Installed]
```

```
Do you wish to install a disk agent for this client node?: YES
```

```
Do you wish to install a media agent for this client node?: YES
```

```
Do you wish to install the command language interface (CLI)? : YES
```

```
Do you wish to install the Oracle Integration Agents? [NO] YES
```

```
Are you satisfied with these options? [YES] YES
```

Data Protector ディレクトリとファイルのデフォルト位置は、以下のとおりです。

```
SYS$SYSDEVICE: [VMS$COMMON.OMNI]
```

ディレクトリ構造は自動的に作成され、ファイルはこのディレクトリ ツリー内に格納されます。

Data Protector の起動コマンド プロシジャおよびシャットダウン コマンド プロシジャは、以下のディレクトリに格納されます。

```
SYS$SYSDEVICE: [VMS$COMMON.SYS$STARTUP]
```

OpenVMS クライアントでは、どんな場合でも 4 つのファイルが存在し、CLI オプションを選択した場合にのみ 5 つ目のファイルが格納されます。これら 5 つのファイルを以下に示します。

- `SYS$STARTUP:OMNI$STARTUP.COM`

ノード上で Data Protector を起動するためのコマンド プロシジャです。

- `SYSS$STARTUP:OMNI$SYSTARTUP.COM`
OMNI\$ROOT の論理名を定義するためのコマンド プロシジャです。このクライアントに必要な他の論理名も、このコマンド プロシジャに追加できます。
- `SYSS$STARTUP:OMNI$SHUTDOWN.COM`
ノード上で Data Protector をシャットダウンするためのコマンド プロシジャです。
- `OMNI$ROOT: [BIN] OMNI$STARTUP_INET.COM`
TCP/IP INET プロセスを起動するのに使用するコマンドプロシジャです。その後、Cell Manager により送信されたコマンドが実行されます。
- `OMNI$ROOT: [BIN] OMNI$CLI_SETUP.COM`
Data Protector CLI の起動に必要なシンボルを定義するためのコマンド プロシジャです。インストール中に CLI オプションが選択された場合のみ、システム上に存在します。

CLI を使用するすべてのユーザに対して、`login.com` プロシジャからこのコマンド プロシジャを実行してください。このプロシジャには、CLI コマンドを正しく実行するために必要ないくつかの論理名が定義されています。

5. `SYSS$MANAGER:SYSTARTUP_VMS.COM` に以下の行を挿入します。

```
@sys$startup:omni$startup.com
```

6. `SYSS$MANAGER:SYSHUTDWN.COM` に以下の行を挿入します。

```
@sys$startup:omni$shutdown.com
```

7. OpenVMS クライアントから、Cell Manager 用のすべての TCP/IP エイリアスに接続できることを確認します。
8. 185 ページの「セルへのクライアントのインポート」の記述に従って、Data Protector グラフィカル ユーザー インタフェースを使用して OpenVMS クライアントを Data Protector セルにインポートします。

OMNIADMIN という名前のアカウントがインストール中に作成されます。OMNI サービスは、このアカウントの下で実行されます。

このアカウントのログイン ディレクトリは `OMNI$ROOT: [LOG]` で、ここに `OMNI$STARTUP_INET.LOG` というログ ファイルが Data Protector コンポーネントの起動ごとに作成されます。このログ ファイルには、要求を実行しているプロセスの名前、使用されている Data Protector イメージの名前、要求のオプションが記録されます。

予期しないエラーは、すべてこのディレクトリの `DEBUG.LOG` ファイルに記録されます。

ネットワークへの Data Protector のインストール Data Protector クライアントのインストール

クラスタ環境でのインストール

共用システム ディスクを使用する場合、クライアント ソフトウェアのインストールが一度のみ必要になります。ただし、OMNI\$STARTUP.COM プロシジャは、Data Protector クライアントとして使用する各ノードで実行する必要があります。共用システム ディスクを使用しない場合、クライアント ソフトウェアは各クライアントにインストールする必要があります。

クラスタの TCP/IP エイリアス名を使用する場合で、クラスタの共用システム ディスクを使用する場合、クライアントのエイリアス名も定義できます。エイリアス クライアントを定義すれば、個々のクライアント ノードで構成作業を行う必要はありません。クライアント定義かエイリアス定義のいずれかを選択し、クラスタ内でバックアップや復元の作業を実行できます。使用する構成によって、テープ デバイスやテープ ライブラリに対する直接パスを、保存や復元に使用できる場合と、使用できない場合があります。

Disk Agent の構成

OpenVMS 上の Data Protector Disk Agent では、マウントされた FILES-11 ODS-2 ディスク ボリュームおよび ODS-5 ディスク ボリュームがサポートされます。OpenVMS では、Disk Agent の構成は必要ではありません。ただし、Disk Agent を使用するバックアップ仕様の作成時には、いくつかの留意点があります。以下に留意点を示します

- GUI に入力される、または CLI に受け渡されるファイル仕様の構文は、UNIX スタイルである必要があります。以下に例を示します。

```
/disk/directory1/directory2/.../filename.ext.n
```

- 文字列はスラッシュ (/) で始め、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記述します。
- ディスク名の後ろにコロンを付けないでください。
- バージョン番号の前には、セミコロンではなくピリオドを使用します。
- OpenVMS ファイルのファイル指定では、大文字と小文字は区別されません (ODS-5 ディスク上のファイルは除く)。

例 :

OpenVMS でのファイル指定を以下に示します。

```
$1$DGA100: [USERS.DOE] LOGIN.COM;1
```

Data Protector では、以下の形式で指定する必要があります。

```
/$1$DGA100/Users/Doe/Login.Com.1
```

注記

暗黙のバージョン番号はありません。バージョン番号は必ず指定する必要がありますが、バックアップ対象として指定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。

一部のオプションでは、バージョン番号のワイルドカードをアスタリスク (*) に置き換えることが可能です。

バックアップにすべてのバージョンのファイルを含めたい場合は、GUI でそれらをすべて選択するか、CLI で `-only` オプションの後ろにファイル指定を含める必要があります。以下のように、バージョン番号にワイルドカードを使用します。以下に例を示します。

```
/DKA1/dir1/filename.txt.*
```

Media Agent の構成

OpenVMS システム上のデバイスは、ハードウェアのマニュアルを参考にして、OpenVMS を使用して構成する必要があります。最初に、テープライブラリの擬似デバイスを、SYSMAN を使用して以下のように作成する必要があります。

```
$ RUN SYS$SYSTEM:SYSMAN
```

```
SYSMAN> IO CONNECT gcan/NOADAPTER/DRIVER=SYS$GcDRIVER
```

各部分の説明：

c = K (SCSI テープライブラリの直接接続の場合)

a = SCSI コントローラのアダプタ文字 (A、B、C...)

n = テープライブラリ ロボティクス制御デバイスのユニット番号

注記

このコマンドは、システムのブート後に実行する必要があります。

SAN に接続されたテープライブラリの場合、SAN デバイスが SAN のガイドラインに従って構成されれば、テープドライブ名やロボットデバイス名が、OpenVMS で自動的に表示されます。

Data Protector で使用するテープジュークボックスをインストールする場合は、Data Protector での構成前に、ハードウェアが正常動作することを確認してください。ハードウェアの検証には、Hewlett-Packard から Media Robot Utility (MRU) を入手して使用することができます。

注記 これらのデバイスを手動または自動で構成するには、通常 Data Protector GUI を使用します。

ただし、一部の旧型テープ ライブラリや、HSx コントローラに接続されたテープ ライブラリでは、自動構成ができません。これらのデバイスを Data Protector に追加するには、手作業で構成してください。

クラスタの Media Agent

クラスタ システムに接続されたデバイスは、以下のように取り扱います。

1. 各テープ デバイスと各テープ ライブラリを構成し、各ノードからアクセスできるようにします。
2. デバイスを識別するため、デバイス名の最後にノード名を付加します。
3. テープ デバイスでは、Devices/Properties/Settings/Advanced/Other に共通の Device Lock Name を設定します。

例：

ノード A とノード B で構成されているクラスタ内で、TZ89 がノード A に接続され、MSCP がノード B で動作しているとします。TZ89_A という名前のデバイスを、ノード A でクライアントとして構成し、TZ89_B という名前のデバイスを、ノード B でクライアントとして構成します。TZ89 は、両方のデバイスに共通なデバイス ロック名です。これで、Data Protector では、いずれのパスを介した場合でも、両方が 1 つのデバイスであると認識されたうえで、デバイスが使用されます。ノード B で TZ89_A を使用してバックアップを実行した場合、Data Protector ではノード B からノード A のデバイスにデータが移されます。ノード B で TZ89_B を使用してバックアップを実行した場合、OpenVMS MSCP サーバによって、ノード B からノード A のデバイスにデータが移されます。

注記 MSCP が動作しているクラスタ内でのテープ デバイス、HSx コントローラを介して接続されているすべてのテープ デバイス、Fibre Channel を介して接続されているすべてのテープ デバイスでは、オンライン ヘルプの索引キーワード「SAN 環境, デバイスの構成」で表示される SAN 構成用のガイドラインに従ってください。

コマンド行インタフェース (CLI)

Data Protector コマンド行インタフェースを OpenVMS 上で使用するには、以下のように CLI コマンド セットアップ プロシジャを実行する必要があります。

```
$ @OMNI$ROOT: [BIN] OMNI$CLI_SETUP.COM
```

使用可能な CLI コマンドの説明は、『HP OpenView Storage Data Protector Command Line Interface Reference』を参照してください。

Oracle 用統合ソフトウェア

『HP OpenView Storage Data Protector インテグレーション ガイド - Oracle、SAP』の手順に従って Oracle 用統合ソフトウェアのインストールと構成を完了したら、OMNI\$ROOT: [CONFIG.CLIENT] omni_info に -key Oracle8 エントリが含まれていることを確認します。例を次に示します。

```
-key oracle8 -desc "Oracle Integration" -nlset 159 -nlid 12172 -flags 0x7  
-ntpath "" -uxpath "" -version A.06.00
```

このエントリが存在しない場合は、OMNI\$ROOT: [CONFIG.CLIENT] omni_format からコピーしてください。このエントリが含まれていないと、OpenVMS クライアント上で Oracle 用統合ソフトウェアがインストール済みとして示されません。

この次に行う作業

追加の構成作業の詳細は、オンライン ヘルプの索引キーワード「OpenVMS」で表示される内容を参照してください。

MPE/iX クライアントのインストール

詳細は『HP OpenView Storage Data Protector MPE/iX System User Guide』を参照してください。ドキュメント パッケージをシステム (HP-UX、Solaris、または Windows) 上にインストールしている場合、このユーザー ガイドは、MPE_user.pdf という名前で、Windows の場合は <Data_Protector_home>\Docs に、UNIX の場合は /opt/omni/doc/C/ に格納されています。また、Data Protector の Windows 用のインストール DVD-ROM の docs ディレクトリにも収録されています。

インストール手順を開始する前に、どのコンポーネントをクライアント システムにインストールするかを決定しておいてください。Data Protector ソフトウェア コンポーネントのリストと説明は、59 ページの「Data Protector コンポーネント」を参照してください。

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

サポート対象のデバイス、MPE/iX プラットフォームのバージョン、Data Protector コンポーネントの詳細は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス』を参照してください。

前提条件

MPE/iX プラットフォームに Data Protector をインストールする前に、以下の条件が満たされていることを確認してください。

- ✓ 使用するコンピュータに、TurboSTORE/iX または TurboSTORE/iX 7x24 True-Online がインストールされていること。
- ✓ TCP/IP プロトコルがインストールされ、構成されていること。
- ✓ 名前解決機能 (ホスト ファイルの DNS) が使用可能であること。
- ✓ ディスク スペース要件は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス』を参照してください。

インストール

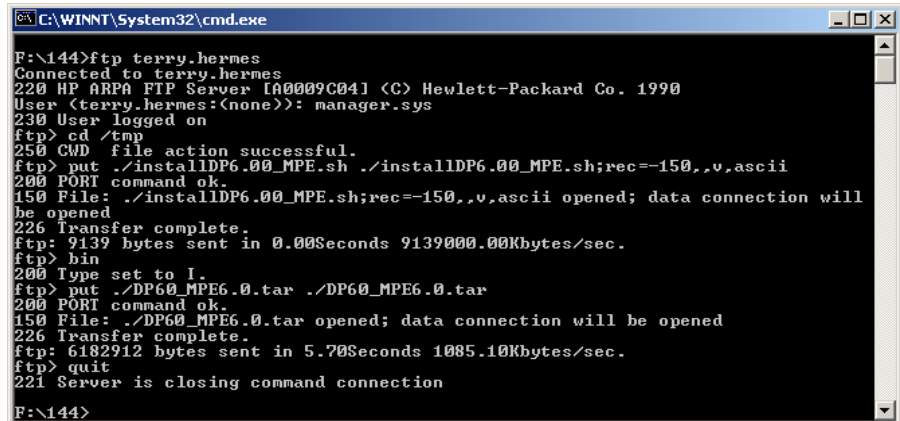
MPE/iX サーバに Data Protector をインストールするには、以下の手順に従ってください。

1. ftpユーティリティで (MPE/iX OS のバージョンに応じて) DP60_MPE6.5.tar パッケージまたは DP60_MPE7.0.tar パッケージのいずれかとともに installDP6.00_MPE.sh スクリプトを /tmp ディレクトリに転送します。詳細については、117 ページの例 2-1 を参照してください。

installDP6.60_MPE.sh ファイルは、以下の設定で転送することが重要です。

- レコード サイズ : -150
- ブロック係数 : -empty
- ファイルのレコードの可変長 : v
- 符号化レコードの種類 : ASCII

例 2-1 installDP6.00_MPE.sh スクリプトと DP60_MPE6.5.tar パッケージの転送
例

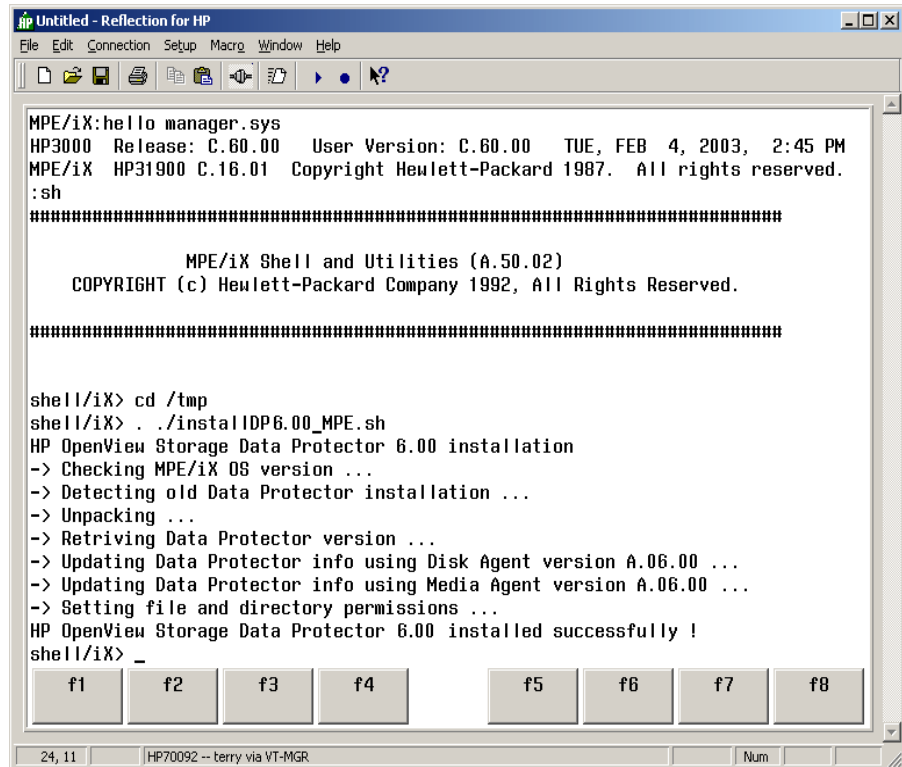


```
C:\WINNT\System32\cmd.exe
F:\144>ftp terry.hermes
Connected to terry.hermes
220 HP ARPA FTP Server [A0009C041 <C> Hewlett-Packard Co. 1990
User (terry.hermes:(none)): manager.sys
230 User logged on
ftp> cd /tmp
250 CWD file action successful.
ftp> put ./installDP6.00_MPE.sh ./installDP6.00_MPE.sh;rec=-150,.,v,ascii
200 PORT command ok.
150 File: ./installDP6.00_MPE.sh;rec=-150,.,v,ascii opened; data connection will
be opened
226 Transfer complete.
ftp: 9139 bytes sent in 0.00Seconds 9139000.00Kbytes/sec.
ftp> bin
200 Type set to I.
ftp> put ./DP60_MPE6.0.tar ./DP60_MPE6.0.tar
200 PORT command ok.
150 File: ./DP60_MPE6.0.tar opened; data connection will be opened
226 Transfer complete.
ftp: 6182912 bytes sent in 5.70Seconds 1085.10Kbytes/sec.
ftp> quit
221 Server is closing command connection
F:\144>
```

2. 次の図の例で示すとおり、ターゲット システムにログインして、ファイルを展開します。

ネットワークへの Data Protector のインストール Data Protector クライアントのインストール

例 2-2 ターゲット システム上でのプロセスの展開



```
Untitled - Reflection for HP
File Edit Connection Setup Macro Window Help

MPE/iX:hello manager.sys
HP3000 Release: C.60.00 User Version: C.60.00 TUE, FEB 4, 2003, 2:45 PM
MPE/iX HP31900 C.16.01 Copyright Hewlett-Packard 1987. All rights reserved.
:sh
#####

MPE/iX Shell and Utilities (A.50.02)
COPYRIGHT (c) Hewlett-Packard Company 1992, All Rights Reserved.

#####

shell/iX> cd /tmp
shell/iX> ./installDP6.00_MPE.sh
HP OpenView Storage Data Protector 6.00 installation
-> Checking MPE/iX OS version ...
-> Detecting old Data Protector installation ...
-> Unpacking ...
-> Retrieving Data Protector version ...
-> Updating Data Protector info using Disk Agent version A.06.00 ...
-> Updating Data Protector info using Media Agent version A.06.00 ...
-> Setting file and directory permissions ...
HP OpenView Storage Data Protector 6.00 installed successfully !
shell/iX> _

f1 f2 f3 f4 f5 f6 f7 f8

24, 11 HP70092 -- terry via VT-MGR Num
```

上記の操作後、すべてのファイルが /usr/omni ディレクトリに置かれます。

注記 下記のファイルを編集するには、EDIT/3000 (editor コマンドで起動) を使用します。詳しくは、『EDIT/3000 Reference Manual』を参照してください。

3. DCNF.NET.SYS ファイルに以下の行を追加します。

```
omni stream tcp nowait MANAGER.SYS /usr/omni/bin/inet inet -log
/tmp/inet.log
```

4. SERVICES.NET.SYS ファイルに以下の行を追加します。

```
omni 5555/tcp #Data Protector inet
```


- inetd を再起動して、新しい設定の構成を更新します。

詳しくは、『Configuring and Managing MPE/iX Internet Services』マニュアルを参照してください。

- Data Protector Inet が動作しているかどうかを確認するには、別のシステムからポート 5555 へ telnet で接続します。

```
telnet <hostname> 5555
```

Data Protector からメッセージが返されます。10 秒経っても応答がない場合は、INETDCNF.NET.SYS ファイルと SERVICES.NET.SYS ファイルの内容を調べてください。

- システムを Data Protector セルにインポートします。作業手順は、185 ページの「セルへのクライアントのインポート」を参照してください。
- クライアントシステムのインポートが正常に行われた後、Data Protector Admin ユーザーグループに MANAGER.SYS ユーザーを追加します。

MPE/iX クライアントの詳細な情報は、『HP OpenView Storage Data Protector MPE/iX System User Guide』を参照してください。このドキュメントは、Windows 用インストール DVD-ROM の %Docs%\MPE_user.pdf でご覧いただけます。

UNIX クライアントのローカル インストール

ネットワーク上に UNIX 用のインストール サーバがない場合、または何らかの理由によりクライアントシステムをリモート インストールできない場合は、HP-UX 用インストール DVD-ROM を使用して Data Protector クライアントをローカルにインストールできます。

インストール手順を開始する前に、どのコンポーネントをクライアントシステムにインストールするかを決定しておいてください。Data Protector ソフトウェア コンポーネントのリストと説明は、59 ページの「Data Protector コンポーネント」を参照してください。

前提条件

- システム要件、ディスク スペース要件、サポートされているプラットフォーム、プロセッサと Data Protector コンポーネントについては、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。
- すべてのターゲットシステムに、root ユーザーのパーミッションが必要です。

制限事項

ksh シェルのみサポートされています。

ネットワークへの Data Protector のインストール

Data Protector クライアントのインストール

注記

以下の手順を実行することにより、UNIX クライアントをローカルにアップグレードすることも可能です。スクリプトを実行すると、従来のインストール状況が検出されて、アップグレードを促すメッセージが表示されます。

手順

UNIX クライアントをローカルにインストールするには、以下の手順に従ってください。

1. UNIX インストール DVD-ROM をドライブに挿入してマウントします。
2. `<Mount_Point>/LOCAL_INSTALL` ディレクトリから、`omnisetup.sh` コマンドを実行します。このコマンドの構文は、以下のとおりです。

```
omnisetup.sh [-source <directory>] [-server <name>] [-install  
<component_list>]
```

各部分の説明：

- `<directory>` には、インストール DVD のマウント位置を指定します。指定しなければ、カレント ディレクトリが使用されます。
- `<name>` には、クライアントのインポート先となるセルの Cell Manager の完全なホスト名を指定します。指定しなければ、クライアントが自動的にセルにインポートされることはありません。

注記

Cell Manager 以外のシステムのクライアントをアップグレードする場合は、`-install <component_list>` を指定する必要はありません。この場合、プロンプトは表示されず、アップグレード前にシステムにインストールされていたのと同じコンポーネントが自動的に選択されます。

ただし、Cell Manager 上のクライアント コンポーネントをアップグレードする場合は、Cell Manager のアップグレード完了後、`omnisetup.sh` コマンドを `-install <component_list>` パラメータを付けて実行してください。

- `<component_list>` には、インストールするコンポーネント コードの一覧をカンマで区切って指定します。スペースは使用できません。`-install` パラメータを指定しなければ、システムで利用可能な各コンポーネントについて、インストールするかどうか確認するプロンプトが個別に表示されます。

注記 クライアントをアップグレードする場合に -install パラメータを指定しなければ、メッセージは返されず、アップグレード開始前にシステム上にインストールされていたのと同じコンポーネントが自動的に選択されます。

次の表はコンポーネントの一覧を示したものです。使用可能なコンポーネントの正確な一覧は、システムによって異なります。コンポーネントの詳細は、59 ページの「Data Protector コンポーネント」を参照してください。

表 2-4 Data Protector のコンポーネント コード

コンポーネント コード	コンポーネント
cc	ユーザー インタフェース
momgui	MoM ユーザー インタフェース
da	Disk Agent
ma	General Media Agent
ndmp	NDMP Media Agent
informix	Informix 用統合ソフトウェア
lotus	Lotus 用統合ソフトウェア
oracle	Oracle 用統合ソフトウェア
ov	HP OpenView Network Node Manager
omnist	OmniStorage 用統合ソフトウェア
sybase	Sybase 用統合ソフトウェア
sap	SAP R/3 用統合ソフトウェア
sapdb	SAP DB 用統合ソフトウェア
db2	DB2 用統合ソフトウェア
emc	EMC Symmetrix Agent

表 2-4 Data Protector のコンポーネント コード (続き)

コンポーネント コード	コンポーネント
ssea	HP StorageWorks Disk Array XP Agent
snapa	HP StorageWorks VA Agent
smisa	HP StorageWorks EVA SMIS-S Agent
fra_ls	フランス語のサポート
jpn_ls	日本語のサポート

例 :

次の例は、Disk Agent、General Media Agent、ユーザー インタフェース、および Informix 用のコンポーネントをクライアントにインストールし、anapola という名前の Cell Manager を持つセルにクライアントを自動的にインポートする場合の指定方法を示したものです。

```
./omnisetup.sh -server anapola.company.com -install da,ma,cc,informix
```

3. 処理が終了すると、インストールが終了してクライアントが Data Protector セルにインポートされたかどうかを示すメッセージが返されます。

いずれかのソフトウェア コンポーネントがインストール対象として選択されると、CORE コンポーネントが最初にインストールされます。

いずれかの統合ソフトウェア コンポーネントがインストールまたは再インストール対象として選択されると、CORE-INTEG コンポーネントが最初にインストールされます。

ハードディスクからのインストール実行

インストール DVD-ROM をコンピュータにコピーして、UNIX クライアントのインストールやアップグレードをハードディスクから実行したい場合は、少なくとも DP_DEPOT ディレクトリと LOCAL_INSTALL/omnisetup.sh コマンドをコピーする必要があります。たとえば、インストールパッケージを /var/dp60 にコピーする場合、DP_DEPOT は /var/dp60 のサブディレクトリにならなければなりません。

```
# pwd  
/var/dp60
```

```
# ls  
DP_DEPOT  
omnisetup.sh
```

これをハード ディスクにコピーした後に、次のコマンドを実行できます。

```
omnisetup.sh -source <directory> [-server <name>] [-install <component_list>]
```

-source オプションが必要なことに注意してください。以下に例を示します。

```
./omnisetup.sh -source /var/dp60
```

この次に行う作業

インストール時に Cell Manager の名前を指定しておかなければ、クライアントはセルにインポートされません。この場合は、Data Protector グラフィカル ユーザー インタフェースを使用して、後からインポートする必要があります。作業手順は、185 ページの「セルへのクライアントのインポート」を参照してください。追加の構成作業の詳細は、オンライン ヘルプを参照してください。

Data Protector 統合クライアントのインストール

Data Protector 用統合ソフトウェアは、Oracle や Microsoft Exchange などのデータベース アプリケーションのオンライン バックアップを Data Protector で実行可能にするソフトウェア コンポーネントです。Data Protector ZDB 統合ソフトウェアは、HP StorageWorks Enterprise Virtual Array などの ZDB ディスク アレイを使用して ZDB を実行可能にするソフトウェア コンポーネントです。

データベース アプリケーションが実行されるシステムを**統合クライアント**と呼びます。また、ZDB ディスク アレイがデータのバックアップと復元に使われるシステムを**ZDB 統合クライアント**と呼びます。これらのクライアントは、Windows や UNIX 上の他のクライアントと同じ手順でインストールできますが、そのためには適切なソフトウェア コンポーネントを選択しておくことが必要です (たとえば、MS Exchange データベースのバックアップには MS Exchange 2000/2003 用統合ソフトウェア コンポーネント、HP StorageWorks Enterprise Virtual Array の ZDB には HP StorageWorks EVA SMI-S Agent コンポーネントなど)。

前提条件

- システム要件、ディスク スペース要件、サポートされているプラットフォーム、プロセッサと Data Protector コンポーネントについては、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。
- データベース アプリケーションで Data Protector 用統合ソフトウェアを使用する場合は、ライセンスが必要です (VSS 用統合ソフトウェアを除く)。ライセンスの詳細は A-8 ページの「機能拡張」を参照してください。
- この時点で、Cell Manager およびインストール サーバ (リモート インストールを行う場合) をネットワーク上にインストールしておく必要があります。詳細は 19 ページの「Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール」を参照してください。

インストール手順を開始する前に、統合コンポーネントとともにクライアント システムにインストールするその他の Data Protector ソフトウェア コンポーネントを決定しておいてください。Data Protector ソフトウェア コンポーネントのリストと説明は、59 ページの「Data Protector コンポーネント」を参照してください。

以下に示すように、特定の Data Protector コンポーネントのインストールが必要となる場合があります。

- Data Protector を使ってファイルシステム データをバックアップする場合、Disk Agent コンポーネントが必要。Disk Agent は、以下の目的に使用することができます。

- データベース アプリケーション バックアップ機能を使用してバックアップできない重要なデータがあるファイルシステムで、バックアップを実行する。
- データベース アプリケーション サーバ (Oracle ServerやMS SQL Serverなど) のファイルシステムでテスト バックアップを実行する。データベース アプリケーションで Data Protector 用統合ソフトウェアを構成し、アプリケーションと Data Protector に関連する通信やその他の問題点を解決する前に、ファイルシステム バックアップをテストする必要があります。
- ディスク イメージとファイルシステムの ZDB を実行する。
- SAP R/3 ZDB 統合ソフトウェアを使用する場合に、LAN 上でバックアップ メディアからアプリケーション システムに復元する。
- Data Protector 統合クライアント上で Data Protector GUI および Data Protector CLI を利用する場合、**ユーザー インタフェース** コンポーネントが必要。
- Data Protector 統合クライアントに接続されたバックアップ デバイスがある場合、General Media Agent コンポーネントが必要。NDMP サーバを介して NDMP 専用ドライブにアクセスするために Data Protector クライアントを使用する場合は、NDMP Media Agent が必要です。

統合クライアントは、Windows 用または UNIX 用のインストール サーバのインストール DVD-ROM を使ってローカルにインストールすることも、Windows 用または UNIX 用のインストール サーバを使ってリモートでインストールすることもできます。

個々の統合クライアントに関するその他の詳細は、以下の該当する項を参照してください。

- Microsoft Exchange Server クライアント
- MS SQL クライアント
- Sybase クライアント
- Informix Server クライアント
- SAP R/3 クライアント
- SAP DB クライアント
- Oracle クライアント
- DB2 クライアント
- NNM クライアント
- NDMP クライアント

ネットワークへの Data Protector のインストール Data Protector 統合クライアントのインストール

- MS Volume Shadow Copy クライアント
- Lotus Notes/Domino Server クライアント
- EMC Symmetrix 用統合ソフトウェア
- HP StorageWorks XP 用統合ソフトウェア
- HP StorageWorks Virtual Array 用統合ソフトウェア
- HP StorageWorks Enterprise Virtual Array 用統合ソフトウェア

上の項に示す Data Protector 統合クライアントへの Data Protector 統合ソフトウェアのインストールが完了していれば、適切な『HP OpenView Storage Data Protector インテグレーション ガイド』、『HP OpenView Storage Data Protector Zero Downtime Backup Administrator’s Guide』、または『HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide』を参照して、Data Protector 統合クライアントを構成します。

ローカル インストール

お使いの環境にそれぞれのオペレーティング システム用のインストール サーバがない場合は、クライアントをインストールするプラットフォームに応じて、Windows 用または UNIX 用のインストール DVD-ROM を使用して、ローカル インストールを行う必要があります。詳細は 63 ページの「Windows 用クライアントのインストール」か 119 ページの「UNIX クライアントのローカル インストール」を参照してください。

インストールする際に Cell Manager を選択しなかった場合、ローカル インストール後にクライアント システムをセルに手動でインポートする必要があります。185 ページの「セルへのクライアントのインポート」も参照してください。

リモート インストール

クライアント ソフトウェアは、Data Protector グラフィカル ユーザー インタフェースを使ってインストール サーバからリモートにインストールできます。ソフトウェアのリモート インストール手順は、50 ページの「Data Protector クライアントのリモート インストール」を参照してください。

リモート インストールが終了すると、クライアント システムは自動的に Data Protector セルのメンバーになります。

クラスタ対応統合ソフトウェアのインストール

Data Protector クラスタ対応統合クライアントは、各クラスタ ノードで、DVD-ROM からローカルにインストールする必要があります。ローカルクライアントのセットアップ中には、他のクライアント ソフトウェア コンポーネントに加え、適切な統合ソフトウェア コンポーネント (Oracle Integration や HP StorageWorks EVA SMI-S Agent など) をインストールしてください。

Data Protector Cell Manager には、クラスタ対応データベース アプリケーションと ZDB Agent もインストールできます。Cell Manager のセットアップ中に、適切な統合ソフトウェア コンポーネントを選択してください。

インストール手順は、統合クライアントをインストールするクラスタ環境により、異なります。該当するオペレーティング システムのクラスタ化に関する項を参照してください。

- 165 ページの「MC/ServiceGuard への Data Protector のインストール」
- 167 ページの「Data Protector の Microsoft Cluster Server へのインストール」
- 178 ページの「Veritas Cluster への Data Protector クライアントのインストール」
- 179 ページの「Novell NetWare Cluster への Data Protector クライアントのインストール」

クラスタ化に関する詳細は、オンライン ヘルプの索引キーワード「クラスタ、MC/ServiceGuard」で表示される内容、および『HP OpenView Storage Data Protector コンセプト ガイド』を参照してください。

この次に行う作業

インストールの完了後に統合ソフトウェアを構成する方法は、適切な『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。

Microsoft Exchange Server クライアント

ここでは、Microsoft Exchange Server が正しく動作していることが前提となります。

Microsoft Exchange Server データベースをバックアップする場合は、インストール手順で MS Exchange 2000/2003 用統合ソフトウェア コンポーネントを選択する必要があります。

Microsoft Exchange シングル メールボックス用統合ソフトウェア エージェントは、Data Protector Microsoft Exchange Server の統合パッケージの一部としてインストールされます。

MS SQL クライアント

ここでは、Microsoft SQL Server が正しく動作していることが前提となります。

Microsoft SQL Server データベースをバックアップする場合は、インストール手順で MS SQL 7.0/2000 用統合ソフトウェア コンポーネントを選択する必要があります。

Sybase クライアント

Sybase Backup Server はすでに実行されているものとします。

Sybase データベースをバックアップする場合は、インストール手順で以下の Data Protector コンポーネントを選択する必要があります。

- Sybase 用統合ソフトウェア - Sybase データベースをバックアップする場合
- Disk Agent - 以下の 2 つの理由で Disk Agent をインストールする場合
 - Sybase Backup Server のファイルシステム バックアップを行うため。Data Protector Sybase 用統合ソフトウェアを構成し、Sybase Backup Server と Data Protector に関連するすべての問題点を解決する前に、このバックアップを行ってください。
 - Sybase Backup Server を使用してバックアップできない重要なデータがあるファイルシステムでのバックアップを実行するため。

Informix Server クライアント

Informix Server はすでに実行されているものとします。

Informix Server データベースをバックアップする場合は、インストール手順で以下の Data Protector コンポーネントを選択する必要があります。

- Informix 用統合ソフトウェア - Informix Server データベースをバックアップする場合
- Disk Agent - 以下の 2 つの理由で Disk Agent をインストールする場合
 - Informix Server のファイルシステム バックアップを行うため。Data Protector Informix 用統合ソフトウェアを構成し、Informix Server と Data Protector に関連するすべての問題点を解決する前に、このバックアップを行ってください。
 - ON-Bar を使用してバックアップできない重要な Informix Server データ (ONCONFIG ファイル、sqlhosts ファイル、ON-Bar 緊急ブート ファイル、oncfg_<INFORMIXSERVER>.<SERVERNUM>、構成ファイルなど) があるファイルシステムでのバックアップを実行するため。

SAP R/3 クライアント

SAP R/3 Database Server はすでに実行されているものとします。

注記

Data Protector の SAP R/3 用統合ソフトウェアのバックアップ仕様では、以前のバージョンの Data Protector に対する互換性が完全に確保されています。Data Protector では、旧バージョンの Data Protector で作成したバックアップ仕様をすべて実行できます。ただし、最新バージョンの Data Protector で作成したバックアップ仕様を、旧バージョンの Data Protector で使用することはできません。

SAP R/3 データベースをバックアップする場合は、インストール手順で以下のコンポーネントを選択する必要があります。

- SAP R/3 用統合ソフトウェア
- Oracle 用統合ソフトウェア

Oracle Recovery Manager を使用して SAP R/3 データベース ファイルのバックアップと復元を行う場合は、このコンポーネントをインストールしてください。

- Disk Agent

Data Protector では、Disk Agent をバックアップ サーバ (バックアップされるファイルシステム データがあるクライアント) にインストールする必要があります。

SAP DB クライアント

SAP DB サーバはすでに実行されているものとします。

SAP DB データベースをバックアップする場合は、インストール手順で以下の Data Protector コンポーネントを選択する必要があります。

- SAP DB 用統合ソフトウェア - SAP DB データベースの統合オンライン バックアップを実行する場合
- Disk Agent - SAP DB データベースの非統合オフライン バックアップを実行する場合

Oracle クライアント

Oracle Server はすでに実行されているものとします。

Oracle データベースをバックアップする場合は、インストール手順で Oracle 用統合ソフトウェア コンポーネントを選択する必要があります。

ネットワークへの Data Protector のインストール Data Protector 統合クライアントのインストール

orasbt.dll の確認

セットアップが完了したら、Oracle サービスを起動し、Data Protector データベース ライブラリの <Drive_Label>:\<%SystemRoot%\system32\orasbt.dll がロードされていることを確認する必要があります。

1. Windows Explorer で、<DriveLabel>:\<%SystemRoot%\system32 ディレクトリに切り替え、orasbt.dll を右クリックします。
2. [プロパティ] を選択し、[orasbt.dll プロパティ] ウィンドウから [バージョン] タブをクリックします。[説明] フィールドで、ファイルが Data Protector 用統合ソフトウェアの一部であるとして説明されていることを確認します。

orasbt.dll が適切にロードされていることを確認するため、ファイルをコピーしてから、元のファイルの削除を試みてください。ファイルが現在使用中であることを示すメッセージが表示されるはずですが。

図 2-20 エラー メッセージ



OpenVMS

『HP OpenView Storage Data Protector インテグレーション ガイド - Oracle、SAP』の手順に従って Oracle 用統合ソフトウェアのインストールと構成を完了したら、

OMNI\$ROOT:[CONFIG.CLIENT]omni_info に -key Oracle8 エントリが含まれていることを確認します。例を次に示します。

```
-key oracle8 -desc "Oracle Integration" -nlssset 159 -nlsId 12172 -flags 0x7  
-ntpath "" -uxpath "" -version A.06.00
```

このエントリが存在しない場合は、OMNI\$ROOT:[CONFIG.CLIENT]omni_format からコピーしてください。このエントリが含まれていないと、OpenVMS クライアント上で Oracle 用統合ソフトウェアがインストール済みとして示されません。

DB2 クライアント

DB2 Server はすでに実行されているものとします。

DB2 データベースをバックアップする場合は、インストール手順で DB2 用統合ソフトウェアコンポーネントおよび Disk Agent コンポーネントを選択する必要があります。

物理的にパーティション化された環境の場合は、データベースが置かれている各物理ノード (システム) に DB2 用統合ソフトウェアコンポーネントおよび Disk Agent コンポーネントをインストールします。

注記 root としてログオンした後、インストールを実行します。

NNM クライアント

NNM システムはすでに実行されているものとします。

NNM データベースをバックアップできるようにするには、インストール手順で HP OpenView NNM Backup 用統合ソフトウェア コンポーネントと Disk Agent コンポーネントを選択する必要があります。

NDMP クライアント

NDMP Server はすでに実行されているものとします。

インストール手順中で、NDMP Media Agent を選択し、NDMP 専用ドライブにアクセスするすべての Data Protector クライアントにインストールします。

注記 Data Protector クライアントが、NDMP Server を介した NDMP 専用ドライブへのアクセスに使用されず、ライブラリ ロボティクスの制御のみに使用される場合、そのようなクライアントには、NDMP Media Agent か General Media Agent のいずれかをインストールできます。

1 台の Data Protector クライアントには、1 つの Media Agent しかインストールできないことに、注意してください。

MS Volume Shadow Copy クライアント

前提条件

MS Volume Shadow Copy 用統合ソフトウェアは、Windows Server 2003 オペレーティング システムでサポートされています。

VSS 対応ライターのシャドウ コピー バックアップを実行する場合は、インストール手順で MS Volume Shadow Copy Integration コンポーネントを選択する必要があります。

VSS へ移すことが可能なようにバックアップを行う場合は、Windows Advanced Server 2003 が必要です。

バックアップ システムとアプリケーション システムに、

MS Volume Shadow Copy 用統合ソフトウェアと General Media Agent のコンポーネントをインストールしてください。

Lotus Notes/Domino Server クライアント

Lotus Notes/Domino Server はすでに実行されているものとします。

Lotus Notes/Domino Server データベースのバックアップを可能にするには、インストール手順で Lotus 用統合ソフトウェア コンポーネントと Disk Agent コンポーネントを選択する必要があります。以下の目的で、Data Protector でファイルシステム データをバックアップできるようにするには、Disk Agent コンポーネントが必要です。

- Lotus 統合エージェントを使用してバックアップできない重要なデータのバックアップを実行するため。これらは、非データベース ファイルと呼ばれており、notes.ini、desktop.dsk、すべての *.id ファイルなどがあります。Lotus Notes/Domino Server では、データを完全に保護するため、これらのファイルのバックアップを実行する必要があります。
- アプリケーションと Data Protector に関連する通信やその他の問題点を解決する目的で、ファイルシステム バックアップをテストするため。

EMC Symmetrix 用統合ソフトウェア

EMC Symmetrix を Data Protector と統合する場合は、以下の Data Protector ソフトウェア コンポーネントをアプリケーション システムとバックアップ システムにインストールします。

- EMC Symmetrix Agent (SYMA)

- General Media Agent

General Media Agent コンポーネントは、バルク データをバックアップする場合に、バックアップ システムにインストールします。またアーカイブ ログのバックアップやアプリケーション システムへの復元を行う場合は、アプリケーション システムにインストールします。

- Disk Agent

Disk Agent コンポーネントは、ディスク イメージおよびファイルシステムの ZDB を実行する場合に、アプリケーション システムとバックアップ システムにインストールします。Disk Agent がインストールされていないクライアントは、ZDB 仕様を作成する際に、[アプリケーション システム] ドロップダウン リストおよび [バックアップ システム] ドロップダウン リストには表示されません。

クラスタ環境でのインストール

EMC Symmetrix 用統合ソフトウェアは、クラスタ環境にインストールできます。サポート対象のクラスタ構成とインストール要件の詳細は、『HP OpenView Storage Data Protector Zero Downtime Backup Administrator's Guide』を参照してください。

他のアプリケーションとの統合

EMC Symmetrix 用統合ソフトウェアをデータベース アプリケーションと組み合わせてインストールする場合は、この組み合わせに必要な Data Protector コンポーネントをアプリケーション システムとバックアップ システムにインストールし、この組み合わせ特有のインストール作業を実行してください。EMC Symmetrix 用統合ソフトウェアは、Oracle と SAP R/3 と組み合わせてインストールできます。

EMC Symmetrix 用統合ソフトウェアと Oracle の組み合わせ

前提条件

- 以下のソフトウェアを、アプリケーション システムの非ミラー ディスクにインストールし、構成を完了しておく必要があります。
 - ✓ Oracle Enterprise Server (RDBMS)
 - ✓ Oracle Net8 ソフトウェア
 - ✓ SQL*Plus
- Oracle サーバ、および、SQL*NET V2 または NET8 は、インストールの最小要件です。

ネットワークへの Data Protector のインストール Data Protector 統合クライアントのインストール

- アプリケーション システムで使用される Oracle データベース ファイルは、バックアップ システムにミラーリングされる EMC Symmetrix デバイスにインストールする必要があります。

データベースは、ディスク イメージ、論理ボリューム、またはファイルシステムにインストールすることが可能です。以下の Oracle ファイルは、ミラーリングする必要があります。

- ✓ 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

アーカイブ REDO ログ ファイルは、非ミラー化ディスクに配置する必要があります。

インストール手順

インストール作業は、以下のとおり実行します。

1. Oracle のリカバリ カタログ データベースをインストールします。

アプリケーション システムの非ミラー化ディスクに Oracle のリカバリ カタログ データベースをインストールする方法については、Oracle のマニュアルを参照してください。リカバリ カタログは、登録しない状態で残しておきます。

2. 以下の Data Protector ソフトウェア コンポーネントをインストールします。

- EMC Symmetrix Agent - アプリケーション システムとバックアップ システムの両方にインストールします。
- Oracle 用統合ソフトウェア - バックアップ セットの ZDB メソッドを使用する場合、アプリケーション システムとバックアップ システムの両方にこのコンポーネントをインストールします。プロキシ コピーの ZDB メソッドを使用する場合は、アプリケーション システムのみにインストールします。

EMC Symmetrix 用統合ソフトウェアと SAP R/3 との組み合わせ

前提条件

- 以下の Oracle ソフトウェアを、アプリケーション システムにインストールし、構成を完了しておく必要があります。
 - ✓ Oracle Enterprise Server (RDBMS)
 - ✓ Oracle Net8 ソフトウェア
 - ✓ SQL*Plus

- アプリケーション システム上のデータベースは、ディスク イメージ、論理ボリューム、またはファイルシステムにインストールすることが可能です。Oracle データファイルは、ディスク アレイのソース ボリューム上に配置する必要があります。

オフライン バックアップを実行する場合は、制御ファイルとオンライン REDO ログ ファイルも、ディスク アレイ上に配置する必要があります。

アーカイブ REDO ログ ファイルは、ディスク アレイ上に配置する必要はありません。

- ユーザー ora<ORACLE_SID> を、プライマリ グループの dba 付きで、アプリケーション システムに作成する必要があります。

UNIX ユーザー <ORACLE_SID>adm を、UNIX グループ sapsys のメンバーとして、アプリケーション システムに作成する必要があります。

- SAP R/3 ソフトウェアは、アプリケーション システムに正しくインストールする必要があります。

SAP R/3 のインストール後にアプリケーション システムにインストールする必要がある標準ディレクトリのリストは、以下のとおりです。

注記 ディレクトリの場所は、環境変数によって変わります。詳細は、SAP R/3 のマニュアルを参照してください。

<ORACLE_HOME>/dbs - Oracle および SAP R/3 のプロファイル

<ORACLE_HOME>/bin - Oracle バイナリ ファイル

<SAPDATA_HOME>/sapbackup - BRBACKUP ログ ファイルが置かれる SAPBACKUP ディレクトリ

<SAPDATA_HOME>/saparch - BRARCHIVE ログ ファイルが置かれる SAPARCH ディレクトリ

<SAPDATA_HOME>/sapreorg

<SAPDATA_HOME>/sapcheck

<SAPDATA_HOME>/saptrace

/usr/sap/<ORACLE_SID>/SYS/exe/run

最後の 6 つのディレクトリが前述の場所がない場合は、適切なリンクを作成してください。

ネットワークへの Data Protector のインストール Data Protector 統合クライアントのインストール

ディレクトリ `/usr/sap/<ORACLE_SID>/SYS/exe/run` の所有者は、UNIX ユーザー `ora<ORACLE_SID>` でなければなりません。SAP R/3 ファイルの所有者は、UNIX ユーザー `ora<ORACLE_SID>` であり、`setuid` ビットがセットされた (`chmod 4755 ...`) UNIX グループ `dba` に属していなければなりません。例外は BRRESTORE ファイルの場合で、その所有者は UNIX ユーザー `<ORACLE_SID>adm` でなければなりません。

例：

`<ORACLE_SID>` が PROD の場合、`/usr/sap/<ORACLE_SID>/SYS/exe/run` ディレクトリ内のパーミッションは、以下のとおりを設定する必要があります。

```
-rwsr-xr-x 1 oraprod dba 4598276 Apr 17 1998 brarchive
-rwsr-xr-x 1 oraprod dba 4750020 Apr 17 1998 brbackup
-rwsr-xr-x 1 oraprod dba 4286707 Apr 17 1998 brconnect
-rwsr-xr-x 1 prodadm sapsys 430467 Apr 17 1998 brrestore
-rwsr-xr-x 1 oraprod dba 188629 Apr 17 1998 brtools
-rwsr-xr-x 1 oraprod dba 6081400 May 8 1998 sapdba.
```

インストール手順

インストール作業は、以下のとおり実行します。

1. SAP R/3 BRTOOLS を、アプリケーション システムにインストールします。
2. 以下の Data Protector ソフトウェア コンポーネントをインストールします。
 - EMC Symmetrix Agent - アプリケーション システムとバックアップ システムの両方にインストールします。
 - SAP R/3 用統合ソフトウェア - アプリケーション システムにのみインストールします。
 - Disk Agent - アプリケーション システムとバックアップ システムの両方にインストールします。

HP StorageWorks XP 用統合ソフトウェア

HP StorageWorks XP を Data Protector と統合する場合は、以下の Data Protector ソフトウェア コンポーネントを、アプリケーション システムとバックアップ システムの両方にインストールします。

- HP StorageWorks XP Agent
- General Media Agent

General Media Agent コンポーネントは、バルク データをバックアップする場合に、バックアップ システムにインストールします。またアーカイブ ログのバックアップやアプリケーション システムへの復元を行う場合は、アプリケーション システムにインストールします。

- Disk Agent

Disk Agent コンポーネントは、ディスク イメージおよびファイルシステムの ZDB を実行する場合に、アプリケーション システムとバックアップ システムにインストールします。Disk Agent がインストールされていないクライアントは、ZDB 仕様を作成する際に、[アプリケーション システム] ドロップダウン リストおよび [バックアップ システム] ドロップダウン リストに表示されません。

クラスタ環境でのインストール

HP StorageWorks XP 用統合ソフトウェアは、クラスタ環境にインストールできます。サポート対象のクラスタ構成とインストール要件の詳細は、『HP OpenView Storage Data Protector Zero Downtime Backup Administrator's Guide』を参照してください。

他のアプリケーションとの統合

HP StorageWorks XP 用統合ソフトウェアをデータベース アプリケーションと組み合わせてインストールする場合は、この組み合わせに必要な Data Protector コンポーネントをアプリケーション システムとバックアップ システムにインストールし、この組み合わせ特有のインストール作業を実行してください。HP StorageWorks XP 用統合ソフトウェアは、Oracle、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server と組み合わせてインストールできます。

HP StorageWorks XP 用統合ソフトウェアと Oracle の組み合わせ

前提条件

- 以下のソフトウェアを、アプリケーション システムのソース ボリュームにインストールし、構成を完了しておく必要があります。
 - ✓ Oracle Enterprise Server (RDBMS)
 - ✓ Oracle Net8 ソフトウェア
 - ✓ SQL*Plus
- Oracle サーバ、および、SQL*NET V2 または NET8 は、インストールの最小要件です。

ネットワークへの Data Protector のインストール Data Protector 統合クライアントのインストール

- アプリケーションシステムで使用される Oracle データベース ファイルは、バックアップ システムにミラーリングされる HP StorageWorks Disk Array XP LDEV にインストールする必要があります。

Oracle の制御ファイル、オンライン REDO ログ ファイル、および Oracle9i/10g SPFILE の配置場所は、次の 2 つのオプションから選択できます。

- Oracle 制御ファイル、オンライン REDO ログ ファイル、および Oracle9i/10g SPFILE を、Oracle データファイルとは異なるボリューム グループ (LVM を使用する場合) またはソース ボリュームに配置する。

この構成では、デフォルトでインスタント リカバリが使用可能です。

- Oracle 制御ファイル、オンライン REDO ログ ファイル、および Oracle9i/10g SPFILE を、Oracle データファイルと同じボリューム グループ (LVM を使用する場合) またはソース ボリュームに配置する。

この構成では、デフォルトではインスタント リカバリは使用不可です。インスタント リカバリを使用可能にするには、ZDB_ORA_INCLUDE_CF_OLF、ZDB_ORA_INCLUDE_SPF、および ZDB_ORA_NO_CHECKCONF_IR の各 omnirc 変数を設定します。詳細は『HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide』の付録を参照してください。

Oracle のアーカイブ REDO ログ ファイルは、ソース ボリュームに配置する必要はありません。

インストール手順

インストール作業は、以下のとおり実行します。

1. Oracle のリカバリ カタログ データベースをインストールします。

アプリケーションシステムの非ミラー化ディスクに Oracle のリカバリ カタログ データベースをインストールする方法については、Oracle のマニュアルを参照してください。リカバリ カタログは、登録しない状態で残しておきます。

2. 以下の Data Protector ソフトウェア コンポーネントをインストールします。

- HP StorageWorks XP Agent - アプリケーション システムとバックアップ システムの両方にインストールします。
- Oracle 用統合ソフトウェア - バックアップ セットの ZDB メソッドを使用する場合、アプリケーション システムとバックアップ システムの両方にこのコンポーネントをインストールします。プロキシ コピーの ZDB メソッドを使用する場合は、アプリケーション システムのみにインストールします。

HP StorageWorks XP 用統合ソフトウェアと SAP R/3 との組み合わせ

前提条件

- 以下の Oracle ソフトウェアをディスク アレイのソース ボリュームにインストールし、構成を完了しておく必要があります。

- ✓ Oracle Enterprise Server (RDBMS)
- ✓ Oracle Net8 ソフトウェア
- ✓ SQL*Plus

Oracle サーバ、および、SQL*NET V2 または NET8 は、インストールの最小要件です。

- アプリケーション システム上のデータベースは、ディスク イメージ、論理ボリューム、またはファイルシステムにインストールすることが可能です。Oracle データファイルは、ディスク アレイのソース ボリューム上に配置することが必要です。

オンラインバックアップを実行する場合は、制御ファイルとオンライン REDO ログ ファイルをディスク アレイ上に配置する必要はありません。

オフラインバックアップを実行する場合は、制御ファイルとオンライン REDO ログ ファイルを、ディスク アレイ上に配置することが必要です。ただし、以下の点に注意してください。

- Oracle8i/9i 制御ファイル、オンライン REDO ログ ファイル、および Oracle9i SPFILE を、Oracle8i/9i データファイルとは異なるボリューム グループ (LVM を使用する場合) またはソース ボリュームに配置する場合は、インスタント リカバリが使用可能です。
- Oracle8i/9i 制御ファイル、オンライン REDO ログ ファイル、および Oracle9i SPFILE を、Oracle8i/9i データファイルと同じボリューム グループ (LVM を使用する場合) またはソース ボリュームに配置する場合は、インスタント リカバリが使用不能です。インスタント リカバリを使用可能にするには、ZDB_ORA_INCLUDE_CF_OLF、ZDB_ORA_INCLUDE_SPF、および ZDB_ORA_NO_CHECKCONF_IR の各 omnirc 変数を設定します。詳細は『HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide』を参照してください。

アーカイブ REDO ログ ファイルは、ディスク アレイ上に配置する必要はありません。

- ユーザー ora<ORACLE_SID> を、プライマリ グループの dba 付きで、アプリケーション システムに作成する必要があります。

UNIX システムでは、UNIX ユーザー <ORACLE_SID>adm を、UNIX グループ sapsys のメンバーとして、アプリケーション システムに作成する必要があります。

ネットワークへの Data Protector のインストール Data Protector 統合クライアントのインストール

- SAP R/3 ソフトウェアは、アプリケーションシステムに正しくインストールする必要があります。

SAP R/3 のインストール後にアプリケーションシステムにインストールする必要がある標準ディレクトリのリストは、以下のとおりです。

注記 ディレクトリの場所は、環境変数 (UNIX システムの場合) またはレジストリ (Windows システムの場合) によって異なります。詳細は、SAP R/3 のマニュアルを参照してください。

<ORACLE_HOME>/dbs (UNIX システムの場合)

<ORACLE_HOME>%database (Windows システムの場合) - Oracle と SAP R/3 のプロファイル

<ORACLE_HOME>/bin or (UNIX システムの場合)

<ORACLE_HOME>%bin (Windows システムの場合) - Oracle のバイナリ

<SAPDATA_HOME>/sapbackup (UNIX システムの場合) または

<SAPDATA_HOME>%sapbackup (Windows システムの場合) - BRBACKUP ログファイルが置かれる SAPBACKUP ディレクトリ

<SAPDATA_HOME>/saparch (UNIX システムの場合) <SAPDATA_HOME>%saparch (Windows システムの場合) - BRARCHIVE ログファイルが置かれる SAPARCH ディレクトリ

<SAPDATA_HOME>/sapreorg (UNIX システムの場合) または <SAPDATA_HOME>%sapreorg (Windows システムの場合)

<SAPDATA_HOME>/sapcheck (UNIX システムの場合) または <SAPDATA_HOME>%sapcheck (Windows システムの場合)

<SAPDATA_HOME>/saptrace (UNIX システムの場合) または <SAPDATA_HOME>%saptrace (Windows システムの場合)

/usr/sap/<ORACLE_SID>/SYS/exe/run (UNIX システムの場合) または BRTOOLS (Windows システムの場合)

UNIX システム

UNIX システムでは、最後の 6 つのディレクトリが前述の場所がない場合、適切なリンクを作成してください。

UNIX システムの場合、ディレクトリ /usr/sap/<ORACLE_SID>/SYS/exe/run の所有者は、UNIX ユーザー ora<ORACLE_SID> でなければなりません。SAP R/3 ファイルの所有者は、UNIX ユーザー ora<ORACLE_SID> であり、setuid ビットがセットされた (chmod 4755 ...) UNIX グループ dba に属していなければなりません。例外は BRRESTORE ファイルの場合で、その所有者は UNIX ユーザー <ORACLE_SID>adm でなければなりません。

UNIX での例

<ORACLE_SID> が PROD の場合、/usr/sap/<ORACLE_SID>/SYS/exe/run ディレクトリ内のパーミッションは、以下のとおりに設定する必要があります。

```
-rwsr-xr-x 1 oraprod dba 4598276 Apr 17 1998 brarchive
-rwsr-xr-x 1 oraprod dba 4750020 Apr 17 1998 brbackup
-rwsr-xr-x 1 oraprod dba 4286707 Apr 17 1998 brconnect
-rwsr-xr-x 1 prodadm sapsys 430467 Apr 17 1998 brrestore
-rwsr-xr-x 1 oraprod dba 188629 Apr 17 1998 brtools
-rwsr-xr-x 1 oraprod dba 6081400 May 8 1998 sapdba.
```

Windows システム

Windows システムの場合、SAPMNT 共有がアプリケーション システム上に作成され、そこに <SAPDATA_HOME> サブディレクトリが含まれている必要があります。

インストール手順

インストール作業は、以下のとおり実行します。

1. SAP R/3 BRTOOLS を、アプリケーション システムにインストールします。
2. Data Protector 用統合ソフトウェアをインストールします。

Windows システムの場合、Data Protector ソフトウェア コンポーネントを SAP R/3 管理者用 ユーザー アカウントを使用してインストールする必要があります。また、このアカウントは、SAP R/3 インスタンスが実行されているシステム上の ORA_DBA ローカル グループか ORA_<SID>_DBA ローカル グループに含まれている必要があります。

以下の Data Protector ソフトウェア コンポーネントをインストールします。

- HP StorageWorks XP Agent - アプリケーション システムとバックアップ システムの両方にインストールします。
- SAP R/3 用統合ソフトウェア - アプリケーション システムにのみインストールします。
- Disk Agent - アプリケーション システムとバックアップ システムの両方にインストールします。

ネットワークへの Data Protector のインストール Data Protector 統合クライアントのインストール

HP StorageWorks XP 用統合ソフトウェアと Microsoft Exchange Server との組み合わせ

前提条件

Microsoft Exchange Server データベースは、アプリケーション システムの HP StorageWorks Disk Array XP ボリューム (LDEV) にインストールする必要があります。このボリュームは、バックアップ システムにミラーリングされます。ミラーリングは、BC または CA で設定でき、データベースはファイルシステムにインストールされます。以下のオブジェクトは、ミラーリングされるボリュームに配置する必要があります。

- Microsoft Information Store (MIS)
- Key Management Service (KMS) (オプション)
- Site Replication Service (SRS) (オプション)

トランザクション ログをバックアップする場合は、Microsoft Exchange Server の循環 ログを無効に設定します。

インストール手順

以下の Data Protector ソフトウェア コンポーネントをインストールします。

- HP StorageWorks XP Agent - アプリケーション システムとバックアップ システムの両方にインストールします。
- MS Exchange 2000/2003 用統合ソフトウェア - アプリケーション システムにのみインストールします。

HP StorageWorks XP 用統合ソフトウェアと Microsoft SQL Server との組み合わせ

前提条件

Microsoft SQL Server は、アプリケーション システムにインストールする必要があります。ユーザー データベースは、ディスク アレイのソース ボリュームに配置することが必要ですが、システム データベースは任意の場所にインストールできます。ただし、システム データベースがディスク アレイ上にもインストールされている場合は、システム データベースはユーザー データベースとは異なるソース ボリューム上にインストールすることが必要です。

インストール手順

以下の Data Protector ソフトウェア コンポーネントを、アプリケーション システムとバックアップ システムの両方にインストールします。

- HP StorageWorks XP Agent
- MS SQL 7.0/2000 用統合ソフトウェア

HP StorageWorks Virtual Array 用統合ソフトウェア

HP StorageWorks VA を Data Protector と統合する場合は、以下の Data Protector ソフトウェア コンポーネントをアプリケーション システムとバックアップ システムにインストールします。

- HP StorageWorks VA Agent
- General Media Agent

General Media Agent コンポーネントは、バルク データをバックアップする場合に、バックアップ システムにインストールします。またアーカイブ ログのバックアップやアプリケーション システムへの復元を行う場合は、アプリケーション システムにインストールします。

- Disk Agent

Disk Agent コンポーネントは、ディスク イメージおよびファイルシステムの ZDB を実行する場合に、アプリケーション システムとバックアップ システムにインストールします。

Disk Agent がインストールされていないクライアントは、ZDB 仕様を作成する際に、[アプリケーション システム] ドロップダウン リストおよび [バックアップ システム] ドロップダウン リストに表示されません。

クラスタ環境でのインストール

HP StorageWorks VA 用統合ソフトウェアは、クラスタ環境にインストールできます。サポート対象のクラスタ構成とインストール要件の詳細は、『HP OpenView Storage Data Protector Zero Downtime Backup Administrator's Guide』を参照してください。

他のアプリケーションとの統合

HP StorageWorks VA 用統合ソフトウェアをデータベース アプリケーションと組み合わせてインストールする場合は、この組み合わせに必要な Data Protector コンポーネントをアプリケーション システムとバックアップ システムにインストールし、この組み合わせ特有のインストール作業を実行してください。HP StorageWorks VA 用統合ソフトウェアは、Oracle、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server と組み合わせてインストールできます。

HP StorageWorks VA 用統合ソフトウェアと Oracle の組み合わせ

前提条件

- アプリケーションシステムのソース ボリュームと、バックアップ セットの ZDB メソッドのバックアップシステムには、以下のソフトウェアをインストールし、構成を完了しておく必要があります。

- ✓ Oracle Enterprise Server (RDBMS)
- ✓ Oracle Net8/9 ソフトウェア
- ✓ SQL*Plus

バックアップシステム上の Oracle ソフトウェアは、アプリケーションシステムと同じディレクトリにインストールする必要があります。また、バックアップシステム上のバイナリは、アプリケーションシステム上のバイナリと同一に設定する必要があります。これは、アプリケーションシステムからバックアップシステムにファイルとシステム環境をコピーするか、アプリケーションシステムと同じインストール パラメータを使用して、バックアップシステムで Oracle バイナリのクリーン インストールを実行することにより、実現できます。

Oracle サーバ、および、SQL*NET V2 または NET8/9 は、インストールの最小要件です。

- アプリケーションシステムで使用される Oracle データベース ファイルは、VA Agent (SNAPA) を使用してレプリケートされるソース ボリュームにインストールする必要があります。

Oracle の制御ファイル、オンライン REDO ログ ファイル、および Oracle9i/10g SPFILE の配置場所は、次の 2 つのオプションから選択できます。

- Oracle 制御ファイル、オンライン REDO ログ ファイル、および Oracle9i/10g SPFILE を、Oracle データファイルとは異なるボリューム グループ (LVM を使用する場合) またはソース ボリュームに配置する。

この構成では、デフォルトでインスタント リカバリが使用可能です。

- Oracle 制御ファイル、オンライン REDO ログ ファイル、および Oracle9i/10g SPFILE を、Oracle データファイルと同じボリューム グループ (LVM を使用する場合) またはソース ボリュームに配置する。

この構成では、デフォルトではインスタント リカバリは使用不可です。インスタント リカバリを使用可能にするには、ZDB_ORA_INCLUDE_CF_OLF、ZDB_ORA_INCLUDE_SPF_OLF、および ZDB_ORA_NO_CHECKCONF_IR の各 omnirc 変数を設定します。詳細は『HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide』の付録を参照してください。

Oracle のアーカイブ REDO ログ ファイルは、ソース ボリュームに配置する必要はありません。

インストール手順

インストール作業は、以下のとおり実行します。

1. Oracle のリカバリ カタログ データベースをインストールします。

アプリケーション システムに Oracle のリカバリ カタログ データベースをインストールする方法については、Oracle のマニュアルを参照してください。リカバリ カタログは、登録しない状態で残しておきます。

2. 以下の Data Protector ソフトウェア コンポーネントをインストールします。

- HP StorageWorks VA Agent - アプリケーション システムとバックアップ システムの両方にインストールします。
- Oracle 用統合ソフトウェア - バックアップ セットの ZDB メソッドを使用する場合、アプリケーション システムとバックアップ システムの両方にこのコンポーネントをインストールします。プロキシ コピーの ZDB メソッドを使用する場合は、アプリケーション システムのみにインストールします。

HP StorageWorks VA 用統合ソフトウェアと SAP R/3 との組み合わせ

前提条件

- 以下の Oracle ソフトウェアを、アプリケーション システムのソース ボリュームにインストールする必要があります。

- ✓ Oracle Enterprise Server (RDBMS)
- ✓ Oracle Net8 ソフトウェア
- ✓ SQL*Plus

Oracle サーバ、および、SQL*NET V2 または NET8 は、インストールの最小要件です。

- アプリケーション システム上のデータベースは、ディスク イメージ、論理ボリューム、またはファイルシステムにインストールすることが可能です。Oracle データファイルは、ディスク アレイのソース ボリューム上に配置することが必要です。

オンラインバックアップを実行する場合は、制御ファイルとオンライン REDO ログ ファイルをディスク アレイ上に配置する必要はありません。

ネットワークへの Data Protector のインストール Data Protector 統合クライアントのインストール

オフラインバックアップを実行する場合は、制御ファイルとオンライン REDO ログ ファイルを、ディスク アレイ上に配置する必要があります。ただし、以下の点に注意してください。

- Oracle8i/9i 制御ファイル、オンライン REDO ログ ファイル、および Oracle9i SPFILE を、Oracle8i/9i データファイルとは異なるボリューム グループ (LVM を使用する場合) またはソース ボリュームに配置する場合は、インスタント リカバリが使用可能です。
- Oracle8i/9i 制御ファイル、オンライン REDO ログ ファイル、および Oracle9i SPFILE を、Oracle8i/9i データファイルと同じボリューム グループ (LVM を使用する場合) またはソース ボリュームに配置する場合は、インスタント リカバリが使用不能です。インスタント リカバリを使用可能にするには、ZDB_ORA_INCLUDE_CF_OLF、ZDB_ORA_INCLUDE_SPF、および ZDB_ORA_NO_CHECKCONF_IR の各 omnirc 変数を設定します。詳細は『HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide』を参照してください。

アーカイブ REDO ログ ファイルは、ディスク アレイ上に配置する必要はありません。

- ユーザー ora<ORACLE_SID> を、プライマリ グループの dba 付きで、アプリケーションシステムに作成する必要があります。

UNIX システムでは、UNIX ユーザー <ORACLE_SID>adm を、UNIX グループ sapsys のメンバーとして、アプリケーションシステムに作成する必要があります。

- SAP R/3 ソフトウェアは、アプリケーションシステムに正しくインストールする必要があります。

SAP R/3 のインストール後にアプリケーションシステムにインストールする必要がある標準ディレクトリのリストは、以下のとおりです。

注記 ディレクトリの場所は、環境変数 (UNIX システムの場合) またはレジストリ (Windows システムの場合) によって異なります。詳細は、SAP R/3 のマニュアルを参照してください。

<ORACLE_HOME>/dbs (UNIX システムの場合)

<ORACLE_HOME>¥database (Windows システムの場合) - Oracle と SAP のプロファイル

<ORACLE_HOME>/bin (UNIX システムの場合)

<ORACLE_HOME>¥bin (Windows システムの場合) - Oracle のバイナリ

<SAPDATA_HOME>/sapbackup (UNIX システムの場合)

<SAPDATA_HOME>%sapbackup (Windows システムの場合) - BRBACKUP ログ ファイルが置かれる SAPBACKUP ディレクトリ

<SAPDATA_HOME>/saparch (UNIX システムの場合) <SAPDATA_HOME>%saparch (Windows システムの場合) - BRARCHIVE ログ ファイルが置かれる SAPARCH ディレクトリ

<SAPDATA_HOME>/sapreorg (UNIX システムの場合) または <SAPDATA_HOME>%sapreorg (Windows システムの場合)

<SAPDATA_HOME>/sapcheck (UNIX システムの場合) または <SAPDATA_HOME>%sapcheck (Windows システムの場合)

<SAPDATA_HOME>/saptrace (UNIX システムの場合) または <SAPDATA_HOME>%saptrace (Windows システムの場合)

/usr/sap/<ORACLE_SID>/SYS/exe/run (UNIX システムの場合) または BRTOOLS (Windows システムの場合)

UNIX システム

UNIX システムでは、最後の 6 つのディレクトリが前述の場所がない場合、適切なリンクを作成してください。

UNIX システムの場合、ディレクトリ /usr/sap/<ORACLE_SID>/SYS/exe/run の所有者は、UNIX ユーザー ora<ORACLE_SID> でなければなりません。SAP R/3 ファイルの所有者は、UNIX ユーザー ora<ORACLE_SID> であり、setuid ビットがセットされた (chmod 4755 ...) UNIX グループ dba に属していなければなりません。例外は BRRESTORE ファイルの場合で、その所有者は UNIX ユーザー <ORACLE_SID>adm でなければなりません。

UNIX での例

<ORACLE_SID> が PROD の場合、/usr/sap/<ORACLE_SID>/SYS/exe/run ディレクトリ内のパーミッションは、以下のとおりに設定する必要があります。

```
-rwsr-xr-x 1 oraprod dba 4598276 Apr 17 1998 brarchive
-rwsr-xr-x 1 oraprod dba 4750020 Apr 17 1998 brbackup
-rwsr-xr-x 1 oraprod dba 4286707 Apr 17 1998 brconnect
-rwsr-xr-x 1 prodadm sapsys 430467 Apr 17 1998 brrestore
-rwsr-xr-x 1 oraprod dba 188629 Apr 17 1998 brtools
-rwsr-xr-x 1 oraprod dba 6081400 May 8 1998 sapdba.
```

ネットワークへの Data Protector のインストール Data Protector 統合クライアントのインストール

Windows システム

Windows システムの場合、SAPMNT 共有がアプリケーション システム上に作成され、そこに <SAPDATA_HOME> サブディレクトリが含まれている必要があります。

インストール手順

インストール作業は、以下のとおり実行します。

1. SAP R/3 BRTOOLS を、アプリケーション システムにインストールします。
2. Data Protector 用統合ソフトウェアをインストールします。

Windows システムの場合、Data Protector ソフトウェア コンポーネントを SAP R/3 管理者用 ユーザー アカウントを使用してインストールする必要があります。また、このアカウントは、SAP R/3 インスタンスが実行されているシステム上の ORA_DBA ローカル グループか ORA_<SID>_DBA ローカル グループに含まれている必要があります。

以下の Data Protector ソフトウェア コンポーネントをインストールします。

- HP StorageWorks VA Agent - アプリケーション システムとバックアップ システムの両方にインストールします。
- SAP R/3 用統合ソフトウェア - アプリケーション システムにのみインストールします。
- Disk Agent - アプリケーション システムとバックアップ システムの両方にインストールします。

HP StorageWorks VA 用統合ソフトウェアと Microsoft Exchange Server との組み合わせ

前提条件

Microsoft Exchange Server データベースは、アプリケーション システムのソース ボリューム上にインストールする必要があります。以下のオブジェクトは、ソース ボリュームに配置する必要があります。

- Microsoft Information Store (MIS)
- Key Management Service (KMS) (オプション)
- Site Replication Service (SRS) (オプション)

トランザクション ログをバックアップする場合は、Microsoft Exchange Server の循環 ログを無効に設定します。

インストール手順

以下の Data Protector ソフトウェア コンポーネントをインストールします。

- HP StorageWorks VA Agent - アプリケーション システムとバックアップ システムの両方にインストールします。
- MS Exchange 2000/2003 用統合ソフトウェア - アプリケーション システムにのみインストールします。

HP StorageWorks VA 用統合ソフトウェアと Microsoft SQL Server との組み合わせ

前提条件

Microsoft SQL Server は、アプリケーション システムにインストールする必要があります。ユーザー データベースは、ディスク アレイのソース ボリュームに配置することが必要ですが、システム データベースは任意の場所にインストールできます。ただし、システム データベースがディスク アレイ上にもインストールされている場合は、システム データベースはユーザー データベースとは異なるソース ボリューム上にインストールする必要があります。

インストール手順

以下の Data Protector ソフトウェア コンポーネントを、アプリケーション システムとバックアップ システムの両方にインストールします。

- HP StorageWorks VA Agent
- MS SQL 7.0/2000 用統合ソフトウェア

HP StorageWorks Enterprise Virtual Array 用統合ソフトウェア

HP StorageWorks EVA を Data Protector と統合する場合は、HP 以下の Data Protector ソフトウェア コンポーネントをアプリケーション システムとバックアップ システムにインストールします。

- HP StorageWorks EVA SMI-S Agent
- General Media Agent

General Media Agent コンポーネントは、バルク データをバックアップする場合に、バックアップ システムにインストールします。またアーカイブ ログのバックアップやアプリケーション システムへの復元を行う場合は、アプリケーション システムにインストールします。

- Disk Agent

ネットワークへの Data Protector のインストール Data Protector 統合クライアントのインストール

Disk Agent コンポーネントは、ディスク イメージおよびファイルシステムの ZDB を実行する場合に、アプリケーション システムとバックアップ システムにインストールします。Disk Agent がインストールされていないクライアントは、ZDB 仕様を作成する際に、[アプリケーション システム] ドロップダウン リストおよび [バックアップ システム] ドロップダウン リストに表示されません。

クラスタ環境でのインストール

HP StorageWorks EVA 用統合ソフトウェアは、クラスタ環境にインストールできます。サポート対象のクラスタ構成とインストール要件の詳細は、『HP OpenView Storage Data Protector Zero Downtime Backup Administrator's Guide』を参照してください。

他のアプリケーションとの統合

HP StorageWorks EVA 用統合ソフトウェアをデータベース アプリケーションと組み合わせてインストールする場合は、この組み合わせに必要な Data Protector コンポーネントをアプリケーション システムとバックアップ システムにインストールし、この組み合わせ特有のインストール作業を実行してください。HP StorageWorks EVA 用統合ソフトウェアは、Oracle、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server、Microsoft VSS と組み合わせてインストールできます。

HP StorageWorks EVA 用統合ソフトウェアと Oracle の組み合わせ

前提条件

- 以下の Oracle ソフトウェアを、アプリケーション システムのソース ボリュームにインストールする必要があります。
 - ✓ Oracle Enterprise Server (RDBMS)
 - ✓ Oracle Net8 ソフトウェア
 - ✓ SQL*Plus
- Oracle サーバ、および、SQL*NET V2 または NET8 は、インストールの最小要件です。
- アプリケーション システムで使用される Oracle データファイルは、インストールした SMI-S Agent を使用してレプリケートされるソース ボリュームにインストールする必要があります。

Oracle の制御ファイル、オンライン REDO ログ ファイル、および Oracle9i/10g SPFILE の配置場所は、次の 2 つのオプションから選択できます。

- Oracle 制御ファイル、オンライン REDO ログ ファイル、および Oracle9i/10g SPFILE を、Oracle データファイルとは異なるボリューム グループ (LVM を使用する場合) またはソース ボリュームに配置する。

この構成では、デフォルトでインスタント リカバリが使用可能です。

- Oracle 制御ファイル、オンライン REDO ログ ファイル、および Oracle9i/10g SPFILE を、Oracle データファイルと同じボリューム グループ (LVM を使用する場合) またはソース ボリュームに配置する。

この構成では、デフォルトではインスタント リカバリは使用不可です。インスタント リカバリを使用可能にするには、ZDB_ORA_INCLUDE_CF_OLF、ZDB_ORA_INCLUDE_SPF、および ZDB_ORA_NO_CHECKCONF_IR の各 omnirc 変数を設定します。詳細は『HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide』の付録を参照してください。

Oracle のアーカイブ REDO ログ ファイルは、ソース ボリュームに配置する必要はありません。

インストール手順

インストール作業は、以下のとおり実行します。

1. Oracle のリカバリ カタログ データベースをインストールします。

アプリケーション システムに Oracle のリカバリ カタログ データベースをインストールする方法については、Oracle のマニュアルを参照してください。リカバリ カタログは、登録しない状態で残しておきます。

2. 以下の Data Protector ソフトウェア コンポーネントをインストールします。

- HP StorageWorks EVA SMI-S Agent - アプリケーション システムとバックアップ システムの両方にインストールします。
- Oracle 用統合ソフトウェア - バックアップ セットの ZDB メソッドを使用する場合、アプリケーション システムとバックアップ システムの両方にこのコンポーネントをインストールします。プロキシ コピーの ZDB メソッドを使用する場合は、アプリケーション システムのみにインストールします。

HP StorageWorks EVA 用統合ソフトウェアと SAP R/3 との組み合わせ

前提条件

- 以下の Oracle ソフトウェアを、アプリケーション システムのソース ボリュームにインストールする必要があります。

- ✓ Oracle Enterprise Server (RDBMS)
- ✓ Oracle Net8 ソフトウェア
- ✓ SQL*Plus

RDBMS、および、SQL*NET V2 または NET8 は、インストールの最小要件です。

- アプリケーション システム上のデータベースは、ディスク イメージ、論理ボリューム、またはファイルシステムにインストールすることが可能です。Oracle データファイルは、ディスク アレイのソース ボリューム上に配置することが必要です。

オンラインバックアップを実行する場合は、制御ファイルとオンライン REDO ログ ファイルをディスク アレイ上に配置する必要はありません。

オフラインバックアップを実行する場合は、制御ファイルとオンライン REDO ログ ファイルを、ディスク アレイ上に配置することが必要です。ただし、以下の点に注意してください。

- Oracle8i/9i 制御ファイル、オンライン REDO ログ ファイル、および Oracle9i SPFILE を、Oracle8i/9i データファイルとは異なるボリューム グループ (LVM を使用する場合) またはソース ボリュームに配置する場合は、インスタント リカバリが使用可能です。
- Oracle8i/9i 制御ファイル、オンライン REDO ログ、および Oracle9i SPFILE を、Oracle8i/9i データファイルと同じボリューム グループ (LVM を使用する場合) またはソース ボリュームに配置する場合は、インスタント リカバリが使用不能です。インスタント リカバリを使用可能にするには、ZDB_ORA_INCLUDE_CF_OLF、ZDB_ORA_INCLUDE_SPF、および ZDB_ORA_NO_CHECKCONF_IR omnirc 変数を設定します。詳細は『HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide』を参照してください。

アーカイブ REDO ログ ファイルは、ディスク アレイ上に配置する必要はありません。

- ユーザー ora<ORACLE_SID> を、プライマリ グループの dba 付きで、アプリケーション システムに作成する必要があります。

UNIX システムでは、UNIX ユーザー <ORACLE_SID>adm を、UNIX グループ sapsys のメンバーとして、アプリケーション システムに作成する必要があります。

- SAP R/3 ソフトウェアは、アプリケーションシステムに正しくインストールする必要があります。

SAP R/3 のインストール後にアプリケーションシステムにインストールする必要がある標準ディレクトリのリストは、以下のとおりです。

注記 ディレクトリの場所は、環境変数 (UNIX システムの場合) またはレジストリ (Windows システムの場合) によって異なります。詳細は、SAP R/3 のマニュアルを参照してください。

<ORACLE_HOME>/dbs (UNIX システムの場合)

<ORACLE_HOME>%database (Windows システムの場合) - Oracle と SAP のプロファイル

<ORACLE_HOME>/bin (UNIX システムの場合)

<ORACLE_HOME>%bin (Windows システムの場合) - Oracle のバイナリ

<SAPDATA_HOME>/sapbackup (UNIX システムの場合) または

<SAPDATA_HOME>%sapbackup (Windows システムの場合) - BRBACKUP ログファイルが置かれる SAPBACKUP ディレクトリ

<SAPDATA_HOME>/saparch (UNIX システムの場合) <SAPDATA_HOME>%saparch (Windows システムの場合) - BRARCHIVE ログファイルが置かれる SAPARCH ディレクトリ

<SAPDATA_HOME>/sapreorg (UNIX システムの場合) または <SAPDATA_HOME>%sapreorg (Windows システムの場合)

<SAPDATA_HOME>/sapcheck (UNIX システムの場合) または <SAPDATA_HOME>%sapcheck (Windows システムの場合)

<SAPDATA_HOME>/saptrace (UNIX システムの場合) または <SAPDATA_HOME>%saptrace (Windows システムの場合)

/usr/sap/<ORACLE_SID>/SYS/exe/run (UNIX システムの場合)

BRTOOLS (Windows システムの場合)

UNIX システム

UNIX システムでは、最後の 6 つのディレクトリが前述の場所がない場合、適切なリンクを作成してください。

ネットワークへの Data Protector のインストール Data Protector 統合クライアントのインストール

UNIX システムの場合、ディレクトリ `/usr/sap/<ORACLE_SID>/SYS/exe/run` の所有者は、UNIX ユーザー `ora<ORACLE_SID>` でなければなりません。SAP R/3 ファイルの所有者は、UNIX ユーザー `ora<ORACLE_SID>` であり、`setuid` ビットがセットされた (`chmod 4755 ...`) UNIX グループ `dba` に属していなければなりません。例外は `BRRESTORE` ファイルの場合で、その所有者は UNIX ユーザー `<ORACLE_SID>adm` でなければなりません。

UNIX での例

`<ORACLE_SID>` が `PROD` の場合、`/usr/sap/<ORACLE_SID>/SYS/exe/run` ディレクトリ内のパーミッションは、以下のとおりに設定する必要があります。

```
-rwsr-xr-x 1 oraprod dba 4598276 Apr 17 1998 brarchive
-rwsr-xr-x 1 oraprod dba 4750020 Apr 17 1998 brbackup
-rwsr-xr-x 1 oraprod dba 4286707 Apr 17 1998 brconnect
-rwsr-xr-x 1 prodadm sapsys 430467 Apr 17 1998 brrestore
-rwsr-xr-x 1 oraprod dba 188629 Apr 17 1998 brtools
-rwsr-xr-x 1 oraprod dba 6081400 May 8 1998 sapdba.
```

Windows システム

Windows システムの場合、`SAPMNT` 共有がアプリケーション システム上に作成され、そこに `<SAPDATA_HOME>` サブディレクトリが含まれている必要があります。

インストール手順

インストール作業は、以下のとおり実行します。

1. SAP R/3 `BRTOOLS` を、アプリケーション システムにインストールします。
2. Data Protector 用統合ソフトウェアをインストールします。

Windows システムの場合、Data Protector ソフトウェア コンポーネントを SAP R/3 管理者用 ユーザー アカウントを使用してインストールする必要があります。また、このアカウントは、SAP R/3 インスタンスが実行されているシステム上の `ORA_DBA` ローカル グループか `ORA_<SID>_DBA` ローカル グループに含まれている必要があります。

以下の Data Protector ソフトウェア コンポーネントをインストールします。

- HP StorageWorks EVA SMI-S Agent - アプリケーション システムとバックアップ システムの両方にインストールします。
- SAP R/3 用統合ソフトウェア - アプリケーション システムにのみインストールします。
- Disk Agent - アプリケーション システムとバックアップ システムの両方にインストールします。

HP StorageWorks EVA 用統合ソフトウェアと Microsoft Exchange Server との組み合わせ

前提条件

Microsoft Exchange Server データベースは、アプリケーション システムのソース ボリューム上にインストールする必要があります。以下のオブジェクトは、ソース ボリュームに配置する必要があります。

- Microsoft Information Store (MIS)
- Key Management Service (KMS) (オプション)
- Site Replication Service (SRS) (オプション)

トランザクション ログをバックアップする場合は、Microsoft Exchange Server の循環ログを無効に設定します。

インストール手順

以下の Data Protector ソフトウェア コンポーネントをインストールします。

- HP StorageWorks EVA SMI-S Agent - アプリケーション システムとバックアップ システムの両方にインストールします。
- MS Exchange 2000/2003 用統合ソフトウェア - アプリケーション システムにのみインストールします。

HP StorageWorks EVA 用統合ソフトウェアと MS SQL との組み合わせ

前提条件

Microsoft SQL Server は、アプリケーション システムにインストールする必要があります。ユーザー データベースは、ディスク アレイのソース ボリュームに配置することが必要ですが、システム データベースは任意の場所にインストールできます。ただし、システム データベースがディスク アレイ上にもインストールされている場合は、システム データベースはユーザー データベースとは異なるソース ボリューム上にインストールすることが必要です。

インストール手順

以下の Data Protector ソフトウェア コンポーネントを、アプリケーション システムとバックアップ システムの両方にインストールします。

- HP StorageWorks EVA SMI-S Agent - アプリケーション システムとバックアップ システムの両方にインストールします。
- MS SQL 7.0/2000 用統合ソフトウェア

各国語版 Data Protector ユーザー インタフェースのインストール

Data Protector A.06.00 には、Windows および UNIX システム上で動作する各国語版 Data Protector ユーザー インタフェースがあります。各国語版ユーザー インタフェースには、Data Protector GUI と CLI があるほか、各国語版のオンラインヘルプと印刷ドキュメントも提供されています。各国語版にローカライズされた Data Protector マニュアルについては、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。

注記 Data Protector のインストール時、デフォルトでは英語サポートがインストールされます。これに加えて他の言語サポートもインストールすると、Data Protector ユーザー インタフェースはシステムの地域設定にあわせて起動されます。

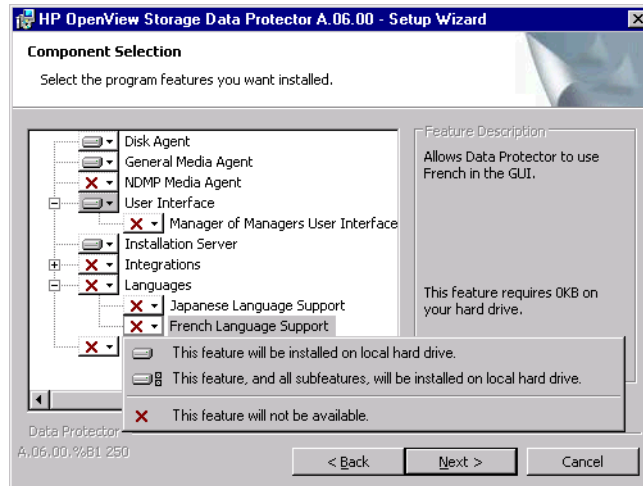
Windows システムへの各国語版 Data Protector ユーザー インタフェースのインストール

ローカル インストール

Windows システムに各国語版 Data Protector ユーザー インタフェースをインストールするには、セットアップウィザードの [Component Selection] ページで、必要な言語サポート (フランス語または日本語) を選択します。図 2-21 を参照してください。

ローカル インストール手順は、19 ページの「Data Protector Cell Manager (CM) およびインストールサーバ (IS) のインストール」を参照してください。

図 2-21 セットアップ時の言語サポートの選択



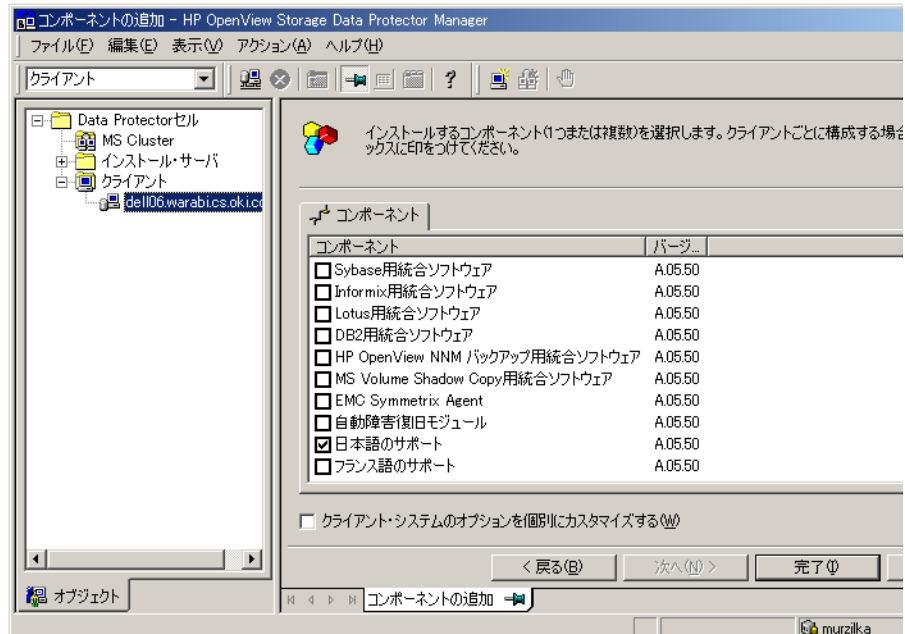
リモート インストール

インストールサーバを利用して Data Protector 言語サポートをリモートで配布するには、[コンポーネント追加] ウィザードの [コンポーネント選択] ページで、必要な言語サポートを選択します。図 2-22 を参照してください。

ネットワークへの Data Protector のインストール 各国語版 Data Protector ユーザー インタフェースのインストール

Data Protector ソフトウェア コンポーネントをクライアントにリモートで追加する手順は、50 ページの「Data Protector クライアントのリモート インストール」を参照してください。

図 2-22 言語サポートのリモート インストール



UNIX システムへの各国語版 Data Protector ユーザー インタフェースのインストール

ローカル インストール

日本語またはフランス語のサポートのローカル インストールは、`omnisetup.sh` コマンドを使用して、Data Protector クライアント上でのみ行えます。必要な言語サポートに応じて、`jpn_ls` または `fra_ls` ソフトウェア コンポーネントを指定してください。手順の詳細は、119 ページの「UNIX クライアントのローカル インストール」を参照してください。

Data Protector Cell Manager またはインストール サーバのインストールに `swinstall`、`pkgadd`、または `rpm` ユーティリティを使用している場合は、英語サポートしかインストールできません。各国語版 Data Protector ユーザー インタフェースを Cell Manager またはインストール サーバと同じシステムにインストールしたい場合は、それらの言語サポートをリモートでインストールする必要があります。

リモート インストール

インストール サーバを利用して Data Protector 言語サポートをリモートで配布するには、[コンポーネント追加] ウィザードの [コンポーネント選択] ページで、必要な言語サポートを選択します。図 2-22 を参照してください。

Data Protector ソフトウェア コンポーネントをクライアントにリモートで追加する手順は、50 ページの「Data Protector クライアントのリモート インストール」を参照してください。

トラブルシューティング

英語以外の言語サポートをインストールした後、英語の Data Protector ユーザー インタフェースが起動した場合は、以下を確認してください。

1. 以下のファイルが存在するかを確認します。

フランス語のサポートの場合

- Windows の場合 : `<Data_Protector_home>%bin%OmniFra.dll`
- HP-UX の場合 : `/opt/omni/lib/nls/fr.iso88591/omni.cat`
- Solaris の場合 : `/opt/omni/lib/nls/fr.ISO8859-1/omni.cat`

日本語のサポートの場合

- Windows の場合 : `<Data_Protector_home>%bin%OmniJpn.dll`
- HP-UX の場合 : `/opt/omni/lib/nls/ja.eucJP/omni.cat` および `/opt/omni/lib/nls/ja.SJIS/omni.cat`
- Solaris の場合 : `/opt/omni/lib/nls/ja.eucJP/omni.cat` および `/opt/omni/lib/nls/ja.PCK/omni.cat`

2. システムの地域設定を確認します。

- Windows の場合 : Windows の **コントロール パネル** で、[**地域のオプション**] をクリックし、地域と言語の設定で適切な言語が選択されているかを確認してください。
- UNIX の場合 : 以下のコマンドを実行して地域設定 (ロケール) 環境を設定してください。

ネットワークへの Data Protector のインストール 各国語版 Data Protector ユーザー インタフェースのインストール

```
export LANG=<lang>  
locale
```

ここで、<lang>には、地域設定を次の形式で指定します。

```
language[_territory].codeset
```

例: ja_JP.eucJP、ja_JP.SJIS、または ja_JP.PCK(日本語の場合)、
fr_FR.iso88591(フランス語の場合)。LANG 変数の codeset 部分は必須であり、対応するディレクトリ名の codeset 部分と一致している必要があります。

Data Protector シングルサーバ版のインストール

Data Protector のシングルサーバ版 (SSE: Single Server Edition) は、1 つの Cell Manager に接続された 1 台のデバイス上でのみバックアップを実行するような、小規模な環境向けに設計されたものです。シングルサーバ版は、サポート対象の Windows プラットフォーム、およびサポート対象の HP-UX または Solaris プラットフォーム上で使用できます。

Cell Manager と (必要に応じて) インストール サーバをインストールする手順は、19 ページの「Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール」を参照してください。

制限事項

SSE ライセンスを使用する場合、以下の制限があることに注意してください。

Windows 用 SSE の制限

- SSE でバックアップを行う場合、一度にバックアップできるのは 1 台の Cell Manager に接続されている 1 台のデバイスのみです。
- 10 スロットの DDS オートチェンジャを 1 台だけ使用できます。
- UNIX (HP-UX) クライアントとサーバはサポートされていません。UNIX のマシンに対してバックアップを行おうとすると、セッションが中止されます。
- Windows 用 Cell Manager を使用するセルの場合は、バックアップ対象は Windows クライアントに限られます。Novell Netware クライアントへのバックアップはサポートされていません。
- 拡張製品を SSE に追加することはできません。
- SSE でクラスタ化を行うことはできません。
- SSE で障害復旧を行うことはできません。

Windows クライアントの数に制限はありません。

サポート対象のデバイスについては、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス』を参照してください。

HP-UX および Solaris 用の SSE の制限事項

- SSE でバックアップを行う場合、一度にバックアップできるのは 1 台の Cell Manager に接続されている 1 台のデバイスのみです。
- 10 スロットの DDS オートチェンジャを 1 台だけ使用できます。
- UNIX 用 Cell Manager では、サーバのバックアップはできません。UNIX、Windows、Solaris、および Novell NetWare の各クライアントのバックアップのみが可能です。
- 拡張製品を SSE に追加することはできません。
- SSE でクラスタ化を行うことはできません。

クライアント (UNIX、Windows) の数に制限はありません。

サポート対象のデバイスについては、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス』を参照してください。

パスワードのインストール

Cell Manager へのパスワードの詳細なインストール手順は、308 ページの「Data Protector のパスワード」を参照してください。

Data ProtectorWeb Reporting のインストール

Data Protector Web Reporting は、デフォルトで他の Data Protector コンポーネントとともにローカルシステムにインストールされます。

したがって、システムからローカルに使用する場合は、このコンポーネントを明示的にインストールする必要はありません。Data Protector Web Reporting は、Web サーバにもインストールできます。

前提条件

システムで Data Protector Web Reporting を使用する場合の前提条件と制限は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。

インストール

Data Protector Web Reporting を Web サーバにインストールするには、以下の手順に従ってください。

1. 以下の Data Protector Java Reporting ファイルをサーバにコピーします。コピー先のサーバは、Data Protector クライアントでなくてもかまいません。
 - Windows 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ている場合は、以下のディレクトリから Web Reporting 用のファイルをコピーします。

```
<Data_Protector_home>%java%bin
```

- UNIX 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ている場合は、以下のディレクトリから Web Reporting 用のファイルをコピーします。

```
/opt/omni/java/bin
```

2. ブラウザで ebReporting.html ファイルを開くと、Data ProtectorWeb Reporting が表示されます。

このファイルは、Web Reporting のユーザーが完全な URL を通じてアクセスできるように設定しておく必要があります。たとえば、イントラネット サイトからこのファイルにアクセスするためのリンクなどを用意します。

ネットワークへの Data Protector のインストール Data Protector Web Reporting のインストール

ヒント デフォルトでは、Data Protector Web Reporting はパスワードなしで使用できます。Web Reporting へのアクセスを制限したい場合は、パスワード保護を追加できます。手順の詳細は、オンライン ヘルプの索引キーワード「Web レポート, ~へのアクセスを制限」で表示される内容を参照してください。

この次に行う作業

インストールが完了したら、オンライン ヘルプの索引キーワード「Web レポート インタフェース, 通知の構成」で表示される内容を参照して、必要な構成作業を実施し、レポートを作成してください。

MC/ServiceGuard への Data Protector のインストール

Data Protector は、HP-UX 用および Linux 用の MC/ServiceGuard (MC/SG) をサポートしています。サポート対象オペレーティング システムのバージョンの詳細は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。

Cell Manager をクラスタ対応にする場合は、ライセンスで仮想サーバ IP アドレスを使用する必要があります。

クラスタ対応 Cell Manager のインストール

前提条件

MC/ServiceGuard に Data Protector Cell Manager をインストールする前に、以下の条件が満たされていることを確認してください。

- ✓ 1 次 Cell Manager となるシステムと 2 次 Cell Manager となるシステムが決定されていること。これらのシステムのすべては、MC/ServiceGuard がインストールされ、クラスタのメンバーとして構成されていること。
- ✓ Data Protector Cell Manager (推奨パッチ適用済み) と、クラスタ内に必要な統合ソフトウェア用のその他すべての Data Protector ソフトウェア コンポーネントが、1 次ノードと各 2 次ノードにインストールされていること。

これらのインストール手順は、Cell Manager システムを標準構成でインストールする場合と同じです。詳細は 19 ページの「Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール」を参照してください。

この次に行う作業

インストールが完了したら、インストールした 1 次 Cell Manager と 2 次 Cell Manager、および Cell Manager パッケージを構成する必要があります。MC/ServiceGuard を Data Protector とともに構成する方法は、オンライン ヘルプの索引キーワード「クラスタ、MC/ServiceGuard」で表示される内容を参照してください。

クラスタ対応クライアントのインストール

重要 Data Protector クラスタ対応クライアントは、クラスタ内のすべてのノードにインストールする必要があります。

インストール手順は、Data Protector を標準構成の UNIX クライアントにインストールする場合と同じです。手順の詳細は、68 ページの「HP-UX クライアントのインストール」および 79 ページの「Linux クライアントのインストール」を参照してください。

この次に行う作業

インストールが完了したら、仮想サーバ (クラスタ パッケージで指定されたホスト名) を Data Protector セルにインポートする必要があります。詳細は 188 ページの「セルへのクラスタ対応クライアントのインポート」を参照してください。

バックアップ デバイスやメディア プールなど、Data Protector の運用に必要な要素の構成方法は、オンライン ヘルプの索引キーワード「構成」で表示される内容を参照してください。

Data Protector の Microsoft Cluster Server へのインストール

Microsoft Cluster Server 用統合ソフトウェアでサポートされているオペレーティング システムの詳細は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス』を参照してください。

Cell Manager をクラスタ対応にする場合は、ライセンスで仮想サーバ IP アドレスを使用する必要があります。

クラスタ対応 Cell Manager のインストール

前提条件

クラスタ対応の Cell Manager をインストールする前に、以下の名前のリソースがクラスタに存在しないことを確認してください。

OBVS_MCRS,OBVS_VELOCIS,OmniBack_Share

新規インストールの場合 (アップグレードではない場合) に、この名前のリソースが存在するときは、これらのリソースを削除するか、または名前を変更してください。これは、Data Protector 仮想サーバが同名のリソースを使用しているためです。

以下の手順に従ってください。

1. [スタート] -> [プログラム] -> [管理ツール] -> [クラスタ アドミニストレータ] を順にクリックします。
2. リソースのリストを確認し、必要な場合はリソースの削除または名前の変更を行います。

Microsoft Cluster Server 環境に Data Protector をインストールして構成するには、適切なユーザー権限を持つアカウントを用意する必要があります。

- ✓ Cell Manager に対する管理者権限を付与します。
- ✓ クラスタ内でのクラスタ管理者権限を付与します。
- ✓ [パスワードを無期限にする] オプションを選択します。
- ✓ [サービスとしてログオン] オプションを選択します。
- ✓ [ユーザーはパスワードを変更できない] オプションを選択します。
- ✓ ログオン時間をすべて可能に設定します。

注記 Microsoft Cluster 環境に、クラスタ対応モードで Data Protector Cell Manager をインストールする場合は、Data Protector ユーザー アカウントは上記のユーザー権限をすべて付与されたドメイン ユーザー アカウントでなければなりません。

ヒント クラスタ サーバをインストールするには、すべてのクラスタ システムに対する管理者権限を付与されたアカウントが必要です。Data Protector のインストールにも、このアカウントを使用することをお勧めします。正しいユーザー権限を使用しない場合、クラスタに対応したモードではなく、標準モードで Data Protector サービスが実行される可能性があります。

Cell Manager ソフトウェアをクラスタ上にインストールする前に、以下の条件が満たされていることを確認してください。

- ✓ クラスタがインストールされており、すべての機能が利用可能であること。たとえば、共有ディスクを使って、問題なく、グループをノード間で必要な回数だけ移動できる必要があります。
- ✓ クラスタ内の最低 1 つのグループに <File Share> リソースが定義されていること。Data Protector は、<File Share> リソースに、データベース コンポーネントをインストールします。<File Share> リソースを定義するには、クラスタ付属のドキュメントを参照してください。<File Share> リソースのファイル共有名を OmniBack にすることはできません。
- ✓ <File Share> リソースと同じグループ内に仮想サーバが存在しない場合は、登録済みのネットワーク IP アドレスのうち未使用のものを使って新しい仮想サーバを作成し、これをネットワーク名と関連付ける必要があります。
- ✓ Data Protector のインストール先となる <File Share> リソースの IP アドレス、ネットワーク名、および物理ディスクが、<File Share> 依存関係に含まれていること。これは、Data Protector クラスタグループが、他のグループと関係なく、いずれのノード上でも実行できるようにするために必要です。
- ✓ クラスタ管理者だけが <File Share> リソースへのアクセス権を持ち、それがフル アクセス権であることを確認します。
- ✓ クラスタの各システムが適切に稼動していること。
- ✓ クラスタ内のシステムに Data Protector ソフトウェアがインストールされている場合、セットアップを行う前にこのソフトウェアをアンインストールすること。アップグレードが可能なのは、既存の Data Protector ソフトウェアがクラスタ対応モードでインストールされた Cell Manager である場合のみです。

- ✓ Data Protector がすべてのクラスタ ノードの同じ場所 (ドライブおよびパス名) にインストールされていること。これらのインストール先が空であることを確認してください。
- ✓ その他の MSI ベースのインストールは、他のクラスタ ノードで実行してはなりません。

ローカル インストール

Data Protector クラスタに対応した Cell Manager ソフトウェアは、DVD-ROM からローカルにインストールする必要があります。以下の手順に従ってください。

1. Windows 用インストール DVD-ROM をドライブに挿入し、以下のコマンドを実行します。

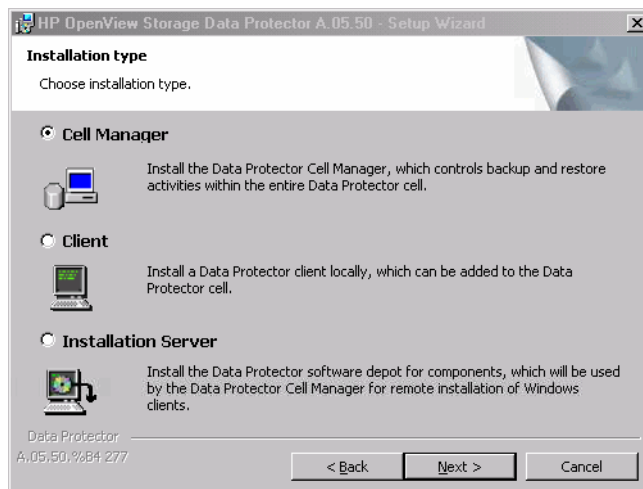
32 ビット システムの場合: %Windows_other%\i386\setup.exe

64 ビット システムの場合: %Windows_other%\x86\64\setup.exe

Data Protector セットアップ用ウィザードが表示されます。

2. セットアップ用ウィザードの指示に従って操作を行い、ライセンス契約を十分にお読みください。記載内容に同意する場合は、[Next] をクリックして次に進みます。
3. [Installation Type] ページで、[Cell Manager] を選択します。[Next] をクリックすると、選択した Data Protector Cell Manager ソフトウェアがインストールされます。

図 2-23 インストールの種類を選択



Data Protector の Microsoft Cluster Server へのインストール

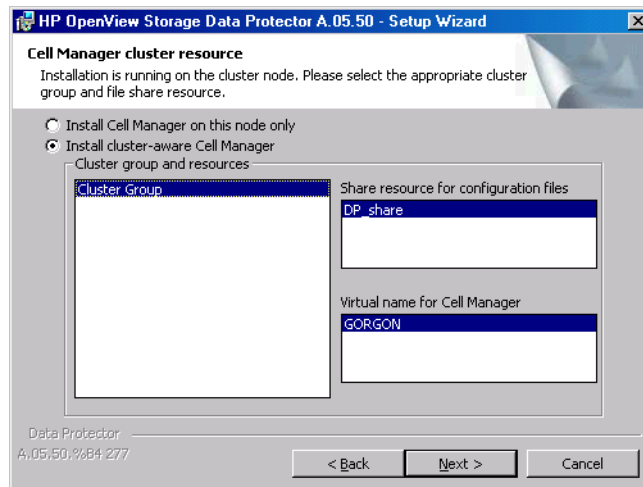
4. セットアップはクラスタ環境で実行していることを自動的に検出します。[Install cluster-aware Cell Manager] を選択して、クラスタ セットアップを有効にします。

クラスタ グループ、仮想ホスト名と、Data Protector の共有ファイルおよびデータベースのインストール先となるクラスタ <File Share> リソースを選択します。

注記

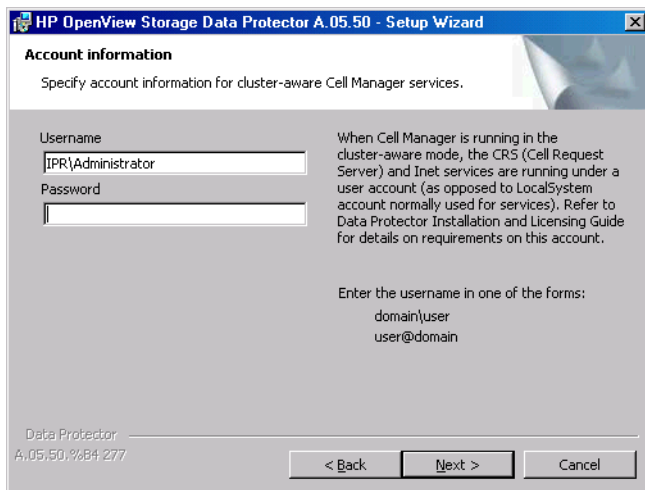
[Install Cell Manager on this node only] を選択した場合、Cell Manager はクラスタ対応にはなりません。詳細は 29 ページの「Windows 用 Cell Manager のインストール」を参照してください。

図 2-24 クラスタ リソースの選択



5. Data Protector サービスの起動に使用されるアカウントのユーザー名とパスワードを入力します。

図 2-25 アカウント情報の入力

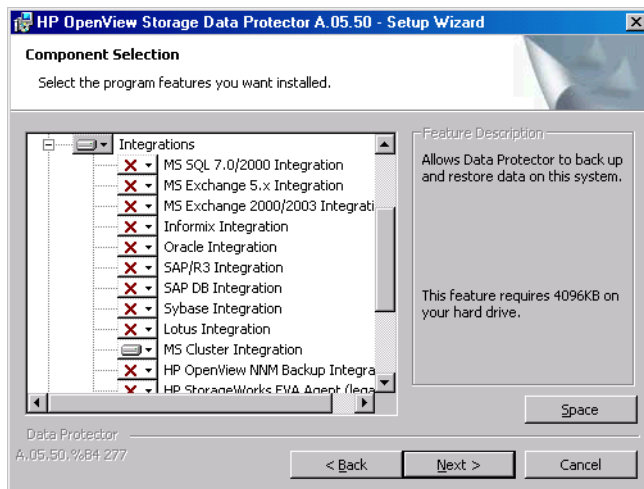


6. Data Protector をデフォルト フォルダにインストールする場合には、[Next] をクリックします。
デフォルト以外のフォルダにインストールする場合には、[Change] をクリックし、[Change Current Destination Folder] ウィンドウを開いて、新しいパスを入力します。
7. [Component Selection] ウィンドウで、すべてのクラスタ ノードとクラスタ仮想サーバにインストールするコンポーネントを選択します。[Next] をクリックします。
MS Cluster Integration コンポーネントが自動的に選択されています。

ネットワークへの Data Protector のインストール Data Protector の Microsoft Cluster Server へのインストール

選択されたコンポーネントは、クラスタ内のすべてのノードにインストールされます。

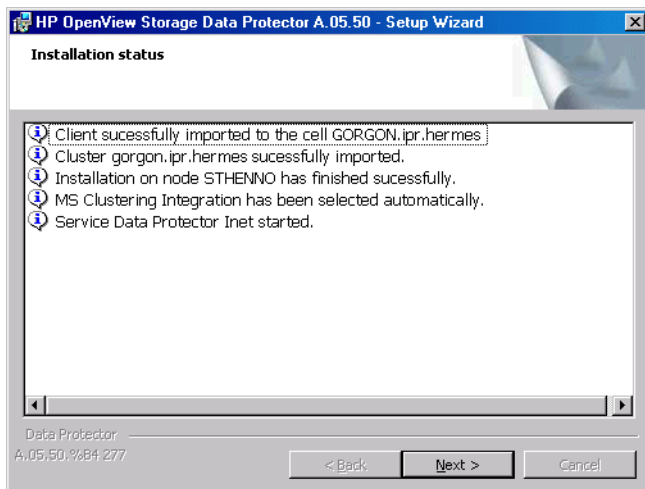
図 2-26 [Component Selection] ページ



8. コンポーネント選択サマリー ページが表示されます。[Install] をクリックします。

9. [Installation status] ページが表示されます。[Next] をクリックします。

図 2-27 [Installation Status] ページ



10. インストール後すぐに Data Protector を起動するには、[Start the Data Protector Manager] を選択します。

『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス』を表示するには、[Open the Product Announcements] を選択します。

Windows x64 以外のオペレーティングシステムで、HP OpenView AutoPass ユーティリティをインストールまたはアップグレードする場合は、[Start AutoPass installation] オプションまたは [Upgrade AutoPass installation] オプションを選択します。

HP OpenView AutoPass ユーティリティは、すべてのノードではなく 1 つのノードにのみインストールされるため、Microsoft Cluster にインストールすることはお勧めできません。ただし、AutoPass をインストールする場合は、Data Protector をシステムから削除するために、インストールされているノードと同じノードから Data Protector をアンインストールする必要があります。

Windows x64 オペレーティングシステムには、AutoPass はインストールされません。

[Finish] をクリックしてインストールを実行します。

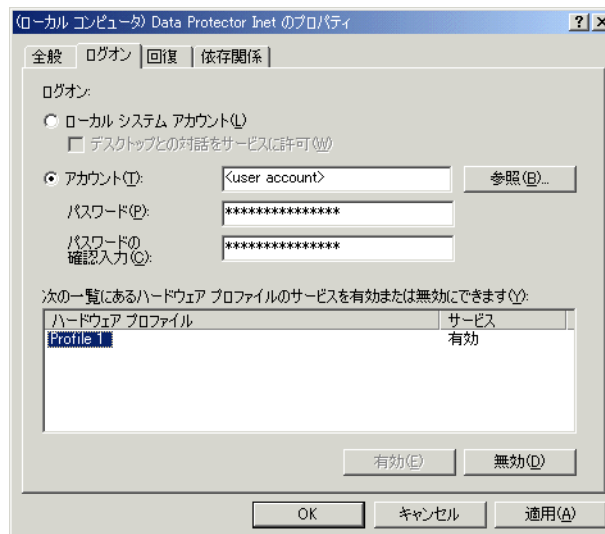
ネットワークへの Data Protector のインストール Data Protector の Microsoft Cluster Server へのインストール

インストールのチェック

セットアップ手順が完了したら、Data Protector ソフトウェアが正しくインストールされているかどうかチェックできます。以下の手順に従ってください。

1. クラスタ サービス アカウントが各クラスタ ノードの Data Protector Inet サービスに割り当てられていることを確認します。さらに、同じユーザーが Data Protector admin ユーザーグループに割り当てられていることを確認します。ログオン アカウント タイプは、174 ページの図 2-28 に示すように設定する必要があります。

図 2-28 Data Protector ユーザー アカウント



2. `<Data_Protector_home>\bin` ディレクトリへ移動し、以下のコマンドを実行します。

```
omnirsh <host> INFO_CLUS
```

`<host>` には、クラスタ仮想サーバの名前を指定します。このコマンドを実行すると、クラスタ内のシステムの名前のリストと仮想サーバの名前が表示されます。「0 "NONE"」と出力された場合は、Data Protector がクラスタ対応モードでインストールされていません。

3. Data Protector GUI を起動し、[クライアント] コンテキストを選択して、[MS Cluster] をクリックします。新たにインストールしたシステムが結果エリアに表示されていることを確認してください。

クラスタ対応クライアントのインストール

前提条件

クラスタ対応の Data Protector クライアントをインストールするには、次の前提条件を満たす必要があります。

- ✓ すべての機能を備えたクラスタがすべてのクラスタ ノード上に正しくインストールされていること。たとえば、共有ディスクを使って、グループをノード間で必要な回数だけ移動できる必要があります。
- ✓ クラスタの各システムが適切に稼動していること。

ローカル インストール

Data Protector のクラスタ対応クライアントは、DVD-ROM を使用して各クラスタ ノードにローカルにインストールしなければなりません。クラスタ ノード (Data Protector クラスタ クライアント) は、インストールプロセス中に指定したセルにインポートされます。

インストールを実行するには、クラスタ管理者のアカウントが必要です。この点を除けば、クラスタ クライアントのセットアップは、Windows クライアントのセットアップと同じです。Data Protector クライアントのコンポーネント (Disk Agent や Media Agent など) に加えて、クラスタ統合ソフトウェア コンポーネントをインストールする必要があります (デフォルトではインストール時に選択されます)。

Data Protector Windows クライアント システムをローカルにインストールする方法は、63 ページの「Windows 用クライアントのインストール」を参照してください。Data Protector では、インストール時にクラスタが検出されたことが通知されます。

Data Protector の Oracle 用統合ソフトウェアをインストールする場合、セットアップ手順は、Oracle リソース グループのすべてのクラスタ ノード上と仮想サーバ上で実行する必要があります。

注記

クラスタ対応クライアントは、標準の Cell Manager が管理する Data Protector セル、またはクラスタ対応の Cell Manager が管理する Data Protector セルのどちらにでもインポートできます。

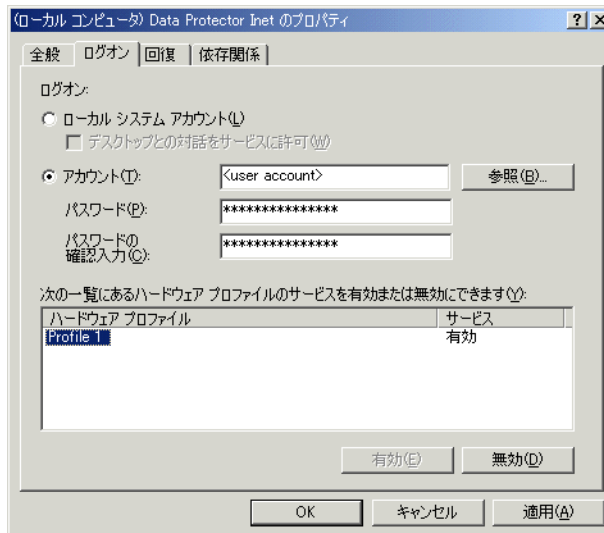
ネットワークへの Data Protector のインストール Data Protector の Microsoft Cluster Server へのインストール

インストールのチェック

セットアップ手順が完了したら、Data Protector ソフトウェアが正しくインストールされているかどうかチェックできます。以下の手順に従ってください。

1. クラスタ サービス アカウントが各クラスタ ノードの Data Protector Inet サービスに割り当てられていることを確認します。さらに、同じユーザーが Data Protector admin ユーザーグループに割り当てられていることを確認します。ログオン アカウント タイプは、174 ページの図 2-28 に示すように設定する必要があります。

図 2-29 Data Protector ユーザー アカウント



2. <Data_Protector_home>\bin ディレクトリに移動します。
3. 次のコマンドを実行します。

```
omnirsh <host> INFO_CLUS
```

<host> には、クラスタ クライアント システムの名前を指定します。クラスタ対応のクライアント システムのリストが出力されます。「0 "NONE"」と出力された場合は、Data Protector がクラスタ対応モードでインストールされていません。

Veritas Volume Manager

クラスタ上に Veritas Volume Manager がインストールされている場合は、Microsoft Cluster Server への Data Protector のインストールが完了した後に、追加作業が必要になります。追加作業の手順は B-76 ページの「Veritas Volume Manager がインストールされた Microsoft Cluster への Data Protector のインストール」を参照してください。

この次に行う作業

インストールが完了したら、仮想サーバのホスト名 (クラスタ対応アプリケーション) を Data Protector セルにインポートする必要があります。詳細は 188 ページの「セルへのクラスタ対応クライアントのインポート」を参照してください。

バックアップ デバイスやメディア プールなど、Data Protector の運用に必要な要素の構成方法は、オンライン ヘルプの索引キーワード「構成」で表示される内容を参照してください。

Veritas Cluster への Data Protector クライアントのインストール

Data Protector クライアントは、クラスタ外にある Cell Manager を使用して、Veritas Cluster ノード上にインストールできます。この構成では、ローカルディスクのバックアップがサポートされません。

共有ディスクまたはクラスタ対応アプリケーションをバックアップする必要がある場合は、仮想サーバの IP アドレスをライセンスに使用する必要がある点に注意してください。

重要 Data Protector では、フェイルオーバー機能を持ったクラスタ対応バックアップはサポートされていない点に注意してください。

クライアントのインストール

インストール手順は、Data Protector を標準構成の Solaris クライアント システムにインストールする場合と同じです。手順の詳細は、72 ページの「Solaris 用クライアントのインストール」を参照してください。

この次に行う作業

インストールが完了したら、以下の作業を行います。

- 仮想サーバをバックアップする必要がある場合は、仮想サーバをセルにインポートしてください。
- 物理ノードをバックアップする必要がある場合は、物理ノードをセルにインポートしてください。

詳細は、188 ページの「セルへのクラスタ対応クライアントのインポート」を参照してください。

バックアップ デバイスやメディア プールなど、Data Protector の運用に必要な要素の構成方法は、オンライン ヘルプの索引キーワード「構成」で表示される内容を参照してください。

Novell NetWare Cluster への Data Protector クライアントのインストール

Data Protector クライアントは、クラスタ外にある Cell Manager を使用して、Novell NetWare 6.0 Cluster Services クラスタ ノード上にインストールすることができます。この構成を使用して、ローカル ディスクのバックアップと仮想サーバを使用した共有クラスタ プールのバックアップが行えます。Novell NetWare Cluster でサポートされているオペレーティング システムの詳細は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス』を参照してください。

共有ディスクまたはクラスタ対応アプリケーションをバックアップする必要がある場合は、仮想サーバの IP アドレスをライセンスに使用する必要がある点に注意してください。

重要 フェイルオーバー機能を持ったクラスタ対応バックアップはサポートされていない点に注意してください。フェイルオーバーが発生した場合は、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。

バックアップ デバイスは、仮想サーバではなくクラスタ ノード上で構成されている必要があります。これは、クラスタ ノードがデバイスを制御するためです。

クライアントのインストール

インストール前に

Novell NetWare Cluster Services クラスタ ノード上に Data Protector クライアントをインストールする前に、クラスタ内のすべての仮想サーバのアンロード スクリプトを編集することをお勧めします。そうすることにより、仮想サーバから他のノードへの移行中でも、セカンダリ IP アドレスはアクティブのままになります。アンロード スクリプトを編集するには、Novell Console One ユーティリティ、または NetWare Remote Manager を使用します。使用方法は Novell NetWare のマニュアルを参照してください。

例：

すべての仮想サーバに対するデフォルトのアンロード スクリプトは、以下のとおりです。

```
del secondary ipaddress 10.81.1.173
CLUSTER CVSBIND DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
NUDP DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
```

ネットワークへの Data Protector のインストール

Novell NetWare Cluster への Data Protector クライアントのインストール

```
nss /pooldeactivate=FIRST /override=question
```

すべての仮想サーバに対する変更済みのアンロード スクリプトは、以下のとおりです。

```
nss /pooldeactivate=FIRST /override=question
```

```
del secondary ipaddress 10.81.1.173
```

```
CLUSTER CVSBIND DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
```

```
NUDP DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
```

変更済みのアンロード スクリプトでは、最初に仮想サーバ上のすべてのクラスタ共有プールをディスマウントおよび非アクティブ化し、その後セカンダリ IP アドレスを削除します。これにより、セカンダリ IP アドレスは移行中もアクティブのままとなります。

変更済みのアンロード スクリプトをアクティブにするには、優先ノード上で仮想サーバをオフラインにし、再びオンラインに戻します。

smsrun.bas スクリプトの編集

アンロード スクリプトの編集後、クラスタのサポートを無効にするパラメータを使用して TSA600.NLM モジュールまたは TSAFS.NLM モジュール (使用するモジュールによって異なる) をロードするように、smsrun.bas スクリプトを編集する必要があります。詳細は、Novell Support Knowledge データベースの「Known Backup/Restore Issues for NetWare 6.x」を参照してください。

smsrun.bas スクリプトの編集は、以下の手順で行います。

1. SYS:NSN/user/smsrun.bas スクリプトの書き込み保護を**読み込み専用**から**読み込み / 書き込み**に変更して、標準のコンソール エディタで開きます。
2. Sub Main() の項の nlmArray = Array("SMDR", "TSA600", "TSAPROXY") (または nlmArray = Array("SMDR", "TSAFS /NoCluster")) の行を次のように変更します。
 - nlmArray = Array("SMDR", "TSA600 /cluster=off", "TSAPROXY") (TSA600 がインストールされている場合)
 - nlmArray = Array("SMDR", "TSAFS /NoCluster") (TSAFS がインストールされている場合)

変更した内容を保存します。

3. ファイル サーバのコンソールで、SMSSTOP と入力します。
4. ファイル サーバのコンソールで、SMSSTART と入力します。

クラスタ共有ボリュームが TSA600.NLM (TSAFS.NLM) モジュールにより表示されます。

インストール

インストール手順は、Data Protector を標準構成の Novell NetWare クライアントにローカル インストールする場合と同じです。手順の詳細は、102 ページの「Novell NetWare クライアントのローカル インストール」を参照してください。

この次に行う作業

インストールが完了したら、以下の作業を行います。

- 物理ノードをバックアップする必要がある場合は、物理ノードをセルにインポートしてください。
- 仮想サーバ (共有クラスタ ボリューム) をバックアップする必要がある場合は、仮想サーバをセルにインポートしてください。

詳細は、188 ページの「セルへのクラスタ対応クライアントのインポート」を参照してください。

バックアップ デバイスやメディア プールなど、Data Protector の運用に必要な要素の構成方法は、オンライン ヘルプの索引キーワード「構成」で表示される内容を参照してください。

ネットワークへの Data Protector のインストール

Novell NetWare Cluster への Data Protector クライアントのインストール

3 インストールの保守

この章の内容

この章では、バックアップ環境の構成変更の中でも最もよく行われる処理について説明します。各項では、以下の情報について示します。

- グラフィカルユーザー インタフェースを使用してクライアントをセルにインポートする方法。詳細は 185 ページの「セルへのクライアントのインポート」を参照してください。
- グラフィカルユーザー インタフェースを使用してインストール サーバをセルにインポートする方法。詳細は 187 ページの「セルへのインストール サーバのインポート」を参照してください。
- グラフィカルユーザー インタフェースを使用してクラスタや仮想サーバをインポートする方法。詳細は 188 ページの「セルへのクラスタ対応クライアントのインポート」を参照してください。
- グラフィカルユーザー インタフェースを使用してクライアントをエクスポートする方法。詳細は 192 ページの「セルからのクライアントのエクスポート」を参照してください。
- グラフィカルユーザー インタフェースを使用して保護を設定する方法。詳細は 195 ページの「保護について」を参照してください。
- Data Protector にインストールされているパッチを確認する方法。詳細は 211 ページの「インストールされている Data Protector パッチの確認」を参照してください。
- Data Protector ソフトウェアをアンインストールする方法。詳細は 213 ページの「Data Protector ソフトウェアのアンインストール」を参照してください。
- Data Protector ソフトウェア コンポーネントを追加または削除する方法。詳細は 226 ページの「Data Protector ソフトウェア コンポーネントの変更」を参照してください。

セルへのクライアントのインポート

インストール サーバからクライアントに Data Protector ソフトウェアを配布した場合は、クライアント システムはセルに自動的に追加されます。リモート インストールが終了すると、クライアントはただちにセルのメンバーになります。

いつインポートを行うか

Novell NetWare クライアントや OpenVMS クライアント、Windows XP Home Edition クライアントなど、一部のクライアントについては、インストール後にセルにインポートする必要があります。**インポート**とは、Data Protector ソフトウェアのインストール後に、コンピュータを手作業でセルに追加することを指します。Data Protector セルに追加されたシステムは、Data Protector クライアントになります。新しくセルのメンバーとなったクライアント システムに関する情報は、Cell Manager 上の IDB に書き込まれます。

1つのクライアントは、1つのセルのメンバーにしかありません。クライアントを別のセルに移動する場合は、最初にそのクライアントを現在のセルからエクスポートし、次に新しいセルにインポートする必要があります。クライアントをエクスポートする手順は、192 ページの「セルからのクライアントのエクスポート」を参照してください。

重要 Data Protector クライアントのインストールと、セルへのクライアントのインポートが完了したら、不適切なセル権限によるアクセスからクライアントを保護することを強くお勧めします。詳細は 198 ページの「クライアントの保護」を参照してください。

インポート方法

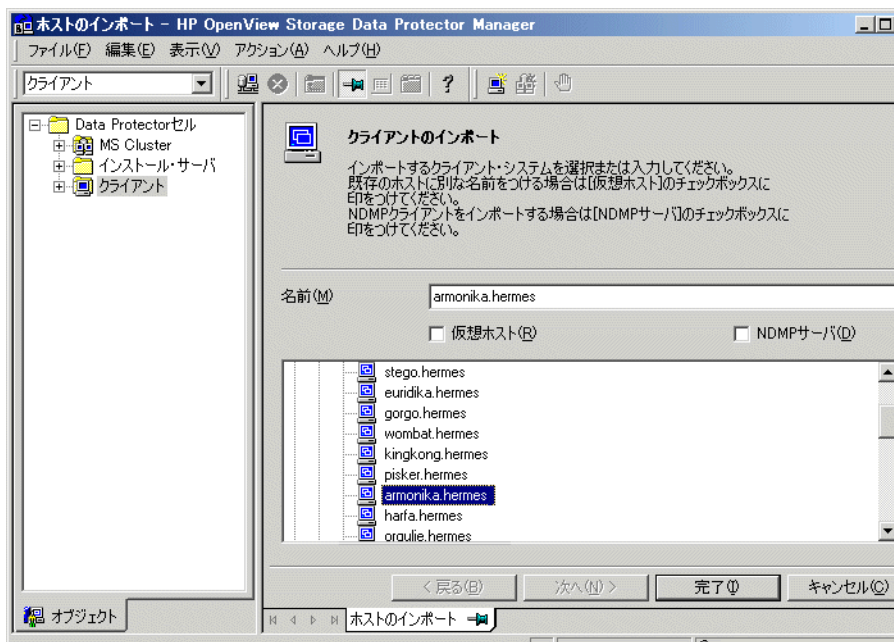
グラフィカル ユーザー インタフェースを使ってクライアント システムをインポートするには、以下の手順に従ってください。

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 ペインの [クライアント] をマウスの右ボタンでクリックし、[クライアントのインポート] を選択します。

インストールの保守 セルへのクライアントのインポート

3. インポートするクライアント名を入力します。Windows GUI を使用している場合は、ネットワークを参照して目的のクライアントを選択することもできます。詳細は図 3-1 を参照してください。

図 3-1 セルへのクライアントのインポート



複数の LAN カードが構成されたクライアントをインポートする場合は、[仮想ホスト] オプションを選択してください。このオプションを選択することにより、そのシステムに割り当てられているホスト名をすべてインポートできます。

NDMP クライアントをインポートする場合は、[NDMP サーバ] オプションを選択し、[次へ] をクリックします。ここで、NDMP サーバに関する情報を指定します。

OpenVMS クライアントをインポートする場合は、OpenVMS クライアントの TCP/IP 名を [名前] テキストボックスに入力します。

[完了] をクリックしてクライアントをインポートします。

インポートしたクライアントの名前が結果エリアに表示されます。

セルへのインストール サーバのインポート

いつ追加を行うか

次の場合は、インストール サーバをセルに追加する必要があります。

- 独立した形で、つまり Cell Manager とは別のシステム上に UNIX インストール サーバをインストールした場合。
この場合、インストール サーバをセルに追加するまでは、セル内のクライアントに対するリモート インストール (プッシュ) は実行できません。
- インストール サーバを Cell Manager 上にインストールしたが、別のセル内でのリモート インストールにもそのインストール サーバを使用したい場合。この場合は、目的のセルの Cell Manager に接続された GUI を使用して、インストール サーバをそのセルに追加しなければなりません。

クライアントの場合とは異なり、インストール サーバは複数のセルのメンバーになることができます。そのため別のセルに追加 (インポート) する場合も、現在のセルから削除 (エクスポート) する必要はありません。

追加方法

インストール サーバのインポート手順は、クライアントのインポート手順とほぼ同じです。インストール サーバの追加先セルの Cell Manager に接続された Data Protector GUI を使用して、以下の操作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、[インストール サーバ] を右クリックし、[インストール サーバの追加] をクリックして、ウィザードを起動します。詳細は 186 ページの図 3-1 を参照してください。
3. インポートするシステムの名前を入力するか、一覧から選択します。[完了] をクリックしてインストール サーバをインポートします。

セルへのクラスタ対応クライアントのインポート

Data Protector ソフトウェアをクラスタ対応クライアント上にローカルにインストールした後、そのクラスタ対応クライアントを表す仮想サーバを Data Protector セルにインポートします。

前提条件

- すべてのクラスタ ノード上に Data Protector がインストールされていること。
- クラスタ内ですべてのクラスタ パッケージが実行されていること。

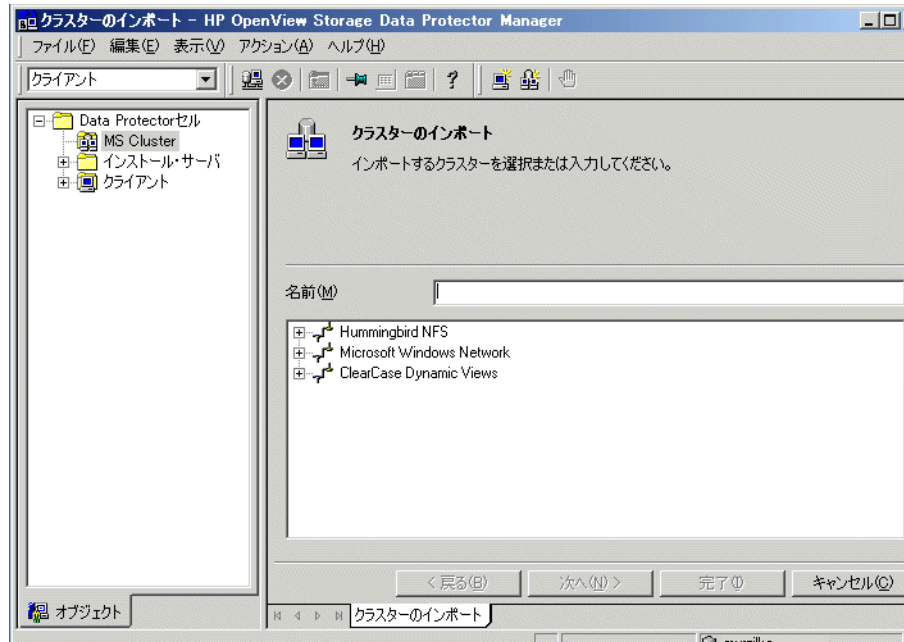
Microsoft Cluster Server

Microsoft Cluster Server クライアントを Data Protector セルにインポートするには、以下の手順に従ってください。

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 ペインの [MS Cluster] をマウスの右ボタンでクリックし、[クラスタのインポート] を選択します。

3. インポートするクラスタ クライアントを表す仮想サーバの名前を入力するか、またはネットワークを参照して目的の仮想サーバを選択します。詳細は図 3-2 を参照してください。

図 3-2 セルへの Microsoft Cluster Server クライアントのインポート



4. [完了] をクリックしてクラスタ クライアントをインポートします。

ヒント 特定のクラスタ ノードまたは仮想サーバをインポートするには、Scoping ペインでクラスタを右クリックし、[クラスタ ノードのインポート] または [クラスタ 仮想サーバのインポート] をクリックします。

その他のクラスタ

Tru64 Cluster の前提条件

クラスタのホスト名をインポートする前に、以下のことを確認してください。

- クラスタ内の共有ディスク上に Data Protector がインストールされていること。

インストールの保守 セルへのクラスタ対応クライアントのインポート

- Tru64 Cluster 内ですべての Tru64 Cluster ノードが実行されていること。
- Data Protector 各ノード上で inetd プロセスが実行されていること。

手順

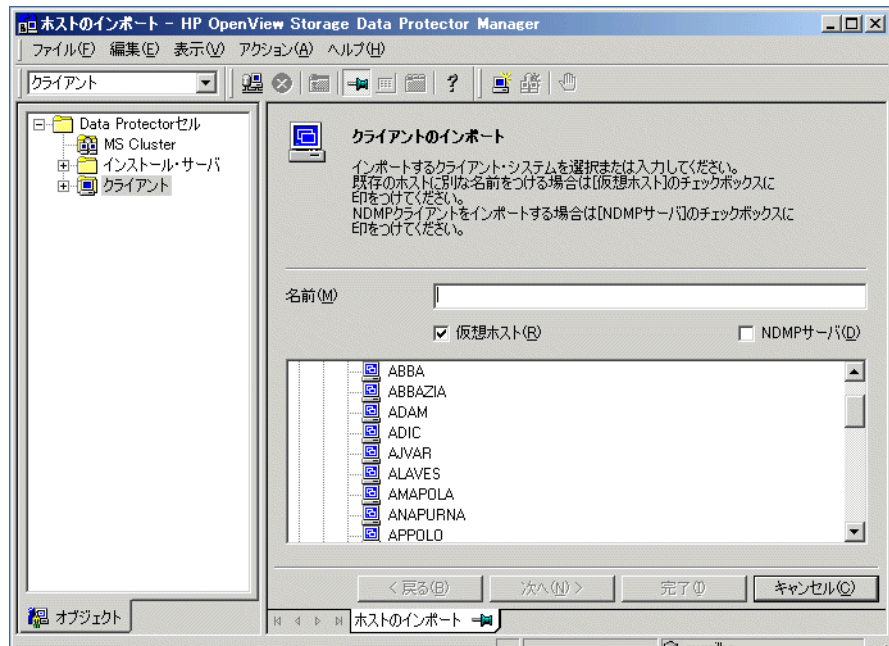
MC/ServiceGuard、Veritas、Tru64 Cluster、Novell NetWare Cluster Services のいずれかのクライアントを Data Protector セルにインポートするには、以下の手順に従ってください。

1. [Data ProtectorManager] で、[クライアント] コンテキストを開きます。
2. Scoping ペインの [クライアント] をマウスの右ボタンでクリックし、[クライアントのインポート] を選択します。
3. 仮想サーバのホスト名をアプリケーション クラスタ パッケージで指定されているとおりに入力します。Windows GUI を使用している場合は、ネットワークを参照して目的の仮想サーバを選択することもできます。

インポートするのが仮想サーバであることを示すために、[仮想] オプションを選択します。詳細は図 3-3 を参照してください。

4. [完了] をクリックして仮想サーバをインポートします。

図 3-3 MC/ServiceGuard クライアント、Veritas クライアント、または Novell NetWare Cluster Services クライアントのセルへのインポート



ヒント クラスタ ノードのローカル ディスク上にあるデータのバックアップも構成できるようにするには、Data Protector クライアントを表すクラスタ ノードをインポートする必要があります。インポート手順については、185 ページの「セルへのクライアントのインポート」を参照してください。

セルからのクライアントのエクスポート

Data Protector セルからクライアントを**エクスポート**すると、そのクライアントへの参照が Cell Manager 上の IDB から削除されます。ただし、クライアント上のソフトウェアはアンインストールされません。クライアントをエクスポートするには、Data Protector GUI を使用します。

エクスポート機能を使うと、以下のような作業を実施できます。

- クライアントを他のセルに移動できます。
- ネットワークに現在含まれていないクライアントを、Data Protector セルから削除できます。
- ライセンスの不足によって発生した問題を解決できます。

セルからクライアントをエクスポートすると、そのシステムで使用していたライセンスを他のシステムで使用できるようになります。

前提条件

クライアントをエクスポートする前に、以下の条件が満たされていることを確認してください。

- ✓ そのクライアントを参照する指定がすべてのバックアップ仕様から削除されていること。アンインストールしたシステムへの参照がバックアップ仕様に残っていると、Data Protector は不明なクライアントのバックアップを実行しようとするため、バックアップ仕様のこの部分が正常に実行されません。バックアップ仕様の変更方法は、オンラインヘルプの索引キーワード「変更, バックアップ仕様」で表示される内容を参照してください。
- ✓ クライアントにバックアップデバイスが接続および構成されていないこと。Data Protector では、エクスポートしたシステムのバックアップ デバイスは、元のセル内で使用できなくなります。

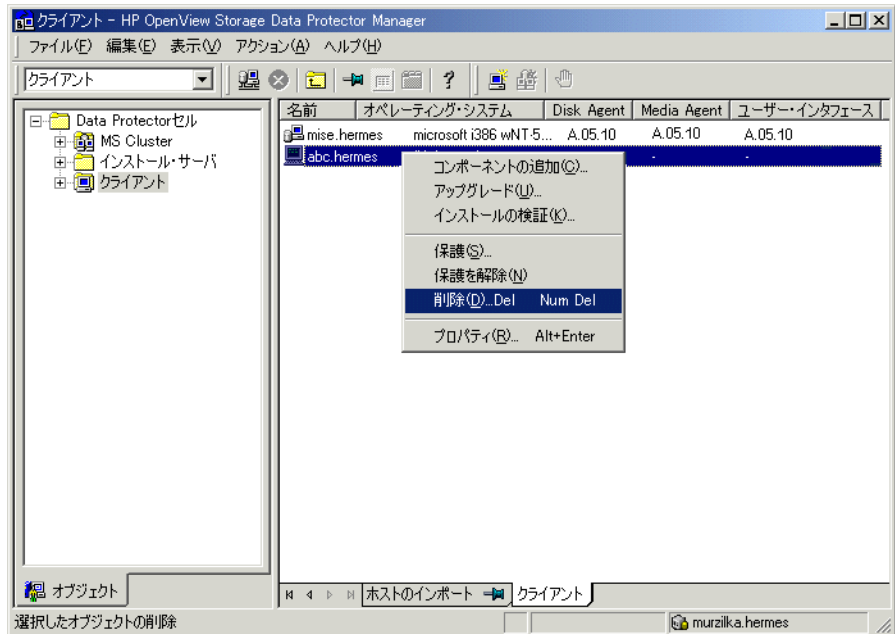
エクスポート方法

Data Protector GUI を使ってクライアントをセルからエクスポートするには、以下の手順に従ってください。

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] をクリックします。次に、エクスポート対象のクライアントシステムを右クリックし、[削除] をクリックします。詳細は 193 ページの図 3-4 を参照してください。

図 3-4 クライアント システムのエクスポート



3. Data Protector ソフトウェアを同時にアンインストールするかどうかを確認するメッセージが表示されます。[いいえ] をクリックしてクライアントのエクスポートのみを指定し、[完了] をクリックします。

選択したクライアントが [結果エリア] のリストから削除されます。

注記 エクスポートするクライアントと同じシステムにインストールされているインストール サーバを使って、Data Protector クライアントをエクスポートすることはできません。

インストールの保守 セルからのクライアントのエクスポート

Microsoft Cluster Server クライアント

Microsoft Cluster Server クライアントを Data Protector セルからエクスポートするには、以下の手順に従ってください。

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 [MS Clusters] を展開し、エクスポートするクライアントを右クリックして、[削除] をクリックします。
3. Data Protector ソフトウェアを同時にアンインストールするかどうかを確認するメッセージが表示されます。[いいえ] をクリックしてクラスタ クライアントだけをエクスポートします。

選択したクラスタ クライアントが [結果エリア] のリストから削除されます。

ヒント	特定のクラスタ ノードまたは仮想サーバをエクスポートするには、Scoping ペインでクラスタ ノードまたは仮想サーバを右クリックし、[削除] をクリックします。
------------	---

保護について

ここでは、Data Protector の保護について説明します。Data Protector の保護を強化するための高度な設定と、その前提条件や考慮すべき点について説明します。

環境全体での保護の強化には、さらなる作業も必要となるため、多くの保護機能は、デフォルトでは有効になっていません。

この章で説明されている考慮すべき点は、保護設定を変更する場合だけでなく、新規ユーザーの構成、クライアントの追加、Application Agent の構成、これらの考慮点があてはまるその他の変更を行う場合にも従う必要があります。保護設定に対するいかなる変更も、セル全体に影響を与える可能性があるため、慎重に検討する必要があります。

保護レイヤー

Data Protector の動作環境を保護するには、重要度の異なる複数の保護レイヤーにおいて、保護設定を計画およびテストし、実装する必要があります。保護レイヤーは、Data Protector クライアント、Cell Manager、およびユーザーの各レイヤーに分けられます。ここでは、それぞれのレイヤーでの保護の構成方法を説明します。

クライアントの保護

セル内のクライアントにインストールされる Data Protector エージェントには、システムのすべてのデータにアクセスできる機能などの数々の強力な機能が備わっています。これらの機能は、**セル権限** (Cell Manager とインストール サーバ) で実行されるプロセスのみが実行できるようにし、それ以外の実行要求は拒否するように設定することが重要です。

クライアントを保護する前に、信頼できるホストのリストを決定することが重要です。リストには、以下の情報を含めるようにしてください。

- Cell Manager
- 対応するインストール サーバ
- (一部のクライアントの場合のみ) ロボティクスにリモートでアクセスするクライアントのリスト

重要

リストには、接続要求を出す可能性があるすべてのホスト名 (または IP アドレス) を含める必要があります。クライアントがマルチホーム (複数のネットワークアダプタや IP アドレスを持つホスト) またはクラスタである場合には、複数のホスト名が必要になることもあります。

インストールの保守 保護について

セル内の DNS 構成が統一されていない場合、さらに考慮が必要になる可能性もあります。詳細は 198 ページの「クライアントの保護」を参照してください。

セル内のすべてのクライアントを常に保護する必要があるわけではありませんが、他のクライアントに信頼される以下のようなコンピュータについては、保護設定が重要です。

- Cell Manager / MoM
- インストール サーバ
- Media Agent (MA) クライアント

注記

ユーザー インタフェース クライアントは、信頼されるクライアントのリストに追加する必要はありません。ユーザーは、各自のユーザー権限に応じて、Data Protector の全機能またはある特定のコンテキストのみに、GUI を使ってアクセスすることができます。

Data Protector ユーザー

Data Protector ユーザーの構成時には、以下の重要点について考慮してください。

- 一部のユーザー権限は非常に強力です。たとえば、User configuration ユーザー権限や Clients configuration ユーザー権限を持つユーザーは、保護設定の変更が可能です。同様に、Restore to other clients も非常に強力なユーザー権限で、単体でも強力ですが、Back up as root ユーザー権限や Restore as root ユーザー権限と組み合わせるとさらに強力になります。
- これほど強力ではないユーザー権限にも、潜在的なリスクがあります。Data Protector では、これらのリスクの軽減のため、一部のユーザー権限を制限するように構成することができます。このような構成の設定については、この章で後述します。207 ページの「Start Backup Specification ユーザー権限」も参照してください。
- Data Protector の出荷時設定では少数のユーザー グループのみが定義されています。各ユーザーに割り当てる権限を最小限に抑えるため、Data Protector 環境内のユーザー タイプ別にグループを定義することをお勧めします。
- ユーザー構成は、ユーザーの検証にも関連します (205 ページの「ホスト名厳密チェック」を参照)。ユーザー構成を注意深く考慮しなければ、検証機能を強化しても意味がありません。逆の場合も同様で、検証機能を強化しなかった場合、最大の注意を払ってユーザー構成を行っても、その効果が発揮されない場合があります。

- Data Protector のユーザー リストに「脆弱な」ユーザー仕様が含まれないようにすることが重要です。ユーザー仕様の host は強固であるのに対し (強化した検証機能と組み合わせると特に強固になります)、user および group は確実に検証できない点に注意してください。強力なユーザー権限を持つユーザーは、Data Protector の管理に使用される特定のクライアントについてのみ構成すべきです。複数のクライアントが使用される場合も、それらのユーザーを user、group、<Any> として指定するのではなく、各クライアントにそれぞれエントリを追加するようにしてください。このようなシステムでは、信頼できないユーザーのログオンを許可してはいけません。

ユーザー構成の詳細は、オンライン ヘルプの索引キーワード「構成, ユーザー」で表示される内容を参照してください。

Cell Manager の保護

Cell Manager は、セル内のすべてのクライアントとデータにアクセスできるため、その保護は重要です。

Cell Manager の保護は、ホスト名厳密チェック機能を使用して強化できます。ただし、Cell Manager をクライアントとして保護し、Data Protector ユーザーを注意深く構成することも重要です。詳細は、205 ページの「ホスト名厳密チェック」および 198 ページの「クライアントの保護」を参照してください。

その他のセキュリティ保護について

他に考慮すべきセキュリティ保護は、以下のとおりです。

- ユーザーは、信頼されるクライアント (Cell Manager、インストール サーバ、MA、ロボティクス クライアント) にアクセスできるように設定しないでください。anonymous ログオンや ftp アクセスを許可することでさえ、セキュリティ保護全般に深刻なリスクをもたらす可能性があります。
- メディアやテープのライブラリ (および、接続されているクライアント) は、権限のない、または信頼されていないユーザーから、物理的に保護する必要があります。
- バックアップ、復元、オブジェクトやメディアのコピー、オブジェクト集約の際には、データがネットワーク経由で転送されます。信頼されないネットワークをネットワークのセグメント化によって十分に分離できない場合は、ローカル接続されたデバイスか、カスタム エンコーディング ライブラリを使用してください。なお、エンコーディング ライブラリを変更したときは、フルバックアップを実行する必要がある場合があります。

その他のセキュリティ保護関連事項の詳細については、『HP OpenView Storage Data Protector コンセプト ガイド』を参照してください。

クライアントの保護

Data Protector クライアントのインストール、およびクライアントのセルへのインポートが完了したら、権限のない他のクライアントによるアクセスからクライアントを保護することを、強くお勧めします。

Data Protector では、どのセル権限 (Cell Manager、MoM、インストール サーバ) からの要求を、クライアントの Data Protector ポート 5555 で承認するかを指定できます。これにより、指定された以外のコンピュータは、そのクライアントにアクセスできなくなります。195 ページの「クライアントの保護」も参照してください。

注記 ライブラリ ロボティクスに対してリモート アクセスを行うクライアントは、ライブラリ ロボティクス クライアントのセル権限リストに追加する必要があります。

バックアップや復元のように、実行前・実行後スクリプトの起動や、クライアントのインポートおよびエクスポートを伴う処理を行う場合、クライアントは、コンピューターがこれらの処理の実行を Data Protector ポート (デフォルト ポートは 5555) 経由で開始することを許可されているかどうかをチェックします。この保護機構によって、クライアントは指定されたセル権限に対してのみ、このような処理を許可します。

例外的状況に対する考慮

クライアントへのアクセスを制限する前に、以下に示す状況において問題が生じる可能性があることを考慮しておいてください。

- セル権限に、複数の LAN カードや複数の IP アドレス / クライアント名がある場合。
- クラスタ対応の Cell Manager を使用する場合。
- テープ ライブラリのロボティクスが別個の (または専用の) システム上で構成されている場合。

Data Protector では、セル権限としてクライアントに接続することが明示的に認められるシステムとして、単一のシステムを指定できるだけでなく、システムのリストを指定することもできます。障害を回避できるようにするため、代替セル権限として使用できる有効なクライアントの名前がすべて含まれるリストをあらかじめ用意しておいてください。

リストには、以下の情報を含めるようにしてください。

- セル権限で使用している、追加分を含めた (すべての LAN カードに対応する) クライアント名。
- Cell Manager がフェイルオーバーする可能性のあるすべてのクラスタ ノードのクライアント名およびクラスタ仮想サーバのホスト名。

- セル権限の全ハードウェアがダウンした場合に、セル権限が移されるターゲット システムの名前。このターゲット システムは、障害復旧対象として事前に定義されている必要があります。
- ライブラリのロボティクスを制御するクライアントへのアクセスが許可されているクライアントについては、そのライブラリのドライブを使用するすべてのクライアント名。

アクセスの承認および拒否の方針は、Data Protector がインストールされているすべてのシステムに適用できます。たとえば、Cell Manager からクライアントへのアクセス、Cell Manager から Cell Manager へのアクセス、インストール サーバからクライアントへのアクセス、またはクライアントからクライアントへのアクセスの承認または拒否が可能です。

注記

Cell Manager 以外のシステム上にあるインストール サーバは、許可クライアントのリストに追加されていないと、保護が設定されているクライアントにアクセスできません。この場合、インストール サーバに依存する操作 (インストールの確認、コンポーネントの追加、クライアントの削除など) は失敗します。これらの操作を保護が設定されたクライアントに対して行いたい場合は、インストール サーバを許可クライアントのリストに追加してください。

クライアントの保護方法

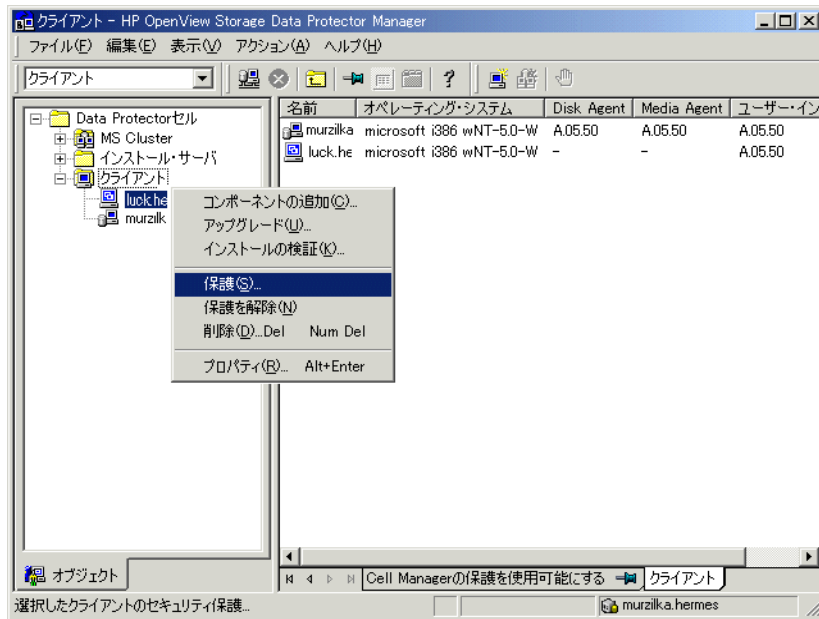
クライアント側でセル権限を確認できるようにする (クライアントを保護する) には、Data Protector GUI で以下の手順を行ってください。

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。

インストールの保守 保護について

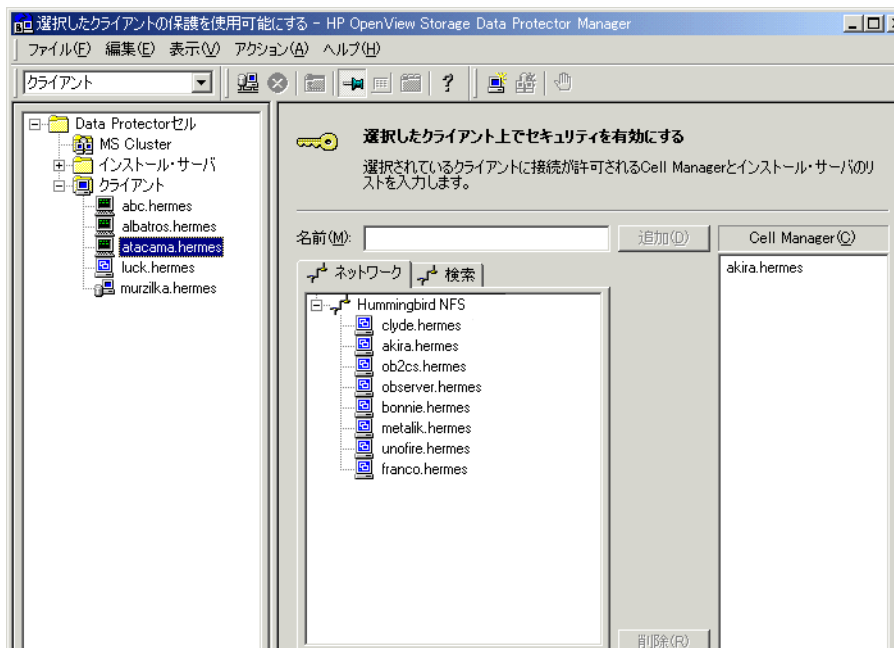
2. Scoping ペインで [クライアント] を展開し、保護するクライアントを右クリックして、[保護] をクリックします。詳細は図 3-5 を参照してください。

図 3-5 クライアントの保護設定



3. [ネットワーク] タブまたは [検索] タブを使用して、選択したクライアントへのアクセスを許可するシステムの名前を直接入力するか、または検索します。[追加] をクリックして、各システムをリストに追加します。詳細は図 3-6 を参照してください。

図 3-6 選択したクライアントの保護を使用可能にする



Cell Manager には、自動的にアクセス権が与えられ、信頼されるクライアントのリストに追加されます。Cell Manager をリストから除外することはできません。

4. [Finish] をクリックして、選択したシステムを `allow_hosts` ファイルに追加します。

どのような処理が行われるか

クライアントは、他のクライアントからの各要求に対してソースを確認し、[選択したクライアントの保護を使用可能にする] ウィンドウで選択されたクライアントからの要求のみを許可します。これらのクライアントは、`allow_hosts` ファイルに記載されています。要求が拒否された場合は、そのイベントのログが以下のディレクトリ内の `inet.log` ファイルに記録されます。

- Windows の場合 : `<Data_Protector_home>\log`
- HP-UX、Solaris、および Linux の場合 : `/var/opt/omni/log`

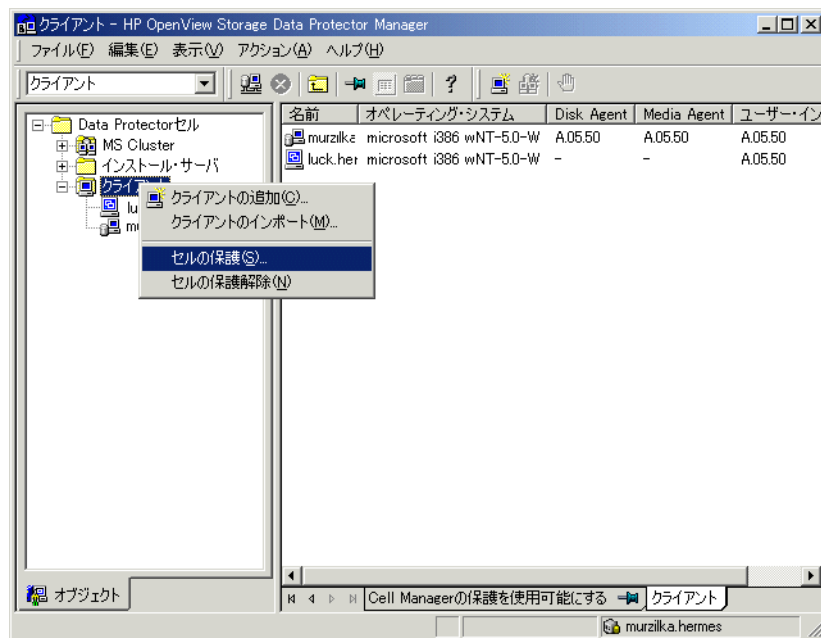
インストールの保守 保護について

- その他の UNIX システムの場合 : /usr/omni/log

セル内のすべてのクライアントに保護を設定する場合は、Data Protector GUI 上で以下の手順に従ってください。

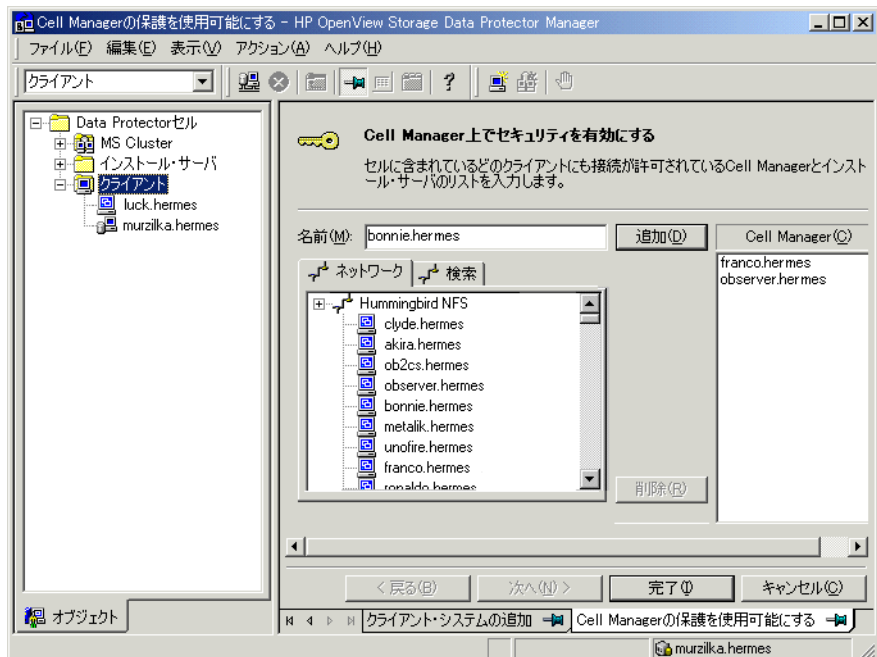
1. コンテキストリストで [クライアント] をクリックします。
2. Scoping ペインの [クライアント] をマウスの右ボタンでクリックし、[セルの保護] を選択します。詳細は図 3-7 を参照してください。

図 3-7 セルの保護設定



3. [ネットワーク] タブ (Windows GUI のみ) または [検索] タブを使用して、セル内の全クライアントへのアクセスを許可するシステムの名前を直接入力するか、または検索します。[追加] をクリックして、各システムをリストに追加します。詳細は図 3-8 を参照してください。

図 3-8 セル内のすべてのクライアントに対する保護の設定



4. [Finish] をクリックして、選択したシステムを allow_hosts ファイルに追加します。

どのような処理が行われるか

クライアントは、他のクライアントからの各要求に対してソースを確認し、[Cell Manager の保護を使用可能にする] ウィンドウで選択されたクライアントからの要求のみを許可します。これらのクライアントは、allow_hosts ファイルに記載されています。要求が拒否された場合は、そのイベントのログが以下のディレクトリ内の inet.log ファイルに記録されます。

- Windows の場合： <Data_Protector_home>%log
- HP-UX、Solaris、および Linux の場合： /var/opt/omni/log
- その他の UNIX システムの場合： /usr/omni/log

インストールの保守 保護について

セル全体に保護を設定した場合は、その時点でこのセルに所属しているすべてのクライアントに保護が設定されます。新しいクライアントをセルに追加した場合は、それらのクライアントにも保護を設定してください。

保護の解除方法

選択したシステムの保護を解除する場合は、Data Protector GUI 上で以下の手順に従ってください。

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、保護を解除したいクライアント (複数選択可能) を右クリックし、[保護を解除] をクリックします。
3. [はい] をクリックして、選択したクライアント (複数選択可能) に対するアクセスを許可することを確認します。

セル内のすべてのクライアントの保護を解除する場合は、以下の手順に従ってください。

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 ペインの [クライアント] をマウスの右ボタンでクリックし、[セルの保護解除] を選択します。
3. [はい] をクリックして、セル内のどのクライアントに対するアクセスも許可することを確認します。

allow_hosts ファイルと deny_hosts ファイル

クライアントに保護を設定すると、そのクライアントに対するアクセスが許可されているシステムのクライアント名が allow_hosts ファイルに書き込まれます。また、クライアントに対する特定のコンピュータからのアクセスを明示的に拒否するには、そのコンピュータの名前を deny_hosts ファイルに追加します。これらの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>%Config%client
- HP-UX、Solaris、および Linux の場合 : /etc/opt/omni/client
- その他の UNIX システムの場合 : /usr/omni/config/client

各クライアント名は行を分けて指定してください。

注記 クライアントへのアクセスが誤って拒否されるようになった場合は、そのクライアント上の allow_hosts ファイルを手作業で編集 (または削除) できます。

これらのファイルは、Windows システムでは 2 バイトの UNICODE 形式で保存され、HP-UX システム、Solaris システム、および Linux システムでは 1 バイト形式またはマルチ バイト形式 (Shift-JIS など) で保存されます。

inet.log ファイルに大量のログが記録される場合

クライアントに保護が設定されていない場合に、Cell Manager が MC/ServiceGuard 環境内に構成されていたり、複数の名前または IP 番号を持っていたりすると、inet.log ファイルに以下のタイプのエントリが多数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、保護が設定されていないクライアントが Cell Manager の第一ホスト名しか認識しないことが原因です。その他のクライアントからの要求もすべて許可されますが、要求は inet.log ファイルに記録されます。

クライアントに保護が設定されている場合は、allow_hosts ファイルに記載されているクライアントからの要求は承認されるため、ログに記録されることはありません。その他のクライアントからの要求は拒否されます。

このようにクライアントに保護を設定すると、不要なエントリが inet.log ファイルに記録されるのを回避できます。ただし、使われる可能性がある Cell Manager のすべてのクライアント名を、各クライアント上の allow_hosts ファイルに登録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場合にも、クライアントにアクセスできます。

何らかの理由により、お使いの環境でこの回避策を使用できない場合は、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 アドレス範囲として「*」を指定します。この結果、クライアントはすべてのシステム (すべての IP アドレス) からの要求を受け入れることになり、現実には保護されません。ただし、前述の大量のログが記録される問題はこれで解決できます。

ホスト名厳密チェック

デフォルトでは、Cell Manager でのユーザー検証には比較的簡単な方法が使用されます。この方法では、ユーザー インタフェースか Application Agent が起動されたクライアントで認識されているホスト名が使用されます。この方法は構成も容易で、(悪意のある攻撃が予測されない) 保護を設定することが「望ましい」レベルの環境では、妥当なレベルの保護を実現できます。

一方、ホスト名厳密チェックを設定すると、ユーザー検証を強化できます。この検証方法では、Cell Manager 上で DNS の逆引きにより接続元 IP アドレスから解決されたホスト名が使用されます。これには、以下の制限と考慮点があります。

インストールの保守 保護について

制限事項

- IP ベースのユーザー検証により提供される保護の強度は、ネットワーク内のスプーフィング行為に対する保護の強度に依存します。保護の設計者は、個々の保護要件において、スプーフィング行為に対する十分な安全対策が既存ネットワークで提供されているかを判断する必要があります。ファイアウォール、ルータ、VPN などを利用してネットワークをセグメント化すると、スプーフィング行為への対策を強化できます。
- 特定のクライアント内でのユーザーの分離は、クライアント間での分離ほど強力ではありません。高度な保護が求められる環境では、標準ユーザーと強力な権限を持つユーザーを同一クライアント内に混在させてはいけません。
- ユーザー仕様に含まれるホストは、DHCP を使用するよう構成してはいけません (固定 IP を割り当てるように設定し、DNS に登録しているホストを除きます)。

ホスト名厳密チェックを使用することで達成できる安全度を正しく判断するためには、これらの制限に留意する必要があります。

ホスト名の解決

以下の状況では、Data Protector で検証に使用されるホスト名が、デフォルトのユーザー検証を行う場合とホスト名厳密チェックを行う場合で異なることがあります。

- DNS の逆引き検索で、異なるホスト名が返される場合。これは、意図的である場合と、クライアントまたは DNS の逆引きテーブルにおける構成ミス場合があります。
- クライアントがマルチホーム (複数のネットワーク アダプタか IP アドレス、またはその両方があるホスト) の場合。特定のマルチホーム クライアントにこの考慮点が当てはまるかどうかは、ネットワーク内でのそのクライアントの役割と、DNS 内での構成方法によって決まります。
- クライアントがクラスタの場合。

ホスト名厳密チェックを有効にすると、Data Protector ユーザーの再構成が必要になる場合があります。Data Protector の既存のユーザー仕様については、前述のいずれかの理由による影響を受けるかどうかを確認する必要があります。状況に応じて、接続要求を出す可能性があるすべての IP について、既存の仕様を変更するか、新しい仕様をアカウントに追加する必要があります。

ホスト名厳密チェックを有効にしたときにユーザー仕様の変更が必要になった場合は、検証方法をデフォルトのユーザー検証に戻すときにもユーザーの再構成が必要になることに注意してください。このため、使用するユーザー検証方法をいったん決定した後は、その方法を使用し続けることをお勧めします。

信頼できる DNS の逆引き検索の前提条件は、DNS サーバが保護されていることです。権限を持たないすべてのユーザーによる物理的なアクセスとログオンを防止する必要があります。

ホスト名の代わりに IP を使用してユーザーを構成すると、DNS に関連する検証上の問題の一部を回避することができます。ただし、このように構成すると保守が困難になります。

要件

強化された検証方法では、特定の内部接続によるアクセスは、自動的には許可されません。したがって、この検証方法を使用するときには、以下のそれぞれの場合に新規ユーザーを追加する必要があります。

- Windows クライアント上に Application Agent (OB2BAR) がインストールされている場合。Windows クライアントについては、Application Agent がインストールされる各クライアントにおいて、SYSTEM、NT AUTHORITY、`<client>` の各ユーザーを追加する必要があります。クライアント上の Inet が特定のアカウントを使用するように設定されている場合は、そのアカウントを構成しておく必要があります。詳細は、オンライン ヘルプの索引キーワード「ホスト名によるチェック」で表示される内容を参照してください。
- Web Reporting を使用する場合は、Web Reporting が使用されるシステムの各ホスト名に対して、java、applet、`<hostname>` の各ユーザーを追加する必要があります。Web Reporting の全機能を使用するユーザーは、admin グループに属している必要があることに注意してください。したがって、クライアントは信頼されている必要があります。また、Web サーバを使用するなどの方法によって Web Reporting のすべてのデータや機能を他のユーザーも使用できるようにする際は、このようなデータを一般に開放した場合のセキュリティ保護への影響を事前に検討してください。

ユーザー構成の詳細は、オンライン ヘルプの索引キーワード「構成、ユーザー」で表示される内容を参照してください。

機能を使用可能にする

ホスト名厳密チェックを有効に設定するには、グローバル オプション ファイルで、StrictSecurityFlags フラグを 0x0003 に設定します。

グローバル オプション ファイルに関する詳細は、『HP OpenView Storage Data Protector トラブルシューティング ガイド』を参照してください。

Start Backup Specification ユーザー権限

Data Protector ユーザーとユーザー権限に関する一般的な情報は、オンライン ヘルプの索引キーワード「ユーザー」で表示される内容を参照してください。

インストールの保守 保護について

Start backup specification ユーザー権限だけが割り当てられているユーザーは、GUI の Backup コンテキストを使用することはできません。ただし、コマンド行で omnib コマンドを -datalist オプションと組み合わせて使用することにより、バックアップ仕様を起動することは可能です。

注記 Start Backup Specification を Start Backup ユーザー権限と組み合わせることにより、ユーザーは、GUI に構成されたバックアップ仕様を参照することができるようになり、バックアップ仕様や会話型バックアップを起動できます。

環境によっては、ユーザーによる会話型バックアップの実行を認める必要がありません。バックアップ仕様を保存する権限を持つユーザーにのみ会話型バックアップの実行を認める場合は、グローバル オプション ファイルで、StrictSecurityFlags フラグを 0x0200 に設定します。

グローバル オプション ファイルに関する詳細は、『HP OpenView Storage Data Protector トラブルシューティング ガイド』を参照してください。

バックアップ仕様の内容の隠蔽

高度な保護が求められる環境では、保存済みのバックアップ仕様の内容を機密情報と見なすことがあります。Data Protector では、「バックアップ仕様を保存」ユーザー権限を持つユーザーを除くすべてのユーザーに対してバックアップ仕様の内容を隠すように構成することができます。このように構成するには、グローバル オプション ファイルで、StrictSecurityFlags フラグを 0x0400 に設定します。

グローバル オプション ファイルに関する詳細は、『HP OpenView Storage Data Protector トラブルシューティング ガイド』を参照してください。

ホスト信頼

ホスト信頼機能を使用すると、一定数以下のクライアントの間で1つのクライアントから別のクライアントにデータを復元するだけのユーザーに対して「別のクライアントへ復元」ユーザー権限を割り当てる手間を減らすことができます。このためには、相互に信頼してデータをやり取りできるホストのグループを定義します。

ホスト信頼は、通常、以下の場合に使用します。

- データをやり取りするクライアントが、いずれも同じクラスター (複数のノードと1つの仮想サーバの組み合わせ) にある場合。
- クライアントのホスト名を変更した後、古いバックアップ オブジェクトのデータを復元する必要が生じた場合。

- DNS の問題が原因で、クライアントのホスト名とバックアップ オブジェクトの間に不適合がある場合。
- 複数のクライアントを所有しており、1つのクライアントのデータを別のクライアントに復元する必要がある場合。
- 1つのホストのデータを別のホストに移行する場合。

構成

ホスト信頼を構成するには、UNIX 用または Linux 用の Cell Manager の場合は `/etc/opt/omni/server/cell/host_trusts` ファイルを、Windows 用 Cell Manager の場合は `<Data_Protector_home>%Config%Server%cell%host_trusts` ファイルを作成します。

相互に信頼し合うホストのグループを定義するには、ホスト名のリストを中括弧で囲みます。以下に例を示します。

例：

```
GROUP="cluster.domain.com"
```

```
{  
    cluster.domain.com  
    node1.domain.com  
    node2.domain.com  
}
```

```
GROUP="Bajo"
```

```
{  
    computer.domain.com  
    anothercomputer.domain.com  
}
```

保護イベントのモニター

Data Protector の使用時に問題が検出された場合は、ログ ファイルの情報を使用して問題を特定できます。たとえば、記録されたイベントを手がかりに、正しく構成されていないユーザーやクライアントを特定できます。

インストールの保守 保護について

クライアントの保護イベント

クライアントの保護イベントは、セル内の各クライアントにある `inet.log` ファイルに記録されます。このファイルの場所は以下のとおりです。

- Windows の場合： `<Data_Protector_home>%log`
- HP-UX、Solaris、および Linux の場合： `/var/opt/omni/log`
- その他の UNIX システムの場合： `/usr/omni/log`

Cell Manager の保護イベント

Cell Manager の保護イベントは、以下の `security.log` ファイルに記録されます。

- Windows 用 Cell Manager の場合： `<Data_Protector_home>%log%server`
- UNIX 用 Cell Manager の場合： `/var/opt/omni/server/log`

インストールされている Data Protector パッチの確認

セル内の各システムにどの Data Protector パッチがインストールされているかについては、確認が可能です。

制限事項

パッチの確認には、以下の制限があります。

- パッチの確認は、Data Protector A.05.10 以降の Data Protector クライアントでのみ可能です。コマンド実行中に旧バージョンの Data Protector クライアントが検出された場合は、エラーメッセージが表示されます。
- このコマンドは、同じセル内のメンバーに対してのみ、インストール済みのパッチの確認を行います。

前提条件

この機能を使用するには、ユーザー インタフェース コンポーネントがインストールされている必要があります。

注記 サイト特定パッチのインストール後は、それが以降のパッチに含まれていたとしても、常にパッチレポートに表示されます。

セル内の特定のシステムにインストール済みの Data Protector パッチを確認するには、Data Protector GUI または CLI を使用します。

GUI を使用した Data Protector パッチの確認

Data Protector GUI を使用して、特定のクライアントにインストールしてあるパッチを確認するには、以下の手順に従ってください。

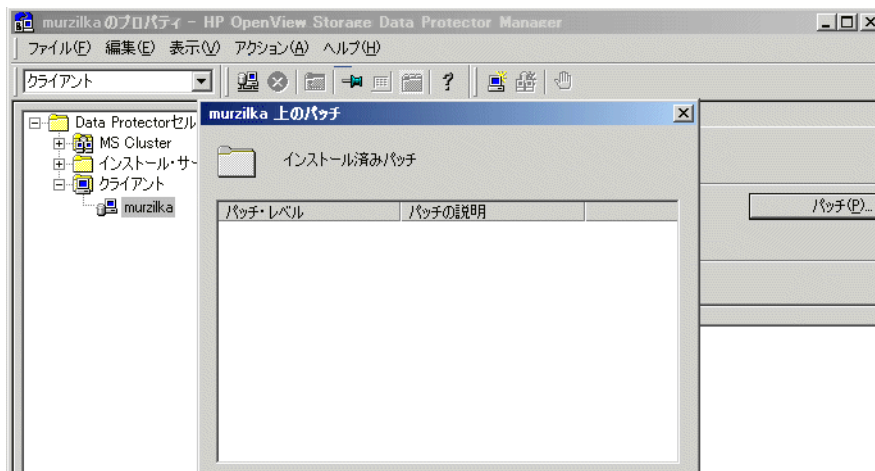
1. コンテキストリストで、[クライアント] を選択します。
2. Scoping ペインで、[クライアント] を展開し、インストール済みのパッチを確認するセル内のシステムを選択します。

インストールの保守

インストールされている Data Protector パッチの確認

3. [結果エリア]で [パッチ] をクリックすると、[パッチ] ウィンドウが開きます。

図 3-9 インストール済みパッチの確認



システム上でパッチが見つかった場合、各パッチのレベルと説明、インストール済みのパッチ数が表示されます。

システム上に Data Protector パッチがない場合は、空のリストが返されます。

確認対象のシステムがセルのメンバーでない場合や利用不能な場合、またはエラーが発生した場合は、エラーメッセージが表示されます。

4. [OK] をクリックしてウィンドウを閉じます。

CLI を使用した Data Protector パッチの確認

Data Protector CLI を使用して特定のクライアントにインストール済みのパッチを確認するには、以下のディレクトリから `omnicheck -patches -host hostname` コマンドを実行します。

- Windows の場合 : `<Data_Protector_home>\bin`
- UNIX または Linux の場合 : `/opt/omni/bin`

ここで、`hostname` は、確認対象システムの名前を表します。

`omnicheck` コマンドの詳細は、`omnicheck` マニュアルを参照してください。

Data Protector ソフトウェアのアンインストール

システム構成を変更した場合は、Data Protector ソフトウェアをシステムからアンインストールしたり、一部のソフトウェア コンポーネントを削除したりすることが必要になる場合があります。

アンインストール処理では、システムからすべての Data Protector ソフトウェア コンポーネントが削除され、さらに、そのシステムへのすべての参照が Cell Manager コンピュータ上の IDB から削除されます。ただし、Data Protector の構成データは、将来 Data Protector をアップグレードする際に必要になる可能性があるため、デフォルトではシステム上に残されます。Data Protector ソフトウェアのアンインストール後に構成データを削除するには、Data Protector のインストール先ディレクトリを削除します。

Data Protector がインストールされているディレクトリに他のデータがある場合は、Data Protector をアンインストールする前にこれらのデータを他の場所にコピーしてください。コピーしておかないと、アンインストール中にこれらのデータも削除されてしまいます。

Data Protector ソフトウェアをセルからアンインストールするには、以下の手順に従ってください。

1. GUI を使用して Data Protector クライアント ソフトウェアをアンインストールします。詳細は 214 ページの「Data Protector クライアントのアンインストール」を参照してください。
2. Data Protector の Cell Manager とインストール サーバをアンインストールします。詳細は 215 ページの「Cell Manager とインストール サーバのアンインストール」を参照してください。

Cell Manager やクライアントをアンインストールせずに、Data Protector ソフトウェア コンポーネントをアンインストールすることも可能です。詳細は 226 ページの「Data Protector ソフトウェア コンポーネントの変更」を参照してください。

UNIX の場合は、Data Protector ソフトウェアを手作業で削除することも可能です。詳細は 224 ページの「UNIX 上の Data Protector ソフトウェアの手動削除」を参照してください。

前提条件

Data Protector ソフトウェアをコンピュータからアンインストールする前に、以下の条件が満たされていることを確認してください。

- ✓ そのコンピュータに対するすべての参照がバックアップ仕様から削除されていること。アンインストールしたシステムへの参照がバックアップ仕様に残っていると、Data Protector は不明なクライアントのバックアップを実行しようとするため、バックアップ仕様のこの部分が正常に実行されません。バックアップ仕様の変更方法は、オンライン ヘルプの索引キーワード「変更, バックアップ仕様」で表示される内容を参照してください。

インストールの保守

Data Protector ソフトウェアのアンインストール

- ✓ アンインストール対象のシステムに接続および構成されているバックアップ デバイスが存在しないこと。Data Protector では、システムがエクスポートされると、そのバックアップ デバイスは元のセル内で使用できなくなります。

Data Protector クライアントのアンインストール

注記

リモートでアンインストールを行う場合は、Data Protector ソフトウェアのアンインストールを実行するプラットフォームにインストール サーバがインストールされている必要があります。

Data Protector GUI で以下の手順を実行すると、クライアントをリモートでアンインストールできます。

1. コンテキスト リストで、[**クライアント**] コンテキストを開きます。
2. Scoping ペインで [**クライアント**] を展開し、アンインストールするクライアントを右クリックして、[**削除**] をクリックします。Data Protector ソフトウェアを同時にアンインストールするかどうかを確認するメッセージが表示されます。
3. [**はい**] をクリックして、クライアントからすべてのソフトウェア コンポーネントをアンインストールするように指定し、[**完了**] をクリックします。

選択したクライアントが [**結果エリア**] のリストから削除され、Data Protector ソフトウェアがそのシステムのハード ディスクから物理的に削除されます。

Data Protector の構成データはクライアント システム上に残される点に注意してください。構成データを削除するには、Data Protector のインストール先ディレクトリを削除します。

クラスタ クライアント

Data Protector 環境内のクラスタ対応クライアントをアンインストールするには、以下の手順をローカルに実行してください。この手順は、Cell Manager やインストール サーバのアンインストール手順と同じです。詳細は 215 ページの「Cell Manager とインストール サーバのアンインストール」を参照してください。

選択したクラスタ クライアントが [**結果エリア**] のリストから削除され、Data Protector ソフトウェアがそのシステムのハード ディスクから物理的に削除されます。

TruCluster

TruCluster クライアントをアンインストールするには、まず仮想ノードをエクスポートします。その後、各ノードから Data Protector クライアントをアンインストールします。

OpenVMS クライアント

Data Protector OpenVMS クライアントは、インストール サーバを使ってリモートでアンインストールすることはできません。ローカルでアンインストールする必要があります。

Data Protector クライアントを OpenVMS システムからアンインストールするには、以下の手順に従ってください。

1. まず、192 ページの「セルからのクライアントのエクスポート」の説明に従って、Data Protector GUI を使用して Data Protector セルから対象クライアントをエクスポートします。

Data Protector ソフトウェアもアンインストールするかを確認するメッセージが表示されたら、[いいえ] を選択します。
2. Data Protector クライアント ソフトウェアを実際に削除するには、OpenVMS クライアント上で SYSTEM アカウントにログインし、以下のコマンドを実行します。

```
$ PRODUCT REMOVE DP
```

プロンプトに [YES] と応答します。

重要

これで Data Protector サービスがシャットダウンされ、OpenVMS システム上の Data Protector に関連するすべてのディレクトリ、ファイル、アカウントが削除されます。

Cell Manager とインストール サーバのアンインストール

ここでは Data Protector の Cell Manager とインストール サーバソフトウェアを Windows、HP-UX、および Solaris システムからアンインストールする方法について説明します。

Windows システムからのアンインストール

MS Cluster Server システムでのアンインストール

HP OpenView AutoPass ユーティリティを Data Protector とともに Microsoft Cluster Server ノードにインストールした場合は、そのノードから Data Protector をアンインストールする必要があります。そうしなければ、AutoPass がアンインストールされません。

Data Protector ソフトウェアを Windows システムからアンインストールするには、以下の手順に従ってください。

1. すべての Data Protector セッションを終了し、グラフィカル ユーザー インタフェース (GUI) を閉じておきます。

- Windows の [コントロール パネル] で [アプリケーションの追加と削除] をクリックします。
- この後の操作は、HP OpenView AutoPass をインストールしたかどうかによって、また Data Protector の構成データを削除するかどうかによって異なります。

重要

Data Protector のアンインストール後もシステム上に構成データを残しておき、後からそのシステムに、アンインストールしたバージョンよりも古い Data Protector Cell Manager をインストールすると、構成データが使用できなくなることに注意してください。

古いバージョンを適切にインストールするには、構成データを削除するオプションをインストール中に選択する必要があります。

以下の手順に従ってください。

- AutoPass ユーティリティが Data Protector とともにインストールされている場合

[HP OpenView Storage Data Protector A.05.50] を選択し、[変更] をクリックします。次に、[Next] をクリックします。[Program Maintenance] ダイアログ ボックスで、[Remove] を選択します。Data Protector の構成データを完全に削除する場合は、[Permanently remove the configuration data] を選択します。それ以外の場合は、[Next] をクリックします。

AutoPass が Data Protector とともにインストールされており、現在 AutoPass を使用しているアプリケーションが Data Protector のみである場合は、AutoPass も削除されます。それ以外の場合、AutoPass は Data Protector に登録されていない状態になるだけであり、インストールされたまま残ります。

- AutoPass がインストールされていない場合

— Data Protector をアンインストールしても、Data Protector の構成データはシステム上に残しておく場合は、[HP OpenView Storage Data Protector A.05.50] を選択し、[削除] をクリックします。

— Data Protector をアンインストールし、Data Protector の構成データも削除する場合は、[HP OpenView Storage Data Protector A.05.50] を選択します。次に、[変更] をクリックし、[Next] をクリックします。[Program Maintenance] ダイアログ ボックスで、[Remove] を選択します。次に [Permanently remove the configuration data] を選択し、[Next] をクリックします。

4. アンインストールが完了したら、[完了] をクリックして、ウィザードを終了します。

Cell Manager のアンインストールの際に AutoPass が削除された場合は、[アプリケーションの追加と削除] ウィンドウで **[F5]** キーを押すと、インストールされているプログラムとコンポーネントのリストが更新されます。

HP-UX システムからのアンインストール

重要

Data Protector のアンインストール後も構成データをシステム上に残しておき、後からそのシステムに、アンインストールしたバージョンよりも古い Data Protector Cell Manager をインストールすると、構成データが使用できなくなることに注意してください。

古いバージョンを適切にインストールするには、アンインストールの終了後に、残っている Data Protector ディレクトリをシステムから削除する必要があります。

Data Protector ソフトウェアをアンインストールする前に、Cell Manager システムおよびインストール サーバシステム上で実行されている Data Protector プロセスをシャットダウンする必要があります。

1. root ユーザーとしてログインし、`/opt/omni/sbin` ディレクトリから `omnisv -stop` コマンドを実行します。
2. `ps -ef | grep omni` コマンドを実行して、すべてのプロセスがシャットダウンされているかどうかを確認します。`ps -ef | grep omni` コマンドを実行しても、Data Protector プロセスは表示されないはずです。

実行中の Data Protector プロセスがある場合は、アンインストールを開始する前に、`kill -9 <process_ID>` コマンドを実行してそのプロセスを停止してください。

3. `/usr/sbin/swremove DATA-PROTECTOR` を実行して、Data Protector ソフトウェアをアンインストールします。
4. HP OpenView AutoPass ユーティリティは、Data Protector のアンインストール中に削除されません。AutoPass ユーティリティは、`/usr/sbin/swremove HPOVLIC` コマンドを root ユーザーとして実行することにより、手作業で削除できます。

残っている Data Protector ディレクトリをシステムから削除する方法は、224 ページの「UNIX 上の Data Protector ソフトウェアの手動削除」を参照してください。

MC/ServiceGuard 上に構成されている Cell Manager およびインストール サーバのアンインストール

MC/ServiceGuard クラスタ上に Cell Manager やインストール サーバを構成している場合は、以下の手順に従ってソフトウェアをアンインストールしてください。

一次ノード

一次ノードにログオンし、以下の手順に従ってください。

1. Data Protector パッケージを停止します。

```
cmhaltpkg <pkg_name>
```

<pkg_name> には、クラスタ パッケージの名前を指定します。

例：

```
cmhaltpkg ob2c1
```

2. ボリューム グループのクラスタ モードを非アクティブ化します。

```
vgchange -c n <vg_name>
```

<vg_name> には、/dev ディレクトリのサブディレクトリ内に存在するボリューム グループのパス名を指定します。

例：

```
vgchange -c n /dev/vg_ob2cm
```

3. ボリューム グループをアクティブ化します。

```
vgchange -a y -q y <vg_name>
```

例：

```
vgchange -a y -q y /dev/vg_ob2cm
```

4. 論理ボリュームを共有ディスクにマウントします。

```
mount <lv_path> <shared_disk>
```

<lv_path> には論理ボリュームのパス名、<shared_disk> にはマウント ポイントまたは共有ディレクトリを指定します。

例：

```
mount /dev/vg_ob2cm/lv_ob2cm /omni_shared
```

5. swremove ユーティリティを使用して、Data Protector を削除します。

6. ソフトリンクを削除します。

```
rm /etc/opt/omni
```

```
rm /var/opt/omni
```

7. バックアップ ディレクトリを削除します。

```
rm -rf /etc/opt/omni.save
```

```
rm -rf /var/opt/omni.save
```

8. Data Protector ディレクトリを、その内容とともに削除します。

```
rm -rf /opt/omni
```

9. HP OpenViewAutoPass ユーティリティは、`/usr/sbin/swremove HPOVLIC` コマンドを root ユーザーとして実行することにより、手作業で削除できます。

10. 共有ディスクのマウントを解除します。

```
umount <shared_disk>
```

例：

```
umount /omni_shared
```

11. ボリューム グループを非アクティブ化します。

```
vgchange -a n <vg_name>
```

例：

```
vgchange -a n /dev/vg_ob2cm
```

二次ノード

二次ノードにログオンし、以下の手順に従ってください。

1. ボリューム グループをアクティブ化します。

```
vgchange -a y <vg_name>
```

2. 共有ディスクをマウントします。

```
mount <lv_path> <shared_disk>
```

3. `swremove` ユーティリティを使用して、Data Protector を削除します。

4. ソフト リンクを削除します。

```
rm /etc/opt/omni
```

```
rm /var/opt/omni
```

5. バックアップ ディレクトリを削除します。

インストールの保守

Data Protector ソフトウェアのアンインストール

```
rm -rf /etc/opt/omni.save
```

```
rm -rf /var/opt/omni.save
```

6. Data Protector ディレクトリを、その内容とともに削除します。

```
rm -rf /opt/omni
```

7. 共有ファイルシステム内のディレクトリを削除します。

```
rm -rf <shared_disk>/etc_opt_omni
```

```
rm -rf <shared_disk>/var_opt_omni
```

例 :

```
rm -rf /omni_shared/etc_opt_omni
```

```
rm -rf /omni_shared/etc_opt_omni
```

8. HP OpenViewAutoPass ユーティリティは、`/usr/sbin/swremove HPOVLIC` コマンドを root ユーザーとして実行することにより、手作業で削除できます。

9. 共有ディスクのマウントを解除します。

```
umount <shared_disk>
```

10. ボリューム グループを非アクティブ化します。

```
vgchange -a n <vg_name>
```

以上で Data Protector がシステムから完全に削除されました。

Solaris システムからのアンインストール

Cell Manager

Solaris 用 Cell Manager は、必ず `omnisetup.sh` コマンドを使用してローカルにインストールされています。そのため、`pkgrm` ユーティリティを使用して、ローカルにアンインストールしなければなりません。

重要

Data Protector のアンインストール後も構成データをシステム上に残しておき、後からそのシステムに、アンインストールしたバージョンよりも古い Data Protector Cell Manager をインストールすると、構成データが使用できなくなることに注意してください。

古いバージョンを適切にインストールするには、アンインストールの終了後に、残っている Data Protector ディレクトリをシステムから削除する必要があります。

Data Protector Cell Manager をアンインストールするには、以下の手順に従ってください。

1. すべての Data Protector セッションを終了し、グラフィカル ユーザー インタフェースを閉じておきます。
2. `pkginfo | grep OB2` コマンドを入力して、Cell Manager 上にインストールされているすべての Data Protector パッケージを一覧表示します。

Cell Manager に関連するパッケージは以下のとおりです。

OB2-CORE	Data Protector のコア ソフトウェア
OB2-C-IS	インストール サーバソフトウェア
OB2-CS	Cell Manager ソフトウェア
OB2-CC	Cell Console ソフトウェアには、グラフィカル ユーザー インタフェースとコマンド行インタフェースが含まれます。

システム上に Data Protector クライアントやインストール サーバもインストールされている場合は、一覧内にその他のパッケージも示されます。

注記 インストールされている Data Protector コンポーネントの中に残しておきたいものがある場合は、OB2-CORE パッケージを削除しないでください。これは、他のパッケージとの関連性を保つためです。

3. インストールとは逆の順番で、前述の手順で挙げたパッケージを削除します。 `pkgrm <package name>` コマンドを実行し、プロンプトに従ってください。
4. HP OpenViewAutoPass ユーティリティは、Data Protector のアンインストール中に削除されません。AutoPass ユーティリティは、以下のコマンドを root ユーザーとして実行することにより、手作業で削除できます。

```
swremove HPOvLic
swremove HPOvLicJ
```

インストール サーバ

Solaris 上の UNIX 用インストール サーバは、必ず `omnisetup.sh` コマンドを使用してローカルにインストールされています。そのため、`pkgrm` ユーティリティを使用して、ローカルにアンインストールしなければなりません。

インストールの保守

Data Protector ソフトウェアのアンインストール

Data Protector インストール サーバをアンインストールするには、以下の手順に従ってください。

1. すべての Data Protector セッションを終了し、グラフィカル ユーザー インタフェース (GUI) を閉じておきます。
2. `pkginfo | grep OB2` コマンドを入力して、インストール サーバシステム上にインストールされているすべての Data Protector パッケージを一覧表示します。

インストール サーバに関連するパッケージは以下のとおりです。

OB2-CORE	Data Protector のコア ソフトウェア
OB2-C-IS	インストール サーバのコア ソフトウェア
OB2-SOLUX	リモートの Solaris システムのための Disk Agent 用、Media Agent 用、および GUI パッケージ
OB2-OTHUX	Solaris 以外のリモートの UNIX システムのための Disk Agent 用および Media Agent 用パッケージ

システム上にその他の Data Protector コンポーネントもインストールされている場合は、一覧内にその他のコンポーネントも示されます。

注記 インストールされている Data Protector コンポーネントの中に残しておきたいものがある場合は、OB2-CORE パッケージを削除しないでください。これは、他のパッケージとの関連性を保つためです。

3. インストールとは逆の順番で、前述の手順で挙げたパッケージを削除します。 `pkgrm <package name>` コマンドを実行し、プロンプトに従ってください。

Linux システムからのアンインストール

Cell Manager

Linux 用 Cell Manager は、必ず `omnisetup.sh` コマンドを使用してローカルにインストールされています。そのため、`rpm` ユーティリティを使用して、ローカルにアンインストールしなければなりません。

重要 Data Protector のアンインストール後も構成データをシステム上に残しておき、後からそのシステムに、アンインストールしたバージョンよりも古い Data Protector Cell Manager をインストールすると、構成データが使用できなくなることに注意してください。

古いバージョンを適切にインストールするには、アンインストールの終了後に、残っている Data Protector ディレクトリをシステムから削除する必要があります。

Data Protector Cell Manager をアンインストールするには、以下の手順に従ってください。

1. すべての Data Protector セッションを終了し、グラフィカル ユーザー インタフェースを閉じておきます。
2. `rpm -qa | grep OB2` コマンドを入力して、Cell Manager 上にインストールされているすべての Data Protector パッケージを一覧表示します。

Cell Manager に関連するパッケージは以下のとおりです。

OB2-CORE	Data Protector のコア ソフトウェア
OB2-CORE-IS	インストール サーバソフトウェア
OB2-CS	Cell Manager ソフトウェア
OB2-CC	Cell Console ソフトウェア (コマンド行インタフェースを含む)

システム上に Data Protector クライアントやインストール サーバもインストールされている場合は、一覧内にその他のパッケージも示されます。

注記 インストールされている Data Protector コンポーネントの中に残しておきたいものがある場合は、OB2-CORE パッケージを削除しないでください。これは、他のパッケージとの関連性を保つためです。

3. インストールとは逆の順番で、前述の手順で挙げたパッケージを削除します。 `rpm -e <package name>` コマンドを実行し、プロンプトに従ってください。

インストール サーバ

Linux 上の UNIX 用インストール サーバは、必ず `omnisetup.sh` コマンドを使用してローカルにインストールされています。そのため、`rpm` を使用して、ローカルにアンインストールしなければなりません。

Data Protector インストール サーバをアンインストールするには、以下の手順に従ってください。

1. すべての Data Protector セッションを終了し、グラフィカル ユーザー インタフェース (GUI) を閉じておきます。
2. `rpm -qa | grep OB2` コマンドを入力して、インストール サーバシステム上にインストールされているすべての Data Protector パッケージを一覧表示します。

インストールの保守

Data Protector ソフトウェアのアンインストール

インストール サーバに関連するパッケージは以下のとおりです。

OB2-CORE	Data Protector のコア ソフトウェア
OB2-CORE-IS	インストール サーバのコア ソフトウェア
OB2-LINUXP	リモートの Linux システムのための Disk Agent 用、Media Agent 用、および GUI パッケージ
OB2-OTHUXP	Linux 以外のリモートの UNIX システムのための Disk Agent 用および Media Agent 用パッケージ

システム上にその他の Data Protector コンポーネントもインストールされている場合は、一覧内にその他のコンポーネントも示されます。

注記 インストールされている Data Protector コンポーネントの中に残しておきたいものがある場合は、OB2-CORE パッケージを削除しないでください。これは、他のパッケージとの関連性を保つためです。

3. インストールとは逆の順番で、前述の手順で挙げたパッケージを削除します。rpm -e <package name> コマンドを実行し、プロンプトに従ってください。

UNIX 上の Data Protector ソフトウェアの手動削除

UNIX クライアントのアンインストールを開始する前に、そのクライアントをセルからエクスポートする必要があります。エクスポート手順については、192 ページの「セルからのクライアントのエクスポート」を参照してください。

HP-UX システム

HP-UX システムからファイルを手作業で削除するには、以下の手順に従ってください。

1. /usr/sbin/swremove DATA-PROTECTOR コマンドを実行して、Data Protector ソフトウェアを削除します。
2. rm コマンドを使って、以下のディレクトリを削除します。

```
rm -fr /var/opt/omni
```

```
rm -fr /etc/opt/omni
```

```
rm -fr /opt/omni
```

この時点で、Data Protector への参照がシステム内に残っていないことを確認してください。

Solaris システム

Solaris システムからファイルを手作業で削除するには、これらのファイルを以下のディレクトリから削除し、次に `rm` コマンドを使用してディレクトリを削除してください。

```
rm -fr /var/opt/omni
rm -fr /etc/opt/omni
rm -fr /opt/omni
```

Linux システム

Linux システムからファイルを手作業で削除するには、これらのファイルを以下のディレクトリから削除し、次に `rm` コマンドを使用してディレクトリを削除してください。

```
rm -fr /var/opt/omni
rm -fr /etc/opt/omni
rm -fr /opt/omni
```

その他の UNIX システムの場合

以下のディレクトリからファイルを削除し、次に `rm` コマンドを使用してディレクトリを削除してください。

```
rm -fr /usr/omni
```

Data Protector ソフトウェア コンポーネントの変更

ここでは Data Protector のソフトウェア コンポーネントを Windows、HP-UX、および Solaris システムに追加または削除する方法について説明します。各オペレーティング システムでサポートされている Data Protector コンポーネントの一覧は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。

Data Protector ソフトウェア コンポーネントは、Data Protector GUI を使用して、Cell Manager またはクライアント上に追加できます。選択したコンポーネントは、インストール サーバの機能を使用して、リモートでインストールします。手順の詳細は、50 ページの「Data Protector クライアントのリモート インストール」を参照してください。

Data Protector コンポーネントは、Cell Manager またはクライアントからローカルに削除できます。

Windows システムの場合

Windows システム上で Data Protector ソフトウェア コンポーネントを追加または削除するには、以下の手順を行います。

1. Windows の [コントロールパネル] で [アプリケーションの追加と削除] をクリックします。
2. [HP OpenView Storage Data Protector A.05.50] を選択し、[変更] をクリックします。
3. [Next] をクリックします。
4. [Program Maintenance] ウィンドウで [Modify] をクリックし、[Next] をクリックします。
5. [Component Selection] ウィンドウで、追加するソフトウェア コンポーネントを選択し、削除するコンポーネントがあれば選択解除します。[Next] をクリックします。
6. [Install] をクリックして、ソフトウェア コンポーネントのインストールまたは削除を開始します。
7. インストールが完了したら、[Finish] をクリックします。

クラスタ対応クライアント

クラスタ対応クライアント上の Data Protector ソフトウェア コンポーネントを変更する場合は、各クラスタ ノード上で DVD-ROM を使用してローカルに変更作業を行う必要があります。その後、GUI を使用して、仮想サーバのホスト名を Data Protector セルに手作業でインポートしてください。

HP-UX システムの場合

新しいコンポーネントの追加には、インストール サーバ機能を使用します。HP-UX システムの場合は、一部の Data Protector ソフトウェア コンポーネントが互いに依存しているため、それらの一部を削除すると正常に動作しなくなる可能性があります。

このようなコンポーネントとそれらの依存関係を、下表に示します。

表 3-1 HP-UX 上の Data Protector ソフトウェア コンポーネントの依存関係

コンポーネント	依存関係
OMNI-MOMGUI	OMNI-CC
OMNI-CC、OMNI-CORE-IS	OMNI-CORE
OMNI-CS	OMNI-CORE、OMNI-CC
OMNI-INTEG、OMNI-DA、 OMNI-MA、または、OMNI-NDMP	OMNI-CORE
OMNI-NDMP-P	OMNI-CORE-IS
OMNI-INF-P、OMNI-SYB-P、 OMNI-ORA-P、OMNI-OR8-P、 OMNI-SAP-P、OMNI-SAPDB-P、 OMNI-DB2-P、OMNI-EMC-P、 OMNI-SSEA-P、OMNI-SNAPA-P、 OMNI-SMISA-P	OMNI-INTEG OMNI-CORE-IS
OMNI-HPUX-P、OMNI-OTHUX-P、 OMNI-OMNIST	OMNI-CORE-IS
OMNI-LOTUS-P、OMNI-OV-P	OMNI-CORE-IS

手順

Data Protector ソフトウェア コンポーネントを削除するには、以下の手順を行います。

1. root としてログインし、swremove コマンドを実行します。
2. [B6960MA]、[DATA-PROTECTOR]、[OB2-CM] を順にダブルクリックして、Data Protector コンポーネントのリストを表示します。
3. 削除対象のコンポーネントを選択します。

インストールの保守

Data Protector ソフトウェア コンポーネントの変更

4. [Actions] メニューで [Mark for Remove] をクリックして、削除対象のコンポーネントをマークします。
5. 削除対象のコンポーネントをマークした後、[Actions] メニューで [Remove] をクリックし、[OK] をクリックします。

注記

削除する Data Protector コンポーネントをマークしたときに、そのコンポーネントを削除するとほかのコンポーネントが正常に動作しなくなる場合は、[Dependency Message Dialog] ボックスが表示されて、依存するコンポーネントのリストが示されます。

Oracle 固有の問題

Oracle server システム上で Data Protector Oracle 用統合ソフトウェアをアンインストールした後も、Oracle Server ソフトウェアは引き続き Data Protector データベース ライブラリとリンクされています。このリンクは削除する必要があります。削除しなかった場合は、統合ソフトウェアの削除以後、Oracle Server は起動しなくなります。詳細は『HP OpenView Storage Data Protector インテグレーション ガイド』の「UNIX システムにおける Data Protector Oracle 用統合ソフトウェア削除後の Oracle の使用」を参照してください。

Solaris システムの場合

新しいコンポーネントの追加には、インストール サーバ機能を使用します。Solaris システムの場合は、一部の Data Protector ソフトウェア コンポーネントが互いに依存しているため、それらの一部を削除すると正常に動作しなくなる可能性があります。

このようなコンポーネントとそれらの依存関係を、下表に示します。

表 3-2 Solaris 上の Data Protector ソフトウェア コンポーネントの依存関係

コンポーネント	依存関係
OB2-MOMGUI	OB2-CC
OB2-CC、OB2-C-IS	OB2-CORE
OB2-CS	OB2-CORE、OB2-CC
OB2-INTGP、OB2-DA、OB2-MA、または、OB2-NDMPP	OB2-CORE

**表 3-2 Solaris 上の Data Protector ソフトウェア
コンポーネントの依存関係 (続き)**

コンポーネント	依存関係
OB2-SOLUX	OB2-C-IS
OB2-INFP、OB2-SYBP、OB2-OR8P、 OB2-SAPP、OB2-SAPDP、 OB2-DB2P、OB2-SSEAP、OB2-SMISP	OB2-INTGP OB2-C-IS
OB2-OTHUX、OB2-OSTP、 OB2-LOTP、OB2-OVP	OB2-C-IS

手順

Solaris システムから Data Protector ソフトウェア コンポーネントを削除するには、以下の手順を行います。

1. すべての Data Protector セッションを終了し、グラフィカル ユーザー インタフェース (GUI) を閉じておきます。
2. `pkginfo | grep OB2` コマンドを入力して、インストールされているすべての Data Protector パッケージを一覧表示します。
3. インストールとは逆の順番で、前述の手順で挙げたパッケージを削除します。 `pkgrm <package name>` コマンドを実行し、プロンプトに従ってください。

その他の UNIX システムの場合

Solaris および HP-UX 以外の他の UNIX システム上の Data Protector クライアントからコンポーネントを手作業で削除した場合は、`/usr/omni/bin/install/omni_info` にある `omni_info` ファイルを更新する必要があります。

アンインストールした各コンポーネントについて、対応するコンポーネント バージョン文字列を `omni_info` ファイルから削除してください。

Data Protector クライアントからコンポーネントを削除しただけで、クライアントをセルからエクスポートしていない場合は、Cell Manager 上にある `cell_info` ファイル内のセル構成情報を更新する必要があります。このためには、セル内の Cell Console コンポーネントがインストールされているシステムから、以下のコマンドを実行します。

```
/opt/omni/bin/omnicc -update_host <HostName>
```

インストールの保守

Data Protector ソフトウェア コンポーネントの変更

4 Data Protector A.06.00 へのアップグレード

この章の内容

この章では、Data Protector のアップグレードと移行の手順について説明します。

アップグレードの概要

作業を開始する前に

既存のプロダクト バージョンを Data Protector A.06.00 にアップグレードする前に、以下の点を考慮してください。

- サポート対象およびサポート対象ではなくなるプラットフォームとバージョンを、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス』で確認してください。
- アップグレード後は、Cell Manager、インストール サーバ、およびすべてのクライアントに同じバージョンの Data Protector がインストールされていなければなりません。
- マルチ セル (MoM) 環境のアップグレード後は、すべての Cell Manager に同じバージョンの Data Protector がインストールされていなければなりません。
- Data Protector A.05.00、Data Protector A.05.10、または Data Protector A.05.50 用の恒久ライセンスをお持ちの場合は、その恒久ライセンスを Data Protector A.06.00 でも使用できます。

上記のいずれにも当てはまらない場合は、暫定ライセンスを使用することになります。この場合、ライセンスの有効期間は、最初のインストール後 60 日間です。

ライセンスの詳細は、293 ページの第 5 章「Data Protector のライセンス」を参照してください。

前提条件

- 既存の Cell Manager システムと内部データベース (IDB) をバックアップしてください。

制限事項

- Data Protector A.06.00 へのアップグレードは、Data Protector の A.05.00、A.05.10、および A.05.50 からのみサポートされています。
- 以前のバージョンの Data Protector で作成した内部データベースのバックアップを、Data Protector A.06.00 で復元することはできません。Cell Manager のアップグレードが終了したら、Data Protector の使用を継続する前に、内部データベースを必ずバックアップしてください。

Data Protector A.06.00 へのアップグレード アップグレードの概要

- Cell Manager プラットフォームの変更は、Data Protector A.06.00 リリースではサポートされていません。アップグレードは同一の Cell Manager プラットフォーム上でのみ可能です (HP-UX から HP-UX、Solaris から Solaris、Windows から Windows)。
- いったん Data Protector A.06.00 にアップグレードすると、それ以前に Data Protector バージョン A.05.00 で作成した Microsoft Exchange Server シングル メールボックスのバックアップからの復元はできなくなります。ただし、ファイルシステムの復元を使用して、既存のバックアップを .pst ファイルに復元することは可能です。
- Windows 上で Data Protector A.06.00 にアップグレードする場合に、Microsoft Installer (MSI) のバージョンが 2.0 より古いと、Data Protector セットアッププログラムにより、自動的にバージョン 2.0 にアップグレードされます。この場合アップグレードの最後に、MSI がアップグレードされたことが Data Protector から通知されます。MSI がアップグレードされた場合は、システムを再起動することを強く推奨します。各種 Windows オペレーティングシステムに対する MSI 2.0 の要件については、Microsoft Support にお問い合わせください。

システム上の MSI のバージョンを確認するには、エクスプローラで `c:\%windnt%\system32\msi.dll` ファイルを右クリックし、[プロパティ] を選択します。[プロパティ] ダイアログ ボックスで [バージョン情報] を選択してください。

アップグレードの手順

以前のバージョンから Data Protector A.06.00 にセルをアップグレードするには、以下の手順で行います。

1. Cell Manager とインストール サーバを Data Protector A.06.00 にアップグレードします。この手順は、UNIX プラットフォームと Windows プラットフォームで異なります。

インストール サーバをアップグレードする前に、まず、現在のセルの Cell Manager をアップグレードする必要があることに注意してください。

一部のセル構成では、Cell Manager のアップグレード後に、IDB 内のファイル名を変換する必要があります。変換が必要な場合はメッセージが表示されます。詳細は、262 ページの表 4-1 および 264 ページの表 4-2 を参照してください。
2. GUI クライアントをアップグレードします。
3. オンライン アプリケーション統合ソフトウェア (Oracle、SAP R/3、Informix Server、Microsoft SQL Server、Microsoft Exchange Server など) がインストールされているクライアントをアップグレードします。

4. Media Agent (MA) がインストールされているクライアントをアップグレードします。Cell Manager とプラットフォームが同一のすべての MA クライアント上で MA がアップグレードされたら、ただちにバックアップの実行が可能になります。Data Protector A.05.00 および A.05.10 の MA クライアントには、一定の制限があります。詳細は、262 ページの表 4-1 および 264 ページの表 4-2 を参照してください。
5. ファイルシステム Disk Agent (DA) がインストールされているクライアントを、2 週間以内にアップグレードします。

IDB ファイル名の変換の前後のバックアップと復元における DA バージョンの影響に関する詳細は、262 ページの「IDB 内でのファイル名の変更」を参照してください。

MoM 環境でのアップグレード

MoM 環境を Data Protector A.06.00 にアップグレードする場合は、最初に MoM Manager システムをアップグレードする必要があります。この作業後、アップグレードされていない以前のバージョンの Cell Manager は、中央 MMDB および中央ライセンス機能にアクセスしてバックアップを実行することはできますが、その他の MoM 機能は使用できなくなります。Data Protector A.06.00 MoM セルと以前のバージョンがインストールされたセルの間でデバイスを共有することはできません。アップグレード中は、MoM 環境内のすべての Cell Manager の動作を停止させておく必要があります。

IDB でのファイル名変換の必要性

Data Protector バージョン A.05.50 および A.06.00 では、異なるプラットフォーム上の異なる地域設定 (ロケール) で作成されたファイル名の処理と表示の機能が改善されています。このため、Data Protector A.05.00 または A.05.10 からアップグレードする場合、一部のセル構成では IDB 内の既存ファイル名の変換が必要になります。

変換は以下のように実行されます。

- UNIX Cell Manager が Windows クライアントのアップグレード後のバックアップの一部として実行
- Windows Cell Manager が Cell Manager のアップグレード後のバックグラウンドプロセスとして実行

IDB の変換が必要な場合は、プロンプトが表示されます。

UNIX

UNIX Cell Manager では、以下の時点までに、Windows クライアントのアップグレード後の IDB の変換が実行されます。

Data Protector A.06.00 へのアップグレード アップグレードの概要

- 変換の期限切れ、または、
- セル内のすべての Windows クライアントに対するフルバックアップが実行されるまで。この手順は非常に重要で、必ず実行しなければなりません。

ファイル名の変換パフォーマンスの詳細については、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。

Windows

Windows Cell Manager では、IDB の変換を延期できますが、これが実行されるまで、一定の制限があります。

Windows 用および UNIX 用 Cell Manager における IDB 内のファイル名変換の詳細については、262 ページの「IDB 内でのファイル名の変更」を参照してください。

Data Protector A.05.x からのアップグレード

Data Protector A.05.x リリースバージョンは、UNIX 用または Windows 用の Data Protector A.06.00 へ直接アップグレードできます。

ライセンス

既存の Data Protector A.05.x ライセンスは、Data Protector A.06.00 と完全に互換性があり、使用可能です。ライセンスの詳細は、293 ページの第 5 章「Data Protector のライセンス」を参照してください。

作業を開始する前に

アップグレード開始前に、アップグレード手順の制限の詳細について、233 ページの「アップグレードの概要」を参照してください。

注記

この章では、DVD-ROM インストールメディアを使用している場合を想定して、Cell Manager およびインストールサーバのインストール手順と、クライアントのローカルインストール手順を説明しています。CD-ROM メディアを使用している場合は、C-1 ページの「付録 C」も参照してください。参照先には、インストール手順の違いと、CD-ROM の一覧が示されています。

UNIX 用 Cell Manager とインストールサーバのアップグレード

前提条件

- `/opt/omni/sbin/omnisv -stop` コマンドを実行して、Data Protector サービスを停止します。
- Solaris 上で古いパッチがインストールされている場合は、アップグレード前にそれらをアンインストールします。
- K シェル (ksh) がインストールされていることを確認します。
- アップグレードを実行するには root パーミッションが必要です。

HP-UX 用または Solaris 用のインストールサーバが Cell Manager とともにインストールされている場合は、`omnisetup.sh` コマンドの実行時に自動的にアップグレードされます。

Data Protector A.06.00 へのアップグレード

Data Protector A.05.x からのアップグレード

HP-UX 用または Solaris 用のインストール サーバが別のシステムにインストールされている場合は、241 ページの「インストール サーバのアップグレード」を参照してください。

Cell Manager のアップグレード

`omnisetup.sh` コマンドの実行時に、HP-UX 用または Solaris 用の Cell Manager は、自動的にアップグレードされます。

HP-UX では、このコマンドは `swinstall` ユーティリティを使用して、既存のパッケージ セットを直接アップグレードします。Solaris では、このコマンドは `pkgrm` ユーティリティを使用して既存のパッケージ セットを削除し、`pkgadd` ユーティリティを使用して新しいパッケージをインストールします。

インストール サーバがクライアント コンポーネントとともにインストールされている場合、インストール サーバは `omnisetup.sh` コマンドで削除されます。この場合、`omnisetup.sh -IS` コマンドを使用して新しいインストール サーバ デポをインストールした後、アップグレード後のインストール サーバを再度インポートしてください。詳細な作業手順は、187 ページの「セルへのインストール サーバのインポート」を参照してください。

MC/ServiceGuard

MC/ServiceGuard 上で構成された Cell Manager のアップグレード手順は、MC/ServiceGuard 環境で実行されていない Cell Manager のアップグレード手順とは異なります。アップグレードに必要な手順の詳細は、285 ページの「MC/ServiceGuard 上で構成されている Cell Manager のアップグレード」を参照してください。

カーネル パラメータの設定

HP-UX では、カーネルパラメータ `maxdsiz` (最大データ セグメント サイズ) を 134217728 バイト (128 MB) 以上に、また、カーネルパラメータ `semnu` (セマフォ取り消し構造体の数) を 256 以上に、それぞれ設定することをお勧めします。パラメータを変更したときは、カーネルを再コンパイルし、マシンを再起動してください。

Solaris システムでは、`/etc/system` のカーネルパラメータ `shmsys:shminfo_shmmax` (最大共有メモリ セグメント サイズ [SHMMAX]) を 67108864 バイト (64 MB) 以上に設定することをお勧めします。変更を行った場合は、マシンを再起動してください。

アップグレード手順

HP-UX 用または Solaris 用の Cell Manager を Data Protector A.06.00 にアップグレードするには、以下の手順に従います。

1. UNIX インストール DVD-ROM をドライブに挿入し、マウント ポイントにマウントします。

例：

```
mkdir /dvdrom  
mount /dev/c0d0t0 /dvdrom
```

オプションで、ディスク上のデポから Data Protector をインストールする場合は、以下の手順を実行します。

- インストールファイルが格納されている DP_DEPOT ディレクトリ、AUTOPASS ディレクトリ、および LOCAL_INSTALL ディレクトリをローカルディスクにコピーする場合は、以下のコマンドを実行します。

```
mkdir <directory>  
cp -r /dvdrom/<platform_dir>/DP_DEPOT <directory>  
cp -r /dvdrom/<platform_dir>/AUTOPASS <directory>  
cp -r /dvdrom/LOCAL_INSTALL <directory>
```

ここで、<platform_dir> には、以下のいずれかの値を指定します。

hpux_ia	IA-64 システム上の HP-UX 11.23
hpux_pa	PA-RISC システム上の HP-UX
solaris	Solaris システム

- DVD-ROM 全体をローカルディスクにコピーする場合は、以下のコマンドを実行します。

```
cp -r /dvdrom <dvd_image_dir>
```

2. omnisetup.sh コマンドを実行します。

このコマンドを DVD-ROM から実行するには、以下のようにして実行します。

```
cd /dvdrom/LOCAL_INSTALL  
./omnisetup.sh
```

ディスクからインストールを開始する場合は、以下の手順を実行します。

- DP_DEPOT ディレクトリ、AUTOPASS ディレクトリ、および LOCAL_INSTALL ディレクトリをローカルディスク上の <directory> にコピーした場合は、omnisetup.sh コマンドが格納されているこのディレクトリに移動して以下を実行します。

```
cd <directory>/LOCAL_INSTALL  
./omnisetup.sh
```

- DVD-ROM 全体を <dvd_image_dir> にコピーした場合は、omnisetup.sh コマンドをパラメータなしで実行します。

Data Protector A.06.00 へのアップグレード

Data Protector A.05.x からのアップグレード

```
cd <dvd_image_dir>/LOCAL_INSTALL
./omnisetup.sh
```

3. omnisetup.sh コマンドを実行するとプロンプトが表示され、購入済みライセンスのパスワードを HP Password Delivery Center の Web サーバからインターネットを介して直接ダウンロードしてインストールする場合は、HP OpenView AutoPass ユーティリティをインストールまたはアップグレードするよう指示されます。AutoPass ユーティリティの詳細は、309 ページの「HP OpenView AutoPass ユーティリティを使用した恒久パスワードの取得とインストール」を参照してください。AutoPass はできるだけインストールすることをお勧めします。

AutoPass を MC/ServiceGuard にインストールする場合は、すべてのノードでインストールまたはアップグレードしなければなりません。

プロンプトが表示されたら、**[Return]** キーを押して AutoPass をインストールまたはアップグレードします。AutoPass をインストールまたはアップグレードしない場合は、**n** と入力します。

Data Protector のバージョン A.05.x が検出されると、アップグレード手順が自動的に開始されます。クリーン インストールを実行する (前のバージョンのデータベースを削除する) 場合は、旧バージョンをアンインストールしてからインストールを再開してください。

インストールの詳細は、20 ページの「UNIX 用 Cell Manager のインストール」および 37 ページの「UNIX 用のインストール サーバのインストール」を参照してください。

4. セル内に Windows クライアントがある場合に、Data Protector A.05.00 または A.05.10 からアップグレードしようとする、IDB 内にあるファイル名の変換が実行されることが表示されます。IDB の変換は、国際文字セットを含むファイル名を正しく処理するために必要です。詳細は 262 ページの「IDB 内でのファイル名の変更」を参照してください。

アップグレード完了後、Data Protector が使用できるようになります。

omnisetup.sh コマンドの説明については、DVD-ROM の <Mount_point>/LOCAL_INSTALL ディレクトリにある README ファイルか、DVD-ROM の <Mount_point>/DOCS/C/MAN ディレクトリにある『HP OpenView Storage Data Protector Command Line Interface Reference』を参照してください。

この次に行う作業

Cell Manager システムとインストール サーバシステムのアップグレードが完了したら、構成ファイルの変更が必要かどうかを確認します。詳細は 247 ページの「構成の変更のチェック」を参照してください。

インストール サーバのアップグレード

omnisetup.sh コマンドの実行時に、HP-UX 用または Solaris 用のインストール サーバは、自動的にアップグレードされます。

HP-UX では、このコマンドは swinstall ユーティリティを使用して、既存のパッケージセットを直接アップグレードします。Solaris では、このコマンドは pkgrm ユーティリティを使用して既存のパッケージセットを削除し、pkgadd ユーティリティを使用して新しいパッケージをインストールします。

インストール サーバがクライアント コンポーネントとともにインストールされている場合、インストール サーバは omnisetup.sh コマンドで削除されます。この場合、omnisetup.sh -IS コマンドを使用して新しいインストール サーバ デポをインストールした後、アップグレード後のインストール サーバを再度インポートしてください。詳細な作業手順は、187 ページの「セルへのインストール サーバのインポート」を参照してください。

重要 まず Cell Manager をアップグレードしなければ、インストール サーバをアップグレードすることはできません。

アップグレード手順

HP-UX 用または Solaris 用のインストール サーバを Data Protector A.06.00 にアップグレードするには、以下の手順に従います。

1. UNIX インストール DVD-ROM をドライブに挿入し、マウント ポイントにマウントします。

例：

```
mkdir /dvdrom
mount /dev/c0d0t0 /dvdrom
```

オプションで、ディスク上のデポから Data Protector をインストールする場合は、以下の手順を実行します。

- インストール ファイルが格納されている DP_DEPOT ディレクトリおよび LOCAL_INSTALL ディレクトリをローカル ディスクにコピーする場合は、以下のコマンドを実行します。

```
mkdir <directory>
cp -r /dvdrom/<platform_dir>/DP_DEPOT <directory>
cp -r /dvdrom/<platform_dir>/AUTOPASS <directory>
cp -r /dvdrom/LOCAL_INSTALL <directory>
```

Data Protector A.06.00 へのアップグレード Data Protector A.05.x からのアップグレード

<platform_dir> は、Data Protector のアップグレードを実行するオペレーティング システムおよびプロセッサからなるプラットフォームに応じて、以下のようになります。

hpux_ia	IA-64 システム上の HP-UX 11.23
hpux_pa	PA-RISC システム上の HP-UX
solaris	Solaris システム

- DVD-ROM 全体をローカル ディスクにコピーする場合は、以下のコマンドを実行します。

```
cp -r /dvdrom <dvd_image_dir>
```

2. omnisetup.sh コマンドを実行します。

このコマンドを DVD-ROM から実行するには、以下のようにして実行します。

```
cd /dvdrom/LOCAL_INSTALL  
./omnisetup.sh
```

ディスクからインストール作業を起動する場合は、以下の手順で行います。

- DP_DEPOT ディレクトリおよび LOCAL_INSTALL ディレクトリをローカル ディスク上の <directory> にコピーした場合は、omnisetup.sh コマンドが格納されているこのディレクトリに移動して以下を実行します。

```
cd <directory>/LOCAL_INSTALL  
./omnisetup.sh
```

- DVD-ROM 全体を <dvd_image_dir> にコピーした場合は、omnisetup.sh コマンドをパラメータなしで実行します。

```
cd <dvd_image_dir>/LOCAL_INSTALL  
./omnisetup.sh
```

アップグレード完了後、Data Protector が使用できるようになります。

omnisetup.sh コマンドの説明については、DVD-ROM の <Mount_point>/LOCAL_INSTALL ディレクトリにある README ファイルか、DVD-ROM の <Mount_point>/DOCS/C/MAN ディレクトリにある『HP OpenView Storage Data Protector Command Line Interface Reference』を参照してください。

この次に行う作業

インストール サーバシステムのアップグレードが完了したら、構成ファイルの変更が必要かどうかを確認します。詳細は 247 ページの「構成の変更のチェック」を参照してください。

Windows Cell Manager とインストール サーバのアップグレード

従来バージョンの Data Protector が発見された場合は、オペレーティング システムにより同じコンポーネント セットがインストール対象と見なされます (廃止されたコンポーネントは除く)。新規 (クリーン) インストールでは、既存パッケージ セットが削除され、新しいパッケージ セットがインストールされます。

Windows 用インストール サーバが Cell Manager と同じシステムにインストールされている場合、アップグレード処理中にインストール サーバも自動的にアップグレードされます。古いインストール サーバ デポは削除され、インストール時にインストール サーバ コンポーネントが選択されている場合は、そこに新しいインストール サーバ デポがコピーされます。

インストール サーバが Data Protector クライアントとともにインストールされており、このクライアントが (Data Protector GUI を使用して) リモートでアップグレードされた場合は、インストール サーバも同時にアップグレードされます。

重要 インストール完了後、アップグレード済みのインストール サーバを再度インポートします。詳細な作業手順は、187 ページの「セルへのインストール サーバのインポート」を参照してください。

注記 Windows NT オペレーティング システムをより新しい Windows オペレーティング システムにアップグレードすることを計画している場合は、最初にオペレーティング システムをアップグレードしてから、従来バージョンの Data Protector を Data Protector A.06.00 にアップグレードしてください。詳細な作業手順は、274 ページの「Windows NT から Windows のより新しいバージョンへのアップグレード」を参照してください。

MS Cluster Server

MS Cluster Server 環境で実行されている Cell Manager のアップグレード手順は、MS Cluster Server 環境で使用するように構成されていない Cell Manager のアップグレード手順とは異なります。アップグレードに必要な手順の詳細は、289 ページの「Microsoft Cluster Server 上で構成されている Cell Manager のアップグレード」を参照してください。

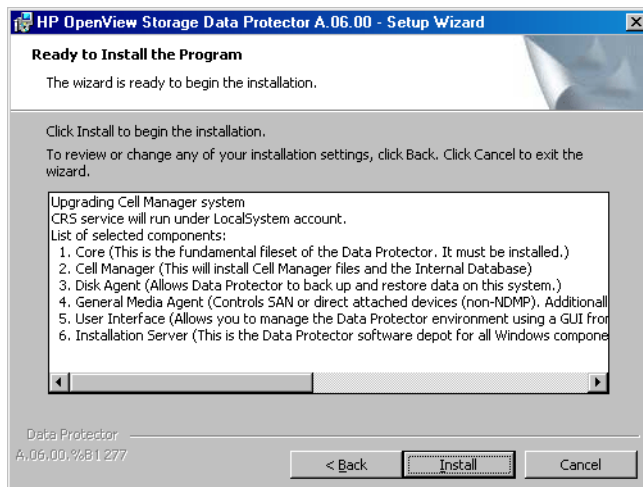
アップグレード手順

Windows 用の Cell Manager とインストール サーバを Data Protector A.06.00 にアップグレードするには、以下の手順に従います。

Data Protector A.06.00 へのアップグレード Data Protector A.05.x からのアップグレード

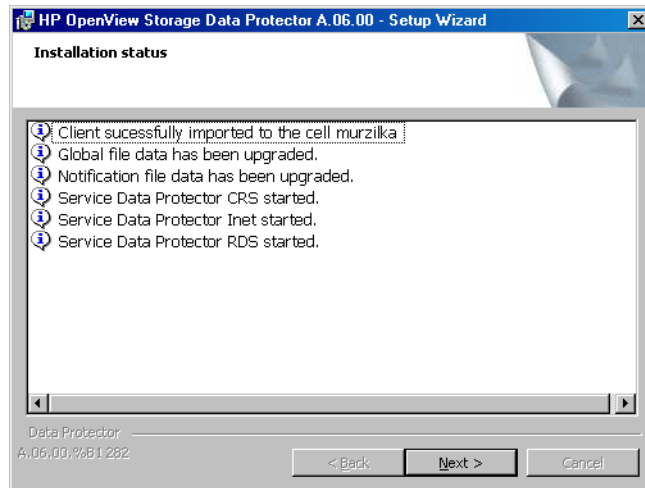
1. Windows 用インストール DVD-ROM をドライブに挿入し、Windows_other¥i386¥setup.exe コマンドを実行します。古い Data Protector がインストールされていることが、セットアップによって検出されます。[Next] をクリックしてアップグレードを開始してください。
2. [コンポーネント選択] ページでは、以前にシステムにインストールしたコンポーネントが選択されています。ここで、コンポーネントを追加選択または選択解除して、コンポーネントセットを変更することも可能です。選択されたコンポーネントの説明は、ウィザードの次の手順で確認できます。[Next] をクリックします。
3. **Windows XP SP2 の場合のみ:** Data Protector によってシステムにファイアウォールが検出されると、[Windows Firewall configuration] ページが表示されます。Data Protector のセットアッププログラムによって、必要なすべての Data Protector 実行可能ファイルが登録されます。デフォルトでは、[Initially, enable newly registered Data Protector binaries to open ports as needed] オプションが選択されています。この時点で、Data Protector によってポートがオープンされないようにするには、オプションを選択解除します。ただし、Data Protector を適切に機能させるには、実行可能ファイルを有効にする必要があります。
[Next] をクリックします。
4. 選択したコンポーネントのサマリー リストが表示されます。[Install] をクリックしてアップグレードを実行します。

図 4-1 コンポーネント選択サマリー ページ



5. [Installation status] ページが表示されます。[Next] をクリックします。

図 4-2 [Installation Status] ページ



6. セル内に UNIX クライアントがある場合は、[IDB Conversion] ページが表示されます。詳細は 262 ページの「IDB 内でのファイル名の変更」を参照してください。
7. この手順は、Cell Manager のアップグレードでのみ実行されます。インストールサーバがアップグレードする Cell Manager とは別のクライアントにインストールされている場合は、この手順は実行されません。

購入済みライセンスのパスワードを HP Password Delivery Center の Web サーバからインターネットを介して直接ダウンロードしてインストールする場合は、セットアップ用ウィザードに従って、HP OpenView AutoPass ユーティリティをインストールまたはアップグレードします。AutoPass ユーティリティに関する詳細は、309 ページの「HP OpenView AutoPass ユーティリティを使用した恒久パスワードの取得とインストール」を参照してください。

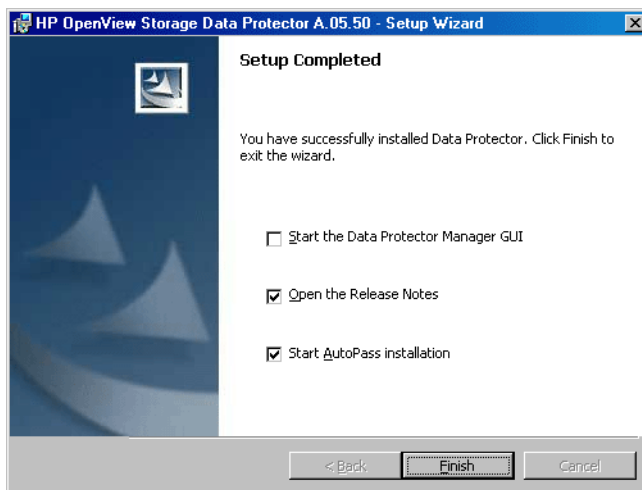
デフォルトでは、[Start AutoPass installation] オプション、または [Upgrade AutoPass installation] オプションが選択されています。HP OpenView AutoPass ユーティリティをインストールすることをお勧めします。AutoPass をインストールまたはアップグレードしない場合は、オプションを選択解除します。

セットアップ後すぐに Data Protector を起動するには、[Start the Data Protector Manager GUI] を選択します。

Data Protector A.06.00 へのアップグレード Data Protector A.05.x からのアップグレード

『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス』を表示するには、[Open the Product Announcements] を選択します。

図 4-3 AutoPass をインストール対象として選択する場合



8. [Finish] をクリックします。

アップグレード完了後、Data Protector が使用できるようになります。

この次に行う作業

Cell Manager システムとインストール サーバシステムがアップグレードされたら、以下を実行します。

- セル内にUNIXクライアントがある場合は、ファイル名に使用されている非ASCII文字をData Protectorで正しく処理できるようにするために、Data Protector IDBが変換されます。IDB変換の詳細は、262ページの「IDB内でのファイル名の変更」を参照してください。
- 構成ファイルの変更が必要かどうかを確認します。詳細は247ページの「構成の変更のチェック」を参照してください。

構成の変更のチェック

グローバル オプション ファイル

アップグレード中に、古いグローバル オプション ファイルの内容は、Cell Manager 上の新しいグローバル オプション ファイルの内容とマージされます。古いグローバル オプション ファイルは、UNIX 用 Cell Manager では /etc/opt/omni/server/options ディレクトリに、Windows 用 Cell Manager では <Data_Protector_home>%Config%server%Options ディレクトリにあります。

- /opt/omni/newconfig/etc/opt/omni/server/options (UNIX Cell Manager の場合)
- <Data_Protector_home>%NewConfig%Server%Options (Windows Cell Manager の場合)

マージ後のファイル名は global で、アップグレード後の製品で使用されます。このファイルは、UNIX Cell Manager では /etc/opt/omni/server/options ディレクトリに、Windows Cell Manager では <Data_Protector_home>%Config%server%Options ディレクトリにあります。古いグローバル オプション ファイルは、アップグレードを行った回数によって、global.1、global.2 などという名前に変更されます。

マージ ファイルの作成時には、以下が適用されます。

- 古いファイル内のアクティブな (コメントではない) グローバル オプション ファイル変数は、マージ後のファイルでもアクティブとなります。変数の値が古いファイルからコピーされたものであることを示す以下のコメントが、マージ後のファイルに追加されます。

```
<variable>=<value>
```

```
# Data Protector A.06.00
```

```
# This value was automatically copied from previous version.
```

- 使用されなくなったグローバル オプション ファイル変数は、マージ後のファイルではコメント化 (非アクティブ化) され、その変数がもう使用されないことを示す以下のコメントが付加されます。

```
# <variable>=<value>
```

```
# Data Protector A.06.00
```

```
# This value is no longer in use.
```

- サポートされなくなった変数と値は、マージ後のファイルではコメント化 (無効化) されます。テンプレート (<variable_template>) を含む以下のコメントが追加され、その変数の従来の値が示されます。

```
# <variable>=<variable_template>
```

```
# Data Protector A.06.00
```

Data Protector A.06.00 へのアップグレード Data Protector A.05.x からのアップグレード

```
# This variable cannot be transferred automatically.  
# The previous setting was:  
# <variable>=<value>
```

- 古いファイルのコメントは、マージ後の新しいファイルには移されません。

Windows システムの場合、グローバル オプション ファイルは UNICODE 形式なため、メモ帳などのエディタを使って編集できます。編集したファイルは必ず UNICODE 形式で保存してください。

新しいオプションの説明はマージ後のグローバル オプション ファイルに記述されています。
/etc/opt/omni/server/options/global (UNIX Cell Manager の場合) または
<Data_Protector_home>%config%server%options%global (Windows Cell Manager の場合)
グローバル オプションの使用方法は、『HP OpenView Storage Data Protector トラブルシューティングガイド』の「グローバル オプションファイル」を参照してください。

手作業で行う作業

以下に示す一覧は、アップグレードが正常に完了した後に手作業で行う作業をまとめたものです。

- Omnirc ファイル

Cell Manager システムとインストール サーバ システムをアップグレードした後で、必要に応じて omnirc ファイルを編集できます。編集方法の詳細は、『HP OpenView Storage Data Protector トラブルシューティングガイド』の「omnirc オプションの使用」を参照してください。

- コマンド行

変更または機能強化されたコマンドの一覧は、B-80 ページの「Data Protector A.06.00 にアップグレードした後のコマンド行ツールの変更」を参照してください。古いコマンドを使用しているスクリプトがないかチェックし、必要に応じて修正する必要があります。スクリプトの構文は、対応するマンページを参照してください。

この次に行う作業

Cell Manager およびインストール サーバをインストールし、必要な変更をすべて実施したら、ソフトウェアをクライアントに配布します。詳細は 249 ページの「クライアントのアップグレード」を参照してください。

クライアントのアップグレード

アップグレードの手順

クライアントのアップグレード手順は 233 ページの「アップグレードの概要」を参照してください。

クライアントのリモート アップグレード

インストール サーバを使ったクライアントのアップグレード手順は、50 ページの「Data Protector クライアントのリモート インストール」を参照してください。UNIX システムでは、新規コンポーネントを追加する前に、既存のコンポーネントをアップグレードする必要があります。新規コンポーネントの追加後には、以前のバージョンからのコンポーネントは Data Protector には表示されません。この場合は、これらのコンポーネントを再インストールする必要があります。

クライアントのローカル アップグレード

ネットワーク上にインストール サーバがない場合、または何らかの理由により Data Protector ソフトウェアをクライアントシステムに配布できない場合は、Data Protector クライアントをローカルにアップグレードできます。

Windows クライアントをローカルにアップグレードする場合は、63 ページの「Windows 用クライアントのインストール」を参照してください。UNIX クライアントをローカルにアップグレードする場合は、119 ページの「UNIX クライアントのローカル インストール」を参照してください。

Novell NetWare

アップグレードしたシステムに Novell NetWare クライアントが含まれている場合は、NDS/eDirectory データベースのバックアップと復元を可能にするための追加手順が必要になります。詳細は 102 ページの「Novell NetWare クライアントのローカル インストール」を参照してください。

Linux クライアント

Linux クライアントのアップグレード時には、Data Protector のバイナリと構成ファイルが /usr/omni から /opt/omni (バイナリ) と /etc/opt/omni (構成ファイル) に移されます。実行前スクリプトや実行後スクリプトは、/opt/omni には移されず、/tmp/usr_omni に保存されています。これらのファイルは /opt/omni/sbin に手動でコピーする必要があります。

Data Protector A.06.00 へのアップグレード Data Protector A.05.x からのアップグレード

inetd サービスの代わりに xinetd サービスが使用されている場合は、/etc/xinetd.d/omni ファイルが置き換えられず、設定は変更されません。xinetd サービスが実行されているかどうかを確認するには、以下のコマンドを実行します。

```
ps -e | grep xinetd
```

設定をデフォルトの Data Protector 設定で置き換える場合か、不具合のあるファイルを置き換える場合は、ファイルを削除し、Data Protector GUI からすべての Data Protector ソフトウェア コンポーネントをプッシュします。デフォルト状態の /etc/xinetd.d/omni ファイルがインストールされます。

重要 /etc/xinetd.d/omni ファイルを置き換えると、変更内容が失われます。変更を残しておく場合は、以前のファイルのバックアップ コピーを作成し、設定を手作業で新規ファイルに追加します。

MC/ServiceGuard 上で構成されているクライアントのアップグレード

アップグレードされる Data Protector 用統合ソフトウェア コンポーネントが Cell Manager と同じノードにインストールされる場合、MC/ServiceGuard を使用しているクライアントのアップグレードを行うには、最初に物理ノードをアップグレードしてから、以下の手順を行います。

1. 以下のコマンドを実行して仮想ホストをエクスポートします。

```
omnicc -export_host <virtual_hostname>
```

2. 仮想ホストを再度インポートします。

```
omnicc -import_host <virtual_hostname> -virtual
```

統合ソフトウェアがインストールされたクライアントのアップグレード

統合ソフトウェア (Oracle、SAP R/3、Informix Server、Sybase、Microsoft Exchange Server、HP StorageWorks Disk Array XP、EMC Symmetrix など) がインストールされた Data Protector クライアントのアップグレードを正常に行うには、以降の項に記述された手順に従ってください。

- Oracle 用統合ソフトウェアのアップグレード方法の詳細は、251 ページの「Oracle 用統合ソフトウェアのアップグレード」を参照してください。
- SAP R/3 用統合ソフトウェアのアップグレード方法の詳細は、253 ページの「SAP R/3 用統合ソフトウェアのアップグレード」を参照してください。

- Informix Server 用統合ソフトウェアのアップグレード方法の詳細は、253 ページの「UNIX システム上の Informix Server 用統合ソフトウェアのアップグレード」および 254 ページの「Windows システム上の Informix Server 用統合ソフトウェアのアップグレード」を参照してください。
- Sybase 用統合ソフトウェアのアップグレード方法の詳細は、255 ページの「UNIX システム上の Sybase 用統合ソフトウェアのアップグレード」および 257 ページの「Windows システム上の Sybase 用統合ソフトウェアのアップグレード」を参照してください。
- MS Exchange、MS SQL、HP StorageWorks Disk Array XP、EMC Symmetrix などの統合ソフトウェアのアップグレード方法の詳細は、260 ページの「他の統合ソフトウェアのアップグレード」を参照してください。

Oracle 用統合ソフトウェアのアップグレード

Oracle 用統合ソフトウェアがインストールされているクライアントのアップグレードは、`omnisetup.sh -install oracle8` コマンド (UNIX システムの場合) または `setup.exe` コマンド (Windows システムの場合) を使用してローカルに行うか、あるいは、Data Protector GUI を使用してリモートから Oracle 用統合ソフトウェア エージェントをクライアントにプッシュする方法で行います。UNIX 上で Cell Manager 以外のシステムのクライアントをアップグレードする場合は、`-install oracle8` を指定する必要はありません。この場合、プロンプトは表示されず、アップグレード前にシステムにインストールされていたのと同じコンポーネントが自動的に選択されます。

アップグレード後の新しいテンプレート Data Protector A.05.00 または A.05.10 からアップグレードする場合は、Oracle テンプレートが新しいバージョンに置き換えられます。新しいテンプレートは以下のディレクトリ内にあります。

`/opt/omni/newconfig/etc/opt/omni/server/dltemplates/lists/oracle8` (UNIX システム)、または、`<Data_Protector_home>%NewConfig%server%dltemplates%lists%oracle8` (Windows システム)

新しいテンプレートを使用するには、Data Protector A.06.00 へのアップグレード後に、`/etc/opt/omni/server/dltemplates/lists%oracle8` ディレクトリ (UNIX システムの場合) または `<Data_Protector_home>%Config%server%dltemplates%lists%oracle8` ディレクトリ (Windows システムの場合) にコピーします。古いテンプレートを残しておく場合は、別の名前で保存してください。

ZDB メソッドの構成 Oracle インスタンス構成ファイルに `<ORACLE_DBID>` パラメータが含まれているかどうかに応じて、Data Protector A.06.00 用の ZDB 方法構成ファイルが以下のように設定されます。

Data Protector A.06.00 へのアップグレード Data Protector A.05.x からのアップグレード

- Oracle インスタンス構成ファイルに <ORACLE_DBID> パラメータが含まれている場合 (Data Protector A.05.10 および A.05.50 の場合) は、アップグレード中に ZDB 方法構成ファイルがデータベース インスタンスごとに作成されます。
- Oracle インスタンス構成ファイルに <ORACLE_DBID> パラメータが含まれていない場合 (Data Protector A.05.00 の場合) は、最初のバックアップセッション中に ZDB 方法構成ファイルがインスタンスごとに作成されます。

Oracle ZDB メソッドはアップグレード中には変更されません。プロキシコピー ZDB メソッドとバックアップセット ZDB メソッドを切り替える方法については、『HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide』を参照してください。

Oracle ZDB のアップグレード Data Protector A.05.00 または A.05.10 からアップグレードする場合は、Oracle ZDB のバックアップ仕様が、Oracle 統合用ソフトウェアの標準アップグレード手順の最後で自動的にアップグレードされます。

バックアップ仕様のアップグレード中に、以下の手順が実行されます。

- OB2DMAP パラメータと OB2SMB パラメータが、最初の RMAN ALLOCATE CHANNEL コマンドに追加されます。OB2DMAP パラメータには、アップグレード前に割り当てられていたチャンネル数が設定されます。たとえば、RMAN スクリプトに 4 つのチャンネルが割り当てられていた場合、OB2DMAP パラメータは 4 に設定されます。
- すべての ALLOCATE CHANNEL コマンドは、最初のを除き、スクリプトから削除されます。
- インスタント リカバリが有効に設定されている場合、バックアップ オブジェクトの TABLESPACE か DATAFILES は、データベース全体のバックアップのみが認められるように、DATABASE に変更されます。
- プロキシコピーによるバックアップ メソッドを使用していた場合は、すべての RELEASE CHANNEL コマンドは、最初の ALOCATE CHANNEL コマンドを参照しているものを除き、削除されます。

詳細は、『HP OpenView Storage Data Protector インテグレーションガイド - Oracle、SAP』か『HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide』を参照してください。

インスタント リカバリのための Oracle インスタンスの構成 制御ファイル、リカバリ カタログ、またはアーカイブ REDO ログ ファイルが、データベース ファイルと同じソース ボリューム グループ (LVM 使用時) またはソース ボリュームに置かれている場合は、Oracle インスタンスを再構成するか、または ZDB_ORA_INCLUDE_CF_OLF、ZDB_ORA_INCLUDE_SPF、ZDB_ORA_NO_CHECKCONF_IR の各 omnirc 変数を設定する必要があります。詳細は『HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide』を参照してください。

SAP R/3 用統合ソフトウェアのアップグレード

SAP R/3 用統合ソフトウェアがインストールされているクライアントのアップグレードは、`omnisetup.sh -install sap` コマンド (UNIX システムの場合) または `setup.exe` コマンド (Windows システムの場合) を使用してローカルに行くか、あるいは、Data Protector GUI を使用してリモートから SAP R/3 用統合ソフトウェア エージェントをクライアントにプッシュする方法で行います。UNIX 上で Cell Manager 以外のシステムのクライアントをアップグレードする場合は、`-install sap` オプションを指定する必要はありません。この場合、プロンプトは表示されず、アップグレード前にシステムにインストールされていたのと同じコンポーネントが自動的に選択されます。

インスタント リカバリのための Oracle インスタンスの構成 制御ファイル、リカバリ カタログ、またはアーカイブ REDO ログ ファイルが、データベース ファイルと同じソース ボリューム グループ (LVM 使用時) またはソース ボリュームに置かれている場合は、Oracle インスタンスを再構成するか、または `ZDB_ORA_INCLUDE_CF_OLF`、`ZDB_ORA_INCLUDE_SPF`、`ZDB_ORA_NO_CHECKCONF_IR` の各 `omnirc` 変数を設定する必要があります。詳細は『HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide』を参照してください。

UNIX システム上の Informix Server 用統合ソフトウェアのアップグレード

Informix Server 用統合ソフトウェアを Data Protector A.05.00 または A.05.10 から Data Protector A.06.00 にアップグレードする際には、環境に応じ、以下の 3 つのアップグレード手順があります。

手順 1

Informix Server クライアントが Cell Manager と同じシステムになく、かつ、Data Protector クラスタ対応クライアントとして構成されていない場合、Data Protector Informix Server 構成パラメータは、アップグレード中に、Data Protector Informix Server クライアントから Cell Manager に自動的に移されます。アップグレード後の Informix Server データベースの再構成は不要です。

`omnisetup.sh` コマンドを実行してクライアントをローカルにアップグレードするか、Data Protector GUI を使用してリモートから Informix Server 用統合ソフトウェア エージェントをクライアントにプッシュし、クライアントをアップグレードします。

手順 2

Informix Server クライアントが Cell Manager と同じシステムになく、かつ、Data Protector クラスタ対応クライアントとして構成されている場合、Data Protector Informix Server 構成パラメータは、アップグレード中に、Data Protector Informix Server クライアントから Cell Manager に自動的に移されます。アップグレード後には、Informix Server データベースを再構成する必要があります。

Data Protector A.06.00 へのアップグレード Data Protector A.05.x からのアップグレード

1. omnisetup.sh コマンドを実行してクライアントをローカルにアップグレードするか、Data Protector GUI を使用してリモートから Informix Server 用統合ソフトウェア エージェントをクライアントにプッシュし、クライアントをアップグレードします。
2. 『HP OpenView Storage Data Protector インテグレーション ガイド』で説明されているとおり、Data Protector GUI か CLI を使用して、Informix Server データベースを構成します。
Informix Server の仮想ホスト名を使用して、Informix Server データベースを構成します。

手順 3

Informix Server クライアントがクラスタ対応 *Cell Manager* と同じシステムにあり、かつ、Data Protector クラスタ対応クライアントとして構成されているかいないかのいずれかの場合、Data Protector Informix Server 構成パラメータは、アップグレード中に、Data Protector Informix Server クライアントから *Cell Manager* に自動的に移されません。アップグレード後には、Informix Server データベースを再構成する必要があります。

1. omnisetup.sh コマンドを実行してクライアントをローカルにアップグレードするか、Data Protector GUI を使用してリモートから Informix Server 用統合ソフトウェア エージェントをクライアントにプッシュし、クライアントをアップグレードします。
2. 『HP OpenView Storage Data Protector インテグレーション ガイド』で説明されているとおり、Data Protector GUI か CLI を使用して、Informix Server データベースを構成します。

Windows システム上の Informix Server 用統合ソフトウェアのアップグレード

Informix Server 用統合ソフトウェアを Data Protector A.05.00 または A.05.10 から Data Protector A.06.00 にアップグレードする際には、環境に応じ、以下の 3 つのアップグレード手順があります。

手順 1

Informix Server クライアントが *Cell Manager* と同じシステムになく、かつ、Data Protector クラスタ対応クライアントとして構成されていない場合、Data Protector Informix Server 構成パラメータは、アップグレード中に、Data Protector Informix Server クライアントから *Cell Manager* に自動的に移されます。アップグレード後の Informix Server データベースの再構成は不要です。

setup.exe コマンドを実行してクライアントをローカルにアップグレードするか、Data Protector GUI を使用してリモートから Informix Server 用統合ソフトウェア エージェントをクライアントにプッシュし、クライアントをアップグレードします。

手順 2

Informix Server クライアントが Cell Manager と同じシステムになく、かつ、Data Protector クラスタ対応クライアントとして構成されている場合、Data Protector Informix Server 構成パラメータは、アップグレード中に、Data Protector Informix Server クライアントから Cell Manager に自動的に移されます。アップグレード後には、Informix Server データベースを再構成する必要があります。

1. setup.exe コマンドを実行してクライアントをローカルにアップグレードするか、Data Protector GUI を使用してリモートから Informix Server 用統合ソフトウェア エージェントをクライアントにプッシュし、クライアントをアップグレードします。
2. 『HP OpenView Storage Data Protector インテグレーション ガイド』で説明されているとおり、Data Protector GUI か CLI を使用して、Informix Server データベースを構成します。

Informix Server の仮想ホスト名を使用して、Informix Server データベースを構成します。

手順 3

Informix Server クライアントがクラスタ対応 *Cell Manager* と同じシステムにあり、かつ、Data Protector クラスタ対応クライアントとして構成されているかいないかのいずれかの場合、Data Protector Informix Server 構成パラメータは、アップグレード中に、Data Protector Informix Server クライアントから Cell Manager に自動的に移されません。アップグレード後には、Informix Server データベースを再構成する必要があります。

1. setup.exe コマンドを実行してクライアントをローカルにアップグレードするか、Data Protector GUI を使用してリモートから Informix Server 用統合ソフトウェア エージェントをクライアントにプッシュし、クライアントをアップグレードします。
2. 『HP OpenView Storage Data Protector インテグレーション ガイド』で説明されているとおり、Data Protector GUI か CLI を使用して、Informix Server データベースを構成します。

UNIX システム上の Sybase 用統合ソフトウェアのアップグレード

Sybase 用統合ソフトウェアを Data Protector A.05.00 または A.05.10 から Data Protector A.06.00 にアップグレードする際には、環境に応じ、以下の 3 つのアップグレード手順があります。

手順 1

Sybase クライアントが Cell Manager と同じシステムになく、かつ、Data Protector クラスタ対応クライアントとして構成されていない場合、Data Protector Sybase 構成パラメータは、アップグレード中に、Data Protector Sybase クライアントから Cell Manager に自動的に移されます。アップグレード後の Sybase Server の再構成は不要です。

Data Protector A.06.00 へのアップグレード Data Protector A.05.x からのアップグレード

omnisetup.sh コマンドを実行してクライアントをローカルにアップグレードするか、Data Protector GUI を使用してリモートから Sybase 用統合ソフトウェア エージェントをクライアントにプッシュし、クライアントをアップグレードします。

手順 2

Sybase クライアントが Cell Manager と同じシステムになく、かつ、Data Protector クラスタ対応クライアントとして構成されている場合、Data Protector Sybase 構成パラメータは、アップグレード中に、Data Protector Sybase クライアントから Cell Manager に自動的に移されます。アップグレード後には、Sybase Server を再構成する必要があります。

1. omnisetup.sh コマンドを実行してクライアントをローカルにアップグレードするか、Data Protector GUI を使用してリモートから Sybase 用統合ソフトウェア エージェントをクライアントにプッシュし、クライアントをアップグレードします。
2. 『HP OpenView Storage Data Protector インテグレーション ガイド』で説明されているとおりに、Data Protector GUI か CLI を使用して、Sybase クライアントを構成します。

Sybase Server の仮想ホスト名を使用して、Sybase Server を構成します。

手順 3

Sybase クライアントがクラスタ対応 Cell Manager と同じシステムにあり、かつ、Data Protector クラスタ対応クライアントとして構成されているかいないかのいずれかの場合、Data Protector Sybase 構成パラメータは、アップグレード中に、Data Protector Sybase クライアントから Cell Manager に自動的に移されません。アップグレード後には、Sybase Server を再構成する必要があります。

1. omnisetup.sh コマンドを実行してクライアントをローカルにアップグレードするか、Data Protector GUI を使用してリモートから Sybase 用統合ソフトウェア エージェントをクライアントにプッシュし、クライアントをアップグレードします。
2. 『HP OpenView Storage Data Protector インテグレーション ガイド』で説明されているとおりに、Data Protector GUI か CLI を使用して、Sybase Server を構成します。

Sybase Server が Data Protector クラスタ対応クライアントとして構成されている場合、Sybase Server の仮想ホスト名を使用して構成します。

Sybase Server が Data Protector クラスタ対応クライアントとして構成されていない場合、Sybase Server のホスト名を使用して構成します。

Windows システム上の Sybase 用統合ソフトウェアのアップグレード

Sybase 用統合ソフトウェアを Data Protector A.05.00 または A.05.10 から Data Protector A.06.00 にアップグレードする際には、環境に応じ、以下の 3 つのアップグレード手順があります。

手順 1

Sybase クライアントが Cell Manager と同じシステムになく、かつ、Data Protector クラスタ対応クライアントとして構成されていない場合、Data Protector Sybase 構成パラメータは、アップグレード中に、Data Protector Sybase クライアントから Cell Manager に自動的に移されます。アップグレード後の Sybase Server の再構成は不要です。

setup.exe コマンドを実行してクライアントをローカルにアップグレードするか、Data Protector GUI を使用してリモートから Sybase 用統合ソフトウェア エージェントをクライアントにプッシュし、クライアントをアップグレードします。

手順 2

Sybase クライアントが Cell Manager と同じシステムになく、かつ、Data Protector クラスタ対応クライアントとして構成されている場合、Data Protector Sybase 構成パラメータは、アップグレード中に、Data Protector Sybase クライアントから Cell Manager に自動的に移されます。アップグレード後には、Sybase Server を再構成する必要があります。

1. setup.exe コマンドを実行してクライアントをローカルにアップグレードするか、Data Protector GUI を使用してリモートから Sybase 用統合ソフトウェア エージェントをクライアントにプッシュし、クライアントをアップグレードします。
2. 『HP OpenView Storage Data Protector インテグレーションガイド』で説明されているとおりに、Data Protector GUI か CLI を使用して、Sybase クライアントを構成します。

Sybase SQL Server の仮想ホスト名を使用して、Sybase Server を構成します。

手順 3

Sybase クライアントがクラスタ対応 Cell Manager と同じシステムにあり、かつ、Data Protector クラスタ対応クライアントとして構成されているかいないかのいずれかの場合、Data Protector Sybase 構成パラメータは、アップグレード中に、Data Protector Sybase クライアントから Cell Manager に自動的に移されません。アップグレード後には、Sybase Server を再構成する必要があります。

1. setup.exe コマンドを実行してクライアントをローカルにアップグレードするか、Data Protector GUI を使用してリモートから Sybase 用統合ソフトウェア エージェントをクライアントにプッシュし、クライアントをアップグレードします。

Data Protector A.06.00 へのアップグレード Data Protector A.05.x からのアップグレード

- 『HP OpenView Storage Data Protector インテグレーションガイド』で説明されているとおりに、Data Protector GUI か CLI を使用して、Sybase クライアントを構成します。

Sybase Server が Data Protector クラスタ対応クライアントとして構成されている場合、Sybase Server の仮想ホスト名を使用して構成します。

Sybase Server が Data Protector クラスタ対応クライアントとして構成されていない場合、Sybase Server のホスト名を使用して構成します。

HP StorageWorks EVA 用統合ソフトウェアのアップグレード

HP StorageWorks EVA 用統合ソフトウェアのアップグレードには、HP StorageWorks EVA Agent (レガシー) から HP StorageWorks EVA SMI-S Agent へのアップグレードが必要です。このアップグレードが必要となるのは、EVA Agent (レガシー) が廃止予定であるためです。

アップグレードが正常に終了すると、以下の結果が得られます。

- EVA Agent (レガシー) で作成されたバックアップ仕様がアップグレードされます。
- バックアップセッション情報が EVADB から SMISDB に移されて、SMI-S Agent による復元が可能になります。
- EVA Agent (レガシー) に対して定義されていたログインおよびディスク グループのルールが SMISDB に移されます。

必要となる製品のどのバージョンやリリースがサポートされており、SMI-S Agent がどのプラットフォームでサポートされているかについては、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。

前提条件

- SMI-S Agent を実行するオペレーティングシステムの最小要件を満たしていることを確認します。
- 実行中の EVA バックアップがないことを確認します。アップグレード手順を開始すると、実行中のバックアップが失敗することがあります。失敗した場合は SMIDB 内にセッション情報が生成されず、そのセッションからの復元は不可能です。
- エージェントのアップグレードは、必ず Cell Manager のアップグレード終了後に開始します。

アップグレード手順

HP StorageWorks EVA Agent (レガシー) から HP StorageWorks EVA SMI-S Agent にアップグレードするには、以下の手順に従ってください。

1. Cell Manager 上で、`upgrade_cm_from_evaa` コマンドを実行して、すべての EVADB エントリを SMISDB エントリにアップグレードします。このコマンドは、必ず Cell Manager のアップグレード終了後に実行してください。

以下の情報が移されます。

- EVA Agent (レガシー) で作成されたバックアップ仕様とバックアップセッション (複製)
- EVA Management Appliance に関連するログイン エントリ

以下の点に注意してください。

ログイン

- ログイン エントリが SMISDB 内にすでに存在している場合は、その Management Appliance に関する新しいエントリは作成されません。
- ログイン ユーザーやパスワードは、CV EVA と SMI-S プロバイダで同一と想定されます。
- SMISDB ログイン エントリは常にポート 5988 を使用します。

ディスク グループ ルール

- 特定のディスク グループに対するルールが SMISDB 内にすでに存在している場合は、更新は行われません。
- EVA Agent (レガシー) に対して定義されていたすべてのディスク グループ ルールは、既存の SMISDB ディスク グループ ルールの最後に追加されます。

`upgrade_cm_from_evaa` コマンドの詳細は、『HP OpenView Storage Data Protector Command Line Interface Reference』を参照してください。

2. ローカル アップグレードを実行する場合は、アプリケーション システム上で、`omnisetup.sh -install smisa` コマンド (UNIX システムの場合) か `setup.exe` コマンド (Windows の場合) を実行します。リモート アップグレードを行う場合は、[コンポーネントの追加] GUI ウィザードを使用し、[HP StorageWorks EVA SMI-S Agent] を選択して、SMI-S Agent をクライアントにプッシュします。

実行前スクリプトによって、EVAA パッケージがシステム上に存在するかどうかチェックされます。パッケージが検出された場合は、そのパッケージに関する情報が Cell Manager から削除されます。

Data Protector A.06.00 へのアップグレード Data Protector A.05.x からのアップグレード

EVAA パッケージのアンインストールにともなって、EVA Agent (レガシー) で作成された EVA バックアップ セッション (複製) の情報が、EVADB から SMISDB に移されます。これにより、アップグレード後に、EVA Agent (レガシー) を使用して作成されたバックアップ セッションを SMI-S Agent を使用して復元できるようになります。

3. アプリケーション システムのアップグレードが終了したら、バックアップ システムもアップグレードする必要があります。スケジュールされたバックアップ仕様は、アプリケーション システムとバックアップ システムの両方が正常にアップグレードされるまで動作しません。
4. omnirc ファイルを手作業で確認し、omnirc 変数が適切にアップグレードされたことを確認します。

他の統合ソフトウェアのアップグレード

Data Protector クライアントに MS Exchange、MS SQL、HP StorageWorks Disk Array XP、EMC Symmetrix などの統合ソフトウェアがインストールされている場合は、それらのクライアントをアップグレードする必要があります。このためには、システム上で `omnisetup.sh -install <component_list>` コマンド (UNIX システムの場合) または `setup.exe` コマンド (Windows システムの場合) を実行してローカルにアップグレードするか、あるいは、Data Protector GUI を使用してリモートでアップグレードします。Data Protector コンポーネント コードの一覧は、119 ページの「UNIX クライアントのローカル インストール」を参照してください。Cell Manager 以外のシステム上のクライアントをアップグレードする場合は、`-install <component_list>` オプションの指定は不要です。この場合、プロンプトは表示されず、アップグレード前にシステムにインストールされていたのと同じコンポーネントが自動的に選択されます。

MoM 環境でのアップグレード

MoM 環境は逐次的にアップグレードできますが、以下の制限に注意してください。

- いったん MoM Manager/CMMDB Server をアップグレードすると、Data Protector A.06.00 MoM GUI から Data Protector A.05.x ファイルシステムまたは統合ソフトウェアを復元することはできなくなります。したがって、古い MoM GUI を使用して復元するか、またはクライアントをアップグレードする必要があります。

Data Protector A.05.x クライアントのファイルシステムおよび統合ソフトウェアのバックアップは、Data Protector A.06.00 MoM GUI から実行できます。

MoM 環境を Data Protector A.06.00 にアップグレードするには、以下の手順に従ってください。

1. MoM Manager/CMMDB Server を Data Protector A.06.00 へアップグレードします。

アップグレードは、MoM 環境内の Cell Manager を停止した状態で行う必要があります。
アップグレード後も、MoM Manager は古い Cell Manager に対して正しく機能します。

2. MoM 環境内の各クライアント Cell Manager をアップグレードします。

アップグレード手順は、237 ページの「UNIX 用 Cell Manager とインストール サーバのアップグレード」および 243 ページの「Windows Cell Manager とインストール サーバのアップグレード」を参照してください。

3. 構成したデバイスでクライアントをアップグレードします。

4. アプリケーション統合ソフトウェアでクライアントをアップグレードします。

ここまでのアップグレード手順が完了すると、Data Protector A.06.00 MoM GUI でファイルシステムと統合ソフトウェアをバックアップおよび復元することが可能になります。

IDB 内でのファイル名の変更

Data Protector A.05.50 および A.06.00 では、異なるプラットフォームの異なる地域設定 (ロケール) で作成されたファイル名の処理と表示の機能が改善されています。このため、Data Protector A.05.00 または A.05.10 からアップグレードする場合、一部のセル構成では IDB 内の既存ファイル名の変換が必要になります。A.05.50 からアップグレードする場合は、変換は不要です。

IDB 内のファイル名の変換は、必ず実行しなければなりません。変換しないと、非 ASCII 文字が含まれるファイル名の参照や復元時の選択にさまざまな要因が影響し、望ましくない結果が生じる可能性が高くなります。

変換は以下のように実行されます。

- UNIX Cell Manager: Windows クライアントのアップグレード後のバックアップの一部として実行。
- Windows Cell Manager: Cell Manager のアップグレード後のバックグラウンド プロセスとして実行。

IDB の変換が必要な場合は、プロンプトが表示されます。

Data Protector A.05.00 または A.05.10 からアップグレードする場合にファイル名変換によって Cell Manager がどのような影響を受けるかについて、262 ページの表 4-1 (Windows Cell Manager の場合) と 264 ページの表 4-2 に示します。

表 4-1 Windows Cell Manager に対するファイル名変換の影響

	UNIX およびその他のクライアント	Windows クライアント
IDB 変換の必要性	はい ¹	いいえ

表 4-1 Windows Cell Manager に対するファイル名変換の影響 (続き)

	UNIX およびその他のクライアント	Windows クライアント
クライアントをアップグレードせず、変換前にバックアップを行った場合	問題あり。 ² 非 ASCII 文字がバックアップ仕様 (ツリーや除外リストなど) に含まれているクライアントは、Data Protector A.06.00 にアップグレードする必要があります。このようなクライアントは、アップグレード作業を優先しやすくするために、アップグレード中に Data Protector イベント ログに記録されます。	問題なし。
クライアントを A.06.00 にアップグレードし、変換前にバックアップを行った場合	問題なし。 変換を実行し、特定のクライアントの IDB データを変換しているときに、そのクライアントをバックアップすると、そのバックアップセッションが No log モードに切り替わります。	問題なし。
変換前に復元対象ファイルを表示し、復元対象として非 ASCII ファイル名 / ツリーを選択した場合	問題あり。 ³ IDB 内に保存されているクライアント用のファイル名を変換しないと、非 ASCII 文字を Data Protector GUI に (復元対象として) 正しく表示できません。	問題なし。
変換後にバックアップを行った場合	問題なし。 クライアントを Data Protector A.06.00 にアップグレードする必要があります。	問題なし。

表 4-1 Windows Cell Manager に対するファイル名変換の影響 (続き)

	UNIX およびその他のクライアント	Windows クライアント
変換後にファイルを表示および復元した場合	問題なし。 クライアントを Data Protector A.06.00 にアップグレードする必要があります。	問題なし。
Disk Agent の互換性 (旧バージョン) ⁴	Data Protector A.05.00 = 互換性なし A.05.10 = 互換性なし A.05.50 = 互換性あり ⁴	Data Protector A.05.00 = 互換性あり ⁴ 、 A.05.10 = 互換性あり ⁴ 、 A.05.50 = 互換性あり ⁴

表 4-2 UNIX Cell Manager に対するファイル名変換の影響

	UNIX およびその他のクライアント	Windows クライアント
IDB 変換の必要性	いいえ	はい ¹

表 4-2 UNIX Cell Manager に対するファイル名
変換の影響 (続き)

	UNIX およびその他のクライアント	Windows クライアント
クライアントをアップグレードせず、変換期間前にバックアップを行った場合	問題なし。	問題あり。 ² 非 ASCII 文字がバックアップ仕様 (ツリーや除外リストなど) に含まれているクライアントは、Data Protector A.06.00 にアップグレードする必要があります。このようなクライアントは、アップグレード作業を優先しやすくするために、Data Protector イベント ログに記録されます。
クライアントを A.06.00 にアップグレードし、変換期間前にバックアップを行った場合	問題なし。	問題なし。 ただし、変換中期間に Windows クライアントをバックアップする必要があります。各クライアントの IDB データは、クライアントのバックアップ中に自動変換されません。 IDB に登録されているクライアント用のすべてのファイル名を変換するには、フルバックアップを実行する必要があります。
変換前に復元対象ファイルを表示し、復元対象として非 ASCII ファイル名 / ツリーを選択した場合	問題なし。	問題あり。 ³ Cell Manager のアップグレード後にフルバックアップを実行しないと、非 ASCII 文字を Data Protector GUI に (復元対象として) 正しく表示できません。

表 4-2 UNIX Cell Manager に対するファイル名
変換の影響 (続き)

	UNIX およびその他のクライアント	Windows クライアント
変換期間後にバックアップを行った場合	問題なし。	問題なし。 クライアントを Data Protector A.06.00 にアップグレードする必要があります。
変換後にファイルを表示および復元した場合	問題なし。	問題なし。 クライアントを Data Protector A.06.00 にアップグレードする必要があります。
Disk Agent の互換性 (旧バージョン) ⁴	Data Protector A.05.00 = 互換性あり ⁴ 、 A.05.10 = 互換性あり ⁴ 、 A.05.50 = 互換性あり ⁴	Data Protector A.05.00 = 互換性なし A.05.10 = 互換性なし ⁴ A.05.50 = 互換性あり

1. ファイル名変換を実行しないと、バックアップされる非 ASCII 文字を含むファイル名が IDB の Catalog Database (CDB) 部分に追加されるため、この部分に含まれるファイル名の数が増えます。変換が必要にもかかわらず未変換のファイルおよびディレクトリを復元対象として選択することはできません。これらを復元するには、ASCII 文字だけで構成される親ツリーを一時的な保存場所に復元する以外に方法はありません。

2. バックアップ仕様内のファイル名 (ツリー) が ASCII 文字だけで構成されている場合は、制限は適用されません。この場合は、ファイル名 (ツリー) 自体に非 ASCII 文字が含まれていても、ツリー内のすべてのファイルとディレクトリがバックアップされ、それらの名前が IDB に正しく登録されます。
3. 復元対象のファイル名 (ツリー) が ASCII 文字だけで構成されている場合は、制限は適用されません。それ以外の場合にこれらを復元するには、ASCII 文字だけで構成される親ツリーを一時的な保存場所に復元する以外に方法はありません。復元先がオリジナルのプラットフォームである限り、その親ツリーに含まれているファイルとディレクトリは (Data Protector GUI 内に正しく表示されていない場合)、すべてオリジナルのファイル名で復元されます。
4. ファイルシステム Disk Agent は Data Protector A.06.00 Cell Manager と互換性があります。以前のバージョンの Disk Agent のサポートは、2 週間までに制限されています。この期間中に、セル内のすべてのクライアントをアップグレードしてください。

留意事項

- ファイルのバックアップと復元が行われる際には、ファイル名処理の問題にかかわらず、ファイル ボディのバイト シーケンスはもとのまま残ります。
- 7 ビット ASCII 文字のみで構成されるファイル名については、関係するすべてのコンポーネント (Cell Manager、クライアント、GUI) に関して、あらゆるプラットフォームの組み合わせが完全にサポートされています。ファイル名に非 ASCII 文字が含まれる場合は、ファイル名を適切に処理するために特定のセットアップと構成が必要です。

IDB 変換は、IDB のファイル名部分のサイズとセルの構成によって、完了するまでに、多くの時間とシステム リソースを要することがあります。しかし、これは、バックアップや復元が正常に行えるかどうかには影響を及ぼしません。

Windows Cell Manager での IDB 変換

概要

この項は、セル内に Windows 以外のクライアントが含まれている Windows 用 Cell Manager を Data Protector A.05.00 または A.05.10 からアップグレードする場合にのみ適用されます。A.05.50 からアップグレードする場合は、変換は不要です。

Data Protector A.06.00 へのアップグレード IDB 内でのファイル名の変更

IDB 変換は、IDB のサイズとセルの構成によって、長い時間を要することがあります。しかし、これは、バックアップや復元が正常に行えるかどうかには影響を及ぼしません。変換は、セル内のすべての非 Windows クライアントに対して、1つのバックグラウンド プロセスとして実行されますが、このとき Data Protector は、通常どおりの動作が可能です。このプロセスでは、まず1つのクライアント上の全データが変換されてから、次のクライアントのデータ変換が開始されます。作業が終了したら、IDB 変換は完了し、再実行する必要はありません。

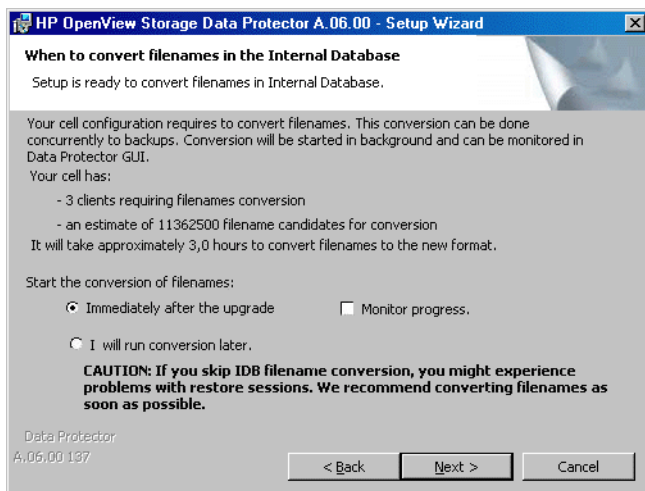
非 ASCII 文字が含まれていないファイル名についても、IDB 変換は実行されますが、IDB 内では何も変更されません。

IDB 変換は、IDB サイズには影響を及ぼしません。

IDB 変換の実行方法

Data Protector のアップグレード完了後、Data Protector セットアップ ウィザードで、IDB 内のファイル名を変換できます。

図 4-4 アップグレード後の IDB 変換



IDB 変換のおおよその所要時間が表示されます。所要時間は、セル内の Windows 以外のクライアントの数と、IDB に格納されているファイル数に基づいて、計算されます。

変換を後でする場合、omnidbupgrade コマンドを使用して、IDB 変換を手作業で実行する必要があります。詳細は『HP OpenView Storage Data Protector Command Line Interface Reference』を参照してください。

注記 クライアントでの IDB 変換と Disk Agents のアップグレードは、できる限り早く実行することをお勧めします。

IDB 変換のステータス (変換が終了したクライアントに関するデータ) は、Data Protector GUI の [モニター] コンテキスト リストでチェックできます。

変換中のバックアップ

変換はバックグラウンドで実行されるため、IDB ファイル名変換中でも、バックアップが可能です。また、Data Protector も通常どおりの動作が可能です。

IDB 内のクライアントのデータがそのクライアントのバックアップ中に変換される場合、バックアップは No Log オプション (このセッションでは、このクライアントの IDB に関するファイルやディレクトリのバックアップ情報は記録されない) を使用して行われます。

変換中の復元

ファイル名の *変換中* でも復元は可能です。ただし、7ビット ASCII 文字で構成される、Windows 以外のシステムからのディレクトリやファイル (オブジェクト全体または選択された一部) の復元のみを行う方が安全です。

特定のクライアントに復元することを選択したファイルやディレクトリに非 ASCII 文字が含まれている場合 (かつ、Windows 以外のプラットフォームからのものである場合)、そのクライアントデータの IDB 変換が完了するのを待つようにしてください。そのクライアント上の Disk Agent を、復元前にアップグレードする必要があります。

IDB 変換後のバックアップと復元

IDB 全体の変換が完了し、セル内の全クライアント上のすべての Disk Agent がバージョン A.06.00 にアップグレードされた後、バックアップと復元は、通常どおりに行われます。

UNIX Cell Manager での IDB 変換

概要

この項は、セル内に Windows クライアントが含まれる UNIX 用 Cell Manager を Data Protector A.05.00 または A.05.10 からアップグレードする場合にのみ適用されます。A.05.50 からアップグレードする場合は、変換は不要です。

IDB 変換は、IDB のサイズとセルの構成によって、長い時間を要することがあります。しかし、これは、バックアップや復元が正常に行えるかどうかには影響を及ぼしません。変換は、一定期間に行われるセル内の Windows クライアントのバックアップ中に、バックグラウンドプロセスとして実行されます。セル内のすべての Windows クライアントにおいて、すべてのファイルシステムバックアップオブジェクトのフルバックアップが終了したら、IDB 変換は完了し、再実行する必要はありません。

バックアップ中の IDB 内のファイル名の変換は、デフォルトで 1 か月間実行されます。これは、ConvertFilenamesInIDBDuringBackup グローバル オプションで定義されます。グローバル オプション ファイルの編集方法の詳細は、『HP OpenView Storage Data Protector トラブルシューティング ガイド』を参照してください。

パフォーマンスへの影響

IDB 内のファイル名の変換は、パフォーマンスに影響を及ぼします。変換の実行中 (ConvertFilenamesInIDBDuringBackup グローバル オプションが有効に設定されている場合) には、クライアントの最初のフルバックアップが実行されるまで、Windows クライアントでのバックアップ速度が少し遅くなります。詳細は『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。

制限事項

以下の制限に留意してください。

- 前のバージョンの Data Protector でバックアップされ、古いエンコーディングを使用して IDB に保存されているファイルは、IDB 変換前にクライアントから削除されている可能性があります。この場合、IDB 内のファイル名は変換されません。変換期間中 (ConvertFilenamesInIDBDuringBackup グローバル オプションで定義) にバックアップが実行されなかった場合も、同じ状況になります。ファイル名に非 ASCII 文字が使用されていると、このようなファイルの復元は、より困難になります。回避策は、『HP OpenView Storage Data Protector トラブルシューティング ガイド』を参照してください。
- その他の制限については、264 ページの表 4-2 を参照してください。

シングルサーバ版からのアップグレード

以下のいずれかのアップグレードが可能です。

- 旧バージョンのシングルサーバ版 (SSE) から Data Protector A.06.00 シングルサーバ版へ。詳細な作業手順は、271 ページの「旧バージョンの SSE から Data Protector A.06.00 SSE へのアップグレード」を参照してください。
- Data Protector A.06.00 シングルサーバ版から Data Protector A.06.00 へ。詳細な作業手順は、271 ページの「Data Protector A.06.00 SSE から Data Protector A.06.00 へのアップグレード」を参照してください。

旧バージョンの SSE から Data Protector A.06.00 SSE へのアップグレード

旧バージョンの SSE から Data Protector A.06.00 SSE へのアップグレード手順は、旧バージョンの Data Protector から Data Protector A.06.00 へのアップグレード手順と同じです。詳細は、237 ページの「Data Protector A.05.x からのアップグレード」を参照してください。

Data Protector A.06.00 SSE から Data Protector A.06.00 へのアップグレード

ライセンス

シングルサーバ版の Data Protector A.06.00 から Data Protector A.06.00 へのアップグレードを行うには、ライセンスが必要です。ライセンスの詳細は、293 ページの第 5 章「Data Protector のライセンス」を参照してください。

Data Protector A.06.00 シングルサーバ版から Data Protector A.06.00 へのアップグレードについては、次の 2 つの状況が考えられます。

- Data Protector シングルサーバ版を 1 つのシステム (Cell Manager) にのみインストールしている場合。詳細は 272 ページの「Cell Manager のアップグレード」を参照してください。
- Data Protector シングルサーバ版を複数のシステムにインストールしており、それらのセルをマージしたい場合。詳細は 272 ページの「複数のシステムからのアップグレード」を参照してください。

注記

以前のバージョンのシングルサーバ版を Data Protector のフル インストール版にアップグレードする場合は、最初にシングルサーバ版を同じバージョンレベルのフル インストール版にアップグレードする必要があります。このフル インストール版を Data Protector A.06.00 にアップグレードする方法は、237 ページの「Data Protector A.05.x からのアップグレード」を参照してください。

Cell Manager のアップグレード

シングルサーバ版の Cell Manager をアップグレードするには、以下の手順に従ってください。

1. 以下のコマンドを実行して、シングルサーバ版のライセンスを削除します。
 - Windows の場合：
`del <Data_Protector_home>%Config%server%Cell%lic.dat`
 - UNIX の場合：
`rm /etc/opt/omni/server/cell/lic.dat`
2. Data Protector GUI を起動し、恒久パスワードを追加します。

複数のシステムからのアップグレード

複数のシステムにインストールされている Data Protector シングルサーバ版をアップグレードするには、以下の手順に従ってください。

1. 既存のシングルサーバ版システムのうち、新しい Cell Manager となるシステムを 1 つ選択します。詳細は 11 ページの「Cell Manager システムの選択」を参照してください。
2. 選択した Cell Manager を以下のようにアップグレードします。
 - a. 以下のコマンドを実行して、シングルサーバ版のライセンスを削除します。
`del <Data_Protector_home>%Config%server%Cell%lic.dat` (Windows システム) または
`rm /etc/opt/omni/server/cell/lic.dat` (UNIX システム)
 - b. Data Protector GUI を起動し、恒久パスワードを追加します。
3. GUI を使用して、他のシングルサーバ版システムを新たに作成した Cell Manager システムに、クライアントとしてインポートします。
4. 他のシステムから Data Protector シングルサーバ版をアンインストールします。詳細は 213 ページの「Data Protector ソフトウェアのアンインストール」を参照してください。

5. 必要に応じて、新しい Cell Manager にメディアをインポートします。

この手順は、他のシングルサーバ版システムで作成したメディアからデータを復元する頻度が高いと思われる場合に実行してください。このような復元の頻度が比較的低い場合は、復元アクションの [**メディアのリスト**] を使用できます。メディアのインポート方法、および [**メディアのリスト**] による復元の詳細は、オンライン ヘルプの索引キーワード「インポート, メディア」で表示される内容を参照してください。

Windows NT から Windows のより新しいバージョンへのアップグレード

Windows NT システム上に Cell Manager がインストールされている場合は、オペレーティングシステムをより新しいバージョンにアップグレードする必要があります。Windows NT は Data Protector A.06.00 の Cell Manager 用プラットフォームとしてサポートされていません。

オペレーティングシステムを Windows NT から Windows のより新しいバージョンにアップグレードする場合は、そのアップグレードが Data Protector に及ぼす影響を考慮する必要があります。

Windows NT 上にインストールされている Data Protector A.05.00 または A.05.10 Cell Manager を Data Protector A.06.00 にアップグレードする場合は、以下の順番でアップグレードしてください。

1. オペレーティングシステムを Windows NT からより新しいバージョンの Windows にアップグレードします。詳細は Windows のマニュアルを参照してください。
2. Data Protector A.05.00 または A.05.10 の Cell Manager を Data Protector A.06.00 にアップグレードします。作業手順は、237 ページの「Data Protector A.05.x からのアップグレード」を参照してください。

Solaris 7/8 から Solaris 9 へのアップグレード

Data Protector A.06.00 Disk Agent (DA) が Solaris 7/8 にインストールされている場合、オペレーティングシステムを Solaris 9 にアップグレードするかどうかについては、そのアップグレードが Data Protector に及ぼす影響を検討した上で決定してください。Data Protector の適切な動作を確保し、拡張属性のバックアップなどの高度なバックアップ オプションを Solaris 9 で使用できるようにするには、システムにインストールされている汎用 Solaris DA を Solaris 9 DA に置き換えることをお勧めします。

以下の順番でアップグレードしてください。

1. オペレーティングシステムを Solaris 7/8 から Solaris 9 にアップグレードします。詳細は Solaris のマニュアルを参照してください。
2. インストール サーバを使用して、アップグレードしたシステムに Disk Agent をリモート インストールします。これにより、汎用の Solaris Disk Agent が Solaris 9 Disk Agent に置換されます。詳細については、50 ページの「Data Protector クライアントのリモート インストール」を参照するか、または `ob2install` のマンページを参照してください。

HP-UX 11.x から HP-UX 11.23 への移行

ここでは、既存の Cell Manager を PA-RISC アーキテクチャ ベースの HP-UX 11.x システムから Intel Itanium 2 (IA-64) アーキテクチャ対応の HP-UX 11.23 に移行する手順を述べます。

制限事項

サポートされているオペレーティング システム バージョン、サポートされているプラットフォーム、サポートされているプロセッサ、サポートされている Data Protector コンポーネント、必要なパッチ、一般情報、およびインストールの必要条件については、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。

- サポートされている移行は、PA-RISC ベースの HP-UX 11.x システム上の Data Protector A.06.00 Cell Manager からの移行だけです。
- サポートされている MoM 構成の組み合わせについては、279 ページの「MoM 固有の手順」を参照してください。

推奨事項

- 移行前に IDB 内のファイル名を変換しておくことをお勧めします。詳細は 262 ページの「IDB 内でのファイル名の変更」を参照してください。

ライセンス

新しい Cell Manager (IA-64 システム) の IP アドレスは古い Cell Manager とは異なるため、移行前にライセンスの移行を適用してください。一定期間は、両方のシステムでライセンスは有効になります。ライセンスが IP の範囲に基づいており、新しい Cell Manager の IP アドレスがこの範囲内にある場合は、ライセンスを再構成する必要はありません。詳細は A-19 ページの「Data Protector A.06.00 へのライセンス移行」を参照してください。

注記

HP-UX 11.23 では GUI がサポートされません。ただし、`omniusers` コマンドを使用して新しい Cell Manager 上にリモート ユーザー アカウントを作成することができます。作成すると、Data Protector GUI をインストールした任意のシステム上でこのユーザー アカウントにより、GUI を起動して新しい Cell Manager に接続できます。`omniusers` のマンページを参照してください。

移行手順

以下の手順に従って移行してください。

1. IA-64 システム上に Data Protector クライアントをインストールし、それを古い Cell Manager のセルにインポートします。Data Protector をクラスタ内に構成する場合は、一次ノード上にクライアントをインストールします。詳細は 68 ページの「HP-UX クライアントのインストール」を参照してください。

2. 古い Cell Manager 上で以下のコマンドを実行し、保護が設定されたクライアントの信頼されるホスト一覧に IA-64 システムのホスト名を追加します。

```
omnimigrate.pl -prepare_clients <New_CM_Name>. ここで <New_CM_Name> は、前の手順の IA-64 システムのクライアント名です。
```

信頼されるホストと Data Protector クライアントの保護設定の詳細は、198 ページの「クライアントの保護」および 208 ページの「ホスト信頼」を参照してください。

3. IDB をバックアップします。オンライン ヘルプの索引キーワード「IDB, バックアップ」で表示される内容を参照してください。
4. IDB を IA-64 システム上の一時保存場所に復元します。オンライン ヘルプの索引キーワード「IDB, 復元」で表示される内容を参照してください。
5. Data Protector クライアントを IA-64 システムからアンインストールします。詳細は 214 ページの「Data Protector クライアントのアンインストール」を参照してください。
6. Data Protector Cell Manager を IA-64 システム上にインストールします。Data Protector をクラスタ内に構成する場合は、Cell Manager をクラスタ対応ではなくスタンドアロン Cell Manager として一次ノード上にインストールします。詳細は 19 ページの「Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール」を参照してください。
7. 古い Cell Manager 上のデフォルトの Data Protector Inet ポートを変更した場合は、新しい Cell Manager 上にも同じ Inet ポートを設定します。詳細は 28 ページの「デフォルトのポート番号の変更」を参照してください。
8. 新しい Cell Manager 上の一時保存場所にある復元された IDB と構成データを、新しい Cell Manager 上の、古い Cell Manager と同じ場所に移動します。オンライン ヘルプの索引キーワード「IDB, 復元」で表示される内容を参照してください。

古い Cell Manager がクラスタ対応である場合は、`/etc/opt/omni/server/sg/sg.conf` ファイルの `SHARED_DISK_ROOT` 変数と `CS_SERVICE_HOSTNAME` 変数をコメントにします。この作業は、新しい Cell Manager がクラスタ対応であっても必要です。

Data Protector A.06.00 へのアップグレード HP-UX 11.x から HP-UX 11.23 への移行

9. IDB とクライアントを新しい Cell Manager に移行し、Cell Manager の設定を再構成するため、新しい Cell Manager 上で以下の手順を実行します。
- スタンドアロン IA-64 Cell Manager を構成する場合は、以下の手順に従ってください。
 - a. `omnimigrate.pl -configure` コマンドを実行します。`omnimigrate.pl` のマンページを参照してください。
 - クラスタ対応 IA-64 Cell Manager を構成する場合は、以下の手順に従ってください。
 - a. `omnimigrate -configure_idb` コマンドを実行して、古い Cell Manager から移した IDB を、新しい Cell Manager 上で使えるように構成します。`omnimigrate.pl` のマンページを参照してください。
 - b. `omnimigrate -configure_cm` コマンドを実行して、古い Cell Manager から移した構成データを、新しい Cell Manager 上で使えるように再構成します。`omnimigrate.pl` のマンページを参照してください。
 - c. `omnicc -export_host <Old_CM_Name>` を実行して、古い仮想サーバをセルからエクスポートします。
 - d. 一次および二次 Cell Manager を構成します。オンライン ヘルプの索引キーワード「MC/ServiceGuard 用統合ソフトウェアの構成」で表示される内容を参照してください。
 - e. `omnimigrate -configure_clients` コマンドを実行して、古い Cell Manager から新しい Cell Manager に移行します。古い Cell Manager の構成ファイルにはクライアントが残っていることに注意してください。そのクライアントの Cell Manager は存在しません。

注記 `/etc/opt/omni/server` ディレクトリが共有クラスタ ボリュームにある場合は、`omnimigrate.pl` スクリプトによる構成の変更がクラスタのすべてのノードに影響します。

注記 古い Cell Manager は、自動的に新しいセルのクライアントになります。古い Cell Manager 上では Cell Manager コンポーネントが不要なため、アンインストールしても構いません。詳細は 226 ページの「Data Protector ソフトウェア コンポーネントの変更」を参照してください。

10. 新しい Cell Manager 上でライセンスを構成します。詳細は A-2 ページの「Data Protector A.06.00 の製品構成とライセンス」を参照してください。

11. 新しい Cell Manager 上でリモート ユーザー アカウントを作成し、Data Protector GUI をインストールした他のシステム上で新しく作成したユーザー アカウントを使用して、GUI を起動して新しい Cell Manager に接続します。詳細は、omniusers のマンページを参照してください。
12. 以下に該当する場合は、さらに手順を実行する必要があります。
 - セルが MoM 環境の一部である場合。279 ページの「MoM 固有の手順」を参照してください。
 - セルがファイアウォールを越えて機能する場合。新しい Cell Manager 上にすべてのファイアウォールに関連する設定を再構成します。オンライン ヘルプの索引キーワード「ファイアウォール環境」で表示される内容を参照してください。
 - 新しい Cell Manager 上にインストール サーバを配置する場合。280 ページの「インストール サーバ固有の手順」を参照してください。

MoM 固有の手順

新しい Cell Manager を MoM に構成する場合、基本的な移行手順が完了した後にさらに手順を実行する必要があります。必要な手順は、環境における新旧 Cell Manager に対する MoM 構成によって異なります。以下の組み合わせがサポートされます。

- 古い Cell Manager が MoM クライアントであり、新しい Cell Manager が同じ MoM Manager の MoM クライアント

この場合、以下の手順を実行します。

1. MoM Manager で、古い Cell Manager を MoM Manager セルからエクスポートし、新しい Cell Manager をインポートします。オンライン ヘルプの索引キーワード「クライアント システム, エクスポート」で表示される内容を参照してください。
2. MoM 管理者を新しい Cell Manager のユーザー リストに追加します。オンライン ヘルプの索引キーワード「MoM 管理者, 追加」で表示される内容を参照してください。

- 古い Cell Manager は MoM Manager であり、新しい Cell Manager も MoM Manager

古い MoM Manager が MoM で唯一のクライアントである場合、処理は必要ありません。それ以外の場合、以下の手順を実行してください。

1. 古い MoM Manager (古い Cell Manager) で、すべての MoM クライアントをエクスポートします。
2. 新しい MoM Manager (新しい Cell Manager) で、すべての MoM クライアントをインポートします。

Data Protector A.06.00 へのアップグレード HP-UX 11.x から HP-UX 11.23 への移行

3. すべての MoM クライアントのユーザー リストに MoM 管理者を追加します。

注記 HP-UX 11.23 では GUI がサポートされません。ただし、`omniusers` コマンドを使用して新しい Cell Manager 上にリモート ユーザー アカウントを作成することができます。作成すると、Data Protector GUI をインストールした任意のシステム上でこのユーザー アカウントにより、GUI を起動して新しい Cell Manager に接続できます。`omniusers` のマンページを参照してください。

インストール サーバ固有の手順

インストール サーバの移行は、Cell Manager 移行の一部としては行われません。古い Cell Manager 上にインストール サーバをインストールしている場合は、インストール サーバが新しい Cell Manager に移行されず、セルに残ります。

新しい Cell Manager もインストール サーバとして使用する場合は、移行後に新しい Cell Manager 上にインストール サーバ コンポーネントをインストールし、セルにインポートします。オンライン ヘルプの索引キーワード「インストール サーバ」で表示される内容を参照してください。

32 ビット Windows から 64 ビット Windows への移行

ここでは、既存の Cell Manager を 32 ビット Windows システムから 64 ビット Windows システムに移行する手順について説明します。

制限事項

サポートされているオペレーティング システム バージョン、サポートされているプラットフォーム、サポートされているプロセッサ、サポートされている Data Protector コンポーネント、必要なパッチ、一般情報、およびインストールの必要条件については、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス』を参照してください。

前提条件

- 移行を開始する前に、32 ビット Windows システム上の Data Protector Cell Manager を Data Protector A.06.00 にアップグレードしなければなりません。

推奨事項

- Data Protector A.05.10 以前のバージョンからアップグレードする場合は、移行前に IDB 内のファイル名を変換しておくことをお勧めします。詳細は 262 ページの「IDB 内でのファイル名の変更」を参照してください。

ライセンス

新しい Cell Manager の IP アドレスは古い Cell Manager とは異なるため、移行前にライセンスの移行を適用してください。一定期間は、両方のシステムでライセンスが有効になります。ライセンスが IP の範囲に基づいており、新しい Cell Manager の IP アドレスがこの範囲内にある場合は、ライセンスを再構成する必要はありません。詳細は A-19 ページの「Data Protector A.06.00 へのライセンス移行」を参照してください。

移行手順

以下の手順に従って移行してください。

1. Data Protector クライアントを 64 ビット システムにインストールし、このシステムを元の Cell Manager のセルにインポートします。詳細は 63 ページの「Windows 用クライアントのインストール」を参照してください。

- 古い Cell Manager 上で、保護が設定されたクライアント上の信頼されるホスト一覧に 64 ビット システムのホスト名を追加します。<Data_Protector_home>%bin ディレクトリから次のコマンドを実行してください。

```
perl.exe winomnimigrate.pl -prepare_clients <New_CM_Name>
```

<New_CM_Name> には 64 ビット システムのクライアント名を指定します。

winomnimigrate.pl の詳細は、『HP OpenView Storage Data Protector Command Line Interface Reference』を参照してください。

信頼されるホストと Data Protector クライアントの保護設定の詳細は、198 ページの「クライアントの保護」および 208 ページの「ホスト信頼」を参照してください。

- IDB をバックアップします。オンライン ヘルプの索引キーワード「IDB, バックアップ」で表示される内容を参照してください。
- IDB を 64 ビット システム上の一時保存場所に復元します。オンライン ヘルプの索引キーワード「IDB, 復元」で表示される内容を参照してください。
- Data Protector クライアントを 64 ビット システムからアンインストールします。詳細は 214 ページの「Data Protector クライアントのアンインストール」を参照してください。
- 64 ビット システムに Data Protector Cell Manager をインストールします。詳細は 19 ページの「Data Protector Cell Manager (CM) およびインストール サーバ (IS) のインストール」を参照してください。
- 古い Cell Manager 上でデフォルトの Data Protector Inet ポートを変更していた場合は、新しい Cell Manager 上でも同じ Inet ポートを設定します。詳細は 28 ページの「デフォルトのポート番号の変更」を参照してください。
- 新しい Cell Manager 上の一時保存場所に復元した IDB と構成データを、新しい Cell Manager 上の、古い Cell Manager と同じ場所に移動します。オンライン ヘルプの索引キーワード「IDB, 復元」で表示される内容を参照してください。
- IDB とクライアントを新しい Cell Manager に移行し、Cell Manager の設定を再構成するため、新しい Cell Manager 上で以下の手順を実行します。

- スタンドアロンの Cell Manager を構成する場合は、<Data_Protector_home>%bin ディレクトリから、次のコマンドを実行してください。

```
perl.exe winomnimigrate.pl -configure
```

- クラスタ対応の Cell Manager を構成する場合は、以下の手順に従ってください。

- a. <Data_Protector_home>%binディレクトリからperl.exe winomnimigrate.pl -configure_idb コマンドを実行して、古い Cell Manager から移した IDB を、新しい Cell Manager 上で使えるように構成します。
- b. <Data_Protector_home>%binディレクトリからperl.exe winomnimigrate.pl -configure_cm コマンドを実行して、古い Cell Manager から移した構成データを、新しい Cell Manager 上で使えるように再構成します。
- c. omnicc -export_host <Old_CM_Name> コマンドを実行して、古い仮想サーバをセルからエクスポートします。
- d. <Data_Protector_home>%binディレクトリからperl.exe winomnimigrate.pl -configure_clients コマンドを実行して、古い Cell Manager から新しい Cell Manager にクライアントを移行します。古い Cell Manager 上の構成ファイルには、そのシステムが Cell Manager ではなくなったにもかかわらず、それらのクライアント情報が残っていることに注意してください。

注記

古い Cell Manager は、自動的に新しいセルのクライアントになります。古い Cell Manager 上の Cell Manager コンポーネントは不要になるため、アンインストールしても構いません。詳細は 226 ページの「Data Protector ソフトウェア コンポーネントの変更」を参照してください。

10. 新しい Cell Manager 上でライセンスを構成します。詳細は A-2 ページの「Data Protector A.06.00 の製品構成とライセンス」を参照してください。
11. 以下の場合は追加の手順が必要になります。
 - セルが MoM 環境の一部である場合。283 ページの「MoM 固有の手順」を参照してください。
 - セルがファイアウォールを越えて機能する場合。新しい Cell Manager 上にすべてのファイアウォールに関連する設定を再構成します。オンライン ヘルプの索引キーワード「ファイアウォール環境」で表示される内容を参照してください。
 - 新しい Cell Manager 上にインストール サーバを配置する場合。284 ページの「インストール サーバ固有の手順」を参照してください。

MoM 固有の手順

新しい Cell Manager を MoM に構成する場合、基本的な移行手順が完了した後にさらに手順を実行する必要があります。必要な手順は、環境における新旧 Cell Manager に対する MoM 構成によって異なります。以下の組み合わせがサポートされます。

32 ビット Windows から 64 ビット Windows への移行

- 古い Cell Manager が MoM クライアントであり、新しい Cell Manager が同じ MoM Manager の MoM クライアント

この場合、以下の手順を実行します。

1. MoM Manager 上で、古い Cell Manager を MoM Manager セルからエクスポートし、新しい Cell Manager をインポートします。オンライン ヘルプの索引キーワード「クライアント システム, エクスポート」で表示される内容を参照してください。
 2. MoM 管理者を新しい Cell Manager のユーザー リストに追加します。オンライン ヘルプの索引キーワード「MoM の管理者, 追加」で表示される内容を参照してください。
- 古い Cell Manager は MoM Manager であり、新しい Cell Manager も MoM Manager
- 古い MoM Manager が MoM で唯一のクライアントである場合、処理は必要ありません。それ以外の場合、以下の手順を実行してください。
1. 古い MoM Manager (古い Cell Manager) で、すべての MoM クライアントをエクスポートします。
 2. 新しい MoM Manager (新しい Cell Manager) で、すべての MoM クライアントをインポートします。
 3. すべての MoM クライアントのユーザー リストに MoM 管理者を追加します。

インストール サーバ固有の手順

インストール サーバの移行は、Cell Manager 移行の一部としては実行されません。古い Cell Manager 上にインストール サーバがインストールされている場合は、インストール サーバが新しい Cell Manager には移行されません。

新しい Cell Manager もインストール サーバとして使用する場合は、移行後に新しい Cell Manager 上にインストール サーバコンポーネントをインストールし、セルにインポートします。オンライン ヘルプの索引キーワード「インストール サーバ」で表示される内容を参照してください。

MC/ServiceGuard 上で構成されている Cell Manager のアップグレード

アップグレード時には、データベースのみがアップグレードされて、古いバージョンは削除されます。Data Protector A.06.00 がデフォルトで選択されるエージェントとともにインストールされ、その他のエージェントは削除されます。アップグレード前と同じ構成にしたい場合は、必要なエージェントをアップグレード時に手作業で選択するか、各物理ノード上に後から再インストールしなければなりません。

Data Protector A.05.00、Data Protector A.05.10、および Data Protector A.05.50 からのアップグレードでは、一次ノードと二次ノードのアップグレードが必要です。以下の手順に従います。

一次ノード

一次ノードにログオンし、以下の手順に従ってください。

`cmhaltpkg <pkg_name>` コマンドを実行して、古い OmniBack II や Data Protector パッケージを停止します (<pkg_name> には、クラスタ パッケージの名前を指定)。以下に例を示します。

```
cmhaltpkg ob2cl
```

4. 以下のようにボリューム グループを排他モードでアクティブ化します。

```
vgchange -a e -q y <vg_name>
```

例：

```
vgchange -a e -q y /dev/vg_ob2cm
```

5. 論理ボリュームを共有ディスクにマウントします。

```
mount <lv_path> <shared_disk>
```

<lv_path> パラメータには論理ボリュームのパス名を、<shared_disk> パラメータにはマウント ポイントまたは共有ディレクトリを指定します。以下に例を示します。

```
mount /dev/vg_ob2cm/lv_ob2cm /omni_shared
```

6. 以降の項に記述されている手順に従って Cell Manager をアップグレードします。Data Protector A.06.00 にアップグレードする製品のバージョンによって一部の手順が異なることに注意してください。237 ページの「UNIX 用 Cell Manager とインストール サーバのアップグレード」を参照してください。
7. 実行されている Data Protector サービスがあれば、停止します。

```
/opt/omni/sbin/omnisv -stop
```

- 共有ディスクのマウントを解除します。

```
umount <shared_disk>
```

例 :

```
umount /omni_shared
```

- ボリューム グループを非アクティブ化します。

```
vgchange -a n <vg_name>
```

例 :

```
vgchange -a n /dev/vg_ob2cm
```

二次ノード

二次ノードにログオンし、以下の手順に従ってください。

- 以下のようにボリューム グループを排他モードでアクティブ化します。

```
vgchange -a e -q y <vg_name>
```

- 論理ボリュームを共有ディスクにマウントします。

```
mount <lv_path> <shared_disk>
```

- Cell Manager をアップグレードします。Data Protector A.06.00 にアップグレードする製品のバージョンによって、手順は異なります。237 ページの「UNIX 用 Cell Manager とインストール サーバのアップグレード」の手順に従ってください。

- /etc/opt/omni/server/sg ディレクトリの csfailover.sh 起動スクリプトと mafailover.ksh 起動スクリプトの名前を csfailover_DP51.sh や mafailover_DP51.ksh に変更し、新しい csfailover.sh スクリプトと mafailover.ksh スクリプトを /opt/omni/newconfig/etc/opt/omni/server/sg ディレクトリから /etc/opt/omni/server/sg ディレクトリにコピーします。

古い起動スクリプトをカスタマイズしていた場合は、新しい起動スクリプトにも変更を再実装します。

注記

Data Protector A.06.00 では、一部の構成ファイル、ログファイル、および (UNIX の場合は) データベースファイルのデフォルトパスが変更されています。このバージョンでは、一部のファイルが `server` ディレクトリと `client` ディレクトリに分かれて配置されるようになりました。詳細は B-77 ページの「UNIX での構成ファイル」を参照してください。

5. 実行されている Data Protector サービスがあれば、停止します。

```
/opt/omni/sbin/omnisv -stop
```

6. 共有ディスクのマウントを解除します。

```
umount <shared_disk>
```

7. ボリューム グループを非アクティブ化します。

```
vgchange -a n <vg_name>
```

一次ノード

一次ノードに再度ログインし、以下の手順に従ってください。

1. Data Protector パッケージを再起動します。

```
cmrunpkg <pkg_name>
```

パッケージ切り替えおよびノード切り替えオプションが有効になっていることを確認します。

2. Cell Manager を構成します。スクリプトを実行するときに `/etc/opt/omni` ディレクトリや `/var/opt/omni` ディレクトリ、あるいはサブディレクトリに配置しないようにします。`/etc/opt/omni` または `/var/opt/omni` のサブディレクトリに何もマウントされていないことも確認します。以下を実行します。

```
/opt/omni/sbin/install/omniforsg.ksh -primary -upgrade
```

3. 仮想ホストを再度インポートします。

```
omnicc -import_host <virtual_hostname> -virtual
```

4. IDB 内の Cell Manager の名前を変更します。

```
omnidbutil -change_cell_name
```

5. インストール サーバが Cell Manager と同じパッケージにある場合は、以下のインストールサーバ仮想ホスト名をインポートします。

```
omnicc -import_is <virtual_hostname>
```

注記

Cell Manager からのすべての要求は、クライアント上の /var/opt/omni/log/inet.log ファイルに記録されます。不要なログ エントリが書き込まれないようにするには、クライアントに保護を設定します。セルに保護を設定する方法は、195 ページの「保護について」を参照してください。

Microsoft Cluster Server 上で構成されている Cell Manager のアップグレード

Microsoft Cluster Server (MSCS) 上の、Data Protector A.05.00、A.05.10 または A.05.50 の Cell Manager から Data Protector A.06.00 へのアップグレードは、Windows 用インストール DVD-ROM からローカルに実行する必要があります。

注記 すべてのクラスタ ノードには、MSI 2.0 のインストールをお勧めします。

アップグレードは、以下の手順で行ってください。

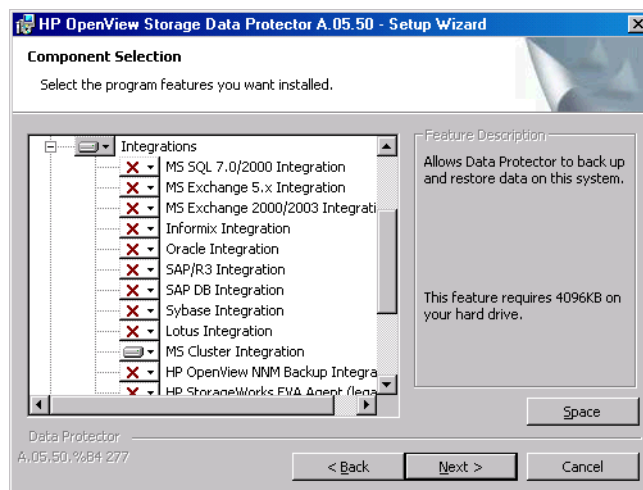
1. Windows 用インストール DVD-ROM を挿入し、%Windows_other%\i386\setup.exe を実行します。現在アクティブ化されている仮想サーバ ノードで、セットアップを起動することをお勧めします。

自動的に旧バージョンの製品が検出され、Data Protector A.06.00 にアップグレードするようプロンプトが表示されます。

[Next] をクリックして次に進みます。

2. インストール済みのコンポーネントが Data Protector によって自動的に選択されます。

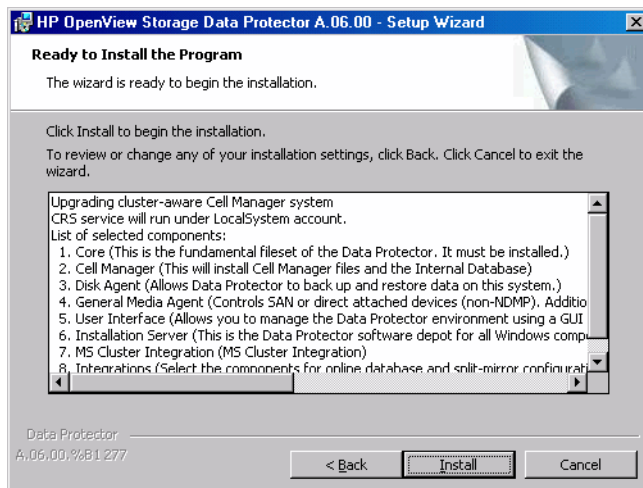
図 4-5 コンポーネントの選択



3. コンポーネントの選択サマリー リストが表示されます。[Install] をクリックしてアップグレードを実行します。

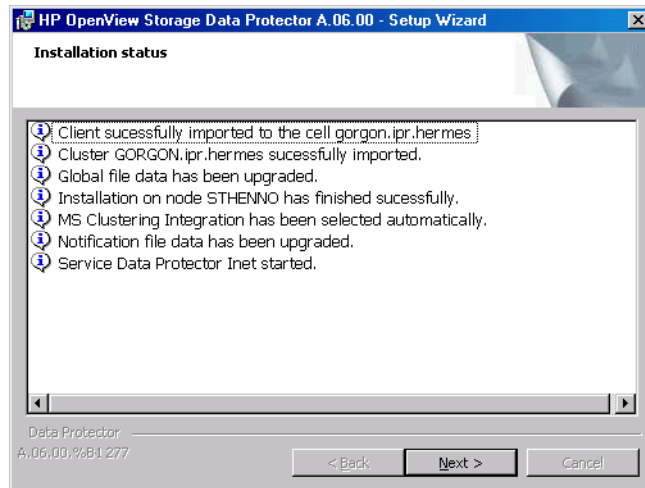
アップグレード後には、すべてのノードに同じコンポーネント セットがインストールされていることに注意してください。

図 4-6 コンポーネント選択サマリー ページ



4. [Installation status] ページが表示されます。[Next] をクリックします。

図 4-7 **[Installation Status] ページ**



5. セル内に UNIX クライアントがある場合は、[IDB Conversion] ページが表示されます。詳細は 262 ページの「IDB 内でのファイル名の変更」を参照してください。
6. セットアップ後すぐに Data Protector を起動するには、[Start the Data Protector Manager GUI] を選択します。

『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を表示するには、[Open the Product Announcements] を選択します。

HP OpenView AutoPass ユーティリティは、すべてのノードではなく 1 つのノードにのみインストールされるため、Microsoft Cluster にインストールすることはお勧めできません。ただし、AutoPass をインストールする場合は、Data Protector をシステムから削除するために、インストールされているノードと同じノードから Data Protector をアンインストールする必要があります。

[Finish] をクリックします。

注記

クラスタ対応クライアントのアップグレードを行う場合は、最初にすべてのクラスタ ノードを個別にアップグレードしてから、仮想サーバを再度インポートしてください。リモート アップグレードはサポートされていません。

5 Data Protector のライセンス

この章の内容

この章では、Data Protector のライセンスのチェック機能とレポート機能、Data Protector のパスワードの取得とインストールについて説明します。

概要

Data Protector A.06.00 の製品構成とライセンスには、大きく分けて以下の 3 種類があります。

1. スターターパック
2. ドライブとライブラリの使用权
3. 機能拡張

注記

UNIX 用の製品ライセンスは、どのプラットフォーム上でも使用でき、すべてのプラットフォームでその機能を提供します。一方、Windows 用の製品ライセンスは、Windows、Linux、および NetWare プラットフォーム上でしか使用できません。

パスワードは Cell Manager にバインドされ、Data Protector セル全体に対して有効です。クライアントでは、ファイルシステムバックアップまたはディスクイメージバックアップ用のライセンスは必要ありません。

ライセンス チェック機能とレポート機能

Data Protector ライセンスは、さまざまな Data Protector オペレーション中にチェックされ、見つからない場合にはレポートされます。以下に例を示します。

- Data Protector のチェックおよび保守管理機能の一部として、ライセンスの存在がチェックされ、見つからなかった場合は、Data Protector イベント ログに記録されます。Data Protector イベント ログは、Cell Manager 上の
`<Data_Protector_home>%log%server%Ob2EventLog.txt` ファイル内にあります。Data Protector のチェックおよび保守管理機能の詳細は、オンライン ヘルプの索引キーワード「イベント ログ , Data Protector」で表示される内容を参照してください。
- Data Protector イベント ログにライセンスがないことが記録されていた場合は、Data Protector ユーザー インタフェースを起動したときに、イベント ログからの通知が表示されます。Data Protector イベント ログの詳細は、オンライン ヘルプの索引キーワード「イベント ログ , Data Protector」で表示される内容を参照してください。
- Data Protector セッションの起動時には、ライセンスがチェックされ、もし見つからなかった場合はレポートされます。

Data Protector ライセンスでは、以下のような特性がグループ化されます。

- Cell Manager 関連ライセンス
- エンティティ ベース使用権
- キャパシティ ベース使用権

Cell Manager 関連ライセンス

Data Protector Cell Manager 関連ライセンスは以下のとおりです。

- スターター パック
- マネージャ・オブ・マネージャ使用権
- シングルサーバ版

Cell Manager (スターター パックに含まれる) や Manager-of-Managers などの一部の Data Protector コンポーネントがセル内に存在する場合は、必要とされる関連ライセンスの存在のみがチェックされます。

エンティティ ベース使用権

Data Protector のエンティティ・ベース使用権は、以下のとおりです。

- 61-250 スロット ライブラリ使用権 (1 台)、および、スロット数無制限ライブラリ使用権 (1 台)
- 追加ドライブ使用権 UNIX, SAN, NAS、および、追加ドライブ使用権 Windows, NetWare, Linux
- オンライン・バックアップ使用権 UNIX (システム 1 台)、および、オンライン・バックアップ使用権 Windows, Linux (システム 1 台)

前述のいずれかのエンティティ・ベース使用権の対象となる製品がセル内で構成されている場合は、必要なエンティティ・ベース使用権の存在とその数がチェックされます。

Data Protector のチェックでは、構成されているエンティティ・ベースの項目数とエンティティ・ベース使用権の数が比較されます。構成されている項目数よりもライセンス数が少ない場合は、通知が発行されます。

前述の最初の 2 つのライセンスでは、以下の作業も必要です。

SAN 環境の複数の Data Protector クライアントでバックアップ デバイスが構成されている場合、Data Protector では、マルチパス機能を使用して、シングルバックアップ デバイスとして認識させる必要があります。

キャパシティ ベース使用権

Data Protector のキャパシティ・ベース使用権は、以下のとおりです。

- ゼロ・ダウンタイム・バックアップ (ZDB) HP XP 使用権 (1 TB、10 TB)
- ゼロ・ダウンタイム・バックアップ HP EVA 使用権 (1 TB、10 TB)
- ゼロ・ダウンタイム・バックアップ EMC Symmetrix 使用権 (1 TB、10 TB)
- インスタント・リカバリ HP XP 使用権 (1 TB、10 TB)
- インスタント・リカバリ HP EVA 使用権 (1 TB、10 TB)
- ダイレクト・バックアップ HP XP 使用権 (1 TB、10 TB)
- ダイレクト・バックアップ HP EVA 使用権 (1 TB、10 TB)
- NDMP ダイレクト・バックアップ使用権 (1 TB、10 TB)
- アドバンスド・バックアップ使用権 (1 TB、10 TB、100 TB)

アドバンスド バックアップ用のキャパシティ ベース使用権は、このグループの他のライセンスと異なる扱いが適用されます。299 ページの「アドバンスド・バックアップ使用権」を参照してください。

キャパシティ・ベース使用権 (アドバンスド・バックアップ使用権以外) のチェックでは、バックアップされる論理ユニット上の合計ディスク容量が、インストールされているライセンス数と比較されます。

ライセンスのチェックでは、ライセンスされている容量を超えていた場合でもインスタント リカバリやバックアップの妨げとなりません。このような場合、ライセンスされている容量を超えたことを通知する警告メッセージがバックアップ中に表示されます。

使用ディスクの容量は、各 ZDB セッションやダイレクト バックアップ セッション中に収集された履歴情報に基づいて計算されます。考慮される時間は 24 時間です。Data Protector では、過去 24 時間の全セッションで使用されたディスクに基づいて使用ディスク容量が計算され、計算された容量とライセンスされている容量が比較されます。

ライセンス違反が発生していると、バックアップ中に警告メッセージが発行されます。また、ライセンスレポート ツールが毎日実行され、ライセンスされている容量を超えた場合は Data Protector イベント ログに通知が書き込まれます。

使用容量の計算

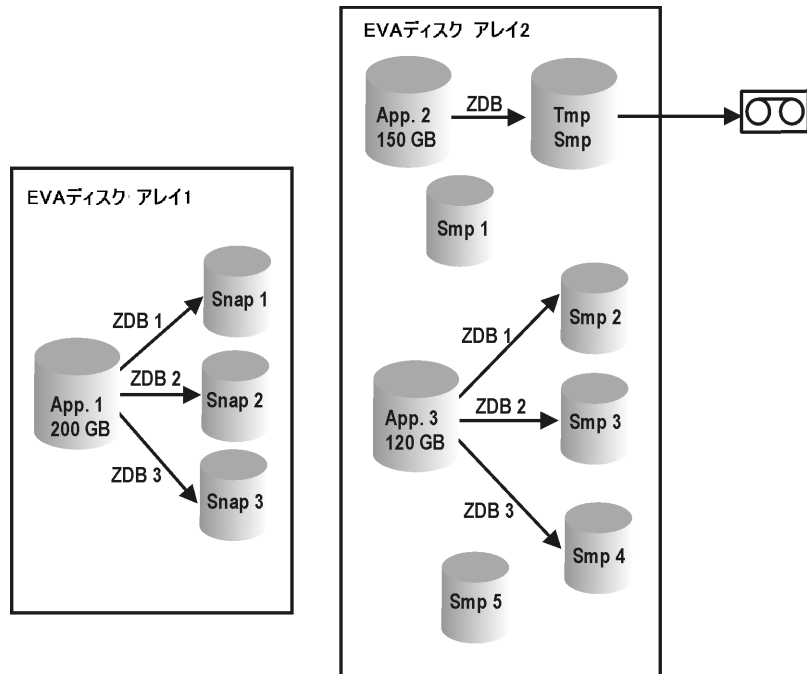
使用容量の計算では、過去 24 時間に使用された各ディスク アレイ タイプのライセンスされている容量が計算されます。指定されている期間に 2 回以上使用されたディスクは一度だけ数えられます。ディスク アレイ ユニットの、各アレイの識別番号によって特定されます。識別番号の使用によって、アレイが計算に入れられた時期がわかります。

インスタント リカバリまたはダイレクト バックアップを含む ZDB セッションが実行された場合は、元のユニットの合計容量がディスク アレイの ZDB 使用容量として計算され、さらに、インスタント リカバリまたはダイレクト バックアップのディスク アレイの使用容量も計算されます。

たとえば、EVA ディスク アレイが 2 つあったとします。1 つ目のアレイには、データの保護用に容量 200 GB のディスク (App. 1) が 1 つあります。1 日 3 回開始される各バックアップ セッションにはインスタント リカバリのオプションが含まれています。同時に 3 つのスナップショットが維持され、ローテーションされて、インスタント リカバリ用に保存されます。2 つ目のディスク アレイには、2 つのディスク (150 GB の App. 2 と 120 GB の App. 3) があります。App. 2 ディス

クでは、バックアップが 1 日に 1 回実行され、データをテープへ移動した後でスナップショットが削除されます。App. 3 では、バックアップが 1 日 3 回実行され、インスタント リカバリ用に 5 つのスナップショットがローテーションされて、保存されます。

図 5-1 使用容量の計算シナリオ



過去 24 時間のバックアップ セッションで使用されたすべてのディスクを ZDB 使用容量として計算すると、200 GB (App.1) + 150 GB (App.2) + 120 GB (App.3) = 470 GB。

インスタント リカバリ用にデータを残した ZDB セッションのソース容量をインスタント リカバリの使用容量として計算すると (同じディスクは一度だけ数える)、200 GB (App.1) + 120 GB (App.3) = 320 GB になります。

アドバンスト・バックアップ使用権

ファイル ライブラリへのバックアップには、アドバンスト・バックアップ使用権が必要になります。仮想テープ ライブラリに対して、ドライブおよびライブラリのライセンスの代わりに、アドバンスト・バックアップ使用権を使うことも可能です。

Data Protector のライセンス

ライセンス チェック機能とレポート機能

アドバンスト・バックアップ使用権のチェック時には、アドバンスト・バックアップ使用権を必要とするデバイス内に構成されたすべてのメディア上の使用スペース容量が、インストールされているライセンス数と比較されます。

すべてのファイル ライブラリ メディアおよび仮想テープ ライブラリ メディア上にバックアップされたデータ 1 TB ごとに、アドバンスト・バックアップ使用権が 1 つずつ必要です。仮想テープ ライブラリの場合は、圧縮率が 2:1 とみなされます。これは、1 つのアドバンスト・バックアップ使用権で、2 TB のデータをバックアップできることを意味します。

10 TB 用および 100 TB 用の使用権も用意されています。1 TB の使用権を 10 個または 100 個購入するよりも、これらのパッケージの方が低価格です。

ファイル ライブラリ メディア、仮想テープ ライブラリ メディア、または仮想メディアを IDB からエクスポートすると、そのメディア上のデータは、このライセンスの計算対象ではなくなります。メディアをインポートし直すと、(メディア上のデータが上書きされていないならば) そのメディア上のデータが再びアドバンスト・バックアップ使用権の計算対象になります。

バックアップまたはオブジェクト コピーの開始時に、前のバックアップ セッションまたはオブジェクト コピー セッションで使用済みのディスク スペース量が計算されます。その数値がライセンスされているバックアップ対象ディスク スペース以下の場合、バックアップしているデータの量に関係なくバックアップが開始され完了します (バックアップ データ量がディスク スペースを超える可能性があります)。前のバックアップ セッションですでに限度を超過している場合、バックアップ セッションが開始されますが、ライセンスの限度を超過したことを示す警告が発行されます。

セル内のディスクへのバックアップに消費したディスク スペースを計算するために、Data Protector ではセル内のファイル ライブラリおよび仮想テープ ライブラリへのバックアップで作成された全メディアのサイズ合計を計算します。

アドバンスト・バックアップ使用権に関しては、バックアップ デバイス、ドライブ、およびスロットの数はチェックされず、Data Protector 内部データベース (IDB) に記録されているデータ容量のみがチェックされます。

注記

Data Protector のデフォルト動作では、仮想テープ ライブラリ デバイスが通常のライブラリ (SCSI II ライブラリなど) として扱われます。アドバンスト・バックアップ使用権を利用するには、デバイス構成中にデバイスを仮想テープ ライブラリとしてマークする必要があります。詳細は、オンライン ヘルプの索引キーワード「仮想テープ ライブラリ」で表示される内容を参照してください。

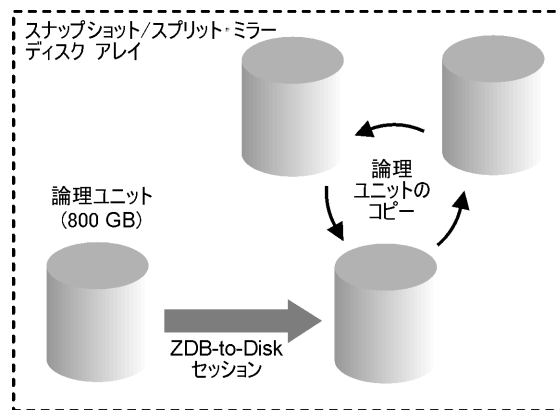
キャパシティ ベース使用権の例

ここでは、キャパシティ・ベース使用権の計算方法例を説明します。

例 1

301 ページの図 5-2 では、800 GB の論理ユニット 1 つからのデータが、ディスクへの ZDB (ZDB-to-Disk) セッションで 1 日に 3 度バックアップされる状況が例として示されています。

図 5-2 ZDB-to-Disk セッション



3 つのスプリット ミラーまたはスナップショット コピー (複製) がローテーションされて、インスタント リカバリの目的で保存されます。キャパシティ・ベース使用権では、以下のように計算されます。

800 GB の論理ユニット 1 つを使用するディスクへの ZDB セッション :

1 TB のゼロ・ダウンタイム・バックアップ使用権の対象となる容量を計算すると、 $1 \times 800 \text{ GB} = 0.8 \text{ TB}$ 。

同じ 800 GB の論理ユニットの複製 3 つが、インスタント リカバリの目的で保存されます。ライセンスの計算対象となるのは、ソース ボリュームの容量であり、複製の容量ではないことに、注意してください。

1 TB のインスタント・リカバリ使用権の対象となる容量を計算すると、 $1 \times 800 \text{ GB} = 0.8 \text{ TB}$ 。

301 ページの図 5-2 に示されている状況では、1 TB のゼロ・ダウンタイム・バックアップ使用権 1 つと、1 TB のインスタント・リカバリ使用権 1 つで、十分です。

Data Protector のライセンス ライセンス チェック機能とレポート機能

例 2

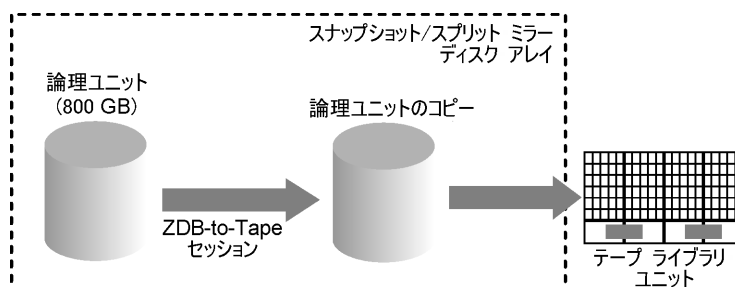
302 ページの図 5-3 では、800 GB の論理ユニット 1 つからのデータが、テープへの ZDB (ZDB-to-Tape) セッションで 1 日に 2 度バックアップされる状況が例として示されています。スプリット ミラーまたはスナップショット コピー (複製) は、インスタント リカバリの目的では保存されません。キャパシティ・ベース使用権では、以下のように計算されます。

800 GB の論理ユニット 1 つを使用するディスクへの ZDB セッション :

1 TB のゼロ・ダウンタイム・バックアップ使用権の対象となる容量を計算すると、 $1 \times 800 \text{ GB} = 0.8 \text{ TB}$ 。

1 TB のゼロ・ダウンタイム・バックアップ使用権 1 つで十分です。

図 5-3 ZDB-to-Tape セッション



例 3

303 ページの図 5-4 では、800 GB の論理ユニット 1 つからのデータが、ディスク + テープへの ZDB (ZDB-to-Disk+Tape) セッションで 1 日に 3 度バックアップされる状況が例として示されています。5 つのスプリット ミラーまたはスナップショット コピー (複製) がローテーションされて、インスタント リカバリの目的で保存されます。キャパシティ・ベース使用権では、以下のように計算されます。

800 GB の論理ユニット 1 つを使用するディスク + テープへの ZDB セッション :

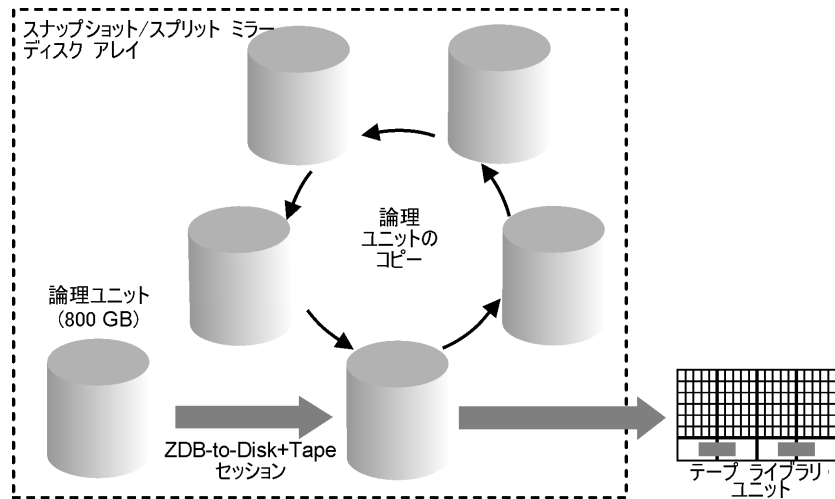
1 TB のゼロ・ダウンタイム・バックアップ使用権の対象となる容量を計算すると、 $1 \times 800 \text{ GB} = 0.8 \text{ TB}$ 。

同じ 800 GB の論理ユニットの複製 5 つが、インスタント リカバリの目的で保存されます。ライセンスの計算対象となるのは、ソース ボリュームの容量であり、複製の容量ではないことに、注意してください。

1 TB のインスタント・リカバリ使用権の対象となる容量を計算すると、 $1 \times 800 \text{ GB} = 0.8 \text{ TB}$ 。

1 TB のゼロ・ダウンタイム・バックアップ使用権 1 つと、1 TB のインスタント・リカバリ使用権 1 つで、十分です。

図 5-4 ZDB-to-Disk+Tape セッション



例 4

304 ページの図 5-5 では、800 GB の論理ユニット 1 つからのデータが、ダイレクト バックアップセッションで 1 日に 4 度バックアップされる状況が例として示されています。ダイレクト バックアップセッション中に作成された 3 つのスプリット ミラーまたはスナップショット コピー (複製) がローテーションされて、インスタント リカバリの目的で保存されます。キャパシティ・ベース使用権では、以下のように計算されます。

800 GB の論理ユニット 1 つを使用するダイレクト バックアップセッション :

1 TB のダイレクト・バックアップ使用権の対象となる容量を計算すると、 $1 \times 800 \text{ GB} = 0.8 \text{ TB}$ 。

ディスク+テープへの ZDB セッションでは、800 GB の同じ論理ユニットが使用され、したがって、以下のとおり他のライセンスの計算対象となります。

1 TB のゼロ・ダウンタイム・バックアップ使用権の対象となる容量を計算すると、 $1 \times 800 \text{ GB} = 0.8 \text{ TB}$ 。

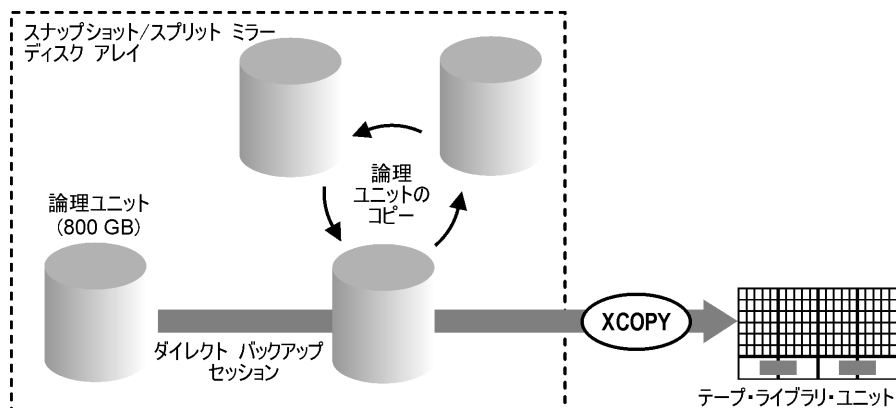
同じ 800 GB の論理ユニットの複製 3 つが、インスタント リカバリの目的で保存されます。ライセンスの計算対象となるのは、ソース ボリュームの容量であり、複製の容量ではないことに、注意してください。

Data Protector のライセンス ライセンス チェック機能とレポート機能

1 TB のインスタント・リカバリ使用権の対象となる容量を計算すると、 $1 \times 800 \text{ GB} = 0.8 \text{ TB}$ 。

304 ページの図 5-5 に示されている状況では、1 TB のダイレクト・バックアップ使用権 1 つ、1 TB のゼロ・ダウンタイム・バックアップ使用権 1 つ、および、1 TB のインスタント・リカバリ使用権 1 つが必要です。

図 5-5 **ダイレクト バックアップ セッション**



例 5

この ZDB セッションでは、200 GB の論理ユニットが 1 つ、500 GB の論理ユニットが 1 つ、120 GB の論理ユニットが 1 つ、300 GB の論理ユニットが 1 つ使用されます。

1 TB のゼロ・ダウンタイム・バックアップ使用権の対象となる容量を計算すると、 $1 \times 200 \text{ GB} + 1 \times 500 \text{ GB} + 1 \times 120 \text{ GB} + 1 \times 300 \text{ GB} = 1.12 \text{ TB}$ 。

200 GB の論理ユニット 1 つ、120 GB の論理ユニット 1 つ、300 GB の論理ユニット 1 つのスプリット ミラーまたはスナップショット コピーが、インスタント リカバリの目的で保存されます。

1 TB のインスタント・リカバリ使用権の対象となる容量を計算すると、 $1 \times 200 \text{ GB} + 1 \times 120 \text{ GB} + 1 \times 300 \text{ GB} = 0.62 \text{ TB}$ 。

ダイレクト バックアップ セッションでは、300 GB の論理ユニット 1 つを使用します。

1 TB のゼロ・ダウンタイム・バックアップ使用権の対象となる容量を計算すると、 $1 \times 300 \text{ GB} = 0.3 \text{ TB}$ 。

5-2 ~ 5-6 の例では、1 TB のダイレクト・バックアップ使用権 1 つ、1 TB のゼロ・ダウンタイム・バックアップ使用権 2 つ、および 1 TB のインスタント・リカバリ使用権 1 つが必要です。

必要に応じたライセンス レポートの作成

ライセンス レポートを作成するには、Data Protector の omnicc コマンドを使用します。以下のよう
にコマンドを実行します。

```
omnicc -check_licenses [-detail]
```

-detail オプションが指定されなかった場合、Data Protector ライセンスが存在するかどうかを示
す情報が返されます。

-detail オプションが指定された場合、詳細レポートが作成されます。セル内の各ライセンスに
ついて、ライセンス名、インストールされているライセンス、使用されているライセンス、必要
なライセンスに関する情報が返されます。

詳細は omnicc のマンページを参照してください。このコマンドでは、ライセンスの期限切れ日
付は表示されないことに注意してください。インストールされている環境とライセンス数によ
り、レポートの生成に時間を要する場合があります。ライセンスの期限切れ日付の情報を表示す
る場合は、以下のコマンドを入力します。

```
omnicc -password_info
```

重要

CMMDB が構成された MoM 環境で、ライブラリとドライブのライセンスの対象
となる製品のライセンス レポートを作成する場合は、CMMDB がインストールさ
れた Cell Manager で、omnicc コマンドを実行する必要があります。

購入可能なライセンス

以下の表には、本製品で使用できるライセンスを示します。各製品番号の詳細は、本書の付録 A を参照してください。

図 5-6 HP OpenView Storage Data Protector の製品構成

1. スターター パック (必須)	すべてのプラットフォーム	Windows	Linux	HP-UX	Solaris
LTU & DVD: 1x 管理システム スターター パック マニュアル - ハードコピー	B6960LA	B6961AA	B6961DA	B6951AA	B6951DA
LTU のみ 1x 管理システム		B6961BA	B6961CA	B6951BA	B6951CA
DVD セット DVD 2枚同梱	B6960MA				
CD セット (DVD セットを推奨) CD 15枚同梱	B6960MB				
2. ドライブ & ライブラリの使用権	すべてのプラットフォーム	Windows, NetWare, Linux		SAN, UNIX, NAS	
ドライブ LTU 1x ドライブ		B6963AA		B6953AA	
ライブラリ LTU 1x 61-250/無制限スロット 1x アップグレード~無制限スロット	B6957BA/B6958BA B6958CA				
3. 機能拡張使用権	すべてのプラットフォーム	WindowsおよびLinux		UNIX	
機能拡張使用権 マニュアル - ハードコピー	B6960EA				
オンライン バックアップ LTU 1x システム		B6965BA		B6955BA	
マネージャ オブ マネージャ LTU 1x システム		B6966AA		B6956AA	
アドバンスド バックアップ LTU 1x TB/10x TB/100x TB	B7038AA/BA/CA				
オープンファイル バックアップ LTU 1x Enterprise Server	BA155AA				
	1x サーバ/1xサーバ10台				
	5x ワークステーション				
	CD のみ				
メディア操作 LTU 1x 2,000/10,000 メディア	B7100AA/B7101AA				
	1x 無制限のメディア				
	CD のみ/マニュアルのみ				
		NDMP			
ゼロ デウンタイム バックアップ LTU 1x TB / 10x TB		HP XP	HP EVA	EMC	
インスタント リカバリ LTU 1x TB / 10x TB		B7023CA/DA	B7025CA/DA	B6959CA/DA	
ダイレクト バックアップ LTU 1x TB / 10x TB	B7022BA/DA	B7026CA/DA	B7028AA/DA		
		B7027AA/DA			
シングルサーバ版		Windows	HP-UX	Solaris	
LTUおよびメディア/ LTU のみ		B7030AA/BA	B7020AA/BA	B7020DA/CA	
スターター パックへの移行		B7031AA	B7021AA	B7021DA	

表内の赤字は新製品の番号を表します。

Data Protector は以前の Data Protector バージョンの製品番号を継承しています。これにより、移行後も既存の Data Protector ライセンスを引き続き使用できます。使用可能なライセンスの詳細は、A-2 ページの「Data Protector A.06.00 の製品構成とライセンス」を参照してください。

パスワードについて

以下の項目を参照して、適切な数のパスワードを取得してください。

- 一時パスワードは、Cell Manager システムとしての使用を予定している任意のシステムで使用できます。ただしその他のタイプのパスワードについては、対応するプラットフォームをまず決定しなければなりません。この中には、Data Protector の集中管理用システムとなる Cell Manager も含まれます。そのため、恒久パスワードを請求する前に、一時パスワードを使用してセル構成の必要条件を十分に把握しておくことが大切です。
- 恒久ライセンスは、他の Cell Manager に移動できます。移動にあたっては、*HP Password Delivery Center (PDC)* の電話相談窓口にご連絡ください。
- パスワードは Cell Manager にインストールされ、セル全体に対して有効です。
- Manager-of-Managers (MoM) 機能を使用すると、集中ライセンスが可能です。複数のセルに対して複数のライセンスを購入すると、すべてのライセンスが MoM システムにインストールできます。
- 各セルごとに、Cell Manager ライセンスが 1 つ必要です。
- Data Protector の構成作業やバックアップセッションを開始するたびに、ソフトウェアによってライセンスが定期的にチェックされます。
- 一時パスワードは任意のシステムで使用できますが、評価用パスワードと恒久パスワードはライセンス請求時に指定した Cell Manager に対してのみ使用できます。
- 複数の IP アドレスを持つシステム (複数アドレスを持つシステム、RAS サーバ、クラスタ) に Cell Manager がインストールされている場合は、ライセンスをこれらの IP アドレスのどれにでもバインドさせることができます。

注記

Cell Manager の IP アドレスを変更する、Cell Manager を別のシステムに移動する、MoM 機能を使用せずにライセンスを別のセルに移動するなどの変更を行う場合は、ライセンスの更新が必要になりますので、*HP パスワード デリバリー センター (PDC)* にご連絡ください。HP パスワード デリバリー センターへの連絡の詳細は、311 ページの「恒久パスワードの取得とインストールのためのその他の方法」を参照してください。

Data Protector のパスワード

Data Protector 製品をインストールすると、60 日間使用できます。この期間を過ぎてからソフトウェアを使用するには、Cell Manager に恒久パスワードをインストールする必要があります。Data Protector の Cell Manager にソフトウェアをロードすることは可能ですが、恒久パスワードがなければ、構成作業を実施できません。特定の Data Protector 機能を使用するにはライセンスが必要で、ライセンスを有効にするにはパスワードが必要です。

Data Protector のライセンスには、以下のパスワードのいずれか 1 つが必要です。

✓ 一時パスワード

一時パスワードは、初回にインストールされた時点で製品に含まれています。Data Protector がサポートしているシステムに製品をインストールすると、60 日間ソフトウェアを使用できます。この期間内に *HP Password Delivery Center* から恒久パスワードを取得して、インストールする必要があります。

✓ 恒久パスワード

Data Protector 製品には、恒久パスワードを取得する権利を保証するライセンス権利証書 (*License Entitlement Certificate*) が付属しています。恒久パスワードを使用すると、ユーザーのバックアップ方針に応じて Data Protector セルを構成できます。ただし、必要な数のライセンスを購入する必要があります。恒久パスワードを請求する前に、どのシステムに Cell Manager をインストールするかを決定するとともに、セル構成の必要条件を把握しておく必要があります。

✓ 緊急用パスワード

現在インストールされているパスワードが、突発的な事態によって現在のシステム構成にあわなくなった場合は、緊急用つまり代替のパスワードを使用できます。緊急用パスワードは、どのシステム上でも使用可能で、120 日間使用できます。

緊急用パスワードは、当社サポートグループが発行します。これらのパスワードは当社社員にしか請求できず、当社社員に対して発行されます。詳細は、サポート担当部署または下記の HP Licensing サイトまでお問い合わせください。

<http://webware.hp.com>

緊急パスワードは、元のシステムを再構成したり別の場所に移動させて恒久パスワードをインストールするまでの間、バックアップ操作を可能にする目的で設定されています。ライセンスを移動する場合は、*HP Password Delivery Center* の電話相談窓口までご連絡ください。また Web ページ <http://webware.hp.com> でもパスワードの生成や移動が可能です。

パスワードの取得には *HP OpenView AutoPass* ユーティリティを使用することをお勧めします。このユーティリティは *Cell Manager* のインストールプロセス中にインストールできます。*Cell Manager* のインストールプロセス中に *HP OpenView AutoPass* ユーティリティをインストールした後、そのユーティリティを使用してパスワードを取得する方法は、309 ページの「*HP OpenView AutoPass* ユーティリティを使用した恒久パスワードの取得と インストール」を参照してください。

HP OpenView AutoPass ユーティリティ以外の手段でパスワードを取得し、インストールする方法については、311 ページの「恒久パスワードの取得とインストールのためのその他の方法」を参照してください。

HP OpenView AutoPass ユーティリティを使用した恒久パスワードの取得とインストール

HP OpenView AutoPass ユーティリティを使用すると、HP パスワード デリバリー センタの Web サーバから *HP OpenView* 製品の購入済みライセンスのパスワードをインターネット経由で直接インストールできます。*HP OpenView AutoPass* ユーティリティの詳細は、『*HP OpenView AutoPass Licensing Guide*』を参照してください。

前提条件

HP OpenView AutoPass ユーティリティを使用して恒久パスワードの取得とインストールを行うには、以下の条件を満たす必要があります。

- *Data Protector* の `omnisetup.sh` スクリプトを使用した *Cell Manager* のインストール中 (UNIX システムの場合) か、*Cell Manager* のインストール中 (Windows システムの場合) に、*HP OpenView AutoPass* ユーティリティをインストールする必要があります。
- *MC/ServiceGuard* では、*HP OpenView AutoPass* ユーティリティをすべてのノードにインストールする必要があります。
- 恒久ライセンス権利証書が必要です。
- 購入済みのライセンスの HP 注文番号が必要です。
- *Cell Manager* か *Manager-of-Managers* の IP アドレスが必要です。

制限事項

HP OpenView AutoPass については、以下の制限に留意してください。

- *HP OpenView AutoPass* ユーティリティは、x64 以外の Windows オペレーティング システムおよび Linux オペレーティング システムにはインストールできません。

Data Protector のライセンス

Data Protector のパスワード

- Microsoft Cluster に HP OpenView AutoPass ユーティリティをインストールすることは推奨できません。なぜなら、このユーティリティは、1つのノードのみにインストールされ、すべてのノードにはインストールされないからです。

これ以外の前提条件や制限は、『HP OpenView AutoPass Licensing Guide』を参照してください。

パスワードは Cell Manager にインストールされ、セル全体に対して有効です。

手順

恒久パスワードを取得し、インストールするには、以下の手順に従ってください。

1. 恒久パスワードを取得するのに必要な情報を収集します。必要な情報は、『HP OpenView AutoPass Licensing Guide』を参照してください。
2. *HP OpenView AutoPass* ユーティリティを使用してパスワードをオンラインで注文します。*HP OpenView AutoPass* ユーティリティを起動するには、Cell Manager で以下のコマンドを実行します。

注記

Manager-of-Managers (MoM) 環境では、MoM システム上 (Data Protector の集中ライセンスを使用する場合)、またはパスワードが注文されインストールされる Cell Manager 上 (Data Protector の集中ライセンスを使用しない場合) で、`omniinstlic` コマンドを実行する必要があります。

`/opt/omni/sbin/omniinstlic` (UNIX 用 Cell Manager の場合)、または、
`<Data_Protector_home>%bin%omniinstlic` (Windows 用 Cell Manager の場合)
`omniinstlic` コマンドの詳細は、このコマンドのマニュアルページを参照してください。

3. *HP OpenView AutoPass* ユーティリティのウィザードに従い、必要な情報を入力します。
ウィザードの手順の最後で [Get password] をクリックすると、*HP Password Delivery Center* から Cell Manager に、購入したライセンスの恒久パスワードが転送されます。
[Finish] をクリックすると、購入したライセンスの恒久パスワードが、Cell Manager にインストールされます。
4. インストールされたパスワードを確認する方法は、313 ページの「パスワードの検証」を参照してください。

恒久パスワードの取得とインストールのためのその他の方法

取得

恒久パスワードを取得するには、以下の手順に従ってください。

1. *Permanent Password Request Form* に記入する情報を収集しておきます。このフォームの場所と記入方法は、A-25 ページの「Data Protector ライセンス フォーム」を参照してください。
2. 製品構成の詳細は、A-2 ページの「Data Protector A.06.00 の製品構成とライセンス」を参照してください。*HP Password Delivery Center* では、申請時と同じ方法で恒久パスワードをユーザーに通知します。たとえば、電子メールによる申請に対しては、恒久パスワードを電子メールでお知らせします。
3. 以下のいずれかの操作を行います。
 - オンラインの *HP Password Delivery Center* サイト (<http://www.webware.hp.com>) にアクセスします。
 - *Permanent Password Request Form* に必要事項を記入して、以下のいずれかの方法で *HP Password Delivery Center* に送信します。デリバリ センターのファックス番号、電話番号、電子メール アドレス、および営業時間については、製品に付属する権利保証書 (Entitlement Certificate) を参照してください。
 - フォームを *HP Password Delivery Center* にファックスで送付します。
 - *HP Password Delivery Center* に電子メールとして送信します。

以下の名前のファイルにデータとして含まれているライセンス フォームも使用できます。このファイルは Cell Manager または配布メディアに含まれています。

- Windows 上 : <Data_Protector_home>%Docs%license_forms.txt
- Windows 用 DVD-ROM 上 : <Disk_Label>:%Docs%license_forms.txt
- UNIX 上 : /opt/omni/doc/C/license_forms_UNIX

このファイルからコピーしてフォームを作成し、*HP Password Delivery Center (HP PDC)* にお送りください。

通常は、*Permanent Password Request Form* をお送りいただいてから 24 時間以内に、恒久パスワードをお届けします。

インストール

HP Password Delivery Center (HP PDC) から通知された恒久パスワードをインストールする方法は、以下のとおりです。

前提条件

HP Password Delivery Center から恒久パスワードを取得する必要があります。恒久パスワードをインストールするには、Cell Manager 上に Data Protector ユーザー インタフェースをインストールしておく必要があります。恒久パスワードは Cell Manager にインストールします。インストールされたパスワードは、セル全体に対して有効です。

GUI の使用

Data Protector GUI を使用して恒久パスワードをインストールするには、以下の手順に従ってください。

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 ペインの [Data Protector セル] をマウスの右ボタンでクリックし、[ライセンスの追加] を選択します。
3. パスワード証明書に示されているとおりにパスワードを入力します。

パスワードは、スペースで区切られた 4 文字のグループが 8 個と、それに続く文字列で構成されています。パスワードの途中に LF などの改行記号を入れないようにしてください。以下にパスワードの例を示します。

```
4PXV EG9S B6WS 2VX3 5967 XEZK AAA9 MQJB "Product: B6965BA"
```

パスワードを入力し終えたら、以下のチェックを行ってください。

- ✓ 画面上のパスワードが正しいことを確認します。
- ✓ パスワードの前後にスペースがなく、また余分な文字が含まれていないことを確認します。
- ✓ 数字の "1" と小文字の "l" を混同していないことを確認します。
- ✓ 大文字の "O" と数字の "0" を混同していないことを確認します。
- ✓ 大文字と小文字を正しく入力していることを確認します。パスワードでは、大文字と小文字が区別されます。

[OK] をクリックします。

以下のファイルにパスワードが書き込まれます。

- Windows の場合 : <Data_Protector_home>%Config%server%Cell%lic.dat
- UNIX の場合 : /etc/opt/omni/server/cell/lic.dat

CLI の使用

Data Protector CLI を使用して恒久パスワードをインストールするには、以下の手順に従ってください。

1. Cell Manager にログオンします。
2. 以下のコマンドを実行します。

- Windows の場合 :
 <Data_Protector_home>%bin%omnicc -install_license <password>
- UNIX の場合 :
 /opt/omni/bin/omnicc -install_license <password>

<password> には、パスワードを入力します。Password Certificate に記載されているとおりに入力する必要があります。

パスワードを以下のファイルに追加することもできます。

- Windows の場合 : <Data_Protector_home>%config%server%cell%lic.dat
- UNIX の場合 : /etc/opt/omni/server/cell/lic.dat

ファイルが存在しない場合は、vi またはメモ帳などのエディタで作成してください。パスワードの例については、上記の GUI の使用の手順 3 を参照してください。

パスワードの検証

GUI の使用

インストールしたライセンスのパスワードが正しいかどうかを検証するには、Data Protector Manager 上で以下の手順を行います。

1. [ヘルプ] メニューで [情報...] をクリックします。
2. [ライセンス] タブをクリックします。インストール済みのすべてのライセンスが表示されます。入力したパスワードが正しくない場合は、「パスワードをデコードできませんでした。」という注釈が付きます。

Data Protector のライセンス Data Protector のパスワード

CLI の使用

インストールしたライセンスのパスワードが正しいかどうかを検証するには、以下の手順を行います。

- Windows の場合：
`<Data_Protector_home>%bin%omnicc -password_info`
- UNIX の場合：`/opt/omni/bin/omnicc -password_info`

コマンドを実行すると、インストール済みのすべてのライセンスが表示されます。入力したパスワードが正しくない場合は、「パスワードをデコードできませんでした。」という注釈が付きます。

インストール済みライセンスの数を調べる

GUI の使用

恒久パスワードのインストール後、Cell Manager 上に現在インストールされているライセンスの数をチェックできます。

1. Data Protector Manager を起動します。
2. メニューバーから、[ヘルプ]、[情報...] をクリックします。[Data Protector Manager について] ウィンドウに、現在インストールされているライセンスが表示されます。

CLI の使用

コマンド行を使用する場合は、以下の手順に従ってください。

1. Cell Manager にログオンします。
2. 以下のコマンドを実行します。
 - Windows の場合：`<Data_Protector_home>%bin%omnicc -query`
 - UNIX の場合：`/opt/omni/bin/omnicc -query`

現在インストールされているライセンスのリストが表示されます。

他の Cell Manager システムへのライセンスの移動

以下のような場合は、*HP Password Delivery Center* にご連絡ください。

- Cell Manager を他のシステムに移動したい場合。

- Cell Manager にインストールされているライセンスのうち、セル内で現在使用していないライセンスを他の Data Protector セルに移動したい場合。

注記 UNIX ライセンスを別の UNIX 用 Cell Manager または Windows 用 Cell Manager に移動することは可能ですが、Windows ライセンスを UNIX 用 Cell Manager に移動することはできません。

ライセンスを Cell Manager 間で移動するには、以下の手順を行います。

1. 新しい Cell Manager のそれぞれにつき、ライセンス移動フォーム (*License Move Form*) が 1 つずつ必要です。フォームに必要事項を記入し、*HP Password Delivery Center* に送付してください。販売終了となった製品のライセンスを移動する場合は、以前のバージョンの製品に付属のライセンス移動フォーム (*License Move Forms*) を使用してください。詳細は A-25 ページの「Data Protector ライセンス フォーム」を参照してください。

フォームには、既存の Cell Manager から移動するライセンスの数を指定する必要があります。

2. 以下のファイルを削除します。

- Windows の場合： <Data_Protector_home>%config%server%cell%lic.dat
- UNIX の場合： /etc/opt/omni/server/cell/lic.dat

3. ライセンス移動フォーム (*License Move Form*) に必要事項を記入し、*HP Password Delivery Center* に送付した後は、移動元の Cell Manager から Data Protector のパスワードをすべて削除してください。
4. 新しいパスワードをインストールします。移動先の各 Cell Manager に対応するパスワードが *HP Password Delivery Center* から提供されます。移動元の Cell Manager 上にライセンスを残す場合は、移動元の Cell Manager 用の新しいパスワードが 1 つ提供されます。この新しいパスワードは、これ以降、移動元の Cell Manager にログオンするときに必要になります。

集中ライセンス

Data Protector では、複数セル環境全体に対して集中ライセンスを構成できます。これによってライセンス管理を単純化できます。すべてのライセンスは Manager-of-Managers (MoM) Manager システムに保持されます。必要に応じてライセンスは特定のセルに割り当てられますが、ライセンス自体は MoM Manager に構成されています。

ライセンスの構成方法の詳細は、Data Protector オンライン ヘルプを参照してください。

注記 UNIX ライセンスを別の UNIX 用 Cell Manager または Windows 用 Cell Manager に割り当てることは可能ですが、Windows ライセンスを UNIX 用 Cell Manager に割り当てることはできません。

MoM 機能を使用すると、MoM セル間でライセンスを移動 (再配布) できます。詳細はオンライン ヘルプの索引キーワード「MoM 環境」で表示される内容を参照してください。

新しい Data Protector ライセンスをインストールする場合は、MoM 機能を使用するかどうかを決めてからライセンスを請求してください。ライセンスの請求後に集中ライセンスの使用を決定した場合は、ライセンス移動の手続きが必要になります。

注記 MoM 機能を使うと、集中ライセンスを行えます。つまりライセンスを MoM Manager にインストールしておき、MoM セルに所属する複数の Cell Manager に、それらのライセンスを配布することができます。配布したライセンスは、MoM セル間で移動 (再配布) できます。詳細はオンライン ヘルプの索引キーワード「MoM 環境」で表示される内容を参照してください。

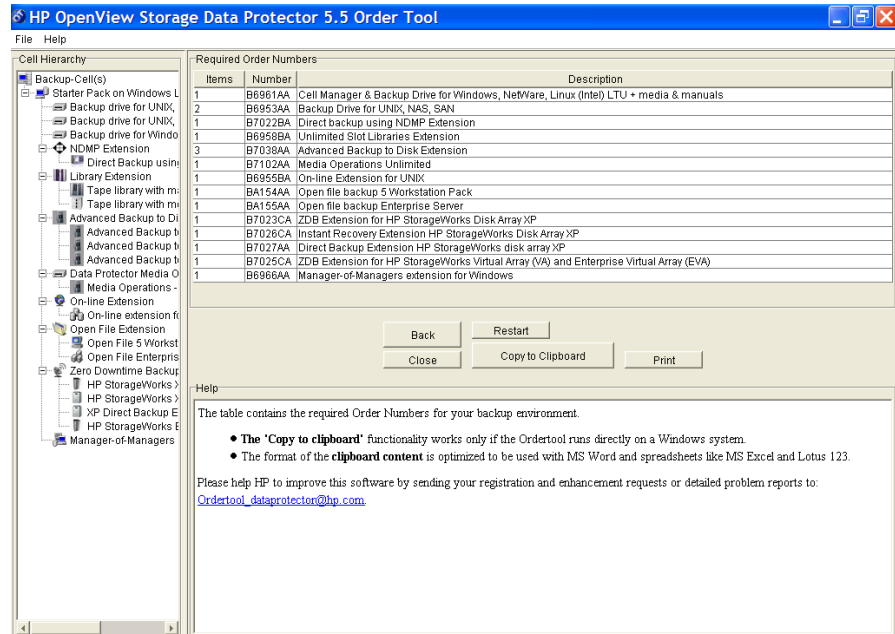
Data Protector Order Tool

Data Protector は、お客様の環境に必要な Data Protector 製品番号の一覧を自動生成するシンプルなツールを備えています。Data Protector Order Tool を起動してシステム構成と使用目的に関する一連の簡単な質問に答えていくと、回答を反映したセル構造が画面上に表示されていきます。

Order Tool のすべての質問に答えると、お客様の環境に必要な製品番号の一覧が示されます。317 ページの図 5-7 に例を示します。

Order Tool は Data Protector DVD に収録されています。

図 5-7 Data Protector Order Tool の例



6 インストールのトラブルシューティング

この章の内容

この章では、インストール時に発生しがちな問題、その原因、および解決方法を述べます。一般的なトラブルシューティング情報については、『HP OpenView Storage Data Protector トラブルシューティング ガイド』を参照してください。

この章には、以下に関する情報が記載されています。

- 321 ページの「Windows 用 Cell Manager インストール時の名前解決に関する問題」
- 322 ページの「Data Protector セル内の DNS 接続の確認」
- 325 ページの「Windows 上での Data Protector のインストールとアップグレード」
- 327 ページの「Solaris 上での Data Protector Cell Manager のインストールに関する問題のトラブルシューティング」
- 328 ページの「UNIX クライアントのインストールに関する問題のトラブルシューティング」
- 330 ページの「Data Protector クライアントのインストール結果の確認」
- 331 ページの「アップグレードのトラブルシューティング」
- 333 ページの「ログファイルの使用」
- 336 ページの「インストール実行トレースの作成」

Windows 用 Cell Manager インストール時の名前解決に関する問題

DNS や LMHOSTS ファイルに必要な設定を行わずに Data Protector Cell Manager を Windows にインストールした場合、Data Protector は問題を検出し、警告します。また、TCP/IP プロトコルがシステムにインストールされていない場合も、Data Protector によって通知されます。

問題

DNS または LMHOSTS の使用時に名前解決に失敗する

名前解決に失敗すると、「error expanding hostname」のメッセージが表示され、インストールが中止されます。

- DNS を使用しているときに名前解決の問題が生じた場合、使用している DNS 構成に関する警告メッセージが表示されます。
- LMHOSTS ファイルを使用しているときに名前解決の問題が生じた場合、LMHOSTS ファイルの構成のチェックを促す警告メッセージが表示されます。
- DNS と LMHOSTS のいずれも構成されていない場合は、TCP/IP のプロパティダイアログで DNS または LMHOSTS の名前解決を有効にするよう、警告メッセージが表示されます。

対応策

DNS ファイルまたは LMHOSTS ファイルの構成をチェックするか、アクティブにします。322 ページの「Data Protector セル内の DNS 接続の確認」を参照してください。

問題

TCP/IP プロトコルがシステム上にインストールおよび構成されていない

Data Protector では、TCP/IP プロトコルを使ってネットワーク通信が行われます。したがって、セル内の各クライアントに TCP/IP プロトコルをインストールし、正しく構成しておく必要があります。先に正しく構成しておかないと、インストールが中止されます。

対応策

TCP/IP 設定をチェックします。B-19 ページの「Windows システム上の TCP/IP プロトコルのセットアップ」を参照してください。

Data Protector セル内の DNS 接続の確認

DNS (Domain Name System) は、TCP/IP ホストのためのネーム サービスです。DNS はホスト名と IP アドレスの一覧で構成されており、ユーザーはリモート システムを IP アドレスではなくホスト名で指定することができます。DNS により、Data Protector セル メンバー間の適切な通信が確実に行われます。

DNS が正しく構成されていないと、Data Protector セル内で名前解決に関する問題が発生し、メンバー相互の通信ができなくなります。

Data Protector は、Data Protector セル メンバー間の DNS 接続を確認するための `omnicheck` コマンドを備えています。このコマンドでセル内のすべての接続を確認できますが、Data Protector セル内で極めて重要な接続である以下の接続を確認すれば十分です。

- Cell Manager から他のいずれかのセル メンバーへの接続、およびその逆。
- Media Agent から他のいずれかのセル メンバーへの接続、およびその逆。

omnicheck コマンドの使用

制限事項

- このコマンドでは、セル メンバー間の接続確認のみが行われます。一般的な DNS 接続の確認は行われません。
- Data Protector A.05.10 以降の Data Protector クライアントでのみ使用可能です。旧バージョンの Data Protector クライアントがあった場合にはエラー メッセージが表示され、コマンドは次のクライアントに対して処理を続行します。

`omnicheck` コマンドは、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>\bin`

UNIX の場合: `/opt/omni/bin`

`omnicheck` コマンドの使用方法は以下のとおりです。

```
omnicheck -dns [-host Client | -full] [-verbose]
```

さまざまなオプションを使用して、Data Protector セル内で以下に示す DNS 接続を確認できます。

- Cell Manager やセル内の各 Media Agent から、セル内の各 Data Protector クライアントへの DNS 接続 (またはその逆) が正しく名前解決されているかを確認するには、次のコマンドを実行します。

```
omnicheck -dns [-verbose]
```

- 特定の Data Protector クライアントからセル内の各 Data Protector クライアントへの DNS 接続 (またはその逆) が正しく名前解決されているかを確認するには、次のコマンドを実行します。

```
omnicheck -dns -host <client> [-verbose]
```

<client> には、確認対象の Data Protector クライアントの名前を指定します。

- セル内のすべての DNS 接続をチェックするには、次のコマンドを実行します。

```
omnicheck -dns -full [-verbose]
```

[-verbose] オプションを指定すると、コマンドはすべてのメッセージを表示します。このオプションを指定しない場合 (デフォルト) は、確認に失敗した結果を示すメッセージのみを表示します。

詳細は、omnicheck マンページを参照してください。

表 6-1 に omnicheck コマンドの出力メッセージ一覧を示します。DNS の名前解決に問題があることを示す出力メッセージが表示された場合は、『HP OpenView Storage Data Protector トラブルシューティング ガイド』の「ネットワークと通信のトラブルシューティング」の項を参照してください。

表 6-1 出力メッセージ

出力メッセージ	意味
<i>client_1</i> が <i>client_2</i> に接続できません。	<i>client_2</i> への接続がタイムアウトしました。
<i>client_1</i> は <i>client_2</i> に接続していますが接続先のシステムは <i>client_3</i> として存在しています。	<i>client_1</i> の <%SystemRoot%>%System32%drivers%etc%hosts ファイル (Windows システムの場合) または /etc/hosts ファイル (UNIX システムの場合) が正しく構成されていないか、 <i>client_2</i> のホスト名が DNS 名と一致していません。

表 6-1 出力メッセージ (続き)

出力メッセージ	意味
<i>client_1</i> から <i>client_2</i> に接続できません	<i>client_2</i> がアクセス不能 (接続されていないなど) か、 <i>client_1</i> の <code><%SystemRoot%>%System32%drivers%etc%hosts</code> ファイル (Windows システムの場合) または <code>/etc/hosts</code> ファイル (UNIX システムの場合) が正しく構成されていません。
<i>client_1</i> と <i>client_2</i> の接続をチェック中	
すべてのチェックが正常に完了しました。	
<i>number_of_failed_checks</i> のチェックが失敗しました。	
<i>client</i> はこのセルのメンバではありません。	
<i>client</i> は旧バージョンの Data Protector を実行しているようです。 <i>hostname</i> は解決されていますが、検証されていません。	

Windows 上での Data Protector のインストールとアップグレード

問題

以下のいずれかのエラー メッセージが表示されることがあります。

- Windows Installer サービスにアクセスできませんでした。
- このアプリケーションを実行するには、インストールを行ってください。
- パッチ パッケージをオープンできませんでした。
- システムは指定されたデバイスまたはファイルをオープンできませんでした。

Data Protector A.06.00 のインストールまたはアップグレード後、Windows が、一部のアプリケーションについて、インストールされていない、または再インストールが必要だというメッセージを出力することがあります。

原因は、Microsoft Installer のアップグレード処理におけるエラーです。Microsoft Installer バージョン 1.x のデータ情報は、Data Protector のインストールを行う Microsoft Installer バージョン 2.x には移行されません。

対応策

この問題の解決方法については、Microsoft Knowledge Base のアーティクル Q324906 を参照してください。

問題

いずれの Windows ドメインにも所属していない Windows システムへの Cell Manager のインストールに失敗する

以下のエラー メッセージが表示されます。

Setup is unable to match the password with the given account name. (入力されたアカウント名とパスワードが一致しません。)

対応策

以下の 2 通りの対応策があります。

- Cell Manager をインストールしようとしている Windows システムをドメインに参加させます。
- CRS サービス用のローカル管理者アカウントを使用します。

問題

以下のエラー メッセージが表示されます。

```
msvcr71.dll file is not found (msvcr71.dll ファイルが見つかりません。)
```

MSVCR71.dll ライブラリ (大文字) を検出できません。これは、ネットワーク共有上に msvcr71.dll (小文字) しかないためです。MSVCR71.dll と msvcr71.dll は同一ファイルとはみなされないため、setup.exe は適切な dll ファイルの検出に失敗します。

対応策

ファイル名を msvcr71.dll (小文字) から MSCVCR71.dll (大文字) に変更するか、または、大文字と小文字を区別しないようにネットワーク共有を構成し直します。

Windows クライアントのリモート インストールに関する問題

問題

セットアッププロセスの起動エラー

Data Protector のリモート インストール機能で Windows クライアントをアップグレードしようとしたときに、次のようなエラーが表示されることがあります。

```
Error starting setup process, err=[1326] Logon failure: unknown user name or bad password.
```

この問題は、インストール サーバ上の OmniBack II 共有へのアクセス権が付与されていないユーザー 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場合に発生します。ローカル ユーザー アカウントが使用されている場合に発生するのが典型的です。

対応策

Data Protector Inet サービスのユーザーを Data Protector 共有へのアクセス権があるユーザーに変更します。

Solaris 上での Data Protector Cell Manager のインストールに関する問題のトラブルシューティング

問題

一時ディレクトリを作成できない

Solaris システムへの Cell Manager のインストール中に一時ディレクトリが作成できないと、以下のメッセージを出力されてインストールが失敗することがあります。

```
Processing package instance <OB2-CORE> from </tmp/DP_A0510_158_SUN78.pkg>  
pkgadd: ERROR: unable to make temporary directory <>//tmp/old//installR.a0j3>
```

対応策

エラー メッセージで示された位置に手作業で一時ディレクトリを作成し、インストール手順を初めからやり直してください。

たとえば、上記のエラー メッセージが出力された場合は、//tmp/old//installR.a0j3 ディレクトリを作成します。

UNIX クライアントのインストールに関する問題のトラブルシューティング

問題

UNIX クライアントのリモート インストールが失敗する

UNIX クライアントのリモート インストールまたはリモート アップグレードが、以下のエラーメッセージで失敗することがあります。

```
Installation/Upgrade session finished with errors.
```

UNIX クライアントをリモートでインストールまたはアップグレードする場合、クライアント システム上の /tmp ディレクトリ下で使用可能なディスク スペースが、インストール対象のパッケージのうち最大のもので、少なくとも同じ大きさである必要があります。Solaris クライアント システム上では、/var/tmp ディレクトリ下でも、同じ容量のディスク スペースが使用可能でなければなりません。

対応策

上記のディレクトリ下に十分なディスク スペースがあるか確認して、インストールまたはアップグレード手順を初めからやり直してください。

ディスク スペース要件は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照してください。

問題

HP-UX クライアントのインストールに関する問題

Data Protector セルに新しい HP-UX クライアントを追加した場合に、以下のエラー メッセージが表示されることがあります。

```
/tmp/omni_tmp/packet: you do not have the required permissions to perform this SD function.....
```

```
Access denied to root at to start agent on registered depot  
/tmp/omni_tmp/packet. No insert permission on host.
```

対応策

swagent デーモンを一度停止し、再起動します。このためには一度プロセスを終了してから /opt/omni/sbin/swagentd コマンドを実行するか、または /opt/omni/sbin/swagentd -r コマンドを実行します。

hosts ファイル (/etc/hosts) にローカル ホストと loopback のエントリがあることを確認してください。

問題

Unix 用 Cell Manager のインストール後に Omniinet を開始できない

Cell Manager の開始時に、以下のエラー メッセージが表示されることがあります。

```
ERROR:  Cannot start "omniinet" service, system error: [1053] Unknown error
1053. ("omniinet" サービスを起動できません。システム エラー : [1053] 不明なエラー
1053。)
```

対応策

inetd サービスまたは xinetd サービスが実行されているかどうかを確認します。

HP-UX および Solaris の場合: `ps -ef | grep inetd`

Linux の場合: `ps -ef | grep xinetd`

サービスを開始するには、以下のコマンドを実行します。

HP-UX の場合: `/usr/sbin/inetd`

Solaris の場合: `/usr/sbin/inetd -s`

Linux の場合: `rcxinetd start`

Data Protector クライアントのインストール結果の確認

Data Protector クライアントのインストール結果の確認では、以下のチェック作業を行います。

- Cell Manager システムとクライアント システム上の DNS 構成をチェックし、Cell Manager およびクライアント システム上で実行した omnichck -dns コマンドの出力結果がそれぞれのシステムと一致することを確認します。
- ソフトウェア コンポーネントがクライアントにインストールされているかをチェックします。
- インストールするソフトウェア コンポーネントに必要なファイルのリストと、クライアントにインストール済みのファイルとを比較します。
- ソフトウェア コンポーネントに必要なすべての読み取り専用ファイルのチェックサムを確認します。

前提条件

選択したクライアント システムの種類 (UNIX または Windows) に合ったインストール サーバが必要です。

制限事項

この確認手順は、Novell NetWare クライアントおよび MPE クライアントには適用できません。

Data Protector GUI を使って Data Protector のインストール結果を確認する場合は、以下の操作を実行します。

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 ペインの [クライアント] を展開し、Cell Manager システムをマウスの右ボタンでクリックします。次に、[インストールの検証] をクリックしてウィザードを起動します。
3. ウィザードに従って、セルにクライアント システムがインストールされたことを確認します。[インストールの検証] ウィンドウが開き、インストール結果が表示されます。

詳しくは、オンライン ヘルプを参照してください。

インストールが正常に完了しなかった場合は、333 ページの「ログファイルの使用」を参照してください。

UNIX システム上のインストール結果を Data Protector CLI で確認する方法については、ob2install のマンページを参照してください。

アップグレードのトラブルシューティング

問題

アップグレード後に IDB および構成ファイルを使用できない

Cell Manager を旧バージョンからアップグレードした後、IDB とすべての構成ファイルが使用できない場合があります。この問題は、何らかの理由によりアップグレード処理が中断された場合に発生します。

対応策

アップグレード前に作成しておいたバックアップから OmniBack II または Data Protector を復元し、処理の中断となった原因を解消してから、アップグレードを再起動してください。

問題

アップグレード後に古い Data Protector パッチが削除されない

Data Protector のアップグレード完了後に `swlist` コマンドを実行すると、インストールされているプログラムの一覧に古い Data Protector パッチが表示されます。このパッチはアップグレード中にシステムから削除されましたが、`sw` データベースに残されています。

どの Data Protector パッチがインストールされているかを確認する方法は、211 ページの「インストールされている Data Protector パッチの確認」を参照してください。

対応策

`sw` データベースから古いパッチを削除するには、次のコマンドを実行します。

```
swmodify -u <patch>.* <patch>
```

たとえば、`sw` データベースから `PHSS_30143` パッチを削除するには、次のコマンドを実行します。

```
swmodify -u PHSS_30143.* PHSS_30143
```

手作業でのアップグレード手順

通常、UNIX 用 Cell Manager およびインストール サーバ上の Data Protector A.05.00、Data Protector A.05.10、Data Protector A.05.50 をアップグレードするには、自動アップグレード処理を行う `omnisetup.sh` コマンドを使用します。ただし、手作業でアップグレードを行うこともできます。16 ページの「ネイティブ ツールを使用した HP-UX システムと Solaris システムでのアップグレード」を参照してください。

ログファイルの使用

Data Protector のインストール時に問題が発生した場合は、以下の各ログ ファイルの内容をチェックして、どのような問題が発生したかを判断することができます。

- セットアップ ログ ファイル (Windows)
- セットアップ ログ ファイル (UNIX)
- Data Protector ログ ファイル

問題発生時にチェックすべきログ ファイルは、インストールの種類 (ローカルまたはリモート) とオペレーティング システムによって異なります。

ローカル インストール

ローカル インストールに関する問題が発生した場合は、以下のログ ファイルをチェックします。

HP-UX 用 Cell Manager の場合:

- /var/adm/sw/swinstall.log
- /var/adm/sw/swagent.log (詳細情報)

Solaris 用および Linux 用 Cell Manager の場合:

/var/opt/omni/log/debug.log

Windows クライアントの場合 (セットアップが稼動しているシステム):

- <Temp>%OB2SetupLauncher.log
- <System_disk>:%<Temp>%OB2_Setup_ui_<Date>_<Time>.txt
- <Temp>%OB2DBG_<did>__setup_<Host><Debug_no>.txt (詳細情報)

各部分の説明:

- <did> (デバッグ ID) には、デバッグ パラメータを受け取る最初のプロセスのプロセス ID が示されます。この ID はデバッグ セッションの ID として使用されます。残りのすべてのプロセスでも、この ID が使用されます。
- <Host> は、トレース ファイルが作成されたシステムの名前です。
- <Debug_no> は、Data Protector によって生成された番号です。

インストールのトラブルシューティング ログファイルの使用

<Temp>ディレクトリの位置は、環境変数 TEMP で指定されています。この変数の値を調べるには、set コマンドを実行します。

リモート インストール

リモート インストールの実行時に問題が発生した場合は、以下のログ ファイルをチェックします。

UNIX インストール サーバの場合:

/var/opt/omni/log/IS_install.log

Windows クライアントの場合(リモート クライアント システムのみ):

- <Temp>%INSTALL_SERVICE*. *
- <System_disk>:%<Temp>%OB2_Setup_exe_<Date>_<Time>.txt

<Temp>は、環境変数 TEMP で指定されているディレクトリです。

セットアップ ログ ファイルが作成されない場合は、debug オプションを指定してリモート インストールを実行してください。詳細は 336 ページの「インストール実行トレースの作成」を参照してください。

Data Protector ログ ファイル

下記の Data Protector ログ ファイルは、以下の場所に保存されています。

Windows の場合: <Data_Protector_home>%log

HP-UX、Solaris、およびLinux の場合: /var/opt/omni/log または
/var/opt/omni/server/log

その他の UNIX の場合: /usr/omni/log

Novell NetWare の場合: SYS:%USR%OMNI%LOG

インストールのトラブルシューティングに役立つログ ファイルを以下に示します。

debug.log	このファイルには、デバッグ用の情報が記録されます。ユーザーが理解できる情報もありますが、主にサポート部門用の情報が記録されます。
inet.log	Data Protector inet サービスに対して発行された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 インスタンスのトレース情報が記録されます。このファイルは、インストール サーバ上に置かれます。
- omnisv.log Data Protector サービスが開始および停止された日時に関する情報が記録されま
す。
- upgrade.log このログは、アップグレード処理中に作成されます。UCP (アップグレード コ
ア パート) と UDP (アップグレード 詳細パート) のメッセージが記録されま
す。
- OB2_Upgrade.log (UNIX のみ) このログは、アップグレード処理中に作成されます。アップグ
レード処理のトレース情報が記録されます。
- その他のログ ファイルについては、『HP OpenView Storage Data Protector トラブルシューティング
ガイド』を参照してください。

インストール実行トレースの作成

HP カスタマ サポート サービスから依頼があった場合は、debug オプション付きでインストールを実行してください。デバッグの詳細 (下記のデバッグ オプションを含む) および HP カスタマ サポート サービスに送付するデータの作成方法については、『HP OpenView Storage Data Protector トラブルシューティング ガイド』を参照してください。

Windows の場合:

Windows システム上のリモート インストールをデバッグするには、以下に示すように、debug オプション付きで Data Protector GUI を実行します。

```
Manager -debug 1-99 <Debug_postfix>
```

セッションを終了または中止した後で、以下のパスからデバッグ出力を収集します。

- インストール サーバシステムの場合:

```
<Data_Protector_home>%tmp%\OB2DBG_<did>__BM_  
<Installation_Server><Debug_no><Debug_postfix>
```

- リモート システムの場合:

```
<System_disk>:%<Temp>%\OB2DBG_<did>__INSTALL_SERVICE<Host_name><Debug_no><D  
ebug_postfix>
```

UNIX の場合:

UNIX システム上のインストールをデバッグするには、以下に示すように、debug オプション付きで Data Protector GUI を実行します。

```
xomni -debug 1-99 <Debug_postfix>
```

または

```
xomniadmin -debug 1-99 <Debug_postfix>
```

セッションを終了または中止した後で、インストール サーバシステムの tmp ディレクトリからデバッグ出力を収集します。

A 付録 A

Data Protector A.06.00 の製品構成とライセンス

この付録では、Data Protector の製品構成について詳しく説明しており、購入する必要がある製品番号を簡単に特定できます。

製品構成は図 A-1（A-3 ページ）に示すように、いくつかのセクションに分かれています。Data Protector ソリューションは、このセクションに沿って、以下の手順でご注文ください。

1. スターターパックを選択します。適切な製品番号は、Cell Manager システムのオペレーティングシステムによって異なります。
2. 環境内に構成されているドライブの数と、使用するテープ ライブラリを確定します。
3. 必要となるその他の機能を特定します。推奨される機能は、オンラインバックアップからインスタント リカバリまで、個々の環境によってさまざまです。

スターターパック ライセンスとメディアは最低 1 つずつ必要です。

注記 UNIX 製品用に提供されるライセンスは、すべてのオペレーティングシステムに適用できます。

図 A-1 HP OpenView Storage Data Protector 製品構成

1. スターター パック (必須)	すべてのプラットフォーム	Windows	Linux	HP-UX	Solaris
LTU & DVD: スターター パック マニュアル – ハードコピー LTU のみ	1x 管理システム – ハードコピー 1x 管理システム	B6961AA B6961BA	B6961DA B6961CA	B6951AA B6951BA	B6951DA B6951CA
DVD セット CD セット (DVD セットを推奨)	DVD 2枚同梱 CD 15枚同梱	B6960MA B6960MB			
2. ドライブ & ライブラリの使用権	すべてのプラットフォーム	Windows, NetWare, Linux		SAN, UNDX, NAS	
ドライブ LTU ライブラリ LTU	1x ドライブ 1x 61-250/無制限スロット 1x アップグレード~無制限スロット	B6963AA B6957BA/B6958BA B6958CA		B6953AA	
3. 機能拡張使用権	すべてのプラットフォーム	WindowsおよびLinux		UNIX	
機能拡張使用権マニュアル – ハードコピー オンライン バックアップ LTU マネージャ オブ マネージャ LTU	1x システム 1x システム	B6965BA B6966AA		B6955BA B6956AA	
アドバンスド バックアップ LTU オープンファイル バックアップ LTU	1x TB/10x TB/100x TB 1x Enterprise Server 1x サーバ/1xサーバ10台 5x ワークステーション CD のみ	B7038AA/BA/CA BA155AA BA153AA/BA BA154AA BA152AA			
メディア操作 LTU	1x2,000/10,000 メディア 1x 無制限のメディア CD のみ/マニュアルのみ	B7100AA/B7101AA B7102AA B7129AA/B7128AA NDMP			
セコ デウンタイム バックアップ LTU	1x TB / 10x TB	HP XP	HP EVA	EMC	
インスタント リカバリ LTU ダイレクト バックアップ LTU	1x TB / 10x TB 1x TB / 10x TB	B7023CA/DA B7026CA/DA B7027AA/DA	B7025CA/DA B7028AA/DA	B6959CA/DA	
シングルサーバ版		Windows	HP-UX	Solaris	
LTUおよびメディア/ LTUのみ スターター パックへの移行		B7030AA/BA B7031AA	B7020AA/BA B7021AA	B7020DA/CA B7021DA	

表内の赤字は新製品の番号を表します。

スターター パック

表 A-1 は、Data Protector A.06.00 スターター パックのライセンス番号一覧です。

表 A-1 HP OpenView Storage Data Protector スターター パックのライセンス番号

B6951AA	Data Protector セルマネージャ HP-UX (DVD)
B6951BA	Data Protector セルマネージャ HP-UX 使用権のみ
B6951DA	Data Protector セルマネージャ Solaris (DVD)
B6951CA	Data Protector セルマネージャ Solaris 使用権のみ
B6961AA	Data Protector セルマネージャ Windows (DVD)
B6961BA	Data Protector セルマネージャ Windows 使用権のみ
B6961DA	Data Protector セルマネージャ Linux (DVD)
B6961CA	Data Protector セルマネージャ Linux 使用権のみ
B6960MA	Data Protector DVD メディア (日本語版、英語版共通)
B6960LA	Data Protector マニュアル (英語版)
B6960LJ	Data Protector マニュアル (日本語版)
B6960LF	Data Protector Manuals (French) (日本では未販売)

スターターパック使用権 (LTU) では、以下の機能が使用可能になります。

- 特定プラットフォーム上の 1 つの Cell Manager
- 任意のプラットフォーム上の数量無制限の Backup Agent
- 1 台のドライブに対する使用権 (B6951xx は 1xB6953AA、B6961xx は 1xB6963AA を含む)
- 組み込みのメディア管理
- 60 スロット以下のライブラリ

- システム障害復旧オプション
- 高度なレポート機能 (Data Protector GUI および Web から使用)
- SAN サポート (HP-UX 用または Solaris 用の Cell Manager とともに使用)
- HP OpenView との統合によるサービス集中管理

メディア

Data Protector A.06.00 は 2 枚の DVD に収録されています。必要に応じて、15 枚組みの CD セット (B6960MB) もご利用いただけますが、可能であれば DVD セットの使用をお勧めします。

マニュアル

すべてのマニュアルは DVD および CD に電子的な形で収録されているほか、<http://www.hp.com/support/manuals> からもダウンロード可能です。

ご注文いただける印刷版マニュアルには、スターターパックセットと機能拡張セットの 2 種類があります。印刷版スターターパックセットには、以下のマニュアルが含まれます。

- HP OpenView Storage Data Protector コンセプトガイド
- HP OpenView Storage Data Protector インストールおよびライセンスガイド
- HP OpenView Storage Data Protector トラブルシューティングガイド
- HP OpenView Storage Data Protector 障害復旧ガイド
- HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート およびリファレンス

注記 「DVD および LTU」製品番号をご注文いただくと、DVD、LTU、および『HP Data Protector スタートアップガイド』を納めた DVD ケースをお渡しします。その他の印刷版マニュアルは付属しません。マニュアルは DVD に電子的な形で収録されているほか、<http://www.hp.com/support/manuals> からもダウンロード可能です。また、マニュアルのみを別途ご注文いただくことも可能です。

ドライブとライブラリの使用権

以下に示すのは 1 台のドライブに対するライセンスです。任意の時点で同時に使用するドライブの数だけライセンスが必要になります。一般的には、すべてのデバイスを同時に使用できるように、構成されたドライブの総数に等しい数のライセンスが必要です。

付録 A

Data Protector A.06.00 の製品構成とライセンス

バックアップドライブは、テープドライブ、ディスク上の論理ドライブ (ファイル デバイスを使用するディスクへのバックアップ)、または光磁気ドライブのいずれかになります。これらのドライブは Data Protector ライセンスを持つシステムから、ローカルにまたはネットワークを介して、アクセスおよび管理できます。

ドライブのライセンスを複数のセルで共有することはできません。

サポートされているドライブの詳細については、<http://www.hp.com/go/dataprotector> の Specifications の下にある Data Protector の Support Matrices を参照してください。

表 A-2 および表 A-4 は、それぞれ Data Protector A.06.00 のドライブ使用権およびライブラリ使用権に関するライセンス番号の一覧です。

**表 A-2 HP OpenView Storage Data Protector の
ドライブ使用権**

B6953AA	Data Protector 追加ドライブ使用権 UNIX, SAN, NAS
---------	---

UNIX システムまたは NAS デバイスに直接接続されるか、SAN 内で使用されるか、またはサーバレス バックアップに使用される 1 台のバックアップドライブに対する使用権 (LTU) です。

HP MPE システムおよび OpenVMS システムに接続されたドライブには、このライセンスが必要です。

この LTU は以下の場合にも必要です。

NDMP を使用して管理される NAS システム (Network Appliance Filer、EMC Celerra File Server など)、または Data Protector 独自のデバイス サーバ (Media Agent) を必要とする NAS システム (HP Storage Works NAS 8000 など)。

Windows、NetWare、または標準の Linux で動作し、標準の Data Protector デバイス サーバ (Media Agent) を実行できる NAS システムには、Data Protector ドライブ使用権 Windows, NetWare, Linux (B6963AA) のみが必要です。

この LTU を、Windows、NetWare、または Linux システムに接続されたシングルドライブ用に使用することも可能ですが、SAN 内に構成されていないドライブについては、LTU B6963AA を使用の方が低価格です。

**表 A-3 HP OpenView Storage Data Protector の
ドライブ使用権**

B6963AA	Data Protector 追加ドライブ使用権 Windows, NetWare, Linux
---------	--

Windows、NetWare、または Linux (Intel) システムに直接接続された、1 台の追加バックアップドライブに対する使用権 (LTU) です。

このライセンスは、Windows、NetWare、または Linux で動作し、標準の Data Protector Media Agent を実行できる NAS デバイスに接続されたドライブに対して適用できます。

任意の時点で同時に使用するドライブの数だけライセンスが必要になります。一般的には、すべてのデバイスを同時に使用できるように、構成されたドライブの総数に等しい数のライセンスが必要です。

サポートされているドライブの詳細については、<http://www.hp.com/go/dataprotector> の Specifications の下にある Data Protector の Support Matrices を参照してください。

**表 A-4 HP OpenView Storage Data Protector の
ライブラリ使用権**

B6957BA	Data Protector 61-250 スロット ライブラリ使用権
B6958BA	Data Protector スロット数無制限 ライブラリ使用権
B6958CA	Data Protector スロット数無制限ライブラリへのアップグレード

ライブラリ使用権 (LTU) は、1 つの Data Protector セル内でテープ ライブラリを管理するのに必要です。個々のライブラリに 1 つのライセンスが必要になります。

- ACSLSを使用するStorageTekサイロおよびDASを使用するGRAU/EMASSライブラリ システムには、B6958BA が必要です。
- 1 つのライブラリ使用権だけを使って、複数セル間でライブラリを共有するためには、ライブラリを共有する個々のセルにマネージャ オブ マネージャ使用権が必要になります。
- このライセンスは、論理スロットではなく、ライブラリ内の物理スロットに基づいて適用されます。
- 仮想パーティションを作成できるライブラリの場合も、個々の物理ライブラリごとに、物理的に使用可能なスロット数に応じたライセンスが 1 つ必要です。

例:

- 120 スロットのライブラリ 1 台を 1 つのセル内で使用し、2 つの 60 スロット ライブラリにパーティション化する場合は、B6957BA が 1 つ必要です。
- 300 スロットのライブラリ 1 台を (Manager-of-Managers は使用せずに) 3 つのセル間で共有し、各セルがそれぞれ 100 スロットずつ使用する場合は、個々のセルに B6957BA が 1 つずつ必要です。

- 300 スロットのライブラリ 1 台を (Manager-of-Managers は使用せずに) 5 つのセル間で共有し、各セルがそれぞれ 60 スロットずつ使用する場合は、ライブラリ使用権は不要です。
- 300 スロットのライブラリ 1 台を (Manager-of-Managers によるメディアとライセンスの集中管理を使用して) 3 つのセル間で共有し、各セルがそれぞれ 100 スロットずつ使用する場合は、セル全体で B6958BA が 1 つ必要です。

サポートされているライブラリの詳細については、<http://www.hp.com/go/dataprotector> の Specifications の下にある Data Protector の Support Matrices を参照してください。

機能拡張

この項の表には、Data Protector A.06.00 の機能拡張に関するライセンス番号を示します。

**表 A-5 HP OpenView Storage Data Protector
オンライン・バックアップ使用権**

B6955BA	Data Protector オンライン・バックアップ使用権 UNIX
B6965BA	Data Protector オンライン・バックアップ使用権 Windows, Linux

オンライン・バックアップ使用権 (LTU) は、特定プラットフォーム上で実行されるデータベースおよびアプリケーションのオンラインバックアップに必要です。

- システムで複数のパーティションを実行している場合は、パーティションごとにこの LTU が必要です。
- クラスタ環境では、クラスタを構成する個々のシステムにこの LTU が必要です。
- ゼロダウンタイムバックアップ (ZDB) を実行するには、オンライン・バックアップ使用権が必要です。
- Windows 2003 ファイルシステムのスナップショット機能である VSS (Volume Shadow copy Service) は標準でサポートされています。ただし、オペレーティングシステムに含まれないデータベースのオンラインバックアップには、このオンラインバックアップ使用権が必要です。システム構成のバックアップには、オンラインバックアップ使用権は必要ありません。
- Microsoft Exchange のシングルメールボックスのバックアップには、この LTU が必要です。
- HP OpenView Network Node Manager のオンラインバックアップには、この LTU は不要です。

サポートされるデータベースについては、<http://www.hp.com/go/dataprotector> の Specifications の下にある Data Protector の Support Matrices を参照してください。

**表 A-6 HP OpenView Storage Data Protector
オープンファイル バックアップ使用権**

BA153AA	Data Protector オープンファイル・バックアップ 1 サーバ使用権
BA153BA	Data Protector オープンファイル・バックアップ 10 サーバ使用権
BA154AA	Data Protector オープンファイル・バックアップ 5 ワークステーション使用権
BA155AA	Data Protector オープンファイル・バックアップ 1 エンタープライズサーバ使用権
BA152AA	Data Protector オープンファイル・バックアップ メディア

オープンファイルバックアップ使用権 (LTU) は、Data Protector プラットフォームおよび統合マトリクスでカバーされていない、特定サーバ上で実行されるアプリケーション、データベース、電子メール (.pst - Microsoft Outlook ファイルなど) のオープン中のファイルをバックアップするのに必要です。

この CD は、Data Protector のスターター パック DVD に同梱されています。また、BA152AA としてオープンファイルバックアップ CD を個別にご注文いただくことも可能です。

サポートされている構成については、<http://www.hp.com/go/dataprotector> の Specifications の下にある Data Protector の Support Matrices を参照してください。

**表 A-7 HP OpenView Storage Data Protector マ
ネージャ・オブ・マネージャ使用権**

B6956AA	Data Protector マネージャ・オブ・マネージャ使用権 UNIX
B6966AA	Data Protector マネージャ・オブ・マネージャ使用権 Windows

マネージャ・オブ・マネージャ使用権 (LTU) は、ある特定のプラットフォーム上で実行されている個々の Data Protector 管理サーバ (Cell Manager) を Manager-of-Managers 環境に参加させる場合に必要です。

複数の Data Protector セル間でテープ ライブラリを共有する場合も、このライセンスが必要になります。これは支店や営業所のバックアップを集中管理するうえで理想的なソリューションです。

B6956AA を Windows 用 Cell Manager に使用することも可能ですが、B6966AA のほうが低価格です。

**表 A-8 HP OpenView Storage Data Protector
Media Operations 使用権 (日本では未販売)**

B7100AA	Media Operations - Entry Level, for 1 x 2,000 media
B7101AA	Media Operations - Enterprise, for 1 x 10,000 media
B7102AA	Media Operations - for unlimited media
B7128AA	Media Operations - Manuals
B7129AA	Media Operations - Media

- Entry Level には、2000 のメディア、1 つの管理サーバ、および台数無制限のクライアントに対する使用権 (LTU) が含まれます。
- Enterprise Level には、10000 のメディア、1 つの管理サーバ、および台数無制限のクライアントに対する使用権 (LTU) が含まれます。
- Unlimited (無制限のメディア) には、数量無制限のメディア、1 つの管理サーバ、および台数無制限のクライアントに対する使用権 (LTU) が含まれます。

メディアとは、Data Protector Media Operations 内部データベースで追跡するテープ メディアの合計数を指します。実際に追跡するテープ メディアの合計数に応じて、Entry Level および Enterprise Level のライセンスを任意の組み合わせで使用できます。

- Data Protector Media Operations マニュアルは Data Protector 印刷版機能拡張マニュアル セットに含まれていますが、B7128AA として個別にご注文いただくことも可能です。
- Data Protector Media Operations CD は Data Protector スターター パック DVD に含まれていますが、B7129AA として個別にご注文いただくことも可能です。

**表 A-9 HP OpenView Storage Data Protector
アドバンスト・バックアップ使用権**

B7038AA	Data Protector アドバンスト・バックアップ 1TB 使用権
B7038BA	Data Protector アドバンスト・バックアップ 10TB 使用権
B7038CA	Data Protector アドバンスト・バックアップ 100TB 使用権

アドバンスト・バックアップ使用権 (LTU) は、バックアップ ディスクストレージ上の使用可能なネイティブ容量に対する容量ベース (TB) の使用権です。使用バックアップ ディスクストレージとは、Data Protector の内部データベースに従って保護されているバックアップ (コピーおよびミラーを含む) により占有されるスペースを指します。

- 使用容量は、RAID によるオーバーヘッドが除外されているという点で raw 容量とは異なります。つまり、RAID 構成を考慮する必要はありません。
- 仮想テープ ライブラリの使用可能なネイティブ容量とは、Data Protector の内部データベースに従って保護されているバックアップ、およびそのコピーとミラーによって占有されるスペースを指します。仮想テープ ライブラリのライセンス管理をシンプルかつ容易にするため、VTL については 2:1 の圧縮率が想定されており、圧縮に伴う追加費用は不要です。
- 使用容量は、RAID によるオーバーヘッドが除外されているという点で raw 容量とは異なります。つまり、RAID 構成を考慮する必要はありません。
- ディスクストレージへのバックアップは、複数のディスク アレイおよびシステムに分散できます。
- この拡張機能には、ドライブやライブラリの LTU は不要です。ドライブおよびライブラリのライセンスは、ファイル デバイスには必要ですが、アドバンスト バックアップには不要です。同様に、アドバンスト バックアップ使用権は、ドライブおよびライブラリのライセンスにはなりません。
- ディスクへのバックアップ機能は、Windows と UNIX のどちらでも実行できます。
- このライセンスは、Data Protector ファイル ライブラリへのバックアップに必要です。
- 仮想テープ ライブラリ (VTL) に対して、このライセンスをドライブおよびライブラリのライセンスの代わりに使うことも可能です。VTL 組み込みの圧縮は、Data Protector 側で意識されることはありません。VTL については 2:1 の圧縮率が想定されています。

たとえば、ネイティブ容量が 5 TB の VTL には、2:1 圧縮により 10 TB のデータをバックアップできます。この場合も、5 つの B7038AA しか必要ではありません。従来のドライブおよびライブラリのライセンスをそのまま使うことも可能です。なお、同一セル内に複数のライセンスモデルを混在させることは可能ですが、同一 VTL 内で混在させることはできません。

注記

1 つのライブラリ使用権だけを使って、複数セル間で仮想ライブラリ容量を共有するためには、ライブラリを共有する個々のセルにマネージャ・オブ・マネージャ使用権が必要になります。

任意のディスク上にある Data Protector ファイル ライブラリの使用可能なネイティブ容量の圧縮に伴う追加料金は不要です。圧縮は、使用しているオペレーティング システムあるいは NAS (Network Attached Storage) により、NFS (Network File System) または CIFS (Common Internet File System) を介して提供されます。NAS アプライアンスのシングル インスタンス化も同様に扱われます。Data Protector A.05.50 の場合は、サード パーティプロバイダによるシングル インスタンス化と圧縮を追加料金なしで可能にするためには、Data Protector ファイル ライブラリの使用可能なネイティブ容量に対する使用権にパッチを適用する必要があります。

例:

- 使用可能な総ネイティブ容量が 2.5 TB のバックアップ ディスク アレイが 1 つあり、全容量をアドバンスド バックアップに使用する場合は、B7038AA が 3 つ必要です。
 - raw 総容量が 2.5 TB のバックアップ ディスク アレイが 1 つあり、全容量が RAID 1 (ミラーリング) として構成されている場合は、使用可能なネイティブ容量は 1.25 TB になります。そのため、全容量をアドバンスド バックアップに使用する場合は、2 つの B7038AA しか必要ではありません。
 - 使用可能な総ネイティブ容量がそれぞれ 2.5 TB のバックアップ ディスク アレイが 2 つあり、全容量をアドバンスド バックアップに使用する場合は、B7038AA が 5 つ必要です。
 - 論理容量がそれぞれ 0.75 TB のブレード サーバが 10 台あり、全容量をアドバンスド バックアップに使用する場合は、B7038AA が 8 つ必要です。
- このライセンスは、合成フルバックアップまたは仮想フルバックアップの実行にも必要です。

**表 A-10 HP OpenView Storage Data Protector
ゼロ・ダウンタイム・バックアップ (ZDB) 使用権**

B7023CA	Data Protector ゼロ・ダウンタイム・バックアップ HP XP 1TB 使用権
B7023DA	Data Protector ゼロ・ダウンタイム・バックアップ HP XP 10TB 使用権
B7025CA	Data Protector ゼロ・ダウンタイム・バックアップ HP EVA/VA 1TB 使用権
B7025DA	Data Protector ゼロ・ダウンタイム・バックアップ HP EVA/VA 10TB 使用権
B6959CA	Data Protector ゼロ・ダウンタイム・バックアップ EMC Symmetrix 1TB 使用権
B6959DA	Data Protector ゼロ・ダウンタイム・バックアップ EMC Symmetrix 10TB 使用権

ゼロ・ダウンタイム・バックアップ使用権 (LTU) は、ゼロダウンタイムバックアップ (ZDB) によってデータを保護し以下の機能を利用する、特定のディスクアレイ上の使用ディスクスペース容量に対する容量ベース (TB) の使用権です。

- HP Business Copy XP/EVA および HP Continuous Access XP/EVA の両方またはいずれか
- EMC TimeFinder および EMC SRDF の両方またはいずれか

使用ディスクスペース容量とは、ゼロダウンタイムバックアップまたはインスタントリカバリ用に使用しているディスクアレイ上のすべてのプライマリボリュームを合計した容量です (プライマリとは、元の実稼動データ量を意味します)。この容量はこれらのボリュームの使用可能な容量を表し、構成されている LDEV サイズに一致します。データ保護の目的で使用されるセカンダリボリューム、ミラー、スナップショットによって消費される容量に対するライセンスは不要です。

- RAID オーバーヘッドは除きます。つまり RAID 構成を考慮する必要はありません。
- ZDB を実行するにはオンライン バックアップ使用権 (B6955BA、B6865BA) が必要です。
- Windows 2003 VSS (Volume Shadow copy Service) ハードウェア プロバイダを使用する ZDB には、この ZDB 使用権 (LTU) が必要です。たとえば、HP ディスク アレイプロバイダを使用して、ファイルシステムのスナップショット、Microsoft Exchange Server、Microsoft SQL Server のバックアップを作成するような場合です。

**表 A-11 HP OpenView Storage Data Protector
インスタント・リカバリ使用権**

B7026CA	Data Protector インスタント・リカバリ HP XP 1TB 使用権
B7026DA	Data Protector インスタント・リカバリ HP XP 10TB 使用権
B7028AA	Data Protector インスタント・リカバリ HP EVA/VA 1TB 使用権
B7028DA	Data Protector インスタント・リカバリ HP EVA/VA 10TB 使用権

インスタント・リカバリ使用権 (LTU) は、使用ディスク スペースに対する容量ベース (TB) の使用権で、インスタント リカバリを利用する特定のディスク アレイタイプのインスタント リカバリで必要になります。Data Protector のインスタント リカバリを利用すると、数テラバイトのデータを 1 つまたは複数の復旧ディスクから数分で復旧でき、テープから復旧する場合のように数時間も要することはありません。

使用ディスク スペース容量とは、ゼロ ダウンタイム バックアップ (ZDB) またはインスタント リカバリ (IR) 用に使用しているディスク アレイ上のすべてのボリュームを合計した容量です (プライマリとは、元の実稼動データ量を意味します)。この容量はこれらのボリュームの使用可能な全容量を表し、構成されている LDEV サイズに一致します。データ保護の目的で使用されるセカンダリ ボリューム、ミラー、スナップショットによって消費される容量に対しては、ライセンスは不要です。

- RAID オーバーヘッドは除きます。つまり RAID 構成を考慮する必要はありません。
- 同量の Data Protector ゼロ・ダウンタイム・バックアップ (ZDB) 使用権が必要で、各 ZDB 使用権にはオンライン・バックアップ使用権が 1 つ必要です。

**表 A-12 HP OpenView Storage Data Protector
ダイレクト・バックアップ使用権 (日本では未販売)**

B7027AA	Data Protector Direct Backup for XP, 1TB LTU
B7027DA	Data Protector Direct Backup for XP, 10TB LTU

ダイレクト・バックアップ使用権 (LTU) は、HP StorageWorks Disk Array XP を使ったダイレクトバックアップに必要です。ダイレクト (サーバレス) バックアップに必要な使用ディスクスペース容量 (TB) に応じたライセンスが必要になります。

同量の Data Protector ゼロ・ダウンタイム・バックアップ (ZDB) 使用権が必要で、各 ZDB 使用権にはオンライン・バックアップ使用権が 1 つ必要です。

**表 A-13 HP OpenView Storage Data Protector
NDMP ダイレクト・バックアップ使用権**

B7022BA	Data Protector NDMP Direct Backup 1TB 使用権
B7022DA	Data Protector NDMP Direct Backup 10TB 使用権

NDMP ダイレクト・バックアップ使用権 (LTU) は、1 台の NDMP サーバ上でデータをバックアップするのに必要な容量ベース (TB) の使用権です。

このライセンスは、NDMP を使用してバックアップされる各ファイラー (Network Appliance Filer、EMC Celerra File Server など) ごとに、使用ディスクスペース容量 (TB) に応じて必要です。

使用ディスクスペース容量とは、NDMP を使用してバックアップされるファイラーの全ボリュームの総容量を指します。この容量はこれらのボリュームの使用可能な総容量を表し、構成されている LDEV サイズに一致します。

**表 A-14 HP OpenView Storage Data Protector
印刷版機能拡張マニュアル**

B6960EA	Data Protector 機能拡張マニュアル (英語版)
B6960EJ	Data Protector 機能拡張マニュアル (日本語版)

マニュアルは DVD および CD に電子的な形で収録されているほか、<http://www.hp.com/support/manuals> からダウンロード可能です。

ご注文いただける印刷版マニュアルには、スターターパックセットと機能拡張セットの2種類があります。印刷版スターターパックセットには、以下のマニュアルが含まれます。スターターパック マニュアルの詳細は、A-18 ページの「マニュアル」を参照してください。

印刷版機能拡張セットには、以下のマニュアルが含まれます。

- 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
- HP OpenView Storage Data Protector インテグレーション ガイド - Oracle、SAP
- HP OpenView Storage Data Protector Integration Guide for IBM Applications: Informix, DB2, and Lotus Notes/Domino
- HP OpenView Storage Data Protector Integration Guide for Sybase, Network Node Manager, and Network Data Management Protocol
- HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide
- 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
- HP OpenView Storage Data Protector Zero Downtime Backup Administrator's Guide
- Integration Guide for OpenView Service Information Portal and OpenView Reporter
- HP OpenView Storage Data Protector Integration Guide for HP OpenView
- HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations for UNIX
- HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations for Windows
- OpenView Operations for UNIX, Product Announcements, Software Notes, and References
- Data Protector Media Operations User's Guide
- Data Protector Media Operations Product Announcements, Software Notes, and References

シングルサーバ版 (SSE)

表 A-15 は、Data ProtectorA.06.00 シングルサーバ版スターターパックのライセンス番号一覧です。

**表 A-15 HP OpenView Storage Data Protector
スターターパックのライセンス番号**

B7020AA	Data Protector シングルサーバ版 HP-UX (DVD)
B7020BA	Data Protector シングルサーバ版 HP-UX 使用権のみ
B7020DA	Data Protector シングルサーバ版 Solaris (DVD)
B7020CA	Data Protector シングルサーバ版 Solaris 使用権のみ
B7030AA	Data Protector シングルサーバ版 Windows (DVD)
B7030BA	Data Protector シングルサーバ版 Windows 使用権のみ
B7021AA	Data Protector シングルサーバ版 スターターパックへのアップグレード HP-UX (DVD)
B7021DA	Data Protector シングルサーバ版 スターターパックへのアップグレード Solaris (DVD)
B7031AA	Data Protector シングルサーバ版 スターターパックへのアップグレード Windows (DVD)
B6960MA	Data Protector DVD メディア (日本語版、英語版共通)
B6960LA	Data Protector マニュアル (英語版)
B6960LJ	Data Protector マニュアル (日本語版)
B6960LF	Data Protector Manuals (French) (日本では未販売)

ライセンス

シングルサーバ版使用权 (LTU) は、特定プラットフォーム上の 1 台のシングルサーバをバックアップするのに必要で、使用できる UNIX または Windows ワークステーションの数に制限はなく、1 台のバックアップドライブを使用できます。さらに、10 スロット以下のオートチェンジャまたはライブラリ 1 台も管理できます。

移行

移行使用权 (LTU) は、SSE または Data Protector Express から Data Protector スターターパックに移行する場合に必要です。

以下の機能を使用するには、シングルサーバ版からスターターパックに移行する必要があります。

- 任意のプラットフォーム上の追加のバックアップクライアント (エージェント)
- 追加のバックアップドライブ
- スロット数 11 以上のオートローダーとライブラリの管理
- システム障害復旧
- 高度なレポート機能 (Data Protector GUI および Web から使用)
- SAN サポート (HP-UX 用または Solaris 用の管理サーバとともに使用)
- OpenView との統合によるサービス集中管理

追加の各種機能拡張移行 LTU を注文するには、シングルサーバ版の LTU が必要です。

メディア

Data Protector A.06.00 は 2 枚の DVD に収録されています。必要に応じて、15 枚組みの CD セット (B6960MB) もご利用いただけますが、可能であれば DVD セットの使用をお勧めします。

マニュアル

すべてのマニュアルは DVD および CD に電子的な形で収録されているほか、<http://www.hp.com/support/manuals> からもダウンロード可能です。

ご注文いただける印刷版マニュアルには、スターターパックセットと機能拡張セットの 2 種類があります。印刷版スターターパックセットには、以下のマニュアルが含まれます。

- HP OpenView Storage Data Protector コンセプトガイド
- HP OpenView Storage Data Protector インストールおよびライセンスガイド

- HP OpenView Storage Data Protector *トラブルシューティングガイド*
- HP OpenView Storage Data Protector *障害復旧ガイド*
- HP OpenView Storage Data Protector Product Announcements *ソフトウェア ノート および リファレンス*

注記 シングルサーバ版 Windows では、Windows ワークステーションしか管理できません。

機能拡張マニュアルの一覧は、A-15 ページの「HP OpenView Storage Data Protector 印刷版機能拡張マニュアル」を参照してください。

Data Protector A.06.00 へのライセンス移行

以前のバージョンの Data Protector からの移行手順は、以下のとおりです。

Data Protector A.05.x

Data Protector A.06.00 に直接移行してください。ライセンスその他の移行は必要ありません。Data Protector A.05.x のサポート契約をされているお客様は、Data Protector A.06.00 を無償で受け取ることができます。従来 A.05.x で使用していた機能は、Data Protector A.06.00 へのアップグレード後も追加コストなしにそのままご利用いただけます。Data Protector A.06.00 が提供する新しい機能拡張を使用する場合のみ、新しいライセンスの購入が必要になります。

ライセンス概要図

図 A-2 スターター パック (HP-UX 用)

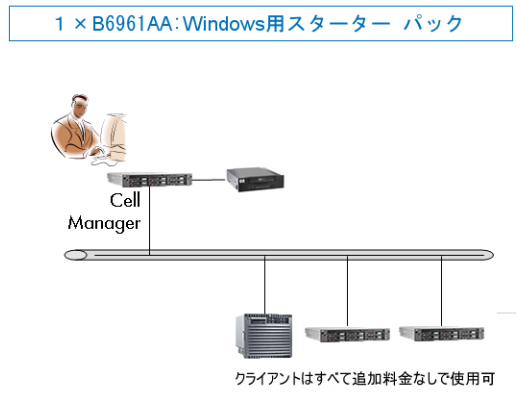


図 A-3 混在環境

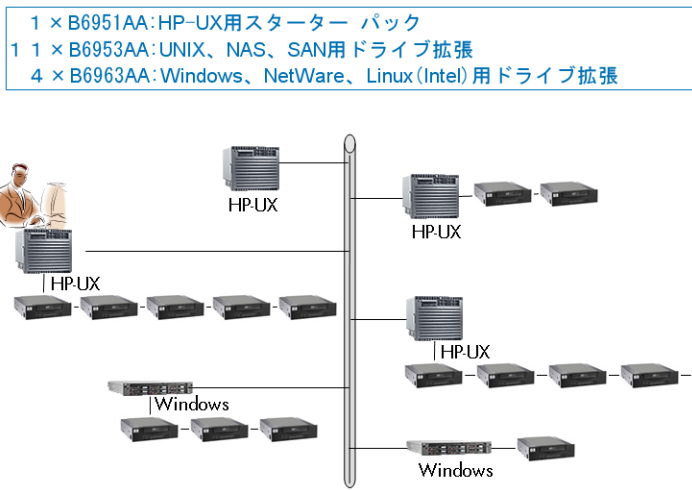


図 A-4 61 ~ 250 スロットのライブラリ - 例 1

- 1 × B6961AA: Windows用スターター パック
- 9 × B6963AA: Windows、NetWare、Linux (Intel) 用ドライブ拡張
- 4 × B6953AA: UNIX、NAS、SAN用ドライブ拡張
- 1 × B6957BA: 61~250スロットのライブラリ拡張
- 1 × B6958BA: スロット数無制限のライブラリ拡張

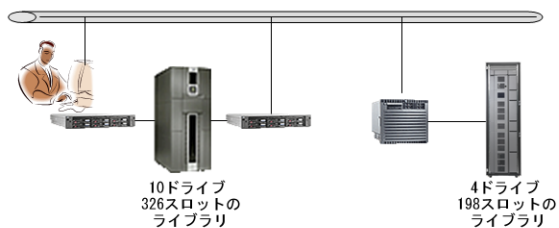


図 A-5 61 ~ 250 スロットのライブラリ - 例 2

- 1 × B6951AA: HP-UX用スターター パック
- 1 3 × B6953AA: UNIX、NAS、SAN用ドライブ拡張
- 1 × B6958BA: スロット数無制限のライブラリ拡張
- 1 × B6957BA: 61~250スロットのライブラリ拡張

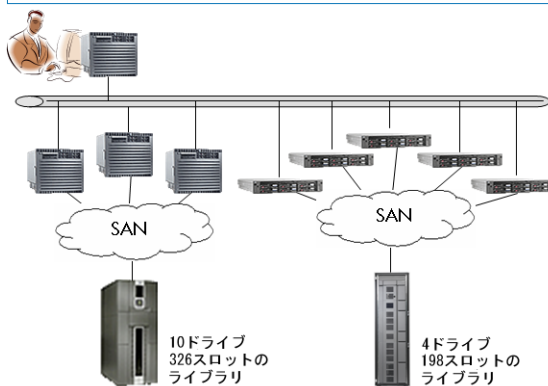


図 A-6 オンラインバックアップ

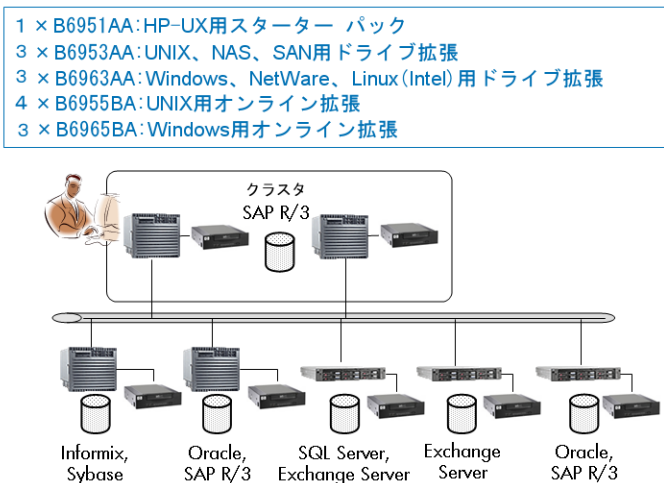


図 A-7 Manager-of-Managers

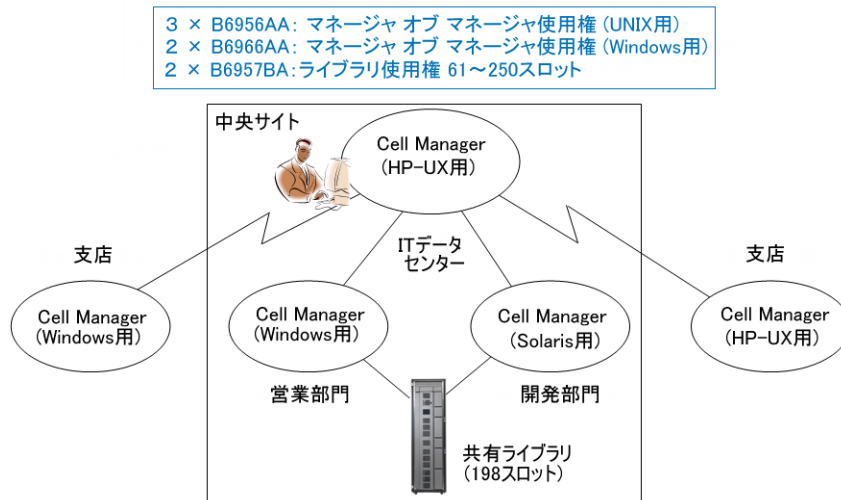


図 A-8 ディスクへのアドバンスト バックアップ

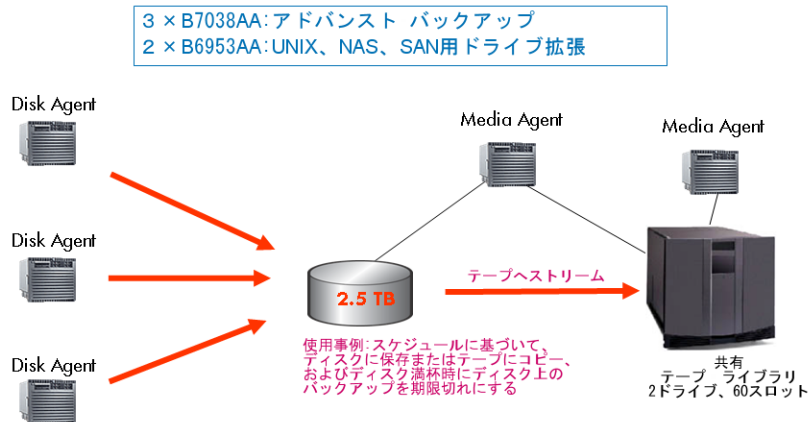
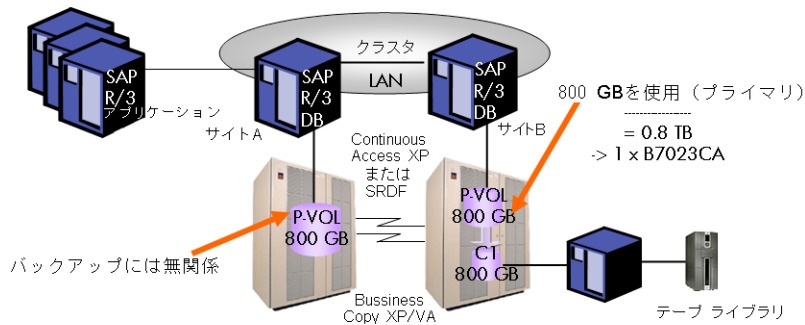


図 A-9 ゼロ ダウンタイム バックアップ

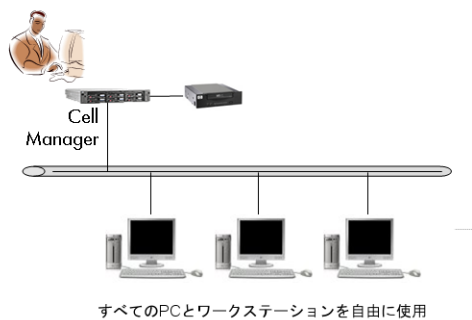
1 × B7023CA:HP Storage Works XP用ゼロ ダウンタイム バックアップ拡張



- 注
- ・ゼロ バックアップの例 (800 GB LDEV)
 - ・RAIDレベルを考慮する必要はありません(プライマリ ボリュームのみを考慮すれば十分です)。
 - ・インスタント リカバリおよびダイレクト バックアップはテラバイトでの計算値内に入ります。

図 A-10 シングルサーバ版

1 × B7030AA: Windows用のシングル サーバ版



Data Protector ライセンス フォーム

この章では、Data Protector のライセンス フォームについて説明します。恒久パスワードをご注文の際は、以下のいずれかの方法でこのフォームに記入してください。

- HP OpenView AutoPass ユーティリティを使用して、HP Password Delivery Center の Web サーバから、インターネットを介して恒久パスワードを直接取得し、インストールします。詳細は 309 ページの「HP OpenView AutoPass ユーティリティを使用した恒久パスワードの取得とインストール」を参照してください。この方法を推奨します。
- 以下の名前のファイルにデータとして含まれているライセンス フォームを印刷することもできます。このファイルは Cell Manager システムまたは配布メディアに含まれています。
 - HP-UX または Solaris: /opt/omni/doc/C/license_forms_UNIX
 - Windows CD-ROM:

`<Disk_Label>:Docs¥license_forms.txt`

または上記ファイルからコピーした内容をメールに貼り付けて、*Password Delivery Center (PDC)* に送ってください。

- オンラインの *Password Delivery Center* サイト (<http://www.webware.hp.com>) から恒久パスワードを注文することも可能です。

重要 情報は正確に記入してください。必要事項に漏れがないように注意してください。

ライセンス フォームで記入が必要な共通のフィールドについて、以下に説明します。

ユーザー情報 (Personal Data) 新しいパスワードの送付先となるユーザーに関する情報を記入してください。

ライセンス データ (Licensing Data) Data Protector セルに関するライセンス情報を記入します。

現在の Cell Manager (Current Cell Manager) 現在の Cell Manager に関して必要な情報を記入します。

新しい Cell Manager (New Cell Manager) 新しい Cell Manager に関して必要な情報を記入します。

注文番号 (Order Number) 権利保証書 (*Entitlement Certificate*) に記載されている *Order Number* を記入します。この *Order Number* は、恒久パスワードを請求する際に必要です。

付録 A

Data Protector ライセンス フォーム

IP アドレス (IP Address)

この欄には、*Password Delivery Center* が発行するパスワードの対象となるシステムの IP アドレスを記入します。集中ライセンス (MoM 環境のみ) を使用する場合は、MoM Manager システムの IP アドレスを記入してください。

Cell Manager に複数の LAN カードが装着されている場合は、どの IP アドレスでも結構です。主に使用する IP アドレスを記入することをお勧めします。

MC/ServiceGuard 環境または Microsoft Cluster 環境で Data Protector をお使いの場合は、仮想サーバの IP アドレスを記入してください。クラスタ環境についての詳細は、オンライン ヘルプを参照してください。

Password Delivery Center

ファックス番号

連絡先は、製品に付属する権利保証書 (*Entitlement Certificate*) でご確認ください。

製品ライセンスの種類

Product Numbers の右の欄に、Cell Manager にインストールするライセンスの数量を記入します。1 つの *Order Number* でライセンスを全数購入することも、ライセンスのサブセットだけを購入することもできます。

B 付録 B

この付録の内容

この付録では、本来は本書の範囲外ですが、インストール手順に特に関係のある作業についての情報を説明します。

以降では、Windows、HP-UX、および Solaris システムについて、システムやデバイスの設定および構成について例を挙げて説明しています。

ネイティブ ツールを使用した、HP-UX、Solaris、および Linux システムへのインストール

注記 HP-UX、Solaris、および Linux へのネイティブ インストール手順は、インストール サーバの制限付きパッケージをインストールする場合にのみ必要です。通常は、omnisetup.sh コマンドを使用して Data Protector をインストールすることをお勧めします。

swinstall を使用した HP-UX システムへの Cell Manager のインストール

HP-UX システムに UNIX 用 Cell Manager をインストールするには、以下の手順に従ってください。

1. UNIX インストール DVD-ROM をドライブに挿入してマウントし、/usr/sbin/swinstall ユーティリティを実行します。
2. [Specify Source] ウィンドウで [Network Directory/CDROM] を選択し、[Source Depot Path] テキスト ボックスに以下のように入力します。

- PA-RISC ベースの HP-UX の場合：
<Mountpoint>/hpux_pa/DP_DEPOT/DP_A0600_UX11x.sd_depot
- IA-64 ベースの HP-UX の場合：
<Mountpoint>/hpux_ia/DP_DEPOT/DP_A0600_UXia64.sd_depot

次に、[OK] をクリックして [SD Install - Software Selection] ウィンドウを開きます。

3. インストール可能なソフトウェア パッケージのリスト内で、B6960MA という名前の下に Data Protector が表示されます。これをダブルクリックすると、UNIX 用 DATA-PROTECTOR プロダクトが表示されます。さらにこれをダブルクリックすると、内容が表示されます。

以下のサブプロダクトが含まれています。

OB2-CM	Cell Manager ソフトウェア
OB2-DOCS	Data Protector ドキュメント サブプロダクト (Data Protector のドキュメントを PDF 形式で収録)

4. DATA-PROTECTOR をマウスの右ボタンでクリックし、[Mark for Install] をクリックして、ソフトウェア全体をインストール対象に含めます。

インストールするかどうかをサブプロダクトごとに指定したい場合は、DATA-PROTECTOR をダブルクリックし、各項目をマウスの右ボタンでクリックします。特定のパッケージをインストールしない場合は、[Unmark for Install] をクリックし、インストールする場合は、[Mark for Install] を選択します。

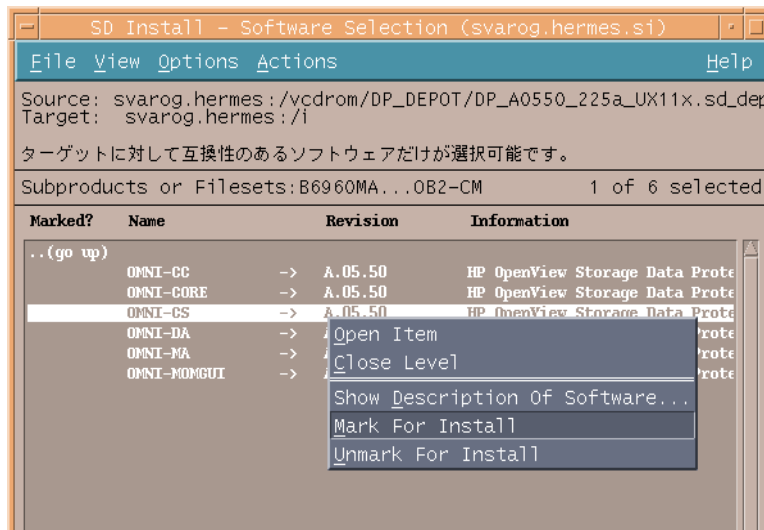
必ず確認していただきたいのは、Marked? ステータスの値 (OB2-CM パッケージの横) が [はい] になっていることです。これは、UNIX 用の Cell Manager を同じシステムにインストールする場合に必要です。詳細は図 B-1 を参照してください。

注記

32 ビットより長いユーザー ID を使用しているときは、Cell Manager のコア ソフトウェア コンポーネントをインストールした後で、その Cell Manager にリモートでユーザー インタフェース コンポーネント (OMNI-CS) をインストールする必要があります。

5. [Actions] メニューの [Install (analysis)] をクリックし、[OK] をクリックして次に進みます。[Install (analysis)] で解析が失敗し、エラー メッセージが表示された場合は、[Logfile] をクリックしてログ ファイルを確認してください。

図 B-1 [SD Install - Software Selection] ウィンドウ



注記 テープ デバイスからネットワークを介して、ソフトウェアをインストールする場合は、まず、コンピュータでソース ディレクトリをマウントする必要があります。

pkgadd を使用した Solaris システムへの Cell Manager のインストール

Solaris システムに Cell Manager をインストールするには、以下の手順に従ってください。

1. UNIX 用インストール DVD-ROM をドライブに挿入します。
2. メインの <package_source> ディレクトリ、つまりインストール デポ ファイルが格納されているディレクトリに移動します (この場合は <Mount_point>/solaris/DP_DEPOT)。

プロダクト内には Cell Manager のインストールに関連する以下のサブプロダクト パッケージが含まれています。

OB2-CORE	Data Protector のコア ソフトウェア
OB2-CC	Cell Console ソフトウェア この中にはグラフィカル ユーザー インタフェースとコマンド行インタフェースが含まれます。
OB2-CS	Cell Manager ソフトウェア
OB2-DA	Disk Agent ソフトウェア このソフトウェアは必須です。このソフトウェアがない場合は、IDB のバックアップを実行できません。
オプション ソフトウェア	
OB2-MA	General Media Agent ソフトウェア。このコンポーネントは、バックアップ デバイスを Cell Manager に接続する場合に必要になります。
OB2-DOCS	Data Protector オンライン マニュアル

3. 上記のパッケージをインストールするには、pkgadd 機能を使用します。

重要 Solaris 上のサブプロダクト パッケージは、互いに依存しています。これらのパッケージは、上記の順序でインストールしなければなりません。

各パッケージをインストールするには、以下のコマンドを実行します。

```
pkgadd -d DP_A0600_SUN8.pkg <package_name>
```

4. Data Protector サービスを再起動します。

```
/opt/omni/sbin/omnisv stop
```

```
/opt/omni/sbin/omnisv start
```

注記

Cell Manager を Solaris 9 にインストールした場合は、インストール サーバを使用して Cell Manager 上に Disk Agent をリモート インストールすることができます。詳細については、50 ページの「Data Protector クライアントのリモート インストール」を参照するか、または ob2install のマンページを参照してください。

rpm を使用した Linux システムへの Cell Manager のインストール

Linux システムに Cell Manager をインストールするには、以下の手順に従ってください。

1. UNIX インストール DVD-ROM をドライブに挿入してマウントします。
2. 以下のいずれかの方法で、個々のパッケージを展開します。

- rpm2cpio を使用します (推奨)。

アーカイブの展開先となる一時ディレクトリに移動して、次のコマンドを実行します。

```
rpm2cpio <pkg_source>/DP_A0600_GPLx86_64.rpm | cpio -ivd
```

<pkg_source> にはインストール アーカイブが格納されているディレクトリを指定します (この場合は <Mount_point>/linux/DP_DEPOT)。

- 別の方法として、次に示すように rpm を使用することもできます。

インストール アーカイブが格納されているディレクトリに移動し (この場合は <Mount_point>/linux/DP_DEPOT)、次のコマンドを実行します。

```
rpm -i DP_A0600_GPLx86_64.rpm
```

注記

この rpm -i コマンドではソフトウェアはインストールされません。個々の rpm パッケージが /opt/omni にコピーされるだけです。

ただし、この場合もパッケージは登録されるため、個々のパッケージのインストール終了後に、OB2-CM パッケージを削除する必要があります。

ネイティブ ツールを使用した、HP-UX、Solaris、および Linux システムへのインストール

3. 個々のパッケージの展開先ディレクトリに移動します。

- rpm2cpio コマンドを使用した場合 : `cd <temporary_directory>/opt/omni`
- rpm コマンドを使用した場合 : `cd /opt/omni`

次のコマンドを実行して、パッケージをインストールします。

```
rpm -i <package_name>-A.06.00-1.x86_64.rpm
```

<package_name> には、サブプロダクト パッケージの名前を指定します。

以下のパッケージは必ずインストールしてください。

OB2-CORE	Data Protector のコア ソフトウェア
OB2-CC	Cell Console ソフトウェア コマンド行インタフェースを含みます。
OB2-CS	Cell Manager ソフトウェア
OB2-DA	Disk Agent ソフトウェア このソフトウェアは必須です。このソフトウェアがない場合は、IDB のバックアップを実行できません。

必要に応じて、以下のパッケージもインストールしてください。

OB2-MA	General Media Agent ソフトウェア。このコンポーネントは、バックアップ デバイスを Cell Manager に接続する場合に必要になります。
OB2-DOCS	Data Protector オンライン マニュアル

重要 Linux 上のサブプロダクト パッケージは、互いに依存しています。これらのパッケージは、上記の順序でインストールしなければなりません。

4. Data Protector サービスを再起動します。

```
/opt/omni/sbin/omnisv stop
```

```
/opt/omni/sbin/omnisv start
```

5. メイン rpm アーカイブの展開に rpm を使用した場合は、次のコマンドで OB2-CM パッケージを削除します。

```
rpm -e OB2-CM
```

HP-UX システムへのインストール サーバのインストール

1. UNIX インストール DVD-ROM をドライブに挿入してマウントします。
2. コマンド行に `/usr/sbin/swinstall` と入力して、インストールプログラムを起動します。
3. [Specify Source] ウィンドウで [Network Directory/CDROM] を選択し、[Source Depot Path] テキスト ボックスに以下のように入力します。

- PA-RISC ベースの HP-UX の場合：

`<Mount_point>/hpux_pa/DP_DEPOT/DP_A0600_UX11x_IS.sd_depot`

- IA-64 ベースの HP-UX の場合：

`<Mount_point>/hpux_ia/DP_DEPOT/DP_A0600_UXia64_IS.sd_depot`

次に、[OK] をクリックして [SD Install - Software selection] ウィンドウを開きます。

4. [SD Install - Software Selection] ウィンドウで、DATA-PROTECTOR をダブルクリックします。インストール可能なソフトウェアのリストが表示されます。OB2-IS をマウスの右ボタンでクリックし、[Mark for Install] をクリックします。
5. [Actions] メニューの [Install (analysis)] をクリックします。[OK] をクリックしてインストール処理を続行します。

インストールが終了すると、UNIX 用のソフトウェア デポは、`/opt/omni/databases/vendor` ディレクトリにインストールされます。

重要

ネットワーク上に UNIX 用のインストール サーバをインストールしない場合は、UNIX インストール DVD-ROM を使用して、すべての UNIX クライアントをローカルにインストールしなければなりません。

pkgadd を使用した Solaris システムへのインストール サーバのインストール

Solaris へのローカル インストール

UNIX 用のインストール サーバを Solaris システムにインストールするには、以下の操作を行います。

1. UNIX 用インストール DVD-ROM をドライブに挿入します。

ネイティブ ツールを使用した、HP-UX、Solaris、および Linux システムへのインストール

2. メインの `<package_source>` ディレクトリ、つまりインストール デポ ファイルが格納されているディレクトリに移動します (この場合は `<Mount_point>/solaris/DP_DEPOT`)。

プロダクト内にはインストール サーバのインストールに関連する以下のサブプロダクト パッケージが含まれています。

OB2-CORE	Data Protector のコア ソフトウェア。Cell Manager システムにインストール サーバをインストールする場合は、コア ソフトウェアはすでにインストールされています。
OB2-C-IS	インストール サーバのコア ソフトウェア
OB2-SOLUX	リモートの Solaris システムのための Disk Agent、Media Agent、および GUI 用プッシュ パッケージ。
OB2-OTHUX	Solaris 以外のリモートの UNIX システムのための、Disk Agent および Media Agent 用プッシュ パッケージ。

さらに、(Cell Manager とは別のシステムに) 独立した形でインストール サーバをセットアップし、ユーザー インタフェースを使用したい場合は、次のコンポーネントが必要です。

OB2-CC	Cell Console ソフトウェア この中にはグラフィカル ユーザー インタフェースとコマンド行インタフェースが含まれます。
--------	---

3. 上記のパッケージをインストールするには、`pkgadd` 機能を使用します。

重要 Solaris 上のサブプロダクト パッケージは、互いに依存しています。これらのパッケージは、上記の順序でインストールしなければなりません。

各パッケージをインストールするには、以下のコマンドを実行します。

```
pkgadd -d DP_A0600_SUN8_IS.pkg <package_name>
```

注記 `pkgadd` 機能はリモートでは使用できず、ローカルな形でのみ実行可能です。

4. これらのコンポーネントのインストールが終了したら、次に `pkgadd` コマンドを使用して、リモート インストールする各統合パッケージに必要なプッシュ パッケージをインストールします。以下に例を示します。

OB2-INTGP	Data Protector コア統合ソフトウェア。このコンポーネントは、統合ソフトウェアをインストールする場合に必要です。
OB2-SAPP	SAP 用統合ソフトウェア コンポーネント

付録 B

ネイティブ ツールを使用した、HP-UX、Solaris、および Linux システムへのインストール

OB2-SAPDBP	SAP DB 用統合ソフトウェア コンポーネント
OB2-INFP	Informix 用統合ソフトウェア コンポーネント
OB2-LOTP	Lotus Notes/Domino 用統合ソフトウェア コンポーネント
OB2-SYBP	Sybase 用統合ソフトウェア コンポーネント
OB2-OR8P	Oracle 用統合ソフトウェア コンポーネント
OB2-DB2P	DB2 用統合ソフトウェア コンポーネント
OB2-EMCP	EMC Symmetrix 用統合ソフトウェア コンポーネント
OB2-SNAPP	HP StorageWorks Virtual Array
OB2-SMISAP	HP StorageWorks Enterprise Virtual Array
OB2-SSEAP	HP StorageWorks Disk Array XP
OB2-NDMP	NDMP Media Agent ソフトウェア
OB2-OVP	OpenView 用統合ソフトウェア コンポーネント
OB2-FRAP	フランス語ローカライズ パッケージ
OB2-JPNP	日本語ローカライズ パッケージ

インストールが終了すると、UNIX 用のソフトウェア デポは、
/opt/omni/databases/vendor ディレクトリにインストールされます。

重要 ネットワーク上に UNIX 用のインストール サーバをインストールしない場合は、UNIX インストール DVD-ROM を使用して、すべての UNIX クライアントをローカルにインストールしなければなりません。

重要 Data Protector は、たとえば次のようなリンク ディレクトリにインストールすることができます。

```
/opt/omni/ -> /<prefix>/opt/omni/  
/etc/opt/omni/ -> /<prefix>/etc/opt/omni/  
/var/opt/omni/ -> /<prefix>/var/opt/omni/
```

このようにする場合は、インストール前にリンクを作成しておき、インストール先ディレクトリが存在することを確認しておかなければなりません。

注記

ユーザー インタフェース コンポーネント (グラフィカル ユーザー インタフェースまたはコマンド行インタフェース) を使用する場合は、事前に環境変数を更新する必要があります。詳細は 27 ページの「環境変数の設定」を参照してください。

複数プラットフォームにわたるバックアップや復元を Data Protector ユーザー インタフェースを使用して実行するよう計画している場合は、『HP OpenView Storage Data Protector Product Announcements ソフトウェア ノート および リファレンス』を参照して制限事項を確認してください。

この次に行う作業

この時点で、UNIX 用のインストール サーバがネットワーク上にすでにインストールされていなければなりません。準備が整ったら、以下の作業を行います。

1. (Cell Manager とは別のシステムに) 独立した形でインストール サーバをセットアップした場合は、このシステムを Data Protector セルに手作業で追加 (インポート) しなければなりません。詳細は 187 ページの「セルへのインストール サーバのインポート」を参照してください。

注記

インストール サーバをインポートすると、Cell Manager 上の `/etc/opt/omni/server/cell/installation_servers` ファイルが更新されて、インストールしたプッシュ パッケージが反映されます。CLI からこのファイルを使用して、使用可能なプッシュ パッケージを確認できます。このファイルを最新状態に保つために、プッシュ パッケージをインストールまたは削除したときは、インストール サーバのエクスポートと再インポートを必ず実行してください。これは、インストール サーバを Cell Manager と同じシステムにインストールしてある場合も同様です。

2. Data Protector セルに Windows システムが含まれている場合は、Windows 用のインストール サーバをインストールする必要があります。詳細は 41 ページの「Windows 用のインストール サーバのインストール」を参照してください。
3. ソフトウェアをクライアントに配布します。詳細は 46 ページの「Data Protector クライアントのインストール」を参照してください。

rpm を使用した Linux システムへのインストール サーバのインストール

Linux へのローカル インストール

UNIX 用のインストール サーバを Linux システムにインストールするには、以下の操作を行います。

1. UNIX 用インストール DVD-ROM をドライブに挿入します。
2. 以下のいずれかの方法で、個々のパッケージを展開します。

- rpm2cpio を使用します (推奨)。

アーカイブの展開先となる一時ディレクトリに移動して、次のコマンドを実行します。

```
rpm2cpio <pkg_source>/DP_A0600_GPLx86_64.rpm | cpio -ivd
```

<pkg_source> にはインストール アーカイブが格納されているディレクトリを指定します (この場合は <Mount_point>/linux/DP_DEPOT)。

- 別の方法として、次に示すように rpm を使用することもできます。

インストール アーカイブが格納されているディレクトリに移動し (この場合は <Mount_point>/linux/DP_DEPOT)、次のコマンドを実行します。

```
rpm -i DP_A0600_GPLx86_64_IS.rpm
```

注記

この rpm -i コマンドではソフトウェアはインストールされません。個々の rpm パッケージが /opt/omni にコピーされるだけです。

ただし、この場合もパッケージは登録されるため、個々のパッケージのインストール終了後に、OB2-CM パッケージを削除する必要があります。

3. 個々のパッケージの展開先ディレクトリに移動します。

- rpm2cpio コマンドを使用した場合 : `cd <temporary_directory>/opt/omni`
- rpm コマンドを使用した場合 : `cd /opt/omni`

個々のパッケージについて、次のコマンドを実行します。

```
rpm -i <package_name>-A.06.00-1.x86_64.rpm
```

プロダクト内にはインストール サーバのインストールに関連する以下のサブプロダクト パッケージ (<package_name>) が含まれています。

ネイティブ ツールを使用した、HP-UX、Solaris、および Linux システムへのインストール

OB2-CORE	Data Protector のコア ソフトウェア。Cell Manager システムにインストール サーバをインストールする場合は、コア ソフトウェアはすでにインストールされています。
OB2-CORE-IS	インストール サーバのコア ソフトウェア
OB2-LINUXP	リモートの Linux システムのための Disk Agent、Media Agent、および GUI 用プッシュ パッケージ。
OB2-OTHUXP	Linux 以外のリモート システムのための Disk Agent 用および Media Agent 用プッシュ パッケージ

さらに、(Cell Manager とは別のシステムに) 独立した形でインストール サーバをセットアップし、ユーザー インタフェースを使用したい場合は、次のコンポーネントが必要です。

OB2-CC	Cell Console ソフトウェア コマンド行インタフェースを含みます。
--------	---

4. これらのコンポーネントのインストールが終了したら、次に rpm コマンドを使用して、リモート インストールする各統合パッケージに必要なプッシュ パッケージをインストールします。以下に例を示します。

OB2-INTGP	Data Protector コア統合ソフトウェア。このコンポーネントは、統合ソフトウェアをインストールする場合に必要です。
OB2-SAPP	SAP 用統合ソフトウェア コンポーネント
OB2-SAPDBP	SAP DB 用統合ソフトウェア コンポーネント
OB2-INFP	Informix 用統合ソフトウェア コンポーネント
OB2-LOTP	Lotus Notes/Domino 用統合ソフトウェア コンポーネント
OB2-SYBP	Sybase 用統合ソフトウェア コンポーネント
OB2-OR8P	Oracle 用統合ソフトウェア コンポーネント
OB2-DB2P	DB2 用統合ソフトウェア コンポーネント
OB2-EMCP	EMC Symmetrix 用統合ソフトウェア コンポーネント
OB2-SNAPP	HP StorageWorks Virtual Array
OB2-SMISAP	HP StorageWorks Enterprise Virtual Array
OB2-SSEAP	HP StorageWorks Disk Array XP
OB2-NDMPP	NDMP Media Agent ソフトウェア
OB2-OVP	OpenView 用統合ソフトウェア コンポーネント
OB2-FRAP	フランス語ローカライズ パッケージ
OB2-JPNP	日本語ローカライズ パッケージ

インストールが終了すると、UNIX 用のソフトウェア デポは、
/opt/omni/databases/vendor ディレクトリにインストールされます。

重要 ネットワーク上に UNIX 用のインストール サーバをインストールしない場合は、UNIX インストール DVD-ROM を使用して、すべての UNIX クライアントをローカルにインストールしなければなりません。

5. メイン rpm アーカイブの展開に rpm を使用した場合は、次のコマンドで OB2-CM パッケージを削除します。

```
rpm -e OB2-CM
```

重要 Data Protector は、たとえば次のようなリンク ディレクトリにインストールすることができます。

```
/opt/omni/ -> /<prefix>/opt/omni/
```

```
/etc/opt/omni/ -> /<prefix>/etc/opt/omni/
```

```
/var/opt/omni/ -> /<prefix>/var/opt/omni/
```

このようにする場合は、インストール前にリンクを作成しておき、インストール先ディレクトリが存在することを確認しておかなければなりません。

この次に行う作業

この時点で、UNIX 用のインストール サーバがネットワーク上にすでにインストールされていないなければなりません。準備が整ったら、以下の作業を行います。

1. (Cell Manager とは別のシステムに) 独立した形でインストール サーバをセットアップした場合は、このシステムを Data Protector セルに手作業で追加 (インポート) しなければなりません。詳細は 187 ページの「セルへのインストール サーバのインポート」を参照してください。

注記 インストール サーバをインポートすると、Cell Manager 上の /etc/opt/omni/server/cell/installation_servers ファイルが更新されて、インストールしたプッシュ パッケージが反映されます。CLI からこのファイルを使用して、使用可能なプッシュ パッケージを確認できます。このファイルを最新状態に保つために、プッシュ パッケージをインストールまたは

ネイティブ ツールを使用した、HP-UX、Solaris、および Linux システムへのインストール

削除したときは、インストール サーバのエクスポートと再インポートを必ず実行してください。これは、インストール サーバを Cell Manager と同じシステムにインストールしてある場合も同様です。

2. Data Protector セルに Windows システムが含まれている場合は、Windows 用のインストールサーバをインストールする必要があります。詳細は 41 ページの「Windows 用のインストールサーバのインストール」を参照してください。
3. ソフトウェアをクライアントに配布します。詳細は 46 ページの「Data Protector クライアントのインストール」を参照してください。

クライアントのインストール

Cell Manager やインストール サーバのインストール中には、クライアントはインストールされません。クライアントは、`omnisetup.sh` コマンドを使用するか、Data Protector GUI からインストール コンポーネントをプッシュしてインストールする必要があります。クライアントのインストール方法の詳細は、46 ページの「Data Protector クライアントのインストール」を参照してください。

ネイティブ ツールを使用した HP-UX システムと Solaris システムでのアップグレード

swinstall を使用した HP-UX システムでの Data Protector のアップグレード

Cell Manager のアップグレードは、UNIX インストール DVD-ROM から実行する必要があります。

インストール サーバもインストールされている Cell Manager をアップグレードする場合には、最初に Cell Manager をアップグレードし、次にインストール サーバをアップグレードする必要があります。

Cell Manager システムにインストールされているクライアント コンポーネントは、Cell Manager のアップグレード中にはアップグレードされません。omnisetup.sh を使用するか、インストール サーバからインストール コンポーネントをプッシュして、アップグレードする必要があります。詳細は 119 ページの「UNIX クライアントのローカル インストール」または 50 ページの「Data Protector クライアントのリモート インストール」を参照してください。

アップグレード手順

Data Protector A.05.00、A.05.10 または A.05.50 を Data Protector A.06.00 にアップグレードするには、swinstall を使用し、以下の手順に従ってください。

1. root でログインし、/opt/omni/sbin/omnisv -stop コマンドを実行して、Cell Manager 上の OmniBack II サービスまたは Data Protector サービスをシャットダウンします。

```
ps -ef | grep omni
```

 コマンドを実行して、すべてのサービスがシャットダウンされているかどうかを確認します。ps -ef | grep omni コマンドの出力結果には、OmniBack II サービスまたは Data Protector サービスは表示されないはずです。

2. Cell Manager をアップグレードする場合は B-3 ページの「swinstall を使用した HP-UX システムへの Cell Manager のインストール」、インストール サーバをアップグレードする場合は B-8 ページの「HP-UX システムへのインストール サーバのインストール」に説明されている手順に従います。

インストール手順では、旧バージョンが自動的に検出され、**選択されたコンポーネントのみ**がアップグレードされます。旧バージョンの Data Protector にインストールされていたコンポーネントが選択されなかった場合、そのコンポーネントのアップグレードは**実行されません**。そのため、アップグレードの必要のあるすべてのコンポーネントを選択しなければなりません。

注記

同じシステム上で Cell Manager とインストール サーバの両方をアップグレードする場合、[Match what target has] オプションはサポートされません。

pkgadd を使用した Solaris システムでの Data Protector のアップグレード

Solaris 用 Cell Manager またはインストール サーバをアップグレードする場合は、製品の旧バージョンをアンインストールしてから、新しいバージョンをインストールします。

Cell Manager システムにインストールされているクライアント コンポーネントは、Cell Manager のアップグレード中にはアップグレードされません。omnisetup.sh を使用するか、インストール サーバからインストール コンポーネントをプッシュして、アップグレードする必要があります。詳細は 119 ページの「UNIX クライアントのローカル インストール」または 50 ページの「Data Protector クライアントのリモート インストール」を参照してください。

アップグレード手順

Data Protector A.05.00 または A.05.10 を Data Protector A.05.50 にアップグレードするには、pkgadd を使用し、以下の手順に従ってください。

1. root でログインし、/opt/omni/sbin/omnisv -stop コマンドを実行して、Cell Manager 上の OmniBack II サービスまたは Data Protector サービスをシャットダウンします。

ps -ef | grep omni コマンドを実行して、すべてのサービスがシャットダウンされているかどうかを確認します。ps -ef | grep omni コマンドの出力結果には、OmniBack II サービスまたは Data Protector サービスは表示されないはずです。

2. pkgrm を使用して Data Protector をアンインストールします。

このユーティリティでは、構成ファイルおよびデータベースは、現在の状態のまま維持されます。

3. pkginfo コマンドを実行し、旧バージョンの Data Protector のアンインストールが完了していることを確認します。Data Protector の旧バージョンは、表示されないはずです。

データベースと構成ファイルが存在していることを確認します。以下のディレクトリが存在し、バイナリが含まれているはずです。

- /opt/omni
- /var/opt/omni
- /etc/opt/omni

4. Cell Manager をアップグレードする場合、UNIX インストール DVD-ROM をドライブに挿入してマウントします。次に、pkgadd を使用して、Cell Manager をインストールします。詳細な作業手順は、B-5 ページの「pkgadd を使用した Solaris システムへの Cell Manager のインストール」を参照してください。

インストール サーバをアップグレードする場合、UNIX インストール DVD-ROM をドライブに挿入してマウントし、インストール サーバをインストールします。詳細な作業手順は、B-8 ページの「pkgadd を使用した Solaris システムへのインストール サーバのインストール」を参照してください。

注記

Solaris 9 上で Cell Manager をアップグレードした場合は、アップグレード完了後にインストール サーバを使用して Cell Manager 上に Disk Agent をリモート インストールすることができます。詳細については、50 ページの「Data Protector クライアントのリモート インストール」を参照するか、または ob2install のマンページを参照してください。

Windows システム上の TCP/IP プロトコルのセットアップ

重要 サポートされているのは、Microsoft によって実装された TCP/IP プロトコルのみです。

Data Protector では、TCP/IP プロトコルを使ってネットワーク通信が行われます。したがって、セル内の各クライアントに TCP/IP プロトコルをインストールし、正しく構成しておく必要があります。

Data Protector ユーザー インタフェースからコマンドを入力したときには、TCP/IP プロトコルを介して Cell Manager への接続が確立されます。

TCP/IP プロトコルは、ネットワーク通信用のプロトコル一式およびユーティリティで構成されます。このプロトコルは、TCP (Transmission Control Protocol) と IP (Internet Protocol) を組み合わせたものです。

このプロトコルを使用する各コンピュータのハード ディスクには、TCP/IP ソフトウェアをインストールしておく必要があります。さらに、各コンピュータに以下のアドレスを割り当てておく必要があります (アドレスの割り当ては、通常、ネットワーク管理者が行います)。

- コンピュータ上にインストールされている各ネットワーク アダプタ カードの **IP アドレス**。これは 32 ビットの数字で、通常はドット区切りのクアド形式またはドット区切りの 10 進形式で表されます。
- コンピュータ上にインストールされている各ネットワーク アダプタ カードの **サブネット マスク**。サブネット マスクを **IP アドレス** と組み合わせることによって、ネットワーク ID およびホスト ID が定義されます。**サブネット マスク** は、**IP アドレス** と同じ形式で表されます。
- デフォルトのローカル ゲートウェイ (**IP ルーター**) からインターネットにアクセスできるようにするには、**デフォルト ゲートウェイ アドレス** が必要です。

前提条件

Windows コンピュータに TCP/IP プロトコルをインストールする前に、以下のことがらに注意してください。

- コンピュータにインストールされている Windows ソフトウェアの種類によって、構成可能なオプションが異なります。

Windows システム上の TCP/IP プロトコルのセットアップ

Windows Server コンピュータは、特に、DHCP (動的ホスト構成プロトコル) サーバ、Windows インターネット ネーム サービス (WINS) サーバ、またはドメイン ネーム システム (DNS) サーバとして構成できます。詳細は、Windows のオンライン ヘルプを参照してください。

- ネットワーク上に DHCP サーバがインストールされている場合は、DHCP を使用して TCP/IP プロトコルを自動構成できます。

ネットワーク上に DHCP サーバがない場合や、DHCP サーバ コンピュータ上で TCP/IP プロトコルを構成する場合は、TCP/IP プロトコルを手作業で構成する必要があります。詳細は、Windows のオンライン ヘルプを参照してください。

- TCP/IP を手作業で構成するには、ローカル コンピュータの管理者グループのメンバーとしてログオンする必要があります。アドレスの重複を防止するために、すべての値をネットワーク管理者から取得してください。前述の IP アドレス、サブネット マスク、デフォルト ゲートウェイに加えて、以下のものを取得する必要があります。
 - ✓ DNS サービスを使用する場合は、DNS ドメインの名前と DNS サーバの IP アドレスが必要です。
 - ✓ ネットワーク上の WINS サーバを利用する場合は、WINS サーバの IP アドレスが必要です。

Windows への TCP/IP プロトコルのインストールと構成

Windows システムへの TCP/IP プロトコルのインストールは、オペレーティング システムのインストール中に行われます。

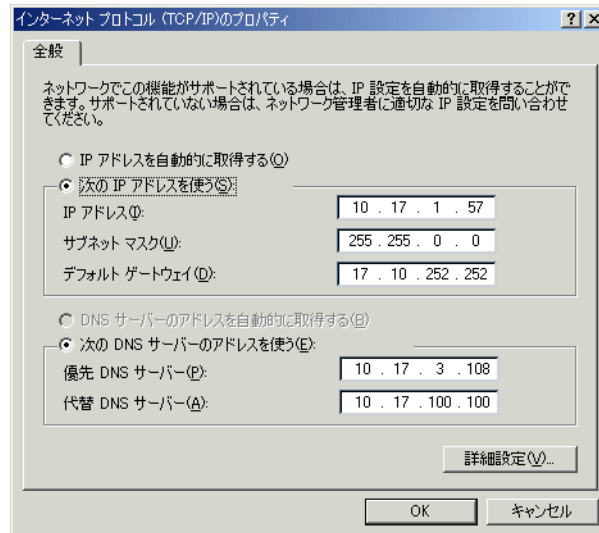
Windows 2000 システムの現在の TCP/IP 設定を確認する場合は、以下の手順に従ってください。

1. Windows の [コントロールパネル] で、[ネットワークとダイヤルアップ接続]、[ローカル エリア接続] を順にダブルクリックします。

Windows システム上の TCP/IP プロトコルのセットアップ

2. [プロパティ] をクリックし、[インターネット プロトコル (TCP/IP)] をダブルクリックします。ここで、IP 設定を編集できます。

図 B-2 Windows の [TCP/IP プロパティ] ウィンドウ



Windows システム上の TCP/IP プロトコルのセットアップ

詳細設定を編集するには、[詳細設定] をクリックします。

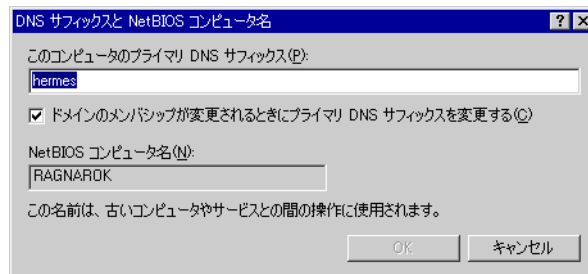
図 B-3 Windows での TCP/IP の詳細設定



DNS サフィックス

Windows 2000 システムの DNS サフィックスを構成する場合は、デスクトップの [マイ コンピュータ] を右クリックし、[プロパティ]、[ネットワーク ID]、[プロパティ]、[詳細] の順に選択します。DNS の新しい設定は、システムの再起動後に有効になります。

図 B-4 Windows の DNS サフィックスと NetBIOS コンピュータ名



TCP/IP 設定をチェックする

TCP/IP プロトコルは、ホスト名を正しく解決できるようにセットアップする必要があります。

- `<%SystemRoot%>%system32%drivers%etc` フォルダにある `hosts` ファイルを使用する場合は、Cell Manager および Media Agent とバックアップ デバイスをインストールしたすべてのシステムのアドレスをセル内の各システムから解決できるようにセットアップしておく必要があります。さらに、Cell Manager から、セル内のすべてのシステムの名前を解決できるようにセットアップする必要があります。
- DNS を使用する場合は、ローカル DNS サーバが適切に構成され、セル内の各システムの IP 設定値に指定されていることを確認してください。

TCP/IP プロトコルのインストール後、TCP/IP 設定を確認するには、`ping` ユーティリティおよび `ipconfig` ユーティリティを使用します。TCP/IP 設定を変更した場合は、まず、コンピュータを再起動してください。

1. コマンド行に `ipconfig /all` と入力すると、ネットワーク アダプタに設定したアドレス設定および TCP/IP 構成に関する詳細情報が表示されます。IP アドレスとサブネット マスクが正しく設定されていることを確認してください。
2. `ping <your_IP_address>` と入力すると、TCP/IP ソフトウェアのインストールおよび構成状況が表示されます。デフォルトでは、4 つのエコー パケットが表示されます。
3. `ping <default_gateway>` と入力します。

ゲートウェイは、サブネット上に存在していなければなりません。ゲートウェイへの `ping` に失敗した場合は、ゲートウェイの IP アドレスが正しく設定されているかどうか、およびゲートウェイが正常に動作しているかどうかを確認してください。

4. 上記の各チェックで問題がなければ、名前の解決メカニズムをテストします。システム名を指定して `ping` コマンドを実行し、`hosts` ファイルと DNS の一方または両方をテストしてください。

たとえば、マシン名が `kesukozi` で、ドメイン名が `campo.com` の場合は、`ping kesukozi.campo.com` と入力します。

これが正常に動作しなかった場合は、[TCP/IP 詳細設定] ウィンドウにアクセスしてください。方法については、B-20 ページの「Windows への TCP/IP プロトコルのインストールと構成」を参照してください。このウィンドウでは、ドメイン名が正しいかどうかをチェックします。また、`hosts` ファイルと DNS もチェックしてください。

Cell Manager となるシステムおよびクライアントとなるシステムに対して、以下の 2 つの方法で、名前が正しく解決されることを確認してください。

- Cell Manager から各クライアントに対して、`ping` コマンドを実行します。

Windows システム上の TCP/IP プロトコルのセットアップ

- 各クライアントから、Cell Manager と、Media Agent がインストールされている他のクライアントに対して、ping コマンドを実行します。

名前の解決に hosts ファイルを使用する場合、前述のテストでは、名前の解決が正しく動作するかどうかは保証されません。このような場合は、Data Protector のインストール後に **DNS チェック ツール**を使用する方法があります。

重要

前述の方法で名前が解決されなかった場合は、Data Protector が適切にインストールされていない可能性があります。

コンピュータ名はホスト名と同じ名前にしてください。同じ名前でない場合は、Data Protector をセットアップする際、警告が表示されます。

ホスト名を確認する場合は、[TCP/IP プロパティ] ウィンドウにアクセスしてください。方法の詳細は、B-20 ページの「Windows への TCP/IP プロトコルのインストールと構成」を参照してください。

5. Data Protector をインストールし、Data Protector セルを作成した後、DNS チェック ツールを使用して、Cell Manager、および Media Agent がインストールされている各クライアントから、同じセル内の他のすべてのクライアントへの DNS 接続、およびその逆の DNS 接続が解決されるかどうかを確認できます。この確認を行うには、<Data_Protector_home>%bin ディレクトリから omnichk -dns コマンドを実行します。詳細は 322 ページの「Data Protector セル内の DNS 接続の確認」を参照してください。

omnichk コマンドの詳細は、『HP OpenView Storage Data Protector Command Line Interface Reference』を参照してください。

MS Proxy

MS Proxy がインストールされていると、これによってポート番号 5555 が使用されるため、Data Protector サービスは失敗します。以下の手順で問題を解決してください。

1. <Data_Protector_home>%bin ディレクトリに、wspcfg.ini, という名前のファイルを作成します。
2. ファイルに以下の行を追加してください。

```
[OmniInet]
```

```
Disable=1
```

Cell Manager 名の変更

Data Protector のインストール時には、Cell Manager 名として現在のホスト名が使用されます。Cell Manager のホスト名を変更する場合は、Data Protector ファイルを手作業で更新する必要があります。

重要 Cell Manager 名に関するクライアント情報を更新する必要があります。Cell Manager のホスト名を変更する前に、クライアントをセルからエクスポートしてください。作業手順は、192 ページの「セルからのクライアントのエクスポート」を参照してください。ホスト名を変更したら、クライアントを再びセルにインポートします。手順の詳細は、185 ページの「セルへのクライアントのインポート」を参照してください。

注記 元の Cell Manager 名を使用して構成されたデバイスやバックアップ仕様には、現在の名前を反映させる必要があります。

UNIX の場合

UNIX 用 Cell Manager では、以下の操作を行ってください。

1. 以下のファイルにある Cell Manager のホスト名のエントリを変更します。

```
/etc/opt/omni/client/cell_server
/etc/opt/omni/server/cell/cell_info
/etc/opt/omni/server/users/UserList
```
2. Data Protector セルのメンバー間で、名前の解決が適切に行われるかどうかを確認します。
3. 以下のコマンドを実行して IDB の Cell Manager 名を変更します。

```
/opt/omni/sbin/omnidbutil -change_cell_name [<old_host>]
```

Windows の場合

Windows 用 Cell Manager で、以下の操作を行ってください。

1. 以下のファイルにある Cell Manager のホスト名のエントリを変更します。

<Data_Protector_home>%config%server%cell%cell_info

<Data_Protector_home>%config%server%users%userlist

- レジストリ キー %HKEY_LOCAL_MACHINE%SOFTWARE%Hewlett-Packard%
OpenView%OmniBack II%Site%CellServer で Cell Manager 名を変更します。

デフォルトのポート番号の変更

Data Protector Inet サービス (プロセス) は、バックアップと復元に必要な他のプロセスを起動するサービスですが、セル内の各システムで同じポート番号を使用する必要があります。

Data Protector では、デフォルトでポート番号 5555 が使われます。同じポート番号が他のプログラムに使用されていないかどうかをチェックするには、`/etc/services` ファイルの内容を調べるか (UNIX の場合)、または、`netstat -a` コマンドを実行します (Windows の場合)。ポート番号 5555 が他のプログラムに使用されている場合は、他の未使用のポート番号に変更する必要があります。このポート番号がクライアントシステム上でのみ使用不能な場合は、Cell Manager をインストールした後でポート番号を変更できます。Cell Manager のインストール先となるシステムでこのポート番号が使用不能な場合は、インストール前にポート番号を変更する必要があります。

UNIX

UNIX システム上でポート番号を変更するには、以下の手順に従ってください。

- Cell Manager をインストールする前に、以下の手順を実行します。
 - 必要なポート番号で、`/tmp/omni_tmp/socket.dat` ファイルを作成します。
- Cell Manager をインストールした後で、以下の手順を実行します。
 1. `/etc/services` ファイルを編集します。このファイルには、デフォルトで次のエントリが含まれています。

```
omni 5555/tcp # DATA-PROTECTOR
```

番号 5555 を未使用のポート番号に変更します。
 2. `kill -HUP <inetd_pid>` コマンドを使用して関連プロセスを停止することによって、Inet サービスを再起動します。プロセス ID (`inetd_pid`) を特定するには、`ps -ef` と入力します。

Windows

Windows システム上でポート番号を変更するには、以下の手順に従ってください。

- Cell Manager をインストールする前に、以下の手順を実行します。
 1. コマンド行から `Regedit.exe` を実行して、**レジストリ エディタ**を開きます。

2. レジストリ エントリ InetPort を、キー
HKEY_LOCAL_MACHINE¥SOFTWARE¥Hewlett-Packard¥
OpenView¥OmniBackII¥Common の下に作成します。

レジストリ エントリ の名前 : InetPort

レジストリ エントリ の種類 : REG_SZ (string)

レジストリ エントリ の値 : <port_number>

- Cell Manager をインストールした後で、以下の手順を実行します。
 1. コマンド行から Regedit.exe を実行して、**レジストリ エディタ**を開きます。
 2. [HKEY_LOCAL_MACHINE]、[Software]、[Hewlett-Packard]、[OpenView]、
[OmniBack II] の順に展開し、[Common] を選択します。
 3. [InetPort] をダブルクリックして、[**文字列の編集**] ダイアログ ボックスを開きます。
[**値のデータ**] テキスト ボックスに、未使用のポート番号を入力します。[Common]
フォルダの [Parameters] サブフォルダについても同様の手順を繰り返します。
 4. Windows コントロールパネルの [**管理ツール**] - [**サービス**] から、[Data Protector
Inet] サービスを選択し、サービスを再起動します (ツールバーの [**サービスの再起動**]
アイコンをクリックします)。

NIS サーバの準備

ここでは、NIS サーバに Data Protector Cell Manager を認識させるための手順を説明します。

NIS サーバに Data Protector の情報を追加するには、以下の手順に従ってください。

1. NIS サーバに root ユーザーとしてログインします。
2. /etc/services ファイルを NIS 経由で管理する場合は、/etc/services ファイルに次の行を追加します。

```
omni 5555/tcp # Data Protector for Data Protector inet server
```

ポート 5555 を使用できない場合は、5555 を別の値に置き換えてください。詳細は B-28 ページの「デフォルトのポート番号の変更」を参照してください。

/etc/inetd.conf ファイルを NIS 経由で管理する場合は、/etc/inetd.conf ファイルに次の行を追加します。

```
#Data Protector
```

```
omni stream tcp nowait root /opt/omni/sbin/inet -log  
/var/opt/omni/log/inet.log
```

3. 以下のコマンドを実行します。これにより NIS サーバがファイルを読み込み、構成を更新します。

```
cd /var/yp; make
```

注記

NIS 環境では、複数の異なる構成ファイルを使用する順序を nsswitch.conf ファイルで定義します。たとえば、/etc/inetd.conf ファイルをローカルマシン上で使用するか、それとも NIS サーバから使用するかを定義できます。また、名前の保存場所を nsswitch.conf で制御するように指定するステートメントをファイルに挿入することもできます。詳細は、マンページを参照してください。

Data Protector をすでにインストールしている場合は、まず NIS サーバを準備し、次に、Data Protector クライアントでもあるすべての NIS クライアント上で kill -HUP <pid> コマンドを実行して関連プロセスを停止することにより、inet サービスを再起動します。

トラブルシューティング

NIS環境にData ProtectorをインストールしてもData Protector Inetサービスを開始できない場合は、`/etc/nsswitch.conf` ファイルをチェックします。

次の行が含まれていないか確認してください。

```
services: nis [NOTFOUND=RETURN] files
```

この行が含まれている場合は、以下のように変更します。

```
services: nis [NOTFOUND=CONTINUE] files
```

Windows でのテープ ドライバおよびロボティクス ドライバの使用

Data Protector では、Windows システムに接続されたテープ ドライブ用としてデフォルトでロードされるネイティブ テープ ドライバをサポートしています。ただし、メディアチェンジャ (ロボティクス) デバイス用としてロードされる Windows のネイティブ ドライバは、Data Protector ではサポートされていません。

以下の例では、Windows システムに HP 4mm DDS テープ デバイスが接続されている場合を想定しています。HP 4mm DDS テープ デバイスを Windows システムに接続して Data Protector で使用できるように構成する場合は、メディアチェンジャ デバイス用にロードされるネイティブ ドライバを無効化する必要があります。ここでは、関連する手順について説明します。

テープ ドライバ

Windows には、Hardware Compatibility List (HCL) に記載されているデバイスが、ドライバとして含まれています。HCL とは Windows でサポートされるデバイスのリストです。詳細は以下のサイトを参照してください。

<http://www.microsoft.com/whdc/hcl/default.mspx>

コンピュータが起動すると、デバイスドライバは使用可能なデバイスすべてに自動的にロードされます。更新はこれで完了です。ネイティブ テープ ドライバを個別にロードする必要はありません。

Windows システム上でネイティブ テープ ドライバを更新するか置き換える場合は、以下の手順に従ってください。

1. Windows の [コントロールパネル] で、[管理ツール] をダブルクリックします。
2. [管理ツール] ウィンドウで [コンピュータの管理] をダブルクリックします。続いて、[デバイス マネージャ] をクリックします。
3. [テープ ドライブ] を展開します。現在デバイスに接続されているドライバを確認するには、テープドライブ名を右クリックし、[プロパティ] をクリックします。
4. [ドライバ] タブを選択し、[ドライバの更新] をクリックします。B-33 ページの図 B-5 を参照してください。現在インストールされているネイティブ テープ ドライバを更新するか、別のドライバに置き換えるかを、ウィザードで指定できます。

5. システムを再起動して、変更した設定を反映させます。

図 B-5 ドライバのプロパティ



重要

ドライバがネイティブ テープ ドライバを使用しないで Data Protector 用として構成されている場合は、そのテープ ドライブを参照しているすべての構成済み Data Protector バックアップ デバイス名を変更する必要があります。たとえば、scsi1:0:4:0 から tape3:0:4:0 のような変更が必要になります。

詳細は B-35 ページの「Windows 上でのデバイス ファイル (SCSI アドレス) の作成」を参照してください。

ロボティクス ドライバ

Windows では、使用可能なテープ ライブラリに対するロボティクス ドライバが自動的にロードされます。Data Protector でライブラリ ロボティクスを使用するには、対応するドライバを無効化する必要があります。

Windows でのテープ ドライバおよびロボティクス ドライバの使用

ここでは、4mm DDS テープを使用する HP 1557A テープ ライブラリを例に取り上げます。Windows システムで自動的にロードされるロボティクス ドライバ (ddsmc.sys) を無効にするには、以下の手順に従ってください。

1. Windows の [コントロールパネル] で、[管理ツール] をダブルクリックします。
2. [管理ツール] ウィンドウで [コンピュータの管理] をダブルクリックします。続いて、[デバイス マネージャ] をクリックします。
3. [デバイス マネージャ] ウィンドウの結果エリアで、[メディア チェンジャ] を展開します。
4. 現在ロードされているドライバを確認するには、[4mm DDS メディア チェンジャ] を右クリックし、[プロパティ] をクリックします。

[ドライバ] タブを選択し、[ドライバの詳細] をクリックします。以下のウィンドウが表示されます。

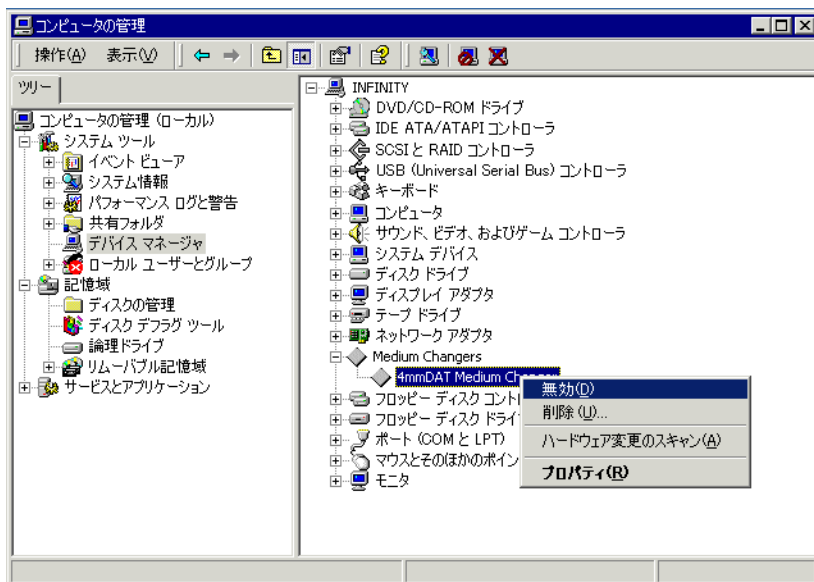
図 B-6 メディア チェンジャのプロパティ



Windows でのテープ ドライバおよびロボティクス ドライバの使用

ネイティブ ロボティクス ドライバを無効にするには、[4mm DDS メディア チェンジャ] を右クリックし、[無効] を選択してください。

図 B-7 ロボティクス ドライバの無効化



5. システムを再起動して、変更した設定を反映させます。これで、ロボティクスを Data Protector 用に構成できるようになります。

Windows 上でのデバイス ファイル (SCSI アドレス) の作成

テープ デバイス ファイル名の構文は、ネイティブ テープ ドライバをテープ ドライブに対してロード (tapeN:B:T:L) またはアンロード (scsiP:B:T:L) するかによって異なります。

ネイティブ テープ ドライバを使用する Windows

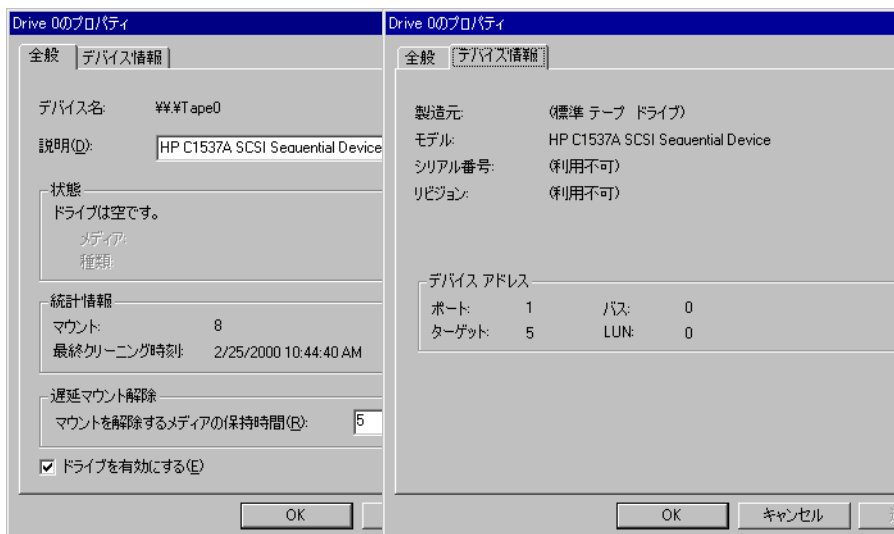
Windows システムに接続され、ネイティブ テープ ドライバを使用するテープ ドライブに対してデバイス ファイルを作成するには、以下の手順に従ってください。

1. Windows の [コントロールパネル] で、[管理ツール] をダブルクリックします。

Windows でのテープ ドライバおよびロボティクス ドライバの使用

2. [管理ツール] ウィンドウで [コンピュータの管理] をダブルクリックします。[リムーバブル記憶域]、[物理的な場所] を順に展開します。テープドライブを右クリックし、[プロパティ] を選択します。
3. ネイティブ テープドライブをロードしている場合、デバイス ファイル名は、プロパティ ページの [全般] に表示されます。または、プロパティ ページの [デバイス情報] で関連する情報を確認することができます。B-36 ページの図 B-8 を参照してください。

図 B-8 テープ ドライブ プロパティ



B-36 ページの図 B-8 のテープ ドライブのファイル名は、以下のように作成されます。

ネイティブ テープドライブを使用している場合 Tape0 または Tape0:0:5:0

ネイティブ テープドライブを使用していない場合 scsi1:0:5:0

光磁気デバイス

Windows システムに光磁気デバイスを接続する場合、ドライブ名は、システムを再ブートした後でデバイスに割り当てられます。デバイスファイルを作成した際は、このドライブ名が使用されます。たとえば、ドライブ名 E を割り当てた光磁気ドライブに対してデバイス ファイルを作成した場合、このデバイス ファイルには E: が使用されます。

HP-UX 上の SCSI ロボティクス構成

HP-UX システムでは、SCSI パス スルードライバを使ってテープ ライブラリ デバイス (HP StorageWorks 12000e など) の SCSI コントローラと制御デバイスの両方を管理します (なお制御デバイスは、「ロボティクス」または「ピッカー」とも呼ばれます)。ライブラリの制御デバイスは、ライブラリ内の個々のドライブに対するメディアのロードとアンロード、および、ライブラリ デバイスに対するメディアのインポートとエクスポートを制御します。

図 B-9 SCSI 制御デバイス

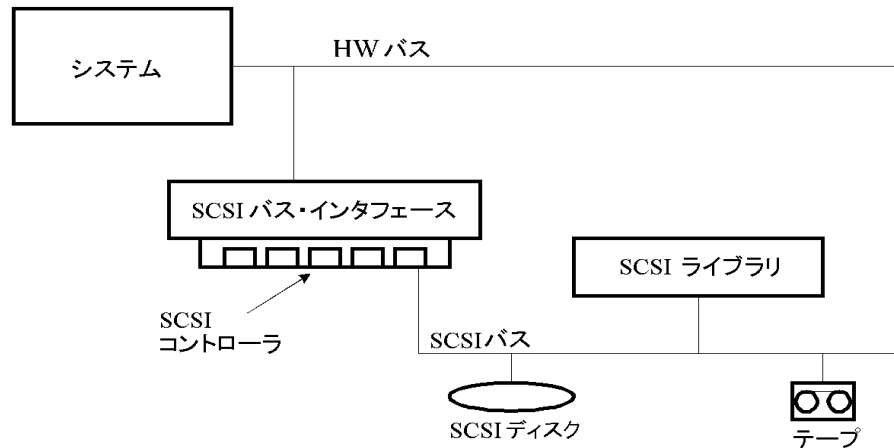
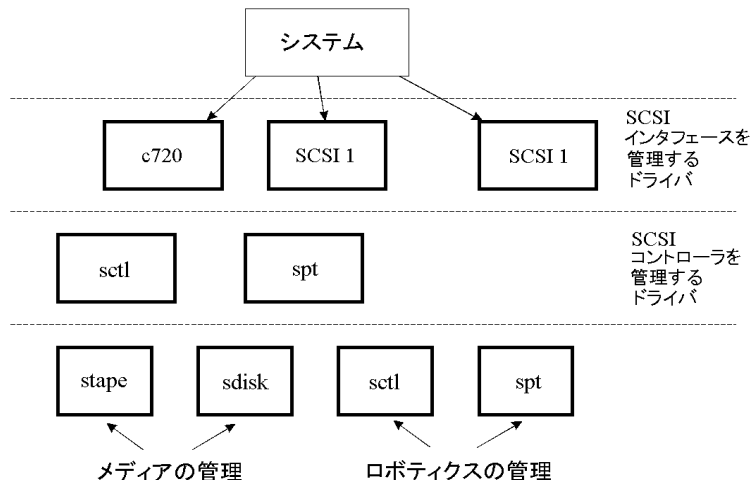


図 B-10 デバイスの管理



SCSI ロボティクスドライバの種類は、ハードウェアに応じて使い分けます。GSC/HSC または PCI バスを搭載しているシステムの場合は SCSI オートチェンジャドライバ `schgr` が、EISA バスを搭載しているシステムの場合は SCSI パススルードライバ `sctl` が、それぞれ事前にカーネルに組み込まれています。ただし、NIO バスを搭載した HP サーバの場合は、`spt` という名前の SCSI パススルードライバを使用します。このドライバは、デフォルトでシステムにインストールされていますが、カーネルには組み込まれていません。

SCSI ロボティクスドライバがカレントカーネルにまだリンクされていない場合は、手作業で追加して、接続されているテープライブラリのロボティクスに割り当てる必要があります。

SCSI ロボティクスドライバを手作業でカーネルに追加して再ビルドするには、以下の手順に従ってください。

ヒント HP-UX プラットフォームの場合、カーネルは、*HP System Administration Manager (SAM)* ユーティリティでビルドすることもできます。第 2 章の 68 ページの「HP-UX クライアントのインストール」を参照してください。

目的のライブラリに SCSI ロボティクスドライバがすでに割り当てられているかどうかをチェックするには、`/opt/omni/sbin/ioscan -f` コマンドを使います。

図 B-11 SCSI パス スルードライバ (sctl) のステータス

```

root@superhik$ ioscan -f
Class      I  H/W Path      Driver      S/W State H/W Type  Description
-----
bc         0          root        CLAIMED    BUS_NEXUS
bc         1  8          ccio        CLAIMED    BUS_NEXUS  I/O Adapter
unknown   -1  8/0        c720        CLAIMED    DEVICE      GSC-to-PCI Bus Bridge
ext_bus    0  8/12       c720        CLAIMED    INTERFACE  GSC Fast/Wide SCSI Interfac
e
target     0  8/12.0     tgt         CLAIMED    DEVICE
disk       0  8/12.0.0   sdisk      CLAIMED    DEVICE      SEAGATE ST19171W
target     1  8/12.1     tgt         CLAIMED    DEVICE
tape       5  8/12.1.0   stape      CLAIMED    DEVICE      QUANTUM DLT7000
target     2  8/12.2     tgt         CLAIMED    DEVICE
ctl        0  8/12.2.0   sctl       CLAIMED    DEVICE      EXABYTE EXB-210
target     3  8/12.7     tgt         CLAIMED    DEVICE
ctl        0  8/12.7.0   sctl       CLAIMED    DEVICE      Initiator
ba         0  8/16       bus_adapter CLAIMED    BUS_NEXUS  Core I/O Adapter
ext_bus    2  8/16/0     CentIf     CLAIMED    INTERFACE  Built-in Parallel Interface
audio      0  8/16/1     audio      CLAIMED    INTERFACE  Built-in Audio
tty        0  8/16/4     asio0      CLAIMED    INTERFACE  Built-in RS-232C
ext_bus    1  8/16/5     c720        CLAIMED    INTERFACE  Built-in SCSI
target     4  8/16/5.2   tgt         CLAIMED    DEVICE
disk       2  8/16/5.2.0 sdisk      CLAIMED    DEVICE      TOSHIBA CD-ROM XM-5401TA
target     7  8/16/5.3   tgt         NO_HW      DEVICE
tape       3  8/16/5.3.0 stape      NO_HW      DEVICE      SONY SDX-300C
target     6  8/16/5.5   tgt         NO_HW      DEVICE
tape       0  8/16/5.5.0 stape      NO_HW      DEVICE      SONY SDX-300C
target     5  8/16/5.7   tgt         CLAIMED    DEVICE

```

B-39 ページの図 B-11 に示す例では、SCSI パス スルードライバ `sctl` が Exabyte テープ デバイスの制御デバイスに割り当てられています。対応するハードウェアパス (H/W Path) は、`8/12.2.0` (SCSI=2, LUN=0) です。

同じ SCSI バスに接続されているテープドライブがありますが、このテープドライブを制御しているドライバは `stape` です。対応するハードウェアパス (H/W Path) は、`8/12.1.0` (SCSI=0, LUN=0) です。

重要

SCSI アドレス 7 は SCSI コントローラが常時使用しています。ただし、`ioscan -f` コマンドによる出力には、それを示す行は表示されません。上記の例では、SCSI コントローラは `sct1` によって管理されています。

図 B-12 SCSI パス スルー ドライバ `spt` のステータス

```
# ioscan -f
-----
Class      I  H/W Path  Driver  S/W State H/W Type  Description
-----
bc          0          root    CLAIMED  BUS_NEXUS
ext_bus    0  52        scsil   CLAIMED  INTERFACE HP 28655A - SCSI Interface
target     4  52.1      target  CLAIMED  DEVICE
disk       4  52.1.0    disc3   CLAIMED  DEVICE  SEAGATE ST15150N
target     1  52.2      target  CLAIMED  DEVICE
disk       0  52.2.0    disc3   CLAIMED  DEVICE  TOSHIBA CD-ROM XM-4101TA
target     3  52.4      target  CLAIMED  DEVICE
tape       0  52.4.0    tape2   CLAIMED  DEVICE  HP C1533A
spt        1  52.4.1    spt     CLAIMED  DEVICE  HP C1553A
target     6  52.5      target  CLAIMED  DEVICE
disk       5  52.5.0    disc3   CLAIMED  DEVICE  SEAGATE ST15150N
target     2  52.6      target  CLAIMED  DEVICE
disk       1  52.6.0    disc3   CLAIMED  DEVICE  SEAGATE ST15150N
lanmux     0  56        lanmux0 CLAIMED  INTERFACE LAN/Console
tty        0  56.0      mux4    CLAIMED  INTERFACE
lan        0  56.1      lan3    CLAIMED  INTERFACE
lantty    0  56.2      lantty0 CLAIMED  INTERFACE
processor  0  62        processor CLAIMED  PROCESSOR Processor
memory    0  63        memory  CLAIMED  MEMORY  Memory
# █
```

B-40 ページの図 B-12 に示す例では、ロボティクス付きのテープ デバイスが接続されており、SCSI パス スルー ドライバ `spt` によって制御されています。このデバイスは HP StorageWorks 12000e テープ ライブラリで、SCSI アドレス 4 を割り当てられており、ハードウェアパス 52 で SCSI バスに接続されています。対応するハードウェアパスは、52.4.1 です。ロボティクスには、SCSI パス スルー ドライバ `spt` が正しく割り当てられています。

ロボティクスに `sct1`、`spt`、または `schgr` ドライバが割り当てられていない場合は、ロボティクスのハードウェアパスをシステム ファイル内のドライバステートメントに追加し、カーネルを再ビルドする必要があります。以下の手順に従ってください。

以下は、SCSI ロボティクス ドライバを手作業でカーネルに追加してロボティクスに割り当て、カーネルを手作業で再ビルドする手順を説明したものです。

1. `root` ユーザーとしてログインし、以下のディレクトリに移動します。

```
cd /stand/build
```

2. 以下のコマンドを実行して、既存のカーネルから新しいシステム ファイルを作成します。

```
/usr/sbin/sysadm/system_prep -s system
```

3. どの SCSI ロボティクスドライバがカレント カーネルに組み込まれているかをチェックします。/stand ディレクトリから、以下のコマンドを入力してください。

```
grep <SCSI Robotic Driver> system
```

ここで、<SCSI Robotic Driver>には、spt、sctl、または schgr を指定します。ドライバがカレント カーネルにすでに組み込まれている場合は、対応する行が表示されます。

4. エディタを使って、/stand/build/system ファイルに以下のドライバステートメントを追加します。

```
driver <H/W Path> spt
```

/stand/build/system ファイルに追加するステートメントの <H/W Path>には、デバイスの完全なハードウェアパスを指定します。

HP StorageWorks 12000e テープライブラリの場合には、以下のように入力します。

```
driver 52.4.1 spt
```

同じシステムに複数のライブラリが接続されている場合は、それぞれのライブラリ ロボティクスについて、適切なハードウェアパスを指定するドライバ行を追加する必要があります。

schgr ドライバを構成する場合は、ドライバステートメントに次の行を追加します。

```
schgr
```

5. `mk_kernel -s./system` コマンドを入力して、新しいカーネルをビルドします。
6. 元のシステム ファイルを別の名前で作成し、新しいシステム ファイルを元のシステム ファイルにコピーして上書きします。これにより、新しいシステム ファイルの内容が適用されます。

```
mv /stand/system /stand/system.prev
```

```
mv /stand/build/system /stand/system
```

7. 元のカーネルを別の名前で作成し、新しいカーネルを元のカーネルにコピーして上書きします。これにより、新しいカーネルの内容が適用されます。

```
mv /stand/vmunix /stand/vmunix.prev
```

```
mv /stand/vmunix_test /stand/vmunix
```

8. 新しいカーネルから以下のコマンドを入力して、システムを再ブートします。

```
shutdown -r 0
```

9. システムを再ブートしたら、もう一度 `/usr/sbin/ioscan -f` コマンドを実行して、変更内容が適用されていることを確認します。

HP-UX 上のデバイス ファイルの作成

前提条件

デバイス ファイルを作成する前に、バックアップ デバイスをシステムに接続しておく必要があります。デバイスが正しく接続されているかどうかをチェックするには、`/usr/sbin/ioscan -f` コマンドを使用します。バックアップ デバイスに対するデバイス ファイルを自動的に作成するには、`/usr/sbin/infs -e` コマンドを使用します。

特定のバックアップ デバイスに対応するデバイス ファイルが、システムの初期化処理 (ブート処理) 中または `infs -e` コマンド実行後に作成されていない場合は、そのデバイス ファイルを手作業で作成する必要があります。ライブラリ制御デバイス (ライブラリ ロボティクス) の管理に必要なデバイス ファイルは、通常、手作業で作成する必要があります。

ここでは、HP-UX 11.00 システムに接続された HP StorageWorks 12000e ライブラリ デバイスのデバイス ファイルを作成する例を示します。このテープドライブのデバイス ファイルは、システムの再ブート時に自動的に作成されていますが、制御デバイスのデバイス ファイルは手作業で作成する必要があります。

B-40 ページの図 B-12 は、HP-UX システム上で `ioscan -f` コマンドを実行したときに表示されるリストの例を示したものです。

図 B-13 接続済みデバイスのリスト

```
# ioscan -f
Class      I  H/W Path  Driver   S/W State H/W Type  Description
-----
bc         0           root     CLAIMED  BUS_NEXUS
ext_bus    0  52       scsi1    CLAIMED  INTERFACE HP 28655A - SCSI Interface
target    4  52.1     target   CLAIMED  DEVICE
disk      4  52.1.0   disc3    CLAIMED  DEVICE      SEAGATE ST15150N
target    1  52.2     target   CLAIMED  DEVICE
disk      0  52.2.0   disc3    CLAIMED  DEVICE      TOSHIBA CD-ROM XM-4101TA
target    3  52.4     target   CLAIMED  DEVICE
tape      0  52.4.0   tape2    CLAIMED  DEVICE      HP      C1533A
spt       1  52.4.1   spt      CLAIMED  DEVICE      HP      C1553A
target    6  52.5     target   CLAIMED  DEVICE
disk      5  52.5.0   disc3    CLAIMED  DEVICE      SEAGATE ST15150N
target    2  52.6     target   CLAIMED  DEVICE
disk      1  52.6.0   disc3    CLAIMED  DEVICE      SEAGATE ST15150N
lanmux    0  56       lanmux0  CLAIMED  INTERFACE LAN/Console
tty       0  56.0     mux4     CLAIMED  INTERFACE
lan       0  56.1     lan3     CLAIMED  INTERFACE
lantty    0  56.2     lantty0  CLAIMED  INTERFACE
processor 0  62       processor CLAIMED  PROCESSOR Processor
memory    0  63       memory   CLAIMED  MEMORY      Memory
# █
```

この例の SCSI バス インタフェースは、`scsi1` システム ドライバによって制御されています。これは、SCSI NIO インタフェースです。SCSI NIO バス上のライブラリ ロボティクスにアクセスするには、SCSI パス スルー ドライバ `spt` を使用する必要があります。このドライバは、すでにインストールされており、HP StorageWorks 12000e テープ デバイスのロボティクスに割り当てられています。ハードウェア パスは、52.4.1 です。

注記 SCSI NIO ベースのバス インタフェースを使用しない場合は、`spt` ドライバではなく、`sctl` ドライバが必要になります。

デバイス ファイルを作成するには、SCSI パス スルー ドライバのメジャー番号とマイナー番号を取得しておく必要があります (なお、マイナー番号は、どちらのドライバの場合も共通です)。

`spt`, のメジャー番号を取得するには、以下のシステム コマンドを実行します。

```
lsdev -d spt
```

B-43 ページの図 B-13 の例の場合、このコマンドを実行すると、メジャー番号 75 が返されます。

`sctl` のメジャー番号を取得するには、以下のシステム コマンドを実行します。

```
lsdev -d sctl
```

付録 B

HP-UX 上の SCSI ロボティクス構成

この場合は、コマンドを実行すると、メジャー番号 203 が返されます。

どちらの SCSI パス スルードライバの場合も、共通のマイナー番号は以下の形式をとります。

0xIIITL00

II -> `ioscan -f` の出力に示される SCSI バス インタフェースのインスタンス番号(デバイスそのものの番号ではない)は、リストの 2 番目の列(I の列)に表示されます。この例の場合、インスタンス番号は 0 なので、2 桁の 16 進値 00 を入力する必要があります。

T -> ライブラリ ロボティクスの SCSI アドレス。この例では、SCSI アドレスは 4 なので、4 を入力します。

L -> ライブラリ ロボティクスの LUN 番号。この例では、LUN 番号は 1 なので、1 を入力します。

00 -> 2 桁の 16 進値ゼロ。

デバイス ファイルの作成

デバイス ファイルは、以下のコマンドで作成します。

```
mknod /dev/spt/<devfile_name> c Major # Minor #
```

通常、spt のデバイス ファイルは、`/dev/spt` ディレクトリまたは `/dev/scsi` ディレクトリに保存します。この例の場合、制御デバイス ファイルを `/dev/spt/SS12000e` という名前で保存します。

`/dev/spt` ディレクトリに `SS12000e` という名前のデバイス ファイルを作成するには、以下のように入力します。

```
mknod /dev/spt/SS12000e c 75 0x004100
```

`sct1` のデバイス ファイルを作成して `SS12000e` という名前で `/dev/scsi` ディレクトリに保存するには、以下のように入力します。

```
mknod /dev/scsi/SS12000e c 203 0x004100
```

SCSI コントローラのパラメータの設定

Data Protector ではデバイスのブロック サイズを変更できますが、一部の SCSI コントローラで 64KB を超えるブロック サイズの書き込みを可能にするには、パラメータ設定の変更が必要になる場合があります。

Windows システムで Adaptec SCSI コントローラや Adaptec チップセット搭載の SCSI コントローラのパラメータを設定するには、そのコントローラのレジストリ値を編集します。

1. 次のレジストリ値を設定します。 `¥¥HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥aic78xx¥Parameters¥Device0¥MaximumSGList`

2. 4KB サイズのブロックの数に 1 を加えた DWORD 値を入力します。

$MaximumSGList = (OBBlockSize \text{ in kB} / 4) + 1$

たとえば、260KB までのブロック サイズを有効にするには、MaximumSGList の値を少なくとも $(260 / 4) + 1 = 66$ に設定します。

3. システムを再起動します。

注記 このレジストリ値では、ブロック サイズの上限を設定します。デバイスで実際に使用するブロック サイズは、デバイス構成用の Data ProtectorGUI を使って設定する必要があります。

HP-UX 上の未使用の SCSI アドレスの取得

HP-UX システムに接続したバックアップ デバイスのアクセスと制御は、デバイス ファイルを通じて行い、各物理デバイスに対応するデバイス ファイルが必要です。デバイス ファイルを作成する前に、新しいデバイスに割り当てることができる未使用の SCSI アドレス (ポート) を見つける必要があります。

HP-UX では、`/usr/sbin/ioscan -f` システム コマンドを実行して、すでに使用されている SCSI アドレスのリストを表示することができます。`/usr/sbin/ioscan -f` コマンドの出力リストに含まれていないアドレスは、未使用のアドレスと見なすことができます。

B-46 ページの図 B-14 は、HP-UX 11.x システム上で `/usr/sbin/ioscan -f` コマンドを実行したときに表示されるリストの例を示しています。

図 B-14 HP-UX システム上で実行した `ioscan -f` コマンドの出力

```
# ioscan -f
Class      I  H/W Path  Driver   S/W State H/W Type  Description
-----
bc         0          root    CLAIMED  BUS_NEXUS
ext_bus    0  52        scsil    CLAIMED  INTERFACE HP 28655A - SCSI Interface
target    4  52.1      target   CLAIMED  DEVICE
disk      4  52.1.0    disc3    CLAIMED  DEVICE      SEAGATE ST15150N
target    1  52.2      target   CLAIMED  DEVICE
disk      0  52.2.0    disc3    CLAIMED  DEVICE      TOSHIBA CD-ROM XM-4101TA
target    3  52.4      target   CLAIMED  DEVICE
tape      0  52.4.0    tape2    CLAIMED  DEVICE      HP      C1533A
spt       1  52.4.1    spt      CLAIMED  DEVICE      HP      C1553A
target    6  52.5      target   CLAIMED  DEVICE
disk      5  52.5.0    disc3    CLAIMED  DEVICE      SEAGATE ST15150N
target    2  52.6      target   CLAIMED  DEVICE
disk      1  52.6.0    disc3    CLAIMED  DEVICE      SEAGATE ST15150N
lanmux    0  56        lanmux0  CLAIMED  INTERFACE LAN/Console
tty       0  56.0      mux4     CLAIMED  INTERFACE
lan       0  56.1      lan3     CLAIMED  INTERFACE
lantty    0  56.2      lantty0  CLAIMED  INTERFACE
processor 0  62        processor CLAIMED  PROCESSOR Processor
memory    0  63        memory   CLAIMED  MEMORY      Memory
# █
```

利用可能な SCSI アドレスは、このリストの 3 番目の列 (H/W Path) と 5 番目の列 (S/W State) の値に基づいて調べることができます。3 番目の列 (H/W Path) の値は、以下の形式で示されます。

```
<SCSI_bus_H/W_Path>.<SCSI_address>.<LUN_number>
```

この例の場合、ハードウェアパス 52 を使用する SCSI バスが 1 つだけ存在します。このバス上のアドレスのうち、リストに表示されていない 0 および 3 が、利用可能なアドレスとなります。

B-46 ページの図 B-14 に示す例では、SCSI バス上の SCSI アドレスのうち、以下のアドレスがすでに使用されています。

- SCSI アドレス 1 は、SCSI ディスクに使用されています。
- SCSI アドレス 2 は、CD-ROM に使用されています。
- SCSI アドレス 4、LUN 0 は、テープドライブに使用されています。
- SCSI アドレス 4、LUN 1 は、テープライブラリ ロボティクスに使用されています。
- SCSI アドレス 5 は、SCSI ディスクに使用されています。
- SCSI アドレス 6 は、SCSI ディスクに使用されています。
- SCSI アドレス 7 は、SCSI コントローラに使用されています。

注記 リストには、SCSI アドレス 7 は示されていませんが、これは SCSI コントローラにデフォルトで割り当てられるアドレスです。

どのデバイスについても、S/W State 列には CLAIMED と示されており、また H/W Type 列には H/W DEVICE と示されていますが、これはデバイスが現在接続されていることを意味していません。システムからアクセスできないデバイスがある場合は、そのデバイスの S/W State 列の値が UNCLAIMED になり、H/W Type 列の値が NO-HW になります。

SCSI アドレス 4 はテープライブラリに使用されています。このアドレスの LUN 0 はテープドライブに、LUN 1 はロボティクスに、それぞれ割り当てられています。このドライブは tape2 ドライバによって制御されており、ロボティクスは SCSI パス スルードライバ spt によって制御されています。Description 列には、このデバイスが HP StorageWorks 12000e ライブラリであることが示されています。HP StorageWorks 12000e ライブラリは、テープドライブとロボティクスに同じ SCSI アドレス上の異なる LUN を割り当てるように設計されており、システムに認識させやすい SCSI ライブラリです。

SCSI バス全体は、scsi1 インタフェース モジュールによって制御されています。

Solaris システム上の未使用の SCSI ターゲット ID の取得

Solaris システムに接続されたバックアップ デバイスのアクセスおよび制御は、デバイス ファイルを通じて行われます。このデバイス ファイルは、バックアップ デバイスを接続してクライアント システムとバックアップ デバイスの電源を投入した時点で、Solaris オペレーティング システムにより `/dev/rmt` ディレクトリに自動的に作成されます。

ただしバックアップ デバイスを接続する前に、使用可能な SCSI アドレスを確認し、未割り当てのアドレスをバックアップ デバイ스에設定するよう注意してください。

Solaris システム上で使用可能な SCSI アドレスを調べるには、以下の操作を行います。

1. Stop+A を押して、システムを停止します。
2. ok プロンプトから `probe-scsi-all` コマンドを実行します。

```
probe-scsi-all
```

ここで、`probe-scsi-all` コマンドを実行する前に、`reset-all` コマンドを実行するよう、システムから求められる場合があります。

3. 通常操作に戻るには、ok プロンプトに `go` と入力します。

```
go
```

使用可能なアドレスを調べてバックアップ デバイス用のアドレスを選択したら、デバイスを接続して起動する前に、関連する構成ファイルを更新しなければなりません。構成ファイルの更新方法は、次の項を参照してください。

Solaris システム上でのデバイスおよびドライバ構成の更新

構成ファイルの更新

デバイスおよびドライバの構成には、以下の構成ファイルが使用されます。接続されたデバイスを使用する前に、これらのファイルを確認し、必要に応じて編集してください。

- `st.conf`
- `sst.conf`

st.conf:

すべてのデバイス

このファイルは、テープ デバイスが接続された各 Data Protector Solaris クライアント上に必要です。ファイル内には、そのクライアントに接続されているすべてのバックアップ デバイスに関するデバイス情報と SCSI アドレスが記述されていなければなりません。シングルドライブ デバイスについては単一の SCSI エントリが、マルチドライブ ライブラリ デバイスについては複数の SCSI エントリが、それぞれ必要です。

1. 前の項の説明に従ってクライアント上で使われていない SCSI アドレスを調べ、接続するデバイス用のアドレスを選択してください。
2. 選択した SCSI アドレスをバックアップ デバイスに設定します。
3. クライアントシステムの電源を切ります。
4. バックアップ デバイスを接続します。
5. 最初にデバイスの電源を投入し、次にクライアント システムの電源を投入します。
6. Stop+A を押して、システムを停止します。
7. ok プロンプトから `probe-scsi-all` コマンドを実行します。

```
probe-scsi-all
```

コマンドを実行すると、接続されている SCSI デバイスに関する情報が表示されます。この中には新しく接続したバックアップ デバイスも含まれ、適切なデバイス ID 文字列が設定されているはずで

8. 通常操作に戻るには、次のように入力します。

```
go
```

9. `/kernel/drv/st.conf` ファイルを編集します。このファイルは Solaris st (SCSI テープ) ドライバで使用されます。ファイル内には、Solaris が正式にサポートするデバイスの一覧と、サードパーティ デバイス用の構成エントリが記述されています。サポート対象のデバイスを使用する場合は、デバイスを接続するだけで、追加の構成作業を行わなくても使用できるはずです。サポート対象外のデバイスについては、次の種類のエントリを `st.conf` ファイルに追加しなければなりません。

- テープ構成リスト エントリ (およびテープ データの変数定義)。ファイル内には、コメントアウトされた形でエントリ例が記述されています。いずれかのエントリをそのまま使用するか (該当する場合)、必要に応じて変更してください。

このエントリは、ファイル内の最初の `name=` エントリよりも前に、次の形式で記述しなければなりません。

```
tape-config-list="<Tape unit>","<Tape reference name>","<Tape data>";
```

各部分の説明 :

`<Tape unit>` テープ デバイスのベンダーおよび製品 ID を指定します。この文字列は、デバイス製造元のドキュメントに記載されているとおりに正確に指定しなければなりません。

`<Tape reference name>` 各自が選択した名前を指定します。システムはこの名前前でテープ デバイスを識別します。指定した名前によりテープ製品 ID が変更されることはありませんが、システムのブート時には、システムにより認識された周辺デバイスの一覧にこの参照名 (reference name) が示されます。

`<Tape data>` 追加されるテープ デバイスの一連の構成項目を参照する変数です。変数定義も、デバイス製造元のドキュメントに記載されているとおりに正確に指定しなければなりません。

例 :

```
tape-config-list="Quantum DLT4000","Quantum DLT4000","DLT-data";
```

```
DLT-data = 1,0x38,0,0xD639,4,0x80,0x81,0x82,0x83,2;
```

2 番目のパラメータである `0x38` は、テープ タイプ `DLTtape` を「その他 SCSI ドライブ」として指定しています。ここに指定する値は `/usr/include/sys/mtio.h` 内に定義されていなければなりません。

注記 テープ構成リスト内の最後のエントリの後ろには、必ずセミコロン (;) を付けてください。

- マルチドライブ デバイスの場合は、ターゲット エントリは次のようになります。

```
name="st" class="scsi"
target=X lun=Y;
```

各部分の説明：

X データドライブ (またはロボティクス機構) に割り当てる SCSI ポート
 です。

Y 論理ユニット番号です。

例：

```
name="st" class="scsi"
target=1 lun=0;
```

```
name="st" class="scsi"
target=2 lun=0
```

通常 `st.conf` ファイルには、ドライブ用のターゲット エントリのみを指定する必要があり、別のターゲット上にあるロボティクス機構用のエントリは必要ありません。ロボティクス機構用のエントリは、通常 `sst.conf` ファイルに指定します (詳細は以下を参照)。ただし HP StorageWorks 24x6 などの一部のデバイスでは、ロボティクス機構が他のドライブと同様に取り扱われます。この場合は、同一のターゲットと異なる LUN を指定した 2 つのエントリ (ドライブ用とロボティクス用に 1 つずつ) が必要です。

例：

```
name="st" class="scsi"
target=1 lun=0;
```

```
name="st" class="scsi"
target=1 lun=1
```

sst.conf:

ライブラリ デバイス

このファイルは、マルチドライブ ライブラリ デバイスが接続された各 Data Protector Solaris クライアント上に必要です。通常このファイルには、クライアントに接続された各ライブラリ デバイスのロボティクス機構の SCSI アドレス用エントリを指定する必要があります。ただし前の項で説明したように、HP StorageWorks 24x6 などの一部の例外もあります。

1. `sst` ドライバ (モジュール) と構成ファイル `sst.conf` を、次のディレクトリにコピーします。

- 32 ビット オペレーティング システムの場合

Solaris システム上でのデバイスおよびドライバ構成の更新

```
$cp /opt/omni/spt/sst /usr/kernel/drv/sst
```

```
$cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
```

- 64 ビット オペレーティング システムの場合

```
$cp /opt/omni/spt/sst.64bit /usr/kernel/drv/sparcv9  
/sst
```

```
$cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
```

2. sst.conf ファイルを開いて、次のエントリーを追加します。

```
name="sst" class="scsi" target=X lun=Y;
```

各部分の説明：

X ロボティクス機構の SCSI アドレスを指定します。

Y 論理ユニットを指定します。

例：

```
name="sst" class="scsi" target=6 lun=0;
```

3. ドライバを Solaris カーネルに追加します。

```
add_drv sst
```

デバイス ファイルの作成とチェック

構成ファイルの設定とドライバのインストールが終了したら、次の手順に従って新しいデバイス ファイルを作成してください。

1. /dev/rmt ディレクトリから、既存のデバイス ファイルをすべて削除します。次のコマンドを入力してください。

```
cd /dev/rmt  
rm *
```

2. 次のコマンドを入力してシステムをシャットダウンします。

```
shutdown -i0 -g0
```

3. 次のコマンドを入力してシステムを再ブートします。

```
boot -rv
```


boot コマンドに `r` スイッチを指定すると、カーネルのコンパイルが実行され、テープ デバイスとの通信に使われる専用のデバイス ファイルが作成されます。また `v` スイッチを指定することで、システムブートの詳細モード表示が有効化されます。詳細モードを指定した場合は、ブート処理の `/devices` ディレクトリ構成フェーズ中に、デバイスが接続されたことを示すために、ユーザが選択した `<Tape reference name>` (テープ参照名) 文字列が表示されます。

4. 次のコマンドを入力してインストール結果を確認します。

```
mt -t /dev/rmt/0 status
```

このコマンドの出力は、構成されたドライブにより異なります。およそ以下のようになります。

```
Quantum DLT7000 tape drive:  
sense key(0x6)= Unit Attention   residual= 0   retries= 0  
file no= 0   block no= 0
```

5. 再ブートが完了したら、`ls -all` コマンドを入力して、作成されたデバイス ファイルをチェックします。ライブラリ デバイスの場合は、このコマンドの出力結果は次のようになります。

```
/dev/rmt/0hb   1 番目のテープ ドライブ用  
/dev/rmt/1hb   2 番目のテープ ドライブ用  
/dev/rsst6     ロボティクス ドライブ用
```

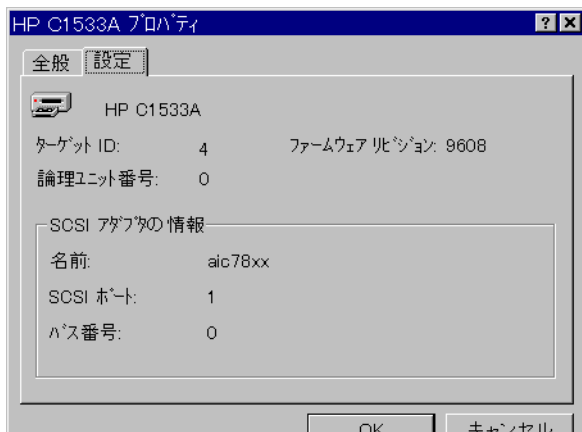
Windows システム上の未使用の SCSI ターゲット ID の取得

Windows システム上で未使用の SCSI ターゲット ID (アドレス) を調べるには、以下の手順に従ってください。

1. Windows の [コントロールパネル] で、[SCSI アダプタ] をクリックします。
2. SCSI アダプタに接続されているデバイスのリストで、各デバイスのプロパティをチェックします。デバイスの名前をダブルクリックし、[設定] をクリックして、プロパティ ページを開きます。B-54 ページの図 B-15 を参照してください。

このページに示される SCSI ターゲット ID と論理ユニット番号 (LUN) を確認してください。この方法で、どの SCSI ターゲット ID と LUN がすでに使用されているかを調べることができます。

図 B-15 デバイスの設定



HP StorageWorks 330fx ライブラリ上の SCSI ID の設定

ロボティクスおよびドライブに割り当てることのできる未使用の SCSI ID を選択し、ライブラリデバイスのコントロールパネルを使って、ロボティクスとドライブをチェックおよび構成することができます。

例： HP StorageWorks 330fx ライブラリを使用する場合は、SCSI ID の構成を以下の手順でチェックできます。

1. READY 状態から [NEXT] を押します。ADMIN* が表示されます。
2. [ENTER] を押し、パスワード プロンプトに対してパスワードを入力します。
3. TEST* が表示されたら、SCSI ID* が表示されるまで [NEXT] を押します。
4. [ENTER] を押します。VIEW IDs* が表示されます。
5. [ENTER] を押します。JKBX ID 6 LUN 0 が表示されます。
6. [NEXT] を押します。DRV 1 ID 5 LUN 0 が表示されます。
7. [NEXT] を押します。DRV 2 ID 4 LUN 0 が表示されます。以下同様に続きます。

READY 状態に戻るには、[CANCEL] を数回押してください。

バックアップ デバイスの接続

ここでは、HP-UX システム、Solaris システム、または Windows システムにバックアップ デバイスを接続する際の一般的な手順を示します。

1. バックアップ デバイスを接続するクライアントを選択します。
2. 選択したシステムに Media Agent をインストールします。詳細は 50 ページの「Data Protector クライアントのリモート インストール」を参照してください。
3. デバイスに割り当て可能な未使用の SCSI アドレスを調べます。HP-UX システムについては、B-46 ページの「HP-UX 上の未使用の SCSI アドレスの取得」を参照してください。Solaris システムについては、B-48 ページの「Solaris システム上の未使用の SCSI ターゲット ID の取得」を参照してください。Windows システムについては、B-54 ページの「Windows システム上の未使用の SCSI ターゲット ID の取得」を参照してください。

- ✓ HP-UX システムにデバイスを接続する場合は、必要なドライバがすでにインストールされており、現在のカーネルに組み込まれていることをチェックします。詳細は 70 ページの「HP-UX のカーネル構成のチェック」を参照してください。

SCSI パス スルードライバを構成する必要がある場合は、B-37 ページの「HP-UX 上の SCSI ロボティクス構成」を参照してください。

- ✓ Solaris システムに接続する場合は、必要なドライバがインストールされており、インストールするデバイスにあわせて構成ファイルが更新されていることを確認してください。詳細は B-49 ページの「Solaris システム上でのデバイスおよびドライバ構成の更新」を参照してください。ここでは、sst.conf ファイルの更新方法についても説明しています。SCSI パス スルードライバを構成する場合は、このファイルを更新する必要があります。
- ✓ Windows クライアントに接続する場合は、Windows システムのバージョンにより、ネイティブ テープドライバをロードまたは無効化します。詳細は B-32 ページの「Windows でのテープドライバおよびロボティクスドライバの使用」を参照してください。

Data Protector 用としてすでに構成されており、ネイティブ テープドライバを使用していないデバイスについて、そのデバイスのネイティブ テープドライバをロードする場合は、そのデバイスを参照しているすべての構成済み Data Protector 論理デバイスのデバイス ファイル名を変更する必要があります。たとえば、scsi1:0:4:0 から tape3:0:4:0 のような変更が必要です。

適切なデバイス ファイル名の詳細は、B-35 ページの「Windows 上でのデバイス ファイル (SCSI アドレス) の作成」を参照してください。

4. デバイスの SCSI アドレスを設定します。デバイスの種類にもよりますが、通常は SCSI アドレスをデバイス上のスイッチを使用して設定できます。詳細は、使用するデバイスのマニュアルを参照してください。

設定例は、B-55 ページの「HP StorageWorks 330fx ライブラリ上の SCSI ID の設定」を参照してください。

サポート対象デバイスの詳細は、<http://www.hp.com/support/manuals> を参照してください。

注記

Adaptec SCSI アダプタがインストールされており、SCSI デバイスが接続されている Windows システムの場合は、システムが正常に SCSI コマンドを実行できるように Host Adapter BIOS オプションを設定する必要があります。

Host Adapter BIOS オプションを設定するには、システムのブート中に Ctrl+A を押して SCSI アダプタ メニューを表示し、[Configure/View Host Adapter Settings]、[Advanced Configuration Options] を選択して、[Host Adapter BIOS] オプションを有効にします。

5. デバイス、コンピュータの順に電源を投入します。ブート処理が完了するまで待ちます。新しいバックアップ デバイスがシステムによって正しく認識されていることを確認します。
- ✓ HP-UX システムの場合は、ioscan ユーティリティを以下のコマンドで実行してください。

```
/usr/sbin/ioscan -fn
```

このコマンドを実行すると、接続済みのデバイスをハードウェアパスおよびデバイス ファイルとともに示すリストが出力されます。このリストを調べて、新しいデバイスに正しい SCSI アドレスが割り当てられていることを確認してください。

デバイス ファイルがブート処理中に自動生成されない場合は、手作業で作成する必要があります。詳細は B-42 ページの「HP-UX 上のデバイス ファイルの作成」を参照してください。
 - ✓ Solaris システム上の /dev/rmt ディレクトリで、ls -all コマンドを実行すると、接続済みのデバイスをハードウェアパスおよびデバイス ファイルとともに示すリストが出力されます。このリストを調べて、新しいデバイスに正しい SCSI アドレスが割り当てられていることを確認してください。
 - ✓ Windows システムの場合は、devbra ユーティリティを使うと、新しいバックアップ デバイスがシステムによって正しく認識されているかどうかを確認できます。
<Data_Protector_home>%bin ディレクトリに移動して、次のコマンドを実行します。

付録 B

バックアップ デバイスの接続

```
devbra -dev
```

devbra コマンドの出力リストでは、接続済みで正しく構成されている各デバイスについて、以下の行が表示されます。

```
<backup device specification>
```

```
<hardware_path>
```

```
<media_type>
```

```
.....
```

たとえば、以下のようなリストが出力されます。

```
HP:C1533A
```

```
tape3:0:4:0
```

```
DDS
```

```
...
```

```
...
```

この例の場合、ドライブ インスタンス番号 3 の HP DDS テープ デバイス (ネイティブ テープ ドライバがロードされている状態) が SCSI バス 0 に接続されており、SCSI ターゲット ID 4 および LUN 番号 0 が割り当てられています。

以下のようなリストが出力される場合もあります。

```
HP:C1533A
```

```
scsi1:0:4:0
```

```
DDS
```

```
...
```

```
...
```

この例の場合、HP DDS テープ ドライブ (ネイティブ テープ ドライバがアンロードされた状態) が SCSI バス 0 上の SCSI ポート 1 に接続されており、テープ ドライブに SCSI ターゲット ID 4 および LUN 番号 0 が割り当てられています。

- ✓ AIX システムの場合は、lsdev ユーティリティを以下のコマンドで実行してください。

```
lsdev -C
```

接続されているデバイスと、対応するデバイスファイルについて、リストが表示されます。

ハードウェア圧縮

現在のバックアップ デバイスのほとんどにはハードウェア圧縮機能が組み込まれており、デバイスの構成でデバイス ファイルまたは SCSI アドレスを作成する際に有効にできます。詳細な手順は、オンライン ヘルプを参照してください。

ハードウェア圧縮は、Media Agent クライアントから元のデータを受信したデバイスによって行われ、デバイスは圧縮モードでデータを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量が少なくなるため、テープドライブのデータ受信速度が向上します。

ソフトウェア圧縮が使用されハードウェア圧縮が無効になっている場合、データは Disk Agent により圧縮され、圧縮された形で Media Agent に送信されます。ソフトウェア圧縮を使用した場合は、圧縮アルゴリズムにより Disk Agent システムのリソースが大量に消費されますが、ネットワークの負荷は低減されます。

ハードウェア圧縮を Windows 上で有効にするには、デバイスやドライブの SCSI アドレスの最後に“C”を追加してください (例: scsi:0:3:0C [テープドライブがロードされている場合は、tape2:0:1:0C])。デバイスがハードウェア圧縮をサポートしていれば圧縮機能が使用され、サポートしていなければ C オプションは無視されます。

ハードウェア圧縮を Windows 上で無効にするには、デバイスやドライブの SCSI アドレスの最後に“N”を追加してください (例: scsi:0:3:0:N)。

ハードウェア圧縮を UNIX 上で有効か無効にするには、適切なデバイス ファイルを選択してください。詳細は、デバイスやオペレーティング システムのマニュアルを参照してください。

この次に行う作業

ここまでの段階で、バックアップ デバイスを正しく接続できたら、次にバックアップ デバイスおよびメディア プールを構成します。構成作業の詳細は、オンライン ヘルプの索引キーワード「バックアップ デバイスの構成」で表示される内容を参照してください。

システム上には、Media Agent をインストールしておく必要があります。手順の詳細は、50 ページの「Data Protector クライアントのリモート インストール」を参照してください。

この後の項では、HP StorageWorks Standalone 24 テープ デバイス、HP StorageWorks 12000e ライブラリ、および HP StorageWorks DLT ライブラリ 28/48 スロットを、それぞれ HP-UX システムまたは Windows システムに接続する場合の手順を説明します。

HP StorageWorks 24 スタンドアロン デバイスの接続

StorageWorks 24 DDS バックアップ デバイスは、DDS3 テクノロジーに基づくスタンドアロン テープドライブです。

HP-UX システムに接続する場合

HP StorageWorks 24 スタンドアロン デバイスを HP-UX システムに接続するには、以下の手順に従ってください。

1. 必要なドライバ (stape または tape2) がすでにインストールされており、カレント カーネルに組み込まれていることをチェックします。詳細は 70 ページの「HP-UX のカーネル構成のチェック」を参照してください。
2. テープドライブに割り当て可能な未使用の SCSI アドレスを探します。詳細は B-46 ページの「HP-UX 上の未使用の SCSI アドレスの取得」を参照してください。
3. デバイスの SCSI アドレス (ID) を設定します。デバイス背面のスイッチを使用してください。詳細は、使用するデバイスのマニュアルを参照してください。
4. デバイス、コンピュータの順に電源を投入し、ブート処理が完了するまで待ちます。
5. 新しいテープドライブがシステムによって正しく認識されていることを確認します。以下のコマンドで `ioscan` ユーティリティを実行してください。

```
/usr/sbin/ioscan -fn
```

このコマンドを実行すると、接続済みのデバイスをハードウェアパスおよびデバイスファイルとともに示すリストが出力されます。このリストを調べて、新たに接続したテープドライブに正しい SCSI アドレスが割り当てられていることを確認してください。なお、このドライブのデバイス ファイルは、ブート処理中に自動生成されます。

この次に行う作業

デバイスを適切に接続し終えたら、オンライン ヘルプの索引キーワード「バックアップ デバイスの構成」で表示される内容を参照して、新たに接続したデバイスに対応する Data Protector バックアップ デバイスを構成してください。

Windows システムに接続する場合

HP StorageWorks 24 スタンドアロン デバイスを Windows システムに接続するには、以下の手順に従ってください。

1. テープドライブに割り当て可能な未使用の SCSI アドレス (ターゲット ID) を探します。詳細は B-54 ページの「Windows システム上の未使用の SCSI ターゲット ID の取得」を参照してください。
2. デバイスの SCSI アドレス (ID) を設定します。デバイス背面のスイッチを使用してください。詳細は、使用するデバイスのマニュアルを参照してください。
3. デバイス、コンピュータの順に電源を投入します。ブート処理が完了するまで待ちます。
4. 新しいテープドライブがシステムによって正しく認識されていることを確認します。
devbra コマンドを <Data_Protector_home>\bin ディレクトリから実行します。以下のように入力してください。

```
devbra -dev
```

devbra コマンドの出力リストに、HP StorageWorks 24 スタンドアロン デバイスのテープドライブが含まれていることを確認してください。

この次に行う作業

デバイスを適切に接続し終えたら、オンライン ヘルプの索引キーワード「バックアップ デバイスの構成」で表示される内容を参照して、新たに接続したデバイスに対応する Data Protector バックアップ デバイスを構成してください。

HP StorageWorks DAT オートローダーの接続

HP StorageWorks 12000e と StorageWorks DAT24x6 の各ライブラリは、6 つのカートリッジを格納できるライブラリです。ドライブとロボティクスアームを 1 つずつ備えています。アームによって、ドライブ上のカートリッジが交換されます。ダーティ テープ検出機能が組み込まれています。

HP-UX システムに接続する場合

HP StorageWorks 12000e ライブラリ デバイスを HP-UX システムに接続するには、以下の手順に従ってください。

1. オートローダーの裏側のモード スイッチを 6 に設定してください。
2. 必要なドライバ (stape または tape2) がすでにインストールされており、カレント カーネルに組み込まれていることをチェックします。詳細は 70 ページの「HP-UX のカーネル構成のチェック」を参照してください。

3. 必要な SCSI パス スルードライバ (sct1 または spt) がインストールされており、カレントカーネルに組み込まれていることを確認します。詳細は B-37 ページの「HP-UX 上の SCSI ロボティクス構成」を参照してください。
4. テープドライブとロボティクスに割り当て可能な未使用の SCSI アドレスを探します。詳細は B-46 ページの「HP-UX 上の未使用の SCSI アドレスの取得」を参照してください。

注記

HP StorageWorks 12000e ライブラリは、テープドライブとロボティクスに同じ SCSI アドレス上の異なる LUN を割り当てるように設計されています。

5. デバイスの SCSI アドレス (ID) を設定します。詳細は、使用するデバイスのマニュアルを参照してください。
6. デバイス、コンピュータの順に電源を投入します。ブート処理が完了するまで待ちます。
7. 新しいテープドライブがシステムによって正しく認識されていることを確認します。以下のコマンドで `ioscan` ユーティリティを実行してください。

```
/usr/sbin/ioscan -fn
```

このコマンドを実行すると、接続済みのデバイスをハードウェアパスおよびデバイスファイルとともに示すリストが出力されます。このリストを調べて、新たに接続したテープドライブに正しい SCSI アドレスが割り当てられていることを確認してください。

8. ドライブのデバイスファイルはブート処理中に自動生成されますが、ロボティクスのデバイスファイルは手作業で作成する必要があります。詳細は 42 ページの「HP-UX 上のデバイスファイルの作成」を参照してください。
9. 新たに作成したライブラリロボティクスのデバイスファイルが、システムによって正しく認識されていることを確認します。`ioscan` ユーティリティを以下のコマンドでもう一度実行してください。

```
/usr/sbin/ioscan -fn
```

コマンドの出力リストに新しいデバイスファイルが含まれていることを確認します。

この次に行う作業

ライブラリ デバイスを適切に接続し終えたら、オンラインヘルプの索引キーワード「バックアップ デバイスの構成」で表示される内容を参照して、新たに接続したデバイスに対応する Data Protector バックアップ デバイスを構成してください。

Windows システムに接続する場合

HP StorageWorks 12000e ライブラリ デバイスを Windows システムに接続するには、以下の手順に従ってください。

1. オートローダーの裏側のモード スイッチを 6 に設定してください。
2. テープドライブとロボティクスに割り当て可能な未使用の SCSI アドレスを探します。詳細は B-54 ページの「Windows システム上の未使用の SCSI ターゲット ID の取得」を参照してください。
3. デバイスの SCSI アドレス (ID) を設定します。詳細は、使用するデバイスのマニュアルを参照してください。

注記 HP StorageWorks 12000e ライブラリは、テープドライブとロボティクスに同じ SCSI アドレス上の異なる LUN を割り当てるように設計されています。

4. デバイス、コンピュータの順に電源を投入し、ブート処理が完了するまで待ちます。
5. 新たに接続したテープドライブとロボティクスが、システムによって正しく認識されていることを確認します。 <Data_Protector_home>\bin ディレクトリに移動して、次のコマンドを実行します。

```
devbra -dev
```

devbra コマンドの出力リストに、HP StorageWorks 12000e ライブラリ デバイスのテープドライブとロボティクスが含まれていることを確認してください。

この次に行う作業

ライブラリ デバイスを適切に接続し終えたら、オンライン ヘルプの索引キーワード「バックアップ デバイスの構成」で表示される内容を参照して、新たに接続したデバイスに対応する Data Protector バックアップ デバイスを構成してください。

HP StorageWorks DLT ライブラリ 28/48 スロットの接続

HP StorageWorks DLT ライブラリ 28/48 スロットは、エンタープライズ環境用のマルチドライブライブラリです。80 ~ 600 GB のバックアップ容量を提供します。複数のデータ チャンネルを持つ DLT 4000 ドライブまたは DLT 7000 ドライブを 4 基搭載しており、メール スロットとバーコード リーダーを 1 つずつ備えています。

HP-UX システムに接続する場合

HP-UX システムに HP StorageWorks DLT ライブラリ 28/48 スロットを接続するには、以下の手順に従ってください。

1. 必要なドライバ (stape または tape2) がすでにインストールされており、カレント カーネルに組み込まれていることをチェックします。詳細は 70 ページの「HP-UX のカーネル構成のチェック」を参照してください。
2. 必要な SCSI パススルー ドライバ (sct1 または spt) がインストールされており、カレントカーネルに組み込まれていることを確認します。詳細は B-37 ページの「HP-UX 上の SCSI ロボティクス構成」を参照してください。
3. テープドライブとロボティクスに割り当て可能な未使用の SCSI アドレスを探します。詳細は B-46 ページの「HP-UX 上の未使用の SCSI アドレスの取得」を参照してください。

注記

HP StorageWorks DLT ライブラリ 28/48 スロットは、4 つのテープドライブとロボティクスを搭載しているため、すべてのテープドライブを使用するには合計 5 つの未使用の SCSI アドレスが必要です。テープドライブとロボティクスごとに、異なる SCSI アドレスを割り当てる必要があります。

4. デバイスの SCSI アドレス (ID) を設定します。詳細は、使用するデバイスのマニュアルを参照してください。
5. デバイス、コンピュータの順に電源を投入し、ブート処理が完了するまで待ちます。
6. 新しいテープドライブがシステムによって正しく認識されていることを確認します。以下のコマンドで `ioscan` ユーティリティを実行してください。

```
/usr/sbin/ioscan -fn
```

このコマンドを実行すると、接続済みのデバイスをハードウェアパスおよびデバイスファイルとともに示すリストが出力されます。このリストを調べて、新たに接続したテープドライブに正しい SCSI アドレスが割り当てられていることを確認してください。

7. ドライブのデバイスファイルはブート処理中に自動生成されますが、ロボティクスのデバイスファイルは手作業で作成する必要があります。詳細は B-42 ページの「HP-UX 上のデバイスファイルの作成」を参照してください。
8. 新たに作成したライブラリ ロボティクスのデバイスファイルが、システムによって正しく認識されていることを確認します。`ioscan` ユーティリティを以下のコマンドでもう一度実行してください。

```
/usr/sbin/ioscan -fn
```

コマンドの出力リストに新しいデバイス ファイルが含まれていることを確認します。

この次に行う作業

HP StorageWorks DLT ライブラリ 24/48 スロットライブラリ デバイスを適切に接続し終えたら、オンライン ヘルプの索引キーワード「バックアップ デバイスの構成」で表示される内容を参照して、新たに接続したデバイスに対応する Data Protector バックアップ デバイスを構成してください。

Solaris システムに接続する場合

Solaris システム上で HP C5173-7000 ライブラリ デバイスを構成するには、以下の手順に従ってください。この例では、2つのドライブを Data Protector に接続するものと想定します。

1. sst ドライバ (モジュール) と構成ファイル sst.conf を、次のディレクトリにコピーします。

- 32 ビット オペレーティング システムの場合

```
$cp /opt/omni/spt/sst /usr/kernel/drv/sst
```

```
$cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
```

- 64 ビット オペレーティング システムの場合

```
$cp /opt/omni/spt/sst.64 /usr/kernel/drv/sparcv9  
/sst
```

```
$cp /opt/omni/spt/sst.conf /usr/kernel/drv  
/sparcv9/sst.conf
```

2. ドライバを Solaris カーネルに追加します。

```
add_drv sst
```

3. /dev/rmt ディレクトリから、既存のデバイス ファイルをすべて削除します。次のコマンドを入力してください。

```
cd /dev/rmt  
rm *
```

4. Stop+A を押して、システムを停止します。

5. ok プロンプトから probe-scsi-all コマンドを実行して、使用可能な SCSI アドレスを調べます。

```
ok probe-scsi-all
```

ここで、`probe-scsi-all` コマンドを実行する前に、`reset-all` コマンドを実行するよう、システムから求められる場合があります。

この例では、SCSI 制御デバイス用にポート 6 を、1 番目のドライブ用にポート 2 を、2 番目のドライブ用にポート 1 を使用し、`lun` は 0 に設定します。

6. 通常操作に戻るには、次のように入力します。

```
ok go
```

7. 構成ファイル `st.conf` を次のディレクトリにコピーします。

```
$cp /opt/omni/spt/st.conf /kernel/drv/st.conf
```

`st.conf` ファイルは各 Solaris Data Protector クライアント上に存在し、そのクライアントに接続されているすべてのバックアップ デバイスの SCSI アドレスが記述されています。

8. `/kernel/drv/st.conf` ファイルを開いて、以下の行を追加します。

```
tape-config-list= "QUANTUM DLT7000", "Digital DLT7000", "DLT-data3";
```

```
DLT-data3 = 1,0x77,0,0x8639,4,0x82,0x83,0x84,0x85,3;
```

```
name="st" class="scsi"  
target=1 lun=0;
```

```
name="st" class="scsi"  
target=2 lun=0;
```

```
name="st" class="scsi"  
target=6 lun=0;
```

これらのエントリにより、ドライブ 1、ドライブ 2、およびロボティクスドライブの SCSI アドレスが、それぞれ定義されます。

9. 手順 1 でコピーした `sst.conf` ファイルを開いて、次の行を追加します。

```
name="sst" class="scsi" target=6 lun=0;
```

このエントリは、`st.conf` ファイル内のロボティクスドライブ用のエントリと一致していません。上の手順 8 を参照してください。

10. クライアント システムの電源を切ってから、ライブラリ デバイスを接続します。
11. 最初にライブラリ デバイスの電源を投入し、次にクライアント システムの電源を投入します。

システムがブートし、ロボティクスドライブおよびテープドライブ用のデバイス ファイルが自動的に作成されます。これらのファイル一覧を出力するには、`ls -all` コマンドを使用します。この例では、次の内容が出力されます。

```
/dev/rmt/0hb      1 番目のテープ ドライブ用  
/dev/rmt/1hb      2 番目のテープ ドライブ用  
/dev/rsst6        ロボティクスドライブ用
```

この次に行う作業

HP StorageWorks DLT ライブラリ 24/48 スロットライブラリ デバイスを適切に接続し終えたら、オンライン ヘルプの索引キーワード「バックアップ デバイスの構成」で表示される内容を参照して、新たに接続したデバイスに対応する Data Protector バックアップ デバイスを構成してください。

Windows システムに接続する場合

Windows システムに HP StorageWorks DLT ライブラリ 28/48 スロットを接続するには、以下の手順に従ってください。

1. テープドライブとロボティクスに割り当て可能な未使用の SCSI アドレス (ターゲット ID) を探します。詳細は 54 ページの「Windows システム上の未使用の SCSI ターゲット ID の取得」を参照してください。
2. デバイスの SCSI アドレス (ターゲット ID) を設定します。詳細は、使用するデバイスのマニュアルを参照してください。

注記

HP StorageWorks DLT ライブラリ 28/48 スロットは、4つのテープドライブとロボティクスを搭載しているため、すべてのテープドライブを使用するには合計5つの未使用の SCSI アドレスが必要です。テープドライブとロボティクスごとに、異なる SCSI ターゲット ID を割り当てる必要があります。

3. デバイス、コンピュータの順に電源を投入し、ブート処理が完了するまで待ちます。
4. 新たに接続したテープドライブとロボティクスが、システムによって正しく認識されていることを確認します。<Data_Protector_home>\bin ディレクトリに移動して、次のコマンドを実行します。

```
devbra -dev
```

devbra コマンドの出力リストに、HP StorageWorks DLT ライブラリ 28/48 スロットのテープドライブとロボティクスが含まれていることを確認してください。

この次に行う作業

HP StorageWorks DLT ライブラリ 24/48 スロットライブラリ デバイスを適切に接続し終えたら、オンラインヘルプの索引キーワード「バックアップ デバイスの構成」で表示される内容を参照して、新たに接続したライブラリ デバイスに対応する Data Protector バックアップ デバイスを構成してください。

Seagate Viper 200 LTO Ultrium テープドライブの接続

Seagate Viper 200 LTO Ultrium テープドライブは、エンタープライズ環境向けのスタンドアロンデバイスで、100 ～ 200 GB のバックアップが可能です。

Solaris システムに接続する場合

Solaris システム上で Seagate Viper 200 LTO Ultrium テープドライブを構成するには、以下の手順に従ってください。

1. このテープドライブに割り当て可能な未使用の SCSI アドレスを探します。modinfo コマンドまたは dmesg コマンドを使用すると、使用されている SCSI コントローラとインストールされている SCSI ターゲット デバイスを確認できます。

```
dmesg | egrep "target" | sort | uniq
```

次のような内容が出力されるはずです。

```
sd32 at ithps0: target 2 lun 0
sd34 at ithps0: target 4 lun 0
st21 at ithps1: target 0 lun 0
st22 at ithps1: target 1 lun 0
```

注記

Viper 200 LTO デバイスを Solaris システムに接続する場合は、glm または isp SCSI コントローラを使用することをお勧めします。また、Ultra2 SCSI コントローラまたは Ultra3 SCSI コントローラの使用もお勧めします。

2. /kernel/drv/st.conf ファイルを開いて、以下の行を追加します。

```
tape-config-list=
"SEAGATE ULTRIUM06242-XXX" , "SEAGATE LTO" , ¥ "SEAGATE_LTO";
SEAGATE_LTO = 1, 0x7a, 0, 0x1d679, 4, 0x00, 0x00, 0x00, ¥ 0x00, 1;
```


3. クライアント システムの電源を切ってから、デバイスを接続します。
4. 最初にデバイスの電源を投入し、次にクライアント システムの電源を投入します。

システムがブートし、テープドライブ用のデバイス ファイルが自動的に作成されます。これらのファイル一覧を出力するには、`ls -all` コマンドを使用します。

この次に行う作業

Seagate Viper 200 LTO Ultrium テープドライブを適切に接続し終えたら、オンライン ヘルプの索引キーワード「バックアップ デバイスの構成」で表示される内容を参照して、新たに接続したデバイスに対応する Data Protector バックアップ デバイスを構成してください。

Windows システムに接続する場合

Windows システムに Seagate Viper 200 LTO Ultrium テープドライブを接続するには、以下の手順に従ってください。

1. テープドライブに割り当て可能な未使用の SCSI アドレス (ターゲット ID) を探します。詳細は 54 ページの「Windows システム上の未使用の SCSI ターゲット ID の取得」を参照してください。
2. デバイスの SCSI アドレス (ターゲット ID) を設定します。詳細は、使用するデバイスのマニュアルを参照してください。
3. デバイス、コンピュータの順に電源を投入し、ブート処理が完了するまで待ちます。
4. 新たに接続したテープドライブとロボティクスが、システムによって正しく認識されていることを確認します。 <Data_Protector_home>\bin ディレクトリに移動して、次のコマンドを実行します。

```
devbra -dev
```

devbra コマンドの出力リストに、新しく接続した Seagate Viper 200 LTO Ultrium テープドライブが含まれていることを確認してください。

この次に行う作業

Seagate Viper 200 LTO Ultrium テープドライブを適切に接続し終えたら、オンライン ヘルプの索引キーワード「バックアップ デバイスの構成」で表示される内容を参照して、新たに接続したデバイスに対応する Data Protector バックアップ デバイスを構成してください。

注記

Seagate Viper 200 LTO Ultrium テープドライブを Data Protector 向けに構成する場合は、圧縮モードが設定されていることを確認してください。このためには、次に示すように、ドライブの SCSI アドレスの後に `c` パラメータを指定します。

```
scsi2:0:0:0C
```

Novell NetWare 上にインストールした General Media Agent の チェック

Novell NetWare プラットフォームにインストールした General Media Agent を確認するには、以下の作業を行います。

- ✓ 記憶デバイスを識別します。
- ✓ Novell NetWare サーバのコンソールで、General Media Agent の起動をテストします。
- ✓ Novell NetWare サーバのコンソールで、HPUMA.NLM および HPDEVBRA.NLM の起動をテストします。

記憶デバイスの識別

Novell NetWare 環境では、以下の形式で記憶デバイスを識別します。

```
<adapter identification number > : <target identification number> : <logical  
unit number> <compression>
```

たとえば、“0:2:0N” という文字列は、アダプタ ID 0、ターゲット ID 2、LUN (論理ユニット番号) 0、および圧縮なしの記憶デバイスを示します。

また、“1:1:0C” という文字列は、アダプタ ID 1、ターゲット ID 1、LUN (論理ユニット番号) 0、および圧縮ありの記憶デバイスを示します。

General Media Agent の起動テスト

Novell NetWare システムに General Media Agent をインストールしたら、Novell NetWare サーバのコンソールから Backup Media Agent (HPBMA.NLM) の起動をテストできます。

ここでは、Adaptec ホスト バス アダプタ AHA-2940 を経由して、エクステンジャ テープ デバイス HP StorageWorks Tape 12000e にアクセスする場合の例を示します。

Data Protector の *.NLM コンポーネントを起動する前に、以下の条件が満たされていることを確認してください。

- ✓ HPINET が実行されていること。
- ✓ Adaptec SCSI ホスト アダプタが実行されていること。
- ✓ General Media Agent ソフトウェアが、SYS:USR%OMNI%BIN ディレクトリにインストールされていること。

Novell NetWare 上にインストールした General Media Agent のチェック

- ✓ 記憶デバイスが正しく接続されていること。
- ✓ Adaptec ホスト バス アダプタおよび TCP/IP 通信プロトコルが正しくインストールされており、実行中であること。

上記の条件が満たされていれば、以下の手順に従ってください。

1. 以下のコマンドを入力して、HPBMA.NLM をロードします。

```
LOAD HPBMA -name testbma -type <type_number> -policy <policy_number> -ioctl  
<control_device> -dev <data_device> -tty <tty_number>
```

type <type_number> オプションでは、Data Protector のデバイスの種類を指定します。
<type_number> に指定可能な値は、以下に示すとおりです。

- 1=DAT/DDS
- 2=1/4 インチ カートリッジ (QIC)
- 3=8mm - Exabyte
- 9=汎用磁気テープドライブ
- 10=デジタルリニアテープ (DLT)

policy <policy_number> オプションでは、Data Protector でデバイスをどのように扱うかを指定します。指定可能な値は、以下に示すとおりです。

- 1=スタンドアロン デバイス
- 10=SCSI - II ライブラリ

ioctl <control_device> オプションでは、ロボティクスの SCSI アドレスを定義します。
以下の形式で指定する必要があります。

```
<adapter_identification_number>:<target_identification_number>:<logical_un  
it_number>
```

例：

- 0:1:1 => 制御デバイス (ロボティクス) が SCSI アダプタ 0 を使用し、SCSI アドレス 1、LUN1 が割り当てられていることを意味します。

dev <data_device> オプションでは、ロボティクスの SCSI アドレスを定義します。以下の形式で指定する必要があります。

```
<adapter_identification_number>:<target_identification_number>:<logical_un  
it_number><compression>
```

Novell NetWare 上にインストールした General Media Agent のチェック

例：

- 0:1:1C => 制御デバイス (ロボティクス) が SCSI アダプタ 0 を使用し、SCSI アドレス 1、LUN1 が割り当てられていることを意味します。さらに、データ圧縮が有効に設定されていることを示します。

-tty <tty_number> オプションでは、TCP/IP 通信プロトコルのポート番号を定義します。

Console Media Agent HPCONMA.NLM が起動し、以下のようなプロンプト画面が表示されます。

```
*** MA listening on port: <number>
```

```
SLOT: [Load(2), Peek(2), Stop(0), Abort(0)]
```

```
SLOT: _
```

現在のリリースでは、以下に示すコマンドを使用できます。

Load(2) - テープをドライブにロードするコマンド。引数を 2 つ指定する必要があります。

```
Load <Slot number> <flipping flag >
```

flipping flag は 0 または 1 に設定できます。0 の場合はメディアのフリップが行われず、1 の場合はフリップが行われます。

Stop(0) - 現在のセッションを正常に終了します。

Abort(0) - 現在のセッションを中止します。

この例では、メディアのフリップなしで、SLOT 3 からテープをロードします。

2. メディアのフリップなしで、SLOT 3 からテープをロードするには、以下のコマンドを入力します。

```
SLOT:LOAD 3 0
```

ドライブにテープがロードされると、以下のメッセージが表示されます。

```
CHECK: [Deny(0), Init(1), Seek(2), Abort(0)]
```

```
CHECK: _
```

以下に示すコマンドを使用できます。

Deny(0) - 現在のアクションを拒否します。

Init(1) - ロードしたテープを初期化します。以下のようにメディア ID を指定する必要があります。

```
Init(1) <medium id>
```

Seek(2) - 指定した位置まで移動します。以下のように引数を指定します。

Novell NetWare 上にインストールした General Media Agent のチェック

Seek <segment number> <block number>

Abort (0) - 現在のセッションを中止します。

3. テープを初期化するには、以下のコマンドを入力します。

CHECK: Init test

4. Backup Media Agent の画面を Novell Netware コンソールに切り替えた後、General Media Agent のアクションコマンドや要求コマンドを実行して、バックアップセッションを開始します。

注記

General Media Agent と Disk Agent を正しく通信させ、HPCONMA.NLM の起動時に正しいバックアップセッション操作ポート番号が表示されるようにするには、選択したホスト上で、load -ma <host> <port> を使って Data Protector Disk Agent を起動する必要があります。バックアップセッションが正常に完了すると、メッセージが表示されます。

5. Backup Media Agent を正常に終了するには、Backup Media Agent 画面で <CTRL-C> キーを押します。しばらくすると、Console Attention Request プロンプトが表示されます。

ATT: [Stop (0), Abort (0), Disconnect (1)]

ここで Stop コマンドを実行して、セッションを終了します。

HPUMA.NLM および HPDEVBRA.NLM の起動テスト

HPUMA.NLM をサーバのコンソールからロードすると、SCSI コマンドを手作業でテストできます。

HPUMA.NLM をロードするには、以下のコマンドを入力します。

```
LOAD HPUMA.NLM -ioctl <control_device> -dev <data_device> -tty
```

ioctl <control_device> オプションでは、ロボティクスの SCSI アドレスを定義します。以下の形式で指定する必要があります。

```
<adapter_identification_number>:<target_identification_number>:<logical_unit_number>
```

例：

- 0:1:1 => 制御デバイス (ロボティクス) が SCSI アダプタ 0 を使用し、SCSI アドレス 1、LUN1 が割り当てられていることを意味します。

dev <data_device> オプションでは、ロボティクスの SCSI アドレスを定義します。以下の形式で指定する必要があります。

Novell NetWare 上にインストールした General Media Agent のチェック

```
<adapter_identification_number>:<target_identification_number>:<logical_unit_number>:<compression>
```

例：

- 0:1:1C=> 制御デバイス (ロボティクス) が SCSI アダプタ 0 を使用し、SCSI アドレス 1、LUN1 が割り当てられていることを意味します。さらに、データ圧縮が有効に設定されていることを示します。

Novell NetWare サーバ コンソールから DEVBRA.NLM を操作するには、-tty オプションを指定する必要があります。

HPUMA が起動し、以下のプロンプト画面が表示されます。

```
prompt>
```

プロンプトは以下の形式で表示されます。

```
<adapter_identification_number>:<target_identification_number>:<logical_unit_number>
```

例：

```
0:2:1>
```

使用可能なコマンドを調べるには、HPUMA 画面で HELP コマンドを入力します。たとえば、未使用のスロットとドライブがあるかどうかを確認するには、プロンプトで STAT と入力します。

確認が完了したら、BYE とタイプして、HPUMA 画面を閉じます。

HPDEVBRA.NLM をローカルにロードすると、Novell NetWare サーバ上にインストールされているデバイスのうち、Novell NetWare サーバによって検出されたデバイスに関する情報を取得できるようになります。

HPDEVBRA.NLM をロードするには、サーバ コンソールで以下のコマンドを入力します。

```
LOAD HPDEVBRA.NLM -dev
```

上記で、-dev オプションは、Novell NetWare サーバに接続されているすべてのデバイスを表示するのに必要です。

現在使用可能なコマンドを調べるには、以下に示すとおり、HELP オプション付きで HPDEVBRA.NLM をロードしてください。

```
LOAD HPDEVBRA -HELP
```

Veritas Volume Manager がインストールされた Microsoft Cluster への Data Protector のインストール

Veritas Volume Manager がインストールされた Microsoft Cluster Server (MSCS) に Data Protector をインストールするには、まず MSCS に Data Protector をインストールする一般的な手順を実行します。詳細は 167 ページの「Data Protector の Microsoft Cluster Server へのインストール」を参照してください。

インストールが完了したら、Data Protector Inet サービスを有効にして、Microsoft のリソースドライバではなく専用のリソース ドライバを使用しているローカルおよびクラスタ ディスク リソースと、そうではないディスク リソースを区別するために、追加作業がいくつか必要となります。

1. Cell Manager 上で `omnisv -stop` コマンドを実行して、Data Protector サービスおよびプロセスを停止します。

```
<Data_Protector_home>%bin%omnisv -stop
```

2. 新しいシステム環境変数 `OB2CLUSTERDISKTYPES` の値を Volume Manager Disk Group にして定義するか、両方のクラスタ ノード上で `omnirc` 変数を以下のように設定します。

```
OB2CLUSTERDISKTYPES=Volume Manager Disk Group
```

NetRAID4 ディスクなど、独自のディスク リソースを追加指定する場合は、`OB2CLUSTERDISKTYPES=Volume Manager Disk Group;NETRaid4M Diskset` のように、`OB2CLUSTERDISKTYPES` 環境変数の値に、単純にリソース タイプ名を追加します。

`omnirc` ファイル変数の使用に関する詳細は、『HP OpenView Storage Data Protector トラブルシューティング ガイド』を参照してください。

3. `omnisv -start` コマンドを実行して、サービスやプロセスを起動します。

```
<Data_Protector_home>%bin%omnisv -start
```


Data Protector A.06.00 での構成ファイルパスの変更

Data Protector A.06.00 では、ログや (UNIX の) データベース ファイルなどの一部の構成で、デフォルトパスが変更されています。ファイルの一部が、server ディレクトリと client ディレクトリに分けて置かれるようになりました。

以下の表で変更点を確認し、必要に応じてパスを変更してください。

UNIX での構成ファイル

クライアントの構成ファイル

アップグレード中に /etc/opt/omni ディレクトリから /etc/opt/omni/client ディレクトリに移動されるファイルとディレクトリを、以下の表に示します。

表 B-1 新しい /etc/opt/omni/client ディレクトリの内容

従来のパス	現在のパス
/etc/opt/omni/cell/cell_server	/etc/opt/omni/client/cell_server
/etc/opt/omni/cell/omni_format	/etc/opt/omni/client/omni_format
/etc/opt/omni/cell/omni_info	/etc/opt/omni/client/omni_info
/etc/opt/omni/cell/allow_hosts	/etc/opt/omni/client/allow_hosts
/etc/opt/omni/cell/deny_hosts	/etc/opt/omni/client/deny_hosts
/etc/opt/omni/customize	/etc/opt/omni/client/customize

Cell Manager の構成ファイルとログ ファイル

/etc/opt/omni ディレクトリにあった残りのファイルは、/etc/opt/omni/server ディレクトリに移動されます。たとえば、/etc/opt/omni/cell/cell_info ファイルは、/etc/opt/omni/server/cell ディレクトリに移動されています。

Data Protector A.06.00 での構成ファイルパスの変更

アップグレード中に /var/opt/omni ディレクトリから /var/opt/omni/server ディレクトリに移動されるファイルとディレクトリを、以下の表に示します。

表 B-2 新しい /var/opt/omni/server ディレクトリの内容

従来のパス	現在のパス
/var/opt/omni/db40	/var/opt/omni/server/db40
/var/opt/omni/sessions	/var/opt/omni/server/sessions
/var/opt/omni/log/<log_file>	/var/opt/omni/server/log/<log_file>

<log_file> は、以下のファイルのいずれかを表しています。HealthCheck.log、Check_*.txt、Ob2Event*、lic.log、omnisv.log、media.log、sm.log、crsevents.log、security.log、purge.log、readascii.log、cleaning.log、upgrade.log、trace.log、cluster.log。

その他のディレクトリ (/var/opt/omni/tmp、/var/opt/omni/windu、/var/opt/omni/emc など) とログ ファイル (/var/opt/omni/log/debug.log など) は、移動されません。

Windows での構成ファイル

クライアントの構成ファイル

アップグレード中に <Data_Protector_home>%Config ディレクトリから <Data_Protector_home>%Config%client ディレクトリと <Data_Protector_home>%tmp ディレクトリに移動されるファイルとディレクトリを、以下の表に示します。

表 B-3 新しい <Data_Protector_home>%Config%client ディレクトリの内容

従来のパス	現在のパス
<Data_Protector_home>%Config%cell%cell_server	<Data_Protector_home>%Config%client%cell_server
<Data_Protector_home>%Config%cell%omni_format	<Data_Protector_home>%Config%client%omni_format
<Data_Protector_home>%Config%cell%omni_info	<Data_Protector_home>%Config%client%omni_info

表 B-3 新しい
(続き
)<Data_Protector_home>%Config%client

従来のパス	現在のパス
<Data_Protector_home>%Config%cell%allow_hosts	<Data_Protector_home>%Config%client%allow_hosts
<Data_Protector_home>%Config%cell%deny_hosts	<Data_Protector_home>%Config%client%deny_hosts
<Data_Protector_home>%Config%EMC	<Data_Protector_home>%Config%client%EMC
<Data_Protector_home>%Config%tmp%EMC	<Data_Protector_home>%tmp%EMC

Cell Manager の構成ファイル

<Data_Protector_home>%Config ディレクトリにあった残りのファイルは <Data_Protector_home>%Config%Server ディレクトリに移動されます。たとえば、<Data_Protector_home>%Config%cell%cell_info ファイルは、<Data_Protector_home>%Config%Server%cell ディレクトリに移動されています。

ログ ファイル

以下のファイルは、<Data_Protector_home>%log から <Data_Protector_home>%log%server に移動されます。HealthCheck.log、Check_*.txt、Ob2Event*、lic.log、omnisv.log、media.log、sm.log、crsevents.log、security.log、purge.log、readascii.log、cleaning.log、upgrade.log、trace.log、cluster.log。

その他のログ ファイル (<Data_Protector_home>%log%debug.log など) は、移動されません。

Data Protector A.06.00 にアップグレードした後のコマンド行ツールの変更

ここでは、Data Protector A.06.00 の新しいオプションに関連して変更または機能拡張されたコマンドを紹介します。スクリプトに古いコマンドが使用されていないかどうかチェックの上、必要に応じて修正してください。スクリプトの構文は、対応するマンページを参照してください。

アップグレード前の Cell Manager のバージョンに応じて、対応する表を参照してください。

- Data Protector A.05.00 からアップグレードした場合は、B-80 ページの表 B-4 を参照してください。
- Data Protector A.05.10 からアップグレードした場合は、B-80 ページの表 B-4 を参照してください。
- Data Protector A.05.50 からアップグレードした場合は、B-80 ページの表 B-4 を参照してください。

表 B-4 Data Protector A.05.00 からのアップグレード

コマンド	サブコマンドとオプション	ステータス
ob2install	-sapdb	新しいソフトウェア コンポーネント
	-smisa	
	-db2	
	-acs	削除されるソフト ウェア コンポーネン ト
	-das	
omniamo		新しいコマンド

表 B-4 Data Protector A.05.00 からのアップグレード (続き)

コマンド	サブコマンドとオプション	ステータス
omnib	-db2_list	新しい統合ソフトウェア
	-msvssw_list	
	-sapdb_list	
	-mbx_list	
	-share_info	新しいオプション
	-mirror	
	-enh_incr	
omnicc	-check_licenses	新しいオプション
	-detail	
	-update_all	
	-force_cs	
	-list_trusted_hosts	
	-secure_client	
	-unsecure_client	
	-trusted_hosts	
omnicheck		新しいコマンド
omniclus	-applid	変更されるオプション

表 B-4 Data Protector A.05.00 からのアップグレード (続き)

コマンド	サブコマンドとオプション	ステータス
omnicreatedl	-snapshot	HP StorageWorks ENTERPRISE VIRTUAL ARRAY 用 の新しいオプション
	-smis	
	-instant_recovery	
	-snapshots <number>	
	-snapshot_type standard	
	-snapshot_type vsnap	
	-snapshot_type clone	
	-snapshot_policy strict	
	-snapshot_policy loose	
	-wait_clonecopy <number>	
	-replica_conf local	
	-replica_conf combined	
	-ca_failover_option follow_replica_direct ion	
-ca_faiover_option maintain_replica_loca tion		

表 B-4 Data Protector A.05.00 からのアップグレード (続き)

コマンド	サブコマンドとオプション	ステータス
omnidb	-db2	新しい統合ソフトウェア
	-vss	
	-sapdb	
	-mbx	
	-copyid	新しいオプション
	-listcopies	
omnidbsmis		新しいコマンド
omnidbupgrade		新しいコマンド
omnidbutil	-extendtblspace	新しいオプション
	-readdb	変更されるオプション
omnidbvss		新しいコマンド
omnidlc		新しいコマンド
omniinstlic		新しいコマンド
omniiso		新しいコマンド
omnimcopy	-permanent -until	新しいオプション
omnim	-[no_]free_pool	変更されるオプション
	-create_free_pool	新しいオプション
omnimigrate.pl		新しいコマンド
omniminit	-[no]barcode_as_label	新しいオプション
omniobjcopy		新しいコマンド

表 B-4 Data Protector A.05.00 からのアップグレード (続き)

コマンド	サブコマンドとオプション	ステータス
omniobjconsolidate		新しいコマンド
omnir	-db2	新しい統合ソフトウェア
	-sapdb	
	-newinstance	SAP DB 用の新しいオプション
	-recover	
	-endlogs	
	-time	
	-nochain	
	-destination	
	-from_disk	
	-instance	HP StorageWorks ENTERPRISE VIRTUAL ARRAY 用の新しいオプション
	-force_prp_replica	
	-instance <SourceInstanceName>	MS SQL 用の新しいオプション
	-destinstance <DestinationInstanceName>	
	-asbase <NewDBName>	
-file <LogicalFileName>		

表 B-4 Data Protector A.05.00 からのアップグレード (続き)

コマンド	サブコマンドとオプション	ステータス
omnir	-instance	IBM DB2 UDB 用の新しいオプション
	-logfile	
	-newdbname	
	-offline	
	-rollforward	
	-tsname	
	-msvssw	新しい統合ソフトウェア
	-mbx	
	-share_info	新しいオプション
	-oracle	ORACLE と SAP R/3 のインスタント リカバリの新しいオプション
	-sap	
	-user	
	-group	
	-recover	
	-restore <tree>	
	-open	
	-resetlogs	
	-paralleism	
	-restore	新しい VSS インスタント リカバリ オプション
	-session	
-vss		
-copyid	新しいオプション	

表 B-4 Data Protector A.05.00 からのアップグレード (続き)

コマンド	サブコマンドとオプション	ステータス
omnirpt	media_list_extended	新しいレポート
	-smtp	新しいオプション
omniresolve		新しいコマンド
omnisetup.sh	-CM	新しいオプション
	-IS	
	-autopass	
	db2	新しいソフトウェア コンポーネント
	smisa	
	sapdb	
	acs	削除されるソフト ウェア コンポーネン ト
	das	
omnistrupdate	-asr	新しいオプション
	-location	
omniusers		新しいコマンド
sanconf	-[no_]multipath	新しいオプション
	-remove_hosts	
	-sanstableaddressing	
uma	-scsiType	-interface オプ ションに置き換え
	-interface	-scsiType オプシ ョンを置き換え

表 B-4 Data Protector A.05.00 からのアップグレード (続き)

コマンド	サブコマンドとオプション	ステータス
upgrade_cm_fro m_evaa		新しいコマンド

表 B-5 Data Protector A.05.10 からのアップグレード

コマンド	サブコマンドとオプション	ステータス
ob2install	-sapdb	新しいソフトウェア コンポーネント
	-smisa	
	-acs	削除されるソフト ウェア コンポーネン ト
	-das	
omnib	-sapdb_list	新しい統合ソフト ウェア
	-vss_list	削除されるオプショ ン
	-msvssw_list	新しいオプション
	-share_info	
	-mirror	
	-enh_incr	

表 B-5 Data Protector A.05.10 からのアップグレード (続き)

コマンド	サブコマンドとオプション	ステータス
omnicc	-check_licenses	新しいオプション
	-detail	
	-update_all	
	-force_cs	
	-list_trusted_hosts	
	-secure_client	
	-unsecure_client	
	-trusted_hosts	
omniclus	-applid	変更されるオプション

表 B-5 Data Protector A.05.10 からのアップグレード (続き)

コマンド	サブコマンドとオプション	ステータス
omnicreatedl	-smis	HP StorageWorks ENTERPRISE VIRTUAL ARRAY 用の 新しいオプション
	-instant_recovery	
	-snapshots <number>	
	-snapshot_type clone	
	-wait_clonecopy <number>	
	-replica_conf local	
	-replica_conf combined	
	-ca_failover_option follow_replica_direct ion	
-ca_faiover_option maintain_replica_loca tion		
omnidb	-sapdb	新しい統合ソフト ウェア
	-copyid	新しいオプション
	-listcopies	
omnidbeva		削除されるコマンド
omnidbsmis		新しいコマンド
omidbupgrade		新しいコマンド
omnidbvss		新しいコマンド

表 B-5 Data Protector A.05.10 からのアップグレード (続き)

コマンド	サブコマンドとオプション	ステータス
omnidbutil	-extendtblspace	新しいオプション
	-readdb	変更されるオプション
omnidlc		新しいコマンド
omnimigrate.pl		新しいコマンド
omniminit	- [no]barcode_as_label	新しいオプション
omnimmm	- [no_]free_pool	変更されるオプション
	-create_free_pool	新しいオプション
omniinstlic		新しいコマンド
omniiso		新しいコマンド
omniobjcopy		新しいコマンド
omniobjconsolidate		新しいコマンド

表 B-5 Data Protector A.05.10 からのアップグレード (続き)

コマンド	サブコマンドとオプション	ステータス
omnir	-sapdb	新しい統合ソフトウェア
	-newinstance	SAP DB 用の新しいオプション
	-recover	
	-endlogs	
	-time	
	-nochain	
	-destination	
	-from_disk	
	-instance	
	-force_prp_replica	HP StorageWorks ENTERPRISE VIRTUAL ARRAY 用の新しいオプション
	-instance <SourceInstanceName>	MS SQL 用の新しいオプション
	-destinstance <DestinationInstanceName>	
	-asbase <NewDBName>	
	-file <LogicalFileName>	

表 B-5 Data Protector A.05.10 からのアップグレード (続き)

コマンド	サブコマンドとオプション	ステータス
omnir	-oracle	ORACLE と SAP R/3 のインスタント リカ バリの新しいオプ ション
	-sap	
	-user	
	-group	
	-recover	
	-open	
	-resetlogs	
	-paralleism	
	-public	MS Exchange シング ル メールボックス用 の新しいオプション
	-originalfolder	
	-keep_msg	
	-overwrite_msg	
	-folder	
	-exclude	
	-restore	新しい VSS インスタ ント リカバリ オプ ション
	-session	
-vss		
-copyid	新しいオプション	
omnirpt	-smtp	新しいオプション
omniresolve		新しいコマンド

表 B-5 Data Protector A.05.10 からのアップグレード (続き)

コマンド	サブコマンドとオプション	ステータス
omnisetup.sh	-CM	新しいオプション
	-IS	
	-autopass	
	smisa	新しいソフトウェアコンポーネント
	sapdb	
	acs	削除されるソフトウェアコンポーネント
das		
omniusers		新しいコマンド
sanconf	-[no_]multipath	新しいオプション
	-remove_hosts	
	-sanstableaddressing	
upgrade_cm_from_evaa		新しいコマンド

表 B-6 Data Protector A.05.50 からのアップグレード

コマンド	サブコマンドとオプション	ステータス
omnib	-enh_incr	新しいオプション

表 B-6 Data Protector A.05.50 からのアップグレード (続き)

コマンド	サブコマンドとオプション	ステータス
omnidbsmis	-ssl	新しいオプション
	-caconf	
	-init	
	-put <filename>	
	-get <filename>	
	-list <EVA Name>	
	-check <DR Group Name>	
omnidbeva		削除されるコマンド
omnicreatedl	-replica_conf local	HP StorageWorks ENTERPRISE VIRTUAL ARRAY 用の 新しいオプション
	-replica_conf combined	
	-ca_failover_option follow_replica_direct ion	
	-ca_faiover_option maintain_replica_loca tion	
omnidbutil	-extendtblspace	新しいオプション
	-readdb	変更されるオプション
omnidbvss		新しいコマンド
omnidlc	-debug_loc	新しいオプション
omnimigrate.pl		更新されたコマンド

表 B-6 Data Protector A.05.50 からのアップグレード (続き)

コマンド	サブコマンドとオプション	ステータス
omnimm	- [no_] free_pool	変更されるオプション
	-create_free_pool	新しいオプション
omniobjconsolidate		新しいコマンド
omnir	-public	MS Exchange シングル メールボックス用の新しいオプション
	-originalfolder	
	-keep_msg	
	-overwrite_msg	
	-folder	
	-exclude	
	-restore	新しい VSS インスタント リカバリ オプション
	-session	
	-vss	
omnirpt	-smtp	新しいオプション
upgrade_cm_from_evaa		新しいコマンド
upgrade_cfg_from_evaa		削除されるコマンド

C 付録 C

インストールメディアとして CD-ROM を使用

Data Protector A.06.00 にはインストール CD-ROM も用意されています。CD-ROM を使用する場合はシステム要件やインストール前後に必要な作業などは DVD-ROM を使用する場合と変わりません。ただし、HP-UX、Solaris、および Linux プラットフォームでは、1つのプラットフォームに対して複数枚の CD-ROM を使用するため、追加の手順が必要になります。

この付録では、インストール CD-ROM 上の製品構成、CD-ROM からインストールする場合の手順の違い、および追加の制限事項について説明します。

Data Protector のインストール CD-ROM

Data Protector は、さまざまなプロセッサアーキテクチャ上でさまざまなオペレーティングシステムをサポートしています。これらのプラットフォームのすべてに対応するには、15枚の CD-ROM を使用する必要があります。それぞれの CD-ROM に収録されているコンポーネントの詳細は、C-2 ページの「Data Protector CD-ROM の一覧」を参照してください。

HP-UX、Solaris、または Linux プラットフォーム用の各 CD-ROM は、その CD-ROM からインストールする Data Protector コンポーネントに合わせた名称で表記しています。たとえば、「**Cell Manager インストール CD-ROM**」は Cell Manager のインストールに使用する CD-ROM、「**インストール サーバ インストール CD-ROM**」はインストール サーバおよびクライアントのインストールに使用する CD-ROM です。

表 C-1 Data Protector CD-ROM の一覧

CD 番号	CD-ROM のタイトル	内容
1	HP Data Protector for HP-UX PA-RISC - Cell Manager 本書では「Data Protector HP-UX 用 Cell Manager インストール CD-ROM」と呼びます。	<ul style="list-style-type: none"> • HP-UX 11.x (PA-RISC アーキテクチャ) 用 Cell Manager • PDF 形式のマニュアル (英語版: DOCS ディレクトリ、日本語版: DOCS/JPN ディレクトリ) • HP-UX 用 OpenView 統合パッケージ • HP-UX 用 AutoPass • Omnisetup.sh インストール スクリプト

表 C-1 Data Protector CD-ROM の一覧 (続き)

CD 番号	CD-ROM のタイトル	内容
2	HP Data Protector for HP-UX PA-RISC - インストール サーバ	<ul style="list-style-type: none"> HP-UX 11.x (PA-RISC アーキテクチャ) 用インストール サーバ とすべての UNIX クライアント
3	本書では「Data Protector HP-UX 用インストール サーバ インストール CD-ROM」(1 および 2) と呼びます。	<ul style="list-style-type: none"> Omnisetup.sh インストール スクリプト
4	HP Data Protector for HP-UX IA-64 - Cell Manager 本書では「HP-UX 用 Cell Manager インストール CD-ROM」 と呼びます。	<ul style="list-style-type: none"> HP-UX 11.23 (IA-64 アーキテクチャ) 用 Cell Manager PDF 形式のマニュアル (英語版 : DOCS ディレクトリ、日本語版 : DOCS/JPN ディレクトリ) HP-UX 用 OpenView 統合パッケージ HP-UX 用 AutoPass Omnisetup.sh インストール スクリプト
5	HP Data Protector for HP-UX IA-64 - インストール サーバ	<ul style="list-style-type: none"> HP-UX 11.23 (IA-64 アーキテクチャ) 用インストール サーバ とすべての UNIX クライアント
6	本書では「Data Protector HP-UX 用インストール サーバ インストール CD-ROM」(1 および 2) と呼びます。	<ul style="list-style-type: none"> Omnisetup.sh インストール スクリプト
7	HP Data Protector for Solaris-Cell Manager 本書では「Data Protector Solaris 用インストール サーバ インストール CD-ROM」 と呼びます。	<ul style="list-style-type: none"> Solaris 8/9/10 用 Cell Manager PDF 形式のマニュアル (英語版 : DOCS ディレクトリ、日本語版 : DOCS/JPN ディレクトリ) Solaris 用 OpenView 統合ソフトウェア パッケージ Solaris 用 AutoPass Omnisetup.sh インストール スクリプト

表 C-1 Data Protector CD-ROM の一覧 (続き)

CD 番号	CD-ROM のタイトル	内容
8	HP Data Protector for Solaris - インストール サーバ	<ul style="list-style-type: none"> Solaris 8/9/10 用インストール サーバとすべての UNIX クライアント^a
9	本書では「Data Protector Solaris 用インストール サーバ インストール CD-ROM」(1 および 2) と呼びます。	<ul style="list-style-type: none"> Omnisetup.sh インストール スクリプト
10	HP Data Protector for Linux x86-64 - Cell Manager 本書では「Data Protector Linux 用 Cell Manager インストール CD-ROM」 と呼びます。	<ul style="list-style-type: none"> Linux 用 Cell Manager PDF 形式のマニュアル (英語版 : DOCS ディレクトリ、日本語版 : DOCS/JPN ディレクトリ) Omnisetup.sh インストール スクリプト
11	HP Data Protector for Linux x86-64 - インストール サーバ	<ul style="list-style-type: none"> Linux 用インストール サーバとすべての UNIX クライアント^a
12	本書では「Data Protector Linux 用インストール サーバ インストール CD-ROM」(1 および 2) と呼びます。	<ul style="list-style-type: none"> Omnisetup.sh インストール スクリプト
13	Data Protector for Windows - Cell Manager & インストール サーバ (Netware クライアント用エージェントを含む) 本書では「Data Protector Windows 用インストール CD-ROM」 と呼びます。	<ul style="list-style-type: none"> Windows 用 Cell Manager Windows 用インストール サーバ Novell NetWare クライアント PDF 形式のマニュアル (英語版 : DOCS ディレクトリ、日本語版 : DOCS/JPN ディレクトリ) Windows 用 AutoPass Windows プラットフォーム用の製品デモ 製品情報

表 C-1 Data Protector CD-ROM の一覧 (続き)

CD 番号	CD-ROM のタイトル	内容
14	HP Data Protector Integrations with OpenView; Open File Backup; and agents for OpenVMS & MPE clients	<ul style="list-style-type: none"> • OpenView 統合ソフトウェア • オープンファイルマネージャ インストールパッケージ • OpenVMS クライアント • MPE クライアント • PDF 形式のマニュアル (英語版 : DOCS ディレクトリ、日本語版 : DOCS/JPN ディレクトリ) • 製品情報
15	HP OpenView Storage Data Protector - Media Operations for Windows	<ul style="list-style-type: none"> • メディア操作のインストールパッケージ • メディア操作のマニュアル

- a. Solaris 用または Linux 用のインストール サーバ インストール CD-ROM から UNIX クライアントをローカルにインストールすることはできません。ローカル インストールには、いずれかの HP-UX 用インストール サーバ CD-ROM を使用してください。

CD-ROM から Data Protector をインストールする場合の追加手順

Data Protector を CD-ROM からインストールする手順は、DVD-ROM を使用する場合とほとんど同じです。

- **UNIX の場合:** インストールパッケージは 3 枚の CD-ROM で構成されています (1 枚は Cell Manager 用、残り 2 枚はインストール サーバ用)。そのためインストール作業には、複数の CD-ROM を使用する必要があります。
- **Windows の場合:** プラットフォーム別にそれぞれ 1 枚の CD-ROM に収録されています。そのため Windows の場合は、CD-ROM からのインストール手順も、DVD-ROM を使用する場合と変わりません。ただし、インストールパスは以下のように異なります。

32 ビット システムの場合: ¥i386¥setup.exe

64 ビット システムの場合: ¥x8664¥setup.exe

CD-ROM からの UNIX 用 Cell Manager のインストール

ヒント Cell Manager とインストール サーバを同一システム上にインストールする場合は、まず DP_DEPOT ディレクトリをディスク上にコピーし、次に omnisetup.sh -CM -IS1 -IS2 コマンドを実行することにより、この作業をワン ステップで実行できます。

omnisetup.sh コマンドの説明については、CD-ROM の <Mount_point>/LOCAL_INSTALL ディレクトリにある README ファイルか、CD-ROM の <Mount_point>/DOCS/C/MAN ディレクトリにある『HP OpenView Storage Data Protector Command Line Interface Reference』を参照してください。

HP-UX システム、Solaris システム、または Linux システムに UNIX 用 Cell Manager をインストールするには、以下の手順に従ってください。

1. 適切な Cell Manager インストール CD-ROM をドライブに挿入し、マウント ポイントにマウントします。

例：

```
mkdir /cdrom
mount /dev/dsk/c0t0d0 /cdrom
```

必要であれば、Data Protector をディスク上のデポからインストールすることもできます。その場合は、以下の手順に従ってください。

- インストール ファイルが格納されている DP_DEPOT ディレクトリ、LOCAL_INSTALL ディレクトリ、および AUTOPASS ディレクトリをローカル ディスクにコピーするには、以下のコマンドを実行します。

```
mkdir <directory>
cp -r /cdrom/DP_DEPOT <directory>
cp -r /cdrom/LOCAL_INSTALL <directory>
cp -r /cdrom/AUTOPASS <directory>
```

- CD-ROM 全体をローカル ディスクにコピーするには、以下のコマンドを実行します。

```
cp -r /cdrom <cd_image_dir>
```

2. omnisetup.sh コマンドを実行します。

このコマンドを CD-ROM から実行するには、以下のように入力します。

```
cd /cdrom/LOCAL_INSTALL
./omnisetup.sh -CM
```

ディスクからインストールを開始するには、以下の手順に従ってください。

- DP_DEPOT ディレクトリ、LOCAL_INSTALL ディレクトリ、および AUTOPASS ディレクトリを CD-ROM からローカル ディスク上の <directory> にコピーした場合は、omnisetup.sh コマンドが格納されているディレクトリに移動して以下を実行します。

```
cd <directory>/LOCAL_INSTALL
./omnisetup.sh -CM
```

- CD-ROM 全体を <cd_image_dir> にコピーした場合は、-CM パラメータ付きで omnisetup.sh コマンドを実行します。

```
cd <cd_image_dir>/LOCAL_INSTALL
./omnisetup.sh -CM
```

3. **HP-UX および Solaris の場合**、omnisetup.sh コマンドを実行するとプロンプトが表示され、購入済みライセンスのパスワードを HP Password Delivery Center の Web サーバからインターネットを介して直接ダウンロードしてインストールする場合は、HP OpenView AutoPass ユーティリティをインストールまたはアップグレードするよう指示されます。詳細は 309 ページの「HP OpenView AutoPass ユーティリティを使用した恒久パスワードの取得とインストール」を参照してください。AutoPass はできるだけインストールすることをお勧めします。

AutoPass を MC/ServiceGuard にインストールする場合は、すべてのノードにインストールする必要があります。

プロンプトが表示されたら、**[Return]** キーを押して AutoPass をインストールまたはアップグレードします。AutoPass をインストールまたはアップグレードしない場合は、**n** と入力します。

Linux には、HP OpenView AutoPass はインストールされません。

注記

Cell Manager を Solaris 9 にインストールした場合は、インストール サーバを使用して Cell Manager 上に Disk Agent をリモート インストールすることができます。詳細については、“Remote Installation of the Data Protector Clients” on page 48 を参照するか、または ob2install のマンページを参照してください。

CD-ROM からの UNIX 用インストール サーバのインストール

UNIX 用インストール サーバは 2 枚のインストール CD に収録されています。そのため、2 枚目のインストール サーバ CD を使用して、インストールを継続する必要があります。

HP-UX システム、Solaris システム、または Linux システムに UNIX 用 Cell Manager をインストールするには、以下の手順に従ってください。

インストールメディアとして CD-ROM を使用

1. 適切なインストール サーバインストール CD-ROM をドライブに挿入し、マウントポイントにマウントします。

例：

```
mkdir /cdrom
mount /dev/dsk/c0t0d0 /cdrom
```

必要であれば、Data Protector をディスク上のデポからインストールすることもできます。その場合は、以下の手順に従ってください。

- インストールファイルが格納されている DP_DEPOT ディレクトリと LOCAL_INSTALL ディレクトリをローカルディスクにコピーするには、以下のコマンドを実行します。

```
mkdir <directory>
cp -r /cdrom/DP_DEPOT <directory>
cp -r /cdrom/LOCAL_INSTALL <directory>
```

2 枚目のインストール サーバインストール CD-ROM をマウントし、1 枚目と同様に、すべてのファイルを DP_DEPOT ディレクトリからインストールディレクトリにコピーします。

```
cp -r /cdrom/DP_DEPOT <directory>
```

- CD-ROM 全体をローカルディスクにコピーするには、以下のコマンドを実行します。

```
cp -r /cdrom <cd_image_dir>
```

2. omnisetup.sh コマンドを実行します。

このコマンドを CD-ROM から実行するには、以下のように入力します。

```
cd /cdrom/LOCAL_INSTALL
./omnisetup.sh -IS1
```

ディスクからインストールを開始するには、以下の手順に従ってください。

- DP_DEPOT ディレクトリおよび LOCAL_INSTALL ディレクトリを両方の CD-ROM からローカルディスク上の <directory> にコピーした場合は、omnisetup.sh コマンドが格納されているディレクトリに移動して以下を実行します。

```
cd <directory>/LOCAL_INSTALL
./omnisetup.sh -IS1 -IS2
```

- CD-ROM 全体を <cd_image_dir> にコピーした場合は、-IS1 パラメータ付きで omnisetup.sh コマンドを実行します。

```
cd <cd_image_dir>/LOCAL_INSTALL  
./omnisetup.sh -IS1
```

- マウントした CD-ROM または CD-ROM イメージからインストールしている場合は、2 枚目のインストール サーバ インストール CD-ROM についても手順 1 と 2 を繰り返します。ただし、今回は `-IS1` パラメータではなく `omnisetup.sh -IS2` パラメータを使用します。

CD-ROM からの UNIX クライアントのインストール

制限事項

UNIX パッケージのローカル インストールには、*HP-UX 用インストール サーバ インストール CD-ROM* を使用する必要があります。この CD-ROM にはすべての UNIX クライアントが含まれています。つまり、Solaris クライアントや Linux クライアントのインストールには、Solaris 用または Linux 用のインストール サーバ インストール CD-ROM ではなく、HP-UX 用インストール サーバ インストール CD-ROM を使用しなければなりません。

インストール手順

インストール手順は、UNIX 用インストール サーバ DVD-ROM を使用する場合とほとんど同じですが、1 枚目の CD-ROM をインストールした後で、2 枚目の CD-ROM を挿入してインストール手順を繰り返す必要があります。

詳細は 119 ページの「UNIX クライアントのローカル インストール」を参照してください。

CD-ROM から Data Protector をアップグレードする場合の追加手順

Data Protector を CD-ROM からアップグレードする手順は、DVD-ROM を使用する場合とほとんど同じです。

- UNIX の場合:** インストール パッケージは 3 枚の CD-ROM で構成されています (1 枚は Cell Manager 用、残り 2 枚はインストール サーバ用)。そのためアップグレード作業には、複数の CD-ROM を使用する必要があります。
- Windows の場合:** プラットフォーム別にそれぞれ 1 枚の CD-ROM に収録されています。そのため Windows の場合は、CD-ROM からのアップグレード手順も、DVD-ROM を使用する場合と変わりません。ただし、インストール パスは以下のように異なります。

32 ビット システムの場合: `%i386%setup.exe`

64 ビット システムの場合: `%x86_64%setup.exe`

UNIX 用 Cell Manager のアップグレード

HP-UX 用または Solaris 用の Cell Manager を Data Protector Draft にアップグレードするには、以下の手順に従います。

1. 適切なインストール CD-ROM をドライブに挿入し、マウント ポイントにマウントします。

例：

```
mkdir /cdrom
mount /dev/c0d0t0 /cdrom
```

オプションで、ディスク上のデポから Data Protector をインストールする場合は、以下の手順を実行します。

- インストール ファイルが格納されている DP_DEPOT ディレクトリ、AUTOPASS ディレクトリ、および LOCAL_INSTALL ディレクトリをローカル ディスクにコピーする場合は、以下のコマンドを実行します。

```
mkdir <directory>
cp -r /cdrom/DP_DEPOT <directory>
cp -r /cdrom/AUTOPASS <directory>
cp -r /cdrom/LOCAL_INSTALL <directory>
```

- CD-ROM 全体をローカル ディスクにコピーする場合は、以下のコマンドを実行します。

```
cp -r /cdrom <cd_image_dir>
```

2. omnisetup.sh コマンドを実行します。

このコマンドを CD-ROM から実行するには、以下のように入力します。

```
cd /cdrom/LOCAL_INSTALL
./omnisetup.sh
```

ディスクからインストールを開始する場合は、以下の手順を実行します。

- DP_DEPOT ディレクトリおよび LOCAL_INSTALL ディレクトリを CD-ROM からローカル ディスク上の <directory> にコピーした場合は、omnisetup.sh コマンドが格納されているディレクトリに移動して以下を実行します。

```
cd <directory>/LOCAL_INSTALL
./omnisetup.sh
```

- CD-ROM 全体を <cd_image_dir> にコピーした場合は、omnisetup.sh コマンドをパラメータなしで実行します。

```
cd <cd_image_dir>/LOCAL_INSTALL
./omnisetup.sh
```

3. omnisetup.sh コマンドを実行するとプロンプトが表示され、購入済みライセンスのパスワードを HP Password Delivery Center の Web サーバからインターネットを介して直接ダウンロードしてインストールする場合は、HP OpenView AutoPass ユーティリティをインストールまたはアップグレードするよう指示されます。AutoPass ユーティリティの詳細は、309 ページの「HP OpenView AutoPass ユーティリティを使用した恒久パスワードの取得とインストール」を参照してください。AutoPass はできるだけインストールすることをお勧めします。

AutoPass を MC/ServiceGuard にインストールする場合は、すべてのノードでインストールまたはアップグレードしなければなりません。

プロンプトが表示されたら、**[Return]** キーを押して AutoPass をインストールまたはアップグレードします。AutoPass をインストールまたはアップグレードしない場合は、**n** と入力します。

Data Protector のバージョン A.05.x が検出されると、アップグレード手順が自動的に開始されます。クリーン インストールを実行する (前のバージョンのデータベースを削除する) 場合は、旧バージョンをアンインストールしてからインストールを再開してください。

インストールの詳細は、20 ページの「UNIX 用 Cell Manager のインストール」および 37 ページの「UNIX 用のインストール サーバのインストール」を参照してください。

4. セル内に Windows クライアントがある場合に、Data Protector A.05.00 または A.05.10 からアップグレードしようとする、IDB 内にあるファイル名の変換が実行されることが表示されます。IDB の変換は、国際文字セットを含むファイル名を正しく処理するために必要です。詳細は “Conversion of File Names in the IDB” on page 255 を参照してください。
5. システム上にインストール サーバがインストールされている場合は、omnisetup.sh コマンドからプロンプトが表示され、適切な HP-UX 用または Solaris 用インストール サーバ インストール CD-ROM を挿入してインストールを継続するよう指示されます。適切な HP-UX 用または Solaris 用インストール サーバ インストール CD-ROM を使用して手順 1 および 2 のみを実行して、インストール サーバをアップグレードしてください。Data Protector インストール CD-ROM の一覧は、C-2 ページの「Data Protector のインストール CD-ROM」を参照してください。

UNIX 用インストール サーバのアップグレード

omnisetup.sh コマンドの実行時に、HP-UX 用または Solaris 用のインストール サーバは、自動的にアップグレードされます。

HP-UX では、このコマンドは `swinstall` ユーティリティを使用して、既存のパッケージセットを直接アップグレードします。Solaris では、このコマンドは `pkgrm` ユーティリティを使用して既存のパッケージセットを削除し、`pkgadd` ユーティリティを使用して新しいパッケージをインストールします。

インストールサーバがクライアント コンポーネントとともにインストールされている場合、インストールサーバは `omnisetup.sh` コマンドで削除されます。この場合、`omnisetup.sh -IS` コマンドを使用して新しいインストールサーバ デポをインストールした後、アップグレード後のインストールサーバを再度インポートしてください。詳細な作業手順は、187 ページの「セルへのインストールサーバのインポート」を参照してください。

アップグレード手順

HP-UX 用または Solaris 用のインストールサーバを Data Protector Draft にアップグレードするには、以下の手順に従います。

1. 適切なインストール CD-ROM をドライブに挿入し、マウント ポイントにマウントします。

例：

```
mkdir /cdrom
mount /dev/c0d0t0 /cdrom
```

オプションで、ディスク上のデポから Data Protector をインストールする場合は、以下の手順を実行します。

- インストールファイルが格納されている `DP_DEPOT` ディレクトリおよび `LOCAL_INSTALL` ディレクトリをローカル ディスクにコピーする場合は、以下のコマンドを実行します。

```
mkdir <directory>
cp -r /cdrom/DP_DEPOT <directory>
cp -r /cdrom/LOCAL_INSTALL <directory>
```

2 枚目のインストールサーバインストール CD-ROM をマウントし、1 枚目と同様に、すべてのファイルを `DP_DEPOT` ディレクトリからインストール ディレクトリにコピーします。

```
cp -r /cdrom/DP_DEPOT <directory>
```

- CD-ROM 全体をローカル ディスクにコピーするには、以下のコマンドを実行します。

```
cp -r /cdrom <cd_image_dir>
```

2. `omnisetup.sh` コマンドを実行します。

このコマンドを CD-ROM から実行するには、以下のように入力します。


```
cd /cdrom/LOCAL_INSTALL  
./omnisetup.sh
```

ディスクからインストール作業を起動する場合は、以下の手順で行います。

- DP_DEPOT ディレクトリおよび LOCAL_INSTALL ディレクトリを CD-ROM からローカルディスク上の *<directory>* にコピーした場合は、omnisetup.sh コマンドが格納されているディレクトリに移動して以下を実行します。

```
cd <directory>/LOCAL_INSTALL  
./omnisetup.sh
```

- CD-ROM 全体を *<cd_image_dir>* にコピーした場合は、omnisetup.sh コマンドをパラメータなしで実行します。

```
cd <cd_image_dir>/LOCAL_INSTALL  
./omnisetup.sh
```

3. CD-ROM から omnisetup.sh を実行したか、CD-ROM 全体をディスクにコピーした場合は、2 枚目のインストール サーバ インストール CD-ROM を使って手順を繰り返します。

付録 C
インストールメディアとして CD-ROM を使用

用語集

ACSLs

(StorageTek 固有の用語)

Automated Cartridge System Library Server の略語。ACS (Automated Cartridge System: 自動カートリッジシステム) を管理するソフトウェア。

Active Directory

(Windows 固有の用語)

Windows ネットワークで使用されるディレクトリ サービス。ネットワーク上のリソースに関する情報を格納し、ユーザーやアプリケーションからアクセスできるように維持します。このディレクトリ サービスでは、サービスが実際に稼動している物理システムの違いに関係なく、リソースに対する名前や説明の付加、検索、アクセス、および管理を一貫した方法で実行できます。

AML

(EMASS/GRAU 固有の用語)

Automated Mixed-Media library (自動混合メディア ライブラリ) の略。

ASR セット

フロッピー ディスク上に保存されたファイルのコレクション。交換用ディスクの適切な再構成 (ディスクパーティション化と論理ボリュームの構成) およびフルクライアントバックアップでバックアップされた元のシステム構成とユーザーデータの自動復旧に必要となります。

これらのファイルは、バックアップメディア上に保存されると共に、Cell Manager 上の <Data_Protector_home>%Config%Server %dr%asr ディレクトリ (Windows 用 Cell Manager の場合) または

/etc/opt/omni/server/dr/asr/ ディレクトリ (UNIX 用 Cell Manager の場合) に保存されます。ASR アーカイブファイルは、障害発生後に複数のフロッピー ディスクに展開されます。32 ビット版の Windows XP/.NET で

は 3 枚のフロッピー ディスクに展開され、64 ビット版の Windows XP/.NET の場合は 4 枚のフロッピー ディスクに展開されます。これらのフロッピー ディスクは、ASR の実行時に必要となります。

BACKINT

(SAP R/3 固有の用語)

SAP R/3 バックアップ プログラムが、オープン インタフェースへの呼び出しを通じて

Data Protector backint インタフェース ソフトウェアを呼び出し、Data Protector ソフトウェアと通信できるようにします。バックアップ時および復元時には、SAP R/3 プログラムが Data Protector backint インタフェースを通じてコマンドを発行します。

BC

(EMC Symmetrix 固有の用語)

Business Continuance の略。BC は、EMC Symmetrix 標準デバイスのインスタントコピーに対するアクセスおよび管理を可能にするプロセスです。

BCV も参照。

BC

(HP StorageWorks Disk Array XP 固有の用語)

Business Copy XP の略。BC を使うと、HP StorageWorks Disk Array XP LDEV の内部コピーをデータバックアップやデータ複製などの目的で維持できます。これらのコピー (セカンダリ ボリュームまたは S-VOL) は、プライマリ ボリューム (P-VOL) から分離して、バックアップや開発などの用途に応じた別のシステムに接続することができます。バックアップ目的の場合、P-VOL をアプリケーション システムに接続し、S-VOL ミラーセットのいずれかをバックアップシステムに接続する必要があります。

HP StorageWorks Disk Array XP LDEV、

CA、Main Control Unit、アプリケーションシステム、およびバックアップシステムも参照。

BC EVA

(HP StorageWorks EVA 固有の用語)

Business Copy EVA は、ローカル複製ソフトウェアソリューションです。EVA ファームウェアのスナップショット機能とクローン機能を使用して、ソース ボリュームのポイントインタイム コピー (複製) を作成できます。**複製、ソース ボリューム、スナップショット、および CA+BC EVA も参照。**

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 Continuity Volumes として規定します。

BCV も参照。

BCV

(EMC Symmetrix 固有の用語)

Business Continuity Volumes の略。BCV デバイスは ICDA 内であらかじめ構成された専用の SLD です。ビジネスの継続運用を可能にするために使用されます。BCV デバイスには、これらのデバイスによりミラー化される SLD のアドレスとは異なる、個別の SCSI アドレスが割り当てられます。BCV デバイスは、保護を必要とする一次 EMC Symmetrix SLD の分割可能なミラーとして使用されます。

BC および BC Process も参照。

BC VA

(HP StorageWorks Virtual Array 固有の用語)

BC は Business Copy の略。Business Copy VA により、HP StorageWorks Virtual Array

LUN の内部コピーをデータ バックアップやデータ複製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、開発などさまざまな目的に使用できます。バックアップ目的で使用されるときは、元 (親) の LUN はアプリケーションシステムに接続され、Business Copy (子) LUN はバックアップシステムに接続されません。

HP StorageWorks Virtual Array LUN、アプリケーションシステム、およびバックアップシステムも参照。

BRARCHIVE

(SAP R/3 固有の用語)

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

SAPDBA、BRBACKUP および BRRESTORE も参照。

BRBACKUP

(SAP R/3 固有の用語)

SAP R/3 バックアップ ツールの 1 つ。制御ファイル、個々のデータ ファイル、またはすべてのテーブルスペースをオンラインでもオフラインでもバックアップできます。また、必要に応じて、オンライン REDO ログ ファイルをバックアップすることもできます。

SAPDBA、BRARCHIVE および BRRESTORE も参照。

BRRESTORE

(SAP R/3 固有の用語)

SAP R/3 のツール。以下の種類のファイルを復元するために使います。

- BRBACKUP で保存されたデータベースデータ ファイル、制御ファイル、オンライン REDO ログ ファイル
- BRARCHIVE でアーカイブされた REDO ログ ファイル
- BRBACKUP で保存された非データベース ファイル

ファイル、テーブル スペース、バックアップ全体、REDO ログ ファイルのログ シーケンス番号、またはバックアップのセッション ID を指定することができます。

SAPDBA、BRBACKUP および **BRARCHIVE** も参照。

BSM

Data Protector Backup Session Manager の略。バックアップ セッションを制御します。このプロセスは、常に Cell Manager システム上で稼動します。

CA

(HP StorageWorks Disk Array XP 固有の用語)

Continuous Access XP の略。CA では、データ複製、バックアップ、および障害復旧などの目的で HP StorageWorks Disk Array XP LDEV のリモート コピーを作成および維持できます。CA を使用するには、メイン (プライマリ) ディスク アレイとリモート (セカンダリ) ディスク アレイが必要です。オリジナルのデータを格納し、アプリケーション システムに接続されている CA プライマリ ボリューム (P-VOL) がメイン ディスク アレイに格納されます。リモート ディスク アレイには、バックアップ システムに接続されている CA セカンダリ ボリューム (S-VOL) が格納されます。

BC (*HP StorageWorks Disk Array XP 固有の*

用語)、**Main Control Unit** および **HP StorageWorks Disk Array XP LDEV** も参照。

CA+BC EVA

(HP StorageWorks EVA 固有の用語)

Continuous Access (CA) EVA と Business Copy (BC) EVA を併用すると、リモート EVA 上にソース ボリュームのコピー (複製) を作成して保持でき、その後、これらのコピーをそのリモート アレイ上でローカル複製のソースとして使用できます。

BC EVA、複製、ソース ボリューム 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

Cell Manager

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。

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 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 コピーおよび集約セッション マネージャ (Copy and Consolidation Session Manager) の略。このプロセスは、オブジェクト コピー セッションとオブジェクト集約セッションを制御し、Cell Manager システム上で動作します。

Data Protector イベント ログ

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

イベントは、Cell Manager の

<Data_Protector_home>%log%server%Ob2EventLog.txt ファイルに記録されます。このイベント ログにアクセスできる Data Protector ユーザーは、Admin ユーザーグループに所属しているか、または「レポートと通知」のユーザー権限が付与されている Data Protector ユーザーだけです。イベントログ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。

Data Replication (DR) グループ

(HP StorageWorks EVA 固有の用語)

EVA 仮想ディスクの論理グループ。共通の性質を持ち、同じ CA EVA ログを共有していれば、最大 8 組のコピー セットを含めることができます。

コピー セットも参照。

Dbject

(Informix Server 固有の用語)

Informix Server の物理的なデータベース オブジェクト。blob space、db space、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。バックアップに使用される Data Protector メディアごとに 1 つの DC バイナリ ファイルが作成されます。

DC ディレクトリ

詳細カタログ (DC) ディレクトリは、詳細カタログ バイナリ ファイル (DCBF) で構成されており、そのファイルの中にはファイルバージョンについての情報が保管されています。これは、IDB の DCBF 部分を表し、IDB 全体の約 80% の容量を占めます。デフォルトの DC ディレクトリは、dcbf ディレクトリと呼ばれ、<Data_Protector_home>%db40 ディレクトリ (Windows 用 Cell Manager の場合) または /var/opt/omni/server/db40 ディレクトリ (UNIX 用 Cell Manager の場合) に配置されています。他の DC ディレクトリを作成して、適切な場所に置くことができます。1 つのセルでサポートされる DC ディレクトリは 10 個までです。DC ディレクトリのデフォルト最大サイズは 4GB です。

DHCP サーバ

Dynamic Host Configuration Protocol

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

Disk Agent

クライアントのバックアップと復元を実行するためにクライアント システム上にインストールする必要があるコンポーネントの 1 つ。Disk Agent は、ディスクに対するデータの読み書きを制御します。バックアップセッション中には、Disk Agent がディスクからデータを読み取って、Media Agent に送信してデー

用語集

Disk Agent の同時処理数

データをデバイスに移動させます。復元セッション中には、Disk Agent が Media Agent からデータを受信して、ディスクに書き込みます。

Disk Agent の同時処理数

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

DMZ

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

DNS サーバ

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

DR OS

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。

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。

EMC Symmetrix Agent (SYMA)

(EMC Symmetrix 固有の用語)

Symmetrix Agent (SYMA) 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平行 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、その反対側には平行 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 と平行 SCSI デバイスの間で移動することができます。

fnames.dat

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

GUI

Data Protector には、各種プラットフォーム (HP-UX、Solaris、Windows) に対応したグラフィカル ユーザー インタフェース (GUI) が用意されており、すべての構成タスク、管理タスクおよび処理タスクに容易にアクセスできます。

Holidays ファイル

休日に関する情報を格納するファイル。このファイルを通じて、休日の設定を変更できます。Holidays ファイルのパスは、
/etc/opt/omni/server/Holidays (UNIX 用 Cell Manager の場合) または
<Data_Protector_home>\¥Config¥Server
¥holidays (Windows 用 Cell Manager の場合) です。

HP ITO

OVO を参照。

HP OpC

OVO を参照。

HP OpenView SMART Plug-In (SPI)

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

HP OVO

OVO を参照。

HP StorageWorks Disk Array XP LDEV

HP StorageWorks Disk Array XP の物理ディスクの論理パーティション。LDEV は、Continuous Access XP (CA) 構成および Business Copy XP (BC) 構成で複製すること

ができるエンティティで、スタンドアロンのエンティティとしても使用できます。

BC (HP StorageWorks Disk Array XP 固有の用語)、**CA** (HP StorageWorks Disk Array XP 固有の用語)、および**複製**も参照。

HP StorageWorks EVA SMI-S Agent

Data Protector のソフトウェア モジュール。HP StorageWorks Enterprise Virtual Array 用統合ソフトウェアに必要なタスクをすべて実行します。EVA SMI-S Agent を使用すると、受信した要求と CV EVA 間のやり取りを制御する HP StorageWorks SMI-S EVA プロバイダを通じてアレイを制御できます。

Command View (CV) EVA、および**HP StorageWorks SMI-S EVA プロバイダ**も参照。

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、どのデバイス上やライブラリ上に構成されているかについての情報が格納されます。

IDB 復旧ファイル

IDB バックアップ、メディア、バックアップ用デバイスに関する情報を含む IDB ファイル (obrindex.dat)。この情報により、IDB の復旧を大幅に簡素化できます。IDB トランザクション ログと共にこのファイルを他の IDB ディレクトリとは別の物理ディスクに移動し、さらにこのファイルのコピーを作成することをお勧めします。

Inet

Data Protector セル内の各 UNIX システムまたは Windows システム上で動作するプロセス。このプロセスは、セル内のシステム間の通信と、バックアップおよび復元に必要なその他のプロセスの起動を受け持ちます。システムに Data Protector をインストールすると、Inet サービスが即座に起動されます。Inet プロセスは、inetd デーモンにより開始されます。

Informix Server

(Informix Server 固有の用語)

Informix Dynamic Server のことです。

Informix Server 用の CMD スクリプト

(Informix Server 固有の用語)

Informix Server データベースの構成時に INFORMIXDIR 内に作成される Windows CMD スクリプト。環境変数を Informix Server にエクスポートするコマンド一式が含まれています。

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。

keychain

秘密キーを復号化する際、手動でパスワードを入力する手間を省くツール。セキュア シェルを使用してリモート インストールを実

行する場合、このツールをインストールサーバにインストールして構成する必要があります。

LBO

(EMC Symmetrix 固有の用語)

Logical Backup Object (論理バックアップオブジェクト)の略。LBOは、EMC

Symmetrix/Fastrax 環境内で保存/取得されるデータオブジェクトです。LBOはEMC Symmetrixによって1つのエンティティとして保存/取得され、部分的には復元できません。

LISTENER.ORA

(Oracle 固有の用語)

Oracleの構成ファイルの1つ。サーバ上の1つまたは複数のTNSリスナを定義します。

log_full シェル スクリプト

(Informix Server UNIX 固有の用語)

ON-Bar に用意されているスクリプトの1つで、Informix Server で logfull イベント警告が発行された際に、論理ログファイルのバックアップを開始するために使用できます。Informix Server の ALARMPROGRAM 構成パラメータは、デフォルトで、<INFORMIXDIR>/etc/log_full.sh に設定されます。ここで、<INFORMIXDIR>は、Informix Server ホームディレクトリです。論理ログファイルを継続的にバックアップしたくない場合は、ALARMPROGRAM 構成パラメータを <INFORMIXDIR>/etc/no_log.sh に設定してください。

Lotus C API

(Lotus Domino Server 固有の用語)

Lotus Domino Server と Data Protector などのバックアップソリューションの間でバックアップ情報および復元情報を交換するためのインタフェース。

LVM

LVM (Logical Volume Manager: 論理ボリューム マネージャ)は、HP-UX システム上で物理ディスクスペースを構造化し、論理ボリュームにマッピングするためのサブシステムです。LVM システムは、複数のボリュームグループで構成されます。各ボリュームグループには、複数のボリュームが含まれます。

Main Control Unit (MCU)

(HP StorageWorks Disk Array XP 固有の用語)

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

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) クライアントです。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 復旧ファイルを参照。

OBDR 対応デバイス

ブート可能ディスクを装填した CD-ROM ドライブをエミュレートできるデバイス。バックアップデバイスとしてだけでなく、障害復旧用のブートデバイスとしても使用可能です。

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 Server 固有の用語)

Informix Server のためのバックアップと復元のシステム。ON-Bar により、Informix Server データのコピーを作成し、後でそのデータを復元することが可能になります。ON-Bar のバックアップと復元のシステムには、以下のコンポーネントが含まれます。

- onbar コマンド

- バックアップソリューションとしての Data Protector
- XBSA インタフェース
- ON-Bar カタログ テーブル。これは、dbobject をバックアップし、複数のバックアップを通して dbobject のインスタンスをトラッキングするために使われます。

ONCONFIG

(Informix Server 固有の用語)

アクティブな ONCONFIG 構成ファイルの名前を指定する環境変数。ONCONFIG 環境変数が存在しない場合、Informix Server が <INFORMIXDIR>%etc (Windows の場合)、または <INFORMIXDIR>/etc/ (UNIX の場合) ディレクトリの ONCONFIG ファイルにある構成値を使います。

OpC

OVO を参照。

OpenSSH

さまざまな認証方式と暗号化方式を採用することにより、リモートマシンへの安全なアクセスを提供するネットワーク接続ツールのセット。セキュアシェルを使用してリモートインストールを実行する場合、インストールサーバとクライアントにこれをインストールして構成する必要があります。

Oracle Data Guard

(Oracle 固有の用語)

Oracle Data Guard は Oracle の主要な障害復旧ソリューションです。プロダクション(一次)データベースのリアルタイムコピーであるスタンバイデータベースを最大 9 個まで保持することにより、破損、データ障害、人為ミス、および災害からの保護を提供します。プロダクション(一次)データベースに障害が発生すると、フェイルオーバーによりスタンバイデータベースの 1 つを新しい一次データベースにすることができます。また、プロダクション処理を現在の一次データベースから

ORACLE_SID

スタンバイ データベースに迅速に切り替えたり、元に戻したりできるため、保守作業のための計画ダウンタイムを縮小することができます。

ORACLE_SID

(Oracle 固有の用語)

Oracle Server インスタンスの一意な名前。別の Oracle Server に切り替えるには、目的の <ORACLE_SID> を指定します。<ORACLE_SID> は、TNSNAMES.ORA ファイル内の接続記述子の CONNECT DATA 部分と LISTENER.ORA ファイル内の TNS リスナの定義に含まれています。

Oracle インスタンス

(Oracle 固有の用語)

1 つまたは複数のシステムにインストールされた個々の Oracle データベース。1 つのコンピュータ システム上で、複数のデータベース インスタンスを同時に稼働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。このユーザーは Oracle SYSDBA 権限または SYSOPER 権限を持っている必要があります。

- <password> は、Oracle パスワード ファイル (orapwd) に指定されているパスワードに一致する必要があります。これは、データベース管理を行うユーザーの認証に使用されるファイルです。

- <service> は、ターゲット データベースの SQL*Net サーバプロセスを識別する名前です。

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.pls というファイル名で保存されます。保存場所は、<Data_Protector_home>%Config%Server %dr%p1s ディレクトリ (Windows 用 Cell Manager の場合) または /etc/opt/omni/server/dr/p1s ディレクトリ (UNIX 用 Cell Manager の場合) です。

RAID

Redundant Array of Inexpensive Disks の略。

RAID Manager XP

(HP StorageWorks Disk Array XP 固有の用語)

RAID Manager XP アプリケーションには、CA アプリケーションおよび BC アプリケーションのステータスを報告 / 制御するコマンドが豊富に用意されています。これらのコマンドは、RAID Manager インスタンスを通じて、StorageWorks Disk Array XP Disk Control Unit と通信します。このインスタンスは、コマンドを一連の低レベル SCSI コマンドに変換します。

RAID Manager ライブラリ

(HP StorageWorks Disk Array XP 固有の用語)

Solaris システム上の Data Protector では、RAID Manager ライブラリを内部的に使用して、HP StorageWorks Disk Array XP の構成データ、ステータス データ、およびパフォーマンス データにアクセスします。さらに、一連の低レベル SCSI コマンドに変換される関数呼び出しを通じて、StorageWorks Disk Array XP の主要な機能にアクセスします。

raw ディスクのバックアップ

ディスク イメージのバックアップを参照。

RCU

(HP StorageWorks 固有の用語)

Remote Control Unit (RCU) は、CA 構成の中で MCU (Main Control 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

Remote Control Unit

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 Control 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 システム上で稼働します。

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、復元、オブジェクト コピー、オブジェクト集約、およびメディア管理のセッション中に生成されたセッション メッセージが格納される部分です。セッションごとに1つのバイナリファイルが作成されます。バイナリファイルは、年と月に基づいて分類されます。

sqlhosts ファイル

(Informix Server 固有の用語)

Informix Server の接続情報ファイル (UNIX) またはレジストリ (Windows)。各データベース サーバの名前の他、ホスト コンピュータ上のクライアントが接続できるエイリアスが格納されます。

SRDF

(EMC Symmetrix 固有の用語)

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

SRD ファイル

SRD (System Recovery Data: システム復旧データ) ファイルには、障害発生時にオペレーティング システムをインストールおよび構成するために必要なシステム情報が含まれています。SRD ファイルは ASCII ファイル

で、CONFIGURATION バックアップが Windows クライアント上で実行され Cell Manager に保存される時に生成されます。

SSE Agent

(HP StorageWorks Disk Array XP 固有の用語)

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

sst.conf ファイル

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

st.conf ファイル

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

StorageTek ACS ライブラリ

(StorageTek 固有の用語)

ACS (Automated Cartridge System) は、1 つのライブラリ管理ユニット (LMU) と、このユニットに接続された 1 ~ 24 個のライブラリ記憶域モジュール (LSM) からなるライブラリシステム (サイロ) です。

Sybase Backup Server API

(Sybase 固有の用語)

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

Sybase SQL Server

(Sybase 固有の用語)

Sybase のクライアント / サーバ アーキテクチャにおけるサーバ。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。

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 Server 固有の用語)

ON-Bar と Data Protector の間の相互通信には、X/Open Backup Services Application Programmer's Interface (XBSA) が使用されます。

XCOPY エンジン

(ダイレクト バックアップ固有の用語)

SCSI-3 のコピー コマンド。SCSI ソース アドレスを持つストレージ デバイスから SCSI あて先アドレスを持つバックアップ デバイスにデータをコピーし、ダイレクト バックアップを可能にします。XCOPY では、ソース デバイスからデータをブロック (ディスクの場合) またはストリーム (テープの場合) としてあて先 デバイスにコピーします。これにより、データをストレージ デバイスから読み込んであて先 デバイスに書き込むまでの一連の処理が、制御サーバをバイパスして行われます。

ダイレクト バックアップも参照。

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、インストール 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 REDO ログ

(Oracle 固有の用語)

オフライン REDO ログとも呼ばれます。Oracle データベースが ARCHIVELOG モードで動作している場合、各オンライン REDO ログが最大サイズまで書き込まれると、アーカイブ先にコピーされます。このコピーを

アーカイブ ロギング

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働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、完全に復元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 固有の用語)

記憶域管理を行う Microsoft Exchange Server のサービス。Microsoft Exchange Server のインフォメーションストアは、メールボックスストアとパブリック フォルダ ストアの 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。

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。

エクステンジャ

SCSI エクステ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。

オブジェクト集約

フルバックアップと 1 回以上の増分バックアップから成るバックアップ オブジェクトの復元チェーンを、新しい集約バージョンのオブジェクトにマージするプロセス。このプロセスは合成バックアップ処理の一部です。このプロセスの結果、指定されたバックアップ オブジェクトの合成フルバックアップが生成されます。

オブジェクト集約セッション

フルバックアップと 1 回以上の増分バックアップから成るバックアップ オブジェクトの復元チェーンを、新しい集約バージョンのオブジェクトにマージするプロセス。

オブジェクトのコピー

オブジェクトのミラーリング

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

オブジェクトのミラーリング

バックアップ セッション中に、同一のデータを複数のメディア セットに書き込むプロセス。Data Protector では、すべてまたは一部のバックアップ オブジェクトを1つまたは複数のメディア セットにミラーできます。

オブジェクト ミラー

オブジェクトのミラーリングを使用して作成されるバックアップ オブジェクトのコピー。オブジェクトのミラーは通常オブジェクト コピーと呼ばれます。

オフライン REDO ログ

アーカイブ REDO ログを参照。

オフライン バックアップ

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

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

ゼロ ダウンタイム バックアップ (ZDB) およびオンライン バックアップを参照。

オフライン復旧

オフライン復旧は、ネットワーク障害などにより Cell Manager にアクセスできない場合に行われます。オフライン復旧には、スタンドアロン デバイスと SCSI ライブラリ デバイスだけを使用できます。Cell Manager の復旧は、常にオフラインで行われます。

オンライン REDO ログ

(Oracle 固有の用語)

まだアーカイブされていないが、インスタンスでデータベース アクティビティを記録するために利用できるか、または満杯になっており、アーカイブまたは再使用されるまで待機している REDO ログ。

アーカイブ REDO ログも参照。

オンライン バックアップ

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

- 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働を再開できます。

場合によっては、データベースを整合性を保って復元するために、トランザクション ログもバックアップする必要があります。

ゼロ ダウンタイム バックアップ (ZDB) およびオフライン バックアップも参照。

階層ストレージ管理 (HSM)

使用頻度の低いデータを低コストの光磁気プラッタに移動することで、コストの高いハード ディスク記憶域を有効利用するための仕組み。移動したデータが必要になった場合は、ハード ディスク記憶域に自動的に戻されます。これにより、ハード ディスクからの高速読み取りと光磁気プラッタの低コスト性のバランスが維持されます。

拡張可能 ストレージ エンジン (ESE)

(Microsoft Exchange Server 固有の用語)

Microsoft Exchange Server で情報交換用の記憶システムとして使用されているデータベース テクノロジー。

拡張増分バックアップ

従来の増分バックアップでは、最後のバックアップの後に変更されたファイルがバックアップされますが、変更の検出には一定の制限があります。拡張増分バックアップでは、従来の増分バックアップとは異なり、属性が変更されたファイルに加えて、名前が変更されたファイルや移動されたファイルも確実に検出され、バックアップされます。

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せん。

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 固有の用語)

SQL Server のプログラミング インタフェースの 1 つ。大容量のデータベースを高速でバックアップおよび復元できます。

仮想フルバックアップ

効率の良い合成バックアップのタイプ。コピーされる代わりに、ポインタの使用によってデータが集約されます。すべてのバックアップ (フルバックアップ、増分バックアップ、およびその結果生成される仮想フルバックアップ) を、配布ファイル メディア形式を使用する単一のファイル ライブラリに書き込む場合に実行します。

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

共有ディスク

(*Microsoft Exchange Server 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 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 Server 固有の用語*)

Informix Server の構成ファイル。

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 (Windows の場合) または <INFORMIXDIR>/etc ディレクトリ (UNIX の場合) に保存されます (<INFORMIXDIR> は Informix 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ライターと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。

差分バックアップ (delta backup)**検証**

指定したメディア上の Data Protector データが読み取り可能かどうかをチェックする機能。また、CRC (巡回冗長検査) オプションをオンにして実行したバックアップに対しては、各ブロック内の整合性もチェックできます。

合成バックアップ

合成フルバックアップを生成するバックアップソリューション。データに関しては従来のフルバックアップと同等ですが、プロダクションサーバまたはネットワークに負荷がかかりません。合成フルバックアップは、前回のフルバックアップと任意の数の増分バックアップから作成されます。

合成フルバックアップ

バックアップオブジェクトの復元チェーンを新しい合成フルバージョンのオブジェクトにマージする、オブジェクト集約処理の結果として生成されます。合成フルバックアップは、復元速度の点では、従来のフルバックアップと同等です。

コピーセット

(HP StorageWorks EVA 固有の用語)

ローカル EVA 上にあるソース ボリュームとリモート EVA 上にあるその複製とのペア。

ソース ボリューム、複製、および CA+BC EVA も参照。

コマンド行インタフェース (CLI)

CLI には、DOS コマンドや UNIX コマンドと同じようにシェル スクリプト内で使用できるコマンドが用意されています。これらを使用して、Data Protector の構成、バックアップ、復元、管理の各タスクを実行することができます。

再解析ポイント

(Windows 固有の用語)

任意のディレクトリまたはファイルに関連付けることができるシステム制御属性。再解析属性の値は、ユーザー制御データをとることができます。このデータの形式は、データを保存したアプリケーションによって認識され、データの解釈用にインストールされており、該当ファイルを処理するファイルシステムフィルタによっても認識されます。ファイルシステムは、再解析ポイント付きのファイルを検出すると、そのデータ形式に関連付けられているファイルシステムフィルタを検索します。

サイト複製サービス

(Microsoft Exchange Server 固有の用語)

Exchange Server 5.5 ディレクトリ サービスをエミュレートすることで 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 (differential 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)

前回のフルバックアップより後の変更をバックアップする増分バックアップ。このタイプのバックアップを実行するには、**Incr1** バックアップタイプを指定します。

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 (sybssystemprocs)
- 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。

自動ストレージ管理

(*Oracle 固有の用語*)

自動ストレージ管理は、**Oracle 10g** によって統合された、**Oracle** データベース ファイルを管理するファイルシステムおよびボリュームのマネージャ機能です。データ管理およびディスク管理の複雑さを軽減し、パフォーマンスを最適化するストライピング機能およびミラー機能を提供します。

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、定期的を上書きされます。循環ログにより、ディスク記憶領域の消費が低減できます。

障害復旧

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

初期化

フォーマットを参照。

所有権

バックアップの所有権は、どのユーザーがバックアップからデータを復元できるかを決定します。あるユーザーが対話型バックアップを開始すると、そのユーザーはセッション オーナーになります。ユーザーが既存のバックアップ仕様を修正せずにそのまま起動した場合、そのバックアップ セッションは対話型とみなされません。この場合、バックアップ仕様内でバックアップ オーナーが指定されていれば、その指定が継承されます。バックアップ仕様内でバックアップ オーナーが指定されていない場合は、バックアップを開始したユーザーがセッション オーナーになります。スケジューリングされたバックアップの場合、UNIX 用 Cell Manager では root.sys@<Cell Manager> がデフォルトのセッション オーナーとなり、Windows 用 Cell Manager では、Cell Manager のインストール時に指定されたユーザーがデフォルトのセッション オーナーとなります。所有権は変更可能なので、特定のユーザーをセッション オーナーにすることができます。

スイッチオーバー

フェイルオーバーを参照。

スキャンング

デバイス内のメディアを識別する機能。これにより、MMDB を、選択した位置 (たとえば、ライブラリ内のスロット) に実際に存在するメディアと同期させることができます。デバイスに含まれる実際のメディアをスキャンしてチェックすると、第三者が Data Protector を使用せずにメディアを操作 (挿入または取り出しなど) していないかどうかなどを確認できます。

スキャン

デバイス内のメディアを識別する機能。これにより、MMDB を、選択した位置 (たとえば、ライブラリ内のスロット) に実際に存在するメディアと同期させることができます。

スケジューラ

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

スタッカー

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

スタンドアロン ファイル デバイス

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

ストレージ グループ

(Microsoft Exchange Server 固有の用語)

同じトランザクション ログ ファイルを共有する複数のデータベース (ストア) のコレクション。Exchange では、各ストレージ グループを個別のサーバ プロセスで管理します。

ストレージ ボリューム

(ZDB 固有の用語)

ストレージ ボリュームは、オペレーティングシステムまたはボリューム管理システム、ファイル システム、または他のオブジェクトが存在可能なその他のエンティティに提供可能なオブジェクトを表します(たとえば仮想化技法)。ボリューム管理システム、ファイルシステムはこの記憶域に構築されます。これらは通常、ディスク アレイなどの記憶システム内に作成または存在します。

スナップショット

(HP StorageWorks VA および HP StorageWorks EVA 固有の用語)

スナップショット作成技法を使用して作成された複製の形式。使用するアレイ/技法に応じて、特徴の異なるさまざまな種類のスナップショットが使用できます。スナップショットで作成された複製は動的なもので、スナップショットの種類や作成時間によって、ソース ボリュームの内容に依存する仮想コピーか、独立した正確な複製(クローン)かのいずれかになります。

複製および**スナップショット作成**も参照。

スナップショット作成

(HP StorageWorks VA および HP StorageWorks EVA 固有の用語)

ソース ボリュームのコピー(ストレージ仮想化技法を使用)を作成する複製技法。複製はある一時点で作成されたものとみなされ、事前構成することなく、即座に使用できます。ただし、通常は複製作成後もコピープロセスはバックグラウンドで継続されます。

スナップショットも参照。

スナップショット バックアップ

(HP StorageWorks VA および HP StorageWorks EVA 固有の用語)

テープへの ZDB、**ディスクへの ZDB**、および**ディスク/テープへの ZDB**を参照。

スパース ファイル

ブロックが空の部分を含むファイル。一部のデータにゼロが含まれているマトリックス、イメージアプリケーションで作成したファイル、高速データベースなどの場合にスパースファイルが生じます。スパースファイルの処理を復元中に有効にしておかないと、スパースファイルを復元できなくなる可能性があります。

スプリット ミラー

(EMC Symmetrix および HP StorageWorks Disk Array XP 固有の用語)

スプリット ミラー技法を使用して作成された複製。複製により、ソース ボリュームの内容について独立した正確な複製(クローン)が作成されます。

複製および**スプリット ミラー バックアップ**も参照。

スプリット ミラーの作成

(EMC Symmetrix および HP StorageWorks Disk Array XP 固有の用語)

事前構成したターゲット ボリュームのセット(ミラー)を、ソース ボリュームの内容の複製が必要になるまでソース ボリュームのセットと同期化し続ける複製技法。その後、同期を停止(ミラーを分割)すると、分割時点でのソース ボリュームのスプリット ミラー複製はターゲット ボリュームに残ります。

スプリット ミラーも参照。

スプリット ミラー バックアップ

(EMC Symmetrix 固有の用語)

テープへの ZDBを参照。

スプリット ミラー バックアップ

(HP StorageWorks Disk Array XP 固有の用語)

テープへの ZDB、**ディスクへの ZDB**、および**ディスク/テープへの ZDB**を参照。

用語集

スプリット ミラー復元

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 固有の用語)

単一のプロセスにのみ所属する実行可能エンティティ。プログラム カウンタ、ユーザー モード スタック、カーネル モード スタック、および 1 式のレジスタ値からなります。同じプロセス内で複数のスレッドを同時に実行できます。

スロット

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

制御ファイル

(Oracle および SAP R/3 固有の用語)

データベースの物理構造を指定するエントリが格納される Oracle データ ファイル。復旧に使用するデータベース情報の整合性を確保できます。

セカンダリ ボリューム (S-VOL)

(HP StorageWorks Disk Array XP 固有の用語)

セカンダリ ボリューム (S-VOL) は、他の

LDEV (P-VOL) のセカンダリ CA ミラーまたは BC ミラーとしての役割を果たす XP LDEV。CA の場合、S-VOL を MetroCluster 構成内のフェイルオーバー デバイスとして使うことができます。S-VOL には、P-VOL によって使用されるアドレスとは異なる、個別の SCSI アドレスが割り当てられます。**プライマリ ボリューム (P-VOL) も参照。**

セッション

バックアップ セッション、メディア管理セッションおよび復元セッションを参照。

セッション ID

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

セッション 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、omnstat、および omniabort のオプション指定に使用されます。

セル

1 台の Cell Manager に管理されているシステムの集合。セルには、一般に、同じ LAN に接続されたサイトや組織エンティティ上のシステムが含まれます。バックアップおよび復元のポリシーとタスクは、1 か所から集中管理できます。

ゼロ ダウンタイム バックアップ (ZDB)

ディスク アレイにより実現したデータ複製技術を用いて、アプリケーション システムのバックアップ処理の影響を最小限に抑えるバックアップ アプローチ。バックアップされるデータの複製がまず作成されます。その後

のすべてのバックアップ処理は、元のデータではなく複製データを使って実行し、アプリケーション システムは通常の処理に復帰します。

ディスクへの ZDB、テープへの ZDB、ディスク/テープへの ZDB、およびインスタントリカバリも参照。

増分 1 メールボックス バックアップ

増分 1 メールボックス バックアップでは、前回のフル バックアップ以降にメールボックス に対して行われた変更をすべてバックアップ します。

増分 ZDB

保護されている最後のフル バックアップまたは増分バックアップより後に変更された部分のみをバックアップする、ファイルシステムのテープへの ZDB セッションまたはディスク + テープへの ZDB セッション。

フル ZDB も参照。

増分バックアップ

前回のバックアップより後に変更があったファイルのみを選択するバックアップ。増分バックアップには、複数のレベルがあり、復元チェーンの長さを詳細に制御できます。

バックアップの種類も参照。

増分バックアップ

(*Microsoft Exchange Server 固有の用語*)

前回のフル バックアップまたは増分バックアップ以降の変更だけをバックアップする Microsoft Exchange Server データのバックアップ。増分バックアップでは、バックアップ対象はトランザクション ログだけです。

バックアップの種類も参照。

増分メールボックス バックアップ

増分メールボックス バックアップでは、前回の各種バックアップ以降にメールボックス に対して行われた変更をすべてバックアップ します。

ソース デバイス (R1)

(*EMC Symmetrix 固有の用語*)

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

ターゲット デバイス (R2) も参照。

ソース ボリューム

(*ZDB 固有の用語*)

複製され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

用語集

ターゲット ボリューム

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。

チャンネル

(Oracle 固有の用語)

Oracle Recovery Manager のリソース割り当て単位。チャンネルが割り当てられるごとに、新しい Oracle プロセスが開始され、そのプロセスを通じてバックアップ、復元、および復

旧が行われます。割り当てられるチャンネルの種類によって、使用するメディアの種類が決まります。

- DISK タイプ
- SBT_TAPE タイプ

Oracle が Data Protector と統合されており、指定されたチャンネルの種類が SBT_TAPE タイプの場合は、上記のサーバプロセスが Data Protector に対してバックアップの読み取りとデータ ファイルの書き込みを試行します。

ディスク イメージ (raw ディスク) のバックアップ

ディスク イメージのバックアップでは、ファイルがビットマップ イメージとしてバックアップされるので、高速バックアップが実現します。ディスク イメージ (raw ディスク) バックアップでは、ディスク上のファイルおよびディレクトリの構造はバックアップされませんが、ディスク イメージ構造がバイト レベルで保存されます。ディスク イメージ バックアップは、ディスク全体か、またはディスク上の特定のセクションを対象にして実行できます。

ディスク クォータ

コンピュータ システム上のすべてのユーザーまたはユーザーのサブセットに対してディスク スペースの消費を管理するためのコンセプト。このコンセプトは、いくつかのオペレーティング システム プラットフォームで採用されています。

ディスク グループ

(Veritas Volume Manager 固有の用語)

VxVM システムにおけるデータ ストレージの基本単位。ディスク グループは、1 つまたは複数の物理ボリュームから作成できます。同じシステム上に複数のディスク グループを置くことができます。

ディスク検出

ディスク検出では、クライアントのバックアップ中にディスクを検出します。このとき **Data Protector** が探索 (検出) するのは、クライアント上に存在するディスクで、バックアップの構成時にシステム上に存在しなかったディスクも検出の対象に含まれます。検出されたディスクがバックアップされます。この機能は、構成が頻繁に変更される動的な環境の場合に特に役立ちます。ディスクが展開されると、それぞれのディスクがマスタークライアント オブジェクトのオプションをすべて継承します。実行前コマンドと実行後コマンドは、1 回しか指定されていなくても、オブジェクトごとに繰り返し起動されることとなります。

ディスク検出によるクライアントのバックアップ

クライアントにマウントされているすべてのファイルシステムのバックアップ。バックアップの開始時に、**Data Protector** がクライアント上のディスクを自動検出します。ディスク検出によるクライアント バックアップでは、バックアップ構成が単純化され、ディスクのマウント / アンマウントが頻繁に行われるシステムに対するバックアップ効率が向上されます。

ディスク ステージング

複数のフェーズでデータをバックアップするプロセス。これにより、バックアップと復元のパフォーマンスが改善し、バックアップデータの保存コストが低減し、復元に対するデータの可用性とアクセス性が向上します。バックアップ ステージは、最初に 1 種類のメディア (たとえば、ディスク) にデータをバックアップし、その後データを異なる種類のメディア (たとえば、テープ) にコピーすることから構成されます。

ディスク / テープへの ZDB

(ZDB 固有の用語)

ゼロ ダウンタイム バックアップの 1 つの形式。ディスクへの ZDB と同様に、作成された複製が特定の時点でのソース ボリュームのバックアップとしてディスク アレイに保持されます。ただし、テープへの ZDB と同様、複製データはバックアップ メディアにもストリーミングされます。このバックアップ方法を使用した場合、同じセッションでバックアップしたデータは、インスタント リカバリ、**Data Protector** 標準のテープからの復元を使用して復元できます。スプリット ミラーアレイではスプリット ミラー復元が可能です。

ゼロ ダウンタイム バックアップ (ZDB)、ディスクへの ZDB、テープへの ZDB、インスタント リカバリ、複製、および複製セット ローテーションも参照。

ディスクへの ZDB

(ZDB 固有の用語)

ゼロ ダウンタイム バックアップの 1 つの形式。作成された複製が、特定の時点でのソース ボリュームのバックアップとしてディスク アレイに保持されます。同じバックアップ仕様を使って別の時点で作成された複数の複製を、複製セットに保持することができます。テープに ZDB した複製はインスタント リカバリ プロセスで復元できます。

ゼロ ダウンタイム バックアップ (ZDB)、テープへの ZDB、ディスク / テープへの ZDB、インスタント リカバリ、および複製セット ローテーションも参照。

ディレクトリ接合

(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。

用語集

データ ストリーム

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。

データベースの差分バックアップ

前回のフル データベース バックアップ以降にデータベースに対して加えられた変更だけを記録するデータベース バックアップ。

データベースの並列処理 (数)

十分な台数のデバイスが利用可能で、並列バックアップを実行できる場合には、複数のデータベースが同時にバックアップされます。

データベース ライブラリ

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

データ保護

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

カタログ保護も参照。

テープへの 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

トランザクション バックアップ

ます。トランザクション バックアップを適用することで、データベースを問題発生以前の特定の時点の状態に復旧することができます。

トランザクション バックアップ

(Sybase および SQL 固有の用語)

トランザクション ログをバックアップすること。トランザクション ログには、前回のフルバックアップまたはトランザクション バックアップ以降に発生した変更が記録されます。

トランザクション ログ

(Data Protector 固有の用語)

IDB に対する変更を記録します。IDB 復旧に必要なトランザクション ログ ファイル (前回の IDB バックアップ以降に作成されたトランザクション ログ) が失われることがないように、トランザクション ログのアーカイブを有効化しておく必要があります。

トランザクション ログ テーブル

(Sybase 固有の用語)

データベースに対するすべての変更が自動的に記録されるシステム テーブル。

トランザクション ログ バックアップ

トランザクション ログ バックアップは、一般に、データベースのバックアップよりも必要とするリソースが少ないため、データベースのバックアップよりもより高い頻度で実行できます。トランザクション ログ バックアップを用いることにより、データベースを特定の時点の状態に復元できます。

トランザクション ログ ファイル

データベースを変更するトランザクションを記録するファイル。データベースが破損した場合にフォールト トレランスを提供します。

トランスポータブル スナップショット

(MS VSS 固有の用語)

アプリケーション システム上に作成されるシャドウ コピー。このシャドウ コピーは、バックアップを実行するバックアップ システムに提供できます。

Microsoft Volume Shadow Copy Service (VSS) も参照。

ハートビート

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

ハード リカバリ

(Microsoft Exchange Server 固有の用語)

トランザクション ログ ファイルを使用し、データベース エンジンによる復元後に実行される Microsoft Exchange Server のデータベース復旧。

配布ファイル メディア形式

ファイル ライブラリで提供されるメディア フォーマット。仮想フルバックアップと呼ばれる、容量効率の良い合成バックアップをサポートしています。仮想フルバックアップではこのフォーマットの使用が前提条件となります。

仮想フル バックアップ も参照。

バックアップ API

Oracle のバックアップ / 復元ユーティリティとバックアップ / 復元メディア管理層の間にある Oracle インタフェース。このインタフェースによってルーチンのセットが定義され、バックアップ メディアのデータの読み書き、バックアップ ファイルの作成や検索、削除が行えるようになります。

バックアップ ID

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

バックアップ オーナー

IDB の各バックアップ オブジェクトにはオーナーが定義されています。デフォルトのオーナーは、バックアップ セッションを開始したユーザーです。

バックアップ オブジェクト

1 つのディスク ボリューム (論理ディスクまたはマウント ポイント) からバックアップされた項目すべてを含むバックアップ単位。バックアップ項目は、任意の数のファイル、ディレクトリ、ディスク全体またはマウント ポイントの場合が考えられます。また、バックアップ オブジェクトはデータベース 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、ZDB ディスクアレイバックアップ デバイスに接続され、複製内のデータのバックアップを実行します。

アプリケーション システム、ターゲット ボリュームおよび複製も参照。

バックアップ仕様

バックアップ対象オブジェクトを、使用するデバイスまたはドライブのセット、仕様内のすべてのオブジェクトに対するバックアップ オプション、バックアップを行いたい日時とともに指定したリスト。オブジェクトとなるのは、ディスクやボリューム全体、またはその一部、たとえばファイル、ディレクトリ、Windows レジストリなどです。インクルード リストおよびエクスクルード リストを使用し、ファイルを選択することもできます。

バックアップ世代

1 つのフル バックアップとそれに続く増分 バックアップを意味します。次のフル バックアップが行われると、世代が新しくなります。

バックアップ セッション

データのコピーを記憶メディア上に作成するプロセス。バックアップ仕様に処理内容を指定することも、対話式に操作を行うこともできます (対話式セッション)。1 つのバックアップ仕様の中で複数のクライアントが構成されている場合、すべてのクライアントが同じバックアップの種類 (フルまたは増分) を使って、1 回のバックアップ セッションで同時にバックアップされます。バックアップ セッションの結果、1 式のメディアにバック

バックアップ セット

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

復元チェーンを参照。

バックアップ デバイス

記憶メディアに対するデータの読み書きが可能な物理デバイスを **Data Protector** で使用できるように構成したもの。たとえば、スタンドアロン DDS/DAT ドライブやライブラリなどをバックアップ デバイスとして使用できます。

バックアップの種類

増分バックアップ、**差分バックアップ (differential backup)**、**トランザクションバックアップ**、**フルバックアップ**および**差分バックアップ (delta backup)**を参照。

バックアップ ビュー

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

パッケージ

(MC/ServiceGuard および Veritas Cluster 固有の用語)

特定のクラスタ対応アプリケーションを実行するために必要なリソース (ボリューム グループ、アプリケーション サービス、IP 名および IP アドレスなど) の集合。

パブリック フォルダ ストア

(Microsoft Exchange Server 固有の用語)

インフォメーション ストアのうち、パブリック フォルダ内に情報を維持する部分。パブリック フォルダ ストアは、バイナリ リッチ テキスト .edb ファイルと、ストリーミング ネイティブ インターネット コンテンツを格納する .stm ファイルから構成されます。

パブリック/プライベート バックアップ データ

バックアップを構成する際は、バックアップ データをパブリックまたはプライベートのいずれにするかを選択できます。

- パブリック データ - すべての **Data Protector** ユーザーに対してアクセスと復元が許可されます。

- プライベート データ バックアップの所有者および管理者に対してのみ表示と復元が許可されます。

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。

ファイルシステム

ハード ディスク上に一定の形式で保存されたファイルの集まり。ファイルシステムは、ファイル属性とファイルの内容がバックアップ メディアに保存されるようにバックアップされます。

ファイル ジュークボックス デバイス

ファイル メディアを格納するために使用する、複数のスロットからなるディスク上に存在するデバイス。

ファイル デポ

バックアップからファイル ライブラリ デバイスまでのデータを含むファイル。

ファイル バージョン

フルバックアップや増分バックアップでは、ファイルが変更されている場合、同じファイルが複数回バックアップされます。バックアップのロギング レベルとして [すべてログに記録] を選択している場合は、ファイル名自体に対応する 1 つのエントリとファイルの各バージョンに対応する個別のエントリが IDB 内に維持されます。

ファイル複製サービス (FRS)

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

ファイル ライブラリ デバイス

複数のメディアからなるライブラリをエミュレートするディスク上に存在するデバイス。ファイル デポと呼ばれる複数のファイルが格納されます。

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

フェイルオーバー

象をより正確に絞り込むことができます。複数単語の検索に演算子を指定しなければ、AND を指定したものとみなされます。たとえば、「consistency checkmanual disaster recovery」という検索条件は、「consistencymanual AND checkdisaster AND recovery」と同じ結果になります。

フェイルオーバー

あるクラスタ ノードから別のクラスタ 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。フェイルオーバーは、主に、プライマリ ノードのソフトウェア/ハードウェア障害発生時や保守時に発生します。

フェイルオーバー

(HP StorageWorks EVA 固有の用語)

CA+BC EVA 構成におけるソースとあて先の役割を逆にする操作。

CA+BC EVA も参照。

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。

復元チェーン

バックアップ オブジェクトをある時点まで復元するのに必要なすべてのバックアップ。復元チェーンは、オブジェクトのフル バックアップと任意の数の関連する増分バックアップで構成されます。

複製

(ZDB 固有の用語)

ユーザー指定のバックアップ オブジェクトを含む、特定の時点におけるソース ボリュームのデータのイメージ。イメージは、作成するハードウェア/ソフトウェアによって、物理ディスク レベルでの記憶ブロックの独立した正確な複製 (クローン) になる (スプリットミラーなど) 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。

フラッシュ リカバリ領域

(Oracle 固有の用語)

フラッシュ リカバリ領域は、Oracle 10g で管理されるディレクトリ、ファイル システム、または自動ストレージ管理のディスク グループです。バックアップと復旧に関するファイル（リカバリ ファイル）の中央格納領域として機能します。

リカバリ ファイルも参照。

フリー プール

フリー プールは、メディア プール内のすべてのメディアが使用中になっている場合にメディアのソースとして補助的に使用できるプールです。ただし、メディア プールでフリー プールを使用するには、明示的にフリー プールを使用するように構成する必要があります。

フル ZDB

以前に行ったバックアップに変更がない場合でも、選択したすべてのオブジェクトがテープにストリーミングされる、テープまたはディスク + テープへの ZDB セッション。

増分 ZDB も参照。

フル データベース バックアップ

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

フル バックアップ

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

バックアップの種類も参照。

フル メールボックス バックアップ

フル メールボックス バックアップでは、メールボックス全体の内容をバックアップします。

分散ファイルシステム (DFS)

複数のファイル共有を単一の名前空間に接続するサービス。対象となるファイル共有は、同じコンピュータに置かれていても、異なるコンピュータに置かれていてもかまいません。DFS は、リソースの保存場所の違いに関係なくクライアントがリソースにアクセスできるようにします。

ペア ステータス

(HP StorageWorks Disk Array XP 固有の用語)

ミラー化されたディスクのペアは、そのペア上で実行されるアクションによって、さまざまなステータス値を持ちます。最も重要なステータス値は以下の 3 つです。

- コピー - ミラー化されたペアは、現在再同期中。データは一方のディスクからもう一方のディスクに転送されます。2 つのディスクのデータは同じではありません。
- ペア - ミラー化されたペアは、完全に同期されており、両方のディスク (プライマリボリュームとミラー ボリューム) は全く同じデータを持ちます。
- 中断 - ミラー化されたディスク間のリンクは中断されています。両方のディスクが別々にアクセスされ、更新されています。ただし、ミラー関係はまだ保持されており、このペアは、ディスク全体を転送することなく、再同期することができます。

並列処理 (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働中の Data Protector クライアント。

ホスト バックアップ

ディスク検出によるクライアント バックアップを参照。

ボリューム グループ

LVM システムにおけるデータ ストレージ単位。ボリューム グループは、1 つまたは複数の物理ボリュームから作成できます。同じシステム上に複数のボリューム グループを置くことができます。

ボリューム マウントポイント

(Windows 固有の用語)

ボリューム上の空のディレクトリを他のボリュームのマウントに使用できるように構成したもの。ボリューム マウント ポイントは、ターゲット ボリュームへのゲートウェイとして機能します。ボリュームがマウントされていれば、ユーザーやアプリケーションがそのボリューム上のデータをフル (マージ) ファイルシステム パスで参照できます (両方のボリュームが一体化されている場合) 。

マージ

復元中のファイル名競合を解決するモードの 1 つ。復元するファイルと同じ名前のファイルが復元先に存在する場合、変更日時の新しい方が維持されます。既存のファイルと名前が重複しないファイルは、常に復元されます。上書きも参照。

マウント ポイント

ディレクトリ構造内において、ディスクまたは論理ボリュームにアクセスするためのアクセスポイント (/opt や d: など)。UNIX では、bdf コマンドまたは df コマンドを使ってマウント ポイントを表示できます。

マウント要求

マウント要求時には、デバイスにメディアを挿入するように促す画面が表示されます。必要なメディアを挿入して確認することでマウント要求に応答すると、セッションが続行されます。

マジック パケット

Wake ONLAN を参照。

マルチドライブ サーバ

単一システム上で Media Agent を無制限に使用できるライセンス。このライセンスは、Cell Manager の IP アドレスにバインドされており、新しいバージョンでは廃止されました。

ミラー

(EMC Symmetrix および HP StorageWorks Disk Array XP 固有の用語)

ターゲット ボリュームを参照。

ミラー ローテーション

(HP StorageWorks Disk Array XP 固有の用語)

複製セット ローテーションを参照。

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

オペレータの不在なしで、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 固有の用語)

インフォメーション ストアのうち、ユーザーメールボックス内の情報を維持する部分。メールボックスストアは、バイナリ データを格納するリッチテキスト .edb ファイルと、ストリーミング ネイティブ インターネット コンテンツを格納する .stm ファイルからなります。

メディア ID

Data Protector がメディアに割り当てる一意な識別子。

メディア管理セッション

初期化、内容のスキャン、メディア上のデータの確認、メディアのコピーなどのアクションをメディアに対して実行するセッション。

メディア集中管理データベース (CMMDB)

CMMDB を参照。

メディア状態要素

使用回数のしきい値と上書きのしきい値。メディアの状態の判定基準となります。

メディア セット

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

メディアの位置

メディアのインポート

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ク

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。ボールティンク手順は、会社のバックアップ戦略やデータ保護/信頼性ポリシーに依存します。

メディアの割り当て方針

メディアをバックアップに使用する順序を決定します。[Strict]メディア割り当てポリシーでは、特定のメディアに限定されます。[Loose]ポリシーでは、任意の適切なメディアを使用できます。[フォーマットされていないメディアを先に割り当てる]ポリシーでは、ライブラリ内に利用可能な非保護メディアがある場合でも、不明なメディアが優先されます。

メディア 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。

元のシステム

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

ユーザー アカウント

Data Protectorを使用するには、Data Protectorのユーザーアカウントが必要です。Data Protectorのユーザーアカウントは、Data Protectorやバックアップされたデータに対する無断アクセスを制限します。Data Protector管理者がこのアカウントを作成するときには、ユーザーログオン名、ユーザーの

ログオン元として有効なシステム、および **Data Protector** ユーザー グループのメンバーシップを指定します。ユーザーが **Data Protector** のユーザー インタフェースを起動するか、または特定のタスクを実行するときには、このアカウントが必ずチェックされます。

ユーザー グループ

各 **Data Protector** ユーザーは、ユーザー グループのメンバーです。各ユーザー グループには 1 式のユーザー権限があり、それらの権限がユーザー グループ内のすべてのユーザーに付与されます。ユーザー権限を関連付けるユーザー グループの数は、必要に応じて定義できます。**Data Protector** には、**admin**、**operator**、**user** の 3 つのデフォルト ユーザーグループがあります。

ユーザー権限

特定の **Data Protector** タスクの実行に必要なパーミッションをユーザー権限またはアクセス権限と呼びます。主なユーザー権限には、バックアップの構成、バックアップセッションの開始、復元セッションの開始などがあります。ユーザーには、そのユーザーの所属先ユーザーグループに関連付けられているアクセス権限が割り当てられます。

ユーザー ディスク割り当て

NTFS のクォータ管理サポートにより、追跡システムが強化されており、共有ストレージボリュームのディスクスペースの使用量を制御できます。**Data Protector** では、システム全体とすべての構成済みユーザーを対象にユーザー ディスク クォータを同時にバックアップします。

ユーザー プロファイル

(Windows 固有の用語)

ユーザー別に維持される構成情報。この情報には、デスクトップ設定、画面表示色、ネッ

トワーク接続などが含まれます。ユーザーがログオンすると、そのユーザーのプロファイルがロードされ、**Windows** 環境がそれに応じて設定されます。

ライセンス集中管理

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

ライター

(MS VSS 固有の用語)

オリジナル ボリューム上のデータの変更を開始するプロセス。主に、永続的なデータをボリューム上に書き込むアプリケーションまたはシステム サービスがライターとなります。ライターは、シャドウ コピーの同期化プロセスにも参加し、データの整合性を保証します。

ライブラリ

オートチェンジャー、ジュークボックス、オートローダ、またはエクステンジャーとも呼ばれます。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、

リカバリ カタログ データベース

Recovery Manager が Oracle データベースのバックアップ、復元、および復旧を管理するために使用されます。リカバリ カタログには、以下の情報が含まれます。

- Oracle ターゲット データベースの物理スキーマ
- データ ファイルおよび archived log バックアップ セット
- データ ファイルのコピー
- アーカイブ REDO ログ
- ストアド スクリプト

リカバリ カタログ データベース

(Oracle 固有の用語)

リカバリ カタログ スキーマを格納する

Oracle データベース。リカバリ カタログはターゲット データベースに保存しないでください。

リカバリ カタログ データベースへのログイン情報

(Oracle 固有の用語)

リカバリ カタログ データベース (Oracle) へのログイン情報の形式は

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

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

リカバリ ファイル

(Oracle 固有の用語)

リカバリ ファイルは、フラッシュ リカバリ領域に置かれる Oracle 10g 固有のファイルで

す。現在の制御ファイル、オンライン REDO ログ、アーカイブ REDO ログ、フラッシュバック ログ、制御ファイル自動バックアップ、データファイル コピー、およびバックアップ ピースがこれにあたります。

フラッシュ リカバリ領域も参照。

リサイクル

メディア上のすべてのバックアップ データのデータ保護を解除して、以降のバックアップで上書きできるようにするプロセス。同じセッションに所属しているデータのうち、他のメディアに置かれているデータも保護解除されます。リサイクルを行っても、メディア上のデータ自体は変更されません。

リムーバブル記憶域の管理データベース

(Windows 固有の用語)

Windows サービスの 1 つ。リムーバブル メディア (テープやディスクなど) と記憶デバイス (ライブラリ) の管理に使用されます。リムーバブル記憶域により、複数のアプリケーションが同じメディア リソースを共有できます。

ローカル復旧とリモート復旧

リモート復旧は、SRD ファイルで指定されている Media Agent ホストがすべてアクセス可能な場合にのみ実行されます。いずれかのホストがアクセス不能になっていると、障害復旧プロセスがローカル モードにフェイルオーバーされます。これは、ターゲット システムにローカル接続しているデバイスが検索されることを意味します。デバイスが 1 台しか見つからない場合は、そのデバイスが自動的に使用されます。複数のデバイスが見つかった場合は、デバイスが選択できるプロンプトが表示され、ユーザーが選択したデバイスが復元に使用されます。

ロギング レベル

ロギングレベルは、バックアップ、オブジェクトのコピー、またはオブジェクトの集約時にファイルとディレクトリに関する情報をどの程度まで詳細に IDB に記録するかを示します。バックアップ時のロギングレベルに関係なく、データの復元は常に可能です。Data Protector には、[すべてログに記録]、[ディレクトリレベルまでログに記録]、[ファイルレベルまでログに記録]、および[ログなし]の4つのロギングレベルがあります。ロギングレベルの設定によって、IDB のサイズ増加、バックアップ速度、復元対象データのブラウズしやすさが影響を受けます。

ログイン ID

(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。

A

- ACS クライアント, 94
- ADIC ライブラリ。ADIC/GRAU ライブラリを参照。
- ADIC/GRAU ライブラリ
 - Media Agent のインストール, 93
 - Media Agent をクライアントにインストール, 96
 - クライアントの準備, 94
 - ドライブの接続, 94
- AIX クライアント
 - インストール, 85
 - バックアップ デバイスの接続, 86
- allow_hosts ファイル, 201, 203, 204
- AutoPass ユーティリティ
 - アンインストール、HP-UX の場合, 217
 - アンインストール、Solaris の場合, 221
 - アンインストール、Windows の場合, 216
 - インストール、UNIX の場合, 23, C-7
 - インストール、Windows の場合, 34
 - ライセンス, 309

C

- CD-ROM
 - インストール, C-2, C-5
 - インストール CD-ROM 一覧, C-2
- Cell Manager
 - Cell Request Server (CRS) サービス, 26, 35
 - Data Protector A.05.x からのアップグレード、HP-UX の場合, 238, 241, C-11
 - Media Management Daemon (MMD) サービス, 27
 - Raima Database Server (RDS) サービス, 27, 36
 - SSE のアップグレード, 272
 - Windows NT から Windows のより新しいバージョンへのアップグレード, 274
 - アップグレード、MC/ServiceGuard 上, 285
 - アップグレード、Microsoft Cluster Server 上, 289
 - アンインストール、HP-UX の場合, 217
 - アンインストール、Linux の場合, 223
 - アンインストール、MC/ServiceGuard の場合, 217
 - アンインストール、Solaris の場合, 221
 - アンインストール、Windows の場合, 215
 - インストール順序, 19
 - インストールの前提条件、UNIX の場合, 20

- インストールの前提条件、Windows の場合, 29
- インストールのトラブルシューティング、UNIX の場合, 27
- インストール、HP-UX, 22
- インストール、HP-UX、ネイティブ ツールの使用, B-3
- インストール、Linux の場合, 22
- インストール、Linux の場合、ネイティブ ツールの使用, B-6
- インストール、MC/ServiceGuard, 165
- インストール、Microsoft Cluster Server, 167
- インストール、Solaris の場合, 22
- インストール、Solaris の場合、ネイティブ ツールの使用, B-5
- インストール、Windows の場合, 29
- インストール、トラブルシューティング, 321
- 概念, 3
- 環境変数の設定、UNIX の場合, 27
- 機能, 11
- 構成の変更のチェック, 247
- 構成、Veritas Volume Manager、Microsoft Cluster Server, B-76
- システムの選択, 11, 12
- 自動構成されるファイル、UNIX の場合, 25
- 手動でアップグレード、UNIX の場合, 332
- 準備、NIS サーバ, B-30
- ソフトウェア コンポーネントの変更, 226
- ディレクトリ構造、UNIX の場合, 24
- トラブルシューティング, 325, 327, 331, 333, 336
- 名前の変更, B-26
- 保護の概念, 195
- Cell Manager のインストール
 - HP-UX システムの場合, 22
 - ネイティブ ツールの使用, B-3
 - Linux システムの場合, 22
 - ネイティブ ツールの使用, B-6
 - MC/ServiceGuard システム, 165
 - Microsoft Cluster Server システム, 167
 - Solaris システムの場合, 22
 - ネイティブ ツールの使用, B-5
 - Windows システム, 29
- 前提条件、UNIX の場合, 20
- 前提条件、Windows の場合, 29
- Cell Request Server (CRS) サービス, 26, 35
- cell_info ファイル, 229

CLI。コマンド行インタフェースを参照。
CRS。Cell Request Server (CRS) サービスを参照。

D

DAS クライアント, 94
Data Protector A.05.x からのアップグレード
Cell Manager、HP-UX の場合, 238, 241, C-11
Cell Manager、MC/ServiceGuard 上, 285
Cell Manager、Microsoft Cluster Server 上, 289
EVA 用統合ソフトウェア, 258
Informix 用統合ソフトウェア、UNIX の場合, 253
Informix 用統合ソフトウェア、Windows の場合, 254
Manager-of-Managers, 260
omnisv コマンド, 237
Oracle 用統合ソフトウェア, 251
SAP R/3 用統合ソフトウェア, 253
Sybase 用統合ソフトウェア、UNIX の場合, 255
Sybase 用統合ソフトウェア、Windows の場合, 257
インストール サーバ、HP-UX の場合, 237, 238
インストール サーバ、Windows の場合, 243
概要, 237
クライアント, 249
クライアント、MC/ServiceGuard の場合, 250
クライアント、Microsoft Cluster Server 上, 292
構成の変更のチェック, 247
前提条件, 237
ライセンスの移行, A-19
Data Protector Inet サービス, 36
DB2 用統合ソフトウェア、インストール, 131
debug オプション
概要, 336
deny_hosts ファイル, 204
Disk Agent
概念, 3
構成、OpenVMS, 112
DNS
omnicheck コマンド, 322

接続の確認、セル内, 322
DNS チェック ツール, B-25
DVD-ROM
インストール DVD-ROM 一覧, 8

E

EVA 用統合ソフトウェア
Data Protector A.05.x からのアップグレード, 258

G

General Media Agent
インストールのチェック、Novell NetWare, B-71
global ファイル, 247
GRAU ライブラリ。ADIC/GRAU ライブラリを参照。
GUI。グラフィカル ユーザー インタフェースを参照。

H

HP StorageWorks 330fx ライブラリ、SCSI ID の設定, B-55
HP StorageWorks DAT 24 テープドライブ、接続, B-60
HP StorageWorks DLT ライブラリ 24/48 スロット、接続, B-63
HP StorageWorks EVA 用統合ソフトウェアインストール, 149
HP StorageWorks VA 用統合ソフトウェアインストール, 143
HP StorageWorks XP 用統合ソフトウェアインストール, 136
HP Surestore 12000e オートローダー、接続, B-61
HPDEVBRA.NLM ファイル, B-74
HPUMA.NLM ファイル, B-74
HP-UX 11.23 へのアップグレード, 276
HP-UX インストール サーバ
インストール、ネイティブ ツールの使用, B-8
HP-UX クライアント
インストール, 68
トラブルシューティング, 328
バックアップ デバイスの接続, 72
HP-UX 用 Cell Manager
Data Protector A.05.x からのアップグレード, 238, 241, C-11

PA-RISC から IA-64 への移行, 276
アンインストール, 217
インストール, 22
インストールの前提条件, 20
インストールのトラブルシューティング, 27
インストール、ネイティブ ツールの使用、
B-3
環境変数の設定, 27
自動構成されるファイル, 25
ディレクトリ構造, 24
トラブルシューティング, 27, 331, 333

I

IDB

アップグレードのトラブルシューティング、
331

サイズ増加, 11

IDB ファイル名変換
概念, 262

inet.conf ファイル, B-30

inet.log ファイル, 201, 203, 205, 288

Inet サービス。Data Protector Inet サービス
を参照。

Informix 用統合ソフトウェア

Data Protector A.05.x からのアップグレード、
UNIX の場合, 253

Data Protector からのアップグレード、
Windows の場合, 254

Informix 用統合ソフトウェア、インストール
, 128

infs コマンド, B-42

installation_servers ファイル, 40

ioscan コマンド, B-39, B-42, B-46

IP アドレス、TCP/IP, B-19

L

license-to-use。ライセンスを参照。

Linux インストール サーバ
インストール、ネイティブ ツールの使用、
B-12

Linux クライアント

インストール, 79

カーネルの構成, 82

バックアップ デバイスの接続, 83

リモート インストールのトラブルシュー
ティング, 81

Linux 用 Cell Manager

アンインストール, 223

インストール, 22

インストールの前提条件, 20

インストールのトラブルシューティング, 27

インストール、ネイティブ ツールの使用、
B-6

環境変数の設定, 27

自動構成されるファイル, 26

トラブルシューティング, 27

Lotus 用統合ソフトウェア、インストール、
132

LTU。ライセンスを参照。

M

Manager-of-Managers

Data Protector A.05.x からのアップグレー
ド, 260

アップグレードの概要, 235

MC/ServiceGuard

Cell Manager のアップグレード, 285

Cell Manager のアンインストール, 217

Cell Manager のインストール, 165

Data Protector A.05.x からのクライアント
のアップグレード, 250

inet.log ファイルに大量のログが記録さ
れる場合, 205

インストール サーバのアンインストール、
217

インポート, 190

クライアントのインストール, 166

Media Agent

ADIC/GRAU ライブラリ用、インストール、
96

StorageTek ACS ライブラリ用、インストー
ル, 101

概念, 3

構成、Novell NetWare, 107

構成、OpenVMS, 113

タイプ, 3

Media Management Daemon (MMD) サービ
ス, 27

Microsoft Cluster Server

Cell Manager と Veritas Volume Manager
の構成, B-76

Cell Manager のアップグレード, 289

Cell Manager のインストール, 167

インポート, 188

エクスポート, 194

クライアントのアップグレード, 292

クライアントのインストール, 175
クライアントの構成、Veritas Volume
Manager, B-76
Microsoft Exchange 2000 用統合ソフトウェア
HP StorageWorks EVA ディスク アレイを備
えたシステムへのインストール, 155
HP StorageWorks VA ディスク アレイを備
えたシステムへのインストール, 148
HP StorageWorks XP ディスク アレイを備
えたシステムへのインストール, 142
Microsoft Exchange 用統合ソフトウェア
インストール, 127
Microsoft Installer, 30, 234, 289, 325
Microsoft SQL 用統合ソフトウェア
HP StorageWorks EVA ディスク アレイを備
えたシステムへのインストール, 155
HP StorageWorks VA ディスク アレイを備
えたシステムへのインストール, 149
HP StorageWorks XP ディスク アレイを備
えたシステムへのインストール, 142
インストール, 128
Microsoft Volume Shadow Copy 用統合ソフ
トウェア、インストール, 132
Microsoft ターミナルサービスクライアント,
29
MMD。Media Management Daemon (MMD)
サービスを参照。
MPE/iX クライアントのインストール, 115
MSI。Microsoft Installer を参照。

N

NDMP Media Agent、概念, 3
NDMP クライアント、インポート, 186
NDMP 用統合ソフトウェア、インストール,
131
netstat コマンド, B-28
NIS サーバの準備, B-30
NNM 用統合ソフトウェア、インストール,
131
Novell NetWare Cluster Services
インポート, 190
クライアントのインストール, 179
制限、フェイルオーバー, 179
Novell NetWare クライアント
General Media Agent のインストールの
チェック, B-71
HPDEVBRA.NLM ファイル, B-74

HPUMA.NLM ファイル, B-74
Media Agent の構成, 107
インストール, 102
ネットワークトラフィックの最小化, 106
nsswitch.conf ファイル, B-30

O

omnicc command, 305
omnicheck コマンド, 212, 322
omniinet プロセス。Data Protector Inet
サービスを参照。
omni_info ファイル, 229
omniirc ファイル, 248
omnisetup.sh, 222, 223
omnisetup.sh コマンド
アップグレード, 238, 241, C-11
インストール, 120, 158
omnisv コマンド, 237
OpenVMS クライアント
Disk Agent の構成, 112
Media Agent の構成, 113
アンインストール, 215
インポート, 186
Oracle 用統合ソフトウェア
Data Protector A.05.x からのアップグレー
ド, 251
EMC Symmetrix ディスク アレイを備えた
システムへのインストール, 133
HP StorageWorks EVA ディスク アレイを備
えたシステムへのインストール, 150
HP StorageWorks VA ディスク アレイを備
えたシステムへのインストール, 144
HP StorageWorks XP ディスク アレイを備
えたシステムへのインストール, 137
アンインストール固有の問題, 228
インストール, 129

P

pkgadd ユーティリティ, 221
pkgrm ユーティリティ, 220, 221

R

Raima Database Server (RDS) サービス, 27,
36
RDS。Raima Database Server (RDS) サー
ビスを参照。
rpm ユーティリティ, 222, 223

S

SAP DB 用統合ソフトウェア、インストール、
129

SAP R/3 用統合ソフトウェア

Data Protector A.05.x からのアップグレード、
253

EMC Symmetrix ディスク アレイを備えた
システムへのインストール、134

HP StorageWorks EVA ディスク アレイを備
えたシステムへのインストール、152

HP StorageWorks VA ディスク アレイを備
えたシステムへのインストール、145

HP StorageWorks XP ディスク アレイを備
えたシステムへのインストール、139

インストール、129

SCO クライアント

インストール、91

バックアップ デバイスの接続、92

SCSI アドレス。SCSI インタフェースを参
照。

SCSI インタフェース

ID の設定、HP StorageWorks 330fx ライブ
ラリ、B-55

SCSI テープドライブの使用、Windows の
場合、B-32

カーネルにロボティクスドライブを追加、
HP-UX、B-40

コントローラパラメータの設定、Windows
の場合、B-45

未使用のアドレスの確認、HP-UX、B-46

未使用のアドレスの確認、Solaris の場合、
B-48

未使用のアドレスの確認、Windows の場合、
B-54

ロボティクスドライブの無効化、Windows
の場合、B-33

ロボティクスの構成、HP-UX、B-37

SCSI コントローラ。SCSI インタフェースを
参照。

SCSI テープドライブ。SCSI インタフェース
を参照。

SCSI ロボティクスドライブの無効化、
Windows の場合、B-33

SCSI ロボティクス。SCSI インタフェースを
参照。

Seagate Viper 200 LTO テープドライブ、接
続、B-68

services ファイル、B-28

Siemens Sinix クライアント

インストール、87

バックアップ デバイスの接続、87

Solaris インストール サーバ

インストール、ネイティブ ツールの使用、
B-8

Solaris クライアント

インストール、72

構成、インストール後、74

トラブルシューティング、328

バックアップ デバイスの接続、77

Solaris 用 Cell Manager

アンインストール、221

インストール、22

インストールの前提条件、20

インストールのトラブルシューティング、27

インストール、ネイティブ ツールの使用、
B-5

環境変数の設定、27

自動構成されるファイル、26

ディレクトリ構造、Linux 用 Cell Manager

ディレクトリ構造、24

トラブルシューティング、27、327、331、333

SSE。シングル・サーバ版を参照

sst.conf ファイル、B-51

st.conf ファイル、74、B-49

STK ACS。StorageTek ACS ライブラリを参
照。

StorageTek ACS ライブラリ

Media Agent のインストール、93

Media Agent をクライアントにインストー
ル、101

クライアントの準備、99

ドライブの接続、94

StorageTek ライブラリ。StorageTek ACS ラ
イブラリを参照。

swagent デーモン、329

Sybase 用統合ソフトウェア

Data Protector A.05.x からのアップグレー
ド、UNIX の場合、255

Data Protector からのアップグレード、
Windows の場合、257

Sybase 用統合ソフトウェア、インストール、
128

T

TCP/IP

IP アドレス、B-19

構成、Windows の場合、B-19
サブネット マスク、B-19
設定のチェック、Windows の場合、B-24
デフォルト ゲートウェイ、B-19
Tru64 クライアント
インストール、89
バックアップ デバイスの接続、90

V

Veritas Cluster

インポート、190
クライアントのインストール、178
制限、フェイルオーバー、178

Veritas Volume Manager

Cell Manager の構成、Microsoft Cluster Server、B-76
クライアントの構成、Microsoft Cluster Server、B-76

W

Web Reporting、インストール、163

Windows NT、Windows のより新しいバージョンへのアップグレード、274

Windows クライアント

インストール、63
トラブルシューティング、325、333
バックアップ デバイスの接続、67

Windows 用 Cell Manager

32 ビットから 64 ビットへの移行、281
アンインストール、215
インストール、29
インストールの前提条件、29
インストールのトラブルシューティング、36
トラブルシューティング、325、331

Z

ZDB 統合クライアント、124
統合ソフトウェアも参照。

あ

アクセス確認を使用可能にする
クライアントの場合、199
セルの場合、202

アクセス権限

root アカウントへの追加、Linux の場合、81

アップグレード

CLI の変更、B-80

global ファイル、247
IDB のトラブルシューティング、331
omnirc ファイル、248
omnisetup.sh コマンド、238、241、C-11
omnisv コマンド、237
SSE から Data Protector A.06.00 SSE へ、271

SSE から Data Protector A.06.00 へ、271
Windows NT から Windows のより新しいバージョンへ、274

アップグレード前の注意点、233

概要、233

構成ファイルの変更、B-77

手動、UNIX の場合、332

制限事項、233

手順、234

トラブルシューティング、UNIX の場合、331

トラブルシューティング、Windows の場合、325、331

アップグレードのトラブルシューティング

Data Protector ソフトウェア、Windows の場合、325

Data Protector バッチ、331

IDB が使用できない、331

Microsoft Installer に関する問題、325

構成ファイルが使用できない、331

アンインストール

AutoPass ユーティリティ、HP-UX の場合、217

AutoPass ユーティリティ、Solaris の場合、221

AutoPass ユーティリティ、Windows の場合、216

Cell Manager、HP-UX の場合、217

Cell Manager、Linux の場合、223

Cell Manager、MC/ServiceGuard の場合、217

Cell Manager、Solaris の場合、221

Cell Manager、Windows の場合、215

Oracle 用統合ソフトウェア固有の問題、228

pkgrm ユーティリティ、220、221

rpm ユーティリティ、222、223

インストール サーバのインストール、

Windows の場合、215

インストール サーバ、HP-UX の場合、217

インストール サーバ、Linux の場合、223

インストール サーバ、MC/ServiceGuard の場合、217

インストール サーバ、UNIX の場合、222
概要、213
クライアント、OpenVMS の場合、215
クライアント、リモート、214
クラスタ クライアント、214
前提条件、213

い

移行

HP-UX 用 Cell Manager、PA-RISC から
IA-64 へ、276
Windows 用 Cell Manager、32 ビットから
64 ビットへ、281
ライセンス、A-19
印刷表記法 - 「ドキュメント表記法」を参照
インストール
ADIC/GRAU ライブラリ用の Media Agent、
93, 96
AutoPass ユーティリティ、UNIX の場合、
23, C-7
AutoPass ユーティリティ、Windows の場
合、34
Cell Manager のトラブルシューティング、
Solaris の場合、327
Cell Manager、トラブルシューティング、
321
DB2 用統合ソフトウェア、131
HP StorageWorks EVA 用統合ソフトウェア
、149
HP StorageWorks VA 用統合ソフトウェア、
143
HP StorageWorks XP 用統合ソフトウェア、
136
Informix 用統合ソフトウェア、128
Lotus 用統合ソフトウェア、132
Microsoft Exchange 用統合ソフトウェア、
127
Microsoft SQL 用統合ソフトウェア、128
Microsoft Volume Shadow Copy 用統合ソフ
トウェア、132
NDMP 用統合ソフトウェア、131
NNM 統合ソフトウェア、131
omnisetup.sh、222, 223
Oracle 用統合ソフトウェア、129
pkgadd ユーティリティ、221
SAP DB 用統合ソフトウェア、129
SAP R/3 用統合ソフトウェア、129

StorageTek ACS ライブラリ用の Media
Agent、93, 101

Sybase 用統合ソフトウェア、128
Web Reporting、163

一般的な手順、5

概要、3

各国語版ユーザー インタフェース、156

クライアントのインストール、概要、46

クライアントの確認、330

クライアントのトラブルシューティング、
UNIX の場合、328

クライアント、トラブルシューティング、
326

クライアント、ローカル、63, 108, 115, 119

クラスタ対応 Cell Manager、165, 167

クラスタ対応クライアント、166, 175, 178,
179

クラスタ対応統合ソフトウェア、127

恒久ライセンス パスワード、309 - 313

コンポーネント。インストール コンポーネ
ントを参照。

実行トレース ファイルの作成、336

シングル・サーバ版、161

ソフトウェア コンポーネント、59

ソフトウェア コンポーネント コード、121
デバッグ、336

統合ソフトウェア、124

統合ソフトウェア、概要、124

トラブルシューティング、Windows の場合、
325

リモート インストール、概要、50

リモート、概念、6

ログ ファイル、333

インストール コンポーネント

Disk Agent、3

General Media Agent、3

Media Agent、3

NDMP Media Agent、3

インストール サーバ、3

ユーザー インタフェース、3

インストール サーバのインストール

HP-UX システムの場合

ネイティブ ツールの使用、B-8

Linux システムの場合

ネイティブ ツールの使用、B-12

Solaris システムの場合

ネイティブ ツールの使用、B-8

UNIX システム、37

Windows システム、41

概要, 37
前提条件、UNIX の場合, 37
前提条件、Windows の場合, 41
インストール サーバ
Data Protector A.05.x からのアップグレード、HP-UX の場合, 237, 238
Data Protector からのアップグレード、Windows の場合, 243
アンインストール、HP-UX の場合, 217
アンインストール、Linux の場合, 223
アンインストール、MC/ServiceGuard の場合, 217
アンインストール、UNIX の場合, 222
アンインストール、Windows の場合, 215
インストール概要, 37
インストール順序, 19
インストールの前提条件、UNIX の場合, 37
インストールの前提条件、Windows の場合, 41
インストール、HP-UX、ネイティブ ツールの使用, B-8
インストール、Linux の場合、ネイティブ ツールの使用, B-12
インストール、Solaris の場合、ネイティブ ツールの使用, B-8
インストール、UNIX の場合, 37
インストール、Windows の場合, 41
概念, 3
手動でアップグレード、UNIX の場合, 332
セルへのインポート, 187
ディレクトリ構造、UNIX の場合, 24
インストールのデバッグ, 336
インストールのトラブルシューティング
Cell Manager、Solaris の場合, 327
Cell Manager、UNIX の場合, 27
Cell Manager、Windows の場合, 36
Data Protector ソフトウェア、Windows の場合, 325
debug オプション, 336
Microsoft Installer に関する問題, 325
omnicheck コマンド, 322
swagent デーモン, 329
各国語版ユーザー インタフェース, 159
クライアント、HP-UX, 328
実行トレース ファイル, 336
デバッグ, 336
リモート インストール、Linux の場合, 81
リモート インストール、UNIX の場合, 328
ログ ファイル, 333

インポート
NDMP クライアント, 186
OpenVMS クライアント, 186
インストール サーバ, 187
クライアント, 185
クラスタ, 188
複数の LAN カードが構成されたクライアント, 186

え

エクスポート
Microsoft Cluster Server クライアント, 194
クライアント, 192

お

オペレーティング システム
Windows NT から Windows のより新しいバージョンへのアップグレード, 274

か

カーネル
Linux クライアント上での構成, 82
SCSI ロボティクス ドライバの追加、HP-UX, B-40
再ビルド、HP-UX, B-40
カーネルの再ビルド、HP-UX, B-40
概念
Cell Manager, 3
Disk Agent, 3
IDB ファイル名変換, 262
Media Agent, 3
NDMP Media Agent, 3
インストール サーバ, 3
インポート, 185
エクスポート, 192
クライアント, 3
グラフィカル ユーザー インタフェース (GUI), 13, 14
セル, 3
バックアップ環境, 3
ユーザー インタフェース, 3
リモート インストール, 6

概要

Data Protector A.05.x からのアップグレード, 237
debug オプション, 336
アップグレード, 233

-
- アプリケーション クラスタ パッケージのインポート, 188
 - アンインストール, 213
 - インストール サーバのインストール, 37
 - クライアントのインストール, 46
 - クライアントのリモート インストール, 50
 - クラスタ対応クライアントのインポート, 188
 - クラスタ対応統合ソフトウェアのインストール, 127
 - 実行トレース ファイル, 336
 - 製品構成, 295
 - ソフトウェア コンポーネント, 59
 - ソフトウェア コンポーネントの変更, 226
 - 統合ソフトウェア, 124
 - 統合ソフトウェアのインストール, 124
 - バックアップ デバイスの接続, B-56
 - ライセンス, 306
 - 各国語版ユーザー インタフェースのトラブルシューティング, 159
 - 各国語版ユーザー インタフェース。ユーザー インタフェースを参照。
 - 確認
 - インストールされたライセンス, 314
 - 必要なライセンス パスワード, 307
 - 未使用の SCSI アドレス、HP-UX, B-46
 - 未使用の SCSI アドレス、Solaris の場合, B-48
 - 未使用の SCSI アドレス、Windows の場合, B-54
 - 仮想サーバ、セルへのインポート, 188
 - 環境変数、設定、UNIX 用 Cell Manager, 27
 - き
 - 起動
 - GUI、UNIX, 13
 - 機能拡張、ライセンス, 295
 - く
 - クライアント
 - ADIC/GRAU ライブラリの準備, 94
 - Data Protector A.05.x からのアップグレード, 249
 - Data Protector A.05.x からのアップグレード、MC/ServiceGuard の場合, 250
 - Microsoft Cluster Server、セルからエクスポート, 194
 - root アクセス権限の追加、Linux の場合, 81
 - StorageTek ACS ライブラリの準備, 99
 - TCP/IP の構成、Windows の場合, B-19
 - TCP/IP の設定のチェック、Windows の場合, B-24
 - アクセス確認を解除する, 204
 - アクセス確認を使用可能にする, 199
 - アップグレード、Microsoft Cluster Server 上, 292
 - インストールの確認, 330
 - インストール後の構成、Solaris の場合, 74
 - インストール、概要, 46
 - カーネルの構成、Linux の場合, 82
 - 概念, 3
 - クラスタ対応統合ソフトウェアのインストール、概要, 127
 - クラスタ対応、セルへのインポート, 188
 - 構成、Veritas Volume Manager、Microsoft Cluster Server, B-76
 - セルからのエクスポート, 192
 - セルへのインポート, 185
 - ソフトウェア コンポーネントの変更, 226
 - デバイス ファイルの作成、HP-UX, B-42
 - デバイス ファイルの作成、Solaris の場合, B-52
 - 統合ソフトウェアのインストール、概要, 124
 - トラブルシューティング, 325, 328, 333, 336
 - バックアップ デバイスを使用できるように構成、Solaris の場合, B-49
 - 保護設定, 199
 - 保護の概念, 195
 - ホストからのアクセスの拒否, 204
 - リモート アンインストール, 214
 - リモート インストール、概要, 50
 - ローカル インストール、Novell NetWare, 102
 - ローカル インストール、OpenVMS, 108
 - クライアントのインストール
 - AIX システム, 85
 - HP-UX システムの場合, 68
 - Linux システムの場合, 79
 - MC/ServiceGuard システム, 166
 - Microsoft Cluster Server システム, 175
 - MPE/iX システム, 115
 - Novell NetWare Cluster Services システム, 179
 - Novell NetWare システム, 102
 - OpenVMS システム, 108
 - SCO システム, 91
-

Siemens Sinix システム, 87
Solaris システムの場合, 72
Tru64 システム, 89
UNIX システム, 119
Veritas Cluster システム, 178
Windows システム, 63
クライアント、インストール
ADIC/GRAU ライブラリ用の Media Agent,
96
AIX システム, 85
DB2 用統合ソフトウェア, 131
HP StorageWorks EVA 用統合ソフトウェア
, 149
HP StorageWorks VA 用統合ソフトウェア,
143
HP StorageWorks XP 用統合ソフトウェア,
136
HP-UX システムの場合, 68
Informix 用統合ソフトウェア, 128
Linux システムの場合, 79
Lotus 用統合ソフトウェア, 132
MC/ServiceGuard システム, 166
Microsoft Cluster Server システム, 175
Microsoft Exchange 用統合ソフトウェア,
127
Microsoft SQL 用統合ソフトウェア, 128
Microsoft Volume Shadow Copy 用統合ソフ
トウェア, 132
MPE/iX システム, 115
NDMP 用統合ソフトウェア, 131
NNM 統合ソフトウェア, 131
Novell NetWare Cluster Services システム,
179
Novell NetWare システム, 102
OpenVMS システム, 108
Oracle 用統合ソフトウェア, 129
SAP DB 用統合ソフトウェア, 129
SAP R/3 用統合ソフトウェア, 129
SCO システム, 91
Siemens Sinix システム, 87
Solaris システムの場合, 72
StorageTek ACS ライブラリ用の Media
Agent, 101
Sybase 用統合ソフトウェア, 128
Tru64 システム, 89
UNIX システム, 119
Veritas Cluster システム, 178
Windows システム, 63
シングル・サーバ版, 161

クライアント、バックアップ デバイスの接続
ADIC/GRAU ライブラリ ドライブ, 94
AIX クライアント, 86
HP-UX クライアント, 72
Linux クライアント, 83
SCO クライアント, 92
Siemens Sinix クライアント, 87
Solaris クライアント, 77
Tru64 クライアント, 90
Windows クライアント, 67

クラスタ

Cell Manager のインストール, 167
Microsoft Cluster Server、セルからエクス
ポート, 194
アンインストール, 214
クライアントのインストール, 175, 178, 179
セルへのインポート, 188
ソフトウェア コンポーネントの変更, 226
統合ソフトウェアのインストール, 127
グラフィカル ユーザー インタフェース (GUI)
概念, 13, 14
起動、UNIX, 13
ビュー, 14

け

権限を認められたシステムのリスト、保護,
198

検証

クライアントのインストール, 330
セル内の DNS 接続, 322
パッチ, 211
ライセンス パスワード, 313

こ

恒久ライセンス パスワードの取得とインス
トール, 309 - 313

構成

Cell Manager と Veritas Volume Manager、
MSCS, B-76
Disk Agent、OpenVMS, 112
Media Agent、Novell NetWare, 107
Media Agent、OpenVMS, 113
SCSI ロボティクス、HP-UX, B-37
Solaris クライアント、インストール後, 74
Solaris クライアント、バックアップ デバイ
スの使用前, B-49
sst.conf ファイル, B-51
st.conf ファイル, 74, B-49

TCP/IP、Windows の場合、B-19
カーネル、Linux クライアントの場合、82
クライアントと Veritas Volume Manager、
Microsoft Cluster Server、B-76

構成ファイル

cell_info, 229
Data Protector A.05.x からのアップグレード後の変更のチェック、247
global, 247
inet.conf, B-30
installation_servers, 40
nsswitch.conf, B-30
omni_info, 229
omnirc, 248
sst.conf, B-51
st.conf, B-49
st.conf ファイル、74
アップグレードに関する問題、331
自動構成されるファイル、UNIX 用 Cell Manager, 25
変更、Solaris クライアントのインストール、74
変更、アップグレード後、B-77

国際化、内部データベース (IDB), 262

コマンド

CLI の変更、アップグレード後、B-80
infs, B-42
ioscan, B-39, B-42, B-46
netstat, B-28
omnicc, 305
omnicheck, 212, 322
omnisetup.sh, 120, 158, 238, 241, C-11
omnisv, 237

コマンド行インタフェース (CLI), 3, 13

さ

削除

Data Protector ソフトウェアを手作業で、UNIX の場合、224
クライアントのアクセス確認、204
ソフトウェア コンポーネント、UNIX の場合、227, 229
ソフトウェア コンポーネント、Windows の場合、226
ソフトウェア コンポーネント、概要、226

作成

実行トレース ファイル、インストール、336
デバイス ファイル、HP-UX, B-42

デバイス ファイル、Solaris の場合、B-52
デバイス ファイル、Windows の場合、B-35
サブネット マスク、TCP/IP, B-19

し

実行トレース ファイル

debug オプション、336
作成、336
準備、NIS サーバ、B-30
使用

SCSI テープドライバ、Windows の場合、B-32

ライセンス、233, 237

ログ ファイル、333

シングル・サーバ版

Data Protector A.06.00 SSE へのアップグレード、271

Data Protector A.06.00 へのアップグレード、271

インストール、161

制限事項、161

製品概要、ライセンス、A-3

複数のシステムからのアップグレード、272

ライセンスのタイプ、A-17

す

スターター パック、ライセンス、295

せ

制限事項

Manager-of-Managers のアップグレード、235

UNIX システム、119

Windows システム、41, 63

アップグレード、233

シングル・サーバ版、161

設定

SCSI ID、HP StorageWorks 330fx ライブラリ、B-55

SCSI コントローラ パラメータ、Windows の場合、B-45

環境変数、UNIX 用 Cell Manager, 27

セル

DNS、接続の確認、322

Microsoft Cluster Server クライアントのエクスポート、194

アップグレード、概要、234

インストール サーバのインポート、187

概念, 3

- クライアントのインポート, 185
- クライアントのエクスポート, 192
- クライアントの保護設定, 199
- クラスタのインポート, 188
- 保護を使用可能にする, 202
- ライセンス, 295, 296

前提条件

- Cell Manager のインストール、UNIX の場合, 20
- Cell Manager のインストール、Windows の場合, 29
- Data Protector A.05.x からのアップグレード, 237
- インストール サーバのインストール、UNIX の場合, 37
- インストール サーバのインストール、Windows の場合, 41

そ

ソフトウェア コンポーネント

- 依存関係、HP-UX の場合, 227
- 依存関係、Solaris の場合, 228
- 概要, 59
- コンポーネント コード, 121
- 削除、UNIX の場合, 227, 229
- 削除、Windows の場合, 226
- 追加、HP-UX の場合, 227
- 追加、Solaris の場合, 228
- 追加、Windows の場合, 226
- 変更、概要, 226
- 変更、クラスタ クライアントの場合, 226

ソフトウェア コンポーネントの追加

- HP-UX システムの場合, 227
- Solaris システムの場合, 228
- Windows システムの場合, 226
- 概要, 226

た

- ターミナルサービスクライアント, 29
- 大量のログの記録, 205

ち

チェック

- General Media Agent のインストール、Novell NetWare, B-71
- TCP/IP の設定、Windows の場合, B-24
- クライアントのインストール, 330

パッチ, 211

- ライセンス, 296
- ログ ファイル、インストール, 333

つ

追加

- アクセス権限、Linux の場合, 81
- カーネルに SCSI ロボティクスドライバを追加、HP-UX, B-40

て

- データベースのサイズ増加。IDB を参照。
- テープドライバ。SCSI インタフェースを参照。
- デバイス ファイル
 - 作成、HP-UX, B-42
 - 作成、Solaris の場合, B-52
 - 作成、Windows の場合, B-35
- デフォルト ゲートウェイ、TCP/IP, B-19
- デフォルト ポート、変更, B-28

と

- 統合クライアント, 124
 - 統合ソフトウェアも参照。
- 統合ソフトウェア
 - EVA, 258
 - Informix のアップグレード、UNIX の場合, 253
 - Informix のアップグレード、Windows の場合, 254
 - Oracle のアップグレード、Windows の場合, 251
 - Oracle、UNIX の場合, 251
 - SAP R/3 のアップグレード、Windows の場合, 253
 - SAP R/3、UNIX の場合, 253
 - Sybase のアップグレード、UNIX の場合, 255
 - Sybase のアップグレード、Windows の場合, 257
 - アップグレード、EVA, 258
 - 概要, 124
 - クラスタ対応、インストール, 127
 - リモート インストール, 126
 - ローカル インストール, 126
- 統合ソフトウェア、インストール
 - DB2 用統合ソフトウェア, 131

-
- HP StorageWorks EVA 用統合ソフトウェア , 149
- HP StorageWorks VA 用統合ソフトウェア , 143
- HP StorageWorks XP 用統合ソフトウェア , 136
- Informix 用統合ソフトウェア , 128
- Lotus 用統合ソフトウェア , 132
- Microsoft Exchange 用統合ソフトウェア , 127
- Microsoft SQL 用統合ソフトウェア , 128
- Microsoft Volume Shadow Copy 用統合ソフトウェア , 132
- NDMP 用統合ソフトウェア , 131
- NNM 統合ソフトウェア , 131
- Oracle 用統合ソフトウェア , 129
- SAP DB 用統合ソフトウェア , 129
- SAP R/3 用統合ソフトウェア , 129
- Sybase 用統合ソフトウェア , 128
- ドキュメント表記法 , xiii
- ドメイン ネーム システム。DNS を参照。
- ドライブ・ライセンス , 295
- トラブルシューティング
- Cell Manager のインストール、Windows, 321
 - クライアントのインストール、Windows, 326
- トレース ファイル。実行トレース ファイルを参照。
- ね**
- ネットワーク トラフィックの最小化、Novell NetWare クライアント , 106
- は**
- バックアップ デバイス
- SCSI ID の設定、HP StorageWorks 330fx ライブラリ , B-55
- バックアップ デバイスの接続
- ADIC/GRAU ライブラリ ドライブ , 94
 - AIX クライアント , 86
 - HP StorageWorks DAT 24 テープドライブ , B-60
 - HP StorageWorks DLT ライブラリ 24/48 スロット , B-63
 - HP Surestore 12000e オートローダー , B-61
 - HP-UX クライアント , 72
 - Linux クライアント , 83
 - SCO クライアント , 92
 - Seagate Viper 200 LTO テープドライブ , B-68
 - Siemens Sinix クライアント , 87
 - Solaris クライアント , 77
 - Tru64 クライアント , 90
 - Windows クライアント , 67
- 概要 , B-56
- バックアップ デバイス、接続
- ADIC/GRAU ライブラリ ドライブ , 94
 - AIX クライアント , 86
 - HP StorageWorks DAT 24 テープドライブ , B-60
 - HP StorageWorks DLT ライブラリ 24/48 スロット , B-63
 - HP Surestore 12000e オートローダー , B-61
 - HP-UX クライアント , 72
 - Linux クライアント , 83
 - SCO クライアント , 92
 - Seagate Viper 200 LTO テープドライブ , B-68
 - Siemens Sinix クライアント , 87
 - Solaris クライアント , 77
 - Tru64 クライアント , 90
 - Windows クライアント , 67
- 概要 , B-56
- バックアップ環境の概念 , 3
- パッチ
- omnicheck コマンド , 212
 - 検証 , 211
- ひ**
- ビュー、グラフィカル ユーザー インタフェース , 14
- 表記法、ドキュメント , xiii
- ふ**
- ファイル
- allow_hosts, 201, 203, 204
 - deny_hosts, 204
 - HPDEVBRA.NLM, B-74
 - HPUMA.NLM, B-74
 - services, B-28
- ファイル名
- エンコーディング。IDB ファイル名変換を参照
 - 変換。IDB ファイル名変換を参照
-

ファイル名の変換。IDB ファイル名変換を参照

複数の LAN カードが構成されたクライアント、インポート、186
プロセス

Cell Request Server (CRS) サービス、26, 35

Data Protector Inet サービス、36

Media Management Daemon (MMD) サービス、27

Raima Database Server (RDS) サービス、27, 36

へ

変更

Cell Manager 名、B-26

ソフトウェア コンポーネント、226

デフォルト ポート、B-28

ほ

保護

allow_hosts ファイル、201, 203, 204

deny_hosts ファイル、204

inet_log ファイルに大量のログが記録される場合、205

クライアントのアクセス確認を解除する、204

クライアントの保護を使用可能にする、199

権限を認められたシステムのリスト、198

セルの保護を使用可能にする、202

潜在的な問題点、198

ホストからのアクセスの拒否、204

保護設定

クライアント、199

セル、202

ホストからのアクセスの拒否、204

ま

マルチバイト文字、262

み

未使用の SCSI アドレス。SCSI インタフェースを参照。

ゆ

ユーザー インタフェース
概念、3

各国語版ユーザー インタフェースのインストール、156

各国語版ユーザー インタフェースのインストールのトラブルシューティング、159

コマンド行インタフェース (CLI)、グラフィカル ユーザー インタフェース (GUI) を参照。

システムの選択、13

ら

ライセンス

AutoPass ユーティリティ、309

Cell Manager 関連ライセンス、296

Data Protector A.05.x からのアップグレード、237

Data Protector A.05.x ライセンスの移行、A-19

SSE からのアップグレード、271

一時パスワード、308

インストールされたライセンスの確認、314

エンティティ・ベース使用権、297

概要、306

機能拡張、295, A-8

キャパシティ・ベース使用権、297

キャパシティ・ベース使用権、例、301 - 304

緊急用パスワード、308

恒久パスワード、308

恒久パスワードの取得とインストール、309 - 313

集中ライセンス、構成、316

取得とインストール、恒久パスワード、309 - 313

シングル・サーバ版、A-17

スターターパック、295

製品概要、A-3

製品構成、295, A-2

製品ライセンスの概要、306

ドライブ使用権、A-5

ドライブ・ライセンス、295

パスワードの検証、313

パスワードのタイプ、308

必要なパスワードの確認、307

ライセンス フォーム、A-25

ライセンス レポートの生成、305

ライセンスの移行、A-19

ライセンスの移動、314

ライセンスの使用、アップグレード後 , 237,
271

ライセンスのチェックとレポート , 296

ライセンス フォーム , A-25

ライセンスの移動 , 314

ライセンスのレポート , 296

リ

リモート インストール

クライアント , 50

統合ソフトウェア , 126

トラブルシューティング、Linux の場合 , 81

ろ

ローカル インストール、クライアント , 63,
108, 115, 119

ログ ファイル

inet.log, 201, 203, 205, 288

説明 , 334

チェック、インストール , 333

保存場所 , 334

ロボティクス。SCSI インタフェースを参照。

